Kap 2: Zahlkörper und ganz algebraische Zahlen

§1 Zahlkörper

Def: Ein Zahlkörper K ist eine Erweiterung $K/\mathbb{Q}$ mit $[K:\mathbb{Q}] < \infty$.

Bem 1: $K/\mathbb{Q}$ ist separabel.
$\overset{\text{Satz v. prim. El.}}{\Rightarrow}$ $K/\mathbb{Q}$ ist einfach, d.h. es ex. $\alpha \in K$ mit $K = \mathbb{Q}[\alpha]$.

Bsp:
- Quadratische Zahlkörper
  $d \in \mathbb{Z}$ quadratfrei, $d \neq 0, 1$.
  $K = \mathbb{Q}(\sqrt{d})$.
- Kreisteilungskörper:
  $n \in \mathbb{N}$, $\zeta_n = e^{\frac{2\pi i}{n}} \in \mathbb{C}$.
  $K = \mathbb{Q}(\zeta_n)$ ist Erw.-Kp vom Grad $\varphi(n)$ über $\mathbb{Q}$.

Def: Eine komplexe Zahl $\alpha \in \mathbb{C}$ heißt algebraisch ganz (über $\mathbb{Z}$), falls es ein normiertes Pol $f \in \mathbb{Z}[x]$ gibt mit $f(\alpha) = 0$.

Bsp:
- $\sqrt{d}$
- ζ_n

Diesen Ganzheitsbegriff wollen wir etwas allgemeiner untersuchen:

§2 Ganze Ringerweiterungen

Ringe sind kommutativ, mit 1.

Def: Sei R Ring. Ein R-Modul ist eine abelsche Gruppe M zusammen mit einer Abb.

$$R \times M \to M, \quad (r,m) \mapsto r \cdot m,$$

so dass die „Vektorraum-Axiome"

$$\begin{aligned} r\cdot(x+y) &= rx + ry \\ (r+s)x &= rx + sx \\ r(sx) &= (rs)x \\ 1\cdot x &= x \end{aligned} \qquad \forall\, r,s \in R,\ x,y \in M$$

erfüllt sind.

Bsp:
- Ein K-VR V (K Kpr) ist ein K-Modul.
- Sind R, S Ringe und $\varphi: R \to S$ Ringhom, so ist S ein R-Modul vermöge
$$r \cdot s = \varphi(r)\cdot s, \quad r \in R,\ s \in S.$$
- Jede ab. Gruppe A ist ein $\mathbb{Z}$-Modul vermöge
$$n \cdot a = \underbrace{a+a+\dots+a}_{n}, \quad n \in \mathbb{Z},\ a \in A.$$
- Modulhomomorphismen, Untermoduln, Faktormoduln, ... wie für Vektorräume.

Def: Eine Ringerweiterung $R \subset R'$ ist eine Inklusion von Ringen.

Def: Eine Ringerw $A \subset B$ heißt endlich, falls B ein endliches (d.h. endl. erzeugtes) A-Modul ist.

- $A \subset B$ heißt von endl. Typ, falls B als A-Algebra endl erz. ist, d.h. falls es einen surj Ringhom gibt

$$A[x_1, \dots, x_n] \longrightarrow B,$$

so dass das Dreieck kommutiert (für $c \in A$ gegeben).

Bsp:
- Endl Körper-Erw $K \subset L$ ist endl Ringerw.
- $\mathbb{Z} \subset \mathbb{Z}[i]$ ist endl Ringerw.
- $\mathbb{Z} \subset \mathbb{Z}[x]$ " nicht endl, aber von endl. Typ.

Lemma 1: Sei $A \subset B$ Ring-Erw. und $b \in B$. Es sind äqu.:

i) Es ex. ganze Gl von b über A, d.h. ein normiertes Pol $f \in A[x]$ mit $f(b) = 0$.

ii) Der Unterring $A[b] \subset B$ ist endl. A-Modul

iii) Es ex endl. A-Untermodul $M = \sum_{i=1}^{n} A m_i$ von B mit $1 \in M$ und $bM \subset M$.

