A. Zvonareva, M. Künzer

Schulmathematik, SoSe 22

Lösung 5

Aufgabe 17 (Lemma von Gauß)
Sei $f(X) = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X] \setminus \{0\}$. Es heißt $f(X)$ *primitiv*, falls $\mathrm{ggT}(a_0, \ldots, a_n) = 1$ ist. Es heißt $f(X)$ *irreduzibel*, wenn $f(X) \notin \{-1, +1\}$, wenn aber in einer Zerlegung $f(X) = g(X) \cdot h(X)$ mit $g(X)$, $h(X) \in \mathbb{Z}[X]$ entweder $g(X) \in \{-1, +1\}$ oder $h(X) \in \{-1, +1\}$ ist. Kurz, wenn man $f(X)$ in $\mathbb{Z}[X]$ nur trivial in Faktoren zerlegen kann.

(1) Seien $g(X) = \sum_{j=0}^{\ell} b_j X^j$, $h(X) = \sum_{k=0}^{m} c_k X^k \in \mathbb{Z}[X] \setminus \{0\}$ primitiv.

Betrachten Sie eine Primzahl p. Sei $\hat{j} \geqslant 0$ minimal mit p teilt nicht $b_{\hat{j}}$. Sei $\hat{k} \geqslant 0$ minimal mit p teilt nicht $c_{\hat{k}}$. Zeigen Sie: p teilt nicht den Koeffizienten von $X^{\hat{j}+\hat{k}}$ in $g(X) \cdot h(X)$.

Beweisen Sie damit: $g(X) \cdot h(X)$ ist primitiv.

(2) Sei $f(X) \in \mathbb{Z}[X] \setminus \{0\}$ ein primitives Polynom von Grad $\geqslant 1$.

Beweisen Sie: Ist $f(X) = g(X) \cdot h(X)$ mit $g(X)$, $h(X) \in \mathbb{Q}[X]$ und sind u, $v \in \mathbb{Q} \setminus \{0\}$ mit $u \cdot g(X)$, $v \cdot h(X) \in \mathbb{Z}[X]$ primitiv gewählt, dann sind $f(X)$ und $u \cdot v \cdot f(X)$ primitiv. Folgern Sie: $u \cdot v \in \{-1, +1\}$.

Beweisen Sie damit: $f(X)$ ist genau dann in $\mathbb{Z}[X]$ irreduzibel, wenn $f(X)$ in $\mathbb{Q}[X]$ irreduzibel ist.

Lösung zu Aufgabe 17:

(1) Sei $f(X) = \sum_{i=0}^{n} a_i X^i = g(X)h(X)$ und sei p, $b_{\hat{j}}$, $c_{\hat{k}}$ wie oben. Dann

$$a_{\hat{j}+\hat{k}} = \sum_{j+k=\hat{j}+\hat{k}} b_j c_k = \cdots + b_{\hat{j}-1} c_{\hat{k}+1} + b_{\hat{j}} c_{\hat{k}} + b_{\hat{j}+1} c_{\hat{k}-1} + \ldots$$

Wenn p alle b_j mit $j < \hat{j}$ und alle c_k mit $k < \hat{k}$ teilt, dann teilt p alle Summanden $b_j c_k$ von $a_{\hat{j}+\hat{k}}$ außer $b_{\hat{j}} c_{\hat{k}}$. Da p weder $b_{\hat{j}}$ noch $c_{\hat{k}}$ teilt, teilt p das Produkt $b_{\hat{j}} c_{\hat{k}}$ auch nicht. Wir bekommen: p teilt nicht $a_{\hat{j}+\hat{k}}$.

