Math 494

Yiwei Fu

Jan 20, 2022

<u>LAST TIME</u> $R =$ ring. $f, g \in R[x], g \neq 0$. If the leading coefficient of g is a unit in R then $\exists q, r \in R[x]$ $s.t.$ $f = gq + r$ and $\deg(r) < \deg(g)$.

Corollary. *For $\alpha \in R$ and $f(x) \in R[x]$, $\exists q(x) \in R[x]$ $s.t.$ $f(x) = (x - \alpha)q(x) + c, c \in R$. Evaluate this at $\alpha \implies c = f(\alpha)$.*

Example. In $\mathbb{Z}[x], 4x^3 + x = (2x)2x^2 + x$. But $4x^3 + x \neq (2x)q(x) + r(x)$ with $\deg(r) < \deg(2x)$.

If K is a field, what are the ideals in $K[x]$?

<u>ANSWER</u> Any nonzero ideal in $K[x]$ is $(g(x))$ where $g(x)$ is any nonzero element of I having the smallest possible degree.

Proof. For $f(x) \in I$, $f = gq + r, q, r \in K[x], \deg(r) < \deg(g)$. Bur $r = f - gq \in I$, so the minimality of $\deg(g) \implies r = 0 \implies g \mid f,\ i.e.\ f \in (g)$. ■

Definition. In a ring R, for any $\alpha \in R$, $(\alpha) := \alpha R$ is called a "principal ideal".

<u>NOTE</u> $(\alpha) = (\alpha u)$ for any $u \in R^*$. If $R =$ integral domain, $\alpha, \beta \in R$, then $(\alpha) = (\beta) \iff \alpha = \beta u, u \in R^*$.

Proof. $\alpha = \beta x, \beta = \alpha y, x, y \in R$. Then $\alpha = \beta x = (\alpha y)x \implies \alpha(1 - yx) = 0$.

Then $\alpha = \beta = 0$ or $yx = 1 \implies x, y \in R^*$. ■

Units in $R[x]$:

If $R =$ integral domain, $(R[x])^* = R^*$.

If $R = \mathbb{Z}/4\mathbb{Z}, (R[x])^* = 1 + 2R[x]$. For $y \in R[x], (1 + 2y)^2 = 1 + 4y + 4y^2 = 1$. If $f, g \in R[x]$ satisfy $fg = 1$ then apply homomorphism: $\varphi : R[x] \to (R/(2))[x]$ to get $\varphi(f) \cdot \varphi(g) = 1$ in $(R/(2))[x] = (\mathbb{Z}/2\mathbb{Z})[x] \implies \varphi(f) = \varphi(g) = 1 \implies f, g = 1 \pmod 2 \implies f =$

$1+2A, g = 1+2B, A, B \in R[x] \implies fg = 1+2(A+B)+4AB = 1+2(A+B)$ which is 1 iff $A = B+2C \implies f = 1+2(B+2C) = 1+2B = g$.

$(\mathbb{Z}/(6)[x])^* = \{\pm 1\}$.

R, S rings, $R \times S$ with coordinate wise addiction and multiplication is a "production ring".

<u>Ring extensions</u>

Some examples:

$$\mathbb{Z}[i] = \mathbb{Z}[x]/(x^2+1), \mathbb{Z}\left[\frac{1}{2}\right] = \mathbb{Z}[x]/(2x-1)$$

If R is a ring and I is an ideal of $R[x]$, then $R[x]/I$ is a ring and $\exists f : R \to R[x]/I, r \mapsto r(x) \mapsto r + I$ is a homomorphism but not necessarily injective.

$(\mathbb{Z}/(4)[x])/(2x-1)$. Let $u =$ image of x in this ring. Then $2u = 1 \implies 0 = 4u^2 = 1 \implies$ it is a zero ring.

If $f(x)$ is a monic polynomial in $R[x]$ of degree n and $S := R[x]/(f(x))$ then each element of S can be written in exactly one way as $a(x) + (f(x))$ with $\deg(a) < n$.

Since if $g(x) \in R[x]$ then $g = fq + r$ for some unique $q, r \in R[x]$ $s.t.$ $\deg(r) < n$.

$K =$ field: $K[x]$ is a principal idea domain, so: for $f, g \in K[x]$, the ideal $(f, g) = (h)$ for some $h \in K[x]$.

So:

$$h = uf + vg, u, v \in K[x]$$
$$f = hr, g = hs, r, s \in K[x].$$

And if $w \in K[x]$ divides both f and g then $w \mid h$.

If $p(x) \in K[x]$ is irreducible (non-zero, non-unit, and not a product of two non-units) and $p \mid fg$, then $p \mid f$ or $p \mid g$.

Proof. If $p \nmid f$ then $(p, f) = (h)$ where $h \mid p$ and $h \mid f$.

Since p is irreducible, either $h = p\cdot$unit or $h =$ unit. Since $p \nmid f$, $h \neq p\cdot$unit. Hence $h =$ unit and since $(h) = 1$ we have $h = 1$.

Hence $pu + fv = 1$. Multiply both sides by g we have $pug + fvg = g$. By hypothesis fg is divisible by p. Hence $p \mid g$. ■