3. Untergruppen

Nachdem wir nun einige grundlegende Gruppen kennengelernt haben, wollen wir in diesem Kapitel eine einfache Möglichkeit untersuchen, mit der man aus bereits bekannten Gruppen viele weitere gewinnen kann: Beginnend mit einer Gruppe G wollen wir versuchen, durch einfaches Einschränken der gegebenen Verknüpfung auf eine Teilmenge von G neue Gruppen zu erzeugen. Gruppen, die auf diese Art als Teilmengen von anderen entstehen, werden als Untergruppen bezeichnet. Falls ihr bereits die Vorlesung „Grundlagen der Mathematik 1: Lineare Algebra“ gehört habt, kennt ihr diese Idee sicher schon von Untervektorräumen [G, Definition 13.5].

Definition 3.1 (Untergruppen)**.** Es sei $(G,\cdot)$ eine Gruppe und U eine Teilmenge von G (wir schreiben dies als $U \subset G$; die Gleichheit $U = G$ ist dabei zugelassen). Man nennt U eine **Untergruppe** von G, wenn „U mit der gegebenen Verknüpfung selbst wieder eine Gruppe ist“, d. h. wenn gilt:

(a) Für alle $a,b \in U$ ist $a \cdot b \in U$, d. h. die Verknüpfung $\cdot : G \times G \to G$ lässt sich auf eine Verknüpfung $\cdot : U \times U \to U$ einschränken (man sagt auch, U ist **abgeschlossen** bezüglich der Gruppenverknüpfung).

(b) $(U,\cdot)$ ist eine Gruppe.

Ist U eine Untergruppe von G, so schreibt man dies oft als $(U,\cdot) \leq (G,\cdot)$ oder auch kurz als $U \leq G$.

Beispiel 3.2.

(a) Nach Beispiel 1.2 (a) ist $(\mathbb{Z},+) \leq (\mathbb{Q},+) \leq (\mathbb{R},+)$.

(b) Es sei G eine beliebige Gruppe. Dann sind offensichtlich sowohl $\{e\}$ als auch G selbst Untergruppen von G. Aus naheliegenden Gründen werden sie die **trivialen Untergruppen** von G genannt.

Bevor wir zu interessanteren Beispielen von Untergruppen kommen, wollen wir zunächst ein Kriterium beweisen, mit dem man in der Praxis einfach überprüfen kann, ob eine gegebene Teilmenge einer Gruppe eine Untergruppe ist oder nicht.

Satz 3.3 (**Untergruppenkriterium**)**.** *Es sei $(G,\cdot)$ eine Gruppe. Eine Teilmenge $U \subset G$ ist genau dann eine Untergruppe von G, wenn die folgenden drei Bedingungen erfüllt sind:*

(U1) *Für alle $a,b \in U$ gilt $a \cdot b \in U$;*

(U2) *das neutrale Element e von G liegt in U;*

(U3) *zu jedem $a \in U$ liegt auch das inverse Element a^{-1} in U.*

Beweis. Wir müssen zwei Richtungen zeigen:

„$\Rightarrow$“: Es sei $U \leq G$. Wir müssen zeigen, dass die Eigenschaften (U1), (U2) und (U3) gelten.

(U1) Dies gilt natürlich nach Definition 3.1 (a).

(U2) Nach Voraussetzung ist $(U,\cdot)$ eine Gruppe, hat also insbesondere ein neutrales Element $\tilde{e}$, d. h. ein $\tilde{e} \in U$ mit $\tilde{e} \cdot a = a$ für alle $a \in U$. Beachte aber, dass wir noch nicht wissen, dass dieses neutrale Element $\tilde{e}$ von U wirklich gleich dem neutralen Element e von G sein muss – denn die Gleichung $\tilde{e} \cdot a = a$ gilt ja zunächst einmal nur für alle $a \in U$, und nicht für alle $a \in G$. Allerdings zeigt dies die folgende einfache Rechnung: Es ist

$$\begin{aligned} \tilde{e} \cdot \tilde{e} &= \tilde{e} && (\tilde{e} \text{ ist neutral in } U) \\ &= e \cdot \tilde{e}, && (e \text{ ist neutral in } G) \end{aligned}$$

und damit folgt nach der Kürzungsregel aus Lemma 1.10 (c), dass $e = \tilde{e} \in U$.

