KAPITEL 13

Polynome

1. Primfaktorzerlegung in den ganzen Zahlen

DEFINITION 13.1 (Primzahl). Eine Zahl $p \in \mathbb{N}$ ist genau dann eine *Primzahl*, wenn folgende beiden Bedingungen gelten:

(1) Es gilt $p > 1$.
(2) Für alle $a, b \in \mathbb{N}$ mit $p = a \cdot b$ gilt $a = 1$ oder $b = 1$.

DEFINITION 13.2 (Teilbarkeit). Seien $x, y \in \mathbb{Z}$. Die Zahl x *teilt* y genau dann, wenn es ein $z \in \mathbb{Z}$ gibt, sodass $y = z \cdot x$ ist.

Wir schreiben dann auch $x \mid y$; die Zahl y heißt ein *Vielfaches* von x.

SATZ 13.3. *Seien $a \in \mathbb{Z}$ und $n \in \mathbb{N}$. Dann gibt es genau ein Paar von Zahlen $(q, r) \in \mathbb{Z} \times \mathbb{Z}$, sodass $a = q \cdot n + r$ und $r \in \{0, \ldots, n-1\}$.*

Wir bezeichnen den Rest r mit $a \bmod n$.

SATZ 13.4 (Euklid, 360-280 v.Chr.). *Es gibt unendlich viele Primzahlen.*

Beweis: Wir nehmen an, dass $p_1, \ldots, p_r$ bereits alle Primzahlen sind. Da 2 prim ist, gilt $r \geq 1$. Dann ist der kleinste Teiler q von $1 + \prod_{i=1}^{r} p_i$ mit $q > 1$ eine Primzahl mit $q \notin \{p_1, \ldots, p_r\}$. ■

DEFINITION 13.5 (Größter gemeinsamer Teiler). Für zwei Zahlen $a, b \in \mathbb{Z}$ (nicht beide 0) ist $\mathrm{ggT}(a, b)$ die größte Zahl $z \in \mathbb{N}$ mit $z \mid a$ und $z \mid b$.

SATZ 13.6. *Seien $a, b \in \mathbb{Z}$ nicht beide 0, und sei $z \in \mathbb{Z}$. Dann gilt:* $\mathrm{ggT}(a, b) = \mathrm{ggT}(a + z \cdot b, b)$.

So gilt zum Beispiel $\mathrm{ggT}(25, 15) = \mathrm{ggT}(40, 15)$.

Beweis: Wir zeigen, dass nicht nur der ggT, sondern sogar die Mengen der gemeinsamen Teiler der beiden Zahlenpaare gleich sind. Wir zeigen also

$$\{t \in \mathbb{Z} \,:\, t \mid a \text{ und } t \mid b\} = \{t \in \mathbb{Z} \,:\, t \mid a + zb \text{ und } t \mid b\}.$$

"$\subseteq$": Falls t sowohl a als auch b teilt, dann auch $a + zb$ und b. "$\supseteq$": Falls t sowohl $a + zb$, als auch b teilt, dann auch $a + zb - zb$ und b, also auch a und b.■

Das nützen wir jetzt möglichst geschickt aus, um ggT(147, 33) zu berechnen:

$$\begin{aligned}\text{ggT}(147, 33) &= \text{ggT}(147 - 4 \cdot 33, 33)\\ &= \text{ggT}(15, 33)\\ &= \text{ggT}(15, 33 - 2 \cdot 15)\\ &= \text{ggT}(15, 3)\\ &= \text{ggT}(0, 3)\\ &= 3.\end{aligned}$$

Günstig ist es also, z so zu wählen, dass $a + zb$ der Rest von a bei der Division durch b wird.

Mit Hilfe des *erweiterten Euklidischen Algorithmus* findet man nicht nur den ggT von a und b, sondern auch $u, v \in \mathbb{Z}$, sodass gilt:

$$ggT(a, b) = u \cdot a + v \cdot b.$$

Beispiel: Wir berechnen ggT(147, 33), und schreiben das so:

	147	33	
147	1	0	$(147 = 1 \cdot 147 + 0 \cdot 33)$
33	0	1	$(33 = 0 \cdot 147 + 1 \cdot 33)$
15	1	-4	$(15 = 1 \cdot 147 - 4 \cdot 33)$
3	-2	9	$(3 = -2 \cdot 147 + 9 \cdot 33)$
0			

Berechnet man ggT(a, b) mithilfe dieses Algorithmus, sieht man, dass sich die Zahlen in der linken Spalte immer als Linearkombination von a und b schreiben lassen. Als Konsequenz davon erhalten wir folgenden Satz:

SATZ 13.7. *Seien $a, b \in \mathbb{Z}$ (nicht beide 0). Dann gibt es $u, v \in \mathbb{Z}$, sodass*

$$\text{ggT}(a, b) = u \cdot a + v \cdot b.$$

Beweis: Wir betrachten zuerst den Fall $a \geq 0$, $b \geq 0$, und zeigen den Satz durch Induktion nach $\min(a, b)$. Wenn $b = 0$, so gilt $a > 0$, und somit nach der Definition des ggT auch $\text{ggT}(a, b) = a$. Wenn $a = 0$, so gilt $b \neq 0$ und $\text{ggT}(a, b) = b$.

