Lecture 3, 4.11.

Last time:

\( f \in \mathbb{U}[X] \) irreducible \implies extension field \( L = \mathbb{U}[X]/(f) \) o\( f \) \( \text{field} \)

\( \mathbb{U}[X] \) \( \Rightarrow \) splitting field

Both, constructive (if \( \mathbb{U} \) is)

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

Proved: if \( f \) isred and char \( \mathbb{U} = 0 \) \( \Rightarrow f \) separable.

Def 2.19:

\( \mathbb{U} \subseteq \mathbb{L} \) is called:

- **finite** if \( \text{dim}_{\mathbb{U}} \mathbb{L} < \infty \).
- **algebraic** if each \( \alpha \in \mathbb{L} \) algebraic over \( \mathbb{U} \).
- **separable** if algebraic and \( \alpha \) separable over \( \mathbb{U} \).

Lemma 2.20:

\( \mathbb{U} \subseteq \mathbb{L} \) finite \( \Rightarrow \) algebraic.

Proof:

Let \( \alpha \in \mathbb{L} \). The powers \( 1, \alpha, \alpha^2, \ldots \) must eventually become linear dependent \( \Rightarrow \alpha \) algebraic. \( \Box \)
Lemma: Let $K \subseteq L$ and let $L \subseteq M$ be a finite separable extension, $n = \dim_K M$. Let $Q = M$ be algebraically closed. Then any $K$-morphism $\tau : L \to Q$ extends in precisely $n$ ways to a $K$-morphism $\sigma : M \to Q$:

$M \xrightarrow{\sigma} Q$

$\downarrow \tau$

$L

Proof: By induction on $n$. Case $n = 1$ clear. Let $n > 1$. Choose $x \in M$, $x \notin L$. Let $f : L \to Q$, $r := \deg f$. Consider $L \subseteq L(x) \subseteq M$.

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

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

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

So $\sigma$ maps roots of $f$ to roots of $\tau(f)$. For any root $\beta$ of $\tau(f)$ in $Q$ get an extension

$L(x) \longrightarrow L$

$b_0 + b_1 x + \cdots + b_r x^r \longmapsto T(b_0) + T(b_1)\beta + \cdots + T(b_r)\beta^r$

Since $f$ separable, also $\tau(f)$ separable $\Rightarrow$ $\deg f = \dim_L L(x)$ choices for $\beta$ $\Rightarrow$ $\dim_L L(x)$ extensions of $\tau$ to $L(x)$.

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

\[\square\]

Ex: Consider $Q \subseteq Q(i)$. There are precisely $2 \cdot \dim_Q Q(i)$ extensions of $Q \to C$ to $Q(i) \to C$, namely $i \mapsto i$ and $i \mapsto -i$. 


Recall: \( f \in K[X] \Rightarrow \text{Gal}(f) = \text{Gal}(L \mid K) \) (splitting field of \( f \)).
Every \( \sigma \in \text{Gal}(f) \) permutes the roots of \( f \).

**Def:**
Roots \( \alpha, \beta \) of \( f \) are called **conjugate** if \( \sigma(\alpha) = \beta \) for some \( \sigma \in \text{Gal}(f) \).

**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 \( \sigma \) so \( i \) and \( -i \) are conjugate.

**Lemma:**
If \( f \) is irreducible, all roots are conjugate.

**Proof:**
Let \( L \) be a splitting field of \( f \).
Have \( L = K(\alpha_1, \ldots, \alpha_r) \) with \( \alpha_i \) the roots of \( f \).
Let \( \alpha, \beta \) be two such roots.
Both \( K(\alpha) \) and \( K(\beta) \) are subfields of \( L \).

\[ L \ni \exists \text{ isomorphism } \tau : K(\alpha) \to K(\beta) \leadsto L \text{ mapping } \alpha \to \beta \]

Can inductively extend this to a morphism \( \tau : L \to L \). This is an isomorphism.

\[ \square \]

§2.5 **Primitive element**

**Theorem 2.23** (Primitive element theorem)
If \( K \subseteq L \) finite and separable, then \( L = K(\alpha) \) for some \( \alpha \).
Proof (Sketch)
$L = \mathbb{K}(x_1, \ldots, x_n)$. Can assume wlog that $n = 2$ and show that $\mathbb{K}(\beta, y) = \mathbb{K}(\alpha)$ for some $\alpha$.

