10 Algebraic Extensions

Review Let F be a field and $p(x)$ be an irreducible polynomial in $F[x]$. Let a be a zero of $p(x)$ in an extension field E of F, If $\deg p(x) = n$, then

$$F[x]/\langle p(x)\rangle \approx F(a) = \{c_0 + c_1 a + c_2 a^2 + \cdots + c_{n-1}a^{n-1} \mid c_0, c_1, \ldots, c_{n-1} \in F\}$$

and as a vector space over F, $F(a)$ is of dimension n and $\{1, a, a^2, \ldots, a^{n-1}\}$ is a basis over F.

Definition 10.1 Let E be an extension field of a field F and let $a \in E$.

1. We call *a algebraic over F* if a is a zero of some nonzero polynomial in $F[x]$.

2. If a is not algebraic over F, it is called *transcendental over F*.

3. An extension E of F is called an *algebraic* extension of F if every element of E is algebraic over F.

4. If E is not an algebraic extension of F, it is called a *transcendental* extension of F.

5. An extension of F of the form $F(a)$ is called a *simple* extension of F.

6. $F(x) = \{f(x)/g(x) \mid f(x), g(x) \in F[x],\ g(x) \neq 0\}$ is the field of quotients of $F[x]$.

Theorem 10.1 (Theorems 21.1, 21.2, 21.3) *Let E be an extension field of the field F and let $a \in E$.*

(i) *If a is transcendental over F, then $F(a) \approx F(x)$.*

(ii) *If a is algebraic over F, then $F(a) \approx F[x]/\langle p(x)\rangle$, where $p(x)$ is a nonzero polynomial in $F[x]$ of minimum degree such that $p(a) = 0$. Moreover, $p(x)$ is irreducible over F.*

(iii) *If the polynomial in (ii) is monic, it is a unique monic irreducible polynomial $p(x) \in F[x]$ such that $p(a) = 0$. Moreover, for $f(x) \in F[x]$, $f(a) = 0$ if and only if $p(x) \mid f(x)$, and $p(x)$ is called the minimal polynomial of a.* *(Ex.1)*

Proof. Let $\phi : F[x] \to F(a)$ $(f(x) \mapsto f(a))$ be a natural ring homomorphism. If a is transcendental over F, ϕ is injective and $F[a] = \mathrm{Im}\phi$ is isomorphic to $F[x]$. Now $\phi : F(x) \to F(a)$ $(f(x)/g(x) \mapsto f(a)/g(a))$ is well-defined and ϕ is an isomorphism.

If a is algebraic over F, then $\mathrm{Ker}\phi \neq 0$ and $F[x]/\mathrm{Ker}\phi \approx \mathrm{Im}\phi \subset F(a)$. Since $\mathrm{Im}\phi$ is a subring of a field containing 1, it is an integral domain. Let $\mathrm{Ker}\phi = \langle f(x)\rangle$ as $F[x]$ is a PID. Since $p(x) \neq 0$, $p(x)$ is primitive and $\mathrm{Im}\phi$ is a maximal ideal. So $\mathrm{Im}\phi$ is a filed containing F and a. Therefore $\mathrm{Im}\phi = F(a)$. Clearly $p(x)$ is a polynomial of minimum degree such that $p(a) = 0$, as $f(a) = 0$ implies $p(x) \mid f(x)$. This proves (i) and (ii).

(iii) is obvious. ■

Definition 10.2 Let E be an extension field of a field F. Then E can be regarded as a vector space over F.

1. We say that E has degree n over F and write $[E : F] = n$ if E has dimension n as a vector space over F.

2. If $[E : F]$ is finite, E is called a *finite extension* of F; otherwise, we say that E is an *infinite extension* of F.

Example 10.1 1. $[\boldsymbol{C} : \boldsymbol{R}] = 2$. Since $\boldsymbol{C} = \boldsymbol{R}(\sqrt{-1})$ and $x^2 + 1$ is the minimal polynomial of $\sqrt{-1}$ over $\boldsymbol{R}$, this follows from the next.

2. If a is algebraic over F and $p(x)$ the minimal polynomial of a, then $[F(a) : F] = \deg(p(x))$.

Theorem 10.2 (Theorem 21.5) $[K : F] = [K : E][E : F]$.

Proof. Let $\{x_i \mid i \in I\}$ be a basis of K over E, and $\{y_j \mid i \in J\}$ a basis of E over F. It suffices to show that $\{x_i y_j \mid i \in I,\ j \in J\}$ is a bssis of K over F.

[Linear Independence:] Let $k_{ij} \in F$ $(i \in I,\ j \in J)$ such that

$$0 = \sum_{i \in I,\, j \in J} k_{ij} x_i y_j = \sum_{j \in J} \left(\sum_{i \in I} k_{ij} x_i \right) y_j$$

Since $\sum_{i \in I} k_{ij} x_i \in E$ and $\{y_j \mid i \in J\}$ is linearly independent over E, we have $\sum_{i \in I} k_{ij} x_i = 0$ for all $j \in J$. Similarly $\{x_i \mid i \in I\}$ is linearly independent over F, $k_{ij} = 0$ for all $i \in I$ and $j \in J$. Thus the set is linearly independent.

