

Albrecht Beutelspacher
Ute Rosenbaum

Projektive Geometrie

vieweg studium

Aufbaukurs Mathematik

Herausgegeben von Martin Aigner, Peter Gritzmann, Volker Mehrmann
und Gisbert Wüstholtz

Martin Aigner

Diskrete Mathematik

Walter Alt

Nichtlineare Optimierung

Albrecht Beutelspacher und Ute Rosenbaum

Projektive Geometrie

Gerd Fischer

Ebene algebraische Kurven

Wolfgang Fischer und Ingo Lieb

Funktionentheorie

Otto Forster

Analysis 3

Klaus Hulek

Elementare Algebraische Geometrie

Horst Knörrer

Geometrie

Helmut Koch

Zahlentheorie

Ulrich Krengel

Einführung in die Wahrscheinlichkeitstheorie und Statistik

Wolfgang Kühnel

Differentialgeometrie

Ernst Kunz

Einführung in die algebraische Geometrie

Werner Lütkebohmert

Codierungstheorie

Reinhold Meise und Dietmar Vogt

Einführung in die Funktionalanalyse

Erich Ossa

Topologie

Jochen Werner

Numerische Mathematik I und II

Jürgen Wolfart

Einführung in die Zahlentheorie und Algebra

Albrecht Beutelspacher
Ute Rosenbaum

Projektive Geometrie

**Von den Grundlagen
bis zu den Anwendungen**

2., durchgesehene und erweiterte Auflage



Bibliografische Information Der Deutschen Bibliothek
Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie;
detaillierte bibliografische Daten sind im Internet über <<http://dnb.ddb.de>> abrufbar.

Prof. Dr. Albrecht Beutelspacher
Justus-Liebig-Universität Gießen
Mathematisches Institut
Arndtstraße 2
35392 Gießen
E-Mail: albrecht.beutelspacher@math.uni-giessen.de

Dr. Ute Rosenbaum
Siemens AG
81737 München
E-Mail: ute.rosenbaum@siemens.com

1. Auflage 1992
- 2., durchgesehene und erweiterte Auflage Februar 2004

Alle Rechte vorbehalten
© Friedr. Vieweg & Sohn Verlag/GWV Fachverlage GmbH, Wiesbaden 2004

Der Vieweg Verlag ist ein Unternehmen von Springer Science+Business Media.
www.vieweg.de



Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Verlags unzulässig und strafbar. Das gilt insbesondere für Vervielfältigungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Umschlaggestaltung: Ulrike Weigel, www.CorporateDesignGroup.de

Gedruckt auf säurefreiem und chlorfrei gebleichtem Papier

ISBN-13: 978-3-528-17241-1 e-ISBN-13: 978-3-322-80329-0
DOI: 10.1007/978-3-322-80329-0

Vorwort

Geometrie? Hat Geometrie heute überhaupt noch eine Bedeutung? In der Schule? Auf der Universität? In der Forschung? – Es ist unübersehbar, dass das Ansehen der Geometrie im allgemeinen Bewusstsein deutlich zurückgegangen ist. Diesen Eindruck gewinnt man nicht nur, wenn man sich die heutige Schulgeometrie vergegenwärtigt, nicht nur, wenn man sich die Vorlesungen und Lehrbücher für Studenten anschaut, nicht nur, wenn man die sich unterordnende Stellung der Geometrie auf internationalen Tagungen betrachtet – dieser Eindruck drängt sich vor allem dann auf, wenn man mit Geometern zu tun hat. Dieser Vorwurf wird nicht von außen erhoben, viel schlimmer: Die Geometer glauben selbst nicht mehr an ihre Sache! Die Gründe, die für den vermeintlichen Niedergang der Geometrie genannt werden, sind vage und wirr: reine Mathematik sei sowieso obsolet, innerhalb der Mathematik hätten andere Disziplinen viel größeres Ansehen und viel größeres Selbstbewusstsein, Geometrie sei in Algebra aufgegangen, ...

Wenn schon Geometrie, warum dann ausgerechnet *projektive* Geometrie? Wenn überhaupt, dann wenigstens algebraische Geometrie oder Differentialgeometrie oder (für diejenigen, die sich noch für philosophische „Scheinprobleme“ interessieren können) Grundlagen der Geometrie. Projektive Geometrie ist doch ein Gebiet, das a priori uninteressant ist, in dem alle Fragen spätestens im vorigen Jahrhundert gelöst wurden, ein Gebiet, das bestenfalls angewandte lineare Algebra ist. Kurz: ein Gebiet, das in der heutigen Zeit, in der es nicht um reine Anschauung, sondern um reale Anwendungen geht, bestenfalls als harmloses Steckenpferd für pensionierte Studienräte taugt, in der modernen Lehre und Forschung aber nichts verloren hat.

