KAPITEL 3

Gruppen

1. Definition und erste Beispiele

DEFINITION. *Eine* **Gruppe** *ist ein Monoid, in dem jedes Element invertierbar ist. Wir schreiben dies nochmals aus:*

- *Eine Menge G mit einer Verknüpfung $*$ ist eine Gruppe, wenn folgende Bedingungen erfüllt sind:*
  (1) *Die Verknüpfung ist assoziativ, d.h. $a*(b*c) = (a*b)*c$ für alle $a, b, c \in G$.*
  (2) *Es existiert eine neutrales Element $e \in G$, d.h. $a*e = e*a = a$ für alle $a \in G$. (Wir wissen, dass e dadurch eindeutig bestimmt ist.)*
  (3) *Zu jedem $a \in G$ existiert ein $b \in G$ mit $b*a = a*b = e$. (Wir wissen, dass b dadurch eindeutig bestimmt ist.) b heißt das zu a* **inverse Element**.
- *Die Verknüpfung kann unterschiedlich geschrieben werden:*
  (1) **Multiplikative Schreibweise:** *Die Verknüpfung schreibt sich dann als Produkt $a \cdot b$ oder einfach ab. Das neutrale Element wird als e oder als 1 geschrieben, das Inverse zu a als a^{-1}.*
  (2) **Additive Schreibweise:** *Die Verknüpfung schreibt sich dann als Summe $a+b$. Das neutrale Element wird in der Regel als 0 geschrieben, d.h. $a+0 = 0+a = a$. Das zu a inverse Element wird als $-a$ geschrieben.*
- *Eine Gruppe heißt* **abelsch** *oder* **kommutativ**, *wenn die Verknüpfung kommutativ ist, d.h. wenn $a*b = b*a$ bzw. $ab = ba$ bzw. $a+b = b+a$ gilt. Andernfalls spricht man von einer* **nichtabelschen** *oder* **nichtkommutativen** *Gruppe.*
- *Eine Gruppe G heißt* **endliche Gruppe**, *wenn G eine endliche Menge ist; $|G|$ heißt dann die* **Gruppenordnung**. *Im andern Fall spricht man von einer* **unendlichen Gruppe**.

Beispiele:

(1) Monoide, in denen jedes Element invertierbar ist, sind Gruppen. Daher ergeben sich unmittelbar folgende Beispiele:
  (a) $(\mathbb{Z}, +)$ ist eine unendliche abelsche Gruppe.
  (b) Für einen Körper K (wie $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$) sind
  $$(K, +), \quad (K^n, +), \quad (\mathrm{Mat}(m \times n, K), +)$$
  abelsche Gruppen.
  (c) $(\mathbb{Z}_n, +)$ ist für jedes $n \in \mathbb{N}$ eine abelsche Gruppe (mit n Elementen).
(2) Monoide, in denen nicht jedes Element invertierbar ist, sind keine Gruppen.
  (a) Für einen Körper K (wie $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$) sind
  $$(K, \cdot), \quad (\mathrm{M}_n(K), \cdot)$$
  keine Gruppen. (0 ist nicht invertierbar.)
  (b) $(\mathbb{Z}_n, \cdot)$ ist für $n \geq 2$ keine Gruppe, da die 0 nicht invertierbar ist, d.h. es gibt kein $x \in \mathbb{Z}_n$ mit $0 \cdot x = 1$.

Bemerkungen: Wir erinnern nochmals an ein paar Formeln aus dem letzten Kapitel:

Datei: alg_gruppen.tex. Version vom 29.11.2023

(1) Ist G eine multiplikativ geschriebene Gruppe, so gelten für die Inversenbildung die Regeln

$$(gh)^{-1} = h^{-1}g^{-1} \quad \text{und} \quad (g^{-1})^{-1} = g.$$

Außerdem gelten die Potenzrechenregeln

$$g^m \cdot g^n = g^{m+n} \quad \text{und} \quad (g^m)^n = g^{mn} \quad \text{für alle } m, n \in \mathbb{Z}.$$

(2) Ist G eine additiv geschriebene Gruppe, so gilt

$$-(g+h) = (-h) + (-g) \quad \text{und} \quad -(-g) = g$$

und

$$m \cdot g + n \cdot g = (m+n) \cdot g \quad \text{und} \quad n \cdot (m \cdot g) = (mn) \cdot g \quad \text{für alle } m, n \in \mathbb{Z}.$$

Bemerkung: Man kann sich fragen, ob die angegebenen Gruppenaxiome alle nötig sind, oder ob sich gewisse Eigenschaften aus anderen ergeben. Dies ist tatsächlich der Fall. Das folgende Lemma zeigt eine solche Situation. Für uns werden solche Fragen aber keine große Rolle spielen.

LEMMA. *Sei G eine Menge mit einer assoziativen Verknüpfung $*$.*

- *Es gebe ein Element $e \in G$, sodass gilt*

$$ea = a \text{ für alle } a \in G.$$

(Existenz eines linksneutrales Elements.)

- *Zu jedem $a \in G$ gebe es ein Element $b \in G$ mit*

$$ba = e.$$

(Existenz von linksinversen Elementen.)

Dann ist G eine Gruppe mit neutralem Element e, jedes linksinverse Element ist auch rechtsinvers.

Beweis: Sei $a \in G$. Dann gibt es ein $b \in G$ mit $ba = e$. Dann ist

$$bab = (ba)b = eb = b.$$

Zu b existiert ein c mit $cb = e$. Wir multiplizieren die Gleichung $b = bab$ mit c von links:

$$e = cb = c(bab) = (cb)ab = eab = ab.$$

Damit ist b auch ein rechtsinverses von a. Damit folgt nun:

$$ae = a(ba) = (ab)a = ea = a.$$

Also ist e auch rechtsneutral. e ist also ein neutrales Element und zu jedem a existiert ein inverses Element. Daher ist G eine Gruppe. ■

Das folgende Lemma zeigt, wie ein Monoid zu einer Gruppe führt.

LEMMA. *Sei $(M, *)$ ein Monoid und M^* die Menge der invertierbaren Elemente, d.h.*

$$M^* = \{a \in M : a \text{ ist invertierbar}\}.$$

Dann ist M^* mit der Verknüpfung $*$ eine Gruppe.

Beweis: Im letzten Kapitel haben wir gezeigt, dass M^* ein Untermonoid ist, und dass mit a auch a^{-1} in M^* liegt. Dies beweist das Lemma. ■

Beispiele:

(1) Ist K ein Körper (wie $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$), so ist im Monoid $(K, \cdot)$ jedes Element ungleich 0 invertierbar. Setzen wir

$$K^* = K \setminus \{0\},$$

so ist also $(K^*, \cdot)$ eine abelsche Gruppe.

(2) Ist K ein Körper, so ist $(\mathrm{M}_n(K), \cdot)$ ein Monoid mit neutralem Element $\mathbf{1}_n$. Die Menge der invertierbaren Elemente schreibt man üblicherweise als

$$\mathrm{GL}_n(K) = \{A \in \mathrm{M}_n(K) : A \text{ ist invertierbar}\}.$$

Die Gruppe $\mathrm{GL}_n(K)$ wird auch die **allgemeine lineare Gruppe** oder **general linear group** genannt. Bekanntlich ist eine quadratische Matrix genau dann invertierbar, wenn ihre Determinante $\neq 0$ ist. Damit erhält die Darstellung

$$\mathrm{GL}_n(K) = \{A \in \mathrm{M}_n(K) : \det A \neq 0\}.$$

Ist $A \in \mathrm{GL}_n(K)$, bringt man die $n \times 2n$-Matrix $(A|\mathbf{1}_n)$ auf reduzierte Zeilenstufenform, so erhält man die Matrix $(\mathbf{1}_n|A^{-1})$:

$$(A|\mathbf{1}_n) \xrightarrow{\text{elementare Zeilentranformationen}} (\mathbf{1}_n|A^{-1}).$$

Dabei steht rechts die zu A inverse Matrix A^{-1}.
Für die inverse Matrix A^{-1} kann man auch eine Formel angeben: Ist A^{adj} die zu A adjungierte Matrix, so gilt

$$A^{-1} = \frac{1}{\det A} A^{\mathrm{adj}}.$$

Im Fall von 2×2-Matrizen erhält man die bekannte Formel

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

(3) Für eine nichtleere Menge M bildet $(\mathrm{Abb}(M, M), \circ)$ ein Monoid. Die invertierbaren Elemente sind gerade die bijektiven Funktionen. Man schreibt $S(M)$ oder $\mathfrak{S}(M)$ für die zugehörige Gruppe:

$$S(M) = \mathfrak{S}(M) = \{f : M \to M : f \text{ bijektiv}\}.$$

Das neutrale Element ist id_M, invers zu f ist die inverse Abbildung f^{-1}.

(4) Wir haben gesehen, dass im Monoid $(\mathbb{Z}_n, \cdot)$ ein Element a genau dann invertierbar ist, wenn $\mathrm{ggT}(n, a) = 1$ gilt. Wir schreiben

$$\mathbb{Z}_n^* = \{a \in \{0, 1, \ldots, n-1\} : \mathrm{ggT}(n, a) = 1\}.$$

Dann ist $(\mathbb{Z}_n^*, \cdot)$ eine abelsche Gruppe. Die Mächtigkeit der Gruppe hat einen eigenen Namen.

DEFINITION. *Die* **Eulersche φ-Funktion** $\varphi : \mathbb{N} \to \mathbb{N}$ *wird definiert durch*

$$\varphi(n) = |\mathbb{Z}_n^*| = |\{a \in \{0, 1, \ldots, n-1\} : \mathrm{ggT}(n, a) = 1\}|.$$

Beispiele:

n	$\mathbb{Z}_n^*$	$\varphi(n)$
1	$\{0\}$	1
2	$\{1\}$	1
3	$\{1,2\}$	2
4	$\{1,3\}$	2
5	$\{1,2,3,4\}$	4
6	$\{1,5\}$	2
7	$\{1,2,3,4,5,6\}$	6
8	$\{1,3,5,7\}$	4
9	$\{1,2,4,5,7,8\}$	6
10	$\{1,3,7,9\}$	4
11	$\{1,2,3,4,5,6,7,8,9,10\}$	10
12	$\{1,5,7,11\}$	4
13	$\{1,2,3,4,5,6,7,8,9,10,11,12\}$	12
14	$\{1,3,5,9,11,13\}$	6
15	$\{1,2,4,7,8,11,13,14\}$	8
16	$\{1,3,5,7,9,11,13,15\}$	8
17	$\{1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16\}$	16
18	$\{1,5,7,11,13,17\}$	6
19	$\{1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18\}$	18
20	$\{1,3,7,9,11,13,17,19\}$	8
21	$\{1,2,4,5,8,10,11,13,16,17,19,20\}$	12
22	$\{1,3,5,7,9,13,15,17,19,21\}$	10
23	$\{1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22\}$	22
24	$\{1,5,7,11,13,17,19,23\}$	8
25	$\{1,2,3,4,6,7,8,9,11,12,13,14,16,17,18,19,21,22,23,24\}$	20
26	$\{1,3,5,7,9,11,15,17,19,21,23,25\}$	12
27	$\{1,2,4,5,7,8,10,11,13,14,16,17,19,20,22,23,25,26\}$	18
28	$\{1,3,5,9,11,13,15,17,19,23,25,27\}$	12
29	$\{1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28\}$	28
30	$\{1,7,11,13,17,19,23,29\}$	8

Bemerkungen:

(1) Für eine Primzahl p sind alle Zahlen zwischen 1 und $p-1$ teilerfremd, während $\mathrm{ggT}(p,0) = p > 1$ gilt. Daher ist
$$\varphi(p) = p - 1.$$
(2) Wir werden später noch eine Reihe von Eigenschaften der Funktion $\varphi(n)$ kennenlernen.

Bemerkungen: Wir erwähnen noch ein paar Eigenschaften, die aus den Gruppeneigenschaften folgen. Sei $(G, \cdot)$ eine Gruppe und seien $a, b, c \in G$.

(1) „Kürzungsregel“: Aus $ac = bc$ oder $ca = cb$ folgt $a = b$. (Dies sieht man, wenn man die Gleichungen von rechts bzw. links mit c^{-1} multipliziert.)
(2) „Lösbarkeit von Gleichungen“: Die Gleichung $ax = b$ hat genau eine Lösung, nämlich $x = a^{-1}b$. Die Gleichung $xa = b$ hat genau eine Lösung, nämlich $x = ba^{-1}$.

Bemerkung: Eine Matrix $A \in \mathrm{M}_n(K)$ beschreibt eine lineare Abbildung $K^n \to K^n$. Nach einem Basiswechsel wird die lineare Abbildung durch eine Matrix der Form $T^{-1}AT$ beschrieben mit einer Matrix $T \in \mathrm{GL}_n(K)$. Die Matrizen A und $T^{-1}AT$ nennt man ähnlich. Dies wird nun verallgemeinert:

Definition. *Sei G eine (multiplikativ geschriebene) Gruppe. Zwei Gruppenelemente $a, b \in G$ heißen* **konjugiert**, *wenn es ein $g \in G$ gibt mit*
$$b = gag^{-1}.$$

Es ist klar, dass Konjugiertheit nur für nichtabelsche Gruppe interessant ist.

LEMMA. *Sei G eine Gruppe mit neutralem Element e.*

(1) *Konjugiertheit von Elementen in G ist eine Äquivalenzrelation.*
(2) *Für $a, b, g \in G$ gilt*
$$gabg^{-1} = gag^{-1} \cdot gbg^{-1}.$$
(3) *Für $a, g \in G$ und $n \in \mathbb{N}$ gilt*
$$ga^n g^{-1} = (gag^{-1})^n.$$

Beweis:

(1)
- Aus $b = gag^{-1}$ und $c = hbh^{-1}$ folgt
$$c = h(gag^{-1})h^{-1} = (hg)a(hg)^{-1},$$
was die Transitivität der Konjugiertheit zeigt.
- Aus $b = gag^{-1}$ folgt
$$a = g^{-1}bg = g^{-1}b(g^{-1})^{-1},$$
was die Symmetrie der Konjugiertheit zeigt.
- Natürlich gilt $a = eae^{-1}$, was die Reflexivität der Konjugiertheit zeigt.

(2) Dies ist klar.
(3) Dies folgt durch Induktion aus (2) oder direkt so:
$$(gag^{-1})^n = \underbrace{gag^{-1} \cdot gag^{-1} \cdot \dots \cdot gag^{-1}}_{n \text{ Faktoren}} = g \cdot \underbrace{a \cdot a \cdot \dots \cdot a}_{n \text{ Faktoren}} \cdot g^{-1} = ga^n g^{-1},$$
wie behauptet. ■

2. Die Ordnung von Gruppenelementen

DEFINITION (Ordnung). *Sei $(G, *)$ eine Gruppe mit neutralem Element e und $g \in G$. Wir betrachten die Menge*
$$\{n \in \mathbb{N} : g^n = e\}.$$
- *Ist $\{n \in \mathbb{N} : g^n = e\} = \emptyset$, so sagen wir, g hat* **unendliche Ordnung** *und schreiben* $\operatorname{ord}(g) = \infty$.
- *Ist $\{n \in \mathbb{N} : g^n = e\} \neq \emptyset$, so definieren wir die* **Ordnung von** *g als*
$$\operatorname{ord}(g) = \min\{n \in \mathbb{N} : g^n = e\}.$$

Schreibt man die Gruppe additiv, so muss man $g^n = e$ durch $n \cdot g = 0$ ersetzen.

Beispiele:

(1) In der multiplikativen Gruppe $(\mathbb{R}^*, \cdot)$ gilt
$$\operatorname{ord}(1) = 1, \quad \operatorname{ord}(-1) = 2, \quad \operatorname{ord}(r) = \infty \text{ für alle } r \in \mathbb{R}^* \setminus \{1, -1\}.$$
(Ist $r \in \mathbb{R}^* \setminus \{\pm 1\}$, so gilt $|r| < 1$ oder $|r| > 1$, also $|r^n| < 1$ oder $|r^n| > 1$ für alle $n \in \mathbb{N}$, woraus sofort $\operatorname{ord}(r) = \infty$ folgt.)
(2) In der multiplikationen Gruppe $(\mathbb{C}^*, \cdot)$ gilt
$$\operatorname{ord}(1) = 1, \quad \operatorname{ord}(-1) = 2, \quad \operatorname{ord}(i) = 4.$$
(Wir werden die Elemente endlicher Ordnung später genau angeben.)
(3) In $(\mathrm{GL}_3(\mathbb{Q}), \cdot)$ gilt für
$$A = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$$
$$A^2 = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}, \quad A^3 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$
Also gilt $\operatorname{ord}(A) = 3$. Aus $A^3 = \mathbf{1}_3$ sieht man auch $A^{-1} = A^2$.

(4) In $(\mathbb{Z}_8^*, \cdot)$ gilt
$$1 = 1, \quad 3^2 = 1, \quad 5^2 = 1, \quad 7^2 = 1,$$
was sofort
$$\operatorname{ord}(1) = 1, \quad \operatorname{ord}(3) = \operatorname{ord}(5) = \operatorname{ord}(7) = 2$$
liefert.

(5) Für $n \geq 3$ gilt in $(\mathbb{Z}_n^*, \cdot)$
$$\operatorname{ord}(1) = 1, \quad \operatorname{ord}(n-1) = 2.$$
Die letzte Beziehung gilt, da in $\mathbb{Z}_n$ die Gleichung $(n-1) \cdot (n-1) = 1$ und die Ungleichung $n - 1 \neq 1$ gilt.

(6) In jeder (multiplikativ geschriebenen) Gruppe G gilt für Gruppenelemente g
$$\operatorname{ord}(g^{-1}) = \operatorname{ord}(g),$$
weil $g^n = e$ äquivalent mit $(g^{-1})^n = g^{-n} = (g^n)^{-1} = e$ ist.

SATZ. *Sei $(G, *)$ eine Gruppe mit neutralem Element e und $g \in G$.*

(1) *Ist die Ordnung von g unendlich, so sind die Elemente g^n für $n \in \mathbb{Z}$ paarweise verschieden.*

(2) *Hat g endliche Ordnung, so gilt:*

(a) *Für $n \in \mathbb{N}$ gilt:*
$$g^n = e \quad \Longleftrightarrow \quad \operatorname{ord}(g) \mid n.$$

(b) *Es gilt*
$$\{n \in \mathbb{N} : g^n = e\} = \mathbb{N} \cdot \operatorname{ord}(g) = \{k \cdot \operatorname{ord}(g) : k \in \mathbb{N}\}.$$

(c) *Für $m, n \in \mathbb{Z}$ gilt:*
$$g^m = g^n \quad \Longleftrightarrow \quad \operatorname{ord}(g) \mid m - n \quad \Longleftrightarrow \quad m \bmod \operatorname{ord}(g) = n \bmod \operatorname{ord}(g).$$

(d) *Die Elemente $g^0, g^1, g^2, \ldots, g^{\operatorname{ord}(a)-1}$ sind paarweise verschieden und*
$$\{g^n : n \in \mathbb{Z}\} = \{g^n : 0 \leq n \leq \operatorname{ord}(g) - 1\}$$
enthält genau $\operatorname{ord}(g)$ *Elemente.*

Beweis:

(1) g habe unendliche Ordnung. Angenommen, es gibt $m, n \in \mathbb{Z}$ mit $g^m = g^n$. O.E. können wir $m > n$ annehmen. Dann folgt
$$g^{m-n} = g^m * g^{-n} = g^m * (g^n)^{-1} = g^m * (g^m)^{-1} = e.$$
Wegen $m - n \in \mathbb{N}$ ist dies aber ein Widerspruch zur Voraussetzung, dass $\{n \in \mathbb{N} : g^n = e\} = \emptyset$ gelten soll. Also ist die Annahme falsch, die Behauptung somit richtig.

