Polynome über Gruppen

Polynomials over Groups

Diplomarbeit zur Erlangung des akademischen Grades eines Magisters in der Studienrichtung Mathematik an der formal- und naturwissenschaftlichen Fakultät

verfaßt von

Peter Balazs

Angefertigt am Institut für Mathematik der Universität Wien bei

Univ. Prof. G. Kowol

Wien, November 2001

Vorwort

Einleitung

"'Polynome haben wir in der Schule gemacht, und von Gruppen habe ich schon gehört! Aber was sind 'Polynome über Gruppen'*?"*

Polynome sind „klassische" Objekte der Mathematik. Es gibt wohl keinen Mathematikstudenten, ja sogar keinen Schüler, der noch nie etwas mit Polynomen zu tun hatte. Bereits in der Mittelschule kommt man damit sehr oft in Kontakt.

Dort kennt man Polynome, genauer Polynomfunktionen, als Funktionen, deren Werte (an einer bestimmten Stelle) durch „einfache" Rechnungen, d.h Addition, Subtraktion und Multiplikation, bestimmt werden kann. Als Term bezeichnet man die Beschreibung dieser Rechnungen mit Unbestimmten („x"). So ist die Funktion (über den reellen Zahlen $\mathbb{R}$)

$$f(x) = x^2 + 1$$

eine Polynomfunktion. Der Term $x^2 + 1$ beschreibt sehr anschaulich, wie man von einem Ausgangswert x auf den Funktionswert $f(x)$ kommt. Man muß gerade den Ausgangswert x mit sich selbst multiplizieren und dann 1 addieren.

Polynome haben (hier) die folgende allgemeine Gestalt:

$$f(x) = a_k \cdot x^k + a_{k-1} \cdot x^{k-1} + \ldots + a_2 \cdot x^2 + a_1 \cdot x + a_0$$

Die a_i nennt man *Koeffizienten*, das höchste k für das $a_k \neq 0$ den *Grad* des Polynoms. Dem Nullpolynom ($a_i = 0 \forall i$) ordnet man keinen Grad zu.

In der Mittelschule werden Polynomfunktionen als Beispielsfunktionen für verschiedenste analytische Methoden wie das Differenzieren und Integrieren sowie das Auffinden von Nullstellen herangezogen, da sie durch ihre Terme leicht beschreibbar sind und diese Operationen bei Polynomfunktionen recht leicht durchführbar sind.

Man denke nur an die endlosen Kurvendiskussionen, wo nur die schwierigeren Beispiele *nicht* Polynomfunktionen waren.

In der Mittelschule wird sowohl für die Koeffizienten als auch für den Wertebereich meist der Körper der rationalen Zahlen $\mathbb{Q}$ oder der reellen Zahlen $\mathbb{R}$ herangezogen.

Doch sind Körper bereits in der Mittelschule nicht die einzigen interessanten Mengen, so sind ist z.B. die Menge der ganzen Zahlen, $\mathbb{Z}$, kein Körper mehr (sondern ein kommutativer Ring mit Eins), da es im allgemeinen kein multiplikatives Inverses gibt.

Behandelt man zum Beispiel Matrizen über $\mathbb{R}$, so geht man mit einer Menge um, wo die Multiplikation im allgemeinen nicht mehr kommutativ ist (d.h. für zwei Matrizen A und B ist im allgemeinen $A \cdot B \neq B \cdot A$).

Aber auch auf diesen beiden Mengen kann man Polynome betrachten und auswerten. So kann die obige Polynomfunktion $f(x) = x^2 + 1$ als Funktion auf diesen beiden Mengen aufgefaßt werden. D.h. wir sind nicht auf Körper beschränkt!

Diese genauere Untersuchung von Polynomen über anderen algebraischen Strukturen bleibt der Hochschule vorbehalten. In der Analysis werden Polynomfunktionen untersucht, diese werden wiederum als Beispiele herangezogen, aber sie dienen auch zur Approximation und man lernt Schemate, um Werte schnell zu berechnen.

