Wednesday, Nov. 14

Last time... We proved:
- If $F$ is a field then every ideal in $F[x]$ is principal,
  and
- Such an ideal $<p(x)>$ is maximal $\iff p$ is irreducible.

Thm (loose end from Mon., Nov. 5): Let $F$ be a field and let $p, r, s \in F[x]$. If $p$ is irreducible and $p | rs$, then $p | r$ or $p | s$.

Proof: $p | rs \iff rs \in <p> \Rightarrow r \in <p>$ or $s \in <p> \iff p | r$ or $p | s$.

Next: Study Fields.

Our first basic goal: Show that every nonconstant polynomial in $F[x]$ (where $F$ is a field) has a zero...

... Somewhere... in some larger field (containing $F$ as a subfield).

Def: If $E$ and $F$ are fields, and $F \subseteq E$, then we say that $E$ is an extension field of $F$. We also write "$E/F$ is a field extension", or write $E/F$ in diagrams.

Example:

\[
\begin{align*}
\{a+bi : a, b \in \mathbb{Q}\} & \quad \text{C} \\
\{a+bi : a, b \in \mathbb{R}\} & \quad \mathbb{R} \\
\{a+bi : a, b \in \mathbb{Q}\} & \quad \mathbb{Q}
\end{align*}
\]

\[
\begin{align*}
\{a+bi : a, b \in \mathbb{Q}\} & \quad \text{C} \\
\{a+bi : a, b \in \mathbb{R}\} & \quad \mathbb{R} \\
\{a+bi : a, b \in \mathbb{Q}\} & \quad \mathbb{Q}
\end{align*}
\]
Kronecker's Theorem ("Basic goal"): Let $F$ be a field and let $f(x) \in F[x]$ be a nonconstant polynomial. Then there exists an extension field $E/F$ and an element $\alpha \in E$ such that $f(\alpha) = 0$.

**Proof:** Let $p(x)$ be an irreducible factor of $f(x)$. It will be enough to find $E$ that contains a root of $p$.

Let $E = F[x]/<p>$. Since $p$ is irreducible, $<p>$ is maximal, therefore $E = F[x]/<p>$ is a field.

Define $\psi : F \to E$ by $F \to F[x] \xrightarrow{\text{canonical map}} F[x]/<p> = E$

Note that $\psi(c) \not\equiv 0$ because $1 + <p> \not\equiv 0$ ($1 \not\equiv <p>$).

Let $\ker \psi = <0>$ (we just showed $\ker \psi \neq F$, i.e., $\ker \psi = <0>$ because $\ker \psi$ is an ideal and there are the only ideals in $F$).

So we can regard $E$ as an extension field of $F$.

Now let $\alpha = x + <p> \in E$. Write $p(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0 \in F$.

Then $p(\alpha) = (a_n + <p>)(x + <p>)^n + (a_{n-1} + <p>)(x + <p>)^{n-1} + \ldots + (a_0 + <p>)$

$= (a_n + <p>) + (a_{n-1} + <p>)(x + <p>)^{n-1} + \ldots + (a_0 + <p>)$

$= (a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0) + <p>$

$= p(x) + <p>$

$= 0 + <p>$. So $\alpha$ is a root of $p(x)$.

$\square$
Examples  

\[ F = \mathbb{Q}, \quad f(x) = x^2 - 2. \]  

This is irreducible, so let \( \rho = \mathbb{F} \).

Then \( \mathbb{E} = F[x]/\langle x^2 - 2 \rangle \), and \( \alpha = x + \langle x^2 - 2 \rangle \).

Since \( \mathbb{Q}[x] \to \mathbb{E} \) is onto, every element \( \beta \in \mathbb{E} \) can be written as \( g(x) + \langle p \rangle \) for some \( g \in \mathbb{Q}[x] \).

For example, \( \beta = x^4 + x^3 + 3x + 7 + \langle p \rangle \)

\[ = \alpha^4 + \alpha^3 + 3\alpha + 7 \]

\[ = 2^2 + 2\alpha + 3\alpha + 7 = 5\alpha + 11. \quad \text{(since } \alpha^2 = 2). \]

Or, we could've used the division algorithm

\[ x^4 + x^3 + 3x + 7 = (x^2 + x + 2)(x^2 - 2) + (3x^2 + 11) \]

\[ \text{mod } \langle \alpha^2 - 2 \rangle \quad \alpha \in \mathbb{E} \]

By the uniqueness part of the division algorithm (for polynomials): for any \( \beta \in \mathbb{E} \) there is exactly one \( r(x) \in \mathbb{Q}[x] \) of degree \( < \deg \rho \) such that \( \beta = r(x) \).

