Wiederholungsblatt zur Gruppentheorie

von Christian Elsholtz, TU Clausthal, WS 1999/2000

Um Ihnen zu helfen, die Gruppentheorie zu wiederholen, stelle ich hier einige wichtige Beispiele und einige Lösungen der Aufgaben zusammen. Definitionen etc. sehen Sie bitte im Skript nach.

Beispiel 1. Wichtigstes Beispiel endlicher Gruppen sind die zyklischen Gruppen.

Sei n eine natürliche Zahl. Dann nehmen Sie einfach ein Element, nennen es g und bilden die Potenzen $g, g^2, g^3, \cdots$. Dann definieren Sie $g^n = e$. Es folgt dann $g^0 = g^n = g^{2n} = \cdots = e$ und entsprechend $g^i = g^{n+i} = g^{2n+i} \cdots$. Es gelten Rechenregeln wie $(g^i)^{-1} = g^{-i} = g^{n-i}$ und $g^i g^j = g^{i+j}$.

Insbesondere gibt es also für jede natürliche Zahl n eine (und bis auf Isomorphie genau eine!) zyklische Gruppe mit n Elementen.

Sie können die Gruppe auch additiv darstellen, das ist dann so, als ob Sie in obiger multiplikativer Schreibweise nur mit dem Exponenten rechnen. Sei $\mathbb{Z}_n = \{0, 1, \cdots, n-1\}$ versehen mit der Addition modulo n. Dann ergibt sich die gleiche Gruppe.

Es gibt zu jedem n bis auf Isomorphie genau eine zyklische Gruppe. Daher ist es egal, ob Sie für die zyklische Gruppe der Ordnung n nun C_n oder $(\mathbb{Z}_n, +)$ schreiben.

Wenn Sie ALLE zyklischen Gruppen aufzählen wollen, dürfen Sie aber die einzige unendliche zyklische Gruppe $(\mathbb{Z}, +)$ nicht vergessen! Die endlichen Gruppen sind homomorphe Bilder von $(\mathbb{Z}, +)$. (Vergleiche große Übung 2, Aufgabe 3 und Blatt 3, Aufgabe 3.)

Das Beispiel der $\mathbb{Z}_n$ kann natürlich auch zum Beispiel für Ringe ausgebaut werden. $(\mathbb{Z}_n, +, \cdot)$ ist ein Ring. Falls n eine Primzahl ist, (und nur dann!), ist $(\mathbb{Z}_n, +, \cdot)$ sogar ein Körper.

Beispiel 2. Weitere wichtige Beispiele endlicher Gruppen sind die symmetrischen und die alternierenden Gruppen. Diese sind im allgemeinen nicht abelsch. (Nur S_1, S_2, A_1, A_2, A_3 sind abelsch.)

Die Gruppe S_3 besteht z.B. aus den folgenden Permutationen:

$$S_3 = \{(id), (1,2), (1,3), (2,3), (1,2,3), (1,3,2)\}.$$

Hiervon sind $(1,2), (1,3)$ und $(2,3)$ ungerade Permutationen, aber $(1,2,3) = (1,3)(1,2)$ und $(1,3,2) = (1,2)(1,3)$ sind gerade Permutationen. (Achtung, von rechts nach links multiplizieren!) Also ist $A_3 = ((id), (1,2,3), (1,3,2)\}$.

Übung: Stellen Sie die Multiplikationstabelle von S_3 auf!

Beispiel 3. Der kleine Satz von Fermat für endliche Gruppen: Ein beliebiges Element hoch die Gruppenordnung ergibt das neutrale Element: $a^{|G|} = e$.
Der Satz von Lagrange: Die Ordnung einer Untergruppe (das heißt die Anzahl der Elemente der Untergruppe) teilt die Gruppenordnung. Da jedes einzelne Element aber auch eine Untergruppe erzeugt, (man nehme die Potenzen so lange, bis man das neutrale Element erhält), teilt auch die Ordnung eines Elementes (und das ist der kleinste derartige Exponent!) die Gesamtgruppenordnung.

