Math 122: Algebra I

Hahn Lheem (as Course Assistant)
Taught by Myrto Mavraki

Fall 2022

Contents

0 Preface

This class is from Fall 2022. Meeting times are Monday and Wednesday from 1:30-2:45pm. There is no designated textbook, but the recommended texts are Dummit and Foote's *Abstract Algebra*, 3rd ed. (Chapters 1-9 is a superset of what will be covered in this class) and Artin's *Algebra*. The first half of the course will be on groups, and the second half will focus on rings.

Problem sets will be assigned weekly and due every Wednesday. Office hours and section times can be found on Canvas. The midterm will be on October 24.

If you see anything wrong or unclear, please let me know at hahnlheem@college.harvard.edu!

1 08/31 - Introducing Groups

A natural place to start is to define what a group is. We start with defining a binary operation:

Definition 1.1 (Binary operation)**.** A **binary operation** $*$ on a set G is a function

$$\begin{aligned} * : G \times G &\to G \\ (a, b) &\mapsto a * b. \end{aligned}$$

Remark 1.2. Two remarks:

1. A binary operation *must always be with respect to a set.* It doesn't make sense to have a binary operation without a set on which it is defined. For instance, when I say multiplication, I mean different things in $\mathbb{Z}$ (the integers), in $\mathbb{Z}/p\mathbb{Z}$ (integers mod p), and in the set of $n \times n$ matrices.

2. We often call this binary operation $*$ as multiplication, and thus a lot of the notation we use with binary operations will be borrowed from our notation for multiplication, i.e. $ab := a * b$. In the beginning, though, it is good practice to not omit the $*$.

All the binary operations that we care about will satisfy **associativity**, that is $\forall\, a, b, c \in G$, $a*(b*c) = (a*b)*c$. Some binary operations are **commutative**, i.e. $\forall\, a, b \in G$, $a*b = b*a$, but this will not always be the case.

Example 1.3 (Binary operations)

This may seem abstract a priori but is a very familiar notion:

- $+$ is a binary operation in $\mathbb{Z}$. It is both associative and commutative.
- $+$ is *not* a binary operation in $\mathbb{Z} \setminus \{0\}$, as $1 + (-1) = 0 \notin \mathbb{Z} \setminus \{0\}$.

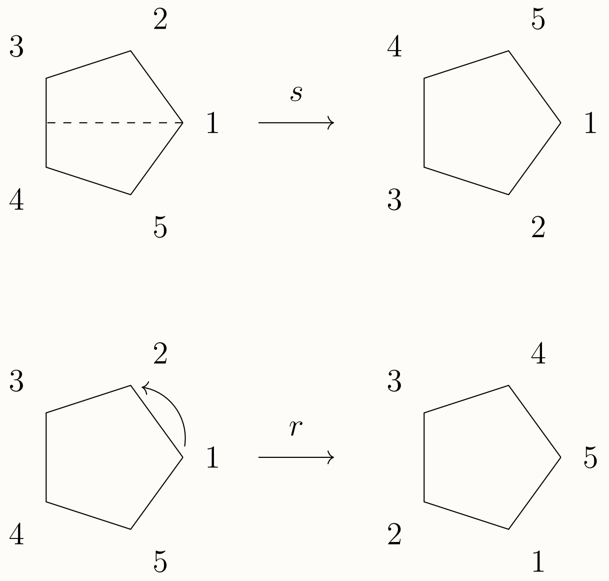
- $\times$ is a binary operation in the reals $\mathbb{R}$. It is both assoc and comm.
- Denote $M_n(\mathbb{R})$ as the set of all $n \times n$ matrices with real entries. Matrix multiplication on this set is a binary operation; it is assoc but not comm.
- $+$ on the set of evens (denoted $2\mathbb{Z}$) is a assoc and comm binary operation.
- Let X be a set, and define $G := \{f : X \to X\}$ the set of all functions from X to itself. Function composition is a binary operation; it is associative but not commutative.

1.1 Dihedral Group

Now perhaps my favorite example, and a pedagogically important one:

Example 1.4 (Symmetries of regular pentagon)

Consider the symmetries of a regular pentagon. By symmetries, we mean rigid motions that involve taking the pentagon, "moving it around" and "placing it back" to the original pentagon. In particular, there are two "types" of symmetries: rotation and reflection. For instance, rotating the pentagon by $\frac{2\pi}{5}$ radians counterclockwise is a symmetry (call r), as is reflecting the pentagon by some axis of symmetry (call reflection across the "vertical" axis as s):



Given this, there is a very natural binary operation: we can apply one symmetry after another. $s \circ r$ involves rotating first, then reflecting. Work through it and convince yourself that this is in fact another symmetry!

We call the set of symmetries of a regular pentagon (resp. n-gon) as D_{10} (resp. D_{2n}). This, as we will see soon, is a group!

1.2 Defining a Group, with Many Examples

Speaking of groups, now we can define what a group is!

Definition 1.5. A **group** is an orderd pair $(G, *)$ for a set G and a binary operation $* : G \times G \to G$ such that

1. $*$ is associative
2. There exists $e \in G$ called the **identity**, so that $e * g = g * e = g$ for all $g \in G$.
3. For every $g \in G$, there exists an inverse $g^{-1} \in G$ such that $g * g^{-1} = e = g^{-1} * g$.

Remark 1.6. Note here that a group is a set with a specified operation. Specifying the operation is important! However, if the operation is well-understood (e.g. for the symmetries of a regular pentagon, there is really only one operation), then we omit specifying the operation.

So a group is a very simple algebraic object! It only has three axioms. But somehow, these three axioms encapsulate a lot of things which interest mathematicians.

Example 1.7 (D_{10} is a group)

The D stands for **dihedral**, so this is called the **dihedral group of order 10**. Let's work through the axioms. We established that composing two symmetries is associative, so Axiom (1) is good. The identity symmetry is the "do nothing" symmetry – think of picking up the pentagon and placing it down exactly as it was. Finally, you can intuitively convince yourself that every symmetry has an inverse, as there is a notion of "undoing" a rotation or reflection.

It's important to note that $*$ *need not be commutative*. But it's damn nice if it happens to be, so much so we give it a name:

Definition 1.8. A group $(G, *)$ is called **abelian** if $*$ is commutative.

Example 1.9

$(\mathbb{R}^\times, \times)$ is an abelian group! $(\mathbb{R}^\times = \mathbb{R} \setminus \{0\})$ As is $(\mathbb{C}^\times, \times)$. (Just work through the axioms.)

We're going to continue working with examples of groups – the more examples, the more intuitive this notion will become. For each one, work through the three axioms (and check that the operation is a binary operation!) and convince yourself that this is in fact a group (I'll help you with some):

Example 1.10 (Special Linear Group)

Let $G := \{A \in M_2(\mathbb{R}) \mid \det(A) = 1\}$, and consider $(G, \times)$. First, this is indeed a binary operation, since $\det(AB) = \det(A)\det(B)$ by something something linear algebra. Matrix multiplication is associative. The identity matrix is $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Finally, any matrix $A \in G$ has an inverse, since $\det(A) = 1 \neq 0$, and $\det(A^{-1}) = (\det(A))^{-1} = 1$, so $A^{-1} \in G$.

Often, we notate this group as $\mathrm{SL}_2(\mathbb{R})$, called the **special linear group**.

Example 1.11 (D_6)

Consider D_6, the symmetries of an equilateral triangle. Again, there are two "types" of symmetries: rotation and reflection. Denote r as rotation by $\frac{2\pi}{3}$ radians counterclockwise. Choose an axis of symmetry, and denote s as the reflection across this axis.

- Consider $s \circ r$, that is, rotating first, then reflecting. Is this another symmetry? (Yes.) Which one? How could we get to this configuration in one "step"?
- Convince yourself that combining any two symmetries gives another symmetry.
- We'll take associativity for granted, but perhaps convince yourself that our binary operation here is indeed associative.
- What is the identity element? Look back at D_{10}.
- Convince yourself that every symmetry has an inverse.
- How many elements are there in D_6? Can you write out all elements of D_6? Even better, can you write out all elements of D_6 in terms of r and s?

Example 1.12 (Symmetric group)

Let S_3 be the set of all bijective functions $f : \{1,2,3\} \to \{1,2,3\}$. (If you like permutations more than functions, you can think of S_3 as the set of all permutations on the set $\{1,2,3\}$.) More generally, S_n is the set of all bijective functions $f : \{1,2,\ldots,n\} \to \{1,2,\ldots,n\}$. One can compute $|S_n| = n!$ (n choices for where 1 goes, then $n-1$ choices for where 2 goes, etc).

Let function composition $\circ$ be our binary operation (it is indeed binary, as two bijective functions composed gives another bijective function). Function composition is always associative, so this checks off the first axiom. The identity is, well, the identity function, i.e. $f(x) = x$. Finally, a bijective function must have an inverse by definition, so all group axioms are satisfied.

The symmetric group is powerful because, for a set with n elements, it encapsulates *all* possible symmetries. And this is what any group is doing: a group is specifying certain symmetries on a set. D_{10} is, in the end, simply permuting five vertices, but with certain restrictions, which restricts the number of symmetries we have ($|D_{10}| = 10 < 120 = |S_5|$). We'll see this more formally stated later on in the class.

1.3 Proving Properties

As this is a proof-oriented class, perhaps we should prove one of two things before class ends.

Theorem 1.13 (Cancellation Law)

If $(G, *)$ is a group and $ab = cb$ (resp. $ba = bc$), then $a = c$ for all $a, b, c \in G$.

Proof. Suppose $ab = cb$. By Axiom 3, the inverse of b exists. Multiply both sides on the right by b^{-1}:

$$\begin{aligned}(ab)b^{-1} &= (cb)b^{-1}\\ a(bb^{-1}) &= c(bb^{-1})\\ a(e) &= c(e)\\ a &= c.\end{aligned}$$

The proof works similarly for showing $ba = bc \implies a = c$. □

It's impressive that the proof above, although short, uses all three axioms! This goes to show the compact yet purposeful nature of the group definition.

Proposition 1.14

If $(G, *)$ is a group,

1. The identity of G is unique.
2. For each $a \in G$, the inverse a^{-1} is unique.
3. $(a^{-1})^{-1} = a$ for $a \in G$.
4. $(ab)^{-1} = b^{-1}a^{-1}$.

Proof. **Statement (1):** Suppose e_1, e_2 are two identities. Then, $e_1 = e_1 * e_2 = e_2$. (Alternately, use Cancellation Law to get $e_1 * e_1 = e_1 = e_1 * e_2 \implies e_1 = e_2$.)

Statement (2): Assume b, c are two inverses for $a \in G$. This means $ab = e = ac \implies b = c$ by uniqueness of identity and Cancellation Law.

Statement (3): Note $aa^{-1} = (a^{-1})^{-1}a^{-1} = e$ by definition of the inverse. In particular, a and $(a^{-1})^{-1}$ are both the inverse of a^{-1}, so by (2) the result follows. (You can also use Cancellation Law, but we're trying not to use the same hammer for every nail.)

Statement (4): Note $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = a(e)a^{-1} = aa^{-1} = e$, so $b^{-1}a^{-1}$ is the inverse of ab. By uniqueness of inverse, the result follows. □

So it seems like from the axioms alone, we can prove a lot. It's really mind-blowing to think that everything we prove in the first half of this class will come from *just these three axioms.* We'll continue proving more fundamental properties about groups next week.

2 09/07 - Group Homomorphisms & Isomorphisms

We start with focusing our attention to two groups we covered last time. Reminder that we need to specify an operation when we introduce a group, but for these examples, the operation is well-understood, so we omit them for notation's sake.

2.1 $D_6 \simeq S_3$

Recall

$$\begin{aligned} S_3 &:= \{f : \{1,2,3\} \to \{1,2,3\} \text{ bijective}\} \\ D_6 &:= \{\text{symmetries of an equilateral triangle}\}. \end{aligned}$$

We established last time that $|S_3| = |D_6| = 6$. This is a fruitful observation.

We're going to investigate the "similarities" between the two groups now. Denote s as reflection of the triangle across the vertical axis, and let r be the rotation of the triangle $2\pi/3$ radians clockwise (last time we specified counterclockwise, but Dummit and Foote uses clockwise, so we've adapted accordingly).

> **Exercise 2.1.** Label the vertices as 1, 2, 3. How does the rotation r map the vertices? Where does vertex 1 go? 2? 3? Can you express the rotation r, then, as a bijective function?

A key observation is that every symmetry of the triangle is simply permuting the vertices of the triangle. In other words, it maps bijectively the set of vertices of the triangle to itself. This means that every element in D_6 is an element in S_3 in disguise!! So we can establish $D_6 \subseteq S_3$.

But now we employ our observation that $|D_6| = |S_3| = 6$. This requires for the inclusion to be an equality, so $D_6 = S_3$.

2.2 Definitions

But wait, what does it even mean for two groups to be equal to each other? We'll provide a formal way of describing these "equalities" before providing a more intuitive explanation.

Definition 2.2 (Group Homomorphism)**.** Let $(G, *_G)$ and $(H, *_H)$ be groups. A function $\varphi : G \to H$ is a **homomorphism** if $\forall\, x, y \in G$,

$$\varphi(x *_G y) = \varphi(x) *_H \varphi(y).$$

To clarify, $*_G$ is the group binary operation for the group G, and $*_H$ likewise for H. The notation is a bit clunky, though, so sometimes we're lazy and adopt the multiplication notation for both: $\varphi(xy) = \varphi(x)\varphi(y)$.

We need something a bit more powerful to make this embody our notion of equality:

Definition 2.3 (Group Isomorphism)**.** A group homomorphism $G \to H$ is called a **group isomorphism** if it is bijective. We write $G \simeq H$.

Intuitively, here's what's happening: a homomorphism is saying that the *group structure* of G and H, respectively, are the same. Whatever operation we take in G has an analogous operation in H. An isomorphism specifies this further by saying that every operation in H has an analogous operation in G as well. This produces a one-to-one correspondence between the two groups where all corresponding operations coincide, so they're the same.

Here's another way of thinking about isomorphisms: you can call two groups different things, label its elements different things, but at the end of the day they're the *same group*. They have the same structure with respect to the group axioms.

2.3 Isomorphism Examples

As always, it's best to learn through examples:

Example 2.4 (Groups with Two Elements)

We already "showed" $D_6 \simeq S_3$. Here is another: let $S_2 = \{e, \sigma\}$ be the symmetric group on two elements, i.e. e is the map sending $e(1) = 1$ and $e(2) = 2$, and σ is the map $\sigma(1) = 2$, $\sigma(2) = 1$. I claim there is an isomorphism

$$\varphi : (\{+1, -1\}, \times) \xrightarrow{\simeq} S_2$$

where $\varphi(1) = e$ and $\varphi(-1) = \sigma$. This is illustrated by the following multiplication tables. Note that they are exactly the same, just with different labels for elements:

$\cdot$	1	-1
1	1	-1
-1	-1	1

$\circ$	e	σ
e	e	σ
σ	σ	e

Example 2.5 (Turning $+$ into $\times$)

A useful one! Denote $\mathbb{R}_{\geq 0}$ as the set of positive real numbers. We have an isomorphism

$$\begin{aligned}\varphi : (\mathbb{R}, +) &\xrightarrow{\simeq} (\mathbb{R}_{\geq 0}, \cdot) \\ x &\mapsto e^x.\end{aligned}$$

First, this is a homomorphism: $e^{x+y} = \varphi(x+y) = \varphi(x) \cdot \varphi(y) = e^x \cdot e^y$, which is true. Note that the left hand side has addition, while the right has multiplication. This aligns with how we define φ, as it takes a group with the addition operation to a group with the multiplication operation. Furthermore, it is an isomorphism as it has an inverse, namely the log function.

2.4 Non-Isomorphism Examples

Example 2.6 (Multiplication by $n \in \mathbb{Z}$)

Fix $n \in \mathbb{Z}$, and define the map $\varphi : (\mathbb{Z}, +) \to (\mathbb{Z}, +)$ where $\varphi(k) = nk$. This is a group homomorphism: if $k, \ell \in \mathbb{Z}$, then

$$n(k+\ell) = \varphi(k+\ell) = \varphi(k) + \varphi(\ell) = nk + n\ell.$$

However, it is not a group isomorphism. An intuitive arguemnt is as follows: if it was, then its inverse map would be multiplication by $1/n$, but this map doesn't guarantee integer outputs. To be more formal, we can show that φ is not surjective: there does not exist a $k \in \mathbb{Z}$ such that $nk = \varphi(k) = 1$.

Example 2.7 (Determinants)

Finally, we can view taking the determinant of a matrix as a map, namely taking in a matrix and outputting a real number. Denote $\mathrm{GL}_n(\mathbb{R})$ as the set of $n \times n$ invertible matrices with real entries, and define the map

$$\begin{aligned}\det : (\mathrm{GL}_n(\mathbb{R}), \times) &\to (\mathbb{R} \setminus \{0\}, \times) \\ A &\mapsto \det(A).\end{aligned}$$

This is a homomorphism! From linear algebra, we know for two matrices $A, B \in \mathrm{GL}_n(\mathbb{R})$, $\det(AB) = \det(A)\det(B)$. However, this is not an isomorphism, as the det map is NOT injective. For instance, $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$ both have determinant 1.

2.5 Conjugation

Finally, a super important isomorphism, one which will come up over and over again in this course (and beyond!):

Example 2.8 (Conjugation)
Let G be a group, and fix an element $g \in G$. Define a map

$$\begin{aligned} \varphi_g : G &\to G \\ a &\mapsto gag^{-1}. \end{aligned}$$

φ_g is called **conjugation by** g. This is indeed a homomorphism: given $a, b \in G$,

$$\begin{aligned} \varphi_g(a)\varphi_g(b) &= (gag^{-1})(gbg^{-1}) = ga(g^{-1}g)bg^{-1} \\ &= (ga)(bg^{-1}) = g(ab)g^{-1} \\ &= \varphi_g(ab). \end{aligned}$$

Even better, it is an isomorphism! We claim that the inverse of our map φ_g is precisely $\varphi_{g^{-1}}$. We verify:

$$\begin{aligned} (\varphi_g \circ \varphi_{g^{-1}})(a) &= \varphi_g(g^{-1}ag) = g(g^{-1}ag)g^{-1} = a \\ (\varphi_{g^{-1}} \circ \varphi_g)(a) &= \varphi_{g^{-1}}(gag^{-1}) = g^{-1}(gag^{-1})g = a, \end{aligned}$$

as desired.

This conjugation map is even more special because it is a map from G to itself. These are so special, they have its own name:

Definition 2.9 (Automorphism)**.** An isomorphism is called an **automorphism** if its domain and codomain are the same. Given a group G, we define

$$\mathrm{Aut}(G) := \{\varphi : G \to G \mid \varphi \text{ isomorphism}\}.$$

2.6 Homomorphisms Respect Structure

The following proposition is a good demonstration of homomorphisms indeed respecting group structures. The first two statements state that homomorphisms map the identity to the other respective identity, and likewise for inverses.

Proposition 2.10
Let $\varphi : G \to H$ be a homomorphism. Then,

1. $\varphi(e_G) = e_H$
2. $\varphi(a^{-1}) = (\varphi(a))^{-1}$
3. If $\varphi : G \to H$ is a group isomorphism, then its inverse $\varphi^{-1} : H \to G$ is also.

Proof. **Statement (1):** Let e_G be the identity element of G. We have $\varphi(e_G) = \varphi(e_G e_G) =$

$\varphi(e_G)\varphi(e_G)$, so by Cancellation Law, we conclude $\varphi(e_G) = e_H$.

Statement (2): Let $a \in G$. We want to show $\varphi(a^{-1})\varphi(a) = e_H$ and $\varphi(a)\varphi(a^{-1}) = e_H$. For the first equality, as φ is a homomorphism, we have $\varphi(a^{-1}\varphi(a) = \varphi(a^{-1}a) = \varphi(e_G) = e_H$ by Statement (1). The second equality follows similarly: $\varphi(a)\varphi(a^{-1}) = \varphi(aa^{-1}) = \varphi(e_G) = e_H$.

Statement (3): Let $a, b \in G$. As φ is a homomorphism,

$$\varphi(\varphi^{-1}(a)\varphi^{-1}(b)) = \varphi(\varphi^{-1}(a))\varphi(\varphi^{-1}(b)) = ab.$$

As φ is bijective (it is an isomorphism), this must mean $\varphi^{-1}(a)\varphi^{-1}(b) = \varphi^{-1}(ab)$, so it is a homomorphism. The conclusion follows since φ^{-1} is bijective as φ is bijective. □

2.7 Defining Orders

We end class by introducing a definition which we'll use many times throughout the course. Corresponding resource: around pg 20 in Dummit and Foote.

Definition 2.11 (Order of element)**.** Let G be a group and $x \in G$. The **order of x** is the smallest positive integer n such that

$$x^n = \underbrace{x * x * \cdots * x}_{n \text{ times}} = e.$$

We notate the order of x by $|x|$. By convention, if no positive power of x is the identity, then $|x| = \infty$.

Exercise 2.12. Find the order of the identity element for any group. Find all elements with finite order in the multiplicative group $(\mathbb{C} \setminus \{0\}, \times)$. (Hint: there are infinitely many of them!)

Exercise 2.13 (Orders in D_{10})**.** Take the symmetries of the pentagon D_{10}. Let r be rotation by $2\pi/5$ radians clockwise, and s be the reflection across some fixed axis. Find $|r|$ and $|s|$. Find $|s \circ r|$.

We'll leave this one for next time:

Proposition 2.14

Let G be a group and $a \in G$. If $a^k = e$ for some $k \in \mathbb{Z}$, then $|a| \mid k$.

3 09/12 - Subgroups, Cyclic, More on Orders

3.1 Orders and Divisibility

Exercise 3.1. Last time, we demonstrated $D_6 \simeq S_3$. But can $D_{2n} \simeq S_n$ if $n > 3$?

Proof. A quick cardinality argument suffices. One can check $|D_{2n}| = 2n$ and $|S_n| = n!$, and if these two groups were isomorphic, then their cardinality must be the same. This is not the case for $n > 3$. □

So isomorphisms must preserve the size of a group. They also preserve other things, like the order of elements. We start here, which we stated last time:

Proposition 3.2

Let G be a group, $a \in G$. If $a^k = e$ for $k \in \mathbb{Z}$, then $|a| \mid k$.

Proof. Let $a \in G$, and denote $n = |a|$. We prove by contradiction using Division Algorithm on k and n: we can write $k = n \cdot b + r$ for $b, r \in \mathbb{Z}$, $0 \leq r < b$. But note that

$$e = a^k = a^{nb+r} = (a^n)^b \cdot a^r = a^r$$

so if $r > 0$, then $a^r = e$ and $r < n$, which contradicts the minimality of the order n. Thus, $r = 0$, which means $k = nb$, so $n \mid k$, as desired. □

Now we make our claim on preserving orders more precise:

Proposition 3.3 1. If $\varphi : G \to H$ is a group homomorphism and $a \in G$, then $|\varphi(a)| \mid |a|$.

2. If $\varphi : G \to H$ is a group isomorphism and $a \in G$, then $|\varphi(a)| = |a|$.

We'll prove the two statements separately.

Proof. (Statement 1) Let $a \in G$. Denote $n = |a|$, so $a^n = e$. Applying φ to both sides, we get $\varphi(a^n) = \varphi(e) = e$. By definition of homomorphism, we have $\varphi(a^n) = \varphi(a)^n$, so $\varphi(a)^n = e$. By our above proposition, this means $|\varphi(a)|$ divides n. □

Proof. (Statement 2) By Statement 1, we already know that $|\varphi(a)|$ divides $|a|$. It then suffices to prove $|a|$ divides $|\varphi(a)|$. Denote $m = |\varphi(a)|$, so $(\varphi(a))^m = e$. But by definition of homomorphism, we can write $(\varphi(a))^m = \varphi(a^m) = e$. As φ is an isomorphism (in particular, it is injective), we must have $a^m = e$. Using Proposition 3.2, we get m divides $|a|$, as desired. □

3.2 Subgroups

This is the start of Section 2 in Dummit and Foote. Very simply, a subgroup is just a subset of a group that happens to be a group itself. We see that this arises pretty naturally – e.g. if you ocnsider only the rotations in the dihedral group, that forms a group – and it is a powerful way of encoding more information about our groups.

Definition 3.4. Let $(G, *)$ be a group. A subset $H \subseteq G$ is a **subgroup** if H is non-empty and H is closed under products and inverses, i.e. if $x, y \in H$, then $xy \in H$ and $x^{-1} \in H$. For notation, if H is a subgroup, we write $H \leq G$.

A quick observation: $e \in H$. Let's prove it! We're going to use all three axioms of a subgroup: (1) it is non-empty, (2) it is closed under products, and (3) it is closed under inverses. Let $H \leq G$. By (1), we have some $x \in H$. By (3), $x^{-1} \in H$ as well. And (2) brings us home since $xx^{-1} = e \in H$.

Note that H inherits the group operation $*$ from G, and equipped with this operation, $(H, *)$ is itself a group. So the name "subgroup" is not a misnomer, whew.

Example 3.5 (Subgroup Examples)

A few, building off of the groups we've introduced before:

1. $(\mathbb{Z}, +) \leq (\mathbb{Q}, +) \leq (\mathbb{R}, +)$.
2. For every G, $\{e\} \leq G$ (the **trivial subgroup**) and $G \leq G$.
3. Reminder $\mathrm{GL}_n(\mathbb{R})$ is the set of $n \times n$ matrices with real entries and determinant non-zero, and $\mathrm{SL}_n(\mathbb{R})$ the same but with determinant 1. Then, $\mathrm{SL}_n(\mathbb{R}) \leq \mathrm{GL}_n(\mathbb{R})$.
4. A **non**-example: $(\mathbb{Q} \setminus \{0\}, \times)$ is NOT a subgroup of $(\mathbb{R}, +)$ because the binary operation is different.

3.3 Subgroups of Dihedral (Square)

Because we like our dihedral groups so much:

Example 3.6 (Subgroups of D_8)

Consider the symmetries of a square D_8. Choose your favorite axis of symmetry, and call s the reflection across that axis. Call r the rotation by 90° clockwise. We can write the elements of D_8 as $D_8 = \{e, r, r^2, r^3, s, rs, r^2s, r^3s\}$.

One subgroup is the one where we only take rotations, i.e. the subset $\{e, r, r^2, r^3\}$. Clearly it is non-empty; we can check it is closed under inverses: $r^{-1} = r^3$, $(r^2)^{-1} = r^2$, and $(r^3)^{-1} = r$. (What is the inverse of e?) It is also closed under products: for example, $r^2r^3 = r^5 = r$ since $r^4 = e$.

Another subgroup is $\{e, s\}$. Verify that this is a subgroup. Can you find another group which is isomorphic to this one? (What groups with two elements do you know?)

Finally, let's take a spicier subgroup. We'll start with three elements: e, s, r^2. Note that each serves as their own inverse. If we are to construct a subgroup, we need to make sure this set is closed under products, so our set must include r^2s. We claim that

r^2s is also its own inverse, proving it via the identity $rs = sr^{-1}$ (from homework):

$$(r^2s)(r^2s) = (r^2s)(rrs) = (r^2s)r(sr^{-1}) = r^2s(rs)r^{-1} = r^2ssr^{-1}r^{-1} = r^2er^{-2} = e.$$

This set $\{e, s, r^2, r^2s\}$, we claim, is a subgroup of D_8. (Check it yourself!)

There's a lot to unpack here.

The nice thing is that we found two subgroups of D_8 with 4 elements! This particular subgroup is actually a really important; we denote it as V_4, called the **Klein four-group**. Note that this subgroup is NOT isomorphic to the subgroup of just rotations: for rotations, r has order 4, but there is no element in V_4 that has order 4 (the identity has order 1, and everything else has order 2).

We can have "chains" of subgroups: for instance, $\{e, s\} \leq V_4 \leq D_8$ and $\{e, r^2\} \leq \{e, r, r^2, r^3\} \leq D_8$. The property of being a subgroup is transitive, that is, if $H' \leq H$ and $H \leq G$, then $H' \leq G$. This follows roughly from the definition of a subgroup, as H' inherits the group operation from G, and closure of product and inverses is independent of the larger group.

3.4 Cyclic (Sub)groups

We spoke a lot about the V_4 subgroup, but the other subgroup with four elements, namely the subgroup of rotations $\{e, r, r^2, r^3\}$, is quite nice as well! Notably, it is generated by a single element (r). Such a subgroup (resp. group) is called a **cyclic** subgroup (resp. group). More specifically, the cyclic subgroup of G generated by a is

$$\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}.$$

If this cyclic subgroup is the entire group, we say the group itself is cyclic.

> **Definition 3.7** (Cyclic group)**.** A group G is **cyclic** if $G = \langle a \rangle$ for some $a \in G$. We say G is *generated by a*.

