Lecture Last
Unique Factorization Domains
and Factoring Polynomials
Big problems beget big movements in math

Number theory's historically big problems:

- How many primes? How many primes of certain forms? What is their density?
- Can we find integer solutions to certain polynomial equations?

Fermat's last theorem: for which $n$ does $x^n + y^n = z^n$ have integer solutions?

This got us principal ideal domains, prime ideals, and some other great ring theory.

Algebra's big problem: When do polynomials factor?

The fundamental theorem of algebra: Every polynomial $f(x) = \sum_{i=0}^{n} a_i x^i$ of degree $n$ has precisely $n$ roots in $\mathbb{C}$ and therefore factors into $n$ degree-one polynomials.

Is there a smaller field where everything in $\mathbb{Z}[x]$ factors? What about $\mathbb{Q}[x]$? If polynomials don't factor, how close can we get?
Big problems beget big movements in math

Number theory’s historically big problems:

- How many primes? How many primes of certain forms? What is their density?
- Can we find integer solutions to certain polynomial equations?
  - Fermat's last theorem: for which \( n \) does \( x^n + y^n = z^n \) have integer solutions?

This got us principal ideal domains, prime ideals, and some other great ring theory.

Algebra's big problem:
- When do polynomial equations factor?
  - The fundamental theorem of algebra: Every polynomial of degree \( n \) has precisely \( n \) roots in \( \mathbb{C} \) and therefore factors into \( n \) degree-one polynomials.

Is there a smaller field where everything in \( \mathbb{Z} \) factors? What about \( \mathbb{Q} \)? If polynomials don't factor, how close can we get?
Big problems beget big movements in math

Number theory’s historically big problems:

(*) How many primes? How many primes of certain forms? What is their density?
Big problems beget big movements in math

Number theory’s historically big problems:

(*) How many primes? How many primes of certain forms? What is their density?

(*) Can we find integer solution to certain polynomial equations?

   *Fermat’s last theorem:* for which $n$ does
   $x^n + y^n = z^n$ have integer solutions?
Big problems beget big movements in math

Number theory’s historically big problems:

(*) How many primes? How many primes of certain forms? What is their density?

(*) Can we find integer solution to certain polynomial equations?

\[ x^n + y^n = z^n \]  

*Fermat’s last theorem: for which \( n \) does \( x^n + y^n = z^n \) have integer solutions?*

This got us principal ideal domains, prime ideals, and some other great ring theory.

Algebra’s big problem:

When do polynomial factor?
Big problems beget big movements in math

Number theory’s historically big problems:

(*) How many primes? How many primes of certain forms? What is their density?

(* ) Can we find integer solution to certain polynomial equations?

Fermat’s last theorem: for which \( n \) does
\[
x^n + y^n = z^n
\]
have integer solutions?

This got us principal ideal domains, prime ideals, and some other great ring theory.

Algebra’s big problem:

When do polynomial factor?

The fundamental theorem of algebra:

Every polynomial \( f(x) \in \mathbb{C}[x] \) of degree \( n \) has precisely \( n \) roots in \( \mathbb{C} \) and therefore factors into \( n \) degree-one polynomials.
Big problems beget big movements in math

Number theory’s historically big problems:

(*) How many primes? How many primes of certain forms? What is their density?

(*) Can we find integer solution to certain polynomial equations?

*Fermat’s last theorem: for which \( n \) does \( x^n + y^n = z^n \) have integer solutions?

This got us principal ideal domains, prime ideals, and some other great ring theory.

Algebra’s big problem:

When do polynomial factor?

*The fundamental theorem of algebra:

Every polynomial \( f(x) \in \mathbb{C}[x] \) of degree \( n \) has precisely \( n \) roots in \( \mathbb{C} \) and therefore factors into \( n \) degree-one polynomials.

Is there a smaller field where everything in \( \mathbb{Z}[x] \) factors? What about \( \mathbb{Q}[x] \)? If polynomials don’t factor, how close can we get?
Definition

Let $R$ be an integral domain.

1. Suppose $r \in R$ is non-zero and not a unit. Then $r$ is irreducible in $R$ if for $r = ab$ with $a, b \in R$, either $a$ or $b$ is a unit in $R$. Otherwise, $r$ is reducible.

2. The non-zero element $p \in R$ is prime in $R$ if the ideal $(p)$ is a prime ideal. Equivalently, $p$ is prime if for $p|ab$ with $a, b \in R$, either $p|a$ or $p|b$.