Beispiel a): $|A_n| = n!/2$ (für $n \geq 2$). und $|S_n| = n!$. Natürlich ist $n!/2$ ein Teiler von $n!$.
Beispiel b): In $(\mathbb{Z}_6, +)$ hat 2 die Ordnung 3. Und 3 ist ein Teiler von 6.

Achtung, die Umkehrung ist im allgemeinen falsch. Das heißt, zu einem Teiler der Gruppenordnung gibt es nicht unbedingt eine Untergruppe mit dieser Ordnung, oder ein Element mit dieser Ordnung. So hat z.B. die Gruppe S_4 die Ordnung 24, aber es gibt kein Element der Ordnung 8.

Nur in einem speziellen Fall haben wir eine Umkehrung bewiesen! Ist nämlich die Gruppenordnung gerade, so gibt es ein Element der Ordnung 2, (und daher auch eine Untergruppe der Ordnung 2). Siehe unten.

Allgemeiner gilt für Primzahlen p (aber das haben wir nur für $p = 2$ bewiesen!): Ist p ein Teiler der Gruppenordnung $|G|$, dann gibt es ein Element mit Ordnung p.

Es folgen einige der behandelten Aufgaben mit Lösungen.
Kleine Übung 3, Aufgabe 1.
Es sei $f \in S_7$, $f = (1,2,3,4,5) \circ (1,2,7)$. Man bestimme:
a) Die Darstellung von f als Produkt disjunkter Zyklen.
b) $sgn f$.
c) f^{-2}.
d) $|[f]|$.

Lösung: a) In der Darstellung von f kommt die 1 und die 2 mehrfach vor. Gesucht ist eine Darstellung, wo jedes Element höchstens einmal vorkommt. Wir berechnen, wie f auf die Elemente wirkt. Von rechts multiplizieren, also $1 \to 2 \to 3, 2 \to 7, 3 \to 4, 4 \to 5, 5 \to 1, 7 \to 1 \to 2$.

Jetzt fängt man mit einem Element an, z.B. der 1. Die 1 geht auf die 3, diese wiederum auf die 4, diese auf die 5 und die 5 wird auf die 1 abgebildet. Also ist $(1,3,4,5)$ ein Zykel. Dann nehmen wir 2, weil 2 noch nicht vorkam; 2 geht auf 7 und 7 wieder auf 2, also ist $(2,7)$ der nächste Zykel. Die 6 ist von dieser Abbildung nicht betroffen. Man braucht sie dann nicht hinschreiben. Also $f = (1,3,4,5)(2,7) = (2,7)(1,3,4,5)$.
Bemerkung: Bei disjunkten Zyklen ist die Reihenfolge egal, bei nicht-disjunkten Zyklen kommt es hingegen auf die Reihenfolge an!

b) $f = (1,3)(3,4)(4,5)(2,7)$. Das sind 4 Transpositionen, also sgn $f = (-1)^4 = 1$.

c) Zykel invertieren heißt, die Reihenfolge umkehren (nachrechnen!!). Also $f^{-1} = (5,4,3,1)(2,7)$ oder auch $(1,5,4,3)(2,7)$.

d) Man betrachte die Potenzen von f.

$$f^0 = id, f^1 = (1,3,4,5)(2,7), f^2 = (1,4)(3,5), f^3 = (1,5,4,3)(2,7), f^4 = id.$$

$[f] = \{f, f^2, f^3, f^4\}$, also $|[f]| = 4$.

Kleine Übung 3, Aufgabe 3.
a) Man beweise: Für alle Elemente a der Gruppe G sei $a^2 = e$. Dann ist G abelsch.
b) Formulieren Sie die Umkehrung der Aussage in a). Beweisen oder widerlegen Sie diese Umkehrung.
c) Sei G eine endliche abelsche Gruppe. Man beweise, daß dann $\prod_{g \in G} g^2 = e$ gilt. Wenn $|G|$ ungerade ist, dann gilt sogar $\prod_{g \in G} g = e$.
d) Sei G eine endliche Gruppe. (G muß also nicht abelsch sein.) Falls $|G|$ gerade ist, dann gibt es ein $g \in G, g \neq e$, so daß $g^2 = e$ gilt.

