Theorem 4.13 (Constructing intermediate fields)

Let $k \subseteq K$ be a field extension, $a \in K$ a root of some non-zero polynomial in $k[x]$. Then

$$k[a] := \{ f(a) \in K \mid f \in k[x] \}$$

is a field with field extensions $k \subseteq k[a] \subseteq K$, and $(1, a, a^2, \ldots, a^{n-1})$ is a basis for $k[a]$ over k, with

$$n = \min \{ \deg(p) \mid p \in k[x], p(a) = 0 \}.$$

Sketch proof

- Apply First Isomorphism Theorem

$$\varphi_a : k[x] \longrightarrow K$$
$$f \longmapsto f(a).$$

$\mathrm{Im}(\varphi_a) = k[a]$.

Since $k[x]$ is PID,

$\exists p \in k[x]$ s.t. $\ker(\varphi_a) = k[x]p$.

So $k[a] \cong k[x] / k[x]p$.

- If p is irreducible, we can apply Theorem 3.17.

- $p = 0$ or p a unit
  contradict $k \subsetneq \mathrm{Ker}(\varphi_a) \neq 0$.
- $p = fg$ with f, g non-zero non-units in $k[x]$

  $\Rightarrow f$ or $g \in \mathrm{Ker}(\varphi_a)$ ⨯

So p is irreducible,
hence $k[a]$ is a field,
$k \subseteq k[a] \subseteq K$ a field
extension, and $n = \deg(p)$.

- Check $(1, a, \ldots, a^{n-1})$ spans:

  let $f(a) \in k[a]$.

Divide f by p with
remainder: $f = qp + r$,
$q, r \in k[x]$, $\deg(r) < \deg(p)$.

Evaluate at a:

$f(a) = r(a)$,
so highest power of a in $f(a)$
is less than n.

- Check linear independence:

  suppose $\sum_{i=0}^{n-1} c_i a^i = 0$

  Let $h = \sum_{i=0}^{n-1} c_i x^i \in k[x]$.

  $\deg(h) < \deg(p)$, $h(a) = 0$,

  so $h = 0 \Rightarrow c_i = 0$. □

Theorem 4.15 (Constructing field extensions containing roots)

Let $p \in \Bbbk[x]$ be irreducible. The field extension $\Bbbk \subseteq K := \Bbbk[x]/\Bbbk[x]p$ has dimension $n := \deg(p)$ as a $\Bbbk$-vector space, and $a := [x] \in K$ is a root of p.

Sketch proof

- $\Bbbk$ a field $\Rightarrow \Bbbk[x]$ a PID $\Rightarrow K$ is a field, since p is irreducible. $\Bbbk \cong \Bbbk[1] \subseteq K$ is a field extension.
- Let $f \in \Bbbk[x]$. Evaluate at $a = [x]$ to get $f(a) = [f]$, so $p(a) = [p] = [0]$ so a is a root of p in K.
- $\Bbbk[a] = \{f(a) \mid f \in \Bbbk[x]\}$
  $= \{[f] \mid f \in \Bbbk[x]\} = K$,

$\dim K = \min\{\deg(f) \mid f \in k[x], f(a) = 0\}$.

- For $h \in k[x]$,
  $h(a) = [0] \Rightarrow p \mid h$,
  so $\dim K = \deg(p)$. □.

Proposition 5.19

Let $\alpha \in \mathrm{End}(V)$, $\Delta_\alpha(t) = (\lambda - t)^r$, $m_\alpha(t) = (t-\lambda)^s$. Write $\alpha_\lambda := (\alpha - \lambda \mathrm{id})$. For $0 \neq v \in V$, let $e := e(v)$ be smallest +ve integer s.t. $\alpha_\lambda^e(v) = 0$.

Write
$v_1 = \alpha_\lambda^{e-1} v$, $v_2 = \alpha_\lambda^{e-2} v$, ...

$v_{e-1} = \alpha_\lambda v$, $v_e = v$.

Then

(1) $(v_1, \dots, v_e)$ is a basis for $W := \mathbb{C}[\alpha]v$.

(2) in this basis, matrix for $\beta := \alpha|_W \in \mathrm{End}(W)$ is

$$J(\lambda, e) = \begin{bmatrix} \lambda & 1 & & \\ & \lambda & 1 & \\ & & \ddots & \\ & & & \lambda \end{bmatrix}$$

(3) $E_\beta(\lambda) = \mathbb{C}v$, $\Delta_\beta(t) = (\lambda - t)^e$,

$m_\beta(t) = (t-\lambda)^e$.

Sketch proof

(1) • $\alpha_\lambda^s(v) = m_\alpha(\alpha)v = 0$ so

e is well-defined.

• Let $w = f(\alpha)v \in W$, $f \in \mathbb{C}[t]$.

Exercise 9.1:

$f(t) = a_0 + a_1(t-\lambda) + \cdots + a_k(t-\lambda)^k$

for some $k \geq 0$, $a_i \in \mathbb{C}$.

So $w = f(\alpha)v$

$= a_0 v + a_1 \alpha_\lambda v + a_2 \alpha_\lambda^2 v + \cdots$

$\in \text{span}\{v_1, \ldots, v_e\}$

• Exercise 9.3: $v_1, \ldots, v_e$ are linearly independent.

$\Rightarrow (v_1, \ldots, v_e)$ is a basis for W.

(2) • Columns of matrix B for $\beta = \alpha|_W$ in this basis are

$\alpha(v_i)$, $1 \leq i \leq e$.

• Compute this using

$\alpha(v_i) = \lambda v_i + (\alpha - \lambda id)v_i$

$= \lambda v_i + \alpha_\lambda v_i$

to get

$\alpha(v_1) = \lambda v_1,$

$\alpha(v_i) = v_{i-1} + \lambda v_i, \quad i \geq 2.$

(3) Exercise 9.4. $\square$.