4th basic algebra

2022年4月23日 星期六 下午1:00

polynomial definitions. ①

division algorithm of polynomials ②

factor theorem ③

Euclidean algorithm of polynomials. ④

$P \Leftrightarrow q$ if p then q $\Leftrightarrow$ if $\neg q$ then $\neg p$

if q then p if $\neg p$ then $\neg q$ □

$P = (a_0, \cdots a_n, 0, 0 \cdots)$ ✓ we can evaluate P at r. fixed.

obtaining a result $P(r) = a_0 + a_1 r + \cdots + a_n r^n$ ⇐ $x = r$.

evaluated at r

$(5,3,0,0\cdots)$
$(3,5,7,0\cdots)$ P → $P(\cdot)$ $\begin{cases} 5 \\ 3 \\ 7 \end{cases}$

$P \in F[x]$ F.

$(P+Q)(r) = P(r) + Q(r)$

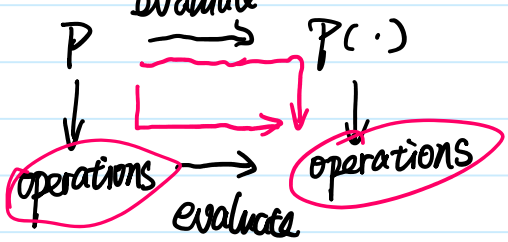
$(P-Q)(r) = P(r) - Q(r)$

$(cP)(r) = c\,P(r)$

$(PQ)(r) = P(r)\,Q(r)$

arithmetic operations.

PQR
$(ab)\cdot c = a(bc)$.



$f(ab) = f(a)f(b)$.

$f(abc) = f(ab)\cdot f(c) = f(a)f(b)f(c)$

the mapping $P \to P(\cdot)$ respects the arithmetic operations.

we say r is a root of P if $P(r) = 0$.

unique factorization.

A factor of a polynomial A is a nonzero polynomial B such that $A = BQ$ for some polynomial Q.

that $A = BQ$ for some polynomial Q.

B divides A. B is a divisor of A. A is a multiple of B.

$B \mid A$.

If A is nonzero, any product formula: $A = BQ_1 \cdots Q_r$ is a factorization of A.

A unit in $\mathbb{F}[x]$ is a divisor of 1

any polynomial of degree 0. a constant polynomial

$A(x) = c$, c is a nonzero scalar.

$A = BQ$ of $A \neq 0$ is called nontrivial if neither B nor Q is a unit.

$(5x+2) \times 2 = 10x+4$ factorization. (trivial).

unit.

A prime P in $\mathbb{F}[x]$ is a nonzero polynomial that is not a unit and has no nontrivial factorization $P = BQ$.

observe that the product of a prime and a unit is always a prime.

R: $x+1 \Rightarrow 2x+2 \Rightarrow 3x+3$ prime.

leading coefficient is 1.

division algorithm: If A and B are polynomials in $\mathbb{F}[x]$ and $B \neq 0$.

then there exist unique polynomial Q and R in $\mathbb{F}[x]$ s.t.

(a) $A = BQ + R$ and

(b) either R is the 0 polynomial or $\deg R < \deg B$.

undefined

$\frac{A}{B} = Q + \frac{R}{B}$

Quotient remainder.

proof: i) uniqueness.

$A = BQ + R = BQ_1 + R_1$

$B(Q - Q_1) = R_1 - R$ if $R_1 - R = 0$ $Q = Q_1$

if $R_1 - R \neq 0$ $\deg B + \deg(Q - Q_1) = \deg(R_1 - R) \leq \max(\deg R, \deg R_1)$.

$< \deg B$.

contradiction.

ii). existence.

If $A = 0$ or $\deg A < \deg B$ then $Q = 0$ and $R = A$. ✓

$\deg A \geq \deg B$. induct on $\deg A$. valid for $n-1$

$\deg A = n$. $A = a_n x^n + A_1$ with $A_1 = 0$ or $\deg A_1 < \deg A$.

$B = b_k x^k + B_1$ with $B_1 = 0$ or $\deg B_1 < \deg B$.

$Q_1 = a_n b_k^{-1} x^{n-k}$ Then.

