Vorlesung Zahlentheorie I (Algebraische ZT)

WiSe '22/'23, hhu
K. Halupczok

§9: Zahlring des Kreisteilungskörpers

Stichworte: Zahlring des Kreisteilungskörpers, Kompositum, Zahlring des Kompositums

---

9.1. **Einleitung:** Wir zeigen in mehreren Schritten, dass $\mathbb{Z}[\omega]$ der Zahlring des Kreisteilungskörpers $\mathbb{Q}(\omega)$ mit $\omega = e^{2\pi i/m}$ ist: Zuerst im Spezialfall, dass m eine Primpotenz ist. Im allgemeinen Fall arbeiten wir induktiv mit dem Kompositum linear disjunkter Kreisteilungskörper.

9.2. **Satz:** Sei $m = p^e$ Primpotenz, $\omega = e^{\frac{2\pi i}{m}}$. Dann ist $\mathbb{A} \cap \mathbb{Q}(\omega) = \mathbb{Z}[\omega]$.

Bem.: Dies gilt für bel. $m \in \mathbb{N}$, vgl. 9.10.

Bew.: Sei $0 \neq m > 2$. Es gilt: $\mathbb{Q}(\omega)$ hat Grad $\varphi(m) = p^{e-1}(p-1) =: n$.

Ferner ist $T^m - 1 = (T^{p^{e-1}})^p - 1 = (T^{p^{e-1}} - 1) \cdot \underbrace{(T^{p^{e-1}(p-1)} + \ldots + T^{p^{e-1}} + 1)}_{=: f(T)}$.

Wegen $\deg f = [\mathbb{Q}(\omega):\mathbb{Q}]$ und $f(\omega) = 0$ ist f das Mipo von $\omega | \mathbb{Q}$. Also ist $f(T) = \prod_{\substack{0 \leq i \leq p^e \\ p \nmid i}} (T - \omega^i)$.

Es ist $N(1-\omega) = \prod_{\sigma \in G} \sigma(1-\omega) = \prod_{\sigma \in G} (1 - \sigma\omega) = f(1) \; (= \prod_{p \nmid i} (1-\omega^i)) = p$.

Da $1-\omega$ alle Faktoren $1-\omega^i$ in $\mathbb{Z}[\omega]$ teilt, folgt daraus:
$(1-\omega)^j | p$ in $\mathbb{Z}[\omega]$, also ist $\frac{p}{(1-\omega)^j} \in \mathbb{Z}[\omega]$, $0 \leq j \leq m$. (**)

Da $\mathbb{Z}[\omega] = \mathbb{Z}[1-\omega]$, genügt es, $\mathbb{Q}(\omega) \cap \mathbb{A} \stackrel{!}{=} \mathbb{Z}[1-\omega]$ zu zeigen.

Daher ist auch: $\operatorname{disc}(\omega) = \prod_{i<j} (\omega^i - \omega^j)^2 = \prod_{i<j} ((1-\omega^i) - (1-\omega^j))^2 = \operatorname{disc}(1-\omega) =: \Delta$.

Sei nun $x \in \mathbb{A} \cap \mathbb{Q}(\omega)$.

Nach 8.2 hat x die Darstellung $x = a_0 \frac{1}{d} + a_1 \cdot \frac{1-\omega}{d} + \ldots + a_{n-1} \cdot \frac{(1-\omega)^{n-1}}{d}$,

die $a_i \in \mathbb{Z}$, $d \in \mathbb{Z}$, $d \mid \operatorname{disc}(1-\omega) = \Delta$, da $\mathbb{Z}[1-\omega] \subseteq \mathbb{A} \cap \mathbb{Q}(\omega)$, vgl. Beweis zu 8.6.

Sei $0 \neq \operatorname{ggT}(\{d\} \cup \{a_i : 0 \leq i < m\}) = 1$.

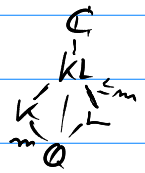
Z.z.: $d = 1$, dann folgt: $x \in \mathbb{Z}[1-\omega]$. Ann.: $d \neq 1$.

Nach 6.22.(1) ist Δ, also auch d, eine Potenz von p, etwa $d = p^f$, $f \geq 1$.

