MAT401 HW5 Solutions

CHAPTER 16

22. Prove that Z[x] is not a principle ideal domain.

Consider the ideal $\langle x, 2\rangle = \{xf(x) + 2g(x) \mid f(x), g(x) \in Z[x]\}$

Claim: $\langle x, 2\rangle$ cannot be generated by a single polynomial p(x).

Proof: Assume $\langle x, 2\rangle \langle p(x)\rangle$, $p(x) \in \mathbf{Z}[x]$. $2 \in \langle x, 2\rangle \rightarrow p(x) = c$, where $c \in \{-2, 2\}$.

$\therefore \langle x, 2\rangle = \langle p(x)\rangle = \langle c\rangle$, $c \in \{-2, 2\}$.

Now for $x \in \langle x, 2\rangle$, $\exists\ h(x) \in Z[x]$ s.t. $x = h(x)c$, where $h(x) = ax$, $a \in Z$.

$\therefore x = h(x)c = axc$, $a \neq 0$, $c \neq 0$.

$\rightarrow 1 = ac$, $c \in \{-2, 2\}$.

$c = 2$, $a = \frac{1}{2}$ or $c = -2$, $a = -\frac{1}{2}$

but $a = \pm \frac{1}{2} \notin Z \Rightarrow h(x) \notin Z$, contradiction.

$\therefore \langle x, 2\rangle$ cannot be generated by a single polynomical p(x), and Z[x] is not a principle ideal domain. ■

27. Let F be a field & let $I = \{a_nx^n + a_{n-1}x^{n-1} + \dots a_1x + a_0 \mid a_i \in F, a_n + a_{n-1} + \dots + a_0 = 0\}$. Show that I is an ideal of F[x] & find a generator for I.

We'll show that I is an ideal using the ideal test. Let $a(x), b(x) \in I$.

1. $a_nx^n + a_{n-1}x^{n-1} + \dots a_1x + a_0$, $b_nx^n + b_{n-1}x^{n-1} + \dots b_1x + b_0 \in I$, $a_i, b_i \in F$, $a_n + a_{n-1} + \dots + a_0 = 0$, $b_n + b_{n-1} + \dots + b_0 = 0$.

$a(x) - b(x)$

$= (a_nx^n + a_{n-1}x^{n-1} + \dots a_1x + a_0) - (b_nx^n + b_{n-1}x^{n-1} + \dots b_1x + b_0)$

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

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

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

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

$= 0 - 0$

$= 0$

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

2. Let $a(x) \in I$, $r(x) \in F[x]$. Then, $a_nx^n + a_{n-1}x^{n-1} + \dots a_1x + a_0 \in I$, $ai \in F$, $a_n + a_{n-1} + \dots + a_0 = 0$ and r(x) is a polynomial with coefficients in F. Note that the sum of the coefficients of r are not necessarily 0.

$r(x)a(x)$

$= r(x)[a_nx^n + a_{n-1}x^{n-1} + \dots a_1x + a_0]$

$= r(x)a_nx^n + r(x)a_{n-1}x^{n-1} + .. r(x)a_1x + r(x)a_0$

$= [r_mx^m + r_{m-1}x^{m-1} + \dots + r_0]a_nx^n + [r_mx^m + r_{m-1}x^{m-1} + \dots + r_0]a_{n-1}x^{n-1} + .. [r_mx^m + r_{m-1}x^{m-1} + \dots + r_0]a_1x + r(x)a_0$

The coefficients of r(x)a(x) are: r_ma_n, r_ma_{n-1}, … r_ma_0, … $r_{m-1}a_n$, $r_{m-1}a_{n-1}$, … $r_{m-1}a_0$, … r_0a_n, r_0a_{n-1}, … r_0a_0

Sum of the coefficients of r(x)a(x):

$r_ma_n + r_ma_{n-1} + \dots + r_ma_0 + \dots + r_{m-1}a_n + r_{m-1}a_{n-1} + \dots + r_{m-1}a_0 + \dots + r_0a_n + r_0a_{n-1} + \dots + r_0a_0$

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

$= r_m(0) + r_{m-1}(0) + \dots + r_0(0)$

$= 0$

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

Similarly, it can be shown that $a(x)r(x) \in I$.

By the ideal test, I is an ideal.

