# Lecture 08 : Fermat's little theorem

Thursday, February 21, 2019 2:34 AM

In the previous lecture we defined the evaluation map and pointed out that two poly. might give us the same functions.

Fermat's little theorem gives us one such example:

<u>Theorem</u>. Suppose $p$ is prime. Then, for any $a \in \mathbb{Z}_p$,

$$a^p = a.$$

<u>Pf.</u> $\mathbb{Z}_p$ has characteristic $p$. In your HW assignment you have proved that $(x+y)^p = x^p + y^p$ in $\mathbb{Z}_p$. ⊛

<u>Claim</u>. $(x_1+x_2+\cdots+x_n)^p = x_1^p+\cdots+x_n^p$ for any $x_i \in \mathbb{Z}_p$.

<u>Pf of claim</u>. We proceed by induction on $n$. ⊛ implies the $n=2$ case.

<u>Induction Step.</u> $((x_1+\cdots+x_n)+x_{n+1})^p \overset{\text{by ⊛}}{=} (x_1+\cdots+x_n)^p + x_{n+1}^p$

$$= x_1^p + \cdots + x_n^p + x_{n+1}^p \quad \text{(induction hypothesis)}$$

For $a \in \mathbb{Z}_p$, $a^p = (\underbrace{1+1+\cdots+1}_{a \text{ times}})^p \underset{\text{by the above claim}}{=} \underbrace{1^p+\cdots+1^p}_{\text{times}} = \underbrace{1+\cdots+1}_{a \text{ times}} = a.$ ∎

# Lecture 08: Evaluation map

Friday, February 22, 2019 1:48 PM

Let's recall the evaluation map: Suppose $A$ is a subring of $B$ and $b \in B$. Then the evaluation at $b$ $\phi_b : A[x] \to B$, $\phi_b(f) = f(b)$ is a ring homomorphism

$\operatorname{Im} \phi_b = \{ a_0 + a_1 b + \cdots + a_n b^n \mid a_i \in A,\ n \in \mathbb{Z}^+ \}$ and

$\ker \phi_b = \{ f(x) \in A[x] \mid b \text{ is a zero of } f(x) \}$.

Ex. Find $\ker(\phi_{\sqrt{2}})$ where $\phi_{\sqrt{2}} : \mathbb{Q}[x] \to \mathbb{C}$ is the evaluation at $\sqrt{2}$.

Solution. $f \in \ker \phi_{\sqrt{2}} \Leftrightarrow f(\sqrt{2}) = 0$.

Notice that $(\sqrt{2})^2 - 2 = 0$; and so $\sqrt{2}$ is a zero of $x^2 - 2$. Next we notice that since $\sqrt{2}$ is irrational, it is not a zero of a degree 1 polynomial in $\mathbb{Q}[x]$:

$$\left.\begin{array}{r} a(\sqrt{2}) + b = 0 \\ a \neq 0 \\ a, b \in \mathbb{Q} \end{array}\right\} \Rightarrow \sqrt{2} = -b/a \in \mathbb{Q}$$ which is a contradiction.

Claim. $\ker \phi_{\sqrt{2}} = (x^2 - 2)\,\mathbb{Q}[x]$ (all the multiples of $x^2 - 2$.)

Pf of Claim. $f(x) = (x^2 - 2)\,q(x) \Rightarrow f(\sqrt{2}) = (\sqrt{2}^2 - 2)\,q(\sqrt{2}) = 0$

# Lecture 08: The evaluation homomorphisms

Friday, August 18, 2017

$\Rightarrow f(x) \in \ker \phi_{\sqrt{2}}$. Suppose $g(x) \in \ker \phi_{\sqrt{2}}$; we have to show $g(x)$ is a multiple of $x^2-2$. So we divide $g(x)$ by $x^2-2$; and we have to argue why remainder is $0$. By long division $\exists\, q, r \in \mathbb{Q}[x]$, $g(x) = (x^2-2)q(x) + r(x)$, $\deg r < 2$.

