5. Äquivalenzrelationen

Wenn man eine große und komplizierte Menge (bzw. Gruppe) untersuchen will, so kann es sinnvoll sein, zunächst kleinere, einfachere Mengen (bzw. Gruppen) zu betrachten, die mit dieser zusammenhängen. Eine solche Möglichkeit ist natürlich, Teilmengen (bzw. Untergruppen) zu betrachten, also einfach einige Elemente wegzulassen. Es gibt aber noch eine andere Möglichkeit, bei der man keine Elemente weglassen muss: Man kann Elemente, die in gewissem Sinne „ähnlich sind“ (also für die betrachtete Anwendung gleiche Eigenschaften haben) miteinander identifizieren, also quasi gleich setzen. Formal heißt das, dass man solche „ähnlichen Elemente“ zu einer sogenannten Äquivalenzklasse zusammenfasst und statt mit den ursprünglichen Elementen dann mit diesen Klassen weiter rechnet.

Ein einfaches und sehr anschauliches Beispiel hierfür ist eine (analoge) Uhr, bei der wir der Einfachheit halber annehmen, dass wir nur ganze Stunden ablesen wollen. Eine solche Uhr kann z. B. zwischen 9 Uhr und 21 Uhr nicht unterscheiden, sie betrachtet also diese Zeiten — oder allgemeiner alle Zeiten, die sich nur um ein Vielfaches von 12 unterscheiden — als äquivalent, bzw. fasst sie zu einer Äquivalenzklasse zusammen.

Um diese Idee in ein mathematisch exaktes Konzept umzuwandeln, benötigen wir den Begriff der Äquivalenzrelation.

Definition 5.1 (Äquivalenzrelationen)**.** Es sei M eine Menge.

(a) Eine **Relation** auf M ist eine Teilmenge R des Produkts $M \times M$. Für $(a,b) \in M \times M$ schreibt man statt $(a,b) \in R$ in der Regel $a \sim_R b$ (oder einfach $a \sim b$, wenn klar ist, um welche Relation es geht) und sagt, „a steht in Relation zu b“. Man kann eine Relation also einfach dadurch angeben, dass man festlegt, für welche $a, b \in M$ gelten soll, dass $a \sim b$ ist.

(b) Eine Relation R heißt **Äquivalenzrelation**, wenn die folgenden Eigenschaften gelten:

(A1) Für alle $a \in M$ gilt $a \sim a$ (**Reflexivität**).

(A2) Sind $a, b \in M$ mit $a \sim b$, so gilt auch $b \sim a$ (**Symmetrie**).

(A3) Sind $a, b, c \in M$ mit $a \sim b$ und $b \sim c$, so gilt auch $a \sim c$ (**Transitivität**).

(c) Ist R eine Äquivalenzrelation, so sagt man statt $a \sim b$ auch, dass a (bezüglich dieser Relation) zu b **äquivalent** ist. Zu $a \in M$ heißt dann die Menge

$$\overline{a} := \{b \in M : b \sim a\}$$

aller Elemente, die zu a äquivalent sind, die **Äquivalenzklasse** von a; jedes Element dieser Menge nennt man einen **Repräsentanten** dieser Klasse. Die Menge aller Äquivalenzklassen bezeichnen wir mit

$$M/\sim \; := \; \{\overline{a} : a \in M\}.$$

Beachte, dass sich die Notation $\overline{a}$ einer Äquivalenzklasse immer auf eine gegebene Äquivalenzrelation bezieht, die aus dieser Schreibweise nicht ersichtlich ist und aus dem Zusammenhang klar sein muss.

Beispiel 5.2.

(a) Die einfachste Äquivalenzrelation ist die *Gleichheitsrelation* auf einer beliebigen Menge M, für die genau dann $a \sim b$ gilt, wenn $a = b$ ist. Die Bedingungen aus Definition 5.1 (b) sind hierfür offensichtlich erfüllt. Für alle $a \in M$ ist in diesem Fall $\overline{a} = \{a\}$: Jedes Element a ist nur zu sich selbst äquivalent; es werden keinerlei verschiedene Elemente miteinander identifiziert.

(b) Um das Uhrenbeispiel aus der Einleitung zu diesem Kapitel in unserer neuen Sprache zu formulieren, definieren wir auf $M = \mathbb{Z}$ die Relation

$$a \sim b \quad :\Leftrightarrow \quad b - a = 12k \text{ für ein } k \in \mathbb{Z} \quad \Leftrightarrow \quad b - a \in 12\mathbb{Z},$$

d. h. es gilt genau dann $a \sim b$, wenn eine Uhr a und b Stunden nicht unterscheiden kann. Man sieht sofort, dass dies eine Äquivalenzrelation ist, also die Eigenschaften aus Definition 5.1 (b) erfüllt:

(A1) Für alle $a \in \mathbb{Z}$ ist $a - a = 0 \in 12\mathbb{Z}$ und damit $a \sim a$.

(A2) Sind $a, b \in \mathbb{Z}$ mit $a \sim b$, also $b - a = 12k$ für ein $k \in \mathbb{Z}$, so folgt $a - b = 12 \cdot (-k) \in 12\mathbb{Z}$ und damit auch $b \sim a$.

(A3) Sind $a, b, c \in \mathbb{Z}$ mit $a \sim b$ und $b \sim c$, also $b - a = 12k$ und $c - b = 12l$ für gewisse $k, l \in \mathbb{Z}$, so ist auch $c - a = 12(k + l) \in 12\mathbb{Z}$ und damit $a \sim c$.

Bezüglich dieser Relation ist z. B.

$$\overline{9} = \{b \in \mathbb{Z} : b - 9 \in 12\mathbb{Z}\} = \{\ldots, -15, -3, 9, 21, \ldots\}$$

die Menge aller Zeiten, die von der Uhr als zu 9 Uhr äquivalent angesehen werden. Die Menge aller Äquivalenzklassen ist

$$\mathbb{Z}/\sim \; = \{\overline{0}, \overline{1}, \ldots, \overline{11}\}$$

und entspricht den möglichen Ständen der Uhr.

Wir sehen in diesem Beispiel, dass jede ganze Zahl in *genau einer* Äquivalenzklasse enthalten ist — nämlich in der, die dem zugehörigen Stand der Uhr entspricht. Die Vereinigung aller Äquivalenzklassen ist also die gesamte Menge $\mathbb{Z}$, und zwei verschiedene Äquivalenzklassen sind immer disjunkt, d. h. haben einen leeren Durchschnitt. Man sagt auch, dass die Äquivalenzklassen eine *Partition* der Menge $\mathbb{Z}$ bilden.

Wir wollen jetzt sehen, dass dies bei jeder Äquivalenzrelation so ist.

05

Lemma 5.3. *Für jede Äquivalenzrelation auf einer Menge M gilt:*

(a) *Für $a, b \in M$ gilt $a \sim b$ genau dann, wenn $\overline{a} = \overline{b}$.*

(b) *Jedes Element $a \in M$ liegt in genau einer Äquivalenzklasse. Insbesondere ist M also die disjunkte Vereinigung aller Äquivalenzklassen.*

Beweis.

(a) Es seien $a, b \in M$.

„⇒“: Es sei $a \sim b$ und damit nach (A2) auch $b \sim a$; wir müssen die Gleichheit $\overline{a} = \overline{b}$ zeigen. Wir tun dies, indem wir beweisen, dass die linke Menge in der rechten enthalten ist und umgekehrt.

„⊂“: Sei $c \in \overline{a}$, also $c \sim a$. Wegen $a \sim b$ ist nach (A3) dann auch $c \sim b$, also $c \in \overline{b}$. Damit gilt $\overline{a} \subset \overline{b}$.

„⊃“: Die umgekehrte Inklusion zeigt man analog durch Vertauschen der Rollen von a und b.

„⇐“: Es sei nun $\overline{a} = \overline{b}$. Nach (A1) ist $a \in \overline{a}$, also auch $a \in \overline{b}$. Damit folgt sofort $a \sim b$ nach Definition 5.1 (c).

(b) Wegen der Reflexivität liegt natürlich jedes $a \in M$ in seiner eigenen Äquivalenzklasse $\overline{a}$. Ist nun auch $a \in \overline{b}$ für ein $b \in M$, also $a \sim b$ nach Definition 5.1 (c), so gilt nach (a) bereits $\overline{a} = \overline{b}$. Also liegt a in genau einer Äquivalenzklasse von $\sim$, nämlich in $\overline{a}$. □

Aufgabe 5.4. Zwei Permutationen $\sigma, \tau \in S_n$ heißen *konjugiert* zueinander, in Zeichen $\sigma \sim \tau$, wenn es ein $\alpha \in S_n$ gibt mit $\sigma = \alpha\tau\alpha^{-1}$. Man beweise:

(a) Die Relation $\sim$ ist eine Äquivalenzrelation auf S_n.

(b) Alle Transpositionen in S_n sind zueinander konjugiert.

(c) Die konstante Abbildung 1 und das Signum sind die einzigen Gruppenhomomorphismen von S_n nach $\mathbb{R}\backslash\{0\}$.

Aufgabe 5.5. Es seien U und V zwei Untergruppen einer endlichen Gruppe G. Man zeige:

(a) Durch
$$(u,v) \sim (u',v') \quad :\Leftrightarrow \quad uv = u'v'$$
wird eine Äquivalenzrelation auf $U \times V$ definiert.

(b) Die Äquivalenzklasse von $(u,v) \in U \times V$ ist $\overline{(u,v)} = \{(ua, a^{-1}v) : a \in U \cap V\}$ und besitzt genau $|U \cap V|$ Elemente.

(c) Es gilt die **Produktformel** für Untergruppen
$$|UV| = \frac{|U| \cdot |V|}{|U \cap V|},$$
wobei $UV = \{uv : u \in U, v \in V\}$.

Auch wenn Äquivalenzrelationen verschiedenster Arten an vielen Stellen in der Mathematik auftreten, werden wir in dieser Vorlesung im Wesentlichen nur eine ganz spezielle benötigen. Diese Äquivalenzrelation, die man immer definieren kann, wenn man eine Gruppe und eine darin liegende Untergruppe hat, wollen wir jetzt einführen.

Lemma und Definition 5.6 (Linksnebenklassen)**.** *Es sei G eine Gruppe und $U \leq G$.*

(a) *Die Relation*
$$a \sim b \quad :\Leftrightarrow \quad a^{-1}b \in U$$
(für $a,b \in G$) ist eine Äquivalenzrelation auf G.

(b) *Für die Äquivalenzklasse $\overline{a}$ eines Elements $a \in G$ bezüglich dieser Relation gilt*
$$\overline{a} = aU := \{au : u \in U\}.$$
*Man nennt diese Klassen die **Linksnebenklassen** von U (weil man das Element $a \in G$ links neben alle Elemente von U schreibt). Die Menge aller Äquivalenzklassen dieser Relation, also die Menge aller Linksnebenklassen, wird mit*
$$G/U := G/\sim = \{aU : a \in G\}$$
*bezeichnet. Man liest G/U oft als „G **modulo** U“ und sagt, dass man G/U aus G erhält, indem man U „herausteilt“. Dementsprechend schreibt man für $a,b \in G$ statt $\overline{a} = \overline{b} \in G/U$ auch „$a = b \mod U$“ (gesprochen: $a = b$ modulo U).*

Beweis.

(a) Wir müssen die drei Eigenschaften aus Definition 5.1 (b) zeigen. In der Tat entsprechen diese Eigenschaften in gewissem Sinne genau den drei Eigenschaften des Untergruppenkriteriums aus Satz 3.3:

(A1): Für alle $a \in G$ gilt $a^{-1}a = e \in U$ nach (U2), und damit $a \sim a$ nach Definition von $\sim$.

(A2): Sind $a,b \in G$ mit $a \sim b$, also $a^{-1}b \in U$, so ist nach Lemma 1.10 (b) und (U3) auch $b^{-1}a = (a^{-1}b)^{-1} \in U$ und damit $b \sim a$.