(U3) Es sei $a \in U$ beliebig. Da U eine Gruppe ist, gibt es in U ein inverses Element $a' \in U$ mit $a' \cdot a = \tilde{e}$, wobei $\tilde{e}$ wie in (U2) das neutrale Element von U bezeichnet. Dieses ist nach (U2) ist aber gleich e, d. h. es ist $a' \cdot a = e$. Also ist a' auch das inverse Element zu a in G. Damit folgt $a^{-1} = a' \in U$.

„$\Leftarrow$“: Nun setzen wir die Eigenschaften (U1), (U2) und (U3) voraus und müssen $U \leq G$ zeigen, d. h. die Bedingungen aus Definition 3.1 nachprüfen.

(a) ist genau die Eigenschaft (U1).

(b) Wir müssen die Gruppenaxiome aus Definition 1.1 (a) für U nachprüfen. Diese sind aber offensichtlich: Die Assoziativität (G1) gilt für alle Elemente von G und damit erst recht für alle Elemente von U, und die Existenz von neutralen und inversen Elementen (G2) bzw. (G3) ergibt sich sofort aus (U2) bzw. (U3). □

03

Bemerkung 3.4.

(a) Satz 3.3 bzw. sein Beweis besagt also insbesondere, dass die neutralen und inversen Elemente einer Untergruppe $U \leq G$ stets dieselben wie von G sind – obwohl wir dies in Definition 3.1 nicht vorausgesetzt haben.

(b) In der Tat kann man (U2) im Untergruppenkriterium sogar noch durch die scheinbar schwächere Bedingung $U \neq \emptyset$ ersetzen: Ist U nicht leer, so gibt es nämlich ein Element $a \in U$, und damit folgt aus (U3) auch $a^{-1} \in U$ und aus (U1) dann $e = a^{-1}a \in U$.

Beispiel 3.5.

(a) In der symmetrischen Gruppe S_n (für ein $n \in \mathbb{N}_{>0}$) ist die Teilmenge

$$U = \{\sigma \in S_n : \sigma(n) = n\}.$$

nach Satz 3.3 eine Untergruppe, da sie die Untergruppenkriterien erfüllt:

(U1) Sind $\sigma, \tau \in U$, also $\sigma(n) = \tau(n) = n$, so ist auch $(\sigma \circ \tau)(n) = \sigma(\tau(n)) = \sigma(n) = n$ und damit $\sigma \circ \tau \in U$.

(U2) Natürlich ist $\mathrm{id}(n) = n$ und damit $\mathrm{id} \in U$.

(U3) Ist $\sigma \in U$, also $\sigma(n) = n$, so gilt auch für die Umkehrabbildung $\sigma^{-1}(n) = n$ und damit $\sigma^{-1} \in U$.

(b) Es sei G eine beliebige Gruppe und $a \in G$. Dann ist die Menge

$$U = \{a^k : k \in \mathbb{Z}\} \subset G$$

aller (positiven und negativen) Potenzen von a eine Untergruppe von G, wie man wieder leicht durch Nachprüfen der Untergruppenkriterien sieht:

(U1) Sind a^k und a^l (für $k, l \in \mathbb{Z}$) zwei Elemente aus U, so ist ihre Verknüpfung $a^k \cdot a^l = a^{k+l}$ (siehe Lemma 1.12 (a)) wieder eine Potenz von a, also ein Element von U.

(U2) Es ist $e = a^0 \in U$.

(U3) Mit $a^k \in U$ ist auch das Inverse $(a^k)^{-1} = a^{-k}$ dieses Elements (siehe Lemma 1.12 (b)) eine Potenz von a, also ein Element von U.

Als konkretes Beispiel ist also für $n \in \mathbb{Z}$

$$n\mathbb{Z} := \{k \cdot n : k \in \mathbb{Z}\},$$

d. h. die Menge aller ganzzahligen Vielfachen von n, eine Untergruppe von $(\mathbb{Z}, +)$ (da wir diese Gruppe additiv schreiben, bezeichnen wir die „Potenzen“ von n natürlich als $k \cdot n$ – siehe Definition 1.11). Beachte auch, dass die Elemente a^k nicht alle verschieden sein müssen: Für die Transposition $(1\ 2) \in S_3$ ist $(1\ 2)^k$ gleich id für gerade und $(1\ 2)$ für ungerade k, und damit ist auch

$$\{\mathrm{id}, (1\ 2)\} = \{(1\ 2)^k : k \in \mathbb{Z}\}$$

eine Untergruppe von S_3.

