1 Einführung in die algebraische Denkweise

1.1 Die natürlichen Zahlen

1.1.1 Natürliche Zahlen als endliche Kardinalitäten

Hintergrund zur Motivation

Inhalt in Kurzfassung: Jede natürliche Zahl entspricht einer Klasse untereinander gleichmächtiger endlicher Mengen. Dieser Grundgedanke wird nun mathematisch streng entwickelt.

1.1.2 Bemerkungen zu Induktionsbeweisen

Hintergrund zur Motivation

Inhalt in Kurzfassung: Wir erläutern hier verschiedene Möglichkeiten, wie man das das Induktionsprinzip in Beweisen einsetzen kann.

1.1.3 Axiomatisierung nach Peano

Hintergrund zur Motivation

Inhalt in Kurzfassung: Die wesentlichen Eigenschaften des (unendlichen) Systems $\mathbb{N}$ der natürlichen Zahlen lassen sich durch einige wenige Forderungen erfassen. Hier wird im Wesentlichen (nicht in der Formalisierung) der berühmte Zugang von Peano gewählt. Dass er das Gewünschte leistet, wird durch einen Eindeutigkeitssatz illustriert.

1.1.4 Das von Neumannsche Modell

Hintergrund zur Motivation

Inhalt in Kurzfassung: Ein mengentheoretisches Modell für die Peanoaxiome (siehe vorangegangener Unterabschnitt) wurde von John von Neumann angegeben. Es hat für sich reizvolle Eigenschaften, zeigt aber vor allem, dass die Mengenlehre mindestens so stark ist wie die Peanoarithmetik (in Wahrheit sogar stärker).

1.1.5 Arithmetik und Ordnung der natürlichen Zahlen

Hintergrund zur Motivation

Inhalt in Kurzfassung: In den bisher behandelten Peanoaxiomen war von einer Nachfolgerfunktion die Rede, nicht jedoch von Addition, Multiplikation und Ordnung auf $\mathbb{N}$. Diese Anreicherungen der Struktur sollen nun, wieder auf mengentheoretischer Grundlage, erfolgen. Außerdem werden die wichtigsten Rechenregeln für natürliche Zahlen hergeleitet.

1.1.6 Zifferndarstellung und Normalform

Leicht aber unverzichtbar

Inhalt in Kurzfassung: Für das Operieren mit konkreten Zahlen sind geeignete Formen der Repräsentation wie die übliche Zahlendarstellung zur Basis 10 unabdingbar. Es folgen dazu einige grundsätzliche Überlegungen.

1.2 Zahlenbereichserweiterungen als Beispielgeber

1.2.1 Die ganzen Zahlen

Wesentliches Fundament

Inhalt in Kurzfassung: Die Konstruktion des Systems $\mathbb{Z}$ der ganzen Zahlen kann ausgehend von $\mathbb{N}$ mit rein mengentheoretischen Mitteln erfolgen. Diese Konstruktion ist typisch für die Denkweise in der Algebra und wird sich, bezogen auf die additive Struktur, später (z.B. in der Theorie der Halbgruppen) auch für Verallgemeinerungen eignen.

1.2.2 Die rationalen Zahlen

Wesentliches Fundament

Inhalt in Kurzfassung: Die Konstruktion von des Systems $\mathbb{Q}$ der rationalen Zahlen aus $\mathbb{Z}$ folgt jener von $\mathbb{Z}$ aus $\mathbb{N}$ aus dem vorangegangenen Abschnitt.

1.2.3 Die reellen Zahlen

Wesentliches Fundament

Inhalt in Kurzfassung: Für die dritte große Zahlenbereichserweiterung, nämlich von $\mathbb{Q}$ zu $\mathbb{R}$, sind mehrere Zugänge möglich. In jedem Fall sind aber neue Ideen erforderlich. Hier beschreiten wir den Weg mittels Cauchyfolgen. (Eine alternative Konstruktion mittels Dedekindscher Schnitte wird in 3.5.3 zur Sprache kommen.) Trotz der nun stärker analytischen Aura treten im Zusammenhang mit den Cauchyfolgen aber wieder Aspekte von großem algebraischen Interesse auf (Idealeigenschaft).

1.2.4 Die komplexen Zahlen

Wesentliches Fundament

Inhalt in Kurzfassung: Komplexe Zahlen können in vertrauter Weise als Paare mit Real- und Imaginärteil als Komponenten aufgefasst werden. Sie bilden einen Körper $\mathbb{C}$, für den ein Eindeutigkeitssatz gilt, außerdem der Fundamentalsatz der Algebra. Der hier skizzierte Beweis verlangt keine höheren Hilfsmittel, lediglich den Satz vom Maximum aus der reellen Analysis. Abschließend werden auch noch kurz die Hamiltonschen Quaternionen besprochen.

1.3 Paradigmen aus der Linearen Algebra

1.3.1 Lineare (Un-)Abhängigkeit

Leicht aber unverzichtbar

Inhalt in Kurzfassung: Der Vollständigkeit halber werden einige Grundlagen aus der Linearen Algebra wiederholt. Besonders interessant in Hinblick auf spätere Verallgemeinerungen: der Fortsetzungssatz für lineare Abbildung und die Existenz von Basen.

1.3.2 Das Austauschlemma und seine Konsequenzen

Leicht aber unverzichtbar

Inhalt in Kurzfassung: Für endlich erzeugte Vektorräume hat das Austauschlemma zur Folge, dass je zwei Basen gleich viele Elemente haben. Auch dieses Motiv wird später Verallgemeinerungen ermöglichen (Schlagwort Transzendenzbasen).

1.3.3 Die Klassifikation beliebiger Vektorräume durch ihre Dimension

Wesentliches Fundament

Inhalt in Kurzfassung: Da je zwei Basen eines Vektorraums gleich viele Elemente enthalten, kann deren Anzahl als Definition der Dimension dieses Vektorraums dienen. Es zeigt sich, dass die Vektorräume über einem gegebenen Körper mit dieser Zahl in folgendem Sinne klassifiziert werden können: Zwei Vektorräume sind genau dann isomorph, wenn sie dieselbe Dimension haben.

1.3.4 Die Klassifikation linearer Abbildungen

Hintergrund zur Motivation

Inhalt in Kurzfassung: Nicht nur Vektorräume können in kanonischer Weise – nämlich bezüglich Isomorphie durch die Dimension – klassifiziert werden, sondern auch lineare Abbildungen (Matrizen) – nämlich bezüglich Äquivalenz durch den Rang. Im Falle von

Abbildungen von einem Vektorraum in sich über einem algebraisch abgeschlossenen Körper bietet sich auch noch eine zweite Klassifikation an – nämlich bezüglich Ähnlichkeit durch die Jordansche Normalform. All diese Konzepte sind Wiederholungen aus der Linearen Algebra unter Hervorhebung gewisser für die Algebra charakteristischer Aspekte.

2 Grundbegriffe

2.1 Der logisch-modelltheoretische Rahmen der allgemeinen Algebra

2.1.1 Notation und Terminologie

Leicht aber unverzichtbar

Inhalt in Kurzfassung: Weitgehend bereits aus dem ersten Semester bekannte Grundbegriffe werden der Vollständigkeit halber zusammengestellt und in der Algebra wichtige Eigenschaften und Gesichtspunkte hervorgehoben. Beispiele solcher Grundbegriffe sind: kartesisches Produkt, geordnetes Paar, Relation, Funktion/Abbildung, injektiv, surjektiv, bijektiv, Relationenprodukt mit der Verkettung von Abbildungen als Spezialfall, inverse Relation/Abbildung, (Halb-)Ordnungsrelation, Äquivalenzrelation und Quasiordnung.

2.1.2 Grundbegriffe der Ordnungstheorie

Leicht aber unverzichtbar

Inhalt in Kurzfassung: Von den zahlreichen Begriffen aus der Theorie der Halbordnungen, die im Folgenden eingeführt werden, werden später vor allem vollständige Verbände und die mit ihnen zusammenhängenden Aussagen immer wieder eine wichtige Rolle spielen. Nützlich für die Veranschaulichung von (endlichen) Halbordnungen sind Hassediagramme.

2.1.3 Operationen und universelle Algebren

Wesentliches Fundament

Inhalt in Kurzfassung: Im Zentrum der Algebra stehen algebraische Strukturen, die nun eingeführt werden sollen. Dabei handelt es sich im Mengen zusammen mit Operationen unterschiedlicher Stelligkeit. Interessante Eigenschaften solcher Operationen sind z.B Gesetze (wie etwa Assoziativ-, Kommutativ- oder Distributivgesetz), die Anlass geben zur Definition interessanter Klassen algebraischer Strukturen (wie etwa Gruppen, Ringe oder Körper). Dieser Unterabschnitt bringt einen systematischen Aufbau zahlreicher derartiger Begriffsbildungen.

2.1.4 Relationale Strukturen

Hintergrund zur Motivation

Inhalt in Kurzfassung: Erlaubt man auf Strukturen, wie sie im vorangegangenen Unterabschnitt definiert wurden, zusätzlich Relationen auf der Trägermenge, so erhält man relationale Strukturen. Wichtige Beispiele sind (halb)geordnete (Halb-)Gruppen oder auch Verbände, die man sowohl in einem algebraischen als auch in einem ordnungstheoretischen Sinn auffassen kann.

2.1.5 Homomorphismen zwischen Algebren

Wesentliches Fundament

Inhalt in Kurzfassung: Verallgemeinert man den Begriff der linearen Abbildung zwischen Vektorräumen auf beliebige (universelle) Algebren, so stößt man auf jenen der Homomorphismen. Bei den meisten Abbildungen, die in der Algebra von Interesse sind, handelt es sich um solche.