How many elements are in $\langle a \rangle$? In the case of $\langle r \rangle \leq D_8$, we have $|\langle r \rangle| = 4$. But if we take $\langle 2 \rangle \leq (\mathbb{R} \setminus \{0\}, \times)$, then the subgroup has infinitely many elements. We can note, though, that $|r| = 4$ and $|2| = \infty$, which is basically exactly what's going on here. Let's make this relation explicit:

Theorem 3.8 (Order of group is order of generator)

Suppose $G = \langle a \rangle$ for some $a \in G$, i.e. G is cyclic. Then, $|G| = |\langle a \rangle| = |a|$.

Proof. First, we take the case where $|a| = n$ is finite. Consider $e, a, a^2, \ldots, a^{n-1} \in G$. By minimality of n, they are all distinct; in particular, if $a^i = a^j$ for $0 \leq i \leq j < n$, then $a^i(a^{j-i}) = a^i \implies a^{j-i} = e$. But by Proposition 3.2, $n \mid j - i$. If $i = j$, we're good;

otherwise, since $0 < j - i$ and $j - i \leq j < n$, we reach a contradiction from the minimality of n, so indeed $i = j$.

Since all the elements $e, a, a^2, \dots, a^{n-1}$ are distinct, we have $n \leq |G|$. Now we wish to show these elements are in fact *all* the elements of G, i.e. $\{e, a, \dots, a^{n-1}\} = \langle a \rangle$. Luckily, this follows directly from Division Algorithm! Take any $k \in \mathbb{Z}$. By Division Algorithm $\exists\, q, r \in \mathbb{Z}$ with $0 \leq r < n$ such that $k = nq + r$. This means that

$$a^k = a^{nq+r} = (a^n)^q \cdot a^r = a^r,$$

so any element of $\langle a \rangle$ ends up being equal to one of $e, a, a^2, \dots, a^{n-1}$, which is what we wanted to prove.

To finish up, we take the case when $|a|$ is infinite. If $a^n = a^k$ for $n, k \in \mathbb{Z}$, then $a^{n-k} = e$, which is only possible if $n = k$ since $|a|$ is infinite. Thus, we can find infinitely many distinct elements in $\langle a \rangle$ (take a^n for any $n \in \mathbb{Z}$), so $|\langle a \rangle| = \infty$. □

Next time, we will see that we can "classify" these cyclic groups completely! If you want to work this out yourself before next lecture, start with trying to find all cyclic groups of order n ($n \in \mathbb{Z}$). Let G_1 and G_2 be two such groups. Can you find an isomorphism between them?

4 09/14 - Subgroup Properties and Examples

4.1 More on Cyclic Groups

We're picking up directly from last time. I think the following result is a good example of where "proof by example" doesn't hurt, i.e. if you take something like $(\mathbb{Z}/5\mathbb{Z}, +)$ and the subgroup of rotations in D_{10} and show that they are isomorphic, then you've basically done it for the general case.

Theorem 4.1

Any two cyclic groups of the same order are isomorphic.

Proof. First, we assume the order is finite. Let $\langle x \rangle$ and $\langle y \rangle$ be two cyclic groups with $|\langle x \rangle| = |\langle y \rangle| < \infty$. We wish to show $\langle x \rangle \simeq \langle y \rangle$.

To show that two groups are isomorphic, we just need to construct an isomorphism between them. Let $\varphi : \langle x \rangle \to \langle y \rangle$ such that $\varphi(x^n) = y^n$. We must first verify that φ is well-defined, i.e. every element gets mapped to a single element. (Showing well-definedness is an often overlooked but crucial step!) Then, we will verify that φ is a isomorphism, i.e. a bijective homomorphism.

Step 1, well-definedness: It suffices to show that if $x^n = x^m$ for $n, m \in \mathbb{Z}$, then $\varphi(x^n) = \varphi(x^m)$. By our definition of φ, this is equivalent to showing $y^n = y^m$. Since $x^n = x^m$, multiply by x^{-m} on both sides to get $x^{n-m} = e$. By Proposition 3.2, we have $|x| \mid n - m$.

But as $|\langle x\rangle| = |x|$ by Theorem 3.8, we get $|x| = |\langle x\rangle| = |\langle y\rangle| = |y|$, so $|y| \mid n-m$. This means $y^{n-m} = e$, which means $y^n = y^m$ as desired.

Step 2, homomorphism: This is not so bad!

$$\varphi(x^n \cdot x^m) = \varphi(x^{n+m}) = y^{n+m}$$
$$\varphi(x^n)\varphi(x^m) = y^n \cdot y^m = y^{n+m}.$$

Step 3, bijective: Surjectivity is clear: given any $y^n \in \langle y\rangle$, we know $\varphi(x^n) = y^n$. But now the finiteness of these two groups gives us injectivity, since if a function $f : S \to T$ is surjective, then $|S| \geq |T|$, with equality iff f is bijective. As $|\langle x\rangle| = |\langle y\rangle|$ and $\varphi : \langle x\rangle \to \langle y\rangle$, we're done with the finite case!

Now we address the case where $|\langle x\rangle| = |\langle y\rangle| = \infty$. We need to go through the same steps: constructing a map, showing it's well-defined, then showing it's an isomorphism. We'll take the same one we took for the finite case: define a map $\varphi : \langle x\rangle \to \langle y\rangle$ where $x^n \mapsto y^n$. This is well-defined, as y has infinite order so $y^n = y^m$ only if $n = m$. This is also a homomorphism from the same reasoning as in the finite case, and it is bijective by construction. The conclusion follows. □

4.2 Subgroups with Multiple Generators

The corresponding section in Dummit and Foote is Section 2.4.

Let G be a group and $A \subseteq G$ be a subset. We want to answer the following question:

> How can we describe the smallest subgroup of G containing A?

By **smallest** here, we mean that if H is the smallest such subgroup, then for any other subgroup $H' \leq G$ which contains A, $H \subseteq H'$. We're going to call this subgroup the *subgroup of* G *generated by* A and denote it as $\langle A\rangle$, since the elements of A are the generators of this subgroup.

Perhaps starting when $A = \{g\}$ is a single element is a good idea to gain some intuition. Suppose $H \leq G$ is a subgroup containing g. Since subgroups are closed under products, we require $g * g = g^2 \in H$, as well as $g * g * g = g^3$ and, more generally, any g^n for $n \geq 1$. H is also closed by inverses, so $g^{-1} \in H$, and through a similar argument, $g^{-n} \in H$. Finally, $gg^{-1} = e \in H$, so we see that H must necessarily contain $\langle g\rangle$. Even better, the smallest such subgroup is exactly $\langle g\rangle$, so $\langle\{g\}\rangle = \langle g\rangle$.

Example 4.2 (Subgroups of D_8, revisited)

Take the symmetries of the square D_8. The subgroup generated by r is $\{e, r, r^2, r^3\}$. (I've been referring to this subgroup in these notes as the "subgroup of rotations.") The subgroup generated by s is $\{e, s\}$. These two are cyclic subgroups, since they only have one generator.

For a more interesting example, let's compute $\langle A\rangle$ for $A = \{r^2, s\}$. Convince yourself that $\langle A\rangle = \{e, r^2, s, r^2 s\}$.

Exercise 4.3. We identified this last subgroup before. What is it? What name did we give it?

4.3 Properties of Subgroups

Before you read the following claims, try to answer the following questions yourself. Let $H_1, H_2 \leq G$ be subgroups. Is $H_1 \cup H_2$ a subgroup? Is $H_1 \cap H_2$ a subgroup?

Claim 4.4. The union of two subgroups is not always a subgroup. (Take $\langle r^2\rangle \cup \langle s\rangle = \{e, r^2, s\} \subset D_8$.)

Things are more hopeful for intersections, though!

Claim 4.5. The intersection of two subgroups is a subgroup!

The proof of this is basically being careful with the definition of a subgroup and making sure the intersection still satisfies all the properties. To give partial work, we know $e \in H_1$ and $e \in H_2$, so $e \in H_1 \cap H_2$. Suppose we have $a, b \in H_1 \cap H_2$. This means $a, b \in H_1$ and $a, b \in H_2$, so by closure of product in each subgroup, $ab \in H_1$ and $ab \in H_2$, which implies $ab \in H_1 \cap H_2$. Proving inverses are closed under the intersection follows a similar argument.

Note that this proof can be generalized to show that the intersection of *arbitrarily many* subgroups is still a subgroup! This allows us to give the following characterization of $\langle A\rangle$:

$$\langle A\rangle = \bigcap_{\substack{H \leq G \\ H \geq A}} H.$$

This may seem intimidating, but it's actually not telling us anything new – rather, it's just a nice, compact way of defining $\langle A\rangle$. You can prove this by showing inclusion in both directions, but the arguments just follow from the definition.

Exercise 4.6. Let $A = \{a, b\} \subseteq G$. Write down as many elements of $\langle A\rangle$ as you can! (This may seem like a silly exercise, but it'll actually be useful in the future. Check out **free groups** for context.)

Example 4.7 (D_8 in terms of generators)

You've probably realized through the problem sets and playing around with the group D_8 (or in general, D_{2n}) that any element of D_8 can be written in terms of r and s. One way of doing this is

$$D_8 = \{e, r, r^2, r^3, s, rs, r^2 s, r^3 s\},$$

and any other expression with r and s can be simplified to one of the eight above elements via the identities $rs = sr^{-1}$ and $r^4 = s^2 = e$. Thus, $D_8 = \langle r, s\rangle$ is the group generated by $\{r, s\}$ equipped with these identities!

Remark 4.8. Here's a better, more complete way to express D_8 in terms of its generators. Note that the generators of D_8 satisfies special identities, i.e. $rs = sr^{-1}$ and $r^4 = s^2 = e$, and in fact, you can use these identities alone to simplify any expression in terms of r and s as an element in D_8.

This is the motivation for what we call a **group presentation**: we specify the generators of the group, and then state the relations of these generators (our identities from before). This is written as $\langle\text{generators} \mid \text{relations}\rangle$, so we can write

$$D_8 = \left\langle r, s \mid rs = sr^{-1}, r^4 = s^2 = e\right\rangle.$$

The fascinating thing about the group presentation is that although we can think of r and s as rotations and reflections, this way of presenting the group completely rips the group away from any geometric context. Every element in this group can be written in terms of two variables which satisfy certain properties – it just happens that there is a nice geometric interpretation of these properties. We'll (hopefully) see more of this later on in the course.

4.4 Centralizers

This is Section 2.2 in Dummit and Foote.

Definition 4.9 (Centralizer)**.** Let $A \subseteq G$ be a subset of group G. The **centralizer** of A is

$$C_G(A) := \{g \in G \mid gag^{-1} = a \forall\, a \in A\},$$

i.e. it is the set of all group elements which commute with every $a \in A$.

Observe $C_G(A) \subseteq G$; it would be nice if it were a subgroup. Luckily, math is often nice (unless you're doing it at 3am on a Tuesday night rip):

Proposition 4.10

$C_G(A) \leq G$ is a subgroup.

Proof. First, it is non-empty, as one can show $e \in C_G(A)$. Next, we show that it is closed under inverses. If $g \in C_G(A)$, then by definition, $gag^{-1} = a$ for all $a \in A$. But this means

$$a = g^{-1}(gag^{-1})g = g^{-1}(a)g,$$

so $g^{-1} \in C_G(A)$ as well. Finally, if $g, h \in C_G(A)$, then for all $a \in A$, $gag^{-1} = hah^{-1} = a$. Thus, we have

$$(gh)a(gh)^{-1} = g(hah^{-1})g^{-1} = gag^{-1} = a,$$

and so $gh \in C_G(A)$ as well. □

Definition 4.11 (Center)**.** $C_G(G) = Z(G)$ is the **center** of G.

Example 4.12 (Centralizers of D_8)

Let $G = D_8$ and $A = \{r\} \subseteq G$. We know that any r^i commutes with r (more powerfully, the subgroup of rotations is abelian), so $C_G(r) \supseteq \{e, r, r^2, r^3\}$. Could there be more?

From the problem set, we showed that $rs = sr^{-1} \neq sr$, so $s \notin C_G(r)$. But could $r^i s \in C_G(r)$ (for $1 \leq i \leq 3$)? Suppose yes, for the sake of contradiction. Since $r^{-i} \in C_G(r)$ and $C_G(r)$ is a subgroup, $r^{-i}r^i s = s \in C_G(r)$ by closure of products, which we already established cannot be the case. Thus, we have $C_G(r) = \{e, r, r^2, r^3\} = \langle r \rangle$!

Exercise 4.13. Compute $C(D_8)$, the center of D_8.

4.5 Kernel and Image

If you know these terms from linear algebra, you're in luck – the terms mean the exact same thing here. The only difference is that in linear algebra, functions are linear maps. Here, they are homomorphisms.

Let $\varphi : (G, *_G) \to (H, *_H)$ be a group homomorphism.

Definition 4.14 (Kernel, Image)**.** The **kernel** and **image** of φ are, respectively,

$$\ker \varphi = \{g \in G \mid \varphi(g) = e_H\}$$
$$\operatorname{Im} \varphi = \{\varphi(g) \mid g \in G\}.$$

Well, I named today's lecture as "Subgroup Properties and Examples" so we better hope that $\ker \phi$ and $\operatorname{Im} \phi$ are both subgroups.

Proposition 4.15

If $\varphi : G \to H$ is a group homomorphism, then $\ker \varphi \leq G$ and $\operatorname{Im} \varphi \leq H$.

Proof. We first show that $\ker \varphi \leq G$. First, it is non-empty, as $\varphi(e_G) = e_H$. Now we show closure of inverses. If $g \in \ker \varphi$, then $\varphi(g) = e_H$, so $\varphi(g^{-1}) = (\varphi(g))^{-1} = e_H^{-1} = e_H$, which means $g^{-1} \in \ker \varphi$. Finally, if $g_1, g_2 \in \ker \varphi$, then $\varphi(g_1) = \varphi(g_2) = e_H$, which means $\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2) = e_H * e_H = e_H$. This implies $g_1 g_2 \in \ker \varphi$.

Now we can show $\operatorname{Im} \varphi$. (Myrto: "this is left as an exercise for the reader.") □

5 09/19 - Lagrange's Theorem

We've been dealing with a lot of results related to divisibility, e.g. if $a^k = e$, then $|a|$ divides k. One may have noticed just by playing with examples that the order of an element always divides the number of elements in the group. Equivalently, for any $g \in G$, $|\langle g \rangle|$ divides $|G|$, and $\langle g \rangle \leq G$. But can we generalize?

A remarkable theorem tells us that yes, this is the case:

Theorem 5.1 (Lagrange's Theorem)
If $H \leq G$, then $|H| \mid |G|$.

This is a very simple result to state, and it'll turn out that it has a simple proof as well. The most difficult part, in my opinion, is setting up the appropriate language to prove it. So we'll start with a series of definitions:

5.1 Partitions and Equivalence Relations

These notions are pretty general – in fact, this entire section is not specific to groups at all – but they will be central to our language for proving our main theorem. Don't be scared by these definitions, as you are probably familiar with these notions already. We just present them in this manner for formalization purposes.

Definition 5.2 (Partition)**.** Let S be a set. A **partition** of S is a a collection of subsets $\{S_i : i \in I\}$ (I is just some indexed set) such that

$$S = \bigsqcup_{i \in I} S_i$$

with the following two conditions:

- $S_i \neq \emptyset$
- If $S_i \neq S_j$, then $S_i \cap S_j = \emptyset$, i.e. they are disjoint.

Example 5.3 (Partitions of $\mathbb{Z}$)
These are kinda stupid, but we'll provide two partitions of $\mathbb{Z}$:

$$\mathbb{Z} = \{n \in \mathbb{Z} \mid n > 0\} \sqcup \{0\} \sqcup \{n < 0 \mid n \in \mathbb{Z}\} = \bigsqcup_{n \in \mathbb{Z}} \{n\}.$$

Another useful (and already familiar) definition is an equivalence relation.

Definition 5.4 (Equivalence relation)**.** An **equivalence relation** on S is a binary relation $\sim$ such that for any $x, y, z \in S$, we have

1. (*Reflexivity.*) $x \sim x$
2. (*Symmetry.*) $x \sim y \iff y \sim x$
3. (*Transitivity.*) $x \sim y$ and $y \sim z$ implies $x \sim z$

Example 5.5 (Equivalence relations on $\mathbb{Z}$)

Perhaps the easiest one, besides our usual notion of equality in any familiar number system, is congruence under some modulus. In particular, for any fixed $n \in \mathbb{Z}$, we can define our equivalence relation $\sim$ as $a \sim b$ iff $n \mid a - b$, i.e. $a \equiv b \pmod{n}$.

Whenever we deal with equivalence relations from here on out, use this one as your point of reference. There are many quirkier examples out there though!

Given an equivalence relation, we can now define **equivalence classes**. This is a powerful concept, as we'll see soon:

Definition 5.6 (Equivalence class)**.** The **equivalence class** of $x \in S$ is the set

$$C_x = \{y \in S \mid y \sim x\} =: \overline{x}.$$

In $\mathbb{Z}$ with the equivalence relation $\equiv \pmod{n}$, $C_0 = n\mathbb{Z}$, and in general $C_a = \{y \in \mathbb{Z} \mid y = ns + a, s \in \mathbb{Z}\}$.

Exercise 5.7. Convince yourself that $C_a = C_{n+a}$, i.e. they are exactly the same set. How many total distinct equivalence classes are there?

I argue this is the pedoagogically correct way to think about modular arithmetic, even if it may be inconvenient at first. I always found it a bit odd that the integers mod n are written as $\{0, 1, \ldots, n-1\}$; for instance, I could write $\mathbb{Z}/3\mathbb{Z} = \{3, 7, 38\}$ with $7 + 7 \equiv 38$, etc. and everything would still be valid. The way to get around this arbitrary choice is to not make an arbitrary choice in the first place, and rather think of these elements as equivalence classes. 0 (or 3, or any multiple of 3) is merely acting as a *representative* of the equivalence class C_0.

From the above exercise, one may understand why we brought up partitions. The equivalence classes form a partition of the set! For instance, the integers can be partitioned into evens and odds, which correspond to the equivalence classes under congruence mod 2. We'll state this more generally:

Proposition 5.8

Any equivalence relation on a set S determines a partition of S, and vice versa.

Proof. Suppose $\sim$ is an equivalence relation on S. First, we'll prove the forward direction: the *distinct* equivalence classes $C_x = \{y \in S \mid y \sim x\} = \overline{x}$ form a partition of S.

We have $x \in C_x$ by reflexivity, so in particular $C_x \neq \emptyset$. Furthermore, we know that every element x belongs in an equivalence class, namely C_x. It remains to show that if $C_x \neq C_y$ for $x, y \in S$, then $C_x \cap C_y = \emptyset$.

Assume for the sake of contradiction that $z \in C_x \cap C_y$. Then, $z \sim x$ and $z \sim y$, so by symmetry, $x \sim z$ and then transitivity gives us $x \sim y$. But then we can show $C_x = C_y$: $z \in C_x \implies z \sim x \implies z \sim y \implies z \in C_y$ by transitivity, and vice versa.

Conversely, we wish to construct an equivalence relation from a partition. Let $\{S_i\}$ be a partition of S. We can define $x \sim y$ if x, y are in the same S_i. By default, we have $x \sim x$ and $x \sim y \implies y \sim x$, so this is both reflexive and symmetric. It is also easy to see that if $x \sim y$ and $y \sim z$, i.e., $x, y \in S_i$ and $y, z \in S_i$, then $x, z \in S_i \implies x \sim z$, so transitivity holds. □

5.2 Specifying to Groups

It's time to apply all this to the context of groups. We can define a natural equivalence relation on G that is induced by a subgroup $H \leq G$.

Definition 5.9 (Equivalence relation induced by subgroup)**.** Let G be a group, and $H \leq G$ subgroup. For $a, b \in G$, we say $a \sim b$ iff $\exists\, h \in H$ such that $a = bh$, i.e. $b^{-1}a \in H$.

From now on, whenever we have an equivalence relation $\sim$, we are referring to this one, with respect to whatever subgroup we have at hand. We see that this naturally generalizes our favorite congruence relation; we'll illustrate this with the $\equiv \pmod 2$ case.

Example 5.10 (Congruence mod 2 via subgroup $2\mathbb{Z}$)

We have $H = 2\mathbb{Z} \leq \mathbb{Z}$ under $+$. The above relation becomes $a \sim b \iff -b + a \in 2\mathbb{Z}$, which is true when $2 \mid a - b$, i.e. $a \equiv b \pmod 2$.

From now on, we'll call the equivalence relation induced by H as "congruence modulo H." We already saw that congruence modulo n for some $n \in \mathbb{Z}$ is just a specific case of this. In general, when we say modulo H, we are basically saying "send every $h \in H$ to the identity." Indeed, for any $h \in H$, we have $h \sim e$ trivially from the definition.

To be thorough, though, we'll actually show that this congruence modulo H relation is an equivalence relation.

Proposition 5.11

Let $H \leq G$ be a subgroup. Then, congruence modulo H in G is an equivalence relation.

Proof. We'll check the three conditions for equivlaence relations one at a time.

1. (Reflexivity) We know $a \sim a$ for any $a \in G$ as $a = a * e$ and $e \in H$.
2. (Symmetry) If $x \sim y$ for $x, y \in G$, then $x = yh$ for some $h \in H$. But then $xh^{-1} = (yh)h^{-1} = y$, and as $h^{-1} \in H$, we get $y \sim x$.
3. (Transitivity) Suppose $x, y, z \in G$ satisfy $x \sim y$ and $y \sim z$. Then, $x^{-1}y, y^{-1}z \in H$, so the product $(x^{-1}y)(y^{-1}z) = x^{-1}z \in H$ as well, which means $x \sim z$.

The conclusion follows. □

5.3 Cosets

Let's investigate our equivalence classes a bit more. We just proved that congruence modulo H is indeed an equivalence relation, and we proved earlier that any equivalence relation induces a partition via its equivalence classes. We're going to call our equivalence classes a special name, the **coset**.

To be more explicit in the construction, start with some $g \in G$. Then, we have the equivalence class of g is

$$\begin{aligned}\overline{g} &= \{b \in G \mid b \sim g\} \\ &= \{b \in G \mid b = gh \text{ for all } h \in H\}.\end{aligned}$$

So $\overline{g}$ is obtained by multiplying g to every element in H. We will use a convenient shorthand notation for this: $gH := \overline{g}$.

Definition 5.12 (Left coset)**.** $g * H$ (usually the $*$ is omitted) is the **left coset** of g in H.

Remark 5.13. We specify "left" because our group G is not necessarily abelian, so the set $Hg = \{b \in G \mid b = hg \text{ for all } h \in H\}$ may be different from gH. For most of this class, though, we won't really care about this distinction, as long as we're consistent with the choice of our cosets (left or right).

Remark 5.14. The coset "represented by" the identity is simply $eH = H$, which is a (sub)group! And likewise, for any $h \in H$, $hH = H$. However, any other coset gH ($g \notin H$) is **not** a subgroup, as the identity doesn't exist in gH! (It also doesn't have closure of products or inverses in the general case.)

If this is hard to believe, test this out for congruence modulo n. In $\mathbb{Z}/5\mathbb{Z}$, the set of all integers congruent to 2 mod 5 does not form a subgroup of $\mathbb{Z}$, as $0 \notin 2 + 5\mathbb{Z}$. Furthermore, if $a, b \in 2 + 5\mathbb{Z}$, then $a + b \in 4 + 5\mathbb{Z} \neq 2 + 5\mathbb{Z}$, and $-a \in 3 + 5\mathbb{Z}$.

5.4 Proving Lagrange's Theorem

Now that we've set up all of our necessary language, we will go towards proving Lagrange's Theorem (Theorem 5.1).

We know that the equivalence classes modulo H partition set set G. We could write $G = \bigcup_{g \in G} gH$, but that would be unnecessarily repeating lots of cosets (we showed that if $g_2 \in g_1 H$, then $g_1 H = g_2 H$). So instead, we'll choose one representative for each distinct coset such that we can write G as a disjoint union:

$$G = \bigsqcup_{i \in I} g_i H.$$

Again, $\{g_i H \mid i \in I\}$ are the distinct left cosets.

Example 5.15 (Clarifying above with $\equiv \pmod 5$)

For congruence modulo 5, we can take the g_i's to be $0, 1, 2, 3, 4$.

We don't care too much about the choice of representatives; what we care about more is the number of distinct left cosets we have. This is exactly the cardinality of I, which we'll denote $[G : H]$.

Definition 5.16 (Index of H)**.** The **index** of a subgroup H in G is $[G : H] := |I|$, the number of elements in I, i.e. the number of distinct left cosets.

Example 5.17

As in the above example, we can take our distinct left cosets modulo n to be $\overline{0}$, $\overline{1}$, ..., $\overline{n-1}$, so $[\mathbb{Z} : n\mathbb{Z}] = n$.

Lagrange's Theorem will follow immediately from the following lemma:

Lemma 5.18

All left cosets of H in G have the same number of elements.

Proof. It suffices to show that any left coset has the same number of elements as H, as then we can have $|g_i H| = |H| = |g_j H|$ for any $g_i, g_j \in G$. We will define a map

$$\begin{aligned} f : H &\to gH \\ h &\mapsto gh. \end{aligned}$$

Consider the map

$$\begin{aligned} F : gH &\to H \\ z &\mapsto g^{-1} z. \end{aligned}$$

We have f is a bijection with inverse F, as $(f \circ F)(z) = f(g^{-1}z) = g(g^{-1}z) = z$ and likewise $(F \circ f)(h) = h$. Since f is a bijection, we muat hve $|H| = |gH|$, as desired. □

Well, each left coset has size $|H|$, and there are $[G : H]$ left cosets, and the left cosets form a partition of G, so we immediately get

Theorem 5.19 ("Counting formula")
For $H \leq G$ subgroup, $|G| = [G : H] \cdot |H|$.

In particular, since $[G : H]$ is an integer by definition, we get

Corollary 5.20 (Lagrange's Theorem)
$|H| \mid |G|$.

There are many, many applications of this theorem (try to prove Fermat's Little Theorem using Lagrange's!) but here's one application:

Corollary 5.21 (Order of element divides order of group)
If $a \in G$, then $|a| \mid |G|$.

Proof. We already know $\langle a \rangle \leq G$. We know $|a| = |\langle a \rangle|$. By Lagrange's, $|\langle a \rangle| \mid |G|$, and the result follows. □

6 09/21 - Quotient Groups

6.1 Groups of Prime Order

A big question in group theory is: Can we classify all groups of order n for any given n? A lot of the things we'll be doing in this class works towards classifying these groups as best as we can. To cap off our work from last time, we have our first big taste of what we can do with the following result.

Proposition 6.1
Every finite group of prime order is cyclic.

This, coupled with Theorem 4.1, tells us that any two groups of order p (where p is prime) are isomorphic. In other words, there is a **unique group of order** p *up to isomorphism.* (And even better, it's abelian!) This is pretty remarkable: we started with just the three group axioms, then specified the number of elements in our set, and somehow restricted ourselves to one group.

Proof. (of Proposition) Let G be a group with $|G| = p$ prime. Let $a \in G$ be a non-identity element, which must exist as $|G| = p \geq 2$. Note that as $a \neq e$, $|a| > 1$. We also know $\langle a \rangle$ is a subgroup with $|\langle a \rangle| = |a|$. By Lagrange's Theorem, we have $|a| = |\langle a \rangle|$ divides $|G| = p$, and as $|a| > 1$, it must follow $|a| = p$. But then $|\langle a \rangle| = p = |G|$, so $\langle a \rangle = G$ and G is cyclic. □

It seems a bit much, though, to think that we brought up the whole theory of left cosets and such *just* to prove Lagrange's Theorem. Luckily, our work has not been in vain. We'll try to take the set of left cosets of a given subgroup and attempt to give it a group structure, but this requires a bit of care.

6.2 Group Structure on Left Cosets

We are entering the notion of quotient groups. This is Section 3 in Dummit and Foote.

As a motivating example, consider the left cosets of $n\mathbb{Z} \subset \mathbb{Z}$. We talked about last time that the left cosets of $n\mathbb{Z}$ in $\mathbb{Z}$ are $\overline{0}, \overline{1}, \ldots, \overline{n-1}$ (recall $\overline{a} = a + n\mathbb{Z}$ is the set of all integers equivalent to $a \pmod{n}$). Note that these cosets partition $\mathbb{Z}$, and any other coset $\overline{a}$ is equal to one if these n cosets.

These left cosets form a group! We call this $\mathbb{Z}/n\mathbb{Z}$, where we define the operation $+$ as $\overline{a} + \overline{b} = \overline{a+b}$. One can check that this is well-defined, and it agrees with our usual notion of addition modulo n. (What is $12 + 27$ mod 7? What is $\overline{12} + \overline{27}$ in $\mathbb{Z}/n\mathbb{Z}$?)

> **Remark 6.2.** Note the name **quotient** group, and that the / indicates we're taking some kind of quotient. This is *not* coincidental at all – in fact, this is why the integers mod n are notated as such. Likewise, the pedagogically correct way of thinking about $\mathbb{Z}/n\mathbb{Z}$ is by thinking of its elements as equivalence classes, rather than as element representatives.

In general, we denote the set of left cosets by this quotienting symbol: for a subgroup $H \leq G$ in group G

$$G/H = \{gH \mid g \in G\}$$

is the set of left cosets of H. Here is our big question:

Can the left cosets of H in G form a group?

