Commuting Polynomials and Fermat's Little Theorem

Karl Zimmermann

Union College
Schenectady, NY

April 6, 2013

All polynomials in this talk will have real number coefficients.

All polynomials in this talk will have real number coefficients.

Definition 1

Let $f(x)$ and $g(x)$ be polynomials. Then f and g commute under composition provided $(f \circ g)(x) = (g \circ f)(x)$.

All polynomials in this talk will have real number coefficients.

Definition 1

Let $f(x)$ and $g(x)$ be polynomials. Then f and g commute under composition provided $(f \circ g)(x) = (g \circ f)(x)$.

In other words, $f(g(x)) = g(f(x))$.

Example

Let f be any polynomial. Then f commutes with itself. More generally, let f^n denote f composed with itself n-times.

Then f commutes with f^n.

Example

Let f be any polynomial. Then f commutes with itself. More generally, let f^n denote f composed with itself n-times.

Then f commutes with f^n.

$f \circ f^n =$

Example

Let f be any polynomial. Then f commutes with itself. More generally, let f^n denote f composed with itself n-times.

Then f commutes with f^n.

$f \circ f^n = f \circ (f \circ f \cdots \circ f) =$

Example

Let f be any polynomial. Then f commutes with itself. More generally, let f^n denote f composed with itself n-times.

Then f commutes with f^n.

$$f \circ f^n = f \circ (f \circ f \cdots \circ f) = (f \circ f \cdots \circ f) \circ f =$$

Example

Let f be any polynomial. Then f commutes with itself. More generally, let f^n denote f composed with itself n-times.

Then f commutes with f^n.

$$f \circ f^n = f \circ (f \circ f \cdots \circ f) = (f \circ f \cdots \circ f) \circ f = f^n \circ f$$

Example

Let f be any polynomial. Then f commutes with itself. More generally, let f^n denote f composed with itself n-times.

Then f commutes with f^n.

$$f \circ f^n = f \circ (f \circ f \cdots \circ f) = (f \circ f \cdots \circ f) \circ f = f^n \circ f$$

Recall that when we compose polynomials, we multiply the degrees.

Example

Let f be any polynomial. Then f commutes with itself. More generally, let f^n denote f composed with itself n-times.

Then f commutes with f^n.

$$f \circ f^n = f \circ (f \circ f \cdots \circ f) = (f \circ f \cdots \circ f) \circ f = f^n \circ f$$

Recall that when we compose polynomials, we multiply the degrees.

Thus, if the degree of f is a, then the degree of f^n is a^n.

Definition 2

$\alpha \in \mathbf{C}$ is a fixed point of f provided $f(\alpha) = \alpha$

Definition 2

$\alpha \in \mathbf{C}$ is a fixed point of f provided $f(\alpha) = \alpha$

Note that if $\deg f = n \geq 2$, the fixed points of f are the roots of the polynomial $g(x) = f(x) - x$.

Definition 2

$\alpha \in \mathbf{C}$ is a fixed point of f provided $f(\alpha) = \alpha$

Note that if $\deg f = n \geq 2$, the fixed points of f are the roots of the polynomial $g(x) = f(x) - x$.

$g(\alpha) = 0$

Definition 2

$\alpha \in \mathbf{C}$ is a fixed point of f provided $f(\alpha) = \alpha$

Note that if $\deg f = n \geq 2$, the fixed points of f are the roots of the polynomial $g(x) = f(x) - x$.

$$g(\alpha) = 0 \iff f(\alpha) - \alpha = 0$$

Definition 2

$\alpha \in \mathbf{C}$ is a fixed point of f provided $f(\alpha) = \alpha$

Note that if $\deg f = n \geq 2$, the fixed points of f are the roots of the polynomial $g(x) = f(x) - x$.

$$g(\alpha) = 0 \iff f(\alpha) - \alpha = 0 \iff f(\alpha) = \alpha.$$

Definition 2

$\alpha \in \mathbf{C}$ is a fixed point of f provided $f(\alpha) = \alpha$

Note that if $\deg f = n \geq 2$, the fixed points of f are the roots of the polynomial $g(x) = f(x) - x$.

$$g(\alpha) = 0 \iff f(\alpha) - \alpha = 0 \iff f(\alpha) = \alpha.$$

So since $g(x)$ can have at most n roots, f can have at most n fixed points.

