Anmerkungen und Lösungen zu

Einführung in die Algebra

Blatt 7

Jendrik Stelzner

Letzte Änderung: 11. Dezember 2017

Aufgabe 3

(a)

Für jedes $n \geq 1$ gilt

$$W_n = \{e^{2\pi ik/n} \mid k = 0, \dots, n-1\} \quad = \{\cos(2\pi k/n) + i \sin(2\pi k/n) \mid k = 0, \dots, n-1\}$$

Aus $\cos(2\pi/3) = \cos(4\pi/3) = -1/2$ und $\sin(2\pi/3) = \sqrt{3}/2$, $\sin(4\pi/3) = -\sqrt{3}/2$ folgen damit, dass

$$\begin{aligned} W_2 &= \{1, -1\}\,, \\ W_3 &= \left\{1, -\frac{1}{2} + i\frac{\sqrt{3}}{2}, -\frac{1}{2} - i\frac{\sqrt{3}}{2}\right\}\,, \\ W_4 &= \{1, i, -1, -i\}\,. \end{aligned}$$

(b)

Für alle $n \geq 1$ ist die Abbildung

$$\varphi_n \colon \mathbb{Z} \to \mathbb{C}^\times\,, \quad k \mapsto e^{2\pi ik/n}$$

ist ein Gruppenhomomorphismus mit $\operatorname{im} \varphi_n = W_n$ und $\ker \varphi = n\mathbb{Z}$. Somit ist W_n eine Untergruppe von $\mathbb{C}^\times$, und φ_n induziert nach der universellen Eigenschaft des Quotienten einen Gruppenisomorphismus

$$\mathbb{Z}/n \to W_n, \quad \overline{k} \mapsto \varphi_n(k) = e^{2\pi ik/n}.$$

Die Abbildung

$$\varphi_\infty\colon \mathbb{Q} \to \mathbb{C}^\times\,, \quad \frac{p}{q} \mapsto e^{2\pi i p/q}\,,$$

ist ein Gruppenhomomorphismus mit $\operatorname{im}\varphi_\infty = \bigcup_{n\geq 1} W_n =: W_\infty$ und $\ker \mathbb{Z}$. Somit ist W_∞ eine Untergruppe von $\mathbb{C}^\times$, und φ_∞ induziert nach der universellen Eigenschaft des Quotienten einen Gruppenisomorphismus

$$\mathbb{Q}/\mathbb{Z} \to W_\infty\,, \quad \overline{\frac{p}{q}} \mapsto \varphi_\infty\left(\frac{p}{q}\right) = e^{2\pi i p/q}\,.$$

Bemerkung 1. Wir werden sehen, dass für einen beliebigen Körper K die Gruppe der Einheitswurzeln

$$W_n(K) \coloneqq \{x \in K \mid x^n = 1\}$$

zyklisch ist; dies wird daraus folgen, dass jede endliche Untergruppe $H \leq K^\times$ zylisch ist. Gilt $\operatorname{char}(K) = 0$, so hat die Gruppe $W_n(K)$ Ordnung n; gilt hingegen $\operatorname{char}(K) = p > 0$, und ist $n = p^r m$ mit $p \nmid m$, so hat die Gruppe $W_n(K)$ Ordnung m.

(c)

Entscheidend ist die folgende Beobachtung:

Lemma 2. *Für alle $n \geq 1$ gilt*

$$t^n - 1 = \prod_{d \mid n} \Phi_d(t)\,.$$

Beweis. Für $\zeta \in W_n$ sei $d \coloneqq \operatorname{ord}(\zeta)$. Es gilt $\zeta^d = 1$, weshalb ζ eine d-te Einheitswurzel ist, d.h. es gilt $\zeta \in W_d$. Da

$$\operatorname{ord}(\zeta) = d = \operatorname{ord}(W_d)$$

gilt, ist ζ bereits ein zyklischer Erzeuger von W_d. Also ist ζ eine primitive d-te Einheitswurzel. Zudem gilt

$$d = \operatorname{ord}(\zeta) \mid \operatorname{ord}(W_n) = n\,.$$

Damit erhalten wir ingesamt, dass

$$W_n = \coprod_{d \mid n} \{\zeta \in W_n \mid \operatorname{ord}(\zeta) = d\} = \coprod_{d \mid n} \{\zeta \in W_d \mid \zeta \text{ ist primitiv}\}\,.$$

