

Jun.-Prof. Dr. Steffen Kionke

Modul 61116

Algebra

LESEPROBE

Fakultät für
**Mathematik und
Informatik**

Das Werk ist urheberrechtlich geschützt. Die dadurch begründeten Rechte, insbesondere das Recht der Vervielfältigung und Verbreitung sowie der Übersetzung und des Nachdrucks bleiben, auch bei nur auszugsweiser Verwertung, vorbehalten. Kein Teil des Werkes darf in irgendeiner Form (Druck, Fotokopie, Mikrofilm oder ein anderes Verfahren) ohne schriftliche Genehmigung der FernUniversität reproduziert oder unter Verwendung elektronischer Systeme verarbeitet, vervielfältigt oder verbreitet werden.

Gesamt-Inhaltsverzeichnis

Kurseinheit 1	1-3
Einleitung zum Kurs Algebra	1-5
Literaturverzeichnis	1-9
Allgemeine Studierhinweise	1-11
1 Grundbegriffe der Gruppentheorie	1-17
1.1 Definitionen und Beispiele	1-18
1.2 Normalteiler, Faktorgruppe und Isomorphiesätze	1-34
1.3 Zyklische Gruppen	1-45
1.4 Operationen von Gruppen auf Mengen	1-50
1.5 p -Gruppen	1-58
Kurseinheit 2	2-1
Grundlagen der Gruppentheorie (Fortsetzung)	2-7
1.6 Kommutatorgruppe und auflösbare Gruppen	2-8
2 Strukturtheorie endlicher Gruppen	2-17
2.1 Die Sylow-Sätze	2-18
2.2 Endliche abelsche Gruppen	2-29
2.3 Klassifikation von Gruppen kleiner Ordnung	2-39
Kurseinheit 3	3-1
Strukturtheorie endlicher Gruppen (Fortsetzung)	3-9
2.4 Symmetrische und alternierende Gruppen	3-10
2.5 Normalreihen und Kompositionsreihen	3-24
3 Unendliche abelsche Gruppen	3-29
3.1 Abelsche Torsionsgruppen	3-30
3.2 Freie abelsche Gruppen. Endlich erzeugte abelsche Gruppen	3-36
Kurseinheit 4	4-1
4 Algebraische Körpererweiterungen	4-9
4.1 Einige Grundbegriffe über Ringe und Ideale	4-11
4.2 Polynomringe	4-21
4.3 Beispiele für Körper. Quotientenkörper	4-29
4.4 Endliche und algebraische Körpererweiterungen	4-34
4.5 Beispiele. Irreduzibilitätskriterien	4-46

4.6	Primkörper und die Charakteristik eines Körpers	4-58
4.7	Konstruktionen mit Zirkel und Lineal	4-61
Kurseinheit 5		5-1
5	Galois-Theorie	5-7
5.1	Zerfällungskörper und normale Körpererweiterungen	5-9
5.2	Separable und inseparable Körpererweiterungen	5-22
5.3	Galois-Erweiterungen	5-31
5.4	Der Hauptsatz der Galois-Theorie	5-40
5.5	Beispiele	5-47
Kurseinheit 6		6-1
6	Anwendungen der Galois-Theorie	6-7
6.1	Endliche Körper	6-8
6.2	Einheitswurzelkörper	6-13
6.3	Norm und Spur. Zyklische Erweiterungen	6-23
6.4	Auflösung von Gleichungen durch Radikale	6-30
6.5	Ergänzungen zur Galois-Theorie	6-37
Kurseinheit 7		7-1
Anwendungen der Galois-Theorie (Fortsetzung)		7-9
6.6	Algebraische Gleichungen vom Grad 3 und 4	7-10
6.7	Algebraische Gleichungen vom Grad n	7-23
6.8	Der Fundamentalsatz der Algebra	7-27
6.9	Algebraisch abgeschlossene Körper	7-29
7	Transzendente Körpererweiterungen	7-33
7.1	Rationale Funktionenkörper	7-34
7.2	Transzendenzbasen	7-41
Inhaltsverzeichnis, Glossar, Symbolverzeichnis, Index		0-1
	Glossar	0-4
	Symbolverzeichnis	0-45
	Index	0-49

Winfried Scharlau

Überarbeitung: Manfred Schulte, Steffen Kionke

Technische Mitarbeit: Martin Dörfer, Frank Rosemeier

In \LaTeX gesetzt von Petra Dittmer, Inge Schlemper und Marlies Benner

Algebra

Kurseinheit 1:

Grundbegriffe der Gruppentheorie

Inhaltsverzeichnis zu Kurseinheit 1

Einleitung zum Kurs Algebra	1-5
Literaturverzeichnis	1-9
Allgemeine Studierhinweise	1-11
Studierhinweise zu Kurseinheit 1	1-13
1 Grundbegriffe der Gruppentheorie	1-17
1.1 Definitionen und Beispiele	1-18
1.2 Normalteiler, Faktorgruppe und Isomorphiesätze	1-34
1.3 Zyklische Gruppen	1-45
1.4 Operationen von Gruppen auf Mengen	1-50
1.5 p -Gruppen	1-58
Lösungen zu den Aufgaben in Kurseinheit 1	1-62

Einleitung zum Kurs Algebra

Man kann die Mathematik zwanglos in drei große Teilgebiete einteilen: Analysis, Geometrie und Algebra. Diese Teilgebiete sind natürlich nicht scharf oder eindeutig voneinander zu trennen, sondern sie sind in vielfältigster Weise miteinander verbunden. Die Geometrie steht üblicherweise im Universitätsstudium hinter der Algebra und Analysis etwas zurück; jedoch enthält der Kurs Lineare Algebra wesentlich geometrische Teile (beispielsweise euklidische Räume). Früher hieß diese Vorlesung an deutschen Universitäten auch noch „Analytische Geometrie“, und erst in den letzten Jahrzehnten wurde der Stoff immer stärker algebraisiert. Heute wird man also die Lineare Algebra – insbesondere in der Form, wie sie von der FernUniversität angeboten wurde – der Algebra zurechnen.

Von den drei genannten Teilgebieten ist die Algebra vielleicht das „abstrakteste“, sicherlich das am wenigsten anschauliche und anwendungsbezogene. Sie hat jedoch innerhalb der Mathematik eine besondere zentrale Stellung, insofern als viele mathematische Grundbegriffe in der Algebra erklärt und genauer untersucht werden. Als Beispiel denken wir nur an den Körperbegriff, der eine fundamentale Rolle in der Algebra spielt. (Die Körper der reellen und komplexen Zahlen bilden dann die Grundlage der Analysis.) Auch ist die Verwendung der axiomatischen Methode, die für die Denkweise der Mathematik ganz besonders charakteristisch ist, in der Algebra am stärksten ausgeprägt. Hier werden ganze „Serien“ von Axiomensystemen systematisch auf ihre Konsequenzen untersucht.

Aus diesen Andeutungen ergibt sich auch schon das Wichtigste zur Stellung der Algebra innerhalb Ihres Mathematik-Studiums. Inhaltlich gesehen sollen Sie einige grundlegende mathematische Begriffe und Theorien (z. B. Gruppenbegriff und Gruppentheorie oder Körperbegriff und Körpertheorie) genauer kennenlernen. Methodisch gesehen sollen Sie in einigen weiteren – besonders wichtigen – Beispielen sehen, wie von einigen wenigen und ganz einfachen Grundprinzipien ausgehend sich eine umfangreiche vielfältige, tiefsinnige und schwierige mathematische Theorie aufbaut. Allerdings ist die Algebra ebenso wenig wie jedes andere mathematische Teilgebiet (nur) ein Gedankenspiel mit inhaltsleeren Symbolen und Formeln. Dies wird sofort deutlich, wenn man die historische Entwicklung der Mathematik verfolgt. So ist z. B. fast alles, was in diesem Kurs

behandelt wird, aus dem Bemühen entstanden, folgende Frage zu beantworten:

Gegeben sei eine algebraische Gleichung

$$a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 = 0$$

(die Koeffizienten a_0, \dots, a_n sind also fest vorgegeben). Was kann man über die Lösungen dieser Gleichungen sagen: Wieviele gibt es, wie hängen sie miteinander zusammen, wie kann man sie finden, welche Eigenschaften haben sie, wie hängen sie insbesondere von den Koeffizienten a_i ab?

Dies ist sicher eine recht konkrete und naheliegende Frage. Im Laufe einer jahrhundertelangen Entwicklung hat sich aber auch herausgestellt, dass dies eine ungeheuer schwierige Frage ist, und dass ein gewaltiger begrifflicher und theoretischer Aufwand notwendig ist, um sie einigermaßen zu beantworten. Sie sollten also beim Durcharbeiten des Kurses gelegentlich daran denken, dass der Stoff in der dargebotenen Form das Ergebnis langer und angestrebter Bemühungen ist (und auch dass die Entwicklung weitergeht und manches in einigen Jahrzehnten schon wieder anders dargestellt werden wird).

Die Algebra hat wenig konkrete Anwendung in anderen Wissenschaften. Am bekanntesten ist die Bedeutung der Gruppentheorie für die Atomphysik (die wirklich ohne Gruppentheorie nicht auskommt) und die Kristallographie. Die Anwendbarkeit der Gruppentheorie ergibt sich daher, dass es in ihr letzten Endes um das Phänomen der Symmetrie geht – die Symmetrien eines Objektes bilden stets eine Gruppe. Anwendungen anderer Teile der Algebra sind in der Informatik, genauer im Bereich der Kryptographie und Codierungstheorie, zu finden. Es ist also schwierig (und auch nicht notwendig) die Beschäftigung mit abstrakter Algebra durch Hinweise auf Anwendungen oder konkrete Bedeutung für andere Wissenschaften zu „rechtfertigen“. Vielmehr zeichnet sich die Algebra dadurch aus, dass sie innerhalb der Mathematik zu einem unabdingbaren Werkzeug geworden ist, mit dessen Hilfe viele schwierige Probleme gelöst werden konnten. Wie prägend die Methoden der Algebra inzwischen sind, sieht man auch an den vielen Teilgebieten der Mathematik die aus dem Einsatz algebraischer Hilfsmittel auf diverse Fragestellungen entstanden sind, z. B. die algebraische Geometrie, die algebraische Topologie oder die algebraische Zahlentheorie.

Es soll jetzt noch etwas mehr zum Inhalt des Kurses Algebra gesagt werden. Der behandelte Stoff ist in zwei große Kapitel eingeteilt:

Gruppentheorie (Kurseinheiten 1 bis 3)

Körpertheorie (Kurseinheiten 4 bis 7)

Ziel ist es jeweils, eine Einführung in diese wichtigen und umfangreichen Teilgebiete der Algebra zu geben. Dies ist wegen des großen Umfanges dieser Gebiete nur in sehr beschränktem Maße möglich. In vieler Beziehung kommen wir über die Grundlagen nicht hinaus, und nur in dem Kapitel über Körpertheorie wird eine gewisse Vollständigkeit erreicht. In jedem der zwei Teile des Kurses verfolgen wir zwei wesentliche Ziele: Einerseits wird – ausgehend von den Axiomen – die Theorie systematisch entwickelt, und einige grundlegende Sätze werden formuliert und bewiesen. Andererseits werden immer wieder konkrete Beispiele ausführlich besprochen. Auf die Behandlung und das Kennenlernen dieser Beispiele sollten Sie besonderen Wert legen. Es nützt wenig (und ist sowieso unmöglich), eine abstrakte Theorie zu lernen wie z. B. die Gruppentheorie und keine oder nur wenige „konkrete“ Beispiele von Gruppen wirklich zu kennen.

Eingangsvoraussetzung für die Teilnahme an diesem Kurs ist die erfolgreiche Teilnahme an den Kursen „Lineare Algebra“ und „Mathematische Grundlagen“. Dies ist natürlich nicht so zu verstehen, dass Sie jederzeit den gesamten Stoff dieser Kurse parat haben müssten. Entscheidend kommt es darauf an, dass Sie sich in diesen Kursen gewisse Grundkenntnisse angeeignet haben, und dass Sie schon Übung und Erfahrung in der Beschäftigung mit mathematischen Gegenständen haben. Die genauen inhaltlichen Voraussetzungen werden zu Beginn jeder Kurseinheit genannt. Methodisch müssen Sie die Gliederung in Definitionen, Sätze und Beweise kennen, die wichtigsten Techniken beherrschen, z. B. wissen, was es bedeutet, wenn ein Beweis mit dem Wort „Angenommen“ beginnt. Die Darstellung ist in diesem Kurs stellenweise weniger ausführlich als in früheren und verlangt von Ihrer Seite etwas größere Selbständigkeit. Diese Selbständigkeit sollte sich insbesondere darin zeigen, dass Sie selbst entscheiden, in welcher Form Sie die einzelnen Kurseinheiten durcharbeiten. Es ist möglich, den Stoff in der dargestellten Reihenfolge durchzuarbeiten. Es gibt aber auch Alternativen, z. B. könnten Sie zunächst eine Übersicht über den Inhalt der jeweiligen Kurseinheit gewinnen und dann mittels des Lehrtextes, der angegebenen Literatur, der Beispiele und der Aufgaben tiefer in den Stoff eindringen. In jedem Fall sollte ein Schwerpunkt Ihrer Arbeit in der Bearbeitung

der Aufgaben und Einsendeaufgaben liegen.

Die für diesen Kurs getroffene Stoffauswahl und die Art der Darstellung ist natürlich nicht kanonisch ist, sondern nur eine von vielen Möglichkeiten. Für Ihren Studienerfolg kommt es darauf an, dass Sie sich von der hier gewählten Darstellung freimachen und die wesentlichen Inhalte in einer Sie interessierenden und Ihrer Denkweise entsprechenden Form verstehen. Der eine orientiert sich mehr an Beispielen und Anwendungen, den anderen interessiert der konsequente Aufbau. Man kann nicht sagen, dass die eine Methode der anderen vorzuziehen ist, es kommt darauf an, dass Sie die Ihnen gemäße Arbeitsweise finden.

Ein wichtiges Hilfsmittel ist die im Literaturverzeichnis angegebene Literatur. Ein genaueres Studium eines der dort empfohlenen Bücher wird es Ihnen ermöglichen, andere Gesichtspunkte kennenzulernen, damit von diesem Text unabhängig zu werden und so schließlich die Algebra besser zu verstehen. Als Begleitlektüre ist das Werk von Meyberg geeignet, das in Inhalt und Zielsetzung weitgehend mit diesem Kurs übereinstimmt. Sehr gut, aber auch anspruchsvoll, ist das Buch von Lang. Es wird dort sehr viel mehr Stoff als in diesem Kurs dargestellt. Einige neuere Lehrbücher sind auch als E-Book verfügbar. Beispielsweise eignet sich der Text von Fischer gut als Begleitlektüre. Auch das umfangreiche Algebrabuch von Jantzen/Schwermer ist eine wertvolle Ergänzung zum Kurstext.

Literaturverzeichnis

Begleitlektüre zum Kurs

Die folgenden Bücher sind kostenlos als Online-Ressource über die Bibliothek der FernUniversität abrufbar.

Böhm, J. *Grundlagen der Algebra und Zahlentheorie*. Springer-Verlag 2016

Bosch, S. *Algebra*. Springer-Verlag, 8. Aufl. 2013

Fischer, G. *Lehrbuch der Algebra*.

Springer Fachmedien Wiesbaden, 4. Aufl. 2017

Jantzen, J. C., Schwermer, J. *Algebra*. Springer-Verlag, 2. Aufl. 2014

Karpfinger, C., Meyberg, K. *Algebra: Gruppen – Ringe – Körper*.

Springer-Verlag, 4. Aufl. 2017

Einige hilfreiche ältere Bücher sind allerdings nur gedruckt verfügbar.

Körner, O. *Algebra*. Studien-Text, Akademische Verlagsgesellschaft Frankfurt 1974 (239 Seiten)

Lang, S. *Algebra* (in englischer Sprache). Rev. 3rd ed. (914 Seiten) Springer-Verlag 2002 (geht über den Stoff des Kurses erheblich hinaus, hervorragend zur Ergänzung und Vertiefung)

Lorenz, F. *Einführung in die Algebra*, Teil I und Teil II. BI-Wissenschaftsverlag, Mannheim/Wien/Zürich 1987, 1990 (338 und 386 Seiten)

Meyberg, K. *Algebra* (in 2 Bänden). Hanser-Verlag, München 1975, 1976 (192 und 182 Seiten) (als Begleittext sehr gut geeignet, Aufbau stimmt weitgehend mit dem Kurs überein)

Meyberg, K., Vachenauer, P. *Aufgaben und Lösungen zur Algebra*.

Hanser-Verlag, München 1978 (241 Seiten)

(enthält 466 Aufgaben mit Lösungen)

Reiffen, H. J., Scheja, G., Vetter, U. *Algebra*.

Bibliographisches Institut, Mannheim 1969 (272 Seiten)

Ergänzende und weiterführende Literatur

- Artin, E. *Galois Theory*. Vorlesungsausarbeitung, in verschiedenen Versionen und Verlagen erschienen
- Bourbaki, N. *Algèbre* (zahlreiche Bände). Hermann, Paris
- Bourbaki, N. *Algèbre commutative* (zahlreiche Bände). Hermann, Paris
(umfassende und grundlegende Darstellung, systematischer Aufbau der Theorie in großer Allgemeinheit)
- Cohn, P. M. *Algebra*, Vol. 1, 2. Wiley & Sons, London 1974, 1977
- Godement, R. *Cours d'Algèbre*. Hermann, Paris, 1963
(ausführliche Darstellung der Grundlagen, einschließlich der Linearen Algebra)
- Hall, M. *The theory of groups*. Mac Millan Co. New York 1964
(Einführung in die Gruppentheorie)
- Jacobson, N. *Lectures in Abstract Algebra*. 3 Bände, Van Nostrand Co., Princeton, 1951, 1953, 1964
- Jacobson, N. *Basic Algebra I, II*. Freeman, San Francisco 1974, 1980
- MacLane, S., Birkhoff, G. *Algebra*. 4. Auflage, Macmillan Co., London, 1970
(ausführliche Darstellung der Grundbegriffe der Algebra und Linearen Algebra)
- Stewart, J. *Galois Theory*. Chapman and Hall, London 1973
- Zariski, O., Samuel, P. *Commutative Algebra*, Vol. I.
Van Nostrand, Princeton, 1958
(behandelt gründlich die Ring- und Körpertheorie)

Allgemeine Studierhinweise

Eingangsvoraussetzungen

Wie schon in der Einleitung gesagt, wird die Kenntnis der Kurse „Lineare Algebra“ und „Mathematische Grundlagen“ vorausgesetzt. Gelegentlich werden auch Begriffe aus dem Kurs „Analysis“ benötigt. Neben den allgemeinen Grundlagen über reelle und komplexe Zahlen werden aber nur an wenigen Stellen, etwa in Beispielen oder Aufgaben, Kenntnisse aus der Analysis benutzt. Die Grundbegriffe der Algebra werden hier von Grund auf entwickelt. Dies führt dazu, dass die Kurseinheiten 1 und 4, in denen die Grundbegriffe über Gruppen, Ringe und algebraische Körpererweiterungen eingeführt werden, ziemlich umfangreich sind. Zwar sind Teile dieser Kurseinheiten eine Wiederholung von Inhalten des Kurses „Lineare Algebra“, dennoch sollten Sie für diese Kurseinheiten mehr Zeit als üblich aufwenden und den Text sorgfältig durcharbeiten. Die in diesen Abschnitten eingeführten Begriffe sind die Grundlage des gesamten Kurses.