Well, in order for a set to be a group, we need a binary operation. Let's define it in the convenient way: $(g_1H) * (g_2H) = (g_1g_2)H$, where the $\underline{g_1g_2}$ uses the operation of G. This aligns with what we did for $\mathbb{Z}/n\mathbb{Z}$, as we defined $\overline{a} + \overline{b} = \overline{a+b}$.

Turns out that the answer to this question is not always. But there is a nice way to characterize the condition that will make the left cosets have a group structure.

6.3 Normal Subgroups

Definition 6.3 (Normal subgroups)**.** Let $N \leq G$. If $gN = Ng$ for all $g \in G$, then N is a **normal** subgroup of G. We write $N \trianglelefteq G$.

The Ng is the right coset of g in H (see Remark 5.13).

This condition may seem very arbitrary, but one can work carefully to show that this condition is exactly what we need to make sure G/H is a group. Maybe this will be covered in section? But believe us for now.

Example 6.4 ($n\mathbb{Z}$ is normal)

$n\mathbb{Z}$ is a normal subgroup of $\mathbb{Z}$. Likewise, the quotient $\mathbb{Z}/n\mathbb{Z}$ is a group, as we know very well.

Fact 6.5. This comes for free from the definition: every subgroup of an abelian group is normal. Another that comes for free: the center $Z(G) \trianglelefteq G$.

Exercise 6.6. Hopefully harmless: show $\{e\} \trianglelefteq G$ and $G \trianglelefteq G$. (Work through the definition.)

We have a few examples of normal subgroups here, but an equally enlightening way of illustrating a concept is through non-examples.

Example 6.7 (Non-example of normal subgroup)

Let $G = D_8$ and s be some reflection. Is $\langle s \rangle = \{e, s\}$ a normal subgroup? We have

$$\begin{aligned} r\langle s \rangle &= \{rs, r\} \\ \langle s \rangle r &= \{sr, r\}, \end{aligned}$$

but as we know $rs = sr^{-1} \neq sr$, these two cosets are not the same, so $\langle s \rangle$ is not normal.

Although it is nice that this normality condition completely encapsulates what we need for G/H to be a group, the downshot is that from our definition alone, it's hard to verify that a subgroup is normal. We'll try to rectify this a little with the following:

Theorem 6.8

$H \trianglelefteq G$ iff $\forall\, h \in H$ and $\forall\, g \in G$, $ghg^{-1} \in H$.

Remark 6.9. Going from h to ghg^{-1} is called **conjugation** by g. This is a concept that will come up again.

Proof. We show implication in both directions. First, assume $H \trianglelefteq G$. Let $h \in H$ and $g \in G$. We want to show $ghg^{-1} \in H$. By normality of H, we know $gH = Hg$, so $gh = h'g$ for some $h' \in H$. Then,

$$(gh)g^{-1} = (h'g)g^{-1} = h' \in H.$$

For the other direction, suppose conjugation on an element in H always stays in H. Let $g \in G$. We want to show $gH = Hg$. We will do this by showing inclusion in both directions. Let $a \in gH$, so $a = g \cdot b$ for some $b \in H$. Then, we can write

$$a = gb = (gbg^{-1})g \in Hg$$

since $gbg^{-1} \in H$ by our assumption. Thus, $gH \subseteq Hg$. Showing the reverse inclusion ($Hg \subseteq gH$) follows a similar argument. □

Just like how we can take any subset of G and construct its centralizer, we can take any subset and construct its *normalizer*. This serves as a natural generalization of our notion of the normal subgroup.

Definition 6.10 (Normalizer)**.** Let $A \subseteq G$. The **normalizer** of A in G is $N_G(A) = \{g \in G \mid gA = Ag\}$.

Fact 6.11. $N \trianglelefteq G \iff N_G(N) = G$. (Convince yourself that this is really an equivalent formulation of the normality condition!)

Example 6.12 ($\mathrm{SL}_n(\mathbb{R}) \trianglelefteq \mathrm{GL}_n(\mathbb{R})$)

Let $G = \mathrm{GL}_n(\mathbb{R})$ and $H = \mathrm{SL}_n(\mathbb{R}) \leq G$. We can check that $H \trianglelefteq G$. Let $A \in \mathrm{SL}_n(\mathbb{R})$ and $B \in \mathrm{GL}_n(\mathbb{R})$. Then,

$$\det(BAB^{-1}) = \det(B)\det(A)\det(B)^{-1} = \det(A) = 1,$$

so $BAB^{-1} \in \mathrm{SL}_n(\mathbb{R})$ and thus $H \trianglelefteq G$. We can also show that $|G/H| = [G : H] = \infty$, as for any $A \in G$, the left coset of A in H contains only matrices of determinant $\det(A)$. Thus, for every nonzero $r \in \mathbb{R}$, we need at least one left coset whose elements are all matrices of determinant r. As $|\mathbb{R}| = \infty$, $[G : H] = \infty$ as well.

Remark 6.13 (Normal subgroups as homomorphism kernel)**.** This also plays on Problem 5 of PSet 2. Consider the homomorphism $\varphi : \mathrm{GL}_n(\mathbb{R}) \to (\mathbb{R} \setminus \{0\}, \times)$ where $A \mapsto \det A$. We've established in the very beginning of class that this is indeed a group homomorphism. The kernel is the set of all matrices with determinant 1, i.e. exactly $\mathrm{SL}_n(\mathbb{R})$. And this subgroup is normal! So we have this interplay between a normal subgroup and the kernel of a homomorphism. We will see that this is true in the general case next week.

One more example for normal subgroups (there is no such thing as too many examples!).

Example 6.14 (Subgroup of rotations is normal)

Consider $\langle r\rangle \le D_8$. We will first show that for any $g \in D_8$, $grg^{-1} \in \langle r\rangle$. When $g \in \langle r\rangle$, then as $\langle r\rangle$ is abelian, this is clearly the case (in fact, then $grg^{-1} = r$). Now suppose $g = s$. Note that $s^2 = e \implies s = s^{-1}$, so $srs^{-1} = srs = (r^{-1}s)s = r^{-1} \in \langle r\rangle$.

In the more general case when $g = r^j s$, we want to show $(r^j s)r(r^j s)^{-1} \in \langle r\rangle$. One can verify that $(r^j s)^{-1} = s^{-1}r^{-j} = sr^{-j}$ (in general, $(ab)^{-1} = b^{-1}a^{-1}$), so

$$(r^j s)r(r^j s)^{-1} = r^j srsr^{-j} = r^j r^{-1}r^{-j} = r^{-1},$$

where in the third equality, we use the fact that $srs = r^{-1}$ from above. Thus, $grg^{-1} \in \langle r\rangle$ for any $g \in D_8$.

Furthermore, our work here immediately gives us the case for any r^j. One can show via induction (or "expanding it out") that if $grg^{-1} \in \langle r\rangle$, then $(grg^{-1})^j = gr^j g^{-1} \in \langle r\rangle$ as well. This means $\langle r\rangle \trianglelefteq D_8$.

Let's explore this a little bit more. What are the left cosets of $\langle r\rangle$? We have $\langle r\rangle$ itself, and then we can consider $s\langle r\rangle = \{s, sr, sr^2, sr^3\}$. Note that $\langle r\rangle \cup s\langle r\rangle = D_8$ and the two cosets are disjoint, so these are the only two left cosets. In particular, we have $|D_8 : \langle r\rangle| = 2$. We already established that $\langle r\rangle$ is normal, but we can obtain the same result given $|D_8 : \langle r\rangle| = 2$ via the following result:

Theorem 6.15 (Subgroup of index 2 is normal)

If $H \le G$ such that $[G : H] = 2$, then $H \trianglelefteq G$.

Proof. Let $g \in G$. We want to show $gH = Hg$. If $g \in H$, then $gH = H = Hg$. If $g \notin H$, then $H \ne gH$; more strongly, $H \cap gH = \emptyset$. Likewise, $g \notin H \implies H \ne Hg$, so $H \cap Hg = \emptyset$. But since $[G : H] = 2$, we must have $G = H \sqcup gH = H \sqcup Hg$ which implies $gH = Hg$. (Intuitively, $[G : H] = 2$ means we only have one other coset besides H, but we have two cosets gH and Hg, so they must be the same coset.) □

6.4 Normality is What We Want

I've kept claiming that normality is exactly the condition that guarantees G/H has a group structure, but now we'll work through the details.

Proposition 6.16

If $N \trianglelefteq G$, then G/N is a group with the operation $*$ such that $(aN) * (bN) = (ab)N$.

Proof. This requires us to first show that $*$ is indeed a well-defined binary operation. Again, we have $*$ is a binary operation $G/N \times G/N \to G/N$ where $(aN, bN) \mapsto (ab)N$. We need to make sure this is well-defined, i.e. if $aN = cN$ and $bN = dN$, then $(ab)N = (cd)N$ (the output is not dependent on our choice of representative). This is for sure the hardest part of establishing that G/N is a group (and where the normality of N comes into play), so I'm going to save this for last and assume that this operation is well-defined for now.

Associativity of our operation on left cosets follow from associativity in G, as $(aN * bN) * cN = (ab)cN = a(bc)N = aN * (bN * cN)$. The identity coset is $eN = N$, and the inverse of gN is $g^{-1}N$ (check this!).

Now we show that $*$ is well-defined. We will prove this in two ways: the more conventional way, and the one Myrto was alluding to in class.

Proof 1: Suppose $aN = cN$ and $bN = dN$. We wish to show that $(ab)N = (cd)N$. This requires a lemma that allows us to work with this equality between cosets:

Lemma 6.17 (Condition for when cosets are equivalent)
$aN = cN \iff c \in aN$.

Proof. First, suppose $aN = cN$. Then, as $e \in N$, we have $ce = c \in cN = aN$. For the reverse implication, suppose $c \in aN$. Then, $c = an$ for some $n \in N$. We wish to show that $aN = (an)N$.

This we can do by showing inclusion in both directions. Take any $an' \in aN$ ($n' \in N$). We have $n, n' \in N \implies n^{-1}n' \in N$, so $an' = (an)(n^{-1}n') \in (an)N$. For the reverse inclusion, again take any $(an)n' \in (an)N$ ($n' \in N$). By closure of products in subgroups, $nn' \in N$, so $(an)n' = a(nn') \in aN$. □

Returning back to proving well-definedness, we now wish to show $(ab)N = (cd)N$. By the lemma, it suffices to show that $cd \in (ab)N$. But from $aN = cN$ and $bN = dN$, the lemma tells us that $c \in aN$, $d \in bN$, i.e. $\exists\, n_1, n_2 \in N$ such that $c = an_1$, $d = bn_2$. Then, $cd = (an_1)(bn_2) = a(n_1b)n_2$. Normality of N tells us that $Nb = bN$, so $\exists\, n_3 \in N$ such that $n_1b = bn_3$. This gives us

$$cd = a(n_1b)n_2 = a(bn_3)n_2 = (ab)(n_3n_2) \in (ab)N,$$

as desired.

Proof 2: We can bypass the concern on choosing a representative by defining the $*$ without any representative! Given sets A and B, we will define $A \cdot B := \{ab \mid a \in A, b \in B\}$. We claim that our operation is equivalent to this "product" between sets. It suffices to show that $aN \cdot bN = (ab)N$.

We will show inclusion in both directions. Any element in aN can be expressed as an_1 for $n_1 \in N$, and likewise bn_2 for bN ($n_2 \in N$). Their product is $(an_1)(bn_2) = a(n_1b)n_2$. By normality of N, $Nb = bN$, so $n_1b = bn_3$ for some $n_3 \in N$, which means our product is $a(bn_3)n_2 = (ab)(n_3n_2)$. Since N is a subgroup, $n_3n_2 \in N$, so $(an_1)(bn_2) \in (ab)N$.

The reverse inclusion is more straightforward: any element in $(ab)N$ can be expressed as $(ab)n$ for some $n \in N$, but we can rewrite that as $(ae)(bn)$. $e \in N$ since N is a subgroup, so $(ae)(bn) \in aN \cdot bN$. Thus, $aN \cdot bN = (ab)N$, and as this set "product" is well-defined, so is our operation $*$ on left cosets. □

Remark 6.18. The proof for showing our operation is well-defined is admittedly a bit clunky. It is enlightening in the sense that it shows you exactly when and why our normality condition is necessary to make sure G/N is a group, but if you're getting bogged down by the details, just taking well-definedness for granted and moving on won't hurt for the time being.

Exercise 6.19 (Sanity check)**.** What is the order (number of elements) of the group G/N? Do we have notation for this already?

7 Week of 09/26 - Isomorphism Theorems

7.1 Statement of Theorems

Professor Mavraki was at a conference for Arithmetic Geometry in Heidelberg, so she prerecorded these lectures. I never got around to transcribing the lectures, but for completeness, I will state the isomorphism theorems here. A Google search of "Group Isomorphism Theorems" will produce plenty of good resources explaining and proving these theorems.

Theorem 7.1 (First Isomorphism Theorem)

If $\varphi : G \to H$ is a group homomorphism, then $\ker\varphi \trianglelefteq G$ and $G/\ker\varphi \simeq \operatorname{Im}\varphi$.

Theorem 7.2 (Third Isomorphism Theorem)

Suppose $K \subseteq H \subseteq G$ and $K \trianglelefteq G$, $H \trianglelefteq G$. Then, $K \trianglelefteq H$, $H/K \trianglelefteq G/K$, and

$$G/K \Big/ H/K \simeq G/H.$$

Example 7.3

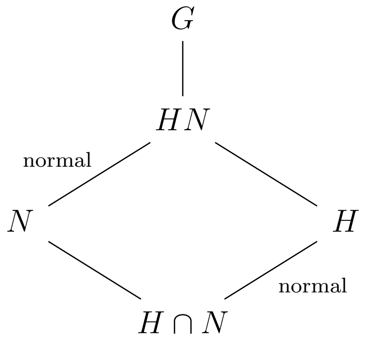
We have $4\mathbb{Z}, 2\mathbb{Z}$ are both normal subgroups of $\mathbb{Z}$. (Reminder that any subgroup of an abelian group is normal.) One can work through that $\mathbb{Z}/2\mathbb{Z} \simeq (\mathbb{Z}/4\mathbb{Z})/(2\mathbb{Z}/4\mathbb{Z})$.

Theorem 7.4 (Second Isomorphism Theorem)

Let G be a group, $H \subseteq G$ a subgroup and $N \trianglelefteq G$ a normal subgroup. Then, (a) $HN \subseteq G$ is a subgroup, (b) $N \trianglelefteq HN$ is a normal subgroup, (c) $H \cap N \trianglelefteq H$ is a normal subgroup, and (d) we have an isomorphism of quotient groups

$$HN/N \simeq (H \cap N)/H.$$

As a diagram, we have the following inclusion of groups. The Second Isomorphism Theorem, also known as the *Diamond Theorem* because of the diamond below, states that the two quotient groups obtained from the two normal subgroup inclusions in the diamond are isomorphic.



8 10/03 - Group Actions

This is, in my opinion, the pedagogically correct way of thinking about groups. We'll give a motivating example. Consider D_{10}, the dihedral group of order 10. We always described of this group as the *symmetries of the pentagon*. This is kind of vague, though. What are the symmetries?

If you go back to the diagrams in Example 1.4, you may notice that this question actually pokes at something extremely subtle. It's easiest in the beginning to simply describe the elements of D_{10} as the different configurations of the pentagon, which is what we did in class, but this makes no sense. How do we combine two configurations under an operation?

What we're actually doing is we're taking the **actions** as elements. The rotation r is not the pentagon itself with relabeled vertices, but it is the *action* itself. This is weird, because if we think of the elements of our group as nouns, then we're taking these actions (rotating, reflecting), which are a priori verbs, and then treating them as nouns.

If this explanation was a bit esoteric, here's another perspective. Consider D_{10} as a subset of S_5 instead, so remove D_{10} from its geometric interpretation. Now, since S_5 is the group of permutations on $\{1, 2, 3, 4, 5\}$, we have that D_{10} is acting on the set with just more restrictions.

In any case, we can understand a group better by looking at how it (inter)acts with a set A.

Definition 8.1 (Group action)**.** Let G be a group and A a set. A **group action of G on A** is a map

$$\begin{aligned} \varphi : G \times A &\to A \\ (g, a) &\mapsto \varphi(g, a) \in A \end{aligned}$$

such that

> 1. (Associativity) $\varphi(g_1, \varphi(g_2, a)) = \varphi(g_1 g_2, a)$
> 2. (Identity) $\varphi(e, a) = a$ for all $a \in A$.
>
> We say that A is a **G-space** if there exists an action of G on A. The action is written $G \curvearrowright A$.

Let's break down these axioms a little bit more. The first axiom basically encapsulates associativity! For notational convenience, we will denote group actions using the $\cdot$ multiplication sign, so $g \cdot a := \varphi(g, a)$. The first axiom is telling us

$$g_1 \cdot (g_2 \cdot a) = (g_1 * g_2) \cdot a.$$

(This looks sort of similar to how scalar multiplication works on vector spaces, if you're familiar with them.)

The second axiom encapsulates the identity action, which naturally is associated with the identity element. Using the $\cdot$ notation, this means that $e \cdot a = a$ for all $a \in A$. Seems reasonable enough.

It's important to remember though that A need not be a group! In the case of S_n, the permutations are acting on the set $\{1, 2, \dots, n\}$, which is not a group (we haven't even defined an operation on this set).

> **Exercise 8.2.** Convince yourself that the following is true: the binary operation in a group G is a group action in disguise, where G is acting on itself. (Consequently, one can see that group actions is a more powerful and general formulation of how we've dealt with groups thus far.)

Example 8.3 (Conjugation is a group action)

From above, we have that multiplication in a group is a group action, where the group is acting on itself. But there can be many group actions for a given group and set! Conjugation is another example of an action $G \curvearrowright G$. We define the action via

$$\begin{aligned} \varphi : G \times G &\to G \\ (g, a) &\mapsto gag^{-1}. \end{aligned}$$

Checking that this is indeed a group action is just a matter of checking the two axioms. For associativity, $\varphi(g_1, \varphi(g_2, a)) = \varphi(g_1, g_2 a g_2^{-1}) = g_1(g_2 a g_2^{-1}) g_1^{-1} = g_1 g_2 a (g_1 g_2)^{-1} = \varphi(g_1 g_2, a)$, whew. For identity, $\varphi(e, a) = eae^{-1} = a$, easy.

Example 8.4 (Symmetric group acts on $\{1, 2, \dots, n\}$)

Thinking of S_n as the group of permutations acting on $A := \{1, 2, \dots, n\}$, we have (literally in the name) that $S_n \curvearrowright \{1, 2, \ldots, n\}$. The action is defined

$$\begin{aligned} \varphi : S_n \times A &\to A \\ (\sigma, i) &\mapsto \sigma(i). \end{aligned}$$

We check that this satisfies both axioms. The easier one is the identity: letting id be the identity permutation, we have $\mathrm{id} \cdot i = \mathrm{id}(i) = i$. For associativity, we have the following equalities: $\varphi(\sigma_1 \varphi(\sigma_2, i)) = \sigma_1 \cdot (\sigma_2(i)) = \sigma_1(\sigma_2(i))$ and $\varphi(\sigma_1 \circ \sigma_2, i) = (\sigma_1 \circ \sigma_2)(i) = \sigma_1(\sigma_2(i))$, so they must be equal.

Example 8.5 ($\mathrm{GL}_n(\mathbb{R})$ acts on $\mathbb{R}^n$)
We have an action $\mathrm{GL}_n(\mathbb{R}) \curvearrowright \mathbb{R}^n$ where the map $\mathrm{GL}_n(\mathbb{R}) \times \mathbb{R}^n \to \mathbb{R}^n$ maps $(M, \vec{v}) \mapsto M\vec{v}$. Check that this is a valid group action!

8.1 Stabilizers

As we now allow groups to not only interact with itself, but also with sets in general, some interesting mathematical plays arise. To discuss this, we're going to introduce some more definitions.

Definition 8.6 (Kernel of a group action)**.** The **kernel** of an action $\varphi : G \times A \to A$ defined to be the set of group elements of the group G that fix all the elements of A under the considered action φ:

$$\ker \varphi = \{g \in G \mid g \cdot a = a \, \forall \, a \in A\}.$$

A slightly weaker notion only requires fixing a specified element in our set.

Definition 8.7 (Stabilizer)**.** Given an element $a \in A$, the **stabilizer** of a is the set of all group elements which fix a under the group action:

$$\mathrm{Stab}(a) := \{g \in G \mid \varphi(g, a) = a\}.$$

Exercise 8.8. Check the following are true (this follows from the definition):

- $\ker \leq \mathrm{Stab}(a)$,
- $\ker \varphi = \bigcap_{a \in A} \mathrm{Stab}(a)$.

It would be nice if $\mathrm{Stab}(a)$ and $\ker \varphi$ were more than just sets. Lucky for us, they inherit a (sub)group structure:

Lemma 8.9 (Stabilizer and Kernel are subgroups)
The stabilizer of $a \in A$ is a subgroup of G. Likewise, the kernel of a group action is also a subgroup.

Proof. First, as $e \cdot a = a$, $e \in \operatorname{Stab}(a)$. It is closed under inverses: if $g \in \operatorname{Stab}(a)$, then $g \cdot a = a$, so then we have $a = (g^{-1} * g) \cdot a = g^{-1} \cdot (g \cdot a) = g^{-1} \cdot a$, voila. It is also closed under products: if $g_1, g_2 \in \operatorname{Stab}(a)$, then $g_1 \cdot a = g_2 \cdot a = a$, so $(g_1 * g_2) \cdot a = g_1 \cdot (g_2 \cdot a) = g_1 \cdot a = a$.

Proving the kernel is a subgroup can be done directly in a similar fashion to the above, or one can take Claim 4.5 (intersection of subgroups is a subgroup) and get the result immediately. □

Definition 8.10 (Faithful action)**.** If $\ker \varphi = \{e\}$, then we say that the action is **faithful**.

8.2 Orbits

Very closely linked to the notion of stabilizers is the notion of orbits. This is kind of the opposite of the stabilizer: whereas the stabilizer of an element keeps only that which fixes it, the orbit encapsulates all the different "places" a group action can send our element.

Definition 8.11 (Orbit)**.** For an element $a \in A$, the **orbit** of a under an action $G \curvearrowright A$ is

$$\mathcal{O}(a) = \{g \cdot a \mid g \in G\}.$$

Note that since $g \cdot a \in A$, $\mathcal{O}(a) \subseteq A$.

Exercise 8.12. (Review) The stabilizer and orbit both take in an element of the set as its argument, say $a \in A$. $\operatorname{Stab}(a)$ and $\mathcal{O}(a)$ are both sets. Where do they live? In G or in A?

Definition 8.13 (Transitive action)**.** An action is **transitive** if the entire set is the orbit of some element, i.e. for some $a \in A$, $A = \mathcal{O}(a)$. Equivalently, if $b \in A$, then $b = g \cdot a$ for some $g \in G$.

8.3 Gaining Familiarity with Actions

We'll use the conjugation action as our case study to review everything that's been going on. Reminder that conjugation is a group action $G \curvearrowright G$ where $g \cdot a = gag^{-1}$.

Fix some $a \in G$. Then, we have

$$\begin{aligned}\operatorname{Stab}(a) &= \{g \in G \mid g \cdot a = a\} \\ &= \{g \in G \mid gag^{-1} = a\} \\ &= \{g \in G \mid ga = ag\} \\ &= C_G(a).\end{aligned}$$

One can also show that

$$\ker\varphi = \bigcap_{a \in G} \operatorname{Stab}(a) = \bigcap_{a \in G} C_G(a) = Z(G),$$

the center of our group G. Aha, so it turns out that the center/centralizer is not totally out of the blue, it just took some time to justify where they came from.

When is the conjugation action faithful? Recall that an action is faithful if $\ker\varphi = \{e\}$, so it is faithful iff $Z(G) = \{e\}$. Thus, from one of the psets, we know that the action is faithful in the group D_{10}.

Finally, we'll see what the orbits look like under this action. For some $a \in G$, we have

$$\mathcal{O}(a) = \{g \cdot a \mid g \in G\} = \{gag^{-1} \mid g \in G\}.$$

We call this the **conjugacy class** of a. This will show up again in full force in a few weeks!

Example 8.14 (Exercises via conjugation)

Summarizing, we have the following for our conjugation action. For everything below, we fix some $a \in G$.

- $\operatorname{Stab}(a) = C_G(a)$
- $\ker\varphi = Z(G)$
- The action is faithful iff $Z(G) = \{e\}$
- $\mathcal{O}(a)$ is the conjugacy class of a

Example 8.15 (Transitive action)

Consider the action $S_3 \curvearrowright \{1, 2, 3\}$ where $\sigma \cdot i := \sigma(i)$. This action is transitive, as $\mathcal{O}(1) = \{\sigma(1) \mid \sigma \in S_3\} = \{1, 2, 3\}$. (If you don't believe, for every $i \in \{1, 2, 3\}$, find a $\sigma \in S_3$ such that $\sigma(1) = i$.)

As an addendum, note that $\ker\varphi = \{\sigma \in S_3 \mid \sigma(i) = i\,\forall\, i \in \{1, 2, 3\}\} = \{\mathrm{id}\}$, so the action is also faithful!

8.4 Cayley's Theorem

Sometimes when a specific mathematical object seems a bit unmotivated, it's enlightening to see how and why the object was first constructed. The story with groups is pretty simple.

The first examples of groups were symmetric groups only, and they were dealt with very tangibly (e.g. using matrices). It was only until later when some dudes were like "wait we can make this stuff a lot more general, so we can apply our knowledge of permutation groups in other contexts." This process of abstraction has transformed our knowledge of group theory into the material that we've been covering in this class.

So it seems like through abstraction, we've uncovered so many "new groups," or in general new information about groups that we couldn't have gleaned just by studying the symmetry groups. But is this really the case? This is where the story takes a surprising turn.

Theorem 8.16 (Cayley's Theorem)
Let G be a finite group with order n. Then, G is isomorphic to a subgroup of S_n.

This result tells us that although the abstraction is useful for having a precise language when discussing groups, it turns out that everything we need in group theory lies in the symmetry groups.[1] This may seem shocking, but it actually shouldn't: we already knew that groups were objects designed to encapsulate symmetries. So it makes perfect sense that any group must be a subgroup of a symmetric group, since it encapsulates particular symmetries of a set.

The following is a very nice way of thinking about group actions. In fact, this perspective – seeing group actions as bijections on your set that somehow respect the group structure – is the starting point of representation theory.

Lemma 8.17
We have a bijection between the group actions $\varphi : G \times A \to A$ and the set of of group homomorphisms $\psi : G \to S_A$, where we define

$$S_A := \{\tau : A \to A \mid \tau \text{ bijection}\}.$$

Proof. We will provide constructions in both directions. First, let $\varphi : G \times A \to A$ be a group action of G on A. Denote $\varphi_g : A \to A$ as the map sending $a \mapsto g \cdot a \in A$. Note that φ_g is a bijection, since $\varphi_{g^{-1}} \circ \varphi_g(a) = g^{-1} \cdot (g \cdot a) = a$. Thus, we can consider the map $\psi : G \to S_A$ given by $g \mapsto \varphi_g$. A priori it is not a group homomorphism, just a map between sets. Yet it is clear from the group action properties that $\varphi_g \circ \varphi_h = \varphi_{gh}$, so ψ is indeed a group homomorphism.

The other direction, I am now realizing, is covered at the beginning of the next lecture, so I invite the reader to go to the (bottom of the) next page! □

To close out this lecture, we will prove Cayley's Theorem very quickly:

Proof. Let G be a finite group, and consider the action $G \curvearrowright G$ of left multiplication. We have a group homomorphism $\psi : G \to S_G \simeq S_{|G|}$. It suffices to show ψ is injective. But this

[1] At least, for finite groups.

is clear from the group action given by left multiplication: if $g \cdot x = h \cdot x$ for any (let alone all) $x \in G$, then $g = h$ by existence of inverses. Hence, ψ is injective, so G embeds into $S_{|G|}$ as a subgroup. □

9 10/05 - Powerful Applications of Group Actions

9.1 More with Group Actions

We'll practice a bit with faithful and transitive actions. For each example, we'll determine whether it is a group action, and if it is, whether it is faithful and/or transitive.

> **Exercise 9.1.** Let $G = (\mathbb{Z}, +)$ and $A = \mathbb{Z}$. 1) Our group action $G \curvearrowright A$ is defined by $g \cdot a := g + a$. 2) Define $g \cdot a := ga$ (multiplication).

Example 9.2

Let $G = (\mathbb{Z}, +)$ and $A = \mathbb{Z}$, and our group action $G \curvearrowright A$ is defined by $g \cdot a := g + a$. The action by 0 is the identity, and associativity follows from associativity of addition. It is faithful, since 0 is the only integer n such that $n \cdot a := n + a = a$. It is also transitive, as $\mathcal{O}(0) = \mathbb{Z}$.

If we take the same group and set but define $G \curvearrowright A$ via $g \cdot a := g \cdot a$, then this is no longer an action as 0 is the identity of $G = (\mathbb{Z}, +)$ but the action by 0 does not preserve the element, i.e. $0 \cdot x = 0x = 0 \neq x$ for $x \neq 0$.