2.1.6 Strukturverträgliche Abbildungen zwischen relationalen Strukturen

Leicht aber unverzichtbar

Inhalt in Kurzfassung: Will man auch noch den Begriff des Homomorphismus verallgemeinern, nämlich von rein algebraischen auf relationale Strukturen, so bieten sich eine schwächere und eine stärkere Variante an (entspricht Monotonie in eine oder in beide Richtungen), die nun kurz zu besprechen sind.

2.1.7 Klassifikation modulo Isomorphie als Paradigma

Hintergrund zur Motivation

Inhalt in Kurzfassung: Unter dem Gesichtspunkt der Algebra unterscheiden sich zwei isomorphe Strukturen nicht wesentlich. Dieser Gesichtspunkt lässt sogenannte Klassifikationssätze (schwächer: Darstellungssätze) besonders interessant erscheinen. Es geht nun darum, was genau darunter zu verstehen ist.

2.1.8 Terme, Termalgebra, Gesetze und Varietäten

Wesentliches Fundament

Inhalt in Kurzfassung: Ähnlich wie in der Logik ist es in der (universellen) Algebra unausweichlich, auch die formale Sprache zum Gegenstand zu machen. Dazu braucht es strenge Definitionen von scheinbar selbstverständlichen Begriffen wie Term etc. Von herausragendem Interesse ist in diesem Zusammenhang die Termalgebra (über gegebenen Mengen von Variablen und Operationssymbolen) sowie, dass beliebige Variablenbelegungen mit Elementen einer Algebra des entsprechenden Typs zu einem eindeutigen

Homomorphismus auf der Termalgebra, dem sogenannten Einsetzungshomomorphismus fortgesetzt werden können.

2.1.9 Ein kurzer Exkurs in die mathematische Logik

Hintergrund zur Motivation

Inhalt in Kurzfassung: Viele Begriffsbildungen der universellen Algebra werden im Lichte der mathematischen Logik noch besser verständlich. Der vorliegende Unterabschnitt dient dem Zweck, die relevanten Verbindungen herzustellen.

2.1.10 Klone

Ergänzung zum Kernstoff

Inhalt in Kurzfassung: Klone entsprechen der Idee, dass nicht nur einstellige Operationen (Funktionen auf einer Menge) durch Verkettung zu Halbgruppen zusammengesetzt werden können, sondern auch mehrstellige Operationen (Funktionen in mehreren Variablen) ineinander eingesetzt werden können. Die bezüglich dieser Operation abgeschlossenen Systeme (die außerdem die sogenannten Projektionen enthalten) nennt man Klone. Der folgende Unterabschnitt soll einen ersten beschiedenen Eindruck von der Theorie der Klone geben.

2.2 Der kategorientheoretische Rahmen

2.2.1 Kategorien

Leicht aber unverzichtbar

Inhalt in Kurzfassung: Dem Begriff der Kategorie liegt die Idee zugrunde, dass es von Interesse ist, Strukturen gleichen Typs (seien es algebraische, relationale, topologische etc.) als sogenannte Objekte zu einer Klasse zusammenzufassen und die strukturverträglichen Abbildungen (Morphismen) zwischen je zwei solchen Objekten zu betrachten. Die formale Definition einer Kategorie ist extrem allgemein und Gegenstand dieses Unterabschnitts.

2.2.2 Beispiele von Kategorien

Leicht aber unverzichtbar

Inhalt in Kurzfassung: Varietäten sind wichtige Beispiele von Kategorien. Von anderer Art aber gleichfalls von Interesse ist, dass man auch Graphen als Kategorien auffassen kann. Grob gesagt sind die Knoten die Objekte der Kategorie, Kanten sind (gewisse) Morphismen.

2.2.3 Universelle Objekte und ihre Eindeutigkeit

Wesentliches Fundament

Inhalt in Kurzfassung: Der einzige rein kategorientheoretische Satz, den wir später verwenden werden (das dafür sehr häufig), besagt, dass universelle (genauer: initiale und terminale) Objekte einer Kategorie bis auf Äquivalenz eindeutig bestimmt sind. Die Definition all dieser Begriffe sowie der (kurze aber sehr typische) Beweis dieses Satzes sind die Hauptinhalte dieses Unterabschnitts.

2.2.4 Funktoren

Ergänzung zum Kernstoff

Inhalt in Kurzfassung: Funktoren zwischen Kategorien spielen ziemlich genau die Rolle, die Homomorphismen zwischen Algebren desselben Typs spielen. Allerdings sind ko- von kontravarianten Funktoren zu unterscheiden. Wir werden wenig Gebrauch von Funktoren machen. Von zentraler Bedeutung sind sie in Gebieten wie etwa der Algebraischen Topologie. Da werden topologischen Räumen und stetigen Abbildungen durch Funktoren in verträglicher und sehr effektiver Weise gewisse algebraische Strukturen und Homomorphismen zugeordnet. Hier begnügen wir uns mit sehr einfachen Beispielen von Funktoren.

2.2.5 Kommutative Diagramme als Funktoren

Ergänzung zum Kernstoff

Inhalt in Kurzfassung: Kommutative Diagramme sind graphische Darstellungen dafür, dass verschiedene Verkettungen gewisser Abbildungen übereinstimmen. Situationen, wo es genau darum geht, sind in der Algebra ubiquitär. Sehr reizvoll ist die Einsicht, dass derartige Konstellationen auch in der Sprache der Kategorien und Funktoren, angewandt auf Kategorien von Graphen ausgedrückt werden können.

2.2.6 Natürliche Transformationen

Ergänzung zum Kernstoff

Inhalt in Kurzfassung: Stehen zwei Funktoren in einer Beziehung, die durch ein bestimmtes kommutatives Diagramm dargestellt werden kann, stößt man schnell auf den Begriff der natürlichen Transformation zwischen zwei Funktoren. Hier berühren wir diesen Themenkreis nur sehr oberflächlich. Wir werden diese Konzepte später nicht mehr brauchen. Dieser Abschnitt wurde hier lediglich deshalb aufgenommen, um die vorliegende Darstellung einiger Grundbegriffe der Kategorientheorie etwas abzurunden.

2.3 Elemente algebraischer Strukturanalyse

2.3.1 Unteralgebren und Erzeugnisse

Wesentliches Fundament

Inhalt in Kurzfassung: In Verallgemeinerung des Begriffs des Unterraums eines Vektorraums sind Unteralgebren einer Algebra genau das, was man sich erwartet: Teilmengen, auf die eingeschränkt wieder eine Algebra desselben Typs vorliegt. Sehr schnell überzeugt man sich: Der Durchschnitt von Unteralgebren ist wieder eine Unteralgebra. Daraus folgt, dass sämtliche Unteralgebren einer gegebenen Algebra bezüglich der Inklusion einen vollständigen Verband bilden. Insbesondere gibt es zu jeder Teilmenge eine kleinste umfassende Unteralgebra, das sogenannte Erzeugnis dieser Teilmenge. Ein häufig verwendetes Ergebnis besagt, dass zwei Homomorphismen, die auf einer Teilmenge übereinstimmen, auch auf deren Erzeugnis übereinstimmen.

2.3.2 Direkte Produkte

Wesentliches Fundament

Inhalt in Kurzfassung: Liegt eine Familie von Algebren des gleichen Typs vor, so trägt das kartesische Produkt ihrer Trägermengen eine natürliche algebraische Struktur desselben Typs. Man spricht vom direkten Produkt der Algebren. Direkte Produkte zeichnen sich durch eine universelle Eigenschaft aus, in der die sogenannten Projektionen vom direkten Produkt in die einzelnen Komponenten eine zentrale Rolle spielen.

2.3.3 Homomorphe Bilder, Kongruenzrelationen und Faktoralgebren

Wesentliches Fundament

Inhalt in Kurzfassung: So wie dem Konzept der Teilmenge einer Menge in der Algebra das Konzept der Unteralgebra entspricht, dem des kartesischen Produktes das direkte Produkt, so entsprechen den Konzepten Äquivalenzrelation und Partition in der Algebra jene von Kongruenzrelation bzw. Faktoralgebra. Eine wichtige Rolle spielen dabei auch Homomorphismen, insbesondere der kanonische Homomorphismus. Dies kommt im Homomorphiesatz zum Ausdruck. Sämtliche Kongrunezrelationen einer gegebenen Algebra bilden einen vollständigen Verband (sehr ähnlich wie auch die Unteralgebren). Die klassischen Beispiele sind die Kongruenzen ganzer Zahlen modulo einer natürlichen Zahl mit den Restklassenringen als Faktoralgebren. Zwei Partitionen induzieren immer auch Faktoralgebren: die einelementige Partition und jene aus ausschließlich einelementigen Klassen. Entsprechend sind die zugehörigen Äquivalenzrelationen stets auch Kongruenzrelationen, die sogenannten trivialen. Eine Algebra, die außer den trivialen Kongruenzrelationen keine weiteren besitzt, heißt einfach.

2.3.4 Direkte Limiten

Ergänzung zum Kernstoff

Inhalt in Kurzfassung: Zu jeder Familie von Mengen gibt es die Vereinigungsmenge. Hat man es jedoch mit algebraischen Strukturen zu tun, so bildet die Vereinigung ihrer Regel keine natürliche algebraische Struktur. Sehr wohl lässt sich eine solche aber unter zusätzlichen Voraussetzungen definieren, zum Beispiel in Varietäten, sofern die Algebren in einer verträglichen Weise ineinander eingebettet sind. Die resultierende Struktur zeichnet sich durch eine universelle Eigenschaft aus.

