

Faktorisieren von Polynomen über den rationalen Zahlen

Jakob Preininger

Vorwort

Schon zu Beginn der 7. Klasse beschloss ich eine Fachbereichsarbeit aus Mathematik zu verfassen. Die Themenwahl gestaltete sich aufgrund der Vielseitigkeit der Mathematik etwas schwieriger. Nach langer Zeit der Überlegung entschied ich mich für Polynomfaktorisierung.

Im Mathematikolympiadekurs trat für mich erstmals das Problem der Polynomfaktorisierung auf. Schon damals interessierte ich mich besonders stark für Polynome und deren Eigenschaften. Einige Methoden hatte ich bereits im Olympiadekurs und später auch im Schulunterricht gelernt. Auch im Vorbereitungskurs zum Bundeswettbewerb der Österreichischen Mathematikolympiade waren Polynome ein Thema. Mittels ausführlichem Literaturstudiums vervollständigte ich mein Wissen über Eigenschaften und Methoden zur Faktorisierung von Polynomen und begann mit dem Verfassen dieser Fachbereichsarbeit.

Besonderer Dank geht an meinen Kursleiter der Mathematikolympiade Herrn Prof. Dr. Rudolf Moser, der mir bei der Literatursuche sowie bei inhaltlichen und strukturellen Fragen stets wertvolle Unterstützung leistete. Außerdem bedanke ich mich bei Frau Prof. Mag. Schachner, für Korrekturlesen und weitere Hilfe bezüglich Inhalt und Struktur.

Inhaltsverzeichnis

Vorwort	3
Kapitel 1. Einleitung	6
Kapitel 2. Grundbegriffe	7
2.1. Definitionen	7
2.1.1. Was sind Polynome?	7
2.1.2. Koeffizienten und Grad eines Polynoms	7
2.1.3. Werte und Nullstellen	7
2.1.4. Rechnen mit Polynomen	8
2.1.5. Der Ring der Polynome	8
2.2. Teilbarkeit	9
2.2.1. Definition	9
2.2.2. Division mit Rest	10
2.2.3. Größter gemeinsamer Teiler	12
2.2.4. Irreduzible Polynome	14
Kapitel 3. Faktorisierung	16
3.1. Konstante und lineare Polynome	16
3.1.1. Konstante Polynome	16
3.1.2. Lineare Polynome	16
3.2. Quadratische Polynome	16
3.2.1. Faktorisierung des ersten Polynoms	16
3.2.2. Nicht normierte Polynome	17
3.2.3. Doppelte Nullstellen	18
3.2.4. Irreduzibel über \mathbb{Z} ?	18
3.2.5. Koeffizienten aus \mathbb{Q} und \mathbb{R}	18
3.2.6. Konjugiert-komplexe Nullstellen	19
3.2.7. Faktorisierung über \mathbb{C}	19
3.3. Polynome höheren Grades	19
3.3.1. Auffinden der ganzzahligen Nullstellen	19
3.3.2. Nicht normierte Polynome	21
3.3.3. Nullstellen von Polynomen über \mathbb{Q}	23
3.3.4. Polynome ohne rationale Nullstellen	25
3.3.5. Irrationale und komplexe Nullstellen	26
3.3.6. Finden von mehrfachen Nullstellen	27
3.3.7. Irreduzibilität über \mathbb{Q} und \mathbb{Z}	28
3.3.8. Irreduzibilität über \mathbb{R} und \mathbb{C}	29

Kapitel 4. Anhang	30
4.1. Gruppe, Ring und Körper	30
4.1.1. Die Gruppe	30
4.1.2. Der Ring	30
4.1.3. Der Integritätsbereich	30
4.1.4. Der Körper	30
Literaturverzeichnis	31

KAPITEL 1

Einleitung

Ziel dieser Fachbereichsarbeit ist die Sammlung von Methoden zur Faktorisierung von Polynomen in einer Unbekannten. Während sich Kapitel 2 mit den theoretischen Grundlagen von Polynomen und deren Teilbarkeitseigenschaften befasst, behandelt Kapitel 3 die Faktorisierung anhand von Beispielen. Kapitel 4 liefert zusätzlich eine kurze Zusammenfassung der algebraischen Strukturen, deren Kenntnis in dieser Arbeit vorausgesetzt wird.

Kapitel 2 ist in zwei größere Teile unterteilt. Teil eins führt den Begriff der Polynome ein, beschäftigt sich etwas mit ihrer Struktur und zeigt die Ringeigenschaften derselben. Teil zwei behandelt die Teilbarkeitseigenschaften von Polynomen und ist die Grundlage für die Faktorisierungen in Kapitel 3.

Kapitel 3 behandelt zunächst kurz die konstanten sowie linearen Polynom und geht dann zur Zerlegung der quadratischen Polynome über, die anhand von ausführlichen Beispielen erklärt wird. Danach werden Polynome höheren Grades auf ähnliche Weise behandelt.

Der Schwerpunkt dieser Fachbereichsarbeit liegt dabei in der Zerlegung von Polynomen mit rationalen Koeffizienten in irreduzible Polynome. Daher wurde der Fundamentalsatz der Algebra sowie Zerlegung von Polynomen über \mathbb{R} und \mathbb{C} nur angeführt und nicht näher behandelt. Eine ausführliche Behandlung derselben würde das Volumen dieser Fachbereichsarbeit mehr als verdoppeln.

Grundbegriffe

2.1. Definitionen

2.1.1. Was sind Polynome? Eine Funktion einer einzigen Variable x heißt *Polynom*, wenn es sich in der folgenden Form anschreiben lässt:

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_2 x^2 + a_1 x + a_0$$

wobei $a_n, a_{n-1}, \dots, a_1, a_0$ Konstanten sind.

Diese Definition besagt, dass jedes Polynom als Summe von endlich vielen Termen $a_k x^k$ ($k \in \mathbb{N}$) darstellen lässt.

2.1.2. Koeffizienten und Grad eines Polynoms. Für das Polynom $a_n x^n + a_{n-1} x^{n-1} + \dots + a_2 x^2 + a_1 x + a_0$ mit $a_n \neq 0$ nennt man die Zahlen a_i ($0 \leq i \leq n$) *Koeffizienten*. a_n ist der *Leitkoeffizient* und $a_n x^n$ der *Leitterm* des Polynoms. a_0 ist der *konstante Koeffizient* oder auch der *konstante Term*. a_1 ist der *lineare Koeffizient* und $a_1 x$ der *lineare Term*. Wenn der Leitkoeffizient a_n gleich 1 ist so spricht man von einem *normierten* Polynom.

BEISPIEL 2.1.1. $x^3 - 3x^2 + 4x - 9$ ist ein normiertes Polynom. Der Leitkoeffizient ist 1, der lineare Koeffizient ist 4 und der konstante Koeffizient ist -9 .

Die natürliche Zahl n heißt *Grad* des Polynoms (englisch: degree) und wird oft mit $n = \deg P$ bezeichnet. Ein konstantes Polynom besteht nur aus einem einzigen Term a_0 . Ist $a_0 \neq 0$ so hat das Polynom den Grad 0. Ist $a_0 = 0$ so heißt es Nullpolynom und hat, nach Definition, den Grad $-\infty$. Polynome von niedrigem Grad erhalten spezielle Namen:

Grad des Polynoms	Typ des Polynoms
0	konstant
1	linear
2	quadratisch
3	kubisch

BEISPIEL 2.1.2. Das Polynom $P(x) = 5x^3 - 2x^2 + 4x - 1$ hat den Grad $n = 3$ und ist daher kubisch.

Sind alle Koeffizienten von $P(x)$ aus einer bestimmten Menge M so nennt man es ein *Polynom über M* .

BEISPIEL 2.1.3. $5x^3 - 2x^2 + 4x - 1$ und $x^3 - x + 5$ sind Polynome über \mathbb{Z} , wohingegen $\frac{x^3}{5} - \frac{2x}{3}$ und $x + \frac{1}{2}$ Polynome über \mathbb{Q} darstellen.

2.1.3. Werte und Nullstellen. Wenn man in $P(x)$ einen fixen Wert x_0 für x einsetzt so erhält man den Wert des Polynoms an der Stelle x_0 .

BEISPIEL 2.1.4. $P(x) = 3x^3 - 2x^2 + 2x - 3, x_0 = 2 \Rightarrow P(x_0) = P(2) = 3 \cdot 8 - 2 \cdot 4 + 2 \cdot 2 - 3 = 17$

Eine *Nullstelle* eines Polynoms ist ein Wert x_0 für den gilt $P(x_0) = 0$.

BEISPIEL 2.1.5. Für dasselbe Polynom wie oben gilt: $P(1) = 3 \cdot 1^3 - 2 \cdot 1^2 + 2 \cdot 1 - 3 = 0$. D.h. $x_0 = 1$ ist Nullstelle von $P(x)$.

2.1.4. Rechnen mit Polynomen. Seien $P(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_2 x^2 + a_1 x + a_0$ und $Q(x) = b_m x^m + b_{m-1} x^{m-1} + \dots + b_2 x^2 + b_1 x + b_0$ zwei Polynome. Dann gelten folgende Definitionen:

Die *Summe* zweier Polynome:

$$(P + Q)(x) = (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \dots$$

BEISPIEL 2.1.6. $(x^3 - 3x^2 + x - 7) + (x^2 + 3) = x^3 - 2x^2 + x - 4$

Das *Produkt* eines Polynoms mit einer Konstanten:

$$(c \cdot P)(x) = ca_0 + ca_1 x + ca_2 x^2 + \dots + ca_{n-1} x^{n-1} + ca_n x^n$$

BEISPIEL 2.1.7. $-7(x^3 - 3x^2 + x - 7) = -7x^3 + 21x^2 - 7x + 49$

Das *Produkt* zweier Polynome:

$$(P \cdot Q)(x) = a_0 b_0 + (a_1 b_0 + a_0 b_1)x + \dots + (a_0 b_r + a_1 b_{r-1} + \dots + a_{r-1} b_1 + a_r b_0)x^r + \dots + a_n b_m x^{m+n}$$

BEISPIEL 2.1.8. $(x^3 - 3x^2 + x - 7)(x^2 + 3) = x^2(x^3 - 3x^2 + x - 7) + 3(x^3 - 3x^2 + x - 7) = x^5 - 3x^4 + 4x^3 - 16x^2 + 3x - 21$

Die *Komposition* (Hintereinanderausführung) zweier Polynome:

$$(P \circ Q)(x) = P(Q(x))$$

Das heißt in P wird jedes x durch $Q(x)$ ersetzt.

BEISPIEL 2.1.9. $P(x) = x^2 + 3$, $Q(x) = x^3 - 3x^2 + x - 7$

$$\Rightarrow P(Q(x)) = (x^3 - 3x^2 + x - 7)^2 + 3 = x^6 - 6x^5 + 11x^4 - 20x^3 + 43x^2 - 14x + 52$$

2.1.5. Der Ring der Polynome. Betrachtet man Polynome nicht als Funktionen sondern als algebraische Ausdrücke über einem Ring R so stellt sich heraus, dass Polynome Ringeigenschaften erfüllen.

SATZ 2.1.10. *Polynome über einem kommutativen Ring R bilden mit der obigen Addition und Multiplikation ebenfalls einen kommutativen Ring.*¹

BEWEIS. Die Abgeschlossenheit von Addition und Multiplikation bezüglich Polynomen folgt direkt aus der Abgeschlossenheit dieser beiden Operationen in R .

