Lineare Algebra individuell
Online-Fassung, Ver. 0.42
Internes Material, **12.4.2004**

Kapitel 1

Erste algebraische Strukturen

Hier werden die grundlegenden Begriffe eingeführt; sie abstrahieren vom historisch entstandenen Zahlbegriff und erlauben uns, mit nicht allzu großem technischem Aufwand eine Reihe von Resultaten gleichzeitig zu gewinnen, die wir sonst Fall für Fall beweisen müssten. Andererseits ergibt sich ein Ansatz für nicht triviale Erweiterungen vertrauter Sätze über das Rechnen mit Zahlen.

1.1 Gruppen

Eine Abbildung $*: M \times M \to M$, die jedem Paar $(a, b) \in M \times M$ das mit $a * b$ bezeichnete Element aus M zuordnet, wird (zweistellige) *Operation* auf der Menge M genannt. 1/1/1

Definition. (*Monoid*)

M sei eine nichtleere Menge und $*$ eine Operation auf M.

(1) Das Paar $(M, *)$ heißt *Monoid*, falls die folgenden beiden Eigenschaften erfüllt sind:

 (i) Für alle $a, b, c \in M$ ist $a * (b * c) = (a * b) * c$.
 (Assoziativgesetz)

 (ii) Es existiert ein $e \in M$ mit der Eigenschaft, dass für alle $a \in M$ gilt $e * a = a * e = a$.
 (Existenz eines neutralen Elements)

(2) $(M, *)$ heißt *abelsches* (oder *kommutatives*) *Monoid*, falls $(M, *)$ ein Monoid ist und überdies $a * b = b * a$ gilt für alle $a, b \in M$.

Dieser sehr einfache Begriff versteckt sich in nahezu allen algebraischen Strukturen, die wir später kennen lernen.

Eigenschaft (i) besagt, dass wir Klammern weglassen dürfen. M heißt die *zugrundeliegende Menge* und $*$ die *Operation des Monoids* $(M, *)$.
e heißt *neutrales Element*; es ist aufgrund der Bedingung (ii) der Definition eindeutig bestimmt. Denn erfüllen e und e' die Eigenschaft (ii), dann gilt $e * e' = e'$ und $e' * e = e$, außerdem ist $e * e' = e' * e$, folglich $e = e'$.
Für die Operation $*$ verwenden wir im Folgenden meist eines der Symbole $\cdot$ oder $+$. Das Operationszeichen $\cdot$ wird häufig weggelassen, so dass wir für $a \cdot b$ kurz ab schreiben; das Zeichen $+$ wird nicht weggelassen.
Besteht kein Zweifel darüber, welche Operation wir meinen, so wird oft auch einfach von dem Monoid M gesprochen, obwohl (unverändert) das Paar $(M, \cdot)$ gemeint ist.

Vorsicht! Es kann eine Vielzahl von Möglichkeiten geben, auf der Menge M eine Operation $*$ mit den angegebenen Eigenschaften zu definieren.

Beispiele für Monoide.

1. $(\mathbb{N}, +)$ (die natürlichen Zahlen mit der Addition; neutrales Element ist 0),
2. $(\mathbb{Z}, \cdot)$ (die ganzen Zahlen mit der Multiplikation; neutrales Element ist 1),
3. $(\mathbb{Z} \setminus \{0\}, \cdot)$ (die von 0 verschiedenen ganzen Zahlen mit der Multiplikation; neutrales Element ist die Zahl 1)

4. $(\mathbb{Q}, +)$ (die rationalen Zahlen mit der Addition; neutrales Element ist 0)
5. $(\mathrm{S}_n, \cdot)$ (die bijektiven Abbildungen der Menge $\{1, \dots, n\}$ in sich mit dem Produkt von Abbildungen; neutrales Element ist die identische Abbildung $\mathrm{id}_{\{1,\dots,n\}}$)
6. $\big(\mathrm{Abb}(X, X), \cdot\big)$ (die Menge aller Abbildungen einer gegebenen Menge X in sich, zusammen mit dem Produkt von Abbildungen; neutrales Element ist die identische Abbildung id_X)
7. $(\mathrm{S}(X), \cdot)$ (die bijektiven Abbildungen einer gegebenen Menge X auf sich mit der Hintereinanderausführung von Abbildungen; neutrales Element ist die identische Abbildung id_X) – Beispiel 5 ist der Spezialfall $X = \{1, \dots, n\}$.

Offenbar sind die Monoide in 1 – 4 abelsch; in 5, 6 und 7 ist dies für $n > 2$ bzw. $|X| > 2$ nicht der Fall.

Bezeichnungen. In Anlehnung an die obigen Beispiele wird für das neutrale Element bezüglich einer mit $\cdot$ bezeichneten Operation oft das Symbol 1 benutzt.
Bei einer mit $+$ bezeichneten Operation verwenden wir das Symbol 0.

Hier verbirgt sich eine böse Falle: Die Verwendung der Symbole 0 und 1 sagt nichts darüber, welches Element eigentlich vorliegt; es ist ja durch die Operation eindeutig bestimmt.

Sind $a_1, \dots, a_n \in M$, dann setzen wir $\displaystyle\prod_{i=1}^{n} a_i := a_1 \cdot \ldots \cdot a_n$ (auch mit $\prod_{i=1}^n a_i$ bezeichnet). Eine exakte Definition für dieses *Produktzeichen* ist induktiv gegeben mittels

$$\prod_{i=1}^{0} a_i := 1, \qquad \prod_{i=1}^{k+1} a_i := \Big(\prod_{i=1}^{k} a_i\Big)\cdot a_{k+1} \quad (k \in \mathbb{N}).$$

Wir werden in ähnlichen Definitionen meist erstere Schreibweise mit „ … “ verwenden und dem Leser die offensichtliche Präzisierung überlassen.

Im Fall $a = a_1 = \ldots = a_n$ schreiben wir für das obige Produkt auch a^n, insbesondere $a^0 = 1$, und es gelten die *Potenzrechengesetze*

$$a^{m+n} = a^m \cdot a^n, \quad (a^m)^n = a^{m\cdot n} \quad \text{für} \quad m, n \in \mathbb{N},\, a \in M.$$

... eine leichte Übungsaufgabe zur vollständigen Induktion.

Ist die Operation mit dem Symbol $+$ bezeichnet und das neutrale Element mit 0, so wird entsprechend die Notation

$$\sum_{i=1}^{0} a_i := 0, \quad \sum_{i=1}^{k+1} a_i := \Big(\sum_{i=1}^{k} a_i\Big) + a_{k+1} \quad (k \in \mathbb{N})$$

(*Summenzeichen*) verwendet und im Fall $a = a_1 = \ldots = a_n$ auch $\sum_{i=1}^n a_i =: n\cdot a$ gesetzt. Die obigen Formeln lauten dann

$$(n+m)\cdot a = n\cdot a + m\cdot a, \quad (n\cdot m)\cdot a = n\cdot(m\cdot a) \quad (n, m \in \mathbb{N}, a \in M\,).$$

Hier wird nur durch unterschiedliche Symbole derselbe Sachverhalt ausgedrückt.

Bemerkung.

(1) Ist $(M, \cdot)$ abelsch, $a_1, a_2 \in M$, dann gilt $(a_1 \cdot a_2)^n = a_1^n \cdot a_2^n \quad (n \in \mathbb{N})$.

Das hätten Sie wohl ohnehin richtig gemacht, nur vergessen Sie die Voraussetzung nicht!

(2) Für eine endliche Familie $(a_i)_{i\in I}$ von Elementen des kommutativen Monoids $(M, \cdot)$ erhält das Symbol $\prod_{i\in I} a_i$ einen Sinn, indem auf beliebige Weise eine Bijektion $f : \{1, \dots, n\} \to I$ hergestellt wird,

$$\prod_{i\in I} a_i := \prod_{i=1}^{n} a_{f(i)}.$$

Für $I = \emptyset$ bezeichnet $\prod_{i\in I} a_i := 1$ das neutrale Element. Im Fall einer endlichen Teilmenge $X \subseteq M$, die gleichzeitig Indexmenge ist, wird das Symbol $\prod_{a\in X} a$ verwendet.

Warnung.
Z.B. ist für $X = \{1, 2, 3\} \subseteq \mathbb{N}$ das Produkt $\prod_{x\in X} x = 1\cdot2\cdot3 = 6$, jedoch für die Familie $(a_i)_{i=1,\dots,4}$ mit der selben zugrundeliegenden Menge und $a_1 = 1$, $a_2 = 2$, $a_3 = a_4 = 3$ gilt $\prod_{i=1,\dots,4} a_i = 1\cdot2\cdot3\cdot3 = 18$.

(3) Entsprechend (1) erhalten wir im „additiven“ Fall für das kommutative Monoid M (Operationszeichen $+$, neutrales Element 0) die Formel

$$n \cdot (a_1 + a_2) = n \cdot a_1 + n \cdot a_2, \quad n \in \mathbb{N}.$$

Die Symbole

$$\sum_{i \in I} a_i \quad \text{bzw.} \quad \sum_{a \in X} a$$

sind für endliche Indexmengen I bzw. endliche Teilmengen $X \subseteq M$ analog zu (2) definiert, insbesondere $\sum_{a \in X} := 0$ für $X = \emptyset$.