(2) (a) $\Longrightarrow$ Sei $n \in \mathbb{N}$ mit $g^n = e$. Wir teilen n durch $\operatorname{ord}(g)$ und erhalten eine Darstellung
$$n = k \cdot \operatorname{ord}(g) + r \text{ mit } k, r \in \mathbb{N}_0 \text{ und } 0 \leq r < \operatorname{ord}(g).$$
Dann gilt
$$g^r = g^{n - k \cdot \operatorname{ord}(g)} = g^n \cdot (g^{\operatorname{ord}(a)})^{-k} = e \cdot e^{-k} = e.$$
Nach Definition von $\operatorname{ord}(g)$ bleibt wegen $0 \leq r < \operatorname{ord}(g)$ nur die Möglichkeit $r = 0$, was zu $n = k \cdot \operatorname{ord}(g)$ führt, d.h. $\operatorname{ord}(g) \mid n$.
$\Longleftarrow$ Es gelte $\operatorname{ord}(g) \mid n$. Dann existiert ein $k \in \mathbb{N}$ mit $n = k \cdot \operatorname{ord}(g)$ und es folgt
$$g^n = g^{k \cdot \operatorname{ord}(g)} = \left(g^{\operatorname{ord}(g)}\right)^k = e^k = e,$$
wie behauptet.

(b) Dies ist einfach die mengentheoretische Formulierung von (a).

(c) Seien $m, n \in \mathbb{Z}$ und o.E. $m > n$. Dann gilt

$$g^m = g^n \quad \Longleftrightarrow \quad g^{m-n} = e \quad \Longleftrightarrow \quad \operatorname{ord}(g) \mid m - n.$$

Die letzte Äquivalenz gilt allgemein: Schreibt man $m = k \cdot \operatorname{ord}(g) + r$, $n = l \cdot \operatorname{ord}(g) + s$ mit den Divisionsresten $r, s \in \{0, 1, \ldots, \operatorname{ord}(g) - 1\}$, so gilt

$$\begin{aligned} \operatorname{ord}(g) \mid m - n \quad &\Longleftrightarrow \quad \operatorname{ord}(g) \mid (k-l)\operatorname{ord}(g) + (r - s) \quad \Longleftrightarrow \\ &\Longleftrightarrow \quad \operatorname{ord}(g) \mid r - s \quad \Longleftrightarrow \; r = s, \end{aligned}$$

wobei die letzte Gleichung aus $|r - s| < \operatorname{ord}(g)$ folgt.

(d) Dies folgt sofort aus (c). ■

Bemerkung: Sind $a, b \in \mathbb{N}$ und gilt für alle $n \in \mathbb{N}$ die Äquivalenz

$$a \mid n \quad \Longleftrightarrow \quad b \mid n,$$

so gilt offensichtlich

$$a = b.$$

Dieses Kriterium werden wir häufiger in Zusammenhang mit Teil (2a) des vorangegangenen Satzes benutzen.

Wir leiten eine Formel für die Ordnungen der Potenzen eines Elements her.

Satz. *Sei G eine multiplikativ geschriebene Gruppe mit neutralem Element e und $g \in G$ ein Element endlicher Ordnung. Dann gilt für alle $k \in \mathbb{Z}$*

$$\operatorname{ord}(g^k) = \frac{\operatorname{ord}(g)}{\operatorname{ggT}(\operatorname{ord}(g), k)}.$$

Beweis: Wegen $\operatorname{ord}(g^k) = \operatorname{ord}(g^{-k})$ können wir $k \geq 0$ annehmen. Für $n \in \mathbb{N}$ erhalten wir folgende Äquivalenzen

$$\begin{aligned} \operatorname{ord}(g^k) \mid n \quad &\Longleftrightarrow \quad (g^k)^n = e \quad \Longleftrightarrow \quad g^{kn} = e \quad \Longleftrightarrow \quad \operatorname{ord}(g) \mid kn \quad \Longleftrightarrow \\ &\Longleftrightarrow \quad \frac{\operatorname{ord}(g)}{\operatorname{ggT}(\operatorname{ord}(g), k)} \mid \frac{k}{\operatorname{ggT}(\operatorname{ord}(g), k)} \cdot n \quad \Longleftrightarrow \quad \frac{\operatorname{ord}(g)}{\operatorname{ggT}(\operatorname{ord}(g), k)} \mid n. \end{aligned}$$

(Dabei haben ausgenutzt, dass $\operatorname{ggT}(\frac{\operatorname{ord}(g)}{\operatorname{ggT}(\operatorname{ord}(g),k)}, \frac{k}{\operatorname{ggT}(\operatorname{ord}(g),k)}) = 1$ gilt.) Aus der Äquivalenz folgt nun sofort

$$\operatorname{ord}(g^k) = \frac{\operatorname{ord}(g)}{\operatorname{ggT}(\operatorname{ord}(g), k)}.$$

Dies sollte gezeigt werden. ■

Bemerkung: Ist g ein Element unendlicher Ordnung, so erhält man einfach

$$\operatorname{ord}(g) = \infty \quad \Longrightarrow \quad \operatorname{ord}(g^k) = \begin{cases} \infty & \text{für } k \neq 0, \\ 1 & \text{für } k = 0. \end{cases}$$

Wir formulieren den letzten Satz nochmals für additiv geschriebene Gruppen:

Satz. *Sei A eine additiv geschriebene Gruppe mit neutralem Element 0 und $a \in A$ ein Element endlicher Ordnung. Dann gilt für alle $k \in \mathbb{Z}$*

$$\operatorname{ord}(k \cdot a) = \frac{\operatorname{ord}(a)}{\operatorname{ggT}(\operatorname{ord}(a), k)}.$$

Folgerung. *In der abelschen Gruppe $(\mathbb{Z}_n, +)$ gilt für $k \in \mathbb{Z}_n$*

$$\operatorname{ord}(k) = \frac{n}{\operatorname{ggT}(n, k)}.$$

Beweis: Für $1 \in \mathbb{Z}_n$ gilt:

$$1 \neq 0, \quad 2 \cdot 1 = 1 + 1 = 2 \neq 0, \quad 3 \cdot 1 = 1 + 1 + 1 = 3 \neq 0, \quad (n-1) \cdot 1 = \underbrace{1 + \cdots + 1}_{n-1 \text{ Summanden}} = n - 1 \neq 0$$

und

$$n \cdot 1 = \underbrace{1 + \cdots + 1}_{n \text{ Summanden}} = n = 0,$$

also

$$\operatorname{ord}(1) = n.$$

Die Behauptung folgt dann aus der Folgerung. ■

Beweis: Für $n \in \mathbb{N}$ gilt:

$$k \cdot a = 0 \iff (ka) \bmod n = 0 \iff n \mid ka \iff \frac{n}{\operatorname{ggT}(n,a)} \mid k \cdot \frac{a}{\operatorname{ggT}(n,a)} \iff$$
$$\iff \frac{n}{\operatorname{ggT}(n,a)} \mid k.$$

Daraus folgt

$$\operatorname{ord}(a) = \frac{n}{\operatorname{ggT}(n,a)},$$

wie behauptet. ■

Beispiele:

(1) In $(\mathbb{Z}_4, +)$ gilt

$$\operatorname{ord}(0) = \frac{4}{\operatorname{ggT}(4,0)} = 1, \quad \operatorname{ord}(1) = \frac{4}{\operatorname{ggT}(4,1)} = 4,$$
$$\operatorname{ord}(2) = \frac{4}{\operatorname{ggT}(4,2)} = 2, \quad \operatorname{ord}(3) = \frac{4}{\operatorname{ggT}(4,3)} = 4.$$

(2) In $(\mathbb{Z}_{100}, +)$ erhalten wir mit obiger Formel:

$\operatorname{ord}(a)$	$a \in \mathbb{Z}_{100}$
1	0
2	50
4	25, 75
5	20,40,60,80
10	10,30,70,90
20	5,15,35,45,55,65,85,95
25	4,8,12,16,24,28,32,36,44,48,52,56,64,68,72,76,84,88,92,96
50	2,6,14,18,22,26,34,38,42,46,54,58,62,66,74,78,82,86,94,98
100	1,3,7,9,11,13,17,19,21,23,27,29,31,33,37,39,41,43,47,49, 51,53,57,59,61,63,67,69,71,73,77,79,81,83,87,89,91,93,97,99

Bemerkung: Mit dem vorangegangenen Satz kann man die Ordnung von Elementen der Gruppen $(\mathbb{Z}_n, +)$ auch für große n schnell bestimmen. Bei den multiplikativen Gruppen $(\mathbb{Z}_n^*, \cdot)$ sieht die Situation ganz anders aus; hier ist kein allgemeines Verfahren bekannt, um Elementordnungen auch für (allgemeine) große n schnell zu bestimmen.

Das folgende Lemma ist manchmal nützlich:

LEMMA. *Sei G eine multiplikativ geschriebene Gruppe und $g \in G$ ein Element endlicher Ordnung. Ist k ein Teiler der Elementordnung $\operatorname{ord}(g)$, d.h. $k \mid \operatorname{ord}(g)$, so hat $g^{\frac{\operatorname{ord}(g)}{k}}$ Ordnung k. In Zeichen:*

$$k \mid \operatorname{ord}(g) \quad \Longrightarrow \quad \operatorname{ord}(g^{\frac{\operatorname{ord}(g)}{k}}) = k.$$

Beweis: Wir nützen die vorangegangene Formel, dass natürlich mit k auch $\frac{\operatorname{ord}(g)}{k}$ ein Teiler von $\operatorname{ord}(g)$ ist:

$$\operatorname{ord}(g^{\frac{\operatorname{ord}(g)}{k}}) = \frac{\operatorname{ord}(g)}{\operatorname{ggT}(\operatorname{ord}(g), \frac{\operatorname{ord}(g)}{k})} = \frac{\operatorname{ord}(g)}{\frac{\operatorname{ord}(g)}{k}} = k.$$

Dies war zu zeigen. ■

LEMMA. *Sei G eine (multiplikativ geschriebene) Gruppe. Konjugierte Elemente haben die gleiche Ordnung, d.h. für $a, g \in G$ gilt*

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

Beweis: Sei e das neutrale Element von G. Für $n \in \mathbb{N}$ gilt:

$$a^n = e \quad \Longleftrightarrow \quad g \cdot a^n \cdot g^{-1} = g \cdot e \cdot g^{-1} = e \quad \Longleftrightarrow \quad (gag^{-1})^n = e,$$

woraus sofort

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

folgt. ■

3. Direkte Produkte

Eine einfache Möglichkeit, aus gegebenen Gruppen neue zu erhalten, besteht in der Produktbildung:

Sind $G_1, \ldots, G_n$ (multiplikativ geschriebene) Gruppen, so definiert man das **direkte Produkt** der Gruppen $G_1, \ldots, G_n$ auf der Menge

$$G_1 \times \cdots \times G_n = \{(a_1, \ldots, a_n) : a_i \in G_i\}$$

durch die Verknüpfung

$$(a_1, \ldots, a_n) \cdot (b_1, \ldots, b_n) = (a_1 b_1, \ldots, a_n b_n).$$

Ist $e_i \in G_i$ das neutrale Element in G_i, so ist $(e_1, \ldots, e_n)$ das neutrale Element des direkten Produkts. Für die Inversenbildung gilt

$$(a_1, \ldots, a_n)^{-1} = (a_1^{-1}, \ldots, a_n^{-1}).$$

Für die Ordnung gilt

$$\operatorname{ord}((a_1, \ldots, a_n)) = \operatorname{kgV}(\operatorname{ord}(a_1), \ldots, \operatorname{ord}(a_n)).$$

Beispiel: Ist K ein Körper (wie $\mathbb{Q}$, $\mathbb{R}$ oder $\mathbb{C}$), so wird K mit der Addition zu einer abelschen Gruppe. Dann ist auch

$$K^n = \underbrace{K \times \cdots \times K}_{n \text{ Faktoren}} = \{(a_1, \ldots, a_n) : a_i \in K\}$$

mit der komponentenweisen Addition eine abelsche Gruppe. Üblicherweise schreibt man K^n als Zeilen- oder Spaltenvektoren.

Beispiel:

$$\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0,0), (0,1), (1,0), (1,1)\}$$

mit der komponentenweisen Addition unter Beachtung von $1+1 = 0$ ist eine abelsche Gruppe der Ordnung 4. Man nennt die Gruppe auch die **Kleinsche Vierergruppe**.

Man kann noch allgemeiner Produkte von Gruppen bilden: Ist I eine Indexmenge und $(G_i)_{i \in I}$ eine Familie von (multiplikativ geschriebenen) Gruppen, so wird das mengentheoretische Produkt

$$\prod_{i \in I} G_i = \{(a_i) : a_i \in G_i \text{ für alle } i \in I\}$$

zu einer Gruppe, dem **direkten Produkt** der Familie $(G_i)_{i \in I}$, wenn man die Verknüpfung durch

$$(a_i)_{i \in I} \cdot (b_i)_{i \in I} = (a_i b_i)_{i \in I}$$

definiert. Ist $e_i \in G_i$ das neutrale Element in G_i, so ist $(e_i)_{i \in I}$ das neutrale Element des Produkts. Für die Inversenbildung gilt

$$((a_i)_{i \in I})^{-1} = (a_i^{-1})_{i \in I}.$$

4. Die symmetrische Gruppe S_n

Für $n \in \mathbb{N}$ sei S_n die Gruppe der bijektiven Abbildungen der Menge $\{1, 2, 3, \ldots, n\}$ in sich, also

$$S_n = S(\{1, 2, 3, \ldots, n\}) = \{\sigma : \{1, 2, 3, \ldots, n\} \to \{1, 2, 3, \ldots, n\} : \sigma \text{ ist bijektiv}\}$$

mit der Komposition $\circ$ als Verknüpfung. (Da man die Elemente aus S_n als Funktionen betrachtet, „liest“ man Produkte $fg = f \circ g$ von rechts nach links: $(fg)(n) = f(g(n))$.) Statt bijektive Abbildung sagt man hier auch Permutation. Die Elemente von S_n kann man durch eine Wertetabelle in folgender Weise beschreiben:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \ldots & \sigma(n) \end{pmatrix}.$$

(Die untere Zeile der Matrix $\begin{pmatrix} \sigma(1) & \sigma(2) & \sigma(3) & \ldots & \sigma(n) \end{pmatrix}$ ist einfach eine Permutation der Zahlen von 1 bis n.) Da es $n!$ Permutationen von n Elementen gibt, ist die Gruppenordnung von S_n einfach $n!$:

n	1	2	3	4	5	6	7	8	9	10
$\lvert S_n \rvert$	1	2	6	24	120	720	5040	40320	362880	3628800

Beispiel: Die symmetrische Gruppe S_3 lässt sich schreiben als

$$S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\}.$$

Aus

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \quad \text{und} \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

sieht man die Nichtkommutativität von S_3. (Verallgemeinert man das Beispiel, so sieht man sofort, dass S_n für alle $n \geq 3$ nichtabelsch ist.)

Graphische Darstellung: Gegeben sei ein $\sigma \in S_n$ in der Form

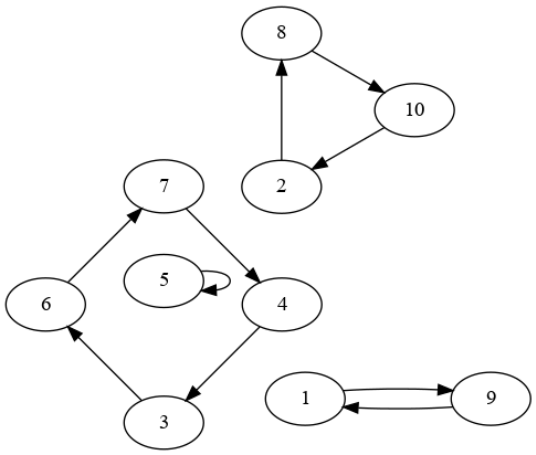
$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \ldots & \sigma(n) \end{pmatrix}.$$

Wir können die Abbildung σ veranschaulichen, indem wir n Punkte, nummeriert mit 1 bis n, zeichnen, und einen Pfeil von i nach $\sigma(i)$ für alle $i = 1, \ldots, n$. Wir beginnen mit Beispielen:

Beispiele:

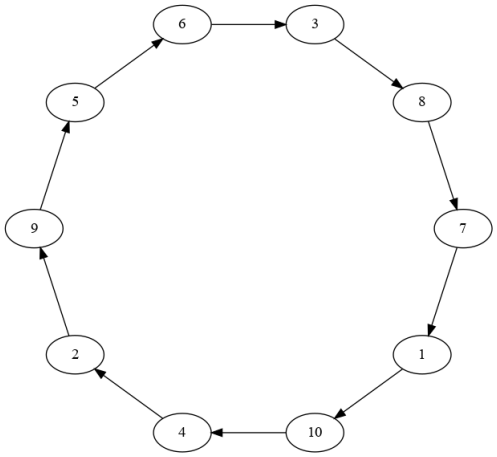
(1)

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



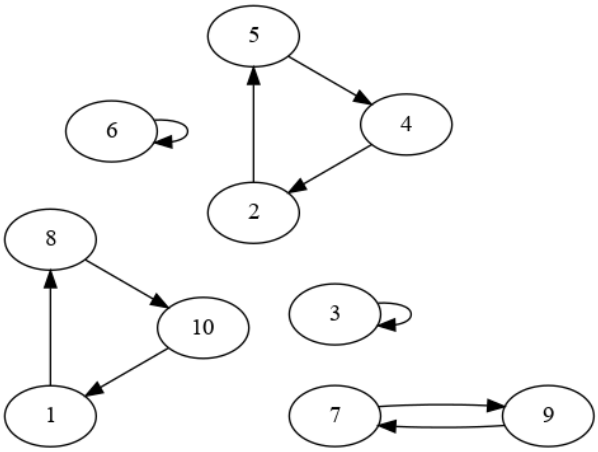
(2)

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



(3)

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



Man sieht hier die Struktur der Permutation wesentlich deutlicher. Der Graph zerlegt sich in „Kreise“.