Last time, we stated a bijection

$$\{\text{group actions } \varphi : G \times A \to A\} \leftrightarrow \{\text{group hom } \psi : G \to S_A\}.$$

Recall $S_A = \{\tau : A \to A \mid \tau \text{ bijective}\}$. Let's define the bijection in both directions.

First, start with a group action $\varphi : G \times A \to A$. We can define a corresponding $\psi : G \to S_A$ where $\psi(g) = \sigma_g : A \to A$ is defined as $\sigma_g(a) := \varphi(g, a)$. One can check that σ_g is a bijection from $A \to A$, and ψ is a group homomorphism.

In the reverse direction, start with some group homomorphism $\psi : G \to S_A$. We can construct a corresponding group action $\varphi : G \times A \to A$ where $\varphi(g, a) := \psi(g)(a)$. We can quickly check that this is a group action. First, $e \cdot a = \psi(e)(a) = \mathrm{id}_{S_A}(a) = a$. Associativity comes from

$$\begin{aligned} g_1 \cdot (g_2 \cdot a) &= g_1 \cdot (\psi(g_2)(a)) = \psi(g_1)(\psi(g_2)(a)) \\ &= (\psi(g_1) \circ \psi(g_2))(a) = \psi(g_1 g_2)(a) \\ &= (g_1 g_2) \cdot a, \end{aligned}$$

where the second-to-last equality follows from ψ being a group homomorphism.

9.2 Orbit-Stabilizer Theorem

After developing all of this stuff about orbits, stabilizers, etc. it would be a shame if the only thing we did with them was prove Cayley's Theorem. Lucky for us, there is a lot more at store.

Here's the statement of the Orbit-Stabilizer Theorem. Recall that $[G : H]$ is the **index** of H, i.e. the number of cosets of H in G.

Theorem 9.3 (Orbit-Stabilizer Theorem)
If $G \curvearrowright A$ and $a \in A$, then $|\mathcal{O}(a)| = [G : \operatorname{Stab}(a)]$. Equivalently, for finite G,

$$|\mathcal{O}(a)| \cdot |\operatorname{Stab}(a)| = |G|.$$

> **Exercise 9.4.** Use the counting formula to show that $|\mathcal{O}(a)| = [G : \operatorname{Stab}(a)]$ and $|\mathcal{O}(a)| \cdot |\operatorname{Stab}(a)| = |G|$ are equivalent for finite G. Note that the former equation is true even for G infinite!

Proof. If we wish to show that $|\mathcal{O}(a)| = [G : \operatorname{Stab}(a)]$, it suffices to construct a bijection between $\mathcal{O}(a)$ (a set) and the set of cosets of $\operatorname{Stab}(a)$ in G. Denote $G/\operatorname{Stab}(a)$ as the set of left cosets of $\operatorname{Stab}(a)$ in G (note that this is *not* necessarily a group, as $\operatorname{Stab}(a)$ is not necessarily normal). We define a bijection

$$\begin{aligned} f : \mathcal{O}(a) &\to G/\operatorname{Stab}(a) \\ g \cdot a &\mapsto g \cdot \operatorname{Stab}(a). \end{aligned}$$

We first need to verify that f is well-defined. Let $g_1, g_2 \in G$ and $a \in A$, and suppose $g_1 \cdot a = g_2 \cdot a$. We want to show that $g_1 \operatorname{Stab}(a) := f(g_1 \cdot a) = f(g_2 \cdot a) =: g_2 \operatorname{Stab}(a)$. Taking the action of g_1^{-1} on both sides, we have

$$\begin{aligned} a = e \cdot a &= (g_1^{-1} g_1)(a) \\ &= g_1^{-1} \cdot (g_1 \cdot a) = g_1^{-1} \cdot (g_2 \cdot a) \\ &= (g_1^{-1} g_2) \cdot a, \end{aligned}$$

so $g_1^{-1} g_2 \in \operatorname{Stab}(a)$, which means $g_2 \in g_1 \operatorname{Stab}(a)$. Using Lemma 6.17, this tells us that $g_1 \operatorname{Stab}(a) = g_2 \operatorname{Stab}(a)$ as desired.

Now we show that f is a bijection. First, we prove injectivity: suppose $f(g_1 \cdot a) = f(g_2 \cdot a)$. By definition, $g_1 \operatorname{Stab}(a) = g_2 \operatorname{Stab}(a)$, so $g_1^{-1} g_2 \in \operatorname{Stab}(a)$, so $(g_1^{-1} g_2) \cdot a = a$. Taking the action of g_1 on both sides and exploiting associativity, we get $g_2 \cdot a = g_1 \cdot a$. For surjectivity, given any $g \cdot \operatorname{Stab}(a) \in G/\operatorname{Stab}(a)$, we have $f(g \cdot a) = g \cdot \operatorname{Stab}(a)$, simple enough. □

9.3 Actions Induce Equivalence Relations

We mentioned before (when proving Lagrange's Theorem) that an equivalence relation gives a partition via its equivalence classes. Conversely, we also saw that a partition induces an equivalence relation: say any two elements are equivalent if they belong in the same subset in the partition. (Check that this is actually an equivalence relation!) It turns out that we can also induce equivalence relations from group actions, which is super neat, because then we can jump from group actions, to equivalence relations, to partitions, which gives us insightful information on the elements of a group.

In particular, we will see that there's a convenient way of partitioning a group via special equivalence classes. This is useful because although counting the number of elements in a group may be difficult, it'll be easier to count the number of elements in each equivalence class, so then we can just add up the sizes of each class to get the order of the group.

We start with a group action $G \curvearrowright A$. We induce an equivalence relation A where $a \sim b$ iff $a \in \mathcal{O}(b)$. We check the equivalence relation axioms:

- Reflexive: since $a \in \mathcal{O}(a)$ (as $e \cdot a = a$), $a \sim a$
- Symmetric: $a \sim b \implies b \sim a$ as if $a \in \mathcal{O}(b)$, then $a = g \cdot b$ for some $g \in G$, which means $g^{-1} \cdot a = g^{-1} \cdot (g \cdot b) = (g^{-1}g) \cdot b = b$.
- Transitive: if $a \sim b$ ($a = g_1 \cdot b$ for some $g_1 \in G$) and $b \sim c$ ($b = g_2 \cdot c$ for some $g_2 \in G$), then $a = g_1 \cdot (g_2 \cdot c) = (g_1 g_2) \cdot c \in \mathcal{O}(c)$, so $a \sim c$.

Well, we mentioned that equivalence classes form a partition on our set. Take any $a \in A$. Then, the equivalence class of a, denote $\overline{a}$, is by definition $\{b \in A \mid b \in \mathcal{O}(a)\} = \mathcal{O}(a)$. So the equivalence classes are just the orbits of the set elements!

Using more of our knowledge about equivalence classes and partitions, these equivalence classes must partition our set A. In other words, we can take some subset of representatives $\{a_i \mid i \in I\}$ (I is our indexed set) such that

$$A = \bigsqcup_{i \in I} \mathcal{O}(a_i).$$

Taking the cardinality on both sides,

$$|A| = \sum_{i \in I} |\mathcal{O}(a_i)|. \tag{1}$$

So somehow, we're able to count the number of elements in our set by looking at the distinct orbits. This becomes even nicer when we take A to be the group G itself and our action $G \curvearrowright G$ to be the conjugation action. (Recall for $g \in G$, $a \in G = A$, $g \cdot a := gag^{-1}$.) This is the premise of the next section.

9.4 Class Equation

The following (admittedly intimidating) result is a direct consequence of our above equation. By conjugacy class, we mean the equivalence class induced by the conjugation action; explicitly, the conjugacy class of $a \in G$ is $\{gag^{-1} \mid g \in G\}$.

Theorem 9.5 (Class Equation)

Let $G \curvearrowright G$ be the conjugation action, and suppose G is finite. Assume that the distinct conjugacy classes of G disjoint from $Z(G)$ are $C_1, \ldots, C_n$, and a_i is some element in C_i for every $1 \leq i \leq n$. Then,

$$|G| = |Z(G)| + \sum_{i=1}^{n} [G : C_G(a_i)],$$

where $C_G(a_i)$ is the centralizer and $Z(G)$ is the center.

Proof. Recall that for $g \in G$, $a \in G = A$, the conjugation action is defined as $g \cdot a := gag^{-1}$. We saw that any action induces an equivalence relation, and the equivalence classes are simply the orbits of the group elements. Thus, the conjugacy classes are of the form $\mathcal{O}(a) = \{gag^{-1} \mid g \in G\}$. Applying this to Equation (1), we have

$$|G| = \sum_{i=1}^{m} |\mathcal{O}(a_i)|,$$

where $\mathcal{O}(a_i)$ $(1 \leq i \leq m)$ are the distinct conjugacy classes, i.e. distinct orbits. But we know an equivalent expression of $|\mathcal{O}(a_i)|$ by the Orbit-Stabilizer Theorem! So we can rewrite

$$|G| = \sum_{i=1}^{m} [G : \mathrm{Stab}(a_i)].$$

But for conjugation,

$$\begin{aligned} \mathrm{Stab}(a) &= \{g \in G \mid g \cdot a = a\} \\ &= \{g \in G \mid gag^{-1} = a\} \\ &= C_G(a), \end{aligned}$$

so $[G : \mathrm{Stab}(a)] = [G : C_G(a)]$. Let $C_1, \ldots, C_m$ be our distinct conjugacy classes, and WLOG let $C_1, \ldots, C_n$ be the classes disjoint from $Z(G)$, and $C_{n+1}, \ldots, C_m$ be the classes with non-empty intersection with $Z(G)$. Backtracking, note that $[G : C_G(a)] = [G : \mathrm{Stab}(a)] = |\mathcal{O}(a)|$. Thus, to get our Class Equation, it suffices to prove that $\sum_{i=n+1}^{m} |\mathcal{O}(a_i)| = |Z(G)|$. This will follow from the following lemma:

Lemma 9.6

For $a \in G$, $\mathcal{O}(a) = \{a\}$ iff $a \in Z(G)$.

Proof. We have the following equivalent statements:

$$\begin{aligned} \mathcal{O}(a) = \{a\} &\iff gag^{-1} = a \,\forall\, g \in G \\ &\iff ga = ag \,\forall\, g \in G \\ &\iff a \in Z(G). \end{aligned}$$

This shows the two statements are equivalent. □

The rest of the proof falls from the observation that if $a \in \mathcal{O}(b)$, then $\mathcal{O}(a) = \mathcal{O}(b)$. (One can show the inclusion goes in both directions.) Thus, if $\mathcal{O}(a_i) \cap Z(G) \neq \emptyset$, we can take some $b_i \in \mathcal{O}(a_i) \cap Z(G)$ and thus $\mathcal{O}(a_i) = \mathcal{O}(b_i) = \{b_i\}$. Furthermore, every element in $Z(G)$ must be in some orbit (namely, it's own), so we can now write our sum as

$$\sum_{i=n+1}^{m} |\mathcal{O}(a_i)| = \sum_{i=n+1}^{m} |\mathcal{O}(b_i)| = \sum_{i=n+1}^{m} 1 = |Z(G)|,$$

and the result follows. □

10 10/12 - Group Actions Review

10.1 Tackling Combinatorics Problems

One nice upshot of all the things we've developed thus far is that they help us solve some neat combinatorics problems. Let's look at one classic application of the Orbit-Stabilizer Theorem: counting the number of rotational symmetries of a cube.

Example 10.1 (Rotational Symmetries of Cube)

Let $\mathcal{R}$ be the group of rotational symmetries of a cube. Similar to how we can think of the dihedral group D_{2n} acting on the set $\{1, 2, \ldots, n\}$ (think of the set as the n vertices of the n-gon), $\mathcal{R}$ can act on the eight vertices of the cube, label $\{1, 2, \ldots, 8\}$.

WLOG choose the vertex $v = 1$. We know from the Orbit-Stabilizer Theorem that $|\mathcal{R}| = |\mathcal{O}(1)| \cdot |\operatorname{Stab}(1)|$. Consider the orbit of $\mathcal{O}(1) = \{r \cdot 1 \mid r \in \mathcal{R}\}$. It's not hard to find a symmetry which maps 1 to any other given vertex v, so in fact $\mathcal{O}(1) = \{1, 2, \ldots, 8\}$ is the whole set. (The action is **transitive**.) Thus, $|\mathcal{O}(1)| = 8$.

Now we count Stab(1). We know the vertex 1 lies at the intersection of three edges of the cube. Let the other endpoint of the edges be v_1, v_2, v_3, respectively. Then, we see that any symmetry fixing 1 in place must rotate the vertices v_1, v_2, v_3, which gives us 3 rotations. Thus, $|\operatorname{Stab}(1)| = 3$, and multiplying gives $|\mathcal{R}| = 8 \cdot 3 = 24$.

Exercise 10.2. Try doing the same thing, but instead let $\mathcal{R}$ act on the set of faces of the cube. Check that you get the same answer for $|\mathcal{R}|$! (Hint: you should end up with $6 \cdot 4$.) Do the same likewise for acting on the set of edges of the cube.

For a combinatorial argument not using the Orbit-Stabilizer Theorem, let $\ell_1, \ell_2, \ell_3, \ell_4$ be the four space diagonals of the cube. Show that any permutation of the ℓ_i's gives a unique rotational symmetry of the cube.

10.2 Unpacking the Class Equation

It's a scary equation. We'll spend some time dissecting what's going on. To restate,

Theorem 10.3 (Theorem 9.5 restatement)
Let $C_1, \dots, C_n$ be the distinct conjugacy classes disjoint from $Z(G)$. Then,

$$\begin{aligned} |G| &= |Z(G)| + \sum_{i=1}^{n} |C_i| \\ &= |Z(G)| + \sum_{i=1}^{n} |\mathcal{O}(a_i)|, \end{aligned}$$

where a_i is a representative of C_i.

We're going to justify why we're considering $|Z(G)|$ separately from all the other conjugacy classes. We could have just gone ahead and summed over all distinct conjugacy classes, even those intersecting $Z(G)$, but if you work through some examples, you'll see that the orbits intersecting $Z(G)$ are pretty stupid. In particular, they're just the element itself, so you're summing a bunch of 1's. Naturally, the orbits intersecting $Z(G)$ are the orbits of the elements of $Z(G)$ itself, so we'd be adding $|Z(G)|$ 1's, hence the $|Z(G)|$ in our sum.

This is clearer when we write it out mathematically:

Lemma 10.4
If $Z_1, \dots, Z_n$ are the distinct conjugacy classes that intersect the center, then

$$\sum_{i=1}^{m} |Z_i| = |Z(G)|.$$

Proof. Choose $a_i \in Z_i$, so $Z_i = \mathcal{O}(a_i)$. Note that $a \in \mathcal{O}(a)$ for any $a \in G$. We proved/it kinda follows from definition that $\mathcal{O}(a_i) = \{a_i\} \iff a_i \in Z(G)$, so it suffices to show that $a_i \in Z(G)$. By assumption, $\mathcal{O}(a_i) \cap Z(G) \neq \emptyset$, so $\exists\, g \in Z(G) \cap \mathcal{O}(a_i)$.

Again, any element g is contained in its own orbit, so $g \in \mathcal{O}(g)$ and $g \in \mathcal{O}(a_i)$, which is only possible if $\mathcal{O}(a_i) = \mathcal{O}(g)$. But $g \in Z(G)$, so $\mathcal{O}(g) = \{g\}$, which forces $a_i = g \in Z(G)$. The conclusion follows. □

As a consequence, any conjugacy class disjoint from $Z(G)$ will have order strictly greater than 1, so in some sense, the class equation divides the sum up into the trivial conjugacy classes (the classes with just one element, which are counted in $|Z(G)|$) and the non-trivial conjugacy classes (with order greater than one).

10.3 Cycle Notation for Permutations

Hands down definitely the best way to write permutations.

Recall that $S_n := \{f : \{1, \dots, n\} \to \{1, \dots, n\} \mid f \text{ bijection}\}$. Equivalently, we can think of S_n as the group of permutations on the set $\{1, 2, \dots, n\}$. For instance, if $\sigma \in S_4$ maps

$\sigma(1) = 1$, $\sigma(2) = 3$, $\sigma(3) = 4$, and $\sigma(4) = 2$, then this corresponds to the permutation where 1 goes to 1, 2 goes to 3, etc.

Cycle notation gives us a really pretty way of writing this concisely. We explain via demonstration: in this case, we can write $\sigma = (1)(2\,3\,4)$. The (1) is by itself because it is fixed. For the cycle $(2\,3\,4)$, this is indicating that 2 goes to 3, 3 goes to 4, and 4 goes to 2. In general, $(a_0\,a_1\,a_2\,\ldots\,a_n)$ is the cycle where a_k goes to a_{k+1} (and a_n wraps around to a_0). This cycle is an example of an n-cycle, i.e. a cycle with n elements.

Oftentimes, fixed points are omitted from the cycle notation, so in our first example it'd be completely acceptable (and even preferred) to write $\sigma = (2\,3\,4)$.

So, cycle notation basically decomposes any permutation into a product of cycles. Work through these exercises to get more familiar:

Exercise 10.5. Take $\sigma \in S_5$ where $\sigma(2) = 3$, $\sigma(3) = 2$, and everything else is fixed. Write σ in cycle notation!

Exercise 10.6. Describe the permutation $\tau = (1\,2)(3\,4) \in S_4$. What is the order of τ?

Exercise 10.7. Suppose $(1, 2, 3, 4, 5, 6, 7) \mapsto (1, 3, 4, 2, 6, 7, 5)$, in that order. Write σ in cycle notation.

Thinking of these permutations as bijective functions, we can compose two permutations together. Suppose we take the two 2-cycles (i.e. transpositions, since we're just swapping two elements) $\sigma_1 = (1\,2)$ and $\sigma_2 = (1\,3)$. Then, $\sigma_1 \circ \sigma_2$ first applies the permutation σ_2, then σ_1. We work in that order: $\sigma_2(1) = 3$, $\sigma_2(2) = 2$, and $\sigma_2(3) = 1$. Then, we have

$$\begin{aligned}\sigma_1(1) &= \sigma_1(\sigma_2(3)) = 2\\ \sigma_1(2) &= \sigma_1(\sigma_2(2)) = 1\\ \sigma_1(3) &= \sigma_1(\sigma_2(1)) = 3,\end{aligned}$$

so $\sigma_1 \circ \sigma_2$ maps $3 \mapsto 2$, $2 \mapsto 1$, and $1 \mapsto 3$. It's a cycle! In particular, $\sigma_1 \circ \sigma_2 = (1\,3\,2)$.

I mentioned this earlier, but I'll make it explicit:

Definition 10.8 (Transposition)**.** A 2-cycle is called a **transposition**.

The following statements are true, and perhaps a bit clunky to prove rigorously, but in this case I think as long as you convince yourself that these are true, then you're good to go.

Fact 10.9. Disjoint cycles commute, e.g. $(1\,2)(3\,4) = (3\,4)(1\,2)$.

Fact 10.10. Any permutation $\sigma \in S_n$ can be written as a product of *disjoint* cycles, called the **cycle decomposition** of σ, e.g. $(1\,2)(1\,3) = (1\,3\,2)$.

10.4 Conjugacy Classes for Permutations

We're now going to investigate the conjugacy classes of the symmetric group S_n. First, a definition:

> **Definition 10.11** (Cycle Type)**.** If $\sigma \in S_n$ is a product of *disjoint* cycles of lengths $n_1, n_2, \dots, n_r$ where $n_1 \leq \dots \leq n_r$ and $n_1 + \dots + n_r = n$, then we say that σ has **cycle type** $(n_1, n_2, \dots, n_r)$.

The cycle type is sort of like the skeleton of our permutation, as it tells us how the permutation decomposes into cycles.

> **Exercise 10.12.** What is the cycle type of the identity permutation? Of a transposition?

The reason why we bring up the notion of cycle type is that it serves as a useful invariant under conjugation. The conjugation actions preserves this "skeleton"; **conjugation preserves the cycle type**. More explicitly,

Proposition 10.13

Let $\sigma, \tau \in S_n$. Suppose that the cycle decomposition of σ is

$$\sigma = (a_1 \, \dots \, a_{k_1})(b_1 \, \dots \, b_{k_2}) \cdots .$$

Then,

$$\tau\sigma\tau^{-1} = (\tau(a_1) \, \dots \, \tau(a_{k_1}))(\tau(b_1) \, \dots \, \tau(b_{k_2})) \cdots .$$

Even better, the converse is also true:

Proposition 10.14

Two elements of S_n are conjugate if and only if they have the same cycle type.

Example 10.15

Let $\sigma_1 = (4\,5)(1\,2\,3)$ and $\sigma_2 = (4\,5)(1\,3\,2)$, both in S_5. Both have cycle type $(2, 3)$, so by Proposition 10.14, they must be conjugates. Comparing σ_1 and σ_2, let $\tau(4) = 4$, $\tau(5) = 5$, $\tau(1) = 1$, $\tau(2) = 3$, and $\tau(3) = 2$, i.e. $\tau = (2\,3)$. Then, one can verify that $\sigma_2 = \tau\sigma_1\tau^{-1}$.

I'm not sure if we'll prove this proposition in this class, but it's good to convince yourself that this is true. In the meantime, we return back to investigating conjugacy classes of S_n. We start:

Let σ be an m-cycle in S_n. How many conjugates does σ have?

Well, Proposition 10.14 pretty much does all the heavy work for us. Any conjugate of σ must have the same cycle type, i.e. it must be an m-cycle as well. It suffices to count the number of m-cycles in S_n.

Any m-cycle is of the form $(a_1\, a_2\, \ldots\, a_m)$ for some $a_i \in \{1, \ldots, n\}$ distinct. We have n options for a_1, $n-1$ options for a_2, etc. until we have $n-m+1$ options for a_m. However, we must be careful with overcounting: note that $(a_1\, a_2\, \ldots\, a_n)$ and $(a_2\, a_3\, \ldots\, a_n\, a_1)$ are the same cycle. Thus, we are overcounting each m times, so we correct by dividing by m. This gives the number of conjugates as

$$|\mathcal{O}(\sigma)| = \frac{n(n-1)\cdots(n-m+1)}{m}.$$

Another basic fact which you should convince yourself is true:

Exercise 10.16. The order of an m-cycle is m.

Problem 10.17. Let $G = S_4$, and let K be the following subset containing all $(2,2)$-type permutations: $K = \{e, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$. (For simplicity sake, I'm going to notate $K = \{e, a, b, c\}$, in that order.)

1. Prove that $K \leq S_4$.
2. Prove that $K \trianglelefteq S_4$.
3. Let $H = \{\sigma \in S_4 \mid \sigma(4) = 4\} \simeq S_3$ be a subgroup of S_4. Show that $S_4/K \simeq S_3$. (Use the Second Isomorphism Theorem.)

Remark 10.18 (Actually an exercise)**.** Before even beginning, note that K has 4 elements. What is the order of a? of b? of c? Have you seen a group like this before?

Proof. (Part 1) K is clearly non-empty. Every element has an inverse – in fact, each element is its own inverse. Finally, one can compute

$$\begin{aligned} ab &= (1\,2)(3\,4)(1\,3)(2\,4) \\ &= (2\,3)(1\,4) = (1\,4)(2\,3) = c, \end{aligned}$$

and likewise $ac = b$ and $bc = a$, so this is closed under product. □

The proofs for the others are left as an ExErCiSe fOr ThE rEaDeR.

11 10/17 - Sylow Theorems

Corresponding reference: Section 4.5 in Dummit and Foote. (Small plug: I cover Sylow's First Theorem in the file on the left titled `oct14`, so check it out :P) Today will be reserved for stating the three theorems and their consequences; Wednesday will be for proving them.

We covered Lagrange's Theorem earlier in the semester, which told us that if $H \leq G$, then $|H| \mid |G|$. As a small example, if $|G| = 36$, then we know that there cannot be a subgroup of order 5.

But is there a converse to Lagrange? That is, if $d \mid |G|$, does there always exist a subgroup of order d?

Sadly (or not, depending on your perspective), this is not always true. To give an example, we're going to introduce a very important subgroup of the symmetric group, using $n = 4$ as our specific case for now:

Example 11.1 (Alternating Group)

Let $n = 4$. Consider the subgroup $A_4 \leq S_4$ containing all permutations of type $(2, 2)$ or $(1, 3)$. Explicitly, the elements of A_4 are

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

so $|A| = 12$. (Check that this is a group!) We have $6 \mid 12$, but we will prove below that A_4 **has no subgroup of order** 6.

Proof. Suppose for the sake of contradiction that there exists $H \leq A_4$ of order 6. Then, $[A_4 : H] = 2$. Let $\sigma \in A_4 \setminus H$ be a 3-cycle. Consider the cosets $eH, \sigma H, \sigma^2 H$. We have $\sigma H \neq \sigma^2 H$ since $\sigma \notin H$, and since $\sigma^2 = \sigma^{-1}$, we have $\sigma^2 H = \sigma^{-1} H \neq eH$ since $\sigma \notin H \implies \sigma^{-1} \notin H$.

But then this means $eH, \sigma H, \sigma^2 H$ are distinct cosets. This contradicts the fact that H only has two cosets in A_4, so no such H can exist. □

Remark 11.2. More generally, the alternating subgroup $A_n \leq S_n$ contains all even permutations of S_n, i.e. permutations whose sign is $+1$. (If you don't know what the sign of a permutation is, it's intuitively saying that "there are an even number of switches.") This group is actually *really* important – the crux of Galois theory is that A_n is simple for $n \geq 5$ – but I don't think we'll have time to explore this in this class. Take Math 123!

11.1 First Sylow Theorem

We start with a definition:

Definition 11.3 (p-group)**.** A group of order p^k for p prime, $k \in \mathbb{N}$ is called a **p-group**.

The statement of the First Sylow Theorem is as follows:

Theorem 11.4 (First Sylow Theorem)
A finite group whose order is divisible by a prime p contains a Sylow p-subgroup. Equivalently, if $|G| = p^e \cdot m$ for $e \in \mathbb{N}$ and $p \nmid m$, then G contains a subgroup H of order p^e. (H is a Sylow p-subgroup.)

This may seem reasonable, but it is not obvious at all a priori! For instance, it's not evidentthat a group of order 21 consisting of the identity element and 20 elements with order 3 does not exist. To make this theorem a bit more tangible, let's look at some consequences.

Corollary 11.5
A finite group G, with $p \mid |G|$ for prime p, contains an element of order p.

Proof. Let $|G| = p^r \cdot m$, where $p \nmid m$. By the First Sylow Theorem, there exists $H \leq G$ with $|H| = p^r$. Let $x \in H$ be a non-identity element. By Lagrange's Theorem, $|x| \mid |H| = p^r$, so $|x| = p^k$ for some $1 \leq k \leq r$. Let $y = x^{p^{k-1}}$. then,

$$y^p = \left(x^{p^{k-1}}\right)^p = x^{p^k} = e.$$

Combining this with the fact that $y \in H$ (it is a product of x's for $x \in H$) and $y \neq e$ (else $|x| \leq p^{k-1}$), we have $|y| \mid p^r$ and $1 < |y| \leq p$, which is only possible if $|y| = p$ as desired. □

11.2 Conjugate Subgroups

Now we build up some tools to help us prove our theorem of interest. The notion of conjugates for subgroups is basically identical to conjugates of elements.

Definition 11.6 (Conjugate Subgroups)**.** If $H_1, H_2 \leq G$, we say that H_1 is **conjugate** to H_2 if $\exists\, g \in G$ such that $H_1 = gH_2g^{-1}$. We denote this $H_1 \sim H_2$.

Remark 11.7. Note $H_1 = gH_2g^{-1} \iff H_2 = g^{-1}H_1g = g^{-1}H(g^{-1})^{-1}$, so conjugates "go both ways."

We bring this definition up because we will show that any two Sylow p-subgroups are conjugates.

Lemma 11.8
If $H_1 \leq G$ is a Sylow p-subgroup of G and $H_1 \sim H_2$, then H_2 is also a Sylow p-subgroup.

Proof. Since $H_1 \sim H_2$, we have $|H_1| = |H_2|$. (Left as exercise, but not hard at all.) Let $H_2 = gH_1g^{-1}$ for some $g \in G$. We need to check that H_2 is actually a subgroup as well.

Since $e \in H_1$, we have $e = geg^{-1} \in H_2$. For closure of inverses, if $g_1 = gh_1g^{-1} \in H_2$ with $h_1 \in H$, then $g_1^{-1} = gh_1^{-1}g^{-1}$, which is also in H_2 since $h_1^{-1} \in H$. Finally, if $g_1 = gh_1g^{-1}$ and $g_2 = gh_2g^{-1}$ are both elements of H_2, then $g_1g_2 = (gh_1g^{-1})(gh_2g^{-1}) = gh_1h_2g^{-1} \in H_2$, as desired. □

11.3 Second Sylow Theorem

Theorem 11.9 (Second Sylow Theorem)

Let G be a finite group with $p \mid |G|$. Then,

1. The Sylow p-subgroups of G are conjugate subgroups, i.e. if P_1, P_2 are two Sylow p-subgroups, then $\exists\, g \in G$ such that $P_2 = gP_1g^{-1}$.
2. Every subgroup of G that is a p-group is contained in a Sylow p-subgroup.