Bew: i $\Rightarrow$ ii:

Sei $f(X) = X^n + a_{n-1}X^{n-1} + \dots + a_0 \in A[X]$ mit $f(\zeta) = 0$.

$\Rightarrow \zeta^n = -a_{n-1}\zeta^{n-1} - \dots - a_1\zeta - a_0 \in \sum_{i=0}^{n-1} A\zeta^i =: M$

Ind.
$\Rightarrow \zeta^i \in M \quad \forall i \in \mathbb{N}_0$

$\Rightarrow A[\zeta] \subset M$

$\Rightarrow A[\zeta] = M$

Rest $\Rightarrow$ ii.

<u>ii $\Rightarrow$ iii</u> : trivial.

<u>iii $\Rightarrow$ i</u> : Sei $M = \sum_{i=1}^{n} Am_i \subset B$ endl. Untermodul mit $1 \in M$ u. $\zeta M \subset M$.

$\rightarrow$
$$\begin{aligned} \zeta m_1 &= a_{11}m_1 + \dots + a_{1n}m_n \\ &\vdots \qquad\qquad \vdots \\ \zeta m_n &= a_{n1}m_1 + \dots + a_{nn}m_n \end{aligned}$$

mit Koeff $a_{ij} \in A$.

$\Rightarrow \quad \Delta \cdot \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = 0$

wobei $\Delta = (\zeta\delta_{ij} - a_{ij})_{i,j} \in B^{n \times n}$.

LA $\Rightarrow$ Sei Δ^* die zu Δ adjungierte Matrix $(\Delta^*_{ij} = (-1)^{i+j}\det(\Delta^{ij}))$

Dann ist $\Delta^*\Delta = (\det\Delta)\cdot E$

(In LA beweist man dies über Körpern, gilt aber auch über Ringen.)

$$\Rightarrow (\det\Delta)\cdot\begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix} = \Delta^*\Delta\begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix} = 0$$

$1\in M$
$\Rightarrow \det\Delta = 0$

$\Rightarrow \det(X\cdot\delta_{ij} - a_{ij}) \in A[X]$
ist normierter Pol, welches b als Nullstelle hat. □

Def: · Sei $A\subset B$ Ringerw. Ein El $b\in B$ heißt ganz über A, wenn b die äqu. Bed. von Lemma 1 erfüllt.
· Die Ringerw $A\subset B$ heißt ganz, falls jedes $b\in B$ ganz über A ist.

Bem 2: Jede endl. Ringerw. $A\subset B$ ist ganz.

Bew: Lemma 1. □

Bem 3)

Bem 4: Sei $A\subset B$ Ringerw. vom endl. Typ, d.h. $B = A[b_1,\dots,b_n]$, mit $b_1,\dots,b_n\in B$. Sind die b_i ganz über A, so ist $A\subset B$ endl. (und damit ganz).

Bew: Betr. die Kette von Ringerw.

$$A\subset A[b_1]\subset A[b_1,b_2]\subset\dots\subset A[b_1,\dots,b_n]=B.$$

Lem 1 (ii) $\Rightarrow$ Jede Teilerw ist endl.
Bem 3 $\Rightarrow$ $A\subset B$ endl □

Bem 3: Sind $A \subset B$, $B \subset C$ endl. Ring-erw., so auch $A \subset C$.

Bew: Ist $B = \sum_{i=1}^{m} A b_i$ und $C = \sum_{j=1}^{n} B c_j$, so ist $C = \sum_{i=1}^{m} \sum_{j=1}^{n} A b_i c_j$. $\square$

Bem 5: Sind $A \subset B$, $B \subset C$ ganze Ring-erw., so auch $A \subset C$.

Bew: Sei $c \in C$.

c ganz/B $\Rightarrow$ $\exists\, f \in B[X]$ normiert mit $f(c) = 0$.

Ist $f = X^n + b_{n-1} X^{n-1} + \ldots + b_0$, so ist c ganz über $A[b_0, \ldots, b_{n-1}] \subset B$.

