Vorlesung Zahlentheorie I (Algebraische ZT)

WiSe '22/'23, Uhu
K. Halupczok

Z5: Kreisteilungskörper

Stichworte:
n-ter Kreisteilungskörper K_n, n-te Einheitswurzeln E_n, $\mathrm{Gal}(K_n|\mathbb{Q}) \cong (\mathbb{Z}/(n))^\times$, alle EW im Kreisteilungskörper, Kreisteilungspolynome sind irreduzibel

---

5.1. **Einleitung:** Der Kummersche Beweisansatz des Fermatproblems für den Exponenten p arbeitet im p-ten Kreisteilungskörper $\mathbb{Q}(\omega)$ und seinem Teilring $\mathbb{Z}[\omega]$, $\omega = e^{2\pi i/p}$, wie in Z1, Z2 gesehen. Wir zeigen, welche Einheitswurzeln den n-ten KTK erzeugen, welche EWn überhaupt darin enthalten sind, und zeigen, dass seine Galoisgruppe isomorph zu $(\mathbb{Z}/(n))^\times$ ist.

5.2. **Def.:** Sei $n \geq 1$. Der Zerfällungskörper K_n von $T^n - 1$ über $\mathbb{Q}$ heißt **n-ter Kreisteilungskörper** (über $\mathbb{Q}$). Die **n-ten Einheitswurzeln** (EW) sind $e^{2\pi i k/n}$, $0 \leq k < n$, d.h. genau die komplexen Nullstellen von $T^n - 1$.

5.3. **Bem.:**
- Die n-ten EW bilden eine zyklische Gruppe E_n der Ordnung n (ω ist offenbar Erzeuger, da $E_n = \{(e^{2\pi i/n})^k ; k \in \mathbb{Z}\}$).
- Es ist $K_n = \mathbb{Q}(e^{2\pi i/n})$.
- Eine EW $\omega \in E_n$ heißt **primitiv**, falls sie E_n erzeugt. [D.h. $E_n = \{\omega^k ; k \in \mathbb{Z}\}$]
- Es gilt: $\omega = e^{2\pi i k/n}$ primitiv $\Leftrightarrow k \in (\mathbb{Z}/(n))^\times \Leftrightarrow (k,n) = 1$.

[Erstes "$\Leftrightarrow$": ω pr. $\Leftrightarrow \exists \ell : e^{2\pi i k\ell/n} = e^{2\pi i/n} \Leftrightarrow \exists \ell : k\ell \equiv 1 \ (n) \Leftrightarrow k \in (\mathbb{Z}/(n))^\times$

Zweites "$\Leftrightarrow$": vgl. Einf. ZT, EZ6.15: $\exists \ell : k \cdot \ell = 1 \Leftrightarrow \exists \ell : k\ell \equiv 1 \ (n)$
$\Leftrightarrow \exists r, \ell : 1 = \ell k + rn$ (Bézout/$\mathbb{Z}$ HIB) $\Leftrightarrow (k,n) = 1$.]

- $\varphi(n) = \#(\mathbb{Z}/(n))^\times = \#\{k \in \{1,\dots,n\} ; (k,n) = 1\}$ ist die **Eulersche φ-Fkt.**

Somit gibt es $\varphi(n)$ viele primitive n-te EWn.

Erinnerung:
- φ ist multiplikativ, d.h. $(n,m) = 1 \Rightarrow \varphi(nm) = \varphi(n)\varphi(m)$.
- $\varphi(p^k) = p^k - p^{k-1} = p^k(1 - \frac{1}{p})$ für p prim, $k \in \mathbb{N}_0$.
- $\varphi(p_1^{e_1} \cdots p_r^{e_r}) = p_1^{e_1} \cdots p_r^{e_r} \cdot \prod_{j=1}^{r} (1 - \frac{1}{p_j})$ für p_j prim, $k_j \in \mathbb{N}_0$, $j = 1,\dots,r$.
- (*) $\varphi(nt) = n\varphi(t)$, falls $\forall p : p \mid n \Rightarrow p \mid t$ [$\varphi(nt) = nt \prod_{p \mid t} (1 - \frac{1}{p}) = n\varphi(t)$ ✓]

