§7 Äquivalenzrelationen

(7.1) **Def** Eine **Relation** auf einer Menge M besteht aus einer Teilmenge $R \subseteq M \times M$. Wir schreiben $a \sim b$ falls $(a,b) \in R$. Ein Relation $\sim$ heißt eine **Äquivalenzrelation** falls folgendes gilt:

i) **Reflexivität**: für alle $a \in M$ gilt $a \sim a$.

ii) **Symmetrie**: $a \sim b \iff b \sim a$.

iii) **Transitivität**: $a \sim b$ und $b \sim c \Rightarrow a \sim c$.

Für $a \in M$ heißt $[a] := \{b \in M \mid b \sim a\}$ die Äquivalenzklasse von a.

Für die Menge $\{[a] \mid a \in M\}$ aller Äquivalenzklassen schreiben wir oft $M/\sim$.

(7.2) **Bsp** i) Auf $\mathbb{Z}$ wird durch

$$a \sim b :\iff b-a \text{ ist gerade}$$

eine Äquivalenzrelation erklärt. Bezüglich dieser Äquivalenzrelation gibt es zwei Äquivalenzklassen: die geraden Zahlen und die ungeraden Zahlen.

ii) Sei $N \in \mathbb{Z}$. Auf $\mathbb{Z}$ wird durch

$$a \sim_N b :\iff N \text{ teilt } b-a$$

eine Äquivalenzrelation erklärt. Oft schreiben wir auch $a \equiv b \ (N)$ für $a \sim_N b$ und sagen "a und b sind **kongruent modulo N**".

iii) Die Relation "$\leq$" auf $\mathbb{Z}$ ist transitiv und reflexiv aber nicht symmetrisch, also keine Äquivalenzrelation.

iv) Sei $f: X \to Y$ eine Abbildung. Dann definiert

$$x_1 \sim_f x_2 :\iff f(x_1) = f(x_2)$$

eine Äquivalenzrelation auf X.

(7.3) **Satz** Sei $\sim$ eine Äquivalenzrelation auf M. Für $a,b \in M$ sind äquivalent: i) $a \sim b$ ii) $[a]=[b]$ iii) $[a] \cap [b] \neq \emptyset$.

Beweis: i) $\Rightarrow$ ii) Sei $a \sim b$. Sei $x \in [a]$. Also $x \sim a$. Da $a \sim b$ folgt $x \sim b$, also $x \in [b]$. Es folgt $[a] \subseteq [b]$. Genauso folgt $[b] \subseteq [a]$ also gilt $[a]=[b]$.

ii) $\Rightarrow$ iii) Sei $[a]=[b]$. Dann ist $[a] \cap [b] \neq \emptyset$ genau dann wenn $[a] \neq \emptyset$. Da $a \sim a$ gilt $a \in [a]$, also ist $[a] \neq \emptyset$.

iii) $\Rightarrow$ i) Sei $[a] \cap [b] \neq \emptyset$. Dann gibt es $x \in M$ mit $x \sim a$, $x \sim b$. Es folgt $a \sim x$, $x \sim b$, also $a \sim b$. □

(7.4) **Korollar** Sei $\sim$ eine Äquivalenzrelation auf M. Dann ist M die disjunkte Vereinigung der Äquivalenzklassen von $\sim$.

Beweis: Da $a \in [a]$ für jedes $a \in M$ ist M die Vereinigung der Äquivalenzklassen von $\sim$. Wegen (7.3) sind die verschiedenen Äquivalenzklassen disjunkt. □

(7.5) **Bsp** Sei $\mathcal{B} := \mathbb{Z} \times \mathbb{Z} \setminus \{0\}$. Dann definiert

$$(z,n) \sim (z',n') :\iff zn' = z'n$$

eine Äquivalenzrelation auf $\mathcal{B}$. Sei $\mathbb{Q} := \mathcal{B}/\sim$.

Dann können wir auf $\mathbb{Q}$ wie folgt eine Summe erklären: Seien $q_1, q_2 \in \mathbb{Q}$. Wähle $(z_1,n_1), (z_2,n_2) \in \mathcal{B}$ mit $q_1 = [(z_1,n_1)]$, $q_2 = [(z_2,n_2)]$. Nun setze

$$q_1 + q_2 := [(z_1 n_2 + z_2 n_1, n_1 n_2)]$$

⚠ Wir müssen zeigen, dass dies wohldefiniert ist, also q_1+q_2 unabhängig von der Wahl von $(z_1,n_1), (z_2,n_2) \in \mathcal{B}$ ist.

Sei $q_1 = [(z_1,n_1)] = [(z_1',n_1')]$ und $q_2 = [(z_2,n_2)] = [(z_2',n_2')]$.