In der Algebra werden Polynome über beliebigen (meist kommutativen) Ringen betrachtet. Sei R ein kommutativer Ring mit Einslement, dann sind Polynome Wörter, d.h„sinnvolle“ Aneinanderreihung von Symbolen (Elemente und Operationen von R und eine „Unbestimmte“ x sind), die man ebenso in symbolischer Art und Weise addieren, subtrahieren und muliplizieren kann. Als „sinnvoll“ läßt man Ausdrücke zu, die, wenn man für die Unbestimmte ein Element aus R einsetzt, wieder ein Element von R ergeben. D.h. man läßt nur jene Ausdrücke zu,wo die Unbestimmte so wie ein Element des Rings verwendet wird. So sind z.B. die Ausdrücke $3 \cdot x$, $x + x + x$ und $-x + 2 \cdot x^2 - x$ sinnvolle Ausdrücke über den ganzen Zahlen, im Gegensatz zu $+ + x + +$ oder $xxx\cdot^{-1}$

Jedes Polynom kann auf die folgende Form gebracht werden:

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

wobei die Koeffizienten a_i in R liegen. Die Potenzschreibweise verwendet man (wie üblich) als Abkürzung des mehrmaligen Produkts mit sich selbst, so ist $x^n = \underbrace{x \cdot x \cdot \ldots \cdot x}_{n}$.

Wenn wir dies als Abbildung $x \mapsto p(x), x \in R$ auffassen, gelangen wir zu Polynomfunktionen. Ein Kernproblem dieser Arbeit wird hier aufgeworfen: Repräsentieren verschiedene Polynome verschiedene Funktionen? Welche Polynome repräsentieren die selbe Funktion? Wann sind Polynome überhaupt verschieden?

Beispiel: Betrachten wir den Körper $\mathbb{Z}_2 = \{0, 1\}$ dessen Operationen $\cdot$ und $+$ wir folgt festgelegt sind:

$+$	0	1
0	0	0
1	0	1

$\cdot$	0	1
0	0	1
1	1	0

Dann induzieren z.B. die Polynome $x^2 - x$ und 0, oder $1 \cdot x$ und x, $x - 1$ und $x^4 - x^3 + x^2 - x - 1$ jeweils dieselbe Polynomfunktion.

Wir wollen in dieser Arbeit einen Schritt weiter als in der klassischen Algebra gehen. Im ersten Kapitel werden wir untersuchen, wie man sich Polynome und Polynomfunktionen über allgemeinen Klassen von algebraischen Strukturen vorstellen kann, sogenannten *Varietäten*, d.h. Klassen von Mengen mit bestimmten Operation und bestimmten Gesetzen. Die meisten bekannten Strukturen wie Ringe, Gruppen oder Verbände sind Varietäten. Wir werden feststellen, welche Ausagen dort getroffen werden können und welche Begriffe dort bereits sinnvoll sind. Wir werden in diesem Kapitel auch die Frage untersuchen, für welche Mengen alle Funktionen Polynomfunktionen sind.

Im zweiten Kapitel studieren wir die Funktionenkomposition (das Hintereinanderausführen von Funktionen) und eine analoge Operation für Polynome. Weiters definieren wir mehrstellige Polynome. Wir werden sehen, daß jeder Strukturhomomorphismus (das ist eine Abbildung φ, die die Operationen „respektiert“, d.h. z.B. für die Multiplikation in Gruppen gilt: $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$) einen Homorphismus auf der Menge der Polynomen bzw. Polynomfunktionen induziert. Wir werden definieren, was wir uns unter einer Polynommatrix verstehen, und Polynomfunktionen betrachten, die Permutationen (d.h. „1 zu 1“ Abbildungen) sind.

Im dritten und letzten Kapitel spezialisieren wir die erlangten Erkenntnisse und Begriffe auf Gruppen. Wir werden untersuchen in welchen Formen wir die Polynome und Polynomfunktionen darstellen können, wie sich spezielle Eigenschaften von Gruppen (Nilpotenz, Auflösbarkeit und Permutationseigenschaften) der Gruppe auf die Gruppe der Polynome und Polynomfunktionen sowie umgekehrt auswirken. Wir werden uns dort auch der Frage stellen,

welche Polynome bijektive Abbildungen oder Homomorphismen induzieren!

