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

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

then (for $x \in L$)

$N_{L/K}(x) := \det(T_x) = \prod_{\sigma} \sigma(x)$

$Tr_{L/K}(x) := \text{trace}(T_x) = \sum_{\sigma} \sigma(x)$

σ ranges over K-embeddings of L in $\overline{K}$. (alg. closure)

if L/K separable (always true if K char 0, K finite)

if $x \in B$, then $N_{L/K}(x) \in K$ (from linear alg.) so $\in K \cap B = A$
$\in B$ (from Galois def'n)

similarly for trace, and all coeffs of char. poly of T_x.

Norms / traces behave well in towers of extensions: $K \subseteq L \subseteq M$

$Tr_{M/K} = Tr_{L/K} \circ Tr_{M/L}$ $\qquad N_{M/K} = N_{L/K} \cdot N_{M/L}$.

(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 $\alpha_1, \dots, \alpha_n$ for L/K, $d(\alpha_1, \dots, \alpha_n)$, given by

$$\det((\sigma_i \alpha_j))^2 = \det(Tr_{L/K}(\alpha_i \alpha_j))$$

Example: $\mathbb{Q}(i) = \langle \underset{\alpha_1}{1}, \underset{\alpha_2}{i} \rangle$ as v.s. over $\mathbb{Q}$. $\quad \sigma \in \langle \underset{\sigma_1}{1}, \underset{\sigma_2}{\tau} \rangle$, $\tau: i \mapsto -i$

Matrix: $\begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix}$ with $\det = -2i$
so disc $(1, i) = -4$.

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

Show such bases always exist for $B \supseteq A$ (int. closure) with A: P.I.D.

Want to use discriminant to show this. First check:

if L/K separable, $\alpha_1, \dots, \alpha_n$ basis for L/K, then

$$d(\alpha_1, \dots, \alpha_n) \neq 0.$$

<u>pf</u>: Follows from fact that $\langle x, y \rangle := \mathrm{Tr}_{L/K}(xy)$ is non-deg. bilinear form

so choosing basis $\alpha_1, \dots, \alpha_n$, the matrix associated is

$$x^T M y \quad \text{with} \quad M = \left(\mathrm{Tr}_{L/K}(\alpha_i \alpha_j) \right), \quad \text{so}$$

$$d(\alpha_1, \dots, \alpha_n) \underset{\uparrow}{=} \det(M) \neq 0 \quad \text{def'n of non-degeneracy.}$$

earlier claim that disc. is $\det(\mathrm{Tr}_{L/K}(\alpha_i \alpha_j))$

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

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

$$M = \mathrm{Tr}_{L/K}(\theta^{i-1}\theta^{j-1}) \quad \text{and} \quad \det(M) = d(1, \theta, \dots, \theta^{n-1})$$

$$= \prod_{i<j} (\theta_i - \theta_j)^2 \neq 0. \quad \text{separable}$$

where $\sigma_i(\theta) =: \theta_i$ //

Now to prove B is a free A-module of rank $n = [L:K]$,

(so has "integral basis" $\omega_1, \dots, \omega_n$ s.t. for any $b = a_1\omega_1 + \dots + a_n\omega_n$, $a_i \in A$)

need two facts:

<u>Fact 1</u>: Let $\alpha_1, \dots, \alpha_n$ be basis for L/K with $\alpha_i \in B$, then

$$d(\alpha_1, \dots, \alpha_n) \cdot B \subseteq A\alpha_1 + A\alpha_2 + \dots + A\alpha_n$$

i.e. is an A-submodule of a free A-module.

① Note that a basis with $\alpha_i \in B$ exists because, if $x_1, \dots, x_n$ are basis for L/K, then x_i satisfy polynomial $a_n x^n + \cdots + a_0 = 0$

$\Rightarrow$ $a_n^{n-1} \cdot x_i$ satisfies monic poly, so is in B (integral closure of A) and doing this adjustment for all x_i gives new basis with $x_i \in B$.

② Note also that Fact 1 implies ~~[illegible]~~ B has rank n, since containment $\Rightarrow$ rank (dB) = rank $(B) \leq n$, and gens. for B as A-module are gens for L as K-module.

To finish we use:

<u>Fact 2</u>: 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.") ← cf. Jacobson p. 179 "Basic Algebra I"

So $d(\alpha_1, \dots, \alpha_n) B$ is free A-module, hence B is a free A-module.

easy corollary: structure thm. analogous to structure thm for abelian gps. Analogy nicely described in Artin's algebra.

More generally one can show that any fin. gen. B-submodule $M^* \neq 0$ of L is free of rank $[L:K]$.

(see Neukirch)

proof of Fact 1 : Given $b \in B$, write

$$b = k_1 \alpha_1 + \cdots + k_n \alpha_n \qquad k_i \in K.$$

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

$$\underbrace{Tr_{L/K}(\alpha_i b)}_{\in B \cap K = A} = \sum_j Tr_{L/K}(\alpha_i \alpha_j)\, x_j$$

so solve system by inverting matrix with entries $Tr_{L/K}(\alpha_i \alpha_j)$

so the resulting entries are elts of A divided by $\det(Tr_{L/K}(\alpha_i \alpha_j)) = \mathrm{disc}(\alpha_1, \ldots, \alpha_n)$

i.e. $k_i \in \frac{1}{d} A$ so

$db \in A\alpha_1 + \cdots + A\alpha_n$ as desired //

—

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

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

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

$$\Rightarrow \quad d(\alpha_1, \ldots, \alpha_n) = d(\alpha_1', \ldots, \alpha_n')$$

(since def'n involved square of det.)

so can define $\mathrm{disc.}(\mathcal{O}_K) = d(\mathcal{O}_K) := d(\alpha_1, \ldots, \alpha_n)$

for any integral basis of B/A.