Kapitel 4

Polynome

4.1 Konstruktion des Potenzreihenrings und des Polynomrings

4.1.1 Definition. Sei $(R, +, 0, -, \cdot, 1)$ ein kommutativer Ring mit Einselement. Wir betrachten $R^{\mathbb{N}_0} = \{(a_n)_{n\in\mathbb{N}_0} = (a_0, a_1, a_2, \ldots) \mid a_n \in R\}$ und setzen $(a_n)_{n\in\mathbb{N}_0} =: \sum_{n=0}^{\infty} a_n x^n$ ($\sum_{n=0}^{\infty} a_n x^n$ heißt *formale Potenzreihe*). Wir wollen nun die Operationen $+, 0, -, \cdot, 1$ auf $R^{\mathbb{N}_0}$ so definieren, dass $(R^{\mathbb{N}_0}, +, 0, -, \cdot, 1)$ wieder ein kommutativer Ring mit Einselement ist:

$$\begin{aligned}
\sum_{n=0}^{\infty} a_n x^n + \sum_{n=0}^{\infty} b_n x^n &:= \sum_{n=0}^{\infty} (a_n + b_n) x^n, & 0 &:= \sum_{n=0}^{\infty} 0 \cdot x^n, \\
\sum_{n=0}^{\infty} a_n x^n \cdot \sum_{n=0}^{\infty} b_n x^n &:= \sum_{n=0}^{\infty} \big(\sum_{k=0}^{n} a_k b_{n-k}\big) x^n, & 1 &:= \sum_{n=0}^{\infty} \delta_{0n} x^n = (1, 0, 0, 0, \ldots), \\
-\big(\sum_{n=0}^{\infty} a_n x^n\big) &:= \sum_{n=0}^{\infty} (-a_n) x^n.
\end{aligned}$$

4.1.2 Satz. (a) $(R^{\mathbb{N}_0}, +, 0, -, \cdot, 1)$ *ist ein kommutativer Ring mit Einselement.*

(b) $\varphi : R \to R^{\mathbb{N}_0}$, $r \mapsto \sum_{n=0}^{\infty} \delta_{0n} r x^n = (r, 0, 0, 0, \ldots)$ *ist ein Monomorphismus* (*injektiver Homomorphismus*).

(c) *Mit* $x := (0, 1, 0, 0, 0, \ldots) = \sum_{n=0}^{\infty} \delta_{1n} x^n$ *gilt:* $(a_0, a_1, \ldots, a_n, 0, 0, 0, \ldots) = \varphi(a_0) + \varphi(a_1)x + \ldots + \varphi(a_n)x^n$.

Beweis. a) Z.B. Assoziativgesetz für die Multiplikation:

$$\begin{aligned}
&\big(\sum_{n=0}^{\infty} a_n x^n \sum_{n=0}^{\infty} b_n x^n\big) \sum_{n=0}^{\infty} c_n x^n = \sum_{n=0}^{\infty} \big(\sum_{k=0}^{n} a_k b_{n-k}\big) x^n \sum_{n=0}^{\infty} c_n x^n = \\
&= \sum_{n=0}^{\infty} \big(\sum_{k=0}^{n} \big(\sum_{j=0}^{k} a_j b_{k-j}\big) c_{n-k}\big) x^n = \sum_{n=0}^{\infty} \big(\sum_{\substack{0\le i,j,k\le n,\\ i+j+k=n}} a_i b_j c_k\big) x^n = \\
&= \ldots = \sum_{n=0}^{\infty} a_n x^n \big(\sum_{n=0}^{\infty} b_n x^n \sum_{n=0}^{\infty} c_n x^n\big).
\end{aligned}$$

Analog rechnet man die anderen Gesetze nach. Anmerkung: Das Symbol $\sum_{n=0}^{\infty} \cdots$ ist nur ein formaler Ausdruck; in der Algebra (genauer: in dieser Vorlesung) betrachten wir keine

unendlichen Summen. Das Symbol $\sum_{n=0}^{k} \cdots$ bezeichnet hingegen die gewöhnliche Summe[1] im Ring R.

b) φ ist offenbar injektiv: $r \neq s \Rightarrow \varphi(r) \neq \varphi(s)$. Weiters gilt: $\varphi(r+s) = (r+s, 0, 0, \ldots) = (r, 0, 0, \ldots) + (s, 0, 0, \ldots) = \varphi(r) + \varphi(s)$, $\varphi(rs) = (rs, 0, 0, \ldots) = (r, 0, 0, \ldots)(s, 0, 0, \ldots) = \varphi(r)\varphi(s)$ und $\varphi(1) = (1, 0, 0, \ldots)$.