(c) Die Teilmenge $\{0,2,4\}$ ist keine Untergruppe von $\mathbb{Z}$, da sie die Elemente 2 und 4, aber nicht $2+4=6$ enthält, und damit das Untergruppenkriterium (U1) nicht erfüllt ist.

Aufgabe 3.6. Überprüfe, ob die folgenden Teilmengen U Untergruppen der gegebenen Gruppe G sind:

(a) $G=(\mathbb{Z},+)\times(\mathbb{Q}\backslash\{0\},\cdot)$, $U=\{(a,b)\in G : b=2^a\}$;

(b) $G=S_4$, $U=\{\sigma\in S_4 : \sigma^2=\mathrm{id}\}$;

(c) $G=S(\mathbb{R})$, $U=\{f\colon \mathbb{R}\to\mathbb{R}$ bijektiv mit $f(x)=x$ für alle $x\geq 0\}$;

(d) $G=\mathbb{R}\times\mathbb{R}$, $U=\{(x,y) : y=ax^2+bx+c\}$ für gegebene $a,b,c\in\mathbb{R}$;

(e) G eine beliebige Gruppe, $U=\{a\in G : a\cdot b=b\cdot a$ für alle $b\in G\}$.

Aufgabe 3.7. Es sei U eine Untergruppe einer Gruppe G. Untersuche, welche der folgenden Teilmengen von G in jedem Fall wieder Untergruppen von G sind:

(a) $V=\{aua^{-1} : u\in U\}$ für ein festes $a\in G$;

(b) $V=\{a\in G : aua^{-1}\in U$ für alle $u\in U\}$.

Aufgabe 3.8. Es sei G eine Gruppe und $U\subset G$ eine nicht-leere Teilmenge. Man beweise die folgenden vereinfachten Untergruppenkriterien:

(a) U ist eine Untergruppe von G genau dann, wenn $ab^{-1}\in U$ für alle $a,b\in U$ gilt.

(b) Hat U nur endlich viele Elemente, so ist U eine Untergruppe von G genau dann, wenn $ab\in U$ für alle $a,b\in U$ gilt, also wenn das Untergruppenkriterium (U1) aus Satz 3.3 gilt.

Bemerkung 3.9 (Vereinigungen und Durchschnitte von Untergruppen)**.**

(a) Sind U und V Untergruppen von G, so ist die Vereinigung $U\cup V$ in der Regel *keine* Untergruppe von G: Betrachten wir z. B. wie in Beispiel 3.5 (b) die Untergruppen $U=2\mathbb{Z}$ und $V=3\mathbb{Z}$ von $\mathbb{Z}$, so liegen in der Vereinigung $2\mathbb{Z}\cup 3\mathbb{Z}$ zwar die Zahlen 2 und 3, nicht aber deren Summe $2+3=5$ – das Untergruppenkriterium (U1) aus Satz 3.3 ist also verletzt.

(b) Im Gegensatz zu (a) sind Durchschnitte von Untergruppen jedoch stets wieder Untergruppen – und zwar nicht nur Durchschnitte von *zwei* Untergruppen, sondern sogar von *beliebig vielen* (also evtl. sogar von unendlich vielen). Die korrekte mathematische Notation hierfür lautet wie folgt: Es sei I eine beliebige Menge (die sogenannte *Indexmenge*) und $U_i\leq G$ für alle $i\in I$. Wir haben also für jedes Element i von I eine Untergruppe U_i von G – hätten wir z. B. nur zwei Untergruppen, die wir miteinander schneiden wollen, so könnten wir als Indexmenge $I=\{1,2\}$ wählen und hätten demzufolge die Untergruppen $U_1,U_2\leq G$. Wir behaupten nun, dass der Durchschnitt aller dieser Untergruppen U_i, geschrieben als

$$U=\bigcap_{i\in I} U_i := \{a\in G : a\in U_i \text{ für alle } i\in I\},$$

wieder eine Untergruppe von G ist. In der Tat prüft man die Untergruppenkriterien aus Satz 3.3 schnell nach:

(U1) Es seien $a,b\in U$, also $a,b\in U_i$ für alle $i\in I$. Da jedes U_i eine Untergruppe von G ist, gilt dann (nach dem Untergruppenkriterium angewendet auf die U_i) auch $ab\in U_i$ für alle $i\in I$. Also ist $ab\in U$.

