Zum Begriff der Gruppe

sowie den Sätzen von

Lagrange, Fermat und Euler

mit einem Ausblick auf das Lösen von Gleichungen
und auflösbare Gruppen

Jochen Ziegenbalg

ziegenbalg.edu@gmail.com

https://jochen-ziegenbalg.github.io/materialien/

Contents

1 Definitionen, Grundbegriffe, erste Beispiele **3**

1.1 Erste Beispiele 4

1.2 Gruppentafeln 5

1.3 Permutationen 7

1.4 Die Eindeutigkeit der inversen Elemente 9

1.5 Strukturerhaltende Abbildungen 10

1.6 Die Links-Multiplikation 11

2 Untergruppen und Nebenklassen **12**

2.1 Untergruppen 12

2.2 Nebenklassen 13

2.3 Der Index einer Untergruppe 14

2.4 Erzeugende Elemente und zyklische Gruppen 15

3 Gruppen primer Restklassen **17**

4 Die Sätze von Fermat, Euler und Wilson **18**

5 Normalteiler, Faktorgruppen, einfache Gruppen **19**

5.1 Normalteiler 19

5.2 Faktorgruppen 21

6 Subnormalreihen, Kompositionsreihen, auflösbare Gruppen 21

6.1 Subnormalteiler und Subnormalreihen 21

6.2 Kommutator, Kommutatorgruppen, Kommutatorreihen 22

6.3 Die Sätze von Schreier und Jordan-Hölder 23

7 Direkte Produkte 24

7.1 Direkte Produkte von Gruppen 24

7.2 Der Hauptsatz über endlich erzeugte abelsche Gruppen 25

8 Skizze: Polynomgleichungen 25

8.1 Gleichungen 2. Grades 26

8.2 Gleichungen 3. Grades 27

8.3 Gleichungen 4. Grades 29

8.4 Gleichungen 5. Grades 29

8.5 Der Satz von Vieta und Symmetrien bei den Wurzeln 29

8.6 Ruffini, Abel und Galois 30

1 Definitionen, Grundbegriffe, erste Beispiele

Definition 1.1 Eine *Gruppe* ist ein "Tripel" $(G, \circ, e)$ bestehend aus einer Menge G, einer zweistelligen Verknüpfung $\circ : G \times G \to G$ und einem speziellen Element $e \in G$ mit den folgenden Eigenschaften:

1. Die Verknüpfung $\circ$ ist assoziativ; d.h.:
   für alle $a, b, c \in G$ gilt $(a \circ b) \circ c = a \circ (b \circ c)$.

2. Existenz eines neutralen Elements:
   Für alle $a \in G$ gilt $a \circ e = e \circ a = a$.

3. Existenz von inversen Elementen:
   Zu jedem Element $a \in G$ gibt es ein Element $b \in G$ mit der Eigenschaft $a \circ b = b \circ a = e$.

Weitere Definitionen:

1. Falls für alle $a, b \in G$ stets $a \circ b = b \circ a$ gilt, so heißt die Gruppe *kommutativ* oder auch *abelsche Gruppe*.

2. Falls G eine *endliche Menge* ist, so heißt G *endliche Gruppe*; andernfalls *unendliche Gruppe*.

3. Die Mächtigkeit (d.h. im Falle einer endlichen Gruppe die Elementezahl) der Gruppe G heißt die *Ordnung* von G; im Zeichen: $|G|$.

Hinweis: Im restlichen Manuskript werden praktisch nur endliche Gruppen betrachtet. Wenn also nichts weiter gesagt ist, ist davon auszugehen, dass mit "Gruppe" stets "endliche Gruppe" gemeint ist.

Bemerkungen

1. Die Menge G wird auch als die *Trägermenge* der Gruppe bezeichnet. Wenn keine Verwechslungsgefahr besteht, spricht man oft auch kurz von der Gruppe G.

2. Als Verknüpfungssymbol für die (zweistellige) Verknüpfung wird auch das gewöhnliche Multiplikationszeichen $(\cdot)$ bzw. das Additionszeichen $(+)$ verwendet; letzteres meist bei kommutativen Gruppen. Das Multiplikationszeichen $\cdot$ wird gelegentlich auch weggelassen, wenn keine Verwechslungsgefahr besteht. An Stelle von $a \circ b$ wird also auch $a \cdot b$ oder ab geschrieben.

3. Das spezielle Element e heißt *neutrales Element*. Wird die Gruppe multiplikativ geschrieben, so verwendet man auch das Symbol 1 für das neutrale Element; wird die Gruppe additiv geschrieben, so verwendet man meist das Symbol 0 für das neutrale Element.

4. Sind $a, b \in G$ mit $a \circ b = b \circ a = e$, so heißt b *invers* zu a.

5. Die in der Definition des Gruppenbegriffs geforderten Eigenschaften ließen sich im Prinzip auch noch etwas „sparsamer“ (d.h. mit etwas weniger Voraussetzungen) formulieren, aber darauf kommt es hier nicht an.

1.1 Erste Beispiele

Beispiel: Die Deckabbildungen eines gleichseitigen Dreiecks

Die Menge D_3 der Deckabbildungen eines gleichseitigen Dreiecks mit der Hintereinanderausführung von Abbildungen als Gruppenverknüpfung und der identischen Abbildung als neutralem Element.

Gruppenelemente sind:

- 3 Drehungen (um 120, 240 und 360 Grad) um den Schwerpunkt
- 3 Achsenspiegelungen an den (ortsfesten) Mittelsenkrechten
- neutrales Element: Die Drehung um 360 Grad (= 0 Grad), also die identische Abbildung

Diese Gruppe wird auch als *Diedergruppe* D_3 bezeichnet.

Etwas genauer: In der folgenden Abbildung seien A, B und C (ortsfeste) Punkte in der Ebene, die ein gleichseitiges Dreieck bestimmen. S sei der Schwerpunkt dieses Dreiecks.

Weiterhin seien:

- δ_1 die Drehung um S (entgegen dem Uhrzeigersinn) um 120 Grad,
- δ_2 die Drehung um S um 240 Grad,
- δ_3 die Drehung um S um 360 Grad (= 0 Grad).

Schließlich seien

- σ_1 die (Achsen-) Spiegelung an der (ortsfesten) Achse AS,
- σ_2 die Spiegelung an der Achse BS, und
- σ_3 die Spiegelung an der Achse CS.

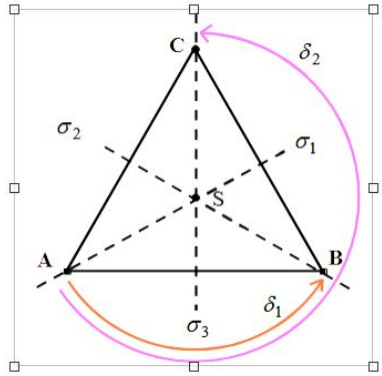

Abbildung 1.1: Die Diedergruppe D_3

1.2 Gruppentafeln

Bei endlichen Gruppen lässt sich die Wirkung der Verknüpfung vollständig in einer tabellenartigen Form, der sogenannten Verknüpfungstafel (auch *Cayley-Tafel*[1] genannt) darstellen. Die folgende Verknüpfungstafel zur Gruppe D_3 ist folgendermaßen zu lesen: Das Ergebnis des Produkts

Spalten-Element (links) mal Zeilen-Element (oben)

ist im „Kreuzungspunkt“ dargestellt.
Dabei ist zuerst die Abbildung in der (linken) Spalte und dann die Abbildung in der (oberen) Zeile auszuführen.

$\circ$	δ_0	δ_1	δ_2	σ_1	σ_2	σ_3
δ_0	δ_0	δ_1	δ_2	σ_1	σ_2	σ_3
δ_1	δ_1	δ_2	δ_0	σ_2	σ_3	σ_1
δ_2	δ_2	δ_0	δ_1	σ_3	σ_1	σ_2
σ_1	σ_1	σ_3	σ_2	δ_0	δ_2	δ_1
σ_2	σ_2	σ_1	σ_3	δ_1	δ_0	δ_2
σ_3	σ_3	σ_2	σ_1	δ_2	δ_1	δ_0

Gruppentafel der Diedergruppe D_3

Weitere Beispiele

1. Verwendet man an Stelle eines gleichseitigen Dreiecks ein regelmässiges n-Eck als Ausgangsfigur, so gibt es n Drehungen und n Spiegelungen, welche das

[1] Arthur Cayley, 1821–1895, engl. Mathematiker

n-Eck in sich überführen. Sie bilden die Trägermenge der (aus $2n$ Elementen bestehenden) *Diedergruppe* D_n.

2. Die Menge $(\mathbb{Z}, +, 0)$ der ganzen Zahlen mit der gewöhnlichen Addition von ganzen Zahlen als Gruppenverknüpfung und der Zahl Null (0) als neutralem Element.

3. Die Menge $(\mathbb{Q}, *, 1)$ der Brüche (d.h. der positiven rationalen Zahlen) mit der gewöhnlichen Multiplikation von Brüchen als Gruppenverknüpfung und der Zahl Eins (1) als neutralem Element.

4. Die Menge $(Pot(2, n), *, 1)$ (mit $Pot(2, n) = 2^x, x \in \mathbb{Z}$) mit der gewöhnlichen Multiplikation von Brüchen als Gruppenverknüpfung und der Zahl Eins 1 ($= 2^0$) als neutralem Element.

5. Die Menge $\mathbb{Z}/n\mathbb{Z}$ (vgl. [Ziegenbalg 2015]) der Restklassen *modulo* n bildet zusammen mit der Restklassenaddition eine endliche, kommutative Gruppe mit neutralem Element $\overline{0}$.

   Definition: Für die natürliche Zahl n und die ganzen Zahlen a und b ist definiert: "a ist *kongruent* zu b modulo n", wenn n ein Teiler von $b - a$ ist.

   In Zeichen: $a = b\ (modulo\ n)$ oder $a = b\ (mod\ n)$ oder $a = b\ (n)$
   oder auch: $a \equiv b\ (modulo\ n)$ oder $a \equiv b\ (mod\ n)$ oder $a \equiv b\ (n)$

   Beispiel $n = 6$:

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{5}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$

Gruppentafel der zyklischen Gruppe $\mathbb{Z}_6$

6. **Tetraeder-Drehgruppe**[2]: Die Menge der (physich im 3-dimensionalen Euklidischen Raum realisierbaren) räumlichen Bewegungen (Drehungen)), die

[2] Tetraeder: Vierflächner oder Vierflach
Bei der (vollen) Tetraedergruppe kommen noch "Spiegelungen" hinzu, die sich aber nicht als räumliche Drehungen, sondern nur in der Permutationsdarstellung realisieren lassen.

ein (regelmäßiges) *Tetraeder* in sich überführen, zusammen mit der Hintereinanderausführung von Abbildungen als Gruppenverknüpfung. Diese Gruppe besitzt die folgenden 12 Elemente:

- Die Drehungen jeweils um die Achse durch eine Ecke und den Schwerpunkt der gegenüberliegenden Seite um 60 bzw. 120 Grad.
  Dies sind 8 ($= 4 \cdot 2$) Drehungen (eine davon ist in der Abbildung anhand der roten Achse dargestellt).
- Die Drehungen jeweils um die Achse durch die Seitenmitten zweier gegenüberliegender Seiten um 180 Grad. Dies sind 3 Drehungen (eine davon ist in der Abbildung anhand der blauen Achse dargestellt).
- Die identische Abbildung (neutrales Element).

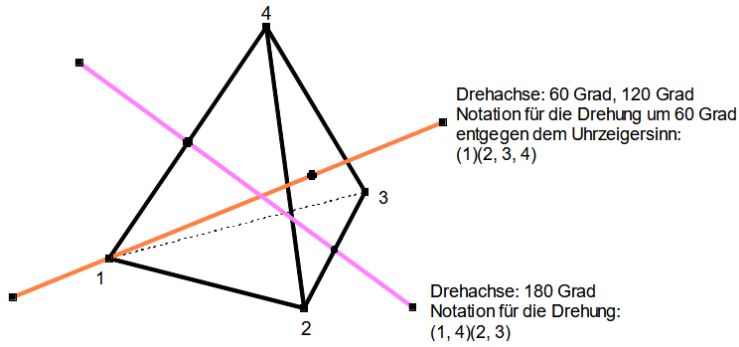

Abbildung 1.2: Räumliche Drehungen eines Tetraeders

***Aufgabe* 1.1**
Stellen Sie die Gruppentafel zu der soeben beschriebenen Gruppe auf.

1.3 Permutationen

Ist M eine beliebige Menge, so ist die Menge der Permutationen von M (= Menge der bijektiven Abbildungen von M auf sich) eine Gruppe mit der Hintereinanderausführung von Abbildungen als Gruppenverknüpfung und der identischen Abbildung als neutralem Element.