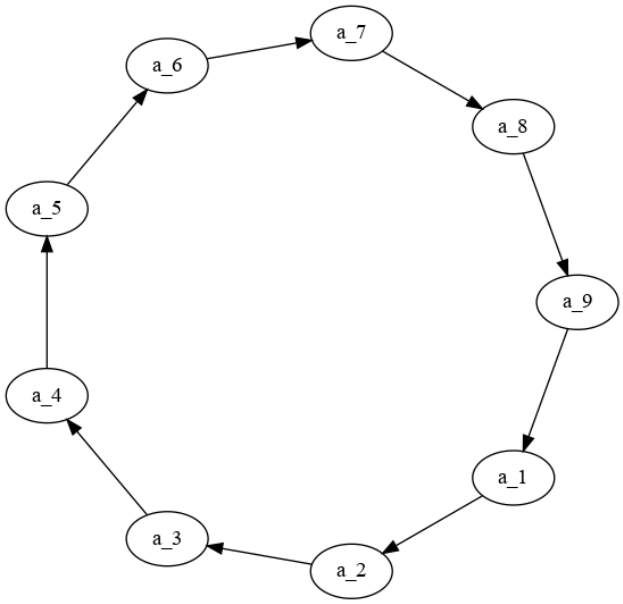
Zykel: Sind $a_1, \ldots, a_\ell$ paarweise verschiedene Zahlen aus $\{1, \ldots, n\}$, so definiert man den **Zykel** $(a_1, a_2, \ldots, a_\ell) \in S_n$ (oder auch $(a_1 a_2 \ldots a_\ell)$) durch

$$(a_1, a_2, \ldots, a_\ell)(x) = \begin{cases} a_{i+1} & \text{für } x = a_i \text{ und } 1 \leq i \leq \ell - 1, \\ a_1 & \text{für } x = a_\ell, \\ x & \text{für } x \in \{1, \ldots, n\} \setminus \{a_1, \ldots, a_\ell\}. \end{cases}$$

Nochmals in Form einer Wertetabelle:

x	a_1	a_2	a_3	$\ldots$	$a_{\ell-1}$	a_ℓ	y für $y \in \{1, \ldots, n\} \setminus \{a_1, \ldots, a_\ell\}$
$(a_1, a_2, \ldots, a_\ell)(x)$	a_2	a_3	a_4	$\ldots$	a_ℓ	a_1	y

Graphisch, wobei die nicht zum Zykel gehörigen Punkte festbleiben und nicht eingezeichnet wurden:



Ein Zykel der Länge 2, also $(a_1 a_2)$, wird **Transposition** genannt.

Das folgende Lemma gibt einige einfache, aber wichtige Eigenschaften von Zykeln wieder:

LEMMA. *Seien $a_1, \ldots, a_\ell$ paarweise verschiedene Zahlen aus $\{1, \ldots, n\}$ und ebenso $b_1, \ldots, b_{\ell'}$ paarweise verschiedene Zahlen aus $\{1, \ldots, n\}$.*

(1) *Es gilt*

$$(a_1, a_2, \ldots, a_{\ell-1}, a_\ell) = (a_2, a_3, \ldots, a_\ell, a_1) = (a_3, a_4, \ldots, a_1, a_2) = \cdots = (a_\ell, a_1, \ldots, a_{\ell-2}, a_{\ell-1}),$$

d.h. die zu einem Zykel gehörige Permutation bleibt unverändert, wenn man die Einträge zyklisch verschiebt.

(2) *Ist*

$$(a_1, a_2, \ldots, a_{\ell-1}, a_\ell) = (b_1, b_2, \ldots, b_{\ell'-1}, b_{\ell'}),$$

so gilt $\ell' = \ell$ und $(b_1, b_2, \ldots, b_{\ell-1}, b_\ell)$ entsteht durch eine zyklische Verschiebung aus $(a_1, a_2, \ldots, a_{\ell-1}, a_\ell)$, d.h. es gibt einen Index i mit

$$b_1 = a_i, \quad b_2 = a_{i+1}, \ldots, b_{1+\ell-i} = a_\ell, \quad b_{2+\ell-i} = a_1, \quad \ldots$$

(3) *Gilt $\{a_1, \ldots, a_\ell\} \cap \{b_1, \ldots, b_{\ell'}\} = \emptyset$, d.h. sind die Zykel $(a_1, \ldots, a_\ell)$ und $(b_1, \ldots, b_{\ell'})$ elementfremd, so ist*

$$(a_1, \ldots, a_\ell)(b_1, \ldots, b_{\ell'}) = (b_1, \ldots, b_{\ell'})(a_1, \ldots, a_\ell),$$

d.h. die Zykel sind vertauschbar, sie kommutieren.

(4) *Ein Zykel der Länge ℓ hat Ordnung ℓ, d.h.*

$$\operatorname{ord}((a_1, a_2, \ldots, a_\ell)) = \ell.$$

(5) *Für den inversen Zykel gilt:*

$$(a_1, a_2, \ldots, a_{\ell-1}, a_\ell)^{-1} = (a_\ell, a_{\ell-1}, \ldots, a_2, a_1).$$

(6) *Für $\sigma \in S_n$ gilt*

$$\sigma(a_1, a_2, \ldots, a_{\ell-1}, a_\ell)\sigma^{-1} = (\sigma(a_1), \sigma(a_2), \ldots, \sigma(a_{\ell-1}), \sigma(a_\ell)).$$

Beweis:

(1) Die Eigenschaft $(a_1, a_2, \ldots, a_{\ell-1}, a_\ell) = (a_2, a_3, \ldots, a_\ell, a_1)$ sieht man sofort, der Rest folgt daraus.

(2) Nach Definition folgt für die Fixpunktmengen der Zykel

$$\{x \in \{1,\dots,n\} : (a_1,a_2,\dots,a_{\ell-1},a_\ell)(x) = x\} = \{1,\dots,n\} \setminus \{a_1,\dots,a_\ell\}$$

und

$$\{x \in \{1,\dots,n\} : (b_1,b_2,\dots,b_{\ell'-1},b_{\ell'})(x) = x\} = \{1,\dots,n\} \setminus \{b_1,\dots,b_{\ell'}\},$$

sodass die Voraussetzung sofort $\{a_1,\dots,a_\ell\} = \{b_1,\dots,b_{\ell'}\}$ liefert. Insbesondere gilt $\ell = \ell'$. Mit (1) können wir nun den Zykel $(b_1,\dots,b_\ell)$ so verschieben, dass $b_1 = a_1$ gilt. Dann sieht man aber induktiv $b_2 = a_2$, $b_3 = a_3$, …, $b_\ell = a_\ell$, und es folgt die Behauptung.

(3) Dies folgt sofort aus der Definition der Zykel.

(4) Für $\sigma = (a_1,a_2,\dots,a_\ell)$ gilt

$$\sigma(a_1) = a_2, \quad \sigma^2(a_1) = a_3, \quad \sigma^3(a_1) = a_4, \quad \dots \sigma^{\ell-1}(a_1) = a_\ell, \quad \sigma^\ell(a_1) = a_1.$$

Da die gleiche Überlegung für jedes andere Element des Zykels gilt, ist

$$\sigma^\ell(a_i) = a_i \text{ für } i = 1,\dots,\ell,$$

woraus dann sofort $\operatorname{ord}((a_1,a_2,\dots,a_\ell)) = \ell$ folgt.

(5) Die Formel

$$(a_1,a_2,\dots,a_{\ell-1},a_\ell)^{-1} = (a_\ell,a_{\ell-1},\dots,a_2,a_1)$$

sieht man sofort, wenn man sich die graphische Zykeldarstellung anschaut.

(6) Ist $x \in \{1,\dots,n\} \setminus \{a_1,\dots,a_\ell\}$, so gilt

$$\Big(\sigma(a_1,\dots,a_\ell)\sigma^{-1}\Big)\sigma(x) = \sigma(a_1,\dots,a_\ell)(x) = \sigma(x) = (\sigma(a_1),\dots,\sigma(a_\ell))(\sigma(x)).$$

Für $1 \le i \le \ell - 1$ gilt

$$\Big(\sigma(a_1,\dots,a_\ell)\sigma^{-1}\Big)\sigma(a_i) = \sigma(a_1,\dots,a_\ell)(a_i) = \sigma(a_{i+1}) = (\sigma(a_1),\dots,\sigma(a_\ell))(\sigma(a_i)).$$

$$\Big(\sigma(a_1,\dots,a_\ell)\sigma^{-1}\Big)\sigma(a_\ell) = \sigma(a_1,\dots,a_\ell)(a_\ell) = \sigma(a_1) = (\sigma(a_1),\dots,\sigma(a_\ell))(\sigma(a_\ell)).$$

Die die Funktionswerte der Abbildungen auf der linken und rechten Seite für alle $\sigma(x)$ mit $x \in M$ übereinstimmen, sind die Abbildungen gleich. ■

SATZ. *Jedes $\sigma \in S_n$ ist Produkt elementfremder Zykel:*

$$\sigma = (a_{1,1},\dots,a_{1,\ell_1})(a_{2,1},\dots,a_{2,\ell_2})\dots(a_{r,1},\dots,a_{r,\ell_r})$$

(mit $\ell_1 + \dots + \ell_r = n$).

Beweis:

(1) Wir definieren rekursiv Mengen

$$M = M_1 \supsetneq M_2 \supsetneq \dots \supsetneq M_r \supsetneq M_{r+1} = \emptyset,$$

wobei $\sigma(M_i) \subseteq M_i$ gelten wird und wir mit $i = 1$ und $M_1 = M$ beginnen.

(2) Sei nun der aktuelle Index i. Die Menge M_i ist bekannt und hat die Eigenschaft $\sigma(M_i) \subseteq M_i$. Wir wählen ein $a_{i,1} \in M_i$ und definieren rekursiv

$$a_{i,j} = \sigma(a_{i,j-1}) \text{ für } j \ge 2.$$

Dann gilt

$$a_{i,j} = \sigma^{j-1}(a_{i,1}) \text{ für } j \ge 1.$$

Da M_i endlich ist, gibt es einen Index ℓ_i mit

$$\#\{a_{i,1},\dots,a_{i,\ell_i}\} = \ell_i \quad \text{und} \quad a_{i,\ell_i+1} \in \{a_{i,1},\dots,a_{i,\ell_i}\}.$$

- **Fall $a_{i,\ell_i+1} = a_{i,1}$:** Wegen $a_{i,1} = a_{i,\ell_i+1} = \sigma(a_{i,\ell_i})$ wird σ auf $\{a_{i,1},\dots,a_{i,\ell_i}\}$ durch den Zykel

$$(a_{i,1},\dots,a_{i,\ell_i})$$

beschrieben.

- **Fall $a_{i,\ell_i+1} = a_{i,j+1}$ mit $1 \le j \le \ell_i - 1$:** Dann gilt
$$\sigma(a_{i,\ell_i}) = a_{i,\ell_i+1} = a_{i,j+1} = \sigma(a_{i,j}),$$
und damit
$$a_{i,\ell_i} = a_{i,j} \text{ mit } 1 \le j \le \ell_i - 1.$$
Dies widerspricht aber der Definition von ℓ_i, sodass dieser Fall nicht eintreten kann.

Wir definieren nun
$$M_{i+1} = M_i \setminus \{a_{i,1}, \dots, a_{i,\ell_i}\}.$$
Da σ bijektiv ist, folgt $\sigma(M_{i+1}) \subseteq M_i$. Ist $M_{i+1} = \emptyset$, so hören wir auf, andernfalls ersetzen wir i durch $i+1$ und gehen zurück zu (2).

(3) Wegen $M_i \supsetneq M_{i+1}$ hört das Verfahren nach endlich vielen Schritten auf. Es folgt die Behauptung. ■

Beispiele: Der demonstrieren den vorangegangenen konstruktiven Beweis durch ein paar Beispiele.

(1)
$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 1 & 8 & 9 & 3 & 2 & 6 & 7 & 5 & 10 & 4 \end{pmatrix}$$
ergibt die Zykelzerlegung
$$\sigma = (1)(2,8,5)(3,9,10,4)(6)(7).$$

(2)
$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 8 & 4 & 3 & 1 & 5 & 9 & 7 & 6 & 10 & 2 \end{pmatrix} = (1,8,6,9,10,2,4)(3)(5)(7).$$

(3)
$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 5 & 8 & 7 & 2 & 3 & 9 & 1 & 6 & 4 & 10 \end{pmatrix} = (1,5,3,7)(2,8,6,9,4)(10).$$

Bemerkung: Die Fixpunkte einer Permutation $\sigma \in S_n$ entsprechen gerade den einelementigen Zykel (a) in der Zykelzerlegung von σ. Man kann man sie beim Schreiben natürlich weglassen, solange es mindestens noch einen weiteren Zykel gibt.

Satz. *Ist $\sigma \in S_n$ das Produkt elementfremder Zykel der Längen $\ell_1, \ell_2, \dots, \ell_r$, d.h.*
$$\sigma = (a_{1,1}, a_{1,2}, \dots, a_{1,\ell_1})(a_{2,1}, a_{2,2}, \dots, a_{2,\ell_2}) \dots (a_{r,1}, a_{r,2}, \dots, a_{r,\ell_r}),$$
so gilt
$$\sigma^{-1} = (a_{1,\ell_1}, a_{1,\ell_1-1}, \dots, a_{1,1})(a_{2,\ell_2}, a_{2,\ell_2-1}, \dots, a_{2,1}) \dots (a_{r,\ell_r}, a_{r,\ell_r-1}, \dots, a_{r,1})$$
und
$$\operatorname{ord}(\sigma) = \operatorname{kgV}(\ell_1, \ell_2, \dots, \ell_r).$$

Beweis: Da elementfremde Zykel kommutieren, ergibt sich die Formel für σ^{-1} sofort aus der entsprechenden Formel für Zykel.
Da σ die Mengen $\{a_{i,1}, \dots, a_{i,\ell_i}\}$ in sich abbildet, d.h.
$$\sigma(\{a_{i,1}, \dots, a_{i,\ell_i}\}) = \{a_{i,1}, \dots, a_{i,\ell_i}\},$$
gilt für $k \in \mathbb{N}$
$$\begin{aligned} \sigma^k = \mathrm{id} &\iff (a_{i,1}, \dots, a_{i,\ell_i})^k = \mathrm{id}_{\{a_{i,1},\dots,a_{i,\ell_i}\}} \text{ für } i = 1, \dots, r &\iff \\ &\iff \operatorname{ord}((a_{i,1}, \dots, a_{i,\ell_i})) \mid k \text{ für } i = 1, \dots, r &\iff \\ &\iff \ell_i \mid k \text{ für } i = 1, \dots, k &\iff \\ &\iff \operatorname{kgV}(\ell_1, \dots, \ell_r) \mid k, \end{aligned}$$
was sofort
$$\operatorname{ord}(\sigma) = \operatorname{kgV}(\ell_1, \dots, \ell_r)$$
liefert. ■

Bemerkung: Mit einem vorangegangenen Lemma sieht man, dass die Zykeldarstellung einer Permutation $\sigma \in S_n$ bis auf Vertauschungen der Zykel und zyklische Permutation der einzelnen Zykel eindeutig ist. Schreibt man

$$\sigma = (a_{1,1}, \ldots, a_{1,\ell_1})(a_{2,1}, \ldots, a_{2,\ell_2}) \ldots (a_{r,1}, \ldots, a_{r,\ell_r}),$$

so kann man

$$\ell_1 \geq \ell_2 \geq \cdots \geq \ell_r$$

annehmen. Wir definieren den **Typ** der Permutation als

$$\mathrm{Typ}(\sigma) = (\ell_1, \ell_2, \ldots, \ell_r).$$

Dies ist eine sogenannte **Partition der Zahl** n wegen $\ell_1 + \cdots + \ell_r = n$. (Auch wenn man die Fixpunkte bei der Zykelzerlegung nicht anschreiben muss, darf man sie bei der Angabe des Typs nicht vergessen.)

Beispiele:

Permutation	Typ
$(1)(2,8,5)(3,9,10,4)(6)(7)$	$(4,3,1,1,1)$
$(1,8,6,9,10,2,4)(3)(5)(7)$	$(7,1,1,1)$
$(1,5,3,7)(2,8,6,9,4)(10)$	$(5,4,1)$

Satz. *In S_n gilt für zwei Elemente σ, τ:*

$$\sigma \text{ und } \tau \text{ sind konjugiert} \quad \Longleftrightarrow \quad \mathrm{Typ}(\sigma) = \mathrm{Typ}(\tau).$$

Genauer: Gilt $\mathrm{Typ}(\sigma) = \mathrm{Typ}(\tau)$*, so kann man schreiben*

$$\begin{aligned} \sigma &= (a_{1,1}, \ldots, a_{1,\ell_1})(a_{2,1}, \ldots, a_{2,\ell_2}) \ldots (a_{r,1}, \ldots, a_{r,\ell_r}), \\ \tau &= (b_{1,1}, \ldots, b_{1,\ell_1})(b_{2,1}, \ldots, b_{2,\ell_2}) \ldots (b_{r,1}, \ldots, b_{r,\ell_r}). \end{aligned}$$

Definiert man nun $\lambda \in S_n$ durch

$$\lambda(a_{i,j}) = b_{i,j} \text{ für } i = 1, \ldots, r \text{ und } j = 1, \ldots, \ell_r,$$

so gilt

$$\tau = \lambda \sigma \lambda^{-1}.$$

Beweis: Hat σ die Zykelzerlegung

$$\sigma = (a_{i,1} \ldots, a_{1,\ell_1})(a_{2,1}, \ldots, a_{2,\ell_2}) \ldots (a_{r,1}, \ldots, a_{r,\ell_r})$$

mit $\ell_1 + \cdots + \ell_r = n$, so folgt aus der entsprechenden Formel für die Zykel für $\lambda \in S_n$

$$\lambda \sigma \lambda^{-1} = (\lambda(a_{1,1}), \ldots, \lambda(a_{1,\ell_1}))(\lambda(a_{2,1}), \ldots, \lambda(a_{2,\ell_2})) \ldots (\lambda(a_{r,1}), \ldots, \lambda(a_{r,\ell_r})).$$

Aus dieser Darstellung kann man alle Behauptungen ablesen. ■

Beispiel: Die Permutationen

$$\sigma = (1,4,5,3)(2,6) \quad \text{und } \tau = (1,8)(4,6,5,7)$$

haben den gleichen Typ in S_8. Wir schreiben

$$\begin{aligned} \sigma &= (1,4,5,3)(2,6)(7)(8), \\ \tau &= (4,6,5,7)(1,8)(2)(3) \end{aligned}$$

und definieren

$$\lambda = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 1 & 7 & 6 & 5 & 8 & 2 & 3 \end{pmatrix} = (1,4,6,8,3,7,2)(5).$$

Dann gilt

$$\tau = \lambda \sigma \lambda^{-1}.$$

Beispiel: Wir betrachten die Typen von Permutationen in S_4:

Typ(σ)	ord (σ)	Anzahl solcher Permutationen
(4)	4	6
$(3,1)$	3	8
$(2,2)$	2	3
$(2,1,1)$	2	6
$(1,1,1,1)$	1	1

Wir rechnen noch etwas mit Zykeln:

Beispiele:

$$\begin{aligned}(12345)(12) &= (1345)(2),\\ (12)(12345) &= (1)(2345),\\ (12345) &= (12)(23)(34)(45),\\ (123)(12345) &= (13452),\\ (12)(23) &= (123).\end{aligned}$$

Man stellt fest, dass man jeden Zykel, und damit auch jede Permutation als Produkt von Transpositionen, d.h. Zykeln der Länge 2 schreiben kann.

LEMMA. *Für paarweise verschiedene Zahlen $a_1, a_2, \ldots, a_\ell$ aus $\{1, \ldots, n\}$ gilt:*

$$(a_1, a_2, a_3, \ldots, a_{\ell-1}, a_\ell) = (a_1, a_2)(a_2, a_3)(a_3, a_4)\ldots(a_{\ell-2}, a_{\ell-1})(a_{\ell-1}, a_\ell).$$

Ein Zykel der Länge ℓ kann also als Produkt von $\ell - 1$ Transpositionen geschrieben werden.

Beweis: Dies überprüft man, indem man schaut, was linke und rechte Seite als Abbildungen auf den Zahlen $a_1, \ldots, a_\ell$ bewirken. ■

DEFINITION. *Für eine Permutation $\sigma \in S_n$ ist ein* **Fehlstand** *ein Zahlenpaar (i, j) mit $1 \le i < j \le n$ und*

$$\sigma(i) > \sigma(j).$$

Die Menge der Fehlstände sei $F(\sigma)$, d.h.

$$F(\sigma) = \{(i, j) : 1 \le i < j \le n \text{ und } \sigma(i) > \sigma(j)\}.$$

Das **Vorzeichen** *oder* **Signum** *einer Permutation σ wird definiert durch*

$$\operatorname{sgn}(\sigma) = (-1)^{|F(\sigma)|} = \begin{cases} 1, & \text{falls } |F(\sigma)| \text{ gerade ist,} \\ -1, & \text{falls } |F(\sigma)| \text{ ungerade ist.} \end{cases}$$

Eine Permutation σ heißt **gerade**, *wenn* $\operatorname{sgn}(\sigma) = 1$ *ist, andernfalls* **ungerade**.

