Lösungsvorschlag zu Aufgabe 2 auf Blatt 6

Voraussetzung: Es sei $c \in \mathbb{C}$ gegeben und $I := \big((X-c)^2\big) = (X^2 - 2cX + c^2) \subseteq \mathbb{C}[X]$.

Behauptung:

(a) $\forall n \in \mathbb{N} : \forall k \in \{1, \dots, n\} : \; X^n - 1 \equiv_I kc^{k-1}X^{n-k+1} - (k-1)c^kX^{n-k} - 1$.

(b) $\forall n \in \mathbb{N} : X^n - 1 \notin I$

(c) $\forall n \in \mathbb{N} : \#\{z \in \mathbb{C} \mid z^n = 1\} = n$

Beweis.

(a) Sei $n \in \mathbb{N}$ gegeben. Wir beweisen die Aussage

$$\forall k \in \{1, \dots, n\} : \; X^n - 1 \equiv_I kc^{k-1}X^{n-k+1} - (k-1)c^kX^{n-k} - 1 \tag{$*$}$$

per vollständiger Induktion nach k.

Induktionsanfang: ($k = 1$)

Für $k = 1$ gilt für die rechte Seite

$$\begin{aligned} kc^{k-1}X^{n-k+1} - (k-1)c^kX^{n-k} - 1 &= 1 \cdot c^{1-1} \cdot X^{n-1+1} - (1-1)x^1X^{n-1} - 1 \\ &= X^n - 1\,. \end{aligned}$$

Insbesondere ist dies natürlich auch kongruent zu $X^n - 1$ modulo I. Damit ist der Induktionsanfang gezeigt.

Induktionsschritt: ($k \rightsquigarrow k+1$)

Sei $k \in \{1, \dots, n-1\}$ gegeben. Wir nehmen an, dass

$$X^n - 1 \equiv_I kc^{k-1}X^{n-k+1} - (k-1)c^kX^{n-k} - 1 \tag{IV}$$

gilt (Induktionsvoraussetzung). Zu zeigen ist, dass dann auch

$$\begin{aligned} X^n - 1 &\equiv_I (k+1)c^{(k+1)-1}X^{n-(k+1)+1} - ((k+1)-1)c^{(k+1)}X^{n-(k+1)} - 1 \\ &= (k+1)c^kX^{n-k} - kc^{k+1}X^{n-k-1} - 1 \end{aligned}$$

gilt (Induktionsbehauptung).

Es gilt

$$X^2 - 2cX + c^2 \equiv_I 0 \quad \Longrightarrow \quad X^2 \equiv_I 2cX - c^2 = c(2X - c)\,. \tag{$**$}$$

Aus der Induktionsvoraussetzung folgt nun

$$\begin{aligned} X^n - 1 &\overset{\text{(IV)}}{\equiv_I} kc^{k-1}X^{n-k+1} - (k-1)c^kX^{n-k} - 1 \\ &= kc^{k-1}X^{n-k-1} \cdot X^2 - (k-1)c^kX^{n-k} - 1 \\ &\overset{(**)}{\equiv_I} kc^{k-1}X^{n-k-1} \cdot c(2X - c) - (k-1)c^kX^{n-k} - 1 \\ &= 2kc^kX^{n-k} - kc^{k+1}X^{n-k-1} - (k-1)c^kX^{n-k} - 1 \\ &= (k+1)c^kX^{n-k} - kc^{k+1}X^{n-k-1} - 1\,. \end{aligned}$$

Damit ist die Induktionsbehauptung gezeigt.

Aus dem Beweisprinzip der vollständigen Induktion folgt, dass $(*)$ gilt. Da $n \in \mathbb{N}$ beliebig war, ist damit die Behauptung gezeigt.

Die Idee im Induktionsschritt war, dass man mittels der Kongruenz $(**)$ jede X-Potenz durch eine um einen Grad niedrigere X-Potenz „ersetzen“ kann. Damit ließ sich das Polynom im „$(k+1)$-Fall“ auf jenes im „k-Fall“ zurückführen.

(b) Sei $n \in \mathbb{N}$ gegeben. Wir argumentieren per Widerspruchsbeweis und nehmen dazu an, dass $X^n - 1 \in I$ gilt. Nach Teil (1) gilt (mit $k = n$)

$$\begin{aligned} X^n - 1 &\equiv_I nc^{n-1}X^{n-n+1} - (n-1)c^n X^{n-n} - 1 \\ &= nc^{n-1}X - (n-1)c^n - 1\,, \end{aligned}$$

also ist auch das untere Polynom ein Element von I. Hieraus ergibt sich nun aber ein Widerspruch, denn obiges Polynom hat Grad 1 und jedes Element des Ideals I ist ein $\mathbb{C}[X]$-Vielfaches des Polynoms $(X-c)^2 = X^2 - 2cX + c^2$ (d.h. ist von der Form $q \cdot (X-c)^2$ für ein $q \in \mathbb{C}[X]$) und hat somit entweder Grad größergleich 2 oder Grad 0 (falls $q = 0$). Also muss doch $X^n - 1 \notin I$ gelten.

(c) Sei $n \in \mathbb{N}$ gegeben. Nach dem Fundamentalsatz der Algebra (Satz 4.2.12) bzw. nach Bemerkung 4.2.13 (a) existieren $a \in \mathbb{C}$ und $z_1, \ldots, z_n \in \mathbb{C}$ mit

$$X^n - 1 = a(X - z_1) \cdots (X - z_n)\,.$$

Es gilt nun offensichtlich $C_n = \{z_1, \ldots, z_n\}$. Um zu zeigen, dass $\#C_n = n$ gilt, müssen wir zeigen, dass $z_1, \ldots, z_n$ alle verschieden sind. Zwecks Widerspruch nehmen wir an, dies sei nicht der Fall. Indem wir gegebenenfalls die Zahlen $z_1, \ldots, z_n$ umnummerieren, dürfen wir annehmen, dass $z_1 = z_2$ gilt. Dann gilt

$$X^n - 1 = (X - z_1)^2 \cdot a(X - z_3)(X - z_4) \cdots (X - z_n) \in \left((X - z_1)^2\right).$$

Dies widerspricht aber Teil (b), denn das Element $c \in \mathbb{C}$ dort war ja beliebig (setze $c = z_1$). Also müssen $z_1, \ldots, z_n$ doch alle voneinander verschieden sein, womit $\#C_n = n$ gezeigt ist.

□