Lecture 3, 4.11.

Last time:

$f \in K[X]$ irreducible $\rightsquigarrow$ extension field $L := K[X]/(f)$ of K (stem field)

$f \in K[X] \rightsquigarrow$ splitting field

Both constructive (if K is)

f called separable if all roots of f in a splitting field are distinct.

Proved: if f irred and char $K = 0 \Rightarrow f$ separable.

Def 2.19:

$K \subseteq L$ is called:

- finite if $\dim_K L < \infty$.
- algebraic if each $\alpha \in L$ algebraic over K $\forall \alpha \in L$
- separable if algebraic and μ_α separable $\forall \alpha \in L$.

always true if char $K = 0$!

Lemma 2.20:

$K \subseteq L$ finite $\Rightarrow$ algebraic

Proof:

Let $\alpha \in L$. The powers $1, \alpha, \alpha^2, \ldots$ must eventually become linear dependent

$\Rightarrow \alpha$ algebraic. $\square$

Lemma 2.21: Let $K \subseteq L$ and let $L \subseteq M$ be a finite separable extension, $n = \dim_L M$. Let $\Omega \supseteq M$ be algebraically closed. Then any K-morphism $\tau : L \to \Omega$ extends in precisely n ways to a K-morphism $\sigma : M \to \Omega$:

$$\begin{tikzcd} M \arrow[r, "\sigma"] & \Omega \\ L \arrow[u] \arrow[ur, "\tau"'] & \end{tikzcd}$$

Proof: By induction on n. Case $n = 1$ clear. Let $n > 1$. Choose $\alpha \in M$, $\alpha \notin L$. Let $f := p_{\alpha, L}$, $r := \deg f$. Consider $L \subset L(\alpha) \subseteq M$.

Have $\dim_L L(\alpha) = r$, $\dim_{L(\alpha)} M = \frac{n}{r}$. Let $\tau : L \to \Omega$ be a morphism.

For any extension $\sigma : M \to \Omega$ have

$$f(\alpha) = 0 \Rightarrow \tau(f)(\sigma(\alpha)) = 0$$

so σ maps roots of f to roots of $\tau(f)$. For any root β of $\tau(f)$ in Ω get an extension

$$L(\alpha) \longrightarrow \Omega$$

$$b_0 + b_1\alpha + \dots + b_{r-1}\alpha^{r-1} \longmapsto \tau(b_0) + \tau(b_1)\beta + \dots + \tau(b_{r-1})\beta^{r-1}$$

Since f separable, also $\tau(f)$ separable $\Rightarrow$ $\deg f = \dim_L L(\alpha)$ choices for β

$\Rightarrow$ $\dim_L L(\alpha)$ extensions of τ to $L(\alpha)$.

By induction, each extension $\sigma : L(\alpha) \to \Omega$ extends in precisely $\frac{n}{r}$ ways to $M \to \Omega$. $\Rightarrow$ claim. $\square$

Ex 2.22: Consider $\mathbb{Q} \subseteq \mathbb{Q}(i)$. There are precisely $2 = \dim_{\mathbb{Q}} \mathbb{Q}(i)$ extensions of $\mathbb{Q} \to \mathbb{C}$ to $\mathbb{Q}(i) \to \mathbb{C}$, namely $i \mapsto i$ and $i \mapsto -i$.

Recall: $f \in K[X] \rightsquigarrow \mathrm{Gal}_K(f) = \mathrm{Gal}_K(\text{splitting field of } f)$.

Every $\sigma \in \mathrm{Gal}_K(f)$ permutes the roots of f.

skipped this part

Def:

Roots α, β of f are called conjugate if $\sigma(\alpha) = \beta$ for some $\sigma \in \mathrm{Gal}_K(f)$.

Ex:

The splitting field of $f = X^2 + 1 \in \mathbb{Q}[X]$ is $\mathbb{Q}(i)$. The two roots of f are i and $-i$. The map sending i to $-i$ is an automorphism $\Rightarrow$ i and $-i$ are conjugate.

Lemma:

If f is irreducible, all roots are conjugate.

Proof:

Let L be a splitting field of f.

Have $L = K(\alpha_1, .., \alpha_r)$ with α_i the roots of f.

Let α, β be two such roots.

Both $K(\alpha)$ and $K(\beta)$ are stem fields of f

$\Rightarrow \exists$ isomorphism $\tau : K(\alpha) \longrightarrow K(\beta) \hookrightarrow L$ mapping α to β

Can inductively extend this to a morphism $\sigma : L \to L$. This is an isomorphism.

