MATH 402A: Introduction to Modern Algebra I

University of Washington

Andrew Chen

Autumn 2025

Hello and welcome! This is my lecture notes on MATH 402A – Introduction to Modern Algebra I. This course is the first of three courses on abstract algebra offered here at UW (why does the series start at 402 and not 401? Who knows). The professor is **Isabella Novik**, and we meet MWF at **10:30 am** for lectures. The textbook that we are using is **Thomas W. Hungerford's Abstract Algebra, an Introduction**. Also note that theorem names might not necessarily be accurate; it's probably just whatever my textbook / professor said it is.

The goal of these lecture notes is to write **understandable** math. As the great Albert Einstein put it, "If you can't explain it to a six year old, then you don't understand it yourself". The hope is that anyone coming across these notes (like you!) will be able to at least take away the gist of these concepts. Should you find any errors in my mathematics, please contact me at zchen66@uw.edu

Contents

List of Definitions

List of Theorems

1 Lecture 01: Sept. 24th

Today was the first lecture of the quarter. We spoke briefly about course logistics and preamble information, as well as a brief overview of the integers. Something cool I learned was a new perspective on the Euclidean Algorithm, which will be described below.

1.1 Course Preamble

This course will cover the basic foundations of Ring Theory. There will be 4 ways in which students are assessed – homeworks, quizzes (of which there are 2), midterm, and final exam.

1.2 Integers

To start off the lecture, we approached a few example problems together as a review of integers.

Example 1.1. Solve the following within the set of integers $\mathbb{Z}$

$$x^2 - y^2 = 31$$
$$(x+y)(x-y) = 31$$

First, notice that 31 is a *prime number.* Thus, our factors $x+y$ and $x-y$ must be $\pm 1, \pm 31$. This leads us to 4 combinations of

$$(x,y) = (16,15), (-16,-15), (16,-15), (-16,-15)$$

Yay! Good start. From there, we went into some definition refreshers.

Definition (Divides)**.** If $a, b \in \mathbb{Z}$ and $b \neq 0$, then we say **"b divides a"** and denote $b \mid a$ or $a \vdots b$ if there exists some $c \in \mathbb{Z}$ such that $a = bc$

Definition (Greatest common divisor)**.** Let $a, b \in \mathbb{Z}$ with at least one being non-zero. We say $d \in \mathbb{Z}$ is the **greatest common divisor** of a and b and denote $\gcd(a,b) = d$ if

1. $d \mid a$ and $d \mid b$
2. d is the *largest* integer to satisfy (1)

Definition (Prime number)**.** We say $p \in \mathbb{Z}_{>1}$ is **prime** if its only positive divisors are 1 and p.

Theorem 1.1 (Fundamental Theorem of Arithmetic).
If $n \in \mathbb{Z}$ with $n \neq 0, \pm 1$, then there exists a unique *prime decomposition of n*

$$n = \pm p_1^{a_1} p_2^{a_2} \cdots p_m^{a_m}$$

where $p_1 < p_2 < \cdots < p_m$ are primes, and $a_1, ..., a_m \geq \mathbb{Z}_{>0}$.

Proof of existence (sketch). Assume $n \in \mathbb{Z}_{>1}$. Now if n is prime, we are done. Otherwise, there must exist some $a \in \mathbb{Z}$ with $1 < a < n$ such that $a \mid n$. Which leads to some $n/a \in \mathbb{Z}$ with $1 < n/a < n$.

By strong induction, both a and n/a have prime decompositions, and hence so does $n = a \cdot n/a$. □

Theorem 1.2 (Division with Remainders).
Let $a, b \in \mathbb{Z}, b \neq 0$. Then there exists unique *$q \in \mathbb{Z}$ and $r \in \mathbb{Z}_{>0}$ such that*

1. *$a = bq + r$, and*
2. *$0 \leq r < |b|$*

Such q is called the quotient, and r is the remainder.

This leads us to a very *powerful* corollary!

Corollary 1.2.1 (Euclidean Algorithm).
This gives us a very fast algorithm to find $\gcd(a, b)$

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

Example 1.2. Find the greatest common divisor of 524 and 148.

$$\begin{aligned}
&\gcd(524, 148) && \\
&= \gcd(148, 80) && [524 = 148 \cdot 3 + 80] \\
&= \gcd(80, 68) && [148 = 80 \cdot 1 + 68] \\
&= \gcd(68, 12) && [80 = 68 \cdot 1 + 12] \\
&\quad\vdots && \\
&= \gcd(4, 0) = 4 &&
\end{aligned}$$

Remark. Instead of dividing with remainder, we can also simply **subtract**.

Let's do an example with this remark in mind!

Example 1.3. Simplify $\frac{2n+13}{n+7}$.

$$\gcd(2n + 13, n + 7) = \gcd(n + 7, n + 6) = \gcd(n + 6, 1) = 1$$

Since both polynomials share a greatest common divisor of 1, the fraction must already be in its simplest form.

We then went over a stronger version of the previous remark.

Corollary 1.2.2.

For $a, b \in \mathbb{Z}$ *and* $b \neq 0$*, if* $a = sb + t$ *for* $s, t \in \mathbb{Z}$*, then* $\gcd(a, b) = \gcd(b, t)$

Proof. We seek to show that the set of all common divisors of a and b is equal to that of b and t. Consequently, the largest elements in both sets are the same.

Let d be some divisor of a and b. Indeed, if $d \mid a$ and $d \mid b$, then $a = dk$ and $b = dl$ for some $k, l \in \mathbb{Z}$. Then

$$t = a - bs = dk - dls = d(k - ls),$$

and so $d \mid t$, that is $d \mid b$ and $d \mid t$.

Conversely, if $d \mid b$ and $d \mid t$, then $d \mid (bs + t)$ so $d \mid a$. Thus, $d \mid a$ and $d \mid b$. □

2 Lecture 02: Sept. 26th

Today in lecture we finished our review of integers, and moved onto more number theoretic concepts like modular arithmetics. I learned that I actually don't remember as much as I'd like about modular arithmetics! Congruence classes is also something that's new to me, but I think I have a good grasp on the concept.

2.1 Integers (cont'd)

We started off with some recollection of important theorems, such as the *fundamental theorem of arithmetics*, *division with remainders* as well as its important corollary, the *Euclidean Algorithm.*

Next up, we have another important theorem.

Theorem 2.1 (GCD Representation).
If $\gcd(a, b) = d$*, then there must exist some* $x, y \in \mathbb{Z}$ *such that* $d = ax + by$*.*

To start off with some intuition, we did an example

Example 2.1. Find $\gcd(7, 9)$.

$$\gcd(7, 9) = \gcd(7, 2) = 7(1) + 2(-3) = 7(1) + (9 - 7)(-3) = 7(4) + 9(-3)$$

Now for the proof of the theorem.

Proof. The idea of the proof is to use the corollary (Euclidean algorithm) and (strong) induction on the minimum of $|a|$ and $|b|$. wlog we'll assume $|a| \geq |b|$.

Base case: for all $a \neq 0$, then $\gcd(a, 0) = |a| = \begin{cases} a \cdot 1 + 0 \cdot 0 & \text{if } a > 0 \\ a \cdot (-1) + 0 \cdot 0 & \text{if } a < 0 \end{cases}$

Induction step: If $|a| \geq |b| > 0$ and $a = bq + r$ with $0 \leq r < |b|$, then by the Euclidean Algo, we have

$$\gcd(a, b) = \gcd(b, r).$$

By the induction hypothesis now, there must exist some $x, y \in \mathbb{Z}$ such that $\gcd(b, r) = bx + ry$. Then

$$\gcd(a, b) = \gcd(b, r) = bx + ry = bx + (a - bq)y = ay + b(x - qy)$$

This completes the proof since $y \in \mathbb{Z}$ and $x - qy \in \mathbb{Z}$. □

We then followed up with a very important property of prime numbers.

Theorem 2.2 (Euclid's lemma).
If p is prime, *$a, b \in \mathbb{Z}$, and $p \mid ab$, then $p \mid a$ or $p \mid b$*

By induction on this property, we get the following corollary.

Corollary 2.2.1.
If p is prime, $a_1, ..., a_n \in \mathbb{Z}$ and $p \mid a_1 a_2 \cdots a_n$, then p divides one of $a_1, ..., a_n$

Proof (sketch). Since p is prime, its only divisors are either 1 or itself. Hence, for any $a \in \mathbb{Z}$, we must have that $\gcd(a, p) = 1$ or $\gcd(a, p) = p$. Two cases:

1) If $\gcd(a, p) = p$, then it must mean $p \mid a$, as desired.

2) If $\gcd(a, p) = 1$, it gets a little tricky. Recall from **Theorem 2.1** that since $\gcd(a, p) = 1$, we must have $1 = ax + py$. Multiplying both sides by b gives us $b = abx + pby$.

From here, from the theorem statement, we're given that $p \mid ab$, and it's also trivial to see that $p \mid p$. $(abx + pby)$ is simply a linear combination of ab and p, meaning we must have that $p \mid abx + pby$.

But wait! Recall that $abx + pby = b$. We've thus proved that $p \mid b$, as desired. □

We then summarized the basic topics that we've reviewed thus far:

- Prime decomposition
- Dividing with remainder
- Euclidean algorithm for finding gcd
- Gcd representation
- if $a, b \in \mathbb{Z}$, p is prime, and $p \mid a \cdot b$, then $p \mid a$ or $p \mid b$

  Similarly, if $a, b, d \in \mathbb{Z}, d \mid a \cdot b$ and $\gcd(a, d) = 1$, then $d \mid b$

2.2 Modular arithmetic

Definition (Modular division)**.** Let $a, b, n \in \mathbb{Z}, n > 0$. We say that a is **congruent** to b modulo n and write $a \equiv b \pmod{n}$ if $n \mid (a - b)$

Theorem 2.3 (Properties of modular arithmetic).
Some properties as outlined below

1. *(reflexivity)* $a \equiv a \pmod{n}$
2. *(symmetry)* $a \equiv b \pmod{n} \implies b \equiv a \pmod{n}$
3. *(transitivity)* $a \equiv b, b \equiv c \implies a \equiv c$

and thus, modular congruence is an equivalence *relation.*

Theorem 2.4.
if $a \equiv b \pmod{n}$ *and* $c \equiv d \pmod{n}$*, then*

$$\begin{cases} a + c \equiv b + d \pmod{n} \\ ac \equiv bd \pmod{n} \qquad\qquad (*) \end{cases}$$

Example 2.2. If $k \equiv 1 \pmod{4}$, what is $6k + 5$ congruent to modulo 4? Well, using theorem 2.4, we see that $6k \equiv 6 \pmod{4}$, and so $6k + 5 \equiv 11 \equiv 3 \pmod{4}$.

Proof. Using the definition of modular division, our goal is to show that (1) $n \mid (a+c)-(b+d)$ and (2) $n \mid ac - bd$.

First, using the given, we see that $n \mid a - b$ and $n \mid c - d$. Since n divides both, it must also divide the sum. In other words, $n \mid (a - b) + (c - d)$.

Now, notice that

$$(a + c) - (b + d) = (a - b) + (c - d)$$

We've thus proven (1), as desired. Similarly,

$$ac - bd = (ac - bc) + (bc - bd) = (a - b)c + b(c - d)$$

Again, since n divides both $a - b$ and $c - d$, it also divides its linear combination. Thus, we've shown (2) as desired. □

Definition (Congruence class)**.** For $a \in \mathbb{Z}, n \in \mathbb{Z}_{>0}$, the **congruence class** of a modulo n is the set

$$[a] := \{b \in \mathbb{Z} : a \equiv b \pmod{n}\}$$

Example 2.3. Find the following congruence class

$$\begin{aligned} &[3] \bmod 5 \\ &= \{..., -7, -2, 3, 8, 13, 18, ...\} \\ &= \{3 + 5k : k \in \mathbb{Z}\} \end{aligned}$$

Remark. In general, $[a] \bmod n = \{a + nk : k \in \mathbb{Z}\}$. Note that $a \in [a]$, and also that $[a]$ is an infinite set

Example 2.4. Give all distinct congruent classes mod 5

$$\begin{aligned}
[0] &= \{..., -5, 0, 5, 10, ...\} = [-5] = [15] = ...\\
[1] &= \{..., -4, 1, 6, 11, ...\} = [-4] = [26] = ...\\
[2] &= \{..., -3, 2, 7, 12, ...\} = [-3] = [37] = ...\\
[3] &= \{..., -2, 3, 8, 13, ...\} = [-2] = [48] = ...\\
[4] &= \{..., -1, 4, 9, 14, ...\} = [-1] = [59] = ...
\end{aligned}$$

Notice how these are the only 5 distinct congruent classes mod 5, and that they're disjoint! Let's formalize this thought.

From the definition of $[a]$ mod n and since mod n is an equivalence relation, we have now

Proposition 2.5. *1.* $[a] = [b] \iff a \equiv b \pmod{n}$

2. If $[a]$ *and* $[b]$ *are two congruence classes mod* n*, then either*

- *The sets* $[a]$ *and* $[b]$ *are equal (iff* $a \equiv b$*) or*
- *The sets* $[a]$ *and* $[b]$ *are disjoint (iff* $a \not\equiv b$*)*

3. There are exactly n *distinct congruence classes mod* n*:* $[0], [1], ..., [n-1]$

- *We can think of* $0, 1, ..., n-1$ *as "canonical representatives" of their respective congruence classes. But again, any representative of* $[a]$ *uniquely represents* $[a]$*.*

3 Lecture 03: Sept. 29th

Today was the first time I felt like lecture *really* picked up its pace and "difficulty". I didn't feel the most comfortable with specific notation, especially regarding congruence classes. Something new I learned was the derivation of fermat's little theorem ($a^p = a \pmod{p}$) for prime p. I've used this fact before in putnam problems but never understood the proof behind it.

3.1 Modular arithmetic (cont'd)

We started off with a recollection of *congruence classes*. The professor also informed us that we will be discussing *rings* by the end of this week.

Note: congruence classes will now also be denoted using the bar notation... just cause. So $[a] = \{a + kn : k \in \mathbb{Z}\} = \bar{a}$.

Definition (Congruent classes of $\mathbb{Z}$)**.** The set of all congruence classes of $\mathbb{Z}$ mod n is denoted by $\mathbb{Z}_n$ or $\mathbb{Z}/n\mathbb{Z}$.

Remark. Though $\mathbb{Z}_n$ is a set of sets, we can think of each set through its representative, since sets are always disjoint. In practice, simply identify integers whose difference is a multiple of n.

We then did a recollection of **Theorem 2.4**. Using that theorem, we also allow ourselves to define addition and multiplication on $\mathbb{Z}_n$ by

$$\bar{a} + \bar{b} := \overline{a+b} \quad \text{and} \quad \bar{a} \cdot \bar{b} := \overline{ab}$$

Furthermore, addition and multiplication are also well-defined. For example, if we choose different representatives a' of $\bar{a}$ and b' of $\bar{b}$, so that $a \equiv a' \pmod{n}$ and $b \equiv b' \pmod{n}$, then

$$a' + b' \equiv a + b \quad \text{and} \quad a'b' \equiv ab$$

Thus, they all represent the same class, and hence, $\overline{a+b} = \overline{a'+b'}$ and $\overline{ab} = \overline{a'b'}$.

Example 3.1. What is $[8^{2025}]$ in $\mathbb{Z}_9$?

To start, notice that we're working with congruent classes mod 9, as denoted by $\mathbb{Z}_9$. From here, let's take a deeper dive of the congruence class represented by 8. Notice that $8 \equiv -1 \pmod{9}$, so we have

$$[8^{2025}] = [-1^{2025}] = [-1].$$

Example 3.2. Show that $5 \mid (n^5 + 4n)$.

To do this, we need to show that in $\mathbb{Z}_5, [n^5+4n]=[0]$. First, notice that $n^5+4n \equiv n^5 - n \pmod 5$, meaning $[n^5+4n]=[n^5-n]$ in $\mathbb{Z}_5$.

From here, recall that $n^5 - n = n(n^2+1)(n+1)(n-1)$. Since we are working within $\mathbb{Z}_5$, we need to now show that for $n = 0, 1, 2, 3, 4$ (or equivalently any 5 consecutive integers), that $n^5 - n \equiv 0 \pmod 5$.

First, since n and $(n-1)$ are factors, its trivial that $n = 0, 1$ works. Further, for $n = 2, 3$, we have that (n^2+1) is divisible by 5. Lastly, whenever $n = 4$, we have that $(n+1)$ is also divisible by 5. We are done!

From there, we covered some basic properties of $\mathbb{Z}_n$.

- It is finite – has n elements
- for all $\bar{a}, \bar{b} \in \mathbb{Z}_n$, $\bar{a}+\bar{b} \in \mathbb{Z}_n$ and $\bar{a}\cdot\bar{b} \in \mathbb{Z}_n$, and addition and multiplication satisfy the following properties:
  1. $\bar{0} \in \mathbb{Z}_n$ and $\bar{a}+\bar{0}=\bar{a} \quad \forall \bar{a} \in \mathbb{Z}_n$
  2. $\bar{a}+\bar{b}=\bar{b}+\bar{a} \quad \forall \bar{a}, \bar{b} \in \mathbb{Z}_n$
  3. $(\bar{a}+\bar{b})+\bar{c}=\bar{a}+(\bar{b}+\bar{c}) \quad \forall \bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_n$
  4. $\forall \bar{a} \in \mathbb{Z}_n, \exists$ its additive inverse $\overline{-a}$ such that $\bar{a}+\overline{-a}=\bar{0}$
  5. $(\bar{a}\cdot\bar{b})\cdot\bar{c}=\bar{a}\cdot(\bar{b}\cdot\bar{c}) \quad \forall \bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_n$.
  6. $\bar{a}\cdot\bar{b}=\bar{b}\cdot\bar{a} \quad \forall \bar{a}, \bar{b} \in \mathbb{Z}_n$
  7. $\bar{1} \in \mathbb{Z}_n$ and $\bar{a}\cdot\bar{1}=\bar{a} \quad \forall \bar{a} \in \mathbb{Z}_n$
  8. $\bar{a}\cdot(\bar{b}+\bar{c})=\bar{a}\cdot\bar{b}+\bar{a}\cdot\bar{c} \quad \forall \bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_n$.

That's it I'VE HAD ENOUGH! From now on, bars are omitted cus I'm lazy.

Since $\mathbb{Z}_n$ is finite, we can write addition and multiplication tables.

Example 3.3. Write down addition and multiplication tables for $\mathbb{Z}_5$.

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Based on this example, does $x^2 = 2$ have a solution in $\mathbb{Z}_5$? No, because take a look at the diagonal entries!

Example 3.4. Now, write down addition and multiplication tables for $\mathbb{Z}_6$.

$+$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\cdot$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

3.2 The structure of $\mathbb{Z}_p$

Now, let's talk about the structure of $\mathbb{Z}_p$.

Theorem 3.1 (Freshmen's dream theorem).
Let p be a prime. Then for all $x, y \in \mathbb{Z}$, $(x+y)^p \equiv x^p + y^p \pmod{p}$.

Hence, in $\mathbb{Z}_p$, $(x+y)^p = x^p + y^p \quad \forall x, y$.

Example 3.5. In $\mathbb{Z}_p$, $2^p = (1+1)^p = 1^p + 1^p = 2$.

Proof. Since p is prime, by one of the HW problems (#25 on pg24),

$$\forall 1 \le k < p, p \mid \binom{p}{k}$$

Hence, by the *binomial theorem*, we have

$$\begin{aligned}(x+y)^p = x^p + y^p + \sum_{k=1}^{p-1} \binom{p}{k} x^{p-k} y^k &= x^p + y^p + (\text{some multiple of } p)\\ &\equiv x^p + y^p \pmod{p}\end{aligned}$$

□

Now, take a look back at the multiplication table for $\mathbb{Z}_5$, doesn't it look nice? Aside from the trivial 0 row, there exists a '1' on every row of that table. There's a reason for that as well.

Theorem 3.2.
Let p be a prime. Then

1. *$\forall a \neq 0$ in $\mathbb{Z}_p$, $\exists x \in \mathbb{Z}_p$ such that $ax = 1$*
2. *$ab \equiv 0 \pmod{p} \iff a \equiv 0 \pmod{p}$ or $b \equiv 0 \pmod{p}$*

   That is, $ab = 0$ in $\mathbb{Z}_p$ if and only if $a = 0$ or $b = 0$ in $\mathbb{Z}_p$.

Proof (sketch). For (1), since we're given p is prime and $a \neq 0$ in $\mathbb{Z}_p$, we then know that $\gcd(a, p) = 1$. From there, using the **GCD representation theorem**, we have $1 = ax+py$ for some $x, y \in \mathbb{Z}$. Finally since $p \mid py$, we then must have $ax \equiv 1 \pmod{p}$.

Now, for (2), since $ab \equiv 0 \pmod{p}$, we know that $p \mid ab$. Utilizing **Euclid's lemma**, we know that $p \mid a$ or $p \mid b$. This leads us to the conclusion that $a \equiv 0 \pmod{p}$ or $b \equiv 0 \pmod{p}$. □

This effectively means that $1/a$ exists for all $a \in \mathbb{Z}_p$ – in other words, all elements of $\mathbb{Z}_p$ are **invertible**.

Example 3.6. Compute the following elements of $\mathbb{Z}_p$.

In $\mathbb{Z}_5$, we have $\frac{1}{2} = 3$, since $2 \cdot 3 = 6 \equiv 1 \pmod{5}$.

In $\mathbb{Z}_{17}$, we have $\frac{1}{8} = 15$, since $8 \cdot 15 = 120 \equiv 1 \pmod{1}7$.

In $\mathbb{Z}_p$, we have $\frac{1}{n-1} = \frac{1}{-1} = -1 = p-1$, since $(n-1) \cdot (p-1) \equiv 1 \pmod{p}$

Does this fact still hold for classes mod n where n isn't prime? Stay tuned.

We ended with a summarization of today's lecture.

- $|\mathbb{Z}_n| = n$
- Addition and multiplication are naturally well-defined within $\mathbb{Z}_n$. In fact, $\mathbb{Z}_n$ with these operations is known as a **commmutative ring with 1**
- For any prime p, $(x+y)^p = x^p + y^p$ in $\mathbb{Z}_p$. Consequently,

$$a^p = a \quad \forall a \in \mathbb{Z}_p$$

- When p is prime, all non-zero elements of $\mathbb{Z}_p$ are invertible. We will later say that $\mathbb{Z}_p$ is a **field**
- If n is not prime, then NOT all non-zero elements of $\mathbb{Z}_n$ will be invertible. More on this next time.

4 Lecture 04: Oct. 1st

Today we wrapped up the structures of modular congruence classes and moved onto rings. This is by far the most content packed lecture, and concepts such as units and zero divisors are something brand new to me and took me some time to wrap my head around. Because of this, I introduced **intuition** blocks to help myself break down difficult formal definitions into layman's terms.

4.1 The structure of $\mathbb{Z}_p$ (cont'd)

We started with some recollection of important theorems from the previous lecture. Specifically, if p is prime, then $ab = 0$ in $\mathbb{Z}_p$ if and only if $a = 0$ or $b = 0$ in $\mathbb{Z}_p$.

Additionally, we recalled that this was not the case when $\mathbb{Z}_n$ for some non-prime n. We then started with a generalization of this theorem.

Theorem 4.1.
$ax = 1$ has a solution in $\mathbb{Z}_n$ if and only if $\gcd(a, n) = 1$

> **Intuition.** *a has an inverse modulo n if and and only if it's relatively prime with n.*

Remark. If $\gcd(a, n) = 1$ then $\gcd(a + kn, n) = 1$ for any $k \in \mathbb{Z}$, and so the assumption $\gcd(a, n) = 1$ is independent of our choice of representative of $[a] \in \mathbb{Z}_n$.

Proof. ($\Leftarrow$) Since $\gcd(a, n) = 1$, we can apply the GCD Representation theorem and say that $ax + ny = 1$ for some $x, y \in \mathbb{Z}$.

From here, note that ny doesn't change our congruence class within $\mathbb{Z}_n$, so we arrive at $ax \equiv 1 \pmod{n}$, as desired.

($\Rightarrow$) Assume $\exists x \in \mathbb{Z}$ with $ax \equiv 1 \pmod{n}$. Let $\gcd(a, n) = d$, meaning $a = ds$ and $n = dt$ for some $s, t \in \mathbb{Z}$.

Since $ax \equiv 1 \pmod{n}$, we know that $ax - 1 = kn$ for some $k \in \mathbb{Z}$. This means $1 = ax - kn = dsx - kdt = d(sx - kt)$. Notice now that $d \mid 1$, meaning $d = 1$, as desired. □

We then started with some terminology of units and zero divisors.