c) Es gilt $x = (0, 1, 0, 0, \ldots)$, $x^2 = (0, 0, 1, 0, \ldots)$, $\ldots$, allgemein: $x^m = \sum_{n=0}^{\infty} \delta_{mn} x^n$, woraus c) folgt. □

4.1.3 Definition. Statt $R^{\mathbb{N}_0}$ schreiben wir $R[[x]]$.
Ist $p(x) = \sum_{k=0}^{\infty} a_k x^k \in R[[x]]$, so heißen die Ringelemente a_k die *Koeffizienten* der Potenzreihe $p(x)$; insbesondere heißt a_0 der „konstante Term“ von $p(x)$, und a_k heißt „Koeffizient“ von x^k.

4.1.4 Definition. Wir fassen nun den Ring R als Unterring von $R[[x]]$ auf, indem wir Elemente von $r \in R$ mit den entsprechenden konstanten Potenzreihen $(r, 0, 0, \ldots)$ identifizieren. Insbesondere sind Null- und Einselement von R auch Null- und Einselement von $R[[x]]$. Der Ring $R[[x]]$ heißt der *Ring der formalen Potenzreihen* in x über R.

4.1.5 Definition. Wir definieren nun den *Polynomring* in x über R als die Menge aller formalen Potenzreihen mit nur endlich vielen nichtverschwindenden Koeffizienten, also

$$R[x] := \{\sum_{n=0}^{\infty} a_n x^n \mid \exists m \, \forall n > m : \ a_n = 0\},$$

also $R[x] := \{a_0 + a_1 x + \cdots + a_n x^n \mid n \in \mathbb{N}_0, \ a_i \in R\}$.

$0 \in R[x]$ ist das *Nullpolynom*.

Man sieht leicht: $(R[x], +, 0, -, \cdot, 1)$ ist genau der von $R \cup \{x\}$ erzeugte Unterring von $(R[[x]], +, 0, -, \cdot, 1)$. Man zeigt dazu:

1) $R[x]$ ist abgeschlossen bezüglich $+, 0, -, \cdot, 1$. (Bezüglich $\cdot$ beachte man: $a_k = 0$ für alle $k > n$, $b_k = 0$ für alle $k > m \Rightarrow \sum_{j=0}^{k} a_j b_{k-j} = 0$ für alle $k > n + m$.)

2) Ist S Unterring von $R[[x]]$ mit $R \cup \{x\} \subseteq S$, so gilt $R[x] \subseteq S$.

x heißt auch „Unbestimmte“.[2] Die Elemente von $R[x]$ heißen *Polynome* und werden als $f(x)$, $p(x)$, $\ldots$ geschrieben.

---

[1] Formal ist diese induktiv definiert: $\sum_{n=0}^{0} f(n) := f(0)$, und $\sum_{n=0}^{k+1} f(n) := (\sum_{n=0}^{k} f(n)) + f(k+1)$. Es ist üblich und auch sinnvoll, $\sum_{n=0}^{-1} f(n) := 0$ zu setzen.

[2] Die Grenzen zwischen „Unbestimmten“, „Variablen“, „Unbekannten“, „Konstanten“, und „Parametern“ sind oft etwas unscharf — unter anderem deshalb, weil der selbe Buchstabe in einem mathematischen Argument oft mehr als eine Rolle spielen kann. *Variable* heißen Symbole dann, wenn man vorhat, die Variable irgendwann durch Werte, und zwar durch beliebige Werte in einer vorgegebenen Menge, zu ersetzen — Variable stehen daher oft hinter einem Allquantor oder Existenzquantor. Das Symbol x in einer formalen Potenzreihe heißt *Unbestimmte*, weil man damit rechnen kann, ohne einen bestimmten Wert einzusetzen. (Das x in einem Polynom spielt abwechselnd die Rolle einer Unbestimmten und einer Variablen.) *Unbekannte* sind jene Variable, deren Wert eigentlich schon fest liegt, aber noch gesucht wird — etwa beim Lösen einer Gleichung. *Konstante* behalten im Verlauf eines mathematischen Arguments meist ihren Wert; allerdings kann z.B. das nullstellige Funktionssymbol oder Konstantensymbol e für das neutrale Element einer Gruppe durchaus in verschiedenen Gruppen mit verschiedenen Werten belegt werden, etwa mit 0 in $(\mathbb{Z}, +)$ und mit 1 in $(\mathbb{Q} \setminus \{0\}, \cdot)$. *Parameter* sind Variable, die länger konstant gehalten werden als die eigentlichen Variablen; wenn man etwa alle Gleichungen der Form $Ax + By = C$ betrachtet, sind x, y für jedes feste A, B, C variabel (und definieren eine Gerade $G_{A,B,C} := \{(x, y) \mid Ax + By = C\}$); durch Variieren der Parameter A, B und C bekommt man alle Geradengleichungen.

