MATH 122, FALL 2018

WITH ANA BALIBANU

CONTENTS

1. LECTURE 1 — SEPTEMBER 5, 2018

The rough outline for the course is:

(1) Group theory
(2) Ring theory
(3) Vector spaces + (more advanced linear algebra)

Homework is assigned on Wednesdays and due the following Wednesday. Office hours can be found on the syllabus.

Textbooks: *Abstract Algebra* by Dummit and Foote, *Algebra* by Michael Artin.

So what is a group?

Motivation: In math, we're interested in symmetries of objects with structure. For example:

- polygons: the symmetries are sequences of rotations and reflections carrying the shape onto itself.
- vector space $\mathbb{R}^n$: a symmetry of this object should preserve the vector space structure, i.e. linear maps $f : \mathbb{R}^n \to \mathbb{R}^n$. These in turn correspond to $n \times n$ matrices. However, when we think of symmetries, we think of things that can be "undone." So we want our symmetries to be invertible, i.e. that our $n \times n$ matrices should be invertible. This space of symmetries of $\mathbb{R}^n$ is usually denoted $\mathrm{Gl}_n(\mathbb{R})$, the space of invertible $n \times n$ matrices.

Generally, we have the following properties of symmetries:

(1) "doing nothing" is a symmetry.
(2) "doing" should be invertible.
(3) "doing" is associative.

This gives us our formal definition:

Definition 1.1. A **group** $(G, *)$ is a set G, together with a binary operation $* : G \times G \to G$ such that

(1) (Identity): $\exists\, e \in G$ such that for all $a \in G$, $a * e = e * a = a$.
(2) (Invertibility) $\forall\, a \in G$, there exists $a^{-1} \in G$ such that $a * a^{-1} = a^{-1} * a = e$.
(3) (Associativity) $\forall\, a, b, c \in G$, we have $a * (b * c) = (a * b) * c$

Example 1.2.
- $G = \{\text{symmetries of a hexagon}\}$, $*$ is composition of symmetries.
- $G = \mathrm{Gl}_n(\mathbb{R})$ with $*$ being matrix multiplication, and $e = I_n$.
- $G = \mathbb{Z}$ with $* = +$, $e = 0$, "a^{-1}" $= -a$. Also, $(\mathbb{R}, +), (\mathbb{Q}, +), (\mathbb{R}, +)$.
- $(\mathbb{R}, \cdot)$ is not a group, since 0 is not invertible.
- $(\mathbb{R} \setminus \{0\}, \cdot)$ with $e = 1$, $a^{-1} = 1/a$ is a group. Likewise with $\mathbb{Q} \setminus \{0\}$, $\mathbb{C} \setminus \{0\}$.
- $(\mathbb{Z} \setminus \{0\}, \cdot)$ **not** a group, $2^{-1} \notin \mathbb{Z}$. But $(\{\pm 1\}, \cdot)$ is a group.

Example 1.3. Let A be a finite set. Then let $G = \{f : A \to A \mid \text{ bijective}\}$ is a group with $* = \circ$, composition, and e identity.
As a subexample, we can take $A = \{1, 2, \ldots, n\}$. Then we denote $G = S_n$, the group of permutations on n letters. This group has $n!$ elements.
As a subsubexample, take $n = 3$. Then let τ be a permutation such that $\sigma(1) = 2$ and $\sigma(2) = 1$, while τ be such that $\tau(2) = 3$ and $\tau(3) = 2$. Then $\sigma \circ \tau(1) = 2$, $\sigma \circ \tau(2) = 3$, $\sigma \circ \tau(3) = 1$. However, $\tau \circ \sigma(1) = 3$, $\tau \circ \sigma(2) = 1$, $\tau \circ (3) = 2$. In this case, $\sigma \circ \tau \neq \tau \circ \sigma$, so the group operation is **not** commutative.

Definition 1.4. A commutative group is called **abelian**.

Example 1.5. $(\mathbb{Z}, +)$, $(\mathbb{R} \setminus \{0\}, \cdot)$, $(\pm 1, \cdot)$ are all abelian.

Example 1.6. S_3, S_n for $n \geq 3$ and GL is $\mathrm{Gl}_n(\mathbb{R})$, $n \geq 2$ are all **non-abelian**.

We will now introduce a class of abelian groups that will be absolutely essential to our remaining study of group theory.

Definition 1.7. Given $a, b \in \mathbb{Z}$, $n \in \mathbb{N}$, a is **congruent** to b modulo a if $n \mid (b - a)$, i.e. $b = a + nk$. This is often written as $a \equiv b \mod n$

Proposition 1.8. *(1) (Reflexivity): $a \equiv a \mod n$.*
(2) (Transitivity): $a \equiv b(n)$ and $b \equiv c(n)$ then $a \equiv c \mod n$.
(3) (Symmetry): $a \equiv b(n)$ implies that $b \equiv a(n)$.
In other words, "$\equiv$" $\mod n$ is an equivalence relation.

This proposition implies that every integer belongs to a unique congruence class modulo n. Given $a \in \mathbb{Z}$, we write $\bar{a} = \{b \in \mathbb{Z} \mid a \equiv b \mod n\}$ is the **congruence class** of a.

Example 1.9. Given $n = 2$, we have the congruence classes $\bar{0} = \{b \in \mathbb{Z} \mid b \equiv 0 \mod 2\} = \{\text{even integers}\}$ and $\bar{1} = \{b \in \mathbb{Z} \mid b \equiv 1 \mod 2\} = \{\text{odd integers}\}$. Note of course $\bar{0} = \bar{2} = \bar{-4} = \dots$.

Definition 1.10. The set of congruence classes $\mod n$ is denoted $\mathbb{Z}/n\mathbb{Z}$. It has n elements, $\{\bar{0}, \bar{1}, \dots \bar{n-1}\}$.

Proposition 1.11. *If $a \equiv c \mod n$ and $b \equiv d \mod n$ then $a + b \equiv c + d \mod n$. Thus, addition makes sense in $\mathbb{Z}/n\mathbb{Z}$, as $\bar{a} + \bar{b} = \bar{a + b}$.*

Example 1.12. Take $n = 5$. Then $\mathbb{Z}/5\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$. We have things like $\bar{3} + \bar{4} = \bar{7} = \bar{2}$.

The proposition above actually tells us that $\mathbb{Z}/n\mathbb{Z}$ is an abelian group! with $e = \bar{0}$ and $\bar{a}^{-1} = \bar{-a}$.

Definition 1.13. The **order** of $(G, *)$ is the cardinality of G.

Example 1.14. We have seen that $|\mathbb{Z}/n\mathbb{Z}| = n$, $|S_n| = n!$, and $|\{\pm 1\}| = 2$. Likewise, $|\mathbb{Z}| = \infty$ (lol we don't care which kind of infinity it is...)

Now for a notational convention: When writing down multiplication of group elements, we usally suppress the start. So $a * b = ab$, and $a * a * \cdots * n$ times is written as a^n.

Definition 1.15. The **order** of an element $a \in G$ is the smallest $n > 0$ such that $a^n = e$.

Example 1.16. In $(\{\pm 1\}, \cdot)$, $(-1)^2 = 1$ so that $\text{ord}(-1) = 2$ while $\text{ord}(1) = 1$. It will make sense later why we use the word "order" to talk about both elements and groups.

Example 1.17. In $\mathbb{Z}/3\mathbb{Z}$, $\bar{2} + \bar{2} + \bar{2} = \bar{6} = \bar{0}$, so $\text{ord}(\bar{2}) = 3$.

Example 1.18. In $(\mathbb{Z}, \cdot)$, what is $\text{ord}(3)$? No matter how many times you add it to itself, you never get to the identity! In this case, we say that $\text{ord}(3) = \infty$.

To look at small order groups, we encode completely the multiplication rule for G in what is called a **group table**. This is easiest to see with examples

Example 1.19. $G = \{\pm 1\}$:

	1	-1
1	1	-1
-1	-1	1

Example 1.20. $G = \mathbb{Z}/3\mathbb{Z}$:

	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$

Of course, we always expect the group table of an abelian group to be symmetric.
An old problem is the following: Given an integer n, how many groups are there of order n? This was really difficult to show, and result in thousands of pages of difficult math in the 1980s. But lucky for us, this is actually not too hard to do for very small n. The group table will help you tremendously for this.

Proposition 1.21. *Let G be a group*

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

Proof. (1) Suppose towards contradiction that there are $e, f \in G$ so that for all $a \in G$, $ae = ea = af = fa = a$. Well, using these conditions, we have that

$$f = ef = e$$

(2) Suppose there exists $b, c \in G$ such that $ab = ba = ac = ca = e$. Then

$$c = ce = c(ab) = (ca)b = eb = b$$

(3) Homework!
(4) Homework!

□

2. Lecture 2 — September 10, 2018

Today we will be talking about Group homomorphisms and subgroups. If you have taken Math 101, this will be review, but don't worry
motivation: Sometimes when we look at 2 groups in our lives, we can see that they actually look really similar!

Example 2.1. We had two groups of order 2:

(1) $(\{\pm 1\}, \cdot)$. This has group table

	1	-1
1	1	-1
-1	-1	1

(2) $(S_2, \circ)$ with one nonidentity element σ with $\sigma(1) = 2, \sigma(2) = 1$. This has group table

	1	σ
1	1	σ
σ	σ	1

These group tables are the same! If we just have -1 correspond to σ, they are in some sense "the same."

To rigorize this idea, we will define the following

Definition 2.2. A **homomorphism** between two groups $(G, *), (H\circ)$ is a function $f : G \to H$ such that $f(a * b) = f(a) \circ f(b)$ for all $a, b \in G$.

These homomorphisms, much like linear maps between vector spaces, "preserve the group structure." That is, the multiplication is preserved.

Example 2.3. For $n \in \mathbb{Z}$, $\phi_n(\mathbb{Z}, +) \to (\mathbb{Z}, +)$ such that $\phi_n(k) = nk$. It is a homomorphism: $\phi_n(k_1 + k_2) = n(k_1 + k_2) = nk_1 + nk_2 = \phi_n(k_1) + \phi_n(k_2)$

Lemma 2.4. *Any homomorphism $\psi : \mathbb{Z} \to \mathbb{Z}$ is of the form ϕ_n for some $n \in \mathbb{Z}$. That is, the homomorphism is multiplication by some integer n.*

Proof. Let $n = \psi(1)$. Then for all $k > 0$, $k \in \mathbb{Z}$, $\psi(k) + \psi(1 + 1 + \cdots + 1) = \psi(1) + \cdots + \psi(1) = \psi(1) \cdot k = nk$. Checking similarly for $k \leq 0$, we get $\psi = \phi_n$, as desired. □

Example 2.5. Let $\phi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ with $\phi(k) = k \mod n$. This is pretty clearly a group homomorphism.

Example 2.6. Consider the determinant function det : $(\mathrm{GL}_n(\mathbb{R}), \circ) \to (\mathbb{R} \setminus \{0\}, \cdot)$ via $A \mapsto \det(A)$. This is a group homomorphism precisely because $\det(AB) = \det(A)\det(B)$.

Proposition 2.7. *Suppose we have a homomorphism $\phi : G \to H$. Then homomorphisms map the identity to the identity and inverses to inverses. That is:*

(1) $\phi(e_G) = \phi e_H$.
(2) For any element $a \in G$, $\phi(a^{-1}) = \phi(a)^{-1}$.

Proof. (1)

$$\begin{aligned} \phi(e) \cdot \phi(e) &= \phi(e \cdot e) = \phi(e) \\ \phi(e) \cdot \phi(e) &= \phi(e) \\ (\phi(e))^{-1} \cdot \phi(e) \cdot \phi(e) &= (\phi(e))^{-1} \cdot \phi(e) \\ \phi(e) &= e \end{aligned}$$

(2)

$$\phi(a^{-1}) \cdot \phi(a) = \phi(a^{-1} \cdot a) = \phi(e) = e$$

But remember in Lecture 1 we proved inverses are unique! Thus, $\phi(a^{-1}) = \phi(a)^{-1}$ □

To actually finish 2.4, we should use the above proposition. In particular, for any $\psi : \mathbb{Z} \to \mathbb{Z}$ such that $\psi(k) = nk$ for $k > 0$. Then using the above proposition, we have that $\psi(0) = 0$ and that for all $k < 0$, $\phi(k) = -\phi(-k) = -(n(-k)) = nk$.

Definition 2.8. We say a homomorphism $\phi : G \to H$ is an **isomorphism** if it is **bijective**. Notationally, we then write

$$G \cong H$$

Example 2.9. $(\pm 1, \cdot) \cong (S_2, \circ)$

Example 2.10. $\phi : \phi : (\mathbb{R}, +) \to (\mathbb{R}_{>0}, \cdot)$ with $\{x \in \mathbb{R}, x > 0\}$ and $\phi(x) = e^x$. We can check this a group homomorphism. For all $x, y \in \mathbb{R}$, $\phi(x + y) = e^{x+y} = e^x e^y = \phi(x)\phi(y)$. Moreover, it is injective and bijective with an inverse of the logarithm.

Example 2.11. Homomorphisms that are **not** isomorphisms:
(1) $\phi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ not injective.
(2) det not injective.
(3) $(\{0\}, +) \hookrightarrow (\mathbb{Z}, +)$ nto surjective.

Example 2.12 (Important Example: Conjugation)**.** Fix a group G and an element $g \in G$. Then define $\phi_g : G \to G$ with $a \mapsto gag^{-1}$. This is called conjugation by g. Some facts about this:

(1) It is a homomorphism: for all $a, b \in G$, we have $\phi_g(ab) = gabg^{-1} = gag^{-1}gbg^{-1} = \phi_g(a)\phi_g(b)$.
(2) It is bijective with inverse of $\phi_{g^{-1}}$. Indeed, $\phi_{g^{-1}}\phi_g(a)\phi_{g^{-1}}(gag^{-1}) = g^{-1}gag^{-1}g = a$. The other side is the exact same calculation, since $(g^{-1})^{-1} = g$.
(3) As a result, ϕ_g is an isomorphism $G \to G$, which is called an **automorphism**. Note that these conjugation homomorphisms are onyl nontrivial when G is a nonabelian group. Otherwise, we would always have $gag^{-1} = agg^{-1} = a$.

Definition 2.13. A subset $H \subset G$ is a **subgroup** if

(1) $e \in H$
(2) for all $h \in H$, $h^{-1} \in H$
(3) for all $h_1, h_2 \in H$, $h_1 \cdot h_2 \in H$.

Example 2.14. We have the chain of subgroups $(\mathbb{Z}, +) \subset (\mathbb{Q}, +) \subset (\mathbb{R}, +)$

Example 2.15. Fix $n > 0$. Then $n\mathbb{Z} = \{k \in \mathbb{Z} : n \mid k\} \subset \mathbb{Z}$ is a subgroup.

(1) $0 \in n\mathbb{Z}$
(2) $k \in n\mathbb{Z} \implies n \mid k \implies n \mid -k \implies -k \in n\mathbb{Z}$
(3) $k_1, k_2 \in n\mathbb{Z} \implies n \mid (k_1 + k_2) \implies k_1 + k_2 \in n\mathbb{Z}$

Example 2.16. $\mathbb{R} \setminus \{0\} \subset \mathbb{R}$), but $(\mathbb{R} \setminus \{0\}, \cdot)$ is **NOT** a subgroup of $(\mathbb{R}, +)$.

Example 2.17. $\{e\} \subset G$ is always a subgroup – the trivial subgroup

Proposition 2.18. *Suppose $\phi : G \to H$ is a homomorphism. The **image** of ϕ*

$$\mathrm{im}(\phi) = \{h \in H : \exists g \in G \text{ with } \phi(g) = h\}$$

is a subgroup of H.

Proof. exercise □

Definition 2.19. Let $\phi : G \to H$ be a homomorphism. The **kernel** of ϕ is $\ker(\phi) = \{g \in G : \phi(g) = e\}$.

Proposition 2.20. *$ker(\phi)$ is a subgroup of G.*

Proof. (1) $\phi(e) = e$, so $e \in \ker(\phi)$.

(2) Given $a \in \ker(\phi)$ $\phi(a^{-1}) = \phi(a)^{-1} = e^{-1} = e$. So $a^{-1} \in \ker(\phi)$.
(3) Given $a, b \in \mathbb{Z}$, $\phi(ab) = \phi(a)\phi(b) = e \cdot e = e$, implying $ab \in \ker(\phi)$.

□

Example 2.21. $\phi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ sending $k \mapsto k \mod n$ has $\ker(\phi) = n\mathbb{Z}$.

Example 2.22. $\det : \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R} \setminus \{0\}$ has $\ker(\det) = \{A \in \mathrm{GL}_n(\mathbb{R}) : \det(A) = 1\} = \mathrm{SL}_n(\mathbb{R})$, called the **special linear group**.

Example 2.23. Let $a \in G$. The subgroup **generated** by a is

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

A (sub)group generated by a single element is called **cyclic**.

Remark 2.24. Cyclic groups are abelian, since powers of $a \in G$ a;ll commute with eachother.

Example 2.25. $n\mathbb{Z} = \langle n \rangle = \{0, \pm n, \pm 2n, \pm 3n, \dots\}$. For $n = 1$, we get $\langle 1 \rangle = 1\mathbb{Z} = \mathbb{Z}$.

Example 2.26. $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, (\bar{n-1})\} = \langle \bar{1} \rangle$.

3. Lecture 3 — September 12, 2018

Recall from last class we had the following definition:

Definition 3.1. Let G be a group and $a \in G$. The cyclic subgroup **generated** by a is $\langle a \rangle = \{e, a^{\pm 1}, a^{\pm 2}, a^{\pm 3}, \dots\}$. If $G = \langle a \rangle$, we say G is **cyclic**.

Example 3.2. $G = \mathbb{Z} = \langle 1 \rangle$ is cyclic, with cyclic subgroups $n\mathbb{Z} = \langle n \rangle$.
$\mathbb{Z}/n\mathbb{Z} = \langle \bar{1} \rangle$ is also cyclic

Remark 3.3. Recall that we showed that cyclic implies abelian. Therefore, any nonabelian group is **not** cyclic!

Example 3.4. The quartenions Q_8 not cyclic. LIkewise, $\mathrm{GL}_n(\mathbb{R})$, S_n also not cyclic.

Theorem 3.5. *Suppose $G = \langle a \rangle$. Then $|G| = \mathrm{ord}(a)$.*

Proof. We have two cases:

(1) $\text{ord}(a) = n < \infty$: Then HW 1, Problem 3 implies that $e, a, a^2, \ldots, a^{n-1} \in G$ are distinct, implying $|G| > n$. BUt moreover, suppose $a^k \in G$ for $k \in \mathbb{Z}$. Then using the division algorithm, we have $k = nq + r$ with $q \in \mathbb{Z}$ and $0 \leq r \leq n-1$. Thus,

$$a^k = a^{nq+r} = (a^n)^q \cdot a^r = a^r \in \{q, a, a^2, \ldots, a^{n-1}\}$$

So that $G \subset \{e, a, \ldots, a^{n-1}\}$. Thus, $|G| \leq n$, implying $|G| = n$.

(2) $\text{ord}(a) = \infty$. Suppose $a^m = a^k$ for some $m, k \in \mathbb{Z}$. But then $a^{m-k} = e$, and $m - k = 0$ since $\text{ord}(a) = \infty$, and thus $m = k$. As a result, all the powers of a are distinct, so G has infinitely many elements.

□

Lemma 3.6. *Let G be a group with $a \in G$ such that $\text{ord}(a) = |a| = n$. If $a^k = e$ for $k \in \mathbb{Z}$, then $n \mid k$.*

Proof. Using the division algorithm on the integers, we have that $k = nq + r$ for $q \in \mathbb{Z}$ and $0 \leq r \leq n-1$. Then

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

implying that $a^r = e$, but $0 \leq r \leq n-1$ and $\text{ord}(a) = n$, so $r = 0$. Thus, $k = nq$, and $n \mid k$. □

Here is a nice consequence of our work:

Theorem 3.7. *Any two cyclic groups of the same order are isomorphic.*

Proof. We again have two cases:

(1) $|G| = n < \infty$: Then $G = \langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$. We will show this group is isomorphic to our favorite cyclic group of order n, namely $\mathbb{Z}/n\mathbb{Z}$ Define $\phi : \mathbb{Z}/n\mathbb{Z} \to G$ sending $\bar{k} \to a^k$. First, ϕ is well-defined, because if $k_1 \equiv k_2 \mod n$ then $k_1 = k_2 + nq$,and so $\phi(k_2) = a^{k_1+nq} = a^{k_1} \cdot e^q = a^{k_1}$, so it makes sense on congruence classes.
Now we check that ϕ is a homomorphism. Indeed, $\phi(\bar{k_1} + \bar{k_2}) = \phi(k_1 \bar{+} k_2) = a^{k_1+k_2} = a^{k_1} \cdot a^{k_2} = \phi(k_1)\phi(k_2)$. Now, ϕ is surjective because for all a^k, we have $\phi(\bar{k}) = a^k$. Now we appeal to the following fact:
Any surjective function between finite sets of the same cardinality is also injective.
From this fact, ϕ is a bijective homomorphism, so it is an isomorphism!

