Lecture 15: Algebraic numbers and minimal polynomial

Sunday, March 17, 2019 2:55 PM

We have proved the following:

<u>Theorem</u>. Suppose $\alpha \in \mathbb{C}$ is an algebraic number. Then

(1) $\exists!$ monic polynomial $m_\alpha(x) \in \mathbb{Q}[x]$ s.t.

$$\text{for } f(x) \in \mathbb{Q}[x],\ f(\alpha)=0 \iff m_\alpha(x) \mid f(x).$$

(2) $m_\alpha(x)$ is irreducible in $\mathbb{Q}[x]$.

(3) $\mathbb{Q}[\alpha] :=$ the smallest subring of $\mathbb{C}$ that contains $\mathbb{Q}$ as a subring and α as an element.

$$\simeq \mathbb{Q}[x]/\langle m_\alpha(x)\rangle \text{ is a field.}$$

In this short lecture we prove:

(a). $\mathbb{Q}[\alpha] = \{a_0 + a_1\alpha + \cdots + a_{d-1}\alpha^{d-1} \mid a_i \in \mathbb{Q}\}$ where $d = \deg m_\alpha(x)$.

(b). If $p(x) \in \mathbb{Q}[x]$ is irreducible and $p(\alpha)=0$, then

$$p(x) = c\, m_\alpha(x) \text{ for some } c \in \mathbb{Q}^\times.$$

<u>Pf</u> (a) We have seen that $\mathbb{Q}[\alpha] = \{h(\alpha) \mid h(x) \in \mathbb{Q}[x]\}$. For any $h(x) \in \mathbb{Q}[x]$ by long division there are $q(x), r(x) \in \mathbb{Q}[x]$ s.t.

$h(x) = m_\alpha(x)\, q(x) + r(x)$ and $\deg r < \deg m_\alpha = d$.

Lecture 15: Algebraic numbers and minimal polynomials

Sunday, March 17, 2019 3:28 PM

Hence $h(\alpha) = q(\alpha)\underbrace{m_\alpha(\alpha)}_{0} + r(\alpha) = r(\alpha)$. Since $\deg r < d$, $r(x) = a_0 + a_1 x + \cdots + a_{d-1}x^{d-1}$ for some $a_i \in \mathbb{Q}$. Therefore $h(\alpha) = r(\alpha) = a_0 + a_1\alpha + \cdots + a_{d-1}\alpha^{d-1}$; and claim follows.

(b) Since $p(\alpha) = 0$, $m_\alpha(x) \mid p(x)$; this means $\exists g(x) \in \mathbb{Q}[x]$ s.t. $p(x) = m_\alpha(x) g(x)$. As $p(x)$ is irreducible in $\mathbb{Q}[x]$, either $m_\alpha(x) \in \mathbb{Q}^\times$ or $g(x) \in \mathbb{Q}^\times$. Since $m_\alpha(x)$ is irreducible in $\mathbb{Q}[x]$, $m_\alpha(x) \notin \mathbb{Q}^\times$. Thus $g(x) = c \in \mathbb{Q}^\times$; and claim follows. ∎

. The (b) part is an effective way to find the minimal polynomial of α over $\mathbb{Q}$.

. The (a) part shows that the main reason to have

$\mathbb{Q}[i] = \{a + bi \mid a, b \in \mathbb{Q}\}$ or $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$

is that the degree of minimal polynomials $m_i(x) = x^2 + 1$ and $m_{\sqrt{2}}(x) = x^2 - 2$ is 2. For instance

$\mathbb{Q}[\sqrt[3]{2}] = \{a_0 + \sqrt[3]{2}\, a_1 + \sqrt[3]{4}\, a_2 \mid a_0, a_1, a_2 \in \mathbb{Q}\}$.