# §3 Gruppen und Ringe

**1. Def** Sei $G$ eine Menge und $\cdot : G \times G \to G$, $(a,b) \mapsto ab$ eine Abbildung (Verknüpfung).
Wir nennen $(G, \cdot)$ eine **Gruppe**, falls gilt:

(NE) Es gibt ein $e \in G$ so, dass für alle $a \in G$ gilt $a \cdot e = e \cdot a = a$ ("Neutralelement")

(IV) Zu jedem $a \in G$ gibt es ein $b \in G$ mit $a \cdot b = b \cdot a = e$ ("Inverses")

(AG) Für alle $a, b, c \in G$ gilt $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
("Assoziativität" → keine Klammern nötig)

**Beispiele** (1) $G = \mathbb{Z}$ mit Verknüpfung $+$ ist Gruppe:

$e = 0$ $\quad a + 0 = 0 + a = a$

$a + (-a) = (-a) + a = 0$

$(a+b)+c = a+(b+c)$ (V)

(2) $G = \mathbb{Z}$ mit Verknüpfung $\cdot$ ist keine Gruppe

$e = 1$ $\quad a \cdot 1 = 1 \cdot a = a$ (V)

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

aber zahlr $2 \cdot b = 1$ hat keine Lösung in $\mathbb{Z}$

$\rightsquigarrow$ (IV) gilt nicht.

(3) Die "Vorzeichengruppe" $C_2 = \{\pm 1\}$ mit Multiplikation ist eine Gruppe, mit $e = 1$.

(4) $(\mathbb{Q}, \cdot)$ ist keine Gruppe, es gibt kein Lösung $a \cdot b = 1$ für $a = 0$.

(5) $\mathbb{Q}^* = \mathbb{Q} - \{0\}$ $(\mathbb{Q}^*, \cdot)$ ist eine Gruppe

$e = 1$ $\quad a = \frac{p}{q}$ $\quad b = \frac{q}{p}$ $\Rightarrow a \cdot b = 1$

(6) $(\mathbb{Q}, +)$ ist eine Gruppe

2. Def Eine Gruppe $(G, \cdot)$ heißt kommutativ oder abelsch, falls für alle $a, b \in G$ gilt

$$a \cdot b = b \cdot a$$

Alle Beispiele oben sind abelsch.

Beispiel einer nicht abelschen Gruppe: $G = \mathrm{Sym}(3)$ Permutationen der Menge $\{1,2,3\}$, $\circ$ = Verknüpfung

$\pi$:
$1 \mapsto 2$
$2 \mapsto 3$
$3 \mapsto 1$

$\sigma$:
$1 \mapsto 2$
$2 \mapsto 1$
$3 \mapsto 3$

$\pi \circ \sigma$:
$1 \mapsto 2 \mapsto 3$
$2 \mapsto 1 \mapsto 2$
$3 \mapsto 3 \mapsto 1$

$\sigma \circ \pi$:
$1 \mapsto 2 \mapsto 1$
$2 \mapsto 3 \mapsto 3$
$3 \mapsto 1 \mapsto 2$

also $\pi \circ \sigma \neq \sigma \circ \pi$

In der Zahlentheorie wird es vor allem um abelsche Gruppen gehen.

3. Satz Sei $(G,\cdot)$ eine Gruppe und seien $a, c \in G$.

Dann gibt es genau ein $x \in G$ und genau ein $y \in G$ mit $a \cdot x = c$ und $y \cdot a = c$.

Beweis: Nach (IV) gibt es $b \in G$ mit $ab = ba = e$.

Für $x = bc$ und $y = cb$ folgt $a \cdot x = abc = ec = c$

$ya = cba = ce = c$. Es bleibt die Eindeutigkeit zu zeigen. Angenommen $a \cdot x = a \cdot x'$. Es folgt $\underbrace{bax}_{ex = x} = \underbrace{bax'}_{ex' = x'}$

(genauso für $ya = y'a$) □

Korollar Sei $(G,\cdot)$ eine Gruppe. Zu jedem $a \in G$ gibt es genau ein $b \in G$ mit $ab = e = ba$.

Man schreibt $b = a^{-1}$ und nennt $b$ das Inverse von $a$.

Korollar: In einer Gruppe darf man kürzen: aus

$ac = bc$ folgt $a = b$, genauso folgt aus

$ca = cb$, dass $a = b$.

Denn: $ac = bc \Rightarrow a\underbrace{cc^{-1}}_{=e} = b\underbrace{cc^{-1}}_{=e} \Rightarrow a = b$

Korollar In jeder Gruppe gibt es nur ein einziges Element $e$ mit der Eigenschaft, dass $ae = a = ea$ für alle $a \in G$ gilt.

