4. Simple extensions

A field extension L/K is said to be *simple* if $L = K(u)$ for some $u \in L$.

In Chapter 2 we considered an element of an extension and associated a polynomial to it, the minimal polynomial. Here we reverse the process: given a polynomial, we construct an extension.

Theorem 4.1. *Let K be a field. Suppose that $f \in K[X]$ is irreducible. Then there exist an extension L of K and $u \in L$ such that u is a root of f and $L = K(u)$.*

Proof. Consider $L = K[X]/(f)$. Since f is irreducible, the ideal (f) is maximal in $K[X]$, so L is a field. The map $\iota\colon K \to L$, $\iota(a) = a + (f)$ is clearly a ring homomorphism. It is also injective: if $\iota(a) = 0$, then $a + (f) = 0 + (f)$, i.e. $a \in (f)$, which forces $a = 0$ because $\deg(f) \geq 1$. So we can identify K with its image $\{a + (f) \mid a \in K\}$ using ι and hence view L as an extension of K.

Write $f = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_0$, $a_n \neq 0$. Let $u = X + (f) \in L$. Then

$$\begin{aligned} f(u) &= (a_n + (f))u^n + \cdots + (a_0 + (f)) = \\ &= (a_n + (f))(X + (f))^n + \cdots + (a_0 + (f)) = \\ &= (a_n X^n + \cdots + a_0) + (f) \\ &= f + (f) = 0 + (f), \end{aligned}$$

so u is a root of f.

It remains to show that $K(u) = L$. Let $g + (f) = b_m X^m + \cdots + b_0 + (f) \in L$. Then $g + (f) = (b_m + (f))(X + (f))^m + \cdots + (b_0 + (f)) \in K(u)$ since $K(u)$ must be closed under addition and multiplication. Thus $K(u) = L$. □

Remark. If L is the field constructed in the preceding proof, then we have: $[L : K] = n$, and a basis of L over K is $\{1 + (f), X + (f), X^2 + (f), \ldots, X^{n-1} + (f)\}$.

Lemma 4.2. *Let $K \subseteq L$ be fields. Suppose that $u_1, \ldots, u_m \in L$ are such that $L = K(u_1, \ldots, u_m)$. Let M be another field, and suppose that two homomorphisms $\alpha\colon L \to M$ and $\beta\colon L \to M$ satisfy $\alpha|_K = \beta|_K$ and $\alpha(u_i) = \beta(u_i)$ for all $i = 1, \ldots, m$. Then $\alpha = \beta$.*

In other words, a homomorphism from $L = K(u_1, \ldots, u_m)$ to another field is uniquely determined by what it does on K and on $u_1, \ldots, u_m$.

Proof. Let $F = \{v \in L \mid \alpha(v) = \beta(v)\}$. We claim that F is a field. This is easy to check: e.g. if $y, z \in F$ and $z \neq 0$ then $\alpha(y/z) = \alpha(y)/\alpha(z) = \beta(y)/\beta(z) = \beta(y/z)$, so $y/z \in F$.

Furthermore, by the hypothesis, $K \subseteq F$ and$\{u_1, \ldots, u_m\} \subseteq F$. It follows that $L = K(u_1, \ldots, u_m) \subseteq F$, whence $L = F$. This means that $\alpha = \beta$. □

We want to show that the simple extension in Theorem 4.1 is in some sense unique.

Idea: Recall from Chapter 2 that if $u \in L \supseteq K$ and $f = \mathrm{minpoly}_K(u)$, then $\epsilon_u \colon K[X] \to K(u)$ is a surjective homomorphism and hence we have an isomorphism $\epsilon_u \colon K[X]/(f) \to K(u)$. Thus, provided $u \in L$ has f as the minimal polynomial, $K(u)$ must be isomorphic to the extension $K[X]/(f)$ that we constructed in the proof of Theorem 4.1.

If $\theta \colon K \to K'$ is an isomorphism between two fields K and K', then we define the map $\tilde{\theta} \colon K[X] \to K'[X]$ by

$$\tilde{\theta}(a_n X^n + \cdots + a_0) = \theta(a_n) X^n + \cdots + \theta(a_0), \quad a_0, \ldots, a_n \in K.$$

It is clear that $\tilde{\theta} \colon K[X] \to K'[X]$ is a ring isomorphism (exercise).

