

## §8 Gruppen und Körper

**(8.1) Definition:** Eine *Gruppe*  $G$  ist eine Menge zusammen mit einer Verknüpfung, die jedem Paar  $(a,b)$  von Elementen aus  $G$  ein weiteres Element  $a \cdot b$  aus  $G$  zuordnet, so dass die folgenden drei Axiome erfüllt sind:

1°  $(a \cdot b) \cdot c = a \cdot (b \cdot c)$  für alle  $a, b, c$  aus  $G$ . („Assoziativgesetz“)

2° Es gibt  $n$  aus  $G$  mit  $a \cdot n = a = n \cdot a$ . ( $n$  heißt *neutrales Element*.)

3° Zu jedem  $a$  aus  $G$  existiert  $a^*$  aus  $G$  mit  $a \cdot a^* = n$ . ( $a^*$  heißt *inverses Element* oder *Inverse* zu  $a$ .)

Die Gruppe heißt *abelsch*, wenn außerdem

4°  $a \cdot b = b \cdot a$  für alle  $a, b$  aus  $G$ .

Folie 1

## Kapitel II, §8

**(8.2) Beispiele:**

1°  $\mathbf{Z}$ , die Menge der ganzen Zahlen, mit  $+$  anstelle von  $\cdot$ :  $n = 0$  und  $a^* = -a$ .

2° Man beachte:  $\mathbf{N}$  mit  $+$  ist keine Gruppe, weil es zu positiven ganzen Zahlen  $a$  keine Inverse  $-a$  in  $\mathbf{N}$  gibt.

3° Analog zu 1°:  $\mathbf{Q}, \mathbf{R}, \mathbf{C}$  mit  $+$  ist abelsche Gruppe.

4°  $\mathbf{R}_+$  mit der Multiplikation ist ebenfalls eine abelsche Gruppe:  $n = 1$  und  $a^* = a^{-1}$ . Ebenso:  $\mathbf{R} \setminus \{0\}$ .

5° Weitere Beispiele sind alle  $T$  aus §7, also die Translationen zu einem Translationsraum  $(A, T, t)$ .

6° Eine zweielementige Gruppe (die Gruppe zum Modell 1 in Beispiel 7.3.1):

$G = \{0, 1\}$  mit  $0+0 = 1+1 = 0$  und  $0+1 = 1+0 = 1$ .

**(8.3) Bemerkungen, Notationen:**

1° Die Verknüpfung einer Gruppe heißt auch *Gruppenoperation* oder (*Gruppen-*) *Multiplikation*. Sie wird auch kurz  $ab$  statt

Folie 2

$a \cdot b$  geschrieben. Die grundlegenden Axiome haben dann die Form:  
 $(ab)c = a(bc)$ ,  $an = na = a$ ,  $a \cdot a^{-1} = a^{-1} \cdot a = e$ .

Das neutrale Element schreibt man auch als 1 und nennt es *Einselement*. Die Inverse schreibt man auch als  $a^{-1}$ .

Im abelschen Fall schreibt man auch  $a+b$  anstelle von  $a \cdot b$  und man spricht von einer *abelschen additiven Gruppe*. Das neutrale Element  $e$  wird dann meist als 0 geschrieben und dann auch als Null (-element) bezeichnet,  $a^{-1}$  wird als  $-a$  geschrieben und  $a \cdot b$  als Abkürzung von  $a+(-b)$ .

2° Das Assoziativgesetz  $(ab)c = a(bc)$  erlaubt die Definition  $abc := (ab)c = a(bc)$  unabhängig von der Klammerung.

Analog hat man für 4 Elemente den klammerfreien Ausdruck  $abcd$ . Entsprechend für beliebig (aber endlich) viele Elemente (Induktion!)

3° *Potenzen*:  $a^0 := e$ ,  $a^{(n+1)} := aa^n$  (rekursive Definition für natürliche Zahlen  $n$ ). Und  $a^{-n} := (a^n)^{-1}$ . Dann gelten die Regeln:

Folie 3

$$a^n a^m = a^{n+m}, (a^n)^m = a^{nm}.$$

4° Allgemeiner lassen sich endliche Summen oder Produkte mit beliebigen Gruppenelementen bilden:

$$\prod_{i=1}^n a_i \text{ oder } \sum_{i=1}^n a_i.$$

**(8.4) Äquivalenzsatz für Gruppen:** Es sei auf der nichtleeren Menge  $G$  eine Verknüpfung gegeben, die dem Assoziativgesetz genügt:  $(ab)c = a(bc)$ . Behauptung:

$G$  ist genau dann eine Gruppe, wenn für alle  $a, b$  aus  $G$  die Gleichungen  $ax = b$  und  $ya = b$  stets Lösungen in  $G$  haben.

**(8.5) Folgerungen:**  $G$  sei Gruppe mit dem neutralen Element  $e$ . Dann gilt für alle  $a, b, c$  aus  $G$ :

1° (*Kürzungsregel*) Aus  $ab = ac$  folgt  $b = c$  und aus  $ab = cb$  folgt  $a = c$ .