Zu zeigen: $[(z_1 n_2 + z_2 n_1, n_1 n_2)] = [(z_1' n_2' + z_2' n_1', n_1' n_2')]$.

Es ist $z_1 n_1' = z_1' n_1$ da $[(z_1,n_1)] = [(z_1',n_1')]$ und
$z_2 n_2' = z_2' n_2$ da $[(z_2,n_2)] = [(z_2',n_2')]$.
Damit folgt $(z_1 n_2 + z_2 n_1) n_1' n_2' = z_1 n_2 n_1' n_2' + z_2 n_1 n_1' n_2' =$
$= z_1' n_2 n_1 n_2' + z_2' n_1 n_1' n_2 = (z_1' n_2' + z_2' n_1') n_1 \cdot n_2$
Also $[(z_1 n_2 + z_2 n_1, n_1 n_2)] = [(z_1' n_2' + z_2' n_1', n_1' n_2')]$.

(7.6) Bem (7.5) liefert eine Konstruktion der rationalen Zahlen. Es gilt $(z,n) \sim (z',n') \iff \frac{z}{n} = \frac{z'}{n'} \in \mathbb{Q}$.

(7.7) Bsp i) Sei H eine Untergruppe der Gruppe G. Dann definiert $g \sim_H g' :\iff \exists h \in H$ mit $gh = g'$ eine Äquivalenzrelation auf G. Die Äquivalenzklassen bzgl. $\sim_H$ heißen die **Linksnebenklassen** von H.
Es gilt $[g]_{\sim_H} = \{ gh \mid h \in H \} =: gH$.
Die Menge der Linksnebenklassen von H bezeichnet man auch mit $G/H := G/\sim_H$.

ii) Sei H eine Untergruppe der Gruppe G. Dann definiert
$g \tilde{\sim}_H g' :\iff \exists h \in H$ mit $hg = g'$
eine Äquivalenzrelation auf G. Die Äquivalenzklassen bzgl. $\tilde{\sim}_H$ heißen die **Rechtsnebenklassen** von H.
Es gilt $[g]_{\tilde{\sim}_H} = \{ hg \mid h \in H \} =: Hg$.
Die Menge der Rechtsnebenklassen bezeichnet man auch mit $H\backslash G := G/\tilde{\sim}_H$.

(7.8) Bem Ist G abelsch so gilt für $g, g' \in G$
i) $g \sim_H g' \iff g \tilde{\sim}_H g'$ ii) $gH = Hg$.
Benutzen wir die additive Schreibweise in G, so schreiben wir auch $g + H = \{ g+h \mid h \in H \} = [g]_{\sim_H}$.

(7.9) Bsp Sei $U \leq V$ ein Untervektorraum. Dann definiert
$v \sim_U v' :\iff v - v' \in U$
eine Äquivalenzrelation auf V. Dann gilt für $v \in V$
$[v]_{\sim_U} = \{ v+u \mid u \in U \} =: v + U$. Die Menge aller Äquivalenzklassen von $\sim_U$ wird mit V/U bezeichnet.

(7.10) Bez Sei V ein K-Vektorraum.
i) Für Teilmengen $S, S' \subseteq V$ setzen wir
$S + S' := \{ s+s' \mid s \in S, s' \in S' \}$.
ii) Für $\lambda \in K$ und $S \subseteq V$ setzen wir
$\lambda \cdot S := \{ \lambda \cdot s \mid s \in S \}$.

(7.11) Lemma Sei $U \leq V$ ein Untervektorraum.
i) Für $v, v' \in V$ gilt $(v+U) + (v'+U) = (v+v') + U$.
ii) Für $\lambda \in K, v \in V$ gilt $\lambda (v+U) = (\lambda v) + U$.

Beweis: i) $v+U + v'+U = \{ v+u+v'+u' \mid u,u' \in U \} = \{ v+v'+u'' \mid u'' \in U \} =$
$= (v+v') + U$.
ii) $\lambda (v+U) = \{ \lambda (v+u) \mid u \in U \} = \{ \lambda v + u' \mid u' \in U \} = (\lambda v) + U$.

(7.12) Def Sei $U \leq V$ ein Unterraum. Dann wird V/U durch die Addition aus (7.10) i) und die Multiplikation aus (7.10) ii) zu einem K-Vektorraum. Er heißt der **Quotientenvektorraum** von V nach U.
Es gilt $0_{V/U} = U = 0 + U$, $-(v+U) = (-v) + U$.

