Polynome

Thomas Huber

Aktualisiert: 18. April 2018
vers. 1.1.0

Inhaltsverzeichnis

1 Grundlagen

Ein *Polynom* p in einer *Variable* x hat die Form

$$p(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0.$$

Die a_i heissen *Koeffizienten* von p und können ganze, rationale, reelle oder auch komplexe Zahlen sein. Gilt $a_n \neq 0$, dann heisst a_n *L*eitkoeffizient, ist $a_n = 1$, dann heisst p *normiert*. Polynome der Form $p(x) = c$ heissen *konstant*, $p(x) = 0$ nennt man auch das *Nullpolynom*. Man kann auch Polynome in mehreren Variablen betrachten, ein Beispiel mit 3 Variablen ist

$$x^3 + y^3 + z^3 - 3xyz.$$

Seien nun $p(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0$ und $q(x) = b_n x^n + b_{n-1}x^{n-1} + \ldots + b_0$ zwei Polynome. Die *Summe* (Differenz) von p und q erhält man, indem man die jeweiligen Koeffizienten addiert (subtrahiert):

$$p(x) \pm q(x) = (a_n \pm b_n)x^n + (a_{n-1} \pm b_{n-1})x^{n-1} + \ldots + (a_0 \pm b_0).$$

Ist c eine Konstante, dann kann man p mit c multiplizieren:

$$c \cdot p(x) = (c \cdot a_n)x^n + (c \cdot a_{n-1})x^{n-1} + \ldots + (c \cdot a_0).$$

Allgemeiner lassen sich beliebige Poylnome miteinander multiplizieren, indem man einfach mit Hilfe des Distributivgesetzes ausmultipliziert und anschliessend nach Potenzen von x zusammenfasst:

$$p(x) \cdot q(x) = (a_n b_n)x^{2n} + (a_n b_{n-1} + a_{n-1}b_n)x^{2n-1} + \ldots + \left(\sum_{i=0}^{k} a_{k-i}b_i\right) x^k + \ldots + (a_0 b_0).$$

Zum Beispiel gilt

$$\begin{aligned}(x^3 - 2x^2 + 5)(2x^2 - 3) =& 2x^5 - 3x^3 - 4x^4 + 6x^2 + 10x^2 - 15\\ =& 2x^5 - 4x^4 - 3x^3 + 16x^2 - 15.\end{aligned}$$

Die grösste Zahl k, sodass gilt $a_k \neq 0$ heisst *Grad* von p und wir mit $\deg(p)$ bezeichnet. Man definiert ausserdem den Grad des Nullpolynoms als $\deg(0) = -\infty$. Offenbar gelten damit stets die Formeln

$$\begin{aligned}\deg(p \pm q) \leq& \max\{\deg(p), \deg(q)\},\\ \deg(p \cdot q) =& \deg(p) + \deg(q).\end{aligned}$$

1.1 Koeffizienten

Beispiel 1 (Weissrussland 94)**.** *Finde alle Paare (P, Q) normierter, reeller Polynome, sodass gilt*

$$P(Q(x)) = x^{1994}.$$

Beweis. Wir verwenden folgendes allgemeines Resultat. Sind $P(x) = a_m x^m + \ldots + a_r x^r$ und $Q(x) = b_n x^n + \ldots + b_s x^s$ zwei Polynome mit $a_m \neq 0, a_r \neq 0$ und $b_n \neq 0$, $b_s \neq 0$ (die Fälle $m = r$ und $n = s$ sind auch erlaubt), dann hat $P(Q(x))$ die Form

$$P(Q(x)) = c_{mn} x^{mn} + \ldots + c_{rs} x^{rs}$$

mit $c_{mn} \neq 0$ und $c_{rs} \neq 0$. Dies sieht man sofort, wenn man die Definition der Ineinanderschachtelung $P(Q(x))$ verwendet. Genauer gilt $c_{mn} = a_m b_n^m$ und $c_{rs} = a_r b_s^r$.

In unserem Fall soll nun $P(Q(x)) = x^{1994}$ gelten. Dies kann nur dann der Fall sein, wenn $P(x) = x^m$ und $Q(x) = x^n$ beides Monome sind (beachte: P und Q sind normiert) mit $m \cdot n = 1994$. Wegen $1994 = 2 \cdot 997$ ergibt dies die Möglichkeiten $(m, n) = (1, 1994), (2, 997), (997, 2)$ und $(1994, 1)$. □

Beispiel 2. *Schreibe $x^5 + x + 1$ als Produkt von zwei nichtkonstanten Polynomen mit ganzen Koeffizienten.*

Beweis. Wir machen den Ansatz

$$x^5 + x + 1 = (x^3 + ax^2 + bx + c)(x^2 + rx + s).$$

Beachte, dass es keine Einschränkung der Allgemeintheit ist, beide Faktoren normiert zu wählen. Denn das Produkt der Leitkoeffizienten muss gleich dem Leitkoeffizienten auf der linken Seite sein, also gleich 1. Somit sind beide gleich 1 oder beide gleich -1, im zweiten Fall ersetze man beide Faktoren durch ihr Negatives. Multipliziert man nun aus und vergleicht die Koeffizienten, erhält man folgendes Gleichungssystem:

$$\begin{aligned} a + r &= 0 \\ b + ar + s &= 0 \\ c + br + as &= 0 \\ bs + cr &= 1 \\ cs &= 1 \end{aligned}$$

Aus der letzen Gleichung folgt $c = s = \pm 1$ und Auflösen ergibt die einzige Möglichkeit $a = -1, b = 0, c = 1, r = 1, s = 1$. Dies liefert

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

□

Ab und zu muss man Polynome konstruieren, die an vorgegebenen Stellen gewisse Werte annehmen sollen. Dies ist immer möglich, wenn der Grad dse Polynoms höchstens 1 kleiner ist, als die Anzahl vorgegebener Stützstellen. Dies ist der Inhalt von folgendem Satz.

Satz 1.1. *Sei n eine natürliche Zahl und seien $a_0, \ldots, a_n$, $b_0, \ldots, b_n$ fest vorgegebene (reelle oder komplexe) Zahlen, wobei die a_k paarweise verschieden sind. Dann gibt es genau ein Polynom P vom Grad $\leq n$ mit*

$$P(a_k) = b_k \qquad \text{für } 0 \leq k \leq n.$$

Man nennt P das Stüztpolynom zu den Punkten (a_k, b_k). Sind die Stützstellen (a_k, b_k) alle rational bzw. reell, dann hat auch P rationale bzw. reelle Koeffizienten.