Lemma

Let f and h commute under composition and let α be a fixed point of h. Then $f(\alpha)$ is a fixed point of h.

Lemma

Let f and h commute under composition and let α be a fixed point of h. Then $f(\alpha)$ is a fixed point of h.

Proof: $h(f(\alpha)) =$

Lemma

Let f and h commute under composition and let α be a fixed point of h. Then $f(\alpha)$ is a fixed point of h.

Proof: $h(f(\alpha)) = f(h(\alpha)) =$

Lemma

Let f and h commute under composition and let α be a fixed point of h. Then $f(\alpha)$ is a fixed point of h.

Proof: $h(f(\alpha)) = f(h(\alpha)) = f(\alpha)$. QED

Lemma

Let f and h commute under composition and let α be a fixed point of h. Then $f(\alpha)$ is a fixed point of h.

Proof: $h(f(\alpha)) = f(h(\alpha)) = f(\alpha)$. QED

Notation: Let $\mathcal{F}_h$ denote the set of fixed points of h.

Lemma

Let f and h commute under composition and let α be a fixed point of h. Then $f(\alpha)$ is a fixed point of h.

Proof: $h(f(\alpha)) = f(h(\alpha)) = f(\alpha)$. QED

Notation: Let $\mathcal{F}_h$ denote the set of fixed points of h.

Corollary

Let f commute with h. Then we have a function, $f : \mathcal{F}_h \to \mathcal{F}_h$ given by $\alpha \mapsto f(\alpha)$.

Example

If f commutes with g then $f \circ (f \circ g) =$

Example

If f commutes with g then $f \circ (f \circ g) = f \circ (g \circ f) =$

Example

If f commutes with g then $f \circ (f \circ g) = f \circ (g \circ f) = (f \circ g) \circ f$.

Example

If f commutes with g then $f \circ (f \circ g) = f \circ (g \circ f) = (f \circ g) \circ f$.

In other words, f commutes with $f \circ g$.

Example

If f commutes with g then $f \circ (f \circ g) = f \circ (g \circ f) = (f \circ g) \circ f$.

In other words, f commutes with $f \circ g$.

By the corollary, letting $h = f \circ g$, we have a function

$f : \mathcal{F}_{f \circ g} \to \mathcal{F}_{f \circ g}$.

Theorem

If f and g are polynomials that commute under composition then $f : \mathcal{F}_{f \circ g} \to \mathcal{F}_{f \circ g}$ is a bijection.

Theorem

If f and g are polynomials that commute under composition then $f : \mathcal{F}_{f \circ g} \to \mathcal{F}_{f \circ g}$ is a bijection.

Proof: f is invertible with inverse g.

Theorem

If f and g are polynomials that commute under composition then $f : \mathcal{F}_{f \circ g} \to \mathcal{F}_{f \circ g}$ is a bijection.

Proof: f is invertible with inverse g.

Let $\alpha \in \mathcal{F}_{f \circ g}$.

Theorem

If f and g are polynomials that commute under composition then $f : \mathcal{F}_{f \circ g} \to \mathcal{F}_{f \circ g}$ is a bijection.

Proof: f is invertible with inverse g.

Let $\alpha \in \mathcal{F}_{f \circ g}$. Then $(f \circ g)(\alpha) = \alpha = \mathrm{Id}(\alpha)$.

Theorem

If f and g are polynomials that commute under composition then $f : \mathcal{F}_{f \circ g} \to \mathcal{F}_{f \circ g}$ is a bijection.

Proof: f is invertible with inverse g.

Let $\alpha \in \mathcal{F}_{f \circ g}$. Then $(f \circ g)(\alpha) = \alpha = \mathrm{Id}(\alpha)$.

Since $f \circ g = g \circ f$, it's clear that $\mathcal{F}_{f \circ g} = \mathcal{F}_{g \circ f}$,

Theorem

If f and g are polynomials that commute under composition then $f : \mathcal{F}_{f \circ g} \to \mathcal{F}_{f \circ g}$ is a bijection.

Proof: f is invertible with inverse g.

