# Algebraische Zahlentheorie

## Algebra B IV

- Kuhlmann -

SS 2013 / 14

15. Vorlesung am 13.06.2013.

---

**Beweis** (Satz von Stickelberger)

**Erinnerung** (ÜB 7 Auf. 7.1)

Sei $L/K$ endl. separable; $\{\mu_1, \dots, \mu_n\}$ eine Basis; $[L:K] = n$

$\sigma_1, \dots, \sigma_n$ die verschiedene Einbettungen von $L$ über $K$ in $\Omega$; dann gilt

$$\det\left(B_{L/K}(\mu_i, \mu_j)\right) = \left(\det\left(\sigma_i(\mu_j)\right)\right)^2 \in \mathbb{Z}$$
$$\neq 0$$

Sei nun $\{\mu_1, \dots, \mu_n\}$ eine Ganzheitsbasis von $\mathcal{O}_L$ über $\mathbb{Z}$; es ist

$$D(\mathcal{O}_L/\mathbb{Z}) = \left[\sum_{\pi \in S_n} (\operatorname{sign} \pi)\, \sigma_{\pi(1)}(\mu_1) \cdots \sigma_{\pi(n)}(\mu_n)\right]^2$$

$$= \left[ \left( \sum_{\pi \in A_n} \operatorname{sign} \pi \cdots \right) + \left( \sum_{\pi \in S_n \setminus A_n} \operatorname{sign} \pi \right) \right]^2$$

$$= (G - U)^2 \in \mathbb{Z}$$

wobei

$$G_i = \left( \sum_{\pi \in A_n} \cdots \right) \in \mathcal{O}_L \subseteq \Omega \quad \text{und}$$

$$U := -\left( \sum_{\pi \in S_n \setminus A_n} \cdots \right) \in \mathcal{O}_L \subseteq \Omega$$

Nun ist $L \subseteq \Omega$ Galois. Für $\tau \in \mathrm{Gal}(\Omega/\mathbb{Q})$

**Bemerkung:** $\sigma_1, \ldots, \sigma_n : L \hookrightarrow \Omega$ ; sei $i \in \{1, \ldots, n\}$:

$$L \xrightarrow{\sigma_i} \Omega \xrightarrow{\tau} \Omega \quad \text{also } \exists\, j \in \{1, \ldots, n\}$$

so daß $\tau \circ \sigma_i = \sigma_j$

Also ist die Abbildung

$$\rho : i \longmapsto j \qquad (\rho(i) = j \Leftrightarrow \tau \circ \sigma_i = \sigma_j)$$

eine Permutation; i.e $\rho \in S_n$.

Wir berechnen:

$$\tau\left(\sigma_{\pi(1)}(\mu_1)\cdots\sigma_{\pi(n)}(\mu_n)\right) =$$

$$\tau\circ\sigma_{\pi(1)}(\mu_1)\cdots\tau\circ\sigma_{\pi(n)}(\mu_n) =$$

$$\sigma_{(\rho\circ\pi)(1)}(\mu_1)\cdots\sigma_{(\rho\circ\pi)(n)}(\mu_n) .$$

Daraus folgt:

$$\rho\in A_n \Rightarrow \begin{matrix}\tau(G)=G\\ \tau(U)=U\end{matrix}$$

und

$$\rho\in S_n\setminus A_n \Rightarrow \begin{matrix}\tau(G)=U\\ \tau(U)=G\end{matrix}$$

und somit ist

$$\tau(G+U)=G+U \quad \text{und} \quad \tau(G\cdot U)=G\cdot U$$

$$\forall\ \tau\in \mathrm{Gal}(\Omega/\mathbb{Q}).$$

Nun $\Omega/\mathbb{Q}$ Galois $\Rightarrow G+U,\ G\cdot U\in$

$$\mathrm{Inv}\ \mathrm{Gal}(\Omega/\mathbb{Q}) = \mathbb{Q}$$

FSGT

(B III Satz 08 25. Vor. 04.02.2013)

Also $G+U,\ G\cdot U\in\mathbb{Q}$ und $\mathbb{Z}$ ganz abgeschlossen $\Rightarrow$

$G+U,\ G\cdot U \in \mathbb{Z}$. Also ist

$$D(\mathcal{O}_L/\mathbb{Z}) = (G-U)^2 = \underbrace{(G+U)^2}_{\in \mathbb{Z}} - \underbrace{4GU}_{\in 4\mathbb{Z}}$$

$\Rightarrow (G-U)^2 \equiv (G+U)^2 \bmod 4$ in $\mathbb{Z}$. ∎

**Definition**: Sei $L/\mathbb{Q}$ ein Zahlkörper

Eine Einbettung von $L$ in $\mathbb{C}$ ist **reell**

wenn ihr Bild in $\mathbb{R}$ liegt, sonst **komplex**.

