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 ∞.

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 ∞ 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 $l = nk + r$, $r \in \{0, 1, \ldots, n-1\}$, then $a^l = a^{nk+r} = (a^n)^k a^r = e^k a^r = a^r$. So

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

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

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

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** $\varphi : G \to G'$ 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 $\varphi(a^{-1}) = \varphi(a)^{-1}$

Mon. 5 Feb 2024

Recall: A **Homomorphism** is a function $\varphi : G \to G'$ satisfying $\varphi(ab) = \varphi(a)\varphi(b)$.

When we talk about functions, we like to talk about the *image* of that function.

Definition.

The **image** (or **range**) of φ is $\varphi(G) = \{\varphi(a) \mid a \in G\}$ is the set of all outputs of φ on its domain.

Definition.

The **Kernel** of φ is $\ker(\varphi) = \{a \in G \mid \varphi(a) = e_{G'}\}$.

A vector space under addition is actually a group!

Proposition

1. $\varphi(G)$ is a subgroup of G'. The image is a subgroup of the codomain.

   Closure

   If $\varphi(a), \varphi(b) \in \varphi(G)$, then $\varphi(a)\varphi(b) = \varphi(ab)$ since φ is a Homomorphism. But notice that $\varphi(ab) \in \varphi(G)$, so we have closure.

   Inverses

   If $\varphi(a) \in \varphi(G)$, then $\varphi(a)^{-1} = \varphi(a^{-1}) \in \varphi(G)$, so it's a subgroup.

2. $\ker(G)$ is a subgroup of G. The kernel is a subgroup of the domain.

   Closure

   If $a, b \in \ker(\varphi)$, $\varphi(ab) = \varphi(a)\varphi(b) = e \cdot e = e$, so $\varphi(ab) \in \ker(\varphi)$.

   Inverses

   If $a \in \ker(\varphi)$, then $\varphi(a^{-1}) = \varphi(a)^{-1} = e^{-1} = e$, so $a^{-1} \in \ker(\varphi)$.

Let's look at an

Example.

Consider the determinant function $\det : \mathrm{GL}_n(\mathbb{R}) \to (\mathbb{R} \setminus \{0\}, \times)$, $A \to \det(A)$

Here, the determinant is onto, so $\det(\mathrm{GL}_n(\mathbb{R})) = \mathbb{R} \setminus \{0\}$. Additionally,

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

To prove that something is a subgroup, it's often useful to find a homomorphism whose kernel (or image) is a subgroup.

Consider the following

Example.

$\exp(\mathbb{R}, +) \to (\mathbb{R} \setminus \{0\}, \times)$ is a homomorphism, $x \to e^x$.

$\exp(\mathbb{R}) = \{x \in \mathbb{R} \mid x > 0\}$, and $\ker(\exp) = \{x \in \mathbb{R} \mid \exp(x) = 1\} = \{0\}$.

Proposition:

$\varphi : G \to G'$ is one to one if and only if $\ker(\varphi) = \{e\}$.

Proof:

($\Rightarrow$): $\varphi(e) = e$, so $e \in \ker(\varphi)$.

If $a \neq e$ and $a \in \ker(\varphi)$, then $\varphi(a) = \varphi(e) = e$ so φ is not injective, and we have a contradiction. Thus $\ker(\varphi) = \{e\}$.

($\Leftarrow$): If $\varphi(a) = \varphi(b)$, then $\varphi(a)\varphi(b)^{-1} = e$, but then $\varphi(a)\varphi(b^{-1}) = \varphi(ab^{-1}) = e$ but since only $\varphi(e) = e$, this means $ab^{-1} = e$ and so $a = b$ and so φ is injective.

4.2 Isomorphisms

Definition.

An **Isomorphism** $\varphi : G \to G'$ is a bijective homomorphism.

Note.

To check that something is an Isomorphism, you need to check two things:

1. It's a Homomorphism
2. It's a Bijection.

   Note that if the function sets are finite, you only need to prove either one to one-ness or onto-ness and the other should follow. Think about why!

4.2.1 Examples

Some examples include:

- $\exp : (\mathbb{R}, \times) \to (\mathbb{R}_{>0}, \times)$
- $\varphi' : (\mathbb{Z}, +) \to \langle a \rangle \leq G$ is an isomorphism **if and only if** $|a| = \infty$.

  This should make sense, as we never get the identity by a non-zero power of a.
- Given any $A \in \mathrm{GL}_n(\mathbb{R})$, the linear map $f_A : (\mathbb{R}^n, +) \to (\mathbb{R}^n, +)$ that sends $\bar{x} \to A\bar{x}$ is an isomorphism.

- If $a \in G$, the map $\varphi_a : G \to G$ that sends $b \to aba^{-1}$ is an isomorphism, called **conjugation by** a

  Check:

  1. **Homomorphism**

$$\begin{aligned}\varphi(bc) &= a(bc)a^{-1} = abeca^{-1} \\ &= (aba^{-1})(aca^{-1}) \\ &= \varphi_a(b)\varphi_a(c)\end{aligned}$$

  2. **One to One**:

     If $\varphi_a(b) = e$, then $aba^{-1} = e$, then $a^{-1}aba^{-1}a = a^{-1}a$, and so $b = e$, so φ_a is injective.

  3. **Onto**: If $c \in G$, we want $b \in G$ such that $\varphi_a(b) = c$, i.e. $aba^{-1} = c$.

     So choose $b = a^{-1}ca$, then $\varphi_a(b) = aba^{-1} = a(a^{-1}ca)a^{-1} = c$, so φ_a is surjective.

Proposition: If $\varphi : G \to G'$ is an isomorphism, then $\varphi^{-1} : G' \to G$ is also an isomorphism.

Proof:

Since isomorphisms are bijections, it suffices to show that φ^{-1} is a homomorphism.

If $x, y \in G'$, we want to show that $\varphi^{-1}(xy) = \varphi^{-1}(x)\varphi^{-1}(y)$.

Say $\varphi^{-1}(x) = a$, $\varphi^{-1}(y) = b$, and $\varphi^{-1}(ab) = c$. Then we want to show that $ab = c$.

Then $ab = c$ if and only if $\varphi(ab) = \varphi(c)$ (since φ is bijective, in fact injectivity is sufficient for this.)

But then this is true if and only if $\varphi(a)\varphi(b) = \varphi(c)$, if and only if $\varphi(\varphi^{-1}(x))\varphi(\varphi^{-1}(y)) = \varphi(\varphi^{-1}(xy))$, if and only if $xy = xy$. Thus $ab = c$ and φ^{-1} is a homomorphism.

$$\begin{aligned} ab = c &\Leftrightarrow \varphi(ab) = \varphi(c) \\ &\Leftrightarrow \varphi(a)\varphi(b) = \varphi(c) \\ &\Leftrightarrow \varphi(\varphi^{-1}(x))\varphi(\varphi^{-1}(y)) = \varphi(\varphi^{-1}(xy)) \\ &\Leftrightarrow xy = xy \end{aligned}$$

Definition.

G and G' are **isomorphic** if there exists an isomorphism $\varphi : G \to G'$.

Note again that since isomorphisms are bijective, this means that the isomorphism goes both ways.

We write $G \cong G'$ or $G \backsimeq G'$, but mostly the former.

Note.

The goal of this class is to give a good classification to a lot of groups. Note that it's not really possible to completely do this, even for groups of a given order, because we have infinitely many possible groups of order one, but that's okay because there's an isomorphism between.

We say that we care about these groups *up to isomorphism*.

What this means is that if we have two groups that are isomorphic, we're going to treat them as the same. When classifying or counting, we can count G and G' are one if $G \cong G'$.

Exercise. There is only one group of order one up to isomorphism.

So if $|G| = |G^{-1}| = 1$, then $G \cong G'$.

Next week we'll talk about specific types of groups and take a break from the theory.

Wed 07 Feb 2024

5 Important Groups

5.1 Groups mod n

$$\mathbb{Z}_n = \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$$

Under $+$.

These are all cyclic, and in fact $\mathbb{Z}_n = \langle \bar{1} \rangle$.

Theorem:

Any cyclic (sub)group is isomorphic to $\mathbb{Z}$ or $\mathbb{Z}_n$, for $n \geq 2$.

Proof Idea:

Write $f : \mathbb{Z}$ or $\mathbb{Z}$ to $\langle a \rangle$ which takes k or $\bar{k}$ to a^k.

Chose $n = |a|$ or $\mathbb{Z}$ if $|a| = \infty$.

We know that subgroups of cyclic groups are cyclic (from Homework 1.) So any subgroup of $\mathbb{Z}_n$ is $H = \langle \bar{m} \rangle$ for some $\bar{m}$.

Example.

If $f|n$, then there exists some subgroup $H \leq \mathbb{Z}_n$ with $|H| = f$.

5.2 Multiplicative Groups

In what context can we define a group under multiplication for subsets of the integer $\pmod n$?

If $\bar{a}$ is multiplicatively invertible $\pmod n$, then there exists a $\bar{n} \in \mathbb{Z}_n$ with $\bar{a} \cdot \bar{b} = \bar{1}$.

We know that $(\mathbb{Z}_4, \times)$, for example, is not a group. So when *is it* a group?

We know that

$$\begin{aligned} \bar{a} \cdot \bar{b} = \bar{1} &\Leftrightarrow ab \equiv 1 \pmod n \\ &\Leftrightarrow \exists k \in \mathbb{Z} \text{ such that } ab = 1 + nk \\ &\Leftrightarrow \exists k \in \mathbb{Z} \text{ with } ab + n(-k) = 1 \\ &\Leftrightarrow \gcd(a, n) = 1 \end{aligned}$$

Let's define $\mathbb{Z}_n^\times = \{\bar{a} \in \mathbb{Z}_n \setminus \{\bar{0}\} \mid \gcd(a, n) = 1\}$

Theorem:

$(\mathbb{Z}_n^\times, \times)$ is a group.

Proof: Omitted.

Example.

$\mathbb{Z}_4^\times = \{\bar{1}, \bar{3}\}$, and looking at the multiplication table

- $\bar{1} \cdot \bar{1} = \bar{1}$
- $\bar{1} \cdot \bar{3} = \bar{3}$
- $\bar{3} \cdot \bar{1} = \bar{3}$
- $\bar{3} \cdot \bar{3} = \bar{1}$

And in fact, we see that $\mathbb{Z}_4^\times \cong (\mathbb{Z}_2, +)$, Where φ takes $\bar{1}$ to $\bar{0}$, and $\bar{3}$ to $\bar{1}$.

Example.

Let's look at $\mathbb{Z}_8^\times = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$.

In $\mathbb{Z}_8^\times$, every element $\bar{a}$ satisfies $\bar{a}^2 = \bar{1}$, so $\mathbb{Z}_8^\times \cong \mathbb{Z}_4$, because in $\mathbb{Z}_4$, $\bar{1} + \bar{1} \neq \bar{0}$ and $\bar{3} + \bar{3} = \bar{0}$.

So they are not isomorphic. If there were, say f, it would be surjective, we could pick $\bar{a} \in \mathbb{Z}_8^\times$ with $f(\bar{a}) = \bar{1}$, then $f(\bar{a} \cdot \bar{a}) = f(\bar{a}) + f(\bar{a})$ but this can't be the case.

Corollary: $\mathbb{Z}_n^\times = \mathbb{Z}_n \setminus \{0\}$ if and only if n is prime.

So $\mathbb{Z}_p^\times = \{\bar{1}, \ldots, \overline{p-1}\}$ is a group under $\times$ when p is prime.

Note.

These are **not** subgroups of Z_n, they have a *different* binary operation! These groups are under multiplication while $\mathbb{Z}_n$ is under addition.

5.3 Symmetric Groups

Recall the definition of S_n

$$\begin{aligned} S_n &= \{ \text{ all permutations of } \{1, \ldots, n\}\} \\ &= \{ \text{ all bijections } \{1, \ldots, n\} \to \{1, \ldots, n\}\} \end{aligned}$$

Furthermore, recall that $S_n = n!$.

Example.

Consider S_4, we say that $\sigma \in S_4$ is a function $\sigma : \{1, 2, 3, 4\} \to \{1, 2, 3, 4\}$ with

- $1 \mapsto 2$
- $2 \mapsto 4$
- $3 \mapsto 3$
- $4 \mapsto 1$

This is really cumbersome to write so instead, we write

TODO Oh my god I can't tex this. See picture

Or,

$$\sigma = (124)(3) = (241)(3) = (3)(412)$$

Because 1, 2, 4 forms a cycle, and 3 is a self loop. And this uniquely describes the picture! Although this notation is compact, it's not unique. This is known as *cycle notation*.

If the group S_4 is understood, we can write $(124)(3)$ as 124. We have a tendency to just leave off the 1-cycles.

Example.

Let's do some multiplication.

$\sigma^2 = (124)(124)$. To do this, we first draw the picture.

TODO

And to do σ^2, we follow the arrows twice (we do σ twice!)

So $\sigma^2 = (142)$.

Example.

Let $\sigma = (124)$, and $\tau = (12)(34)$, what is $\tau\sigma$?

Again, we can draw the graphs.

TODO

Note that order matters here! It may not always be the case that $\sigma\tau$ equals $\tau\sigma$.

So $\tau\sigma = (12)(34)(124) = (234)$.

QUESTION How would I simplify $(123)(136)$?

Note.

It should make sense that $(123) = (12)(23)$, and more generally,

$$(a_1 a_2 \cdots a_k) = (a_1 a_2)(a_2 a_3) \cdots (a_{k-1} a_k)$$

A 2-cycle (a, b) is called a **transposition**. Every $\sigma \in S_n$ can be written as a product of transpositions.

Definition.

$\sigma \in S$ is **even** if it's the product of an even number of transpositions.

$\sigma \in S_n$ is **odd** if it's the product of an odd number of transpositions.

Proposition:

No $\sigma \in S_n$ is both even and odd.

Proof

(My idea here is that you can probably represent the permutation as a graph and color the vertices and make some statement about where it takes you or something like that.)

Next time!

What we get out of this is a map $\text{sgn} : S_n \to (\{\pm 1, \times\})$ with

$$\sigma \to \begin{cases} 1 & \sigma \text{ even} \\ -1 & \sigma \text{ odd} \end{cases}$$

Claim: sgn is a homomorphism called the *signature* homomorphism.

Fri. 9 Feb 2024

Today we keep talking about the symmetric group and introduce the *Dyhedral Group!*

Recall: Last time, we defined S_n is the symmetric group of permutations. We talked about transpositions, $(ab) \in S_n$ for $a \neq b$ every element $\sigma \in S_n$ can be written as a product of transpositions

Example.

We said that $(1234) = (12)(23)(34)$.

TODO More graphs here. Explain how this works.

Recall: Last time, we said that $\sigma \in S_n$ is **even** if it can be written as product of an even number of transpositions, or $\sigma \in S_n$ is **odd** otherwise. We also claimed that it couldn't be both.

We can consider the following table

	σ even	σ odd
τ even	even	odd
τ odd	odd	even

Hence $\text{sgn} : S_n \to (\{\pm 1\}, \times)$ defined as

$$\text{sgn}(\sigma) = \begin{cases} 1 & \sigma \text{ even} \\ -1 & \sigma \text{ odd} \end{cases}$$

is called the signature.

The kernel $\ker(\text{sgn})$ is a subgroup of S_n called the **alternating group** A_n

$$A_n = \{\sigma \in S_n \mid \sigma \text{ even}\}$$

QUESTION Why is it that $\ker(\text{sgn}) = A_n$? I thought that A_n was the subset of S_n for which the permutation was even? Also, isn't the kernel of a function just the subset of the function that maps to the identity? even permutations don't map to the identity, what's going on with that?

Let's look at an

Example.

$S_4 = \{e, (12), (13), (14), (23), (24), (34), (123), (132), (124), (142), (134), (143), (234), (243), (12)(34), (1$

and

$A_4 = \{e, (123), (132), (124), (142), (134), (143), (234), (243), (12)(34), (13)(24), (14)(23), \}$

Fact: $|S_n| = n!$ so $|A_n| = n!/2$.

Let's talk about order of elements.

Suppose we have a cycle $(12 \dots k)$. What's the order of this cycle?

Since $\sigma^j(1) = j$, so if we want $\sigma^j(1) = 1$ with $j < k$, we need $j = k$. And moreover, $\sigma^k(i) = i$ which means that $\sigma^k = e$.

If σ has cycle notation, that is the product of a k-1 cycle, a k-2 cycle... Then

$$|\sigma| = \text{lcm}(k_1, k_2, \dots)$$

Let's look at some

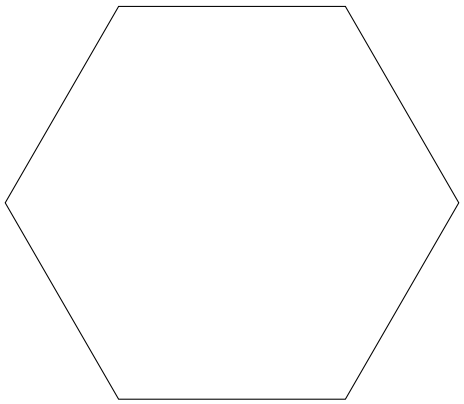
Example.

- $|(12)(345)| = \text{lcm}(2, 3) = 6$
- $|(12)(34)| = \text{lcm}(2, 2) = 2$
- $|(12)(23)(34)| = |(1234)| = 4$

  This looks like a bunch of 2-cycles, but it's actually a 4-cycle. Be sure to use cycle notation to figure this out!

6 Symmetry Groups

Consider a regular polygon



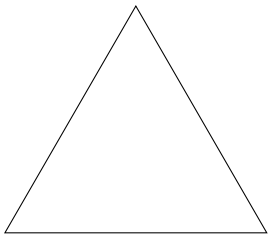
TODO This looks so bad

We call this D_{2n}, the group of symmetries of a regular n-gon, also known as the **Dyhedral Group** of order $2n$.

We have that D_n is generated by 2 elements, ρ, its rotations, and μ, its reflections. Furthermore, $\rho^n = e$, $\mu^2 = e$, and $(\mu\rho)^2 = e$. We say that $D_n = \langle \rho, \mu \rangle$.

Example.

$D_6 = \{e, y, y^2, x, yx, y^2x\}$ is the symmetries of a triangle.



To keep track of what's going on, put names on your vertices.

There are only 6 possible symmetries of this group. Symmetries are determined by where the labels on the vertices go.

Consider an n-gon and take A_1, any vertex of this n-gon. You can take A_1 to any of n vertices, then chose whether to put A_2 (a neighbor of A_1) clockwise or counter-

clockwise of A_1. Then, everything else is determined!

Note.

D_{2n} is **not** Abelian. Simply convince yourself that rotate then reflect is *different* from reflect, then rotate. If you're not convinced, draw it!

Example.

In D_{2n}, if x is a reflection, y is not counter-clockwise by $2\pi/n$ radians

Fact: $D_{2n} \leq S_n$ for $n \geq 3$. Since symmetry in D_{2n} is a permutation of vertex labels.

Exercise: Show that $D_6 \cong S_3$.

Definition.

If $H \leq G$, define

$$aH = \{ah \mid h \in H\} \subseteq G$$

is called a **left coset** of H, with $a \in G$ fixed.

Proposition: If we have a homomorphism $\varphi : G \to G'$, and $a, b \in G$, then if $K = \ker(\varphi)$ (which remember is a subgroup of G), then

$$\varphi(a) = \varphi(b) \Leftrightarrow a^{-1}b \in K \Leftrightarrow b \in aK \Leftrightarrow aK = bK$$

What we have is that cosets determine when elements map to the same spot under a homomorphism.

Proof:

$\varphi(a) = \varphi(b) \Leftrightarrow \varphi(a)^{-1}\varphi(b) = e \Leftrightarrow \varphi(a^{-1}b) = e \Leftrightarrow a^{-1}b \in K \Leftrightarrow a^{-1}b = k$ for some $k \in K$, which is true if and only if $b = ak$ for some $k \in K$, again if and only if $b \in aK$

$$\begin{aligned}
&\varphi(a) = \varphi(b) \\
\Leftrightarrow &\varphi(a)^{-1}\varphi(b) = e \\
\Leftrightarrow &\varphi(a^{-1}b) = e \\
\Leftrightarrow &a^{-1}b \in K \\
\Leftrightarrow &a^{-1}b = k \\
\Leftrightarrow &ab = k
\end{aligned}$$

TODO

Similarly, $a \in bK$.

> **Example**.
>
> $a \in bk$ and $b \in ak$ if and only if $aK = bK$.

In fact, for any subgroup $H \leq G$, $a^{-1}b \in H \Leftrightarrow b \in aH \Leftrightarrow aH = bH$.

So given $H \leq G$, define a relation $\sim$ no G by $a \sim b \Leftrightarrow a \in bH$. But by the above, this true if and only if $aH \Leftrightarrow bH$. Hence $\sim$ is an equivalence relation.