2.3.5 Triviale und nichttriviale Varietäten

Leicht aber unverzichtbar

Inhalt in Kurzfassung: Für Varietäten gilt eine bemerkenswerte Dichotomie. Und zwar enthält eine Varietät entweder nur höchstens einelementige Algebren und eventuell die leere Algebra (trivialer Fall) oder Algebren beliebig großer Kardinalität.

2.3.6 Isomorphiesätze

Ergänzung zum Kernstoff

Inhalt in Kurzfassung: In den beiden Isomorphiesätzen geht es vor allem darum, dass verschiedene Konstruktionen zu isomorphen Strukturen führen. Im ersten wird die Reihenfolge der Bildung einer Unter- und einer Faktoralgebra vertauscht; im zweiten werden zwei Faktorisierungen durch eine einzige ersetzt. Der zweite besagt darüber hinaus die Isomorphie des Kongruenzverbandes der ersten Faktoralgebra mit einem Teilintervall des Kongruenzverbandes der ursprünglichen Algebra.

3 Elementare Strukturtheorien

3.1 Halbgruppen und Monoide

3.1.1 Potenzen und Inverse

Leicht aber unverzichtbar

Inhalt in Kurzfassung: Wir beginnen die Halbgruppentheorie mit einfachen Konzepten, die weitgehend aus der elementaren Arithmetik in den Zahlbereichen vertraut sind. Die Tatsache, dass Inverse nicht zu allen Elementen eines Monoids existieren, führt zum Begriff der Einheiten, die stets eine Untergruppe bilden und auch in späteren Kapiteln eine wichtige Rolle spielen werden. Die üblichen Rechenregeln für Potenzen gelten allgemeiner in Halbgruppen bzw. in kommutativen Halbgruppen und zeigen überdies, dass sich jede abelsche Gruppe in natürlicher Weise auch als $\mathbb{Z}$-Modul auffassen lässt.

3.1.2 Wichtige Beispiele von Halbgruppen

Wesentliches Fundament

Inhalt in Kurzfassung: Als wichtigste Beispiele von Halbgruppen bzw. Monoiden werden das freie und das symmetrische Monoid samt Darstellungssatz von Cayley ausführlicher besprochen.

3.1.3 Algebraische Strukturanalyse auf $\mathbb{N}$

Wesentliches Fundament

Inhalt in Kurzfassung: Wir geben einen ersten Beweis von der Eindeutigkeit der Primfaktorzerlegung natürlicher Zahlen und deuten diesen als Struktursatz: Das multiplikative Monoid auf $\mathbb{N}^+$ ist isomorph zur direkten Summe abzählbar unendlich vieler Kopien des additiven Monoids auf $\mathbb{N}$. Ein damit verwandter Struktursatz beschreibt den vollständigen Verband, der durch die Teilerrelation auf $\mathbb{N}$ gegeben ist. Für spätere Zwecke wird auch die Division mit Rest auf $\mathbb{N}$ und $\mathbb{Z}$ bereitgestellt.

3.1.4 Quotienten- bzw. Differenzenmonoid

Hauptziel der Vorlesung

Inhalt in Kurzfassung: Hat man die Konstruktion der additiven Gruppe $\mathbb{Z}$ aus der Halbgruppe $\mathbb{N}$ vor Augen, so stellt sich die Frage, unter welchen Bedingungen sich diese Konstruktion von $\mathbb{N}$ auf beliebige Halbgruppen bzw. Monoide M verallgemeinern lässt. Wie

man sich schnell überzeugt, ist für die Existenz von Inversen eines Halbgruppenelements dessen Kürzbarkeit notwendig. Ist diese für alle Elemente gegeben, so ist Kommutativität hinreichend (nicht notwendig) für die Existenz einer Erweiterung zu einer Gruppe, der sogenannten Quotienten- oder (bei additiver Notation) Differenzengruppe. Varianten dieser Konstruktion betreffen die Möglichkeit, Inverse nicht für alle Elemente, sondern nur für jene aus einem regulären Untermonoid zu fordern. Die resultierenden Strukturen lassen sich auch durch eine universelle Eigenschaft charakterisieren, nämlich als initiale Objekte in einer geeigneten Kategorie.

3.2 Gruppen

3.2.1 Nebenklassenzerlegung

Wesentliches Fundament

Inhalt in Kurzfassung: Jede Untergruppe induziert zwei Partitionen der Gruppe, nämlich in Links- und in Rechtsnebenklassen, von denen jeweils eine die Untergruppe selbst ist. Alle Nebenklassen haben die gleiche Mächtigkeit wie die Untergruppe, und es gibt gleich viele Links- wie Rechtsnebenklassen. Deren Anzahl nennt man den Index der Untergruppe in der Gruppe. Offensichtlich folgt: Die Ordnung (= Kardinalität) der Gruppe ist das Produkt aus der Ordnung der Untergruppe und dem Index. Daraus ergibt sich für endliche Gruppen der Satz von Lagrange: Die Ordnung einer Untergruppe ist Teiler der Ordnung der Gruppe.

3.2.2 Faktorgruppen und Normalteiler

Wesentliches Fundament

Inhalt in Kurzfassung: Im Zusammenhang mit Kongruenzrelationen und Faktoralgebren ist bei Gruppen eine Beobachtung zentral: Kennt man die Kongruenzklasse des neutralen Elementes, so kennt man die gesamte Partition (Kongruenzrelation). Deshalb spielen jene Teilmengen von Gruppen eine besondere Rolle, die als Kongruenzklassen des neutralen Elements auftreten. Sie heißen Normalteiler und sind dadurch charakterisiert, dass es sich bei ihnen um Untergruppen handelt, für die überdies Links- und Rechtsnebenklassenzerlegung übereinstimmen oder, äquivalent, die invariant bezüglich sämtlicher innerer Automorphismen sind. Zahlreiche interessante Sachverhalte lassen sich mit Hilfe von Normalteilern einfach formulieren. Wichtige Beispiele dafür sind die Isomorphiesätze. Der vorliegende Unterabschnitt bringt aber auch einige andere einfache Sachverhalte, die in der Gruppentheorie immer wieder nützlich sind.

3.2.3 Direkte Produkte von Gruppen

Wesentliches Fundament

Inhalt in Kurzfassung: Im Gegensatz zum allgemeinen Fall direkter Produkte treten bei Gruppen die einzelnen Faktoren nicht nur als homomorphe Bilder, sondern auch als Unterstrukturen auf. Somit ergibt sich umgekehrt die Frage, ob eine gegebene Gruppe als direktes Produkt gewisser Untergruppen gedeutet werden kann. Die Ergebnisse dieses Unterabschnitts beschäftigen sich mit dieser und ähnlichen Fragen, vorwiegend für den Fall endlich vieler Komponenten.

3.2.4 Zyklische Gruppen

Wesentliches Fundament

Inhalt in Kurzfassung: Eine Gruppe heißt zyklisch, wenn sie von einem Element erzeugt wird. Die additive Gruppe $\mathbb{Z}$ der ganzen Zahlen ist bis auf Isomorphie die einzige unendliche zyklische Gruppe. Darüber hinaus gibt es zu jedem positiven $n \in \mathbb{N}$ bis auf Isomorphie genau eine zyklische Gruppe dieser Ordnung und keine weiteren. Jede zyklische Gruppe lässt sich als homomorphes Bild von $\mathbb{Z}$ realisieren (Restklassengruppen modulo n). Im vorliegenden Unterabschnitt werden diese und einige weitere Strukturaussagen über zyklische Gruppen hergeleitet. Eine Folgerung, die auch in anderem Zusammenhang immer wieder eine Rolle spielen wird, betrifft ganzzahlige Linearkombinationen zweier ganzer Zahlen: Ihre Werte sind genau die Vielfachen des größten gemeinsamen Teilers dieser Zahlen.

3.2.5 Permutationsgruppen

Hauptziel der Vorlesung

Inhalt in Kurzfassung: Die große Bedeutung von Permutationsgruppen für die gesamte Gruppentheorie ergibt sich aus dem Darstellungssatz von Cayley: Jede Gruppe ist isomorph zu einer Untergruppe der symmetrischen Gruppe auf ihrer Trägermenge, also zu einer Gruppe von Permutationen (= Permutationsgruppe). Dies allein rechtfertigt ein etwas ausführlicheres Studium von Permutationsgruppen, es ergeben sich aber darüber hinaus einige weitere reizvolle Aspekte. Einiges aus diesem Unterabschnitt dürfte schon aus dem Kapitel über Determinanten aus der Linearen Algebra bekannt sein, insbesondere die Unterscheidung zwischen geraden und ungeraden Permutationen.

3.2.6 Symmetrie

Ergänzung zum Kernstoff

Inhalt in Kurzfassung: Der Begriff der Symmetrie hat eindeutig geometrischen Ursprung. Die adäquate mathematische Fassung dieses Phänomens fußt jedoch auf dem Gruppenbegriff. Im vorliegenden, letzten Unterabschnitt zur elementaren Gruppentheorie wird das ausblicksartig beleuchtet, vorwiegend unter historischen Gesichtspunkten und völlig ohne technische Beweise neuer Resultate.