$$\Rightarrow 0 = g(\sqrt{2}) = \underbrace{(\sqrt{2}^2-2)}_{0} q(\sqrt{2}) + r(\sqrt{2}) = r(\sqrt{2}).$$

Since $\ker \phi_{\sqrt{2}}$ has no degree 1 element, $\deg r < 2$, and $r(\sqrt{2}) = 0$, we deduce that $r(x) = c$ is constant. As $r(\sqrt{2}) = 0$, we have $r(x) = 0$; and so $g(x) = (x^2-2)q(x) \in (x^2-2)\mathbb{Q}[x]$. ■

<u>Ex.</u> Is there a non-zero element in $\ker \phi_\pi$ where $\phi_\pi : \mathbb{Q}[x] \to \mathbb{C}$ is the evaluation at the Pi?

<u>Solution.</u> No, it is a not-so-easy theorem in number theory that $\pi$ is NOT a zero of a polynomial with rational coefficients. Such a number is called a transcendental number. ■

# Lecture 08: Factor theorem

Friday, August 18, 2017 12:29 AM

<u>Def.</u> $a \in \mathbb{C}$ is called <u>algebraic</u> if $\ker \phi_a \neq \{0\}$

where $\phi_a : \mathbb{Q}[x] \to \mathbb{C}$ is the evaluation at $a$.

- $a \in \mathbb{C}$, which is not algebraic, is called a <u>transcendental</u> number.

Next we use the division algorithm to study zeros of a polynomial.

<u>Factor theorem.</u> Let $R$ be an integral domain and $f(x) \in R[x]$. Then $a \in R$ is a zero of $f$ if and only if $f(x) = (x-a)\, q(x)$ for some $q(x) \in R[x]$.

<u>Pf.</u> ($\Rightarrow$) Since the leading coeff. of $x-a$ is $1$ and $1 \in U(R)$, by the division algorithm $\exists\, q(x), r(x) \in R[x]$ s.t.

① $\deg r < \deg(x-a) = 1$. $\rightsquigarrow$ $r$ is constant.

② $f(x) = (x-a)\,q(x) + r(x)$

Since $a$ is a zero of $f$, ② implies

$$0 = f(a) = (a-a)\,q(a) + r(a) \; ; \text{ and so } r(a) = 0.$$

Since $r$ is constant, we get that $r(x)=r(a)=0$.

So $f(x)=(x-a)q(x)$. And so $a$ is a zero of $f$. ∎

<u>Theorem</u>. Let $D$ be an integral domain, and $f(x)\in D[x]$.

Suppose $a_1,\ldots,a_k$ are distinct zeros of $f(x)$. Then

$\exists q(x)\in D[x]$ s.t. $f(x)=(x-a_1)\cdots(x-a_k)\,q(x)$.

In particular, a polynomial $f$ has at most $\deg(f)$ zeros.

<u>Pf</u>. We proceed by induction on $k$.

<u>Base of induction</u>. $k=1$.

$a_1$ is a zero of $f$. So by the factor theorem,

$f(x)=(x-a_1)\,q(x)$ for some $q(x)\in D[x]$; this

proves the base of induction.

<u>Induction step</u>. Suppose $a_1,\ldots,a_{k+1}$ are distinct zeros

of $f(x)$.

Since $a_{k+1}$ is a zero of $f$, by the factor theorem

$\exists\, h(x)\in D[x]$ s.t. $f(x)=(x-a_{k+1})\,h(x)$. So, for any

# Lecture 08 : Zeros of a polynomial

Friday, August 18, 2017 2:15 PM

$1 \le i \le k$, $0 = f(a_i) = (a_i - a_{k+1})\, h(a_i)$. Since

$$\left.\begin{array}{l} 0 = (a_i - a_{k+1})\, h(a_i) \\ a_i \ne a_{k+1} \text{ for } 1 \le i \le k \\ D \text{ has no zero-divisor} \end{array}\right\} \Rightarrow h(a_1) = h(a_2) = \cdots = h(a_k) = 0.$$

So $a_1, \ldots, a_k$ are distinct zeros of $h$. Hence by the induction hypothesis we have that

$$h(x) = (x-a_1)\cdots(x-a_k)\, q(x)$$

for some $q(x) \in D[x]$. Therefore

$$f(x) = (x - a_{k+1})\, h(x) = (x-a_1)\cdots(x-a_k)(x-a_{k+1})\, q(x).$$

This gives us the first part of theorem.

