B4: Algebraische Zahlentheorie
Sommersemester 2021
Frau Prof. Dr. Salma Kuhlmann

19.Vorlesung

24. Juni 2021

In diesem Skript werden wir die Sätze von Stickelberger und von Brill beweisen. Wir werden diese Ergebnisse anwenden zur Berechnung der Diskriminante.

Ansatz und Notation wie in Skript 16, 17 und 18.

Erinnerung (Bem. 17.1; ÜB)**:** Sei L/K eine endliche separable Erweiterung, $n = [L : K]$, $\{\mu_1, \dots, \mu_n\}$ eine Basis für L/K, $\sigma_1, \dots, \sigma_n$ die verschiedene Einbettungen von L über K in Ω; dann gilt

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

Beweis von Stickelberger. Sei nun $\{\mu_1, \dots, \mu_n\}$ eine Ganzheitsbasis von $\mathcal{O}_L$ über $\mathbb{Z}$. Nach Definition von $D(\mathcal{O}_L/\mathbb{Z})$ berechnen wir:

$$\begin{aligned} D(\mathcal{O}_L/\mathbb{Z}) &= (\sum_{\pi\in\mathbf{S_n}} (\operatorname{sign}(\pi)\sigma_{\pi(1)}(\mu_1)\dots\sigma_{\pi(n)}(\mu_n)\ )^2 \\ &= (\sum_{\pi\in\mathbf{A_n}} \operatorname{sign}(\pi)\sigma_{\pi(1)}(\mu_1)\dots\sigma_{\pi(n)}(\mu_n) + \sum_{\pi\in\mathbf{S_n}\setminus\mathbf{A_n}} \operatorname{sign}(\pi)\sigma_{\pi(1)}(\mu_1)\dots\sigma_{\pi(n)}(\mu_n)\ )^2 \\ &= (G-U)^2 \in \mathbb{Z} \end{aligned}$$

wobei

$$G := \sum_{\pi\in A_n} \operatorname{sign}(\pi)\sigma_{\pi(1)}(\mu_1)\dots\sigma_{\pi(n)}(\mu_n)$$

und

$$U := -(\sum_{\pi\in S_n\setminus A_n} \operatorname{sign}(\pi)\sigma_{\pi(1)}(\mu_1)\dots\sigma_{\pi(n)}(\mu_n)\ )\,.$$

• Aus den Definitionen folgt daß $G, U \in \mathcal{O}_L$, $\mathcal{O}_L \subseteq \Omega$, $\mathbb{Q} \subseteq L \subseteq \Omega$ ist Galois Erweiterung.

• Sei nun $\tau \in \operatorname{Gal}(\Omega/\mathbb{Q})$. Für jedes $i \in \{1, \dots, n\}$ haben wir die Einbettungen σ_i und $\tau \circ \sigma_i$:

$$\sigma_i : L \hookrightarrow \Omega \text{ und } L \xrightarrow{\sigma_i} \Omega \xrightarrow{\tau} \Omega\,.$$

Es folgt daß $\forall i \in \{1, \dots, n\}\ \exists j \in \{1, \dots, n\}$, so daß $\tau \circ \sigma_i = \sigma_j$.
Also ist die Abbildung

$$\rho : i \mapsto j \text{ definiert durch } \rho(i) = j \Leftrightarrow \tau \circ \sigma_i = \sigma_j$$

eine Permutation, das heißt $\rho \in S_n$.

• Per Definition von ρ berechnen wir nun für jedes $\pi \in S_n$:

$$\begin{aligned}&\tau(\,\sigma_{\pi(1)}(\mu_1)\dots\sigma_{\pi(n)}(\mu_n)\,) = \\ &(\tau\circ\sigma_{\pi(1)})(\mu_1)\dots(\tau\circ\sigma_{\pi(n)})(\mu_n) = \\ &\sigma_{(\rho\circ\pi)(1)}(\mu_1)\dots\sigma_{(\rho\circ\pi)(n)}(\mu_n)\end{aligned}$$

• Wir betrachten nun zwei Fälle und in jedem Fall:

(i) $\rho \in A_n \Rightarrow \tau(G) = G, \tau(U) = U$ oder

(ii) $\rho \in S_n \backslash A_n \Rightarrow \tau(G) = U, \tau(U) = G$.

Somit ist

$$(*) \qquad \tau(G+U) = G+U \text{ und } \tau(GU) = GU \quad \forall \tau \in \mathrm{Gal}(\Omega/\mathbb{Q})\,.$$

• Es folgt nun aus $(*)$ und Hauptsatz der Galoistheorie (B3, Skript 24, Satz 24.5) daß

$$G+U, GU \in \mathrm{Inv}(\Omega/\mathbb{Q}) \underset{HSGT}{=} \mathbb{Q}\,.$$

Also sind $G+U, GU \in \mathbb{Q}$ und $\mathbb{Z}$ ist ganz abgeschlossen$\Rightarrow G+U, GU \in \mathbb{Z}$.