Definition (Unit in $\mathbb{Z}_n$)**.** We say that $a \in \mathbb{Z}_n$ is a **unit** if $ax = 1$ has a solution in $\mathbb{Z}_n$. We call such $x \in \mathbb{Z}_n$ the **inverse** of a.

> **Intuition.** *a is a unit if it's invertible in $\mathbb{Z}_n$, and so by the theorem we just proved, a is a unit iff it's coprime with n.*

Definition (Zero divisor in $\mathbb{Z}_n$)**.** We say that $a \in \mathbb{Z}_n$, $a \neq 0$ is a **zero divisor** if $ax = 0$ has a nonzero solution in $\mathbb{Z}_n$.

> **Intuition.** *Basically, a zero divisor is a non-zero integer that, when multiplied with some other non-zero integer, produces n – which is 0 in mod n.*

Example 4.1. Find all units and zero divisors of $\mathbb{Z}_6$ and $\mathbb{Z}_{15}$.

In $\mathbb{Z}_6$, we have the unit 5, and zero divisors $1, 2, 3, 4$.
In $\mathbb{Z}_{15}$, we have the units $2, 4, 6, 7, 8, 11, 13, 14$, and zero divisors $1, 3, 5, 9, 10, 12$.

Notice that every non-zero elements in $\mathbb{Z}_n$ will be either a *unit* or a *zero divisor.* And this makes sense because a has to be either coprime or not with n. If a is coprime, then a is a unit. But if a is not coprime, then there must exist some other number x so that $ax = n = 0$.

The theorems and definiton we've just proved shows that integers $1 \le a < n$ where $\gcd(a, n) = 1$ are special, and we probably need a good way to find them.

Because of this, we introduced the Euler phi.

Definition (The Euler phi function)**.** For $n \in \mathbb{Z}_{>0}$, define

$$\varphi(n) := |\{a : 1 \le a \le n, \gcd(a, n) = 1\}|$$

> **Intuition.** *φ represents the numbers up to n which are relatively prime with n.*

Example 4.2. If p is prime, then what is $\varphi(p)$? How about $\varphi(p^2)$?

Well, only numbers that divide p are itself and 1, and thus the numbers up to p which are coprime with p has to be simply all numbers but itself – $\varphi(p) = p - 1$.

As for p^2, a similar idea still holds. Every number up to p^2 are coprime with p^2, with the exception of the ones that are multiples of p. This gives us $\varphi(p^2) = p^2 - p$.

There are now a couple very interesting theorems about $\varphi(n)$.

Theorem 4.2.
If $\gcd(a, n) = 1$, then $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Let's prove the following special case known as **Fermat's little theorem**.

Theorem 4.3 (Fermat's little theorem).
If p is prime and $a \not\equiv 0 \pmod{p}$, then $a^{p-1} \equiv 1 \pmod{p}$.

Proof. (Fermat's little theorem)
Recall from last time that in $\mathbb{Z}_p$, we have $(x + y)^p = x^p + y^p$.

Thus, $a^p = (a-1)^p + 1^p = (a-1)^p + 1$, and by induction, we get $a^p = a$.

Then $0 = a^p - a = a(a^{p-1} - 1)$.

Since p is prime and $a \neq 0$ in $\mathbb{Z}_p$, it means that we must have $a^{p-1} - 1 = 0$ in $\mathbb{Z}_p$. □

Consequently, we now have a super short proof of the fact that $5 \mid (n^5 + 4n)$ that we spent 15 years trying to show last time (see **Example 3.2**).

Proof. Since $5 \mid (n^5 + 4n)$, we want to show $n^5 + 4n \equiv 0 \pmod 5$. We have now by FLT that $n^5 \equiv n \pmod 5$, so $n + 4n \equiv 5n \equiv 0 \pmod 5$. This concludes our proof. □

Now let's look at it from another perspective.

Proof. (Fermat's little theorem)
Consider the following list: $a, 2a, 3a, ..., (p-1)a$.

Can one of the numbers in the list be divisible by p?
No! Let $1 \leq k \leq p-1$, we know k is not divisible by p. Also a is given to be not divisible by p since they're relatively prime.

Can two of the numbers in the list be congruent mod p?
No! Say $la \equiv ka \pmod p$, then $p \mid a(l-k)$, which is not possible since, again, p and a are relatively prime.

The list is distinct, and actually shows ALL nonzero elements of $\mathbb{Z}_p$, since $\mathbb{Z}_p$ has only $p-1$ nonzero elements, namely $[1], [2], ..., [p-1]$.

Hence $\{[a], [2a], ..., [(p-1)a]\}$ is just a permutation of $\{[1], [2], ..., [p-1]\}$

Therefore,

$$\begin{aligned} a \cdot 2a \cdot ... \cdot (p-1)a &\equiv 1 \cdot 2 \cdot ... \cdot (p-1) && \pmod p \\ (p-1)! \cdot (a^{p-1}) &\equiv (p-1)! && \pmod p \end{aligned}$$

Since $(p-1)!$ is not divisible by p, it then must be invertible in modulo p, and thus we can cancel it out from both sides.

This means that $a^{p-1} \equiv 1 \pmod p$. It should now be trivial to see that $a^{p-1} - 1$ is divisible by p. □

We then discussed a quick summary to wrap up our discussion on $\mathbb{Z}_n$ and $\mathbb{Z}_p$:

- Units and zero divisors in $\mathbb{Z}_n$
- A criterion for being a unit in $\mathbb{Z}_n$
- The Euler phi function
- Fermat's little theorem and its proof(s)

4.2 Rings

We started with perhaps the most important definition from this course.

Definition (Ring)**.** A set R with two operations on R

$$+ : R \times R \to R, (a, b) \to a + b$$
$$\times : R \times R \to R, (a, b) \to a \cdot b$$

is called a **ring** if these operations satisfy the following axioms:

1. Axioms of $+$:
   (a) associativity: $a + (b + c) = (a + b) + c \quad \forall a, b, c \in R$
   (b) commutativity: $a + b = b + a \quad \forall a, b \in R$
   (c) zero: $\exists$ an element of R, called zero, s.t. $a + 0 = 0 + a = a \quad \forall a \in R$
   (d) additive inverse: $\forall a \in R, \exists x \in R$ s.t. $a + x = 0$ (Notation: $x = -a$)
2. Axioms of $\times$
   (a) associativity: $(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \forall a, b, c \in R$
3. Distributivity: $(a + b)c = ac + bc$ and $a(b + c) = ab + ac \quad \forall a, b, c \in R$

Notice the axioms of multiplication are very simple – only associativity is needed! That's because sometimes, we need additional classifications for these additional properties.

Definition (Commutative ring)**.** A ring R that satisfies multiplicative commutativity $ab = ba \quad \forall a, b \in R$ is called a **commutative ring**.

Definition (Ring with 1)**.** We say that a ring R has an **identity** if there exists an element $1 = 1_R$ in R such that $a \cdot 1 = 1 \cdot a \quad \forall a \in R$.

Note: for rings with identity, we assume that $1 \neq 0$.

Definition (Field)**.** Let R be a commutative ring with identity. We say that R is a **field** if $\forall a \in R, a \neq 0, \exists x \in R$ such that $ax = 1$

We write $x = a^{-1}$ and call x a *multiplicative inverse* of a.

Intuition. *A commutative ring with 1 is a field iff its elements are invertible.*

5 Lecture 05: Oct. 3rd

Today in lecture we went over many examples of rings, even rings of objects that we would not expect. Something new I learned was that rings can arise out of unexpected objects, so long as binary operations are well-defined, making the concept of *rings* very flexible.

5.1 Examples of rings

We started with a recollection of the definition of a ring, what makes it commutative, what identity is defined as, and what a field is. Picking up from there, we did an example.

Example 5.1. For each of the following sets, identify if its a ring? If so, does it have an identity? Is it a commutative ring? Is it a field?

1) $\mathbb{Z}$ – this is a ring, with an identity 1, and is commutative. However, not all integers have an inverse and therefore it is not a field.

2) $\mathbb{Z}_n$, where n is not prime – this is also a ring, with identity 1, and is commutative. Still though, it is not a field, because there still does not exist an multiplicative inverse for *every* element.

3) $\mathbb{Z}_p$, where p is a prime – this is now a field, as it satisfies all properties, and always have a multiplicative inverse.

4) $\mathbb{C}$ – this is a field, as there exists multiplicative inverses for complex numbers as well.

5) $2\mathbb{Z}$ (even integers) – this is a ring since it's closed under addition and multiplication, and is commutative. However, it does not contain an identity.

6) Odd integers – this is NOT a ring, as addition is not well-defined and is not closed.

We then moved onto examples over more complex objects like **matrices**.

Let's start with 2×2 matrices over $\mathbb{R}$.

$$M_2(\mathbb{R}) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{R}\}$$

Let's check it is a ring.

$$\textbf{Addition:} \;\; \begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} a + a' & b + b' \\ c + c' & d + d' \end{pmatrix} \in M_2(\mathbb{R})$$

Notice that addition is both commutative and associative, as the entries of the matrix is defined over all real numbers, and thus carries their properties.

The corresponding *zero* element is a matrix of all zeroes, and the additive inverse would simply be a matrix with all negative numbers.

Now, for multiplication.

$$\textbf{Multiplication:}\quad \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} + \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11}b_{11} + a_{12}b_{21} & ... \\ ... & ... \end{pmatrix} \in M_2(\mathbb{R})$$

It is associative, as defined by matrix multiplication. There exists a multiplicative identity, being I_2. It satisfies distributivity as well.

Thus, $M_2(\mathbb{R})$ is a ring. Now, is it commutative? *No.* For some intuition, recall that matrices encode some transformation in some vector space, and sometimes these transformations cannot be done out of order.

Is it invertible? Again, *not always.* Recall from linear algebra that

Theorem 5.1 (Invertible matrices).
A matrix $A \in M_2(\mathbb{R})$ is invertible if and only if $\det A \neq 0$.

To generalize our findings about the ring properties of a matrix, we say that if *R is any ring (with 1)*, then

$$M_2(R) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in R\}$$

is a **ring (with 1)**.

We now investigate **functions**. $F(\mathbb{R}) := \{f : \mathbb{R} \to \mathbb{R}\}$ the set of all functions from $\mathbb{R}$ to $\mathbb{R}$.

We define $+$ and $\times$ by

$$(f + g)(x) = f(x) + g(x) \quad \text{and} \quad (fg)(x) = f(x)g(x)$$

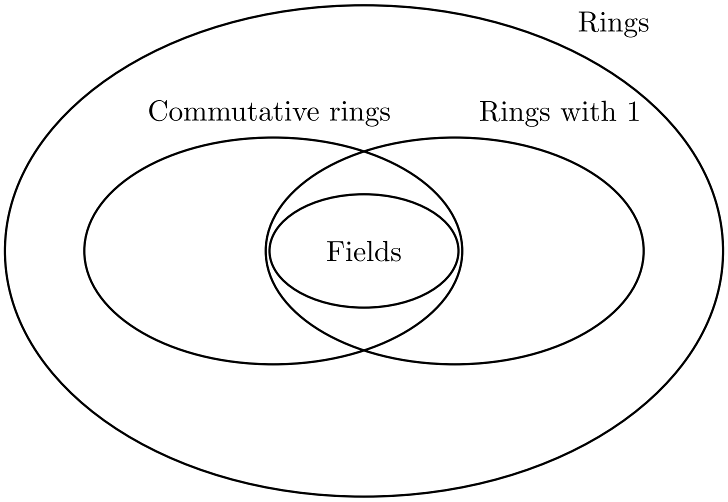
We check now that $F(\mathbb{R})$ **is a commutative ring with identity**.

What is 0 is this ring? The constant 0 function.
What is 1 in this ring? The constant 1 function.
What is the additive inverse of f? It is $g(x) := -(f(x))$
Is $F(\mathbb{R})$ a field? No: for instance, consider f given by $f(x) = x \quad \forall x$. Then $f \neq 0$, but f has no inverse since $1/x$ does not exist at $x = 0$.

We ended off with a brief note regarding the difference between *rings* and *rings with identity.*

Specifically, **for readers**, most textbooks reserve the name RING for what our book calls "ring with identity". In other words, having a multiplicative identity is, majority of the times, baked into the definition of a ring.

Not us tho we're quirky :D


Rings
Commutative rings
Rings with 1
Fields

6 Lecture 06: Oct. 6th

Today in lecture we covered a very important concept: **integral domains**. With that, this covers (almost) completely our venn diagram regarding rings. I still need a lot of practice with these objects to get completely familiar, but we followed up with many examples that I need to take some time to digest.

6.1 Rings, subrings, and products

We started, once again, with a recollection of rings, with or without identity, are or aren't commutative, and fields!

Definition (Integral domain)**.** A commutative ring R with 1 is called an **integral domain** if $\forall a, b \in R, a \cdot b = 0 \iff a = 0$ or $b = 0$.

> **Intuition.** *Basically, its a commutative ring with identity that has no zero divisors!*

Example 6.1. Is $\mathbb{Z}_p$ an integral domain? How about $\mathbb{Z}_n$?

$\mathbb{Z}_p$ **IS** an integral domain. This is because we know that if $p \mid ab$, then $p \mid a$ or $p \mid b$, which means

$$[a][b] = 0 \Leftrightarrow [a] = 0 \text{ or } [b] = 0$$

$\mathbb{Z}_n$ for any $n > 1$ **IS NOT** an integral domain. This is because if n is not prime, then it can be factored into two integers, making both of those integers zero divisors.

One example of a commutative ring with 1 that isn't an integral domain is $\mathbb{Z}$.

From there, we started with some motivation of the notion of *subrings.*

Notice that $\mathbb{R}$ and $\mathbb{C}$ are both rings (and fields!), and that $\mathbb{R} \subset \mathbb{C}$. So can we say that $\mathbb{R}$ is a subring (or even a subfield) of $\mathbb{C}$? What about $2\mathbb{Z}$ and $\mathbb{Z}$?

Definition (Subrings)**.** Assume R is a ring and $S \subseteq R$. Then S is a **subring** of R if S with addition and multiplication in R is itself a ring

Is there a quick way to check whether S is a subring of R? Well, yes!

Theorem 6.1 (Identifying subrings).
Assume R is a ring and $S \subseteq R$. Then S is a subring of R if and only if

1. *For all $a, b \in S$, the sum $a + b$ is in S*
2. *For all $a, b \in S$, the product ab is in S*
3. $0_R \in S$

4. *For all $a \in S$, $-a$ is in S.*

Notice that properties like associativity and commutativity of addition is automatically "carried over" from R when constructing S, since S is a subset.

Example 6.2. Let $F(\mathbb{R})$ be the set of *all functions* from $\mathbb{R}$ to $\mathbb{R}$, and let $C(\mathbb{R})$ be the set of *all continuous functions* from $\mathbb{R}$ to $\mathbb{R}$.

Notice that if f and g are both continuous functions, then $(f+g)(x) = f(x) + g(x)$ must be continuous. Similarly, $(fg)(x) = f(x) \cdot g(x)$ must also be continuous. The constant 0 function is continuous, and the additive inverse function exists ($f^{-1}(x) = -f(x)$). Thus, $C(\mathbb{R})$ must be a subring of $F(\mathbb{R})$.

Note here that $C(\mathbb{R})$ (and thereby $F(\mathbb{R})$) *isn't* an integral domain. Consider

$$f(x) = \begin{cases} 0 & x \geq 0 \\ x & x < 0 \end{cases} \qquad g(x) = \begin{cases} x & x \geq 0 \\ 0 & x < 0 \end{cases}$$

Example 6.3. We then did some more interesting examples.

$\mathbb{Z}[i] := \{a + bi : a, b \in \mathbb{Z}\} \subset \mathbb{C}$. Is $\mathbb{Z}[i]$ a subring of $\mathbb{R}$? Is $\mathbb{Z}[i]$ a subring of $\mathbb{C}$? Well, obviously not of $\mathbb{R}$ – it's not even a subset! But $\mathbb{Z}[i]$ is actually closed under addition and multiplication, and the additive identity and inverse both exist as well, and therefore it's a subring of $\mathbb{C}$!

This set is known as the *Gaussian Integers.* We'll speak more about this later.

What about when $x^2 = 17$? Consider

$$\mathbb{Z}[\sqrt{17}] := \{a + b\sqrt{17} : a, b \in \mathbb{Z}\}$$

Well, still yes! Following a very similar process from the example above, we see that $\mathbb{Z}[\sqrt{17}]$ is a subring of $\mathbb{C}$!

From there, we continued with a discussion on the **product** of rings.

Definition (Products of rings)**.** $R \times S := \{(r, s) : r \in R, s \in S\}$ with addition and multiplication defined by $(r, s) + (r', s') = (r + r', s + s')$ and $(r, s) \cdot (r', s') = (r \cdot r', s \cdot s')$

Think now, is $\mathbb{Z} \times \mathbb{Z}$ an integral domain?

No!! $(0, 1) \cdot (1, 0) = (0, 0)$ which is the zero element, making both pairs zero divisors and thus $\mathbb{Z}$ not an integral domain.

We then went into a brief summary of everything we've covered so far, which included integral domains as well as subrings and products.

6.2 Basic properties of rings

Assume R is a ring. Is the additive identity necessarily *unique*? Can there be a 0 and a $0'$? What about multiplicative identity?

No both both! $0 + 0' = 0$ but also $0 + 0' = 0'$, meaning $0 = 0'$. Same logic for 1 and $1'$.

7 Lecture 07: Oct. 8th

Today we went over another subset of rings called division rings, and discovered that through an example via introducing the quaternions! Ts is like meeting my legend fr cus ive heard of quaternions for a while but never *truly* learned what they mean. The proof we ended lecture on was also really elegant.

7.1 Quaternions

Today, we began with a discussion of another example of rings: the ring of $\mathbb{H}$ of **quaternions**.

This is an example of a **division ring**.

Definition (Non-commutative division ring)**.** A *non-commutative* ring with *identity*, where every non-zero element is *invertible*, so it's almost like a "non-commutative field". Such a structure is known as a **(non-commutative) division ring**.

Remark. Technically, more rigorously, in general, "division rings" refer to rings where all elements are invertible, and doesn't imply non-commutativity.

To start, we considered the 4-dimensional vector space $\mathbb{H}$ with basis $1, i, j, k$. So elements are of the form $a + bi + cj + dk$, where $a, b, c, d \in \mathbb{R}$.

Addition is simple- we add like-terms!

$$\begin{gathered} v = a + bi + cj + dk \\ w = a' + b'i + c'j + d'k \\ (v + w) = (a + a') + (b + b')i + (c + C')j + (d + d')k \end{gathered}$$

Now we need to define multiplication. We define these products as follows:

- 1 is the identity, and $rq = qr$ for any quaternion $q \in \mathbb{H}$ and $r \in \mathbb{R}$.
- For other basis vectors

$$\begin{gathered} i^2 = j^2 = k^2 = -1 \\ ij = k \quad jk = -k \\ jk = i \quad kj = -i \\ ki = j \quad ik = -j \end{gathered}$$

> **Intuition.** *Here, imagine i, j, and k lie on a circle in that order when traversed clockwise. Now, multiplication is simply traversing along that circle from the first element to the second, where CW implies positive and CCW implies negative.*

The product is then extended to all elements of $\mathbb{H}$ by using the distributive law.

Example 7.1. Compute $(a+bi+cj+dk)(a'+b'i+c'j+d'k)$

$$\begin{aligned}(a+bi+cj+dk)(a'+b'i+c'j+d'k) = {} & aa'+ab'i+ac'j+ad'k+ \\ & ba'i+bb'(-1)+bc'k+bd'(-j)+ \\ & ca'j+cb'(-k)+cc'(-1)+cd'i+ \\ & da'k+db'j+dc'(-i)+dd'(-1)\end{aligned}$$

$$\begin{aligned}(a+bi+cj+dk)(a'+b'i+c'j+d'k) = {} & (aa'-bb'-cc'-dd')+(ab'+ba'+cd'-dc')i \\ & +(ac'-bd'+ca'+db')j+(ad'+bc'-cb'+da')k\end{aligned}$$

Here comes the fun- let's now prove that $\mathbb{H}$ is a ring. We need to check that + and × satisfy the desired properties.

Remember that $\mathbb{H}$ is just some vector space $\mathbb{R}^4$, so properties of + simply follow. × and distributivity will be proved in HW3, and the identity is simple as well: $1 = 1+0i+0j+0k$.

How do we check that $\mathbb{H}$ has a multiplicative inverse? Well, recall from $\mathbb{C}$ that $\frac{1}{a+bi} = \frac{1}{a^2+b^2}(a-bi)$, and so by analogy, the inverse

$$v = a+bi+cj+dk \neq 0$$
$$\frac{1}{v} = \frac{1}{a+bi+cj+dk} = \frac{1}{a^2+b^2+c^2+d^2}(a-bi-cj-dk)$$

(a more rigorous proof will be given on the hw)

Note also that $\mathbb{R}$ and $\mathbb{C}$ are commutative *subrings* of $\mathbb{H}$.

Finally, as a summary, the ring $\mathbb{H}$ of quaternions is a non-commutative **division ring** (ring with 1 and each element has an inverse).

7.2 Basic properties of rings (cont'd)

Assume R is a ring. We already saw that the zero element, the identity, and for each element, its additive inverse, are all *unique*! This means that we can now define subtraction.

That is, we define $a - b := a + (-b)$.

Canncellation property: In a ring R, $a+b = a+c$ if and only if $b = c$.

Note that unless R is a division ring, we cannot apply the same logic to multiplication (elements don't have an inverse, and there may not even be a multiplicative identity!)

That doesn't necessarily mean the multiplication cancellation won't hold if R is not a division ring though!! In fact, we now discuss the cancellation property in integral domains.

Proposition 7.1.

If R is an integral domain, then $ab = ac, a \neq 0$ does imply $b = c$.

Proof. Begin by subtracting both sides by ac. We get

$$ab - ac = a(b - c) = 0$$

Since R is an integral domain and $a \neq 0$, we must have by definition of integral domains that $b - c = 0$. □

Here is another useful fact

Proposition 7.2.

Any field F is an integral domain.

Proof. We need to show that for $a, b \in F$, if $ab = 0$ and wlog $a \neq 0$, then $b = 0$. Simply multiply both sides by a^{-1}, we get

$$a^{-1}(ab) = (a^{-1}a)b = b = 0 = 0 \cdot a^{-1}$$

□

In general, not all integral domains can be fields. One example of this is $\mathbb{Z}$.

But is there some property to say that *some* integral domains are fields? Yes. There is.

Theorem 7.3.

If R is a finite *integral domain (i.e., $|R| < \infty$), then R is a field.*

> **Intuition.** *The intuition here is that if R is finite, then it will have modular arithmetic-esque behavior. Meaning if you multiply every pair of elements then it has to like "circle back" at some point and go back to 1, and that's where we find the inverse.*

Proof. We need to show that every element in R has a multiplicative inverse. Since R is finite, let's first list out all of its elements

$$R = \{0, a_1, a_2, ..., a_n\}$$

(here we suppose R has n non-zero elements)

Pick any a_i. We'll show that there exist some a_i^{-1}. We do this by writing out the "row" of the multiplication table of R, aka $\{a_i a_1, a_i a_2, ..., a_i a_n\}$

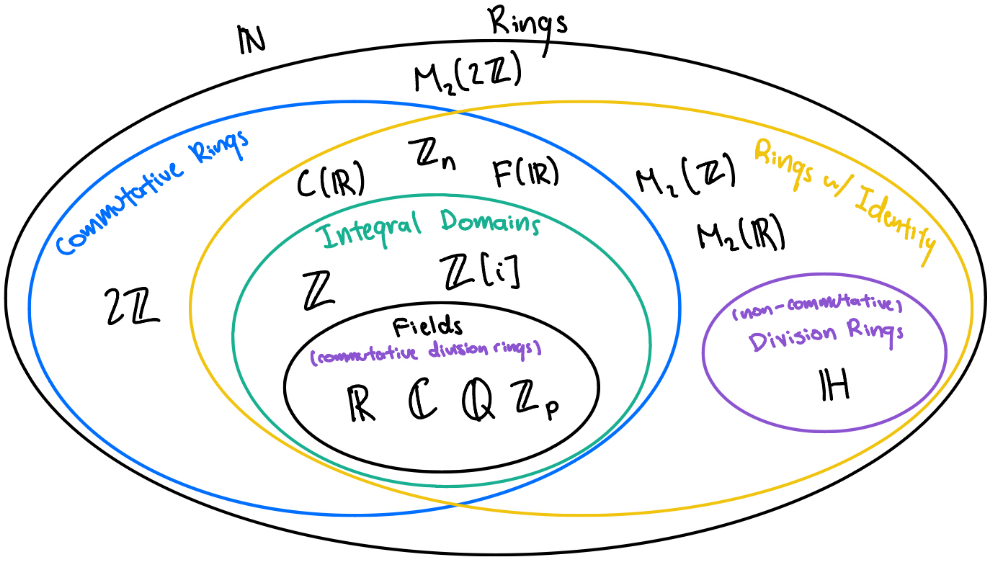
Notice two things about this row: (1) none of these elements can be 0, since R is an integral domain. (2) there cannot be any duplicate elements, since by the cancellation property, we have $a_i a_j = a_i a_k$ implies that $a_j = a_k$ which means $j = k$.

