# Algebraische Zahlentheorie: [MTH-1483]

Ilia Pirashvili

Arbeitsblatt 4

## Aufgaben 4

*Aufgabe* 1 (1 Punkt). Sei $f(x) \in K[X]$ ein Polynom. Beweise, dass es genau dann irreduzibel ist, wenn $f(x+a), a \in K$ irreduzibel ist.

**Lösung.** Wir benutzen die Tatsache, dass aus $f(x) = g(x)h(x)$ folgt $f(x+a) = g(x+a)h(x+a)$. Anders gesagt, dass die Abbildung $K[X] \to K[X], f(x) \mapsto f(x+a)$ mit der Multiplikation verträglich ist (es ist ja auch wohlbekannt ein Ringhomomorphismus, sogar ein Isomorphismus).

Sei also $f(x)$ reduzibel. Daher, es gibt $g(x), h(x) \in K[X]$, mit $\mathsf{grad}(g(x)), \mathsf{grad}(h(x)) \geq 1$. Dann gilt auch $f(x+a) = g(x+a)h(x+a)$ und da $\mathsf{grad}(f(x)) = \mathsf{grad}(f(x+a))$ ist unser Beweis gegeben. □

*Aufgabe* 2 (2 Punkte). Beweise mithilfe von Eisensteins Kriterium, dass folgende Polynome irreduzibel sind:

(i) $x^4 + 2x^3 + 2x + 2$

(ii) $x^4 + 9$.

**Lösung.** (i) Man benutze einfach nur $p = 2$.

(ii) Natürlich kann man hier nicht einfach das Eisenstein Kriterium verwenden, da 3 die einzige Primzahl ist, welches 9 teilt, aber $3^2 \mid 9$ auch gilt. Hierzu verwenden wir die vorige Aufgabe 1 und beweisen, dass $f(x+1)$ irreduzibel ist. Es gilt $(x+1)^4 + 9 = x^4 + 4x^3 + 6x^2 + 4x + 10$. Nun können wir Eisenstein für $p = 2$ anwenden. □

*Aufgabe* 3 (3 Punkte). *Kreisteilungspolynome* bzw. *zyklotomische Polynome* sind die irreduziblen Teiler des Polynoms $x^n - 1 \in \mathbb{Z}[X]$. Diese werden mit $\Phi_n$ bezeichnet. Für den Fall $n = p$ Primzahl, sind diese besonders einfach (und wichtig). Basierend auf die vorige Aufgabe 1, beweise, dass

$$\Phi_p := x^{p-1} + x^{p-2} + \cdots + x^2 + x + 1.$$

Also, dass das obige Polynom $(1 + x + \cdots + x^{p-1})$ irreduzibel ist und ein Teiler von $x^p - 1$.

**Lösung.** Als erstes bemerken wir, dass

$$\Phi_p(x)(x-1) = (x^{p-1} + x^{p-2} + \cdots + x^2 + x + 1)(x-1) = x^p - 1.$$

Oder, anders gesagt,

$$\frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x^2 + x + 1.$$

Nun benutze wir die vorige Aufgabe für $a = 1$ und erhalten

$$\frac{(x+1)^p - 1}{(x+1) - 1} = \frac{(x+1)^p - 1}{x}.$$

Wir haben

$$(x+1)^p = x^p + \binom{p}{1}x^{p-1} + \binom{p}{2}x^{p-2} + \cdots + \binom{p}{p-2}x^2 + px + 1.$$

Daher

$$\begin{aligned}\Phi_p(x+1) &= \frac{(x+1)^p - 1}{(x+1)-1} = \frac{(x+1)^p - 1}{x} \\ &= \frac{x^p + \binom{p}{1}x^{p-1} + \binom{p}{2}x^{p-2} + \cdots + \binom{p}{p-2}x^2 + px + 1 - 1}{x} \\ &= x^{p-1} + \binom{p}{1}x^{p-2} + \cdots + \binom{p}{p-2}x + p.\end{aligned}$$

Dass $\binom{p}{k}$ ein Vielfaches von $p$ ist, wenn $p$ eine Primzahl ist, ist nicht schwer. Daher ist das Eisensteinkriterium für $p$ erfüllt. □

*Aufgabe* 4 (4 Punkte). Finde alle reduziblen Polynome (über $\mathbb{Q}$) der Form

$$t^5 + at^3 + bt + 1,$$

wobei $a, b \in \mathbb{Z}$.

**Lösung.** Ein Polynom vom Grad 5 kann nur in Polynome von Grad $1+4$ und $2+3$ zerfallen. Beim Grad $1+4$ muss $f(t)$ eine Lösung $\alpha$ haben.

Wie in der Vorlesung gezeigt, muss $\alpha$ ein Teiler von 1 sein, daher $\alpha = \pm 1$. Also, $f(\pm 1) = 0$ muss gelten.