What we get out of this is that

1. **the cosets of H partition G.**
2. The number of cosets of H is the index of $H \in G$, written $[G : H]$, which may be ∞.

QUESTION How do we compute $[G : H]$?

Mon 12 Feb 2024

> **Note**.
>
> - Homework 3 is due Thursday this week
> - Midterm 1 is two Fridays from today.
>
> Exam content will be up until Monday, and there will be a review on Wednesday.

7 Cosets

Recall: If $H \leq G$, and $a \in G$, the *left coset* $aH = \{ah \mid h \in H\}$.

Last time we saw that $a \in bH$ if and only if $b \in aH$, if and only if $aH = bH$, which gives us this equivalence relation $a \sim b \Leftrightarrow a \in bH$, which means we get a partition on the set G of this group, and it's partitioned on the cosets! So the cosets of H partition G.

Lemma: The size of any coset is the same as the original size of the subgroup for any element $a \in G$. In other words, all cosets are the same size!

Proof: We can write a map $f : H \to aH$ where $h \mapsto ah$.

Let's prove that this is bijective.

- **Injective**: If $f(h) = f(h')$, then $ah = ah'$, but then because this is a group, we can multiply by a^{-1} on both sides and so $h = h'$.
- **Surjective**: Given $ah \in aH$, then $f(h) = ah$.

So f is a bijection, so $|H| = |aH|$.

> **Note**.
>
> We only care about this when our sets are finite! In that case, injectivity and surjectivity are the same **as long as the domain and codomain are the same size!**

We finally get to one of the landmars of Group Theory, this is

8 Lagrange's Theorem

Theorem.

If $H \leq G$ and G is finite, then $|H|$ divides $|G|$.

> **Proof.**
> The cosets of H partition G, and all have the same size. Therefore

$$|G| = \sum_{aH} |aH| = \sum_{[G:H]} = |H|[G:H]$$

Where aH is a left coset of G.

Furthermore, $|H|$ divides $|G|$ and $[G:H] = \frac{|G|}{|H|}$

■

Corollary.

If $a \in G$, then $|a|$ divides $|G|$

Proof
$|a| = |\langle a \rangle|$ and $\langle a \rangle \leq G$ so we are done by Lagrange's Theorem.

■

Note.

The converse is not necessarily true!

Corollary.

If $|G| = p$ a prime, then G is cyclic.

Proof
Take $a \in G$, $a \neq e$, then $|a| \neq 1$ (because its not the identity.) But $|a| \mid p$, so in fact $|a| = p$. But $|G| = p$ and $\langle a \rangle \leq G$, and $\langle a \rangle = G$, so G is cyclic.

In fact, every element in G which is not the identity is a generator of the group!

■

Lemma.

If G, G' are cyclic groups of order n, then $G \cong G'$.

Proof.
We saw that $G \cong \mathbb{Z}_n$, and $G' \cong \mathbb{Z}_n$, and so it follows that $G \cong G'$.

■

Corollary.

All order p groups, p a prime, are isomorphic.

Proof
Proof Omitted. It just follows from everything we've seen so far!

Up to isomorphism, there is only one group of order p.

■

Let's go back and talk about those left cosets.

Remark. We can also define **right cosets**

$$Ha = \{ha \mid h \in H\}$$

And in fact, everything we proved so far could have worked with right cosets too!

A priori, the partitions generated by a left and right coset might be different.

Definition.

A subgroup $H \leq G$ is a **normal subgroup** if

$$aH = Ha$$

for all $a \in G$. We write $H \trianglelefteq G$.

If $\varphi : G \to G'$ is a homomorphism, then $K = \ker(\varphi)$ is normal. The claim here is that kernels are normal subgroups.

Proof:

Given $a \in G$, $aK = \varphi^{-1}(\varphi(a)) = \{b \in G \mid \varphi(b) = \varphi(a)\}$. Since the inverse function might not exist, we're just looking for the *pre-image* here (Recall the proposition from last week.)

Note.

We could have redone this proposition with right cosets!

$$aK = Ka$$

We have lots of normal subgroups because we have lots of Homomorphisms.

Example.

- $\text{sgn} : S_n \to (\{\pm 1\}, \times)$ with

$$\sigma \mapsto \begin{cases} 1 & \sigma \text{ even} \\ -1 & \sigma \text{ odd} \end{cases}$$

- $\ker(\text{sgn}) = An$ implies $An \trianglelefteq S_n$.

An alternative way to prove that $H \trianglelefteq G$:

$aH = Ha$ if and only if $aHa^{-1} = H$.

Note.

Warning:

- If $ah \in aH = Ha$, it's **not necessarily the case** that $ah = ha$.

  Remember, the sets are equal, but not necessarily the elements! Instead, $ah = h'a$ for some $h' \in H$.

- Similarly, $aha^{-1} = h^{-1}$, not necessarily h.

Normal subgroups are perfectly designed for doing algebra with cosets! $H \trianglelefteq G$, then

$$(aH)(bH) = \{(ah)(bh') \mid h, h' \in H\}$$

What is this set?, Well

$$\begin{aligned}(aH)(bH) &= \{(ah)(bh') \mid h, h' \in H\} \\ &= \{a \underbrace{(hb)}_{\in Hb=bH} h' \mid h, h' \in H\} \\ &= \{a(bh'')h' \mid h', h'' \in H\} \\ &= \{(ab)(h''h') \mid h', h'' \in H\}\end{aligned}$$

As h' and h'' range over H, we get all elements of H. So this set is (ab) times all elements of H, so we have

$$(aH)(bH) = (ah)H$$

Alternatively, we may write

$$\begin{aligned}aHbH = a(Hb)H = a(bH)H \\ = ab(HH) = abH\end{aligned}$$

With these cosets, we can form new groups! This multiplication of cosets is a binary operation on the set of cosets.

In order to simplify notation, let $\bar{a} = aH$, and we let

$$G/H = \{aH \mid a \in G\} = \{\bar{a} \mid a \in G\}$$

With binary operation $\bar{a} \cdot \bar{b} = \overline{ab}$

Claim: G/H is a group, and furthermore, $\pi : G \to G/H$ where $a \mapsto \bar{a}$, is a group homomorphism, with $\ker(\pi) = H$.

> **Definition**.
>
> G/H is called the **quotient group** of G by H.

Proof of Claim:

- **Proof of Group**
  - **Associativity**: $(\bar{a} \cdot \bar{b}) \cdot \bar{c} = \overline{ab} \cdot \bar{c} = \overline{(ab)c}$. Since G is associative, $\overline{(ab)c} = \overline{a(bc)}$ and furthermore, $\bar{a} \cdot \overline{bc} = \bar{a}(\bar{b} \cdot \bar{c})$.
  - **Identity**: $\bar{e} = eH = H$ is the identity.
  - **Inverses**: $\overline{a^{-1}} \cdot \overline{a} = \overline{a^{-1}a} = \bar{e}$. So $\overline{a}^{-1} = \overline{a^{-1}}$.
- **Group Homomorphism**: $\pi(ab) = \overline{ab} = \bar{a} \cdot \bar{b} = \pi(a)\pi(b)$
- **Kernel**: $\pi(a) = \bar{e}$ if and only if $aH = eH = H$, if and only if $a \in eH = H$. So $H = \ker(\pi)$

Wed 14 Feb 2024

> **Note**.
>
> Recall: the Exam is next Friday, there are 2 practice Midterms. Not necessarily from this class, but they are the right material.
>
> Also on there is Exam 1 material not on homework. Homework style questions on material that we didn't have a Homework on. Quotient Groups, First Isomorphism Theorem, ...

We are talking about normal subgroups and quotient groups. Let's talk about normal subgroups some more before getting into examples.

We saw that a subgroup is normal if $aH = Ha$ for all $a \in G$, $H \leq G$.

Claim: H is normal if and only if $aHa^{-1} = H$ for all $a \in G$. Why is this the same thing?

Proof

$\Rightarrow$

Assume H is normal. Let $a \in G$, then we know that $aH = Ha$ (that's what it means to be normal.) If we want to show that $aHa^{-1} = H$, we must show that these two sets are subsets of each other.

If $aha^{-a} \in aHa^{-1}$, then $ah \in aH$, but since $aH = Ha$, there exists some h' with $ah = h'a$. Hence $aha^{-a} = h'aa^{-1} = h' \in H$. So $aHa^{-1} \subseteq H$. We wanna prove the other direction now.

If $h \in H$, we want to show that $h \in aHa^{-1}$. We know that $h = haa^{-1}$, but $ha = ah'$ for some h', so $haa^{-1} = ah'a^{-1}$, so $H \subseteq aHa^{-1}$.

So $H = aHa^{-1}$.

$\Leftarrow$

Assume $aHa^{-1} = H$ for all $a \in G$. We want to show that $aH = Ha$, let $ah \in aH$, we know that $aha^{-1} \in H$, which means that there exist some element of H with $aha^{-1} = h'$, and so $ah = h'a \in Ha$. So $aH \subseteq Ha$.

The other direction works in the exact same way.

–

Example.

If $K = \ker(\varphi : G \to G')$, then $K \trianglelefteq G$, because if $aka^{-1} \in aKa^{-1}$, then

$$\varphi(aka^{-1}) = \varphi(a)\varphi(k)\varphi(a)^{-1} = e$$

So $aka^{-1} \in K$, so $aKa^{-1} \leq K$.

In fact, aKa^{-1} is the same size as K is conjugation does not change the size, so $aKa^{-1} = K$.

Now let's talk about quotient groups.

Let $G = S_n$ and $H = A_n$. We saw last time that $A_n \trianglelefteq S_n$ since $A_n = \ker(\text{sgn})$. Let's check this explicitly.

Given a permutation $\sigma \in A_n$ and $\tau \in S_n$. We want to show that $\tau\sigma\tau^{-1} \in A_n$.

Well, σ is even. If τ is odd, then so is τ^{-1} so $\tau\sigma\tau^{-1}$ is even. If τ is even, then so is τ^{-1}, so again $\tau\sigma\tau^{-1}$, so $\tau\sigma\tau^{-1} \in A_n$.

Side Note.

> Why is it that $|\sigma| = |\sigma^{-1}|$, with $\sigma \in S_n$? Well, just think of
>
> $$\sigma = (a_1a_2)(a_2a_3)\cdots(a_{k-1}a_k)$$

Then

$$\sigma^{-1} = (a_{k-1}a_k)\cdots(a_2a_3)(a_1a_2)$$

so $|\sigma| = |\sigma^{-1}|$.

■

So $\tau\sigma\tau^{-1} \in A_n$, and A_n is normal.

9 Quotient Groups

Assume that $H \trianglelefteq G$. Last time, we defined that

$$G/H = \{aH \mid a \in G\} = \{\bar{a} \mid a \in G\}$$

With the binary operation $\bar{a} \cdot \bar{b} = \overline{ab}$.

Example.

If $G = S_n$ and $H = A_n$. Since $|S_n| = n!$, $|A_n| = n!/2$. We know that

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

and so $|S_n/A_n| = 2$ and thus $S_n/A_n \cong \mathbb{Z}_2$. **QUESTION** Why is this isomorphic?

Remark: "Identify the quotient group" means "Find a familiar group to which the quotient group is isomorphic."

Example.

Identify S_n/A_n. The answer is $S_n/A_n \cong \mathbb{Z}_2$

S_n/A_n in more detail.

The cosets of A_n are: either

- A_n (the coset of even permutations)
- $(12)A_n$ (the coset of odd permutations)

So $S_n/A_n = \{\bar{e}, \overline{(12)}\}$

TODO see multiplication table.

This is clearly isomorphic to $\mathbb{Z}_2$, where we just send $\bar{e} \to \bar{0}$ and $\overline{(12)} \to \bar{1}$.

Example.

Consider $G = \mathbb{Z}_n$, $H = \langle \bar{m} \rangle$ for $\bar{m} \in \mathbb{Z}_n$.

Fact: Any subgroup of an Abelian group is normal. This should make sense, because left and right cosets only different by the order in which you write, which doesn't matter for Abelian groups!

Say that $\gcd(m, n) = d$, then $|\bar{m}| = \frac{n}{d}$. Take $[G : H] = |G/H|$, and we know by Lagrange's theorem that $|G/H| = |G|/|H| = n/(n/d) = d$.

On Homework 2, we showed that if $\varphi : G \to G'$ is onto and G is cyclic, then G' is cyclic.

Here, we have the onto homomorphism $\pi : G \to G/H$. Since G is cyclic, so is G/H, which means G/H is a cyclic group of order d, hence $G/H \cong \mathbb{Z}_d$.

Alternatively: Assume that $\bar{m}$ is the smallest element in H (i.e. $\bar{m} = \bar{d}$.)

What are the cosets?

The cosets of H are

$\{\bar{0} + H, \bar{1} + H, \ldots, \overline{d-1} + H\}$, and $\bar{a} + H = H \Leftrightarrow \bar{a} \in H$, since $aH = eH \Leftrightarrow a \in eH = H$.

We can already see that G/H is cyclic, generated by $\bar{1} + H$. Hence $G/H \cong \mathbb{Z}_d$, where $\varphi(\bar{k} + H) = \bar{k}$.

Our goal is to prove the 1st Isomorphism Theorem.

Example.

Take $\text{sgn} : S_n \to \mathbb{Z}_2$, but this time with

$$\sigma \to \begin{cases} \bar{0} & \sigma \text{ even} \\ \bar{1} & \sigma \text{ odd} \end{cases}$$

sgn is onto, so image $= \mathbb{Z}_2$. $\ker(\text{sgn}) = A_n$, then $S_n/A_n \cong \mathbb{Z}_2$.

Example.

$\varphi : \mathbb{Z} \to \mathbb{Z}_n$ with $k \to \bar{k}$.

φ is onto, $\ker \varphi = n\mathbb{Z}$, then $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$

Fri. 16 Feb 2024

Let's look at some examples of homs

Example.

Consider $\det : \mathrm{GL}_n(\mathbb{R}) \to (\mathbb{R} \setminus \{0\}, \times)$. We know that $\ker(\det) = \{A \in \mathrm{GL}_s(\mathbb{R}) \mid \det(A) = 1\} = \mathrm{SL}_n(\mathbb{R})$, and we now see that this is a normal subgroup.

$\mathrm{SL}_n(\mathbb{R}) \trianglelefteq \mathrm{GL}_n(\mathbb{R})$, as given any $A \in \mathrm{SL}_n(\mathbb{R})$, $B \in \mathrm{GL}_n(\mathbb{R})$, BAB^{-1} has $\det = 1$, so $BAB^{-1} \in \mathrm{SL}_n(\mathbb{R})$, so $\mathrm{SL}_n(\mathbb{R})$ is normal.

Because both of these groups are infinite, and so is the index, we can't just cheat like last time and take a look at what this is isomorphic to. We also know that det is surjective, but the 1st isomorphism theorem tells us that $\mathrm{GL}_n(\mathbb{R})/\mathrm{SL}_n(\mathbb{R}) \cong \mathbb{R} \setminus \{0\}$.

One more example before the proof.

Example.

Consider $\varphi : \mathbb{C} \setminus \{0\} \to \mathbb{R} \setminus \{0\}$ with $\varphi(z) = |z|$, the map which takes a complex number to its modulus (its length.)

Fact: $|zw| = |z||w|$, so φ is a homomorphism.

Notice that that the image of φ is only positive numbers, and $\ker(\varphi)$ is all the complex numbers with modulus 1 (or length 1.) This is all complex numbers of the form $a + bi = 1$, so $a^2 + b^2 = 1$, which is the unit circle!

Here, our 1st isomorphism theorem tells us that $\mathbb{C} \setminus \{0\}/\text{unit circle} \cong \mathbb{R}_{\geq 0}$.

Think about this:

$$\mathbb{C} \setminus \{0\} = \{re^{i\theta} \mid r \in \mathbb{R}_{\geq -0}, e^{i\theta} \in \text{ unit circle}\}$$

What we're left with is just the module information.

Question: Can you quotient out by the real numbers? Well remember that complex numbers under multiplication is Abelian, so every subgroup is normal, which means that you can! Do you get something isomorphic to the unit circle? Think about it!

Ok! Time for the theorem.

10 1st Isomorphism Theorem

Given a homomorphism $\varphi : G \to G'$, we have that

$$G/\ker(\varphi) \cong \text{image}(\varphi)$$

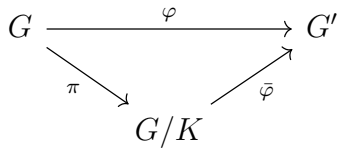
Proof

We have a hom $\varphi : G \to G'$. Let's assume that it's onto. If it's not, replace G' to image(φ) (Basically, we just change the codomain to make it onto.)

Let $K = \ker(\varphi)$, and we want to show that $G/K \cong G'$. Let $\pi : G \to G/K$ (since K is normal, we can do this!) This is the map $\pi(a) = \bar{a}$.

We define $\bar{\varphi} : G/K \to G'$, which takes $\bar{\varphi}(\bar{a}) = \varphi(a)$

Here's a picture.



We check that $\bar{\varphi}$ is well-defined, i.e. if $\bar{a} = \bar{b}$, check that $\bar{\varphi}(\bar{a}) = \bar{\varphi}(\bar{b})$

$$\begin{aligned}\bar{a} = \bar{b} &\Leftrightarrow aK = bK \\ &\Leftrightarrow \varphi(a) = \varphi(b) \\ &\Leftrightarrow \bar{\varphi}(\bar{a}) = \bar{\varphi}(\bar{b})\end{aligned}$$

So $\bar{\varphi}$ is a function.

Claim: $\bar{\varphi}$ is an isomorphism.

- **Homomorphism**:

  $\bar{\varphi}(\bar{a} \cdot \bar{b}) = \bar{\varphi}(\overline{ab}) = \varphi(ab) = \varphi(a)\varphi(b) = \bar{\varphi}(\bar{a})\bar{\varphi}(\bar{b})$.

- **One to one**:

  We'll show that $\ker(\bar{\varphi}) = \{\bar{e}\}$ (usefull trick btw, if you have a hom, you only need to check this)

  if $\bar{\varphi}(\bar{a}) = e$, then $\varphi(a) = e$, but then $a \in \ker(\varphi) = K$, so $\bar{a} = aK = K = \bar{e}$.

- **Onto**:

  if $b \in G'$, then there exists $a \in G$ with $\varphi(a) = b$ (remember, since we assumed φ to be onto!)

  So we get $\bar{\varphi}(\bar{a}) = \varphi(a) = b$.

Hence $\bar{\varphi} : G/K \to G'$ is an isomorphism, which concludes the proof.

> **Note**.
>
> For the exam, don't worry about being able to prove, this. You should be able to *use* these techniques. You should be able to use the tools and techniques from class.
>
> The techniques that go into proofs are good to understand though!

TODO draw tetrahedron with colors. Oh god

Let G be the group of symmetries of the regular tetrahedron. Symmetry is determined by what it does to vertices. All permutations of vertices are possible since all vertices are neighbors. Immediately, we see that

$$G \cong S_4$$

Every symmetry also permutes the colors of the edges.

$$\{\text{red}, \text{green}, \text{blue}\}$$

The group of permutations of this set is isomorphic to S_3 of course! Because we have 3 things in it.

So we get a map $\varphi : S_4 \to S_3$ which takes σ, a symmetry of the tetrahedron, to the number of ways to permute the 3 colors.

We're not going to prove that φ is a homomorphism.

Let $C_1 = \text{green}, C_2 = \text{blue}, C_3 = \text{red}$. Then $(12) \in S_4$ is a reflection of the tetrahedron.

TODO draw this somehow

Another way to think about is is that vertices 3 and 4 don't move, but 1 and 2 switch.

So $\varphi((12)) = (C_1C_2)(C_3) \in S_3$. It swaps green and blue and keeps red fixed.

Exercise 1: φ is surjective. Every way of permuting the colors is possible.

Exercise 2: $\ker(\varphi) = \{e, (12)(34), (13)(24), (14)(23)\}$. This is the Klein-4 group!!! Also known as K_4.

This is a group of order 4 which is **not** isomorphic to $\mathbb{Z}_4$, since all elements of K_4 are order 1 or 2.

Here, the 1st isomorphism theorem tells us that $S_4/K_4 \cong S_3$.

Warning: K_4 and $\mathbb{Z}_4$ are Abelian groups of order 4. Both have normal subgroups of order 2. If $K_4 = \{e, a, b, ab\}$, $H = \{e, a\}$ and $\{\bar{0}, \bar{2}\} \leq \mathbb{Z}_4$, and $K_4/H \cong \mathbb{Z}_2$, $H \cong \mathbb{Z}_2$, and $\mathbb{Z}_4/H \cong \mathbb{Z}_2$.

Why is this a warning? Because we **cannot** reconstruct the original group from H and G/H.

Note.

We'll do product groups on Monday, which is testable. The rest will not be.

