Reminder:

Consider a ring extension $A \subset B$.

Definition 1.1.1:

(a) An element $b \in B$ is called *integral over* A if there exists a monic $f \in A[X]$ with $f(b) = 0$.

(b) The ring B is called *integral over* A if every $b \in B$ is integral over A.

(c) The *integral closure of* A *in* B is the set $\tilde{A} := \{b \in B \mid b \text{ integral over } A\}$.

Proposition 1.1.4:

(b) The subset $\tilde{A}$ is a subring of B that contains A.

(c) The subring $\tilde{A}$ is its own integral closure in B.

1.3 Normalization

From now on we assume that A is an integral domain with quotient field K.

Definition 1.3.1: (a) The integral closure of A in K is called the *normalization of A*.

(b) The ring A is called *normal* if this normalization is A.

Proposition 1.3.2: (a) The normalization of A is normal.

(b) Any unique factorization domain is normal.

$\nu_i \in \mathbb{Z}$.

Proof of (b): Take $b \in \tilde{A} \subset K$, $b \neq 0$. Write $b = u \cdot \prod p_i^{\nu_i}$

unit in A inequivalent primes in A.

Suppose some $\nu_j < 0$.

Write $b^n + a_1 b^{n-1} + \dots + a_n = 0$ with $a_i \in A$.

$$\Rightarrow u^n \cdot \prod_i p_i^{\nu_i n} + a_1 u^{n-1} \prod p_i^{\nu_i (n-1)} + \dots + a_n = 0.$$

Multiply by $\prod_{i \neq j} p_i^{\max(0,-\nu_i)\cdot n} \cdot p_j^{-\nu_j n}$

$$\Rightarrow \underbrace{(\text{not divisible by } p_j)}_{\in A} + \underbrace{(\text{divisible by } p_j)}_{\in A} = 0 \Rightarrow \text{Contradiction.}$$

So all $\nu_j \geq 0$

$\Rightarrow b \in A$.

qed.

1.4 Localization

Definition 1.4.1: A subset $S \subset A \setminus \{0\}$ is called *multiplicative* if it contains 1 and is closed under multiplication.

Definition-Proposition 1.4.2: For any multiplicative subset $S \subset A$ the subset

$$\boxed{S^{-1}A \; := \; \left\{ \tfrac{a}{s} \;\middle|\; a \in A,\; s \in S \right\}}$$

is a subring of K that contains A and is called the *localization of A with respect to S.*

Proof: $\frac{a}{1} \in S^{-1}A$, $1 = \frac{1}{1} \in S^{-1}A$, $\frac{a}{s} \cdot \frac{a'}{s'} = \frac{aa'}{ss'}$, $\frac{a}{s} + \frac{a'}{s'} = \frac{as' + a's}{ss'} \in S^{-1}A$. qed

Example 1.4.3: For every prime ideal $\mathfrak{p} \subset A$ the subset $A \setminus \mathfrak{p}$ is multiplicative. The ring $A_{\mathfrak{p}} := (A \setminus \mathfrak{p})^{-1}A$ is called the *localization of A at $\mathfrak{p}$*.

Proposition 1.4.4: For every multiplicative subset $S \subset A$ we have:

(a) $S^{-1}\tilde{A} = \widetilde{S^{-1}A}$.

(b) If A is normal, then so is $S^{-1}A$.

Proof (a): $\forall\, b \in \tilde{A}$: $b^n + a_1 b^{n-1} + \ldots + a_n = 0$ with $a_i \in A$

$\forall\, s \in S$: $\left(\frac{b}{s}\right)^n + \frac{a_1}{s} \cdot \left(\frac{b}{s}\right)^{n-1} + \ldots + \frac{a_n}{s^n} = 0 \Rightarrow \frac{b}{s}$ integral over $S^{-1}A$.

$\Rightarrow \subseteq$.

Take $c \in (S^{-1}A)^{\sim}$, with $c^n + u_1 c^{n-1} + \dots + u_n = 0$ with $u_i \in S^{-1}A$.

