Last time, introduced more notation.

Given a ring $R$ and a set $S$,

$$(S) = \langle S \rangle,$$ the ideal generated by $S$

**Proved:** Every Euclidean domain is a PID

For a commutative ring $R$,

- $x \in R$ is irreducible if $x \neq 0$, $x$ is not a unit and $x = ab$ implies $a$ or $b$ are units.
- $p \in R$ is prime if $p \neq 0$ and $(p) \subseteq R$ is a prime ideal.

This translates into: $p \mid (ab) \Rightarrow p \mid a$ or $p \mid b$.

Note: Nobody seems to think that $0$ is prime.

(However, $0 = \langle 0 \rangle$ is a prime ideal.)

**We proved:** In an integral domain primes are irreducible.

But the converse is false:

$\mathbb{Z}[\sqrt{5}]$ is an integral domain, $2 \in \mathbb{Z}[\sqrt{5}]$ is irreducible but not prime: $2 \nmid (1 + \sqrt{5})(1 - \sqrt{5})$ but $2 \mid (1 + \sqrt{5})$.

We also proved:
- Euclidean domains are PID’s.
- In a PID, irreducible $\iff$ prime

Moreover, $x$ irreducible/prime $\iff (x)$ is maximal.

**Definition:** Let $R$ be a commutative ring. $x, y \in R$ are associated if there is a unit $u \in R$ so that $x = uy$ (and $y = u^{-1}x$).

**Lemma 29.1:** Let $R$ be an integral domain, $x, y \in R$, $x, y \neq 0$. Then $x \mid y$ and $y \mid x \iff x$ and $y$ are associated.
Proof \((\Leftarrow)\) not much to prove.
\((\Rightarrow)\). Suppose \(x|y\) and \(y|x\). Then \(\exists u, v \in R\) so that
\[ y = ux \quad \text{and} \quad x = vy. \]
\[ y = (uv)y \Rightarrow y(1-uv) = 0 \Rightarrow 1-uv = 0 \quad \text{since} \ y \neq 0 \]
and \(R\) is an integral domain. \(\Rightarrow\) \(uv = 1\), i.e. \(u, v\) are units. \(\Box\)

Remark: Recall that: \((x) \subseteq (y) \iff x \in y\) for some \(q \in R\).
Therefore, \(x, y \neq 0\) and \((x) \subseteq (y) \iff (y) \cap x \subseteq x|y, y\)
\[ \Rightarrow x \& y \text{ are associates.} \]

Definition: An integral domain \(R\) is a unique factorization domain (UFD) if

(i) Every \(r \in R\), \(r \neq 0\), \(r\) not a unit in a product of irreducibles

(ii) If \(u p_1 \cdots p_m = v q_1 \cdots q_n\), \(u, v\) units, \(p_i, q_i\) irreducibles,

Then \(n = m\) and \(2 \in \{\mathbb{S}\}c.\) so that \(p_1\) and \(q_{c.}\) are associates.

**Ex:** \(\mathbb{Z}\) is a UFD

**NonEx:** \(\mathbb{Z}[\sqrt{-5}]\) is not a UFD:
\[ 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}) \]

We have seen: Euclidean domain \(\Rightarrow\) PID.
We'll prove: PID \(\Rightarrow\) UFD.
There are PID's that are not Euclidean and UFD's that are not PID's.

So Euclidean domains \(\neq\) PID's \(\neq\) UFD's

We now start proving: if \(R\) is a PID then it is a UFD

Definition: Let \(R\) be a commutative ring, \(\mathbb{I}_n\) a collection of ideals. The collection is a chain.
if \( I_j \leq I_{j+1} \) for all \( j \). That is:
\[
I_1 \leq I_2 \leq I_3 \leq \ldots \leq I_j \leq I_{j+1} \leq \ldots
\]

Example: Let \( R = \text{Map}(\mathbb{N}, \mathbb{R}) = f(\mathbb{N}, \mathbb{R}) \) functions from \( \mathbb{N} \) to \( \mathbb{R} \).
Let \( I_1 = \left\{ f \in \mathbb{R} \mid f|_{\mathbb{N}} = 0 \right\} \), it's an ideal in \( R \).
\( I_2 = \left\{ f \in \mathbb{R} \mid f|_{\mathbb{N}} = 0 \right\} \).
\[
I_j = \left\{ f : \mathbb{N} \to \mathbb{R} \mid f|_{\{0, 1, \ldots, j\}} = 0 \right\}
\]

Then \( I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots \subseteq I_j \subseteq I_{j+1} \subseteq \ldots \).