(Hier steht $\coprod$ für die disjunkte Vereinigung.)

$$t^n - 1 = \prod_{\zeta \in W_n} (t - \zeta) = \prod_{d \mid n} \prod_{\substack{\zeta \in W_d \\ \text{primitiv}}} (t - \zeta) = \prod_{d \mid n} \Phi_d(t)\,.$$

Das zeigt die Gleichheit. $\square$

Bemerkung 3. Die obige Argumentation lässt sich dahingehend verallgemeinern, dass für jede Gruppe G die disjunkte Zerlegung

$$\begin{aligned} G &= \coprod_{H \leq G} \{h \in H \text{ ist ein zyklischer Erzeuger von } H\} \\ &= \coprod_{\substack{H \leq G \\ \text{zyklisch}}} \{h \in H \text{ ist ein Erzeuger von } H\} \end{aligned}$$

gilt. Dies ist nur eine Umformulierung der Tatsache, dass jedes Element $g \in G$ eine eindeutige (zyklische) Untergruppe $\langle g \rangle \leq G$ erzeugt.

Bemerkung 4. Aus Lemma 2 folgt insbesondere, dass für jede natürliche Zahl $n \geq 1$ die Gleichheit

$$n = \deg(t^n - 1) = \sum_{d|n} \deg \Phi_d(t) = \sum_{d|n} \phi(t),$$

gilt, wobei φ die Eulersche Phi-Funktion bezeichnet.

Aus der Vorlesung ist bereits bekannt, dass

$$\Phi_p(t) = t^{p-1} + t^{p-2} + \cdots + t + 1 = \frac{t^p - 1}{t - 1}$$

für jede Primzahl p. Aus Lemma 2 ergibt sich eine Verallgemeinerung dieser Gleichheit:

Korollar 5. *Für alle $n \geq 1$ gilt*

$$\Phi_n(t) = \frac{t^n - 1}{\prod_{d|n, d \neq n} \Phi_d(t)} \,.$$

Mithilfe von Korollar 5 und Polynomdivision lassen sich die Kreisteilungspolynome $\Phi_n(t)$ nun induktiv berechnen. Für $n = 1, \ldots, 8$ erhalten wir die folgenden Ergebnisse:

$$\begin{aligned}
&\Phi_1(t) = t - 1 \,, \\
&\Phi_2(t) = t + 1 \,, \\
&\Phi_3(t) = t^2 + t + 1 \,, \\
&\Phi_4(t) = \frac{t^4 - 1}{\Phi_1(t)\Phi_2(t)} = \frac{t^4 - 1}{(t-1)(t+1)} = \frac{t^4 - 1}{t^2 - 1} = t^2 + 1 \,, \\
&\Phi_5(t) = t^4 + t^3 + t^2 + t + 1 \,, \\
&\Phi_6(t) = \frac{t^6 - 1}{\Phi_1(t)\Phi_2(t)\Phi_3(t)} = \frac{t^6 - 1}{(t-1)(t+1)(t^2+t+1)} = \frac{t^6 - 1}{t^4 + t^3 - t - 1} = t^2 - t + 1 \,, \\
&\Phi_7(t) = t^6 + t^5 + t^4 + t^3 + t^2 + t + 1 \,, \\
&\Phi_8(t) = \frac{t^8 - 1}{\Phi_1(t)\Phi_2(t)\Phi_4(t)} = \frac{t^8 - 1}{(t-1)(t+1)(t^2+1)} = \frac{t^8 - 1}{t^4 - 1} = t^4 + 1 \,.
\end{aligned}$$

Bemerkung 6. Es fällt auf, dass alle bisher bekannten Kreisteilungspolynome (also $\Phi_p(t)$ mit p prim, und $\Phi_n(t)$ für $n = 1, \ldots, 8$) jeweils nur $1, 0, -1$ als Koeffizienten haben. Dieses Muster setzt sich bis $\Phi_{104}(t)$ vor; das Kreisteilungspolynome $\Phi_{105}(t)$ hat schließlich den Koeffizienten -2.