

Chapter 16

#27

Let F be a field and let

$$I = \{ a_n x^n + a_{n-1} x^{n-1} + \dots + a_0 \mid a_n, a_{n-1}, \dots, a_0 \in F \text{ and } a_n + a_{n-1} + \dots + a_0 = 0 \}$$

Show that I is an ideal of $F[x]$ and find a generator for I .

Let $a(x)$ and $b(x) \in I$.

$$\Rightarrow a_n x^n + a_{n-1} x^{n-1} + \dots + a_0 \in I$$

$$b_n x^n + b_{n-1} x^{n-1} + \dots + b_0 \in I$$

$$a_i, b_i \in F$$

$$a_n + a_{n-1} + \dots + a_0 = 0$$

$$b_n + b_{n-1} + \dots + b_0 = 0$$

by def'n of I .

$$\Rightarrow a(x) - b(x) = (a_n x^n + \dots + a_0) - (b_n x^n + \dots + b_0)$$

$$= (a_n - b_n) x^n + (a_{n-1} - b_{n-1}) x^{n-1} + \dots + (a_0 - b_0)$$

Since $a_i, b_i \in F \Rightarrow a_i - b_i \in F$

$$(a_n - b_n) + (a_{n-1} - b_{n-1}) + \dots + (a_0 - b_0)$$

$$= \underbrace{(a_n + a_{n-1} + \dots + a_0)}_0 - \underbrace{(b_n + b_{n-1} + \dots + b_0)}_0$$

$$= 0 - 0 = 0$$

$$\therefore a(x) - b(x) \in I.$$

Now let $r(x) \in F[x]$ and $a(x) \in I$ as above

$$\Rightarrow a_n x^n + a_{n-1} x^{n-1} + \dots + a_0 \in I$$

$$a_i \in F,$$

$$a_n + a_{n-1} + \dots + a_0 = 0$$

$r(x)$: polynomial with coefficients in F .

But, these coefficients may be different from $a_n + a_{n-1} + \dots + a_0 = 0$, meaning sum of coefficients of $r(x)$ may not be 0.

must see if coefficients of $r(x)a(x)$ are sum to 0.

$$\begin{aligned}
 & \therefore r(x)a(x) \\
 &= r(x)[a_n x^n + a_{n-1} x^{n-1} + \dots + a_0] \\
 &= r(x)a_n x^n + r(x)a_{n-1} x^{n-1} + \dots + r(x)a_0 \\
 &= [r_m x^m + r_{m-1} x^{m-1} + \dots + r_0] a_n x^n + \dots + [r_m x^m + \dots + r_0] a_0 \\
 &= r_m a_n x^n x^m + r_{m-1} a_n x^n x^{m-1} + \dots + r_0 a_n x^n \\
 &+ \dots + r_m a_0 x^m + \dots + r_0 a_0
 \end{aligned}$$

\Rightarrow coefficients of $r(x)a(x)$ are

$$r_m a_n, r_{m-1} a_n, \dots, r_0 a_n,$$

$$r_m a_{n-1}, r_{m-1} a_{n-1}, \dots, r_0 a_{n-1},$$

$$r_m a_0, \dots, r_0 a_0.$$

$$\Rightarrow \sum_{i=0}^m r_i a_j = r_m a_n + r_{m-1} a_n + \dots + r_m a_0 + \dots + r_0 a_0$$

$$\begin{aligned}
 &= r_m (a_n + a_{n-1} + \dots + a_0) + r_{m-1} (a_n + a_{n-1} + \dots + a_0) \\
 &+ \dots + r_0 (a_n + a_{n-1} + \dots + a_0) = r_m(0) + r_{m-1}(0) \\
 &+ \dots + r_0(0) = 0 + \dots + 0 = 0
 \end{aligned}$$

$$\therefore r(x)a(x) \in I$$

$$\begin{aligned}
 & a(x)r(x) \\
 &= a(x)[r_m x^m + r_{m-1} x^{m-1} + \dots + r_0] \\
 &= a(x)r_m x^m + a(x)r_{m-1} x^{m-1} + \dots + a(x)r_0 \\
 &= (a_n x^n + a_{n-1} x^{n-1} + \dots + a_0) r_m x^m + \dots + (a_n x^n + a_{n-1} x^{n-1} + \dots + a_0) r_0 \\
 &= a_n r_m x^n x^m + a_{n-1} r_m x^{n-1} x^m + \dots + a_0 r_m x^m + \dots + \\
 &\dots + a_n r_0 x^n + \dots + a_0 r_0
 \end{aligned}$$

\Rightarrow coefficients of $a(x)r(x)$ are

$$a_n r_m, a_{n-1} r_m, \dots, a_0 r_m, \dots, a_n r_0, \dots, a_0 r_0$$

\Rightarrow Sum of coefficients are

$$a_n r_m + a_{n-1} r_m + \dots + a_0 r_m + \dots + a_n r_0 + \dots + a_0 r_0$$

$$= r_m (a_n + a_{n-1} + \dots + a_0) + \dots + r_0 (a_n + \dots + a_0)$$

$$= r_m(0) + \dots + r_0(0) = 0 + \dots + 0 = 0$$

$$\therefore a(x)r(x) \in I$$

Since $a(x) - b(x) \in I$,
 $a(x) r(x) \in I$
 $r(x) a(x) \in I$
by Ideal test, I is an Ideal.