Eine Prüfung der Assoziativität, Kommutativität und Distributivität ist leicht durchzuführen. Wir begnügen uns hier mit dem Beweis des Assoziativgesetzes der Multiplikation. Dazu seien $P(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$, $Q(x) = b_m x^m + b_{m-1} x^{m-1} + \dots + b_1 x + b_0$ und $R(x) = c_k x^k + c_{k-1} x^{k-1} + \dots + c_1 x + c_0$ Polynome über R . Dann gilt:

$$(P(x)Q(x))R(x) = (a_0 b_0 + (a_1 b_0 + a_0 b_1)x + \dots + a_n b_m x^{n+m})(c_0 + c_1 x + \dots + c_k x^k) = (a_0 b_0)c_0 + ((a_1 b_0)c_0 + (a_0 b_1)c_0 + (a_0 b_0)c_1)x + \dots + (a_n b_m)c_k x^{n+m+k}$$

Es gilt aber auch:

$$P(x)(Q(x)R(x)) = a_0(b_0 c_0) + (a_1(b_0 c_0) + a_0(b_1 c_0) + a_0(b_0 c_1))x + \dots + a_n(b_m c_k)x^{n+m+k}$$

¹vgl. OKUNJEW, L. J.: Der Ring der Polynome und der Körper der rationalen Funktionen. In: Alexandroff P.S. u.a. (Hrsg.): Enzyklopädie der Elementarmathematik. Band II. Algebra. VEB Deutscher Verlag der Wissenschaften. Berlin ⁶1977. S. 120

Aufgrund der Assoziativität der Multiplikation in R folgt $(P(x)Q(x))R(x) = P(x)(Q(x)R(x))$. \square

SATZ 2.1.11. *Polynome über einem Integritätsbereich R bilden ebenfalls einen Integritätsbereich.*²

BEWEIS. Wir müssen zeigen, dass es ein Einselement gibt und die Nullteilerfreiheit erfüllt ist. Das Einselement e von R ist gleichzeitig Einselement des Polynomrings, denn für $P(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ und $Q(x) = e$ gilt:

$$P(x)Q(x) = Q(x)P(x) = ea_n x^n + \dots + ea_1 x + ea_0 = a_n x^n + \dots + a_1 x + a_0 = P(x)$$

Die Nullteilerfreiheit ist leicht zu zeigen denn es gilt für $P(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ und $Q(x) = b_m x^m + b_{m-1} x^{m-1} + \dots + b_1 x + b_0$ mit $a_n, b_m \neq 0$:

$$P(x)Q(x) = a_0 b_0 + (a_1 b_0 + a_0 b_1)x + \dots + a_n b_m x^{n+m}$$

Da das Produkt $a_n b_m$ wegen der Nullteilerfreiheit von R nicht gleich Null ist gilt: $\deg(P \cdot Q) = n + m \geq 0$. Also ist $P(x)Q(x) \neq 0$. \square

Polynome können jedoch nie einen Körper bilden da alle Polynome mit Grad größer als 0 kein inverses Element besitzen.

2.2. Teilbarkeit

2.2.1. Definition. Ein Polynom $P_1(x)$ heißt *über einem Ring R teilbar* durch das Polynom $P_2(x)$ wenn ein Polynom $Q(x)$ über R existiert, sodass

$$P_1(x) = P_2(x) \cdot Q(x)$$

gilt.³

BEISPIEL 2.2.1. $x^3 - x^2 + x - 1$ ist über \mathbb{Z} durch $x - 1$ teilbar, denn es gilt:

$$x^3 - x^2 + x - 1 = (x - 1)(x^2 + 1)$$

Da das Produkt zweier Polynome vom Grad n und m den Grad $n + m$ hat, folgt aus der Teilbarkeit von P_1 durch P_2 notwendigerweise:

$$\deg P_1 \geq \deg P_2$$

Die einzige Ausnahme ist das Nullpolynom $P_1(x) = 0$, welches durch jedes Polynom teilbar ist.

Daraus folgt folgender Satz:

SATZ 2.2.2. *Sind $P_1(x)$ und $P_2(x)$ Polynome über R derart, dass P_1 durch P_2 und umgekehrt P_2 durch P_1 teilbar ist, so unterscheiden sich die Polynome nur durch einen Faktor c vom Grad Null.*⁴

Ist R überdies ein Körper so gilt auch die Umkehrung dieses Satzes, da der konstante Faktor c dann ein inverses Element c^{-1} besitzt.

BEISPIEL 2.2.3. Sei $P_1(x) = 3x^2 + 6x + 9$ und $P_2(x) = x^2 + 2x + 3$. Dann ist $P_1(x) = 3 \cdot P_2(x)$ und $P_2 = \frac{1}{3} \cdot P_1$. Die beiden Polynome unterscheiden sich nur durch den Faktor $c = 3$. Über \mathbb{Z} (kein Körper) ist P_1 durch P_2 nicht aber P_2 durch P_1 teilbar. Über dem Körper \mathbb{Q} ist P_1 durch P_2 und auch P_2 durch P_1 teilbar.

²vgl. OKUNJEV, L. J.: Der Ring der Polynome und der Körper der rationalen Funktionen. Berlin ⁶1977. S. 128

³vgl. OKUNJEV, L. J.: Der Ring der Polynome und der Körper der rationalen Funktionen. Berlin ⁶1977. S. 130

⁴vgl. OKUNJEV, L. J.: Der Ring der Polynome und der Körper der rationalen Funktionen. Berlin ⁶1977. S. 130

2.2.2. Division mit Rest. Um zu entscheiden ob ein Polynom durch ein anderes teilbar ist verwendet man meist die *Division mit Rest*. Dazu benötigt man den folgenden Satz:

SATZ 2.2.4. *Satz über Division mit Rest: Zu je zwei Polynomen $F(x)$ und $G(x) \neq 0$ über einem Körper K gibt es genau ein Paar von Polynomen $Q(x)$ (Quotient) und $R(x)$ (Rest) über K , sodass*

$$F(x) = G(x)Q(x) + R(x)$$

gilt und $\deg R < \deg G$ ist.⁵

BEWEIS. Sei

$$F(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_2 x^2 + a_1 x + a_0 \quad (a_n \neq 0)$$

$$G(x) = b_m x^m + b_{m-1} x^{m-1} + \dots + b_2 x^2 + b_1 x + b_0 \quad (b_m \neq 0)$$

Ist $n < m$ wird obige Gleichung von $Q(x) = 0$ und $R(x) = F(x)$ mit der gegebenen Nebenbedingung erfüllt.

Ist $n \geq m$ so gilt:

$$F(x) - \frac{a_n}{b_m} x^{n-m} G(x) = F_1(x)$$

Dadurch verschwindet der Leitterm von $F(x)$ in $F_1(x)$ und es folgt $\deg F_1 < \deg F$:

$$F_1(x) = a'_{n_1} x^{n_1} + a'_{(n_1-1)} x^{n_1-1} + \dots + a'_2 x^2 + a'_1 x + a'_0 \quad (a'_{n_1} \neq 0, n_1 < n)$$

Falls $\deg F_1 \geq \deg G$, so verringert man auf dieselbe Weise den Grad von F_1 :

$$F_1(x) - \frac{a'_{n_1}}{b_m} x^{n_1-m} G(x) = F_2(x)$$

usw. Da die Grade n, n_1, n_2, \dots nicht unbeschränkt kleiner werden können, muss man nach endlich vielen Schritten zu einem Polynom $R(x)$ (mit $\deg R < \deg G$) kommen. Dabei erhält man eine endliche Kette von Beziehungen:

$$F(x) - \frac{a_n}{b_m} x^{n-m} G(x) = F_1(x)$$

$$F_1(x) - \frac{a'_{n_1}}{b_m} x^{n_1-m} G(x) = F_2(x)$$

...

$$F_k(x) - \frac{a^{(k)}_{n_k}}{b_m} x^{n_k-m} G(x) = R(x)$$

Eliminiert man aus dieser Kette die Polynome F_1, F_2, \dots, F_k , so erhält man:

$$F(x) - \left(\frac{a_n}{b_m} x^{n-m} + \frac{a'_{n_1}}{b_m} x^{n_1-m} + \dots + \frac{a^{(k)}_{n_k}}{b_m} x^{n_k-m} \right) G(x) = R(x)$$

also

$$F(x) = G(x)Q(x) + R(x)$$

mit

$$Q(x) = \frac{a_n}{b_m} x^{n-m} + \frac{a'_{n_1}}{b_m} x^{n_1-m} + \dots + \frac{a^{(k)}_{n_k}}{b_m} x^{n_k-m}.$$

Also haben wir ein Paar von Polynomen $Q(x)$ und $R(x)$ über dem Körper K gefunden.

⁵vgl. OKUNJEV, L. J.: Der Ring der Polynome und der Körper der rationalen Funktionen. Berlin ⁶1977. S. 132

Es bleibt noch zu zeigen, dass Quotient und Rest eindeutig bestimmt sind. Dazu nehmen wir an es gäbe neben $Q(x)$ und $R(x)$ noch $Q_1(x)$ und $R_1(x)$ die die Gleichung

$$F(x) = G(x)Q_1(x) + R_1(x)$$

erfüllen, wobei $\deg R_1 < \deg G$ gilt. Dann folgt:

$$G(x)(Q(x) - Q_1(x)) = R_1(x) - R(x)$$

Wäre aber $Q(x) \neq Q_1(x)$ so würde gelten, dass $\deg(G \cdot (Q - Q_1)) > \deg G > \deg(R_1 - R)$. Dies ergibt einen Widerspruch zur Gleichung. Daraus ergibt sich, dass $Q(x) = Q_1(x)$ und damit auch $R(x) = R_1(x)$ gilt. \square

BEISPIEL 2.2.5. Man dividiere $F(x) = x^3 - 2x^2 - 2x + 1$ durch $G(x) = 3x - 5$.

$$\begin{array}{r} (3x^3 - 2x^2 - 2x + 1) : (3x - 5) = x^2 + x + 1 \\ -3x^3 + 5x^2 \\ \hline 3x^2 - 2x \\ -3x^2 + 5x \\ \hline 3x + 1 \\ -3x + 5 \\ \hline 6 \end{array}$$

Der Quotient beträgt $Q(x) = x^2 + x + 1$ und der Rest beträgt $R(x) = 6$.

Mit einer geringfügigen Einschränkung lässt sich der Satz über die Division mit Rest für beliebige kommutative Ringe mit Einselement $e \neq 0$ übertragen.

SATZ 2.2.6. Sei $F(x)$ ein Polynom über einem kommutativen Ring R mit Einselement $e \neq 0$ und $G(x) \neq 0$ ein normiertes Polynom über R , so gibt es genau ein Paar von Polynomen $Q(x)$ und $R(x)$, sodass

$$F(x) = G(x)Q(x) + R(x)$$

gilt und $\deg R < \deg G$ ist.⁶

BEWEIS. Der Beweis verläuft analog zu dem obigen, wobei das Verfahren zur Bestimmung der Koeffizienten und des Restes noch einfacher ist als dort, weil hier an Stelle der Faktoren $\frac{a_n}{b_m}x^{n-m}, \frac{a'_{n_1}}{b_m}x^{n_1-m}, \dots, \frac{a^{(k)}_{n_k}}{b_m}x^{n_k-m}$ einfach die Faktoren $a_n x^{n-m}, a'_{n_1} x^{n_1-m}, \dots, a^{(k)}_{n_k} x^{n_k-m}$ stehen. Beim Eindeutigkeitsbeweis für Quotienten und Rest hat man zu berücksichtigen, dass das Einselement e des Ringes R kein Nullteiler und daher $\deg(G(Q - Q_1)) = \deg G + \deg(Q - Q_1)$ ist. \square

Mithilfe des Divisionsalgorithmus kann man nun leicht feststellen, ob ein Polynom $F(x)$ durch ein Polynom $G(x)$ teilbar ist. Ein Polynom $F(x)$ ist nämlich genau dann durch $G(x)$ teilbar, wenn der Rest bei der Division gleich Null ist. Denn ist $R(x) = 0$ so folgt:

$$F(x) = G(x)Q(x)$$

Aus der Eindeutigkeit von $Q(x)$ und $R(x)$ folgt auch die Umkehrung.⁷

Dividiert man durch ein normiertes Polynom vom Grad 1, also ein Polynom der Form $x - a$, so empfiehlt es sich das sogenannte Horner Schema zu verwenden. Für die Division des Polynom $P(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ durch das Polynom $x - a$ sieht das wie folgt aus:

⁶vgl. OKUNJEW, L. J.: Der Ring der Polynome und der Körper der rationalen Funktionen. Berlin ⁶1977. S. 134

⁷vgl. OKUNJEW, L. J.: Der Ring der Polynome und der Körper der rationalen Funktionen. Berlin ⁶1977. S. 135

$$\begin{array}{r|cccccc}
 & a_n & a_{n-1} & a_{n-2} & \dots & a_1 & a_0 \\
 & 0 & a \cdot b_{n-1} & a \cdot b_{n-2} & \dots & a \cdot b_1 & a \cdot b_0 \\
 \hline
 a & a_n & a \cdot b_{n-1} + a_{n-1} & a \cdot b_{n-2} + a_{n-2} & \dots & a \cdot b_1 + a_1 & a \cdot b_0 + a_0
 \end{array}$$

wobei $b_{n-1} = a_n$, $b_{n-2} = a \cdot b_{n-1} + a_{n-1}$, ..., $b_0 = a \cdot b_1 + a_1$ ist. Der Quotient $Q(x)$, und der Rest $R(x)$ lauten dann $Q(x) = b_{n-1}x^{n-1} + b_{n-2}x^{n-2} + \dots + b_1x + b_0$ und $R(x) = a \cdot b_0 + a_0$.