(2) $|G| = \infty$: In this case we will show that G is isomorphic to the integers $\mathbb{Z}$. Once again define $\phi : \mathbb{Z} \to G$ via $k \mapsto a^k$. It is a homomorphism, as $\phi(k_1 + k_2) = a^{k_1+k_2} = a^{k_1} \cdot a^{k_2} = \phi(k_1)\phi(k_2)$. ϕ is surjective because for all $a^k \in G$. To show ϕ is injective, suppose

$$\begin{aligned} \phi(k_1) &= \phi(k_2) \\ a^{k_1} &= a^{k_2} \\ a^{k_1-k_2} &= e \\ \implies k_1 - k_2 &= e \\ k_1 &= k_2 \end{aligned}$$

Thus, ϕ is bijective.

□

We have thus shown any two cyclic groups G, H of order n (where n can be ∞) are isomorphic to the same group. The reason then that G, H are isomorphic is because isomorphism of groups is an **equivalence relation**.

Definition 3.8. Let S be a set. A **partition** of S is a subdivision of S into subsets S_i such that:

- $S_i \neq 0$ (nonempty)
- $S_i \neq S_j \implies S_i \cap S_j =$ (disjoint)

Example 3.9. $S = \mathbb{Z}$, we have the partition $\mathbb{Z} = \{\text{even}\#'s\} \cup \{\text{odd}\#'s\}$.

Definition 3.10. An **equivalence relation** on S is a binary relation " $\sim$ " such that for any $x, y, z \in S$ we have:

- (Reflexivity): $x \sim x$.
- (Symmetry): $x \sim y \iff y \sim x$.
- (Transitivity): $x \sim y$ and $y \sim z \implies z \sim z$.

Example 3.11. S = $\mathbb{Z}$. Then we can take $a \sim b \iff a \equiv b \mod n$ for some integer n.

Proposition 3.12. *Any equivalence relation on S determines a partition, and vice-versa.*

Proof. Given a partition intro subsets S_i, $a \sim b \iff \exists S_i$ such that $a \in S_i, b \in S_i$. Exercise: this is an equivalence relation.
Conversely, suppose you have an equivalence relation $\sim$ on S. Then for all $x \in S$, the **equivalence class** of x is defined to be $C_x = \{y \in S \mid x \sim y\}$. Claim: the subsets C_x form a partition. First, we have $x \in C_x$, so $C_x \neq$. Moreover, if $C_i \neq C_j$ implies there exists $z \in C_x \cap C_y$, so that $z \sim x$ and $z \sim y$. But then by transitivity, we must have $x \sim y$, so it follows that $C_x = C_y$. So we have a partition into sets. □

Example 3.13. $S = \mathbb{Z}$, given $a \sim b \iff a \equiv b \mod 2$ has the partition $C_0 = \{$ even $\#'s\}$. Likewise, $C_1 = \{$ odd $\#'s\}$.

We are now going to introduce a fundamental way in which we can build new groups from smaller groups.

Definition 3.14. Two groups $(G, *), (H, \cdot)$, then the **product** is the groups

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

with the group operation $(g, h) \cdot (g', h') = (g * g', h \cdot h')$.

Example 3.15. $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ with $\{(0,0),(0,1),(1,0),(1,1)\}$. This group is abelian, with $|(0,0)| = 1$, and other elements order 2. This is our first example of a noncyclic abelian group, as no elements have order 4.

4. Lecture 4 — September 17, 2018

Recall from last time the following definition:

Definition 4.1. An **equivalence relation** on a set S is a binary relation $\sim$ satisfying

(1) $a \sim a$ (reflexive)
(2) $a \sim b \implies b \sim a$ (symmetry)
(3) $a \sim b$ and $b \sim c$ implies that $a \sim c$ (transitivity)

And the punchline was that an equivalence relation partitions S into nonempty disjoint equivalence classes.
We will now define a natural equivalence relation on a group G that is induced by a subgroup $H \subset G$.

Definition 4.2. Let G be a group, $H \subset G$ a subgroup. Define a binary relation $\sim$ so that for $a, b \in G$

$$a \sim b \iff \exists h \in Hsuchthata = bh \iff b^{-1}a \in H$$

Proposition 4.3. *$\sim$ is an equivalence relation.*

Proof. (1) $a = a \cdot e$. Since $a \sim a$
(2) $a \sim b \implies a = bh$ for $h \in H$. Then $h^{-1} \in H$, and $b = ah^{-1}$, so $b \sim a$.
(3) Say $a \sim b$ and $b \sim c$, so that $a = bh_1$ and $b = ch_2$. Then $a = ch_2h_1$. Since $h_2h_1 \in H$, $a \sim c$.

□

Remark 4.4. For the 3 steps to show this is an equivalence relation, we used all 3 aspects of a subgroup. As a result, it doesn't really make sense to define this equivalence relation for anything except a subgroup.

We now use this equivalence relation to define a very important concept.

Definition 4.5. Let $a \in G$. Then the **left coset** of a is equivalence class of a, namely,

$$aH = \{b \in G \mid \exists h \in H \text{ such that } b = ah\} = \{ah \mid h \in H\}$$

(Note: $a \sim b \implies aH = bH$)

Remark 4.6. $H = eH$, so H is the left coset of the identity.

Example 4.7. $G = \mathbb{Z}$, $H = 2\mathbb{Z}$.

$$\begin{aligned} a \sim b &\iff \exists k \in 2\mathbb{Z} \text{ such that } a = b + k \\ &\iff \exists k \in 2\mathbb{Z} \text{ such that } a - b = k \\ &\iff a, b \text{ have the same parity} \end{aligned}$$

The cosets are $0 + 2\mathbb{Z} = \{0, \pm 2, \pm 4, \dots\}$, $1 + 2\mathbb{Z} = \{\pm 1, \pm 3, \pm 5\}$.

Remark 4.8. Today every coset will be a left coset, but you can do each of these things analogously for left and right cosets. We will approach the difference between these two things next lecture.

Example 4.9. $G = \mathbb{Z}$, $H = n\mathbb{Z}$.

$$\begin{aligned} a \sim b &\iff \exists k \in n\mathbb{Z} \text{ such that } a = b + k \\ &\iff \exists k \in n\mathbb{Z} \text{ such that } a - b = k \\ &\iff a \equiv b \mod n \end{aligned}$$

So the left cosets are the congruence classes modulo n, i.e. $0 + n\mathbb{Z}, 1 + n\mathbb{Z}, \dots (n-1) + n\mathbb{Z}$.

Example 4.10. $G = \mathbb{R}^2 = \{(x, y)\}$ under addition. Let $K = \{(0, y) \mid y \in \mathbb{R}\} = y -$ axis. The left cosets are $(x_0, y_0) \sim (x_1, y_1) \iff \exists (0, y) \in K$ such that $(x_0, y_0) = (x_1, y_1) + (0, y) \iff x_0 = x_1$. So cosets are vertical lines, constant x-value.

Definition 4.11. The **index** $[G : H]$ of H in G is the number of (left) cosets of H in G

Example 4.12. $G = \mathbb{Z}$, $H = n\mathbb{Z}$, $[G : H] = n$.

Example 4.13. $G = \mathbb{R}^2$, $K = y -$ axis. Then $[G : K] = \infty$.

Remark 4.14. Notation: G/H is the set of (left) cosets of H. $\mathbb{Z}/n\mathbb{Z} =$ set of left cosets of $n\mathbb{Z}$. This is fantastically suggestive of order cyclic group of order n, and this is no accident. We will be very soon defining an idea of a **quotient group**

Remark 4.15. In general, cosets are NOT subgroups. In fact, since the cosets are disjoint equivalence classes, the only coset that will end up being a subgroup will be the coset of the identity, namely H.

Lemma 4.16. *All left cosets of H in G have the same number of elements.*

Proof. Fix $a \in G$. Then define a map $\alpha : H \to aH$ where $h \mapsto ah$. Likewise, define another map $\beta aH \to H$ via the map $x \mapsto a^{-1}x$. Then

$$\alpha \circ \beta(x) = \alpha(a^{-1}x) = aa^{-1}x = x\beta \circ \alpha(h) = \beta(ah) = a^{-1}ah = h$$

Therefore, α, β are inverses of one another, and α is bijective. Thus, $|H| = |aH|$. □

This lemma gives us the important

Corollary 4.17 (Counting Formula)**.**

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

Remark 4.18. If $|G|$ is finite then $|H|$ is also finite, and then $[G : H] = |G|/|H|$. Moreover, everything we have done is the exact same for right cosets, except you multiply on the other side.

Another very important corollary is the following

Corollary 4.19 (Lagrange's Theorem)**.** *If G is a finite group and $H \subset G$ a subgroup, then $|H|$ divides $|G|$.*

Corollary 4.20. *Let G be a finite group with $a \in G$. Then $|a|$ divides $|G|$.*

Proof. $|a| = |\langle a \rangle|$ divides $|G|$. □

Corollary 4.21. *Let G be a finite group whose order p is prime. Let $a \in G$, $a \neq e$. Then $G = \langle a \rangle$.*

Proof. $|a|$ divides $|G| = p$. So either $|a| = 1$ or $|a| = p$. Bute $a \neq e$, so $|a| \neq 1$. Therefore $|a| = |\langle a \rangle| = p$, so $\langle a \rangle = G$. □

Remark 4.22. If G has prime order p, then $G \cong \mathbb{Z}/p\mathbb{Z}$.

Proposition 4.23. *Let G be a group with subgroups $K \subset H \subset G$. Then*

$$[G : K] = [G : H] \cdot [H : K]$$

Proof. Suppose $[G : H] = n$ and $[H : K] = m$, so that we can decompose $G = g_1H \sqcup g_2H \sqcup \cdots \sqcup g_nH$ and $H + h_1K \sqcup h_2K \sqcup \cdots \sqcup h_mK$. Then

$$\begin{aligned} G &= \bigsqcup_{i=1}^{k} g_i H \\ &= \bigsqcup_{i=1}^{k} g_i \left(\bigsqcup_{j=1}^{m} h_j K \right) \\ &= \bigsqcup_{i=1}^{k} \left(\bigsqcup_{j=1}^{m} (g_i h_j K) \right) \end{aligned}$$

There are mn distinct terms that are being taken for a disjoint union. Thus,

$$[G : K] = mn = [G : H] \cdot [H : K]$$

□

Remark 4.24. Perhaps you're thinking "Hey, why can't we just use the counting formula and immediately solve this proposition!!" Well, this proposition works even for groups G, H, K **that are infinite**, provided that we have finite index subgroups! However, the formula $[G : H] = |G|/|H|$ only holds when G, H are finite groups. So that proof would work less generally than the proof detailed above.

5. Lecture 5 — September 19, 2018

A note about the homework: Since we are assuming a bunch of facts about arithmetic of integers, Hunter has written something on the website for a reference.
Moreover, questions related to linear algebra background will often be added to the homework so that you all can get a refresher on this material.
Let G be a group and $H \subset G$ a subgroup. The **(left) cosets** of H in G

$$aH = \{ah \mid h \in H\} \text{ for } a \in G$$

We then denoted the **index** of H in G $[G : H]$, which is the number of left cosets. We then had this magic counting formula

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

Example 5.1. $G = \mathbb{Z}$, $H = n\mathbb{Z}$. The cosets are then of the form $0 + n\mathbb{Z}, 1 + n\mathbb{Z}, \ldots (n-1) + n\mathbb{Z}$, which are in bijection with congruence classes $\mod n$. Note we have $[\mathbb{Z} : n\mathbb{Z}] = n$.

Example 5.2. $G = \mathbb{R}^2$. and we took $H = \{(0, y) \mid y \in \mathbb{R}\}$. The cosets are then the vertical lines in the coordinate plane, i.e. the sets of the form $x = x_0$ for some constant $x_0 \in \mathbb{R}$.

Example 5.3. $G = S_3$ with $|S_3| = 3! = 6$. Consider the two permutations $x(1) = 2, x(2) = 3, x(3) = 1$ and $y(1) = 2, y(2) = 1, y(3) = 3$. Then $x^3 = 1, y^2 = 1$, but less obviously, $yx = x^2y$ with $yx(1) = 1, yx(2) = 3, yx(3) = 2$.
We can then write $\{e, x, x^2, y, xy, x^2y\}$ and pretty easy to show that all 6 of these elements are distinct, so they make up the whole group. We can then say that this group is **generated** by x, y. Consider the subgroup $H = \langle y \rangle = \{e, y\}$. Then the left cosets of H are $H = yH, xH = \{x, xy\} = xyH$, and $x^2H = \{x^2, x^2y\} = x^2yH$. So we have foudn all 3 cosets.

But why are we just looking at left cosets?

Definition 5.4. The **right cosets** of H are the sets

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

They are equivalence classes of $a \sim b \iff \exists h \in H$ such that $a = hb$.

Remark 5.5. Right cosets and left cosets ARE NOT THE SAME. To explain this, go back to the previous example of $G = S_3$, $H = \langle y \rangle = \{e, y\}$. There are 3 right cosets of H with $H = \{e, y\} = Hy$, $Hx = \{x, yx\} = \{x, x^2y\} = Hx^2y$, and $Hx^2 = \{x^2, yx^2\} = \{x^2, xy\} = Hxy$. In this last coset lies hidden the following claim for you to show: $yx^2 = xy$.

This discussion will lead us to discussing the right properties to say that right and left cosets are actually the same!

Definition 5.6. The subgroup $H \subset G$ is called **normal** if for any $h \in H$ and $g \in G$, $ghg^{-1} \in H$.

Example 5.7. First example is that if G is abelian then any subgroup is normal, since ghg^{-1}.

Example 5.8. G = $\mathrm{GL}_n(\mathbb{R})$ and $H = \mathrm{SL}_n(\mathbb{R})$. Then if $A \in \mathrm{SL}_n(\mathbb{R})$, so that $\det A = 1$ and $B \in \mathrm{GL}_n(\mathbb{R})$. Then

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

so $BAB^{-1} \in \mathrm{SL}_n(\mathbb{R})$.

Example 5.9 (Nonexample)**.** $G = S_3$, $H = \langle y \rangle$. Then $xyx^{-1} = xyx^2 = x(yx)x = xx^2yx = yx = x^2y \notin H$. So H is not a normal subgroup.

Remark 5.10. Are there any nonabelian groups in which every subgroup is normal?
Exercise: Every subgroup of Q, the quaternions, is normal.

Proposition 5.11. *Let $H \subset G$ be a subgroup. The following are equivalent:*

(1) H is a normal subgroup.
(2) For all $g \in G$, $gHg^{-1} = H$.
(3) $\forall g \in G$, $gH = Hg$.
(4) Every left coset is a right coset.

Proof.
- 1 $\implies$ 2: for all $h \in H$, by normality we have $ghg^{-1} \in H$, so $gHg^{-1} \subset H$. Likewise, we have that by substituting $g \to g^{-1}$ that $g^{-1}Hg \subset H$, so $H \subset gHg^{-1}$. 2 $\implies$ 1 is obvious.
- 2 $\iff$ 3: $gHg^{-1} = H \iff gHg^{-1}g = Hg \iff gH = Hg$.
- 3 $\implies$ 4 is clear. For 4 $\implies$ 3, fix a left coset gH. By 4. we have that $gH = Ha$ for some $a \in G$. $Ha \cap Hg = gH \cap Hg \in g$. So Ha, Hg overlap, and so $Ha = Hg$ since they are partitions into equivalence classes.

□

Remark 5.12. H is normal $\iff$ left cosets and right cosets are the same. This will be very important because it will let us turn cosets into a group.

Now we will introduce a new equivalence relation of G. Let $\phi : G \to G'$ be a group homomorphism. Define the following relation on G by $a \sim b \iff \phi(a) = \phi(b)$. First we check this is an equivalence relation. But this is pretty clear to see. We then have a correspondence between equivalence classes under this relation, and elements of $\text{im}(\phi)$. Given $z \in \text{im}(\phi)$. We define

$$\phi^{-1}(z) = \{a \in G \mid \phi(a) = z\}$$

which is called the **preimage** of z or the **fiber** of ϕ above z.

Example 5.13. $G = \mathbb{R}^2$, $G' = \mathbb{R}$. Then consider the mapping $\phi : \mathbb{R}^2 \to \mathbb{R}$ sending $(x, y) \to x$ with $\phi(a_0, y_0) = \phi(x_1, y_1) \iff x_0 = x_1$. So the fibers of ϕ correspond to vertical lines, which maybe geometrically think of why we call them "fibers." They're just strings!

Question: Does the partition of G into fibers of ϕ coincide with a partition into cosets of some $H \subset G$?
Answer: $H = \ker \phi = \phi^{-1}(e) = \{a \in G \mid \phi(a) = e\}$.

Proposition 5.14. *$a, b \in G$. are in the same fiber of $\phi \iff$ they are in the same (left) coset of* $\ker \phi$.

Proposition 5.15. *$a, b \in G$ in the same fiber*

$$\begin{aligned}
&\iff \phi(a) = \phi(b) \\
&\iff \phi(b)^{-1}\phi(a) = e \\
&\iff \phi(b^{-1} \cdot a) = e \\
&\iff b^{-1}a \in \ker \phi \\
&\iff \exists h \in \ker \phi \text{ with } b^{-1}a = h \\
&\iff \exists h \in \ker \phi \text{ with } a = bh \iff \quad a, b \text{ in same left coset of } \ker \phi
\end{aligned}$$

6. Lecture 6 — September 24, 2018

Recall last time we were talking about **normal** subgroups. Namely, subgroups $N \subset G$ such that $\forall h \in N, g \in G$, we have $ghg^{-1} \in N$. We had the following classification which will be very convenient to us:

Proposition 6.1. *TFAE*

(1) N is normal
(2) For all $g \in G$, $gNg^{-1} = N$.
(3) For all $g \in G$, $gN = Ng$.
(4) For all $g \in G$, there exists $a \in G$ such that $gN = Na$.

Definition 6.2. Let $A, B \subset G$ be subsets of G. Their **product** is

$$AB = \{ab \mid a \in A, b \in B\}$$

Remark 6.3. This is NOT the same as $A \times B$.

Example 6.4. $G = \mathbb{Z}/4\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$, With $A = B = \{\bar{0}, \bar{2}\}$. Then $AB = \{\bar{0}, \bar{2}\} \neq A \times B$

Here is an essential lemma about normal subgroups:

Lemma 6.5. *Let $N \subset G$ be a normal subgroup. Then for all $a, b \in G$ we have*

$$(aN)(bN) = (ab)N$$

Proof. To show this we will show mutual containments. First, let $an \in aN$, $bm \in bN$ (i.e. $n, m \in N$) Then using Proposition 6.1, we have $bNb^{-1} = N$, so $\exists n' \in N$ such that $bn'b^{-1} = n$. Then

$$\begin{aligned}(an)(bm) &= (abn'b^{-1})(bm) \\ &= abn'm \in (ab)N\end{aligned}$$

so $(aN)(bN) \subseteq bN$. For the other containment, note that $(ab)n = (a \cdot 1)(bn) \in (aN)(bN)$ □

Note that in this proof, we always have $(aN)(bN) \supset (ab)N$. However, the opposite containment only holds when N is a normal subgroup.

Proposition 6.6. *The set G/N is a group with operation $(aN)(bN) = (ab)N$.*

Proof. (1) identity is N, the identity coset.
(2) inverses: $(aN)^{-1} = a^{-1}N$.
(3) Associative: immediate form the definition of the multiplication.

□

Definition 6.7. G/N is called the **quotient group** of G by N

Definition 6.8. $G = \mathbb{Z}$ $N = n\mathbb{Z}$. N is normal because G is abelian. The quotient $n\mathbb{Z}$ is $\mathbb{Z}/n\mathbb{Z}$ with $(a + n\mathbb{Z}) + (b + n\mathbb{Z}) = (a + b) + n\mathbb{Z}$.