Vorsicht: Ist $G$ nicht abelsch, so folgt aus

$ax = x \cdot b$ nicht unbedingt, dass $a = b$ !!

**Bem** Wenn man das "+" - Zeichen für die Verknüpfung benutzt, dann schreibt man das Inverse von $a$ als $-a$ und **nicht** als $a^{-1}$.

In dem Fall wird das Neutralelement $e$ als Null "0" geschrieben, also

$$a + (-a) = a - a = 0$$
$$= (-a) + a$$

Das "+" Zeichen wird nur bei abelschen Gruppen benutzt.

**Bem** In jeder Grp $(G, \cdot)$ gilt

$$(a^{-1})^{-1} = a \quad \text{und} \quad (ab)^{-1} = b^{-1} a^{-1}$$

denn: $e = a^{-1} \cdot a = a^{-1} (a^{-1})^{-1}$

$$ab(b^{-1}a^{-1}) = a e a^{-1} = a a^{-1} = e = ab(ab)^{-1}$$

#

4. **Def** Sei $(G,\cdot)$ eine Gruppe, sei $H \subseteq G$ eine Teilmenge. Wir nennen $H$ eine **Untergruppe** von $G$, falls gilt:

(i) $e \in H$ ($e$ Neutralelement von $G$)

(ii) für alle $a,b \in H$ gilt $a \cdot b \in H$

(iii) Für alle $a \in H$ gilt $a^{-1} \in H$

**Beispiel** • Die Gruppe $(\mathbb{Z},+)$. Sei $d \in \mathbb{N}$ und $H = d\mathbb{Z} = \{d \cdot z \mid z \in \mathbb{Z}\}$. Es gilt $0 \in H$ (i) ✓

$a,b \in d\mathbb{Z} \Rightarrow a+b \in d\mathbb{Z}$ ($a = s \cdot d$, $b = t \cdot d \Rightarrow a+b = (s+t)\cdot d$) (ii) ✓ sowie $a \in d\mathbb{Z} \Rightarrow -a \in d\mathbb{Z}$ (iii) ✓

• Daher ist $\mathbb{N} \subseteq \mathbb{Z}$ keine Untergruppe von $(\mathbb{Z},+)$. Zwar gelten (i) und (ii) für $\mathbb{N}$, aber (iii) gilt nicht, z.B. $-1 \notin \mathbb{N}$.

**Satz** (Sparsames Kriterium für Untergruppen)
Sei $(G,\cdot)$ eine Gruppe, sei $H \subseteq G$. Dann sind äquivalent:

(i) $H$ ist eine Untergruppe

(ii) $H \neq \emptyset$ und für alle $a,b \in H$ gilt $a^{-1} \cdot b \in H$

**Beweis** (i) $\Rightarrow$ (ii): $e \in H \Rightarrow H \neq \emptyset$. Für $a,b \in H$ folgt $a^{-1}, b \in H$ aus (iii) oben, mit (ii) oben folgt $a^{-1} \cdot b \in H$.

(ii) $\Rightarrow$ (i): Weil $a \in H$ beliebig (das geht, weil $H \neq \emptyset$). Es folgt $e = a^{-1} \cdot a \in H$. Damit auch $a^{-1} = a^{-1} \cdot e \in H$. Ist also $a, b \in H$, so auch $a \cdot b = (a^{-1})^{-1} \cdot b \in H$ □

Bem • In jeder Gpp $G$ sind $\{e\}$ sowie $G$ Untergruppen.
• Jede Untergpp $H \leq G$ ist ihrerseits eine Gruppe.

5. Theorem Die Untergpp von $(\mathbb{Z}, +)$ sind genau die Mengen $d\mathbb{Z}$, für $d \in \mathbb{N}$.

Beweis In §3.4 hatten wir schon überlegt, dass $d\mathbb{Z}$ immer eine Untergruppe ist.
In §1.6 haben wir bewiesen: ist $H \subseteq \mathbb{Z}$ mit $H \neq \emptyset$ und gilt für alle $a, b \in H$, dass $a - b \in H$, so folgt $H = d\mathbb{Z}$ für ein $d \in \mathbb{N}$.
Das ist genau das Kriterium (ii) aus dem Satz §3.4, additiv geschrieben □

Erinnerung: in §2.10 hatten wir Kongruenzklassen in $\mathbb{Z}$ definiert als $[a]_m = \{a + m \cdot t \mid t \in \mathbb{Z}\}$.
Wir erinnern das Konzept jetzt auf Gruppen.