(4) Wir vereinbaren, dass eine Bedingung für *fast alle* Elemente einer Menge I gilt, wenn sie bis auf endlich viele Ausnahmen erfüllt ist.
Nun lassen sich (2) und (3) auch auf beliebige Indexmengen I übertragen, sofern a_i bis auf endlich viele Ausnahmen das neutrale Element ist. Wir setzen beispielsweise

$$\prod_{i \in I} a_i := \prod_{i \in I'} a_i \quad \text{in (2) bzw.} \quad \sum_{i \in I} a_i := \sum_{i \in I'} a_i \quad \text{in (3)},$$

wobei I' jeweils die Menge derjenigen $i \in I$ bezeichnet, für die a_i vom neutralen Element verschieden ist.

Von nun an wird das Operationszeichen $+$ nur noch für abelsche Monoide verwendet. Benutzen wir die multiplikative Schreibweise, so deuten wir dadurch an, dass eine solche Einschränkung nicht von vornherein gemacht wird.

Gruppen und Untergruppen

Definition. (*Gruppe*) 1/1/2

(1) Ein Monoid $(G, \cdot)$ heißt *Gruppe*, falls für alle $a \in G$ ein $b \in G$ existiert mit $b \cdot a = e$ (wobei e das neutrale Element in G bezeichnet).

(2) Eine Gruppe $(G, \cdot)$ heißt *abelsche* (oder *kommutative*) *Gruppe*, falls $(G, \cdot)$ ein abelsches Monoid ist.

Es werden verschiedene (äquivalente) Axiomensysteme für Gruppen verwendet. Dieses ist etwas stärker als unbedingt nötig, für unsere Zwecke jedoch gut brauchbar.

Sind keine Verwechslungen zu befürchten, so lassen wir wieder die Angabe der Operation weg und sprechen kurz von der Gruppe G.

Bemerkung. Mit den obigen Bezeichnungen gilt:

1. Wenn $b \cdot a = e$, so ist auch $a \cdot b = e$.
2. Durch $a \in G$ und die Bedingung $b \cdot a = e$ ist b eindeutig bestimmt. Wir nennen dieses Element das *inverse Element* zu a.
3. Für beliebige $a, b, c \in G$ gilt

$$a \cdot c = b \cdot c \;\Rightarrow\; a = b$$
$$c \cdot a = c \cdot b \;\Rightarrow\; a = b \quad (\textit{Kürzungsregeln}).$$

Beweis. 1. Ist $ba = e$, so ergibt sich mit Hilfe des Assoziativgesetzes $b(ab) = (ba)b = eb = b$. Wir wählen $c \in G$ mit $cb = e$. Dann folgt aus $b(ab) = b$ offenbar $(cb)(ab) = c\big(b(ab)\big) = cb$, also $e(ab) = e$ und folglich $ab = e$.
2. Wenn $ba = e$ und $b'a = e$, so ist $b'(ab) = (b'a)b = eb = b$. Nach 1. gilt $ab = e$, folglich ist $b' = b$.
3. ergibt sich aus 1. und 2., indem die jeweilige Voraussetzung von rechts bzw. links mit dem inversen Element zu c multipliziert wird. ❑

Beispiele. Unter den Beispielen für Monoide (1/1/1) sind (1), (2), (3) keine Gruppen, (4), (5), (7) sind Gruppen, und in (6) erhalten wir genau dann eine Gruppe, wenn die Menge X weniger als zwei Elemente enthält.

Empfehlung: Überprüfen Sie diese Eigenschaften.

Die Gruppe $\big(\mathrm{S}(X), \bullet\big)$ der bijektiven Abbildungen einer Menge X auf sich mit der Komposition von Abbildungen werden wir von nun an auch die *symmetrische Gruppe* oder *Permutationsgruppe* von X nennen, ihre Elemente heißen *Permutationen*.

Hier folgen weitere Beispiele für Gruppen:

1. $(\mathbb{Z}, +)$ (die ganzen Zahlen mit der Addition),
2. $(\mathbb{Q} \setminus \{0\}, \bullet)$ (die Menge der von 0 verschiedenen rationalen Zahlen mit der Multiplikation),
3. $(\{1, -1\}, \bullet)$ (die aus den Zahlen 1, -1 bestehende Menge mit der Multiplikation ganzer Zahlen),
4. $(\{1\}, \bullet)$ (die einelementige Gruppe mit der einzig möglichen Operation).

In Anlehnung an vertraute Schreibweisen verwenden wir künftig die folgenden

Bezeichnungen.

(1) Für eine Gruppe $(G, \cdot)$ wird das neutrale Element meist mit 1, das inverse zu $x \in G$ mit x^{-1} bezeichnet (*multiplikatives Inverses*). Nach der Bemerkung 1 gilt $x \cdot x^{-1} = x^{-1} \cdot x = 1$.

(2) Wird für die Gruppenoperation auf G das Symbol $+$ verwendet, so bezeichnet 0 das neutrale Element und $-x$ das inverse von $x \in G$ (*additives Inverses*). Anstelle der Summe $x + (-y)$ schreiben wir auch $x - y$. Entsprechend gilt $x - x = -x + x = 0$.

(3) Beziehen wir uns in einem gegebenen Zusammenhang auf eine mit $+$ bezeichnete Gruppenoperation, dann sprechen wir auch von einer *additiven* Gruppe, bei Verwendung des Operationszeichens $\cdot$ von einer *multiplikativen* Gruppe.

Strukturtafeln für Gruppen

1/1/3

Ist $(G, \cdot)$ eine Gruppe, so wird die Anzahl $|G|$ der Elemente als ihre *Ordnung* bezeichnet, eine Gruppe endlicher Ordnung auch endlich genannt. Endliche Gruppen können durch sog. *cayleysche Tafeln* (*Gruppentafeln*) angegeben werden.

Diese Illustration des Begriffs der endlichen Gruppe kann beim ersten Lesen auch ignoriert werden

Wir betrachten dazu eine n-elementige Menge $G = \{a_1, \ldots, a_n\}$ und suchen nach einer Gruppenoperation $\bullet$ auf G, für die $e = a_1$ das neutrale Element ist. Nun bilden wir eine Tabelle mit n Zeilen und n Spalten, in der an der j-ten Position der i-ten Zeile das Element $a_i \cdot a_j$ eingetragen wird.

Aus den Gruppeneigenschaften ergeben sich zwei notwendige Bedingungen, die beim Ausfüllen jedenfalls zu beachten sind:

1. Erste Zeile und erste Spalte enthalten (in dieser Reihenfolge) $a_1, \ldots, a_n$.
2. In jeder Zeile steht eine Permutation von $a_1, \ldots, a_n$, ebenso in jeder Spalte.

Dafür g.z.z. $a \cdot a_i = a \cdot a_j \iff a_i = a_j$.

Diese Bedingungen sichern, dass a_1 neutrales Element ist und jedes Element ein inverses besitzt. Schwieriger ist die Überprüfung der Assoziativität; wenn wir nicht aus anderen Gründen wissen, dass eine Gruppe vorliegt, ist der Nachweis dieser Eigenschaft durch explizite Prüfung aller möglichen Fälle sehr aufwändig.

Beispiele.

1. Die zweielementige multiplikative Gruppe $\{1, -1\}$:

$\cdot$	1	-1
1	1	-1
-1	-1	1

2. Die dreielementige Gruppe.

Wir sehen, dass es nur eine einzige Möglichkeit gibt, eine Tafel für $G = \{a_1, a_2, a_3\}$ entsprechend obigen Bedingungen auszufüllen. Denn wäre z.B. $a_2 \cdot a_2 = a_1$, somit $a_2 \cdot a_3 = a_3$, dann hätte die letzte Spalte zwei gleiche Einträge, $\lightning$ (vgl. 2. oben).

Das Auffinden der möglichen Gruppentafeln hat gewisse Ähnlichkeit mit dem Lösen eines Kreuzworträtsels.

$\cdot$	a_1	a_2	a_3
a_1	a_1	a_2	a_3
a_2	a_2	a_3	a_1
a_3	a_3	a_1	a_2

Später zeigt sich, dass tatsächlich eine dreielementige Gruppe existiert, so dass wir uns den Nachweis der Assoziativität hier ersparen können.

vgl. auch die Bemerkung in 1/1/25

Kommutativität einer Gruppe G lässt sich leicht anhand ihrer Strukturtafel überprüfen. Diese Eigenschaft ist genau dann erfüllt, wenn die Tafel von G „symmetrisch zur Hauptdiagonale“ ist (damit ist die Linie gemeint, die von der linken oberen zur rechten unteren Ecke verläuft). Im vorhergehenden und in den beiden folgenden Fällen ist dies erfüllt.