In our example, if \( c, c', d, d' \in \mathbb{Q} \) and \( \alpha x + d = c\alpha + d' \), then

\( (c - c') \alpha = d' - d \), so we must have \( c = c' \), otherwise we'd have \( \alpha = \frac{d' - d}{c - c'} \in \mathbb{Q} \), which isn't true.

Also, there always exist such an \( r(x) \).

So \( \mathbb{E} = \{ a\alpha + b : a, b \in \mathbb{Q} \} \supseteq \{ a\alpha^2 + b : a, b \in \mathbb{Q} \} \)

(As in the earlier homework problems).

More generally, we can do this for any irreducible polynomial \( \rho(x) \); for example, if \( \rho \in \mathbb{Q}[x] = x^2 - 2x^2 + 4x - 2 \in \mathbb{Q}[x] \)

(irreducible since it's Eisenstein for the prime \( 2 \)).

Then for this \( \rho \), \( \mathbb{E} = \mathbb{Q}[x]/\langle \rho \rangle = \{ a\alpha^2 + b\alpha + c : a, b, c \in \mathbb{Q} \} \mathbb{C} \mathbb{R} \)

when \( \alpha \) is a real root of \( \rho \).

Def: Let \( \mathbb{E}/\mathbb{F} \) be a field extension. Then an element \( \alpha \in \mathbb{E} \) is algebraic over \( \mathbb{F} \) if there is a nonzero polynomial \( f(x) \in \mathbb{F}[x] \) such that \( f(\alpha) = 0 \). Otherwise, it is said to be transcendental over \( \mathbb{F} \).

Elements of \( \mathbb{C} \) are said to be algebraic numbers if they are algebraic over \( \mathbb{Q} \), and transcendental numbers otherwise.
Example: \( \sqrt{2}, \sqrt[3]{18}, \sin 1^\circ \) are algebraic numbers. 
\( e \) is transcendental (can't prove in this class).

**Theorem:** Let \( E/F \) be a field extension. Then an element \( x \in E \) is transcendental over \( F \) if and only if the evaluation homomorphism \( \Phi_x : F[x] \rightarrow E \) is one-to-one.

**Proof:** \( x \) is algebraic over \( F \) \( \iff \ker(\Phi_x) = \{0\} \) \( \iff \Phi_x \) is not one-to-one. \( \Box \)

**Interlude on rings and polynomials.**

**Proposition:** Let \( R \) be a commutative ring with unity 1. Let \( x, y \in R \), not zero divisors and not zero. Then \( \langle x \rangle = \langle y \rangle \) if and only if \( x = uy \) for some unit \( u \in R \).

**Proof:** "\( \Rightarrow \): If \( x = uy \) then \( x \in \langle y \rangle \), so \( \langle x \rangle \subseteq \langle y \rangle \).

"\( \Leftarrow \): \( \langle x \rangle = \langle y \rangle \Rightarrow x \in \langle y \rangle \), so \( x = ay \) for some \( a \in R \). Also \( \langle x \rangle = \langle y \rangle \Rightarrow y \in \langle x \rangle \), so \( y = bx \) for some \( b \in R \).

\( x = ay = a(bx) \), so \( 1x = (ab)x \). Cancellation \( x \) since \( x \) is not a zero divisor and not 0) gives \( ab = 1 \).
\( a \) is a unit, and \( x = ay \). \( \Box \)

**Corollary:** Let \( F \) be a field and \( p, q \in F[x] \), both \( \neq 0 \). Then the proposition applies, and \( \langle p \rangle = \langle q \rangle \Rightarrow p = uq \) for some unit \( u \in F[x] \). But units in \( F[x] \) are exactly nonzero elements of \( F \) (or a hoot problem), so \( p \) is a constant multiple of \( q \) (and vice versa). \( \Box \)

Then \( \langle p \rangle = \langle q \rangle \iff \) they are constant multiples of each other.