Freie Universität Berlin
Institut für Mathematik
Prof. Victoria Hoskins

WiSe 2018/19

Algebra und Zahlentheorie
Übungsblatt 11

Lösungsvorschlag Martin Günther

Aufgabe 3 (14 Punkte)

Sei $n \in \mathbb{N}$ und $\varphi(n)$ die Eulersche Phi-Funktion von n. Eine Nullstelle $\alpha \in \mathbb{C}$ von $t^n - 1$ heißt *primitive n-te Einheitswurzel*, wenn die Ordnung von α in $\mathbb{Q}^\times$ gleich n ist.

a) Zeigen Sie, dass es genau $\varphi(n)$ primitive Einheitswurzeln von Eins $\alpha_{n,1}, \dots, \alpha_{n,\varphi(n)}$ gibt.

Zunächst machen wir uns klar, dass alle n-ten Einheitswurzeln eine endliche Untergruppe U_n des $\mathbb{C}^\times$ mit Gruppenordnung $|U_n| = n$ bilden, denn seien α, β zwei Einheitswurzeln, dann gilt $(\alpha \cdot \beta)^n = \alpha^n \beta^n = 1$. Außerdem ist diese nicht leer, da mindestens die 1 enthalten ist. Insbesondere ist $U_n < \mathbb{C}^\times$ zyklisch. D.h. es gibt einen Erzeuger $\alpha \in U_n : \langle \alpha \rangle = U_n$
Wir wissen, dass jede zyklische Gruppe isomorph zu einer Faktorgruppe $(\mathbb{Z}/n\mathbb{Z}, +)$ ist. Einen Isomorphismus ψ können wir explizit durch $\psi(\overline{1}) = \alpha$ angeben. Es gilt also $\psi(\overline{m}) = \alpha^m$. Wir behaupten, dass $\overline{m} \in \mathbb{Z}/n\mathbb{Z}$ Erzeuger ist genau dann, wenn $\mathrm{ggT}(m, n) = 1$. Denn

$$\mathrm{ggT}(m,n) = 1 \Leftrightarrow \exists a, b \in \mathbb{Z} : 1 = am + bn \equiv_n am \Leftrightarrow \overline{1} \in \langle \overline{m} \rangle$$

Da Elementordnungen unter Isomorphismen erhalten bleiben, erhalten wir $\mathrm{ggT}(m,n) = 1 \Leftrightarrow \mathrm{ord}(\alpha^m) = n$. Mit Aufgabe 2 folgt nun, dass es genau $\varphi(n)$ primitive n-te Einheitswurzeln gibt. □

b) Beweisen Sie, dass $t^n - 1 = \prod_{d|n} \Phi_d(t)$ wobei

$$\Phi_d(t) = \prod_{i=1}^{\varphi(d)} (t - \alpha_{d,i}).$$

$\Phi_d(t)$ ist also das Produkt der linear Faktoren aus den d-ten primitiven Einheitswurzeln.
Wir nutzen die Tatsache, dass $\alpha_n := e^{2\pi i/n}$ primitive n-te Einheitswurzeln sind. Sei α_n^k eine n-te Einheitswurzel mit $\mathrm{ggT}(n,k) = 1$, nach vorheriger Überlegung ist α_n^k auch eine primitive n-te Einheitswurzel. Sei nun $\mathrm{ggT}(n,k) = t > 1$, dann gibt es ganze Zahlen, so dass $n = dt$, $k = lt$. Damit erhalten wir

$$\alpha_n^k = e^{\frac{2k\pi i}{n}} = e^{\frac{2lt\pi i}{dt}} = e^{\frac{2l\pi i}{d}} = \alpha_d^l.$$

Zudem gilt $\mathrm{ggT}(d,l) = 1$[†], also ist $\alpha_d^l = \alpha_n^k$ eine d-te primitive Einheitswurzel. Jede n-te Einheitswurzel ist also für einen Teiler $d|n$ eine d-te primitive Einheitswurzel und daher Nullstelle von $\Phi_d(t)$ für einen Teiler d.
Sei nun $d|n$ ein Teiler von $n = dt$ und α eine Nullstelle von $\Phi_d(t)$. Dann ist klar $\alpha^n = (\alpha^d)^t = 1^t = 1$, also ist α n-te Einheitswurzel.

Wir haben nun, dass jede Nullstelle von $t^n - 1$ eine Nullstelle eines Polynom $\Phi_d(t)$ ist und umgekehrt. Somit sind beide Polynome gleich. □

[†] d und l erhalten wir durch Teilen von n und k durch $t = \mathrm{ggT}(n,k)$, also grade durch kürzen aller gemeinsamen Primfaktoren.

c) Beweisen Sie, dass Φ_n ein normiertes Polynom in $\mathbb{Z}[t]$ ist.
Wir führen den Beweis per Induktion über n. Das Polynom $\Phi_1(t) = t - 1 \in \mathbb{Z}[t]$ ist normiert. Für den Induktionsschritt betrachten wir das Polynom $t^n - 1$. Nach b) gilt

$$t^n - 1 = \Phi_n(t) \cdot \prod_{\substack{d|n \\ d<n}} \Phi_d(t) := \Phi_n(t) \cdot \Omega(t)$$