Zur Veranschaulichung des Horner Schemas geben wir folgendes Beispiel:

BEISPIEL 2.2.7. Man dividiere $x^3 + 2x^2 - 5x + 4$ durch $x + 3$.

Das Horner Schema sieht hier wie folgt aus:

$$\begin{array}{r|cccc}
 & 1 & 2 & -5 & 4 \\
 & 0 & -3 & 3 & 6 \\
 \hline
 -3 & 1 & -1 & -2 & 10
 \end{array}$$

Also gilt:

$$(x^3 + 2x^2 - 5x + 4) : (x + 3) = x^2 - x - 2 + \frac{10}{x + 3}$$

Man vergleiche dazu die Polynomdivision:

$$\begin{array}{r}
 (x^3 + 2x^2 - 5x + 4) : (x + 3) = x^2 - x - 2 \\
 \underline{-x^3 - 3x^2} \\
 -x^2 - 5x \\
 \underline{x^2 + 3x} \\
 -2x + 4 \\
 \underline{2x + 6} \\
 10
 \end{array}$$

2.2.3. Größter gemeinsamer Teiler. Ein Polynom $T(x)$ heißt *gemeinsamer Teiler* der Polynome $P(x)$ und $Q(x)$, wenn $T(x)$ sowohl $P(x)$ als auch $Q(x)$ teilt. Im besonderen heißt $D(x)$ ein *größter gemeinsamer Teiler*, wenn $D(x)$ durch jeden gemeinsamen Teiler $T(x)$ von $P(x)$ und $Q(x)$ teilbar ist.⁸

Um den größten gemeinsamen Teiler zu bestimmen wendet man den *Euklidischen Algorithmus* an. Dabei wird zunächst $P(x)$ durch $Q(x)$ dividiert. Der dabei auftretende Quotient wird mit $Q_1(x)$ und der Rest mit $R_1(x)$ bezeichnet. Danach wird $Q(x)$ durch $R_1(x)$ dividiert, wobei sich der Quotient $Q_2(x)$ und der Rest $R_2(x)$ ergeben. Danach wird jeweils der vorangegangene Rest durch den folgenden dividiert. Dabei verringert sich der Grad der auftretenden Reste ständig. Daher muss das Verfahren nach endlich vielen Schritten abbrechen, bzw. man erhält nach endlich vielen Schritten einen Rest $R_k(x)$ der Teiler des vorangegangenen Restes $R_{k-1}(x)$ ist. Wir behaupten $R_k(x)$ ist dann der größte gemeinsame Teiler von $P(x)$ und $Q(x)$.⁹

BEWEIS. Wir schreiben den Algorithmus zunächst mathematisch an:

$$P(x) = Q(x)Q_1(x) + R_1(x)$$

$$Q(x) = R_1(x)Q_2(x) + R_2(x)$$

...

$$R_{k-2}(x) = R_{k-1}(x)Q_k(x) + R_k(x)$$

⁸vgl. OKUNJEV, L. J.: Der Ring der Polynome und der Körper der rationalen Funktionen. Berlin ⁶1977. S. 135

⁹vgl. OKUNJEV, L. J.: Der Ring der Polynome und der Körper der rationalen Funktionen. Berlin ⁶1977. S. 135

$$R_{k-1}(x) = R_k(x)Q_{k+1}(x)$$

Zuerst zeigen wir, dass $R_k(x)$ ein gemeinsamer Teiler von $P(x)$ und $Q(x)$ ist. Dazu betrachten wir zunächst die vorletzte Beziehung des Systems:

$$R_{k-2}(x) = R_{k-1}(x)Q_k(x) + R_k(x)$$

Da auf Grund der letzten Beziehung $R_{k-1}(x)$ durch $R_k(x)$ teilbar ist, ergibt sich, dass $R_{k-2}(x)$ ebenfalls durch $R_k(x)$ teilbar ist. Danach betrachten wir die vorangegangene Beziehung des Systems:

$$R_{k-3}(x) = R_{k-2}(x)Q_{k-1}(x) + R_{k-1}(x)$$

Da R_{k-1} und R_{k-2} durch R_k teilbar sind so gilt dies auch für $R_{k-3}(x)$. Setzt man dieses Verfahren schrittweise bis nach oben fort, so ergibt sich schließlich, dass $P(x)$ und $Q(x)$ durch $R_k(x)$ teilbar sind.

Es bleibt dann noch zu zeigen, dass $R_k(x)$ der größte gemeinsame Teiler ist. Zu diesem Zweck gehen wir von der ersten Beziehung

$$P(x) = Q(x)Q_1(x) + R_1(x)$$

aus und untersuchen, was man bezüglich eines beliebigen gemeinsamen Teilers $T(x)$ aussagen kann. Sind $P(x)$ und $Q(x)$ durch $T(x)$ teilbar, so ist auch $R_1(x)$ durch $T(x)$ teilbar. Entsprechend, erhält man auf Grund der zweiten Beziehung des Systems,

$$Q(x) = R_1(x)Q_2(x) + R_2(x)$$

dass auch $R_2(x)$ durch $T(x)$ teilbar ist. Setzt man das Verfahren schrittweise nach unten fort so erhält man, dass $R_k(x)$ durch $T(x)$ teilbar ist. Damit ist gezeigt, dass R_k wirklich der größte gemeinsame Teiler von $P(x)$ und $Q(x)$ ist. \square

Es ist nicht schwer zu zeigen, dass der größte gemeinsame Teiler bis auf einen konstanten Faktor eindeutig bestimmt ist.¹⁰

Dazu seien $D_1(x)$ und $D_2(x)$ größte gemeinsame Teiler der Polynome $P(x)$ und $Q(x)$. Gemäß Definition gilt dann, dass $D_1(x)$ durch $D_2(x)$ und $D_2(x)$ durch $D_1(x)$ teilbar ist, woraus unmittelbar folgt dass $D_2(x) = cD_1(x)$ gilt.

BEISPIEL 2.2.8. Man bestimme den größten gemeinsamen Teiler von $P(x) = x^4 - x^3 - 2x + 2$ und $Q(x) = x^3 - x^2 + 5x - 5$.

Man dividiert:

$$(x^4 - x^3 - 2x + 2) : (x^3 - x^2 + 5x - 5) = x + \frac{-5x^2 + 3x + 2}{x^3 - x^2 + 5x - 5}$$

$$(x^3 - x^2 + 5x - 5) : (-5x^2 + 3x + 2) = -\frac{x}{5} + \frac{2}{25} + \frac{\frac{129x}{25} - \frac{129}{25}}{-5x^2 + 3x + 2}$$

$$(-5x^2 + 3x + 2) : \left(\frac{129x}{25} - \frac{129}{25}\right) = \frac{25}{129} (-5x^2 + 3x + 2) : (x - 1) = \frac{25}{129} (-5x - 2)$$

$x - 1$ ist also ein Teiler von $-5x^2 + 3x + 2$ also ist $x - 1$ der größte gemeinsame Teiler von $P(x)$ und $Q(x)$.

Ist der größte gemeinsame Teiler zweier Polynome $P(x)$ und $Q(x)$ ein Polynom vom Grad Null so heißen $P(x)$ und $Q(x)$ *teilerfremd*.¹¹

¹⁰vgl. OKUNJEW, L. J.: Der Ring der Polynome und der Körper der rationalen Funktionen. Berlin ⁶1977. S. 136

¹¹vgl. OKUNJEW, L. J.: Der Ring der Polynome und der Körper der rationalen Funktionen. Berlin ⁶1977. S. 137

2.2.4. Irreduzible Polynome. Ein Polynom $P(x)$ heißt *über dem Körper K reduzibel*, wenn es als Produkt von Polynomen über K niedrigeren Grades dargestellt werden kann.¹²

Dagegen heißt ein Polynom $P(x)$, dessen Grad größer als 0 ist, *über K irreduzibel*, wenn es nicht als Produkt von Polynomen niedrigeren Grades darstellbar ist.¹³

Irreduzible Polynome haben also offenbar ähnliche Eigenschaften wie Primzahlen. Wir beweisen hier einige:

SATZ 2.2.9. *Sind $P_1(x)$ und $P_2(x)$ über K irreduzible Polynome und ist $P_1(x)$ durch $P_2(x)$ teilbar, so stimmen $P_1(x)$ und $P_2(x)$ bis auf einen konstanten Faktor überein.*¹⁴

BEWEIS. Aus $P_1(x) = P_2(x)Q(x)$ folgt aufgrund der Irreduzibilität von $P_1(x)$ unmittelbar, dass $\deg Q = 0$ gilt. Also ist $Q(x) = c \neq 0$, also gilt: $P_1(x) = cP_2(x)$. \square

SATZ 2.2.10. *Ein Polynom $Q(x)$ über K ist genau dann durch das über K irreduzible Polynom $P(x)$ nicht teilbar, wenn $Q(x)$ und $P(x)$ teilerfremd sind.*¹⁵

BEWEIS. Sei $Q(x)$ nicht durch $P(x)$ teilbar. Außerdem sei $D(x)$ der größte gemeinsame Teiler der beiden Polynome. Da $P(x)$ über K irreduzibel ist ergeben sich für $D(x)$ nur zwei Möglichkeiten. $D(x)$ ist ein Polynom vom Grad Null oder $D(x)$ ist bis auf einen konstanten Faktor gleich $P(x)$. Die zweite Möglichkeit entfällt, weil dann $Q(x)$ durch $P(x)$ teilbar wäre. Also sind $Q(x)$ und $P(x)$ teilerfremd.

Seien umgekehrt $Q(x)$ und $P(x)$ teilerfremd, so kann $Q(x)$ nicht durch $P(x)$ teilbar sein, denn dann wäre der größte gemeinsame Teiler gleich $P(x)$ und kein Polynom vom Grad Null. \square

SATZ 2.2.11. *Ist das Produkt $F(x)G(x)$ der Polynome $F(x)$ und $G(x)$ über K durch das über K irreduzible Polynom $P(x)$ teilbar, so ist mindestens einer der Faktoren $F(x)$ und $G(x)$ durch $P(x)$ teilbar.*¹⁶

BEWEIS. Wäre weder $F(x)$ noch $G(x)$ durch $P(x)$ teilbar, so wäre $P(x)$ zu $F(x)$ und $G(x)$ teilerfremd. Dann wäre aber auch das Produkt $F(x)G(x)$ zu $P(x)$ teilerfremd und damit nicht durch $P(x)$ teilbar. \square

SATZ 2.2.12. *Jedes Polynom über einem Körper K , dessen Grad größer als Null ist, läßt sich als Produkt aus über K irreduziblen Polynomen darstellen:*

$$F(x) = P_1(x) \cdot P_2(x) \cdot \dots \cdot P_r(x)$$

und diese Darstellung ist bis auf die Reihenfolge der Faktoren und auf Polynome vom Grad Null eindeutig.¹⁷

BEWEIS. Wir zeigen zunächst die Existenz einer solchen Darstellung von $F(x)$. Ist $F(x)$ über K irreduzibel so ist die Behauptung offensichtlich wahr. Ist nun $F(x)$ über K reduzibel so gilt:

$$F(x) = F_1(x)F_2(x)$$

wobei $F_1(x)$ und $F_2(x)$ Polynome über K sind, deren Grad kleiner ist als der Grad von $F(x)$. Ist mindestens einer der Faktoren reduzibel so kann man ihn (oder eventuell beide) weiter zerlegen.