3.3 Ringe

3.3.1 Kongruenzrelationen und Ideale

Wesentliches Fundament

Inhalt in Kurzfassung: Ideale spielen in der Ringtheorie die völlig analoge Rolle wie Normalteiler in der Gruppentheorie. Entsprechend folgt der vorliegende Unterabschnitt auch ganz analogen Gesichtspunkten wie jener aus der Gruppentheorie über Normalteiler (3.2.2). Betrachtet man einen Ring als Links- bzw. Rechtsmodul über sich selbst, so stößt man analog auf Links- bzw. Rechtsideale

3.3.2 Ideale in kommutativen Ringen mit 1

Wesentliches Fundament

Inhalt in Kurzfassung: Unter den kommutativen Ringen mit 1 spielen die Integritätsbereiche und Körper eine besondere Rolle, die sich durch Faktorisierung nach Prim- bzw. maximale Ideal ergeben. Im endlichen Fall ist jeder Integritätsbereich sogar ein Körper. Generell sind Körper unter den kommutativen Ringen mit 1 genau die einfachen (die also nur die trivialen Ideale enthalten).

3.3.3 Charakteristik

Leicht aber unverzichtbar

Inhalt in Kurzfassung: So wie $\mathbb{Z}$ haben auch alle endlichen zyklische Gruppen mit Ordnungen $n \in \mathbb{N}^+$ neben der additiven auch eine multiplikative Struktur, die sie zu kommutativen Ringen mit 1 machen. Jeder kommutative Ring mit 1 enthält die Kopie genau eines dieser Ringe als Unteralgebra. Ist dies $\mathbb{Z}$, so definiert man die Charakteristik des Ringes als 0, sonst als das entsprechende n. Dies drückt sich auch dadurch aus, dass $\mathbb{Z}$ ein initiales Objekt in der Kategorie der kommutativen Ringe mit 1 ist. Die Charakteristik eines Integritätsbereichs ist stets entweder 0 oder eine Primzahl.

3.3.4 Die binomische Formel

Leicht aber unverzichtbar

Inhalt in Kurzfassung: Die aus der elementaren Arithmetik bekannte binomische Formel für die Potenz einer Summe gilt allgemeiner in beliebigen kommutativen Ringen mit 1. Besonders einfache Gestalt nimmt diese Formel an, wenn die Charakteristik des Ringes eine Primzahl ist und der Exponent eine Potenz dieser Primzahl. In diesem Fall ist das Potenzieren nämlich ein Homomorphismus nicht bezüglich der Multiplikation, sondern auch bezüglich der Addition. Die wird in der Theorie endlicher Körper noch eine wichtige Rolle spielen.

3.3.5 Quotientenkörper

Hauptziel der Vorlesung

Inhalt in Kurzfassung: Wendet man die Konstruktion der Quotientengruppe aus einem regulären kommutativen Monoid (siehe 3.1.4) auf die multiplikative Struktur eines Integritätsbereich an, so entspricht dies dem Übergang von ganzen Zahlen zu Brüchen. So wie dort (d.h. beim elementaren Bruchrechnen) kann im allgemeinen Fall ebenfalls auch die additive Struktur ausgedehnt werden, so dass man einen Körper (den Quotientenkörper des Integritätsbereichs erhält. Auch die Beschränkung auf reguläre multiplikative Teilmengen als zugelassene „Nenner“ ist möglich. Die abstrakte Definition der resultierenden Objekts erfolgt als initiales Objekt in einer geeigneten Kategorie, legt die Struktur daher bis auf Äquivalenz (insbesondere also bis auf Isomorphie) eindeutig fest.

3.3.6 Polynome und formale Potenzreihen

Wesentliches Fundament

Inhalt in Kurzfassung: Formale Potenzreihen über einem kommutativen Ring R mit 1 (d.h. mit Koeffizienten aus R) sind durch die Folge ihrer Koeffizienten gegeben, können daher als eben diese Folgen definiert werden. In üblicher Weise kann die Menge $R[[x]]$ aller formalen Potenzreihen sie sowohl mit einer additiven als auch mit einer multiplikativen Struktur (gliedweise bzw. Cauchyprodukt) ausgestattet werden. Offenbar enthält $R[[x]]$ auch den Ring $R[x]$ aller Polynome über R (nur endlich viele Koeffizienten $\neq 0$). Ist R ein Integritätsbereich, so auch $R[[x]]$ und $R[x]$, und es kann der Quotientenkörper von $R[[x]]$ gebildet werden. Dieser lässt sich als Ring $R[[[x]]]$ der formalen Laurentreihen auffassen, die auch endlich viele Glieder mit negativen Potenzen enthalten dürfen. Durch Iteration des Übergangs von R zu $R[x]$ lassen sich auch Polynomringe in mehreren Variablen bilden. Polynomringe zeichnen sich durch eine universelle Eigenschaft aus, die in 4.2.3 noch näher beleuchtet werden wird.

3.3.7 Der Chinesische Restsatz

Nebenziel der Vorlesung

Inhalt in Kurzfassung: Darstellungen als direkte Produkte spielen bei Ringen keine so große Rolle wie bei Gruppen. Von Interesse ist aber immerhin der Chinesische Restsatz. Er wird zunächst in einer allgemeinen, dann in seiner klassischen Fassung gebracht.

3.3.8 Beispiele nichtkommutativer Ringe

Nebenziel der Vorlesung

Inhalt in Kurzfassung: Die wichtigsten Beispiele nichtkommutativer Ringe entstehen als Endomorphismenringe von abelschen Gruppen oder von Moduln. Wir begnügen uns mit

einer sehr kurzen Präsentation.

3.4 Moduln, insbesondere abelsche Gruppen

3.4.1 Unter- und Faktormoduln, Homomorphismen und direkte Summen

Nebenziel der Vorlesung

Inhalt in Kurzfassung: Diese grundlegenden Konstruktionen für Moduln verlaufen weitgehend analog zur Situation bei (abelschen) Gruppen bzw. bei Vektorräumen aus der Linearen Algebra. Technisch treten dabei keine nennenswerten Neuigkeiten auf.

3.4.2 Schwache Produkte – direkte Summen

Nebenziel der Vorlesung

Inhalt in Kurzfassung: Schwache direkte Produkte oder direkte Summen lassen sich im Kontext von Moduln als Unteralgebren der direkten Produkte deuten. Und zwar enthalten sie nur die Elemente mit endlichem Träger. Wichtig sind direkte Summen vor allem aufgrund einer universellen Eigenschaft als initiales Objekt einer geeigneten Kategorie. (Im Gegensatz dazu ist das volle direkte Produkt ein terminales Objekt.) Das wird uns in Gestalt von Koprodukten in 4.2 wieder begegnen.

3.4.3 Abelsche Gruppen als Moduln über $\mathbb{Z}$ und $\mathbb{Z}_m$

Nebenziel der Vorlesung

Inhalt in Kurzfassung: Die übliche Notation für additive Potenzen zusammen mit den elementaren Potenzrechenregeln aus 3.1.1 zeigt unmittelbar, dass jede abelsche Gruppe in natürlicher Weise auch ein Modul über dem Ring $\mathbb{Z}$ ist. In diesem Zusammenhang werden für abelsche Gruppen auch Begriffe wie Torsionselement, Torsionsanteil, p-Element ($p \in \mathbb{P}$), Exponent u.ä. definiert.

3.4.4 Zerlegung von Torsionsgruppen in ihre p-Anteile

Hauptziel der Vorlesung

Inhalt in Kurzfassung: Technische Vorüberlegungen zur Ordnung von Elementen in abelschen Gruppen zielen auf das Hauptergebnis dieses Unterabschnitts ab: Jede Torsionsgruppe ist die direkte Summe ihrer p-Komponenten. Abschließend wird dieser Satz auf die universelle Prüfergruppe und ihre p-Anteile, die p-Prüfergruppen angewendet.

3.4.5 Endliche abelsche Gruppen

Hauptziel der Vorlesung

Inhalt in Kurzfassung: Im Falle endlicher abelscher Gruppen führt die Zerlegung in ihre p-Anteile zum Hauptsatz, wonach eine direkte Zerlegung in zyklische Gruppen möglich ist. Allerdings muss man zuvor die entsprechende Aussage für Gruppen von Primzahlpotenzordnung beweisen.

3.4.6 Abelsche Gruppen als Moduln über ihrem Endomorphismenring

Nebenziel der Vorlesung

Inhalt in Kurzfassung: Beispiele von Moduln über nichtkommutativen Ringen erhält man sehr natürlich aus 3.3.8, nämlich abelsche Gruppen als Moduln über ihrem eigenen Endomorphismenring.

3.5 Geordnete Gruppen und Körper

3.5.1 Grundlegende Definitionen

Leicht aber unverzichtbar

Inhalt in Kurzfassung: So wie in den reellen Zahlen das Monotoniegesetz für Addition (eingeschränkt auch für die Multiplikation) gilt, treten auch allgemeinere relationale Strukturen auf, wo Verträglichkeitsbedingungen für Operationen und Relationen gelten. Beispiele sind geordnete Gruppen u.ä.

3.5.2 Geordnete Gruppen

Leicht aber unverzichtbar

Inhalt in Kurzfassung: Unter den geordneten abelschen Gruppen sind die archimedisch angeordneten insofern von besonderem Interesse, als es dabei bis auf Isomorphie genau um die additiven Untergruppen von $\mathbb{R}$ handelt.