Aufteilung der Kurseinheiten

Wie üblich sind die Kurseinheiten aufgeteilt in: Studierhinweise (gelb), Lehrtext (weiß), Lösungen zu den Aufgaben im Lehrtext (blau) sowie Symbolverzeichnis und Index (weiß). Ein „L“ am Rand des Lehrtextes verweist auf den (blauen) Lösungsteil. Abschnitte des Lehrtextes in *Kleindruck* können von Ihnen ohne Nachteil übergangen werden. Sie gehören nicht unbedingt zum „Standardstoff“ und sind als weiterführende Ergänzung gedacht, sie werden in diesem Kurs in der Regel nicht mehr benötigt.

Aufgaben im Lehrtext

In den Lehrtext sind zahlreiche Übungsaufgaben eingearbeitet. Im Idealfall sollten Sie sich mit allen Aufgaben beschäftigen und nur dann auf die vorgeschlagenen Lösungen zurückgreifen, wenn Sie nicht weiterkommen. Vermutlich wird es Ihnen aber schon aus Zeitgründen nicht möglich sein, alle Aufgaben zu bearbeiten. Außerdem bestehen die meisten Aufgaben nicht aus schematischen Rechnungen, sondern verlangen von Ihnen eigenständige Ideen. Einige Aufgaben sind etwas schwieriger; um sie zu lösen, müssen Sie den Stoff schon sehr gut verarbeitet haben. Daher brauchen Sie nicht gleich zu erschrecken, wenn Sie viele Aufgaben nicht bearbeiten und lösen können. Auf jeden Fall sollten Sie die Formulierung jeder Aufgabe *lesen* (wenn Sie sie schon nicht *lösen*), da

die Ergebnisse der Aufgaben im Lehrtext benutzt werden. Wenn eine Aufgabe etwa in einem Beweis zitiert wird, dann sollten Sie sich die Aufgabe und ihre Lösung (noch einmal) ansehen. Die Aufgaben enthalten viele Beispiele und konkrete Anwendungen der allgemeinen Theorie. Deshalb sollten Sie sich mit möglichst vielen von ihnen befassen, insbesondere dann, wenn Sie die allgemeinen Begriffe der Theorie noch nicht richtig verstanden haben.

Einige technische Hinweise

Auf den Seiten des Textes steht rechts oben jeweils die letzte auf der Seite behandelte Ziffer. Damit können Sie durch Zurückblättern schnell eine Stelle wiederfinden, die später im Text zitiert wird. \square markiert das Ende eines Beweises. Bei Zitaten aus anderen Kursen steht LA für „Lineare Algebra“.

Autoren

Dieser Kurs, den Sie jetzt in den Händen halten, ist eine überarbeitete Fassung der ersten Hälfte des Kurses „Algebra I/II“, der 1977/78 von Winfried Scharlau allein geschrieben worden ist. Der Text wurde 1981 (und geringfügig 1996/97 für die \LaTeX -Fassung) von Manfred Schulte überarbeitet. Um den Kurs dem aktuellen Curriculum der FernUniversität anzupassen, wurde der Kurstext 2019 von Steffen Kionke leicht abgeändert.

Winfried Scharlau, Prof. Dr.

Geb. am 12.8.1940 in Berlin. Studium der Mathematik 1959–66 in Bonn und New York, Promotion 1967 in Bonn. 1965–70 Assistent an den Universitäten in Bonn und Bielefeld. Seit 1970 ord. Professor an der Universität Münster, 2005 emeritiert.

Manfred Schulte, Dr.

Geb. am 18.9.1949 in Hengsen (Kreis Unna). Studium der Mathematik 1968–74 in Münster, Diplom 1974, Promotion 1977 (bei W. Scharlau) in Münster. 1974–78 Assistent (m.d.V.b.) an der Universität in Münster. Seit 1978 wiss. Mitarbeiter im Fachbereich Mathematik der FernUniversität, 1983 Akademischer Rat, 1987 Akademischer Oberrat.

Studierhinweise zu Kurseinheit 1

Vorbemerkung

In dieser Kurseinheit wird nicht nur neuer Stoff erarbeitet, sondern es werden auch grundlegende Begriffe der Gruppentheorie, die bereits im Kurs „Lineare Algebra“ behandelt wurden, wiederholt. Entsprechend den Hinweisen im Lehrtext und im folgenden Abschnitt sollten Sie überprüfen, ob Sie die notwendigen Kenntnisse zum Einstieg in den Kurs besitzen, und gegebenenfalls vorhandene Lücken schließen. Dazu ist zu bemerken, dass die Voraussetzungen für die zunächst dargestellte Theorie sehr gering sind; für die wichtigen Beispiele wird gelegentlich etwas mehr vorausgesetzt.

Lehrziele

Nach dem Durcharbeiten dieser ersten Kurseinheit sollen Sie

- die Grundbegriffe der Gruppentheorie wie Gruppe, Untergruppe, Normalteiler, Homomorphismus, Faktorgruppe, Ordnung und Index kennen,
- einige wichtige Beispiele von Gruppen kennen, insbesondere zyklische Gruppen, symmetrische Gruppen, die Matrizen­gruppen $GL(n, K)$, die Dieder-Gruppe D_4 und die Quaternionen-Gruppe Q_8 ,
- den Homomorphiesatz und die Isomorphiesätze kennen und anwenden können,
- den Begriff der Operation einer Gruppe auf einer Menge kennen und wichtige Beispiele dafür wissen,
- die Technik der Klassengleichung beherrschen und beweisen können, dass das Zentrum einer p -Gruppe nicht trivial ist.

Eingangsvoraussetzungen und Literatur

Aus dem Kurs „Lineare Algebra“ sollten Sie schon mit den folgenden Begriffen vertraut sein, um diese Kurseinheit erfolgreich durchzuarbeiten.

Gruppe,
Körper,
Vektorraum,
Matrix, invertierbare Matrix,

Determinante,
Permutation.

Der Stoff dieser Kurseinheit ist in den im Literaturverzeichnis aufgeführten Büchern jeweils in den folgenden Abschnitten dargestellt. Eine (teilweise) Lektüre in einem dieser Bücher könnte eine nützliche Ergänzung sein, da Sie einige andere Gesichtspunkte kennenlernen würden.

Fischer:	1.1 – 1.3.1, 1.4 – 1.4.4 , 1.5.1, 1.6.7
Jantzen/Schwermer:	I. (ohne §5) und II. §3
Lang:	I 2. – 5.
Meyberg I:	1.3–1.8, 2.1, 2.6
Reiffen/Scheja/Vetter:	§§ 1–4, §§ 6, 8 teilweise.

Spezielle Hinweise

1.1 Der Abschnitt **1.1** enthält fast nur Definitionen, Beispiele und einfache Resultate, die Ihnen wahrscheinlich schon in Teilen bekannt sind.

1.1.1 – 1.1.6 *Definition der Gruppe, Rechenregeln und einfache Beispiele*

Wenn Sie Aufgabe **1.1.6** ohne Mühe lösen können, brauchen Sie den Text davor nur flüchtig zu lesen, um sich die Bezeichnungen und Symbole zu merken.

1.1.7 – 1.1.12 *Wichtige Beispiele für Gruppen*

Das Beispiel $GL(n, K)$ aus **1.1.7**(1) wird öfter vorkommen, insbesondere in dem Fall, dass K ein endlicher Körper ist. Noch wichtiger ist das Beispiel **1.1.9**, das schon in der Linearen Algebra bei der Definition der Determinante vorkam.

1.1.13 – 1.1.16 *Homomorphismus von Gruppen*

Homomorphismen sind strukturerhaltende Abbildungen zwischen Gruppen und spielen im Kurs eine wichtige Rolle. Sie sollten die Aufgaben in **1.1.16** bearbeiten, da (1) und (2) zum Beweis von **1.1.23** und **1.1.24** benötigt werden.

1.1.17 – 1.1.22 *Untergruppe einer Gruppe*

Das Kriterium **1.1.18** ist wichtig, weil es zum Nachweis einer Untergruppe immer wieder benutzt wird, z. B. auch in **1.1.21**.

1.1.23 – 1.1.25 *Einbettung einer Gruppe in Permutationsgruppen*

Satz 1.1.23 ist ein wichtiges Resultat, dessen Beweis Sie gründlich durcharbeiten sollten. Wie so oft bei einfachen Resultaten besteht die wesentliche Aufgabe darin, ganz präzise zu erkennen, was eigentlich bewiesen werden muß. Der eigentliche Beweis ist dann recht einfach. Die Aufgaben in 1.1.25 sind sehr lehrreich; Sie sollten sich damit beschäftigen.

1.1.26 – 1.1.28 *Konstruktion von Gruppen*

Die Bemerkungen in 1.1.26 sind mehr erläuternder Art, sie sollen Ihnen Hinweise geben, wie Gruppen in natürlicher Weise entstehen. Das Beispiel 1.1.27 – die Dieder-Gruppe D_4 – ist noch einmal wichtig. Diese Gruppe wird Ihnen im Laufe des Kurses (in verschiedenen Zusammenhängen) mehrmals wieder begegnen.

1.2 Der Stoff von 1.2 ist verhältnismäßig einfach.**1.2.1 – 1.2.6** *Ordnung und Index einer Untergruppe*

Der Satz von Lagrange wird oft angewendet werden. Falls Sie die Aussagen in 1.2.6 noch nicht kennen, sollten Sie diese Aufgaben bearbeiten.

1.2.7 – 1.2.13 *Normalteiler, Faktorgruppe*

Die Beispiele in 1.2.9 und die Aufgabe 1.2.10 sollten Sie genau durcharbeiten. Den Begriff der Faktorgruppe nach einem Normalteiler sollten Sie noch aus früheren Kursen kennen.

1.2.14 – 1.2.18 *Homomorphiesatz, Isomorphiesätze*

Diese Sätze sind ein wichtiges Hilfsmittel in vielen Beweisen. Sie sollten sich die Aussagen gut einprägen.

1.3 Die in 1.3 besprochenen zyklischen Gruppen sind wichtige Beispiele abelscher Gruppen, die auch für die noch zu beweisenden Struktursätze über abelsche Gruppen von fundamentaler Bedeutung sind. Die Resultate dieses Abschnittes, insbesondere 1.3.3, werden immer wieder benutzt werden. Auch die mehr technischen Aussagen 1.3.7 und 1.3.8 werden oft benutzt werden. Von der Aufgabe 1.3.10 sollten Sie zumindest den Teil (1) bearbeiten.

1.4, 1.5 Die Abschnitte 1.4 und 1.5 bilden den Kern dieser Kurseinheit. In 1.4 wird eine fundamentale Methode zur Untersuchung endlicher Gruppen besprochen, die dann in 1.5 erstmals angewendet wird. Entsprechend sorgfältig und gründlich sollten Sie diese Abschnitte durcharbeiten.

1.4.1 – 1.4.6 *Operation einer Gruppe auf einer Menge*

Machen Sie sich die vielen eingeführten Begriffe an den Beispielen in 1.4.5 und 1.4.6 klar.

1.4.7 – 1.4.12 *Bahnengleichung*

Besonders wichtig ist die Version der Bahnengleichung (1.4.10) in 1.4.12.

1.4.13 – 1.4.17 *Operation durch Konjugation, Klassengleichung*

Diesen Teil müssen Sie besonders sorgfältig bearbeiten. Sie sollten genau nachvollziehen, wie die Klassengleichung aus der Bahnengleichung in 1.4.12 für die Operation einer Gruppe durch Konjugation auf sich entsteht. Die Klassengleichung 1.4.15 wird in 1.5 und in 2.1 immer wieder benutzt werden. Auch 1.4.16, 1.4.17 werden später in 2.1 benötigt.

1.5 Das zentrale Ergebnis in 1.5 ist der Satz 1.5.3 über das Zentrum einer p -Gruppe. Wenn Sie gerne auf dieses konkrete Resultat hinarbeiten wollen (anstatt die Theorie systematisch zu entwickeln), lesen Sie zuerst die Definition 1.5.1 einer p -Gruppe, dann Satz 1.5.3, und versuchen dann, sich durch den Beweis von 1.5.3 zu arbeiten, indem Sie die dort benutzten Begriffe und Resultate in 1.4 nachlesen.

Die Aufgaben 1.5.4 und 1.5.6 sollten Sie unbedingt bearbeiten. Mittels 1.5.6 können Sie gut überprüfen, ob Sie die Methode dieses Abschnittes beherrschen. Wenn Sie diese Aufgabe lösen können, können Sie sicher sein, dass Sie diesen Abschnitt verstanden haben.

Die Technik der Bahnengleichung wird in 1.5.7 nochmals verwendet; dieses Lemma ist auch für den Abschnitt 2.1 wichtig (Kontroll-Aufgabe: 1.5.8).

1 Grundbegriffe der Gruppentheorie

- 1.1 Definitionen und Beispiele
- 1.2 Normalteiler, Faktorgruppe und Isomorphiesätze
- 1.3 Zyklische Gruppen
- 1.4 Operationen von Gruppen auf Mengen
- 1.5 p -Gruppen

Einige wenige Grundbegriffe der Gruppentheorie sind Ihnen bereits aus dem Kurs „Lineare Algebra“ bekannt. Wir werden diese kurz wiederholen und darauf aufbauend in diesem Kapitel und in den nächsten die Grundlagen der Gruppentheorie darstellen.

1.1 Definitionen und Beispiele

1.1.1 Definition

Eine *Gruppe* ist ein Paar, bestehend aus einer Menge G und einer Abbildung

$$G \times G \rightarrow G, \quad (a, b) \mapsto ab,$$

die *Multiplikation* genannt wird, so dass folgende Axiome erfüllt sind:

- (1) Für alle $a, b, c \in G$ gilt $(ab)c = a(bc)$ (*Assoziativgesetz*).
- (2) Es gibt ein Element $e \in G$, das sogenannte *neutrale Element*, so dass für alle $a \in G$ gilt
 - (i) $ae = ea = a$.
 - (ii) Zu jedem Element $a \in G$ existiert ein Element $b \in G$ mit $ab = ba = e$.

1.1.2 Bemerkungen und Ergänzungen

(1) Um unsere Sprechweise und Bezeichnungen zu vereinfachen, werden wir in Zukunft immer sagen „ G ist eine Gruppe“, ohne dabei die Multiplikation zu erwähnen. In unserer Ausdrucksweise werden wir also keinen Unterschied machen zwischen einer Gruppe und der dieser Gruppe zugrunde liegenden Menge.

(2) In einer Gruppe G gibt es nur ein Element, das die Eigenschaften des neutralen Elements hat. Hat nämlich e' auch die Eigenschaften des neutralen Elements, gilt also $ae' = e'a = a$ für alle $a \in G$, so folgt $e' = e'e = e$.

Das Element e heißt auch *Einselement*.

(3) Zu $a \in G$ ist das Element b mit der Eigenschaft $ab = ba = e$ eindeutig bestimmt. Gilt nämlich auch $ac = e$ für ein $c \in G$, so ist $b = c$, denn es ist $b = be = b(ac) = (ba)c = ec = c$.

(4) Das, wie gerade bewiesen, zu a eindeutig bestimmte Element b mit $ab = ba = e$ heißt das *Inverse* von a und wird mit a^{-1} (lies „ a hoch minus eins“ oder „ a invers“) bezeichnet. Für das Inverse von a gilt also

$$aa^{-1} = a^{-1}a = e,$$

und mit (3) ergibt sich daraus $(a^{-1})^{-1} = a$.

(5) Für alle $a, b \in G$ gilt

$$(ab)^{-1} = b^{-1}a^{-1}.$$

Bei der Bildung des Inversen wird also die Reihenfolge der Faktoren vertauscht! Auf die Beachtung dieser Regel müssen Sie beim Rechnen in Gruppen besonders achten.

Beweis: Aus $(ab)(b^{-1}a^{-1}) = a((bb^{-1})a^{-1}) = a(ea^{-1}) = aa^{-1} = e$ folgt wegen (3) die Behauptung. \square

(6) Durch Induktion nach der Anzahl der Faktoren kann man zeigen, dass ein Produkt von n Faktoren a_1, \dots, a_n einer Gruppe unabhängig davon ist, wie die Klammern gesetzt sind. Zum Beispiel gilt

$$((a_1a_2)a_3)a_4 = (a_1a_2)(a_3a_4) = a_1(a_2(a_3a_4)) = a_1((a_2a_3)a_4) = (a_1(a_2a_3))a_4.$$

Wegen dieser – intuitiv ziemlich offensichtlichen – Tatsache lässt man die Klammern soweit wie möglich weg und benutzt sie meistens nur, um den Gang einer Rechnung deutlich zu machen.

(7) Für wiederholte Produkte desselben Gruppenelements benutzt man die Potenzschreibweise. Für $n \in \mathbb{N}$ definiert man also

$$a^n := a \cdot \dots \cdot a \quad (n \text{ Faktoren } a).$$

Diese Definition dehnt man auf alle ganzen Zahlen n aus, indem man definiert

$$a^0 := e, \quad a^{-n} := (a^{-1})^n \text{ für } n \in \mathbb{N}.$$

Es ist also $a^2 = aa$, $a^3 = aaa$, $a^{-2} = a^{-1}a^{-1} = (a^2)^{-1}$, usw. Es gelten dann für alle ganze Zahlen m, n die folgenden – von Potenzen her gewohnten – Rechenregeln

$$a^{m+n} = a^m a^n, \quad (a^m)^n = a^{mn}, \quad \text{und } (a^m)^{-1} = (a^{-1})^m.$$

Allerdings gilt die Rechenregel $(ab)^n = a^n b^n$ im Allgemeinen *nicht*. Sie ist aber gültig, falls a und b vertauschen, d.h., wenn $ab = ba$ gilt.