¹²vgl. OKUNJEW, L. J.: Der Ring der Polynome und der Körper der rationalen Funktionen. Berlin ⁶1977. S. 141

¹³vgl. OKUNJEW, L. J.: Der Ring der Polynome und der Körper der rationalen Funktionen. Berlin ⁶1977. S. 141

¹⁴vgl. OKUNJEW, L. J.: Der Ring der Polynome und der Körper der rationalen Funktionen. Berlin ⁶1977. S. 143

¹⁵vgl. OKUNJEW, L. J.: Der Ring der Polynome und der Körper der rationalen Funktionen. Berlin ⁶1977. S. 143

¹⁶vgl. OKUNJEW, L. J.: Der Ring der Polynome und der Körper der rationalen Funktionen. Berlin ⁶1977. S. 143

¹⁷vgl. OKUNJEW, L. J.: Der Ring der Polynome und der Körper der rationalen Funktionen. Berlin ⁶1977. S. 143

Dieser Prozess muss nach endlich vielen Schritten abbrechen, weil die Grade der Polynome bei jedem Schritt geringer werden. Somit kommen wir schließlich zu einer Zerlegung von $F(x)$ in irreduzible Faktoren.

Es bleibt noch die Eindeutigkeit dieser Zerlegung zu beweisen. Dazu nehmen wir an es gäbe zwei Darstellungen von $F(x)$ als Produkt von irreduziblen Faktoren:

$$F(x) = P_1(x)P_2(x) \cdot \dots \cdot P_k(x)$$

$$F(x) = Q_1(x)Q_2(x) \cdot \dots \cdot Q_l(x)$$

wobei $P_i(x)$ und $Q_j(x)$ irreduzible Polynome über K darstellen. Ohne Beschränkung der Allgemeinheit können wir annehmen, dass $k \leq l$ ist. Es folgt:

$$P_1(x)P_2(x) \cdot \dots \cdot P_k(x) = Q_1(x)Q_2(x) \cdot \dots \cdot Q_l(x)$$

Die linke Seite ist offensichtlich durch $P_1(x)$ teilbar. Also muss auch die rechte Seite durch $P_1(x)$ teilbar sein. Nach Satz 2.2.11 muss dann mindestens einer der Faktoren durch $P_1(x)$ teilbar sein. Sei also ohne Beschränkung der Allgemeinheit $Q_1(x)$ durch $P_1(x)$ teilbar. Nach Satz 2.2.9 müssen dann $P_1(x)$ und $Q_1(x)$ bis auf einen konstanten Faktor gleich sein. Das heißt es gilt, dass $Q_1(x) = c_1P_1(x)$ ist. Wir setzen dies in die obige Gleichung ein und kürzen durch $P_1(x)$. Das ergibt:

$$P_2(x)P_3(x) \cdot \dots \cdot P_k(x) = c_1Q_2(x)Q_3(x) \cdot \dots \cdot Q_l(x)$$

Analog zur obigen Überlegung erhalten wir nun $Q_2(x) = c_2P_2(x)$. Daraus ergibt sich

$$P_3(x)P_4(x) \cdot \dots \cdot P_k(x) = c_1c_2Q_3(x)Q_4(x) \cdot \dots \cdot Q_l(x)$$

usw. Schlussendlich erhalten wir:

$$1 = c_1c_2 \cdot \dots \cdot c_kQ_{k+1}(x) \cdot \dots \cdot Q_l(x)$$

Wäre $k < l$ so müsste 1 durch die Polynome Q_{k+1}, \dots, Q_l deren Grade größer als Null sind teilbar sein, was nicht möglich ist. Also gilt $k = l$ und $Q_1(x) = c_1P_1(x), \dots, Q_l(x) = c_lP_l(x)$, was zu beweisen war. \square

Eine Faktorisierung eines Polynoms bis auf die irreduziblen Polynome ist daher auch sinnvoll da eine solche Faktorisierung (bis auf konstante Faktoren) eindeutig ist. Das Ziel des nachfolgenden Kapitels ist es nun diese Zerlegung in irreduzible Polynome zu finden.

Faktorisierung

3.1. Konstante und lineare Polynome

3.1.1. Konstante Polynome. Konstante Polynome sind nach Definition weder reduzibel noch irreduzibel. Für Polynome haben sie etwa dieselbe Bedeutung wie die Zahl 1 bei den ganzen Zahlen, die weder eine Primzahl noch eine zusammengesetzte Zahl ist. Eine Faktorisierung konstanter Polynome ist daher nicht sinnvoll.

3.1.2. Lineare Polynome.

SATZ 3.1.1. *Alle linearen Polynome $P(x) = ax + b$ über einem Körper K sind über K irreduzibel.*

BEWEIS. Wäre $P(x)$ über K reduzibel, so ließe es sich als Produkt zweier Polynome $Q(x)$ und $R(x)$ niedrigeren Grades darstellen. Die Grade von $Q(x)$ und $R(x)$ müssen also kleiner als 1 sein. Daraus folgt aber, dass $Q(x)$ und $R(x)$ konstante Polynome sind. Dann ist aber das Produkt $Q(x)R(x)$ auch ein konstantes Polynom, was zu einem Widerspruch führt. Also sind alle linearen Polynome irreduzibel. \square

Eine Faktorisierung linearer Polynome ist also ebenfalls nicht sinnvoll möglich.

3.2. Quadratische Polynome

3.2.1. Faktorisierung des ersten Polynoms.

BEISPIEL 3.2.1. Gegeben sei das Polynom $P(x) = x^2 - 5x + 6$. Um es faktorisieren zu können müssen wir zunächst die Nullstellen des Polynoms (also die Lösungen der Gleichung $P(x) = 0$) berechnen. Dazu benützen wir die »Methode der quadratischen Ergänzung«:

$$\begin{aligned}
 x^2 - 5x + 6 &= 0 \\
 x^2 - 5x &= -6 \\
 \Leftrightarrow x^2 - 5x + \frac{25}{4} &= -6 + \frac{25}{4} \\
 \Leftrightarrow \left(x - \frac{5}{2}\right)^2 &= \frac{1}{4} \\
 \Leftrightarrow x - \frac{5}{2} &= \pm \sqrt{\frac{1}{4}} \\
 \Leftrightarrow x &= \frac{5}{2} \pm \frac{1}{2} \\
 \Leftrightarrow (x = 2) \vee (x = 3) &
 \end{aligned}$$

Diese Methode funktioniert auch allgemein für $x^2 + px + q = 0$:

$$\begin{aligned}
 x^2 + px + q &= 0 \\
 \Leftrightarrow x^2 + px &= -q
 \end{aligned}$$

$$\begin{aligned} \Leftrightarrow x^2 + px + \frac{p^2}{4} &= \frac{p^2}{4} - q \\ \Leftrightarrow \left(x + \frac{p}{2}\right)^2 &= \frac{p^2}{4} - q \\ \Leftrightarrow x_{1,2} + \frac{p}{2} &= \pm \sqrt{\frac{p^2}{4} - q} \\ \Leftrightarrow x_{1,2} &= -\frac{p}{2} \pm \sqrt{\frac{p^2}{4} - q} \end{aligned}$$

Damit haben wir die allgemeine Lösungsformel für die quadratische Gleichung hergeleitet. Mithilfe dieser Lösungsformel und dem Satz von Vieta können wir das quadratische Polynom faktorisieren.

SATZ 3.2.2. *Satz von Vieta für quadratische Polynome*

Sei $P(x) = x^2 + px + q$ ein quadratisches Polynom mit den Nullstellen x_1 und x_2 . Dann gilt: $x_1 + x_2 = -p$, $x_1x_2 = q$ und $x^2 + px + q = (x - x_1)(x - x_2)$.¹

BEWEIS.

$$\begin{aligned} x^2 + px + q = 0 &\Leftrightarrow x_{1,2} = -\frac{p}{2} \pm \sqrt{\frac{p^2}{4} - q} \\ \Rightarrow x_1 + x_2 &= -\frac{p}{2} + \sqrt{\frac{p^2}{4} - q} - \frac{p}{2} - \sqrt{\frac{p^2}{4} - q} = -p \Rightarrow p = -(x_1 + x_2) \\ x_1x_2 &= \left(-\frac{p}{2} + \sqrt{\frac{p^2}{4} - q}\right) \left(-\frac{p}{2} - \sqrt{\frac{p^2}{4} - q}\right) = \left(-\frac{p}{2}\right)^2 - \left(\sqrt{\frac{p^2}{4} - q}\right)^2 = \frac{p^2}{4} - \frac{p^2}{4} + q = q \Rightarrow q = x_1x_2 \\ &\Rightarrow x^2 + px + q = x^2 + x(-x_1 - x_2) + x_1x_2 = (x - x_1)(x - x_2) \end{aligned}$$

□

Damit können wir das Polynom $x^2 - 5x + 6$ faktorisieren:

$$x^2 - 5x + 6 = (x - 2)(x - 3)$$

3.2.2. Nicht normierte Polynome.

BEISPIEL 3.2.3. Versuchen wir nun ein weiteres Polynom zu faktorisieren: $2x^2 + 9x - 5$. Dieses Polynom ist nicht normiert aber wir können den Satz von Vieta dennoch anwenden:

Zuerst berechnen wir wieder die Nullstellen des Polynoms:

$$2x^2 + 9x - 5 = 0$$

Wir dividieren den Leitkoeffizienten um die Lösungsformel anwenden zu können:

$$\begin{aligned} \Leftrightarrow x^2 + \frac{9}{2}x - \frac{5}{2} &= 0 \\ \Leftrightarrow x_{1,2} &= -\frac{9}{4} \pm \frac{11}{4} \end{aligned}$$

Als Lösungen erhalten wir: $x_1 = -5$ und $x_2 = \frac{1}{2}$. Nach dem Satz von Vieta gilt dann:

$$x^2 + \frac{9}{2}x - \frac{5}{2} = (x + 5) \left(x - \frac{1}{2}\right)$$

Nun multiplizieren wir den Leitkoeffizienten wieder und erhalten:

$$2x^2 + 9x - 5 = 2(x + 5) \left(x - \frac{1}{2}\right)$$

¹vgl. OKUNJEV, L. J.: Der Ring der Polynome und der Körper der rationalen Funktionen. Berlin ⁶1977. S. 193

Um die Koeffizienten der Faktoren ganzzahlig werden zu lassen können wir auch:

$$2x^2 + 9x - 5 = (x + 5)(2x - 1)$$

schreiben.