Beweis. Wir beweisen zuerst die Existenz eines solchen Stüztpolynoms. Dazu führen wir die sogenannten Lagrange-Polynome ein. Sei

$$L_k(x) = \prod_{i \neq k} \frac{x - a_i}{a_k - a_i},$$

wobei das Produkt über alle $i = 0, \ldots, n$ läuft, $i = k$ ausgenommen. Nach Konstruktion gilt $L_k(a_l) = 0$ falls $k \neq l$ und $L_k(a_k) = 1$. Das Polynom

$$P(x) = \sum_{k=0}^{n} b_k \cdot L_k(x)$$

erfüllt dann alle Bedingungen. Ausserdem haben die L_k lauter rationale bzw. reelle Koeffizienten, wenn alle a_k rational bzw. reell sind. Gilt dies auch für die b_k, dann besitzt P ebenfalls rationale bzw. reelle Koeffizienten. Die Eindeutigkeit werden wir später beweisen, sie folt unmittelbar aus Satz 1.10. □

Es sei hier ausdrücklich darauf hingewiesen, dass P nicht notwendig *ganze* Koeffizienten hat, wenn a_k, b_k alle ganz sind. Ein Gegenbeispiel ist das Polynom $P(x) = \frac{x(x+1)}{2}$, welches keine ganzen Koeffizienten hat, dennoch ist $P(x) \in \mathbb{Z}$ für alle $x \in \mathbb{Z}$.

Beispiel 3. *Sei P ein Poylnom vom Grad $\leq n$, sodass gilt*

$$P(k) = \binom{n+1}{k}^{-1}, \qquad k = 0, 1, \ldots, n.$$

Bestimme den Wert von $P(n+1)$.

Lösung. Die Konstruktion mittels des Lagrange-Polynome ergibt

$$P(x) = \sum_{k=0}^{n} \prod_{i \neq k} \left(\frac{x - i}{k - i} \right) P(k).$$

Nun gilt

$$\begin{aligned}\prod_{i\neq k}\left(\frac{n+1-i}{k-i}\right) =& \frac{n+1}{k}\cdot\frac{n}{k-1}\cdots\frac{n-k+2}{1}\cdot\frac{n-k}{-1}\cdots\frac{1}{k-n}\\ =&(-1)^{n-k}\binom{n+1}{k}.\end{aligned}$$

Somit erhalten wir

$$P(n+1)=\sum_{k=0}^{n}(-1)^{n-k}=\begin{cases}0 & \text{für } n \text{ ungerade}\\ 1 & \text{für } n \text{ gerade.}\end{cases}$$

□

Nicht immer ist der Weg über die Lagrange-Polynome der einfachste. Oft geht es schneller, ein Gleichungssystem für die gesuchten Koeffizienten aufzustellen.

Beispiel 4. *Bestimme ein Polynom P vom Grad 3, sodass gilt $P(n)=2^{n-1}$ für $n=1,2,3,4$.*

Lösung. Wir setzen $P(x)=ax^3+bx^2+cx+d$ und erhalten ein Gleichungssystem

$$\begin{aligned}a+b+c+d=&P(1)=1\\ 8a+4b+2c+d=&P(2)=2\\ 27a+9b+3c+d=&P(3)=4\\ 64a+16b+4c+d=&P(4)=8\end{aligned}$$

mit der einzigen Lösung $a=\frac{1}{6}$, $b=-\frac{1}{2}$, $c=\frac{4}{3}$ und $d=0$.

□

1.2 Teilbarkeit

Unter Polynomen verstehen wir in diesem Abschnitt Polynome mit Koeffizienten in $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ oder $\mathbb{C}$. Als Abkürzung verwenden wir dabei den Buchstaben K stellvertretend für eine der Mengen $\mathbb{Z},\mathbb{Q},\mathbb{R}$ oder $\mathbb{C}$. Eine Zahl $a\in K$ heisst eine *Einheit*, falls a in K invertierbar ist. Das heisst, falls eine Zahl $b\in K$ existiert mit $ab=1$. Offensichtlich sind ±1 die einzigen Einheiten in $\mathbb{Z}$. während für $K=\mathbb{Q},\mathbb{R},\mathbb{C}$ alle von 0 verschiedenen Elemente Einheiten sind. Diese kleine aber feine Sonderrolle für $\mathbb{Z}$ ist mit die Ursache vieler Probleme und letzlich der Grund dafür, dass viele der folgenden Resultat im Fall $K=\mathbb{Z}$ etwas anders lauten, respektive nur für normierte Polynome gelten. Zwei Polynome $p,q\in K[x]$ heissen *äquivalent*, falls eine Einheit $a\in K$ existiert mit $p=a\cdot q$.

Seien $p,q\in K[x]$ beliebige Polynome. Wir sagen, dass p durch q in K *teilbar* ist, falls ein Polynom $a\in K[x]$ existiert mit $p=a\cdot q$. Ein Polynom $p\in K[x]$ heisst *irreduzibel* in $K[x]$

oder auch irreduzibel über K, falls es keine Einheit ist und falls aus einer Darstellung der Form $p = a \cdot b$ mit Polynomen aus $K[x]$ stets folgt, dass a oder b eine Einheit ist. Es ist dabei sehr entscheidend, welche Koeffzienten man betrachtet. Zum Beispiel ist das Polynom $2x - 4$ irreduzibel über $\mathbb{Q}$ aber nicht irreduzibel über $\mathbb{Z}$, denn es gilt $2x - 4 = 2(x - 2)$ und keiner der Faktoren ist eine Einheit in $\mathbb{Z}$. Als weiteres Beispiel betrachten wir das Polynom $p(x) = x^4 - 2$. Man rechnet leicht nach, dass p irreduzibel über $\mathbb{Z}$ und $\mathbb{Q}$ ist (man kann zum Beispiel das Kriterium von Eisenstein verwenden, siehe unten). Andererseits zerfällt p über $\mathbb{R}$ bzw. $\mathbb{C}$ wie folgt in Faktoren:

$$p(x) = (x^2 - \sqrt{2})(x^2 + \sqrt{2}) = (x - \sqrt[4]{2})(x + \sqrt[4]{2})(x - i\sqrt[4]{2})(x + i\sqrt[4]{2}).$$

