Prof. Dr. H. Brenner **Osnabrück SS 2015**

Elemente der Algebra

Vorlesung 4

Terme und Gleichungen

Unter einem (arithmetischen) „Term“ versteht man einen „zahlähnlichen“ Ausdruck, der sich aus „Zahlen“ und „Variablen“ mit Hilfe der Verknüpfungssymbole $+$ und $\cdot$ (eventuell mit $-$ und $:$ oder daraus abgeleiteten Operationen wie Potenzen) und mit Klammern „korrekt“ bilden lässt. Das sind typischerweise auch die Ausdrücke, die auf einer Seite einer Gleichung (oder Ungleichung) stehen können. Beispielsweise sind

$$3 \cdot (4+5),\ x,\ 2x+7,\ 4x^3-y,\ (a+b)^2,\ a^2+2ab+b^2,\ 0 \cdot 1,$$

Terme. Dagegen sind

$$3 \cdot (4+5)),\ 2x+7=0,$$

keine Terme. Bei

$$n!,\ \binom{n}{k},\ \pi,\ e^u, x^y,\ 5^x,\ \sqrt{x},\ \heartsuit$$

kann man sich darüber streiten (in der mathematischren Logik wird der Termbegriff unter Bezug auf Funktionssymbole präzisiert), es sind jedenfalls keine rein algebraischen Terme. Wichtig ist, dass man Terme nur dann als gleich ansieht, wenn es sich um dieselbe Zeichenreihe handelt. Beispielsweise sind $(a+b)^2$ und $a^2+2ab+b^2$ verschiedene Terme. Gleichheit zwischen diesen Ausdrücken gilt nur bei einer bestimmten Interpretation, wenn man a und b als Elemente eines kommutativen Ringes interpretiert (erste binomische Formel).

Eine wichtige Funktion von Termen ist ihr Auftreten in Gleichungen. Gleichungen und Terme treten in der Mathematik in verschiedener Bedeutung auf.

1) Identitäten von Elementen

Das sind Gleichungen der Form $2+4 = 6$ oder

$$3 \cdot 7 = 21,$$

die besagen, das zwei irgendwie gegebene Elemente einer Menge gleich sind. $2+4$ und 6 sind unterschiedliche Terme, haben aber denselben Zahlwert. In solchen Gleichungen kommen keine Variablen vor. Häufig werden solche Gleichungen verwendet, um etwas auszurechnen, also einen komplizierten Ausdruck in eine Standardfrom zu bringen.

2) Termidentitäten (Formeln, Rechengesetze)

Beispiel dazu sind

$$a(b+c) \;=\; ab+ac$$

oder

$$(a+b)^2 \;=\; a^2+2ab+b^2$$

oder

$$a^2+b^2 \;=\; c^2.$$

Sie drücken eine Gesetzmäßigkeit aus, die unter bestimmten Bedingungen gilt, beispielsweise wenn a, b Elemente eines kommutativen Ringes sind oder wenn a, b Kathetenlängen und c die Hypothenusenlänge eines rechtwinkligen Dreiecks ist. Charakteristisch für solche Gleichungen ist, dass in ihnen Variablen vorkommen und dass, wenn man für die Variablen simultan (also an jeder Stelle, wo die Variable steht) Elemente, die die Bedingung erfüllen, einsetzt, eine wahre Elementgleichung entsteht. Eine solche Identität repräsentiert also eine Vielzahl an einzelnen Elementgleichungen. Aus dem Distributivgesetz ensteht beispielsweise durch Einsetzen die spezielle Identität $3 \cdot (5+4) \;=\; 3 \cdot 5 + 3 \cdot 4$.

3) Gleichungen als Bedingung

Damit sind Gleichungen wie

$$4x = 9,\; 2x+7 = 0,\; 5x^2-3x+4 = 0,\; x = y$$

gemeint. In diesen kommen (in aller Regel) Variablen vor, es wird aber nicht eine allgemeingültige Formel zum Ausdruck gebracht, sondern es wird eine Bedingung an die auftretenden Variablen formuliert. D.h. es werden die Elemente gesucht, die die Gleichungen erfüllen, die man also für die Variablen einsetzen kann, damit eine wahre Elementidentität entsteht. Gleichungen in diesem Sinne definieren die Aufgabenstellung, nach Lösungen zu suchen. Statt einer einzigen Gleichung kann auch ein (beispielsweise lineares) Gleichungssystem vorliegen.