1.1.3 Definition

Eine Gruppe G heißt *kommutativ* oder *abelsch* (nach dem norwegischen Mathematiker NIELS HENRIK ABEL, 1802–1829), falls für alle $a, b \in G$ gilt

$$ab = ba \quad (\text{Kommutativgesetz}).$$

1.1.4 Bemerkungen und Ergänzungen

(1) Durch Induktion nach der Anzahl der Faktoren beweist man, dass ein Produkt von n Faktoren a_1, \dots, a_n in einer abelschen Gruppe unabhängig von der Reihenfolge der Faktoren ist. Zum Beispiel gilt

$$abc = acb = cab = cba = bca = bac.$$

(2) In abelschen Gruppen verwendet man oft die *additive Schreibweise*: Statt des Produktes ab schreibt man also $a+b$, und für diese Summenbildung gelten die entsprechenden Axiome. Das neutrale Element wird mit 0 bezeichnet und das Inverse zu a mit $-a$. Statt $a + (-b)$ schreibt man der Einfachheit halber $a - b$. Die Potenzschreibweise wird durch eine multiplikative Schreibweise ersetzt: Für jede natürliche Zahl n sei

$$\begin{aligned} na &= a + \dots + a \quad (n \text{ Summanden } a), \\ (-n)a &= -(a + \dots + a), \quad 0a = 0. \end{aligned}$$

Für beliebige $a, b \in G$ und $m, n \in \mathbb{Z}$ gelten dann die folgenden Formeln

$$\begin{aligned} n(a + b) &= na + nb, \\ (n + m)a &= na + ma, \\ n(ma) &= (nm)a, \\ 1a &= a. \end{aligned}$$

Diese Formeln sollten Sie an die Definition eines Vektorraumes über einem Körper erinnern. Denkt man sich m, n aus dem Körper und a, b aus dem Vektorraum, so benutzt man genau diese Formeln in der axiomatischen Definition des Vektorraumes. Lässt man in den Vektorraum-Axiomen Skalare aus einem Ring (anstelle eines Körpers) zu, dann gelangt man zum Begriff des Moduls. Die obigen Formeln besagen also, dass abelsche Gruppen immer Moduln über dem Ring \mathbb{Z} der ganzen Zahlen sind.

(3) Bei der Betrachtung von Beispielen wird die „Verknüpfung“ in der Gruppe oft natürlich noch mit anderen Symbolen bezeichnet, z. B. mit \cdot oder \circ . Ebenso wird das neutrale Element oft anders als mit e bezeichnet.

1.1.5 Einfache Beispiele

(1) Die Menge der ganzen Zahlen \mathbb{Z} bildet bezüglich der Addition eine abelsche

Gruppe. Das gleiche gilt für die Mengen $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ der rationalen, reellen und komplexen Zahlen. Allgemeiner liegt jedem Ring, Körper oder Vektorraum eine abelsche Gruppe bezüglich der Addition zugrunde.

(2) Die von 0 verschiedenen rationalen, reellen oder komplexen Zahlen bilden jeweils eine abelsche Gruppe bezüglich der Multiplikation. Allgemeiner ist für einen Körper K die Menge K^* der von 0 verschiedenen Elemente eine abelsche Gruppe bezüglich der Multiplikation.

1.1.6 Aufgabe

Welche der folgenden Mengen sind mit der jeweils angegebenen Verknüpfung eine Gruppe? Welche Gruppenaxiome sind erfüllt bzw. verletzt?

- (1) \mathbb{N} mit der Addition,
- (2) \mathbb{N} mit der Multiplikation,
- (3) $\mathbb{N}^0 = \{0, 1, 2, \dots\}$ mit der Addition,
- (4) \mathbb{N}^0 mit der Multiplikation,
- (5) $\mathbb{R}_+ = \{x \in \mathbb{R} \mid x > 0\}$ mit der Multiplikation,
- (6) \mathbb{Z} mit der Multiplikation,
- (7) $\{1, -1\}$ mit der Multiplikation,
- L** (8) $S := \{z \in \mathbb{C} \mid |z| = 1\}$ mit der Multiplikation.

1.1.7 Wichtige Beispiele

Es sei K ein Körper. Mit $M(n, K)$ bezeichnen wir die Menge der $n \times n$ -Matrizen mit Koeffizienten aus K . Aus der Linearen Algebra kennen Sie die folgenden Gruppen, bei denen das Produkt jeweils das Matrizenprodukt ist.

(1) $GL(n, K) := \{A \mid A \in M(n, K), A \text{ invertierbar}\}$. Diese Gruppe heißt *allgemeine lineare Gruppe* über K . Statt A invertierbar könnten wir auch $\det(A) \neq 0$ verlangen.

(2) $SL(n, K) := \{A \mid A \in M(n, K), \det(A) = 1\}$. Diese Gruppe heißt *spezielle lineare Gruppe*.

(3) $O(n, K) := \{A \mid A \in M(n, K), AA^t = E\}$. Hierbei ist mit A^t die transponierte Matrix zu A bezeichnet, und E ist die Einheitsmatrix. Diese Gruppe heißt *orthogonale Gruppe*.

(4) $SO(n, K) := \{A \mid A \in O(n, K), \det(A) = 1\}$. Diese Gruppe heißt *spezielle orthogonale Gruppe*.

1.1.8 Bemerkungen

In der linearen Algebra wird gezeigt, dass Matrizen lineare Abbildungen zwischen Vektorräumen beschreiben: Entsprechend hat man für einen endlich-dimensionalen K -Vektorraum V dann die folgenden Gruppen

$$GL(V) := \{\alpha \mid \alpha : V \rightarrow V \text{ linear und invertierbar}\}$$

(allgemeine lineare Gruppe von V),

$$SL(V) := \{\alpha \mid \alpha : V \rightarrow V \text{ linear und } \det(\alpha) = 1\}$$

(spezielle lineare Gruppe von V).

Der orthogonalen Gruppe entspricht die Gruppe der Isometrien bezüglich einer symmetrischen Bilinearform.

1.1.9 Besonders wichtiges Beispiel

(1) Es sei M eine nichtleere Menge. Es sei

$$S(M) := \{\alpha : M \rightarrow M \mid \alpha \text{ bijektiv}\}.$$

Dann ist $S(M)$ bezüglich der Verknüpfung von Abbildungen eine Gruppe. Das neutrale Element ist die identische Abbildung $\text{id} = \text{id}_M$. Das Inverse von $\alpha \in S(M)$ ist die Umkehrabbildung α^{-1} , die existiert, weil α bijektiv ist. $S(M)$ heißt die *Permutations-Gruppe* oder *symmetrische Gruppe* von M .

(2) Ist insbesondere $M = \{1, 2, \dots, n\}$, $n \in \mathbb{N}$, so schreiben wir S_n statt $S(\{1, \dots, n\})$. Die Gruppe S_n heißt *symmetrische Gruppe* (in n Ziffern). Die Elemente von S_n nennt man *Permutationen*. Will man ein Element α von S_n explizit angeben, so geschieht das oft in Form des folgenden Schemas

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

Unter der Ziffer i steht also die i zugeordnete Ziffer $\alpha(i)$. Auf die obere Zeile verzichtet man oft auch und schreibt die Permutation α einfach als

$$(\alpha(1), \alpha(2), \dots, \alpha(n))_{\curvearrowright}.$$

1.1.10 Aufgabe

L Zeigen Sie (durch Induktion nach n), dass S_n genau $n!$ Elemente enthält.

1.1.11 Ergänzungen

Eine *Transposition* ist eine Permutation aus S_n , $n \geq 2$, die zwei verschiedene Ziffern miteinander vertauscht und alle anderen Ziffern festlässt.

Aus der Linearen Algebra sind Ihnen folgende Tatsachen bekannt (die wir später auch noch einmal beweisen werden):

(1) *Jede Permutation aus S_n , $n \geq 2$, ist ein Produkt von Transpositionen.*

(2) *Die Anzahl der Transpositionen in einer beliebigen Produktdarstellung einer Permutation ist unabhängig von der Darstellung entweder gerade oder ungerade.* Entsprechend heißt eine Permutation *gerade* oder *ungerade*. Eine Permutation σ ist genau dann gerade, wenn die Signatur $\text{sgn}(\sigma) = 1$ erfüllt.

Transpositionen selbst sind natürlich ungerade Permutationen.

1.1.12 Aufgaben

(1) Berechnen Sie die Produkte folgender Permutationen

$$\begin{aligned} (2, 1, 3, 5, 4)_{\curvearrowright} \quad \text{und} \quad (5, 3, 4, 1, 2)_{\curvearrowright}, \\ (1, 4, 6, 3, 5, 2)_{\curvearrowright} \quad \text{und} \quad (4, 3, 1, 2, 6, 5)_{\curvearrowright}. \end{aligned}$$

(2) Welche der folgenden Permutationen sind gerade, welche ungerade?

$$(2, 1, 7, 6, 3, 4, 5)_{\curvearrowright},$$

$$(4, 3, 6, 1, 2, 5)_{\curvearrowright},$$

$$(n, n-1, \dots, 2, 1)_{\curvearrowright}, \quad n \geq 2,$$

L
$$(2, 4, 6, \dots, 2n, 1, 3, 5, \dots, 2n-1)_{\curvearrowright}.$$

1.1.13 Definition

Es seien G, G' zwei Gruppen. Eine Abbildung $f : G \rightarrow G'$ heißt *Homomorphismus* (oder *Gruppenhomomorphismus*), falls für alle $a, b \in G$ gilt

$$f(ab) = f(a)f(b).$$

Ist f bijektiv, so heißt f *Isomorphismus*. Ist $G = G'$ und f bijektiv, so heißt f *Automorphismus* von G .

1.1.14 Beispiel

Aus der linearen Algebra ist Ihnen folgender Homomorphismus bekannt

$$\det : GL(n, K) \rightarrow K^*,$$

wobei K^* die multiplikative Gruppe des Körpers K bezeichnet.

1.1.15 Bemerkungen und Ergänzungen

(1) Ist $f : G \rightarrow G'$ ein Homomorphismus von Gruppen G und G' , e das neutrale Element von G und e' das von G' , so gilt

- a) $f(e) = e'$,
- b) $f(a^{-1}) = f(a)^{-1}$ für alle $a \in G$.

Beweis: Aus $f(e) = f(ee) = f(e)f(e)$ folgt a) nach Multiplikation mit $f(e)^{-1}$. Die Aussage b) ergibt sich aus $e' = f(e) = f(aa^{-1}) = f(a)f(a^{-1})$. \square

(2) Den *Kern* eines Homomorphismus $f : G \rightarrow G'$ definiert man durch

$$\text{Kern}(f) := \{a \in G \mid f(a) = e'\}.$$

Dann gilt: f ist injektiv $\iff \text{Kern}(f) = \{e\}$.

Beweis:

„ \Rightarrow “: Ist f injektiv und $a \in \text{Kern}(f)$, also $f(a) = e' = f(e)$, so folgt $a = e$. Weil das neutrale Element e selbst nach (1) immer zu $\text{Kern}(f)$ gehört, gilt dann $\text{Kern}(f) = \{e\}$.

„ \Leftarrow “: Sei umgekehrt $\text{Kern}(f) = \{e\}$ und $f(a) = f(b)$ für $a, b \in G$. Dann gilt $f(ab^{-1}) = f(a)f(b^{-1}) = f(a)f(b)^{-1} = e'$, also $ab^{-1} \in \text{Kern}(f) = \{e\}$ und damit $ab^{-1} = e$, also $a = b$. Daher ist f injektiv. \square

(3) Sind $f : G \rightarrow G'$ und $f' : G' \rightarrow G''$ Homomorphismen, so ist auch $f' \circ f : G \rightarrow G''$ ein Homomorphismus. Sind f und f' beide Isomorphismen, so ist auch $f' \circ f$ ein Isomorphismus.

(4) Ist $f : G \rightarrow G'$ ein Isomorphismus, also ein bijektiver Homomorphismus, so ist die Umkehrabbildung $f^{-1} : G' \rightarrow G$ ein Homomorphismus, also auch ein Isomorphismus. Offenbar ist die identische Abbildung $\text{id}_G : G \rightarrow G$ einer Gruppe G immer ein Automorphismus von G .

(5) Zwei Gruppen G und G' heißen *isomorph*, in Zeichen $G \cong G'$, falls ein Isomorphismus $f : G \rightarrow G'$ existiert. Nach (3) und (4) ist Isomorphie eine Äquivalenzrelation. Isomorphe Gruppen sind vom Standpunkt der Gruppentheorie ununterscheidbar: Alle Eigenschaften, die die eine Gruppe hat, hat auch die andere.

(6) Die Menge $\text{Aut}(G)$ der Automorphismen von G ist wegen (3) und (4) bezüglich der Komposition \circ eine Gruppe mit dem neutralen Element id_G . $\text{Aut}(G)$ heißt *Automorphismen-Gruppe* von G .

(7) Für alle $g \in G$ ist die Abbildung

$$i_g : G \rightarrow G, i_g(x) := gxg^{-1} \text{ für alle } x \in G$$

ein Automorphismus, i_g heißt der durch g definierte *innere Automorphismus* von G .

Beweis: Wegen $i_g(xy) = gxyg^{-1} = gxg^{-1}gyg^{-1} = i_g(x)i_g(y)$ ist i_g ein Homomorphismus. Man rechnet leicht $i_g \circ i_{g^{-1}} = i_{g^{-1}} \circ i_g = \text{id}_G$ nach und erhält damit, dass i_g ein Automorphismus von G ist. \square

1.1.16 Aufgaben

(1) Sei G eine Gruppe. Zeigen Sie:

a) Für $a \in G$ ist die Abbildung

$$L(a) : G \rightarrow G, L(a)(x) := ax \text{ für alle } x \in G$$

bijektiv, also ein Element von $S(G)$. $L(a)$ heißt *Linksmultiplikation* mit a .

b) Für $a \neq e$ ist $L(a)$ kein Homomorphismus.

c) Die Abbildung

$$L : G \rightarrow S(G), a \mapsto L(a)$$

ist ein Homomorphismus.

(2) Sei $\varphi : M \rightarrow M'$ eine bijektive Abbildung zwischen Mengen M und M' . Zeigen Sie:

a) Für $\alpha \in S(M)$ liegt $\varphi \circ \alpha \circ \varphi^{-1}$ in $S(M')$.

b) Die Abbildung

$$f : S(M) \rightarrow S(M'), f(\alpha) := \varphi \circ \alpha \circ \varphi^{-1} \text{ für alle } \alpha \in S(M)$$

ist ein Isomorphismus.

(3) Die Abbildung

$$i : G \rightarrow \text{Aut}(G), g \mapsto i_g \text{ mit } i_g(x) = gxg^{-1}$$

L ist ein Homomorphismus.

1.1.17 Definition

Eine nichtleere Teilmenge H einer Gruppe G heißt eine *Untergruppe* von G , wenn H unter der Multiplikation von G abgeschlossen ist (d. h. für alle $a, b \in H$ ist auch $ab \in H$) und mit dieser Multiplikation selbst eine Gruppe ist.

Das folgende Lemma liefert eine nützliches Kriterium, um festzustellen, wann eine Teilmenge einer Gruppe eine Untergruppe ist.

1.1.18 Lemma

Eine nichtleere Teilmenge H einer Gruppe G ist genau dann eine Untergruppe von G , wenn folgende Bedingungen gelten:

- (1) Für alle $a, b \in H$ ist $ab \in H$.
- (2) Für alle $a \in H$ ist $a^{-1} \in H$.

Beweis:

Ist H eine Untergruppe von G , so ist $e_{HeG} = e_H = e_{HeH}$, also $e_G = e_H$, für das Inverse $a' \in H$ von $a \in H$ folgt dann $a' = a^{-1}$, also ist $a^{-1} \in H$.

Gelten umgekehrt (1) und (2) für eine nichtleere Teilmenge H von G , so ist H nach (1) abgeschlossen unter der Multiplikation von G , und es gilt das Assoziativgesetz, weil H eine Teilmenge von G ist. Wegen $H \neq \emptyset$ existiert ein Element a in H . Nach (2) ist auch $a^{-1} \in H$, und mit (1) folgt $e = aa^{-1} \in H$, also enthält H das neutrale Element. Nach (2) gibt es zu jedem Element in H ein Inverses. Damit ist H eine Untergruppe von G . \square

1.1.19 Einfache Beispiele

- (1) In jeder Gruppe G sind $\{e\}$ und G Untergruppen von G , die sogenannten *trivialen* Untergruppen von G .
- (2) Es sind $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ jeweils Untergruppen von \mathbb{C} bezüglich der Addition.
- (3) Für jedes $n \in \mathbb{Z}$ ist $n\mathbb{Z} := \{nm \mid m \in \mathbb{Z}\}$ eine Untergruppe von \mathbb{Z} .

1.1.20 Aufgabe

Sei H eine nichtleere *endliche* Teilmenge einer Gruppe G . Zeigen Sie (mit Hilfe der Linksmultiplikationen):

L H ist Untergruppe von $G \iff$ Für alle $a, b \in H$ ist $ab \in H$.

1.1.21 Sätze über Untergruppen

(1) Es sei $f : G \rightarrow G'$ ein Homomorphismus von Gruppen G und G' . Dann gilt:

a) Für eine Untergruppe H von G ist das Bild $f(H)$ eine Untergruppe von G' , insbesondere ist $\text{Bild}(f) = f(G)$ eine Untergruppe von G' .

b) Für eine Untergruppe H' von G' ist das Urbild $f^{-1}(H')$ eine Untergruppe von G , insbesondere ist $\text{Kern}(f) = f^{-1}(\{e'\})$ eine Untergruppe von G .

(2) Der Durchschnitt von beliebig vielen Untergruppen einer Gruppe ist eine Untergruppe.

Beweis:

Für alle Aussagen benutzen wir das Kriterium 1.1.18.

(1) In a) ist $f(H)$ offenbar eine nichtleere Teilmenge von G' , weil H nichtleer ist. Zu $a', b' \in f(H)$ gibt es $a, b \in H$ mit $a' = f(a)$ und $b' = f(b)$. Dann folgt

$$\begin{aligned} a'b' &= f(a)f(b) = f(ab) \in f(H) \quad \text{und} \\ (a')^{-1} &= f(a)^{-1} = f(a^{-1}) \in f(H), \end{aligned}$$

weil ab und a^{-1} in der Untergruppe H liegen. Nach 1.1.18 ist dann $f(H)$ eine Untergruppe von G' .

b) wird ebenfalls mit 1.1.18 bewiesen. Es ist eine hilfreiche Übung, diesen Beweis selbst auszuführen!