Jedes $p(x) \in R[x]$ hat die Gestalt $p(x) = \sum_{k=0}^{n} a_k x^k$ mit $n \in \mathbb{N}_0$. Sei weiters $q(x) = \sum_{k=0}^{m} b_k x^k$ mit $m \leq n$. Wann gilt $p(x) = q(x)$? Wir schreiben $q(x) = \sum_{k=0}^{n} b_k x^k$, wobei $b_k = 0$ für $m < k \leq n$. Dann gilt: $p(x) = q(x) \Leftrightarrow a_k = b_k$ für $k = 0, \ldots, n$.

Mit Polynomen wird nach den Gesetzen des kommutativen Ringes $R[x]$ mit Einselement gerechnet.

4.1.6 Definition. Ist $p(x) = \sum_{k=0}^{n} a_k x^k$ mit $a_n \neq 0$, so heißt n der *Grad* von $p(x)$ ($n = \operatorname{grad} p(x)$).
Wenn n der Grad des Polynoms p ist, dann heißt a_n (der Koeffizient von x^n) auch „Koeffizient des höchsten Terms“.

Es gilt:

$$\operatorname{grad}(p(x) + q(x)) \leq \max(\operatorname{grad} p(x), \operatorname{grad} q(x))$$
$$\operatorname{grad}(p(x)q(x)) \leq \operatorname{grad} p(x) + \operatorname{grad} q(x)$$

falls $p(x)$, $q(x)$, $p(x)+q(x)$ und $p(x)q(x) \neq 0$ sind. Dem Polynom 0 wird oft kein Grad zugeordnet. Gelegentlich setzt man auch $\operatorname{grad}(0) = -\infty$, dann gelten die obigen Abschätzungen auch dann, wenn p oder q oder $p + q$ oder pq das Nullpolynom sind (sofern man die Rechenregeln $(-\infty) + k = -\infty = (-\infty) + (-\infty)$ vereinbart).

4.1.7 Definition. Gilt $\operatorname{grad} p(x) = n$ und $a_n = 1$, so heißt $p(x)$ ein *normiertes* (oder auch „monisches“) Polynom. Polynome der Gestalt $ax + b$ mit $a \neq 0$ heißen *lineare* Polynome.

4.1.8 Satz. *Ist R ein Integritätsbereich, dann ist auch $R[x]$ ein Integritätsbereich, und für $p(x), q(x) \in R[x] \setminus \{0\}$ gilt:* $\operatorname{grad}(p(x)q(x)) = \operatorname{grad} p(x) + \operatorname{grad} q(x)$.

Beweis. $p(x) = \sum_{k=0}^{n} a_k x^k$, $a_n \neq 0$, $q(x) = \sum_{k=0}^{m} b_k x^k$, $b_m \neq 0 \Rightarrow p(x)q(x) = \sum_{k=0}^{n+m} c_k x^k$ mit $c_k = \sum_{j=0}^{k} a_j b_{k-j}$, insbesondere: $c_{n+m} = a_n b_m \neq 0$. □

4.1.9 Anmerkung. Ist R kein Integritätsbereich, so ist auch $R[x]$ keiner, da R Unterring von $R[x]$ ist.

4.1.10 Anmerkung. Wenn R Integritätsbereich ist, dann ist auch $R[[x]]$ Integritätsbereich. (Beweis: Übungsbeispiel 77.)

4.1.A Potenzreihen und Polynome in n Unbestimmten $x_1, \ldots, x_n$

Wenn es bereits ein Element von R gibt, das wir mit x bezeichnen, dann wählen wir einen anderen Namen für die Unbestimmte[3] im Polynomring bzw. im Ring der formalen Potenzreihen über R, z.B. y.
Sei R Ring, $R[x]$ Polynomring über R. Den Polynomring über $R[x]$ bezeichnen wir mit $R[x][y]$ oder einfach $R[x, y]$. Elemente von $R[x, y]$ kann man entweder (gemäß der Definition) als Polynome über $R[x]$ in der Unbestimmten y auffassen, oder auch als Polynome über dem Polynomring $R[y]$ (welcher in natürlicher Weise zu $R[x]$ isomorph ist) in der Variablen x.
Unter dem „Grad“ eines solchen Polynoms versteht man je nach Kontext bzw. nach Auffassung etwas anderes. Zum Beispiel hat das Polynom $3x^2y + xy - 5x \in \mathbb{Z}[x, y]$, als Element von $\mathbb{Z}[y][x]$ aufgefasst, den Grad 2 („quadratisch in der Variablen x“); die Koeffizienten von