3.2.3. Doppelte Nullstellen.

BEISPIEL 3.2.4. Faktorisiert man das Polynom $x^2 - 4x + 4$ so erhält man:

$$\begin{aligned} x^2 - 4x + 4 &= 0 \\ \Leftrightarrow x_{1,2} &= 2 \pm \sqrt{4 - 4} = 2 \end{aligned}$$

Die beiden Lösungen der quadratischen Gleichung sind hier identisch. Die Nullstelle des Polynoms heißt dann *doppelte Nullstelle* oder *Nullstelle mit der Vielfachheit 2*. Das Polynom faktorisieren wir wieder mit dem Satz von Vieta:

$$x^2 - 4x + 4 = (x - 2)(x - 2) = (x - 2)^2$$

3.2.4. Irreduzibel über \mathbb{Z} ?

BEISPIEL 3.2.5. Wir faktorisieren nun das Polynom $x^2 - 2x - 1$:

$$\begin{aligned} x^2 - 2x - 1 &= 0 \\ \Leftrightarrow x_{1,2} &= 1 \pm \sqrt{2} \\ x^2 - 2x - 1 &= (x - \sqrt{2} - 1)(x + \sqrt{2} - 1) \end{aligned}$$

Die beiden Faktoren sind keine Polynome über \mathbb{Z} obwohl das Ausgangspolynom über \mathbb{Z} war. Offensichtlich kann ein Polynom $ax^2 + bx + c$ über \mathbb{Z} nur dann über \mathbb{Z} und über \mathbb{Q} reduzibel sein, wenn der Ausdruck unter der Wurzel (Diskriminante) das Quadrat einer rationalen Zahl ist. Dies ist genau dann der Fall wenn gilt, dass $b^2 - 4ac$ eine Quadratzahl ist, denn $ax^2 + bx + c = a(x^2 + \frac{b}{a}x + \frac{c}{a}) = 0$ hat die Lösungen $x_{1,2} = -\frac{b}{2a} \pm \sqrt{\frac{b^2}{4a^2} - \frac{c}{a}} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$.

Umgekehrt gilt:

SATZ 3.2.6. Ist $b^2 - 4ac = t^2$ ein vollständiges Quadrat so ist $ax^2 + bx + c$ über \mathbb{Z} (und damit auch über \mathbb{Q}) reduzibel.²

BEWEIS.

$$ax^2 + bx + c = \left(\frac{1}{4a}\right)(2ax + b - t)(2ax + b + t) = \left(\frac{u}{v}\right)(px + q)(rx + s)$$

mit $\text{ggT}(u, v) = \text{ggT}(p, q) = \text{ggT}(r, s) = 1$. Durch Koeffizientenvergleich finden wir, dass $v \mid pr$, $v \mid (ps + qr)$ und $v \mid qs$ gelten muss. Ist $d \in \mathbb{P}$ nun ein Primfaktor von v , so gilt oBdA: $d \mid p \Rightarrow d \nmid q \Rightarrow d \mid s \Rightarrow d \nmid r$. Dann würde aber gelten, dass: $d \mid ps \wedge d \nmid qr \Rightarrow d \nmid ps + qr$. Dies ergibt einen Widerspruch. Das heißt v enthält keinen Primteiler und es gilt somit $v = 1$. Daher ist $ax^2 + bx + c$ über \mathbb{Z} und \mathbb{Q} genau dann reduzibel wenn $b^2 - 4ac$ ein vollständiges Quadrat ist. \square

3.2.5. Koeffizienten aus \mathbb{Q} und \mathbb{R} .

BEISPIEL 3.2.7. Wir wollen nun das Polynom $x^2 - \frac{38}{5}x - \frac{16}{5}$ faktorisieren.

$$x^2 - \frac{38}{5}x - \frac{16}{5} = 0$$

²vgl. BARBEAU, E. J.: Polynomials. Springer-Verlag, New York 1989.

$$\Leftrightarrow x_{1,2} = \frac{19}{5} \pm \frac{21}{5}$$

$$x^2 - \frac{38}{5}x - \frac{16}{5} = (x - 8) \left(x - \frac{2}{5} \right)$$

Es ist also möglich, dass einige Faktoren in der Faktorisierung Polynome über \mathbb{Z} sind, obwohl das Polynom auch nichtganzzahlige Koeffizienten besitzt. Es ist jedoch nicht möglich, dass alle Faktoren über \mathbb{Z} sind, da dann ihr Produkt (das Ausgangspolynom) nur ganzzahlige Koeffizienten enthalten würde.

Enthält das Polynom irrationale Koeffizienten so gilt dasselbe wie oben für Faktoren über \mathbb{Q} .

BEISPIEL 3.2.8. $x^2 - (\sqrt{2} - \frac{1}{2})x - \frac{1}{\sqrt{2}}$:

$$x^2 - \left(\sqrt{2} - \frac{1}{2} \right) x - \frac{1}{\sqrt{2}} = 0$$

$$\Leftrightarrow x_{1,2} = \frac{2\sqrt{2} - 1}{4} \pm \frac{\sqrt{9 + 4\sqrt{2}}}{4}$$

$$\Leftrightarrow x^2 - \left(\sqrt{2} - \frac{1}{2} \right) x - \frac{1}{\sqrt{2}} = \left(x - \frac{1}{2} \right) (x - \sqrt{2})$$

3.2.6. Konjugiert-komplexe Nullstellen.

BEISPIEL 3.2.9. Das Polynom $x^2 + 2x + 2$ liefert folgende Faktorisierung:

$$x^2 + 2x + 2 = 0$$

$$\Leftrightarrow x_{1,2} = -1 \pm \sqrt{-1} = -1 \pm i$$

$$x^2 + 2x + 2 = (x + 1 + i)(x + 1 - i)$$

Dieses Polynom ist über \mathbb{R} offensichtlich irreduzibel, denn die Nullstellen sind nicht reell. Dies ist für $ax^2 + bx + c$ offensichtlich genau dann der Fall wenn $b^2 - 4ac < 0$ erfüllt ist. Die Nullstellen sind dann zwei konjugiert-komplexe Zahlen.

3.2.7. Faktorisierung über \mathbb{C} . Über der Menge der komplexen Zahlen ist jedes quadratische Polynom reduzibel, da die Lösungsformel und der Satz von Vieta hier immer genau zwei (oder eine doppelte) Nullstellen liefern.

BEISPIEL 3.2.10.

$$x^2 - (5 + i)x + 8 + i = 0$$

$$\Leftrightarrow x_{1,2} = \frac{5 + i}{2} \pm \frac{\sqrt{24 + 10i - 32 - 4i}}{2}$$

$$\Leftrightarrow x_{1,2} = \frac{5 + i \pm (1 + 3i)}{2}$$

$$\Leftrightarrow x^2 - (5 + i)x + 8 + i = (3 + 2i)(2 - i)$$

3.3. Polynome höheren Grades

3.3.1. Auffinden der ganzzahligen Nullstellen.

BEISPIEL 3.3.1. Wir wollen das Polynom $P(x) = x^3 - 2x^2 - x + 2$ faktorisieren. Dazu benötigen wir den allgemeinen Satz von Vieta.

SATZ 3.3.2. *Satz von Vieta*

Für die Nullstellen x_1, x_2, \dots, x_n des Polynoms $x^n + a_{n-1}x^{n-1} + \dots + a_2x^2 + a_1x + a_0$ gelten die folgenden Beziehungen:

$$\begin{aligned} a_{n-1} &= \sum_{i=1}^n x_i = x_1 + x_2 + \dots + x_n \\ a_{n-2} &= \sum_{1 \leq i < j \leq n} x_i x_j = x_1 x_2 + x_1 x_3 + \dots + x_{n-1} x_n \\ &\quad \dots \\ a_0 &= \prod_{i=1}^n x_i = x_1 x_2 \cdot \dots \cdot x_n \\ x^n + a_{n-1}x^{n-1} + \dots + a_2x^2 + a_1x + a_0 &= (x - x_1)(x - x_2) \cdot \dots \cdot (x - x_n) \end{aligned}$$

3

Wir können also wieder mit Hilfe der Nullstellen das Polynom faktorisieren. Dazu benötigen wir jedoch noch den folgenden Satz:

SATZ 3.3.3. *Jede ganzzahlige Nullstelle x_0 eines Polynoms $a_n x^n + a_{n-1} x^{n-1} + \dots + a_2 x^2 + a_1 x + a_0$ über \mathbb{Z} ist Teiler des konstanten Koeffizienten a_0 .*⁴

BEWEIS. Für eine Nullstelle $x_0 \in \mathbb{Z}$ gilt:

$$a_n x_0^n + a_{n-1} x_0^{n-1} + \dots + a_2 x_0^2 + a_1 x_0 + a_0 = 0$$

Würde $x_0 \nmid a_0$ gelten, dann folgt:

$$\begin{aligned} x_0 &| a_n x_0^n + a_{n-1} x_0^{n-1} + \dots + a_2 x_0^2 + a_1 x_0 \\ \Rightarrow x_0 &\nmid a_n x_0^n + a_{n-1} x_0^{n-1} + \dots + a_2 x_0^2 + a_1 x_0 + a_0 \\ &\Leftrightarrow x_0 \nmid 0 \end{aligned}$$

Dies ergibt einen Widerspruch. Also muss $x_0 | a_0$ gelten. □

Für unser Polynom kommen also nur die Teiler von $a_0 = 2$ als Nullstellen in Frage. Die Teiler sind: $T_2 = \{-2, -1, 1, 2\}$. Wir probieren nun aus welche Zahlen Nullstellen sind:

$$\begin{aligned} P(x) &= x^3 - 2x^2 - x + 2 \\ \Rightarrow P(1) &= 1^3 - 2 \cdot 1^2 - 1 + 2 = 0 \end{aligned}$$

Wir haben also bereits die erste Nullstelle gefunden. Nach Satz von Vieta gilt nun:

$$x^3 - 2x^2 - x + 2 = (x - 1)R(x)$$

wobei $R(x)$ ein unbekanntes quadratisches Polynom darstellt. Um es zu berechnen dividieren wir das Polynom $P(x)$ durch $(x - 1)$. Dazu verwenden wir das Horner-Schema:

$$\begin{array}{r|rrrr} & 1 & -2 & -1 & 2 \\ & 0 & 1 & -1 & -2 \\ \hline 1 & 1 & -1 & -2 & 0 \end{array}$$

Damit erhalten wir:

$$x^3 - 2x^2 - x + 2 = (x - 1)(x^2 - x - 2)$$

³vgl. OKUNJEW, L. J.: Der Ring der Polynome und der Körper der rationalen Funktionen. Berlin ⁶1977. S. 192

⁴vgl. OKUNJEW, L. J.: Der Ring der Polynome und der Körper der rationalen Funktionen. Berlin ⁶1977. S. 155

Um das quadratische Polynom $R(x) = x^2 - x - 2$ zu faktorisieren wenden wir die Methode erneut an⁵:

$$R(1) = 1^2 - 1 - 2 = -2 \neq 0$$

$$R(-1) = (-1)^2 - (-1) - 2 = 0$$

Wir dividieren $R(x)$ durch $(x + 1)$:

$$\begin{array}{r|rrr} & 1 & -1 & -2 \\ & 0 & -1 & 2 \\ \hline -1 & 1 & -2 & 0 \end{array}$$

$$\Rightarrow x^3 - 2x^2 - x + 2 = (x - 1)(x + 1)(x - 2)$$

BEISPIEL 3.3.4. Wir werden das Polynom $x^3 + 2x^2 - 15x$ faktorisieren. Dieses Polynom besitzt keinen konstanten Koeffizienten. Offensichtlich ist dann 0 eine Nullstelle des Polynoms. Um es zu faktorisieren heben wir also zuerst x heraus:

$$x^3 + 2x^2 - 15x = x(x^2 + 2x - 15)$$

Danach faktorisieren wir das Restpolynom $R(x) = x^2 + 2x - 15$:

$$T_{15} = \{-15, -5, -3, -1, 1, 3, 5, 15\}$$

$$R(1) = 1^2 + 2 \cdot 1 - 15 = -12$$

$$R(-1) = (-1)^2 + 2(-1) - 15 = -16$$

$$R(3) = 3^2 + 2 \cdot 3 - 15 = 0$$

$$\begin{array}{r|rrr} & 1 & 2 & -15 \\ & 0 & 3 & 15 \\ \hline 3 & 1 & 5 & 0 \end{array}$$

$$\Rightarrow x^3 + 2x^2 - 15x = x(x - 3)(x + 5)$$

3.3.2. Nicht normierte Polynome.

BEISPIEL 3.3.5. Man faktorisiere das Polynom $18x^3 - 3x^2 - 7x + 2$. Nach der bisher bekannten Methode gilt:

$$P(x) = 18x^3 - 3x^2 - 7x + 2$$

$$T_2 = \{-2, -1, 1, 2\}$$

$$P(1) = 18 - 3 - 7 + 2 = 10$$

$$P(-1) = -18 - 3 + 7 + 2 = -12$$

$$P(2) = 18 \cdot 8 - 3 \cdot 4 - 7 \cdot 2 + 2 = 120$$

⁵Man kann bei quadratischen Polynomen stattdessen auch die Lösungsformel verwenden um die Nullstellen herauszufinden.

$$P(-2) = -18 \cdot 8 - 3 \cdot 4 + 7 \cdot 2 + 2 = -140$$

Das Polynom besitzt also keine ganzzahligen Nullstellen. Um das Polynom trotzdem faktorisieren zu können müssen wir die Methode zum Auffinden der Nullstellen auf die rationalen Zahlen erweitern.