Mon. 19 Feb 2024

Today we are talking about Product Groups!

11 Product Groups

Today we try to build up larger groups from smaller groups.

Let's write out explicitly the binary operations. Let $(G, p), (G', p')$ be two groups.

The set

$$G \times G' = \{(g, g') \mid g \in G, g' \in G'\}$$

Can be given a binary operation

$$(g, g') \cdot (h, h') = (p(g, h), p'(g', h'))$$

Basically, you do the operations component-wise.

Claim: This is a group!

1. **Identity**: $(e_G, e_{G'})$
2. **Inverses**: $(g, g')^{-1} = (g^{-1}, (g')^{-1})$

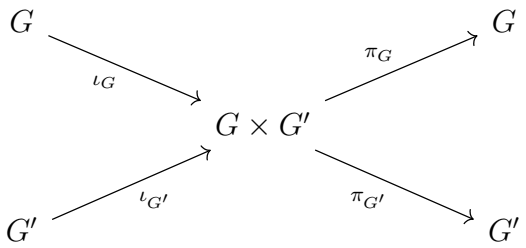
Definition.

$G \times G'$ is the **product** of G and G'. It's also known as the **direct product**.

Note.

$|G \times G'| = |G| \cdot |G'|$

From this we can get special Homomorphisms. Quite a few in fact.



All of these are homomorphisms. We say that ι_G and $\iota_{G'}$ are **inclusions**, and that π_G and $\pi_{G'}$ are **projections**. Let's look at them in more detail

Inclusions

- $\iota_G(g) = (g, e)$. We have no other choice here for the second element. Think about why.
- $\iota_{G'}(g') = (e, g')$

Projections

- $\pi_G(g, g') = g$
- $\pi_{G'}(g') = g'$

Note that these maps are onto, and in fact $\ker(\pi_G) = \{(e_G, g') \mid g' \in G'\}$. Similarly, $\ker(\pi_{G'}) = \text{image}(\iota_G)$.

Now using the 1st isomorphism theorem, we know that $G \times G'/G' \cong G$. This means that $\iota_{G'}(G') \leq G \times G'$.

Similarly, $G \times G'/G \cong G$, meaning that $\iota_G(G) \leq G \times G'$.

This is fairly inline with how we expect the quotient group to behave.

Let's look at an

Example.

$$\mathbb{Z}_2 \times \mathbb{Z}_3 = \{(\bar{0}, \bar{0}), (\bar{1}, \bar{0}), (\bar{0}, \bar{1}), (\bar{0}, \bar{2}), (\bar{1}, \bar{2})\}$$

Let's turn our attention to $\langle(\bar{1}, \bar{1})\rangle$. We have that

$$\langle(\bar{1},\bar{1})\rangle = \{(\bar{0},\bar{0}),(\bar{1},\bar{1}),(\bar{0},\bar{2}),(\bar{1},\bar{0}),(\bar{0},\bar{1}),(\bar{1},\bar{2})\}$$

So in fact $(\bar{1},\bar{1})$ is a generator of $\mathbb{Z}_2 \times \mathbb{Z}_3$. This means that $\mathbb{Z}_2 \times \mathbb{Z}_6$ is not a new group, it's isomorphic to $\mathbb{Z}_6$! In fact, this is generalizable.

Proposition

$\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$ if and only if $\gcd(m,n) = 1$.

Proof

All we have to do is figure out when the group on the left is cyclic.

Lemma:

The order of $(g,g') \in G \times G'$ is the $\text{lcm}(|g|,|g'|)$.

Proof of Lemma

If $\gcd(m,n) = 1$, then the $\text{lcm}(|\bar{1}|,|\bar{1}|) = \text{lcm}(m,n)$. Moreover,

$$\text{lcm}(m,n) = \frac{mn}{\gcd(m,n)}$$

This means that $(\bar{1},\bar{1})$ generates $\mathbb{Z}_m \times \mathbb{Z}_n$, so it is cyclic, and so it is isomorphic to $\mathbb{Z}_{mn}$

On the other hand, if $\gcd(m,n) \neq 1$, then for any $(\bar{a},\bar{b}) \in \mathbb{Z}_m \times \mathbb{Z}_n$, then $|(\bar{a},\bar{b})| = \text{lcm}(|\bar{a}|,|\bar{b}|) \leq \text{lcm}(m,n) < mn$, in which case $\mathbb{Z}_m \times \mathbb{Z}_n$ cannot be cyclic! And so it is **not** isomorphic to $\mathbb{Z}_{mn}$

For instance, $\mathbb{Z}_2 \times \mathbb{Z}_2 \ncong \mathbb{Z}_4$.

Proposition: There are two groups of order 4, up to isomorphism.

$$\mathbb{Z}_4 \text{ or } \mathbb{Z}_2 \times \mathbb{Z}_2$$

Proof: Let G be a group of order 4. If G is cyclic, then $G \cong \mathbb{Z}_4$. If not, then $|a| = 2$ for all non-trivial elements in our group. Pick $a \in G$, and $b \in G$ with $b \neq e$ and $b \neq a$. Then

$$ab \neq \begin{cases} e & \text{as } b \neq a^{-1} = a \\ a & \text{as } b \neq e \\ b & \text{as } a \neq e \end{cases}$$

So ab is the 4 element of G, and thus $G = \{e, a, b, ab\}$. Then we have that $\varphi : \mathbb{Z}_2 \times \mathbb{Z}_2 \to G$ with

- $(\bar{0}, \bar{0}) \mapsto e$
- $(\bar{1}, \bar{0}) \mapsto a$
- $(\bar{0}, \bar{1}) \mapsto b$
- $(\bar{1}, \bar{1}) \mapsto ab$

Is an isomorphism.

Structure Theorem for Finitely Generated Abelian Groups

If G is finitely generated, (i.e. there is a finite set $S \subseteq G$ such that all elements of G are products of elements of S and their inverses) and G is Abelian, then

$$G \cong \mathbb{Z} \times \cdots \times \mathbb{Z} \times \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_k}$$

Moreover, if G is finite and Abelian, then

$$G \cong \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_k}$$

Author Note.

This is all the material you need to know for this Exam. From this point forward is **not** exam material.

12 Semidirect Product

Given a group G, the set $\mathrm{Aut}(G)$ of **automorphisms** of G (i.e. isomorphisms $G \to G$) is a group under composition.

Definition.

Let G, H be groups, $\varphi : H \to \text{Aut}(G)$ be a homomorphism with $\varphi(h) = \varphi_h$. Then the group

$$G \times_\varphi H \text{ or } G \rtimes H$$

is called a **semidirect product**, where the elements $(g, h) \in G \times H$, but the binary operation

$$(g, h)(g', h') = (g \cdot (\varphi_h(g')), hh')$$

The set is the same! But the binary operation is different, so we have a new group structure.

The identity: $(g, h)(e, e) = (g\varphi_h(e), he) = (ge, he) = (g, h)$. On the other side: $(e, e)(g, h) = (e\varphi_e(g), eh) = (eg, eh) = (g, h)$, since $\varphi_e = \varphi(e) = e_{\text{Aut}(G)}$ so $\varphi_e(g) = g$.

Example.

If $\varphi : H \to \text{Aut}(G)$ is the identity, then

$$(g, h)(g', h') = (g\varphi_h(g'), hh') = (gg', hh')$$

So

$$G \times_\varphi H = G \times H$$

Example.

Let $G = \mathbb{Z}_n$ and $H = \mathbb{Z}_2$ with $\varphi : \mathbb{Z}_2 \to \text{Aut}(\mathbb{Z}_n)$ with $\bar{0} \mapsto e$ and $\bar{1} \mapsto f$. $f : \mathbb{Z}_n \to \mathbb{Z}_n$ is determined by $f(\bar{1})$.

We need $f \circ f = id$ as $\varphi(\bar{1} + \bar{1}) = \varphi(\bar{0}) = id$. For any n, $f = id$ or $f(\bar{1}) = \overline{-1} = \overline{(n-1)}$.

With the former, $\mathbb{Z}_n \times_\varphi Z_2 \cong \mathbb{Z}_n \times \mathbb{Z}_2$. With the latter, $\mathbb{Z}_n \times_\varphi \mathbb{Z}_2 \cong D_{2n}$.

Wed. 21 Feb 2024

Today is review!

Structure of the Exam:

- 4 Questions
- First question is short answer. Similar to the 2019 Midterm
- 3 Longer questions, similar to the 2019 midterm.

Exam Questions

13 Exam 1 Review

13.1 Common Groups and their properties

Useful for having a repertoire of questions.

- $\mathbb{Z}$, $\mathbb{Z}_n$. This is **always** under addition by default, **even if n is prime!** These are
  1. Cyclic
  2. Abelian
  3. Sometimes infinite? Or order n

  Note.

  All subgroups of cyclic groups are cyclic.

- $(\mathbb{Z}_n^\times, \times)$. This is the group of integers relatively prime to n $(\text{mod } n)$ under $\times$. It is
  1. Abelian
  2. Not necessarily cyclic, so the order is complicated.
  3. Does not include $\bar{0}$.

- S_n. The Symmetric group. It is
  1. Non-Abelian

2. Not cyclic
3. $|S_n| = n!$

We have some nice isomorphisms

1. $S_3 \cong D_6$, where D_6 is the symmetries of a **triangle**.
2. $S_2 \cong \mathbb{Z}_2$

- D_{2n}. The dyhedral group. The symmetries of a regular n-gon. It is
  1. Non-Abelian
  2. Not cyclic
  3. Order $2n$

  And we have that $D_{2n} \leq S_n$, but we only have $D_6 \cong S_3$.

  We have a nice notation for this. We say that it is generated by x, a reflection, and y a rotation.

$$D_{2n} = \{e, x, y, \ldots, y^{n-1}, yx, \ldots, y^{n-1}x\}$$

  And we have that $yx = y^{-1}x$.

- A_n. The alternating group. $A_n \leq S_n$ with
  1. $|A_n| = n!/2$, subgroup of even permutations.
- $\mathbb{R}, \mathbb{C}$ (under addition), $\mathbb{R} \setminus \{0\}, \mathbb{C} \setminus \{0\}, \mathbb{Q} \setminus \{0\}$ (under multiplication)

  These are
  1. Infinite
  2. Non-cyclic.
- $\mathrm{GL}_n(\mathbb{R}), \mathrm{SL}_n(\mathbb{R})$. These are
  1. Infinite
  2. Non-Abelian

  Where the binary operation is Matrix multiplication.

- Product Groups $G \times H$ with
  1. $|G \times H| = |G| \cdot |H|$.
  2. $|(a, b)| = \text{lcm}(|a|, |b|)$.

  These groups are Abelian if and only if both G and H are Abelian.

  We saw

  1. $\mathbb{Z}_2 \times \mathbb{Z}_2 \ncong \mathbb{Z}_4$, the Klein-4 Group.

  We also saw $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$

Z_2 Can be written a number of different ways.

Example.

Groups of order 30.

We know that $30 = 3 \cdot 5 \cdot 2$.

1. If we want an Abelian group, we have no choice but to use $\mathbb{Z}_{30}$. **TODO** why?

   What about $\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5$? Well that's isomorphic to $\mathbb{Z}_{30}$, since $2, 3$ are coprime, and $6, 5$ are also coprime.

2. Non-Abelian: D_{30}, the symmetries of a regular 15-gon, or $\mathbb{Z}_3 \times D_{10}$, or $\mathbb{Z}_5 \times D_6$.

   Why are these 3 groups different? Why are they not isomorphic?

   The approach is to think about many different things. Usually the approach is to find a property that holds in one group that does not hold in the other.

   - It could be size. If the sizes don't match, no chance that there can be an isomorphism.
   - Abelian-ness
   - One of them could be that a group has a normal subgroup of order 5, and the other does not.
   - This group has an element of order 15, and the other does not.

   All those things can be used to show that things are not isomorphic.

In the example above, we know that D_{30} has 15 elements of order 2, D_{10} for sure has 5. The claim is that this is all of them. Simply notice that

$$|(\bar{a}, g)| = \operatorname{lcm}(|\bar{a}|, |g|) = \begin{cases} \operatorname{lcm}(1, |g|) = |g| \\ \operatorname{lcm}(3, |g|) = 3|g| \end{cases}$$

The problem is that $3|g|$ is never equal to 2, so it has to be $|g|$.

TODO finish. So they cannot be isomorphic.

- $\mathbb{Z}_2 \cong (\{\bar{0}, \bar{1}\}, +) \cong (\{\pm 1\}, \times)$

2018, 7b

We have a group of order 40, we want to know all Abelian groups of order 40.

How many ways can we write 40 as a product of cyclic groups which are not isomorphic?

We know that

$$40 = 2 \cdot 2 \cdot 2 \cdot 5$$

Well, we have

1. $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5$
2. $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_5 \cong \mathbb{Z}_{10} \times \mathbb{Z}_4 \cong \mathbb{Z}_2 \times \mathbb{Z}_{20}$
3. $\mathbb{Z}_8 \times Z_5 \cong \mathbb{Z}_{40}$

Recall that we were asked for Abelian groups, so its just a product of cyclic groups.

How do we show something is normal?

There are several ways. Two big ones:

1. **By the definition**:

   Show that $aH = Ha$ are the same coset for all $a \in G$.

   If there's not many cosets, this isn't too bad.

2. **Show that $aHa^{-1} \in H$ for all $a \in G$, and for all $h \in H$**

   This implies that $aHa^{-1} = H$.

   In fact, it's sufficient to show the one direction for all elements. This is because we know that we have a bijection between a group and its conjugation.

3. **If G is Abelian**

   Then all your subgroups are normal, so we're done!

   This one is less applicable, but useful!

Example.

2019, number 4

If G is a group and $Z(G) = \{a \in G \mid ab = ba \forall b \in G\}$ is the center of the group.

We want to show that $Z(G) \trianglelefteq G$, in order words, that it's a normal subgroup.

Proof

$e \in Z$, so $Z \neq \varnothing$

Closure: If $z, z' \in Z$, then for any $a \in G$, then $zz'a = zaz' = azz'$ so $zz' \in Z$. So Z is closed.

Inverses: If $z \in Z$, $a \in G$, $az^{-1} = (za^{-1})^{-1} = (a^{-1}z)^{-1} = z^{-1}a$ so $z^{-1} \in Z$.

WARNING: If you aren't told it's a subgroup, you have to show that too!

Normal: To show that it's normal, if $z \in Z, a \in G$ then $aza^{-1} = aa^{-1}z = z \in Z$ so $Z \trianglelefteq G$.

What's an example of a Bijection that's not a Homomorphism?

Here's one

$$\varphi : \mathbb{Z}_4 \to \mathbb{Z}_4$$

where

- $\bar{0} \mapsto \bar{1}$

- $\bar{1} \mapsto \bar{2}$
- $\bar{2} \mapsto \bar{3}$
- $\bar{3} \mapsto \bar{0}$

Here, the identity does not map to the identity. Also

$$\varphi(\bar{0} + \bar{1}) = \varphi(\bar{1}) = \varphi(\bar{2})$$

But

$$\varphi(\bar{0}) + \varphi(\bar{1}) = \bar{1} + \bar{2} = \bar{3}$$

and $\bar{3} \neq \bar{2}$.

2018, question 2

$\sigma = (137)(2465)$, and $\tau = (152)(3647)$, want to find $\sigma\tau^{-1}$

Well, $\tau^{-1} = (125)(3746)$

Then $\sigma\tau^{-1} = (1453)(67)$ **TODO** Show

How do we write this in terms of transpositions? Well

$$= (14)(45)(53)(67)$$

Mon. 26 Feb 2024

Two more weeks of Group Theory, then we talk about Rings and Fields.

14 Group Operations

We've seen two examples of groups that have to do with sets. S_n, and D_{2n}. S_n is a bijection from $\{1, \ldots, n\}$ to itself, and D_{2n} whose elements are special examples of bijections of the regular n-gon itself.

These are examples of group actions.

Definition.

If S is a set and G is a group. We say that G **acts** on S (notated as $G \curvearrowright S$) if there is a map $\alpha : G \times S \to S$ satisfying two properties.

1. $\alpha(e, s) = s$. On the identity, we just want our set back, unchanged.
2. $\alpha(ab, s) = \alpha(a, \alpha(b, s))$. Basically the combination of both of these is the same as doing one after the other.

We often write $\alpha_a(s)$ for $\alpha(a, s)$. Then $\alpha_a : S \to S$ for every $a \in G$.

We can also write $a * s$ for $\alpha(a, s) = \alpha_a(s)$. In this case, our definition becomes

1. $e * s = s$ for all $s \in S$
2. $(ab) * s = a * (b * s)$ for all $s \in S$ and for all $a, b \in G$.

Let's look at an example

Example.

$S = \{1, 2, \ldots, n\}, G = S_n$, then $\alpha(\sigma, i) = \sigma(i)$.

Here, σ is a bijection from S to S.

In our other notation, $\sigma * i = \sigma(i)$.

Example.

S is a regular n-gon. Let $G = D_{2n}$, then $a * s = a(s)$, so here, symmetry is a function from S to S

Note.

Group actions are just functions on the sets! Nothing crazy is happening here, we're just formalizing some natural ideas.

Example.

$S = \mathbb{R}^n$, $G = \mathrm{GL}_n(\mathbb{R})$ and $A * \bar{v} = A\bar{v}$ where $A \in \mathrm{GL}_n(\mathbb{R})$, $\bar{v} \in \mathbb{R}^n$.

Example.

if $G = \mathrm{Mat}_n(\mathbb{R})$, the set of all matrices under addition, then

$$(A+B)*\bar{v} = (A+B)\bar{v}$$

But also

$$A*(B*\bar{v}) = A\bar{v}(B\bar{v}) = AB\bar{v}$$

which are not equal, so this doesn't work.

Example.

Let $S = G$ and $G = G$, any group G. Then what's the action? Well, it's just the group operation.

$$a*s = as$$

Left multiplication by our group element is a group action!

Note.

It's worth noting that all these things are happening on the left! If you multiplied on the right, that would not be a group action!

$$a*s = sa$$

Is not a group action! We only do left group actions in this class.

This is because of how we've set up function composition.

$$(ab)*s = s(ab) \neq s(ba) = a*(sb) = a*(b*s)$$

Example.

Let $G = \mathrm{GL}_n(\mathbb{R})$, and let S be the set of ordered bases for $\mathbb{R}^n$.

Definition.

If $s \in S$, then the **orbit** of s is

$$O_s = \{a * s \mid a \in G\}$$

It's all the images of s from G, the set of all things that can happen to it. The collection of all those images is the orbit.

Example.

If S is the triangle, and G is D_6, then if s is a vertex, O_s is *all* the vertices. If s is the midpoint of a line segment of the triangle, then O_s is the set of all such midpoints.

In general, if s is a point on the triangle, its orbit will be all the points that you can get to by taking that point, and either rotating the triangle or flipping it around.

The orbit of the center is just itself.

Note.

We always have that $s \in O_s$.

If $s' \in O_s$, then $s' = a * s$ for some $a \in G$. Then

$$\begin{aligned} s = e * s &= (a^{-1}a) * s \\ &= a^{-1} * (a * s) \\ &= a^{-1} * s' \in O_{s'} \end{aligned}$$

If $s' \in O_s$, then $s \in O_{s'}$.

What we get here is an equivalence relation! $s \sim s'$ if $s \in O_{s'}$. What we get out of this is that **the orbits partition** S**.** It follows that if $O_s \cap O_{s'} \neq \varnothing$, then $O_s = O_{s'}$.

Definition.

A group action is called **transitive** if there is only one orbit. In other words, $O_s = S$ for any $s \in S$.

Example.

Let $O(n) \curvearrowright \mathbb{R}^n$ (where $O(n)$ is the orthogonal group. This is a subset of $\mathrm{GL}_n(\mathbb{R})$ where the columns form an orthonormal basis.)

$A * \bar{v} = A\bar{v}$ is **not** transitive, as for $\bar{v} = \bar{0}$, so $O_{\bar{0}} = \{0\}$ (the only place that 0 goes to under linear transformations is 0.)

In fact $||A\bar{v}|| = \bar{v}$ for any $\bar{v}$. So orbits of this group action are n dimensional spheres centered at the origin!

Note.

You will never get a transitive group action from a matrix group since the origin is alone.

TODO what????

Example.

$S_n \curvearrowright \{1, \ldots, n\}$ is transitive. If $s = 1$, then if $\sigma = (1k)$, then $\sigma * 1 = \sigma(1) = k$. So $k \in O_1$ for all $k = 1, \ldots, n$. So $O_1 = \{1, \ldots, n\}$.

14.1 Stabilizers

Definition.

If $s \in S$, the **stabilizer** of s is

$$\text{Stab}(s) = G_s = \{a \in G \mid a * s = s\}$$

It's all the group elements that don't do anything to s. They *stabilize* s.

