Reminder:

We consider a ~~principal ideal~~ domain A with quotient field K, a finite separable field extension L/K, and let B be the integral closure of A in L.

Definition 1.7.3: The *discriminant* of any ordered basis $(b_1, \ldots, b_n)$ of L over K is the determinant of the associated *Gram matrix*

$$\operatorname{disc}(b_1, \ldots, b_n) := \boxed{\det\big(\operatorname{Tr}_{L/K}(b_i b_j)\big)_{i,j=1,\ldots,n} \in K.}$$

Proposition 1.7.4: If $L = K(b)$ and $n = [L/K]$, then $\operatorname{disc}(1, b, \ldots, b^{n-1})$ is the discriminant of the minimal polynomial of b over K.

Proposition 1.7.5: (a) We have $\operatorname{disc}(b_1, \ldots, b_n) \in K^\times$.

(b) If $b_1, \ldots, b_n \in B$, then $\operatorname{disc}(b_1, \ldots, b_n) \in A \smallsetminus \{0\}$ and

$$\boxed{B \subset \frac{1}{\operatorname{disc}(b_1, \ldots, b_n)} \cdot \big(Ab_1 + \ldots + Ab_n\big).}$$

Proposition 1.7.6: If A is a principal ideal domain, then:

(a) B is a free A-module of rank $[L/K]$.

(b) For any basis $(b_1, \ldots, b_n)$ of B over A, the number $\operatorname{disc}(b_1, \ldots, b_n)$ is independent of the basis up to the square of an element of $A^\times$.

Definition 1.7.7: This number is called the *discriminant of B over A* or *of L over K* and is denoted $\operatorname{disc}_{B/A}$ or $\operatorname{disc}_{L/K}$.

Proof: (a) $\forall\, b_1, \ldots, b_n \in B$ basis of L over K:

$$\underbrace{Ab_1 + \ldots + Ab_n}_{\text{free } A\text{-module of rank } n} < B < \underbrace{\frac{1}{\operatorname{disc}(b_1, \ldots, b_n)} \cdot (Ab_1 + \ldots + Ab_n)}_{\text{also}}$$

B: A-module, fin. gen. because A is noetherian. torsion free $\Rightarrow$ free A-module $\Rightarrow$ rank $= n$.

(b) $\left.\begin{matrix} b_1, \ldots, b_n \\ b_1', \ldots, b_n' \end{matrix}\right\}$ bases of B as A-module $\Rightarrow b_i' = \sum a_{ij} b_j$

$$\Rightarrow \left(\operatorname{tr}_{L/K}(b_i' b_j')\right)_{i,j} = U^T \cdot \left(\operatorname{tr}_{L/K}(b_i b_j)\right) \cdot U \quad \text{for } U = (a_{ij})_{i,j} \in GL_n(A)$$

$$\Rightarrow \operatorname{disc}(b_1', \ldots, b_n') = \underbrace{\det(U)^2}_{\in A^\times} \cdot \operatorname{disc}(b_1, \ldots, b_n)$$

qed.

1.8 Linearly disjoint extensions

$L \hookrightarrow L'$

Definition 1.8.1: Two finite separable field extensions $L, L'/K$ are called *linearly disjoint* if $L \otimes_K L'$ is a field.

Proposition 1.8.2: For any two finite separable field extensions $L, L'/K$ within a common overfield M the following statements are equivalent:

(a) L and L' are linearly disjoint over K.

(b) $[LL'/K] = [L/K] \cdot [L'/K]$

(c) $[LL'/L] = [L'/K]$

(d) $[LL'/L'] = [L/K]$

If at least one of L/K and L'/K is galois, they are also equivalent to

(e) $L \cap L' = K$.

Example: $\mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3})$

$\mathbb{Q}(\sqrt{2}) \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{3}) \to \mathbb{Q}(\sqrt{2}, \sqrt{3})$

$\underbrace{\mathbb{Q}(\sqrt{2})}_{2}, \underbrace{\mathbb{Q}(\sqrt[3]{2})}_{3}$

$\underbrace{\mathbb{Q}(\sqrt[3]{2})}_{3}, \underbrace{\mathbb{Q}(\sqrt[3]{2} \cdot e^{\frac{2\pi i}{3}})}_{3}$. $e^{\frac{2\pi i}{3}} = \frac{-1 + i \cdot \sqrt{3}}{2}$

NOT LIN. DISJOINT:

$\underbrace{\mathbb{Q}(\sqrt[3]{2}) \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt[3]{2} e^{\frac{2\pi i}{3}})}_{9} \longrightarrow \mathbb{Q}(\sqrt[3]{2}, e^{\frac{2\pi i}{3}})$ degree 6 over $\mathbb{Q}$.

$\mathbb{Q}(\sqrt[3]{2}) \cap \mathbb{Q}(\sqrt[3]{2} \cdot e^{\frac{2\pi i}{3}}) = \mathbb{Q}$.

Theorem 1.8.3: Consider linearly disjoint finite separable field extensions $L, L'/K$. Assume that A is a principal ideal domain and that $d := \mathrm{disc}_{L/K}$ and $d' := \mathrm{disc}_{L'/K}$ are $\boxed{\text{relatively prime in } A.}$ Let $B, B', \tilde{B}$ be the integral closures of A in L, L', LL'. Then:

(a) $B \otimes_A B' \xrightarrow{\sim} \tilde{B}$.

(b) $\mathrm{disc}_{LL'/K} = d^{[L'/K]} \cdot d'^{[L/K]}$ up to the square of a unit in A.

$LL' = L \otimes_K L'$.

Proof (a): Let $b_1, \dots, b_n$ be a basis of B over A; $b'_1, \dots, b'_{n'}$ — — — B' — — — $\Rightarrow$ they are bases of $\left\{ \begin{matrix} L \\ L' \end{matrix} \right\}$ over K.

$\Rightarrow \{ b_i \otimes b'_j \mid 1 \le i \le n,\ 1 \le j \le n' \}$ basis of $\underset{\sim}{L \otimes_K L'}$ over K. Drop $\otimes$.

$B \otimes_A B' =$ fin. gen. A-module $\Rightarrow B \otimes_A B' \subset \tilde{B}$.

Take $\tilde{b} \in \tilde{B}$ arbitrary. Write $\tilde{b} = \sum_{i,j} a_{ij} b_i b'_j$ with $a_{ij} \in K$.

Claim: $\forall i,j : d' \cdot a_{ij} \in A$.

Proof: Write $\tilde{b} = \sum_{j=1}^{n'} c_j b'_j$ with $c_j = \sum_{i=1}^{n} a_{ij} b_i \in L$.

$\mathrm{Hom}_L(LL', \bar{K}) = \{\tau_1, \dots, \tau_{n'}\} \xrightarrow[\text{res}]{\sim} \mathrm{Hom}_K(L', \bar{K})$.

$T' = [\tau_i(b'_j)]_{i,j=1..n'} \Rightarrow d' = \det(T')^2$. Put $\underline{c} := \begin{pmatrix} c_1 \\ \vdots \\ c_{n'} \end{pmatrix} \in L^{n'}$

$T'\underline{c} = \left(\sum_j \tau_i(b'_j) \cdot c_j \right)_{i=1..n'} = \left(\tau_i\left(\sum_j b'_j c_j \right) \right)_i = (\tau_i(\tilde{b}))_i =: \underline{w}$

$\in \tilde{B}$

$\tilde{T}'$ adjoint of T' $\Rightarrow$ $\det(T')\cdot \underline{c} = \tilde{T}'\cdot T'\cdot \underline{c} = \tilde{T}'\cdot \underline{v}$

$\Rightarrow$ $\underbrace{d'\cdot \underline{c}}_{\in L^{n'}} = \underbrace{\det(T')\cdot \tilde{T}'\cdot \underline{v}}_{\text{integral over } A}$ $\Bigg] \Rightarrow d'\cdot \underline{c} \in B^n$.

$\Rightarrow \forall j: \sum_{i=1}^{n} \underbrace{d' a_{ij}}_{\in A} b_i = d'\cdot c_j \in B$ $\quad \leftarrow$ basis of B over A.

qed (Claim).

<u>Claim</u>: $\forall i,j: \; d\cdot a_{ij} \in A$ same argument!

d, d' relatively prime $\Rightarrow \forall i,j: \; a_{ij} \in A$.

Whence (a).

(b): Write $\mathrm{Hom}_{L'}(LL', \bar{K}) = \{\sigma_1, \dots, \sigma_n\}$

$\Rightarrow \mathrm{Hom}_K(LL', \bar{K}) = \{\sigma_i \tau_j \mid i,j\}$

$$\tilde{T} := \left(\sigma_i\tau_j(b_{i'} b'_{j'})\right)_{(i,j),(i',j')} = \left(\sigma_i(b_{i'})\cdot \tau_j(b'_{j'})\right)_{(i,j),(i',j')}$$

$$= \underbrace{\left(\sigma_i(b_{i'})\cdot \delta_{jj'}\right)_{(i,j),(i',j')}}_{\det = \det(T)^{n'}} \cdot \underbrace{\left(\delta_{ii'}\cdot \tau_j(b'_{j'})\right)_{(i,j),(i',j')}}_{\substack{\text{block diagonal matrix with} \\ n \text{ blocks } (\tau_j(b'_{j'}))_{j,j'} = T'}}$$

$\det(\dots) = \det(T')^n$

$$\Rightarrow \mathrm{disc}_{LL'/K} = \det(\tilde{T})^2 = \det(T)^{2n'}\cdot \det(T')^{2n} = d^{n'}\cdot d'^{n}.$$

qed.

1.9 Dedekind Rings

Definition 1.9.1: (a) A ring A is *noetherian* if every ideal is finitely generated.

(b) An integral domain A has *Krull dimension* 1 if it is not a field and every non-zero prime ideal is a maximal ideal.

(c) A noetherien normal integral domain of Krull dimension 1 is called a *Dedekind ring*.

