Chapter 5. Fields and Galois Theory

1. Field extensions

Definition 1.1 A field F is an extension field of K (or simply an extension of K) if
K is a subfield of F.

Remark Let F be an extension field of K.
Then (1) $1_F = 1_K$
(2) F is a vector space over K
(3) the dimension of the K-vector space F is denoted by $[F:K]$ (rather than $\dim_K F$)
(4) F is a finite (respectively, infinite) dimensional extension of K if
$[F:K] < \infty$ (respectively, $[F:K] = \infty$)

Theorem 1.2 Let F be an extension field of E and E be an extension field of K.
Then $[F:K] = [F:E][E:K]$, and hence
$[F:K] < \infty \iff [F,E] < \infty$ and $[E:K] < \infty$

Proof This follows from Theorem 2.16 in Chapter IV. ///

Definition (1) If $K \subseteq E \subseteq F$ are extensions of fields, then E is an intermediate field of K and F.
(2) If X is a subset of a field F, then the subfield generated by X is the intersection

of all subfields of F containing X.

(3) If F is an extension field of K and $X \subseteq F$, then the subfield generated by $K \cup X$ is the subfield generated by K and X and is denoted by $K(X)$.

(4) If $X = \{u_1, \cdots, u_n\}$, then $K(X) := K(u_1, \cdots, u_n)$ is a finitely generated extension of K.

(5) If $X = \{u\}$, then $K(u)\ (= K(X))$ is a simple extension of K.

Remark A finitely generated extension need not be finite dimensional.

Theorem 1.3 Let F be an extension field of a field K, $u, u_i \in F$ and $X \subseteq F$. Then

(1) $K[u] = \{f(u) \mid f \in K[x]\}$

(2) $K[u_1, \cdots, u_m] = \{f(u_1, \cdots, u_m) \mid f \in K[x_1, \cdots, x_m]\}$

(3) $K[X] = \{f(u_1, \cdots, u_n) \mid u_i \in X,\ n \in \mathbb{N},\ f \in K[x_1, \cdots, x_n]\}$

(4) $K(u) = \left\{ \dfrac{f(u)}{g(u)} \;\middle|\; f, g \in K[x],\ g(u) \neq 0 \right\}$

(5) $K(u_1, \cdots, u_n) = \left\{ \dfrac{f(u_1, \cdots, u_n)}{g(u_1, \cdots, u_n)} \;\middle|\; \begin{array}{l} f, g \in K[x_1, \cdots, x_n], \\ g(u_1, \cdots, u_n) \neq 0 \end{array} \right\}$

(6) $K(X) = \left\{ \dfrac{f(u_1, \cdots, u_n)}{g(u_1, \cdots, u_n)} \;\middle|\; \begin{array}{l} f, g \in K[x_1, \cdots, x_n],\ n \in \mathbb{N}, \\ u_1, \cdots, u_n \in X,\ g(u_1, \cdots, u_n) \neq 0 \end{array} \right\}$

(7) $\forall v \in K(X),\ \exists Y \subseteq X \ni |Y| < \infty$ and $v \in K(Y)$.

(8) $\forall v \in K[X],\ \exists Y \subseteq X \ni |Y| < \infty$ and $v \in K[Y]$.

Proof These are clear. ///

Definition If L and M are subfields of F, then the composition of L and M in F, denoted by LM, is a subfield of F generated by $L \cup M$.

Remark (1) $LM = L(M) = M(L)$

(2) If K is a subfield of $L \cap M$ $\ni$ $M = K(S)$ for some $S \subseteq M$, then $LM = L(S)$.

(3) The composition of any finite number of subfields $E_1, \cdots, E_n$ is defined to be the subfield generated by $E_1 \cup \cdots \cup E_n$ and is denoted by $E_1 \cdots E_n$.

Definition 1.4 Let F be an extension field of K and $u \in F$.

Then (1) u is algebraic over K if

$$\exists\, \underset{0}{\overset{}{f}} \neq\!\!\!\! \quad \in K[x] \ni f(u) = 0.$$

(2) u is transcendental over K if

$$\nexists\, 0 \neq f \in K[x] \ni f(u) = 0.$$

(3) F is an algebraic extension of K if every element of F is algebraic over K.

(4) F is a transcendental extension of K if F is not an algebraic extension of K.

