Anmerkungen und Lösungen zu

Einführung in die Algebra

Blatt 7

Jendrik Stelzner

Letzte Änderung: 16. Dezember 2017

Aufgabe 3

Für alle $n \geq 1$ schreiben im Folgenden

$$\mu_n \coloneqq \{\zeta \in W_n \mid \zeta \text{ ist eine primitive } n\text{-te Einheitswurzel}\}\,.$$

(a)

Für jedes $n \geq 1$ gilt

$$\begin{aligned} W_n &= \left\{ e^{2\pi i k/n} \,\middle|\, k = 0, \dots, n-1 \right\} \\ &= \{\cos(2\pi k/n) + i \sin(2\pi k/n) \mid k = 0, \dots, n-1\}\,. \end{aligned}$$

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

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

ein Gruppenhomomorphismus mit $\operatorname{im} f_n = W_n$ und $\ker f_n = n\mathbb{Z}$. Somit ist W_n eine Untergruppe von $\mathbb{C}^\times$, und f_n induziert nach dem ersten Isomorphiesatz einen Gruppenisomorphismus

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

Die Abbildung

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

ist ein Gruppenhomomorphismus mit $\operatorname{im} f_\infty = \bigcup_{n \geq 1} W_n =: W_\infty$ und $\ker f_\infty = \mathbb{Z}$. Somit ist W_∞ eine Untergruppe von $\mathbb{C}^\times$, und f_∞ induziert nach dem ersten Isomorphiesatz einen Gruppenisomorphismus

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

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

$$W_n = \coprod_{d \mid n} \{\zeta \in W_n \mid \operatorname{ord}(\zeta) = d\} = \coprod_{d \mid n} \mu_n$$

gilt. (Hier steht $\coprod$ für die disjunkte Vereinigung.) Es folgt, dass

$$t^n - 1 = \prod_{\zeta \in W_n} (t - \zeta) = \prod_{d \mid n} \prod_{\zeta \in \mu_d} (t - \zeta) = \prod_{d \mid n} \Phi_d(t)$$

gilt. Das zeigt die Gleichheit. □

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 von G erzeugt (nämlich $\langle g \rangle$).

Bemerkung 4. Aus Lemma 2 folgt für jede natürliche Zahl $n \geq 1$ die Identität

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

wobei φ die Eulersche Phi-Funktion bezeichnet.

Aus der Vorlesung ist bereits bekannt, dass für jede Primzahle p das Kreisteilungspolynom $\Phi_p(t)$ durch

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

gegeben ist. Aus Lemma 2 ergibt sich eine Verallgemeinerung dieser Formel:

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 $n = 1, \dots, 8$) jeweils nur $1, 0, -1$ als Koeffizienten haben. Dieses Muster setzt sich bis $\Phi_{104}(t)$ vor. Das Kreisteilungspolynome $\Phi_{105}(t)$ hingegen hat den Koeffizienten -2.

(d)

Wir geben zwei mögliche Beweise.

Möglichkeit 1: Durch primitive Einheitswurzeln

Entscheidend ist die Beobachtung, dass für alle $\zeta \in \mathbb{C}$ die Äquivalenz

$$\zeta \in W_{np} \iff \zeta^p \in W_n$$

gilt. Die Bedingung $p \mid n$ sorgt dafür, dass sich diese Äquivalenz auf die primitiven Einheitswurzeln einschränkt:

Behauptung 1. *Eine Einheitswurzel $\zeta \in W_{np}$ ist genau dann primitiv, wenn $\zeta^p \in W_n$ primitiv ist.*

Beweis. Wir geben zwei mögliche Beweise:

- Ist $\zeta \in W_{np}$ primitiv, so gilt $\operatorname{ord}(\zeta) = np$, und somit

  $$\operatorname{ord}(\zeta^p) = \frac{\operatorname{kgV}(\operatorname{ord}(\zeta), p)}{p} = \frac{\operatorname{kgV}(np, p)}{p} = \frac{np}{p} = n\,.$$

  Also ist auch $\zeta^p \in W_n$ primitiv.

  Ist andererseits $\zeta \in W_{np}$ nicht primitiv, so gilt $\operatorname{ord}(\zeta) < np$. Also ist $\operatorname{ord}(\zeta)$ dann ein echter Teiler von np. Es gibt daher einen echten Teiler d von np mit $\operatorname{ord}(\zeta) \mid d$, so dass np/d prim ist (während $\operatorname{ord}(\zeta)$ einige Primfaktoren von np fehlen, fehlt d nur noch ein Primfaktor). Es gilt $p \mid n$, weshalb der Primfaktor p in np mindestens zweimal vorkommt; somit muss er in d mindestens einmal vorkommen, weshalb $p \mid d$ gilt. Aus $\operatorname{ord}(\zeta) \mid d$ folgt $\zeta^d = 1$, und aus $p \mid d$ folgt damit, dass $(\zeta^p)^{d/p} = 1$ gilt. Deshalb gilt $\operatorname{ord}(\zeta) = d/p < np/p = n$. Also ist ζ^p keine primitive n-te Einheitswurzel.

