(G3) Inverses Element: Zu jedem $a \in G$ gibt es ein $b \in G$ mit $a * b = b * a = e$. Das Element b heißt Inverses zu a.

Eine Gruppe G heißt kommutativ (oder abelsch), falls für alle $a, b \in G$ zusätzlich $a * b = b * a$ gilt.

Propo 3.2 Sei G eine Gruppe und e, e' zwei neutrale Elemente, so gilt $e = e'$

Beweis Nach (G2) gilt $a = a * e$ und $e' * b = b$ für alle $a, b \in G$. Für $a = e'$ und $b = e$ folgt

$$e' = e' * e = e.$$

Propo 3.3 Sei G eine Gruppe und $a \in G$. Seien b und b' zwei Inverse zu a, so gilt $b = b'$

Beweis Übungsblatt.

Bsp 3.4 • Die Menge $\mathbb{Z}$ mit „+" als Verknüpfung ist eine Gruppe. Neutrales Element ist 0 und inverses zu a ist $-a$.

• Die Menge $\mathbb{Q}\setminus\{0\}$ mit „$\cdot$" als Verknüpfung ist eine Gruppe. Neutrales Element ist 1. Zu einem Element $\frac{n}{m} \in \mathbb{Q}\setminus\{0\}$ ist $\frac{m}{n}$ das inverse.

Beide Gruppen sind kommutativ. Es gibt aber auch Gruppen, welche nicht kommutativ sind.

Bsp 3.5 Sei X eine Menge und

$$G = \{ f : X \to X \mid f \text{ bijektiv} \}.$$

Dann ist G mit der Verknüpfung „Komposition" eine Gruppe. Das neutrale Element ist die Identitätsabbildung $id_X : X \to X$, $a \mapsto a$ und das Inverse zu f ist die Umkehrabbildung f^{-1}.

Diese Gruppe ist im Allgemeinen nicht kommutativ.
Sei etwa $X = \{1, 2, 3\}$ und f und g definiert durch die Wertetabelle

	1	2	3
$f(a)$	2	3	1
$g(a)$	1	3	2.

Dann ist $f(g(1)) = 2$ und $g(f(1)) = 3$, also $f \circ g \neq g \circ f$.

Notation:
Sei G eine Gruppe und $a \in G$. So bezeichnen wir das Inverse zu a mit a^{-1}.

Propo 3.6 Sei G eine Gruppe. Dann gilt:

(i) $e^{-1} = e$

(ii) $(a^{-1})^{-1} = a$

(iii) $(a * b)^{-1} = b^{-1} * a^{-1}$

Beweis

(i) Es gilt $e * a = a$ für alle $a \in G$. Insbesondere für $a = e$ gilt $e * e = e$. Also folgt $e^{-1} = e$.

(ii) $a * a^{-1} = e = a^{-1} * a$. Aus Proposition 3.3 folgt direkt $(a^{-1})^{-1} = a$.

(iii)
$$
\begin{aligned}
(a * b) * (b^{-1} * a^{-1}) &\overset{(G1)}{=} a * (b * (b^{-1} * a^{-1})) \\
&\underset{(G1)}{=} a * ((b * b^{-1}) * a^{-1}) \\
&= a * (e * a^{-1}) \\
&\overset{(G2)}{=} a * a^{-1} = e
\end{aligned}
$$

Genau so zeigt man $(b^{-1} * a^{-1}) * (a * b) = e$.

Wir kommen nun zu interessanten Beispielen von Gruppen.

Sei $X = \{1, 2, \ldots, n\}$ und G die Gruppe

$$G = \{\sigma : X \to X \mid \sigma \text{ bijektiv}\}.$$

Diese Gruppe bezeichnet man als

symmetrische Gruppe und schreibt
$S_n = G$.

Wie wir bereits gesehen haben, ist S_3 nicht kommutativ.

Die Elemente $\sigma \in S_n$ nennt man auch Permutationen. Gilt für eine Permutation σ etwa $\sigma(i) = a_i$ für $i = 1, \ldots, n$, so schreibt man

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ a_1 & a_2 & \cdots & a_n \end{pmatrix}.$$

Bsp. 3.7 $X = \{1, 2, 3\}$, $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \in S_3$.

