Endliche Gruppen

Thomas Keilen
Fachbereich Mathematik
Universität Kaiserslautern

Skript zum Proseminar im WS 2000/01

August 1997 / Juni 2000 / Januar 2001

Inhaltsverzeichnis

Vorwort zur ersten Auflage

Allen Zweigen der Mathmatik ist eines gemeinsam, sie beschäftigen sich mit der Analyse von Objekten, die sich durch gewisse Strukturen auszeichnen. Wie diese Strukturen im jeweiligen Falle aussehen, variiert sehr stark. Die für den Bereich der Algebra grundlegendste Struktur dürfte wohl die der Gruppe sein, die trotz - oder gerade wegen - ihrer Einfachheit eine große Vielfalt zuläßt. Wann immer man sich nun mit Objekten beschäftigt, betrachtet man auch Abbildungen zwischen diesen. Haben die Objekte eine gegebene Struktur, so ist es natürlich, nur solche Abbildungen zu betrachten, die diese Struktur respektieren, sog. (Homo-)Morphismen. Besitzt ein solcher Homomorphismus nun eine eindeutige Umkehrabbildung, die ihrerseits wieder ein Homomorphismus ist, so nennt man sie einen Isomorphismus, und Objekte, die isomorph sind, wird man im folgenden nicht mehr als verschieden ansehen wollen. Das ist insofern durchaus sinnvoll, als für gewöhnlich von Objekten nur solche Eigenschaften betrachtet werden, die unter Isomorphismen erhalten bleiben. Man faßt also isomorphe Objekte zu einer Isomorphieklasse oder einem Isomorphietypen - wenn man so will, einer neuen Art von Objekten - zusammen, identifiziert dabei aber meist stillschweigend die Elemente einer Isomorphieklasse mit der ganzen Klasse. Hat man sich einmal auf dieses Konzept eingelassen, dann ist der Wunsch, alle Objekte mit der zu betrachtenden Struktur, kennenzulernen, ganz natürlich, und man spricht davon, die Objekte zu *klassifizieren*. Für uns würde das bedeuten, wir wollen alle Gruppen - oder genauer, alle Isomorphietypen von Gruppen - kennenlernen, sie klassifizieren - ein hoffnungsloses Unterfangen. Wir werden uns mit weniger zufrieden geben müssen, sogar mit viel weniger.

Als gute Mathematiker gehen wir nun nicht kopflos, sondern mit System an die Aufgabe heran. Wir unterteilen die Gesamtklasse der Objekte, die uns interessiert - d. h. die Klasse aller (Isomorphietypen von) Gruppen in - mehr oder weniger - sinnvolle Unterklassen. Eine Möglichkeit, dies zu tun, ist die, nach der Anzahl der Elemente zu fragen, die eine Gruppe besitzt - der sog. Ordnung der Gruppe -, und so zwischen endlichen und unendlichen Gruppen zu unterscheiden. Diese Einteilung ist in der Tat sehr sinnvoll, da die beiden Unterklassen sehr unterschiedliche Untersuchungsmethoden erfordern. Hingegen ist die von uns gewählte Methode, die endlichen Gruppen dann weiter nach ihrer Ordnung in Unterklassen einzuteilen, sehr willkürlich, und wohl allein für unser Ziel geeignet, mit dem Begriff der Gruppe und mit einfachen Klassifikationsmethoden vertraut zu werden. Am Ende des Kurses sollten jedem Seminarteilnehmer die endlichen Gruppen sympathisch geworden sein, und er sollte das Gefühl haben, daß die von Mathematikern so sehr erwartete Fähigkeit des analytischen Denkens, ein wenig geschult wurde.

Nun, zu Beginn habe ich erwähnt, daß die Struktur der Gruppe in der *Algebra* von grundlegender Bedeutung ist. Das könnte den Eindruck vermitteln, daß sie für andere Felder der Mathematik nicht von Interesse sei. Dem ist aber durchaus nicht so. Die Gruppen gehören zu den wenigen Strukturen, die in nahezu allen Bereichen der Mathematik eine wichtige Rolle spielen, und das hat einen guten Grund. Sie besitzen die *Fähigkeit*, auf andersartigen Objekten zu *operieren*, das soll heißen, sie treten - häufig in ganz natürlicher Weise - als Mengen von (Auto-)Morphismen von Objekten mit zum Teil völlig anderer Struktur in Erscheinung. So kennen wir zum Beispiel die $Gl_n(K)$, die Gruppe der invertierbaren $n \times n$-Matrizen über einem Körper K, zugleich als Menge von (linearen) Automorphismen des Vektorraumes K^n; die Elemente der $Gl_n(K)$ *operieren* also auf dem Vektorraum K^n. Interessiert man sich etwas näher für Mathematik, so wird man demnach gar nicht umhinkommen, sich mit dem Begriff der Gruppe etwas anzufreunden, und dazu besteht hier die Möglichkeit.

Abschließend noch einige Bemerkungen zum Seminar selbst und zu diesem Skript. Für manche wird es das erste Mal sein, daß sie an einem Seminar teilnehmen, andere haben bereits Erfahrungen gesammelt. Mag sein, daß erstere sich an letzteren orientieren, was ihr Verhalten betrifft, so wie diese sich vielleicht an ihren Vorgängern orientiert haben. Das könnte dazu führen, daß das Seminar verläuft wie schon manch anderes, an dem ich teilgenommen habe - nämlich stumm von Seiten der Zuhörer. Das sollte nicht sein. Es ist nicht zu erwarten, daß man dem, was der Vortragende erzählt und anschreibt, stets folgen kann, und dazu sollte man getrost stehen. Weder wirft eine Frage ein schlechtes Licht auf den, der fragt, noch bringt man den, der vorträgt, in Verlegenheit, falls er keine Antwort weiß. Mathematik erfordert *Diskussion*, und die Seminare sind die Orte, an denen man das *Diskutieren*, das *Sich-Verständigen*, über mathematische Inhalte lernen kann. Diese Gelegenheit sollte genutzt werden - und sie ist es ggf. wert, auf Inhalte zu verzichten.

Für die einzelnen Vorträge stehen jeweils 90 Minuten zur Verfügung, die voll genutzt werden können, über die aber nicht hinausgegangen werden sollte. Zu den didaktischen Zielen des Seminars gehört es auch, eine sinnvolle Auswahl an Inhalten zu treffen und den darzubietenden Stoff zu straffen. Der Einsatz eines Overheadprojektors, kann Zeit einsparen, aber man sollte sich stets bewußt sein, daß es für die Zuhörer weit schwerer ist, einem schnellen Ritt über fertige Ergebnisse auf einer Folie zu folgen, als der meist weit langsameren Entwicklung selbiger Resultate an der Tafel. Von daher ist eher davon abzuraten, Beweise in allen Details auf Folien vorzubereiten, während es durchaus sinnvoll sein kann, grobe Raster von Beweisen auf diese Art zu präsentieren oder Ergebnisse, auf die mehrfach zurückgegriffen werden muß, so leicht verfügbar zu machen. Den Ideen und Phantasien für eine gute und ansprechende Präsentation sind sicher keine Grenzen gesetzt, und ich würde diesbezüglich gerne von den Teilnehmern lernen.

Zuletzt also noch ein Wort zu dem vorliegenden Skript. Es ist in den vergangenen vier Wochen rasch und in einiger Zeitnot niedergeschrieben worden. Als Grundlage diente für weite Teile eine Vorlesung, die ich vor einigen Jahren bei Herrn Klaus Doerk in Mainz gehört habe. Danken möchte ich Florentine Bunke und Mathias Schulze sowie allen anderen, die mir geholfen haben, die vielen kleinen und großen Unkorrektheiten des Werkes zu beseitigen. Fehler, die das Skript nun noch enthält - und derer sind es zweifelsohne immer noch etliche - obliegen dennoch alleine meiner Verantwortung, und für Hinweise, die zur Ergreifung selbiger Fehler führen, wird eine Belohnung von zehn Gummibärchen je Fehler ausgesetzt. So bleibt mir nur, den Leser um Nachsicht zu bitten, und ihm beim Lesen ein *hinreichendes* Vergnügen zu wünschen.

Thomas Keilen Kaiserslautern, den 04. September 1997

VORWORT ZUR DRITTEN AUFLAGE

Ein Proseminar baut stets auf den Grundvorlesungen auf, die die Teilnehmer besucht haben. Für den zweiten Jahrgang, der dieses Skript verwendet hat, sind deshalb in den Kapiteln fünf und zehn Änderungen erforderlich gewesen. Während des Seminars sind zudem viele - zum Teil gravierende - Fehler zutage getreten, die unter anderem eine gründliche Überarbeitung der Kapitel sechs und sieben bedingten. Schließlich ist ein Mangel des Skriptes zutage getreten, der zwingend Abhilfe einforderte: die Teilnehmer lernten nicht wirklich Beispiele endlicher Gruppen kennen. Dies alles führte zu der vorliegenden dritten Fassung des Skriptes. Dabei begegne ich dem Mangel an Beispielen durch eine Änderung des Konzeptes, die ich mir bei Stefan Nickel entleihe. Am Ende eines jeden Kapitels befinden sich einige Aufgaben, die von den Teilnehmern des Seminars jeweils bis zum folgenden Vortrag zu bearbeiten sind. Jedem Teilnehmer obliegt es dann, die Lösungsvorschläge seiner Kommilitonen zu den Aufgaben seines Vortrags zu korrigieren, dem Leiter des Seminars vor Rückgabe zur Einsicht vorzulegen und für die Teilnehmer eine Musterlösung der Aufgaben zu erstellen. Bei den Aufgaben handelt es sich ausschließlich um Beispiele zu den bis dahin eingeführten Begriffen, so daß ich hoffe, auf diese Weise dem oben beschriebenen Mangel Abhilfe schaffen zu können. Zudem sollten die Aufgaben für die Teilnehmer der Veranstaltung einen zusätlichen Anreiz bieten, sich am Seminar auch über den eigenen Vortrag hinaus zu beteiligen. Und schließlich dürfte die Erfahrung, sich mit den Lösungen der Aufgaben und ihrer Korrektur auseinandersetzen zu müssen, für den Vortragen in vielerlei Hinsicht eine lehrreiche Erfahrung sein.

Thomas Keilen Kaiserslautern, den 22. Januar 2001

0 GRUNDLEGENDE BEGRIFFE

0.1 Allgemeine Hinweise

a. Nachdem wir den Begriff der Gruppe mit einem Minumum an erforderlichen Axiomen eingeführt haben, wird eine Reihe von wohlbekannten Beispielen von Gruppen betrachtet, die zum Teil auch in späteren Kapiteln wieder aufgegriffen werden. In Satz 0.5 werden dann erste einfache Folgerungen aus der Definition gezogen, die den Umgang mit Gruppen wesentlich erleichtern. Im zweiten Teil des Kapitels wollen wirTeilmengen von Gruppen betrachten, auf die sich die Struktur der Gruppe überträgt. Es wird ferner untersucht, wie sich solche *Untergruppen* bei Schnitt und Vereinigung verhalten, und wie man aus einer beliebigen Teilmenge eine Untergruppe gewinnen kann.

b. Eine ausführliche Darstellung der in diesem Kapitel aufgeführten Definitionen und Sätze findet sich in [Hup69] Kapitel I. § 1 und § 2 sowie in [Hup67] Kapitel I. § 1 und § 2. Die hier benutzten Notationen orientieren sich jedoch stärker an [Doe72] II.1.6-1.15 sowie [Doe74] Kapitel VII. § 1. Die ausführlichste Darstellung mit einer Vielzahl von Beispielen bietet zweifellos [Hum96] §§ 1-4.

c. Alle in diesem Kapitel gegebenen Definitionen, Sätze und Beispiele sollen im Vortrag auch dargeboten werden. Die Beweise der Aussagen in Satz 0.5 sind bereits Bestandteil der Vorlesung Lineare Algebra I gewesen und sollten nur dann in den Vortrag integriert werden, wenn die Zeit dies erlaubt. Gleiches gilt für ausführlichere Beweise bei den Beispielen.

0.2 Definition

Eine **Gruppe** $(G, \circ)$ ist eine nicht leere Menge G zusammen mit einer Verknüpfung $\circ : G \times G \to G$, so daß folgende Axiome erfüllt sind:

(i) $g \circ (h \circ k) = (g \circ h) \circ k$ für alle $g, h, k \in G$ (Assoziativität)

(ii) $\exists\, e \in G : e \circ g = g$ für alle $g \in G$ (Existenz eines Linksneutralen)

(iii) $\forall\, g \in G\ \exists\, h \in G : h \circ g = e$ (Existenz von Linksinversen)

Gilt ferner $g \circ h = h \circ g$ für alle $g, h \in G$, so heißt die Gruppe G **abelsch**.
Ist $|G| < \infty$, so heißt die Gruppe G **endlich**, und $|G|$ heißt die **Ordnung** von G.

0.3 Notation

Statt $g \circ h$ werden wir fortan meist kurz gh (oder $g \cdot h$) schreiben und von der Gruppen*multiplikation* sprechen. Abelsche Gruppen werden für gewöhnlich *additiv* geschrieben - $(G, +)$.

0.4 Beispiel

a. Ist $(R, +, \cdot)$ ein Ring, so ist $(R, +)$ eine abelsche Gruppe.
Insbesondere: $(\mathbb{Z}, +)$ und $(K, +)$, wenn K ein Körper ist.

b. Ist $(R, +, \cdot)$ ein Ring und $R^* := \{r \in R \mid r \text{ ist Einheit}\}$, dann ist $(R^*, \cdot)$ eine (i. a. nicht abelsche) Gruppe.
Insbesondere: $(K^* = K \backslash \{0\}, \cdot)$, wenn K ein Körper ist.

c. Ist $(R, +, \cdot)$ ein Ring und $(M, +, \cdot)$ ein R-Modul, so ist $(M, +)$ eine abelsche Gruppe, und es gilt sogar: die additiven Gruppen der $\mathbb{Z} - Moduln$ sind genau die abelschen Gruppen.

d. Ist R ein Ring, dann ist der Ring der $n \times n$-Matrizen $(\mathrm{Mat}(n \times n, R), +)$ ein weiteres Beispiel entsprechend Teil a.

e. Ist K ein Körper, so bilden die regulären $n \times n$-Matrizen über K bezüglich der Matrizenmultiplikation ein weiteres Beispiel entsprechend Teil b - $(\mathrm{Gl}_n(K) := \{A \in \mathrm{Mat}(n \times n, K) \mid \det(A) \neq 0\}, \circ)$.
Ist speziell $K = GF(q)$ - *der* Körper mit $q = p^k$ Elementen (p Primzahl) -, so schreiben wir statt $\mathrm{Gl}_n(K)$ auch $\mathrm{Gl}_n(q)$ und diese Gruppe ist endlich der Ordnung $|\mathrm{Gl}_n(q)| = (q^n - 1)(q^n - q) \cdots (q^n - q^{n-1})$.
Insbesondere ist $\mathrm{Gl}_2(2)$ eine nicht abelsche Gruppe der Ordnung 6.
(Vgl. [Hum96] 23.2-23.4.)

f. Es sei Ω eine Menge und $\mathbb{S}(\Omega)$ die Menge der Bijektionen von Ω in sich selbst. Dann ist $\mathbb{S}(\Omega)$ mit der Komposition von Abbildungen als Verknüpfung eine Gruppe, und die Elemente von $\mathbb{S}(\Omega)$ nennen wir **Permutationen**.
Ist speziell $\Omega = \{1, \ldots, n\}$, so schreiben wir statt $\mathbb{S}(\Omega)$ auch $\mathbb{S}_n$ und sprechen von der **symmetrischen Gruppe** vom Grad n.

0.5 Satz

In einer Gruppe G *gelten die folgenden Aussagen:*

a. *Ist* $e \in G$ *ein linksneutrales Element, so gilt* $ge = g$ *für alle* $g \in G$. *(Linksneutrales=Rechtsneutrales)*

b. *Es gibt genau ein Element* $e \in G$ *mit* $eg = g$ *für alle* $g \in G$. *(Eindeutigkeit des neutralen Elements)*

c. *Sind* $g, h \in G$ *mit* $gh = e$*, so gilt* $hg = e$. *(Linksinverse=Rechtsinverse)*

d. *Zu* $g \in G$ *gibt es genau ein* $h \in G$ *mit* $hg = e$. *(Eindeutigkeit der Inversen)*

e. *Sind* $g, h, k \in G$*, so folgt aus* $kg = kh$ *stets* $g = h$. *(Kürzungsregel)*

f. *Sind* $g, h \in G$*, so gilt:* $(gh)^{-1} = h^{-1}g^{-1}$ *und* $(g^{-1})^{-1} = g$.

g. *Definieren wir* $g^0 := e$ *und rekursiv* $g^{i+1} := g^i \cdot g$ *sowie* $g^{-i} := (g^i)^{-1}$ *für* $i \in \mathbb{N}_0$*, so gilt für alle* $i, j \in \mathbb{Z}$*:* $g^i \cdot g^j = g^{(i+j)}$. *(Potenzgesetze)*

Beweis: Vgl. auch: [Hup67] I.1.3-1.6 oder [Hum96] § 3. □

0.6 Definition

Es sei $(G, \circ)$ eine Gruppe, $\emptyset \neq U \subseteq G$ eine Teilmenge.
U heißt **Untergruppe** von G, falls U bezüglich der Verknüpfung $\circ$ selbst eine Gruppe ist. Wir schreiben hierfür: $U \leq G$ (bzw. $U < G$, falls sicher gilt $U \neq G$).

Eine Untergruppe $U < G$ heißt **maximal**, falls aus $U < V \leq G$ stets $V = G$ folgt. In diesem Fall schreiben wir kurz: $U \lessdot G$.

0.7 Satz
Es sei G *eine Gruppe,* $\emptyset \neq U \subseteq G$ *eine Teilmenge.*
Die folgenden Aussagen sind äquivalent:

a. U *ist eine Untergruppe von* G.

b. *Für alle* $u, v \in U$ *gilt:*
   (i) $u \cdot v \in U$ *(Abgeschlossenheit bez. "·")*
   (ii) $u^{-1} \in U$ *(Abgeschlossenheit bez. Inversion)*

c. *Für alle* $u, v \in U$ *gilt* $u \cdot v^{-1} \in U$.

d. *(Falls* $|U| < \infty$*!) Für* $u, v \in U$ *gilt* $u \cdot v \in U$.

Beweis: Vgl. [Doe74] VII.1.2 - 1.4, [Hum96] 4.2 + Remark 4, [Hup67] I.2.1-2.2 oder [Kur77] 1.2. □

0.8 Beispiel

a. Eine Gruppe G hat stets die trivialen Untergruppen G und $\mathbb{1} := \{e\}$.

b. Die Untergruppen von $(\mathbb{Z}, +)$ entsprechen genau den Idealen des Ringes $(\mathbb{Z}, +, \cdot)$ und haben die Gestalt $n\mathbb{Z} := \{nz \mid z \in \mathbb{Z}\}$ für $n \in \mathbb{Z}$.

c. Es sei K ein Körper.
   Dann ist $\{(a_{ij})_{i,j=1,2} \in Gl_2(K) \mid a_{12} = 0\}$ eine Untergruppe von $Gl_2(K)$.

0.9 Satz
Sei G *eine Gruppe,* $U_1, U_2, U_i \leq G$ *mit* $i \in I$.

a. $\bigcap_{i \in I} U_i \leq G$

b. *Genau dann gilt* $U_1 \cup U_2 \leq G$, *wenn* $U_1 \subseteq U_2$ *oder* $U_2 \subseteq U_1$.

Beweis: Vgl. [Doe74] VII.1.5 oder [Hup67] I.2.3 sowie [Hum96] 4.6. □

0.10 Beispiel
Sind $n, m \in \mathbb{Z}$ und ist $k := kgV(n, m)$, so ist $n\mathbb{Z} \cap m\mathbb{Z} = k\mathbb{Z}$.

0.11 Definition
Sei G eine Gruppe, $M \subseteq G$ eine Teilmenge von G.
$\langle M \rangle := \bigcap \{U \mid M \subseteq U \leq G\}$ heißt das **Erzeugnis** von M.
Offenbar ist $\langle M \rangle$ die kleinste Untergruppe von G, die M enthält.

0.12 Notation
Ist $(G, +)$ abelsch und sind $U, V \leq G$, so schreiben wir auch $U+V$ statt $\langle U \cup V \rangle$.

0.13 Satz
Ist G *eine Gruppe,* $\emptyset \neq M \subseteq G$.
Dann gilt: $\langle M \rangle = \{m_1^{a_1} \cdots m_n^{a_n} \mid n \in \mathbb{N}, m_1, \ldots, m_n \in M, a_1, \ldots, a_n \in \mathbb{Z}\}$.

Beweis: Vgl. [Doe74] VII.1.7, [Hup67] I.2.4 oder [Kur77] 1.16. □

0.14 Beispiel

a. Sei G eine Gruppe. $\langle\emptyset\rangle = \mathbb{1}$.

b. Seien wieder $n, m \in \mathbb{Z}$ und $g := \mathrm{ggT}(n, m)$, so gilt $n\mathbb{Z} + m\mathbb{Z} = g\mathbb{Z}$.

AUFGABEN

0.15 Aufgabe

Wir definieren die **Diedergruppe** $\mathbb{D}_8$ durch $\mathbb{D}_8 := \left\langle \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right) \right\rangle < \mathrm{Gl}_2(\mathbb{R})$. Man bestimme die Elemente von $\mathbb{D}_8$.

0.16 Aufgabe

Zeige, $\mathbb{Z}_{p^\infty} := \left\{ e^{\frac{2\pi i k}{p^\nu}} \,\middle|\, k \in \mathbb{Z}, \nu \in \mathbb{N} \right\}$ ist eine Untergruppe der multiplikativen Gruppe $(\mathbb{C}^*, \cdot)$ des Körpers $\mathbb{C}$, die sogenannte **Prüfergruppe**, und bestimme die Untergruppen von $\mathbb{Z}_{p^\infty}$.

1 Der Satz von Lagrange

1.1 Allgemeine Hinweise

a. Bei endlichen Gruppen wird die Vielfalt der möglichen Struktur bereits sehr stark durch Ordnung der Gruppe eingeschränkt. Erste wichtige und doch zugleich elementare Ergebnisse bilden die Produktformel und der Satz von Lagrange. Hierfür werden die Begriffe des Produktes sowie der Nebenklassen von Untergruppen eingeführt. Im letzten Teil des Kapitels wird der Begriff der zyklischen Gruppe vorgestellt, und abschließend werden zwei elementare Klassifikationssätze zu zyklischen und abelschen Gruppen bewiesen.

b. Sehr ausführlich wird der Inhalt dieses Kapitels in [Doe74] Kapitel VII. § 1 behandelt sowie in [Hup69] Kapitel I. § 2. Es empfiehlt sich aber, auch einen Blick in [Hum96] § 5, [Kur77] § 1 sowie in [Hup67] Kapitel I. § 2 zu werfen.

c. Alle in diesem Kapitel gegebenen Definitionen, Sätze und Beispiele sollten behandelt werden. Aus Zeitgründen können ggf. die Beweise der Sätze 1.3 sowie 1.12 und u. U. der von Satz 1.4 wegfallen.

1.2 Definition

Es sei G eine Gruppe, $A, B \subseteq G$. Definiere $AB := \{ab \mid a \in A, b \in B\}$.
Also gilt insbesondere $\emptyset A = A\emptyset = \emptyset$. Für $\{g\}A$ schreiben wir auch kurz gA und für $A\{g\}$ kurz Ag.

1.3 Satz

Es sei G *eine Gruppe,* $U, V \leq G$.
Genau dann ist $UV \leq G$*, wenn* $UV = VU$.
In diesem Fall gilt: $UV = \langle U \cup V \rangle$.

Beweis: Vgl. [Doe74] VII.1.10 sowie [Hum96] 5.17. □

1.4 Satz (Produktformel)

Es sei G *eine endliche Gruppe,* $U, V \leq G$.
Dann gilt:

$$|UV| = \frac{|U| \cdot |V|}{|U \cap V|}.$$

Beachte: es ist nicht gefordert, daß UV *eine Untergruppe von* G *ist!*

Beweis: Vgl. [Kur77] 1.4 (wesentlich kürzer), [Doe74] VII.1.22, [Hum96] 5.18 oder [Hup67] I.2.12. Der Beweis sollte erst nach Bemerkung 1.9 geführt werden, da er auf die in Bemerkung 1.5 eingeführten Begriffe zurückgreift. □

1.5 Bemerkung

Es sei G eine Gruppe, $U \leq G$.
Für $g, h \in G$ definieren wir: $g \sim_U h :\Leftrightarrow g^{-1}h \in U$.
Dann ist $\sim_U$ eine Äquivalenzrelation auf G, und die zu $g \in G$ gehörende Äquivalenzklasse hat die Gestalt gU. Wir nennen gU auch **Linksnebenklasse**

von g nach U.
Damit gilt also $G = \bigcup_{g\in G} gU$ sowie entweder $gU \cap hU = \emptyset$ oder $gU = hU$.
Analog liefert die Äquivalenzrelation $g \approx_U h :\Leftrightarrow gh^{-1} \in U$ die **Rechtsnebenklassen** Ug als Äquivalenzklassen, und wieder gilt $G = \bigcup_{g\in G} Ug$ sowie entweder $Ug \cap Uh = \emptyset$ oder $Ug = Uh$.
Man beachte, da für $g \in U$ gilt $gU = U = Ug$, ist U sowohl eine Links-, als auch eine Rechtsnebenklasse. Ferner beachte man, daß i. a. $gU \neq Ug$.
(Vgl. auch [Hum96] 5.3-5.5.)

1.6 Beispiel

Sei $G = Gl_2(2)$, $U = \{(a_{ij})_{i,j=1,2} \in G \mid a_{12} = 0\} = \left\{E, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\right\}$.

Dann erhalten wir folgende Zerlegungen von G in Links- bzw. Rechtsnebenklassen:

$$\begin{aligned} G &= \left\{E, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\right\} \cup \left\{\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}\right\} \cup \left\{\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\right\} \\ &= U \cup \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} U \cup \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} U \end{aligned} \tag{1}$$

und

$$\begin{aligned} G &= \left\{E, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\right\} \cup \left\{\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\right\} \cup \left\{\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}\right\} \\ &= U \cup U\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cup U\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}. \end{aligned} \tag{2}$$

1.7 Definition und Satz

Es sei G eine Gruppe, $U \leq G$.
Dann sind die Menge der Linksnebenklassen von U in G und die Menge der Rechtsnebenklassen gleichmächtig.
Sind diese endlich, so nennen wir ihre Mächtigkeit den **Index** von U in G und schreiben kurz $|G : U|$, ansonsten setzen wir $|G : U| = \infty$.

Beweis: Sei $\mathcal{M} := \{gU \mid g \in G\}$ und $\mathcal{N} := \{Ug \mid g \in G\}$.
Die Abbildung $\alpha : \mathcal{M} \to \mathcal{N} : gU \mapsto Ug^{-1}$ ist wohldefiniert ($gU = hU \Rightarrow g^{-1}h \in U \Rightarrow Ug^{-1}h = U \Rightarrow Ug^{-1} = Uh^{-1}$) und offensichtlich bijektiv ($\alpha^{-1} : \mathcal{N} \to \mathcal{M} : Uh \mapsto h^{-1}U$). Also stimmt die Anzahl der Linksnebenklassen mit der Anzahl der Rechtsnebenklassen überein. (Vgl. auch [Kur77] p. 5.) □

1.8 Theorem (Lagrange)

Es sei G *eine endliche Gruppe,* $U \leq G$.
Dann gilt: $|G| = |G : U| \cdot |U|$.
Insbesondere gilt stets, daß die Ordnung einer Untergruppe die Ordnung der Gesamtgruppe teilt!

Beweis: Vgl. [Doe74] VII.1.18-1.19, [Hum96] 5.9, [Hup69] I.2.13 sowie auch [Hup67] I.2.7. □

1.9 Bemerkung
Dieser Satz schränkt die Zahl der kombinatorisch scheinbar möglichen Untergruppen erheblich ein. So kann beispielsweise die Gruppe $\mathrm{Gl}_2(2)$ nur Untergruppen der Ordnung 1, 2, 3 und 6, nicht aber der Ordnung 4 und 5 enthalten. Es stellt sich unmittelbar die Frage, ob die Umkehrung des Satzes ebenfalls richtig ist, sprich ob eine Gruppe G für jeden Teiler d der Gruppenordnung $|G|$ auch eine Untergruppe U der Ordnung $|U| = d$ besitzt.
Die Antwort ist ja, falls die Gruppe abelsch ist (siehe Korollar 11.12), ist i. a. aber nein (siehe Satz 5.3). Eine teilweise Umkehrung, die in jeder endlichen Gruppe gilt, liefert der Satz von Cauchy (12.2), und weitere Erkenntnisse, die immerhin für eine recht große Klasse von Gruppen gelten, liefert der Satz von Hall (16.16).

1.10 Folgerung
Es sei G *eine endliche Gruppe und* $V \leq U \leq G$.
Dann gilt $|G : V| = |G : U| \cdot |U : V|$.

Beweis: Nach Lagrange gilt $|G : V| = \frac{|G|}{|V|} = \frac{|G|}{|U|} \cdot \frac{|G|}{|V|} = |G : U| \cdot |U : V|$.
(Die Aussage gilt auch, wenn statt $|G| < \infty$ nur $|G : V| < \infty$ vorausgesetzt wird. Vgl. hierzu [Hup67] I.2.6 und [Doe74] VII.1.21.) □

1.11 Definition
Es sei G eine Gruppe, $g \in G$.
Wir setzen $o(g) := |\langle g\rangle|$, falls diese Kardinalität endlich ist, und $o(g) := \infty$ sonst. Sodann bezeichnen wir mit $o(g)$ die **Ordnung** von g.
Gilt $G = \langle g\rangle$, so heißt die Gruppe G **zyklisch**.
Ist $|G| < \infty$, so heißt $\mathrm{Exp}(G) := \mathrm{kgV}\{o(g) \mid g \in G\}$ der **Exponent** von G.