Beispiel: Für

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

ist

$$F(\sigma) = \{(1,2), (1,4), (1,5), (2,4), (3,4), (3,5)\} \quad \text{und} \quad \operatorname{sgn}(\sigma) = 1.$$

LEMMA. *Jede Transposition $(k, \ell) \in S_n$ hat Vorzeichen -1.*

Beweis: Wir können $k < \ell$ annehmen. Sei $\sigma = (k, \ell)$, also

$$\sigma = \begin{pmatrix} 1 & \dots & k & k+1 & \dots & \ell-1 & \ell & \ell+1 & \dots & n \\ 1 & \dots & \ell & k+1 & \dots & \ell-1 & k & \ell+1 & \dots & n \end{pmatrix}.$$

Die Fehlstände sind dann

$$F(\sigma) = \{(k,k+1),(k,k+2),\dots,(k,\ell-1),(k,\ell)\} \cup \{(k+1,\ell),(k+2,\ell),\dots,(\ell-1,\ell)\},$$

woraus sich

$$|F(\sigma)| = \Big(\ell + 1 - (k+1)\Big) + \Big((\ell-1) + 1 - (k+1)\Big) = 2\ell - 2k - 1$$

ergibt. $|F(\sigma)|$ ist also eine ungerade Zahl, und somit ist das Vorzeichen $\operatorname{sgn}(\sigma) = -1$. ■

Überlegung: Seien $x_1, \dots, x_n$ beliebige Zahlen und

$$\begin{aligned} D &= \{x_j - x_i : 1 \le i < j \le n\} = \\ &= \{x_2 - x_1, \\ &\quad x_3 - x_1, x_3 - x_2, \\ &\quad x_4 - x_1, x_4 - x_2, x_4 - x_3, \\ &\quad\quad \vdots \\ &\quad x_n - x_1, x_n - x_2, x_n - x_3, \dots, x_n - x_{n-1}\} \end{aligned}$$

Sei (i,j) ein Zahlenpaar mit $1 \le i < j \le n$.

- **Fall** $(i,j) \notin F(\sigma)$**:** Dann gilt $\sigma(i) < \sigma(j)$ und
$$x_{\sigma(j)} - x_{\sigma(i)} \in D.$$
- **Fall** $(i,j) \in F(\sigma)$**:** Dann gilt $\sigma(i) > \sigma(j)$,
$$x_{\sigma(j)} - x_{\sigma(i)} = -(x_{\sigma(i)} - x_{\sigma(j)}) \text{ und } x_{\sigma(i)} - x_{\sigma(j)} \in D.$$

Durch Produktbildung erhalten wir

$$\prod_{1 \le i < j \le n} (x_{\sigma(j)} - x_{\sigma(i)}) = (-1)^{|F(\sigma)|} \prod_{1 \le i < j \le n} (x_j - x_i),$$

weil jeder Fehlstand ein Minuszeichen zum Produkt beträgt. Wir formulieren das Ergebnis als Lemma, wobei wir $\operatorname{sgn}(\sigma)$ statt $(-1)^{|F(\sigma)|}$ schreiben:

LEMMA. *Ist $\sigma \in S_n$, sind $x_1, \dots, x_n$ beliebige Zahlen, so gilt*

$$\prod_{1 \le i < j \le n} (x_{\sigma(j)} - x_{\sigma(i)}) = \operatorname{sgn}(\sigma) \prod_{1 \le i < j \le n} (x_j - x_i).$$

Mit der letzten Darstellung des Vorzeichens einer Permutation erhalten wir leicht folgenden Satz:

SATZ. *Sei $n \in \mathbb{N}_{\ge 2}$.*

(1) *Für Permutation $\sigma, \tau \in S_n$ gilt*
$$\operatorname{sgn}(\sigma\tau) = \operatorname{sgn}(\sigma)\operatorname{sgn}(\tau).$$

(2) *Für einen Zykel $(a_1, \dots, a_\ell)$ der Länge ℓ gilt*
$$\operatorname{sgn}((a_1, \dots, a_\ell)) = (-1)^{\ell-1} = \begin{cases} 1, & \text{falls } \ell \text{ ungerade ist,} \\ -1, & \text{falls } \ell \text{ gerade ist.} \end{cases}$$

(3) *Hat $\sigma \in \mathbb{N}_2$ die Zykelzerlegung*

$$\sigma = (a_{1,1}, \ldots, a_{1,\ell_1})(a_{2,1}, \ldots, a_{2,\ell_2}) \ldots (a_{r,1}, \ldots, a_{r,\ell_r}),$$

so gilt

$$\operatorname{sgn}(\sigma) = (-1)^{|\{i:\ell_i \text{ gerade}\}|},$$

was auch so ausgedrückt werden kann:

$$\operatorname{sgn}(\sigma) = \begin{cases} 1, & \text{falls die Anzahl der Zykel gerader Länge in der Zykelzerlegung von } \sigma \text{ gerade ist,} \\ -1, & \text{falls die Anzahl der Zykel gerader Länge in der Zykelzerlegung von } \sigma \text{ ungerade ist.} \end{cases}$$

Beweis:

(1) Wir wählen paarweise verschiedene Zahlen $x_1, \ldots, x_n$ und setzen $y_i = x_{\sigma(i)}$. Dann ist $y_{\tau(i)} = x_{\sigma(\tau(i))}$. Es folgt

$$\begin{aligned} \operatorname{sgn}(\sigma\tau) \prod_{1\le i<j\le n} (x_j - x_i) &= \prod_{1\le i<j\le n} (x_{(\sigma\tau)(j)} - x_{(\sigma\tau)(i)}) = \prod_{1\le i<j\le n} (x_{\sigma(\tau(j))} - x_{\sigma(\tau(i))}) = \\ &= \prod_{1\le i<j\le n} (y_{\tau(j)} - y_{\tau(i)}) = \operatorname{sgn}(\tau) \prod_{1\le i<j\le n} (y_j - y_i) = \\ &= \operatorname{sgn}(\tau) \prod_{1\le i<j\le n} (x_{\sigma(j)} - x_{\sigma(i)}) = \\ &= \operatorname{sgn}(\tau)\operatorname{sgn}(\sigma) \prod_{1\le i<j\le n} (x_j - x_i), \end{aligned}$$

und damit

$$\operatorname{sgn}(\sigma\tau) = \operatorname{sgn}(\sigma)\operatorname{sgn}(\tau).$$

(2) Da wir $(a_1, \ldots, a_\ell)$ als Produkt

$$(a_1, \ldots, a_\ell) = (a_1, a_2)(a_2, a_3)(a_3, a_4) \ldots (a_{\ell-2}, a_{\ell-1})(a_{\ell-1}, a_\ell)$$

von $\ell - 1$ Transpositionen schreiben können, da Transpositionen Sigum -1 haben, folgt die Behauptung mit (1).

(3) Mit (1) und (2) ergibt sich

$$\operatorname{sgn}(\sigma) = \prod_{i=1}^{r} (-1)^{\ell_i - 1} = \prod_{\substack{1\le i\le r \\ \ell_i \text{ gerade}}} (-1) = (-1)^{|\{1\le i\le r:\ell_i \text{ gerade}\}|},$$

woraus dann der Rest folgt. ■

5. Untergruppen

DEFINITION. *Sei G eine Gruppe mit einer Verknüpfung $*$. Eine Teilmenge $H \subseteq G$ heißt* **Untergruppe** *von G, wenn $*$ auch eine Verknüpfung auf H definiert, d.h. wenn $a * b \in H$ für alle $a, b \in H$ gilt, und wenn H mit der Verknüpfung $*$ eine Gruppe ist.*

Das folgende Kriterium ist unmittelbar klar, da die Assoziativität auch für jede Teilmenge einer Gruppe gilt.

LEMMA. *Eine Teilmenge H einer Gruppe G (mit Verknüpfung $*$) ist genau dann eine Untergruppe von G, wenn folgende Bedingungen erfüllt sind:*

(1) *Für alle $a, b \in H$ gilt $a * b \in H$.*
(2) *Das neutrale Element von G liegt in H.*
(3) *Ist $a \in H$ und b das in G zu a inverse Element, so gilt $b \in H$.*

Beispiele:

(1) Ist $(G, *)$ eine Gruppe mit neutralem Element e, so sind
$$\{e\} \quad \text{und} \quad G$$
Untergruppen von G. (Manchmal bezeichnet man diese auch als „triviale“ Untergruppen.)
(2) $(\mathbb{R}, +)$ ist eine abelsche Gruppe. Offensichtlich sind $(\mathbb{Q}, +)$ und $(\mathbb{Z}, +)$ Untergruppen.
(3) $(\mathbb{R}^*, \cdot)$ ist eine abelsche Gruppe. Untergruppen sind beispielsweise $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}_{>0}, \cdot)$ und $\{\pm 1\}$.

Die spezielle lineare Gruppe $\mathrm{SL}_n(K)$**:** Für einen Körper K (wie $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$) definiert man
$$\mathrm{SL}_n(K) = \{A \in \mathrm{M}_n(K) : \det(A) = 1\}.$$

Lemma. *Für einen Körper K ist $\mathrm{SL}_n(K)$ mit der Matrizenmultiplikation eine Untergruppe von $\mathrm{GL}_n(K)$ und damit selbst eine Gruppe.*

Beweis: Natürlich gilt $\mathrm{SL}_n(K) \subseteq \mathrm{GL}_n(K) = \{A \in \mathrm{M}_n(K) : \det(A) \neq 0\}$. Wir zeigen, dass $\mathrm{SL}_n(K)$ mit der Matrizenmultiplikation eine Untergruppe von $\mathrm{GL}_n(K)$ ist, indem wir die Bedingungen des Lemmas überprüfen:

(1) Sind $A, B \in \mathrm{SL}_n(K)$, so gilt $\det(A) = \det(B) = 1$, und mit der Determinantenmultiplikationsregel
$$\det(AB) = \det(A) \cdot \det(B) = 1 \cdot 1 = 1,$$
woraus $AB \in \mathrm{SL}_n(K)$ folgt.
(2) Das neutrale Element von $\mathrm{GL}_n(K)$ ist die Einheitsmatrix $\mathbf{1}_n$, die natürlich Determinante 1 hat, sodass also $\mathbf{1}_n \in \mathrm{SL}_n(K)$ gilt.
(3) Ist $A \in \mathrm{SL}_n(K)$, so gilt $\det(A) = 1$. In $\mathrm{GL}_n(K)$ ist die Matrix A^{-1} zu A invers. Nun gilt aber $\det(A^{-1}) = \det(A)^{-1} = 1^{-1} = 1$, sodass auch $A^{-1} \in \mathrm{SL}_n(K)$ gilt.

Daher ist $\mathrm{SL}_n(K)$ eine Untergruppe von $\mathrm{GL}_n(K)$ und damit selbst eine Gruppe. ■

Die alternierende Gruppe A_n besteht als Menge aus den geraden Permutationen der Gruppe S_n, d.h.
$$A_n = \{\sigma \in S_n : \mathrm{sgn}(\sigma) = 1\}.$$

Lemma. *A_n ist eine Untergruppe von S_n und hat für $n \geq 2$ Ordnung*
$$|A_n| = \frac{1}{2} \cdot n!.$$

Beweis:

- Die Untergruppeneigenschaften überprüft man ähnlich wie bei $\mathrm{SL}_n(K)$ mit Hilfe der Multiplikativität der Signum-Funktion sgn.
- Es ist $\mathrm{sgn}((12)) = -1$. Man sieht leicht, dass die Abbildung
$$A_n \to S_n \setminus A_n, \quad \sigma \mapsto \sigma \cdot (12)$$
bijektiv ist, was $|A_n| = |S_n \setminus A_n|$ und damit
$$|A_n| = \frac{1}{2}|S_n| = \frac{1}{2} \cdot n!$$
liefert. ■

Beispiel: In S_3 haben wir
$$A_3 = \{(1), (123), (132)\} \quad \text{und} \quad S_3 \setminus A_3 = \{(12), (13), (23)\}.$$
In S_4 ist
$$A_4 = \{(1), (123), (132), (124), (142), (134), (143), (234), (243), (12)(34), (13)(24), (14)(23)\}.$$

In jeder Gruppe kann man folgende Untergruppe betrachten:

DEFINITION. *Ist G eine (multiplikativ geschriebene) Gruppe, so heißt*

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

das **Zentrum** *von G. (Das Zentrum besteht also aus den Gruppenelementen, die mit allen anderen kommutieren.)*

Einfach zu beweisen ist das folgende Lemma:

LEMMA. *Für eine Gruppe G ist das Zentrum $Z(G)$ eine Untergruppe von G.*

Bemerkung: Ist G abelsch, so ist natürlich das Zentrum die ganze Gruppe: $Z(G) = G$. Ist G nicht abelsch, so gilt natürlich $Z(G) \subsetneq G$.

Beispiel: Ist G eine multiplikativ geschriebene Gruppe und $g \in G$, so ist offensichtlich

$$\{g^k : k \in \mathbb{Z}\}$$

eine Untergruppe von G.

Wir werden das letzte Beispiel gleich verallgemeinern. Zuvor erwähnen wir noch ein wichtiges Resultat, das im Fall endlicher Gruppen die Gruppenordnung mit den Untergruppenordnungen vergleicht.

SATZ. *Ist G eine endliche Gruppe und H eine Untergruppe, so teilt die Ordnung von H die Ordnung von G, d.h.*

$$|H| \mid |G|.$$

Der Beweis wird später nochmals aufgegriffen, die grundlegende Idee sei aber hier bereits skizziert.

Beweis:

- Wir definieren eine Relation $\sim$ auf G:

  $$a \sim b \quad \Longleftrightarrow \quad a^{-1}b \in H.$$

  Sei e das neutrale Element von G, das natürlich auch in H liegt. Wir zeigen, dass $\sim$ eine Äquivalenzrelation ist:
  - *Transitivität:*

    $$a \sim b, b \sim c \quad \Longrightarrow \quad a^{-1}b, b^{-1}c \in H \quad \Longrightarrow \quad a^{-1}c = (a^{-1}b)(b^{-1}c) \in H \quad \Longrightarrow \quad a \sim c.$$

  - *Symmetrie:*

    $$a \sim b \quad \Longrightarrow \quad a^{-1}b \in H \quad \Longrightarrow \quad b^{-1}a = (a^{-1}b)^{-1} \in H \quad \Longrightarrow \quad b \sim a.$$

  - *Reflexivität:*

    $$a^{-1}a = e \in H \quad \Longrightarrow \quad a \sim a.$$

- Die Äquivalenzklasse von $a \in G$ ist

  $$\{b \in G : b \sim a\} = \{b \in G : a \sim b\}.$$

  Wir zeigen, dass

  $$f_a : H \to \{b \in G : b \sim a\}, \quad h \mapsto ah$$

  wohldefiniert und bijektiv ist:
  - *Wohldefiniertheit:* Für $h \in H$ ist $a^{-1}(ah) = h \in H$, also $ah \sim a$, und damit $ah \in \{b \in G : b \sim a\}$, die Abbildung f_a ist also wohldefiniert.
  - *Injektivität:* $f_a(h) = f_a(h')$ bedeutet $ah = ah'$, woraus natürlich sofort $h = h'$ folgt.
  - *Surjektivität:* Sei $c \in \{b \in G : b \sim a\} = \{b \in G : a \sim b\}$. Dann ist $a \sim c$, also $a^{-1}c \in H$. Die Behauptung folgt dann aus $f_a(a^{-1}c) = a(a^{-1}c) = c$.

  Insbesondere folgt für die Mächtigkeit der Äquivalenzklasse:

  $$|\{b \in G : b \sim a\}| = |H|.$$

- Die Äquivalenzklassen haben also alle genau $|H|$ Elemente. Da G die G die disjunkte Vereinigung der Äquivalenzklassen ist, folgt
$$|G| = k \cdot |H|,$$
wenn k die Anzahl der Äquivalenzklassen bezeichnet. Daher gilt $|H| \mid |G|$, wie behauptet. ■

LEMMA. *Ist G eine Gruppe, ist $(U_i)_{i\in I}$ eine Familie von Untergruppen von G, so ist auch der Durchschnitt*
$$\bigcap_{i\in I} U_i$$
eine Untergruppe von G.

Beweis: Man überprüft direkt die drei Eigenschaften des zuvor angegebenen Untergruppenkriteriums. ■

Bemerkung: Ist G eine Gruppe und $S \subseteq G$ eine nichtleere Teilmenge, so ist offensichtlich
$$\bigcap_{\substack{U \text{ Untergruppe} \\ S\subseteq U}} U$$
die kleinste S enthaltende Untergruppe. Dies führt zu folgender Definition:

DEFINITION. *Sei G eine Gruppe.*

(1) *Ist $S \subseteq G$ eine nichtleere Teilmenge, dann heißt die kleinste, S enthaltende Untergruppe von G*
$$\bigcap_{\substack{U \text{ Untergruppe} \\ S\subseteq U}} U$$
die von S **erzeugte Untergruppe** *und man schreibt $\langle S\rangle$. Ist $S = \{s_1, \dots, s_r\}$ endlich, so schreibt man auch $\langle s_1, \dots, s_r\rangle$ statt $\langle\{s_1, \dots, s_r\}\rangle$.*

(2) *Die Gruppe G heißt* **endlich erzeugt***, wenn es endlich viele Gruppenelemente $s_1, \dots, s_r \in G$ gibt mit*
$$G = \langle s_1, \dots, s_r\rangle.$$
Die Elemente $s_1, \dots, s_r$ nennt man dann ein Erzeugendensystem.

(3) *Die Gruppe G heißt* **zyklisch***, wenn sie sich von einem Element erzeugen lässt, d.h. wenn es ein $g \in G$ gibt mit*
$$G = \langle g\rangle.$$

Bemerkung: Ist G eine additiv geschriebene abelsche Gruppe, sind $a_1, a_2, \dots, a_r \in G$, so sieht man leicht, dass
$$\langle a_1, a_2, \dots, a_r\rangle = \{n_1a_1 + n_2a_2 + \cdots + n_ra_r : n_1, \dots, n_r \in \mathbb{Z}\}$$
gilt.

6. Zyklische Gruppen

Wir betrachten zyklische Gruppen. (Die meisten Aussagen haben wir bereits kennengelernt, als wir die Ordnung von Gruppenelementen besprochen haben.)