(2) Es sei $(H_i)_{i \in I}$ eine nichtleere Familie von Untergruppen einer Gruppe G . Da jede Untergruppe H_i das neutrale Element e von G enthält (Warum?), ist $\bigcap_{i \in I} H_i$ nichtleer. Sind $a, b \in \bigcap_{i \in I} H_i$, also $a, b \in H_i$ für alle $i \in I$, so sind $ab, a^{-1} \in H_i$ für alle $i \in I$, also $ab, a^{-1} \in \bigcap_{i \in I} H_i$. Mit 1.1.18 folgt nun die Behauptung. \square

Die Vereinigung von Untergruppen ist dagegen im allgemeinen keine Untergruppe:

1.1.22 Aufgabe

Zeigen Sie für Untergruppen H und H' einer Gruppe G : $H \cup H'$ ist genau dann eine Untergruppe von G , wenn $H \subset H'$ oder $H' \subset H$ gilt.

Wir beweisen jetzt einen wichtigen Satz, in dem mit den eingeführten Begriffen gearbeitet wird.

1.1.23 Satz

Es sei G eine beliebige Gruppe. Dann ist G isomorph zu einer Untergruppe der Permutations-Gruppe $S(G)$.

Beweis:

Wir haben schon in 1.1.16 gesehen, dass die Abbildung

$$L : G \rightarrow S(G) \text{ mit } L(a)(x) = ax \text{ für alle } a, x \in G$$

ein Homomorphismus ist, also ist $L(G)$ nach 1.1.21 eine Untergruppe von $S(G)$. Wir behaupten, dass $L : G \rightarrow S(G)$ injektiv ist, also $L : G \rightarrow L(G)$ ein Isomorphismus ist. Sei $a \in \text{Kern}(L)$, also $L(a) = \text{id}_G$. Dann gilt insbesondere $ae = L(a)(e) = e$, also $a = e$. Damit folgt $\text{Kern}(L) = \{e\}$, und nach 1.1.15(2) ist L dann injektiv. Damit ist G isomorph zur Untergruppe $L(G)$ von $S(G)$, und es ist alles bewiesen. \square

1.1.24 Korollar

Ist G eine endliche Gruppe mit n Elementen, so ist G isomorph zu einer Untergruppe von S_n .

Beweis:

Wir haben den injektiven Homomorphismus $L : G \rightarrow S(G)$. Hat G nun n Elemente, so können wir eine bijektive Abbildung $\varphi : G \rightarrow \{1, \dots, n\}$ wählen und erhalten nach 1.1.16(2) einen Isomorphismus $f : S(G) \rightarrow S_n$. Damit ist

$$G \xrightarrow{L} S(G) \xrightarrow{f} S_n$$

ein injektiver Gruppenhomomorphismus, also ist G isomorph zum Bild dieses Homomorphismus in S_n . \square

1.1.25 Aufgaben

(1) Sei K ein Körper und $n \in \mathbb{N}$. Zeigen Sie:

Man erhält einen injektiven Homomorphismus $GL(n, K) \rightarrow S(K^n \setminus \{0\})$ durch $A \mapsto \hat{A}$ mit $\hat{A}(x) := Ax$ für alle $A \in GL(n, K)$ und $x \in K^n$, $x \neq 0$.

(2) Es sei \mathbb{F}_2 der Körper mit zwei Elementen. Bestimmen Sie alle Elemente von $GL(2, \mathbb{F}_2)$. Beweisen Sie, dass $GL(2, \mathbb{F}_2)$ und S_3 zueinander isomorph sind.

(3) Es sei \mathbb{F}_3 der Körper mit drei Elementen, die mit $0, 1, 2$ bezeichnet werden (also $1 + 2 = 0$, $2 + 2 = 1$, $2^{-1} = 2$, usw.).

Wieviele Elemente hat $GL(2, \mathbb{F}_3)$? Zeigen Sie, dass $GL(2, \mathbb{F}_3)$ isomorph zu

L einer Untergruppe von S_8 ist.

1.1.26 Bemerkungen

Die wichtigsten und interessantesten Beispiele von Gruppen sind immer Gruppen von bijektiven Abbildungen einer Menge M in sich. Je nachdem, welche zusätzliche Struktur auf der Menge M gegeben ist, stellt man noch weitere Forderungen an die betrachteten Abbildungen. Unter diesem Gesichtspunkt behandeln wir noch einmal die bisher erwähnten Beispiele.

(1) Haben wir einfach eine Menge M (ohne jede weitere Struktur), so können wir an die Bijektionen $\alpha : M \rightarrow M$ keine weiteren Bedingungen stellen. Wir erhalten die symmetrische Gruppe $S(M)$.

(2) Es sei jetzt M ein Vektorraum über einem Körper K . Die Abbildungen $\alpha : M \rightarrow M$, die die Vektorraumstruktur von M „erhalten“, sind gerade die K -linearen Abbildungen. Wir erhalten die Gruppe der K -Automorphismen von M , die wir mit $GL(M)$ bezeichnet hatten.

(3) Es sei jetzt M ein euklidischer Raum über dem Körper der reellen Zahlen. Außer der Vektorraumstruktur auf M hat man also auch eine „geometrische“ Struktur, nämlich das Skalarprodukt $\langle \cdot, \cdot \rangle : M \times M \rightarrow \mathbb{R}$. Dann betrachten wir Abbildungen $\alpha : M \rightarrow M$, die sowohl linear sind als auch das Skalarprodukt erhalten, also $\langle \alpha(x), \alpha(y) \rangle = \langle x, y \rangle$ für alle $x, y \in M$ erfüllen. Diese Abbildungen, die in der Linearen Algebra *orthogonale* Abbildungen genannt wurden, nennt man auch *Isometrien*. Die Menge aller Isometrien bildet ebenfalls

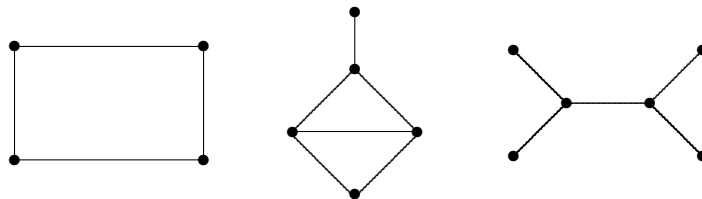
eine Gruppe $O(M)$: die *orthogonale Gruppe* von M (oder Automorphismen-Gruppe von M). Zu der orthogonalen Gruppe gehören insbesondere Drehungen und Spiegelungen.

(4) Ist M eine Gruppe, so können wir die Gruppe der bijektiven Gruppenhomomorphismen betrachten. Hier lassen wir also nur solche Abbildungen zu, die die Gruppenstruktur in M erhalten. Dies liefert die Automorphismen-Gruppe $\text{Aut}(M)$ von M .


(5) Wir wollen dasselbe Prinzip jetzt an einer ganz anderen Situation erläutern. Wir betrachten einen Graphen, der aus endlich vielen Punkten besteht, die durch Kanten verbunden sind. Dabei sollen zwei Punkte höchstens durch eine Kante verbunden sein, und keine Kante soll einen Punkt mit sich selbst verbinden. Folgendes ist also *verboten*:



Graphen sehen also z. B. so aus:



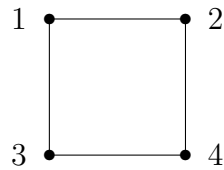
Auf die spezielle geometrische Gestalt kommt es nicht an, nur auf die Zahl der Punkte und ob sie jeweils verbunden sind oder nicht. Auf eine formale Definition verzichten wir.

Unter einem *Automorphismus eines Graphen* versteht man dann eine bijektive Abbildung der Menge der Punkte auf sich, die verbundene Punkte in verbundene überführt. Sind z. B. in dem Graphen alle Punkte miteinander verbunden – wie in  –, so ist diese Bedingung bei jeder bijektiven Abbildung erfüllt, und wir erhalten die volle symmetrische Gruppe der Menge der Punkte des Graphen.

1.1.27 Beispiel

Als Beispiel wollen wir  betrachten. Wir numerieren die Punkte folgen-

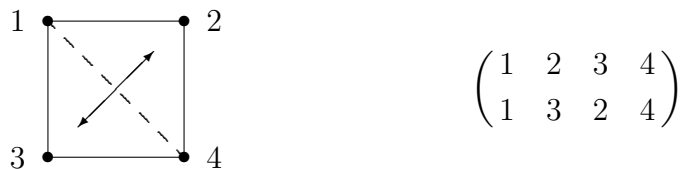
dermaßen



und beschreiben dann jeden Automorphismus durch die zugehörige Permutation. Wir erhalten folgende Automorphismen:

a) Die Identität.

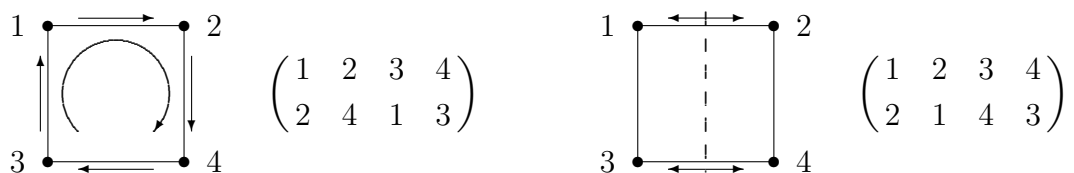
b) Es werde 1 festgelassen. Dann müssen 2 und 3 vertauscht werden (andernfalls erhalten wir wieder die Identität), und 4 wird automatisch festgelassen. Dies ergibt also:



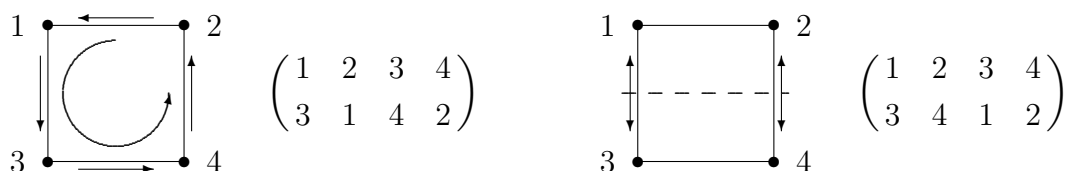
c) Wird 2 festgelassen, haben wir analog



d) Wird 1 auf 2 abgebildet, so wird notwendig 2 auf 1 oder 4 abgebildet, und wir haben folgende Möglichkeiten



e) Wird 1 auf 3 abgebildet, so haben wir analog (wie eben) die beiden Möglichkeiten



f) Wird 1 auf 4 abgebildet und bleibt 2 nicht wie in c) fest, so ergibt sich



Weitere Möglichkeiten gibt es nicht.

Wir stellen also fest, dass die betrachtete Gruppe genau 8 Elemente hat. Es sei σ der unter d) durch $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$ beschriebene Automorphismus und τ der unter b) beschriebene. Dann gelten folgende Gleichungen

$$\sigma^4 = \text{id}, \quad \tau^2 = \text{id}, \quad \tau\sigma\tau = \sigma^3.$$

Die Gruppe besteht aus folgenden Elementen

$$\text{id}, \sigma, \sigma^2, \sigma^3, \tau, \tau\sigma, \tau\sigma^2, \tau\sigma^3.$$

Aus naheliegenden geometrischen Gründen heißt diese Gruppe auch die Automorphismen-Gruppe des Quadrates. Man nennt sie – und jede zu ihr isomorphe Gruppe – auch die *Dieder-Gruppe* (man spricht „Di-eder“) der Ordnung 8 und bezeichnet sie mit D_4 , da sie aus Automorphismen eines Graphen mit 4 Punkten besteht.

Die Dieder-Gruppe ist eine wichtige endliche Gruppe, die uns noch oft begegnen wird. Sie sollten sich mit der Struktur dieser Gruppe vertraut machen, z. B. indem Sie einige Gleichungen berechnen, wie

$$\sigma^2\tau\sigma\tau\sigma^3 = ?, \quad \sigma\tau\sigma\tau\sigma^2\tau = ?.$$

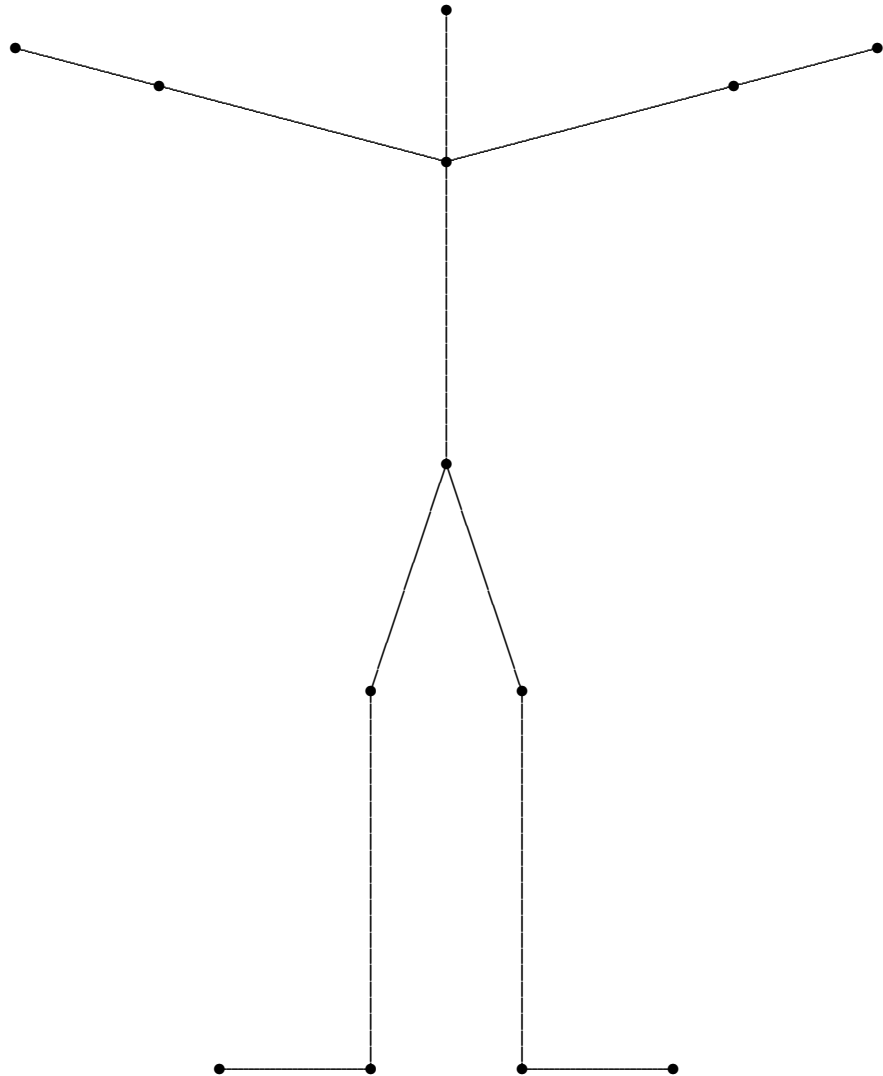
(Benutzen Sie die obigen Gleichungen).

1.1.28 Aufgaben

(1) Diskutieren Sie die Automorphismen-Gruppe von  .

Bestimmen Sie insbesondere die Anzahl ihrer Elemente.

L (2) Bestimmen Sie alle Automorphismen von



1.2 Normalteiler, Faktorgruppe und Isomorphiesätze

In diesem Abschnitt führen wir grundlegende Begriffe ein und besprechen einige wichtige (aber relativ einfache) Tatsachen, auf die wir im Laufe des Kurses häufig zurückgreifen werden. Einige Konzepte sind Ihnen vielleicht schon im Kurs „Lineare Algebra“ begegnet.

Ist M eine Menge, so bezeichne $|M|$ die Anzahl der Elemente von M . Es ist $|M|$ eine nicht-negative ganze Zahl oder ∞ , unendliche Mengen werden in diesem Kurs also nicht nach ihrer Mächtigkeit unterschieden. Es sei $n \cdot \infty = \infty$ für $n \geq 1$ und $\infty \cdot \infty = \infty$, das Produkt $0 \cdot \infty$ ist nicht definiert.

Für eine Gruppe G heißt $|G|$ die *Ordnung* von G .

1.2.1 Definition

Es sei G eine Gruppe und H eine Untergruppe. Die Teilmengen

$$aH := \{ah \mid h \in H\}, \quad a \in G,$$

$$Ha := \{ha \mid h \in H\}, \quad a \in G$$

heißen *Linksnebenklassen* bzw. *Rechtsnebenklassen* von H in G .

1.2.2 Einige Eigenschaften

(1) *Alle Links- bzw. Rechtsnebenklassen von H enthalten gleich viele Elemente, nämlich so viele wie H .*

Beweis: Für $a \in G$ ist $H \rightarrow aH$, $h \mapsto ah$ eine bijektive Abbildung (nach 1.1.16(1)). Daraus folgt $|H| = |aH|$ und ebenso $|H| = |Ha|$. \square

(2) *Für $a, b \in G$ gilt: $aH = bH \iff aH \cap bH \neq \emptyset \iff a^{-1}b \in H$.*

Insbesondere sind zwei Linksnebenklassen entweder gleich oder disjunkt.

Analoges gilt für Rechtsnebenklassen.

Beweis: Aus $aH = bH \neq \emptyset$ folgt natürlich $aH \cap bH \neq \emptyset$. Existiert ein $g \in aH \cap bH$, also $g = ah_1 = bh_2$ mit $h_1, h_2 \in H$, so ist $a^{-1}b = h_1h_2^{-1} \in H$. Ist umgekehrt $a^{-1}b = h \in H$, so gilt $bH = ahH = aH$, denn für $h \in H$ ist $hH = \{hh' \mid h' \in H\} = H$. \square

(3) Die Gruppe G ist Vereinigung der Links- bzw. Rechtsnebenklassen, nach (2) also disjunkte Vereinigung der verschiedenen Links- oder Rechtsnebenklassen von H .

(4) Die Anzahl der verschiedenen Linksnebenklassen aH von H ist gleich der Anzahl der verschiedenen Rechtsnebenklassen Ha .

Beweis: Wir zeigen, dass durch $aH \mapsto Ha^{-1}$ eine bijektive Abbildung von der Menge der Linksnebenklassen auf die Menge der Rechtsnebenklassen von H gegeben wird. Für $a, b \in G$ gilt nach (2):

$$aH = bH \iff a^{-1}b \in H \iff Ha^{-1}b = H \iff Ha^{-1} = Hb^{-1}.$$

Nun zeigt „ \Rightarrow “, dass die Abbildung $aH \mapsto Ha^{-1}$ wohldefiniert ist, und „ \Leftarrow “ liefert die Injektivität der Abbildung. Wegen $Ha = H(a^{-1})^{-1}$ für $a \in G$ ist die Abbildung auch surjektiv. \square

1.2.3 Definition

Die Anzahl der verschiedenen Linksnebenklassen von H in G , die nach (4) mit der Anzahl der verschiedenen Rechtsnebenklassen übereinstimmt, heißt *Index* von H in G und wird mit $[G : H]$ bezeichnet.