1.12 Satz
Es sei G *eine Gruppe,* $g \in G$ *mit* $o(g) = n < \infty$.
Dann gilt:

a. *Aus* $g^m = e$ *für* $m \in \mathbb{N}$ *folgt* $n \mid m$.
   Insbesondere ist n *die kleinste positive natürliche Zahl* k *mit* $g^k = e$.
b. $\langle g\rangle = \{e, g, g^2, \ldots, g^{n-1}\}$.

Beweis: Vgl. [Hup67] I.2.9 oder [Doe74] VII.4.2 sowie [Hum96] 3.10. □

1.13 Satz
Eine Gruppe von Primzahlordnung ist zyklisch.

Beweis: Vgl. [Hup67] I.2.10 oder [Doe74] VII.4.10 sowie [Hum96] 5.19. □

1.14 Satz
Sei G *eine Gruppe mit* $\mathrm{Exp}(G) = 2$. *Dann ist* G *abelsch.*

Beweis: Seien $g, h \in G$. Dann gilt $o(gh) = 2$, also $(gh)^2 = e$, also $gh = (gh)^{-1} = h^{-1}g^{-1} = hg$. □

1.15 Aufgabe
Bestimme die Elemente der $Gl_2(2)$, ihre Ordnungen und die Untergruppen der Gruppe.

1.16 Aufgabe
Bestimme die Untergruppen der Diedergruppe $\mathbb{D}_8$. (Vgl. [Wei77] Example 4.3.)

2 Normalteiler

2.1 Allgemeine Hinweise

a. In der Theorie der Vektorräume konnte man bezüglich jedes Unterraumes den zugehörigen Faktorraum bilden und auf diese Weise den gegebenen Vektorraum *schrumpfen*. Der neue Vektorraum unterschied sich von dem ursprünglichen im wesentlichen nur durch seine Größe (Dimension). Bei Gruppen sieht das etwas anders aus. Nicht für jede Gruppe würde die Menge der Nebenklassen mit der kanonischen Operation eine Gruppe werden. Dies ist i. a. nur für einen Teil der Untergruppen der Fall, denen man deshalb einen besonderen Namen gibt, und denen dieses Kapitel gewidmet ist. Aber dafür unterscheiden sich die entstehenden Faktorgruppen in ihrer Struktur in aller Regel auch ganz massiv von der Struktur der Ursprungsgruppe. So braucht eine Gruppe, mit einer abelschen Faktorgruppe keineswegs mehr abelsch zu sein. Die Umkehrung gilt natürlich, und in abelschen Gruppen sind auch alle Untergruppen Normalteiler. Ferner gilt für Untergruppen vom Index zwei stets, daß sie Normalteiler sind, ein unscheinbarer Satz, der aber für die Klassifikation von Gruppen von hohem Wert ist. Neben der Einführung der Begriffe Normalteiler und Faktorgruppe sowie einiger Aussagen zu dem Verhalten von Normalteilern bei Schnitten und ähnlichem, findet sich ein Exkurs über einfache Gruppen, die in gewisser Weise das Baumaterial sind, aus dem die anderen Gruppen zusammengesetzt sind. (Letzteres wird klarer, wenn in Kapitel 15 der Begriff der Kompositionsreihe eingeführt ist.)

b. Als Grundlage für dieses Kapitel hat Paragraph zwei in [Doe74] Kapitel VII. gedient. Desgleichen bieten auch [Hum96] § 7, [Hup67] Kapitel I. § 3, [Hup69] Kapitel I. § 4 sowie [Kur77] Kapitel I. § 2 Informationen zu Normalteilern.

c. Alle im folgenden Kapitel aufgeführten Definitionen und Sätze sollten im Vortrag dargeboten und bewiesen werden. Auf die Beispiele sollte hinreichend viel Zeit verwandt werden, die Bemerkung kann entfallen.

2.2 Definition

Es sei G eine Gruppe.
Eine Untergruppe $N \leq G$ heißt **Normalteiler** von G, falls für $g \in G$ stets gilt: $gNg^{-1} \subseteq N$ (d. h. $\forall\, g \in G, n \in N$ gilt $gng^{-1} \in N$).
Wir schreiben dann kurz: $N \trianglelefteq G$ (bzw. $N \triangleleft G$, falls sicher $N \neq G$).

2.3 Satz

Es sei G *eine Gruppe,* $N \leq G$.
Dann sind die folgenden Aussagen äquivalent:

a. *N ist ein Normalteiler von* G.

b. *Für alle* $g \in G$ *ist* $gNg^{-1} = N$.

c. *Für alle* $g \in G$ *ist* $gN = Ng$.

d. *Für alle* $g, h \in G$ *ist* $(gN)(hN) = ghN$.

Beweis: Vgl. [Doe74] VII.2.1, [Hum96] 7.4, [Hup69] I.4.6 oder [Hup67] I.3.2. □

2.4 Beispiel

a. Die trivialen Untergruppen $\mathbb{1}$ und G von G sind stets Normalteiler.

b. In einer abelschen Gruppe sind alle Untergruppen Normalteiler.

c. Die Untergruppe U von $G = \mathrm{Gl}_2(2)$ in Beispiel 1.6 ist kein Normalteiler von G, da offenbar $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} U \neq U \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

Hingegen gilt für $N := \left\langle \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \right\rangle$ nach dem folgenden Satz 2.5 $N \lhd G$.

2.5 Satz
Es sei G *eine Gruppe,* $N < G$ *mit* $|G : N| = 2$.
Dann ist $N \lhd G$.

Beweis: N besitzt außer der trivialen nur je eine weitere Links- bzw. Rechtsnebenklasse. Also stimmen die Rechtsnebenklassen offenbar für jeden Repräsentanten mit den zugehörigen Linksnebenklassen überein. Dann ist aber N ein Normalteiler. (Vgl. [Doe74] VII.2.3 oder [Hup67] I.3.3 sowie [Hum96] 7.6.) □

2.6 Beispiel
Es sei K ein Körper. $(G := \left\{ \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}, \begin{pmatrix} 0 & a \\ a^{-1} & 0 \end{pmatrix} \mid 0 \neq a \in K \right\}, \circ)$ ist eine Untergruppe der $\mathrm{Gl}_2(K)$ und $Z := \left\{ \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \mid 0 \neq a \in K \right\}$ ist ein Normalteiler in G vom Index 2.

2.7 Satz
Es sei G *eine Gruppe,* $N, N_1, N_2 \trianglelefteq G$, $U \leq G$.
Dann gilt:

a. $NU \leq G$

b. $N_1 N_2 \trianglelefteq G$

c. $N \cap U \trianglelefteq U$

d. $N_1 \cap N_2 \trianglelefteq G$

e. *Aus* $N_1 \cap N_2 = \mathbb{1}$ *folgt* $n_1 n_2 = n_2 n_1$ *für alle* $n_i \in N_i$.

Beweis: Vgl. [Hup67] I.3.11-3.13 sowie [Hum96] 7.8-7.10. □

2.8 Definition
Es sei G eine Gruppe. Besitzt G außer den trivialen Normalteilern keine weiteren, so heißt G **einfach**.

2.9 Satz
Eine Gruppe von Primzahlordnung ist einfach.

Beweis: Folgt unmittelbar aus dem Satz von Lagrange (1.8). □

2.10 Bemerkung
"Eines der vorrangigsten Ziele jeder wissenschaftlichen Forschung besteht darin, die »grundlegenden Objekte«zu bestimmen und zu untersuchen, aus denen alle anderen Objekte gebildet sind. In der Biologie sind dies die Zellen (oder vielleicht die Moleküle), in der Chemie die Atome, in der Physik die Elementarteilchen (nach jetzigem Wissensstand die Quarks). Ebenso verhält es sich in vielen Zweigen der Mathematik. Das klassische Beispiel ist die Zahlentheorie mit den Primzahlen als den grundlegenden Bausteinen aller Zahlen [...]. In jedem der genannten Beispiele sind die elementaren Objekte der Theorie »strukturell einfach«, insofern sie im Rahmen der Theorie nicht weiter in kleinere Einheiten der gleichen Art aufgelöst werden können. [...] Die fundamentalen Bausteine der Gruppentheorie sind die »einfachen Gruppen«." (Siehe: [Dev94] p. 140.)
Dieses *vorrangige Ziel* der vollständigen Klassifikation der endlichen einfachen Gruppen, an dem einige hundert Mathematiker über 30 Jahre hinweg intensiv arbeiteten - obwohl bis zum Ende nicht klar war, ob eine vollständige Klassifikation überhaupt möglich sein würde -, wurde 1981 vollendet. Die notwendigen Beweise sind in ca. 500 Artikeln mit zusammen nahezu 15.000 Seiten veröffentlicht worden. Damit stellt der Klassifikationssatz ein Ergebnis dar, das seinesgleichen innerhalb der Mathematik sucht. Die einfachen abelschen Gruppen sind genau die im vorigen Satz 2.9 erwähnten Gruppen von Primzahlordnung (siehe Korollar 10.6), die *einfachsten* nicht abelschen einfachen Gruppen, die alternierenden Gruppen $\mathbb{A}_n$ mit $n \geq 5$ werden wir im folgenden Kapitel kennenlernen (siehe Definition 5.2). Für einen elementaren Beweis, daß $\mathbb{A}_5$ die kleinste nicht abelsche einfache Gruppe ist, siehe [Hum96] 18.12.
Wer mehr über einfache Gruppen erfahren möchte, der greife zu [Gor82], und für die groben Züge der Klassifikation zu [Gor83] und [Gor96]. Einen ersten - sehr lesenswerten - Eindruck vermittelt der Artikel von Keith Devlin ([Dev94] Kapitel 5), dem obiges Zitat entstammt.

2.11 Definition und Satz
Es sei G eine Gruppe, $N \trianglelefteq G$.
Dann wird die Menge der Linksnebenklassen $G/N := \{gN \mid g \in G\}$ durch $(gN) \cdot (hN) := (gh)N$ für $g, h \in G$ zu einer Gruppe, der sog. **Faktorgruppe** von G nach N, mit $|G/N| = |G : N|$, falls der Index von N in G endlich ist.
Das neutrale Element in G/N ist die Linksnebenklasse N und das Inverse zu gN ist $g^{-1}N$.

Beweis: Folgt unmittelbar aus Satz 2.3, vgl. auch [Hum96] 7.11. □

2.12 Beispiel

Sei $G = (\mathbb{Z}, +)$ und $N = n\mathbb{Z}$ mit $n \in \mathbb{Z}$. Dann ist $G/N = \mathbb{Z}/n\mathbb{Z}$ die additive abelsche Gruppe der ganzen Zahlen modulo n.

2.13 Satz

Es sei G *eine Gruppe,* $N \trianglelefteq G$.
Dann sind die folgenden Abbildungen bijektiv:

$$\begin{array}{ccc} \{U \mid U \leq G, N \subseteq U\} & \to & \{\bar{U} \mid \bar{U} \leq G/N\} \\ U & \mapsto & U/N \end{array}$$

und

$$\begin{array}{ccc} \{M \mid M \trianglelefteq G, N \subseteq M\} & \to & \{\bar{M} \mid \bar{M} \trianglelefteq G/N\} \\ M & \mapsto & M/N. \end{array}$$

D. h. die Untergruppen (bzw. Normalteiler) von G/N *entsprechen eineindeutig den Untergruppen (bzw. Normalteilern) von* G*, welche* N *enthalten.*

Beweis: Vgl. [Hum96] 7.14. □

AUFGABEN

2.14 Aufgabe

Bestimme die Normalteiler der Gruppen $\mathrm{Gl}_2(2)$ und $\mathbb{D}_8$. (Vgl. [Wei77] Example 4.2 und 4.5.)

2.15 Aufgabe

Wir nennen $\mathbb{Q}_8 := \left\langle \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & i \\ i & 0 \end{smallmatrix}\right) \right\rangle < \mathrm{Gl}_2(\mathbb{C})$ die **Quaternionengruppe** der Ordnung 8. Man bestimme die Elemente von $\mathbb{Q}_8$ und deren Ordnungen sowie die Untergruppen und Normalteiler der Gruppe. (Vgl. [Wei77] Example 4.4.)

3 Homomorphismen

3.1 Allgemeine Hinweise

a. Wann immer man Objekte mit gewissen Strukturen innerhalb der Mathematik studiert, interessiert man sich auch für Abbildungen zwischen solchen Objekten, die diese Strukturen respektieren. Solche Abbildungen nennt man Homomorphismen. In diesem Kapiel werden wir also Gruppenhomomorphismen sowie deren Bilder und - was wichtiger ist - deren Kerne betrachten. Es stellt sich heraus, daß letztere genau die Normalteiler der Gruppen sind. Wie bei Vektorräumen werden wir den Homomorphiesatz beweisen, der im wesentlichen sagt, daß man sich, wenn man an der Information interessiert ist, die ein Homomorphismus zwischen zwei Gruppen über selbige enthält, getrost auf i. a. wesentlich kleinere Gruppen zurückziehen kann. Den Satz selbst und die daraus resultierenden Isomorphiesätze werden immer wieder angewandt, um zu zeigen, daß gewisse Gruppen, die man auf Anhieb nicht für *gleich* gehalten hätte, letztlich doch *gleich* (d. h. isomorph) sind. In Satz 3.9 lernen wir dann einen besonderen Normalteiler von G kennen, das Zentrum von G. Und abschließend bestimmen wir die Automorphismengruppe von $(\mathbb{Z},+)$.

b. Als Grundlage für dieses Kapitel hat Paragraph drei in [Doe74] Kapitel VII. gedient. Desgleichen bieten auch [Hum96] § 8, [Hup67] Kapitel I. § 3, [Hup69] Kapitel I. § 5 sowie [Kur77] Kapitel I. § 2 Informationen zu Homomorphismen.

c. Es sollen alle Definitionen, Sätze und Beispiele des Kapitels inklusive der Beweise im Vortrag gebracht werden, wobei die Sätze 3.11 und 3.12 ggf. aus Zeitgründen enfallen können.

3.2 Definition

Es seien G und H zwei Gruppen.

Eine Abbildung $\alpha : G \to H$ heißt ein **(Gruppen-)Homomorphismus**, falls für $g, \tilde{g} \in G$ stets gilt:

$$\alpha(g\tilde{g}) = \alpha(g)\alpha(\tilde{g}).$$

(Wir sagen, α ist mit der Gruppenstruktur *verträglich*.)

Gilt ferner, α ist injektiv (bzw. surjektiv bzw. bijektiv), so heißt α ein **Monomorphismus** (bzw. **Epimorphismus** bzw. **Isomorphismus**). Ist $H = G$, so sprechen wir von einem **Endomorphismus**, und ein bijektiver Endomorphismus wird auch ein **Automorphismus** genannt.

Mit $\mathrm{Hom}(G,H)$ bezeichnen wir die Menge aller Gruppenhomomorphismen von G nach H und mit $\mathrm{End}(G)$ (bzw. $\mathrm{Aut}(G)$) die Menge der Endomorphismen (bzw. Automorphismen) von G.

Mit **Kern** von α bezeichnen wir die Menge $\mathrm{Ker}(\alpha) := \{g \in G \mid \alpha(g) = e_H\}$ und mit **Bild** von α - $\mathrm{Im}(\alpha)$ - die Menge $\{\alpha(g) \mid g \in G\}$

3.3 Beispiel

a. Es sei K ein Körper, $0 \neq n \in \mathbb{N}$, dann ist $\det : \mathrm{Gl}_n(K) \to (K^*, \cdot)$ ein Epimorphimus von der $\mathrm{Gl}_n(K)$ in die multiplikative Gruppe des Körpers. Dies folgt unmittelbar aus dem Determinantenmultiplikationssatz. Der Kern von det ist $\mathrm{Sl}_n(K) := \{A \in \mathrm{Gl}_n(K) \mid \det(A) = 1\}$ und heißt **spezielle lineare Gruppe**.

b. Es sei G eine Gruppe, $h \in G$.
Die Abbildung $\alpha_h : G \to G : g \mapsto g^h := hgh^{-1}$ heißt die **Konjugation** mit h und ist ein Automorphismus.
Automorphismen dieser Form heißen **innere Automorphismen** und die Gruppe $\mathrm{Inn}(G) := \{\alpha \in \mathrm{Aut}(G) \mid \alpha \text{ ist ein innerer Automorphismus}\}$ ist ein Normalteiler von $\mathrm{Aut}(G)$. (Vgl. hierzu [Doe74] VII.3.6.)

c. Genau dann ist die Inversion $G \to G : g \mapsto g^{-1}$ ein Gruppenisomorphismus, wenn G abelsch ist.

d. Es sei $m \in \mathbb{Z}$ und G abelsch, dann ist $\mu_m : G \to G : g \mapsto g^m$ ein Gruppenhomomorphismus.

3.4 Satz

Es seien G und H Gruppen, e_G und e_H das neutrale Element von G respektive H und $\alpha \in \mathrm{Hom}(G, H)$.
Dann gilt:

a. $\alpha(e_G) = e_H$ *und* $\alpha(g^{-1}) = (\alpha(g))^{-1}$ *für alle* $g \in G$.

b. $\mathrm{Im}(\alpha) \leq H$.

c. $\mathrm{Ker}(\alpha) \trianglelefteq G$.

d. α *ist genau dann ein Monomorphismus, wenn* $\mathrm{Ker}(\alpha) = \mathbb{1}$.

e. *Ist* $N \trianglelefteq G$, *so gilt für den (natürlichen) Epimorphismus* $\nu : G \to G/N$ *mit* $\nu(g) = gN$ *gerade* $\mathrm{Ker}(\nu) = N$.

Beweis: Vgl. [Doe74] VII.3.2, [Hup67] I.3.7-3.8 oder [Kur77] p. 7 sowie auch [Hum96] 8.6-8.7, 8.13. □

3.5 Bemerkung

Teil c. und e. des letzten Satzes 3.4 implizieren, daß die Kerne der Homomorphismen von G in andere Gruppen genau die Normalteiler von G sind.

3.6 Theorem (Homomorphiesatz)

Es seien G und H Gruppen, $\alpha \in \mathrm{Hom}(G, H)$. Ferner bezeichne ν den natürlichen Epimorphismus von G auf $G/\mathrm{Ker}(\alpha)$.
Dann gibt es genau einen Monomorphismus $\beta \in \mathrm{Hom}(G/\mathrm{Ker}(\alpha), H)$ mit $\alpha = \beta \circ \nu$.
Insbesondere gilt:

$$G/\mathrm{Ker}(\alpha) \cong \mathrm{Im}(\alpha).$$

Beweis: Vgl. [Doe74] VII.3.2, [Hup67] I.3.8 oder [Kur77] 1.7 sowie [Hum96] 8.13. □

3.7 Beispiel

Es sei K ein Körper, $0 \neq n \in \mathbb{N}$. Dann folgt mittels der Determinante als Homomorphismus: $\mathrm{Gl}_n(K)/\,\mathrm{Sl}_n(K) \cong (K^*, \cdot)$.

3.8 Folgerung (Isomorphiesätze)

Es sei G *eine Gruppe,* $L, N \trianglelefteq G$, $M \leq G$, $L \subseteq M$.

a. $MN/N \cong M/(M \cap N)$

b. $(G/L)/(M/L) \cong (G/M)$

Beweis: Vgl. [Doe74] VII.3.4 (siehe insbesondere dort die Strukturdiagramme!) oder [Hum96] 8.15-8.16. □

3.9 Satz

Es sei G *eine Gruppe. Für* $g \in G$ *bezeichne* α_g *den inneren Automorphismus von* G*, der durch Konjugation mit* g *gegeben ist (vgl. Beispiel 3.3). Ferner sei* $\beta : G \to \mathrm{Inn}(G)$ *definiert durch* $\beta(g) := \alpha_g$.
Dann ist β *ein Epimorphismus.*
Den Kern von β *bezeichnen wir mit* $Z(G)$ *und nennen ihn das* ***Zentrum*** *von* G. *Es gilt offenbar:*

$$Z(G) = \{g \in G | gh = hg \; \forall \; h \in G\} \textit{ und } G/Z(G) \cong \mathrm{Inn}(G).$$

Beweis: Vgl. [Doe74] VII.3.6 sowie [Hum96] 8.11 und 8.17. □

3.10 Korollar

Eine Gruppe G *ist genau dann abelsch, wenn* $Z(G) = G$.

3.11 Satz

Es seien G *und* H *endliche Gruppen gleicher Mächtigkeit,* $\alpha \in \mathrm{Hom}(G, H)$.
Dann sind die folgenden Aussagen äquivalent:

a. α *ist ein Isomorphismus.*

b. α *ist ein Monomorphismus.*

c. α *ist ein Epimorphismus.*

Beweis: Es reicht die Äquivalenz von bijektiv, injektiv und surjektiv zu zeigen. Das ist elementar. □

3.12 Satz

Es gilt: $\mathrm{Aut}(\mathbb{Z}) \cong (\mathbb{Z}^* = \{-1, 1\}, \cdot)$.

Beweis: Die abelsche Gruppe $(\mathbb{Z}, +)$ ist erzeugt durch das Element $1 \in \mathbb{Z}$. Mithin gilt für $\alpha \in \mathrm{Hom}(\mathbb{Z}, \mathbb{Z})$, daß α festgelegt ist durch das Bild von 1. Sei nun $\alpha(1) = n \in \mathbb{Z}$, dann ist $\mathrm{Im}(\alpha) = n\mathbb{Z}$. Da α surjektiv ist, gilt also $n\mathbb{Z} = \mathbb{Z}$ und somit $n = 1$ oder $n = -1$, d. h. $|\mathrm{Aut}(\mathbb{Z})| \leq 2$.
Die Abbildung $\beta : \mathbb{Z}^* \to \mathrm{Aut}(\mathbb{Z})$ mit $n \mapsto (\mathbb{Z} \ni z \mapsto n \cdot z \in \mathbb{Z})$ ist, wie man leicht sieht, ein Gruppenmonomorphismus, also ist $|\mathrm{Aut}(\mathbb{Z})| = 2$ und mit Satz 3.11 ist β ein Isomorphismus. □

AUFGABEN

3.13 Aufgabe
Für $k \in \mathbb{Z}$ definieren wir eine Abbildung

$$\alpha_k : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} : \overline{z} \mapsto \overline{k} \cdot \overline{z}.$$

Man zeige, daß α_k stets ein Epimorphismus ist, und daß α_k genau dann ein Automorphismus ist, wenn $(k, n) = 1$.

3.14 Aufgabe
Ist $\mathbb{Z}_{p^\infty}$ die Prüfergruppe aus Aufgabe 0.16, so zeige man, daß für $\nu \in \mathbb{N}$ die Abbildung

$$\alpha_\nu : \mathbb{Z} \to \mathbb{Z}_{p^\infty} : z \mapsto e^{\frac{2\pi i z}{p^\nu}}$$

ein Gruppenhomomorphismus ist mit $\mathrm{Ker}(\alpha_\nu) = p^\nu\mathbb{Z}$.

3.15 Aufgabe
Man zeige, daß die Abbildung

$$\alpha : (\mathbb{R}, +) \to (\mathbb{R} \setminus \{0\}, \cdot) : t \mapsto e^t$$

ein Gruppenhomomorphismus ist.

3.16 Aufgabe
Für $n \geq 1$ bestimme man $\left| \mathrm{Gl}_2(n) : \mathrm{Sl}_2(n) \right|$.

3.17 Aufgabe
Welche Mächtigkeit besitzen $\mathrm{Gl}_2(3)$ und $\mathrm{Sl}_2(3)$?

3.18 Aufgabe
Man bestimme das Zentrum von $\mathrm{Gl}_2(2)$.

4 Die symmetrische Gruppe $\mathbb{S}_n$

4.1 Allgemeine Hinweise

a. Bereits in Kapitel 0 wurde die symmetrische Gruppe vom Grad n als Gruppe der Permutationen von n Elementen eingeführt. Wir werden zunächst zwei unterschiedliche Darstellungsformen für Permutationen kennenlernen, die je ihre besonderen Vorteile haben und auch beide zur Anwendung kommen werden. Für die Darstellung durch Zyklen werden wir in Satz 3 einige nützliche Resultate herleiten, und schließlich die Existenz und Eindeutigkeit eines nicht trivialen Homomorphismus von $\mathbb{S}_n$ in die zyklische Gruppe der Ordnung 2 zeigen. Dieses Resultat impliziert, daß $\mathbb{S}_n$ genau eine Untergruppe vom Index 2 besitzt, die sog. alternierende Gruppe $\mathbb{A}_n$ vom Grad n. Im Falle $n = 4$ ist sie ein Beispiel dafür, daß der Satz von Lagrange nicht umkehrbar ist.

b. Es empfiehlt sich, Kapitel I. § 4 in [Doe72] sowie Kapitel I. § 5 in [Hup69] oder [Hum96] § 9 zu lesen. Dort ist die symmetrische Gruppe ausführlich dargestellt. Wesentlich weiter geht Kapitel III. § 5 in [Kur77].

c. Alle in diesem Kapitel gegebenen Definitionen, Sätze und Beispiele sollen im Vortrag dargestellt und bewiesen werden.

4.2 Definition

Es sei $\mathbb{S}_n$ die symmetrische Gruppe vom Grad n aus Beispiel 0.4 f.

a. Ist $\sigma \in \mathbb{S}_n$, so kann σ beschrieben werden durch das folgende Schema:

$$\begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}.$$

b. Eine Permutation $\sigma \in \mathbb{S}_n$, für die eine Zerlgung $\{1, \dots, n\} = \{a_1, \dots, a_k\} \cup \{b_1, \dots, b_{n-k}\}$ existiert, so daß gilt:

$$\sigma = \begin{pmatrix} a_1 & a_2 & \dots & a_{k-1} & a_k & b_1 & \dots & b_{n-k} \\ a_2 & a_3 & \dots & a_k & a_1 & b_1 & \dots & b_{n-k} \end{pmatrix},$$

heißt ein **k-Zyklus**.

Wir schreiben kurz: $\sigma = (a_1 \dots a_k)$.

Beachte: die Zyklen $(a_1 \dots a_k)$, $(a_k a_1 \dots a_{k-1})$, etc. stimmen überein!

Ein $2-$ Zyklus wird auch eine **Transposition** genannt.

4.3 Beispiel

a. Ist $\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}$, so ist $\sigma^{-1} = \begin{pmatrix} \sigma(1) & \sigma(2) & \dots & \sigma(n) \\ 1 & 2 & \dots & n \end{pmatrix}$.

b. Die Verknüpfung der beiden Permutationen $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ und $\pi = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ erhält man folgendermaßen. π wirft 1 auf 2, σ wirft 2 weiter auf 3, also $1 \to 2 \to 3$, d. h. $\sigma\pi(1) = 3$. Analog: $2 \to 1 \to 2$ und $3 \to 3 \to 1$, also insgesamt:

$$\sigma\pi = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

Man sieht sofort, daß σ und π Zyklen sind, nämlich $\sigma = (123)$ und $\pi = (12)$, also ist π sogar eine Transposition.

4.4 Satz
$|\mathbb{S}_n| = n!$.

Beweis: Vgl. [Doe72] I.4.2 oder [Hup69] I.6.2. □

4.5 Satz
Sei $\sigma, \pi \in \mathbb{S}_n$ *eine Permutation.*

a. *Es gibt eine disjunkte Zerlegung von* $\{1, \dots, n\} = \bigcup_{i=1}^{t} \{a_{i1}, \dots, a_{ik_i}\}$ *derart, daß gilt*

$$\sigma = (a_{11} \dots a_{1k_1}) \cdots (a_{t1} \dots a_{tk_t}). \tag{3}$$

Die Zyklen $\zeta_i = (a_{i1} \dots a_{ik_i})$ *sind dabei bis auf die Reihenfolge ihrer Anordnung eindeutig bestimmt.*
Die Darstellung (3) nennt man die ***Zyklenzerlegung*** *von* σ *und das Tupel* $(k_1, \dots, k_t)$ *heißt der* ***Typ*** *von* σ*, falls gilt* $k_1 \leq \dots \leq k_t$.
(Anmerkung: Zyklen der Länge 1 werden bei der Zyklenzerlegung für gewöhnlich weggelassen.)

b. *Genau dann sind* σ *und* π *zueinander konjugiert (d. h.* $\exists\, \theta \in \mathbb{S}_n : \theta\sigma\theta^{-1} = \pi$*), wenn* σ *und* π *den gleichen Typ haben.*

c. *Es gibt Transpositionen* $\tau_1, \dots, \tau_l \in \mathbb{S}_n$*, so daß* $\sigma = \tau_1 \cdots \tau_l$.

Beweis: Vgl. [Doe72] I.4.15/17, [Hup69] I.6.5 und [Kur77] 3.23 sowie auch [Hum96] 9.5, 9.10 und 9.20. □

4.6 Beispiel
Betrachten wir $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 1 & 5 & 6 & 7 & 4 \end{pmatrix} \in \mathbb{S}_7$.
Dann erhalten wir folgende Zyklenzerlegung: $\sigma = (13)(2)(4567) = (13)(4567)$ und σ ist somit vom Typ (1,2,4).
$(13)(47)(46)(45)$ wäre eine Darstellung von σ als Produkt von Transpositionen.

4.7 Satz
Für $n \geq 2$ *gibt es genau einen Gruppenhomomorphismus* $\operatorname{sgn} : \mathbb{S}_n \to (\{-1, 1\}, \cdot)$ *mit* $\operatorname{sgn}(\tau) = -1$ *für alle Transpositionen* $\tau \in \mathbb{S}_n$.
Wir nennen sgn *das* ***Signum***.

Beweis: Vgl. [Doe72] I.4.20 sowie [Hup69] I.6.6. Für einen alternativen Ansatz siehe [Hum96] 9.11-9.18. □

4.8 Folgerung

a. *Eine Permutation läßt sich entweder in eine gerade oder in eine ungerade Anzahl von Transpositionen zerlegen.*

b. *Ist* $\sigma \in \mathbb{S}_n$ *ein k-Zyklus, so ist* $\operatorname{sgn}(\sigma) = (-1)^{k-1}$.

Beweis: Vgl. [Doe72] I.4.21 sowie [Hup69] I.6.7 und [Kur77] p. 51. □

AUFGABEN

4.9 Aufgabe
Man zeige, $\mathbb{S}_3 \cong \mathrm{Gl}_2(2)$.

4.10 Aufgabe
Wir wollen nun die symmetrische Gruppe $\mathbb{S}_4$ etwas näher betrachten. Dazu bestimme man:

a. die Elemente von $\mathbb{S}_4$ und ihre Ordnungen,

b. die Untergruppen von $\mathbb{S}_4$,

c. die Normalteiler von $\mathbb{S}_4$ und

d. das Zentrum $Z(\mathbb{S}_4)$.

