

Lecture 31: Finite extensions, compositums of fields

①

§6-9 of [R3]

§B.3 of [DF]

Last time: K/F field extension.

An $\alpha \in K$ is algebraic over F when $\exists f \in F[x]$ with $f(\alpha) = 0$. Ex: $\sqrt{2} \in \mathbb{R}$ is alg. over \mathbb{Q} .

K/F is algebraic when all $\alpha \in K$ are alg. over F .

Thm: $[K:F] < \infty \Rightarrow K/F$ algebraic.

Thm: Suppose $K = F(\alpha)$ with α algebraic over F .

Then $[K:F(\alpha)] = \deg(m_{\alpha,F}(x))$, and so

K/F is algebraic.

Ex: $\mathbb{Q}^{\text{alg}} = \{ \alpha \in \mathbb{C} \mid \alpha \text{ is algebraic over } \mathbb{Q} \}$

[To do: show this is a field.]

An extension K/F is finite when $[K:F] < \infty$

Prop: If $F \subseteq K \subseteq L$ are fields with L/K and K/F finite, then so is L/F . ($\Rightarrow L/F$ is alg.)

Pf: $[L:F] = [L:K][K:F]$.

Thm: Suppose $F \subseteq K \subseteq L$ with L/K and K/F algebraic. Then L/F is algebraic.

Pf: A given $\beta \in L$ is a root of some

$$p(x) = x^n + \alpha_{n-1}x^{n-1} + \dots + \alpha_0 \in K[x]$$

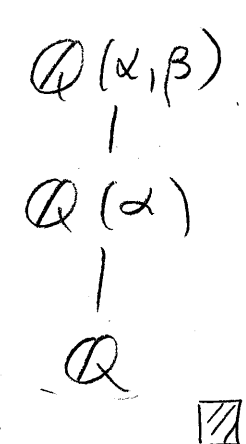
Consider

$$F \subseteq F(\alpha_0) \subseteq F(\alpha_0, \alpha_1) \subseteq \dots \subseteq F(\alpha_0, \alpha_1, \dots, \alpha_{n-1}, \beta) = M$$

Each of these extensions is simple and algebraic (as all α_i are alg / F and β is a root of p), and hence finite. By the proposition, M/F is finite $\Rightarrow M/F$ is alg $\Rightarrow \beta$ is alg. over F . ▣

Cor: \mathbb{Q}^{alg} is a field.

Pf: Suppose $\alpha, \beta \in \mathbb{Q}^{alg}$. Apply theorem to $\mathbb{Q}(\alpha, \beta)/\mathbb{Q}$ to see that $\mathbb{Q}(\alpha, \beta)/\mathbb{Q}$ is algebraic, and hence $\alpha + \beta, \alpha \cdot \beta, \alpha - \beta, \alpha/\beta$ are all in \mathbb{Q}^{alg} . ▣



Def: A field K is algebraically closed

when every $f \in K[x]$ has a root in K .

$\Leftrightarrow f$ splits into linear factors

$\Leftrightarrow K$ has no proper algebraic extension.

Ex: \mathbb{C} (Fund. Thm of Algebra.)

\mathbb{Q}^{alg} : A given $f(x) = \sum_{i=1}^n \alpha_i x^i \in \mathbb{Q}^{\text{alg}}[x]$ has a root $\beta \in \mathbb{C}$. Then $\mathbb{Q}^{\text{alg}}(\beta) / \mathbb{Q}^{\text{alg}}$ is algebraic $\xrightarrow{\text{thm}}$ $\mathbb{Q}^{\text{alg}}(\beta) / \mathbb{Q}$ is alg $\Rightarrow \beta \in \mathbb{Q}^{\text{alg}}$.

Algebraic closure: An algebraic extension \bar{F}/F where \bar{F} is alg. closed.

Ex: \mathbb{C} is an alg. closure of \mathbb{R}

\mathbb{Q}^{alg} is an alg closure of \mathbb{Q} ; write $\bar{\mathbb{Q}} = \mathbb{Q}^{\text{alg}}$.

Fact: Alg. closures exist and are unique up to isom.

Q: Does one of $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt[3]{2})$ contain the other? (both $\subseteq \mathbb{R}$).

A: No. First $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ and $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$.

Now if $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt[3]{2})$, would have

$2 \cdot [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}(\sqrt{2})] = 3$, which is silly.

Def: The compositum of subfields $K_1, K_2 \subseteq L$

is the smallest subfield of L which contains both; it is denoted $K_1 K_2$.

Ex: $F(\alpha)F(\beta) = F(\alpha, \beta)$

Ex: $\mathbb{Q}(\sqrt{2})\mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q}(\sqrt[6]{2})$

Pf 1: $\mathbb{Q}(\sqrt[6]{2})$ contains $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt[3]{2})$

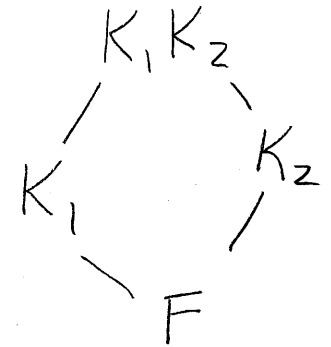
and $\sqrt{2}/\sqrt[3]{2} = 2^{1/2} \cdot 2^{-1/3} = 2^{1/6} = \sqrt[6]{2} \left(\Rightarrow \mathbb{Q}(\sqrt[6]{2}) \right)$
 is contained in the compositum

Pf 2: Any field containing $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt[3]{2})$ must have $[K:\mathbb{Q}]$ divisible by 2 and 3 $\Rightarrow [K:\mathbb{Q}] \geq 6$. As $[\mathbb{Q}(\sqrt[6]{2}):\mathbb{Q}] = 6$, it must be the compositum.

Thm: $F \subseteq K_1, K_2 \subseteq L$ fields, with $[K_i:F] < \infty$.

Then $[K_1 K_2:F] \leq [K_1:F][K_2:F]$

Pf: Let $\{\alpha_i\}$ be an F -basis for K_1
 Let $\{\beta_j\}$ be an F -basis for K_2



Set $K = \left\{ \sum a_{ij}(\alpha_i \beta_j) \mid a_{ij} \in F \right\} \subseteq L$

Claim: $K_1 K_2 = K$.

This will suffice as $\dim_F K \leq (\dim_F K_1)(\dim_F K_2)$.

(5)

Clearly, $K_i \subseteq K \subseteq K_1 K_2$ so the issue is whether K is a subfield. Note K is closed under $+$ and also \times since:

$$\begin{aligned}(\alpha_i \beta_j)(\alpha_k \beta_l) &= (\alpha_i \alpha_k)(\beta_j \beta_l) \\ &= \left(\sum_m a_m \alpha_m\right) \left(\sum_n b_n \beta_n\right) = \sum_{m,n} \underbrace{a_m b_n}_{\text{in } F} \alpha_m \beta_n\end{aligned}$$

What about mult. inverses?

Fix $\gamma \in K$. Consider $T: K \rightarrow K$ which is
 $\delta \mapsto \gamma \delta$

↙ finite dim'l / F

an F -linear transformation. As L is an int. domain, $\text{Ker } T = \{0\} \Rightarrow T$ is surjective as $\dim_F K < \infty$. In particular, $\exists \delta \in K$ with $T(\delta) = 1$, i.e. $\gamma \delta = 1 \Rightarrow \gamma^{-1} = \delta \in K$.

So K is a subfield and hence $= K_1 K_2$ \square

Note: The idea of field operations as linear transformations is very useful to us.