(A3): Sind $a,b,c \in G$ mit $a \sim b$ und $b \sim c$, also $a^{-1}b \in U$ und $b^{-1}c \in U$, so ist nach (U1) auch $a^{-1}c = (a^{-1}b)(b^{-1}c) \in U$ und damit $a \sim c$.

(b) Für $a \in G$ ist

$$\begin{aligned}
\overline{a} &= \{b \in G : b \sim a\} && \text{(Definition von } \overline{a}\text{)} \\
&= \{b \in G : a \sim b\} && \text{(A2)} \\
&= \{b \in G : a^{-1}b = u \text{ für ein } u \in U\} && \text{(Definition von } \sim\text{)} \\
&= \{b \in G : b = au \text{ für ein } u \in U\} \\
&= aU
\end{aligned}$$

genau die Linksnebenklasse von a. □

Bemerkung 5.7. Es sei G eine Gruppe und $U \leq G$.

(a) Nach Lemma 5.3 (a) und Definition 5.6 gilt also für $a, b \in G$ und die dort betrachtete Äquivalenzrelation

$$\overline{a} = \overline{b} \quad \Leftrightarrow \quad a^{-1}b \in U.$$

Wenn wir im Folgenden mit dieser Äquivalenzrelation arbeiten, ist dies vermutlich das Einzige, was wir dafür benötigen werden, da es uns ermöglicht, jede Gleichung zwischen Äquivalenzklassen auf Relationen in der ursprünglichen Gruppe zurückzuführen.

Insbesondere ist also $\overline{b} = \overline{e}$ genau dann, wenn $b \in U$: Es werden genau die Elemente von G mit dem neutralen Element identifiziert, die in U liegen — was noch einmal anschaulich die Sprechweise des „Herausteilens“ von U erklärt.

(b) Es war in Definition 5.6 etwas willkürlich, dass wir $a \sim b$ durch $a^{-1}b \in U$ und nicht umgekehrt durch $ba^{-1} \in U$ definiert haben. In der Tat könnten wir genauso auch für diese „umgekehrte“ Relation eine zu Lemma 5.6 analoge Aussage beweisen, indem wir dort die Reihenfolge aller Verknüpfungen umdrehen. Wir würden dann demzufolge als Äquivalenzklassen also auch nicht die Linksnebenklassen, sondern die sogenannten **Rechtsnebenklassen**

$$Ua = \{ua : u \in U\}$$

erhalten. Ist G abelsch, so sind Links- und Rechtsnebenklassen natürlich dasselbe. Im nichtabelschen Fall werden sie im Allgemeinen verschieden sein, wie wir im folgenden Beispiel 5.8 (b) sehen werden — allerdings wird auch hier später (siehe Lemma 6.5) der Fall, in dem Links- und Rechtsnebenklassen übereinstimmen, eine besonders große Rolle spielen.

Wir vereinbaren im Folgenden, dass wie in Definition 5.6 die Notationen $\overline{a}$ bzw. G/U stets für die *Links*nebenklasse aU bzw. die Menge dieser *Links*nebenklassen stehen. Wollen wir zwischen Links- und Rechtsnebenklassen unterscheiden, müssen wir sie explizit als aU bzw. Ua schreiben.

Beispiel 5.8.

(a) Ist $G = \mathbb{Z}$, $n \in \mathbb{N}_{>0}$ und $U = n\mathbb{Z}$, so erhalten wir die Situation wie in Beispiel 5.2 (b): Für $a, b \in \mathbb{Z}$ ist $a \sim b$ nach Definition 5.6 genau dann, wenn $b - a \in n\mathbb{Z}$ (beachte, dass wir die Gruppenverknüpfung hier additiv schreiben), und die Äquivalenzklassen (also die Linksnebenklassen) sind

$$\overline{a} = a + n\mathbb{Z} = \{\ldots, a-2n, a-n, a, a+n, a+2n, \ldots\},$$

also für $a \in \{0, \ldots, n-1\}$ alle ganzen Zahlen, die bei Division durch n den Rest a lassen. Demzufolge ist die Menge aller Linksnebenklassen die n-elementige Menge

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\},$$

also die „Menge aller möglichen Reste bei Division durch n“. Da dieses Beispiel besonders wichtig ist, hat die Menge $\mathbb{Z}/n\mathbb{Z}$ eine besondere Bezeichnung: Wir setzen

$$\mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z},$$

und schreiben statt $a = b \bmod n\mathbb{Z}$ (also $\overline{a} = \overline{b}$ in $\mathbb{Z}_n$) oft auch kurz $a = b \bmod n$.

