Carmen's Core Concepts (Math 135)

Carmen Bruni

University of Waterloo

Week 11 Part 1

Polynomial Statements

Let $f(x)$ and $g(x)$ be nonzero polynomials over a field $\mathbb{F}$ such that they are not additive inverses. Then

- $\deg(f(x)+g(x)) \leq \max\{\deg(f(x)), \deg(g(x))\}$
- $\deg(f(x)g(x)) = \deg(f(x)) + \deg(g(x))$
- If $f(x) \mid g(x)$ and $g(x) \mid f(x)$, then $f(x) = cg(x)$ for some $c \in \mathbb{F}$

Remainder Theorem (RT)

Theorem: (Remainder Theorem (RT)) Suppose that $f(x) \in \mathbb{F}[x]$ and that $c \in \mathbb{F}$. Then, the remainder when $f(x)$ is divided by $x - c$ is $f(c)$.

Remainder Theorem (RT)

Theorem: (Remainder Theorem (RT)) Suppose that $f(x) \in \mathbb{F}[x]$ and that $c \in \mathbb{F}$. Then, the remainder when $f(x)$ is divided by $x - c$ is $f(c)$.

Proof: By the Division Algorithm for Polynomials, there exists unique $q(x)$ and $r(x)$ in $\mathbb{F}[x]$ such that

$$f(x) = (x - c)q(x) + r(x)$$

with $r(x) = 0$ or $\deg(r(x)) < \deg(x - c) = 1$. Therefore, $\deg(r(x)) = 0$. In either case, $r(x) = k$ for some $k \in \mathbb{F}$. Plug in $x = c$ into the above equation to see that $f(c) = r(c) = k$. Hence $r(x) = f(c)$.

Factor Theorem (FT)

Theorem: (Factor Theorem (FT)) Suppose that $f(x) \in \mathbb{F}[x]$ and $c \in \mathbb{F}$. Then the polynomial $x - c$ is a factor of $f(x)$ if and only if $f(c) = 0$, that is, c is a root of $f(x)$.

Factor Theorem (FT)

Theorem: (Factor Theorem (FT)) Suppose that $f(x) \in \mathbb{F}[x]$ and $c \in \mathbb{F}$. Then the polynomial $x - c$ is a factor of $f(x)$ if and only if $f(c) = 0$, that is, c is a root of $f(x)$.

Proof: Note that $x - c$ is a factor of $f(x)$ if and only if $r(x) = 0$ via the Division Algorithm for Polynomials (DAP) which holds if and only if $r(x) = f(c) = 0$ via the Remainder Theorem (RT). ■

Roots Over a Field

Proposition: Prove that a polynomial over any field $\mathbb{F}$ of degree $n \geq 1$ has at most n roots.

Proof: Let $P(n)$ be the statement that all polynomials over $\mathbb{F}$ of degree n have at most n roots. We prove this by induction on n.

Roots Over a Field

Proposition: Prove that a polynomial over any field $\mathbb{F}$ of degree $n \geq 1$ has at most n roots.

Proof: Let $P(n)$ be the statement that all polynomials over $\mathbb{F}$ of degree n have at most n roots. We prove this by induction on n.

Base Case: If $n = 1$, let $ax + b \in \mathbb{F}[x]$, with $a \neq 0$. Solving for a root gives $x = -a^{-1}b$ which exists since a is a nonzero element in a field and hence has a multiplicative inverse.

Roots Over a Field

Proposition: Prove that a polynomial over any field $\mathbb{F}$ of degree $n \geq 1$ has at most n roots.

Proof: Let $P(n)$ be the statement that all polynomials over $\mathbb{F}$ of degree n have at most n roots. We prove this by induction on n.

Base Case: If $n = 1$, let $ax + b \in \mathbb{F}[x]$, with $a \neq 0$. Solving for a root gives $x = -a^{-1}b$ which exists since a is a nonzero element in a field and hence has a multiplicative inverse.

Induction Hypothesis: Assume that $P(k)$ is true for some $k \in \mathbb{N}$.

Roots Over a Field

Proposition: Prove that a polynomial over any field $\mathbb{F}$ of degree $n \geq 1$ has at most n roots.

Proof: Let $P(n)$ be the statement that all polynomials over $\mathbb{F}$ of degree n have at most n roots. We prove this by induction on n.

Base Case: If $n = 1$, let $ax + b \in \mathbb{F}[x]$, with $a \neq 0$. Solving for a root gives $x = -a^{-1}b$ which exists since a is a nonzero element in a field and hence has a multiplicative inverse.

Induction Hypothesis: Assume that $P(k)$ is true for some $k \in \mathbb{N}$.

Inductive step: Let $p(x) \in \mathbb{F}[x]$ be a degree $k+1$ polynomial. Either $p(x)$ has no root in which case we are done or $p(x)$ has a root, say $c \in \mathbb{F}$. By the Factor Theorem, $x - c$ is a factor of $p(x)$. Write $p(x) = (x - c)q(x)$ for some $q(x) \in \mathbb{F}[x]$ of degree k. By the inductive hypothesis, $q(x)$ has at most k roots. Thus, $p(x)$ has at most $k + 1$ roots. Therefore, by the Principle of Mathematical Induction, $P(n)$ is true for all natural numbers n. ■

Fundamental Theorem of Algebra (FTA)

Theorem: (Fundamental Theorem of Algebra (FTA)) Every non-constant complex polynomial has a complex root.

Fundamental Theorem of Algebra (FTA)

Theorem: (Fundamental Theorem of Algebra (FTA)) Every non-constant complex polynomial has a complex root.