**Bemerkung:** Setze $L := \mathbb{Q}(\alpha)$ $[L:\mathbb{Q}] = n$

$f := \operatorname{Min Pol}_{\mathbb{Q}} \alpha$ $f = \prod(x-\alpha_i) \in \mathbb{C}[x]$

mit $r$ reellen NS und $2S$ komplexen NS

so daß $r+2S = n$; dann hat $L$ genaus

$r$ reelle Einbettungen in $\mathbb{C}$ und
$2S$ komplexe " " "

**Satz von Brill** sign $D(\mathcal{O}_L/\mathbb{Z}) = (-1)^S$
(Ansatz wie oben)

**Beweis**. Sei $\{\alpha_1, \dots, \alpha_n\} \subseteq \mathcal{O}_L$ Basis für $L/\mathbb{Q}$
(es ist immer möglich solch eine Basis zu finden)
(e.g. $\alpha$ primitives element $\in \mathcal{O}_L$ und $\alpha_i := \alpha^i$ )

und es ist

$$D(\alpha_1, \dots, \alpha_n) = (\det P)^2 \, D(\mathcal{O}_L / \mathbb{Z})$$

[ $P \in M_{n \times n}(\mathbb{Z})$ nicht

unbedingt invertierbar ! ]

Insbesondere

$$\operatorname{Sign}(D(\alpha_1, \dots, \alpha_n)) = \operatorname{Sign} D(\mathcal{O}_L / \mathbb{Z}) .$$

Wir berechnen nun $\operatorname{Sign} D(1, \alpha, \dots, \alpha^{n-1})$

i.e wir berechnen $\operatorname{Sign} D(f)$ wobei

$f := \operatorname{Min} \operatorname{Pol}_{\mathbb{Q}} \alpha$

Seien $\beta_1, \dots, \beta_r, z_1, \dots, z_s, \bar{z}_1, \dots, \bar{z}_s$

alle NS von $f$ in $\mathbb{C}$

$$f = \prod (x - \alpha_i) = \prod_r (x - \beta_j) \prod_s (x - z_k) \prod_s (x - \bar{z}_k)$$

$\Rightarrow$ Def. 14. Vor

$$D(f) = \prod_{i<j} (\beta_i - \beta_j)^2 \prod_{i,k} (\beta_i - z_k)^2 \prod_{i,k} (\beta_i - \bar{z}_k)^2$$

$$\prod_{k<\ell} (z_k - z_\ell)^2 \prod_{k,\ell} (z_k - \bar{z}_\ell)^2 \prod_{k<\ell} (\bar{z}_k - \bar{z}_\ell)^2$$

15. Vor.  12.01.2006

sign $D(f)$ ? Bezeichnung: $\mathbb{R}_+ = \mathbb{R}^{>0}$ ; $\mathbb{R}_- := \mathbb{R}^{<0}$

Nun ist $\prod_{i<j} (\beta_i - \beta_j)^2 \in \mathbb{R}^2 > 0$

$(\beta_i \neq \beta_j)$

$\underbrace{\prod_{i,k} (\beta_i - z_k)^2 \prod_{i,k} (\beta_i - \bar{z}_k)^2}_{:= w \bar{w}} = w\bar{w} \in \mathbb{R}_+$

Analog für

$\prod_{k<\ell} (z_k - z_\ell)^2 \prod_{k<\ell} (\bar{z}_k - \bar{z}_\ell)^2 \in \mathbb{R}_+$.

Also bleibt $\prod_{k,\ell} (z_k - \bar{z}_\ell)^2$ übrig

Zu behandeln:

ist $k \neq \ell$ dann erscheinen die Faktoren

$z_k - \bar{z}_\ell$ sowie $z_\ell - \bar{z}_k$ im Produkt

also $(z_k - \bar{z}_\ell)^2 (z_\ell - \bar{z}_k)^2 =$

$\Big[ \underbrace{-(z_k - \bar{z}_\ell)(\bar{z}_k - z_\ell)}_{\in \mathbb{R}+} \Big]^2 \in \mathbb{R}_+$

Letztendlich ist also $\operatorname{sign}\left(D(1, \alpha, \ldots, \alpha^{n-1})\right) =$

$\operatorname{sign}\left(\prod_{k=1}^{s} (z_k - \bar{z}_k)^2\right)$.

Aber $z_k - \bar{z}_k \in i\mathbb{R}$ also ist

$(z_k - \bar{z}_k)^2 \in \mathbb{R}_-$ also ist

Produkt von $s$ negative reelle Zahlen;

und damit ist sein Zeichen $(-1)^s$. ∎

<u>Proposition</u> Sei $L/K$ endlich separabel,

($\sigma_1, \ldots, \sigma_n$ die Einbettungen von $L$ über $K$ in $\Omega$)

$\alpha$ Primitives element; $f := \operatorname{Min Pol}_{\mathbb{Q}} \alpha$;

($\alpha_1, \ldots, \alpha_n$ die verschiedene NS von $f$).