SATZ. *Sei G eine (multiplikativ geschriebene) zyklische Gruppe und $g \in G$ mit $G = \langle g\rangle$.*

(1) *Es ist*
$$G = \{g^i : i \in \mathbb{Z}\}.$$

(2) **Fall** $\operatorname{ord}(g) = \infty$**:**
   (a) *Die Potenzen g^i, $i \in \mathbb{Z}$ sind paarweise verschieden.*
   (b) *Die einzigen Erzeuger von G sind g und g^{-1}.*

(3) **Fall** $\operatorname{ord}(g) < \infty$**:**
   (a) *G enthält genau $\operatorname{ord}(g)$ Elemente, nämlich*
$$G = \{g^0, g^1, g^2, \dots, g^{\operatorname{ord}(g)-1}\}.$$

(b) *Für $i, j \in \mathbb{Z}$ gilt*
$$g^i = g^j \quad \Longleftrightarrow \quad \operatorname{ord}(g) \mid j - i.$$
(c) *Genau dann erzeugt g^i die Gruppe G, wenn gilt* $\operatorname{ggT}(i, \operatorname{ord}(g)) = 1$.
(d) *G hat genau $\varphi(\operatorname{ord}(g))$ Erzeuger, nämlich*
$$g^i \text{ mit } 0 \leq i \leq \operatorname{ord}(g) - 1 \text{ und } \operatorname{ggT}(\operatorname{ord}(g), i) = 1.$$

Beweis:

(1) Die kleinste g enthaltende Untergruppe von G ist offensichtlich
$$\{g^i : i \in \mathbb{Z}\},$$
woraus dann die Behauptung folgt, da G nach Voraussetzung von g erzeugt wird.
(2) $\operatorname{ord}(g) = \infty$.
(a) Dies haben wir bereits zuvor behandelt.
(b) Gilt auch $\langle h \rangle = G$, so gibt es $i, j \in \mathbb{Z}$ mit
$$h = g^i \quad \text{und} \quad g = h^j.$$
Es folgt
$$g = h^j = (g^i)^j = g^{ij},$$
und damit nach (a) die Gleichung $ij = 1$, die in $\mathbb{Z}$ genau zwei Lösungen hat: $i = j = 1$ und $i = j = -1$. Im ersten Fall gilt $h = g$, im zweiten $h = g^{-1}$. Dass tatsächlich $\langle g^{-1} \rangle = \langle g \rangle$ gilt, ist klar.
(3) $\operatorname{ord}(g) < \infty$.
(a) und (b) haben wir bereits bei der Behandlung der Ordnungsfunktion gesehen.
(c) Es gilt, wenn e das neutrale Element bezeichnet:
$$\begin{aligned}
\langle g^i \rangle = \langle g \rangle \quad &\Longleftrightarrow \quad \langle g^i \rangle \subseteq \langle g \rangle \text{ und } \langle g \rangle \subseteq \langle g^i \rangle \quad \Longleftrightarrow \\
&\Longleftrightarrow \quad \langle g \rangle \subseteq \langle g^i \rangle \quad \Longleftrightarrow \quad g \in \langle g^i \rangle \quad \Longleftrightarrow \\
&\Longleftrightarrow \quad g = (g^i)^j \text{ für ein } j \in \mathbb{Z} \quad \Longleftrightarrow \\
&\Longleftrightarrow \quad g^{ij-1} = e \text{ für ein } j \in \mathbb{Z} \quad \Longleftrightarrow \\
&\Longleftrightarrow \quad \operatorname{ord}(g) \mid ij - 1 \text{ für ein } j \in \mathbb{Z} \quad \Longleftrightarrow \\
&\Longleftrightarrow \quad (ij) \bmod \operatorname{ord}(g) = 1 \text{ für ein } j \in \mathbb{Z} \quad \Longleftrightarrow \\
&\Longleftrightarrow \quad (i \bmod \operatorname{ord}(g)) \in \mathbb{Z}^*_{\operatorname{ord}(g)} \quad \Longleftrightarrow \\
&\Longleftrightarrow \quad \operatorname{ggT}(\operatorname{ord}(g), i) = 1.
\end{aligned}$$
(d) Dies folgt sofort aus der Definition der φ-Funktion. ■

FOLGERUNG. *Ist G eine endliche Gruppe mit neutralem Element e und $g \in G$, so gilt*
$$\operatorname{ord}(g) \mid |G| \quad \text{und} \quad g^{|G|} = e.$$

Beweis: g erzeugt die Untergruppe $\langle g \rangle$ der Ordnung $\operatorname{ord}(g)$. Da die Untergruppenordnung die Gruppenordnung teilt, gilt $\operatorname{ord}(g) \mid |G|$. Daraus folgt aber sofort $g^{|G|} = e$. ■

SATZ. *Ist G eine endliche Gruppe mit Primzahlordnung p, so gilt für jedes vom neutralen Element verschiedene Element $g \in G$*
$$G = \langle g \rangle.$$
Insbesondere ist G eine zyklische Gruppe.

Beweis: Es gilt $\operatorname{ord}(g) \mid |G|$. Da g nicht das neutrale Element ist, gilt $\operatorname{ord}(g) > 1$. Da G eine Primzahl sein sollte, folgt $\operatorname{ord}(g) = |G|$ und damit natürlich $\langle g \rangle = G$. ■

Beispiele:

(1) Die Standardbeispiele für zyklische Gruppen sind die additiv geschriebenen Gruppen $(\mathbb{Z}_n, +_{\bmod n})$. Für $n \geq 2$ werden alle diese Gruppen von 1 erzeugt.
(2) Das „kleinste“ Beispiel einer nichtzyklischen Gruppe ist die Kleinsche Vierergruppe

$$\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0,0),(0,1),(1,0),(1,1)\}.$$

Es ist

$$\langle (0,0)\rangle = \{(0,0)\}$$

und

$$\langle (1,0)\rangle = \{(0,0),(1,0)\}, \quad \langle (0,1)\rangle = \{(0,0),(0,1)\}, \quad \langle (1,1)\rangle = \{(0,0),(1,1)\}.$$

Insbesondere gibt es drei zyklische Untergruppen der Ordnung 2.

Wir wollen nun die Untergruppen von $(\mathbb{Z}, +)$ bestimmen.

Satz. *Die Untergruppen von $(\mathbb{Z}, +)$ sind $\mathbb{Z}\,d$ für $d \in \mathbb{N}_0$. Dabei ist*

$$\mathbb{Z}\,0 = \{0\} = \langle 0\rangle \quad \textit{und} \quad \mathbb{Z}\,d = \{0, \pm d, \pm 2d, \pm 3d, \pm 4d, \dots\} = \langle d\rangle \textit{ für } d \geq 1.$$

Dabei gilt für eine Untergruppe $U = \mathbb{Z}\,d \subseteq \mathbb{Z}$, $U \neq \{0\}$

$$d = \min\{n \in U : n > 0\}.$$

Jede Untergruppe ist also ebenfalls eine zyklische Gruppe.

Beweis: Es ist klar, dass die Mengen $\mathbb{Z}\,d$ Untergruppen von $\mathbb{Z}$ sind. Sei umgekehrt $U \subseteq \mathbb{Z}$ eine Untergruppe mit $U \neq \{0\}$. Ist $m \in U \setminus \{0\}$, so auch das Inverse $-m \in U$. Daher enthält U Zahlen > 0, sodass

$$d = \min\{n \in U : n > 0\}$$

wohldefiniert ist. Aus der Untergruppeneigenschaft von U folgt mit $d \in U$ sofort

$$\mathbb{Z}\,d \subseteq U.$$

Sei nun $n \in U$ beliebig gegeben. Wir dividieren n durch d und erhalten eine Darstellung $n = qd + r$ mit $q, r \in \mathbb{Z}$ mit $0 \leq r < d$. Die Gruppeneigenschaft von U impliziert

$$r = n - qd \in U.$$

Aus der Definition von d folgt $r = 0$, und damit $n = qd \in \mathbb{Z}\,d$. Daher folgt

$$U = \mathbb{Z}\,d,$$

was wir zeigen wollten. ■

Der folgende Satz zeigt, wie ggT und kgV bei den Untergruppen von $(\mathbb{Z}, +)$ ins Spiel kommen.

Satz. *Für $a, b \in \mathbb{Z}$ gilt in der Gruppe $(\mathbb{Z}, +)$*

$$\langle a, b\rangle = \mathbb{Z}\,\mathrm{ggT}(a,b) = \langle \mathrm{ggT}(a,b)\rangle \quad \textit{und} \quad \langle a\rangle \cap \langle b\rangle = \langle \mathrm{kgV}(a,b)\rangle.$$

Beweis:

(1) Wir zeigen zunächst $\langle a, b\rangle = \mathbb{Z}\,\mathrm{ggT}(a,b)$.
   - $\subseteq$ Wegen $\mathrm{ggT}(a,b) \mid a$ und $\mathrm{ggT}(a,b) \mid b$ gilt $a, b \in \mathbb{Z}\,\mathrm{ggT}(a,b)$, und damit $\langle a, b\rangle \subseteq \mathbb{Z}\,\mathrm{ggT}(a,b)$.
   - $\supseteq$ Nach dem erweiterten euklidischen Algorithmus existieren $x, y \in \mathbb{Z}$ mit $\mathrm{ggT}(a,b) = xa + yb$. Daher gilt $\mathrm{ggT}(a,b) \in \langle a, b\rangle$, und damit $\mathbb{Z}\,\mathrm{ggT}(a,b) \subseteq \langle a, b\rangle$.

   Dies beweist die Behauptung.
(2) Wir zeigen nun $\langle a\rangle \cap \langle b\rangle = \langle \mathrm{kgV}(a,b)\rangle$.
   - $\subseteq$ Sei $c \in \langle a\rangle \cap \langle b\rangle$. Dann existieren $x, y \in \mathbb{Z}$ mit $c = xa$ und $c = yb$. Also ist c ein gemeinsames Vielfaches von a und b, woraus sofort $\mathrm{kgV}(a,b) \mid c$, und damit $c \in \mathbb{Z}\,\mathrm{kgV}(a,b)$ folgt.
   - $\supseteq$ Wegen $a \mid \mathrm{kgV}(a,b)$ gilt $\mathrm{kgV}(a,b) \in \langle a\rangle$, wegen $b \mid \mathrm{kgV}(a,b)$ gilt $\mathrm{kgV}(a,b) \in \langle b\rangle$. Dies impliziert $\mathrm{kgV}(a,b) \in \langle a\rangle \cap \langle b\rangle$, und damit $\langle \mathrm{kgV}(a,b)\rangle \subseteq \langle a\rangle \cap \rangle b\rangle$.

Daher gilt auch die zweite Aussage. ■

Wir betrachten nun die Untergruppen der endlichen zyklischen Gruppen.

SATZ. *Sei G eine zyklische Gruppe der Ordnung n, erzeugt von einem Element g.*

(1) *Zu jedem Teiler d von n gibt es genau eine Untergruppe der Ordnung d, nämlich*
$$U_d = \{x \in G : x^d = e\},$$
wobei e das neutrale Element von G bezeichnet. Es gilt
$$U_d = \langle g^{\frac{n}{d}} \rangle.$$
Insbesondere ist jede Untergruppe wieder zyklisch.

(2) *Für $a \in \mathbb{Z}$ gilt*
$$\langle g^a \rangle = \langle g^{\mathrm{ggT}(n,a)} \rangle = U_{\frac{n}{\mathrm{ggT}(n,a)}}.$$

(3) *Zu jedem Teiler d von n gibt es genau $\varphi(d)$ Elemente der Ordnung d in G, d.h.*
$$|\{x \in G : \mathrm{ord}\,(x) = d\}| = \varphi(d).$$

Beweis:

(1)
- Es gilt (wegen $\mathrm{ord}\,(g) = n$) für $d \mid n$
$$g^i \in U_d \iff g^{di} = e \iff n \mid di \iff \frac{n}{d} \mid i.$$
Also gilt
$$U_d = \{g^{\frac{n}{d}j} : j \in \mathbb{Z}\} = \langle g^{\frac{n}{d}} \rangle.$$
Wegen $\mathrm{ord}\,(g^{\frac{n}{d}}) = d$ gilt
$$|U_d| = |\langle g^{\frac{n}{d}} \rangle| = \mathrm{ord}\,(g^{\frac{n}{d}}) = d.$$
- Ist umgekehrt $U \subseteq G$ eine Untergruppe der Ordnung d, so folgt aus $g^{|U|} = e$ für alle $g \in U$ sofort $U \subseteq U_d$. Da beide Gruppen Ordnung d haben, folgt $U = U_d$.

(2) Aus $\mathrm{ggT}(n,a) \mid a$ folgt $g^a \in \langle g^{\mathrm{ggT}(n,a)} \rangle$, also
$$\langle g^a \rangle \subseteq \langle g^{\mathrm{ggT}(n,a)} \rangle.$$
Umgekehrt findet man mit dem erweiterten euklidischen Algorithmus $i, j \in \mathbb{Z}$ mit $\mathrm{ggT}(n,a) = in + ja$. Es folgt wegen $g^n = e$
$$g^{\mathrm{ggT}(n,a)} = (g^n)^i \cdot (g^a)^j = (g^a)^j \in \langle g^a \rangle,$$
und damit
$$\langle g^{\mathrm{ggT}(n,a)} \rangle \subseteq \langle g \rangle.$$
Zusammen erhalten wir
$$\langle g^a \rangle = \langle g^{\mathrm{ggT}(n,a)} \rangle.$$
Der zweite Teil der Gleichheit folgt aus (1) für $d = \frac{n}{\mathrm{ggT}(n,a)}$.

(3) Sei d ein Teiler von n. Ist $x \in G$ mit $\mathrm{ord}\,(x) = d$, so hat $\langle x \rangle$ Ordnung d, also gilt $\langle x \rangle = U_d$. Das Element x ist dann Erzeuger der zyklischen Gruppe U_d der Ordnung d. So sieht man, dass die Elemente der Ordnung d genau die Erzeuger der zyklischen Gruppe U_d sind. Davon gibt es $\varphi(d)$ Stück, was die Behauptung beweist. ■

Wir ziehen gleich eine Folgerung aus dem letzten Satz:

SATZ. *Für die Eulersche φ-Funktion gilt*
$$\sum_{d|n} \varphi(d) = n.$$

Beweis: Wir wählen eine zyklische Gruppe G der Ordnung n. (Ein additives Beispiel ist $(\mathbb{Z}_n, +)$.) Da für $x \in G$ die Elementordnung $\operatorname{ord}(x)$ die Gruppenordnung $|G|$ teilt, erhalten wir folgende Zerlegung von G in disjunkte Teilmengen:

$$G = \bigcup_{d|n} \{x \in G : \operatorname{ord}(x) = d\}.$$

Daher folgt mit Teil (3) des vorangegangenen Satzes

$$n = |G| = \sum_{d|n} |\{x \in G : \operatorname{ord}(x) = d\}| = \sum_{d|n} \varphi(d),$$

was wir zeigen wollten. ■

FOLGERUNG. *Für die Eulersche φ-Funktion gilt: Ist p eine Primzahl und $e \in \mathbb{N}$, so ist*

$$\varphi(p) = p - 1 \quad \textit{und} \quad \varphi(p^e) = p^e - p^{e-1} = p^{e-1}(p-1) = p^e(1 - \frac{1}{p}).$$

Beweis:

- Die Eigenschaft $\varphi(p) = p - 1$ haben wir bereits zuvor bemerkt. Sie liegt einfach daran, dass von den Zahlen $0, 1, \ldots, p-1$ alle Zahlen $1, \ldots, p-1$ teilerfremd zu p sind, da p ja keinen nichttrivialen Teiler besitzt, d.h.

  $$\{0 \le a \le p-1 : \operatorname{ggT}(p, a) = 1\} = \{1, 2, \ldots, p-1\},$$

  womit natürlich

  $$\varphi(p) = |\{0 \le a \le p-1 : \operatorname{ggT}(p, a) = 1\}| = p - 1$$

  gilt. (Es ist $\operatorname{ggT}(p, 0) = p$.)
- Die Eigenschaft $\varphi(p^e) = p^e - p^{e-1}$ kann man auch direkt aus der Definition ableiten. Wir zeigen hier, wie man die Formeln durch Induktion mit Hilfe der Formel

  $$\sum_{d|n} \varphi(d) = n$$

  erhält. Für $e = 1$ haben wir die Formel gezeigt. Sei nun $e \ge 2$ und die Formel für alle p^i mit $1 \le i \le e-1$ bereits gezeigt. Dann folgt

  $$\begin{aligned} p^e &= \sum_{d|p^e} \varphi(d) = \sum_{i=0}^{e} \varphi(p^i) = \varphi(1) + \varphi(p) + \varphi(p^2) + \cdots + \varphi(p^{e-1}) + \varphi(p^e) = \\ &= 1 + (p-1) + (p^2 - p) + (p^3 - p^2) + \cdots + (p^{e-1} - p^{e-2}) + \varphi(p^e) = \\ &= p^{e-1} + \varphi(p^e), \end{aligned}$$

  woraus sofort

  $$\varphi(p^e) = p^e - p^{e-1}$$

  folgt. Der Rest folgt durch Ausklammern von p^{e-1} bzw. p^e. ■

Die Untergruppen der zyklischen Gruppe $(\mathbb{Z}_n, +_{\bmod n})$: Dies ist natürlich nichts Neues. Wir geben dies an, weil hier die additive Schreibweise verwendet wird. Für jeden Teiler d von n gibt es genau eine Untergruppe der Ordnung d, nämlich

$$U_d = \{0, \frac{n}{d}, 2 \cdot \frac{n}{d}, \ldots (d-1) \cdot \frac{n}{d}\}.$$

Beispiel: Die Untergruppen von $(\mathbb{Z}_{12}, +)$ sind

$$\begin{aligned} U_1 &= \{0\}, \\ U_2 &= \{0, 6\}, \\ U_3 &= \{0, 4, 8\}, \\ U_4 &= \{0, 3, 6, 9\}, \\ U_6 &= \{0, 2, 4, 6, 8, 10\}, \\ U_{12} &= \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}. \end{aligned}$$

Wir haben vorhin gesehen, dass es in einer zyklischen Gruppe zu jedem Teiler der Gruppenordnung genau eine Untergruppe mit dieser Ordnung gibt. Der folgende Satz zeigt, dass diese Eigenschaft die zyklischen Gruppen auszeichnet.

SATZ. *Ist G eine endliche (abelsche oder nichtabelsche) Gruppe der Ordnung n, sodass es zu jedem Teiler d der Gruppenordnung n höchstens eine Untergruppe der Ordnung d gibt, so ist G eine zyklische Gruppe.*

Beweis:

(1) Wir definieren
$$E_d = \{g \in G : \operatorname{ord}(g) = d\}.$$
Da die Elementordnung die Gruppenordnung teilt, erhalten wir eine disjunkte Zerlegung
$$G = \bigcup_{d|n} E_d.$$

(2) Ist $E_d \neq \emptyset$, so wählen wir ein $g \in E_d$. Dann ist $\langle g \rangle$ eine Untergruppe der Ordnung d. Ist $g' \in E_d$, so ist auch $\langle g' \rangle$ eine Untergruppe der Ordnung d. Da es aber nur eine solche Gruppe gibt, gilt $\langle g \rangle = \langle g' \rangle$. Damit sind die Elemente von E_d genau die Erzeuger der zyklischen Gruppe $\langle g \rangle$. Insbesondere folgt
$$|E_d| = \varphi(d).$$

(3) Aus
$$n = |G| = \sum_{d|n} |E_d| \leq \sum_{d|n} \varphi(d) = n$$
folgt, dass für alle $d \mid n$ gilt $|E_d| = \varphi(d)$. Insbesondere gilt $|E_n| = \varphi(n)$, also gibt es Elemente der Ordnung n, was beweist, dass G zyklisch ist. ■

Wir folgern aus dem vorangegangenen Satz eine weiteres Kriterium für eine zyklische Gruppe:

SATZ. *Ist G eine endliche (abelsche oder nichtabelsche) Gruppe der Ordnung n, sodass für jeden Teiler d der Gruppenordnung die Menge*
$$U_d = \{x \in G : x^d = e\}$$
höchstens d Elemente enthält, d.h. $|U_d| \leq d$, so ist G eine zyklische Gruppe.