Dieser Eindruck ist falsch! Und zwar mindestens aus den folgenden Gründen.

Zum ersten ist projektive Geometrie ein *Glanzstück der Mathematik*, das neben der Entdeckung der nichteuklidischen Geometrie und der Entwicklung der Analysis und Algebra zu den Höhepunkten des an Mathematik reichen 19. Jahrhunderts zählt, auf das wir mit Recht stolz sind. Projektive Geometrie gehört ebenso zur mathematischen Allgemeinbildung wie etwa Funktionentheorie und Galoistheorie. Projektive Geometrie ist überdies die Grundlage für algebraische Geometrie, ein zentrales Gebiet der modernen Mathematik.

Zweitens hat die projektive Geometrie in der Mitte unseres Jahrhunderts in der Forschung einen neuen kräftigen Impuls durch die Verbindung mit der Kombinatorik erhalten. Die Herausforderung, klassische geometrische Strukturen durch ihre Parameter, also scheinbar nur äußerliche Eigenschaften, zu beschreiben, hat zur Entwicklung der *endlichen Geometrie* geführt, einer Blüte der Forschung, die bis heute andauert.

Schließlich hat projektive Geometrie in den letzten Jahren als *Quelle für viele Anwendungen* neue Bedeutung erlangt. Überraschenderweise eignen sich nämlich Strukturen der klassischen projektiven Geometrie in idealer Weise dazu, Szenarien und Anforderungen aus der Welt der Kommunikation zu beschreiben. Besonders hervorzuheben

sind die Anwendungen, die die projektive Geometrie in der Codierungstheorie und Kryptographie gefunden hat.

Bis weit ins 19. Jahrhundert galt Geometrie als die Wissenschaft, deren Aufgabe es ist, den uns umgebenden physikalischen Raum zu beschreiben. Die bahnbrechende Leistung von David HILBERTS (1862 - 1943) einflussreichem Buch *Grundlagen der Geometrie* (1899) war die Erkenntnis, dass Geometrie *rein innermathematisch* begründet werden kann. Dies hat zwar prinzipiell den Weg gebahnt, mit der Geometrie ganz andere Strukturen als den Anschauungsraum zu beschreiben. Diese Chance wurde jedoch zunächst nicht wahrgenommen; vielmehr wurde in der Nachfolge HILBERTS dem Bezug der Geometrie zur Wirklichkeit wenig Beachtung geschenkt. Dies ist zwar historisch verständlich, aber darin besteht aber auch eine Gefahr. Dieser Gefahr suchen wir in diesem Buch zu begegnen, indem wir viele Anwendungen behandeln – und zwar solche, die sich auch HILBERT wahrscheinlich nicht vorgestellt hat.

Was Geometrie heute ist, können wir natürlich auch nicht genau sagen. In jedem Fall ist Geometrie eine außerordentlich gute Sprache zur Beschreibung zahlreicher inner- und außermathematischer Phänomene. Auch dies soll in diesem Buch zum Ausdruck kommen.

* * *

Die ersten vier Kapitel sind in ihrem Großteil der reinen Geometrie gewidmet. Im ersten wird der synthetische Aufbau der projektiven Geometrie beschrieben; hier werden die Begriffe Basis, Dimension, Unterraum und affiner Raum eingeführt. Das zweite Kapitel führt die wichtigste Klasse projektiver Räume, nämlich die mit Hilfe eines Vektorraums konstruierbaren („koordinatisierbaren“) ein. In der analytischen Geometrie wird meist stillschweigend so getan als wären dies *alle* projektiven und affinen Räume und keine anderen Strukturen wären denkbar. Wir untersuchen diese Frage in Kapitel 3 genau: Das entsprechende Kernstück klassischer Geometrie (der Struktursatz für projektive Räume) sagt, dass jeder projektiver oder affiner Raum, in dem der Schließungssatz von DESARGUES gilt, koordinatisierbar ist. Insbesondere werden wir zeigen, dass jeder projektiver oder affiner Raum einer Dimension ≥ 3 über einem Vektorraum koordinatisiert werden kann. Anschließend werden wir auch alle Kollineationen desarguesscher projektiver Räume beschreiben. In Kapitel 4 betrachten wir die vermutlich am intensivsten untersuchten Objekte der klassischen Geometrie, nämlich die Quadriken. Wir machen uns dabei den modernen synthetischen Standpunkt zu eigen und versuchen, möglichst weit mit dem Begriff der „quadratischen Menge“ zu kommen. Dies hat neben der größeren Übersichtlichkeit auch den Vorteil der besseren Einsicht in das geometrische Verhalten dieser Strukturen.