Write $u_i = \frac{a_i}{s}$ with $a_i \in A$, $s \in S$.

$$\Rightarrow \quad (sc)^n + s u_1 (sc)^{n-1} + \dots + s^n u_n = 0$$

$$\Rightarrow \quad (sc)^n + \underbrace{a_1} (sc)^{n-1} + \dots + \underbrace{s^{n-1} a_n}_{\in A} = 0$$

$$\Rightarrow \quad sc \in \tilde{A} \quad \Rightarrow \quad c = \frac{sc}{s} \in S^{-1}\tilde{A}.$$

qed.

1.5 Field extensions

In the following we consider a $\boxed{\text{normal}}$ integral domain A with quotient field K, and an algebraic field extension L/K, and let B be the integral closure of A in L.

Proposition 1.5.1: For any homomorphism $\sigma\colon L \to M$ of field extensions of K, an element $x \in L$ is integral over A if and only if $\sigma(x)$ is integral over A.

Proof: $\forall f \in A[X]$ monic: $f(\sigma(x)) = \sigma(f(x))$

$$\begin{array}{ccc} \shortparallel & & \shortparallel \\ 0 & \Longleftrightarrow & 0 \end{array}$$

qed.

Proposition 1.5.2: An element $x \in L$ is integral over A if and only if the minimal polynomial of x over K has coefficients in A.

$\mu(K)$

Proof: $$\mu(X) = \prod_{\sigma \in \mathrm{Hom}_K(L,\overline{K})} (X - \sigma(x))^d \quad \text{in } \overline{K}[X].$$

If x is integral over A, then so are all $\sigma(x)$.

$\Rightarrow$ the coefficients of $\mu(X)$ are integral over A and lie in K $\Big]$ $\Rightarrow$ lie in A.

qed

Proposition 1.5.3: We have $(A \smallsetminus \{0\})^{-1}B = L$.

<u>Proof:</u> $\forall\, y \in L$. Choose $x_1, \dots, x_n \in K$ with $y^n + x_1 y^{n-1} + \dots + x_n = 0$.

Write each $x_i = \frac{a_i}{s}$ with $a_i \in A$, $s \in A \smallsetminus \{0\}$.

$$\Rightarrow \quad (sy)^n + \underbrace{s x_1}_{\in A} (sy)^{n-1} + \dots + \underbrace{s^n x_n}_{\in A} = 0$$

$$\Rightarrow \quad sy \in B \quad \Rightarrow \quad y = \frac{sy}{s} \in (A \smallsetminus \{0\})^{-1} B.$$

<u>qed</u>.

1.6 Norm and Trace

Assume that L/K is finite separable. Let $\bar{K}$ be an algebraic closure of K.

Definition 1.6.1: For any $x \in L$ we consider the K-linear map $T_x \colon L \to L$, $u \mapsto ux$.

(a) The *norm of x for L/K* is the element $\mathrm{Nm}_{L/K}(x) := \det(T_x) \in K$.

(b) The *trace of x for L/K* is the element $\mathrm{Tr}_{L/K}(x) := \mathrm{tr}(T_x) \in K$.

Proposition 1.6.2: (a) For any $x, y \in L$ we have $\mathrm{Nm}_{L/K}(xy) = \mathrm{Nm}_{L/K}(x) \cdot \mathrm{Nm}_{L/K}(y)$.

(b) The map $\mathrm{Nm}_{L/K}$ induces a homomorphism $L^\times \to K^\times$.

(c) The map $\mathrm{Tr}_{L/K} \colon L \to K$ is K-linear.

Proof: (a) $T_{xy} = T_x \circ T_y \Rightarrow \det(T_{xy}) = \det(T_x) \cdot \det(T_y)$.

(b) $x \neq 0 \Rightarrow T_x$ bijective $\Rightarrow \det(T_x) \neq 0$.

(c) $T_{x+y} = T_x + T_y \Rightarrow \mathrm{tr}(T_{x+y}) = \mathrm{tr}(T_x) + \mathrm{tr}(T_y)$

$\forall a \in K$: $T_{ax} = a \cdot T_x \Rightarrow \mathrm{tr}(T_{ax}) = a \cdot \mathrm{tr}(T_x)$.

qed.