Permutationen *endlicher* Mengen können in der Form von Zuordnungstabellen dargestellt werden; die Permutation σ z.B. in der Form

$$\sigma = \begin{pmatrix} a & b & c & d & e & f & g & h & j & k \\ f & e & c & k & b & g & j & h & a & d \end{pmatrix} \tag{1.1}$$

Dabei ist $\sigma(a) = f,\ \sigma(b) = e,\ \sigma(c) = c,\ \sigma(d) = k,\ \sigma(e) = b,$
$\sigma(f) = g,\ \sigma(g) = j,\ \sigma(h) = h,\ \sigma(j) = a,\ \sigma(k) = d.$

Permutationen lassen sich auch in der *Zyklenschreibweise* darstellen; im obigen Beispiel: $\sigma = (a, f, g, j)(b, e)(c)(d, k)(h)$.

Ein Element x mit $\sigma(x) = x$ heißt *Fixpunkt* der Permutation σ. Permutationen ohne Fixpunkte heissen *fixpunktfrei*. Zyklen der Form (x) stellen Fixpunkte dar. Zyklen der Länge 1 werden meist weggelassen; für das obige Beispie gilt also: $\sigma = (a, f, g, j)(b, e)(d, k)$.

Bemerkung: Da es bei den Permutationen einer Menge M aus mathematischer Sicht im wesentlichen nur auf die Elementezahl der Menge M ankommt, werden wir uns im Folgenden mit Permutationen der Standard-Mengen $\{1, 2, 3, \ldots, n\}$ befassen.

Mit S_n wird die Gruppe aller Permutationen der Menge $\{1, 2, 3, \ldots, n\}$ bezeichnet. Sie heißt die *symmetrische Gruppe* über der Menge $\{1, 2, 3, \ldots, n\}$.

Satz 1.1 $|S_n| = n!$ *(Beweis: Übung)*

Satz 1.2 *Die Gruppe D_3 ist strukturgleich (isomorph) zur Gruppe S_3.*

***Aufgabe* 1.2** Auch wenn bisher keine formale Definition des Begriffs "strukturgleich" gegeben wurde, erläutern Sie, was damit gemeint sein könnte und beweisen Sie den Satz.

Definition: Zyklen der Länge 2 heißen *Transpositionen.*

Es gilt der **Satz**: Jede Permutation lässt sich als Produkt von Transpositionen darstellen.

Demonstration anhand eines Beispiels

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 6 & 5 & 3 & 8 & 2 & 7 & 9 & 10 & 1 & 4 \end{pmatrix} \tag{1.2}$$

Die entsprechende Zyklendarstellung lautet dann:
(1 6 7 9) (2 5) (3) (4 8 10)

Dies lässt sich wie folgt in ein Verknüpfungs-Produkt von Transpositionen auflösen:
(1 6 7 9) = (1 6)(6 7)(7 9)
(4 8 10) = (4 8)(8 10)
also
(1 6 7 9) (2 5) (3) (4 8 10) = (1 6)(6 7)(7 9)(4 8)(8 10)

Definition: Jede Eine Permutation heisst *gerade*, wenn sie sich als Produkt einer *geraden Anzahl von Transpositionen* darstellen lässt.

Bemerkung: Zur Reihenfolge der Ausführung von Permutationen[3]

Bei der Reihenfolge der Ausführung von Permutationen $\sigma \circ \tau$ gibt es unterschiedliche Praktiken. Bei einigen Autoren bedeutet dies: Man führe ("von rechts nach links") zuerst die Permutation τ aus, dann die Abbildung σ. Bei anderen Autoren ist es umgekehrt. Für jede dieser Praktiken gibt es gute Gründe. Es geht immer darum, wie die Hintereinanderausführung

$$\sigma \circ \tau$$

zu interpretieren ist.

* Verfahren "von rechts nach links": $(\sigma \circ \tau)(x) = \sigma(\tau(x))$ legt nahe, dass $\sigma \circ \tau$ als "zuerst τ, dann σ" zu interpretieren ist. Bei diesem Verfahren wird also die übliche Leserichtung durch eine Verschränkung der Symbole σ und τ unterbrochen.

* Verfahren "von links nach rechts": $(\sigma \circ \tau)(x)$ bedeutet dann "zuerst σ dann τ", also $(\sigma \circ \tau)(x) = \tau(\sigma(x))$. Auch hier tritt ein Verschränkungseffekt auf.
Beim zweiten Verfahren lässt sich die "Verschränkung" vermeiden, indem man es im Zusammenhang mit der "umgekehrten polnischen Notation (UPN)" verwendet. Beim UPN-Verfahren schreibt man Funktionen bzw. Funktionsanwendungen nicht wie sonst oft in der Form $f(x)$ sondern in der Form xf. In der Konsequenz schreibt man dann statt $(\sigma \circ \tau)(x)$ in UPN $x(\sigma \circ \tau)$, und das lässt sich ohne Verschränkungsprobleme und klammerfrei[4] als $x\sigma\tau$ darstellen.

Definition 1.2 In der symmetrischen Gruppe S_4 gibt es 12 gerade Permutationen (Transpositionen). Sie bilden die Untergruppe A_4 der der symmetrischen Gruppe (zum Begriff der Untergruppe siehe Abschnitt 2.1). Man nennt sie die „alternierende Gruppe" A_4.

***Aufgabe* 1.3** Zeigen Sie: Die alternierende Gruppe A_4 ist isomorph zur Tetraeder-Drehgruppe.

1.4 Die Eindeutigkeit der inversen Elemente

Satz 1.3 *(Eindeutigkeit des inversen Elements)*
Es sei G eine Gruppe und $x \in G$. Ist y ein zu x inverses Element und z ein Element von G mit der Eigenschaft $x \circ z = e$, so ist $y = z$.

Beweis: $y = y \circ e = y \circ (x \circ z) = (y \circ x) \circ z = e \circ z = z$

Bemerkung: Ein zu x inverses Element y ist also *eindeutig* bestimmt. Es heißt somit **das** Inverse von x und wird (in funktionaler Schreibweise) in der Form x^{-1} geschrieben. Es gilt also $x \circ x^{-1} = x^{-1} \circ x = e$.

[3] Zur Verdeutlichung der Sachlage wird im Rahmen dieser Bemerkung das Verknüpfungszeichen $\circ$ bewusst verwendet.

[4] Klammern verursachen bei Computerprogrammen in der Regel, dass ein spezieller Speicher für die Zwischenergebnisse angelegt werden muss. Das kostet Speichplatz und Zeit (für das Umspeichern). Programmiersprachen, die auf hochgradige Effizienz hin konzipiert sind, wie z.B. Forth, verwenden deshalb gern die umgekehrte polnische Notation.

Im Falle der additiven Schreibweise $(G, +, 0)$ wird das Inverse von x in der Form $-x$ geschrieben. Es gilt dann $x + (-x) = (-x) + x = 0$.

***Aufgabe* 1.4** Es sei G eine Gruppe und $x, y \in G$. Zeigen Sie $(x \circ y)^{-1} = y^{-1} \circ x^{-1}$.

Definition: (aggregierende Schreibweisen)

(i) In multiplikativer Schreibweise: *Potenzierung*
Gruppe: $(G, \circ, e)$; meist mit $e = 1$
$x^1 := x, x^2 := x \circ x, x^3 := x \circ x \circ x, \ldots, x^n := x \circ x^{n-1}, \ldots$
$x^0 = e \quad (= 1)$
$x^{-2} = x^{-1} \circ x^{-1}, x^{-3} = x^{-1} \circ x^{-2}, \ldots, x^{-n} := x^{-1} \circ x^{-(n-1)}, \ldots$

(ii) In additiver Schreibweise: *Vervielfachung*
Gruppe: $(G, +, e)$; meist mit $e = 0$
$1 \cdot x = x, 2 \cdot x = x + x, 3 \cdot x = x + x + x, \ldots, n \cdot x = x + (n-1) \cdot x, \ldots$
$0 \cdot x = e \quad (= 0)$
$-2 \cdot x = (-x) + (-x), -3 \cdot x = (-x) + (-x) + (-x), \ldots,$
$-n \cdot x = (-x) + (-(n-1)) \cdot x, \ldots$

Bemerkung: Beim Potenzieren von (gewöhnlichen) Zahlen entsteht immer wieder die Frage: Warum ist $a^0 = 1$ (und nicht etwa, wie manchmal vermutet, gleich 0)? Für eine angemessene Beantwortung dieser Frage ist die Beschäftigung mit dem *Permanenzprinzip* von Hankel[5] hilfreich; siehe z.B.:

https://jochen-ziegenbalg.github.io/materialien/Manuskripte/Zum-Permanenzprinzip.pdf

1.5 Strukturerhaltende Abbildungen

Die Mathematik des 20. Jahrhunderts war dadurch charakterisiert, dass sie sich besonders der strukturellen Merkmale der untersuchten Objekte annahm. Mit den Strukturen selber rückten dabei fast automatisch die strukturerhaltenden Abbildungen in das Blickfeld. In der Algebra werden derartige strukturerhaltende Abbildungen als *Homomorphismen* bezeichnet. Ist ein Homomorphismus zudem noch bijektiv, dann wird er als *Isomorphismus* bezeichnet.

Definition 1.3 Es seien $(G, \circ)$ und $(H, \cdot)$ beliebige Gruppen und $f : G \to H$ eine Abbildung von G in H. Wenn für alle $x, y \in G$ gilt

$$f(g \circ h) = f(g) \cdot f(h) \text{ und } f(g^{-1}) = f(g)^{-1}$$

dann nennt man f einen (Gruppen-) *Homorphismus*[6].

Ist f darüber hinaus bijektiv, so nennt man f einen *Isomorphismus*[7]. Wenn es einen Isomorphismus zwischen den Gruppen G und H gibt, dann werden die Gruppen "isomorph" genannt; im Zeichen $G \cong H$.

[5] Hermann Hankel, 1838–1873, deutscher Mathematiker
[6] homomorph: strukturerhaltend; von ähnlicher Gestalt
Homomorphismus: verknüpfungstreue Abbildung
[7] isomorph: strukturerhaltend; von gleicher Gestalt

Bemerkung: In der Algebra pflegt man, isomorphe Objekte nicht mehr zu unterscheiden; sie werden dort als "gleich" angesehen. So bezieht sich z.B. die Klassifikation der "einfachen" Gruppen (siehe Definition 5.2) jeweils auf einen Isomorphietyp von jeder Gruppe.

***Aufgabe* 1.5** $f : G \to H$ sei ein Homomorphismus. Zeigen Sie:
* $f(1) = 1$
* $f(x^{-1}) = f(x)^{-1}$

Beispiele

1. Die "Verdreifachungs-Abbildung" $f : (\mathbb{Z}, +) \to (\mathbb{Z}, +) : \quad f(x) := 3x$ ist ein Homomorphismus, aber kein Isomorphismus (Übung).
2. Die Verdreifachungs-Abbildung $f : \mathbb{R} \to \mathbb{R} : \quad f(x) := 3x$ ist ein Isomorphismus. (Übung)
3. Die Menge $Z2 := 0, 1$ ist mit der folgendermassen definierten Verknüpfung + eine Gruppe: $0 + 0 = 0 \quad 0 + 1 = 0 \quad 1 + 0 = 1 \quad 1 + 1 = 0$.
   Die Abbildung $f : (\mathbb{Z}, +) \to (Z2, +)$ sei wie folgt definiert:
   $$f(x) := \begin{cases} 0, & \text{wenn x eine gerade Zahl ist} \\ 1, & \text{wenn x eine ungerade Zahl ist} \end{cases}$$
   Zeigen Sie: f ist ein Homomorphismus.
4. Es sei $\mathbb{R}^+ := \{x \in \mathbb{R} : x > 0\}$ die Menge der positiven reellen Zahlen.
   Für die Gruppen $G = (\mathbb{R}, +)$ und $H = (\mathbb{R}^+, \cdot)$ ist die Abbildung
   $\Phi : G \to H$ mit $\Phi(x) = 2^x$ ein Isomorphismus, denn
   • Φ ist verknüpfungstreu: $\Phi(x + y) = 2^{x+y} = 2^x \cdot 2^y = \Phi(x)\Phi(y)$
   • Φ ist injektiv:
   Aus $\Phi(x) = \Phi(y)$ folgt $2^x = 2^y$ und somit $2^{x-y} = 1$.
   Daraus folgt $x - y = 0$ und somit (wie zu zeigen war): $x = y$
   • Φ ist surjektiv:
   Es sei $y \in \mathbb{R}^+$.
   Mit $\quad x := \log_2 y \quad$ ist dann $\quad \Phi(x) = 2^x = 2^{\log_2 y} = y$.
   Also ist Φ ein Isomorphismus

1.6 Die Links-Multiplikation

Definition: Sei $a \in G$. Die Abbildung $\lambda_a : G \to G$ mit $\lambda_a(x) = a \cdot x$ heißt *Links-Multiplikation* (genauer eigentlich: Links-Verknüpfung) mit dem Element a.