Weil nach (3) die Gruppe G disjunkte Vereinigung der verschiedenen Linksnebenklassen von H ist, die alle jeweils $|H|$ Elemente haben, ergibt sich sofort der folgende Satz des französischen Mathematikers Joseph Louis de LAGRANGE (1736–1813):

1.2.4 Satz von Lagrange

Ist H eine Untergruppe einer Gruppe G , so gilt

$$|G| = [G : H] \cdot |H|.$$

Insbesondere sind bei endlichen Gruppen Ordnung und Index einer Untergruppe immer Teiler der Gruppenordnung. \square

Wir wenden diese Tatsache auf einen Spezialfall an:

1.2.5 Definition

Für ein $a \in G$ ist

$$\langle a \rangle := \{a^n \mid n \in \mathbb{Z}\}$$

offensichtlich eine Untergruppe von G , sie heißt die *von a erzeugte Untergruppe*. Ihre Ordnung heißt *Ordnung* $\text{ord}(a)$ von a , also

$$\text{ord}(a) := |\langle a \rangle|.$$

Nach dem Satz von Lagrange ist dann die Ordnung jedes Gruppenelementes ein Teiler der Gruppenordnung.

1.2.6 Aufgabe

Sei a ein Element einer Gruppe G . Zeigen Sie:

(1) Die Ordnung von a ist entweder ∞ oder gleich der kleinsten Zahl $n \in \mathbb{N}$ mit $a^n = e$. Im zweiten Fall ist $\langle a \rangle = \{e, a, \dots, a^{n-1}\}$.

(2) Hat a endliche Ordnung, so gilt für $k \in \mathbb{Z}$:

$$a^k = e \iff \text{ord}(a) \text{ teilt } k.$$

(3) Ist G endlich, so gilt $a^{|G|} = e$ für alle $a \in G$. Diese Aussage heißt auch „Kleiner FERMATScher Satz“ (nach dem französischen Mathematiker Pierre FERMAT (1601–1665)).

(4) Sind H und K endliche Untergruppen von G mit teilerfremden Ordnungen, so gilt $H \cap K = \{e\}$.

L

1.2.7 Definition

Eine Untergruppe H einer Gruppe G heißt *Normalteiler* (oder *normale Untergruppe*) von G , falls Links- und Rechtsnebenklassen von H übereinstimmen, also

$$aH = Ha \text{ für alle } a \in G \text{ gilt.}$$

Man hat die folgenden äquivalenten Charakterisierungen:

- (1) H ist Normalteiler von G ,
- (2) $aHa^{-1} = H$ für alle $a \in G$, wobei $aHa^{-1} := \{aha^{-1} \mid h \in H\}$,
- (3) $aha^{-1} \in H$ für alle $a \in G$, $h \in H$.

Beweis: (1) \Leftrightarrow (2) und (2) \Rightarrow (3) sind klar. Aus (3) folgt zunächst $aHa^{-1} \subset H$ für alle $a \in G$. Ersetzt man hier a durch a^{-1} , so folgt $a^{-1}Ha \subset H$, also $H \subset aHa^{-1}$ und damit $aHa^{-1} = H$. \square

Zum praktischen Nachweis eines Normalteilers benutzt man die Bedingung (3), die häufig auch zur Definition von „Normalteiler“ verwendet wird.

Triviale Beispiele für Normalteiler sind die Untergruppen $\{e\}$ und G . Interessantere Beispiele ergeben sich aus Folgendem:

1.2.8 Sätze über Normalteiler

(1) *Jede Untergruppe einer abelschen Gruppe ist ein Normalteiler.*

Beweis: Das ist offensichtlich, denn in einer abelschen Gruppe ist $aha^{-1} = h$. Die Bedingung $aha^{-1} \in H$ für $h \in H$ ist also trivialerweise erfüllt. \square

(2) *Der Durchschnitt von beliebig vielen Normalteilern ist wieder ein Normalteiler.*

(3) *Es sei $f : G \rightarrow G'$ ein Gruppenhomomorphismus und N' ein Normalteiler von G' . Dann ist das Urbild $f^{-1}(N')$ ein Normalteiler von G . Insbesondere ist $\text{Kern}(f) = f^{-1}(\{e\})$ ein Normalteiler von G .*

Beweis: Nach 1.1.21 ist $f^{-1}(N')$ eine Untergruppe von G . Ist $a \in G$ und $h \in f^{-1}(N')$, also $f(h) \in N'$, so gilt

$$f(aha^{-1}) = f(a)f(h)f(a)^{-1} \in N',$$

weil N' ein Normalteiler ist. Also ist $aha^{-1} \in f^{-1}(N')$. \square

(4) *Es sei $f : G \rightarrow G'$ ein surjektiver Gruppenhomomorphismus. Ist N ein Normalteiler von G , so ist $f(N)$ ein Normalteiler von G' .*

In diesem Satz ist die Voraussetzung „ f surjektiv“ wesentlich, ohne sie wird die Behauptung falsch (s. 1.2.10).

Beweis: Wiederum nach 1.1.21 ist $f(N)$ eine Untergruppe von G' . Zu zeigen bleibt $a'f(h)a'^{-1} \in f(N)$ für $a' \in G'$, $h \in N$. Weil f surjektiv ist, existiert ein $a \in G$ mit $a' = f(a)$. Weil N Normalteiler ist, gilt $aha^{-1} \in N$, also folgt

$$a'f(h)a'^{-1} = f(a)f(h)f(a)^{-1} = f(aha^{-1}) \in f(N). \quad \square$$

(5) Es sei G eine beliebige Gruppe und H eine Untergruppe vom Index 2. Dann ist H ein Normalteiler von G .

Beweis: Es ist $aH = Ha$ für alle $a \in G$ zu zeigen. Für $a \in H$ gilt trivialerweise $aH = H = Ha$. Für $a \notin H$ ist aH die einzige Linksnebenklasse $\neq H$ in G . Weil G disjunkte Vereinigung seiner beiden Nebenklassen ist, muss

$$aH = G \setminus H$$

gelten. Ebenso folgt $Ha = G \setminus H$, also $aH = G \setminus H = Ha$ für $a \notin H$. \square

1.2.9 Beispiele

(1) Die Menge A_n aller geraden Permutationen (siehe 1.1.11 (2)) ist eine Untergruppe der Permutationsgruppe S_n für $n \geq 2$, denn es ist $\text{id} \in A_n$, und das Produkt von geraden Permutationen ist offensichtlich gerade, ebenso wie das Inverse einer geraden Permutation. Die Gruppe A_n heißt die *alternierende Gruppe* (in n Ziffern).

Wir zeigen nun, dass A_n in S_n den Index 2 hat, also nach 1.2.8 (5) ein Normalteiler von S_n ist.

Beweis: Ist τ eine beliebige Transposition in S_n , so ist die Nebenklasse τA_n genau die Menge der ungeraden Permutationen. Für eine ungerade Permutation σ ist nämlich $\tau\sigma$ gerade, also in A_n , und damit gilt wegen $\tau\tau = \text{id}$

$$\sigma = \tau(\tau\sigma) \in \tau A_n.$$

Umgekehrt enthält τA_n nur ungerade Permutationen.

Daher ist $S_n = A_n \cup \tau A_n$, und A_n hat damit genau zwei Nebenklassen in S_n , also den Index 2. \square

Nach dem Satz von Lagrange und 1.1.10 gilt ferner

$$|A_n| = \frac{|S_n|}{[S_n : A_n]} = \frac{n!}{2},$$

also $|A_2| = 1$, $|A_3| = 3$, $|A_4| = 12$, $|A_5| = 60$ usw.

(2) Für eine beliebige Gruppe G ist das *Zentrum*

$$Z(G) := \{g \in G \mid gx = xg \text{ für alle } x \in G\}$$

von G ein Normalteiler von G .

Beweis 1 (das Zentrum als Kern): Es ist

$$Z(G) = \{g \in G \mid i_g(x) = gxg^{-1} = x \text{ für alle } x \in G\} = \{g \in G \mid i_g = \text{id}_G\}$$

der Kern des in 1.1.16 (3) konstruierten Homomorphismus $i : G \rightarrow \text{Aut}(G)$, $g \mapsto i_g$. Nach 1.2.8 (3) ist $Z(G)$ also ein Normalteiler von G .

Beweis 2 (direkt): Sei $g \in G$. Da für jedes $z \in Z(G)$ die Gleichung $gzg^{-1} = z$ gilt, ist auch $gZ(G)g^{-1} = Z(G)$. \square

Mit dem direkten Argument sieht man auch, dass jede Untergruppe N von G , die im Zentrum enthalten ist, ein Normalteiler von G ist. Das Zentrum $Z(G)$ besteht aus denjenigen Elementen von G , die mit allen Gruppenelementen vertauschbar sind. Insbesondere ist $Z(G)$ selbst abelsch, und G ist genau dann abelsch, wenn $G = Z(G)$ gilt.

(3) Die Menge $\text{Inn}(G)$ aller inneren Automorphismen i_g mit $i_g(x) = gxg^{-1}$ für $g, x \in G$ ist ein Normalteiler von $\text{Aut}(G)$.

Beweis: $\text{Inn}(G)$ ist das Bild des Homomorphismus $G \rightarrow \text{Aut}(G)$, $g \mapsto i_g$, also eine Untergruppe von $\text{Aut}(G)$. Ist $f \in \text{Aut}(G)$ beliebig, so gilt für alle $g, x \in G$:

$$(fi_gf^{-1})(x) = f(gf^{-1}(x)g^{-1}) = f(g)xf(g)^{-1} = i_{f(g)}(x).$$

Also ist $fi_gf^{-1} = i_{f(g)} \in \text{Inn}(G)$. \square

1.2.10 Aufgaben

(1) Bestimmen Sie alle Untergruppen von S_3 und von D_4 (vgl. 1.1.27). Welche dieser Untergruppen sind jeweils Normalteiler? Bestimmen Sie die Zentren $Z(S_3)$ und $Z(D_4)$.

(Hinweis: Nutzen Sie insbesondere den Satz von Lagrange aus.)

(2) Geben Sie einen Gruppenhomomorphismus $f : G \rightarrow G'$ und einen Normalteiler N von G an, so dass $f(N)$ kein Normalteiler von G' ist.

L

Von grundlegender Bedeutung in der Gruppentheorie und der gesamten Algebra ist die Tatsache, dass man mittels eines Normalteilers N einer Gruppe eine neue Gruppe, die *Faktorgruppe* G/N (lies „ G nach N “ oder „ G modulo N “), konstruieren kann.

1.2.11 Konstruktion der Faktorgruppe G/N

Es sei im folgenden immer N ein Normalteiler von G .

(1) Es sei G/N die Menge der Nebenklassen von N in G . Wegen 1.2.7 ist es gleichgültig, ob wir Links- oder Rechtsnebenklassen nehmen, denn diese stimmen überein. Zunächst ist also G/N eine Menge von Teilmengen von G . Man hat eine kanonische Abbildung

$$\pi_N : G \rightarrow G/N, \quad \pi_N(g) := gN,$$

die wir oft die *kanonische Projektion* von G auf G/N nennen werden. π_N ordnet also jedem Gruppenelement die Nebenklasse zu, in der dieses Element liegt. Offensichtlich ist π_N surjektiv.

(2) Auf der Menge G/N definieren wir eine Multiplikation durch

$$G/N \times G/N \rightarrow G/N, \quad (gN)(g'N) := (gg')N.$$

Dann muss man sich zunächst überlegen, dass diese Definition wirklich eindeutig ist. Man muss zeigen:

$$\text{Ist } gN = g_1N \text{ und } g'N = g'_1N, \text{ so ist } (gg')N = (g_1g'_1)N.$$

Das Produkt ist also unabhängig davon, wie die Nebenklassen geschrieben sind. Zum Beweis schreiben wir

$$g_1 = ga \quad \text{mit } a \in N, \quad g'_1 = g'a' \quad \text{mit } a' \in N.$$

Dann erhalten wir wegen $a'N = N = aN$ und $g'N = Ng'$

$$\begin{aligned} (g_1g'_1)N &= (gag'a')N = (gag')(a'N) \\ &= gag'N = ga(Ng') = g(aN)g' = gNg' = gg'N. \end{aligned}$$

(3) Nachdem wir also bewiesen haben, dass das Produkt eindeutig definiert ist, müssen wir nun die Gruppenaxiome verifizieren. Das ist nicht schwierig. Zum Beispiel prüft man die Assoziativität durch folgende Rechnung

$$((gN)(hN))(kN) = (ghN)(kN) = ghkN = (gN)(hkN) = (gN)((hN)(kN)),$$

die für beliebige $g, h, k \in G$ gültig ist. Genauso prüft man, dass N das neutrale Element von G/N und $g^{-1}N$ das inverse Element zu gN ist.

(4) Aus unserer Definition folgt weiter unmittelbar: $\pi_N : G \rightarrow G/N$ ist ein Homomorphismus mit Kern N .

1.2.12 Aufgaben

(1) Zeigen Sie für eine Teilmenge N einer Gruppe G : N ist genau dann ein Normalteiler von G , wenn es eine Gruppe G' und einen Homomorphismus $f : G \rightarrow G'$ gibt mit $\text{Kern}(f) = N$. (In anderen Worten: Normalteiler sind genau jene Untergruppen, die Kern eines Homomorphismus sind.)

(2) Sei H eine Untergruppe einer Gruppe G . Zeigen Sie: Wenn es auf der Menge G/H der Linksnebenklassen von H eine Multiplikation gibt, so dass G/H eine Gruppe und $\pi_H : G \rightarrow G/H$, $\pi_H(g) := gH$ ein Homomorphismus

L ist, dann ist H bereits ein Normalteiler von G .

1.2.13 Satz

Es sei $f : G \rightarrow G'$ ein Gruppenhomomorphismus, N ein Normalteiler von G und $\pi : G \rightarrow G/N$ die kanonische Projektion. Dann gilt:

Es existiert genau dann ein Homomorphismus $\bar{f} : G/N \rightarrow G'$ mit $f = \bar{f} \circ \pi$, wenn $N \subset \text{Kern}(f)$ gilt.

In diesem Fall ist also das Diagramm

$$\begin{array}{ccc} G & \xrightarrow{\pi} & G/N \\ & \searrow f & \downarrow \bar{f} \\ & & G' \end{array}$$

kommutativ, \bar{f} ist durch $f = \bar{f} \circ \pi$ eindeutig bestimmt, und es gilt

$$\text{Bild}(\bar{f}) = \text{Bild}(f), \quad \text{Kern}(\bar{f}) = \{gN \in G/N \mid g \in \text{Kern}(f)\} = \text{Kern}(f)/N.$$

Beweis:

Wenn ein Homomorphismus $\bar{f} : G/N \rightarrow G'$ mit $f = \bar{f} \circ \pi$ existiert, dann muss $N \subset \text{Kern}(f)$ gelten, denn wegen $N = \text{Kern}(\pi)$ gilt für $a \in N$:

$$f(a) = \bar{f}(\pi(a)) = \bar{f}(e) = e, \quad \text{also } a \in \text{Kern}(f).$$

Gelte nun umgekehrt $N \subset \text{Kern}(f)$. Wir definieren $\bar{f}: G/N \rightarrow G'$ durch

$$\bar{f}(gN) := f(g).$$

Diese Definition ist unabhängig von der Darstellung gN der Nebenklasse; ist nämlich $gN = g'N$, also $g^{-1}g' \in N \subset \text{Kern}(f)$, so folgt

$$f(g') = f(gg^{-1}g') = f(g)f(g^{-1}g') = f(g),$$

also ist \bar{f} wohldefiniert. \bar{f} ist ein Homomorphismus, denn für $g, g' \in G$ gilt

$$\bar{f}((gN)(g'N)) = \bar{f}(gg'N) = f(gg') = f(g)f(g') = \bar{f}(gN)\bar{f}(g'N).$$

Ferner gilt für beliebiges $g \in G$

$$f(g) = \bar{f}(gN) = \bar{f}(\pi(g)), \quad \text{also } f = \bar{f} \circ \pi.$$

Gilt umgekehrt $f = \bar{f} \circ \pi$, so ist

$$\bar{f}(gN) = \bar{f}(\pi(g)) = f(g) \quad \text{für } g \in G,$$

damit ist \bar{f} durch $f = \bar{f} \circ \pi$ eindeutig bestimmt.

Weil $\pi: G \rightarrow G/N$ surjektiv ist, gilt außerdem

$$\text{Bild}(\bar{f}) = \bar{f}(G/N) = \bar{f}(\pi(G)) = f(G) = \text{Bild}(f).$$

Schließlich gilt für $g \in G$

$$\begin{aligned} gN \in \text{Kern}(\bar{f}) &\iff \bar{f}(gN) = e \\ &\iff f(g) = e \iff g \in \text{Kern}(f). \end{aligned}$$

Also folgt $\text{Kern}(\bar{f}) = \{gN \in G/N \mid g \in \text{Kern}(f)\} = \text{Kern}(f)/N$. □

In der Situation des Satzes spricht man für $N \subset \text{Kern}(f)$ davon, dass f *kanonisch den Homomorphismus* $\bar{f}: G/N \rightarrow G'$ *induziert* und nennt \bar{f} *den von f (kanonisch) induzierten Homomorphismus*.

Wenden wir die obige Konstruktion für $N = \text{Kern}(f)$ an, so erhalten wir

1.2.14 Korollar (Homomorphiesatz)

Jeder Gruppenhomomorphismus $f: G \rightarrow G'$ induziert kanonisch einen Isomorphismus

$$G/\text{Kern}(f) \xrightarrow{\sim} \text{Bild}(f).$$

Ist insbesondere f surjektiv, so gilt $G/\text{Kern}(f) \cong G'$.

