5. Gruppen, Ringe, Körper

5.1. Gruppen

Die Gruppentheorie, als mathematische Disziplin im 19. Jahrhundert entstanden, ist ein Wegbereiter der modernen Mathematik. Beispielsweise folgt die Gruppe, die aus den Drehungen eines regulären n-Ecks in der Ebene um Vielfache des Winkels 360°/n besteht, denselben Gesetzen wie die Addition der ganzen Zahlen modulo n. Neutrales Element – entsprechend der Null bei der Addition – ist die Drehung um einen Winkel von 0° (die Nicht-Drehung).

Gruppen werden in der Mathematik verwendet, um vom Rechnen mit konkreten Zahlen zu abstrahieren (*sprich*: um mit Symbolen anstelle von Zahlen zu rechnen). Entsprechend besteht eine Gruppe aus einer Menge von abstrakten Dingen oder Symbolen und einer „Rechenvorschrift“ (Verknüpfung), die angibt, wie mit diesen Dingen umzugehen ist.
Genauer gesagt: Von einer Gruppe spricht man, falls für eine Menge zusammen mit einer Verknüpfung je zweier Elemente dieser Menge, zum Beispiel „$a \times b$“, die folgenden weiteren Anforderungen erfüllt sind:
Die Verknüpfung zweier Elemente der Menge ist wiederum ein Element derselben Menge (*Abgeschlossenheit*).
Die Klammerung beim Ausrechnen ist unerheblich (*Assoziativität*): $a\times(b\times c) = (a\times b)\times c$ für alle a,b,c.
Es gibt ein Element e in der Menge, das nichts bewirkt (*neutrales Element*): $a \times e = e \times a = a$ für alle a.
Zu jedem Element a gibt es ein „Spiegelbild“ (*inverses Element*) a^* mit der Eigenschaft, beim Verknüpfen mit a das neutrale Element zu ergeben: $a \times a^* = a^* \times a = e$.
Spezialfall: Wenn man zudem noch die Operanden vertauschen darf, also stets $a \times b = b \times a$ gilt (*Kommutativität*), dann liegt eine abelsche oder kommutative Gruppe vor.

Beispiele für abelsche Gruppen sind

- die ganzen Zahlen $\mathbb{Z}$ mit der Addition „+“ als Verknüpfung und der Null als neutralem Element,
- die rationalen Zahlen $\mathbb{Q}$ ohne Null mit der Multiplikation „×“ als Verknüpfung und der Eins als neutralem Element. Die Null muss hierbei ausgeschlossen werden, da sie kein inverses Element besitzt: „1/0“ ist nicht definiert.

Die sehr allgemeine Definition von Gruppen ermöglicht es, nicht nur Mengen von Zahlen mit entsprechenden Operationen als Gruppen aufzufassen, sondern auch andere abstrakte Dinge und Symbole, die die geforderten Eigenschaften erfüllen wie zum Beispiel die Menge der Drehungen und Spiegelungen (Symmetrietransformationen), durch die ein n-Eck auf sich selbst abgebildet wird, mit der Hintereinanderausführung der Transformationen als Verknüpfung.

5.1.1. Mathematische Definition des Gruppenbegriffs

Ein Paar $(G, *)$ mit einer Menge G und einer inneren zweistelligen Verknüpfung
$*: G \times G \to G, (a,b) \mapsto a * b$ heißt ***Gruppe***, wenn folgende ***Axiome*** erfüllt sind:

- *Abgeschlossenheit:* Für alle Gruppenelemente a und b gilt: $(a * b) \in G$
- *Assoziativität*: Für alle Gruppenelemente a, b und c gilt: $(a * b) * c = a * (b * c)$.
- *Neutrales Element*: Es gibt ein neutrales Element $e \in G$, mit dem für alle Gruppenelemente a gilt: $a * e = e * a = a$.
- *Inverses Element*: Zu jedem Gruppenelement a existiert ein Element $a^{-1} \in G$ mit $a*a^{-1} = a^{-1}*a = e$.