Der folgende Satz gibt Auskunft über Erzeuger/primitive Elemente des n-ten Kreisteilungskörpers K_n, und über seine Galoisgruppe

$\mathrm{Gal}(\mathbb{Q}(\omega)|\mathbb{Q}) := \{\sigma \text{ Auto von } \mathbb{Q}(\omega)|\mathbb{Q},\ \sigma|_{\mathbb{Q}} = id_{\mathbb{Q}}\}$.

5.4. **Satz:** Sei $\omega \in E_n$ primitive n-te EW. Dann ist $K_n = \mathbb{Q}(\omega)$, und

$$\psi : \mathrm{Gal}(\mathbb{Q}(\omega)|\mathbb{Q}) \to (\mathbb{Z}/(n))^\times$$
$$\sigma \mapsto \underline{k} = k + (n), \text{ def. durch } \sigma\omega = \omega^k,$$

ist bijektiver Gruppenmorphismus.

Bew.: • Morph.: Sei $\sigma \mapsto \underline{k}$, $\tau \mapsto \underline{l}$, dann: $(\sigma\tau) \mapsto \underline{j} \overset{?}{=} \underline{k}\cdot\underline{l}$. Nach Def. ist $\omega^j = (\sigma\tau)(\omega) = \sigma(\tau\omega) = \sigma(\omega^l) = (\sigma\omega)^l = (\omega^k)^l = \omega^{kl}$, also $\underline{k}\cdot\underline{l} = \underline{j}$.

• inj.: Sei $\underline{k} = \underline{1} = 1 + (n)$, dann ist $\sigma\omega = \omega^1 = \omega$, also $\sigma = id$.

• surj.: z.z.: $\#\mathrm{Gal}(\mathbb{Q}(\omega)|\mathbb{Q}) \overset{!}{=} \varphi(n)$, bzw. $[\mathbb{Q}(\omega):\mathbb{Q}] \overset{!}{=} \varphi(n)$, da $\#\mathrm{Gal}(\mathbb{Q}(\omega)|\mathbb{Q}) = [\mathbb{Q}(\omega):\mathbb{Q}]$ laut Algebra A 22.4, (denn $K_n|\mathbb{Q}$ ist galois, d.h. normal und separabel).

Dies erhalten wir mit 5.11. □

5.5 **Kor.:** $\mathrm{Gal}(K_n|\mathbb{Q}) \cong (\mathbb{Z}/(n))^\times$.

Bew.: $\#\mathrm{Gal}(K_n|\mathbb{Q}) = [K_n:\mathbb{Q}] \overset{5.11}{=} \varphi(n) = \#(\mathbb{Z}/(n))^\times$, ψ inj. $\Rightarrow$ ψ surj., also Isom. □

Das folgende Korollar gibt an, welche EWn in einem Kreisteilungskörper liegen, es sind i.a. nicht nur die Potenzen von $e^{2\pi i/n}$. Wir haben dieses Kor. für $n = p \geq 3$ bereits im Beweis des Kummerschen Lemmas 1,14 benutzt, vgl. 2.2 (i).

5.6. **Kor.:** Sei $\omega = e^{2\pi i/n}$. Die (n-ten) EWn in $\mathbb{Q}(\omega)$ sind genau die

$$\begin{cases} n\text{-ten}, & \text{falls } n \text{ gerade}, \\ 2n\text{-ten}, & \text{falls } n \text{ ungerade}. \end{cases}$$

Bsp.: Im 5-ten KTK $\mathbb{Q}(\omega)$ mit $\omega := e^{2\pi i/5}$ sind alle EWn die Potenzen von $\underbrace{e^{2\pi i/10}}_{= e^{\pi i/5}}$

d.h. $\{z \in \mathbb{Q}(\omega);\ \exists m \in \mathbb{Z} : z^m = 1\} = \{(e^{\pi i/5})^l ;\ l \in \mathbb{Z}\}$.