Nach Induktionsvoraussetzung sind die Faktoren $\Phi_d \in \mathbb{Z}[t]$ normiert, insbesondere ist auch das Produkt $\Omega(t)$ normiert und in $\mathbb{Z}[t]$. Division mit Rest in $\mathbb{Q}[t]$ gibt uns

$$q, r \in \mathbb{Q}[t] : t^n - 1 = q(t) \cdot \Omega(t) + r(t)$$

mit $\deg(\Omega) > \deg(r)$. Da nach b) die Nullstellen von Ω auch Nullstellen von $t^n - 1$ sind folgt $r = 0$. Es gilt also $q = \Phi_n \in \mathbb{Q}[t]$ und nach dem Lemma von Gauß ist Φ_n normiert und hat Koeffizienten in $\mathbb{Z}$. □

d) Sei $\alpha := e^{2\pi i/n}$ und $m_\alpha(t) \in \mathbb{Q}[t]$ das Minimalpolynom von α. Zeigen Sie, dass $m_\alpha \in \mathbb{Z}[t]$.
α ist eine primitive n-te Einheitswurzel, d.h. das $\Phi_n(\alpha) = 0$, insbesondere teilt das Minimalpolynom $m_\alpha | \Phi_n$. Da das Minimalpolynom per Definition normiert ist, sowie auch nach 3.c) Φ_n folgt nach dem Lemma von Gauß $\mathbb{Z}[t] \ni \Phi_n = m_\alpha \cdot g \Rightarrow m_\alpha, g \in \mathbb{Z}[t]$.

e) Sei β eine andere Nullstelle von m_α und p eine Primzahl mit $p \nmid n$. Dann zeigen Sie, dass β^p eine Nullstelle von m_α ist.
Sei β eine Nullstelle von m_α, dann ist β auch eine Nullstelle von Φ_n. β ist also eine primitive n-te Einheitswurzel und daher auch β^p. Beide sind Nullstellen von $t^n - 1$ und es gilt, dass das Minimalpolynom $m_\alpha | t^n - 1$ mit

$$t^n - 1 = m_\alpha(t) \cdot g(t), \qquad m_\alpha, g \in \mathbb{Z}[t]$$

Angenommen β^p ist keine Nullstelle von m_α, dann ist sie folglich Nullstelle von g. D.h. $g(\beta^p) = 0$ und daher ist β Nullstelle von dem Polynom $g(t^p)$. Da β eine Nullstelle von m_α ist, teilt dieses auch $g(t^p)$

$$g(t^p) = m_\alpha(t) \cdot h(t), \qquad m_\alpha, h \in \mathbb{Z}[t].$$

Wir reduzieren nun die Koeffizienten um p und erhalten, da in $\mathbb{F}_p$ $a^p = a$ und dank Frobenius $(a+b)^p = a^p + b^p$:

$$t^n - \overline{1} = \overline{m}_\alpha(t) \cdot \overline{g}(t) \quad \text{und} \quad \overline{g}(t)^p = \overline{g}(t^p) = \overline{m}_\alpha(t) \cdot \overline{h}(t)$$

Sei nun $\overline{\gamma} \in \overline{\mathbb{F}_p}$ eine Nullstelle von m_α dann ist $\overline{0} = \overline{m}_\alpha(\overline{\gamma}) = \overline{g}(\overline{\gamma})^p = \overline{g}(\overline{\gamma})$. $\overline{\gamma}$ ist also eine vielfache Nullstelle von $t^n - \overline{1}$. Jedoch ist die Ableitung von $(t^n - 1)' = \overline{n} t^{n-1}$ und offensichtlich hat diese nur Null als Nullstelle. $t^n - 1$ und dessen Ableitung haben also keine gemeinsamen Nullstellen daraus folgt, dass $t^n - 1$ separabel ist. Widerspruch zur vielfachen Nullstelle $\overline{\gamma}$. β^p ist also Nullstelle von m_α. □

f) Beweisen Sie, dass $\Phi_n = m_\alpha$ und insbesondere ist Φ_n irreduzibel.
Wir führen vorherige Überlegung weiter. Sei β eine beliebige n-te primitive Einheitswurzel. Es gilt also $\beta = \alpha^k$ wobei $\mathrm{ggT}(n, k) = 1$. Betrachte die Primfaktorzerlegung von $k = p_1 p_2 \cdots p_l$, dann ist $\alpha^k = ((\alpha^{p_1})^{p_2} \cdots)^{p_l}$.[‡] Nach 3.e) folgt nun, dass jede einzelne Potenz $\alpha^{p_1}, \alpha^{p_1 p_2}, \ldots, \alpha^k$ Nullstelle von m_α ist. Es folgt $\Phi_n | m_\alpha$ und mit 3.d) auch $m_\alpha | \Phi_n$. Da beide Polynome normiert sind folgt die Gleichheit. Als Minimalpolynom ist Φ_n irreduzibel. □

g) Berechnen Sie $[\mathbb{Q}(e^{2\pi i/n}) : \mathbb{Q}]$. Da wir bereits das Minimalpolynom von $e^{2\pi i/n}$ kennen und nach 3.f) dieses gleich Φ_n ist. Schauen wir in die Definition von Φ_n und sehen dass es $\varphi(n)$ verschiedene Nullstellen hat. Also ist der Erweiterungsgrad der einfachen Körpererweiterung

$$[\mathbb{Q}(e^{2\pi i/n}) : \mathbb{Q}] = \deg \Phi_n = \varphi(n)$$

□

[‡]Man beachte, dass die p_i nicht zwangsweise verschieden sind. Für jeden Primfaktor gilt in der Tat $\mathrm{ggT}(n, p_i) = 1$ auf Grund von $\mathrm{ggT}(n, k) = 1$