Neben dem begrifflichen synthetischen Ansatz betrachten wir schon in diesen Kapiteln die jeweiligen *endlichen* Situationen; insbesondere bestimmen wir die Parameter der uns interessierenden Objekte. Ferner ist jedem Kapitel als Anhang eine Anwendung hinzugefügt. So wird deutlich, dass manche Anwendungen auch auf ganz einfachen geometrischen Strukturen aufbauen.

In den beiden Abschlusskapiteln werden dann wichtige Anwendungen, nämlich Codierungstheorie und Kryptographie thematisiert. Das Ziel der Codierungstheorie ist die Entwicklung von Methoden, die zufällige Fehler, die bei der Übertragung oder Speicherung von Daten entstehen, erkennen. Man kann viele Probleme der Codierungstheorie direkt in geometrische Probleme übersetzen. In der Kryptographie geht es einerseits darum, Daten geheim zu halten (zu verschlüsseln), andererseits darum, Daten gegen Veränderung zu schützen. Überraschenderweise haben Kryptosysteme, die auf projektiver Geometrie basieren, ganz herausragende Eigenschaften: Sie sind – im Gegensatz zu den meisten heute gebräuchlichen Verfahren – beweisbar sicher! Einige dieser Systeme werden in Kapitel 6 dargestellt.

* * *

Dieses Buch basiert aus didaktischer Sicht auf drei Axiomen.

1. Wir setzen nicht voraus, dass der Leser aus der Schule oder aus den Grundvorlesungen eine intensive Erfahrung der affinen oder projektiven Geometrie mitbringt. Daher haben wir auch die elementaren Dinge ausführlich dargestellt. Wir setzen allerdings eine Vertrautheit im Umgang mit den mathematischen Begriffen voraus, wie sie im ersten Semester vermittelt werden: Wörter wie „Äquivalenzrelation“, „Basis“ oder „surjektiv“ sollten Sie nicht erschrecken.
2. Es mussten diejenigen Teile der projektiven Geometrie dargestellt werden, die für die Anwendungen wichtig sind.
3. Schließlich handelt es sich um den Stoff, der wirklich in einer zweisemestrigen Vorlesung dargestellt werden kann.

Dies bedeutet schmerzliche Einschnitte in den im 19. Jahrhundert kanonisierten Stoff der projektiven Geometrie: Bei uns gibt es weder Doppelverhältnisse noch harmonische Lagen; nichtdesarguessche Ebenen tauchen nur am Rande auf, Projektivitäten fehlen und Kollineationsgruppen werden nicht thematisiert. Dies mag man bedauern. Dem stehen aber unserer Meinung nach folgende positiven Punkte gegenüber:

- Dies ist ein Buch, das auch von Studierenden selbständig *gelesen* werden kann.
- Die meisten der zahlreichen Übungsaufgaben sind sehr einfach gehalten, so dass sie dem Leser als Kontrolle dienen können.
- Wir sind stolz darauf, einige wichtige Dinge zum ersten Mal in einem Lehrbuch verarbeitet zu haben: Dazu gehört die Klassifikation von Quadriken (Satz 4.4.4) in endlichen Räumen, die hier durch rein kombinatorische Überlegungen erhalten wurde. Ein weiteres Beispiel ist die rein geometrisch-kombinatorische Beschreibung der REED-MULLER-Codes. Schließlich ist hier der Satz von GILBERT, MACWILLIAMS und SLOANE zu nennen (siehe 6.3.1), dessen Beweis – wie wir meinen – sehr durchsichtig geworden ist.
- Last not least beschreiben wir die in Kapitel 1 und 4 behandelten geometrischen Strukturen mit Hilfe von *Diagrammen*. Dies ist eine Beschreibungsmethode für geometrische Strukturen, die in der Forschung seit etwa 20 Jahren angewandt wird und die weite Teile der geometrischen Forschung von Grund auf neu strukturiert hat.

* * *

Ein Buch gemeinsam zu schreiben ist ein echtes Abenteuer, bei dem man zu Beginn nicht weiß, worauf man sich einlässt. In unserem Fall gab es eine durchweg sehr positive Zusammenarbeit, die (auch über weite Entfernungen hinweg) intensiv und spannend war. Viele Sachverhalte wurden uns dadurch klarer, dass einer von uns eine sogenannte „dumme Frage“ stellte und wir uns dann scheinbar klare Dinge nochmals gründlich klarmachen mussten. Jeder hat den anderen davor bewahrt, zu verdrängen, dass Beweise noch nicht klar formuliert waren, zu ignorieren, dass der Aufbau eines Abschnitts noch nicht schlüssig war, zu vergessen, dass Zitate noch nicht nachgeprüft waren, ... Wir sind in der Hoffnung, dass dieses intensive Durchhackern des Stoffes Ihnen zugute kommt.