6. Def Sei $(G,\cdot)$ eine Gruppe und sei $H \leq G$ eine Untergruppe. Sei $a \in G$. Die Linksnebenklasse (bzw Rechtsnebenklasse) von $a$ bezüglich $H$ ist die Menge

$$aH = \{ah \mid h \in H\} \subseteq G$$

beziehungsweise

$$Ha = \{ha \mid h \in H\} \subseteq G$$

Die Menge aller Linksnebenklassen (bzw. Rechtsnebenklassen) ist

$$G/_H = \{aH \mid a \in G\}$$

bzw $$_H\backslash G = \{Ha \mid a \in G\}$$

Bem Falls die Verknüpfung mit Plus "+" geschrieben wird, dann schreibt man

$$a + H = \{a + h \mid h \in H\}.$$

7. Beispiel Betrachte die Gruppe $(\mathbb{Z}, +)$ und die Untergruppe $H = d\cdot\mathbb{Z}$ für ein $d \in \mathbb{N}$, vgl. §3, 5. Die Linksnebenklasse von $a \in \mathbb{Z}$ bezüglich $H$ ist dann

$$a + d\cdot\mathbb{Z} = \{a + dz \mid z \in \mathbb{Z}\} = [a]_d$$

stimmt also genau mit der Kongruenzklasse

von $a$ modulo $d$ überein: Kongruenzklassen sind (spezielle) Nebenklassen.

**8. Satz** (Eigenschaften von Nebenklassen)

Sei $(G,\cdot)$ eine Gruppe und $H \leq G$ eine Untergruppe. Dann gilt für $a,b \in G$:

(i) $aH = bH \Leftrightarrow aH \cap bH \neq \emptyset \Leftrightarrow b \in aH$

"Nebenklassen sind gleich oder disjunkt"

(ii) Die Abbildung $H \to aH$, $h \mapsto ah$ ist eine bijektive Abbildung

"Alle Nebenklassen sind gleich lang"

**Beweis** (i) Angenommen, $c \in aH \cap bH$, also gibt es $h_1, h_2 \in H$ mit $c = a \cdot h_1 = b \cdot h_2$. Es folgt

$$b = a \cdot \underbrace{h_1 \cdot h_2^{-1}}_{=h_3 \in H} = a \cdot h_3 \in aH.$$

Daraus folgt $bH = \{bh \mid h \in H\} = \{a h_3 h \mid h \in H\}$

$$\overset{(*)}{=} \{a\tilde{h} \mid \tilde{h} \in H\} = aH$$

[(*) $a\tilde{h} = a h_3 h$ mit $\tilde{h} = h_3 h$ bzw. $h = h_3^{-1}\tilde{h}$]

Ist $aH = bH$, so gilt natürlich $aH \cap bH \neq \emptyset$.

(ii) Sei $\lambda_a(h) = ah$, $\lambda_a : H \to aH$.

Betrachte $\lambda_{a^{-1}} : aH \to H$, $ah \longmapsto a^{-1}ah = h$

es folgt $\lambda_{a^{-1}} \circ \lambda_a = id_H$ und $\lambda_a \circ \lambda_{a^{-1}} = id_{aH}$

□

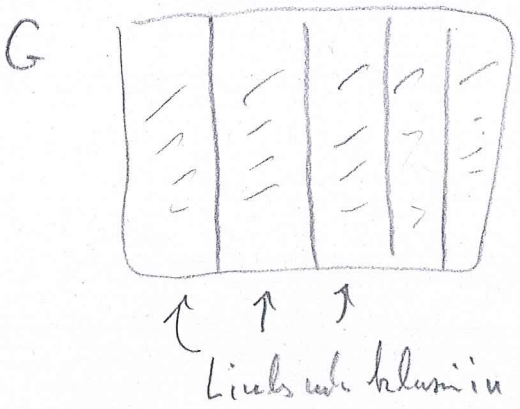
Konvention: Ist $M$ eine Menge, so ist $\#M$ die Anzahl der Elemente von $M$, falls $M$ endlich ist und $\#M = \infty$ falls $M$ nicht endlich ist.
($\#M = 0 \Leftrightarrow M = \emptyset$).

