Lecture 15: Evaluation at an algebraic number

Monday, May 7, 2018 10:11 AM

In the previous lecture we proved parts of the following theorem:

<u>Theorem</u>. Let $\alpha \in \mathbb{C}$ be an algebraic element. Let

$\phi_\alpha : \mathbb{Q}[x] \to \mathbb{C}$, $\phi_\alpha(f(x)) := f(\alpha)$ be the evaluation at α

map. Then $\exists\, m_\alpha(x) \in \mathbb{Q}[x]$ s.t.

(a) $\ker \phi_\alpha = \langle m_\alpha(x) \rangle$ (b) $m_\alpha(x)$ is irreducible in $\mathbb{Q}[x]$

(c) $\mathrm{Im}\, \phi_\alpha$ is a field (d) Suppose $\deg m_\alpha = n$. Then

$$\mathrm{Im}\, \phi_\alpha = \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \mid a_i \in \mathbb{Q}\}.$$

<u>Pf</u>. We have already proved (a) and (b).

(c) Since $\mathbb{Q}[x]$ is a PID and $m_\alpha(x)$ is irreducible, $\langle m_\alpha(x) \rangle$ is a maximal ideal. Hence $\ker \phi_\alpha$ is a maximal ideal. Therefore $\mathbb{Q}[x]/\ker \phi_\alpha$ is a field. And so by the 1^{st} isomorphism thm,

$\mathrm{Im}\, \phi_\alpha \simeq \mathbb{Q}[x]/\ker \phi_\alpha$ is a field.

(d) . $\forall a_i \in \mathbb{Q}$, $\phi_\alpha(a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}) = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \in \mathrm{Im}\, \phi_\alpha$

And so LHS $\supseteq$ RHS.

. $\forall f(x) \in \mathbb{Q}[x]$, let q, r be the quotient and the remainder of $f(x)$ divided by $m_\alpha(x)$, respectively. Then

$$f(x) = q(x)\, m_\alpha(x) + r(x) \quad \text{and} \quad \deg r < \deg m_\alpha = n.$$

And so $r(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}$ for some $a_i \in \mathbb{Q}$ and

$$\phi_\alpha(f(x)) = q(\alpha) \underbrace{m_\alpha(\alpha)}_{0} + r(\alpha) = r(\alpha) = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}.$$

$\Rightarrow$ LHS $\subseteq$ RHS. ∎

So if we manage to find the minimal polynomial $m_\alpha(x)$ of α, then we understand $\ker \phi_\alpha$ and $\operatorname{Im} \phi_\alpha$; and we would be in a good shape. But how can we do that? In this course we will learn some techniques that can help us; but this problem is hard in general. The key starting point is the following observation.

<u>Lemma</u>. If $p(x) \in \ker \phi_\alpha$ is irreducible in $\mathbb{Q}[x]$ for some $\alpha \in \mathbb{C}$, then $\ker \phi_\alpha = \langle p(x) \rangle$ and $p(x)$ is a minimal polynomial of α.

<u>Pf.</u> Since $\mathbb{Q}[x]$ is a PID and $p(x)$ is irreducible,

Lecture 15: Irreducible polynomials

Monday, May 7, 2018 10:42 AM

$\langle p(x)\rangle$ is a maximal ideal. Since $p(x)\in\ker\phi_\alpha$, $\langle p(x)\rangle\subseteq\ker\phi_\alpha$.

Since $1\notin\ker\phi_\alpha$, $\ker\phi_\alpha\neq\mathbb{Q}[x]$. And so

$$\ker\phi_\alpha=\langle p(x)\rangle,$$

and claim follows. ■

So we need certain tools that can help us determine if a given polynomial is irreducible or not. Let's go over an example that we have done earlier.

<u>Ex.</u> $\mathbb{Q}[x]/\langle x^2+1\rangle\simeq\mathbb{Q}[i]=\{a+bi\mid a,b\in\mathbb{Q}\}$; and $\mathbb{Q}[i]$ is a field.

<u>Solution</u>. It is enough to show a minimal polynomial $m_i(x)$ of i is x^2+1. If we show this, then by the previous theorem:

- $\ker\phi_i=\langle x^2+1\rangle$
- $\operatorname{Im}\phi_i=\{a_0+a_1 i\mid a_0,a_1\in\mathbb{Q}\}$ is a field
- $\operatorname{Im}\phi_i\simeq\mathbb{Q}[x]/\ker\phi_i$; and claim follows.

To show x^2+1 is a minimal poly. of i over $\mathbb{Q}$, by the previous lemma, it is enough to show: i is a zero of x^2+1 and x^2+1 is irred. in $\mathbb{Q}[x]$.

Lecture 15: Irreducible polynomial

Monday, May 7, 2018 10:10 AM

$i^2+1=-1+1=0$ and so i is a zero of x^2+1.

- x^2+1 is not zero, zero-divisor, and a unit in $\mathbb{Q}[x]$ (we will discuss this in more generality later). So if x^2+1 is not irreduc., then $\exists\, a(x), b(x)$ not unit in $\mathbb{Q}[x]$ and $x^2+1=a(x)\,b(x)$.

Since $\mathbb{Q}\setminus\{0\}$ consists of units, $\deg a\neq 0$ and $\deg b\neq 0$.

On the other hand, $2=\deg x^2+1=\deg a+\deg b$. Hence

$\deg a=\deg b=1$. Therefore $\exists\, a_0, a_1, b_0, b_1\in\mathbb{Q}$, $a_1\neq 0$, $b_1\neq 0$,

$a(x)=a_0+a_1x$ and $b(x)=b_0+b_1x$; and so

$x^2+1=(a_0+a_1x)(b_0+b_1x)$. Let's evaluate both sides at $\left(-\frac{a_0}{a_1}\right)$

$\left(\frac{-a_0}{a_1}\right)^2+1=0$, which is a contradiction as the LHS ≥ 1. $\blacksquare$

In the above example we see an important technique:

a deg 2 poly. is irreducible $\Leftrightarrow$ it has no zero.

We will prove this later. For now we go back to the ring of polynomials and study them thoroughly:

Lecture 15: Degree of polynomials

Monday, May 7, 2018 11:24 AM

Recall. $\deg(a_n x^n + a_{n-1}x^{n-1} + \dots + a_0) = n$ if $a_n \neq 0$ and

$\deg(0) = -\infty$.

Convention: . $(-\infty) + n = -\infty$ for any $n \in \mathbb{Z}$

. $(-\infty) + (-\infty) = -\infty$

. $\forall n \in \mathbb{Z}$, $-\infty < n$.

Proposition. Suppose D is an integral domain. Then $\forall f, g \in D[x]$,

$$\deg(fg) = \deg f + \deg g.$$

Pf.. If $f=0$ or $g=0$, then $fg=0$; and because of our convention

$\deg fg = \deg f + \deg g$.

. Suppose $f \neq 0$ and $g \neq 0$. Hence $f(x) = a_n x^n + \dots + a_0$ and $a_n \neq 0$,

$g(x) = b_m x^m + \dots + b_0$ and $b_m \neq 0$, for some $a_i, b_j \in D$.

By distribution, $f(x)\,g(x) =$

$$\left[a_n x^n + (\text{terms of } \deg \leq n-1)\right]\left[b_m x^m + (\text{terms of } \deg \leq m-1)\right] =$$

$$a_n b_m x^{n+m} + (\text{terms of } \deg \leq n+m-1).$$

Since $a_n \neq 0$, $b_m \neq 0$, and D is an integral domain, $a_n b_m \neq 0$. Hence

$\deg(fg) = n+m = \deg f + \deg g$. ■