Def. (Gruppe)

Eine Gruppe $(G, \cdot)$ ist eine Menge G zusammen mit einer Verknüpfung

$\cdot : G \times G \to G$

so dass die folgenden Eigenschaften erfüllt sind:

(i) $\forall\, a, b, c \in G: \quad (a \cdot b) \cdot c = a \cdot (b \cdot c)$

(Assoziativität)

(ii) $\exists\, e \in G\ \forall a \in G: \quad a \cdot e = a = e \cdot a$

(Existenz des neutralen Elements)

(iii) $\forall a \in G\ \exists\, b \in G: \quad a \cdot b = e = b \cdot a$

(Existenz des inversen Elements)

Gilt zusätzlich

(iv) $\forall\, a, b \in G: \quad a \cdot b = b \cdot a$

(Kommutativität)

so heißt die Gruppe kommutativ oder abelsch.

Bem.:

(1) Das Element $e \in G$ in (ii) ist eindeutig bestimmt und heißt neutrales Element von G.

(2) Das Element $b \in G$ in (iii) ist eindeutig bestimmt und heißt inverses Element von a. