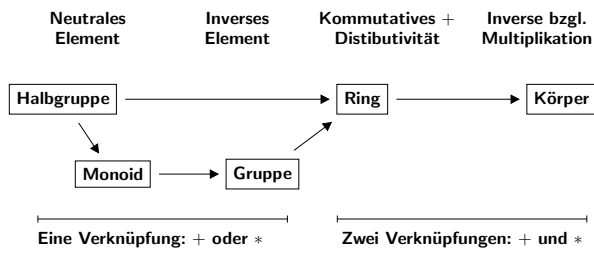


Hierarchie algebraischer Grundstrukturen



◀ ▶ ↺ ↻ 🔍

A-4 Äquivalenzrelationen und Quotientenstrukturen

Bemerkung

Die Menge der **unsigned chars** B basiert nicht direkt auf der Zahlenhierarchie, sie ergibt sich als sogenannter Quotientenring von \mathbb{Z} .

Entsprechend bilden die Drehungen in der Ebene S^1 eine Quotientengruppe von \mathbb{R} , wobei alle Drehwinkel φ_1, φ_2 , deren Differenz ein ganzes Vielfaches von 2π ist, zusammengelegt werden, da sie als äquivalent betrachtet werden.

◀ ▶ ↺ ↻ 🔍

Definition A.31 (Äquivalenzrelationen)

Man nennt $\mathcal{R} \subset \mathcal{M} \times \mathcal{M}$ eine Äquivalenzrelation auf \mathcal{M} und schreibt dann

$$x \sim y \iff (x, y) \in \mathcal{R}$$

wenn für alle $x \in \mathcal{M}$ die folgenden Eigenschaften gelten :

$x \sim x$	Reflexivität
$x \sim y \wedge y \sim z \implies x \sim z$	Transitivität
$x \sim y \implies y \sim x$	Symmetrie

Für jedes $x \in \mathcal{M}$ bezeichnet

$$[x]_{\mathcal{R}} \equiv \{y \in \mathcal{M} : x \sim y\}$$

die Äquivalenzklasse von x bezüglich \sim .

Falls \mathcal{R} klar schreibt man einfach $[x]$.

◀ ▶ ↺ ↻ 🔍

Beispiel A.32

Für $x, y \in \mathbb{R}$ gilt:

$$x \sim y \iff x * x = y * y \implies [x] = \{+x, -x\}$$

Beispiel A.33

Geraden in der Ebene sind äquivalent, wenn sie parallel sind. Äquivalenzmengen sind alle Geraden mit derselben Steigung.

Lemma A.34 (Quotientenäquivalenz)

Für $x = (x_1, x_2) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\}) \ni y = (y_1, y_2)$ gilt:

$$x \sim y \iff x_1 * y_2 = y_1 * x_2$$

◀ ▶ ↺ ↻ 🔍

Lemma A.35 (Restklassen bezüglich Untergruppe)

$U \subset G$ kommutative Untergruppe impliziert, dass
 $x \sim y \iff x - y \in U \iff \exists z \in U : x = y + z$
eine Äquivalenzrelation ist.

Beispiel A.36

Für festes $m \in \mathbb{Z}$ gilt: $x \sim y \iff m$ teilt $x - y$.



Lemma A.37 (Partitionierung)

Sei \sim Äquivalenzrelation auf \mathcal{M} .

- (i) $[x] = [y] \iff x \sim y$
- (ii) $[x] \cap [y] = \emptyset \iff x \not\sim y$
- (iii) Es existiert eine Repräsentantenmenge $\mathcal{M}' \subset \mathcal{M}$ so dass

$$\forall y \in \mathcal{M}, x \in \mathcal{M}' \cap [y] \ni z \implies z = x$$

und somit

$$x, y \in \mathcal{M}' \wedge (x \neq y) \implies [x] \neq [y]$$

sowie

$$\mathcal{M} = \bigcup_{x \in \mathcal{M}'} [x]$$



Beispiel A.38

Für Beispiel A.36 nehme Repräsentant $0 \leq x < m$.