Remark (1) K is algebraic over K

($\because$ For $u \in K$, u is a root of $x - u \in K[x]$)

(2) If $u \in F$ is algebraic over K' and $K' \subseteq K$, then u is algebraic over K.

(3) If $u \in F$ is a root of $f \in K[x]$, then we may assume that f is monic.

(4) A transcendental extension contains elements that are algebraic over K.

Example (1) $i\ (=\sqrt{-1}) \in \mathbb{C}$ is algebraic over $\mathbb{Q}$.

(2) $\pi\ (\in \mathbb{R})$ is transcendental over $\mathbb{Q}$.

(3) The quotient field of $K[x_1, \cdots, x_n]$ is $K(x_1, \cdots, x_n)$

More precisely, $K(x_1, \cdots, x_n) = \left\{ \frac{g}{f} \,\middle|\, f, g \in K[x_1, \cdots, x_n],\ f \neq 0 \right\}$

We call $K(x_1, \cdots, x_n)$ the field of rational functions in $x_1, \cdots, x_n$ over K.

Theorem 1.5 Let F be an extension field of K and $u \in F$ be transcendental over K.

Then $\exists$ an isomorphism of fields $K(u) \cong K(x)$ whose restriction on K is the identity map.

Proof Define $\varphi : K(x) \to F$ by

$$\varphi\left(\frac{f}{g}\right) = \frac{f(u)}{g(u)}, \quad {}^{\forall} \frac{f}{g} \in K(x)$$

$\Rightarrow$ φ is a monomorphism $\ni$ $\varphi|_K = 1_K$.

($\because$) Clearly, φ is a well-defined homomorphism.

Assume that $\frac{f_1(u)}{g_1(u)} = \frac{f_2(u)}{g_2(u)}$.

$\Rightarrow (f_1 g_2 - f_2 g_1)(u) = 0$

Since u is transcendental over K,

$f_1 g_2 - f_2 g_1 = 0$

$\Rightarrow \frac{f_1}{g_1} = \frac{f_2}{g_2}$

Note that $\mathrm{Im}(\varphi) = K(u)$.

$\Rightarrow K(x) \cong K(u)$. ///

Theorem 1.6 Let F be an extension field of K and $u \in F$ be algebraic over K. Then

(1) $K(u) = K[u]$

(2) $K(u) \cong K[x]/(f)$, where f is an irreducible monic polynomial of degree $n \geq 1$ uniquely determined by the condition that $f(u)=0$ and $g(u)=0$ ($g \in K[x]$) $\Leftrightarrow f \mid g$.

(3) $[K(u):K] = n$

(4) $\{1, u, u^2, \ldots, u^{n-1}\}$ is a basis for K-vector space $K(u)$

(5) Every element of $K(u)$ can be written uniquely in the form $a_0 + a_1 u + \cdots + a_{n-1} u^{n-1}$ for some $a_0, \ldots, a_{n-1} \in K$.

Proof (1), (2) Note that the map $\varphi: K[x] \to K[u]$ defined by $\varphi(f) = f(u)$ is an epimorphism.

$\Rightarrow K[u] \cong K[x]/\ker(\varphi)$.

Since $K[x]$ is a PID, $\ker(\varphi) = (f)$ for some $f \in K[x]$.

(In fact, $f(u)=0$)

Since u is algebraic, $\ker(\varphi) \neq (0)$

Since $\varphi \neq 0$, $\ker(\varphi) \neq K[x]$

Since $K[u]$ is an integral domain, f is prime in $K[x]$

Since $K[x]$ is a PID, f is irreducible in $K[x]$

$\Rightarrow$ (f) is a maximal ideal of $K[x]$

$\Rightarrow$ $K[u]$ is a field.

Note that $K(u)$ is the smallest field containing K and u.

$\Rightarrow$ $K(u) = K[u]$.

The uniqueness of f is clear.

(3), (4), (5) Let $a \in K(u)$ $(= K[u]$ by (1)).

Then $a = g(u)$ for some $g \in K[x]$

Note that $g = fq + r$ for some $q, r \in K[x]$

$\Rightarrow$ $a = g(u) = r(u)$.