$$3y \cdot x^2 + (y - 5) \cdot x^1 + 0 \cdot x^0$$

[3] formal: für die Folge $(0, 1, 0, 0, \ldots)$

sind $3y$, $y-5$ und 0. Wenn wir das Polynom aber als Element von $\mathbb{Z}[x][y]$ auffassen, ist es linear: Das Polynom

$$(3x^2+x)\cdot y^1 - 5x\cdot y^0$$

hat die Koeffizienten $3x^2+x$ und -5.
Oft ist es auch sinnvoll, einem Polynom in den Variablen x, y einen gemeinsamen Grad zuzuweisen; dieser gemeinsame Grad ist als die maximale vorkommende Summe der Exponenten von x und y definiert. Im Polynom $3x^2y^1 + x^1y^1 - 5x^1y^0$ kommen als Summen von Exponenten $2+1$, $1+1$, $1+0$ vor, der gemeinsame Grad ist also 3. Das Polynom $xy+1$ hat dann gemeinsamen Grad $1+1=2$; es ist aber „linear in x“ und auch „linear in y“.

Allgemeiner definieren wir induktiv:

$$R[[x_1]] := R[[x]], \qquad R[[x_1,\dots,x_n]] := (R[[x_1,\dots,x_{n-1}]])[[x_n]],\ n>1,$$

und entsprechend:

$$R[x_1] := R[x], \qquad R[x_1,\dots,x_n] := (R[x_1,\dots,x_{n-1}])[x_n],\ n>1.$$

Dann gilt (Beweis durch vollständige Induktion nach n):

$$R[x_1,\dots,x_n] = \{\sum_{0\le i_1,\dots,i_n\le m} a_{i_1\dots i_n} x_1^{i_1}\cdots x_n^{i_n} \mid m\in\mathbb{N}_0,\ a_{i_1\dots i_n}\in R\}.$$

Z.B. hat ein Element aus $R[x_1,x_2]$ die allgemeine Form: $p(x_1,x_2) = a_{00} + a_{10}x_1 + a_{01}x_2 + a_{20}x_1^2 + a_{11}x_1x_2 + a_{02}x_2^2 + \cdots + a_{jk}x_1^jx_2^k$.

4.2 Polynome und Funktionen

4.2.1 Satz (Einsetzungsprinzip). *Sei $(R,+,0,-,\cdot,1)$ ein kommutativer Ring mit Einselement und $p(x) = a_nx^n + \cdots + a_1x + a_0 \in R[x]$. Für $a\in R$ ist dann $p(a) := a_na^n + \cdots + a_1a + a_0$ wieder ein Element von R, genannt der* Wert des Polynoms an der Stelle a. *Die Funktion*

$$\begin{cases} R\to R \\ a\mapsto p(a)\end{cases}$$

heißt die durch das Polynom $p(x)$ induzierte Polynomfunktion *und wird oft ebenfalls mit p bezeichnet.*

Der folgende Satz betrachtet eine etwas allgemeinere Situation.

4.2.2 Satz. *Seien R und S kommutative Ringe mit Einselement, und sei $f: R\to S$ ein Homomorphismus. Sei c ein Element von S.*
Dann ist die Abbildung $\varphi_c: R[x]\to S$, die durch

$$\varphi_c(\sum_{k=1}^n a_kx^k) = \sum_{k=1}^n f(a_k)c^k$$

definiert ist, ein Homomorphismus. Überdies ist φ_c der einzige Homomorphismus ψ, der f fortsetzt und $\psi(x)=c$ erfüllt.