Remark 6.9. $|G/N| = [G : N]$, and using the counting formula, we have that if G is a finite group then $|G/N| = |G|/|N|$.

Proposition 6.10. *The map $\pi : G \to G/N$ sending $a \to aN$ is a surjective homomorphism of groups with* $\ker \pi = N$.

Proof. $\pi(ab) = abN = (aN)(bN) = \pi(a)\pi(b)$. It is pretty clearly surjective. Moreover, given

$$\begin{aligned}a \in \ker \pi &\iff \pi(a) \in N \\ &\iff aN = N \\ &\iff a \in N \\ &\implies \ker \pi = N\end{aligned}$$

□

Corollary 6.11. *Any normal subgroup of G is the kernel of some group homomorphism.*

Recall now from last time that we had $\phi : G \to G'$ a homomorphism of groups and we have the correspondence between

(1) $$\{\text{cosets of } \ker\phi\} \longleftrightarrow \{\text{fibers of } \phi\}$$

(2) $$g\ker\phi \to \phi^{-1}(g)$$

(3)

Lemma 6.12. *$\phi : G \to G'$ group homomorphism. Then $\ker\phi$ is a normal subgroup of G*

Proof. Suppose $k \in \ker\phi$, $g \in G$. Then

$$\begin{aligned}\phi(ghg^{-1}) &= \phi(g)\phi(h)\phi(g)^{-1} \\ &= \phi(g)\phi(g)^{-1} = e \\ &\implies ghg^{-1} \in \ker\phi\end{aligned}$$

□

Theorem 6.13 (First Isomorphism Theorem)**.** *Let $\phi : G \to G'$ be a group homomorphism. Then*

$$G/\ker\phi \cong \operatorname{Im}\phi$$

Proof. Let $K = \ker\phi$. Then define $\alpha : G/K \to \operatorname{Im}(\phi)$ sending $aK \mapsto \phi(a)$. α is well-defined because $aK = bK \iff \phi(a) = \phi(b)$, so $\alpha(aK) = \alpha(bK)$.

Now, α is a homomorphism since $\alpha((aK)(bK)) = \alpha(abK) = \phi(ab) = \phi(a)\phi(b) = \alpha(aK)\alpha(bK)$.

α is injective because $\alpha(aK) = \alpha(bK) \implies \phi(a) = \phi(b) \implies aK = bK$.

α is surjective because for all $\phi(a) \in \operatorname{Im}(\phi)$, we have $\alpha(aK) = \phi(a)$. □

Corollary 6.14. $|G| = |\operatorname{Im}(\phi)| \cdot |\ker(\phi)|$

Proof. $|G| = [G : K] \cdot |K| = |G/K||K| = |\operatorname{Im}(\phi)| \cdot |K|$. □

Corollary 6.15. *ϕ is injective $\iff \ker\phi = \{e\}$.*

Proof.

$$\begin{aligned}\phi \text{ is injective} &\iff \text{any fiber has 1 element} \\ &\iff \text{any } K\text{-coset has 1 element} \\ &\iff |K| = |\ker\phi| = 1 \\ &\iff \ker\phi = \{e\}\end{aligned}$$

□

Remark 6.16. We totally could have proved corollary this easily from the definitions, but it is nice to flex the language we have built up and get a quick proof.

Example 6.17. $G = \mathrm{GL}_n(\mathbb{R})$ and $K = \mathrm{SL}_n(\mathbb{R})$, the the determinany map $\det : G \to \mathbb{R} \setminus 0$ sending $A \mapsto \det A$ has kernel $\ker\phi = K$ and ϕ is surjective. By the First Isomorphism Theorem, we have

$$\mathrm{GL}_n(\mathbb{R}) / \mathrm{SL}_n(\mathbb{R}) \cong \mathbb{R} \setminus 0$$

Theorem 6.18 (Third Isomorphism Theorem)**.** *Suppose $K \subset H \subset G$ are normal subgroups of G (so that K is also normal in H). Then*

(1) $H/K = \{hK \mid h \in H\} \subset G/K$ is a normal subgroup.
(2)

$$(G/K)/(H/K) \cong G/H$$

Essentially, this theorem tells us that the quotient groups work like fractions. Namely, we can "cancel denominators."

Proof. (1) We will show that H/K is the **image** of a normal subgroup under a group homomorphism. Namely, consider the normal quotient map $\pi : G \to G/K$ sending $a \mapsto aK$. Then $\phi(H) = H/K \subset G/K$. Then by a question on HW 3, the image of a normal subgroup under a sujrective homomorphism is normal.

(2) Define $\phi : G/K \to G/H$ sending $aK \mapsto aH$. Recall that the cosets of H are larger than the cosets of K, since $K \subset H$. So a bunch of cosets $a'K$ will go to a coset aH.
First, we show the map is well-defined. Namely, if $aK = bK$ then there exists $k \in K$ such that $a = bk$. Then note also $k \in H$, so $aH = bH$, and $\phi(a) = \phi(b)$
It is a group homomorphism because $\phi(abK) = abH = (aH)(bH) = \phi(aK)\phi(bK)$.
It is surjective because for all $aH \in G/H$, we have $\phi(aK) = aH$.
Lastly,

$$\begin{aligned}\ker\phi &= \{aK \mid \phi(aK) = H\} \\ &= \{aK \mid aH = H\} \\ &= \{aK \mid a \in H\} = H/K\end{aligned}$$

Then by the First Isomorphism Theorem we have

$$(G/K)/(H/K) \cong G/H$$

as desired.

□

7. Lecture 7 — September 26, 2018

Last time we talked about the First and Third Isomorphism Theorems. So where is the Second Isomorphism Theorem? It needs some build up.
Recall that if $A, B \subset G$ subsets of a group, then we defined $AB = \{ab \mid a \in A, b \in B\}$.

Proposition 7.1. *Let $H, K \subset G$ be finite subgroups. Then $|HK| = \frac{|H|\cdot|K|}{|H\cap K|}$.*

Proof. $HK = \bigcup_{h\in H} = hK$ is a union of K-cosets, each of which have order K. It suffices to find the number of distinct cosets hK. Suppose $h_1, h_2 \in H$. Then

$$\begin{aligned}h_1K = h_2K &\iff h_2^{-1}h_1K = K \\ &\iff h_2^{-1}h_1 \in K \\ &\iff h_2^{-1}h_1 \in K \\ &\iff h_1 \in h_2(H\cap K) \\ &\iff h_1(H\cap K) = h_2(H\cap K)\end{aligned}$$

which are cosets of $H \cap K$, a finite subgroup of H. So to know how many cosets there are of this form, suffices to know how many cosets of $H \cap K$ there are in H. By counting formula, we have the number of cosets $[H : H \cap K] = |H|/|H : H \cap K|$. Therefore since each coset has size $|K|$, we have

$$|HL| = \frac{|H|}{|H \cap K|} \cdot |K|$$

□

Remark 7.2. HK is not in general a subgroup. For example, take $G = S_3$ with $H = \{e, \sigma\}$ and $K = \{e, \tau\}$ for $\sigma : (1,2,3) \to (2,1,3)$ and $\tau : (1,2,3) \to (1,3,2)$. Note that $H \cap K - \{e\}$. Then $|HK| = |H| \cdot |K|/|H \cap K| = 2 \cdot 2/1 = 4 \not| 6$ so it is not a subgroup.

For amend for this remark, we have the following criterion:

Proposition 7.3. *HK is a subgroup of G iff $HK = KH$.*

Proof. First suppose that HK is a subgroup. Then $H \subset HK$ and $K \subset KH$ and so since we assumed HK is a subgroup and is thus closed under multiplication, we have $KH \subset HK$. For the other containment, fix $hk \in HK$. Then since HK is a subgroup, $k^{-1}h^{-1} = (hk)^{-1} \in HK$, so there exists $h_1 \in H, k_1 \in K$ such that $k^{-1}h^{-1} = h_1k_1$. Then

$$hk = (h_1k_1)^{-1} = k_1^{-1}h_1^{-1} \in KH$$

so $HK \subset KH$, and equality holds.

Now supposed that $HK = KH$. To show HK is a subgroup, we need to check all of the axioms.

- (Identity): $e \in H, e \in K$, so $e = e \cdot e \in HK$.
- (Inverses): Suppose $hk \in HK$. Then $(hk)^{-1} = k^{-1}h^{-1} \in KH = HK$.
- (Closure under products): Given $h_1k_1, h_2k_2 \in HK$, the product $k_1h_2 \in HK = KH$ so there exists $h' \in H, k' \in H$ with $k_1h_2 = h'k'$. Then

$$(h_1k_1)(h_2k_2) = h_1(k_1h_2)k_2 = (h_1h')(k'k_2) \in HK$$

So we have a subset closed under inverses, multiplication, and contains the identity, so it is a subgroup. □

Remark 7.4. $HK = KH$ does NOT imply that elements of H commute with elements of K. For example, consider $G = S_3$ with $x : (1,2,3) \to (2,3,1)$ and $y : (1,2,3) \to (2,1,3)$ so that $x^3 = e, y^2 = e, yx = x^2y$. Then taking $H = \langle x \rangle$ and $K = \langle y \rangle$. Then $|HK| = |H| \cdot |K|/|H \cap K| = 3 \cdot 2/1 = 6$. Therefore, $HK = G$ and $HK = KH$ but $xy \neq yx$.

The reason we're doing all of this stuff is to arrive at the Second Isomorphism Theorem. But before we do that, we need to build up some more theory:

Definition 7.5. The **normalizer** of K

$$N_G(K) = \{g \in G \mid gKg^{-1} = K\}$$

Proposition 7.6. *Let $H, K \subset G$ be subgroups such that $H \subset N_G(K)$. Then HK is a subgroup of G.*

Proof. By our handy criterion from before, it suffices to show that $HK = KH$. We show mutual containment. First, given $hk \subset HK$, since $H \subset N_G(K)$ implies that $hKh^{-1} = K$ implies that any individual element $hkh^{-1} \in K$, so $hk \in Kh \subset KH$. For the opposite containment, given $kh \in KH$ we do the exact same thing (since these proofs are symmetric). Namely, by the defintion of the normalizer, $hkh^{-1} \in h^{-1}Kh = K$, implying $kh \in hK \subset HK$. □

Corollary 7.7. *If $K \subset G$ is a normal subgroup, then $\forall$ $H \subset G$ subgroup, HK is a subgroup.*

This is all building up to the Second Isomorphism Theorem. Before we state that, recall that the **First** Isomorphism Theorem states that given a group homomorphism $\phi : G \to G'$, we have that $G/(\ker \phi) \cong \text{Im}(\phi)$.

Theorem 7.8 (Second Isomorphism Theorem)**.** *Ler $H, K \subset G$ be subgroups and $H \subset N_G(K)$. Then*

(1) HK is a subgroup.
(2) $K \subset HK$ is a normal subgroup.
(3) $H \cap K \subset H$ is a normal subgroup.
(4) $H/(H_{\cap}K) \cong HK/K$.

Diagrammatically, we can think of this theorem as a tree: (INSERT DIAGRAM HERE)

Proof. (1) Follows from the Proposition 7.6.
(2) $H, K \subset N_G(K), \implies HK \subset HK \subset N_G(K)$ since $N_G(K)$ is a subgroup and thus closed under multiplication. Then given $a \in HK$, $aKa^{-1} = K$, so $K \subset HK$ is normal.
(3) Follows from the homework and part 2)!
(4) Define the function $\phi : H \to HK/K$ sending $h \mapsto hK$. ϕ is a homomorphism because $\phi(h_1h_2) = h_1h_2K = (h_1K)(h_2K) = \phi(h_1)\phi(h_2)$ where we use the normality of K in HK. Now we show that ϕ is surjective. Given $hkK \in HK$, we have $hkK = hK$, so $\phi(h) = hkK = hK$. Now, the kernel is elements h such that $hK = K \iff h \in K \iff j \in H \cap K$. Therefor, using the First Isomorphism we get

$$H/(H \cap K) \cong HK/K$$

as desired.

□

SO why do we care

Remark 7.9 (Intuition for Second Isomorphism Theorem)**.** $N \subset G$ normal subgroup. Then $\pi : G \to G/N$. Given $H \subset G$ a subgroup of G, what is the image $\pi(H)$? it is a subgroup of G/N, but now we can completely classify it now:

$$\begin{aligned}\pi(H) &= \{hN \mid h \in H\} \\ &= \{h(H \cap N) \mid h \in H\} \\ &\implies \pi(H) \cong H/(H \cap N) \cong HN/N \subset G/N\end{aligned}$$

8. Lecture 8 — October 1, 2018

Today it will seem like we are pivoting, but this material will be extremely important for the cool theorems that we do after the midterm.

Let G be a group, A a set

Definition 8.1. An **action** (group action) of G on A is a map

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

such that for all $a \in A$ we have

(1) $g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a$ for all $g_1, g_2 \in G$.
(2) $e \cdot a = a$.

Example 8.2. $G = S_n$, $A = \{1, 2, \ldots, n\}$, we have the group action $G \times A \to A$ defined by $(\tau, h) \mapsto \tau(h)$.

Example 8.3. $G = \mathrm{GL}_n(\mathbb{R})$ and $A = \mathbb{R}^n$, we have the group action $G \times A \to A$ via $(M, \vec{v}) \mapsto M\vec{v}$.

Remark 8.4. This $\cdot$ is NOT a multiplication, it is a symbolic way of representation the group action. Think of a group action as a set of symmetries acting on some sort of set.

Definition 8.5. A **permutation** of A is a bijective map $\tau : A \to A$.

Proposition 8.6. *Let $G \times A \to A$ be a group action. Then for all $g \in G$, construct $\sigma_g : A \to A$ sending $a \mapsto g \cdot a$. We then have*

(1) σ_g is a permutation of A.
(2) Let S_A be the set of permutations of A, which is a group under composition $\circ$. Then

$$\begin{aligned} \phi : G &\to S_A \\ g &\mapsto \sigma_g \end{aligned}$$

Proof. (1) Fix $g \in G$. Need to show that $\sigma_g : A \to A$ is bijective. We claim $\sigma_{g^{-1}}$ is an inverse to this map. Indeed,

$$\begin{aligned} (\sigma_{g^{-1}} \circ \sigma_g)(a) &= g^{-1} \cdot (g \cdot a) = (g^{-1} g) \cdot a = a \\ (\sigma_g \circ \sigma_{g^{-1}})(a) &= g \cdot (g^{-1} \cdot a) = (g g^{-1}) \cdot a = a \end{aligned}$$

Therefore, $\sigma_{g^{-1}} = (\sigma_g)^{-1}$, so σ_g is bijective, so σ_g is a permutation of A.

(2) We first check that this map is a group homomorphism, that $\phi(g_1g_2) = \phi(g_1) \circ \phi(g_2)$ for all $g_1, g_2 \in G$. for all $a \in A$, we have

$$\begin{aligned}[\phi(g_1g_2)](a) &= \sigma_{g_1g_2}(a) \\ &= (g_1g_2) \cdot a \\ &= g_1 \cdot (g_2 \cdot a) \\ &= \sigma_{g_1}(\sigma_{g_2}(a)) = [\phi(g_1) \circ \phi(g_2)](a)\end{aligned}$$

□

Definition 8.7. Let $G \times A \to A$ be a group action. The **kernel** is $\{g \in G \mid \sigma_g(a) = a \text{ for all } a\} = \{g \in G \mid \sigma_g = \mathrm{id}\} = \ker \phi$ where ϕ is the map from the previous proposition.

Example 8.8. $G \times A \to A$ via $(g, a) \mapsto a$ is called the **trivial** group action, since for all $g \in G$, $\sigma_g(a) = a$. Then the kernel is all of G, since every element of G acts by the identity on A.

Definition 8.9. The action $G \times A \to A$ is **faithful** if distinct elements of G induce distinct permutations of A. This happens iff the map $\phi : G \to S_A$ is injective, or $\ker \phi = \{e\}$.

Example 8.10. $G = S_n$, $A = \{1, \dots n\}$ is a faithful action, as is $G = \mathrm{GL}_n(\mathbb{R})$, $A = \mathbb{R}^n$ by matrix multiplication.

Remark 8.11. In its origins, groups were introduced to study symmetries of polyhedra. These groups were encoded as matrices, usually as subsets of some sort of group of permutations. So whenever we had a group, it was some sort of subset of a symmetric group. But now comes, as we know it, as abstract group theory. Here, we just define groups are intrinsic groups in their own right. Was this really a new field of study? Not exactly, because we have the following result.

Example 8.12. Let $A = G$ and take the action of G on G by left multiplication: $G \times G \to G$ via $(g, a) \mapsto g \cdot a$ (note this map is NOT a group homomorphism, since G is not abelian). We claim this is an action, but these properties follow immediately from the axioms of group multiplication.
We now claim this is action is faithful. SUppose that $\sigma_g = \sigma'_g$, so that $ga = g'a$ for all $a \in A$. Then $ge = g = g'e = g'$, so $g = g'$. THus the action is faithful.

Corollary 8.13 (Cayley's Theorem)**.** *Let G be a finite group with $|G| = n$. Then G is isomorphic to a subgroup of S_n.*

Proof. Consider the left-multiplication action

$$G \times G \to G$$
$$(g, a) \mapsto ga$$

It is faithful, so $G \to S_{|G|} = S_n$ is injective, so $G \cong \phi(G) \subset S_n$. □

Definition 8.14. Given $a \in A$, the **stabilizer** of a is $G_a = \{g \in G \mid g \cdot a = a\}$.

Example 8.15. $G = S_3$, $A = \{1, 2, 3\}$. Then $G_3 = \{e, \sigma\} = H$ where $\sigma : (1, 2, 3) \to (2, 1, 3)$.

Proposition 8.16. *G_a is a subgroup of G.*

Proof. We check the subgroup axioms. $e \cdot a = a \implies e \in G_a$. Given $g \in G_a$ so that $g \cdot a = a$, we have

$$\begin{aligned} g \cdot a &= a \\ g^{-1}(g \cdot a) &= g^{-1} \cdot a \\ (g^{-1}g) \cdot a &= g^{-1}a \\ a &= g^{-1}a \\ \implies g^{-1} &\in G_a \end{aligned}$$

Lastly, if $g_1 a = a$ and $g_2 \cdot a = a$ then $g_1 g_2(a) = g_1 \cdot (g_2 \cdot a) = g_1 \cdot a = a$, so $g_1 g_2 \in G_a$, so G_a ia a subgroup. □

Remark 8.17. It may not be too surprising to you all that $\bigcap_{a \in A} G_a = \ker \phi$.

Proposition 8.18. *Define a relation on A as follows: $a \sim b$ if there exists $g \in G$ such that $a = gb$. Then*

(1) This is an equivalence relation.
(2) If C_a is the equivalence class of a then $|C_a| = [G : C_a]$

Proof. (1) We check the three things first. Namely, $a \sim a$ since $a = e \cdot a$. If $a \sim b$ so that $a = g \cdot b$, then $g^{-1} \cdot a = b$, so $b \sim a$. Lastly, if $a \sim b$ and $b \sim c$ so that $a = g_1 \cdot b$ and $b = g_2 \cdot c$ then $a = g_1 \cdot g_2 \cdot c = (g_1 g_2) \cdot c$, so $a \sim c$.

(2) Note that $C_a = \{g \cdot a \mid g \in G\}$. Then we define a function

$$C_a \to G/G_a$$
$$g \cdot a \mapsto gG_a$$

First, we show that this map is well-defined. Say that $g \cdot a = h \cdot a$, so that $(h^{-1}g) \cdot a = a$, so that $h^{-1}g \in G_a$, implying that $g \in hG_a$ and thus $gG_a hG_a$, so $\alpha(g \cdot a) = \alpha(h \cdot a)$.

Now we show the map is injective. Suppose that $\alpha(g \cdot a) = \alpha(h \cdot a)$. Then $gG_a = hG_a$, so there exists $x \in G_a$ so that $g = hx$. Therefore, $g \cdot a = (hx) \cdot a = h \cdot a$, so $g \cdot a = h \cdot a$.

To show surjectivity, for all $gG_a \in G/G_a$, it is the image $\alpha(g \cdot a) = gG_a$. Therefore, $|C_a| = |G/G_a| = [G : G_a]$.

□

Remark 8.19. We usually call C_a the **orbit** of $a \in A$ under the action of G.