Eine Gruppe $(G, *)$ heißt *abelsch* oder *kommutativ*, wenn die Verknüpfung $*$ symmetrisch ist, d. h., wenn zusätzlich das folgende Axiom erfüllt ist:

- *Kommutativität*: Für alle Gruppenelemente a und b gilt $a * b = b * a$.

5.1.2. Bemerkungen zur Notation

Häufig wird für die Verknüpfung $*$ das Symbol $\cdot$ benutzt, man spricht dann von einer multiplikativ geschriebenen Gruppe. Das neutrale Element heißt dann *Einselement* und wird durch 1 symbolisiert. Wie auch bei der gewöhnlichen Multiplikation üblich, kann in vielen Situationen der Malpunkt weggelassen werden.
Die Gruppeneigenschaften lassen sich auch additiv notieren, indem für die Verknüpfung $*$ das Symbol + benutzt wird. Das neutrale Element heißt dann Nullelement und wird durch 0 symbolisiert. Das zum Gruppenelement a inverse Element wird in einer additiv geschriebenen Gruppe nicht durch a^{-1}, sondern durch $-a$ symbolisiert. Üblich ist die additive Schreibweise bei abelschen Gruppen, während nicht abelsche oder beliebige Gruppen zumeist multiplikativ geschrieben werden.
Ist die Verknüpfung klar, so schreibt man für die Gruppe häufig nur G.

5.1.3. Ordnung einer Gruppe

Die Mächtigkeit (Kardinalität) $|G|$ der Trägermenge der Gruppe nennt man *Ordnung der Gruppe* oder kurz *Gruppenordnung*. Für endliche Mengen ist dies einfach die Anzahl der Elemente.

5.1.4. Ordnung von Elementen

Ergibt ein Element a der Gruppe, endlich viele Male n mit sich selbst verknüpft, das neutrale Element 1, d. h. gilt für ein geeignetes n: $a^n = 1$, so nennt man das kleinste derartige n die Ordnung des Elements a. Falls kein solches n existiert, sagt man, dass a unendliche Ordnung hat. In beiden Fällen entspricht die Ordnung des Elements der Ordnung der von ihm erzeugten Untergruppe.
Davon ausgehend kann man zeigen, dass die Ordnung jedes Elements einer endlichen Gruppe endlich ist und die Gruppenordnung teilt (Satz von Lagrange).

5.1.5. Untergruppen

Ist H eine Teilmenge der Trägermenge G einer Gruppe $(G, *)$ und ist $(H, *)$ selbst eine Gruppe, so nennt man H eine Untergruppe von G.
Hierzu ein wichtiger Satz (Satz von Lagrange): Die Ordnung (Anzahl der Elemente) jeder Untergruppe H einer endlichen Gruppe G ist ein Teiler der Ordnung der Gruppe G. Ist speziell $|G|$ eine Primzahl, dann hat G nur die (trivialen) Untergruppen $\{e\}$ (bestehend aus dem neutralen Element) und G selbst.

5.1.6. Beispiele für Gruppen

- Alle Zahlenbereiche (außer $\mathbb{N}$) bezüglich der Addition
- $\mathbb{Q}\backslash\{0\}$, $\mathbb{R}\backslash\{0\}$ und $\mathbb{C}\backslash\{0\}$ bezüglich Multiplikation
- $S_M := \{f: M \longrightarrow M \wedge f \text{ bijektiv}\}$ bezüglich der Hintereinanderausführung von Abbildungen (symmetrische Gruppe)
- Alle regulären Matrizen über den reellen bzw. komplexen Zahlen bezüglich Multiplikation
- Ist M = {1,2,3}, so kann man die Menge aller bijektiven Abbildungen von M auf M als Gruppe der ***Permutationen*** (Vertauschungen der Anordnung der Elemente) betrachten.

