Aufgabe (26). *Finden Sie drei verschiedene normierte Primpolynome $f, g, h \in \mathbb{Z}_3[x]$ vom Grad 2 (Nachweis!) und dann jeweils ein Erzeugendes Element a, b und c der zyklischen Gruppen*

$$G_f = G(\mathbb{Z}_3[x]_{2,f}),\ G_g = G(\mathbb{Z}_3[x]_{2,g}) \text{ und } G_h = G(\mathbb{Z}_3[x]_{2,h}).$$

Ein Polynom vom Grad 2 ist genau dann irreduzibel, wenn es keine Nullstellen besitzt. Setzt man in das Polynom $f := x^2 + 1$ der Reihe nach die Elemente aus $\mathbb{Z}_3$ ein, so ergibt sich

$$f(0) = 1,\ f(1) = 2 \text{ und } f(2) = 4 + 1 \equiv_3 2.$$

Also ist das normierte Polynom f irreduzibel. Die Einsetzmorphismen π_{x+1} und π_{x+2} sind zueinander inverse Automorphismen von $\mathbb{Z}_3[x]$. Da Automorphismen die Irreduzibelität erhalten, sind auch

$$g := \pi_{x+1}(f) = f(x+1) = x^2 + 2x + 2 \ \text{ und } \ h := \pi_{x+2}(f) = f(x+2) = x^2 + x + 2$$

irreduzibel über $\mathbb{Z}_3[x]$. Offenbar sind beide ebenfalls normiert und f, g und h paarweise verschieden. Da weiterhin irreduzible Elemente in Hauptidealbereichen wie $\mathbb{Z}_3[x]$ stets prim sind, ist der erste Teil der Aufgabe fertig.

Die Menge $K := \mathbb{Z}_3[x]_{2,f}$ enthält neun Elemente und ist ein Körper nach Beispiel 1 in § 12. Damit sind alle Elemente außer der Null Einheiten, und es gelten $|G_f| = 8$ und analog $|G_g| = |G_h| = 8$. Ein Element $a \in G_f$ ist also genau dann ein Erzeuger, wenn seine Ordnung $\operatorname{ord}(a) = 8$ ist.

Da K ein Körper ist, hat das Polynom $y^2 + 2 \in K[y]$ genau zwei Nullstellen, nämlich die Elemente 1 und $2 \in K$. Also sind die einzigen Elemente einer Ordnung von 2 oder weniger in G_f gerade 1 und 2. Ein Element besitzt genau dann die Ordnung 8, wenn sein Quadrat die Ordnung 4 besitzt, also nicht 1 oder 2 ist.[1]

Damit ist nun $a := x + 1 \in K$ ein Erzeuger von G_f, denn es ist

$$a^2 = x^2 + 2x + 1 \equiv_f 2x \notin \{1, 2\}\ .$$

Analog sind $b := x \in \mathbb{Z}_3[x]_{2,g}$ bzw. $c := x \in \mathbb{Z}_3[x]_{2,h}$ Erzeuger von G_g bzw. G_h, denn es ist

$$b^2 = x^2 \equiv_g x + 1 \notin \{1, 2\} \ \text{ bzw. } \ c^2 = x^2 \equiv_h 2x + 1 \notin \{1, 2\}\ .$$

[1] Man beachte, dass wegen dem Satz von Lagrange (Folgerung 6 in § 2) überhaupt nur die Ordnungen 1, 2, 4 oder 8 auftreten können.