ALGEBRA, WINTERSEMESTER 2014/15

KARIN BAUR

ZUSAMMENFASSUNG. Algebra, 4stündig, Wintersemester 2014/15, KFU Graz. Kurze Übersicht über den Inhalt der Vorlesung.

TEIL I: GRUPPEN

Im ersten Teil geht es vor allem um das Klassifikationsproblem endlicher Gruppen. Einerseits: Symmetrische Gruppen, alternierende Gruppen, einfache Gruppen, Diedergruppen.
Andrerseits: die Sylow-Sätze.

Einfache Gruppen als Grundbausteine. Ist G endlich, so kann man G über seine Kompositionsreihe verstehen/studieren. Dazu sucht man in G einen Normalteiler G_1, für den $|G_1|$ maximal ist (unter allen Normalteilern von G). Der Quotient G/G_1 ist dann einfach. Ist G_1 einfach, so ist man fertig. Andernfalls sucht man in G_1 einen Normalteiler G_2 mit $|G_2|$ maximal, dann ist G_1/G_2 einfach. Etc. Eine Kompositionsreihe von G ist von der Gestalt

$$G = G_0 \supsetneq G_1 \supsetneq G_2 \supsetneq \cdots \supsetneq G_t$$

mit den Eigenschaften: $G_i \lhd G_{i-1}$ und G_i/G_{i+1} ist einfach. Jede Kompositionsreihe von G hat dieselben einfachen sukzessiven Quotienten, in dem Sinne ist die Kompositionsreihe eindeutig. (Ohne Beweis in der Vorlesung).

Endliche einfache Gruppen. Die gehören zu 4 verschiedenen Arten von Gruppen: $\mathbb{Z}_p$ mit p prim (das sind die einzigen abelschen einfachen Gruppen); A_n mit $n > 4$ (A_2 und A_3 gehören zu den abelschen Gruppen, sind also schon in $\mathbb{Z}_p$ abgedeckt); Lietypen (in der Vorlesung nicht behandelt); 26 Ausnahmefälle (die sporadischen Gruppen)

Permutationsgruppen. S_n. Begriffe: k-Zykeln, Transpositionen, gerade, ungerade Permutation.
Permutationen sind Produkte von disjunkten Zykeln. Sie sind Produkte von gerader oder ungerader Anzahl Transpositionen (damit die Definition von gerader/ungerader Permutation). Die alternierenden Gruppen A_n sind die Mengen der geraden Permutationen in S_n, das ist eine Untergruppe, sogar ein Normalteiler in S_n Es ist $|A_n| = \frac{n!}{2}$ (Satz 1.11, Beweis kennen).

Sylowsätze. Diese diskutieren den Zusammenhang zwischen der Struktur einer endlichen Gruppe G und den Eigenschaften von $|G|$. (Die Beweise werden nicht verlangt). Die Aussagen sollten man kennen:
1. Sylowsatz: Ist $|G| < \infty$, $p^k \mid |G|$: dann hat G eine Untergruppe der Ordnung p^k.
Untergruppen der Ordnung p^k mit k maximal heissen p-Sylowuntergruppen, die existieren nach dem 1. Sylowsatz.
2. Sylowsatz: Je zwei p-Sylowuntergruppen von G sind konjugiert. (Als Folge: je zwei p-Sylowuntergruppen von G sind isomorph).
3. Sylowsatz: Die Anzahl der p-Sylowuntergruppen von G (mit $|G| < \infty$) ist ein Teiler von $|G|$ und von der Gestalt $1 + kp$ für ein $k \geq 0$.
Folgerungen:
Satz von Cauchy als Folge des 1. Sylow-Satzes (teilt p die Ordnung von G, so enthält G ein Element der Ordnung p).
Eine p-Sylowuntergruppe $H \leq G$ ist Normalteiler $\iff$ H ist die einzige p-Sylowuntergruppe von G.
Anwendungen: Beispiele $|G| = 63$ und $|G| = 56$: solche Gruppen können nicht einfach sein (Argumente für diese Beispiele anwenden können).
Die Klassengleichung kennen (verschiedene Formen davon).

