2. CLASSIFYING EXTENSIONS

We already defined some classifications for $K \hookrightarrow L$:

- finitely generated, if $L = K(\alpha_1, \dots, \alpha_n)$, $\alpha_i \in L$
- simple, if $L = K(\alpha)$, $\alpha \in L$
- finite, if $[L:K] < \infty$

Definition 2.1

Let $K \hookrightarrow L$ be a field extension.

- an element $\alpha \in L$ is <u>algebraic over K</u> if $\exists p \in K[t]$, $p \neq 0$, such that $p(\alpha) = 0$

  If no such p exists, α is <u>transcendental over K</u>

- The extension $K \hookrightarrow L$ is algebraic if every $\alpha \in L$ algebraic over K.

  The extension is transcendental if some element $\alpha \in L$ is transcendental over K.

- "algebraic" = algebraic over $\mathbb{Q}$

  "transcendental" = transcendantal over $\mathbb{Q}$

<u>Relations</u> (to be proved)

$$\begin{tikzcd}
 & \text{nontrivial} \arrow[dl] \arrow[r] & \, & \text{simple} \arrow[d, Rightarrow] \\
\text{algebraic} & & \text{finite} \arrow[ll, Rightarrow] \arrow[ur, Rightarrow] \arrow[r, Rightarrow] & \text{finitely gen} \arrow[d, Rightarrow] \\
\text{transcendental} \arrow[rr, Rightarrow] & & \text{infinite} & \text{infinitely gen}
\end{tikzcd}$$

Example 2.2

- $\sqrt{2}$ is algebraic as a root of $t^2-2 \in \mathbb{Q}[t]$
- $\mathbb{Q} \hookrightarrow \mathbb{Q}(\sqrt{2}) = \{a+b\sqrt{2} : a, b \in \mathbb{Q}\}$ is algebraic: $a+b\sqrt{2}$ is a root of $(t-a)^2 - 2b^2 \in \mathbb{Q}[t]$
- $\pi, e, \sin\sqrt{2}$ are transcendental (Lindemann - Weierstrass)

Example 2.3

Let K be a field and $L = K(x)$ the field of rational functions in the indeterminate x. Then $K \hookrightarrow L$ is transcendental:

Let $p = a_n t^n + \dots + a_0 \in K[t]$ such that

$$p(x) = a_n x^n + \dots + a_0 = 0 \in L$$

But then $a_n = \dots = a_0 = 0$, so $p = 0$.

Theorem 2.4

Let $K \subset \mathbb{C}$ subfield and $\alpha \in \mathbb{C}$. Every simple transcendental extension $K \hookrightarrow K(\alpha)$ is isomorphic to $K \hookrightarrow K(x)$ with $K(x)$ the field of rational functions in the indeterminate x.

Proof

$$\begin{tikzcd} K(x) \arrow[r, "\phi"] & K(\alpha) \\ K \arrow[u, hook] \arrow[r, "id"] & K \arrow[u, hook] \end{tikzcd}$$

Define $\phi(p/q) = p(\alpha)/q(\alpha)$

$\phi|_K : K \to K$ is the identity, so suffices to show ϕ is a field isomorphism.

ϕ homomorphism:

$$\phi\left(\frac{p}{q}+\frac{\hat{p}}{\hat{q}}\right)=\phi\left(\frac{p\hat{q}+\hat{p}q}{q\hat{q}}\right)=\frac{p(\alpha)\hat{q}(\alpha)+\hat{p}(\alpha)q(\alpha)}{q(\alpha)\,\hat{q}(\alpha)}=\frac{p(\alpha)}{q(\alpha)}+\frac{\hat{p}(\alpha)}{\hat{q}(\alpha)}$$

similarly $\phi\left(\frac{p}{q}\cdot\frac{\hat{p}}{\hat{q}}\right)=\frac{p(\alpha)}{q(\alpha)}\cdot\frac{\hat{p}(\alpha)}{\hat{q}(\alpha)}$.

ϕ injective:

If $\phi(p/q)=p(\alpha)/q(\alpha)=0$, then $p(\alpha)=0$.

By assumption α transcendental over $K \Rightarrow p=0 \Rightarrow p/q=0$.

