Earlier notation: \( A \): integrally closed integral domain, \( K \): field of fractions

\( B \): integral closure of \( A \) in \( L/K \): finite extension,

\[
N_{L/K}(x) := \det(T_x) = \prod \delta(x)
\]
(for \( x \in L \))

\[
\text{Tr}_{L/K}(x) := \text{trace}(T_x) = \sum \delta(x)
\]

if \( L/K \) separable

\[
\frac{1}{n} \sum_{\sigma \in \text{Gal}(L/K)} \delta(x)
\]

\( 6 \) ranges over \( K \)-embeddings of \( L \) in \( \bar{K} \).

(alg. closure)

( always true if \( K \)

cover 0, \( K \) finite)

if \( x \in B \), then \( N_{L/K}(x) \in K \) (from linear alg.) \( \Rightarrow \) \( x \in K \cap B = A \)

( from Galois defn)

if \( n \) extensions of separable, use Galois theoretic definition. If not,

similarly for trace, and

all coeffs of charpoly

\( \text{Norms/Traces behave well in towers of extensions:} \)

\[ K = L \subseteq M \]

\[
\text{Tr}_{M/K} = \text{Tr}_{L/K} \circ \text{Tr}_{M/L}
\]

\[
N_{M/K} = N_{L/K} \cdot N_{M/L}
\]

(If extensions are separable, use Galois theoretic definition. If not,

use fact that trace equal up to fixed constant to trace of max. sep.

extension)

discriminant of a basis \( x_1, \ldots, x_n \) for \( L/K \), \( d(x_1, \ldots, x_n) \), given by

\[
\det\left( b_{ij} \right) = \det\left( \text{Tr}_{L/K}(x_i x_j) \right)
\]

\( i \mapsto -i \)

Example:

\( Q(i) = \langle 1, i \rangle \) as \( \mathbb{R} \) v.s. over \( Q \).

\( 6 \in \langle 1, i \rangle \)

\( \langle 6 \rangle = \langle 1, i \rangle \)

Matrix:

\[
\begin{pmatrix}
1 & i \\
1 & -i
\end{pmatrix}
\]

so disk \( (1, i) = -4 \).

Last time, we argued this was a good basis since integral for \( \mathbb{Z}[i] = \mathbb{Q}_K/\mathbb{Z} \)

Show such bases always exist for \( B \supseteq A \) with \( A: \text{P.1.D.} \)

int. closure
Want to use discriminant to show this. First check:

if \( L/k \) separable, \( \alpha_i, \ldots, \alpha_n \) basis for \( L/k \), then

\[
d(\alpha_1, \ldots, \alpha_n) \neq 0.
\]

**pf:** Follows from fact that \( \langle x, y \rangle := \text{Tr}_{L/k}(x y) \) is non-deg. bilinear form

so choosing basis \( \alpha_i, \ldots, \alpha_n \), the matrix associated is

\[
x^T M y \quad \text{with} \quad M = (\text{Tr}_{L/k}(\alpha_i \alpha_j))
\]

so

\[
d(\alpha_1, \ldots, \alpha_n) = \det(M) \neq 0
\]

earlier claim that
disc. is \( \det(\text{Tr}_{L/k}(\alpha_i \alpha_j)) \)

To show \( \langle x, y \rangle \) non-deg., we can pick any convenient basis.

e.g. \( 1, \theta, \theta^2, \ldots, \theta^{n-1} \) if \( L = K(\theta) \). Then associated matrix

\[
M = \text{Tr}_{L/k}(\theta^{-1} \theta^{-1}) \quad \text{and} \quad \det(M) = d(1, \theta, \ldots, \theta^{n-1}) \quad \text{separable}
\]

\[
= \prod_{i < j} (\theta_i - \theta_j)^2 \neq 0.
\]

where \( \theta_i(\theta) = \theta_i \)

Now to prove \( B \) is a free \( A \)-module of rank \( w = [L:k] \),

( so has "integral basis" \( \omega_1, \ldots, \omega_n \) s.t. for any \( b = a_1 \omega_1 + \cdots + a_n \omega_n \), \( \alpha_i \in A \)

need two facts:

Fact 1: Let \( \alpha_i, \ldots, \alpha_n \) be basis for \( L/k \) with \( \alpha_i \in B \), then

\[
d(\alpha_1, \ldots, \alpha_n) \cdot B \subseteq A \alpha_1 + A \alpha_2 + \cdots + A \alpha_n
\]

i.e. is an \( A \)-submodule of a free \( A \)-module.
Note that a basis with $d \in B$ exists because, if 

$x_1, \ldots, x_n$ are basis, then $x_i$ satisfy polynomial 

for $\mathbb{K}$, then $x_i$ satisfy polynomial 

$$a_n x^n + \cdots + a_0 = 0$$

$\Rightarrow$ $a_{n-1} x_i$ satisfies monic poly, so is in $B$ (integral closure of A)

and doing this adjustment for all $x_i$ gives new basis with $x_i \in B$.

Note also that Fact 1 implies $B$ has rank $n$, since containment $\Rightarrow$ rank $(dB) = \operatorname{rank} B \leq n$, and gens. for $B$ as $A$-module are gens for $L$ as $K$-module.

To finish we use:

Fact 2: Over a P.I.D. $A$, every submodule $M'$ of a free $A$-module $M$ of rank $n$ is free of rank $\in [0,n]$.

(Neukirch "Main thm. on modules over P.I.D." ) $\Leftrightarrow$ cf. Jacobson p.179 "Basic Algebra I"

So $d(a_1, \ldots, a_n)B$ is free $A$-module, hence $B$ is a free $A$-module.

More generally one can show that any fin-gen.

$B$-submodule $M^g \neq 0$ of $L$ is free of rank $[L:K]$.

(see Neukirch )

easy corollary: structure thm. analogous to structure thm. for abelian gps.

Analogly nicely described in Artin's Algebra.
proof of Fact 1: Given \( b \in B \), write

\[
b = k_1 \alpha_1 + \ldots + k_n \alpha_n \quad k_i \in K.
\]

Then \( k_i \) give solution to the system of equations in \( x_i \):

\[
\text{Tr}_{H_k}(\alpha_i b) = \sum_j \text{Tr}_{H_k}(\alpha_i \alpha_j) x_j
\]

\( e \in B \cap K = A \) so solve system by inverting matrix

with entries \( \text{Tr}_{H_k}(\alpha_i \alpha_j) \)

so the resulting entries are \( x_i \)s of

\( A \) divided by \( \det (\text{Tr}_{H_k}(\alpha_i \alpha_j)) \)

\( \text{disc} (\alpha_1, \ldots, \alpha_n) \)

i.e. \( k_i \in A^* \) so

\[ db = A \alpha_1 + \ldots + A \alpha_n \text{ as desired} \]

Finally if \( A = \mathbb{Z} \), \( B = \mathbb{Z} \) in \( L \), then given two bases \( \alpha_1, \ldots, \alpha_n \), \( \alpha_1', \ldots, \alpha_n' \)

they differ by change of basis matrix \( (a_{ij}) \) \( a_{ij} \in \mathbb{Z} \)

which is invertible, so must have \( \det = \pm 1 \).

\[
\Rightarrow d(\alpha_1, \ldots, \alpha_n) = d(\alpha_1', \ldots, \alpha_n') \quad \text{(since \( \det \) involved square of det.)}
\]

so can define \( \text{disc.} (\theta_k) = d(\theta_k) := d(\alpha_1, \ldots, \alpha_n) \)

for any integral basis of \( B/A \).