Beispiel A.39

Für Lemma A.34 nehme gekürzten Bruch wo x_1 und x_2 teilerfremd sind.

Beispiel A.40

Für Beispiel A.33 nehme Gerade durch Nullpunkt.



Definition A.41 (Quotientenmenge)

$$\mathcal{M}/R = \mathcal{M}/\sim = \{[x] : x \in \mathcal{M}\}$$

bezeichnet die Mengen aller Äquivalenzklassen von \sim in \mathcal{M} . Ihre Elemente werden häufig mit denen von \mathcal{M}' identifiziert.

Satz A.42 (Quotientengruppe)

Ist \sim durch eine Untergruppe U der kommutativen Gruppe G induziert so definiert die additive Verknüpfung

$$[x] + [y] \equiv [x + y]$$

auf der Partitionierung G/\sim eine Gruppenstruktur, welche mit G/U bezeichnet wird. Die Restklasse $[0]$ bildet die Null in G/U und $[-x]$ das negative Element zu $[x]$.



Beispiele A.43 (Symmetrische Gruppe)

- ▶ $G = \mathbb{R}$, $U = \{2\pi k : k \in \mathbb{Z}\}$
- ▶ $S^1 = G/U = \text{Richtungen in Ebene} = \{-\pi \leq x < \pi\} \cong \mathcal{M}'$

Beispiel A.44 (Restklassenringe)

$$G = \mathbb{Z}, \quad U = \{mx : x \in \mathbb{Z}\} = m\mathbb{Z}, \\ \mathbb{Z}_m = \mathbb{Z}/(m\mathbb{Z}) = \{x \in \mathbb{Z} : 0 \leq x < m\}$$

Bemerkung:

\mathbb{Z}_m ist nicht nur Gruppe sondern sogar Ring, da U nicht nur Untergruppe sondern sogar Ideal im Ring \mathbb{Z} ist.



Definition A.45 (Ideal)

Eine Untergruppe $U \subset \mathcal{M}$ heisst **Ideal des kommutativen Ringes** \mathcal{M} falls

$$a \in U \wedge b \in \mathcal{M} \implies a * b \in U$$

m.a.W. Produkte mit einem Faktor in U gehören auch zu U .

Speziell ist für jedes $a \in \mathcal{M}$ die *Gruppe*

$$U = a * \mathcal{M} = \{a * b : b \in \mathcal{M}\}$$

ein sogenanntes *Hauptideal* in \mathcal{M} .

Bemerkung:

Jedes Ideal ist insbesondere ein Unterring. Körper haben keine Hauptideale außer sich selbst und $\{0\}$.



Beispiel A.46

$m\mathbb{Z}$ ist Hauptideal in \mathbb{Z} .

Beispiel A.47

$\mathcal{M} = \mathbb{Z}[x]$ = Menge aller reellen Polynome enthält $x * \mathcal{M} \equiv x * \mathbb{Z}[x]$ = Menge aller Polynome, deren nullter Koeffizient (= konstanter Term) verschwindet.



Satz A.48 (Quotientenringe)

Gilt Satz A.42 und ist U sogar Ideal im kommutativen Ring \mathcal{G} , dann macht die zusätzliche multiplikative Verknüpfung

$$[x] * [y] \equiv [x * y]$$

die Quotientengruppe \mathcal{G}/U selbst zu einem kommutativen Ring. Hat \mathcal{G} die Eins 1, so ist die Äquivalenzklasse $[1]$ die Eins im Quotientenring.



Schlussbemerkung

- ▶ $\mathcal{B} = \text{unsigned char} = \mathbb{Z}_{256} = \mathbb{Z}/256\mathbb{Z}$ ist ein endlicher kommutativer Ring mit Nullteilern. (z.B. $[32] * [8] = [256] = [0]$)
- ▶ Obwohl a/b für $b \neq 0$ auf dem Rechner immer ein Ergebnis liefert bedeutet dies nicht, dass $a/b = a * b^{-1}$ für ein Inverses Element b^{-1} in \mathbb{Z}_{256} gilt. Vielmehr gilt $a/b = r_b(a)$ wie im Folgenden definiert.