(Vgl. [Wei77] Example 4.6 und 4.9.)

5 Die alternierende Gruppe $\mathbb{A}_n$

5.1 Allgemeine Hinweise

a. Die alternierende Gruppe $\mathbb{A}_n$ ist für $n \geq 5$ von besonderem Interesse, da sie die erste Serie einfacher Gruppen liefert. Nun stehen einfache Gruppen und nicht auflösbare Gruppen in engem Zusammenhang miteinander, und nicht auflösbare Gruppen sind im Rahmen der Galoistheorie als Galoisgruppen von Polynomen sehr gefragt. Dies motiviert die Einfügung von Satz 5.7 über die Struktur der $\mathbb{S}_p$ (mit p Primzahl), der in der Galoistheorie Anwendung findet. Die symmetrischen Gruppen stehen aber nicht nur mit den nicht auflösbaren Gruppen in Beziehung, sondern in ihnen spiegeln sich alle endlichen Gruppen wieder, wie aus dem wichtigen Resultat von Cayley (5.9) folgt. Abschließen wollen wir das Kapitel mit einem Satz, der eine Möglichkeit zur Definition der Determinante einer Matrix mit Hilfe der symmetrischen Gruppe bietet.

b. Es empfiehlt sich, Kapitel III. § 4 in [Doe72] sowie Kapitel I. § 5 in [Hup69] und § 9 in [Hum96] zu lesen. Dort ist die symmetrische Gruppe ausführlich dargestellt. Die meisten hier angeführten Ergebnisse finden sich jedoch in [Kur77] Kapitel I. § 5 sowie in [Hum96] §16.

c. Alle in diesem Kapitel angeführten Definitionen und Sätze sollen im Vortrag eingebracht werden. Satz 5.7 kann ggf. wegfallen, ebenso kann auf die Bemerkungen verzichtet werden.

5.2 Definition und Satz

$\mathbb{A}_n := \mathrm{Ker}(\mathrm{sgn})$ heißt die **alternierende Gruppe** vom Grad n, und es gilt offenbar $\mathbb{A}_n \lhd \mathbb{S}_n$ mit $|\mathbb{S}_n : \mathbb{A}_n| = 2$.

5.3 Satz

$\mathbb{A}_4$ hat Ordnung 12, aber keine Untergruppe der Ordnung 6.
Insbesondere: die Umkehrung des Satzes von Lagrange gilt nicht.

Beweis: Wir wissen $\mathbb{A}_4 = \{(1), (ab)(cd), (abc) \mid \{a, b, c, d\} = \{1, 2, 3, 4\}\}$, insbesondere enthält $\mathbb{A}_4$ den Normalteiler $K = \{(1), (12)(34), (13)(24), (14)(23)\}$.
Angenommen, $\mathbb{A}_4$ enthält eine Untergruppe V mit $|V| = 6$.
Die Produktformel (Satz 1.4) impliziert $|V \cap K| \geq 2$ und aus dem Satz von Lagrange folgt dann wegen $V \cap K \leq V$ und $V \cap K \leq K$, $|V \cap K| = 2$.
Also enthält V ein Element der Form $(ab)(cd)$ sowie vier 3-Zyklen. Wir unterscheiden folgende Fälle:

a. Sind $(abc), (acb) \in V$, dann gilt $(ac)(bd) = (acb)(ab)(cd)(abc) \in V$, Widerspruch.

b. Sind $(abd), (adb) \in V$, dann gilt $(ad)(bc) = (adb)(ab)(cd)(abd) \in V$, Widerspruch.

c. Sind $(acd), (adc) \in V$, dann gilt $(ac)(bd) = (adc)(ab)(cd)(acd) \in V$, Widerspruch.

Aber eines der drei Paare müßte in V sein. Also haben wir insgesamt einen Widerspruch hergeleitet. □

5.4 Lemma

a. *Die 3-Zykel in $\mathbb{S}_n$ erzeugen die alternierende Gruppe $\mathbb{A}_n$.*

b. *Ist $n \geq 5$, so sind alle 3-Zykel in $\mathbb{A}_n$ zueinander konjugiert.*

Beweis: Vgl. [Kur77] 3.26 sowie [Hum96] 16.14-16.15. □

5.5 Satz
Für $n \geq 5$ ist die alternierende Gruppe $\mathbb{A}_n$ einfach.

Beweis: Vgl. [Kur77] 3.27 sowie [Hum96] 16.13 und 16.16. □

5.6 Bemerkung
Also ist insbesondere $\mathbb{A}_5$ einfach. Sie ist die kleinste nicht abelsche einfache Gruppe, und es gilt sogar, daß jede einfache Gruppe der Ordnung 60 isomorph zur $\mathbb{A}_5$. Vgl. hierfür [Kur77] 3.28.

5.7 Satz
Es sei p eine Primzahl, $\tau \in \mathbb{S}_p$ eine Transposition und $\zeta \in \mathbb{S}_p$ ein p-Zyklus. Dann gilt: $\mathbb{S}_p = \langle \tau, \zeta \rangle$.

Beweis: O. E. ist $\tau = (1\,2)$. Da ζ ein p-Zyklus ist, gibt es ein $k \in \{1, \ldots, p-1\}$ mit $\zeta^k(1) = 2$. Da nun p eine Primzahl ist, ist ζ^k ein p-Zyklus und $\zeta^k \in \langle \tau, \zeta \rangle =: U$, also o. E. $\zeta = (1\,2\,c_3 \ldots c_p)$.
Sei nun $h = \begin{pmatrix} 1 & 2 & c_3 & \ldots & c_p \\ 1 & 2 & 3 & \ldots & p \end{pmatrix} \in \mathbb{S}_p$.
Dann ist $\tau^h = \tau$ und $\zeta^h = (1\,2\,3 \ldots p)$. Also o. E. $\tau = (1\,2)$ und $\zeta = (1\,2\,3 \ldots p)$ (da das Erzeugnis der gegebenen Elemente nun isomorph zu dem der speziellen Elemente ist).
Damit erhalten wir für $i = 1, \ldots, p-2$:

$$(i+1\;\; i+2) = (\zeta^i(1)\;\; \zeta^i(2)) = \tau^{(\zeta^i)} \in U,$$

und ferner rekursiv für $i = 2, \ldots, p-1$:

$$(1\;\; i+1) = (i\;\; i+1)^{(1\, i)} \in U.$$

Damit gilt dann für $i \neq j$:

$$(i\, j) = (1\, j)^{(1\, i)} \in U,$$

und damit ist nach Satz 4.5 $U = \mathbb{S}_p$.
(Für ein Teilergebnis vgl. man auch [Hum96] 9.21.) □

5.8 Bemerkung
Den letzten Satz benötigt man in der Galoistheorie, um zu zeigen, daß die Galoisgruppe des Zerfällungskörpers eines irreduziblen Polynoms $f \in \mathbb{Q}[x]$ vom Grad p mit genau zwei nicht-reellen Nullstellen isomorph zur $\mathbb{S}_p$ ist. Daraus folgt insbesondere, daß das Polynom $f = x^5 - 4x + 2 \in \mathbb{Q}[x]$ nicht durch Radikale auflösbar ist, daß mithin keine allgemeine Lösungsformel für die Nullstellen

von Polynomen des Grades 5 existieren kann, die nur auf sukkzessiven Wurzelausdrücken in den Koeffizienten des Polynoms aufbaut. (Vgl. hierzu auch den Ausblick im letzten Kapitel.)

5.9 Satz (Cayley)
Ist G *eine endliche Gruppe mit* $n = |G|$, *so gilt,* G *ist isomorph zu einer Untergruppe von* $\mathbb{S}_n$.

Beweis: Vgl. [Hup69] I.6.10 oder [Doe74] VII.3.5 sowie [Hup67] I.6.3. Ein alternativer Zugang findet sich in [Hum96] 9.24. □

5.10 Bemerkung
Der letzte Satz sagt aus, daß es eigentlich ausreicht, die symmetrischen Gruppen und ihre Untergruppen zu studieren, um alle endlichen Gruppen kennenzulernen. Da eine Vielzahl von endlichen Gruppen aber ganz natürlich auf andere Weise gegeben ist, scheint diese einschränkende Sicht wenig wünschenswert. Durchaus vielversprechend ist jedoch der Ansatz, Gruppenhomomorphismen einer gegebenen Gruppe G in eine symmetrische Gruppe - sog. *Permutationsdarstellungen* - zu studieren, um Erkenntnisse über G zu gewinnen, und wir werden auf diesen Ansatz im folgenden Kapitel 6 etwas näher eingehen.
Da symmetrische Gruppen eine recht komplexe Struktur aufweisen, begann man nach anderen Typen von Gruppen zu suchen, die leichter handhabbar sind, und bei denen die Homomorphismen von G in diese Gruppen dennoch Rückschlüsse auf die Struktur von G zulassen. Als besonders geeignet erwiesen sich die linearen Gruppen $\mathrm{Gl}_n(K)$, und den Zweig der Mathematik, der sich mit der Untersuchung solcher *linearen Darstellungen* befaßt, nennt man *Darstellungstheorie.*

AUFGABEN

5.11 Aufgabe
Man zeige, $\mathbb{D}_8 \cong \big\langle (1\ 2\ 3\ 4), (2\ 4) \big\rangle$.

5.12 Aufgabe
Aufgrund von Aufgabe 5.11 wollen wir die Gruppen $\mathbb{D}_8$ und $\big\langle (1\ 2\ 3\ 4), (2\ 4) \big\rangle$ im folgenden nicht mehr unterscheiden. In diesem Sinne zeige man $\mathbb{D}_8 = \big\langle (1\ 2)(3\ 4), (2\ 4) \big\rangle$.

5.13 Aufgabe
Man bestimme die Konjugationsklassen von Dreizykeln in der $\mathbb{S}_4$, d. h. die Mengen der zueinander konjugierten Dreizykel.

6 OPERIEREN

6.1 Allgemeine Hinweise

a. Wir haben Gruppen schon in den ersten Kapiteln als Gruppen von (bijektiven) Abbildungen auf Mengen kennengelernt. In dieser Form spielen Gruppen in allen Bereichen der Mathematik eine wichtige Rolle, und wir sagen kurz, sie operieren auf den Mengen. Wir wollen uns zunächst einige Beispiele für Gruppenoperationen etwas näher betrachten, einige neue Begriffe einführen und dann einen recht unscheinbaren Satz mit einigen Folgerungen beweisen. Die durchaus nicht geringe Bedeutung des Satzes und seiner Folgerungen wird im folgenden Kapitel 7 und dann im Beweis des Satzes von Sylow voll zur Entfaltung kommen. Wir schließen das Kapitel mit dem *Frattiniargument*, das bei der näheren Betrachtung von nilpotenten und auflösbaren Gruppen von unschätzbarem Wert ist.

b. Der Inhalt dieses Kapitels findet sich im Wesentlichen wieder in [Hup67] Kapitel I. § 2 sowie §§ 4-6 und [Kur77] Kapitel III. §§ 1-2. Nicht alles, was dort aufgeführt ist, wurde hier übernommen, aber besonders letztere Literaturstelle sollte einen Eindruck von den Zielen, die verfolgt werden, wiedergeben. Eine sehr schöne Darstellung der hier aufgeführten Ergebnisse findet sich auch in [Hum96] § 10. [Hum96] zeichnet sich durch ein reiches Angebot an Beispielen für die eingeführten Begriffe aus.

c. Alle vorliegenden Definitionen und Sätze sollen im Vortrag wiedergegeben und bewiesen werden, wobei ggf. auf Satz 6.8 sowie auf das Frattiniargument verzichtet werden kann. Ein besonderes Augenmerk gilt den Beispielen in 6.4; die Teile b. und c. sollten eingehend betrachtet werden.

6.2 Definition

Es sei G eine Gruppe, Ω eine Menge.
Ein Gruppenhomomorphismus $\alpha : G \to \mathbb{S}(\Omega)$ von G in die Menge der Permutationen von Ω nennt man eine **Permutationsdarstellung**.
Ist $\operatorname{Ker}(\alpha) = 1$, so heißt α **treu**, ist $\operatorname{Ker}(\alpha) = G$, so heißt α **trivial**.

6.3 Notation

Ist G eine Gruppe, Ω eine Menge, $\alpha \in \operatorname{Hom}(G, \mathbb{S}(\Omega))$ eine Permutationsdarstellung, so führen wir folgende Schreib- und Sprechweisen ein:

a. Statt $\alpha(g)(\omega)$ für $g \in G$ und $\omega \in \Omega$ schreiben wir auch $g\omega$, falls über die Permutationsdarstellung α keine Unklarheiten bestehen.
In letzter Form gilt dann: $e\omega = \omega$ und $(gh)\omega = g(h\omega)$ für alle $\omega \in \Omega, g, h \in G$.

b. Wir sagen G **operiert** auf Ω (via α) und nennen Ω eine G-**Menge**.

6.4 Beispiel

a. Es seien G und H Gruppen. Wir nennen einen Gruppenhomomorphismus $\alpha : G \to \operatorname{Aut}(H) \leq \mathbb{S}(H)$ von G in die Automorphismengruppe von H eine

Operation von G auf H **(via Automorphismen)**. Jede Operation (via Automorphismen) von G auf H ist offenbar eine Permutationsdarstellung von G auf H.

Beachte: wenn wir davon sprechen, daß eine Gruppe auf einer anderen *Gruppe* operiert, so ist stets eine Operation via Automorphismen gemeint!

b. Es sei G eine Gruppe, $\emptyset \neq A \subseteq G$, $\Omega = \{A^g \mid g \in G\}$.
Dann operiert G auf Ω durch Konjugation, d. h. $G \to \mathbb{S}(\Omega) : h \mapsto (\Omega \ni A^g \mapsto (A^g)^h = A^{hg} \in \Omega)$ ist eine Permutationsdarstellung.

c. Es sei G eine Gruppe, $U \leq G$ mit $|G : U| = n$, $\Omega := \{g_1U, \ldots, g_nU\}$ die Menge der Linksnebenklassen von U in G.
Dann operiert G auf Ω durch $\alpha : G \to \mathbb{S}(\Omega) : h \mapsto (\Omega \ni g_iU \mapsto hg_iU \in \Omega)$.
Dabei gilt $\mathrm{Ker}(\alpha) = \bigcap_{g \in G} U^g =: \mathrm{Core}_G(U)$, das **Core** oder Herz von U in G, der größte Normalteiler von G, der in U enthalten ist. (Vgl. [Hup67] I.6.2 oder [Hum96] 9.22.)

d. Betrachte $\alpha : \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/3\mathbb{Z})$ wobei $\alpha(\bar{1})$ die Inversion auf $\mathbb{Z}/3\mathbb{Z}$ sein soll und $\alpha(\bar{0})$ die Identität. Dann ist α ein Gruppenhomomorphismus und somit operiert $\mathbb{Z}/2\mathbb{Z}$ auf $\mathbb{Z}/3\mathbb{Z}$ via Automorphismen.

(Beachte dazu nur, daß die Inversion nach Beispiel 3.3 c. ein Gruppenhomomorphismus auf $\mathbb{Z}/3\mathbb{Z}$ ist und daß gilt: $\alpha(\bar{1})\alpha(\bar{1}) = \mathrm{id}_{\mathbb{Z}/3\mathbb{Z}} = \alpha(\bar{1} + \bar{1})$.)

e. Es sei $G = (\mathbb{R}, +)$ die additive Gruppe der reellen Zahlen und $\Omega = \mathbb{C}$ die Menge der komplexen Zahlen. Durch $\alpha(t)(c) := c \cdot e^{2\pi i t}$ für $t \in \mathbb{R}$ und $c \in \mathbb{C}$ wird eine Permutationsdarstellung $\alpha : G \to \mathbb{S}(\Omega)$ definiert. Der Kern von α ist die additive Gruppe $(\mathbb{Z}, +)$ der ganzen Zahlen.

f. Die alternierende Gruppe $\mathbb{A}_n$ operiert durch Konjugation auf der Menge $\Omega = \{\sigma \in \mathbb{S}_n \mid \sigma \text{ ist ein 3-Zykel}\}$ der 3-Zykel.

6.5 Definition

Die Gruppe G operiere auf der Menge Ω via α.

a. Erkläre auf Ω eine Äquivalenzrelation (nachprüfen! - vgl. [Hum96] 10.13) $\sim$ durch:

$$\omega \sim \tau :\Leftrightarrow \exists\, g \in G : g\omega = \tau.$$

Dann erhalten wir eine disjunkte Zerlegung von Ω in Äquivalenzklassen Ω_i, $i \in I$. Die Ω_i heißen die **Bahnen** von G auf Ω.
Schreibweise: Ist $\omega \in \Omega$, so bezeichnet $\omega^G := \{\tau \in \Omega \mid \tau \sim \omega\}$ die **Bahn von ω unter** G.

b. Wir sagen, G operiert **transitiv** auf Ω (bz. Ω ist eine transitive G-Menge), falls Ω selbst eine Bahn von G auf Ω ist.

c. Die Menge $G_\omega := \{g \in G \mid g\omega = \omega\}$ heißt der **Stabilisator** von $\omega \in \Omega$.

6.6 Beispiel

a. Die Operationen in den Beispielen 6.4 b. und c. sind transitiv.

b. In Beispiel 6.4 e. gilt für $0 \neq c \in \mathbb{C}$, daß die Bahn $c^{\mathbb{R}}$ von c unter $\mathbb{R}$ ein Kreis vom Radius $|c|$ ist und daß der Stabilisator $\mathbb{R}_c$ gerade die additive Gruppe $(\mathbb{Z}, +)$ ist.

c. In Lemma 5.4 haben wir gezeigt, daß die Operation in 6.4 f. für $n \geq 5$ transitiv ist. Für $n = 3$ und $n = 4$ besitzt sie jeweils zwei Bahnen, wie man leicht nachprüft. (Vgl. Aufgabe 5.13.)

6.7 Satz (Orbit-Stabiliser-Theorem)
Die Gruppe G *operiere auf der Menge* Ω, $\omega \in \Omega$.
Dann gilt:

a. $G_\omega \leq G$

b. $|G : G_\omega| = |\omega^G|$, *falls* $|\Omega| < \infty$.

Beweis: Vgl. [Hup67] I.5.10 oder [Kur77] 3.4 sowie [Hum96] 10.9 und 10.16. □

6.8 Folgerung
Die Gruppe G *operiere auf der endlichen Menge* Ω, *und es sei* $n \in \mathbb{N}$.
Gilt $n \,\big|\, |\omega^G|$ *für alle* $\omega \in \Omega$, *so ist* n *ein Teiler von* $|\Omega|$.

Beweis: Vgl. [Kur77] 3.5. □

6.9 Folgerung
Die endliche Gruppe G *operiere transitiv auf der endlichen Menge* Ω.
Dann gilt: $|\Omega|$ *teilt* $|G|$.

Beweis: Folgt unmittelbar aus Teil b. von Satz 6.7 zusammen mit dem Satz von Lagrange (1.8). □

6.10 Korollar
Sei G *eine endliche Gruppe und* $U \leq G$ *mit* $|G : U| = n$.
Dann besitzt G *einen Normalteiler* $N \trianglelefteq G$ *mit* $n \,\big|\, |G : N|$ *und* $|G : N| \,\big|\, n!$.

Beweis: Vgl. [Hup67] I.6.6 oder [Hum96] 9.23. (Verwende Beispiel 6.4 c. sowie die letzte Folgerung 6.9.) □

6.11 Korollar
Es sei G *ein endliche Gruppe,* p *der minimale Primteiler von* $|G|$ *und* $N < G$ *mit* $p = |G : N|$. *Dann ist* $N \triangleleft G$.

Beweis: Vgl. [Hum96] 9.25. □

6.12 Satz (Frattiniargument)
Die Gruppe G *operiere auf der Menge* Ω, $N \trianglelefteq G$ *und* Ω *sei transitive* N*-Menge.*
Dann gilt für alle $\omega \in \Omega$*:* $G = G_\omega N$.

Beweis: Vgl. [Kur77] 3.3. □

AUFGABEN

6.13 Aufgabe
Man prüfe die Aussagen in Beispiel 6.4 e. und 6.6 b. nach.

6.14 Aufgabe
Analog zu Beispiel 6.4 zeige man, daß $\mathbb{Z}_2$ auf einer beliebigen abelschen Gruppe durch Inversion via Automorphismus operiert.

6.15 Aufgabe
Sowohl die Gruppen $\mathbb{S}_4$ als auch $\mathbb{A}_4$ operieren durch Konjugation auf der Kleinschen Vierergruppe $\mathbb{K}_4 := \{(1), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} \lhd \mathbb{S}_4$. Man bestimme den Stabilisator von $\omega := (1\ 2)(3\ 4)$ unter beiden Gruppenoperationen.

7 KONJUGIEREN

7.1 Allgemeine Hinweise

a. Eine besondere Form des Operation einer Gruppe auf einer Menge ist die der Konjugation. Mit ihrer Hilfe führen wir die Begriffe des Normalisators und des Zentralisators ein und beweisen dann die sog. Klassengleichung, die ein wichtiges Hilfsmittel im Beweis des Satzes von Cauchy ist. Des weiteren läßt sich aus ihr ein wichtiger Satz über die Struktur von Normalteilern in p-Gruppen ableiten, der für die im weiteren Verlauf angestrebte Klassifikation endlicher Gruppen sehr hilfreich ist. Eine unmittelbare Folgerung ist die Tatsache, daß Gruppen von Primzahlquadratordnung abelsch sind. Wir schließen das Kapitel mit einer *negativen* Aussage über die Struktur nicht abelscher Gruppen, nämlich daß sie modulo ihrem Zentrum nie zyklisch sein können. Anwendungen der Ergebnisse finden sich im Kapitel zum Satz von Sylow sowie in einer Reihe von Klassifikationssätzen.

b. Der Inhalt dieses Kapitels findet sich im Wesentlichen wieder in [Hup67] Kapitel I. § 2 sowie §§ 4-6 und [Kur77] Kapitel III. §§ 1-2. Nicht alles, was dort aufgeführt ist, wurde hier übernommen, aber besonders letztere Literaturstelle sollte einen Eindruck von den Zielen, die verfolgt werden, wiedergeben. Eine sehr schöne Darstellung der hier aufgeführten Ergebnisse findet sich auch in [Hum96] § 10. [Hum96] zeichnet sich durch ein reiches Angebot an Beispielen für die eingeführten Begriffe aus.

c. Alle Definitionen und Sätze des vorliegenden Kapitels werden benötigt und sollen inklusive der Beweise im Vortrag dargestellt werden. Auf den Beweis von Bemerkung 7.3 kann ggf. verzichtet werden.

7.2 Definition

Es sei G eine Gruppe, $U \leq G$, $A \subseteq G$.

a. $C_U(A) := \{h \in U \mid a^h = a \,\forall\, a \in A\}$ heißt der **Zentralisator** von A in U.

b. $N_U(A) := \{h \in U \mid A^h = A\}$ heißt **Normalisator** von A in U.

7.3 Bemerkung

Es sei G eine Gruppe, $U \leq G$, $A \subseteq G$, $g \in G$.
Dann gilt offenbar:

a. $N_U(A) \leq U$.

b. $C_G(U) \trianglelefteq N_G(U)$ und $N_G(U)/C_G(U)$ ist isomorph zu einer Untergruppe von $\mathrm{Aut}(U)$.

c. $C_U(g) = C_G(g) \cap U$.

Beweis: Zu b. betrachte $N_G(U) \to \mathrm{Aut}(U) : g \mapsto (U \ni h \mapsto h^g \in U)$ und wende den Homomorphiesatz an, vgl. auch [Hum96] 10.26. Zu c. vgl. [Hum96] 10.19. □

7.4 Satz
Es sei G *eine endliche Gruppe,* $A \subseteq G$, $\Omega := \{A^g \mid g \in G\}$.
Dann gilt: $|\Omega| = |G : N_G(A)|$.
Insbesondere: Ist $A = \{a\}$, *dann ist* $N_G(a) = C_G(a)$ *und* $|a^G| = |G : C_G(a)|$.

Beweis: Folgt unmittelbar aus Beispiel 6.4 b. und Satz 6.7. (Vgl. [Hup67] I.2.18.) □

7.5 Korollar (Klassengleichung)
Es sei G *eine endliche Gruppe, dann operiert* G *auf* G *durch Konjugation (via Automorphismen), d. h.* $G \to \mathrm{Aut}(G) : g \mapsto (G \ni h \mapsto h^g \in G)$ *ist ein Homomorphismus.*
Damit zerfällt $G = \bigcup_{i=1}^{h} K_i$ *in die Bahnen* K_i *von* G *auf* G, *wobei* $K_i = \{g_i^g \mid g \in G\}$ *für geeignete* $g_i \in G$ *und o. E.* $K_1 = \{e\}$ *sowie* $K_j, \ldots, K_h$ *genau die Bahnen mit mehr als einem Element.*
Aus Satz 7.4 folgt unmittelbar die ***Klassengleichung****:*

$$|G| = \sum_{i=1}^{h} |K_i| = \sum_{i=1}^{h} |G : C_G(g_i)| = |Z(G)| + \sum_{i=j}^{h} |G : C_G(g_i)|.$$

Beweis: Klar! (Vgl. auch [Hup67] I.2.16 bzw. ebd. I.6.8 oder [Kur77] 3.6.) □

7.6 Definition
Eine Gruppe G mit $|G| = p^n$ für eine Primzahl p heißt **p-Gruppe**.

7.7 Satz
Es sei G *eine p-Gruppe und* $\mathbb{1} \neq N \trianglelefteq G$ *ein nicht trivialer Normalteiler von* G.
Dann gilt $N \cap Z(G) \neq \mathbb{1}$.
Insbesondere besitzt eine nicht triviale p-Gruppe ein nicht triviales Zentrum.

Beweis: Vgl. [Hup67] I.6.9. Für ein Teilergebnis vgl. auch [Hum96] 10.20. □

7.8 Korollar
Ist $G \neq \mathbb{1}$ *eine einfache* p*-Gruppe, so ist* G *zyklisch mit* $|G| = p$.

Beweis: Da G einfach ist, folgt aus $\mathbb{1} \neq Z(G) \trianglelefteq G$, daß $G = Z(G)$, und damit ist G abelsch. Ist $e \neq g \in G$ beliebig, dann gilt $o(g) = p^n$ für ein $0 \neq n \in \mathbb{N}$. Setzen wir $e \neq h := g^{p^{n-1}} \in G$, dann gilt $o(h) = p$. Da G abelsch ist, gilt außerdem $\mathbb{1} \neq \langle h \rangle \trianglelefteq G$. Aber dann ist $\langle h \rangle = G$ und $p = o(h) = |G|$. □

7.9 Satz
Es sei G *eine Gruppe, so daß* $G/Z(G)$ *zyklisch ist.*
Dann ist G *abelsch.*

Beweis: $G/Z(G) = \langle gZ(G) \rangle$, dann gilt $G = \langle g \rangle Z(G)$, also folgt für $h, \tilde{h} \in G$ $\exists\, z, \tilde{z} \in Z(G)$ mit $h = g^k z$, $\tilde{h} = g^{\tilde{k}} \tilde{z}$. Also gilt: $h\tilde{h} = g^k z g^{\tilde{k}} \tilde{z} = g^{\tilde{k}} \tilde{z} g^k z = \tilde{h} h$, da z und $\tilde{z}$ aus dem Zentrum von G stammen. (Vgl. auch [Hum96] 10.21 oder den Beweis von [Hup67] I.6.10.) □

7.10 Korollar
Sei G *eine Gruppe der Ordnung* p^2 *für eine Primzahl* p.
Dann ist G *abelsch.*

Beweis: Aus Satz 1.13 und Satz 7.7 folgt, daß $G/Z(G)$ zyklisch ist, und aus Satz 7.9 folgt dann, daß G abelsch ist. (Vgl. auch [Hup67] I.6.10 oder [Hum96] 10.22.) □

7.11 Lemma
Sei G *eine p-Gruppe und* $U < G$ *eine echte Untergruppe.*
Dann gilt: $U < N_G(U)$.

Beweis: Idee: betrachte die Zerlegung von G in Doppelnebenklassen.
Definiere dazu für $g, h \in G$: $g \sim h :\Leftrightarrow h \in UgU$.
Man sieht leicht, daß $\sim$ eine Äquivalenzrelation definiert und daß die zu g gehörende Äquivalenzklasse gerade UgU ist. Mithin erhalten wir eine disjunkte Zerlegung von G in $G = \cup_{i=1}^{n} Ug_iU$ für $g_1 = e, g_2, \ldots, g_n \in G$ geeignet, und damit $|G| = \sum_{i=1}^{n} |Ug_iU|$. Nun gilt $|Ug_iU| = |Ug_iUg_i^{-1}| = |UU^{g_i}| = \frac{|U||U^{g_i}|}{|U \cap U^{g_i}|} = |U| \cdot |U : (U \cap U^{g_i})|$, und dabei ist $U \cap U^e = U$.
Insgesamt erhalten wir: $1 \neq p^k = |G|/|U| = 1 + \sum_{i=2}^{n} |U : (U \cap U^{g_i})|$.
Da aber $|U : (U \cap U^{g_i})|$ eine p-Potenz ist, muß für ein weiteres $i \in \{2, \ldots, n\}$ gelten, daß $U \cap U^{g_i} = U$, d. h. $g_i \in N_G(U)$ und $g_i \notin U$. □

7.12 Lemma
Sei G *eine Gruppe der Ordnung* p^n, $n \geq 1$, p *Primzahl.*
Die maximalen Untergruppen von G *haben Ordnung* p^{n-1} *und sind Normalteiler.*

Beweis: Sei $M <\cdot\, G$, dann gilt nach Lemma 7.11: $M < N_G(M)$. Da M maximal ist, folgt also $N_G(M) = G$ und somit $M \lhd G$. Außerdem folgt aus der Maximalität von M, daß G/M eine einfache p-Gruppe ist, also $|G/M| = p$ nach Korollar 7.8. □

AUFGABEN

7.13 Aufgabe
Bestimme $N_{\mathbb{S}_4}(\mathbb{S}_3)$, $N_{\mathbb{S}_4}(\mathbb{K}_4)$, $C_{\mathbb{S}_4}\big((1\ 2)(3\ 4)\big)$ und $C_{\mathbb{D}_8}\big((1\ 2)(3\ 4)\big)$.

