STICHWORTE ZU ALGEBRA I

Hans Peter Rehm, Karlsruhe 2006/2007

Dieser Text mit ziemlich vielen Stichworten soll eine kleine Hilfestellung zum Wiederholen und Lernen des Inhalts meiner Vorlesung geben. (Er wird fortlaufend erweitert werden). Gelegentlich schreibe ich auch einen kleinen Beweis der Vorlesung auf, wenn man das so in der Literatur suchen müsste. Zudem sind hier auch Nummerierungen der Abschnitte, die als verbindlich zu denken sind (in der Vorlesung interessieren mich solche Nummern nicht; daher wird auf die Nummerierung der Sätze zugunsten merkbarer Labels wie z.B. Untergruppenentsprechungssatz verzichtet, was die Sätze ebensogut identifiziert wie Satz 3.2.1 und für den Menschen besser verständlich ist.) Ich stelle mir folgenden Gebrauch vor (Algebra-Brain-Jogging): Sie nehmen sich die Stichworte einzeln vor und notieren, was Ihnen dazu einfällt. In den meisten Fällen sollte das eine Definition, bei Sätzen auch deren hauptsächlicher Inhalt sein. Weiter sollten Sie überdenken, was damit angefangen wurde und wie und wo die Begriffe vorkamen (Beispiele!) und was über sie berichtet wurde. (Notieren Sie am besten einen kurzen Bericht.) Dann können Sie das Ergebnis mit Ihrem Vorlesungsmitschrieb vergleichen (was natürlich besonders nötig ist, wenn Ihnen nichts eingefallen ist: dann sollten Sie den entsprechenden Teil der Mitschrift noch einmal sorgfältig lesen und sich den Inhalt einprägen). Es fehlen die Kenntnisse, die Sie in den Übungen erwerben, die aber auch ein wesentlicher Bestandteil des Algebra-Kurses sind.

KAPITEL I : Erste Schritte in der Gruppentheorie

S1. Halbgruppen und Monoide

Verknüpfung. Halbgruppe, Monoid, (Homo-)Morphismen solcher. Isomorphismus, Automorphismus, Untermonoid. Die allgemeine Assoziativregel und Kommutativregel. Das Monoid A^A der Abbildungen $A \to A$. (wo A Menge). Das Monoid 2^M der Teilmengen eines Monoids M. Das freie Monoid $\mathrm{Fr_{Mon}(A)}$ und dessen UAE (universelle Abbildungseigenschaft).

Zum **freien Monoid**:

Wir gehen aus von einer Menge A, die in diesem Zusammenhang Alphabet genannt wird. Ein *Wort* über A ist einfach ein n-Tupel $(a_1, \dots, a_n) \in A^n,\ n \in \mathbb{N}$. Wenn keine Missverständnisse zu befürchten sind, schreibt man kürzer $m = a_1 \dots a_n$ (Weglassen der Klammer und der Kommata). Dann besteht $\mathrm{Fr(A)} = \mathrm{Fr_{Mon}(A)}$ aus allen solchen Wörtern. Die Verknüpfung ist einfach das Hintereinanderschreiben:

$$(a_1, \dots, a_n) \cdot (b_1, \dots, b_m) := (a_1, \dots, a_n, b_1, \dots, b_m).$$

Das ist offensichtlich assoziativ und das leere Wort $e = () \in A^0$ kann als neutrales Element dienen.
Man hat die injektive Abbildung $i : A \to \mathrm{Fr(A), a \mapsto (a)}$, die durch die Kurzschreibweise zu der Identifizierung von $a \in A$ mit $(a) \in \mathrm{Fr(A)}$ führt. Dadurch entsteht kein Fehler, weil $(a_1) \cdot \ldots \cdot (a_n) = (a_1, \dots, a_n)$ ist.

Satz (UAE=universelle Abbildungseigenschaft des freien Monoids)
Sei M ein Monoid und $f : A \to M$ eine Abbildung. Dann hat f **genau eine** *Fortsetzung* zu einem Homomorphismus $\tilde{f} : \mathrm{Fr(A)} \to \mathrm{M}$. (Fortsetzung besagt: $\tilde{f} \circ i = f$).

Der Beweis ist sehr leicht: Man rechnet nach, dass $\tilde{f}(m)$ aus m entsteht, indem für die a_i die $f(a_i)$ eingesetzt werden (die Verknüpfung muss natürlich durch die in M ersetzt werden). Damit ist die Fortsetzung eindeutig, und umgekehrt liefert dieses Einsetzen ein Homomorphismus, der f fortsetzt.