Now let h(x) be the generator of I. By Thm 16.4, g(x) is a nonzero polynomial of minimum degree, where minimum degree is 1.
$\Rightarrow h(x) = a_1x + a_0$
but $a_1 + a_0 = 0$, so $a_0 = -a_1$
$\therefore h(x) = a_1x - a1 = a1(x - 1)$
$\therefore h(x) \in \langle x\text{-}1\rangle$, and $g(x) = x - 1$ is a generator for I ■

31. For every prime p, show that $x^{p-1} - 1 = (x - 1)(x - 2) \ldots [x - (p - 1)]$ in $Z_p[x]$.

Let $f(x) = x^{p-1} - 1 - (x - 1)(x - 2) \ldots [x - (p - 1)]$. By Corollary 3, f(x) can have at most (p – 1) zeros.
Claim: 1, 2, … (p – 1) are zeros of f(x).
Recall:
Fermat's Little Theorem: $a^{p-1} \equiv 1 \bmod p$, gcd(a, p) = 1
It's easy to see that 1, 2, … (p – 1) are zeros for $[(x - 1)(x - 2) \ldots (x - (p - 1))]$
For $x^{p-1} - 1$, 1, 2, … (p – 1) are all relatively prime to p
Then by Fermat's Little Theorem, $x^{p-1} \equiv 1 \bmod p$ for x = 1, 2, … (p – 1)
$\Rightarrow x^{p-1} - 1 \equiv 1 - 1 \bmod p$
$\Rightarrow x^{p-1} - 1 \equiv 0 \bmod p$
$\therefore f(x) = 0$ for x = 1, 2, … (p – 1)
$\therefore f(x) = 0$ in $Z_p[x]$
$\Rightarrow 0 = x^{p-1} - 1 - (x - 1)(x - 2) \ldots [x - (p - 1)]$
$\Rightarrow x^{p-1} - 1 = (x - 1)(x - 2) \ldots [x - (p - 1)]$ ■

39. Let F be a field & let f, g ∈ 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 ∃ polynomicals h, k ∈ F[x] s.t. fh + gk = 1.

By Thm 16.3, F[x] is a principle ideal domain.
$\therefore \langle f, g\rangle = \langle r\rangle$, $r \in F[x]$
$\Rightarrow r \mid f$ & $r \mid g$, but f, g relatively prime so $r = a_0$, $a_0 \neq 0$, $a_0 \in F$
$\therefore \langle f, g\rangle = \langle a_0\rangle$, so ∃ m, n ∈ F[x] s.t. $fm + gn = a_0$.
$\Rightarrow \frac{fm}{a_0} + \frac{gn}{a_0} = 1$, let $h(x) = \frac{m}{a_0}$, $k(x) = \frac{n}{a_0}$
$\Rightarrow fh + gk = 1$ ■

41. Let f ∈ R[x]. If f(a) = 0, f'(a) = 0, show that $(x - a)^2$ divides f(x).

$f(a) = 0 \Rightarrow$ a is a zero of $f(x) \Rightarrow (x - a) \mid f(x)$
$f'(x) = g(x) + (x - a)g'(x)$
$f'(a) = 0 \Rightarrow f'(a) = g(a) + (a - a)g'(a) = g(a) = 0$
$\therefore g(a) = 0$, a is a zero of g and $(x - a) \mid g$
$\Rightarrow g(x) = (x - a)h(x)$, $h \in \mathbf{R}[x]$
Thus,
$f(x) = (x - a)g(x) = (x - a)(x - a)h(x) = (x - a)^2h(x)$
$\Rightarrow (x - a)^2 \mid f(x)$ ■

CHAPTER 17

4. Suppose $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0 \in Z[x]$. if r is rational & (x – r) divides f(x), show that r is an integer.

$(x - r) \mid f(x) \Rightarrow$ r is a zero of f(x). Since $r \in Q$, let $r = \frac{p}{q}$, (p, q) = 1, p, q ∈ Z. Now,

$0 = f(r) = f(\frac{p}{q}) = (\frac{p}{q})^n + a_{n-1}(\frac{p}{q})^{n-1} + \ldots + (\frac{p}{q})a_1 + a_0$

Multiplying by q^n,

$0 = p^n + a_{n-1}qp^{n-1} + \ldots + a_1q^{n-1}p + a_0q^n = p^n + q(a_{n-1}p^{n-1} + q(a_{n-2}p^{n-2} + \ldots + qa_0))$
$\Rightarrow$ By above, it must be that $q \mid p^n$, but $(p, q) = 1$ so q must be ± 1 and hence r is an integer ■