$\square$

§2.5 Primitive elements

Theorem 2.23 (Primitive element theorem)

If $K \subseteq L$ finite and separable, then $L = K(\alpha)$ for some α.

Proof (sketch)

$K \subseteq L$ finite $\Rightarrow L = K(\alpha_1, \dots, \alpha_n)$. Can assume wlog that $n=2$ and show that $K(\beta, \gamma) = K(\alpha)$ for some α.

Let L be the splitting field of $\mu_\beta \cdot \mu_\gamma$. Let $\beta = \beta_1, \dots, \beta_r$ be the roots of μ_β in L and $\gamma = \gamma_1, \dots, \gamma_s$ be the roots of μ_γ in L.

Since μ_γ is separable, $\gamma_j \neq \gamma$ $\forall j > 1$. Hence, for $j > 1$ the equation

$$\beta_i + X\gamma_j = \beta + X\gamma \iff X(\gamma - \gamma_j) = \beta_i - \beta$$

has exactly one solution, namely $X = \dfrac{\beta_i - \beta}{\gamma - \gamma_j}$

If K is infinite, there is $c \in K$ different from all these solutions. Let

$$\alpha := \beta + c\gamma.$$

Can now show that $K(\beta, \gamma) = K(\alpha)$.

(More details in e.g. Gathmann, Algebra. Also works for K finite.) $\square$

Remark: 2.24

The proof is constructive!

Def: 2.25

A <u>number field</u> L is a finite extension of $\mathbb{Q}$.

These are the extension fields we will mostly be concerned with.

By the theorem

$$L = \mathbb{Q}(\alpha) \simeq \mathbb{Q}[X]/(\mu_\alpha),$$ a stem field, constructive!

§ 2.6 Characteristic polynomial, norm, trace.

Recall that for an $n \times n$ matrix $A = (a_{ij})$ over a commutative ring R:

$$\mathrm{Tr}(A) := \sum_i a_{ii} \qquad \underline{\text{trace}}$$

$$\det(A) := \sum_{\sigma \in S_n} \mathrm{sgn}(\sigma) a_{1\sigma(1)} \cdots a_{n\sigma(n)} \qquad \underline{\text{determinant}}$$

$$\chi_A(X) := \det(\underbrace{XI_n - A}_{\substack{\text{matrix over} \\ \text{polynomial ring } R[X]}}) \qquad \underline{\text{characteristic polynomial of } A}$$

<u>Lemma</u> 2.26

$\chi_A(X) = X^n - \mathrm{Tr}(A) X^{n-1} + \dots + (-1)^n \det(A)$, in particular χ_A monic, $\deg \chi_A = n$.

<u>Proof:</u> Left as exercise. $\square$

<u>Theorem 2.27 (Cayley–Hamilton):</u> $\chi_A(A) = 0$.

<u>Proof</u> (sketch): For any i,j let m_{ij} be the (i,j) minor of A i.e. the determinant of the $(n-1)\times(n-1)$ matrix obtained from A by deleting the i-th row and j-th column of A.

Let $\mathrm{adj}(A) := ((-1)^{i+j} M_{ji})$, the <u>adjugate</u> of A. Can show that

$A \cdot \mathrm{adj}(A) = \det(A) I$.

Hence

$$(XI_n - A) \cdot \mathrm{adj}(XI_n - A) = \det(XI_n A) I_n = \chi_A(X) I_n$$

Plugging in A yields $0 = \chi_A(A) I_n \Rightarrow \chi_A(A) = 0$. $\square$

Tr, det, χ_A unchanged when replacing A by UAU^{-1}

So, if α endomorphism of a finite-dim vector space, can define

$$\mathrm{Tr}(\alpha) := \mathrm{Tr}(A), \quad \det(\alpha) = \det(A), \quad \chi_\alpha = \chi_A$$

for a matrix A of α wrt any basis.

Now, $K \subseteq L$ finite field extension. Every $\alpha \in L$ defines an endomorphism

$$\alpha_L : L \to L$$
$$x \mapsto \alpha x.$$

<u>Def:</u> 2.28

$$\left.\begin{aligned} \mathrm{Tr}_{L|K}(\alpha) &:= \mathrm{Tr}(\alpha_L) \\ N_{L|K}(\alpha) &:= \det(\alpha_L) \\ \chi_{L|K,\alpha} &:= \chi_{\alpha_L} \end{aligned}\right\} \text{all constructive (linear algebra)}$$

<u>Lemma:</u> 2.29

$\mathrm{Tr}_{L|K}$ is additive, $N_{L|K}$ is multiplicative. $\square$

<u>Ex:</u> 2.30

Consider $\mathbb{Q} \subseteq \mathbb{Q}(i)$. Basis is $\{1, i\}$. Let $\alpha = a + bi$.