4) Definitionsgleichungen

Das sind Gleichungen, durch die eine abkürzende Schreibweise für einen komplexeren Ausdruck eingeführt wird. Beispiele sind

$$a^3 = a \cdot a \cdot a,\; n! = n(n-1) \cdot 3 \cdot 2 \cdot 1,\; |a+bi| = \sqrt{a^2+b^2},\; P = 4x^2+7x-5\,.$$

Hierbei schreibt man häufig := statt =.

Manche Gleichungen kann man in mehrfacher Weise auffassen. So kann man die Gleichung

$$a^2+b^2 \;=\; c^2$$

als Gesetzmäßigkeit in einem rechtwinkligen Dreieck auffassen (bei richtiger Interpretation der einzelnen Variablen) oder als Aufgabenstellung, alle Tripel (a, b, c) zu bestimmen, die diese Gleichung erfüllen.

Polynomringe in einer Variablen

Zu einem kommutativen Ausgangsring wie $\mathbb{Z}$ oder $\mathbb{R}$ und einer fixierten Variablen X kann man sich fragen, welche Terme man mit dieser Variablen über diesem Ring „basteln“ kann. Dazu gehören

$$5,\ 3X+3,\ 3(X+1),\ (2X-6)(4X+3),\ X\cdot(X\cdot X),\ 5+3X-6X^2+7X^3,\\ X^2-4+5X^2+7X-13X,$$

wobei wir Potenzschreibweise verwendet und einige Klammern wegelassen haben. Als Terme sind $3X+3$ und $3(X+1)$ verschieden. Bei jeder Interpertation von X in einem Ring sind diese Ausdrücke aber gleich. Der Polynomring besteht aus genau diesen Termen, wobei allerdings Terme miteinander identifiziert werden, wenn dies in jedem kommutativen Ring gilt (die Menge aller Terme ist kein Ring)!

Definition 4.1. Der *Polynomring* über einem kommutativen Ring R besteht aus allen *Polynomen*

$$P = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n$$

mit $a_i \in R$, $i = 0, \ldots, n$ $n \in \mathbb{N}$, und mit komponentenweiser Addition und einer Multiplikation, die durch distributive Fortsetzung der Regel

$$X^n \cdot X^m := X^{n+m}$$

definiert ist.

Ein Polynom

$$P = \sum_{i=0}^{n} a_iX^i = a_0 + a_1X + \cdots + a_nX^n$$

ist formal gesehen nichts anderes als das Tupel $(a_0, a_1, \ldots, a_n)$, die die *Koeffizienten* des Polynoms heißen. Der Ring R heißt in diesem Zusammenhang der *Grundring* des Polynomrings. Aufgrund der komponentenweisen Definition der Addition liegt unmittelbar eine Gruppe vor, mit dem *Nullpolynom* (bei dem alle Koeffizienten null sind) als neutralem Element. Zwei Polynome sind genau dann gleich, wenn sie in allen ihren Koeffizienten übereinstimmen. Die Polynome mit $a_i = 0$ für alle $i \geq 1$ heißen *konstante Polynome*, man schreibt sie einfach als a_0. Ein von 0 verschiedenes Polynom kann man als $\sum_{i=0}^{n} a_iX^i$ mit $a_n \neq 0$ schreiben. Der Koeffizient a_n heißt dann der *Leitkoeffizient* des Polynoms.

Die für ein einfaches Tupel zunächst ungewöhnliche Schreibweise deutet in suggestiver Weise an, wie die Multiplikation aussehen soll, das Produkt X^iX^j ist nämlich durch die Addition der Exponenten gegeben. Dabei nennt man X die *Variable* des Polynomrings. Für beliebige Polynome ergibt sich die Multiplikation aus dieser einfachen Multiplikationsbedingung durch distributive

Fortsetzung gemäß der Vorschrift, „alles mit allem“ zu multiplizieren. Die Multiplikation ist also explizit durch folgende Regel gegeben:

$$\left(\sum_{i=0}^{n} a_i X^i\right) \cdot \left(\sum_{j=0}^{m} b_j X^j\right) = \sum_{k=0}^{n+m} c_k X^k \text{ mit } c_k = \sum_{r=0}^{k} a_r b_{k-r}\,.$$