Stellt man sich unbeeinflußt, ohne (größere) Vorkenntnisse die Frage, was Polynome über Gruppen sind, dann denkt man darüber nach, was mit den obigen Formen der Polynome (über Ringen) „passiert“ wenn es keine Multiplikation gibt und die Addition nicht kommutativ ist. Man würde wohl vermuten (zumindest hat das der Autor beim ersten Kontakt mit diesem Thema getan), daß (einstellige) Polynome über Gruppen in der folgenden Art und Weise dargestellt werden können:

$$p = a_0 + \sum_{i=1}^{n} (k_i \cdot x + a_i) \text{ für } k_i \in \mathbf{Z}$$

wobei die k_i ganzen Zahlen sind, sodaß $k_i \cdot x = \underbrace{x + x + \ldots + x}_{k_i}$. Zu beachten ist auch, daß in Gruppen die Operation (hier die Addition $+$) im allgemeinen eben nicht kommutativ ist. Die hier präsentierte Theorie der Polynome leistet genau das, angewandt auf Ringe liefert sie die bekannten Polynome, auf Gruppen angewandt liefert sie Ausdrücke der obigen Form. Sie ist somit eine recht „natürliche“ Theorie.

Warum wendet man sich überhaupt so ausgiebig dieser Klasse von Funktionen zu? Polynomfunktionen sind weit verbreitet in der Mathematik. Ihre Bedeutung kommt daher, dass sie mit einem einfachen, nur Grundrechnungsarten enthaltenden Term darstellbar und dadurch leicht beschreib- und berechenbar sind. Dadurch kann man nicht nur eine Funktion, die eventuell auf einer unendlichen Menge wirkt, mit einem endlichen Term beschreiben, man kann auch durch diese Beschreibung bereits einige Eigenschaften „sehen“ ohne viel berechnen zu müssen. Analytische Eigenschaften von Polynomfunktionen sind leicht berechenbar, wodurch sie sich eben auch in vielen (Schul-) Aufgaben wiederfinden.

In der numerischen Mathematik verwendet man Polynomfunktionen, um andere Funktionen zu approximieren. Man versucht nach Möglichkeit immer zu Polynomfunktionen zu gelangen, da diese eben leicht berechenbar und darstellbar sind. Anwendungen für Polynomfunktion gibt es sehr viele:

So kann man zum Beispiel jede stetige reelle Funktion beliebig genau durch eine Polynomfunktion approximiert werden, und somit der Wert einer solche Funktion an jeder Stelle beliebig genau durch den einer Polynomfunktion bestimmt werden.

In der numerischen Akustik kombiniert man mit der „Chaospolynom“-

methode verschiedene Lösungsmethoden (BEM, FEM und andere) um Schallfelder zu berechnen.

In der Physik wird ein Ausgleichspolynom durch Werte der Experimentmessungen gelegt, um damit Modelle zu bilden. Auch haben viele physikalischen Aussagen polynomialen Charakter (z.B. die Gleichung für die gleichmäßig beschleunigte Bewegung $s = \frac{at^2}{2}$)

Das wohl wichtigste Buch für diese Arbeit war *„Algebra of Polynomials“* [18]. Neben den zahlreichen anderen Artikeln und Arbeiten möchte ich *„Interpolation with Near-rings of Polynomial Functions“* [1] hervorheben, das mir einen anderen, „frischeren “ Zugang zu dem Thema bot.

Ziel

Ziel dieser Arbeit ist es eine möglichst verständliche Erarbeitung und Einführung der Grundlagen, einen möglichst ausführlichen Überblick über die existierenden Ergebnisse und einen exemplarischer Einblick in die Methoden der Beweisführung zu geben.