9. Theorem (Satz von Lagrange) Sei $(G, \cdot)$ eine Gruppe und sei $H \leq G$ eine Untergruppe. Falls zwei der Zahlen $\#G$, $\#G/H$, $\#H$ endlich sind, so ist es die dritte auch und es gilt dann

$$\#G = \#G/H \cdot \#H$$

Beweis Wenn $\#G < \infty$, so gilt natürlich auch $\#G/H < \infty$ und $\#H < \infty$ (jede Teilmenge einer endlichen Menge ist endlich; eine endliche Menge hat nur endlich viele Teilmengen).
Angenommen, $\#G/H$ und $\#H$ sind endlich.
Jedes Element $a \in G$ liegt nach § 3.8 (i) in genau einer Linksnebenklasse, nämlich $aH$.
Jede

Links wie Klasse aH hat genau $\#H$ Elemente nach §3.8. (ii). Folglich hat damit $G$ genau $\#H \cdot \#G/H$ Elemente, also $\#G = \#G/H \cdot \#H$.




Man schreibt $\#G/H = [G:H]$ und nennt diese Zahl den Index der Untergruppe $H$ in $G$. Damit schreibt sich der Satz von Lagrange als

$$\#G = [G:H] \cdot \#H.$$

## 10. Bemerkungen

(1) In den vorigen Sätzen §3.8 und §3.9 haben wir Linksnebenklassen betrachtet. Für Rechtsnebenklassen gelten entsprechende Aussagen.

(2) Ist $(G,\cdot)$ eine nicht-abelsche Gruppe, so gilt für $a \in G$ und $H \subseteq G$ Untergruppe im Allgemeinen $aH \neq Ha$, obwohl
($a \in aH \cap Ha$, also $aH \cap Ha \neq \emptyset$ !)
Wenn $(G,\cdot)$ abelsch ist, so gilt dann
$aH = \{ah \mid h \in H\} = \{ha \mid h \in H\} = Ha$.
In abelschen Gruppen stimmen Rechts- und Linksnebenklassen überein.

## 11. Lemma

Sei $(G,\cdot)$ eine abelsche Gruppe und sei $H \subseteq G$ eine Untergruppe. Sei $a,b \in G$ und sei $a' \in aH$, $b' \in bH$. Dann gilt

$$a \cdot bH = a' \cdot b'H$$

Beweis: Schreibe $a' = ah_1$, $b' = b \cdot h_2$. Dann gilt $a' \cdot b' = ah_1 bh_2 = abh_1h_2 \in abH$,
($h_1 b = b h_1$, $G$ abelsch!)
also nach §3.8 (i) $a'b'H = abH$ □

**Korollar** Ist $(G,\cdot)$ eine abelsche Gruppe, $H \leq G$ eine Untergruppe, so erhalten wir eine wohldefinierte Verknüpfung

$$\cdot : G/H \times G/H \longrightarrow G/H, \quad (aH, bH) \longmapsto abH.$$

**Beweis** Das vorige Lemma zeigt: wenn $aH = a'H$ und $bH = b'H$, so ist $a'b'H = abH$, das heißt genau die wohldefiniertheit der Verknüpfung. □

**Theorem** Sei $(G,\cdot)$ eine abelsche Gruppe und sei $H \leq G$ eine Untergruppe. Dann ist $G/H$ mit der Verknüpfung $aH \cdot bH = abH$ eine abelsche Gruppe. Das Neutralelement ist $eH = H$, das Inverse von $aH$ ist $a^{-1}H$.

**Beweis** Wir prüfen alle Axiome aus §3.1.
Sei $e \in G$ das Neutralelement von $G$.

(i) es gilt $eH = H$ und
$$eH \cdot aH = eaH = aH = aeH = aH \cdot eH$$

(ii) es gilt $aH \cdot a^{-1}H = aa^{-1}H = eH = H$

(iii) für $a,b,c \in G$ gilt
$$(aH \cdot bH) \cdot cH = abH \cdot cH = abcH$$
$$= aH \cdot (bH \cdot cH)$$

(iv) für alle $a,b \in G$ gilt $ab = ba$, also auch $aH \cdot bH = abH = baH = bH \cdot aH$ □

12. Beispiel Die abelsche Gruppe $(\mathbb{Z},+)$. Sei $m \in \mathbb{N}$ und $H = m\cdot\mathbb{Z}$. Dann ist $H$ eine Untergruppe nach §3.4. Also wird die Menge

$$\mathbb{Z}/_{m\mathbb{Z}} = \{ [a]_m \mid a \in \mathbb{Z} \}$$
$$= \{ a + m\mathbb{Z} \mid a \in \mathbb{Z} \}$$

aller Kongruenzklassen eine abelsche Gruppe, mit Verknüpfung

$$[a]_m + [b]_m = (a+m\mathbb{Z}) + (b+m\mathbb{Z}) = (a+b) + m\mathbb{Z}$$
$$= [a+b]_m$$

Wie groß sind diese Gruppen?

