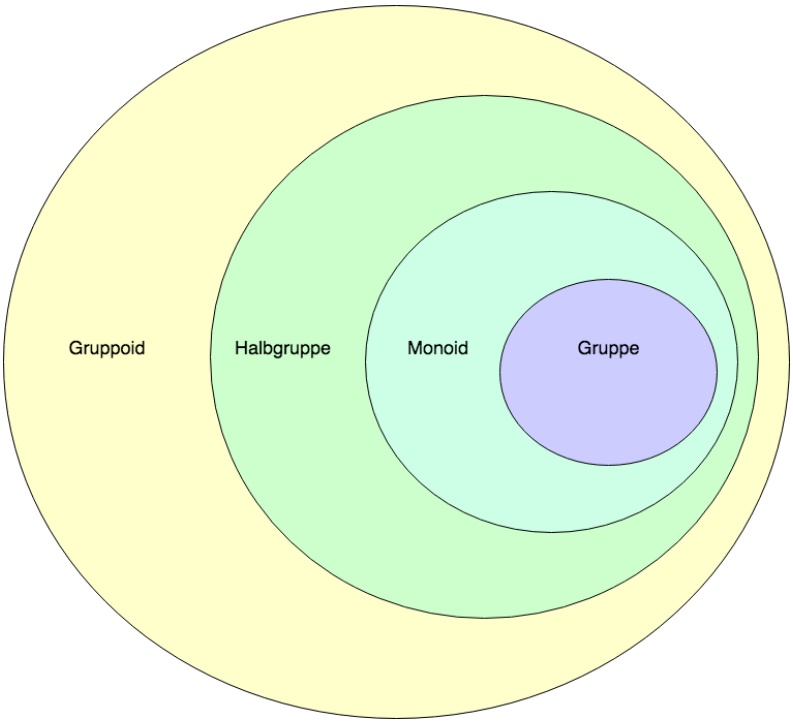
Gruppen, Ringe, Körper

Anton Lammert

Dezember 2018

1 Idee

In vielen Fällen ist es nötig zu wissen, welche Eigenschaften bestimmte Operationen auf einer Menge erfüllen. D.h. ob die Assoziativität, Kommutativität, etc. gilt. Um die Eigenschaften einer Operation $\circ$ auf Elementen x,y einer Menge M formal zu beschreiben, wurden hierfür die Begriffe Gruppoid, Halbgruppe, Monoid sowie Gruppe eingeführt. Gruppoide, Halbgruppen, Monoide und Gruppen bauen aufeinander auf und können hierarchisch dargestellt werden.



Man schreibt formal (M,$\circ$), wobei M die Menge der Elemente, welche verknüpft werden, beschreibt und $\circ$ die Verknüpfung spezifiziert. Die Addition auf den natürlichen Zahlen wird wie folgt beschreiben: $(\mathbb{N}, +)$. Auf die genauen Eigenschaften wird später eingegangen. Da für praktische Rechnungen häufig zwei Operationen vonnöten sind, wird weiterhin zwischen Ringen und Körpern unterschieden. Man beschreibt zwei Operationen $\circ, \diamond$ auf einer Menge M wie folgt: (M, $\circ, \diamond$). Hierbei spielt jedoch die Reihenfolge der Operationen eine Rolle. Auch hierauf wird im weiteren Verlauf eingegangen.

2 Gruppoid

Ein Gruppoid auch Magma, Binar oder Operativ genannt, besteht aus einer Verknüpfung $\circ$ zwischen zwei Elementen x,y einer Menge M, deren Ergebnis erneut Element der Menge M ist.

$$x, y \in M : x \circ y \in M$$

Die Ordnung eines Gruppoids ist gleich der Anzahl der Elemente der Menge bzw. $|M|$.

Gilt weiterhin die Kommutativität also gilt: $a, b \in M : a \circ b = b \circ a$, so bezeichnet man das Gruppoid als abelsch.

Für endliche Mengen werden häufig Verknüpfungstabellen angegeben. Diese besitzen folgende Form:

$\circ$	...	b	...
...	...	...	...
a	...	$a \circ b$	...
...	...	...	...

Ist eine Kommutativität vorhanden, so ist diese symmetrisch bezüglich ihrer Hauptdiagonalen.

Bsp. $(\mathbb{Z}_5, \cdot)$, wobei $\cdot$ der Multiplikation entspricht, ist kommutativ.