Beweis: Wir wollen den Satz mit Hilfe des vorangegangenen Satzes beweisen. Sei also d ein Teiler der Gruppenordnung n und U irgendeine Untergruppe der Ordnung d. Da für $x \in U$ die Beziehung $x^{|U|} = e$, also $x^d = e$, und damit $x \in U_d$ gilt, folgt
$$U \subseteq U_d.$$
Wegen $|U| = d$ und $|U_d| \leq d$ folgt
$$U = U_d.$$
Also ist U_d eine Untergruppe der Ordnung d. Da U beliebig gewählt werden konnte, ist U_d auch die einzige Untergruppe der Ordnung d.
Existiert also eine Untergruppe der Ordnung d, so ist dies U_d. Aus dem vorangegangenen Satz folgt, dass G zyklisch ist. ■

7. Diedergruppen

DEFINITION. *Eine Gruppe G heißt eine* **Diedergruppe** *der Ordnung $2n$ (für ein $n \in \mathbb{N}_{\geq 3}$), wenn es Elemente $\delta, \sigma \in G$ gibt mit*

$$G = \langle \delta, \sigma \rangle, \quad \operatorname{ord}(\delta) = n, \quad \operatorname{ord}(\sigma) = 2, \quad \sigma\delta\sigma^{-1} = \delta^{-1}.$$

(Die letzte Relation kann man wegen $\operatorname{ord}(\sigma) = 2$ natürlich auch in der Form $\sigma\delta\sigma = \delta^{-1}$ schreiben.) Man findet dafür auch die Schreibweise D_n, manchmal auch D_{2n}.

SATZ. *Sei G eine Diedergruppe der Ordnung $2n$ (mit $n \geq 3$), also*

$$G = \langle \delta, \sigma \rangle, \quad \operatorname{ord}(\delta) = n, \quad \operatorname{ord}(\sigma) = 2, \quad \sigma\delta\sigma^{-1} = \delta^{-1}.$$

Dann gelten folgende Aussagen:

(1) *Für alle $i, j \in \mathbb{Z}$ gilt*

$$\delta^i \cdot \delta^j = \delta^{(i+j) \bmod n}, \quad \delta^i\sigma \cdot \delta^j\sigma = \delta^{(i-j) \bmod n},$$
$$\delta^i \cdot \delta^j\sigma = \delta^{(i+j) \bmod n}\sigma, \quad \delta^i\sigma \cdot \delta^j = \delta^{(i-j) \bmod n}\sigma$$

und

$$(\delta^i)^{-1} = \delta^{(-i) \bmod n}, \quad (\delta^i\sigma)^{-1} = \delta^i\sigma.$$

(2) *Es ist*

$$G = \{\delta^i : 0 \leq i \leq n-1\} \cup \{\delta^i\sigma : 0 \leq j \leq n-1\} \text{ mit } |G| = 2n.$$

(3) *Für alle $i \in \mathbb{Z}$ gilt*

$$\operatorname{ord}(\delta^i\sigma) = 2 \quad \text{und} \quad (\delta^i\sigma)\,\delta\,(\delta^i\sigma)^{-1} = \delta^{-1}.$$

(Die Rolle von σ in der Definition einer Diedergruppe kann also auch von jedem andern Element $\delta^i\sigma$ übernommen werden.)

Beweis:

(1) Mit $\operatorname{ord}(\delta) = n$, $\sigma\delta^i\sigma^{-1} = \delta^{-i}$ und $\sigma = \sigma^{-1}$ ergibt sich:

$$\begin{aligned}
\delta^i \cdot \delta^j &= \delta^{i+j} = \delta^{(i+j) \bmod n}, \\
\delta^i \cdot \delta^j\sigma &= \delta^{i+j}\sigma = \delta^{(i+j) \bmod n}\sigma, \\
\delta^i\sigma \cdot \delta^j &= \delta^i \cdot \sigma\delta^j\sigma^{-1}\sigma = \delta^i \cdot \delta^{-j}\sigma = \delta^{(i-j) \bmod n}\sigma, \\
\delta^i\sigma \cdot \delta^j\sigma &= \delta^i\sigma\delta^j\sigma^{-1} = \delta^i\delta^{-j} = \delta^{(i-j) \bmod n}, \\
(\delta^i)^{-1} &= \delta^{-i} = \delta^{(-i) \bmod n}, \\
(\delta^i\sigma)^{-1} &= \sigma^{-1}\delta^{-i} = \sigma\delta^{-i}\sigma^{-1}\sigma = \delta^i\sigma.
\end{aligned}$$

(2) Die Formeln in (1) zeigen, dass

$$\{\delta^i : 0 \leq i \leq n-1\} \cup \{\delta^i\sigma : 0 \leq i \leq n-1\}$$

abgeschlossen unter Multiplikation und Inversenbildung ist. Da das neutrale Element δ^0 auch in der Menge enthalten ist, ist die Menge eine Untergruppe, und damit

$$G = \langle \delta, \sigma \rangle = \{\delta^i : 0 \leq i \leq n-1\} \cup \{\delta^i\sigma : 0 \leq i \leq n-1\}.$$

Wir müssen noch zeigen, dass die $2n$ Elemente in der Menge paarweise verschieden sind: Für $i, j \in \{0, 1, \ldots, n-1\}$ gilt:

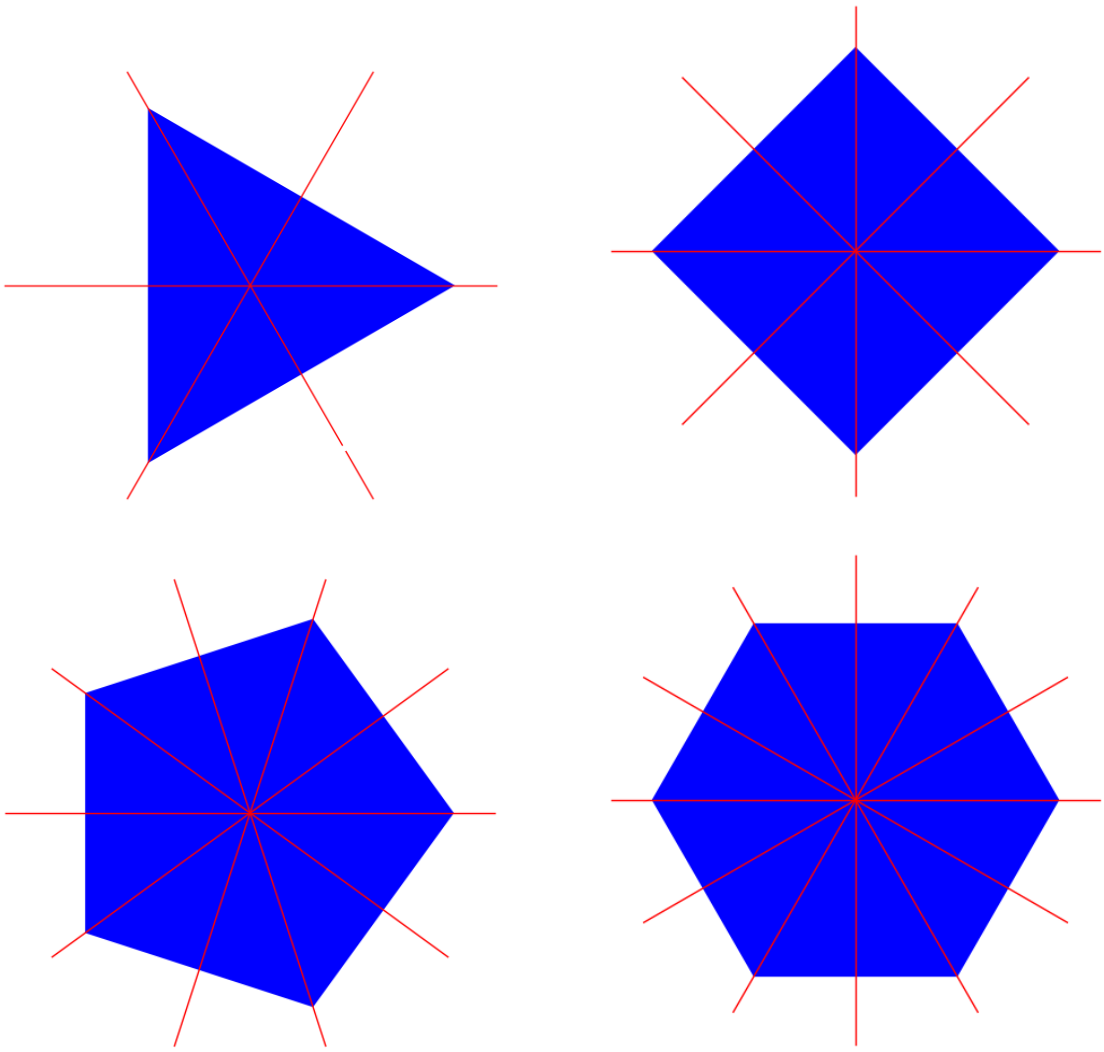
- $\delta^i = \delta^j$ ist wegen $\operatorname{ord}(\delta) = n$ nur für $i = j$ möglich.
- $\delta^i\sigma = \delta^j$ würde $\sigma = \delta^{j-i}$ implizieren, δ würde mit σ kommutieren, und aus $\sigma\delta\sigma^{-1} = \delta^{-1}$ würde $\delta = \delta^{-1}$, also $\delta^2 = 1$, im Widerspruch zu $\operatorname{ord}(\delta) = n \geq 3$.
- $\delta^i\sigma = \delta^j\sigma$ liefert $\delta^i = \delta^j$, also $i = j$ wie eben.

(3) Aus $(\delta^i\sigma)^{-1} = \delta^i\sigma$ und $\delta^i\sigma \neq \delta^0$ folgt $\operatorname{ord}(\delta^i\sigma) = 2$. Weiter gilt

$$(\delta^i\sigma)\delta(\delta^i\sigma)^{-1} = \delta^i\sigma\delta\sigma^{-1}\delta^{-i} = \delta^i\,\delta^{-1}\delta^{-i} = \delta^{-1}.$$

Damit ist alles gezeigt. ■

Bemerkungen: Ist R_n ein regelmäßiges/reguläres n-Eck in der Ebene, d.h. alle n Seiten sind gleich lang und alle n Innenwinkel sind gleich groß, so bilden die Kongruenzabbildungen, die das n-Eck festlassen, eine Gruppe, die aus n Drehungen und n Spiegelungen besteht. Es handelt sich um eine Diedergruppe der Ordnung $2n$.
Die folgenden Bilder zeigen jeweils ein reguläres n-Eck mit den n Spiegelachsen für $n = 3, 4, 5, 6$:



8. Gruppenhomomorphismen - Isomorphe Gruppen

DEFINITION. *Seien $(G, *)$ und $(H, \times)$ zwei Gruppen. Eine Abbildung $\phi : G \to H$ heißt ein* **Gruppenhomomorphismus**, *falls gilt*

$$\phi(a * b) = \phi(a) \times \phi(b) \text{ für alle } a, b \in G.$$

Bemerkungen:

(1) In obiger Definition haben wir die Verknüpfungen in den beiden Gruppen unterschiedlich geschrieben. Dies werden wir im Folgenden meist nicht mehr tun.
(2) Im Folgenden werden wir auch manchmal sagen „Sei $\phi : G \to H$ ein Gruppenhomomorphismus.“ und meinen damit, dass G und H Gruppen sind, und dass $\phi : G \to H$ ein Gruppenhomomorphismus ist.

Beispiele:

(1) Sei K ein Körper (wie $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$). Dann bilden die Menge der Spaltenvektoren K^m und K^n mit der Vektoraddition abelsche Gruppen. Ist nun $A \in \mathrm{Mat}(m \times n, K)$ eine $m \times n$-Matrix, so definiert

$$\phi : K^n \to K^m \text{ mit } \phi(x) = Ax$$

bekanntlich eine lineare Abbildung. Wegen

$$\phi(x+y) = A(x+y) = Ax + Ay = \phi(x) + \phi(y)$$

ist ϕ auch ein Gruppenhomomorphismus.

(2) Für zwei $n \times n$-Matrizen $A, B \in \mathrm{M}_n(K)$ gilt bekanntlich die Produktformel $\det(AB) = \det(A) \cdot \det(B)$. Daher definiert

$$\mathrm{GL}_n(K) \to K^*, \quad A \mapsto \det(A)$$

einen Gruppenhomomorphismus zwischen den Gruppen $(\mathrm{GL}_n(K), \cdot)$ und $(K^*, \cdot)$.

(3) $(\{1, -1\}, \cdot)$ ist eine Gruppe mit zwei Elementen ebenso wie $(\mathbb{Z}_2, +)$. Definieren wir

$$\phi : \mathbb{Z}_2 \to \{1, -1\} \text{ mit } \phi(0) = 1, \phi(1) = -1,$$

so gilt

$$\begin{aligned}
\phi(0+0) &= \phi(0) = 1 = 1 \cdot 1 = \phi(0) \cdot \phi(0), \\
\phi(0+1) &= \phi(1) = -1 = 1 \cdot (-1) = \phi(0) \cdot \phi(1), \\
\phi(1+0) &= \phi(1) = -1 = (-1) \cdot 1 = \phi(1) \cdot \phi(0), \\
\phi(1+1) &= \phi(0) = 1 = (-1) \cdot (-1) = \phi(1) \cdot \phi(1).
\end{aligned}$$

Daher ist ϕ ein Gruppenhomomorphismus. (Da ϕ auch bijektiv ist, ist ϕ sogar ein sogenannter Gruppenisomorphismus.)

(4) Das Vorzeichen bei Permutationen ist multiplikativ, d.h.

$$\mathrm{sgn}(\sigma\tau) = \mathrm{sgn}(\sigma)\mathrm{sgn}(\tau) \text{ für alle } \sigma, \tau \in S_n.$$

Daher ist

$$(S_n, \circ) \to (\{1, -1\}, \cdot), \quad \sigma \mapsto \mathrm{sgn}(\sigma)$$

ein Gruppenhomomorphismus.

(5) Ist G eine multiplikativ geschriebene Gruppe und $g \in G$, so gilt bekanntlich nach den Potenzrechenregeln für $m, n \in \mathbb{Z}$

$$g^{m+n} = g^m \cdot g^n.$$

Definieren wir

$$\phi : \mathbb{Z} \to G, \quad \phi(m) = g^m,$$

so gilt

$$\phi(m+n) = g^{m+n} = g^m \cdot g^n = \phi(m)\phi(n),$$

also ist ϕ ein Gruppenhomomorphismus von der additiven Gruppe $(\mathbb{Z}, +)$ in G.

(6) Ist G eine Gruppe und H eine Untergruppe von G, definiert man

$$\phi : H \to G, \quad x \mapsto x,$$

so ist ϕ trivialerweise ein Gruppenhomomorphismus.

(7) Sind $m, n \in \mathbb{N}$ mit $n \mid m$, so ist

$$\phi : \mathbb{Z}_m \to \mathbb{Z}_n, \quad x \mapsto x \bmod n$$

ein Gruppenhomomorphismus zwischen den additiven Gruppen $(\mathbb{Z}_m, +_{\bmod m})$ und $(\mathbb{Z}_n, +_{\bmod n})$, denn für $x, y \in \mathbb{Z}_m$ gilt (unter Benutzung der Regel $x \bmod m = (x+km) \bmod m$ für alle $x, k \in \mathbb{Z}$)

$$\begin{aligned}
\phi(x +_{\bmod m} y) &= \varphi((x+y) \bmod m) = \big((x+y) \bmod m\big) \bmod n = \\
&= \big(x+y - \left\lfloor \frac{x+y}{m} \right\rfloor m\big) \bmod n \overset{n|m}{=} (x+y) \bmod n, \\
\phi(x) +_{\bmod n} \phi(y) &= (x \bmod n) +_{\bmod n} (y \bmod n) = \\
&= \big((x \bmod n) + (y \bmod n)\big) \bmod n = \\
&= \big(x - \left\lfloor \frac{x}{n} \right\rfloor n + y - \left\lfloor \frac{y}{n} \right\rfloor n\big) \bmod n = \\
&= (x+y) \bmod n,
\end{aligned}$$

also

$$\phi(x +_{\bmod m} y) = \phi(x) +_{\bmod n} \phi(y).$$

(8) Obwohl

$$\phi : \mathbb{Z}_2 \to \mathbb{Z}_4, \quad x \mapsto x$$

wohldefiniert ist, ist ϕ kein Gruppenhomomorphismus, denn

$$\phi(1 +_{\bmod 2} 1) = \phi(0) = 0, \text{ während } \phi(1) +_{\bmod 4} \phi(1) = 1 +_{\bmod 4} 1 = 2 \neq 0.$$

LEMMA. *Seien $(G, *)$, $(H, \times)$ Gruppen und $\phi : G \to H$ ein Gruppenhomomorphismus. Dann gilt:*

(1) *Das neutrale Element e_G von G wird auf das neutrale Element e_H von H abgebildet:*

$$\phi(e_G) = e_H.$$

(2) *Ist $b \in G$ das zu $a \in G$ inverse Element, so ist $\phi(b)$ das zu $\phi(a)$ inverse Element. Kurz:*

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

(Dabei steht $\phi(a)^{-1}$ für $(\phi(a))^{-1}$.)

Beweis:

(1) Es gilt:

$$e_H \times \phi(e_G) = \phi(e_G) = \phi(e_G * e_G) = \phi(e_G) \times \phi(e_G),$$

woraus durch Multiplikation mit $\phi(e_G)^{-1}$ von rechts sofort $e_H = \phi(e_G)$ folgt.

(2) Mit den Bezeichnungen aus (1) gilt $a*b = b*a = e_G$, woraus sofort $\phi(a)\times\phi(b) = \phi(b)\times\phi(a) = e_H$, und damit die Behauptung folgt. ■

FOLGERUNG. *Ist $\phi : G \to H$ ein Gruppenhomomorphismus, so gilt für alle $g \in G$ und alle $n \in \mathbb{Z}$*

$$\phi(g^n) = \phi(g)^n.$$

Beweis: Wir unterscheiden die Fälle $n \geq 1$, $n = 0$ und $n \geq -1$.