Corollary 11.10

A group G has a unique Sylow p-subgroup H iff H is a normal Sylow p-subgroup.

Proof. For the reverse direction, we know from Lemma 11.8 that any two Sylow p-subgroups are conjugates. But if H is normal, then any conjugate of H is itself, so it is the only such subgroup.

For the forward direction, the Second Sylow Theorem tells us that $H = gHg^{-1}$ for any $g \in G$, which means H is normal, as desired. □

11.4 Third Sylow Theorem

An absolute banger of a theorem.

Theorem 11.11 (Third Sylow Theorem)

Let G be a finite group, with $|G| = n = p^r \cdot m$ for $r \in \mathbb{N}$ and $p \nmid m$. Let n_p denote the number of Sylow p-subgroups of G. Then,

$$n_p \mid m \qquad n_p \equiv 1 \pmod{p}.$$

This is perhaps the most tangible theorem of them all, and also personally the most surprising. To investigate some applications, we're going to define what a simple group is.

Definition 11.12 (Simple group)**.** A **simple group** G is a group with no non-trivial normal subgroups, i.e. if $H \trianglelefteq G$, then $H = G$ or $H = \{e\}$.

Some really cool results that fall from the three theorems, with the Third carrying a lot of the weight.

Proposition 11.13

There is no simple group of order pq, where $p \neq q$ are primes.

Proof. Let n_p, n_q be the number of Sylow p, q-subgroups, respectively. Sylow I tells us that $n_p, n_q > 0$. If either of $n_p, n_q = 1$, then Corollary 11.10 tells us that there is a non-trivial normal subgroup of G. Thus, suppose $n_p, n_q > 1$.

WLOG assume $p > q$. By Sylow III, $n_p \mid q$ and $n_p \neq 1$, so $n_p = q$. We also have $n_p \equiv 1 \pmod p$, so $q \equiv 1 \pmod p \implies p \mid q - 1$. But then $p < q$, a contradiction to $p > q$, so we conclude. □

Proposition 11.14

A group of order 30 is not simple.

Proof. By Sylow III, $n_2 \mid 3 \cdot 5$ and $n_2 \equiv 1 \pmod 2$, so $n_2 \in \{1, 3, 5, 15\}$. Also by Sylow III, we have $n_3 \mid 10$ and $n_3 \equiv 1 \pmod 3$, so $n_3 \in \{1, 10\}$. Finally, $n_5 \mid 6$ and $n_5 \equiv 1 \pmod 5$, so $n_5 \in \{1, 6\}$. If any of n_2, n_3, n_5 is 1, then Corollary 11.10 immediately gives us our desired result. Thus, assume none are 1.

This forces $n_3 = 10$ and $n_5 = 6$. But these numbers are too big! In particular, $n_3 = 10$ means we have 10 Sylow 3-subgroups, which gives us $2 \cdot 10 = 20$ distinct non-identity elements, and $n_5 = 6$ gives us another $4 \cdot 6 = 24$ distinct non-identity elements. We already have $20 + 24 = 44 > 30$, so this is not possible! The result follows. □

I really like this proof; Sylow III sets us up with a lot of information, enough such that it reduces the problem into a simple counting puzzle. There's not that many problems in higher-level math where you can finish a proof by just saying "$20 + 24 > 30$ so we're done."

12 10/19 - Proving Sylow I, and More Sylow Applications

Recall the First Sylow Theorem (Theorem 11.4), which we'll prove first.

Example 12.1 (Sylow I on S_4)

Let $G = S_4$. We know $|G| = 24 = 2^3 \cdot 3$, so Sylow I tells us that there exists a Sylow

2-subgroup of S_4. This subgroup has order $2^3 = 8$. Indeed, one can prove that D_8 is a Sylow 2-subgroup of S_4. Even better, $|S_5| = 120 = 2^3 \cdot 3 \cdot 5$, and one can show that D_8 is still a Sylow 2-subgroup of S_5.

12.1 Proof of Sylow I

Now we prove the theorem.

Proof. We're going to define a very peculiar group action. Suppose $|G| = p^r \cdot m$ where $p \nmid m$. Then, we will define A to be the set of all subsets of G with size p^r, i.e.

$$A = \{S \subset G \text{ subset} \mid |S| = p^r\}.$$

Note that any Sylow p-subgroups must lie in A. Now, we define a group action $G \curvearrowright A$ where, for $g \in G$ and $S \in A$, $g \cdot S := \{g * s \mid s \in S\}$.

We need to verify that this is a valid group action. The first thing we must verify is that $g \cdot S$ is actually in A, i.e. $|g \cdot S| = p^r$. Consider the function $f : S \to g \cdot S$ where $s \mapsto g * s$. This is injective ($g * s_1 = g * s_2 \implies s_1 = s_2$) and surjective (the pre-image of any $g * s$ is simply s), so it is a bijection, which means the cardinalities must match. Verifying that this action satisfies the group action axioms (identity action, associativity) is not difficult so I'll leave it for the reader.

We will now present a series of results that'll build up to our conclusion. The first lemma concerns the number of elements of S. Note that S consists of all subsets of size p^r; a simple combinatorial argument tells us that there are $\binom{p^r \cdot m}{p^r} = \frac{(p^r \cdot m)!}{p^r!(p^r(m-1))!}$ total elements in S. (Myrto calls this Lemma 0; I think it's self-evident enough to just state it without calling it a lemma.)

Lemma 12.2

$p \nmid |A| = \binom{p^r \cdot m}{p^r}$.

Proof. This isn't even related to group theory lol this is strictly a number theory argument. We can simplify

$$\begin{aligned}\binom{p^r \cdot m}{p^r} &= \frac{p^r m(p^r m-1)(p^r m-2)\cdots(p^r m - p^r + 1)}{p^r(p^r-1)\cdots 1} \\ &= \frac{p^r m}{p^r} \cdot \frac{p^r m - 1}{p^r - 1} \cdot \cdots \cdot \frac{p^r m - p^r + 1}{1} \\ &= \frac{p^r m - 0}{p^r - 0} \cdot \frac{p^r m - 1}{p^r - 1} \cdot \cdots \cdot \frac{p^r m - (p^r - 1)}{p^r - (p^r - 1)}.\end{aligned}$$

We wish to show that this product is not divisible by p, so it suffices to show that every term in the product, which is of the form $\frac{p^r m - (p^r - i)}{p^r - i}$ for $1 \le i \le p^r$, is not divisible by p.

Suppose p^k is the largest power of p dividing $p^r - i$. Then, since $p^k \mid p^r$, $p^k \mid p^r m - (p^r - i)$ as well. But suppose p^j is the largest power of p dividing $p^r m - (p^r - i)$. Since $p^j \mid p^r$, we must have $p^j \mid p^r - i$. Thus the largest power of p dividing the numerator and the denominator, respectively, must be the same, which means the quotient is not divisible by p. The conclusion follows. □

Lemma 12.3

Let $S \in A$. Then, $|\operatorname{Stab}_G(S)| \leq |S| = p^r$.

Proof. Recall $g \cdot S = \{g * s \mid s \in S\}$ and $\operatorname{Stab}_G(S) = \{g \in G \mid g \cdot S = S\}$. Pick any $s \in S$. Then, $\forall\, g \in \operatorname{Stab}_G(S)$, $g \cdot S = S \implies g * s \in S$, so $\operatorname{Stab}_G(S) \cdot s = \{g * s \mid g \in \operatorname{Stab}_G(S)\} \subseteq S$. But similar to what we did earlier in the proof, we can construct a bijection $f : \operatorname{Stab}(S) \to \operatorname{Stab}(S) \cdot s$ where $s' \mapsto s' * s$. Thus, with the information $|\operatorname{Stab}(S)| = |\operatorname{Stab}(S) \cdot s|$ and $\operatorname{Stab}(S) \cdot s \subseteq S$, we have $|\operatorname{Stab}(S)| = |\operatorname{Stab}(S) \cdot s| \leq |S|$ as desired. □

Now we start digging into the group theoretic parts of the proof. We know that the distinct orbits of our action partition our set A, so write

$$A = \bigsqcup_{i=1}^{k} \mathcal{O}(S_i)$$

where $\mathcal{O}(S_i)$ are the distinct orbits. But by our first lemma (12.2), $p \nmid |A|$, so

$$p \nmid \sum_{i=1}^{k} |\mathcal{O}(S_i)|.$$

It follows then that $p \nmid |\mathcal{O}(S_i)|$ for some i. But by Orbit-Stabilizer Theorem, we know $|\mathcal{O}(S_i)| = |G|/|\operatorname{Stab}(S_i)|$, and if $p \nmid |G|/|\operatorname{Stab}(S_i)|$ but $p^r \mid |G|$, it must be true that $p^r \mid |\operatorname{Stab}(S_i)|$. Consequently, $p^r \leq |\operatorname{Stab}(S_i)|$.

But our second lemma (12.3) tells us that $|\operatorname{Stab}(S_i)| \leq p^r$, so equality must hold. Thus, $\operatorname{Stab}(S_i)$ is a Sylow p-subgroup of G, and we conclude. □

This proof is definitely quite funky: we construct this very unusual (but admittedly clever) group action on the set of all *subsets* of our desired order, and then the crux of the argument follows from some combinatorial and divisibility arguments.

For a more straightforward proof, check out the `oct14.tex` file on the left! I first prove Cauchy's Theorem, which is a weaker form of Sylow I, before proving Sylow I itself. I think despite having to prove an intermediary theorem, that proof is more streamlined and closer to the spirit of group theory.

12.2 Applications of the Sylow Theorems

So apparently we're only going to prove the First Sylow Theorem.

Problem 12.4. Show that S_4 has no subgroup isomorphic with Q_8.

Proof. Note $|Q_8| = 8$. It suffices to show that there is no Sylow 2-subgroup of S_4 that is isomorphic to Q_8.

We showed in the beginning of today's class (Example 12.1) that D_8 is a Sylow 2-subgroup of S_4. By Lemma 11.8, any Sylow 2-subgroup of S_4 must be conjugates with D_8. But conjugation is an isomorphism, i.e. $H \xrightarrow{\simeq} gHg^{-1}$ for any $g \in G$ (prove this yourself if you don't believe me!), so it suffices to show that D_8 is not isomorphic to Q_8.

We use an order argument. Q_8 only has one element of order 2 (namely, -1) whereas D_8 has 5 elements of order 2 (the 4 reflections and r^2), so they cannot be isomorphic. QED □

We're going to apply Sylow III for this next one. I encourage you to try it yourself before looking at the proof!

Proposition 12.5

Every group of order 15 is cyclic.

Consequently, note that any group of order 15 must be abelian.

Proof. By Sylow III, $n_3 \mid 5$ and $n_3 \equiv 1 \pmod 3$, which forces $n_3 = 1$. Let H be the unique Sylow 3-subgroup of G; by Corollary 11.10 (follows from Sylow II), $H \trianglelefteq G$ is normal. It is also cyclic since it has order 3, so $H = \langle h \rangle$.

Also by Sylow III, $n_5 \mid 3$ and $n_5 \equiv 1 \pmod 5$, so $n_5 = 1$ as well. Let K be the unique Sylow 5-subgroup of G. Likewise, K is normal and cyclic ($K = \langle k \rangle$).

Since $H \trianglelefteq G$, we will consider the subgroup $HK \leq G$. We will now show that $HK = G$, i.e. $|HK| = |G| = 15$. A priori we have $HK \leq G \implies |HK| \leq |G| = 15$. But we know $H, K \leq HK$, so by Lagranges, we have $3 = |H| \mid |HK|$ and $5 = |K| \mid |HK|$, so $15 \mid |HK|$. Coupled with $|HK| \leq 15$, this is only possible if $|HK| = 15$.

It remains to show $G = HK$ is cyclic. We claim that the map

$$\begin{aligned} \varphi : H \times K &\to HK \\ (a, b) &\mapsto ab \end{aligned}$$

is an isomorphism. This completes the proof, since then we'd have $HK \simeq H \times K = \langle h \rangle \times \langle k \rangle = \langle (h, k) \rangle$, so HK would be cyclic. It is not hard to show that φ is a homomorphism (use the fact that $H, K \trianglelefteq HK$). Bijectivity follows from the fact that φ is surjective (the preimage of $ab \in HK$ is $(a, b) \in H \times K$) and $|H \times K| = |HK| = 15$, so we're done. □

13 10/26 - Rings

10/24 (Monday) was the midterm. Now that it's over, we can move on to the second half of the course! The corresponding reference will be Section 7.1 of Dummit and Foote.

The key distinction here is that a ring has *two* binary operations: addition and multiplication. So the setting here is a *lot* more specific than that for groups. The most classic example of a ring is the integers $\mathbb{Z}$; think about them as you go through the following definitions, examples, results, etc.

Definition 13.1 (Ring)**.** A **ring** R is a set together with two binary operations $(+, \cdot)$, called addition and multiplication, such that:

1. $(R, +)$ is an abelian group.
2. $\cdot$ is associative, i.e. $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in R$.
3. The distribution laws hold in R, i.e. $\forall\, a, b, c \in R$, $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(b + c) \cdot a = b \cdot a + c \cdot a$.

A few remarks: although addition is commutative since $(R, +)$ is abelian, multiplication does not need to be commutative. As we'll see in our examples, the set of $n \times n$ matrices with real entries forms a ring, but multiplication is not commutative.

Also, there are additive inverses (from $(R, +)$ being a group) but we do not require the existence of multiplicative inverses. In other words, $(R, \cdot)$ does NOT need to be a group. (Even if we take away 0, $(R \setminus \{0\}, \cdot)$ is not necessarily a group.) Once we require multiplicative inverses, though, we get something called a **field**, which we may cover in this class?? not sure. Definitely in Math 123 though!

To highlight these remarks, we'll start with a more sophisticated examples, then cover the easier ones:

Example 13.2 (Matrices)

Let $M_n(\mathbb{R})$ be the set of $n \times n$ matrices with real entries. We covered in Lecture 1 that this set under addition forms a ring, and it is not difficult to see that with multiplication, it satisfies associativity and distributivity. But note that there are matrices that are not invertible, e.g. $\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$, or more generally anything with determinant 0.

Example 13.3 (Most things we like are rings)

$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/n\mathbb{Z}$ are all examples of rings! ($+$ and $\cdot$ in $\mathbb{Z}/n\mathbb{Z}$ are taken modulo n.) The set of odd integers under $+$ and $\cdot$ is not a ring, though, since under addition they don't form a group. (It's not closed under $+$.) On the other hand, the set of even integers, $(2\mathbb{Z}, +, \cdot)$, does form a ring.

When multiplication is commutative for a ring, we aren't pretentious like in the group setting and call them abelian. Instead, we just call them commutative.

Definition 13.4 (Commutative Ring)**.** The ring R is **commutative** if multiplication is commutative.

If we're really pedantic, note that our definition of rings don't even require the multiplicative identity 1 to exist! Some conventions require us to say that a ring R **has identity** (or has unity) if $\exists 1 \in R$ such that $1 \cdot a = a \cdot 1 = a$ for all $a \in R$ – seems like Myrto wants us to not assume identity.

On the other hand, you may see other references go ahead and assume all rings have a multiplicative identity $1 \neq 0$ (thus, $(\{0\}, +, \cdot)$ is not a ring). Cleverly, the call rings without identity as a rng, since you take away i for identity. This is just mathematicians being (annoying) fastidious, though – for basically everything in our class, we assume rings have identity.

Example 13.5 (Gaussian integers)

Number theorists love this one! The set $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$ forms a ring. Addition works like $(a + bi) + (c + di) = (a + c) + (b + d)i$ and is commutative, and multiplication works like $(a + bi)(c + di) = (ac - bd) + (ad + bc)i \in \mathbb{Z}[i]$. In fact, multiplication is also commutative, so $\mathbb{Z}[i]$ is a commutative ring! Even better, $\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$ also forms a commutative ring (for the Gaussian integer case, $d = -1$).

13.1 Preliminary Results

A fun result, gaining something out of nothing:

Lemma 13.6

If R is a ring with identity, then distributivity already implies that $+$ is commutative.

In other words, if we assume that rings have identity, then we don't even need to specify that $(R, +)$ must be abelian in our definition, since we can prove it from the other axioms!

Proof. We have

$$\begin{aligned}(1 + 1)(a + b) &= (1 + 1)(a + b)\\ \implies 1(a + b) + 1(a + b) &= (1 + 1)a + (1 + 1)b\\ \implies a + b + a + b &= a + a + b + b\\ \implies b + a &= a + b,\end{aligned}$$

and as this works for any $a, b \in R$, the result follows. □

The ring axioms, although still barebones, are powerful, because from them we can prove results which are seemingly so basic they feel unprovable/we've always taken them for granted.

Proposition 13.7 ("Back to first grade")
Let R be a ring. Then,

1. $0 \cdot a = a \cdot 0 = 0$ for all $a \in R$.
2. $(-a)b = a(-b) = -(ab)$ for all $a, b \in R$.
3. $(-a)(-b) = ab$.
4. If R has identity 1, then the identity is unique, and $-a = (-1) \cdot a$.

Proof. **Statement (1):** We have $0 \cdot a = (0+0) \cdot a = 0 \cdot a = 0 \cdot a$, so Cancellation Law on $(R, +)$ gives $0 \cdot a = 0$ for any $a \in R$.

(2): We have $ab + (-a)b = (a + (-a))b = 0 \cdot b = 0$, which means $-(ab) = (-a)b$. A similar argument holds for $a(-b) = -(ab)$. Then for **(3)**, $(-a)(-b) = -(a(-b)) = -(-(ab)) = ab$ since inverses in a group are unique.

(4): If $1, 1'$ are both identities, then $1 = 1 \cdot 1' = 1'$. (This mimics the uniqueness of identity in groups.) □

13.2 Zero divisors, Units

Some rings are "annoying" in that you can have two elements, both non-zero, which multiply to 0. We have special names for such elements, as well as a special name for rings with such elements.

Definition 13.8 (Zero divisor)**.** A non-zero element $a \in R$ is called a **zero-divisor** if there is a non-zero element $b \in R$ such that $a \cdot b = 0$ or $b \cdot a = 0$.

Definition 13.9 (Integral domain)**.** (Technically not covered in class yet) A ring with no zero-divisors is caleld an **integral domain**.

Example 13.10 ($\mathbb{Z}/6\mathbb{Z}$ is not integral domain)
Note $2 \cdot 3 = 0$ in $\mathbb{Z}/6\mathbb{Z}$, so $2, 3$ are both zero-divisors, and $\mathbb{Z}/6\mathbb{Z}$ is not an integral domain. Many things we like are integral domains, though! e.g. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/p\mathbb{Z}$ for p prime, etc.

Thinking opposite, if an element has a multiplicative inverse, we call it a unit.

Definition 13.11 (Unit)**.** Assume R has identity $1 \neq 0$. An element $u \in R$ is called a **unit** if $\exists v \in R$ such that $u \cdot v = v \cdot u = 1$. We cay that v is the multiplicative inverse

> of u, and write $v = u^{-1}$ (likewise, $u = v^{-1}$). We denote the set of units of R as
>
> $$R^{\times} = \{u \in R \mid u \text{ is a unit}\}.$$

Example 13.12 (Units of $\mathbb{Z}$, $\mathbb{Z}/p\mathbb{Z}$)
The units of $\mathbb{Z}$ are only $1, -1$. On the other hand, $(\mathbb{Z}/p\mathbb{Z})^{\times}$ contains everything other than 0. (This is a number theoretic fact.) We call $(\mathbb{Z}/p\mathbb{Z})^{\times}$ the **group of units** of $\mathbb{Z}/p\mathbb{Z}$ (and more generally, the set of units of a ring under multiplication forms a group, which we call the group of units of that ring).

Rings with "only" units (except for 0) have a special name, too:

> **Definition 13.13** (Division ring)**.** A non-trivial ring R such that $\forall\, R \setminus \{0\}$, $\exists\, a^{-1} \in R$ such that $aa^{-1} = a^{-1}a = 1$ is called a **division ring**.

14 10/31 - Integral Domains and Fields

A short exercise to demonstrate why we don't like rings with zero divisors:

> **Exercise 14.1.** Find a ring R and $a, b, c \in R \setminus \{0\}$ such that $ab = ac$ but $b \neq c$.

Proof. $\mathbb{Z}/n\mathbb{Z}$ is our friend, where n is composite. Simplest example: in $\mathbb{Z}/4\mathbb{Z}$, $2 \cdot 1 = 2 \cdot 3$ but $1 \neq 3$ clearly. You can do a similar thing for, say, $\mathbb{Z}/6\mathbb{Z}$, since $2 \cdot 1 = 2 \cdot 4$ but $1 \neq 4$. □

On the other hand, if a is **not** a zero-divisor, then we can indeed proceed with the Cancellation Law. Reasoning: if $a \in R \setminus \{0\}$ is not a zero-divisor and $ab = ac$, then $a(b - c) = 0$, which is only true if $b - c = 0$ since a is not a zero-divisor.

Because we like the Cancellation Law so much, most of our time spent on rings will be with rings that allow, in general, cancellation, i.e. rings that have no (non-zero) zero-divisors. One such example of such a ring is what we saw at the very end of last class, a **division ring**! (See Definition 13.13; any unit cannot be a zero divisor.)

14.1 Fields

When we require division rings to be commutative, then we get another truly lovely mathematical object.

> **Definition 14.2** (Field)**.** A **field** is a commutative division ring.

Aside from these seemingly-random names (I still have no idea why fields are called fields), groups, rings, and fields are arguably the three most important objects in algebra.

Example 14.3 (Fields! and not fields)

$\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are all examples of fields: they are commutative, and every non-zero element has an inverse/is invertible. $\mathbb{Z}$ and $\mathbb{Z}[i]$ are not fields, because although they are commutative, you can't invert every element, e.g. $\frac{1}{2} \notin \mathbb{Z}, \mathbb{Z}[i]$.

Example 14.4 (Quaternions)

Note that a field is a commutative division ring, which suggests that there exists division rings which are not commutative. Indeed, we have the following fancy example. Recall the quaternion group Q_8 and its generators $i, j, k \in Q_8$. We can construct the **quaternion ring**

$$\mathbb{H} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\}.$$

Addition and multiplication behaves in the way you'd expect (think complex numbers but more general).

14.2 Integral Domains

Scoping outwards, we'll give a name to the most general kind of ring that exhibits Cancellation Law for any non-zero element, i.e. rings where every non-zero element is not a zero-divisor.

Definition 14.5 (Integral domain)**.** A commutative ring with $1 \neq 0$ is called an **integral domain** if it has no zero-divisors.

Remark 14.6. All fields are integral domains, which in turn are always rings. There are many other types of rings we could fill into this "inclusion chain"! For instance, commutative rings where every element has unique factorization into irreducibles forms another kind of ring, called **unique factorization domains (UFDs)**. All fields are UFDs, and all UFDs are integral domains.

Example 14.7 (Integral domains)

Perhaps the easiest example (and where the name *integral* comes from) is the integers $\mathbb{Z}$. Note that $\mathbb{Z}$ is an example of an integral domain which is not a field. Similarly, $\mathbb{Z}[i]$ is an integral domain. As we mention above, all fields are integral domains.

14.3 Some Results

Integral domains and fields are closer than you may imagine:

Proposition 14.8

Any finite integral domain is a field.

Proof. Let R be a finite integral domain. R is commutative by definition. Let $0 \neq a \in R$. It suffices to show that a is a unit, i.e. $\exists\, b \in R$ such that $ab = 1$.

Let $f : R \to R$ map $x \mapsto ax$. Note that f is injective since if $f(x) = f(y)$, for $x, y \in R$, then $ax = ay \implies x = y$ since integral domains satisfy the Cancellation Law. At the same time, since R is finite, this means f must be surjective by a simple cardinality argument.

Thus, $\exists\, b \in R$ such that $f(b) = 1$, which is equivalent to saying $ab = 1$, as desired. □

We observed before that some cases of $\mathbb{Z}/n\mathbb{Z}$, particularly when n is composite, are annoying because zero divisors arise. (If $n = ab$ is composite, $a, b \neq 1$, then $ab = 0$ in $\mathbb{Z}/n\mathbb{Z}$.) Luckily, though, when n is prime, we're happy:

Proposition 14.9

$\mathbb{Z}/n\mathbb{Z}$ is a field iff n is a prime.

Proof. From the above argument, if n is composite, then n is not an integral domain, and hence not a field. We wish to show that when $n = p$ is prime, then $\mathbb{Z}/p\mathbb{Z}$ is a field. From the above proposition (14.8), it suffices to show that $\mathbb{Z}/p\mathbb{Z}$ is an integral domain, as it is clearly finite.

Suppose $a, b \in \mathbb{Z}/p\mathbb{Z}$ such that $ab = 0$ in $\mathbb{Z}/p\mathbb{Z}$. Then, $p \mid ab$, which is only possible if $p \mid a$ or $p \mid b$, i.e. $a = 0$ or $b = 0$. Thus, it is an integral domain, and we conclude. □

14.4 Polynomial Rings

Lowkey the heart of the study of commutative algebra. This is an object you're very familiar with already (we all know what polynomials are!), we're just taking the time to formalize the notion.

First, we'll define what we mean by a polynomial. Let R be a ring. Then, a polynomial in x is an expression

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0,$$

where $n \in \mathbb{N} \cup \{0\}$, and $a_i \in R$ for $0 \leq i \leq n$. We call the a_i's as **coefficients**, and if $a_n \neq 0$, then $n = \deg f$ is called the **degree** of f. If $a_n \neq 0$, then it is called a **leading coefficient**, and if $a_n = 1$ (assuming $1 \in R$), then we say that $f(x)$ is **monic**.

All of this checks out with how we normally understand polynomials, e.g. over $R = \mathbb{Z}$, the expression $2x^2 + 3x - 2$ is a polynomial of degree 2 with leading coefficient 2, so it is not monic.

Considering the set of all polynomials in x over R, we can endow it with addition and multiplication operations! (It's the same as how we'd normally add and multiply polynomials.) One can check that this satisfies the axioms of a ring. We notate this ring as $R[x]$. People often read this ring out loud as "R adjoin x" or "polynomials over R in x." Explicitly...

Definition 14.10 (Polynomial ring over R)**.** The set of all polynomials of any degree with coefficients in a ring R is called the **ring of polynomials in one variable over R** and is denoted by $R[x]$. Even more explicitly,

$$R[x] = \{a_n x^n + \cdots + a_1 x + a_0 \mid n \in \mathbb{N} \cup \{0\}, a_i \in R \,\forall\, 0 \leq i \leq n\}.$$

Addition and multiplication works as you expect; Myrto writes it out in class, but I'm too lazy to write it out.

Remark 14.11. If R is commutative with identity, then $R[x]$ is also commutative with identity $1 \neq 0$.

Remark 14.12. Warning: a polynomial is a "formal object" and should not be identified with the function it may define. To explain more: in school, we often thought of polynomials as functions – think of all the times you were forced to graph quadratic equations and stuff. But bounding ourselves to the "polynomial is a function" perspective is really restrictive in higher-level math. Instead, we think of polynomials as *just expressions*, a sum of a bunch of powers of x each multiplied to a ring element.

Here's one situation in which the "polynomial is a function" perspective causes problems. Take $R = \mathbb{Z}/2\mathbb{Z}$, and consider $p(x) = x + 1 \in R[x]$ and $q(x) = x^2 + 1 \in R[x]$. But then we have $p(0) = q(0) = 1$ and $p(1) = q(1) = 0$, but clearly $p \neq q$ (p has degree 1 while q has degree 2). Thus, *polynomials cannot be determined by their point evaluations*, i.e. polynomials shouldn't be thought of as functions.

15 11/02 - Ring Homs, Ideals

Happy November! (Wait, it's already November??)

15.1 Wrapping Up Integral Domains

Example 15.1 (Why zero-divisors suck, revisited)

Half exercise, half remark. We know that for polynomials over the integers (which we now have a nice way of notating: $\mathbb{Z}[x]$), given $f, g \in \mathbb{Z}[x]$, we have $\deg(fg) = \deg(f) \cdot \deg(g)$. But this is only true because $\mathbb{Z}$ is an integral domain!

To consider a polynomial ring over a non-integral domain, take $(\mathbb{Z}/4\mathbb{Z})[x]$. Although it is true that $\deg(2x^2 + 1)(x + 1) = 3 = \deg(2x^2 + 1) + \deg(x + 1)$, this is not true for $\deg(2x^2 + 1)(2x + 1) = \deg(4x^3 + 2x^2 + 2x + 1) = \deg(2x^2 + 2x + 1) = 2 \neq$

$\deg(2x^2+1)+\deg(2x+1)$.

As alluded in the above, everything is good for integral domains.

Theorem 15.2

Let R be an integral domain and $p(x), q(x) \in R[x]$ are non-zero. Then,

1. $\deg pq = \deg p + \deg q$;
2. $(R[x])^\times = R^\times$;
3. $R[x]$ is an integral domain.