- Mit den Isomorphismen

  $$\varphi\colon \mathbb{Z}/(np) \to W_{np}\,, \quad \overline{k} \mapsto e^{2\pi i k/(np)}$$

  und

  $$\psi\colon \mathbb{Z}/n \to W_n\,, \quad \overline{k} \mapsto e^{2\pi i k/n}$$

  erhalten wir für die Gruppenhomomorphismen

  $$f\colon W_{np} \to W_n\,, \quad \zeta \mapsto \zeta^p$$

und

$$g\colon \mathbb{Z}/(np) \to \mathbb{Z}/n\,, \quad \overline{k} \mapsto \overline{k}$$

das folgende kommutative Diagramm:

$$\begin{array}{ccc} W_{np} & \xrightarrow{f} & W_n \\ {\scriptstyle\varphi}\uparrow & & \uparrow{\scriptstyle\psi} \\ \mathbb{Z}/(np) & \xrightarrow{g} & \mathbb{Z}/n \end{array}$$

Somit erhalten wir, dass

$$\begin{aligned} & (\zeta \in W_{np} \text{ ist primitiv } \iff \zeta^p \in W_n \text{ ist primitiv}) \\ \iff & (\zeta \in W_{np} \text{ ist ein zykl. Erzeuger } \iff \zeta^p \in W_n \text{ ist ein zykl. Erzeuger}) \\ \iff & (\overline{k} \in \mathbb{Z}/(np) \text{ ist ein zykl. Erzeuger } \iff \overline{k} \in \mathbb{Z}/n \text{ ist ein zkyl. Erzeuger}) \\ \iff & (k \text{ und } np \text{ sind teilerfremd } \iff k \text{ und } n \text{ sind teilerfremd})\,. \end{aligned}$$

Da $p \mid n$ gilt, haben n und np die gleichen Primfaktoren, weshalb k und np genau dann teilerfremd sind, wenn k und n teilerfremd sind. □

Für den Gruppenhomomorphismus

$$f\colon W_{np} \to W_n\,, \quad \zeta \mapsto \zeta^p$$

gilt $\ker f = W_{np} \cap W_p = W_p$ mit $|W_p| = p$, weshalb für jedes $\xi \in W_n$ die Faser $f^{-1}(\xi)$ aus p Elementen besteht. Aus der obigen Behauptung folgt, dass sich f zu einer Abbildung

$$\tilde{f}\colon \mu_{np} \to \mu_n\,, \quad \zeta \mapsto f(\zeta) = \zeta^p$$

einschränkt, wobei für jedes $\xi \in W_n$ die Gleichheit $\tilde{f}^{-1}(\xi) = f^{-1}(\xi)$ gilt, und die Faser $f^{-1}(p)$ somit aus p Elementen besteht. Wir erhalten somit eine disjunkte Zerlegung

$$\mu_{np} = \coprod_{\xi \in \mu_n} \tilde{f}^{-1}(\xi) = \coprod_{\xi \in \mu_n} \{\zeta \in \mu_n \,|\, \zeta^p = \xi\}$$

in p-elementige Teilmengen. Somit gilt, dass

$$\Phi_{np}(t) = \prod_{\zeta \in \mu_{np}} (t - \zeta) = \prod_{\xi \in \mu_n} \prod_{\substack{\zeta \in \mu_{np} \\ \zeta^p = \xi}} (t - \zeta)\,. \tag{1}$$

Dabei besteht $\tilde{f}^{-1}(\xi) = \{\zeta \in \mu_{np} \,|\, \zeta^p = \xi\}$ aus Nullstellen des Polynoms $t^p - \xi$; da es sich zum p Nullstellen handelt, gilt bereits

$$t^p - \xi = \prod_{\substack{\zeta \in \mu_{np} \\ \zeta^p = \xi}} (t - \zeta)\,.$$

Damit erhalten wir aus (1), dass

$$\Phi_{np}(t) = \prod_{\xi \in \mu_n} (t^p - \xi) = \Phi_n(t^p)\,.$$

Möglichkeit 2: Mithilfe der Eulerschen Phi-Funktion

Über $\mathbb{C}$ zerfallen die Polynome $\Phi_{np}(t)$ und $\Phi_n(t^p)$ in Linearfaktoren; es genügt daher zu zeigen, dass beide Polynome die gleichen Linearfaktoren mit jeweils gleicher Vielfachheit haben.