3. Gruppen mit vier Elementen.

Für eine Gruppe der Ordnung 4 erhalten wir (bis auf Umnummerieren der Elemente) die folgenden Möglichkeiten:

vgl. auch die Bemerkung in 1/1/25

$\cdot$	a_1	a_2	a_3	a_4
a_1	a_1	a_2	a_3	a_4
a_2	a_2	a_3	a_4	a_1
a_3	a_3	a_4	a_1	a_2
a_4	a_4	a_1	a_2	a_3

$\cdot$	a_1	a_2	a_3	a_4
a_1	a_1	a_2	a_3	a_4
a_2	a_2	a_1	a_4	a_3
a_3	a_3	a_4	a_1	a_2
a_4	a_4	a_3	a_2	a_1

Später werden wir sehen, dass auch hier in beiden Fällen die Operation assoziativ ist, also tatsächlich Gruppen vorliegen. Aussichtslos wäre es wohl, mit der angegebenen Methode alle 10.494.213 Gruppen aus 512 Elementen zu suchen.

Wir bemerken, dass alle relevanten Eigenschaften der endlichen Gruppen aus ihren Strukturtafeln abgelesen werden können. Dies führt uns später zum Begriff der Isomorphie.

Erste Rechenregeln für Gruppen

Bemerkung. (*Potenzen, direktes Produkt*) 1/1/4

Die Verifikation darf wohl als trivial bezeichnet werden. Führen Sie einzelne der Beweise aus, falls Sie sich mit den Begriffen noch nicht genügend vertraut fühlen. Vollständige Induktion wird wiederholt erforderlich sein.

(1) G sei eine Gruppe. Für $a \in G$ und $n \in \mathbb{N}$ setzen wir $a^{-n} := (a^{-1})^n$. Damit ist a^n für alle ganzen Zahlen n definiert und es gilt

$$a^{m+n} = a^m \cdot a^n \quad \text{sowie} \quad (a^m)^n = a^{m+n} \quad \text{für} \quad m, n \in \mathbb{Z}.$$

Ist G abelsch, so gilt überdies $(a \cdot b)^n = a^n \cdot b^n$ für $a, b \in G$ und $n \in \mathbb{Z}$.

(2) $M_1, \dots, M_n$ seien Monoide. Dann ist die Produktmenge $M_1 \times \dots \times M_n$ ein Monoid mit der Operation

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

wobei (etwas nachlässig) dasselbe Multiplikationszeichen die jeweilige Operation bezeichnet. Dieses Monoid wird künftig das (*direkte*) *Produkt der Monoide* M_i genannt. Im Spezialfall $M_1 = \dots = M_n =: M$ erhalten wir die n-te Potenz M^n von M.
Sind alle Monoide M_i kommutativ, so ist auch ihr Produkt kommutativ. Sind alle M_i Gruppen, dann bildet $M_1 \times \dots \times M_n$ mit der angegebenen Operation eine Gruppe.
Besonders häufig verwenden wir die Gruppenstrukturen auf $\mathbb{Z}^n$ und $\mathbb{Q}^n$, die gemäß der obigen Vereinbarung durch komponentenweise Addition gegeben sind.

Der Begriff unter (2) überträgt sich ohne Schwierigkeiten auf das Produkt M einer beliebigen, nicht notwendig endlichen Familie $(M_i)_{i \in I}$ von Monoiden:

$$M := \bigtimes_{i \in I} M_i, \quad (a_i)_{i \in I} \cdot (b_i)_{i \in I} := (a_i \cdot b_i)_{i \in I}.$$

Warnung. Unsere stillschweigende Übereinkunft hinsichtlich einer einmal fixierten Gruppenoperation sollte nicht zur Nachlässigkeit verleiten. Es können auch scheinbar absurde Situationen auftreten; dafür geben wir ein Beispiel:
Die Menge $\mathbb{Z}$ *der ganzen Zahlen bildet mit der Operation* $m \diamond n := m + n - 1$ *eine abelsche Gruppe* $(\mathbb{Z}, \diamond)$.
Dieser „pathologische" Fall spielt künftig keine Rolle. $\mathbb{Z}$ wird immer mit der vertrauten Operation $+$ betrachtet, und auch andere Gruppen behalten bis auf Widerruf die Operation, mit der sie einmal eingeführt wurden.

Das vorliegende, eher lustige Beispiel kann leicht verifiziert werden.
Assoziativität der Operation:
$m \diamond (n \diamond k) = m + n + k - 2 = (m \diamond n) \diamond k$.
Neutrales Element ist hier die Zahl 1, und $2 - m$ ist invers zu m, denn $m \diamond (2 - m) = m + (2 - m) - 1 = 1$.

Bemerkung. *Es sei* $(G, \cdot)$ *eine Gruppe und* $a, b \in G$. *Dann gilt:* 1/1/5
(1) *Die Gleichungen* $a \cdot x = b$ *und* $y \cdot a = b$ *besitzen jeweils eine eindeutig bestimmte Lösung* $x \in G$ *bzw.* $y \in G$.
(2) $(a^{-1})^{-1} = a$.
(3) $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$.

Beweis. Die Verifikation ist recht einfach; wir zeigen die Eigenschaft (3).
Es gilt $(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1}eb = b^{-1}b = e$, also erfüllt $b^{-1}a^{-1}$ die Definition für das zu ab inverse Element. ❏

Definition. (*Untergruppe*) 1/1/6
Es sei $(G, \cdot)$ eine Gruppe und U eine Teilmenge von G. Dann heißt U eine *Untergruppe* von $(G, \cdot)$, falls die Operation $\cdot$ eine Einschränkung auf U besitzt und U mit dieser eine Gruppe bildet.

Natürlich kann die Menge U nicht leer sein, das neutrale Element von G muss in U liegen und dort ebenfalls das neutrale Element sein. Schließlich ist das inverse Element von $a \in U$ auch in G zu a invers, wir können also dasselbe Symbol a^{-1} dafür verwenden.

Satz. (*Untergruppenkriterium*) 1/1/7

Eine nichtleere Teilmenge U einer Gruppe G ist genau dann Untergruppe, wenn die folgende Bedingung erfüllt ist:

Daraus könnte natürlich auch eine Definition gemacht werden ...

$(*)$ *Für alle* $a, b \in U$ *ist* $a^{-1} \cdot b \in U$.

Beweis. $(\Rightarrow)$ ergibt sich definitionsgemäß aus den Gruppeneigenschaften. Zum Beweis von $(\Leftarrow)$ zeigen wir zunächst, dass das neutrale Element e von G in U liegt. Wegen $U \neq \emptyset$ gibt es ein Element a in G. Voraussetzungsgemäß ist daher $e = a^{-1} \cdot a \in U$ (wir wählen $b = a$ in $(*)$). Weiter ist mit $a \in U$ auch $a^{-1} = a^{-1} \cdot e \in U$ (wir wählen $b = e$ in $(*)$). Nun wenden wir $(*)$ ein weiteres Mal an und finden, dass aus $a, b \in U$ auch $a^{-1}, b \in U$ und damit $a \cdot b = (a^{-1})^{-1} \cdot b \in U$ folgt; die Gruppenoperation besitzt also eine Einschränkung auf U. Da das Assoziativgesetz in der Teilmenge $U \subseteq G$ ohnehin erfüllt ist, folgt die Behauptung. ❑

Beispiele.

1. Jede Gruppe $(G, \cdot)$ besitzt die „trivialen“ Untergruppen $\{e\}$ und G.
2. $(\mathbb{Z}, +)$ ist Untergruppe von $(\mathbb{Q}, +)$.
3. $\{1, -1\}$ ist Untergruppe von $(\mathbb{Q} \setminus \{0\}, \cdot)$.
4. Die bijektiven Abbildungen $\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\}$ mit $\sigma(1) = 1$ bilden eine Untergruppe von S_n.
5. $(G, \cdot)$ sei eine Gruppe, $a \in G$ ein fest gewähltes Element. Dann ist $U := \{a^n \mid n \in \mathbb{Z}\}$ eine Untergruppe (dies folgt nach dem Potenzrechengesetz 1/1/4 (1)). Wir nennen U die von a *erzeugte Untergruppe*.
   Existiert ein Element $a \in G$ mit $G = \{a^n \mid n \in \mathbb{Z}\}$, so heißt $(G, \cdot)$ *zyklisch*.

Das letzte Beispiel lässt sich auf beliebige Teilmengen einer Gruppe verallgemeinern, wir erhalten dann die von einer Teilmenge erzeugte Untergruppe, die nachfolgend konstruiert wird.

Bemerkung. (*Durchschnitt von Untergruppen*) 1/1/8

$\{U_i \mid i \in I\}$ sei eine Menge von Untergruppen der Gruppe G, dann ist auch ihr Durchschnitt $\bigcap\limits_{i \in I} U_i$ eine Untergruppe von G.

Es wird hier nicht verlangt, dass die Indexmenge I endlich ist!