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Beispiele für reine Gruppoide sind:

$(\mathbb{Z}, -)$
$(\mathbb{N}, \diamond)$ mit $a \diamond b = a^b$

Kein Gruppoid wäre z.B.:

$(\mathbb{N}, -)$

3 Halbgruppe

Halbgruppen sind Gruppoide, für welche zusätzlich die Assoziativität gilt. D.h. für alle Elemente a, b & $c \in$ M gilt:

$$a \circ (b \circ c) = (a \circ b) \circ c$$

Beispiele für reine Halbgruppen sind:

$(\mathbb{N}, +)$
$(\mathbb{N} \setminus \{1\}, *)$

4 Monoid

Monoide sind Halbgruppen, welche ein neutrales Element bezüglich ihrer Verknüpfung besitzen. Es gibt also genau ein $e \in$ M, für welches gilt:

$$\forall a \in \text{M}: e \circ a = a \circ e = a$$

Die Eindeutigkeit des neutralen Elements kann über einen Gegenteilsbeweis bewiesen werden. In der Regel werden Monoide mit ihrem neutralen Element angegeben. Man schreibt also (M,$\circ, e$), wenn e das neutrale Element ist.

Existiert ein neutrales Element, so gibt es in der Verknüpfungstabelle eine Zeile sowie eine Spalte, in welcher die Werte unverändert sind.

Bsp: $(\mathbb{Z}_5, +)$ wobei $+$ für die Addition steht.

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Zeile 1 sowie Spalte 1 sind unverändert bezüglich a bzw. b.

Beispiele für reine Monoide sind:

$(\mathbb{N}_0, +, 0)$
$(\mathbb{N}, *, 1)$
$(\Sigma^*, \diamond, \varepsilon)$, wobei $\diamond$ die Konkatination, ε der leere String und Σ^* die Menge aller Zeichenketten über dem Alphabeth Σ ist.
$(\mathbb{R}^{n \times n}, \cdot, E)$, wobei $\cdot$ für die Matrixmultiplikation und E für die Einheitsmatrix steht.

5 Gruppe

Gruppen sind Monoide, für welche, zusätzlich zum neutralen Element, für jedes Element ein inverses Element existiert, welches verknüpft mit dem ursprünglichen Element das neutrale Element erzeugt. Sei a^{-1} das inverse Element von a und e das neutrale Element, so gilt:

$$a^{-1} \circ a = a \circ a^{-1} = e$$

Auch hier lässt sich die Eindeutigkeit des Inversen eines Elements a der Menge M durch einen Gegenteilbeweis zeigen.

Weiterhin gilt für alle Gruppen, dass in jeder Zeile und jeder Spalte der Verknüpfungstabelle jedes Element der Menge M genau einmal vorkommt.
Bsp: $(\mathbb{Z}_5 \setminus \{0\}, \cdot)$, wobei $\cdot$ der Multiplikation entspricht.

$\cdot$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Gibt es ein Element a, welches durch seine Potenzen alle Elemente der Gruppe erzeugt, so spricht man auch von einer zyklischen Gruppe und bezeichnet a als Erzeuger.

Alle zyklische Gruppen sind kommutativ bzw. abelsch.

Die Potenz eines Elementes a, welche auch häufig als a^n geschrieben wird, ist wie folgt definiert:

$$(M, \circ), a \in M : a^n = \underbrace{a \circ a ... \circ a}_{n}$$

Die Ordnung eines Elementes $a \in M$ mit dem neutr. Element $e \in M$ ist gleich dem kleinsten $n \in \mathbb{N}$, für welches gilt:

$$a^n = e$$

Sei $(M, \circ)$ eine Gruppe, dann ist $(T, \circ)$ eine Untergruppe, wenn gilt:

$$T \subseteq M \text{ und } (T, \circ) \text{ ist eine Gruppe}$$

Um zu überprüfen, ob es sich bei $(T, \circ)$ um eine Untergruppe handelt, muss $(T, \circ)$ auf Abgeschlossenheit, das neutrale sowie auf die inversen Elemente hin untersucht werden.

Um den Kreis zur Idee des Gruppenkonzeptes zu schließen, kann die Notwendigkeit über die Existenz von Gruppeneigenschaften zum Lösen von Gleichungen an einem Beispiel dargestellt werden.

Gegeben sei die Gleichung: $3 + x = 5$ für die Gruppe $(\mathbb{Z}, +)$.

