Day 24 July 10, 2024

Ideals in $F[x]$

Thm. If F is a field, then every ideal in $F[x]$ is principal.

(Proof idea.) Choose $p(x) \in I$ nonzero and of minimal degree. Use the division algorithm to show that $I = \langle p(x) \rangle$. $\blacksquare$

Thm. For any $p(x) \in F[x]$, with F a field, the ideal $\langle p(x) \rangle$ is maximal iff $p(x)$ is irreducible.

(Proof.)

Suppose $\langle p(x) \rangle$ is maximal.

Then $\langle p(x) \rangle$ is prime.

Suppose $p(x) = a(x)b(x)$ for some $a(x), b(x) \in F[x]$.

Since $\langle p(x) \rangle$ is prime, either $a(x) \in \langle p(x) \rangle$ or $b(x) \in \langle p(x)$. Assume $a(x) \in \langle p(x) \rangle$.

Note that $p(x) \in \langle a(x) \rangle \Rightarrow \langle p(x) \rangle \subseteq \langle a(x) \rangle$.

If $\deg a(x) < \deg p(x)$, then $\langle p(x) \rangle \subsetneq \langle a(x) \rangle$.

Since $\langle p(x) \rangle$ is maximal, $\langle a(x) \rangle = F[x]$.

So $\deg a(x) = 0$.

$\therefore$ $p(x)$ is irreducible.

Suppose $p(x)$ is irreducible.

Let $I \subseteq F[x]$ is an ideal with $\langle p(x) \rangle \subseteq I$.

By previous thm, $I = \langle f(x) \rangle$ for some $f(x)$.

So $p(x) = f(x) \cdot g(x)$, for some $g(x) \in F[x]$.

Since $p(x)$ is irreducible, either

$$\deg f(x) = 0 \Rightarrow I = F[x]$$

OR $\deg g(x) = 0 \Rightarrow \langle f(x)\rangle = \langle p(x)\rangle$.

So $\langle p(x)\rangle$ is maximal. $\blacksquare$

Extension fields

Def. A field E is an extension field of a field F if $F \subset E$ is a subfield. In this case, we call F the base field of the extension.

Ex. Consider $F = \mathbb{Z}_2$ and the polynomial

$$p(x) = x^2 + x + 1 \in F[x].$$

Note that $p(x)$ is irreducible since reducibility would require linear factors, but $p(0) = 1$; $p(1) = 1$.

Goal: Build an extension $E \supset F$ over which $p(x)$ is reducible.

B/c $p(x)$ is irred. in $F[x]$, $\langle p(x)\rangle \subseteq F[x]$ is maximal. Then $F[x]/\langle p(x)\rangle$ is a field.

Call this field E.

Given $f(x) \in F[x]$, the division algorithm gives

$$f(x) = p(x)\, q(x) + r(x),$$

with $\deg r(x) < \deg p(x) = 2$.

So $r(x) = 0$ OR $r(x) = 1$ OR $r(x) = x$ or $r(x) = 1 + x$.

In $F[x]/\langle p(x)\rangle$,

$$f(x)+\langle p(x)\rangle = \big(p(x)q(x)+r(x)\big)+\langle p(x)\rangle$$

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

So $E=\{\langle p(x)\rangle,\ 1+\langle p(x)\rangle,\ x+\langle p(x)\rangle,\ 1+x+\langle p(x)\rangle\}$.

We can identify F with the subfield

$$\{\langle p(x)\rangle,\ 1+\langle p(x)\rangle\}\subset E,$$

So E is an extension of F.

Finally, $x+\langle p(x)\rangle$ is a root of $p(x)$:

$$(x+\langle p(x)\rangle)^2+(x+\langle p(x)\rangle)+(1+\langle p(x)\rangle)$$

$$\begin{aligned}
&= (x^2+\langle p(x)\rangle)+(x+\langle p(x)\rangle)+(1+\langle p(x)\rangle)\\
&= (x^2+x+1)+\langle p(x)\rangle\\
&= p(x)+\langle p(x)\rangle\\
&= \langle p(x)\rangle.
\end{aligned}$$

So E is a field extension of F where $p(x)$ is reducible.

<u>Thm</u>. [Fundamental theorem of field theory]
Let F be a field, $p(x)\in F[x]$ nonconstant. There exists an extension field of F containing a zero of $p(x)$.

(Proof idea.) Repeat the example, replacing $p(x)$ with an irreducible factor. ∎

Def. Let $E \supset F$ be an extension field.

1. We call $\alpha \in E$ algebraic over F if $\exists\, f(x) \in F[x]$ for which α is a root. Otherwise, α is transcendental over F.

2. We call E algebraic over F if every elt. of E is algebraic over F.

3. For any $\alpha_1, \ldots, \alpha_n \in E$, the smallest subfield of E containing F and $\alpha_1, \ldots, \alpha_n$ is denoted $F(\alpha_1, \ldots, \alpha_n)$.

4. If $\exists\, \alpha \in E$ s.t. $E = F(\alpha)$, we call E a simple extension of F.

Thm. Let $E \supset F$ be an extension field and let $\alpha \in E$ be algebraic over F. Then there is a unique irreducible, monic polynomial $p(x) \in F[x]$ of smallest degree for which α is a zero, and if α is a zero of $f(x) \in F[x]$, then $p(x)$ divides $f(x)$.

(Proof idea.)

α algebraic $\Rightarrow \exists\, g(x) \in F[x]$ for which α is a zero

Decompose $g(x)$ into irred. factors and α will be a zero of at least one of these. ∎

Def. Let $E \supset F$ be an extension field, with $\alpha \in E$ algebraic over F. The unique monic, irred. polynomial $p(x)$ given by the previous theorem is called the minimal polynomial for α over F. The degree of $p(x)$ is called the degree of α over F.

Ex. $\alpha \in E \supset F$ has degree 1 $\longleftrightarrow$ $\alpha \in F$

Prop. Let $E \supset F$ be a field extension, with $\alpha \in E$ algebraic over F. Then $F(\alpha) \cong F[x]/\langle p(x) \rangle$, where $p(x)$ is the minimal polynomial for α over F.

(Proof.) Consider the evaluation homomorphism at α:

$$\phi_\alpha : F[x] \longrightarrow E.$$

According to the previous theorem, $\ker \phi_\alpha = \langle p(x) \rangle$.
By F.I.T.,

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

check

$\blacksquare$