Theorem 4.3. *Let K and K' be fields, and suppose that $\theta \colon K \to K'$ is an isomorphism. Let $L = K(u)$ and $L' = K'(u')$ be two finite simple extensions. Let $f = \mathrm{minpoly}_K(u)$ and $f' = \mathrm{minpoly}'_K(u')$, and suppose that $f' = \tilde{\theta}(f)$. Then there exists a unique isomorphism $\alpha \colon L \to L'$ such that $\alpha|_K = \theta$ and $\alpha(u) = u'$.*

Corollary 4.4. *Let $L = K(u)$ and $L' = K(u')$ simple extensions of K. Suppose that u and u' are algebraic over K and have the same minimal polynomial. Then there is a unique isomorphism $\alpha \colon L \to L'$ such that $\alpha(u) = u'$ and $\alpha(a) = a$ for all $a \in K$.*

Proof. Take $\theta = \mathrm{id}_K$ in the previous theorem. □

Lemma 4.5. *Let $\theta \colon K \to K'$ be an isomorphism between two fields K and K'. Then, for every $f \in K[X]$, $\tilde{\theta}$ induces a ring homomorphism $\phi_f \colon K[X]/(f) \to K'[X]/(\tilde{\theta}(f))$, given by $\phi_f(g + (f)) = \tilde{\theta}(g) + (\tilde{\theta}(f))$.*

Proof. Let $I = (f)$ and $I' = (\tilde{\theta}(f))$. Let $\pi \colon K'[X] \to K'[X]/I'$ be the canonical surjection, given by $\pi(g) = g + I'$. Then $\pi \circ \tilde{\theta} \colon K[X] \to K[X']/I'$ is a surjective homomorphism. We have $\ker(\pi \circ \tilde{\theta}) = I$. Indeed, if $h \in K[X]$, then $(\pi \circ \tilde{\theta})(h) = 0$ if and only if $\tilde{\theta}(h) \in I'$ iff $\tilde{\theta}(h)$ is a multiple of $\tilde{\theta}(f)$ iff h is a multiple of f iff $h \in I$.

Hence, by the First Isomorphism Theorem, there is an isomorphism

$$\phi_f \colon K[X]/I \to K'[X]/I'$$

given by

$$\phi_f(g + I) = (\pi \circ \tilde{\theta})(g) = \tilde{\theta}(g) + I'.$$

□

Proof of Theorem 4.3. First, observe that, if α exists, then it is unique by Lemma 4.2.

By Lemma 2.13 and the First Isomorphism Theorem, the evaluation map $\epsilon_u \colon K[X] \to K(u)$ yields an isomorphism

$$\bar{\epsilon}_u \colon K[X]/(f) \to K(u)$$

given by $\bar{\epsilon}_u(g + (f)) = \epsilon_u(g) = g(u)$. Similarly, there is an isomorphism

$$\bar{\epsilon'}_u \colon K'[X]/(f') \to K'(u')$$

given by $\bar{e'}_u(h) = h(u')$. Finally, Lemma 4.5 yields an isomosphism

$$\phi_f \colon K[X]/(f) \to K'[X]/(f')$$

given by $\phi_f(g + (f)) = \tilde{\theta}(g) + (f')$. Let $\alpha = \bar{\epsilon'}_u \circ \phi_f \circ \bar{e}_u^{-1} \colon L \to L'$. Then $\alpha(u) = \bar{\epsilon'}_u \circ \phi_f(X + (f)) = \bar{\epsilon'}_u(X + (f')) = u'$. Also, for every $a \in K$, we have $\alpha(a) = \bar{\epsilon'}_u \circ \phi_f(a + (f)) = \bar{\epsilon'}_u(\theta(a) + (f')) = \theta(a)$. Thus $\alpha|_K = \theta$. □

Example. The field $\mathbb{C}$ is obtained from $\mathbb{R}$ by "adding" a root of the polynomial $X^2 + 1$, so $\mathbb{C} \cong \mathbb{R}[X]/(X^2 + 1)$.