7.14 Aufgabe
Die Gruppe $\mathbb{D}_8$ operiert auf sich selbst durch Konjugation. Zerlege $\mathbb{D}_8$ in disjunkte Bahnen.

7.15 Aufgabe
Bestimme $Z(\mathbb{D}_8)$ und $Z(\mathbb{Q}_8)$. (Vgl. [Wei77] Example 4.3 und 4.4.)

8 DIREKTE UND SEMIDIREKTE PRODUKTE

8.1 Allgemeine Hinweise

a. Hat man einmal eine Anzahl von Gruppen gegeben, so strebt man danach, aus diesen neue Gruppen zu basteln. Innerhalb einer festen Gruppe G haben wir bereits gelernt, daß das Produkt eines Normalteilers N mit einer Untergruppe U stets wieder eine Untergruppe ist, wobei innerhalb dieser die Gruppe U auf der Gruppe N operiert. Liegt nun letztere Situation ohne umgebende Gruppe G vor, so kann man sich obige Situation künstlich schaffen. Dieser Ansatz führt zu semidirekten Produkten und damit zu *neuen* Gruppen, deren Struktur natürlich wesentlich von den *Ausgangsdaten* abhängt. Ein ähnliches, wenn auch simpleres Verfahren stellen die direkten Produkte dar, orientiert am Produkt von endlich vielen Normalteilern. Nachdem wir die beiden Verfahren kennengelernt haben, kommen wir zum Kern dieses Kapitels, den Diedergruppen als Beispiel für ein semidirektes Produkt sowie einem ersten konkreten Klassifikationssatz für Gruppen der Ordnung 18, in dessen Formulierung und Beweis semidirekte Produkte eine zentrale Rolle spielen, der aber zugleich eine Anwendung der Kenntnisse aus der linearen Algebra darstellt.

b. Semidirekte Produkte sind sehr schön erklärt in [Gor80] Kapitel 2 § 5. Als weitere Referenz, die direkte und semidirekte Produkte gleichermaßen behandelt, sei [Kur77] Kapitel I. § 4 genannt. [Hup67] Kapiel I. § 14 bringt in I.14.4 semidirekte Produkte als Spezialfall der Erweiterung eines Normalteilers durch seine Faktorgruppe. Die Definition des äußeren semidirekten Produktes in den bisher erwähnten Quellen differiert jedoch leicht von unserer Definition, die sich an [DH92] A.4.22 orientiert und der aus Gründen, die weiter unten klar werden, der Vorzug zu geben ist. Eine wahre Fundgrube, was die verschiedensten Konstruktionsmöglichkeiten für Gruppen und zugehörige Beispiele betrifft, ist [Wei77]. Mit semidirekten Produkten beschäftigt sich Chapter 1.2. Direkte Produkte sind ausführlich behandelt in [Hum96] § 13, mit semidirekten Produkten beschäftigt sich § 19. [Wei77] und [Hum96] verwenden ebenfalls die von uns bevorzugte Definition des äußeren semidirekten Produktes.

c. Beispiel 8.11 und Lemma 8.12 sind unabdingbarer Bestandteil des Vortrages. Hierzu ist es notwendig, die Definitionen der inneren und äußeren (semi-)direkten Produkte vorgestellt und an den einfachen Beispielen erläutert zu haben. Die hierzu gehörenden Beweise sollen nur gebracht werden, sofern dies im zeitlichen Rahmen möglich ist. Gleiches gilt für die schriftliche Fixierung der Bemerkung 8.8 sowie Satz 8.10.

8.2 Definition

Es sei G eine Gruppe, $N_1, \ldots, N_r, N \trianglelefteq G$, $U \leq G$.

a. Gilt $G = N_1 \cdots N_r$ und $N_i \cap (N_1 \cdots N_{i-1}) = \mathbb{1}$ für alle $i = 2, \ldots, r$, dann nennen wir G auch das **(innere) direkte Produkt** von $N_1, \cdots, N_r$ und schreiben $G = N_1 \times \cdots \times N_r$.

b. Gilt $N \cap U = \mathbb{1}$ und $NU = G$, so sagt man G ist das **(innere) semidirekte Produkt** von N und U, und wir schreiben auch: $G = N \ltimes U$.

8.3 Bemerkung

Ist G eine Gruppe und sind $N, M \trianglelefteq G$ mit $G = NM$ und $N \cap M = \mathbb{1}$, so ist $G = N \times M$ ein inneres direktes Produkt, und somit ist selbiges ein Spezialfall eines inneren semidirekten Produktes.

8.4 Beispiel

a. Es sei $\mathbb{K}_4 := \{(1), (12)(34), (13)(24), (14)(23)\} \leq \mathbb{S}_4$ die **Kleinsche Vierergruppe**. Setzen wir $N := \langle (12)(34) \rangle$ und $M := \langle (13)(24) \rangle$, dann sind N und M als Gruppen vom Index 2 Normalteiler (siehe 2.5), $N \cap M = \mathbb{1}$ und $NM = \mathbb{K}_4$ (wegen $|NM| = \frac{|N| \cdot |M|}{|N \cap M|} = 4$), also $\mathbb{K}_4 = N \times M$.

b. Es sei $N := \langle (123) \rangle, U := \langle (12) \rangle \leq \mathbb{S}_3$. Wieder ist N als Gruppe vom Index 2 ein Normalteiler, und es gilt $N \cap U = \mathbb{1}$. Wie in a. sieht man $|NU| = 6$, also $S_3 = N \ltimes U$.

8.5 Definition und Satz

a. Es seien $N_1, \ldots, N_r$ Gruppen.
Betrachten wir das karthesische Produkt $G := \{(n_1, \ldots, n_r) \mid n_i \in N_i\}$ von $N_1, \ldots, N_r$ mit der komponentenweise Multiplikation (d. h. $(n_1, \ldots, n_r) \cdot (m_1, \ldots, m_r) := (n_1 m_1, \ldots, n_r m_r)$), so erhalten wir wieder eine Gruppe, das **(äußere) direkte Produkt** von $N_1, \ldots, N_r$, und schreiben wieder $G = N_1 \times \cdots \times N_r$.

b. Die Gruppe $\tilde{U}$ operiere auf der Gruppe $\tilde{N}$ via φ via Automorphismen, d. h. $\varphi : \tilde{U} \to \mathrm{Aut}(\tilde{N})$ ist ein Homomorphismus (vgl. Beispiel 6.4 a.).
Dann definieren wir auf $G := \left\{(n, u) \mid u \in \tilde{U}, n \in \tilde{N}\right\}$ eine Verknüpfung durch:

$$(n, u) \cdot (m, v) := (n \cdot {}^u m, uv) \text{ für } n, m \in \tilde{N}, u, v \in \tilde{U}.$$

(Wir erinnern uns, daß ${}^u m$ die Kurzschreibweise für $\varphi(u)(m)$ ist - vgl. 6.3.)
Man prüft nach, daß G mit dieser Verknüpfung eine Gruppe wird, das **(äußere) semidirekte Produkt** von $\tilde{N}$ und $\tilde{U}$, und wir schreiben auch: $G = \tilde{N} \ltimes_\varphi \tilde{U}$ (bzw. $\tilde{N} \ltimes \tilde{U}$, falls bezüglich φ keine Unklarheiten bestehen).

Beweis: Vgl. [Gor80] pp. 25-26 oder [Kur77] pp. 17-18, die das semidirekte Produkt jedoch auf dem kartesischen Produkt $\tilde{U} \times \tilde{N}$ definieren. Eine gute Darstellung findet sich auch in [DH92] A.4.22. Dort ist das semidirekten Produkt wie hier auf $\tilde{N} \times \tilde{U}$ definiert. Gleiches gilt für [Wei77] pp. 7-8 und [Hum96] 19.5. □

8.6 Bemerkung
Operiert in 8.5 b. U trivial auf N, so ist das äußere semidirekte Produkt $N \ltimes_\varphi U$ ein direktes Produkt (und umgekehrt), so daß wieder direkte Produkte zweier Gruppen als Spezialfall von semidirekten Produkten aufgefaßt werden können.

8.7 Beispiel
In Beispiel 6.4 wurde gezeigt, daß $\mathbb{Z}/2\mathbb{Z}$ auf $\mathbb{Z}/3\mathbb{Z}$ durch *Inversion* operiert. Das semidirekte Produkt $\mathbb{Z}/3\mathbb{Z} \ltimes \mathbb{Z}/2\mathbb{Z}$ ist eine nicht-abelsche Gruppe der Ordnung 6. (Vgl. auch [Hum96] 19.7.)

8.8 Bemerkung
Die folgenden beiden Sachverhalte, rechtfertigen es, nicht wirklich zwischen inneren und äußeren (semi-)direkten Produkten zu unterscheiden:

a. *Gegeben seien die Voraussetzungen und Bezeichnungen von Definition 8.5. Dann setzen wir* $N := \{(n, e_U) \mid n \in \tilde{N}\}$ *und* $U := \{(e_N, u) \mid u \in \tilde{U}\}$, *und es gilt:* $U \leq G$, $N \trianglelefteq G$, $U \cap N = \mathbb{1}$ *und* $NU = G$, *also ist* $G = N \ltimes U$ *das innere semidirekte Produkt von* N *und* U. *Dabei gilt* $N \cong \tilde{N}$, $U \cong \tilde{U}$ *und die Konjugation von* U *auf* N *entspricht dabei der Operation von* $\tilde{U}$ *auf* $\tilde{N}$.

b. *Gegeben seien nun die Voraussetzungen und Bezeichnungen von Definition 8.2.*
Dann operiert U *auf* N *durch Konjugation, d. h.* $\varphi : U \to \mathrm{Aut}(N) : u \mapsto (N \ni n \mapsto n^u \in N)$ *ist ein Homomorphismus, und* $G \cong N \ltimes_\varphi U$ *als äußeres semidirektes Produkt.*

Analoges gilt für innere und äußere direkte Produkte. (Vgl. [Hum96] 13.7.)

8.9 Beispiel
Die Gruppen $\mathbb{S}_3 = \langle(123)\rangle \ltimes \langle(12)\rangle$ aus 8.4 und $\mathbb{Z}/3\mathbb{Z} \ltimes \mathbb{Z}/2\mathbb{Z}$ aus 8.7 sind also isomorph.

8.10 Satz
Es sei G *eine endliche Gruppe und* $P_1, \ldots, P_r \trianglelefteq G$ *mit paarweise teilerfremder Ordnung und* $G = P_1 \cdots P_r$.
Dann ist $G = P_1 \times \cdots \times P_r$.

Beweis: Vgl. [Kur77] 3.13 (mit leichten Modifikationen). □

8.11 Beispiel
Es sei $N = \langle g \rangle$ eine zyklische Gruppe der Ordnung n und $U = \langle u \rangle$ eine zyklische Gruppe der Ordnung 2. Wie in Beispiel 6.4 d. sieht man, daß U auf N durch Inversion operiert. Das semidirekte Produkt $N \ltimes U$ nennt man eine **Diedergruppe** der Ordnung $2n$, kurz: $\mathbb{D}_{2n}$.
Man beachte, daß gilt: $g^n = u^2 = e$ und $g^u = g^{-1}$.
(Vgl. [Gor80] p. 27 sowie Beispiel 9.10. Diedergruppen werden in aller Ausführlichkeit behandelt in [Wei77] pp. 10-14.)

8.12 Lemma

Sei $N = (GF(3)^2, +)$ *die additive abelsche Gruppe des Vektorraumes* $GF(3)^2$ *über* $GF(3)$ *und* $\varphi : \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(N) = \mathrm{Gl}_2(3)$ *ein nicht-trivialer Gruppenhomomorphismus.*

Dann ist $N \ltimes_\varphi \mathbb{Z}/2\mathbb{Z}$ *isomorph zu genau einer der beiden Gruppen* $N \ltimes \langle A\rangle$ *(d. h.* $N \ltimes_\psi \langle A\rangle$ *mit* $\psi(A) = A$*) mit*

a. $A = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \in \mathrm{Gl}_2(3)$ *oder*

b. $A = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \in \mathrm{Gl}_2(3)$.

Beweis: Es gilt: $\varphi(\mathbb{Z}/2\mathbb{Z}) = \langle A\rangle$ mit $E \neq A \in \mathrm{Gl}_2(3)$ und $A^2 = E$, damit also $N \ltimes_\varphi \mathbb{Z}/2\mathbb{Z} = N \ltimes \langle A\rangle$.

Zeige: Für $B, C, D \in \mathrm{Gl}_2(3)$ mit $D = C^{-1} \cdot B \cdot C$ gilt: $N \ltimes \langle D\rangle \cong N \ltimes \langle B\rangle$.
Definiere dazu die Abbildung $\alpha : N \ltimes \langle D\rangle \to N \ltimes \langle B\rangle : (n, D^k) \mapsto (Cn, B^k)$.
Für $(n, D^k), (m, D^l) \in N \ltimes \langle D\rangle$ gilt:

$$\begin{aligned}\alpha(n, D^k) \cdot \alpha(n, D^l) &= (Cn, B^k) \cdot (Cm, B^l) = (Cn + B^kCm, B^{k+l}) = \\ &= (Cn + B^{k-1} \cdot BCm, B^{k+l}) = (Cn + (CDC^{-1})^{k-1} \cdot CDm, B^{k+l}) = \\ &= (Cn + CD^km, B^{k+l}) = \alpha(n + D^km, D^{k+l}) = \alpha((n, D^k) \cdot (m, D^l)).\end{aligned}$$

Also ist α ein Gruppenhomomorphismus, und die Abbildung $(n, B^k) \mapsto (C^{-1}n, D^k)$ ist offenbar die Umkehrabbildung.

Zeige: $\exists\, 0 \neq n \in N : An = -n$.
Sonst gilt für alle $n \neq 0$: $(0, E) \neq (n + An, E) = (n, A)^2$, also: $o((n, A)) \neq 2$. Dann hat aber $N \ltimes \langle A\rangle$ nur ein Element der Ordnung 2 (denn: $o((n, E)) = o(n) \mid |N| = 9$). Dieses muß dann invariant unter der Konjugation mit allen Gruppenelementen sein, erzeugt also einen Normalteiler $\langle (0, A)\rangle$ von $N \ltimes_\varphi \mathbb{Z}/2\mathbb{Z}$. Also ist die Gruppe direktes Produkt von N und $\mathbb{Z}/2\mathbb{Z}$, im Widerspruch dazu, daß φ nicht der triviale Homomorphismus war.

Zeige: $A \sim \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ oder $A \sim \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$.
Wir haben gezeigt, daß A den Eigenwert -1 besitzt. Also folgt aus dem Satz über die Jordansche Normalform: $A \sim \begin{pmatrix} -1 & k \\ 0 & l \end{pmatrix} \in \mathrm{Gl}_2(3)$, wobei $k \in \{0, 1\}$, falls $l = -1$, und $k = 0$ sonst.
Da $A^2 = E$, gilt ferner: $E = \begin{pmatrix} -1 & k \\ 0 & l \end{pmatrix}^2 = \begin{pmatrix} 1 & k(l-1) \\ 0 & l^2 \end{pmatrix}$.
Also: $(k = 0$ und $l = -1)$ oder $(k = 0$ und $l = 1)$.

Bleibt noch zu zeigen: Die so gewonnenen Gruppen sind nicht isomorph zueinander.
Es sei $g = ((a, b), A) \in N \ltimes \langle A\rangle$.

1. Fall: $A = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$.

$g^2 = ((a-a, b-b), A^2) = ((0,0), E)$, also gilt: $o(g) = 2$, d. h. die Gruppe besitzt neun Elemente der Ordnung 2.

2. Fall: $A = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$.

$g^k = \begin{cases} ((0, k \cdot b), E) & \text{falls } k \equiv 0 (\text{mod } 2) \\ ((a, k \cdot b), A) & \text{falls } k \equiv 1 (\text{mod } 2) \end{cases}.$

Für $b = 0$ gilt also $o(g) = 2$ und für $b \neq 0$ gilt $o(g) = 6$.

Insbesondere hat die Gruppe nur 3 Elemente der Ordnung 2, kann also nicht isomorph zu der im 1. Fall sein.

□

AUFGABEN

8.13 Aufgabe

Zeige, $D_8 = \langle (1\,2\,3\,4) \rangle \ltimes \langle (2\,4) \rangle$.

8.14 Aufgabe

Zeige, $\mathbb{A}_4 = \mathbb{K}_4 \ltimes \langle (1\,2\,3) \rangle$.

8.15 Aufgabe

Ist die Quaternionengruppe $\mathbb{Q}_8$ ein semidirektes Produkt?

8.16 Aufgabe

Man zeige:

$$D_{2n} \cong \begin{cases} \langle (1\,2\,\ldots\,n), (1\,n)(2\,n-1) \cdots \left(\frac{n}{2}-1, \frac{n}{2}+1\right) \rangle < \mathbb{S}_n, & n \text{ gerade} \\ \langle (1\,2\,\ldots\,n), (2\,n)(3\,n-1) \cdots \left(\frac{n-1}{2}, \frac{n+1}{2}\right) \rangle < \mathbb{S}_n, & n \text{ ungerade.} \end{cases}$$

8.17 Aufgabe

Wir werden im folgenden die Diedergruppe $\mathbb{D}_{2n}$ mit der in Aufgabe 8.16 angegebenen Gruppe identifizieren. Bestimme die Elemente und Untergruppen von $\mathbb{D}_{10}$.

9 Freie Gruppen und Relationen

9.1 Allgemeine Hinweise

a. Das vielleicht wirkungsvollste Mittel, sich Gruppen aus dem Nichts zu erschaffen, ist das, Erzeuger und Relationen anzugeben. Dieses Verfahren, so einfach es ist, nachdem man sich in 9.2 und 9.4 einmal davon überzeugt hat, daß es gut geht, hat einen entscheidenden Nachteil. Man weiß i. a. über die entstehenden Gruppen so gut wie gar nichts. Einer Präsentation anzusehen, welche Eigenschaften die Gruppe besitzt, ist alles andere als einfach. Häufig ist nicht einmal zu entscheiden, ob die Gruppe endlich ist, und zwei gegebenen Präsentationen sieht man selten an, ob sie eine isomorphe Gruppe beschreiben. Dennoch wird in den folgenden Klassifikationssätzen neben semidirekten Produkten gerade den Präsentationen die entscheidende Rolle für die Angabe der Gruppen und der Festlegung ihres Isomorphietyps zukommen. Das Verdienst hierfür kommt dem Satz von *von Dyck* und dem daraus abzuleitenden Korollar 9.8 zu. Die zwei für unsere Zwecke wichtigsten Serien von Gruppen, die durch Präsentationen beschrieben werden, sind die Diedergruppen und die dizyklischen Gruppen. Ihnen ist je ein eigener Abschnitt gewidmet, und wir wollen das Kapitel schließen mit der Klassifikation der nicht abelschen Gruppen der Ordnung 8, bei der es eben nur eine Diedergruppe und eine dizyklische Gruppe gibt.

b. Eine kurze Einführung in das Arbeiten mit Relationen inklusive einiger Beispiele findet sich in [Hup67] Kapitel I. § 19. Wesentlich ausführlicher ist dagegen [Wei77] Chapter 2. Fast alle Beispiele endlicher Gruppen, die in [Wei77] vorgestellt werden, sind mittels Präsentationen gegeben. Die Klassifikation der Gruppen der Ordnung 8 findet sich u. a. auch in [Hum96] § 5. Die ausführlichste Darstellung findet sich in [Suz82] Chapter 2 §6.

c. Alle in dem Kapitel vorgestellten Definitionen, Sätze und Beispiele sollten im Vortrag vorkommen. Das Hauptgewicht sollte dabei auf den Beispielen und dem Satz 9.12 liegen, so daß ggf. der Beweis von 9.2 gekürzt werden muß und der Beweis von 9.7 u. U. entfallen kann. Ebenso kann auf die Bemerkung 9.9 verzichtet werden.

9.2 Definition und Satz

Es sei I eine Menge.

Dann gibt es bis auf Isomorphie genau eine Gruppe $\mathcal{F}$ sowie $x_i \in \mathcal{F}$ für $i \in I$ mit folgenden Eigenschaften:

(i) $\mathcal{F} = \langle x_i \mid i \in I \rangle$.

(ii) Ist $G = \langle g_i \mid i \in I \rangle$, so gibt es genau einen Epimorphismus $\pi : \mathcal{F} \to G$ mit $\pi(x_i) = g_i$ für alle $i \in I$.

Diese Gruppe $\mathcal{F}$ heißt **frei** in I (oder frei in den Erzeugenden $(x_i \mid i \in I)$ oder frei vom Rang $|I|$).

Beweis: Vgl. [Hup67] I.19.2 oder [Wei77] pp. 53-56. □

9.3 Beispiel

Die freie Gruppe in einer Erzeugenden ist die abelsche Gruppe $\mathbb{Z}$, wie wir in Satz 10.2 zeigen werden. Sie sowie die freie Gruppe in 0 Erzeugenden, $\mathbb{1}$, sind die einzigen freien Gruppen, die abelsch sind.

9.4 Definition

Es sei I eine Menge, $\mathcal{F}$ die freie Gruppe in $\{x_i \mid i \in I\}$, $R \subseteq \mathcal{F}$.
Wir setzen $\mathcal{R} := \bigcap\{\mathcal{N} \trianglelefteq \mathcal{F} \mid R \subseteq \mathcal{N}\}$ - der kleinste Normalteiler von $\mathcal{F}$, der R enthält. Dann betrachten wir die Faktorgruppe $\mathcal{F}/\mathcal{R}$ und schreiben $\mathcal{F}/\mathcal{R} =: \langle x_i \mid i \in I, R\rangle$.
Wir nennen $\langle x_i \mid i \in I, R\rangle$ eine **Präsentation** der Gruppe $\mathcal{F}/\mathcal{R}$ und die Elemente in R die **Relationen** der Präsentation.

9.5 Bemerkung

Ist $\langle x_i \mid i \in I, R\rangle$ die Präsentation einer Gruppe H, so sind die Elemente von H streng genommen Restklassen der Form $x_{i_1}^{\nu_1} \cdots x_{i_n}^{\nu_n}\mathcal{R}$. Stattdessen werden wir jedoch etwas ungenau nur $x_{i_1}^{\nu_1} \cdots x_{i_r}^{\nu_n}$ schreiben.
Ferner werden wir dann, wenn die Menge $R = \{r_1, \dots, r_l\}$ endlich ist, meist nicht $\langle x_i \mid i \in I, \{r_1, \dots, r_l\}\rangle$ für die Präsentation schreiben, sondern $\langle x_i \mid i \in I, r_1 = e, \dots, r_l = e\rangle$, gemäß dem Umstand, daß r_j aufgefaßt als Element von H gerade das neutrale Element $r_j\mathcal{R} = \mathcal{R}$ von H repräsentiert.
Und zu guter Letzt werden wir eine Relation vom Typ $x_{i_1}^{\nu_1} \cdots x_{i_n}^{\nu_n} = e$ manchmal auch als $x_{i_1}^{\nu_1} \cdots x_{i_s}^{\nu_s} = x_{i_n}^{-\nu_n} \cdots x_{i_{s+1}}^{-\nu_{s+1}}$ schreiben.

9.6 Beispiel

a. $\langle x \mid x^n = e\rangle \cong \mathbb{Z}_n$, vgl Satz 10.2 und Notation 10.3.

b. $\langle x, y \mid xy = yx\rangle \cong \mathbb{Z} \times \mathbb{Z}$.

9.7 Satz (von Dyck)

Es sei I *eine Menge,* $G = \langle g_i \mid i \in I\rangle$ *eine Gruppe,* $\mathcal{F} = \langle x_i \mid i \in I\rangle$ *die freie Gruppe in* I *und* $\pi : \mathcal{F} \to G$ *der nach 9.2 existierende eindeutige Epimorphismus von* $\mathcal{F}$ *nach* G. *Ferner sei* $R \subseteq \mathcal{F}$ *eine Menge von* Relationen.
Gilt $\pi(R) = \mathbb{1}$ *(wir sagen dann, die* g_i *genügen den Relationen* R*), dann gibt es genau einen Epimorphismus* $\bar{\pi} : \langle x_i \mid i \in I, R\rangle \to G$ *mit* $\bar{\pi}(x_i) = g_i$ *für alle* $i \in I$ *(nämlich den durch* π *induzierten).*

Beweis: Vgl. [Hup67] I.19.4 sowie [Wei77] 2.2.5 - für das folgende Korollar vgl. [Wei77] 2.2.6. □

9.8 Korollar

Es sei $\langle x_1, \dots, x_n \mid R\rangle$ *die Präsentation einer endlichen Gruppe* H, *es sei* $G = \langle g_1, \dots, g_n\rangle$ *und die* g_i *mögen den Relationen* R *genügen.*
Gilt ferner, daß $|G| \geq |H|$, *so gilt* $G \cong H$.

9.9 Bemerkung
Jede endliche Gruppe besitzt eine endliche Präsentation, d. h. zu einer endlichen Gruppe G gibt es eine freie Gruppe von *endlichem* Rang sowie eine *endliche* Menge von Relationen, so daß die zugehörige Präsentation eine zu G isomorphe Gruppe liefert. (Vgl. [Suz82] Chapter 2 §6 Corollary 2.)

9.10 Beispiel (Diedergruppe)

a. $\langle x, y \mid x^n = y^2 = e, x^y = x^{-1}\rangle \cong \mathbb{D}_{2n}$ und für $z \notin \langle x\rangle$ gilt $o(z) = 2$.

b. $\langle a, b \mid a^2 = b^2 = (ab)^n = e\rangle \cong \mathbb{D}_{2n}$

c. Das Untergruppendiagramm der $\mathbb{D}_8$ entnehme man [Wei77] Example 4.3.

(Zu Diedergruppen i. a. vgl. auch [Kur77] 5.2 sowie [Wei77] pp. 10-14 und insbesondere Example 4.1 (pp. 101-103) !!! Siehe auch [Hum96] 4.10.)

Beweis: a. Beachte, wegen 8.11 und Korollar 9.8 reicht es zu zeigen, daß die Präsentation höchstens $2n$ Elemente enthält. Nun folgt aus $x^y = x^{-1}$ und $x^n = e$, daß gilt $yx = x^{n-1}y$. Also läßt sich jedes Element auf die Gestalt $x^\nu y^\mu$ bringen, wobei wegen $x^n = y^2 = e$ gilt, daß $0 \leq \mu \leq 1$ und $0 \leq \nu \leq n-1$. Daraus folgt die erste Behauptung. Ferner gilt für $z \notin \langle x\rangle$, z ist von der Gestalt $z = x^\nu y$, also $z^2 = x^\nu y x^\nu y = x^\nu y x^\nu y^{-1} = x^\nu x^{-\nu} = e$.

b. Vgl. [Hup67]I.19.5.

□

9.11 Beispiel (Dizyklische Gruppe, verallg. Quaternionengruppe)
Für $n \in \mathbb{N}$ heißt die Gruppe $\mathbb{H}_n = \langle x, y \mid x^{2n} = e, y^2 = x^n, x^y = x^{-1}\rangle$ die **Dizyklische Gruppe** der Ordnung $4n$.
Ist speziell $n = 2^{k-2}$ eine 2-Potenz, so heißt $\mathbb{H}_{2^{k-2}}$ auch **verallgemeinerte Quaternionengruppe** der Ordnung 2^k und wir schreiben $\mathbb{Q}_{2^k}$, ist $k = 3$, so heißt die Gruppe schlicht die **Quaternionengruppe**.
Für die Dizyklische Gruppe $\mathbb{H}_n$ gilt:

(i) $|\mathbb{H}_n| = 4n$.

(ii) $\langle x\rangle \lhd \mathbb{H}_n$ mit $|\mathbb{H}_n : \langle x\rangle| = 2$.

(iii) $\langle x^n\rangle$ die einzige Untergruppe von $\mathbb{H}_n$ der Ordnung 2 und ist für $n > 1$ das Zentrum von $\mathbb{H}_n$. Insbesondere gilt also: $\mathbb{H}_n \ncong \mathbb{D}_{4n}$.

Beweis: Wie in 9.10 zeigt man: $\mathbb{H}_n = \left\{x^k y^l \mid 0 \leq l \leq 1, 0 \leq k \leq 2n-1\right\}$ und $o(x^k y) = 4$ für alle k. Beachtet man dann, daß eine zyklische Untergruppe gerader Ordnung genau eine Untergruppe der Ordnung 2 besitzt (vgl. Satz 10.4), so ist man fertig.
(Die einzige Schwierigkeit besteht darin, zu zeigen, daß $|\mathbb{H}_n| \geq 4n$. Wegen Korollar 9.8 reicht es hierfür, eine Gruppe der Ordnung 4n zu finden, die von zwei Elementen, die den Relationen von $\mathbb{H}_n$ genügen, erzeugt wird.
Wir betrachten dazu die Menge G der Ausdrücke der Form (x^k, y^l) mit $0 \leq l \leq 1, 0 \leq k \leq 2n-1$. Dann enthält G gerade $4n$ Elemente. Unser Ziel ist es, auf G eine Gruppenstruktur zu definieren. Dazu bezeichnen wir für $k \in \mathbb{Z}$ mit $\overline{k}$ den zwischen 0 und $2n-1$ liegenden Vertreter der Restklasse $k + 2n\mathbb{Z}$

und definieren auf G eine Multiplikation durch:

$$(x^j, y^i)(x^k, y^l) := \begin{cases} (x^{\overline{k+i}}, y^l), & \text{falls } j = 0, \\ (x^{\overline{-k+i}}, y^1), & \text{falls } j = 1 \text{ und } l = 0, \\ (x^{\overline{-k+i+n}}, y^0), & \text{falls } j = 1 \text{ und } l = 1. \end{cases}$$

Man prüft nach, daß G mit dieser Multiplikation assoziativ ist mit neutralem Element (x^0, y^0) und daß das Inverse zu (x^k, y^l) gegeben ist durch:

$$(x^k, y^l)^{-1} := \begin{cases} (x^{2n-k}, y^0), & \text{falls } l = 0, \\ (x^{\overline{k-n}}, y^1), & \text{falls } l = 1. \end{cases}$$

Ferner sieht man sofort, daß $G = \langle (x^1, y^0), (x^0, y^1) \rangle$ und daß diese Erzeuger den Relationen der $\mathbb{H}_n$ genügen.)