The polynomial $x^2 + 1$ over $\mathbb{R}$ shows that this does not happen over all fields.

Complex Polynomials of Degree n Have n Roots (CPN)

Theorem: (Complex Polynomials of Degree n Have n Roots (CPN)) A complex polynomial $f(z)$ of degree $n \geq 1$ can be written as

$$f(z) = c(z - c_1)(z - c_2)...(z - c_n)$$

for some $c \in \mathbb{C}$ where $c_1, c_2, ..., c_n \in \mathbb{C}$ are the (not necessarily distinct) roots of $f(z)$.

Example: The polynomial $2z^7 + z^5 + iz + 7$ can be written as

$$2(z - z_1)(z - z_2)...(z - z_7)$$

for some roots $z_1, z_2, ..., z_7 \in \mathbb{C}$.

CPN Proof

Proof: (of CPN) We prove that a complex polynomial $f(z)$ of degree $n \geq 1$ can be written as $f(z) = c(z - c_1)(z - c_2)...(z - c_n)$.
Base Case: When $n = 1$, take $az + b \in \mathbb{C}[z]$ where $a \neq 0$ and rewrite this as $a(z - \frac{-b}{a})$.

CPN Proof

Proof: (of CPN) We prove that a complex polynomial $f(z)$ of degree $n \geq 1$ can be written as $f(z) = c(z - c_1)(z - c_2)...(z - c_n)$.
Base Case: When $n = 1$, take $az + b \in \mathbb{C}[z]$ where $a \neq 0$ and rewrite this as $a(z - \frac{-b}{a})$.
Inductive Hypothesis: Assume all polynomials over $\mathbb{C}$ of degree k can be written in the given form for some $k \in \mathbb{N}$.

CPN Proof

Proof: (of CPN) We prove that a complex polynomial $f(z)$ of degree $n \geq 1$ can be written as $f(z) = c(z - c_1)(z - c_2)...(z - c_n)$.
Base Case: When $n = 1$, take $az + b \in \mathbb{C}[z]$ where $a \neq 0$ and rewrite this as $a(z - \frac{-b}{a})$.
Inductive Hypothesis: Assume all polynomials over $\mathbb{C}$ of degree k can be written in the given form for some $k \in \mathbb{N}$.
Inductive Step: Take $f(z) \in \mathbb{C}[z]$ of degree $k + 1$. By the Fundamental Theorem of Algebra and the Factor Theorem there is a factor $z - c_{k+1}$ of $f(z)$ for some $c_{k+1} \in \mathbb{C}$. Write $f(z) = (z - c_{k+1})g(z)$ where $g(z)$ has degree k. By the inductive hypothesis, write $g(z) = c(z - c_1)...(z - c_k)$ for $c_1, c_2, ...c_k \in \mathbb{C}$. Combine to get

$$f(z) = c \prod_{i=1}^{k+1} (z - c_i).$$

Therefore, by the Principle of Mathematical Induction, the given statement is true for all $n \in \mathbb{N}$.

Rational Roots Theorem (RRT)

Theorem: Rational Roots Theorem (RRT) If $f(x) = a_n x^n + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$ and $r = \frac{s}{t} \in \mathbb{Q}$ is a root of $f(x)$ over $\mathbb{Q}$ in lowest terms, then $s \mid a_0$ and $t \mid a_n$.

Rational Roots Theorem (RRT)

Theorem: Rational Roots Theorem (RRT) If $f(x) = a_n x^n + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$ and $r = \frac{s}{t} \in \mathbb{Q}$ is a root of $f(x)$ over $\mathbb{Q}$ in lowest terms, then $s \mid a_0$ and $t \mid a_n$.

Proof: Plug r into $f(x)$:

$$0 = a_n(\tfrac{s}{t})^n + \ldots + a_1(\tfrac{s}{t}) + a_0.$$

Multiply by t^n

$$0 = a_n s^n + a_{n-1} s^{n-1} t + \ldots + a_1 s t^{n-1} + a_0 t^n.$$

Rearranging gives

$$a_0 t^n = -s(a_n s^{n-1} + a_{n-1} s^{n-2} t + \ldots + a_1 t^{n-1})$$

and hence $s \mid a_0 t^n$. Since $\gcd(s, t) = 1$, we see that $\gcd(s, t^n) = 1$ and hence $s \mid a_0$ by Coprimeness and Divisibility. Similarly, $t \mid a_n$.

Conjugate Roots Theorem (CJRT)

Theorem: (Conjugate Roots Theorem (CJRT)) If $c \in \mathbb{C}$ is a root of a polynomial $p(x) \in \mathbb{R}[x]$ (over $\mathbb{C}$) then $\overline{c}$ is a root of $p(x)$.

Conjugate Roots Theorem (CJRT)

Theorem: (Conjugate Roots Theorem (CJRT)) If $c \in \mathbb{C}$ is a root of a polynomial $p(x) \in \mathbb{R}[x]$ (over $\mathbb{C}$) then $\overline{c}$ is a root of $p(x)$.

Proof: Write $p(x) = a_n x^n + \ldots + a_1 x + a_0 \in \mathbb{R}[x]$ with $p(c) = 0$. Then:

$$\begin{aligned} p(\overline{c}) &= a_n(\overline{c})^n + \ldots + a_1\overline{c} + a_0 \\ &= \overline{a_n(c)^n} + \ldots + \overline{a_1 c} + \overline{a_0} && \text{Since coefficients are real and PCJ.} \\ &= \overline{a_n(c)^n + \ldots + a_1 c + a_0} && \text{By PCJ} \\ &= \overline{p(c)} \\ &= 0 \end{aligned}$$