6.9 The field extension $\mathbb{F}(\alpha)$

Let $\mathbb{F}$ be a field and let $\mathbb{E}$ be an extension of $\mathbb{F}$.

- Let $\alpha \in \mathbb{E}$. The **minimal polynomial of** α **over** $\mathbb{F}$ is the monic irreducible polynomial $m_{\alpha,\mathbb{F}}(x) \in \mathbb{F}[x]$ such that

$$m_{\alpha,\mathbb{F}}(x) \quad \text{generates} \quad \ker(\mathrm{ev}_\alpha \colon \mathbb{F}[x] \to \mathbb{E}).$$

- Let $\alpha \in \mathbb{E}$. The ring

$$\mathbb{F}[\alpha] = \mathrm{im}(\mathrm{ev}_\alpha \colon \mathbb{F}[x] \to \mathbb{E})$$

  is the image of the evaluation homomorphism ev_α.

- Let $\alpha \in \mathbb{E}$. The field generated by $\mathbb{F}$ and α is the subfield $\mathbb{F}(\alpha)$ of $\mathbb{E}$ such that
  (a) $\mathbb{F}(\alpha)$ contains $\mathbb{F}$ and α,
  (b) If $\mathbb{K}$ is a subfield of $\mathbb{E}$ which contains $\mathbb{F}$ and α then $\mathbb{K} \supseteq \mathbb{F}(\alpha)$.

Proposition 6.19. *Let $\mathbb{E}$ be an extension of $\mathbb{F}$ and let $\alpha \in \mathbb{E}$. Then*

$$\mathbb{F}(\alpha) = \mathbb{F}[\alpha] \cong \frac{\mathbb{F}[x]}{(m_{\alpha,\mathbb{F}}(x))}.$$

6.10 The theorem of the primitive element

Let $\mathbb{F}$ be a field.

- The *Frobenius map* is the field morphism $F\colon \mathbb{F} \to \mathbb{F}$ given by

$$\text{if } \mathrm{char}(\mathbb{F}) = 0 \text{ and } \alpha \in \mathbb{F} \qquad \text{then } F(\alpha) = \alpha,$$

$$\text{if } p \in \mathbb{Z}_{>0} \text{ and } \mathrm{char}(\mathbb{F}) = p \text{ and } \alpha \in \mathbb{F} \qquad \text{then } F(\alpha) = \alpha^p.$$

- A *perfect field* is a field $\mathbb{F}$ such that the Frobenius map $F\colon \mathbb{F} \to \mathbb{F}$ is an automorpihsm.

Theorem 6.20. *(Theorem of the primitive element) Assume that*

$$\mathbb{F} \textit{ is perfect} \quad \textit{and} \quad \dim_{\mathbb{F}}(\mathbb{K}) \textit{ is finite.}$$

Then there exists $\theta \in \mathbb{K}$ such that $\mathbb{K} = \mathbb{F}(\theta)$.