(Vgl. auch [Wei77] Example 4.4 (pp. 108-112), insbesondere Note 1. Siehe ferner auch [Hum96] 22.7.) □

9.12 Satz

Ist G eine nicht abelsche Gruppe der Ordnung 8, so ist G entweder isomorph zur Diedergruppe $\mathbb{D}_8$ oder zur Quaternionengruppe $\mathbb{Q}_8$.

Beweis: Da G nicht abelsch ist, kann es kein Element der Ordnung 8 in G geben, muß aber zugleich wegen Satz 1.14 ein Element n der Ordnung $o(n) > 2$ existieren. Also ist $o(n) = 4$ und damit $N := \langle n \rangle \lhd G$, wegen $|G : N| = 2$. Wähle $u \in G \backslash N$. Wegen $o(n^u) = o(n) = 4$ und $n^u \neq n$, gilt: $n^u = n^{-1}$, und aus Ordnungsgründen gilt: $G = N\langle u \rangle$.

1. Fall: $o(u) = 2$: Dann mit 9.8: $G = \langle n, u \mid n^4 = e, u^2 = e, n^u = n^{-1} \rangle \cong \mathbb{D}_8$.

2. Fall: $o(u) = 4$: Dann mit 9.8: $G = \langle n, u \mid n^4 = e, u^2 = n^2, n^u = n^{-1} \rangle \cong \mathbb{Q}_8$.

(Vgl. auch [Wei77] Example 4.3 & 4.4 (pp. 106-112) sowie [Hum96] pp. 46-47 und [Hup67] I.14.10.) □

AUFGABEN

9.13 Aufgabe

Wir wollen in dieser Aufgabe die Diedergruppen etwas näher kennen lernen.

a. Bestimme die Elemente $\mathbb{D}_{2n}$ und ihre Ordnungen.

b. Bestimme $Z(D_{2n})$.

c. Zeige, $D_{4n}/Z(D_{4n}) \cong D_{2n}$.

d. Zeige, gilt $m|n$, dann gibt es einen Monomorphismus $\alpha : D_{2m} \to D_{2n}$.

(Vgl. [Wei77] Example 4.1.)

9.14 Aufgabe

Zwecks besserem Verständnis der Gruppe $\mathbb{H}_3$ bestimme man:

a. die Elemente von $\mathbb{H}_3$ und ihre Ordnungen,

b. die Untergruppen und Normalteiler von $\mathbb{H}_3$ sowie

c. $Z(\mathbb{H}_3)$.

(Vgl. [Wei77] Example 4.5.)

10 Zyklische Gruppen

10.1 Allgemeine Hinweise

a. Gruppen, die von nur einem Element erzeugt werden, sind besonders einfach. Dies zeigt sich in ihrer Klassifikation, die wir gleich im ersten Satz (ohne Verwendung des Hauptsatzes über endliche abelsche Gruppen) durchführen, sowie in der Struktur ihrer Untergruppen, die wir dann in 10.4 durchleuchten. Aus letzterer Untersuchung folgt unmittelbar, daß zyklische Gruppen von Primzahlordnung die einzigen einfachen abelschen Gruppen sind. Eine Frage, die bei der Untersuchung konkreter Gruppen immer wieder auftaucht, ist die Frage, wie sich die Ordnung von Elementen auf deren Produkte überträgt. Einige Antworten finden sich in den Lemmata 10.7 und 10.8. Von gleichem Interesse ist die Frage, was sich aus der Gruppenordnung über die Existenz von Elementen mit vorgegebener Ordnung sagen läßt. Eine negative Aussage in Form der Begrenzung der möglichen Elementordnungen stellte der Satz von Lagrange dar. In den Folgerungen 10.9 und 10.11 geben wir nun positive Aussagen im Fall von abelschen Gruppen und wenden diese an, um zu zeigen, daß endliche Untergruppen der multiplikativen Gruppe eines Körpers stets zyklisch sein müssen.

b. Eine ausführliche Darstellung zur Struktur der zyklischen Gruppen findet sich in [Doe74] Kapitel VII. § 4 sowie in [Kur77] Kapitel II. § 1.

c. Von großer Bedeutung für die angestrebte Klassifikation sind die Resultate in 10.2, 10.4 b. sowie 10.7–10.11. Sie sollten inklusive der Beweise Bestandteil des Vortrags sein. Alle anderen Ergebnisse des vorliegenden Kapitels können entfallen.

10.2 Satz

Es sei G *eine zyklische Gruppe.*

a. *Ist* $|G| = \infty$*, so ist* $G \cong (\mathbb{Z}, +)$.

b. *Ist* $|G| = n < \infty$*, so ist* $G \cong (\mathbb{Z}/n\mathbb{Z}, +)$.

Beweis: Vgl. [Doe74] VII.4.4 oder [Kur77] 2.2. $\square$

10.3 Notation

Für die bis auf Isomorphie eindeutig bestimmte zyklische Gruppe der Ordnung $n < \infty$ schreiben wir von nun an $\mathbb{Z}_n$.

10.4 Satz

Es sei $G = \langle g \rangle$ *eine zyklische Gruppe.*

a. *Ist* $|G| = \infty$*, so ist* $U \leq G$ *genau dann, wenn es ein* $k \in \mathbb{N}_0$ *gibt mit* $U = \langle g^k \rangle =: U_k$*. Für* $k \in \mathbb{N}$ *gilt dabei:* $|G : U_k| = k$.
Insbesondere gilt: $U_k \neq U_l$ *für* $k \neq l$ *- es gilt aber sehr wohl* $U_k \cong G$ *für alle* $k \in \mathbb{N}$.

b. *Ist* $|G| = n < \infty$, *so ist* $U \leq G$ *genau dann, wenn es ein* $d|n$ *gibt mit* $U = \langle g^{\frac{n}{d}} \rangle$. *Dann gilt:* $|U| = d$.
Insbesondere gibt es zu jedem Teiler d *von* $|G|$ *also* genau eine *Untergruppe der Ordnung* d.

Beweis: Vgl. [Doe74] VII.4.5 oder [Kur77] 2.1 und 2.4 sowie [Hum96] 4.13-15. □

10.5 Korollar
Jede Untergruppe einer zyklischen Gruppe ist zyklisch.

10.6 Korollar
Eine abelsche Gruppe $G \neq \mathbb{1}$ *ist genau dann einfach, wenn* $|G|$ *eine Primzahl ist.*

Beweis: Vgl. [Doe74] VII.4.11. (Verwende Satz 2.9.) □

10.7 Lemma
Es sei G *eine Gruppe,* $g \in G$ *mit* $o(g) = n < \infty$ *und* $k \in \mathbb{N}$.
Dann gilt: $o(g^k) = \frac{n}{(n,k)}$.

Beweis: Vgl. [Doe74] VII.4.6. □

10.8 Folgerung
Sei G *eine Gruppe,* $g, h \in G$ *mit* $gh = hg$, $o(g), o(h) < \infty$ *und* $(o(g), o(h)) = 1$.
Dann gilt $o(gh) = o(g)o(h)$.
Insbesondere folgt: $\mathbb{Z}_n \times \mathbb{Z}_m \cong \mathbb{Z}_{nm}$, *falls nur* $(n, m) = 1$.

Beweis: Vgl. [Doe74] VII.4.9. □

10.9 Folgerung
Es sei G *eine endliche abelsche Gruppe mit* $d \mid \mathrm{Exp}(G)$.
Dann gibt es in G *ein Element der Ordnung* d.

Beweis: Es sei $m = p_1^{\gamma_1} \cdots p_r^{\gamma_r}$ die Primfaktorzerlegung von $m := \mathrm{Exp}(G)$. Dann gibt es nach der Definiton des Exponenten für jedes $i = 1, \ldots, r$ ein $g_i \in G$ mit $p_i^{\gamma_i} | o(g_i)$. Wegen Lemma 10.7 gilt o. E. $o(g_i) = p_i^{\gamma_i}$, und dann folgt mit 10.8 für $g := g_1 \cdots g_r :\ o(g) = m$. Aber nach Lemma 10.7 gilt dann für $h := g^{\frac{m}{d}}$ dann $o(h) = d$. □

10.10 Lemma
Es sei G *eine endliche Gruppe und* $N \trianglelefteq G$, *dann gilt* $\mathrm{Exp}(G/N) \,\big|\, \mathrm{Exp}(G)$.

Beweis: Für $gN \in G/N$ gilt $(gN)^{o(g)} = g^{o(g)}N = N$, und damit $o(gN) \mid o(g)$. Aber dann gilt auch $\mathrm{Exp}(G/N) = \mathrm{kgV}\{o(gN) \mid g \in G\} \,\big|\, \mathrm{kgV}\{o(g) \mid g \in G\} = \mathrm{Exp}(G)$. □

10.11 Folgerung
Es sei G *eine endliche abelsche Gruppe und* p *eine Primzahl mit* $p \mid |G|$.
Dann gilt auch $p \mid \mathrm{Exp}(G)$.
Insbesondere gibt es ein Element der Ordnung p *in* G.

Beweis: Wir führen den Beweis durch Induktion nach $n := |G|$. Für $n = 1$ ist nichts zu zeigen. Sei also $n > 1$. Dann gibt es ein Element $g \in G$ mit $d := o(g) > 1$. Falls $p \mid d$, dann gilt auch $p \mid \operatorname{Exp}(G)$. Es gelte also $p \nmid d$. Für $H := G/\langle g\rangle$ gilt dann $p \mid \frac{n}{d} = |H| < n$, und per Induktion folgt $p \mid \operatorname{Exp}(H)$. Aber mit Lemma 10.10 folgt dann $p \mid \operatorname{Exp}(G)$. $\square$

10.12 Satz

Es sei $G \leq K^*$ *eine* endliche *Untergruppe der multiplikativen Gruppe des Körpers* K*, dann ist* G *zyklisch.*
Insbesondere ist die multiplikative Gruppe eines endlichen Körpers zyklisch.

Beweis: Es sei $m := \operatorname{Exp}(G)$, dann gilt für $g \in G$, $g^m = e$, also ist g Nullstelle des Polynoms $f := x^m - 1 \in K[x]$. Dann ist aber $|G| \leq m$.
Nun gilt nach Folgerung 10.9, daß es ein Element h in G gibt mit $o(h) = m$.
Folglich gilt: $|G| \leq m = o(h) = |\langle h\rangle| \leq |G|$, und somit ist $G = \langle h\rangle$.
(Vgl. auch [Hum96] 14.15.) $\square$

AUFGABEN

10.13 Aufgabe

Betrachte die Untergruppe $G := \left\{z \in \mathbb{C} \;\middle|\; |z| = 1\right\}$ der multiplikativen Gruppe $\left(\mathbb{C}^*, \cdot\right)$ des Körpers $\mathbb{C}$. Man zeige, $(G, \cdot) \cong (\mathbb{Z}_n, +)$.

10.14 Aufgabe

Man bestimme folgende Exponenten: $\operatorname{Exp}(\mathbb{D}_8)$, $\operatorname{Exp}(\mathbb{A}_4)$ und $\operatorname{Exp}(\mathbb{S}_4)$.

10.15 Aufgabe

Man finde je einen Erzeuger der zyklischen Gruppen $(Z_2^*, \cdot)$, $(Z_3^*, \cdot)$, $(Z_5^*, \cdot)$ und $(Z_7^*, \cdot)$.

11 ABELSCHE GRUPPEN

11.1 Allgemeine Hinweise

a. Bisher ist es uns gelungen, die zyklischen Gruppen zu klassifizieren, bei welchen die Vielfalt nicht sehr groß war. Der nächst schwierigere Schritt ist die Klassifikation aller abelschen Gruppen, und es zeigt sich, daß auch deren Vielfalt eigentlich nicht größer ist, denn sie lassen sich aus zyklischen Gruppen durch die einfache Methode der direkten Produkte gewinnen. Dies ist die Aussage des zentralen Satzes in dem vorliegenden Kapitel. Eine unmittelbare Folgerung ist die, daß für abelsche Gruppen die Umkehrung des Satzes von Lagrange gilt, ein Ergebnis, das auch für eine weitere Klasse von Gruppen zutrifft, die wir hier jedoch nicht betrachten können, die nilpotenten Gruppen. Wir wollen das Kapitel mit der Einführung des Begriffes der elementarabelschen Gruppe abschließen und zeigen, daß die elementarabelschen Gruppen mit den Vektoräumen über Körpern von Primzahlordnung und ihre Automorphismen mit den zugehörigen linearen Automorphismen identifiziert werden können.

b. Die endlichen abelschen Gruppen werden in [Kur77] Kapitel II. § 2 rein gruppentheoretisch klassifiziert, während der Hauptsatz über abelsche Gruppen in [Hup67] Kapitel I. § 13 aus dem Struktursatz für endlich erzeugbare Moduln über Hauptidealringen hergeleitet wird. Eine alternative Formulierung sowie einen weiteren gruppentheoretischen Beweis findet man in [Hum96] § 14.

c. Die Ergebnisse in 11.6–11.10 dienen ausschließlich dazu, das wesentliche Resultat des Abschnitts, den Hauptsatz über endliche abelsche Gruppen, zu beweisen. Die Beweise der einzelnen Schritte sollten - unter Berücksichtigung der zur Verfügung stehenden Zeit - vorgeführt werden; ebenso der Beweis von Korollar 11.12. Korollar 11.11 kann entfallen.

11.2 Definition

Es sei G eine endliche Gruppe, p eine Primzahl.
Eine **p-Sylowgruppe** (korrekter p-Sylowuntergruppe) P von G ist eine maximale p-Untergruppe von G, d. h. $|P| = p^\nu$ für ein $\nu \in \mathbb{N}_0$ und für jedes $P \leq \tilde{P} \leq G$ mit $|\tilde{P}| = p^\mu$ gilt $P = \tilde{P}$.
Die Menge der p-Sylowgruppen von G bezeichnen wir mit $\mathrm{Syl}_p(G)$.

11.3 Theorem (Hauptsatz über endliche abelsche Gruppen)

Es sei G *eine endliche abelsche Gruppe der Ordnung* $|G| = p_1^{\nu_1} \cdot \ldots \cdot p_r^{\nu_r}$ *mit paarweise verschiedenen Primzahlen* p_i.
Dann ist G *das direkte Produkt seiner Sylowgruppen* A_{p_i}, $i = 1, \ldots, r$, *und für jedes* A_{p_i} *gilt:*

$$\exists_! \; 1 \leq \nu_{i,1} \leq \ldots \leq \nu_{i,s_i} : \sum_{j=1}^{s_i} \nu_{i,j} = \nu_i \text{ und } A_{p_i} \cong \mathbb{Z}_{p_i^{\nu_{i,1}}} \times \ldots \times \mathbb{Z}_{p_i^{\nu_{i,s_i}}},$$

d. h. A_{p_i} *ist (in eindeutiger Weise) direktes Produkt zyklischer Gruppen von Primzahlpotenzordnung.*
Das Tupel $(p_1^{\nu_{1,1}},\ldots,p_1^{\nu_{1,s_1}},p_2^{\nu_{2,1}}\ldots,p_2^{\nu_{2,s_2}},\ldots,p_r^{\nu_{r,1}},\ldots,p_r^{\nu_{r,s_r}})$ *heißt der* ***Typ*** *der Gruppe* G *und bestimmt diese bis auf Isomorphie eindeutig.*

Beweis: Der Beweis folgt aus den beiden Lemmata 11.7 und 11.10.
Alternativ läßt er sich aus dem Struktursatz über endlich erzeugte Moduln über Hauptidealringen folgern, vgl. Bertram Huppert, Endliche Gruppen I, Satz I.13.2. □

11.4 Beispiel

a. Die möglichen Typen von abelschen Gruppen der Ordnung $18 = 2\cdot 3^2$ sind $(2,3,3)$ und $(2,3^2)$.

b. Es gibt bis auf Isomorphie genau eine abelsche Gruppe der Ordnung 7905, sie besitzt den Typ $(3,5,17,31)$ und ist somit zyklisch.

c. Die abelsche Gruppe $\mathbb{Z}_6\times\mathbb{Z}_{10}\times\mathbb{Z}_{15}$ hat den Typ $(2,2,3,3,5,5)$, die Gruppe $\mathbb{Z}_9\times\mathbb{Z}_{10}\times\mathbb{Z}_{10}$ hat hingegen den Typ $(2,2,3^2,5,5)$.

11.5 Definition und Bemerkung

Es sei G eine endliche abelsche Gruppe und $m\in\mathbb{N}$. Dann betrachten wir den Gruppenhomomorphismus μ_m aus Beispiel 3.3 und definieren $G_m := \mathrm{Ker}(\mu_m) = \{g\in G \mid g^m = e\}\trianglelefteq G$.
Aus den Definitionen folgt unmittelbar $\mathrm{Exp}(G_m)\mid m$, und falls $m = \mathrm{Exp}(G)$, so gilt stets $G = G_m$.

11.6 Lemma

Ist G *eine abelsche Gruppe mit* $|G| = m_1m_2$ *und* $(m_1,m_2) = 1$*, dann ist* $G = G_{m_1}\times G_{m_2}$ *und* $|G_{m_i}| = m_i$ *für* $i = 1,2$.

Beweis: Wir setzen $H := G_{m_1}G_{m_2}\le G$ und zeigen zunächst, daß $H = G$. Da $(m_1,m_2) = 1$, gibt es ganze Zahlen $a,b\in\mathbb{Z}$ mit $1 = m_1a+m_2b$. Für $g\in G$ gilt $e = g^{m_1m_2}$, und somit $g^{m_1}\in G_{m_2}$ und $g^{m_2}\in G_{m_1}$. Aber damit folgt

$$g = g^{m_1a+m_2b} = \left(g^{m_1}\right)^a\cdot\left(g^{m_2}\right)^b\in G_{m_1}G_{m_2} = H.$$

Ferner gilt für $g\in G_{m_1}\cap G_{m_2}$

$$o(g)\;\Big|\;\big(\mathrm{Exp}(G_{m_1}),\mathrm{Exp}(G_{m_2})\big)\;\Big|\;(m_1,m_2) = 1,$$

also ist $G_{m_1}\cap G_{m_2} = \mathbb{1}$.
Damit ist G das innere direkte Produkt von G_{m_1} und G_{m_2}. Da $\mathrm{Exp}(G_{m_i})$ ein Teiler von m_i ist, kommen nach Lemma 10.11 in $|G_{m_i}|$ nur Primteiler von m_i vor, und da $(m_1,m_2) = 1$ und $|G_{m_1}|\cdot|G_{m_2}| = |G| = m_1m_2$, folgt $|G_{m_i}| = m_i$. (Vgl. [Kur77] II.2.8.) □

11.7 Lemma

Es sei G *eine endliche abelsche Gruppe der Ordnung* $|G| = p_1^{\nu_1}\cdot\ldots\cdot p_r^{\nu_r}$ *mit paarweise verschiedenen Primzahlen* p_i.

Dann besitzt G *für jedes* $i = 1, \dots, r$ *genau eine* p_i*-Sylowgruppe* $A_{p_i} = G_{p_i^{\nu_i}}$, G *ist das direkte Produkt dieser Sylowgruppen, und es gilt* $|A_{p_i}| = p_i^{\nu_i}$.

Beweis: Wir führen den Beweis durch Induktion über die Anzahl r der Primteiler von $|G|$. Im Fall $r = 0$ oder $r = 1$ ist nichts zu zeigen. Sei deshalb $r \geq 2$. Wir setzen $m = p_2^{\nu_2} \cdot \dots \cdot p_r^{\nu_r}$, dann gilt nach Lemma 11.6 $G = G_{p_1^{\nu_1}} \times G_m$, $|G_{p_1^{\nu_1}}| = p_1^{\nu_1}$ und $|G_m| = m$. Insbesondere ist $G_{p_1^{\nu_1}}$ eine p_1-Gruppe. Per definitionem enthält sie zudem alle Elemente von G von p_1-Potenzordnung und ist somit die eindeutig bestimmte p_1-Sylowgruppe von G. Ferner gilt per Induktion, daß $G_m = G_{p_2^{\nu_2}} \times \dots \times G_{p_r^{\nu_r}}$, wobei die $G_{p_i^{\nu_i}}$ die eindeutig bestimmten p_i-Sylowgruppen von G_m, und aus Ordnungsgründen damit von G, sind mit $|G_{p_i^{\nu_i}}| = p_i^{\nu_i}$. (Vgl. [Kur77] II.2.9.) □

11.8 Satz

Eine nicht-triviale abelsche p*-Gruppe ist genau dann zyklisch, wenn sie nur eine Untergruppe der Ordnung* p *besitzt.*

Beweis: Ist $G \neq \mathbb{1}$ eine zyklische p-Gruppe, so besitzt G nach Satz 10.4 genau eine Untergruppe der Ordnung p.
Sei also umgekehrt G eine abelsche p-Gruppe mit nur einer Untergruppe der Ordnung p. Dann ist diese gerade $G_p = \mathrm{Ker}(\mu_p)$, und mittels des Homomorphiesatzes erhalten wir

$$p = |G_p| = |G/\mathrm{Im}(\mu_p)|.$$

Ist $\mathrm{Im}(\mu_p) = \mathbb{1}$, so ist G zyklisch nach Satz 1.13. Andernfalls ist $\mathrm{Im}(\mu_p)$ eine Untergruppe von G kleinerer Ordnung und besitzt in Anbetracht von Folgerung 10.11 ebenfalls exakt eine Untergruppe der Ordnung p. Mithin ist $\mathrm{Im}(\mu_p) = \langle h \rangle$ zyklisch per Induktion. Sei nun $g \in G$ mit $h = \mu_p(g) = g^p$, dann gilt nach Lemma 10.7

$$o(g) = p \cdot o(h) = p \cdot |\mathrm{Im}(\mu_p)| = |G|,$$

und mithin ist $G = \langle g \rangle$. (Vgl. [Kur77] II.2.13.) □

11.9 Lemma

Es sei G *eine abelsche* p*-Gruppe und* $g \in G$ *mit* $o(g) = \mathrm{Exp}(G)$. *Dann gibt es eine Untergruppe* $H \leq G$ *mit* $G = \langle g \rangle \times H$.

Beweis: Vgl. [Kur77] II.2.14. □

11.10 Lemma

Es sei G *eine abelsche* p*-Gruppe mit* $|G| = p^\nu$, *dann gilt*

$$\exists_! \; 1 \leq \nu_1 \leq \dots \leq \nu_s : \sum_{j=1}^{s} \nu_j = \nu \text{ und } G \cong \mathbb{Z}_{p^{\nu_1}} \times \dots \times \mathbb{Z}_{p^{\nu_s}}.$$

Beweis: Vgl. [Kur77] II.2.15. □

11.11 Korollar

Eine endliche abelsche Gruppe ist genau dann zyklisch, wenn ihre p*-Sylowgruppen zyklisch sind.*

Beweis: Dies folgt unmittelbar aus dem Hauptsatz über abelsche Gruppen und der Folgerung 10.8. □

11.12 Korollar

Es sei G *eine endliche abelsche Gruppe und* d *ein Teiler von* $|G|$, *dann gibt es eine Untergruppe der Ordnung* d.

Beweis: Aus dem Hauptsatz über abelsche Gruppen (Satz 11.3) folgt, ist $|G| = p_1^{\nu_1} \cdots p_r^{\nu_r}$ die Primfaktorzerlegung von $|G|$, so ist G direktes Produkt von Gruppen A_i mit $|A_i| = p_i^{\nu_i}$, $i = 1, \dots, r$, und die A_i sind direkte Produkte von zyklischen p_i-Gruppen. Nach Satz 10.4 besitzen letztere zu jeder p_i-Potenz, die ihre Ordnung teilt, eine Untergruppe der entsprechenden Ordnung. Ist nun $d = p_1^{l_1} \cdots p_r^{l_r}$, so besitzt A_i eine Untergruppe B_i (= direktes Produkt von gewissen Untergruppen der zyklischen p_i-Gruppen) mit $|B_i| = p_i^{l_i}$ und $B_1 \times \ldots \times B_r$ ist eine Untergruppe von G von der Ordnung d. □

AUFGABEN

11.13 Aufgabe

Man bestimme die Untergruppen von $\mathbb{Z}_4 \times \mathbb{Z}_2$.

12 Der Satz von Sylow

12.1 Allgemeine Hinweise

a. Bereits im Kapitel zum Satz von Lagrange haben wir uns die Frage gestellt, für welche Teiler der Gruppenordnung Untergruppen der entsprechenden Ordnung existieren. Der Satz von Cauchy sagt nun, daß das für jede Primzahlpotenz, die die Gruppenordnung teilt, gilt, und der Satz von Sylow sagt des weiteren, daß die Untergruppen zu maximalen Primzahlpotenzen alle zueinander konjugiert sind. Die weitere Aussage des Satzes, daß nämlich die Anzahl solcher Gruppen modulo der zugehörigen Primzahl stets eins ist, ist eines der wichtigsten Hilfsmittel der Kapitel 14 und 15. Auf die Bedeutung des Frattiniargumentes, das hier in einer spezielleren Formulierung gegeben wird, haben wir bereits in Kapitel 6 hingewiesen. Ebenso ist Satz 12.9 ein starkes Hilfsmittel bei der Untersuchung nilpotenter und auflösbarer Gruppen. Wir schließen das Kapitel mit einer sehr simplen Folgerung aus dem Satz von Sylow und der Produktformel, daß nämlich die Sylowgruppen einer Gruppe selbige erzeugen.

b. Wir folgen im vorliegenden Kapitel [Kur77] Kapitel III. § 3. Einen leicht modifizierten Zugang, der sich im wesentlichen auf die Verallgemeinerung des Satzes von Cauchy in Bemerkung 12.5 stützt, findet sich in [Hup67] Kapitel I. § 7. Eine wiederum leicht modifizierte Beweisvariante, die gänzlich auf den Satz von Cauchy verzichtet, findet sich in [Hum96] § 11.

c. Die Sätze, die in engerem Zusammenhang mit dem Satz von Sylow stehen, sollen im Vortrag enthalten sein und bewiesen werden. Dazu zählen 12.2 bis 12.4 sowie 12.9 und 12.11, wobei bei letzterem ggf. auf den Beweis verzichtet werden kann. Ebenfalls entfallen können die Bemerkung 12.5 und das Frattiniargument sowie u. U. der Beweis zu 12.7. Hingegen sollten die Beispiele auf alle Fälle enthalten sein, und nach Möglichkeit auch Satz 12.10, sofern nicht bereits in Kapitel 5 ein Beweis erfolgt ist.

12.2 Satz (Cauchy)

Es sei G *eine endliche Gruppe und* p *eine Primzahl mit* $p^i \mid |G|$.
Dann besitzt G *eine Untergruppe* $U \le G$ *der Ordnung* p^i.

Beweis: Vgl. [Kur77] 3.9. □

12.3 Lemma

Es sei G *eine endliche Gruppe,* p *eine Primzahl und* $P \in \mathrm{Syl}_p(G)$. *Dann gilt* $\mathrm{Syl}_p(N_G(P)) = \{P\}$.

Beweis: Vgl. [Kur77] 3.10 c). Siehe auch [Hum96] 11.9. □

12.4 Theorem (Sylow)

Es sei G *eine endliche Gruppe und* p *eine Primzahl mit* $|G| = p^\nu m$ *und* $p \nmid m$.

a. $P \in \mathrm{Syl}_p(G) \;\Leftrightarrow\; |P| = p^\nu$.

b. *Die p-Sylowgruppen von* G *sind zueinander konjugiert in* G, *d. h. für* $P, \tilde{P} \in \mathrm{Syl}_p(G)\ \exists g \in G\ :\ \tilde{P} = P^g$.
Insbesondere gilt also für jedes $P \in \mathrm{Syl}_p(G)\ :\ |\mathrm{Syl}_p(G)| = |G : N_G(P)|$.

c. $|\mathrm{Syl}_p(G)| \equiv 1 (\mathrm{mod}\ p)$.

Beweis: Vgl. [Kur77] 3.11. □

12.5 Bemerkung

Die letzte Aussage im Satz von Sylow 12.4 läßt sich verschärfen (vgl. [Hup67] I.7.2 oder [Hum96] Remark on p. 101):
Ist G *eine endliche Gruppe,* p *eine Primzahl mit* $p^a \mid |G|$ *und* $N(p^a)$ *bezeichne die Anzahl der Untergruppen von* G *der Ordnung* p^a, *so gilt:*

$$N(p^a) \equiv 1 (\mathrm{mod}\ p).$$

Dies ist zugleich eine Verallgemeinerung des Satzes von Cauchy (12.2). Eine weitere Verschärfung der Aussage findet sich in [Hup67] I.7.9.

12.6 Beispiel

a. $\mathrm{Syl}_2 \mathbb{S}_3 = \{\langle(12)\rangle, \langle(13)\rangle, \langle(23)\rangle\}$ und $\mathrm{Syl}_3(\mathbb{S}_3) = \{\langle(123)\rangle\}$.

b. $\mathrm{Syl}_2(\mathbb{S}_4) = \{\langle(1234),(24)\rangle, \langle(1243),(23)\rangle, \langle(1324),(34)\rangle\}$ und die 2-Sylowgruppen von $\mathbb{S}_4$ sind alle isomorph zur $\mathbb{D}_8$.

12.7 Korollar

Es sei G *eine endliche Gruppe,* p *eine Primzahl,* $P \in \mathrm{Syl}_p(G)$, $N \trianglelefteq G$, $U \leq G$.

a. $P \trianglelefteq G \ \Leftrightarrow\ \mathrm{Syl}_p(G) = \{P\}$

b. $P \cap N \in \mathrm{Syl}_p(N)$

c. $PN/N \in \mathrm{Syl}_p(G/N)$

d. *Ist* $Q \in \mathrm{Syl}_p(U)$, *dann* $\exists \tilde{P} \in \mathrm{Syl}_p(G)\ :\ Q \subseteq \tilde{P}$.

e. *Ist* $Q \in \mathrm{Syl}_p(G/N)$, *dann* $\exists \tilde{P} \in \mathrm{Syl}_p(G)\ :\ Q = \tilde{P}N/N$.

