Aufgabe F20T3A5

Wir betrachten das Polynom $f_1 := x^5 + 10x + 5$ in $\mathbb{Q}[x]$ und definieren induktiv Polynome $f_n(x) := f_1(f_{n-1}(x))$ für $n \in \mathbb{N}$ mit $n \geq 2$. Zeigen Sie, dass die Polynome f_n für alle $n \in \mathbb{N}$ irreduzibel sind. Zeigen Sie dazu folgende Zwischenschritte durch Induktion nach n:

(a) f_n liegt in $\mathbb{Z}[x]$, und die Klasse von f_n in $\mathbb{Z}/5\mathbb{Z}[x]$ ist durch x^{5^n} gegeben.

(b) Zeigen Sie, dass die Klasse von $f_n(0)$ in $\mathbb{Z}/25\mathbb{Z}$ nicht verschwindet.

Lösung:

zu (a) Für alle $n \in \mathbb{N}$ sei $\bar{f}_n$ jeweils das Bild von $f_n \in \mathbb{Z}[x]$ in $\mathbb{Z}/5\mathbb{Z}[x]$. Wir beweisen nun die angegebene Aussage durch vollständige Induktion nach n. Das Polynom f_1 ist nach Definition in $\mathbb{Z}[x]$ enthalten und das Bild von f_1 in $\mathbb{Z}/5\mathbb{Z}[x]$ ist gegeben durch $\bar{f}_1 = x^5 + \overline{10}x + \bar{5} = x^5 = x^{5^1}$. Damit ist die Aussage für $n = 1$ bewiesen. Sei nun $n \in \mathbb{N}$, und setzen wir die Aussage für n voraus. Dann gilt also $f_n \in \mathbb{Z}[x]$ und $\bar{f}_n = x^{5^n}$. Allgemein gilt: Setzt man in ein Polynom $f \in \mathbb{Z}[x]$ ein Polynom $g \in Z[x]$ ein, dann ist $f(g(x))$ wiederum in $\mathbb{Z}[x]$ enthalten. Daraus folgt $f_{n+1}(x) = f_1(f_n(x)) \in \mathbb{Z}[x]$. Betrachten wir auf beiden Seiten dieser Gleichung das Bild in $\mathbb{Z}/5\mathbb{Z}[x]$, so erhalten wir $\bar{f}_{n+1}(x) = \bar{f}_1(\bar{f}_n(x)) = \bar{f}_n(x)^5 + \overline{10}\bar{f}_n(x) + \bar{5} = \bar{f}_n(x)^5 = (x^{5^n})^5 = x^{5^{n+1}}$. Damit ist die Aussage für $n + 1$ bewiesen.

zu (b) Hier beweisen wir durch vollständige Induktion über n, dass $f_n(0)$ jeweils zwar durch 5, aber nicht durch 25 teilbar ist. Daraus ergibt sich unmittelbar, dass das Bild von $f_n(0)$ in $\mathbb{Z}/25\mathbb{Z}$ ungleich null ist. Für $n = 1$ ist die Aussage wegen $f_1(0) = 5$, $5 \mid 5$ und $25 \nmid 5$ offenbar erfült. Sei nun $n \in \mathbb{N}$, und setzen wir die Aussage für n voraus. Dann gilt laut Annahme $5 \mid f_n(0)$ und $25 \nmid f_n(0)$. Nach Definition ist $f_{n+1}(x) = f_1(f_n(x))$ und somit $f_{n+1}(0) = f_1(f_n(0)) = f_n(0)^5 + 10f_n(0) + 5$. Wegen $5 \mid f_n(0)$ ist $f_n(0)^5$ durch 5^5 und somit erst recht durch 25 teilbar. Aus $5 \mid f_n(0)$ und $5 \mid 10$ folgt auch $25 \mid 10f_n(0)$. Damit gilt insgesamt $f_{n+1}(0) \equiv 5 \bmod 25$. Dies zeigt, dass auch $f_{n+1}(0)$ zwar durch 5, aber nicht durch 25 teilbar ist.

Die Irreduzibilität von f_n für alle $n \in \mathbb{N}$ folgt nun aus dem Eisenstein-Kriterium. Um nachzuweisen, dass die Voraussetzungen dieses Kriteriums jeweils erfüllt sind, zeigen wir noch durch vollständige Induktion, dass x^{5^n} jeweils der Leitterm von f_n, das Polynom also insbesondere normiert ist. Für f_1 ist dies offenbar erfüllt, der Leitterm ist x^5. Sei nun $n \in \mathbb{N}$, und setzen wir voraus, dass x^{5^n} der Leitterm von f_n ist. Es ist $f_{n+1} = f_n^5 + 10f_n + 5$. Nach Induktionsvoraussetzung ist f_n vom Grad 5^n, also ist f_n^5 vom Grad $5 \cdot 5^n = 5^{n+1}$ und $10f_n$ vom Grad 5^n. Der Leitterm von f_{n+1} ist also gleich dem Leitterm von f_n^5, und dieser ist durch $(x^{5^n})^5 = x^{5^{n+1}}$ gegeben.

Jedes f_n ist also normiert vom Grad 5^n, x^{5^n} ist der Leitterm und 1 der Leitkoeffizient. Weil das Bild von f_n in $\mathbb{Z}/5\mathbb{Z}[x]$ nach Teil (a) gleich x^{5^n} ist, sind alle übrigen Koeffizienten von f_n durch 5 teilbar. Nach Teil (b) ist der konstante Termn $f_n(0)$ aber nicht durch 25 teilbar. Also sind tatsächlich alle Voraussetzungen des Eisenstein-Kriteriums erfüllt.