Nicht unmittelbar klar ist wohl $e^{\pi i/5} \in \mathbb{Q}(\omega)$. Dies gilt aber, da

$$e^{\pi i/5} = -\underbrace{e^{5\pi i/5}}_{=-1}\cdot e^{\pi i/5} = -e^{6\pi i/5} \overset{\text{de Moivre}}{=} -(e^{2\pi i/5})^3 = -\omega^3 \in \mathbb{Q}(\omega).$$

Bew.: (i): Sei n gerade. Sei $m \geq 1$, E_m von ζ erzeugt. Dann ist $E_m \cdot E_m \subseteq (\mathbb{Q}(\omega))^\times$, mit $E_k \supseteq E_m \cdot E_m$, wo $k = \mathrm{ggV}(m,m)$ [also $\varphi(k) \geq \varphi(m)$]. Somit ist $\mathbb{Q}(E_k) \subseteq \mathbb{Q}(\omega) = \mathbb{Q}(E_m)$, mit 5.4 folgt $\varphi(k) \leq \varphi(m)$. Also ist $\varphi(k) = \varphi(m)$, wobei $m \mid k$, $2 \mid m$.

Dies zeigt, dass $k = m$ ist. [• Sei $k = mr$, haben $r = \gamma_m(r)\tau_m(r)$, wobei $\gamma_m(r) := \prod_{\substack{p^\ell \| r \\ p \mid m}} p^\ell$, $\tau_m(r) := \prod_{\substack{p^\ell \| r \\ p \nmid m}} p^\ell$, dabei gilt $\forall p$: $p \mid \gamma_m(r) \Rightarrow p \mid m\tau_m(r)$, ferner $(m, \tau_m(r)) = 1$.

• Also: $\varphi(m) = \varphi(k) = \varphi(mr) = \varphi(m\,\gamma_m(r)\tau_m(r)) \overset{5.3}{\underset{\circledast}{=}} \gamma_m(r)\,\varphi(m\tau_m(r)) \overset{\leq}{=} \gamma_m(r)\,\varphi(m)\,\varphi(\tau_m(r))$, und es folgt $1 = \gamma_m(r) \cdot \varphi(\tau_m(r))$, also $\gamma_m(r) = 1 = \varphi(\tau_m(r))$.

• Aus $\varphi(\tau_m(r)) = 1$, d.h. $\tau_m(r) = 1$ oder $\tau_m(r) = 2$, folgt $r = 1$ oder $r = 2$. • Mit $\gamma_m(r) = 1$ ist $(r,m) = 1$, und da $2 \mid m$ ist also $2 \nmid r$ und somit $r = 1$, d.h. $k = m$.]

Also: $m \mid n$, somit ist jede (m-te) EW in $\mathbb{Q}(\omega)$ auch eine n-te.

(ii): Sei n ungerade, dann ist $-\omega$ primitive $2n$-te EW. [$-\omega = e^{\pi i} \cdot e^{2\pi i/n} = e^{(n+2)2\pi i/2n}$ mit $(\underbrace{n+2}_{\text{ungerade}}, 2n) = 1$]

Anwenden von (i) auf $-\omega$ liefert:

Die EW in $\mathbb{Q}(-\omega) = \mathbb{Q}(\omega)$ sind genau die $2n$-ten. □

Im folgenden Konstruieren wir das Minimalpolynom von ω.

5.7. **Def.:** Sei $\Phi_n(T) \in \mathbb{C}[T]$ das normierte Polynom, dessen Nst. genau aus den primitiven n-ten EW besteht, d.h. $\Phi_n(T) := \prod_{\substack{j \leq n \\ (j,n)=1}} (T - \omega_n^j)$, $\omega_n := e^{2\pi i/n}$.