Beweis. Die Eindeutigkeit ist klar, weil $R[x]$ von $R \cup \{x\}$ erzeugt wird.
Sei $p(x) = \sum_{k=0}^{n} a_k x^k$ und $q(x) = \sum_{k=0}^{n} c_k x^k$. Dann gilt:

$$\begin{aligned}\varphi_c(p(x) + q(x)) &= \sum_{k=0}^{n} (f(a_k + b_k))c^k \\ &= \sum_{k=0}^{n} (f(a_k) + f(b_k))c^k \\ &= \sum_{k=0}^{n} f(a_k)c^k + \sum_{k=0}^{n} f(b_k)c^k \\ &= \varphi_c(p(x)) + \varphi_c(q(x)).\end{aligned}$$

Analog sieht man: $\varphi_c(p(x)q(x)) = \varphi_c(p(x))\varphi_c(q(x))$. □

Im Spezialfall $S = R$ und $f = id_R$ erhalten wir den Einsetzungshomomorphismus $p(x) \mapsto p(c)$. Im Spezialfall $S = R^R$ (das heißt, S ist die Menge aller Funktionen von R nach R), $f(r)$ die konstante Funktion auf R mit Wert r, und $c = id_R$ erhalten wir eine Abbildung $\varphi : R[x] \to R^R$, die jedem Polynom $p(x) = \sum_{n=0}^{k} a_n x^n$ die Funktion $\varphi(p) : r \mapsto \varphi_r(p) = \sum_{n=0}^{k} a_n r^n$ zuordnet. Diese Funktion $\varphi(p)$ ist dann die „durch $p(x)$ induzierte“ Funktion.

4.2.3 Anmerkung. In der Analysis ist es üblich, nicht zwischen einem Polynom p und der durch p induzierten Polynomfunktion zu unterscheiden. Diese Identifikation kann man durch Satz 4.2.12 rechtfertigen. Wenn wir aber endliche Strukturen oder Ringe mit Nullteilern betrachten, ist die gerade definierte Abbildung φ nicht injektiv, zwei verschiedene Polynome können also dieselbe Funktion induzieren; mit $p(x) = q(x)$ meinen wir im Allgemeinen die Gleichheit der Polynome (d.h., die Gleichheit aller einander entsprechenden Koeffizienten), und nicht die bloße Gleichheit der Polynomfunktionen.

4.2.4 Beispiel. Die Polynome $p(x) = x^2 + x$ und $q(x) = 0$ induzieren auf dem zweielementigen Ring $\mathbb{Z}_2$ dieselbe Polynomfunktion. Es gilt also $p(x) \neq q(x)$, aber $\varphi(p(x)) = \varphi(q(x))$

4.2.5 Beispiel. Gilt etwa $f(x)^2 - g(x)h(x) + k(x) = f(x)^4 + k(x)^2$ mit $f(x), g(x), h(x), k(x) \in R[x]$ und ist $a \in R$, so gilt auch $f(a)^2 - g(a)h(a) + k(a) = f(a)^4 + k(a)^2$.

4.2.6 Definition. Sei $p(x) \in R[x]$ (R kommutativer Ring mit Einselement). Dann heißt $a \in R$ *Nullstelle* von $p(x) :\Leftrightarrow p(a) = 0$. $p(x)$ heißt *teilbar* durch $q(x) \in R[x]$ (in Zeichen: $q(x)|p(x)) :\Leftrightarrow p(x) = q(x)r(x)$ mit $r(x) \in R[x]$.

4.2.7 Satz. *Ist a Nullstelle von $p(x)$, so ist $p(x)$ teilbar durch das lineare Polynom $x - a$ (und umgekehrt).*

Beweis. Sei $p(x) = a_n x^n + \cdots + a_1 x + a_0$. Man bildet

$$\begin{aligned}q(x) &:= p(x) - a_n x^{n-1}(x - a) = b_{n-1}x^{n-1} + \cdots + b_1 x + b_0, \\ r(x) &:= q(x) - b_{n-1}x^{n-2}(x - a) = c_{n-2}x^{n-2} + \cdots + c_1 x + c_0, \\ s(x) &:= r(x) - c_{n-2}x^{n-3}(x - a) = d_{n-3}x^{n-3} + \cdots + d_1 x + d_0 \text{ usw.}\end{aligned}$$

und erhält $p(x) = a_n x^{n-1}(x - a) + q(x) = a_n x^{n-1}(x - a) + b_{n-1}x^{n-2}(x - a) + r(x) = a_n x^{n-1}(x - a) + b_{n-1}x^{n-2}(x - a) + c_{n-2}x^{n-3}(x - a) + s(x) = \ldots = a_n x^{n-1}(x - a) + \cdots + k_1(x - a) + k_0$. Wegen $0 = p(a) = a_n a^{n-1}(a - a) + \cdots + k_1(a - a) + k_0 = k_0$ ist $k_0 = 0$ und $p(x) = (x - a)(a_n x^{n-1} + \cdots + k_1)$. Also gilt: $x - a$ teilt $p(x)$. (Wir haben praktisch $p(x)$ durch $x - a$ dividiert und den Rest $k_0 = 0$ erhalten!) □