Beispielsweise ist

$$\begin{aligned} & \left(iX^2 + (3-i)X + 5\right)\left(-X^2 + 4X + 2i\right) \\ = \;& -iX^4 + (4i - (3-i))X^3 + (2ii + (3-i)4 - 5)X^2 + ((3-i)2i + 20)X + 10i \\ = \;& -iX^4 + (-3+5i)X^3 + (5-4i)X^2 + (22+6i)X + 10i \end{aligned}$$

Lemma 4.2. *Sei R ein kommutativer Ring und sei $R[X]$ der Polynomring über R. Dann gelten folgende Aussagen.*

(1) *R ist ein Unterring von $R[X]$.*
(2) *R ist genau dann ein Integritätsbereich, wenn $R[X]$ ein Integritätsbereich ist.*

Beweis. (1) Ein Element $r \in R$ wird als konstantes Polynom aufgefasst, wobei es egal ist, ob man Addition und Multiplikation in R oder in $R[X]$ ausführt.

(2) Wenn $R[X]$ integer ist, so überträgt sich dies sofort auf den Unterring R. Sei also R ein Integritätsbereich und seien $P = \sum_{i=0}^{n} a_i X^i$ und $Q = \sum_{j=0}^{m} b_j X^j$ zwei von null verschiedene Polynome. Wir können annehmen, dass a_n und b_m von null verschieden sind. Dann ist $a_n b_m \neq 0$ und dies ist der Leitkoeffizient des Produktes PQ, das damit nicht null sein kann.

□

Korollar 4.3. *Sei R ein kommutativer Ring. und sei $S \subseteq R$ ein Unterring. Dann ist auch $S[X]$ ein Unterring von $R[X]$.*

Beweis. Siehe Aufgabe 4.7. □

Die vorstehende Aussage bedeutet einfach, dass man ein Polynom mit Koeffizienten aus S direkt auch als Polynom mit Koeffizienten aus R auffassen kann. So ist ein Polynom mit ganzzahligen Koeffizienten insbesondere auch ein Polynom mit rationalen Koeffizienten und mit reellen Koeffizienten. Die Addition und die Multiplikation von zwei Polynomen hängt nicht davon ab, ob man sie über einem kleineren oder einem größeren Grundring ausrechnet, so lange dieser nur alle beteiligten Koeffizienten enthält. Es gibt aber auch viele wichtige Eigenschaften, die vom Grundring abhängen, wie beispielsweise die Eigenschaft, irreduzibel zu sein, siehe Beispiel 6.8.

In ein Polynom $P \in R[X]$ kann man ein Element $r \in R$ einsetzen. Dabei ersetzt man überall die Variable X durch r und rechnet das Ergebnis in R

aus. Dieses Ergebnis wird mit $P(r)$ bezeichnet. Ein fixiertes Element $r \in R$ definiert dann eine Abbildung (die *Auswertungsabbildung* zu r)

$$R[X] \longrightarrow R,\ P \longmapsto P(r).$$

Andererseits definiert ein fixiertes Polynom $P \in R[X]$ die zugehörige Polynomfunktion, die durch

$$R \longrightarrow R,\ x \longmapsto P(x).$$

Diese wird insbesondere bei einem Körper $R = K$ studiert, siehe weiter unten.

Der Grad eines Polynoms

DEFINITION 4.4. Der *Grad* eines von 0 verschiedenen Polynoms

$$P = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n$$

mit $a_n \neq 0$ ist n.

Wenn der Leitkoeffizient $a_n = 1$ ist, so nennt man das Polynom *normiert*. Dem Nullpolynom wird im Allgemeinen kein Grad zugewiesen; manchmal sind gewisse Gleichungen oder Bedingungen aber auch so zu verstehen, dass dem Nullpolynom jeder Grad zugewiesen wird. Polynome vom Grad 0 heißen *konstante Polynome*, Polynome vom Grad 1 heißen *lineare Polynome* und Polynome vom Grad 2 heißen *quadratische Polynome*.