Das Polynom $\Phi_n(T)$ heißt n-tes Kreisteilungspolynom.

5.8. **Lemma:** $T^n - 1 = \prod_{d \mid n} \Phi_d(T)$.

Bew.: $l.S. = \prod_{k \leq n} (T - \omega_n^k) \overset{\text{mit } k \text{ durchläuft auch } n/d \text{ alle Teiler von } n \text{ sortiert die } k \text{ gemäß ggT mit } n}{=} \prod_{d \mid n} \prod_{\substack{k \leq n \\ (k,n) = n/d}} (T - \omega_n^q) \overset{\Leftrightarrow \left(\frac{k}{n/d}, \frac{n}{n/d}\right) = 1}{=} \prod_{d \mid n} \prod_{\substack{j \leq d \\ (j,d)=1}} (T - \omega_n^{jn/d}) = r.S.$ □

5.9. **Kor.:** $\Phi_n(T) \in \mathbb{Z}[T]$ für alle $n \geq 1$.

Bew.: Induktiv aus 5.8: • Für $n = 1$ ist $\Phi_1(T) = T - 1 \in \mathbb{Z}[T]$ trivial.

• Im Fall $n > 1$ zerlege $T^n - 1 \overset{5.8}{=} \Phi_n(T) \cdot \prod_{d \mid n,\, d \neq n} \Phi_d(T)$, das $\prod$ ist $\in \mathbb{Z}[T]$ laut Ind.vor. Laut Polynomdivision ex. (eind.) $\tau, q \in \mathbb{Z}[T]$ mit $T^n - 1 = q \cdot \prod_{d \mid n,\, d \neq n} \Phi_d(T) + r$ mit $r = 0$ oder $r \neq 0$ mit $\deg r < \deg \prod_{d \mid n,\, d \neq n} \Phi_d(T)$. Die Darstellung gilt auch in $\mathbb{Q}(\omega)[T]$ und ist dort eindeutig, also ist $r = 0$ und $\Phi_n(T) = q \in \mathbb{Z}[T]$. □

5.10. **Lemma:** Φ_n ist irreduzibel über $\mathbb{Q}$.

Bew.: Haben $\Phi_n \neq 0, \pm 1$ für $n \geq 1$. Weiter ist Φ_n primitiv, da normiert.
Nach einer Folgerung des Gaußschen Lemma 3.19, nämlich Algebra Lemma A15.6, ist Φ_n irreduzibel in $\mathbb{Q}[T]$ genau dann, wenn Φ_n in $\mathbb{Z}[T]$ irreduzibel ist. Daher:
Sei $\Phi_n = PQ$ mit $P, Q \in \mathbb{Z}[T]$, $\deg P > 0$ normiert und $\mathbb{C} \supseteq E$ irreduzibel, d.h. P ist das Mipo von jeder Nst. von P. Z.z.: $P = \Phi_n$.

(i): Sei p prim mit $p \nmid n$, betr. $\mathbb{Z}[T] \to (\mathbb{Z}/p)[T]$, $R \mapsto \overline{R}$.
Ist $F := T^n - 1$, wo $nF(T) - TF'(T) = -n$, haben wir $(\overline{F}, \overline{F}') = 1$ da $p \nmid n$, also ist $\overline{F}$ separabel (vgl. Algebra A20.5). Haben $\overline{PQ} = \overline{\Phi}_n \mid \overline{F}$ wegen 5.8.