Man sieht leicht, daß S_n aus genau $n!$ vielen Elementen besteht. (Übung)

Die Anzahl der Elemente einer Gruppe G nennt man Ordnung. Man schreibt $\operatorname{ord}(G)$.

Def 3.8 Sei $\sigma \in S_n$, so nennt man

$$\operatorname{sgn}(\sigma) = \prod_{1 \le i < j \le n} \frac{\sigma(j) - \sigma(i)}{j - i} \in \mathbb{Q}$$

das Signum von σ.

Propo 3.9 Sei $\sigma \in S_n$, so gilt $\mathrm{sgn}(\sigma) \in \{\pm 1\}$.

Beweis Eine Permutation $\sigma \in S_n$ bildet die zwei-elementigen Teilmengen von $\{1, \dots, n\}$ bijektiv auf sich selbst ab.
Daher gilt

$$\prod_{i<j} (j-i) = \pm \prod_{i<j} (\sigma(j) - \sigma(i))$$

und somit $\mathrm{sgn}(\sigma) \in \{\pm 1\}$.

Wir benötigen das Signum später für die Determinante.

Propo 3.10 Seien $\sigma, \tau \in S_n$, so gilt
$\mathrm{sgn}(\sigma \circ \tau) = \mathrm{sgn}(\sigma)\, \mathrm{sgn}(\tau)$.

Beweis Übungsblatt.

Ist $\mathrm{sgn}(\sigma) = 1$, nennt man σ gerade, andernfalls ungerade.

Bsp 3.11 $n = 2$, $\mathrm{ord}(S_2) = 2$. Elemente sind

$$\sigma = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} \quad \text{und} \quad \tau = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}.$$

Nun ist $sgn(\sigma) = \prod_{1<2} \frac{\sigma(2) - \sigma(1)}{2-1} = \frac{2-1}{2-1} = 1$

gerade und $sgn(\tau) = \prod_{1<2} \frac{\tau(2) - \tau(1)}{2-1} = \frac{1-2}{2-1} = -1$

ungerade.

Als nächstes wollen wir außer den Gruppen $(\mathbb{Z},+)$ oder S_n weitere Beispiele für Gruppen kennenlernen. Dafür sei $m \in \mathbb{Z}$ und $n \in \mathbb{N}_{>0}$. Wir teilen m durch n und erhalten ein $q \in \mathbb{Z}$ und einen Rest r, so daß

$$m = q \cdot n + r, \quad 0 \leq r < n$$

gilt. Hier sind q und r eindeutig bestimmt.

Bsp 3.12 $m = 37$ und $n = 5$. Dann gilt
$37 = 7 \cdot 5 + 2$ und 2 ist der Rest.

Wir definieren nun folgende Menge

$$\mathbb{Z}/_{n\mathbb{Z}} = \{[0], [1], \ldots, [n-1]\}$$

und fassen zunächst $[a]$, $0 \leq a \leq n-1$ als formale Symbole auf. Wir haben

$$a = 0 \cdot n + a, \quad \text{also Rest von } a =: [a].$$

Wir definieren auf der Menge $\mathbb{Z}/n\mathbb{Z}$ eine Verknüpfung „+" durch

$$[a] + [b] = \text{Rest von } a+b$$

Dadurch wird $(\mathbb{Z}/n\mathbb{Z}, +)$ zu einer Gruppe.

<u>Propo 3.13</u> Für jedes $n \geq 1$ ist $(\mathbb{Z}/n\mathbb{Z}, +)$ eine kommutative Gruppe.

<u>Beweis</u>

(G2): $[0]$ ist neutrales Element. Klar, da $[a] + [0] = \text{Rest von } a = [a]$ und $[0] + [a] = \text{Rest von } a = [a]$.

(G3): Sei $[0] \neq [a] \in \mathbb{Z}/n\mathbb{Z}$. Dann ist $[n-a] \in \mathbb{Z}/n\mathbb{Z}$ das Inverse zu $[a]$.

$[a] + [n-a] = \text{Rest von } n = 0 = [0]$

$[n-a] + [a] = \text{Rest von } n = 0 = [0]$

Falls $[a] = [0]$, so ist $[0]$ das Inverse.

(G1): Dies ist ein wenig schwieriger.