Beispiele:
Gruppe: $(\mathbb{Q}, \cdot, 1)$; $\quad a = 2$: $\quad \lambda_2(x) = 2 \cdot x$
Gruppe: $(\mathbb{Z}, +, 0)$; $\quad a = 17$: $\quad \lambda_{17}(x) = 17 + x$

Satz 1.4 *Die Links-Multiplikation ist bijektiv.*

Beweis: Die Umkehrabbildung von λ_a ist die durch das Inverse von a gegebene Links-Multiplikation $\lambda_{a^{-1}}$. Für alle $x \in G$ gilt also $\lambda_a(\lambda_{a^{-1}}(x)) = \lambda_{a^{-1}}(\lambda_a(x)) = x$.

Entsprechend ist der Begriff der Rechts-Multiplikation ρ_a definiert:
$\rho_a : G \to G$ mit $\rho_a(x) := x \cdot a$.

***Aufgabe* 1.6**

- Zeigen Sie anhand von geeigneten Beispielen: Die Links-Multtiplikation ist in der Regel kein Homomorphismus.
- Untersuchen Sie, unter welchen Bedingungen die Links-Multiplikation ein Homomorphismus ist.

2 Untergruppen und Nebenklassen

2.1 Untergruppen

Definition: Sei $(G, \circ, e)$ eine Gruppe und U eine Teilmenge von G mit den Eigenschaften:

- $e \in G$
- Für alle $x, y \in U$ gilt $x \circ y \in U$.
- Für alle $x \in U$ ist $x^{-1} \in U$.

Dann heißt U *Untergruppe* von G; im Zeichen: $U \leq G$.

Bemerkungen:

- Die Menge U ist also eine Untergruppe von G, wenn sie das neutrale Element von G enthält und bezüglich der Gruppenverknüpfung von G und der Inversenbildung abgeschlossen ist.
- Mit anderen Worten: Ist $(U, \circ, e)$ mit der auf U eingeschränkten Verknüpfung von G und mit dem neutralen Element $e \in G$ ebenfalls eine Gruppe, so ist U eine Untergruppe von G.

Beispiele:

Wir betrachten die Gruppe D_3 der Deckabbildungen eines gleichseitigen Dreiecks (siehe Definition des Gruppenbegriffs).

Mit Hilfe ihrer Gruppentafel ermitteln wir die folgenden Untergruppen:

- die "trivialen" Untergruppen: $\{\delta_0\}$ und D_3 selbst,
- die Untergruppen der Ordnung 2: $\{\sigma_1, \delta_0\}$, $\{\sigma_2, \delta_0\}$ und $\{\sigma_3, \delta_0\}$,
- die Untergruppe der Ordnung 3: $\{\delta_0, \delta_1, \delta_2\}$.

***Aufgabe* 2.1**
Zeigen Sie, dass dies alle Untergruppen von D_3 sind. (Hinweis: Nehmen Sie an, dass ein beliebiges Element x in einer Untergruppe U von enthalten ist und ziehen Sie Schlüsse daraus, welche weiteren Elemente noch in U enthalten sein müssen, damit die Untergruppenkriterien erfüllt sind.)

***Aufgabe* 2.2**

(a) Ermitteln Sie alle Untergruppen der Gruppe aus Beispiel 6.
(b) Ermitteln Sie alle Untergruppen der Restklassengruppen für n = 5, 6, 8 und 12.

Untergruppen von Permutationsgruppen

Wiederholung: Zyklen der Länge 2 heißen *Transpositionen.*
Eine Permutation heisst *gerade*, wenn sie sich als Produkt einer geraden Anzahl von Transpositionen darstellen lässt.

Satz 2.1 *Die Gesamtheit A_n der geraden Transpositionen über der Menge $\{1, 2, 3, \ldots, n\}$ ist (mit der Hintereinanderausführung von Abbildungen) eine Gruppe; genauer: eine Untergruppe von S_n.*
Beweis: Übung

Definition: Die Gruppe aller geraden Permutationen von n Elementen wird als *alternierende Gruppe* A_n bezeichnet.

***Aufgabe* 2.3** Ermitteln Sie A_3 und A_4.

***Aufgabe* 2.4** Zeigen Sie: A_n hat die halbe Ordnung von S_n: $|S_n| = 2 \cdot |A_n|$.

2.2 Nebenklassen

Definition: Es sei G eine Gruppe, U eine Untergruppe von G und a ein beliebiges Element von G. Dann heißt die Menge
$a \circ U := \{a \circ x / x \in U\}$
die durch a gegebene Links-Nebenklasse (engl. left coset) von U. Entsprechend ist der Begriff der Rechts-Nebenklasse definiert durch
$U \circ a := \{x \circ a / x \in U\}$.

Bei multiplikativ geschriebenen Gruppen schreibt man meist kurz aU an Stelle von $a \circ U$ bzw. Ua an Stelle von $U \circ a$.

Bemerkung: Offensichtlich ist $aU = \{\lambda_a(x) : x \in U\} =: \lambda_a(U)$.

Beispiele: Wir betrachten die Gruppe D_3 der Deckabbildungen eines gleichseitigen Dreiecks (s.o.). Die Links-Nebenklassen der Untergruppe $U := \{\sigma_1, \delta_0\}$ sind:

- $\delta_0 \circ U = \delta_0 \circ \{\sigma_1, \delta_0\} = \{\sigma_1, \delta_0\}$
- $\delta_1 \circ U = \delta_1 \circ \{\sigma_1, \delta_0\} = \{\sigma_2, \delta_1\}$
- $\delta_2 \circ U = \delta_2 \circ \{\sigma_1, \delta_0\} = \{\sigma_3, \delta_2\}$
- $\sigma_1 \circ U = \sigma_1 \circ \{\sigma_1, \delta_0\} = \{\delta_0, \sigma_1\}$
- $\sigma_2 \circ U = \sigma_2 \circ \{\sigma_1, \delta_0\} = \{\delta_1, \sigma_2\}$
- $\sigma_3 \circ U = \sigma_3 \circ \{\sigma_1, \delta_0\} = \{\delta_2, \sigma_3\}$

Die Nebenklassen stimmen paarweise überein; es gibt also drei Links-Nebenklassen zur Untergruppe U von G.

***Aufgabe* 2.5**
Geben Sie die Links-Nebenklassen der restlichen Untergruppen von G an.

***Aufgabe* 2.6**

(a) Ermitteln Sie die Links-Nebenklassen aller Untergruppen der Gruppe aus Beispiel 6 (Seite 5).

(b) Ermitteln Sie die Links-Nebenklassen aller Untergruppen der Restklassengruppen $\mathbb{Z}/n\mathbb{Z}$ für $n = 5, 6, 8, 12$.

(c) Führen Sie Entsprechendes für die Rechts-Nebenklassen durch.

Satz 2.2 *(Eigenschaften von Nebenklassen)*
Es sei G eine Gruppe und U eine Untergruppe von G. Dann gilt

1. *Für alle $a, b \in G$ und $x, y \in U$ gilt: Aus $ax = by$ folgt $aU = bU$.*
2. *Für alle $x \in G$ gilt: $x \in U \iff xU = U$.*
3. *Die Nebenklasse xU ist stets gleichmächtig zu U.*
4. *Für alle $x, y \in G$ gilt: $xU = yU \iff y^{-1}x \in U$*
5. *Für alle x und $y \in G$ gilt $xU \cap yU = \emptyset$ oder $xU = yU$.*
   D.h.: Je zwei Nebenklassen von G sind entweder elementefremd oder gleich.
6. *$G = \dot{\bigcup}_{x \in G} xU$. D.h. G ist die disjunkte Vereinigung der Nebenklassen von U.*

Beweis:

1. Aus $ax = by$ folgt $a = byx^{-1}$. Also gilt für ein beliebiges $w \in U$: $aw = byx^{-1}w \in bU$ und somit, da w ein beliebiges Element von U war: $aU \subseteq bU$. Umgekehrt folgt aus einer symmetrischen Argumentation in a und b: $bU \subseteq aU$. Insgesamt gilt somit $aU = bU$.
2. "$\Rightarrow$": Es sei $x \in U$. Dann ist (wegen der Abgeschlossenheitseigenschaft von U) $xU = \{xy : y \in U\} \subseteq U$. Weiterhin kann jedes Element $t \in U$ in der Form $t = xy$ (mit einem geeigneten Element $y \in U$) geschrieben werden. Man verwende dazu $t = x^{-1}y$. Also ist $xU = U$.
   "$\Leftarrow$": Es sei nun $xU = U$. Dann ist insbesondere $xe \in U$, also $x \in U$.
3. Dies folgt aus der Tatsache, dass die Links-Multiplikation als Abbildung bijektiv ist.
4. Übung
5. Angenommen $xU \cap yU \neq \emptyset$. Dann gibt es ein Element z mit $z \in xU \cap yU$. Es gibt also Elemente $u, v \in U$ mit $z = xu = yv$. Daraus folgt $x = xuu^{-1} = yvu^{-1}$ und somit $x \in yU$. Hieraus folgt sofort $xU \subseteq yU$. Aus Symmetriegründen folgt ebenso $yU \subseteq xU$ und insgesamt ist $xU = yU$.
6. Für jedes $x \in G$ gilt $x \in xU$.

Bemerkung: Die Eigenschaften (v) besagt, dass verschiedene Nebenklassen von U disjunkt sind. Die Eigenschaften (v) und (vi) besagen, dass die Gesamtheit der Nebenklassen von U eine Zerlegung von G darstellt.

Satz 2.3 *Folgerung*
Es sei G eine Gruppe und U eine Untergruppe von G. Dann gilt: G ist die disjunkte Vereinigung der (gleichmächtigen) Nebenklassen von U.

$$G = \dot{\bigcup}_{x \in G} xU \tag{2.1}$$

2.3 Der Index einer Untergruppe

Definition: Es sei G eine Gruppe und U eine Untergruppe von G. Die Anzahl der Links-Nebenklassen von U in G heißt der *Index* von U in G. Im Zeichen: $|G : U|$.

Beispiel: Die additive Gruppe $Z_{12} := \mathbb{Z}/12\mathbb{Z}$ der Restklassen *modulo* 12.

+	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$	$\overline{11}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$	$\overline{11}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$	$\overline{11}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$	$\overline{11}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$	$\overline{11}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$	$\overline{11}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{5}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$	$\overline{11}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{6}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$	$\overline{11}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{7}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$	$\overline{11}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{8}$	$\overline{8}$	$\overline{9}$	$\overline{10}$	$\overline{11}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$
$\overline{9}$	$\overline{9}$	$\overline{10}$	$\overline{11}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$
$\overline{10}$	$\overline{10}$	$\overline{11}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$
$\overline{11}$	$\overline{11}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$

Gruppentafel der additiven Gruppe Z_{12}

Eine der Untergruppen von Z_{12} ist $\{0, 3, 6, 9\}$. Die Links-Nebenklassen von U sind: $0+U = \{0, 3, 6, 9\}, 1+U = \{1, 4, 7, 10\}$ und $2+U = \{2, 5, 8, 11\}$. Plausibilitäts-Argument: Es gibt 3 (Links-) Nebenklassen zu je 4 Elementen; 3 * 4 = 12.

Eine disjunkte Vereinigungen einer Menge wird auch als *Zerlegung* bezeichnet.

Satz 2.4 *(Satz von Lagrange[8])*
Es sei G eine endliche Gruppe und U eine Untergruppe von G.
Dann gilt: $|G| = |G : U| \cdot |U|$.
(Insbesondere gilt: Die Ordnung der Untergruppe ist stets ein Teiler der Gruppenordnung.)

