§2. Gruppen, Ringe, Körper und Kongruenzen

1. **Def** Eine **abelsche Gruppe** (oder **kommutative Gruppe**) $(G,*)$ besteht aus einer Menge G mit einer Verknüpfung $*: G\times G \to G$, $(x,y)\mapsto x*y$ und einem Element $e\in G$, so dass gilt:

(i) $(x*y)*z = x*(y*z)$ für alle $x,y,z\in G$, die Verknüpfung ist **assoziativ**

(ii) $x*y = y*x$ für alle $x,y\in G$, die Verknüpfung ist **kommutativ**

(iii) $x*e = e*x$ für alle $x\in G$, das Element e ist ein **Neutralelement**.

(iv) Für jedes $x\in G$ gibt es ein $x'\in G$ mit $x*x' = e = x'*x$, jedes Element x hat ein **Inverses** x'.

Beispiele

(a) $G = \mathbb{Z}$, $x * y = x + y$. Das ist eine abelsche Gruppe $(\mathbb{Z}, +)$ mit Neutralelement 0, das Inverse von x ist $-x = x'$ #

(b) $G = \{\pm 1\} = C_2$, $x * y = x \cdot y$. Das ist eine abelsche Gruppe $(C_2, \cdot)$ mit Neutralelement 1, das Inverse von x ist $x' = \frac{1}{x}$, die Vorzeichengruppe.

(c) $G = \mathbb{R}^* = \{t \in \mathbb{R} \mid t \neq 0\}$, $x * y = x \cdot y$ ist eine abelsche Gruppe $((\mathbb{R}^*, \cdot))$ mit Neutralelement $\underline{1}$; das Inverse von x ist $x' = \frac{1}{x}$.

(d) $G = \mathbb{N}$ mit Verknüpfung $x * y = x + y$ ist keine Gruppe. Es gelten (i), (ii), (iii) (mit $e = 0$) aber (iv) gilt nicht, denn zu keinem $e \in \mathbb{N}$ gibt es $y \in \mathbb{N}$ so, dass $\underbrace{(e+1)}_{x} + y = e$ gilt.

(e) $G = \mathbb{Z}$ mit Verknüpfung $x * y = x \cdot y$ ist keine Gruppe: es gelt (i), (ii), (iii) mit $e = 1$ aber es gibt kein $y \in \mathbb{Z}$ mit

$$0 \cdot y = 1.$$

2. Beobachtungen und Konventionen in Gruppen

Sei $(G,*)$ eine (abelsche) Gruppe mit Neutralelement $e \in G$.

(a) Es gibt genau ein Neutralelement in G.

Denn: ist $f \in G$ ein weiteres Neutralelement, so folgt $f = f*e = e$.

(b) Jedes $x \in G$ hat genau ein Inverses x'.

Denn: sind y, z Inverse zu x, so folgt

$$y = y*e = y*x*z = e*z = z.$$

(c) Ist $a, b \in G$, so gibt es genau ein $x \in G$ mit $a*x = b$.

Existenz: Sei a' das Inverse zu a, setze $x = a'*b$. Es folgt $a*x = a*a'*b = e*b = b$.

Eindeutigkeit: Sei a' das Inverse zu a.

$$a*x = b \Rightarrow \underbrace{a'*a}_{=e}*x = a'*b$$

$$\Rightarrow x = a'*b.$$

Konvention. Wenn wir die Verknüpfung in einer (abelschen) Gruppe G mit "$+$"-Zeichen schreiben, dann bezeichnen wir das Neutralelement mit $\underline{e = 0}$ und das Inverse von x mit $\underline{x' = -x}$, also

$$x + (-x) = 0 = (-x) + x.$$

Wenn wir die Verknüpfung in einer (abelschen) Gruppe G mit "$\cdot$"-Zeichen schreiben, dann bezeichnen wir das Neutralelement mit $\underline{e = 1}$ und das Inverse von x mit $\underline{x' = x^{-1}}$, also

$$x^{-1} \cdot x = 1 = x \cdot x^{-1}.$$

3. **Definition** Sei $(G, *)$ eine abelsche Gruppe. Ein Teilmenge $H \subseteq G$ heißt Untergruppe von G, wenn gilt

(i) $H \neq \emptyset$

(ii) für alle $x, y \in H$ gilt $x * y \in H$

(iii) für jedes $x \in H$ liegt auch das Inverse x' von x in H.