Wie bei den ganzen Zahlen steht auch für Polynome eine Division mit Rest zur Verfügung. Wir formulieren den folgenden wichtigen Satz nur für den Fall, wo das Polynom q normiert ist. Für $K = \mathbb{Q}, \mathbb{R}$ oder $\mathbb{C}$ ist das natürlich unerheblich, man kann beliebige Polynome q zulassen, da der Leitkoeffzient von q stets eine Einheit in K ist. Genauer: Man dividiere p und q einfach durch den Leitkoeffzienten von q und befindet sich dann in der normierten Situation. Für $K = \mathbb{Z}$ ist das eben nicht möglich, und der Satz ist für nicht normierte Polynome q im Allgemeinen falsch. Wir betonen diese Tatsache daher, weil sie der Grund für alle Schwierigkeiten ist, die sich im Folgenden für $K = \mathbb{Z}$ ergeben werden.

Satz 1.2 (Division mit Rest)**.** *Sei $p(x) \in K[x]$ ein beliebiges Polynom und $q(x) \in K[x]$ ein normiertes Polynom. Dann gibt es eindeutig bestimmte Polynome $d(x)$ und $r(x)$ aus $K[x]$ mit $\deg(r) < \deg(q)$, sodass gilt*

$$p(x) = d(x) \cdot q(x) + r(x).$$

$r(x)$ heisst Rest *der Division. Es gilt genau dann $r(x) = 0$, wenn p durch q teilbar ist.*

Die Division mit Rest ist nun der Ausgangspunkt für die ganze Arithmetik von Polynomen, genau wie bei den ganzen Zahlen. So mag es auch nicht erstaunen, dass alle Resultate im ersten Abschnitts des Zahlentheorieskripts wörtlich auch für Polynome gelten. Wir geben die Resultate ohne Begründung an, vieles beweist man analog zum Fall der ganzen Zahlen. Genau wie für ganze Zahlen existiert eine "Primfaktorzerlegung"für Polynome:

Theorem 1.3. *Sei $p \in K[x]$ ein Polynom, welches nicht das Nullpolynom ist. Dann existieren nichtäquivalente irreduzible Polynome $p_1, \ldots, p_r \in K[x]$ und natürliche Zahlen $a_1, \ldots, a_r$ mit*

$$p = p_1^{a_1} \cdot p_2^{a_2} \cdots p_r^{a_r}.$$

Die Zahlen a_i sind dabei eindeutig bestimmt, die Polynome p_i sind eindeutig bis auf Äquivalenz.

Etwas störend mag hier sein, dass die irreduziblen Faktoren p_i nur nur bis auf Äquivalenz eindeutig bestimmt sind. Dies lässt sich aber einfach beheben. Im Fall $K = \mathbb{Q}, \mathbb{R}$ oder $\mathbb{C}$ ist jedes Polynom äquivalent zu einem einzigen normierten Polynom. Wir können uns also quasi auf normierte Polynome beschränken und die normierten, irreduziblen Polynome als Standardvertretersystem betrachten. Auf diese Weise erhält 1.3 folgende schöne Form.

Theorem 1.4. *Sei $K = \mathbb{Q}, \mathbb{R}$ oder $\mathbb{C}$. Sei $p \in K[x]$ ein Polynom, welches nicht das Nullpolynom ist. Dann existieren verschiedene normierte, irreduzible Polynome $p_1, \ldots, p_r \in K[x]$, natürliche Zahlen $a_1, \ldots, a_r$ und eine Einheit $u \in K$ mit*

$$p = u \cdot p_1^{a_1} \cdot p_2^{a_2} \cdots p_r^{a_r}.$$

Die a_i , die p_i und die Einheit u sind dabei eindeutig bestimmt.

Im Fall $K = \mathbb{Z}$ ist die Situation etwas anders. Die einzigen Einheiten in $\mathbb{Z}$ sind ± 1. Daraus folgt, dass jedes Polynom äquivalent ist zu einem einzigen Polynom mit positivem Leitkoeffzient. Als Vertretersystem der irreduziblen Polynome über $\mathbb{Z}$ können wir also diejenigen irreduziblen Polynome mit positivem Leitkoeffzient wählen. Theorem 1.3 wird in diesem Fall also zu

Theorem 1.5. *Sei $p \in Z[x]$ ein Polynom, welches nicht das Nullpolynom ist. Dann existieren verschiedene irreduzible Polynome $p_1, \ldots, p_r \in K[x]$ mit positivem Leitkoeffzient, natürliche Zahlen $a_1, \ldots, a_r$ und ein Vorzeichen $\epsilon = \pm 1$ mit*

$$p = \epsilon \cdot p_1^{a_1} \cdot p_2^{a_2} \cdots p_r^{a_r}.$$

Die a_i , die p_i und das Vorzeichen ϵ sind dabei eindeutig bestimmt.

Es drängt sich nun natürlich die Frage auf, wie man die Menge aller irreduziblen Polynome über K beschreiben kann. Wir werden dies für $K = \mathbb{R}$ und $\mathbb{C}$ in Satz 1.14 vollständig beantworten. Für $K = \mathbb{Z}$ und $\mathbb{Q}$ ist das Problem allerdings sehr viel komplizierter. Zum Beispiel sind alle Primzahlen irreduzible, konstante Polynome in $\mathbb{Z}[x]$. Wir zeigen zuerst die etwas überraschende Tatsache, dass Irreduzibilität über $\mathbb{Z}$ bzw. $\mathbb{Q}$ im Wesentlichen dasselbe ist. Dazu benötigen wir zwei Resultate, die sehr nützlich sind, leider aber nicht ganz einfache Beweise haben.