* * *

Wir danken vor allem den Studierenden und Mitarbeitern, die die Entstehung dieses Buches auf mannigfaltige Weise gefördert haben – unter anderem dadurch, dass sie frühe Versionen dieses Buches heftig kritisiert haben. Unser besonderer Dank gilt den Herren Uwe Blöcher, Jörg Eisfeld, Udo Heim, Joachim Hilgert und Klaus Metsch, die das Manuskript und die erste Auflage dieses Buchs äußerst kritisch gelesen und zahlreiche Fehler jeder Kategorie gefunden haben.

Ferner danken wir dem Verlag Vieweg für die gewohnt freundliche, engagierte und effiziente Zusammenarbeit.

Schließlich danken wir unseren Frauen und Männern für die zwar nicht immer freiwillige, aber notwendige und äußerst großzügige Unterstützung.

Großen-Buseck und Kempten im Januar 2004

Albrecht Beutelspacher
Ute Rosenbaum

Inhaltsverzeichnis

Kapitel 1 Synthetische Geometrie	1
1.1 Grundbegriffe	1
1.2 Die Axiome der projektiven Geometrie	5
1.3 Aufbau der projektiven Geometrie	9
1.4 Quotientengeometrien	19
1.5 Endliche projektive Räume	21
1.6 Affine Geometrie	26
1.7 Diagramme	31
1.8 Anwendung: Effiziente Kommunikation	39
Übungsaufgaben	41
Richtig oder falsch?	48
Projekt	49
Sie sollten mit folgenden Begriffen umgehen können:	51
Kapitel 2 Analytische Geometrie	53
2.1 Der projektive Raum $P(V)$	53
2.2 Der Satz von Desargues und der Satz von Pappos	57
2.3 Homogene und inhomogene Koordinaten	63
2.4 Das Hyperboloid	67
2.5 Rationale Normkurven	71
2.6 Die Moulton-Ebene	73
2.7 Räumliche Geometrien sind desarguessch	75
2.8 Anwendung: Ein Verkabelungsproblem	78
Übungsaufgaben	86
Richtig oder falsch?	90
Projekt	90
Sie sollten mit folgenden Begriffen umgehen können:	91
Kapitel 3 Die Struktursätze oder	
Wie lassen sich projektive und affine Räume gut beschreiben?	93
3.1 Zentralkollineationen	93
3.2 Die Gruppe der Translationen	102
3.3 Der Schiefkörper	108
3.4 Die ersten Struktursätze	113
3.5 Die zweiten Struktursätze	116
3.6 Projektive Kollineationen	124
Übungsaufgaben	130
Richtig oder falsch?	133
Sie sollten mit folgenden Begriffen umgehen können:	134

Kapitel 4	Quadratische Mengen	135
4.1	Grundlegende Definitionen	135
4.2	Der Index einer quadratischen Menge	139
4.3	Quadratische Mengen in Räumen kleiner Dimension	141
4.4	Quadratische Mengen in endlichen projektiven Räumen	144
4.5	Elliptische, parabolische und hyperbolische quadratische Mengen	147
4.6	Die Kleinsche quadratische Menge	155
4.7	Quadriken	158
4.8	Plücker-Koordinaten	162
4.9	Fachwerke	171
	Übungsaufgaben	182
	Richtig oder falsch?	185
	Sie sollten mit folgenden Begriffen umgehen können:	185
Kapitel 5	Anwendungen von Geometrie in der Codierungstheorie	187
5.1	Grundlegende Begriffe der Codierungstheorie	187
5.2	Lineare Codes	191
5.3	Hamming-Codes	196
5.4	MDS-Codes	201
5.5	Reed-Muller-Codes	208
5.6	WOM-Codes	213
	Übungsaufgaben	215
	Richtig oder falsch?	218
	Projekte	218
	Sie sollten mit folgenden Begriffen umgehen können:	219
Kapitel 6	Anwendungen von Geometrie in der Kryptographie	221
6.1	Grundlegende Begriffe der Kryptographie	221
6.2	Verschlüsselung	224
6.3	Authentifikation	231
6.4	Shared Secret Schemes	240
6.5	Speicherplatzreduktion für kryptographische Schlüssel	248
	Übungsaufgaben	251
	Projekt	253
	Sie sollten mit folgenden Begriffen umgehen können:	254
	Literaturverzeichnis	255
	Stichwortverzeichnis	261
	Symbolverzeichnis	265