5.1.7. Halbgruppe und Monoid

Es gibt auch Verallgemeinerungen der Gruppentheorie. Dabei wird auf einzelne Axiome der Gruppe verzichtet.
Beispiele dafür sind die Definitionen der Halbgruppe und des Monoids:
Für Halbgruppen wird nur die Assoziativität verlangt.
Existiert in einer Halbgruppe ein neutrales Element, so spricht man von einem Monoid.

Beispiele und Gegenbeispiele

$(\mathbb{N}_0, +, 0)$ ist ein Monoid

$(\mathbb{N}, \cdot, 1)$	ist ein Monoid.
$(\mathbb{N}, :, 1)$	ist kein Monoid, da die Division nicht assoziativ ist.
$(\mathbb{Z}, +, 0)$	(die Menge der ganzen Zahlen mit der Addition) ist ein Monoid
$(\mathbb{Z}, -, 0)$	ist kein Monoid, da die Subtraktion nicht assoziativ ist.
$(\mathbb{R}^{n\times n}, \cdot, E)$	(die Menge der n×n-Matrizen mit der üblichen Matrizenmultiplikation und der Einheitsmatrix *E*) ist ein nichtkommutatives Monoid.
$(\mathbb{R}^3, \times, \vec{0})$	(der dreidimensionale reelle Raum mit dem Vektorprodukt) ist kein Monoid, da das Assoziativgesetz verletzt ist: Bezeichnen wir mit e_i den i-ten Einheitsvektor, so ist $(e_1 \times e_1) \times e_2 = 0$, aber $e_1 \times (e_1 \times e_2) = -e_2$.
$(n\mathbb{Z}, +, 0)$	(die Menge der Vielfachen der ganzen Zahl n mit der Addition) ist ein Monoid.
$(\mathbb{Q}_+, +, 0)$	(die Menge der nichtnegativen rationalen Zahlen mit der Addition) ist ein Monoid.

5.2. Ringe

Ein Ring ist eine Menge R mit zwei inneren binären Verknüpfungen „+“ und „·“, sodass gilt:

- (R, +) ist eine abelsche Gruppe,
- (R, ·) ist eine Halbgruppe,
- Die Distributivgesetze $a \cdot (b + c) = a \cdot b + a \cdot c$ und $(a + b) \cdot c = a \cdot c + b \cdot c$ sind für alle *a*,*b*,*c* ∈ *R* erfüllt.

Das neutrale Element 0 von (R, +) heißt Nullelement von R.
Ein Ring heißt kommutativ, falls er bezüglich der Multiplikation kommutativ ist.

5.2.1. Unter-/Oberring

Eine nichtleere Untermenge U eines Ringes R heißt Unterring von R, wenn U zusammen mit den beiden auf U eingeschränkten Verknüpfungen von R wieder ein Ring ist.
Ein Ring S heißt Oberring oder Erweiterung eines Ringes R, wenn R ein Unterring von S ist.

5.2.2. Einselement

Besitzt ein Ring ein neutrales Element bezüglich der Multiplikation, so nennt man dieses die Eins oder das Einselement des Ringes. Dieses Element wird meist mit 1 bezeichnet und hat die Eigenschaft
$1 \cdot a = a \cdot 1 = a \quad \forall a \in R.$
Ein Ring mit Einselement (oder kurz: Ring mit Eins) wird auch **unitärer Ring** genannt.