Satz Sei $m \in \mathbb{N}$. Dann gilt

$$\#\,\mathbb{Z}/_{m\mathbb{Z}} = \begin{cases} \infty & \text{falls } m = 0 \\ m & \text{falls } m > 0 \end{cases}$$

Beweis Für $m = 0$ gilt: $[a]_0 = [b]_0 \Leftrightarrow a = b$, die Abbildung $a \mapsto [a]_0$, $\mathbb{Z} \to \mathbb{Z}/_{0\mathbb{Z}}$ ist also bijektiv und damit ist $\mathbb{Z}/_{0\mathbb{Z}}$ unendlich.

Sei nun $m > 0$. Dann mit Teilen durch $m$ mit Rest: Für jedes $a \in \mathbb{Z}$ gibt es genau ein $r \in \mathbb{N}$ mit $0 \le r < m$ so, dass $a = m\cdot s + r$

Es gibt zu $a \in \mathbb{Z}$ also genau ein $r \in \mathbb{N}$ mit $0 \leq r < m$ und $a \equiv r \pmod m$.

Folglich gilt

$$\mathbb{Z}/m\mathbb{Z} = \{ \underbrace{[0]_m, [1]_m, \dots, [m-1]_m}_{\text{genau } m \text{ verschiedene Nebenklassen Kongruenzklassen}} \}$$

□

Man kann den vorigen Satz auch kurz schreiben als

$$[\mathbb{Z} : m\mathbb{Z}] = \begin{cases} \infty & \text{falls } m = 0 \\ m & \text{falls } m > 0 \end{cases}$$

#

13. Def Sei $(G, \cdot)$ eine Gruppe, sei $g \in G$.

Für $l \in \mathbb{Z}$ definieren wir

$$g^l = \begin{cases} e & \text{falls } l = 0 \\ \underbrace{g \cdots g}_{l\text{-mal}} & \text{falls } l > 0 \\ \underbrace{g^{-1} \cdots g^{-1}}_{-l \text{ mal}} & \text{falls } l < 0 \end{cases}$$

Damit gilt $(g^l)^{-1} = g^{-l} = (g^{-1})^l$

(einsehen)

**Lemma** Mit dieser Konvention gilt für alle $k, l \in \mathbb{Z}$ die Formel

$$g^k \cdot g^l = g^{k+l}$$

**Beweis** Ist $k, l \geq 0$, so folgt das direkt aus der Definition. Ist $k, l \leq 0$, so gilt

$$g^k \cdot g^l = (g^{-1})^{-l} \cdot (g^{-1})^{-k}$$

und wir sind in vorigem Fall, da $-k, -l \geq 0$.

Ist $k > 0$ und $l < 0$, so ist

$$g^k \cdot g^l = \underbrace{g \cdots g}_{k} \cdot \underbrace{g^{-1} \cdots g^{-1}}_{-l} = g^{k+l}$$

Der Fall $k < 0$ und $l > 0$ geht entsprechend. □

**Bem** Wenn die Verknüpfung als "+" geschrieben wird, so setzt man für $g \in G$ und $l \in \mathbb{Z}$

$$l \cdot g = \begin{cases} \underbrace{g + g + \cdots + g}_{l \text{ mal}} & \text{falls } l > 0 \\ 0 & \text{falls } l = 0 \\ \underbrace{(-g) + (-g) + \cdots + (-g)}_{-l \text{ mal}} & \text{falls } l < 0 \end{cases}$$

14. **Def und Satz** Sei $(G,\cdot)$ eine Gruppe, sei $g \in G$. Dann ist

$$\langle g \rangle = \{ g^l \mid l \in \mathbb{Z} \} \subseteq G$$

eine abelsche Untergruppe von $G$, die von $g$ erzeugte zyklische Untergruppe.

Ist $H \subseteq G$ eine beliebige Untergruppe mit $g \in H$, so gilt $\langle g \rangle \subseteq H$.

**Beweis** Wir benutzen §3.4 um zu zeigen, dass $\langle g \rangle \subseteq G$ eine Untergruppe ist. Es ist $e = g^0 \in \langle g \rangle$, also $\langle g \rangle \neq \emptyset$. Für $k, l \in \mathbb{Z}$ ist $(g^k)^{-1} = g^{-k} \in \langle g \rangle$ und damit $(g^k)^{-1} \cdot g^l = g^{-k+l} \in \langle g \rangle$, also ist $\langle g \rangle$ eine Untergruppe. Wegen

$$g^k \cdot g^l = g^{k+l} = g^{l+k} = g^l \cdot g^k$$

ist $\langle g \rangle$ abelsch.