Proposition 1.6.3: For any $x \in L$ we have

$$\mathrm{Nm}_{L/K}(x) = \prod_{\sigma\in\mathrm{Hom}_K(L,\bar{K})} \sigma(x) \qquad \text{and} \qquad \mathrm{Tr}_{L/K}(x) = \sum_{\sigma\in\mathrm{Hom}_K(L,\bar{K})} \sigma(x).$$

Proof: Write $K' := K(x)$ $\Rightarrow$ min. Pol $p(X) = \prod_{\sigma\in\mathrm{Hom}_K(K',\bar{K})} (X - \sigma(x))$

$[L/K'] = d$ $\Rightarrow$ char. Pol. of T_x is $\prod_{\sigma\in\mathrm{Hom}_K(K',\bar{K})} (X-\sigma(x))^d = \prod_{\sigma\in\mathrm{Hom}_K(L,\bar{K})} (X-\sigma(x))$

$L \cong (K')^d$

qed.

Proposition 1.6.4: The map $\mathrm{Tr}_{L/K} : L \to K$ is non-zero.

Proof: The $\sigma \in \mathrm{Hom}_K(L,\bar{K})$ are $\bar{K}$-linearly independent.

$$\Rightarrow \sum_{\sigma\in\mathrm{Hom}_K(L,\bar{K})} \sigma \neq 0.$$

qed.

Proposition 1.6.5: For any two finite separable field extensions $M/L/K$ we have:

(a) $\mathrm{Nm}_{L/K} \circ \mathrm{Nm}_{M/L} = \mathrm{Nm}_{M/K}$.

(b) $\mathrm{Tr}_{L/K} \circ \mathrm{Tr}_{M/L} = \mathrm{Tr}_{M/K}$. ← same with Σ

Proof: $\mathrm{Nm}_{M/K}(x) = \prod_{\sigma\in \mathrm{Hom}_K(M,\bar K)} \sigma(x) = \prod_{\rho\in \mathrm{Hom}_K(L,\bar K)} \Big(\prod_{\substack{\sigma\in \mathrm{Hom}_K(M,\bar K) \\ \sigma|_L = \rho}} \sigma(x) \Big)$

For each $\rho \in \mathrm{Hom}_K(L,\bar K)$ choose extension $\tilde\rho \in \mathrm{Hom}_K(M,\bar K)$

$$= \prod_{\rho} \Big(\prod_{\tau \in \mathrm{Hom}_L(M,\bar K)} \tilde\rho\,\tau(x) \Big)$$

$$= \underbrace{\prod_{\rho} \tilde\rho}_{\mathrm{Nm}_{L/K}} \Big(\underbrace{\prod_{\tau} \tau(x)}_{\mathrm{Nm}_{M/L}(x)} \Big) .$$

qed.

$$\begin{array}{ccc} L & \supset & B \ni x \\ | & & | \\ K & \supset & A \end{array}$$

Proposition 1.6.6: For any $x \in B$ we have:

(a) $\mathrm{Nm}_{L/K}(x) \in A$. ✓

(b) $\mathrm{Nm}_{L/K}(x) \in A^\times$ if and only if $x \in B^\times$.

(c) $\mathrm{Tr}_{L/K}(x) \in A$. ✓

Proof: $x \in B \Rightarrow$ any $\sigma(x)$ integral over A. $\Rightarrow \mathrm{Nm}_{L/K}(x)$, $\mathrm{Tr}_{L/K}(x)$ integral over A, in K.

A normal $\Rightarrow\ \in A$.

(b) $x \in B^\times \Rightarrow x^{-1} \in B \Rightarrow \mathrm{Nm}_{L/K}(x^{-1}) \in A$; $\mathrm{Nm}_{L/K}(x)\cdot \mathrm{Nm}_{L/K}(x^{-1}) = 1$.
$\in A^\times$.

$a := \mathrm{Nm}_{L/K}(x) \in A^\times \Rightarrow 1 = a^{-1}\cdot a = \underbrace{x}\cdot \underbrace{a^{-1}\cdot \prod_{\sigma\neq id} \sigma(x)}$ ← integral over A, in L $\Rightarrow\ \in B$. $\Rightarrow x \in B^\times$. qed

1.7 Discriminant

Proposition 1.7.1: The map

$$L \times L \longrightarrow K, \quad (x, y) \mapsto \mathrm{Tr}_{L/K}(xy).$$

is a non-degenerate symmetric K-bilinear form.