(U2) Das neutrale Element e liegt in jedem U_i und damit auch im Durchschnitt U dieser Untergruppen.

(U3) ist ganz analog zu (U1): Ist $a\in U$, also $a\in U_i$ für alle $i\in I$, so ist auch $a^{-1}\in U_i$ für alle $i\in I$ (da jedes U_i eine Untergruppe von G ist) und somit $a^{-1}\in U$.

Die Untergruppenkriterien aus Satz 3.3 übertragen sich also direkt von den U_i auf ihren Durchschnitt U.

Aufgabe 3.10. Es seien U und V Untergruppen einer gegebenen Gruppe G. Zeige, dass man das Resultat aus Bemerkung 3.9 (a) wie folgt präzisieren kann: Die Vereinigung $U \cup V$ ist genau dann eine Untergruppe von G, wenn $U \subset V$ oder $V \subset U$ gilt (also wenn sozusagen „gar keine echte Vereinigung vorliegt“ und $U \cup V$ bereits eine der Untergruppen U oder V ist).

Mit Hilfe des Durchschnitts von Untergruppen können wir nun eine sehr wichtige und allgemeine Konstruktion durchführen, die es uns erlaubt, aus *jeder* Teilmenge M einer Gruppe G eine Untergruppe zu erzeugen. Wollen wir z. B. aus der Teilmenge $M = \{0,2,4\}$ der Gruppe $G = (\mathbb{Z},+)$ aus Beispiel 3.5 eine Untergruppe machen, so müssen wir zu ihr zunächst die Zahlen $2+2+2=6$, $2+2+2+2=8$ usw. hinzufügen, damit das Untergruppenkriterium (U1) erfüllt ist, und dann für (U3) auch die Inversen $-2,-4,-6,\dots$ der Elemente $2,4,6,\dots$. Wir erhalten so die Menge $2\mathbb{Z}$ aller geraden Zahlen, die wir in Beispiel 3.5 (b) schon als Untergruppe von G erkannt haben. Wir können sie uns also anschaulich als die kleinste Untergruppe von G vorstellen, die M enthält. In der Linearen Algebra – falls ihr sie bereits kennt – wäre das entsprechende Konzept der von gegebenen Vektoren aufgespannte Untervektorraum, der ganz analog der kleinste Untervektorraum ist, der die gegebenen Vektoren enthält [G, Lemma 14.4].

Diese Konstruktion der kleinsten Untergruppe, die eine gegebene Teilmenge enthält, wird formal wie folgt durchgeführt.

Definition 3.11 (Erzeugte Untergruppen)**.** Es sei M eine beliebige Teilmenge einer Gruppe G. Wir setzen

$$\langle M \rangle := \bigcap_{\substack{U \leq G \\ \text{mit } M \subset U}} U,$$

d. h. $\langle M \rangle$ ist der Durchschnitt aller Untergruppen von G, die M enthalten. Nach Bemerkung 3.9 (b) ist $\langle M \rangle$ als Durchschnitt von (in der Regel unendlich vielen) Untergruppen wieder eine Untergruppe von G. Man nennt sie die von M **erzeugte Untergruppe**. Ist $M = \{a_1,\dots,a_n\}$ eine endliche Menge, so schreibt man statt $\langle M \rangle = \langle \{a_1,\dots,a_n\} \rangle$ meistens abgekürzt $\langle a_1,\dots,a_n \rangle$.

Diese Definition sieht auf den ersten Blick sicher sehr technisch und abschreckend aus. Ihre Grundidee ist aber sehr einfach: Wenn wir die *kleinste* Untergruppe von G haben wollen, die M enthält, dann schneiden wir einfach *alle* diese Untergruppen miteinander – wenn das dann wieder eine Untergruppe ist (was wir ja in Bemerkung 3.9 (b) gezeigt haben), dann muss das ja offensichtlich die kleinste sein. Allerdings habt ihr natürlich Recht, wenn ihr vermutet, dass man die von M erzeugte Untergruppe $\langle M \rangle$ ganz sicher nicht dadurch ausrechnen will, dass man wirklich konkret alle Untergruppen U mit $M \subset U$ bestimmt und dann deren Durchschnitt berechnet. Stattdessen ist für die konkrete Bestimmung von $\langle M \rangle$ das folgende Lemma viel handlicher.

