Evaluation homomorphism

Algebra Level 3

A. Ram

Let F be a subfield of a field K.

Let $\alpha \in K$.

$F(\alpha)$ is the smallest subfield of K containing F and α.

$F[x]$ is the smallest subcommutative ring of K containing F and α.

The **evaluation homomorphism** is

$$ev_{\alpha,F} : F[x] \longrightarrow K$$
$$c_0 + c_1 x + \cdots + c_k x^k \longmapsto c_0 + c_1\alpha + \cdots + c_k\alpha^k.$$

The **minimal polynomial of α over F** is

$m_{\alpha,F}(x) \in F[x]$ such that

$$\ker(ev_{\alpha,F}) = \{ m_{\alpha,F}(x)\, g(x) \mid g(x) \in F[x] \}$$

HW: Show that $\mathrm{im}(ev_{\alpha,F}) = F[\alpha]$

Notation: The **ideal of $F[x]$ generated by $m_{\alpha,F}(x)$'s**

$$(m_{\alpha,F}(x)) = m_{\alpha,F}(x)\, F[x]$$
$$= \{ m_{\alpha,F}(x)\, g(x) \mid g(x) \in F[x] \}.$$

Proposition

$$F(\alpha) = F[\alpha] = \frac{F[x]}{\ker(ev_{\alpha,F})}.$$

and $F(\alpha)$ has F-basis $\{1, \alpha, \alpha^2, \ldots, \alpha^{l-1}\}$ where $l = \deg(m_{\alpha,F}(x))$.

Example Let $K = \mathbb{C}$ and $F = \mathbb{R}$ and $\alpha = i$

$$ev_{i,\mathbb{R}} : \mathbb{R}[x] \longrightarrow \mathbb{C}$$

$$1 + 3x + 5x^2 + 7x^3 \longmapsto 1 + 3i + 5i^2 + 7i^3$$
$$= 1 + 3i - 5 - 7i$$
$$= -4 - 4i.$$

Then

$$\ker(ev_{i,\mathbb{R}}) = (x^2+1) = (x^2+1)\mathbb{R}[x]$$
$$= \{(x^2+1)g(x) \mid g(x) \in \mathbb{R}[x]\}$$
$$= \{\text{multiples of } (x^2+1)\}.$$

Then

$$\mathbb{R}(i) = \mathbb{C} = \text{im}(ev_{i,F}) = \mathbb{R}[i] = \frac{\mathbb{R}[x]}{(x^2+1)} = \frac{\mathbb{R}[x]}{\ker(ev_i)}.$$

Theorem Let $\varphi : A \to R$ be a ring homomorphism. Then

$$\operatorname{Im}\varphi \cong \frac{A}{\ker\varphi}, \text{ where}$$

$\ker(\varphi) = \{a \in A \mid \varphi(a) = 0\}$ and

$\operatorname{Im}(\varphi) = \{\varphi(a) \mid a \in A\}$.

The isomorphism is

$$\frac{A}{\ker\varphi} \xrightarrow{\sim} \operatorname{Im}(\varphi)$$

$$a + K \longmapsto \varphi(a), \quad \text{where } K = \ker(\varphi).$$

Proof of the Proposition

To show: (a) $F(\alpha) = F[\alpha]$

(b) $m_{\alpha, F}(x)$ exists

(c) $\{1, \alpha, \ldots, \alpha^{d-1}\}$ are linearly independent

(d) $F\text{-span}\{1, \alpha, \ldots, \alpha^{d-1}\} = F[\alpha]$

(a) To show: (aa) $F[\alpha] \subseteq F(\alpha)$

(ab) $F(\alpha) \subseteq F[\alpha]$.

(aa) Since a field is a ring and $\mathbb{F}(\alpha)$ contains $\mathbb{F}$ and α then $\mathbb{F}[\alpha] \subseteq \mathbb{F}(\alpha)$.

(ab) To show: $\mathbb{F}[\alpha]$ is a field.

To show: If $\beta \in \mathbb{F}[\alpha]$ and $\beta \neq 0$ then $\beta^{-1} \in \mathbb{F}[\alpha]$

Assume $\beta \in \mathbb{F}[\alpha]$ and $\beta \neq 0$.

$$\mathbb{F}[\alpha] \xrightarrow{\cdot\beta} \mathbb{F}[\alpha]$$
$$\gamma \longmapsto \gamma\beta$$

is a ring homomorphism.

and

$$\ker(\cdot\beta) = \{\gamma \in \mathbb{F}[\alpha] \mid \gamma \cdot \beta = 0\} = \{0\}.$$

Since $\mathbb{F}[\alpha]$ is a finite dimensional $\mathbb{F}$-vector space then

$$\operatorname{Im}(\cdot\beta) = \mathbb{F}[\alpha].$$

So $1 \in \operatorname{Im}(\cdot\beta)$

So there exists $\gamma \in \mathbb{F}[\alpha]$ such that $\gamma\beta = 1$.

So $\beta^{-1} = \beta^{-1} \cdot 1 = \beta^{-1}\beta\gamma = 1 \cdot \gamma = \gamma$.

So $\beta^{-1} \in \mathbb{F}[\alpha]$.

So $\mathbb{F}[\alpha]$ is a field containing $\mathbb{F}$ and α.

So $\mathbb{F}[\alpha] \supseteq \mathbb{F}(\alpha)$.

So $\mathbb{F}[\alpha] = \mathbb{F}(\alpha) = \operatorname{Im}(ev_{\alpha, \mathbb{F}})$.