Sei $g(X)$, $h(X)$ primitiv. Das Polynom $f(X) = g(X)h(X)$ ist nicht gleich Null, da $g(X) \neq 0$, $h(X) \neq 0$. Nehmen wir an, dass $f(X)$ nicht primitiv ist. Das bedeutet, dass $\mathrm{ggT}(a_0, \ldots, a_n) \neq 1$ und dass es eine Primzahl p gibt, die alle Koeffizienten $a_0, \ldots, a_n$ teilt. Da $g(X)$ und $h(X)$ primitiv sind, gibt es minimale $\hat{j} \geqslant 0$, sodass $p \nmid b_{\hat{j}}$ und minimale $\hat{k} \geqslant 0$, sodass $p \nmid c_{\hat{k}}$. Dann teilt p auch nicht $a_{\hat{j}+\hat{k}}$, und wir bekommen einen Wiederspruch.

(2) Nach dem Teil (1), wenn $u \cdot g(X)$, $v \cdot h(X)$ primitiv sind, ist $u \cdot v \cdot f(X) = u \cdot g(X) \cdot v \cdot h(X)$ auch primitiv. Da $f(X)$ primitiv ist, gibt es keine $q \in \mathbb{Z} \setminus \{\pm 1\}$, sodass q die Zahlen $a_0, \ldots, a_n$ teilt. Also: $u \cdot v = \frac{p}{q} \in \mathbb{Q}$ muss eine ganze Zahl sein (da $u \cdot v \cdot f(X) \in \mathbb{Z}[X]$). Das Produkt $u \cdot v$ kann aber keinen Teiler p außer ± 1 haben, sonst ist p auch der Teiler aller Koeffizienten von $u \cdot v \cdot f(X)$, was im Wiederspruch damit steht, dass $u \cdot v \cdot f(X)$ primitiv ist. Wir bekommen: $u \cdot v \in \{\pm 1\}$.

Beweisen wir nun: $f(X)$ ist genau dann in $\mathbb{Z}[X]$ irreduzibel, wenn $f(X)$ in $\mathbb{Q}[X]$ irreduzibel ist. Wenn $f(X)$ in $\mathbb{Q}[X]$ irreduzibel ist, und $f(X) = g(X)h(X)$ mit $g(X)$, $h(X)$ in $\mathbb{Z}[X]$, dann ist entweder $g(X)$ oder $h(X)$ invertierbar in $\mathbb{Q}[X]$, also ist entweder $g(X)$ oder

$h(X)$ ein Element aus $\mathbb{Z}$. Da $f(X)$ primitiv ist, heißt das, dass entweder $g(X)$ oder $h(X)$ gleich ± 1 ist und $f(X)$ in $\mathbb{Z}[X]$ irreduzibel ist. Nehmen wir jetzt an, dass $f(X)$ in $\mathbb{Z}[X]$ irreduzibel ist, aber in $\mathbb{Q}[X]$ eine Zerlegung $f(X) = g(X)h(X)$ hat (als Produkt von Polynomen von Grad ≥ 1). Es gibt $u \in \mathbb{Q}$, sodass $u \cdot g(X)$ primitiv ist. Z.B. können wir zuerst $g(X)$ mit dem Produkt von allen Nennern der Koeffizienten multiplizieren und dann durch den ggT der neuen Koeffizienten teilen. Genau so gibt es $v \in \mathbb{Q}$, sodass $v \cdot h(X)$ primitiv ist. Dann $u \cdot v \in \{\pm 1\}$, und $f(X) = u \cdot v \cdot (u \cdot g(X))(v \cdot h(X))$ ist eine Zerlegung im $\mathbb{Z}[X]$. Das liefert einen Wiederspruch. Also ist $f(X)$ im $\mathbb{Q}[X]$ irreduziebel.

Aufgabe 18 (Eisensteinkriterium)

Sei $f(X) = \sum_{j=0}^{n} a_j X^j \in \mathbb{Z}[X]$ ein normiertes Polynom von Grad $n \geqslant 1$. Es ist also $a_n = 1$.

Sei p eine Primzahl. Sei p ein Teiler der Koeffizienten $a_0, a_1, \ldots, a_{n-1}$. Sei p^2 kein Teiler des Koeffizienten a_0.

Beweisen Sie: Falls $g(X), h(X) \in \mathbb{Z}[X]$ von Grad $\geqslant 1$ vorliegen mit $f(X) = g(X) \cdot h(X)$, dann teilt p alle Koeffizienten von $g(X)$ und $h(X)$, ausgenommen die Leitkoeffizienten.