Beweis: Vgl. [Kur77] 3.12 und 3.10 sowie [Hup67] I.7.7 oder [Hum96] 11.14. □

12.8 Satz (Frattiniargument)

Es sei G *eine endliche Gruppe,* p *eine Primzahl,* $N \trianglelefteq G$, $P \in \mathrm{Syl}_p(N)$.
Dann gilt $G = N_G(P)N$.

Beweis: Vgl. [Hup67] I.7.8 oder [Kur77] 3.14. □

12.9 Satz

Es sei G *eine endliche Gruppe,* p *eine Primzahl,* $P \in \mathrm{Syl}_p(G)$ *und* $U \leq G$ *mit* $N_G(P) \subseteq U$. *Dann gilt:* $U = N_G(U)$.

Beweis: Vgl. [Kur77] 3.15 oder [Hup67] I.7.6. □

12.10 Folgerung

$\mathbb{A}_4$ *enthält keine Untergruppe der Ordnung 6 (vgl. 5.3).*

Beweis: Angenommen, $\mathbb{A}_4$ besitzt eine Untergruppe U mit $|U| = 6$. Da $|\mathbb{A}_4 : U| = 2$, ist $U \lhd \mathbb{A}_4$. Aus dem Satz von Sylow folgt $|\mathrm{Syl}_3(U)| \equiv 1 (\mathrm{mod}\ 3)$ und ist zudem ein Teiler von $|U| = 6$, also besitzt U nur eine 3-Sylowgruppe P. Für $g \in G$ gilt nun $P^g \subset U^g = U$, also $P^g = P$. Dann ist $P \lhd \mathbb{A}_4$, aber $P \in \mathrm{Syl}_3(\mathbb{A}_4)$ und folglich würde $\mathbb{A}_4$ nur eine 3-Sylowgruppe besitzen. Widerspruch.
(Alternativ kann man folgendermaßen argumentieren:
Es sei $P \in \mathrm{Syl}_3(\mathbb{A}_4)$. Dann gilt $|P| = 3$. Ferner gilt $N_{\mathbb{A}_4}(P) \neq \mathbb{A}_4$, da $\mathbb{A}_4$ mehr als eine 3-Sylowgruppe besitzt. Wegen $P \subseteq N_{\mathbb{A}_4}(P)$ gilt also $|N_{\mathbb{A}_4}(P)| = 3$ oder $|N_{\mathbb{A}_4}(P)| = 6$.
Nach Satz 12.9 gilt nun, daß $N_{\mathbb{A}_4}(P)$ kein Normalteiler von $\mathbb{A}_4$ ist, also wegen Satz 2.5 auch nicht Ordnung 6 haben kann. Also gilt: $N_{\mathbb{A}_4}(P) = P$.
Angenommen nun, es gäbe eine Untergruppe $U \leq \mathbb{A}_4$ mit $|U| = 6$. Dann enthält U nach dem Satz von Sylow eine Untergruppe P der Ordnung 3, die dann eine 3-Sylowgruppe von $\mathbb{A}_4$ ist. Wieder folgt mit Satz 12.9, daß $U = N_{\mathbb{A}_4}(U)$ kein Normalteiler von $\mathbb{A}_4$ ist, im Widerspruch zu $|\mathbb{A}_4 : U| = 2$.) □

12.11 Satz
Es sei G *eine endliche Gruppe und* $|G| = p_1^{\nu_1} \cdots p_r^{\nu_r}$ *sei die Primfaktorzerlegung von* $|G|$. *Ferner sei* $P_i \in \mathrm{Syl}_{p_i}(G)$, $i = 1, \ldots, r$.
Dann gilt:

a. $G = \langle P_1 \cup \ldots \cup P_r \rangle$.

b. *Falls zudem* $P_i \trianglelefteq G$ *für alle* $i = 1, \ldots, r$ *gilt, so ist* $G = P_1 \times \cdots \times P_r$.
(Vgl. hierzu auch den Hauptsatz über abelsche Gruppen 11.3.)

Beweis: Vgl. [Kur77] 3.13 (verwende Satz 8.10). □

AUFGABEN

12.12 Aufgabe
Finde alle Sylowgruppen von $\mathbb{Z}_{36} \times \mathbb{Z}_{21} \times \mathbb{Z}_{45}$.

12.13 Aufgabe
Man bestimme $\mathrm{Syl}_2(\mathbb{D}_{12})$.

12.14 Aufgabe
Man bestimme alle Sylowgruppen von $G = \langle x, y \mid x^5 = y^4 = e, x^y = x^2 \rangle$.

13 Automorphismen zyklischer Gruppen

13.1 Allgemeine Hinweise

a. Nicht nur die zyklischen Gruppen selbst sind sehr einfach, dies trifft auch für ihre Automorphismen zu, die ja durch das Bild des einen Erzeugenden bestimmt sind. Interessiert man sich nun für die Automorphismengruppe einer zyklischen Gruppe, so kann man sich auf den Fall zurückziehen, daß die Ordnung der Gruppe eine Primzahlpotenz ist. Das ist die Aussage des Satzes 13.4. In Satz 13.5 zeigen wir dann, daß auch letztere abelsche Gruppen mit recht einfacher Struktur sind. In der Tat sind sie sogar zyklisch, wenn die Primzahl nicht eben 2 ist, was wir aber nur als Bemerkung in 13.6 anführen wollen. Stattdessen widmen wir das Ende des Kapitels der Auflistung einiger Beispiele, die im Verlaufe des Skriptes noch benötigt werden, sowie der Untersuchung von Automorphismengruppen einiger nicht zyklischer Gruppen.

b. Eine ausführliche Darstellung zur Struktur der zyklischen Gruppen und ihrer Automorphismen findet sich in [Doe74] Kapitel VII. § 4 sowie in [Kur77] Kapitel II. § 1 und § 3. Zu den Automorphismen vergleiche man auch [Hup67] pp. 83-86.

c. Alle Sätze des Kapitels sind im Vortrag inklusive ihrer Beweise darzustellen. Selbiges gilt für das Beispiel. Die Bemerkungen können entfallen.

13.2 Bemerkung

In Satz 3.12 wurde bereits gezeigt: $\mathrm{Aut}(\mathbb{Z}) \cong \mathbb{Z}_2$.

13.3 Satz

Sei $G = \langle g \rangle$ *eine zyklische Gruppe von Ordnung* $n < \infty$, $\alpha_k : G \to G : g^i \mapsto g^{ki}$.
Dann gilt: $\mathrm{Aut}(G) = \{\alpha_k \mid k \in \{1, \dots, n-1\}$ *mit* $(k, n) = 1\}$.
Insbesondere ist $\mathrm{Aut}(G)$ *abelsch.*

Beweis: Vgl. [Kur77] 2.16-2.17 oder [Doe74] VII.4.12-4.13. □

13.4 Satz

Die natürliche Zahl $n \in \mathbb{N}$ *habe die Primfaktorzerlegung* $n = p_1^{\nu_1} \cdots p_r^{\nu_r}$.
Dann gilt: $\mathrm{Aut}(\mathbb{Z}_n) \cong \mathrm{Aut}(\mathbb{Z}_{p_1^{\nu_1}}) \times \cdots \times \mathrm{Aut}(\mathbb{Z}_{p_r^{\nu_r}})$.

Beweis: Vgl. [Kur77] p. 33 oder [Hup67] I.4.6. □

13.5 Satz

Es sei p *eine Primzahl,* $\nu \in \mathbb{N}$.
Dann gilt: $\mathrm{Aut}(\mathbb{Z}_{p^\nu}) \cong \mathbb{Z}_{p-1} \times H$, *wobei* H *eine abelsche Gruppe mit* $|H| = p^{\nu-1}$ *ist.*

Beweis: Vgl. [Kur77] 2.18 oder [Hup67] I.4.6 und I.13.19. □

13.6 Korollar

Ist p *eine Primzahl, so gilt:* $\mathrm{Aut}(\mathbb{Z}_p) \cong \mathbb{Z}_{p-1}$.

13.7 Bemerkung

a. Um einen Erzeuger für die zyklische Gruppe $\mathrm{Aut}(\mathbb{Z}_p)$ zu finden, bleibt i. a. nur die *trial and error* Methode.

b. Ist p eine ungerade Primzahl, so gilt: $\mathrm{Aut}(\mathbb{Z}_{p^\nu}) \cong \mathbb{Z}_{(p-1)p^{\nu-1}}$.

c. Ist $\nu \geq 3$, so hat $\mathrm{Aut}(\mathbb{Z}_{2^\nu})$ den Typ $(2, 2^{\nu-2})$.

Beweis: Vgl. [Hup67] I.13.19 sowie [Hum96] 22.3. In [Hum96] 22.2 ist das Beispiel $\mathrm{Aut}(\mathbb{Z}_{17})$ näher betrachtet. □

13.8 Beispiel

a. $\mathrm{Aut}(\mathbb{Z}_4) \cong \mathbb{Z}_2$

b. $\mathrm{Aut}(\mathbb{Z}_6) \cong \mathbb{Z}_2$

c. $\mathrm{Aut}(\mathbb{Z}_9) \cong \mathbb{Z}_6$

d. $\mathrm{Aut}(\mathbb{Z}_{15}) \cong \mathbb{Z}_2 \times \mathbb{Z}_4$

Beweis: Dies folgt unmittelbar aus den Sätzen 13.4 und 13.5. □

13.9 Definition
Eine endliche abelsche Gruppe G vom Typ $(p, \ldots, p)$ mit p Primzahl nennt man **elementarabelsch**.

13.10 Satz
Eine elementarabelsche p-Gruppe der Ordnung p^n *ist kanonisch isomorph zur additiven Gruppe des Vektorraums* $(\mathrm{GF}(p))^n$ *der Dimension* n *über* $\mathrm{GF}(p)$*, und ihre Automorphismengruppe* $\mathrm{Aut}(G)$ *ist kanonisch isomorph zu dessen Automorphismengruppe* $\mathrm{Gl}_n(p)$.

Beweis: Vgl. [Hum96] 22.4, [Gor80] I.3.2 und [DH92] pp. 14-15. □

13.11 Beispiel
$\mathrm{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2) \cong \mathrm{Gl}_2(2)$.

13.12 Satz
$\mathrm{Aut}(\mathbb{S}_3) \cong \mathbb{S}_3$.

Beweis: Da ein Automorphismus die Ordnung eines Elementes erhält, permutiert er die Menge der Transpositionen von $\mathbb{S}_3$. Da ferner die $\mathbb{S}_3$ von ihren Transpositionen erzeugt wird, ist ein Automorphismus durch die Bilder der drei Transpositionen festgelegt. Es gibt also höchstens sechs verschiedene Automorphismen. Nun gilt aber nach Satz 7.9 $Z(\mathbb{S}_3) = \mathbb{1}$, und somit $\mathbb{S}_3 \cong \mathbb{S}_3/Z(\mathbb{S}_3) \cong \mathrm{Inn}(\mathbb{S}_3) \leq \mathrm{Aut}(\mathbb{S}_3)$. Also ist gilt aus Ordnungsgründen $\mathrm{Aut}(\mathbb{S}_3) = \mathrm{Inn}(\mathbb{S}_3) \cong \mathbb{S}_3$. (Vgl. auch [Hum96] 22.6.) □

AUFGABEN

13.13 Aufgabe
Man zeige $\mathrm{Aut}(\mathbb{Z}_4 \times \mathbb{Z}_2) \cong \mathbb{D}_8$, $\mathrm{Aut}(\mathbb{D}_8) \cong \mathbb{D}_8$ und $\mathrm{Aut}(\mathbb{Q}_8) \cong \mathbb{S}_4$.
Hinweis: Man darf die Präsentation $\langle a, b \mid a^4 = b^3 = (ab)^2 = e \rangle$ von $\mathbb{S}_4$ verwenden.

14 Klassifikation der Gruppen von Ordnung pq und $4p$

14.1 Allgemeine Hinweise

a. Das Ziel dieses Kapitels ist es, einige Klassifikationssätze zu zeigen, bei denen der *Input* nur aus der Gruppenordnung besteht. Für unsere Zwecke reicht es, die Gruppen der Ordnung pq und $4p$ exakt zu bestimmen, und ferner für Gruppen der Ordnung p^2q zu wissen, daß sie semidirekte Produkte zweier Sylowgruppen sind. Die Aussagen über Normalisatoren von Untergruppen in p-Gruppen sowie über die maximalen Untergruppen von p-Gruppen gehören ihrer Natur nach in den Rahmen der Betrachtung allgemeiner nilpotenter Gruppen und interessieren uns nur als Hilfsmittel auf dem Weg zur Klassifikation. Gleiches gilt für das erste Lemma des Kapitels, das der Zahlentheorie entnommen ist.

b. Eine Vielzahl von einzelnen Klassifikationssätzen findet sich in [Hup67] an den verschiedensten Stellen oder kann Originalquellen wie [Höl93] entnommen werden. Alle hier angeführten Sätze sind aber mit (u. U. verbesserungswürdigen) Beweisvorschlägen versehen.

c. Alle im folgenden Kapitel enthaltenen Sätze sollen im Vortrag zu diesem Kapitel dargeboten werden. Aus Zeitgründen kann ggf. der Beweis von Lemma 14.2 entfallen.

14.2 Lemma

Seien $p < q$ *Primzahlen mit* $q \equiv 1 (\mathrm{mod}\ p)$ *und sei* $a \in \{1, \dots, q-1\}$ *so, daß für* $\bar{a} \in \mathbb{Z}_q^*$ *gilt:* $o(\bar{a}) = p$. *Für* $b \in \{1, \dots, q-1\}$ *gilt genau dann* $b^p \equiv 1 (\mathrm{mod}\ q)$, *wenn* $b \equiv a^\mu (\mathrm{mod}\ q)$ *für ein* $\mu \in \{0, \dots, p-1\}$.

Beweis: Zunächst wollen wir uns klar machen, daß es auch ein a mit der gewünschten Eigenschaft gibt.
Beachte dazu, daß $q \equiv 1 (\mathrm{mod}\ p)$ gilt, daß also $p \mid (q-1)$. Nach Satz 10.12 ist die multiplikative Gruppe $\mathbb{Z}_q^*$ zyklisch der Ordnung $q-1$ und besitzt somit wegen $p \mid (q-1)$ nach Satz 10.4 ein Element $\bar{a} \in \mathbb{Z}_q^*$ der Ordnung p.
Die Bedingung $o(\bar{a}) = p$ bedeutet, daß $p > 1$ minimal ist bezüglich der Bedingung, daß $a^p \equiv 1 (\mathrm{mod}\ q)$.
Zeigen wir nun also obige Äquivalenz:

"$\Leftarrow$": Sei $b \equiv a^\mu (\mathrm{mod}\ q)$, dann gilt $b^p \equiv (a^\mu)^p = (a^p)^\mu \equiv 1^\mu = 1 (\mathrm{mod}\ q)$.

"$\Rightarrow$": Wir gehen nun von $\mathbb{Z}$ nach $\mathbb{Z}/q\mathbb{Z}$ über. Für ein $z \in \mathbb{Z}$ bezeichne $\bar{z}$ die Restklasse von z in $\mathbb{Z}/q\mathbb{Z}$.
Das Polynom $x^p - 1$ hat in dem Körper $\mathbb{Z}/q\mathbb{Z}$ höchstens p verschiedene Nullstellen. Ein $\bar{b}$ mit $b \in \{1, \dots, q-1\}$ und $b^p \equiv 1 (\mathrm{mod}\ q)$ entspricht aber genau einer solchen Nullstelle. Also reicht es zu zeigen, daß die $\overline{a^\mu}$ mit $\mu \in \{0, \dots, p-1\}$ paarweise verschieden sind.
Sei dazu $a^\mu \equiv a^\nu (\mathrm{mod}\ q)$ mit $0 \le \nu \le \mu \le p-1$, dann gilt $a^{(\mu-\nu)} \equiv 1 (\mathrm{mod}\ q)$ und $0 \le \mu - \nu < p - 1$, also nach Voraussetzung $\mu - \nu = 0$.

□

14.3 Satz

Sei G *eine Gruppe der Ordnung* $|G| = p \cdot q$ *mit* $p < q$ *zwei Primzahlen.*

a. $|\mathrm{Syl}_q(G)| = 1$, *d. h.* die *q-Sylowgruppe von* G *ist ein Normalteiler.*

b. *Gilt* $q \not\equiv 1 (\mathrm{mod}\ p)$.
Dann ist $G \cong \mathbb{Z}_{pq}$ *zyklisch.*

c. *Gilt* $q \equiv 1 (\mathrm{mod}\ p)$.
Dann ist entweder $G \cong \mathbb{Z}_{pq}$ *oder* $G \cong \langle x, y \mid x^q = y^p = e, x^y = x^b \rangle$, *wobei* $b \in \{2, \ldots, q-1\}$ *mit* $b^p \equiv 1 (\mathrm{mod}\ q)$ *beliebig.*
In letzterem Fall gilt außerdem: $G \cong \mathbb{Z}_q \ltimes_{\varphi_b} \mathbb{Z}_p$ *mit* $\varphi_b : \mathbb{Z}_p \to \mathrm{Aut}(\mathbb{Z}_q) : \bar{l} \mapsto (\mathbb{Z}_q \ni \overline{m} \mapsto \overline{m} \cdot \overline{b^l} \in \mathbb{Z}_q)$.

d. *Ist* G *nicht abelsch der Ordnung* $2q$, *so gilt* $G \cong \mathbb{D}_{2q}$.

Beweis: Es seien $Q \in \mathrm{Syl}_q(G)$ und $P \in \mathrm{Syl}_p(G)$.

a. Dann gilt $r := |\mathrm{Syl}_q(G)| = |G : N_G(Q)|$ teilt $p = |G : Q|$, also $r \in \{1, p\}$.
Zugleich gilt aber nach 12.4: $r = |\mathrm{Syl}_q(G)| \equiv 1 (\mathrm{mod}\ q)$.
Da $p < q$, also $p \not\equiv 1 (\mathrm{mod}\ q)$, bleibt nur $r = 1$.

b. Nach a. gilt, daß Q Normalteiler von G ist, und wie in Teil a. sieht man auch, daß $P \lhd G$. Also ist $G \cong Q \times P \cong \mathbb{Z}_{pq}$.

c. Für $b \in \{0, \ldots, q-1\}$ mit $b^p \equiv 1 (\mathrm{mod}\ q)$ setzen wir $H_b := \langle x, y \mid x^q = y^p = e, x^y = x^b \rangle$.

Zeige: $\varphi_b(\bar{l})$ ist wohldefiniert, liegt in $\mathrm{Aut}(\mathbb{Z}_q)$ und φ_b ist ein Homomorphismus.
Es sei $r \in \mathbb{Z}$ beliebig, dann gilt $b^{l+rp} = b^l \cdot (b^p)^r \equiv b^l \cdot 1^r = b^l (\mathrm{mod}\ q)$, wegen $b^p \equiv 1 (\mathrm{mod}\ q)$, also ist φ_b wohldefiniert.
Da $q \nmid b$ und q Primzahl, ist $\overline{b^l} \neq \bar{0}$, also eine Einheit im Ring $\mathbb{Z}_q$. Dann ist aber die Multiplikation mit $\overline{b^l}$ ein Automorphismus der additiven Gruppe $(\mathbb{Z}_q, +)$.
Wegen $b^{l+k} = b^l \cdot b^k$, ist φ_b ein Homomorphismus.
(Beachte, daß damit die Multiplikation auf $\mathbb{Z}_q \ltimes_{\varphi_b} \mathbb{Z}_p$ erklärt ist durch $(\overline{m}, \bar{k}) \cdot (\bar{n}, \bar{l}) = (\overline{m} + \varphi_b(\bar{k})(\bar{n}), \bar{k} + \bar{l}) = (\overline{m + nb^k}, \overline{k+l})$, wobei $\overline{m}, \bar{n} \in \mathbb{Z}_q, \bar{k}, \bar{l} \in \mathbb{Z}_p$.)

Zeige: $H_b \cong \mathbb{Z}_q \ltimes_{\varphi_b} \mathbb{Z}_p$, insbesondere $|H_b| = pq$.
Aus den Relationen folgt sofort $H_b = \left\{ x^k y^l \mid 0 \leq l < p, 0 \leq k < q \right\}$, also $|H_b| \leq pq$.
Mit 9.8 reicht es zu zeigen, daß $\mathbb{Z}_q \ltimes_{\varphi_b} \mathbb{Z}_p = \langle (\bar{1}, \bar{0}), (\bar{0}, \bar{1}) \rangle$, wobei die beiden Erzeuger den Relationen von H_b genügen. Daß $(\bar{1}, \bar{0})$ und $(\bar{0}, \bar{1})$ die Gruppe erzeugen, folgt unmittelbar aus $(\overline{m}, \bar{l}) = (\overline{m}, \bar{0}) \cdot (\bar{0}, \bar{l}) = (\bar{1}, \bar{0})^m \cdot (\bar{0}, \bar{1})^l$, ebenso die ersten beiden Relationen. Außerdem gilt $(\bar{1}, \bar{0})^{(\bar{0}, \bar{1})} = (\bar{0}, \bar{1})(\bar{1}, \bar{0})(\bar{0}, \overline{-1}) = (\bar{0}, \bar{1})(\bar{1}, \overline{-1}) = (\bar{b}, \bar{0}) = (\bar{1}, \bar{0})^b$.

Zeige: Für $b \neq 1$ gilt $H_b \cong H_a = \langle \tilde{x}, \tilde{y} \mid \tilde{x}^q = \tilde{y}^p = e, \tilde{x}^{\tilde{y}} = \tilde{x}^a \rangle$, wobei für $a \in \{1, \ldots, q-1\}$ gilt, daß $o(\bar{a}) = p$ in $\mathbb{Z}_q^*$ (vgl. Lemma 14.2).
Nach Lemma 14.2 gibt es ein $\nu \in \{1, \ldots, p-1\}$ mit $b \equiv a^\nu (\mathrm{mod}\ q)$.
Setzen wir nun $\hat{y} := \tilde{y}^\nu$, so gilt $H_a = \langle \tilde{x}, \hat{y} \rangle$ (da $o(\tilde{y}^\nu) = o(\tilde{y}) = p$) und

die neuen Erzeuger erfüllen wieder die Relationen von H_b ($\tilde{x}^{\tilde{y}} = \tilde{x}^{(\tilde{y}^{\nu})} = \tilde{x}^{(a^{\nu})} = \tilde{x}^{b}$). Also folgt mit 9.8 wegen $|H_b| = |H_a|$, daß $H_b \cong H_a$.

Zeige: $G \cong H_b$ für b geeignet.

Es sei $Q = \langle\overline{x}\rangle$ und $P = \langle\overline{y}\rangle$.

Dann gilt nach a., $\overline{x}^{\overline{y}} = \overline{x}^{b}$ für $b \in \{0, \dots, q-1\}$ geeignet. Ferner gilt: $\overline{x} = \overline{x}^{e} = \overline{x}^{(\overline{y}^{p})} = \overline{x}^{(b^{p})}$. Also gilt $b^p \equiv 1 (\mathrm{mod}\ q)$. Mit 9.8 erhalten wir $G \cong H_b$.

Beachten wir nun, daß $H_1 \cong \mathbb{Z}_{pq}$, also nicht isomorph zu H_b für $b \neq 1$, so erhalten wir genau die beiden oben angegebenen Isomorphietypen von Gruppen. (Für einen alternativen Beweis mittels Erweiterungen von Gruppen siehe [Hum96] 21.9.)

d. Es gilt $(q-1)^2 \equiv 1 (\mathrm{mod}\ q)$, also gilt nach c.: $G \cong \langle x, y \mid x^q = y^2 = e, x^y = x^{q-1}\rangle = \mathbb{D}_{2q}$.
(Alternativ dazu ein Beweis, der ohne c. auskommt:
Seien $N \in \mathrm{Syl}_q(G)$ und $U = \langle u\rangle \in \mathrm{Syl}_2(G)$.
Nach Satz 2.5 gilt: $N \lhd G$. Lagrange $\Rightarrow N \cap U = \mathbb{1}$
Produktformel $\Rightarrow NU = G$
Also ist G semidirektes Produkt von N und U, d. h. U operiert auf N, d. h. es gibt einen Gruppenhomomorphismus $\varphi : U \cong \mathbb{Z}_2 \to \mathrm{Aut}(N) \cong \mathbb{Z}_{q-1}$. Da G nicht abelsch ist, ist G nicht das direkte Produkt der beiden abelschen Gruppen N und U, d. h. φ ist nicht der triviale Homomorphismus, also $|\varphi(U)| = 2$.
Da eine zyklische Gruppe zu jedem Gruppenteiler genau eine Untergruppe dieser Ordnung besitzt, ist $\varphi(U)$ und damit (aus Ordnungsgründen) auch φ selbst festgelegt. Es gilt $\varphi(u)$ invertiert die Elemente von N
Also ist: $G = NU \cong \mathbb{D}_{2q}$. - Vgl. auch [Hum96] § 12 (1).)

□

14.4 Lemma

Sei G eine Gruppe der Ordnung pq^2 mit p, q Primzahlen.
Dann ist (mindestens) eine der Sylowgruppen von G Normalteiler.

Beweis: **1. Fall:** $q \not\equiv 1 (\mathrm{mod}\ p)$**:** Seien $P \in \mathrm{Syl}_p(G)$ und $Q \in \mathrm{Syl}_q(G)$.
Es gilt: $r := |\mathrm{Syl}_p(G)|$ teilt $|G| = pq^2$, also $r \in \{1, p, q, pq, q^2, pq^2\}$.
Außerdem gilt: $r \equiv 1 (\mathrm{mod}\ p)$, also: $r \in \{1, q, q^2\}$.
Aufgrund der Zusatzvoraussetzung scheidet der Fall $r = q$ aus.
Falls $r = 1$, dann ist P Normalteiler von G, sonst besitzt G $q^2(p-1)$ Elemente der Ordnung p. Dann bleiben aber nur q^2 Elemente von anderer Ordnung übrig, also besitzt G nur eine q-Sylowgruppe und Q ist ein Normalteiler.

2. Fall: $q \equiv 1 (\mathrm{mod}\ p)$**:** Dann ist $p < q$, und wir sind fertig mit Satz 6.11.
(Alternativ kann man den Beweis für $p < q$ auch direkt mit Satz 6.10 führen:
Da $|G : Q| = p$, gibt es nach Satz 6.10 ein $N \trianglelefteq G$ mit p teilt $|G : N|$ und

$|G : N|$ teilt $p!$. Da zugleich $|G : N|$ die Gruppenordnung pq^2 teilt (also $|G : N| \in \{1, p, q, pq, q^2, pq^2\}$) und q und sicher kein Teiler von $p!$ ist, bleibt nur $|G : N| = p$ und $N \in \mathrm{Syl}_q(G)$.)

(Eine Beweisalternative mittels des Satzes von Sylow:

Es ist nun $p < q$, und analog zu obiger Argumentation sieht man, daß $s := |\mathrm{Syl}_q(G)| \in \{1, p\}$ und o. E. $s = p$.

Angenommen, G hat zwei verschiedene q-Sylowgruppen $Q_1, Q_2 \in \mathrm{Syl}_q(G)$ mit $D := Q_1 \cap Q_2 \neq \mathbb{1}$, so gilt $|D| = q$. Da D echte Untergruppe der q-Gruppe Q_1 ist, folgt aus Lemma 7.11: $D < N_{Q_1}(D)$, also $N_{Q_1}(D) = Q_1$, und analog $N_{Q_2}(D) = Q_2$, also $D \lhd \langle Q_1, Q_2 \rangle = G$. Nun ist $|G/D| = pq$ und damit besitzt G/D nach Satz 14.3 nur eine q-Sylowgruppe Q/D mit $Q \in \mathrm{Syl}_q(G)$, im Widerspruch zu $Q_1/D, Q_2/D \in \mathrm{Syl}_q(G/D)$.

Also haben je zwei q-Sylowgruppen von G trivialen Schnitt, und G enthält $p(q^2 - 1) + 1 = |G| - (p - 1)$ Elemente von q-Potenzordnung und damit nur eine p-Sylowgruppe, die deshalb ein Normalteiler sein muß.)

(Vgl. auch [Hum96] 12.4.) □

14.5 Satz

Sei G *eine nicht abelsche Gruppe der Ordnung* $|G| = 4p$, $p \geq 5$ *Primzahl.*
Dann gilt:

a. *Falls* $4 \nmid (p - 1)$, *dann gilt entweder* $G \cong \mathbb{D}_{4p}$ *oder* $G \cong \mathbb{H}_p$.

b. *Falls* $4 \mid (p - 1)$, *dann gibt es genau einen weiteren Isomorphietyp, nämlich* $G \cong \mathbb{Z}_p \ltimes_\varphi \mathbb{Z}_4$, *wobei* φ *treu ist.*

Beweis: Es gilt $r := |\mathrm{Syl}_p(G)| \equiv 1 (\mathrm{mod}\ p)$.

Angenommen, $r > 1$, dann wäre $r \geq (p + 1)$ und G hätte $r(p - 1) \geq p^2 - 1 \geq 5p - 1 > 4p$ Elemente der Ordnung p, Widerspruch.

Also besitzt G nur eine p-Sylowgruppe $N \cong \mathbb{Z}_p$, die dann Normalteiler ist, und somit ist G semidirektes Produkt von N mit einer 2-Sylowgruppe V, $G \cong N \ltimes_\varphi V$ mit $\varphi : V \to \mathrm{Aut}(N)$.