Satz 1.6 (Gauss)**.** *Sei $p \in \mathbb{Z}[x]$ ein normiertes Polynom und es gelte $p = a \cdot b$ mit normierten Polynomen $a, b \in \mathbb{Q}[x]$. Dann haben a und b automatisch ganze Koeffzienten.*

Für das nächste Resultat benötigen wir den Begriff der Primitivität eines Polynoms. Sei $p(x) = a_n x^n + \ldots + a_1 x + a_0$ ein Polynom. Dann heisst p primitiv, falls alle Koeffzienten ganz sind und falls $\mathrm{ggT}(a_n, \ldots, a_1, a_0) = 1$ gilt. Zum Beispiel ist jedes normierte Polynom mit ganzen Koeffzienten primitiv. Beachte, dass jedes Polynom mit rationalen Koeffzienten äquivalent ist zu einem primitiven Polynom. Man multipliziere dieses einfach mit dem kleinsten gemeinsamen Vielfachen der Nenner aller Koeffzienten.

Satz 1.7. *Sei $p \in \mathbb{Z}[x]$ ein Polynom. p ist genau dann irreduzibel über $\mathbb{Z}$, wenn eine der folgenden Bedingungen erfüllt ist:*

1. *p ist bis auf das Vorzeichen eine Primzahl.*
2. *p ist primitiv und irreduzibel über $\mathbb{Q}$.*

Wir beschränken uns im Folgenden also auf nichtkonstante, primitive Polynome. Ein sehr nützliches Irreduzibilitätskriterium ist jenes von Eisenstein.

Satz 1.8 (Eisenstein). *Sei $f(x) = a_n x^n + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$ ein primitives Polynom vom Grad > 0. Weiter sei p eine Primzahl mit*

$$p \nmid a_n, \qquad p \mid a_i \text{ für } i < n, \qquad p^2 \nmid a_0.$$

Dann ist f irreduzibel über $\mathbb{Z}$.

Zur Illustration beweisen wir die Irreduzibilität einer wichtigen Familie von Polynomen. Es handelt sich um sogenannte Kreisteilungspolynome, auf die wir später eingehen werden. Dieses Beispiel zeigt unter anderem, dass es über $\mathbb{Z}$ irreduzible Polynome von beliebig hohem Grad gibt.

Beispiel 5. *Sei p eine Primzahl. Beweise, dass das Polynom $f(x) = x^{p-1} + x^{p-2} + \ldots + x + 1$ irreduzibel ist über $\mathbb{Z}$.*

Lösung. Wir betrachten anstelle von $f(x)$ das Polynom $f(x+1)$. Offensichtlich zerfallen beide Polynome in gleicher Weise in irreduzible Faktoren, es genügt also zu zeigen, dass letzteres irreduzibel ist. Mittels geometrischer Reihe findet man

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

Die Irreduzibilität folgt nun direkt aus dem Satz von Eisenstein, denn alle Koeffzienten ausser dem ersten sind durch p teilbar, und der konstante Koeffzient ist gleich p und daher sicher nicht durch p^2 teilbar. □

1.3 ggT und kgV

Aufgrund der Division mit Rest überträgt sich der entsprechende Abschnitt aus dem Zahlentheorieskript wörtlich. Im Fall $K = \mathbb{Z}$ funktioniert der Euklidsche Algorithmus im allgemeinen allerdings nicht mehr.

1.4 Nullstellen

Sei $p \in K[x]$ ein beliebiges Polynom und $a \in K$ eine Zahl. Wir sagen, dass a eine *Nullstelle* von p ist, falls $p(a) = 0$ gilt. Division mit Rest für p und das lineare Polynom $(x - a)$ liefert eindeutige Polynome d und r mit $p(x) = d(x) \cdot (x - a) + r$, wobei r einen kleineren Grad als $x - a$ hat und daher konstant ist. Setzt man in dieser Gleichung $x = a$, dann folgt $r = p(a)$. Dies ergibt das folgende wichtige Resultat.

Satz 1.9. *Sei $p \in K[x]$ ein Polynom und sei $a \in K$ eine Zahl. Dann existiert ein eindeutig bestimmtes Polynom $d(x) \in K[x]$ mit*

$$p(x) = d(x) \cdot (x - a) + p(a).$$

Insbesondere ist a genau dann eine Nullstelle von p, wenn das lineare Polynom $(x-a)$ ein Faktor ist von p.

Nun kann es natürlich sein, dass p nicht nur durch $(x-a)$, sondern sogar durch eine grössere Potenz dieses Linearfaktors teilbar ist. Dementsprechend muss man a in diesem Falle auch mehrfach als Nullstelle zählen. Wir sagen daher, dass a eine *k-fache Nullstelle* von p (oder eine Nullstelle *der Vielfachheit k* von p) ist, wenn p durch $(x-a)^k$ teilbar ist, nicht aber durch $(x-a)^{k+1}$. Wir erhalten nun folgende Abschätzung für die Anzahl Nullstellen eines Polynoms:

Satz 1.10 (Identitätssatz)**.**

(a) Sei $p \in K[x]$ ein Polynom vom Grad $n \geq 0$. Dann besitzt p höchstens n Nullstellen in K, dabei werden mehrfache Nullstellen auch mehrfach gezählt. Ausserdem besitzt p genau dann n Nullstellen in K, wenn p über K vollständig in Linearfaktoren zerfällt (also ein Produkt von Polynomen vom Grad ≤ 1 mit Koeffzienten in K ist).

(b) Ist p ein Polynom vom Grad $\leq n$ und besitzt p mindestens $n+1$ Nullstellen (mit Vielfachheit gezählt), dann ist p das Nullpolynom.

(c) Sind p, q zwei Polynome vom Grad $\leq n$ und stimmen p und q an mindestens $n+1$ Stellen überein, dann gilt $p = q$.

Beweis. Nehme an, p habe die Nullstellen $a_1, \ldots, a_r \in K$ mit Vielfachheiten $m_1, \ldots, m_r$. Nach Satz 1.9 gibt es ein Polynom $d \in K[x]$ mit

$$p(x) = (x-a_1)^{m_1} \cdots (x-a_r)^{m_r} \cdot d(x).$$

Wegen $p \neq 0$ ist auch $d \neq 0$, sei $m := \deg d \geq 0$. Vergleicht man die Grade auf beiden Seiten der Gleichung, dann folgt $\sum m_i = n - m \leq n$, dies beweist (a). Die Aussage in (b) folgt nun direkt, denn wäre p nicht das Nullpolynom, ergäbe dies ein Widerspruch zu (a). Schliesslich folgt (c) aus (b), angewendet auf die Differenz $p - q$. □

Beispiel 6 (Spanien 2000)**.** *Betrachte die Polynome*

$$\begin{aligned} P(x) =& x^4 + ax^3 + bx^2 + cx + 1, \\ Q(x) =& x^4 + cx^3 + bx^2 + ax + 1, \end{aligned}$$

wobei a, b, c reelle Zahlen sind mit $a \neq c$. Finde Bedingungen an a, b, c, sodass P und Q mindestens zwei gemeinsame Nullstellen haben, und finde in diesen Fällen alle Nullstellen von P und Q.