SATZ 3.3.6. *Für jede rationale Nullstelle $x_0 = \frac{p}{q}$ ($p, q \in \mathbb{Z}$, $\text{ggT}(p, q) = 1$) eines Polynoms $a_n x^n + a_{n-1} x^{n-1} + \dots + a_2 x^2 + a_1 x + a_0$ über \mathbb{Z} gilt $p \mid a_0$ und $q \mid a_n$.⁶*

BEWEIS. Es gilt:

$$\begin{aligned} a_n x_0^n + a_{n-1} x_0^{n-1} + \dots + a_2 x_0^2 + a_1 x_0 + a_0 &= 0 \\ \Leftrightarrow a_n \left(\frac{p}{q}\right)^n + a_{n-1} \left(\frac{p}{q}\right)^{n-1} + \dots + a_2 \left(\frac{p}{q}\right)^2 + a_1 \left(\frac{p}{q}\right) + a_0 &= 0 \\ \Leftrightarrow a_n p^n + a_{n-1} p^{n-1} q + \dots + a_2 p^2 q^{n-2} + a_1 p q^{n-1} + a_0 q^n &= 0 \end{aligned}$$

Würde $p \nmid a_0$ gelten, dann folgt, dass $p \nmid a_0 q^n$ da $\text{ggT}(p, q) = 1$ und weiters:

$$\begin{aligned} p \mid a_n p^n + a_{n-1} p^{n-1} q + \dots + a_2 p^2 q^{n-2} + a_1 p q^{n-1} \\ \Rightarrow p \mid a_n p^n + a_{n-1} p^{n-1} q + \dots + a_2 p^2 q^{n-2} + a_1 p q^{n-1} + a_0 q^n \\ \Leftrightarrow p \mid 0 \end{aligned}$$

Dies ergibt einen Widerspruch. Also muss $p \mid a_0$ gelten.

Analoges gilt für q und a_n :

Würde $q \nmid a_n$ gelten, dann folgt:

$$\begin{aligned} q \mid a_{n-1} p^{n-1} q + \dots + a_2 p^2 q^{n-2} + a_1 p q^{n-1} + a_0 q^n \\ \Rightarrow q \mid a_n p^n + a_{n-1} p^{n-1} q + \dots + a_2 p^2 q^{n-2} + a_1 p q^{n-1} + a_0 q^n \\ \Leftrightarrow q \nmid 0 \end{aligned}$$

Dies ergibt ebenfalls einen Widerspruch. Also gilt auch $q \mid a_n$. □

Also kommen für unser Polynom noch folgende rationale Nullstellen in Frage:

$$\pm \frac{1}{2}, \pm \frac{1}{3}, \pm \frac{2}{3}, \pm \frac{1}{6}, \pm \frac{1}{9}, \pm \frac{2}{9}, \pm \frac{1}{18}.$$

$$P\left(\frac{1}{2}\right) = 18 \left(\frac{1}{2}\right)^3 - 3 \left(\frac{1}{2}\right)^2 - 7 \left(\frac{1}{2}\right) + 2 = 0$$

$$\begin{array}{r|rrrr} & 18 & -3 & -7 & 2 \\ & 0 & 9 & 3 & -2 \\ \hline \frac{1}{2} & 18 & 6 & -4 & 0 \end{array}$$

$$\begin{aligned} P(x) &= \left(x - \frac{1}{2}\right) (18x^2 + 6x - 4) \\ &\Leftrightarrow (2x - 1) (9x^2 + 3x - 2) \end{aligned}$$

Für $R(x) = 9x^2 + 3x - 2$ kommen noch folgende Nullstellen in Frage: $\pm \frac{1}{3}, \pm \frac{2}{3}, \pm \frac{1}{9}, \pm \frac{2}{9}$

$$R\left(\frac{1}{3}\right) = 9 \left(\frac{1}{3}\right)^2 + 3 \left(\frac{1}{3}\right) - 2 = 0$$

$$\begin{array}{r|rrr} & 9 & 3 & -2 \end{array}$$

⁶vgl. OKUNJEV, L. J.: Der Ring der Polynome und der Körper der rationalen Funktionen. Berlin ⁶1977. S. 155

$$\begin{array}{c|ccc} & 0 & 3 & 2 \\ \hline \frac{1}{3} & 9 & 6 & 0 \end{array}$$

$$R(x) = \left(x - \frac{1}{3}\right)(9x + 6)$$

$$\Leftrightarrow P(x) = (2x - 1)(3x - 1)(3x + 2)$$

3.3.3. Nullstellen von Polynomen über \mathbb{Q} .

BEISPIEL 3.3.7. Sind die Koeffizienten aus \mathbb{Q} wie zum Beispiel bei $3x^3 - \frac{31}{6}x^2 + \frac{5}{2}x - \frac{1}{3}$ so müssen wir zuerst den Kehrwert des kleinsten gemeinsamen Vielfachen der Nenner herausheben.

$$P(x) = \frac{1}{6}(18x^3 - 31x^2 + 15x - 2)$$

Der zweite Faktor ist dann ein Polynom mit ganzzahligen Koeffizienten und wir können es wie oben faktorisieren. Die möglichen Nullstellen sind: $\pm 1, \pm 2, \pm \frac{1}{2}, \pm \frac{1}{3}, \pm \frac{2}{3}, \pm \frac{1}{6}, \pm \frac{1}{9}, \pm \frac{2}{9}, \pm \frac{1}{18}$.

$$P(1) = \frac{1}{6}(18 - 31 + 15 - 2) = 0$$

$$\begin{array}{c|cccc} & 18 & -31 & 15 & -2 \\ \hline & 0 & 18 & -13 & 2 \\ \hline 1 & 18 & -13 & 2 & 0 \end{array}$$

$$P(x) = \frac{1}{6}(x - 1)(18x^2 - 13x + 2)$$

$$R(x) = 18x^2 - 13x + 2$$

$$R(1) = 18 - 13 + 2 = 17$$

$$R(-1) = 18 + 13 + 2 = 33$$

$$R(2) = 18 \cdot 4 - 13 \cdot 2 + 2 = 48$$

$$R\left(\frac{1}{2}\right) = 18 \left(\frac{1}{2}\right)^2 - 13 \left(\frac{1}{2}\right) + 2 = 0$$

$$\begin{array}{c|ccc} & 18 & -13 & 2 \\ \hline & 0 & 9 & -2 \\ \hline \frac{1}{2} & 18 & -4 & 0 \end{array}$$

$$R(x) = \left(x - \frac{1}{2}\right)(18x - 4)$$

$$P(x) = \frac{1}{6}(x - 1)(2x - 1)(9x - 2)$$

Ein weiteres Beispiel:

BEISPIEL 3.3.8. Man faktorisiere $P(x) = 5x^3 - \frac{23}{6}x^2 - \frac{7}{6}x + 1$. Wir heben wieder heraus:

$$P(x) = \frac{1}{6}(30x^3 - 23x^2 - 7x + 6)$$

Für Nullstellen kommen folgende Werte für x in Frage:

$\pm 1, \pm 2, \pm 3, \pm 6, \pm \frac{1}{2}, \pm \frac{3}{2}, \pm \frac{1}{3}, \pm \frac{2}{3}, \pm \frac{1}{5}, \pm \frac{2}{5}, \pm \frac{3}{5}, \pm \frac{6}{5}, \pm \frac{1}{6}, \pm \frac{1}{10}, \pm \frac{3}{10}, \pm \frac{1}{15}, \pm \frac{2}{15}, \pm \frac{1}{30}$. Es gibt also 36 mögliche Werte für x . Alle 36 Werte direkt zu prüfen ist daher ziemlich mühsam. Daher verwenden wir hier den folgenden Satz:

SATZ 3.3.9. Ist $\frac{p}{q}$ (mit $p, q \in \mathbb{Z}$, $q > 0$ und $\text{ggT}(p, q) = 1$) eine rationale Nullstelle des Polynoms $P(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ über \mathbb{Z} , so ist für jede ganze Zahl k , für die $p - kq \neq 0$ ist, der Wert $P(k)$ durch $p - kq$ teilbar.⁷

BEWEIS. Wir multiplizieren $P(x)$ mit q^n :

$$q^n P(x) = a_n (qx)^n + qa_{n-1} (qx)^{n-1} + \dots + q^n a_0$$

Setzt man $qx = y$ so erhält man:

$$q^n P(x) = a_n y^n + qa_{n-1} y^{n-1} + \dots + q^n a_0 = Q(y)$$

Da nun $\frac{p}{q}$ eine Nullstelle von $P(x)$ sein sollte, ist die Zahl p Nullstelle von $Q(y)$. Daraus folgt nach Satz von Vieta:

$$Q(y) = (y - p)R(y)$$

wobei $Q(y)$ und $R(y)$ Polynome über \mathbb{Z} sind. Daher muss

$$\frac{q^n P(k)}{p - kq} = \frac{Q(kq)}{p - kq} = -R(kq)$$

eine ganze Zahl sein. Also gilt $q^n P(k)$ ist durch $p - kq$ teilbar. Nun ist aber q^n zu $p - kq$ teilerfremd, denn wäre dies nicht der Fall so ließe sich

$$\frac{p - kq}{q} = \frac{p}{q} - k$$

kürzen, was der Normiertheit von $\frac{p}{q}$ widerspräche. Also ist $P(k)$ durch $p - kq$ teilbar. \square

Für unser Beispiel $P(x) = \frac{1}{6}(30x^3 - 23x^2 - 7x + 6) = \frac{1}{6}R(x)$ gehen wir folgendermaßen vor.

Wir berechnen zunächst $R(1) = 6$. 1 ist also keine Nullstelle von $R(x)$. Für jede mögliche Nullstelle $\frac{p}{q}$ gilt nun nach dem gerade bewiesenen Satz, dass $R(1) = 6$ durch $p - q$ teilbar sein muss. Es verbleiben nur noch folgende mögliche Nullstellen $-1, \pm 2, 3, \pm \frac{1}{2}, \frac{3}{2}, \frac{1}{3}, \frac{2}{3}, -\frac{1}{5}, \frac{2}{5}, \frac{3}{5}, \frac{6}{5}$.

Nun berechnen wir $R(-1) = -40$. Auch -1 ist keine Nullstelle von $R(x)$. -40 muss also durch $p + q$ teilbar sein. Noch einmal wird unsere Schar von möglichen Lösungen kürzer: $-2, 3, -\frac{1}{2}, \frac{3}{2}, \frac{1}{3}, \frac{2}{3}, -\frac{1}{5}, \frac{3}{5}$.

$R(-2) = -312$. -312 ist durch $p + 2q$ teilbar für: $-\frac{1}{2}, \frac{2}{3}, \frac{3}{5}$.

$R(-\frac{1}{2}) = 0$. Wir dividieren $R(x)$ durch $x + \frac{1}{2}$:

$$\begin{array}{r|rrrr} & 30 & -23 & -7 & 6 \\ & 0 & -15 & 19 & -6 \\ \hline -\frac{1}{2} & 30 & -38 & 12 & 0 \end{array}$$

$$R(x) = (x + \frac{1}{2})(30x^2 - 38x + 12) = (2x + 1)(15x^2 - 19x + 6)$$

Für $R_1(x) = 15x^2 - 19x + 6$ kommen nur die obigen Nullstellen in Frage, wobei man gegebenenfalls noch Nullstellen streichen kann, die aufgrund der veränderten Koeffizienten a_n und a_0 nicht in Frage kommen.