Let $\alpha \in \mathcal{F}_{f \circ g}$. Then $(f \circ g)(\alpha) = \alpha = \mathrm{Id}(\alpha)$.

Since $f \circ g = g \circ f$, it's clear that $\mathcal{F}_{f \circ g} = \mathcal{F}_{g \circ f}$, so $\alpha \in \mathcal{F}_{g \circ f}$.

Theorem

If f and g are polynomials that commute under composition then $f : \mathcal{F}_{f \circ g} \to \mathcal{F}_{f \circ g}$ is a bijection.

Proof: f is invertible with inverse g.

Let $\alpha \in \mathcal{F}_{f \circ g}$. Then $(f \circ g)(\alpha) = \alpha = \mathrm{Id}(\alpha)$.

Since $f \circ g = g \circ f$, it's clear that $\mathcal{F}_{f \circ g} = \mathcal{F}_{g \circ f}$, so $\alpha \in \mathcal{F}_{g \circ f}$.

Therefore $(g \circ f)(\alpha) = \alpha = \mathrm{Id}(\alpha)$. QED

Setting

In the theorem, let $g = f^{p-1}$ where p is a prime integer.

Setting

In the theorem, let $g = f^{p-1}$ where p is a prime integer.

Then $f \circ g =$

Setting

In the theorem, let $g = f^{p-1}$ where p is a prime integer.

Then $f \circ g = f \circ f^{p-1} =$

Setting

In the theorem, let $g = f^{p-1}$ where p is a prime integer.

Then $f \circ g = f \circ f^{p-1} = f^p$ and

Setting

In the theorem, let $g = f^{p-1}$ where p is a prime integer.

Then $f \circ g = f \circ f^{p-1} = f^p$ and $f : \mathcal{F}_{f^p} \to \mathcal{F}_{f^p}$ is a bijection.

Setting

In the theorem, let $g = f^{p-1}$ where p is a prime integer.

Then $f \circ g = f \circ f^{p-1} = f^p$ and $f : \mathcal{F}_{f^p} \to \mathcal{F}_{f^p}$ is a bijection.

Note 1

If the degree of f is a, then the degree of f^p is a^p. It follows that f^p has at most a^p fixed points. In other words $|\mathcal{F}_{f^p}| \leq a^p$. We'll choose f so that $|\mathcal{F}_{f^p}| = a^p$.

Setting

In the theorem, let $g = f^{p-1}$ where p is a prime integer.

Then $f \circ g = f \circ f^{p-1} = f^p$ and $f : \mathcal{F}_{f^p} \to \mathcal{F}_{f^p}$ is a bijection.

Note 1

If the degree of f is a, then the degree of f^p is a^p. It follows that f^p has at most a^p fixed points. In other words $|\mathcal{F}_{f^p}| \leq a^p$. We'll choose f so that $|\mathcal{F}_{f^p}| = a^p$.

Note 2

Observe that $\mathcal{F}_f \subseteq \mathcal{F}_{f^p}$. If $f(\alpha) = \alpha$ then $f(f(\alpha)) = f(\alpha) = \alpha$. Continue ...

Now, since $f : \mathcal{F}_{f^p} \to \mathcal{F}_{f^p}$ is a bijection of finite sets and

Now, since $f : \mathcal{F}_{f^p} \to \mathcal{F}_{f^p}$ is a bijection of finite sets and

f maps any element of $\mathcal{F}_f$ to itself,

Now, since $f : \mathcal{F}_{f^p} \to \mathcal{F}_{f^p}$ is a bijection of finite sets and

f maps any element of $\mathcal{F}_f$ to itself,

it follows that f must map the points that aren't fixed by f to the points that aren't fixed by f.

Now, since $f : \mathcal{F}_{f^p} \to \mathcal{F}_{f^p}$ is a bijection of finite sets and

f maps any element of $\mathcal{F}_f$ to itself,

it follows that f must map the points that aren't fixed by f to the points that aren't fixed by f.

Corollary

Let f be a polynomial. Then $f : \mathcal{F}_{f^p} \setminus \mathcal{F}_f \to \mathcal{F}_{f^p} \setminus \mathcal{F}_f$ is a bijection.

