Lecture 38

(38.0) Let K be a field (fixed throughout). An <u>algebra</u> over K or <u>K-algebra</u> (always assumed to be unital and associative) is a K-vector space A, together with a

- K-bilinear multiplication $\begin{array}{ccc} A \times A & \longrightarrow & A \\ (a,b) & \longmapsto & a.b \end{array}$ s.t.

$\forall a,b,c \in A$; $(a.b).c = a.(b.c)$ [A is associative ring]

- $1_A \in A$ (unit), s.t. $1_A . a = a = a . 1_A$ $\forall a \in A$

Identifying $K \ni 1 \longleftrightarrow 1_A \in A$, allows us to view $K \subset A$

[i.e. we have a map of rings $\begin{array}{ccc} K & \longrightarrow & A \\ 1 & \longmapsto & 1_A \end{array}$. As K is a field, this map is injective, and we identify K with its image: $K \subset A$]

A is commutative if $a.b = b.a$ $\forall a,b \in A$.

Our main example would be $A = L \supset K$ a field exention.

Or $A = K[X]/f(X)$, $f(x) \in K[X]$ a monic [NOT necessarily irred.] polynomial.

$\cup$

K (= constant polynomials)

Notation: $(A:K) = \dim_{K\text{-v.s.}}(A)$

(38.1) Norm and trace. Let A be a finite-dimensional K-algebra. $\forall \alpha \in A$, we have two linear maps:

$\mathfrak{L}_\alpha$ = left mult. by α : $A \longrightarrow A$, $\beta \longmapsto \alpha\beta$

$\mathfrak{R}_\alpha$ = right " " " : $\beta \longmapsto \beta\alpha$

We assume that A is commutative, and only use $\mathfrak{L}_\alpha$ for the mult. by α. $\mathfrak{L}_\alpha \in \mathrm{End}_{K\text{-v.s.}}(A)$

Norm of α, denoted by $N_{A/K}(\alpha) \in K$, is the determinant:

$$N_{A/K}(\alpha) = \det(\mathfrak{L}_\alpha)$$

Similarly $\mathrm{Tr}_{A/K}(\alpha)$ (trace of α) $= \mathrm{Tr}(\mathfrak{L}_\alpha)$

Example. – $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in K[x]$

$A = K[x]/(f(x))$. Basis: $\{1, x, x^2, \ldots, x^{n-1}\}$

$\alpha = \bar{x} \in A$. $\mathfrak{L}_\alpha : 1 \mapsto x \mapsto x^2 \mapsto \cdots \mapsto x^{n-1} \mapsto -a_0 - a_1 x - \cdots - a_{n-1} x^{n-1}$

Matrix $\mathfrak{L}_\alpha = \begin{bmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & & & -a_1 \\ 0 & 1 & \ddots & & \vdots \\ \vdots & 0 & \ddots & 0 & \\ 0 & 0 & \cdots & 1 & -a_{n-1} \end{bmatrix}$

$\mathrm{Tr}_{A/K}(\alpha) = -a_{n-1}$

$N_{A/K}(x) = (-1)^n a_0$

(38.2) Prop. Consider an extension of fields $K \subset L$ and a f.d. commutative algebra A over L. Let $m = (A:L)$ and $\alpha \in L$. Then

$$N_{A/K}(\alpha) = N_{L/K}(\alpha)^m$$

$$Tr_{A/K}(\alpha) = m\, Tr_{L/K}(\alpha)$$

$$\left[\begin{array}{c} A \\ \cup \\ \alpha \in L \\ \cup \\ K \end{array}\right] \Big\} \deg m$$

Proof. Let $k = (\not{*}L : K)$ and $\{\omega_1, \dots, \omega_k\}$ a basis of L as K-v.s.

View mult. by α as a linear (over K) map from L to itself, denote it by $\mathcal{L}_\alpha : \not{*}L \longrightarrow L$, $\beta \longmapsto \alpha\beta$. Let $X \in Mat_{k\times k}(L)$ be defined by

$$\mathcal{L}_\alpha \omega_i = \sum_{j=1}^{k} X_{ij}\, \omega_j \qquad (X_{ij} \in K)$$

Let $\{\lambda_1, \dots, \lambda_m\}$ be a basis of A as an L-vector space.

$\tilde{\mathcal{L}}_\alpha : A \to A$, $\beta \longmapsto \alpha\beta$ maps $\lambda_s \omega_t \longmapsto \sum_{j=1}^{k} X_{tj}\, \lambda_s \omega_j$

Thus matrix of $\tilde{\mathcal{L}}_\alpha$ in (ordered basis) $\{\lambda_1\omega_1, \dots, \lambda_1\omega_k, \lambda_2\omega_1, \dots, \lambda_2\omega_k, \dots \dots \lambda_m\omega_1, \dots, \lambda_m\omega_k\}$

$\lambda_1\omega_1 \cdots \lambda_1\omega_k \lambda_2\omega_1 \cdots \lambda_2\omega_k \cdots$ [m blocks]

is

$$\begin{bmatrix} \boxed{X} & 0 & 0 & \cdots \\ 0 & \boxed{X} & 0 & \\ 0 & 0 & \boxed{X} & \\ \vdots & & & \ddots \\ & & & \boxed{X} \end{bmatrix}$$

and the prop. follows

□

Remark: For an arbitrary f.d. comm. A/K, proceed as follows. Given $\alpha \in A$, let $L = K[\alpha]$. As A is f.d. so is L. So $L \simeq K[x]/(f(x))$. If $f(x)$ is irred. Prop. ~~39~~ (38.2) helps compute $N_{A/K}(\alpha) = \left((-1)^{\deg f} \cdot \text{constant term of } f\right)^{\dim_K A}$ (dim of v.s.)