3. Let $a, b \in R$ and $u \in R^\times$ such that $a = ub$. We say $a$ and $b$ are associate in $R$. 

Proposition

In an integral domain, a prime element is always irreducible.

Proposition

In a PID a nonzero element is prime if and only if it is irreducible.
Definition
Let $R$ be an integral domain.

1. Suppose $r \in R$ is non-zero and not a unit. Then $r$ is **irreducible** in $R$ if for $r = ab$ with $a, b \in R$, either $a$ or $b$ is a unit in $R$. Otherwise, $r$ is **reducible**.

2. The non-zero element $p \in R$ is **prime** in $R$ if the ideal $(p)$ is a prime ideal. Equivalently, $p$ is prime if for $p|ab$ with $a, b \in R$, either $p|a$ or $p|b$.

3. Let $a, b \in R$ and $u \in R^\times$ such that $a = ub$. We say $a$ and $b$ are **associate** in $R$.

Proposition

*In an integral domain, a prime element is always irreducible.*
Definition
Let $R$ be an integral domain.

1. Suppose $r \in R$ is non-zero and not a unit. Then $r$ is **irreducible** in $R$ if for $r = ab$ with $a, b \in R$, either $a$ or $b$ is a unit in $R$. Otherwise, $r$ is **reducible**.

2. The non-zero element $p \in R$ is **prime** in $R$ if the ideal $(p)$ is a prime ideal. Equivalently, $p$ is prime if for $p|ab$ with $a, b \in R$, either $p|a$ or $p|b$.

3. Let $a, b \in R$ and $u \in R^\times$ such that $a = ub$. We say $a$ and $b$ are **associate** in $R$.

Proposition
*In an integral domain, a prime element is always irreducible.*

Proposition
*In a PID a nonzero element is prime if and only if it is irreducible.*
Definition
An Unique Factorization Domain (U.F.D.) is an integral domain $R$ in which every $r \in R$ that is not a unit has the properties

1. $r$ can be written as a finite product of irreducibles $p_i$ in $R$ (not necessarily distinct): $r = p_1 p_2 \ldots p_n$

2. The decomposition above is unique up to associates, i.e. if $r = q_1 \ldots q_m$, then $m = n$ and there is a reordering of the factors such that $q_i$ and $p_i$ are associate in $R$ for all $i$. 
Proposition

In a Unique Factorization Domain, a nonzero element is a prime if and only if it is irreducible.
Proposition

In a Unique Factorization Domain, a nonzero element is a prime if and only if it is irreducible.

Proposition

Let $a$ and $b$ be nonzero elements of the Unique Factorization Domain $R$ with prime factorizations

$$a = u p_1^{e_1} p_2^{e_2} \ldots p_n^{e_n} \quad \text{and} \quad b = v p_1^{f_1} p_2^{f_2} \ldots p_n^{f_n}$$

such that $u, v \in R^\times$, the prime $p_1, p_2, \ldots, p_n$ are distinct and $e_i, f_i \geq 0$. Then

$$d = p_1^{\min(e_1,f_1)} p_2^{\min(e_2,f_2)} \ldots p_n^{\min(e_n,f_n)}$$

is the greatest common divisor of $a$ and $b$. 
Theorem
Every PID is a UFD. In particular, every Euclidean Domain is a UFD.
Theorem
Every PID is a UFD. In particular, every Euclidean Domain is a UFD.

Fundamental Theorem of Arithmetic
The integers \( \mathbb{Z} \) are a Unique Factorization Domain.
Polynomials

Recall:

1. If $p, q \in R[x]$, then $\deg pq = \deg p + \deg q$.
2. The units of $R$ are exactly the units of $R[x]$.
3. If $R$ is an integral domain, then so is $R[x]$.
4. $R[x]$ is a Euclidean domain if and only if $R$ is a field.
Polynomials

Recall:
1. If \( p, q \in R[x] \), then \( \deg pq = \deg p + \deg q \).
2. The units of \( R \) are exactly the units of \( R[x] \).
3. If \( R \) is an integral domain, then so is \( R[x] \).
4. \( R[x] \) is a Euclidean domain if and only if \( R \) is a field.