Beweis: Für jede Gruppe G gilt $G = \dot{\bigcup}_{x \in G} xU$. Da G eine endliche Gruppe ist, gibt es nur endlich viele verschiedene Links-Nebenklassen von U; diese seien mit $g_1U, g_2U, g_3U \ldots, g_nU$ bezeichnet. Also ist (wegen der Disjunktheits-Eigenschaft[9] der Links-Nebenklassen)
$|G| = |g_1U \,\dot\cup\, g_2U \,\dot\cup\, g_3U, \,\dot\cup, \ldots, \,\dot\cup\, g_nU| = |g_1U| + |g_2U| + |g_3U| + \ldots + |g_nU|$.
Da alle Links-Nebenklassen von U gleichmächtig sind, folgt daraus: $|G| = n \cdot |U|$.
Da n als die Anzahl der Links-Nebenklassen von U in G (also als der Index von U in G) definiert war, folgt $|G| = |G : U| \cdot |U|$.

Folgerung und Bemerkung zur und Motivation der Bezeichnungsweise: $|G : U| = \frac{|G|}{|U|}$.

2.4 Erzeugende Elemente und zyklische Gruppen

Satz 2.5 *(Durchschnittsbildung und Untergruppen):*

[8] Joseph-Louis de Lagrange, 1736–1813, franz. Mathematiker, primäre Wirkungsorte (Mathematik): Berlin und Paris

[9] Das Symbol $\dot\cup$ soll "disjunkte Vereinigung" andeuten.

1. *Der Durchschnitt zweier Untergruppen einer Gruppe G ist eine Untergruppe von G.*
2. *Der Durchschnitt beliebig vieler Untergruppen einer Gruppe G ist eine Untergruppe von G.*

Beweis: Übung

Definition 2.1 Es sei G eine Gruppe und M eine Teilmenge von G. Weiterhin sei

$$D = \bigcap_{M \subseteq U \leq G} U$$

der Durchschnitt aller Untergruppen U von G, welche die Menge M enthalten. Dann ist D ebenfalls eine Untergruppe von G; sie wird als die von der Menge M *erzeugte* Untergruppe bezeichnet; Im Zeichen: $<M>$.

Besteht die Menge M aus endlich vielen Elementen so sagt man, die Untergruppe $<M>$ ist *endlich erzeugt*.

Besteht die Menge M nur aus einem Element x, ist also $M = \{x\}$, so schreibt man auch kurz $<x>$ an Stelle von $<\{x\}>$ und bezeichnet $<x>$ als die von dem Element x erzeugte Untergruppe.

Gruppen, die von einem Element x erzeugt sind, heißen *zyklische* Gruppen.

Bemerkung: Es sei G eine zyklische Gruppe; etwa $G = <x>$. Aufgrund der Abgeschlossenheit von G, muss G alle Produkte der Form $x, x^2, x^3, \ldots, x^n, \ldots$ sowie das neutrale Element e enthalten. In endlichen Gruppen sind diese Element jedoch nicht alle verschieden. Es muss also ein $n \in \mathbb{N}$ geben mit der Eigenschaft $x^n = e$. Das kleinste derartige n ist die Ordnung der zyklischen Gruppe $<x>$.

Beispiele:

1. Die Menge der rationalen Zahlen (mit der gewöhnlichen Multiplikation) enthält die zyklische Gruppe $<2> = \{2^x : x \in \mathbb{Z}\}$; m.a.W.: die (multiplikativ geschriebene) zyklische Gruppe besteht aus den Elementen $2, 2^2, 2^3, \ldots, 2^n, \ldots$ sowie $2^{-1}, 2^{-2}, 2^{-3} \ldots, 2^{-n}, \ldots$ und dem neutralen Element $2^0 (= 1)$.
2. Die Menge der ganzen Zahlen (mit der gewöhnlichen Addition) enthält die zyklische Gruppe $<6>$ der durch 6 teilbaren ganzen Zahlen; m.a.W.: die (additiv geschriebene) zyklische Gruppe $<6>$ besteht aus den Elementen $6, 12, 18, 24, \ldots$, sowie $-6, -12, -18, -24, \ldots$ und dem neutralen Element 0.
3. Die zyklische Gruppe der ebenen Drehungen eines regelmäßigen 8-Ecks besteht aus den 8 folgenden Drehungen (etwa im Uhrzeigersinn):
   δ_1 = Drehung um 45 *Grad*
   δ_2 = Drehung um 90 *Grad*
   δ_3 = Drehung um 135 *Grad*
   ...
   δ_6 = Drehung um 270 *Grad*
   δ_7 = Drehung um 315 *Grad*
   δ_8 = Drehung um 360 *Grad* = Drehung um 0 *Grad* =: δ_0
   (letzteres ist das neutrale Element bzw. die identische Abbildung)
4. Die (additive) Gruppe $\mathbb{Z}/n\mathbb{Z}$ der Restklassen *modulo* n ist eine zyklische Gruppe, die z.B. von dem Element (der Restklasse) $\overline{1}$ erzeugt wird.
   Für $n = 6$ ist z.B.: $\mathbb{Z}/6\mathbb{Z} = \{\overline{1},\ \overline{1}+\overline{1},\ \overline{1}+\overline{1}+\overline{1},\ \overline{1}+\overline{1}+\overline{1}+\overline{1},\ \overline{1}+\overline{1}+\overline{1}+\overline{1}+\overline{1},\ \overline{1}+\overline{1}+\overline{1}+\overline{1}+\overline{1}+\overline{1}\}$ bzw. $\mathbb{Z}/6\mathbb{Z} = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}\} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$ (mit $\overline{6} = \overline{0}$)

Bemerkung: Es sei G eine endliche zyklische Gruppe der Ordnung n; etwa $G = <x> = \{x, x^2, x^3, x^4, x^5, x^6\}$. Dann gilt $x^n = e$ und $x^{-1} = x^{n-1}$.

Definition 2.2
Sei G eine Gruppe und $x \in G$. Als *Ordnung* des Elements x (im Zeichen: $ord(x)$) wird die kleinste positive natürliche Zahl n bezeichnet, für die die Gleichung $x^n = e$ gilt.
Mit anderen Worten: Die Ordnung des Elements x ist gleich der Ordnung der Untergruppe $<x>$ von G; im Zeichen: $ord(x) = | <x> |$.

***Aufgabe* 2.7**
G sei eine Gruppe, in der jedes Element höchstens die Ordnung 2 hat. Zeigen Sie: G ist kommutativ.

Bemerkung: Die wohl bekannteste Gruppe mit dieser Eigenschaft ist die *Kleinsche Vierergruppe.*

***Aufgabe* 2.8**
Informieren Sie sich über die Kleinsche Vierergruppe.

Satz 2.6 *(Ordnung von Gruppenelementen):*
Sei G eine endliche Gruppe der Ordnung n und x ein beliebiges Element von G. Dann gili:

(i) Die Ordnung des Elements x ein Teiler der Gruppenordnung: $ord(x) \mid |G|$.
(ii) $x^n = e$

Beweis: (i) Dies ist eine unmittelbare Folgerung aus dem Satz von Lagrange.
(ii) Es sei k der Index der Untergruppe $<x>$ in G und r die Ordnung von x. Nach dem Satz von Lagrange gilt $|G| = |G : <x>| \cdot ord(x)$ bzw. $n = k \cdot r$. Mit diesen Bezeichnungen gilt: $x^n = x^{k \cdot r} = (x^r)^k = e^k = e$.

Folgerung 1 Jede zyklische Gruppe ist kommutativ.

Folgerung 2 Jede Gruppe von Primzahlordnung ist zyklisch.

3 Gruppen primer Restklassen

Bezeichnungen und Basiswissen: siehe [Ziegenbalg 2015]

Satz 3.1 *(Gruppen primer Restklassen)*
Es sei $R_n := \mathbb{Z}/n\mathbb{Z}$ die Menge der Restklassen modulo n. Die Menge $G_n \subseteq R_n$ sei wie folgt definiert: $G_n := \{x \in R_n : ggT(x, n) = 1\}$. G_n enthält also genau die Restklassen, deren Repräsentant teilerfremd zu n ist. Dann bildet G_n mit der Restklassenmultiplikation eine Gruppe. Sie wird als die Gruppe der primen Restklassen modulo n bezeichnet.

Beweis:

- Zum neutralen Element: Das neutrale Element $\overline{1}$ ist offensichtlich in R_n enthalten.
- Zur multiplikativen Abgeschlossenheit: Es ist zu zeigen: Sind $\overline{a}$ und $\overline{b}$ Elemente von G_n , dann ist auch $\overline{a} \cdot \overline{b}$ ein Element von G_n. Dazu ist zu zeigen: Ist $ggT(a, n) = 1$ und $ggT(b, n) = 1$, dann ist auch $ggT(a \cdot b, n) = 1$. Dies folgt aber unmittelbar aus dem Satz von der eindeutigen Primfaktorzerlegung.

- Zur Abgeschlossenheit bezüglich der Inversenbildung: Zu zeigen: Jedes Element $\overline{a}$ besitzt ein Inverses. Sei also $ggT(a,n) = 1$. Dann gibt es nach dem Satz von der Vielfachsummendarstellung ganze Zahlen x und y mit der Eigenschaft $1 = x \cdot a + y \cdot n$. Man findet diese ganzen Zahlen x und y mit Hilfe des erweiterten Euklidischen Algorithmus (Berlekamp Algorithmus).
  In R_n bedeutet dies $\overline{1} = \overline{x} \cdot \overline{a}$. Es ist noch zu zeigen, dass x teilerfremd zu n ist. Wäre es dies nicht, so hätte erst recht das Produkt $x \cdot a$ einen gemeinsamen Primfaktor mit n und könnte nicht kongruent zu 1 *modulo* n sein. Das mit dem Berlekamp Algorithmus zu findende Element $\overline{x}$ liegt also in G_n und ist somit das Inverse von $\overline{a}$.

Folgerungen

- Die Gruppe der primen Restklassen *modulo* n hat per Definition die Ordnung $\varphi(n)$, wo φ die *Eulersche Funktion* ("Totientenfunktion") ist.
- Ist p eine Primzahl, so hat die Gruppe der primen Restklassen *modulo* p die Ordnung $p - 1$.

Beweis: Dies sind nur direkte Umsetzungen der Definition der Eulerschen Totientenfunktion [vgl. z.B. Ziegenbalg 2015].

4 Die Sätze von Fermat, Euler und Wilson

Satz 4.1 *(Fermat[10])*
Es sei p ein Primzahl und a eine ganze Zahl, die nicht von p geteilt wird. Dann gilt $a^{p-1} = 1 \,(mod\, p)$.

Satz 4.2 *(Euler[11])*
Es sei n eine ganze Zahl und a eine zu n teilerfremde ganze Zahl. Dann gilt $a^{\varphi(n)} = 1 \,(mod\, n)$.

Beweis: Die beiden letzten Sätze folgen unmittelbar aus dem Satz von Lagrange (bzw. dem Satz über die Ordnung von Gruppenelementen), angewandt auf die Gruppe der primen Restklassen.

Satz 4.3 *(Wilson[12]) Für jede natürliche Zahl n gilt:*

$$n \text{ ist eine Primzahl} \iff (n-1)! = -1 \,(mod\, n) \tag{4.1}$$

Beweis: (i) Es sei n eine Primzahl. Die (zyklische, multiplikative) Gruppe $\mathbb{Z}/n\mathbb{Z}$ der primen Restklassen modulo n besteht aus den $n - 1$ Elementen

$$\mathbb{Z}/n\mathbb{Z} = \overline{1}, \overline{2}, \overline{3}, \ldots, \overline{k}, \ldots, \overline{n-3}, \overline{n-2}, \overline{n-1}. \tag{4.2}$$

Zwischenbehauptung: Aus $\overline{k}^2 = \overline{1}$ folgt $k = 1$ oder $k = n - 1$. Denn aus $k^2 = 1 \,(mod\, n)$ folgt n teilt $k^2 - 1$. Das heisst n teilt $(k-1) \cdot (k+1)$ und da n nach Voraussetzung eine

[10] Pierre de Fermat, 1607–1665, französischer Jurist und Mathematiker
[11] Leonhard Euler, 1707–1783, Schweizer Mathematiker; primäre Wirkungsorte (Mathematik): Basel, Berlin, St.Petersburg
[12] John Wilson, 1741–1793, britischer Mathematiker

Primzahl ist, folgt daraus n teilt $k-1$ oder n teilt $k+1$. Die einzig möglichen Fälle für k sind dann $k=1$ (d.h. $k-1=0$) oder $k=n-1$ (d.h. $(k+1=n)$. (Ende der Zwischenbehauptung)
Für $n-1$ gilt: $(n-1)^2 = n^2-2n+1$ ist kongruent zu 1 modulo n. Die einzigen *selbstinversen* Element in $\mathbb{Z}/n\mathbb{Z}$ sind also $\overline{n-1}$ und $\overline{1}$. In der Gruppentafel der Gruppe $\mathbb{Z}/n\mathbb{Z}$ hat also, abgesehen von $\overline{n-1}$ und $\overline{1}$, jedes Element ein von ihm verschiedenes Inverses. Und deshalb ergänzen sich im Ausdruck

$$(n-1)! \quad (= \overline{1}\cdot\overline{2}\cdot\overline{3}\cdot\ldots\cdot\overline{k}\cdot\ldots\cdot\overline{n-3}\cdot\overline{n-2}\cdot\overline{n-1}\,) \tag{4.3}$$

(abgesehen von den Faktoren $\overline{n-1}$ und $\overline{1}$) alle Faktoren paarweise (zu $\overline{1}$) auf und wir erhalten das Ergebnis:

$$(n-1)! = n-1 = -1 \ (mod\ n) \tag{4.4}$$

(ii) Es sei nun andererseits n keine Primzahl, etwa $n = a\cdot b$. Dann sind a und b kleiner als n und die Restklassen $\overline{a}$ und $\overline{b}$ treten im Produkt (4.3) als Faktoren auf. Das Produkt ist dann also gleich Null modulo n – und die Gleichung in (4.1) gilt nicht.