Lemma 3.12 (Alternative Charakterisierung erzeugter Untergruppen)**.** *Es sei M eine Teilmenge einer Gruppe G. Dann ist eine Teilmenge $V \subset G$ genau dann die von M erzeugte Untergruppe $\langle M \rangle$, wenn gilt:*

(1) *V ist eine Untergruppe von G, die M enthält; und*

(2) *ist U eine beliebige Untergruppe von G, die M enthält, so ist bereits $V \subset U$.*

Anschaulich ist $\langle M \rangle$ also „die kleinste Untergruppe von G, die M enthält“.

Beweis.

„$\Rightarrow$“: Es sei $V = \langle M \rangle$ wie in Definition 3.11. Wir müssen also die Eigenschaften (1) und (2) für $\langle M \rangle$ zeigen.

(1) Nach Bemerkung 3.9 (b) ist $\langle M \rangle \leq G$. Außerdem schneiden wir in Definition 3.11 nur Mengen miteinander, die M enthalten. Ihr Durchschnitt $\langle M \rangle$ enthält damit natürlich ebenfalls M.

(2) Ist $U \leq G$ mit $M \subset U$, so ist U natürlich eine der Untergruppen, über die wir in Definition 3.11 den Durchschnitt bilden. Dieser Durchschnitt kann daher höchstens kleiner als U sein, d. h. es ist $\langle M \rangle \subset U$.

„$\Leftarrow$“: Wir setzen jetzt voraus, dass V die Bedingungen (1) und (2) des Lemmas erfüllt. Außerdem wissen wir nach dem obigen Teil „$\Rightarrow$“, dass auch $\langle M \rangle$ diese Eigenschaften hat, d. h. dass gilt:

(3) $\langle M \rangle$ ist eine Untergruppe von G, die M enthält; und

(4) ist U eine beliebige Untergruppe von G, die M enthält, so ist bereits $\langle M \rangle \subset U$.

Wir kombinieren nun (1) mit (4): Nach (1) ist V eine Untergruppe, die M enthält. Also können wir (4) auf den Fall $U = V$ anwenden und erhalten $\langle M \rangle \subset V$. Analog können wir (3) mit (2) kombinieren, also (2) auf den Fall $U = \langle M \rangle$ anwenden und erhalten $V \subset \langle M \rangle$. Insgesamt gilt damit also wie behauptet $V = \langle M \rangle$. □

Beispiel 3.13.

(a) Es sei G eine Gruppe und $a \in G$. Wir behaupten, dass dann

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

genau die Untergruppe ist, die wir bereits in Beispiel 3.5 (b) gesehen haben. In der Tat ist dies mit dem Kriterium aus Lemma 3.12 sehr schnell überprüft:

(1) Nach Beispiel 3.5 (b) ist $\{a^k : k \in \mathbb{Z}\}$ eine Untergruppe von G, und natürlich enthält sie das Element a.

(2) Ist U eine beliebige Untergruppe von G, die a enthält, so muss sie wegen des Untergruppenkriteriums aus Satz 3.3 auch alle Verknüpfungen von a und a^{-1}, also alle Potenzen a^k mit $k \in \mathbb{Z}$ enthalten.

Konkret ist z. B. nach Beispiel 3.5 (b)

$$\langle n \rangle = n\mathbb{Z} \text{ in } \mathbb{Z} \text{ für alle } n \in \mathbb{Z}, \text{ insbesondere also } \langle 1 \rangle = \mathbb{Z}, \text{ und}$$
$$\langle (1\ 2) \rangle = \{\mathrm{id}, (1\ 2)\} \text{ in } S_3.$$

(b) Mit der gleichen Begründung wie in (a) ist die in $\mathbb{R}$ von zwei Zahlen $a, b \in \mathbb{R}$ erzeugte Untergruppe gleich

$$\langle a, b \rangle = \{ka + lb : k, l \in \mathbb{Z}\}.$$

(c) In Lemma 2.11 (b) haben wir gesehen, dass jede Permutation eine Verkettung von Transpositionen ist. Nach dem Untergruppenkriterium aus Satz 3.3 bedeutet dies, dass jede Untergruppe von S_n, die alle Transpositionen enthält, bereits die gesamte symmetrische Gruppe S_n ist. Ist $M \subset S_n$ die Menge aller Transpositionen, so gilt also $\langle M \rangle = S_n$.