Ist $g \in H$, so ist $g^0 = e \in H$ und $g^k = \underbrace{g \cdots g}_{k \text{ mal}} \in H$ für alle $k > 0$.

Damit also auch $g^{-k} = (g^k)^{-1} \in H$, also $\langle g \rangle \subseteq H$ □

15. Def Sei $(G,\cdot)$ eine Gruppe. Wir nennen $G$ zyklisch, falls es $g \in G$ gibt mit $\langle g \rangle = G$.

Bemerkung: zyklische Gruppen sind stets abelsch, aber nicht jede abelsche Gruppe ist zyklisch.

Bsp. • $(\mathbb{Z},+)$ ist zyklisch, mit $\langle 1 \rangle = \mathbb{Z}$. $= \langle -1 \rangle$

Denn für jedes $k \in \mathbb{Z}$ gilt $k = k \cdot 1$

• $(d\mathbb{Z},+)$ ist für jedes $d \in \mathbb{N}$ zyklisch:
ist $k \in d\mathbb{Z}$, so gibt es $l \in \mathbb{Z}$ mit $k = l \cdot d$,
also $d\mathbb{Z} = \langle d \rangle = \langle -d \rangle$

• $(\mathbb{Q},+)$ ist nicht zyklisch. Denn:
$\langle 0 \rangle = \{0\} \neq \mathbb{Q}$. Für $a \in \mathbb{Q} - \{0\}$
ist $\frac{1}{2}a \notin \langle a \rangle = \{ka \mid k \in \mathbb{Z}\}$, also
auch $\langle a \rangle \neq \mathbb{Q}$.

Satz Jede Untergruppe einer zyklischen Gruppe ist zyklisch.

Beweis Sei $(G,\cdot)$ zyklische Gruppe, sei $g \in G$ mit $\langle g \rangle = G$. Sei $H \leq G$ eine Untergruppe. Falls $H = \{e\}$, so gilt $H = \langle e \rangle$
$\Rightarrow$ Lotsj.

Ist $H \neq \{e\}$, so gibt es $k \in \mathbb{Z}$, $k \neq 0$ mit $g^k \in H$. Dann gilt auch $(g^k)^{-1} = g^{-k} \in H$.

Wir setzen $n = \min \underbrace{\{k \in \mathbb{N} \mid k \geq 1 \text{ und } g^k \in H\}}_{\text{nicht leer!}}$

sowie $h = g^n \in H$. Beh: $H = \langle h \rangle$.

Sei $g^l \in H$ beliebig. Teilen durch $n$ mit Rest ergibt $l = n \cdot k + r$ mit $0 \leq r < n$.

$$g^l = g^{n \cdot k} \cdot g^r = (g^n)^k \cdot g^r = h^k \cdot g^r \in H,$$

also auch $g^r \in h^{-k} \cdot H = H \Rightarrow r = 0$, $g^r = e$

$\Rightarrow g^l = h^k \in \langle h \rangle$ (vgl. §1.6 Nr.)  □

16. Def Sei $(G, \cdot)$ eine Gruppe, sei $g \in G$.

Die Ordnung von $g$ ist definiert als

$$o(g) = \begin{cases} \infty & \text{falls } g^k \neq e \text{ für alle } k \geq 1 \\ \min\{k \in \mathbb{N} \mid k \geq 1 \text{ und } g^k = e\} & \text{sonst} \end{cases}$$

Also insbesondere $o(g) = 1 \iff g = e$.

$o(g) = 2 \iff g \neq e$ und $g^2 = e$

Bemerkung: $o(g) = o(g^{-1})$

**Satz** Sei $(G,\cdot)$ eine Gruppe und sei $g \in G$.

Dann gilt

$$o(g) = \#\langle g \rangle$$

**Beweis** Angenommen, $o(g) = \infty$. Beh: Für alle $1 \leq k < l$ gilt $g^k \neq g^l$. Denn sonst $g^k = g^l \Rightarrow g^{l-k} = e$ ↯ weil $l-k > 0$.