Proposition 1.9.2: Any principal ideal domain that is not a field is a Dedekind ring.

Proof: . — — — . End

Examples 1.9.3: Take $A = \mathbb{Z}$ or $A = \mathbb{Z}[i]$ or $A = k[t]$ or $A = k[[t]]$ for a field k.

L/K finite sep.
$B =$ int. closure of A in L.

In the following we assume that $\boxed{A \subset K \text{ is Dedekind and that } B \subset L \text{ is as above.}}$ (with $K = \mathrm{Quot}(A)$)

Proposition 1.9.4: (a) For every multiplicative subset $S \subset A$ the ring $S^{-1}A$ is Dedekind or a field.

(b) For every prime ideal $0 \neq \mathfrak{p} \subset A$ the localization $A_{\mathfrak{p}}$ is a discrete valuation ring.

Proof (a) {prime ideals of $S^{-1}A$} $\longleftrightarrow$ {prime ideals $\mathfrak{p} \subset A$ with $\mathfrak{p} \cap S = \emptyset$}.
Check $S^{-1}A$ noetherian.

(b) $A_{\mathfrak{p}} = (A \setminus \mathfrak{p})^{-1} A$ not a field, ... (later). qed.

Theorem 1.9.5: The ring B is Dedekind and finitely generated as an A-module.

Proof: $b_1, \dots, b_n \in B$ basis of L over K. $\Rightarrow$ $B \subset \underbrace{\frac{1}{\mathrm{disc}(b_1,\dots,b_n)} \cdot (Ab_1 + \dots + Ab_n)}_{\text{fin. gen. } A\text{-module}}$.

$\Rightarrow$ B fin. gen. A-module.

— $\mathfrak{b} \subset B$ ideal $\Rightarrow$ $\mathfrak{b}$ is an A-submodule of B. A noetherian $\Rightarrow$ $\mathfrak{b}$ fin. gen. A-module.
$\Rightarrow$ $\mathfrak{b}$ fin. gen. B-module $\Longrightarrow$ B noetherian.

— B integral domain, normal by construction.

— A has Krull dim. 1 $\Rightarrow$ $\exists\, \mathfrak{p}$ prime ideal of A nonzero.
Lying over $\Rightarrow$ $\exists\, \mathfrak{P}$ prime ideal of B with $\mathfrak{P} \cap A = \mathfrak{p}$ $\Longrightarrow$ $\mathfrak{P} \neq (0)$ $\Rightarrow$ B not a field.

— Let $\mathfrak{P} \subset B$ be a nonzero prime ideal. $\Rightarrow$ $\mathfrak{P} \cap A$ is a prime ideal. If $\mathfrak{P} \cap A = (0) = (0) \cap A$,
§1.2 $\Rightarrow$ $\mathfrak{P} = (0)$ $\Rightarrow$ ↯.
Else $\mathfrak{P} \cap A =$ max. ideal. Take a max. ideal $\mathfrak{P} \subset \tilde{\mathfrak{P}} \subset B$.

$\Rightarrow \tilde{\mathfrak{q}} \cap A \supset \mathfrak{q} \cap A$, prime $\Rightarrow \tilde{\mathfrak{q}} \cap A = \mathfrak{q} \cap A$. $\Rightarrow$ §1.7.2 $\Rightarrow \tilde{\mathfrak{q}} = \mathfrak{q}$. $\Rightarrow \mathfrak{q}$ maximal.

1.10 Fractional Ideals

Definition 1.10.1:

Quot(A).
||

(a) A non-zero finitely generated A-submodule of K is called a *fractional ideal of* A.

(b) A fractional ideal of the form $(x) := Ax$ for some $x \in K^\times$ is called *principal*.

(c) The *product* of two fractional ideals $\mathfrak{a}, \mathfrak{b}$ is defined as

$$\mathfrak{a}\mathfrak{b} \; := \; \left\{ \textstyle\sum_{i=1}^r a_i b_i \;\middle|\; r \geqslant 0,\; a_i \in \mathfrak{a}, b_i \in \mathfrak{b} \right\}.$$

(d) The *inverse* of a fractional ideal $\mathfrak{a}$ is defined as

$$\mathfrak{a}^{-1} \; = \; \left\{ x \in K \;\middle|\; x \cdot \mathfrak{a} \subset A \right\}.$$

Proposition 1.10.2: For any fractional ideals $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ we have:

(a) There exist $a, b \in A \smallsetminus \{0\}$ with $(a) \subset \mathfrak{a} \subset (\frac{1}{b})$.

(b) $\mathfrak{a}\mathfrak{b}$ and $\mathfrak{a}^{-1}$ are fractional ideals.

(c) $\mathfrak{a}\mathfrak{b} = \mathfrak{b}\mathfrak{a}$ and $(\mathfrak{a}\mathfrak{b})\mathfrak{c} = \mathfrak{a}(\mathfrak{b}\mathfrak{c})$ and $(1)\mathfrak{a} = \mathfrak{a}$.

(d) $\mathfrak{a} \subset A$ if and only if $A \subset \mathfrak{a}^{-1}$.