Es gilt $\Phi_{np}(t^p) = \prod_{\zeta\in\mu_{np}}(t-\zeta)$. Für jede primitive (np)-te Einheitswurzel $\zeta \in \mu_{np}$ ist ζ^p eine primitive n-te Einheitswurzel, also $\zeta^p \in \mu_n$. Somit ist ζ dann eine Nullstelle von $\Phi_n(t) = \prod_{\xi\in\mu_n}(t^p - \xi)$. Das zeigt, dass jeder Linearfaktor von $\Phi_{np}(t)$ auch in $\Phi_n(t^p)$ auftritt.

Da jeder Linearfaktor in $\Phi_{np}(t)$ Vielfachheit 1 hat, genügt es nun zu zeigen, dass $\deg \Phi_{np}(t) = \deg \Phi_n(t^p)$ gilt. Ist $n = p_1^{\nu_1} p_2^{\nu_2} \cdots p_r^{\nu_r}$ die Primfaktorzerlegung von n mit $p_1 = p$ (und $p_i \neq p_j$ für $i \neq j$, sowie $\nu_i \geq 0$ für alle i), so ist $np = p_1^{\nu_1+1} p_2^{\nu_2} \cdots p_r^{\nu_r}$ die Primfaktorzerlegung von np. Es gilt deshalb

$$\begin{aligned}
\deg \Phi_{np}(t) &= \varphi(np) \\
&= \varphi(p_1^{\nu_1+1} p_2^{\nu_2} \cdots p_r^{\nu_r}) \\
&= \varphi(p_1^{\nu_1+1})\varphi(p_2^{\nu_2}) \cdots \varphi(p_r^{\nu_r}) \\
&= (p_1^{\nu_1+1} - p_1^{\nu_1}) \cdot (p_2^{\nu_2} - p_2^{\nu_2-1}) \cdots (p_r^{\nu_r} - p_r^{\nu_r-1}) \\
&= p_1(p_1^{\nu_1} - p_1^{\nu_1-1}) \cdot (p_2^{\nu_2} - p_2^{\nu_2-1}) \cdots (p_r^{\nu_r} - p_r^{\nu_r-1}) \\
&= \cdots \\
&= p_1\varphi(n) = p\,\varphi(n) = p \deg \Phi_n(t) = \deg \Phi_n(t^p)\,.
\end{aligned}$$

Explizite Formel für $\Phi_{p^k}(t)$

Damit ergibt sich nun für alle $k \geq 1$, dass

$$\Phi_{p^k}(t) = \Phi_{p^{k-1}}(t^p) = \Phi_{p^{k-2}}((t^p)^p) = \Phi_{p^{k-2}}\left(t^{(p^2)}\right) = \cdots = \Phi_p\left(t^{(p^{k-1})}\right)\,,$$

und mit $\Phi_p(t) = \sum_{\ell=0}^{p-1} t^\ell$ somit die Identität

$$\Phi_{p^k}(t) = \sum_{\ell=0}^{p-1}\left(t^{(p^{k-1})}\right)^\ell = \sum_{\}ll=0}^{p-1} t^{\ell p^{(k-1)}}\,.$$

(e)

Da $\mathbb{Q}$ ein Körper ist, gibt es eindeutige Polynome $q, r \in \mathbb{Q}[t]$ mit den gewünschten Bedingungen. Das Polynom q lässt sich durch Polynomdivision von g durch f ausrechnen. Die Rechenoperationen, die dabei in $\mathbb{Q}[t]$ verwendet werden, sind

- Ringoperationen, d.h. Addition, Subtraktion und Multiplikation, und
- Division durch den Leitkoeffizienten von f.

Da f nomiert sind, verlassen wir ausgehend von $g \in \mathbb{Z}[t]$ dabei den Ring $\mathbb{Z}[t]$ nicht. Somit ergibt sich, dass bereits $g \in \mathbb{Z}[t]$ gilt. Damit gilt auch $r = g - qf \in \mathbb{Z}[t]$.

Das zeigt die Existenz und Eindeutig der gewünschten Polynome $q, r \in \mathbb{Z}[t]$; sie können durch die übliche Polynomdivision berechnet werden.

(f)

Die Normiertheit von $\Phi_n(t)$ ergibt sich dadurch, dass es sich (per Definition) um ein Produkt von Linearfaktoren handelt. Dass bereits $\Phi_n(t) \in \mathbb{Z}[t]$ gilt, ergibt sich induktiv: Wir wissen bereits, dass $\Phi_1(t) \in \mathbb{Z}[t]$ gilt. Für alle $n > 1$ haben wir nach Korollar 5, dass

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

gilt. Die die Polynome $\Phi_d(t)$ mit $d \mid n$, $d < n$ normiert und nach Induktionsvoraussetzung ganzzahlig sind, ist auch $\prod_{d \mid n, d \neq n} \Phi_d(t)$ normiert und ganzzahlig. Aus dem vorherigen Aufgabenteil ergibt sich damit, dass auch $\Phi_n(t)$ bereits ganzzahlig ist.