5.2.3. Abschwächung der Axiome

Wenn ein Ring eine Eins besitzt, dann muss nicht gefordert werden, dass die Addition kommutativ ist. Diese Eigenschaft folgt dann aus den restlichen Ringaxiomen. Für alle *a*,*b* ∈ *R* gilt:
$$a + a + b + b = 1 \cdot a + 1 \cdot a + 1 \cdot b + 1 \cdot b = (1+1) \cdot a + (1+1) \cdot b = (1+1) \cdot (a+b) =$$
$$1 \cdot (a+b) + 1 \cdot (a+b) = a + b + a + b$$
Addiert man diese Gleichung von links mit $(-a)$ und von rechts mit $(-b)$, so erhält man:
$a + b = b + a$.
Insgesamt wurden mit Ausnahme des Assoziativgesetzes der Multiplikation alle Axiome eines unitären Rings benutzt. Die Argumentation ist also auch für nicht-assoziative unitäre Ringe gültig.

5.2.4. Invertierbarkeit, Einheit

Existiert in einem Ring mit Eins zu einem Element *x* ein Element *y*, so dass $y \cdot x = 1$ (bzw. $x \cdot y = 1$) gilt, so nennt man *y* ein Linksinverses (bzw. Rechtsinverses) von *x*. Besitzt *x* sowohl Links- als auch Rechtsinverses, so nennt man *x* invertierbar oder Einheit des Ringes. Die Menge der Einheiten eines Ringes R mit

Eins wird gewöhnlich mit R* bezeichnet. R* bildet bezüglich der Ringmultiplikation eine Gruppe – die Einheitengruppe des Ringes.
In kommutativen Ringen mit Eins (insbesondere Integritätsringen) definiert man alternativ die Einheiten auch als diejenigen Elemente, die die Eins teilen. Dass *x* die Eins teilt, heißt nämlich dass es *y* gibt mit $y \cdot x = x \cdot y = 1$. Man sieht, dass die Eigenschaft, Teiler von Eins zu sein, und die Eigenschaft, invertierbar zu sein, hier dasselbe bedeuten. Diese Alternativdefinition funktioniert aber erst in kommutativen Ringen, da erst dort die Teilbarkeit erklärt wird.

5.2.5. Beispiele

Das wichtigste Beispiel eines Ringes ist die Menge $(\mathbb{Z},+,\cdot)$ der ganzen Zahlen mit der üblichen Addition und Multiplikation. Es handelt sich dabei um einen nullteilerfreien kommutativen Ring mit Einselement, also einen Integritätsring.

Ebenso bildet $(\mathbb{Q},+,\cdot)$ der rationalen Zahlen mit der üblichen Addition und Multiplikation einen Ring. Da in diesem Fall nicht nur $(\mathbb{Q},+)$, sondern auch $(\mathbb{Q}\backslash\{0\},\cdot)$ eine abelsche Gruppe bildet, liegt sogar ein Körper vor; es handelt sich dabei um den Quotientenkörper des Integritätsringes $(\mathbb{Z},+,\cdot)$.

Kein Ring ist die Menge $(\mathbb{N},+,\cdot)$ der natürlichen Zahlen mit der üblichen Addition und Multiplikation, da die Addition über den natürlichen Zahlen nicht invertierbar ist.

Weitere wichtige Beispiele von Ringen sind

- Restklassenringe,
- Polynomringe und
- quadratische Matrizen mit fixer Dimension.

Insbesondere Restklassenringe und quadratische Matrizen liefern Beispiele von Ringen, die nicht nullteilerfrei sind.
Quadratische Matrizen sind darüber hinaus ein Beispiel eines Rings, bei dem die Multiplikation nicht kommutativ ist.

Ein Beispiel eines Rings ohne Eins sind die geraden ganzen Zahlen, ebenso bilden alle ganzen Zahlen, die Vielfache einer gegebenen ganzen Zahl größer eins sind, einen Ring ohne Eins.
Allgemein ist jedes echte **Ideal** eines Rings ein Ring ohne Eins.

Aber was ist ein **Ideal**?

Um auch für *nichtkommutative* Ringe geeignete Begriffe zu haben, unterscheidet man zwischen Links-, Rechtsidealen und zweiseitigen Idealen:
Es sei I eine Teilmenge eines Ringes R. I heißt dann Linksideal, wenn gilt:

1: Die Null des Ringes liegt in I.