Lösung. Jede gemeinsame Nullstelle von P und Q ist auch eine Nullstelle ihrer Differenz. Wegen

$$P(x) - Q(x) = (a-c)x(x^2-1)$$

und $a \neq c$ kommen für diese gemeinsamen Nullstellen nur $x = 0, 1, -1$ in Frage. Nun ist aber $x = 0$ nie eine Nullstelle von P oder Q, also müssen $x = \pm 1$ die gemeinsamen

Nullstellen sein. Die Gleichungen $P(1) = P(-1) = 0$ liefern die Bedingungen $a+b+c+2 = -a+b-c+2 = 0$, also $a = -c$ und $b = -2$. In diesem Fall gilt nun aber

$$\begin{aligned} P(x) =& x^4 - 2x^2 + 1 + a(x^3 - x) = (x^2-1)^2 + ax(x^2-1) = (x^2 + ax - 1)(x^2-1), \\ Q(x) =& x^4 - 2x^2 + 1 - a(x^3 - x) = (x^2-1)^2 - ax(x^2-1) = (x^2 - ax - 1)(x^2-1). \end{aligned}$$

Die Nullstellen von P sind also

$$x = 1, -1, \frac{-a + \sqrt{a^2+4}}{2}, \frac{-a - \sqrt{a^2+4}}{2}.$$

Die Nullstellen von Q sind

$$x = 1, -1, \frac{a + \sqrt{a^2+4}}{2}, \frac{a - \sqrt{a^2+4}}{2}.$$

Insbesondere haben P und Q wirklich die beiden gemeinsamen Nullstellen $x = \pm 1$. □

Für Polynome mit ganzen (oder rationalen) Koeffzienten sind die *rationalen* Nullstellen einfach zu finden. Das folgende Lemma schränkt die Möglichkeiten für solche Nullstellen stark ein.

Lemma 1.11. *Sei $p(x) = a_n x^n + \ldots + a_1 x + a_0$ ein Polynom mit ganzen Koeffzienten und $a_n, a_0 \neq 0$. Ist u eine rationale Nullstelle von p und gilt $u = r/s$ mit teilerfremden ganzen Zahlen r, s, dann gilt $r \mid a_0$ und $s \mid a_n$.*

Beweis. Nach Voraussetzung gilt $a_n u^n + \ldots + a_1 u + a_0 = 0$. Multipliziert man diese Gleichung mit s^n, dann folgt

$$a_n r^n + a_{n-1} r^{n-1} s + \ldots + a_1 r s^{n-1} + a_0 s^n = 0.$$

Da s alle Summanden ausser dem ersten teilt, und die Summe gleich 0 ist, muss auch $s \mid a_n r^n$ gelten. Da aber s und r teilerfremd sind, folgt in der Tat $s \mid a_n$. Analog folgt $r \mid a_0 s^n$ und somit $r \mid a_0$. □

Für reelle Polynome treten nicht reelle Nullstellen immer in konjugierten Paaren auf, dies ist der Inhalt vom nächsten Satz. Für eine komplexe Zahl $z = x + iy$ ist die Konjugierte Zahl definiert durch $z = x - iy$ und ist das Spiegelbild von z n der reellen Achse.

Satz 1.12. *Ist $p \in \mathbb{R}[x]$ ein reelles Polynom und ist $a \in C$ eine komplexe Zahl. Dann gilt $p(\overline{a}) = \overline{p(a)}$. Ist a insbesondere eine Nullstelle der Vielfachheit n von p, dann ist auch $\overline{a}$ eine Nullstelle der Vielfachheit n von p.*

Beweis. Sei $p(x) = a_n x^n + \ldots + a_1 x + a_0$. Es gilt nun

$$\begin{aligned} p(\overline{a}) =& a_n \cdot (\overline{a})^n + \ldots + a_1 \cdot \overline{a} + a_0 = \overline{a_n} \cdot \overline{(a^n)} + \ldots + \overline{a_1} \cdot \overline{a} + \overline{a_0} \\ =& \overline{a_n \cdot a^n + \ldots + a_1 \cdot a + a_0} = \overline{p(a)}. \end{aligned}$$

Daraus folgt insbesondere, dass a genau dann eine Nullstelle von p ist, wenn $\overline{a}$ ebenfalls eine Nullstelle ist. Ist dies der Fall, dann gilt $p(x) = (x-a)(x-\overline{a}) \cdot p_1(x)$. Da $(x-a)(x-\overline{a}) = x^2 - 2Re(a)x + |a|^2$ ein reelles Polynom ist, hat auch p_1 reelle Koeffzienten. Ist nun a auch eine Nullstelle von p_1 , kann man wieder einen Faktor $(x-a)(x-\overline{a})$ abspalten. Wiederholung dieses Verfahrens zeigt, dass die Vielfachheit der Nullstellen a und $\overline{a}$ dieselbe sein muss. □

Wir haben nun schon viel über die Nullstellen von Polynomen gesagt, die Frage nach der Existenz solcher Nullstellen wurde aber noch nicht beantwortet.

Theorem 1.13 (Fundamentalsatz der Algebra)**.** *Jedes nichtkonstante komplexe Polynom besitzt eine komplexe Nullstelle*

Durch sukzessives Abspalten von Linearfaktoren folgt daraus nun sofort, dass jedes komplexe Polynom vom Grad $n \geq 1$ genau n komplexe Nullstellen besitzt, mit Vielfachheit gezählt. Wir sind nun endlich in der Lage, alle irreduziblen reellen und komplexen Polynome zu klassifizieren.

Satz 1.14.