3.5.3 Angeordnete Körper und nochmals $\mathbb{R}$

Nebenziel der Vorlesung

Inhalt in Kurzfassung: Wir beginnen mit der bereits in 1.2.3 angekündigten Konstruktion der reellen Zahlen mittels Dedekindscher Schnitte. Bis auf Isomorphie ist $\mathbb{R}$ eindeutig bestimmt durch die Eigenschaften eines vollständig angeordneten Körpers. Dies zu beweisen ist das Ziel. Das wichtigsten Zwischenergebnis auf diesem Weg sind auch für sich bemerkenswert. Sie lauten: Jeder vollständig angeordnete Körper ist archimedisch angeordnet. Jeder archimedisch angeordnete Körper lässt sich (sogar auf eindeutige Weise) in

$\mathbb{R}$ einbetten. Abschließend wird der Körper der gebrochen rationalen Funktionen über $\mathbb{Q}$.

3.5.4 Modelltheoretische Bemerkungen

Ergänzung zum Kernstoff

Inhalt in Kurzfassung: Andeutungen in Richtung Logik und Entscheidbarkeit der Theorie reell abgeschlossener Körper.

3.6 Verbände und Boolesche Algebren

3.6.1 Elementare Eigenschaften

Leicht aber unverzichtbar

Inhalt in Kurzfassung: Einfachste Begriffe, Rechenregeln und Beispiele zu Verbänden.

3.6.2 Unterverbände

Leicht aber unverzichtbar

Inhalt in Kurzfassung: Der Begriff des Unterverbandes fügt sich nahtlos in das allgemeinere Konzept der Unteralgebra ein.

3.6.3 Kongruenzrelationen; Filter und Ideale

Leicht aber unverzichtbar

Inhalt in Kurzfassung: Kongruenzrelationen auf Verbänden haben auch ordnungstheoretisch interessante Eigenschaften. So sind die Kongruenzklassen stets konvexe Unterverbände. Eine besondere Rolle spielen Filter und noch spezieller Primfilter und maximale Filter (Ultrafilter). Dual zu Filtern definiert man Ideale (im ordnungs- oder verbandstheoretischen Sinn), Primideale und maximale Ideale.

3.6.4 Vollständige Verbände

Leicht aber unverzichtbar

Inhalt in Kurzfassung: Wiederholung des Begriffs des vollständigen Verbands.

3.6.5 Distributive und modulare Verbände

Leicht aber unverzichtbar

Inhalt in Kurzfassung: Zwei wichtige Teilklassen innerhalb der Verbände bilden die modularen und, noch spezieller, die distributiven. Es folgen die Definitionen und einfachste

Beispiele dazu mit Übungen.

3.6.6 Boolesche Ringe

Leicht aber unverzichtbar

Inhalt in Kurzfassung: Boolesche Ringe sind Ringe mit 1, in denen die Multiplikation idempotent ist. Sie entsprechen in bijektiver Weise den Booleschen Algebren mit derselben Trägermenge. Dieser Zusammenhang ermöglicht es, Konzepte und Ergebnisse aus der Ringtheorie auf Boolesche Algebren zu übertragen,

3.6.7 Einfache Rechenregeln

Leicht aber unverzichtbar

Inhalt in Kurzfassung: Das Dualitätsprinzip macht sich zunutze, dass die Menge der definierenden Gesetze für Boolesche Algebren (analog für Verbände) in sich selbst übergeht, wenn man $\vee$ und $\wedge$ sowie 0 und 1 vertauscht. Auch die übrigen Ergebnisse dieses Unterabschnitts folgen sehr schnell aus der Definition Boolescher Algebren.

3.6.8 Atome

Leicht aber unverzichtbar

Inhalt in Kurzfassung: Atome in Booleschen Algebren sind definitionsgemäß obere Nachbarn der 0. Der Stronesche Darstellungssatz für endliche Boolesche Algebren besagt, dass jede solche isomorph ist zur Potenzmengenalgebra über der Menge ihrer Atome. Die allgemeinere Version dieses Satzes folgt dann in 3.6.9.

3.6.9 Der Darstellungssatz von Stone

Nebenziel der Vorlesung

Inhalt in Kurzfassung: Der Darstellungssatz von Stone in seiner allgemeinen Formulierung besagt, dass sich jede Boolesche Algebra in eine Potenzmengenalgebra einbetten lässt. Die Menge, deren Potenzmenge hier auftritt, ist die Menge aller Ultrafilter in der gegebenen Booleschen Algebra. Die Beweismethode ist insofern sehr lehrreich, als ähnliche Methoden in verschiedenen Teilgebieten der Mathematik auftreten. Aus dem Darstellungssatz kann u.a. die sehr bemerkenswerte Aussage gefolgert werden, dass jedes Gesetz, das in der zweielementigen Booleschen Algebra gilt, automatisch in allen Booleschen Algebren gilt.

4 Universelle Konstruktionen in Varietäten

4.1 Freie Algebren und der Satz von Birkhoff

4.1.1 Motivation

Hintergrund zur Motivation

Inhalt in Kurzfassung: Motivation des Satzes von Birkhoffs, des Hauptergebnisses dieses Abschnitts.

4.1.2 Bekannte Beispiele und Definition einer freien Algebra

Hauptziel der Vorlesung

Inhalt in Kurzfassung: Der aus der Linearen Algebra bekannte Satz von der linearen Fortsetzbarkeit von Abbildungen, die zunächst nur auf einer Basis eines Vektorraums definiert sind, die bereits in 3.1.2 behandelte freie Halbgruppe und die universelle Eigenschaft der Termalgebra aus 2.1.8.1 sind Beispiele für ein uns denselben allgemeinen Begriff: den der freien Algebra. Die Definition ist sowohl in der Sprache der universellen Algebra als auch, noch allgemeiner, in jener der Kategorientheorie (freies Objekt) möglich. Freie Objekte in einer Kategorie sind aufgrund ihrer Definition initiale Objekte in einer geeignet angepassten anderen Kategorie. Daraus folgt, dass sie bis auf Isomorphie eindeutig bestimmt sind. Der Unterabschintt schließt mit einigen einfachen Beispielen, meist in Form von Übungsaufgaben.

4.1.3 Die freie Algebra als homomorphes Bild der Termalgebra

Hauptziel der Vorlesung

Inhalt in Kurzfassung: Für uns mit Abstand am wichtigsten sind freie Algebren innerhalb von Varietäten. Sie existieren immer und können ziemlich anschaulich verstanden werden als Termalgebren, wobei allerdings manche Terme identifiziert werden, und zwar genau dann, wenn sie stets dieselben Elemente darstellen. Abstrakt formuliert: Die freie Algebra ist ein homomorphes Bild der Termalgebra mit einem Kern, der sich als Durchschnitt aller möglichen Kerne in irgendwelche Algebren der Varietät ergibt. Erwas anders und ungenau gesprochen: In der freien Algebra gelten genau jene Gesetze, die in allen Algebren und für alle Elemente der Varietät gelten.

4.1.4 Die freie Gruppe

Nebenziel der Vorlesung

Inhalt in Kurzfassung: Freie Gruppen spielen nicht nur unter den Gesichtspunkten der Universellen Algebra eine wichtige Rolle, sondern treten auch in anderen mathematischen Zusammenhängen auf, beispielsweise in der algebraischen Topologie als Fundamentalgruppen oder im Paradoxon von Hausdorff-Banach-Tarski. Die Elemente freier Gruppen stellt man sich am besten als „reduziert“ Gruppenwörter vor, d.h. als Ausdrücke wie $x^2y^{-1}x^5$, d.h. als Zeichenfolgen, in denen Potenzen der frei erzeugenden Variablen so aneinandergefügt sind, dass keine Kürzungen mehr möglich sind. Eine sorgfältige Durchführung dieser Konstruktion ist Hauptgegenstand dieses Unterabschnitts.

4.1.5 Die freie Boolesche Algebra

Ergänzung zum Kernstoff

Inhalt in Kurzfassung: Nun wird für Boolesche Algebren das analoge Ziel verfolgt wie zuletzt für Gruppen. Wir geben eine Beschreibung freier Boolescher Algebren als Mengenalgebren. Anwendungen haben sie beispielsweise in Aussagenlogik.

4.1.6 Die freie Algebra als subdirektes Produkt

Nebenziel der Vorlesung

Inhalt in Kurzfassung: Die Konstruktion der freien Algebra innerhalb einer Varietät als homomorphes Bild der Termalgebra aus 4.1.3 ergänzen wir nun durch eine zweite Konstruktion, nämlich als subdirektes Produkt, d.h. als Unteralgebra eines (in der Regel sehr „großen“) direkten Produktes. Diese Konstruktion ist zwar abstrakter und weniger anschaulich als jene mit Hilfe der Termalgebra. Sie hat aber einen entscheidenden Vorteil in Hinblick auf den Beweis des Satzes von Birkhoff im nachfolgenden Unterabschnitt. In der Konstruktion muss man nicht alle Eigenschaften einer Varietät voraussetzen, sondern nur die Abgeschlossenheit bezüglich dreier Konstruktionen, nämlich bezüglich Unteralgebren, direkter Produkte und isomorpher Bilder. Genau das wird hinreichen, um die nichttriviale Implikation im Satz von Birkhoff zu beweisen.

4.1.7 Der Satz von Birkhoff

Nebenziel der Vorlesung

Inhalt in Kurzfassung: Mit dem Beweis des Satzes von Birkhoff, einem der wichtigsten Ergebnisse der Universellen Algebra, erreichen wir nun das erste große Ziel dieses Kapitels.