Zur Lösung der Gleichung wollen wir die Gleichung nach x umstellen.
Da wir jedoch nur die Addition als Operation besitzen, müssen wir uns der Existenz des Inversen Elementes sowie der Assoziativität bedienen.
Wir addieren also auf beiden Seiten das Inverse Element der 3 hinzu.

$$(-3) + 3 + x = (-3) + 5$$

Nun nutzen wir den Fakt, dass $a \circ a^{-1} = a^{-1} \circ a = e$ ist.

$$0 + x = (-3) + 5$$

Dadurch, dass die 0 das neutrale Element bezüglich der Addition ist, gilt:

$$0 + x = x + 0 = x \rightarrow 0 + x = (-3) + 5 \text{ wird zu } x = (-3) + 5.$$

Da $(-3) + 5$ erneut ein Element von $\mathbb{Z}$ ist, können wir den Wert ermitteln und erhalten:

$$x = 2$$

Da in der Theoretische Informatik das Rechnen Modulo einer Menge eine wichtige Rolle spielt, ist es notwendig den Begriff der Äquivalenzrelation, der Nebenklasse sowie des Normalteilers zu klären.
Erst durch diese Eigenschaften ist ein Rechnen Modulo möglich.

Sei $(M, \circ)$ eine Gruppe mit $(T, \circ)$ als Untergruppe, so ist eine Äquivalenzrelation wie folgt definiert:

$$a \sim_{\text{left}} b :\Longleftrightarrow a^{-1} \circ b \in T$$

Da $a^{-1} \circ b \in T$, ist auch $(a^{-1} \circ b)^{-1} = b^{-1} \circ a \in T$, da T eine Gruppe ist.

$$\text{Somit ist } \sim_{\text{left}} \text{ symmetrisch und aus } a \sim_{\text{left}} b \text{ folgt } b \sim_{\text{left}} a.$$

Bsp: Sei $(\mathbb{Z}, +)$ die Gruppe M und $(5\mathbb{Z}, +)$ die Untergruppe T, wobei $5\mathbb{Z}$ für die Vielfachen der 5 in $\mathbb{Z}$ (also ..., -5, 0, 5 , ...) steht.

$$\text{Es gilt: } 6 \sim_{\text{left}} 1 :\Longleftrightarrow -6 + 1 \in T$$

Da -5 ein Element von $5\mathbb{Z}$ ist, ist die 6 äquivalent zur 1, wenn wir Modulo 5 mit der Addition als Operator rechnen.

Die Äquivalenzklasse eines Elementes $a \in M$ ist beschrieben durch:

$$aT := \{a \circ t | t \in T\}$$

aT wird auch als Linksnebenklasse von T bezüglich des Elementes a bezeichnet.

Sei $a \in M$ aus unserem Beispiel gleich 3, so sehen wir, dass die Äquivalenzklasse der 3 der Menge $\{3 + t | t \in T\}$ entspricht. Da T alle Vielfachen der 5 enthält, entspricht die Äquivalenzklasse der 3 also:

$$\{3 + (-n) \cdot 5, 3 + (-n + 1) \cdot 5, ..., 3 + (-5), 3 + 0, 3 + 5, ..., 3 + (n - 1) \cdot 5, 3 + n \cdot 5\}, n \in \mathbb{N}$$

Alle Vielfachen der 5, auf welche 3 addiert wird, befinden sich also in der Äquivalenzklasse der 3.
Da es nur 5 Werte für a gibt, bei welchen sich die Äquivalenzklassen in ihren Elementen voneinander unterscheiden, ist die Menge der Äquivalenzklassen für $(\mathbb{Z}/5\mathbb{Z})$ gleich $\{0T, 1T, 2T, 3T, 4T\}$.

Analog existiert die Äquivalenzrelation

$$a \sim_{\text{right}} b :\Longleftrightarrow a \circ b^{-1} \in T$$

mit der Äquivalenzklasse

$$Ta := \{t \circ a | t \in T\}$$

, welche wir als Rechtsnebenklasse von T bezüglich dem Element a bezeichnen.

Man bezeichnet mit M/T ("M modulo T") die Menge aller Linksnebenklassen, welche auch als Faktorgruppe bezeichnet wird, und mit $T\backslash M$ die Menge aller Rechtsnebenklasse.

Gilt für eine Gruppe:

$$\forall a : aT = Ta$$

so bezeichnet man T als Normalteiler. Man schreibt $T \lhd M$.