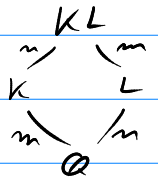
Nun sei $\mathbb{Q}$ $f=1$ [ersetzen x durch $p^{f-1}x$].
Sei nun $i := \min\{j;\ p \nmid a_j\}$. Somit ist $y := a_i \frac{(1-\omega)^i}{p} + \dots + a_{m-1}\frac{(1-\omega)^{m-1}}{p} \in \mathbb{Z}[\omega]$,
wo $p \nmid a_i$ nach Wahl von i.
Es folgt: $\underbrace{\frac{p}{(1-\omega)^{i+1}} y}_{\in \mathbb{Z}[\omega] \text{ nach } (**)} = \frac{a_i}{1-\omega} + c$ mit $c \in \mathbb{Z}[\omega]$.
Somit ist $\frac{a_i}{1-\omega} \in \mathbb{Z}[\omega] \subseteq A \cap \mathbb{Q}(\omega)$. Also ist $\mathbb{Z} \ni N\left(\frac{a_i}{1-\omega}\right) = N(a_i)\, N(1-\omega)^{-1} = \frac{a_i^m}{p}$,
↯ zu $p \nmid a_i$. □

9.3. Bem.: Nicht jeder Zahlkörper hat eine G+IB der Gestalt $1, x, \dots, x^{m-1}$.

9.4. Def.: Seien K, L Zahlkörper, dann heißt $KL := \bigcap \{E \subseteq \mathbb{C}$ Körper; $K, L \subseteq E\}$,
der von $K \cup L$ in $\mathbb{C}$ erzeugte Körper, das Kompositum von K und L.

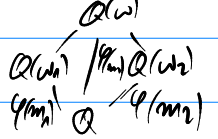


9.5. Bem.: (1) Ist $K = \mathbb{Q}(x)$ und $L = \mathbb{Q}(y)$, so ist $KL = \mathbb{Q}(x,y)$.
Es folgt: $[KL:\mathbb{Q}] \leq [K:\mathbb{Q}] \cdot [L:\mathbb{Q}]$.
(2) Es ist $KL = \{\sum_{i=1}^{n} x_i y_i;\ n \in \mathbb{N}$, alle $x_i \in K$, alle $y_i \in L\}$.
„$\supseteq$" ✓, „$\subseteq$": KL Körper: Ring klar, da k.U. der von $K \cup L$ erzeugte Ring.
Dieser besteht aus algebraischen Zahlen, ist also Körper. ↯
(3) Seien A, B, C die Zahlringe von K, L und KL.
Sei AB der von $A \cup B$ erzeugte Ring, d.h. $AB = \{\sum_{i=1}^{n} x_i y_i;\ n \in \mathbb{N}, x_i \in A, y_i \in B\}$.
Dann ist $AB \subseteq C$.



9.6. Def.: Seien K, L Zahlkörper. Diese heißen linear disjunkt, falls $[KL:\mathbb{Q}] = [K:\mathbb{Q}] \cdot [L:\mathbb{Q}]$.

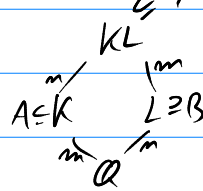
9.7. Bsp.: (1) Sind $m = [K:\mathbb{Q}]$ und $n = [L:\mathbb{Q}]$ teilerfremd,
so sind K und L linear disjunkt.
$r := [KL:\mathbb{Q}] \Rightarrow m, n \mid r$, also $mn \mid r$. Nach 9.5(1) folgt $r \leq mn$, also $r = mn$. ↯
(2) Seien $m_1, m_2 > 1$, $m = kgV(m_1, m_2)$, $\omega_1 = e^{\pi i/m_1}$, $\omega_2 = e^{2\pi i/m_2}$, $\omega = e^{2\pi i/m}$.
Dann gilt: $\mathbb{Q}(\omega_1, \omega_2) = \mathbb{Q}(\omega_1) \cdot \mathbb{Q}(\omega_2) = \mathbb{Q}(\omega)$.