• Schließlich berechnen wir:

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

Also ist $D(\mathcal{O}_L/\mathbb{Z})$ ein Quadrat mod 4 wie behauptet. □

Definition 19.1
Sei $L/\mathbb{Q}$ ein Zahlkörper. Eine Einbettung von L in $\mathbb{C}$ ist reell, wenn ihr Bild in $\mathbb{R}$ liegt; sonst ist sie komplex.

Erinnerung: Setze $L = \mathbb{Q}(\alpha)$, $[L:\mathbb{Q}] = n$, $f(x) := \mathrm{MinPol}_{\mathbb{Q}}(\alpha)$. Dann ist (Fundamentaler Satz der Algebra) $f(x) = \prod(x-\alpha_i) \in \mathbb{C}[x]$ mit r reellen Nullstellen und $2s$ komplexen Nullstellen, so daß $n = 2s+r$. L hat genau r relle Einbettungen in $\mathbb{C}$ und $2s$ komplexe Einbettungen in $\mathbb{C}$. **Bezeichnung:** $\mathbb{R}_+ = \mathbb{R}^{>0}, \mathbb{R}_- := \mathbb{R}^{<0}$.

Satz 19.1 (Satz von Brill)
Es gilt $\mathrm{sign}D(\mathcal{O}_L/\mathbb{Z}) = (-1)^s$

Beweis. $L = \mathbb{Q}(\alpha)$, $[L:\mathbb{Q}] = n$, $f := \mathrm{MinPol}_{\mathbb{Q}}(\alpha)$. Sei $\{\alpha_1,\dots,\alpha_n\} \subseteq \mathcal{O}_L$ Basis für $L/\mathbb{Q}$ [1].
Sei P wie im Beweis vom Satz 17.2.[2] Es ist:

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

Insbesondere ist aufjedenfall $\mathrm{sign}D(\alpha_1,\dots,\alpha_n) = \mathrm{sign}D(\mathcal{O}_L/\mathbb{Z})$.

[1] Wir haben schon gesehen daß es immer möglich ist, solch eine Basis zu finden, z.B. für ein primitives Element α in $\mathcal{O}_L$ setze $\alpha_i := \alpha^i$.

[2] $P \in M_{n\times n}(\mathbb{Z})$, $\det P \neq 0$ aber nicht unbedingt invertierbar in $\mathbb{Z}$.

Wir berechnen nun $\text{sign}D(1, \alpha, \ldots, \alpha^{n-1})$, d.h wir berechnen $\text{sign}D(f)$.

Seien $\beta_1, \ldots, \beta_r, z_1, \ldots, z_s, \bar{z}_1, \ldots, \bar{z}_s$ alle Nullstellen von f in $\mathbb{C}$. Also gilt die Faktorisierung:

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

$$\underset{\text{Definition}}{\Rightarrow} D(f) = \prod_{i<j} (\beta_i - \beta_j)^2 \prod_{i,k} (\beta_i - z_k)^2 \prod_{i,k} (\beta_i - \bar{z}_k)^2 \prod_{k<l} (z_k - z_l)^2 \prod_{k,l} (z_k - \bar{z}_l)^2 \prod_{k<l} (\bar{z}_k - \bar{z}_l)^2$$

.

Wir untersuchen diese Produkte genau und bestimmen das Signum:

- $\prod_{i<j}(\beta_i - \beta_j)^2 \in \mathbb{R}^2 > 0$ (da $\beta_i \neq \beta_j$) also $\in \mathbb{R}_+$.
- $\underbrace{\prod_{i,k}(\beta_i - z_k)^2}_{:=w} \underbrace{\prod_{i,k}(\beta_i - \bar{z}_k)^2}_{\bar{w}} = w\bar{w} \in \mathbb{R}_+$.
- Analog für $\prod_{k<l}(z_k - z_l)^2 \prod_{k<l}(\bar{z}_k - \bar{z}_l)^2 \in \mathbb{R}_+$.
- Also bleibt $\prod_{k,l}(z_k - \bar{z}_l)^2$ übrig zu behandeln:

Ist $k \neq l$, dann erscheinen tatsächlich die Faktoren $z_k - \bar{z}_l$ sowie $z_l - \bar{z}_k$ im Produkt, also

$$(z_k - \bar{z}_l)^2 (z_l - \bar{z}_k)^2 = [-\underbrace{(z_k - \bar{z}_l)(\bar{z}_k - z_l)}_{\in \mathbb{R}^+}]^2 \in \mathbb{R}_+$$

Letztendlich ist also

$$\text{sign}D(1, \alpha, \ldots, \alpha^{n-1}) \;=\; \text{sign} \prod_{k=1}^{s} (z_k - \bar{z}_k)^2 \,.$$

Aber $z_k - \bar{z}_k \in i\mathbb{R}$, also ist $(z_k - \bar{z}_k)^2 \in \mathbb{R}_-$, also ist $\prod_{k=1}^{s}(z_k - \bar{z}_k)^2$ Produkt von s negativen reellen Zahlen, und damit ist sein Signum $(-1)^s$. □