Beweis. Zunächst ist $\bigcap U_i \neq \emptyset$, da das neutrale Element von G darin liegt. Sind $x, y \in G$ für alle $i \in I$, so auch $x^{-1}y$. Die Behauptung folgt nun unmittelbar aus dem Untergruppenkriterium. ❑

Es gibt insbesondere zu jeder Teilmenge $M \subseteq G$ eine kleinste Untergruppe, die diese enthält; sie kann folgendermaßen charakterisiert werden. 1/1/9

Satz. (*Erzeugung von Untergruppen*)

M sei eine Teilmenge von G. Die Menge aller Produkte $a_1^{\nu_1} \cdot \ldots \cdot a_n^{\nu_n}$ mit $n \in \mathbb{N}$, $a_i \in M$, $(i = 1, \ldots, n)$ und $\nu_i \in \{1, -1\}$ ist eine Untergruppe U der Gruppe $(G, \cdot)$.

U ist Durchschnitt aller Untergruppen, die M enthalten und damit kleinste Untergruppe mit dieser Eigenschaft; sie heißt die von M erzeugte Untergruppe. Gleichbedeutend wird M ein Erzeugendensystem der Untergruppe U genannt.

Beweis. Nach dem Untergruppenkriterium bilden die angegebenen Produkte $a_1^{\nu_1} \cdot \ldots \cdot a_n^{\nu_n}$ eine Untergruppe U von G. Diese enthält offensichtlich M (die obigen Produkte mit $n = 1$ und $\nu_1 = 1$). Ist nun U' eine weitere Untergruppe von G, die M enthält, so müssen definitionsgemäß zu allen Elementen von M auch deren Inverse und beliebige Produkte der so erhaltenen in U' liegen, d.h. $U \subseteq U'$. ❑

Besonders einfach lässt sich die im Satz beschriebene Menge von Produkten angeben, wenn $M = \{a_1, \ldots, a_n\}$ und G abelsch ist; wir erhalten dann $\{a_1^{\nu_1} \cdot \ldots \cdot a_n^{\nu_n} \mid \nu_i \in \mathbb{Z}\}$ als die von M erzeugte Untergruppe.

Satz. (*Untergruppen von* $(\mathbb{Z}, +)$) 1/1/10

Jede Untergruppe U *von* $(\mathbb{Z}, +)$ *ist zyklisch, d.h. es existiert eine Zahl* $n \in \mathbb{Z}$, *für die*

$$U = n\mathbb{Z} := \{n \cdot m \mid m \in \mathbb{Z}\}.$$

O.B.d.A. ist $n \geq 0$, denn $n\mathbb{Z} = (-n)\mathbb{Z}$.

Beweis. Für $U = \{0\}$ ist nichts zu beweisen, wir können also annehmen, dass U ein von 0 verschiedenes Element n enthält. Da dann auch $-n \in U$ ist, kann o.B.d.A. $n > 0$ und in U minimal dieser Eigenschaft gewählt werden. Wir zeigen $U = n\mathbb{Z}$:
Für $m \in U$ gilt $m = q \cdot n + r$ mit $0 \leq r < n$ (*Division mit Rest*). Also ist $r = m - q \cdot n \in U$, und die Minimalitätseigenschaft von n impliziert $r = 0$, also $m = q \cdot n \in n\mathbb{Z}$. ❑

Homomorphismen und Isomorphismen 1/1/11

Die cayleyschen Tafeln zeigten uns, dass im Wesentlichen höchstens eine zweielementige und höchstens eine dreielementige Gruppe existieren. Dieses „im Wesentlichen" soll nun präzisiert werden. Um unnötig komplizierte Bezeichnungen zu vermeiden, werden Operationszeichen nur ausnahmsweise angegeben, insbesondere dann, wenn sonst Verwechslungen zu befürchten sind.

Definition. (*Homomorphismen und Isomorphismen*)

G und G' seien Gruppen.

(1) Eine Abbildung $f : G \to G'$ heißt *Homomorphismus von Gruppen* (hier kurz auch *Homomorphismus*), falls $f(ab) = f(a)f(b)$ gilt für alle $a, b \in G$. Werden durch $f : (G, \bullet) \to (G', \bullet')$ die Gruppenoperationen explizit angegeben, so erhält die Definition die Gestalt $f(a \bullet b) = f(a) \bullet' f(b)$.

(2) f heißt *Isomorphismus von Gruppen* (hier kurz auch *Isomorphismus*), falls überdies ein inverser Homomorphismus existiert, d.h. falls ein Homomorphismus $g : G' \to G$ existiert mit $f \cdot g = \mathrm{id}_{G'}$ und $g \cdot f = \mathrm{id}_G$.

Nachlässig ausgedrückt bedeutet (1): Eine Abbildung einer Gruppe in eine andere ist ein Homomorphismus, falls sie die Operationen respektiert. Unter (2) wird für einen Isomorphismus überdies gefordert, das dies in eineindeutiger Weise geschieht.

Bemerkung. Ist $f : G \to G'$ ein Gruppenhomomorphismus und bezeichnen e, e' die neutralen Elemente, so gilt $f(e) = e'$. Weiter wird das inverse eines beliebigen Elements $x \in G$ auf das inverse von $f(x)$ in G' abgebildet.
Die erste dieser Eigenschaften lässt sich beispielsweise dadurch gewinnen, dass auf die Gleichheit $e \cdot e = e$ in G der Homomorphismus f angewendet wird. Wir erhalten $f(e) \cdot f(e) = f(e)$ und nach Multiplikation mit dem inversen Element von $f(e)$ in G' wie behauptet $f(e) = e'$. ❑

Die Eigenschaft $f(x^{-1}) = x^{-1}$ sollten Sie selbst überprüfen.

Beispiele.

1. G sei eine Gruppe, dann ist die identische Abbildung $\mathrm{id}_G : G \to G$ ein Gruppenhomomorphismus.
2. $f : (\mathbb{Z}, +) \to (\mathbb{Z}, +)$ mit $f(n) := -n$ ist ein Gruppenhomomorphismus.
3. $f : (\mathbb{Z}, +) \to (\mathbb{Q} \setminus \{0\}, \cdot)$ mit $f(n) := (-1)^n$ ist ein Gruppenhomomorphismus.
4. $f : (\mathbb{R}, +) \to (\mathbb{R}_{>0}, \cdot)$, ist ein Gruppenhomomorphismus, wenn $f(x)$ die Exponentialfunktion in $\mathbb{R}$ bezeichnet und $\mathbb{R}_{>0} := \{x \in \mathbb{R} \,|\, x > 0\}$ die Menge der positiven reellen Zahlen.
5. Wir betrachten die Untergruppe U einer Gruppe G. Dann ist die Inklusionsabbildung $j : U \to G$ mit $j(x) := x$ für $x \in G$ ein Gruppenhomomorphismus.
6. D_3 sei die Gruppe der Drehungen der Ebene um einen Punkt P, die ein gegebenes gleichseitiges Dreieck mit dem Mittelpunkt P in sich überführen. Die Ecken des Dreiecks bezeichnen wir mit den Zahlen 1, 2, 3. Nun ordnen wir einem Element σ von D_3 die entsprechende Permutation $\sigma : \{1,2,3\} \to \{1,2,3\}$ mit $i \mapsto \sigma(i)$ aus S_3 zu.
   Es entsteht ein injektiver Homomorphismus $D_3 \to \mathrm{S}_3$.

Im 3. bzw. 4. Beispiel ist natürlich die Gruppenoperation in $\mathbb{Q} \setminus \{0\}$ bzw. $\mathbb{R}_{>0}$ gemeint, die durch Einschränkung aus der Multiplikation reeller Zahlen entsteht.
Wir erinnern daran: $\mathrm{e}^{x+y} = \mathrm{e}^x \cdot \mathrm{e}^y$.

Bemerkung. Ein Gruppenhomomorphismus ist genau dann ein Isomorphismus, wenn er bijektiv ist. 1/1/12

Damit lässt sich leicht feststellen, welche der Homomorphismen in den obigen Beispielen auch Isomorphismen sind.
Sind G und G' Gruppen, für die ein Isomorphismus $G \to G'$ existiert, so schreiben wir $G \cong G'$. Offenbar ist $\cong$ eine Äquivalenzrelation auf jeder Menge von Gruppen. ❑

Zum Beweis haben wir nur zu zeigen, dass die inverse Abbildung eines bijektiven Homomorphismus ebenfalls Gruppenhomomorphismus ist.

Die Überprüfung der Homomorphieeigenschaft ist nicht immer leicht. Ein interessantes Beispiel ergibt sich bei der Untersuchung der symmetrischen Gruppe.