ϕ surjective:

By Lemma 1.6, every element of $K(\alpha)$ can be obtained as a finite sequence of field operations using K and α. Since $\phi(K)=K$ and $\phi(x)=\alpha$, surjectivity follows. $\square$

$\rightsquigarrow$ complete classification of simple transcendental extensions:

$K(x)$ is the only one!

<u>Corollary 2.5</u>

If $K \hookrightarrow K(\alpha)$ is a transcendental extension, then $[K(\alpha):K] < \infty$.

<u>Proof</u>

$K \hookrightarrow K(\alpha)$ is isomorphic to $K \hookrightarrow K(x)$.

In $K(x)$, the elements $1, x, x^2, x^3, \dots$ are all K-linearly independent. $\square$

Recall: a polynomial $p = a_n t^n + \dots + a_0$ is monic if $a_n = 1$.

Definition 2.6

Let $K \hookrightarrow L$ be a field extension and $\alpha \in L$ algebraic over K.
The <u>minimal polynomial of α over K</u> is
a monic polynomial $m \in K[t]$ of minimal degree s.t. $m(\alpha) = 0$

Lemma 2.7

Let $\alpha \in L$ be algebraic over K and m its minimal polynomial.
If $p \in K[t]$ has $p(\alpha) = 0$, then $m \mid p$ (m divides p)

Proof

Polynomial division $\Rightarrow \exists q, r \in K[t]$ such that

$$p = qm + r, \qquad \deg r < \deg m$$

Then $r(\alpha) = p(\alpha) - q(\alpha) m(\alpha) = 0$.
By definition m has minimal degree among nonzero polynomials with α as a root $\Rightarrow r = 0 \Rightarrow m \mid p$ $\square$

Lemma 2.7 $\Rightarrow$ the minimal polynomial is unique:
If $m, \hat{m}$ monic and $m \mid \hat{m}$, $\hat{m} \mid m$, then $m = \hat{m}$.

Example 2.8

$\alpha = e^{2\pi i/5} \in \mathbb{C}$ is algebraic : $\alpha^5 = e^{2\pi i} = 1$

So α is a root of $p = t^5 - 1 \in \mathbb{Q}[t]$.

However p is not the minimal polynomial. The minimal poly is

$$m = t^4 + t^3 + t^2 + t + 1 \in \mathbb{Q}[t] \qquad (p = (t-1)m)$$

Proposition 2.9

Let $K \hookrightarrow L$ and $\alpha \in L$ algebraic over K.

The minimal polynomial of α over K is irreducible over K.

Proof

Suppose $m = pq$ with $p, q \in K[t]$, $\deg p, \deg q < \deg m$.

$0 = m(\alpha) = p(\alpha)q(\alpha) \Rightarrow$ either $p(\alpha) = 0$ or $q(\alpha) = 0$.

But this contradicts the minimality in degree of m. $\square$

Proposition 2.10

Let K be a subfield of $\mathbb{C}$ and $m \in K[t]$ irreducible, monic

Let $\alpha \in \mathbb{C}$ be any root of m. Then

m is the minimal polynomial of α over K.

Proof

Let $\hat{m}$ be the minimal polynomial of α over K.

Lemma 2.7 $\Rightarrow$ $\hat{m} \mid m$.

m irreducible $\Rightarrow \hat{m} = m$. $\square$

Definition 2.11

Let $m \in K[t]$. The ideal generated by m is

$$\langle m \rangle = \{ pm : p \in K[t] \} \subset K[t]$$

Theorem 2.12

The quotient ring $K[t]/\langle m \rangle$ is a field if and only if m is irreducible.

Proof

"$\Rightarrow$" If m is reducible, then $m = fg$ with $\deg f, \deg g < \deg m$. Since $\deg f < \deg m$, $f \notin \langle m \rangle$, so its coset $[f] \in K[t]/\langle m \rangle$ is not zero. Similarly $0 \neq [g] \in K[t]/\langle m \rangle$.

However $[f][g] = [fg] = [m] = 0 \in K[t]/\langle m \rangle$

so $[f]$ is a zero divisor, which is impossible in a field.

"$\Leftarrow$" Let $0 \neq [f] \in K[t]/\langle m \rangle$. We need to find $[f]^{-1}$, i.e. a polynomial $g \in K[t]$ such that $[fg] = [1]$.

Since $[f] \neq 0$, $m \nmid f$. By irreducibility of m, $\gcd(m, f) = 1$.