Zudem wurde versucht, einen etwas anderen Zugang als in [18] (und dadurch dem Großteil der Literatur) mit etwas (zumindest für den Autor) intuitiverer Symbolik zu erreichen. Einige Aussagen konnten verallgemeinert werden. Der Großteil davon wird in der Literatur erwähnt, jedoch nicht ausformuliert. Darüber hinaus konnten auch z.B. einige Aussagen von *Scott* [29] für den nicht unbedingt endlichen und den mehrstelligen Fall, $k > 1$, untersucht und teilweise verallgemeinert werden.

Beweise wurden dann aufgenommen,

- wenn sie guten Einblick in die Materie bieten
- wenn sie einer genaueren Ausformulierung bedurften, um das Verständnis zu erleichtern, bzw. wenn „Trivialitäten“ es verdienten, genauer durchdacht und ausformuliert zu werden
- wenn sie durch Umformulierung leichter verständlich wurden
- wenn sie Beweise für Aussagen sind, die nicht oder nicht so in der Literatur erwähnt werden

Da aber ein Überblick angestrebt ist und der Rahmen dieser Arbeit nicht all zu sehr gesprengt werden sollte, kann nur ein Bruchteil der Aussagen bewiesen werden. Nur ausformulierte Beweise enden mit □, bei anderen ist ein Zitat angegeben. Sollte beides fehlen, so ist die Beweisführung durch die vorangegangenen Überlegungen und Sätze klar.

Danksagung

Ich bin *Prof. F. Punz* für seinen Mathematikunterricht dankbar, der neben den „Rechnereien“ doch noch immer wieder genug Platz für Logik und Nachdenken fand. Ich bin ihm auch dankbar, daß er mich mit den Worten "Versuch das nicht, das ist Dir zu schwer!“ erst recht motiviert hat, mich dem Studium der Mathematik zuzuwenden.

Neben vielen anderen Professoren möchte ich Herrn *Univ. Prof. S. Grosser* danken, der in mir das Interesse an Algebra und Topologie geweckt und gefördert hat. In diesem Zusammenhang möchte ich *Dr. G. Landsmann* für die zahllosen Gespräche nach den Proseminaren danken. Hr. *Mag. Alexej Tajmel* danke ich für die vielen gemeinsamen Stunden, in denen wir doch auch manchmal etwas für unser Studium gemacht haben.

Ausdrücklich möchte ich noch *Univ. Prof. H. Schoißengeier* danken, der nicht nur mein Interesse an der Algebra und der Topologie weiter verstärkte, sondern mir auch beim Abschluß (gemeinsam mit *Univ. Prof . F. Haslinger*) geholfen hat, einige bürokratische Hürden zu überwinden.

Ich bin der *Akademie der Wissenschaften*, insbesondere dem *Insitut für Schallforschung* unter der Leitung von *Univ. Doz. W.A. Deutsch* zu Dank verpflichtet, da ich nicht nur durch den Posten als Programmierer dort nun finanziell abgesichert bin, Freiheiten in der Arbeitseinteilung habe, um das Studium voranzutreiben, und zur Fertigstellung der Diplomarbeit Sonderurlaub bekommen habe, sondern v.a., da ich dort auch wissenschaftlich tätig sein darf.

Zu großem Dank bin ich verpflichtet:

- Meiner ganzen Familie, besonders meiner *Mutter* , die mich nun 30 Jahre lang unterstützt hat und nur ein bissschen die Geduld verloren hat.

- *Dr. Robert Baumgartner* , der nicht nur im gemeinsamen Studium half, Motivationslöcher zu überwinden (aber auch andere zu öffnen),

sondern der sich auch die Aufgabe auferlegt hat, sich in diese Arbeit einzulesen und sie auch inhaltlich Korrektur zu lesen.

- Meinem Betreuer, *Univ. Prof. G. Kowol* , der mich für dieses Thema interessieren konnte, der mir auch beim bürokratischen Abschluß des zweiten Studienabschnitts sehr half und der immer für Fragen offen war.

- Und ganz besonderen Dank gilt meiner Frau, *Claudia* , die mich all die Jahre mit Geduld und Liebe unterstützt hat. Sie macht mich vollständig!