Folie 4

2°  $ax = b$  und  $ya = b$  sind eindeutig lösbar.

3° Die Inverse  $a^{-1}$  zu  $a$  ist eindeutig bestimmt.

4°  $e$  ist eindeutig bestimmt.

**(8.6) Beispiel:** Sei  $M$  eine Menge. Die Menge  $S(M)$  der bijektiven Abbildungen von  $M$  nach  $M$  bildet mit der Identität  $\text{id}$  als neutralem Element eine Gruppe.

$S(M)$  ist nicht abelsch, wenn  $M$  drei verschiedene Elemente enthält.

**(8.7) Beispiel:** Die Menge  $E_{(n)}$  der  $n$ -ten Einheitswurzeln bildet eine abelsche Gruppe bezüglich der Multiplikation: Die *zyklische* Gruppe der Ordnung  $n$ .

**(8.8) Definition:** (Homomorphismus) Ein *Homomorphismus* zwischen den Gruppen  $G$  und  $H$  ist eine Abbildung

$$f : G \rightarrow H$$

mit  $f(ab) = f(a)f(b)$  für alle  $a, b$  aus  $G$ .

Folie 5

Ein Homomorphismus  $f$  ist Isomorphismus, wenn  $f$  bijektiv ist.

**Beispiele:**  $f(a) := 2a$ ;  $g(a) := \exp(a)$  für  $a$  aus  $\mathbf{R}$ .  $f$  und  $g$  sind Isomorphismen von  $\mathbf{R}$  nach  $\mathbf{R}$  bzw. von  $\mathbf{R}$  nach  $\mathbf{R}_+$ .

**(8.9) Lemma:** Für einen Homomorphismus  $f$  von Gruppen gilt:

1°  $f(e)$  ist das neutrale Element von  $H$ , wenn  $e$  das neutrale Element von  $G$  ist.

2°  $f(a^{-1})$  ist die Inverse zu  $f(a)$  für alle  $a$  aus  $G$ :  $[f(a)]^{-1} = f(a^{-1})$

3° Sei  $f$  ein Isomorphismus von Gruppen, dann ist die Umkehrabbildung ein Homomorphismus.

**(8.10) Definition:** (Untergruppen) Eine Teilmenge  $U$  einer Gruppe  $G$  ist eine Untergruppe, wenn  $U$  bezüglich der restringierten Verknüpfung  $\cdot, \dots$ ,  $a, b$  aus  $U$ , eine Gruppe ist.

Folie 6

**(8.11) Lemma:** Eine Teilmenge  $U$  einer Gruppe  $G$  ist genau dann eine Untergruppe, wenn gilt: Für alle  $a, b$  aus  $U$  sind auch  $ab$  und  $a^{-1}$  Elemente aus  $U$ .

**(8.12) Lemma:** Für einen Homomorphismus  $f : G \rightarrow H$  sei

$$\text{Ker } f := \{a : f(a) = e\} = f^{-1}(e),$$

$$\text{Im } f := \{f(a) : a \text{ aus } G\} = f(G).$$

Es gilt:

1°  $\text{Im } f$  ist Untergruppe von  $H$ .

2°  $\text{Ker } f$  ist Untergruppe von  $G$ .

3°  $f$  ist genau dann injektiv, wenn  $\text{Ker } f = \{e\}$  gilt.

Für den Kern  $\text{Ker } f$  eines Homomorphismus gilt außerdem: Für alle  $u$  aus  $\text{Ker } f$  und alle  $a$  aus  $G$  ist  $a^{-1}ua$  wieder ein Element von  $\text{Ker } f$ .  $\text{Ker } f$  ist also ein Normalteiler:

**(8.13) Definition:** Eine Untergruppe  $U$  einer Gruppe  $G$  ist ein *Normalteiler* von  $G$ , wenn für alle  $u$  aus  $U$  und alle  $a$  aus  $G$   $a^{-1}ua$  wieder ein Element von  $U$  ist.

**(8.14) Definition:** Ein Körper  $K$  ist eine additive abelsche Gruppe, zu der es eine Multiplikation gibt mit den folgenden Eigenschaften:

1°  $K \setminus \{0\}$  ist eine abelsche Gruppe bezüglich der Multiplikation.

$$2^\circ a(b+c) = ab + ac \text{ für alle } a, b, c \text{ aus } K.$$

**(8.15) Beispiele:** 1°  $\mathbf{R}$  und  $\mathbf{Q}$ , und dazu  $\mathbf{C}$ .  $\mathbf{Z}$  ist aber nicht Körper.

2° Die zweielementige Gruppe aus 8.2.6°:  $G = \{0, 1\}$  mit  $0+0 = 1+1 = 0$ ,  $0+1 = 1+0 = 1$  und  $0 \cdot 0 = 0 \cdot 1 = 1 \cdot 0 = 0$ ,  $1 \cdot 1 = 1$ .

3° Der Körper mit 3 Elementen.

**(8.16) Definition:** Unterkörper, Homomorphismus, Isomorphismus analog zu Gruppen.