4.2 Koprodukte und Polynomalgebren

4.2.1 Bekannte Beispiele und Definition des Koproduktes

Wesentliches Fundament

Inhalt in Kurzfassung: Koprodukte in Varietäten ähneln in vielerlei Hinsicht freien Algebren. In beiden Fällen geht es darum, Elemente, die zunächst nichts miteinander zu tun haben, so einer einzigen Algebra der Varietät unterzubringen, dass sie sich im Rahmen gewisser Vorgaben möglichst ungebunden verhalten. Der Unterschied: Bei freien Algebren waren die Elemente völlig ohne Beziehung zueinander, wie Variablen, die nur den Gesetzen der Varietät unterworfen sind. Bei Koprodukten entstammen die Elemente bereits vorgegebenen Algebren der Varietät, wobei die Struktur der beteiligten Algebren möglichst erhalten bleiben soll, Elemente aus derselben Algebra sich also sehr wohl weiterhin als solche verhalten sollen. Tatsächlich ähneln Koprodukte in vielen Varietäten tatsächlich freien Algebren (z.B. Gruppen und Vektorräume). Die allgemeine Definition ist aber kategorientheoretischer Natur, wieder als initiales Objekt in einer geeigneten Kategorie. Als Folgerung sind Koprodukte bis auf Isomorphie eindeutig bestimmt.

4.2.2 Konstruktion des Koproduktes als freie Algebra

Nebenziel der Vorlesung

Inhalt in Kurzfassung: Die bereits in 4.2.1 angedeutete Ähnlichkeit zwischen freien Algebren und Koprodukten schlägt sich auch technisch wieder: In Varietäten existieren Koprodukte uneingeschränkt, und der Beweis dafür lässt sich zurückführen auf die uneingeschränkte Existenz freier Objekte in Varietäten.

4.2.3 Polynomalgebren

Nebenziel der Vorlesung

Inhalt in Kurzfassung: Schon bei der Einführung von Polynomringen im klassischen Sinn in 3.3.6 haben wir eine universelle Eigenschaft festgestellt (siehe Proposition 3.3.6.13), die nun zum Ausgangspunkt für den viel allgemeineren Begriff der Polynomalgebra über einer beliebigen Algebra einer Varietät. Und zwar handelt es sich um die Kombination der beiden wichtigsten Konstruktionen dieses Kapitels, nämlich der freien Algebra und des Koproduktes. Für den Beweis, dass auch Polynomalgebren in Varietäten uneingeschränkt existieren ergibt sich nun mehr oder weniger als Korollar bereits verfügbarer Ergebnissen.

4.2.4 Der Gruppenring und Monoidring als Polynomring

Ergänzung zum Kernstoff

Inhalt in Kurzfassung: Auch beim Gruppenring werden (so wie beim Koprodukt zweier Algebren) zwei Strukturen in eine einzige „verklebt“, so dass man darin beide ursprünglichen möglichst „frei“ wiederfindet. Allerdings handelt es sich diesmal nicht um Algebren des gleichen Typs, sondern, wie der Name andeutet, um eine Verschmelzung aus Gruppe und Ring.

5 Teilbarkeit

5.1 Elementare Teilbarkeitslehre

5.1.1 Der Fundamentalsatz der Zahlentheorie als Paradigma

Hintergrund zur Motivation

Inhalt in Kurzfassung: Erste Überlegungen zur Frage, was bei einer eventuellen Verallgemeinerung des Satzes von der eindeutigen Primfaktorzerlegung in $\mathbb{N}$ auf allgemeinere Situationen zu beachten ist.

5.1.2 Teilbarkeit als Quasiordnung auf kommutativen Monoiden

Leicht aber unverzichtbar

Inhalt in Kurzfassung: Der Begriff der Teilbarkeit wird von $\mathbb{N}$ auf kommutative Monoide verallgemeinert, wo es sich i.a. zwar um keine Halbordnung, immerhin aber um eine Quasiordnung handelt. Die zugehörige Äquivalenzrelation (im Sinne von Satz 2.1.1.11) nennt man Assoziiertheit.

5.1.3 Teilbarkeit in Integritätsbereichen

Leicht aber unverzichtbar

Inhalt in Kurzfassung: Von besonderem Interesse ist Teilbarkeit bezüglich des multiplikativen Monoids in Integritätsbereichen. Zusätzliche Aspekte kommen ins Spiel, weil es in diesem Kontext ja auch noch eine zweite binäre Operation, die Addition gibt, die durch das Distributivgesetz mit der Multiplikation verbunden ist. Als interessante Beispiele kommen quadratische Zahlringe zur Sprache, nämlich Unterringe der komplexen Zahlen, die von $\mathbb{Z}$ und der Wurzel einer quadratfreien ganzen Zahl erzeugt werden.

5.1.4 Teilbarkeit und Hauptideale – prime und irreduzible Elemente

Wesentliches Fundament

Inhalt in Kurzfassung: Die Teilbarkeit von Elementen übersetzt sich in die umgekehrte Inklusionsbeziehung der erzeugten Hauptideale, was besonders in Hauptidealringen (das sind Integritätsbereiche, in denen jedes Ideal ein Hauptideal ist) wirksame Möglichkeiten der Strukturanalyse eröffnet. Eine wichtige Rolle spielen dabei irreduzible und Primelemente. In $\mathbb{Z}$ sind beide Begriffe äquivalent, in beliebigen Integritätsbereichen ist jedes

Primelement irreduzibel, nicht jedoch umgekehrt.

5.2 Faktorielle, Hauptideal- und euklidische Ringe

5.2.1 Faktorielle Ringe

Hauptziel der Vorlesung

Inhalt in Kurzfassung: Faktorielle Ringe sind, so definiert, dass für sie ein Analogon des Satzes von der eindeutigen Primfaktorzerlegung gilt. Präziser lässt sich diese Eigenschaft durch mehrere äquivalente Bedingungen charakterisieren, die ungenau (modulo Assoziiertheit und Reihenfolge von Faktoren und bei Vernachlässigung der 0) durch folgende Schlagworte angedeutet seien: Existenz und Eindeutigkeit von Faktorisierungen in irreduzible Elemente; Existenz von Faktorisierungen in Primelemente; irreduzible Elemente sind prim, und es gilt die Teilerkettenbedingung (d.h. es gibt keine unendlichen echt absteigenden Teilerketten); das multiplikative Monoid ist frei. Der Hauptteil dieses Unterabschnitts ist dem Beweis der Äquivalenz gewidmet. Ordnungstheoretisch gelten, wenig überraschend, für den Teilerverband eines faktoriellen Ringes modulo Assoziiertheit ganz ähnliche Aussagen wie für den Teilerverband von $\mathbb{N}$. Insbesondere gibt es größte gemeinsame Teiler etc.

5.2.2 Hauptidealringe

Hauptziel der Vorlesung

Inhalt in Kurzfassung: Hauptidealringe erweisen sich als faktoriell. Der Beweis erfolgt mit Hilfe des Kriteriums mit der Teilerkettenbedingung. Als Folgerung klärt sich die ordnungstheoretische Struktur des Kongruenz-, d.h. des Idealverbandes eines Hauptidealrings mit Hilfe der bereits aus 5.2.1 bekannten Ergebnisse über den Teilerverband eines faktoriellen Ringes auf sehr befriedigende Weise verstehen. Als Folgerung erhält man den wichtigen, im Falle des Ringes $\mathbb{Z}$ bereits bekannten Satz, dass sich der größte gemeinsame Teiler von Elementen in einem Hauptidealring als Linearkombination dieser Elemente schreiben lässt.

5.2.3 Euklidische Ringe

Hauptziel der Vorlesung

Inhalt in Kurzfassung: Euklidische Ringe sind solche Integritätsbereiche, in denen eine Art Division mit Rest möglich ist. Sehr schnell sieht man, dass es sich dabei um Hauptideal- und somit um faktorielle Ringe handelt. Iterierte Division mit Rest führt zum Euklidischen Algorithmus zur algorithmischen Berechnung des größten gemeinsamen Teilers zweier Ringelemente und darüber hinaus zur Darstellung desselben als Linearkombination. (Später wird das auch eine effektive Berechnung multiplikativer Inverser in endlichen Körpern von Primzahlordnung ermöglichen.) Wichtige Beispiele euklidischer

Ringe: $\mathbb{Z}$, $K[x]$ und $K[[x]]$ (K Körper) und $\mathbb{Z}[i]$, der Ring der ganzen Gaußschen Zahlen.

5.3 Anwendungen und Ergänzungen

5.3.1 Der Quotientenkörper eines faktoriellen Rings

Nebenziel der Vorlesung

Inhalt in Kurzfassung: Ist ein Integritätsbereich sogar ein faktorieller oder gar Euklidischer Ring, so wird das Rechnen im Quotientenkörper besonders übersichtlich, weil dort jedes Element als Bruch gekürzte Darstellungen hat, unter denen bei Vorliegen einer sogenannten Normierungsvorschrift sogar eine Normalform ausgezeichnet werden kann. Das wichtigste Beispiel (neben dem Ring $\mathbb{Z}$ und seinem Quotientenkörper $\mathbb{Q}$) ist der Polynomring über einem Körper mit dem Körper der gebrochen rationalen Funktionen als Quotientenring.

5.3.2 Polynomringe über faktoriellen Ringen sind faktoriell

Hauptziel der Vorlesung

Inhalt in Kurzfassung: Dieser Unterabschnitt steht gänzlich im Zeichen des Beweises folgenden Satzes von Gauß: Der Polynomring über einem faktoriellen Ring ist wieder faktoriell.