Bezout's identity $\Rightarrow$ $\exists h, g \in K[t]$ such that $hm + gf = 1$

$\Rightarrow$ $[1] = [hm + gf] = [hm] + [gf] = [g][f]$ $\square$

Theorem 2.13

Let $K \hookrightarrow K(\alpha)$ be a simple algebraic extension.
Let $m \in K[t]$ be the minimal polynomial of α.
Then $K \hookrightarrow K(\alpha)$ is isomorphic to $K \hookrightarrow K[t]/\langle m \rangle$.

Proof

$$\begin{tikzcd} K[t]/\langle m \rangle \arrow[r, "\phi"] & K(\alpha) \\ K \arrow[u, hook] \arrow[r, "id"] & K \arrow[u, hook] \end{tikzcd}$$

Define ϕ by $[p] \mapsto p(\alpha)$

i) ϕ is well defined:

If $[p] = [q]$, then $m \mid (p-q)$

$\Rightarrow (p-q)(\alpha) = 0 \Rightarrow p(\alpha) = q(\alpha)$

ii) $\phi : K \to K$ is the identity (evaluation of constant poly)

iii) ϕ is a field homomorphism:

$\phi([p]+[q]) = \phi([p+q]) = p(\alpha) + q(\alpha) = \phi[p] + \phi[q]$

$\phi([p][q]) = \phi([pq]) = p(\alpha)q(\alpha) = \phi[p] \cdot \phi[q]$

iv) ϕ is injective: by (i), $\phi[0] = 0 \in K(\alpha)$

v) ϕ is surjective: $\phi[t] = \alpha$

$\Rightarrow$ image of ϕ is a field containing K and α

By definition of $K(\alpha)$, ϕ is surjective. $\square$

Corollary 2.14

Let $K \hookrightarrow K(\alpha)$ and $K \hookrightarrow K(\beta)$ be two simple algebraic extensions such that α and β have the same minimal polynomial $m \in K[t]$. Then $K \hookrightarrow K(\alpha)$ and $K \hookrightarrow K(\beta)$ are isomorphic.

Proof

Both field extensions are isomorphic to $K \hookrightarrow K[t]/\langle m \rangle$ $\square$

Proposition 2.15

Let $K \hookrightarrow K(\alpha)$ simple algebraic extension, $m \in K[t]$ minimal polynomial of α.
Then $[K(\alpha):K] = \deg m$ and $\{1, \alpha, \alpha^2, \dots, \alpha^{\deg m - 1}\}$ is a K-vector space basis of $K(\alpha)$.

Proof Let $n = \deg m$.

i) Linear independence: suppose $k_0 + k_1\alpha + \dots + k_{n-1}\alpha^{n-1} = 0$, with $k_i \in K$. Then $[k_0 + k_1 t + \dots + k_{n-1} t^{n-1}] = 0 \in K[t]/\langle m \rangle$

$\Rightarrow m \mid k_0 + \dots + k_{n-1} t^{n-1}$.

Since $\deg m = n$, this is only possible if $k_0 = \dots = k_{n-1} = 0$.

ii) $\{1, \dots, \alpha^{n-1}\}$ span all of $K(\alpha)$:

Every element $\beta \in K(\alpha)$ is given by a finite sequence of field operations

$$\Longrightarrow \quad \beta = \frac{p(\alpha)}{q(\alpha)}, \quad p, q \in K[t] \text{ (see Exercise 1)}$$

Since $q(\alpha) \neq 0$, Thm 2.13 implies $m \nmid q$.

Then $1 = am + bq$ for some $a, b \in K[t]$,

so $\frac{1}{q(\alpha)} = b(\alpha) \quad \Longrightarrow \quad \beta = p(\alpha) b(\alpha)$.

So every element has the form $\beta = \tilde{p}(\alpha)$, $\tilde{p} \in K[t]$

By polynomial division

$$\tilde{p} = qm + r, \quad q, r \in K[t], \quad \deg r < \deg m.$$

Hence $\beta = \tilde{p}(\alpha) = q(\alpha) m(\alpha) + r(\alpha) = r(\alpha)$

and $r(\alpha)$ is a K-linear combination of $1, \dots, \alpha^{n-1}$. $\square$

$$\text{simple algebraic extensions } K \hookrightarrow K(\alpha) \text{ of degree } n$$

$$\Updownarrow$$

$$\text{irreducible polynomials } m \in K[t] \text{ of degree } n$$