Also enthält $\langle g \rangle$ die unendlich Menge

$$\{g^k \mid k \geq 1\} \Rightarrow \#\langle g \rangle = \infty.$$

Angenommen, $o(g) = n < \infty$. Beh: Für alle $1 \leq k < l \leq n$ gilt $g^k \neq g^l$. Denn sonst $g^k = g^l \Rightarrow g^{l-k} = e$ und $1 \leq l-k \leq n$ ↯

Damit $\#\{g, g^2, \dots, g^n = g^0\} = n$

Für $l \in \mathbb{N}$ beliebig gilt mit Teilen durch $n$ mit Rest, dass $l = n \cdot k + r$ $\quad 0 \leq r < n$

$$\Rightarrow g^l = (g^n)^k \cdot g^r = g^r \in \{g, g^2, \dots, g^n = g^0\}$$

also $\langle g \rangle \subseteq \{g, g^2, \dots, g^n = g^0\} \subseteq \langle g \rangle$ □

**Korollar** Ist $(G,\cdot)$ eine endliche Gruppe und $g \in G$, so gilt

$$o(g) \mid \#G$$

**Beweis** Da $\langle g \rangle \leq G$ ist $\langle g \rangle$ endlich, also $o(g) = \#\langle g \rangle < \infty$. Sei $H = \langle g \rangle$. Nach Lagrange gilt

$$\#G = [G:H] \cdot \underbrace{\#H}_{= o(g)}$$

□

In $\mathbb{Z}$ haben wir zwei Verknüpfungen "+" und "$\cdot$".

17. **Def** Ein **Ring** $(R,+,\cdot)$ besteht aus einer Menge $R$ mit zwei Verknüpfungen "+" und "$\cdot$", mit folgenden Eigenschaften:

(R1) $(R,+)$ ist eine abelsche Gruppe, mit Neutralelement $0 \in R$

(R2) Für alle $a,b,c \in R$ gilt $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ (Assoziativität der Multiplikation)

(R3) Es gibt ein **Einselement** $1 \in R$,

so dass $1 \cdot a = a = a \cdot 1$ für alle $a \in R$ gilt

(R4) Für alle $a, b, c \in R$ gelten die Distributivgesetze
$$a \cdot (b+c) = a \cdot b + b \cdot c$$
$$(b+c) \cdot a = b \cdot a + c \cdot a$$

(Konvention: statt Klammern Punktrechung vor Strichrechnung)

Falls zusätzlich für alle $a, b \in R$ gilt $a \cdot b = b \cdot a$, so heißt der Ring $R$ kommutativ.

Bsp (i) $(\mathbb{Z}, +, \cdot)$ ist ein Ring (kommutativ)

(ii) $(\mathbb{Q}, +, \cdot)$ ist ein kommutativer Ring.

(iii) $(\mathbb{N}, +, \cdot)$ ist kein Ring, denn $(\mathbb{N}, +)$ ist keine Gruppe

(iv) $\mathbb{R}^{2\times 2} = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{R} \right\}$ ist mit Matrizenmultiplikation und -addition ein nicht-kommutativer Ring.

(v) $R = \{0\}$ mit $0 \cdot 0 = 0 + 0 = 0$ ist ein Ring, der Nullring. In dem Ring gilt $1 = 0$. ($\nabla$)

18. **Lemma** (vom Rechnen in Ringen) Sei $(R,+,\cdot)$ ein Ring. Dann gilt für alle $a,b \in R$:

(i) $a \cdot 0 = 0 = 0 \cdot a$

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

(iii) $(-a)\cdot(-b) = a\cdot b$

**Beweis** (i) $0 = 0+0$, also $a\cdot 0 = a\cdot(0+0) = a\cdot 0 + a\cdot 0$ $\overset{\text{Kürzen}}{\Rightarrow}$ $a\cdot 0 = 0$. Genauso $0\cdot a = 0$

(ii) $0 = 1-1$, also $0 = (1-1)\cdot a = 1\cdot a + (-1)\cdot a$

$= a + (-1)\cdot a \Rightarrow (-1)a = -a$, genauso $a\cdot(-1) = a$

(iii) $0 = (a-a)\cdot(b-b) = (a-a)\cdot b + (a-a)(-b)$

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

$= a\cdot b + (-1)ab + (-1)ab + (-a)\cdot(-b)$

$= \underbrace{(a\cdot b - ab)}_{=0} - ab + (-a)\cdot(-b) \Rightarrow$ Beh. □

**Bem** In (R1) hätten wir gar nicht verlangen müssen, daß "+" kommutativ ist, das folgt aus den Distributivgesetzen:

$$(a+1)\cdot(b+1) = a\cdot(b+1) + 1\cdot(b+1) = ab + a + b + 1$$

$$\| \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad$$

$$(a+1)\cdot b + (a+1)\cdot 1 = ab + b + a + 1 \quad \Rightarrow \text{Kürzen.}$$

19. **Def** Sei $(R,+,\cdot)$ ein Ring. Die **Einheitengruppe** des Rings ist

$$R^* = \{ a \in R \mid \text{es gibt } b \in R \text{ mit } a\cdot b = 1 = b\cdot a \}$$

Es folgt $1 \in R^*$ und $(R^*, \cdot)$ ist eine Gruppe. Die Elemente von $R^*$ heißen Einheiten.