9. Lecture 9 — October 3, 2018

Midterm is next Wednesday! You are allowed to use any fact that is proved in class/homework, unless the problem is specifically telling you to reprove some sort of fact. Note: the midterm will NOT be a test of how well you learn all the random lemmata we have proved, but rather how well you can apply things such as the main theorems and definitions to solve problems.

Recall that on Monday we were talking about group actions. Namely, given a group G and a set A, an **action** of G on A is a map $G \times A \to A$ sending $(g, a) \to g \cdot a$ with $g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a$ and $e \cdot a = a$.

The **orbit** of $a \in A$ is $C_a = \{g \cdot a \mid g \in G\} \subset A$, and the **stabilizer** of $a \in A$ is $G_a = \{g \in G \mid g \cdot a = a\} \subset G$ is a subgroup. We had a big theorem relating the size of these two things:

Theorem 9.1 (Orbit-Stabilizer)**.**

$$|C_a| = [G : G_a]$$

Remark 9.2. When G is finite, we can using the counting formula to say $|C_a| = |G|/|G_a| \implies |C_a| \cdot |G_a| = |G|$. This in turn implies that when $a = g \cdot b$ we have $|G_a| = |G_b|$.

Example 9.3. Let $A = G$ and let G act on itself by **conjugation**, i.e. $G \times G \to G$ with $(g, a) \mapsto g \cdot a = gag^{-1}$. This is an action, as $g_1 \cdot (g_2 \cdot a) = g_1 \cdot (g_2 a g_2^{-1}) = g_1 g_2 a g_2^{-1} g_1^{-1} = g_1 g_2 a (g_1 g_2)^{-1}$. Likewise, $e \cdot a = eae^{-1} = eae = a$.

Definition 9.4. Let $a, b \in G$. If $\exists g \in G$ such that $a = gbg^{-1}$, then a, b are **conjugate**. $C_a = \{gag^{-1} \mid g \in G\}$ is the **conjugacy class** of a.

Example 9.5. $G = \mathrm{GL}_n(\mathbb{R})$. $A = \mathrm{diag}(\lambda_1, \lambda_2, \ldots, \lambda_n)$ for $\lambda_i \neq \lambda_j$ for $i \neq j$. Then there exists $g \in \mathrm{GL}_n(\mathbb{R})$ such that $A = gBg^{-1}$. This implies that B has the same eigenvalues as A.

Example 9.6. Say G is abelian. Then for all $g \in G$ and $a \in G$, $gag^{-1} = gg^{-1}a = a$, which implies that conjugation is the trivial action, so $C_a == \{gag^{-1} \mid g \in G\} = \{a\}$.

Remark 9.7. For $a \in G$, the stabilizer of a

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

which is known as the **centralizer** of A. Orbit Stabilizer tells us that $|C_a| = [G : C_G(a)]$.

Remark 9.8. The kernel of the conjugation homomorphism is $\{g \in G \mid gag^{-1} = a \text{ for all } a \in G\} = \{g \in G \mid ga = ag \text{ for all } a \in G\} = \mathcal{Z}(G)$, which is known as the **center** of G. Note of course that $\bigcap_{a \in G} C_G(a) = \mathcal{Z}(G)$.

Lemma 9.9. *An element $a \in \mathcal{Z}(G)$ iff $C_a = \{a\}$.*

Proof. This is very straightforward. Given $a = \mathcal{Z}(G)$, we have $gag^{-1} = gg^{-1}a = a$. Conversely, suppose that for any $g \in G$ we have $gag^{-1} = a \iff ga = ag \iff a \in \mathcal{Z}(G)$. □

Remark 9.10. For any group G we have $e \in \mathcal{Z}(G)$.

Theorem 9.11 (Class Equation)**.** *Let G be a finite group, with conjugacy classes $C_1, \ldots, C_n$ that do not intersect the center $\mathcal{Z}(G)$. Fix $a_i \in C_i$ for all $i \leq n$. Then*

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

Proof. G is partitioned by its conjugacy classes $G = C_1 \sqcup C_2 \sqcup \cdots \sqcup C_n \sqcup \mathcal{Z}(G)$, which is a disjoint union. Then

$$\begin{aligned} |G| &= |\mathcal{Z}(G)| + |C_1| + \cdots + |C_n| \\ &= |\mathcal{Z}(G)| + [G : C_1] + \cdots + [G : C_n] \\ &= |\mathcal{Z}(G)| + \sum_{i=1}^{n} [G : C_G(a_i)] \end{aligned}$$

□

Remark 9.12. All we are really doing for this theorem is saying that a group action breaks up a group into its orbits, which in turn have size equal to the index of their stabilizers.

Remark 9.13. Each term on RHS of the Theorem divides $|G|$, which we will crucially use.

Theorem 9.14. *Suppose G is finite with $|G| = p^k$ and $k \geq 1$. Then $\mathcal{Z}(G) \neq \{e\}$.*

Proof. Using the class equation, we get

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

If $a_i \notin \mathcal{Z}(G)$, then $[G : C_G(a_i)] > 1$. But we also have by Orbit-Stabilizer that $[G : C_G(a_i)]|C_G(a_i)| = G$, implying $[G : C_G(a_i)] = p^l$ for $0 < l \leq k$. Now, since $p \mid |G|$ and $p \mid [G : C_G(a_i)]$ then the class equation tells us that $p \mid \mathcal{Z}(G)$. Therefore, $|\mathcal{Z}(G)| \geq p$ (since $|\mathcal{Z}(G)| \geq 1$ as $e \in \mathcal{Z}(G)$. □

We actually have an even more interesting corollary, which is the following:

Corollary 9.15. *Suppose $|G| = p^2$. Then G is abelian.*

Proof. $\mathcal{Z}(G) \subset G$ is always a normal subgroup, and by the theorem we have $|\mathcal{Z}(G)| = p$ or p^2. If $|\mathcal{Z}(G)| = p$ then $|G/\mathcal{Z}(G)| = p$, so $G/\mathcal{Z}(G)$ is cyclic, which in turn by your homeowkr implies that G is abelian (which is actually contradiction our assumption on the size of p). If $|\mathcal{Z}(G)| = p^2$ then the group is automatically abelian. □

We can in fact say more!

Proposition 9.16. *Suppose $|G| = p^2$. Then either $G \cong \mathbb{Z}/p^2\mathbb{Z}$ or $G = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.*

Proof. Case 1: G has an element a of order p^2. Then $G = \langle a \rangle$, so $G \cong \mathbb{Z}/p^2\mathbb{Z}$.

Suppose G has no elements of order p^2. Then for all $a \neq e$, $|a| = p$ and $|e| = 1$. Fix $a \in G$ of order p, as well another element $b \in G \setminus \langle a \rangle$. THen consider the subgroup $\langle a, b \rangle = \{a_1^k b_2^k \mid k_1, k_2 \in \mathbb{Z}\}$, the smallest subgroup containing both a and b. By consturction we have $]langlea\rangle \subsetneq \langle a, b \rangle$, so $|\langle a, b \rangle| > p$, implying $|\langle a, b \rangle| = p^2$, which implies in turn that $G = \langle a, b \rangle$.

We can now construct a map $\phi : \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \to G$ sending $(1, 0) \mapsto a$ and $(0, 1) \mapsto b$. Since a, b have order p, this map is well defined. It is rather straightforward to show this is a homomorphism, and it is clearly surjective as $\langle a, b \rangle$. Since both of these sets are finite and of the same size, we have this map is also injective, implying it is an isomorphism. □

10. Lecture 10 — October 15, 2018

We're almost finished tlking about groups! Not surprisingly, there is much more to say about groups generally, but for this class we will soon move on to ring theory. We will finish our discussion of groups with something called the Sylow theorems, which have pretty wide-ranging applications about groups. Let G be a finite group.

Recall we had by Lagrange's theorem that for any subgroup H we had that $|H| \mid |G|$. We can then ask a converse question:

Suppose $|G| = n$ and $d \mid n$. Does G have a subgroup H with $|H| = d$? In general, the answer is no, but the smallest example is a group of order 12. There is a counterexample on the homework.

However, we can saying something along these lines with the first Sylow Theorem:

Theorem 10.1 (First Sylow Theorem)**.** *Let p be a prime with $|G| = p^k \cdot m$ with $p \nmid m$. Then G has a subgroup of order p^k.*

Theorem 10.2. *Suppose G is abelian, with $p \mid |G|$. Then G contains an element of order p.*

Proof. By Induction on $|G| = n$. The Base Case is $|G| = 1$, which has no prime p dividing its order, so there is nothing to prove. Now, our induction hypothesis is: for all finite groups G' such that $|G'| < n$, $p \mid |G'| \implies G'$ contains an element of order p. Fix $a \in G$, $a \neq e$. Let $H = \langle a \rangle$.

- Case I: $p \mid H$. Then $|a| = |H| = p \cdot d$, which implies that $(a^d)^p = a^{d \cdot p} = e$. Thus, $|a^d| \mid p$, but $|a^d| \neq 1$, so we must have $|a^d| = p$.

- Case II: $p \nmid |H|$. If this is the case, then $p \mid |G|/|H| = |G/H|$ where the quotient group is well-defined since we assumed G is abelian (and thus all of the subgroups are normal). But $|G/H| < |G|$, so by the induction hypothesis G/H contains a coset bH of order p. Now consider $\pi : G \to G/H$ sending $g \mapsto gH$. We have by homework (it's not super hard to intuitively see), $|bH| = |\pi(b)|| \mid |b|$. Therefore $p \mid |b|$. Then by taking the subgroup $H' = \langle b \rangle$, we note $p \mid H'$, so we are reduced to Case I.

□

Definition 10.3. Let p be a prime.

(1) A group of order p^k is called a p **- group**. A subgroup $H \subset G$ of order p^k is a p**-subgroup**.
(2) $|G| = p^k \cdot m$ with $p \nmid m$. A subgroup $P \subset G$ such that $|P| = p^k$ is a **Sylow-p-subgroup**.

Example 10.4. $|G| = 72 = 9 \cdot 8 = 3^2 \cdot 2^3$. The Sylow-3 subgroup corresponds to a subgroup of order 3^2. The Sylow-2 subgroup corresponds to a subgroup of order 2^3.

$P \subset G$ is a Sylow p-subgroup are maximal p-subgroups, or equivalently, $p \nmid [G : P]$.

Restating the First Sylow Theorem, the result says that if $p \mid |G|$ then G contains a Sylow-p-subgroup. Let's now prove this statement.

Proof of the First Sylow Theorem. We again use induction. Base case: $n = 1$, nothing to prove.

We again $\forall G'$ such that $|G'| < n$, $p \mid |G'| \implies G'$ has a Sylow-p-subgroup. We then have several cases:

- Case 1: $p \mid |\mathcal{Z}(G)|$. Since $\mathcal{Z}(G)$ is abelian, by our previous theorem we have that $\exists a \in \mathcal{Z}(G)$ such that $|a| = p$. Let $H = \langle a \rangle$. Then $|H| = |a| = p$, and we claim $H \subset G$ is normal. For all $h \in H, g \in G$, we have $ghg^{-1} = gg^{-1}h = h$. Let $G = p^k \cdot m$, $p \nmid m$. Then $G' = G/H$ has order $p^k \cdot m/p = p^{k-1} \cdot m$. Then $|G'| < n$, implying G' contains a Sylow-p-subgroup P' with $|P'| = p^{k-1}$. Again, not consider the quotient map $G \to G/H$. Let $P' = \pi^{-1}(P')$. P is a subgroup of G, $P \supset H = \ker \pi$. $\tilde{\pi} : P \to P'$ is surjective. Then $|P| = |\operatorname{Im}(\tilde{\pi})| \cdot |\ker(\tilde{\pi})| = |P'| \cdot |H| = p^{k-1} \cdot p = p^k$. So P is a Sylow-p-subgroup of G.
- Case 2: $p \nmid |\mathcal{Z}(G)|$. Let $C_1, \ldots, C_r \subset G$ be the conjugacy classes of G that do not intersect the center. Pick $a_i \in C_i$ for all $1 \leq i \leq r$. Then by the class equation we have
$$|G| = \mathcal{Z}(G) + \sum_{i=1}^{r} [G : C_G(a_i)]$$
Note note that $p \mid |G|$ and $p \nmid |\mathcal{Z}(G)|$, so p cannot divide every $[G : C_G(a_i)]$, because otherwise $|G|$ could not be a multiplice of p. Therefore, there exists a_i such that $p \nmid [G : C_g(a_i)] = |G|/|C_G(a_i)|$. Therefore, $|C_G(a_i)| = p^k \cdot m'$ with $p \nmid m'$. Now, $|C_G(a_i)| < n$ since $|G|/|C_G(a_i)| > 1$ (because a_i is not in the center of G), so by our

induction hypothesis $C_G(a_i)$ contains a Sylow-p-subgroup P with $|P| = p^k$, so P is also a Sylow-p-group of G.

□

Corollary 10.5 (Cauchy's Theorem)**.** *Suppose $p \mid |G|$. Then G contains an element of order p.*

Proof. $p \mid |G| \implies G$ has a non-trivial Sylow p-subgroup P with $|P| = p^k$ for $k > 0$. Then by Problem on HW 2, we have P contains an element of order p, as desired. □

On Wednesday we will prove the 2nd and 3rd Sylow Theorems.

11. Lecture 11 — October 17, 2018

Last time we proved the first Sylow theorem, which says given G a finite group with $|G| = p^k \cdot m$ for $p \nmid m$, there exists a **Sylow p-subgroup**, i.e. a subgroup $H \subset G$ of order $|H| = p^k$. Now that we know these exists, we are going to explore more properties of them, and next class we will explain some very cool applications to the structure og groups.

Lemma 11.1. *Suppose P is a Sylow p-subgroup, Q is some Sylow p-subgroup. Then $Q \cap N_G(P) = Q \cap P$.*

Proof. We show both containments. Namely, $N_G(P) \supset P$, so $Q \cap N_G(P) \supset Q \cap P$. For the other containment, let $H = Q \cap N_G(P)$. We already know $H \subset Q$, so it is sufficient to show $H \subset P$.
Our plan is to show PH is a p-subgroup. This is a subgroup because $H \subset N_G(P)$, so $HP = PH$. In that case, $P \subset PH$, and $|PH| \leq p^k = |P| \implies P = PH$, so that for all $g \in P$, $gh \in PH = P$, so $h \in g^{-1}P = P$. Thus, we would have $H \subset P$. Alternatively, $|HP| = |P| \cdot |H|/|P \cap H|$, so id $|HP| = |P|$ then $|H| = |H \cap P| \iff H \subset P$.
To show our "plan," examine $|HP| = |H| \cdot |P|/|H \cap P|$. We have $|P| = p^k$ and $H \subset Q \implies |H| = p^a$ $H \cap P \subset P$ so $|H \cap P| = p^b$ for $b \leq k$. Then $|PH| = p^{k+a-b}$, so it is a p-subgroup. □

We can use this relatively boring lemma to prove something more exciting:

Theorem 11.2 (2nd Sylow Theorem)**.** *If P is a Sylow p-subgroup, and Q is any p subgroup. Then there exists $g \in G$ such that*

$$Q \subset gPg^{-1}$$

where we note gPg^{-1} is another Sylow p-subgroup.

Corollary 11.3. *(1) Any p-subgroup is contain in a Sylow p-subgroup.*
(2) Any two Sylow p-subgroups are conjugate. That is, for all Sylow p-subgroups, we have $\exists g \in G$ such that $P_2 = gP_1g^{-1}$.

Proof of 2nd Sylow Theorem. This proof will use group actions in a very crucial way. Fixing a Sylow p-subgroup P, let $S = \{P_1, \ldots, P_r\}$ be the set of Sylow p-subgroups conjugate to P. This has one orbit, as for all $P_i \in S$, there exists $g_i \in G$ such that $g_iPg_i^{-1} = P_i$. Then G acts on S via $G \times S \to S$ with $g, P_i \to gP_ig^{-1}$. Then by definition, S is a single orbit, since

if $P_i = g_i P g_i^{-1}$ and $P + j = g_j P g_j^{-1}$, we have $(g_j g_i)^{-1} P_i (g_j g_i^{-1})^{-1} = g_j (g_i^{-1} g_i P g_i^{-1} g_i) g_j^{-1} = g_j P g_j^{-1} = P_j$, as desired.

Thus, the the orbit $O_P = S$, so by orbit stabilizer we have that

$$|S| = |O_P| = [G : G_P]$$

Where the stabilizer $G_P = \{g \mid gPg^{-1} = P\} = N_G(P)$. Note that $P \subset N_G(P)$, so $p^k \mid |N_G(P)|$. Thus, $|N_G(P)| = p^k \cdot m'$ for $p \nmid m'$. So $|S| = |G|/|N_G(P)| = p^k \cdot m/(p^k \cdot m') = m/m'$ so $p \nmid |S|$.

Now, given an arbitrary p-subgroup $Q \subset G$, Q acts on S by conjugation. Now we appeal to the following fact, which was HW #5, Problem 7: Suppose Q is a p-group acting on a set A. Suppose that $p \nmid |A|$. Then there exists a **fixed point**. That is there is $a \in A$ such that $h \cdot a = a$ for all $h \in H$.

Applying the fact, there exists $P_i \in S$ such that for all $h \in Q$ with $hP_ih^{-1} = P_i$, so $Q \subset N_G(P_i)$. Now using the lemma, $Q = Q \cap N_G(P_i) = Q \cap P_i$. Then this implies $Q = Q \cap P_i \implies Q \subseteq P_i$. Thus, $Q \subseteq g_i P g_i^{-1}$. □

Well, now that that the all Sylow p-subgroups are conjugate to eachother, so S consists of ALL Sylow p-subgroups! The 3rd Sylow Theorem examines the ramification of the action.

Theorem 11.4 (3rd Sylow Theorem)**.** *Let $N_p = \#$ of Sylow p-subgroups in G. Then*

(1) $N_p \mid m$

(2) $N_p \equiv 1 \mod p$

Proof. (1) Using the action from the proof of Sylow 2, we have $N_p = |S| = |G|/|N_G(P)| = p^k \cdot m/(p^k \cdot m') = m/m' \mid m$.

(2) Let $Q = P_1$. P_1 acts on S. Let $C_1 = \{P_1\}, \dots C_T$ be the orbits under this action. Suppose $C_J \ni P_j$. The stabilizer is $\{g \in P_i \mid gP_jg^{-1} = P_j\} = P_1 \cap N_G(P_j) = P_1 \cap P_j \subsetneq P_1$ where we used our lemma from the beginning of class that $Q \cap N_G(P) = Q \cap P$. Therefore, we have $P_1 \cap P_j$ is a p-subgroup, so $|P_1 \cap P_j| = p^a$. Then the size of the conjugacy class $|C_1| = [P_1 : P_1 \cap P_J] = |P_1|/|P_1 \cap P_J| = p^k/p^a = p^{k-a}$ for $k - a > 0$. Partitioning S into orbits, we have $P_1 = C_1 \sqcup C_2 \dots C_{t-1} \sqcup C_t$, we have $N_p = |S| = |C_1| + |C_2| + \cdots + |C_t| = 1 + p^{b_2} + \cdots + p^{b_t} \equiv 1 \mod p$.

□

12. Lecture 12 — October 22, 2018

So we were going to do the classification of finite abelian groups, but the proof is kind of annoying, so we encourage you to take Math 123 to learn a much more general result! Instead, we will begin our new unit of ring theory

Definition 12.1. A **ring** is a set R with two binary operations $+, \cdot$ such that

(1) (R, +) is an abelian group with identity $0 \in R$ and $\forall a \in R$, the inverse $-a \in R$.

(2) $\cdot$ is associative, i.e. $\forall a, b, c \in R$ we have $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

(3) $\cdot$ is distributive over $+$ with $\forall a, b, c \in R$, $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(b + c) \cdot a = b \cdot a + c \cdot a$.

Remark 12.2.
- If $\cdot$ is commutative, we call R a **commutative ring**.
- If $\exists 1 \in R$ such that $\forall a \in R\ 1 \cdot a = a \cdot 1 = a$, R is a **unital ring**

Example 12.3. $(\mathbb{Z}, +, \cdot)$ is a ring. In fact, it is commutative and unital.

Remark 12.4. Since $\cdot$ is not even required to have a multiplicative identity, in general there may not be multiplicative inverses. Also in general, 0 will denote the additive identity and 1 the multiplicative identity.

Example 12.5. $R = \{0\}$ the **zero** ring In this case additive identity = multiplicative identity. On the homework you will show that this is in fact the **only** ring with this property.