Von nun an sei R ein Integritätsbereich (z.B. $R = \mathbb{Z}$ oder R Körper). In Integritätsbereichen kann man Gleichungen „kürzen“, das heißt:

> Sei $a \neq 0$. Dann[4] gilt: $ab = ac \Rightarrow b = c$.
> (Wenn nämlich $ab = ac$, dann $ab - ac = a(b - c) = 0$, also $b - c = 0$.)

Ist $\operatorname{grad} p(x) = n$ und gilt $(x-a)^k | p(x)$, d.h., $p(x) = (x-a)^k q(x)$, dann ist $k + \operatorname{grad} q(x) = \operatorname{grad} p(x) = n$, woraus $k \leq n$ folgt.

4.2.8 Definition. Sei $p(x) \in R[x] \setminus \{0\}$ und $a \in R$ Nullstelle von $p(x)$. Dann heißt das größte k mit $(x-a)^k | p(x)$ die *Vielfachheit* der Nullstelle a. (Nach der eben gemachten Bemerkung ist $k \leq n$.)

4.2.9 Satz. *Seien $a_1, \ldots, a_r$ paarweise verschiedene Nullstellen von $p(x) \in R[x]$ mit den Vielfachheiten $k_1, \ldots, k_r$. Dann gilt:*

$$(x-a_1)^{k_1} \cdots (x-a_r)^{k_r} | p(x).$$

Beweis. Für $r = 1$ ist nichts mehr zu zeigen. Für $r > 1$ ist aufgrund der Voraussetzung $p(x) = (x-a_1)^{k_1} q_1(x) = (x-a_2)^{k_2} q(x)$. Da $p(a_2) = (a_2-a_1)^{k_1} q_1(a_2) = 0$ und $(a_2-a_1)^{k_1} \neq 0$, muss $q_1(a_2) = 0$ und damit $q_1(x) = (x-a_2)q_2(x)$ gelten.
Also ist $p(x) = (x-a_1)^{k_1}(x-a_2)q_2(x) = (x-a_2)^{k_2} q(x)$. Durch „Kürzen“ dieser Gleichung durch $x - a_2$ (dieses Polynom ist ja $\neq 0$) erhalten wir daraus $(x-a_1)^{k_1} q_2(x) = (x-a_2)^{k_2-1} q(x)$. Falls $k_2 - 1 > 0$ ist, erhält man analog $p(x) = (x-a_1)^{k_1}(x-a_2)^2 q_3(x) = (x-a_2)^{k_2} q(x)$, d.h., $(x-a_1)^{k_1} q_3(x) = (x-a_2)^{k_2-2} q(x)$. Nach k_2 Schritten erhält man so $p(x) = (x-a_1)^{k_1}(x-a_2)^{k_2} q_{k_2+1}(x)$, d.h., $(x-a_1)^{k_1}(x-a_2)^{k_2} | p(x)$. Mit den restlichen Nullstellen $a_3, \ldots, a_r$ verfährt man ebenso und erhält schließlich die Behauptung. □

4.2.10 Folgerung. Seien $a_1, \ldots, a_r$ paarweise verschiedene Nullstellen von $p(x) \in R[x]$ mit den Vielfachheiten $k_1, \ldots, k_r$. Dann gilt: $k_1 + \cdots + k_r \leq \operatorname{grad} p(x)$.

Ein Polynom vom Grad n über einem Integritätsbereich hat also höchstens n Nullstellen, wobei jede Nullstelle mit ihrer Vielfachheit gezählt wird.

4.2.11 Satz. *Seien $p(x), q(x) \in R[x]$, $\operatorname{grad} p(x), \operatorname{grad} q(x) \leq n$ und $p(b_i) = q(b_i)$ für $n+1$ paarweise verschiedene Elemente $b_0, \ldots, b_n$ von R. Dann gilt $p(x) = q(x)$.*

Beweis. $(p-q)(b_i) = 0$ für $0 \leq i \leq n \Rightarrow p-q$ hat $n+1$ Nullstellen $\Rightarrow p-q = 0 \Rightarrow p = q$. □

4.2.12 Satz. *Sei R ein unendlicher Integritätsbereich, und seien $p(x), q(x) \in R[x]$ Polynome. Dann gilt: $p(x) = q(x)$ gilt genau dann, wenn $\varphi(p(x)) = \varphi(q(x))$, das heißt, wenn $p(r) = q(r)$ für alle $r \in R$ gilt.*

Ein Polynom braucht keine Nullstellen zu besitzen.