Bsp. • $\mathbb{Z}^* = \{\pm 1\}$ Vorzeichengruppe

• $\mathbb{Q}^* = \{r \in \mathbb{Q} \mid r \neq 0\}$

• Für den Nullring $R = \{0\}$ ist $R^* = R$. ($1 = 0$)

20. Def Sei $(R, +, \cdot)$ ein kommutativer Ring. Ein Teilmenge $J \subseteq R$ heißt Ideal, falls gilt: (I1) $J \neq \emptyset$ ist eine Untergruppe von $(R, +)$ (insbesondere also $0 \in J$)

(I2) Für alle $a \in R$ und $j \in J$ gilt $a \cdot j \in J$ ("absorbierende Eigenschaft")

Schreibe dann $J \trianglelefteq R$.

Bsp. • In jedem Ring $R$ sind $\{0\}$ sowie $R$ Ideale (die sogenannten triviale Ideale).

• In $(\mathbb{Z}, +, \cdot)$ ist $J = d\cdot\mathbb{Z}$ $(d \in \mathbb{N})$ ein Ideal: $a \in \mathbb{Z}$, $j \in d\mathbb{Z} \Rightarrow j = k \cdot d$ für ein $k \in \mathbb{Z} \Rightarrow a \cdot j = akd \in d\mathbb{Z}$, also

$$d\mathbb{Z} \trianglelefteq \mathbb{Z}$$

**Lemma** Sei $(R,+,\cdot)$ ein kommutativer Ring, sei $J \trianglelefteq R$ ein Ideal. Wenn gilt $J \cap R^* \neq \emptyset$, so ist $J = R$.

**Beweis** Angenommen, $a \in J \cap R^*$. Wähle $b \in R$ mit $ab = 1 \Rightarrow a \cdot b = 1 \in J \Rightarrow$ für jedes $x \in R$ gilt $x = x \cdot 1 \in J$ □

**21. Lemma** Sei $(R,+,\cdot)$ ein kommutativer Ring, sei $J \trianglelefteq R$ ein Ideal. Sind $a, a', b, b' \in R$ mit $a - a', b - b' \in J$, so folgt $a \cdot b - a' \cdot b' \in J$.

**Beweis** Schreibe $a = a' + j_1$, $b = b' + j_2$ $j_1, j_2 \in J$.

Es folgt $a \cdot b - a' \cdot b' = a' \cdot b' + \underbrace{j_1 \cdot b + a' j_2 + j_1 j_2}_{\in J} - a' \cdot b'$ □

**Theorem** Sei $(R,+,\cdot)$ ein kommutativer Ring, sei $J \trianglelefteq R$ ein Ideal. Dann erhalten wir auf der Menge der Restklassen $R/J = \{a + J \mid a \in R\}$ wohldefinierte Verknüpfungen $+$ und $\cdot$ durch

$$(a + J) + (b + J) = a + b + J$$

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

und $(R/I, +, \cdot)$ ist wieder ein (kommutativer) Ring

der Quotientring modulo $J$.

Bem: Wir wissen schon aus §3.11, dass jeweils auf die Gruppe $(R,+)$ mit Untergruppe $J \subseteq R$, dass $(R/J,+)$ eine abelsche Gruppe ist. Ist $a+J = a'+J$ und $b+J = b'+J$, so zeigt das vorige Lemma, dass $a\cdot b + J = a'\cdot b' + J$ gilt, also ist die Verknüpfung "$\cdot$" auf $R/J$ wohldefiniert. Es gilt

$$(a+J)\cdot(1+J) = a\cdot 1 + J = a + J = (1+J)\cdot(a+J)$$

$$((a+J)\cdot(b+J))\cdot(c+J) = \ldots\; abc+J = \ldots\; (a+J)\cdot((b+J)\cdot(c+J))$$

$$(a+J)\cdot(b+J) = ab+J = ba+J = (b+J)\cdot(a+J)$$

genauso die Distributivgesetze... □

Korollar: Für jedes $d \in \mathbb{N}$ ist $(\mathbb{Z}/d\mathbb{Z}, +, \cdot)$ ein kommutativer Ring. #