Example 12.6. $\mathbb{Z}/n\mathbb{Z}$ with $\bar{a} + \bar{b} = \overline{a+b}$ and $a \bar{\cdot} b + \bar{a} \cdot \bar{b}$. Multiplicative identity is $\bar{0}$. Likewise, the multiplicative identity is $\bar{1}$.

Example 12.7. $M_n(\mathbb{R}) = \{n \times n \text{ matrices with entries in } \mathbb{R}\}$. $+$ is mateix addition, and $-$ is matrix multiplication. 0 is the all 0's matrix while $1 = I_n$. We know from past experience that matrix multiplication is **not** commutative, and also the elements with determinant 0 have no inverse.

For the future: When taking more advanced classes, we actually will often assume that rings are unital, and even commutative, since we can just say so much more about such rings. Here's one interesting things that unital rings buy us:

Remark 12.8. Suppose R is unital. Then distributivity implies that $+$ is commutative.

Proof. Fix $a, b \in R$. Then

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

□

Definition 12.9. Suppose R is unital, nonzero, and $\forall R \setminus \{0\}$, there exists $a^{-1} \in R$ such that $a \cdot a^{-1} = a^{-1} \cdot a = 1$. Then we call R a **division ring**.

If R is **commutative division ring**, we call it a **field**.

Example 12.10. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are fields.

Example 12.11. Non-commutative division ring:

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

we call this the **quarternion ring**. It has the properties $i^2 = j^2 = k^2 = -1$, $ij = k$, $jk = i$, $ki = j$, $ji = k$, $kj = -i$, $ik = -j$, and $(a + bi + cj + dk)^{-1} = \frac{a-bi-cj-dk}{a^2+b^2+c^2+d^2}$.

Proposition 12.12. *Let R be a ring. Then $\forall a, b \in R$ we have*

(1) $0 \cdot a = a \cdot 0 = 0$.
(2) $(-a) \cdot b = a \cdot (-b) = -(a \cdot b)$.
(3) $(-a) \cdot (-b) = a \cdot b$.
(4) If $1 \in R$, then 1 is unique with $-a = (-1) \cdot a$.

Proof. (1) $0 \cdot a = (0 + 0) \cdot a = 0 \cdot a + 0 \cdot a$, implying $0 = 0 \cdot a$. We can then apply the exact same argument to the righthand side to get $a \cdot 0 = 0$.

□

Just as in our build up of groups, we will build up rings by defining natural constructions. Here we begin this task:

Definition 12.13. A subset $R' \subset R$ is a **subring** if $('R, +)$ is a subgroup of $(R, +)$ and R' is closed under multiplication.

Example 12.14. $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ is a series of inclusions of subrings.

Example 12.15. $\mathbb{Z}[i] = \{a + bi \in \mathbb{C} \mid a, b \in \mathbb{Z}\}$ is a ring called the **Gaussian integers**.

Example 12.16 (Polynomial Ring)**.** Fix a commutative, unital ring R. A **polynomial** in the variable x with coefficients in R is a sequence symbolically written as $a_n x^n + \ldots a_0$ for $a_i \in R$. IMPORTANT MESSAGE: we usually think of polynomials as functions, but these are formal sequences, NOT functions! The **ring of polynomials** in one variable over R is

$$R[x] = \{\sum_{k=0}^{n} a_k x^k \mid n \in \mathbb{N}, a_k \in R\}$$

Addition is defined by $\sum_{k=0}^{n} a_k x^k + \sum_{k=0}^{n} b_k x^k = \sum_{k=0}^{n} (a_k + b_k) x^k$. Meanwhile, multiplication is defined by

$$(a_0 + a_1 x + \cdots + a_n x^n)(b_0 + b_1 x + \cdots + b_n x^n) = a_0 b_0 + (a_1 b_0 + a_0 b_1) x + \ldots$$

where the coefficient of x^k is $\sum_{i+j=k} a_i b_j$. We observe that R is the subring of constant polynomials in $R[x]$. The additive identity is $p(x) = 0$, and the multiplicative identity is the constant polynomial $q(x) = 1$.

We now want to define a notion of a structure-preserving map between rings:

Definition 12.17. Ler R, S be rings. A function $\phi : R \to S$ is a **homomorphism** if $\forall a, b \in R$, we have $\phi(a+b) = \phi(a) + \phi(b)$ and $\phi(a \cdot b) = \phi(a) \cdot \phi(b)$.

Remark 12.18. If $\phi : R \to S$ is a homomorphism of rings, then it is also a homomorphism of groups $(R, +) \to (S, +)$ with $\phi(0) = 0$ and $\phi(-a) = -\phi(a), \ldots$

Example 12.19. $\phi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ sending $a \mapsto a(\mod n)$ with $\ker \phi = n\mathbb{Z}$.

Definition 12.20. Let $\phi : R \to S$ be a homomorphism. The **kernel** of ϕ is $\ker \phi = \{a \in R \mid \phi(a) = 0\}$.

Example 12.21. $\phi : \mathbb{Q}[x] \to \mathbb{Q}$ sending $f \to f(0)$ is a homomorphism with $\ker \phi = \{f(x) \mid f(0) = 0\} = \{f(x) = \sum a_k x^k \mid a_0 = 0\}$.

Example 12.22 (Non-example)**.** A homomorphism of groups is not always a homomorphism of rings! Consider $\phi : Z \to Z$ sending $a \mapsto n \cdot a$. Then $\phi(ab) = nab$ but $\phi(a)\phi(b) = n^2 ab$, so ϕ is only a ring homomorphism when $n^2 = n \iff n = 0, 1$.

Note: what do we call the set of elements that map to 1? Later, we will talk a bout the group of units of a ring, and the induced homomorphism on the group of units will have a kernel, and this construct will be closely related.

Proposition 12.23. *Suppose $\phi : R \to S$ be a homomorphism. Then*

(1) $\mathrm{Im}(\phi) \subset S$ *is a subring.*
(2) $\ker \phi \subset R$ *is a subring.*
(3) $\forall x \in \ker \phi$*, for all* $a \in R$*, we have* $ax, xa \in \ker \phi$*.*

Proof. (1) $(\mathrm{Im}(\phi))$ is a subgroup of $(S, +)$. For all $\phi(a), \phi(b) \in \mathrm{Im}(\phi), \phi(a)\phi(b) = \phi(ab) \in \mathrm{Im}(\phi)$, implying $\mathrm{Im}(\phi)$ is closed under $\cdot$.
(2) Exercise! (Follows from (3))
(3) Fix $x \in \ker \phi, a \in R$. Then $\phi(ax) = \phi(a)\phi(x) - \phi(a) \cdot 0 = 0 \implies ax \in \ker \phi$. Likewise, Then $\phi(xa) = \phi(x)\phi(a) = 0 \cdot \phi(a) = 0 \implies xa \in \ker \phi$.

□

Our new goal is to reconstruct the notion of quotients and the First Isomorphism Theorem, so we need to build up the notion of a "normal" subring.

13. Lecture 13 — October 24, 2018

Recall last time that we defined a ring, a subring, and a homomorphism of rings. See the previous lecture for the definition.

Suppose we have a subring $J \subset R$. We then have $(J, +) \subset (R, +)$. Since $(R, +)$ is abelian, we must have $(I, +)$ is normal. We can thus always form a quotient group $(R/I, +)$ with the operation $(a + I) + (b + I) = (a + b) + I$. We now ask: When can we attach a multiplication structure so that R/J is a ring? The ring structure we would

want is not surprisingly $(a+I)(b+I) = (ab)+I$ where $a+I = \{a+i \mid i \in I\}$, or at least $(a+I)(b+I) \subset (ab)+I$. The reason is that we would like the natural quotient map $\pi : R \to R/I$ to not only a group homomorphism, but a **ring** homomorphism. In particular, we would need to define $\pi(a)\pi(b) = (a+I)(b+I) = \pi(ab) = ab+I$. Now, for any $a, b \in R$ and $x, y \in I$, we need

$$\begin{aligned}(a+x)(b+y) &\in ab+I \\ ab+ay+xb+xy &\in ab+I \\ ay+xb+xy &\in I\end{aligned}$$

When we take $a = b = 0$, we get $xy \in I$, so I needs ot be a subring. Thus, $ay+xb+xy-xy = ay+xb \in I$. Now plugging in $a = 0$, we have for all $b \in R$ and $x \in I$ that $xb \in I$. Likewise, plugging in $b = 0$, for any $a \in R, y \in I$, we have $ay \in I$. This analysis motivates us to make the following definition:

Definition 13.1. A subset $I \subset R$ is an **ideal** if

- $(J, +) \subset (R, +)$ is a subgroup.
- For all $a \in R$ and $x \in I$ we have $ax, xa \in I$.

An ideal is the analogue of a normal subgroup for rings.

Example 13.2. If $\phi : R \to S$ is a ring homomorphism then $\ker \phi \subset R$ is an ideal.

Example 13.3. Let $R = \mathbb{Z}$. Fix any $n \in \mathbb{N}$. Then $n\mathbb{Z} \subset \mathbb{Z}$ is an ideal, as it is an additive subgroup, and if $m \in n\mathbb{Z}$ then $km \in n\mathbb{Z}$ for any $k \in \mathbb{Z}$.

Example 13.4. Let $\mathbb{R}[x] = \{\text{polynomials in } x \text{ with coefficients in } \mathbb{R}\}$. Then consider $I = \{f(x) \in \mathbb{R}[x] \mid f(0) = 0\}$. Then for all $g(x) \in \mathbb{R}[x]$, we have $g(0)f(0) = g(0) \cdot 0 = 0$, so $g(x)f(x) \in I$. Thus, I is an ideal.

Proposition 13.5. *Suppose $I \subset R$ is an ideal. Then R/I is a ring with $(a+I)+(b+I) := (a+b)+I$ and $(a+I)(b+I) := ab+I$.*

Proof. First we check that this multiplication is well-defined. If $x, y \in I$ we have

$$\begin{aligned}(a+x)(b+y) &= ab+ay+xb+xy \\ &= (ab)+(ay+xb+xy) \in (ab)+J\end{aligned}$$

Check associativity, distributivity in your (possibly nonexistent) free time. □

Remark 13.6. We are sweeping a confusing detail under the rug. Namely, as **sets** we do not necessarily have that $(a+I)(b+I) = ab+I$ (meaning the left hand side could be a proper subset of the righthand side). In fact, this set theoretic statement is almost never true (we would need the ideal $Ia+Ib+ab = I$). But the multiplication we define will still set theoretically land in $ab+I$, meaning $ab+I$ is the **unique** coset that contains the product set (since $(a+I)(b+I)+I$

We will now attempt to pour over the isomorphism theorem from the land of groups to the land of rings. But since we have the isomorphism theorems for groups, this will be surpisingly easy.

Theorem 13.7 (First Isomorphism Theorem for Rings)**.** *Suppose $\phi : R \to S$ is a homomorphism of rings. Then*

$$R/\ker\phi \cong \operatorname{Im}\phi$$

is a ring isomorphism.

Proof. We have $\ker\phi = \{a \in R \mid \phi(a) = 0\}$. Then we have that

$$\alpha : R/\ker\phi \to \operatorname{Im}(\phi)$$

sending $a + \ker\phi \mapsto \phi(a)$. By the First Isomorphism Theorem for groups, we have that α is a well-defined map of sets, a group homomorphism and bijective. Now, let $a, b \in R$. Then

$$\begin{aligned}\alpha((a+\ker\phi)(b+\ker\phi)) &= \alpha(ab+\ker\phi)\\ &= \phi(ab)\\ &= \phi(a)\phi(b)\\ &= \alpha(a+\ker\phi)\alpha(b+\ker\phi)\end{aligned}$$

Thus, α respects multiplication, so we have an isomorphism of rings. (Here we are noting that a bijective ring homomorphism is an isomorphism). □

Theorem 13.8 (Third Isomorphism Theorem for Rings)**.** *Suppose $J \subset I \subset R$ are ideals of R. Then*

$$(R/J)/(I/J) \cong R/I$$

Proof. By the Third Isomorphism Theorem for Groups (or rather, the proof of said theorem), we have $\alpha : R/J \to R/I$ sending $(a + J \mapsto a + I$ satisfies α is well-defined (as a map of sets), surjective, group homomorphism, and $\ker\alpha = I/J$. Now let $a, b \in R$. Then

$$\begin{aligned}\alpha((a+J)(b+J)) &= \alpha(ab+J)\\ &= ab + I = (a+I)(b+I)\\ \alpha(a+J)\alpha(b+J)&\end{aligned}$$

so α is a ring homomorphism. Thus, the First Isomorphism theorem for rings says that $R/J/\ker(\alpha) \cong R/I$ so $(R/J)/(I/J) \cong R/I$, as desired. □

Theorem 13.9 (2nd Isomorphism Theorem For Rings)**.** *Suppose $A \subset R$ is a subring and $I \subset R$ is an ideal. Then*

(1) $A + I$ is a subring of R
(2) $A \cap I$ is an ideal of A
(3) $A + I/I \cong A/(A \cap I)$

Proof. (1) It is quite easy to see that $(A + I, +) \subset (R, +)$ is a subgroup. For all $a, b \in A, x, y \in I$, we have

$$(a+x)(b+y) = ab + (ay + xb + xy) \in A + I$$

so $A + I$ is closed under multiplication, and thus is a subring of R.

(2) It is quite easy to see $(A \cap I, +) \subset (A, +)$ is a subgroup. Let $a \in A, x \in A \cap I$. Then $ax \in A$ because A is a subring. Moreover, since I is an ideal, $ax \in I$, so $ax \in A \cap I$. Thus, $A \cap I$ is an ideal of A.

(3) Homework!

□

14. Lecture 14 — October 29, 2018

Let R be a ring. Recall $I \subset R$ is an **ideal** if $(I, +) \subset (R, +)$ is a subgroups and for all $a \in R, x \in I$, we have $ax, xa \in I$.

Example 14.1. $\{0\} \subset R$ is an ideal, since for all $a \in R$, $a \cdot 0 = 0 \cdot a = 0$.

Example 14.2. $R \subseteq R$ is an ideal.

Remark 14.3. Let R be unital - $1 \in R$. Suppose I is an ideal $I \subset R$ with $1 \in I$. Then for all $a \in R$, $a = a \cdot 1 \in I$, so $I = R$

To generalize this remark, we make the following definition:

Definition 14.4. Suppose R is unital with $1 \in I$. Then $u \in R$ is a **unit** if there exists $v \in R$ such that $uv = vu = 1$. We denote the units of a ring

$$R^\times = \{u \in R \mid u \text{ is a unit}\}$$

Example 14.5. $\mathbb{Z}^\times = \{\pm 1\}$

Example 14.6. $\mathbb{R}[x]^\times = \{f(x) \mid \exists g(x) : f(x)g(x) = 1\} = \mathbb{R}^\times = \mathbb{R} \setminus \{0\}$ since the degree of a product is the sum of the degrees.

Example 14.7. Let F be a field. Then $F^\times = F \setminus \{0\}$. For example, $\mathbb{R}^\times = \mathbb{R} \setminus 0$, $\mathbb{C}^\times = C \setminus \{0\}$.

Example 14.8. $M_n(\mathbb{R})^\times = \mathrm{GL}_n(\mathbb{R})$

Proposition 14.9. *Suppose $u_1, u_2 \in R$ are units. Then u_1u_2 is also a unit.*

Proof. u_1, u_2 beign units implies that there exist $v_1, v_2 \in R$ such that $u_1v_1 = u_2v_2 = 1$ (and the same if we switch the order of multiplication.) THen

$$(u_1u_2)(v_2v_1) = u_1(u_2v_2)v_1 = u_1v_1 = 1$$

The same argument applies to multiplication in the opposite order with $(v_2v_1)u_1u_2$. □

Corollary 14.10. *$R^\times$ forms a group under $\cdot$, which we call the **group of units** of R.*

Proof. $\cdot$ is a binary operation on $R^\times$, with $1 \in R^\times$ as a multiplicative identity and $\forall u \in R^\times \implies \exists v = u^{-1} \in R^\times$. So we have inverses. Moreover, $\times$ is associative because the multiplication is inherited from the ring. □

Remark 14.11. There probably exist examples of rings R such that there are elements $x, y \in R$ with $xy = 1$ and $yx \neq 1$, but we will not put in effort to find such a ring. It is just important that in the definition of a unit, it is necessary that we require both left and right inverse.

Proposition 14.12. *Suppose $I \subset R$ an ideal containing a unit $u \in R$. Then $I = R$.*

Proof. u is a unit implies that $\exists v \in R$ such that $uv = vu = 1$. Thus, $1 = vu \in I$, so $I = R$. □

Corollary 14.13. *Suppose F is a field. Then the only ideals of F are $\{0\}$ and F.*

Proof. Suppose $I \neq 0$ is an ideal. Then there exists $a \neq 0$ such that $a \in I$. But a is a unit, so $I = F$. □

Example 14.14. $\mathbb{Z}/6\mathbb{Z} \ni \bar{2}, \bar{3}$ are nonzero elements abd $\bar{2} \cdot \bar{3} = \bar{6} = \bar{0}$.

Proof. An element $a \in R$ is a **zero divisor** if there exists $b \neq 0$ such that $ab = 0$ or $ba = 0$. □

Example 14.15. $M_2(\mathbb{R})$, consider the matrices $a = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ and $b = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$. Then $ab = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ implies that a, b are zero divisors. However, $ba = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, so we actually only need one of the multiplications to be zero to have zero divisors.

Remark 14.16. A zero-divisor can **never** be a unit. Suppose that a is a zero divisor, so that there exists $b \in R \setminus 0$ such that $ab = 0$ or $ba = 0$. Suppose a is a unit, so that there exists $v \in R$ with $av = va = 1$. Then $vab = 1 \cdot b = 0$ in one case, and if $ba = 0$ then $bav = b \cdot 1 = 0$. So in either case, we get a contradiction with $b = 0$.

The 0 ring has no zero divisors since it has no nonzero elements!

Definition 14.17. Suppose R is a nonzero, commutative, unital ring. Then we say R is an **integral domain** if $ab = 0 \implies a = 0$ or $b = 0$. In other words, R has no nontrivial zero divisors.

Example 14.18. $\mathbb{Z}, \mathbb{R}[x], \mathbb{Z}[i]$, any field (since fields contain only units).

Proposition 14.19. *$\mathbb{Z}/n\mathbb{Z}$ is an integral domain iff n is a prime number.*

Proof.
- Only if: Suppose n not prime, so that $n = ab$ for $a, b \neq \pm 1, \pm n$. Then $\bar{a}, \bar{b} \in \mathbb{Z}/n\mathbb{Z}$ and $\bar{a} \cdot \bar{b} = \bar{ab} = \bar{n} = \bar{0}$. So these are nonzero zero divisors, and thus $\mathbb{Z}/n\mathbb{Z}$ is not an integral domain.
- If: Suppose n is prime. Suppose we have elements $\bar{a}, \bar{b} \in \mathbb{Z}/n\mathbb{Z}$ with $\bar{a} \cdot \bar{b} = \bar{0}$. Equivalently, we have $ab \equiv 0 \mod n$ so $n \mid a \cdot b$. Since n is prime, we must have either $n \mid a$ or $n \mid b$, so either $\bar{a} = \bar{0}$ or $\bar{b} = \bar{0}$, as desired. Thus $\mathbb{Z}/n\mathbb{Z}$ is an integral domain.

□

Proposition 14.20 (Cancellation)**.** *Suppose R is an integral domain. Then $ab = ac \implies a = 0$ or $b = c$.*

Proposition 14.21. *$ab = ac \implies a(b - c) = 0$, so $a = 0$ or $b - c = 0$.*

Example 14.22. $\mathbb{Z}/6\mathbb{Z}$ is not an integral domain, and we have setting $a = b = \bar{3}$ and $c = \bar{5}$. Then $a \neq 0$ and $b \neq c$ but $ab = \bar{9} = \bar{3}$ and $ac = \bar{15} = \bar{3}$, so $ab = ac$. We really need the hypothesis of integral domain in order to cancel things.