Wir müssen zeigen, daß
$$([a]+[b])+[c] = [a]+([b]+[c]).$$ Nun ist
$$a+b = q'n + r' \quad , \quad 0 \leq r' \leq n-1 \text{ und}$$
$$r'+c = qn + r \quad , \quad 0 \leq r \leq n-1.$$
Dann gilt:
$$r = r'+c-qn = a+b-q'n+c-qn$$
$$= a+b+c-(q+q')n \text{ , d.h.}$$

$$a+b+c = (q+q')n + r \quad , \quad 0 \leq r \leq n-1.$$
Die rechte Seite ergibt sich durch:

$$b+c = p'n + s' \quad , \quad 0 \leq s' \leq n-1 \quad \text{und}$$
$$a+s' = pn + s \quad , \quad 0 \leq s \leq n-1.$$ Wie oben folgt: $a+b+c = (p+p')n + s$. Auf Grund der Eindeutigkeit bei der Division mit Rest, folgt $p+p' = q+q'$ und $r = s$. Also gilt

$$([a]+[b])+[c] = [a]+([b]+[c]).$$
Kommutativität ist klar, da
$$[a]+[b] = \text{Rest von } a+b = \text{Rest von } b+a =$$
$$[b]+[a].$$

Das Element $[a] \in \mathbb{Z}/n\mathbb{Z}$ nennt man Kongruenzklasse mod n. Wir werden später sehen wieso.

Wir bemerken, daß $\operatorname{ord}(\mathbb{Z}/n\mathbb{Z}) = n$.

Nun kennen wir schon folgende Gruppen: $(\mathbb{Z},+)$, $(\mathbb{Q}\setminus\{0\},\cdot)$, $(\mathbb{Q},+)$, S_n und $\mathbb{Z}/n\mathbb{Z}$.

Mit dem Begriff „Gruppe" lassen sich nun „Zahlenmengen" abstrahieren.

Def 3.14 Ein assoziativer Ring, kurz Ring, ist Menge R, mit zwei Verknüpfungen

$$+ : R \times R \to R \quad \text{und} \quad \cdot : R \times R \to R,$$

so daß folgendes erfüllt ist:

(R1) $(R,+)$ ist kommutative Gruppe.

(R2) $a\cdot(b\cdot c) = (a\cdot b)\cdot c$ für alle $a,b,c \in R$

(R3) es gibt ein Element $1 \in R$ mit $1\cdot a = a \cdot 1 = a$ für alle $a \in R$.

(R4) Für alle $a,b,c \in R$ gilt

$$a(b+c) = a\cdot b + a\cdot c$$

$$(b+c)\cdot a = b\cdot a + c\cdot a.$$

Man nennt (R4) das Distributivgesetz und 1 das neutrale Element bezüglich der Multiplikation „·"

Das neutrale Element bezüglich der Addition „+" schreiben wir als 0 und nennen es das Nullelement. Die 1 heißt Einselement.

Das Inverse zu $a \in R$ bezüglich der Addition „+" schreibt man $-a \in R$ und nennt es das Negative von a.

Wir machen nun einige Beobachtungen.

Propo 3.15 Sei R ein Ring. Dann gilt für alle $a \in R$

$$0 \cdot a = 0 = a \cdot 0$$

Beweis Es gilt

$$0 \cdot a = (0+0) \cdot a \overset{(R4)}{=} 0 \cdot a + 0 \cdot a.$$

Da $(R,+)$ kommutative Gruppe ist können wir auf beide Seiten

$-(0 \cdot a)$ addieren.

Das ergibt

$$0 = 0 \cdot a - 0 \cdot a = 0 \cdot a.$$

<u>Propo 3.16</u> Sei R ein Ring. Dann gilt für alle $a \in R$

$$(-1) \cdot a = -a = a \cdot (-1)$$

<u>Beweis</u> Übungsaufgabe.

<u>Propo 3.17</u> Sei R ein Ring. Dann ist R der Nullring genau dann, wenn $0 = 1$.

<u>Beweis</u> Falls R Nullring, so gilt $0 = 1$.
Nehmen wir also an, $0 = 1 \in R$.
Wir müssen also jetzt zeigen, daß $R = \{0\}$.
Sei hierfür $a \in R$ beliebig.
Es gilt

$$a \cdot 1 = a \overset{3.15}{=} a \cdot 0 = 0$$

Also $a = 0$, dh $R = \{0\}$.