Man prüft nun noch die drei restlichen Möglichkeiten $R_1(-\frac{1}{2}) = \frac{77}{4}$, $R_1(\frac{2}{3}) = 0$, $R_1(\frac{3}{5}) = 0$ und erhält:

$$P(x) = \frac{1}{6}(2x + 1)(3x - 2)(5x - 3)$$

⁷vgl. OKUNJEV, L. J.: Der Ring der Polynome und der Körper der rationalen Funktionen. Berlin ⁶1977. S. 156

3.3.4. Polynome ohne rationale Nullstellen. Besitzt ein Polynom über \mathbb{Q} keine rationale Nullstelle so kann es dennoch sein, dass das Polynom über \mathbb{Q} reduzibel ist. Zum Beispiel hat

$$P(x) = x^4 - x^3 + 3x^2 + 8x + 14$$

keine rationale Nullstelle. Es ist aber trotzdem reduzibel, denn es gilt:

$$P(x) = (x^2 + 2x + 2)(x^2 - 3x + 7)$$

Für das Auffinden benötigt man folgenden Satz:

SATZ 3.3.10. *Jedes Polynom über \mathbb{Z} , das über den rationalen Zahlen reduzibel ist, läßt sich als Produkt von Polynomen niedrigeren Grades mit ganzen Koeffizienten darstellen.*⁸

Auf den Beweis des Satzes wird hier verzichtet. Zur Anwendung des Satzes bei der Suche nach Faktoren eines Polynoms folgendes Beispiel:

BEISPIEL 3.3.11. Man zerlege das Polynom

$$P(x) = x^6 - x^5 - x^4 + x^3 - 3x^2 + 5x - 2$$

in über \mathbb{Q} irreduzible Faktoren.

Zunächst suchen wir alle Nullstellen. Es kommen $\pm 1, \pm 2$ in Frage. $P(1) = 0$

$$\begin{array}{r|cccccc} 1 & 1 & -1 & -1 & 1 & -3 & 5 & -2 \\ & 0 & 1 & 0 & -1 & 0 & -3 & 2 \\ \hline 1 & 1 & 0 & -1 & 0 & -3 & 2 & 0 \end{array}$$

$$P(x) = (x - 1)(x^5 - x^3 - 3x + 2) = (x - 1)Q(x)$$

$Q(x)$ hat keine Nullstellen denn es gilt: $Q(1) = -1$, $Q(-1) = 5$, $Q(2) = 20$, $Q(-2) = -16$.

Da der Grad von $Q(x)$ gleich 5 ist muss $Q(x)$ entweder über \mathbb{Q} irreduzibel sein oder einen Faktor vom Grad ≤ 2 besitzen. Nehmen wir an $Q(x)$ ist reduzibel. Da $Q(x)$ keine Nullstellen hat muss also ein Faktor den Grad 2 haben. Nach obigem Satz müssen die Koeffizienten der beiden Faktoren ganzzahlig sein. Also lauten die beiden Faktoren $R_1(x) = x^2 + px + q$ und $R_2(x) = x^3 + ax^2 + bx + c$. Zur Bestimmung der Koeffizienten p und q verwendet man, dass für jede ganze Zahl m der Wert $Q(m)$ durch $R_1(m)$ teilbar ist.

Da $Q(0) = 2$ und $Q(1) = -1$ ist, kommen für $R_1(0)$ und $R_1(1)$ nur folgende Wertkombinationen in Frage:

- | | |
|------------------------------------|------------------------------------|
| 1) $R_1(0) = 1$ und $R_1(1) = 1$ | 5) $R_1(0) = 2$ und $R_1(1) = 1$ |
| 2) $R_1(0) = 1$ und $R_1(1) = -1$ | 6) $R_1(0) = 2$ und $R_1(1) = -1$ |
| 3) $R_1(0) = -1$ und $R_1(1) = 1$ | 7) $R_1(0) = -2$ und $R_1(1) = 1$ |
| 4) $R_1(0) = -1$ und $R_1(1) = -1$ | 8) $R_1(0) = -2$ und $R_1(1) = -1$ |

Wir untersuchen nun der Reihe nach die Kombinationen:

(1) $R_1(0) = q = 1$, $R_1(1) = 1 + p + q = 1 \Rightarrow p = -1$. Nun dividieren wir:

$$(x^5 - x^3 - 3x + 2) : (x^2 - x + 1) = x^3 + x^2 - x - 2 + \frac{-4x + 4}{x^2 - x + 1}$$

Also ergibt 1. keine Lösung.

⁸vgl. OKUNJEV, L. J.: Der Ring der Polynome und der Körper der rationalen Funktionen. Berlin ⁶1977. S. 168

(2) $R_1(0) = q = 1$, $R_1(1) = 1 + p + q = -1 \Rightarrow p = -3$. Wir dividieren:

$$(x^5 - x^3 - 3x + 2) : (x^2 - 3x + 1) = x^3 + 3x^2 + 7x + 18 + \frac{44x - 16}{x^2 - 3x + 1}$$

Also ergibt auch 2. keine Lösung.

(3) $R_1(0) = q = -1$, $R_1(1) = 1 + p + q = 1 \Rightarrow p = 1$.

$$(x^5 - x^3 - 3x + 2) : (x^2 + x - 1) = x^3 - x^2 + x - 2$$

$$P(x) = (x - 1)(x^2 + x - 1)(x^3 - x^2 + x - 2)$$

Da $Q(x)$ keine rationalen Nullstellen hat, sind $R_1(x)$ und $R_2(x)$ über \mathbb{Q} irreduzibel.

Hätte auch nach Prüfung aller acht Wertkombinationen keine passenden p und q gefunden so wäre $Q(x)$ über den rationalen Zahlen irreduzibel gewesen. Wir haben also eine Methode gefunden rationale Polynome in endlich vielen Schritten in über \mathbb{Q} irreduzible Polynome zu zerlegen. Diese Methode wird aber für Polynome höheren Grades so aufwendig, dass man oftmals zu anderen Methoden greifen muss.

3.3.5. Irrationale und komplexe Nullstellen. Für das Auffinden irrationaler und komplexer Nullstellen gibt es keine universelle Methode die immer zum Ziel führt. Ihre Bestimmung ist nur von Fall zu Fall und meist nur näherungsweise möglich.

Über die Existenz von Nullstellen lassen sich jedoch folgende beiden Sätze beweisen.

SATZ 3.3.12. Fundamentalsatz der Algebra:

Ein Polynom n -ten Grades über \mathbb{C} besitzt genau n (nicht notwendig verschiedene) komplexe Nullstellen.⁹

Der Beweis dieses Satzes würde mehrere Seiten füllen und wird daher hier nicht angeführt.

SATZ 3.3.13. Jedes Polynom über \mathbb{R} mit ungeradem Grad besitzt mindestens eine reelle Nullstelle.¹⁰

Für den Beweis dieses Satzes benötigt man den Fundamentalsatz der Algebra und den folgenden Hilfssatz:

Ist eine echte komplexe Zahl z eine Nullstelle eines Polynoms $P(x)$ über \mathbb{R} mit der Vielfachheit n so ist auch die konjugiert komplexe Zahl \bar{z} eine Nullstelle mit Vielfachheit n .¹¹

BEWEIS. (des Hilfssatzes): Sei $z = a + bi$ ($a, b \in \mathbb{R}$, $b \neq 0$) eine echte komplexe Nullstelle von $P(x)$ mit Vielfachheit n . Wir dividieren $P(x)$ durch $Q(x) = (x - z)(x - \bar{z}) = x^2 - 2ax + (a^2 + b^2)$ und erhalten da $Q(x)$ vom Grad zwei ist:

$$P(x) = Q(x) \cdot P'(x) + cx + d \quad (c, d \in \mathbb{R})$$

Dabei ist $P'(x)$ ein Polynom über \mathbb{R} .

Da $P(z) = 0$ und $Q(z) = 0$ sind gilt für $x = z$:

$$\begin{aligned} cz + d &= 0 \\ \Rightarrow c(a + bi) + d &= 0 \\ \Rightarrow (ac + d) + bci &= 0 \\ \Rightarrow ac + d = 0 \wedge bc &= 0 \end{aligned}$$

⁹vgl. OKUNJEV, L. J.: Der Ring der Polynome und der Körper der rationalen Funktionen. Berlin ⁶1977. S. 183f

¹⁰vgl. OKUNJEV, L. J.: Der Ring der Polynome und der Körper der rationalen Funktionen. Berlin ⁶1977. S. 185

¹¹vgl. OKUNJEV, L. J.: Der Ring der Polynome und der Körper der rationalen Funktionen. Berlin ⁶1977. S. 184

Da $b \neq 0$ ist, gilt $c = 0$ und damit auch $d = 0$. Daher ist

$$P(x) = (x - z)(x - \bar{z}) \cdot P'(x)$$

woraus folgt das \bar{z} ebenfalls eine Nullstelle ist. In $P'(x)$ ist z eine Nullstelle mit Vielfachheit $n - 1$. Induktiv folgt, dass \bar{z} in $P'(x)$ ebenfalls mit Vielfachheit $n - 1$ vorkommt. \square

Nun können wir auch den eigentlichen Satz beweisen:

BEWEIS. Sei $P(x)$ ein Polynom über \mathbb{R} vom Grad $2n + 1$. $P(x)$ besitzt nach dem Fundamentalsatz der Algebra genau $2n + 1$ komplexe Nullstellen. Zu jeder echt komplexen Nullstelle muss nach dem Hilfssatz die entsprechende konjugiert komplexe Nullstelle mit gleicher Vielfachheit auftreten. Daher ist die Anzahl der echt komplexen Nullstellen gerade. Also muss $P(x)$ mindestens eine reelle Nullstelle besitzen. \square

3.3.6. Finden von mehrfachen Nullstellen. Es gibt eine Methode um mehrfache Nullstellen leichter zu finden. Dazu folgendes Beispiel:

BEISPIEL 3.3.14. Man faktorisiere $P(x) = x^5 + \sqrt{3}x^4 - 4x^3 - 4\sqrt{3}x^2 + 4x + 4\sqrt{3}$. Um hier mehrfache Nullstellen herauszufinden leiten wir $P(x)$ nach x ab:

$$P'(x) = 5x^4 + 4\sqrt{3}x^3 - 12x^2 - 8\sqrt{3}x + 4$$

Nun bestimmen wir den größten gemeinsamen Teiler von $P(x)$ und $P'(x)$:

$$\begin{aligned} (x^5 + \sqrt{3}x^4 - 4x^3 - 4\sqrt{3}x^2 + 4x + 4\sqrt{3}) &: (5x^4 + 4\sqrt{3}x^3 - 12x^2 - 8\sqrt{3}x + 4) = \\ &= \frac{x}{5} + \frac{\sqrt{3}}{25} + \frac{-\frac{4}{25}(13x^3 + 12\sqrt{3}x^2 - 26x - 24\sqrt{3})}{5x^4 + 4\sqrt{3}x^3 - 12x^2 - 8\sqrt{3}x + 4} \\ (5x^4 + 4\sqrt{3}x^3 - 12x^2 - 8\sqrt{3}x + 4) &: (13x^3 + 12\sqrt{3}x^2 - 26x - 24\sqrt{3}) = \\ &= \frac{5x}{13} - \frac{8\sqrt{3}}{169} + \frac{-50(x^2 - 2)}{13x^3 + 12\sqrt{3}x^2 - 26x - 24\sqrt{3}} \\ (13x^3 + 12\sqrt{3}x^2 - 26x - 24\sqrt{3}) &: (x^2 - 2) = 13x + 12\sqrt{3} \end{aligned}$$

Der größte gemeinsame Teiler von $P(x)$ und $P'(x)$ ist also $x^2 - 2$. Daher ist $x^2 - 2$ ein Teiler von $P(x)$ und wir erhalten:

$$P(x) = x^5 + \sqrt{3}x^4 - 4x^3 - 4\sqrt{3}x^2 + 4x + 4\sqrt{3} = (x^2 - 2)(x^3 + \sqrt{3}x^2 - 2x - 2\sqrt{3})$$

Nun ist aber $x^2 - 2$ auch Teiler von $x^3 + \sqrt{3}x^2 - 2x - 2\sqrt{3}$. Also gilt $P(x) = (x^2 - 2)^2(x + \sqrt{3}) = (x - \sqrt{2})^2(x + \sqrt{2})^2(x + \sqrt{3})$.