2: $\forall a,b \in I : (a-b) \in I.$

3L: Für jedes $a \in I$ und $r \in R$ gilt: $r \cdot a \in I$.

Entsprechend ist I ein Rechtsideal, wenn für I neben 1 und 2 auch gilt:

3R: Für jedes $a \in I$ und $r \in R$ gilt: $a \cdot r \in I$.

I nennt man schließlich zweiseitiges Ideal oder nur kurz **Ideal**, falls I Links- und Rechtsideal ist, also 1, 2, 3L und 3R erfüllt.

5.3. Körper

Ein Körper ist im mathematischen Teilgebiet der Algebra eine ausgezeichnete algebraische Struktur, in der die Addition, Subtraktion, Multiplikation und Division wie bei den „normalen“ (reellen) Zahlen durchgeführt werden können.
Die Bezeichnung Körper wurde im 19. Jahrhundert von Richard Dedekind eingeführt.

5.3.1. Allgemeine Definition

Ein Tripel (K,+,·), bestehend aus einer Menge K und zwei binären Verknüpfungen „ + “ und „·“ (die üblicherweise Addition und Multiplikation genannt werden), ist genau dann ein Körper, wenn folgende Eigenschaften erfüllt sind:

- (K,+) ist eine abelsche Gruppe (mit Neutralelement 0)
- ($K \setminus \{0\}$,·) ist eine abelsche Gruppe (mit Neutralelement 1)
- $a \cdot (b + c) = a \cdot b + a \cdot c$ und $(a + b) \cdot c = a \cdot c + b \cdot c$ (Distributivgesetz)

5.3.2. Einzelaufzählung der benötigten Axiome

Ein Körper muss also folgende Einzelaxiome erfüllen:

Additive Eigenschaften:

- $a + (b + c) = (a + b) + c$ (Assoziativgesetz)
- $a + b = b + a$ (Kommutativgesetz)
- Es gibt ein Element $0 \in K$ mit $0 + a = a$ (neutrales Element)
- Zu jedem $a \in K$ existiert das additive Inverse $(-a)$ mit $(-a) + a = 0$

Multiplikative Eigenschaften:

- $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ (Assoziativgesetz)
- $a \cdot b = b \cdot a$ (Kommutativgesetz)
- Es gibt ein Element $1 \in K$ mit $1 \cdot a = a$ (neutrales Element), und es ist $1 \neq 0$.
- Zu jedem $a \in K \setminus \{0\}$ existiert das multiplikative Inverse a^{-1} mit $a^{-1} \cdot a = 1$

Zusammenspiel von additiver und multiplikativer Struktur:

- $a \cdot (b + c) = a \cdot b + a \cdot c$ (Links-Distributivgesetz)

Das Rechts-Distributivgesetz $(a + b) \cdot c = a \cdot c + b \cdot c$ folgt dann aus den übrigen Eigenschaften:
$(a + b) \cdot c = c \cdot (a + b) = c \cdot a + c \cdot b = a \cdot c + b \cdot c$

5.3.3. Definition als spezieller Ring

Ein kommutativer unitärer Ring, der nicht der Nullring ist, heißt ein Körper, wenn in ihm jedes von Null verschiedene Element multiplikativ invertierbar ist.
Anders formuliert, ist ein Körper ein kommutativer unitärer Ring K, in dem die Einheitengruppe K^* gleich $K \setminus \{0\}$, also maximal groß, ist.

Bemerkungen

Die Definition sorgt dafür, dass in einem Körper in der "gewohnten" Weise Addition, Subtraktion und Multiplikation funktionieren (und die Division mit Ausnahme der verbotenen Division durch 0):
Das Inverse von a bezüglich der Addition ist $-a$ und wird meist das additiv Inverse zu a oder auch das Negative von a genannt.