Die Bedeutung dieses Satzes ist zweifach:
1. wurden gewissermaßen alle Homomorphismen von $\mathrm{Fr(A)}$ nach M bestimmt: Die Homomorphismen entsprechen genau den Abbildungen von A nach M. Genauer: Die Abbildung $f \mapsto \tilde{f}$,

$$M^A \to \mathrm{Hom(Fr(A), M)},$$

ist bijektiv.
2. Das freie Monoid ist bis auf Isomorphie durch die UAE charakterisiert.
Genauer: Ist N ein Monoid und $j : A \to N$ eine Abbildung, so dass die UAE für N und j gilt (d.h. für jedes Monoid M und jede Abbildung $f : A \to M$ gibt es genau einen Homomorphismus $\bar{f}$ mit $\bar{f} \circ j = f$), so ist $\bar{i} : N \to \mathrm{Fr(A)}$ ein Isomorphismus mit Umkehrung $\tilde{j}$.
Denn offenbar ist $\bar{j} = \mathrm{id}_N$ wegen $\mathrm{id} \circ j = \mathrm{id}$. Andererseits gilt $\tilde{j} \circ \bar{i} \circ j = \tilde{j} \circ i = j$, also $\mathrm{id}_N = \bar{j} = \tilde{j} \circ \bar{i}$. Durch Vertauschen der Rollen von N und $\mathrm{Fr(A)}$ sieht man genauso $\bar{i} \circ \tilde{j} = \mathrm{id}_{\mathrm{Fr(A)}}$. Demnach sind $\bar{i}$ und $\tilde{j}$ zueinander inverse bijektive Abbildungen, also Isomorphismen.

S**2. Gruppen (Grundbegriffe)**

2.1 Definition, Beispiele

Invertierbares Element eines Monoids. Gruppe. Einheitengruppe $M^\times$ eines Monoids M. Die symmetrischen Gruppen $\mathrm{S_A}$ und $\mathrm{S_n}$, die lineare Gruppe $\mathrm{GL}_n(R)$, die Automorphismengruppe $\mathrm{Aut}(M)$ eines Monoids M. Zyklus $(a_1, \ldots, a_n)$ und Darstellung von $\pi \in S_n$ als Produkt disjunkter Zyklen. Formel für $\pi(a_1, \ldots, a_n)\pi^{-1}$.

2.2 Gruppentheoretisches Erzeugnis und der Untergruppenverband.

Untergruppe, (gruppentheoretisches) Erzeugnis $\langle A \rangle$ einer Teilmenge A einer Gruppe G. Untergruppenverband $\mathcal{U}(G)$ der Gruppe G. Zusammenhang von $\mathcal{U}(\mathbb{Z})$ mit dem Verband $\mathbb{N}$ bei Teilbarkeitsanordnung $|$. Zyklische Untergruppe $\langle a \rangle$ und Ordnung $\mathrm{ord}(a)$ von $a \in G$ und von G. $\mathcal{U}(\mathrm{S}_3)$.

2.3 Rechter und linker Quotient, Normalteiler und Faktorgruppe

Rechnen in 2^G für eine Gruppe G, besonders mit Nebenklasse xU bzw. Ux einer Untergruppe $U \le G$. Der rechte bzw. linke Quotient G/U bzw. $U \backslash G$, Index $G : U$. Die Sätze und Lagrange und Cayley. Normale Untergruppe $N \trianglelefteq G$, Faktorgruppe G/N als Unterhalbgruppe von 2^G, Normalteilerkriterium.

2.4 Der Homomorphiesatz

Quotient $M/\sim$ einer Menge nach einer Äquivalenzrelation $\sim$, kanonische Abbildung $\kappa : M \to M/\sim$. Fasern X_y zu einer Abbildung $f : X \to Y$, zugehörige Äquivalenzrelation $x \sim_f y$, Homomorphiesatz für Mengen (kanonische Faktorisierung einer Abbildung). Homomorphisatz für Gruppen. Zyklische–Gruppen–Satz. Elementordnungssatz. 2. Noethersche Regel.

S**3 Operierende Gruppen**

3.1 Grundbegriffe, Beispiele

Operation einer Gruppe G auf einer Menge M, Fixpunkt von $g \in G$ oder von $H \leq G$, Fixgruppe G_m von $m \in M$, Bahn Gm von m. Satz über Bahnzerfall, Bahnbeschreibung und Bahnbilanz (Bahnensatz). Der p-Fixpunktsatz. Standardoperation von Untergruppen von $\mathrm{S_M}$ auf M und der Potenzmenge 2^M von M. Standardoperation der symmetrischen Gruppe S_n.

3.2 Symmetriegruppen.

Satz von Euler, Gruppe der Bwegungen im $\mathbb{R}^n$, Symmetriegruppe einer geometrischer Figur, die Symmetriegruppe einer Gerade, Translation, Spiegelung. Operation von $H \leq G$ auf G durch gruppentheoretische Translation.

