**Recall:** $A$ is Dedekind if

- $A$ is a domain,
- $A$ is integrally closed,
- every non-zero prime ideal is maximal,
- $A$ is noetherian.

**Key properties:** (1) Unique factorization into prime ideals

(2) Stability under finite separable extension

**Thm:**

„Q

> Let $A$ Dedekind, $K/\mathrm{Frac}(A)$ finite separable, then $\mathcal{O}_K(A)$ is Dedekind and finitely generated as an $A$-module.

Today we prove the stability theorem.

A few easy observations. Let $A$ and $K$ as in the theorem.

1) $K$ a field $\Rightarrow \mathcal{O}_K(A)$ is a domain

2) $\mathcal{O}_K(A)$ is integrally closed in $K$ and, since, $Q = \mathrm{Frac}(\mathcal{O}_K(A)) \subseteq K$, $\mathcal{O}_K(A)$ is integrally closed.
Details as exercise.

3) Suppose $\mathcal{O}_K(A)$ is $A$-f.t. Since $A$ is noetherian, every $A$-submodule of $\mathcal{O}_K(A)$ is $A$-f.t. and, in particular, every $\mathcal{O}_K(A)$-submodule of $\mathcal{O}_K(A)$ (i.e., every ideal) is $A$-f.t. and, therefore, also $\mathcal{O}_K(A)$-f.t., i.e., $\mathcal{O}_K(A)$ is noetherian.

Hence, in order to prove the theorem, we only need to show that

1) $\mathcal{O}_K(A)$ is $A$-f.t.

2) non-zero primes in $\mathcal{O}_K(A)$ are maximal.

Recall: Let $K/\mathbb{Q}$ a finite field extension, then

$$[\times\cdot]_{K/\mathbb{Q}} : K \longrightarrow \mathrm{End}_{\mathbb{Q}}(K)$$
$$z \longmapsto [\times z]_{K/\mathbb{Q}} : y \longmapsto y\cdot z$$

is an injective $\mathbb{Q}$-algebra homomorphism. In particular, for every $P\in\mathbb{Q}[X]$, $z\in K$, we have

$$[\times P(z)]_{K/\mathbb{Q}} = P([\times z]_{K/\mathbb{Q}}). \qquad (*)$$

Definition:

Let $K/\mathbb{Q}$ finite extension, $z\in K$. Then

$$\mathrm{tr}_{K/\mathbb{Q}}(z) := \mathrm{tr}([\times z]_{K/\mathbb{Q}}) \qquad \text{"trace"}$$

$$\mathrm{Nr}_{K/\mathbb{Q}}(z) := \det([\times z]_{K/\mathbb{Q}}) \qquad \text{"norm"}$$

Note that, given $K/\mathbb{Q}$ finite extension, the map $\langle\cdot,\cdot\rangle_{K/\mathbb{Q}} : K^2 \longrightarrow \mathbb{Q}$

$$\langle z, z'\rangle_{K/\mathbb{Q}} := \mathrm{tr}([\times z.z']_{K/\mathbb{Q}})$$

is $\mathbb{Q}$-bilinear.

One can show that $P_{\mathbb{Q},\min,z} = P_{\min,[\times z]_{K/\mathbb{Q}}}$. We define $P_{K/\mathbb{Q},car,z} = P_{car,[\times z]_{K/\mathbb{Q}}}$.

## Theorem

Let $K/Q$ finite extension. The following are equivalent:

- $\forall z \in K$ $[\times z]_{K/Q}$ is diagonalizable (over $\overline{Q}$),
- $\forall z \in K$ $P_{Q,\min,z}$ has only simple roots,
- $\langle \cdot , \cdot \rangle_{K/Q}$ is non-degenerate (i.e., $z \mapsto z^* \in K^*$, $z \mapsto \langle \cdot , z \rangle_{K/Q}$ is an isomorphism)
- $|\mathrm{Hom}_Q(K, \overline{Q})| = [K:Q]$

## Definition:

Let $K/Q$ finite extension. If $\forall z \in K$ $P_{Q,\min,z}$ has only simple roots, then $K/Q$ is separable.

From now on we fix $A$ Dedekind, $Q = \mathrm{Frac}(A)$, $K/Q$ finite separable, $B = \mathcal{O}_K(A)$.

Lemma

$B = \{ z \in K : P_{K/Q,car,z} \in A[X] \}$.

Pf: If $P_{K/Q,car,z} \in A[X]$, then $z \in B$ as $P_{K/Q,car,z}$ is monic, (*), and Cayley-Hamilton.