Let $L$ be the splitting field of $p_\alpha$. Let $\beta = \beta_1, \ldots, \beta_r$ be the roots of $p_\alpha$ in $L$ and $y = y_1, \ldots, y_s$ be the roots of $p_y$ in $L$.

Since $p_y$ is separable, $y_i \neq y_j$ for $i > j$. Hence, for $j > 1$ the equation

$$\beta_i + Xy_j = \beta + Xy_j \iff X(y_j - y_i) = \beta_i - \beta$$

has exactly one solution, namely $X = \frac{\beta_i - \beta}{y_j - y_i}$.

If $\mathbb{K}$ is infinite, there is cell different from all these solutions. Let

$$\alpha = \beta + cy.$$ 

Can now show that $\mathbb{K}(\beta, y) = \mathbb{K}(\alpha)$.

More details in e.g. Gathmann, Algebra. Also works for $\mathbb{K}$ finite.)

Remark 2.24
The proof is constructive!

Def 2.25
A number field $L$ is a finite extension of $\mathbb{Q}$.

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

By the theorem

$$L = \mathbb{Q}(\alpha) = \mathbb{Q}[x]/(p_\alpha),$$

a claim field, constructive!
§ 2.6 Characteristic polynomial, norm, trace.

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

\[ \text{Tr}(A) := \sum_i a_{ii} \quad \text{trace} \]

\[ \det(A) := \sum_{\sigma \in S_n} \text{sgn}(\sigma) a_{(\sigma(1)(1))} \cdots a_{(\sigma(n)(n))} \quad \text{determinant} \]

\[ X_A(X) := \det(XI_n - A) \quad \text{characteristic polynomial of } A \]

Lemma 2.26

\[ X_A(X) = X^n - \text{Tr}(A)X^{n-1} + \ldots + (-1)^n \det(A), \quad \text{in particular } X_A \text{ monic, } \deg X_A = n. \]

Proof: Left as exercise.

Theorem (Cayley–Hamilton): $X_A(A) = 0$.

Proof (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 $\text{adj}(A) := (-1)^{i+j}M_{ji}$, the adjugate of $A$. Can show that

\[ A \cdot \text{adj}(A) = \det(A)I. \]

Hence

\[ (XI_n - A) \cdot \text{adj}(XI_n - A) = \det(XI_n - A)I_n = X_A(X)I_n \]

Plugging in $A$ yields $0 = X_A(A)I_n \Rightarrow X_A(A) = 0$. \qed
Tr, det, $\chi_A$ unchanged when replacing $A$ by $UAU^{-1}$

So, if $\alpha$ endomorphism of a finite-dim vector space, can define

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

for a matrix $A$ of $\alpha$ w.r.t any basis.

Now $K \subseteq L$ finite field extension. Ever $\alpha \in L$ defines an endomorphism $\alpha_L : L \to L$

$$x \mapsto \alpha x.$$  

**Def. 2.28**

$$\begin{align*}
\text{Tr}_{LK}(\alpha) &:= \text{Tr}(\alpha_L) \\
\text{det}_{LK}(\alpha) &:= \det(\alpha_L) \\
\chi_{LK,\alpha} &:= \chi_{\alpha_L}
\end{align*}$$

The above all constructive (linear algebra).

**Lemma 2.29**

$\text{Tr}_{LK}$ is additive, $\text{det}_{LK}$ is multiplicative.