Note that $\deg(r) < \deg(f)$

$\Rightarrow a \in 1K + u\cdot K + \cdots + u^{\deg(r)}K$

$\subseteq \langle 1, u, \cdots, u^{n-1} \rangle$

By the choice of f, $\{1, u, \cdots, u^{n-1}\}$ is linearly independent. //

Definition 1.7 Let F be an extension field of K and $u \in F$ be algebraic over K.

Then (1) the monic irreducible polynomial in Theorem 1.6 (1) is the irreducible (or minimal) polynomial of u.

(2) the degree of u over K is $\deg(f)$ $(= [K(u):K])$.

Example Let $u \in \mathbb{R}$ be a root of $x^3 - 3x - 1 \in \mathbb{Q}[x]$.

(1) Note that $x^3 - 3x - 1$ is irreducible over $\mathbb{Q}$.

$\Longrightarrow$ u has degree 3 over $\mathbb{Q}$ (by Theorem 1.6)

and $\{1, u, u^2\}$ is a basis for $\mathbb{Q}(u)$.

(2) Let $x^4 + 2x^3 + 3 \in \mathbb{Q}[x]$.

Then $x^4 + 2x^3 + 3 = (x+2)(x^3 - 3x + 1) + (3x^2 + 7x + 5)$

$\Longrightarrow u^4 + 2u^3 + 3 = 3u^2 + 7u + 5$.

(3) Note that $(x^3 - 3x + 1, 3x^2 + 7x + 5) = 1$.

Since $K[x]$ is a PID,

$1 = (x^3 - 3x + 1)g(x) + (3x^2 + 7x + 5)h(x)$

for some $g, h \in K[x]$

$\Longrightarrow$ $1 = (3u^2 + 7u + 5)h(u)$

$\Longrightarrow$ $h(u)$ is the multiplicative inverse of $3u^2 + 7u + 5$.

Question Let E be an extension field of K, F be an extension field of L and $\sigma: K \to L$ be an isomorphism. Then $\exists$ an isomorphism $\tau: E \to F$ $\ni$ $\tau|_K = \sigma$?

Remark (1) Let $\sigma: R \to S$ be a ring homomorphism. Then the map $R[x] \to S[x]$ given by

$$r_0 + r_1 x + \cdots + r_n x^n \mapsto \sigma(r_0) + \sigma(r_1) x + \cdots + \sigma(r_n) x^n$$

is a ring homomorphism whose contraction to R is σ.

(2) We write the map $R[x] \to S[x]$ by σ.

Theorem 1.8 Let $\sigma: K \to L$ be an isomorphism of fields, u an element of some extension field of K and v an element of some extension field of L.

Assume that either

(1) u is transcendental over K and v is transcendental over L ; or

(2) u is a root of an irreducible polynomial $f \in K[x]$ and v is a root of $\sigma(f) \in L[x]$.

$\Rightarrow$ σ extends to an isomorphism of fields $K(u) \cong L(v)$ which maps u onto v.

Proof (1) By Remark above,

σ extends to an isomorphism $K[x] \cong L[x]$

$\Rightarrow$ the map $K(x) \to L(x)$ defined by

$$\frac{h(x)}{g(x)} \mapsto \frac{\sigma(h(x))}{\sigma(g(x))}$$

is an isomorphism.

By Theorem 1.5. $K(u) \cong K(x) \cong L(x) \cong L(v)$.

(2) W.L.O.G., we may assume that f is monic.

Since $\sigma: K[x] \to L[x]$ is an isomorphism,

$\sigma(f(x))$ is monic irreducible.

Now, consider

$$K(u) \cong K[x]/(f) \xrightarrow{\theta} L[x]/(\sigma(f(x))) \cong L(v)$$

Note that $\theta: K[x]/(f) \to L[x]/(\sigma(f(x)))$

defined by $\theta(g + (f)) = \sigma(g) + (\sigma(f(x)))$

is an isomorphism.

$\Longrightarrow$ $K(u) \cong L(v)$ whose contraction to K is σ

and u maps to v. ///

Corollary 1.9 Let E and F be extensions of a field K and

$u \in E$ and $v \in F$ be algebraic over K.

Then u and v are roots of the same irreducible

polynomial $f \in K[x]$

$\Longleftrightarrow$ $\exists$ an isomorphism of fields $K(u) \cong K(v)$

which sends u to v and is the identity map on K.