- Für $n \geq 1$ folgt dies durch Induktion:
$$\phi(g^{n+1}) = \phi(g^n \cdot g) = \phi(g^n) \cdot \phi(g) = \phi(g)^n \cdot \phi(g) = \phi(g)^{n+1}.$$
- Für $n = 0$ haben wir dies im vorangegangenen Lemma gezeigt:
$$\phi(g^0) = \phi(e_G) = e_H = \phi(g)^0.$$
- Für $n \geq -1$ schreiben wir $n = -m$ und erhalten mit dem vorangegangenen Lemma und dem ersten Teil
$$\phi(g^n) = \phi(g^{-m}) = \phi((g^{-1})^m) = \phi(g^{-1})^m = (\phi(g)^{-1})^m = \phi(g)^{-m} = \phi(g)^n.$$

Damit ist alles gezeigt. ■

FOLGERUNG. *Ist $\phi : G \to H$ ein Gruppenhomomorphismus, ist $g \in G$ von endlicher Ordnung, so hat auch $\phi(g)$ endliche Ordnung und es gilt*

$$\operatorname{ord}(\phi(g)) \mid \operatorname{ord}(g).$$

Beweis: Aus

$$\phi(g)^{\mathrm{ord}\,(g)} = \phi(g^{\mathrm{ord}\,(g)}) = \phi(e_G) = e_H$$

folgt mit den Eigenschaften der Ordnung

$$\mathrm{ord}\,(\phi(g)) \mid \mathrm{ord}\,(g),$$

was wir zeigen wollten. ■

DEFINITION. *Ist $\phi : G \to H$ ein Gruppenhomomorphismus (und e_H das neutrale Element von H), so wird der* **Kern von** ϕ *definiert durch*

$$\mathrm{Kern}(\phi) = \{g \in G : \phi(g) = e_H\}$$

und das **Bild von** ϕ *durch*

$$\mathrm{Bild}(\phi) = \{\phi(g) : g \in G\} = \phi(G).$$

LEMMA. *Für einen Gruppenhomomorphismus $\phi : G \to H$ ist* $\mathrm{Kern}(\phi)$ *eine Untergruppe von G und* $\mathrm{Bild}(\phi)$ *eine Untergruppe von H.*

Beweis:

(1) Wir überprüfen die Untergruppeneigenschaften:
- Sind $a, b \in \mathrm{Kern}(\phi)$, so gilt $\phi(a) = \phi(b) = e_H$ und damit
$$\phi(ab) = \phi(a)\phi(b) = e_H e_H = e_H, \text{ also } ab \in \mathrm{Kern}(\phi).$$
$\mathrm{Kern}(\phi)$ ist also abgeschlossen unter der Verknüpfung.
- Ist $a \in \mathrm{Kern}(\phi)$, so gilt
$$\phi(a^{-1}) = \phi(a)^{-1} = e_H^{-1} = e_H, \text{ also } a^{-1} \in \mathrm{Kern}(\phi).$$
- Aus $\phi(e_G) = e_H$ folgt sofort $e_G \in \mathrm{Kern}(\phi)$.

Daher ist $\mathrm{Kern}(\phi)$ eine Untergruppe von G.

(2) Wir überprüfen die Untergruppeneigenschaften für $\mathrm{Bild}(\phi)$:
- Sind $\widetilde{a}, \widetilde{b} \in \mathrm{Bild}(\phi)$, so gibt es $a, b \in G$ mit $\widetilde{a} = \phi(a)$ und $\widetilde{b} = \phi(b)$. Es folgt
$$\widetilde{a} \cdot \widetilde{b} = \phi(a) \cdot \phi(b) = \phi(ab) \in \mathrm{Bild}(\phi),$$
also ist $\mathrm{Bild}(\phi)$ abgeschlossen unter der Verknüpfung.
- Ist $\widetilde{a} \in \mathrm{Bild}(\phi)$, so gibt es ein $a \in G$ mit $\widetilde{a} = \phi(a)$. Es folgt
$$\widetilde{a}^{-1} = \varphi(a)^{-1} = \varphi(a^{-1}) \in \mathrm{Bild}(\phi).$$
- Weiter gilt
$$e_H = \varphi(e_G) \in \mathrm{Bild}(\phi).$$

Alle Untergruppeneigenschaften sind erfüllt, also ist $\mathrm{Bild}(\phi)$ eine Untergruppe von H. ■

Beispiele:

(1) Für einen Körper K und $n \in \mathbb{N}$ definiert
$$\det : \mathrm{GL}_n(K) \to K^*$$
einen Gruppenhomomorphismus zwischen den multiplikativen Gruppen $\mathrm{GL}_n(K)$ und K^*. Da 1 das neutrale Element in K^* ist, die Matrizen mit Determinante 1 aber gerade die Elemente von $\mathrm{SL}_n(K)$ sind, gilt
$$\mathrm{Kern}(\det) = \mathrm{SL}_n(K).$$
Natürlich ist det surjektiv, also
$$\mathrm{Bild}(\det) = K^*.$$

(2) Das Vorzeichen definiert einen Gruppenhomomorphismus

$$\mathrm{sgn} : S_n \to \{\pm 1\}.$$

Der Kern sind die Permutationen mit Vorzeichen 1, also

$$A_n = \mathrm{Kern}(\mathrm{sgn}(\sigma)).$$

(3) Ist G eine multiplikativ geschriebene Gruppe und $g \in G$, so ist

$$\phi : \mathbb{Z} \to G, \quad n \mapsto g^n$$

ein Gruppenhomomorphismus. Dann ist

$$\mathrm{Bild}(\phi) = \{g^n : n \in \mathbb{Z}\} = \langle g \rangle.$$

Der Kern ist

$$\mathrm{Kern}(\phi) = \begin{cases} \{0\}, & \text{falls ord}\,(g) = \infty, \\ \mathbb{Z}\,\mathrm{ord}\,(g), & \text{falls ord}\,(g) < \infty. \end{cases}$$

LEMMA. *Für einen Gruppenhomomorphismus $\phi : G \to H$ gilt:*

$$\phi \text{ injektiv} \quad \Longleftrightarrow \quad \mathrm{Kern}(\phi) = \{e_G\},$$

wobei e_G das neutrale Element von G bezeichnet.

Beweis: Ist ϕ injektiv, so wird natürlich nur e_G auf e_H abgebildet, d.h. $\mathrm{Kern}(\phi) = \{e_G\}$. Gilt nun umgekehrt $\mathrm{Kern}(\phi) = \{e_G\}$, so folgt für beliebige $a, b \in G$:

$$\begin{aligned} \phi(a) = \phi(b) &\iff \phi(a)\phi(b)^{-1} = e_H \iff \phi(a)\phi(b^{-1}) = e_H \iff \phi(ab^{-1}) = e_H \iff \\ &\iff ab^{-1} \in \mathrm{Kern}(\phi) = \{e_G\} \iff ab^{-1} = e_G \iff a = b. \end{aligned}$$

Also ist ϕ injektiv. ■

SATZ. *Sei $\phi : G \to H$ ein Gruppenhomomorphismus. Die den Kern von ϕ enthaltenden Untergruppen von G stehen dann in Bijektion zu den Untergruppen von* $\mathrm{Bild}(\phi)$*:*

$$\begin{aligned} \{U \text{ Untergruppe von } G \text{ mit } \mathrm{Kern}(\phi) \subseteq U \subseteq G\} &\leftrightarrow \{V \text{ Untergruppe von } H \text{ mit } V \subseteq \mathrm{Bild}(\phi)\} \\ U &\mapsto \phi(U) \\ \phi^{-1}(V) &\leftarrow V \end{aligned}$$

$$\begin{array}{ccccccccc} \{e_G\} & \overset{\subseteq}{\longrightarrow} & \mathrm{Kern}(\phi) & \overset{\subseteq}{\longrightarrow} & U & \overset{\subseteq}{\longrightarrow} & \phi^{-1}(V) & \overset{\subseteq}{\longrightarrow} & G \\ & & \downarrow & & \downarrow & & \updownarrow & & \downarrow \\ & & \{e_H\} & \overset{\subseteq}{\longrightarrow} & \phi(U) & \overset{\subseteq}{\longrightarrow} & V & \overset{\subseteq}{\longrightarrow} & \mathrm{Bild}(\phi) \overset{\subseteq}{\longrightarrow} H \end{array}$$

Beweis:

(1) Wir wissen bereits: Ist U eine Untergruppe von G, so ist $\phi(U)$ eine Untergruppe von H, also natürlich auch eine Untergruppe von $\phi(G) = \mathrm{Bild}(\phi)$.

(2) Sei V eine (beliebige) Untergruppe von H. Wir zeigen, dass $\phi^{-1}(V) = \{x \in G : \phi(x) \in V\}$ eine Untergruppe von G ist. Sind $x, y \in \phi^{-1}(V)$, so gilt $\phi(x), \phi(y) \in V$, also $\phi(xy) = \phi(x)\phi(y) \in V$, und damit $xy \in \phi^{-1}(V)$. Ist $x \in \phi^{-1}(V)$, so gilt $\phi(x) \in V$, und damit auch $\phi(x^{-1}) = \phi(x)^{-1} \in V$, also $x^{-1} \in \phi^{-1}(V)$. Natürlich gilt auch $\phi(e_G) = e_H \in V$, also $e_G \in \phi^{-1}(V)$.

(3) Ist V eine Untergruppe von V, so gilt für $x \in \mathrm{Kern}(\phi)$ zunächst $\phi(x) = e_H \in V$, also $x \in \phi^{-1}(V)$, insgesamt also $\mathrm{Kern}(\phi) \subseteq \phi^{-1}(V)$.

(4) Sei U eine Untergruppe von G mit $\mathrm{Kern}(\phi) \subseteq U \subseteq G$. Dann zeigen wir:

$$\phi^{-1}(\phi(U)) = U.$$

- $\subseteq$ Sei $x \in \phi^{-1}(\phi(U))$. Dann ist $\phi(x) \in \phi(U)$, es gibt also ein $u \in U$ mit $\phi(x) = \phi(u)$. Dies impliziert $\phi(xu^{-1}) = \phi(x)\phi(u)^{-1} = e_H$, also $xu^{-1} \in \mathrm{Kern}(\phi)$. Da nach Voraussetzung $\mathrm{Kern}(\phi) \subseteq U$ gilt, folgt $xu^{-1} \in U$, und damit $x \in U$. Dies beweist $\phi^{-1}(\phi(U)) \subseteq U$.

- $\supseteq$ Sei $u \in U$. Dann ist $\phi(u) \in \phi(U)$, und damit $u \in \phi^{-1}(\phi(U))$. Dies beweist $U \subseteq \phi^{-1}(\phi(U))$.

(5) Sei V eine Untergruppe von H mit $V \subseteq \phi(G)$. Wir wollen zeigen, dass gilt

$$\phi(\phi^{-1}(V)) = V.$$

- $\subseteq$ Sei $y \in \phi(\phi^{-1}(V))$. Dann existiert ein $x \in \phi^{-1}(V)$ mit $y = \phi(x)$. Dann ist $\phi(x) \in V$, es existiert also ein $v \in V$ mit $\phi(x) = v$. Dann ist aber $y = \phi(x) = v \in V$. Dies zeigt $\phi(\phi^{-1}(V)) \subseteq V$.
- $\supseteq$ Sei $v \in V$. Wegen $V \subseteq \text{Bild}(\phi)$ existiert ein $x \in G$ mit $v = \phi(x)$. Dann ist $x \in \phi^{-1}(V)$, und damit $v = \phi(x) \in \phi(\phi^{-1}(V))$. Dies zeigt $V \subseteq \phi(\phi^{-1}(V))$.

Damit haben wir nachgewiesen, dass die angegebenen Abbildungen invers zueinander sind. Es folgt die Behauptung. ■

LEMMA. *Sind $\alpha : G_1 \to G_2$ und $\beta : G_2 \to G_3$ Gruppenhomomorphismen, so ist auch die Komposition $\beta \circ \alpha : G_1 \to G_3$ ein Gruppenhomomorphismus.*

Beweis: Für $a, b \in G_1$ gilt

$$(\beta \circ \alpha)(ab) = \beta(\alpha(ab)) = \beta(\alpha(a)\alpha(b)) = \beta(\alpha(a))\beta(\alpha(b)) = (\beta \circ \alpha)(a)(\beta \circ (\alpha)(b),$$

was die Behauptung zeigt. ■

LEMMA. *Ist $\phi : G \to H$ ein bijektiver Gruppenhomomorphismus, so ist auch $\phi^{-1} : H \to G$ ein Gruppenhomomorphismus.*

Beweis: Seien $\widetilde{a}, \widetilde{b} \in H$ und $a = \phi^{-1}(\widetilde{a})$, $b = \phi^{-1}(\widetilde{b})$. Dann folgt

$$\phi^{-1}(\widetilde{a} \cdot \widetilde{b}) = \phi^{-1}(\phi(a) \cdot \phi(b)) = \phi^{-1}(\phi(ab)) = ab = \phi^{-1}(\widetilde{a})\phi^{-1}(\widetilde{b}),$$

was beweist, dass ϕ^{-1} ein Gruppenhomomorphismus ist. ■

DEFINITION. *Seien G und H Gruppen.*

(1) *Ein* **Gruppenisomorphismus** *$\phi : G \to H$ ist ein bijektiver Gruppenhomomorphismus. (Dann ist auch $\phi^{-1} : H \to G$ ein Gruppenisomorphismus.) Man spricht auch kurz von einem* **Isomorphismus**.
(2) *Die Gruppen G und H heißen* **isomorph**, *wenn es einen Gruppenisomorphismus $\phi : G \to H$ gibt. Man schreibt dann auch $G \simeq H$.*
(3) *Im Fall $H = G$ nennt man einen Gruppenisomorphismus $\phi : G \to G$ einen* **Automorphismus** *der Gruppe G.*
(4) *Die Menge der Automorphismen einer Gruppe G bildet mit der Verknüpfung $\circ$ eine Gruppe, so sogenannte* **Automorphismengruppe** $\text{Aut}(G)$.

Bemerkungen:

(1) Dass Gruppen G und H isomorph sind, bedeutet, dass H aus G einfach durch „Umbenennung“ der Elemente und der Verknüpfung entsteht. Gruppentheoretisch definierte Eigenschaften bleiben dann natürlich erhalten, beispielsweise die Ordnung von Elementen.
(2) Die Isomorphie von Gruppen ist natürlich eine Äquivalenzrelation.
(3) Eine wichtige Aufgabe der Gruppentheorie ist die Klassifikation der Gruppen bis auf Isomorphie.

Beispiele:

(1) Wir hatten zuvor die Gruppen $(\{1, -1\}, \cdot)$ und $(\mathbb{Z}_2, +)$ betrachtet und gezeigt, dass

$$\phi : \mathbb{Z}_2 \to \{1, -1\} \text{ mit } \phi(0) = 1, \phi(1) = -1$$

ein Gruppenhomomorphismus ist. Da ϕ offensichtlich bijektiv ist, ist ϕ ein Gruppenisomorphismus, die Gruppen $(\mathbb{Z}_2, +)$ und $(\{\pm 1\}, \cdot)$ sind also isomorph.
(2) Das folgende Beispiel aus der Analysis setzt Kenntnisse der Exponential-Funktion und der Logarithmus-Funktion voraus.

- $(\mathbb{R}_{>0}, \cdot)$ ist eine Untergruppe von $(\mathbb{R}^*, \cdot)$. Die Abbildung
$$\phi : (\mathbb{R}, +) \to (\mathbb{R}_{>0}, \cdot) \text{ mit } \phi(x) = e^x$$
ist ein Gruppenhomomorphismus, da
$$e^{x+y} = e^x \cdot e^y$$
gilt.
- Die Abbildung
$$\psi : (\mathbb{R}_{>0}, \cdot) \to (\mathbb{R}, +) \text{ mit } \psi(x) = \ln(x)$$
ist ein Gruppenhomomorphismus, da
$$\ln(xy) = \ln(x) + \ln(y)$$
gilt.
- Für $x \in \mathbb{R}$ gilt $\psi(\phi(x)) = \ln(e^x) = x$ und für $x \in \mathbb{R}_{>0}$ gilt $\phi(\psi(x)) = \ln(e^x) = x$. Deswegen sind ϕ und ψ zueinander inverse Abbildungen. Also sind ϕ und ψ Gruppenisomorphismen. Insbesondere sind die Gruppen $(\mathbb{R}, +)$ und $(\mathbb{R}_{>0}, \cdot)$ isomorph.

Bemerkung: Ist $\phi : G \to H$ ein injektiver Gruppenhomomorphismus, so ist die Einschränkung
$$\phi : G \to \text{Bild}(G) \subseteq G$$
ein Isomorphismus. G ist also isomorph zur Untergruppe Bild(ϕ) von G. Man nennt ein solches ϕ dann auch eine **Einbettung** und schreibt
$$\phi : G \hookrightarrow H.$$

LEMMA. *Sei G eine zyklische Gruppe und $g \in G$ mit $G = \langle g \rangle$.*

(1) *Hat G unendliche Ordnung, also* $\text{ord}\,(g) = \infty$*, so ist*
$$\phi : (\mathbb{Z}, +) \to (G, \cdot), \quad a \mapsto g^a$$
ein Gruppenisomorphismus.

(2) *Hat G endliche Ordnung n, also* $\text{ord}\,(g) = n$*, so ist*
$$\phi : (\mathbb{Z}_n, +_{\bmod n}) \to (G, \cdot), \quad a \mapsto g^a$$
ein Gruppenisomorphismus.

Beweis:

(1) $\text{ord}\,(g) = \infty$: Bei den Eigenschaften der Ordnung haben wir gesehen, dass ϕ injektiv, und damit natürlich auch bijektiv ist. Die Potenzrechenregeln zeigen, dass ϕ ein Gruppenhomomorphismus ist. Also ist ϕ ein Isomorphismus.

(2) $\text{ord}\,(g) = n < \infty$: Nach den Eigenschaften, die wir für zyklische Gruppen gezeigt haben, ist ϕ bijektiv. Wir müssen noch zeigen, dass ϕ ein Gruppenhomomorphismus ist. Seien also $a, b \in \mathbb{Z}_n = \{0, 1, \ldots, n-1\}$. Dann ist
$$a +_{\bmod n} b = (a + b) \bmod n = a + b - \left\lfloor \frac{a+b}{n} \right\rfloor n.$$
Mit $g^n = e_G$ folgt
$$\phi(a +_{\bmod n} b) = \phi(a + b - \left\lfloor \frac{a+b}{n} \right\rfloor n) = g^{a+b-\lfloor \frac{a+b}{n} \rfloor n} = g^{a+b} = g^a \cdot g^b = \phi(a) \cdot \phi(b).$$
ϕ ist also ein Gruppenhomomorphismus und damit ein Gruppenisomorphismus. ■

Als direkte Folgerung erhalten wir:

FOLGERUNG. *Alle zyklischen Gruppen einer gegebenen Ordnung sind isomorph.*

Wir haben gesehen, dass jede Gruppe von Primzahlordnung p zyklisch ist. Damit erhalten wir:

FOLGERUNG. *Sei p eine Primzahl. Bis auf Isomorphie gibt es genau eine Gruppe der Ordnung p, nämlich $(\mathbb{Z}_p, +_{\bmod p})$.*

SATZ. *Sei G eine (multiplikativ geschriebene) Gruppe mit neutralem Element e und H, K Untergruppen von G mit der Eigenschaft*

$$H \cap K = \{e\}, \quad HK = \{xy : x \in H, y \in K\} = G \quad \text{und} \quad xy = yx \text{ für alle } x \in H, y \in K.$$

Dann ist

$$\phi : H \times K \to G, \quad (x, y) \mapsto xy$$

ein Isomorphismus.

Beweis: Wir überprüfen die Kriterien dafür, dass ϕ ein Gruppenisomorphismus ist:

- Warum ist ϕ ein Gruppenhomomorphismus? Mit $x_2y_1 = y_1x_2$ gilt:
$$\begin{aligned}\phi((x_1, y_1)(x_2, y_2)) &= \phi((x_1x_2, y_1y_2)) = x_1x_2y_1y_2 = x_1(x_2y_1)y_2 = x_1(y_1x_2)y_2 = \\ &= (x_1y_1)(x_2y_2) = \phi((x_1, y_1))\phi((x_2, y_2)).\end{aligned}$$
Dies zeigt, dass ϕ ein Gruppenhomomorphismus ist.
- Die Voraussetzung $G = \{xy : x \in H, y \in K\}$ besagt gerade, dass ϕ surjektiv ist.
- Zur Injektivität bestimmen wir den Kern von ϕ:
$$\begin{aligned}(x, y) \in \operatorname{Kern}(\phi) &\iff \phi((x, y)) = e \iff xy = e \iff \\ &\iff y = x^{-1} \iff y = x^{-1} \in H \cap K = \{e\} \iff \\ &\iff y = x^{-1} = e \iff (x, y) = (e, e).\end{aligned}$$
Also ist $\operatorname{Kern}(\phi) = \{(e, e)\}$, weswegen ϕ injektiv ist.