Seien nun $a > 0$, $b > 0$, $b \leq a$. Durch Division mit Rest erhalten wir $q \in \mathbb{N}_0$, $r \in \{0, \ldots, b - 1\}$ sodass $a = qb + r$. Wegen Satz 13.6 gilt $\text{ggT}(a, b) = \text{ggT}(r, b)$. Da $r < b$, gibt es nach Induktionsvoraussetzung $u', v' \in \mathbb{Z}$, sodass $\text{ggT}(r, b) = u'r + v'b$. Dann gilt $\text{ggT}(a, b) = \text{ggT}(r, b) = u'r + v'b = u'(a - qb) + v'b = u'a + (v' - u'q)b$, also ist auch ggT$(a, b)$ als Kombination von a und b darstellbar. Der Fall $a > 0$, $b > 0$, $a \leq b$ funktioniert genauso. ■

Eine Folgerung davon ist:

SATZ 13.8. *Seien $a, b \in \mathbb{Z}$, nicht beide* 0, *und sei $t \in \mathbb{Z}$ so, dass $t \mid a$ und $t \mid b$. Dann gilt auch $t \mid \mathrm{ggT}(a, b)$.*

Beweis: Seien $u, v \in \mathbb{Z}$ so, dass $\mathrm{ggT}(a, b) = ua + vb$. Da t die Zahl a teilt, ist auch ua ein Vielfaches von t. Ebenso ist vb ein Vielfaches von t. Somit ist auch die Summe $ua + vb$ ein Vielfaches von t. Die Zahl t ist also ein Teiler von $\mathrm{ggT}(a, b)$. ■

Wenn a und b größten gemeinsamen Teiler 1 haben, so heißen sie *teilerfremd* oder *relativ prim*.

ÜBUNGSAUFGABEN 13.9.

(1) [**Remmert and Ullrich, 1987**, p. 28] Sei p_n die n-te Primzahl, d. h. $p_1 = 2$, $p_2 = 3$, usw. Zeigen Sie

$$p_n \leq 2^{(2^{n-1})}.$$

(2) Seien $a, b, x \in \mathbb{N}$ und $u, v \in \mathbb{Z}$ so, dass

$$x = ua + vb.$$

Zeigen Sie: Wenn x sowohl a als auch b teilt, so gilt $x = \mathrm{ggT}(a, b)$.

(3) Seien $a, b \in \mathbb{N}$, $y \in \mathbb{Z}$ so, dass $a \mid y$, $b \mid y$, $\mathrm{ggT}(a, b) = 1$. Zeigen Sie (ohne Vorgriff auf die Primfaktorzerlegung): $a \cdot b \mid y$.

(4) Seien $a, b \in \mathbb{Z}$ (nicht beide 0), und sei $k \in \mathbb{N}$. Zeigen Sie: $\mathrm{ggT}(ka, kb) = k\,\mathrm{ggT}(a, b)$. Gelingt es Ihnen, $\mathrm{ggT}(ka, kb) \mid k\,\mathrm{ggT}(a, b)$ auch ohne Verwendung der Primfaktorzerlegung zu zeigen?

(5) Seien $a, c \in \mathbb{Z}$, $b, d \in \mathbb{N}$. Zeigen Sie: Wenn die Brüche $\frac{a}{b}$ und $\frac{c}{d}$ gekürzt, und die Nenner b und d teilerfremd sind, so ist auch der Bruch $\frac{ad+bc}{bd}$ gekürzt.

SATZ 13.10. *Seien $a, b, c \in \mathbb{Z}$, und sei zumindest eine der Zahlen a und b nicht* 0. *Wir nehmen an, dass a die Zahl $b \cdot c$ teilt und dass $\mathrm{ggT}(a, b) = 1$ gilt. Dann gilt: a teilt c.*

Beweis: Es gibt $u, v \in \mathbb{Z}$, sodass $1 = u \cdot a + v \cdot b$. Es gilt $a \mid uac$. Da nach Voraussetzung $a \mid bc$ gilt, gilt auch $a \mid vbc$. Daraus erhalten wir

$$a \mid (ua + vb)c,$$

und somit $a \mid c$. ■

KOROLLAR 13.11. *Seien $b, c \in \mathbb{Z}$, und sei p eine Primzahl. Wenn p das Produkt bc teilt, so teilt p einen der beiden Faktoren b und c.*

SATZ 13.12. *Sei $\langle p_i \mid i \in \mathbb{N} \rangle = (2, 3, 5, 7, 11, \ldots)$ die Folge aller Primzahlen, und sei $n \in \mathbb{N}$. Dann gibt es genau eine Funktion $\alpha : \mathbb{N} \to \mathbb{N}_0$ mit folgenden Eigenschaften:*

(1) $\{i \in \mathbb{N} \mid \alpha(i) > 0\}$ *ist endlich.*
(2) $n = \prod_{i \in \mathbb{N}} p_i^{\alpha(i)}$.

Beweis: Wir zeigen zunächst durch Induktion nach n, dass es ein solches α gibt. Für $n = 1$ setzen wir $\alpha(i) := 0$ für alle $i \in \mathbb{N}$. Für $n > 1$ sei q der kleinste Teiler von n mit $q > 1$. Die Zahl q ist eine Primzahl; es gibt also $j \in \mathbb{N}$ mit $q = p_j$. Nach

Induktionsvoraussetzung gibt es $\beta : \mathbb{N} \to \mathbb{N}_0$ mit

$$\frac{n}{q} = \prod_{i \in \mathbb{N}} p_i^{\beta(i)},$$

also gilt $n = p_j^{\beta(j)+1} \cdot \prod_{i \in \mathbb{N} \setminus \{j\}} p_i^{\beta(i)}$.

Nun zeigen wir die Eindeutigkeit. Seien $\alpha, \beta : \mathbb{N} \to \mathbb{N}_0$ so, dass $\{i \in \mathbb{N} \mid \alpha(i) > 0\}$ und $\{i \in \mathbb{N} \mid \beta(i) > 0\}$ beide endlich sind und

$$\prod_{i \in \mathbb{N}} p_i^{\alpha(i)} = \prod_{i \in \mathbb{N}} p_i^{\beta(i)}.$$

Wir zeigen, dass für alle $j \in \mathbb{N}$ gilt: $\alpha(j) = \beta(j)$. Sei dazu $j \in \mathbb{N}$. Wir nehmen an $\alpha(j) > \beta(j)$. Dann gilt

$$p_j^{\alpha(j)-\beta(j)} \prod_{i \in \mathbb{N} \setminus \{j\}} p_i^{\alpha(i)} = \prod_{i \in \mathbb{N} \setminus \{j\}} p_i^{\beta(i)}.$$

Nach Korollar 13.11 teilt p_j also ein $p_i^{\beta(i)}$ mit $i \neq j$. Im Fall $\beta(i) = 0$ widerspricht das $p_j > 1$, im Fall $\beta(i) > 0$ gilt $p_j \mid p_i$. Da p_i eine Primzahl ist, gilt dann $p_i = p_j$, im Widerspruch zu $i \neq j$. ■

ÜBUNGSAUFGABEN 13.13.

(1) Sei p_n die n-te Primzahl, d. h. $p_1 = 2$, $p_2 = 3$, usw. Zeigen Sie, auch, ohne die Eindeutigkeit der Primfaktorzerlegung zu verwenden, dass Folgendes gilt: Wenn

$$\begin{aligned} a &= \Pi\, p_i^{\alpha_i} \\ b &= \Pi\, p_i^{\beta_i}, \end{aligned}$$

wobei $\alpha_i, \beta_i \in \mathbb{N}_0$, und fast alle $\alpha_i, \beta_i = 0$ sind, dann gilt $a \mid b$ genau dann, wenn für alle i gilt: $\alpha_i \leq \beta_i$. (Zeigen Sie, dass diese Aussage für alle Primfaktorzerlegungen von a und b gilt. Folgt daraus die Eindeutigkeit der Primfaktorzerlegung?)

(2) Sei p_n die n-te Primzahl, d. h. $p_1 = 2$, $p_2 = 3$, usw. Zeigen Sie: Wenn

$$\begin{aligned} a &= \Pi\, p_i^{\alpha_i} \\ b &= \Pi\, p_i^{\beta_i}, \end{aligned}$$

wobei $\alpha_i, \beta_i \in \mathbb{N}_0$, und fast alle $\alpha_i, \beta_i = 0$ sind, dann gilt

$$\mathrm{ggT}(a, b) = \prod p_i^{\min(\alpha_i, \beta_i)}.$$

(3) Welche Zahlen $q \in \mathbb{N}$ erfüllen folgende Eigenschaft?
Für alle $a, b \in \mathbb{Z}$ mit $q \mid a \cdot b$ gilt $q \mid a$ oder es gibt ein $n \in \mathbb{N}$, sodass $q \mid b^n$.

2. Polynome

DEFINITIONSVERSUCH 13.14. Sei $\boldsymbol{K}$ kommutativer Ring mit Eins. Dann ist $K[x]$ die Menge aller Ausdrücke

$$a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots + a_n x^n$$

mit $n \in \mathbb{N}_0$ und $a_0, a_1, \ldots, a_n \in K$. Die Elemente von $K[x]$ nennen wir *Polynome*.

Was heißt aber *Ausdruck*? Und welche Rolle spielt x? Mit folgender Definition stehen wir auf dem sicheren Boden der Mengenlehre.

DEFINITION 13.15. Sei $\boldsymbol{K}$ kommutativer Ring. Dann ist ein *Polynom über K* eine Folge $(a_0, a_1, a_2, a_3, \ldots)$, sodass es ein $i \in \mathbb{N}_0$ gibt, sodass für alle $j \in \mathbb{N}_0$ mit $j \geq i$ gilt: $a_j = 0$.

Wir haben also Polynome als unendliche Liste ihrer Koeffizienten definiert.

DEFINITION 13.16. Sei $\boldsymbol{K}$ ein kommutativer Ring, und seien $(a_0, a_1, a_2, \ldots)$, $(b_0, b_1, b_2, \ldots)$ Polynome über K. Wir definieren

(1) $(a_0, a_1, a_2, \ldots) + (b_0, b_1, b_2, \ldots) := (a_0 + b_0, a_1 + b_1, a_2 + b_2, \ldots)$
(2) $(a_0, a_1, a_2, \ldots) \cdot (b_0, b_1, b_2, \ldots) := (c_0, c_1, c_2, \ldots)$ mit

$$c_k := \sum_{\substack{(i,j)\in\{0,\ldots,k\}\times\{0,\ldots,k\} \\ i+j=k}} a_i \cdot b_j$$

für alle $k \in \mathbb{N}_0$.

SATZ 13.17. *Sei $\boldsymbol{K}$ ein kommutativer Ring mit Eins, seien p, q, r Polynome über K, und sei e das Polynom* $(1, 0, \ldots, 0)$. *Dann gilt:*

(1) $(p \cdot q) \cdot r = p \cdot (q \cdot r)$.
(2) $p \cdot q = q \cdot p$.
(3) $p \cdot (q + r) = p \cdot q + p \cdot r$.
(4) $p \cdot e = p$.

SATZ 13.18. *Sei $\boldsymbol{K}$ ein kommutativer Ring mit Eins, und sei P die Menge aller Polynome über K. Dann ist $\langle P, +, -, \cdot, (0, 0, 0, \ldots), (1, 0, 0, \ldots)\rangle$ ein kommutativer Ring mit Eins.*

SATZ 13.19. *Sei $\boldsymbol{K}$ ein kommutativer Ring mit Eins, sei $p = (a_0, a_1, a_2, \ldots)$ ein Polynom über K, und sei $x := (0, 1, 0, 0, \ldots, 0)$. Dann gilt:*

(1) $x^i = (\underbrace{0, 0, \ldots, 0}_{i \text{ Nuller}}, 1, 0, 0, \ldots)$.
(2) $p = \sum_{\substack{i\in\mathbb{N}_0 \\ a_i\neq 0}} a_i * x^i$.

Wir werden die Menge der Polynome über K nun oft mit $K[x]$ oder $K[t]$ bezeichnen. Sobald wir $K[t]$ verwenden, haben wir die Bedeutung von 2 Variablen erklärt:

(1) $K[t] = \left\{(a_0, a_1, \ldots) \in K^{\mathbb{N}_0} \mid \{i \in \mathbb{N}_0 \mid a_i \neq 0\} \text{ ist endlich}\right\}$.
(2) $t = (0, 1, 0, 0, \ldots)$.

3. Polynomfunktionen

DEFINITION 13.20. Sei $\boldsymbol{K}$ ein kommutativer Ring mit Eins, und sei $p = \sum_{i=0}^{n} a_i * x^i$ ein Element von $K[x]$. Dann bezeichen wir *die von p induzierte Funktion* mit $p^{\boldsymbol{K}}$ und definieren sie durch

$$\begin{array}{rccc} p^{\boldsymbol{K}} & : & K & \longrightarrow & K \\ & & y & \longmapsto & \sum_{i=0}^{n} a_i y^i. \end{array}$$

SATZ 13.21. *Sei $\boldsymbol{K}$ ein kommutativer Ring mit Eins, und seien $p, q \in K[x]$. Dann gilt für alle $y \in K$: $(p \cdot q)^{\boldsymbol{K}}(y) = p^{\boldsymbol{K}}(y) q^{\boldsymbol{K}}(y)$.*

4. Teilbarkeit von Polynomen

DEFINITION 13.22 (Grad eines Polynoms). Für $f := (a_0, a_1, a_2, \ldots) \in K[x] \setminus \{0\}$ ist der *Grad* von f, $\deg f$, jenes $n \in \mathbb{N}_0$, sodass $a_n \neq 0$ und $a_i = 0$ für alle $i > n$. Dann nennen wir a_n den *führenden Koeffizienten* von f. Wir definieren $\deg 0 := -1$.

DEFINITION 13.23. Sei $\boldsymbol{K}$ ein Körper, und seien $f, g \in K[x]$.

(1) f *teilt* g, wenn es ein $q \in K[x]$ gibt, sodass $g = q \cdot f$.
(2) f ist *irreduzibel über* $\boldsymbol{K}$ (ein irreduzibles Polynom in $K[x]$), wenn $\deg f \geq 1$ und für alle $a, b \in K[x]$ mit $a \cdot b = f$ entweder a oder b Grad 0 hat.
(3) f ist *normiert*, wenn es führenden Koeffizienten 1 hat.

SATZ 13.24 (Division). *Sei $\boldsymbol{K}$ ein Körper, und seien $f, g \in K[x]$. Wenn $f \neq 0$, so gibt es genau ein Paar $(q, r) \in K[x] \times K[x]$ mit $g = q \cdot f + r$ und $\deg r < \deg f$.*

DEFINITION 13.25 (ggT in $\boldsymbol{K}[x]$). Sei $\boldsymbol{K}$ ein Körper, und seien $f, g \in K[x]$, nicht beide 0. Dann ist $d \in K[x]$ ein *größter gemeinsamer Teiler* von f und g, wenn folgende Bedingungen gelten:

(1) $d \mid f$ und $d \mid g$,
(2) Für alle $h \in K[x]$ mit $h \mid f$ und $h \mid g$ gilt $\deg(h) \leq \deg(d)$,
(3) d ist normiert.

Wir bezeichnen den Rest von g bei der Division durch f mit $(g \bmod f)$. Da das Paar (g, f) die gleichen gemeinsamen Teiler wie das Paar $(f, g \bmod f)$ hat, können wir einen größten gemeinsamen Teiler mithilfe des Euklidschen Algorithmus berechnen.

Wir rechnen dazu zwei Beispiele:

AUFGABE 13.26. Wir berechnen einen größten gemeinsamen Teiler von $f, g \in \mathbb{R}[x]$ für

$$f = -8x + 4x^2 + 6x^3 - 5x^4 + x^5$$

und

$$g = 4 - 4x - x^2 + x^3.$$

Wir bilden die gleiche Tabelle wie beim Euklidschen Algorithmus für ganze Zahlen und erhalten:

$$\begin{array}{ccc} -8x+4x^2+6x^3-5x^4+x^5 & 1 & 0 \\ 4-4x-x^2+x^3 & 0 & 1 \\ -24+32x-10x^2 & 1 & -6+4x-x^2 \\ -\left(\frac{32}{25}\right)+\frac{16x}{25} & \frac{11}{50}+\frac{x}{10} & -\left(\frac{8}{25}\right)+\frac{7x}{25}+\frac{9x^2}{50}-\frac{x^3}{10} \\ 0 & & \end{array}$$

Um einen normierten gemeinsamen Teiler zu erhalten, multiplizieren wir die vorletzte Zeile dieser Tabelle mit $\frac{25}{16}$ und erhalten $-2+x$ als einen größten gemeinsamen Teiler. Außerdem gilt

$$-2+x=(\frac{11}{32}+\frac{5x}{32})\cdot f+(-\frac{1}{2}+\frac{7x}{16}+\frac{9x^2}{32}-\frac{5x^3}{32})\cdot g.$$

AUFGABE 13.27. Wir berechnen den größten gemeinsamen Teiler der Polynome

$$f=1+x^3+x^5$$

und

$$g=1+x+x^3$$

in $\mathbb{Z}_2[x]$. Wir erhalten

$$\begin{array}{ccc} 1+x^3+x^5 & 1 & 0 \\ 1+x+x^3 & 0 & 1 \\ 1+x^2 & 1 & x^2 \\ 1 & x & 1+x^3 \\ 0 & & \end{array}$$

Daher ist 1 ein größter gemeinsamer Teiler, und es gilt

$$1=x\cdot f+(1+x^3)\cdot g.$$

Wir können also einen größten gemeinsamen Teiler mithilfe des Euklidschen Algorithmus bestimmen. Daraus ergibt sich:

SATZ 13.28. *Sei $\boldsymbol{K}$ ein Körper, und seien $f,g\in K[x]$, nicht beide 0. Dann gibt es einen größten gemeinsamen Teiler d von f und g, für den es $u,v\in K[x]$ gibt, sodass $u\cdot f+v\cdot g=d$.*

SATZ 13.29. *Sei $\boldsymbol{K}$ ein Körper, seien $f,g\in K[x]$, nicht beide 0, und sei $d\in K[x]$. Wir nehmen an, dass es $u,v\in K[x]$ gibt, sodass $d=u\cdot f+v\cdot g$. Dann teilt jeder gemeinsame Teiler von f und g auch das Polynom d.*

Beweis: Sei h ein gemeinsamer Teiler von f und g. Dann gilt $h\mid uf+vg$, also $h\mid d$. ■

KOROLLAR 13.30. *Sei $\boldsymbol{K}$ ein Körper, und seien $f,g\in K[x]$, nicht beide 0. Seien $d_1,d_2\in K[x]$ beide* ggT *von f und g. Dann gilt $d_1=d_2$.*

Beweis: Nach Satz 13.28 gibt es einen größten gemeinsamen Teiler d von f und g, der sich als $uf+vg$ mit $u, v \in K[x]$ schreiben lässt. Wegen Satz 13.29 gilt $d_1 \mid d$. Sowohl d_1 als auch d haben den maximal möglichen Grad unter allen gemeinsamen Teilern von f und g. Also gilt $\deg(d_1) = \deg(d)$. Somit gibt es ein $\alpha \in K$, sodass $d = \alpha d_1$. Da d und d_1 normiert sind, gilt $\alpha = 1$ und somit $d = d_1$. Ebenso gilt $d = d_2$, also $d_1 = d_2$. ■

Sei $\boldsymbol{K}$ ein Körper. Ein Polynom $f \in K[x]$ ist irreduzibel über $\boldsymbol{K}$, wenn $\deg(f) \geq 1$, und wenn für alle $h, g \in K[t]$ mit $hg = f$ gilt, dass $\deg(h) = 0$ oder $\deg(g) = 0$. Jedes Polynom vom Grad 1 ist offensichtlich irreduzibel.

SATZ 13.31. *Sei $\boldsymbol{K}$ ein Körper, und seien $f, g, h \in K[x]$ so, dass f irreduzibel über $\boldsymbol{K}$ ist. Wenn $f \mid gh$, so gilt $f \mid g$ oder $f \mid h$.*

Beweis: Wenn f das Polynom g nicht teilt, so gilt $\mathrm{ggT}(f, g) = 1$. Also gibt es $u, v \in K[x]$ mit $1 = uf + vg$, und somit $h = ufh + vgh$. Da $f \mid ufh$ und $f \mid vgh$, gilt auch $f \mid h$. ■

SATZ 13.32 (Zerlegung in irreduzible Polynome). *Sei $\boldsymbol{K}$ ein Körper, sei* $\mathrm{Irr}(\boldsymbol{K})$ *die Menge aller normierten, über $\boldsymbol{K}$ irreduziblen Polynome in $K[x]$, sei $f \in K[x] \setminus \{0\}$, sei $n := \deg(f)$, und sei f_n der führende Koeffizient von f.*

Dann gibt es genau eine Funktion $\alpha : \mathrm{Irr}(\boldsymbol{K}) \to \mathbb{N}_0$, sodass $\{g \in \mathrm{Irr}(\boldsymbol{K}) \mid \alpha(g) \neq 0\}$ endlich ist, und

$$f = f_n * \prod_{g \in \mathrm{Irr}(\boldsymbol{K})} g^{\alpha(g)}.$$

5. Polynomfunktionen und Nullstellen

Wir erinnern uns, dass für

$$f = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \in K[x]$$

die von f auf $\boldsymbol{K}$ induzierte Funktion $f^{\boldsymbol{K}}$ durch

$$\begin{array}{rccc} f^{\boldsymbol{K}} & : & K & \longrightarrow & K \\ & & k & \longmapsto & a_0 + a_1 k + a_2 k^2 + \cdots + a_n k^n \end{array}$$

definiert ist.

DEFINITION 13.33. Sei $\boldsymbol{K}$ ein Körper, sei $f \in K[x]$, und sei $\alpha \in K$. Die Zahl α ist eine *Nullstelle* von f, wenn $f^{\boldsymbol{K}}(\alpha) = 0$.

SATZ 13.34. *Sei $\boldsymbol{K}$ ein Körper, sei $f \in K[x]$, und sei $\alpha \in K$. Dann ist α genau dann eine Nullstelle von f, wenn $x - \alpha \mid f$ gilt.*

ÜBUNGSAUFGABEN 13.35.

(1) Zeigen Sie:
Sei $\boldsymbol{K}$ ein Körper, und sei $f \in K[x]$ ein Polynom mit $\deg(f) \geq 2$ und einer Nullstelle $\alpha \in K$. Dann ist f nicht irreduzibel.

(2) Sei $\boldsymbol{K}$ ein Körper. Zeigen Sie, dass jedes Polynom vom Grad 2 oder 3 über $\boldsymbol{K}$, das keine Nullstelle hat, irreduzibel ist.
(3) Finden Sie ein nicht irreduzibles Polynom vom Grad 4 über $\mathbb{Q}$, das keine Nullstelle in $\mathbb{Q}$ hat und nicht irreduzibel ist.
(4) Zeigen Sie: jedes irreduzible Polynom über $\mathbb{R}$ hat Grad 1 oder geraden Grad. (Tatsächlich gilt sogar: hat Grad 1 oder 2, aber das ist viel schwieriger zu zeigen.)

SATZ 13.36. *Sei $\boldsymbol{K}$ ein Körper, sei $n \in \mathbb{N}$, und sei $f \in K[x]$ ein Polynom mit* $\deg(f) = n$. *Dann hat f höchstens n Nullstellen.*

Beweis: Wir beweisen diese Aussage durch Induktion nach n. Die Aussage stimmt für $n = 1$: ein Polynom der Form $\alpha_1 x + \alpha_2$ hat, wenn $\alpha_1 \neq 0$, nur die Nullstelle $-\alpha_2 \cdot (\alpha_1)^{-1}$.

Wir nehmen nun an, dass $n \geq 1$ ist, und dass jedes Polynom vom Grad n höchstens n Nullstellen hat. Wir zeigen, dass dann jedes Polynom vom Grad $n+1$ höchstens $n+1$ Nullstellen haben kann. Sei dazu f ein Polynom vom Grad $n+1$. Wenn f keine Nullstellen hat, dann sind wir fertig, denn"keine Nullstellen" heißt natürlich auch "weniger als $n+2$ Nullstellen". Wenn f zumindest eine Nullstelle hat, dann wählen wir eine Nullstelle α. Wir können dann ein Polynom g vom Grad n finden, sodass

$$f = (x - \alpha) \cdot g.$$

Sei nun β eine Nullstelle von f mit $\beta \neq \alpha$. Dann gilt $f^{\boldsymbol{K}}(\beta) = (\beta - \alpha) \cdot g^{\boldsymbol{K}}(\beta)$. Also gilt $0 = (\beta - \alpha) \cdot g^{\boldsymbol{K}}(\beta)$. Wegen $\beta - \alpha \neq 0$ gilt $g^{\boldsymbol{K}}(\beta) = 0$. Das Element β ist daher eine Nullstelle von g.

Da wir angenommen haben, dass jedes Polynom vom Grad n höchstens n Nullstellen hat, hat g höchstens n Nullstellen. Jede Nullstelle von f ist entweder gleich α oder unter diesen n Nullstellen von g. Somit hat f höchstens $n+1$ Nullstellen. ■

DEFINITION 13.37. Sei $\boldsymbol{K}$ ein Körper, sei $f \in K[x] \backslash \{0\}$, und sei $\alpha \in K$ eine Nullstelle von f. Wir definieren die *Vielfachheit der Nullstelle α von f* als

$$\max \{n \in \mathbb{N} : (x - \alpha)^n \mid f\}.$$

6. Polynome über den reellen und den komplexen Zahlen

DEFINITION 13.38. Wir definieren $\mathbb{C} := \{\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \mid a, b \in \mathbb{R}\}$ als die *Menge der komplexen Zahlen*.

LEMMA 13.39. *Die Menge* $\mathbb{C} := \{\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \mid a, b \in \mathbb{R}\}$ *hat folgende Eigenschaften:*

(1) $\forall c_1, c_2 \in \mathbb{C} : c_1 + c_2 \in \mathbb{C}, -c_1 \in \mathbb{C}, c_1 \cdot c_2 \in \mathbb{C}$.
(2) $\forall c \in \mathbb{C} \setminus \{\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}\} : c^{-1} \in \mathbb{C}$.
(3) $\forall c_1, c_2 \in \mathbb{C} : c_1 \cdot c_2 = c_2 \cdot c_1$.

$(\mathbb{C}, +, -, \cdot, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix})$ ist also ein Körper.

Mit den Abkürzungen $e := \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, $i := \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ lässt sich die komplexe Zahl $\left(\begin{smallmatrix} a & -b \\ b & a \end{smallmatrix}\right)$ auch als $a * e + b * i$, oder kürzer als $a + b\,i$ schreiben. Es gilt $i^2 = -1$, das Polynom $x^2 + 1$ hat also in $\mathbb{C}$ die Nullstellen i und $-i$. Komplexe Zahlen der Form $a + 0i$ bezeichnen wir auch als *reell*.

Für die Zahl $z = a + b\,i$ bezeichnen wir $\overline{z} := a - b\,i$ als die zu z *konjugiert komplexe* Zahl. Schreiben wir die komplexe Zahl $z = \left(\begin{smallmatrix} a & -b \\ b & a \end{smallmatrix}\right)$ als Matrix, so gilt $\overline{z} = z^T$.

SATZ 13.40. *Seien $z_1, z_2, z \in \mathbb{C}$. Dann gilt $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$ und $\overline{z_1 \cdot z_2} = \overline{z_1} \cdot \overline{z_2}$. Die Zahlen $\overline{z} \cdot z$ und $\overline{z} + z$ sind stets reell.*

SATZ 13.41 (Hauptsatz der Algebra, Gauß(1799), Argand (1806)). *Sei f ein Polynom in $\mathbb{C}[x]$ mit $\deg(f) > 0$. Dann besitzt f eine Nullstelle $\alpha \in \mathbb{C}$.*

KOROLLAR 13.42.

(1) *Jedes über $\mathbb{C}$ irreduzible Polynom in $\mathbb{C}[x]$ hat Grad 1.*
(2) *Jedes über $\mathbb{R}$ irreduzible Polynom in $\mathbb{R}[x]$ hat Grad 1 oder 2.*

Beweis: (1): Sei $f \in \mathbb{C}[x]$ irreduzibel über $\mathbb{C}$. Nach dem Hauptsatz der Algebra hat f eine Nullstelle $\alpha \in \mathbb{C}$, also gilt $x - \alpha \mid f$. Somit gilt $x - \alpha = f$. (2): Sei $f \in \mathbb{R}[x]$ irreduzibel über $\mathbb{R}$. Nach dem Hauptsatz der Algebra hat f eine Nullstelle $\alpha \in \mathbb{C}$. Wenn $\alpha \in \mathbb{R}$, so gilt $x - \alpha \mid f$, also $f = x - \alpha$. Wenn $\alpha \notin \mathbb{R}$, so verwenden wir, dass alle Koeffizienten von f reell sind und folglich gilt: $f^{\mathbb{C}}(\overline{\alpha}) = \sum_{i=0}^{n} f_i \cdot \overline{\alpha}^i = \sum_{i=0}^{n} \overline{f_i} \cdot \overline{\alpha}^i = \sum_{i=0}^{n} \overline{f_i \alpha^i} = \overline{\sum_{i=0}^{n} f_i \alpha^i} = \overline{f^{\mathbb{C}}(\alpha)} = \overline{0} = 0$. Also gilt in $\mathbb{C}[x]$, dass $x - \alpha \mid f$ und $x - \overline{\alpha} \mid f$. Somit gilt in $\mathbb{C}[x]$, dass $(x - \alpha)(x - \overline{\alpha}) \mid f$. Das Polynom $g := (x - \alpha)(x - \overline{\alpha})$ hat nur reelle Koeffizienten. Es gilt $g \mid f$ in $\mathbb{C}[x]$. Somit gilt auch $g \mid f$ in $\mathbb{R}[x]$ (denn gäbe es bei der Division in $\mathbb{R}[x]$ einen Rest $\neq 0$, wäre der Rest bei der Division in $\mathbb{C}[x]$ nicht eindeutig). Es gilt also $g = f$. ■

KOROLLAR 13.43. *Sei $n \in \mathbb{N}$, und sei $f \in \mathbb{C}[x]$ ein normiertes Polynom vom Grad n. Dann gibt es $m \in \mathbb{N}$, $\lambda_1, \ldots, \lambda_m \in \mathbb{C}$ und $\nu_1, \ldots, \nu_m \in \mathbb{N}$ sodass*

$$f = \prod_{i=1}^{m} (x - \lambda_i)^{\nu_i}$$

und $\nu_1 + \cdots + \nu_m = n$.

Literaturverzeichnis

[Halmos, 1976] Halmos, P. R. (1976). *Naive Mengenlehre*. Vandenhoeck & Ruprecht, Göttingen. Vierte Auflage, Aus dem Englischen übersetzt von Manfred Armbrust und Fritz Ostermann, Moderne Mathematik in elementarer Darstellung, No. 6.

[Remmert and Ullrich, 1987] Remmert, R. and Ullrich, P. (1987). *Elementare Zahlentheorie*. Birkhäuser Verlag, Basel.