Lösung:
Ein Beispiel für eine solche Gruppe ist die Gruppe $C_2 \times C_2$, siehe unten.

a) Beh. ($\forall a \in G$ gilt $a^2 = e$) $\Rightarrow$ (G ist abelsch).
Beweis: Wir zeigen für beliebiges $x, y \in G : xy = yx$.

$$\begin{array}{lcll} (xy)(xy) & = & e & \text{von links mit } x \text{ multiplizieren.} \\ x^2yxy & = & x & \\ yxy & = & x & \text{von rechts mit } y \text{ multiplizieren.} \\ yxy^2 & = & xy & \\ yx & = & xy. & \end{array}$$

b) Umkehrung: Nur den Pfeil umdrehen, also

($\forall a \in G$ gilt $a^2 = e$) $\Leftarrow$ (G ist abelsch)
bzw.
(G ist abelsch) $\Rightarrow$ ($\forall a \in G$ gilt $a^2 = e$).

Schon die zyklische Gruppe mit drei Elementen, also $C_3 = \{e, g, g^2\}$, ist ein Gegenbeispiel, sie ist abelsch, aber es gilt nicht $g^2 = e$.

c) Die Umkehrung gilt nach b) nicht, hier wird eine Art sehr schwacher Umkehrung bewiesen. (wenn man die Umkehrung hätte, wäre diese Aussage völlig klar.)

Vorbemerkung: falls $|G|$ ungerade ist, dann gibt es kein Element g mit $g^2 = e$. Dann wäre nämlich $\{e, g\}$ eine Untergruppe und nach dem Satz von Lagrange müßte die Gruppenordnung gerade sein. Also sind in Gruppen mit ungerader Ordnung g und g^{-1} verschiedene Elemente. Für Gruppen mit gerader Ordnung kann es aber Elemente der Ordnung 2 geben, (siehe d). Diese nennen wir $h_1, ...h_k$, wobei wir $k = 0$ erlauben, wenn es solche Elemente gar nicht gibt.

Sei $G = \{g_1 = e, g_2, \cdots, g_n, g_{n+1} = h_1, \cdots, g_{n+k} = h_k\}$, dann ist

$$\begin{array}{lcl} \prod\limits_{g \in G} g^2 & = & e^2 g_2^2 g_3^2 \cdots g_n^2 h_1^2 \cdots h_k^2 \text{ umsortieren erlaubt, da } G \text{ abelsch} \\ & & \text{sortiere jeweils in Paare von einem Element und dem Inversen} \\ & = & \left(e^2 g_2 g_2^{-1} \cdots g_n g_n^{-1} h_1^2 \cdots h_k^2\right) \\ & = & e^2 e^{n-1} e^k = e. \end{array}$$

Man beachte, daß jedes der g_i in der Tat doppelt hingeschrieben wurde, da g und g^{-1} ja verschieden sind!

Falls $|G|$ ungerade ist, fallen die h's weg (s.o.), und man braucht die Elemente ja gerade nicht doppelt hinzuschreiben, sondern man schreibt jeweils Element und Inverses nebeneinander.

$$\begin{array}{lcl} \prod\limits_{g \in G} g & = & e g_2 g_3 \cdots g_n \\ & = & e e^{(n-1)/2} = e. \end{array}$$

d) Dies ist nach obiger Überlegung einfach. Sei $|G|$ gerade. Wenn man die Elemente g mit verschiedenem Inversen $g^{-1} \neq g$ paarweise sortiert, hat man eine gerade Anzahl an Elementen betrachtet. Es bleiben nur noch Elemente, für die $g = g^{-1}$ gilt, also für die die Ordnung 1 oder 2 ist. Das neutrale Element ist das einzige Element mit Ordnung 1, also gibt es eine ungerade Anzahl an Elementen (also mindestens eines!) mit Ordnung 2.