To bring it back, we pick an element of a set s, and using this element, we can look at its orbit: the set of places it will go under every possible group action, or we can look at its stabilizer, the set of elements of G that keep it as it is.

Note.

The Stabilizer is elements of G, but the orbit is elements of S.

Claim: The stabilizer is a subgroup of G.

Check:

1. **Closed**:

   If $a, b \in G_s$. Then

$$\begin{aligned}(ab) * s &= a * (b * s) \\ &= a * s \\ &= s\end{aligned}$$

so $ab \in G_s$.

2. **Inverses**:

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

If $a \in G_s$, then $a * s = s$, so $s = a^{-1} * s$ and so $a^{-1} \in G_s$

Hence $G_s \leq G$.

Example.

If $S_n \curvearrowright \{1, \ldots, n\}$, let $s = n$, then

$$G_s = \{\sigma \in S_n \mid \sigma(n) = n\}$$

This is all the permutations where n does not appear in the cycle notation! This is all the permutations that use 1 to $n - 1$.

Example.

$\mathrm{GL}_n(\mathbb{R}) \curvearrowright \mathbb{R}^n$. If $\bar{v} = \bar{0}$, then

$$G_{\bar{0}} = \{A \in \mathrm{GL}_n(\mathbb{R}) \mid A\bar{0} = \bar{0}\} = \mathrm{GL}_n(\mathbb{R})$$

So the stabilizer can be the whole group.

Note that if $\bar{v} \neq 0$, then $G_{\bar{v}} < \mathrm{GL}_n(\mathbb{R})$.

Example.

$\text{Isom}(\mathbb{R}^n) \curvearrowright \mathbb{R}^n$, then $G_{\bar{0}} \cong O(n)$.

TODO what?????

Wed. 28 Feb 2024

Note.

Most questions on the homework are on actions. By the end of this class you should be able to do all questions up to 4.

Recall: $G \curvearrowright S$ is a group action. Given $s \in S$, we have

1. **Orbit** $O_s = \{a * s \mid a \in G\} = \{s' \in S \mid s' = a * s \text{ for some } a \in G\} \subseteq S$
2. **Stabilizer** $\text{Stab}(s) = G_s = \{a \in G \mid a * s = s\} \leq G$.

Proposition:

If $G \curvearrowright S$ and $s \in S$. Then

1. $a, b \in G$, then $a * s = b * s$ if and only if $a^{-1}b \in G_s$
2. If $a * s = s'$, then $G_{s'} = aG_sa^{-1} = \{aga^{-1} \mid g \in G_s\}$ is the conjugate subgroup!

   So the stabilizers are related, they are conjugate subgroups.

   Corollary: If G is finite, and $a * s = s'$, then $|G_s| = |G_{s'}|$ because conjugation is a bijection so they must have the same size.

Note.

Compare (a) to: If $\varphi : G \to G'$ is a hom, $\varphi(a) = \varphi(b)$ if and only if $a^{-1}b \in \ker(\varphi)$.

Proof of Proposition.

1. $a * s = b * s$ if and only if $a^{-1}(a * s) = a^{-1} * (b * s)$, if and

$$\begin{aligned} a * s = b * s &\Leftrightarrow a^{-1}(a * s) = a^{-1} * (b * s) \\ &\Leftrightarrow (a^{-1}a) * s = (a^{-1}b) * s \\ &\Leftrightarrow s = (a^{-1}b) * s \\ &\Leftrightarrow (a^{-1}b) \in G_s \end{aligned}$$

2. Let $a * s = s'$. (this implies that $s = a^{-1} * s'$)

   If $aga^{-1} \in aG_sa^{-1}$, then $(aga^{-1}) * s'$.

$$\begin{aligned} (aga^{-1}) * s' &= a * (g * (a^{-1} * a')) \\ &= a * (g * s) = a * s = s' \qquad \text{since } g \in G_s \end{aligned}$$

   So $aga^{-1} \in G_{s'}$. Hence $aGa^{-1} \subseteq G_{s'}$.

   Similarly, $(a^{-1})G_{s'}(a^{-1})^{-1} \subseteq G_s$, since $a^{-1} * s' = s$. Since conjugation is a bijection, can conjugate by a:

$$a(a^{-1})G_{s'}(a^{-1})^{-1}a^{-1} \subseteq aG_sa^{-1}$$

   So $G_{s'} \subseteq aG_sa^{-1}$.

   Hence $aG_sa^{-1} = G_{s'}$

15 Orbit Stabilizer Theorem

If $G \curvearrowright S$ and $s \in S$, then there is a bijection $f : \{aG_s\} \to O_s$ with $aG_s \mapsto a * s$.

Proof:

1. f **is well-defined**.

   If $aG_s = bG_s$, then $a^{-1}b \in G_s$. Which implies that $a * s = b * s$ by the Proposition. So if the input cosets are the same, then the output is consistent, and f is well-defined.

2. f **is injective**.

   If $f(aG_s) = f(bG_s)$, then $a * s = b * s$, which implies that $a^{-1}b \in G_s$ by the Proposition. But this implies that $aG_s = bG_s$.

3. f **is surjective**.

   If $s' \in O_s$, then $a' = a * s$ for some $a \in G$. then $f(aG_s) = a * s = s'$.

15.1 Counting via Orbit Stabilizer

Anytime that we want to talk about the number of cosets, we can talk about the number of orbits instead, since they are in bijection!

Recall Lagrange's Theorem: If $G \leq G$, then $[G : H]$ is the number of cosets, and $|G| = [G : H] \cdot |H|$.

If $G \curvearrowright S$, and $s \in S$, then $[G : G_s] = |O_s|$, by the Orbit Stabilizer Theorem. So

$$|G| = |O_s| \cdot |G_s|$$

Similarly, the orbits partition S, so

$$|S| = \sum |O_i|$$

We can get the size of S be adding up the sizes of the orbits.

Let's do some counting

Example.

Let G be the rotational symmetries of a cube. If s is a vertex, then the orbit by rotation is the set of all 8 vertices. So $|O_s| = 8$, since G acts transitively on all the vertices of the cube. Every vertex can be taken to every other vertex.

What's the order of the stabilizer? $|G_s| = 3$. When you fix s, you can only rotate 3 ways. (If you want to know where they number comes from, take a cube and fix one vertex, rotate it about that vertex until the same piece comes back. You can only do this 3 times.)

This tells us that $|G| = |O_s||G_s| = 8 \cdot 3 = 24$, so there are 24 symmetries of a cube.

Example.

If s is the middle of an edge, we want to know $|G_s|$? We know that the orbits of s is the middle of all edges, so $|O_s|= 2$. Since we know now that the size of the group of symmetries is 24, we have that

$$|G_s|= \frac{|G|}{|O_s|} = \frac{24}{12} = 2$$

But what is G_s ? One of them is always the identity, and the other is just to rotate about that edge. Then you can rotate 180 degrees, which is its own inverse.

Definition.

The **center** of a group G is $Z(G) = \{a \in G \mid ab = ba \text{ for all } b \in G\}$

And in fact, $Z(G) \leq G$.

Definition.

If p is prime and $|G|= p^k$ for some $k \geq 1$, then G is called a p-group.

Proposition: If G is a p-group, then $|Z(G)|> 1$.

Proof: Let $G \curvearrowright G$ by conjugation (i.e. $a * b = aba^{-1}$.) An element $a \in Z(G)$ if and only if $ab = ba$ for all $b \in G$, if and only if $a = bab^{-1}$ for all $b \in G$, if and only if $a = b * a$, if and only if $O_a = \{a\}$.

So being in the center means that you are in an orbit of size 1. **QUESTION** What? Make more sense of this?

Given any $a \in G$, then $|O_a|$ divides $|G|= p^k$, so $|O_a|= p^m$ for some m, for each $a \in G$. Note that each orbit might have a different power m.

The orbits partition G, so $|G|= \sum|O_i|$, and since p divides $|G|$, we know that $p \mid \sum|O_i|$. Since $e \in Z(G)$, $O_e = \{e\}$, then $\sum|O_i|= 1 + \sum_{O_i \neq O_e}|O_i|$ (where the 1 here is the orbit of e.)

If $Z(G) = \{e\}$, then $|O_i|> 1$ for every $O_i \neq O_e$ (otherwise, it would be in the center.) But then $\sum|O_i|= 1 + p^{m_1} + \cdot p^{m_k}$, which is not divisible by p, but we showed that it is, so in fact, the center is **not** just the identity. $Z(G) = \{e\}$, and $|Z(G)|> 1$.

Fri. 1 March 2024

16 Class equation

We have the conjugation action of $G \curvearrowright G$, with $a * b = aba^{-1}$. This is so important that we have names for it: orbits and stabilizers.

Definition.

The orbit of $b \in G$ is called the **conjugacy class** of b, written as

$$C(b) = \{aba^{-1} \mid a \in G\}$$

This is all the things that are conjugates of b.

Definition.

The stabilizer of $b \in G$ is called the **centralizer** of b, written as

$$Z(b) = \{a \in G \mid aba^{-1} = b\}$$

This is the set of group elements that commute!

But the Orbit Stabilizer Theorem from last class tells us that $|G| = |C(b)||Z(b)|$ for all $b \in G$. This isn't a new definition, we just have new names for things.

There's a couple things to note.

Remarks

- $Z(a)$ contains $Z(G)$, the center of the group, as a subgroup.

  Remember, the center of the group $Z(G)$ is the set of elements that commute with everything, so certainly, they commute with a.

  $$Z(G) \leq Z(a)$$

- $Z(a)$ contains $\langle a \rangle$ as a subgroup.

For this one, just think about the fact that $Z(a)$ is the set of all things that commute with a, then certainly, they'll commute with a^4, or a^7...

Another note here is the direction of size. The center of G might be small or trivial, but $Z(a)$ might be rather large if $|a|$ is large.

- $a \in Z(G)$ if and only if $Z(a) = G$.

  a being in the center means that it commutes with everything. So certainly, the set of things that commute with *it* is *everything!*

  If it commutes with everything, then it's in the center!

  Moreover, every conjugate of every element in the center is itself, so we have

  $$a \in Z(G) \Leftrightarrow Z(a) = G \Leftrightarrow C(a) = \{a\}$$

  Being in the center means that you have the largest possible centralizer, G, and the smallest possible conjugacy class, $C(a)$.

Recall: The orbits of a group action $G \curvearrowright S$ partition S. This means that the conjugacy classes partition G.

If G is finite, then that means that we have finitely many conjugacy classes, call them $C_1, \ldots, C_k$.

The **class equation** of G is

$$|G| = |C_1| + \cdots + |C_k|$$

In practice, C_1 is the conjugacy class of the identity, and $C_1 = C(e) = \{e\}$, so $C_1 = 1$.

Also, by the Orbit Stabilizer Theorem, each $|C_1|$ must divide $|G|$

Let's look at some examples.

Example.

Let G be an Abelian group of order n.

Here, $Z(G) = G$, so $C(a) = \{a\}$ for all $a \in G$, every conjugacy class is size 1, and the class equation is

$$n = 1 + \cdots + 1$$

Each 1 corresponds to an element in the center, so we can count the number of ones.

Fact: The class equation of G is $n = 1 + \cdots + 1$ if and only if G is Abelian.

Example.

Let $G = S_3$ is the first non Abelian group. Here,

- $|G| = 6$
- $C(e) = \{e\}$
- $C((123)) = \frac{|G|=6}{|Z((123))|}$ By the Orbit Stabilizer Theorem.

  The centralizer of (123), $Z((123))$ contains $\langle(123)\rangle$, which is order 3, so the size of the centralizer is at least 3. But we know that the order of subgroups divides the order, so it's either 3 or 6, but if it's 6, it's the entire group. But this is only true if $(123) \in Z(G)$, but it isn't, since $(12)(123) = (12)(12)(23) = (23)$ and $(123)(12) = (13)$ which is not equal.

  So the size of the centralizer must be 3, and the conjugacy class must be order 2. We see that $(12)(123)(12) = (12)(12)(23)(12) = (23)(12) = (32)(21) = (321) = (132)$. So $C((123)) = \{(123), (132)\}$.

  Fact: Conjugates in S_n have the same cycle type.

  i.e. $\sigma(\text{3-cycle})\sigma^{-1} = \text{3-cycle}$

- $|C((12))| = \frac{6}{Z((12))}$ and $Z((12))$ contains $\{e, (12)\}$, so it's size $2, 3$ or 6. We know it can't be 6 since $(12) \notin Z(G)$. If it were size 3, it would imply that $|C((12))| = 2$ so either (13) or (23) is in a conjugacy class of size 1, which is a contradiction since neither is in $Z(G)$, so it must be size 2, and the class equation of S_3 is $6 = 1 + 2 + 3$.

  Going backwards here, if G has the class equation above, there's a few things we can gather.

  1. One 1 means the center of G has size 1.

Note that you always have at least one 1, since the identity is always in your center.

2. Not all 1s means that G is not Abelian
3. 2 means that $\exists a \in G$ such that $|C(a)|= 2$ so $|Z(a)|= 3$ so G has a subgroup of order 3.

   Similarly, 3 means that G has a subgroup of order 2.

16.1 Normal Subgroups

If $H \trianglelefteq G$, then this means that $aHa^{-1} = H$. If $h \in H$, then $aha^{-1} \in G$ for all $a \in G$, but this means that the entire conjugacy class of a is in the subgroup

$$C(a) = H$$

Then, normal subgroups are unions of conjugacy classes! In fact, this is an if and only if! Normal subgroups corresponds exactly to being a union of conjugacy classes.

In S_3, $\langle(123)\rangle$ is normal, since it's $C(e) \cup C((123))$. We can also see that $\langle(12)\rangle$ isn't normal, as it doesn't contain $C((12))$.

More Remarks:

When we have a class equation $n = \underbrace{1 + \cdots + 1}_{m} + a + b + \cdots$.

This implies that

- $|Z(G)|= m$
- a tells us that there exists an element whose centralizer $Z(a)$ is such that

$$|Z(a)|= \frac{n}{|C(a)|} = \frac{n}{a}$$

Since $Z(G) \leq Z(a)$, we can additionally say that m divides $\frac{n}{a}$.

Proposition: If $|G|= p^2$, with p is prime, then G is Abelian.

Proof: We already shows that $|Z(G)|> 1$, so it's p or p^2.

If it's p^2, then $G = Z(G)$, and we have an Abelian group.

If it's p, consider $a \notin Z(G)$. Then $Z(a)$ contains $Z(G)$ and it contains a, which means that $|Z(a)|\geq p+1$, but $|Z(a)|$ divides p^2, so $|Z(a)|= p^2$, which means in fact $a \in Z(G)$. Contradiction!

This means that $|Z(G)|= p^2$, and G is Abelian.

> **Note**.
>
> If you have a centralizer of an element that's not in the center, it must be at least one larger than the center.

Mon. 4 March 2024

Recall: A p-group G is a group with order p^k, where $k \geq 1$ and p is prime. We've shown the following things:

1. $|Z(G)|\geq 1$
2. If $|G|= p^2$, then G is Abelian.

Corrolary: If $|G|= p^2$, then $G \cong \mathbb{Z}_{p^2}$ or $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$.

Proof: We could use the Theorem of finite Abelian Groups, but that's kind of cheating, but we can do this directly!

(Not using the structure theorem) If $\exists a \in G$ with $|a|= p^2$, then G is cyclic so $G \cong Z_{p^2}$. If not, then every non-trivial element has order p by Langrange's Theorem.

Pick $a \in G$ with $|a|= p$, and $b \notin \langle a\rangle$ also with $|b|= p$. Then $\langle a\rangle \cap \langle b\rangle = \{e\}$.

We know that $\langle a\rangle \cap \langle b\rangle \leq \langle b\rangle$, so $|\langle a\rangle \cap \langle b\rangle| \in \{1, p\}$. If its order is p, then $b \in \langle a\rangle \cap \langle b\rangle$, so $b \in \langle a\rangle$ which is a contradiction.

We know that G is Abelian, then $a^i b^j$ for $i = 0, \ldots, p-1$, and $j = 0, \ldots, p-1$ are p^2 elements of G and the subgroup they generate is isomorphic to $\mathbb{Z}_p \times \mathbb{Z}_p$, where $a^i, b^j \mapsto (\bar{i}, \bar{j})$. So

$$G \cong \mathbb{Z}_p \times \mathbb{Z}_p$$

Group Actions on Subsets

If $G \curvearrowright S$, and $U \subseteq S$ is any subset, then we can define

$$a * U = \{a * u \mid u \in U\}$$

So here, we take subsets to other subsets.

Claim: $|U| = |a * U|$

Proof: Let $f : U \to a*U$ defined as $u \mapsto a*u$. There's many ways to show that this is surjective, but perhaps more interestingly, let's instead define an inverse function.

Let $g : a * U \to U$ defined as $x \mapsto a^{-1} * x$. First, we check that $\text{Im}(g) \subseteq U$. If $x \in a * U$, then $x = a * u$, for some $u \in U$. Then $g(x) = a^{-1} * x = a^{-1} * (a * u) = (a^{-1}a) * u = e * u = u \in U$.

Now we check that, in fact, $g = f^{-1}$,

$$g(f(u)) = g(a * u) = a^{-1} * (a * u) = u$$

Similarly, $f(g(x)) = x$, so f and g are bijections.

Note.

So group actions on subsets take subsets to other subsets of the same size!

So G acts on the subsets of order n for any $n \leq |S|$ by $G \curvearrowright \{U \subseteq S \mid |U| = n\}$ with

$$\underbrace{a * U}_{\text{Group Action}} = \underbrace{a * U}_{\text{Action on subsets as defined above}}$$

Let's look at an

Example.

$S_3 \curvearrowright \{1, 2, 3\}$ by permutation. Also $S_3 \curvearrowright \{\{1, 2\}, \{1, 3\}, \{2, 3\}, \}$. For example

- $(123) * \{1, 2\} = \{2, 3\}$
- $(123) * \{1, 3\} = \{2, 1\}$

- $(123) * \{2, 3\} = \{3, 1\}$

17 Permutation Representation

Definition.

A **permutation representation** of G is a homomorphism $\varphi : G \to S_n$ for some n.

let $S = \{1, \ldots, n\}$

Proposition: There is a bijection

$$\{\text{actions } G \curvearrowright S\} \leftrightarrow \{\text{permutation representations } \varphi : G \to S_n\}$$

Proof: Given an action $G \curvearrowright S$ we want a hom $\varphi : G \to S_n$. Given $a \in G$, let $\varphi(a) = \sigma_a \in S_n$, where $\sigma_a : S \to S$ is the bijection $\sigma_a(i) = a * i$.

We can check that φ is a hom:

$$\begin{aligned} \varphi(ab)(i) &= \sigma_{ab}(i) = (ab) * i \\ &= a * (b * i) = \sigma_a(\sigma_b(i)) \\ &= (\varphi(a) \circ \varphi(b))(i) \end{aligned}$$

So $\sigma_{ab} = \sigma_a \sigma_b$ so φ is a homomorphism.

Conversely, given $\varphi : G \to S_n$ a hom, define an action $G \curvearrowright S$ by $a * i = \varphi(a)(i)$

(i.e. check that this is a group action.)

These correspondences are inverses, so we have a bijection.

Similarly: If S is any set, we have a group $\text{Perm}(S)$, the group of permutations of S, the set of bijections $S \to S$.

Then, $\{G \curvearrowright S\} \leftrightarrow \{$ hom $\varphi : G \to \text{Perm}(S)\}$ is one to one.

So group actions are really just homomorphisms in disguise!

Recall: If $\varphi : G \to G'$ is injective, then $\ker \varphi$ is trivial, and so the first isomorphism theorem tells us that $G \cong \text{Im}(G)$, and furthermore, $G \cong$ subgroup of G'

Definition.

A permutation representation $\varphi : G \to \text{Perm}(S)$ is called **faithful** if it's injective.

An action $G \curvearrowright S$ is **faithful** if the only $a \in G$ with $a * s = s$ for all $s \in S$ is $a = e$.

Note: $a * s = s$ for all $s \in S$ if and only if $\varphi(a) = e \in \text{Perm}(S)$ if and only if $a \in \ker(\varphi)$

So $\varphi : G \to \text{Perm}(S)$ is faithful if and only if $G \curvearrowright S$ is faithful.

18 Cailey's Theorem

Every group is isomorphic to a subgroup of some (potentially infinite) permutation group.

Proof: Our goal is to find a faithful permutation representation $\varphi : G \to \text{Perm}(S)$, then G is isomorphic to a subgroup of $\text{Perm}(S)$.

So let $G \curvearrowright G$ by $a * g = ag$. If $a * g = g$ for all $g \in G$, then $a * e = e$, which tells us that $a = e$, so this is a faithful action. Hence the corresponding permutation representation $\varphi : G \to \text{Perm}(S)$ is faithful.

In particular, if $|G| = n$, then $\text{Perm}(G) \cong S_n$, so $G \cong H \leq S_n$.