5 Normalteiler, Faktorgruppen, einfache Gruppen

5.1 Normalteiler

***Aufgabe* 5.1**
Sei $U \leq G$ [13]. Zeigen Sie (etwa am Beispiel der Gruppe D_3), dass für Nebenklassen in der Regel **nicht** gilt:

$$xU = Ux \tag{5.1}$$

Definition 5.1: Falls die Gleichung (5.1) für alle $x \in G$ erfüllt ist, nennt man U einen *Normalteiler*[14] von G.

Bezeichnungen:

$U \trianglelefteq G$:	U ist ein Normalteiler von G; dabei ist möglich: $U = G$.
$U \triangleleft G$;	U ist ein (i.d.R.) echter Normalteiler von G; d.h. $U \neq G$.
$U \underset{\neq}{\triangleleft} G$:	U ist ein von G verschiedener Normalteiler von G.

Bemerkung: Die Bedingung (5.1) kann als eine Art verallgemeinerter Kommutativität angesehen werden. Dies spielt besonders im Zusammenhang mit der Lösung von Polynomgleichungen und "auflösbaren" Gruppen eine wichtige Rolle.

***Aufgabe* 5.2**

1. Zeigen Sie: Bedingung (5.1) ist gleichwertig zu:
   (a) $\forall x \in G : \forall u \in U : xux^{-1} \in U$

[13] Diese Ausdrucksweise wird als Abkürzung für den Ausdruck "Sei G eine Gruppe und U eine Untergruppe von G" verwendet
[14] ältere Bezeichnung: invariante Untergruppe; engl.: normal subgroup

(b) $\forall x \in G : xUx^{-}1 = U$

2. Zeigen Sie anhand der bisher behandelten Beispiele Normalteiler auf.
3. Zeigen Sie anhand der bisher behandelten Beispiele Untergruppen auf, die keine Normalteiler sind.
4. Zeigen Sie: Jede Untergruppe einer abelschen Gruppe ist ein Normalteiler.
5. Zeigen Sie: Jede Untergruppe vom Index 2 ist ein Normalteiler.

Die Untergruppen einer Gruppe bilden einen *Verband*. Dies ist eine algebraische Struktur, die hier nicht näher erläutertwerden soll. Verbände lassen sich aber gut visualisieren. In Abbildung 5.1 ist der Untergruppen-Verband der Symmetrischen Gruppe S_4 dargestellt. Die Normalteiler sind dabei durch dicke Punkte und die Normalteiler-Relationen durch dick gezeichnete Verbindungslinien dargestellt.

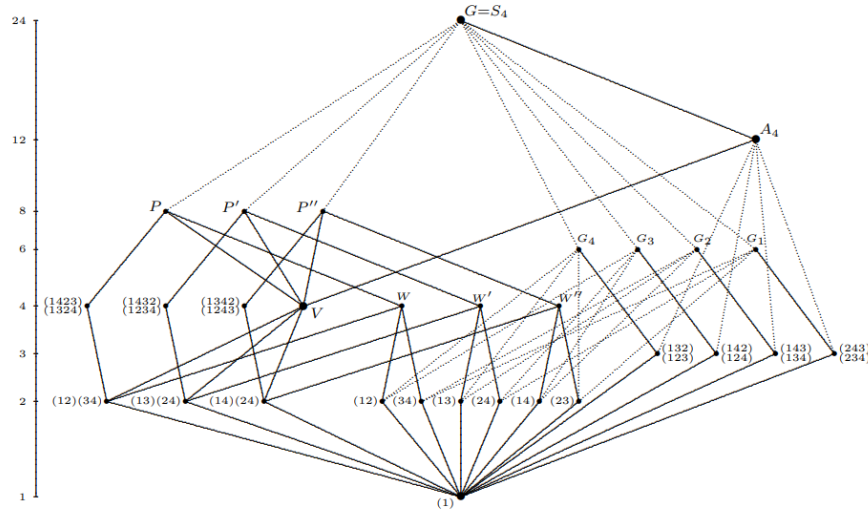

Figure 5.1: Der Verband der Untergruppen der Gruppe S_4
Mit freundlicher Genehmigung von Seiten der Quelle:
`https://www.math.uni-bielefeld.de/~sek/alg/s_4.pdf`

Offensichtlich ist: Jede Gruppe G besitzt die "trivialen" Normalteiler 1 und G.

Definition 5.2 Gruppen, die nur die trivialen Normalteiler besitzen, heissen *einfache Gruppen*[15].

Wir wir in Abschnitt 2.4 gesehen haben, ist jede Gruppe von Primzahlordnung zyklisch und einfach (Satz von Lagrange). Dies führt zu einem unendlichen Vorrat von kommutativen einfachen Gruppen. Die nichtkommutativen einfachen Gruppen treten sehr viel

[15] An dieser Stelle ist das folgende Zitat (sinngemäss) von H. Wielandt (Univ. Tübingen) unverzichtbar: „Eine Gruppe heisst einfach, wenn sie besonders kompliziert ist.“

seltener auf. Ihre Ordnungen sind z.B. in der *Online Encyclopedia of Integer Sequences*, OEIS A001034, beschrieben. Die Ordnungen der ersten Glieder dieser Folge lauten: $60, 168, 360, 504, 660, 1092, 2448, 2520, 3420, 4080, 5616, 6048, 6072, 7800, 7920, 9828, \ldots$
(Man vergleiche hierzu das Zitat von Wielandt in der Fussnote.)

5.2 Faktorgruppen

Definition 5.3 Es sei N ein Normalteiler der Gruppe G. Mit G/N sei die Menge der Nebenklassen von N in G bezeichnet. Dann kann durch die folgende Definition

$$xN \cdot yN := xyN \tag{5.2}$$

eine Gruppenverknüpfung auf der Menge der Nebenklassen definiert werden.

Die so gebildete neue Gruppe $(G/N, \cdot, N)$ wird als *Faktorgruppe* von G modulo N (gelegentlich sprachlich aus ausgedrückt als „Faktorgruppe von G nach N“) bezeichnet.

***Aufgabe* 5.3** Erläutern Sie, warum die Definition (5.2) sinnvoll ist und warum etwas Entsprechendes nicht funktioniert, wenn N nur eine Untergruppe (und kein Normalteiler) von G ist.

***Aufgabe* 5.4** Es sei N ein Normalteiler der Gruppe G. Dann ist die Abbildung

$$\varphi : G \to G/N$$

mit $\varphi(g) := gN$ ein Gruppen-Homomorphismus.

Definition 5.4 Die Abbildung $\varphi : G \to H$ sei ein Homomorphismus der Gruppe G in die Gruppe H. Die Menge $Ker(\varphi) := \{x \in G : \varphi(x) = 1\}$ wird als der *Kern* von φ bezeichnet.
Die Menge $Im(\varphi) := \varphi(G) := \{\varphi(x) : x \in G\}$ wird als das *Bild* von G unter der Abbildung φ bezeichnet.

***Aufgabe* 5.5** Die Abbildung $\varphi : G \to H$ sei ein Homomorphismus der Gruppe G in die Gruppe H.

1. Zeigen Sie: Der Kern von φ ist ein Normalteiler von G.
2. Das Bild $Im(\varphi)$ ist eine Untergruppe von H.
3. Die Faktorgruppe $G/Ker(\varphi)$ ist isomorph zu $Im(\varphi)$.

6 Subnormalreihen, Kompositionsreihen, auflösbare Gruppen

6.1 Subnormalteiler und Subnormalreihen

Definition 6.1 Ist N ein Normalteiler der Gruppe G und M ein Normalteiler von N, so wird M als *Subnormalteiler* (engl. *subnormal subgroup*) von G bezeichnet.
Im Zeichen: $M \lhd N \lhd G$

***Aufgabe* 6.1** Zeigen Sie anhand der bisher behandelten Untergruppen: Es sein G eine Gruppe und M ein Subnormalteiler von G. Dann muss M nicht notwendigerweise ein Normalteiler von G sein.

Eine endliche, absteigende Reihe von Untergruppen der Gruppe G

$$G = G_0 > G_1 > \cdots > G_n = \{1\} \tag{6.1}$$

heißt *Subnormalreihe*, wenn jede Untergruppe der Reihe ein Normalteiler ihres Vorgängers ist, wenn also für $1 \leq k \leq n$ stets gilt: $G_k \lhd G_{k-1}$. Die "Faktoren" dieser Reihe sind die Faktorgruppen G_{k-1}/G_k.

Ist jede der Untergruppen G_i sogar ein Normalteiler von G, dann heißt die Reihe *Normalreihe*.

Eine Subnormalreihe, die von G bis 1 absteigt, heißt *Kompositionsreihe*, falls jeder ihrer Faktoren G_{k-1}/G_k eine einfache Gruppe ist, sie heißt *auflösbare Reihe*, wenn jeder ihrer Faktoren eine kommutative Gruppe (abelsche Gruppe) ist.

Eine Gruppe heisst *auflösbar*, wenn sie eine Subnormalreihe mit abelschen Faktorgruppen (also eine auflösbare Reihe) besitzt.

***Aufgabe* 6.2** Machen Sie sich klar: Ist G eine abelsche Gruppe, so ist jede ihrer Untergruppen ein Normalteiler und jede Reihe von Untergruppen eine Normalreihe und damit auch eine Subnormalreihe.

Bemerkung: Eines der berühmtesten Ergebnisse über auflösbare Gruppen ist der **Satz von Feit-Thompson**: *Jede Gruppe ungerader Ordnung ist auflösbar.*
Zitat (`https://de.wikipedia.org/wiki/Satz_von_Feit-Thompson`)

> *Trotz der beeindruckend einfachen Formulierung dieses Satzes sind keine zugänglichen Beweise bekannt. Der Satz wurde bereits 1911 von William Burnside vermutet, konnte aber erst 1963 von W. Feit und J. G. Thompson bewiesen werden. Der originale Beweis umfasst mehr als 250 Seiten ...*[16]

In der Gruppentheorie spielen die Gruppen, deren Ordnung durch 2 teilbar ist, oft eine besondere (Aussenseiter-) Rolle. Dies soll den Gruppentheoretiker Ph. Hall[17] zu der pointierten Bemerkung “Two is the oddest of all primes” veranlasst haben.

6.2 Kommutator, Kommutatorgruppen, Kommutatorreihen

***Aufgabe* 6.3** Zeigen Sie: Ist G eine Gruppe und $g, h \in G$, dann ist $(g \cdot h)^{-1} = h^{-1} \cdot g^{-1}$.

Man sagt, die Elemente g und h einer Gruppe G *kommutieren* (sind vertauschbar), wenn $g \cdot h = h \cdot g$ ist.

Der *Kommutator*[18] $[g, h]$ zweier Elemente g und h einer Gruppe G ist definiert durch $[g, h] := g^{-1}h^{-1}gh \quad (= (hg)^{-1}gh)$.

[16] William Burnside, 1852–1927, englischer Mathematiker (besonders Gruppentheorie)
Walter Feit, 1930–2004, US-amerikanischer Mathematiker (Gruppentheorie)
John Griggs Thompson, geb. 1932, US-amerikanischer Mathematiker (Gruppentheorie)

[17] Philip Hall, 1904–1982 englischer Mathematiker (Gruppentheorie und Kombinatork)

[18] lateinisch commutare: vertauschen

***Aufgabe* 6.4** Was kann man über die Kommutatoren in abelschen Gruppen sagen?

Bemerkung: Der *Kommutator* ist ein Indikator dafür, wie sehr zwei Elemente einer Gruppe das Kommutativgesetz verletzen.

