Ideals in $F[x]$ (continued)

*Throughout this class, $F$ is a field.*

Recall from last time...

**Theorem.** *All ideals in $F[x]$ are principal.*
Theorem. Let $p(x) \in F[x]$, and let $I = \langle p \rangle$. Then:

(a). $I = \langle 0 \rangle$ if and only if $p = 0$,

(b). $I$ is the unit ideal if and only if $p$ is a nonzero constant, and

(c). $I$ is a maximal ideal if and only if $p$ is irreducible.

Proof. (a) is clear. Note also that $\langle 0 \rangle$ is not maximal, because $\langle 0 \rangle \subsetneq \langle x \rangle \subsetneq F[x]$.

(b). $p$ is a nonzero constant $\iff p$ is a unit in $F[x] \iff \langle p \rangle$ is the unit ideal.

(c). In parts (a) and (b), $p$ is constant and $\langle p \rangle$ is not maximal.
Therefore we may assume that $p$ is not constant and that $I$ is a nonzero proper ideal.

If $p$ is not irreducible, then $p$ is reducible, say $p = fg$ with $f$ and $g$ nonconstant. Considering the ideals $\langle p \rangle \subseteq \langle f \rangle \subseteq F[x]$, we have $\langle f \rangle \neq F[x]$ because $f$ is not constant, and $\langle p \rangle \neq \langle f \rangle$ because $f \in \langle p \rangle$ would imply $p \mid f$, so $\deg f \geq \deg p$, and then $g$ would have to be constant. Therefore $\langle p \rangle \nsubseteq \langle f \rangle \nsubseteq F[x]$, and we conclude that $\langle p \rangle$ is not maximal.

Conversely, assume that $p$ is irreducible. Let $\langle p \rangle \subseteq \langle f \rangle \subseteq F[x]$ be ideals. Since $p \in \langle f \rangle$ we have $p = fg$ for some $g \in F[x]$. Since $p$ is irreducible, $f$ or $g$ must be constant (and they're nonzero because $p \neq 0$). Therefore either $f \in F^*$ (implying $\langle f \rangle = F[x]$) or $g \in F^*$ (which implies $f = g^{-1}p \in \langle p \rangle$, so $\langle f \rangle = \langle p \rangle$). In either case, we do not have $\langle p \rangle \nsubseteq \langle f \rangle \nsubseteq F[x]$. Since this is true for all ideals $\langle f \rangle$ between $I$ and $F[x]$, $I$ is maximal.
A Loose End

**Theorem 23.18.** Let $F$ be a field, and let $p, r, s \in F[x]$. If $p$ is irreducible and $p \mid rs$, then $p \mid r$ or $p \mid s$.

**Proof.** Since $p$ is irreducible, $\langle p \rangle$ is maximal, hence prime. Therefore

$$p \mid rs \iff rs \in \langle p \rangle \iff r \in \langle p \rangle \text{ or } s \in \langle p \rangle \iff p \mid r \text{ or } p \mid s.$$
A “Basic Goal”

Stated imprecisely: Let $F$ be a field. Then every nonconstant polynomial in $F[x]$ has a zero in some field containing $F$ as a subfield.

**Definition.** An extension field of a field $F$ is a field that contains $F$ as a subfield.

The words “$E/F$ is a field extension” mean that $E$ is an extension field of $F$.

**Examples.** [Diagram on board; lines indicate field extensions]
Kronecker's Theorem

**Theorem ("Basic Goal").** Let $F$ be a field and let $f \in F[x]$ be a nonconstant polynomial. Then there exists a field extension $E/F$ and an element $\alpha \in E$ such that $f(\alpha) = 0$.

**Proof.** Let $p$ be an irreducible factor of $f$. It will be enough to find $E$ and $\alpha$ such that $p(\alpha) = 0$.

Let $E = F[x]/\langle p \rangle$. Since $p$ is irreducible, $\langle p \rangle$ is maximal, so $E$ is a field. Let $\psi: F \rightarrow E$ be the composition

$$\psi: F \rightarrow F[x] \rightarrow F[x]/\langle p \rangle = E$$

(so that $\psi(a) = a + \langle p \rangle$). Note that $\psi(1) = 1 + \langle p \rangle \neq 0 + \langle p \rangle$ because $1 \notin \langle p \rangle$. Therefore $\psi$ is injective [why?].

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


Let $\alpha = x + \langle p \rangle \in E$.