Dann ist $(H, *)$ wieder eine (abelsche) Gruppe, denn:

$*$ ist assoziativ und kommutativ (klar).
Ist $x \in H$ mit Inverse x', so folgt
$x' \in H$ und $x * x' = e \in H \Rightarrow e \in H$
und $x' \in H$. □

Beispiel • $G = \mathbb{R}^*$ mit Multiplikation wie in §2.1 (c) $H = \{\pm 1\} \Rightarrow H$ ist Untergruppe

• $G = \mathbb{R}$ mit Addition als Verknüpfung, $H = \mathbb{Z}$ ist Untergruppe

• $G = \mathbb{Z}$ mit Addition, $H = \mathbb{N} \subseteq \mathbb{Z}$ ist keine Untergruppe, denn (iii) gilt nicht.

4. Lemma (Sparsames Kriterium für Untergruppen)
Sei $(G, *)$ eine abelsche Gruppe, sei H eine Teilmenge. Für $x \in G$ sei x' das Inverse von x. Dann ist H genau dann eine Untergruppe von G, wenn gilt:
(i) $H \neq \emptyset$
(ii) Für alle $x, y \in H$ gilt $x * y' \in H$

Beis: Klar: jede Untergruppe erfüllt (i) und (ii). Umgekehrt: Wenn (i) und (ii) gelten, so folgt: dass es $h \in H$ gibt $\Rightarrow e = h * h' \in H$.
$\Rightarrow$ zu jedem $x \in H$ ist $x' = e * x' \in H$
und zu jedem $x, y \in H$ ist $x * y = x * (y')' \in H$ □

Verfeinert auf § 1.7

5. Satz (über die Untergruppen von $(\mathbb{Z}, +)$)
Sei $H \leq \mathbb{Z}$ eine Untergruppe der additiven Gruppe $(\mathbb{Z}, +)$ der ganzen Zahlen. Dann gibt es genau ein $d \in \mathbb{N}$ mit

$$H = d \cdot \mathbb{Z} = \{ d \cdot z \mid z \in \mathbb{Z} \}$$

Umgekehrt ist $d \cdot \mathbb{Z}$ stets eine Untergruppe von $(\mathbb{Z}, +)$.

Beis: Das haben wir in § 1.7 schon bewiesen.

Denn: wir weisen das sparsame Kriterium § 2.4 an: $H \leq \mathbb{Z}$ ist genau dann eine Untergruppe, wenn $H \neq \emptyset$ und wenn für alle $x, y \in H$ gilt $x - y \in H$. Nach § 1.7 sind die Mengen, die die Eigenschaft haben, genau die Teilmengen der Form $H = d \cdot \mathbb{Z}$, für ein eindeutiges $d \in \mathbb{N}$ □
Umgekehrt ist $d \cdot \mathbb{Z} \leq \mathbb{Z}$ stets Untergruppe.

Beobachtung Untergruppen von $\mathbb{Z}$

(a) $2\cdot\mathbb{Z}$ ist genau die Menge der <u>geraden Zahlen</u>. Die gerade Zahlen bilden also eine Untergruppe von $\mathbb{Z}$. Allgemein bilden für jedes $d \in \mathbb{N}$ die durch d teilbaren Zahlen eine Untergruppe von $\mathbb{Z}$, nämlich die Menge $d\cdot\mathbb{Z}$. Der weise Satz sagt: So sehen alle Untergruppen von $\mathbb{Z}$ aus,

$$\{\text{Untergruppen von } \mathbb{Z}\} \longleftrightarrow \left\{\begin{array}{l}\text{Mengen aller durch } d \\ \text{teilbaren Zahlen } d\cdot\mathbb{Z}, \text{ für} \\ d = 0, 1, 2, 3, \ldots\end{array}\right\}$$

(b) die Menge aller <u>ungerader Zahlen</u>

$U = \{2\cdot z + 1 \mid z \in \mathbb{Z}\} \subseteq \mathbb{Z}$ ist <u>keine</u> <u>Untergruppe</u> von $\mathbb{Z}$ - die Differenz von zwei ungeraden Zahlen ist je eine gerade Zahl ($\Leftrightarrow$ Spezielles Kriterium)

Wir können aber auch solche Mengen durch (Nebenklassen von) Untergruppen beschreiben, wie wir sehen werden.