Proposition 14.23. *Suppose R is a finite integral domain. Then R is a field.*

Proof. Fix $a \in R, a \neq 0$. Consider the mapping $\phi : R \to R$ sending $x \to ax$. Then $\phi : (R, +) \to (R, +)$ is a group homomorphism, with $\ker \phi = \{x \in R \mid ax = 0\} = \{0\}$ since R is an integral domain and $a \neq 0$. Thus ϕ is injective. But now we note the following wonderful fact: ANY injective (or surjective) function between two finite sets of the same size is bijective. Thus ϕ is bijective, so it is surjective. There then exists $x \in R$ such that $\phi(x) = 1$, i.e. $ax = xa = 1$ (since R is commutative). So a is a unit, and a was an arbitrary nonzero element of R, so R is a field. □

Corollary 14.24. *For $n > 0$, $\mathbb{Z}/n\mathbb{Z}$ is a field iff n is prime.*

To enhance our discussion of fields and integral domains, it is absolutely necessary to talk more about ideals. So let us do that now.

Definition 14.25. Let $I, J \subset R$ be ideals. Then their **sum** is

$$I + J = \{x + y \mid x \in I, y \in J\}$$

Their **product** is

$$I \cdot J = \{\sum_{k=1}^{n} x_k \cdot y_k \mid x_k \in I, y_k \in J\}$$

so it is sums of products, not just products (otherwise wouldn't be closed under addition).

Proposition 14.26. *$I + J$ is an ideal. In fact,it is the smallest ideal containing both I and J. In other words, any ideal containing I, J contains $I + J$.*

Proof. Exercise! □

Proof. IJ is an ideal and $IJ \subset I \cap J$ □

Proof. First you would want to show that IJ is an additive subgroup, but this is true by definition. The rest is straightforward. □

Remark 14.27. $\{xy \mid x \in I, y \in J\}$ is **not** closed under $+$.

15. Lecture 15 — October 31, 2018

Happy Halloween everyone! For the purposes of today we will assume R is a commutative, unital, nonzero ring.

Proposition 15.1. *Let $A \subset R$ be a subset. Then*

$$(A) = \{\sum_{i=1}^{n} c_i a_i \mid n \in \mathbb{N}, a_i \in A, c_i \in R\}$$

is the smallest ideal of R containing A.

Proof. We first proof that (A) is an ideal. (A) is an additive subgroup, with $0 = 0 \cdot a$ for all $a \in \mathbb{A}$, and it has inverses with the inverse of $\sum_{i=1}^{n} c_i a_i$ being $\sum_{i=1}^{n} (-c_i) a_i$. It is also closed under addition because the sum will still be a finite R-linear combination of elements in A. To show it is an ideal, we have $\forall b \in R$, if $\sum_{i=1}^{n} c_i a_i \in (A)$ then $b\,(\sum_{i=1}^{n} c_i a_i) = \sum_{i=1}^{n} (bc_i) a_i \in (A)$. Now suppose that $I \supset R$ is an ideal such that $I \supset A$. Then take any $\sum_{i=1}^{n} c_i a_i \in (A)$, we have $a_i \in I$, so $c_i a_i \in I$. Then by additivity $\sum c_i a_i$. Since this element was arbitrary, we have that $(A) \subset I$. □

Remark 15.2. You can make this definition of the **ideal generated by** A for any ring, but it is much more annoying just because we need to distinguish between left and right multiplication, and we would rather not worry about that in the current moment.

Definition 15.3. (A) is called the **ideal generated by** A.

Definition 15.4. An ideal **I** is called **principal** if there exists $a \in R$ such that $I = (a)$.

Example 15.5. $R = (1)$ is also principal

Example 15.6. $\mathbb{Z} \supset n\mathbb{Z} = (n)$ is principal. By homework, every ideal is of this form, so that every ideal of $\mathbb{Z}$ is a principal ideal.

Example 15.7. Let $R = \mathbb{Z}[x]$. Then the principal ideal $(x) = \{xp(x) \mid p(x) \in \mathbb{Z}[x]\} = \{f(x) \in \mathbb{Z}[x] \mid f(0) = 0\}$.

Example 15.8. Sometimes the way you present an ideal is by generating by more than 1 element, but it still is principal. For example, consider $\mathbb{Z} \supset (2, 4)$. But $(2) \supset (4)$, so $(2, 4) = (2)$.

Not all ideals of rings are principal, but it is somewhat subtle to find our first example. The point is that even if we say the ideal is generated by more than 1 element, we need to prove the ideal cannot be generated a single element.

Let $R = \mathbb{Z}[x]$ and take the ideal $I = (2, x)$. Then $(2, x) = \{2 \cdot p(x) + xg(x) \mid p(x), q(x) \in \mathbb{Z}[x]\}$. We first claim that $(2, x) = \{f(x) \in \mathbb{Z}[x] \mid f(0) \equiv 0 \mod 2\}$. Take any $2p(x) + xq(x) \in (2, x)$. Then $2p(0) + 0 \cdot q(0) \equiv 0 \mod 2$, so $2p(x) + xq(x) \in I$. Conversely, given $f(x) \in I$ with $f(x) = 2 \cdot c + x(a_1 + \cdots + a_n x^{n-1})$ such that $f(x) = 1$. Then set $p(x) = c$, $q(x) = a_1 + a_2 x + \cdots + a_n x^{n-1}$ and we get $f(x) = 2 \cdot p(x) + x \cdot q(x)$.

Proposition 15.9. *The ideal $I = (2, x) \subset \mathbb{Z}[x]$ is not principal.*

Proof. Suppose towards contradiction that $(2, x) = (f(x))$ for some polynomial. Then $2 \in (f(x))$, so that $\exists g$ such that $f(x)g(x) = 2$, so that $\deg g(x) = \deg f(x) = 0$, so $f(x), g(x) \in \{\pm 1, \pm 2\}$. If $f(x) = \pm 1 \implies \{f(0)$ is not even or $(f(x)) = \mathbb{Z}[x]$. Either way, this is a contradiction. If $f(x) = \pm 2$ then $(f(x)) = (2, x) = (2)$, so then we would need there to be $h(x)$ such that $h(x) \cdot 2 = x$, but this is contradiction over $\mathbb{Z}$. Thus, $(2, x)$ cannot be a principal ideal.

Note of course this argument generalizes to show any ideal that looks like $(m, f(x))$ with $f(x) = a_n x^n + \cdots + a_0$ with $(m, a_n) = 1$ will not be principal. □

Recall now that R is a field implies that the only ideals of R are $\{0\}$ and R. We now show the converse:

Proposition 15.10. *Suppose the only ideals of R are $\{0\}$ and R. Then R is a field.*

Proof. Take $a \in R$ with $a \neq 0$. Consider (a). Then $a \neq 0 \implies (a) \neq \{0\} \implies (a) = R \ni 1$, so there exists $b \in R$ such that $ba = 1$. a is a unit, so R is a field. □

Definition 15.11. An ideal $M \subsetneq R$ is **maximal** if the only ideals containing are M and R.

Recall that all ideals of $\mathbb{Z}$ are of the form $n\mathbb{Z}$ with a containinment $n\mathbb{Z} \subset m\mathbb{Z} \iff m \mid n$.

Proposition 15.12. *$n\mathbb{Z} \subset \mathbb{Z}$ is maximal iff n is prime.*

Proof. $\leftarrow$ Assume n is prime. Suppose that $n\mathbb{Z} \subset m\mathbb{Z}$. Then $m \mid n$, so since n is prime we have $m = 1$ or $m = n$, so that $m\mathbb{Z} = \mathbb{Z}$ or $m\mathbb{Z} = n\mathbb{Z}$. $\rightarrow$ Now suppose n is not prime. Then $n = ab$ for $n > a, b > 1$. Then $n\mathbb{Z} \subsetneq a\mathbb{Z}$. But $a \neq 1$ so $a\mathbb{Z} \neq \mathbb{Z}$ and $a < n$ so $a\mathbb{Z} \neq n\mathbb{Z}$, so $n\mathbb{Z}$ cannot be maximal. □

Example 15.13. Here is an example of a nonmaximal ideal. $(x) \subset \mathbb{Z}[x]$ is not maximal since $(x) \subsetneq (2, x) \subsetneq \mathbb{Z}[x]$

Suppose now $J \subset R$ is an ideal, and let $\pi : R \to R/J$ be the quotient mapping. Then on the homework we proved that

$$\begin{aligned} \{\text{ideals of } R/J\} &\leftrightarrow \{\text{ideals of } R \text{ containing } J\} \\ I' &\mapsto \pi^{-1}(I') \\ \pi(I) &\leftarrow I \end{aligned}$$

Proposition 15.14. *Let $M \subset R$ be an ideal. Then M is maximal $\iff$ R/M is a field.*

Proof. Suppose that M is maximal, which is true iff theonly ideals of R containing M are R and M. By what we recalled above, M is maximal the only ideals of R/M are R/M and 0, which is true iff R/M is a field. □

Example 15.15. $(2, x) \subset \mathbb{Z}[x]$ is maximal.

Proof. Consider a mapping $\phi : \mathbb{Z}[x] \to \mathbb{Z}/2\mathbb{Z}$ mapping $f(x) \mapsto f(0) \mod 2$. ϕ is surjective with $\ker \phi = \{f(x) \mid f(0) \text{ is even}\} = (2, x)$. By the first isomorphism, we then have that

$$\mathbb{Z}[x]/(2, x) \simeq \mathbb{Z}/2\mathbb{Z}$$

where our target ring is a field. Therefore, since the quotient is a field, $(2, x)$ is maximal. □

Remark 15.16. In general, we have a nice way of checking where or not an ideal is maximal. Construct a surjective map with kernel equal to

Remark 15.17. An interesting fact of life is that **every** ideal is contained in a maximal ideal. The proof relies on a form of the Axiom of Choice using something called Zorn's Lemma.

16. Lecture 16 — November 5, 2018

Let R be a commutative, unital nonzero ring. Recall that we were talking about ideals that are called **maximal**, ideals M such that the only ideals containing M are M and R. We had the result that $M \subset R$ is maximal iff R/M is a field.

We now introduce a more general class of ideals, called prime ideals

Definition 16.1. An ideal $P \subsetneq R$ is **prime** if $ab \in P$ implies that $a \in P$ or $b \in P$.

Remark 16.2. R is an **integral domain** iff $\{ab = 0 \mid a = 0 \text{ or } b = 0\}$, iff $\{0\} \subset R$.

Recall now that $p \in \mathbb{N}$ is prime provided that $p \mid ab \implies p \mid a$ or $p \mid b$.

Proposition 16.3. *Let $n \geq 0$, $n \in \mathbb{Z}$. Then $n\mathbb{Z} \subset \mathbb{Z}$ is a prime ideal iff $n = 0$ or n is prime.*

Proof. If $n = 0$ then $n\mathbb{Z} = \{0\}$, which is prime because $\mathbb{Z}$ is an integral domain. If $n = p$ is prime then suppose that $ab \in p\mathbb{Z}$. Then $p \mid ab$, so either $p \mid a$ or $p \mid b$, so $a \in p\mathbb{Z}$ or $b \in p\mathbb{Z}$, so $p\mathbb{Z}$ is a prime ideal.

If $n = 1$, then $n\mathbb{Z} = \mathbb{Z}$ so not a prime ideal. If n is compositie, then $n = ab$ for $1 < a, b, < n$. Then $ab \in n\mathbb{Z}$ but $n \nmid a$ and $n \nmid b$, so $a \notin n\mathbb{Z}$ and $b \notin n\mathbb{Z}$, so $n\mathbb{Z}$ is not prime. □

Proposition 16.4. *Let $P \subsetneq R$ be an ideal. Then P is a prime iff R/P is an integral domain.*

Proof. Suppose that P is prime. Then if

$$(a + P)(b + P) = (0 + P)$$
$$ab + P = P$$
$$ab \in P$$
$$a \in P \text{ or } b \in P$$
$$a + P = 0 + P \text{ or } b + P = P$$

So $\mathbb{R}/P$ is an integral domain.

For the opposite direction, suppose P not prime. Then $\exists\, a, b \in R$ such that $a, b \notin P$ and $ab \in P$. Then $(a+P)(b+P) = ab + P = 0 + P$. So that $a \notin P \implies a + P \neq 0 + P$. and $b \notin P \implies b + P \neq 0 + P$. Thus, R/P is not an integral domain. □

Example 16.5. Consider $(x) = \{f(x) \mid f(0) = 0\} \subset \mathbb{Z}[x]$. Consider the mapping $\phi : \mathbb{Z}[x] \to \mathbb{Z}$ sending $f(x) \mapsto f(0)$. Then ϕ is surjective with kernel $\ker\phi = \{f \mid f(0) = 0\} = (x)$, so applying the First Isomorphism Theorem, we have that $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$, which is an integral domain since (x) is prime.

Corollary 16.6. *Maximal ideals are prime.*

Proof. M is maximal iff R/M is a field, and fields are integral domains, so M must also be prime. □

Definition 16.7. Two ideals $A, B \subset R$ are **comaximal** if $A + B = R$ where $A + B = \{a + b \mid a \in A, b \in B\}$.

Example 16.8. On your homework, you proved that $n\mathbb{Z} + m\mathbb{Z} = d\mathbb{Z}$ where $d = \gcd(m, n)$. Then $n\mathbb{Z} + m\mathbb{Z} = \mathbb{Z} \iff \gcd(n, m) = 1 \iff n, m$ coprime.

Now recall that we define the product of two ideals to be $AB = \{\sum a_i b_i \mid \forall n \in \mathbb{N}, a_i \in A, b_i \in B\}$ This is an ideal with the property that $AB \subset A \cap B$.

Proposition 16.9. *Let $A, B \subset R$ be comaximal ideals. Then*

$$\phi : R \to R/A \times R/B$$

*sending $r \mapsto (r + A, r + B)$ is **surjective** and has $\ker\phi = AB$, so that $R/(AB) \cong R/A \times R/B$.*

Proof.

$$\begin{aligned} \ker\phi &= \{r \in R \mid \phi(r) = (0 + A, 0 + B)\} \\ &= \{r \in R \mid r + A = A, r + B = B\} \\ &= \{r \in R \mid r \in A, r \in B\} && = A \cap B = AB \end{aligned}$$

where the last line holds by Question 5 d) on Problem Set 9.

$A + B = R$ implies there exists $a \in A, b \in B$ with $a + b = 1$. Then $a = 1 - b$, so that $a + B = 1 + B$. Therefore, $\phi(a) = (0 + A, 1 + B)$ Similar, $b = 1 - a$, so that $b + A = 1 + A$, and thus $\phi(b) = (1 + A, 0 + B)$. Let $(r_1 + A, r_2 + B) \in R/A \times R/B$. Then

$$\begin{aligned} \phi(r_1 b + r_2 a) &= \phi(r_1)\phi(b) + \phi(r_2)\phi(a) \\ &= (r_1 + A, r_1 + B)(1 + A, 0 + B) + (r_2 + A, r_2 + B)(0 + A, 1 + B) \\ &= (r_1 + A, 0 + B) + (0 + A, r_2 + B) = (r_1 + A, r_2 + B) \end{aligned}$$

Thus, it is surjective. □

This result leads to a ring-theoretic analogue of a theorem that maybe be a little more familiar to you:

Theorem 16.10 (Chinese Remainder Theorem)**.** *Let $A_1, \dots, A_n \subset R$ be a collection of pairwise comaximal ideals, i.e. $A_i + A_J = R$ for all $i \neq j$. Then*

$$\phi : R \to R/A_1 \times R/A_2 \times \cdots \times R/A_n$$

with $r \mapsto (r + A_1, r + A_2, \dots, r + A_n)$ has ϕ is surjective and that $\ker \phi = A_1 A_2 \dots A_n$. So $R/(A_1 \dots A_n) \cong R/A_1 \times R/A_2 \cdots \times R/A_n$.

Proof. By induction on n. For the base case $n = 1$, there is nothing to prove since then $A_1 = R$. For the induction hypothesis, suppose $R \to R/A_1 \times R/A_2 \times \cdots \times R/A_{n-1}$ is surjective with kernel $A_1 \dots A_{n-1}$. We now bootsrap to the n case with the prove position just proved. Let $A = A_1 \dots A_{n-1}$ and $B = A_n$.

we claim $A + B = R$. Enough to show there exists $a \in A, b \in B$ with $a + b = 1$. We know for any $i < n$, $A_i + A_n = R$, so there exists $a_i \in A, b_i \in A_n$ such that $a_i + b_i = 1$. Then multiplying them all together, we have that

$$\prod_{i=1}^{n-1} (a_i + b_i) = a_1 a_2 \dots a_{n-1} + b' = 1$$

for $b' \in B$, since each summand will contain some b_i. However, $a_1 a_2 \dots a_{n-1} + b' \in A + B$, so $A + B = R$.

Now, applying the proposition from before, we have that $\phi' : R \to R/A \times R/B$ is a surjection with $\ker \phi' = AB$. By the induction hypothesis, we have that $\alpha : R/A = R/A_1 A_2 \dots A_{n-1} \cong R/A_1 \times R/A_2 \times \cdots \times R/A_{n-1}$, so by composing with this mapping $\alpha \times 1$, we have a surjective mapping $\beta = (\phi \times 1) \circ \phi' : R \to R/A \times R/B \to R/A_1 \times R/A_2 \times \cdots \times R/A_{n-1} \times R/A_n$, as desired. □

What does this theorem have to do with the normal Chinese Remainder Theorem? Well, if we have integers $n_1, \dots, n_k$ are pairwise coprime and we have a system of congruences

$$\begin{aligned} x &\cong a_1 \mod n_1 \\ x &\cong a_2 \mod n_2 \\ &\vdots \\ x &\cong a_k \mod n_k \end{aligned}$$

Has a unique solution modulo $n_1 \dots n_k$. In other words, we are saying these is a surjective mapping

$$\mathbb{Z} \to \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$$

that is surjective, with an induced isomorphism

$$\mathbb{Z}/(n_1 \dots n_k)\mathbb{Z} \to \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$$

17. Lecture 17 — November 7,2018

Let R be an integral domain. We want to define a notion of **division with remainder** for such rings, analogous to that for the integers. We therefore define

Definition 17.1. A function $N : R \setminus 0 \to \mathbb{Z}_{\geq 0}$ is a **Euclidean function** if for all $a, b \in R$ and $b \neq 0$ we have $\exists\, q, r \in R$ such that $a = qb + r$ and $r = 0$ or $N(R) < N(b)$.

Definition 17.2. If a Euclidean function exists on R, R is called a **Euclidean domain**.

Proposition 17.3 (First Example)**.** *$\mathbb{Z}$ is a Euclidean domain*

Proof. Our candidate Euclidean function will be $N : \mathbb{Z} \setminus \{0\} \to \mathbb{Z}_{>0}$ sending $a \mapsto |a|$. Let $a, b, \in \mathbb{Z}$, $b \neq 0$. Then assuming $b > 0$ (the other case is the exact same), the intervals $[nb, (n+1)n) = \{k \in \mathbb{Z} \mid nb \leq < k < (n+1)b\}$ partition $\mathbb{Z}$. Thus, there exists q such that $a \in [qb, (q+1)b)$, which implies $a - qb \in [0, b)$. Let $r = a - qb$. Then $a = qb + r$ with $r \in [0, b)$, so that $r = 0$ or $|r| < |b|$, as desired. □

Example 17.4. Let F be a field. Then F is a Euclidean domain with candidate $N : F \setminus \{0\} \to \mathbb{Z}_{\geq 0}$ sending $a \mapsto 1$. Indeed, this is sort of silly, since given $a, b \in F$ with $b \neq 0$, we have that $a = ab^{-1} \cdot b + 0$, so that if $q = ab^{-1} \in F$ then $r = 0$, satisfying the desired property.

Theorem 17.5. *Suppose F is a field. Then the polynomial ring $F[x] = \{\sum_{k=0}^{n} \mid n \in \mathbb{N}, a_k \in F\}$ is a Euclidean domain.*

Proof. Define $N : F[x] \setminus \{0\} \to \mathbb{Z}_{\geq 0}$ sending $f \mapsto \deg f$. Where deg is the maximal k in $\sum_k a_k x^k$. Let $a(x), b(x) \in F[x]$, $b(x) \neq 0$. We will prove this by induction on $n = \deg a(x)$. The base case is $n = 0$, so that $a(x) \equiv C$, a constant. Then if $\deg b(x) = 0$, so $b(c) \equiv C_2$ a constant, and setting $q(x) \equiv C_1 C_2^{-1}$, we have $a(x) = q(x)b(x) + 0$ (this is basically just the case that F is a Euclidean domain). If $\deg b(x) > 0$. Then setting $q(x) = 0, r(x) \equiv C_1$, we have $a(x) = q(x)b(x) + r(x)$ where $\deg r(x) = 0 < \deg b(x)$.