Since no elements of the row are 0, and no elements repeat, we thus know that the row must contain every non-zero element in R. This is huge(!), as it implies that there exists some j where

$$a_i a_j = 1$$

where 1 is the identity, meaning $a_j = a_i^{-1}$. □

We now have a complete picture of the types of rings!



8 Lecture 08: Oct. 10th

Quite honestly, I was not in-person for this lecture. But I learned from reviewing that we finished covering the basic properties of rings by ending on (my worst nightmare) units and zero divisors. We then started talking about "functions" on rings, with a special type called a "homomorphism". Sounds fancy, but isn't all that (i hate the whole inject/surject btw prolly bottom 2 definitions in math)

8.1 Basic properties of rings (cont'd)

Woah, before we get to the cool stuff, we started with a (pretty in-depth) review.

First, recall the cancellation properties discussed last lecture, which includes: $a+b=a+c$ iff $b=c$ for all rings, and $ab=ac, a\neq 0$ implies $b=c$ which only applies to **integral domains** and **division rings**.

We also showed that (1) any *field* is an *integral domain*, and (2) any *finite integral domain* is a *field*.

In any ring R, for any $a\in R$ and $n\in\mathbb{Z}$, we can define na as

- If $n=0$, then $na := 0$
- If $n>0$, then $na := a+a+\cdots+a$ (n summands) and
  $(-n)a := (-a)+\cdots+(-a)$ (n summands)

That might've seen *trivial* just now, but note that n not necessarily be an element of R, it just has to be some integer. And with this now, we can generalize the definition of *units* and *zero divisors* to all rings (beyond just $\mathbb{Z}_n$).

Definition (Unit (general))**.** If R is a *ring with identity*, then $u\in R$ is called a **unit** if $\exists a\in R$ such that $au=1_R=ua$

Note here that since R may not be commutative, it's important to require both au and ua to be equal to 1. Also note that such an a is *unique*, meaning we can denote it by u^{-1}.

> **Intuition.** *Ok ngl this tripped me up a bit when I first learned it, but essentially, a set not need be a division ring in order to have SOME (not all) elements be invertible. And the invertible few (if they exist) are known as units*

Definition (Zero divisor (general))**.** Assume R is a ring. An element $a\neq 0$ of R is a **zero divisor** if there exists a *nonzero* element $c\in R$ such that $ac=0$ or $ca=0$.

Example 8.1. We explored the units and zero divisors of $M_2(\mathbb{R})$.

Any $a = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with $\det A = ad - bc \neq 0$ is a *unit* and

$$A^{-1} = \frac{1}{\det A} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

On the other hand, any $A \neq 0$ with $\det A = ad - bc = 0$ is a *zero divisor* because

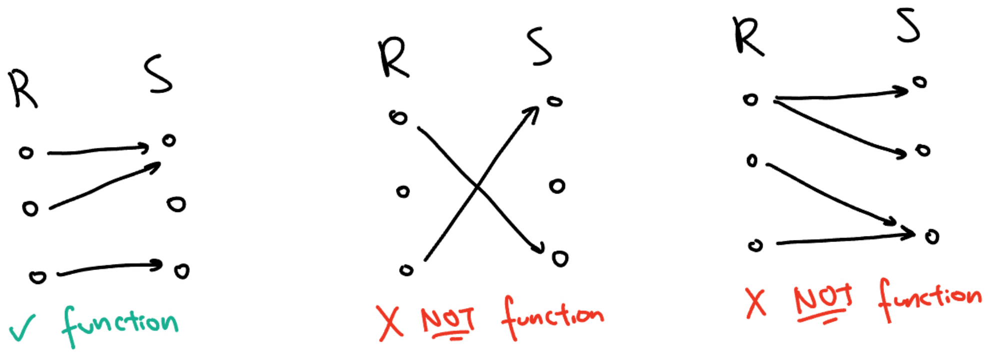
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

So here, every nonzero element in $M_2(\mathbb{R})$ is a unit or a zero divisor.

8.2 Homomorphisms of rings

Now, recall from earlier courses the definition of a function (aka a map)- a rule $f : R \to S$ that assigns to every element a of R a unique element $f(a)$ of S.

Intuition. *Below is a picture for intuition:*



Now, we moved onto a really important definition.

Definition (Ring homomorphism)**.** Assume R and S are rings. A map $f : R \to S$ is a **ring homomorphism** if

$$\forall a, b \in R, f(a+b) = f(a) + f(b) \text{ and } f(a \cdot b) = f(a) \cdot f(b)$$

Further, we have

- A ring homomorphism is a **monomorphism** if f is injective, that is $f(a) = f(b)$ implies $a = b$
- A ring homomorphism is a **epimorphism** if f is surjective, that is for every $s \in S$ there is $a \in R$ such that $f(a) = s$

- A ring homomorphism is a **isomorphism** if f is bijective (both injective and surjective)

Intuition. *Bro ok basically "homomorphism" is just some fancy ahh name for a function (obeying vertical line rule) where addition and multiplication on the domain is the same as it is in the co-domain*

Example 8.2. Consider $f : \mathbb{Z} \to \mathbb{Z}, f(a) = 2a$. Is this a ring homomorphism?

Well, notice $f(a+b) = 2(a+b) = 2a+2b = f(a)+f(b)$. Looks good so far...
BUT WAIT! $f(ab) = 2ab \neq 4ab = 2a \cdot 2b = f(a) \cdot f(b)$.

Thus we conclude that f is NOT a ring homomorphism.

Example 8.3. We then did a whole bunch of examples, but for sake of brevity, I will cover a select few.

$f : \mathbb{R} \to \mathbb{C}, f(a) = a + 0i$. Note here that for all $a, b \in \mathbb{R}$,

$$f(a+b) = (a+b) + 0i = (a+0i) + (b+0i) = f(a) + f(b)$$
$$f(ab) = ab + 0i = (a+0i)(b+0i) = f(a)f(b)$$

and so f is a homomorphism. More specifically, f is a monomorphism since it is injective (one-to-one, since each input has a unique output, but not all outputs are matched)

$h : \mathbb{Z} \to \mathbb{Z}_2, h(a) = a \bmod 2 = [a]_2$. From the results on modular arithmetic, we have

$$h(a+b) = [a+b] = [a] + [b] = h(a) + h(b)$$
$$h(ab) = [ab] = [a] \cdot [b] = h(a)h(b)$$

Thus, h is a homomorphism. More specifically, h is an epimorphism since it is surjective (more possible inputs than outputs). In fact, this is true not just for $\mathbb{Z}_2$ but extends to all of $\mathbb{Z}_n$.

Some facts now about homomorphisms.

Theorem 8.1 (Properties of ring homomorphisms).
If $f : R \to S$ is a homomorphism, then

1. $f(0_R) = 0_S$
2. $f(-a) = -f(a) \quad \forall a \in R$
3. *If f is surjective and R is a ring with identity 1_R, then*
   (a) *$f(1_R)$ is the identity of S (and hence S must be a ring with identity)*
   (b) *if u is a unit in R, then $f(u)$ must be a unit in S; furthermore, $f(u)^{-1} = f(u^{-1})$*

9 Lecture 09: Oct. 13th

Today in lecture we explored more rings and properties of rings, and specifically how to identify isomorphic rings. We ended lecture with a brief summary of the entire course thus far, because there will be a cumulative quiz in the coming lecture. Overall not too challenging of a lecture today.

9.1 Homomorphisms of rings (cont'd)

We started with a review of the properties listed at the end of the previous lecture (**theorem 8.1**). We then proved it, as promised.

Proof. For fact 1), we have that if f is a homomorphism, then

$$f(0_R) = f(0_R + 0_R) = f(0_R) + f(0_R)$$

Subtracting $f(0_R)$ on both sides gives us

$$\begin{aligned} f(0_R) - f(0_R) = f(0_R) + f(0_R) - f(0_R) \\ 0_S = f(0_R) \end{aligned}$$

This concludes fact 1. For fact 3a, we have that if f is an epimorphism, then $\exists a \in R$ with $f(a) = s$

Then $s = f(a) = f(1_R \cdot a) = f(1_R)f(a) = f(1_R) \cdot s$

Similarly, $s = f(a) = f(a \cdot 1_R) = f(a)f(1_R) = s \cdot f(1_R)$

We've proved thus for every $s \in S$, $s \cdot f(1_R) = f(1_R) \cdot s = s$, and thus, $f(1_R)$ must be the identity of S. □

9.2 Isomorphic rings

Definition (Isomorphic rings)**.** We say that the rings R and S are **isomorphic** if there exists an isomorphism $f : R \to S$.

Intuition. *Basically, R and S are like the "same ring", just labeled slightly differently.*

Example 9.1. Is $2\mathbb{Z}$ isomorphic to $\mathbb{Z}$? No! Because if it was, then the homomorphism must be surjective and maps the identity of $\mathbb{Z}$ to the identity of $2\mathbb{Z}$, which doesn't exist!

Is $\mathbb{Z}_4$ isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$? No! Notice that adding any element to itself in $\mathbb{Z}_2 \times \mathbb{Z}_2$ will always result in the zero element $(0, 0)$, but that's not always the case in $\mathbb{Z}_4$.

Is $\mathbb{Z}_6$ isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_3$? Let's think a bit harder about this. We have

$$\begin{aligned} f(0) &= (0,0) \\ f(1) &= (1,1) \\ f(2) &= f(1) + f(1) = (1,1) + (1,1) = (0,2) \\ f(3) &= f(1) + f(2) = (1,1) + (0,2) = (1,0) \\ f(4) &= f(2) + f(2) = (0,2) + (0,2) = (0,1) \\ f(5) &= f(2) + f(3) = (0,2) + (1,0) = (1,2) \end{aligned}$$

Notice $f(a) = (a \bmod 2, a \bmod 3)$. f is both a bijection and a homomorphism, and therefore, f is an ismorphism.

Example 9.2. We then did a cooler example. Consider $S = \{\begin{pmatrix} a & b \\ -b & a \end{pmatrix} : a, b \in \mathbb{R}\}$

First, check that S is a subring of $M_2(\mathbb{R})$, and so S is a ring. But further, notice that

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} + \begin{pmatrix} 0 & b \\ -b & 0 \end{pmatrix} = aI + bJ$$

where $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ and $J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$.

Not that also $J^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -I$. Doesn't this feel... familiar?

Feels like S is isomorphic to $\mathbb{C}$. And actually, it is! If we define $f : S \to \mathbb{C}$ where $f\begin{pmatrix} a & b \\ -b & a \end{pmatrix} = a + bi$.

Proof is left as an execrise to the reader :D

To summarize,

1. To check that R and S are isomorphic, suffices to construct an isomorphism $f : R \to S$.
2. To check that R and S are *not* isomorphic, suffices to find ONE property that isn't shared by both.

We then ended lecture with a summary of *everything* that we've covered in the course thus far (there's a quiz next lecture ahhhhhhhhh)

Chapters 1 and 2 discussed $\mathbb{Z}$, modular arithmetic, and $\mathbb{Z}_n$.

$\mathbb{Z}$: with integers, we talked about *divisors*, *gcd*, and *division with remainder.*

Division with remainder led us to the *Euclidean algorithm* and the *gcd representation theorem*, which in turn allowed us to prove *uniqueness of prime decomposition.*

$\mathbb{Z}_n$: we proved that $\mathbb{Z}_n$ is a ring and that $|\mathbb{Z}_n| = n$.

We also proved that the *units* od $\mathbb{Z}_n$ are all $[a]$ such that $\gcd(a, n) = 1$. Similarly, the *zero divisors* of $\mathbb{Z}_n$ are all $[a]$ such that $\gcd(a, n) \neq 1$.

Finally, we proved that when p is prime, $\mathbb{Z}_p$ is a *field*.

10 Lecture 10: Oct. 15th

Today in lecture we spent around 30 minutes taking a quiz, then we discussed a bit about the next chapter, which is rings of polynomials. I am pretty confident about the quiz overall, but I think I misapplied a few properties here and there. The lecture itself wasn't too challenging as well.

10.1 Polynomial rings

We started the lecture with a quiz!!!!! It wasn't too bad I think. Anyway, let's dive in.

Let F be a field.

Definition (Polynomials)**.** Consider the set of polynomials over F

$$F[x] := \{a_0 + a_1x + a_2x^2 + \cdots + a_nx^n : n \in \mathbb{Z}_{\geq 0}, a_0, a_1, ..., a_n \in F\}$$

We call a_n the *leading coefficient* of $f(x)$, and we call n the *degree* of f. We write $\deg(f) = n$. If $f(x) = 0$, then we define $\deg(f) = -\infty$

Addition is defined by combining like-terms. We define multiplication by defining $x^k \cdot x^m = x^{k+m}$, and $a \cdot x^k = x^k \cdot a = ax^k$, and then using distributivity from there.

Example 10.1. Compute $(1 + x^2)(3 + x + 4x^2)$ in $\mathbb{Z}_7[x]$.

$$\begin{aligned}(1 + x^2)(3 + x + 4x^2) &= 3 + x + 4x^2 + 3x^2 + x^3 + 4x^4 \\ &= 3 + x + 7x^2 + x^3 + 4x^4 \\ &= 3 + x + x^3 + 4x^4\end{aligned}$$

Not too surprisingly, $F[x]$ **is a ring.**

$F[x]$ with addition and multiplication we defined has the following properties:

- $F[x]$ contains 0 (the zero polynomial)
- $F[x]$ has an additive inverse when we negate all $a_0, ..., a_n$
- Addition is commutative and associative and so is multiplication (trust me bro)
- The polynomial 1 is the identity
- Distributivity holds (it came to me in a dream)

This makes $F[x]$ into a **commutative ring with identity**.

Let's challenge our thinking a bit, does F necessarily have to be a field? Let's consider $R[x]$, where R is any ring. Show that

1. If R is commutative, then so is $R[x]$
2. If R has identity, then so does $R[x]$
3. R is a subring of $R[x]$ consisting of constant polynomials

11 Lecture 11: Oct. 17th

Today in lecture we continued our discussion on polynomial rings. Specifically, the way that it's defined, many of its properties are starting to reflect those of $\mathbb{Z}$, which means we can slowly begin to bring back some basic number theory things, but applied to polynomials. This was a super content-packed lecture, but I think I understood the main message.

11.1 Polynomial rings (cont'd)

We began with a recollection of the definition and some basic properties of polynomial rings as discussed in the previous lecture. We then started with a motivating example for the next property.

Example 11.1. What is $2x \cdot 3x$ in $\mathbb{Z}_6$? Is $\mathbb{Z}_6[x]$ an integral domain?

Well, $2x \cdot 3x = 6x$ but since $6 = 0$ in $\mathbb{Z}_6$, we then have that $2x \cdot 3x = 0$, meaning $\mathbb{Z}_6[x]$ isn't an integral domain. But wait, $\mathbb{Z}_6$ also isn't an integral domain... is there a way we can relate this?

Theorem 11.1.
If R is an integral domain, then so is $R[x]$.

Proof. Since R is an integral domain, it must be a commutative ring with identity. Hence, so is $R[x]$.

All that remains to be shown is that for some $f, g \in R[x]$ with $f, g \neq 0$, we must have $f \cdot g \neq 0$.

Let $f = a_0 + a_1x + \cdots + a_nx^n$ and $g = b_0 + b_1x + \cdots + b_mx^m$ be arbitrary, where $n = \deg f$ and $m = \deg g$.

If $f, g \neq 0$, we know that $n, m \geq 0$ and $a_n, b_m \neq 0$. Now when we multiply the two, we get

$$f \cdot g = (\text{terms of lower degree}) + a_nb_mx^{n+m}$$

Since $a_n, b_m \neq 0$ and since R is an integral domain, $a_nb_m \neq 0$. Thus, $\deg(f \cdot g) = n+m \geq 0$, and so $f \cdot g \neq 0$. □

This leads us to some powerful corollaries.

Corollary 11.1.1.
All of the following are implied by the theorem.

1. *If R is an integral domain, then $\forall f, g \in R[x]$, we have* $\deg(fg) = \deg(f) + \deg(g)$
2. *If F is a field, then $F[x]$ is an integral domain*
3. *If R is an integral domain, then $f(x)$ is a unit of $R[x]$ iff $f(x) = c$, where $c \in R$ is a unit of R.*

Proof. (⇒) Let $f \in R[x]$ be arbitrary, where f is a unit. Then $\exists g \in R[x]$ where $fg = 1$.

Hence, $\deg(fg) = \deg(f) + \deg(g)$, but also $\deg(fg) = \deg(1) = 0$. So we conclude $\deg(f) + \deg(g) = 0$ and $\deg(f) = \deg(g) = 0$.

This means f and g are constant polynomials, where $f(x) = c$, $g(x) = c'$, and $fg = cc' = 1$, implying that c is a unit of R.

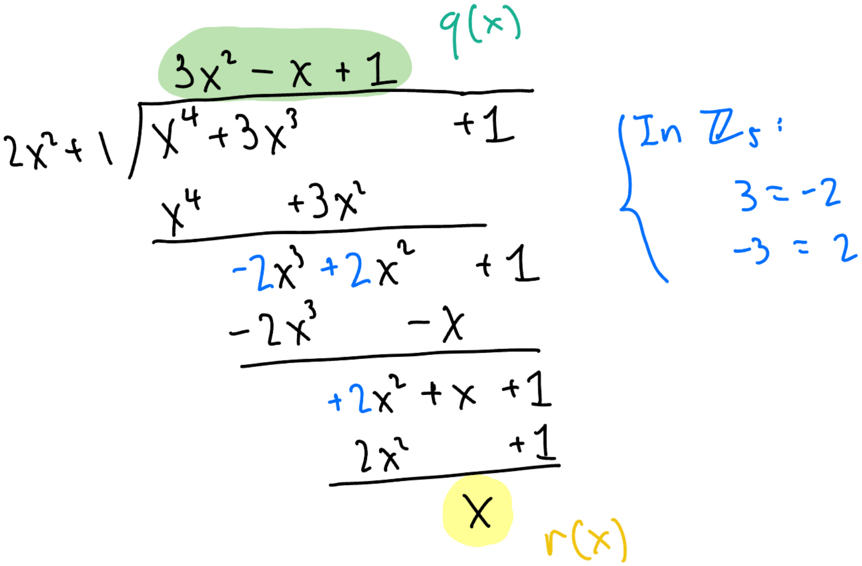
(⇐) If $f(x) = c$ and c is a unit, then $\exists c' \in R$ with $cc' = 1$. This would imply $f(x)$ is a unit in $R[x]$. □

For the rest of this lecture, we were told to assume that F is a field. In particular, for $f, g \in F[x]$,

$$\deg(fg) = \deg(f) + \deg(g)$$

And so, a very important result about $F[x]$ (where F is a field) is that we can have division with remainder (And so $F[x]$ is quite similar to $\mathbb{Z}$.) This is outlined by the long division algorithm.

Example 11.2. Divide $f(x) = x^4 + 3x^3 + 1$ by $g(x) = 2x^2 + 1$ in $\mathbb{Z}_5[x]$.



Thus, $x^4 + 3x^3 = (2x^2 + 1)(3x^2 - x + 1) + x$

The long division algorithm leads us to

Theorem 11.2 (Polynomial division).

Assume F is a field, $f(x), g(x) \in F[x]$ and $g(x) \neq 0$. Then there ***exists unique*** *polynomials $q(x), r(x) \in F[x]$ such that $f(x) = g(x) \cdot q(x) + r(x)$ and $\deg r(x) < \deg g(x)$.*

Existance and uniqueness remains to be proved. But actually, the division algorithm itself is enough to always prove existance. But can we have uniqueness?

Proof of uniqueness. Suppose for contradiction that $g(x)\cdot q_1(x)+r_1(x) = g(x)\cdot q_2(x)+r_2(x)$, where $\deg r_1(x) < \deg g(x)$, $\deg r_2(x) < \deg g(x)$, and $r_1(x) \neq r_2(x)$.

Then, doing some manipulation, we have

$$g(x)(q_1(x) - q_2(x)) = r_2(x) - r_1(x)$$

Notice that based on previous rules we've established, RHS of this equation must be nonzero, meaning LHS must also be nonzero. From here, based on **Corollary 11.1.1.**, we have that $\deg \text{LHS} \geq \deg g(x)$.

On the other hand, $\deg \text{RHS} \leq \max\{\deg r_1, \deg r_2\} < \deg g$. This is a contradiction as both sides should have the same degree!

Thus, $r_1(x) = r_2(x)$, and since $F[x]$ is an integral domain, we also have $q_1(x) = q_2(x)$. □

Notice that everything we've explore about polynomial rings so far are all analogous to $\mathbb{Z}$. This leads us to be able to bring back some number theoretic definitions.

Definition (Divides (polynomial))**.** Assume $f, g \in F[x], g(x) \neq 0$. We say that $g(x)$ **divides** $f(x)$ and write $g(x) \mid f(x)$ if $\exists h \in F[x]$ such that $f(x) = g(x) \cdot h(x)$.

Let's now make an interesting observation. Say $F = \mathbb{Q}$.

Then

$$x^5 - x = (x^2 - 1)(x^3 + x)$$

but also

$$x^5 - x) = (2x^2 - 2)\left(\frac{1}{2}x^3 + \frac{1}{2}x\right)$$

Thus, $(x^3 + x) \mid (x^5 - x)$ and $\left(\frac{1}{2}x^3 + \frac{1}{2}x\right) \mid (x^5 - x)$.

More generally, for any field F, if $g(x) \mid f(x)$ and u is any nonzero element of F (and thus a unit), then $f = gh = (ug)(u^{-1}h)$. Hence $(u \cdot g(x)) \mid f(x)$.

And so because of this, when we talk about the divisors of $f(x)$, we can concencrate on those with *leading coefficient 1.* We call these **monic** polynomials.

Example 11.3. In $\mathbb{Q}[x]$, the *monic* representative of $g(x) = 2 - 3x^{50}$ is $x^{50} - \frac{2}{3}$.

> **Intuition.** *As long as F is a field, these monic representations will exist for EVERY $f \in F[x]$, and that's because every coefficient should be invertible.*

We can also mimic this situation in $\mathbb{Z}$ and formally define the **gcd** of two polynomials.

Definition (Greatest common divisor (polynomial))**.** If $f, g \in F[x], g(x) \neq 0$, then the **greatest common divisor (gcd)** of f and g is $d(x)$ such that

- $d(x) \mid f(x)$ and $d(x) \mid g(x)$
- If $\exists c(x)$ where $c(x) \mid f(x)$ and $c(x) \mid g(x)$, then $\deg(c(x)) \leq \deg(d(x))$
- $d(x)$ is monic

12 Lecture 12: Oct. 20th

Today in lecture we continued down the rabbit-hole of trying to establish a relationship between polynomial rings and the ring of integers. We explored many mirroring concepts such as euclidean algo, prime numbers vs irreducible polynomials, fundamental theorem vs factoring polynomials. The prof also dropped a few hints here and there as to show that there are much more of these types of rings that "mirror" the integers, which we will explore in the future.

12.1 The Euclidean Algorithm

We started, as usual, with a recollection of division with remainder of polynomials. Then, we picked up where we left of last lecture by discussing whether or not the gcd of two polynomials is *unique*.

To answer this question, we make two key observations:

1. If $r(x) \neq 0$, then $\gcd(r(x), 0)$ is the *unique* monic polynomial representing $r(x)$
2. Assume $f, g \in F[x], g(x) \neq 0$, and $f(x) = g(x) \cdot q(x) + r(x)$. Then the set of common divisors of $f(x)$ and $g(x)$ is the same as the set of common divisors of $g(x)$ and $r(x)$. Basically, if one pair has unique gcd, then so must the other pair.

> **Intuition.** *Imagine some c that divides f and g. Then bring to the same side and factor, and see that c also divides r. Conversely, imagine some c that divides g and r. Factor and see that it also divides f.*

This leads us back to the **Euclidean Algorithm**. To find $\gcd(f(x), g(x))$, where $\deg(f) \geq \deg(g)$.

Then, divide f by g with remainder: $f(x) = g(x) \cdot q(x) + r(x)$ (and so $\deg r(x) < \deg g(x)$.

- If $r(x) = 0$, then $g(x)$ divides $f(x)$, and the gcd is the *monic* representative of $g(x)$
- Otherwise, $r(x) \neq 0$. Replace pair (f, g) with the pair (g, r). Repeat and stop when the remainder becomes 0.

Let's do a couple examples!