Wir können die Stände einer analogen Uhr also mit der Menge $\mathbb{Z}_{12}$ identifizieren.

(b) Wir betrachten die Gruppe $G = S_3$ und darin die Untergruppe

$$U = \langle (1\ 2) \rangle = \{\mathrm{id}, (1\ 2)\}.$$

Ist nun $\sigma_1 = (1\ 2\ 3)$ und $\sigma_2 = (1\ 3\ 2)$, so bilden die drei Linksnebenklassen

$$\begin{aligned}
\overline{\mathrm{id}} &= \mathrm{id} \circ U &&= \{\mathrm{id}, (1\ 2)\}, \\
\overline{\sigma_1} &= \sigma_1 \circ U &&= \{(1\ 2\ 3), (1\ 2\ 3)(1\ 2)\} = \{(1\ 2\ 3), (1\ 3)\}, \\
\overline{\sigma_2} &= \sigma_2 \circ U &&= \{(1\ 3\ 2), (1\ 3\ 2)(1\ 2)\} = \{(1\ 3\ 2), (2\ 3)\}
\end{aligned}$$

offensichtlich eine disjunkte Zerlegung von S_3. Also sind dies nach Lemma 5.3 (b) bereits alle Linksnebenklassen, und wir erhalten

$$S_3/U = \{\overline{\mathrm{id}}, \overline{\sigma_1}, \overline{\sigma_2}\}.$$

Berechnen wir außerdem noch die Rechtsnebenklasse von σ_1, so sehen wir weiterhin, dass

$$U \circ \sigma_1 = \{(1\ 2\ 3), (1\ 2)(1\ 2\ 3)\} = \{(1\ 2\ 3), (2\ 3)\} \neq \sigma_1 \circ U.$$

Links- und Rechtsnebenklassen sind hier also verschieden.

An Beispiel 5.8 (b) fällt auf, dass dort alle Linksnebenklassen gleich viele Elemente haben. Dies ist in der Tat allgemein so, wie das folgende Lemma zeigt.

Lemma 5.9. *Es sei G eine Gruppe und $U \leq G$ eine endliche Untergruppe. Dann hat jede Links- und jede Rechtsnebenklasse von U genauso viele Elemente wie U.*

Beweis. Für $a \in G$ betrachten wir die Abbildung

$$f \colon U \to aU,\ f(u) = au.$$

Nach Definition von aU ist f surjektiv. Die Abbildung f ist aber auch injektiv, denn aus $f(u) = f(v)$, also $au = av$, folgt mit der Kürzungsregel in Lemma 1.10 (c) natürlich sofort $u = v$. Also ist f bijektiv, und damit müssen die Startmenge U und die Zielmenge aU gleich viele Elemente haben. Die Aussage für Ua ergibt sich analog. □

Eine sehr einfache, aber dennoch mächtige Folgerung aus diesem Lemma ist der folgende Satz, der oft beim Auffinden aller Untergruppen einer gegebenen (endlichen) Gruppe nützlich ist.

Satz 5.10 (Satz von Lagrange). *Für jede Untergruppe U einer endlichen Gruppe G gilt*

$$|G| = |U| \cdot |G/U|.$$

Insbesondere ist die Ordnung jeder Untergruppe von G also ein Teiler der Ordnung von G.

Beweis. Nach Lemma 5.3 (b) ist G die disjunkte Vereinigung aller Linksnebenklassen. Die Behauptung des Satzes folgt nun sofort daraus, dass es $|G/U|$ Linksnebenklassen gibt und nach Lemma 5.9 jede von ihnen $|U|$ Elemente hat. □

Wir wollen nun noch ein paar nützliche Folgerungen aus dem Satz von Lagrange ziehen. Dazu benötigen wir die folgende Definition.