Die von allen Kommutatoren erzeugte Untergruppe einer Gruppe G wird als *Kommutatorgruppe* oder *abgeleitete Gruppe* von G bezeichnet; im Zeichen $K(G)$ oder $G^{(1)}$. Die Iterierung der Kommutatorgruppenbildung

$$G^{(n+1)} := K(G^n)$$

führt zur *Kommutatorreihe* oder *abgeleiteten Reihe* von G.

***Aufgabe* 6.5** Es sei G eine Gruppe und K ihre Kommutatorgruppe. Zeigen Sie G/K ist kommutativ.

Bemerkung: Wenn die Kommutatorreihe einer Gruppe G nach endlich vielen (etwa n) Schritten bei der trivialen Gruppe $G^{(n)} = \{e\}$ endet, so ist die Gruppe auflösbar. Die Kommutatorreihe stellt eine Möglichkeit dar, zu entscheiden, ob eine Gruppe auflösbar ist oder nicht und ggf. eine Subnormalreihe mit abelschen Faktoren zu konstruieren.

***Aufgabe* 6.6** (i) Bestimmen Sie die Kommutatorgruppe der symmetrischen Gruppe S_4. Zeigen Sie $K(A_4) = A_4$.
(ii) Führen Sie dies für $n = 5$ an Stelle von $n = 4$ durch.

6.3 Die Sätze von Schreier und Jordan-Hölder

***Aufgabe* 6.7** Beschreiben Sie, was man unter einer *Verfeinerung* einer Reihe von Untergruppen zu verstehen hat (bzw. haben sollte).

Die folgenden Ergebnisse werden in diesem Manuskript nur zitiert.

Satz 6.1 *Jede endliche abelsche Gruppe besitzt eine Normalreihe bzw. Subnormalreihe mit zyklischen Faktorgruppen.*

Folgerung Jede Subnormalreihe einer (endlichen) abelschen Gruppe kann zu einer Subnormalreihe mit zyklischen Faktoren verfeinert werden.

Satz 6.2 *(Satz von Schreier[19]) Je zwei Subnormalreihen einer Gruppe G besitzen isomorphe Verfeinerungen.*

Satz 6.3 *(Satz von Jordan-Hölder[20]) Je zwei Kompositionsreihen einer Gruppe G sind isomorph.*

[19] Otto Schreier, 1901–1929, österreichischer Mathematiker
[20] Camille Jordan, 1838–1922, französischer Mathematiker
Otto Ludwig Hölder, 1859–1937, deutscher Mathematiker

7 Direkte Produkte

Die Konstruktion des "direkten Produkts" gibt es praktisch in jeder mathematischen Struktur. Sie dient dazu,

- neue Objekte aus bekannten, bestehenden Objekten zu konstruieren
- die Struktur komplexer Objekte durch den Rückgriff auf einfachere, bereits bekannte Objekte des jeweiligen Typs transparent zu machen.

Die Konstruktion von direkten Produkten basiert zunächst immer auf dem cartesischen Produkt der beteiligten Trägermengen.

7.1 Direkte Produkte von Gruppen

Definition 7.1 Das *direkte Produkt* zweier Gruppen G und H ist wie folgt definiert:

1. Die *Trägermenge* des direkten Produkts ist das *cartesische Produkt*[21] der Mengen G und H:
$$G \times H = \{(x, y) : x \in G \text{ und } y \in H\} \tag{7.1}$$
2. Die wichtigsten Basis-Operationen werden in direkten Produkten meist "komponentenweise" definiert; für Gruppen z.B. folgendermassen (wobei links mit $\circ$ das neue und rechts mit $\cdot$ die alten Verknüpfungszeichen gemeint ist):
$$(a, b) \circ (c, d) := (a \cdot b, c \cdot d) \tag{7.2}$$
Folgerung Das neutrale Element ist $(1, 1)$ und für die inversen Elemente gilt: $(a, b)^{-1} = (a^{-1}, b^{-1})$.

Bemerkung und Aufgabe Zeigen Sie: Für drei Gruppen A, B und C sind offenbar die direkten Produkte $(A \times B) \times C$ und $A \times (B \times C)$ isomorph.

Man lässt deshalb (auch im Fall von 4 und mehr Gruppen) die Klammern weg und schreibt einfach $A \times B \times C$.

Beispiele

1. $\mathbb{Z}_2 \times \mathbb{Z}_2$: *Kleinsche Vierergruppe*[22]. Sie Unterscheidet sich von der einzigen anderen Gruppe, der zyklischen Gruppe $\mathbb{Z}_4$, z.B. dadurch, dass letztere (aber nicht erstere) Elemente der Ordnung 4 enthält.
2. $\mathbb{Z}_2 \times \mathbb{Z}_3$: Sie ist isomorph zu $\mathbb{Z}_6$, aber nicht zu D_3, da erstere (aber nicht letztere) kommutativ ist.
3. $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ und $\mathbb{Z}_2 \times \mathbb{Z}_4$: Dies sind die die nichtzyklischen, aber kommutativen Gruppen der Ordnung 8.

[21] nach René Descartes, genannt Cartesius, 1596–1650, französischer Philosoph, Mathematiker und Naturwissenschaftler

[22] Felix Klein, 1849–1925, deutscher Mathematiker. (Es sind aber eher andere Leistungen als die Kleinsche Vierergruppe, durch die er berühmt wurde.)

4. $\mathbb{Z}_3 \times \mathbb{Z}_3$: Dies ist die einzige nichtzyklissche Gruppe der Ordnung 9.
5. $\mathbb{Z}_2 \times \mathbb{Z}_5$: Sie ist isomorph zur zyklischen Gruppe $\mathbb{Z}_{10}$
6. $\mathbb{Z} \times \mathbb{Z}$
7. $2\mathbb{Z} \times 3\mathbb{Z}$ Dies ist das direkte Produkt aus den geraden und den durch 3 teilbaren Zahlen.
8. Auch gemischte direkte Produkte aus endlichen und unendlichen Gruppen sind möglich. Z.B. (im Falle von additiv geschriebenen Gruppen) $\mathbb{Z}_7 \times \mathbb{Z}$ $Z \times \mathbb{Z}$ u.s.w.
9. Auch direkte Produkte aus abelschen und nicht-abelschen Gruppen sind möglich; z.B. $D_3 \times \mathbb{Z}_2$

***Aufgabe* 7.1**

- Interpretieren und begründen Sie: $|A| \times B| = |A| \cdot |B|$.
- Zeigen Sie: Sind A und B abelsche Gruppen, so auch $A \times B$.
- Zeigen Sie: Die natürliche Zahl n sei das Produkt zweier unterschiedlicher Primzahlen p und q ($n = p \cdot q$). Dann gilt: $\mathbb{Z}_p \times \mathbb{Z}_q$ ist isomorph zu der zyklischen Gruppe $\mathbb{Z}_n$ ($= \mathbb{Z}_{p \cdot q}$).

7.2 Der Hauptsatz über endlich erzeugte abelsche Gruppen

Der Hauptsatz über endlich erzeugte abelsche Gruppen (auch als *Struktursatz* bezeichnet), liefert eine vollständige Klassifikation dieser Gruppen.

Die einfachsten Bausteine abelscher Gruppen sind:

- Im Fall endlicher Gruppen: Die (additiven) zyklischen Gruppen von Primzahlordnung.
- Im unendlichen Fall: Die (additive) Gruppe der ganzen Zahlen $\mathbb{Z}$.

Der Hauptsatz über endlich erzeugte abelsche Gruppen besagt, dass alle endlich erzeugten abelschen Gruppen aus diesen Bausteinen zusammengesetzt sind:

Satz 7.1 *Hauptsatz über endlich erzeugte abelsche Gruppen*
Jede endlich erzeugte abelsche Gruppe G ist zu einer endlichen direkten Summe von zyklischen Gruppen, deren Ordnung die Potenz einer Primzahl ist, und unendlichen zyklischen Gruppen isomorph.

8 Skizze: Polynomgleichungen

Im Folgenden ist eine grobe Skizze anhand der einschlägigen Schritte gegeben. Für wesentlich detailliertere Darstellungen sei z.B. auf [Pésic] und [Bewersdorf] verwiesen. Eine sehr schöne, lebendige kulturhistorische Beschreibung der Verwicklungen bei der Lösung von Gleichungen 3. Grades findet man in [de Padova].

Zunächst sei klargestellt, was mit der "Lösung"[23] einer Gleichung gemeint ist. Gleichungen lassen sich in vielfältiger Weise lösen, z.B. auch numerisch in der Form von

[23] Im Kontext dieser Thematik werden die Lösungen oft auch als "Wurzeln" bezeichnet.

Näherungslösungen, oder sogar graphisch. Dies ist hier nicht gemeint. Im Folgenden geht es um exakte Lösungen. Aber was heisst "exakt"? Was ist eine exakte Lösung der Gleichung $x^2 - 3 = 0$? Exakter als dass man sagt die Lösung ist "Wurzel 3" (im Zeichen: $\sqrt{3}$) geht es nicht. Man muss dann allerdings auch erläutern, wie man mit so einer Lösung rechnet.

Zum Rechnen mit Wurzeln

Wie soll man mit $\sqrt{3}$ rechnen? Es geht nicht anders als dass man seinen bisherigen "Rechenbereich", die rationalen Zahlen, verlässt und in einen neuen Rechenbereich eintritt; ähnlich, wie man, als es notwendig war, den Rechenbereich der ganzen Zahlen zu verlassen, um die dort nicht mehr möglichen Rechnungen im Bereich der Bruchzahlen durchzuführen. Man muss also alle Zahlen der Art $a + b\sqrt{3}$ hinzunehmen, wobei a und b rationale Zahlen sind und mit dem Symbol $\sqrt{3}$ folgendermaßen zu rechnen ist: $\sqrt{3} \cdot \sqrt{3} = 3$. Wie man weiter mit diesen "Zahlen" rechnen muss, ist klar, wenn die bisherigen Rechengesetze möglichst uneingeschränkt weiter bestehen sollen (entsprechend dem *Permanenzprinzip* von H. Hankel[24]). Für die Multiplikation bedeutet das z.B. $(a+b\sqrt{3})\cdot(c+d\sqrt{3}) = (ac+3bd)+(ad+bc)\cdot\sqrt{3}$. Entsprechend müssen dann aber in dieser Art Schritt für Schritt noch andere Quadratwurzeln wie $\sqrt{5}$, und andere Wurzeln, wie $\sqrt[k]{n}$ hinzugenommen werden. Man gelangt so zum Zahlbereich der algebraischen Zahlen. Allgemein sind die *algebraischen Zahlen* definiert als die Nullstellen von Polynomen der Art

$$a_n x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \ldots a_2 x^2 + a_1 x + a_0 \tag{8.1}$$

mit rationalen Koeffizienten $a_n, a_{n-1}, \ldots, a_2, a_1, a_0$.

***Aufgabe* 8.1** Zeigen Sie: Die Menge $\mathbb{A}$ der algebraischen Zahlen ist abzählbar.

8.1 Gleichungen 2. Grades

Eine Gleichung der Form

$$ax^2 + bx + c = 0 \tag{8.2}$$

(mit den rationalen Koeffizienten a, b und c, mit $a \neq 0$) wird als *quadratische Gleichung* (über den rationalen Zahlen) bezeichnet. Ihre Lösungen ("Wurzeln") sind

$$x_1 = \frac{-b + \sqrt{b^2 - 4ac}}{2a} \quad \text{und} \quad x_2 = \frac{-b - \sqrt{b^2 - 4ac}}{2a} \tag{8.3}$$

Sie waren i.w. schon im Altertum bekannt; wenn sich auch die Darstellung stark von der heutigen Form unterschied. Der Mathematiker Al-Khwarizmi[25] hat ihre Lösungen in systematischer Form behandelt und dargestellt.

Ein Polynom (über einem Körper) ist ein Ausdruck der Form

$$a_n x^n + a_{n-1}x^{n-1} + \ldots + a_3 x^3 + a_2 x^2 + a_1 x + a_0 \tag{8.4}$$

[24] Hermann Hankel, 1839–1873, deutscher Mathematiker

[25] Al-Khwarizmi, ca. 780 – ca. 850, persisch-arabischer Mathematiker; auf seinen Namen geht der Begriff des *Algorithmus* und auf den Titel eines seiner Bücher geht auch der Begriff der *Algebra* zurück

wobei $a_n, a_{n-1}, \ldots, a_2, a_1, a_0$ beliebige Elemente des Körpers sind. Wie werden es hier nur mit dem Körper $\mathbb{Q}$ der rationalen Zahlen zu tun haben. Der *Grad* des Polynoms ist n, wenn $a_n \neq 0$ ist.