Beweis:

Nach 1.2.13 induziert f einen Homomorphismus $\bar{f} : G/\text{Kern}(f) \rightarrow G'$. Es gilt $\text{Bild}(\bar{f}) = \text{Bild}(f)$ und $\text{Kern}(\bar{f}) = \{g\text{Kern}(f) \mid g \in \text{Kern}(f)\} = \{\text{Kern}(f)\}$, also ist \bar{f} injektiv und liefert daher einen Isomorphismus $G/\text{Kern}(f) \cong \text{Bild}(f)$. \square

1.2.15 Aufgaben

- (1) Sei G eine Gruppe. Zeigen Sie: $G/Z(G) \cong \text{Inn}(G)$.
- (2) Zeigen Sie für einen Körper K und $n \in \mathbb{N}$:

$$\mathbf{L} \quad GL(n, K)/SL(n, K) \cong K^*.$$

1.2.16 Korollar

Ist $f : G \rightarrow G'$ ein Gruppenhomomorphismus, so gilt

$$|G| = |\text{Kern}(f)| \cdot |\text{Bild}(f)|.$$

Beweis:

Sei $N = \text{Kern}(f)$. Es gilt $|G/N| = [G : N]$, und aus dem Satz von Lagrange folgt $|G| = |N| \cdot |G/N|$. Nach dem Homomorphiesatz ist $|G/N| = |\text{Bild}(f)|$, denn beide Gruppen sind isomorph. Es folgt $|G| = |N| \cdot |\text{Bild}(f)|$, wie behauptet. \square

Als Anwendung des Homomorphiesatzes beweisen wir nun die „Isomorphiesätze“:

1.2.17 Satz (Erster Isomorphiesatz)

Es seien H und K Untergruppen einer Gruppe G . Für alle $h \in H$ gelte $hKh^{-1} = K$. Dann gilt:

- (1) $H \cap K$ ist ein Normalteiler von H .
- (2) $HK := \{hk \mid h \in H, k \in K\}$ ist eine Untergruppe von G .
- (3) K ist ein Normalteiler von HK .
- (4) Es besteht ein kanonischer Isomorphismus

$$H/(H \cap K) \cong HK/K.$$

Beweis:

(1) $H \cap K$ ist eine Untergruppe von G (nach 1.1.21). Ist $k \in H \cap K$ und $h \in H$, so ist nach Voraussetzung $hkh^{-1} \in K$ und trivialerweise $hkh^{-1} \in H$, also $hkh^{-1} \in H \cap K$, daher ist $H \cap K$ ein Normalteiler von H .

(2) Offenbar ist $e \in HK$, und für $hk, h'k' \in HK$ haben wir

$$(hk)(h'k') = (hh')(h'^{-1}kh')k' \in HK$$

wegen $h'^{-1}kh' \in K$. Für $hk \in HK$ ist

$$(hk)^{-1} = k^{-1}h^{-1} = h^{-1}(hk^{-1}h^{-1}) \in HK.$$

Also ist HK nach 1.1.18 eine Untergruppe von G .

(3) Wegen $K \subset HK$ ist K eine Untergruppe von HK . Für $hk \in HK$ und $k' \in K$ gilt

$$(hk)k'(hk)^{-1} = h(kk'k^{-1})h^{-1} \in K,$$

also ist K ein Normalteiler von HK .

(4) Der Homomorphismus

$$f : H \rightarrow HK/K, f(h) := hK$$

ist surjektiv, denn $(hk)K = hK = f(h)$. Der Kern von f ist $H \cap K$. Aus dem Homomorphiesatz folgt

$$H/(H \cap K) \cong HK/K. \quad \square$$

1.2.18 Satz (Zweiter Isomorphiesatz)

Seien K und N Normalteiler einer Gruppe G mit $K \subset N$. Dann ist N/K ein Normalteiler von G/K , und es besteht ein kanonischer Isomorphismus

$$G/N \cong (G/K)/(N/K).$$

Beweis:

Die kanonische Projektion $\pi_N : G \rightarrow G/N$ induziert wegen $K \subset N = \text{Kern}(\pi_N)$ nach 1.2.13 einen surjektiven Homomorphismus

$$\bar{\pi}_N : G/K \rightarrow G/N, gK \mapsto gN$$

mit $\text{Kern}(\bar{\pi}_N) = \{gK \mid g \in N\} = N/K$. Also ist N/K ein Normalteiler von G/K , und aus dem Homomorphiesatz folgt

$$(G/K)/(N/K) \cong G/N. \quad \square$$

1.3 Zyklische Gruppen

Ein wesentliches Ziel der Gruppentheorie ist es, eine möglichst vollständige Übersicht über alle nur existierenden Gruppen zu gewinnen. Da wir isomorphe Gruppen vom Standpunkt der Gruppentheorie nicht unterscheiden können, käme es darauf an, alle Gruppen bis auf Isomorphie vollständig zu „klassifizieren“. Dieses Ziel ist sowohl praktisch als auch theoretisch völlig unerreichbar: es gibt einfach „zu viele“ Gruppen. Selbst eine vollständige Klassifikation aller endlichen Gruppen ist gänzlich außer Reichweite. Man wird sich also auf Teilziele beschränken müssen, z. B. besonders ausgezeichnete Klassen von Gruppen zu klassifizieren oder genauer zu untersuchen.

In diesem Kurs werden wir jetzt Methoden darstellen, mit denen man eine gewisse grobe Einteilung aller Gruppen in verschiedene Klassen gewinnt und mit denen man einige solcher Klassen genauer untersuchen kann. So werden wir z. B. alle endlichen abelschen Gruppen vollständig beschreiben. In diesem Abschnitt betrachten wir eine Klasse von ganz besonders einfach gebauten Gruppen, die wir genauer untersuchen wollen. Es handelt sich um die zyklischen Gruppen.

1.3.1 Definition

Eine Gruppe G heißt *zyklisch*, falls ein $a \in G$ existiert mit

$$G = \langle a \rangle = \{a^n \mid n \in \mathbb{Z}\},$$

wenn sie also von einem Element erzeugt wird.

Jede zyklische Gruppe $\langle a \rangle$ ist abelsch, denn a^n und a^m sind für alle $m, n \in \mathbb{Z}$ vertauschbar: $a^n a^m = a^{n+m} = a^m a^n$.

1.3.2 Beispiel

Die additive Gruppe \mathbb{Z} der ganzen Zahlen ist zyklisch. Sie wird nämlich von 1 erzeugt, denn bei Beachtung der additiven Schreibweise gilt natürlich

$$\mathbb{Z} = \{n1 \mid n \in \mathbb{Z}\}.$$

Für jede ganze Zahl n ist die Menge $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$ aller Vielfachen von n eine Untergruppe von \mathbb{Z} , also auch ein Normalteiler, weil \mathbb{Z} abelsch ist. Es sei

$$Z_n := \mathbb{Z}/n\mathbb{Z}.$$

Dann ist Z_n zyklisch, denn Z_n wird von der Nebenklasse $1 + n\mathbb{Z}$ (additive Schreibweise beachten!) erzeugt.

Wir zeigen nun, dass jede zyklische Gruppe isomorph zu \mathbb{Z} oder Z_n für ein $n \in \mathbb{N}$ ist.

1.3.3 Satz (Klassifikation der zyklischen Gruppen)

- (1) Jede Untergruppe von \mathbb{Z} ist von der Form $n\mathbb{Z}$ für ein $n \in \mathbb{N} \cup \{0\}$.
- (2) Jede unendliche zyklische Gruppe ist isomorph zu \mathbb{Z} .
- (3) Ist G eine endliche zyklische Gruppe der Ordnung n , so gilt $G \cong Z_n$.

Beweis:

(1) Sei H eine Untergruppe von \mathbb{Z} . Für $H = \{0\}$ ist $H = 0\mathbb{Z}$. Im Fall $H \neq \{0\}$ enthält H auch positive ganze Zahlen, weil mit k auch $-k$ in H liegt. Sei n die kleinste natürliche Zahl in H . Wir zeigen nun $H = n\mathbb{Z}$. Weil H eine Untergruppe von \mathbb{Z} ist und $n \in H$ gilt, ist offenbar $n\mathbb{Z} \subset H$. Ist umgekehrt $a \in H$, so dividieren wir a mit Rest durch n und erhalten $q, r \in \mathbb{Z}$ mit

$$a = qn + r \quad \text{und} \quad 0 \leq r < n.$$

Weil a, n in der Untergruppe H von \mathbb{Z} liegen, gilt

$$r = a - qn \in H.$$

Wegen $r \in H$, $0 \leq r < n$ muss nach Definition von n dann $r = 0$ gelten, also $a = qn \in n\mathbb{Z}$.

Zu (2) und (3): Für $G = \langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$ ist

$$f : \mathbb{Z} \rightarrow G, \quad f(n) := a^n$$

ein surjektiver Gruppenhomomorphismus. Ist $\text{Kern}(f) = \{0\}$, so ist f ein Isomorphismus, also G isomorph zu \mathbb{Z} . Weil $\text{Kern}(f)$ eine Untergruppe von \mathbb{Z} ist, gibt es nach (1) für $\text{Kern}(f) \neq \{0\}$ ein $m \in \mathbb{N}$ mit $\text{Kern}(f) = m\mathbb{Z}$. Nach dem Homomorphiesatz ist dann

$$Z_m = \mathbb{Z}/m\mathbb{Z} = \mathbb{Z}/\text{Kern}(f) \cong G.$$

Z_m hat genau m Elemente, nämlich die m Nebenklassen $m\mathbb{Z}, 1 + m\mathbb{Z}, \dots, (m-1) + m\mathbb{Z}$.

Ist G in (2) unendlich, so muss daher $\text{Kern}(f) = \{0\}$, also $G \cong \mathbb{Z}$ gelten.

Hat G in (3) die Ordnung n , so folgt $m = |Z_m| = |G| = n$, also $G \cong Z_n$. \square

1.3.4 Satz

Es sei p eine Primzahl und G eine beliebige Gruppe der Ordnung p . Dann gilt $G \cong Z_p$.

Beweis:

Es sei $a \in G$ vom neutralen Element e verschieden. Nach dem Satz von Lagrange ist die Ordnung von a ein Teiler der Primzahl $p = |G|$, also gleich p , weil a wegen $a \neq e$ nicht die Ordnung 1 hat. Damit gilt $|\langle a \rangle| = p = |G|$ für die Untergruppe $\langle a \rangle$, also ist $G = \langle a \rangle$. \square

1.3.5 Satz

(1) Das Bild einer zyklischen Gruppe unter einem Homomorphismus ist zyklisch, insbesondere ist jede Faktorgruppe einer zyklischen Gruppe zyklisch.

(2) Jede Untergruppe einer zyklischen Gruppe ist zyklisch.

L Beweis als Übungsaufgabe.

1.3.6 Beispiel

Die komplexen Zahlen $\exp(\frac{2\pi ik}{n}) = \cos(\frac{2\pi k}{n}) + i \sin(\frac{2\pi k}{n})$, $k \in \{0, \dots, n-1\}$ für $n \in \mathbb{N}$ bilden bezüglich der Multiplikation eine zyklische Gruppe der Ordnung n , die z. B. von $\exp(\frac{2\pi i}{n})$ erzeugt wird.

Beweis: Wegen $\exp(z+w) = \exp(z)\exp(w)$ für $z, w \in \mathbb{C}$ (Multiplikativität der Exponentialfunktion) gilt

$$\exp\left(\frac{2\pi i(k+m)}{n}\right) = \exp\left(\frac{2\pi ik}{n}\right) \exp\left(\frac{2\pi im}{n}\right) \quad \text{für } k, m \in \mathbb{Z},$$

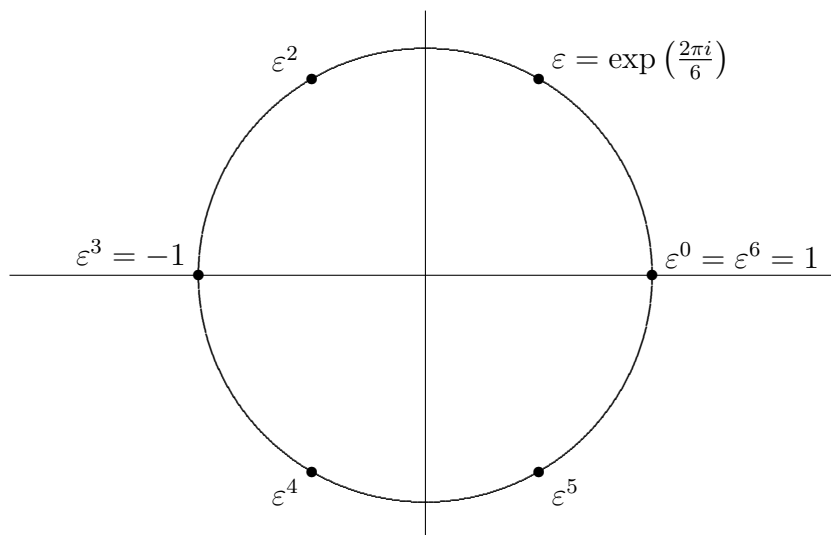
also erhält man einen Gruppenhomomorphismus

$$f: \mathbb{Z} \rightarrow \mathbb{C}^*, \quad f(k) = \exp\left(\frac{2\pi ik}{n}\right).$$

Das Bild ist eine zyklische Gruppe, die von $f(1) = \exp(\frac{2\pi i}{n})$ erzeugt wird. Wegen $f(1)^n = f(n) = \exp(2\pi i) = 1$ besteht die Gruppe gerade aus den Elementen $\exp(\frac{2\pi ik}{n})$ für $k \in \{0, \dots, n-1\}$. \square

Diese Gruppe heißt die *Gruppe der n -ten Einheitswurzeln*, denn für jedes Element ε dieser Gruppe gilt $\varepsilon^n = 1$.

In der komplexen Zahlenebene bilden die Elemente dieser Gruppe ein regelmäßiges n -Eck im Einheitskreis, z. B.



1.3.7 Lemma

Das Element $a \in G$ habe die Ordnung n . Für $m \in \mathbb{Z}$ hat dann a^m die Ordnung $\frac{n}{k}$ mit $k = \text{ggT}(n, m)$.

($\text{ggT}(n, m)$ bezeichnet den größten gemeinsamen Teiler von n, m .)

Ist insbesondere $m \in \mathbb{N}$ ein Teiler von n , so hat a^m die Ordnung $\frac{n}{m}$.

Beweis:

Weil k der größte gemeinsame Teiler von n, m ist, können wir $n = kn'$ und $m = km'$ mit teilerfremden $n', m' \in \mathbb{Z}$ schreiben. Zunächst gilt

$$(a^m)^{\frac{n}{k}} = a^{\frac{mn}{k}} = a^{m'n} = (a^n)^{m'} = e,$$

also ist $\text{ord}(a^m) \leq \frac{n}{k}$. Für $r := \text{ord}(a^m)$ gilt andererseits $e = (a^m)^r = a^{mr}$, also ist mr ein Vielfaches von n , etwa $mr = ns$ mit $s \in \mathbb{Z}$. Hier kürzt man k und erhält $m'r = n's$, d. h. n' teilt $m'r$. Weil n', m' teilerfremd sind, muss n' bereits r teilen. Insbesondere folgt $\frac{n}{k} = n' \leq r = \text{ord}(a^m)$. Insgesamt erhält man $\text{ord}(a^m) = \frac{n}{k}$. □

1.3.8 Korollar

Es seien a, b Elemente endlicher Ordnung in einer Gruppe G . Dann gilt:

$$\langle a \rangle = \langle b \rangle \iff b = a^m \text{ für ein } m, \text{ das teilerfremd zur Ordnung von } a \text{ ist.}$$

Beweis:

„ \Rightarrow “: Ist $\langle a \rangle = \langle b \rangle$, so gilt $b = a^m$ für ein m . Wegen $\langle a \rangle = \langle b \rangle$ hat $b = a^m$ dieselbe Ordnung wie a , also muss nach dem letzten Lemma m teilerfremd zur Ordnung von a sein.

„ \Leftarrow “: Wegen $b = a^m$ ist $\langle b \rangle \subset \langle a \rangle$. Weil m teilerfremd zur Ordnung von a ist, haben $b = a^m$ und a nach dem letzten Lemma dieselbe Ordnung, also gilt $\langle b \rangle = \langle a \rangle$. \square

1.3.9 Aufgabe

(1) Sei G eine zyklische Gruppe der Ordnung $n \in \mathbb{N}$. Zeigen Sie, dass es zu jedem Teiler k von n *genau* eine Untergruppe der Ordnung k in G gibt.

(2) Sei $G \neq \{e\}$ eine Gruppe, und es seien $\{e\}$ und G die einzigen Untergruppen von G . Zeigen Sie: Es gilt $G \cong Z_p$ für eine Primzahl p .

L

1.3.10 Aufgabe

(1) Es seien a, b Elemente der Ordnung m bzw. n ($m, n \in \mathbb{N}$) in einer Gruppe G mit $ab = ba$. Zeigen Sie:

$$\text{ord}(ab) = mn \iff m, n \text{ sind teilerfremd.}$$

(2) Zeigen Sie, dass jede abelsche Gruppe der Ordnung pq (p, q verschiedene Primzahlen) zyklisch ist.

(3) Zeigen Sie, dass jede abelsche Gruppe der Ordnung $p_1 p_2 \cdots p_r$ (p_1, p_2, \dots, p_r paarweise verschiedene Primzahlen) zyklisch ist.

L (4) Wieviele Elemente enthält die Gruppe $\text{Aut}(Z_p)$ (p Primzahl)?

Lösungen zu den Aufgaben in Kurseinheit 1

1.1.6 (1) \mathbb{N} mit der Addition ist keine Gruppe.

Das Assoziativgesetz ist erfüllt. Aber es existiert in \mathbb{N} kein neutrales Element, denn es ist $0 \notin \mathbb{N}$.

(2) \mathbb{N} mit der Multiplikation ist keine Gruppe.

Das Assoziativgesetz gilt. Es existiert das neutrale Element 1 mit $a1 = 1a = a$ für $a \in \mathbb{N}$, aber zu $a \in \mathbb{N}$, $a \neq 1$ gibt es kein Inverses in \mathbb{N} wegen $\frac{1}{a} \notin \mathbb{N}$.

(3) \mathbb{N}^0 mit der Addition ist keine Gruppe.

Es gilt das Assoziativgesetz, und es gibt das neutrale Element $0 \in \mathbb{N}^0$ mit $a + 0 = 0 + a = a$, aber zu $a \in \mathbb{N}^0$, $a \neq 0$ existiert kein Inverses wegen $-a \notin \mathbb{N}^0$.

(4) genau wie (2).

(5) $\mathbb{R}_+ = \{x \in \mathbb{R} \mid x > 0\}$ ist bezüglich der Multiplikation eine Gruppe.

Das Produkt positiver reeller Zahlen ist wieder positiv, liegt also in \mathbb{R}_+ . Die Multiplikation reeller Zahlen ist assoziativ, es existiert das neutrale Element 1, und zu jedem $a \in \mathbb{R}_+$ liegt wegen $\frac{1}{a} > 0$ das Inverse $\frac{1}{a}$ in \mathbb{R}_+ .

(6) genau wie (2).

(7) $\{1, -1\}$ ist mit der Multiplikation (ganzer Zahlen) eine Gruppe.

Das Assoziativgesetz ist erfüllt, und es existiert das neutrale Element 1; die Elemente 1, -1 sind jeweils zu sich selbst invers.

