

Pflichtmodul Algebra

– Vorlesungsskript –

Algebra

Dietrich Burde

2019

Inhaltsverzeichnis

1	Einleitung	5
2	Gruppen	7
2.1	Gruppenaxiome	7
2.2	Gruppenhomomorphismen	11
2.3	Nebenklassen und Faktorgruppen	14
2.4	Symmetrische Gruppen	22
2.5	Gruppen kleiner Ordnung	25
2.6	Gruppenoperationen	29
2.7	Die Klassengleichung	32
2.8	Die Sylowsätze	38
2.9	Semidirekte Produkte	46
2.10	Auflösbare und nilpotente Gruppen	49
3	Ringe	59
3.1	Ringaxiome	59
3.2	Ideale und Restklassenringe	61
3.3	Einheiten, Nullteiler, Integritätsringe	64
3.4	Hauptidealringe und Euklidische Ringe	66
3.5	Polynomringe	70
3.6	Primideale und maximale Ideale	72
3.7	Bruchringe und Quotientenkörper	75
3.8	Teilbarkeit und faktorielle Ringe	77
3.9	Der Satz von Gauß	84
3.10	Irreduzibilitätskriterien für Polynome	89
4	Körper	95
4.1	Grundlagen	95
4.2	Körpererweiterungen	96

Inhaltsverzeichnis

4.3	Algebraische Erweiterungen	103
4.4	Automorphismen von Körpererweiterungen	105
4.5	Zerfällungskörper	108
4.6	Algebraischer Abschluss	114
4.7	Endliche Körper	118
4.8	Galoiserweiterungen	122
4.9	Kreisteilungskörper	137
4.10	Auflösbarkeit durch Radikale	139
4.11	Konstruierbarkeit mit Zirkel und Lineal	145
4.12	Der Fundamentalsatz der Algebra	151

1 Einleitung

Die Vorlesung *Algebra* ist Bestandteil des Bachelor-Studiengangs in Mathematik der Universität Wien. Es stellt den Kernpunkt der Ausbildung im Bereich der Algebra im Bachelorstudium dar. Aufbauend auf Vorkenntnisse aus linearer Algebra und Zahlentheorie werden die Studierenden mit dem abstrakt-strukturellen Zugang zur Algebra vertraut gemacht. Die Studierenden erhalten eine fundierte Ausbildung auf den zentralen Teilgebieten der Algebra.

Das Wort *Algebra* kommt aus dem Arabischen - al-ğabr - das Zusammenfügen gebrochener Teile, und bezeichnet das Rechnen mit Gleichungen in Unbekannten. Als Begründer der Algebra gilt der Grieche *Diophantos von Alexandria*, der wahrscheinlich zwischen 100 v. Chr. und 350 n. Chr. lebte. Sein 13 Bände umfassendes Werk *Arithmetica* ist das älteste bis heute erhaltene, in dem Gleichungen in Unbekannten verwendet werden. Bei Gleichungen geht es hauptsächlich um Polynomgleichungen wie etwa

$$x^5 - 4x + 2 = 0$$

in einer Unbekannten x . Allerdings kann man auch mehrere Unbekannte betrachten, wie etwa

$$y^2 = x^3 - 36x.$$

Diese Gleichungen sollen in gewissen Zahlbereichen gelöst werden. Das sind oft Körper wie \mathbb{R} oder \mathbb{C} . Es können aber auch ganzzahlige Lösungen gemeint sein. Für \mathbb{Z} oder \mathbb{Q} spricht man von *Diophantischen Gleichungen*, und das ist ein Zweig der Zahlentheorie. Sind die Exponenten höchstens 1, spricht man von linearen Gleichungen, oder linearen Gleichungssystemen, die in der linearen Algebra behandelt werden. Lineare und quadratische Gleichungen in einer Variablen sind leicht zu lösen. Interessanter wird es aber schon bei kubischen Gleichungen. Es bedurfte schon einiger Anstrengungen, um auch nur eine Lösung in einem Spezialfall zu finden. Das gelang

1 Einleitung

Tartaglia im Jahr 1535 mit der Gleichung

$$x^3 + ax = b,$$

mit reellen Zahlen $a, b > 0$. Er zeigte, dass

$$x = \sqrt[3]{\frac{b}{2} + \sqrt{\left(\frac{b}{2}\right)^2 + \left(\frac{a}{3}\right)^3}} + \sqrt[3]{\frac{b}{2} - \sqrt{\left(\frac{b}{2}\right)^2 + \left(\frac{a}{3}\right)^3}}$$

eine reelle Lösung ist. Cardano konnte 1545 die allgemeine kubische Gleichung $x^3 + ax^2 + bx + c = 0$ auf den obigen Fall $x^3 + px + q = 0$ reduzieren und fand Lösungsformeln, mit Ferrari auch für Grad 4. Er motivierte damit auch die Einführung komplexen Zahlen.

In der Neuzeit wurde die Theorie der Gleichungen weiter ausgebaut, durch Leonhard Euler, Joseph-Louis Lagrange und insbesondere auch durch Carl Friedrich Gauß, der 1799 den *Fundamentalsatz der Algebra* bewies: jede Polynomgleichung

$$a_n x^n + \cdots + a_1 x + a_0 = 0$$

vom Grad $n \geq 1$ besitzt genau n Lösungen in den komplexen Zahlen.

Um 1830 entwickelte Évariste Galois (1811-1832) die Galoistheorie. Diese kann als der Beginn der modernen Algebra verstanden werden. Galois und unabhängig Niels Henrik Abel lösten das lange offene Problem der Lösung algebraischer Gleichungen von höherem als viertem Grad, wobei man unter Lösung damals die Darstellung durch die üblichen Rechenoperationen und Wurzelausdrücke (Radikale genannt) verstand, indem sie zeigten, dass dies ab dem fünften Grad im Allgemeinen nicht mehr möglich ist (Satz von Abel-Ruffini). Von Galois stammen in diesem Zusammenhang die Anfänge der Gruppentheorie, vor allen Dingen Permutationsgruppen, und Körpertheorie, also endliche Körper, auch Galois-Felder genannt, und Körpererweiterungen. Natürlich kamen dann auch viele weitere algebraische Strukturen hinzu, oft motiviert aus der Zahlentheorie oder Geometrie und anderen Bereichen.

Notationen: Mit \mathbb{N} bezeichnen wir die natürlichen Zahlen $0, 1, 2, \dots$