**Lemma.** For any polynomial $g \in F[x]$, $g(\alpha) = g + \langle p \rangle$.

**Proof.** Write

$$g(x) = a_n x^n + \cdots + a_0.$$  

Then

$$g(\alpha) = (a_n + \langle p \rangle)(x + \langle p \rangle)^n + \cdots + (a_0 + \langle p \rangle)$$  

$$= (a_n + \langle p \rangle)(x^n + \langle p \rangle) + \cdots + (a_0 + \langle p \rangle)$$  

$$= (a_n x^n + \langle p \rangle) + \cdots + (a_0 + \langle p \rangle)$$  

$$= (a_n x^n + \cdots + a_0) + \langle p \rangle$$  

$$= g(x) + \langle p \rangle.$$

In particular, $p(\alpha) = p(x) + \langle p \rangle = 0 + \langle p \rangle = 0$ (in $E$).
Example. \( F = \mathbb{Q} \), \( p(x) = x^2 - 2 \) (irreducible over \( \mathbb{Q} \)). Then \( E = F[x]/\langle x^2 - 2 \rangle \) and \( \alpha = x + \langle x^2 - 2 \rangle \). Note that

\[
\alpha^2 - 2 = x^2 + \langle p \rangle - (2 + \langle p \rangle) = (x^2 - 2) + \langle p \rangle = p + \langle p \rangle = 0 + \langle p \rangle.
\]

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

(Subexample: \( f(x) = x^4 + 3x^3 - x - 1 = (x^2 + 3x + 2)(x^2 - 2) + (5x - 3) \) according to the Division Algorithm, with \( r(x) = 5x - 3 \), so \( f(x) + \langle p \rangle = 5x - 3 + \langle p \rangle = 5\sqrt{2} - 3 \).

Or, just plug in \( \alpha^2 = 2 \): \( f(\alpha) = 2^2 + 6\alpha - \alpha - 1 = 5\alpha - 3 = 5\sqrt{2} - 3 \).
Clicker Questions!

(And please remind Prof. Vojta to return homeworks and pass out handouts)
Structure of \( E \)

**Theorem.** Let \( F \) be a field, let \( p = F[x] \) be an irreducible polynomial, let \( E \) be the field \( F[x]/\langle p \rangle \), regarded as an extension field of \( F \), and let \( \alpha = x + \langle p \rangle \in E \). Also let \( n = \deg p \). Then every element \( \beta \in E \) can be expressed uniquely as a sum

\[
\beta = b_{n-1} \alpha^{n-1} + \cdots + b_0 \quad \text{with} \quad b_0, \ldots, b_n \in F .
\]

**Proof.** Existence. Let \( \beta \in E \), say \( \beta = f + \langle p \rangle \) with \( f \in F[x] \). Using the Division Algorithm, write \( f = qp + r \) with \( q, r \in F[x] \) and \( \deg r < n \). Then (since \( p(\alpha) = 0 \) in \( E \)), \( f(\alpha) = r(\alpha) \). By the earlier lemma, we then have \( \beta = f(x) + \langle p \rangle = f(\alpha) = r(\alpha) \), which can be written in the above form.
Uniqueness. If

\[ \beta = b_{n-1}\alpha^{n-1} + \cdots + b_0 = b'_{n-1}\alpha^{n-1} + \cdots + b'_0, \]

then \( c_{n-1}\alpha^{n-1} + \cdots + c_0 = 0 \), where \( c_i = b_i - b'_i \) for all \( i \). Let

\[ g(x) = c_{n-1}x^{n-1} + \cdots + c_0 \in F[x]. \]

Then \( g(x) + \langle p \rangle = g(\alpha) = 0 \), so \( g \in \langle p \rangle \). For degree reasons, this can happen only if \( g = 0 \). Therefore \( b'_i = b_i \) for all \( i \), which gives uniqueness.
Interlude on Rings and Polynomials

Proposition. Let $R$ be a commutative ring with unity. Let $x$ and $y$ be nonzero elements of $R$ that are not zero divisors. Then $\langle x \rangle = \langle y \rangle$ if and only if $x = uy$ for some unit $u$ of $R$.

Proof. “$\implies$”: $\langle x \rangle = \langle y \rangle$ implies $x \in \langle y \rangle$, so $x = ay$ for some $a \in R$. Also, $y \in \langle x \rangle$ implies that $y = bx$ for some $b \in R$. Therefore $x = abx$. Cancelling $x$ gives $1 = ab$, so $a$ and $b$ are units.

“$\impliedby$”: Assume that $x = uy$, where $u$ is a unit in $R$. Then $x \in \langle y \rangle$, so $\langle x \rangle \subseteq \langle y \rangle$. Similarly $y = u^{-1}x$ gives $\langle y \rangle \subseteq \langle x \rangle$. Therefore $\langle x \rangle = \langle y \rangle$. □
Corollary. Let $F$ be a field and let $p, q \in F[x]$, both nonzero. Then $\langle p \rangle = \langle q \rangle$ if and only if $p$ and $q$ are (nonzero) constant multiples of each other.

Corollary. Let $N$ be a nonzero ideal in $F[x]$. Then there is a unique monic polynomial $f \in F[x]$ such that $N = \langle f \rangle$.