In der Tat zeigt die folgende Aufgabe, dass die Gruppe S_n sogar schon von nur zwei Elementen erzeugt werden kann:

Aufgabe 3.14. Es sei $n \in \mathbb{N}_{>0}$. Aus Lemma 2.11 (b) wissen wir bereits, dass jede Permutation in S_n eine Verkettung von Transpositionen ist.

(a) Zeige, dass jedes Element von S_n sogar eine Verkettung von *Nachbartranspositionen* $(i\ \ i+1)$ mit $i \in \{1, \ldots, n-1\}$ ist.

(b) Schreibe $(3\ 1\ 2\ 5) \in S_5$ als eine solche Verkettung von Nachbartranspositionen.

(c) Zeige, dass $S_n = \langle (1\ 2\ 3\ \cdots\ n), (1\ 2) \rangle$.

In manchen Fällen ist für die von einer Menge M erzeugte Untergruppe $\langle M \rangle$ auch die folgende explizite „Formel“ nützlich:

Aufgabe 3.15. Es sei M eine Teilmenge einer Gruppe G. Zeige, dass dann

$$\langle M \rangle = \{a_1 \cdot \cdots \cdot a_n : n \in \mathbb{N},\ a_i \in M \text{ oder } a_i^{-1} \in M \text{ für alle } i = 1, \ldots, n\}$$

gilt, d. h. dass $\langle M \rangle$ aus allen Verknüpfungen besteht, die man aus den Elementen von M und ihren Inversen bilden kann.

Aufgabe 3.16. Es sei $n \in \mathbb{N}$ mit $n \geq 3$. Zeige, dass

$$\langle (1\ 3), (1\ 2\ 3) \rangle = \{\sigma \in S_n : \sigma(i) = i \text{ für alle } i \geq 4\}$$

in S_n gilt.

Aufgabe 3.17 (Diedergruppen)**.** Für eine gegebene Zahl $n \in \mathbb{N}_{\geq 3}$ betrachten wir in S_n die Permutationen

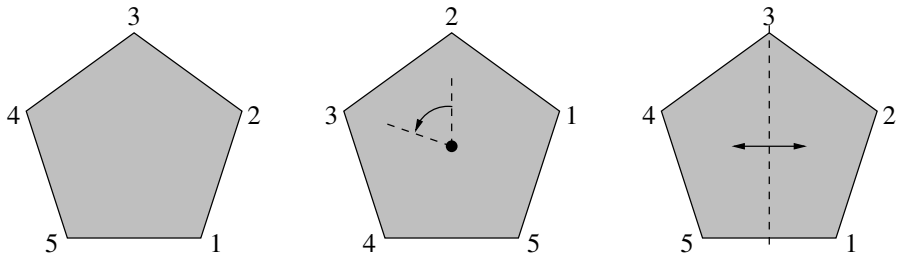
$$\sigma = (1\ 2\ 3\ \cdots\ n) \quad \text{und} \quad \tau\colon \{1,\dots,n\} \to \{1,\dots,n\},\ i \mapsto n+1-i$$

und setzen $D_n := \{\sigma^k \tau^l : k,l \in \mathbb{Z}\} \subset S_n$.

(a) Zeige, dass D_n eine Untergruppe von S_n ist. Offensichtlich ist dann $D_n = \langle \sigma, \tau \rangle$.
(Hinweis: Zeige und benutze die Gleichung $\sigma^{-1}\tau = \tau\sigma$.)

(b) Zeige, dass $|D_n| = 2n$.

Die Gruppe D_n hat eine einfache geometrische Interpretation: Betrachten wir (wie im Bild unten links für $n = 5$ dargestellt) ein regelmäßiges n-Eck in der Ebene, dessen Eckpunkte der Reihe nach mit den Zahlen $1,\dots,n$ bezeichnet sind, so entspricht die Permutation σ genau einer Drehung um den Winkel $\frac{2\pi}{n}$, die Permutation τ einer Spiegelung.



σ: Drehung τ: Spiegelung

Lassen wir in $D_n = \langle \sigma, \tau \rangle$ nun alle möglichen Verknüpfungen dieser beiden Transformationen zu, so erhalten wir insgesamt *alle* möglichen Drehungen und Spiegelungen der Ebene, die das n-Eck auf sich selbst abbilden. Wir können uns D_n also als die *Gruppe aller Symmetrieoperationen bzw. Kongruenzabbildungen eines regelmäßigen n-Ecks* vorstellen.

