Chapter 21 Algebra Extensions

Different Extensions

Definition Let $\mathbb{E}$ be an field extension of $\mathbb{F}$.

An element $a \in \mathbb{E}$ is algebraic if it is the zero of some $f(x) \in \mathbb{F}[x]$.

Otherwise, it is transcendental over $\mathbb{F}$.

We say that $\mathbb{E}$ is an algebraic extension of $\mathbb{F}$ if every $a \in \mathbb{E}$ is algebraic over $\mathbb{F}$.

If $\mathbb{E}$ is not an algebraic extension of $\mathbb{F}$, it is a transcendental extension.

If $\mathbb{E} = \mathbb{F}(a)$, then $\mathbb{E}$ is a simple extension. Here a can be algebraic or transcendental.

Theorem 21.1/21.2/21.3 Let $\mathbb{E}$ is an extension of $\mathbb{F}$, and $a \in \mathbb{E}$.

- If a is transcendental over $\mathbb{F}$, then

$$\mathbb{F}(a) \sim \mathbb{F}(x) = \{f(x)/g(x) : f(x), g(x) \in \mathbb{F}[x], g(x) \neq 0\}.$$

- If a is algebraic over $\mathbb{F}$, then there is a unique monic irreducible polynomial $p(x) \in \mathbb{F}[x]$ with minimum degree such that $p(a) = 0$ and $F(a)$ is isomorphic to $\mathbb{F}[x]/\langle p(x)\rangle$.

  The polynomial $p(x)$ is called the minimal polynomial of a, and it is a factor of any polynomial $f(x) \in \mathbb{F}[x]$ such that $f(a) = 0$.

Proof. Define $\phi(f(x)) = f(a)$. Then $\mathbb{F}[x] \sim \mathbb{F}(a)$.
Let $p(x) \in \mathbb{F}[x]$ be a monic polynomial of minimum degree satisfying $f(a) = 0$.
For any $f(x) \in \mathbb{F}[x]$ such that $f(a) = 0$, we have $f(x) \in \langle p(x)\rangle$. Else, ...
So, if $f(x)$ is another monic polynomial of minimum degree satisfying $f(a) = 0$, then $f(x) = p(x)$.
By Theorem 20.3, $\mathbb{F}[x]/\langle p(x)\rangle \sim \mathbb{F}(a)$. □

Extension fields and vector spaces

Let $\mathbb{E}$ be an extension of $\mathbb{F}$, and let $[\mathbb{E} : \mathbb{F}]$ be the degree of the extension, i.e., the dimension of the vector space $\mathbb{E}$ over $\mathbb{F}$. Then $\mathbb{E}$ is a finite or infinite extension of $\mathbb{F}$ depending on $[\mathbb{E} : \mathbb{F}]$ is finite or infinite.

Theorem 21.4 If $\mathbb{E}$ is a finite extension of $\mathbb{F}$, then it is an algebraic extension of $\mathbb{F}$.

Proof. Let $a \in \mathbb{E} \setminus \mathbb{F}$, and $\{1, a, a^2, \ldots, a^r\}$ be a maximal linearly independent set. Then ...

Theorem 21.5 Let $\mathbb{K}$ be a finite extension of $\mathbb{E}$, which is a finite extension of $\mathbb{F}$. Then $[\mathbb{K} : \mathbb{F}] = [\mathbb{K} : \mathbb{E}][\mathbb{E} : \mathbb{F}]$.

Proof. Use the bases $\{x_1, \ldots, x_m\}$ and $\{y_1, \ldots, y_n\}$ ...

Theorem 21.6 Let a, b are algebraic over a perfect field $\mathbb{F}$ such that $[\mathbb{F}(a) : \mathbb{F}] = m$ and $[\mathbb{F}(b) : \mathbb{F}] = n$. If $|F| > \min\{mn - n, mn - m\}$, then there is $c \in \mathbb{F}(a, b)$ such that $\mathbb{F}(a, b) = \mathbb{F}(c)$.

Proof. Let $p(x) = (x - a_1) \cdots (x - a_m), q(x) = (x - b_1) \cdots (x - b_n) \in \mathbb{F}[x]$ be the monic minimal polynomials of $a = a_1$, $b = b_1$ with distinct zeros (as $\mathbb{F}$ is perfect).

Without lost of generality assume $mn - n \le mn - m$. By the assumption on $|\mathbb{F}|$, there d be such that $d \neq (a_i - a)/(b - b_j)$ for all $i \ge 1$ and $j > 1$, $c = a + db$.

Then $\mathbb{F}(c) \subseteq \mathbb{F}(a, b)$.

For the reverse inclusion, consider $q(x) \in \mathbb{F}[x] \subseteq \mathbb{F}[c)[x]$ and $r(x) = p(c - dx) \in \mathbb{F}(c)[x]$. Then

$$q(b) = 0 \quad \text{and} \quad r(b) = p(c - db) = p(a) = 0.$$

Then the monic minimal polynomial $s(x) \in \mathbb{F}(c)[x]$ of b divides $q(x)$ and $r(x)$. Thus, $s(x)$ should be the product of some linear factors of $q(x)$. But

$$r(b_j) = p(c - db_j) = p(a + d(b - b_j)) \neq 0$$

as $a + d(b - b_j) \neq a_i$ for all i.

So, $s(x) = (x - b)$, i.e., $b \in \mathbb{F}(c)$ and so is $a = c - db$. □

Theorem 21.7 If $\mathbb{K}$ is an algebraic extension of $\mathbb{E}$, and $\mathbb{E}$ is an algebraic extension of $\mathbb{F}$, then $\mathbb{K}$ is an algebraic extension of $\mathbb{F}$.

Proof. Let $a \in \mathbb{K}$. Suppose $p(x) = b_0 + b_1 x + \cdots + b_{n-1}x^{n-1} + x^n \in \mathbb{E}[x]$ is the monic minimal polynomial of a. Then $p(x) \in \mathbb{F}(b_0, \ldots, b_{n-1})[x]$ and $a \in \mathbb{F}(b_0, \ldots, b_{n-1}, a)$ is a finite extension, and is therefore algebraic. □

Corollary Let $\mathbb{E}$ is an extension of $\mathbb{F}$. Then the set of elements of $\mathbb{E}$ is algebraic over $\mathbb{F}$ is a subfield of $\mathbb{E}$.

Proof. Need only show that if a, b are algebraic over $\mathbb{F}$, then so are $a + b, a - b, ab$ and also $1/b$ if b is nonzero. □