5.3.3 Faktorisierung von Polynomen

Wesentliches Fundament

Inhalt in Kurzfassung: Aus der Polynomdivision mit Rest folgt sehr schnell: Ein Polynom ist genau dann durch einen Linearfaktor mit Nullstelle α teilbar, wenn es selbst α als Nullstelle hat. Daraus ergibt sich eine Verschärfung des Fundamentalsatzes der Algebra: Jedes komplexe Polynom lässt sich in Linearfaktoren zerlegen. Daraus lässt sich folgern, dass jedes reelle Polynom in Linear- und quadratische Faktoren zerfällt. Das Ende des Unterabschnitts bildet die bekannte Lösungsformel für quadratische Gleichungen und ein kurzer Ausblick auf die Frage nach Lösungsformeln für Gleichungen höheren Grades (Schlagwort Galoistheorie, Kapitel 9).

5.3.4 Symmetrische Polynome

Ergänzung zum Kernstoff

Inhalt in Kurzfassung: Ein Polynom oder eine gebrochen rationale Funktion in mehreren Variablen heißt symmetrisch, wenn es invariant bleibt unter allen Permutationen der Variablen. Einfache Beispiele symmetrischer Polynome sind die elementarsymmetrischen.

Der Hauptsatz über symmetrische Polynome besagt, dass sich jedes beliebige symmetrische Polynom in eindeutiger Weise als Polynom in diesen elementarsymmetrischen Polynomen darstellen lässt. Die elementarsymmetrischen Polynome treten auch im Satz von Vieta auf.

5.3.5 Gebrochen rationale Funktionen und ihre Partialbruchzerlegung

Nebenziel der Vorlesung

Inhalt in Kurzfassung: Gebrochen rationale Funktionen können als Brüche dargestellt werden, die vermittels Kürzung und Normierung in eine Normalform gebracht werden können. Eine weitere Normalform gebrochen rationaler Funktionen ist aus der elementaren Analysis bekannt, wenn es um die Ermittlung einer Stammfunktion geht. Der Hintergrund ist ein algebraischer, nämlich die Primfaktorzerlegung. Dies soll nun dargelegt werden.

5.3.6 Interpolation nach Lagrange und nach Newton

Nebenziel der Vorlesung

Inhalt in Kurzfassung: Zu je $n+1$ Elementen eines Körpers K zusammen mit vorgegebenen Funktionswerten gibt es genau eine interpolierende Polynomfunktion vom Grad $\leq n$. Die Formel von Lagrange liefert eine Darstellung dieses Interpolationspolynoms, dem man die geforderte Eigenschaft sehr unmittelbar ansieht. Vom algorithmischen Standpunkt ist die Interpolation nach Newton effektiver. Die Eindeutigkeit der Lösung folgt, weil die Differenz zweier Interpolationspolynome Grad $\leq n$ mit $\geq n+1$ Nullstellen hat, also das Nullpolynom sein muss.

6 Körper

6.1 Prim-, Unter- und Erweiterungskörper

6.1.1 Primkörper

Leicht aber unverzichtbar

Inhalt in Kurzfassung: Der Durchschnitt beliebig vieler Unterkörper eines Körpers K ist wieder ein Unterkörper. Folglich erhält man, wenn man überhaupt alle Unterkörper schneidet, den kleinsten, den man auch den sogenannten Primkörper von K nennt. Umgekehrt bedeutet das: Jeder Körper lässt sich als Erweiterung eines Primkörpers auffassen. Die Charakteristik eines Integritätsbereichs und erst recht eines Körpers kann nur 0 oder eine Primzahl p sein. Im ersten Fall erhält man einen Primkörper, der zu $\mathbb{Q}$ isomorph ist, bei Primzahlcharakteristik zum Restklassenkörper $\mathbb{Z}_p$. Jeder Primkörper hat die Identität als einzigen Automorphismus.

6.1.2 Das Vektorraumargument

Leicht aber unverzichtbar

Inhalt in Kurzfassung: Jeder Erweiterungskörper lässt sich auch als Vektorraum über dem Grundkörper auffassen. Bei dieser Sichtweise schwächt man zwar die Struktur ab, gleichzeitig wird aber der Begriff der Dimension auch für Körpererweiterungen verfügbar. Der äußerst nützliche Gradsatz besagt, dass sich bei iterierten Körpererweiterungen Dimensionen aufmultiplizieren.

6.1.3 Algebraische und transzendente Elemente

Wesentliches Fundament

Inhalt in Kurzfassung: Für ein Element α eines Erweiterungskörpers sind in Bezug auf den Grundkörper K zwei grundsätzlich verschiedene Möglichkeiten denkbar. Entweder es besteht eine algebraische Beziehung zwischen α und Elementen aus K. In diesem Fall gibt es auch eine einfachste solche Beziehung, nämlich $f(\alpha) = 0$, wobei $f \in K[x] \setminus \{0\}$ das normierte Polynom von kleinstem Grad über K mit dieser Eigenschaft ist, das sogenannte Minimalpolynom von α. Dieses ist stets irreduzibel. Alle weiteren Polynome über K mit α als Nullstelle sind Vielfache des Minimalpolynoms. In diesem Fall heißt α algebraisch über K.Im anderen Fall, d.h. wenn α nicht Nullstelle eines $f \in K[x] \setminus \{0\}$ ist, heißt α transzendent über K. In beiden Fällen lässt sich die Struktur des Erweiterungskörpers einfach beschreiben: $K(\alpha) \cong K[x]/fK[x]$ (Faktorisierung des Polynomrings nach dem

vom Minimalpolynom erzeugten Hauptideal) im algebraischen Fall, $K(\alpha \cong K(x)$ (Körper der gebrochen rationalen Funktionen über K) im transzendenten Fall. Auch einige verfeinerte Aussagen in diese Richtung, die später noch verwendet werden, sind Inhalt dieses Unterabschnitts.

6.1.4 Algebraische Erweiterungen und endliche Dimension

Wesentliches Fundament

Inhalt in Kurzfassung: Auf den ersten Blick ist überhaupt nicht klar, dass die Iteration rein algebraischer Körpererweiterungen stets wieder rein algebraische Erweiterungen erzeugt. Verständlich wird dies aber sehr schnell mit Hilfe des Dimensionsarguments, weil nämlich Endlichdimensionalität und Algebraizität sehr eng miteinander zusammenhängen und somit das eine auf das andere zurückgeführt werden kann. Denn die Iteration endlichdimensionaler Erweiterungen ist wegen des Gradsatzes in offensichtlicher Weise wieder endlichdimensional.

6.1.5 Transzendente Körpererweiterungen

Nebenziel der Vorlesung

Inhalt in Kurzfassung: Rein transzendente Körpererweiterungen E eines Grundkörpers K lassen sich (bis auf Isomorphie) recht klar beschreiben, nämlich als Körper gebrochen rationaler Funktionen $K(X)$ in einer geeigneten Menge X von Variablen. Aber auch beliebige Körpererweiterungen werden dadurch zugänglich. Und zwar lassen sie sich beschreiben als Iteration einer vorangehenden rein transzendenten Körpererweiterung, gefolgt von einer rein algebraischen Erweiterung. Dabei geht es lediglich darum, eine sogenannte Transzendenzbasis, d.h. eine maximale algebraisch unabhängigen Menge zu finden. Das gelingt ganz ähnlich (z.B. mit Hilfe des Lemmas von Zorn) wie bei dem Satz aus der Linearen Algebra, dass sich linear unabhängige Mengen in Vektorräumen zu Basen ergänzen lassen. Es gilt auch ein Analogon zum Austauschsatz von Steinitz, wonach (hier für den endlichen Fall bewiesen) je zwei Transzendenzbasen gleich viele Elemente haben, weshalb der Begriff des Transzendenzgrades einer Körpererweiterung wohldefiniert ist.

6.1.6 Anwendung: Konstruierbarkeit mit Zirkel und Lineal

Nebenziel der Vorlesung

Inhalt in Kurzfassung: Übersetzt man die klassischen geometrischen Konstruktionsaufgaben mittels Zirkel und Lineal in eine algebraische Sprache, so entsprechen sie der Lösung von Gleichungen ersten und zweiten Grades, ausgehend vom Grundkörper $\mathbb{Q}$. Gleichungen ersten Grades haben innerhalb eines Körpers stets eine Lösung, bei zweitem Grad sind in der Regel Quadratwurzeln zu adjungieren, d.h. Körpererweiterungen vom Grad 2 nötig. Durch Iteration entstehen laut Gradsatz Erweiterungen, deren Dimension in

jedem Fall von der Form 2^n sind. Dies hat beispielsweise zur Folge, dass Konstruktionen dritter Wurzeln wie $\sqrt[3]{2}$ (Diagonale des Würfels vom Volumen 2, Delisches Problem der Würfelverdopplung), sofern sie nicht schon im Grundkörper liegen, ebenso wenig mit Zirkel und Lineal ausgeführt werden können wie die Dreiteilung beliebig vorgegebener Winkel. Auch die Konstruktion regelmäßiger n-Ecke mit Zirkel und Lineal wird durch derartige Überlegungen angreifbar, auch wenn für eine endgültige Klassifikation jener n, für die das möglich ist, auch noch Galoistheorie erforderlich wird. Weiß man, dass die Kreizahl π transzendent ist, folgt auch die Unmöglichkeit der legendären Quadratur des Kreises, d.h. die Konstruktion des Radius eines Kreises mit Einheitsfläche.

6.2 Adjunktion von Nullstellen von Polynomen

6.2.1 Adjunktion einer Nullstelle

Hauptziel der Vorlesung

Inhalt in Kurzfassung: Die Erkenntnisse aus dem vorangegangenen Abschnitt über algebraische Körpererweiterungen werden nun verwendet, um den umgekehrten Weg zu beschreiten. Zu gegebenem Körper K und Polynom $f \in K[x]$ ist ein Erweiterungskörper E von K gesucht, der eine Nullstelle von f enthält. Ist f irreduzibel (andernfalls ist f durch einen irreduziblen Faktor zu ersetzen), so gelingt dies mit $E := K[x]/fK[x]$, der Faktorisierung des Polynomrings nach dem von f erzeugten Hauptideal (Satz von Kronecker).