Multiplication

$$\begin{aligned} \alpha \cdot 1 &= a + bi \\ \alpha \cdot i &= -b + ai \end{aligned} \quad \rightsquigarrow \text{matrix of } \alpha = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$$

Hence

$$\mathrm{Tr}_{\mathbb{Q}(i)|\mathbb{Q}}(\alpha) = 2a = 2\,\mathrm{Re}(\alpha), \quad N_{\mathbb{Q}(i)|\mathbb{Q}}(\alpha) = a^2 + b^2 = |\alpha|^2.$$

Prop 2.31

$$\chi_{\alpha, L/K} = p_{\alpha,K}^m, \quad m = \dim_{K(\alpha)} L$$

Proof: First, suppose $L = K(\alpha)$. Have.

$$\deg p_\alpha = \dim_K K(\alpha) = \dim_K L = \deg \chi_\alpha$$

Since $\chi_\alpha(\alpha) = 0$ by Cayley-Hamilton $\Rightarrow p_\alpha = \chi_\alpha$.

Now, general case: Let $\beta_1, \dots, \beta_n$ be a K-basis of $K(\alpha)$, and let $\gamma_1, \dots, \gamma_m$ be a $K(\alpha)$-basis of L. Then $\{\beta_i \gamma_k\}_{i,k}$ is a K-basis of L. Can write

$$\alpha \beta_i = \sum_j a_{ji} \beta_j, \quad a_{ji} \in K$$

This gives multiplication by α on $K(\alpha)$. Hence, setting $A := (a_{ij})$ we have $\chi_A = p_\alpha$ by first case above.

Have $\alpha(\beta_i \gamma_k) = (\alpha \beta_i)\gamma_k = \sum_j (a_{ji}\beta_j)\gamma_k = \sum_j a_{ji}(\beta_j \gamma_k)$

$\rightsquigarrow$ matrix of mult by α on L = $\begin{pmatrix} A & & \\ & A & \\ & & \ddots & \\ & & & A \end{pmatrix}$, $m = \dim_{K(\alpha)} L$ blocks

$$\rightsquigarrow \chi_\alpha = \chi_A^m = p_\alpha^m.$$

$\square$

Cor 2.32: Let $\alpha_1, \dots, \alpha_n$ be the roots of p_α in a splitting field. Then

$$\mathrm{Tr}_{L/K}(\alpha) = m \sum_{i=1}^{n} \alpha_i \quad , \quad N_{L/K}(\alpha) = \left(\prod_{i=1}^{n} \alpha_i \right)^m$$

where $m = \dim_{K(\alpha)} L$.

Proof: Let

$$p_\alpha = X^n + a_1 X + \dots + a_n = \prod (X - \alpha_i)$$

Then $\quad a_1 = -\sum_i \alpha_i \quad$ and $\quad a_n = (-1)^n \prod \alpha_i$.

By Prop 2.31 have

$$\chi_\alpha = p_\alpha^m = X^{mn} + m a_1 X^{mn-1} + \dots + a_n^m$$

Hence by Lemma 2.26 have

$$\mathrm{Tr}_{L/K}(\alpha) = -m a_1 = m \sum_i \alpha_i$$

$$N_{L/K}(\alpha) = (-1)^{mn} a_n^m = \left(\prod_i \alpha_i \right)^m.$$

$\square$

Cor 2.33:

If $K \subseteq L$ is separable and $\Omega \supseteq K$ is algebraically closed, then

$$\mathrm{Tr}_{L/K}(\alpha) = \sum_\sigma \sigma(\alpha) \, , \quad N_{L/K}(\alpha) = \prod_\sigma \sigma(\alpha)$$

where σ runs through the K-morphisms $L \to \Omega$.

Proof: First suppose $L = K(\alpha)$. This is a stem field of p_α, so for every root β of p_α in Ω get a morphism $L \to \Omega$, and these are precisely the morphisms, so (9)

$$p_\alpha = \prod_\sigma (X - \sigma\alpha).$$

Now general case. By Lemma 2.21 each $\tau : K(\alpha) \to L$ extends in precisely $\dim_{K(\alpha)} L = m$ ways to $\sigma : L \to \Omega$, mapping α to the roots of p_α. So, in $\{\sigma\alpha\}_\sigma$ each root of p_α occurs precisely m times.