Note.

All of finite Group Theory is isomorphic to subgroups of the symmetric group.

Wed. Mar 6 2024

Author Note.

Question 6 is challenging. We have a class equation: $20 = 1 + 4 + 5 + 5 + 5$. We're looking for subgroups, we should be looking for the $Z(a)$ for certain elements.

We know that the order is equal to $\frac{20}{|C(a)|}$

We know that normal subgroups are unions of conjugacy classes, including the conjugacy class of the identity $C(e)$.

A subgroup of order 4 is not possible, 5 is and we want to prove it. If $|Z(a)|= 5$, then $Z(a) = \{e, a, a^2, a^3, a^4\}$. We want to show that $Z(a) = C(e) \cup C(a)$, i.e. we want to show that $C(a) = \{a, a^2, a^3, a^4\}$. Instead of finding b such that $aba^{-1} = a^2$, etc...

Show that $|C(a^2)|= 4$, but there is only one such conjugacy class, so it must be the same and $a^2 \in C(a)$ and so $C(a^2) = C(a)$.

The way that you would say this is by saying $\frac{20}{|Z(a^2)|}$. Remember: the larger the centralizer, the smaller the conjugacy class.

Question 2: $H \leq \text{Stab}(S)$, don't forget to prove that H is also a subgroup.

19 Sylow Theorems

This is the last topic in Group Theory for this class.

Recall: We know from Lagrange's Theorem that if $H \leq G$, then $|H|$ divides $|G|$, but in general, the converse is false.

Our goal is to come up with the best converse that we can, in generality.

Definition.

If $|G|= p^e m$ where p is prime, $e > 0$ and $p \nmid m$, then $H \leq G$ is a **Sylow p subgroup of G** if $|H|= p^e$, in other words, it's the highest power of p possible.

The set of Sylow p subgroups of G is denoted by $\text{Syl}_p(G)$.

19.1 First Sylow Theorem

If p divides $|G|$, then there exists a Sylow p subgroup of G.

Proof: Say $|G|= n = p^e m$ where $p \nmid m$.

Let $S = \{U \subseteq G \mid |U|= p^e\}$ (our hope is that one of these is actually a subgroup, if so great!) Immediately, we know that $|S|= \binom{n}{p^e} = \frac{n!}{p^e!(n-p^e)!}$.

Lemma: $|S|$ is not divisible by p. This is just a counting question, if you're not convinced, just expand the form above and see for yourself.

Consider $G \curvearrowright S$ by left multiplication. We know that the orbits partition S, so

$$|S| = \sum_{\text{orbits}} |\text{orbits}|$$

By our lemma, the left hand side is not divisible by p, which means that there exists at least one orbit O_u with $|O_u|$ not divisible by p.

Let $H = \text{Stab}(U) = \{a \in G \mid aU = U\}$. Then elements of H permute the elements of U. Consider $H \curvearrowright U$, where $h * u = hu$ by left multiplication (same action as above.) The orbit of $u \in U$, is Hu, which is a right coset of H, which means that the orbit of U has the same size as the coset, in other words

$$|O_u| = |Hu| = |H|$$

Just like before, the orbits partition U, so we know that $|U| = \sum_{\text{orbits}} |\text{orbit}|$, but then $p^e = \sum_{\text{orbits}} |H|$, which means that $p^e = |H| * (\text{number of orbits})$, so then $|H|$ must be a power of p.

$$H = p^i$$

So we have a subgroup, and it's a p group! But now we need to figure out what power it is.

Going back to our group action, by the Orbit Stabilizer Theorem,

$$|G| = |H||O_u| = |\text{Stab}(U)| \cdot |O_u|$$

But recall that $|O_u|$ is not divisible by p, in other words, $p^e m = p^i k$, where k is not divisible by p, so in fact, $i = e$ and $|O_u| = m$, and H in fact, is a Sylow p subgroup.

Corollary: (Cauchy's Theorem)

If p is prime and p divides $|G|$, then G contains an element of order p.

Proof: Let H be a Sylow p subgroup of G, and let $a \in H$ be non-trivial. Then $|a|$ divides $|H|$ meaning that $|a| = p^i$ for some $i \geq 1$. Then $a^{p^{i-1}}$ has order p (as an example, consider $p = 2$ and $i = 3$).

19.2 Second Sylow Theorem

1. All Sylow p subgroups are conjugate

   i.e. if H and H' are Sylow p subgroups, then, there's an element $a \in G$ such that $aHa^{-1} = H'$.

   This means that you can get from any H to H' on some element $a \in G$, where $H, H' \in \text{Syl}_p(G)$

2. If $K \leq G$, and $|K| = p^i$, then there exists a group $H \in \text{Syl}_p(G)$ such that $K \leq H \leq G$.

   Every p group sits inside a Sylow p subgroup.

Corollary:

$$\text{Syl}_p(G) = \{H\} \Leftrightarrow H \trianglelefteq G$$

Having only a single Sylow p subgroup means that it is normal!

Proof: $\text{Syl}_p(G) = \{H\}$ if and only if $aHa^{-1} = H$ for all $a \in G$, and this means that H is normal.

19.3 Third Sylow Theorem

Let $n_p = |\text{Syl}_p(G)|$ and let $|G| = p^e m$, $e \geq 1$, p is prime, and p does not divide m. Then

- $n_p | m$

  The number of Sylow p subgroups divides m.

- $n_p \equiv 1 \pmod{p}$

  The number of Sylow p subgroups is one more than a multiple of p.

- $n_p = [G : N_G(H)]$, where $N_G(H)$ is the normalizer, defined as

$$N_G(H) = \{a \in G \mid aHa^{-1} = H\}$$

Even if H is not normal, the normalizer is the things in G that make H look normal.

QUESTION Does that mean the center is the normalizer of G?

Theorem: If $|G|= 35$, then $G \cong \mathbb{Z}_{35}$

Proof: $35 = 5 \cdot 7$, let $H \in \text{Syl}_5(G)$, $K \in \text{Syl}_7(G)$. Then $n_5 \mid 7$ and $n_5 \equiv 1 \pmod 5$, which means that $n_5 = 1$ and H is normal.

$n_7 \mid 5$ and $n_7 \equiv 1 \pmod 7$, which means $n_7 = 1$ and K is normal.

We have that $H = \langle h \rangle$ and $K = \langle k \rangle$, and $H \cap K = \{e\}$, so we can write the isomorphism $\mathbb{Z}_5 \times \mathbb{Z}_7 \to G$, defined as $(i, j) \mapsto h^i k^j$

Check: $hk = kh$, so it's Abelian!

Fri. 8 Mar 2024

Today is the final day of Group Theory! We're going to move over to Rings!

We've been using a Theorem without stating it this whole time!

How to recognize your group is a product?

Theorem.

If $H, K \trianglelefteq G$, with $H \cap K = \{e\}$ and $G = \{hk \mid h \in H, k \in K\}$, then

$$G \cong H \times K$$

Proof: Let $\varphi : H \times K \to G$ for which $(h, k) \mapsto hk$. Since $HK = G$, we automatically know that φ is surjective. Since G might not be finite, we still need to show injectivity.

If $\varphi(h, k) = \varphi(h', k')$, then $hk = h'k'$, which means $(h')^{-1}h = k'k^{-1}$, which are both in $H \cap K = \{e\}$, so in fact $h = h'$ and $k = k'$ and φ is injective.

To show that φ is a hom, simply notice that $\varphi(hh', kk') = hh'kk'$. This is equal to $hkh'k' = \varphi(h, k)\varphi(h', k')$ if H and K commute.

So given $h \in H$ and $k \in K$, consider $(hkh^{-1})k^{-1}$. Notice that, since K is normal, $(hkh^{-1}) \in K$, and so in fact, $(hkh^{-1})k^{-1} \in K$. However notice that $(hkh^{-1})k^{-1} =$

$h(kh^{-1}k^{-1}) \in H$ since H is normal, so $hkh^{-1}k^{-1} \in H \cap K = \{e\}$ so $hkh^{-1}k^{-1} = e$ and so $hk = kh$.

Let's take this for a spin in another

Theorem:

If $|G| = pq$, where p and q are prime with $p > q$ and $q \equiv 1 \pmod{p}$, then

$$G \cong \mathbb{Z}_{pq}$$

Proof. We know that $n_p = |\mathrm{Syl}_p(G)|$ satisfies $n_p \mid q$ and $n_p \equiv 1 \pmod{q}$. But $q \not\equiv 1 \pmod{p}$, so $n_p = 1$. Additionally, n_q satisfies $n_q \mid p$ and $n_q \equiv 1 \pmod{q}$ so $n_q = 1$.

Remember: $n_p = 1$ if and only if $H \in \mathrm{Syl}_p(G)$ is normal. So there exists $H, K \trianglelefteq G$ with $|H| = p$ and $|K| = q$.

We should see that $H \cap K = \{e\}$ since it must divide both orders but only 1 divides two different primes.

Now we need only check that their product is the entire group, but these groups are finite, so simply notice that $HK = G$, since $|HK| = |H||K| = pq = |G|$, *because* their intersection is trivial.

So in fact, $G \cong H \times K \cong \mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq}$ since $\gcd(p, q) = 1$. □

20 Group Presentations

Recall: Every element of D_{2n} is a product of x and y where $x^2 = e$, $y^n = e$, and $xyx = y^{-1}$. Then, we can write the group as follows

$$\langle x, y \mid x^2 = y^n = xyxy = e \rangle$$

Similarly, we could say that

- Every element of $\mathbb{Z}_n$ is a sum of $\bar{1}$ and $\bar{1} \cdot n = \bar{0}$

Definition.

A set $\{x_1, \ldots, x_n\} \subseteq G$ **generates** G if every element in G is a product of the x_i and their inverses.

Definition.

A **relation** in the generators is a product of x_i and their inverses that is $e \in G$.

For example $x^2, y^n, xyxy \in D_{2n}$.

Definition.

A **word** in the generators is any product of x_i and their inverses.

Definition.

The **free group** on n generators is

$$F_n = \langle x_1, \ldots, x_n \rangle$$

Is the group with n generators and the only relations are the "obvious ones", i.e. conjugates of the identity. For example

$$x_1 x_2 x_3 x_3^{-1} x_2^{-1} x_1^{-1} = e$$

Example.

$F_1 = \langle x \rangle \cong (\mathbb{Z}, +)$ by $\varphi : \mathbb{Z} \to F_1$ for which $n \mapsto x^n$.

Example.

$F_2 = \langle x, y \rangle$ has elements

$$F_2 = \{e, x, x^2, \ldots, x^{-1}, x^{-2}, \ldots, y, y^2, \ldots, y^{-1}, y^{-2}, \ldots, xy, xy^2, \ldots, xy^{-1}, x^{-1}y, \ldots, xyx^{-2}y^3x^{-7}, \ldots, y$$

Let $R \subseteq F_n$ be some subset. For example $R = \{x^2, y^n, xyxy\} \subseteq F_2$. We define $N_R \trianglelefteq F_2$ to be the smallest normal subgroup of F_n that contains R.

What does this look like? Well

Lemma:

An element $g \in N_R$ if and only if g can be attained by a finite sequence of

1. products by elements in R
2. inversions
3. conjugation by elements of F_n

Let's look at an

Example.

$R = \{x^2, y^n, xyxy\} \subseteq F_2$. Then N_R contains $(xy)(y^n xyxy)(xy)^{-1}(yx^2)(x^2)^{-1}(yx^2)^{-1}$.

We have a product of conjugates of elements inside R.

Definition.

The group $\langle x_1, \ldots, x_n \mid R\rangle$ is F_n/N_R. In fact we write it as

$$\langle x_1, \ldots, x_n | r_1, \ldots\rangle$$

Where $R = \{r_1, \ldots\}$

Example.

We know that $\mathbb{Z}_n \cong \mathbb{Z}/\langle n\rangle \cong F_1/\langle x^n\rangle = \langle x|x^n\rangle$.

Example.

The product group $\mathbb{Z} \times \mathbb{Z} \cong \langle x, y \mid xyx^{-1}y^{-1}\rangle$, or in other words $xy = yx$ (it commutes).

We can do a little more!

Example.

Say we have $\mathbb{Z}_n \times \mathbb{Z}_m \cong \langle x, y \mid x^n, y^n, xyx^{-1}y^{-1}\rangle$

Unsurprisingly,

Example.

$D_{2n} \cong \langle x, y \mid x^2, y^n, xyxy \rangle$

These are called **group presentations**, G is called finitely generated if it has a finite generating set.

G is **finitely presented** if it has presentation

$$\langle x_1, \ldots, x_n \mid r_1, \ldots, r_m \rangle$$

Mon 11 Mar 2024

21 Rings

Definition.

A **ring** is a set R with binary operations $+$ and $\times$ satisfying:

1. $(R, +)$ is an Abelian group. We denote its identity by 0.
2. $(R, \times)$ is associative, and has an identity denoted 1.

   We write ab instead of $a \cdot b$

   We do not necessarily have multiplicative inverses!
3. $+$ and $\times$ satisfy
   (a) $a(b + c) = ab + ac$
   (b) $(b + c)a = ba + ca$

   For all $a, b, c \in R$

Definition.

A **commutative ring** has commutative multiplication.

i.e. $ab = ba$ for all $a, b \in R$

Note.

In fact, for us, "ring" really means "commutative ring" unless otherwise stated.

Example.

A basic example is $\mathbb{Z}$, but we also have $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ under the regular addition and multiplication.

Example.

A **non-commuting** example: $\text{Mat}_n(\mathbb{R})$, the set of $n \times n$ matrices with entries in $\mathbb{R}$.

non-commuting here meaning multiplication of course. Addition is still Abelian. This is still a Ring, just not a commutative one.

Definition.

A **subring** of a ring is a subset that

1. is closed under $+$ and $\times$.
2. has additive inverses.
3. contains 1.

There is no notation for subrings!

Example.

$Z \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$ is a list of subrings.

Example.

$\mathbb{Z}[i]$ (pronounced $\mathbb{Z}$ adjoin i, or in this very particular case, the Gaussian integers)

This is the set of complex numbers $a + bi$, but a, b are integers, and the usual $+$ and $\times$ from $\mathbb{C}$.

Check Closure:

1. $(a + bi) + (c + di) = (a + c) + (b + d)i$
2. $(a + bi)(c + di) = (ac - bd)(ad + bc)i$

Example.

If $\alpha \in \mathbb{C}$, $\mathbb{Z}[\alpha]$ (Z adjoin α) is the subring of $\mathbb{C}$ generated by α.

$\mathbb{Z}[\alpha]$ is the smallest subring of $\mathbb{C}$ that contains α.

What's in $\mathbb{Z}[\alpha]$

1. $1 \in \mathbb{Z}[\alpha]$, so it contains the integers
2. $\alpha \in \mathbb{Z}[\alpha]$, so $a + b\alpha$ for $a, b \in \mathbb{Z}$, also $\alpha^2 = \alpha \cdot \alpha$, α^3, or

$$a_0 + a_1\alpha + a_2\alpha^2 + \cdots a_n\alpha^n$$

for $a_i \in Z$

Example.

What about $\mathbb{Z}[1/2]$. This contains all powers of $1/2$, and hence any $\frac{x}{2^n}$ for $x \in \mathbb{Z}$.

Example.

Let's look at $\mathbb{Z}[\sqrt[3]{2}] = \{a + b\sqrt[3]{2} + c\sqrt[3]{2} \mid a, b, c \in Z\}$

Similarly, we can look at $\mathbb{Q}[\alpha]$, or $\mathbb{R}[\alpha]$. These are the smallest subrings of the complex numbers containing $\mathbb{Q}$ (or $\mathbb{R}$) and α.

Additionally, $\beta \in \mathbb{Q}[\alpha] \Leftrightarrow \beta$ is a polynomial in α with the coefficients in $\mathbb{Q}$, i.e.

$$\beta = a_0 + a_1\alpha + a_2\alpha^2 + \cdots a_n\alpha^n$$

Example.

$\mathbb{Z}_n$ with operations $+ \pmod n$ and $\times \pmod n$ is a ring. However this is not a subring $\mathbb{C}$

Definition.

A **unit** in R is a $r \in R$ that has a multiplicative inverse, i.e. $r' \in R$ with $rr' = r'r = 1$.

Example.

1. In $\mathbb{Z}$, our units are ± 1.
2. In $\mathbb{Q}, \mathbb{R}, \mathbb{C}$, our units are any non-zero elements.
3. In $\mathbb{Z}_n$, units are $\bar{k}$ where $\gcd(k, n) = 1$
4. In $\mathbb{Z}[i]$, units are ± 1, and $\pm i$

Check:

$$\frac{1}{a+bi} = \frac{a-bi}{(a+bi)(a-bi)} = \frac{a-bi}{a^2+b^2} = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}i \in \mathbb{C}$$

If this is in $\mathbb{Z}[i]$, then we need $\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2} \in \mathbb{Z}$. But if $|a| > 1$, that won't work, Similarly for b.

Note of course that, even if $|a| = 1$ and $|b| = 1$, this still doesn't work. So in fact, one of these absolute values must be zero. So in fact, ± 1 and $\pm i$ are the only possible units.

Example.

Exactly from this work, we get that in $\mathbb{Q}[i]$, units are all non-zero elements.

In $\mathbb{Z}[\sqrt{2}]$, units are... **TODO** too lazy to write this!

Definition.

A **field** is a commutative ring where every non-zero element is a unit.

i.e. $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p, \mathbb{Q}[i], \mathbb{Q}[\sqrt{2}]$

Wed 13 Mar 2024

Note.

Homework is due tomorrow on the Sylow Theorem. For number 4, you can use the theorem used in class.

22 Polynomial Rings

If x is a variable (i.e. not a specific element of $\mathbb{C}$) then

$$\mathbb{Z}[x] = \{a_0 + a_1 x + \cdots a_n x^n \mid a_i \in \mathbb{Z}, n \geq 0\}$$

Is the polynomial ring with variable x and coefficients in $\mathbb{Z}$.

Example.

If R is any ring, then $R[x]$ is the ring of polynomials in variable x with coefficients in R.

If we have $f(x) = a_0 + a_1x + \cdots a_nx^n \in R[x]$ and $a_n \neq 0$, then

1. the **degree** of $f(x)$ is n
2. the **leading coefficient** is a_n
3. f is **monic** if $a_n = 1$
4. f is **constant** if $\deg f = 0$ or $f = 0$

Note.

Convention says that the degree of $f(x) = 0$ is undefined.

Let's define addition and multiplication. If $f(x) = a_0 + a_1x + \cdots a_nx^n$ and $g(x) = b_0 + b_1x + \cdots b_mx^m$ and assume that $n \geq m$. Then

1. $f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + \cdots (a_n + b_n)x^n$ where $b_n = 0$ for $n > m$.
2. $f(x)g(x) = (a_0b_0) + (a_0b_1 + a_1b_0)x + \cdots$

We have our **additive identity**: $f(x) = 0$ and our **multiplicative identity**: $f(x) = 1$.

R can be thought of as a subring of $R[x]$, in fact elements in our ring correspond to polynomials

$$r \in R \leftrightarrow f(x) = r$$

22.1 Division with Remainder

If R is a ring, and $f, g \in R[x]$ and f is monic, then there exists unique $q, r \in R[x]$ with

$$g = fq + r$$

and $r(x) = 0$ or $\deg r < \deg f$.

Existence; Long Division

Uniqueness: If $g = fq + r = fq' + r'$ with $q' \neq q$ and $r' \neq r$, then $r - r' = f(q' - q)$ and so the left hand side must have deg $< f$, but the right hand side has deg$f$ because f is monic.

The leading coefficient of $f(q - q')$ = leading coefficient of $q - q'$.

Why does being monic matter here?

Consider $\mathbb{Z}_4[x]$, $(\bar{2}x)(\bar{2}x) = \bar{4}x^2 = \bar{0}$ so two polynomials of degree 1 multiply to a polynomial of undefined degree.

The point is that if the leading coefficient of one of them is 1, then the degree does not increase.

Example.

In $\mathbb{Z}_4[x]$, let's take $g = \bar{2}x^2 + \bar{1}x + \bar{3} = \bar{2}x^2 + x + \bar{3}$, and $f = x + \bar{2}$.

Long Division:

TODO See picture for Mar 13 2024

So $q = \bar{2}x + \bar{1}$, $r = \bar{1}$, and $g = fq + r$.

Similarly, if the leading coefficient of f is a unit $u \in R$, then we can write $f = f \cdot \bar{f}$, where $\bar{f}$ is a monic, where $\bar{f}$ is effectively f with u factored out.

If $g = \bar{f}q + r$, then $g = (u\bar{f})(u^{-1}q) + r = f(u^{-1}q) + r$. So we can do the division algorithm with f as well.