Beispiele für Gruppen sind:
$(\mathbb{Z}_p, \cdot)$, wobei p eine Primzahl ist und $\cdot$ für die Multiplikation steht
$(\mathbb{Z}, +)$
$(\mathbb{Z}_n, +)$
$(\mathbb{Q} \setminus \{0\}, \cdot)$, wobei $\cdot$ für die Multiplikation steht.

6 Homomorphismen

Homomorphismen sind Abbildungen, welche die mathematische Struktur erhalten. In der linearen Algebra werden lineare Abbildungen häufig genutzt um Räume zu verformen, ohne die ihnen zu Grunde liegende Struktur zu verändern.

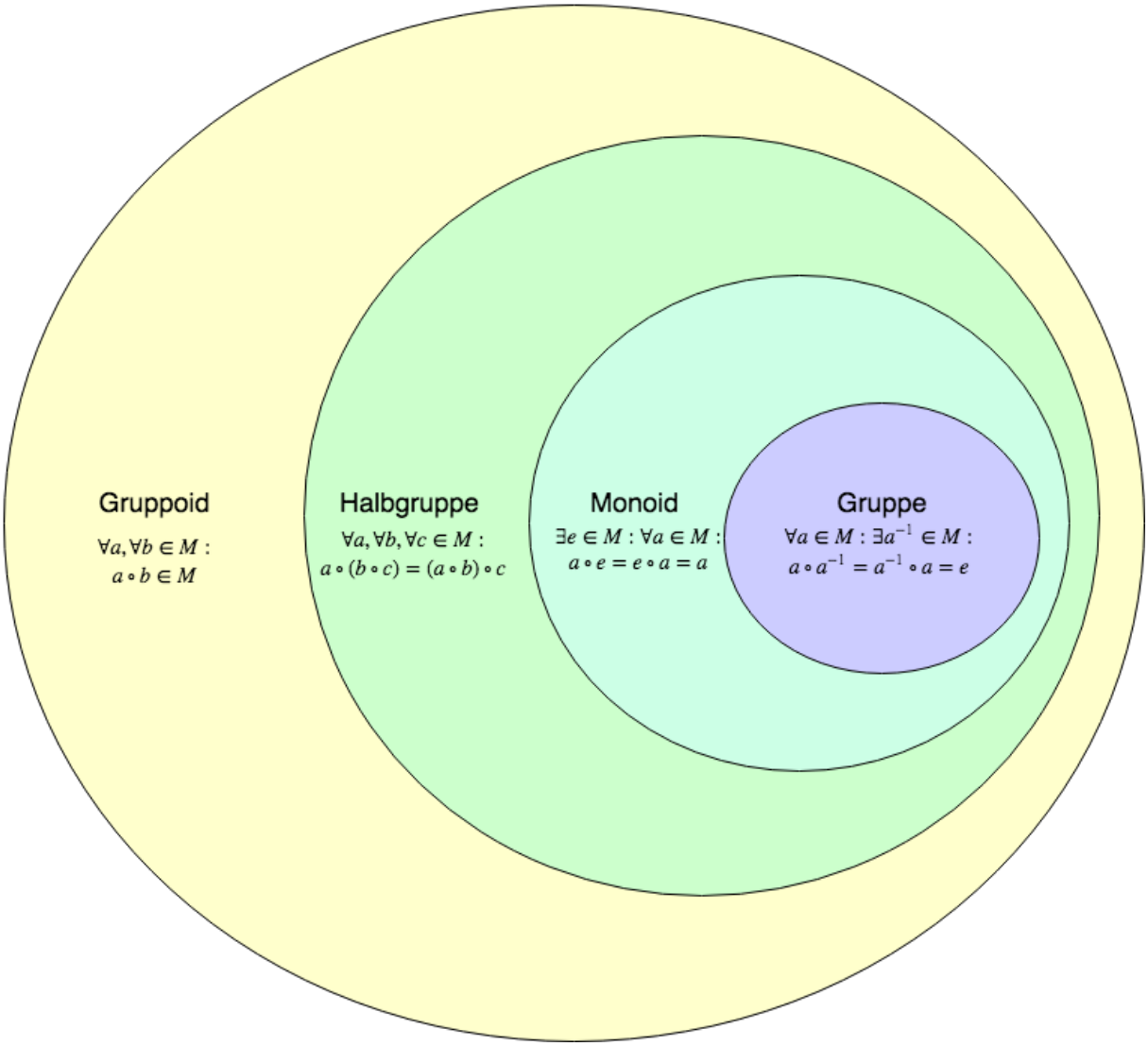
Sind $(M, \circ)$ und $(T, \diamond)$ Halbgruppen, so nennen wir $\tau : M \to T$ eine Abbildung wenn gilt:

$$\forall a, b \in M : \tau(a \circ b) = \tau(a) \diamond \tau(b)$$

Ist diese Abbildung bijektiv, so redet man von einer Isomorphie.