1. **Fall:** $\mathrm{Ker}(\varphi) \neq \mathbb{1}$**:** Da φ nicht der triviale Homomorphismus ist, gilt dann $\mathrm{Ker}(\varphi) \cong \mathbb{Z}_2$ und $\mathbb{Z}_{2p} \cong N \times \mathrm{Ker}(\varphi) \lhd G$, d. h. G enthält ein Element der Ordnung $2p$. Da ferner $\mathrm{Aut}(\mathbb{Z}_p) \cong \mathbb{Z}_{p-1}$ nur ein Element der Ordnung 2 besitzt, die Inversion, und $|\mathrm{Im}(\varphi)| = 2$, bleiben die folgenden beiden Fälle:
   - **Fall a.** $V \cong \mathbb{Z}_2 \times \mathbb{Z}_2$**:** Dann besitzt G also ein Element der Ordnung 2, welches das Element der Ordnung $2p$ invertiert, also ist $G \cong \mathbb{D}_{4p}$. (Verwende 9.8 und 9.10.)
   - **Fall b.** $V \cong \mathbb{Z}_4$**:** Dann besitzt G also ein Element der Ordnung 4, welches das Element der Ordnung $2p$ invertiert, also ist $G \cong \mathbb{H}_p$. (Verwende 9.8 und 9.11.)
2. **Fall:** $\mathrm{Ker}(\varphi) = \mathbb{1}$**:** Da dann $\mathrm{Aut}(Z_p) \cong \mathbb{Z}_{p-1}$ je genau eine Untergruppe der Ordnungen 2 und 4 besitzt, ist $V \cong \mathbb{Z}_4$ und läßt sich auf genau zwei Weisen in $\mathrm{Aut}(N)$ einbetten. Die entstehenden Gruppen sind zueinander isomorph.

(Beachte dazu, daß die Elemente, die das Bild von V in Aut(N) erzeugen, zueinander invers sind. Wir können also die beiden möglichen semidirekten Produkte schreiben als $G_1 := \{(n^l, v^k) \mid 0 \le k \le 3, 0 \le l \le p-1\}$ sowie $G_2 := \{(n^l, \tilde{v}^k) \mid 0 \le k \le 3, 0 \le l \le p-1\}$, wobei $n \in N$ und $v \in V$ fest gewählte Erzeuger sind und $\tilde{v} = v^{-1}$. Definieren wir eine Abbildung $\alpha : G_1 \to G_2$ durch $(n^l, v^k) \mapsto (n^l, (\tilde{v})^{-k})$, so gilt aufgrund der Multiplikation in semidirekten Produkten für $g = (n^i, v^k), h = (n^j, v^l) \in G_1$: $\alpha(gh) = \alpha(n^i \cdot v^{-k} n^j, v^{k+l}) = (n^i \cdot v^{-k} n^j, \tilde{v}^{-(k+l)}) = (n^i \cdot \tilde{v}^k n^j, \tilde{v}^{-k} \tilde{v}^{-l}) = (n^i, \tilde{v}^{-k})(n^j, \tilde{v}^{-l}) = \alpha(g)\alpha(h)$. Also ist α ein Homomorphismus und offenbar auch bijektiv.)

Nun braucht man nur noch zu beachten, daß der 2. Fall nicht auftreten kann, wenn $4 \nmid (p-1)$ gilt, sowie daß die Gruppe im 2. Fall kein Element der Ordnung $2p$ besitzt, also nicht isomorph zu denen im 1. Fall sein kann. □

AUFGABEN

14.6 Aufgabe

Bestimme die Untergruppen und Normalteiler von $\mathbb{Z}_5 \ltimes \mathbb{Z}_4$ aus Satz 14.5. Ferner bestimme man das Zentrum der Gruppe. (Vgl. auch Aufgabe 12.14.)

15 KLASSIFIKATION DER GRUPPEN BIS ORDNUNG 23

15.1 Allgemeine Hinweise

Der Klassifikationsbeweis für die Gruppen bis zur Ordnung 23 sollte vollständig ausgeführt werden. Ggf. kann bei den Gruppen der Ordnung 16 gekürzt werden. Es empfiehlt sich, den Klassifikationssatz auf Folie zu bannen, so daß er mittels eines Overheadprojektors stets präsent ist. Keinesfalls sollte er an die Tafel geschrieben werden. Die Klassifikation ist ebenfalls durchgeführt in [Hum96].

15.2 Theorem (Klassifikation)

Es sei G *eine Gruppe der Ordnung* $|G| \leq 35$, $(|G| \neq 32)$.
Dann ist G *isomorph zu genau einer der Gruppen in folgender Tabelle:*

$\lvert G\rvert$	**Isomorphie-typ von** G	**Präsentationen**	**isomorphe Gruppen**	**WichtigeEigenschaften**
1	$\mathbb{1}$			
2	$\mathbb{Z}_2$			*zyklisch, einfach*
3	$\mathbb{Z}_3$			*zyklisch, einfach*
4	$\mathbb{Z}_2 \times \mathbb{Z}_2$ $\mathbb{Z}_4$			*Kleinsche Vierergruppe: abelsch* *zyklisch*
5	$\mathbb{Z}_5$			*zyklisch, einfach*
6	$\mathbb{Z}_2 \times \mathbb{Z}_3$ $\mathbb{S}_3$	 $\langle x, y \mid x^3 = y^2 = e, x^y = x^{-1} \rangle$	$\mathbb{Z}_6$ $\mathbb{D}_6 \cong \mathbb{Z}_3 \ltimes \mathbb{Z}_2 \cong \mathrm{PSL}_2(2) \cong \mathrm{Gl}_2(2) \cong \mathrm{Sl}_2(2)$	*zyklisch* *Diedergruppe / symmetrische Gruppe: nicht abelsch, auflösbar, (nicht nilpotent)*
7	$\mathbb{Z}_7$			*zyklisch, einfach*
8	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ $\mathbb{Z}_2 \times \mathbb{Z}_4$ $\mathbb{Z}_8$ $\mathbb{D}_8$ $\mathbb{Q}_8$	 $\langle x, y \mid x^4 = y^2 = e, x^y = x^{-1} \rangle$ $\langle x, y \mid x^4 = e, y^2 = x^2, x^y = x^{-1} \rangle$	 $\mathbb{Z}_4 \ltimes \mathbb{Z}_2$ $\mathbb{H}_2$	*elementarabelsch* *abelsch,* $\mathrm{Aut}(\mathbb{Z}_4 \times \mathbb{Z}_2) \cong \mathbb{D}_8$ *zyklisch* *Diedergruppe: nicht abelsch, auflösbar, (nilpotent),* $\mathrm{Aut}(\mathbb{D}_8) \cong \mathbb{D}_8$, $\mathrm{Inn}(\mathbb{D}_8) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ *Quaternionengruppe: nicht abelsch, auflösbar, (nilpotent); hamiltonsch (d. h. alle (6) Untergruppen sind Normalteiler),* $\mathbb{Q}_8$ *ist kein semidirektes Produkt,* $\mathrm{Aut}(\mathbb{Q}_8) \cong \mathbb{S}_4$
9	$\mathbb{Z}_3 \times \mathbb{Z}_3$ $\mathbb{Z}_9$			*elementarabelsch* *zyklisch*
10	$\mathbb{Z}_2 \times \mathbb{Z}_5$ $\mathbb{D}_{10}$	 $\langle x, y \mid x^5 = y^2 = e, x^y = x^{-1} \rangle$	$\mathbb{Z}_{10}$ $\mathbb{Z}_5 \ltimes \mathbb{Z}_2$	*zyklisch* *Diedergruppe: nicht abelsch, auflösbar, (nicht nilpotent)*

$\lvert G \rvert$	**Isomorphie-typ von** G	**Präsentationen**	**isomorphe Gruppen**	**WichtigeEigenschaften**
11	$\mathbb{Z}_{11}$			*zyklisch, einfach*
12	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$		$\mathbb{Z}_2 \times \mathbb{Z}_6$	*abelsch*
	$\mathbb{Z}_4 \times \mathbb{Z}_3$		$\mathbb{Z}_{12}$	*zyklisch*
	$\mathbb{A}_4$	$\langle x, y \mid x^3 = y^3 = (xy)^2 = e \rangle = \langle x, y, z \mid x^2 = y^2 = z^3 = e, x^y = x, x^z = y, y^z = xy \rangle$	$(\mathbb{Z}_2 \times \mathbb{Z}_2) \ltimes \mathbb{Z}_3 \cong \mathrm{PSL}_2(3)$	*Tetraedergruppe/ alternierende Gruppe: nicht abelsch, auflösbar, (nicht nilpotent); besitzt keine Untergruppe der Ordnung 6 und kein Element der Ordnung 4,* $\mathrm{Aut}(A_4) \cong \mathbb{S}_4$
	$\mathbb{D}_{12}$	$\langle x, y \mid x^6 = y^2 = e, x^y = x^{-1} \rangle$	$\mathbb{Z}_6 \ltimes \mathbb{Z}_2 \cong \mathbb{D}_6 \times \mathbb{Z}_2$	*Diedergruppe: nicht abelsch, auflösbar, (nicht nilpotent); besitzt kein Element der Ordnung 4*
	$\mathbb{H}_3$	$\langle x, y \mid x^6 = e, y^2 = x^3, x^y = x^{-1} \rangle$	$\mathbb{Z}_3 \ltimes \mathbb{Z}_4$	*Dizyklische Gruppe: nicht abelsch, auflösbar, (nicht nilpotent); besitzt 3 zyklische Untergruppen der Ordnung 4*
13	$\mathbb{Z}_{13}$			*zyklisch, einfach*
14	$\mathbb{Z}_2 \times \mathbb{Z}_7$		$\mathbb{Z}_{14}$	*zyklisch*
	$\mathbb{D}_{14}$	$\langle x, y \mid x^7 = y^2 = e, x^y = x^{-1} \rangle$	$\mathbb{Z}_7 \ltimes \mathbb{Z}_2$	*Diedergruppe: nicht abelsch, auflösbar, (nicht nilpotent)*
15	$\mathbb{Z}_3 \times \mathbb{Z}_5$		$\mathbb{Z}_{15}$	*zyklisch*
16	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$			*elementarabelsch*
	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4$			*abelsch*
	$\mathbb{Z}_2 \times \mathbb{Z}_8$			*abelsch*
	$\mathbb{Z}_4 \times \mathbb{Z}_4$			*abelsch*
	$\mathbb{Z}_{16}$			*zyklisch*
	$\mathbb{D}_{16}$	$\langle x, y \mid x^8 = y^2 = e, x^y = x^{-1} \rangle$	$\mathbb{Z}_8 \ltimes \mathbb{Z}_2$	*Diedergruppe: nicht abelsch, auflösbar, (nilpotent)*
	$\mathbb{Z}_8 \ltimes \mathbb{Z}_2$	$\langle x, y \mid x^8 = y^2 = e, x^y = x^3 \rangle$		*Quasi-Diedergruppe: nicht abelsch, auflösbar, (nilpotent)*
	$\mathbb{Z}_8 \ltimes \mathbb{Z}_2$	$\langle x, y \mid x^8 = y^2 = e, x^y = x^5 \rangle$		*nicht abelsch, auflösbar, (nilpotent); alle echten Untergruppen sind abelsch,* $\mathrm{Aut}(G) \cong \mathbb{D}_8 \times \mathbb{Z}_2$
	$\mathbb{H}_4$	$\langle x, y \mid x^8 = e, y^2 = x^4, x^y = x^{-1} \rangle$		*verallgemeinerte Quaternionengruppe: nicht abelsch, auflösbar, (nilpotent)*
	$(\mathbb{Z}_4 \times \mathbb{Z}_2) \ltimes \mathbb{Z}_2$	$\langle x, y, z \mid x^4 = y^2 = z^2 = e, x^y = x, y^z = y, x^z = xy \rangle = \langle x, u \mid x^4 = e, u^4 = e, (xu)^2 = e, (x^3u)^2 = e \rangle = \langle x, z \mid x^4 = z^2 = e, [x, z]^2 = e \rangle$		*nicht abelsch, auflösbar, (nilpotent)*

$\lvert G\rvert$	**Isomorphie-typ von** G	**Präsentationen**	**isomorphe Gruppen**	**WichtigeEigenschaften**
	$(\mathbb{Z}_4 \times \mathbb{Z}_2) \ltimes \mathbb{Z}_2$	$\langle x, y, z \mid x^4 = y^2 = z^2 = e, x^y = x, x^z = x^{-1}, y^z = y\rangle$	$\mathbb{D}_8 \times \mathbb{Z}_2$	*nicht abelsch, auflösbar, (nilpotent)*
	$(\mathbb{Z}_4 \times \mathbb{Z}_2) \ltimes \mathbb{Z}_2$	$\langle x, y, z \mid x^4 = y^2 = z^2 = e, x^y = x, x^z = x, y^z = x^2 y\rangle$		*nicht abelsch, auflösbar, (nilpotent)*
	$\mathbb{Z}_4 \ltimes \mathbb{Z}_4$	$\langle x, y \mid x^4 = e, y^4 = e, x^y = x^3\rangle$		*nicht abelsch, auflösbar, (nilpotent), metazyklisch, (alle echten Untergruppen sind abelsch)*
	$\mathbb{H}_2 \times \mathbb{Z}_2$	$\langle x, y, z \mid x^4 = y^2 = e, z^2 = x^2, x^z = x^{-1}, x^y = x, y^z = y\rangle$		*nicht abelsch, auflösbar, (nilpotent); hamiltonsch (d. h. alle Untergruppen sind Normalteiler)*
17	$\mathbb{Z}_{17}$			*zyklisch, einfach*
18	$\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3$		$\mathbb{Z}_3 \times \mathbb{Z}_6$	*abelsch*
	$\mathbb{Z}_2 \times \mathbb{Z}_9$		$\mathbb{Z}_{18}$	*zyklisch*
	$\mathbb{D}_{18}$	$\langle x, y \mid x^9 = y^2 = e, x^y = x^{-1}\rangle$	$\mathbb{Z}_9 \ltimes \mathbb{Z}_2$	*Diedergruppe: nicht abelsch, auflösbar, (nicht nilpotent)*
	$(\mathbb{Z}_3 \times \mathbb{Z}_3) \ltimes \langle A\rangle$	$\langle x, y, z \mid x^3 = y^3 = z^2 = e, x^y = x, x^z = x^{-1}, y^z = y^{-1}\rangle$		*mit* $A = \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$*; nicht abelsch, auflösbar, (nicht nilpotent)*
	$(\mathbb{Z}_3 \times \mathbb{Z}_3) \ltimes \langle A\rangle$	$\langle x, y, z \mid x^3 = y^3 = z^2 = e, x^y = x, x^z = x^{-1}, y^z = y\rangle$	$D_6 \times \mathbb{Z}_3$	*mit* $A = \left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$*; nicht abelsch, auflösbar, (nicht nilpotent)*
19	$\mathbb{Z}_{19}$			*zyklisch, einfach*
20	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5$		$\mathbb{Z}_2 \times \mathbb{Z}_{10}$	*abelsch*
	$\mathbb{Z}_4 \times \mathbb{Z}_5$		$\mathbb{Z}_{20}$	*zyklisch*
	$\mathbb{D}_{20}$	$\langle x, y \mid x^{10} = y^2 = e, x^y = x^{-1}\rangle$	$\mathbb{Z}_{10} \ltimes \mathbb{Z}_2 \cong \mathbb{D}_{10} \ltimes \mathbb{Z}_2$	*nicht abelsch, auflösbar, (nicht nilpotent); besitzt Elemente der Ordnung 10*
	$\mathbb{H}_5$	$\langle x, y \mid x^{10} = e, y^2 = x^5, x^y = x^{-1}\rangle$		*nicht abelsch, auflösbar, (nicht nilpotent)*
	$\mathbb{Z}_5 \ltimes \mathrm{Aut}(Z_5)$	$\langle x, y \mid x^5 = y^4 = e, x^y = x^2\rangle$		*nicht abelsch, auflösbar, (nicht nilpotent); besitzt kein Element der Ordnung 10*
21	$\mathbb{Z}_3 \times \mathbb{Z}_7$		$\mathbb{Z}_{21}$	*zyklisch*
	$\mathbb{Z}_7 \ltimes \mathbb{Z}_3$	$\langle x, y \mid x^7 = y^3 = e, x^y = x^2 \text{ bzw. } x^4\rangle$		*nicht abelsch, auflösbar, (nicht nilpotent)*
22	$\mathbb{Z}_2 \times \mathbb{Z}_{11}$		$\mathbb{Z}_{22}$	*zyklisch*
	$\mathbb{D}_{22}$	$\langle x, y \mid x^{11} = y^2 = e, x^y = x^{-1}\rangle$		*Diedergruppe: nicht abelsch, auflösbar, (nicht nilpotent)*
23	$\mathbb{Z}_{23}$			*zyklisch, einfach*
24	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$		$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_6$	*abelsch*
	$\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3$		$\mathbb{Z}_2 \times \mathbb{Z}_{12}$	*abelsch*
	$\mathbb{Z}_8 \times \mathbb{Z}_3$		$\mathbb{Z}_{24}$	*zyklisch*
	$\mathbb{D}_8 \times \mathbb{Z}_3$	$\langle x, y, z \mid x^4 = y^2 = z^3 = e, x^y = x^{-1} x^z = x, y^z = y\rangle$		*nicht abelsch, auflösbar, (nilpotent)*

$\lvert G\rvert$	**Isomorphie-typ von** G	**Präsentationen**	**isomorphe Gruppen**	**WichtigeEigenschaften**
	$\mathbb{H}_2 \times \mathbb{Z}_3$	$\langle x,y,z \mid x^4 = z^3 = e, y^2 = x^2, x^y = x^{-1}, x^z = x, y^z = y\rangle$		*nicht abelsch, auflösbar, (nilpotent)*
	$\mathbb{Z}_3 \ltimes \mathbb{Z}_8$	$\langle x,y \mid x^8 = y^3 = e, y^x = y^{-1}\rangle$		*nicht abelsch, auflösbar, (nicht nilpotent)*
	$\mathbb{H}_6$	$\langle x,y \mid x^{12} = e, y^2 = x^3, x^y = x^{-1}\rangle$	$\mathbb{Z}_6 \ltimes \mathbb{Z}_4$	*Dizyklische Gruppe: nicht abelsch, auflösbar, (nicht nilpotent)*
	$\mathbb{Z}_{12} \ltimes \mathbb{Z}_2$	$\langle x,y \mid x^{12} = y^2 = e, x^y = x^5\rangle = \langle a,b,c \mid a^3 = b^4 = c^2 = e, a^b = a, b^c = b, a^c = a^{-1}\rangle$	$\mathbb{Z}_3 \ltimes (\mathbb{Z}_4 \times \mathbb{Z}_2)$	*nicht abelsch, auflösbar, (nicht nilpotent)*
	$\mathbb{A}_4 \times \mathbb{Z}_2$	$\langle x,y,z,u \mid u^2 = x^2 = y^2 = z^3 = e, x^u = x, y^u = y, z^u = z, x^z = y, y^z = xy\rangle$		*nicht abelsch, auflösbar, (nicht nilpotent)*
	$\mathbb{S}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	$\langle x,y,u,v \mid u^2 = v^2 = x^2 = y^3 = e, x^u = x^v = x, y^u = y^v = y, x^y = x^{-1}\rangle$		*nicht abelsch, auflösbar, (nicht nilpotent)*
	$\mathrm{Sl}_2(3)$	$\langle x,y,z \mid x^4 = z^3 = e, y^2 = x^2, x^y = x^{-1}, x^z = y, y^z = xy\rangle = \langle a,b \mid a^3 = b^3, (ab)^2 = b^3\rangle$	$\mathbb{H}_2 \ltimes \mathbb{Z}_3$	*Spezielle lineare Gruppe: nicht abelsch, auflösbar, (nicht nilpotent)*
	$\mathbb{Z}_3 \ltimes \mathbb{H}_2$	$\langle x,y,z \mid x^4 = z^3 = e, y^2 = x^2, x^y = x^{-1}, z^x = z, z^y = z^{-1}\rangle$		*nicht abelsch, auflösbar, (nicht nilpotent)*
	$\mathbb{D}_{24}$	$\langle x,y \mid x^{12} = y^2 = e, x^y = x^{-1}\rangle = \langle a,b,c \mid a^3 = b^4 = c^2 = e, a^b = a, a^c = a^{-1}, b^c = b^{-1}\rangle$	$\mathbb{Z}_{12} \ltimes \mathbb{Z}_2 \cong \mathbb{Z}_3 \ltimes \mathbb{D}_8$	*Diedergruppe: nicht abelsch, auflösbar, (nicht nilpotent)*
	$\mathbb{Z}_3 \ltimes \mathbb{D}_8$	$\langle a,b,c \mid a^3 = b^4 = c^2 = e, a^b = a^{-1}, a^c = a, b^c = b^{-1}\rangle$		*nicht abelsch, auflösbar, (nicht nilpotent)*
	$\mathbb{S}_4$	$\langle x,y \mid x^4 = y^3 = (xy)^2 = e\rangle$		*Symmetrische Gruppe: nicht abelsch, auflösbar, (nicht nilpotent)*
25	$\mathbb{Z}_5 \times \mathbb{Z}_5$			*elementarabelsch*
	$\mathbb{Z}_{25}$			*zyklisch*
26	$\mathbb{Z}_2 \times \mathbb{Z}_{13}$	$\langle x,y \mid x^{13} = y^2 = e, x^y = x^{-1}\rangle$	$\mathbb{Z}_{26}$	*zyklisch*
	$\mathbb{D}_{26}$			*Diedergruppe: nicht abelsch, auflösbar, (nicht nilpotent)*
27	$\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$			*elementarabelsch*
	$\mathbb{Z}_3 \times \mathbb{Z}_9$			*abelsch*
	$\mathbb{Z}_{27}$			*zyklisch*
	$\mathbb{Z}_9 \ltimes \mathbb{Z}_3$	$\langle x,y \mid x^9 = y^3 = e, x^y = x^4\rangle$		*nicht abelsch, auflösbar, (nilpotent)*
	$(\mathbb{Z}_3 \times \mathbb{Z}_3) \ltimes \mathbb{Z}_3$	$\langle x,y,z \mid x^3 = y^3 = z^3 = e, z^x = z, z^y = z, y^x = yz\rangle$		*nicht abelsch, auflösbar, (nilpotent); Exponent von* G *ist 3*
28	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_7$		$\mathbb{Z}_2 \times \mathbb{Z}_{14}$	*abelsch*
	$\mathbb{Z}_4 \times \mathbb{Z}_7$		$\mathbb{Z}_{28}$	*zyklisch*
	$\mathbb{D}_{28}$	$\langle x,y \mid x^{14} = y^2 = e, x^y = x^{-1}\rangle$	$\mathbb{Z}_{14} \ltimes \mathbb{Z}_2$	*nicht abelsch, auflösbar, (nicht nilpotent)*

$\lvert G\rvert$	**Isomorphie-typ von G**	**Präsentationen**	**isomorphe Gruppen**	**WichtigeEigenschaften**
	$\mathbb{H}_7$	$\langle x, y \mid x^7 = y^4 = e, x^y = x^{-1}\rangle$	$\mathbb{Z}_7 \ltimes \mathbb{Z}_4$	*nicht abelsch, auflösbar, (nicht nilpotent)*
29	$\mathbb{Z}_{29}$			*zyklisch, einfach*
30	$\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5$		$\mathbb{Z}_{30}$	*abelsch*
	$\mathbb{D}_{10} \times \mathbb{Z}_3$	$\langle x, y \mid x^{15} = y^2 = e, x^y = x^4\rangle$		*nicht abelsch, auflösbar, (nicht nilpotent)*
	$\mathbb{S}_3 \times \mathbb{Z}_5$	$\langle x, y \mid x^{15} = y^2 = e, x^y = x^{11}\rangle$		*nicht abelsch, auflösbar, (nicht nilpotent)*
	$\mathbb{D}_{30}$	$\langle x, y \mid x^{15} = y^2 = e, x^y = x^{-1}\rangle$		*nicht abelsch, auflösbar, (nicht nilpotent)*
31	$\mathbb{Z}_{31}$			*zyklisch, einfach*
32	*51 Gruppen*			*Siehe* [HS64].
33	$\mathbb{Z}_3 \times \mathbb{Z}_{11}$		$\mathbb{Z}_{33}$	*zyklisch*
34	$\mathbb{Z}_2 \times \mathbb{Z}_{17}$			*zyklisch*
	$\mathbb{D}_{34}$	$\langle x, y \mid x^{17} = y^2 = e, x^y = x^{-1}\rangle$		*Diedergruppe: nicht abelsch, auflösbar*
35	$\mathbb{Z}_5 \times \mathbb{Z}_7$		$\mathbb{Z}_{35}$	*zyklisch*

Bei den semidirekten Produkten in der Tabelle wurde der zugehörige Homomorphismus stets weggelassen, kann aber aus der angegebenen Präsentation der Gruppe unmittelbar abgelesen werden. (Vgl. auch [Hum96] *Appendix B.)*

Beweis: Aufgrund des Hauptsatzes über abelsche Gruppen können wir o. E. annehmen, daß G nicht abelsch ist. Da Gruppen von Primzahl- und Primzahlquadratordnung abelsch sind (siehe Satz 1.13 sowie Korollar 7.10), sind somit die Fälle $|G| = 1, 2, 3, 4, 5, 7, 9, 11, 13, 17, 19, 23, 25, 29, 31$ behandelt. Es bleiben also die nicht abelschen Gruppen G mit $|G| = 6, 8, 10, 12, 14, 15, 16, 18, 20, 21, 22, 26, 28, 30, 33, 34, 35, (24, 27, 32)$ zu betrachten.

$\underline{|G| = 6, 10, 14, 22, 26, 34}$**:** Satz 14.3 liefert, daß $G \cong \mathbb{D}_{|G|}$.

$\underline{|G| = 15, 33, 35}$**:** Nach Satz 14.3 gilt: $G \cong \mathbb{Z}_{|G|}$.

$\underline{|G| = 20}$**:** Nach Satz 14.5 gilt: $G \cong \mathbb{D}_{20}$, $G \cong \mathbb{H}_5$ oder $G \cong \mathbb{Z}_5 \ltimes \mathrm{Aut}(\mathbb{Z}_5)$.

$\underline{|G| = 28}$**:** Nach Satz 14.5 gilt: $G \cong \mathbb{D}_{28}$ oder $G \cong \mathbb{H}_7$.

$\underline{|G| = 8}$**:** Siehe Satz 9.12.

$\underline{|G| = 12}$**:** Es seien $U \in \mathrm{Syl}_2(G)$ und $V \in \mathrm{Syl}_3(G)$.

Aus Lemma 14.4 folgt, daß entweder U oder V ein Normalteiler ist, also ist $G = U \cdot V$ und das Produkt ist semidirekt.

1. Fall: $U \lhd G$**:** Dann ist $G \cong U \ltimes_\varphi V$ mit $\varphi : V \to \mathrm{Aut}(U)$.

Angenommen, $U \cong \mathbb{Z}_4$. Da φ nicht der triviale Homomorphismus ist, also $|\varphi(V)| = 3$, müßte $\mathbb{Z}_4$ einen Automorphismus der Ordnung 3 besitzen, aber $\mathrm{Aut}(\mathbb{Z}_4) \cong \mathbb{Z}_2$, Widerspruch.

Also gilt: $U \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. Damit ist $\mathrm{Aut}(U) \cong \mathrm{Gl}_2(2)$. Da nun $\mathrm{Gl}_2(2)$ genau eine Untergruppe der Ordnung drei besitzt, gibt es also zwei Möglichkeiten, φ zu definieren. Die entstehenden Gruppen sind offensichtlich isomorph zueinander.

2. Fall: $V \lhd G$**:** Wie im Beweis von Satz 14.5 folgt: $G \cong \mathbb{D}_{12}$ oder $G \cong \mathbb{H}_3$.

(Vgl. auch [Hum96] 22.8.)

$|G| = 16$**:** Wir zeigen zunächst, daß höchstens die angegebenen Isomorphietypen in Frage kommen, und überlegen uns dann, daß diese alle nicht isomorph sind. Dabei wird vorausgesetzt, daß die angegebenen Präsentationen wirklich Gruppen der Ordnung 16 ergeben, wie man leicht nachprüft.

1. Fall: $\operatorname{Exp}(G) = 8$**:** Es existiert also ein Normalteiler $N = \langle x \rangle \lhd G$ von G mit $o(x) = 8$. Wir unterscheiden die folgenden beiden Fälle:

(i) $\exists\, y \in G \backslash N$ mit $o(y) = 2$.
Dann gilt $o(x^y) = 8$ und $x^y \neq x$, also $x^y \in \{x^3, x^5, x^7\}$ und wir erhalten eine der ersten drei angegebenen nicht abelschen Gruppen der Ordnung 16. (Diese unterscheiden sich dadurch, daß sie 9 bzw. 3 bzw. 5 Elemente der Ordnung 2 enthalten.)

(ii) $\forall\, y \in G \backslash N$ gilt: $o(y) > 2$.
Angenommen, $o(y) = 8$ für alle $y \in G \backslash N$. Wähle ein solches y. Dann gilt $y^2 = x^r$ mit $r = 2$ oder $r = 6$. Ferner gilt $x^y = x^s$ mit $s \in \{3, 5, 7\}$, und damit $yx = x^s y$.

a. $s = 5$: Dann gilt: $(xy)^2 = x^6 y^2 = x^{6+r} \in \{x^8, x^{12}\} = \{e, x^4\}$ und somit $o(xy) = 2$ oder $o(xy) = 4$, im Widerspruch zu $xy \notin N$.

b. $s = 3$ oder $s = 7$: Nun gilt: $(x^{8-r} y)y = x^{8-r+r} = e$, also $e = y(x^{8-r} y) = x^{s(8-r)} y^2 = x^{r+s(8-r)} = x^{(1-s)r}$. Daraus folgt: $8 | (1-s)r \in \{-4, -12, -36\}$, was offenbar nicht der Fall ist.

Also gibt es ein $y \in G \backslash N$ mit $o(y) = 4$, und es gilt $x^y \in \{x^3, x^5, x^7\}$. Wegen $y \notin \langle x \rangle$, gilt $y^2 \notin y\langle x \rangle$, also $y^2 \in \langle x \rangle$ und damit $y^2 = x^4$.
Angenommen, $x^y = x^3$ (bzw. $x^y = x^5$), dann gilt: $(xy)^2 = e$ (bzw. $(x^6 y)^2 = e$), im Widerspruch zu $o(xy) \neq 2$ (bzw. $o(x^6 y) \neq 2$).
Also gilt: $x^y = x^7$ und damit $G = \langle x, y \mid x^8 = e, y^2 = x^4, x^y = x^{-1} \rangle$.
(Diese Gruppe enthält nur ein Element der Ordnung 2, kann also nicht isomorph zu den drei vorhergehenden sein.)

