13.2 Algebraic extensions.

Question. Which finite extensions K/F are of the form $F[x]/(p(x))$?

Definition. $\alpha \in K$ is *algebraic over F* if $\exists\, p(x) \in F[x] \setminus \{0\}$: $p(\alpha) = 0$; else α is *transcendental* over F.

Example. π, e are transcendental over $\mathbb{Q}$. (hard analytic proofs)

Proposition. Let $\alpha \in K$ be algebraic over F. Then

(1) $\exists$ unique monic irreducible $m_{\alpha,F}(x) \in F[x]$ with $m_{\alpha,F}(\alpha) = 0$;
(2) $p(x) \in F[x]$ has root α iff $m_{\alpha,F}(x) \mid p(x)$.

Definition. $m_{\alpha,F}(x)$ above is the *minimal polynomial* for α over F. $\deg m_{\alpha,F}(x)$ is the *degree* of α.

Example. $m_{\sqrt{2},\mathbb{Q}}(x) = x^2 - 2$

Proof. 1) Let $g(x) \in F[x]$ monic, of min degree s.t. $g(\alpha) = 0$.

- Suppose $g(x) = a(x)\, b(x)$ with $\deg a(x), \deg b(x) < \deg g(x)$.
  Then $0 = g(\alpha) = a(\alpha)\, b(\alpha)$ implies $a(\alpha) = 0$ or $b(\alpha) = 0$. $\lightning$
  So $g(x)$ is irreducible.
- For uniqueness and 2) Let $p(x) \in F[x]$ be such that $p(\alpha) = 0$.
  Then $p(x) = q(x)\, g(x) + r(x)$ for $\deg r < \deg g$.
  Then $0 = p(\alpha) = q(\alpha) \underbrace{g(\alpha)}_{=0} + r(\alpha)$
  and $r(\alpha) = 0$ by minimality of $g(x)$.
  Thus $g \mid p$. Uniqueness of $g(x)$ follows since $g(x)$ is monic. $\square$

Corollary. *Let $F \subseteq K \subseteq L$ and $\alpha \in L$ algebraic over F. Then α is algebraic over K and $m_{\alpha,K}(x) \mid m_{\alpha,F}(x)$.*

Corollary. *Let α be algebraic over F. Then*
$F(\alpha) \cong F[x]/m_{\alpha,F}(x)$,
$\underbrace{[F(\alpha) : F]}_{\dim_F F(\alpha)} = \deg m_{\alpha,F}(x)$.

Proposition. α is algebraic over F iff $F(\alpha)/F$ is finite.

Proof. $\Rightarrow$ by previous Cor.

$\Leftarrow$ Assume $[F(\alpha):F] = n$.

Then

$1, \alpha, \alpha^2, \dots \alpha^n$

is lin dependent over F, i.e. $a_0, \dots, a_n \in F$, not all 0, s.t.

$$\sum_{i=0}^{n} a_i \alpha^i = 0.$$

Then $p(x) = \sum a_i x^i$ has α as root. Hence α is algebraic. □

Definition. K/F is *algebraic* if every $\alpha \in K$ is algebraic over F.

Example. $\mathbb{R}/\mathbb{Q}$ is not algebraic.

Corollary. *If K/F is finite, then K/F is algebraic.*

Proof. Every $\alpha \in K$ is the root of some pol of degree $\le [K:F]$. □

Question. Is the converse true? No, example below.

Lagrange's Theorem for field extensions.

Theorem. *For fields $F \subseteq K \subseteq L$*

$$[L:F] = [L:K] \cdot [K:F].$$

Proof. Let B be a basis of K over F
C — L over K.

Claim: $BC = \{bc \mid b \in B, c \in C\}$ is a basis for L over F.