Proof. (Statement 1) Let $p(x) = a_n x^n + \cdots + a_0$ where $a_n \neq 0$ so $n = \deg p$, and let $q(x) = b_m x^m + \cdots + b_0$, where $b_m \neq 0$ so $m = \deg q$. Since $p, q \in R[x]$, we require every $a_i, b_j \in R$. Then, the leading term of the product $p(x)q(x)$ is clearly $a_n b_m x^{n+m}$, with $a_n b_m \neq 0$ since $a_n \neq 0, b_m \neq 0$ and R is an integral domain (hence no zero divisors). Thus, $\deg pq = n + m$.

(Statement 2) Suppose $p(x) \in (R[x])^\times$, so $\exists\, q(x) \in R[x]$ such that $p(x)q(x) = q(x)p(x) = 1$. Taking the degree on both sides, we have $\deg pq = \deg 1 = 0$. By Statement 1, this is equivalent to $\deg p + \deg q = 0$, which can only be possible if $\deg p = \deg q = 0$, so $p(x) \in R$ is constant. But if $p \in R$, then p can only be a unit if $p \in R^\times$.

(Statement 3) First, one can show that $R[x]$ is commutative since R itself is commutative. Furthermore, $R \subset R[x]$, so as $1 \in R$ and $1 \neq 0$ in R, the same applies in $R[x]$.

Now we show that $R[x]$ has no zero divisors. Suppose $p(x), q(x) \in R[x]$ where $q(x) \neq 0$ but $p(x)q(x) = 0$. Then, $\deg pq = \deg 0 = 0$, so $\deg p(x) + \deg q(x) = 0$, which can only be true if $\deg p(x) = \deg q(x) = 0$. Thus, $p(x) = p_0 \in R$ and $q(x) = q_0 \in R$ are both constants. But since R is an integral domain and $q_0 \neq 0$ but $p_0 q_0 = 0$, it must follow that $p(x) = p_0 = 0$, as desired. □

15.2 Ring Homomorphisms

The following several sections correspond to Section 7.3 in Dummit and Foote.

Whenever we introduce a new mathematical object, it is important to specify how the objects interact with each other, i.e. how to map from one such object to another. Like with groups, we call maps between rings preserving the ring structure as homomorphisms. But since rings have two operations, we need to make sure that the map preserves the structure with respect to both operations. This will be made clear in the definition.

Definition 15.3 (Ring homomorphism)**.** Let R, S be rings. A **ring homomorphism** is a function $\varphi : (R, +, \cdot) \to (S, +, \cdot)$ such that $\forall\, r_1, r_2 \in R$,

1. (Preserves additive structure) $\varphi(r_1 + r_2) = \varphi(r_1) + \varphi(r_2)$

2. (Preserves multiplicative structure) $\varphi(r_1 r_2) = \varphi(r_1)\varphi(r_2)$

A bijective ring homomorphism is called a **ring isomorphism**.

Remark 15.4 (Ring homs are group homs)**.** The first requirement (preserving additive structure) is equivalent to saying φ is a group homomorphism under $+$, where we consider R, S as additive groups.

We continue carrying over some of our knowledge of group homomorphisms/functions in general.

Definition 15.5 (Kernel)**.** The **kernel** of a ring homomorphism $\varphi : R \to S$ is

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

Remark 15.6 (Notions of kernel coincide)**.** Viewing φ as a group homomorphism (Remark 15.4), the group-theoretic kernel of φ coincides with the ring-theoretic $\ker \varphi$.

Example 15.7 (Important: reduction maps)

This flavor of maps, where a ring is sent to some quotient, will come up many times! We'll look at the reduction map mod n, i.e. the map

$$\begin{aligned} \varphi : \mathbb{Z} &\to \mathbb{Z}/n\mathbb{Z} \\ a &\mapsto \overline{a}. \end{aligned}$$

Note that this is a ring homomorphism: $\varphi(a+b) = \overline{a+b} = \overline{a} + \overline{b} = \varphi(a) + \varphi(b)$ and $\varphi(ab) = \overline{ab} = \overline{a}\overline{b}$. The kernel of φ are all integers which are $0 \mod n$, i.e. the subgroup $n\mathbb{Z}$. This checks out: we know φ is surjective, so we could use the First Isomorphism Theorem to verify (tautologically) $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/\ker\varphi \simeq \operatorname{Im}\varphi = \mathbb{Z}/n\mathbb{Z}$.

Example 15.8 (Evaluation at 0 map)

Another map that will recur in this class. We can take the map $\varphi : R[x] \to R$ where we evaluate each polynomial at 0; in other words, plug in 0 for x. One can check that this is a ring homomorphism (by "one" I mean you, because I'm too lazy to write stuff out).

Exercise 15.9. Let $\varphi_n : \mathbb{Z} \to \mathbb{Z}$ be the map sending $a \mapsto na$. For which integers n is φ_n a ring homomorphism? (Hint: issues arise when you require $\varphi(ab) = \varphi(a)\varphi(b)$.)

15.3 Subrings, Ideals

Just like how in groups, we have the notion of a subgroup, i.e. a subset which also has a group structure, we can have "rings" contained in larger rings.

Definition 15.10 (Subring)**.** A **subring** S of a ring R is a subgroup of $(R, +)$ that is closed under mutliplication (i.e. if $a, b \in S$, then $ab \in S$).

Remark 15.11. Note that a subring does NOT have the identity 1, unless the subring is the whole ring itself.

Example 15.12 (Subrings)

$\mathbb{Z}$ is a subring of $\mathbb{Q}$ (in turn, $\mathbb{Q}$ is a subring of $\mathbb{R}$, which is a subring of $\mathbb{C}$, which is a subring of the quaternion ring $\mathbb{H}$, see Example 14.4). For any ring R, R is a subring of $R[x]$.

Like with groups, the image and kernel of a ring homomorphism are subrings.

Proposition 15.13

Let R, S be rings, $\varphi : R \to S$ be a ring homomorphism. Then,

1. $\operatorname{Im} \varphi$ is a subring of S.
2. $\ker \varphi$ is a subring of R.

Proof. We already know that since φ is a group homomorphism (under $+$), $\ker \varphi, \operatorname{Im} \varphi$ are subgroups of R, S, respectively. Thus, we only need to check that they are closed under multiplication.

Let $a, b \in \operatorname{Im} \varphi$. Then, $a = \varphi(a'), b = \varphi(b')$ for some $a', b' \in R$. Then, $ab = \varphi(a')\varphi(b') = \varphi(a'b')$, and as $a'b' \in R$, we get $ab \in \operatorname{Im} \varphi$.

Likewise, let $r, s \in \ker \varphi$. Then, $\varphi(rs) = \varphi(r)\varphi(s) = 0 \cdot 0 = 0$, so $rs \in \ker \varphi$. □

We can strengthen the notion of "closed under multiplication" though, which will serve to be magically useful. We'll use the kernel as our motivation. Note that even if $s \notin \ker \varphi$, we would still have $\varphi(rs) = \varphi(r)\varphi(s) = 0 \cdot \varphi(s) = 0 \implies rs \in \ker \varphi$, so in some sense, the kernel "absorbs" everything in multiplication: whenever I multiply an element in the kernel with something else, the product will always be in the kernel.

We have a special name for this.

Definition 15.14 (Ideal)**.** Let R be a ring and $I \subseteq R$ a subring.

1. If $\forall r \in R, a \in I$, we have $ra \in I$, then I is a **left ideal**.

2. If $\forall r \in R, a \in I$, we have $ar \in I$, then I is a **right ideal**.
3. If I is both a left and right ideal, then it is a **two-sided ideal**.

Remark 15.15 (Etymology of ideal)**.** Given the name "ideal," one may suspect that ideals are really useful. Indeed, in lots of number theory, ideals are the "ideal" way to think about things. Hopefully we can elaborate on this later in class!

Example 15.16 (Ideals)

Many examples! As we observed already, if $\varphi : R \to S$ is a ring homomorphism, then $\ker \varphi$ is an ideal of R. (This suggests an analogy between normal subgroups for groups and ideals for rings! And indeed, as we'll see very soon, we can quotient a ring by an ideal.)

- $n\mathbb{Z}$ is an ideal of $\mathbb{Z}$. In terms of the kernel, we already observed that $n\mathbb{Z}$ is the kernel of the reduction map $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$. (See Example 15.7.)
- The subset of $R[x]$ containing all polynomials with 0 as its constant term forms an ideal of $R[x]$. Indeed, this is just the kernel of the evaluation at 0 map. (Example 15.8.)
- For any ring R, we have the zero ideal $\{0\}$. Also, R is an ideal of itself.
- The subring
$$I = \left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \mid a, b \in \mathbb{R} \right\} \subseteq M_2(\mathbb{R})$$
is a left ideal. It is NOT a right ideal! (Verify this yourself.)

16 11/07 - Analogous Group Properties for Rings

16.1 Quotient Rings

As mentioned last time, it turns out that the analogous notion of normal subgroups for rings is ideals. So let's take the following setup: let $(I, +) \leq (R, +)$. A priori, let's just assume I is a subring. We can consider the set of (additive) cosets $R/I = \{r + I \mid r \in R\}$. In the perspective of groups under the addition operation, we get that $(R/I, +)$ is a group! That's half of the ring axioms.

But it'd be really nice if we could equip this quotient with a ring structure, which would require multiplication. Let's define multiplication the natural way: given cosets $a + I$ and $b + I$, we want $(a + I)(b + I) = (ab) + I$. This is where we require stronger conditions, like how quotients didn't make sense for any subgroup.

The following theorem tells us that the condition we exactly want is that I should be an ideal:

Theorem 16.1

Let $I \subset R$ be a subgroup of $(R, +)$. Then, the multiplication on R/I given by $(a + I)(b + I) = ab + I$ is well-defined and makes a ring $(R/I, +, \cdot)$ iff I is an ideal of R.

Proof. First, assume the multiplication operation is well-defined, i.e. for any $a, b \in R$, $(a + I)(b + I) = ab + I$. This means that if we choose any $i, j \in I$, then the product of elements $(a + i)(b + j) \in ab + I$.

Since the above is true for any choice of $a, b \in R$ and $i, j \in I$, we will choose appropriately to show that I satisfies all the ideal axioms. If $a = b = 0$, then we get $ij \in I$ for all $i, j \in I$, so I is a subring. If $a = j = 0$, then we get $ib \in I$, which tells us that I is a right ideal. Likewise, if $b = i = 0$, then we get $aj \in I$, so I is a left ideal. Thus, I is a (two-sided) ideal, as desired.

Now we assume I is an ideal. First, we will verify that multiplication is well-defined, i.e. our multiplication operation is independent on choice of representative. Suppose $a' \in a + I$ and $b' \in b + I$. (Note this implies $a' + I = a + I$ and $b' + I = b + I$ by Lemma 6.17.) Equivalently, this means $a' = a + i$ and $b' = b + j$ for some $i, j \in I$. Then, we have $a'b' = (a + i)(b + j) = ab + aj + ib + ij$. Since I is an ideal, $aj, ib, ij \in I$, so $a'b' \in ab + I$, which tells us (again by Lemma 6.17) that $a'b' + I = ab + I$, so indeed our choice of representatives does not matter.

Finally, we observe that the multiplication operation here is associative and distributive as multiplication in our ring R is associative and distributive, so we conclude. □

To really wrap things up formally:

Definition 16.2 (Quotient ring)**.** Let R be a ring and I an ideal. Then, R/I is called the **quotient ring** of R by I. Note we just showed that the quotient only makes sense as a ring iff I is an ideal.

Example 16.3 ($\mathbb{Z}/n\mathbb{Z}$)

Prototypical example of quotient ring is $\mathbb{Z}/n\mathbb{Z}$. I suspect most quotient rings you'll encounter in this class won't be too far off in flavor from $\mathbb{Z}/n\mathbb{Z}$.

16.2 First Isomorphism Theorem

The reason why I had a clear preference for the First Isomorphism Theorem when studying groups is that this one, unlike the others, can be generalized to algebraic objects beyond groups, like rings!

Before we state the theorem, let's see perhaps the simplest example of how we can use the First Isomorphism Theorem. If I is an ideal of R, then we can construct a projection map

$R \to R/I$ where $r \mapsto r+I$. It is not hard to see that this is a surjective ring homomorphism, and that the kernel of the map is exactly I. Tautologically, the First Isomorphism Theorem tells us that since the image of the map is R/I and the kernel is I, we get $R/I \simeq R/I$, which checks out.

Theorem 16.4 (First Isomorphism Theorem, for rings)
If $\varphi : R \to S$ is a ring homomorphism, then $\ker\varphi$ is an ideal of R and $R/\ker\varphi \simeq \operatorname{Im}\varphi$ as rings.

Proof. An isomorphism of rings must respect the additive and multiplicative structures of both rings. The additive part is covered from our work in groups: if $\varphi : R \to S$ is a ring homomorphism, then $\varphi : (R,+) \to (S,+)$, where we only remember the group structure, is a group homomorphism, so by the First Isomorphism Theorem for groups, we get $(R/\ker\varphi, +) \simeq (\operatorname{Im}\varphi, +)$ as groups.

Even more explicitly, this means we have a map

$$\begin{aligned} \psi : R/\ker\varphi &\to \operatorname{Im}\varphi \\ r + \ker\varphi &= \varphi(r) \end{aligned}$$

which is a well-defined bijective group homomorphism. To have ψ be a ring isomorphism, it simply remains to show that ψ preserves multiplicative structure, i.e. for any $r, s \in R$, $\psi((r+\ker\varphi)(s+\ker\varphi)) = \psi(rs+\ker\varphi)$. But we have

$$\begin{aligned} \psi(rs+\ker\varphi) &= \varphi(rs) = \varphi(r)\varphi(s) \\ &= \psi(r+\ker\varphi)\psi(s+\ker\varphi), \end{aligned}$$

as desired. □

Example 16.5 (First Iso Theorem for rings)
Consider the ring homomorphism $\varphi : \mathbb{Z}[x] \to \mathbb{Z}$ where $p(x) \mapsto p(0)$. Clearly, the map is surjective, so $\operatorname{Im}\varphi = \mathbb{Z}$. Furthermore, $\ker\varphi = \{p(x) \in \mathbb{Z}[x] \mid p(0) = 0\} = \{a_1x + a_2x^2 + \cdots + a_nx^n \mid n \in \mathbb{N}, a_i \in \mathbb{Z}\} = x \cdot \mathbb{Z}[x]$ (intuitively, if a polynomial has zero constant term, then it must be divisible by x), so the First Isomorphism Theorem tells you that $\mathbb{Z}[x]/x\mathbb{Z}[x] \simeq \mathbb{Z}$.

A similar example: consider now $\varphi : \mathbb{Z}[x] \to \mathbb{Z}/2\mathbb{Z}$ where $\underline{p(x)} = \overline{p(0)}$. Again, this map is surjective so $\operatorname{Im}\varphi = \mathbb{Z}/2\mathbb{Z}$, and $\ker\varphi = \{p(x) \in \mathbb{Z}[x] \mid \overline{p(0)} = \overline{0}\} = \{2a + xq(x) \mid a \in \mathbb{Z}, q(x) \in \mathbb{Z}[x]\} = (2, x)$, the ideal generated by 2 and x. (If the last equality scares you, it's just notation, so don't fret.) The First Isomorphism Theorem tells us that $\mathbb{Z}[x]/(2,x) \simeq \mathbb{Z}/2\mathbb{Z}$.

Being comfortable with this kind of stuff will be immensely helpful for classes like Math 123 and 129! (and honestly any algebra class lol)

16.3 Finitely Generated Ideals

It is hard to overstress the importance of ideals in ring theory – it's like saying addition is important in math – so we're going to talk more about ideals. The following material will discuss ideals generated by a finite set. The corresponding reference is Section 7.4 of the textbook.

For now, our convention will be that all rings have identity ($1 \in R$) and $1 \neq 0$. We start with a general result about ideals:

Lemma 16.6

If R is a ring and $I, J \subset R$ are ideals, then $I \cap J$ is an ideal.

Proof. Honestly a good (and very simple!) exercise for working with the ideal axioms, so I suggest you work this out on your own before proceeding :)

First, given $x, y \in I \cap J$, we know that as I and J are each ideals, $x+y \in I$ and $x+y \in J$, so $x + y \in I \cap J$, so it is closed under addition. Now let $r \in R$ and $a \in I \cap J$. It suffices to show both $ar, ra \in I \cap J$. But since I and J are each ideals, it follows that $ar, ra \in I$ and $ar, ra \in J$, so they both must lie in the intersection as well, and we conclude. □

We didn't talk about this too much in groups, but even in the group setting, we like things being finitely generated. Lots of groups we worked with were generated by one element – cyclic groups – and they were arguably the nicest kind of groups we could work with. Groups like D_8 are generated by two element (r and s), and although some problems arose (e.g. D_8 is not abelian), we still had ways to work around them. There's also this quite remarkable statement called the Classification of Finitely Generated Abelian Groups, which allows us to characterize all such groups.

This is all to say that it makes sense to care about finitely generated cases in rings as well. So we'll talk about finitely generated ideals.

Definition 16.7 (Ideals generated by subset)**.** Let $A \subset R$ be a subset.

1. Let (A) be the smallest ideal of R containing A, i.e.

$$(A) = \bigcap_{\substack{I \supseteq A \\ I \text{ ideal}}} I.$$

   (A) is called the **ideal generated by A**.

2. If $A = \{a\}$ is a singleton, we write $(A) = (a)$ and call it a **principal ideal**.
3. If $A = \{a_1, \ldots, a_n\}$, then we write $(A) = (a_1, \ldots, a_n)$ and call it a **finitely generated ideal**.

This definition is good because it's generic, but bad because it's difficult to grasp these ideals. What are its elements?

We'll take the simplest case: consider the principal ideal (a). By definition, $a \in (a)$, and since (a) is an ideal, $0 \in (a)$. We can now work through the ideal axioms to generate more elements of (a). Given any $r \in R$, we must have $ar \in (a)$ and $ra \in (a)$. This also means that $r_1 a r_2 \in (a)$ for any $r_1, r_2 \in R$. Also, since ideals are closed under addition, $ar + ra \in (a)$ as well. This is a good start; we'll continue to characterize this better.

Definition 16.8. If $A = \{a_1, \dots, a_n\}$, we have the sets

$$\begin{aligned} RA &= \{r_1 a_1 + \cdots + r_n a_n \mid r_i \in R, a_i \in A\} \\ AR &= \{a_1 r_1 + \cdots + a_n r_n \mid a_i \in A, r_i \in R\} \\ RAR &= \{r_1 a_1 s_1 + \cdots + r_n a_n s_n \mid r_i, s_i \in R, a_i \in A\}. \end{aligned}$$

These sets are interesting because...

Claim 16.9. For finite subset A in ring R, the set RA is a left ideal, AR is a right ideal, and RAR is an ideal.

I won't prove the claim because I'm lazy (also it's a good exercise to work out for yourself – it's mostly definitional!), but within each set, you can add two elements "componentwise" to show closure under addition, and (to give an example) for multiplication in RA, for any $b := r_1 b_1 + \cdots + r_n b_n \in RA$ and $r \in R$, we have $r \cdot b = r(r_1 b_1 + \cdots + r_n b_n) = (rr_1)b_1 + \cdots + (rr_n)b_n \in RA$, yay!

Turns out that these sets are exactly what we wanted, so we tie our two loose ends.

Proposition 16.10

If $A \subseteq R$ is finite, then $(A) = RAR$.

Proof. Claim 16.9 tells us that RAR is an ideal, and since $1 \in R$ (we're assuming all rings have identity in this section), we have $1 \cdot a \cdot 1 = a \in RAR$ for all $a \in A$, so $A \subseteq RAR$. Thus, $(A) \subseteq RAR$ since (A) is the smallest ideal containing A.

The opposite inclusion follows from our construction of RAR. Any ideal that contains A must contain all elements of RAR, as an ideal must be closed under addition and multiplication by ring elements on both sides. In particular, this means (A) must contain RAR, as it is an ideal containing A, and we conclude. □

Note that if our ring is commutative, then $RA = AR = RAR$, since all left or right ideals are two-sided. All of this might not seem useful, but maybe these examples will convince you otherwise.

Example 16.11

First, take the ring $\mathbb{Z}$, and consider (n), the ideal generated by n. Then, the above tells us that $(n) = RnR = \{n \cdot a \mid a \in \mathbb{Z}\} = n\mathbb{Z}$, the multiples of n.

Now consider the ideal $(2,x)$ in $\mathbb{Z}[x]$. We have $(2,x) = \{2p(x) + xq(x) \mid p(x), q(x) \in \mathbb{Z}[x]\} = \{2n + xr(x) \mid n \in \mathbb{Z}, r(x) + \mathbb{Z}[x]\}$, which is how we characterized this ideal in Example 16.5.

Exercise 16.12. Describe the ideal $(2,x) \cap (3,x)$.

Proof. Note that Lemma 16.6 tells us that the intersection is indeed another ideal. Suppose $p(x) \in (2,x) \cap (3,x)$. Then, $p(0) \in 2\mathbb{Z}$ and $p(0) \in 3\mathbb{Z}$, so $p(0) \in 6\mathbb{Z}$, which means $(2,x) \cap (3,x) \subseteq (6,x)$. But clearly the reverse inclusion is also true, so $(2,x) \cap (3,x) = (6,x)$. □

17 11/09 - Special Types of Ideals

17.1 Finitely Generated Ideals, cont.

We continue our discussion from last time on ideals generated by some finite subset of the ring. A very convenient type of ideal is a principal ideal, which is generated by just one element, an example being $(n) = n\mathbb{Z}$ an ideal of $\mathbb{Z}$. We also saw an ideal with more than one generator, like $(2,x) \subset \mathbb{Z}[x]$.

But sometimes, you can simplify things, i.e. there are situations where you can reduce the number of generators. This is always the case for the integers: the ideal $(9,15) = \{9a + 15b \mid a, b \in \mathbb{Z}\}$ is actually equivalent to the principal ideal (3)! (You should take some time and try to see what's going on here.)

What about the ideal $(2,x)$? Is this a principal ideal of $\mathbb{Z}[x]$ in disguise?

Claim 17.1. The ideal $(2,x) \subset \mathbb{Z}[x]$ is not a principal ideal.

Proof. Suppose it were, so $(2,x) = (f(x))$ for some $f(x) \in \mathbb{Z}[x]$. We know $2 \in (2,x) = (f(x))$, so $2 = f(x)g(x)$ for some $g(x) \in \mathbb{Z}[x]$. Taking degrees, we get $0 = \deg 2 = \deg f(x) + \deg g(x)$, but as $\deg f, \deg g \geq 0$, this is only possible if $\deg f = \deg g = 0$. This means that $f, g \in \mathbb{Z}$ are both constants; denote $f(x) = a_0$, $g(x) = b_0$ integers. Given $f(x)g(x) = a_0 b_0 = 2$, our possibilities are reduced to $f(x) = a_0 \in \{\pm 1, \pm 2\}$.

We also know $x \in (f(x))$, which means $x = f(x) \cdot q(x)$ for some $q(x) \in \mathbb{Z}[x]$. Write $q(x) = c_0 + c_1 x + \cdots + c_n x^n$, so $x = f(x)q(x) = a_0(c_0 + \cdots + c_n x^n)$, which forces $a_0 c_1 = 1$ and $a_0 c_i = 0$ for all other $i \neq 1$.

The equality $a_0 c_1 = 1$ (with $a_0 \in \{\pm 1, \pm 2\}$, $c_1 \in \mathbb{Z}$) further restricts our possibilities to $f(x) = a_0 \in \{\pm 1\}$, so $(2,x) = (f(x)) = (1)$ or (-1). But both generate the entire ring, so this means $(2,x) = \mathbb{Z}[x]$. But this is clearly not true, since all elements of $(2,x)$ must have even constant term, and we conclude. □

Turns out that although we care a lot about fields, the study of ideals is not very fruitful in fields. It is a very ring-specific object.

Proposition 17.2

Let R be a commutative ring with $1 \neq 0$. Then, R is a field iff its only ideals are $\{0\}$ and the ring R itself.

So in a way, fields are the ring-equivalent of simple groups. (Recall simple groups are groups with only the trivial group and the entire group as its normal subgruops.) This is a corollary of the following result:

Proposition 17.3

Let I be an ideal of R with $1 \neq 0$. Then, $I = R$ iff I contains a unit.

Proof. If $I = R$, then $1 \in R = I$ is a unit, done. Now suppose I contains a unit a, with $ab = 1$ for some $b \in R$. Then, $(a) \subset I$, but also $1 = ab \in (a) \subset I \implies (1) = R \subset I$, which is only possible if $I = R$. □

Now we quickly prove Proposition 17.2.

Proof. Suppose the only ideals of R are the zero ideal and the ring itself. Let $a \in R \setminus \{0\}$. We wish to show $a \in R^\times$. Consider the principal ideal $I = (a)$. Since $a \neq 0$, we have $I \neq 0$, so by assumption we force $(a) = I = R$. But then $1 \in (a) \implies ab = 1$ for some $b \in R$, which means a is a unit.

For the forward direction, if R is a field and $\{0\} \neq I \subset R$ a non-zero ideal, then I must contain some non-zero field element, which is a unit, so Proposition 17.3 tells us that $I = R$ as desired. □

17.2 Maximal Ideals

Another special type of ideals are called maximal ideals. As the name suggests, you can't find any ideals which strictly contain them.

Definition 17.4 (Maximal ideal)**.** An ideal M in R is **maximal** if $M \neq R$ and the only ideals of R containing M is M and R itself.

Remark 17.5. Maximal ideals are not necessarily unique! A ring can have multiple maximal ideals. (Most simple example: in $\mathbb{Z}$, the ideal (p) generated by a prime number is maximal, and there are infinitely many primes.)

We won't prove the following result (the proof uses Zorn's Lemma, if you're interested) but it should be fairly intuitive once you understand what's going on:

Fact 17.6. Every ideal is contained in a maximal ideal.

Our current definition makes it a bit hard to determine whether an ideal is maximal. How can we guarantee there are no "larger" ideals? Luckily, we have a *super* useful characterization of maximal ideals:

Proposition 17.7 (Quotient of maximals is field)
Assume R is commutative with $1 \neq 0$. Then the ideal M is maximal iff R/M is a field.

Example 17.8 ($(2, x)$ is maximal)
From Example 16.5, we showed using the First Isomorphism Theorem that $\mathbb{Z}[x]/(2, x) \simeq \mathbb{Z}/2\mathbb{Z}$, which is a field! So $(2, x)$ is a maximal ideal. Likewise, we can do a similar argument to say that $(3, x)$ is maximal, as $\mathbb{Z}[x]/(3, x) \simeq \mathbb{Z}/3\mathbb{Z}$ is a field.

Example 17.9 (Primes induce maximal ideals)
If $p \in \mathbb{Z}$ is a prime, then $(p) = p\mathbb{Z}$ is a maximal ideal. It is useful to convince yourself of this via "showing" that no ideal strictly contains $p\mathbb{Z}$ other than $\mathbb{Z}$ itself, but you can also observe that $\mathbb{Z}/p\mathbb{Z}$ is a field, so the conclusion is immediate.

The proof of the above proposition will require this very sexy result, which regrettably it seems like we won't prove for the time being.

Theorem 17.10 (Lattice Isomorphism Theorem)
Let I be an ideal of R. Then, the ideals of R/I are of the form A/I, where $A \subset R$ is an ideal containing I.

Example 17.11 (Ideals of $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$)
Let's try to find all the ideals of $\mathbb{Z}/2\mathbb{Z}$. We know from Proposition 17.2 that since $\mathbb{Z}/2\mathbb{Z}$ is a field, the only ideals are $\{0\}$ and $\mathbb{Z}/2\mathbb{Z}$. But using the Lattice Isomorphism Theorem, it suffices to find all ideals of $\mathbb{Z}$ containing $4\mathbb{Z}$. Turns out the only such ideals are $\mathbb{Z}$ and $2\mathbb{Z}$, which gives us the ideals $\mathbb{Z}/2\mathbb{Z}$ and $2\mathbb{Z}/2\mathbb{Z} = \{0\}$, as desired.

For $\mathbb{Z}/4\mathbb{Z}$, we can find ideals of $\mathbb{Z}$ containing $4\mathbb{Z}$, which are $4\mathbb{Z}, 2\mathbb{Z}, \mathbb{Z}$. This gives us three ideals of $\mathbb{Z}/4\mathbb{Z}$, namely $\mathbb{Z}/4\mathbb{Z}$, $2\mathbb{Z}/4\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z}$, and $4\mathbb{Z}/4\mathbb{Z} \simeq \{0\}$.

Assuming this, we'll now prove Proposition 17.7.

Proof. The Lattice Isomorphism Theorem really does all the heavy lifting for us. The ideal $M \neq R$ is maximal iff (by definition) there are no ideals I such that $M \subsetneq I \subsetneq R$, which is true iff (by Lattice Isomorphism Theorem) the only ideals of R/M are R/M and $\{0\}$. But Proposition 17.2 tells us that this is true iff R/M is a field, QED. □

17.3 Prime Ideals

Even juicier than maximal ideals are *prime ideals*. Here's our motivation for the definition. Our standard definition for an integer n being prime is if the "only factors of n are 1 and n." But this is kind of stupid – clearly -1 is a factor, but why don't we mention that? I propose a sturdier way of defining primes, one that bypasses these technicalities. We know $p \in \mathbb{Z}$ is prime if $p \mid ab \implies p \mid a$ or $p \mid b$.