Example 12.1. Find the gcd of $f(x) = x^4 + 3x^3 + 2x + 1$ and $g(x) = x^2 - 1$ in $\mathbb{Z}_5[x]$.

$$x^4 + 3x^3 + 2x + 1 = (x^2 - 1)(x^2 + 3x + 1) + 2$$

But remember, we're in a field! So the $r(x) = 2$ should divide literally everything (including g).

Thus, $\gcd(f, g) = \gcd(g, r) = (2) = 1$

12.2 Irreducible polynomials

We then moved onto a class of polynomials that mirrors that of *prime* numbers in $\mathbb{Z}$.

Definition (Associates)**.** Let R be a commutative ring with 1. We say that $f, g \in R$ are **associate** if there a *unit* $u \in R$ such that $f = ug$.

Recall also from last time that units in $F[x]$ are nonzero constant polynomials, which implies that for two polynomials to be associates, they must have the same degree.

Definition (Irreducible polynomials)**.** A *nonconstant* polynomial $f(x) \in F[x]$ is called **irreducible** if the only divisors of $f(x)$ are

- The associates of $f(x)$, and
- Nonzero constant polynomials

Otherwise, we say f is **reducible**.

> **Intuition.** *The intuition here is that f is irreducible if it can't be "factored" into polynomials with smaller degrees.*

An easier to state version is

Lemma 12.1.
*$f(x) \in F[x]$ is **reducible** if and oly if $\exists g, h \in F[x]$ such that $f(x) = g(x)h(x)$ and* $\deg g < \deg f$*,* $\deg h < \deg f$*.*

We moved onto the main theorem of this section, describing the unique factorization of polynomials.

Theorem 12.2 (Unique factorization of polynomials).
Let F be a field and let $f(x) \in F[x]$ be a nonconstant polynomial. Then

1. *$f(x)$ is a product of irreducible polynomials in $F[x]$:*

$$f(x) = p_1(x) \cdot ... \cdot p_n(x)$$

2. *This representation of $f(x)$ as a product of irreducibles is **unique**. That is, if also $f(x) = q_1(x) \cdot ... \cdot q_m(x)$ where $q_1, ..., q_m$ are irreducible polynomials, then*
   - *$m = n$, and*
   - *there is a rearrangement of $q_1, ..., q_n$ such that* $p_i \text{ is associate of } q_i \quad \forall 1, ..., n$

> **Intuition.** *Once again, this is a direct mirror of something from the integers- Fundamental Theorem of Arithmetics! Except now, we classify the "same prime factors" as "associate irreducible polynomials".*

13 Lecture 13: Oct. 22nd

Today's lecture is *insanely* content packed. We began by discussing a full proof (both existence and uniqueness) of the unique factorization of polynomials theorem. Along the way, we also established more mirroring between polynomials and integers. We then pivoted to a different direction and discussed polynomial roots, where we are finally starting to evaluate these polynomials and exploring their properties based on the results. Definitely worth reviewing this lecture again, it was a lot of content.

13.1 Irreducible polynomials (cont'd)

We began lecture with a brief summary of what was discussed last time: polynomial rings, associates, what it means to be irreducible, and the unique factorizations of polynomials theorem. We now seek to prove the latter.

In fact, the proof of existence will look very much familiar from when we proved the fundamental theorem of arithmetic.

Proof of existence. We argue by strong induction on $n = \deg f > 0$.

Base case: $n = 1$. f must be irreducible at this point, so it is a valid factorization of itself.

Induction step: Assume all polynomials with degree $< n$ have a valid factorization. We now have 2 cases for f:

- **Case 1:** f is *irreducible*, in which case the result is trivial.
- **Case 2:** f is *reducible*. Then $f = gh$ for some g and h with $0 < \deg g < \deg f$ and $0 < \deg h < \deg f$. By the inductive hypothesis,

  $$g = p_1 \cdots p_i \text{ and } h = p_{i+1} \cdots p_n$$

  where p_i are irreducible polynomials. Then $f = p_1 \cdots p_i p_{i+1} \cdots p_n$ and we've found the factorization, as desired.

□

We then worked towards the proof of uniqueness. But remember that proving uniqueness was tricky even when we were discussing integers! So, before we get to the proof, we need to establish a few more "tools".

Lemma 13.1 (GCD Representation for polynomials).
If $\gcd(f(x), g(x)) = d(x)$*, then* $\exists a(x), b(x) \in F[x]$ *such that*

$$d(x) = f(x)a(x) + g(x)b(x)$$

Consequently, if $\gcd(f(x), g(x)) = 1$*, then* $\exists a(x), b(x) \in F[x]$ *such that*

$$f(x)a(x) + g(x)b(x) = 1.$$

Further, in $\mathbb{Z}$, the proof of uniqueness of prime factorization relied on the fact that if p is a prime and $p \mid ab$, then p must divide at least one of a and b. Let's try to find an analogous version in $F[x]$.

Lemma 13.2.

If $p(x)$ is irreducible, $\gcd(p(x), f(x)) = 1$, and $p(x) \mid f(x)g(x)$, then $p(x) \mid g(x)$.

Proof. Since $\gcd(p(x), f(x)) = 1$, by GCD representation, $\exists a(x), b(x) \in F[x]$ such that

$$1 = p(x)a(x) + f(x)b(x)$$

Then, multiplying both sides by $g(x)$ gives us

$$g(x) = g(x)p(x)a(x) + g(x)f(x)b(x)$$

Since $p(x) \mid p(x)$ and $p(x) \mid g(x)f(x)$, $p(x)$ must also divide the linear combination of the two. Thus, $p(x) \mid g(x)$. □

Lemma 13.3.

If $p(x)$ is irreducible and $p(x) \mid f(x)g(x)$, then $p(x) \mid f(x)$ or $p(x) \mid g(x)$.

Proof. If $p(x) \mid f(x)$, we are done. Otherwise, since $p(x)$ is irreducible, we must have $\gcd(p(x), f(x)) = 1$. By the previous lemma proved, we must have $p(x) \mid g(x)$. □

We are now ready to tackle the big boy. Let's get back to the proof of uniqueness of the unique factorization of polynomials.

Proof of uniqueness. We argue by strong induction on $n = \deg f > 0$.

Base case: $n = 1$. Then f is irreducible by definition, and thus is a unique factorization of itself.

Inductive step: Assume all polynomials of degree $< n$ all have unique factorizations. Then let $f \in F[x]$ be some polynomial of degree n, and assume that

$$f = p_1 ... p_k = q_1 ... q_m \tag{1}$$

Then $p_1 \mid (q_1 ... q_m)$. Since p_1 is irreducible, by the lemmas we've just proven, p_1 divides one of $q_1, ..., q_m$. By renumbering, we can say that $p_1 \mid q_1$, and since q_1 is irreducible, p_1 and q_1 must be associates. In other words, $p_1 = uq_1$ for some nonzero $u \in F$.

From here, dividing both sides of (1) by p_1, we get

$$p_2 \cdots p_k = (uq_2)q_3 \cdots q_m := f'$$

Then $\deg f' < \deg f$, and so by the inductive hypothesis, f' has a unique factorization. Hence so does f. □

We ended the discussion of irreducible polynomials with a brief summary . We saw that

- $F[x]$ is a *ring of polynomials*; F is a subring of $F[x]$
- For each $f \in F[x]$, we defined $\deg f$. If $f \neq 0$, then $\deg f$ is a nonnegative integer
- $F[x]$ is an *integral domain*; $\deg(fg) = \deg(f) + \deg(g) \quad \forall f, g \in F[x]$
- In $F[x]$, we can *divide with remainder*: $\forall f, g \in F[x], g \neq 0, \exists! q, r \in F[x]$ such that $f = gq + r$ and $\deg r < \deg g$
- This leads to the *Euclidean Algorithm* for finding *gcd* of polynomials
- This, in turn, leads to the **gcd representation theorem** and **uniqueness of factorization**.

13.2 Roots of polynomials

Recall that a polynomials is just a formal expression- at the end of the day, it's still a function, and sometimes, the result of that function might be 0, at which point a few interesting events can occur. Let's take a look.

Definition (Roots of polynomials)**.** Let $f(x) \in R[x]$, we say that $b \in R$ is a **root** of $f(x)$ if $f(b) = 0_R$.

This leads us to a powerful theorem.

Theorem 13.4 (Factor theorem).
Let F be a field, $f(x) \in F[x]$, and $a \in F$. Then the remainder of $f(x)$ when divided by $x - a$ is $f(a)$, that is, $f(x) = (x - a) \cdot q(x) + f(a)$.

In particular, a is a root of f if and only if $(x - a) \mid f(x)$.

> **Intuition.** *It's like testing how "far off" $x = a$ is from being a root of f.*

Proof. Divide $f(x)$ by $x - a$ with remainder: $f(x) = (x - a)q(x) + r(x)$. Here, we must have by definition of division with remainder that $\deg r(x) < \deg(x - a) = 1$, so $r(x)$ must be a constant polynomial. Let's call $r(x) = c$.

Plugging in $x = a$ now gives us $f(a) = 0 \cdot q(x) + c$, hence $f(a) = c$. This completes

$$f(x) = (x - a)q(x) + f(a)$$

In particular, $f(a) = 0$ iff $(x - a) \mid f(x)$. □

How is this theorem useful? Let's take a look at a few examples.

Example 13.1. Is $x^3 + x - 2$ irreducible in $\mathbb{R}[x]$? Well, we see that $x = 1$ is a solution to this equation, since $1 + 1 - 2 = 0$.

From the factor theorem, we thus know that $(x - 1) \mid (x^3 + x - 2)$, meaning it is, in fact, reducible in $\mathbb{R}[x]$. In general, if we have $(x - 1) \mid f(x)$, it would imply f is reducible, UNLESS of course, $f(x) = u(x - 1)$.

In fact, we have some comments about the factor theorem.

Corollary 13.4.1.

Let F be a field, $f(x) \in F[x]$ a nonconstant polynomial, and $a \in F$. If $f(a) = 0$, then f is divisible by $x - a$, and so f is reducible in $F[x]$ unless $\deg f = 1$.

Remark. Since $2 = 1 + 1$ and $3 = 1 + 2$ are the only ways to represent 2 and 3 using sums of integers (agnostic of ordering), we can see then that if f has degree 2 or 3, then f must be reducible *if and only if* f has a root in F.

(this is NOT the case with degree ≥ 4!!!!!!)

14 Lecture 14: Oct. 24th

This might be one of the hardest lectures for me so far. I was completely lost at multiple points throughout, but I think I was able to piece it together towards the end. The story lines with polynomials has deviated away from mirroring integers and more into the "idfk whats going on" category.

14.1 Roots of polynomials (cont'd)

We began lecture with a recollection of the previous discussion on polynomials and their roots. Specifically, recall the factor theorem.

We now continued with a discussion regarding the idea of a "polynomial". Here, it's important to stress that a polynomial $f(x) = a_0 + a_1x + \cdots + a_nx^n$ is NOT a function from R to R, but we should rather perceive it as a formal expression in $R[x]$.

The following example shows why this distinction is important:

Example 14.1. Let p be prime and consider $f(x) = x^p - x$ in $\mathbb{Z}_p[x]$. This is a polynomial of degree p, and clearly not the zero polynomial. But what is $f(a)$ for any $a \in \mathbb{Z}_p$?

Well, recall from **theorem 3.1** (quite a while ago!) that we showed

$$f(a) = a^p - a = a - a = 0$$

This would mean that two *clearly distinct* polynomials $f, g \in F[x]$ may induce **the same function** $F \to F$.

> **Intuition.** *Here, "inducing" a function basically just means the function produced by $f(x)$ when we plug in a. For example, $f(x) = x^2 + 1$ induces the function that sends each number a to $a^2 + 1$.*
>
> *In the above example, we've found two different polynomials that induces the same function: the function that sends any input a in $\mathbb{Z}_p$ to the zero element.*

But soon, we will see that this cannot happen if F is an infinite field. This brings us to two important theorems:

Theorem 14.1.

If $f(x) \in F[x]$ and $\deg f(x) = n$, then f has at most n distinct roots.

Theorem 14.2.

If F is an ***infinite*** *field and $f(x), g(x) \in F[x]$, then f and g induce the the* ***same functions*** *$F \to F$ if and only if $f(x) = g(x)$ as polynomials.*

We are going to prove them a bit out of order.

Proof of 14.2. ($\Leftarrow$) This is trivial. If $f(x) = g(x)$ then they have to induce the same functions.

($\Rightarrow$) We prove by contrapositive in this case: if $f(x) \neq g(x)$, then they *must* induce different functions on F.

Consider $h(x) = f(x) - g(x)$. Since $f(x) \neq g(x)$, we know that $h(x)$ is a nonzero polynomial. Call $\deg h = n$ for some $n \geq 0$.

By theorem 1, $h(x)$ has at most n roots. Since F is given as an **infinite** field, we thus know that there must exist some $a \in F$ where a is not a root of $h(x)$, so $h(a) \neq 0$.

Then, for that same a, we must have $f(a) \neq g(a)$. Thus f and g must induce different functions on F. □

Proof of 14.1. Assume $a_1, ..., a_k \in F$ are all roots of some of $f(x)$. Then, by factor theorem, we know that $(x - a_1) \mid f$, so

$$f(x) = (x - a_1)g_1(x)$$

for some $g_1(x) \in F[x]$. But $a_2 \in F$ is also a root! So we must have

$$0 = f(a_2) = (a_2 - a_1) \cdot g_1(a_2)$$

Since $a_2 - a_1 \neq 0$ and F is an integral domain, then we must have $g_1(a_2) = 0$. By factor theorem, this means $(x - a_2) \mid g_1$, and so

$$f(x) = (x - a_1)(x - a_2)g_2(x)$$

for some $g_2(x) \in F[x]$.

Continuing like this, we conclude

$$f(x) = (x - a_1)(x - a_2) \cdots (x - a_k)g_k(x)$$

for some $g_k(x) \in F[x]$. Hence $n = \deg f = k + \deg g_k$, and so $k \leq n$. □

We ended our discussion of polynomial roots with a quick summary of the three main theorems:

- Factor theorem: $\forall f \in F[x]$ and $a \in F$, $f(x) = (x - a) \cdot q(x) + f(a)$
- A polynomial $f \in F[x]$ of degree n has at most n distinct roots
- If F is finite, then $f(x), g(x) \in F[x]$ induce the same functions $F \to F$ if and only if $f(x) = g(x)$ as polynomials

14.2 Polynomials in $\mathbb{Q}[x]$

To begin with some motivation, we'd like to find some ways to test if $f(x) \in \mathbb{Q}[x]$ is reducible or not. We began with an observation:

If $f(x) \in \mathbb{Q}[x]$, then there is some $a \in \mathbb{Z}, a \neq 0$ such that $af(x) \in \mathbb{Z}[x]$.

Example 14.2. $\frac{1}{3}x^2 + 5x + \frac{1}{6} \xrightarrow{\times 6} 2x^2 + 30x + 1$

Recall also that if $f(x)$ has a root in $\mathbb{Q}$ and $\deg f > 1$, then $f(x)$ is reducible. This brings us to an important theorem.

Theorem 14.3 (Rational root test).
1) If $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in \mathbb{Z}[x]$ with $n \geq 1$ is a monic polynomial, then all rational roots of $f(x)$ are integers.

2) More generally, if $f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in \mathbb{Z}[x]$ with $n \geq 1$ and $\alpha = \frac{r}{s} \in \mathbb{Q}$ is a nonzero root of $f(x)$ written in the reduced form, then $r \mid a_0$ and $s \mid a_n$.

> **Intuition.** *If a rational number makes a polynomial with integer coefficients equal to zero, then the integer parts (the coefficients) must already be set up so that all the fractions clear out perfectly.*

To break this down a bit, let's try out some examples.

Example 14.3. Is $f(x) = x^3 - x - 1$ irreducible in $\mathbb{Q}[x]$?

Well, since $\deg f = 3$, we know that $f(x)$ is reducible if and only if $f(x)$ has a rational root. Now, by the rational root test, we can see that any root must divide $a_0 = -1$, meaning the only two possible roots are $x = \pm 1$. But

$$f(1) = 1 - 1 - 1 \neq 0 \text{ and } f(-1) = -1 + 1 - 1 \neq 0.$$

Hence f has no rational roots, and so f is irreducible.

Example 14.4. Does $f(x) = 2x^7 - 9x + 3$ have a root in $\mathbb{Q}$?

If $\alpha = \frac{r}{s} \in \mathbb{Q}$ is a root, then by the theorem we must have $r \mid 3$ and $s \mid 2$, which gives us $r = \pm 1, \pm 3$ and $s = \pm 1, \pm 2$.

Hence the only choices would be $\pm 1, \pm 3, \pm\frac{1}{2}, \pm\frac{3}{2}$. Plug and chug. Notice that none of them are roots.

Let's now slowly build towards the proof for this mad boy.

Proof. Since $\alpha = \frac{r}{s}$ is in reduced form, $\gcd(r, s) = 1$. Also, since $\alpha = \frac{r}{s}$ is a root,

$$a_n\frac{r^n}{s^n} + a_{n-1}\frac{r^{n-1}}{s^{n-1}} + \cdots + a_1\frac{r}{s} + a_0 = 0$$

Hence

$$a_n r^n + a_{n-1} r^{n-1} s + \cdots + a_1 r s^{n-1} + a_0 s^n = 0.$$

Notice here that all summands of this equation but the first one has a factor of s, and the sum is zero. We must then have $s \mid a_n r^n$, but $\gcd(r, s) = 1$, so $s \mid a_n$.

Similarly, all summands of the equation but the last one has a factor of r, and the sum is zero. We must then have $r \mid a_0 s^n$, but $\gcd(r, s) = 1$, so $r \mid a_0$. □

Banggggg!!! This is actually one of the few times where the proof made the theorem statement more intuitive for me. Anyway,

It turns out that testing irreducibility over $\mathbb{Q}$ is equivalent to testing irreducibility over $\mathbb{Z}$:

Theorem 14.4 (Gauss lemma).
Assume $f(x) \in \mathbb{Z}[x]$. Then $f(x)$ factors as $g(x)h(x)$ in $\mathbb{Q}[x]$ if and only if $f(x)$ factors as $\tilde{g}(x)\tilde{h}(x)$ in $\mathbb{Z}[x]$, where $\tilde{g}(x)$ is an associate of $g(x)$ in $\mathbb{Q}[x]$ and $\tilde{h}(x)$ is an associate of $h(x)$ in $\mathbb{Q}[x]$.

> **Intuition.** *This is actually a HUGE result. Essentially, we're saying if some f can be factored to $g \cdot h$ with rational exponents, then that factorization would have already existed with integer exponents- it's just been rewritten with fractions.*

Let's take a look at an example:

Example 14.5. Is $f(x) = x^4 - 5x^2 + 1$ reducible over $\mathbb{Q}$?

Well, first, by the rational root test, the only possible rational roots are ±1. But $f(\pm 1) = 1 - 5 + 1 \neq 0$, so no rational roots.

From here, by Gauss lemma, if $f(x)$ is reducible over $\mathbb{Q}$, then it has to be reducible over $\mathbb{Z}$. And since there's no rational roots, we would logically need to find potential roots hidden within the quadratic factors (complex roots!)

In other words, we're looking for $a, b, c, d \in \mathbb{Z}$ such that

$$\begin{aligned} x^4 - 5x^2 + 1 &= (x^2 + ax + b)(x^2 + cx + d) \\ &= x^4 + (a + c)x^3 + (ac + b + d)x^2 + (bc + ad)x + bd \end{aligned}$$

Then $bd = 1$, $bc + ad = 0$, $ac + b + d = -5$, $a + c = 0$, and now the problem reduces down to finding an integer solution to this systems of equations (woahhhhhhh).

Does such a solution exist? To. Be. Continued...

15 Lecture 16: Oct. 31st

Today in lecture we dived even deeper into the world of irreducibility with respect to $\mathbb{Q}[x]$. I like that we were able to "zoom out" a bit and re-establish the bigger picture, since this was the first lecture back from the midterm. Much of the lecture was dedicated to showing and proving Eisenstei'n criterion, but the bigger picture of how all the lemmas and theorems we've discussed so far play into factoring polynomials in $\mathbb{Q}[x]$ is starting to make more sense.

15.1 Polynomials in $\mathbb{Q}[x]$ (cont'd)

We are back! The last two days of lecture were dedicated to a midterm review session and an actual midterm. Additionally, today we opened with a summary of the midterm problems as well as an overview of the score distributions.

Let's dive back into the content. We first went over a summary of polynomials in $\mathbb{Q}[x]$ so far. Continuing the example from the previous set of notes, we were discussing the following example.

Example 15.1. Is $f(x) = x^4 - 5x^2 + 1$ reducible over $\mathbb{Q}$?

First, by the rational root tests we found that there cannot be any rational roots. From there, by Gauss lemma, we found that

$$\begin{aligned} x^4 - 5x^2 + 1 &= (x^2 + ax + b)(x^2 + cx + d) \\ &= x^4 + (a + c)x^3 + (ac + b + d)x^2 + (bc + ad)x + bd \end{aligned}$$

So this problem boils down to a systems of equations problem. Does $bd = 1$, $bc + ad = 0$, $ac + b + d = -5$, $a + c = 0$ have an integer solution?

Since $b, d \in \mathbb{Z}$, we must have $b = d = \pm 1$. $a + c = 0$ gives us $a = -c$. Then $ac + b + d = -5$ gives us $-a^2 + 2b = -5$. Since $b = \pm 1$, we have $a^2 = 3$ or 7, neither of which are perfect squares.

We conclude that no such a, b, c, d can exist, and $f(x)$ cannot be reducible in $\mathbb{Q}$.

Before we dive into the examples from today, we first discussed all the ways to determine if $f(x) \in \mathbb{Q}[x]$ is irreducible. Specifically, we had three important techniques

- If $f(x) \in \mathbb{Q}[x]$, then there exists some $a \in \mathbb{Z}$ with $a \neq 0$ such that $af(x) \in \mathbb{Z}[x]$
- Rational root test - helps determine factors based on divisibility by the leading coefficient and the constant term
- Gauss lemma - allows us to reduce factors to their integer-coefficient counterparts

And today, we will discuss an additional tool to test irreducibility over $\mathbb{Q}$.

Theorem 15.1 (Eisenstein's criterion).
Assume $f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in \mathbb{Z}[x]$, $n \geq 1$. If for some ***prime*** *p, $f(x)$ satisfies the following conditions:*

1. $\gcd(a_n, p) = 1$
2. $p \mid a_0, p \mid a_1, ..., p \mid a_{n-1}$
3. *a_0 is not divisible by p^2*

then $f(x)$ is ***irreducible*** *in $\mathbb{Q}[x]$.*

Let's do some examples!

Example 15.2. Is $f(x) = 2x^7 - 99x^3 + 3$ reducible in $\mathbb{Q}[x]$?

Pick $p = 3$. We see that $\gcd(2, 3) = 1$, and that $3 \mid 99$, $3 \mid 3$, and 3 is not divisible by 9. Thus, by Eisenstein's criterion, we can clearly see that $f(x)$ is irreducible in $\mathbb{Q}[x]$.

Remark. This theorem allows us to show that for every positive integer n, there has to exist a polynomial of degree n that is irreducible in $\mathbb{Q}[x]$.

We now work towards the proof of this criterion.

Proof. We are given $f(x) = a_nx^n + \cdots + a_1x + a_0 \in \mathbb{Z}[x]$ with $n \geq 1$. We are also given that for some prime p,

$$\gcd(a_n, p) = 1; p \mid a_0, ..., p \mid a_{n-1}; a_0 \text{ is not divisible by } p^2$$

We have to show that $f(x)$ is irreducible in $\mathbb{Q}[x]$. Here, by Gauss lemma, suffices to prove irreducibility in $\mathbb{Z}[x]$.

Assume here for contradiction that there exists *nonconstant* polynomials $g(x), h(x) \in \mathbb{Z}[x]$ such that $f(x) = g(x) \cdot h(x)$, where $g(x) = b_mx^m + b_{m-1}x^{m-1} + \cdots b_0 \in \mathbb{Z}[x]$ and $h(x) = c_lx^l + c_{l-1}x^{l-1} + \cdots c_0 \in \mathbb{Z}[x]$.

Let's now take a clever step! Since $\gcd(a_n, p) = 1$ and $p \mid a_0, ..., p \mid a_{n-1}$, it follows that in modulo p,

$$\bar{g}(x) \cdot \bar{h}(x) = \bar{f}(x) = [a_n]x^n, \text{ where } [a_n] \neq 0 \text{ in } \mathbb{Z}_p$$

By uniqueness of factorization in $\mathbb{Z}_p[x]$, $\bar{g}(x) = [b_m]x^m$ and $\bar{h}(x) = [c_l]x^l$. Thus, all other coefficients $[b_{m-1}, ..., [b_0], [c_{l-1}], ..., [c_0]$ are **zeros** in $\mathbb{Z}_p$. This means that $b_{m-1}, ..., b_0, c_{l-1}, ..., c_0$ are divisible by p.