6. **Definition** (Kongruenz) Sei $d \in \mathbb{N}$.
Wir nennen zwei Zahlen $x, y \in \mathbb{Z}$ **kongruent modulo d**, falls gilt:

$$d \mid (x-y) \qquad \#$$

und schreiben dafür kurz: $x \equiv y \pmod d$
(lies: "x kongruent y modulo d")

Lemma Sei $d \in \mathbb{N}$. Dann gilt

(a) Kongruenz modulo d ist eine **Äquivalenzrelation** auf $\mathbb{Z}$, d.h. es gilt für alle $x,y,z \in \mathbb{Z}$

$x \equiv x \pmod d$ (reflexiv)

$x \equiv y \pmod d \Rightarrow y \equiv x \pmod d$ (symmetrisch)

$x \equiv y \pmod d$ und $y \equiv z \pmod d$
$\Rightarrow x \equiv z \pmod d$ (transitiv)

(b) $x \equiv y \pmod d$ gilt genau dann, wenn es ein $l \in \mathbb{Z}$ gibt mit $x = y + l \cdot d$.

Beis Zuerst Beh (b).

$x \equiv y \pmod d \overset{\text{Def}}{\Leftrightarrow} d \mid (x-y) \overset{\text{Def}}{\Leftrightarrow}$ es gibt $l \in \mathbb{Z}$ mit $l \cdot d = x - y \Leftrightarrow$ es gibt $l \in \mathbb{Z}$ mit $x = y + l \cdot d$ □

Jetzt ist (a) klar, denn

$x = x + 0 \cdot d$

$x = y + l \cdot d \Rightarrow y = x - l \cdot d = x + (-l) d$

$x = y + l \cdot d$, $y = z + m \cdot d \Rightarrow x = z + (l+m) \cdot d$ □

Beacht: $x \equiv 0 \pmod d \Leftrightarrow d \mid x$

insbesondere: $x \equiv 0 \pmod 2 \Leftrightarrow x$ gerade

$x \equiv 1 \pmod 2 \Leftrightarrow x$ ungerade.

Definition (Kongruenzklasse) Sei $d \in \mathbb{N}$.

Wir definieren die Kongruenzklasse modulo d von $x \in \mathbb{Z}$ als

$$[x]_d = \{ z \in \mathbb{Z} \mid x \equiv z \pmod d \}$$

Bsp $[0]_2$ = Menge aller geraden Zahlen

$[1]_2$ Menge aller ungeraden Zahlen.

Beachte auch: $[x]_0 = \{x\}$ gilt für jedes $x \in \mathbb{Z}$.

7. Lemma Sei $d \in \mathbb{N}$. Dann gilt folgt.

(a) $\tilde{x} \in [x]_d \Leftrightarrow [\tilde{x}]_d = [x]_d$

(b) Ist $[x]_d = [\tilde{x}]_d$ und $[y]_d = [\tilde{y}]_d$, für $x, y, \tilde{x}, \tilde{y} \in \mathbb{Z}$, so folgt

$$[x+y]_d = [\tilde{x}+\tilde{y}]_d$$

Beweis (a) folgt direkt aus §2.6.

Genauer: $\tilde{x} \in [x]_d \overset{\text{Def}}{\Leftrightarrow} x \equiv \tilde{x} \pmod d$

$\overset{\text{Def}}{\Leftrightarrow} [\tilde{x}]_d = [x]_d$ □

(b) $\left.\begin{aligned} \tilde{x} &= x + u \cdot d \\ \tilde{y} &= y + u \cdot d \end{aligned}\right\} \Rightarrow \tilde{x}+\tilde{y} = x+y+(u+u)\cdot d$

also, $\tilde{x}+\tilde{y} \equiv x+y \pmod d$

$\Rightarrow [\tilde{x}+\tilde{y}]_d = [x+y]_d$ □

□

Sei $d \in \mathbb{N}$ fest. Es liegt nahe, auf der Menge der Kongruenzklassen $G = \{[x]_d \mid x \in \mathbb{Z}\}$ eine Verknüpfung zu definieren durch

$$[x]_d + [y]_d = [x+y]_d$$

Wird das eine abelsche Gruppe?