Permutationen

$\mathrm{S}_n = \mathrm{S}(I_n)$ bezeichnet die *Gruppe der Permutationen* (*Permutationsgruppe*, auch *symmetrische Gruppe*) der n-elementigen Menge $I_n = \{1, \dots, n\}$. Ihre Elemente $\sigma \in \mathrm{S}_n$ (*Permutationen*) sind die bijektiven Abbildungen von I_n auf sich; wir beschreiben sie durch Wertetafeln und verwenden (etwas nachlässig) die Notation 1/1/13

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

Ist $\tau \in \mathrm{S}_n$ eine weitere Permutation,

$$\begin{pmatrix} 1 & \dots & n \\ \tau(1) & \dots & \tau(n) \end{pmatrix} = \tau,$$

so erhalten wir für das Produkt $\sigma \cdot \tau$ die Wertetafel

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

Die identische Permutation wird durch

$$\mathrm{id} = \begin{pmatrix} 1 \dots n \\ 1 \dots n \end{pmatrix}$$

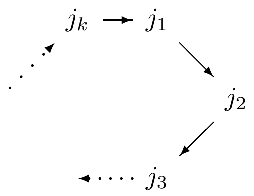
gegeben. In S_3 gilt beispielsweise

$$\begin{pmatrix} 1\,2\,3 \\ 3\,2\,1 \end{pmatrix} \cdot \begin{pmatrix} 1\,2\,3 \\ 2\,3\,1 \end{pmatrix} = \begin{pmatrix} 1\,2\,3 \\ 2\,1\,3 \end{pmatrix}.$$

Es wird hier nicht zwischen einer Permutation und ihrer Wertetafel unterschieden.
Quelle, Ziel und Graph bestimmen natürlich eine Abbildung vollständig.

Definition. (*Zyklus*)

(1) Ein *Zyklus* der Länge $k > 1$ ist eine Permutation $\sigma \in \mathrm{S}_n$, für die paarweise verschiedene Zahlen $j_1, \dots, j_k \in I_n$ (*Elemente des Zyklus*) existieren mit $\sigma(j_i) = j_{i+1}$ für $1 \leq i < k$ und $\sigma(j_k) = j_1$ sowie $\sigma(l) = l$ für $l \notin \{j_1, \dots, j_k\}$. Wir schreiben in diesem Fall auch $\sigma = (j_1 \dots j_k)$.



So stellen wir uns den Ringelreihen vor, der hier *Zyklus* heißt.

(2) Zwei Zyklen $(j_1 \dots j_k)$ und $(j'_1 \dots j'_{k'})$ heißen *elementfremd* (*disjunkt*), wenn sie keine gemeinsamen Elemente besitzen, d.h. falls $\{j_1, \dots, j_k\} \cap \{j'_1, \dots, j'_{k'}\} = \emptyset$ ist.

(3) Zyklen der Länge 2 heißen *Transpositionen.* Dies sind die Zyklen $(j_1 j_2)$, deren Elemente zwei Zahlen $j_1 \neq j_2$ aus I_n sind.

Wir erhalten z.B.

$$(1\,3) = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \text{ in } \mathrm{S}_3, \quad (2\,5\,3) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 2 & 4 & 3 & 6 \end{pmatrix} \text{ in } \mathrm{S}_6,$$

aber $(2\,5\,3)$ kann auch das Element $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 2 & 4 & 3 \end{pmatrix}$ von S_5 bezeichnen – was gemeint ist, haben wir jeweils aus dem Zusammenhang zu entnehmen. Weiter ist $(2\,5\,3) = (5\,3\,2) = (3\,2\,5)$ (die Einträge gehen durch „zyklisches Vertauschen" auseinander hervor), jedoch $(2\,5\,3) \neq (2\,3\,5)$.

Die Bedeutung der Zyklenschreibweise hängt also auch noch davon ab, in welcher der Gruppen S_n wir gerade arbeiten!

Das Rechnen mit Zyklen ist besonders einfach. Beispielsweise gilt $\tau^2 = \mathrm{id}$ für jede Transposition $\tau \in \mathrm{S}_n$.

Satz. *Wir betrachten Permutationen aus* S_n, $n > 1$. 1/1/14

(1) *Sind* σ, τ *elementfremde Zyklen, so ist* $\sigma \cdot \tau = \tau \cdot \sigma$.

(2) *Jede von der Identität verschiedene Permutation ist Produkt elementfremder Zyklen. Die Faktoren dieses Produkts sind bis auf Reihenfolge eindeutig bestimmt* (kanonische Zerlegung).

(3) *Jeder Zyklus ist Produkt von Transpositionen.*

(1) und (2) bilden zusammen einen Klassifikationssatz, der gewisse Ähnlichkeit mit dem Satz über die Primfaktorzerlegung ganzer Zahlen besitzt.

Beweis. (1) und (2) werden offensichtlich, wenn wir uns jeweils den „Weg" eines Elements von $\{1, \dots, n\}$ bei wiederholter Anwendung einer festen Permutation vorstellen – er „schließt sich" nach endlich vielen Schritten.
(3) folgt durch Induktion über die Länge des gegebenen Zyklus $(j_1 \dots j_k)$: Für $k = 2$ ist nichts zu beweisen, und für $k > 2$ ergibt sich $(j_1 \dots j_k) = (j_2 \dots j_k) \cdot (j_1 j_k)$ als Produkt von Zyklen der Länge $< k$. ❏

Beispiele.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 6 & 5 & 4 \end{pmatrix} = (1\,3\,2)\cdot(4\,6) = (4\,6)\cdot(1\,3\,2),$$

$$(1\,3\,2) = (3\,2)\cdot(1\,2) \neq (1\,2)\cdot(3\,2) = (1\,2\,3).$$

Empfehlung: Rechnen Sie das doch einmal nach.

Korollar. (*Zerlegbarkeit in Transpositionen*) 1/1/15

Für $n > 1$ *ist jede Permutation aus* S_n *Produkt von Transpositionen.*

Beweis. Zunächst gilt $\mathrm{id} = (1\,2)^2$. Die Behauptung folgt nun aus dem Satz, indem für jeden Faktor der in (2) gefundenen Zerlegung die Eigenschaft (3) verwendet wird. ❏

Wir dürfen nicht erwarten, dass die Zerlegung in Transpositionen eindeutig ist. Beispielsweise kann zu jeder Faktorzerlegung eine beliebige gerade Anzahl von Faktoren hinzugenommen werden, denn das Quadrat einer Transposition ist die Identität.

Definition. (*Signum*) 1/1/16

$\sigma \in \mathrm{S}_n$ sei eine Permutation.

(1) Eine *Inversion* (*Fehlstellung*) der Permutation σ ist ein Paar $(i,j) \in I_n \times I_n$ mit $i < j$ und $\sigma(i) > \sigma(j)$.

(2) Ist k die Anzahl der Inversionen von σ, so heißt $\operatorname{sign}(\sigma) := (-1)^k$ das *Signum* (*Vorzeichen*) von σ, d.h. $\operatorname{sign}(\sigma) = 1$, falls σ eine gerade Zahl von Inversionen besitzt und anderenfalls $\operatorname{sign}(\sigma) = -1$. Entsprechend wird σ auch eine *gerade* bzw. *ungerade Permutation* genannt.

Beispiele. $\sigma = \binom{1\,2\,3}{3\,2\,1}$ besitzt die Inversionen $(1,2),(1,3),(2,3)$ und $\tau = \binom{1\,2\,3}{2\,3\,1}$ die Inversionen $(1,3),(2,3)$, daher ist $\operatorname{sign}(\sigma) = -1$ und $\operatorname{sign}(\tau) = 1$. Das Produkt $\sigma\cdot\tau = \binom{1\,2\,3}{2\,1\,3}$ hat genau eine Inversion $(1,2)$ und wir erhalten $\operatorname{sign}(\sigma\cdot\tau) = -1$.

Das Ergebnis ist kein Zufall. Es lässt bereits einen Zusammenhang zwischen $\operatorname{sign}(\sigma\cdot\tau)$ und den Vorzeichen von σ und τ vermuten.

Lemma. 1/1/17

(1) *Für* $\sigma \in \mathrm{S}_n$ *ist*
$$\operatorname{sign}(\sigma) \cdot \prod_{(l,m)\in I_n\times I_n,\, l<m} (l-m) = \prod_{(l,m)\in I_n\times I_n,\, l<m} \big(\sigma(l)-\sigma(m)\big).$$

(2) *Ist* $\tau \in \mathrm{S}_n$ *eine Transposition,* $\sigma \in \mathrm{S}_n$ *beliebig, so gilt*
$$\operatorname{sign}(\sigma\cdot\tau) = -\operatorname{sign}(\sigma).$$

(3) $\tau \in \mathrm{S}_n$ *sei eine Transposition. Dann ist* $\operatorname{sign}(\tau) = -1$.

Hier verstecken wir die technischen Vorbereitungen zum Beweis des Satzes, der dann wieder recht einprägsam wird.

(3) können Sie auch als Übung im Zählen von Inversionen betrachten, zu $\tau = (i\,j)$ mit $i < j$ sind dies:
(i,k), $i < k < j$
(l,j), $i < l < j$ und (i,j).