Die linke Seite der Gleichung (8.2) ist ein Polynom des Grades 2. Wir werden später auch Polynome höheren Grades betrachten. Dabei wird es sich als günstig erweisen, wenn man davon ausgeht, dass der "führende Koeffizient" des jeweils betrachteten Polynoms gleich 1 ist, wenn also das Polynom, wie man sagt, *normiert* ist. Im Fall von (8.4) ist dies der zu x^n gehörende Koeffizient, also a_n. Man kann dies stets dadurch erreichen, dass man die Gleichung durch diesen (per Definition von Null verschiedenen) Koeffizienten "durchdividiert".

In schulischer Darstellung wird die normierte quadratische Gleichung meist in der Form

$$x^2 + px + q = 0 \tag{8.5}$$

geschrieben. Ihre Lösungen sind

$$x_1 = \frac{-p + \sqrt{p^2 - 4q}}{2} \quad \text{und} \quad x_2 = \frac{-p - \sqrt{p^2 - 4q}}{2} \tag{8.6}$$

Bei näherem Hinschauen fällt auf, dass es zwischen den Koeffizienten der Gleichung und den Lösungen folgende Beziehungen gibt:

$$\begin{aligned} x_1 \cdot x_2 &= q \\ x_1 + x_2 &= -p \end{aligned} \tag{8.7}$$

Die Gleichungen (8.7) gehen auf Vieta[26] zurück. Man bezeichnet sie daher als die Gleichungen (bzw. *Wurzelgleichungen* von Vieta). Man kann die Gleichung durch direktes Nachrechnen belegen.

Es gilt aber auch: Die quadratische Gleichung

$$(x - x_1) \cdot (x - x_2) = x^2 - (x_1 + x_2) \cdot x + x_1 \cdot x_2 = 0 \tag{8.8}$$

hat dieselben Wurzeln wie (8.5). Es handelt sich also um dieselbe Gleichung und die Koeffizienten sind paarweise gleich. Die Gleichungen in (8.7) ergeben sich damit durch einen einfachen *Koeffizientenvergleich*[27].

8.2 Gleichungen 3. Grades

Im Folgenden werden die Koeffizienten der jeweiligen Polynome passend zum Exponenten von x^k durchnumeriert, wobei der führende Koeffizient stets gleich 1 ist. Das Auffinden einer Lösungsformel von Gleichungen der Form

$$x^3 + a_2 x^2 + a_1 x + a_0 = 0 \tag{8.9}$$

[26] François Viète, in latinisierender Form auch Vieta genannt, 1540–1603, französischer Advokat und Mathematiker

[27] Zwei Polynom-Darstellungen stellen dasselbe Polynom dar, wenn ihre Koeffizienten gleich sind.

war in der Geschichte der Mathematik mit erheblichen Problemen verbunden, bis N. Tartaglia[28] und G. Cardano[29] schliesslich die hochgradig komplizierten Lösungen fanden. Eine sehr lebendige Erzählung der verworrenen Geschichte um das Auffinden der "Cardanischen Formeln" ist in dem Buch [de Padova] zu finden. in heutiger Notation lauten die Lösungen[30]:

$$x_1 = \left(\frac{-1}{2} - \frac{\sqrt{3}\,i}{2}\right)\left(\frac{\sqrt{4\,a_0\,a_2^3 - a_1^2\,a_2^2 - 18\,a_0\,a_1\,a_2 + 4\,a_1^3 + 27\,a_0^2}}{2\,3^{\frac{3}{2}}} + \frac{(-1)\;a_2^3}{27} + \frac{a_1\,a_2 - 3\,a_0}{6}\right)^{\frac{1}{3}}$$
$$- \frac{\left(\frac{\sqrt{3}\,i}{2} + \frac{-1}{2}\right)\left(\frac{(-1)\,a_2^2}{9} + \frac{a_1}{3}\right)}{\left(\frac{\sqrt{4\,a_0\,a_2^3 - a_1^2\,a_2^2 - 18\,a_0\,a_1\,a_2 + 4\,a_1^3 + 27\,a_0^2}}{2\,3^{\frac{3}{2}}} + \frac{(-1)\,a_2^3}{27} + \frac{a_1\,a_2 - 3\,a_0}{6}\right)^{\frac{1}{3}}} + \frac{(-1)\;a_2}{3}$$

$$x_2 = \left(\frac{\sqrt{3}\,i}{2} + \frac{-1}{2}\right)\left(\frac{\sqrt{4\,a_0\,a_2^3 - a_1^2\,a_2^2 - 18\,a_0\,a_1\,a_2 + 4\,a_1^3 + 27\,a_0^2}}{2\,3^{\frac{3}{2}}} + \frac{(-1)\;a_2^3}{27} + \frac{a_1\,a_2 - 3\,a_0}{6}\right)^{\frac{1}{3}}$$
$$- \frac{\left(\frac{-1}{2} - \frac{\sqrt{3}\,i}{2}\right)\left(\frac{(-1)\,a_2^2}{9} + \frac{a_1}{3}\right)}{\left(\frac{\sqrt{4\,a_0\,a_2^3 - a_1^2\,a_2^2 - 18\,a_0\,a_1\,a_2 + 4\,a_1^3 + 27\,a_0^2}}{2\,3^{\frac{3}{2}}} + \frac{(-1)\,a_2^3}{27} + \frac{a_1\,a_2 - 3\,a_0}{6}\right)^{\frac{1}{3}}} + \frac{(-1)\;a_2}{3}$$

$$x_3 = \left(\frac{\sqrt{4\,a_0\,a_2^3 - a_1^2\,a_2^2 - 18\,a_0\,a_1\,a_2 + 4\,a_1^3 + 27\,a_0^2}}{2\,3^{\frac{3}{2}}} + \frac{(-1)\;a_2^3}{27} + \frac{a_1\,a_2 - 3\,a_0}{6}\right)^{\frac{1}{3}}$$
$$- \frac{\frac{(-1)\,a_2^2}{9} + \frac{a_1}{3}}{\left(\frac{\sqrt{4\,a_0\,a_2^3 - a_1^2\,a_2^2 - 18\,a_0\,a_1\,a_2 + 4\,a_1^3 + 27\,a_0^2}}{2\,3^{\frac{3}{2}}} + \frac{(-1)\,a_2^3}{27} + \frac{a_1\,a_2 - 3\,a_0}{6}\right)^{\frac{1}{3}}} + \frac{(-1)\;a_2}{3}$$

So kompliziert die Lösungen auch aussehen mögen, es gelten auch hier wieder "Vietaschen" Gleichungen:

$$\begin{aligned} x_1 \cdot x_2 \cdot x_3 &= -a_0 \\ x_1 \cdot x_2 + x_1 \cdot x_3 + x_2 \cdot x_3 &= a_1 \\ x_1 + x_2 + x_3 &= -a_2 \end{aligned} \tag{8.10}$$

Auch im Hinblick auf die Bestätigung der Gleichungen in (8.10) ist die "Vieta-Darstellung"

$$\begin{aligned} x^3 + a_2 x^2 + a_1 x + a_0 &= (x - x_1) \cdot (x - x_2) \cdot (x - x_3) \\ &= x^3 - x^2 \cdot (x_1 + x_2 + x_3) + x \cdot (x_1 \cdot x_2 + \cdot x_1 \cdot x_3 + x_2 \cdot x_3) \\ &\quad - x_1 \cdot x_2 \cdot x_3 \end{aligned} \tag{8.11}$$

hilfreich.

[28] Niccolo Tartaglia, 1500–1557, italienischer Mathematiker der Renaissance

[29] Gerolamo Cardano, auch Geronimo oder Girolamo Cardano, 1501–1576, italienischer Arzt, Philosoph und Mathematiker der Renaissance

[30] erstellt mit Hilfe des (open source) Computeralgebra Systems **Maxima** `https://maxima.sourceforge.io/de/index.html`

8.3 Gleichungen 4. Grades

Auch für Gleichungen der Art

$$x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 = 0$$

mit rationalen Koeffizienten fand man in der Folgezeit Lösungen mit Wurzelausdrücken (Radikalen), indem man sie trickreich auf Gleichungen niedrigeren Grades reduzierte. Die Lösungen fallen aber nochmals komplizierter aus als im Falle der Gleichungen dritten Grades. Deswegen sei hier auf ihre Darstellung verzichtet.

***Aufgabe* 8.2** Spielen Sie den Prozess der Lösungsfindung auf Ihrem bevorzugten Computeralgebra System (CAS) durch und überprüfen Sie insbesondere die Gültigkeit der Vietaschen Wurzelgleichungen.

***Aufgabe* 8.3** Formulieren Sie für Gleichungen vierten Grades die Analoga zu den Vietaschen Gleichungen in (8.10) und begründen Sie diese.

8.4 Gleichungen 5. Grades

Für Gleichungen fünften Grades fand man (ausser in Spezialfällen) keine Lösungen. Aufgrund der Kompliziertheit der Lösungen von Gleichungen dritten und vierten Grades nahm man lange Zeit an, dass die Lösungen für Gleichungen fünften Grades noch mal wesentlich komplizierter ausfallen würden und dass man sich dementsprechend noch mehr anstrengen müsse, die Lösungen zu finden. Da dies trotz aller Bemühungen nicht gelang, kam langsam der Verdacht auf, dass es für "allgemeine" Gleichungen fünften Grades, also Gleichungen der Form

$$1 \cdot x^5 + a_4 \cdot x^4 + a_3 \cdot x^3 + a_2 \cdot x^2 + a_1 \cdot x + a_0 = 0 \tag{8.12}$$

ausser in Spezialfällen keine Lösungsformel mit Radikalen gibt.

8.5 Der Satz von Vieta und Symmetrien bei den Wurzeln

Zur *Symmetrie* gibt es wohl so viele Zitate wie zu kaum einem anderen Thema in der Mathematik. Ein Mathematiker, der sich besonders intensiv mit Fragen der Symmetrie befasst und ein Standardwerk dazu geschrieben hat (siehe Literaturverzeichnis), ist Hermann Weyl[31]. Im Folgenden seien zwei Zitate von ihm wiedergegeben.

> *Die Symmetrie ist diejenige Idee, mit deren Hilfe der Mensch im Laufe der Jahrhunderte versuchte, Ordnung, Schönheit und Vollkommenheit zu begreifen und zu schaffen.*
>
> *Symmetrisch ist ein Gebilde dann, wenn man irgend etwas damit machen kann und das Ergebnis so aussieht wie zuvor.*

Eine Funktion f bzw. ein Ausdruck (Term) in den Variablen $x_1, x_2, \ldots, x_n$ heisst *symmetrisch*, wenn sich ihr Wert (wie auch immer er definiert sein mag) bei eine beliebigen Vertauschung (Permutation) der Variablen nicht ändert.

[31] Hermann Weyl, 1885–1955, deutscher Mathematiker, Physiker und Philosoph

Ein Beispiel: $f(x,y,z) = x^2 + y^2 + z^2$.
Es ist $f(x,y,z) = f(y,z,x) = f(z,x,y) = f(y,x,z) = f(x,z,y) = f(z,y,x)$

Im Zusammenhang mit dem Lösen von Polynomgleichungen spielen die "elementarsymmetrischen Funktionen" des Satzes von Vieta eine besondere Rolle.

Satz 8.1 *Satz von Vieta*
Es sei

$$x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \ldots a_2x^2 + a_1x + a_0 = 0 \tag{8.13}$$

eine Polynomgleichung vom Grad n mit rationalen Koeffizienten und den Wurzeln $x_1, x_2, .x_3, \ldots x_n$ [32].

Dann gilt

$$\begin{aligned}
a_0 &= (-1)^n \cdot x_1 \cdot x_2 \cdot x_3 \cdot \ldots \cdot x_{n-2} \cdot x_{n-1} \cdot x_n \\
a_1 &= (-1)^{n-1} \cdot (x_1x_2x_3 \ldots x_{n-1} + x_1x_3 \ldots x_n + \ldots + x_2 \ldots x_{n-1}x_n) \\
a_2 &= (-1)^{n-2} \cdot (x_1x_2x_3 \ldots x_{n-2} + \ldots + x_3x_4 \ldots x_{n-1}x_n) \\
&\ldots \\
a_{n-3} &= (-1)^3 \cdot (x_1x_2x_3 + x_1x_2x_4 + \ldots + x_{n-2}x_{n-1}x_n) \\
a_{n-2} &= (-1)^2 \cdot (x_1x_2 + x_1x_3 + \ldots + x_1x_n + x_2x_3 + \ldots + x_{n-1}x_n) \\
a_{n-1} &= (-1)^1 \cdot (x_1 + x_2 + x_3 + \ldots + x_{n-1} + x_n)
\end{aligned} \tag{8.14}$$

Wie im Falle $n = 2$ (vgl. Gleichung 8.8) folgt dies aus dem Vergleich der Koeffizienten der Polynome (8.13) und $(x - x_1) \cdot (x - x_2) \cdot \ldots \cdot (x - x_{n-1}) \cdot (x - x_n)$; letzteres in ausmultiplizierter Form.