1. *Die irreduziblen komplexen Polynome sind genau die linearen.*
2. *Jedes irreduzible reelle Polynom ist entweder linear oder quadratisch von der Form $ax^2 + bx + c$ mit negativer Diskriminante $D = b^2 - 4ac < 0$*

Beweis. (a) folgt direkt aus Theorem 1.13. Sei nun p ein reelles irreduzibles Polynom. Ebenfalls nach Theorem 1.13 besitzt p eine komplexe Nullstelle u. Ist u reell, dann besitzt p einen linearen Faktor, muss also selbst liner sein. Ist u nicht reell, dann besitzt $p(x)$ den reellen Faktor $(x-u)(x-\overline{u})$, muss also ein konstantes Vielfaches davon sein. Ein quadratisches Polynom $ax^2 + bx + c$ besitzt aber bekanntlich die komplexen Nullstellen $(-b \pm \sqrt{D})/(2a)$. Diese sind genau dann nicht reell und das Polynom somit irreduzibel über $\mathbb{R}$, wenn $D < 0$ ist. □

Beispiel 7. *Sei P ein reelles Polynom, sodass für alle in $x \in \mathbb{R}$ gilt $P(x) \geq 0$. Beweise, dass es reelle Polynome Q_1 und Q_2 gibt mit $P = Q_1^2 + Q_2^2$.*

Beweis. Der Leitkoeffzient c von P muss positiv sein, denn sonst gilt $P(x) < 0$ für grosse x. Nach Satz 1.14 gibt es reelle Zahlen $a_1, \ldots, a_r$ und $b_1, \ldots, b_s, c_1, \ldots, c_s$ mit $b_i^2 - 4c_i <$ und

$$P(x) = c \prod_{i=1}^{r} (x - a_i) \prod_{i=1}^{s} (x^2 + b_i x + c_i).$$

Da P überall nichtnegativ ist, müssen die reellen Nullstellen a_i alle eine gerade Vielfachheit haben. Das bedeutet aber, dass das erste Produkt das Quadrat eines reellen Polynoms ist Ausserdem ist $c = (\sqrt{c})^2$ natürlich ebenfalls das Quadrat eines reellen Polynoms. Es genügt somit zu zeigen, dass das zweite Produkt die Summe von zwei Quadraten reeller

Polynome ist. Jeder Faktor lässt sich schreiben als

$$x^2 + b_i x + c_i = \left(x + \frac{b_i}{2}\right)^2 + \left(c_i - \frac{b_i^2}{4}\right),$$

und wegen $c_i > b_i^2/4$ ist der zweite Summand positiv, also das Quadrat einer reellen Zahl. Somit ist jeder Faktor die Summe von zwei Quadraten, also auch deren Produkt, denn es gilt die berühmte Formel von Euler

$$(X^2 + Y^2)(Z^2 + U^2) = (XZ + YU)^2 + (XU - YZ)^2.$$

□

Beispiel 8. *Finde alle Polynome P, sodass die folgende Identität gilt*

$$P(x)P(x+1) = P(x^2).$$

Beweis. Das Nullpolynom ist offentsichtlich eine Lösung. Wir nehmen im Folgenden $P \neq 0$ an. Sei α eine komplexe Nullstelle von P. Setze $x = \alpha$, dann folgt $P(\alpha^2) = 0$, also ist auch α^2 eine Nullstelle. Wiederholt man dies, dann folgt, dass $\alpha, \alpha^2, \alpha^4, \alpha^8, \ldots$ alles Nullstellen von P sind. Da P nicht identisch verschwindet, kann P nur endlich viele Nullstellen haben. Daraus folgt aber $\alpha = 0$ oder $|\alpha| = 1$. Setzt man nun $x = \alpha - 1$, dann folgt ähnlich, dass auch $(\alpha - 1)^2$ eine Nullstelle von P ist. Wiederum nach obigem Argument ist somit $\alpha - 1 = 0$ oder $|\alpha - 1| = 1$. Wir nehmen nun an, es gelte $\alpha \neq 0, 1$ und führen dies zu einem Widerspruch. Es muss also $|\alpha| = |\alpha - 1| = 1$ gelten, das heisst beide Zahlen liegen auf dem Einheitskreis und haben eine horizontale Distanz von 1. Man überlegt sich mit einer kleinen Skizze sofort, dass dies nur für $\alpha_1 = e^{i\pi/3}$ und $\alpha^2 = e^{i5\pi/3}$ gilt. Nun ist nach obiger Diskussion aber auch α_1^2 bzw. α_2^2 eine Nullstelle. Wegen $\alpha_1^2 = e^{i2\pi/3} \neq \alpha_1, \alpha_2, 0, 1$ und $\alpha_2^2 = e^{i4\pi/3} \neq \alpha_1, \alpha_2, 0, 1$ ergibt dies den gewünschten Widerspruch.
Die einzigen möglichen Nullstellen von P sind daher 0 und 1. Die gesuchten Polynome sind also von der Form $P(x) = cx^m(x-1)^n$ mit einer komplexen Zahl $c \neq 0$ und nichtnegativen ganzen Zahlen m, n. Einsetzen in die Gleichung ergibt nun

$$c^2(x+1)^m x^{m+n}(x-1)^n = cx^{2m}(x^2-1)^n.$$

Verwendet man die Identität $x^2 - 1 = (x-1)(x+1)$ und vergleicht die Linearfaktoren und den Leitkoeffzienten auf beiden Seiten, dann folgt $c = 1$ und $m = n$. Die Lösungen sind also $P = 0$ sowie für $n \geq 1$ die Polynome

$$P(x) = x^n(x-1)^n$$

□

2 Symmetrische Polynome

2.1 Elementarsymmetrische Polynome

Wir betrachten in diesem Abschnitt Polynome in n Variablen $x_1, \ldots, x_n$. Ein solches Polynom heisst *symmetrisch*, falls es sich nicht ändert, wenn man die Variablen in irgendeiner Weise permutiert. Etwas formaler kann man es so ausdrücken: Ein Polynom $P(x_1, \ldots, x_n)$ ist symmetrisch, falls für jede Permutation π von $\{1, 2, \ldots, n\}$ gilt

$$P(x_{\pi(1)}, x_{\pi(2)}, \ldots, x_{\pi(n)}) = P(x_1, \ldots, x_n)$$

Beispiele von symmetrischen Polynomen in drei Variablen x, y, z sind

$$x^n + y^n + z^n + xyz, \qquad xy + yz + zx - 4, \qquad (x-y)^{2n} + (y-z)^{2n} + (z-x)^{2n}.$$