To get the second part of theorem, we have

$$\deg f = \deg\big((x-a_1)\cdots(x-a_k)\, q(x)\big) = k + \deg q,$$

which implies $\deg f \ge k$. So $f$ has at most $\deg(f)$ zeros. ■

# Lecture 08 :Zeros of a polynomial

Friday, August 18, 2017 2:24 PM

Notice that $x^2-1$ has 4 zeros in $\mathbb{Z}_{15}$.

$(\pm 1)^2 = 1$ in $\mathbb{Z}_{15}$ and $(\pm 4)^2 = 1$ in $\mathbb{Z}_{15}$; hence

in the previous statement it is important that D is an integral domain. We can use Chinese Remainder Theorem to show that $x^2-1$ has exactly 4 solutions in $\mathbb{Z}_{15}$. By CRT, $\mathbb{Z}_{15} \simeq \mathbb{Z}_3 \times \mathbb{Z}_5$; since $\mathbb{Z}_3$ and $\mathbb{Z}_5$ are field, $x^2-1$ has at most two zeros in $\mathbb{Z}_3$ and $\mathbb{Z}_5$; and they are $\pm 1$.

So $x^2-1$ has exactly 4 zeros in $\mathbb{Z}_3 \times \mathbb{Z}_5$ which are $(\pm 1, \pm 1)$.

# Lecture 08: Fermat's theorem and finding zeros

Friday, August 18, 2017 12:16 AM

Next we see how Fermat's little theore can help us determine if a given polynomial has a zero in $\mathbb{Z}_p$ or not.

It is essentially based on the following observation:

__Lemma__. For any prime $p$, positive integer $n$, and $a \in \mathbb{Z}_p$, $a^{(p^n)} = a$ in $\mathbb{Z}_p$.

__Pf.__ We proceed by induction on $n$. Fermat's little theorem gives us the base case of $n=1$. __Induction Step__.

$$a^{(p^{n+1})} = \left(a^{(p^n)}\right)^p \underset{\uparrow}{=} a^{(p^n)} \underset{\uparrow}{=} a.$$

Fermat's little theorem    Induction hypothesis ∎

__Ex__. Does $x^{(5^{10})} - x + 2$ have a zero in $\mathbb{Z}_5$?

__Solution__. By the previous lemma, for any $a \in \mathbb{Z}_5$, we have $a^{(5^{10})} - a + 2 = a - a + 2 = 2 \neq 0$. So $x^{(5^{10})} - x + 2$ does not have a zero in $\mathbb{Z}_5$. ∎

# Lecture 08: Finding zeros and Fermat's theorem

Monday, August 21, 2017 9:52 PM

Ex. Does $x^{50} - x + 2$ have a zero in $\mathbb{Z}_5$?

Solution. We write 50 in base-5: $50 = (5^2)(2)$.

For any $a \in \mathbb{Z}_5$, $a^{50} - a + 2 = (a^2)^{(5^2)} - a + 2$

$$= a^2 - a + 2.$$

Now that we have a polynomial with small degree we can evaluate at all the elements of $\mathbb{Z}_5$.

| $a$ | 0 | 1 | -1 | 2 | -2 |
|---|---|---|---|---|---|
| $a^2-a+2$ | 2 | 2 | 4 | 4 | 3 |

So $x^{50} - x + 2$ does not have a zero in $\mathbb{Z}_5$. ∎