Definition 5.11 (Ordnung eines Gruppenelements)**.** Es sei G eine Gruppe und $a \in G$. Gibt es ein $n \in \mathbb{N}_{>0}$ mit $a^n = e$, so heißt das kleinste solche n die **Ordnung** $\operatorname{ord} a$ von a. Existiert kein solches n, so schreibt man oft formal $\operatorname{ord} a = \infty$.

Beispiel 5.12.

(a) Es sei $G = S_n$ und $\sigma = (a_1\ a_2\ \cdots\ a_k)$ ein k-Zykel wie in Notation 2.8 (a). Dann ist $\sigma^k = \mathrm{id}$, denn jedes a_i für $i = 1, \ldots, k$ wird durch k-maliges zyklisches Vorwärtsschieben in der Liste $a_1, \ldots, a_k$ natürlich wieder auf sich selbst abgebildet. Weiterhin ist $\sigma^i \neq \mathrm{id}$ für $1 \leq i < k$, denn in diesem Fall ist z. B. $\sigma^i(a_1) = a_{i+1} \neq a_1$. Also ist $\operatorname{ord} \sigma = k$: Jeder k-Zykel hat die Ordnung k.

(b) In $G = \mathbb{Z}$ ist $\operatorname{ord} 1 = \infty$, denn $n \cdot 1 \neq 0$ für alle $n \in \mathbb{N}_{>0}$.

Aufgabe 5.13. Zeige, dass in jeder Gruppe G für beliebige Elemente $a, b \in G$ gilt:

(a) $\operatorname{ord}(a^{-1}) = \operatorname{ord} a$.

(b) $\operatorname{ord}(ab) = \operatorname{ord}(ba)$.

(c) Ist $\operatorname{ord} a < \infty$ und $f\colon G \to H$ ein Morphismus, so ist $\operatorname{ord} f(a)$ ein Teiler von $\operatorname{ord} a$.

Beachte, dass wir den Begriff „Ordnung“ in den Definitionen 1.1 (c) und 5.11 für zwei zunächst erst einmal verschiedene Konzepte verwendet haben. Der Zusammenhang zwischen ihnen wird aus dem folgenden Lemma deutlich, das zeigt, dass die Ordnung $\operatorname{ord} a$ eines Elements a auch als die Ordnung der von a erzeugten Untergruppe interpretiert werden kann.

Lemma 5.14 (Ordnungen von Elementen und Untergruppen)**.** *Es seien G eine Gruppe und $a \in G$.*

(a) *Ist $\operatorname{ord} a =: n < \infty$, so gilt $\langle a \rangle = \{a^0, \dots, a^{n-1}\}$, und diese n Elemente sind alle verschieden.*

(b) *Ist $\operatorname{ord} a = \infty$, so gilt $\langle a \rangle = \{a^k : k \in \mathbb{Z}\}$, und alle a^k für $k \in \mathbb{Z}$ sind verschieden.*

Insbesondere ist in beiden Fällen also $\operatorname{ord} a = |\langle a \rangle| \in \mathbb{N}_{>0} \cup \{\infty\}$.

Beweis. Nach Beispiel 3.13 (a) ist in jedem Fall zunächst einmal $\langle a \rangle = \{a^k : k \in \mathbb{Z}\}$.

(a) Mit Division durch n mit Rest lässt sich jedes $k \in \mathbb{Z}$ schreiben als $k = qn + r$ mit $q \in \mathbb{Z}$ und $0 \le r \le n-1$. Wegen $a^n = e$ ist damit

$$\begin{aligned}\langle a \rangle &= \{a^{qn+r} : q \in \mathbb{Z} \text{ und } 0 \le r \le n-1\} = \{(a^n)^q \cdot a^r : q \in \mathbb{Z} \text{ und } 0 \le r \le n-1\} \\ &= \{a^r : 0 \le r \le n-1\}.\end{aligned}$$

Weiterhin sind diese n Elemente alle verschieden: Wäre $a^i = a^j$ für gewisse $0 \le i < j \le n-1$, so hätten wir $a^{j-i} = e$, was wegen $0 < j - i < n$ ein Widerspruch dazu ist, dass n nach Definition 5.11 die *kleinste* positive Zahl ist mit $a^n = e$.