In particular, $p \mid b_0$ and $p \mid c_0$. But then $a_0 = b_0c_0$ is divisible by p^2. This creates a contradiction with our assumption that a_0 is not divisible by p^2. Thus, we conclude that $f(x)$ must be irreducible. □

Idk about yall, but reducing to mod p feels clever but also at the same time feels a little like cheating and not very obvious. So let's rework the proof a little bit for version 2:

Proof. Assume again for contradiction that $f(x) = g(x)h(x)$ where $g(x) = b_m x^m + \cdots + b_1 x + b_0 \in \mathbb{Z}[x]$ and $h(x) = c_l x^l + \cdots c_1 x + c_0 \in \mathbb{Z}[x]$ are nonconstant. I.e., $f(x)$ is reducible.

Then $a_n = b_m c_l$, and since $p \nmid a_n$, we know that $p \nmid b_m$ and $p \nmid c_l$.

We also know that $a_0 = b_0 c_0$, and since $p \mid a_0, p^2 \nmid a_0$, we know that p divides exactly one of b_0 or c_0. WLOG assume $p \mid b_0$ but $p \nmid c_0$.

Since p divides b_0 but not b_m, we know there must exist some smallest $0 < i \leq m < n$ where p does not divide b_i.

Now consider the coefficient of such x^i. We know that since $f(x) = g(x)h(x)$, we have the coefficient of x^i is $b_i c_0 + b_{i-1} c_1 + \cdots + b_0 c_i = a_i$.

Since $p \mid b_0, p \mid b_1, ..., p \mid b_{i-1}$, but p divides neither b_i nor c_0, this sum is thus *not* divisible by p. Thus, p does not divide a_i for some $i \leq n$, contradicting the assumptions. □

16 Lecture 17: Nov. 3rd

Today in lecture we wrapped up our discussion irreducibility in $\mathbb{Q}[x]$, which was the bulk of the content within this chapter. From there, we moved on to discussing irreducibility within other fields such as $\mathbb{R}$ and $\mathbb{C}$, which all turned out to be a bit boring, since fields like $\mathbb{R}$ and $\mathbb{C}$ are so powerful. We then started a new discussion regarding congruence of polynomials under any generalized field $F[x]$. The lecture wasn't too challenging I suppose, but there are a lot of small bits and pieces of information I need to fully conceptualize.

16.1 Polynomials in $\mathbb{Q}[x]$ (cont'd)

We began lecture with a discussion of the 3 tools that are used to test irreducibility in $\mathbb{Q}[x]$:

1. Rational root test
2. Gauss lemma (used for "brute force" irreducibility; also handy for Eisenstein's proof)
3. Eisenstein's Criterion

And as a recollection, when we proved Eisenstein's Criterion last lecture, we used an interesting technique- arguing by mod p. Let's now explore this proof technique a bit.

If $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ is reducible over $\mathbb{Z}$, and p is a prime that does not divide a_n, then

$$\bar{f}(x) := [a_n]x^n + [a_{n-1}]x^{n-1} + \cdots + [a_1]x + [a_0] \in \mathbb{Z}_p[x] \text{ is reducible over } \mathbb{Z}_p.$$

In other words, if $\bar{f}(x) \in \mathbb{Z}_p[x]$ is *irreducible* over $\mathbb{Z}_p$, then $f(x)$ is *irreducible* over $\mathbb{Z}$ (the contrapositive).

But why is this helpful? Well, since $\mathbb{Z}_p[x]$ has only finitely many polynomials of degree smaller than $\deg(f)$, it could be feasible for us to check.

Proof. The map $\mathbb{Z}[x] \to \mathbb{Z}_p[x]$ as defined by $f \mapsto \bar{f}$ is a homomorphism! This means that for some $f(x) = g(x)h(x)$, we have $\bar{f}(x) = \bar{g}(x)\bar{h}(x)$. Further, since p does not divide a_n, we know that the term of highest degree will not be "reduced" out by the mapping. In other words, $\deg \bar{g} = \deg g$ and $\deg \bar{h} = \deg h$. Thus if g and h are non-constant polynomials, then so are $\bar{g}$ and $\bar{h}$. □

Remark. The converse *does not* hold! If $\bar{f}(x)$ is reducible over $\mathbb{Z}_p$, that doesn't tell us anything about $f(x)$.

Example 16.1. Is $f(x) = x^5 + 4x^3 + 3x^2 + 8x + 1$ reducible over $\mathbb{Z}$?

Well, let's try to argue in **mod 2**:

We have $\bar{f}(x) = x^5 + x^2 + 1$. Does $\bar{f}$ have roots in $\mathbb{Z}_2$? Since there are only two elements in $\mathbb{Z}_2$, it makes our job very very easy. We see that $\bar{f}(0) \neq 0$ and $\bar{f}(1) \neq 0$.

Okay, can we have $x^5+x^2+1 = (x^3+\cdots)(x^2+\cdots)$? Well since $\bar{f}(x)$ has no roots, we know that neither the cubic nor quadratic term can have roots. Again, since we are in $\mathbb{Z}_2$, we only have 4 possible quadratic polynomials (of which only *one* is irreducible). We simply check that it does not divide.

Since $\bar{f}(x)$ is irreducible over $\mathbb{Z}_p$, we thus know that $f(x)$ is irreducible over $\mathbb{Z}$, and by Gauss's lemma, we know $f(x)$ is irreducible over $\mathbb{Q}$.

16.2 Irreducibility in $\mathbb{C}[x]$

Unlike with $\mathbb{Q}[x]$, where for all $n > 0$ there must exist an irreducible polynomial of degree n, in $\mathbb{C}[x]$, we have the following theorem.

Theorem 16.1 (Fundamental Theorem of Algebra).

Every nonconstant polynomial in $\mathbb{C}[x]$ has a root.

This leaves us with some corollaries.

Corollary 16.1.1.

(1) The only irreducible polynomial in $\mathbb{C}[x]$ are polynomials of degree 1
(2) If $f(x) = a_nx^n + \cdots + a_1x + a_0 \in \mathbb{C}[x], n \geq 1, a_n \neq 0$, then there exist $c_1, ..., c_n \in \mathbb{C}$ such that $f(x) = a_n(x-c_1)\cdots(x-c_n)$

Example 16.2. Factor x^4+4 over $\mathbb{C}$.

Well observe that $2i = (1+i)^2$ and $-2i = (1-i)^2$, and so

$$\begin{aligned} x^4+4 &= (x^2)^2 - (2i)^2 \\ &= (x^2-2i)(x^2+2i) \\ &= (x-(1-i))(x+(1-i))(x-(1+i))(x+(1+i)) \end{aligned}$$

Now, let's see if we can work on transitioning this thought to the real numbers! Assume $f(x) \in \mathbb{R}[x] \subset \mathbb{C}[x]$.

Observation 1: If $z = a+bi \in \mathbb{C}$ is a root of f, then $\bar{z} = a - bi$ is also a root of f. In other words, for some real valued polynomial, its non-real roots *will always* come in pairs!

Observation 2: $(x-(a+bi))(x-(a-bi)) = x^2 - 2ax + (a^2+b^2)$ has real coefficients. This leads us to

Theorem 16.2.

Every nonconstant polynomial $f(x) \in \mathbb{R}[x]$ factors as a product of linear and quadratic polynomials in $\mathbb{R}[x]$. Further, a quadratic polynomial $f(x) = ax^2+bx+c$ is irreducible if and only if $b^2-4ac < 0$.

Corollary 16.2.1.

Every $f(x) \in \mathbb{R}[x]$ of odd degree has at least one real root. In fact, it must have an odd number of real roots.

16.3 Congruence in $F[x]$

We've discussed many similarities between $\mathbb{Z}$ and $F[x]$: divisibility, Euclidean algorithm, primes / irreducibles, unique factorizations

Well, let's now talk about "modular arithmetic":

- In $\mathbb{Z}$, we can work with $\bmod p$, where $p \neq 0$ (not necessarily prime)
- So in $F[x]$, can we work with some $\bmod p(x)$, where $p(x) \neq 0$ is some polynomial??

How should we define $f(x) \equiv g(x) \pmod{p(x)}$?

Definition (Polynomial congruence)**.** If $f(x), g(x) \in F[x]$ and $p(x) \in F[x], p(x) \neq 0$, then we say that $f(x)$ and $g(x)$ are congruent mod $p(x)$ and write $f(x) \equiv g(x) \pmod{p(x)}$ if $f(x) - g(x)$ is divisible by $p(x)$.

Example 16.3. Are $x^3 + x$ and $x + 1$ congruent mod $x - 1$ over any field F?

Yes. Because $(x^3 + x) - (x + 1) = x^3 - 1 = (x - 1)(x^2 + x + 1)$ which is clearly divisible by $(x - 1)$.

Example 16.4. If $f(x) \in F[x]$ and $p(x) = x - a \in F[x]$, what constant polynomial is congruent to $f(x)$ mod $p(x)$?

By the factor theorem, we know $f(x) = (x - a)g(x) + f(a)$. This implies $f(x) \equiv f(a) \pmod{p(x)}$.

17 Lecture 18: Nov. 5th

Today in lecture we further explored modular properties within polynomial rings. Specifically, many of the familiar rings from the integers of the form $\mathbb{Z}_n$ are carried over to their polynomial counterparts over any generalized field F in the form $F[x]/p(x)$. Things are getting pretty abstract, and there's constantly representatives and equivalent forms that we need to juggle around.

17.1 Congruence in $F[x]$ (cont'd)

We started with a recollection of the previous lecture, specifically regarding the idea of "congruence" on polynomials. Recall: $f(x) \equiv g(x) \pmod{p(x)}$ if $p(x) \mid f(x) - g(x)$, almost an exact mirror version of its $\mathbb{Z}$ counterpart.

Theorem 17.1.

Congruence mod $p(x)$ is an equivalence relation, that is, it is reflexive, symmetric, and transitive.

And because of this, we can once again extend the idea of "congruence classes" to polynomials as well.

Definition (Polynomial Congruence Classes)**.** The **congruence class** of $f(x)$ mod $p(x)$ is the set

$$\{g(x) \in F[x] : f(x) \equiv g(x) \pmod{p(x)}\}$$

and we denote this class by $[f(x)]$ or $\bar{f}(x)$ or $f(x)$ mod $p(x)$

Remark. Important to remark that unlike with integers, where mod n always produced a finite set, when we mod by a polynomial $p(x)$, depending on the field F, the resulting congruence class may *not* be finite.

Example 17.1. Name some polynomials that are in the congruence class of $x^2 + 1$ mod $x + 1$.

Well, let's start with some of the obvious

$$x^2 + 1, x^2 + x + 2, x^2 + 2x + 3, ...$$

But perhaps more generally, we have $(x^2 + 1) - x(x + 1) = -x + 1$, which means $-x + 1$ is in this class.

Further, $(x^2 + 1) - (x - 1)(x + 1) = 2$, which means 2 is also in this class. In general, any polynomial of the form

$$(x^2 + 1) + (x + 1)h(x)$$

should be in this class.

And once again, since mod $p(x)$ is an equivalence relation, exactly as in $\mathbb{Z}$ and p, we can propose that

Proposition 17.2.

The set $F[x]$ is some ***disjoint union*** *of congruence classes, meaning for all $f(x), g(x) \in F[x]$, we either have $[f(x)] = [g(x)]$ or $[f(x)] \cap [g(x)] = \emptyset$.*

We will denote the set of all congruence classes of $F[x]$ mod $p(x)$ by $F[x]/(p(x))$

And with the existance of congruence classes, we should also discuss *canonical representatives*, much like we did with the integers.

Proposition 17.3.

For every $f(x) \in F[x]$, there exists a unique $r(x)$ such that

1. $f(x) \equiv r(x) \pmod{p(x)}$
2. $\deg r < \deg p$

For the proof of this, we need to show both existence and uniqueness.

Proof. **Existence:** Divide $f(x)$ by $p(x)$, and we see that $f(x) = p(x)q(x) + r(x)$. Then we have $\deg r < \deg p$ by definition of polynomial division. Further, we see that $r(x) \equiv f(x) \pmod{p(x)}$. This shows existence.

Uniqueness: Suppose not unique. That means $f(x) \equiv r'(x) \pmod{p(x)}$ for some $r'(x)$ where $\deg r' < \deg p$. This would mean $r(x) \equiv r'(x) \pmod{p(x)}$, and so $p(x) \mid r(x) - r'(x)$.

But wait! We must also have $\deg(r(x) - r'(x)) < \deg p(x)$. This implies that $r(x) - r'(x)$ must be 0, since p divides their difference but also has a greater degree. This is a contradiction and shows that $r(x)$ must be unique. □

We then discussed a brief summary on congruence in $F[x]$ thus far:

- Congruence classes are defined $[f(x)] = \{g(x) \in F[x] : f(x) \equiv g(x) \pmod{p(x)}\}$.
- We proved that canonical representatives exist and are unique in this case. This actually gives us a **bijection**:

  $$\{\text{Congruence classes mod } p(x)\} \leftrightarrow \{\text{polynomials in } F[x] \text{ of deg} < \text{deg } p\}$$

  Intuition. *Very similar to the integers; each congruence class mod $p(x)$ will be a possible remainder in division by $p(x)$, and all possible remainders $r(x)$ should be reachable, creating a bijection.*
- We denote the set of congruence classes mod $p(x)$ by $F[x]/(p(x))$.

This is a random thought, but I think I need more examples in these notes because sometimes raw dogging these proofs might be kinda hard to conceptualize. So from now on I'll try to jog down more notes on examples to solve.

Example 17.2. What is the cardinality of $\mathbb{Z}_2[x]/(x^4+x+1)$?

Well, we know that the cardinality of the congruence class must be the same as the cardinality of the set of all polynomials in $\mathbb{Z}_2[x]$ with degree less than 4.

This gives us: 2 constant polynomials (including the zero polynomial), 2 degree 1 polynomials (x and $x+1$), $2^2 = 4$ degree 2 polynomials, and $2^3 = 8$ degree 3 polynomials, making the **cardinality of the set to be 16**.

17.2 Modular Arithmetic in $F[x]$

From hereon today, let's assume $p(x)$ is nonzero to avoid discussing trivial examples.

Now of course, basic properties of modular arithmetic still holds as we transition to $F[x]$. That is, if $f(x) \equiv h(x) \pmod{p(x)}$ and $g(x) \equiv k(x) \pmod{p(x)}$, then

$$f(x)+g(x) \equiv h(x)+k(x) \qquad f(x)g(x) \equiv h(x)k(x)$$

This implies that addition and multiplication on canonical representatives of congruence classes are also maintained like their $\mathbb{Z}$ counterparts.

Example 17.3. Consider $\mathbb{Q}[x]$ and $p(x) = x^2+1$. Since $\deg(p) = 2$, the congruence classes must be of the form $[ax+b]$, where $a, b \in \mathbb{Q}$ (possibly zero).

Given this, what is $[x+1][x+2]$?

Well, multiplication of congruence classes are carried over, a good first instinct would be to just multiply the two! We get $(x+1)(x+2) = x^2+3x+2$.

This certainly works since it is a valid member of the congruence class we're looking for, but remember that we prefer to represent canonical representatives with degree less than $p(x)$. So notice

$$x^2+3x+2 \equiv 3x+1 \pmod{x^2+1}$$

Thus, our final solution would be $[x+1][x+2] = [3x+1]$.

To tie this back to the overarching theme of the course (rings!), we have the following theorem.

Theorem 17.4.
If $p(x) \in F[x]$ is a nonconstant polynomial, then

- *$F[x]/(p(x))$ is a **commutative ring with identity**.*

- *Furthermore, the mapping $i : F \to F[x]/(p(x))$ as defined by $a \mapsto [a]$ that takes any constant polynomial to its congruence class is a **monomorphism** (injective).*

Example 17.4. To explore some more properties, let's consider $F = \mathbb{Z}_2$ with $p(x) = x^2 + x + 1$ (notice the irreducibility!). What are the elements of $\mathbb{Z}_2[x]/(p(x))$? Can we potentially write addition and/or multiplication tables?

Well, the elements are $[0], [1], [x], [x + 1]$ (all polynomials with degree $< \deg p$. And yes, we can definitely write addition and multiplication tables.

$+$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x=1$	x	1	0

$\times$	1	x	$x+1$
1	1	x	$x+1$
x	x	$x+1$	1
$x+1$	$x+1$	1	x

Remark. Notice that every row of the multiplication table contains 1, which means that $\mathbb{Z}_2[x]/(p(x))$ is a field!

Let's formalize the thoughts we had throughout this example.

Theorem 17.5.
*If $p(x) \in F[x]$ is a nonconstant polynomial (not necessarily irreducible!) and $f(x) \in F[x]$ is such that $\gcd(f, p) = 1$, then $[f]$ is a **unit** in $F[x]/(p(x))$.*

Proof. Since $\gcd(f, p) = 1$, we know that $\exists u(x), v(x) \in F[x]$ such that $f(x)u(x)+p(x)v(x) = 1$ (gcd representation of polynomials).

Then, we know that $f(x)u(x) \equiv 1 \pmod{p(x)}$, and hence, $[f]$ is a unit in $F[x]/(p(x))$ and the multiplicative inverse of $[f]$ is $[u]$. □

Theorem 17.6.
*If $p(x) \in F[x]$ is irreducible, then $F[x]/(p(x))$ is a **field** (and F is a subfield of that field).*

Proof. Since $p(x)$ is irreducible in $F[x]$, for every $f(x) \in F[x]$, we have 2 cases:

- either $p(x) \mid f(x)$, in which case $[f] = [0]$ in $F[x]/(p(x))$,
- or $\gcd(f, p) = 1$, in which case the previous theorem applies and says that $[f]$ is invertible in $F[x]/(p(x))$.

And thus, all nonzero elements in $F[x]/(p(x))$ are units, and so $F[x]/(p(x))$ is a field by definition. □

We might soon realize that finding inverses in $F[x]/(p(x))$ is trickier than $\mathbb{Z}_p$.

Example 17.5. In $\mathbb{Q}[x]$, consider $f(x) = x^3 - x^2 - 1$ and $p(x) = x^2 - 1$. Is $[f]$ a unit in $\mathbb{Q}[x]/(p(x))$? And if so, what is the inverse of $[f]$?

To translate this task into doable pieces, we need to check if $\gcd(f, p) = 1$. And if the answer is 'yes', then we need to write 1 as a linear combination of f and p.

We start by applying the Euclidean algorithm.

$$\begin{aligned} x^3 - x^2 - 1 &= (x^2 - 1)(x - 1) + (x - 2) \\ x^2 - 1 &= (x - 2)(x + 2) + 3 \end{aligned}$$

and thus,

$$\gcd(f, p) = \gcd(x^3 - x^2 - 1, x^2 - 1) = \gcd(x^2 - 1, x - 2) = \gcd(x - 2, 3) = 1$$

Now, we need to use these equations to somehow express 1 in the form $fu + vp$, in which case $[u]$ will be the inverse of $[f]$. To be continued...

18 Lecture 19: Nov. 7th

Holy giga lecture bro. NGL this was both the most INTERESTING and the most CONFUSING lecture of all quarter so far. We started with more modular arithmetics with polynomials. Through that, we discussed the concept of extending fields in order to find roots, and that's when polynomials crashed my mind and I had to write a 5 paragraph essay just to be sane again. Then we started a whole new chapter in talking about absorption rings known as ideals.

18.1 Modular Arithmetic in $F[x]$ (cont'd)

Lecture started with a recollection of arithmetics on congruence classes of polynomials in $F[x]$ mod $p(x)$. Most importantly, recall that $F[x]/(p(x))$ is a commutative ring with identity that contains F as a subring.

Perhaps an example will best jog our memory.

Example 18.1. How would we construct a field of size 81?

We find any irreducible polynomial $p(x)$ of degree 4 in $\mathbb{Z}_3[x]$. Then by the theorems we've discussed previously, $\mathbb{Z}_3[x]/(p(x))$ is a field. Furthermore, recall that there is a bijection between congruence classes mod $p(x)$ and polynomials in $\mathbb{Z}_3[x]$ of degree less than p.

Using these information, we see that all canonical representatives of congruence classes in $\mathbb{Z}_3[x]/(p(x))$ are of the form $ax^3 + bx^2 + cx + d$. This gives us 3 choices for each of a, b, c, d, making a total of $3^4 = 81$ possible congruence classes, thereby creating a 81-element field.

Oh, and another thing we promised to finish last time:

Example 18.2. In $\mathbb{Q}[x]$, consider $f(x) = x^3 - x^2 - 1$ and $p(x) = x^2 - 1$. Is $[f]$ a unit in $\mathbb{Q}[x]/(p(x))$? And if so, what is the inverse of $[f]$?

Recall that we started by applying the euclidean algorithm to find that $\gcd(f, p) = 1$. We now apply the "extended" part of the euclidean algorithm. Using the information previously, we can represent $f = x^3 - x^2 - 1 = p(x-1) + (x-2)$ and $p = x^2 - 1 = (x-2)(x+2) + 3$. Combining the two gives us

$$\begin{aligned} 3 &= p - (x-2)(x+2) \\ &= p - (x+2)(f - p(x-1)) \\ &= (x^2 + x - 1)p - (x+2)f \end{aligned}$$

This tells us that $f \cdot (-x-2) \equiv 3 \pmod{p}$, which gives us $f \cdot (-\frac{1}{3}x - \frac{1}{2}) \equiv 1 \pmod{p}$. We conclude that $-\frac{x}{3} - \frac{2}{3}$ is the inverse of $\bar{f}$ in $\mathbb{Q}[x]/(p(x))$.

We now moved into some definitions.

Definition (Field Extension)**.** When F is a subfield of a field L, we say that L is an *extension field* of F (or simply an *extension* of F). Such a pair $F \subset L$ is called a **field extension**.

Some basic examples include $\mathbb{R} \subset \mathbb{C}$, $\mathbb{Q} \subset \mathbb{R}$, and as seen on one of the problem sets, $\mathbb{Q} \subset \mathbb{Q}[\sqrt{2}]$.

Applying this terminology to our focus, we see that if $p(x)$ is irreducible in $F[x]$, then $F[x]/(p(x))$ is an extension field of F. A simple example is that since $x^2 + 1$ is irreducible in $\mathbb{R}$, we say that $\mathbb{R}[x]/(x^2 + 1)$ is an extension field of $\mathbb{R}$.

> **Intuition.** *Everything builds off of each other! Since $F[x]/(p(x))$ contains all polynomial congruence classes with degree $< \deg p$, we know that it will contain all possible constant polynomials, which is exactly the field F.*

But wait, let's take a closer look at this example. Let's consider a very unique element $[x] \in \mathbb{R}[x]/(x^2 + 1)$. First, note that $x^2 \equiv -1 \pmod{x^2 + 1}$, which means the congruence class $[x]$ is the solution to this expression. In other words, $[x]^2 = -1$ in $\mathbb{R}[x]/(x^2 + 1)$.

Woah... we've just *kinda* recreated an element that acts like the imaginary unit i in our field $\mathbb{R}[x]/(x^2 + 1)$. To put this more rigorously,

Proposition 18.1.

The map $\rho : \mathbb{R}[x]/(x^2 + 1) \to \mathbb{C}$ defined by $[a + bx] \mapsto a + bi$ is an isomorphism of fields.

Let's take a look at a similar example.

Example 18.3. $\mathbb{Z}_2[x]/(x^2 + x + 1)$.

We know that $x^2 + x + 1$ is irreducible in $\mathbb{Z}_2[x]$. So $\mathbb{Z}_2[x]/(x^2 + x + 1)$ is a field that contains $\mathbb{Z}_2$. Let's relabel a couple of things:

Let $\alpha = [x]$ in $K \coloneqq \mathbb{Z}[x]/(x^2 + x + 1)$. Then $\alpha^2 + \alpha + 1 = 0$ in this field. In other words, $f(x) = x^2 + x + 1$ has a root in K, and that root is a *congruence class* (which is a polynomial on its own). Woah.

The previous two examples gives us a powerful theorem.

Theorem 18.2.

Let $p(x) \in F[x]$ be an irreducible polynomial. Then $F[x]/(p(x))$ is an extension field of F in which $p(x)$ ***has a root****.*

Proof. $\alpha = [x]$ is a root of $p(x)$ in $F[x]/(p(x))$ because $p(\alpha) = [p(x)] = [0]$. □

Corollary 18.2.1.

Let $f(x) \in F[x]$ be a nonconstant polynomial. Then there exists a field extension $E \supset F$ such that $f(x)$ has a root in E.

Proof. Factor $f(x)$ into irreducibles: $f(x) = f_1(x) \cdots f_k(x)$. Then consider $F[x]/(f_1(x))$. In this field, we have a root of f_1, which is a root of f. □

18.1.1 A note on polynomials [addendum]

This was not a part of the original lecture, but rather added on afterwards as I realized my intuition about polynomials is getting quite murky, and considering that it's the most important thing pertaining to everything we're discussing, I thought I'd clear up some things via intuition.