3.3 Die Operation durch innere Automorphismen und Bestimmung der Gruppen mit p^2 Elementen.

Der innere Automorphismus $\mathrm{in_x}$. Operation durch innere Auromorphismen auf G und dem Untergruppenverband $\mathcal{U}(G)$, Konjugiertenklasse und Zentralisator $C_G(x)$ von $x \in G$, Konjugiertenklasse und Normalisator $N_G(H)$ von $H \leq G$ als Fixgruppen, Zentrum $Z(G)$ von G. Bahnbeschreibung in diesen Fällen. Nichttrivialität des Zentrums von p-Gruppen. Bestimmung aller Gruppen der Ordnung p^2. Untergruppenverband $\mathcal{U}(C_p \times C_p)$.

3.4 Untergruppen bei Homomorphismen

Untergruppenentsprechungssatz für einen surjektiven Homomorphismus $\phi : G \to H$. 1.Noethersche Regel (Kürzungsregel). Satz über Untergruppen von p-Gruppen.

Da mich in der Vorlesung die Geduld verlassen hat, soll hier der Beweis von (ii) im Entsprechungssatz im Detail aufgeschrieben werden, auch damit Sie sehen, wie eine saubere Ausführung der empfohlenen Übungsaufgabe aussieht. Als Verkenntnisse benötigt man a) den Homomorphiesatz für Mengen, b) das Rechnen im Monoid 2^G, besonders mit Nebenklassen $vU = \{v\}U$, insbesondere $vU = U \Leftrightarrow v \in U$, c) das Rechnen mit Homomorphismen von Gruppen, d) die Definition des Raums G/H der Nebenklassen einer Untergruppe H und der kanonischen surjektiven Abbildung $G \to G/H$ und ihrer Fasern xH d) die Kenntnis bijektiven Abbildung $\phi_* : \mathcal{U}(G, \text{Kern } \phi) \to \mathcal{U}(H)$ und ihrer Inversen ϕ^* aus (i) des Beweises. Wer die

Vorlesung nachgearbeitet hat, sollte damit keine Probleme haben. Wenn doch: Sie können jederzeit eine e-mail an mich oder Herrn Januschewski schicken oder die Tutoren fragen.
Es handelt sich um die Aussage (ii) Sei $\phi : G \to H$ ein Gruppenhomomorphismus, und sind U, V Untergruppen von G mit $\mathrm{Kern}(\phi) \le U \le V \le G$ und $\kappa : \phi(V) \to \phi(V)/\phi(U)$ kanonisch, so hat man die bijektive Abbildung $\bar{f} : V/U \to \phi(V)/\phi(U)$. Insbesondere gilt für die Indizes $V : U = \phi(V) : \phi(U)$.

Beweis: In diesem Beweis soll die kanonische Abbildung $V \to V/U$ mit λ bezeichnet werden, weil κ schon vergeben ist. Man hat die surjektive Abbildung $f := \kappa \circ \phi : V \to \phi(V)/\phi(U)$. Mit den zugehörigen Äquivalenzrelationen ist definitionsgemäß $V/U = V/{\sim_\lambda}$, und laut Homomorphiesatz für Mengen ist $\bar{f} : V/{\sim_f} \to f(V) = \phi(V)/\phi(U)$ bijektiv. Es genügt also der Nachweis von $\sim_\lambda = \sim_f$. Man findet für $v, w \in V$:
$v \sim_f w \;\Leftrightarrow\; f(v) = f(w) \;\Leftrightarrow\; \kappa(\phi(v)) = \kappa(\phi(w)) \;\Leftrightarrow\; \phi(v)\phi(U) = \phi(w)\phi(U) \;\Leftrightarrow\; \phi(w^{-1}v)\phi(U) = \phi(U) \;\Leftrightarrow\; \phi(w^{-1}v) \in \phi(U) \;\Leftrightarrow\; w^{-1}v \in \phi^{-1}(\phi(U)) = \phi^* \circ \phi_*(U) = U$ (letzteres laut (i) im Untergruppenentsprechungssatz, was in der Vorlesung ausführlich nachgeprüft wurde) $\Leftrightarrow w^{-1}vU = U \;\Leftrightarrow\; \lambda(w) = wU = vU = \lambda(v) \;\Leftrightarrow\; v \sim_\lambda w$.
Das besagt auch, dass die Äquivalenzklassen (Fasern $f^{-1}(\{\alpha)\}$ für $\alpha \in \phi(V)/\phi(U)$ von f bzw. Nebenklassen nach U identisch sind. Das hätte man auch direkt nachprüfen können, was aber die Arbeit nicht erleichtert hätte. **q.e.d.**