Damit haben wir bewiesen, dass ϕ ein Gruppenisomorphismus ist. ■

Wann ist das Produkt (endlicher) zyklischer Gruppen wieder zyklisch? Der folgende Satz gibt eine Charakterisierung an:

SATZ. *Seien G und H endliche zyklische Gruppen. Dann gilt:*

$$G \times H \text{ ist eine zyklische Gruppe} \iff \operatorname{ggT}(|G|, |H|) = 1.$$

Genauer: Sei $G = \langle g \rangle$ und $H = \langle h \rangle$. Dann gilt:

(1) *In $G \times H$ gilt*
$$\operatorname{ord}((g, h)) = \operatorname{kgV}(|G|, |H|).$$
(2) *Ist $\operatorname{ggT}(|G|, |H|) = 1$, so ist*
$$G = \langle (g, h) \rangle,$$
d.h. (g, h) erzeugt die Gruppe $G \times H$, die also zyklisch ist. Für alle $x, y \in \mathbb{Z}$ gibt es also ein $z \in \mathbb{Z}$ mit
$$(g^x, h^y) = (g, h)^z.$$
Bestimmt man mit dem erweiterten euklidischen Algorithmus $u, v \in \mathbb{Z}$ mit $u|G| + v|H| = 1$, so kann man $z = v|H|x + u|G|y$ wählen, also
$$(g^x, h^y) = (g, h)^{v|H|x + u|G|y}.$$

Beweis: Wir schreiben die Gruppen multiplikativ, die neutralen Elemente als e_G und e_H.

(1) Für $k \in \mathbb{N}$ gilt:
$$\begin{aligned}\operatorname{ord}((g, h)) \mid k &\iff (g, h)^k = (e_G, e_H) \iff (g^k, h^k) = (e_G, e_H) \iff \\ &\iff g^k = e_G \text{ und } h^k = e_H \iff \operatorname{ord}(g) \mid k \text{ und } \operatorname{ord}(h) \mid k \iff \\ &\iff \operatorname{kgV}(\operatorname{ord}(g), \operatorname{ord}(h)) \mid k \iff \operatorname{kgV}(|G|, |H|) \mid k.\end{aligned}$$
Da die natürlichen Zahlen $\operatorname{ord}((g, h))$ und $\operatorname{kgV}(|G|, |H|)$ die gleichen Vielfachen haben, sind sie gleich:
$$\operatorname{ord}((g, h)) = \operatorname{kgV}(|G|, |H|),$$

wie behauptet.

(2) Im Fall $\mathrm{ggT}(|G|,|H|)=1$ folgt aus (1)

$$\mathrm{ord}\,((g,h)) = \mathrm{kgV}(|G|,|H|) = |G|\cdot|H| = |G\times H|,$$

woraus sich sofort

$$G\times H = \langle (g,h)\rangle$$

ergibt. Also ist $G\times H$ zyklisch und (g,h) ein erzeugendes Element.
Wir beweisen die letzte Gleichung in (2):

$$\begin{aligned}(g,h)^{v|H|x+u|G|y} &= (g^{v|H|x+u|G|y}, h^{v|H|x+u|G|y}) = (g^{(1-u|G|)x+u|G|y}, h^{v|H|x+(1-v|H|)y}) = \\ &= (g^x\cdot(g^{-ux+uy})^{|G|}, h^y\cdot(h^{vx-vy})^{|H|}) = (g^x,h^y).\end{aligned}$$

(3) Wir müssen noch zeigen, dass im Fall $\mathrm{ggT}(|G|,|H|)>1$ die Gruppe $G\times H$ nicht zyklisch ist. Wir geben dafür zwei Beweise an.

- *1. Beweis:* Angenommen, $G\times H$ wäre zyklisch. Dann gäbe es $a,b\in\mathbb{Z}$, sodass (g^a,h^b) die Gruppe erzeugt. Es gäbe also $x,y\in\mathbb{Z}$ mit

  $$(g^a,h^b)^x = (g,e_H) \quad \text{und} \quad (g^a,h^b)^y = (e_G,h).$$

  Betrachtung der Komponenten liefert die vier Gleichungen

  $$g^{ax}=g,\quad h^{bx}=e_H,\quad g^{ay}=e_G,\quad h^{by}=h$$

  beziehungsweise

  $$g^{ax-1}=e_G,\quad h^{bx}=e_H,\quad g^{ay}=e_G,\quad h^{by-1}=e_H.$$

  Diese Gleichungen sind wegen $|G|=\mathrm{ord}\,(g)$ und $|H|=\mathrm{ord}\,(h)$ gleichwertig mit

  $$|G|\mid ax-1,\quad |H|\mid bx,\quad |G|\mid ay,\quad |H|\mid by-1.$$

  Sei p ein Primteiler von $\mathrm{ggT}(|G|,|H|)$. Dann folgt

  $$p\mid ax-1,\quad p\mid bx,\quad p\mid ay,\quad p\mid by-1.$$

  Aus der ersten und letzten Beziehung folgt

  $$p\nmid a,\quad p\nmid x,\quad p\nmid b,\quad p\nmid y.$$

  Dies ist aber ein Widerspruch zu $p\mid bx$ und $p\mid ay$. Also können x und y mit den angegebenen Eigenschaften nicht existieren. Die Annahme war falsch, also ist $G\times H$ nicht zyklisch.
- *2. Beweis:* Sei $d=\mathrm{ggT}(|G|,|H|)>1$. Die Gleichung

  $$x^d = e_{G\times H}$$

  hat in $G\times H$ die d^2 Lösungen

  $$(g^{\frac{|G|}{d}\cdot i}, h^{\frac{|H|}{d}\cdot j}),\quad i=0,\dots,d-1,\quad j=0,\dots,d-1.$$

  Wäre $G\times H$ zyklisch, so hätte die Gleichung $x^d=e_{G\times H}$ aber nur d Lösungen. Also kann $G\times H$ nicht zyklisch sein. ■

Der erste Teil des folgendes Satzes ist eine konkrete additive Variante des vorangegangenen Satzes:

Satz. *Seien $m,n\in\mathbb{N}$ mit $\mathrm{ggT}(m,n)=1$ und $u,v\in\mathbb{Z}$ mit $um+vn=1$.*

(1) *Durch*

$$\alpha:\mathbb{Z}_{mn}\to\mathbb{Z}_m\times\mathbb{Z}_n,\quad x\mapsto(x \bmod m, x \bmod n)$$

und

$$\beta:\mathbb{Z}_m\times\mathbb{Z}_n\to\mathbb{Z}_{mn},\quad (y,z)\mapsto (yvn+zum) \bmod mn$$

werden zueinander inverse Gruppenisomorphismen definiert. Insbesondere gilt

$$(\mathbb{Z}_{mn},+_{\bmod mn}) \simeq (\mathbb{Z}_m,+_{\bmod m})\times(\mathbb{Z}_n,+_{\bmod n}).$$

(2) *Durch*

$$\gamma : \mathbb{Z}_{mn}^* \to \mathbb{Z}_m^* \times \mathbb{Z}_n^*, \quad x \mapsto (x \bmod m, x \bmod n)$$

und

$$\delta : \mathbb{Z}_m^* \times \mathbb{Z}_n^* \to \mathbb{Z}_{mn}^*, \quad (y,z) \mapsto (yvn + zum) \bmod mn$$

werden zueinander inverse Gruppenisomorphismen definiert. Insbesondere gilt

$$(\mathbb{Z}_{mn}^*, \cdot \bmod mn) \simeq (\mathbb{Z}_m^*, \cdot \bmod m) \times (\mathbb{Z}_n^*, \cdot \bmod n).$$

Beweis:

- Wir bemerken, dass aus $(x + km) \bmod m = x \bmod m$ sofort
$$(x \bmod mn) \bmod m = (x - \Big\lfloor \frac{x}{mn} \Big\rfloor mn) \bmod m = x \bmod m$$
folgt.
- Natürlich sind α und β wohldefiniert. Wir betrachten $\alpha \circ \beta$ und $\beta \circ \alpha$. Für $(y,z) \in \mathbb{Z}_m \times \mathbb{Z}_n$ gilt:
$$\begin{aligned}
(\alpha \circ \beta)((y,z)) &= \alpha(\beta((y,z))) = \alpha\big((yvn + zum) \bmod mn\big) = \\
&= \big(((yvn + zum) \bmod mn) \bmod m, ((yvn + zum) \bmod mn) \bmod n\big) = \\
&= \big((yvn + zum) \bmod m, (yvn + zum) \bmod n\big) = \\
&= \big((yvn) \bmod m, (zum) \bmod n\big) = \\
&= \big(y(1 - um) \bmod m, z(1 - vn) \bmod n\big) = \big(y \bmod m, z \bmod n\big) = \\
&= (y,z).
\end{aligned}$$
Für $x \in \mathbb{Z}_{mn}$ gilt:
$$\begin{aligned}
(\beta \circ \alpha)(x) &= \beta(\alpha(x)) = \beta(\big(x \bmod m, x \bmod n\big)) = \\
&= \big((x \bmod m)vn + (x \bmod n)um\big) \bmod mn = \\
&= \big((x - \Big\lfloor \frac{x}{m} \Big\rfloor m)vn + (x - \Big\lfloor \frac{x}{n} \Big\rfloor n)um\big) \bmod mn = \\
&= \big(xvn + xum\big) \bmod mn = \big(x(um + vn)\big) \bmod mn = \\
&= x \bmod mn = x.
\end{aligned}$$
Damit haben wir bewiesen, dass α und β zueinander invers sind.
- Wir zeigen, dass α ein Gruppenhomomorphismus ist. Seien $x, y \in \mathbb{Z}_{mn}$:
$$\begin{aligned}
\alpha(x +_{\bmod mn} y) &= \alpha((x+y) \bmod mn) = \\
&= (((x+y) \bmod mn) \bmod m, ((x+y) \bmod mn) \bmod n) = \\
&= ((x+y) \bmod m, (x+y) \bmod n), \\
\alpha(x) +_{\bmod m,\, \bmod n} \alpha(y) &= (x \bmod m, x \bmod n) +_{\bmod m,\, \bmod n} (y \bmod m, y \bmod n) = \\
&= \big((x \bmod m) +_{\bmod m} (y \bmod m), (x \bmod n) +_{\bmod n} (y \bmod n)\big) = \\
&= ((x - \Big\lfloor \frac{x}{m} \Big\rfloor m + y - \Big\lfloor \frac{y}{m} \Big\rfloor m) \bmod m, (x - \Big\lfloor \frac{x}{n} \Big\rfloor n + y - \Big\lfloor \frac{y}{n} \Big\rfloor n) \bmod n) = \\
&= ((x+y) \bmod m, (x+y) \bmod n),
\end{aligned}$$

Also ist
$$\alpha(x +_{\bmod mn} y) = \alpha(x) +_{\bmod m,\, \bmod n} \alpha(y).$$
Daher ist α ein bijektiver Gruppenhomomorphismus. Also ist auch β ein Gruppenhomomorphismus. Damit sind α, β zueinander inverse Gruppenisomorphismen und Teil (1) des Satzes ist bewiesen.
- Wir zeigen, dass γ wohldefiniert ist. Dazu müssen wir zeigen:
$$\mathrm{ggT}(x, mn) = 1 \quad \Longrightarrow \quad \mathrm{ggT}(x \bmod m, m) = 1 \text{ und } \mathrm{ggT}(x \bmod n, n) = 1.$$
Nun gilt aber für $\mathrm{ggT}(x, mn) = 1$ auch $\mathrm{ggT}(x, m) = 1$, und damit
$$\mathrm{ggT}(x \bmod m, m) = \mathrm{ggT}(x - \Big\lfloor \frac{x}{m} \Big\rfloor m, m) = \mathrm{ggT}(x, m) = 1,$$
und ganz analog für n. Die Abbildung γ ist also wohldefiniert.

- Wir zeigen, dass δ wohldefiniert ist. Seien also $y \in \mathbb{Z}_m^*$, $z \in \mathbb{Z}_n^*$ gegeben, d.h. $y, z \in \mathbb{Z}$, $0 \leq y < m$, $0 \leq z < n$, $\mathrm{ggT}(m, y) = 1$, $\mathrm{ggT}(n, z) = 1$. Natürlich gilt
$$0 \leq (yvn + zum) \bmod mn < mn.$$
Es ist
$$\begin{aligned}
\mathrm{ggT}(m, (yvn + zum) \bmod mn) &= \mathrm{ggT}(m, yvn + zum - \left\lfloor \frac{yvn + zum}{mn} \right\rfloor mn) = \\
&= \mathrm{ggT}(m, yvn) = \mathrm{ggT}(m, y(1 - um)) = \mathrm{ggT}(m, y) = 1, \\
\mathrm{ggT}(n, (yvn + zum) \bmod mn) &= \mathrm{ggT}(n, yvn + zum - \left\lfloor \frac{yvn + zum}{mn} \right\rfloor mn) = \\
&= \mathrm{ggT}(n, zum) = \mathrm{ggT}(n, z(1 - vn)) = \mathrm{ggT}(n, z) = 1,
\end{aligned}$$
woraus
$$\mathrm{ggT}(mn, (yvn + zum) \bmod mn) = 1$$
folgt. Also gilt $(yvn + zum) \bmod mn \in \mathbb{Z}_{mn}^*$, was beweist, dass die Abbildung δ wohldefiniert ist.
- Da γ die Einschränkung von α auf $\mathbb{Z}_{mn}^*$, δ die Einschränkung von β auf $\mathbb{Z}_m^* \times \mathbb{Z}_n^*$ ist, folgt sofort, dass γ und δ invers zueinander sind.
- Wir zeigen, dass γ ein Gruppenhomomorphismus ist. Seien $x, y \in \mathbb{Z}_{mn}^*$.
$$\begin{aligned}
\gamma(x \cdot_{\bmod mn} y) &= \gamma((xy) \bmod mn) = \\
&= ((xy) \bmod m, (xy) \bmod n), \\
\gamma(x) \cdot_{\bmod m,\, \bmod n} \gamma(y) &= (x \bmod m, x \bmod n) \cdot_{\bmod m,\, \bmod n} (y \bmod m, y \bmod n) = \\
&= ((x \bmod m)(y \bmod m) \bmod m, (x \bmod n)(y \bmod n) \bmod n) = \\
&= ((x - \left\lfloor \frac{x}{m} \right\rfloor m)(y - \left\lfloor \frac{y}{m} \right\rfloor m) \bmod m, (x - \left\lfloor \frac{y}{n} \right\rfloor n)(y - \left\lfloor \frac{y}{n} \right\rfloor n) \bmod n) = \\
&= (xy \bmod m, xy \bmod n).
\end{aligned}$$
Dies zeigt, dass gilt
$$\gamma(x \cdot_{\bmod mn} y) = \gamma(x) \cdot_{\bmod m,\, \bmod n} \gamma(y).$$
Also ist γ ein Gruppenhomomorphismus. Weil γ bijektiv ist, ist auch δ ein Gruppenhomomorphismus. Also sind γ und δ zueinander inverse Gruppenisomorphismen. ■

FOLGERUNG. *Jede endliche zyklische Gruppe ist isomorph zu einem Produkt zyklischer Gruppen mit Primzahlpotenzordnung: Ist $n = p_1^{e_1} \dots p_r^{e_r}$, so gilt*
$$\mathbb{Z}_n \simeq \mathbb{Z}_{p_1^{e_1}} \times \cdots \times \mathbb{Z}_{p_r^{e_r}}.$$

Bemerkung: Wir werden sehen, dass sich jede endliche abelsche Gruppe A sich als Produkt von zyklischen Gruppen schreiben lässt. Mit der letzten Folgerung kann man dann A sogar als Produkt von zyklischen Gruppen von Primzahlpotenzordnung schreiben.

FOLGERUNG. *Für $m, n \in \mathbb{N}$ gilt:*
$$\mathrm{ggT}(m, n) = 1 \quad \Longrightarrow \quad \varphi(mn) = \varphi(m)\varphi(n).$$

Beweis: Dies folgt aus dem zweiten Teil des vorangegangenen Satzes durch Bestimmung der Anzahl:
$$\varphi(mn) = |\mathbb{Z}_{mn}^*| = |\mathbb{Z}_m^* \times \mathbb{Z}_n^*| = |\mathbb{Z}_m^*| \cdot |\mathbb{Z}_n^*| = \varphi(m)\varphi(n). \quad ■$$

Wir stellen jetzt die wichtigsten Formeln der Berechnung der Eulerschen φ-Funktion zusammen:

SATZ. *Für die Eulersche φ-Funktion gilt:*

(1) *Sind $m, n \in \mathbb{N}$ so gilt*
$$\mathrm{ggT}(m, n) = 1 \quad \Longrightarrow \quad \varphi(mn) = \varphi(m)\varphi(n).$$

(2) *Ist p eine Primzahl und $e \in \mathbb{N}$ so gilt*

$$\varphi(p) = p - 1 \quad \textit{und} \quad \varphi(p^e) = p^e - p^{e-1} = p^{e-1}(p-1) = p^e(1 - \frac{1}{p}).$$

(3) *Hat $n \in \mathbb{N}$ die Primfaktorzerlegung $n = p_1^{e_1} \dots p_r^{e_r}$ (mit $e_1, \dots, e_r \geq 1$), so gilt*

$$\varphi(n) = p_1^{e_1-1}(p_1 - 1) \dots p_r^{e_r-1}(p_r - 1) = n(1 - \frac{1}{p_1}) \dots (1 - \frac{1}{p_r}) = n \prod_{p|n} (1 - \frac{1}{p}).$$

Beweis: (1) haben wir eben gezeigt, (2) wurde zuvor gezeigt. (3) ergibt sich direkt aus (1) und (2). ■

Ausblick: Wir stellen noch kurz ein paar Aussagen zur Struktur der multiplikativen Gruppen $\mathbb{Z}_n^*$ zusammen. Ist $n = p_1^{e_1} \dots p_r^{e_r}$, so liefert ein zuvor angegebener Satz

$$\mathbb{Z}_n^* \simeq \mathbb{Z}_{p_1^{e_1}}^* \times \dots \times \mathbb{Z}_{p_r^{e_r}}^*.$$

Für $\mathbb{Z}_{p^e}^*$ gilt folgender Satz[1]:

SATZ. *Sei p eine Primzahl und $e \geq 1$.*

(1) *Für $p = 2$ gilt:*

$$\mathbb{Z}_2^* = \{1\} \simeq \mathbb{Z}_1, \quad \mathbb{Z}_{2^2}^* \simeq \mathbb{Z}_2, \quad \mathbb{Z}_{2^e} \simeq \mathbb{Z}_2 \times \mathbb{Z}_{2^{e-2}} \textit{ für } e \geq 3.$$

Für $e \geq 3$ ist $\mathbb{Z}_{2^e}^*$ nicht zyklisch.

(2) *Für $p > 2$ gilt:*

$$\mathbb{Z}_p^* \simeq \mathbb{Z}_{p-1}, \quad \mathbb{Z}_{p^e} \simeq \mathbb{Z}_{p^{e-1}(p-1)} \simeq \mathbb{Z}_{p-1} \times \mathbb{Z}_{p^{e-1}} \textit{ für } e \geq 2.$$

Insbesondere sind alle Gruppen $\mathbb{Z}_{p^e}^*$ zyklisch. Erzeugende Elemente heißen Primitivwurzeln modulo p^e.

[1] S. Lang. Algebra. Revised Third Edition. Springer, 2002. Exercise II.8, S.115.