To find a generator for I ,
let $p(x)$ be generator of I .
By Theorem 16.4, which states
for F , a field, I a nonzero ideal in
 $F[x]$, and $g(x)$ an element of $F[x]$.
Then, $I = \langle g(x) \rangle$ iff $g(x)$ is a nonzero
polynomial of minimum degree in I .
In this case, minimum degree is 1.

$\therefore p(x) = a_1 x + a_0$
but $a_1 + a_0 = 0$ by initial condition
 $\Rightarrow a_1 = -a_0$ or $a_0 = -a_1$
 $\therefore p(x) = a_1 x - a_1 = a_1 (x - 1)$
 $\Rightarrow p(x) \in \langle x - 1 \rangle$
 $\Rightarrow (x - 1) = g(x)$
 $\Rightarrow I = \langle g(x) \rangle = \langle x - 1 \rangle$
or $x - 1$ is generator for I .

Chapter 16

#31 For every prime p , show that

$$x^{p-1} - 1 = (x-1)(x-2) \cdots [x-(p-1)] \text{ in } \mathbb{Z}_p[x]$$

$$\text{let } g(x) = x^{p-1} - 1 - (x-1)(x-2) \cdots [x-(p-1)].$$

corollary 3 states that a polynomial of degree n over a field has at most n zeros counting multiplicity.

$\Rightarrow g(x)$ can have at most $p-1$ zeros.

by Fermat's little theorem

$$a^{p-1} \equiv 1 \pmod{p}$$

then, $1, 2, \dots, p-1$ are zeros for $[(x-1)(x-2) \cdots (x-(p-1))]$ since the theorem can be rewritten as $a^{p-1} - 1 \equiv 0 \pmod{p}$.

$$\therefore x^{p-1} \equiv 1 \pmod{p} \text{ by Fermat's theorem}$$

$$\Rightarrow x^{p-1} \equiv 1 - 1 \pmod{p}$$

$$\Rightarrow x^{p-1} - 1 \equiv 0 \pmod{p}$$

$$\therefore g(x) = 0 \text{ for } x = 1, 2, \dots, (p-1)$$

$$\therefore g(x) = 0 \text{ in } \mathbb{Z}_p[x]$$

$$\Rightarrow 0 = x^{p-1} - 1 - (x-1)(x-2) \cdots [x-(p-1)]$$

$$\Rightarrow x^{p-1} - 1 = (x-1)(x-2) \cdots [x-(p-1)]$$

Chapter 16

#39. Let F be a field. & let $f, g \in F[x]$.
If there is no polynomial of positive degree in $F[x]$ that divides both f & g
(in this case, f and g are said to be relatively prime), prove that there exist polynomials $h(x)$ and $k(x)$ in $F[x]$ with property that $f(x)h(x) + g(x)k(x) = 1$.

Since F is a field, $F[x]$ is a principal ideal domain by Thm 16.3.
 \Rightarrow every ideal has form $\langle a \rangle = \{ra \mid r \in R\}$.

$$\Rightarrow \text{for } a \in F[x], \quad \langle f, g \rangle = \langle a \rangle$$

$$\Rightarrow a \mid f \text{ and } a \mid g$$

but since f and g are relatively prime

$a \neq 0$, and $a = b$ for some $b \in F$.

$$\Rightarrow \langle f, g \rangle = \langle b \rangle$$

there must be some
such that

$$f \cdot c + g \cdot d = b.$$

$$\Rightarrow \frac{f \cdot c}{b} + \frac{g \cdot d}{b} = 1$$

$$\Rightarrow \text{if } h = \frac{c}{b}, \quad k = \frac{d}{b}, \text{ then}$$

$$fh + gk = 1$$

$$\text{or } f(x) \cdot h(x) + g(x) \cdot k(x) = 1$$

□.

Chap 17

#4. Suppose that $f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_0 \in \mathbb{Z}[x]$.
If r is rational and $x-r$ divides $f(x)$,
show that r is an integer.

Since $x-r$ divides $f(x)$, r is zero of $f(x)$
by Corollary 2 of Chapter 16 which states
that r is a zero of $f(x)$ iff $x-r$
is a factor of $f(x)$.

Since r is rational, let $r = \frac{m}{p}$ where

$\gcd(m, p) = 1$ and $m, p \in \mathbb{Z}$.

$$f(r) = 0 = f\left(\frac{m}{p}\right) = \left(\frac{m}{p}\right)^n + a_{n-1}\left(\frac{m}{p}\right)^{n-1} + \dots + \left(\frac{m}{p}\right)a_1 + a_0$$

multiplying both sides by p^n

$$0 = m^n + a_{n-1}m^{n-1}p + \dots + a_1mp^{n-2} + a_0p^{n-1}$$

$$\Rightarrow -m^n = p(a_{n-1}m^{n-1} + \dots + a_1mp^{n-2} + a_0p^{n-1})$$

$$\Rightarrow p \mid m^n \text{ but by above } \gcd(m, p) = 1$$

$$\Rightarrow p = \pm 1$$

$$\Rightarrow r = \frac{m}{\pm 1} \Rightarrow r = \pm m$$

Since $m \in \mathbb{Z}$
 $r \in \mathbb{Z}$

$\therefore r$ is an integer.