Proof. We know that $N = \langle f_0 \rangle$ for some nonzero $f_0 \in F[x]$. Take $f = c^{-1} f_0$, where $c$ is the leading coefficient of $f_0$. This is the desired monic polynomial. It is unique because if $\langle f \rangle = \langle g \rangle$ with $f$ and $g$ monic, then $f = cg$ for some $c \in F$, but $c = 1$ because both $f$ and $g$ are monic. Thus $f = g$. \qed
Algebraic and Transcendental Elements

**Definition.** Let $E/F$ be a field extension. Then an element $\alpha \in E$ is **algebraic** over $F$ if there is a nonzero polynomial $f \in F[x]$ such that $f(\alpha) = 0$. Otherwise we say that $\alpha$ is **transcendental** over $F$.

**Definition.** A **transcendental number** is an element of $\mathbb{C}$ which is transcendental over $\mathbb{Q}$. An **algebraic number** is defined similarly.

**Examples.** As noted earlier, $\pi$ and $e$ (the base of the natural logarithms) are transcendental numbers; $\sqrt{2}$ and $3$ are algebraic numbers.
Theorem. Let $E/F$ be a field extension and let $\alpha \in E$. Let $\phi_\alpha : F[x] \to E$ be the evaluation homomorphism $f(x) \mapsto f(\alpha)$. Then $\alpha$ is transcendental over $F$ if and only if $\phi_\alpha$ is injective.

Proof.

$\alpha$ is transcendental over $F \iff f(\alpha) \neq 0 \text{ for all } 0 \neq f \in F[x]$

$\iff \ker(\phi_\alpha) = \langle 0 \rangle$

$\iff \phi_\alpha$ is injective.
Theorem. Let $E/F$ be a field extension and let $\alpha \in E$ be algebraic over $F$. Then there is an irreducible polynomial $p \in F[x]$ such that $p(\alpha) = 0$. It is a nonzero element of $\ker \phi_\alpha$ of smallest degree. If we require it to be monic, then it's unique, and is the unique monic element of $\ker \phi_\alpha$ of smallest degree.
Proof. By Theorem 27.24, \( \ker \phi_\alpha = \langle p \rangle \) for some \( p \in F[x] \) (recall that \( \phi_\alpha \) is a homomorphism \( F[x] \to E \)).

We claim that \( p \) is irreducible. To show this, assume that \( p \) is not irreducible. Since \( p \) is nonconstant, it must be reducible. Therefore \( p = fg \) with \( f \) and \( g \) nonconstant. Then \( f(\alpha)g(\alpha) = p(\alpha) = 0 \); hence \( f(\alpha) = 0 \) or \( g(\alpha) = 0 \). This gives \( f \in \ker \phi_\alpha \) or \( g \in \ker \phi_\alpha \); therefore \( p \mid f \) or \( p \mid g \); and that gives \( \deg f \geq \deg p \) or \( \deg g \geq \deg p \), and that implies that \( g \) or \( f \) must be constant, respectively. This is a contradiction, so \( p \) is irreducible.

You can make \( p \) monic (divide it by its leading coefficient).

Then \( p \) is the unique monic irreducible polynomial such that \( p(\alpha) = 0 \). Indeed, if \( q \) is another such polynomial, then \( q(\alpha) = 0 \), so \( q \in \ker \phi_\alpha = \langle p \rangle \), so \( p \mid q \), and this gives \( q = cp \) for some \( c \in F[x] \). But since \( q \) is irreducible, \( c \) must be a constant. In fact, since both \( p \) and \( q \) are monic, \( c = 1 \), so \( q = p \). \( \square \)
Notes

(1) Of all nonzero \( f \in F[x] \) such that \( f(\alpha) = 0 \), \( p \) has the smallest degree

(2) All \( f \in F[x] \) such that \( f(\alpha) = 0 \) are multiples of \( p \).

Definition. This (monic) polynomial \( p(x) \) is called the (monic) irreducible polynomial of \( \alpha \) over \( F \), and is written \( \text{irr}(\alpha, F) \) or \( \text{irr}_{\alpha, F} \) or \( \text{irr}_{\alpha, F}(x) \). The degree of \( \alpha \) over \( F \) is the degree of \( \text{irr}_{\alpha, F}(x) \), and is written \( \deg(\alpha, F) \).

Note: The image of \( \phi_\alpha : F[x] \to E \) is denoted \( F(\alpha) \). We have

\[
F(\alpha) \cong F[x]/\langle p \rangle.
\]

It is a field (because \( p \) is irreducible, hence \( \langle p \rangle \) is maximal).

\( F(\alpha) \) is the smallest subfield of \( E \) that contains both \( F \) and \( \alpha \) (this follows from \( \beta = b_{n-1}\alpha^{n-1} + \cdots + b_0 \) with \( b_{n-1}, \ldots, b_0 \in F \), as above).
Finis

Have a good weekend!

Good luck on your exams