Bem 4 $\overset{A \subset B \text{ ganz}}{\Rightarrow}$ $A[b_0, \ldots, b_{n-1}]$ ist endl. über A

Bem 3 $\Rightarrow$ $A[b_0, \ldots, b_{n-1}, c]$ " " " A.

$\Rightarrow$ " " " ganz " A.

$\Rightarrow$ c ganz über A. $\square$

Def: Sei $A \subset B$ Ringerw. Die Menge

$$\bar{A} = \{ b \in B;\ b \text{ ganz über } A \}$$

heißt ganzer Abschluss von A in B.

A heißt ganz abgeschlossen in B, falls $\bar{A} = A$.

Bem 6: i) $\bar{A} \subset B$ Unterring.

ii) $\overline{\bar{A}} = \bar{A}$.

Bew: i) Seien $b_1, b_2 \in \bar{A}$.

$\overset{\text{Bem 4}}{\Rightarrow} A \subset A[b_1, b_2]$ ist endl.

$\overset{\text{Bem 2}}{\Rightarrow}$ " " ganz

$\Rightarrow b_1 \pm b_2,\ b_1 \cdot b_2 \in \bar{A}$.

ii) $b \in B$ ganz über $\bar{A}$ $\Rightarrow \bar{A} \subset \bar{A}[b]$ ganz

$\overset{A \subset \bar{A} \text{ ganz}}{\Rightarrow} A \subset \bar{A}[b]$ ganz

$\Rightarrow b$ ganz über A. □

Kor 7: $\Sigma = \{a \in \mathbb{C};\ a \text{ ganz alg über } \mathbb{Z}\}$

$= \bar{\mathbb{Z}} \subset \mathbb{C}$ ist Unterring.

Def: Sei A Integritätsring mit Quot.kp K.
Der ganze Abschluss $\bar{A}$ von A in K
heißt Normalisierung von A.
A heißt ganz abgeschlossen (g.a.)
falls $A = \bar{A}$.

Bsp: Jeder faktorielle Ring ist g.a.

Bew: Übung.

Satz 8: Sei A g.a. IR mit $K = \mathrm{Quot}(A)$ und sei L/K separable Körpererw.
Sei $\beta \in L$ mit Mipo $f \in K[X]$.
Es ist β ganz über $A \Leftrightarrow f \in A[X]$.

Bew: „$\Leftarrow$": klar.

„$\Rightarrow$": Sei $g \in A[X]$ normierter Pol mit $g(\beta) = 0$

$\Rightarrow f \mid g$ in $K[X]$.

Sei $\bar{L}$ alg Abschluss von L.
Alle Nullst von g in $\bar{L}$ sind ganz $/A$
$\overset{f|g}{\Rightarrow}$ " " $\beta_1, \ldots, \beta_n$ " f " " " "

$\overset{f \text{ normiert}}{\Rightarrow}$ $f(X) = (X - \beta_1) \cdot \ldots \cdot (X - \beta_n)$.

Koeff von f sind el.-symm. Pol in $\beta_1, \ldots, \beta_n$ $\Rightarrow$ ganz $/A$
$\overset{A \text{ g.a.}}{\Rightarrow}$ $f \in A[X]$. $\square$

Bem 9: $\Omega \subset \mathbb{C}$ ist g.a. mit $\mathrm{Quot}\,\Omega = \overline{\mathbb{Q}}$.

Ende der Vorlesung?

§3 Norm und Spur (Erinnerung)

Sei L/K endl. Körpererw.

Sei $x \in L$ bel. Dann ist K-VR-Hom

$$T_x : L \to L, \quad T_x(\lambda) = x\lambda.$$

Man definiert

$$\mathrm{Tr}_{L/K}(x) := \mathrm{Tr}(T_x) \quad \text{„Spur von } x\text{"}$$

$$N_{L/K}(x) := \det(T_x) \quad \text{„Norm von } x\text{"}$$

- $\mathrm{Tr}_{L/K} : L \to K$ ist K-Lin Abb.
- $N_{L/K} : L^\times \to K^\times$ ist Gruppenhom.
- Sei $f_x(t) = \det(t \cdot \mathrm{id} - T_x)$
$$= t^n + a_{n-1} t^{n-1} + \dots + a_1 t + a_0 \in K[t]$$
das char. Pol von T_x.