Man nennt diese Gruppe D_n die **Diedergruppe** (gesprochen: Di-eder) der Ordnung $2n$. Der Name kommt aus dem Griechischen: Ein Dieder ist wörtlich genommen ein „Körper mit zwei Seiten" – ihr kennt analog dazu wahrscheinlich alle ein Tetraeder als eine Figur im Raum, die von vier Seiten begrenzt wird (also eine „Pyramide mit dreieckiger Grundfläche"). Man kann sich nun ein n-Eck wie oben als „degenerierten" Körper mit Volumen 0 im Raum vorstellen, der von zwei Seiten (der Vorderseite und Rückseite) begrenzt wird. Die Symmetriegruppen dieser „Körper" werden daher Diedergruppen genannt.

Im Allgemeinen ist es sehr schwierig, zu einer gegebenen Gruppe alle Untergruppen konkret anzugeben oder auch nur die Anzahl der möglichen Untergruppen zu bestimmen. Im speziellen (und auch wichtigen) Fall der Gruppe $\mathbb{Z}$ hingegen wollen wir nun zeigen, dass es außer den Untergruppen $n\mathbb{Z}$, die wir in Beispiel 3.5 (b) gefunden haben, keine weiteren mehr gibt:

Satz 3.18 (Untergruppen von $\mathbb{Z}$)**.** *Die Untergruppen von $\mathbb{Z}$ sind genau die Mengen $\langle n \rangle = n\mathbb{Z}$ mit $n \in \mathbb{N}$ aus Beispiel 3.5 (b) bzw. 3.13 (a).*

Beweis. Wir wissen aus Beispiel 3.5 (b) bereits, dass $n\mathbb{Z} \leq \mathbb{Z}$ gilt. Wir müssen also nur noch zeigen, dass es zu einer beliebigen Untergruppe $U \leq \mathbb{Z}$ ein $n \in \mathbb{N}$ gibt mit $U = n\mathbb{Z}$.

Nach dem Untergruppenkriterium (U2) muss U die Zahl 0 enthalten. Ist $U = \{0\}$, so ist natürlich $U = 0\mathbb{Z}$ und wir sind fertig. Andernfalls gibt es ein Element $a \in U$ mit $a \neq 0$. Da nach (U3) mit a auch $-a$ in U liegen muss, gibt es dann also sogar eine positive Zahl in U. Es sei nun n die *kleinste* positive Zahl in U. Wir behaupten, dass dann $U = n\mathbb{Z}$ gilt und zeigen diese Gleichheit, indem wir die beiden Inklusionen „$\supset$" und „$\subset$" separat beweisen.

„$\supset$“: Natürlich ist U eine Untergruppe von $\mathbb{Z}$, die das Element n enthält. Nach Lemma 3.12 muss U dann auch die von n erzeugte Untergruppe $\langle n \rangle = n\mathbb{Z}$ enthalten. Es gilt also $U \supset n\mathbb{Z}$.

„$\subset$“: Es sei $a \in U$ beliebig. Indem wir die ganze Zahl a mit Rest durch n dividieren, können wir a schreiben als

$$a = qn + r,$$

wobei $q \in \mathbb{Z}$ gilt und $r \in \{0, \ldots, n-1\}$ der Rest der Division ist. Wir schreiben dies um als

$$r = a - qn.$$

Nun ist $a \in U$ nach Wahl von a, und außerdem auch $-qn \in n\mathbb{Z} \subset U$ nach dem Teil „$\supset$“, den wir bereits gezeigt haben. Wegen der Abgeschlossenheit (U1) von U liegt damit auch die Summe $r = a - qn$ dieser beiden Zahlen in U. Aber r war als Rest der obigen Division kleiner als n, und n war schon als die kleinste positive Zahl in U gewählt! Dies ist natürlich nur dann möglich, wenn r gar nicht positiv ist, also $r = 0$ gilt. Setzen wir dies nun aber oben ein, so sehen wir, dass dann $a = qn + 0 \in n\mathbb{Z}$ folgt. Dies zeigt auch die Inklusion $U \subset n\mathbb{Z}$. $\square$