(8) $S = \{z \in \mathbb{C} \mid |z| = 1\}$ ist mit der Multiplikation eine Gruppe.

Das Produkt zweier Elemente von S liegt wegen $|zz'| = |z||z'|$ wieder in S . Die Multiplikation komplexer Zahlen ist assoziativ, und es ist $1 \in S$. Zu $z \in S$ existiert das Inverse z^{-1} in S , denn aus $|z| = 1$ folgt auch $|z^{-1}| = 1$.

1.1.10 Wir zeigen $|S_n| = n!$ durch Induktion nach n :

Für $n = 1$ ist die Behauptung klar. Für den Induktionsschluß sei nun $n > 1$. Ist α eine Permutation aus S_n , so gibt es n Möglichkeiten für $\alpha(n)$, nämlich die Zahlen $1, 2, \dots, n$. Für jede dieser n Möglichkeiten können die restlichen

$n-1$ Zahlen $1, 2, \dots, n-1$ auf die $n-1$ Ziffern $\neq \alpha(n)$ verteilt werden. Nach Induktionsvoraussetzung gibt es dafür genau $(n-1)!$ Möglichkeiten, und wir erhalten insgesamt $n \cdot (n-1)! = n!$ Möglichkeiten, die Zahlen $1, 2, \dots, n$ zu permutieren.

- 1.1.12** (1) Wir bezeichnen die Permutation $(2, 1, 3, 5, 4)_\curvearrowright$ mit α und die Permutation $(5, 3, 4, 1, 2)_\curvearrowright$ mit β . Dann gilt

$$\begin{array}{ccc} & \alpha & \beta \\ 1 & \mapsto 2 & \mapsto 3 \\ 2 & \mapsto 1 & \mapsto 5 \\ 3 & \mapsto 3 & \mapsto 4 \\ 4 & \mapsto 5 & \mapsto 2 \\ 5 & \mapsto 4 & \mapsto 1. \end{array}$$

Die Komposition $\beta \circ \alpha$ (auf richtige Reihenfolge achten!) ist also $(3, 5, 4, 2, 1)_\curvearrowright$. Für $\alpha \circ \beta$ ergibt sich analog

$$\begin{array}{ccc} & \beta & \alpha \\ 1 & \mapsto 5 & \mapsto 4 \\ 2 & \mapsto 3 & \mapsto 3 \\ 3 & \mapsto 4 & \mapsto 5 \\ 4 & \mapsto 1 & \mapsto 2 \\ 5 & \mapsto 2 & \mapsto 1, \end{array}$$

also $(4, 3, 5, 2, 1)_\curvearrowright$.

Das zweite Beispiel wird genauso behandelt: Bezeichnen wir $(1, 4, 6, 3, 5, 2)_\curvearrowright$ mit α und $(4, 3, 1, 2, 6, 5)_\curvearrowright$ mit β , so erhalten wir

$$\beta \circ \alpha = (4, 2, 5, 1, 6, 3)_\curvearrowright \quad \text{und} \quad \alpha \circ \beta = (3, 6, 1, 4, 2, 5)_\curvearrowright.$$

- (2) Eine solche Aufgabe löst man am schnellsten, indem man durch Vertauschen von Ziffern die Permutation in $(1, 2, 3, \dots)_\curvearrowright$ überführt und die Zahl der Vertauschungen abzählt.

$$\begin{aligned} (2, 1, 7, 6, 3, 4, 5)_\curvearrowright &\rightsquigarrow (1, 2, 7, 6, 3, 4, 5)_\curvearrowright \rightsquigarrow (1, 2, 3, 6, 7, 4, 5)_\curvearrowright \rightsquigarrow \\ &(1, 2, 3, 4, 7, 6, 5)_\curvearrowright \rightsquigarrow (1, 2, 3, 4, 5, 6, 7)_\curvearrowright. \end{aligned}$$

Man braucht vier Vertauschungen (Transpositionen), die Permutation ist also gerade.

Die Permutation $(4, 3, 6, 1, 2, 5)_{\circlearrowleft}$ ist ebenfalls gerade.

Man vertauscht 1 mit n , 2 mit $n - 1$, 3 mit $n - 2$ usw. Ist $n = 2m$ gerade, so braucht man m Vertauschungen. Ist $n = 2m + 1$, so braucht man m Vertauschungen. Also ist die Permutation

gerade, falls $n = 4k$ oder $4k + 1$, ungerade, falls $n = 4k + 2$ oder $4k + 3$.

Bei $(2, 4, \dots, 2n, 1, 3, \dots, 2n - 1)_{\circlearrowleft}$ vertauscht man 1 mit den n davorstehenden geraden Zahlen, dann 3 mit den $n - 1$ davorstehenden Zahlen $4, \dots, 2n$, usw. und schließlich $2n - 1$ mit der davorstehenden Zahl $2n$. Insgesamt braucht man

$$n + (n - 1) + \dots + 1 = \frac{n(n + 1)}{2} \text{ Vertauschungen.}$$

Also ist die Permutation

gerade, falls $n = 4k$ oder $4k + 3$, ungerade, falls $n = 4k + 1$ oder $4k + 2$.

- 1.1.16** (1) a) Für $a \in G$ ist die Abbildung $L(a) : G \rightarrow G$, $L(a)(x) = ax$ injektiv, denn aus $L(a)(x) = L(a)(y)$ für $x, y \in G$, also $ax = ay$, folgt $x = y$ nach Multiplikation mit a^{-1} von links. $L(a)$ ist surjektiv, denn für jedes $x \in G$ liegt

$$x = (aa^{-1})x = a(a^{-1}x) = L(a)(a^{-1}x)$$

im Bild von $L(a)$. Damit ist $L(a)$ bijektiv, also ein Element von $S(G)$.

b) Für $a \neq e$ ist $L(a)(e) = ae = a \neq e$. Also ist $L(a)$ kein Gruppenhomomorphismus (wegen 1.1.15(1)).

c) Für alle $a, b \in G$ und alle $x \in G$ gilt

$$L(ab)(x) = (ab)x = a(bx) = L(a)(L(b)(x)) = (L(a) \circ L(b))(x),$$

also ist $L(ab) = L(a) \circ L(b)$. Daher ist $L : G \rightarrow S(G)$ ein Homomorphismus.

(2) a) Für $\alpha \in S(M)$ ist $\varphi \circ \alpha \circ \varphi^{-1}$ als Hintereinanderschaltung von bijektiven Abbildungen wieder bijektiv, also ein Element von $S(M')$.

b) Weil für alle $\alpha, \beta \in S(M)$

$$f(\alpha\beta) = \varphi\alpha\beta\varphi^{-1} = (\varphi\alpha\varphi^{-1})(\varphi\beta\varphi^{-1}) = f(\alpha)f(\beta)$$

gilt, ist f ein Homomorphismus. Wegen

$$f(\alpha) = \varphi \circ \alpha \circ \varphi^{-1} = \text{id}_{M'} \iff \alpha = \varphi^{-1} \circ \text{id}_{M'} \circ \varphi = \text{id}_M$$

ist $\text{Kern}(f) = \{\text{id}_M\}$, also f injektiv. Für $\alpha' \in S(M')$ ist

$$f(\varphi^{-1}\alpha'\varphi) = \varphi\varphi^{-1}\alpha'\varphi\varphi^{-1} = \alpha',$$

also liegt α' im Bild von f . Damit ist f surjektiv, also ein Isomorphismus $S(M) \rightarrow S(M')$.

(3) Für alle $g, g' \in G$ und alle $x \in G$ gilt

$$i_{gg'}(x) = (gg')x(gg')^{-1} = g(g'xg'^{-1})g^{-1} = i_g(i_{g'}(x)),$$

also ist $i_{gg'} = i_g \circ i_{g'}$. Somit ist $i : G \rightarrow \text{Aut}(G)$, $g \mapsto i_g$ ein Homomorphismus.

1.1.20 Für eine Untergruppe H von G gilt natürlich $ab \in H$ für alle $a, b \in H$. Sei nun umgekehrt H eine endliche nichtleere Teilmenge von G , die unter der Multiplikation abgeschlossen ist. Sei $a \in H$, wegen $ab \in H$ für alle $b \in H$ liefert die Linksmultiplikation mit a eine Abbildung $L(a) : H \rightarrow H$, die nach 1.1.16 (1) injektiv ist. Weil H eine endliche Menge ist, muss $L(a)$ auch surjektiv sein. Insbesondere gibt es ein $b \in H$ mit $a = L(a)(b) = ab$, dann ist $b = e$, also $e \in H$.

Weil $L(a) : H \rightarrow H$ für jedes $a \in H$ bijektiv ist, gibt es zu $e \in H$ ein $b \in H$ mit $e = L(a)(b) = ab$, also $b = a^{-1} \in H$. Damit ist H eine Untergruppe von G .

1.1.22 Wenn $H \subset H'$ oder $H' \subset H$ für Untergruppen H, H' von G gilt, so ist $H \cup H'$ gleich H' oder H , also eine Untergruppe von G .

Sei umgekehrt $H \cup H'$ eine Untergruppe, und sei H nicht in H' enthalten. Dann ist $H' \subset H$ zu zeigen. Es existiert ein $h \in H$, $h \notin H'$. Ist $h' \in H'$ beliebig, so ist $hh' \in H \cup H'$, weil $H \cup H'$ eine Gruppe ist. Also gilt $hh' \in H$ oder $hh' \in H'$.

Wäre $hh' \in H'$, so wäre $h = (hh')h'^{-1} \in H'$, Widerspruch. Also ist $hh' \in H$, damit folgt $h' = h^{-1}(hh') \in H$. Also gilt $H' \subset H$.

1.1.25 (1) Für jede Matrix $A \in GL(n, K)$ ist $\hat{A} : K^n \rightarrow K^n$ mit $\hat{A}(x) = Ax$ für $x \in K^n$ eine bijektive lineare Abbildung. Weil $Ax = 0$ genau für $x = 0$ gilt, ist dann auch $\hat{A}|_{K^n \setminus \{0\}}$ bijektiv, also ein Element von $S(K^n \setminus \{0\})$. Für alle $A, B \in GL(n, K)$ und alle $x \in K^n$ gilt

$$(AB)x = A(Bx) = \hat{A}(\hat{B}(x)) = (\hat{A} \circ \hat{B})(x),$$

also ist die Abbildung $GL(n, K) \rightarrow S(K^n \setminus \{0\})$, $A \mapsto \hat{A}$ ein Gruppenhomomorphismus. Dieser Homomorphismus ist injektiv, denn nur die Einheitsmatrix liefert die identische Abbildung auf $K^n \setminus \{0\}$.

(2) $\mathbb{F}_2^2 \setminus \{0\}$ besteht aus drei Elementen, nämlich den Vektoren $\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix}$. Nach 1.1.16 (2) ist also

$$S(\mathbb{F}_2^2 \setminus \{0\}) \cong S_3.$$

Nach (1) haben wir also einen injektiven Homomorphismus

$$GL(2, \mathbb{F}_2) \rightarrow S_3.$$

Nun bestehen beide Gruppen aus sechs Elementen, denn

$$GL(2, \mathbb{F}_2) = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\}$$

und $|S_3| = 3! = 6$ nach 1.1.10. Also ist der injektive Homomorphismus $GL(2, \mathbb{F}_2) \rightarrow S_3$ bereits ein Isomorphismus.

(3) \mathbb{F}_3^2 hat $3^2 = 9$ Elemente, also 8 Elemente $\neq 0$. Die Konstruktion in (1) liefert einen injektiven Homomorphismus

$$GL(2, \mathbb{F}_3) \rightarrow S(\mathbb{F}_3^2 \setminus \{0\}) \cong S_8.$$

Also ist $GL(2, \mathbb{F}_3)$ isomorph zu einer Untergruppe von S_8 . Die Menge aller 2×2 -Matrizen über \mathbb{F}_3 enthält $3^4 = 81$ Elemente, denn für jeden der 4 Matrixkoeffizienten gibt es 3 Möglichkeiten. Weil in einer nicht invertierbaren Matrix die beiden Spalten linear abhängig sind, sind genau die folgenden Matrizen

$$\begin{pmatrix} 0 & a_{12} \\ 0 & a_{22} \end{pmatrix} \text{ mit beliebigen } a_{12}, a_{22} \in \mathbb{F}_3,$$

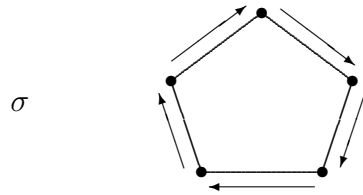
$$\begin{pmatrix} a_{11} & ba_{11} \\ a_{12} & ba_{12} \end{pmatrix} \text{ mit } \begin{pmatrix} a_{11} \\ a_{12} \end{pmatrix} \neq \begin{pmatrix} 0 \\ 0 \end{pmatrix} \text{ und } b \in \mathbb{F}_3 \text{ beliebig}$$

nicht invertierbar. Das sind insgesamt

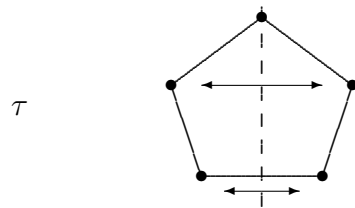
$$3^2 + (3^2 - 1)3 = 33$$

Matrizen. Also besteht $GL(2, \mathbb{F}_3)$ aus $81 - 33 = 48$ Elementen.

1.1.28 (1) Wir führen die Diskussion nicht in allen Einzelheiten aus, sondern geben nur ihren Gang an. Es seien σ und τ wie folgt definiert:



also „zyklische“ Vertauschung,



also eine „Spiegelung“.

Dann gelten folgende Gleichungen:

$$\begin{aligned} \sigma^5 &= e, \quad \tau^2 = e, \\ \tau\sigma\tau &= \sigma^{-1} = \sigma^4, \quad \text{also } \tau\sigma = \sigma^4\tau. \end{aligned}$$

Ein Automorphismus $\alpha \neq e$, der einen Eckpunkt festläßt, ist notwendig eine „Spiegelung“ (von der Art wie τ). Davon gibt es insgesamt 5 Stück, für jeden Punkt eine. Jeder andere Automorphismus ist eine zyklische Vertauschung, also eine Potenz von σ . Insgesamt hat die Gruppe also 10 Elemente, und zwar die zyklischen Vertauschungen

$$e, \sigma, \sigma^2, \sigma^3, \sigma^4$$

und die Spiegelungen

$$\tau, \sigma\tau, \sigma^2\tau, \sigma^3\tau, \sigma^4\tau.$$

(2) Arme und Beine können unabhängig voneinander vertauscht werden. Das ergibt vier Automorphismen einschließlich der Identität.

1.2.6 (1) Wenn alle Potenzen $\dots, a^{-2}, a^{-1}, e, a, a^2, \dots$ von a paarweise verschieden sind, dann ist $\langle a \rangle = \{a^m \mid m \in \mathbb{Z}\}$ unendlich, also hat a unendliche Ordnung. Andernfalls gibt es $i, j \in \mathbb{Z}$ mit $a^i = a^j$ und $i > j$. Für $k = i - j > 0$ folgt daraus $a^k = a^{i-j} = a^i(a^j)^{-1} = e$, also gibt es ein $k \in \mathbb{N}$ mit $a^k = e$. Sei n die kleinste natürliche Zahl mit $a^n = e$. Dann sind in $H = \{e, a, \dots, a^{n-1}\}$ alle Elemente voneinander verschieden, denn sonst gäbe es i, j mit $a^i = a^j$ und

$0 \leq j < i \leq n-1$, also $a^{i-j} = e$ mit $1 \leq i-j \leq n-1$, was der Minimalität von n widerspricht. Damit ist $|H| = n$, und wir zeigen nun $\langle a \rangle = H$.

Offenbar ist $H \subset \langle a \rangle$. Zu jedem $m \in \mathbb{Z}$ erhält man bei Division von m durch n mit Rest ganze Zahlen q, r mit

$$m = qn + r \quad \text{und} \quad 0 \leq r < n.$$

Dann ist $a^m = a^{qn+r} = (a^n)^q a^r = e^q a^r = a^r \in H$, also gilt auch $\langle a \rangle \subset H$. Es folgt $\text{ord}(a) = |\langle a \rangle| = |H| = n$, damit sind beide Aussagen von (1) bewiesen.

(2) Sei $n \in \mathbb{N}$ die Ordnung von a .

„ \Rightarrow “: Ist $k \in \mathbb{Z}$ mit $a^k = e$, so dividieren wir k mit Rest durch n und erhalten $q, r \in \mathbb{Z}$ mit

$$k = qn + r \quad \text{und} \quad 0 \leq r < n.$$

Dann gilt $e = a^k = a^{qn+r} = a^r$. Weil n nach (1) die kleinste natürliche Zahl mit $a^n = e$ ist, muss $r = 0$ gelten. Also ist $k = qn$ ein Vielfaches von $n = \text{ord}(a)$.

„ \Leftarrow “: Ist n ein Teiler von k , also $k = qn$ für ein $q \in \mathbb{Z}$, so gilt natürlich $a^k = a^{qn} = (a^n)^q = e$.

(3) Nach dem Satz von Lagrange ist $\text{ord}(a)$ ein Teiler von $|G|$, nach (2) folgt $a^{|G|} = e$.

(4) Für $a \in H \cap K$ ist $\text{ord}(a)$ ein Teiler von $|H|$ und $|K|$. Weil die Ordnungen teilerfremd sind, folgt $\text{ord}(a) = 1$, also $a = e$ und damit $H \cap K = \{e\}$.

1.2.10 (1) Wir betrachten zunächst die symmetrische Gruppe S_3 in drei Ziffern. Der Normalteiler A_3 der geraden Permutationen besteht aus

$$e = \text{id}, \quad \alpha := (2, 3, 1)_{\circlearrowleft}, \quad (3, 1, 2)_{\circlearrowleft} = \alpha^2.$$

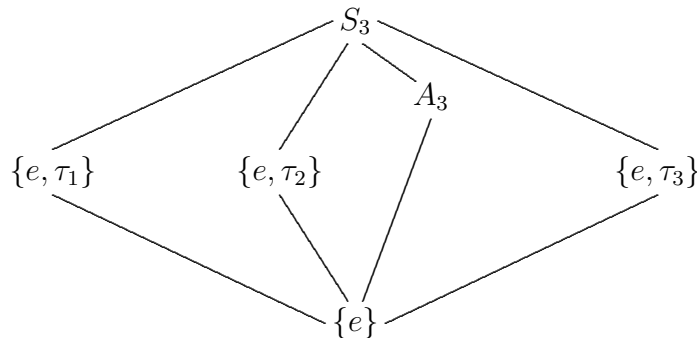
Wegen $|S_3| = 3! = 6$ sind die drei verschiedenen Transpositionen

$$\tau_1 = (1, 3, 2)_{\circlearrowleft}, \quad \tau_2 = (3, 2, 1)_{\circlearrowleft}, \quad \tau_3 = (2, 1, 3)_{\circlearrowleft}$$

die drei restlichen Elemente von S_3 . Für jede Transposition τ_i ist $H_i = \{e, \tau_i\}$ wegen $\tau_i^2 = \text{id} = e$ eine Untergruppe von S_3 . Umgekehrt enthält jede Untergruppe H der Ordnung 2 ein Element der Ordnung 2 in S_3 , also eine Transposition τ_i (weil α und α^2 die Ordnung 3 haben). Damit ist $H = \{e, \tau_i\} = H_i$

für ein $i \in \{1, 2, 3\}$. Jede Untergruppe A der Ordnung 3 von S_3 muss zwei Elemente der Ordnung 3 enthalten (weil die Ordnung der Elemente ein Teiler von 3 ist), also sind $\alpha, \alpha^2 \in A$, und es folgt $A = A_3$.