Corollary: If $f \in R[x]$ and $\alpha \in R$, then the remainder of dividing f by $x - \alpha$ is $f(\alpha)$

Proof: $x - \alpha$ is monic, so write $f = (x - \alpha)q + r$, where $r = 0$, or constant, since $\deg r < \deg(x - \alpha) = 1$.

Plug in α, then $f(\alpha) = r(\alpha)$, but r is constant, so $r(x) = f(\alpha)$.

Note.

This is the same as saying that you can factor out a root out of your polynomial, which should make sense!

If we work with more than one variable, we can make the polynomial ring

$$R[x_1, \ldots, x_n] = \text{polynomials in } x_i \text{ with coefficients in } R$$

Definition.

The characteristic of R is the smallest $n \in \mathbb{N}$ such that

$$\underbrace{1 + 1 + \cdots + 1}_{n \text{ times}} = 0$$

And $\text{char}R = 0$ if no such n exists.

Example.

1. $\text{char}\mathbb{Z} = 0$
2. $\text{char}\mathbb{Z}_n = n$
3. $\text{char}R[x] = \text{char}R$

22.2 Homomorphisms

Definition.

$\varphi : R \to R'$ is a **ring homomorphism** if 3 properties hold.

1. $\varphi(a + b) = \varphi(a) + \varphi(b)$
2. $\varphi(ab) = \varphi(a) o \varphi(b)$
3. $\varphi(1_R) = 1_{R'}$ (The multiplicative identity is preserved)

Definition.

We say that φ is a **ring isomorphism** if it's a bijective ring homomorphism.

Let's look at some

Example.

$\varphi_k : \mathbb{Z} \to \mathbb{Z}$ is the map that takes $n \mapsto kn$ for some fixed $k \in \mathbb{Z}$. And

$$\varphi_k(a+b) = k(a+b) = ka + kb = \varphi_k(a) + \varphi_k(b)$$

But multiplication causes some issues

$$\varphi_k(ab) = k(ab)$$

and

$$\varphi_k(a)\varphi_k(b) = k^2ab$$

But now, the identity rule tells us that $\varphi_k(1)_k = k = 1$, so in fact, $id_{\mathbb{Z}} : \mathbb{Z} \to \mathbb{Z}$ with $n \mapsto n$ is the only ring homomorphism $\mathbb{Z} \to \mathbb{Z}$

Fri. 15 March 2024

We've been talking about Ring Homomorphisms $\varphi : R \to R'$, which satisfies 3 conditions:

1. $\varphi(a+b) = \varphi(a) + \varphi(b)$
2. $\varphi(ab) = \varphi(a) o \varphi(b)$
3. $\varphi(1_R) = 1_{R'}$ (The multiplicative identity is preserved)

Let's look at some more examples

Example.

$\varphi : \mathbb{Z} \to \mathbb{Z}_n$ is a ring homomorphism which maps $x \mapsto \bar{x}$

Example.

If R is any ring, there is a **unique** hom $\varphi : \mathbb{Z} \to R$ and the map is $\varphi(1) = 1_R$ and

$$\varphi(n) = \begin{cases} 1_R + \cdots + 1_R & n > 0 \\ 0 & n = 0 \\ -1_R - \cdots - 1_R & n < 0 \end{cases}$$

This is the only map from the integers to a ring that satisfies the conditions of ring homomorphisms.

On the other hand,

Example.

There is **no** ring hom $\varphi : \mathbb{Z}_n \to \mathbb{Z}_n$. If $\varphi(\bar{1}) = x$, then

$$\varphi(\underbrace{\bar{1} + \cdots + \bar{1}}_{n}) = \varphi(\bar{0}) = 0$$

But $\varphi(\bar{1} + \cdots + \bar{1}) = nx$ which means $x = 0$. The problem is that ring homs must take the multiplicative identity of the input to the multiplicative identity of the output. So we need $\varphi(\bar{1}) = 1$, so no such φ exists.

Example.

If R is a ring, with $r \in R$ any element, there is a hom $\text{eval}_r : R[x] \to R$ with $f(x) \mapsto f(r)$. It takes a polynomial and plugs in r instead of x.

This is a hom since plugging in before you add an multiply in a polynomial is the same thing as plugging in after you add and multiply the polynomial.

Example.

If $R \subseteq R'$ is a subring, and $\alpha \in R'$, then there is a hom $\text{eval}_\alpha : R[x] \to R'$ where $f(x) = f(\alpha)$.

Note here that the point is that this is still a good homomorphism even if $\alpha \notin R$. For instance, If R is the rationals and R' is the reals, plugging in π into your polynomial now gives you real outputs instead of just rationals. But this is completely fine.

Of course if $\alpha \in R$ then $\Im(\text{eval}_\alpha) = R$, however if $\alpha \in R'$, then $\Im(\text{eval}_\alpha) = R[\alpha]$, the smallest subring which contains both R and α.

QUESTION We keep saying that $R[\alpha]$ is the smallest subring which contains R and α but never proved it. Why not?

Example.

If we have any $\varphi : R \to R'$ a hom, we can get another homomorphism

$$R[x] \to R'$$

Where $\sum a_i x^i \mapsto \sum \varphi(a_i) x^i$. In other words, we apply φ to all the coefficients

We can actually use these last two examples to create different polynomial rings and evaluate them.

Let's look at one more

Example.

For any ring R, $\varphi : R \to R[x]$ with $r \mapsto f(x) = r$ is a ring hom.

In other words, we take a number and map it to the constant polynomial of that number. Exhilarating.

Now we get to talk about Kernels.

Definition.

If $\varphi : R \to R'$ is a ring homomorphism, the **kernel** of φ is

$$\ker(\varphi) = \{r \in R \mid \varphi(r) = 0\}$$

Note: Not 1!

Under every ring homomorphism is a group homomorphism, if we just *forget* about multiplication in R and R', we're left with Abelian groups.

In other words, the kernel of the ring homomorphism is the same as the kernel of the group homomorphism.

So in fact $\ker(\varphi)$ is still a subgroup! Moreover, its a normal subgroup since R and R' are Abelian groups.

Remark: If $s \in \ker(\varphi)$ and $r \in R$, then $\varphi(rs) = \varphi(r)\varphi(s) = \varphi(r) \cdot 0 = 0$, which means that $rs \in \ker(\varphi)$.

This is interesting because, we already knew that $\ker(\varphi)$ is a subgroup, but now we also see that it has multiplicative properties. If you take anything in this kernel, and *scale it* by any element of your ring, it stays in the kernel!

Note.

$\ker(\varphi)$ is **not necessarily** a ring, as it does not necessarily contain 1.

This is motivation for our next

Definition.

An **Ideal** I of a ring R is a non-empty subset $I \subseteq R$ that satisfies

1. $(I, +) \leq (R, +)$

   It is a subgroup of R as an additive group. We can also note that it is normal since R as a group is normal (although this is not part of the definition.)

2. If $s \in I$ and $r \in R$, then $rs \in I$

This captures what our kernel is!

Note.

If you don't have commutative multiplication, you can talk about *left ideals* and *right ideals* based on which side you multiply from.

For the kernel, this doesn't make any difference between you're multiplying by zero, so it's always both a left and right ideal.

Equivalently, $I \neq \varnothing$, and for any $s_1, \ldots, s_n \in I$,

$$r_1 s_1 + \cdots + r_n s_n \in I \text{ for all } r_i \in R$$

Example.

The **principal ideal** generated by $a \in R$ is

$$I = (a) = \{ra \mid r \in R\}$$

Also sometimes denoted aR or Ra

Check: $(a) \neq \varnothing$ as $0, a \in (a)$

If $r_1 a, r_2 a, \ldots, r_n a \in (a)$ and $r_1' \ldots, r_n' \in R$, then

$$r_1'(r_1 a) + \cdots + r_n'(r_n a) = (r_1' r_1 + \cdots + r_n' r_n)a \in (a)$$

So it's closed under linear combinations in R, and non-empty.

We have two principal ideals:

1. $(1) = R$, called the **unit ideal**

   This gives you the whole ring

2. $(0) = \{0\}$, called the **zero ideal**

Any other ideal is called a **proper ideal**.

Note.

Ideals are *almost* subrings, except they don't contain 1 unless your ideal is the entire ring.

Because once you have 1, you get all multiples of 1, so you get the whole ring.

Besides that, it satisfies all the properties of a subring!

Example.

$\text{eval}_2 : \mathbb{R}[x] \to R$ which maps $f(x) \mapsto f(2)$, now

$$\begin{aligned}\ker(\text{eval}_2) &= \{f(x) \in \mathbb{R}[x] \mid f(2) = 0\} \\ &= \{f(x) \mid \ f(x) \text{ is divisible by } (x-2)\}\end{aligned}$$

So in fact, this is all polynomials which are multiples of $(x-2)$, so

$$\begin{aligned}\ker(\text{eval}_2) &= \{f(x) \mid \ f(x) \text{ is divisible by } (x-2)\} \\ &= \{(x-2)g(x) \mid g(x) \in \mathbb{R}[x]\} \\ &= (x-2)\end{aligned}$$

So this is an ideal generated by $(x-2)$

Example.

Similarly, if $\text{eval}_r : R[x] \to R$ and $r \in R$ for which $f(x) \mapsto f(r)$, then

$$\ker(\text{eval}_r) = (x - r)$$

Definition.

The ideal generated by $a_1, \ldots, a_n \in R$ is

$$(a_1, \ldots, a_n) = \{r_1 a_1 + \cdots + r_n a_n \mid r_1, \ldots, r_n \in R\}$$

So by design, satisfies the properties of an ideal.

This gives us interesting examples.

Example.

Look at $(2, x) \subseteq \mathbb{Z}[x]$. This contains all polynomials with an even constant term. Why? Well, when you take multiples of x, you get polynomials with no constant terms. But then, we can start adding multiples of 2 and get any even constants.

This ideal cannot be written as a principal ideal, which is generated by a single element.

Proposition: If F is a field, $I \subseteq F$ is an ideal, then $I = (0)$ or $I = (1) = F$.

Proof. If $I \neq (0)$, then there is some $a \in I$ with $a \neq I$, but since F is a field, $a^{-1} \in F$, but then $a^{-1}a = 1 \in I$. But then $1 \in I$ so $I = (1) = F$.

Once you have a unit, you have 1, and once you have 1, you have everything.

Mon. 25 March 2024

Recall: An ideal $I \subseteq R$ is a subgroup under addition, and for all $s \in I$, $r \in R$, $rs \in I$.

Here's one thing that we talked about last time.

Proposition: If F is a field, $I \subseteq F$ is an ideal, $I = F$ or $I = (0)$. We proved this last time.

Today, we want to go the other way.

Proposition: If R is a ring with only 2 ideals, R and (0), then R is a field.

Proof: Let $a \neq 0$ be in R, then consider (a), we know that $(a) \neq (0)$, because it contains a. So it must be that this ideal is the entire ring, and $(a) = R$. Additionally, this must mean that $1 \in (a)$, which means that there exist some element $r \in R$ such that $ra = 1$. But this is exactly what we mean by a unit, it has an inverse. Since a was arbitrary, R must be a field.

From this proof, we actually see that, if you take a principal ideal (a) generated by an element, that

$$(a) = R \Leftrightarrow a \text{ is a unit}$$

Corollary: If $\varphi : F \to R$ is a ring hom, where F is a fiel, then φ is injective.

Proof: $\ker(\varphi) \subseteq F$ is an ideal. So in fact, $\ker(\varphi)$ is either (0), or all of F. If $\ker(0) = \{0\}$, then φ is injective. If $\ker(\varphi) = F$, then $\varphi(1) = 0$, but we needed $\varphi(1) = 1$, so this can't be the case and thus $\ker(\varphi) = \{0\}$ and φ is injective.

Remark. The second case above actually *can* happen in a special case. The set $\{0\}$ *can* be thought of as a ring, where $0 = 1$. But usually and for subtle reasons, we don't consider this a ring and we enforce 0 and 1 to be different.

22.3 Ideals of $\mathbb{Z}$

Example.

Any ideals $I \subseteq \mathbb{Z}$ is also a subgroup of $(\mathbb{Z}, +)$, which means that $I = n\mathbb{Z}$ for some $n \in \mathbb{Z}$ (since it must be a subgroup of $\mathbb{Z}$)

And these are all possible ideals! In other words: $n\mathbb{Z} = (n)$ is an ideal in $\mathbb{Z}$.

Proposition: If F is a field, then every ideal in $F[x]$ is a *principal ideal* (generated by one element.) In other words, if $I \subseteq F[x]$ is an ideal, then $I = (f)$ for some $f \in F[x]$.

Proof: The idea for this proof is to emulate the proof of the subgroups of $\mathbb{Z}$. Let $I \subseteq F[x]$ be an ideal, and assume $I \neq (0)$. Choose $f \in I$ of smallest possible degree.

We want to show that $I = (f)$.

If $g \in (f)$, then $g = fh$ for some $h \in F[x]$, but since $f \in I$, $fh \in I$ and $g \in I$. Hence $(f) \subseteq I$.

Conversely, if we have a $g \in I$, we can write $g = fq + r$ where $r = 0$ or $\deg(r) < f$. We can do this because the leading coefficient of f is a unit, **because f is a field.** **QUESTION** What's this about again? Why does this work?

Now, $f \in I$, so $fq \in I$, so $g, fq \in I$ which means that $r = g - fq \in I$. If $r \neq 0$, then r is an element of I of smaller degree than f, which is a contradiction because we chose f least. This must mean that $r = 0$, and so $g = fq \in (f)$, hence $I \subseteq (f)$.

Therefore $I = (f)$.

Remark: This will work in $R[x]$ anytime we have some sort of division algorithm. We'll return to this.

Definition.

If F is a field, $f, g \in F[x]$, then the **greatest common divisor** of f, g is

$$\gcd(f, g) = d \in F[x]$$

where $(f, g) = (d)$ and d is monic.

Similarly to $\mathbb{Z}$

1. $d \mid f$
2. $d \mid g$
3. $\exists p, q \in F[x]$ such that $fp + gq = d$.

Moreover, $\gcd(f, g) = 1 \Leftrightarrow \exists p, q \in F[x]$ with $fp + gq = 1$.

23 Quotient Rings

If $I \subseteq R$ is an ideal, then $(I, +) \trianglelefteq (R, +)$ is a normal subgroup, since $(R, +)$ is Abelian.

We can get quotient group R/I, where the cosets of I are $a+I$, **written additively**, so as not to confuse $+$ and $\times$.

For ease of notation, we write $\bar{a} = a+I$ so $R/I = \{\bar{a} \mid a \in R\}$, and we want to define a ring structure on R/I.

Addition is from the quotient group, $\bar{a} + \bar{b} = \overline{a+b}$.

For multiplication, we define the obivous thing: $\bar{a} \cdot \bar{b} = \overline{ab}$.

Is this well defined? In other words, if $\bar{a} = \bar{c}$ and $\bar{b} = \bar{d}$, then is $\overline{ab} = \overline{cd}$?

Check: If $\bar{a} = \bar{c}$, then $c \in a + I$. That means that $c = a + s$ for some $s \in I$. Similarly, if $\bar{b} = \bar{d}$, then $d \in b + I$, meaning that $d = b + s'$ for some $s' \in I$. So $cd = (a+s)(b+s') = ab+as'+bs+ss'$, but of course, this is means that $cd \in ab+I$, and in fact $\overline{cd} = \overline{ab}$.

So in fact, this natural choice for multiplication is actually well defined! Now, we need to check our ring axioms.

- $(R/I, +)$ is an Abelian group, since it's the quotient of an Abelian group
- Multiplication on R/I is associative, as

$$(\bar{a}\bar{b})\bar{c} = \overline{ab} \cdot \bar{c} = \overline{(ab)c} = \overline{a(bc)} = \bar{a} \cdot \overline{bd} = \bar{a}(\bar{b}\bar{c})$$

- Multiplication is commutative as

$$\bar{a} \cdot \bar{b} = \overline{ab} = \overline{ba} = \bar{b} \cdot \bar{a}$$

- Multiplicative Identity $\bar{1}$, as $\bar{1} \cdot \bar{a} = \overline{1 \cdot a} = \bar{a}$.
- Distributivity, as above, because it's true in R.

So R/I is a ring!

Remark: When we defined quotient groups, we defined this map $\pi : R \to R/I$ that takes $a \mapsto \bar{a}$. We have a similar map here, but this time, it's a surjective ring homomorphism, and $\ker(\pi) = I$.

Similar to groups, we have the **First Isomorphism Theorem**: If $\varphi : R \to R'$ is a ring homomorphism, and $I = \ker(\varphi)$, then $R/I \cong \text{Im}(\varphi)$.

Wed. 27 Mar 2024

Today we are covering Quotient Rings!

This is probably the hardest Ring day, because a lot of calculations and work is required for even small examples.

Let's remind ourselves of the First Isomorphism Theorem.

$\varphi : R \to R'$ is a ring hom, then $R/\ker(\varphi) \cong \text{Im}(\varphi)$

Example.

If we take any ring R, and the identity map $\varphi : R \to R$, then $\ker(\varphi) = (0), \text{Im}(\varphi) = R$, then $R/(0) \cong R$

Example.

Here, let's look at the unique ring hom $\varphi : \mathbb{Z} \to \mathbb{Z}_n$ where $k \mapsto \bar{k}$. Now of course φ is surjective, and moreover

$$\ker(\varphi) = \{k \in \mathbb{Z} \mid k \equiv 0 \pmod{n} \} = n\mathbb{Z}$$

Which is an ideal, as we know. So

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$$

Since we use this a lot, we also write the notation $\mathbb{Z}/n$ for $\mathbb{Z}/n\mathbb{Z}$, (even if of course, we know that we can't mod out by a number, only by an ideal.) **QUESTION** Why can we only mod out by ideals?

Example.

Consider the evaluation map $\varphi_i : \mathbb{Z}[x] \to \mathbb{C}$ defined as $f(x) \mapsto f(i)$. It plugs in x as i. This is a ring homomorphism, and in fact

$$\text{Im}(\varphi_i) = \mathbb{Z}[i]$$

You should try to convince yourself that this is true!

What is $\ker(\varphi_i)$ **?**

Well, we know that

$$\begin{aligned}
\ker(\varphi_i) &= \{f \in \mathbb{Z}[x] : f(i) = 0\} \\
&= \{f \in \mathbb{Z}[x] \subseteq \mathbb{C}[x] : f(i) = 0\} && \text{Let's think of them as complex polynomials} \\
&= \{f \in \mathbb{Z}[x] \subseteq \mathbb{C}[x] : (x-i) \mid f\} && \text{Since } f(i) = 0
\end{aligned}$$

However, this is not $(x-i)$, because it's not an ideal of $\mathbb{Z}[x]$. If we did this in $\mathbb{C}[x]$, then it would be, but because we're only working with integers, we're somewhat restricted to what our polynomials could be.

If $(x-i) \mid f$, then $f(x) = (x-i)g(x)$, for some $g \in \mathbb{C}[x]$. But then, we can take complex conjugates

$$\overline{f(x)} = \overline{(x-i)} \cdot \overline{g(x)}$$

Now, x is a variable, not a complex number, so we will ignore the conjugation on x. Also notice that f has *real* coefficients. So in fact $\overline{f(x)} = f(x)$, so we have that $f(x) = \overline{(x-i)} \cdot \overline{g(x)}$ and so $x + i \mid f$.

As a sidenote, we know when working with polynomials that complex roots come in pairs. This is how it's proven!

What we get from this is that $x - i$ and $x + i$ are factors, and so $(x-i)(x+i) \mid f$ so $x^2 + 1 \mid f$.

So $\ker(\varphi) \subseteq (x^2+1)$, but if $g \in (x^2+1)$, then $g(x) = (x^2+1)h(x)$, which means that $g(i) = 0$ so $g \in \ker(\varphi)$, which means that $\ker(\varphi_i) = (x^2+1)$.

So the First Isomorphism Theorem tells us that $\mathbb{Z}[x]/(x^2+1) \cong \mathbb{Z}[i]$

One more easier example before we get to the hard stuff.

| **Example**.

Consider another evaluation map $\varphi_r : R[x] \to R$ for which $f(x) \mapsto f(r)$, with $r \in R$. Then, $\text{Im}(\varphi_r) = R$, since $\varphi(f(x) = a) = a$ for all $a \in R$. In other words, we can get any element of the ring just by evaluating the polynomial of that constant.

The question now is

What is $\ker(\varphi_r)$ **?**

Well, once again

$$\begin{aligned}\ker(\varphi_r) &= \{f \in R[x] : f(r) = 0\} \\ &= \{f \in R[x] : (x - r) \mid f\} \\ &= (x - r)\end{aligned}$$

Which tells us that $R[x]/(x - r) \cong R$. We'll use this quite a lot!

Note.

If $\varphi : R \to R'$ is an isomorphism, and $\varphi(a) = b$, then

$$R/(a) \cong R'/(b)$$

And we can write down the explicit map! This shouldn't be that weird. An isomorphism is just a renaming of elements.

