Einführung in die Algebra (BIII) – Stichworte zum Inhalt

Gottfried Barthel, FB Mathematik, Uni Konstanz

Sommersemester 2003

Vorbemerkung: Diese Sammlung von Stichworten zum Inhalt der Vorlesung ist insofern nicht ganz vollständig, als einige wichtige Aussagen nur in Form von Übungsaufgaben behandelt worden sind, die hier größtenteils noch nicht berücksichtigt sind; die Sammlung müsste also in diesen Punkten noch ergänzt werden!

1 Halbgruppen und Gruppen

Verknüpfungen, Halbgruppen, Monoide

Zweistellige Verknüpfungen, Beispiele, Assoziativitätsgesetz Halbgruppe (Menge mit assoz. Verknüpfung), Potenzen, links-, rechts-, beidseitig neutrale, reguläre, inverse Elemente; Links- und Rechts-Translationen, entgegengesetzte Struktur; Monoid (Halbgruppe mit neutralem Element), Kommutativgesetz, Gruppe.

Unterhalbgruppen und -monoide, Erzeugende, Wortehalbgruppe; Homomorphismen zwischen Halbgruppen und Monoiden, Iso-, Endo-, Automorphismen, idempotente Elemente, Komposition von Morphismen; Bilder und Urbilder von Unterhalbgruppen.

Äquivalenz- und Kongruenzrelationen (d.h. mit Verknüpfung verträglich: $a \sim b$, $c \sim d$ impliziert $ac \sim bd$), Restklassenstruktur, Faktorisierungssatz für Homomorphismen.

Kartesische Produkte, Projektionen, universelle Eigenschaft.

Gruppen

Gruppenaxiome, Charakterisierungen der Gruppeneigenschaft (alle Gleichungen $ax = b$, $ya = b$ lösbar; Charakterisierung durch Verknüpfungstafel bei endlichen Halbgruppen); Beispiele: Einheitengruppe eines Monoids, eines Ringes bzw. einer Algebra; symmetrische Gruppe.

Gruppenhomomorphismen, Kern, Charakterisierung der Injektivität, Translations- (oder Permutations-) Darstellung einer Gruppe, Satz von Cayley.

Konjugationen und innere Automorphismen, Konjugationsdarstellung, Zentrum als Kern der Konjugationsdarstellung, Beispiel $Z(S_n) = E$ für $n \geqq 3$.

Untergruppen, Durchschnittsstabilität, erzeugte Untergruppe, zyklische Gruppen, Beispiele, Def. Ordnung von Gruppen bzw. Elementen, Klassifikation der zyklischen Gruppen.

Nebenklassen, Ordnung und Index, Satz von Lagrange und Folgerungen, Gruppen von Primzahlordnung sind zyklisch; Gruppen ohne nicht-triviale Untergruppen haben Primzahlordnung.

Permutationen, invariante Teilmengen, Fixpunktmenge und Träger, verschiedene Möglichkeiten der Darstellung, Transpositionen, Zykel, disjunkte Zykelzerlegung, Signum, die alternierende Gruppe A_n ist für $n \geqq 4$ nicht abelsch.

(Konjugations-) Invariante und charakteristische Untergruppen: Beispiel Zentrum, Kommutatoruntergruppe, Beispiel $K(S_3) = A_3$, $K(D_4) = Z(D_4) = C_2$, höhere Kommutatorgruppen, Bsp. $K^2(S_4) = K(A_4) = V_4$ (Kleinsche Vierergruppe), also $K^3(S_4) = E$, Bsp.: Kerne von Homomorphismen sind konjugationsinvariant, Charakterisierung der Konjugationsinvarianz über die Nebenklassen, Nebenklassenzerlegung ist dann Kongruenzrelation, Def. Normalteiler (normale Untergruppe), zugehörige Restklassengruppe. Untergruppen vom Index 2 sind normal. Durchschnitt von Normalteilern, erzeugter Normalteiler. Faktorisierungsproblem und -satz, Isomorphiesätze.

Wirkung von Halbgruppen bzw. Gruppen auf Mengen, Bahnen, Klassengleichung: Beispiele, invariante Teilmengen, Bahnenzerlegung, Isotropiegruppe, Identifikation von Bahnen mit der Menge der Nebenklassen der Isotropiegruppe (d.h. Bahnen als homogene Räume), Ordnung einer Bahn ist Index der Isotropiegruppe, Repräsentanten, Bahnengleichung.