(ii): Sei p prim mit $p \nmid n$. Ist ζ eine bel. Nst. von P, dann ist auch ζ^p Nst. von P.
Mit ζ ist auch ζ^p primitive n-te EW, da $p \nmid n$, somit ist ζ^p Nst. von Φ_n.
Daher ist $\Phi_n(\zeta^p) = 0 = P(\zeta^p) \cdot Q(\zeta^p)$. Ann.: $Q(\zeta^p) = 0$, dann ist $Q(T^p)$ durch das Mipo von ζ teilbar, also durch P, es folgt $Q(T^p) = P(T) \cdot H(T)$ für ein $H \in \mathbb{Z}[T]$.
Anwenden von $\mathbb{Z}[T] \to (\mathbb{Z}/p)[T]$ liefert $\overline{Q}(T^p) = \overline{P}(T) \cdot \overline{H}(T) \in (\mathbb{Z}/p)[T]$.
Für jedes Polynom $G(T) = \sum a_i T^i \in (\mathbb{Z}/p)[T]$ gilt $\overline{G}(T)^p = (\sum \overline{a_i} T^i)^p = \sum \overline{a_i}^p T^{pi} = \overline{G}(T^p)$, $\overline{a_i}^p = \overline{a_i}$
es folgt $\overline{Q}(T)^p = \overline{P}(T) \cdot \overline{H}(T)$, und in einem Zerfällungskörper von $\overline{F}$ haben also $\overline{P}$ und $\overline{Q}$ eine gemeinsame Nst., diese ist $(\text{dort})^n$ also (mind.) doppelte Nst. von $\overline{F}$, $\lightning$ zu (i).

(iii): Sei nun ζ eine Nst. von P, insb. ist ζ eine primitive n-te EW.
Für jedes k mit $(k,n) = 1$ schreibe $k = p_1 \cdots p_r$, die p_i nicht notw. p.w.v. mit $p_i \nmid n$.
Nach (ii) ist dann ζ^{p_1} Nst. von P, dann auch $(\zeta^{p_1})^{p_2}$, usw., also ist auch ζ^k eine Nst. von P. Damit ist jede primitive n-te EW Nst. von P, es folgt $P = \Phi_n$ und $Q = 1$. □

5.11. **Satz:** $[\mathbb{Q}(\omega) : \mathbb{Q}] = \varphi(n)$ für $\omega = e^{2\pi i/n}$.
Bew.: Es ist $[\mathbb{Q}(\omega) : \mathbb{Q}] \overset{5.10}{=} \deg \Phi_n = \varphi(n)$. □

5.12. **Kor.:** $\Phi_n(T) = \prod_{d \mid n} (T^d - 1)^{\mu(n/d)}$ mit Möbiusfunktion $\mu(t) := \begin{cases} 0, & \exists p : p^2 \mid t, \\ (-1)^r, & t = p_1 \cdots p_r \text{ für } p_i \text{ p.w.v. prim.} \end{cases}$

Bew.: Möbius-Inversion, d.h. $\sum_{t \mid n} \mu(t) = \begin{cases} 1, & n = 1 \\ 0, & \text{sonst} \end{cases}$, vgl. Anl 22.10, ergibt

$$\text{r.S.} \overset{5.8}{=} \prod_{d \mid n} \Big(\prod_{t \mid d} \Phi_t(T) \Big)^{\mu(\frac{n}{d})} = \prod_{d \mid n} \prod_{t \mid d} \Big(\Phi_t(T)^{\mu(\frac{n}{d})} \Big) = \prod_{d \mid n} \prod_{t \mid \frac{n}{d}} \Phi_t(T)^{\mu(d)} \overset{t \mid \frac{n}{d} \Leftrightarrow d \mid \frac{n}{t}}{=} \prod_{t \mid n} \Phi_t(T)^{\sum_{d \mid \frac{n}{t}} \mu(d)} = \Phi_n(T). \quad \square$$

(=1 genau für $t = n$, sonst $= 0$)

5.13. **Bem.:** • Mit 5.12 lassen sich per Polynomdivision Kreisteilungspolynome berechnen, z.B. $\Phi_6(T) = T^2 - T + 1$.
• $\Phi_{105}(T)$ ist das "erste" KT-polynom mit Koeff. vom Betrag > 2. Die Koeffizienten können bel. groß werden.