Okay! Now the hard stuff!

Example.

Identify $\mathbb{Z}[i]/(i - 2)$. We want to quotient by all multiples of $i - 2$. Here, when we say "identify", we really mean "determine a simpler ring which is isomorphic to this quotient ring."

It's hard to work with $\mathbb{Z}[i]$, and it's easier to work with $\mathbb{Z}[x]$. Remember, we have an isomorphism $\varphi : \mathbb{Z}[x]/(x^2 + 1) \to \mathbb{Z}[i]$. (The examples we've done up to this point were very intentional, as they are very useful.) And, $\varphi(\overline{x - 2}) = i - 2$. And of course,

$$\mathbb{Z}[i]/(i-2) \cong \frac{(\mathbb{Z}[x]/(x^2+1))}{(\overline{x-2})}$$

So we have a map ψ defined as

$$\mathbb{Z}[x] \xrightarrow{\pi_1} \mathbb{Z}[x]/(x^2+1) \xrightarrow{\pi_2} \frac{\mathbb{Z}[x]/(x^2+1)}{(\overline{x-2})}$$

Now we know that ψ is surjective since π_1 and π_2 are both surjective. But again, we ask the age-old question

What's the $\ker(\psi)$ **?**

Well,

$$\begin{aligned}\ker(\psi) &= \{f \in \mathbb{Z}[x] \mid \pi_1(f) = \bar{0} \text{ or } \pi_2(\pi_1(f)) = \bar{0}\} \\ &= \{f \in \mathbb{Z}[x] \mid \underbrace{f \in (x^2+1)}_{\text{redundant}} \text{ or } \pi_1(f) \in (\underbrace{\overline{x-2}}_{\bar{g}\cdot(\overline{x-2})})\}\end{aligned}$$

But at this point, remember what $(\overline{x-2})$ is

$$(\overline{x-2}) = g \cdot \underbrace{(x-2)}_{\in \mathbb{Z}[x]} + \underbrace{(x^2-2)}_{\text{The ideal}}$$

So $(\overline{x-2})$ is a coset! It's a coset of $x-2$, plus the ideal (x^2+1). But now, we're looking at the ideal generated by this coset, which means *all multiples of that coset*, hence g times $x-2$.

But what's in that set? Well

$$\begin{aligned}\ker(\psi) &= \{f \in \mathbb{Z}[x] \mid f \in (x^2+1) \text{ or } \pi_1(f) \in (\overline{x-2})\} \\ &= \{f \in \mathbb{Z}[x] \mid f = f \cdot (x-2) + h(x^2+1)\} \\ &= (x-2, x^2+1)\end{aligned}$$

Moral of the story:

$$\frac{R/(a)}{(\bar{b})} \cong R/(a,b) \cong \frac{R/(b)}{(\bar{a})}$$

We can reverse the order!!! Applying this to our example from earlier, we have that

$$\frac{\mathbb{Z}[x]/(x^2+1)}{(\overline{x-2})} \cong \mathbb{Z}[x]/(x^2+1, x-2) \cong \frac{\mathbb{Z}[x]/(x-2)}{(\overline{x^2+1})}$$

But we saw ealier that $\mathbb{Z}[x]/(x-2) \cong \mathbb{Z}$, with $\overline{f(x)} \mapsto f(2)$. This is the "evaluate at 2" map. This means that

$$(\mathbb{Z}[x]/(x-2))/(\overline{x^2+1}) \cong \mathbb{Z}/((2)^2+1) \cong \mathbb{Z}/(5) \cong \mathbb{Z}_5$$

Example.

Identify

$$\underbrace{\mathbb{Z}[x]}_{R}/\overbrace{(x^2-3, 2x+4)}^{I}$$

Our goal here is to understand (and simplify) I. In other words, find a simpler set of generators for I.

First, we can look at I and try to cancel our some higher powers to come up with something simpler.

Note that

$$\begin{aligned} (2)(x^2-3) + (2-x)(2x+4) &\in I \\ = 2x^2 - 6 + 4x + 8 - 2x^2 - 4x = 2 &\in I \end{aligned}$$

So now

Claim: $I = (x^2 - 3, 2)$

Proof 1: $I = (x^2 - 3, 2x + 4) = (x^2 - 3, 2x + 4, 2)$ doesn't change anything. But now, since $2x + 4$ is a multiple of 2, we can remove it since it's redundant, and so $I = (x^2 - 3, 2)$

Proof 2: Set inclusion both ways. Omitted.

So our quotient ring $R/I \cong \mathbb{Z}[x]/(2, x^2 - 3)$. At this point, we can use our trick from earlier

$$\begin{aligned} & R/I \\ \cong & \mathbb{Z}[x]/(2, x^2 - 3) \\ \cong & (\mathbb{Z}[x]/(2))/(\overline{x^2 - 3}) \\ \cong & \mathbb{Z}_2[x]/(x^2 - \bar{3}) \\ \cong & \mathbb{Z}_2[x]/(x^2 + \bar{1}) \qquad \text{Since in } \mathbb{Z}_2,\ \overline{-3} = \bar{1} \end{aligned}$$

For this particular example, we can't go any further. However we can spend *some* time to understand what our elements look like.

Elements of R/I are $\bar{f}$, for $f \in \mathbb{Z}_2[x]$. Say that

$$f = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \in \mathbb{Z}_2[x]$$

So $a_i \in \{\bar{0}, \bar{1}\}$. Now, in R/I, $\overline{x^2 + \bar{1}} = \bar{\bar{0}}$. Since we're quotienting by $(x^2 + \bar{1})$. What this tells us is that $x^2 = \overline{\overline{-1}} = \bar{\bar{1}}$.

What this all means is that

$$\bar{f} = \bar{a}_0 + \bar{a}_1 x + \cdots + \bar{a}_n \{\bar{x}/\bar{1}\}$$

$$\begin{aligned}\bar{f} &= \bar{a}_0 + \bar{a}_1 x + \cdots + \bar{a}_n \{\bar{x}/\bar{1}\} \\ &= \left(\sum_{i \text{ even}} \bar{a}_i\right) + \left(\sum_{i \text{ odd}} \bar{a}_i\right) x\end{aligned}$$

Since we're working mod 2. So

$$R/I = \{\bar{\bar{0}}, \bar{\bar{1}}, \bar{x}, \overline{x+\bar{1}}\}$$

Now this group structure is not $\mathbb{Z}_4$, it's $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Fri. 29 Mar 2024

We'll push back product rings for a while and get back to them later.

Suppose we have $\mathbb{Z}$ and we want to "add" a multiplicative inverse to $2 \in \mathbb{Z}$. We're going to *force* this. We'll add a new element called x

$$\mathbb{Z} \to \mathbb{Z}[x]$$

But x doesn't yet do what we need to do. If x is a multiplicative inverse to 2, it must satisfy $2x = 1$, or $2x - 1 = 0$.

The way that we do that is by making all multiples of $2x - 1$ be zero. So in fact we can quotient out by $2x - 1$. Let $R = \mathbb{Z}[x]/(2x-1)$. Let $\alpha = \bar{x}$. Then $\bar{2}\alpha - \bar{1} = \bar{0}$. Why? Because α is the coset corresponding to $2x - 1$, which is the zero coset, since we mod out by it. So $2x - 1$ is a multiplicative inverse of $\bar{2}$.

In general, if R is a ring, and α is the solution to

$$f(x) = a_n x^n + \cdots + a_0 = 0$$

where $f(x) \in R[x]$. We call $R' = R[x]/(f)$ is called a **ring extension** of R, by adjoining $\alpha = \bar{x}$ to R. We write $R' = R[\alpha]$.

Also, we could require α to satisfy a system of polynomial equations

$$\alpha \models \begin{cases} f_1(x) = 0 \\ \vdots \\ f_n(x) = 0 \end{cases}$$

And get $R[\alpha] = R[x]/(f_1, \ldots, f_n)$.

We already saw that $\mathbb{Z}[i] \cong Z[x]/(x^2+1)$, and we can now interpret this differently. We're adding a new element which is $\sqrt{-1}$.

If $f \in \mathbb{Z}[x]$ is monic, $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ and $R[\alpha] = R[x]/(f)$, where $\alpha = \bar{x}$, then

- $R[\alpha]$ has a **basis** $\{1, \alpha, \ldots, \alpha^{n-1}\}$

  In other words, we can write every element as

  $$\bar{a}_0 \cdot 1 + \bar{a}_1 \cdot \alpha + \cdots + \bar{a}_{n-1}\alpha^{n-1}$$

  for $\bar{a}_0, \ldots, \bar{a}_{n-1} \in R$. This is nothing new, we saw this even when we introduced $\mathbb{Z}[i]$.

  Since

  $$\alpha^n + \bar{a}_{n-1}\alpha^{n-1} + \cdots + \bar{a}_0 = \bar{0}$$

  We can actually write $\alpha^n = -\bar{a}_{n-1}\alpha^{n-1} - \cdots - \bar{a}_0$, and in fact, $\alpha^{n+m} = \alpha^m\alpha^n = \alpha^m(\cdots)$

- If $\beta, \beta' \in R[\alpha]$, what's $\beta\beta'$?

  Let $\beta = g(x)$, $\beta' = g'(\alpha)$ for some $g, g' \in R[x]$. Then, $gg' = fq + r$, where $\deg r < \deg f$ or $r = 0$. Then

  $$\begin{aligned} \overline{gg'} &= \overline{fq} + \bar{r} \\ g(\alpha)g'(\alpha) &= f(\alpha)q(\alpha) + r(\alpha) \\ \beta\beta' &= r(\alpha) \end{aligned}$$

Let's look at an

Example.

Let's investigate $\mathbb{Z}_5[\sqrt{\bar{3}}]$. This is $\mathbb{Z}_5[x]/(x^2 - \bar{3})$.

Claim: This is a field with 25 elements.

Proof: $x^2 - 3$ is monic, so $\mathbb{Z}_5[\sqrt{\bar{3}}]$ has a basis $\{1, \alpha\}$ where $\alpha = \bar{x}$. We'll write $\sqrt{\bar{3}} = \alpha$. So $\mathbb{Z}_5[\sqrt{3}] = \{A + B\sqrt{3} \mid A, B \in \mathbb{Z}_5\}$. We have 5 choices for A, 5 choices for B, which gives us 25 total choices!

Now $A + 0\sqrt{\bar{3}}$ is a unit for $A = \bar{0}$, since $\mathbb{Z}_5$ is a field. If $B \neq \bar{0}$, then $(A + B\sqrt{3})(A - B\sqrt{3}) = A^2 - \bar{3}B^2$. If $A^2 - \bar{3}B^2 \neq 0$, then it's invertible, so

$$(A + B\sqrt{\bar{3}}) \underbrace{(A - B\sqrt{\bar{3}})(A^2 - \bar{3}B^2)^{-1}}_{=(A+B\sqrt{\bar{3}})^{-1}} = \bar{1}$$

If $A^2 - \bar{3}B^2 = \bar{0}$, then $\bar{3} = A^2(B^{-1})^2 = (AB^{-1})^2$ so $\bar{3}$ has a square root in $\mathbb{Z}_5$, but of course it doesn't. So $A^2 - \bar{3}B^2 \neq \bar{0}$ and $A + B\sqrt{\bar{3}}$ is a unit.

Hence $\mathbb{Z}_5[\sqrt{\bar{3}}]$ is a field.

Let's try the following

Example.

Let $\mathbb{Z}[\alpha]$ where $2\alpha - 1 = 0$ and $3\alpha - 1 = 0$. So we have

$$\mathbb{Z}[\alpha] = \mathbb{Z}[x]/\underbrace{(2x - 1, 3x - 1)}_{I}$$

So

$$\begin{aligned} (3x - 1) - (2x - 1) = x \in I \\ 2(x) - 2(x - 1) = 1 \in I \\ \Rightarrow I = \mathbb{Z}[x] \end{aligned}$$

So in fact $\mathbb{Z}[\alpha] = \mathbb{Z}[x]/\mathbb{Z}[x] = \{\bar{0}\}$

Exercise: See what happens when you try to add restrictions to 2 and 4.

23.1 Fractions

Given a ring R, a **fraction** is a/b, for $a, b \in R$ and $b \neq 0$.

Consider $a/1$ as a.

- $a/b = a'/b' \Leftrightarrow ab' = a'b$
- $a/b + c/d = \frac{ad+bc}{bd}$, $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$

But at this point, we have a problem. What if $b, d \neq 0$, but $bd = 0$? This might happen in $\mathbb{Z}_4$ if $b = 1/2$ and $d = 1/2$.

Definition.

A **zero divisor** in R is an element $a \in R$ with $a \neq 0$ and $ab = 0$ for some $b \in R$.

Definition.

An **integral domain** (also called a domain) is a ring with no zero divisors.

Of course we know that $ab = 0 \Rightarrow a = 0$ or $b = 0$

Integral Domains (often abbreviated I.D.) have a *cancellation law*. If $ab = ac, a \neq 0$, then $b = c$. Since

$$\begin{aligned} ab &= ac \\ \Rightarrow a(b-c) &= 0 \\ \Rightarrow b - c &= 0 \end{aligned}$$

Since $a \neq 0$.

Theorem: If R is an integral domain, and F is the set of equivalence classes of fractions in R. Then F is a field called the field of fractions of R.

Proof: Omitted.

Instead, let's look at some examples.

Example.

If R is an integral domain, then $R[x]$ is an integral domain.

If $f, g \in R[x]$, then $\deg(fg) = \deg(f) + \deg(g)$. If you're not convinced of this just multiply two polynomials and see for yourself.

What we gather from this is that multiplying polynomials only makes your degree larger (or keeps it as is.)

But now we can take the **field of rational functions** over R is $R(x)$, the fraction field of $R[x]$. It is defined as

$$R(x) = \left\{ \frac{f}{g} \mid f, g \in R[x], g \neq 0 \right\} / \approx$$

QUESTION what's this $/\approx$ business??

Similarly, $R(\alpha)$ is the field of fractions of $R[\alpha]$, if it's an I.D. In particular, subrings of integral domains are also integral domains. So $\mathbb{Q}[\alpha]$ for $\alpha \in \mathbb{C}$ is also an I.D., and $\mathbb{Q}(\alpha)$ is its field of fractions.

Mon. 1 Apr 2024

Let's remember what we have done so far.

Recall:

- A Field is a ring in which all non-zero elements are *units*.
- An **Integral Domain** is a ring with no zero divisors.

  In particular, $ab = 0$ implies that $a = 0$ or $b = 0$. (Unlike for example in $\mathbb{Z}_4$ where $(\bar{2})(\bar{2}) = \bar{0}$)

  As an

  Example.

  - $\mathbb{Z}_p$ is an integral domain (and also a field) when p is prime.
  - $\mathbb{Z}$ is an integral domain (but *not* a field)

– $\mathbb{Z}_n$ is not an integral domain for n composite.

As if $n = ab$, then $\bar{a} \cdot \bar{b} = \bar{n} = \bar{0} \in \mathbb{Z}_n$

A natural question might be:

Question: If R is any ring, and $I \subseteq R$ is an ideal, under what condition is R/I an integral domain or a field?

Recall: A ring is a field **if and only if** the only proper ideal is (0).

Definition.

An ideal $I \subseteq R$ is a **maximal ideal** if $I \neq R$ and if $I \subseteq J \subseteq R$, then either $J = I$ or $J = R$.

Let's first look at a non-example.

$I = (x) \subseteq \mathbb{Z}[x]$ is not maximal. This is because $(x) \subsetneq (2, x) \subsetneq \mathbb{Z}[x]$.

1. The first non-equality is because $2 \in (2, x)$, but $2 \notin (x)$.
2. The second is because $1 \in Z[x]$ but $1 \notin (2, x)$.

Exercise: $(2, x)$ is a maximal ideal. Think about why

Now, a real

Example.

$I = (x) \subseteq \mathbb{Q}[x]$ is maximal

Why? Well if $(x) \subseteq J \subseteq \mathbb{Q}[x]$, then J is an ideal in $\mathbb{Q}[x]$, and since $\mathbb{Q}$ is a field, $J = (f)$ for some $f \in \mathbb{Q}[x]$.

Since $x \in (x) \subseteq J$, so $x \in (f)$ which means that there exists some $g \in \mathbb{Q}[x]$ such that $x = fg$.

Looking at the degrees, either ($\deg(f) = 1$ and $\deg(g) = 0$), or ($\deg(f) = 0$ and $\deg(g) = 1$.)

If $\deg(f) = 0$, then f is a non-zero constant, which means it's a unit. Then $J = (f) = \mathbb{Q}[x]$.

If $\deg(f) = 1$, then $f = ax + b$ and $g = c$ for $a, b, c \in \mathbb{Q}$. This means that $x = 1 \cdot x + 0 = fg = acx + bc$, meaning $ac = 1$ and $bc = 0$. From this, we know

$b = 0$, and $ac = 1$, which means

$$f = ax \in (x) \Rightarrow (f) \subseteq (x)$$

So $J = (x)$ or $J = \mathbb{Q}[x]$ hence (x) is a maximal ideal.

Theorem.

R/I is a field **if and only if** I is a maximal ideal.

Proof. Consider $\pi : R \to R/I$ for which $a \mapsto \bar{a}$. We already know that R/I is a field if and only if its only proper ideal is $(\bar{0})$.

Claim. If $J \subseteq R/I$ is an ideal, then $\pi^{-1}(J) = \{s \in R \mid \pi(s) \in J\}$ is an ideal of R that contains $\ker(\pi) = I$.

Proof: Exercise!

So if $J \subseteq R/I$ is an ideal, then $\pi^{-1}(J)$ is an ideal and $I \subseteq \pi^{-1}(J) \subseteq R$ and in fact, π is surjective, so $\pi(\pi^{-1}(J)) = J$.

$\Leftarrow$. If I is maximal, then $\pi^{-1}(J)$ is either I or R. If $\pi^{-1}(J) = I$, then $J = \pi(\pi^{-1}(J)) = (\bar{0})$ as $I = \ker(\pi)$. If $\pi^{-1}(J) = R$, then $J = \pi(\pi^{-1}(J)) = R/I$. So R/I has only one proper ideal, $(\bar{0})$, so is a field.

$\Rightarrow$. If R/I is a field, then consider $I \subsetneq J \subseteq R$. Then $\pi(J) \neq (\bar{0})$

Exercise: Show that $\pi(J)$ is an ideal of R/I. (Use surjectivity of π.)

Since R/I is a field, $\pi(J) \neq (\bar{0})$ so $\pi(J) = R/I$, so $J = \pi^{-1}(\pi(J)) = R$, so I is a maximal ideal.

(One key idea here is to use the fact that fields only have two ideals.)

Example.

$(0) \subseteq F$ is a maximal ideal when F is a field.

Example.

$(2, x) \subseteq \mathbb{Z}[x]$ is maximal, as

$$\mathbb{Z}[x]/(2, x) \cong (\mathbb{Z}[x]/(x))/(\bar{2}) \cong \mathbb{Z}/(2) = \mathbb{Z}_2$$

Hence $(n, x) \subseteq \mathbb{Z}[x]$ is maximal *if and only if* n is prime, as $\mathbb{Z}[x]/(n, x) \cong \mathbb{Z}_n$, and we know when that's a field.

Definition.

An ideal is called a **prime ideal** if

$$ab \in I \Rightarrow a \in I \text{ or } b \in I$$

If you're wondering what the relation to prime numbers is, think that: if $p|ab$, then $p|a$ or $p|b$. The parallel here is that, if $ab \in (p)$, then $a \in (p)$ or $b \in (p)$.

Theorem.

R/I is an integral domain **if and only if** I is a proper prime ideal in R.

Proof.

$\Leftarrow$. If $I \subsetneq R$ is a prime ideal, consider $\bar{a}, \bar{b} \in R/I$ such that $\bar{a} \cdot \bar{b} = \bar{0}$. This tells us that $\overline{ab} = \bar{0}$, which means $ab \in I$. Now, I is prime, so either $a \in I$, or $b \in I$, which means either $\bar{a} = \bar{0}$, or $\bar{b} = \bar{0}$, so R/I is an integral domain.

$\Rightarrow$. If R/I is an integral domain, then consider $a, b \in R$ such that $ab \in I$. Then $\overline{ab} = \bar{0}$, which means that $\bar{a} \cdot \bar{b} = \bar{0}$, so either $a \in I$ or $b \in I$.

A natural follow up question to ask might be

When is a principal ideal maximal or prime?

Definition.

- An element $p \in R$ is **prime** if
  1. p is not a unit or 0, **and**
  2. If $p|ab$, then $p|a$ or $p|b$.
- An element $a \in R$ is **irreducible** if
  1. a is not a unit or 0, **and**
  2. If $a = bc$, then one of b or c is a unit.

     In other words, there's no "non-trivial" factorization of a.