Bei $+1$ führt $f(1) = 0$ zu $a + b = -2$ und bei $-1$ führt es uns zu $a + b = 0$.

Sei nun $f = gh$ mit $\mathsf{grad}(g) = 2$, $\mathsf{grad}(h) = 3$. Also

$$t^5 + at^3 + bt + 1 = (t^2 + ct + d)(t^3 + pt^2 + qt + r).$$

Wir erhalten 5 Gleichungen

$$\begin{aligned}\text{I} &: dr = 1 \\ \text{II} &: cr + dq = b \\ \text{III} &: r + cq + dp = 0 \\ \text{IV} &: q + cp + d = a \\ \text{V} &: p + c = 0\end{aligned}$$

Gleichung I gibt uns zwei Möglichkeiten:

Möglichkeit 1:

$$\begin{aligned}\text{I} &: d = r = 1 \\ \text{II} &: c + q = b \Rightarrow q = b - c \\ \text{III} &: 1 + cq + p = 0 \\ \text{IV} &: q + cp + d = a \\ \text{V} &: p + c = 0 \Rightarrow p = -c\end{aligned}$$

was zu

$$\begin{aligned}\text{III}^* &: 1 + c(b-c) + p = 1 + c(b-c) - c = 0 \\ \text{IV}^* &: (b-c) + c(-c) + d = b - c - c^2 + d = a\end{aligned}$$

führt. Aus III $^*$ schließen wir, dass $c \mid 1$ und daher $c = \pm 1$.

Möglichkeit 1.1: Sei $c = 1$. Es folgt $b = 1$ (aus III $^*$), $p = -1$ und $q = a = 0$, also

$$(t^2 + t + a)(t^3 - t^2 + 1) = (t^5 + t + 1)$$

als die einzige Lösung.

Möglichkeit 1.2: Sei $c = -1$. Es folgt $p = b = 1$ und $q = a = 2$, also

$$(t^2 - t + 1)(t^3 + t^2 + 2t + 1) = t^5 + 2t^3 + t + 1$$

als die einzige Zerlegung.

Möglichkeit 2:

$$\begin{aligned} \text{I} &: d = r = -1 \\ \text{II} &: c + q = -b \Rightarrow -q = b + c \\ \text{III} &: 1 + p = cq \\ \text{IV} &: q + cp - 1 = a \\ \text{V} &: p + c = 0 \Rightarrow p = -c. \end{aligned}$$

Dies führt zu

$$\begin{aligned} \text{III}^* &: 1 - c = -c(b + c) \Rightarrow 1 = c(1 - b - c) \\ \text{IV}^* &: (b + c) + c^2 + 1 = -a. \end{aligned}$$

Aus III $^*$ können wir schließen, dass $c|1$ also $c = \pm 1$.

Möglichkeit 2.1: Sei $c = 1$. Wir erhalten $b = -1$ (aus III $^*$), $p = -1$, $a = -2$ und $q = 0$, daher

$$t^5 - 2t^3 - t + 1 = (t^2 + t - 1)(t^3 - t^2 - 1).$$

Möglichkeit 2.2: Sei $c = -1$. Wir erhalten $b = 3$ (aus III $^*$), $p = 1$, $a = -4$ und $q = -2$, daher

$$t^5 - 4t^3 + 3t + 1 = (t^2 - 1t - 1)(t^3 + t^2 - 2t - 1).$$

Zusammengefasst ergibt es die Möglichkeiten

$$\{(a, -2 - a)\} \cup \{(a, -a)\} \cup \{(0, 1)\} \cup \{(1, 2)\} \cup \{(-2, -1)\} \cup \{(-4, 3)\} \subseteq \mathbb{Z}^2.$$

□

*Aufgabe* 5 (2 Punkte). Ist das Polynom

$$x^6 + 7x^5 + 2x^2 + 18x + 28$$

irreduzibel? Wenn ja, beweise. Wenn nicht, faktorisiere es in irreduzible Komponente.

**Lösung.** Als erstes setzen wir die Teiler von 28 ein, da $f(x) = x^5 + 2x^2 + 4$ in unserem Fall normiert ist. Für normierte Polynome haben wir schon bewiesen, dass Wurzen über $\mathbb{Q}$ genau die Teiler des

freien Terms sind. Wenn man nun $-7$ einsetzt, bekommt man 0. Daher ist $x+7$ ein Teiler. Mit der Division von Polynomen (man erinnere sich, wie dies ging) erhalten wir

$$x^6 + 7x^5 + 2x^2 + 18x + 28 = (x^5 + 2x + 4)(x + 7).$$

Eisenstein für $p = 2$ kann man nicht anwenden, da $2^2 \mid 4$, aber wir wollen nun beweisen, dass $g(x) = x^5 + 2x + 4 \equiv x^5 + 2x + 1$ modulo 3 irreduzibel ist. Wir merken direkt, dass $x = -1.0, 1$ keine Wurzeln sind. Es bleibt also nur noch zu überprüfen, dass es nicht das Produkt von Polynomen vom Grad 2 und 3 sein kann. Sei dazu

$$x^5 + 2x + 4 \equiv x^5 + 2x + 1 = p(x)q(x) = (a_0 + a_1x + x^2)(b_0 + b_1x + b_2x^2 + x^3). \tag{1}$$