$A - BQ_1 = a_n x^n + A_1 - a_n x^n - a_n b_k^{-1} x^{n-k} B_1 = A_1 - a_n b_k^{-1} x^{n-k} B_1$

$= 0$ or $\deg(\cdot) < \deg A$.

$A = B(Q_1 + Q_2) + R$. is required decomposition. $BQ_2 + R$. □.

Factor theorem. If r is in F and if P is a polynomial in $F[X]$.

then $X - r$ divides P if and only if $P(r) = 0$.

$(x-1)\cdot\cdots = P$ $P(1) = 0$

Proof: $\Rightarrow P = (x-r)\cdot Q$, $P(r) = (r-r)\cdot Q = 0$.

$\Leftarrow P(r) = 0$ take $B(x) = x - r$ in the division algorithm.

$P = (x-r)\cdot Q + R$ with $R = 0$ or $\deg R < \deg(x-r) = 1$

R is a consitant polynomial, or 0. $R = c$

$P(r) = 0 = (r-r)\cdot Q(r) + R(r)$ $R = 0$

$P(r) = 0 = (r-r)\cdot Q(r) + R(r)$ $\quad R = 0$

$P = (x-r)\cdot Q \Rightarrow x-r$ divides P. $\square$

Corollary: If P is a nonzero polynomial with coefficients in $\mathbb{F}$ and if $\deg P = n$, then P has at most n distinct roots.

$P = x^2-1$ $\deg P = 2$ $\quad P = x^8 + x^7 - x^5 + 7x^3 - 1$ $\deg P = 8$

$= (x-1)(x+1)$ $\quad x=1$ or $x=-1$

$P = x^2 - 2x + 1$ $\deg P = 2$

$= (x-1)^2$ $\quad x = 1$

$\mathbb{Q}, \mathbb{R}, \mathbb{C}$. $\quad \mathbb{F} \to 0$

observe. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$. $\quad \mathbb{F} \to P(r)$

infinite. $\quad$ cannot be identically 0.

$\mathbb{F} = \{0, 1\}$. $\quad 1+1=0$ $\quad P(x) = x^2 + x$. $\quad P(r) = 0 \Rightarrow r = 0$ or $r = 1$ ↯

proof: Let $r_1, \cdots r_{n+1}$ be distinct roots of $P(x)$

By the factor theorem: $x - r_1$ is a factor of $P(x)$,

induct $(x-r_1)(x-r_2)\cdots(x-r_k)$ is a factor of $P(x)$ ⇐

Assume it holds for k: $P(x) = (x-r_1)\cdots(x-r_k)\cdot Q(x)$.

$$0 = P(r_{k+1}) = (r_{k+1}-r_1)\cdots(r_{k+1}-r_k)\cdot Q(r_{k+1})$$

since r_j are distinct. we must have $Q(r_{k+1}) = 0$.

By factor theorem: $Q(x) = (x - r_{k+1})\cdot R(x)$ for some $R(x)$.

$$P(x) = (x-r_1)\cdots(x-r_k)(x-r_{k+1})\cdot R(x)$$

this completes the induction.

$P(x) = (x-r_1)\cdots(x-r_{n+1})\cdot S(x)$ for some polynomial $S(x)$.

$\deg = n$ $\quad \deg = n+1$

deg = n deg = n+1

deg $g(x) = -1$ contradiction. □

A greatest common divisor of polynomials A and B with $B \neq 0$. is any polynomial D of maximum degree such that D divides A and D divides B.

D is unique up to multiplication by nonzero scalar.

A: $10x+4$. B: $15x+6$.

GCD(A, B) = $5x+2$. degree = 1

$1 \to (x+\frac{2}{5})$.

$2x+\frac{4}{5}$.

Euclidean algorithm:

$A = BQ_1 + R_1$ $\quad R_1 = 0$ or $\deg R_1 < \deg B$.