Satz Sei $d \in \mathbb{N}$ und sei $G = \{[x]_d \mid x \in \mathbb{Z}\}$ die Menge aller Kongruenzklassen modulo d. Dann ist die Verknüpfung "+" auf G,

$$[x]_d + [y]_d = [x+y]_d$$

wohldefiniert und $(G,+)$ ist eine abelsche Gruppe. Wenn $d=0$ gilt, ist G unendlich. Wenn $d>0$ gilt, hat G genau d Elemente.

Beweis Wenn gilt $[x]_d = [\tilde{x}]_d$ und $[y]_d = [\tilde{y}]_d$, so gilt nach dem vorigen Lemma $[x+y]_d = [\tilde{x}+\tilde{y}]_d$, also ist die Verknüpfung + wohldefiniert. Weiter gilt für $x,y,z \in \mathbb{Z}$

$$([x]_d + [y]_d) + [z]_d = [x+y]_d + [z]_d = [x+y+z]_d$$
$$= [x]_d + [y+z]_d = [x]_d + ([y]_d + [z]_d) \quad \text{sowie}$$

$$[x_d] + [y]_d = [x+y]_d = [y+x]_d = [y]_d + [x]_d$$

d.h. Assoziativ- und Kommutativgesetz gelten. Weiter gilt $[x]_d + [0]_d = [x]_d = [0]_d + [x]_d$, $\rightsquigarrow [0]_d$ ist Neutralelement. Schließlich ist $[x]_d + [-x]_d = [0]_d = [-x]_d + [x]_d$

Folglich ist (G,t) eine abelsche Gruppe.

Wenn $d=0$, so ist $[x]_0 = \{x\}$, also ist $G = \{\{x\} \mid x \in \mathbb{Z}\}$ unendlich.

Annahme, $d>0$. Für jedes $x \in \mathbb{Z}$ gibt es genau ein $\tilde{x} \in \mathbb{N}$ mit $0 \le \tilde{x} < d$ und

$$x = s \cdot d + \tilde{x} \qquad \text{(Teilen mit Rest, §1.6)}$$

Es folgt $[x]_d = [\tilde{x}]_d \Rightarrow G = \{[0]_d, [1]_d, \ldots, [d-1]_d\}$

$\Rightarrow \le d$ Kongruenzklassen.

Für $\tilde{x}, \tilde{y} \in \mathbb{N}$ mit $0 \le \tilde{x} < d$, $0 \le \tilde{y} < d$ gilt $|\tilde{x} - \tilde{y}| < d$, also: $d \mid \tilde{x} - \tilde{y} \Leftrightarrow \tilde{x} = \tilde{y}$

damit $[\tilde{x}]_d = [\tilde{y}]_d \Leftrightarrow \tilde{x} = \tilde{y}$, d.h. hat G genau d Elemente. □

Konvention Die additive Gruppe $G = \{[x]_d \mid x \in \mathbb{Z}\}$ bezeichnen wir mit

$$\mathbb{Z}/d = \{[x]_d \mid x \in \mathbb{Z}\} \qquad (d \ge 1)$$

$(\mathbb{Z}/d, t)$ ist also eine abelsche Gruppe, mit d Elementen falls $d>0$ und unendlich vielen Elementen für $d=0$.

Beispiel $d = 2$

$$\mathbb{Z}/2 = \{ [0]_2, [1]_2 \}$$

$[0]_2 = \{x \in \mathbb{Z} \mid x \equiv 0 \pmod 2\}$ gerade Zahlen

$[1]_2 = \{x \in \mathbb{Z} \mid x \equiv 1 \pmod 2\}$ ungerade Zahlen

Wir betrachten diese Konstruktion jetzt allgemeiner.

8. Nebenklassen in abelschen Gruppen

Sei $(G, *)$ eine abelsche Gruppe und sei $H \subseteq G$ eine Untergruppe. Für $a \in G$ setzen wir

$$a * H = \{a * h \mid h \in H\} \subseteq G$$

Solche Mengen heißen Nebenklassen (bezüglich H) in G. (Wenn die Verknüpfung mit "+" geschrieben wird, schreibt man $a + H = \{a + h \mid h \in H\}$.)

Beispiel $G = \mathbb{Z}$ (additive Gruppe der ganzen Zahlen), $H = d \cdot \mathbb{Z}$ für ein $d \in \mathbb{N}$. Für $a \in \mathbb{Z}$ ist

$$\begin{aligned} a + d\mathbb{Z} &= \{a + d \cdot z \mid z \in \mathbb{Z}\} \\ &= \{b \in \mathbb{Z} \mid a \equiv b \pmod d\} \\ &= [a]_d \end{aligned}$$

Kongruenzklassen sind also spezielle Nebenklassen.