Im Falle einer Polynomgleichung wie (8.13) hängt die Struktur der Lösungen natürlich auf das Engste mit den Koeffizienten $a_{n-1}, a_{n-2}, \ldots a_2, a_1, a_0$ zusammen. Aber der Satz von Vieta macht es möglich, den Fokus bei Fragen zur Lösbarkeit der Gleichung weg von den Koeffizienten und hin zu den Wurzeln $x_n, x_{n-1}, \ldots x_2, x_1$ zu verschieben – und deren Symmetrieen ins Spiel zu bringen.

8.6 Ruffini, Abel und Galois

Nachdem die Lösungen für Polynomgleichungen dritten und vierten Grades gefunden waren und man sich bei den Gleichungen fünften Grades die Zähne ausbiss, lenkten (aufbauend auf der Arbeit von Vieta) Mathematiker wie Ruffini[33] und Abel[34] das Augenmerk hin zu den Wurzeln der Gleichungen, deren Symmetrien sie zunehmend besser in den Griff bekamen.

Aufbauend auf den Arbeiten von Ruffini konnte Abel zeigen, dass für die Auflösung von Polynomgleichungen gewisse Vertauschungs-Operationen unter den Wurzeln notwendig waren. Indem er zeigte, dass es eine solche hinreichend uneingeschränkte Vertauschbarkeit nicht gab, konnte er zeigen, dass es keine allgemeine Lösungsformel für Gleichungen fünften Grades geben konnte.

[32] Dass es gerade n Lösungen gibt, folgt aus dem *Fundamentalsatz der Algebra.*
[33] Paolo Ruffini, 1765–1822, italienischer Mathematiker, Mediziner und Philosoph
[34] Niels Henrik Abel, 1802–1829, norwegischer Mathematiker

Über diese Vertauschbarkeit von Permutationen kam der Aspekt der Kommutativität ins Spiel. Da Abel sich als erster in systematischer Weise damit befasst hat, werden kommutative Gruppen heute als *abelsche Gruppen* bezeichnet.

Abels Vorgehensweise machte allerdings eine allgemeine Klassifizierung der durch Radikale lösbaren Polynomgleichungen noch nicht möglich. Beim Vorliegen einer konkreten Gleichung lieferte seine Vorgehensweise nicht eine Aussage der Art: Diese Gleichung ist lösbar bzw. nicht lösbar.

Unabhängig davon waren aber für spezielle Gleichungen 5. Grades die Lösungen bekannt. So z.B. die "Kreisteilungsgleichung" $x^5 - 1 = 0$, deren Lösungen schon Gauß[35] kannte. Und natürlich kann man für jedes 5-Tupel von (rationalen) Zahlen leicht ein Polynom angeben, das genau diese 5 Zahlen als Wurzeln besitzt (Begründung!).

Entscheidend im Zusammenhang mit dem Beweis von Abel ist, dass es keine "allgemeine Lösung" bzw. Lösungsformel gibt, mit der man die Lösung, wie im Falle der quadratischen Gleichung, in jedem Fall "ausrechnen" kann.

Dieser letzte Schritt blieb Galois[36] vorbehalten, der auf der Basis seiner Arbeit mit Permutationen auch den für die Mathematik fundamentalen Begriff der *Gruppe* prägte. Er zeigte, dass zu jeder Polynomgleichung eine spezifische Gruppe von Permutationen gehört und dass die Gleichung durch Radikale genau dann lösbar ist, wenn diese Gruppe auflösbar ist (im Sinne von Abschnitt 6).

Speziell für Polynome vom Grad 5 (oder höher) konnte er zeigen, dass diese Symmetriegruppe gleich der gesamten Gruppe S_5 sein müsste. Da aber die Untergruppe A_5 von S_5 einfach ist (und somit keine Subnormalreihe besitzt), ist die Gruppe S_5 nicht auflösbar. Und somit gibt es für Polynomgleichungen vom Grad grösser oder gleich fünf keine "Lösungsformel", mit der ihre Wurzeln bestimmt werden können.

Die nach ihm benannte *Galois-Theorie* stellt einen ein-eindeutigen Zusammenhang zwischen der Galois-Gruppe eines Polynoms und gewissen Körpererweiterungen des Grundkörpers her, aus dem die Koeffizienten des Polynoms stammen (in unserem Fall $\mathbb{Q}$).

Die Galois-Theorie macht auch eine algorithmische Erschliessung des Themas "Lösung von Polynomgleichungen durch Radikale" moglich. Sie ist zu diesem Zweck auch in viele Computeralgebra-Systeme "eingebaut".

Im historischen Prozess der Theorie des Gleichungslösens entstanden immer kompliziertere Lösungen. Man vergleiche dazu etwa die Gleichungen von Abschnitt 8.2. Da diese Ausdrücke von Hand kaum noch zu bewältigen waren, entwickelte man zur besseren Strukturierung des Prozesses hilfreiche Begriffe wie *Determinanten* und *Resolventen*. Sie sind auch heute noch selbst im Zusammenhang mit der Nutzung von Computeralgebra Systemen hilfreich und sinnvoll.

Ausblick: Im Laufe des 20. Jahrhunderts zeigte sich in vielen Feldern der Wissenschaft, wie fundamental und fruchbar das Konzept der Gruppe ist – nicht nur in der Mathematik sondern z.B. auch in der Physik. Das folgende Zitat von Irving Adler (amerikanische Mathematiker, Wissenschaftsauthor und Pädagoge, 1913–2021) wirft ein helles Licht auf die Bedeutung der Gruppentheorie für die Physik: The importance of group theory was emphasized very recently when some physicists using group theory predicted the existence

[35] Carl Friedrich Gauß, 1777–1855, deutscher Mathematiker
[36] Évariste Galois, 1811–183,2 französischer Mathematiker

of a particle that had never been observed before, and described the properties it should have. Later experiments proved that this particle really exists and has those properties.

Literaturhinweise

Alexandroff P. S.: Einführung in die Gruppentheorie ; VEB Deutscher Verlag der Wissenschaften, Neunte Auflage Berlin 1975

Baumgartner L.: Gruppentheorie; Walter de Gruyter & Co., Sammlung Göschen, Berlin 1964

Baumslag G. and Chandler B.: Theory and Problems of Group Theory; Schaum's Outline Series, McGraw-Hill, 1968

Bewersdorff J.: Algebra für Einsteiger; Springer Spektrum, 6. Auflage, Springer Spektrum, Wiesbaden 2019

Budden F. J.: The Fascination of Groups; Cambridge University Press 1972

Burnside W.: Theory of groups of finite order; Dover Publications, 1955 (2nd ed.)

de Padova Th.: Alles wird Zahl; Carl Hanser Verlag, München 2021

Edwards H.M.: Galois Theory; Springer Verlag, New York 1984

Gorenstein D.: Finite Groups; Harper & Row Publishers, New York 1968

Grossmann J. und Magnus W.: Gruppen und ihre Graphen, Ernst Klett Verlag, Stuttgart 1971

Hall M.: The theory of groups; The Macmillan Company, New Yorck 1961 (2nd ed.)

Huppert B.: Endliche Gruppen I; Springer Verlag, Berlin 1967

Kochendörffer R.: Lehrbuch der Gruppentheorie unter besonderer Berücksichtigung der endlichen Gruppen; Akademische Verlagsgesellschaft, Leipzig 1966

Kurosh A. G.: The Theory of Groups; Chelsea Publishing Company, New York 1960

Ledermann: Introduction to Group Theory; Oliver & Boyd, Edinburgh 1973

Pésic P.: Abels Beweis; Springer-Verlag, Berlin 2005$\tilde{/}\tilde{2}$007

Weyl H.: Symmetrie, 3. Auflage, Springer Spektrum, Berlin 2017

Wielandt H.: Finite permutation groups; Academic Press, New York 1964

Ziegenbalg J.: Elementare Zahlentheorie – Beispiele, Geschichte, Algorithmen (2-te Aufl.); Springer Spektrum, Wiesbaden 2015

Internet-Quellen

Wikipedia; Gruppen / Reihe(Gruppentheorie)
`https://de.wikipedia.org/wiki/Gruppentheorie`
`https://de.wikipedia.org/wiki/Reihe_(Gruppentheorie)`

Liste kleiner Gruppen:
`https://de.wikipedia.org/wiki/Liste_kleiner_Gruppen#Glossar`

alternierende Gruppen A4:
`https://de.wikipedia.org/wiki/A4_(Gruppe)`

Wolfram Inc. / Mathworld / Tetraedergruppen:
`https://mathworld.wolfram.com/TetrahedralGroup.html`

Online Encyclopedia of Integer Sequences (OEIS):
`https://oeis.org/wiki/Number_of_groups_of_order_n#Solvable_groups`
`https://oeis.org/wiki/Classification_of_finite_simple_groups`
Number of groups of order n:
`https://oeis.org/A000001`
Number of Abelian groups of order n:
`https://oeis.org/A000688`
Orders of non-abelian simple groups (= Orders of non-cyclic simple groups):
`https://oeis.org/A001034`
Orders of non-solvable groups:
`https://oeis.org/A056866`

Computeralgebra software GAP

GAP - Groups, Algorithms, Programming - a System for Computational Discrete Algebra
`https://www.gap-system.org/`

Index

φ-Funktion, 18

abelsche Gruppe, 3
alternierende Gruppe, 13
assoziativ, 3
auflösbare Gruppe, 21, 22, 25
auflösbare Reihe, 22

cartesisches Produkt, 24
Cayley-Tafel, 5

Diedergruppe, 4, 12, 13
disjunkte Vereinigung, 15
Durchschnitt von Untergruppen, 15

einfache Gruppe, 20
elementarsymmetrische Funktion, 30
endlich erzeugte Gruppe, 16, 25
erzeugendes Element, 16
Euler, 18
Eulersche φ-Funktion, 18
Eulersche Totienten-Funktion, 18

Faktorgruppe, 21
Fermat, 18
Fixpunkt, 8

gerade Permutation, 8, 13
Gruppe, 3
    abelsch, 3
    auflösbar, 21
    einfach, 20
    endlich erzeugt, 16
    kommutativ, 3
    zyklisch, 16
Gruppentafel, 5

Homomorphismus, 11

Index einer Untergruppe, 14
invariante Untergruppe, 19
inverses Element, 3
isomorphe Gruppen, 11
Isomorphismus, 11

Koeffizientenvergleich, 27
kommutaiv, 3
Kommutativität, 19
Kommutator, 22
Kommutatorreihe, 23
Kompositionsreihe, 22
Kreisteilungsgleichung, 31

Links-Multiplikation, 11
Links-Nebenklasse, 13

Nebenklasse, 12, 13
neutrales Element, 3
Normalreihe, 22
Normalteiler, 19

Ordnung einer Gruppe, 3
Ordnung eines Elements, 17

Permutation, 7, 13
Polynom, 26
Polynomgleichung, 25
Potenzierung, 10
prime Restklassen, 17

Rechts-Multiplikation, 11
Rechts-Nebenklasse, 13
Restklassen, 6, 14, 17

Satz von Euler, 18
Satz von Feit-Thompson, 22
Satz von Fermat, 18
Satz von Jordan-Hölder, 23
Satz von Lagrange, 15, 20
Satz von Schreier, 23
Satz von Vieta, 30
Satz von Wilson, 18
Subnormalreihe, 22
Subnormalteiler, 21
Symmetrie, 29
symmetrische Gruppe, 8

Tetraeder, 7
Tetraeder-Drehgruppe, 7
Totienten-Funktion, 18
Transposition, 8
triviale Untergruppe, 12
trivialer Normalteiler, 20

Untergruppe, 12
Untergruppen-Verband, 20

Verband, 20

Vervielfachung, 10
Vieta, 27
Vietasche Wurzelgleichungen, 27

Wurzelgleichungen von Vieta, 27

Zerlegung, 15
Zyklenschreibweise, 8
zyklische Gruppe, 16