Last time: In a commutative ring \( R \) with 1, an ideal \( M \) is maximal \( \iff \) \( R/M \) is a field.

**Example:** An ideal \( n\mathbb{Z} \) in \( \mathbb{Z} \) is maximal \( \iff \) \( n \) is prime

\( \mathbb{Z}/n\mathbb{Z} \) is a field \( \iff n \) is prime (\( \Rightarrow \) )

\( \mathbb{Z}/0\mathbb{Z} \) is not a field, and 0 is not prime

**Def:** Let \( R \) be a commutative ring. An ideal \( N \) in \( R \) is prime if:

1. \( N \neq R \) and
2. \( ab \in N \) implies \( a \in N \) or \( b \in N \), for \( a, b \in R \).

**Thm:** In a commutative ring \( R \) with 1, an ideal \( N \) is prime \( \iff \) \( R/N \) is an integral domain.

**Proof:** First, \( R/N \) is always commutative and always has 1.

1. \( N \neq R \iff R/N \neq \{0\} \iff R/N \) has 1\( \neq 0 \).
2. \( ab \in N \) implies \( a \in N \) or \( b \in N \), for \( a, b \in R \) \( \iff \) \( R/N \) has no zero divisors.

"\( \iff \)": If \( R/N \) has no zero divisors, then

\[
(a+N)(b+N) = 0 \implies a+N = 0 \text{ or } b+N = 0 \text{ in } R/N
\]

\[
\iff \quad (a+N)(b+N) = ab+N
\]

\( \iff \) (2): \( ab \in N \)

\( \iff \) \( N \) is prime \( \iff \) (1) and (2) are true \( \iff \) there are no other cases in \( R/N \) is an integral domain.

**Cor:** In a commutative ring with 1, every maximal ideal is prime.

**Proof:** Let \( R \) be such a ring, and let \( M \) be an ideal in \( R \).

Then \( M \) is maximal \( \iff \) \( R/M \) is a field \( \Rightarrow \) \( R/M \) is an integral domain \( \iff M \) is prime.
Examples: In \( \mathbb{Z} \), an ideal \( n\mathbb{Z} \) prime \( \iff \) \( n \) is prime or \( n = 0 \).

And, \( \mathbb{Z}/n\mathbb{Z} \cong \begin{cases} \mathbb{Z} & \text{if } n \neq 0 \\ \mathbb{Z}/n & \text{if } n = 0 \end{cases} \) \( \iff \) \( n \) is prime or \( n = 0 \).

Recalls \[ \text{Prime subfield of a field} \]

Recalls: Let \( R \) be a ring with 1. Then there’s a group homomorphism \( \varphi: \mathbb{Z} \to R \) such that \( \varphi(1) = 1 \). This is a group homomorphism from \( \langle \mathbb{Z}, + \rangle \) to \( \langle R, + \rangle \). It is also a ring homomorphism by the distributive laws.

Its kernel is \( n\mathbb{Z} \), where \( n = \text{char } R \).

Cor: \( R \) contains a subring isomorphic to \( \mathbb{Z} \) if \( \text{char } R = 0 \), or isomorphic to \( \mathbb{Z}/n\mathbb{Z} \) if \( \text{char } R = n \neq 0 \).

Proof: The subring is \( \varphi[\mathbb{Z}] \), which is isomorphic to \( \mathbb{Z}/\ker \varphi \) \( \cong \mathbb{Z}/n\mathbb{Z} \cong \begin{cases} \mathbb{Z} & \text{if } n \neq 0 \\ \mathbb{Z}/n & \text{if } n = 0 \end{cases} \) where \( n = \text{char } R \).

(Recall “direction of a ring homomorphism.”)

Cor: A field \( F \) contains a subfield isomorphic to \( \mathbb{Z}/p \) (if \( \text{char } F = p \)) or isomorphic to \( \mathbb{Q} \) if \( \text{char } F = 0 \).