Dann gilt

$$\mathrm{Tr}_{L/K}(x) = -a_{n-1}$$

$$N_{L/K}(x) = (-1)^n a_0.$$

Satz 1: Sei $\{\sigma_1, \dots, \sigma_n\} = \mathrm{Hom}_K(L, \bar{K})$ die K-Hom von L in einen alg. Abschluss $\bar{K}$ von K.

Dann gilt

i) $$f_x(t) = \prod_{i=1}^{n} (t - \sigma_i(x))$$

ii) $$\mathrm{Tr}_{L/K}(x) = \sum_{i=1}^{n} \sigma_i(x)$$

iii) $$N_{L/K}(x) = \prod_{i=1}^{n} \sigma_i(x).$$

Satz: Algebra. □

Satz 2: Sei A g.a. Ist mit $\mathrm{Quot}A = K$ auch L/K endl. Erw.
Satz. Ist $x \in L$ ganz über A,
so ist $N_{L/K}(x) \in A$ und
$N_{L/K}(x) \in A$.

Satz: Ω, Satz $\Rightarrow p(t) :=$ Kgv von x
über K mit $\in A[t]$.
Für alle $\sigma \in \mathrm{Hom}_K(L, \bar{K})$ ist
$\sigma(x)$ Nullst von $p(t)$.
$\Rightarrow \sigma(x)$ ganz über A.
$\Rightarrow$ Satz $N_{L/K}(x)$, $\mathrm{Sp}_{L/K}(x)$ ganz über A.
A g.a.
$N_{L/K}(x)$, $\mathrm{Sp}_{L/K}(x) \in A$. □

Satz 3: Seien $K \subset L \subset \Omega$ endl. Körpererw.
Es gilt für $x \in \Omega$
$N_{L/K}(N_{M/L}(x)) = N_{M/K}(x)$
$N_{L/K}(N_{M/L}(x)) = N_{M/K}(x)$.

Satz: Algebra. □

Satz: Quadratische Zahlkörper
Sei $d \in \mathbb{Z}$ quadratfrei, $d \neq 0, 1$.
$K = \mathbb{Q}(\sqrt{d})$ ist Erw vom Grad 2.
Sei $\alpha = a + b\sqrt{d} \in K$.

$\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = 2a$, $N_{K/\mathbb{Q}}(\alpha) = a^2 - 5b^2$

$\mathrm{Pol}_\alpha(t) = t^2 - \mathrm{Tr}(\alpha)\,t + N(\alpha)$

$= t^2 - 2a \cdot t + (a^2 - 5b^2)$

Sei $\mathcal{O}_K$ = Ring der ganz ab. Z. in K

= ganzer Abschluss von $\mathbb{Z}$ in K

Satz: $\alpha \in \mathcal{O}_K \Leftrightarrow \mathrm{Pol}_\alpha \in \mathbb{Z}[t]$

$\Leftrightarrow$ i) $2a \in \mathbb{Z}$ und ii) $a^2 - 5b^2 \in \mathbb{Z}$.

i) $\Leftrightarrow a = \frac{1}{2}a'$, $a' \in \mathbb{Z}$

in ii) $a'^2 - 5b^2 \in 4\mathbb{Z}$

$\Rightarrow 5b^2 \in \mathbb{Z}$

$\Rightarrow 5b \in \mathbb{Z}$

$\Rightarrow b = \frac{1}{5}b'$, $b' \in \mathbb{Z}$

$\Rightarrow$ ii) $a'^2 - 5b'^2 \in 4\mathbb{Z}$

Ein Quadrat ist kongruent $\equiv 0, 1 \pmod 4$.