Das Inverse von a bezüglich der Multiplikation ist a^{-1} und wird das (multiplikativ) Inverse zu oder der Kehrwert von a genannt.
0 ist das einzige Element des Körpers, das keinen Kehrwert hat, die multiplikative Gruppe eines Körpers ist also $K^\times = K \setminus \{0\}$.

Anmerkung: Die Bildung des Negativen eines Elementes hat nichts mit der Frage zu tun, ob das Element selbst negativ ist; beispielsweise ist das Negative der reellen Zahl −2 die positive Zahl 2. In einem allgemeinen Körper gibt es keinen Begriff von negativen oder positiven Elementen. (Siehe auch geordneter Körper.)

5.3.4. Verallgemeinerung: Schiefkörper

Verzichtet man auf die Bedingung, dass die Multiplikation kommutativ ist, so gelangt man zur Struktur des Schiefkörpers. Es gibt jedoch auch Autoren, die für einen Schiefkörper explizit voraussetzen, dass die Multiplikation nicht kommutativ ist. In diesem Fall ist ein Körper nicht mehr zugleich Schiefkörper. Ein Beispiel ist der Schiefkörper der *Quaternionen*, der kein Körper ist.
Andererseits gibt es Autoren, so Bourbaki, die Schiefkörper als Körper und die hier besprochenen Körper als kommutative Körper bezeichnen.

5.3.5. Eigenschaften

- Es gibt genau eine „0“ (Null-Element, neutrales Element bzgl. der Körper-Addition) und eine „1“ (Eins-Element, neutrales Element bzgl. der Körper-Multiplikation) in einem Körper.
- Jeder Körper ist ein Ring. Die Eigenschaften der multiplikativen Gruppe heben den Körper aus den Ringen heraus. Wenn die Kommutativität der multiplikativen Gruppe nicht gefordert wird, erhält man den Begriff des Schiefkörpers.
- Jeder Körper ist ein Vektorraum über sich selbst (das heißt mit sich selbst als zugrundeliegendem Skalarkörper).
- Jeder Körper ist nullteilerfrei. Das heißt, dass ein Produkt zweier Elemente des Körpers genau dann 0 ist, wenn mindestens einer der beteiligten Faktoren 0 ist.

5.3.6. Beispiele

Bekannte Beispiele für Körper sind

- die Menge der rationalen Zahlen $(\mathbb{Q},+,\cdot)$,
- die Menge der reellen Zahlen $(\mathbb{R},+,\cdot)$ und
- die Menge der komplexen Zahlen $(\mathbb{C},+,\cdot)$

jeweils mit der üblichen Addition und Multiplikation.

Weitere Beispiele sind

- endliche Körper und
- die Körper der *p-adischen* Zahlen.

Kein Beispiel für einen Körper ist die Menge der ganzen Zahlen $(\mathbb{Z},+,\cdot)$: Zwar ist $(\mathbb{Z},+)$ eine Gruppe mit neutralem Element 0 und jedes $a \in \mathbb{Z}$ besitzt das additive Inverse $-a$, aber $(\mathbb{Z} \setminus \{0\},\cdot)$ ist keine Gruppe. Immerhin ist 1 das neutrale Element, aber außer zu 1 und −1 gibt es keine multiplikativen Inversen (zum Beispiel ist $3^{-1} = 1/3$ keine ganze, sondern eine echt rationale Zahl). Die ganzen Zahlen bilden lediglich einen Integritätsring, dessen Quotientenkörper die rationalen Zahlen sind.

Ein Beispiel für einen **endlichen Körper** ist der Restklassenkörper $\mathbb{Z}_5$. Nachfolgend sind die Additionstabelle und die Multiplikationstabelle für den Körper $\mathbb{Z}_5$ angegeben.
($\mathbb{Z}_5$ ist der Körper der Restklassen modulo 5 im Bereich der ganzen Zahlen $\mathbb{Z}$!)

Additionstabelle

+	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

Multiplikationstabelle

*	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