Theorem
(Ideals of \( R \) pass naturally to ideals of \( R[x] \))
If \( I \) is an ideal of \( R \) and \( (I) \) is the ideal of \( R[x] \) gen’d by \( I \), then
1. \( (I) \) is the set of polynomials in \( x \) with coefficients in \( I \);
2. \( R[x]/(I) \cong (R/I)[x] \);
3. If \( I \) is prime in \( R \) then \( (I) \) is prime in \( R \).
When does a polynomial factor?

**Gauss’s lemma**

Let $R$ be a UFD and $F$ its field of fractions. Then if $p(x) \in R[x]$ is reducible in $F[x]$, then $p(x)$ is reducible in $R[x]$.

**Proof:** factor in $F[x]$ and then move the denominators around.

**Example:** $R = \mathbb{Z}$, $F = \mathbb{Q}$. If $p(x) \in \mathbb{Z}[x]$ factors in $\mathbb{Q}(x)$, then it factors in $\mathbb{Z}[x]$. 
When does a polynomial factor?

**Gauss’s lemma**
Let $R$ be a UFD and $F$ its field of fractions. Then if $p(x) \in R[x]$ is reducible in $F[x]$, then $p(x)$ is reducible in $R[x]$.

**Proof:** factor in $F[x]$ and then move the denominators around.

**Example:** $R = \mathbb{Z}$, $F = \mathbb{Q}$. If $p(x) \in \mathbb{Z}[x]$ factors in $\mathbb{Q}(x)$, then it factors in $\mathbb{Z}[x]$. **Careful:** $2x$ is reducible in $\mathbb{Z}[x]$ but not in $\mathbb{Q}[x]$. 
When does a polynomial factor?

Gauss’s lemma
Let $R$ be a UFD and $F$ its field of fractions. Then if $p(x) \in R[x]$ is reducible in $F[x]$, then $p(x)$ is reducible in $R[x]$.

Proof: factor in $F[x]$ and then move the denominators around.

Example: $R = \mathbb{Z}$, $F = \mathbb{Q}$. If $p(x) \in \mathbb{Z}[x]$ factors in $\mathbb{Q}(x)$, then it factors in $\mathbb{Z}[x]$. Careful: $2x$ is reducible in $\mathbb{Z}[x]$ but not in $\mathbb{Q}[x]$.

Corollary
If a gcd of the coefficients of $p(x) \in R[x]$ is 1, then $p(x)$ is irreducible in $R[x]$ if and only if it is irreducible in $F[x]$. 
When does a polynomial factor?

Gauss’s lemma
Let \( R \) be a UFD and \( F \) its field of fractions. Then if \( p(x) \in R[x] \) is reducible in \( F[x] \), then \( p(x) \) is reducible in \( R[x] \).

Proof: factor in \( F[x] \) and then move the denominators around.

Example: \( R = \mathbb{Z} \), \( F = \mathbb{Q} \). If \( p(x) \in \mathbb{Z}[x] \) factors in \( \mathbb{Q}(x) \), then it factors in \( \mathbb{Z}[x] \). Careful: \( 2x \) is reducible in \( \mathbb{Z}[x] \) but not in \( \mathbb{Q}[x] \).

Corollary
If a gcd of the coefficients of \( p(x) \in R[x] \) is 1, then \( p(x) \) is irreducible in \( R[x] \) if and only if it is irreducible in \( F[x] \).

Theorem
\( R \) is a UFD if and only if \( R[x] \) is a UFD if and only if \( R[x_1, \ldots, x_n] \) is a UFD.
Finally: picking away at factorization

Proposition

If $F$ is a field and $p \in F[x]$. Then $p(x)$ has a factor of degree one if and only if $p(f) = 0$ for some $f \in F$. 
Finally: picking away at factorization

**Proposition**

If $F$ is a field and $p \in F[x]$. Then $p(x)$ has a factor of degree one if and only if $p(f) = 0$ for some $f \in F$.

**Proposition**

A polynomial of degree 2 or 3 over a field $F$ is reducible if and only if it has a root in $F$. 
Finally: picking away at factorization

Proposition

If $F$ is a field and $p \in F[x]$. Then $p(x)$ has a factor of degree one if and only if $p(f) = 0$ for some $f \in F$.

Proposition

A polynomial of degree 2 or 3 over a field $F$ is reducible if and only if it has a root in $F$.

Eisenstein’s Criterion

Let $P$ be a prime ideal in a domain $R$ and let

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

be a polynomial in $R[x]$. If $a_i \in P$ for all $i$ and $a_0 \notin P^2$, then $f(x)$ is irreducible in $R[x]$. 