To prove the opposite inclusion, note that

$$P_{K/Q,car,z} = \left(P_{Q,min,z}\right)^{[K:Q[z]]}$$

and thus it suffices to show that $P_{Q,min,z} \in A[X]$ (à priori, we only know that there is some monic elmt. in $A[X]$ annihilating $z$).

Let $P \in A[X]$ monic s.t. $P(z) = 0$. Then $P_{Q,min,z} \mid P$ in $Q[X]$ and thus all the zeroes of $P_{Q,min,z}$ lie in $B$.

Let $P_{Q,min,z} = \prod_{i=1}^{r} (X - z_i)$, and $R = A[z_1, \dots, z_r]$. Then $R \subseteq B$ and

$$P_{Q,min,z} \in R[X] \cap Q[X].$$

But $R \cap Q \subseteq B \cap Q = A$ as $A$ is integrally closed. Thus $P_{Q,min,z} \in A[X]$.

Corollary

Let $z \in B$, then $tr_{K/Q}(z), Nr_{K/Q}(z) \in A$

Proof: $P_{K/Q,car,z}(X) = det(X \cdot Id_K - [xz]_{K/Q}) = X^d - tr([xz]_{K/Q}) X^{d-1} + \dots + (-1)^d det([xz]_{K/Q})$

**Lemma**

$\forall z \in K \ \exists \alpha \in A \quad \alpha . z \in B$

**Pf:** $K/Q$ finite $\Rightarrow \exists\, a_0, \dots, a_{d-1} \in Q$ s.t.

$$z^d + a_{d-1} z^{d-1} + \dots + a_0 = 0$$

Choose $\alpha \in A$ s.t. $\alpha a_i \in A$ for all $0 \leq i < d$ (clearing denominators of the coefficients).

Then

$$(\alpha z)^d + \alpha a_{d-1} (\alpha z)^{d-1} + \dots + \alpha^d a_0 = 0$$

and, hence, $\alpha z \in B$.

**Corollary:**

B contains a $Q$-basis of $K$.

**Proof:** $[K:Q] < \infty \Rightarrow \exists (z_1, \dots, z_d)$ $Q$-basis of $K$. Choose $\alpha \in A - \{0\}$ s.t. $\alpha . z_1, \dots, \alpha . z_d \in B$.

Then $(\alpha . z_1, \dots, \alpha . z_d)$ is a $Q$-basis of $K$.

**Proposition:**

B is A-f.t. ($\Rightarrow$ B noetherian ring)

If A is a PID, then B is free of rank $[K:Q] = d$.

**Proof:** Let $(z_1, \dots, z_d) \in B^d$ a $Q$-basis of $K$ and, as $\langle \cdot, \cdot \rangle_{K|Q}$ is non-degenerate, let $(z_1^*, \dots, z_d^*) \in K^d$ a dual basis, i.e.,

$$\langle z_i, z_j^* \rangle_{K|Q} = \delta_{ij}.$$

Then

(Claim:) $B \subseteq A . z_1^* + \dots + A . z_d^*$.

Indeed, given $z \in B$, let $z = \sum_{i=1}^{d} q_i \cdot z_i^*$, then

$$q_i := \langle z_i, z \rangle = tr_{K|Q}(\underbrace{z_i . z}_{\in B}) \in A.$$

As $A$ is noetherian, $A\cdot z_1^* + \dots + A\cdot z_d^*$ is noetherian and, hence, $B$ is $A$-f.t.

Note that

$$A\cdot z_1^* + \dots + A\cdot z_d^*,\ \overbrace{A\cdot z_1 + \dots + A\cdot z_d}^{\subseteq B}$$

are free of rank $d$ ($(z_1^*, \dots, z_d^*), (z_1, \dots, z_d)$ are $\mathbb{Q}$-bases of $K$). Hence $B$ contains and is contained in free $A$-modules of rank $d$. If $A$ is a PID, this implies that $B$ is free of rank $d$.

<u>Corollary</u>

If $A$ is a PID, every non-zero ideal $\underline{a} \lhd B$ is a free $A$-module of rank $d = [K:\mathbb{Q}]$.

<u>Pf</u>: $B$ is $A$-f.t., $A$-noetherian, thus every ideal in $B$ is $A$-f.t.