Proof: If \( \text{char } F = 0 \), then \( F \) contains a subring \( \cong \mathbb{Z} \).

Here \( \mathbb{Z} \) is an integral domain (it’s a subfield of \( F \)), \( \mathbb{Z} \) is prime (otherwise it would be the trivial ring \( \{0\} \)), hence zero divisors (if \( n \) is composite). Thus \( n = p \) is prime, and \( \mathbb{Z}/p \) is a field.

If \( \text{char } F = p \), then \( F \) contains a subring \( \cong \mathbb{Z}/p \) (it’s also a subring of \( \mathbb{F}_p \), the fraction field of \( \mathbb{Z}/p \), which is \( \mathbb{Q} \)).

Def: The above subfield (\( \cong \mathbb{Z}/p \) or \( \mathbb{Q} \)) is called the prime subfield of \( F \).
For the rest of today's class:

**F is a field.**

Thus, for every field $F$, every ideal in $F[x]$ is principal.

**Proof:** Let $F$ be a field and $N$ an ideal in $F$.

**Case 1:** If $N = 0$ then it's principal: $N = \langle 0 \rangle$.

**Case 2:** $N \neq 0$. Let $g(x)$ be a nonzero element of $N$ of smallest degree. Since $g \in N$, $\langle g \rangle \subseteq N$.

(In any commutative ring $R$ with identity, if $N$ is an ideal and $g \in N$, then $\langle g \rangle \subseteq N$, because any $a \in \langle g \rangle$ is equal to $g$ times some element of $R$, and $a = g \cdot r \in N$ because $g \in N$, $r \in R$, and $N$ is an ideal. So $\langle g \rangle$ is the smallest ideal of $R$ that contains $g$.)

To show $N \subseteq \langle g \rangle$, let $f \in N$. Write $f(x) = q(x)g(x) + r(x)$ with $q, r \in F[x]$ and $\deg r < \deg g$. Then $r = f - qg$ is in $N$; so if $r \neq 0$ then $g$ is not the nonzero element of $N$ of smallest degree, because $r \in N$, $r \neq 0$, and $\deg r < \deg g$; contradiction. Then $r = 0$, so $f = qg$, \( \vdash f \in \langle g \rangle \), $N \subseteq \langle g \rangle$, so $N = \langle g \rangle$ is principal.

(Compare this with the proof of Thm. 6.6.)

**Thm:** An ideal $\langle p \rangle$ in $F[x]$ is maximal $\iff$ $p$ is irreducible.

**Proof:** **Case 1:** $p = 0$. Then $p$ is not irreducible and $\langle p \rangle = \langle 0 \rangle$ is not maximal ($\langle 0 \rangle \not\supset \langle x \rangle \supset F[x]$).

**Case 2:** $p \neq 0$. Then $1 = pp^{-1}$. Since $p$ is a unit in $F[x]$ $\iff$ $1 \in \langle p \rangle \iff \langle p \rangle = F[x]$.

**Case 2a:** $p$ is reducible $\iff$ $p = fg$ with $f, g \in F[x]$ not constant, \( \vdash \langle p \rangle \not\supset \langle f \rangle \supset F[x] \). $p$ is nonconstant.

$p \in \langle f \rangle$ and $\neq 0$ because if $\langle p \rangle = \langle f \rangle$ then $f \in \langle p \rangle$, so $f = ph$, \( \vdash g = f h \in F[x] \).
So $p$ is irreducible $\iff$ both conditions on the left are false ($p$ not constant and $p$ not reducible).

And $<p>$ is maximal $\iff$ both conditions on the right are false ($<p> \neq F[x]$ and there is no ideal $<f>$ such that $<p> \not\subseteq <f> \subseteq F[x]$).

$p$ is irreducible $\iff$ $<p>$ is maximal. \(\Box\)

Again! This is similar to the situation in $\mathbb{Z}$:

$<n> = n \mathbb{Z}$ is maximal $\iff$ $n$ is prime. (Hint)