Lemma Sei $(G,*)$ eine abelsche Gruppe, sei $H \leq G$ eine Untergruppe, seien $a,b \in G$. Dann gilt

(i) Wenn $b \in a*H$, so ist $a*H = b*H$

(ii) Wenn $(a*H) \cap (b*H) \neq \emptyset$, so gilt $a*H = b*H$. Nebenklassen sind entweder disjunkt oder gleich.

Beweis (i) $b \in a*H \rightsquigarrow b = a*h$ für ein $h \in H$

$\rightsquigarrow b*H = a*h*H = a*H$, denn:

$h*H = \{h*x \mid x \in H\} = H$, weil

$h*x \in H$ und $y \in H \Rightarrow y = h*(\underbrace{h'*y}_{=x})$

(ii) $x \in (a*H) \cap (b*H)$

$\Rightarrow a*H = x*H$ und $b*H = x*H$ nach (i). □

Man schreibt die Menge aller Nebenklassen bzgl H mit $G/H = \{a*H \mid a \in G\}$

Satz Sei $(G,*)$ eine abelsche Gruppe und $H \leq G$ eine Untergruppe, sei $G/H = \{a*H \mid a \in H\}$ die Menge der Nebenklassen bzgl. H. Dann ist die Abbildung

$$(a*H, b*H) \longmapsto a*b*H$$

eine wohldefinierte Verknüpfung auf G/N und G/N ist bezüglich dieser Verknüpfung eine abelsche Gruppe, mit Neutralelement $e*H = H$.

Beweis Angenommen, $a*H = \tilde{a}*H$ und $b*H = \tilde{b}*H$ für $a, \tilde{a}, b, \tilde{b} \in G$. Es folgt $\tilde{a} = a*x$, $\tilde{b} = b*y$ für Elemente $x, y \in H$, damit

$$\tilde{a}*\tilde{b}*H = a*x*b*y*H = a*b*\underbrace{(x*y*H)}_{=H}$$

(Kommutativgesetz)

$= a*b*H$, die Verknüpfung ist also wohldefiniert.

Für $a, b, c \in G$ folgt nun

$$((a*H)*(b*H))*(c*H) = a*b*c*H$$

$$= (a*H)*((b*H)*(c*H))$$

sowie $(a*H)*(b*H) = (a*b)*H$
$= (b*a)*H = (b*H)*(a*H)$
$\Rightarrow$ Assoziativ- und Kommutativgesetz gelten.
Weiter gilt $H = e*H$ und
$(a*H)*H = a*H = H*(a*H)$
$\Rightarrow$ H ist Neutralelement. Ist a' das Inverse
von a, so gilt $(a*H)*(a'*H) = (a*a')*H = H$
$\Rightarrow$ $a'*H$ ist Invers zu $a*H$ □

9. <u>Lemma</u> Sei $(G,*)$ eine abelsche Gruppe und sei $H \leq G$ eine Untergruppe. Für jedes $a \in G$ ist die Abbildung

$$H \to a*H \qquad h \mapsto a*h$$

bijektiv. "Alle Nebenklassen bezüglich H sind gleich lang".

<u>Bew.</u> Die Abbildung ist nach Konstruktion surjektiv. Angenommen, $a*h = a*\tilde{h}$ für $h,\tilde{h} \in H$. Linksmultiplikation mit dem Inversen a' von a liefert $\underbrace{a'*a*h}_{h} = \underbrace{a'*a*\tilde{h}}_{\tilde{h}}$. □

Def Sei $(G,*)$ eine abelsche Gruppe, sei $H \leq G$ eine Untergruppe. Die Anzahl der Nebenklassen $a*H \subseteq G$ bzgl. H nennt man den **Index** von H in G und schreibt dafür

$$[G:H] = \#\{a*H \mid a \in G\} = \#(G/H)$$

Satz (Satz von Lagrange) Sei G eine abelsche Gruppe, sei H eine Untergruppe. Wenn H und $[G:H]$ endlich sind, so ist auch G endlich und es gilt

$$\#G = [G:H] \cdot \#H \quad \text{oder} \quad \#G = \#(G/H) \cdot \#H$$

Beweis Nach §2.8 sind Nebenklassen bzgl H entweder gleich oder disjunkt. Nach dem vorigen Lemma haben alle Nebenklassen gleich viele Elemente wie H. Also können wir die Elemente in G zählen, indem wir die Anzahl der Elemente von H mit der Anzahl der Nebenklassen multiplizieren. □