[Generation] Let $x \in K$. Since $\{y_j \mid i \in J\}$ is a basis of K over E, there are $l_j \in E$ $(j \in J)$ such that $x = \sum_{j \in J} l_j y_j$. Similarly, since $\{x_i \mid i \in I\}$ is a basis of E over F, for each $j \in J$, there exist $k_{ij} \in F$ $(i \in I)$ such that $l_j = \sum_{i \in I} k_{ij} x_i$. By substituting this in the previous formula, we have

$$x = \sum_{j \in J} l_j y_j = \sum_{i \in I,\, j \in J} k_{ij} x_i y_j.$$

Therefore all elements of K can be expressed as a F linear combination of $\{x_i y_j \mid i \in I,\ j \in J\}$. ■

Corollary 10.3 *Let E be an extension field of F. If $a_1, a_2, \ldots, a_n \in E$ are algebraic over F, then $F(a_1, a_2, \ldots, a_n)$ is a finite extension of F.* *(Exercise 20.20)*

Proof. We show by induction. Let $E = F(a_1, a_2, \ldots, a_{n-1})$. Then

$$[F(a_1, a_2, \ldots, a_n) : F] = [E(a_n) : E][E : F] < \infty.$$

Thus we have the assertion. ■

Proposition 10.4 (Theorems 21.4, 21.7) 1. *If E is a finite extension of F, then E is an algebraic extension of F.*

2. *If K is an algebraic extension of E and E is an algebraic extension of F, then K is an algebraic extension of F.*

3. *If E is an extension field of the field F. Then the set A of all elements of E that are algebraic over F is a subfield of E. A is called the algebraic closure of F in E.*

Proof. Let $[E : F] = n$ and $a \in E$. Then $1, a, a^2, \ldots, a^n$ is not linearly independent over F. Hence there exist $c_0, c_1, \ldots, c_n \in F$ such that $c_0 + c_1 a + c_2 a^2 + \cdots + c_n a^n = 0$. Let $f(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_n x^n \in F[x]$. Then $f(x) \neq 0$ and $f(a) = 0$. Hence a is algebraic over F.

Let $a \in K$. Then a is algebraic over E. Hence there is a polynomial $0 \neq f(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_n x^n \in E[x]$ such that $f(a) = 0$. Since $c_0, c_1, \ldots, c_n$ are algebraic over F, $[F(c_0, c_1, \ldots, c_n) : F] < \infty$ and $a \in F(c_0, c_1, \ldots, c_n)$. Thus a is algebraic over F.

Let A be the set of all elements of E that are algebraic over F. Let a and b be algebraic over F. Then $F(a, b)$ is a finite extension of F. Hence $a - b$ and a/b with $b \neq 0$ are elements of $F(a, b) \subset A$. Therefore, A is a field. ∎

Definition 10.3 Let E be a field. If there is no proper algebraic extension of E, then E is called *algebraically closed*. Every field F has a unique, up to isomorphism, algebraic extension that is algebraically closed. This field is called the algebraic closure of F. (This result requires the Axiom of Choice.)

Example 10.2 Let A be the set of all algebraic elements of $\boldsymbol{C}$ over $\boldsymbol{Q}$. Then A is an infinite extension of $\boldsymbol{Q}$. Note that A contains $\{\sqrt[n]{2}\}$. So A contains a field E_n with $[E_n : \boldsymbol{Q}] = n$. Elements of A is called algebraic numbers and $|A| = \aleph_0$.

Theorem 10.5 (Primitive Element Theorem (Theorem 21.6), Steinitz, 1910) *If F is a field of characteristic 0, and a and b are algebraic over F, then there is an element $c \in F(a, b)$ such that $F(a, b) = F(c)$.*

Proof. Let $p(x)$ and $q(x)$ be minimal polynomials of a and b and $a_1 = a, a_2, \ldots, a_m$ and $b_1 = b, b_2, \ldots, b_n$ are roots of $p(x)$ and $q(x)$ in a splitting field of $p(x)q(x)$. Choose $d \in F \setminus \{(a_i - a)/(b - b_j) \mid i \geq 1, j > 1\}$. In particular $a_i \neq a + d(b - b_j)$ for $j > 1$. We shall show that $c = a + db$ has the property. Note that $d \neq 0$ by definition.

Consider $q(x)$ and $r(x) = p(c - dx)$ in $F(c)[x]$. Since $q(b) = 0 = p(a) = p(c - db) = r(b)$. Let $s(x)$ be the minimal polynomial of b in $F(c)[x]$. We claim that $s(x) = x - b$. This is because $s(x) \mid r(x)$, and $r(b_j) = p(c - db_j) = p(a + db - db_j) = p(a + d(b - b_j)) \neq 0$.

Therefore, $b \in F(c)$, $a = c - db \in F(c)$ and $F(a, b) \subset F(c) = F(a + db) \subset F(a, b)$. ∎

Thus any finite extension of a field of characteristic 0 is a simple extension. An element a with the property that $E = F(a)$ is called a *primitive element* of E.

Example 10.3 $F = \boldsymbol{Q}(\sqrt{2}, \sqrt{3})$. Then $[F : \boldsymbol{Q}] = 4$ and $F = \boldsymbol{Q}(\sqrt{2} + \sqrt{3})$.

Example 10.4 $F = \boldsymbol{Q}(\sqrt[4]{2}, \sqrt{-1}) \supset \boldsymbol{Q}(\sqrt[4]{2})$. Then $[F : \boldsymbol{Q}] = 8$.