This is the inspiration of the below definition; in fact, the example below it will show that in $\mathbb{Z}$, our definition of prime and the definition of a prime ideal are equivalent.

Definition 17.12 (Prime ideal)**.** Let R be a commutative ring with $1 \neq 0$. An ideal $\mathfrak{p} \subsetneq R$ is **prime** if $\forall\, a, b \in R$ such that $ab \in \mathfrak{p}$, then $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$.

Example 17.13 (Primes, thankfully, generate prime ideals)

It would be kind of a disaster if, given a prime number, it didn't generate a prime ideal. Thankfully, if $p \in \mathbb{Z}$ is prime, then (p) is a prime ideal: if $ab \in (p)$ for $a, b \in \mathbb{Z}$, this is equivalent to saying $p \mid ab$, which means $p \mid a$ or $p \mid b$, i.e. $a \in (p)$ or $b \in (p)$. So the definition of prime ideal is basically just our primality condition we discussed earlier in disguise. The upshot of writing it like this is that we can generalize to rings that aren't as nice as $\mathbb{Z}$.

If n is composite, then we can show (n) is not prime. We can write $n = ab$ where $a, b \neq 1$, $a, b < n$, so $ab = n \in (n)$ but $a \notin (n)$, $b \notin (n)$. Finally, $\mathbb{Z}$ cannot be prime because we require prime ideals to be strict subsets.

As with maximal ideals, our current definition is a bit sad because it's hard to manually verify if a given ideal is prime. But just like with maximal ideals, we have a super useful characterization:

Proposition 17.14 (Quotient by prime is integral domain)

If R is a commutative ring with $1 \neq 0$, then $\mathfrak{p} \subseteq R$ is prime iff $R/\mathfrak{p}$ is an integral domain.

Consequently,

Fact 17.15. All maximal ideals are prime.

Proof. This follows from the fact that any field is an integral domain, so if $\mathfrak{m}$ is maximal, then $R/\mathfrak{m}$ is a field, hence an integral domain, hence $\mathfrak{m}$ is prime. □

So there are more primes than maximal ideals. Note that although all primes turn out to be maximal in $\mathbb{Z}$, this is not always the case: the ideal $(x) \subset \mathbb{Z}[x]$ is prime, since $\mathbb{Z}[x]/(x) \simeq \mathbb{Z}$ is an integral domain, but $\mathbb{Z}$ is not a field, so (x) is not maximal.

We now prove our characterization of prime ideals.

Proof. An ideal $\mathfrak{p} \subsetneq R$ is prime iff for any $ab \in \mathfrak{p}$, we have $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$. But this is equivalent to saying $R/\mathfrak{p} \neq \{0\}$ and if $ab + \mathfrak{p} = 0 + \mathfrak{p}$ in $R/\mathfrak{p}$, then either $a + \mathfrak{p} = 0 + \mathfrak{p}$ or $b + \mathfrak{p} = 0 + \mathfrak{p}$. But we defined multiplication of cosets as $(a + \mathfrak{p})(b + \mathfrak{p}) = ab + \mathfrak{p}$, so this is equivalent to saying if $(a + \mathfrak{p})(b + \mathfrak{p}) = 0 + \mathfrak{p}$, then one of the cosets must be $0 + \mathfrak{p}$. Equivalently, this means $R/\mathfrak{p} \neq \{0\}$ has no zero divisors, i.e. it is an integral domain, as desired. □

18 11/14 - Euclidean Domains

18.1 Larger Picture and Motivation

Yet another definition. But before you raise your hands and shout in disapproval, let's take a step back and see all the types of rings we have so far.

We start with additive groups. If it's abelian and it has a particular multiplicative structure, then it becomes a ring. If multiplication is also commutative, then we call it a commutative ring. Within commutative rings, if there are no zero divisors, then we call it an integral domain. Specifying even further, if every ideal is principal, we call it a **principal ideal domain**. (These have appeared in the most recent pset.) And finally, if the non-zero elements of the ring form a commutative group under multiplication, then we call it a field.

This is just to show that the collection of all rings (if we want to be pretentious, the *category* of rings) is like an ogre: it has many layers. We continue to impose restrictions on our ring axioms to form more and more specific rings, each having their own unique purpose in mathematics at large. Fields form the core of Galois theory; many scenarios in algebraic geometry deal with rings with certain conditions, e.g. integral domains.

Our next type of ring, called Euclidean domain, fits in between PIDs and fields: all fields are Euclidean domains, and all Euclidean domains are principal ideal domains. (The former is kinda stupid if you think about it long enough (or see Example 18.5); the latter is a consequence of PSet 9 Problem 4 and is explicitly proven in Proposition 18.6.)

Here's our motivation for Euclidean domains. In $\mathbb{Z}$, we have a Division Algorithm that allows us to find gcd's. (If you're a CS or number theory kid, this is the Euclidean Algorithm, which comes from the Division Algorithm, and from which the name "Euclidean domain" comes from.) Explicitly, Division Algorithm tells us that for any integers $m, n \in \mathbb{Z}$ with $n \neq 0$, $\exists\, q, r \in \mathbb{Z}$ such that $m = qn + r$ and $0 \leq r < n$.

The condition $0 \leq r < n$ suggests that we must have some notion of "size" which is not entirely clear in most rings. (How do we compare two polynomials?) So let's construct some way to measure size.

18.2 Definitions

Definition 18.1 (Norm)**.** Any function $N : R \to \mathbb{Z}_{\geq 0}$ with $N(0) = 0$ is called a **norm** in an integral domain. If $N(a) > 0$ for $a \in R \setminus \{0\}$, then the norm is called **positive**.

> **Author's Note 18.2.** I must comment that this definition of a norm is pretty unusual. Usually, norms are more restrictive, e.g. it must satisfy Triangle Inequality, but I guess Myrto's word is supreme in this class :)

Example 18.3 (Norms in $\mathbb{Z}$)

In the ring $\mathbb{Z}$, we have an obvious norm $N(a) = |a|$. We could also take something more creative: fix integers $a_1, \dots, a_n$, and let $N(a) = a_1 a + a_2 a^2 + \cdots + a_n a^n$.

We are now ready to define Euclidean domains.

> **Definition 18.4** (Euclidean Domain)**.** R is an **Euclidean domain** if there is a norm N on R such that $\forall\, m, n \in R$, $n \neq 0$, $\exists\, q, r \in R$ with $m = qn + r$ and $N(r) < N(n)$ or $r = 0$.

Example 18.5 (Euclidean domains)

$\mathbb{Z}$ is a Euclidean domain with $N(a) = |a|$; this is our Division Algorithm. All fields are Euclidean domains. Let F be a field. If $a, b \in F$ with $b \neq 0$, then $a = (ab^{-1})b$, i.e. the remainder is always 0, so we can take a stupid norm function like $N(a) = 0$ for all $a \in F$.

For something a little less trivial, $\mathbb{Q}[x]$ is a Euclidean domain with $N : \mathbb{Q}[x] \to \mathbb{Z}_{\geq 0}$ where $N(p(x)) = \deg p(x)$. This is because for any $p, q \in \mathbb{Q}[x]$, $q \neq 0$, there exists $q_1(x), r_1(x) \in \mathbb{Q}[x]$ such that $p(x) = q_1(x)q(x) + r_1(x)$ and $\deg r_1 < \deg q$. More generally, $F[x]$ is a Euclidean domain for any field F by the same argument.

18.3 Euclidean implies PID

I mentioned that every Euclidean domain is a principal ideal domain. We will now prove this.

Proposition 18.6

Every ideal in a Euclidean domain R is principal. More precisely, if I is an ideal of R, then $I = (d)$ for some $d \in R$.

Proof. The zero ideal is generated by 0, i.e. $\{0\} = (0)$. Let $I \neq \{0\}$. Let $d \neq 0$ be an element of I with smallest norm (i.e. there are no non-zero elements in I with norm less than $N(d)$). We claim $I = (d)$.

Suppose $a \in I$. Since R is a Euclidean domain, we may write $a = dq + r$ where $q, r \in R$ and either $r = 0$ or $N(r) < N(d)$. But by minimality of $N(d)$, it must follow that $r = 0$, which means $a = dq$, or equivalently $a \in (d)$. But this is true for any $a \in I$, so $I \subseteq (d)$. But $d \in I \implies (d) \subseteq I$, which forces equality. □

Corollary 18.7 ($\mathbb{Z}$ is PID)
$\mathbb{Z}$ is a principal ideal domain.

Thus, all ideals are of the form $(n) = n\mathbb{Z}$ for some $n \in \mathbb{Z}$. Even more, all prime ideals are of the form (p) for some prime $p \in \mathbb{Z}$. These are also all the maximal ideals. On the other hand...

Corollary 18.8
$\mathbb{Z}[x]$ is not a Euclidean domain.

Proof. We showed earlier (Claim 17.1) that $(2, x)$ is not a principal ideal, so $\mathbb{Z}[x]$ is not a PID and hence not Euclidean. (Note, on the other hand, $\mathbb{Q}[x]$ (or $F[x]$ for any field F) is a Euclidean domain by Example 18.5!) □

A very important statement: let R be a commutative ring with $1 \neq 0$. Let $a, b \in R$ with $b \neq 0$. Then,

$$\begin{aligned} b \mid a &\iff \exists\, r \in R \text{ such that } a = br \\ &\iff (a) \subseteq (b). \end{aligned}$$

This is a bit funky to remember at first, since the "order" switches ($b \mid a \iff (a) \subseteq (b)$), but this will get more intuitive as you play with it more. When in doubt, always think about what happens in $\mathbb{Z}$! $2 \mid 6$ means $(6) \subseteq (2)$, i.e. all multiples of 6 are also multiples of 2. The "smaller" the generator, the larger the ideal is.

18.4 GCD

Definition 18.9 (Greatest common divisor)**.** Let R be a commutative ring with $1 \neq 0$. Let $a, b \in R$ with $b \neq 0$. Then, d is a **greatest common divisor** of a and b (denoted by $\gcd(a, b)$) if

1. $d \mid a$ and $d \mid b$,
2. if $0 \neq d' \in R$ satisfies $d' \mid a$ and $d' \mid b$, then $d' \mid d$. (Equivalently, if $a \in (d')$ and $b \in (d')$, then $(d) \subseteq (d')$.

An equivalent definition:

Definition 18.10 (GCD, defined by ideals)**.** A **greatest common divisor** of a and b (if it exists) is a generator for the smallest principal ideal containing both a and b.

> **Remark 18.11.** Note we say "a" greatest common divisor, not "the." Turns out that GCDs are unique up to units, i.e. any two GCDs of two elements differ by a factor of a unit. However, the ideal generated by any two GCDs are the same, so we have uniqueness when discussing GCDs in the language of ideals. Yet another reason why we love ideals!

Example 18.12 (GCD is not unique)

To expand on the above: in $\mathbb{Z}$, we could have $\gcd(2, 2)$ as either 2 or -2, which are clearly different as elements, but $(2) = (-2) = 2\mathbb{Z}$. In a field F, if we take any two non-zero $a, b \in F$, then $\gcd(a, b)$ could be any non-zero element in F!

Example 18.13 (GCD may not exist!)

Even if R is something nice like an integral domain, the GCD may not always exist! Consider the ring $R = \mathbb{Z}[\sqrt{-3}]$. Clearly there exists GCDs in some cases, e.g. $\gcd(2, 2)$ is either 2 or -2. But consider $a = 4$ and $b = 2(1 + \sqrt{-3})$. Note we can factor

$$a = 4 = 2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3}),$$

so one may think that 2 or $1 + \sqrt{-3}$ can be the GCD, but $2 \nmid 1 + \sqrt{-3}$ and $1 + \sqrt{-3} \nmid 2$, so it doesn't satisfy the definition of GCD. Spooky stuff.

Example 18.14 ($\gcd(2, x)$)

Example 17.8 tells us that $(2, x)$ is maximal, and Claim 17.1 informs us that it is not principal. Thus, we see that any principal ideal containing both 2 and x must strictly contain $(2, x)$, but then by maximality, the principal ideal must be $(1) = R$ itself. Thus, $\gcd(2, x) = 1$ (or -1).

As a consequence of the second definition of GCD:

Proposition 18.15

If $a, b \in R$ are non-zero elements and $(a, b) = (d)$, then d is a greatest common divisor of a, b in R.

Theorem 18.16

Let R be a Euclidean domain with $a, b \in R$ non-zero. Let $d = r_n$ be the last non-zero remainder in the Euclidean algorithm for a and b. Then,

1. d is a GCD of a, b,
2. $(d) = (a, b)$. In particular, $d = ax + by$ for $x, y \in R$.

Proof. Let R be an Euclidean domain with norm N. Let $a, b \in R$ non-zero and $d = r_n$ as in the statement. We will show $(a, b) = (d)$ via inclusion in both directions.

Showing $(a, b) \subseteq (d)$ is equivalent to showing $d \mid a$ and $d \mathcal{I} b$. Our Euclidean algorithm looks like

$$\begin{aligned} a &= q_0 b + r_0 \\ b &= q_1 r_0 + r_1 \\ &\vdots \\ r_{n-2} &= q_n r_{n-1} + r_n \\ r_{n-1} &= q_{n+1} r_n, \end{aligned}$$

where $N(r_n) < N(r_{n-1}) < \cdots < N(r_1) < N(r_0) < N(b)$ and each $r_i \neq 0$. We prove by induction down to 0 that $r_n \mid r_i$ for all $i \leq n$.

It is obvious when $i = n$. Let $k \leq$ and assume $r_n \mid r_i$ for all $k \leq i \leq n$. But then we have $r_{k-1} = q_{k+1} r_k + r_{k+1}$, so r_n divides the right hand side, which means $r_n \mid r_{k-1}$, completing the inductive step. Thus, $r_n \mid q_1 r_0 + r_1 = b$, so $r_n \mid q_0 b + r_0 = a$, as desired.

Now we show $(a, b) \supseteq (d)$. It suffices to show $d = r_n \in (a, b)$. We will show $r_i \in (a, b)$ for all i via induction upwards. Since we can express $r_0 = a - q_0 b$, we have $r_0 \in (a, b)$, completing the base case. Suppose $r_i \in (a, b)$ for $0 \leq i \leq k$. Then, $r_{k+1} = r_{k-1} - q_{k+2} r_k \in (a, b)$, completing the inductive step. Thus, we can conclude $d = r_n \in (a, b)$.

The first statement follows from proposition immediately above. □

18.5 Principal Ideal Domains

I've admittedly been talking about principal ideal domains for a while, but I guess we never explicitly defined them in class, so:

> **Definition 18.17** (Principal ideal domain)**.** An integral domain is called a **principal ideal domain** (PID) if every ideal I of R is principal.

Corollary 18.18

If R is a PID and $a, b \in R$ are two non-zero elements, then $\gcd(a, b)$ always exists.

Proof. Consider the ideal (a, b). R is a PID, so $(a, b) = (d)$ must be a principal ideal. By the above theorem (18.16), $d = \gcd(a, b)$, done. □

So to recap, we have the following inclusions: all fields are Euclidean domains, all Euclidean domains are PIDs, and all PIDs are integral domains.

Example 18.19 (Rings in each layer)

$\mathbb{Q}$ is a field. $\mathbb{Z}$ is a Euclidean domain which is not a field. Using Example 18.13 as inspiration, $\mathbb{Z}[\sqrt{-3}]$ is a PID (not obvious a priori but believe me) but not a Euclidean domain. $\mathbb{Z}[x]$ is an integral domain but not a PID (we know $(2, x)$ is not principal).

Proposition 18.20

Every non-zero prime ideal in a PID is maximal.

This gives concrete justification to our claim that "all prime ideals of $\mathbb{Z}$ (of the form $(p) = p\mathbb{Z}$ for p prime) are maximal."

Proof. Let R be a PID and $(a) \subsetneq R$ a prime ideal. Suppose $(a) \subsetneq (b)$ for $b \in R$. It suffices to show that $(a) = (b)$ or $(b) = R$.

From $(a) \subseteq (b)$, we have $a \in (b)$, so $a = rb$ for some $r \in R$. Thus, $rb \in (a)$. But (a) is prime, so either $r \in (a)$ or $b \in (a)$. If the latter, then $b \in (a) \implies (b) \subseteq (a)$ which implies $(a) = (b)$. If the former, i.e. $r \in (a)$, then $r = sa$ for some $s \in R$. Thus,

$$\begin{aligned} a &= rb = sab \\ \implies a(1 - sb) &= 0 \\ \implies 1 &= sb \\ \implies 1 &\in (b) = R. \end{aligned}$$

(The third line follows from the fact that $a \neq 0$ and R is a PID, hence an integral domain.) The conclusion follows. □

19 11/16 - Prime and Irreducible Elements

Recall Proposition 18.20 above. Note that the non-zero condition is really important, as $\{0\} = (0)$ is always a prime ideal, but it is almost never maximal. (Before moving on, can you determine for which rings (0) is maximal?)

Corollary 19.1

If R is an integral domain such that $R[x]$ is a PID, then R is a field.

We know from Corollary 18.8 that $\mathbb{Z}[x]$ is not a Euclidean domain. From this corollary, we can strengthen this statement: $\mathbb{Z}[x]$ is not even a PID since $\mathbb{Z}$ is not a field. On the other hand, Example 18.5 shows (informally) $\mathbb{Q}[x]$ is a Euclidean domain, hence it is a PID. This checks out, since $\mathbb{Q}$ is a field.

Proof. I won't hash out this first claim here, but one can use the First Isomorphism Theorem (using the map $R[x] \to R$ mapping $p(x) \mapsto p(0)$) to show $R[x]/(x) \simeq R$. This means (x) is a prime ideal, since R is, by assumption, an integral domain. But if $R[x]$ is a PID, then Proposition 18.20 tells us that (x) must be maximal, which is equivalent to saying $R[x]/(x) \simeq R$ is a field, and we conclude. □

19.1 Prime vs Irreducible

We now make a very important distinction. We start in the integers, where this distinction is not necessary. We know that any integer has a unique prime factorization, e.g. if I give you 2022, you can factor it into $2 \times 3 \times 337$ and this factorization is unique up to ordering of the primes. And luckily, these primes obey our definition of primes we discussed before defining prime ideals (Definition 17.12); namely, $p \in \mathbb{Z}$ is prime if $p \mid ab \implies p \mid a$ or $p \mid b$.

However, things aren't always so nice. (Both a blessing and a curse in math: a curse for obvious reasons, but a blessing because some *really* interesting math arises from this. Yet another plug for Math 123/129!)

Example 19.2 (When unique factorization fails)

Consider the ring $\mathbb{Z}[\sqrt{-5}]$. We have the following factorizations of 6:

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

We can't "break down" each of the four terms $2, 3, 1 + \sqrt{-5}, 1 - \sqrt{-5}$ any further, and yet they are not prime: we have $2 \mid (1 + \sqrt{-5})(1 - \sqrt{-5})$ but 2 does not divide either of the terms in $\mathbb{Z}[\sqrt{-5}]$.

The above example suggests that the notion of a "prime," which brought us to the definition of a prime ideal, is different from the notion of an "irreducible" element, something which "can't be broken down into something smaller." (Many words here are not well-defined, but the big picture is what's important.) We'll attempt to define this rigorously.

Definition 19.3 (Irreducible). Let R be an integral domain. Suppose $r \in R \setminus \{0\}$ is not a unit. Then, r is called **irreducible** if whenever $r = ab$, $a, b \in R$, then one of a or b is a unit. Otherwise, r is reducible.

Thus, any $r \in R$ is either a unit, irreducible, or reducible.

Exercise 19.4. Find a unit, irreducible, and reducible element in $\mathbb{Z}$, respectively.

We contrast this with our definition of prime:

> **Definition 19.5** (Prime element)**.** A non-zero element $p \in R$ is **prime** if it is not a unit and if $p \mid ab$ for $a, b \in R$, then $p \mid a$ or $p \mid b$. Equivalently, $0 \neq p \in R$ is prime iff (p) is a prime ideal of R.

Finally, we only care about elements up to multiplication by units. For example, we could factorize 2022 as $-2 \cdot -3 \cdot 337$; by our definition of prime/irreducible (they're the same in $\mathbb{Z}$), -2 and -3 are still primes/irreducibles, but this is clearly not "exactly" the same factorization as $2 \cdot 3 \cdot 337$. But we can declare them to be the same, by saying they are the same up to multiplication by units. We call these *associates*.

> **Definition 19.6** (Associates)**.** Elements $a, b \in R$ are **associates** iff $(a) = (b)$, or equivalently, iff $a = ub$ for some unit $u \in R^\times$.

19.2 Relating Primes with Irreducibles

We've stated already that in $\mathbb{Z}$, primes and irreducibles are the same. We can make a slightly more general statement to relate primes and irreducibles:

Proposition 19.7

In an integral domain, a prime element is always irreducible.

Proof. Let $p \in R$ be a prime element. Say $p = ab$ for $a, b \in R$. We wish to show a or b is a unit. By definition, we know (p) is prime, which means either $a \in (p)$ or $b \in (p)$. WLOG, suppose $a \in (p)$. Then, $a = p \cdot c$ for some $c \in R$. Then,

$$p = ab = pcb \implies p(1 - cb) = 0.$$

By definition, $p \neq 0$ as p is prime, so $1 = cb = bc$, which means $b \in R^\times$, as desired. □

Okay, that's cool, but when is an irreducible element prime? We already observed this is true in $\mathbb{Z}$. Turns out it is true in any PID.

Proposition 19.8

In a PID, a non-zero element is prime iff it is irreducible.

Proof. We know any prime ideal is irreducible by Proposition 19.7 and the fact that any principal ideal domain is an integral domain. So we just need to show every irreducible is prime.

Assume that $p \in R$ is irreducible; we wish to show (p) is prime. Fact 17.15 (all maximals are prime) and Proposition 18.20 (every non-zero prime ideal is maximal in a PID) tells us that in a PID, an ideal is prime iff it is maximal. Thus, as $(p) \neq (0)$, it suffices to show (p) is maximal.

Suppose M is an ideal such that $M \supseteq (p)$. It suffices to show $M = (p)$ or $M = R$. Since R is a PID, we may write $M = (m)$ for some $m \in M$. Then, $(p) \subseteq (m)$ means $p = mr$ for some $r \in R$. But p is irreducible, so either $r \in R^\times$ or $m \in R^\times$. If $r \in R^\times$, then p, m are associates, so by definition $(p) = (m) = M$. Otherwise, if $m \in R^\times$, then $(m) = R$ (it is clearly contained in R, but any $r \in R$ can be expressed as $m \cdot m^{-1}r \in (m)$, so $(m) \supseteq R$), and we conclude. □

19.3 Interlude: Chinese Remainder Theorem

We take a brief commercial break from our discussion of primes and irreducibles to introduce the Chinese Remainder Theorem. Some of you may have seen this in the context of the integers, but this is a more general (and equally important) statement in integral domains.

> **Author's Note 19.9.** Chinese Remainder Theorem is often abbreviated as CRT, not to be confused with critical race theory. Don't be scared, Ron DeSantis!

Here's the situation for the integers. Suppose $a, b \in \mathbb{Z}$ are coprime, i.e. $\gcd(a, b) = 1$. Then, if I take any $0 \leq r_1 < a$ and $0 \leq r_2 < b$, then I can guarantee $\exists\, x \in \mathbb{Z}$ such that $x \equiv r_1 \pmod{a}$ and $x \equiv r_2 \pmod{b}$. Moreover, this is unique modulo ab, i.e. if $y \equiv r_1 \pmod{a}$ and $y \equiv r_2 \pmod{b}$, then $x \equiv y \pmod{ab}$. This a priori seems more like a number theory fact, but we shall generalize to make it more algebraic.

Let's break down the above, starting from the very top. We supposed $a, b \in \mathbb{Z}$ are coprime. Well, what does coprime mean in a ring in general? We'll use the following for inspiration: in the integers, if a, b are coprime (i.e. $\gcd(a, b) = 1$), then $\exists\, x, y \in \mathbb{Z}$ such that $ax + by = 1$. This means that any $n \in \mathbb{Z}$ can be written as a linear combination of a and b.

> **Definition 19.10** (Comaximal/coprime)**.** The ideals A and B of a ring R are **comaximal** or **coprime** if $A + B = R$. Recall the sum of two ideals is the set $\{a + b \mid a \in A, b \in B\}$.

Relating this to what we said about the integers:

> **Lemma 19.11**
>
> If R is a PID and $a, b \in R$ with $\gcd(a, b) = 1$, then $(a) + (b) = R$.

Proof. We have $\gcd(a, b) = 1 \implies (a, b) = (1) = R$, so $1 = ax + by \implies 1 \in (a) + (b) \implies R = (1) \subseteq (a) + (b)$. But inclusion in the other direction is obvious, so equality follows. □

Let's go back to breaking down our little blurb about CRT for the integers. The rest of the paragraph is just two statements: existence of an integer that satisfies both congruence relations, and uniqueness of that integer up to mod ab. Let's address the existence statement first.

Recall that $\mathbb{Z}/n\mathbb{Z}$, being a quotient ring, can be thought of as cosets of our ideal (n). Thus, $x \equiv r_1 \pmod{a}$ is equivalent to saying $x+(a) = r_1+(a)$ in $\mathbb{Z}/(a)$, so we can generalize by saying $\exists\, x \in R$ such that $x + (a) = r_1 + (a)$ in $R/(a)$ and $x + (b) = r_2 + (b)$ in $R/(b)$. Equivalently, $\exists\, x \in R$ such that

$$(x + (a), x + (b)) = (r_1 + (a), r_2 + (b))$$

in $R/(a) \times R/(b)$. (This is a product ring, which I'm too lazy to rigorously define, but it's a set where addition and multiplication are defined coordinate-wise. The ring structure follows because it is a ring in each coordinate.)

The nice thing is that uniqueness is embedded into the language. This may be easiest seen in the integers: if $x, y \in \mathbb{Z}$ satisfy $x \equiv y \pmod{ab}$, then $(x+(a), x+(b)) = (y+(a), y+(b))$ in $R/(a) \times R/(b)$ by construction.

We now state the "more general" version of CRT (I put "more general" in quotations because the correct perspective should be that the integer case is a specific example of CRT, not the other way around).

Theorem 19.12 (Chinese Remainder Theorem)
Let R be an integral domain and $A, B \subset R$ are ideals. Then, the map

$$\begin{aligned} \varphi : R &\to R/A \times R/B \\ r &\mapsto (r + A, r + B) \end{aligned}$$

is a ring homomorphism with $\ker \varphi = A \cap B$. If further A and B are comaximal, then

$$R/AB \cong R/A \times R/B.$$

To give a super abbreviated version of the proof, it goes like this: if A, B are comaximal, observe $A \cap B = AB = \{\sum_{i=1}^{n} a_i b_i \mid a_i \in A, b_i \in B\}$ and $\operatorname{Im} \varphi = R/A \times R/B$, so the result follows from First Isomorphism Theorem. We flesh this out:

Proof. We first show φ is a ring homomorphism. This is pretty chill:

$$\begin{aligned} \varphi(r_1 r_2) &= (r_1 r_2 + A, r_1 r_2 + B) \\ &= ((r_1 + A)(r_2 + A), (r_1 + B)(r_2 + B)) \\ &= (r_1 + A, r_1 + B) \cdot (r_2 + A, r_2 + B) \\ &= \varphi(r_1)\varphi(r_2). \end{aligned}$$

Similarly, $\varphi(r_1 + r_2) = \varphi(r_1) + \varphi(r_2)$. Note that $\varphi(r) = (0 + A, 0 + B)$ iff $r + A = 0 + A$ and $r + B = 0 + B$, i.e. $r \in A$ and $r \in B$, so $r \in A \cap B \implies \ker \varphi = A \cap B$, woohoo.

finish next time? □

20 11/21 - Unique Factorization Domains

We'll finish up our discussion on the Chinese Remainder Theorem. Recall the statement from above, and let's look at some applications. We already have the application in the integers, which inspired the more general statement of the theorem in the first place.

Theorem 20.1 (CRT for PID)
Let R be a PID and $I = (a), J = (b)$ be two coprime ideals, e.g. $(a, b) = R$. Then,

$$R/(ab) \cong R/(a) \times R/(b).$$

Claim 20.2. Let $a_1 \neq a_2 \in Q$ and $b_1, b_2 \in Q$, then $\exists! f \in Q[X]$ where $\deg f \leq 1$ such that $f(a_1) = b_1$ and $f(a_2) = b_2$.

Colloquially, this means you can find a "line" that goes through two specified points. Nothing too enlightening, but the tools we've built up allows us to discuss such a geometric fact from a purely algebraic perspective, which is useful because lots of rings don't have a corresponding geometric picture (at least, for now... take Math 137/232 if you want some spice in your life).