**Ex. 2.30**

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

$\alpha \cdot 1 = a + bi \rightarrow$ matrix of $\alpha = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$

$\alpha \cdot i = -b + ai \rightarrow$ matrix of $\alpha = \begin{pmatrix} b & a \\ -a & b \end{pmatrix}$

Hence

$$\text{Tr}_{\mathbb{Q}(i)}(\alpha) = 2a = 2\Re(\alpha), \quad \text{det}_{\mathbb{Q}(i)}(\alpha) = a^2 + b^2 = |\alpha|^2.$$
Prop 2.31

\[ x, y = p^m, \quad m = \dim_{K(x)} L \]

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

\[ \deg p = \dim_K K(x) = \dim_K L = \deg x \]

Since \( x(\alpha) = 0 \) by Cayley–Hamilton \( \Rightarrow p = x \).

Now, general case: Let \( \beta_1, \ldots, \beta_n \) be a \( K \)-basis of \( K(x) \) and let \( \gamma_1, \ldots, \gamma_m \) be a \( K(x) \)-basis of \( L \). Then \( \{ \beta_1, \ldots, \beta_n, \gamma_1, \ldots, \gamma_m \} \) is a \( K \)-basis of \( L \). Can write

\[ x = \sum_{i,j} a_{ij} \beta_i \gamma_j, \quad a_{ij} \in K \]

This gives multiplication by \( x \) on \( K(x) \). Hence, setting \( A = (a_{ij}) \) we have \( x_A = p \) by first case above.

Have \( x(\beta_1 \gamma_1) = (x \beta_1) \gamma_1 = \sum_{i,d} (a_{ij} \beta_i) \gamma_1 = \sum_{i,j} a_{ij} (\beta_i \gamma_1) \)

\( \Rightarrow \) matrix of mult by \( x \) on \( L = \begin{pmatrix} A \cdots A \\ \cdots \cdots \cdots \\ A \end{pmatrix} \), \( m = \dim_{K(x)} L \)

\( \Rightarrow x_A = x^m = p^m \).
Corollary 2.32: Let \( \alpha_1, \ldots, \alpha_n \) be the roots of \( \alpha_k \) in a splitting field. Then
\[
\text{Tr}_{L/K}(\alpha) = m \sum_{i=1}^{n} \alpha_i, \quad N_{L/K}(\alpha) = \left( \prod_{i=1}^{n} \alpha_i \right)^m
\]
where \( m = \dim_{K(\alpha)} L \).

Proof: Let
\[
\psi_L = x^n + a_1 x^{n-1} + \ldots + a_n = \prod_{i=1}^{n} (x - \alpha_i)
\]
Then \( \alpha = -\sum \alpha_i \) and \( \alpha = (-1)^n \prod \alpha_i \).

By Prop 2.31 have
\[
\chi_L = \psi_L^m = x^{mn} + ma_1 x^{mn-1} + \ldots + a_n^m
\]
Hence by Lemma 2.26 have
\[
\text{Tr}_{L/K}(\alpha) = -ma = m \sum \alpha_i,
\]
\[
N_{L/K}(\alpha) = (-1)^m a_m = \left( \prod \alpha_i \right)^m.
\]
\[\square\]

Corollary 2.33: If \( K \leq L \) is separable and \( \Omega \supseteq \Omega \) is algebraically closed, then
\[
\text{Tr}_{L/K}(\alpha) = \sum_{\sigma(\alpha)} \sigma(\alpha), \quad N_{L/K}(\alpha) = \prod_{\sigma} \sigma(\alpha)
\]
where \( \sigma \) runs through the \( K \)-morphisms \( L \to \Omega \).
Proof: First suppose \( L = \mathbb{U}(\omega) \). This is a skin field of \( \mathcal{L} \), so for every root \( \beta \) of \( \mathcal{L} \) in \( \Omega \) get a morphism \( \mathcal{L} \to \Omega \), and thus are precisely the morphisms, so \( \nu = \Pi (x - \sigma \omega) \).

Now general case. By Lemma 2.21 each \( \tau : \mathbb{U}(\omega) \to \mathcal{L} \) extends in precisely \( \dim \mathbb{U}(\omega) \) ways to \( \sigma : \mathcal{L} \to \Omega \), mapping \( \omega \) to the root of \( \mathcal{L} \).