6.2.2 Die Konstruktion von Zerfällungskörper und algebraischem Abschluss

Hauptziel der Vorlesung

Inhalt in Kurzfassung: Durch Iteration der Konstruktion aus 6.2.1 lässt sich zu vorgegebenem $f \in K[x]$ eine Erweiterung E von K konstruieren, in der f nicht nur eine Nullstelle hat, sondern sogar in Linearfaktoren zerfällt. Eine minimale Erweiterung mit dieser Eigenschaft heißt Zerfällungskörper. Offenbar ist damit auch die Verallgemeinerung zunächst auf endlich viele Polynome $f_1, \ldots, f_n$ möglich, sodann, bei transfiniter Fortsetzung des Erweiterungsprozesses, auf eine beliebige Teilmenge von $K[x]$. Im Extremfall kann man auch die gesamte Menge $K[x]$ wählen. Der resultierende Zerfällungskörper Z erweist sich sogar als algebraisch abgeschlossen, enthält also nicht nur sämtliche Nullstellen von Polynomen über K sondern sogar aller Polynome aus $Z[x]$. Man spricht auch von einem algebraischen Abschluss von K.

6.2.3 Die Eindeutigkeit von Zerfällungskörpern und algebraischem Abschluss

Hauptziel der Vorlesung

Inhalt in Kurzfassung: Die Konstruktionen in 6.2.2 haben gezeigt, dass es zu jeder Menge von Polynomen über einem Körper einen Zerfällungskörper gibt. Dieser ist (bis auf Äqui-

valenz, also erst recht bis auf Isomorphie) sogar eindeutig bestimmt. Das entscheidende technische Hilfsmittel für den Beweis ist ein Fortsetzungssatz für Körperisomorphismen auf entsprechende Zerfällungskörper.

6.2.4 Mehrfache Nullstellen und formale Ableitung

Leicht aber unverzichtbar

Inhalt in Kurzfassung: Hat ein reelles Polynom eine mehrfache Nullstelle, so liegt in dieser eine waagrechte Tangente vor. Es gilt auch die Umkehrung sowie eine Verallgemeinerung auf beliebige Körper. Dazu ist die Definition einer formalen Ableitung erforderlich, für die auch auf rein algebraischem Wege aus der Analysis vertraute Differentiationsregeln bewiesen werden können. Mit Hilfe der Produktregel können dann die angedeuteten Zusammenhänge zwischen mehrfachen Nullstellen und dem Verschwinden von Ableitungen bewiesen werden.

6.2.5 Einheitswurzeln und Kreisteilungspolynome

Nebenziel der Vorlesung

Inhalt in Kurzfassung: Die Zerlegung eines Polynoms $x^n - 1$ in Linearfaktoren entspricht dem Aufsuchen von n-ten Einheitswurzeln, was in $\mathbb{C}$ geometrisch als Konstruktion des dem Einheitskreis eingeschriebenen regelmäßigen n-Ecks interpretiert werden kann. Daher rührt die Bezeichnung „Kreisteilungspolynom“ für gewisse, rekursiv definierte (sich bei Charakteristik 0 sogar als irreduzibel erweisende) Faktoren des Polynoms $x^n - 1$, dessen Nullstellen offenbar eine endliche multiplikative Untergruppe des Körpers bilden. Eine solche ist stets zyklisch.

6.2.6 Beispiele einfacher Erweiterungen

Ergänzung zum Kernstoff

Inhalt in Kurzfassung: Der Satz vom primitiven Element wird bewiesen: In Charakteristik 0 ist jede endlichdimensionale Erweiterung einfach (d.h. sie wird von einem einzigen, geeignet zu wählenden Element erzeugt). Erwähnt wird außerdem der Satz von Lüroth: Jeder Zwischenkörper Z mit $K \leq Z \leq K(x)$ ist eine einfache, für $K \neq Z$ transzendente Erweiterung über K.

6.3 Endliche Körper (Galoisfelder)

6.3.1 Klassifikation endlicher Körper

Hauptziel der Vorlesung

Inhalt in Kurzfassung: Sei K ein endlicher Körper, $P \cong \mathbb{Z}_p$, $p \in \mathbb{P}$, sein Primkörper und n die Dimension von K über P. Dann gilt offenbar $|K| = p^n$. Außerdem erweist sich K sehr schnell als Zerfällungskörper des Polynoms $x^{p^n} - x$ über P. Als solcher ist K aufgrund der Ergebnisse aus 6.2.3 durch seine Kardinalität bis auf Isomorphie eindeutig bestimmt. Umgekehrt lässt sich mit Hilfe der Methoden aus 6.2.2 der Zerfällungskörper des Polynoms $x^{p^n} - x$ über P konstruieren und hat auch tatsächlich p^n Elemente. Damit ist ein Klassifikationssatz für endliche Körper vollständig bewiesen.

6.3.2 Die Unterkörper eines endlichen Körpers

Nebenziel der Vorlesung

Inhalt in Kurzfassung: Ist K ein Unterkörper des endliche Körpers E, so muss, weil beide denselben Primkörper $P \cong \mathbb{Z}_p$ haben, ihre Charakteristik $p \in \mathbb{P}$ übereinstimmen. Folglich gilt $|K| = p^k$ und $|E| = p^n$ mit geeigneten positiven natürlichen Zahlen k und n. Aus dem Gradsatz folgt daraus fast unmittelbar $k|n$. Umgekehrt erweist sich bei $k|n$ das Polynom $x^{p^k} - x$ (dessen Zerfällungskörper ja K ist) als Teiler des Polynoms $x^{p^n} - x$ (dessen Zerfällungskörper wiederum E ist), dass jeder Körper E mit p^n Elementen einen (sogar eindeutig bestimmten) Unterkörper K mit p^k Elementen als Unterkörper enthält. Damit sind die Inklusionsbeziehungen zwischen endlichen Körpern vollständig geklärt.

6.3.3 Irreduzible Polynome über endlichen Primkörpern

Nebenziel der Vorlesung

Inhalt in Kurzfassung: Die Klassifikation endlicher Körper aus 6.3.1 zusammen mit der Zerlegung der Polynome $x^{p^n} - x$ über $P \cong \mathbb{Z}_p$, $p \in \mathbb{P}$, $n \in \mathbb{N}^+$, in (normierte) irreduzible Faktoren zeigt, dass als solche Faktoren genau jene irreduziblen (und normierten) Polynome über P auftreten, deren Grad ein Teiler von n ist, jeder Faktor mit Vielfachheit 1. Daraus ergeben sich mehrere interessante Folgerungen: Zu jedem positiven Grad gibt es mindestens ein irreduzibles Polynom über P, das sogar als primitiv gewählt werden kann. Letzteres bedeutet, dass seine Nullstellen die multiplikative Gruppe seines Zerfällungskörpers K erzeugen. Da jeder Automorphismus von K die Nullstellen jedes irreduziblen Faktors von $x^{p^n} - x$ permutiert, schließt man daraus, dass K genau n verschiedene Automorphismen hat — ein erstes Ergebnis im Geiste der Galoistheorie, siehe Kapitel 9.

6.3.4 Konstruktion endlicher Köper

Hauptziel der Vorlesung

Inhalt in Kurzfassung: Wir wissen bereits, dass jeder endliche Körper K der Kardinalität p^n, $p \in \mathbb{P}$, $n \in \mathbb{N}^+$, als Zerfällungskörper des Polynoms $x^{p^n} - x$ über seinem Primkörper $P \cong \mathbb{Z}_p$, bis auf Isomorphie eindeutig bestimmt ist. Was also soll es heißen, wenn von der „Konstruktion“ von K die Rede ist? Weil K ein Vektorraum über P ist, entpuppt sich

seine additive Struktur sehr schnell als die direkte Summe $C_p \oplus \ldots \oplus C_p$ von n Kopien der zyklischen Gruppe C_p mit p Elementen. Ähnlich ist die multiplikative Gruppe wegen Satz 6.2.5.1) als zyklische Gruppe $\cong C_{p^n-1}$ für sich ebenfalls bereits geklärt. Um mit diesen Darstellungen effektiv zu arbeiten, ist allerdings für die additive Struktur eine Basis von K über P gefragt, für die multiplikative hingegen ein primitives Element, d.h. ein erzeugendes Element der multiplikativen Gruppe. Ein Zusammenhang der beiden ist zunächst aber noch nicht sichtbar. In Hinblick auf eine algorithmische Bewältigung der Körperstruktur von entscheidendem Wert ist daher eine Art „Übersetzungstabelle“. Dafür genügt es, für ein (durch eine multiplikative Eigenschaft definiertes) primitives Element auch die Darstellung seiner Potenzen bezüglich einer Basis der Vektorraumstruktur anzugeben. Wir untersuchen in Folgenden, wie das mit Hilfe der mittlerweile entwickelten Strukturtheorie gelingt. Als Beispiel wird ein Körper mit $9 = 3^2$ Elementen konstruiert.

6.3.5 Der algebraische Abschluss eines endlichen Körpers

Nebenziel der Vorlesung

Inhalt in Kurzfassung: Für festes $p \in \mathbb{P}$ haben alle endlichen Körper der Charakteristik p (bis auf Isomorphie) denselben algebraischen Abschluss. Dieser lässt sich als direkter Limes endlicher Körper realisieren.