Moreover, for any $b \in \underline{a} - \{0\}$

$$(b) = \underbrace{b.B}_{\text{free rank } d} \subseteq \underline{a} \subseteq \underbrace{B}_{\text{free rank } d} \Rightarrow \underline{a} \text{ is free of rank } d.$$

Lemma

Every non-zero prime ideal of $B$ is maximal

Proof: Let $\mathfrak{P} \subseteq B$ non-zero prime. Then $\mathfrak{p} = A \cap \mathfrak{P}$ is a non-zero prime ideal:

$z \in \mathfrak{P} - \{0\} \Rightarrow \exists a_0, \dots, a_{d-1} \in A$ s.t. $a_0 \neq 0$ and

$$\mathfrak{P} \ni z^d + a_{d-1} z^{d-1} + \dots + a_1 z = -a_0 \in A.$$

Hence

$$A/\mathfrak{p} \longrightarrow B/\mathfrak{P} \xleftarrow{} \text{domain} \Rightarrow A/\mathfrak{p} \text{ is a domain} \Rightarrow \mathfrak{p} \text{ prime.}$$

$A$ Dedekind $\Rightarrow A/\mathfrak{p} =: k_\mathfrak{p}$ is a field. $B$ is $A$-f.t. $\Rightarrow B/\mathfrak{P}$ is finite dim. over $k_\mathfrak{p}$.

As $B/\mathfrak{P}$ is a domain, $B/\mathfrak{P}$ is a field. ∎

## Relative Theory

Let $A \hookrightarrow Q \hookrightarrow K$ a finite sep. extension of the field of fractions of the Dedekind ring $A$.

Let $B = \mathcal{O}_K$. We obtain maps

$$\{\underline{\mathfrak{b}} \triangleleft B\} \longrightarrow \{\underline{\mathfrak{a}} \triangleleft A\}, \quad \underline{\mathfrak{b}} \longmapsto \underline{\mathfrak{b}} \cap A \qquad \text{"contraction"}$$

$$\{\underline{\mathfrak{a}} \triangleleft A\} \longrightarrow \{\underline{\mathfrak{b}} \triangleleft B\}, \quad \underline{\mathfrak{a}} \longmapsto B.\underline{\mathfrak{a}} = (\underline{\mathfrak{a}}) \qquad \text{"extension"}$$

**Proposition:**

The contraction is a surjective map between non-zero prime ideals.
Given $\mathfrak{p} \in \operatorname{Spec}(A)^*$, the fiber is exactly

$$\operatorname{Spec}_{\mathfrak{p}}(B) := \{\mathfrak{P} \in \operatorname{Spec}(B)^* : v_{\mathfrak{P}}(B.\mathfrak{p}) > 0\}.$$

primes lying above $\mathfrak{p}$, short: $\mathfrak{P} | \mathfrak{p}$

finite!

**Corollary:**

Let $\mathfrak{p} \in \operatorname{Spec}(A)^*$, then $\mathfrak{p} = B.\mathfrak{p} \cap A$.

## Some terminology :

Let $\mathfrak{p} \in \operatorname{Spec}(A)^\times$, $\mathfrak{P} \in \operatorname{Spec}_{\mathfrak{p}}(B)$. Then

- the ramification index of $\mathfrak{P}$ (at $\mathfrak{p}$) is $e_{\mathfrak{P}|\mathfrak{p}} := v_{\mathfrak{P}}(B.\mathfrak{p})$
- $k_{\mathfrak{p}} := A/\mathfrak{p}$ is the residue field at $\mathfrak{p}$
- $k_{\mathfrak{p}} \hookrightarrow k_{\mathfrak{P}} = B/\mathfrak{P}$ is finite extension (as $B$ is $A$-f.t.) and the inertia degree of $\mathfrak{P}$ (at $\mathfrak{p}$) is $f_{\mathfrak{P}|\mathfrak{p}} := [k_{\mathfrak{P}} : k_{\mathfrak{p}}]$

Remarks: $\mathfrak{p}$ is unramified in $B$ if $e_{\mathfrak{P}|\mathfrak{p}} = 1$ for all $\mathfrak{P} \in \operatorname{Spec}_{\mathfrak{p}}(B)$.

- $B.\mathfrak{p} = \prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P}^{e_{\mathfrak{P}|\mathfrak{p}}}$

**Theorem** (Degree formula)

Let $\mathfrak{p} \in \operatorname{Spec}(A)^{*}$, $K_{\mathfrak{p}} := B/B\cdot\mathfrak{p}$. Then $K_{\mathfrak{p}}$ is a finite dimensional $k_{\mathfrak{p}}$-algebra and

$$[K:\mathbb{Q}] \overset{(i)}{=} \dim_{k_{\mathfrak{p}}}(K_{\mathfrak{p}}) \overset{(ii)}{=} \sum_{\mathfrak{P}\mid\mathfrak{p}} e_{\mathfrak{P}\mid\mathfrak{p}} \cdot f_{\mathfrak{P}\mid\mathfrak{p}} .$$

In particular, $|\operatorname{Spec}_{\mathfrak{p}}(B)| \leq [K:\mathbb{Q}]$