For the induction step, assume $\forall\, a'(x) \in F[x]$ such that $\deg a'(x) \leq n - 1$, there exists $q'[x], r'[x] \in F[x]$ such that $a'(x) = q'(x)b(x) + r'(x)$, so that $r'(x) \equiv 0$ or $\deg r'(x) < \deg b$.

Now, let $m = \deg b(x)$. We have two cases

- $m > n$: Then set $q(x) = 0$, $r(x) = a(x)$, so that $a(x) = q(x)b(x) + r(x)$ for $\deg r = \deg a < \deg b$.
- $m \leq n$: For $a(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ $a(x) = b_m x^m + b_{m-1} x^{m-1} + \cdots + b_1 x + b_0$ for $a_n, b_m \neq 0$. Define $a'(x) = a(x) - \frac{a_n}{b_m} x^{n-m} b(x)$, which is well-defined because $m \leq n$, $b_m \neq 0$. This canceles out the leading term of $a(x)$, since $\frac{a_n}{b_m} x^{n-m} b_m x^m = a_n x^n$. Therefore, $\deg a'(x) \leq n - 1$, so by our induction hypothesis there exists $q'[x], r'[x] \in F[x]$ such that $a'(x) = q'(x)b(x) + r'(x)$, so that $r'(x) \equiv 0$ or $\deg r'(x) < \deg b$.

Define $q(x) = q'(x) + \frac{a_n}{b_m}x^{n-m}$ and $r(x) = r'(x)$. We have

$$\begin{aligned} a(x) &= a'(x) + \frac{a_n}{b_m}x^{n-m}b(x) \\ &= q'(x)b(x) + r'(x) + \frac{a_n}{b_m}x^{n-m}b(x) \\ &= (q'(x) + \frac{a_n}{b_m}x^{n-m})b(x) + r'(x) \\ & q(x)b(x) + r(x) \end{aligned}$$

with $r(x) = 0$ or $\deg r < \deg b$.

so we are done. □

Now that we have some examples of Euclidean domains, let's talk about some very nice properties of them.

Theorem 17.6. *If R is a Euclidean domain, then every ideal $I \subset R$ is **principal**, In particular, $I = (a)$ for some $a \in R$.*

Proof. Let $N : R \setminus 0 \to \mathbb{Z}_{\geq 0}$ be a Euclidean function. Then $I = \{0\} = (0)$ is principal. If $I \neq 0$, let $d \in I \setminus \{0\}$ be an element of **minimal norm**, i.e. $N(d)$ is minimal.

We claim $(d) = I$. Since $d \in I$, $(d) \subseteq I$. Conversely, suppose $a \in I$. Then there exists $q, r \in R$ such that $a = qd + r$ for $r = 0$ or $N(r) < N(d)$. But $r = a - qd \in I$, so it cannot have norm smaller than d (by our choice of element of smallest norm). Thus, $r = 0$ and $q = qd \in (d)$. So $I \subseteq (d)$, as desired. □

Remark 17.7. Where have we used the fact that R is an integral domain in this discussion? Well, technically we haven't, but the Euclidean norm function will not be so well-defined. In particular, often we will want a norm function to be multiplicative, or have other properties relating $N(ab)$ to $N(a), N(b)$, but recall that the Euclidean function is not defined on 0! So if $ab = 0$, then we cannot relate $N(ab)$ to $N(a), N(b)$, since $N(ab)$ is not well-defined.

Example 17.8. $\mathbb{Z}[x]$ is **not** a Euclidean domain, since it is not principal! In particular, the ideal $(2, x)$ was not principal, and the theorem just proved implies $\mathbb{Z}[x]$ cannot be Euclidean.

We will now assume that R is an arbitrary ring.

Definition 17.9. Let $a, b \in R$, $b \neq 0$. Then we day

- b **divides** a if $a = bx$ for some $x \in R$.
- a **greatest common divisor** of a and b is $d \in R$ if $d \mid a$ and $d \mid b$ so that if $f \mid a, b$ then $f \mid d$.

Remark 17.10. Note that gcd's are not unique! In particular, $3, -3$ are both gcd's of $6, 15$.

Remark 17.11. $b \mid a \iff a \in (b) \iff (a) \subseteq (b)$. More generally, d is a gcd of a and b provided that $(a, b) \subset (d)$ and if $(a, b) \subseteq (f)$ then $(d) \subseteq (f)$. Therefore, (d) is the minimal principal ideal containing (a, b).

Corollary 17.12. *If (a, b) is principal with $(a, b) = (d)$ then d is a gcd of a and b.*

18. Lecture 18 — November 12, 2018

Let R be an integral domain. Recall that given $a, b \in R$, we said $d \in R$ is a **greatest common divisor** (gcd) if $d \mid a$, $d \mid b$, and $d' \mid a$, $d' \mid b$ implies that $d' \mid d$. Recall that gcd's are not necessarily unique.

Remark 18.1.

$$\begin{aligned} d \mid a &\iff \exists x \in R \text{ such that } a = xd \\ &\iff a \in (d) \\ &\iff (a) \subseteq (d) \end{aligned}$$

Using this remark, we can rephrase the definition of greatest common divisor. Namely, we have that d is a gcd of a and b if

(1) $(a) \subseteq (d), (b) \subseteq (d)$, or equivalently, $(a, b) \subset (d)$
(2) If $(a, b) \subset (d')$ implies that $(d) \subseteq (d')$

Remark 18.2. Further rephrasing this definition, we have that d is a gcd of a and b iff (d) is the **minimal** principal ideal containing (a, b). Note then that in this case, for any gcds d, d', we have by minimality that $(d) = (d')$, so the idela generated by a gcd is unique.

Corollary 18.3. *Suppose (a, b) is principal $(a, b) = (f)$ then f is a gcd of a and b.*

Remark 18.4. The converse does not hold. For example, we have previously showed $(2, x) \subset \mathbb{Z}[x]$ is **not** principal, but the gcd of $2, x$ is 1 since only $\pm 2, \pm 1$ divides 2 and $\pm 1, \pm x$ divides x.

So how can we describe gcds? This next proposition does this.

Proposition 18.5. *Suppose $x, y \in R \setminus \{0\}$. Then $(x) = (y) \iff$ there is a unit $u \in R$ such that $y = ux$.*

Proof. If two elements x, y differ by a unit, then we have that $(x) = (y)$ by a question on the homework.

If $y \in (x)$ then there exists $u \in R$ such that $y = ux$. Likewise, if $x \in (y)$ then there exists $v \in R$ such that $x = vy$. Then $y = ux = uvy$. By the cancellation property of **integral domains**(this is where we use the fact that R is an integral domain), we have $1 = uv$, so u is a unit. □

Corollary 18.6. *Suppose d is a gcd of a and b. Then $d' \in R$ is a gcd of a, b iff there exists $u \in R$ a unit such that $d' = ud$*

Proof. d' is a gced of a, b iff $(d') = (d)$, iff there exists a unit u such that $d' = ud$. □

Lemma 18.7. *Suppose $a, b, q, r \in R$ such that $a = qb + r$. Then $(a, b) = (b, r)$*

Proof. We show mutual containments. First, $b \in (b, r)$ and $a = qb + r \in (b, r)$, so $(a, b) \subseteq (b, r)$. Likewise, $b \in (a, b)$ and $r = a - qb \in (a, b)$, so $(b, r) \subseteq (a, b)$, finishing both containments. □

Suppose R is a Euclidean domain. Then $N : \mathbb{R} \setminus \{0\} \to \mathbb{Z}_{\geq 0}$ such that for all $a, b \in R$ and $b \neq 0$. Then there exists $q, r \in R$ such that $a = qb + r$ for $r = 0$ or $N(r) < N(b)$. We will use this fact to compute the gcd, via the Euclidean Algorithm.

The Euclidean Algorithm arises via iterated division algorithm

$$\begin{aligned} a &= q_1 b + r_1, N(r_1) < N(b) \\ b &= q_2 r_1 + r_2, N(r_2) < N(r_1) \\ r_2 &= q_3 r_2 + r_3, N(r_3) < N(r_2) \\ &\vdots \end{aligned}$$

Lemma 18.8. $\exists r_{k+1} = 0$. *In other words, the Euclidean algorithm terminates.*

Proof. Let r_k be the last nonzero remainder of the Euclidean algorithm applies to a, b. Then $(a, b) = (r_k)$ so r_k is a gcd of a, b. □

Using the general lemma about the division algorithm, we have that in the Euclidean Algorithm we have $(a, b) = (b, r_1) = (r_1, r_2) = (r_2, r_3) \cdots = (r_{k-2}, r_k) = (r_k, r_{k+1}) = (r_k)$ since eventually $r_{k+1} = 0$.

Example 18.9. $R = \mathbb{Z}$, $a = 2210$, $b = 1131$.

$$\begin{aligned} 2210 &= 1 \cdot 1131 + 1079 \\ 1131 &= 1 \cdot 1079 + 52 \\ 1079 &= 20 \cdot 52 + 39 \\ 52 &= 1 \cdot 39 + 13 \\ 39 &= 3 \cdot 13 + 0 \end{aligned}$$

Thus, $\gcd(a, b) = 13$.

Generally, Euclidean algorithm terminates quite quickly. Just as a note, the whole intuition of the Euclidean algorithm is that when one does division with remainder, the gcd of the original numbers is the same as the gcd of the remainder and the smaller number. Iterating down then yields the gcd.

In this section we will construct an integral domain in which every ideal is principal and proof that we cannot put a Euclidean function on it.

Example 18.10. Let $\theta = \frac{1}{2}(1 + \sqrt{-19})$. Then $\mathbb{Z}[\theta] = \{a + b\theta \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$. One can easily check that $\mathbb{Z}[\theta]$ is a subring of $\mathbb{C}$. For all complex numbers $x + iy$, let $\|x + iy\| = x^2 + y^2 = (x + iy)(x - iy)$. Then $a + b\theta = a + \frac{b}{2} + \frac{\sqrt{-19}}{2}b$. Then $\|a + b\theta\| = (a + b/2)^2 + (g\sqrt{19}/2)^2 = a^2 + ab + b^2/4 + 19b^2/4 = a^2 + ab + 5b^2$.

Remark 18.11. If $(a + b\theta) \mid (c + d\theta)$ then $\|a + b\theta\| \mid \|c + d\theta\|$.

We then claim that $\mathbb{Z}[\theta]^\times = \pm$, since if $a + b\theta$ is a unit then $(a + b\theta) \mid 1 \implies \|a + b\theta\| \mid N(1) = 1$, so $a^2 + ab + 5b^2 = 1$. It is easy to check that the only way to get 1 is by $a = \pm 1$,

$b = 0$.

We then claim (without justification, since we do not have time)

(1) The only divisors of $2 \in \mathbb{Z}[\theta]$ are $\pm 1, \pm 2$.
(2) The only divisors of $3 \in \mathbb{Z}[\theta]$ are $\pm 1, \pm 3$.

Suppose that $\mathbb{Z}[\theta]$ is a Euclidean domain, so that it has Euclidean function N. Choose $x \in \mathbb{Z}[\theta]$ such that $x \neq 0, \pm 1$ and $N(x)$ is minimal. Then we have $2 = qx + r$ with $N(r) < N(x)$ or $r = 0$. We have some cases

- $r = 0 \implies x \mid 2 \implies x = \pm 2$
- $r = -1 \implies x \mid 3 \implies x = \pm 3$
- $r = 1 \implies 2x \mid 1$, contradiction.

Then $\theta = q'x + r'$ with $N(r') < N(r)$ or $r' = 0$. Then for

- $r' = 0 \implies x \mid \theta$, so $\|x\| \mid \|\theta\| = 5$, contradicting that $N(x) = 4$ or 9.
- $r' = -1 \implies x \mid \theta + 1$, so $\|x\| \mid \|\theta + 1\| = 7$, contradicting that $N(x) = 4$ or 9.
- $r' = 1 \implies x \mid \theta - 1$, so $\|x\| \mid \|\theta - 1\| = 5$, contradicting that $N(x) = 4$ or 9.

Thus, such a Euclidean function cannot exist. In a sense, the onyl way to measure the size of numbers in a subring of $\mathbb{C}$ should rise from the usual norm on $\mathbb{C}$, but that does not quite work in this case.

19. Lecture 19 — November 19, 2018

Definition 19.1. An integral domain R is said to be a **principal ideal domain**.

Example 19.2. All Euclidean domains are principal ideal domains! For example, $\mathbb{Z}$, fields ($\mathbb{R}, \mathbb{C}, \mathbb{Q}, \mathbb{Z}/p\mathbb{Z}$).
The ideals of $\mathbb{Z}$ are all of the form $n\mathbb{Z}$, and a field F has ideals $0, F$.

Example 19.3. $\mathbb{Z}[x]$ is **not** a principal ideal domain, since $(2, x)$ is not principal.
As a sillier example, $\mathbb{Z}/n\mathbb{Z}$ is **not** in general a principal ideal domain even though all ideals are principal, since it is not an integral domain!

Recall that we had

Theorem 19.4. *R Euclidean domain $\implies$ R principal ideal domain*

Proof. We used the Euclidean algorithm. □

What is the main difference between a Euclidean domain and a principal ideal domain?

Remark 19.5. In a Euclidean domain, every ideal is principal **and** there is an algorithm to compute **how** an ideal is principal. In particular, if the ideal $(a, b) = (d)$ whenever R is a PID, but computing x, y such that $ax + by = d$ is hard without a Euclidean function.

Remark 19.6. Note that by iterating the construction of $(a, b) = (d)$, we cna find larger gcd's, such as $(a_1, \ldots, a_k) = (d)$.

Here's big theorem about principal ideal domains:

Theorem 19.7. *If R is a PID then every nonzero prime ideal P is maximal.*

Proof. Let $P \subseteq R$ be a nonzero prime ideal. Then $P = (\alpha)$. Suppose $\exists \beta$ such that $(\alpha) \subsetneq (\beta) \subsetneq R$. (α) beign prime implies that the element $\alpha \mid ab \implies \alpha \mid a$ or $\alpha \mid b$. Recall also that $(\alpha) \subsetneq (\beta) \subsetneq R$ is equivalent to $\beta \mid \alpha$, so that there exists γ such that $\beta\gamma = \alpha$.

Then $\alpha \mid \beta\gamma \implies \alpha \mid \beta$ or $\alpha \mid \gamma$. Suppose $\alpha \mid \beta$. Then $(\beta) \subseteq (\alpha)$, a contradiction. Suppose instead that $\alpha \mid \gamma$. Then there exists δ such that $\gamma = \alpha\delta$. Then $\alpha = (\beta\delta)\alpha$, which by cancellation (using that fact that R is an integral domain!), we have $\beta\delta = 1$, so β is a unit and $(\beta) = R$, contradiction! □

Example 19.8. $\mathbb{Z}[i]$ is a Euclidean domain.

Proof. The proof is very geometric, so you all will have to wait on getting a diagram from me.....

Consider any α in $\mathbb{Z}[i]$ and $\beta \in \mathbb{Z}[i]$. Our candidate Euclidean function is $N(a+bi) = |a+bi|^2 = a^2 + b^2$. We then want $q, r \in \mathbb{Z}[i]$ such that $\alpha = q\beta + r$. Note now that $|r| < \beta$ such that $|r| < |\beta|$ or $r = 0$. In otherwords, we want $|\alpha - q\beta| < |\beta| \iff |\alpha/\beta - q| < 1$. To show that this last part is possible, one notes that the lattice of squares inside $\mathbb{Z}[i]$ is tiled by squares of side length 1, and so any point in $\mathbb{C}$ is distance at most $\sqrt{2}/2$ from a point in $\mathbb{Z}[i]$. Therefore, by translating a complex number, we can find q such that $|\alpha/\beta - q| \leq \sqrt{2}/2 < 1$, as desired. Geometrically, what we are saying is that the circles of radius 1 on points of $\mathbb{Z}[i]$ cover the entire complex plane. □

Example 19.9. A very analogous example is $\mathbb{Z}[\omega] = \mathbb{Z}[1/2(1+\sqrt{-3})]$. In this case, our lattice is spanned by equilateral triangles of side length 1, and so again radius 1 balls around each of the lattice points fill the region.

Example 19.10. However, $\mathbb{Z}[\sqrt{-3}]$ is NOT a PID. In particular, we have that the lattice is spanned by $30-60-90$ righ triangles, with side lengths $\sqrt{3}, 1, 2$. Then consider the mid points of any hypotenuse. It is distance exactly 1 to the closest lattice point. but our proof from before required a distance of strictly less than 1!
Since our proof from before does not work, let's see if we can actually find an ideal that is not principal. We claim that $I = (2, 1+\sqrt{-3})$ is not principal. But this is kind of annoying to prove, so we will instead show that the ideal $I = (2, 1+\sqrt{-5})$ is not principal in the ring $\mathbb{Z}[\sqrt{-5}]$. If $(2, 1+\sqrt{-5}) = (a + b\sqrt{-5})$ then $(2, 1-\sqrt{-5}) = (a - b\sqrt{-5})$ Then we have that $(2, 1+\sqrt{-5})(2, 1-\sqrt{-5}) = (4, 2(1-\sqrt{-5}), 2(1+\sqrt{-5}), 6) = (2) = (a^2 + 5b^2)$. So $a^2 + 5b^2 = u \cdot 2$ where u is a unit in $\mathbb{Z}[\sqrt{-5}]$. But since $u \cdot 2$ is real, $u = 1$, but there are no solutions to $a^2 + 5b^2 = 2$ in the integers, contradiction.

All of these examples are setting us up to proof the following big boy.

Theorem 19.11. $\omega = \frac{1+\sqrt{-19}}{2}$, $\mathbb{Z}[\omega]$ *is a PID.*

Proof. See Hunter's handout. It has all the annoying details you need to show this... □

20. Lecture 20 — November 26, 2018

So far in this class we have defined Integral domains, Principal Ideal domains, Euclidean domains, and fields. We have the following containments of ideals

$$\{\text{Fields}\} \subset \{\text{EDs}\} \subset \{\text{PIDs}\} \subset \{\text{IDs}\}$$

Note that further, we can take the GCD of any two elements a, b in a PID by noting the ideal $(a, b) = (d)$ for some d, and this d is a GCD in some sense. But remember that we usually find GCD's by prime factorizing numbers, and taking the minimum amount of powers for each factor between the two numbers. To bring this intuition to the land of domains, we will develop another class of domains that contain PIDs.

We will now make a definition:

Definition 20.1. A nonzero, non-unit element $x \in R$ is **irreducible** if

$$x = ab \implies a \text{ or } b \text{ is a unit}$$

Example 20.2.
- $2 \in \mathbb{Z}$,all primes $\in \mathbb{Z}$.
- $x \in \mathbb{R}[x]$ since all constants are units in $\mathbb{R}[x]$ (since $\mathbb{R}$ is a field).

Definition 20.3. A pair of nonzero non-unit elements a,b are **associate** if there exists a unit $u \in R^\times$ such that $a = ub$.

Example 20.4. $\mathbb{Z}^\times = \{\pm 1\}$. Thus, the associates of 2 are ± 2.

Example 20.5. $\mathbb{Z}^\times = \{\pm 1, \pm i\}$. Thus, the associates of 2 are $\pm 2, \pm 2i$.

Example 20.6. $\mathbb{R}[x]^\times = \mathbb{R} \setminus \{0\}$. Thus, the associates of x are cx for $c \neq 0$.

Lemma 20.7. *The following are equivalent:*

(1) a, b *are associates*
(2) $a \mid b$ *and* $b \mid a$
(3) $(a) = (b)$.

Definition 20.8. A nonzero $p \in R$ is **prime** if (p) is a prime ideal.

Note that (p) is prime iff $ab \in (p) \implies a \in (p)$ or $b \in (p)$. In other words, $p \mid ab \implies p \mid a$ or $p \mid b$.

- In $\mathbb{Z}$, prime and irreducible are equivalent conditions. This you prove in an elementary number theory course, but it is not too hard! We encourage you to try it.

Example 20.9. $x \in \mathbb{Z}[x]$ is prime because $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$ is an integral domain, so (x) is prime.

