Vorlesung Zahlentheorie I (Algebraische ZT)

WiSe '22/'23, hhu
K. Halupczok

Z17: Satz von Hermite

Stichworte: Satz von Hermite: Es gibt nur endl. viele ZK mit vorgegebener Diskriminante.

17.1. Einleitung: Es gibt verschiedene, nichtisomorphe ZK mit derselben Diskriminante. Zu einer vorgegebenen Diskriminante d kann es aber nur (höchstens) endlich viele ZK K mit $\operatorname{disc} K = d$ geben – dies besagt der Satz von Hermite. Dieser Satz ist eine Folgerung des Minkowskischen Gitterpunktsatzes. Im Beweis unterscheiden wir den Fall, dass K reelle Einbettungen besitzt, vom anderen Fall.

17.2. Satz (von Hermite): Es gibt nur endlich viele Zahlkörper K mit vorgegebener Diskriminante d.

Bew.: Wegen 16.20 haben Zahlkörper K mit $\operatorname{disc} K = d$ beschränkten Grad. Daher genügt es, z.z.: Zu festen s,t mit $n = s+2t$ gibt es nur endlich viele K mit s reellen und $2t$ nichtreellen Einbettungen, sowie $\operatorname{disc} K = d$.
Sei OE $n>1$ und K ein solcher ZK, A sein ZR. Nach 16.12 ist dann $\operatorname{vol}(\mathbb{R}^n/\sigma A) = 2^{-t}\sqrt{|\operatorname{disc} K|} = 2^{-t}\sqrt{|d|}$.
Falls $s \geq 1$: Betr. die kanonische Einbettung $\sigma: K \to \mathbb{R}^n$, $x \mapsto (\sigma_1 x, \dots, \sigma_s x, \operatorname{Re}\tau_1 x, \operatorname{Im}\tau_1 x, \dots, \operatorname{Re}\tau_t x, \operatorname{Im}\tau_t x)$, und sei $S := \{(x_1, \dots, x_s, u_1, v_1, \dots, u_t, v_t);\ |x_i| \leq \frac{1}{2}$ für $2 \leq i \leq s$,
$|u_j|, |v_j| \leq \frac{1}{2}$ für $1 \leq j \leq t$, $|x_1| \leq 2^{n-t-1}\sqrt{|d|}\}$,
ist kompakt, konvex und zentralsymmetrisch.

Ferner ist $\operatorname{vol}(S) = 2^{n-t}\sqrt{|d|} = 2^n \operatorname{vol}(\mathbb{R}^n/\sigma A)$. Mit 16.7 folgt: Es ex. ein $0 \neq x \in A$ mit $\sigma x \in S$ und $\sigma x = (\sigma_1 x, \dots, \sigma_s x, \operatorname{Re}\tau_1 x, \operatorname{Im}\tau_1 x, \dots, \operatorname{Re}\tau_t x, \operatorname{Im}\tau_t x)$.
Für jede Einbettung $\rho: K \to \mathbb{C}$ mit $\rho \neq \sigma_1$ gilt: $|\rho x| \leq \frac{\sqrt{2}}{2}$ $\left(= \sqrt{(\frac{1}{2})^2 + (\frac{1}{2})^2}\right)$,
sogar $|\rho x| \leq \frac{1}{2}$, falls ρ reell.

Also: wegen $1 \leq |N(x)| = \prod_{i=1}^{s} \overbrace{|\sigma_i x|}^{\text{Faktoren} \leq \frac{1}{2}, \text{ außer } |\sigma_1 x|} \cdot \prod_{j=1}^{t} \overbrace{|\tau_j x|}^{\text{Faktoren} \leq \frac{\sqrt{2}}{2} < 1}$ ist $|\sigma_1 x| > 1$. Daher ist $[\mathbb{Q}(x):\mathbb{Q}] = n$, d.h. $K = \mathbb{Q}(x)$, da $\sigma_1 x \neq \rho x$ für alle $\rho \neq \sigma_1$. ⌜Sonst ist K und σ_1 auf mehrere $\mathbb{Q}(x) \xrightarrow{\sigma_1} \mathbb{C}$, $\mathbb{Q}$, Arten, nämlich $[K:\mathbb{Q}(x)] > 1$ viele, fortsetzbar zu Einbettungen $\rho: K \to \mathbb{C}$, ↯.⌟

Da alle $|\sigma_i x|$, $|\tau_j x|$ beschränkt sind durch $2^{n-t-1}\sqrt{|d|}$, sind die Koeff. des Mipos von x beschränkt, etwa durch $\delta > 0$. Da es nur endlich viele ganzzahlige Polynome vom Grad n mit durch δ beschränkten Koeff. gibt, kommen auch für x nur endlich viele Werte in Frage.
Also gibt es nur endl. viele solcher ZK K mit $\operatorname{disc} K = d$.
Fall $s = 0$: Ersetzen in der Def. von S x_1 durch v_1,
d.h. $S := \{(u_1, v_1, \dots, u_t, v_t);\ |u_j|, |v_j| \leq \frac{1}{2}$ für $2 \leq j \leq t$, $|u_1| \leq \frac{1}{2}$, $|v_1| \leq 2^{n-t-1}\sqrt{|d|}\}$.
Damit kann der Fall genau analog behandelt werden (mit τ_1 anstelle σ_1). □