Proof ($\Longrightarrow$) Apply Theorem 1.8 to $\sigma = 1_K$

($\Longleftarrow$) Let $\sigma: K(u) \to K(v)$ be an isomorphism

s.t. $\sigma(u) = v$ and $\sigma(a) = a$ for all $a \in K$.

Choose the irreducible polynomial $f \in K[x]$ of u

$$\overset{\shortparallel}{\sum_{i=0}^{n} k_i x^i}$$

$$\Longrightarrow 0 = f(u) = \sum_{i=0}^{n} k_i u^i$$

$$\Longrightarrow 0 = \sigma\left(\sum_{i=0}^{n} k_i u^i\right)$$

$$= \sum_{i=0}^{n} k_i \sigma(u)^i$$

$$= \sum_{i=0}^{n} k_i v^i = f(v).$$ ///

Theorem 1.10 If K is a field and $f \in K[x]$ a polynomial of degree $n \geq 1$ then $\exists$ a simple extension field $F = K(u)$ of K $\ni$

(1) $u \in F$ is a root of f

(2) $[K(u) : K] \leq n$ with the equality holding if and only if f is irreducible in $K[x]$

(3) if f is irreducible in $K[x]$, then $K(u)$ is unique up to an isomorphism which is the identity on K.

Proof By replacing one of irreducible factors of f, we may assume that f is irreducible in $K[x]$

$\Rightarrow$ (f) is maximal in $K[x]$

$\Rightarrow$ $K[x]/(f)$ is a field and let $F := K[x]/(f)$

Note that the canonical projection $\pi : K[x] \to K[x]/(f)$ $(= F)$ is a monomorphism on K, because $\deg(f) \geq 1$.

$\Rightarrow$ F can be regarded as an extension of K because $\pi(K) \cong K$.

Let $u = \pi(x)$.

Claim: $F = K(u)$

$\because$ $(\supseteq)$ $\pi(x) (= u) \in F$

$\Rightarrow K(u) \subseteq F$

$(\subseteq)$ Let $(a_0 + a_1 x + \cdots + a_m x^m) + (f) \in F$

Then $(a_0 + a_1 x + \cdots + a_m x^m) + (f)$

$= \pi(a_0 + a_1 x + \cdots + a_m x^m)$

$= a_0 + a_1 u + \cdots + a_m u^m$

$\in K(u)$

(1) $f(u) = 0$

$\because$ Let $f = a_0 + a_1 x + \cdots + a_m x^m$

Then $f(u) = a_0 + a_1 u + \cdots + a_m u^m$

$= a_0 + a_1 (x + (f)) + \cdots + a_m (x^m + (f))$

$= f + (f) = 0$ $\because f \in K[x]$ ...

(2) Theorem 1.6

(3) Corollary 1.9. ///

Theorem 1.11 If F is a finite dimensional extension field of K, then F is finitely generated and algebraic over K.

Proof Let $[F:K]=n$ and $u\in F$.

Then $\{1_K, u, \cdots, u^n\}$ is linearly dependent

$\Rightarrow \exists\, a_0,\cdots,a_n\in K$, not all zero,

$\ni a_0+a_1u+\cdots+a_nu^n=0$

$\Rightarrow u$ is algebraic over K

$\Rightarrow F$ is algebraic over K

Let $\{v_1,\cdots,v_n\}$ be a basis for K-vector space F.

Then $F=K(v_1,\cdots,v_n)$.

$(\because)$ $(\supseteq)$ Clear.

$(\subseteq)$ $F=K\cdot v_1+\cdots+K\cdot v_n$

$=\langle v_1,\cdots,v_n\rangle$

$\subseteq K(v_1,\cdots,v_n)$. ///

Theorem 1.12 If F is an extension field of K and $X\subseteq F \ni F=K(X)$ and every element of X is algebraic over K, then F is an algebraic extension of K.

If $|X|<\infty$, then F is finite dimensional over K.

Proof Let $v\in F$.

Then $v\in K(u_1,\cdots,u_n)$ for some $u_i\in X$.

Consider a chain $K\subseteq K(u_1)\subseteq\cdots\subseteq K(u_1,\cdots,u_n)$.

Since u_i is algebraic over K, u_i is algebraic over $K(u_1,\cdots,u_{i-1})$ for $i=2,\cdots,n$