First: *polynomials*. Intuitively, in algebra, **a polynomial is simply a "recipe" regarding addition and multiplication on some objects**. Back in high school algebra, these objects that we would plug in always have been *real numbers*, but that's not always the case. **As long as the objects we're plugging in have well-defined addition and multiplication** (i.e., they are a part of some ring R), we can plug them in, since addition and multiplication can be executed.

Furthermore, these "recipes" themselves also have well-defined addition and multiplication with respect to *other* such recipes, making the total set of *all* such recipes a ring. **This is what we refer to as a "polynomial ring"**, and denote with $F[x]$.

The notation "$F[x]$" represents the polynomial (recipe) where coefficients of that polynomial live in the ring F. Because of this, I actually lied a bit earlier when I said that "we can plug in any object that has well-defined addition and multiplication with each other". That's because we know that whatever objects we're plugging into a polynomial **must *also* have well-defined addition and multiplication with respect to elements in** F (the coefficients).

That doesn't necessarily mean the objects we're plugging in have to be in F though! We can plug in anything that behaves well with elements of F, which is where the idea of "field extensions" come in. Elements of a field E that contains the field F will also behave well with the elements strictly within F.

This is the reason why we were able to plug in congruence class elements like "$[x]$" into polynomials in $\mathbb{R}[x]$ to find that $[x]$ behaves like i. Since $\mathbb{R}[x]/(x^2+1)$ is an extension of $\mathbb{R}$, we know $[x]$ will have well-defined addition and multiplication with respect to real numbers, which is how we came up with $[x]^2 = -1 \pmod{x^2+1}$.

Having a polynomial of polynomials (congruence classes) can be real confusing, but I hope this was able to clear things up a bit.

18.2 Ideals

To start off the new section, we revisited the integers once again for some intuition. Recall that we said if $a \equiv b \pmod{n}$, then $a - b \in \{nk : k \in \mathbb{Z}\} =: n\mathbb{Z}$.

From here $n\mathbb{Z}$ had some nice properties- it's actually a subring of $\mathbb{Z}$, since elements of $n\mathbb{Z}$ have closed addition and multiplication. But perhaps even stronger than that, we have

$$\forall a \in n\mathbb{Z} \text{ and } \forall r \in \mathbb{Z}, \text{ the product } ra \in n\mathbb{Z}$$

As we've always done in this course, let's extend this definition to rings!

Definition (Ideals)**.** Let R be any ring and $I \subseteq R$, $I \neq \emptyset$. We say that I is an **ideal** in R if

1. I is a subring, and
2. $\forall a \in I$ and $\forall r \in R$, both ra and ar are also in I

We call (1) the subring property, and (2) the "absorption" property.

Theorem 18.3.

A nonempty subset I of R is an ideal in R if and only if

1. *I is closed under subtraction, i.e., $a, b \in I \Rightarrow a - b \in I$, and*
2. *$\forall a \in I$ and $\forall r \in R$, both ra and ar are also in I*

Let's now do a ton of examples to familiarize ourselves with this concept.

Example 18.4. Is $S = \{n \in \mathbb{Z} : |n| > 100\}$ an ideal in $\mathbb{Z}$?

NO: S doesn't contain 0, so it is not a subring.

Example 18.5. Let $p(x) \in \mathbb{Q}[x]$ and let $I = \{g(x)p(x) : g(x) \in \mathbb{Q}[x]\}$. Is I an ideal in $\mathbb{Q}[x]$?

YES, indeed. $p(x) \in I$, so $I \neq \emptyset$. Also if $a(x), b(x) \in I$, then $a(x) = g(x)p(x)$ and $b(x) = h(x)p(x)$ for some $g(x), h(x) \in \mathbb{Q}[x]$. Hence $a(x) - b(x) = (g(x) - h(x)) \cdot p(x) \in I$.

Also, for any $r(x) \in \mathbb{Q}[x]$ and for all $a(x) \in I$, we have

$$r(x)a(x) = r(x) \cdot (g(x)p(x)) = (r(x)g(x)) \cdot p(x) \in I$$

We ended lecture with a just a couple more theorems and definitions. Notice that if R is a commutative ring with identity, $c \in R$, and $I := \{rc : r \in R\}$, then I is an ideal in R.

Definition (Principal Ideals)**.** An ideal of this form is called a **principal ideal** and is denoted (c) or $\langle c \rangle$.

> **Intuition.** *This is very similar to cyclic groups that we discussed in cryptography (hence the same notation). But basically a principal ideal is a set that's generated from just one element, through multiplication of any other element in that ring with the "generator".*

As some examples, $(n) \subset \mathbb{Z}$ and $(p(x)) \subset F[x]$ are principal ideals. Lastly, we write $I = (a_1, ..., a_n)$ and say that this ideal is generated by $a_1, ..., a_n$. Note here than I may not always be a principal ideal.

19 Lecture 20: Nov. 10th

Today in lecture we dove deeper into the world of ideals. We started with a TON of examples just to familiarize ourselves with the definiiton. We then went into modular congruence in terms of ideals. I found it quite interesting that ideals are yet *another* layer of abstraction on top of what we're already doing. We began the course with congruence wrt a number, then congruence wrt a function, and now congruent wrt a ring.

19.1 Ideals (cont'd)

We started lecture with a recollection of the definition of ideals. A subset in which subtraction is closed and follows that ra and ar are also in I. Basically, like an "absorbent" subring.

Example 19.1. Is the set $T = \{(k, k) : k \in \mathbb{Z}\}$ an ideal in $\mathbb{Z} \times \mathbb{Z}$?

No, it's not closed. Take any $(k, k) \times (0, 1) = (0, k)$ which is not in T.

Example 19.2. Assume R is a ring with identity and let $I \subseteq R$ be an ideal. What can we say about I if we know that I contains a unit?

Well, say $a \in I$ is a unit, then we know $a^{-1} \in R$ (but not necessarily I). By definition of an idea, we know that $aa^{-1} \in I$, which implies $1 \in I$. But then for all $r \in R$, we have $1 \cdot r \in I$. This would mean $I = R$.

Remark. We've just discovered that if an ideal I contains a unit from R, then we must have $I = R$.

Example 19.3. Consider the ring $M_2(\mathbb{R})$ of 2×2 matrices, and let $T \subset M_2(\mathbb{R})$ be the set of matrices of the form $\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}$ for $a, b \in \mathbb{R}$. Is T a subring? is T an ideal?

For sure a subring. But if we take $a = 1$ and $b = 0$, then we have the identity matrix, which, following from the previous remark, means *everything* in $M_2(\mathbb{R})$ must *also* be in T. This is clearly not the case, so we conclude T is not an ideal.

Example 19.4. Is $K = \{\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} : a, b \in \mathbb{R}\}$ an ideal in $M_2(\mathbb{R})$?

K is obviously a subring. Additionally K will always *absorb the products on the right.* However, it fails to absorb elements when multiplied on the left.

For example,

$$\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \notin K$$

and thus K is not an ideal.

We then did a recollection of principal ideals in some commutative ring with identity R, i.e., ideals of the form

$$(c) := \{rc : r \in R\}$$

And more generally, we talked about ideals generated by $a_1, ..., a_n$, i.e., ideals of the form

$$(a_1, ..., a_n) := \{r_1a_1 + \cdots + r_na_n : r_1, ..., r_n \in R\}$$

Example 19.5. In $\mathbb{Z}_{15}$, is $\{0, 3, 6, 9, 12\}$ an ideal?

Yes! A principal ideal in fact. Take $c = 3$, we have that everything in the set is a multiple of c.

Example 19.6. In $\mathbb{Z}$, is $(6, 15)$ a principal ideal?

Well, everything in the ideal $(6, 15)$ is of the form $a = 6x + 15y$. We can factor out the common divisor 3 and say $a = 3(2x + 5y)$. We now see that $(6, 15) \subseteq (3)$.

On the other hand, $3 = (-2)6 + 15$, so $3 \in (6, 15)$, hence $3r \in (6, 15)$, meaning $(3) \subseteq (6, 15)$. This implies that the set is equivalent to the principal ideal (3).

Example 19.7. In $\mathbb{Z}[x]$, is $I = \{f(x) = a_nx^n + \cdots + a_1x + a_0 : 5 \mid a_0\}$ an ideal? Is it a principal ideal?

Let's first confirm that it's an ideal. Notice that I is closed under subtraction, since subtraction is done by on the constant terms. Similarly, with multiplication of polynomials, the constant terms are also being multiplied, maintaining divisibility by 5 in both cases.

Assume I is a principal ideal. Then $\exists p(x) \in \mathbb{Z}[x]$ such that $I = (p(x))$. Since $5 \in I$, we know that I is multiples of $5p(x)$, meaning $p(x) \mid 5$. But since $p(x)$ is also in I, this forces $p(x) = \pm 5$.

On the other hand, we see that $x = x + 0$ is in I. But in $\mathbb{Z}[x]$, it doesn't make sense for us to say that x is a multiple of 5. This gives us a desired contradiction.

Example 19.8. If I and J are ideals in R, is $I \cup J$ an ideal?

NO! Take a counter example. Let $I = \mathbb{R} \times 0$ (x-axis) and $J = 0 \times \mathbb{R}$ (y-axis). Take $(0, 1) \in J$ and $(1, 0) \in I$. We then have $(1, 0) + (0, 1) = (1, 1)$ which is not in $I \cup J$ (not in either of the axes).

Example 19.9. Assume F is a field. List all ideals of F.

There are only 2: (0) and F itself. This is because every element in F is invertible and therefore a unit. We've shown earlier in **Example 19.2** that if a unit is in the ideal, then the ideal has to be the ring itself. (0) is an exception since it's the only non-invertible element in F.

Remark. To summarize, a field F has only two ideals: (0) and $(1) = F$.

On the other hand, if R is a commutative ring with identity, then for some $c \in R$ where c is not a unit, interesting ideals can actually occur. In fact, we will have at least three distinct ideals being: $(0) \subset (c) \subset (1) = R$.

This is the part of the course where we will analyze more *nuanced* objects that aren't all-powerful like a field. Cool!

We continue the analogy with modular arithmetic, let's make the following

Definition (Ideal Modular Congruence)**.** Let I be an ideal in R and let $a, b \in R$. We say that a is congruent to b modulo I, and we write $a \equiv b \pmod{I}$, if $a - b \in I$.

> **Intuition.** *Recall that if $a, b \in I$, then $a - b \in I$. This definition explores the converse of that statement: if $a - b \in I$, it's not necessarily true that $a, b \in I$, but instead, we say a, b are modular congruent wrt I.*
>
> *Being congruent modulus a ring basically means that a and b are like the "same amount away" from some subring ideal I.*

Example 19.10. Let $R = \{f : \mathbb{R} \to \mathbb{R}\}$ and let $I = \{g \in R : g(0) = 0\}$. Consider $f(x) = \cos x$ and $h(x) = x + 1$. Is f congruent to h mod I?

YES! $(f - h)(0) = f(0) - h(0) = \cos 0 - 1 = 1 - 1 = 0$. Hence f is congruent to h mod I.

We now talked about some theorems.

Theorem 19.1.

The relation of congruence modulo I is an equivalence relation.

Theorem 19.2.

Let $I \subseteq R$ be an ideal. If $a \equiv b \pmod{I}$ and $c \equiv d \pmod{I}$, then

$$a + c \equiv b + d \pmod{I} \quad \textit{and} \quad ac \equiv db \pmod{I}$$

Proof. Let's check that $ac \equiv bd \pmod{I}$.

We start by subtracting $ac - bd = (ac - bc) + (bc - bd) = (a - b)c + b(c - d)$. Since $a \equiv b \pmod{I}$, we know $(a - b) \in I$, and since $c \in R$, it implies $(a - b)c \in I$. Similarly, $c \equiv d \pmod{I}$ which means $(c - d) \in I$, and by definition of ideals, $b(c - d) \in I$.

Finally, since subtraction is closed in I by def, we have $ac - bd = (a - b)c + b(c - d) \in I$, which means $ac \equiv bd \pmod{I}$. □

As with "mod n" and "mod $p(x)$" arithmetic, we make the following

Definition (Cosets)**.** Let $I \subseteq R$ be an ideal and let $a \in R$. The congruence class of a mod I is $a + I := \{b \in R : b \equiv a \text{ mod } I\}$. We call $a + I$ the **coset** of a mod I.

> **Intuition.** *In case this wasn't clear enough, cosets are the equivalent of congruence classes in the Ideals world. It's the* set *of all elements that are the "same amount away" from some I.*

Since "mod I" is an equivalence relation, $a + I$ and $b + I$ are either equal or disjoint.

Example 19.11. Let $R = \{f : \mathbb{Z}_{10} \to \mathbb{Z}_{10}\}$, $I = \{f \in R : f(2) = 0\}$. Decsribe all cosets mod I. How many of them are there?

Two functions f and g are in the same coset iff $(f - g)(2) = 0$, which happens iff $f(2) = g(2)$. Thus, the sets are

$$\{f : f(2) = 0\}, \{f : f(2) = 1\}, ..., \{f : f(2) = 9\},$$

There are 10 such cosets.

Intuitively speaking, the ideal contains all functions in $\mathbb{Z}_{10}$ where $f(2) = 0$. So there are only 10 distinct "distances" away from this ideal, depending on the value of the function f at $x = 2$.

We denote the set of all distinct cosets of R mod I by R/I. This should look familiar! We've discussed many objects like these prior in this course with $\mathbb{Z}/\mathbb{Z}_p$, $F[x]/(p(x))$, etc.

And as with modular arithmetic on $\mathbb{Z}_n = \mathbb{Z}/(n)$ and $F[x]/(p(x))$, we can define addition and multiplication on R/I by

$$(a + I) + (b + I) := (a + b) + I \text{ and } (a + I)(b + I) := ab + I$$

Now that we have well-defined addition and multiplication, we discussed an important theorem.

Definition (Quotient Rings)**.** R/I with addition and multiplication as defined above is a **quotient ring**.

- Its zero is the coset $0 + I = I$
- If R is commutative, then so is R/I
- If R has identity and $I \neq R$, then $1 + I$ is the identity of R/I.

20 Lecture 21: Nov. 12th

Today in lecture we familiarized ourselves more with the definition of a quotient ring, the most generalized version of the whole "modular congruence" theme that we've been following along with this quarter. We then built up a lot of theorems, ultimately resulting in the discussion about the First Isomorphism Theorem- the pinnacle of this course. Overall I think I'm comfortable with the material, just needs practice tbh.

20.1 Quotient rings

We began lecture with a quick summary of quotient rings as discussed last time. If R is a ring and $I \subseteq R$ is an ideal in R, then the **quotient ring** of R by I, denoted R/I, is defined as follows

- the elements of R/I are distinct cosets of R mod I
- addition and multiplication are well-defined:

$$(a+I)+(b+I) := (a+b)+I \text{ and } (a+I)(b+I) := ab+I$$

Let's now do some examples to build up intuition.

Example 20.1. Last time we saw that in $\mathbb{Z}_{15}$, $I = \{0, 3, 6, 9, 12\}$ is an ideal. How many cosets does $\mathbb{Z}_{15}/I$ have?

There are three such cosets:

$$0+I = \{0,3,6,9,12\} \quad 1+I = \{1,4,7,10,13\} \quad 2+I = \{2,5,8,11,14\}$$

Writing down the addition and multiplication tables, we can see

$+$	$0+I$	$1+I$	$2+I$
$0+I$	$0+I$	$1+I$	$2+I$
$1+I$	$1+I$	$2+I$	$0+I$
$2+I$	$2+I$	$0+I$	$1+I$

$+$	$1+I$	$2+I$
$1+I$	$1+I$	$2+I$
$2+I$	$2+I$	$1+I$

In other words, this ring is isomorphic to $\mathbb{Z}_3$!

Example 20.2. Let R be a noncommutative ring and let $I \subset R$ be an ideal such that $ab - ba \in I$ for all $a, b \in R$. Prove that R/I is commutative.

Let a, b be any element in R. We're given that $ab - ba \in I$, which means $ab \equiv ba \pmod{I}$. This gives us $ab + I = ba + I$. From here, by multiplication as defined, we see that $(a+I)(b+I) = ab+I = ba+I = (b+I)(a+I)$. Hence, R/I is commutative. □

Definition (Kernels & Images)**.** Let $f : R \to S$ be a homomorphism of rings. Then

- the **kernel** of f is the set $\operatorname{Ker} f := \{r \in R : f(r) = 0\}$

- the **image** of f is the set Im $f \coloneqq \{s \in S : s = f(r) \text{ for some } r \in \mathbb{R}\}$

  Intuition. *Just like in linalg, kernel is all the elements that get mapped to 0. Image is all the reachable elements within the co-domain.*

Example 20.3. For each homomorphism f, compute its kernel and image. Is f an epimorphism? Is f a monomorphism?

1) $f : \mathbb{Z} \to \mathbb{Z}_{100}, a \mapsto a \bmod 100$.
All elements that are multiples of 100 will get mapped to 0, and thus Ker $f = (100)$. The image will simply remain Im $f = \mathbb{Z}_{100}$ as all elements are reachable. f is surjective, but not injective.

3) $f : \mathbb{Z}[x] \to \mathbb{Q}, a_nx^n + \cdots + a_nx + a_0 \mapsto a_0$
Here, Im $f = \mathbb{Z}$, Ker $f = (x)$, the principal ideal, all polynomials with zero constant term. f turns out to be neither surjective nor injective, since clearly multiple polynomials can map to the same integer, and not all rational numbers are reachable (only the integers are).

We now discussed some stepping-stone theorems.

Theorem 20.1.

Let $f : R \to S$ be a homomorphism of rings. Then the kernel of f is an ideal in R, while the image of f is a subring of S.

> **Intuition.** *The kernel is kinda like a black hole since any element multiplied by 0 will always be 0. So any element multiplied by something in the kernel will now also be in the kernel. This is precisely what makes something an ideal (absorption).*

Proof. Since f is a homomorphism, we know $f(0) = 0$, so $0 \in$ Ker f, and so Ker $f \neq \emptyset$.

Now, assume $a, b \in$ Ker f. Then $f(a) = f(b) = 0$. Since f is a homomorphism, we know that $f(a - b) = f(a) - f(b) = 0 - 0 = 0$, and so $(a - b) \in$ Ker f.

Finally, if $a \in$ Ker f and $r \in R$, then $f(ra) = f(r)f(a) = f(r) \cdot 0 = 0$; hence $ra \in$ Ker f. Similarly, $ar \in$ Ker f.

We thus conclude that Ker f is an ideal in R. □

Theorem 20.2.

Let $f : R \to S$ be a homomorphism of rings. Then f is a monomorphism if and only if Ker $f = (0)$.

> **Intuition.** *f can only be one-to-one if the only thing that maps to 0 is the ideal* (0)*, which should only contain 0 lol*

Proof. ($\Rightarrow$) If f is a monomorphism, then $\forall a \neq 0, f(a) \neq f(0)$. Hence $\forall a \neq 0, f(a) \neq 0$ and so Ker $f = (0)$.

($\Leftarrow$) If f is not a monomorphism, then $\exists a, b \in R, a \neq b$ such that $f(a) = f(b)$. Then $a - b \neq 0$, but $f(a-b) = f(a) - f(b) = 0$. Hence $a - b \in$ Ker f, and so Ker $f \neq (0)$. □

By the previous theorems, we found that the kernel of any homomorphism is an ideal. Can we say the converse? Turns out, we can! That is, every ideal is the kernel of some homomorphism.

Theorem 20.3.

Let $I \subseteq R$ be an ideal in R. Then the map $\pi : R \to R/I$ given by $\pi(a) = a + I$ is a surjective homomorphism with Ker $\pi = I$.

We call π the "natural" homomorphism from R to R/I.

> **Intuition.** *We take the ring R, which is a super complex structure with hella intricacies, and SMASH it down into a pancake where the only distinguishing features left are the elements' relations with I.*
>
> *That "smashing" is us creating the kernel, and all the elements that map exactly to I is now in the kernel.*

Proof. π is a homomorphism follows from definitions; for instance,

$$\pi(a)\pi(b) = (a+I)(b+I) = ab + I = \pi(ab)$$

Further, Ker $\pi = \{a \in R : a + I = 0 + I\} = \{a \in R : a \equiv 0 \bmod I\} = \{a \in R : a \in I\} = I$.

Surjectivity should be trivial. Let $a + I \in R/I$ be arbitrary. By definition, $a \in R$, which implies $\pi(a) = a + I$. □

The generalization of all the results that we proved today can be condensed into one theorem. The professor hyped this up to be the ***MAIN THEOREM*** of the course, as in, if you were to take *anything* away from this set of notes, it should be this one theorem.

Theorem 20.4 (First Isomorphism Theorem).

If $f : R \to S$ is a homomorphism of rings, then there is a (natural) isomorphism $R/$Ker $f \to$ Im f.

(In other words, a homomorphic image of R is always isomorphic to a quotient ring of R)

Corollary 20.4.1.

If $f : R \to S$ is an epimorphism, then S is isomorphic to $R/$Ker f.

Woah, crazy stuff. So anyway, we're gonna prove it next time as the proof is something we have to slowly build up to. For now, let's see some applications of this powerful theorem.

Theorem 20.5 (Decomposition theorem).
Let a, b be positive integers. If $\gcd(a, b) = 1$, then $\mathbb{Z}/(ab)$ is isomorphic to $\mathbb{Z}/(a) \times \mathbb{Z}/(b)$.

Proof. 1) We first define $f : \mathbb{Z} \to \mathbb{Z}/(a) \times \mathbb{Z}/(b)$ by $n \mapsto (n \bmod a, n \bmod b)$. This is a homomorphism of rings.

2) Notice Ker $f = \{n \in \mathbb{Z} : a \mid n, b \mid n\}$. Since $\gcd(a, b) = 1$, we know that $a \mid n$ and $b \mid n$ iff $ab \mid n$. Thus,

$$\text{Ker } f = \{n \in \mathbb{Z} : a \mid n, b \mid n\} = \{n \in \mathbb{Z} : ab \mid n\} = (ab).$$

By the first isomorphism theorem, we conclude Im f is isomorphic to $\mathbb{Z}/(ab)$.

3) It remains to be shown that f is surjective. By definition of f, Im $f \subseteq \mathbb{Z}/(a) \times \mathbb{Z}/(b)$. At the same time, by step (2),

$$|\text{Im } f| = |\mathbb{Z}/(ab)| = ab = |\mathbb{Z}/(a)| \cdot |\mathbb{Z}/(b)| = |\mathbb{Z}/(a) \times |\mathbb{Z}/(b)|$$

Thus, the image of f must be the entire $\mathbb{Z}/(a) \times \mathbb{Z}/(b)$.

It follows from the above steps that

$$\mathbb{Z}/(a) \times \mathbb{Z}/(b) = \text{Im } f \text{ is isomorphic to } \mathbb{Z}/(ab)$$

□

We ended of the lecture with one of the racism theorems that's as a corollary of the first isomorphic theorem.

Corollary 20.5.1 (Chinese remainder theorem).
If $m_1, ..., m_k$ are positive integers that are pairwise relatively prime, then $\mathbb{Z}/(m_1 m_2 ... m_k)$ is isomorphic to $\mathbb{Z}/(m_1) \times \mathbb{Z}/(m_2) \times \cdots \times \mathbb{Z}/(m_k)$

21 Lecture 22: Nov. 14th

Today's lecture was very proof heavy. We began with a recollection of kernels and images, and the theorem statement (and corollaries) of the first isomorphism theorem. We did some heavy proofs as applications of the theorem, then moved on to proving the mf thing itself! We then began discussing prime ideals before getting cut off. I am really enjoying this course rn ngl.

21.1 First Isomorphism Theorem

We started lecture with a recollection of some important definitions from the previous lecture, specifically regarding the idea of a *kernel* and an *image* of a homomorphism.

Further recall the properties of homomorphisms in terms of kernels and images: (1) the kernel of f is an ideal in R, while the image of f is a subring of S, and (2) f is a monomorphism if and only if Ker $f = (0)$.

We then discussed the theorem statement of the first isomorphism theorem, which says that there always exists a natural isomorphism $R/\text{Ker } f \to \text{Im } f$, where if f is an epimorphism, then S is isomorphic to $R/\text{Ker } f$.

And as a first application, we proved $\mathbb{Z}/(a) \times \mathbb{Z}/(b) \cong \mathbb{Z}/(ab)$, and extended this result to the chinese remainder theorem. Let's prove that theorem statement.

Proof. We induct on k. The case $k = 2$ is simply the decomposition theorem as proven previously.

