4.4 The normal basis theorem

L/K finite Galois

$G = Gal(L/K)$

Then L is a K-linear G-repr. via $\sigma . a = \sigma(a)$.

Lemma 1: There is an $a \in L$ s.t. $(\sigma(a))_{\sigma \in G}$ is a basis of L as K-v.s.

iff. $L \cong K[G]$ as G-repr's.

the regular repr. of G

proof: • For every $a \in L$, the map

$$\varphi_a : K[G] \longrightarrow L$$

$$\sum_{\sigma \in G} c_\sigma \cdot \sigma \longmapsto \sum_{\sigma \in G} c_\sigma \sigma(a) \qquad (c_\sigma \in K)$$

is a G-hom. since:

- K-lin.: • $\varphi_a(b \cdot \sum c_\sigma \cdot \sigma) = \varphi_a(\sum b c_\sigma \cdot \sigma)$

$= \sum b c_\sigma \cdot \sigma(a) = b \cdot \varphi_a(\sum c_\sigma \cdot \sigma)$

• $\varphi_a(\sum c_\sigma \cdot \sigma + \sum d_\sigma \cdot \sigma) = \varphi_a(\sum (c_\sigma + d_\sigma) \cdot \sigma)$

$= \sum (c_\sigma + d_\sigma) \cdot \sigma(a) = \varphi_a(\sum c_\sigma \cdot \sigma) + \varphi_a(\sum d_\sigma \cdot \sigma)$

- G-equiv: $\varphi_a(\tau . \sum c_\sigma \sigma) = \varphi_a(\sum c_\sigma \cdot (\tau\sigma)) = \sum c_\sigma (\tau\sigma)(a)$

$= \tau(\sum c_\sigma \sigma(a)) = \tau . \varphi_a(\sum c_\sigma \sigma)$ ✓

- Conversely every G-hom $\varphi: K[G] \to L$ is of this form since $\varphi(\sigma) = \sigma . \varphi(id_L) = \sigma(a)$ for $a = \varphi(id_L)$ and thus

$$\varphi\left(\sum c_\sigma \cdot \sigma\right) \underset{\uparrow}{=} \sum c_\sigma \varphi(\sigma) = \sum c_\sigma \sigma(a) = \varphi_a\left(\sum c_\sigma \sigma\right).$$

(φ is K-linear)

- Since $\dim_K K[G] = \# G = \dim_K L$,

φ_a is an isom. of G-repr. (i.e. bijective)

$\iff \varphi_a$ is surjective

$\iff (\sigma(a))_{\sigma \in L}$ is a basis for L/K. $\square$

<u>Thm. 2:</u> $L \simeq K[G]$ as G-repr.

<u>proof</u>:
- $L \otimes_K L$ is an $L[G]$-module via

$$\left(\sum c_\sigma \sigma\right). a \otimes b = \sum c_\sigma a \otimes \sigma(b)$$

(exercise!)

- For $\sigma \in G$, the map

$$\lambda_\sigma : L \otimes_K L \longrightarrow L$$
$$a \otimes b \longmapsto a\sigma(b)$$

is L-linear, i.e.
- $\sigma(ca \otimes b) = c\, \sigma(a \otimes b)$
- $\sigma((a+a') \otimes b) = \sigma(a \otimes b) + \sigma(a' \otimes b)$

for $a, a', b, c \in L$. (exercise!)

Thus

$$\lambda_\sigma \in (L \otimes_K L)^* = \mathrm{Hom}_L(L \otimes_K L, L).$$

- Assume that $\sum_{\sigma\in G} c_\sigma \cdot \lambda_\sigma = 0$ for some $c_\sigma \in L$.

  $\Rightarrow \quad 0 = \sum c_\sigma \cdot \lambda_\sigma(1\otimes b) = \sum c_\sigma\, \sigma(b) \quad \forall b\in L$

  $\Rightarrow \quad c_\sigma = 0 \quad \forall \sigma\in G$

(Artin's Thm. I.4.4.3 on lin. indep. of char.)

  Thus $\{\lambda_\sigma\}_{\sigma\in G}$ is lin. indep. over L.

- Since $\#\{\lambda_\sigma\}_{\sigma\in G} = \# G = \dim_L (L\otimes_K L)^*$,

  $\{\lambda_\sigma\}_{\sigma\in G}$ is a basis of $(L\otimes_K L)^*$.

- Thus the L-linear map

$$\begin{aligned} \Phi : L\otimes_K L &\longrightarrow L[G] \\ a\otimes b &\longmapsto \sum_{\sigma\in G} \lambda_\sigma(a\otimes b)\,\sigma^{-1} \end{aligned}$$

  is an isomorphism of L-v.s. (exercise !)

- Φ is G-equiv. since for $\tau\in G$, $a\otimes b\in L\otimes_K L$,

$$\Phi(\tau.(a\otimes b)) = \sum_\sigma \lambda_\sigma(a\otimes \tau(b))\,\sigma^{-1}$$

$$= \tau\Big(\sum_\sigma a\otimes \sigma\tau(b)\Big)\tau^{-1}\sigma^{-1}$$

($\sum_\sigma a\otimes\sigma\tau(b)$ is conj.-inv.)

$$= \tau.\Big(\sum_{\tilde\sigma} a\otimes\tilde\sigma(b)\Big)\tilde\sigma^{-1}$$

($\tilde\sigma = \sigma\tau$)

$$= \tau.\Phi(a\otimes b).$$

- Let $\{a_1 \ldots a_n\}$ be a basis of L as K-v.s.

  Then

$$L \otimes_K L \simeq \bigoplus_{i=1}^{n} a_i \otimes L \xrightarrow{\sim} \bigoplus_{i=1}^{n} L$$
$$(a_i \otimes b_i)_{i=1,\dots,n} \longmapsto (b_i)_{i=1,\dots,n}$$

and

$$\bigoplus_{i=1}^{n} K[G] \xrightarrow{\sim} L[G]$$
$$\left(\sum_\sigma c_{\sigma,i}\,\sigma\right)_{i=1,\dots,n} \longmapsto \sum_\sigma \left(\sum_{i=1}^{n} c_{\sigma,i} a_i\right) \sigma$$

as $K[G]$-modules. (exercise!)

Thus

$$\bigoplus_{i=1}^{n} K[G] \simeq L[G] \simeq L \otimes_K L \simeq \bigoplus_{i=1}^{n} L$$

as $K[G]$-modules.

- Let $V_1, \dots, V_s$ be non-isom. irred. G-repr. and

$$K[G] \simeq \bigoplus_{i=1}^{s} V_i^{d_i}, \qquad L \simeq \bigoplus_{i=1}^{s} V_i^{e_i}.$$

Then

$$\bigoplus_{i=1}^{s} V_i^{n \cdot d_i} \simeq \bigoplus_{i=1}^{n} K[G] = \bigoplus_{i=1}^{n} L \simeq \bigoplus_{i=1}^{s} V_i^{n \cdot e_i}$$

$\Rightarrow$ $d_i = e_i$ for $i = 1, \dots, s$

$\Rightarrow$ $K[G] \simeq \bigoplus V_i^{d_i} \simeq L$ as $K[G]$-repr. $\square$

Thm 3 (Normal basis theorem)
L/K finite Galois with Galois group G.
Then there is an $a \in L$ s.t. $(\sigma(a))_{\sigma \in G}$ is a basis of L/K.

proof: Immediate from Thm. 2 & Lemma 1. $\square$