LEMMA 4.5. *Sei R ein kommutativer Ring und sei $R[X]$ der Polynomring über R. Dann gelten für den Grad folgende Aussagen.*

(1) $\operatorname{grad}(P+Q) \leq \max\{\operatorname{grad}(P), \operatorname{grad}(Q)\}$
(2) $\operatorname{grad}(P \cdot Q) \leq \operatorname{grad}(P) + \operatorname{grad}(Q)$
(3) *Wenn R ein Integritätsbereich ist, so gilt in (2) die Gleichheit.*

Beweis. Siehe Aufgabe 4.8. □

Polynomringe in mehreren Variablen

Die Konstruktion von Polynomringen aus einem Grundring kann man iterieren. Aus R kann man $R[X]$ machen und daraus mit einer neuen Variablen den Ring $(R[X])[Y]$ bilden. Für diesen Ring schreibt man auch $R[X,Y]$. Ein Element darin hat die Gestalt

$$\sum_{i,j} a_{ij}X^iY^j\,,$$

wobei die Summe endlich ist. Ein Ausdruck der Form X^iY^j heißt Monom. Polynome kann man auf unterschiedliche Art sortieren. Man kann die Potenz

einer Variablen (etwa Y) herausnehmen und schauen, welche Polynome in X sich darauf beziehen. Dann sieht ein Polynom folgendermaßen aus:

$$2+3X-X^2-5X^3+(1+3X-X^2+3X^5)Y+(4+X+7X^2-6X^4)Y^2+(2-X^3)Y^3\,.$$

Oder man kann entlang dem Summengrad sortieren, dies ergibt

$$2+3X+Y-X^2+3XY+4Y^2-5X^3-X^2Y+XY^2+2Y^3+7X^2Y^2+3X^5Y \\ +6X^4Y^2-X^3Y^3.$$

Polynomiale Identitäten haben viel mit allgemeingültigen Termidentitäten zu tun. In $\mathbb{Z}[X,Y]$ gilt beispielsweise

$$(X+Y)^n=\sum_{k=0}^{n}\binom{n}{k}X^kY^{n-k}$$

Diese Identität zwischen zwei Polynomen entspricht der allgemeinen binomischen Formel. Einerseits ist sie ein Spezialfall davon, da wir in dem kommutativen Ring $\mathbb{Z}[X,Y]$ sind und die speziellen Elemente X und Y anschauen. Andererseits kann man aus dieser polynomialen Identität die allgemeine binomische Formel zurückgewinnen, da man für X und Y beliebige Elemente a und b eines kommutativen Ringes einsetzen kann (und man weiß, wie man ganze Zahlen in jedem Ring interpretiert) und sich dabei die Identität erhält. Natürlich gibt es auch Polynomringe in beliebig vielen Variablen, dafür schreibt man $R[X_1,X_2,\ldots,X_n]$.

Polynomringe über einem Körper

Für uns sind zunächst die Polynomringe über einem Körper von besonderer Bedeutung.

Definition 4.6. Es sei K ein Körper und seien $a_0,a_1,\ldots,a_n\in K$. Eine Funktion