Bsp Die (abelsche) Gruppe $(\mathbb{Z}, +)$ ist unendlich. Ist $d \in \mathbb{N}$ und $d \geq 1$, so gilt für die Untergruppe $d\mathbb{Z}$

$$[\mathbb{Z} : d\mathbb{Z}] = d \quad \text{nach } \S 2.7.$$

Der Index einer unendlich Untergruppe kann also endlich sein.

Wir gehen zurück zu Kongruenzklassen in $\mathbb{Z}$.

10. Lemma Sei $d \in \mathbb{N}$. Angenommen, $x, \tilde{x}, y, \tilde{y} \in \mathbb{Z}$ sind Zahlen mit

$$x \equiv \tilde{x} \pmod{d}$$
$$y \equiv \tilde{y} \pmod{d}.$$

Dann ist auch $x \cdot y \equiv \tilde{x} \cdot \tilde{y} \pmod{d}$.

Beweis Schreibe $\tilde{x} = x + m \cdot d$ und $\tilde{y} = y + n \cdot d$ für $m, n \in \mathbb{Z}$. Es folgt

$$\tilde{x} \cdot \tilde{y} = x \cdot y + d \cdot (n \cdot x + m \cdot y + m \cdot n) \qquad \square$$

Korollar Sei $d \in \mathbb{N}$. Dann ist die Abbildung

$$[a]_d \cdot [b]_d \longrightarrow [a \cdot b]_d$$

eine wohldefinierte Verknüpfung auf der Menge $\mathbb{Z}/d = \{ [x]_d \mid x \in \mathbb{Z} \}$. $\square$

11. **Definition** Ein **kommutativer Ring** $(R,+,\cdot)$ besteht aus einer abelschen Gruppe $(R,+)$ mit Neutralelement $0 \in R$ und einer Verknüpfung "$\cdot$" auf R mit folgenden Eigenschaften:

(i) die Verknüpfung "$\cdot$" ist **assoziativ** und **kommutativ**,

$$x\cdot(y\cdot z) = (x\cdot y)\cdot z \quad \text{und} \quad x\cdot y = y\cdot x$$

für alle $x,y,z \in R$

(ii) Es gibt ein **Einselement** $1 \in R$ so, dass

$$1\cdot x = x = x\cdot 1$$ für alle $x \in R$ gilt

(iii) Es gilt das **Distributivgesetz**

$$x\cdot(y+z) = x\cdot y + x\cdot z$$
$$(y+z)\cdot x = y\cdot x + z\cdot x$$

für alle $x,y,z \in R$.

Es folgt daraus:

$$0\cdot x = 0 = x\cdot 0$$

denn: $0 = 0+0$, also $0\cdot x = (0+0)\cdot x = 0\cdot x + 0\cdot x$; $0\cdot x$ additiv kürzen

$$(-x)\cdot y = -(x\cdot y)$$

denn: $0 = (x-x)\cdot y = x\cdot y + (-x)\cdot y$

u.s.w.

Beispiele (a) $(\mathbb{Z},+,\cdot)$ ist ein kommutativer Ring,

(b) $(\mathbb{R},+,\cdot)$ oder $(\mathbb{Q},+,\cdot)$ sind kommutative Ringe.

Unser nächstes Ziel ist zu zeigen, dass $\mathbb{Z}/d$ mit der in §2.10 definierten Verknüpfung ein kommutativer Ring ist. Es lohnt sich, das etwas allgemeiner zu machen.

12. Definition Sei $(R,+,\cdot)$ ein kommutativer Ring. Eine Teilmenge $J \subseteq R$ heißt Ideal in R, wenn gilt:

(i) $J \subseteq R$ ist Untergruppe von $(R,+)$

(ii) Für alle $z \in R$ und $j \in J$ gilt $z \cdot j \in J$.

