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 polynomials might give us the same functions.

Fermat's little theorem gives us one such example:

**Theorem.** Suppose \( p \) is prime. Then, for any \( a \in \mathbb{Z}_p \),

\[ a^p = a. \]

**Proof.** \( \mathbb{Z}_p \) has characteristic \( p \). In your HW assignment you have proved that \((x+y)^p = x^p + y^p \) in \( \mathbb{Z}_p \).

**Claim.** \((x_1 + x_2 + \cdots + x_n)^p = x_1^p + \cdots + x_n^p \) for any \( x_i \in \mathbb{Z}_p \).

**Proof of claim.** We proceed by induction on \( n \). By the above implies the \( n=2 \) case.

**Induction Step.** \((x_1 + \cdots + x_n + x_{n+1})^p = (x_1 + \cdots + x_n)^p + x_{n+1}^p \)

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

For \( a \in \mathbb{Z}_p \), \( a^p = (1+1+\cdots+1)^p = 1^p + \cdots + 1^p = 1 + \cdots + 1 = a. \)

(\( a \) times) (\( a \) times) (by the above claim)
Lecture 08: Evaluation map

Let's recall the evaluation map: Suppose $A$ is a subring of $B$ and $b \in B$. Then the evaluation at $b$

\[ \phi_b : A[x] \rightarrow B, \quad \phi_b(f) = f(b) \]

is a ring homomorphism

\[ \text{Im } \phi_b = \{ \sum a_n x^n : a_n \in A, n \in \mathbb{Z}^+ \} \]

and

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

Ex. Find \( \ker(\phi_{\sqrt{2}}) \) where \( \phi_{\sqrt{2}} : \mathbb{Q}[x] \rightarrow \mathbb{C} \)

is the evaluation at \( \sqrt{2} \).

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

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 \( \mathbb{Q}[x] \):

\[
\begin{cases}
\alpha(\sqrt{2}) + b = 0 \\
\alpha \neq 0
\end{cases} \Rightarrow \sqrt{2} = -\frac{b}{\alpha} \in \mathbb{Q} \quad \text{which is a contradiction.}
\]

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

Proof of Claim. \( f(x) = (x^2 - 2)q(x) \Rightarrow f(\sqrt{2}) = (\sqrt{2})^2 q(\sqrt{2}) = 0 \)
Lecture 08: The evaluation homomorphisms
Friday, August 18, 2017

\[ f(x) \in \ker \Phi_{\sqrt{2}}. \] 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

\[ \exists q, r \in \mathbb{Q}[x], \quad g(x) = (x^2 - 2)q(x) + r(x), \quad \deg r < 2. \]

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

Ex. Is there a non-zero element in \( \ker \Phi_{\pi} \) where 
\[ \Phi_{\pi} : \mathbb{Q}[x] \to \mathbb{C} \] is the evaluation at the \( \pi \)?

**Solution.** 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.*


Def. \( a \in \mathbb{C} \) is called \underline{algebraic} if \( \ker \phi_a \neq \{0\} \),

where \( \phi_a : \mathbb{Q}[x] \rightarrow \mathbb{C} \) is the evaluation at \( a \).

- \( a \in \mathbb{C} \), which is not algebraic, is called a \underline{transcendental} number.

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

**Factor theorem.** 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

\[ f(x) = (x-a)q(x) \quad \text{for some } q(x) \in R[x] \]

**Pf.** \((\Rightarrow)\) 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. \( \deg r < \deg (x-a) = 1 \). \( \Rightarrow \) \( r \) is constant.

2. \( f(x) = (x-a)q(x) + r(x) \)

Since \( a \) is a zero of \( f \), \( \Rightarrow \) 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 \( f \). \( \blacksquare \)

**Theorem.** 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

\[ \exists q(x) \in D[x] \text{ s.t. } f(x) = (x-a_1) \ldots (x-a_k) q(x). \]

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

**Proof.** We proceed by induction on \( k \).

**Base of induction.** \( k = 1 \).

\( a_1 \) is a zero of \( f \). So by the factor theorem,

\[ f(x) = (x-a_1)q(x) \text{ for some } q(x) \in D[x]; \text{ this proves the base of induction.} \]

**Induction step.** 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

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

...
\[ 1 \leq i \leq k, \quad o = f(a_i) = (a_i - a_{k+1}) h(a_i). \] Since

\[ o = (a_i - a_{k+1}) h(a_i) \implies h(a_1) = h(a_2) = \ldots = h(a_k) = 0. \]

for \( 1 \leq i \leq k \), where \( D \) has no zero-divisor.

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

\[ h(x) = (x-a_1) \ldots (x-a_k) q(x) \]

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

\[ f(x) = (x-a_{k+1}) h(x) = (x-a_1) \ldots (x-a_k) (x-a_{k+1}) q(x). \]

This gives us the first part of the theorem.

To get the second part of the theorem, we have

\[ \deg f = \deg (x-a_1) \ldots (x-a_k) q(x) = k + \deg q, \]

which implies \( \deg f \geq k \). So \( f \) has at most \( \deg f \) zeros. \[ \Box \]
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, $\mathbb{Z}_{15} \cong \mathbb{Z}_3 \times \mathbb{Z}_5$; 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 $(\pm 1, \pm 1)$. 
Next we see how Fermat’s little theorem 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 $a \in \mathbb{Z}_p$, 

$$a^{p^n} = a \quad \text{in} \quad \mathbb{Z}_p.$$  

**Proof.** We proceed by induction on $n$. Fermat’s little theorem gives us the base case of $n=1$. **Induction Step.**

$$a^{p^{n+1}} = (a^{p^n})^p = (a^p)^n = a.$$  

**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 $\mathbb{Z}_5$.  ■
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 $a \in \mathbb{Z}_5$, 

$a^{50} - a + 2 = (a^{5^2}) - a + 2$ 

$= a^2 - a + 2$.

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

<table>
<thead>
<tr>
<th>a</th>
<th>0</th>
<th>1</th>
<th>-1</th>
<th>2</th>
<th>-2</th>
</tr>
</thead>
<tbody>
<tr>
<td>$a^2 - a + 2$</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>4</td>
<td>3</td>
</tr>
</tbody>
</table>

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