Da nach dem Satz von Lagrange eine echte Untergruppe von S_3 die Ordnung 2 oder 3 hat, ergeben sich damit alle Untergruppen wie folgt:



Die Untergruppen $\{e, \tau_i\}$ für $i = 1, 2, 3$ sind keine Normalteiler, denn für $\{i, j, k\} = \{1, 2, 3\}$ gilt

$$\tau_j \tau_i \tau_j^{-1} = \tau_k \notin \{e, \tau_i\}.$$

A_3 liegt nicht in $Z(S_3)$, denn für $\alpha \in A_3$ gilt

$$\alpha \tau_1 = \tau_3 \neq \tau_2 = \tau_1 \alpha.$$

Weil das Zentrum $Z(S_3)$ ein Normalteiler von S_3 ist, muss $Z(S_3) = \{e\}$ gelten.

Etwas schwieriger ist die Situation bei der Dieder-Gruppe

$$D_4 = \{e, \sigma, \sigma^2, \sigma^3, \tau, \tau\sigma, \tau\sigma^2, \tau\sigma^3\}$$

mit $\sigma^4 = \tau^2 = e$, $\tau\sigma\tau = \sigma^3$. Man rechnet nach, dass genau folgende Elemente die Ordnung 2 haben

$$\sigma^2, \tau, \tau\sigma, \tau\sigma^2, \tau\sigma^3.$$

Zum Beispiel gilt $(\tau\sigma)^2 = \tau\sigma\tau\sigma = \sigma^3\sigma = e$.

Diese Elemente zusammen mit dem neutralen Element bilden jeweils Untergruppen der Ordnung 2. $\{e, \sigma^2\}$ ist ein Normalteiler, denn σ^2 ist mit σ und τ vertauschbar ($\sigma^2\tau = \sigma\tau\sigma^3 = \tau\sigma^2$), also mit allen Gruppenelementen α ,

somit ist $\alpha\sigma^2\alpha^{-1} = \sigma^2$ und $\sigma^2 \in Z(D_4)$. Die anderen vier Untergruppen der Ordnung 2 sind keine Normalteiler, denn z. B. gilt

$$\sigma\tau\sigma^{-1} = \tau\sigma^3\sigma^{-1} = \tau\sigma^2 \notin \{e, \tau\}.$$

Eine weitere Untergruppe ist

$$\langle \sigma \rangle = \{e, \sigma, \sigma^2, \sigma^3\}.$$

Diese ist ein Normalteiler, weil sie vom Index 2 ist (nach 1.2.8 (5)). Aus demselben Grund sind auch die Untergruppen

$$\begin{aligned} &\{e, \sigma^2, \tau, \tau\sigma^2\}, \\ &\{e, \sigma^2, \tau\sigma, \tau\sigma^3\} \end{aligned}$$

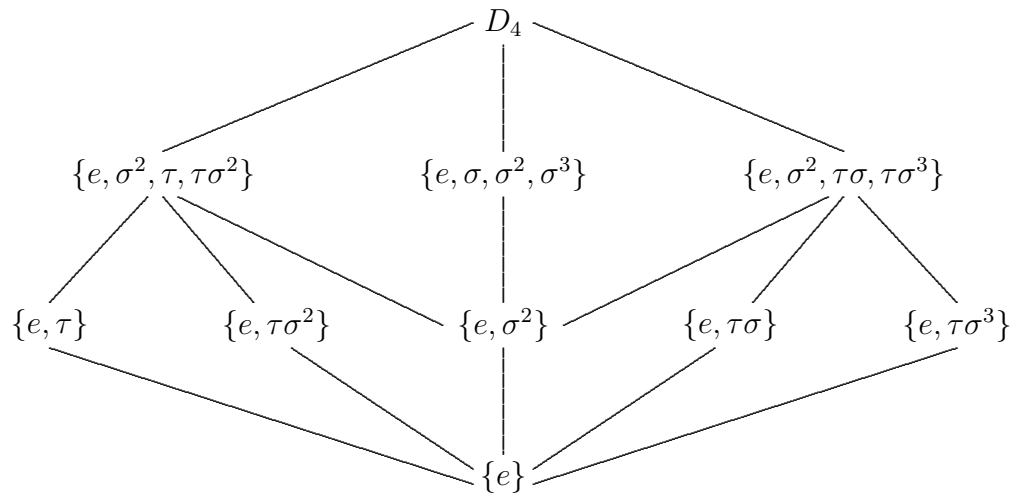
Normalteiler. Wir zeigen nun, dass wir damit alle echten Untergruppen gefunden haben.

Nach dem Satz von Lagrange hat eine echte Untergruppe die Ordnung 2 oder 4. Da eine Untergruppe der Ordnung 2 ein Element der Ordnung 2 enthält, gehört sie zu den fünf oben gefundenen Gruppen. Sei nun H eine Untergruppe der Ordnung 4. Für die Untergruppe $H \cap \langle \sigma \rangle$ sind die Ordnungen 1, 2 oder 4 möglich. Im Fall der Ordnung 4 ist $H = \langle \sigma \rangle$. Wäre $H \cap \langle \sigma \rangle = \{e\}$, so gäbe es wegen

$$h\langle \sigma \rangle = h'\langle \sigma \rangle \iff h^{-1}h' \in H \cap \langle \sigma \rangle \iff h = h' \text{ für } h, h' \in H$$

vier verschiedene Nebenklassen $h\langle \sigma \rangle$, $h \in H$, was $[D_4 : \langle \sigma \rangle] = \frac{8}{4} = 2$ widerspricht. Im Fall $H \neq \langle \sigma \rangle$ hat also $H \cap \langle \sigma \rangle$ die Ordnung 2, daraus folgt $\sigma^2 \in H$. Da H nun mit einem der verbleibenden Elemente $a = \tau, \tau\sigma, \tau\sigma^2, \tau\sigma^3$ auch $a\sigma^2$ enthalten muss, ergeben sich genau die beiden Gruppen $\{e, \sigma^2, \tau, \tau\sigma^2\}$ und $\{e, \sigma^2, \tau\sigma, \tau\sigma^3\}$.

Wir fassen das Ergebnis in folgendem Diagramm zusammen:



Normalteiler sind genau die Gruppen der Ordnung 4 und die der mittleren Achse. Wegen $\tau\sigma\tau^{-1} = \sigma^3 \neq \sigma$ liegt σ nicht im Zentrum von D_4 . Weil $Z(D_4)$ ein Normalteiler ist und $\sigma^2 \in Z(D_4)$ gilt, folgt $Z(D_4) = \{e, \sigma^2\}$.

(2) Ist H eine Untergruppe einer Gruppe G , die kein Normalteiler ist, so ist die Inklusionsabbildung $i : H \hookrightarrow G$ ein Homomorphismus. $\text{Bild}(i) = H$ ist kein Normalteiler in G , obwohl H natürlich in H ein (trivialer) Normalteiler ist.

Man kann also z. B. die Inklusion $\{e, \tau\} \hookrightarrow S_3$ für eine Transposition $\tau \in S_3$ betrachten.

1.2.12 (1) Für einen Normalteiler N ist die kanonische Projektion $\pi_N : G \rightarrow G/N$ ein Homomorphismus mit $\text{Kern}(\pi_N) = N$. Ist umgekehrt N der Kern eines Gruppenhomomorphismus, so ist N nach 1.2.8 (3) ein Normalteiler.

(2) Wenn G/H eine Gruppe und $\pi_H : G \rightarrow G/H$ ein Homomorphismus ist, dann ist $\pi_H(e) = H$ das neutrale Element von G/H . Es folgt

$$g \in \text{Kern}(\pi_H) \iff gH = \pi_H(g) = H \iff g \in H,$$

also ist $H = \text{Kern}(\pi_H)$ und damit ein Normalteiler von G .

1.2.15 (1) Für den in 1.1.16 (3) konstruierten Homomorphismus

$$i : G \rightarrow \text{Aut}(G), \quad g \mapsto i_g \quad \text{mit} \quad i_g(x) = gxg^{-1}$$

gilt (siehe 1.2.9 (2) und (3))

$$Z(G) = \text{Kern}(i) \quad \text{und} \quad \text{Inn}(G) = \text{Bild}(i).$$

Aus dem Homomorphiesatz folgt also sofort $G/Z(G) \cong \text{Inn}(G)$.

(2) Der Gruppenhomomorphismus $\det : GL(n, K) \rightarrow K^*$ ist surjektiv und hat $SL(n, K)$ als Kern. Nach dem Homomorphiesatz ist dann

$$GL(n, K)/SL(n, K) \cong K^*.$$

1.3.5 (1) Ist $G = \langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$ zyklisch und $f : G \rightarrow G'$ ein Homomorphismus, so ist

$$\text{Bild}(f) = \{f(a^n) \mid n \in \mathbb{Z}\} = \{f(a)^n \mid n \in \mathbb{Z}\} = \langle f(a) \rangle,$$

also ist $\text{Bild}(f)$ zyklisch und wird von $f(a)$ erzeugt. Weil eine Faktorgruppe G/N einer zyklischen Gruppe G das Bild von $\pi_N : G \rightarrow G/N$ ist, ist insbesondere G/N zyklisch.

(2) Zu jeder zyklischen Gruppe $G = \langle a \rangle$ gibt es einen surjektiven Homomorphismus $f : \mathbb{Z} \rightarrow G$, $f(n) = a^n$. Für eine Untergruppe H von G ist $f^{-1}(H)$ eine Untergruppe von \mathbb{Z} (nach 1.1.21), also nach 1.3.3 (1) von der Form $n\mathbb{Z}$ für ein n . Weil $n\mathbb{Z}$ von n erzeugt wird, ist daher $f^{-1}(H) = n\mathbb{Z}$ zyklisch. Weil f surjektiv ist, gilt

$$H = f(f^{-1}(H)) = f(n\mathbb{Z}).$$

Als Bild der zyklischen Gruppe $n\mathbb{Z}$ ist H dann nach (1) zyklisch.

1.3.9 (1) Sei $G = \langle a \rangle$ zyklisch mit der Ordnung $n \in \mathbb{N}$ und k ein Teiler von n , also $n = km$ für ein $m \in \mathbb{N}$. Nach 1.3.7 hat a^m wegen $ggT(n, m) = m$ die Ordnung $\frac{n}{m} = k$, also ist $H = \langle a^m \rangle$ eine Untergruppe der Ordnung k . Wir zeigen nun, dass dies die einzige Untergruppe der Ordnung k von G ist. Ist K eine weitere Untergruppe der Ordnung k , so ist K nach 1.3.5 (2) zyklisch, also $K = \langle a^i \rangle$. Mit $d := ggT(i, n)$ folgt nach 1.3.7

$$k = |K| = \text{ord}(a^i) = \frac{n}{d} = \frac{km}{d},$$

also $m = d$. Damit ist $m = ggT(i, n)$ ein Teiler von i , etwa $i = jm$. Dann ist

$$K = \langle a^{jm} \rangle = \langle (a^m)^j \rangle \subset \langle a^m \rangle = H.$$

Daraus folgt $K = H$ wegen $|K| = k = |H|$.

(2) Für jedes $a \in G$, $a \neq e$ ist $\langle a \rangle$ eine Untergruppe $\neq \{e\}$ von G , also ist $G = \langle a \rangle$ zyklisch. Weil \mathbb{Z} echte Untergruppen hat, kann nicht $G \cong \mathbb{Z}$ gelten. Also ist G nach 1.3.3 endlich, und es gibt ein $n \in \mathbb{N}$ mit $G \cong Z_n$. Wäre n keine Primzahl, so gäbe es zu einem Teiler $k \neq 1, n$ von n nach (1) eine Untergruppe der Ordnung k . Also ist $p = n$ eine Primzahl.

1.3.10 (1) „ \Rightarrow “: Sei $\text{ord}(ab) = mn$ und k ein gemeinsamer Teiler von m und n , also $m = km'$ und $n = kn'$ mit $m', n' \in \mathbb{Z}$. Dann gilt wegen $ab = ba$

$$(ab)^{km'n'} = a^{mn'}b^{m'n} = ee = e,$$

also ist $\text{ord}(ab) = mn$ ein Teiler von $km'n' = \frac{mn}{k}$. Dies ist nur für $k = 1$ möglich, also sind m, n teilerfremd.

„ \Leftarrow “: Seien m, n teilerfremd und $k = \text{ord}(ab)$. Wegen

$$(ab)^{mn} = a^{mn}b^{mn} = ee = e$$

ist k ein Teiler von mn . Andererseits gilt

$$e = (ab)^{kn} = a^{kn}b^{kn} = a^{kn}e = a^{kn},$$

also ist $m = \text{ord}(a)$ ein Teiler von kn . Weil m, n teilerfremd sind, muss m bereits k teilen. Ebenso zeigt man, dass n ein Teiler von k ist. Weil m, n teilerfremd sind, ist dann mn ein Teiler von k . Insgesamt folgt $mn = k = \text{ord}(ab)$.

(2) Wir nehmen an, dass G nicht zyklisch ist, also kein Element der Ordnung pq in G existiert. Dann wählen wir ein $a \neq e$. Die Ordnung von a ist ein Teiler von pq , also entweder p oder q . Ohne Einschränkung sei $\text{ord}(a) = p$ (der andere Fall wird genauso behandelt). In der abelschen Gruppen G ist $\langle a \rangle$ ein Normalteiler, wir können also $G/\langle a \rangle$ bilden, $G/\langle a \rangle$ hat die Ordnung $[G : \langle a \rangle] = q$. Wir wählen nun ein $b \notin \langle a \rangle$. Hätte b die Ordnung p , so wäre $b^p \langle a \rangle = \langle a \rangle$ in $G/\langle a \rangle$. Die Ordnung von $b \langle a \rangle$ in $G/\langle a \rangle$ müßte dann ein Teiler von p und der Gruppenordnung q von $G/\langle a \rangle$ sein, sie wäre also 1 und damit

$b\langle a \rangle = \langle a \rangle$ im Widerspruch zu $b \notin \langle a \rangle$. Weil nach Annahme kein Element der Ordnung pq existiert, muss b also die Ordnung q haben. Weil p, q teilerfremd sind, hat dann ab die Ordnung pq im Widerspruch zur Annahme.

(3) Der Beweis wird durch Induktion nach r geführt. Der Induktionsanfang $r = 1$ ist nach 1.3.4 trivial; der Fall $r = 2$ wurde gerade in (2) behandelt. Angenommen, es gibt in G kein Element der Ordnung $p_1 \cdots p_r$. Dann sei a ein beliebiges Element $\neq e$, und zwar ohne Beschränkung der Allgemeinheit von der Ordnung $p_1 \cdots p_s$ mit $1 \leq s < r$. Die Ordnung der Faktorgruppe $G/\langle a \rangle$ ist dann $p_{s+1} \cdots p_r$. Diese ist nach Induktionsvoraussetzung zyklisch, es gibt also ein Element $b\langle a \rangle$ der Ordnung $p_{s+1} \cdots p_r$ in $G/\langle a \rangle$. Ist n die Ordnung von b in G , so folgt aus $b^n\langle a \rangle = \langle a \rangle$, dass n ein Vielfaches von $\text{ord}(b\langle a \rangle)$ ist, etwa $n = p_{s+1} \cdots p_r m$. Dann hat b^m nach 1.3.7 die Ordnung $\frac{n}{m} = p_{s+1} \cdots p_r$. Weil p_1, \dots, p_r paarweise verschieden sind, sind $p_1 \cdots p_s, p_{s+1} \cdots p_r$ teilerfremd, also hat ab^m nach (1) die Ordnung $p_1 \cdots p_r$ im Widerspruch zur Annahme.

(4) Wir behaupten, dass $\text{Aut}(Z_p)$ eine Gruppe der Ordnung $p - 1$ ist. Für $i = 1, \dots, p - 1$ sei

$$\alpha_i : Z_p \rightarrow Z_p, \alpha_i(k + p\mathbb{Z}) = ki + p\mathbb{Z}.$$

α_i ist ein wohldefinierter Homomorphismus. Wegen $\alpha_i(1 + p\mathbb{Z}) \neq p\mathbb{Z}$ ist $\text{Kern}(\alpha_i) \neq Z_p$. Weil Z_p nur die Untergruppen $\{0\}, Z_p$ hat, folgt $\text{Kern}(\alpha_i) = \{0\}$, also α_i injektiv. Weil Z_p endlich ist, ist α_i dann bijektiv, also ein Automorphismus. Weitere Automorphismen kann es nicht geben, denn ist $\alpha : Z_p \rightarrow Z_p$ ein Automorphismus und $\alpha(1 + p\mathbb{Z}) = i + p\mathbb{Z}$ für $i \in \{1, \dots, p - 1\}$, so folgt $\alpha(k + p\mathbb{Z}) = \alpha(k(1 + p\mathbb{Z})) = k(i + p\mathbb{Z}) = ki + p\mathbb{Z}$, also $\alpha = \alpha_i$. Damit ist gezeigt, dass $\text{Aut}(Z_p)$ genau $p - 1$ Elemente besitzt.

1.4.3 Ist $\alpha : G \rightarrow S(M)$ ein Homomorphismus und setzt man $gx := \alpha(g)(x)$ für $g \in G, x \in M$, so gilt für alle $g, h \in G, x \in M$

$$(1) \quad ex = \alpha(e)(x) = \text{id}(x) = x,$$

$$(2) \quad g(h(x)) = \alpha(g)(\alpha(h)(x)) = (\alpha(g) \circ \alpha(h))(x) = \alpha(gh)(x) = (gh)x.$$

Damit sind die Bedingungen aus 1.4.1 erfüllt, also operiert G auf M .