Übung: Machen Sie noch einmal Aufgabe 4 der 3. kleinen Übung.

Große Übung 3, Aufgabe 1.
Unter dem direkten Produkt $G \bigotimes H$ zweier Gruppen G und H versteht man das kartesische Produkt $G \times H$, versehen mit folgender Verknüpfung:

$$(a, b) \cdot (c, d) = (ac, bd).$$

Man zeige:

a) $G \bigotimes H$ ist eine Gruppe.
b) Konstruieren Sie mit Hilfe von a) eine nicht zyklische Gruppe G_1 mit 4 Elementen und eine Gruppe G_2 mit 6 Elementen. (Bemerkung: Es gilt $G_1 = C_2 \times C_2 \not\simeq C_4$ aber $G_2 = C_2 \times C_3 \simeq C_6$.)
c) Geben Sie alle (nichtisomorphen) Gruppen mit höchstens 7 Elementen an.

Lösung:
Wir rechnen komponentenweise. Da in jeder Komponente alle Gesetze gelten, folgen sie auch für beide Komponenten gleichzeitig. Man beachte, daß in $(a, b) \cdot (c, d) = (ac, bd)$ drei verschiedene Verknüpfungen vorkommen. Eigentlich müßte man $(a, b) \cdot_1 (c, d) = (a \cdot_2 c, b \cdot_3 d)$ schreiben, wobei die Verknüpfung $\cdot_1$ in $G \bigotimes H$ liegt, aber $\cdot_2$ in G und $\cdot_3$ in H liegt! Aber so will man es natürlich nicht immer schreiben, da klar ist, in welcher Gruppe die jeweiligen Verknüpfungen operieren. Genauso schreibt man für das direkte Produkt meist nur $G \times H$, wenn von dem Zusammenhang her klar ist, daß man von der Gruppe $G \bigotimes H$ redet, und nicht nur von dem kartesischen Produkt $G \times H$.

a) Abgeschlossenheit: $(g_1, h_1)(g_2, h_2) = (g_1 g_2, h_1 h_2) \in G \bigotimes H$.
neutrales Element: (e_G, e_H), (nachrechnen!)
inverses Element: Zu (g, h) ist (g^{-1}, h^{-1}) invers, (nachrechnen!)
Assoziativität:

$$\begin{aligned}
((g_1, h_1)(g_2, h_2))\,(g_3, h_3) &= (g_1 g_2, h_1 h_2)(g_3, h_3) \\
&= ((g_1 g_2) g_3), ((h_1 h_2) h_3) \\
&= (g_1 (g_2 g_3)), (h_1 (h_2 h_3)) \\
&= (g_1, h_1)(g_2 g_3, h_2 h_3) \\
&= (g_1, h_1)\,((g_2, h_2)(g_3, h_3))\,.
\end{aligned}$$

b) Für endliche Gruppen G und H gilt: $|G \bigotimes H| = |G| \cdot |H|$.

Kennt man also Gruppen mit m und n Elementen, kann man Gruppen mit mn Elementen konstruieren.

Es ist $C_2 \times C_2 \simeq (\mathbb{Z}_2, +) \times (\mathbb{Z}_2, +) = (\{(0,0), (0,1), (1,0), (1,1)\}, \cdot)$. Man rechnet in jeder Komponente additiv modulo 2. Die Gruppenverknüpfung ist also:

$\cdot$	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
$(0,0)$	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
$(1,0)$	$(1,0)$	$(0,0)$	$(1,1)$	$(0,1)$
$(0,1)$	$(0,1)$	$(1,1)$	$(0,0)$	$(1,0)$
$(1,1)$	$(1,1)$	$(0,1)$	$(1,0)$	$(0,0)$

Diese Gruppe ist nicht isomorph zu der zyklischen Gruppe mit 4 Elementen, C_4. Denn in C_4 gibt es zwei Elemente der Ordnung 4, aber in $C_2 \times C_2$ haben alle Elemente Ordung 1 oder 2. (Vergleiche die Diagonale!)