Die in gewissem Sinne einfachsten symmetrischen Polynome Variablen sind die sogenannten *elementarsymmetrischen* Polynome $s_1, \ldots, s_n$. Sie sind wie folgt definiert:

$$s_k = \sum_{i_1 < i_2 < \ldots < i_k} x_{i_1} x_{i_2} \cdots x_{i_k}, \qquad 1 \leq k \leq n.$$

Mit anderen Worten, s_k ist die Summe von allen möglichen Produkten von k verschiedenen der n Variablen. Zur Veranschaulichung schreiben wir sie im Fall $n = 2, 3$ explizit hin. Für $n = 2$ ist (mit den Variablen x, y)

$$u = s_1 = x + y, \qquad v = s_2 = xy.$$

Für $n = 3$ ist (in den Variablen x, y, z)

$$u = s_1 = x + y + z, \qquad v = s_2 = xy + yz + zx, \qquad w = s_3 = xyz.$$

Die Bezeichnungen u, v, w sind in diesem Falle üblich.

Sehr wichtig ist nun die Tatsache, dass man *jedes* symmetrische Polynom auf genau eine Art als Polynom in den elementarsammetrischen Polynomen ausdrücken kann.

Theorem 2.1. *Sei P ein symmetrisches Polynom in n Variablen $x_1, \ldots, x_n$. Dann gibt es genau ein Polynom Q in n Variablen, sodass gilt*

$$P(x_1, x_2, \ldots, x_n) = Q(s_1, s_2, \ldots, s_n).$$

Wir übergehen den etwas technischen Beweis, bemerken aber, dass die Existenz des Polynoms Q durch eine explizite Konstruktionsvorschrift gesichert ist. Diese ist aber für den praktischen Gebrauch doch etwas unhandlich. Wir geben gleich Beispiele dafür, wie man für ein gegebenes symmetrisches Polynom vorgeht, um Q zu konstruieren. Die Grundregel ist stets: "Die reinen Potenzen zuerst!"

Beispiel 9. *Faktorisiere das Polynom*

$$x^3 + y^3 + z^3 - 3xyz.$$

Beweis. Wir drücken das Polynom durch u, v, w aus. Zuerst gilt $u^2 = x^2 + y^2 + z^2 + 2(xy + yz + zx)$ und somit $x^2 + y^2 + z^2 = u^2 - 2v$. Daraus folgt nun $u \cdot (u^2 - 2v) = (x + y + z)(x^2 + y^2 + z^2) = (x^3 + y^3 + z^3) + (x^2y + x^2z + y^2x + y^2z + z^2x + z^2y)$. Andererseits ist $uv = (x^2y + x^2z + y^2x + y^2z + z^2x + z^2y) + 3xyz$. Zusammen ergibt dies

$$x^3 + y^3 + z^3 = u(u^2 - 2v) - (uv - 3w) = u^3 - 3uv + 3w$$

Daraus erhält man schliesslich

$$\begin{aligned} x^3 + y^3 + z^3 - 3xyz =& (u^3 - 3uv + 3w) - 3w = u(u^2 - 3v) \\ =& (x + y + z)(x^2 + y^2 + z^2 - xy - yz - zx). \end{aligned}$$

□

Beispiel 10. *Sei $n \geq 0$ eine ganze Zahl und sei $P_n = x^n + y^n + z^n$. Beweise für $n \geq 2$ die folgende Rekursionsformel:*

$$P_{n+1} = uP_n - vP_{n-1} + wP_{n-2}.$$

Drücke damit P_n als Polynom in u, v, w aus für $n \leq 5$.

Lösung. Die Rekursionsformel ergibt sich aus folgender Rechnung:

$$\begin{aligned} uP_n =& (x + y + z)(x^n + y^n + z^n) \\ =& (x^{n+1} + y^{n+1} + z^{n+1}) + (x^ny + x^nz + y^nx + y^nz + z^nx + z^ny) \\ =& P_{n+1} + (xy + yz + zx)(x^{n-1} + y^{n-1} + z^{n-1}) - (x^{n-1}yz + y^{n-1}zx + z^{n-1}xy) \\ =& P_{n+1} + vP_{n-1} - wP_{n-2}. \end{aligned}$$

Ausserdem gilt $P_0 = 3, P_1 = u$ und $P_2 = u^2 - 2v$. Damit ergibt sich der Reihe nach

$$\begin{aligned} P_3 =& uP_2 - vP_1 + wP_0 = u^3 - 3uv + 3w, \\ P_4 =& uP_3 - vP_2 + wP_1 = u^4 - 4u^2v + 2v^2 + 4uw, \\ P_5 =& uP_4 - vP_3 + wP_2 = u^5 - 5u^3v + 5uv^2 + 5u^2w - 5vw. \end{aligned}$$

□

Am letzten Beispiel sieht man gut, dass die Sache recht schnell kompliziert wird.

2.2 Der Satz von Vieta

In diesem Abschnitt besprechen wir den sehr wichtigen Satz von Vieta. Wir betrachten dazu ein Polynom $P(x) = a_n x^n + \ldots + a_1 x + a_0$ in *einer* Variablen. Dieses Polynom besitzt genau n komplexe Nullstellen $\alpha_1, \ldots, \alpha_n$ (mit Vielfachheit gerechnet). Diese Nullstellen sind natürlich durch die Koeffzienten des Polynoms eindeutig bestimmt. Es ist aber sehr kompliziert (und für $n \geq 5$ im Allgemeinen sogar unmöglich), diese Nullstellen explizit zu berechnen. Die umgekehrte Richtung, nämlich die Koeffzienten aus den Nullstellen zu berechnen, ist jedoch sehr einfach, wie der folgende Satz zeigt.

