Thema 5: Algebraische Grundstrukturen: Halbgruppe

Donnerstag, 28. Dezember 2023 18:12

Halbgruppe:

Besteht aus einem Tupel $(\mathbb{N}, +)$

$(\mathbb{N}, +)$ Halbg

$0 + 1 = 1$
$(3+2)+9 = 3+(2+9)$

$(\mathbb{N}, \cdot)$

$3\mathbb{Z} = \{3 \cdot n : n \in \mathbb{Z}\} = \{0, 3, -3, 6, -6 \ldots\}$

$(3\mathbb{Z}, +)$
$(3\mathbb{Z}, \cdot)$

Monoid:

Besteht aus einem Tripel $(M, \circ, e)$

$(M, \circ, e)$ — e ist ein neutrales Element und ändert nichts an der Rechnung

Eigenschaften

1. $M \neq \{\}$
2. $(M, \circ)$ ist Halbgruppe
3. $\forall a \in M$ gilt: $a \cdot e = e \cdot a = a$

$(\mathbb{N}, \cdot, 1)$
$3 \cdot 1 = 1 \cdot 3 = 3$

Primzahlen: Annahme endl. viele P.

$p_1, \ldots, p_n$ = alle Primzahlen

$m = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$

$m = p_1 \cdot k \; (\in \mathbb{N})$

$p_1 \cdot k = p_1 \cdot \ldots \cdot p_n + 1 \quad / - p_1 \cdot \ldots \cdot p_n$
$p_n \cdot k - p_1 \cdot \ldots \cdot p_n = 1$

≥ 2 $\in \mathbb{N}$ ↯

Primfaktorzerlegung:

$2, 3, 5, 7, 11, 13, 17, 19$

$18 = 2 \cdot 9 = 2 \cdot 3 \cdot 3$
$35 = 7 \cdot 5$

$264 = 2 \cdot 132 = 2 \cdot 2 \cdot 66 = 2 \cdot 2 \cdot 2 \cdot 33 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 11$

Permutationen: (alle Vertauschungen)

$(1\ 2\ 3) \Rightarrow (1\ 3\ 2)$

S_n = alle Permutationen von $\{1, 2, \ldots, n\}$

$S_3 = \{(1\ 2\ 3), (1\ 3\ 2), (3\ 1\ 2)\}$

$p = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (2\ 1\ 3)$

$q = (3\ 2\ 1)$

$p \cdot q = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$

$c = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \overset{c^{-1}}{\Rightarrow} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$

Nullteiler:

$a \neq 0 \quad b \neq 0 \Rightarrow a \cdot b = 0$

$\mathbb{Z}_4$

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

$10 = 2 \cdot 5$

$\mathbb{Z}_{10}$: [2], [5], [4], [6], [8]

Einheit:

$a \cdot b = [1]$ Alle Einheiten die nicht Nullteiler sind, sind Einheiten

$\mathbb{Z}_3/\mathbb{Z}$: $[4] \cdot [7] = [4 \cdot 7] = [28] = [1]$

$\mathbb{Z}/15\mathbb{Z}$

1. Primfaktorzerlegung $15 = 3 \cdot 5$
2. Nullteiler $N = \{3, 5, 6, 9, 10, 12\}$
   alle Zahlen die durch 3 oder 5 teilbar sind Nullteiler,
   der Rest Einheiten $E = \{1, 2, 4, 7, 8, 11, 13, 14\}$

if $\mathbb{Z}_n$: [a] Nullteiler $\Leftrightarrow ggT(a, n) > 1$

if [a] Einheit $\Leftrightarrow ggT(a, n) = 1$

Gruppe:

$(M, \circ, e)$

1. $(M, \circ, e)$ ist Monoid
2. $\forall a \in M \; \exists b \in M: b \cdot a = e$

Gruppe → $(\mathbb{Q}^*, \circ, 1)$ $\quad 2 \cdot \frac{1}{2} = 1$
keine Gruppe → $(\mathbb{Z}, \circ, 1)$

3. $a \cdot b = b \cdot a$

Inverse Element:

Inverse Elemente sind Elemente, die in Bezug auf eine bestimmte Operation das ursprüngliche Element rückgängig machen oder aufheben

Beispiel mit der Addition: $(\mathbb{Z}, +, 0)$

$a + 0 = 0 + a = a$
Das Inverse zu einer ganzen Zahl a ist die Zahl $-a$:

$a + (-a) = (-a) + a = 0$
$1 + (-1) = (-1) + 1 = 0$

Untergruppe:

$(\mathbb{Z}, +, 0)$ Gruppe

alle Zahlen die mit 2 teilbar sind → $(2\mathbb{Z}, +, 0)$ Untergruppe } Eine Teilmenge von einer Gruppe $c (\mathbb{Z}, +, 0)$

Ringe:

$(M, +, \circ, 0)$

1. $(M, +, 0)$ abelsche Gruppe (kommutative Gruppe)
2. $(M, \cdot)$ Halbgruppe
3. $\forall a, b, c \in M: \underbrace{a \cdot (b + c) = ab + ac}_{\text{Distributivgesetz}}$

Körper:

$(M, +, \circ, 0, 1)$

$(M \setminus \{0\}, \circ, 1)$ abelsche Gruppe

Bekannteste Mengen: $\mathbb{Q}, \mathbb{R}, \mathbb{C}$

ggT: Der ggT ist die letzte Zahl vor dem Rest 0

$ggT(440, 700)$

$440 = 2 \cdot 2 \cdot 2 \cdot 5 \cdot 11$
$700 = 2 \cdot 2 \cdot 5 \cdot 5 \cdot 7$

1. Beide Zahlen Primfaktorzerlegung
2. Alle gleichen Zahlen Streichen
3. Dann die Zahlen miteinander multiplizieren

$2 \cdot 2 \cdot 5 = 20$

$ggT(17, 60)$

1. Teile $60 \; // \; 17$
   $60 = 17 \cdot 3 + 9$
   Rest = 9
2. Ersetze 60 durch 17 und 17 durch 9 und wiederhole bis Rest von 0
   $17 = 9 \cdot 1 + 8$
   Rest = 8
   $9 = 8 \cdot 1 + 1$
   Rest = 1
   $8 = 1 \cdot 8 + 0$
   Rest 0

Restklassenringe:

$\mathbb{Z}/\mathbb{Z}_3 = \underbrace{\{[0], [1], [2]\}}_{\text{alle Reste die bei einer Division durch 3 entstehen können}} \} \; 0 - (n-1)$

$[a] + [b] = [a + b]$

in $\mathbb{Z}/\mathbb{Z}_3$: $[1] + [2] = [3] \sim [0]$

$\mathbb{Z}_4$

+	0	1	2	3
0	0	1	2	3
1	1	1	3	0
2	2	3	0	1
3	3	0	1	2

4 ≈ 0
5 ≈ 1
6 ~ 2

$a \equiv b \mod n$