Analog folgt für $C_2 \times C_3$: Die Gruppe hat 6 Elemente:

$$C_2 \times C_3 \simeq (\mathbb{Z}_2, +) \times (\mathbb{Z}_3, +) = (\{(0,0),(0,1),(0,2),(1,0),(1,1),(1,2)\}, \cdot)\,.$$

Die Verknüpfungstafel berechnet man leicht, indem man in der ersten Komponente additiv modulo 2, in der zweiten Komponente modulo 3 rechnet.

$\cdot$	$(0,0)$	$(0,1)$	$(0,2)$	$(1,0)$	$(1,1)$	$(1,2)$
$(0,0)$	$(0,0)$	$(0,1)$	$(0,2)$	$(1,0)$	$(1,1)$	$(1,2)$
$(0,1)$	$(0,1)$	$(0,2)$	$(0,0)$	$(1,1)$	$(1,2)$	$(1,0)$
$(0,2)$	$(0,2)$	$(0,0)$	$(0,1)$	$(1,2)$	$(1,0)$	$(1,1)$
$(1,0)$	$(1,0)$	$(1,1)$	$(1,2)$	$(0,0)$	$(0,1)$	$(0,2)$
$(1,1)$	$(1,1)$	$(1,2)$	$(1,0)$	$(0,1)$	$(0,2)$	$(0,0)$
$(1,2)$	$(1,2)$	$(1,0)$	$(1,1)$	$(0,2)$	$(0,0)$	$(0,1)$

Diese Gruppe ist jedoch zyklisch. Die Vielfachen von $(1,1)$ erzeugen die ganze Gruppe. $(1,1), (1,1)\cdot(1,1) = (0,2), (1,1)\cdot(1,1)\cdot(1,1) = (1,0)$, etc. $(0,1), (1,2), (0,0)$.

Allgemein besagt der Chinesische Restsatz (ohne Beweis!): Falls m und n teilerfremd sind, dann gilt $C_{mn} \simeq C_m \times C_n$. In diesem Spezialfall haben wir bewiesen: $C_6 \simeq C_2 \times C_3$.

c) Eine Auflistung aller kleinen Gruppen ergibt sich wie folgt. Es gibt immer die zyklische Gruppe $C_n = (\mathbb{Z}_n, +)$. Und alle zyklischen Gruppen derselben Ordnung sind isomorph. Für Primzahlordnung kann es außer der zyklischen Gruppe keine weitere Gruppe geben. (Kleine Übung 3, Aufgabe 4). Für die Ordnung 4 und 6 muß man versuchen, alle möglichen Gruppentafeln aufzustellen, die die Axiome erfüllen. Überlegen Sie sich, daß dazu z.B. in jeder Zeile und in jeder Spalte jedes Element genau einmal vorkommen muß. Versuchen Sie es noch einmal für die Ordnung 4. Bei der Ordnung 6 ist es ganz schön mühsam! Es ergibt sich, daß außer den bereits bekannten Gruppen keine weitere Gruppe mit 4 Elementen existiert, und für 6 Elemente kommt noch eine weitere hinzu, die isomorph zu der Gruppe S_3 ist.

Ordnung 1: C_1.
Ordnung 2: C_2.
Ordnung 3: $C_3 = A_3$.
Ordnung 4: $C_4, C_2 \times C_2$.
Ordnung 5: C_5.
Ordnung 6: $C_6 = C_2 \times C_3, S_3$.
Ordnung 7: C_7.

Es gibt 5 verschiedene Gruppen mit Ordnung 8. Und für große Ordnungen wird das noch viel komplizierter.

Übung: Stellen Sie die Verknüpfungstafel der Gruppe S_3 auf, falls Sie es nicht schon oben gemacht haben, und zeigen Sie, daß die Gruppe nicht isomorph zu der zyklischen Gruppe ist.

$\cdot$	(id)	(123)	(132)	(12)	(13)	(23)
(id)						
(123)						
(132)						
(12)						
(13)						
(23)						