Beweisen Sie: $f(X)$ ist irreduzibel in $\mathbb{Z}[X]$.

Folgern Sie unter Verwendung von Aufgabe 17.(2): $f(X)$ ist irreduzibel in $\mathbb{Q}[X]$.

Lösung zu Aufgabe 18:

Wie in der Aufgabe 17 schreiben wir $g(X) = \sum_{j=0}^{\ell} b_j X^j$ und $h(X) = \sum_{k=0}^{m} c_k X^k$ auf. Seien $\hat{j} \geqslant 0$ der minimale Index, sodass p den Koeffizienten $b_{\hat{j}}$ nicht teilt, und $\hat{k} \geqslant 0$ der minimale Index, sodass p den Koeffizienten $c_{\hat{k}}$ nicht teilt. Dann teilt p nicht $a_{\hat{j}+\hat{k}}$, und $\hat{j} + \hat{k}$ muss gleich n sein. Daraus folgt: $\hat{j} = l$ und $\hat{k} = m$, und p teilt alle Koeffizienten von $g(X)$ und $h(X)$, ausgenommen die Leitkoeffizienten.

Das Polynom $f(X)$ ist primitiv, da $a_n = 1$. Nehmen wir an, dass $f(X)$ nicht irreduziebel in $\mathbb{Z}[X]$ ist. Das bedeutet, dass $f(X) = g(X)h(X)$ mit $g(X), h(X) \in \mathbb{Z}[X]$, Grad $g(X), h(X) \geqslant 1$ (wir können nicht $g(X) \in \mathbb{Z}, g(X) \neq \pm 1$ haben, da $f(X)$ primitiv ist). Wie oben teilt p alle Koeffizienten von $g(X)$ und $h(X)$, ausgenommen die Leitkoeffizienten. Das bedeutet: p^2 muss $b_0 c_0 = a_0$ teilen, und wir bekommen einen Wiederspruch. Also ist $f(X)$ in $\mathbb{Z}[X]$ irreduziebel. Nach der Aufgabe 17.(2): $f(X)$ ist irreduzibel in $\mathbb{Q}[X]$.

Aufgabe 19

(1) Zeigen Sie: $X^4 - 8X^3 + 12X^2 - 6X + 2$ ist irreduzibel in $\mathbb{Q}[X]$.

(2) Zeigen Sie: $X^5 - 12X^3 + 36X - 12$ ist irreduzibel in $\mathbb{Q}[X]$.

(3) Sei p eine Primzahl.

Zeigen Sie mit Eisensteinkriterium: $((X+1)^p - 1)/X$ ist irreduzibel in $\mathbb{Q}[X]$.

Folgern Sie: $(X^p - 1)/(X - 1)$ ist irreduzibel in $\mathbb{Q}[X]$.

Folgern Sie: $X^{p-1} + X^{p-2} + \ldots + X + 1$ ist irreduzibel in $\mathbb{Q}[X]$.

Bestimmen Sie das Minimalpolynom $\mu_{\zeta_p}(X)$.

Lösung zu Aufgabe 19:

(1) Für $f(X) = X^4 - 8X^3 + 12X^2 - 6X + 2$ können wir $p = 2$ nehmen, um den Eisensteinkriterium anzuwenden, denn 2 teilt $-8, 12, -6$ und 2, aber 4 teilt nicht 2. Also $f(X)$ ist irreduzibel in $\mathbb{Q}[X]$.

(2) Für $f(X) = X^5 - 12X^3 + 36X - 12$ können wir $p = 3$ nehmen, um den Eisensteinkriterium anzuwenden, denn 3 teilt $-12, 36$ und -12, aber 9 teilt nicht -12. Also $f(X)$ ist irreduzibel in $\mathbb{Q}[X]$.