Konjugationswirkung einer Gruppe auf sich, Zentralisator, Klassengleichung, Anwendungen auf Gruppen von Primzahlpotenzordnung: Existenz eines nicht-trivialen Zentrums, Gruppen von Primzahlquadratordnung sind abelsch. Zentralreihe (ohne den Begriff zu verwenden), Kommutatorreihe bricht ab (Begriff „Auflösbarkeit“ aber nicht eingeführt). Satz: Zu jeder Primzahlpotenz $p^m \mid \mathrm{ord}(G)$ gibt es eine Untergruppe der Ordnung p^m; Folgerung: Satz von Cauchy, p-Gruppen.

2 Ringe und Ideale

Erinnerung an Stoff aus B I/II

Aus der Linearen Algebra bekannte Begriffe über Ringe, Polynome, Algebren, Teilbarkeit, euklidische Division mit Rest, ggT, kgV, Hauptidealringe, Operationen mit Idealen (Summe, Durchschnitt), faktorielle Ringe.

„Neuer Stoff“

Ringhomomorphismen, Unterringe, Restklassenringe nach Idealen, Idealprodukt, Isomorphiesätze, Verbandsstruktur (noch informell) auf der Menge der Ideale, Satz: Ein Ring R, dessen

Polynomring $R[T]$ ein Hauptidealring ist, muss bereits ein Körper sein. Satz: Ein kommutativer Ring mit mindestens zwei Elementen ohne nicht-triviale Ideale ist Körper oder ist zyklische Gruppe $\mathbb{Z}/(p)$ von Primzahlordnung mit trivialer Multiplikation.

Primideale und maximale Ideale: Ideal $\mathfrak{p}$ (in einem kommutativen Ring R mit $1_R \neq 0_R$) ist Primideal genau dann, wenn $R/\mathfrak{p}$ ein Integritätsbereich ist; entsprechend: Ideal $\mathfrak{m}$ ist maximales Ideal genau dann, wenn $R/\mathfrak{m}$ ein Körper ist. Beispiele für maximale Ideale.

Teilbarkeitstheorie in Integritätsringen (Erinnerung und Ergänzungen): Charakterisierung von Primelementen bzw. irreduziblen Elementen über Eigenschaften der erzeugten Hauptideale (Primideal bzw. maximales Hauptideal), nicht-triviale Primideale in Hauptidealringen sind maximale Ideale, $\mathbb{Z}[\sqrt{-5}]$ als Beispiel eines Zahlringes ohne eindeutige Faktorisierung, Normfunktion in diesem Ring, dto. für das reell-quadratische Gegenstück $\mathbb{Z}[\sqrt{5}]$, Konjugationshomomorphismus $\sqrt{5} \leftrightarrow -\sqrt{5}$, Normfunktion, Beispiel $4 = 2^2 = (3+\sqrt{5})(3-\sqrt{5})$; Mitteilung (ohne Beweis): Mit $\omega := (1+\sqrt{5})/2$ ist $\mathbb{Z}[\omega]$ ein faktorieller Erweiterungsring von $\mathbb{Z}[\sqrt{5}]$.

Quotientenkörper eines Integritätsbereiches: Konstruktion des Ringes der Brüche bzgl. eines multiplikativ abgeschlossenen Systems, Eigenschaften, Beispiele: Zahlkörper $\mathbf{Q}[\sqrt{5}] = \mathrm{Quot}(\mathbb{Z}[\sqrt{5}])$, rationale Funktionen $K(T)$, meromorphe Funktionen; auch $R_\mathfrak{p}$ (Lokalisierung nach Primideal), Laurent-Polynome $R[T, T^{-1}]$.

Ergänzung: Zornsches Lemma, Anwendung auf Existenz maximaler Ideale über gegebenem Ideal. Bemerkung: „Filtrierende“ Vereinigung von Untergruppen, Normalteilern, Idealen ist wieder Untergruppe usw.