$B = R_1Q_2 + R_2$ $\quad R_2 = 0$ or $\deg R_2 < \deg R_1$

$R_1 = R_2Q_3 + R_3$ $\quad R_3 = 0$ or $\deg R_3 < \deg R_2$

$\vdots$

$R_{n-2} = R_{n-1}Q_n + R_n$ $\quad R_n = 0$ or $\deg R_n < \deg R_{n-1}$

$R_{n-1} = R_n \cdot Q_{n+1} + R_{n+1}$ $\quad R_{n+1} = 0$.

such n must exist since $\deg B > \deg R_1 > \cdots \geq 0$.

n is defined as $R_n \neq 0$. $R_{n+1} = 0$

Proposition: Let A and B be polynomials in $\mathbb{F}[x]$ with $B \neq 0$. Let $R_1, \cdots R_n$ be the remainders generated by the Euclidean algorithm when applied to A and B. Then:

a) R_n is a greatest common divisor of A and B.

b) any D_1 that divides both A and B necessarily divides R_n.

c) the GCD of A and B is unique up to multiplication by a nonzero scalar ⇐.

d) any GCD D has the property that there exist polynomials.

nonzero scalar ⇐

d). any GCD. D has the property that there exist polynomials. P and Q with $AP+BQ=D$.

proof: a) and b). similarly. } d) $D=R_n$.

c) If D is a greatest common divisor of A and B.

from a), b). $\deg D = \deg R_n$. thus. C □.

lemma: If A and B are non zero polynomials with coefficients in F and if P is a prime polynomial such that P divides AB, then P divides A or P divides B.

proof: If P does not divide A then 1 is the GCD of A and P.

from ⇑ d) $AS+PT=1$.

$ABS+PTB=B$.

$P|AB$ $P|PTB$ $P|B$. □.

unique factorization of polynomials. Every member of $F[X]$ of degree ≥ 1 is a product of primes.

This factorization is unique up to order and up to multi.. of each prime factor by a unit. a non-zero scalar.

proof: induction, similarly as FToA. □.

$F=\mathbb{R}$. x^2+1 is prime. $r^2+1=0$ for some r.

$F=\mathbb{C}$ x^2+1 is not prime $x^2=(x+i)(x-i)$.

Fundamental theorem of Algebra. Any polynomial in $\mathbb{C}[X]$ with degree ≥ 1 has at least one root. ✓ $p(r)=0$

proof: 1). Liouville's theorem from complex analysis.

2) Heine-Borel theorem from real analysis.

3). compactness.

4). sylow theory. Galois theory. elementary calculus. proposition.

Proposition 4) Any polynomial in $\mathbb{R}[X]$ with odd degree has at least one root. ✓

Corollary. Let P be a nonzero polynomial of degree n in $\mathbb{C}[X]$. Let $r_1, \cdots r_k$ be the distinct roots. Then there exist unique integers $m_j > 0$ for $1 \leq j \leq k$ s.t. $P(x)$ is a scalar multiple $\prod_{j=1}^{k} (X - r_j)^{m_j}$ The number m_j have $\sum_{j=1}^{k} m_j = n$.

proof: $\deg(P) > 0$.

we apply unique factorization to $P(X)$.

up to, $15 = 5 \times 3$, 3×5

$10x+2 = (5x+1) \times 2$

in $\mathbb{C}(X)$, prime polynomial has degree 1.

in $\mathbb{R}(X)$ $n \cdots 2$.

$P(X) = c \cdot \prod_{i=1}^{n} (X - z_i)$ for some $c \neq 0$. for some complex number z_i that are unique up to order.

z_i are roots.

Grouping like factors proves the existense and uniqueness. □.

my multiplicities of the roots of the polynomial $P(x)$.

Proof: 4) $P(x)$: leading coefficient is 1.

$$P(x) = x^{2n+1} + a_{2n}x^{2n} + \cdots a_1 x + a_0 = x^{2n+1} + R(x).$$

$\to 0$

$$\lim_{x\to\pm\infty} \frac{P(x)}{x^{2n+1}} = 1$$

$x \to -\infty$: $\lim_{x\to-\infty} \frac{1}{x^{2n+1}} = 0^-$

$x \to +\infty$: $\lim_{x\to+\infty} \frac{1}{x^{2n+1}} = 0^+$

$\Rightarrow \lim_{x\to+\infty} P(x) > 0$

$\lim_{x\to-\infty} P(x) < 0$.

there is some positive r_0 s.t. $P(-r_0) < 0$

$P(r_0) > 0$.

By intermediate value theorem. ✱

$[-r_0, r_0]$ $P(r) = 0$ for some r with $-r_0 \le r \le r_0$.

□.

14 May. 4 pm. (China)