2. Fall: $\operatorname{Exp}(G) = 4$**:** Wir zeigen zunächst: $\exists\, N \lhd G$ mit $N \cong \mathbb{Z}_4 \times \mathbb{Z}_2$.
Angenommen, dies ist nicht der Fall. Da der Exponent von G vier ist, besitzt G ein Element der Ordnung 4 und somit eine maximale Untergruppe N, die dieses enthält. Lemma 7.12 impliziert, daß N ein Normalteiler der Ordnung 8 ist. Nun gilt: $N \not\cong \mathbb{Z}_8$ und $N \not\cong \mathbb{Z}_4 \times \mathbb{Z}_2$. Es bleiben also die beiden folgenden Fälle:

(i) $N \cong \mathbb{D}_8$. Dann besitzt N genau zwei Elemente der Ordnung 4, also eine Untergruppe $\langle x \rangle$ der Ordnung 4, die normal in G ist.
Angenommen, es gibt ein $y \in G \backslash \langle x \rangle$ mit $x^y = x$, dann gilt $\langle x, y \rangle \cong \mathbb{Z}_4 \times \mathbb{Z}_2$ oder $\langle x, y \rangle \cong \mathbb{Z}_4 \times \mathbb{Z}_4$, was beides zum Widerspruch führt.
Also gilt für alle $y \in G \backslash \langle x \rangle$, $x^y = x^{-1}$. Da $|G/\langle x \rangle| = 4$, gibt es $y, z \in G \backslash \langle x \rangle$ mit $y \not\equiv z^{-1} (\operatorname{mod} \langle x \rangle)$. Es folgt $yz \notin \langle x \rangle$, im Widerspruch zu $x^{(yz)} = x$.
Also gilt o. E., G besitzt keine Untergruppe isomorph zu $\mathbb{D}_8$.

(ii) $N \cong \mathbb{Q}_8$. Es sei $N = \langle x, y \mid x^4 = e, y^2 = x^2, x^y = x^{-1} \rangle$. Wähle $z \in G \backslash N$ sowie eine maximale Untergruppe $M \lessdot G$, die z enthält. Dann gilt $|M \cap N| = \frac{8 \cdot 8}{16} = 4$, also ist $U := M \cap N \lhd N, M$ und damit $U \lhd MN = G$. Da $N \cong \mathbb{Q}_8$ muß U zyklisch sein, also o. E. $U = \langle x \rangle$, und damit $M = \langle x, z \rangle$.
Nach Voraussetzung gilt auch $M \cong \mathbb{Q}_8$, also $x^z = x^{-1} = x^y$ und damit $x^{(zy)} = x$. Wegen $z \notin N$, gilt $zy \notin \langle x \rangle$, also $\langle x, zy \rangle \cong \mathbb{Z}_4 \times \mathbb{Z}_2$ oder $\langle x, zy \rangle \cong \mathbb{Z}_4 \times \mathbb{Z}_4$, was wiederum beides zum Widerspruch führt.

Damit ist gezeigt, es gibt $\mathbb{Z}_4 \times \mathbb{Z}_2 \cong N = \langle x, y \rangle \lhd G$ mit $o(x) = 4$ und $o(y) = 2$.
Für $z \in G$ beliebig gilt $o(x^z) = 4$ und $x^z \in N$, also

$$x^z \in \{x, x^3, xy, x^3y\}. \tag{4}$$

Fall a.: $\exists z \in G \backslash N : o(z) = 2$: Es gilt $o(y^z) = 2$ und $y^z \in N$, also $y^z \in \{x^2, y, x^2y\}$. Aus (4) folgt, $x^2 = (x^z)^2 = (x^2)^z$, also $y^z \neq x^2$.
Es bleibt $y^z = y$ oder $y^z = x^2y$.
Vermittels (4) ergeben sich nun folgende Fälle:

(i) $x^z = x, y^z = y$, dann wäre G abelsch, Widerspruch.

(ii) $x^z = x, y^z = x^2y$, dann gilt $G = \langle x, y, z \mid x^4 = y^2 = z^2 = e, x^y = x, x^z = x, y^z = x^2y \rangle$.

(iii) $x^z = x^3, y^z = y$, dann gilt $G = \langle x, y, z \mid x^4 = y^2 = z^2 = e, x^y = x, x^z = x^3, y^z = y \rangle$.

(iv) $x^z = x^3, y^z = x^2y$. Setze $\tilde{x} := xy$, dann gilt $\tilde{x}^z = x^3x^2y = \tilde{x}$ und wir befinden uns wieder im Unterfall (ii).

(v) $x^z = xy, y^z = y$, dann gilt $G = \langle x, y, z \mid x^4 = y^2 = z^2 = e, x^y = x, x^z = xy, y^z = y \rangle$.

(vi) $x^z = xy, y^z = x^2y$, dann würde gelten $x^{(z^2)} = (xy)^z = xyx^2y = x^3 \neq x$, im Widerspruch zu $o(z) = 2$.

(vii) $x^z = x^3y, y^z = y$. Setzen wir $\tilde{y} := x^2y$, so gilt $x^z = x\tilde{y}, \tilde{y}^z = \tilde{y}$ und wir sind wieder im Unterfall (v).

(viii) $x^z = x^3y, y^z = x^2y$, dann würde wieder gelten $x^{(z^2)} = (x^3y)^z = x^3 \neq x$, im Widerspruch zu $o(z) = 2$.

Fall b.: $\forall z \in G \backslash N$ gilt $o(z) = 4$, aber $\exists z \in G \backslash N : \langle x \rangle \cap \langle z \rangle = \mathbb{1}$:
Es gilt $o(z^2) = 2$ und $z^2 \neq x^2$, also $z^2 \in \{y, x^2y\}$. Dann gilt aber: $y \in \{z^2, x^2z^2\}$.
Aufgrund von (4) und $\{x, x^3, xy, x^3y\} = \{x, x^3, xz^2, x^3z^2\}$ ergeben sich folgende Fälle:

(i) $x^z = x$, dann wäre $G = \langle x \rangle \times \langle z \rangle$ abelsch, Widerspruch.

(ii) $x^z = x^3$, dann ist $G = \langle x, z \mid x^4 = z^4 = e, x^z = x^3 \rangle$.

(iii) $x^z = xz^2$, dann gilt $zx = xz^3$ und damit $z^x = xzx^3 = x^2z^3x^2 = x^3z^9x = x^3zx = x^4z^3 = z^3$. Also sind wir nach Vertauschen von x und z im gleichen Fall wie zuvor.

(iv) $x^z = x^3z^2$. Da $o(z^2) = 2$, muß gelten $z^2 \in N$, also kommutiert z^2 mit x. Folglich gilt $zx = zxz^{-1}z = x^z z = x^3z^3 = (zx)^{-1}$, also $o(zx) = 2$ und damit $zx \in N$, im Widerspruch zu $z \notin N$.

Fall c.: $\forall z \in G\backslash N$ **gilt** $o(z) = 4$ **und** $\langle x\rangle \cap \langle z\rangle = \left\langle x^2\right\rangle$ **:**

Wähle $z \in G\backslash N$ beliebig.
Angenommen, $x^z = xy$ (bzw. $x^z = x^3y$).
Man beachte, daß $x^2 = z^2$ sowohl mit x als auch mit z vertauscht!
Dann gilt $(xz)^2 = xzxz^3z^2 = xx^zz^2 = x^3x^z$, also $(xz)^2 = y$ (bzw. $(xz)^2 = x^2y$) und damit $\langle x\rangle \cap \langle xz\rangle \neq \left\langle x^2\right\rangle$, im Widerspruch zu $xz \in G\backslash N$.
Also ist wegen (4) $z \in N_G(\langle x\rangle)$. Dann gilt aber $U := \langle x, z\rangle = \langle x\rangle \cdot \langle z\rangle$ und damit $|U| = 8$ nach der Produktformel.
Ferner gilt $o(y^z) = 2$, also $y^z \in \left\{y, x^2, x^2y\right\}$. Da $y \notin U$ gilt $y^z \neq x^2$.
Angenommen, $y^z = x^2y$, so würde folgen, $(yz)^2 = yzyz = y^zz^2 = yx^2yx^2 = e$, also $o(yz) = 2$ und damit $yz \in N$, im Widerspruch zur Wahl von $z \notin N$.
Also gilt: $y^z = y$.
Da G nicht abelsch ist, gilt $x^z \neq x$, also folgt aus (4): $x^z = x^3$. ($G = \left\langle x, y, z \;\middle|\; x^4 = y^2 = e, x^y = x, x^2 = z^2, x^z = x^3, y^z = y\right\rangle$.)

(Die Gruppen in Teil a. enthalten 7 bzw. 11 bzw. 7 Elemente der Ordnung zwei, die Gruppen in b. und c. jeweils nur 3. Die beiden Gruppen in a. mit je 7 Involutionen unterscheiden sich dadurch, daß erstere nicht abelsche Untergruppen hat, letztere nicht. Ebenso besitzt die Gruppe in c. nicht abelsche Untergruppen, während die Gruppe in b. nur abelsche Untergruppen besitzt. Die fünf Gruppen sind also paarweise nicht isomorph zueinander.)

$\underline{|G| = 18}$**:** Wie im Beweis von Satz 14.3 Teil d. sieht man $G \cong N \ltimes_\varphi U$ mit $|N| = 9$ und $|U| = 2$ sowie $\varphi : U \cong \mathbb{Z}_2 \to \operatorname{Aut}(N)$.

1. Fall: $N \cong \mathbb{Z}_9$**:** Dann ist $\operatorname{Aut}(N) \cong \mathbb{Z}_6$. Wie im Beweis von Satz 14.3 Teil d. sieht man, $G \cong \mathbb{D}_{18}$.

2. Fall: $N \cong \mathbb{Z}_3 \times \mathbb{Z}_3$**:** Dann ist N isomorph zur additiven Gruppe des Vektorraumes $GF(3)^2$ über dem Körper $GF(3)$ und damit $\operatorname{Aut}(N) \cong Gl_2(3)$. Da φ nicht der triviale Homomorphismus ist, folgt Fall 2 aus Lemma 8.12.

$\underline{|G| = 21}$**:** Folgt aus Satz 14.3 Teil c.
(Alternativ kann man unmittelbar sehen:
Es gilt: $r := |\mathrm{Syl}_7(G)| \equiv 1 (\mathrm{mod}\ 7)$. Wäre $r \geq 8$, dann hätte G mindestens $8 \cdot (7-1) = 48$ Elemente der Ordnung 7, was nicht geht. Also ist $r = 1$.
Seien $N \in \mathrm{Syl}_7(G)$ und $U \in \mathrm{Syl}_3(G)$, so ist also $N \lhd G$ und $G = N \ltimes_\varphi U$ mit $\varphi : U \to \operatorname{Aut}(N) \cong \mathbb{Z}_6$. Da es in $\mathbb{Z}_6$ nur eine Untergruppe der Ordnung 3 gibt, gibt es genau zwei Möglichkeiten für φ (da φ nicht trivial ist!), die

aber beide offenbar isomorphe Gruppen liefern. - Vgl. auch [Hum96] § 12 (2).)

$\underline{|G| = 24}$: Vgl. [Bur11] Chapter 126.

$\underline{|G| = 27}$: Vgl. [Hup67] I.14.10 oder [Hum96] 18.11.

$\underline{|G| = 30}$: Angenommen: $r := |\mathrm{Syl}_5(G)| \neq 1$.

Dann gilt $r \geq 6$ und damit gibt es mindestens $6 \cdot 4 = 24$ Elemente der Ordnung 5 in G. Dann enthält G aber nur eine 3-Sylowgruppe, die somit Normalteiler ist und deren Produkt mit einer 2-Sylowgruppe eine Untergruppe U der Ordnung 6 bildet, die aus Ordnungsgründen Normalteiler sein muß. Also operiert ein Element der Ordnung 5 auf einer Gruppe der Ordnung 6. Aber die einzigen Gruppen der Ordnung 6 sind $\mathbb{Z}_6$ und $\mathbb{S}_3$ mit $\mathrm{Aut}(\mathbb{Z}_6) \cong \mathbb{Z}_2$ und $\mathrm{Aut}(\mathbb{S}_3) \cong \mathbb{S}_3$. Also operiert der Fünfer trivial auf U und ist damit ein Normalteiler von G, im Widerspruch zu $r \neq 1$.

Also gilt: $\mathrm{Syl}_5(G) = \{N\}$.

Ist $V \in \mathrm{Syl}_3(G)$, so ist $NV < G$ mit $|NV| = 15$, also $NV \lhd G$. Ferner ist $NV \cong \mathbb{Z}_{15}$. Ist nun $U \in \mathrm{Syl}_2(G)$, so ist $G = (NV)U \cong \mathbb{Z}_{15} \ltimes_\varphi \mathbb{Z}_2$.

Betrachte also: $\varphi : \mathbb{Z}_2 \to \mathrm{Aut}(\mathbb{Z}_{15}) \cong \mathbb{Z}_2 \times \mathbb{Z}_4$.

Es gibt genau drei nicht-triviale Automorphismen der Ordnung 2, die zu folgenden drei nicht abelschen Gruppen führen:

a. $\langle x, y \mid x^{15} = y^2 = e, x^y = x^4 \rangle$,

b. $\langle x, y \mid x^{15} = y^2 = e, x^y = x^{11} \rangle$,

c. $\langle x, y \mid x^{15} = y^2 = e, x^y = x^{14} \rangle$.

Daß diese Gruppen nicht isomorph sind, sieht man leicht daran daß sie genau 5 bzw. 3 bzw. 14 Elemente der Ordnung 2 besitzen.

(Vgl. auch [Hum96] 12.5-12.6 und 13.8.)

□

AUFGABEN

15.3 Aufgabe

Auf Seite 63 im Beweis der Klassifikation der Gruppen von Ordnung 16 werden viele Aussagen über Elemente und ihre Ordnungen sowie über Untergruppen gemacht, die dort nicht bewiesen sind. Man prüfe diese Aussagen nach.

AUSBLICK: AUFLÖSBARE GRUPPEN

16.1 Allgemeine Hinweise

a. Das letzte Kapitel des Skriptes beschäftigt sich vornemlich mit auflösbaren Gruppen. Für ihr Studium sowie für das Studium anderer wichtiger Klassen von endlichen Gruppen ist die Betrachtung von gewissen subnormalen Ketten von Untergruppen extrem wichtig. So liefert etwa die Betrachtung des einfachsten Typs subnormaler Ketten, der Kompositionsreihen, durch die Tatsache, daß die Kompositionsfaktoren alle einfache Gruppen sind, die in Kapitel 2 angedeutete Interpretation der einfachen Gruppen als Bausteine der endlichen Gruppen. Die besondere Bedeutung der verschiedenen Typen von subnormalen Ketten hängt eng mit dem Satz von Jordan-Hölder zusammen, der aussagt, daß es im wesentlichen von jedem Typus subnormaler Ketten nur einen gibt. Der erste Teil dieses Kapitels befaßt sich deshalb mit dem Satz von Jordan-Hölder.
Auflösbare Gruppen verdanken ihren Namen einem Umstand, der mit Gruppen scheinbar gar nichts zu tun hat. Betrachten wir ein Polynom - der Einfachheit halber in $\mathbb{Q}[x]$ - und können wir seine Nullstellen durch einen Ausdruck in den Koeffizienten des Polynoms darstellen, in dem neben Addition und Multiplikation nur (ggf. verschachtelte) Wurzeln vorkommen, so sagt man, das Polynom ist durch Radikale (Radix = Wurzel) auflösbar. Das Beispiel $x^2 + px + q$ mit den Nullstellen $-\frac{p}{2} \pm \sqrt{\frac{p^2}{4} - q}$ ist hinreichend bekannt. Auch für Polynome vom Grad 3 und 4 sind solche allgemeinen Lösungsformeln seit dem 16. Jahrhundert bekannt. So verwundert es nicht, daß die Mathematiker lange Zeit nach vergleichbaren Resultaten für höhere Grade suchten, wenn auch ohne Erfolg. Nun ist es ein besonderes Charakteristikum der Mathematik, daß sie innerhalb eines Modells nicht nur die Existenz gewisser Sachverhalte zeigen, sondern selbige auch als unmöglich erweisen kann. Und genau das tat Evariste Galois in seinem bedeutendsten Werk "Über die Bedingungen der Auflösbarkeit von Gleichungen durch Radikale" 1831 - im Alter von zarten 20 Jahren. Was aber noch erstaunlicher erscheinen mag, er tat dies, indem er gewisse Gruppen mit den Polynomen assoziierte und zeigte, daß die Polynome genau dann durch Radikale auflösbar sind, wenn die zugehörigen Gruppen die Eigenschaft aufweisen, die ihnen dann den Namen *auflösbare Gruppen* einbrachte.
Nun wird in diesem Kapitel aber nicht weiter auf diesen Zusammenhang eingegangen. Vielmehr werden einige äquivalente Möglichkeiten der Definition auflösbarer Gruppen mittels subnormaler Ketten von Untergruppen - den Hauptreihen, den Kompositionsreihen und den Kommutatorreihen - vorgestellt. Für uns wesentlich interessanter ist jedoch die Charakterisierung über die π-Hallgruppen, die eine Verallgemeinerung des Satzes von Sylow darstellt und weitere Einblicke in die Frage gewährt,

ob eine Gruppe zu einem Teiler der Gruppenordnung auch eine entsprechende Untergruppe besitzt. Abschließend werden noch einige Resultate angeführt, die es erlauben, allein aus der Gruppenordnung bereits Rückschlüsse auf die Auflösbarkeit der Gruppe zu ziehen.

b. Den ersten Teil, der sich mit dem Satz von Jordan-Hölder befaßt, kann man in [DH92] Kapitel A. § 3 nachlesen, und die Beweise finden sich in [Hup67] Kapitel I. § 11. Für den zweiten Teil, der sich mit auflösbaren Gruppen beschäftigt, kann man [Kur77] Kapitel VI. § 1 oder [Hup67] Kapitel I. § 8 heranziehen. Diese beiden geben zwei unterschiedliche Zugänge zum Begriff der auflösbaren Gruppe. Wir geben hier einen dritten möglichen Zugang, der [DH92] Kapitel A. § 10 folgt. Die Äquivalenz der Zugänge folgt aus [Kur77] 6.4.

16.2 Definition
Es sei G eine Gruppe, Ω eine Menge, $U \leq G$.
Ist jedem $\omega \in \Omega$ ein Endomorphismus von G zugeordnet (den wir der Einfachheit halber selbst kurz mit ω bezeichnen), so nennen wir G eine **Ω-Gruppe**. Ferner sagen wir U ist **Ω-zulässig**, falls für alle $\omega \in \Omega$ gilt: $\omega(U) \subseteq U$.

16.3 Bemerkung
Ist Ω eine Menge, G eine Ω-Gruppe und $N \trianglelefteq G$ Ω-zulässig.
Dann induziert jeder Endomorphismus *aus* Ω einen Endomorphismus von G/N, und wir können G/N selbst als Ω-Gruppe auffassen.

16.4 Definition
Es sei Ω eine Menge, G und H zwei Ω-Gruppen, $\alpha \in \mathrm{Hom}(G, H)$.
α heißt ein **Ω-Homomorphismus**, falls für alle $g \in G$ und $\omega \in \Omega$ gilt: $\alpha(\omega(g)) = \omega(\alpha(g))$, d. h. $\alpha \circ \omega = \omega \circ \alpha$.

16.5 Beispiel

a. Es sei $\Omega = \emptyset$, dann ist jede Gruppe eine Ω-Gruppe, jede Untergruppe ist Ω-zulässig und jeder Homomorphismus ist ein Ω-Homomorphismus.

b. Ist G eine Gruppe und $\Omega = \mathrm{Inn}(G)$, so ist eine Untergruppe genau dann Ω-zulässig, wenn sie ein Normalteiler von G ist.

c. Ist G eine Gruppe und $\Omega = \mathrm{Aut}(G)$, so nennt man eine Ω-zulässige Untergruppe U eine **charakteristische** Untergruppe und schreibt $U \operatorname{char} G$.

16.6 Definition
Es sei Ω eine Menge, G eine Ω-Gruppe.

a. Eine Kette von Untergruppen $\mathbb{1} = U_0 < U_1 < \ldots < U_n = G$ heißt **subnormal**, wenn für alle $i = 1, \ldots, n$ gilt: $U_{i-1} \triangleleft U_i$.

b. Eine subnormale Kette $\mathbb{1} = U_0 < U_1 < \ldots < U_n = G$ Ω-zulässiger Untergruppen von G, so heißt diese eine **Ω-Kompositionsreihe**, falls für alle $i = 1, \ldots, n$ gilt, daß U_i/U_{i-1} Ω-einfach ist, d. h. U_i/U_{i-1} enthält nur die trivialen Ω-zulässigen Normalteiler. Die U_i/U_{i-1} nennt man die Ω-**Kompositionsfaktoren**.

c. Ist $\Omega = \emptyset$, so nennt man eine Ω-Kompositionsreihe auch schlicht eine **Kompositionsreihe** und die Ω-Kompositionsfaktoren kurz **Kompositionsfaktoren**.

d. Ist $\Omega = \mathrm{Inn}(G)$, so nennt man eine Ω-Kompositionsreihe auch schlicht eine **Hauptreihe** und die Ω-Kompositionsfaktoren einfach **Hauptfaktoren**.

e. Ist $\Omega = \mathrm{Aut}(G)$, so nennt man eine Ω-Komositionsreihe auch eine **charakteristische Reihe**.

16.7 Satz (Jordan-Hölder)
Es sei Ω eine Menge und G eine Ω-Gruppe. Ferner seien $\mathbb{1} = U_0 < U_1 < \ldots < U_r = G$ und $\mathbb{1} = V_0 < V_1 < \ldots < V_s = G$ zwei Ω-Kompositionsreihen in G. Dann gilt: $r = s$ und es gibt eine Permutation $\pi \in \mathbb{S}_r$ so, daß für alle $i = 1, \ldots, r$ gilt: $U_i/U_{i-1} \cong V_{\pi(i)}/V_{\pi(i)-1}$.

Beweis: Vgl. [Hup67] 11.5 (oder [Kur77] p. 11 für den Fall $\Omega = \emptyset$). □

16.8 Definition
Eine endliche Gruppe G heißt **auflösbar**, falls sie eine Hauptreihe besitzt, deren Hauptfaktoren alle abelsch sind.

16.9 Beispiel
Eine nicht abelsche einfache Gruppe ist nicht auflösbar, insbesondere ist also $\mathbb{A}_5$ nicht auflösbar. Sie ist zugleich die Gruppe kleinster Ordnung, die nicht auflösbar ist, denn für jede nicht auflösbare Gruppe gilt, sie enthält einen nicht abelschen einfachen Hauptfaktor und $\mathbb{A}_5$ ist die kleinste nicht abelsche einfache Gruppe. (Vgl. 5.5.)

16.10 Satz
Es sei G eine endliche Gruppe, $U \leq G$, $N, M \trianglelefteq G$.

a. *Ist G auflösbar, so ist U auflösbar.*

b. *G ist auflösbar genau dann, wenn N und G/N auflösbar sind.*

c. *Sind N und M auflösbar, so ist NM auflösbar.*

d. *Sind G/N und G/M auflösbar, so ist $G/(N \cap M)$ auflösbar.*

Beweis: Vgl. [DH92] A.10.2. □

16.11 Definition und Satz
Es sei G eine Gruppe, $g, h \in G$.
Wir nennen $[g, h] := ghg^{-1}h^{-1}$ den **Kommutator** von g mit h, und die Gruppe $G^{(1)} := [G, G] := \langle [a, b] \mid a, b \in G \rangle$ die **(erste) Kommutatorgruppe** von G.
Ferner setzen wir $G^{(k)} := [G^{(k-1)}, G^{(k-1)}]$.
Man sieht leicht, daß $G^{(k)} \trianglelefteq G$, und wir bezeichnen die Reihe $G \supseteq G^{(1)} \supseteq G^{(2)} \supseteq G^{(3)} \supseteq \ldots$ als die **Kommutatorreihe** von G.

16.12 Satz

Es sei G *eine endliche Gruppe.*
Dann sind die folgenden Aussagen äquivalent:

a. G *ist auflösbar.*

b. *Es gibt eine Kette* $\mathbb{1} = N_0 < N_1 < \ldots < N_n = G$ *von Normalteilern von G, so daß für alle* $i = 1, \ldots, n$ *gilt:* N_i/N_{i-1} *ist abelsch.*

c. *Die Kompositionsfaktoren von* G *haben Primzahlordnung.*

d. *Es gibt eine Zahl* $n \in \mathbb{N}$*, so daß* $G^{(n)} = 1$.

Beweis: Vgl. [DH92] A.10.3. □

16.13 Definition

Es sei G eine endliche Gruppe, π eine Menge von Primzahlen und π' die Menge aller Primzahlen, die nicht in π sind. Wir nennen eine Zahl eine π-Zahl, falls sie nur von Primzahlen in π geteilt wird.
Eine Untergruppe H von G heißt eine **π-Hall(unter)gruppe** von G, falls $|H|$ eine π-Zahl ist und $|G : H|$ eine π'-Zahl.

16.14 Beispiel

Es sei G eine endliche Gruppe und $\pi = \{p\}$, dann sind die π-Hallgruppen von G gerade die p-Sylowgruppen von G.

16.15 Theorem (Hall)

Eine endliche Gruppe G *ist auflösbar genau dann, wenn* G *für jede Primzahlmenge* π π*-Hallgruppen besitzt.*
In diesem Falle bilden die π*-Hallgruppen eine Konjugiertenklasse und jede* π*-Untergruppe von* G *ist in einer* π*-Hallgruppe von* G *enthalten.*

Beweis: Vgl. [DH92] I.3.3 und I.3.6. □

16.16 Korollar

Ist G *eine endliche auflösbare Gruppe und gilt* $m := p_1^{\nu_1} \cdots p_r^{\nu_r} \mid |G|$*, während* $p_i \nmid \frac{|G|}{m}$*, dann besitzt* G *auch eine Untergruppe der Ordnung* m.

16.17 Bemerkung

Betrachtet man die Klassifikation der Gruppen bis zur Ordnung 20, so könnte der Eindruck entstehen, alle Gruppen ungerader Ordnung seien abelsch. Daß dies nicht so ist, zeigt bereits die Gruppe $\mathbb{Z}_7 \ltimes_\varphi \mathbb{Z}_3$ der Ordnung 21 mit $\varphi : \mathbb{Z}_3 \hookrightarrow \mathrm{Aut}(\mathbb{Z}_7) \cong \mathbb{Z}_6$, und das verwundert zweifelsohne auch niemanden. Eine so wesentliche Strukturaussage nur daran festzumachen, ob zwei ein Teiler der Gruppenordnung ist oder nicht, erscheint recht unwahrscheinlich. Umso bemerkenswerter ist der folgende tiefliegende Satz von Feit-Thompson, an den wir zwei weitere Sätze ähnlicher Art anschließen, bei denen allein aus Eigenschaften der Gruppenordnung auf die Auflösbarkeit der Gruppe geschlossen wird.

16.18 Theorem (Feit-Thompson)

Sei G *ein Gruppe ungerader Ordnung, dann ist* G *auflösbar.*

Beweis: Siehe [FT63]. Man beachte, daß diese fast 300 Seiten ausschließlich dem Beweis dieses einen Satzes gewidmet sind und etliche weitere nicht triviale Ergebnisse verwenden! □

16.19 Theorem (Thompson)
Sei G *eine Gruppe mit* $3 \nmid |G|$ *und* $5 \nmid |G|$, *dann ist* G *auflösbar.*

16.20 Theorem (Burnside)
Es sei G *eine Gruppe der Ordnung* $p^a q^b$ *mit* p *und* q *Primzahlen.*
Dann ist G *auflösbar.*

Beweis: Vgl. [DH92] I.2. □

INDEX

Literatur

[Bur11] W. Burnside, *Theory of groups of finite order*, Dover, 1911.

[Dev94] Keith Devlin, *Sternstunden der Mathematik*, dtv wissenschaft, no. 4591, dtv, 1994.

[DH92] Klaus Doerk and Trevor Hawkes, *Finite soluble groups*, De Gruyter Expositions in Mathematics, no. 4, De Gruyter, 1992.

[Doe72] Klaus Doerk, *Lineare Algebra I*, Mainz, 1972.

[Doe74] Klaus Doerk, *Lineare Algebra II, Kapitel VII*, Mainz, 1974.

[FT63] Walter Feit and J. G. Thompson, *Solvability of groups of odd order*, Pacific Journal of Mathematics **13** (1963), 755–1029.

[Gor80] Daniel Gorenstein, *Finite groups*, 2 ed., Chelsea Publ. Co. , New York, 1980.

[Gor82] Daniel Gorenstein, *Finite simple groups*, Plenum Print, New York, 1982.

[Gor83] Daniel Gorenstein, *The classification of finite simple groups*, vol. 1, Plenum Print, New York, 1983.

[Gor96] Daniel Gorenstein, *The classification of finite simple groups*, vol. 2, Plenum Print, New York, 1996.

[Höl93] Otto Hölder, *Die Gruppen der Ordnungen* p^3, pq^2, pqr, p^4, Math. Ann. **43** (1893), 301–412.

[HS64] Marshall Hall and James Senior, *The groups of order* 2^n *(*$n \leq 6$*)*, Macmillan, New York, 1964.

[Hum96] John F. Humphreys, *A course in group theory*, OUP, Oxford, 1996.

[Hup67] Bertram Huppert, *Endliche Gruppen*, vol. 1, Die Grundlehren der mathematischen Wissenschaften, no. 134, Springer, Berlin, 1967.

[Hup69] Bertram Huppert, *Lineare Algebra I*, Mainz, 1969.

[Kur77] Hans Kurzweil, *Endliche Gruppen*, Springer Hochschultext, Springer, 1977.

[Suz82] Michio Suzuki, *Group theory I*, Die Grundlehren der mathematischen Wissenschaften, no. 247, Springer, 1982.

[Wei77] Michael Weinstein, *Examples of groups*, Polygonal Publishing House, 1977.