Chapter 1: Galois Theory

Author: Meng-Gen Tsai
Email: plover@gmail.com

Section 1.1: Field Extensions

Exercise 1.1.1. *Let K be a field extension of F. By defining scalar multiplication for $\alpha \in F$ and $a \in K$ by $\alpha \cdot a = \alpha a$, the multiplication in K, show that K is an F-vector space.*

Proof.

(1) K is an additive group.

(2) *Show that $(\alpha\beta) \cdot a = \alpha \cdot (\beta \cdot a)$ for $\alpha, \beta \in F$ and $a \in K$.* In fact,

$$\begin{aligned}(\alpha\beta) \cdot a &= \alpha\beta a \in K, \\ \alpha \cdot (\beta \cdot a) &= \alpha\beta a \in K.\end{aligned}$$

(3) *Show that $(\alpha + \beta) \cdot a = \alpha \cdot a + \beta \cdot a$ for $\alpha, \beta \in F$ and $a \in K$.*

$$\begin{aligned}(\alpha + \beta) \cdot a &= (\alpha + \beta)a \\ &= \alpha a + \beta a \in K, \\ \alpha \cdot a + \beta \cdot a &= \alpha a + \beta a \in K.\end{aligned}$$

(4) *Show that $\alpha \cdot (a + b) = \alpha \cdot a + \alpha \cdot b$ for $\alpha \in F$ and $a, b \in K$.*

$$\begin{aligned}\alpha \cdot (a + b) &= \alpha(a + b) \\ &= \alpha a + \alpha b \in K, \\ \alpha \cdot a + \alpha \cdot b &= \alpha a + \alpha b \in K.\end{aligned}$$

(5) *Show that $1 \cdot a = a$ for $a \in K$.* $1 \cdot a = 1a = a \in K$.

By (1) to (5), K is an F-vector space. □

Exercise 1.1.2. *If K is a field extension of F, prove that $[K : F] = 1$ if and only if $K = F$.*

Proof.

(1) $[K : F] = 1 \Longleftarrow K = F$. Take a basis $\{1\}$ for K as an F-vector space.

(2) $[K : F] = 1 \Longrightarrow K = F$. Take a basis $\{a\}$ for K as an F-vector space where $a \in K$. Since $1 \in K$, there exists $\alpha \in F$ such that $1 = \alpha a$. $a = \alpha^{-1} \in F$, or $K \subseteq F$, or $K = F$.

$\square$

Exercise 1.1.5. *Show that* $\mathbb{Q}(\sqrt{5}, \sqrt{7}) = \mathbb{Q}(\sqrt{5} + \sqrt{7})$.

Proof.

(1) $\mathbb{Q}(\sqrt{5}, \sqrt{7}) \supseteq \mathbb{Q}(\sqrt{5} + \sqrt{7})$ since $\sqrt{5} + \sqrt{7} \in \mathbb{Q}(\sqrt{5}, \sqrt{7})$.

(2)

$$\begin{aligned}
(\sqrt{7} + \sqrt{5})^{-1} &= \frac{1}{\sqrt{7} + \sqrt{5}} \\
&= \frac{\sqrt{7} - \sqrt{5}}{(\sqrt{7} + \sqrt{5})(\sqrt{7} - \sqrt{5})} \\
&= \frac{\sqrt{7} - \sqrt{5}}{2} \in \mathbb{Q}(\sqrt{5} + \sqrt{7}),
\end{aligned}$$

Or $\sqrt{7} - \sqrt{5} \in \mathbb{Q}(\sqrt{5} + \sqrt{7})$. Thus

$$\begin{aligned}
\sqrt{7} &= \frac{1}{2} \cdot ((\sqrt{7} + \sqrt{5}) + (\sqrt{7} - \sqrt{5})) \in \mathbb{Q}(\sqrt{5} + \sqrt{7}), \\
\sqrt{5} &= \frac{1}{2} \cdot ((\sqrt{7} + \sqrt{5}) - (\sqrt{7} - \sqrt{5})) \in \mathbb{Q}(\sqrt{5} + \sqrt{7}).
\end{aligned}$$

Thus, $\mathbb{Q}(\sqrt{5}, \sqrt{7}) \subseteq \mathbb{Q}(\sqrt{5} + \sqrt{7})$.

By (1)(2), $\mathbb{Q}(\sqrt{5}, \sqrt{7}) = \mathbb{Q}(\sqrt{5} + \sqrt{7})$. $\square$

Exercise 1.1.9. *If K is an extension of F such that $[K : F]$ is prime, show that there are no intermediate fields between K and F.*

Proof. Let L be any field such that $F \subseteq L \subseteq K$. By Proposition 1.20,

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

Since $[K : F]$ is prime, $[K : L] = 1$ or $[L : F] = 1$. By Exercise 1.1.2, $L = K$ or $L = F$, or there are no intermediate fields between K and F. $\square$