a) Falls $a' \equiv 0, 2 \pmod 4$:

Einsetzen $a'^2 \equiv 5b'^2 \pmod 4$

Nur möglich falls $a', b' \equiv 0 \pmod 4$

$\Rightarrow a = b' \equiv 0 \pmod 2$

$\Rightarrow a, b \in \mathbb{Z}$

$\Rightarrow \mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\sqrt{5}$

b) $a' \equiv 1 \pmod 4$

Einsetzen $a'^2 \equiv b'^2 \pmod 4$

$\Leftrightarrow a' \equiv b' \pmod 2$

$\Rightarrow \mathcal{O}_K = \mathbb{Z} + \frac{1+\sqrt{5}}{2}\mathbb{Z}$.

§ 4 Die Diskriminante

Sei L/K sep. vom Grad n, $\mathrm{Hom}_K(L,\bar{K}) = \{\sigma_1, \dots, \sigma_n\}$

Def: Die Diskriminante eines n-Tupels $(\alpha_1, \dots, \alpha_n)$ von El. von L ist def als

$$d(\alpha_1, \dots, \alpha_n) = \det\left((\sigma_i \alpha_j)_{i,j}\right)^2$$

Satz 1: Es gilt

$$d(\alpha_1, \dots, \alpha_n) = \det\left((\mathrm{Tr}_{L/K}(\alpha_i \alpha_j))_{i,j}\right)$$

Satz: Es ist

$$\mathrm{Tr}_{L/K}(\alpha_i \alpha_j) = \sum_{\tau=1}^{n} \sigma_\tau(\alpha_i) \cdot \sigma_\tau(\alpha_j).$$

Dies ist der (i,j)-Eintrag der Matrix, die man als Produkt von

$$(\sigma_k \alpha_i)^t \quad \text{und} \quad (\sigma_k \alpha_j)$$

erhält.

$$\Rightarrow \det\left(\mathrm{Tr}_{L/K}(\alpha_i \alpha_j)\right)_{i,j} = \det(\sigma_k \alpha_i)^t \det(\sigma_k \alpha_j)$$

$$= d(\alpha_1, \dots, \alpha_n). \quad \square$$

Bem 2: Sei $\Theta \in L$ prim. El von L/K, so dass $1, \Theta, \dots, \Theta^{n-1}$ Basis von L ist. Es sei

$$d(1, \Theta, \dots, \Theta^{n-1}) = \prod_{i<j} (\Theta_i - \Theta_j)^2 = \pm N_{L/K} f'(\Theta),$$

wobei $\Theta_i = \sigma_i(\Theta)$ und f = Kpia von Θ/K.

Bem:

$$(\sigma_i \Theta^{j-1})_{i,j=1,\dots,n} = \begin{pmatrix} 1 & \Theta_1 & \Theta_1^2 & \cdots & \Theta_1^{n-1} \\ \vdots & & & & \vdots \\ 1 & \Theta_n & \Theta_n^2 & \cdots & \Theta_n^{n-1} \end{pmatrix}$$

Dies ist eine Vandermonde-Matrix, deren Det man in LA 1 berechnet

=> erste Gleichung.

Für die zweite Gl. beachte

$$\prod_{i<j} (\theta_i - \theta_j)^2 = \pm \prod_{i \neq j} (\theta_i - \theta_j)$$

und

$$N_{L|K}\, f'(\theta) = \prod_{i=1}^{n} \sigma_i(f'(\theta))$$

$f \in K[x]$

$$= \prod_{i=1}^{n} f'(\sigma_i(\theta))$$

$$= \prod_{i=1}^{n} \underbrace{f'(\theta_i)}_{\prod_{j=1, j\neq i}^{n} (\theta_i - \theta_j)}$$

$$= \pm \prod_{i \neq j} (\theta_i - \theta_j) \,. \qquad \square$$

Bem.: in der 2. Gl. vom Satz 2 gilt das "+" Zeichen <=> $n \equiv 0,1\ (4)$.