Es ist $D(f) = (-1)^{\frac{n(n-1)}{2}} N_{L/K}(f'(\alpha))$

<u>Beweis.</u> $f = \prod (x - \alpha_i) \Rightarrow$

$$f' = \sum_{\lambda=1}^{n} \left( \prod_{j \neq i} (x - \alpha_j) \right) \quad (\dagger\dagger)$$

Anderseits (per Definition der $N_{L/K}$) haben wir

$$N_{L/K}(f'(\alpha)) = \prod_{k=1}^{n} \sigma_k(f'(\alpha)) = \prod_{k=1}^{n} [f'(\sigma_k(\alpha))]$$

$$= \prod_{k=1}^{n} f'(\alpha_k) \,.$$

Einsetzen von $\alpha_k$ in (††) ergibt

$$f'(\alpha_k) = \prod_{\substack{j \neq k \\ j,k : 1,\dots,n}} (\alpha_k - \alpha_j)$$

Also ist

$$N_{L/K}(f'(\alpha)) = \prod_{k=1}^{n} \prod_{j \neq k} (\alpha_k - \alpha_j)$$

Wir vergleichen nun dieses Produkt mit

$$D(f) = \prod_{j<k} (\alpha_k - \alpha_j)^2$$

Hier erscheint jede Differenz $(\alpha_k - \alpha_j)$

zweimal und zwar für $(j,k)$ und $(k,j)$

Wir berechnen nun: für jedes $k = 1,\dots,n$:

$j < k \Rightarrow (\alpha_j - \alpha_k)^2$ erscheint in $D(f)$

dagegen erscheint $\begin{cases} (\alpha_j - \alpha_k)(\alpha_k - \alpha_j) & \text{ein Produkt} \\ = -(\alpha_j - \alpha_k)^2 \end{cases}$

d.h $\underbrace{\forall k = 1, \dots, n \text{ und } j < k}$ wird ein Faktor

$(-1)$ beigetragen, insgesamt also

$(n-1) + (n-2) + \dots + 0$ Beiträge. ∎

---

**Proposition**

**Beispiel:** Sei $f(x) = x^n + ax + b$ irreduzibel.

$\alpha$ NS

$L := \mathbb{Q}(\alpha)$ $\quad [L : \mathbb{Q}] = n$

Setze $\gamma := f'(\alpha) = n\alpha^{n-1} + a$

Wir berechnen $N_{L/\mathbb{Q}}(\gamma)$ (damit wir eine Formel für $D(f)$ bekommen).

Nun erfüllt $\alpha$: $\alpha^n + a\alpha + b = 0$

Multiplizieren mit $\alpha^{-1}$ ergibt

$$\alpha^{n-1} + a + b\alpha^{-1} = 0$$

Also ist $\gamma = -n(a + b\alpha^{-1}) + a$

$= -n(n-1)a - (nb\alpha^{-1})$;

d.h

$$\alpha = \frac{-nb}{\gamma + (n-1)a},$$

und somit ist

$L = \mathbb{Q}(\alpha) = \mathbb{Q}(\gamma)$ und

$[\mathbb{Q}(\gamma) : \mathbb{Q}] = n$

Andererseits ist

$$f\left(\frac{-nb}{x + (n-1)a}\right) = \frac{p(x)}{q(x)} \in \mathbb{Q}(x)$$

so $f(\alpha) = \frac{p(\gamma)}{q(\gamma)} = 0$

und somit ist $p(\gamma) = 0$.

Nun ist aber $p(x) = (x + (n-1)a)^n - na(x + (n-1)a)^{n-1} +$

(direktes Berechnen: $f(Y) = Y^n + aY + b$) $(-1)^n n^n b^{n-1}$

Also ist $p(x)$ normiert; $\deg p = n$ und $p(\gamma) = 0$.

D.h $p(x)$ ist das Min $\mathrm{Pol}_{\mathbb{Q}}\ \gamma$.

Wir berechnen nun (Lemma 2 11. Vor):

$$N_{L/\mathbb{Q}}(\gamma) = (-1)^n \left( \text{Konstanterm von Min Pol}_{\mathbb{Q}}\ \gamma \right)$$

was ist der Konstant Term von $p(x)$?

Wir berechnen:

$$= (n-1)^n a^n - n a (n-1)^{n-1} a^{n-1} + (-1)^n n^n b^{n-1}.$$

So $N_{L/\mathbb{Q}}(\gamma) = n^n b^{n-1} + (-1)^{n-1} (n-1)^{n-1} a^n$

und

$$D(f) = (-1)^{\frac{n(n-1)}{2}} \left( \qquad \right). \quad \square$$

mehrere Beispiele in ÜB 8

---

Beispiel $f(x) = x^3 - x - 1$ ist irreduzibel in $\mathbb{Q}[x]$

Sei $\alpha \in \mathbb{C}$ eine NS; berechne

$$D(1, \alpha, \alpha^2) = D(f) \overset{\text{Prop}}{=} -23$$ ist quadratfrei,

und $\alpha \in \mathcal{O}_L$ (weil $\mathrm{Min\ Pol}_{\mathbb{Q}}\ \alpha = f(x) \in \mathbb{Z}[x]$), also ist $\{1, \alpha, \alpha^2\}$ Ganzheitsbasis von $\mathcal{O}_L$ über $\mathbb{Z}$ und $\mathcal{O}_L = \mathbb{Z}[\alpha]$.