Offenbar enthält der größte gemeinsame Teiler von $P(x)$ und $P'(x)$ alle Faktoren die mehr als einmal vorkommen.

SATZ 3.3.15. Für das, als Produkt von paarweise teilerfremden irreduziblen Polynomen dargestellte, Polynom $P(x) = c \cdot \prod_{i=1}^r P_i(x)^{\alpha_i}$ gilt, dass der größte gemeinsame Teiler $D(x)$ von $P(x)$ und seiner Ableitung in der Unbekannten x $P'(x)$ gleich $c' \cdot \prod_{i=1}^r P_i(x)^{\alpha_i - 1}$ ist.¹²

¹²vgl. KAPLAN, Michael: Computeralgebra. Springer-Verlag, Berlin 2005. S. 230

BEWEIS. Wir zeigen, dass $P'(x)$ alle irreduziblen Faktoren $P_i(x)$ genau mit der Vielfachheit $\alpha_i - 1$ auftreten. Nach der Produktregel gilt:

$$P'(x) = c \cdot \sum_{i=1}^r \left((P_i(x)^{\alpha_i})' \cdot \prod_{j=1, j \neq i}^r P_j(x)^{\alpha_j} \right) = c \cdot \sum_{i=1}^r \left(P_i'(x) \cdot P_i(x)^{\alpha_i-1} \prod_{j=1, j \neq i}^r P_j(x)^{\alpha_j} \right)$$

$$P'(x) = c \cdot \prod_{i=1}^r P_i(x)^{\alpha_i-1} \sum_{i=1}^r \left(P_i'(x) \prod_{j=1, j \neq i}^r P_j(x) \right)$$

Damit ist $P'(x)$ für alle i durch $P_i(x)^{\alpha_i-1}$ teilbar.

Wir müssen noch zeigen, dass jeder Faktor $P_k(x)$ mit $1 \leq k \leq r$ in $S(x) = \sum_{i=1}^r \left(P_i'(x) \prod_{j=1, j \neq i}^r P_j(x) \right)$

nicht vorkommt. Für $i \neq k$ gilt $P_i'(x) \prod_{j=1, j \neq i}^r P_j(x)$ ist durch $P_k(x)$ teilbar, da es ein $j \neq i$ gibt mit

$j = k$. Für $i = k$ gilt aber $P_i'(x) \prod_{j=1, j \neq i}^r P_j(x)$ ist nicht durch $P_k(x)$ teilbar da $P_j(x)$ für alle $j \neq i$

zu P_k teilerfremd ist und $P_k'(x)$ aufgrund des Grades und der Irreduzibilität von $P_k(x)$ ebenfalls zu $P_k(x)$ teilerfremd ist. Also ist $S(x)$ nicht durch $P_k(x)$ teilbar. \square

3.3.7. Irreduzibilität über \mathbb{Q} und \mathbb{Z} . Mit der Methode aus Kapitel 3.3.4 kann man für jedes Polynom über \mathbb{Z} und \mathbb{Q} in endlicher Zeit bestimmen ob es über \mathbb{Q} (und damit auch über \mathbb{Z}) irreduzibel ist oder nicht. Da eine solche Bestimmung mit wachsendem Grad sehr schnell unhandlich und langwierig wird, empfiehlt sich oft eine Benützung von Irreduzibilitätskriterien. Eines der bekanntesten und am häufigsten benützte ist das folgende:

SATZ 3.3.16. *Irreduzibilitätskriterium von Eisenstein*

Ein Polynom $P(x)$ mit ganzzahligen Koeffizienten, dessen sämtliche Koeffizienten mit Ausnahme des Leitkoeffizienten durch eine Primzahl p teilbar sind und dessen konstanter Term sich zwar durch p nicht aber durch p^2 teilen lässt, ist über \mathbb{Q} irreduzibel.¹³

BEWEIS. Wir nehmen an das Polynom $P(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ erfüllt die Bedingungen des Kriteriums, ist aber über \mathbb{Q} reduzibel. Dann läßt sich $P(x)$ nach Satz 3.3.10 als Produkt von Polynomen $Q(x)$ und $R(x)$ über \mathbb{Z} darstellen. Also ist

$$P(x) = Q(x)R(x)$$

mit

$$Q(x) = b_k x^k + b_{k-1} x^{k-1} + \dots + b_1 x + b_0 \quad (b_k \neq 0, 0 < k < n)$$

$$R(x) = c_l x^l + c_{l-1} x^{l-1} + \dots + c_1 x + c_0 \quad (c_l \neq 0, 0 < l < n)$$

Dann gilt:

$$a_0 = b_0 c_0$$

$$a_1 = b_0 c_1 + b_1 c_0$$

$$a_2 = b_0 c_2 + b_1 c_1 + b_2 c_0$$

...

$$a_k = b_0 c_k + b_1 c_{k-1} + \dots + b_k c_0$$

...

¹³vgl. OKUNJEW, L. J.: Der Ring der Polynome und der Körper der rationalen Funktionen. Berlin 61977. S. 171

$$a_n = b_k c_l$$

Nach Voraussetzung ist $a_0 = b_0 c_0$ durch eine Primzahl p teilbar. Dann muss b_0 oder c_0 durch p teilbar sein. Da a_0 aber nicht durch p^2 teilbar ist, können nicht beide durch p teilbar sein. Sei ohne Beschränkung der Allgemeinheit p ein Teiler von b_0 aber nicht von c_0 . Da aber $a_1 = b_0 c_1 + b_1 c_0$ nach Voraussetzung durch p teilbar ist muss auch b_1 durch p teilbar sein. Aus $a_2 = b_0 c_2 + b_1 c_1 + b_2 c_0$ schließt man ähnlich auf die Teilbarkeit von b_2 durch p usw. Schließlich erhält man aus

$$a_k = b_0 c_k + b_1 c_{k-1} + \dots + b_k c_0$$

dass b_k durch p teilbar ist.

Da aber $a_n = b_k c_l$ muss auch a_n durch p teilbar sein, was der Voraussetzung widerspricht. \square

3.3.8. Irreduzibilität über \mathbb{R} und \mathbb{C} .

SATZ 3.3.17. *Ein Polynom ist über \mathbb{C} genau dann irreduzibel, wenn es linear ist.*¹⁴

Dieser Satz folgt direkt aus dem Fundamentalsatz der Algebra da sich jedes Polynom vom Grad $n > 2$ als Produkt von n linearen Polynomen darstellen lässt.

SATZ 3.3.18. *Ein Polynom über \mathbb{R} ist genau dann über \mathbb{R} irreduzibel, wenn es ein lineares Polynom oder ein quadratisches Polynom mit negativer Diskriminante ist.*¹⁵

BEWEIS. Gäbe es ein Polynom $P(x)$ über \mathbb{R} mit $\deg P > 2$ und $P(x)$ irreduzibel so besitzt sie nach dem Fundamentalsatz der Algebra mindestens eine komplexe Nullstelle x_0 . $x_0 = a + bi$ kann nicht reell sein, da sonst $P(x)$ über \mathbb{R} reduzibel wäre. Nach dem Hilfssatz aus 3.3.4 gilt, dass dann auch $\bar{x}_0 = a - bi$ Nullstelle von $P(x)$ ist. Nach Satz von Vieta gilt dann:

$$P(x) = (x - z)(x - \bar{z})Q(x) = (x^2 - 2ax + (a^2 + b^2))Q(x)$$

$x^2 - 2ax + (a^2 + b^2)$ und $Q(x)$ sind Polynome über \mathbb{R} und da $\deg Q = \deg P - 2$ ist, gilt $\deg Q > 0$. Damit ist das Polynom $P(x)$ aber reduzibel, was zu einem Widerspruch führt. \square

¹⁴vgl. OKUNJEW, L. J.: Der Ring der Polynome und der Körper der rationalen Funktionen. Berlin ⁶1977. S. 184

¹⁵vgl. OKUNJEW, L. J.: Der Ring der Polynome und der Körper der rationalen Funktionen. Berlin ⁶1977. S. 185

Anhang

4.1. Gruppe, Ring und Körper¹

4.1.1. Die Gruppe. Eine Gruppe (G, \circ) ist eine nichtleere Menge G mit einer Operation $\circ : G \times G \rightarrow G$ die folgende Eigenschaften (Axiome) erfüllt:

- (1) $\forall a, b \in G : a \circ b \in G$ (Abgeschlossenheit)
- (2) $\forall a, b, c \in G : a \circ (b \circ c) = (a \circ b) \circ c$ (Assoziativität)
- (3) Es existiert ein »neutrales« Element: $\exists e \in G : \forall a \in G : e \circ a = a \circ e = a$
- (4) Zu jedem Gruppenelement existiert ein »inverses« Element: $\forall a \in G : \exists a^{-1} \in G : a \circ a^{-1} = a^{-1} \circ a = e$

Gilt außerdem $a \circ b = b \circ a$ für alle $a, b \in G$, so heißt (G, \circ) eine kommutative (oder Abelsche) Gruppe.

4.1.2. Der Ring. Ein Ring (R, \oplus, \odot) ist eine Menge R mit zwei Operationen $\oplus/\odot : R \times R \rightarrow R$ sodass gilt:

- (1) (R, \oplus) ist eine kommutative Gruppe.
- (2) $\forall a, b \in R : a \odot b \in R$ (Abgeschlossenheit)
- (3) Assoziativität: $\forall a, b, c \in R : a \odot (b \odot c) = (a \odot b) \odot c$.
- (4) Distributivität: $\forall a, b, c \in R, a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$ und $(a \oplus b) \odot c = (a \odot c) \oplus (b \odot c)$.

\oplus und \odot stellen dabei im allgemeinen zwei beliebige Operationen dar. Meist nennt man \oplus »Addition« und \odot »Multiplikation«, obwohl sie mit der bekannten Addition und Multiplikation der reellen Zahlen nicht identisch sein müssen.

(R, \oplus, \odot) nennt man kommutativen Ring, wenn zusätzlich gilt, dass \odot kommutativ ist. Existiert darüber hinaus noch ein neutrales Element bezüglich \odot so heißt die Menge ein kommutativer Ring mit »Einselement«.

4.1.3. Der Integritätsbereich. Ein Integritätsbereich (R, \oplus, \odot) ist ein kommutativer Ring mit Einselement der Nullteilerfrei ist. Das heißt: $\forall a, b \in R, a \odot b = 0 \Rightarrow (a = 0) \vee (b = 0)$

4.1.4. Der Körper. Ein Körper (K, \oplus, \odot) ist ein kommutativer Ring mit Einselement, wobei auch alle inversen Elemente bezüglich \odot existieren. Das heißt (K, \oplus) und $(K \setminus \{0\}, \odot)$ sind kommutative Gruppen. Dabei ist 0 das neutrale Element bezüglich \oplus und heißt »Nullelement«.

¹Eine ausführlichere Behandlung findet man in: VAN DER WAERDEN, B. L.: Algebra I. Springer-Verlag. Berlin 1993.

Literaturverzeichnis

- [1] BARBEAU, E. J.: Polynomials. Springer-Verlag. New York 1989.
- [2] KAPLAN, Michael: Computeralgebra. Springer-Verlag. Berlin 2005.
- [3] OKUNJEW, L. J.: Der Ring der Polynome und der Körper der rationalen Funktionen. In: Alexandroff P.S. u.a. (Hrsg.): Enzyklopädie der Elementarmathematik. Band II. Algebra. VEB Deutscher Verlag der Wissenschaften. Berlin ⁶1977.
- [4] VAN DER WAERDEN, B. L.: Algebra I. Springer-Verlag. Berlin ⁹1993.