Struktur endlicher Gruppen. EInige Resultate, die helfen, die Isomorphieklassen von endlichen Gruppen kleiner Ordnung zu kennen, etwa:
Hat G Ordnung p^n (p prim), so ist das Zentrum von G nicht trivial und $|Z(G)| = p^k$ mit $1 \leq k \leq n$. Ausserdem ist dann G nicht einfach.
Hat G Ordnung p^2, so ist G abelsch, also $G \cong \mathbb{Z}_{p^2}$ oder $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$.
Etc.
Diedergruppe D_n: die Symmetriegruppe eines regelmässigen n-gons. Wird erzeugt von einer Rotation (um $360/n$ Grad) und einer Spiegelung (mit Relationen).
Hat G Ordnung $2p$, p prim, $p > 2$, so ist $G \cong \mathbb{Z}_{2p}$ oder $G \cong D_p$.
Ideen des Lemma 3.8 anwenden können (dort ist G eine Gruppe der Ordnung 8 und man untersucht, welche Gruppe G sein kann).
Damit auch verstehen können, wie man die Liste der endlichen Gruppen von Ordnung ≤ 15 (bis auf Isomorphie) findet.

Teil II: Integritätsbereiche

Begriffe: Integritätsbereiche, Teilbarkeit, Einheiten, Assoziiertheit, Primelelemente/irreduzible Elemente.

Zur Illustration sollte man Beispiele gut kennen, insbesondere $\mathbb{Z}$, $k[x]$ (für k einen Körper), $\mathbb{Z}[\sqrt{d}]$ (für $d \in \mathbb{Z}$, speziell $d = -1$). Überlegen, was im jeweiligem Beispiel die Begriffe Einheit, assoziiertes Element, irreduzibel etc. bedeuten!

Euklidische Bereiche. Definition davon, Beispiele sind $k[x]$ (mit δ die Gradfunktion), $\mathbb{Z}$ (mit δ die Betragsfunktion), $\mathbb{Z}[i]$ mit $\delta(s + ti) = s^2 + t^2$.

Hauptidealbereiche, faktorielle Bereiche. Bemerkung: $\mathbb{Z}[x]$ ist *kein* Hauptidealbereich.
Euklidische Bereiche sind Hauptidealbereiche (Umkehrung stimmt i.a. nicht).
Faktorielle Bereiche (UFD oder ZPE): eindeutige Faktorisierungen existieren (Beispiele: Euklidische Bereiche, Hauptidealbereiche).
Hauptidealbereiche sind faktoriell (Umkehrung gilt i.a. nicht, so ist etwa $\mathbb{Z}[x]$ faktoriell, aber nicht Hauptidealbereich!).
Eigenschaften von faktoriellen Bereichen sollte man kennen, etwa die Aussagen der Sätze 5.2 (man kann zwei Elemente mit Hilfe der gleichen irreduziblen Darstellen), 5.3 (teilt ein Primelement ein Produkt, so teilt es einen der Faktoren des Produkts), 5.4 (ggT's einer Menge von Elementen eines faktoriellen Bereichs existieren).

Quotientenkörper zu Integritätsbereichen. Dies ist wichtig für Kapitel 7. Definition des Quotientenkörpers kennen. Beispiele: $\mathbb{Q}$ als Quotientenkörper von $\mathbb{Z}$. Der Quotientenkörper vom Polynomring $k[x]$ ist der Körper $k(x)$ der rationalen Funktionen.
Satz 6.6 fasst die Aussagen dieses Kapitels zusammen.
Der Quotientenkörper eines Rings als der kleinste Körper, der den Ring enthält (Aussage von Satz 6.7).

Eindeutige Faktorisierung in $R[x]$, für R faktoriell. Idee: $f(x) \in R[x]$ faktorisieren, bis irreduzible Elemente dastehen, dazu benutzt man $k[x]$, wobei k der Quotientenkörper von R ist.
Was sind die Einheiten von $R[x]$, die irreduziblen konstanten Polynome in $R[x]$? Wie sieht dies bei $\mathbb{Z}[x]$ aus?
Begriff der primitiven Elemente kenne.
Satz 7.1: Faktorisierungen existieren in $R[x]$ (Beweis kennen).
Satz 7.7: Faktorisierungen sind eindeutig. Da sollte man die Zutaten kennen (Aussagen von Korollar 7.3, Satz 7.4, Korollare 7.6 und 7.7) als Übersicht oder Beweisstrategie für Satz 7.8.