Beispiel • $R = \mathbb{Z}$, $J = d \cdot \mathbb{Z}$ für $d \in \mathbb{N}$ beliebig. Ist $z \in \mathbb{Z}$ und $j = m \cdot d \in J$, so folgt

$z \cdot j = (z \cdot m) \cdot d \in d\mathbb{Z}$, also ist $J = d \cdot \mathbb{Z}$ ein Ideal in $\mathbb{Z}$. Die Ideale in $\mathbb{Z}$ entsprechen also 1-1 den natürlichen Zahlen, via $d \leftrightarrow d \cdot \mathbb{Z}$.

Satz Sei $(R,+,\cdot)$ ein kommutativer Ring und sei $J \subseteq R$ ein Ideal. Dann ist die Menge der Nebenklassen

$$R/J = \{ x+J \mid x \in R \} \qquad (\text{lies } R \text{ mod } J)$$

wieder ein kommutativer Ring mit Verknüpfungen

$$(x+J)+(y+J) = x+y+J$$

$$(x+J)\cdot(y+J) = x\cdot y + J$$

Das Nullelement in R/J ist $0+J = J$, das Einselement ist $1+J$.

Beweis Wir wissen schon nach §2.8, dass $(R/J,+)$ eine abelsche Gruppe ist. Wir müssen zeigen, dass die Multiplikation "$\cdot$" wohldefiniert ist. Angenommen, $x+J = \tilde{x}+J$ und $y+J = \tilde{y}+J$ für $x, \tilde{x}, y, \tilde{y} \in R$. Dann gibt es $i,j \in J$ mit $\tilde{x} = x+i$ und $\tilde{y} = y+j$, also

$$\tilde{x}\cdot\tilde{y}+J = (x+i)(y+j)+J = x\cdot y + \underbrace{i\cdot y + x\cdot j + i\cdot j}_{\text{in } J} + J$$

$$= x\cdot y + J$$

Also ist die Verknüpfung "$\cdot$" auf Nebenklassen wohldefiniert.

Sei nun $x, y, z \in R$. Wir prüfen (i), (ii), (iii) aus §2.11.

Zu (i)

$$(x+J)((y+J)\cdot(z+J)) = (x+J)(yz+J) = xyz+J$$

$$= ((x+J)\cdot(y+J))\cdot(z+J) \quad (\checkmark)$$

$$(x+J)\cdot(y+J) = xy+J = yx+J = (y+J)\cdot(x+J) \quad (\checkmark)$$

Zu (ii)

$$(1+J)(x+J) = x+J = (x+J)(1+J) \quad (\checkmark)$$

Zu (iii)

$$(x+J)\cdot((y+J)+(z+J)) = (x+J)\cdot(y+z+J)$$

$$= x(y+z)+J = xy+xz+J = (xy+J)+(xz+J) \quad (\checkmark)$$

□

analog zum ganzen.

<u>Korollar</u> Sei $d \in \mathbb{N}$. Dann ist $\mathbb{Z}/d$ ein kommutativer Ring, mit Einselt $[1]_d$ und Verknüpfung "$\cdot$" durch

$$[x]_d \cdot [y]_d = [x \cdot y]_d$$

13. Def Sei $(R,+,\cdot)$ ein kommutativer Ring.
Ein Elt $x \in R$ heißt Einheit, wenn es $y \in R$ gibt mit $x \cdot y = y \cdot x = 1$.
Ein Elt $x \in R$ heißt Nullteiler, wenn es $y \in R$, $y \neq 0$ gibt mit $x \cdot y = 0 = y \cdot x$.

Beispiele: (a) In jedem kommutativen Ring ist 1 ein Einheit und 0 ein Nullteiler.

(b) Im Ring $(\mathbb{Z},+,\cdot)$ sind genau die Zahlen ± 1 Einheiten. Die Zahl 0 ist der einzige Nullteiler

(c) Im Ring $(\mathbb{Z}/4,+,\cdot)$ gilt:
$[1]_4$, $[-1]_4 = [3]_4$ sind Einheiten
$[0]_4$, $[2]_4$ sind Nullteiler
$[2]_4 \cdot [2]_4 = [4]_4 = [0]_4$

(d) Im Ring $(\mathbb{Q},+,\cdot)$ oder $(\mathbb{R},+,\cdot)$ ist jedes $x \neq 0$ eine Einheit und 0 ist der einzige Nullteiler.