4.2.13 Beispiele. 1) $x^2 - 2 \in \mathbb{Q}[x]$ hat keine Nullstellen in $\mathbb{Q}$, wohl aber in $\mathbb{R} \supset \mathbb{Q}$, nämlich $\pm\sqrt{2}$.

2) $x^2 + 1 \in \mathbb{R}[x]$ hat keine Nullstellen in $\mathbb{R}$, wohl aber in $\mathbb{C} \supset \mathbb{R}$, nämlich $\pm i$.

[4] Achtung! Die hier betrachtete „Kürzbarkeit“ bezieht sich nur auf die Multiplikation in R, nicht aber auf Multiplikation mit Elementen von $\mathbb{Z}$, d.h. auf iterierte Addition. Zum Beispiel kann man aus $2b = 2c$ (also $b + b = c + c$) im Allgemeinen nicht auf $b = c$ schließen, auch nicht in nullteilerfreien Ringen. Man betrachte etwa den nullteilerfreien Ring — sogar Körper — $\mathbb{Z}_2$.

4.2.14 Definition. Ein Körper K heißt *algebraisch abgeschlossen*, wenn jedes $p(x) \in K[x] \setminus K$ mindestens eine Nullstelle besitzt.

4.2.15 Anmerkung. Hat in einem Integritätsbereich jedes lineare Polynom eine Nullstelle, so ist dieser bereits ein Körper ($ax - 1$ ($a \neq 0$) habe die Nullstelle $c \Rightarrow ac = 1 \Rightarrow c = a^{-1}$).

4.2.16 Satz (Fundamentalsatz der Algebra von Gauß). *$\mathbb{C}$ ist algebraisch abgeschlossen.*

Der Beweis wird in Kapitel 7 geführt. □

4.2.17 Satz. *Ist K ein Körper, dann sind folgende Aussagen äquivalent:*

a) *K ist algebraisch abgeschlossen.*

b) *Für alle $p(x) \in K[x]$ mit $\operatorname{grad} p(x) = n > 0$ gilt: $p(x) = c(x - b_1)^{k_1} \cdots (x - b_r)^{k_r}$ mit $b_1, \ldots, b_r, c \in K$ und $k_1 + \cdots + k_r = n$.*

Beweis. b) $\Rightarrow$ a): trivial.
a) $\Rightarrow$ b): Sei $p(x) \in K[x]$, $\operatorname{grad} p(x) > 0$. Dann gibt es ein $a_1 \in K$ mit $p(a_1) = 0$, d.h., $p(x) = (x - a_1)p_1(x)$. Ist $\operatorname{grad} p_1(x) > 0$, erhält man analog $p_1(x) = (x - a_2)p_2(x)$, also $p(x) = (x - a_1)(x - a_2)p_2(x)$. Fortgesetzte Anwendung dieser Überlegung ergibt schließlich $p(x) = (x - a_1)(x - a_2) \cdots (x - a_n)c$. Faßt man gleiche Faktoren $(x - a_i)$ zu Potenzen zusammen, erhält man die behauptete Darstellung. □

Berechnung von Nullstellen von Polynomen über Körpern.
1) $\operatorname{grad} p(x) = 1$: trivial.
2) $\operatorname{grad} p(x) = 2$: $p(x) = ax^2 + bx + c$ ($a \neq 0$) hat die Nullstellen $\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$ („2“ bzw. „4“ steht hier für $1 + 1$ bzw. $1 + 1 + 1 + 1$; der Wurzelausdruck muss existieren und $1 + 1 \neq 0$ sein).
3) $\operatorname{grad} p(x) = 3, 4$: Formeln von Cardano (Tartaglia).
4) $\operatorname{grad} p(x) > 4$: Hier gibt es keine allgemeinen „Formeln“ (bestehend aus Grundrechnungsarten und Wurzelausdrücken) mehr.