$$P\colon\ K\longrightarrow K,\ x\longmapsto P(x),$$

mit

$$P(x)\ =\ \sum_{i=0}^{n}a_ix^i\ =\ a_0+a_1x+\cdots+a_nx^n$$

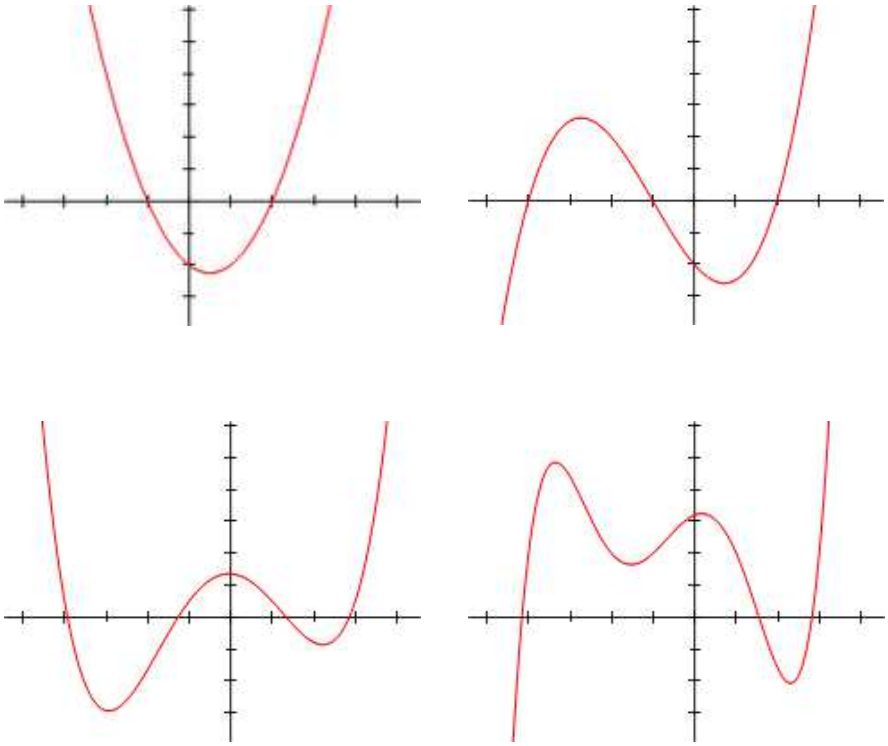
heißt *Polynomfunktion.*

Man muss zwischen Polynomen und Polynomfunktionen unterscheiden, insbesondere für $K=\mathbb{Z}/(p)$. Das Polynom

$$X^p-X$$

hat beispielsweise nach dem kleinen Fermat für jedes $a\in K$ den Wert $a^p-a=0$. D.h. die durch dieses Polynom definierte Polynomfunktion ist die Nullfunktion, obwohl das Polynom selbst nicht das Nullpolynom ist.

Bei $K=\mathbb{R}$ lassen sich die Polynomfunktionen graphisch veranschaulichen.



Eine wichtige Frage ist, für welche Elemente $x \in K$ die Polynomfunktion einen bestimmten Wert annimmt. Hierbei ist insbesondere der Wert 0 wichtig, da ja die Gleichung $P(x) = a$ äquivalent zu

$$P(x) - a = 0$$

ist und $P - a$ wieder ein Polynom ist. Für lineare Polynome $aX + b$ (mit $a \neq 0$) ist $x = \frac{-b}{a}$ die einzige Lösung. Für quadratische Polynome der reinen Form $X^2 + c$ sind die Quadratwurzeln von $-c$ aus K, falls sie denn existieren, die Lösungen. Für ein quadratisches Polynom $aX^2 + bX + c$ kann man das Bestimmen der Nullstellen durch quadratisches Ergänzen auf die reine Form zurückführen, siehe Aufgabe 4.13.

Der folgende Satz heißt *Interpolationssatz* und beschreibt die Interpolation von vorgegebenen Funktionswerten durch Polynome.

Satz 4.7. *Es sei K ein Körper und es seien n verschiedene Elemente $a_1, \ldots, a_n \in K$ und n Elemente $b_1, \ldots, b_n \in K$ gegeben. Dann gibt es ein eindeutiges Polynom $P \in K[X]$ vom Grad $\leq n-1$ derart, dass $P(a_i) = b_i$ für alle i ist.*

Beweis. Wir beweisen die Existenz und betrachten zuerst die Situation, wo $b_j = 0$ ist für alle $j \neq i$. Dann ist

$$(X - a_1) \cdots (X - a_{i-1})(X - a_{i+1}) \cdots (X - a_n)$$

ein Polynom vom Grad $n-1$, das an den Stellen $a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n$ den Wert 0 hat. Das Polynom

$$\frac{b_i}{(a_i - a_1)\cdots(a_i - a_{i-1})(a_i - a_{i+1})\cdots(a_i - a_n)} \\ (X - a_1)\cdots(X - a_{i-1})(X - a_{i+1})\cdots(X - a_n)$$

hat an diesen Stellen ebenfalls eine Nullstelle, zusätzlich aber noch bei a_i den Wert b_i. Nennen wir dieses Polynom P_i. Dann ist

$$P \;=\; P_1 + P_2 + \cdots + P_n$$

das gesuchte Polynom. An der Stelle a_i gilt ja

$$P_j(a_i) \;=\; 0$$

für $j \neq i$ und $P_i(a_i) = b_i$.

Die Eindeutigkeit folgt aus Korollar 5.6. □

Abbildungsverzeichnis