7 Grafik

Zusammenfassend kann man die hierarchische Darstellung um die jeweiligen Eigenschaften erweitern:



8 Ring

Ein Ring besteht aus einer Menge, sowie zwei Verknüpfungen bzw. Operationen. Im Folgenden werden diese Verknüpfungen durch + & $\cdot$ bezeichnet. Mit 0 bezeichnen wir, wenn vorhanden, das neutrale Element der Operation + und mit 1, wenn vorhanden, das neutrale Element der Operation $\cdot$.

Damit es sich bei $(M, +, \cdot)$ um einen Ring handelt, müssen drei Eigenschaften erfüllt sein:

1. $(M, +)$ ist eine kommutative Gruppe
2. $(M, \cdot)$ ist eine Halbgruppe
3. $\forall a, b, c \in M : a \cdot (b + c) = a \cdot b + a \cdot c$ und $(a + b) \cdot c = a \cdot c + b \cdot c$

Es gilt:

$$0 \cdot a = a \cdot 0 = 0$$

Dies kann durch die Gruppeneigenschaft von $(M, +)$ sowie das Distributivgesetz bewiesen werden.

Ist $(M, \cdot)$ ein Monoid, so wird $(R, +, \cdot)$ auch als Ring mit Eins bezeichnet.
Für einen Ring mit Eins gilt:

$$\forall a, b \in M : (-a) \cdot b = a \cdot (-b) = -(a \cdot b)$$

Beispiele für Ringe sind:
$(\mathbb{Z}_k, +, \cdot)$, wobei + für die Addition,$\cdot$ für die Multiplikation und $k \in \mathbb{N}, k \neq$ prim steht.
$(K[X]_{p(x)}, +, \cdot)$, wobei $K[X]_{p(x)}$ die Menge aller Polynome Modulo dem Polynom $p(x)$ ist,
+ für die Addition und $\cdot$ für die Multiplikation steht.

9 Körper

Sei $(M, +, \cdot)$ ein Ring. Ist $(M \setminus \{0\}, \cdot)$ eine kommutative Gruppe, so bezeichnen wir $(M, +, \cdot)$ als Körper.

Gegeben sei die Gleichung $4 + 3 \cdot (x + 1) = 16$ für den Körper $(\mathbb{R}, +, \cdot)$.

Zur Lösung der Gleichung nutzen wir zuerst die Existenz der additiven Inversen.

$$-4 + 4 + 3 \cdot (x + 1) = -4 + 16 \Leftrightarrow 0 + 3 \cdot (x + 1) = 12$$

Durch das Distributivgesetz, sowie die 0 als neutrales Element der Addition erhalten wir:

$$0 + 3 \cdot x + 3 \cdot 1 = 12 \Leftrightarrow 3 \cdot x + 3 = 12$$

Nutzen wir erneut die Existenz der additiven Inversen erhalten wir:

$$3 \cdot x + 3 - 3 = 12 - 3 \Leftrightarrow 3 \cdot x + 0 = 9 \Leftrightarrow 3 \cdot x = 9$$

Nun nutzen wir die Existenz der multiplikativen Inversen.

$$3^{-1} \cdot 3 \cdot x = 3^{-1} \cdot 9 \Leftrightarrow 1 \cdot x = \tfrac{1}{3} \cdot 9 \Leftrightarrow x = 3$$

Hätte es sich bei $(\mathbb{R}, +, \cdot)$ um keinen Körper gehandelt, so hätten wir diese Gleichung nicht lösen können.

Beispiel für Gruppen sind:
$(\mathbb{R}, +, \cdot)$, wobei + für die Addition und $\cdot$ für die Multiplikation steht.
$(Z_p, +, \cdot)$, wobei + für die Addition und $\cdot$ für die Multiplikation steht und p prim ist.