Teil III: Körpererweiterungen

Begriff der Körpererweiterung kennen.
Sei $k \subseteq K$ Körpererweiterung. Definition von $[K : k]$, Satz 8.1: die Dimensionen im Fall von Verschachtelungen von Körpererweiterungen.

Erweiterungen rauf und runter. *Aufwärts:* zu einem irreduziblen Polynom $p(x) \in k[x]$ (vom Grad > 1) sucht man einen Körper, der eine Nullstelle von $p(x)$ hat. Dazu definiert man die Kongruenz modulo $p(x)$. Diesen Begriff kennen. Als Beispiel: In $\mathbb{Q}[x]$ ist $x^2 + x + 1$ kongruent zu $x + 2$ modulo $x + 1$.
Satz 9.4: Die Menge $k[x]/(p(x))$ der Kongruenzklassen mod $p(x)$ ist ein Körper (wenn $p(x)$ irreduzibel ist), es ist eine Körpererweiterung von k, sie enthält eine

Nullstelle von $p(x)$. (Beweisidee/-schritte kennen).
Runter: Zu $u \in K$ definiert man $k(u)$. Zwei Fälle: u algebraisch über k, u transzendent über k.
Beispiele: $\mathbb{C} = \mathbb{R}(i)$, i ist algebraisch über $\mathbb{R}$. Ist $c \in k$, so ist c algebraisch über k (und $k(c) = k$). π und e sind transzendent über $\mathbb{Q}$.
Minimalpolynom (zu u): Satz 9.5 (Definition vom Minimalpolynom, Eindeutigkeit, Existenz, es teilt alle andern Polynome, die u als Nullstelle haben).
Wie sieht z.B. das Minimalpolynom von $\sqrt{3}$ über $\mathbb{Q}$ aus, wie über $\mathbb{R}$?
Satz 9.6: Grad von $k(u)$ über k, wenn das Minimalpolynom $p(x)$ von u Grad n hat. Basis von $k(u)$ über k? (Beweisschritte/-idee kennen).

Algebraische Erweiterungen. $\mathbb{C}$ ist algebraisch über $\mathbb{R}$.
Satz 10.1: endlich-dim. Erweiterungen sind algebraisch. (Beweis kennen) (Umkehr gilt i.a. nicht, siehe Beispiel Körper der algebraischen Zahlen).
Konsequenz: ist $u \in K$ transzendent über k, so ist K unendlich-dimensional über k.
Definition von $k(u_1, \dots, u_n)$ kennen. Mit Beispielen wie $\mathbb{Q}(\sqrt{5}, i)$ rechnen können.
Aussage: Körpererweiterung endlich-dimensional $\Longrightarrow$ endlich erzeugt.
Mit Verschachtelungen von Körpererweiterungen arbeiten können, etwa
$\mathbb{Q}(\sqrt{3}, i) = \mathbb{Q}(\sqrt{3})(i) \supseteq \mathbb{Q}(\sqrt{3}) \supseteq \mathbb{Q}$, Grade berechnen können.
Ist $K = k(u_1, \dots, u_n)$ mit $u_i \in K$ algebraisch über k, so ist K endlich-dimensional. (vgl. mit Satz 10.1). (Beweis?)

Zerfällungskörper=ZK. Im ZK eines Polynoms liegen alle seine Nullstellen. So $f(x) = c(x - u_1)\cdots(x - u_n)$, der ZK von $f(x)$ ist $K = k(u_1, \dots, u_n)$.
Beispiele von ZK's: $\mathbb{C}$ für $x^2 + 1 \in \mathbb{R}[x]$ (aber nicht über $\mathbb{Q}$). $\mathbb{Q}(\sqrt{3})$ für $x^2 - 3$. k selbst für $x - c \in k[x]$.
Satz 11.2 gibt Existenz des ZK für $f(x) \in k[x]$ an und Abschätzung des Grades dieses ZK über k. Beweis kennen.
Aussage von Satz 11.3 (je zwei ZK zu $f(x)$ sind isomorph).
Begriff der normalen Körpererweiterung. Beispiele oder Nicht-Beispiele dafür? (Körpererweiterung $\mathbb{Q}(\sqrt[3]{2})$ von $\mathbb{Q}$, Polynom $f(x) = x^3 - 2 \in \mathbb{Q}[x]$ - das Polynom hat komplexe Nullstellen, diese KE kann nicht normal sein, damit kann diese KE nicht ZK eines Polynoms in $\mathbb{Q}[x]$ sein).
Über algebraisch abgeschlossenen Körpern zerfallen alle Polynome (das wäre $\mathbb{C}$ z.B.).