Satz 2.2 (Vieta)**.** *Sei $P(x) = a_n x^n + \ldots + a_1 x + a_0$ ein Polynom mit $a_n \neq 0$. Seien $\alpha_1, \ldots, \alpha_n$ die komplexen Nullstellen von P (mit Vielfachheit gerechnet), und sei s_k das k-te elementarsymmetrische Polynom in den α_i. Dann gilt*

$$s_k := s_k(\alpha_1, \ldots, \alpha_n) = (-1)^k \cdot \frac{a_{n-k}}{a_n}, \qquad \text{für } 1 \leq k \leq n.$$

Beweis. Es gilt nach Voraussetzung

$$P(x) = a_n x^n + \ldots + a_1 x + a_0 = a_n (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n).$$

Multipliziert man das Produkt auf der rechten Seite aus, dann folgt per Definition der elementarsymmetrischen Polynome s_k

$$\prod_{k=1}^{n} (x - \alpha_k) = x^n - s_1 x^{n-1} + s_2 x^{n-2} - + \ldots + (-1)^n s_n.$$

Setzt man dies oben ein und vergleicht die Koeffzienten auf beiden Seiten der Gleichung, dann folgt die Behauptung. □

Der Satz von Vieta erlaubt es also, die elementarsymmetrischen Polynome der Nullstellen direkt durch die Koeffzienten auszudrücken, ohne die Nullstellen selber zu kennen. Zusammen mit Theorem 2.1 lassen sich damit natürlich *alle* symmetrischen Polynome in den Nullstellen berechnen. Dies ist entscheidend und kann sehr oft verwendet werden.

Beispiel 11 (Kananda 96)**.** *Seien α, β und γ die Nullstellen des Polynoms $x^3 - x - 1$. Finde den Wert von*

$$A = \frac{1-\alpha}{1+\alpha} + \frac{1-\beta}{1+\beta} + \frac{1-\gamma}{1+\gamma}.$$

1. Lösung. Wir verwenden die übliche Notation $u = \alpha + \beta + \gamma$, $v = \alpha\beta + \beta\gamma + \gamma\alpha$ und $w = \alpha\beta\gamma$. Eine kurze Rechnung zeigt

$$\begin{aligned} A =& \frac{(1-\alpha)(1+\beta)(1+\gamma) + (1-\beta)(1+\gamma)(1+\alpha) + (1-\gamma)(1+\alpha)(1+\beta)}{(1+\alpha)(1+\beta)(1+\gamma)} \\ =& \frac{3 + u - v - 3w}{1 + u + v + w}. \end{aligned}$$

Der Satz von Vieta liefert nun

$$u = 0, \qquad v = -1, \qquad w = 1,$$

und somit gilt $A = 1$. □

2. Lösung. Etwas einfacher wird die Lösung, wenn man direkt mit $\alpha' = 1+\alpha, \beta' = 1+\beta$ und $\gamma' = 1+\gamma$ rechnet. Offenbar sind diese drei Zahlen die Nullstellen des Polynoms $(x-1)^3 - (x-1) - 1 = x^3 - 3x^2 + 2x - 1$. Seien u', v', w' die entsprechenden elementarsymmetrischen Polynome in α', β', γ'. Es gilt

$$A = \frac{2-\alpha'}{\alpha'} + \frac{2-\beta'}{\beta'} + \frac{2-\gamma'}{\gamma'} = \frac{2v'}{w'} - 3.$$

Der Satz von Vieta ergibt in diesem Fall $v' = 2$ und $w' = 1$. Somit erhalten wir wieder $A = 1$. □

Beispiel 12 (APMO 03)**.** *Seien a, b, c, d, e, f reelle Zahlen, sodass die Nullstellen des Polynoms*

$$p(x) = x^8 - 4x^7 + 7x^6 + ax^5 + bx^4 + cx^3 + dx^2 + ex + f$$

alle reell und positiv sind. Bestimme alle möglichen Werte von f.

Lösung. Seien $\alpha_1, \ldots, \alpha_8 > 0$ die acht reellen Nullstellen von p. Nach Vieta gilt nun einerseits

$$s_1 = \sum_{k=1}^{8} \alpha_k = 4, \qquad s_2 = \sum_{1 \le k < l \le 8} \alpha_k \alpha_l = 7.$$

Andererseits folgt mit der Ungleichung von McLaurin (oder AM-GM)

$$\left(\frac{s_1}{8}\right)^2 \ge \frac{s_2}{28}.$$

Wegen $s_1 = 4$ und $s_2 = 7$ gilt in dieser Ungleichung das Gleichheitszeichen. Dies ist aber nur dann der Fall, wenn $\alpha_1 = \ldots = \alpha_8$ gilt. Zusammen mit $s_1 = a$ folgt daraus, dass alle α_k den Wert $\frac{1}{2}$ haben. Wiederum nach Vieta ergibt dies den einzigen möglichen Wert $f = (\frac{1}{2})^8 = \frac{1}{256}$. □

Beispiel 13 (USA 77)**.** *Seien a und b zwei verschiedene Nullstellen des Polynoms $x^4 + x^3 - 1$. Zeige, dass ab eine Nullstelle des Polynoms $x^6 + x^4 + x^3 - x^2 - 1$ ist.*

Lösung. Wir bezeichnen die vier Nullstellen von $p(x) = x^4 + x^3 - 1$ mit a, b, c, d. Man rechnet leicht nach, dass diese vier Nullstellen alle verschieden sind, da p und p_0 keine gemeinsamen Nullstellen haben. Ausserdem ist keine davon gleich 0. Nach Vieta gilt nun

$$\begin{aligned} a + b + c + d &= -1, \\ ab + ac + ad + bc + bd + cd &= 0, \\ abc + bcd + cda + dab &= 0, \\ abcd &= -1. \end{aligned}$$

Wir setzen nun $r = ab, s = cd, u = a + b, v = c + d$. Die obigen Gleichungen lauten dann

$$\begin{aligned} u + v &= -1, \\ r + s + uv &= 0, \\ rv + su &= 0, \\ rs &= -1. \end{aligned}$$

Aus der ersten Gleichung folgt $v = -1 - u$, aus der vierten folgt $s = -1/r$. Setzt man dies in die dritte Gleichung ein, dann folgt $-r(1 + u) - u/r = 0$, also $u = -r^2/(1 + r^2)$. Setzt man das in die zweite Gleichung ein, dann folgt

$$\begin{aligned} & r - \frac{1}{r} + \frac{-r^2}{1+r^2} \cdot \frac{-1}{1+r^2} = 0 \\ \Longleftrightarrow & (r^2 - 1)(r^2 + 1)^2 + r^3 = 0 \\ \Longleftrightarrow & r^6 + r^4 + r^3 - r^2 - 1 = 0, \end{aligned}$$

Dies war zu zeigen. □