Lemma 29.2: Let \( R \) be a commutative ring.
\( I_1 \subseteq I_2 \subseteq \ldots \subseteq I_j \subseteq \ldots \) an ascending chain of ideals. Then \( J = \bigcup_{k=1}^{\infty} I_k \) is an ideal in \( R \).

Proof: Suppose \( x, y \in J \). Then \( \exists k, l \in \mathbb{N} : x \in I_k, y \in I_l \).
No loss of generality to assume \( n \leq l \). Then \( I_{l-k} \subseteq I_l \).
\[
x, y \in I_l \implies x-y \in I_{l-k} \subseteq \bigcup_{k=1}^{\infty} I_k = J
\]
Also, \( \forall r \in R \), \( rz \in I_l \subseteq \bigcup_{k=1}^{\infty} I_k = J \).
\[
\therefore J \text{ is an ideal.}
\]

Theorem 29.3: Let \( R \) be a PID and
\( I_1 \subseteq I_2 \subseteq \ldots \subseteq I_j \subseteq \ldots \) an ascending chain of ideals.
Then \( \exists m \in \mathbb{N} : I_m = I_{m+1} = I_{m+2} = \ldots \) and \( \bigcup_{k=1}^{\infty} I_k = I_m \).

Proof: Since \( R \) is a PID and \( \bigcup_{k=1}^{\infty} I_k \) is an ideal, \( \exists \alpha \in R \) with
\[
(a) = \bigcup_{k=1}^{\infty} I_k \implies a \in \bigcup_{k=1}^{\infty} I_k \implies \exists m \in \mathbb{N} : a \in I_m \implies (a) \subseteq I_m \]
That is \( \bigcup_{k} I_k \subseteq \text{Im.} \). In particular, \( \forall j \geq m, I_j \subseteq \text{Im} \).

But \( \text{Im} \subseteq I_j \) for \( j \geq m \). We conclude that \( I_j = \text{Im} \) for all \( j \geq m \) (and \( U I_k = \text{Im.} \)).

**Theorem 29.4** Any PID is a UFD.

**Proof.** Let \( R \) be a PID. We want to show: \( \forall r \in R, r \neq 0, r \) not unit

\( \exists \) irreducibles \( p_1 \ldots p_n \) so that \( r = p_1 \ldots p_n \).

Moreover, if \( q_1 \ldots q_m \) are irreducibles with \( r = q_1 \ldots q_m \) then \( m \geq n \) and \( \exists (S_m) \) s.t. \( p_j \) and \( q_j \) (or \( \bar{q_j} \)) are associates \( \forall j \).

(Existence) Suppose \( r \in R, r \neq 0, r \) not a unit. If \( r \) is irreducible we're done. If not, \( r \) can be factored: \( \exists r_1, r_2 \in R \) so that \( r = r_1 r_2 \) and \( r_1, r_2 \) are not units.

If both \( r_1, r_2 \) are irreducible, we're done. If not, one of the \( r_i \)'s can be factored. Say \( r_1 = r_{11} r_{12} \), \( r_1, r_{12} \) are not units.

Keep going. We're done if the process stops.

Does it stop?

Suppose not. We then have \( r = r_1 r_2 \)

\[ r_1 = r_{11} r_{12} \]

\[ r_{11} = r_{111} r_{112} \]

As a result we get a chain of ideals \( (r) \supseteq (r_1) \supseteq (r_{11}) \supseteq (r_{111}) \ldots \)

which is infinite. This is impossible in a PID by 29.3.

**Conclusion:** Any element \( r \in R, r \neq 0, r \) a product of finitely many irreducibles.

Next time: uniqueness.