Teilbarkeit in Polynomringen, speziell über faktoriellen Ringen. Inhalt eines Polynoms, primitive Polynome („Einheitsformen“), Zerlegung in „Inhalt · Einheitsform“, Lemma von Gauß (R faktoriell, dann ist ein Produkt von Einheitsformen wieder eine Einheitsform), Einheitsformen bilden also Untermonoid von $R[T]$, Zerlegung in „Inhalt · Einheitsform“ für Polynome in $K[T]$ für $K = \mathrm{Quot}(R)$; Vergleich von Faktorisierung in $R[T]$ und in $K[T]$, Satz von Gauß.

Irreduzibilitätskriterien: Eisenstein (Übungsaufgabe), Einsetzungsendomorphismus; Anwendung auf Irreduzibilität; Reduktion von Polynomen modulo Primidealen, Beispiel: Irreduzibilität von $T^5 - T^2 + 1$ durch Reduktion modulo p=2.

3 Körper

Erinnerung an bereits bekannte Resultate

Diskussion frühere Beispiele, etwa im Zusammenhang mit Quotientenkörpern; Diskussion des Beispiels: Irreduzibilität von $T^5 - T^2 + 1$ modulo p=2 liefert Körper mit 32 Elementen, $\mathbf{F}_3[T]/(T^2+1)$ liefert Körper mit 9 Elementen.

Grundbegriffe: Charakteristik, Körpererweiterungen usw.

Charakteristik (auch für Integritätsringe), Körpererweiterungen, Teilkörper, Primkörper, Frobenius-Endomorphismus in kommutativen $\mathbf{F}_p$-Algebren, Ring- und Körperadjunktion.

Körpererweiterungen: Grad einer KE, Zwischenkörper, Gradsatz, Erweiterungen von Primzahlgrad haben keine echten Zwischenkörper; Begriffe einfache Körpererweiterung, primitives Element.

Algebraische und transzendente Elemente einer Körpererweiterung, algebraische Zahlen. Kleiner Exkurs: Einige Beispiele von transzendenten Zahlen wie e, π, Liouville-Beispiel $\sum 10^{-n!}$ (Mitteilungen ohne Beweis). Charakterisierung von algebraischen bzw. transzendenten Elementen, transzendente KE besitzen unendlich viele Zwischenkörper.

Minimalpolynom eines algebraischen Elementes: Definition, charakteristische Eigenschaften, endliche Körpererweiterungen sind algebraisch, Transitivität der Algebraizität, relativer algebraischer Abschluss, Körper $\overline{\mathbf{Q}}$ der algebraischen Zahlen.

Konstruktion von Körpererweiterungen: Abspalten einer Nullstelle, Zerfällungskörper, normale Körpererweiterungen, Beispiele: Quadratische Erweiterungen sind normal; Nicht-Transitivität der Normalität: Beispiel $\mathbf{Q}[\sqrt[4]{2}]/\mathbf{Q}[\sqrt{2}]/\mathbf{Q}$.

Separable Polynome, Elemente, Körpererweiterungen; Fortsetzung von Isomorphismen (Anzahlformel), vollkommene Körper, Satz vom primitiven Element.

Galois-Erweiterungen, Hauptsatz der Galois-Theorie

Definition von Galois-Erweiterungen (stets als endlich vorausgesetzt!), Galois-Gruppe, Gleichheit von Gruppenordnung und Körpergrad.

„Galois-Zwischenkörper-Satz“: Ist L/K Galoissch, so ist L/E ebenfalls Galoissch für jeden Zwischenkörper, Diskussion von $\mathrm{Gal}(E/K)$ im Fall, dass auch E/K Galoissch ist. Verhalten von Normalität und Separabilität; Transitivität der Separabilität (allerdings ohne den Beweis der nicht-trivialen Richtung, dass nämlich aus E/K separabel, L/E separabel auch L/K separabel folgt).

„Fixkörper-Satz“: Ist $G < \mathrm{Aut}(L)$ endlich, so ist L/L^G Galoissch. Beweis reduziert auf „Endlichkeitssatz“: In dieser Situation ist L/L^G endlich. Charaktere, lineare Unabhängigkeit von Charakteren, Spur bzgl. einer endlichen Untergruppe von $\mathrm{Aut}(L)$.

Hauptsatz der Galois-Theorie: Formulierung und Abschluss des Beweises. Ausblick auf Anwendungen.

Ende der Vorlesung