Beweis. Zum Beweis für (1) können wir $n > 1$ annehmen. Die Produkte
$$\prod_{(l,m)\in I_n\times I_n,\, l<m} (l-m) \quad\text{und}\quad \prod_{(l,m)\in I_n\times I_n,\, l<m} (\sigma(l)-\sigma(m))$$
unterscheiden sich höchstens durch das Vorzeichen, denn σ ist eine bijektive Abbildung und vermittelt durch
$$l-m \quad\mapsto\quad \sigma(l)-\sigma(m)$$
eine Permutation der Beträge der Faktoren. Dabei haben die Zahlen $l-m$ und $\sigma(l)-\sigma(m)$ genau dann verschiedene Vorzeichen, wenn (l,m) eine Inversion von σ ist. Die Produkte auf der rechten und linken Seite der behaupteten Beziehung unterscheiden sich damit um den Faktor $(-1)^k$, wobei k die Anzahl der Inversionen von σ bezeichnet.
Zum Beweis für (2) sei $\tau = (i\,j)$ mit $i < j$. Nach (1) ist
$$\operatorname{sign}(\sigma\tau) \cdot \prod_{(l,m)\in I_n\times I_n,\, l<m} (l-m) = \prod_{(l,m)\in I_n\times I_n,\, l<m} \big((\sigma\tau)(l)-(\sigma\tau)(m)\big).$$
Wir vergleichen die Faktoren auf der rechten Seite mit denen der durch (1) gegebenen entsprechenden Formel für $\operatorname{sign}(\sigma)$. Aus $l,m \notin \{i,j\}$ folgt
$$(\sigma\tau)(l)-(\sigma\tau)(m) = \sigma(l)-\sigma(m),$$
und für $(l,m) = (i,j)$ erhalten wir
$$(\sigma\tau)(i)-(\sigma\tau)(j) = \sigma(\tau(i))-\sigma(\tau(j)) = \sigma(j)-\sigma(i) = -\big(\sigma(i)-\sigma(j)\big).$$
Die übrigen Faktoren haben keinen Einfluss auf das Resultat, denn sie lassen sich folgendermaßen zu Paaren zusammenfassen:

Die Faktorenpaare treten auf den entsprechenden Seiten in (2) auf.

$k > j$:
$\big((\sigma\tau)(j) - (\sigma\tau)(k)\big) \cdot \big((\sigma\tau)(i) - (\sigma\tau)(k)\big) = \big(\sigma(j) - \sigma(k)\big) \cdot \big(\sigma(i) - \sigma(k)\big)$,
$i < k < j$:
$\big((\sigma\tau)(k) - (\sigma\tau)(j)\big) \cdot \big((\sigma\tau)(i) - (\sigma\tau)(k)\big) = \big(\sigma(k) - \sigma(j)\big) \cdot \big(\sigma(i) - \sigma(k)\big)$,
$k < i$:
$\big((\sigma\tau)(k) - (\sigma\tau)(i)\big) \cdot \big((\sigma\tau)(k) - (\sigma\tau)(j)\big) = \big(\sigma(k) - \sigma(i)\big) \cdot \big(\sigma(k) - \sigma(j)\big)$.

Daraus ergibt sich

$$\prod_{(l,m)\in I_n\times I_n,\, l<m} \big((\sigma\tau)(l) - (\sigma\tau)(m)\big) = - \prod_{(l,m)\in I_n\times I_n,\, l<m} \big(\sigma(l) - \sigma(m)\big)$$

und so nach (1) die Behauptung (2).
(3) folgt aus (2) als Spezialfall mit $\sigma = \mathrm{id}$. ❏

Satz. 1/1/18

(1) *Sind* $\tau_1, \dots, \tau_k \in \mathrm{S}_n$ *Transpositionen, so gilt* $\mathrm{sign}(\tau_1 \cdot \ldots \cdot \tau_k) = (-1)^k$.

(2) $\mathrm{sign} : \mathrm{S}_n \to \{1, -1\}$ *ist ein Homomorphismus von* S_n *in die multiplikative Gruppe* $\{1, -1\}$, *d.h. für beliebige* $\sigma, \sigma' \in \mathrm{S}_n$ *ist* $\mathrm{sign}(\sigma \cdot \sigma') = \mathrm{sign}(\sigma) \cdot \mathrm{sign}(\sigma')$.

Wir sehen, dass es für die Bestimmung von $\mathrm{sign}(\sigma)$ belanglos ist, welche Ordnung wir auf der Menge $I_n = \{1, \dots, n\}$ gewählt haben.

Beweis. Der Beweis für (1) ergibt sich induktiv mittels (3) und (2) aus dem Lemma. Die Aussage (2) folgt aus (1) und dem vorigen Korollar, denn ist $\sigma = \tau_1 \cdot \ldots \cdot \tau_k$ und $\sigma' = \tau'_1 \cdot \ldots \cdot \tau'_{k'}$ mit Transpositionen τ_i, τ'_j, so gilt $\mathrm{sign}(\sigma) = (-1)^k$, $\mathrm{sign}(\sigma') = (-1)^{k'}$ und daher
$\mathrm{sign}(\sigma \cdot \sigma') = \mathrm{sign}(\tau_1 \cdot \ldots \cdot \tau_k \cdot \tau'_1 \cdot \ldots \cdot \tau'_{k'}) = (-1)^{k+k'} = \mathrm{sign}(\sigma) \cdot \mathrm{sign}(\sigma')$. ❏

Klasseneinteilung durch Untergruppen und Homomorphie 1/1/19

Wir wenden uns einer allgemeinen Eigenschaft von Untergruppen zu: Diese definieren (wie nachfolgend erläutert) eine Äquivalenzrelation und damit eine Klasseneinteilung der gegebenen Gruppe. Im Fall einer *normalen* Untergruppe bilden die Äquivalenzklassen sogar eine Gruppe.

Zunächst wird ein Beispiel betrachtet. In der Gruppe $(\mathbb{Z}, +)$ der ganzen Zahlen bildet die Teilmenge $U = 3\mathbb{Z} := \{3m \mid m \in \mathbb{Z}\}$ eine Untergruppe. Eine ganze Zahl ist genau dann durch 3 teilbar, wenn sie in U liegt. Jede andere ganze Zahl liegt offensichtlich in $\overline{1} := \{1 + u \mid u \in U\}$ oder $\overline{2} := \{2 + u \mid u \in U\}$. Wir setzen noch $\overline{0} := U$. Damit ist jede ganze Zahl aus genau einer der Mengen $\overline{0}, \overline{1}, \overline{2}$, die deshalb eine Klasseneinteilung für $\mathbb{Z}$ bilden. Wir versuchen, auf der dreielementigen Menge $G = \{\overline{0}, \overline{1}, \overline{2}\}$ eine Gruppenoperation anzugeben. Dazu addieren wir beliebige Elemente der Klassen und sehen nach, in welcher Klasse das Resultat liegt; diese Klasse soll als Summe der Klassen definiert werden. So müsste z.B. $\overline{1} + \overline{1} = \overline{2}$ sein, da $1 \in \overline{1}$ und $1 + 1 \in \overline{2}$, oder $\overline{1} + \overline{2} = \overline{0}$, da $1 \in \overline{1}$, $2 \in \overline{2}$ und $1 + 2 \in \overline{0}$ ist. Als Resultat ergibt sich die Tafel:

. . . je nachdem, welchen Rest sie bei Division durch 3 hat.

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

Haben wir beim Ausfüllen nicht etwas falsch gemacht? Es wurde immer nur an einzelnen Beispielen geprüft, in welcher Klasse die Summe zweier Elemente liegt. Nun ist aber auch $6 \in \overline{0}$ und $13 \in \overline{1}$. Wegen $6+13 = 19 = 1+3\cdot 6 \in \overline{1}$ haben wir „Glück“ gehabt. Genau genommen liegt ein allgemeines Prinzip vor. Zwei Zahlen r, r' befinden sich gerade dann in derselben Klasse, wenn $r - r' \in \overline{0}$. Sind s, s' weitere Zahlen, die zur selben Klasse gehören, so folgt entsprechend $s - s' \in \overline{0}$, insgesamt also $(r+s)-(r'+s') = (r-r')+(s-s') \in \overline{0}$, denn U ist als Untergruppe von $\mathbb{Z}$ gegenüber der Addition abgeschlossen. Daher liegen $r + s$ und $r' + s'$ in derselben Klasse, d.h. die obige Definition ist tatsächlich unabhängig von der Wahl der Repräsentanten. Die hier gefundene Tafel stimmt offensichtlich mit der überein, die wir im Beispiel 2 unter 1/1/3 – bis auf die Namen der Einträge – als einzige Möglichkeit für eine dreielementige Gruppe erkannt haben. ❑

Der allgemeine Fall erfordert etwas mehr Vorsicht, denn wir wollen unsere Überlegungen nicht auf kommutative Gruppen beschränken.

Satz – Definition. *U sei eine Untergruppe der Gruppe $(G, \cdot)$. Dann ist durch $\{a\cdot U \mid a \in G\}$ eine Klasseneinteilung von G gegeben;* die Mengen $a\cdot U := \{a\cdot x \mid x \in U\}$ heißen *linke Nebenklassen* von U. 1/1/20
Die entsprechende Aussage gilt auch für die rechten Nebenklassen $U\cdot a := \{x\cdot a \mid x \in U\}$.