14. Def Sei $(R,+,\cdot)$ ein kommutativer Ring.
Wir setzen $R^* = \{x \in R \mid x \text{ ist Einheit}\}$
Dann ist $(R^*,\cdot)$ eine abelsche Gruppe
(denn $(R^*,\cdot)$ erfüllt alle Bedingungen aus
§2.1), die Einheitengruppe von R. #

Bsp • $\mathbb{Z}^* = \{\pm 1\}$

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

• $(\mathbb{Z}/4)^* = \{[1]_4, [3]_4\} = \{[1]_4, [-1]_4\}$

15. Eulersche φ-Funktion Sei $d \in \mathbb{N}$, $d \geq 1$.
Wir definieren die Eulersche φ-Funktion
durch

$$\varphi(d) = \#(\mathbb{Z}/d)^*,$$

die Anzahl der Einheiten im Ring $\mathbb{Z}/d$.

Satz Sei $d \in \mathbb{N}$, $d \geq 1$. Sei $x \in \mathbb{Z}$.

Dann sind äquivalent:

(i) $[x]_d$ ist Einheit in $\mathbb{Z}/d$

(ii) $ggT(x,d) = 1$

Bew. $[x]_d$ Einheit in $\mathbb{Z}/d$ $\Leftrightarrow$ es gibt $g \in \mathbb{Z}$ mit

$[x]_d \cdot [g]_d = [x \cdot g]_d = [1]_d$

$\Leftrightarrow$ es gibt $g \in \mathbb{Z}$, mit

$x \cdot g \equiv 1 \pmod{d}$

$\Leftrightarrow$ es gibt $g \in \mathbb{Z}$ und $m \in \mathbb{Z}$ mit

$x \cdot g = 1 + m \cdot d$

$\Leftrightarrow$ es gibt $g \in \mathbb{Z}$ und $l \in \mathbb{Z}$ mit

$x \cdot g + l \cdot d = 1$

§1.10 $\Leftrightarrow$ $ggT(x,d) = 1$ □

Korollar (klassische Definition der φ-Funktion)

Sei $d \in \mathbb{N}$, $d \geq 1$. Dann gilt

$$\varphi(d) = \#\{x \in \mathbb{N} \mid 0 \leq x < d \text{ und } ggT(x,d) = 1\}$$

Anzahl der Zahlen $< d$, die teilerfremd zu d sind. □

17. **Def** Ein kommutativer Ring $(K, +, \cdot)$ heißt **Körper**, wenn gilt $K^* = K - \{0\}$, d.h. Einheiten in K sind genau die von Null verschiedenen Elemente.

Bsp: • $\mathbb{Z}$ ist kein Körper, denn $\mathbb{Z}^* = \{\pm 1\} \neq \mathbb{Z} - \{0\}$.

• $\mathbb{Q}$ und $\mathbb{R}$ sind Körper

• $\mathbb{Z}/2 = \{[0]_2, [1]_2\}$ ist ein Körper, denn $(\mathbb{Z}/2)^* = \{[1]_2\}$.

Satz Sei $d \in \mathbb{N}$. Dann sind äquivalent:

(i) der Ring $\mathbb{Z}/d$ ist ein Körper

(ii) d ist eine Primzahl.

Beweis (i) $\Rightarrow$ (ii) Annahme, $d > 1$.

$\mathbb{Z}/d$ Körper $\Rightarrow$ $ggT(d, x) = 1$ für alle $x \in \mathbb{N}$ mit $0 < x < d$ $\Rightarrow$ $p(d) = d$

($p(d) = \min\{k \geq 2 \mid k | d\}$ vgl. § 1.11)

$\Rightarrow d \in \mathbb{P}$.

$d = 0$: $[2]_0 = \{2\}$, es gibt kein $y \in \mathbb{Z}$ mit $[2]_0 \cdot [y]_0 = \{2 \cdot y\} = \{1\}$ $\Rightarrow$ kein Körper

$d = 1$ $\mathbb{Z}/1 = \{[0]_1\}$ $\mathbb{Z}/1 - \{[0]_1\} = \emptyset$ ist kein Gruppe.

(ii) $\Rightarrow$ (i) $\quad d \in \mathbb{P} \Rightarrow ggT(x,d) = 1$ f.a. $0 < x < d \Rightarrow (\mathbb{Z}/d)^* = \{ [1]_d, \dots, [d-1]_d \} = \mathbb{Z}/d - \{[0]_d\}$

□

Für $p \in \mathbb{P}$ schreibt man auch

$$\mathbb{F}_p = \mathbb{Z}/p$$

das ist der Körper mit p Elementen.