$\square$

Ex 2.34:

Consider $\mathbb{Q} \subseteq \mathbb{Q}(i)$. The two morphisms $\mathbb{Q}(i) \to \mathbb{C}$ are

$$\sigma_1 : a + bi \longmapsto a + ib$$
$$\sigma_2 : a + bi \longmapsto a - ib$$

Hence,

$$\operatorname{Tr}(\underset{a+ib}{\underset{\shortparallel}{\alpha}}) = a + ib + a - ib = 2a = 2\operatorname{Re}(\alpha)$$

$$N(\alpha) = (a+ib)(a-ib) = a^2 + b^2 = |\alpha|^2.$$

2.7 Trace form and discriminant

Let V be a finite-dim K-vector space and let $\psi : V \times V \to K$ be a symmetric bilinear form.

Consider the map

$$V \longrightarrow V^* := \operatorname{Hom}_K(V, K)$$
$$v \longmapsto (w \mapsto \psi(v, w))$$

Def 2.35 ψ is called non-degenerate if this is an isomorphism.

This can be decided as follows.

<u>Def 2.36</u> The <u>Gram matrix</u> of ψ wrt a basis $v_1,\dots,v_n$ of V is

$$Gr_\psi(v_1,\dots,v_n) := (\psi(v_i,v_j))_{ij}$$

If $w_1,\dots,w_n$ is another basis and $w_j = \sum_i a_{ij} v_i$, then

$$\psi(w_k,w_l) = \sum_{i,j} a_{ki}\,\psi(v_i,v_j)\,a_{lj},$$

So

$$Gr_\psi(w_1,\dots,w_n) = A \cdot Gr_\psi(v_1,\dots,v_n)\,A^t.$$

<u>Def</u> 2.37
The <u>discriminant</u> of ψ wrt $v_1,\dots,v_n$ is

$$d_\psi(v_1,\dots,v_n) := \det Gr_\psi(v_1,\dots,v_n)$$

We have

$$d_\psi(w_1,\dots,w_n) = \det(A)^2\, d_\psi(v_1,\dots,v_n)$$

<u>Lemma</u> 2.38
TFAE:
a) ψ is non-degenerate.
b) $d_\psi \neq 0$ wrt one (hence any) basis

<u>Proof</u>: Left as exercise. $\square$

Now, let $K \subseteq L$ be a finite extension.

<u>Def</u> 2.39
The <u>trace form</u> of L over K is the symmetric bilinear form $L \times L \to K$ defined by

$$(\alpha,\beta)_{L/K} := Tr_{L/K}(\alpha\cdot\beta)$$

The <u>discriminant</u> of $K \subseteq L$ wrt a basis $\alpha_1, \dots, \alpha_n$ of L is

$$d_{L|K}(\alpha_1, \dots, \alpha_n) := d_{Tr_{L|K}}(\alpha_1, \dots, \alpha_n) = \det\left((\alpha_i, \alpha_j)_{L|K} \right)$$

<u>Ex</u> 2.40

Consider $\mathbb{Q} \subset \mathbb{Q}(i)$ with basis $\{1, i\}$. Then

$$G_{L|K} = \begin{pmatrix} Tr(1 \cdot 1) & Tr(1 \cdot i) \\ Tr(i \cdot 1) & Tr(i \cdot i) \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & -2 \end{pmatrix}$$

$\rightsquigarrow d_{L|K} = -4.$

<u>Lemma</u> 2.41

If $K \subseteq L$ is separable, then
$$d_{L|K}(\alpha_1, \dots, \alpha_n) = \det\left((\sigma_i \alpha_j) \right)^2,$$
where the σ_i are the K-morphisms $L \to \Omega$, $\Omega \supseteq K$ algebraically closed.

<u>Proof</u>: By Cor 2.33 we have
$$Tr_{L|K}(\alpha_i \alpha_j) = \sum_k \sigma_k(\alpha_i \alpha_j) = \sum_k \sigma_k(\alpha_i) \sigma_k(\alpha_j)$$

$\Rightarrow$ The matrix $\left(Tr_{L|K}(\alpha_i \alpha_j) \right)$ is the product of $\left(\sigma_k(\alpha_i) \right)^t$ and $\left(\sigma_k(\alpha_i) \right)$,

so
$$d_{L|K}(\alpha_1, \dots, \alpha_n) = \det\left(Tr(\alpha_i \alpha_j) \right) = \det\left((\sigma_k \alpha_i) \right) \cdot \det\left((\sigma_k \alpha_i) \right)$$
$$= \det\left((\sigma_k \alpha_i) \right)^2.$$
$\square$