Proof: $1.6.4 \Rightarrow \exists\, x \in L:\ \mathrm{Tr}_{L/K}(x) \neq 0$. $\Rightarrow$ image of $(x,1)$ is nonzero.

qed.

Lemma 1.7.2: Write $\mathrm{Hom}_K(L, \bar{K}) = \{\sigma_1, \ldots, \sigma_n\}$ with $[L/K] = n$ and consider the matrix $T := (\sigma_i(b_j))_{i,j=1,\ldots,n}$. Then

Gram Matrix

Note: $T \in \mathrm{Mat}_{n\times n}(\bar{K})$

$$T^T \cdot T \;=\; \big(\mathrm{Tr}_{L/K}(b_i b_j)\big)_{i,j=1,\ldots,n}. \in \mathrm{Mat}_{n\times n}(K).$$

Proof: $T^T \cdot T = (\sigma_k(b_i))_{i,k} \cdot (\sigma_k(b_j))_{k,j} = \Big(\underbrace{\sum_k \sigma_k(b_i) \cdot \sigma_k(b_j)}_{\sum_k \sigma_k(b_i b_j) = \mathrm{Tr}_{L/K}(b_i b_j)} \Big)_{i,j} =$

$\sum_k \sigma_k(b_i b_j) = \mathrm{Tr}_{L/K}(b_i b_j)$. qed.

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*

$$\mathrm{disc}(b_1, \ldots, b_n) \;:=\; \det\big(\mathrm{Tr}_{L/K}(b_i b_j)\big)_{i,j=1,\ldots,n} \;=\; \det(T)^2 \;\in\; K.$$

$\det(T) \in \bar{K}$.

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

Proof: $\det(T) = \det\big(\sigma_i(b^{j-1})\big)_{i,j} = \det\big(\sigma_i(b)^{j-1}\big)_{i,j}$ Vandermonde

$$= \prod_{1 \le i < j \le n} \big(\sigma_j(b) - \sigma_i(b)\big).$$

$$\Rightarrow \mathrm{disc}(1, b, \ldots, b^{n-1}) = \prod_{i<j} \big(\sigma_j(b) - \sigma_i(b)\big)^2 = \text{discriminant}.$$

qed

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

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

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

Proof: (a) $\big(\mathrm{Tr}_{L/K}(b_i b_j)\big)_{i,j}$ is invertible, because $\mathrm{Tr}: L \times L \to K$ is nondegenerate.

(b). $b_i \in B \Rightarrow \mathrm{disc}(\ldots b_i \ldots)$ integral over A, in $K \Rightarrow$ is in A. nonzero by (a).

(c) Take $y \in B$; write $y = \sum_j b_j y_j$ with $y_j \in K$.

$$\Rightarrow x_i := \mathrm{Tr}_{L/K}(\underbrace{b_i y}_{\in B}) = \sum_j \mathrm{Tr}_{L/K}(b_i b_j)\, y_j. \Rightarrow$$

$$\Rightarrow \quad \underline{x} := \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \underbrace{\left(\mathrm{Tr}_{L/K}(b_i b_j')\right)_{i,j}}_{M} \cdot \underbrace{\begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}}_{\underline{y}} \qquad \underline{x} = M \cdot \underline{y}$$

$$\tilde{M} := \text{adjoint of } M \quad \Rightarrow \quad \tilde{M} \cdot \underline{x} = \tilde{M} \cdot M \cdot \underline{y} = \det(M) \cdot \underline{y} = \mathrm{disc}(b_1, \dots, b_n) \cdot \underline{y}$$

$$x_i \in A. \quad \Rightarrow \qquad \underline{y} = \frac{1}{\mathrm{disc}(b_1, \dots, b_n)} \cdot \underbrace{\tilde{M} \cdot \underline{x}}_{\text{coeff. in } A.}$$

$$\Rightarrow \quad y = \sum_j b_j y_j \in \frac{1}{\mathrm{disc}(b_1, \dots, b_n)} \cdot \sum_{j=1}^{n} b_j' A \, .$$

qed.