Next time, we'll see how this relates to our ideals!

Wed. 3 Apr 2024

Note.

- Homework due tomorrow
- Exam next Friday
- Review next Wednesday

Recall:

- $I \subseteq I$ is **maximal** if $I \subseteq J \subseteq R$ and $I \neq R$, then $I = J$, or $J = R$.
- $I \subseteq R$ is **prime** if $I \neq R$, $ab \in I$ implies that $a \in I$ or $b \in I$.
- $p \in R$ is **prime** if $p \neq 0$ or a unit, and $p|ab$ implies that $a|b$ or $p|b$.
- $a \in R$ is **irreducible** if $a \neq 0$ or a unit, and $a = bc$ implies b is a unit or c is unit.

Question: When are principal ideals prime or maximal?

Proposition: If R is a ring, and I is an ideal generated by some element a, and $a \neq 0$, or a unit, then I is a prime ideal if and only if a is prime element.

Note.

Prime principal ideals correspond to prime elements!

Proof.

$\Rightarrow$. Consider $b, c \in R$ such that $a|bc$, this tells us that $bc \in (a)$. Now, if (a) is prime, then $b \in (a)$ or $c \in (a)$ (i.e.) $a|b$ or $a|c$. Hence a is a prime element of R.

$\Leftarrow$. Consider two elements of R b and c, for which $bc \in (a)$. This tells us that $a|bc$. Now, a being a prime element tells us that $a|b$ or $a|c$, so either $b \in (a)$ or $c \in (a)$, and so we have a prime ideal.

Note.

Some prime ideals are not principal ideals, hence don't correspond to a prime element.

Proposition: If R is an integral domain, and we have a principal ideal $I = (a)$ with $a \neq 0$, or a unit. Then if I is maximal, a is irreducible.

Warning: The converse is **false**!

Why Integral Domain: In $\mathbb{Z}_{10}$, the ideal $(\bar{2})$ is maximal.

$$(\bar{2}) = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}\}$$

I can't make this any larger without making it the whole group. So here, the only non-unit missing is $\bar{5}$, but if we add $\bar{5}$, we get $\bar{5} - \bar{4} = \bar{1}$, so we get all of $\mathbb{Z}_{10}$.

Against the Converse: In $\mathbb{Z}[x]$, 2 is irreducible, but (2) is not maximal, as we have

$$(2) \subseteq (2, x) \subseteq \mathbb{Z}[x]$$

Which we talked about last time. So the only thing stopping us from going backwards is that we have non-principal ideals. If all our ideals were principal, then the statement would be an if and only if.

Proof. If $I = (a)$ is maximal, let $a = bc$ for some $b, c \in R$, and assume that b is not a unit. We want to show that c is a unit. So, a is a multiple of b, which means that $a \in (b)$, and hence all multiples of a are also multiples of b and so

$$(a) \subseteq (b) \subseteq (R)$$

But we assumed that (a) is maximal, which means that $(a) = (b)$ or $(b) = R$. But we assumed that b was not a unit, so the ideal generated cannot be the entire ring and so $(b) \neq R$. This tells us that $(a) = (b)$. Hence $b \in (a)$ and $b = ad$, for some $d \in R$.

So $a = bc = adc$. Because we are in an integral domain, we have a cancellation law, so we may write $a \cdot 1 = a \cdot dc$ which means that $1 = dc$. But this tells us that c is a unit with inverse d.

Exercise: If all ideals in R are principal, then the converse is true.

Example.

In $F[x]$, all ideals are principal, and $F[x]$ is an integral domain, so (f) is maximal whenever f is irreducible, which means that

$$F[x]/(f) \text{ is a field}$$

Question: How do we find irreducible and prime elements?

Example.

Consider the ring $R = \mathbb{Z}[\sqrt{-5}]$, we know that

$$\mathbb{Z}[\sqrt{-5}] \cong \mathbb{Z}[x]/(x^2+5) = \{A + B\sqrt{-5} \mid A, B \in \mathbb{Z}\}$$

What we know is that R is an integral domain, since $R \subseteq \mathbb{C}$ (remember that any subring of an integral domain is also an integral domain.)

So $(x^2+5) \subseteq \mathbb{Z}[x]$, and it must be a prime ideal, because we quotiented by this ideal and got an integral domain. So we know that $x^2+5 \in \mathbb{Z}[x]$ is a prime element.

This is our first example of an non-trivial prime element

Claim: $6 \in R$ is **not** irreducible. Why? Well

$$6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$$

and $2, 3, 1 \pm \sqrt{-5}$ are irreducible and not units.

How do we know? We need to know what the units are in R. We have a tool for this.

The tool: Modulus Squared

$$|x+iy|^2 = (\sqrt{x^2+y^2})^2 = x^2+y^2$$

This is very useful when $|a|^2 \in \mathbb{Z}$ for all $a \in R \subseteq \mathbb{C}$. In our case, $|A + B\sqrt{-5}|^2 = A^2 + 5B^2 \in \mathbb{Z}$ since $A, B \in \mathbb{Z}$.

This is useful as it transfers equations from R to $\mathbb{Z}$, which we know how to work with! Especially products, since $|ab|^2 = |a|^2|b|^2$.

Units in R: If $a \in R$ is a unit, then there exists a $b \in R$ such that $ab = 1$, which means that $|ab|^2 = |1|^2 = 1$, which further means that $|a|^2|b|^2 = 1$. Now, a and b are positive integers, so $|a|^2 = 1$.

Conversely, if $|a|^2 = 1$, then $|a|^2 = a \cdot \bar{a} = 1$. If $a = A + B\sqrt{-5}$, then $\bar{a} = A - B\sqrt{-5} \in R$, so a is a unit.

> **Note**.
>
> So understanding units in this ring is equivalent to understanding elements that have norm 1.

If $a = A + B\sqrt{-5}$, and $|a|^2 = A^2 + 5B^2 = 1$. Now, if $B \neq 0$, then we can't get 1, so B must be zero, and $A = \pm 1$. So the only units in R are ± 1.

Proof that 2 **is irreducible**. If $2 = ab$ for some $a, b \in R$, then

$$|2|^2 = |a|^2|b|^2 = 4$$

If a and b are not units, then it must be the case that $|a|^2 = |b|^2 = 2$. But is it possible?

Well if $a = A + B\sqrt{-5}$, and $|a|^2 = A^2 + 5B^2 = 2$, but there are no integer solutions to this system and $|a|^2 \neq 2 \neq |b|^2$. So $|a|^2 = 1$ and $|b|^2 = 4$, or vice versa. Hence, either a or b is a unit and 2 is irreducible.

3 **is a unit**. The reason is similar.

$1 \pm \sqrt{-5}$: Similar again.

$$|1 \pm \sqrt{-5}|^2 = 6 = \begin{cases} 1 \cdot 6 \\ 6 \cdot 1 \\ 2 \cdot 3 \\ 3 \cdot 2 \end{cases}$$

But $|a|^2 \neq 2$ or 3, so again, similar to the above.

Claim: $2, 3, 1 \pm \sqrt{-5}$ are not prime in R.

Proof. $2|6 = (1+\sqrt{-5})(1-\sqrt{-5})$, but $2 \nmid 1 \pm \sqrt{-5}$. Why? Well if $2a = 1 \pm \sqrt{-5}$, then $|2a|^2 = |1 \pm \sqrt{-5}|^2 = 6$ and furthermore $4|a|^2 = 6$ with $a \in \mathbb{Z}$, which is a contradiction.

Similarly, $3 + 1 \pm \sqrt{-5}$, but $3|(1\sqrt{-5})(1 - \sqrt{-5}) = 6$, similarly for $1 \pm \sqrt{-5}|6$.

Fri. 5 Apr 2024

Note.

Exam is next Friday. Everything since Exam 2 until today and part of Monday is fair game. That includes

- Group Actions (mostly this)
- Orbit Stabilizer (and this)
- Class Equation (with the conjugation action)
- Cayley's Theorem (know what it is)
- Sylow Theorem
- **not presentation, nor free groups**
- rings, homs, isoms, ideals, quotient rings, adjoining elements, fractions, prime/maximal ideals, primes/irreducibles, Euclidean Domains, PIDs.

Format of the Exam

- One page of short answer
- One page of true/false
- Two long questions (one on group theory, one on ring theory)

Back to primes and irreducibles.

Remember: In $\mathbb{Z}[\sqrt{-5}]$ (which is an integral domain), we show that 2, 3, and $1 \pm \sqrt{-5}$ are irreducible but not prime. The way that we showed this was that, if you multiply 2, and 3, you get 6, all of which divide 6.

So irreducible does not imply prime. In general, prime does not imply irreducible. For

Example.

In $\mathbb{Z}_6$, $\bar{2}$ is prime. Why? Well, $\bar{2} \mid \bar{0}$, $\bar{2} \mid \bar{2}$, and $\bar{2} \mid \bar{4}$, and the only products in $\mathbb{Z}_6$ giving $\bar{0}, \bar{2}, \bar{4}$ involve a $\bar{0}, \bar{2}, \bar{4}$. So $\bar{2}$ divides one of the factors.

But $\bar{2}$ is not irreducible, since $\bar{2} = \bar{2} \cdot \bar{4}$, and neither $\bar{2}$ nor $\bar{4}$ is a unit.

Theorem.

In an integral domain, primality implies irreducibility.

Proof. Suppose that R is an I.D. and $p \in R$ is prime. Let $p = ab$, then $p \mid ab$. Since p is prime, it must divide a or b, suppose it's a. This means that $a = px$ for some $x \in R$, and $p = ab = pxb$.

Since R is an integral domain, we have the cancellation law, so $p = pxb$ implies that $1 = xb$, and hence b is a unit. So p is irreducible.

23.2 Division Algorithm

Definition.

Given a ring R, a **size function** is any function $\sigma : R \setminus \{0\} \to \mathbb{N}_{\geq 0}$.

Note that there are no further requirements on this function.

Definition.

A **Euclidean Domain** is an integral domain R with a size function σ such that "the division algorithm works."

More concretely, for all $a, b \in R$, $b \neq 0$, these exists $q, r \in R$ such that

$$a = bq + r$$

and $r = 0$ or $\sigma(r) < \sigma(b)$. Now, q, r may not be unique. In other words, σ is a sort of "decider" of size. It defines what "size" means in the structure we're working in.

Example.

$R = \mathbb{Z}$, and $\sigma(n) = |n|$. Here, q, r are not necessarily unique (unless $r = 0$.)

For instance

$$3 = 2 \cdot 1 + 1 = 2 \cdot 2 + (-1)$$

Now, the way that we make it unique for the integers is by requiring that $r > 0$, and while this works for $\mathbb{Z}$, it may not work for other rings.

Example.

If F is a field, $R = F[x]$, and $\sigma(f) = \deg(f)$. And we've worked with this property before!

Example.

$R = \mathbb{Z}[i]$ with $\sigma(x + iy) = |x + iy|^2 + x^2 + y^2$.

The claim is that this is a Euclidean Domain.

Given $\alpha, \beta \in \mathbb{Z}[i]$, if $\beta \mid \alpha$, then $\alpha = \beta\gamma$ for some $\gamma \in \mathbb{Z}[i]$, so set $\alpha = \beta\gamma + \rho$.

If $\beta \nmid \alpha$, then we want γ and ρ such that $\alpha = \beta\gamma + \rho$ and $\sigma(\rho) < \sigma(\beta)$. i.e.

$$|\rho|^2 < |\beta|^2 \Leftrightarrow |\rho| < |\beta|$$

TODO I cannot draw this grid of βs.

It means that $\mathbb{C}$ is tiled by squares of side length β. We know that α is not a vertex of a square, since it's not divisible by β, so it must be inside some square.

Now, pick a nearest vertex to α and call it $\gamma\beta$ (note that it might not be unique!)

Let $\rho = \alpha - \gamma\beta$, so $\alpha = \gamma\beta + \rho$. Now calculate $|\rho|$.

So $\mathbb{Z}[i]$ is a Euclidean Domain with size function σ.

Note of course that we could have chosen another size function.

Let's look at another

Example.

Let $R = \mathbb{Z}[\sqrt{-5}]$ with $\sigma(x + y\sqrt{-5}) = |x + y\sqrt{-5}|^2 - x^2 + 5y^2$. This is **not** is a Euclidean domain.

This leaves the question open of "is there a different σ that works?"

This question is too hard to answer directly. Later, we will develop tools to analyze properties of Euclidean domains more carefully.

For contradiction, we assume that (R, σ) is a E.D. Let $a = 1 + \sqrt{-5}$ and $b = 2$. If $1 + \sqrt{-5} = 2q + r$ and we know that $r \neq 0$ as $2 \nmid 1 + \sqrt{-5}$. This tells us that $\sigma(r) < \sigma(2) = 4$. But we showed last time that $\sigma = 2, 3$ is impossible, so $\sigma(r) = 1$ and $r = \pm 1$ is a unit.

So we have that

$$1 + \sqrt{-5} = 2q \pm 1$$

Meaning that $2q$ is either $\sqrt{-5}$, or $2 + \sqrt{-5}$. If $2q = \sqrt{-5}$, then $|2q|^2 = |\sqrt{-5}|^2$ so $4|q|^2 = 5$, which is a contradiction, and similarly if $2q = 2 + \sqrt{-5}$, so no such q exists and (R, σ) cannot be a E.D.

Mon. 8 Apr 2024

Note.

Things today are not going to be on the exam.

You are expected to know what a Euclidean domain is though. You need to know what it is, how to define it, examples, etc...

Recall: A Euclidean Domain is a ring R and a size function $\sigma : R \setminus \{0\} \to \mathbb{N}_{\geq 0}$, and where, for all $a, b \in R$, with $b \neq 0$, these exists $q, r \in R$ with

$$a = bq + r$$

and $r = 0$, or $\sigma(r) < \sigma(b)$.

Definition.

A **Principle Ideal Domain** (P.I.D.) is an *integral domain* in which all ideals are principle (i.e. can be generated by only one element.)

Example.

Some examples of PIDs include:

- The integers $\mathbb{Z}$
- F a field.
- $F[x]$ where F is a field.

  We spent some time proving this.

Non-examples

These are **not** PIDs

- $\mathbb{Z}_n$ for n composite.

  Here, all ideals are principle, but it's not an integral domain.

- $\mathbb{Z}[x]$.

  This is an integral domain, but it has non principle ideals, for instance $(2, x)$, which can't be written in any simpler way.

On the other hand

Theorem.

A Euclidean Domain is a P.I.D.

Proof: The proof is the same as for $\mathbb{Z}$ and for $F[x]$. The idea is as follows:

1. Consider a non-zero ideal.
2. Pick the smallest element. Notice that "smallest" means something in a Euclidean Domain!

   In $\mathbb{Z}$, this was the smallest absolute value, and in $F[x]$ it was the smallest degree. In general, its the element a which yields the smallest $\sigma(a)$.

   There's always going to be something smaller of course, since σ outputs a natural number. Notice of course that there may be more than one choice for this.

3. Now we just show that this generates the entire ideal: $I = (a)$.

   Now of course $(s) \subseteq I$ is the easy direction, and $I \subseteq (s)$ is harder. For that direction, the idea is to go by contradiction, write the division algorithm, and

show that the remainder must be zero.

Theorem: In a PID, irreducibility implies primality.

Recall: In an I.D. prime implies irreducible, but not the converse. What we see now is that we *can* get the converse if we assume that all our ideal are principle.

A consequence of this is that, if all our ideals are principle, an irreducible element gives us a maximal ideal.

Corollary: $\mathbb{Z}[\sqrt{-5}]$ is not a E.D. with any size function σ. It's not even a PID.

Proof of Corollary: 2, 3, and $1 \pm \sqrt{-5}$ are irreducible but not prime, in $\mathbb{Z}[\sqrt{-5}]$. So by our theorem above, this is not a PID, so it's not a Euclidean Domain.

Proof of Theorem: Assume that R is a PID, and $a \in R$ is irreducible. Assume that $a \mid bc$, and $a \nmid b$. We now want to show that $a \mid c$.

Consider $I = (a, c) \subseteq R$. Since R is a PID, we know that I can be written as $I = (d)$ for some $d \in R$.

Since $a \in I$, a is a multiple of d, so $a = de$ for some $e \in R$. Keeping in mind that a is irreducible, consider the two possibilities

1. If d is not a unit, then e must be a unit (since a is irreducible)

   Since e is a unit, that means d can be written as a multiple of a

   $$d = ae^{-1}$$

   Which means that $d \in (a)$ and so $(d) \subseteq (a)$. Since $c \in (a, c) = (d) \subseteq (a)$, c is a multiple of a and so $a \mid c$.

2. If d is a unit, then $(a, c) = (d) = R$, since units generate the entire ring as an ideal. But this means that $1 \in (d)$, which means that there exist $x, y \in R$ with $ax + cy = 1$. Multiplying both sides by b, we have

   $$\begin{aligned} ax + cy &= 1 \\ a(bx) + (bc)y &= b \end{aligned}$$

We know that a is divisible by a, and that bc is divisible by a, by assumption, so b must also be divisible by a.

However this contradicts $a \nmid b$, which means that d is not a unit, and $a \mid c$. Hence a is prime.

–

Are all PIDs also EDs?

No!

Example.

Consider $R = \mathbb{Z}[\alpha]$, where $\alpha = \frac{1+\sqrt{-19}}{2}$. Where does α come from as a polynomial? Well

$$\begin{aligned}(2\alpha - 1)^2 &= -19 \\ \alpha^2 - \alpha + 5 &= 0\end{aligned}$$

Claim: R is a PID, but but a E.D.

Why is R not a ED?

Note that $|a + b\alpha|^2 \in \mathbb{Z}$. This is not obvious, so let's check it.

$$\begin{aligned}a + b\alpha &= a + b\left(\frac{1+\sqrt{-19}}{2}\right) \\ &= \left(a + \frac{b}{2}\right) + \frac{b}{2}\sqrt{-19}\end{aligned}$$

So

$$
\begin{aligned}
|a+b\alpha|^2 &= \left(a+\frac{b}{2}\right)^2 + 19\left(\frac{b}{2}\right)^2 \\
&= a^2 + ab + \frac{b^2}{4} + 19\frac{b^2}{4} \\
&= a^2 + ab + 5b^2 \in \mathbb{Z}
\end{aligned}
$$

Now, we check that $a \in R$ is a unit if and only if $a = \pm 1$, and $2, 3$ are irreducible.

(This is similar to what we did for $\mathbb{Z}[\sqrt{-5}]$) **TODO** know how this works and how to do this.

If (R, σ) is a E.D., chose $x \in R$ such that

- x is not a unit
- $\sigma(x) \leq \sigma(y)$ for $y \in R$, not a unit.

So x is a smallest, non-unit.

If $2 = xq + r$, then $r = 0$ or $\sigma(r) < \sigma(x)$, but that means r must be a unit. Moreover, $r = 0$ or $r = \pm 1$ because we know what our units are in $\mathbb{Z}$.

- If $r = 0$, then $x = \pm 2$, since $2 = xq$ and 2 is irreducible so $q = \pm 1$ is a unit
- If $r = 1$, then $1 = xq$, but this can't happen since x is not a unit.
- If $r = -1$, then we get $x = \pm 3$, since $3 = xq$, and 3 is irreducible, so $q = \pm 1$ is a unit.

Hence $x = \pm 2$ or $x = \pm 3$.

Now, write $\alpha = xq' + r'$. Similarly, $r' = 0$ or $r' = \pm 1$. So $xq' = \alpha$ or $\alpha + 1$, or $\alpha - 1$.

But $x = \pm 2$ or $x = \pm 3$, and we can check that 2, and 3 do not divide α or $\alpha \pm 1$.

You can check this using norm squared.

$$
|2|^2 = 4, |3|^2 = 9
$$

But

$$|\alpha|^2 = 5, |\alpha + 1|^2 = 7, |\alpha - 1|^2 = 5$$

So no solution for q' and r' and hence R is not a E.D.

Why is R a PID?

Let $I \subseteq R$ be a non-zero ideal. Chose $s \in I$ with $|s|^2$ minimal, and $s \neq 0$. We want to show that $I = (s)$. Note here that we cannot use the division algorithm, since of course, this is not an E.D. so this proof will be a little different from what we've seen thus far.

We know that $(s) \subseteq I$, since $s \in I$, but if $(s) \neq I$, then there is some $a \in I$ such that $a \subseteq (s)$, but since $a, s \in I$, we know that any linear combination $ap + sq \in I$ for $p, q \in R$. We want to find $p, q \in R$ such that

$$0 < |ap + sq|^2 < |s|^2$$

which would lead us to a contradiction. We're not going to prove this, as it's a massive mess, but just trust that it's true.

Hence $a \in (s)$, which means that $I = (s)$, and R is a PID.

What we gather from this, is the fundamental fact that

$$\{\text{EDs}\} \subsetneq \{\text{PIDs}\}$$