For the inductive step, assume the CRT holds for $k-1$. Let $m_1, ..., m_k$ be pairwise relatively prime. Then $\gcd(m_1 \cdots m_{k-1}, m_k) = 1$, because since m_k is coprime with all the others, it must also be coprime with the product as well.

Now, by the decomposition theorem and inductive hypothesis,

$$\begin{aligned}\mathbb{Z}/(m_1 m_2 \dots m_k) = \mathbb{Z}((m_1 m_2 \cdots m_{k-1})m_k) &\cong \mathbb{Z}/(m_1 m_2 \dots m_{k-1}) \times \mathbb{Z}/(m_k)\\ &\cong \mathbb{Z}/(m_1) \times \cdots \times \mathbb{Z}/(m_{k-1}) \times \mathbb{Z}/(m_k)\end{aligned}$$

□

Let's take a look at more applications of the first isomorphism theorem! Recall that really confusing thing that I made a whole addendum about, where $\mathbb{R}[x]/(x^2+1)$ is *isomorphic* to $\mathbb{C}$. We can use the first isomorphism theorem to provide an alternative proof.

Proof. $\mathbb{R}[x]/(x^2+1)$ is *isomorphic* to $\mathbb{C}$.

1. Define $\varphi : \mathbb{R}[x] \to \mathbb{C}$ by $f([x]) \mapsto f(i)$. That is, $x \mapsto i$, $1 \mapsto 1$, and more generally $\sum_{k=1}^{n} a_k x^k \mapsto \sum_{k=1}^{n} a_k i^k$.

   For instance, $1 + x + x^2 + x^3 \mapsto 1 + i + i^2 + i^3 = 0$.

2. Check that φ is a homomorphism of rings. (trust me bro)
3. We claim that φ is surjective. Indeed, for some arbitrary $z = a + bi \in \mathbb{C}$, we have $\varphi(a + bx) = z$.

   Since φ is an epimorphism, by the first isomorphism theorem, $\mathbb{R}[x]/\text{Ker } \varphi \cong \mathbb{C}$.
4. We now investigate the kernel of φ and see that $\text{Ker } \varphi = \{f(x) \in \mathbb{R}[x] : f(i) = 0\}$. But lowk wtf does this mean? Maybe we can visit some examples to understand this kernel.

   Note that i is a root of $x^2 + 1$, and so $x^2 + 1$ is in $\text{Ker } \varphi$. Thus, $(x^2 + 1) \subseteq \text{Ker } \varphi$. By the result in step (3), the theorem would follow if we prove that $\text{Ker } \varphi = (x^2 + 1)$. Nested proof time!

   (a) $\text{Ker } \varphi = (x^2 + 1)$, i.e., $x^2 + 1$ is the "minimal" polynomial in $\mathbb{R}[x]$ with root i.

   Proof. Let $f(x)$ be an arbitrary polynomial in $\text{Ker } f$. Divide $f(x)$ by $x^2 + 1$ with remainder: $f(x) = (x^2 + 1) \cdot q(x) + r(x)$, where $\deg r(x) \leq 1$, $r(x) \in \mathbb{R}[x]$.

   Then $0 = f(i) = 0 + r(i)$, and so $r(i) = 0$. But since $i \notin \mathbb{R}$, the only polynomial with real coefficient of degree ≤ 1 that has i as a root is the zero polynomial. Hence, $r = 0$, meaning $x^2 \mid f(x)$, and so $f(x) \in (x^2 + 1)$.

   We conclude that $\text{Ker } \varphi \subseteq (x^2 + 1)$. Since $x^2 + 1 \in \text{Ker } \varphi$, we also have $(x^2 + 1) \subseteq \varphi$. Therefore, $\text{Ker } \varphi = (x^2 + 1)$. □

   And finally, since we've shown $\text{Ker } f = (x^2 + 1)$, this is enough for us to conclude that by the result found in step (3), we have $\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C}$.

□

The first isomorphic theorem gives us so many power corollaries and can also be used as a powerful proof technique when showing isomorphism. Isn't it neat? Maybe it's time for us to lift up the hood a bit and really investigate how it works.

We're given a ring homomorphism $f : R \to S$ with $\text{Ker } f = K$ and $\text{Im } f = S'$. We have to show that R/K is isomorphic to S'. Let's draw a picture!

$$\begin{tikzcd}
R \arrow[r, "f"] \arrow[d, "\pi"'] & S' \subset S \\
R/K \arrow[ur, "\bar{f}"'] &
\end{tikzcd}$$

Here π is the natural projection: $\pi(a) = a + K$, and f is a given map. We want to construct a (natural) map $\bar{f} : R/K \to S'$ and show that it is an isomorphism.

Since we want $\bar{f}$ to be "natural", let's then go with the choice that feels the most obvious and *effortless*. We define $\bar{f} : R/K \to S'$ by $\bar{f}(a + K) = f(a)$ for all $a + K \in R/K$. We now need to answer the following questions:

- Is $\bar{f}$ well-defined?
- Is $\bar{f}$ a homomorphism?
- Is $\bar{f}$ surjective?
- Is $\bar{f}$ injective?

And if we were to find that the answer to all of these questions are overwhelmingly YES, then $\bar{f} : R/K \to S'$ is an isomorphism, and so $R/\text{Ker } f$ is isomorphic to $\text{Im } f$, as desired. Let's start one by one:

1. Is $\bar{f}$ well-defined?

   YES! This is because

   (a) if $a + K = b + K$, then $a - b \in K = \text{Ker } f$. Hence $f(a - b) = 0$, and so $f(a) = f(b)$.

   (b) $\bar{f}(a + K) = f(a) \in \text{Im } f = S'$.

2. Is $\bar{f}$ a homomorphism?

   YES!

$$\begin{gathered}\bar{f}((a+K)+(b+K)) \\ = \bar{f}((a+b)+K) = f(a+b) = f(a) + f(b) = \bar{f}(a+K) + \bar{f}(b+K)\end{gathered}$$

   Similarly, for $\bar{f}((a+K)(b+K))$,

$$\bar{f}((ab)+K) = f(ab) = f(a) \cdot f(b) = \bar{f}(a+K)\bar{f}(b+K)$$

3. Is $\bar{f}$ surjective?

   YES! By definition we have $S' = \text{Im } f$, which means $\forall s \in S', \exists a \in R$ such that $s = f(a)$. By definition we then have $s = \bar{f}(a + K)$

4. Is $\bar{f}$ injective?

   YES! To show this, suffices to check that Ker $\bar{f} = (0)$. Indeed, $\bar{f}(a + K) = f(a)$, and so
   $$\bar{f}(a + K) = 0 \Leftrightarrow f(a) = 0 \Leftrightarrow a \in \text{Ker } f = K \Leftrightarrow a + K = 0 + K$$

   But $0 + K$ is the zero of R/K, and so Ker $\bar{f} = (0)$. Thus $\bar{f}$ is injective.

To summarize, $\bar{f} : R/K \to S'$ is a homomorphism that is both surjective and injective. Thus, $\bar{f}$ is an isomorphism, and so $R/\text{Ker } f$ is isomorphic to Im f.

This completes the proof. □

Holy aura. We just proved the first isomorphism theorem. W. Anyway, we went on to go over a summary of the previous chapters, which included concepts like

- *ideals*: principal ideals, and ideals generated by a given set of elements
- *Congruence* mod I
- Quotient ring R/I
- Homomorphisms, kernels, and images.

Some important theorems to keep in mind are

- R/I is a ring (the *quotient ring*, by definition)
- Kernels of ring homomorphisms are ideals, while images are subrings
- A ring homomorphism f is a monomorphism iff Ker $f = (0)$.
- First isomorphism theorem: $R/\text{Ker } f \cong \text{Im } f$.

21.2 Prime and maximal ideals

Recall from previous sections that if $p \in \mathbb{Z}$ is a prime and $p \mid ab$, then we must have either $p \mid a$ or $p \mid b$. This will be our guiding intuition in defining *prime* ideals.

Definition (Prime ideals)**.** Let R be a ring and $I \subset R$, $I \neq R$ be an ideal. We say that I is a **prime ideal** if $\forall a, b \in R$, $ab \in I \Rightarrow a \in I$ *or* $b \in I$.

> **Intuition.** *This is the other implication direction based on the def of ideals. Regular ideals are $a \in I$ implies $ab \in I$, but now its the other way where $ab \in I$ implies $a \in I$ (or $b \in I$ wlog).*

> *Also, having $ab \in I$ is essentially saying I "divides" ab, as in ab is a perfect multiple of the ideal I. That's why it would also imply that I "divides" a or b, making it "prime".*

As always, hit em with the examples.

Example 21.1. Check if the following ideals are prime:

(1) (0) in $\mathbb{Z}$.
Recall that $\mathbb{Z}$ is an integral domain. Hence $ab = 0 \Rightarrow a = 0$ or $b = 0$, and so $(0) \subset \mathbb{Z}$ is a prime ideal.

(2) (p) is $\mathbb{Z}$ when p is prime.
If $ab \in (p)$, then $p \mid ab$. Since p is prime, this implies that $p \mid a$ or $p \mid b$. In the former case $a \in (p)$, and in the latter case $b \in (p)$. Hence $(p) \subset \mathbb{Z}$ is a prime ideal.

22 Lecture 23: Nov. 17th

Today in lecture we talked more about special ideals that mirror integers with special properties, through the discussion of more prime ideals, and even with the introduction of maximal ideals. Within the world of ideals and cosets and things, there are definitely a lot to keep in mind and I often feel quite overwhelmed. But it's important to keep in mind that this is just another layer of abstraction– if I tried to "list up the hood" and figure out why definitions / theorems hold from first principles, I will lose my mind. This ability to just blindly trust something works because I've understood it before and can now abstract it away is something quite scary and something I need to work on.

22.1 Prime and maximal ideals (cont'd)

We began lecture with a very brief recollection of the definition of a prime ideal, and the specific intuition that it is the "ideals" counterpart of the property in $\mathbb{Z}$ where if $p \mid ab$, then $p \mid a$ or $p \mid b$. We are going to be exploring more examples today.

Example 22.1. Assume F is a field and $f(x) \in F[x]$ is an irreducible polynomial. Is $(f(x))$ a prime ideal in $F[x]$?

Recall that we've discussed if $f(x) \in F[x]$ is irreducible and $f(x) \mid g(x)h(x)$ then $f \mid g$ or $f \mid h$.

Thus $g(x)h(x) \in (f(x)) \Rightarrow g(x) \in (f(x))$ or $h(x) \in (f(x))$, and so $(f(x)) \subset F[x]$ is a prime ideal.

Do note that in general, irreducible $\neq$ prime, but we would need much more complicated rings to find examples.

Example 22.2. In $\mathbb{Z}[x]$, is (x) a prime ideal?

First note that the result from the previous example does *not* apply here, since although x is irreducible, $\mathbb{Z}$ is not a field.

But regardles of that, YES, (x) is a prime ideal. To show this, notice that $f(x)g(x) \in (x)$ if and only if $f \cdot g$ has a zero constant term. Further, the constant term of fg is a result of multiplication of the constant term of f and the constant term of g.

From here, since $\mathbb{Z}$ is an integral domain, this would directly imply that in order for their product to have a zero constant term, either f or g must have a zero constant term, thus implying existence in (x).

Through the examples thus far, we've noticed that there is some sort of connection between prime ideals and elements of integral domains. Let's use a theorem to formalize this thought.

Theorem 22.1.

Let R be a commutative ring with identity. Then an ideal $P \subset R$ is prime if and only if R/P is an integral domain.

Proof. We will approach this proof through contraposition. Since R is a commutative ring with identity, we know that R/P must also be a commutative quotient ring with identity. We now show that *P is not prime if and only if R/P has zero divisors.*

We follow the chain of biconditionals: P is **not** a prime ideal $\Leftrightarrow \exists a, b \in R$ such that $a \notin P, b \notin P$ but $ab \in P$
$\Leftrightarrow \exists a, b \in R$ such that $a + P \neq 0 + P, b + P \neq 0 + P$ but $ab + P = 0 + P$

From here, by multiplication as defined on cosets, we have $(a + P)(b + P) = (ab + P) = 0$, but since $a+P \neq 0+P, b+P \neq 0$, we've shown that they are both zero divisors of R/P. □

From here, we move on to discuss more interesting forms of ideals.

Definition (Maximal ideals)**.** We say that an ideal $I \subset R, I \neq R$ is a **maximal ideal** if for every ideal J such that $I \subseteq J \subseteq R$, either $J = I$ or $J = R$.

In other words, $I \subset R$ is maximal if there are no ideals between I and R.

As usual, let's do some examples.

Example 22.3. Check if the following ideals are maximal:

(1) Is $(6) \in \mathbb{Z}$ a maximal ideal?
No. We have $(6) \subset (3) \subset \mathbb{Z}$.

(2) More generally, for $1 < n \in \mathbb{Z}$ not a prime, is n a maximal ideal in $\mathbb{Z}$?
No. If $1 < n \in \mathbb{Z}$ is not prime, then we can represent $n = kl$ for some $1 < k, l < n$. From here we see $(n) \subset (k) \subset \mathbb{Z}$.

(3) What about (p) where $p \in \mathbb{Z}$ is a prime?
We claim that for any ideal $(p) \subsetneq J \subseteq \mathbb{Z}$, we must have $J = \mathbb{Z}$. Since $J \neq P$, J must contain some $n \in \mathbb{Z}$ where n is not an integer multiple of p. This means $\gcd(n, p) = 1$. By GCD representation, we have $an + bp = 1$ for some $a, b \in \mathbb{Z}$.

From here, since $n, p \in J$, we must then have $an+bp \in J$. Thus $1 \in J$ and hence $J = \mathbb{Z}$. □

To summarize the results of these examples, we say that in $\mathbb{Z}$, if $n \neq 0$, then (n) is a maximal ideal if and only if (n) is a prime ideal.

And with this result, it looks like maximal ideals is almost a "step up" from prime ideals. We can see that with the following theorem:

Theorem 22.2.

Assume R is a commutative ring with identity. Then $M \subset R$ is a maximal ideal if and only if R/M is a field.

Corollary 22.2.1.

In a commutative ring with identity, every maximal ideal is prime.

Proof. If M is a maximal ideal, then by the previous theorem, R/M must be a field. But all fields are integral domains, meaning R/M is an integral domain as well. From the theorem proven previously, M must be prime. □

Given this corollary is a one-directional implication, what are some potential examples to show that the converse does not hold?

Well trivially, we have that $(0) \subset \mathbb{Z}$ is a prime ideal but clearly not maximal. But this is boorriingggggg. Let's try something else. We've shown earlier that $(x) \subset \mathbb{Z}[x]$ is a prime ideal. Now consider $(x, 2)$, i.e. the set of polynomials with even constant term. We have $(x) \subsetneq (x, 2) \subsetneq \mathbb{Z}[x]$ and thus (x) is not a maximal ideal in $\mathbb{Z}[x]$.

Let's try to prove the theorem now.

Proof. ($\Rightarrow$) Let $M \subset R$ be a maximal ideal. We have to show that R/M is a field. That is, for every $a \in R \setminus M$, we must have that $(a + M)$ is a unit in R/M.

To start, let's fix our a. Now consider $J = M + (a) = \{m + ra : m \in M, r \in R\}$. Then J is an ideal (source trust me bro), $M \subseteq J$, and since $a \in R \setminus M$, we have $M \subsetneq J$.

But M is a maximal ideal, which would mean $J = R$, which means $1 \in J$. From here, by definition, we know $\exists m \in M, r \in R$ such that $1 = m + ra$. This means $1 \equiv ra \pmod{M}$, giving us

$$1 + M = ra + M = (r + M)(a + M)$$

and therefore $a + M$ is a unit in R/M. And since this results holds for all $a \in R \setminus M$, we conclude that R/M is a field.

($\Leftarrow$) Let R/M be a field. Let J be any ideal such that $M \subsetneq J \subseteq R$. We will show $J = R$, hence M is a maximal ideal.

Since $M \subsetneq J$, there exists some $a \in J \setminus M$. And since R/M is a field, we know that $a + M \neq 0 + M$ is a unit in R/M. This implies the existence of some $r \in R$ such that $(a + M)(r + M) = 1 + M$.

Then $ar + M = 1 + M$ and so $1 - ar \in M \subsetneq J$. Thus by definition we have $ar \in J$ and $1 - ar \in J$. Since J is an ideal, this implies $1 = ar + (1 - ar) \in J$, and so $J = R$. This completes the proof. □

As a summary of today's lecture, we have that if R is a commutative ring with identity, then

1. an ideal $P \subset R$ is prime if and only if R/P is an integral domain.

2. an ideal $M \subset R$ is maximal if and only if R/M is a field.
3. all maximal ideals are prime

23 Lecture 24: Nov. 19th

Very short and friendly lecture. We started off with quiz 2, which honestly I didn't think I did that well on, because I had trouble formalizing my thoughts despite having all the intuition for the problems. From there, we wrapped up our discussion on prime and maximal ideals with a final theorem regarding principal ideal domains. We ended with a brief review of complex numbers.

23.1 Prime and maximal ideals (cont'd)

Quiz 2!! AHHHHHHHH

We began lecture with a quick recollection of prime and maximal ideals. Specifically, we proved that if R is a commutative ring with identity, then

1. an ideal $P \subset R$ is prime if and only if R/P is an integral domain
2. an ideal $M \subset R$ is maximal if and only if R/M is a field
3. any maximal ideal is a prime ideal

The converse of (3), however, does not hold. But we do have a the tools now to state a new theorem:

Theorem 23.1 (Principal ideal domain).
If R is an integral domain such that all ideals in R are principal ideals, then every nonzero prime ideal in R is maximal.

Such a ring R is called a principal ideal domain.

> **Intuition.** *Integers! Every ideal in $\mathbb{Z}$ is a principal ideal, and we've shown previously that every prime ideal is maximal in $\mathbb{Z}$.*

Proof. Let $I \subset R$ be a nonzero prime ideal. Let J be *any* ideal such that $I \subseteq J \subseteq R$. We have to show that either $J = I$ or $J = R$.

Since all ideals in R are principal, $\exists p, m \in R$ such that $I = (p)$, $J = (m)$. Also, since $I \neq (0)$, $p \neq 0$.

Since $p \in (p) \subseteq (m)$, $p \in (m)$, and so $p = am$ for some $a \in R$. Since (p) is prime and $am = p \in (p)$, we conclude that either $a \in (p)$ or $m \in (p)$. So we have either $a = up$ or $m = vp$ for some $u, v \in R$.

1. If $a = up$, then we have $p = am = (up)m = (um)p$. Since R is an integral domain, we apply the cancellation property and see that $1 \cdot p = (um)p$ implies $1 = um$. Thus, m is a unit in R and hence $(m) = R$.
2. Similarly, if $m = vp$, then we have $am = avp = p$. By the cancellation property, $avp = 1 \cdot p$ implies $av = 1$. Hence a is a unit, and so $(m) = (am) = (p)$.

□

In the next lectures, we will be discussing the ring of Gaussian Integers in detail. And before that, we should have a quick refresher on complex numbers.

Recall that each complex number $z = a + bi \in \mathbb{C}$ can be represented as a vector $(a, b) \in \mathbb{R}^2$ (also called the complex plane). We define the angle formed between the vector and the positive x-axis as the **argument** of z, denoted $\arg(z)$ or φ. Further, we define the distance from the origin, the magnitude of the vector, as the **modulus** of z, denoted $|z| = \sqrt{a^2 + b^2}$.

We can represent any z as $z = |z|(\cos\varphi + i \sin\varphi)$. Here, we call $N(z) := |z|^2$ the **norm** of z. Moreover, for any $z, w \in \mathbb{C}$,

$$\begin{aligned} N(zw) &= zw \cdot \overline{zw} = (z\bar{z})(w\bar{w}) = N(z)N(w) \\ \arg(zw) &= \arg(z) + \arg(w) \end{aligned}$$

Finally, recall that multiplication of z by i represents a rotation by 90-degrees in $\mathbb{R}^2$.

24 Lecture 25: Nov. 21st

Today in lecture we discussed the gaussian integers and how it has properties very similar to $\mathbb{Z}$ and $F[x]$ which we have been discussing for the quarter. The lecture was very intuitive overall, and the proofs were beautiful. But most importantly, I feel like this is about to build up to an insane generalization regarding rings that we can do Euclidean algorithms on, which is what we've been hinting at since like week 4. Can't wait.

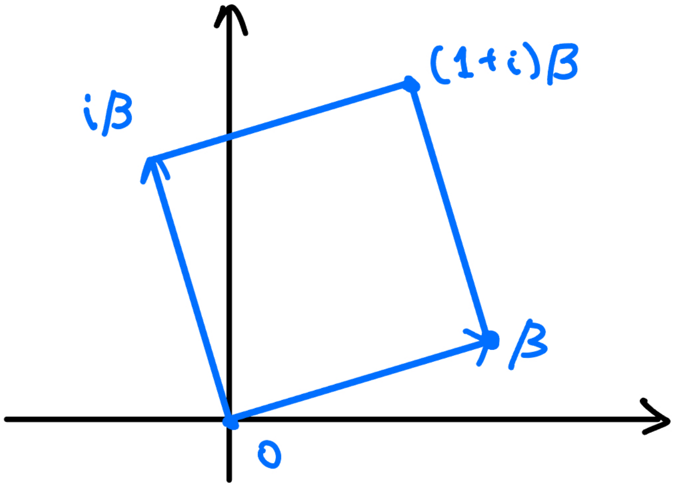
24.1 Gaussian integers $\mathbb{Z}[i]$

We began lecture with a summary of the rings $\mathbb{Z}$ and $F[x]$. Specifically, recall that both rings have unique properties that doesn't seem to carry over to other rings that we've discussed:

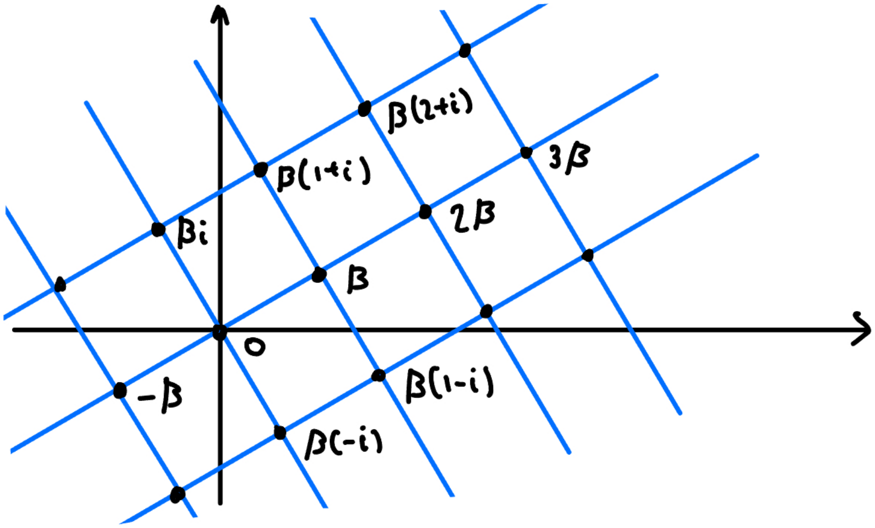
- Both rings have a notion of "division". $n = mq + r$ with $0 \leq r < |m|$ and $f(x) = g(x)q(x) + r(x)$ with $\deg r(x) < \deg g(x)$.
- Division with remainder leads to the existence of the **Euclidean algorithm** in both.
- Euclidean algorithm leads to the existence of the gcd, which is an equivalent to the fact that **all ideals of these rings are principal**.
- This leads to **unique "prime" factorization** in both rings.

Our goal this lecture is to investigate as to whether or not Gaussian integers also have similar properties. But first, recall that $\mathbb{Z}[i] := \{a + bi : a, b \in \mathbb{Z}\} \subset \mathbb{C}$. The elements of $\mathbb{Z}[i]$ are known as the **Gaussian integers**.

Gaussian integers hold the same properties as complex numbers do. Namely, multiplying by i still performs a 90 degree rotation. Moreover, similar to $\mathbb{C}$, for some $\beta \in \mathbb{Z}[i]$, we have that $0, \beta, (1+i)\beta, i\beta$ form the vertices of a square whose side length is $\sqrt{N(\beta)}$.



Inducting on this logic, for some $\beta \in \mathbb{Z}[i]$, $\beta \neq 0$, the ideal $(\beta) \subseteq \mathbb{Z}[i]$ is given by the following lattice:



Before diving into the properties of $\mathbb{Z}[i]$, let's do another round of refreshers to *really* makes sure we're all on the same page. Recall that if R is an integral domain, then

1. If $a, b \in R$ with $b \neq 0$, then we say "b divides a" or "b is a factor of a" and write $b \mid a$ if $\exists c \in R$ such that $a = bc$.
2. $a \in R$ is a **unit** if $\exists b \in R$ such that $ab = 1$.
3. $a, b \in R$ are **associates** if $\exists$ unit $u \in R$ such that $a = bu$.
4. A nonzero element $p \in R$ is **irreducible** if p is not a unit, and the only divisors of p are 0 and associates of p.