Satz 3: i) Für $\alpha_1, \dots, \alpha_n \in L$ ist

$d(\alpha_1, \dots, \alpha_n) \neq 0$ <=> $\alpha_1, \dots, \alpha_n$ eine K-VR Basis von L.

ii) $(x,y) = Tr_{L|K}(xy)$ ist eine n.a. K-Bilinearform auf L.

Bew.: ii) $Tr(xy)$ n.a.:

Sei $\theta \in L$ prim. El. $1, \theta, \dots, \theta^{n-1}$

ist K-VR Basis von L. Gleichzeitig das

die Bil-Form der Gram-Matrix (23)

$$M = \left(\mathrm{Tr}_{L|K}(\theta^{i-1}\theta^{j-1})\right)_{i,j}$$

hat.

Die $\theta_i = \sigma_i \theta \in L$ sind paarw. versch. (da $L|K$ sep und θ primit. El).

$\Rightarrow \det M = d(1, \theta, \ldots, \theta^{n-1}) = \prod_{i<j} (\theta_i - \theta_j)^2 \neq 0.$

$\Rightarrow$ Bil-Form ist n.a.

(ii) Ist $\alpha_1, \ldots, \alpha_n$ bel. Basis von $L|K$, so ist die Gram-Det

$$\det\left(\mathrm{Tr}_{L|K}(\alpha_i \alpha_j)\right)_{i,j} = d(\alpha_1, \ldots, \alpha_n)$$

$\|$

$s^2 \cdot \det M$ mit $s \in K^*$.

$\Rightarrow d(\alpha_1, \ldots, \alpha_n) \neq 0.$

Sind $\alpha_1, \ldots, \alpha_n$ K-lin. abh., so sieht man leicht $d(\alpha_1, \ldots, \alpha_n) = 0$. □

Sei A g.a. IR mit $K = \mathrm{Quot}(A)$, und $L|K$ endl. sep. Erw. und $B \subset L$ der ganze Abschluss von A in L.

$$\begin{array}{ccc} B & \subset & L \\ | & & | \\ B \cap K = A & \subset & K \end{array}$$

(A g.a.)

Bsp:

$$\begin{array}{ccc} \mathcal{O}_L & \subset & L \\ | & & | \\ \mathbb{Z} & \subset & \mathbb{Q} \end{array}$$

Lemma 4:
Sei $\alpha_1, \dots, \alpha_n$ Basis von L/K mit $\alpha_i \in \mathfrak{o}_L$, und sei $d = d(\alpha_1, \dots, \alpha_n)$. Dann gilt

$$d\mathfrak{o}_L \subseteq A\alpha_1 + \dots + A\alpha_n \qquad (\subseteq \mathfrak{o}_L)$$

Beweis: Sei $\alpha = c_1\alpha_1 + \dots + c_n\alpha_n \in \mathfrak{o}_L$ mit Koeff. $c_i \in K$.
Dann gilt für $i = 1, \dots, n$

$$\alpha_i \alpha = c_1 \alpha_i \alpha_1 + \dots + c_n \alpha_i \alpha_n$$

$$\Rightarrow \quad \mathrm{Tr}_{L/K}(\alpha_i \alpha) = c_1 \mathrm{Tr}_{L/K}(\alpha_i \alpha_1) + \dots + c_n \mathrm{Tr}_{L/K}(\alpha_i \alpha_n)$$

$$\Rightarrow \quad \underbrace{\begin{pmatrix} \mathrm{Tr}_{L/K}(\alpha_1 \alpha) \\ \vdots \\ \mathrm{Tr}_{L/K}(\alpha_n \alpha) \end{pmatrix}}_{=: v \in A^n} = \underbrace{\left(\mathrm{Tr}_{L/K}(\alpha_i \alpha_j)\right)_{ij}}_{=: \Delta \in A^{n \times n}} \cdot \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix}$$

$$\Rightarrow \det(\Delta) \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} = \Delta^* \Delta \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} = \Delta^* \cdot v$$

$$d = \det(\Delta) \Rightarrow d \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} = \underbrace{\Delta^* \cdot v}_{\in A^n}$$

$$\Rightarrow d c_i \in A \qquad \forall\, i = 1, \dots, n.$$

$$\Rightarrow d\alpha = dc_1\alpha_1 + \dots + dc_n\alpha_n \in A\alpha_1 + \dots + A\alpha_n.$$

□

Eine Basis wie in Lemma 4 ex. immer wegen

Lemma 5: Sei $\alpha \in L$, α ganz, $N \in A$ mit $N\alpha \in \mathfrak{o}_L$.