Fermat's Little Theorem

Let $a, p \in \mathbf{Z}$ with p a prime. Then $a^p \equiv a \pmod{p}$.

Fermat's Little Theorem

Let $a, p \in \mathbf{Z}$ with p a prime. Then $a^p \equiv a \pmod{p}$.

Proof: We want to show that $p \mid a^p - a$ for all $a \in \mathbf{Z}$.

Fermat's Little Theorem

Let $a, p \in \mathbf{Z}$ with p a prime. Then $a^p \equiv a \pmod{p}$.

Proof: We want to show that $p \mid a^p - a$ for all $a \in \mathbf{Z}$.

Let $a \geq 2$ and let f be any polynomial of degree a such that f^p has a^p distinct fixed points.

Fermat's Little Theorem

Let $a, p \in \mathbf{Z}$ with p a prime. Then $a^p \equiv a \pmod{p}$.

Proof: We want to show that $p \mid a^p - a$ for all $a \in \mathbf{Z}$.

Let $a \geq 2$ and let f be any polynomial of degree a such that f^p has a^p distinct fixed points.

Let $S = \mathcal{F}_{f^p} \setminus \mathcal{F}_f$. Then $|S| = a^p - a$ and $f : S \to S$ is a permutation.

Fermat's Little Theorem

Let $a, p \in \mathbf{Z}$ with p a prime. Then $a^p \equiv a \pmod{p}$.

Proof: We want to show that $p \mid a^p - a$ for all $a \in \mathbf{Z}$.

Let $a \geq 2$ and let f be any polynomial of degree a such that f^p has a^p distinct fixed points.

Let $S = \mathcal{F}_{f^p} \setminus \mathcal{F}_f$. Then $|S| = a^p - a$ and $f : S \to S$ is a permutation.

Note that $f^p(\alpha) = \alpha$ for all $\alpha \in S$ since $S \subseteq \mathcal{F}_{f^p}$.

It follows that $f^p = \mathrm{Id}$, in other words, the order of f is p.

It follows that $f^p = \mathrm{Id}$, in other words, the order of f is p.

But f can be written as a product of it's disjoint cycles, say $f = (\quad\quad)(\quad\quad)\ldots(\quad\quad)$ and the order of f is the lcm of the lengths of these disjoint cycles.

It follows that $f^p = \mathrm{Id}$, in other words, the order of f is p.

But f can be written as a product of it's disjoint cycles, say $f = (\quad)(\quad)\ldots(\quad)$ and the order of f is the lcm of the lengths of these disjoint cycles.

But since the lcm of all the lengths is p, all cycles must be of length 1 or p,

It follows that $f^p = \mathrm{Id}$, in other words, the order of f is p.

But f can be written as a product of it's disjoint cycles, say $f = (\quad)(\quad)\ldots(\quad)$ and the order of f is the lcm of the lengths of these disjoint cycles.

But since the lcm of all the lengths is p, all cycles must be of length 1 or p, ie, all are of length p.

It follows that $f^p = \mathrm{Id}$, in other words, the order of f is p.

But f can be written as a product of it's disjoint cycles, say $f = (\quad)(\quad)\ldots(\quad)$ and the order of f is the lcm of the lengths of these disjoint cycles.

But since the lcm of all the lengths is p, all cycles must be of length 1 or p, ie, all are of length p.

If there are k such cycles, $a^p - a = kp$, so $p \mid a^p - a$.

Probably the easiest polynomial of degree $a \geq 2$ with p^{th} iterate having a^p distinct roots is $f(x) = x^a$.

In this case, $f^p(x) = x^{a^p}$ which has fixed points the roots of $x^{a^p} - x$.

Here are two papers using iteration of functions / fixed points to prove Fermat's Little Theorem.

Here are two papers using iteration of functions / fixed points to prove Fermat's Little Theorem.

1. "Fixed Points and Fermat: A Dynamical Systems Approach to Number Theory," by Michael Frame, Brenda Johnson, and Jim Sauerberg, The American Mathematical Monthly, Volume 107, No. 5 (May 2000), pp 422 - 428.

2. "Fermat's little theorem: a proof by function iteration," Lionel Levine, Mathematics Magazine 72, no 4 (1999), 308 - 309.