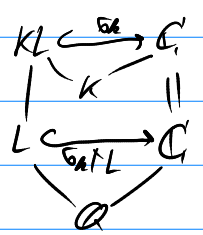
Sind m_1, m_2 teilerfremd, so sind
$\mathbb{Q}(\omega_1), \mathbb{Q}(\omega_2)$ linear disjunkt.
[Denn: $m = m_1 m_2 \Rightarrow \varphi(m_1 m_2) = \varphi(m_1)\varphi(m_2) = \varphi(m)$, Def. ↯

9.8. **Satz:** Seien K, L linear disjunkte Zahlkörper mit Zahlringen A, B, sei C der Zahlring von KL, $g := ggT(\operatorname{disc} K, \operatorname{disc} L)$.
Dann gilt: $A \cdot B \subseteq C \subseteq \frac{1}{g} A \cdot B$.

Bew.: Sei $x_1, \dots, x_m$ G+B von K, und $y_1, \dots, y_n$ G+B von L.
Dann ist $x_i y_j$ mit $1 \le i \le m$, $1 \le j \le n$, eine Basis von $KL \mid \mathbb{Q}$.
Sei $z \in C$, Schreiben $z = \sum_{i,j} \frac{m_{ij}}{r} (x_i y_j)$ mit $m_{ij}, r \in \mathbb{Z}$ ohne gemeinsamen Teiler.
Z.Z.: $r \mid \operatorname{disc} K$ und $r \mid \operatorname{disc} L$.



Sei $u_j = \sum_i \frac{m_{ij}}{r} x_i \in K$. Dann ist $z = \sum_j u_j y_j$.
Seien $\sigma_1, \dots, \sigma_m$ die Einbettungen von $KL \mid K$ in $\mathbb{C}$.
Dann sind $\sigma_1 \mid L, \dots, \sigma_m \mid L$ Einbettungen von $L \mid \mathbb{Q}$ in $\mathbb{C}$.



Dann ist $\sigma_k z = \sum_j u_j (\sigma_k y_j)$ für $1 \le k \le m$.
Dies ist ein LGS für u_j mit Koeff.matrix $(\sigma_k y_j)$,
wo $(\det(\sigma_k y_j))^2 =: \delta^2 = d := \operatorname{disc} L$ ist.
Nach der Cramerschen Regel folgt $u_j = \frac{e_j}{\delta}$, wo $e_j \in A$, $1 \le j \le m$.
Somit ist $\underbrace{d u_j}_{\in K} = \underbrace{e_j \delta}_{\in A} \in K \cap A = A = \bigoplus_{i=1}^{m} \mathbb{Z} x_i$,
d.h. es ist $d \cdot \frac{m_{ij}}{r} \in \mathbb{Z}$ für alle i, j.
Also gilt: $r \mid d = \operatorname{disc} L$. Genau analog folgt: $r \mid \operatorname{disc} K$. □

9.10. **Kor.:** Sei $m \in \mathbb{N}_{>1}$, $\omega = e^{2\pi i/m}$. Dann ist $A \cap \mathbb{Q}(\omega) = \mathbb{Z}[\omega]$.
Bew.: Vollst. Ind. nach m: • Falls $m = p^e$ Primpotenz, vgl. 9.2.
• Sonst Schreiben $m = m_1 m_2$ mit $(m_1, m_2) = 1$.
Sei $\omega_1 = \omega^{m_2} = e^{2\pi i/m_1}$, $\omega_2 = \omega^{m_1} = e^{2\pi i/m_2}$, $K_1 = \mathbb{Q}(\omega_1)$, $K_2 = \mathbb{Q}(\omega_2)$.
Nach 9.7 (2) sind K_1, K_2 linear disjunkt, und $K_1 K_2 = \mathbb{Q}(\omega)$.
Nach Ind.vor. ist $\mathbb{Z}[\omega_i]$ der Zahlring von K_i, $i = 1, 2$.
Nach 6.22 (2) ist $\operatorname{disc} K_i \mid m_i^{\varphi(m_i)}$ für $i = 1, 2$,
also ist $ggT(\operatorname{disc} K_1, \operatorname{disc} K_2) = 1$.
Mit 9.8 folgt also $\mathbb{Q}(\omega) \cap A = \mathbb{Z}[\omega_1] \cdot \mathbb{Z}[\omega_2] = \mathbb{Z}[\omega]$. □