Indem wir ausmultiplizieren und die Koeffizienten gleichsetzten, erhalten wir

$$\begin{aligned} a_0b_0 &= 1 \\ a_0b_1 + a_1b_0 &= -1 \\ a_0b_2 + a_1b_1 + b_0 &= 0 \\ a_0 + a_1b_2 + b_1 &= 0 \\ a_1 + b_2 &= 0. \end{aligned}$$

Da $b_2 = -a_1$, können wir es zu

$$\begin{aligned} a_0b_0 &= 1 \\ a_0b_1 + a_1b_0 &= -1 \\ -a_0a_1 + a_1b_1 + b_0 &= 0 \\ a_0 - a_1^2 + b_1 &= 0 \end{aligned}$$

umformen. Wieder ersetzen wir $b_1$ mit $a_1^2 - a_0$, was uns

$$\begin{aligned} a_0b_0 &= 1 \\ a_0^2 - a_0a_1^2 - a_1b_0 &= 1 \\ a_0a_1 + a_1 + b_0 &= 0 \end{aligned}$$

ergibt. Hier haben wir $a_1^3 = a_1$ in $\mathbb{Z}/3\mathbb{Z}$ benutzt (und $-2a_0a_1 = a_0a_1$). Wiederum schreiben wir $b_0 = -a_1(a_0 + 1)$ und vereinfachen zu

$$\begin{aligned} -a_0a_1(a_0 + 1) &= 1 \\ a_0^2 + a_1^2 &= 1. \end{aligned}$$

Da wir wissen, dass $a_0b_0 = 1$, muss über $\mathbb{Z}/3\mathbb{Z}$ $a_0 = b_0 = \pm 1$ sein.

Fall 1: $a_0 = 1$. Wir erhalten

$$\begin{aligned} a_1 &= 1 \\ a_1^2 &= 0, \end{aligned}$$

was natürlich nicht geht, oder

fall 2: $a_0 = -1$, was uns von $-a_0a_1(a_0+1) = 1$, die Gleichung $0 = 1$ und somit auch ein Widerspruch liefert.

Daher kann $f(x)$ keinen Teiler vom Grad 2 haben und auch eine Wurzel und wir sind fertig. Die Zerlegung in irreduzible Komponente ist also □

*Aufgabe* 6 (2 Punkte). Sei $f(x) = a_0 + a_1x + \cdots + a_{n_1}x^{n-1} + a_nx^n$ irreduzibel. Beweise, dass auch $g(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$ irreduzibel ist. (*Tipp*: Man schreibe $g(x) = x^n f\left(\frac{1}{x}\right)$.)

**Lösung.** Sei $g(x) = p(x)q(x) = \left(p_0 + p_1x + \cdots + p_kx^k\right)\left(q_0 + q_1x + \cdots + q_{n-k}x^{n-k}\right)$, mit $\mathsf{grad}(p(x)) \geq 1$, $\mathsf{grad}(q(x)) \geq 1$. Dann gilt $x^n f\left(\frac{1}{x}\right) = p(x)q(x)$. Es folgt, dass

$$f\left(\frac{1}{x}\right) = \frac{p(x)q(x)}{x^n} = \frac{p(x)}{x^k}\frac{q(x)}{x^{n-k}} = \left(\frac{p_0}{x^k} + \frac{p_1}{x^{k-1}} + \cdots + \frac{p_k}{1}\right)\left(\frac{q_0}{x^{n-k}} + \frac{q_1}{x^{n-k-1}} + \cdots + \frac{q_{n-k}}{1}\right).$$

Indem wir einfach $\frac{1}{x}$ mit $y$ bezeichnen, haben wir nun, dass $f(y) = (p_0y^k + p_1y^{k-1} + \cdots + p_k)(q_0y^{n-k} + q_1y^{n-k-1} + \cdots + q_{n-k})$. Da $\mathsf{grad}(p_0y^k + p_1y^{k-1} + \cdots + p_k) = \mathsf{grad}(p(x))$ und $\mathsf{grad}(q_0y^{n-k} + q_1y^{n-k-1} + \cdots + q_{n-k}) = \mathsf{grad}(q(x))$ ist auch $f(x)$ reduzibel. Die Aussage folgt nun von der Tatsache, dass $x^n\left(g(\frac{1}{x}))\right) = x^n\left(\left(\frac{1}{x}\right)\right) = f(x)$. □