(38.3) Theorem. — Let L/K be a finite Galois extension. $G = \mathrm{Gal}(L/K)$. Then, for any $\alpha \in L$,

$$N_{L/K}(\alpha) = \prod_{\sigma \in G} \sigma \cdot \alpha \quad ; \quad Tr_{L/K}(\alpha) = \sum_{\sigma \in G} \sigma \cdot \alpha$$

(Note: R.H.S. of each equation above $\in L^G = K$.)

Proof. — We are going to use: $f(x) =$ min'l poly of α

$$= \prod_{\tilde{\alpha} \in G\cdot\alpha} x - \tilde{\alpha}$$

($G\cdot\alpha$ = orbit of α)

(Proof. $\sigma \cdot f(x) = f(x) \ \forall \sigma \in G \Rightarrow f(x) \in K[x]$.

Now if $p(x) \in K[x]$ is s.t. $p(\alpha) = 0$. we get $p(\sigma\cdot\alpha) = 0$.

$\Rightarrow \deg(p) \geq \deg(f) = |G\cdot\alpha| = \dfrac{|G|}{|\mathrm{Stab}_G(\alpha)|}$)

By the remark above, and

$$\left.\begin{array}{c} L \\ | \\ K(\alpha) \end{array}\right\} \text{Galois, of group } \mathrm{Stab}_G(\alpha)$$

$$\left.\begin{array}{c} K(\alpha) \\ | \\ K \end{array}\right\} \deg = \text{degree of } f = |G\cdot\alpha|$$

we get

$$N_{L/K}(\alpha) = N_{K(\alpha)/K}(\alpha)^{|\mathrm{Stab}_G(\alpha)|}$$

$$= \left((-1)^{\deg(f)} \cdot \text{Constant term of } f\right)^{|\mathrm{Stab}_G(\alpha)|}$$

$$\left(f(x) = (x-\alpha_1)\dots(x-\alpha_r)\right.$$
$$\left.\text{where } \{\alpha_1,\dots,\alpha_r\} = G\cdot\alpha, \text{ implies } f(0) = (-1)^{\deg f}\alpha_1\cdots\alpha_r\right)$$

$$= \left(\prod_{\tilde{\alpha}\in G\cdot\alpha} \tilde{\alpha}\right)^{|\mathrm{Stab}_G(\alpha)|}$$

$$= \prod_{\sigma\in G} (\sigma\cdot\alpha)$$

— exactly same argument for trace, left as an exercise. □

(38.4) Theorem (Hilbert's 90th problem). — Assume L/K is a finite Galois extn with $G = \mathrm{Gal}(L/K)$ a cyclic gp. of order m. Then $\forall\ \beta\in L^\times$ s.t. $N_{L/K}(\beta) = 1$, $\exists\ \alpha\in L^\times$ s.t.

$$\beta = \frac{\alpha}{\sigma(\alpha)} \qquad \left(\langle\sigma\rangle = G\ ;\ \sigma^m = e\right)$$

Proof Define $\eta : G \longrightarrow L^\times$

$$\sigma^k \longmapsto \beta\cdot\sigma(\beta)\cdot\ldots\cdot\sigma^{k-1}(\beta)$$

$N_{L/K}(\beta) = \beta \cdot (\sigma\beta) \cdot \ldots \cdot (\sigma^{m-1}\beta) = 1 \Rightarrow \eta$ satisfies

$$\eta(\sigma_1\sigma_2) = \sigma_1(\eta(\sigma_2))\,\eta(\sigma_1) \quad \forall\ \sigma_1, \sigma_2 \in G(=\langle\sigma\rangle)$$

As $H^1(G; L^\times) = \{1\}$ (see Noether's eqⁿs), $\exists\ \alpha \in L^\times$

s.t. $\beta = \dfrac{\alpha}{\sigma(\alpha)}$.

$$\left(\begin{array}{ccc} \| & & \| \\ \eta(\sigma) & = & (d\alpha)(\sigma) \end{array}\right)$$

(38.5) Cor. (alternate proof of Kummer's theorem - for cyclic groups). Let L/K be a Galois extn with cyclic Galois group $G = \mathrm{Gal}(L/K) \simeq \mathbb{Z}/m\mathbb{Z}$. If K contains a primitive

$$\begin{array}{ccc} \sigma & \leftarrow & \tau \\ \Downarrow & & \\ \end{array}$$

m^{th} root of unity, then L = splitting extn. of a polynomial

$X^m - a$ $(a \in K)$.

Proof ~~As~~ Let $\zeta \in K^\times$ be a primitive m^{th} root of unity.

Then $N_{L/K}(\zeta^{-1}) = (\zeta^{-1})^{|G|} = \zeta^{-m} = 1 \Rightarrow \exists\ \alpha \in L^\times$ s.t.

$\dfrac{\alpha}{\sigma(\alpha)} = \zeta^{-1}$. Hence $G\cdot\alpha = \{\alpha, \zeta\alpha, \zeta^2\alpha, \ldots, \zeta^{m-1}\alpha\}$ (all distinct)

and $\alpha^m \in K^\times$ (say a)

This also proves $L \simeq K(\alpha)$ = splitting extn of $X^m - a$. □