Separabilität. Polynome vom Grad n, die n verschiedene Nullstellen haben (in geeigneter Körpererweiterung) heissen separabel. Entsprechend $u \in K$ heisst separabel, falls... und $K \supseteq k$ heisst separabel, falls... (in dem Fall ist K auch algebraisch über k).
Satz 12.3: Ist K endlich erzeugte separable Körpererweiterung von k, so ist $K = k(u)$ für ein u. (Beweis-Schritte?).

Teil IV: Galoistheorie

Zu den drei Kapiteln (13, 14 und 15) sind die drei Beispiele sehr wichtig
a) komplexe Zahlen über reellen Zahlen (siehe Beispiele 13.2, 13.5, 13.13)
b) $Q(\sqrt{3},\sqrt{5})$ über $\mathbb{Q}$ (Beispiel 13.7, Bemerkung nach Beispiel 13.9, Beispiele 13.10, 13.12, 14.1, 14.6)
c) K=Zerfällungskörper von x^3-2 über $\mathbb{Q}$ und $\mathbb{Q}(\sqrt[3]{2})$ über $\mathbb{Q}$ (siehe Beispiele 13.9, 13.14, 14.4, 14.8).

Diese immer wieder auftretenden Beispiele illustrieren die drei Kapitel sehr gut.

Zum Inhalt der drei Kapitel:
13.) Galoistheorie: Aussagen der Sätze 13.3, 13.6, Korollar 13.8 (Zwischenkörper, Fixkörper).

14.) Fundamentalsatz (v.a. Teil (1) von dem Satz): Galoiskorrespondenz (diese ist immer subjektiv, ist nicht immer injektiv, ist injektiv bei endlich-dimensionalen, normalen, separaten Körpererweiterung, das sind gerade die Galois-Erweiterungen).

15.) Auflösbarkeit: Aussage von Satz 15.1 verstehen. Die Gruppe S_n ist nicht auflösbar für $n > 4$, damit erhält man: Es kann keine allgemeine Lösungsformel (mit Wurzelausdrücken) für Polynome 5. Grades geben.

V. Modultheorie

Begriffe (Links-)Modul, Untermodul, freie Moduln. Quotientenmoduln, direkte Summen. Kurze exakte Folgen: zerfallende (siehe Satz 17.6) und nicht-zerfallende (Beispiel mit $n\mathbb{Z}$, $\mathbb{Z}$ und $\mathbb{Z}/n\mathbb{Z}$). Freier Modul als direkte Summe (Satz 17.9). Lineare Unabhängigkeit, maximale linear unabhängige Familie, Torsionsmodul.
Satz 17.13: Aussage und Beweisschritte kennen.
Einfacher Modul. Halbeinfache Moduln. Beispiele kennen ($R = k$: alle Moduln sind halbeinfach. $R = \mathbb{Z}$: Moduln, die nicht halbeinfach sind?). Aussage von Satz 20.4 (Charakterisierung von halb-einfachen Moduln).

Wichtige Sätze

Sätze, die sich gut fürs mündliche Vorstellen eignen sind hier aufgelistet:

Kapitel I	S. 1.11, S. 2.1, S. 2.3, ev. S. 3.1
Kapitel II	S. 6.6 (Ideen dazu), S. 7.1, S. 7.8
Kapitel III	ev. S. 9.4, S. 9.5, S 9.7, S. 11. 2, S. 11.4, S. 12.3
Kapitel IV	S. 14.7, S. 15.1, S. 15.3 (bei allen dreien: Aussagen erkären können)
Kapitel V	S. 17.7, S 18.2, S. 18.3, S. 20.4 (Schritte dazu).