We now have a proposition.

Proposition 24.1.
$\mathbb{Z}[i]$ is an integral domain, and the units of $\mathbb{Z}[i]$ are ± 1, $\pm i$.

Proof. Let $\alpha, \beta \in \mathbb{Z}[i]$ where $\alpha, \beta \neq 0$. This would mean $N(\alpha), N(\beta) \geq 1$. Multiplying the two gives us $N(\alpha\beta) = N(\alpha)N(\beta) \geq 1$, and so $\alpha\beta \neq 0$. Since the multiplication of two nonzero elements cannot produce 0, we conclude that $\mathbb{Z}[i]$ is an integral domain.

$\pm i$, ± 1 are units since $i(-i) = 1$, $(-1)(-1) = 1$, $1 \cdot 1 = 1$.

To see that these are the only possible units, suppose there existed $\alpha, \beta \in \mathbb{Z}[i]$ where $\alpha\beta = 1$. This would mean $1 = N(\alpha\beta) = N(\alpha)N(\beta)$. Since norms are nonnegative integers, we must have $N(\alpha) = N(\beta) = 1$. The only elements for which this would hold would be $\{\pm i, \pm 1\}$, since all other elements $\gamma = c + di$ would result in $N(\gamma) = c^2 + d^2 \geq 2$. □

We've now established $\mathbb{Z}[i]$ as an integral domain and defined its units. The next thing on the bucket list is the notion of "division".

Theorem 24.2.

For all $\alpha, \beta \in \mathbb{Z}[i]$ with $\beta \neq 0$, there exists $q, r \in \mathbb{Z}[i]$ such that $\alpha = \beta q + r$ and $N(r) \leq \frac{1}{2}N(\beta)$ (and consequently, $N(r) < N(\beta)$.

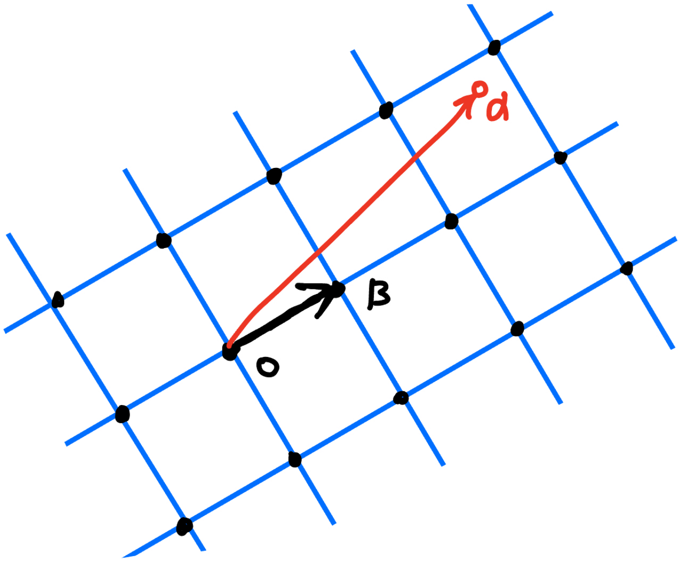
Remark. q and r are not unique, but we can still perform the Euclidean algorithm!

As a consequence of this theorem, we now unlocked a bunch more properties!

- All ideals are principal ideals (known as "square lattices"). The same proof as for $\mathbb{Z}$ and $F[x]$
- The "fundamental theorem of arithmetic" holds. That is, there exists a unique factorization property for $\mathbb{Z}[i]$
- Irreducible elements form prime ideals.

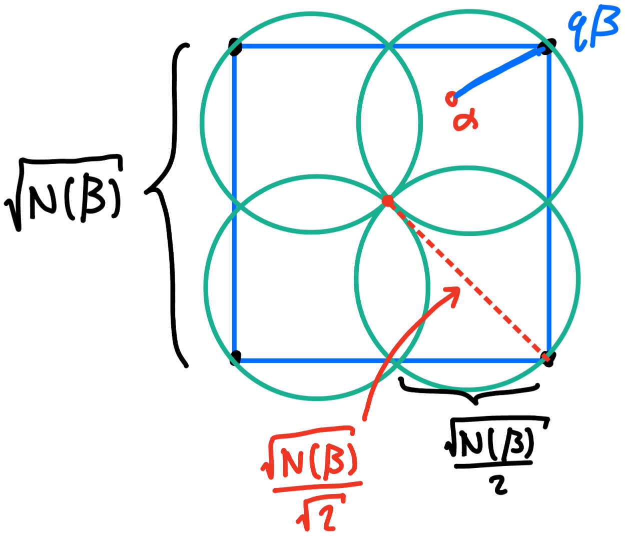
As a note, irreducible elements in $\mathbb{Z}[i]$ are referred to as **Gaussian primes**. Let's prove this theorem!

Proof. To begin, consider the lattice formed by (β). Each square within the lattice has side length $\sqrt{N(\beta)}$. Place α within the lattice. It should fall within some square.



The vertices of that square should be multiples of β. We will now show that the distance between α and the closest lattice point must be $\leq \sqrt{N(\beta)}/\sqrt{2}$.

Zooming into the square within the lattice that contains α. Notice that the distance between any lattice point to the center of that square must be exactly $\sqrt{N(\beta)}/\sqrt{2}$. This is because we can treat that distance as the hypotenuse of some right triangle with side lengths $\sqrt{N(\beta)}/2)$, then the distance follows from the Pythagorean theorem.



$q\beta$
α
$\sqrt{N(\beta)}$
$\frac{\sqrt{N(\beta)}}{\sqrt{2}}$
$\frac{\sqrt{N(\beta)}}{2}$

This means that the distance from α to the closest lattice point must be $\leq \sqrt{N(\beta)}/\sqrt{2}$. Since the lattice point some multiple $q\beta$, we can represent the distance between it and α as $r = \alpha - q\beta$.

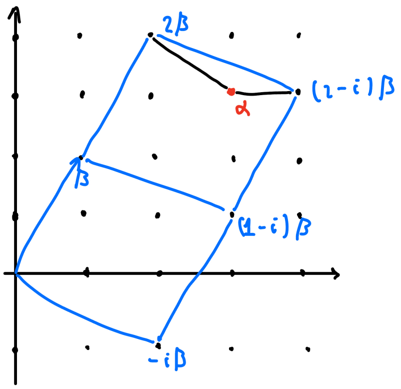
Then $\alpha = q\beta + r$ and $\sqrt{N(r)} = |\alpha - q\beta| \leq \sqrt{N(\beta)}/\sqrt{2}$, so $N(r) \leq N(\beta)/2 < N(\beta)$. □

(self remark: bro this proof is deadass so beautiful wtf! like how did we prove something about division with geometry and Pythagorean theorem and distances)

I think it's time for some examples to really solidify our understanding!

Example 24.1. Find a generator for the ideal (α, β) in $\mathbb{Z}[i]$, where $\alpha = 3 + 3i$, $\beta = 1 + 2i$.

To do this, we need to use the Euclidean algorithm to find $\gcd(\alpha, \beta)$. As our first step, we need to find $\alpha = q\beta + r$ where $N(r) < N(\beta)$. Let's do this by picture. Draw a lattice formed by β and place α within it.



We see that

$$\alpha = 3 + 3i = (2-i)(1+2i) - 1 = (2-i)\beta - 1$$

So our remainder is -1. But since -1 is a unit, we conclude that $(\alpha, \beta) = (-1) = (1) = \mathbb{Z}[i]$.

What happens if it's infeasible for us to draw a diagram? I'm legit getting tired of drawing diagrams lol.

Example 24.2. Let $\alpha = 12 + 5i$ and $\beta = 7 + 4i$. Find a generator of (α, β).

We need to find q, r such that $\alpha = q\beta + r$. It is quite infeasible for us to draw a huge lattice this time, so let's divide and guess-timate. We have

$$\frac{12+5i}{7+4i} = \frac{(12+5i)(7-4i)}{(7+4i)(7-4i)} = \frac{(84+20)+(35-48)i}{65} = \frac{104-13i}{65}$$

This quotient is obviously not a Gaussian integer. But the closest Gaussian integer seems to be 2, so we can try $q = 2$. This give us $r = (12+5i) - 2(7+4i) = -(2+3i)$, and since $N(r) < N(\beta)$, this is a valid choice.

From here, we divide again and see that

$$\frac{7+4i}{2+3i} = \frac{26-13i}{13} = 2 - i$$

Which means the $7 + 4i = (2+3i)(2-i) + 0$. This gives us $\gcd(12+5i, 7+4i) = 2 + 3i$ or any associate of $2 + 3i$. Hence $(\alpha, \beta) = (2+3i) \subset \mathbb{Z}[i]$.

25 Lecture 26: Nov. 24th

Today in lecture we wrapped up the discussion regarding Gaussian integers with the Gaussian primes. Definitely a little bit confusing, but it's interesting to see how the idea of "irreducibility" carries over to complex elements. We then finally began discussing the grand generalization of the class: what makes a set have division, factorization, and integer-esque properties.

25.1 Gaussian Primes

To begin lecture, we did a brief recollection of the work that we've done together on the Gaussian integers. Recall that Gaussian integers refers to the set $\mathbb{Z}[i]$ defined as $\{a + bi : a, b \in \mathbb{Z}\}$. Further, we defined the *norm* of a Gaussian integer to be $N(a + bi) := a^2 + b^2$.

Lastly, we also proved a theorem regarding division with remainder in the Gaussian integers. Specifically, there exists q, r such that $\alpha = \beta q + r$ and $N(r) \leq \frac{1}{2}N(\beta) < N(\beta)$. This brought us a couple useful corollaries, namely, the ability to use the Euclidean Algorithm, which allows us to conclude that

- all ideals of $\mathbb{Z}[i]$ are principal
- The fundamental theorem of arithmetic holds in $\mathbb{Z}[i]$: there always exists a unique factorization of irreducibles.

Today, we will explore what exactly makes a Gaussian integer "irreducible"? What are these numbers that we refer to as *Gaussian primes*?

To begin our conversation, recall that the (only) units in $\mathbb{Z}[i]$ are $\pm 1, \pm i$. We now make the following proposition:

Proposition 25.1.

(1) If $c \in \mathbb{Z} \setminus 0, a + bi \in \mathbb{Z}[i]$, then $c \mid a + bi$ if and only if $c \mid a$ and $c \mid b$.

(2) Let $\alpha, \beta \in \mathbb{Z}[i]$ with $\beta \neq 0$. If $\beta \mid \alpha$, then $N(\beta) \mid N(\alpha)$.

Proof. (1) is relatively trivial and left as an exercise for the reader.

(2) If $\beta \mid \alpha$, then there exists $\gamma \in \mathbb{Z}[i]$ such that $\alpha = \beta\gamma$. This means $N(\alpha) = N(\beta\gamma) = N(\beta)N(\gamma)$. But since both $N(\beta)$ and $N(\gamma)$ are integers, we conclude that $N(\beta) \mid N(\alpha)$. □

Remark. The converse of (2) does *not* hold! For instance, consider $\beta = 2 - i$ and $\alpha = 1 + 3i$. This gives us $N(\alpha) = 10$ and $N(\beta) = 5$. It is clear that $5 \mid 10$. However, α is not divisible by β because

$$\frac{1 + 3i}{2 - i} = \frac{(1 + 3i)(2 + i)}{5} = \frac{-1 + 7i}{5} = -\frac{1}{5} + \frac{7}{5}i \notin \mathbb{Z}[i]$$

In general, the norm is too crude of an invariant to hope for the converse of a statement like this; two Gaussian integers can have the same norm but not be associates of each other.

But regardless, this proposition gives way for a very powerful corollary.

Corollary 25.1.1.

If $\alpha \in \mathbb{Z}[i]$ is such that $N(\alpha)$ is a prime integer, then α is a Gaussian prime.

Example 25.1. Both $2+i$ and $2-i$ are Gaussian primes. So are $1+i$ and $1-i$, but these two are associates of each other.

This implies $5 = (2+i)(2-i)$ is the prime decomposition of 5. Similarly, $2 = (1+i)(1-i) = -i(1+i)(1+i)$ is the prime decomposition of 2. Note that these two are both prime decompositions of 2 since $-i$ is a unit. Additionally, recall that this doesn't violate the "uniqueness" criterion since we say decompositions with respect to associates are the same.

Based on all that we've covered so far regarding Gaussian primes, let's make a wacky claim (and surprise ourselves).

Claim. If $p \in \mathbb{Z}_{>0}$ is a prime and $p \equiv 3 \pmod 4$, then p is also a Gaussian prime.

Proof. For some $a \in \mathbb{Z}$ in mod 4, the only possible remainders of a^2 are

$$0^2 \equiv 0 \pmod 4 \qquad (\pm 1)^2 \equiv 1 \pmod 4 \qquad 2^2 \equiv 0 \pmod 4$$

So, if $z = a + bi$, then $N(z) = a^2 + b^2 \equiv 0, 1, 2 \text{ mod } 4$, but **never 3 mod 4**. This means that there are no $z \in \mathbb{Z}[i]$ that has norm p.

With this fact in mind, suppose that p wasn't a Gaussian prime and $p = \alpha\gamma$. Then, we'd have $p^2 = N(\alpha)N(\gamma)$. Neither $N(\alpha)$ nor $N(\gamma)$ can be p, as we've just discovered.

So then one of $N(\alpha), N(\gamma)$ must be 1, and the other must be p^2. Wlog suppose $N(\alpha) = 1$. This would mean that α is a unit, making γ an associate of p. We conclude that p must be a Gaussian prime, since its only possible divisors are units or associates of itself. □

Woah that's kinda neat. A strange property of squares mod 4 carried over to the world of Gaussian integers. Let's continue.

Theorem 25.2.

Let $p \in \mathbb{Z}_{>0}$ be a prime integer such that $p \equiv 1 \pmod 4$. Then $\exists a, b \in \mathbb{Z}$ such that $a^2 + b^2 = p$. Consequently, $p = (a+bi)(a-bi)$.

Note that this would imply p is *not* a Gaussian prime. However, since $a \pm bi$ both have norm p, it would make the both of them Gaussian primes.

Also note that I am lazy (and there are many much proofs out there) so I will skip this proof. Left as an exercise for the reader!!

As a summary of Gaussian primes, we have

- If $p = 2$ or $p \in \mathbb{Z}_{>0}$ is a prime such that $p \equiv 1 \pmod 4$, then there exists Gaussian integers with norm p. All of them are Gaussian primes.
- Each prime integer $p \equiv 3 \pmod 4$ is a Gaussian prime (and so are all of its associates)
- Furthermore, **there are no other Gaussian primes**. (We will skip the proof for this also, but I will give a brief intuition)

  Intuition. *As for a quick intuition for that last point, notice that for any Gaussian integer z, we have $N(z) = z \cdot \bar{z}$. This means that $z \mid N(z)$ for all Gaussian integers. Now, if $N(z)$ is weird, then z is its own norm. Otherwise, the norm can be split into different Gaussian integers (i.e., not prime).*

  The underlying rule is that primality in Gaussian integers are connected to primality in the integers. There are no "alien" Gaussian integers that are disconnected from the primes that we know and love.

25.2 Euclidean domains and Principal ideal domains

As we wrap up our discussion regarding Gaussian integers, we should notice that much of the time we've spent discussing different algebraic sets this quarter all revolved around the same properties (that we've even hinted at as early as lecture 10): the ability for us to perform the Euclidean Algorithm on elements of these algebraic sets.

So now, finally at last, we generalize these types of sets with the following definition.

Definition (Euclidean domains & PIDs)**.** Let R be an integral domain. We say that

1. R is an **Euclidean Domain** if there exists a function $\delta : R \setminus \{0\} \to \mathbb{Z}_{\geq 0}$ such that:
   (a) $\delta(a) \leq \delta(ab)$ for all nonzero a and b in R, and
   (b) $\forall a, b \in R$ with $b \neq 0$, we can represent a as $a = bq + r$ for some $q, r \in R$ where $r = 0$ or $\delta(r) < \delta(b)$

   Intuition. *The δ function just represents the way we measure the "size" of an element in an Euclidean domain. In integers, it would be absolute value. In $F[x]$, it would be degree of polynomial. And most recently, in $\mathbb{Z}[i]$, it would be the norm.*

2. R is a **Principal Ideal Domain** if all ideals of R are principal ideals: $I = (a)$ for $a \in R$.

Example 25.2. A bit of a silly example, but if F is a field, we can take $\delta : F \setminus \{0\} \to \mathbb{Z}_{>0}$ as the constant zero function, which allows us to convert every field to a Euclidean domain.

We can do this by taking advantage of the field property in which every element is invertible, giving us $a = (a \cdot b^{-1})b + r$ where $r = 0$ is satisfied every time.

It should now be clear that there definitely exists some "subset-ish" relationships between the big players in fields, Euclidean domains, PIDs, and integral domains. Let's explore this thought.

Theorem 25.3.

Every Euclidean domain is a principal ideal domain.

Proof. Assume R is an Euclidean domain. We will now show that all ideals $I \subseteq R$ must be principal ideals.

Trivially, if $I = (0)$, we are done. We now consider the case in which $I \neq (0)$. Let a be a nonzero element of I with the smallest $\delta(a)$. Since $a \in I \setminus \{0\}$, by definition, we have $(a) \subseteq I$.

Conversely, let $b \in I$. Since R is an Euclidean domain, $\exists q, r \in R$ such that $b = aq + r$ with either $r = 0$ or $\delta(r) < \delta(a)$. By closure of subtraction on ideals, we know $r = b - aq \in I$.

From here, since $\delta(a)$ is smallest in I and $r \in I$, we have to have $r = 0$, meaning $b = aq$. This implies $b \in (a) \forall b \in I$, hence $I \subseteq (a)$. We conclude that $I = (a)$. □

26 Lecture 27: Dec. 1st

Today's lecture was short and sweet, and it covered the rest of the content within this course. Towards the end, I definitely did get a bit confused as I think I haven't been able to completely grasp the ideal of a PID yet (where all ideals are principal). I did love the build-up up to this point throughout the quarter, building intuition with x and $F[x]$ and ultimately Euclidean domains and what it means to be factorable and divisible.

26.1 ED, PID, UFD

We began our last content lecture with a review of the definition of an Euclidean Domain. Essentially, Euclidean domains are integral domains where there is a natural measurement of magnitude as defined by $\delta : R \setminus \{0\} \to \mathbb{Z}_{\geq 0}$. And as an effect, division with remainder, where elements a can be represented as $a = bq + r$ for $b, q, r \in R$, is well-defined on these sets.

We also recalled the definition of a *different* type of domain called the Principal ideal domain, which is an integral domain R where all ideals are principal. From there, we proved that every Euclidean domain is a PID.

Remark. The converse of that statement does not hold- that is, *not* every PID is an Euclidean domain (albeit counter examples are difficult to come by)

We then went on to establish the final definition of the course.

Definition (Unique Factorization Domain)**.** An integral domain is called a **Unique Factorization Domain** (UFD) if $\forall a \in R$ such that $a \neq 0$ and a is not a unit, $\exists!$ expression of a as $a = p_1 p_2 \cdots p_r$, where p_i's are irreducible.

Uniqueness implies that if $p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_m$, then $r = m$ and after reordering the elements, $q_i = u_i p_i$ where u_i is a unit in R.

This brings us to the final couple of theorems as well.

Theorem 26.1.

Every principal ideal domain is a unique factorization domain.

The converse of this statement does not hold. that is, not every UFD is a PID.

Theorem 26.2.

If R is a unique factorization domain, then so is $R[x]$.

We can now see *why* the converse of **Theorem 26.1** does not hold. Consider $\mathbb{Z}[x]$. Since $\mathbb{Z}$ is a UFD, we know that $\mathbb{Z}[x]$ must also be a UFD. However, as discussed previously, $(x, 2)$ is not a principal ideal.

Similarly, perhaps more interestingly, $F[x, y] = (F[x])[y]$ where F is a field, is also a UFD but not a PID; the ideal (x, y) is not principal.

Furthermore, not every integral domain is a UFD, that is, not every integral domain will have a unique factorization of elements. For instance, $\mathbb{Z}[\sqrt{5}]$ is not a UFD, because the element $6 = 2 \cdot 3 = (1 + \sqrt{5})(1 - \sqrt{5})$ clearly has two different factorizations of *unique elements*.

As a final remark, we explored the superset / subset properties of all of these domains that we've explored.

$$\text{Integral domains} \supseteq \text{UFD} \supseteq \text{PID} \supseteq \text{ED} \supseteq \text{Fields}$$

and this "nested-doll" relationship is actually quite cool! We can really see how properties get stacked on top of each other until we've reached a field:

1. Integral domains: no zero divisor elements
2. UFD: elements have unique factorizations
3. PID: all ideals are principal
4. ED: division algorithm exists
5. Field: all elements are invertible

27 Afterwords

This was a very cool class, I enjoyed it. It's cool how the entire course was really just revolved around 3 main sets: $\mathbb{Z}$, $F[x]$, and $\mathbb{Z}[i]$.

We started off in the world of analytic number theory, working strictly over the integers $\mathbb{Z}$ (everything was so nice back then...), and analyzing all of these properties that we thought were *so unique* belonging to the integers, like Euclidean algorithm, unique factorization, modular arithmetic, etc.

We then introduced the concept of a "Ring", and used ring definitions as a stepping stone to start exploring other sets with interesting properties. This is where we dove into algebraic number theory and introduced polynomial rings.

We quickly realized that when F is a field, then $F[x]$ had a TON of similar properties as compared to $\mathbb{Z}$. All those integer properties that we thought were unique and special, were not anymore. We began to conjecture that maybe there are other rings out there that *also* holds these unique properties...

But we were quite young and naive, and there was still much to learn before we make that big leap of generalization. This is, imo, where the content of the course started getting a little fked.

We really began to explore the "abstract" part of abstract algebra. Rather than working with concretely defined sets, we started working with ideals, congruence classes, isomorphisms, kernels, images, and all of these objects that could be generalized over so many different sets / rings. This all built up to the First Isomorphism Theorem, an incredibly powerful tool that allows us to analyze and construct relationships between different rings.

This is all to build up to the final point of the class, where we went back to the good old ways and started exploring another concrete set: the ring of Gaussian Integers $\mathbb{Z}[i]$. We quickly realized that $\mathbb{Z}[i]$ held much of the same properties as $\mathbb{Z}$ and $F[x]$.

But we are now much less naive than before, and can finally attempt that generalization that we talked about early on in the course. Using the knowledge and tools that we have now though the abstraction process, we were able to define what it means for a set to be one of (1) Euclidean domain, (2) Principal ideal domain, or (3) Unique factorization domain. These three domains are ultimately what determines the interesting properties that all three sets $\mathbb{Z}$, $F[x]$, $\mathbb{Z}[i]$ (amongst many others out there) held.

Below is a (non-exhaustive) list of topics covered by this course:

1. The Euclidean division algorithm for $\mathbb{Z}$, $F[x]$ and $\mathbb{Z}[i]$
2. **Theorem.** If $a, b \in \mathbb{Z}$ and $d = \gcd(a, b)$. Then there exists $x, y \in \mathbb{Z}$ such that $ax + by = d$. (Same result holds for $F[x]$ and $\mathbb{Z}[i]$)

3. The fundamental theorem of arithmetic for $\mathbb{Z}$, $F[x]$, $\mathbb{Z}[i]$
4. **Theorem.** Let $p \in \mathbb{Z}$ be a prime, then $\mathbb{Z}_p$ is a field. In other words, $\forall a \in \mathbb{Z}$ where p does not divide a, the congruence class $[a] \in \mathbb{Z}_p$ is invertible. (Same result holds for $F[x]$)
5. Every finite integral domain is a field
6. The units in $\mathbb{Z}$ are ± 1, the units in $F[x]$ are $F \setminus 0$, and the units in $\mathbb{Z}[i]$ are $\pm 1, \pm i$
7. **Theorem.** a is a root of $f(x) \in F[x]$ if and only if $x - a \mid f(x)$

   The next 4 items relate to polynomials in $\mathbb{Q}$.
8. Rational roots test. In particular, any rational root of a monic polynomial where coefficients are integers must also be an integer
9. Eisenstein's criterion
10. Gauss' lemma
11. Mod p criterion for irreducibility of polynomials
12. Every odd-degree polynomial in $\mathbb{R}[x]$ has a real root
13. Let F be a field and $p(x)$ be a nonconstant polynomial in $F[x]$. Then $\gcd(f(x), p(x)) = 1$ if and only if $f(x) + (p(x))$ is a unit in $F[x]/(p(x))$
14. Extensions of fields and roots of polynomials
15. First isomorphism theorem
16. Chinese remainder theorem
17. Characterization of prime and maximal ideals in commutative rings with identity in terms of quotients