(7.13) Bsp Für $n \in \mathbb{Z}$, $n \geq 2$ ist $n\mathbb{Z} = \{ n \cdot k \mid k \in \mathbb{Z} \} = \{ z \in \mathbb{Z} \mid z \text{ ist ein Vielfaches von } n \}$ eine Untergruppe. Auf $\mathbb{Z}/n\mathbb{Z} = \{ k + n\mathbb{Z} \mid k \in \mathbb{Z} \}$ erhalten wir durch $(k+n\mathbb{Z}) + (k'+n\mathbb{Z}) := (k+k') + n\mathbb{Z}$

und $(k+n\mathbb{Z})\cdot(k'+n\mathbb{Z}) := (k\cdot k')+n\mathbb{Z}$
eine wohldefinierte Addition und Multiplikation.

(7.14) Bem Es gelten
$(k+n\mathbb{Z})+(k'+n\mathbb{Z}) = \{a+a' \mid a\in k+n\mathbb{Z}, a'\in k'+n\mathbb{Z}\}$ und
$(k+n\mathbb{Z})\cdot(k'+n\mathbb{Z}) \supseteq \{a\cdot a' \mid a\in k+n\mathbb{Z}, a'\in k'+n\mathbb{Z}\}$.
Aber $(2+4\mathbb{Z})\cdot(2+4\mathbb{Z}) = \underbrace{4+4\mathbb{Z}}_{\text{U}} \supsetneq \underbrace{\{a\cdot a' \mid a,a'\in 2+4\mathbb{Z}\}}_{\text{U}}$.

(7.15) Def Eine Halbgruppe ist eine Menge H mit einer Verknüpfung
$H\times H\to H, (a,b)\mapsto a\cdot b$ so dass folgende Axiome gelten:
i) Assoziativität: Für alle $a,b,c\in H$ gilt $a(bc)=(ab)c$.
ii) Neutrales Element: Es gibt $e\in H$ so dass für alle $a\in H$ gilt $e\cdot a = a\cdot a\cdot e$.
Eine Halbgruppe heißt abelsch falls für alle $a,b\in H$ gilt $ab=ba$.

(7.16) Def Ein Ring ist eine Menge R mit zwei Verknüpfungen,
$(r,s)\mapsto r+s$ und $(r,s)\mapsto r\cdot s$ die die folgenden Axiome erfüllen.
i) $(R,+)$ ist eine abelsche Gruppe mit neutralem Element 0.
ii) $(R\setminus\{0\},\cdot)$ ist eine abelsche Halbgruppe mit neutralem Element 1.
iii) Es gilt das Distributivgesetzt: für alle $r,s,t\in R$: $r(s+t)=rs+rt$.

(7.17) Bem $\mathbb{Z}/n\mathbb{Z}$ wird mit der Addition und Multiplikation aus (7.13) zu einem Ring.

(7.18) Satz Sei p eine Primzahl. Dann ist $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ ein Körper mit p Elementen.

Beweis: Es ist $\mathbb{Z}/p\mathbb{Z} = \{0+p\mathbb{Z}, 1+p\mathbb{Z}, \dots, (p-1)+p\mathbb{Z}\}$. Also hat $\mathbb{Z}/p\mathbb{Z}$ p-Elemente und ist insbesondere endlich.

Wir müssen noch zeigen das es multiplikative Inverse in $\mathbb{F}_p$ gibt. Sei $a+p\mathbb{Z}\in \mathbb{Z}/p\mathbb{Z}\setminus(0+p\mathbb{Z})$.
Betrachte die Abbildung $f_a: \mathbb{Z}/p\mathbb{Z}\to\mathbb{Z}/p\mathbb{Z}$
$b+p\mathbb{Z}\mapsto ab+p\mathbb{Z} = (a+p\mathbb{Z})(b+p\mathbb{Z})$.

Beh: f_a ist injektiv:
Sei $f_a(b+p\mathbb{Z}) = f_a(b'+p\mathbb{Z})$. Dann $ab-ab'\in p\mathbb{Z}$.
Also teilt p a oder $b-b'$. Da $a+p\mathbb{Z}\neq 0+p\mathbb{Z}$ teilt p nicht a. Also teilt p $b-b'$. Es folgt $b+p\mathbb{Z}=b'+p\mathbb{Z}$.
Damit folgt die Beh.
Da f_a eine injektive Selbstabbildung einer endlichen Menge ist, muss f_a auch surjektiv sein. Folglich gibt es $b+p\mathbb{Z}\in\mathbb{Z}/p\mathbb{Z}$ mit $1+p\mathbb{Z}=f_a(b+p\mathbb{Z})=(a+p\mathbb{Z})(b+p\mathbb{Z})$.
$b+p\mathbb{Z}$ ist das multiplikative Inverse von $a+p\mathbb{Z}$. □