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 $1 \in K$ as an F-vector space, there exists $\alpha \in F$ such that $1 = \alpha a$. $a = \alpha^{-1} \in F$, or $K \subseteq F$, or $K = F$.

□

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), $\mathbb{Q}(\sqrt{5}, \sqrt{7}) = \mathbb{Q}(\sqrt{5} + \sqrt{7})$. □

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. □

Exercise 1.1.23. *Recall that the characteristic of a ring R with identity is the smallest positive integer n for which $n \cdot 1 = 0$, if such an n exists, or else the characteristic is 0. Let R be a ring with identity. Define $\varphi : \mathbb{Z} \to R$ by*

$\varphi(n) = n \cdot 1$, *where* 1 *is the identity of* R. *Show that* φ *is a ring homomorphism and that* $\ker(\varphi) = m\mathbb{Z}$ *for a unique nonnegative integer* m, *and show that* m *is the characteristic of* R.

Proof.

(1) φ *is a ring homomorphism.*

  (a) $\varphi(a+b) = \varphi(a)+\varphi(b)$. $\varphi(a+b) = (a+b)\cdot 1 = a\cdot 1+b\cdot 1 = \varphi(a)+\varphi(b)$.

  (b) $\varphi(ab) = \varphi(a)\varphi(b)$. $\varphi(ab) = (ab)\cdot 1 = (a\cdot 1)(b\cdot 1) = \varphi(a)\varphi(b)$ since $1 \times 1 = 1$. (Here $\times$ is the multiplication operator of R.)

(2) $\ker(\varphi) = m\mathbb{Z}$ *for a unique nonnegative integer* m. Since $\ker(\varphi)$ is an ideal of a PID $\mathbb{Z}$, there is a unique nonnegative integer m such that $\ker(\varphi) = m\mathbb{Z}$.

(3) m *is the characteristic of* R. There are only two possible cases, $\text{char}(R) = 0$ or else $\text{char}(R) > 0$.

  (a) *char*$(R) = 0$. $\ker(\varphi) = 0$. Thus $m = 0 = \text{char}(R)$.

  (b) *char*$(R) = n > 0$. $n \in \ker(\varphi)$, so $m > 0$ and $m \mid n$. By the minimality of n, $m = n = \text{char}(R)$.

□

Exercise 1.1.24. *For any positive integer* n, *give an example of a ring of characteristic* n.

Proof. The ring $\mathbb{Z}/n\mathbb{Z}$. □

Exercise 1.1.25. *If* R *is an integral domain, show that either char*$(R) = 0$ *or char*(R) *is prime.*

Proof.

(1) 1 has infinite order. $\text{char}(R) = 0$. (Nothing to do.)

(2) 1 has finite order n. Want to show n is prime. If $n = ab$ where $a, b \in \mathbb{Z}^+$, then

$$0 = n \cdot 1 = (a \cdot 1)(b \cdot 1).$$

Since R is an integral domain, $a \cdot 1 =$ or $b \cdot 1 = 0$. By the minimality of n, $a \geq n$ or $b \geq n$. $a = n$ or $b = n$. That is, n is prime.

□