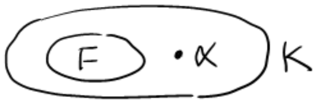
Section 13.2 Algebraic Extensions

Recall Given fields $F \subseteq K$, we say K is an extension of F and write this as K/F. Then K is a vector space over F. Its dimension is called its <u>degree</u>, denoted $[K:F]$. Extension is <u>finite</u> if if it's finite dimensional.



Definitions Suppose K/F and $\alpha \in K$.

- α is <u>algebraic over F</u> if $f(\alpha)=0$ for some $f(x) \in F[x]$
- α is <u>transcendental over F</u> if no such $f(x)$ exists.
- Extension K/F is <u>algebraic</u> if every $\alpha \in K$ is algebraic.

(Note: Every $\alpha \in F$ is algebraic over F, because $f(\alpha)=0$ if $f(x)=x-\alpha \in F[x]$)

Example Consider $\mathbb{R}/\mathbb{Q}$

$\sqrt[3]{5}$ is algebraic over $\mathbb{Q}$ because $f(\sqrt[3]{5})=0$ when $f(x)=x^3-5$.

π is transcendental over $\mathbb{Q}$; it's the root of no polynomial in $\mathbb{Q}[x]$.

$\sqrt{2+\sqrt[3]{5}}$ is algebraic over $\mathbb{Q}$. It's root of $f(x)=(x^2-2)^3-5$

Proposition 9 If $\alpha \in K$ is algebraic over F, then there is a unique monic irreducible polynomial $m_\alpha(x) \in F[x]$. Also $[f(x)$ has root $\alpha] \iff [m_\alpha(x)$ divides $f(x)$ in $F[x]]$.

Proof Take ideal $A=\{f(x) \in F[x] \mid f(\alpha)=0\}$. Then $A=(m(x))$ in PID $F[x]$. Let $m_\alpha(x)=\lambda m(x)$ be monic. Etc.

Definitions $m_\alpha(x)$ is called the <u>minimal polynomial</u> for α. It's the smallest-degree monic polynomial that has α as a root. The <u>degree</u> of α is the degree of $m_\alpha(x)$.

Example In $\mathbb{R}/\mathbb{Q}$.

$\alpha=\sqrt[3]{5}$ $\quad m_\alpha(x)=x^3-5$ so $\sqrt[3]{5}$ has degree **3**.

m_α could not have lower degree. Else it would divide irreducible x^3-5

$\alpha=\sqrt{2+\sqrt[3]{5}}$. Question $m_\alpha(x)=(x^2-2)^3-5$? More on this later

Proposition 11 $F(\alpha) \cong F[x]/(m_\alpha(x))$, and $[F(\alpha):F]=\deg(m_\alpha)$

Moreover, $F(\alpha)$ has basis $1, \alpha, \alpha^2 \cdots \alpha^{n-1}$ where $n=\deg(m_\alpha)$.

Proof: Homomorphism $F[x] \to F(\alpha)$ has kernel $(m_\alpha(x))$

$$f(x) \to f(\alpha)$$

Apply First isomorphism theorem, then Theorem 4.

Proposition 12 $(\alpha$ algebraic over $F) \iff (F(\alpha)/F$ is finite dimensional$)$

Theorem 14 For fields $F \subseteq K \subseteq L$, have $[L:F] = [L:K][K:F]$.

$$\overbrace{\underbrace{F \subseteq K}_{[K:F]} \underbrace{\subseteq L}_{[L:K]}}^{[L:F]}$$

Given a basis $\{\alpha_1, \alpha_2, \ldots, \alpha_\ell\}$ for L over K
and a basis $\{\beta_1, \beta_2 \ldots \alpha_k\}$ for K over F,
then $\{\alpha_i \beta_j \mid 1 \leq i \leq \ell,\ 1 \leq j \leq k\}$ is basis for L over F.

Corollary 15 If L/F is finite and $F \subseteq K \subseteq L$, then $[K:F]$ and $[L:K]$ both divide $[L:F]$.

Application Find min. polynomial of $\alpha = \sqrt{2+\sqrt[3]{5}}$ over $\mathbb{Q}$.
Note $m_\alpha(x)$ must divide $f(x) = (x^2-2)^3 - 5 = x^6 - 6x^4 + 12x^2 - 13$
by Proposition 9. Observe:

$$\overbrace{\underbrace{\underset{F}{\mathbb{Q}} \subset \underset{K}{\mathbb{Q}(\sqrt[3]{5})}}_{[K:F]=3} \underbrace{\subset \underset{L}{\mathbb{Q}(\sqrt{2+\sqrt[3]{5}})}}_{[L:K]=2}}^{[L:F] \leq 6}$$

Note $\sqrt[3]{5}$ is in here because $\sqrt[3]{5} = \left(\sqrt{2+\sqrt[3]{5}}\right)^2 - 2$

Note $K \subset L$, i.e. $\sqrt{2+\sqrt[3]{x}} \notin \mathbb{Q}(\sqrt[3]{x})$. Otherwise

$$\sqrt{2+\sqrt[3]{5}} = a + b\sqrt[3]{5} + c\sqrt[3]{5}^2 \quad \text{with } a, b, c \in \mathbb{Q}$$

Square both sides, isolate. Get $g(\sqrt[3]{5}) = 0$ for quadratic $g(x) \in \mathbb{Q}[x]$.
Impossible since $\sqrt[3]{5}$ has degree 3 (previous page).
Thus $[L:K] > 1$ but $h(x) = x^2 - (2+\sqrt[3]{5}) \in \mathbb{Q}(\sqrt[3]{5})[x]$
gives $h(\sqrt{2+\sqrt[3]{5}}) = 0$. Hence $[L:K] < 2$ so $[L:K] = 2$

Therefore, by Theorem 14 $[L:F] = 6$ so $f(x)$ (above) is indeed the minimal polynomial for α.

Lemma 16 $F(\alpha, \beta) = (F(\alpha))(\beta)$

Theorem 17 K/F finite $\iff$ $K = F(\alpha_1, \alpha_2, \dots, \alpha_k)$ with each α_i algebraic over F. Also $[K:F] \le \prod_{i=1}^{k} \deg(\alpha_i)$

Corollary 18 If α, β are algebraic over F, then so are $\alpha \pm \beta$, $\alpha\beta$, $\frac{\alpha}{\beta}$ and α^{-1}.

Proof: By Theorem 17, $K = F(\alpha, \beta)$ is finite dimensional. Therefore $\alpha+\beta$ $(\alpha+\beta)^2$ $(\alpha+\beta)^3 \dots$ $(\alpha+\beta)^N$ is a linearly dependent set for sufficiently large N. Get degree-N polynomial $f(x) \in F[x]$ with $f(\alpha+\beta) = 0$. etc.

Corollary 19 If L/F is an arbitrary extension, then $K = \{\alpha \in L \mid \alpha \text{ is algebraic over } F\}$ is a subfield of L

Proof By previous corollary.

Example $\mathbb{Q}[x] \leftarrow$ countable set.

$F = \{\alpha \in \mathbb{R} \mid f(\alpha) = 0, \text{ for some } f(x) \in \mathbb{Q}[x]\} \leftarrow$ countable subset of $\mathbb{R}$

Countable subfield $F \subseteq \mathbb{R}$ of all algebraic numbers.

Theorem 20 If $\underbrace{F \subseteq K}_{\text{algebraic}} \underbrace{\subseteq L}_{\text{algebraic}}$, then $\underbrace{F \subseteq L}_{\text{algebraic}}$

Read about composite fields at the end of the section