Spanning: Let $a \in L$, $a = \sum \beta_i c_i$ for $\beta_i \in K$
$= \sum (B_{ij} b_j) c_i$ for $B_{ij} \in F$

Linear independence:

Example. $\sqrt{2} \notin \mathbb{Q}(\sqrt[3]{2})$ because $\mathbb{Q}(\sqrt{2}) \not\subseteq \mathbb{Q}(\sqrt[3]{2})$

$$\underbrace{[\mathbb{Q}(\sqrt{2}):\mathbb{Q}]}_{=2} \nmid \underbrace{[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}]}_{=3}$$

Finitely generated algebraic extensions.

Definition. K/F is *finitely generated* if $\exists \alpha_1, \dots, \alpha_n \in K$ such tht
$$K = F(\alpha_1, \dots, \alpha_n).$$

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

Proof. Both are minimal fields containing F, α, β. □

Theorem. $[K : F] < \infty$ *iff there exist algebraic* $\alpha_1, \dots, \alpha_n \in K$ *such that* $K = F(\alpha_1, \dots, \alpha_n)$.

Proof. $\Rightarrow$ Assume $[K : F] = n$.
Let $\alpha_1, \dots, \alpha_n$ be a basis of K over F.
As in above Thm, $\alpha_1, \dots, \alpha_n$ are algebraic over F.
$K = F(\alpha_1, \dots, \alpha_n)$.

$\Leftarrow$ Let $K = F(\alpha_1, \dots, \alpha_n)$ for $\alpha_1, \dots, \alpha_n$ algebraic.
For $F_i := F(\alpha_1, \dots, \alpha_i) = F_{i-1}(\alpha_i)$
$F = F_0 \leq F_1 \leq \dots \leq F_n = K$
So $[K:F] = \underbrace{[K : F_{n-1}]}_{< \infty} \cdot \underbrace{[F_{n-1} : F_{n-2}]}_{< \infty} \cdots \underbrace{[F_1 : F_0]}_{< \infty}$ by Lagrange's Thm □

Note: $[F_i : F_{i-1}] = \deg m_{\alpha_i, F_{i-1}}(x) \leq \deg m_{\alpha_i, F}(x)$.

Consequences.

Corollary. *If* α, β *are algebraic over* F*, then also* $\alpha \pm \beta, \alpha\beta, \alpha^{-1}$ *(for* $\alpha \neq 0$*) are algebraic.*

Proof. All are contained in $F(\alpha, \beta)$. □

Corollary. *Let* K/F*. The elements in* K *that are algebraic over* F *form a subfield of* K.

Example. $\overline{\mathbb{Q}} := \{\alpha \in \mathbb{C} \mid \alpha \text{ is algebraic over } \mathbb{Q}\}$ is called the *field of algebraic numbers*.

Q: What is $|\overline{\mathbb{Q}}|$?

Corollary. *If L is algebraic over K and K is algebraic over F, then L is algebraic over F.*

Definition. The *composite field* K_1K_2 of subfields K_1, K_2 of L is the smallest subfield of L containing K_1, K_2.

Example. $\mathbb{Q}(\sqrt{2})\,\mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$ has degree 6 over $\mathbb{Q}$.

Proposition. Let K_1, K_2 be finite extensions of F. Then

$$[K_1K_2 : F] \leq [K_1 : F] \cdot [K_2 : F]$$

with equality iff an F-basis for one field is linearly independent over the other field.

Proof. Let $\alpha_1, \ldots, \alpha_m$ basis of K_1 over F
$\beta_1, \ldots, \beta_n$ K_2

Then $K_1K_2 = F(\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_n) = K_1(\beta_1, \ldots, \beta_n)$

with $\beta_1, \ldots, \beta_n$ spanning K_1K_2 over K_1.

So $[K_1K_2 : K_1] \leq n$ with $=$ iff $\beta_1, \ldots, \beta_n$ are lin independent over K_1

By Lagrange's Thm $[K_1K_2 : F] = \underbrace{[K_1K_2 : K_1]}_{\leq [K_2 : F]} \cdot [K_1 : F]$

$\square$

Corollary. *If* $\gcd([K_1 : F], [K_2 : F]) = 1$, *then*

$$[K_1K_2 : F] = [K_1 : F] \cdot [K_2 : F].$$

Proof. HW $\square$