(b) Wäre $a^i = a^j$ für gewisse $i, j \in \mathbb{Z}$ mit $i < j$, so wäre wie eben $a^{j-i} = e$ mit $j - i > 0$, im Widerspruch zu $\operatorname{ord} a = \infty$. □

Aus diesem Lemma ergibt sich wieder eine interessante und nützliche Folgerung.

Folgerung 5.15. *Es sei G eine endliche Gruppe und $a \in G$. Dann gilt:*

(a) *$\operatorname{ord} a$ ist ein Teiler von $|G|$.*

(b) ***(Kleiner Satz von Fermat)*** *$a^{|G|} = e$.*

Beweis. Nach Lemma 5.14 hat die von a erzeugte Untergruppe $\langle a \rangle$ die Ordnung $\operatorname{ord} a$. Da diese Ordnung nach dem Satz 5.10 von Lagrange ein Teiler von $|G|$ sein muss, ergibt sich sofort Teil (a). Weiterhin ist (wiederum nach dem Satz von Lagrange)

$$a^{|G|} = a^{|\langle a \rangle| \cdot |G/\langle a \rangle|} = \left(a^{|\langle a \rangle|}\right)^{|G/\langle a \rangle|} = \underbrace{\left(a^{\operatorname{ord} a}\right)}_{=e}^{|G/\langle a \rangle|} = e,$$

und damit folgt auch Teil (b). □

Beispiel 5.16 (Untergruppen von S_3)**.** Mit unseren Ergebnissen können wir nun sehr schnell eine vollständige Liste aller Untergruppen der symmetrischen Gruppe S_3 angeben: Natürlich gibt es zunächst die trivialen Untergruppen $\{\mathrm{id}\}$ und S_3. Ist U eine andere Untergruppe von S_3, muss U sicher ein Element $\sigma \neq \mathrm{id}$ enthalten. Da alle diese Elemente 2-Zykel oder 3-Zykel sind und damit nach Beispiel 5.12 (a) die Ordnung 2 oder 3 haben, können wir die folgenden Fälle unterscheiden:

(a) $\operatorname{ord} \sigma = 2$, d. h. σ ist eine Transposition: Dann ist 2 ein Teiler von $|U|$ nach Folgerung 5.15 (a) und $|U|$ ein Teiler von 6 nach Satz 5.10. Wegen $U \neq G$ ist also $|U| = 2$ und damit $U = \langle \sigma \rangle$. Wir erhalten so die drei Untergruppen

$$\langle (1\ 2) \rangle, \langle (1\ 3) \rangle \quad \text{und} \quad \langle (2\ 3) \rangle.$$

(b) $\operatorname{ord}\sigma = 3$, d. h. σ ist ein Dreierzykel: Wie oben ist dann 3 ein Teiler von $|U|$ und $|U|$ ein Teiler von 6, also $|U| = 3$ und damit wieder $U = \langle\sigma\rangle$. In diesem Fall gibt es nur eine solche Untergruppe, die beide Dreierzykel von S_3 enthält, nämlich

$$\langle(1\ 2\ 3)\rangle = \{\mathrm{id}, (1\ 2\ 3), (1\ 3\ 2)\} = A_3$$

wie in Beispiel 4.17.

Insgesamt hat S_3 also die sechs Untergruppen $\{\mathrm{id}\}, \langle(1\ 2)\rangle, \langle(1\ 3)\rangle, \langle(2\ 3)\rangle, \langle(1\ 2\ 3)\rangle$ und S_3.

Aufgabe 5.17. Es seien $\sigma, \tau \in S_4$ mit $\operatorname{ord}\sigma = 3$ und $\operatorname{ord}\tau = 2$. Welche Ordnung kann dann die von diesen beiden Elementen erzeugte Untergruppe $\langle\sigma, \tau\rangle$ haben? Man gebe für jede solche mögliche Ordnung ein Beispiel an.

Aufgabe 5.18. Bestimme alle Untergruppen der Diedergruppe D_5 aus Aufgabe 3.16.

06