4.3 Interpolation durch Polynome

Sei K ein Körper und $f : K \to K$ eine Funktion.
Gegeben: $b_i = f(a_i)$ für paarweise verschiedene $a_i \in K$, $1 \leq i \leq n$ (z.B.: Messreihe).
Gesucht: $p(x) \in K[x]$ mit $p(a_i) = b_i = f(a_i)$, $1 \leq i \leq n$ und $\operatorname{grad} p(x) < n$. (Es kann höchstens ein solches Polynom $p(x)$ geben: aus $p(a_i) = q(a_i)$, $1 \leq i \leq n$, mit $\operatorname{grad} p(x), \operatorname{grad} q(x) < n$ folgt nämlich $p = q$.)

4.3.A Interpolationsformel von Lagrange

Sei

$$q_i(x) := \prod_{\substack{1 \leq j \leq n, \\ j \neq i}} (x - a_j) = (x - a_1) \cdots (x - a_{i-1})(x - a_{i+1}) \cdots (x - a_n).$$

Dann gilt:

$$q_i(a_k) = \begin{cases} 0 & \text{für } i \neq k, \\ \prod_{1 \leq j \leq n,\, j \neq i} (a_k - a_j) \neq 0 & \text{für } i = k. \end{cases}$$

Für

$$p(x) := \sum_{i=1}^{n} b_i \frac{q_i(x)}{q_i(a_i)}$$

gilt dann $p(a_j) = b_j$, $1 \le j \le n$.

4.3.1 Folgerung. Ist K ein *endlicher* Körper (z.B. $K = \mathbb{Z}_p$, p Primzahl), $f : K \to K$, dann gibt es ein Polynom $p(x) \in K[x]$ mit $f(a) = p(a)$ für alle $a \in K$.

4.3.2 Beispiel. Um ein quadratisches Polynom $p(x) \in \mathbb{Q}[x]$ zu erhalten, das an den Stellen 1, 2, 3 die Werte 10, 41, 62 hat, definiert man einfach

$$p(x) := 10\frac{(x-2)(x-3)}{(1-2)(1-3)} + 41\frac{(x-1)(x-3)}{(2-1)(2-3)} + 62\frac{(x-1)(x-2)}{(3-1)(3-2)} = (-5)x^2 + 46x^1 + (-31)x^0.$$

4.3.B Interpolationsformel von Newton

Sei K ein Körper, $n \in \mathbb{N}$, $K_{n-1}[x] := \{p(x) \in K[x] \mid \operatorname{grad} p(x) < n\} \cup \{0\}$. Dann gilt: $K_{n-1}[x] = \{a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} \mid a_i \in K\}$ ist n-dimensionaler Vektorraum über K mit der Basis $\{1, x, \ldots, x^{n-1}\}$.

Man sieht leicht: Ist $\varphi_i(x) \in K[x]$, $\operatorname{grad} \varphi_i(x) = i-1$, $1 \le i \le n$, dann ist $\{\varphi_1(x), \ldots, \varphi_n(x)\}$ ebenfalls Basis von $K_{n-1}[x]$. (Die Matrix, die den Basiswechsel beschreibt, ist nämlich eine Dreiecksmatrix, in deren Diagonale genau die höchsten Koeffizienten der Polynome φ_i stehen.)

Sei nun $f : K \to K$, $a_1, \ldots, a_n \in K$, $f(a_i) = b_i$, $1 \le i \le n$. Setzt man $\varphi_1(x) := 1$ und

$$\varphi_i(x) := \prod_{j=1}^{i-1}(x - a_j), \qquad 2 \le i \le n,$$

so ist $\{\varphi_1(x), \ldots, \varphi_n(x)\}$ nach der eben gemachten Bemerkung Basis von $K_{n-1}[x]$. Für das gesuchte Interpolationspolynom $p(x)$ mit $p(a_i) = b_i$, $1 \le i \le n$, muss daher gelten:

$$p(x) = \sum_{i=1}^{n} \lambda_i \varphi_i(x)$$

für geeignete $\lambda_i \in K$. Diese lassen sich aus dem folgenden Gleichungssystem in Halbdiagonalform berechnen:

$$\begin{aligned}
p(a_1) &= b_1 = \lambda_1 \\
p(a_2) &= b_2 = \lambda_1 + \lambda_2(a_2 - a_1) \\
p(a_3) &= b_3 = \lambda_1 + \lambda_2(a_3 - a_1) + \lambda_3(a_3 - a_1)(a_3 - a_2) \\
&\vdots
\end{aligned}$$

Vorteil dieser Interpolationsmethode: bei Hinzufügen einer neuen Stützstelle $b_{n+1} = f(a_{n+1})$ bleiben $\lambda_1, \ldots, \lambda_n$ unverändert, nur λ_{n+1} muss neu berechnet werden.