Beweis. Offenbar ist $a = a\cdot e \in a\cdot U$ und somit $\bigcup_{a\in G} a\cdot U = G$. Wir haben nur zu beweisen, dass aus $a\cdot U \cap b\cdot U \neq \emptyset$ stets $a\cdot U = b\cdot U$ folgt. Dazu wählen wir x aus dem Durchschnitt und erhalten $x = au = bv$ mit geeigneten $u, v \in U$, also gilt $a = b(vu^{-1}) \in b\cdot U$. Nun sei $c \in a\cdot U$, dann existiert ein $z \in U$ mit $c = az$. Wegen $a = bvu^{-1}$ ist $c = b(vu^{-1}z) \in b\cdot U$. Es folgt $a\cdot U \subseteq b\cdot U$ und analog auch $b\cdot U \subseteq a\cdot U$, daher $a\cdot U = b\cdot U$. ❑

Bemerkung. Alle linken Nebenklassen $a\cdot U$ einer Untergruppe U der Gruppe G sind gleichmächtig. Die entsprechende Aussage gilt für die rechten Nebenklassen $U\cdot a$.

Beweis. Die Abbildung $f : U \to a\cdot U,\ x \mapsto a\cdot x$ ist bijektiv, denn die Gleichung $a\cdot x = b$ besitzt stets eine eindeutig bestimmte Lösung $x \in G$ (vgl. 1/1/5 (2)). ❑

Da U selbst unter den Nebenklassen vorkommt, folgt unmittelbar 1/1/21

Satz. (*Lagrange*)

Ist G eine endliche Gruppe und U eine Untergruppe von G, so ist ihre Ordnung $|G|$ ein ganzzahliges Vielfaches der Ordnung $|U|$.

Diese Teilbarkeitseigenschaft ist grundlegend für die Untersuchung endlicher Gruppen.

Die vorhergehende Bemerkung ergibt weiter: *Die Anzahl der rechten Nebenklassen stimmt mit der Anzahl der linken Nebenklassen von U überein.* Diese Zahl heißt auch *Index* von U in G. 1/1/22

Wir wenden uns nun der Untersuchung von Homomorphismen zu. Das Ziel besteht darin, in gewisser Weise eine Klassifikation zu erhalten.

Definition. (*Kern eines Gruppenhomomorphismus*) 1/1/23

Ist $f : G \to G'$ ein Gruppenhomomorphismus, dann heißt das Urbild $\ker(f) := \{x \in G \,|\, f(x) = e'\}$ des neutralen Elements aus G' der *Kern des Homomorphismus* f.

Bemerkung. $f : G \to G'$ sei ein Gruppenhomomorphismus, dann gilt:

(1) $\ker(f)$ ist Untergruppe von G und $\mathrm{im}(f)$ ist Untergruppe von G'.

(2) f ist genau dann injektiv, wenn $\ker(f)$ nur aus dem neutralen Element der Gruppe G besteht.

Beweis. (1) lässt sich mit Hilfe des Untergruppenkriteriums nachweisen: $\ker(f) \neq \emptyset$, da das neutrale Element $e \in G$ enthalten ist (vgl. 1/1/11, Bemerkung). Aus $x, y \in \ker(f)$ folgt $f(x \cdot y^{-1}) = f(x) \cdot f(y)^{-1} = e \cdot e = e$, also $x \cdot y^{-1} \in \ker(f)$.
In (2) ist ($\Leftarrow$) trivial; ($\Rightarrow$) ergibt sich so: Es sei $f(x) = f(y)$, dann ist $f(x^{-1} \cdot y) = f(x^{-1}) \cdot f(y) = f(x)^{-1} \cdot f(y) = e'$. Nach Voraussetzung gilt daher $x^{-1} \cdot y = e$, d.h. $y = x$. ❑

Die Verifikation von Eigenschaften dieser Art ist nachfolgend nicht mehr ausgeführt, wird allerdings zur Übung empfohlen.

Definition. (*Normalteiler*) 1/1/24

Eine Untergruppe U von G heißt *normal* (oder *Normalteiler*) in G, falls für jedes $a \in G$ rechte und linke Nebenklasse übereinstimmen: $U \cdot a = a \cdot U$.

Der Kern eines Homomorphismus ist stets normal; tatsächlich gilt auch die Umkehrung: *Jede normale Untergruppe ist Kern eines geeigneten Gruppenhomomorphismus.* Dies ergibt sich aus der nachfolgenden Konstruktion.

Dass ein Kern normal ist, ergibt sich durch leichte Rechnung.

Satz – Definition. (*Faktorgruppe*) 1/1/25

U sei Normalteiler der Gruppe G und $G/U := \{a \cdot U \,|\, a \in G\}$ die durch U gegebene Klasseneinteilung von G.
Dann besitzt G/U eine eindeutig bestimmte Operation, für die die kanonische surjektive Abbildung $p : G \to G/U$, $a \mapsto a \cdot U$ ein Gruppenhomomorphismus ist. Die mit dieser Struktur versehene Menge G/U heißt *Faktorgruppe* von G nach U und p der *kanonische Homomorphismus* auf die Faktorgruppe. *Es gilt* $\ker(p) = U$.

Hier liegt ein allgemeines Prinzip vor: Mit Hilfe geeigneter Äquivalenzrelationen werden aus einer gegebenen Gruppe weitere konstruiert, ihre Faktorgruppen.

Beweis. Wir schreiben wie üblich $\overline{a} := a \cdot U$ für die Klasse von $a \in G$ und definieren eine Operation auf der Menge G/U aller Klassen durch

$(*) \quad \overline{a} \cdot \overline{b} := \overline{a \cdot b}.$

Dies ist allerdings nicht a priori sinnvoll, denn die rechte Seite von $(*)$ könnte von der Wahl der Repräsentanten innerhalb der Klassen der Elemente a und b abhängen.
Es sei also $\overline{a} = \overline{a_1}$ und $\overline{b} = \overline{b_1}$. Dann ist $a_1 \in U \cdot a$ und $b_1 \in b \cdot U$ (rechte und linke Nebenklassen stimmen voraussetzungsgemäß überein). Daher gilt $a_1 \cdot b_1 = (u_1 ab) u_2$ mit $u_1, u_2 \in U$ und $u_1 ab = abu_3$ mit $u_3 \in U$, folglich $a_1 b_1 = abu_3 u_2 \in (ab)U$; die Klassen von ab und $a_1 b_1$ haben also einen nichtleeren Durchschnitt und sind deshalb gleich. Damit ergibt sich die Repräsentantenunabhängigkeit von $(*)$.
Nun ist die auf G/U erklärte Operation offenbar assoziativ, besitzt ein neutrales Element $\overline{e}$ (wobei e das neutrale Element in G bezeichnet), und $\overline{a^{-1}} \in G/U$ ist zu $\overline{a}$ invers.
Wir bemerken noch, dass durch $(*)$ die einzig mögliche Operation definiert wird, für die $a \mapsto \overline{a}$ ein Gruppenhomomorphismus ist. ❑

Überprüfen Sie diese Eigenschaften!

Bemerkung. U sei Untergruppe einer kommutativen Gruppe, so ist U normal, daher existiert in diesem Fall stets die Faktorgruppe G/U. Insbesondere gibt es für alle $n \in \mathbb{N}$ mit $n > 0$ eine n-elementige Gruppe $\mathbb{Z}/n\mathbb{Z}$, die offensichtlich zyklisch ist (da von $\overline{1}$ erzeugt). Die Gruppen $\mathbb{Z}/2\mathbb{Z}$ und $\mathbb{Z}/3\mathbb{Z}$ sind vom Isomorphietyp der anfangs durch cayleysche Tafeln angegebenen Gruppen (vgl. 1/1/3). Die dort aufgeführten Tafeln für 4 Elemente gehören zu den Gruppen $\mathbb{Z}/4\mathbb{Z}$ und $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$.

Zum Begriff der zyklischen Gruppe vgl. 1/1/7, 1/1/8.

Wir zeigen die Existenz einer kanonischen Faktorisierung beliebiger Gruppenhomomorphismen. 1/1/26

Satz. (*Homomorphiesatz*)

Für jeden Gruppenhomomorphismus $f : G \to G'$ existiert ein eindeutig bestimmter injektiver Homomorphismus $\iota : G/\ker(f) \to G'$ mit $f = \iota \cdot p$, wobei p den kanonischen Homomorphismus von G auf die Faktorgruppe $G/\ker(f)$ bezeichnet, d.h. es entsteht das folgende Diagramm:

$$\begin{tikzcd} G \arrow[rr, "f"] \arrow[dr, "p"'] & & G' \\ & G/\ker(f) \arrow[ur, "\iota"'] & \end{tikzcd}$$

Insbesondere gilt $\operatorname{im}(f) \cong G/\ker(f)$.

Die Formel $\operatorname{im}(f) \cong G/\ker(f)$ ist eine „populäre“ Formulierung des Homomorphiesatzes. Dabei geht allerdings ein Teil der Information verloren.