Beweis: Sei $f = X^n + a_{n-1}X^{n-1} + \dots + a_0 \in K[X]$ das Polynom von α über K.
Schreibe $a_i = \frac{p_i}{q_i}$ mit $p_i, q_i \in A$.

Sei $N := q_{n-1} \cdot \dots \cdot q_0 \in A$.

Es gilt $N^n \cdot f(\alpha) = 0$

$$\Rightarrow (\alpha N)^n + \underbrace{N a_{n-1}}_{\in A}(\alpha N)^{n-1} + \dots + \underbrace{N^{n-1} a_1}_{\in A}(\alpha N) + \underbrace{N^n a_0}_{\in A} = 0$$

$\Rightarrow \alpha N$ ist ganz über A. □

Def: Ein n-Tupel $(w_1, \dots, w_n) \in B^n$ heißt ganze Basis von B über A (oder A-Basis von B), falls man jedes $b \in B$ eindeutig als Linearkombination
$$b = a_1 w_1 + \dots + a_n w_n$$
mit Koeff. $a_i \in A$ schreiben kann.

Bem 6: Hat ein A-Modul B eine K-VR-Basis $\omega_1, \dots, \omega_n$ ($K = \mathrm{Quot}(A)$)
$\Rightarrow n = [L:K]$.

- L.U. ist A-Modul.
- Sie existieren nicht, falls A kein HIR.

Satz 7: Seien A, B, K, L wie oben. Zusätzlich sei A ein HIR.
Jeder endl. erz. B-Untermodul $\neq 0$ von L ist ein freier A-Modul vom Rang $[L:K]$.
Insbesondere hat B eine A-Basis.

Bew: Sei $\alpha_1, \dots, \alpha_n$ Basis von L/K.
Bem. 5 $\Rightarrow \exists\, d \in A$ $d\alpha_i \in B$.
Lem. 4 $\Rightarrow$ $dB \subset A\alpha_1 + \dots + A\alpha_n =: M_0$ mit $d = d(\alpha_1, \dots, \alpha_n)$ ← freier A-Mod, rang n
$\Rightarrow \operatorname{rang}_A(B) = \dim_K(B \otimes_A K) \leq n = [L:K]$.

Erzeugendensystem des A-Moduls B ist auch Erz-Syst. des K-VR L
$\Rightarrow \operatorname{rang}_A(B) \geq n$
$\Rightarrow \operatorname{rang}_A(B) = n = [L:K]$.

Sei $\mu_1, \dots, \mu_r$ Erz-Syst. des B-Moduls M, d.h. $M = \sum_{i=1}^{r} B\mu_i$.
Sei $a \in A$, $a \neq 0$ mit $a\mu_i \in B$ $\forall i$
$\Rightarrow aM \subset B$
$\Rightarrow adM \subset dB \subset A\alpha_1 + \dots + A\alpha_n = M_0$.

Hauptsatz für endl. erz. Moduln über Hauptidealringen impliziert, dass endl. erz. Untermod. eines freien Moduls frei ist.
(Dies ist Verallg. des HS über endl. erz. ab. Gruppen = $\mathbb{Z}$-Moduln.)