Remark 20.10. Observe that primes cannot be units, since units generate the whole ring, which is

Proposition 20.11. *Suppose $p \in \mathbb{R}$ is prime. Then p is irreducible.*

Proof. Suppose that $p = ab$. Then by primality, $p \mid a$ or $p \mid b$. WLOG suppose $p \mid a$, so that $a = pu$ for $u \in R$. Then $p = ab = pub$. Since we are working in an integral domain, we have $p = pub \implies 1 = ub$, so that b is a unit. □

Remark 20.12. Irreducible does **not** implies prime, however. For example in $\mathbb{Z}[\sqrt{-5}]$. We claim the element 3 is irreducible. If $3 = (a + b\sqrt{-5})(c + d\sqrt{-5})$ then $a^2 + 5b^2 = 1, 3, 9$. It is not 1 since we are assuming $a + b\sqrt{-5}$ is not a unit (otherwise $a^2 + 5b^2 = (a + b\sqrt{-5})(a - b\sqrt{-5}) = 1$, so it would be a unit). There are no solutions $a^2 + 5b^2 = 3$, so we must have $\|a + b\sqrt{-5}\| = 9$, and thus $\|c + d\sqrt{-5}\| = 1$ so $c + d\sqrt{-5}$ is a unit.

On the other hand, we also claim 3 is **not** prime. In need, $3 \mid 9 = (2 + \sqrt{-5})(2 - \sqrt{-5})$ but $3 \nmid (2 \pm \sqrt{-5})$, so 3 is not prime.

Proposition 20.13. *Suppose R is a PID. Then $p \in R$ is prime iff it is irreducible.*

Proof. $\implies$ was already proved for any integral domain. Now, suppose $p \in R$ is irreducible. Let I be an ideal such that $I \supset (p)$. Recall now from last class that all nonzero prime ideals are **maximal**. So instead, the goal will be to show that any ideal $I \supset (p)$ implies $I = (p)$ or $I = R$. We know that since R is the PID that $I = (a)$. Then $(a) \supset (b)$ implies that $p = ab$ for some $b \in R$. But since p is irreducible, $a \in R^\times$ or $b \in R^\times$. If a is a unit then $a = R$, and if $b \in r^\times$ then $I = (a) = (p)$. Thus, (p) is maximal, and thus also prime. □

Definition 20.14. R is a **unique factorization domain**(UFD) if for all nonzero, nonunit $a \in R$ we have

- $a = p_1 \dots p_k$ a finite product of irreducibles.
- This factorization is unique: If $a = q_1 \dots q_m$ another product of irreducibles. Then $m = n$, and up to indexing, p_i and q_i are associate.

Example 20.15. $\mathbb{Z}$ is a UFD. For example, $42 = 2 \cdot 3 \cdot 7 = (-7) \cdot (-2) \cdot 3$.

Example 20.16. All fields are UFDs... Nothing to check since all nonzero elements are units.

Proposition 20.17. *Suppose R is a UFD. Then $x \in R$ is prime iff it is irreducible.*

Proof. The forward direction we have already done. Conversely, let $p \in R$ be irreducible. Suppose $p \mid ab$ so that there exists c such that $pc = ab$. Then write in prime factors $a = p_1 \dots p_n$, $b = q_1 \dots q_m$ and $c = r_1 \dots r_l$ so that

$$pr_1 \dots r_l = p_1 \dots p_n q_1 \dots q_m$$

p is assocate to some p_i or q_i by unique factorization. WLOG, say p is associate to p_1. Then there exists $u \in R^\times$ such that $p_1 = up$. Then $a = upp_2 \dots p_n$ and $p \mid a$, so p is prime. □

21. Lecture 21 — November 28, 2018

Last time we introduction the notion of irreducible and prime elements, and how they relate to a class of integral domains called **unique factorization domains**. We showed any prime element is irreducible, and in a PID or UFD that an irreducible is prime.

But in the case of a UFD, we have a converse of sorts:

Proposition 21.1. *R is a UFD $\iff$:*

(1) every nonzero, non-unit element is a finite product of irreducibles.
(2) irreducible $\implies$ prime.

Example 21.2. Here is an example where property 1) does not hold: Let

$$R = \{f(x) \in \mathbb{Q}[x] \mid f(0) \in \mathbb{Z}\}$$

We note that the units are $R^\times = \{\pm 1\}$ since these are the only integers with integer inverses. The key to this example is that when we try to factor a polynomial into irreducibles, our factoring never ends! For example,

$$x = 2 \cdot (x/2) = 2 \cdot (2 \cdot x/4) = 8 \cdot x/8 \cdots = 2^n(x/2^n)$$

where all the elements in these factorization are not units. Note that all of the 2's are irreducible, and infinitely many keep showing up in the factorization,

Proof. We already showed that UFD implies $1), 2)$. For the opposite direction, since we already know that any $a \in R$ is a finite product of irreducibles, Suppose that

$$a = p_1 \dots p_n = q_1 \dots q_m$$

are two different factorizations into irreducibles. We wish to show that $n = m$ and up to reindexing, p_i is associate to q_i. We will show this by induction on n.

Base case: $n = 1$ then $p_1 = q_1 q_2 \dots q_m$ but p_1 irreducible, so $m = 1$ and $p_1 = q_1$.

Induction hypothesis: If $p_1 \dots p_{n-1} = q_1 \dots q_l$ then $n - 1 = l$ and up to reindexing, $p_i \sim q_i$. Now consider the the case of n:

$$a = p_1 \dots p_n = q_1 \dots q_m$$

Then $p_n \mid q_1 \dots q_m$ and since p_n is prime, $p_n \mid q_i$ for some i. WLOG say that $p_n \mid q_m$. Then $q_m = up_n$ for $u \in R^\times$, so $p_n = q_m$. So then

$$p_1 \dots p_n = q_1 \dots up_n$$

Since we are in an integral domain, we can cancel to get

$$p_1 \dots p_{n-1} = q_1 \dots (uq_{n-1}) = q_1 \dots q'_{m-1}$$

is an equality of products of irreducibles. Now, applying the induction hypothesis says $n-1 = m-1 \implies n = m$ and up to reindexing $p_i \sim q_i$, for $i \leq m-2$, $p_{n-1} \sim q'_{n-1} \sim q_{n-1}$ and $p_n \sim q_n$, as desired. □

Here is a very nice application of the proposition:

Theorem 21.3. *If R is a PID then R is a UFD*

Proof. Irreducible $\iff$ prime has already been proved, so it suffices to show that any $a \in R$ is a finite product of irreducibles. Suppose towards contradiction that $\exists$ nonzero non-unit $a_0 \in R$ with no finite product of irreducibles. Then if a_0 not irreducible then $a_0 = a_1 b_1$ with a_1, b_1 nonzero non-units, and WLOG a_1 ia not a finite product of irreducibles. Then a_2 is not irreducible (since it is not a finite product of irreducibles) so $a_1 = a_2 b_2$ where a_2, b_2 nonzero non-unit and a_2 is not a finite product of irreducibles.

This process yields an infinite sequence of elements $a_0, a_1, \dots$ such that $a_{i+1} \mid a_i \implies (a_i) \subsetneq (a_{i+1})$ since $b_{i+1} \notin R^\times$ by assumption. Therefore, we have a strictly ascednign sequence of ideals

$$(a_0) \subsetneq (a_1) \subsetneq (a_2) \subsetneq \dots$$

Now consider the ideal $I = \cup_{i=0}^{\infty}(a_i)$. By homeowkr, since this is a nested sequence, this is an ideal. Since we are in a PID, $I = (x)$ for some $x \in R$. Moreover, there exists $n \in \mathbb{N}$ such that $x \in (a_n)$. But then $I = (x) \subseteq (a_n) \subsetneq (a_{n+1}) \subset I$. But since $I = (x)$, $(a_n) = (a_{n+1})$, contradicting the strict containment. □

So now we can further detail our set of inclusions:

$$\{\text{Fields}\} \subsetneq \{\text{EDs}\} \subsetneq \{\text{PIDs}\} \subseteq \text{UFDs} \subsetneq \{\text{IDs}$$

So this may beckon the following question: are there UFDs that are not PIDs? The answer is yes, and the examples will not be as far-fetched in particular, we will show that $\mathbb{Z}[x]$ is a UFD at some point, but we already know this is not a PID since $(2, x)$ is not principal.

Here is a general construction: Given an integral domain R, we can form a field $\text{Fr}(R)$, called its **field of fractions**. Namely

$$\text{Fr}(R) = \{a/b \mid a, b \in \mathbb{R}, b \neq 0\}/\sim$$

where $\sim$ is the relation $a/b \sim c/d \iff ad = bc$. This is a generalization of going from the integers to fractions. We claim that $\sim$ is an equivalence relation. We can then define operations on $\text{Fr}(R)$ via $a/b + c/d = (ad + bc)/bd$ and $a/b \cdot c/d = ac/bd$. We claim $+, \cdot$ are well-defined under this equivalence relation.

22. Lecture 22 — December 3, 2018

Let R be an integral domain. Last time we constructed a set $\text{Fr}(R) = \{(a, b) \mid a, b \in R, b \neq 0\}/\sim$. With the equivalence relation $(a, b) \sim (c, d) \iff ad - bc = 0$. The fact that $\sim$ is an equivalence relation is left to the reader. We write $(a, b) = a/b$ usually. We then defined $a/b + c/d = (ad + bc)/bd$ and $a/b \cdot c/d = (ac)/bd$.

Proposition 22.1. *$+$ and $\cdot$ are well-defined.*

Proof. We will only prove that $+$ is well-defined. We leave the case of $\cdot$ as an exercise. Note that $a_1/b_1 \sim a_2/b_2 \iff a_1b_2 = a_2b_1$ and $c_1/d_2 \simeq c_2/d_2 \iff c_1d_2 = c_2d_1$.

Then $a_1/b_1 + c_1/d_1 = (a_1d_1 + b_1c_1)/b_1d_1$ and $a/b + c/d = (a_2d_2 + b_2c_2)/b_2d_2$. Now,

$$(a_1d_1 + b_1c_1) \cdot (b_2d_2) = a_1b_2d_1d_2 + b_1b_2c_1d_2 = a_2b_1d_1d_2 + b_1b_2c_2d_1 = (a_2d_2 + b_2c_2) \cdot (b_1d_1)$$

In turn implies that $+$ is well-defined. □

Proposition 22.2. $\mathrm{Fr}(R)$ *is a field under* $+, \cdot$*, usually called the* ***field of fractions of*** R*.*

Proof. It is easy to check that $+, \cdot$ are commutative and associative. For additive identity, we take $0 = 0/b$ for all $b \neq 0$. For inverses of a/b we take $-(a/b) = (-a)/b = a/(-b)$. For multiplicative identity we take $1 = b/b$ for all $b \neq 0$, and for multiplicative inverse of a/b we take $(a/b)^{-1} = (b/a)$. □

Example 22.3. $\mathrm{Fr}(\mathbb{Z}) = \mathbb{Q}$.
$\mathrm{Fr}(\mathbb{R}[x]) = \{p(x)/q(x) \mid p, q \in \mathbb{R}[x], q \neq 0\}$.

Example 22.4. $\mathrm{Fr}(\mathbb{Z}[i]) = \mathbb{Q}[i] = \{r + is \mid r, s \in \mathbb{Q}\}$. The reason for this is that we can always rationality the denominators of quotients of complex numbers by multiplying by the conjugate.

Remark 22.5. There is an injective ring homomorphism $R \to \mathrm{Fr}(R)$ sending $a \mapsto a/1$ (it is injective since $a/1 = b/1 \implies a = b$.) We can thus view $R \subset \mathrm{Fr}(R)$.

Recall now that $R[x] = \{\sum_{k=0}^{n} a_k x^k \mid a_k \in R\}$ and $R[x_1, \ldots, x_n] = \{\sum_{k_1,\ldots,k_n} a_{k_1,\ldots,k_n} x_1^{k_1} \ldots x_n^{k_n}\}$.

Definition 22.6. Given $f(x) = \sum_{k=0}^{n} a_k x^k$ with $a_n \neq 0$ (leading coefficient), then the **degree** of f is denoted $\deg f = n$.

Proposition 22.7. *(1)* $f(x), g(x) \in R[x]$ *are nonzero* $\implies \deg(fg) = \deg(f) + \deg(f)$.
(2) R *integral domain* $\implies R[x]$ *integral domain.*
(3) $(R[x])^\times = R^\times$.

Proof. (1) Suppose f, g have leading terms $a_n x^n$ and $b_m x^m$. Then $f(x)g(x) = a_n b_m x^{n+m} +$ (lowerdegreeterms). R being an integral domain $a_n b_m \neq 0$ so $\deg(fg) = n + m$.
(2) Follows immediately from 1.
(3) If $p(x) \in (R[x])^\times$ then there exists $g(x) \in R[x]$ such that $p(x)q(x) = 1$ which has degree 0, so by 1. we must have $\deg p = \deg q = 0$. Thus, $p \in R^\times$.
□

Proposition 22.8. *Let* $I \subset R$ *be an ideal and let* $I[x] = \{\sum_{k=0}^{n} a_k x^k \mid a_k \in I\}$*, i.e. the ideal generated by* I *in* $R[x]$*. Then*
(1) $(R[x]/I[x]) \cong (R/I)[x]$
(2) I *prime implies* $I[x]$ *is prime.*

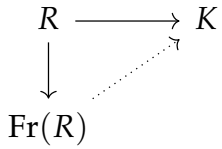
Proof. (1) HW

(2) I prime $\implies$ R/I is an integral domain, which then by our previous proposition implies that $R[x]/I[x]$ is an integral domain. Therefore, $I[x] \subset R[x]$ is also prime.

□

Now let $F = \text{Fr}(R)$ and consider the inclusion $R[x] \subset F[x]$. Recall that F field implies that $F[x]$ is a Euclidean domain, and thus also a PID and UFD. Note that $R[x]$ UFD implies R is a UFD, by looking at degree 0 terms. But if R is a UFD, must $R[x]$ be a UFD?

Remark 22.9. The field of fractions is actually a special case of a more general procedure in algebra called **localization**. Here is an insight as to how it works: Suppose that there is an injective homomorphism from $R \to K$ where K is a field then there is a unique homomorphism $\text{Fr}(R) \to K$ that makes the diagram commute:



This philosphy is what leads to the construction of localization.

To say anything about factorization in $R[x]$, we will need the following lemma:

Proposition 22.10 (Gauss' Lemma)**.** *Suppose R is a UFD, $f(x) \in R[x]$. If $f(x)$ is a reducible in $F[x]$ then it is reducible in $R[x]$. More generally, if $f(x) = P(x)Q(x)$, $P, Q \in F[x]$ nonunits then there exists $r, s \in F$ such that $p(x) = rP(x) \in R[x]$ and $q(x) = sQ(x) \in R[x]$ with $f(x) = p(x)q(x)$.*

Proof. Suppose that $f(x) = P(x)Q(x)$. Then $P(x) = a_0/b_0 + a_1/b_1 x + \cdots + a_n/b_n x^n$ and $Q(x) = c_0/d_0 + c_1/d_1 x + \cdots + c_m/d_m x^m$. Then let $d = b_0 \dots b_n d_0 \dots d_m$. Then $df(x) = g(x)h(x)$ where $g(x) = b_0 \dots b_n P(x)$ and $h(x) = d_0 \dots s_n Q(x)$ so that $g(x), h(x) \in R[x]$. Now we have two cases:

- $d \in R^\times$. Then we can set $p(x) = d^{-1} f(x)$ and $q(x) = h(x)$ so that $f(x) = p(x)q(x)$.
- If $d \notin R^\times$ then $d = p_1 p_2 \dots p_n$ such the p_i are irreducible in R, and thus prime in R since R is a UFD. Then $(p_1) \subset R$ prime. Then $(p_1)[x] \subset R[x]$ is prime, so p_1 is a prime in $R[x]$. Since $p_1 \mid g(x)h(x) \implies p_1 \mid g(x)$ or $p_1 \mid h(x)$. WLOG suppose $p_1 \mid g(x)$. Then $p_1 \dots p_n f(x) = g(x)h(x)$ implies $p_2 \dots p_n f(x) = (\frac{1}{p_1} g(x))h(x)$ where $\frac{1}{p_1} g(x) \in R[x]$. Then following the same procedure we can cancel to get a factorization in $R[x]$ of $f(x) = p(x)q(x)$.

□

What about the **converse**? If $f(x) \in R[x]$, and f is reducible in $R[x]$, must f be reducible in $F[x]$? The Answer

Example 22.11 (Reducible in $\mathbb{Z}$ does NOT imply reducible in $\mathbb{Q}$)**.** Let $R = \mathbb{Z}$. Consider the polynomial $f(x) = 2x + 2 \in \mathbb{Z}[x]$. Then $f = 2 \cdot (x + 1) \in \mathbb{Z}[x]$ is a factorization. But in $\mathbb{Q}[x]$, $2x + 2$ is irreducible because $\mathbb{Q}$ is a field and all degree 1 polynomials in polynomial ring over a field are irreducible (since it will be a product of a degree 0 and degree 1 piece, and all constants are invertible).

23. Lecture 23 — December 5, 2018

The goal for today (the final lecture) is to proof that if R is a UFD then $R[x]$. We already saw that $R[x]$ being a UFD implied that R is a UFD. To get there, we will build on Gauss' lemma, proved yesterday in class. First, we start with a Lemma:

Lemma 23.1. *R is a UFD implies that $f(x) = a_0 + a_1x + \cdots + a_nx^n \in R[x]$. Suppose that $\gcd(a_0, a_1, \ldots, a_n) = 1$. Then $f(x)$ is reducible in $F[x]$ iff it is reducible in $R[x]$.*

Proof. The forward direction follows from Gauss' Lemma. For the backward direction, suppose $f(x) = p(x)q(x)$ with $p(x), q(x) \in R[x]$ non-units. Since gcd of the coefficients of f is 1, p, q are both nonconstant, so $\deg p, \deg q > 0$, so $p(x), q(x)$ are not units in $F[x]$. Therefore, $f(x)$ is reducible in $F[x]$. □

Now we are ready to prove our theorem:

Theorem 23.2. *R is a UFD $\iff$ $R[x]$ is a UFD.*

Proof. The backward direction was already done. Now, consider $f(x)$ R$[x]$ and let d be the gcd of the f coefficients. Then $f(x) = dg(x)$ with g having the gcd of its coefficients 1. This choice of g is unique up to multiplication by a unit. Since R is a UFD, d has a unique factorization into irreducibles, so it is sufficient to show that $g(x)$ has a unique factorization as well.

Therefore, WLOG assume the gcd of the coefficients of f is 1. Then $\deg f > 0$, so $f(x)$ is not a unit in the ring of polynomials with coefficients. Now we have two cases:

- f is irreducible in $F[x]$: Then by the lemma we just proved, $f(x)$ irreducible in $R[x]$ iff it is irreducible in $R[x]$, so f is also irreducible in $R[x]$.
- f is reducible in $F[x]$: Then we have a factorization

  $$f(c) = P_1(x) \ldots P_n(x)$$

  where $P_i(x)$ is irreducible in $F[x]$. Then by Gauss' Lemma we have there exists a collection of $r_i \in F$ such that $p_i = r_iP_i \in R[x]$ and $f(x) = p_i(x) \ldots p_n(x)$. Since the gcd of the coefficients of f is 1, we also have that the gcd of the coefficients of each p_i is 1, so $p_i(x)$ is irreducible in $R[x]$. Therefore $r_i \in F^\times$, so p_i is irreducible in $F[x]$.

  We now wish to show that this decomposition is unique. Say that

  $$f(x) = p_1(x) \ldots p_n(x) = q_1(x) \ldots q_m(x)$$

  for p_i, q_i irreducible in $R[x]$. Since the GCD of the coefficients of f is 1, the gcd of the coefficients of all the p_i, q_i is also 1. Our lemma then tells us that p_i, q_i is irreducible in $F[x]$. $F[x]$ is a UFD, so $n = m$ up to ordering, $p_i \sim q_i$ in $F[x]$. so there exists

$a/b \in F$ such that $p_i = a/bq_i$. We wish to show $a/b \in R^\times$. Indeed, $bp_i = aq_i$ and $\gcd(bp_i \text{ coeffs}) = b = \gcd(aq_i \text{ coeffs}) = a$. Therefore, $a \sim b$ in R, and so $a/b \in R^\times$. □

Corollary 23.3. *If R is a UFD, then $R[x_1, \ldots, x_n]$ is a UFD.*

Remark 23.4. $R[x_1, \ldots, x_n] = (R[x_1, \ldots, x_{n-1}])[x_n]$.

Proof. Induction on n using the remark. The base case is that if R is a UFD then $R[x_1]$ is a UFD by our theorem just proved. The induction follows analogously. □

Note that this now gives an example of a UFD that is not a PID, showing strict inclusion of PI