Beweis. $\overline{a}$ bezeichne die Menge $a \cdot \ker(f)$. Falls ein Homomorphismus ι mit der angegebenen Eigenschaft existiert, so muss $f(a) = \iota\big(p(a)\big) = \iota(\overline{a})$ für alle $a \in G$ gelten. Damit ist ι eindeutig bestimmt.
Zum Beweis der Existenz eines Homomorphismus ι mit den geforderten Eigenschaften zeigen wir zunächst, dass durch

$$\left(\begin{smallmatrix}*\\*\end{smallmatrix}\right) \qquad \iota(\overline{a}) := f(a)$$

eine Abbildung definiert ist, d.h. die rechte Seite von $\left(\begin{smallmatrix}*\\*\end{smallmatrix}\right)$ nicht von der Wahl des Repräsentanten der Klasse von a abhängt. Ist $\overline{a} = \overline{a_1}$, so gilt offenbar $a_1 \cdot a^{-1} \in \ker(f)$. Daher ist $f(a_1 \cdot a^{-1}) = e'$ das neutrale Element der Gruppe G', d.h. $f(a_1) \cdot f(a)^{-1} = e'$, und wir erhalten leicht $f(a_1) = f(a)$.
Offenbar gilt $f = \iota \cdot p$, und ι ist ein Homomorphismus. Zum Beweis der Injektivität von ι untersuchen wir den Kern:
Definitionsgemäß gilt $f(a) = e' \iff a \in \ker(f)$, und die Klasse $\ker(f)$ bildet das neutrale Element in $G/\ker(f)$. Also ist $\ker(\iota)$ einelementig und somit ι nach Bemerkung 1/1/23 (2) injektiv. ❏

Das angegebene Diagramm macht die Aussage des Satzes besonders anschaulich. 1/1/27 Wir nennen es *kommutativ*, da das Bild eines Elements nicht von der Wahl des Weges abhängt, der beim „Durchlaufen in Richtung der Pfeile“ gewählt wird. Auch künftig werden wir den Begriff *kommutatives Diagramm* sinngemäß verwenden und dadurch Schreibarbeit sparen, wenn Produkte von Abbildungen angegeben werden.

Das Homomorphieprinzip gehört zu den zentralen Ideen der Algebra. Es wird uns in ähnlicher Gestalt noch wiederholt begegnen.

Als erstes Beispiel betrachten wir das Vorzeichen $\operatorname{sign} : \mathrm{S}_n \to \{1, -1\}$. Der Kern dieses Homomorphismus ist die *alternierende Gruppe* A_n. Für $n > 1$ ist sign surjektiv, also $\mathrm{S}_n/A_n \cong \operatorname{im}(\operatorname{sign}) = \{1, -1\}$.

Eine weitere Anwendung des Homomorphiesatzes ist das folgende

Korollar. *Jede zyklische Gruppe ist zu einer der Gruppen* $\mathbb{Z}/n\mathbb{Z}$ *mit* $n \in \mathbb{N}$ *isomorph.* 1/1/28

Beweis. $G = \{a^\nu \mid \nu \in \mathbb{Z}\}$ sei eine zyklische Gruppe. $f : \mathbb{Z} \to G$, $a \mapsto a^\nu$ definiert dann einen Homomorphismus mit $\mathrm{im}(f) = G$. Aus dem Homomorphiesatz folgt $G \cong \mathbb{Z}/\ker(f)$ und so die Behauptung, da der Kern als Untergruppe von $\mathbb{Z}$ die Gestalt $\ker(f) = n\mathbb{Z}$ hat (vgl. 1/1/10). ❑

Schwerpunkte zum gewählten Stoff

• Monoid (Begriff, erste Beispiele)	[1/1/1]
• Produkt- und Summen-Notation in Monoiden	[1/1/1]
• Gruppe (Begriff und elementare Eigenschaften)	[1/1/2, 1/1/4 – 1/1/5]
• Erste Beispiele für Gruppen	[1/1/2 – 1/1/3]
• Untergruppen (Untergruppenkriterium, Erzeugendensysteme)	[1/1/6 – 1/1/10]
• Gruppenhomomorphismen (Begriff, Eigenschaften)	[1/1/11 – 1/1/12]
• Die Gruppe S_n (Rechnen mit Permutationen)	[1/1/13 – 1/1/18]
• Zyklen und Transpositionen	[1/1/13]
• Vorzeichen (Signum) einer Permutation	[1/1/16 – 1/1/18]
• Zerlegung von Permutationen in Zyklen bzw. Transpositionen	[1/1/14]
• Linke und rechte Nebenklassen einer Untergruppe	[1/1/19 – 1/1/20]
• Satz von Lagrange, Index einer Untergruppe	[1/1/21 – 1/1/22]
• Kern eines Gruppenhomomorphismus	[1/1/23]
• Bild und Kern als Untergruppen	[1/1/23]
• Faktorgruppe und kanonischer Homomorphismus	[1/1/24 – 1/1/25]
• Jeder Normalteiler ist Kern eines Gruppenhomomorphismus	[1/1/25]
• Der Homomorphiesatz	[1/1/26]
• Klassifikation der zyklischen Gruppen	[1/1/28]

Sachverzeichnis

Symboles
$(j_1 \dots j_k)$, Zyklus [1/1/13], 10
G/U Faktorgruppe [1/1/25], 14
$U \cdot a$, rechte Nebenklasse [1/1/20], 13
$\prod_{a \in X} a$ [1/1/1], 2
$\prod_{i \in I} a_i$ [1/1/1], 2
$\sum_{a \in X} a$ [1/1/1], 3
$\sum_{i \in I} a_i$ [1/1/1], 3
$a \cdot U$, linke Nebenklasse [1/1/20], 13
S_n [1/1/13], 9

A
abelsches Monoid [1/1/1], 1
additive Gruppe [1/1/2], 4
additives Inverses [1/1/2], 4
alternierende
– Gruppe [1/1/27], 15
Assoziativgesetz
– für Monoide [1/1/1], 1

C
cayleysche Tafeln [1/1/3], 4

D
direktes Produkt
– von Monoiden [1/1/4], 6
disjunkte Zyklen [1/1/13], 10
Durchschnitt
– von Untergruppen [1/1/8], 7

E
elementfremde Zyklen [1/1/13], 10
Erzeugendensystem
– einer Gruppe [1/1/9], 7
Erzeugung von Untergruppen [1/1/9], 7

F
Faktorgruppe [1/1/25], 14
fast alle [1/1/1], 3
Fehlstellung [1/1/16], 11

G
gerade Permutation [1/1/16], 11
Gruppe
– abelsche (kommutative) [1/1/2], 3
– Definition [1/1/2], 3
Gruppenhomomorphismus [1/1/11], 8
Gruppentafeln [1/1/3], 4

H
Homomorphiesatz
– für Gruppen [1/1/26], 15
Homomorphismus
– von Gruppen [1/1/11], 8

I
Index
– einer Untergruppe [1/1/22], 13
inverses Gruppenelement [1/1/2], 3
Inversion [1/1/16], 11
Isomorphismus
– von Gruppen [1/1/11], 8

K
kanonische
– Zerlegung einer Permutation [1/1/14], 10
kanonischer Homomorphismus
– auf die Faktorgruppe [1/1/25], 14
Kern
– eines Gruppenhomomorphismus [1/1/23], 14
Kerne und Bilder von Gruppenhomomorphismen, Gruppenstruktur [1/1/23], 14
kommutatives Diagramm [1/1/27], 15
Kürzungsregel
– für Gruppen [1/1/2], 3

L
linke Nebenklasse [1/1/20], 13

M
Monoid [1/1/1], 1
multiplikative Gruppe [1/1/2], 4
multiplikatives Inverses [1/1/2], 4

N
neutrales Element [1/1/1], 1
normale Untergruppe [1/1/24], 14
Normalteiler [1/1/24], 14

O
Operation
– auf einer Menge [1/1/1], 1
– eines Monoids [1/1/1], 1
Ordnung einer Gruppe [1/1/3], 4

P
Permutation
– [1/1/13], 9
– [1/1/2], 4
Permutationsgruppe
– [1/1/13], 9
– [1/1/2], 4
Potenzrechengesetze [1/1/1], 2
Potenzrechengesetze [1/1/4], 6
Produkt
– von Monoiden [1/1/4], 6

R
rechte Nebenklasse [1/1/20], 13
Repräsentantenunabhängigkeit
– [1/1/25], 14

S
Satz
– von Lagrange [1/1/21], 13
Signum einer Permutation [1/1/16], 11
symmetrische Gruppe [1/1/2], 4

T
Transposition [1/1/13], 10
triviale Untergruppen [1/1/7], 7

U
ungerade Permutation [1/1/16], 11

Untergruppe [1/1/6], 6
Untergruppen der ganzen Zahlen [1/1/10], 8
Untergruppenkriterium [1/1/7], 7

V
Vorzeichen (Signum) einer Permutation [1/1/16], 11

Z
zugrundeliegende Menge
– eines Monoids [1/1/1], 1
zyklische
– Gruppe [1/1/7], 7
– Gruppen, Klassifikation [1/1/27], 16
Zyklus [1/1/13], 10