Proof. Since $a_1 \neq a_2$, the linear terms $X - a_1$ and $X - a_2$ are comaximal, since we can write

$$1 = \frac{(X - a_1) - (X - a_2)}{a_2 - a_1} \in (X - a_1) + (X - a_2).$$

Then, CRT tells us that $Q[X]/(X - a_1) \times Q[X]/(X - a_2) \cong Q[X]/(X - a_1)(X - a_2)$, so $(b_1, b_2) \mapsto \overline{f}$ for some $f(X) \in Q[X]$, $\deg f \leq 1$. (This is because we can always reduce $f(X) = q(X)(X - a_1)(X - a_2) + r(X)$ such that $\deg r(X) < \deg(X - a_1)(X - a_2) = 2$.

Our mapping tells us that $f(X) = b_1$ in $Q[X]/(X - a_1)$, which means $f(X) = (X - a_1)P_1 + b_1$ for some constant P_1, and likewise $f(X) = (X - a_2)P_2 + b_2$. This f is unique, because if $\overline{f} = \overline{g}$ where $\deg f, \deg g \leq 1$, then $f = g + (X - a_1)(X - a_2)q$ for some constant q. But the latter term has degree 2, so we must have $q = 0$, so $f = g$. □

20.1 Unique Factorization Domains

Before we define this, let's specify where this falls into the picture of rings. These lie in between integral domains and principal ideal domains – that is, all principal ideal domain are unique factorization domains, which are always integral domains.

The name pretty much tells you what these rings are: unique factorization is guaranteed. A place where this fails: Example 19.2.

Definition 20.3 (Unique factorization domain)**.** A **unique factorization domain (UFD)** R is an integral domain in which every non-zero $r \in R$ which is not a unit has the following properties:

1. r can be written as a finite product $r = p_1 \cdots p_n$ of (not necessarily distinct) irreducibles $p_i \in R$, and
2. The above decomposition is unique up to associates, namely if $r = p_1 \cdots p_n = q_1 \cdots q_m$ for irreducible p_i, q_i, then $n = m$ and, up to permutation, q_i is associated to p_i.

Example 20.4 ($\mathbb{Z}$ is a UFD)

$\mathbb{Z}$ is a UFD: every integer has a unique prime factorization. Explicitly, we can express any non-zero $n \in \mathbb{Z}$ as $n = \varepsilon p_1 \cdots p_k$ where $\varepsilon = \pm 1$ and p_i is prime. Even more explicitly, this is unique up to associates and permutation, e.g. we count the factorizations $10 = 2 \cdot 5 = -5 \cdot -2$ as the same since $2, -2$ and $5, -5$ are each associates.

For a less obvious example:

Example 20.5 (Polynomials can form UFDs)

$\mathbb{C}[X]$ forms a UFD. The irreducible elements are of the form $\alpha X - \beta$ where $\alpha \neq 0$ and $\alpha, \beta \in \mathbb{C}$. If you know the Fundamental Theorem of Algebra, you know that any $P(X) \in \mathbb{C}[X]$ can be factored into linear terms, i.e. if $\deg P = n$, then it has exactly n complex roots, counting multiplicity. (For a baby example, the quadratic formula tells you that you can *always* factor a quadratic into linear factors, whereas this is not the case in the reals.)

Taking this in mind, we can write mathematically that $\forall\, P(X) \in \mathbb{C}[X[$, $P = c \prod_i (X - \alpha_i)$ where $c \in \mathbb{C} \setminus \{0\}$ and $\alpha_i \in \mathbb{C}$. This is unique up to permutation and associates.

Example 20.6 (Fields and UFDs)

For a stupid example, any field F is a UFD since every nonzero element is invertible. More interesting, though, is that the above example generalizes to any field F, even if F is not algebraically closed: if F is a field, then $F[X]$ is a UFD. Even more exciting, we'll prove next time that $R[X]$ is a UFD iff R is a UFD.

Now for some counterexamples. We already have a counterexample in Example 19.2, where in $\mathbb{Z}[\sqrt{-5}]$, $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$. For a slightly more pathological example:

Example 20.7 (Not UFDs)

$\mathbb{Z}[2i] = \{a + 2ib \mid a, b \in \mathbb{Z}\}$ is not a UFD. We can factor $4 = 2 \cdot 2 = (-2i)(2i)$. Although $2, 2i$ are associates in $\mathbb{C}$, they are not associates in $\mathbb{Z}[2i]$. In fact, i is not even an element in $\mathbb{Z}[2i]$!

Furthermore, it is good practice to check that the two factorizations given are indeed factorizations into irreducibles. Suppose for the sake of contradiction that 2 is not irreducible, so $2 = z_1 \cdot z_2$. Write $z_i = \alpha_i + 2i\beta_i$. Then, denoting $N(\alpha + 2i\beta) = \alpha^2 + 4\beta^2$ and noting that $N(ab) = N(a)N(b)$ (some form of this was on your problem set),

$$4 = N(2) = (\alpha_1^2 + 4\beta_1^2)(\alpha_2^2 + 4\beta_2^2).$$

If $\beta_i \neq 0$, then $\alpha_i^2 + 4\beta_i^2 \geq 4$, so some β_i must be 0. WLOG let $\beta_1 = 0$. Then, $4 = \alpha_1^2(\alpha_2 + 4\beta_2^2)$. If $\alpha_1 = 1$, then $z_1 = 1$ is a unit; if $\alpha_1 = 2$, then $(\alpha_2, \beta_2) = (0, \pm 1)$, so z_2 is a unit. This means 2 must be an irreducible. Similar arguments hold for showing $2i, -2i$ are also irreducible.

Remark 20.8. As we also saw in Example 19.2, irreducible elements are not prime when unique factorization fails. Likewise, $2i$ is not prime in $\mathbb{Z}[2i]$, since $2i \mid 2 \cdot 2$ but $2i \nmid 2$. We could also see this via the isomorphism $\mathbb{Z}[2i]/(2i) \cong \mathbb{Z}/4\mathbb{Z}$, where the isomorphism is given by the map $a + 2ib \mapsto \overline{a}$. Since $\mathbb{Z}/4\mathbb{Z}$ is not an integral domain, $(2i)$ cannot be prime.

We now reach the main result of today's class: every principal ideal domain, and thus every Euclidean domain, is a unique factorization domain.

Theorem 20.9 (All PIDs are UFDs)

If R is a PID, then R is a UFD.

An example of a UFD that is not a PID: $\mathbb{Z}[x]$. Convince yourself that it's actually a UFD, and recall from Claim 17.1 that $(2, x) \subset \mathbb{Z}[x]$ is not principal. Another example if $\mathbb{C}[x, y]$.

Proof. Let R be a PID, and let $- \neq r \in R$ which is not a unit. We need to prove the two conditions in the definition of a UFD, starting with the second one.

Assume that r has a decomposition into irreducibles. We will proceed by induction on the minimal number n of irreducible factors in some decomposition of r. The base case is $n = 1$ (if $n = 0$, then r is a unit), in which case r is itself irreducible. But then if we have some decomposition $r = q_1 \cdots q_m$, then $r \mid q_1 \cdots q_m$.

But in a PID, irreducible elements are prime, so this means $r \mid q_i$ for some i. Consequently, since q_i itself is irreducible, r and q_i are associates. WLOG letting $i = 1$, we have $r = q_1 \cdot c$ for some unit c, But then since R is an integral domain, we have $q_2 \cdots q_m = c$, which means q_2 is also invertible, a contradiction an irreducible element is by definition not invertible.

Now we proceed with our inductive step: suppose that $n \geq 1$ and uniqueness holds if r has a factorization into n irreducible elements. Assume that $r = p_1 \cdots p_{n+1} = q_1 \cdots q_m$ are two distinct factorizations into irreducibles. We can assume $m \geq n+1$, otherwise we can simply apply the inductive hypothesis on m to guarantee uniqueness.

Like before, we have $p_{n+1} \mid r = q_1 \cdots q_m$, which means $p_{n+1} \mid q_i$ for some i. WLOG let $i = 1$. Like in the base case, this means p_{n+1} is associated to q_1, so up to associates, we have $r' = p_1 \cdots p_n = q_2 \cdots q_m$. But by the inductive hypothesis on r', this means r' has unique factorization, which means $r = r' \cdot p_{n+1}$ also has unique factorization, as desired.

Now we prove the first condition in the definition of UFD: existence. Let $r \neq 0$ be a non-unit element. If r is irreducible, then we have the obvious decomposition $r = r$. Otherwise, we have $r = r_1 r_2$ where r_1, r_2 are not units. If r_1, r_2 are both irreducible, we are done (we have the factorization $r = r_1 r_2$); else, (WLOG r_1 is not irreducible) we can write $r_1 = r_3 r_4$ where r_3, r_4 are not units. This process eventually has to stop eventually. (clear up this proof next time) □

21 11/28 - More on UFDs, and Gauss's Lemma

To recap, we have all Euclidean domains are PIDs, and from the above theorem, all PIDs are UFDs. Also recall that in PIDs, we have the notion of a GCD. Turns out that we have GCDs in UFDs as well. Just think about the integer case! Say $a = up_1^{e_1} \cdots p_n^{e_n}$ and $b = vp_1^{f_1} \cdots p_n^{f_n}$, where u, v are units and p_i are irreducibles. Then, $\gcd(a,b) = p_1^{\min\{e_1,f_1\}} \cdots p_n^{\min\{e_n,f_n\}}$.

The rest of the class will be largely devoted to proving the following theorem:

Theorem 21.1 (Polynomial ring of UFD is UFD)
If R is a UFD, then $R[x]$ is a UFD.

Let's see what this means in practice. Recall that $\mathbb{Z}[x]$ is *not* a PID, since the ideal $(2, x)$ is not principal (Claim 17.1). However, $\mathbb{Z}$ is a UFD, so this theorem tells us that $\mathbb{Z}[x]$ is a UFD. This is an interesting case with respect to GCDs: in PIDs, if $\gcd(a,b) = d$, then $\exists\, x, y \in R$ such that $ax + by = d$, but this is not necessarily the case in UFDs, even if GCDs always exist. For example, the gcd of 2 and x is 1, but $1 \notin (2, x)$.

Example 21.2 (Polynomial rings as UFDs)
From above, $\mathbb{Z}[x]$ is a UFD but not a PID. But if we apply the theorem on $\mathbb{Z}[x]$ itself, then we have that $(\mathbb{Z}[x])[y] = \mathbb{Z}[x, y]$ is also a UFD. We can adjoin an arbitrary number of variables to get...

Corollary 21.3
If R is a UFD, then $R[x_1, \ldots, x_n]$ is also a UFD.

21.1 Field of fractions

To prove Theorem 21.1, we'll introduce the notion of a **field of fractions**. This corresponds to Section 7.5 in Dummit and Foote.

Start with an integral domain; for the mot canonical example, take $\mathbb{Z}$. Then, $\mathbb{Q}$ is the field of fractions of $\mathbb{Z}$, since any element in $\mathbb{Q}$ can be expressed as $\frac{a}{b}$ where $b \neq 0$ and $a, b \in \mathbb{Z}$. Our goal is to generalize this; I'll point out some subtleties before proceeding.

First, the $b \neq 0$ is important, so we'll keep this condition moving forward. Second, these fractions are technically defined up to equivalence classes, where the equivalence relation in $\mathbb{Q}$ is just equality. To demonstrate, note that $1/2$ and $2/4$ are the same fraction even though they are written differently, so we have this notion of equivalence that a priori doesn't exist if we just say "all elements of $\mathbb{Q}$ are of the form $\frac{a}{b}$."

So as the name suggests, we're going to take an integral domain R and then force it to become a field, i.e. make every non-zero element have an inverse. We do this by constructing fractions where the numerator and denominator are both in R, then saying two fractions are equal if you can "simplify" one to the other.

21.2 Construction of Field of Fractions

Enough with the big-picture talk; let's construct a fraction formally. Take $R \times (R \setminus \{0\}) = \{(a, b) \mid a, b \in R, b \neq 0\}$. Define the relation $(a, b) \sim (a', b') \iff ab' = a'b$. This is an equivalence relation (left as exercise to the reader haha, but believe me for now).

Now, we may define a **fraction** $\frac{a}{b}$ to be the **equivalence class** of (a, b). Again, going back to the $1/2 = 2/4$ case, the equivalence class of $(1, 2)$ when $R = \mathbb{Z}$ is the set $\{(1, 2), (-1, -2), (2, 4), \dots\}$.

Great, now we have a set of equivalence classes. We want this to be a ring (more specifically, a field), so we want to endow it with addition and multiplication operations. This is going to be just like how we do it for the rationals: we define

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$
$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

We must check that these operations are well-defined. I'm going to largely leave this as an exercise because it's tedious and not very enlightening, but this is how you'd start: if $(a, b) \sim (a', b')$ and $(c, d) \sim (c', d')$, then we want $\frac{a}{b} + \frac{c}{d} = \frac{a'}{b'} + \frac{c'}{d'}$, i.e. $\frac{ad+bc}{bd} = \frac{a'd'+b'c'}{b'd'}$, i.e. $b'd'(ad + bc) = bd(a'd' + b'c')$. Now use the fact that $(a, b) \sim (a', b')$ and $(c, d) \sim (c', d')$ to finish.

Since we have the addition and multiplication operations, we now have a ring, and it's clear from construction that this is a field.

Definition 21.4 (Field of fractions)**.** Given an integral domain R, the field of fractions of R is

$$F = \{a/b \mid a, b \in R, b \neq 0\}/ \sim,$$

where $a/b \sim c/d$ iff $ad = bc$.

Example 21.5 (Fraction field of Rational Polynomials)
The field of fractions of $\mathbb{Q}[x]$ is $\mathbb{Q}(x) = \{f(x)/g(x) \mid f(x), g(x) \in \mathbb{Q}[x], g(x) \neq 0\}$. An example of an element in $\mathbb{Q}(x)$ is $x^2 + \frac{2}{x^3+5x-4}$.

A few remarks. First, I oftentimes see the field of fractions denoted as $K(R)$. Second, although having the rationals as your standard example is useful, remember that "a/b" is just a formal symbol denoting an equivalence class. We could've written the elements of F as $\overline{(a,b)}$ to demonstrate this more clearly, but that's clunky and less intuitive.

Next, we always have an injection from the ring R to its field of fractions, since any ring element r corresponds to the fraction $\frac{r}{1}$. And finally, to bring this back to $R[x]$ (Theorem 21.1, which is why we brought up field of fractions in the first place), note that since $R \subseteq F$, we have $R[x] \subseteq F[x]$. But F is a field, so $F[x]$ is a Euclidean domain, hence a UFD.

But this doesn't yet give us Theorem 21.1, since the above remark only tells us that $R[x]$ can be uniquely factored into irreducibles in $F[x]$, but we want to factor it into irreducibles in $R[x]$. The next result, though, will ensure that unique factorization in $F[x]$ suffices.

21.3 Gauss's Lemma

Theorem 21.6 (Gauss's Lemma)
Let R be a UFD with field of fractions F. Let $p(x) \in R[x]$. If $p(x) \in F[x]$ is reducible in $F[x]$, then it is reducible in $R[x]$. More precisely, if $p(x) = A(x)B(x)$ for non-constant polynomials $A(x), B(x) \in F[x]$, then there exists non-zero $r, s \in R$ such that $\frac{r}{s}A(x) = a(x) \in R[x]$ and $\frac{s}{r}B(x) = b(x) \in R[x]$.

Remark 21.7. Note that the converse is not true. In $\mathbb{Z}[x]$, the polynomial $2(1+x)$ is reducible, but since 2 is a unit in $\mathbb{Q}$, $2+2x$ is irreducible in $\mathbb{Q}[x]$.

To prove Gauss's Lemma, we will use the following lemma, a generalization of Proposition 19.8 for UFDs.

Lemma 21.8
In UFDs, irreducibles are primes.

Proof. Let R be a UFD and suppose $p \in R$ is irreducible. We wish to show p is prime. Suppose $p \mid ab$ for $a, b \in R$, so $ab = cp$ for some $c \in R$. Writing each term as a product of irreducibles (with the factorization of p being itself), it must follow that p is associates with some irreducible factor of either a or b, which means either $p \mid a$ or $p \mid b$, as desired. □

Now we prove Gauss's Lemma.

Proof. Let $p(X) \in R[x]$. Suppose $p(x)$ factors in $F[x]$ as $p(x) = A(x)B(x)$ where $A(x), B(x) \in F[x]$. Putting all coefficients of A and B, respectively, under the same denominator, we can write $A(x) = \frac{1}{r}A'(x)$ and $B(x) = \frac{1}{s}B'(x)$ for some $r, s \in R$, with $A(x), B(x) \in R[x]$. Thus, we have $rs \cdot p(x) = A'(x)B'(x)$.

Suppose $d = rs \in R$. If d is a unit in R, then $p(x) = d^{-1}A'(x)B'(x)$, and we get our desired result. If not, then we may write $d = p_1 \cdots p_k$ where each $p_i \in R$ is irreducible. We're going to show that each p_i also divides the right side in $R[x]$, which will give us our desired result.

To show the right side is divisible by p_i, we will consider the equation in the quotient ring $R[x]/(p_i)$. By the above lemma, every irreducible is prime, so each p_i is prime. This means R/p_iR is an integral domain, which further means $R/p_iR[x] = R[x]/(p_i)$ is also an integral domain.

Start with $i = 1$. We can reduce the equation $rs \cdot p(x) = A'(x)B'(x)$ mod p_1 to get $0 = \overline{A'(x)} \cdot \overline{B'(x)}$. But we are working in an integral domain, so this means either $\overline{A'(x)} = 0$ or $\overline{B'(x)} = 0$. WLOG suppose the former. Then, all coefficients of $A'(x)$ are divisible by $p_1 \in R$, so we can write $A'(x) = p_1 \cdot A''(x)$ for some $A'' \in R[x]$, and thus we have $p_2 \cdots p_k \cdot p(x) = A''(x) \cdot B'(x)$.

Continuing this process, we can cancel out all the irreducibles p_i to get $p(x) = a(x) \cdot b(x)$ for some $a(x), b(x) \in R[x]$, and we may conclude. □

> **Author's Note 21.9.** The "continuing this process" is hand-wavy, I admit. The proofs I've encountered are slightly more formal, but this is the general idea: you factor the polynomial in $F[x]$, scale each factor such that it lives in $R[x]$, then take the equation modulo the irreducibles in R to show that one of your factors is divisible by the irreducible.

Corollary 21.10

Let R be a UFD, F its field of fractions, and $p(x) \in R[x]$. Suppose that the gcd of the coefficients of $p(x)$ is 1. Then, $p(x)$ is irreducible in $R[x]$ iff $p(x)$ is irreducible in $F[x]$.

Proof. By Gauss's Lemma, if $p(x)$ is reducible in $F[x]$, then it it reducible in $R[x]$. Conversely, if $p(x)$ is reducible in $R[x]$, then $p(x) = a(x)b(x)$ where $a(x), b(x) \in R[x]$ are not units. Even better, they are non-constant since the gcd of the coefficients of $p(x)$ is 1. (If $a(x) = c$ were a constant, then c would divide every coefficient of $p(x)$.) Thus, $a(x), b(x)$ are non-units in $F[x]$, so $p(x)$ is reducible in $F[x]$. □

Great, NOW we can finally prove Theorem 21.1.

Proof. Showing that $R[x]$ is a UFD requires that for every $f \in R[x]$, there exists a factorization of $f(x)$ and that factorization is unique. First, we will show existence of factorization for any element in $R[x]$. Take any $f \in R[x]$. Suppose the gcd of the coefficients of f is d, so we have $f(x) = d \cdot g(x)$ for some $g \in R[x]$. Then, if we have a factorization of g, then we have a factorization of $d \cdot g(x) = f(x)$, so it suffices to show that any polynomial whose coefficients have gcd 1 has a factorization.

For notational purposes, we will call the gcd of the coefficients of f as the *content* of f, denoted $c(f)$. So we can assume $c(f) = 1$.

Let $p(x) \in R[x]$ such that the gcd of its coefficients is 1. Thinking of $p(x) \in R[x]$ as a polynomial in $F[x]$, where $F = K(R)$, we have $p(x) = p_1(x) \cdots p_n(x)$, where each $p_i(x) \in F[x]$ is irreducible. We will return to this later.

We know $F[x]$ is a UFD, so we can factor $p(x) = A(x)B(x)$ for some $A(x), B(x) \in F[x]$. We can clear out denominators in the coefficients of A and B by some constants $c_1, c_2 \in F$, respectively, such that $\widetilde{A}(x) = c_1 \cdot A(x) \in R[x]$, $\widetilde{B}(x) = c_2 \cdot B(x) \in R[x]$, and $c(\widetilde{A}) = c(\widetilde{B}) = 1$. Then, $c_1c_2p(x) = \widetilde{A}\widetilde{B}$. Note that since $\widetilde{A}\widetilde{B} \in R[x]$ and $c(p) = 1$, c_1c_2 must be in R.

If c_1c_2 is a unit, then we are happy. Else, $\exists\, a$ irreducible dividing c_1c_2. This means that $a \mid \widetilde{A}\widetilde{B}$. Considering our polynomials in $R/(a)[x]$ and noting that a irreducible (hence prime) means $R/(a)$ is integral, we have $\widetilde{A}\widetilde{B} = 0$ in $R/(a)[x]$, forcing one of them to be 0. WLOG $a \mid \widetilde{A}$, so $a \mid c(\widetilde{A}) = 1$. But then a is a unit, a contradiction, so c_1c_2 is a unit.

Now return to $p = p_1 \cdots p_n$ in $F[x]$. Using our above work, we can scale each p_i such that $p = c(p) \cdot \widetilde{p_1} \cdots \widetilde{p_n}$, where each $\widetilde{p_i} \in R[x]$ is irreducible in $F[x]$ and $c(\widetilde{p_i}) = 1$. But then they are clearly irreducible in $R[x]$, so we conclude the existence part.

Now we show that this factorization is unique. We know this holds over $F[x]$, as $F[x]$ is a Euclidean domain, which is always a UFD. Let $P(x) \in R[x]$. If $\deg P = 0$, then $P \in R$, and we conclude since R is a UFD. Suppose then that $\deg P > 0$, and suppose we have two factorizations

$$P(x) = a_1 \cdots a_r q_1(X) \cdots q_n(X) = b_1 \cdots b_s q_1'(x) \cdots q_m'(x),$$

where a_i, b_i are irreducible in R, and q_i, q_i' are irreducible in $R[x]$ with degree > 0 and $c(q_i) = c(q_i') = 1$.

I'm going to gloss over a few details and just say that $c(P) = a_1 \cdots a_r = b_1 \cdots b_s \in R$, but R is a UFD, so these factorizations must be unique up to units. So it suffices to show $q_1(x) \cdots q_n(x) = q_1'(x) \cdots q_m'(x)$ are the same factorization up to units.

Thinking of this product in $F[x]$ and using our above work to show that a polynomial $q(x) \in R[x]$ with $c(q) = 1$ is irreducible in $F[x]$ iff it is irreducible in $R[x]$, we have each q_i, q_i' is irreducible in $F[x]$. Because $F[x]$ is a UFD, we have $n = m$ and, up to ordering of the factors, q_i and q_i' are associates. Explicitly, $\exists\, \alpha_i \in F(x)^\times = F$ such that $q_i = \alpha_i q_i'$. Writing $\alpha_i = a_i/b_i$ for $a_i, b_i \in R$, we get $b_i q_i = a_i q_i'$. Taking the content of both, $b = c(b_i q_i) = c(a_i q_i') = a$, so $a = b$ up to units of R, meaning α_i is a unit in R. We may thus conclude. □

22 11/30 - Irreducibility Criteria

Last class lfg. We finished up the above proof at the beginning of this class, which I'm just including in the above section instead of splitting the proof across two lectures.

In the above proof, we work a lot with irreducible polynomials, which are nice when we are given that they are irreducible. But it turns out that determining if a polynomial is irreducible is a pretty tricky problem. Luckily, we have one super goated tool under our belt: Gauss's Lemma (Theorem 21.6) and the following Corollary (21.10). We'll prove a few more things:

Proposition 22.1

A polynomial of degree 2 or 3 over a field F is reducible iff it has a root in F.

Proof. We start with the forward direction. Let $P = F[x]$, and suppose $2 \leq \deg P \leq 3$. If $\deg P = 2$, then P must factor into two linear terms, which means it has a root. If $\deg P = 3$, then it either factors into three linear terms or a quadratic term and a linear term. In either case, it has a linear term factor which means it has a root.

For the reverse direction, if P has a root, then P has a linear factor. Since $\deg P > 1$, it follows that P is reducible, yay. □

Now we will investigate cases where we attempt to recover information on irreducibility in our original ring given information in a quotient ring. Recovering information on reducibility is easy. As an example, take the polynomial $P(x) = (X-1)(x-2)$ in $\mathbb{Z}[x]$. Modulo p, for some prime p, we get $\overline{P}(x) = (x-1)(x-2)$ in $\mathbb{Z}/p\mathbb{Z}[x]$. Thus, $\overline{p}$ is reducible implies p is also reducible.

But for irreducibility, this is not so nice. If $P(x) = (2x-1)(X-1) \in \mathbb{Z}[x]$ and we take $p = 2$, the in $\mathbb{Z}/2\mathbb{Z}[x]$, $\overline{P}(x) = -(x-1)$ which is irreducible in $\mathbb{Z}/2\mathbb{Z}[x]$, whereas $P(x)$ is reducible in $\mathbb{Z}[x]$. So we can ask,

> If I know $\overline{P}(x)$ is irreducible in $R/I[x]$, when is $P(x)$ itself irreducible in $R[x]$?

We answer:

Proposition 22.2

Let $I \subsetneq R$ be an ideal and R an integral domain. Let $P(x) \in R[x]$ be a non-constant monic polynomial. If $\overline{P}(x) \in R/I[x]$ cannot be factored into a product of two polynomials of smaller degree, then $P(x)$ is irreducible in $R[x]$.

Proof. If $P(x)$ is monic and reducible in $R[x]$, then we can choose monic $A(x), B(x)$ such that $P(x) = A(x)B(x)$. Taking modulo I, we have $\overline{P} = \overline{AB}$, but by our assumption we must have (WLOG) $\deg \overline{P} = \deg \overline{A}$. But since A, B, P are monic and $I \neq R$, we must have $\deg P = \deg A$ in $R[x]$, so $P = A$ and B is a unit. □

22.1 Eisenstein's Criterion

A really nice condition for irreducibility in $\mathbb{Z}[x]$. This will highlight the importance of reduction modulo p in polynomials.

Theorem 22.3 (Eisenstein Criterion)
Let p be a prime in $\mathbb{Z}$ and $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ with $n \geq 2$. Suppose $p \mid a_i$ for all $0 \leq i \leq n-1$ but $p^2 \nmid a_0$. Then, $f(x)$ is irreducible in $\mathbb{Z}[x]$ (and hence in $\mathbb{Q}[x]$).

We can generalize Eisensteion Criterion for any R UFD and $p \in R$ irreducible, but we'll stick with the $\mathbb{Z}[x]$ case for now.

Proof. Suppose f is reducible in $\mathbb{Z}[x]$, so $f = q_0q_1$ where $q_0, q_1 \in \mathbb{Z}[x]$ are monic and $\deg q_0, \deg q_1 > 0$. Reducing mod p, we have $x^n = \overline{f} = \overline{q_0q_1}$ in $\mathbb{F}_p[x]$ (for people who have not seen this notation before, $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ is the field with p elements). Then, $\overline{q_0} = x^{r_0}$ and $\overline{q_1} = x^{r_1}$ where $r_0 + r_1 = n$. Then, we can write

$$\begin{aligned} q_0 &= x^{r_0} + b_{r_0-1}x^{r_0-1} + \cdots + b_0 \\ q_1 &= x^{r_1} + c_{r_1-1}x^{r_1-1} + \cdots + c_0, \end{aligned}$$

where $p \mid b_0, c_0$. But then $a_0 = f(0) = q_0(0) \cdot q_1(0) = b_0c_0$ and $p^2 \nmid a_0$ but $p^2 \mid b_0c_0$, a contradiction. This, f is irreducible. □

Let's apply Eisenstein's Criterion on some concrete examples (yum!):

> **Exercise 22.4.** Let $f(x) = x^3 + 6x^2 + 12x + 18$. Show that $f(x)$ is irreducible in $\mathbb{Q}[x]$.

Proof. Seems pretty hard a priori, but with Eisenstein's Criterion in our hands, we just need to consider mod $p = 2$. Note $2 \mid 6, 12, 18$ but $2^2 \nmid 18$, so f is irreducible. □

A clever use of the criterion:

> **Exercise 22.5.** Let $f(x) = x^4 + 1$. Show that $f(x)$ is irreducible in $\mathbb{Q}[x]$.

Proof. We can't use Eisenstein directly, but the key observation is that a polynomial stays irreducible under transformation, i.e. $f(x)$ is irreducible iff $f(x + \alpha)$ is irreducible. We can compute $f(x+1) = (x+1)^4 + 1 = x^4 + 4x^3 + 6x^2 + 4x + 2$, and we can use Eisenstein's Criterion for $p = 2$ like above, yay. □

Alright, that's a wrap for the semester. Congrats on finishing! And good luck with finals :)