So, in \( \{ \sigma \omega \} \) each root of \( \mathcal{L} \) occurs precisely \( m \) times. \( \square \)

**EX:**

Considers \( \Omega \subseteq \mathbb{C}^2 \). The two morphisms \( 
 \begin{align*}
\sigma_1 &: a + bi \mapsto a + i \beta \\
\sigma_2 &: a + bu \mapsto a - i \beta
\end{align*}
\)

Hence,

\[ 
\text{Tr} (\omega) = a + i \beta + a - i \beta = 2a = 2 \text{Re}(\omega)
\]

\[ 
\text{N}(\omega) = (a + i \beta)(a - i \beta) = a^2 + b^2 = |x|^2.
\]

2.7 Trace form and discriminant

Let \( V \) be a finite-dimensional \( K \)-vector space and let \( \eta : V \times V \to K \) be a symmetric bilinear form.

Consider the map

\[ 
V \to V^* := \text{Hom}_K(V, K)
\]

\[ 
\nu \to (\omega \mapsto \eta(\omega, \nu))
\]

**Def.** \( \eta \) is called non-degenerate if this is an isomorphism.

This can be decided as follows.
Def 2.36 The Gram matrix of $\psi$ w.r.t. a basis $\nu_1, \ldots, \nu_n$ of $V$ is

$$G_{\psi}(\nu_i, \nu_j) := (\psi(\nu_i, \nu_j))_{ij}$$

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

$$\psi(w_i, w_j) = \sum_i a_{ik} \psi(\nu_i, \nu_k) a_{kj}$$

So

$$G_{\psi}(w_i, w_j) = A^T G_{\psi}(\nu_i, \nu_j) A.$$

Def 2.37 The discriminant of $\psi$ w.r.t $\nu_1, \ldots, \nu_n$ is

$$d_{\psi}(\nu_1, \ldots, \nu_n) := \det G_{\psi}(\nu_1, \nu_n)$$

We have

$$d_{\psi}(w_1, \ldots, w_n) = \det(A)^2 d_{\psi}(\nu_1, \nu_n).$$

Lemma 2.38 TFAE:

a) $\psi$ is non-degenerate.
b) $d_{\psi} \neq 0$ w.r.t. one (hence any) basis.

Proof: Left as exercise. \(\square\)

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

Def 2.39 The trace form of $L$ over $K$ is the symmetric bilinear form $L \times L \rightarrow K$ defined by

$$(\alpha, \beta)_L := \text{tr}_{L/K} (\alpha \beta).$$
The discriminant of $V \leq \mathbb{L}$ with a basis $x_1, \ldots, x_n$ of $L$ is

$$d_{\mathbb{K}L}(x_1, \ldots, x_n) = \det \left( (x_i, x_j)_{L/K} \right)$$

**Ex 2.40**

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

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

$\Rightarrow d_{\mathbb{O}L} = -4$.

**Lemma 2.41**

If $V \leq \mathbb{L}$ is separable, then

$$d_{\mathbb{K}L}(x_1, \ldots, x_n) = \det ( (\sigma_i x_j) )^2,$$

where the $\sigma_i$ are the $K$-morphisms $L \to \mathbb{R}$, $\mathbb{R} \cong K$ algebraically closed.

**Proof:** By Cor 2.33 we have

$$\text{Tr}_{\mathbb{K}L} (x_i x_j) = \sum_k \sigma_k(x_i x_j) = \sum_k \sigma_k(x_i) \sigma_k(x_j)$$

$\Rightarrow$ The matrix $(\text{Tr}_{\mathbb{K}L}(x_i x_j))$ is the product of $(\sigma_k(x_i))^2$ and $(\sigma_k(x_j))^2$.

So

$$d_{\mathbb{K}L}(x_1, \ldots, x_n) = \det (\text{Tr}(x_i x_j)) = \det ( (\sigma_k(x_i))^2 \cdot (\sigma_k(x_j))^2)$$

$$= \det ( (\sigma_k x_i))^2.$$  \qed