(3)

$$f(X) = \frac{(X+1)^p - 1}{X} = \frac{\sum_{k=0}^{p} \binom{p}{k} X^{p-k} - 1}{X} = \sum_{k=0}^{p-1} \binom{p}{k} X^{p-k-1} \in \mathbb{Z}[X] \text{ von Grad } \geqslant 1.$$

Bezeichnen wir die Koeffizienten von $f(X)$ wie immer durch a_i, dann $f(X) = \sum_{i=0}^{p-1} a_i X^i$. Dann

$$a_{p-1} = \binom{p}{0} = \frac{p!}{0!p!} = 1;$$

$$a_0 = \binom{p}{p-1} = \frac{p!}{(p-1)!1!} = p \text{ ist durch } p \text{ aber nicht durch } p^2 \text{ teilbar;}$$

$$a_{p-k-1} = \binom{p}{k} = \frac{p!}{k!(p-k)!} \text{ ist durch } p \text{ für } k = 1, \ldots, p-2 \text{ teilbar.}$$

Nach Eisensteinkriterium ist $f(X)$ in $\mathbb{Q}[X]$ irreduziebel.

Sei $Y = X - 1$, dann $f(Y) = f(X-1) = (X^p - 1)/(X - 1)$. Wenn $f(Y)$ in $\mathbb{Q}[X]$ nicht irreduziebel wäre, hätten wir eine nicht triviale Zerlegung $f(Y) = g(Y)h(Y)$, aber dann auch eine nicht triviale Zerlegung $f(X) = f(Y+1) = g(Y+1)h(Y+1) = g(X)h(X)$. Das gäbe einen Wiederspruch. Also ist $f(X-1) = (X^p - 1)/(X - 1)$ irreduziebel in $\mathbb{Q}[X]$.

$$(X^{p-1} + X^{p-2} + \ldots + X + 1)(X - 1) = X^p + X^{p-1} + X^{p-2} + \ldots + X - X^{p-1} - X^{p-2} - \ldots - X - 1 = X^p - 1$$

$$\text{Also } X^{p-1} + X^{p-2} + \ldots + X + 1 = \frac{X^p - 1}{X - 1}.$$

Da ζ_p eine Nullstelle von $X^p - 1$ aber nicht von $X - 1$ ist, ist sie eine Nullstelle von $X^{p-1} + X^{p-2} + \ldots + X + 1$. Da $(X^p - 1)/(X - 1) = X^{p-1} + X^{p-2} + \ldots + X + 1$ irreduziebel ist, muss das das Minimalpolynom von ζ_p sein. Und

$$\mu_{\zeta_p}(X) = X^{p-1} + X^{p-2} + \ldots + X + 1.$$

Aufgabe 20 Sei $t \in \mathbb{C}$ transzendent. Sei $a \in \mathbb{C}$ algebraisch.
Beweisen Sie, dass die folgenden Zahlen transzendent sind.

(1) $t + a$

(2) $t \cdot a$, falls $a \neq 0$.

(3) $f(t)$, wobei $f(X) \in \mathbb{Q}[X]$ von Grad $\geqslant 1$.

Lösung zu Aufgabe 20:

(1) Wenn $t + a$ algebraisch wäre, hätten wir $t + a, a \in \overline{\mathbb{Q}}$ und auch $t = (t + a) - a \in \overline{\mathbb{Q}}$ (ein Wiederspruch). Also $t + a$ ist transzendent.

(2) Wenn $t \cdot a$ algebraisch wäre, hätten wir $t \cdot a, a \in \overline{\mathbb{Q}}$ und auch $t = (t \cdot a) \cdot a^{-1} \in \overline{\mathbb{Q}}$ (ein Wiederspruch). Also $t \cdot a$ ist transzendent.

(3) Nehmen wir an, dass $f(t)$ algebraisch ist. Dann existiert ein Polynom $g(X) \in \mathbb{Q}[X]$, Grad von $g(X) \geqslant 1$ so, dass $g(f(t)) = 0$. Das Polynom $g(f(X)) \in \mathbb{Q}[X]$ hat Grad $\geqslant 1$, folglich ist t algebraisch (ein Wiederspruch). Also $f(t)$ ist transzendent.