M_0 ist freier A Modul, rang n
$\Rightarrow adM$ ist frei
$\Rightarrow M$ " "

Es gilt
$[L:K] = \operatorname{rang} B \leq \operatorname{rang} M = \operatorname{rang} adM \leq \operatorname{rang} M_0 = [L:K]$.
$\Rightarrow \operatorname{rang} M = [L:K]$. □

(Fortsetzung Kap 8)

Kor 8: Sei $L/\mathbb{Q}$ Zahlkp.
vom Grad n, $\mathcal{O}_L$ = Ring der ganzen alg. Zahlen in L, $L = L/\mathbb{R}$.
Dann besitzt $\mathcal{O}_L$ eine $\mathbb{Z}$-Basis $\omega_1, \dots, \omega_n$ mit $n = [L:\mathbb{Q}]$.

Bem: Satz 7 mit $R = \mathbb{Z}$, $K = \mathbb{Q}$, $S = \mathcal{O}_L$.

Allgemein: Sei $\alpha \in L$ stets ein $\mathcal{O}_L$-Vielfaches einer $\mathbb{Q}$-Basis von L (z.B. eine Basis von $\mathcal{O}_L$). Dann hat $\mathcal{O}_L$ eine $\mathbb{Z}$-Basis $\omega_1, \dots, \omega_n$,
$\alpha\mathcal{O}_L = \mathbb{Z}\omega_1 + \dots + \mathbb{Z}\omega_n$.

Die Diskriminante
$$d(\omega_1, \dots, \omega_n) = \det((\sigma_i \omega_j))^2$$
ist unabh. von der Wahl der $\mathbb{Z}$-Basis:
Ist $\omega_1', \dots, \omega_n'$ eine zweite $\mathbb{Z}$-Basis, so hat die Basiswechselmatrix $T \in \mathbb{Z}^{n\times n}$ stets ± 1 ganze Koeff.
$\Rightarrow \det T = \pm 1$.

$\Rightarrow d(\omega_1', \dots, \omega_n') = \det(T)^2 d(\omega_1, \dots, \omega_n)$.

Def: Die Diskriminante von α $d(\alpha) := d(\omega_1, \dots, \omega_n)$ ist unabh. von der Wahl der $\mathbb{Z}$-Basis.

Die Diskriminante von L ist def. als
$$d_L = d(\mathcal{O}_L) = d(\omega_1, \dots, \omega_n).$$

Bsp: $L = \mathbb{Q}(\sqrt{d})$, $d \in \mathbb{Z} \setminus \{0,1\}$ q-frei.

$$\mathcal{O}_L = \begin{cases} \mathbb{Z} + \mathbb{Z}\sqrt{d}, & d \not\equiv 1 \ (4) \\ \mathbb{Z} + \mathbb{Z}\frac{1+\sqrt{d}}{2}, & d \equiv 1 \ (4) \end{cases}$$

$$d_L = \begin{cases} \det\begin{pmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{pmatrix}^2 = (-\sqrt{d}-\sqrt{d})^2 = 4d, & d \not\equiv 1 (4) \\ \det\begin{pmatrix} 1 & \frac{1+\sqrt{d}}{2} \\ 1 & \frac{1-\sqrt{d}}{2} \end{pmatrix}^2 = \left(\frac{1-\sqrt{d}}{2} - \frac{1+\sqrt{d}}{2}\right)^2 = d, & d \equiv 1 (4). \end{cases}$$

<u>Lemma 9</u>: Seien $\mathfrak{a} \subset \mathfrak{a}'$ zwei endl. erz. $\mathcal{O}_L$-Untermod. von L. Dann ist $[\mathfrak{a}' : \mathfrak{a}] < \infty$ und

$$d(\mathfrak{a}) = [\mathfrak{a}' : \mathfrak{a}]^2 \, d(\mathfrak{a}') .$$

<u>Bew</u>: Folgt aus HS über endl. erz. ab. Gr. □

Genauso zeigt man:

<u>Lemma 10</u>:
Ein n-Tupel $\alpha_1, \dots, \alpha_n \in \mathcal{O}_L$ ist eine $\mathbb{Z}$-Basis von $\mathcal{O}_L$ $\Longleftrightarrow$ $d(\alpha_1, \dots, \alpha_n) = d(\mathcal{O}_L)$.

→ Vl. §3, → Vorz. Bew.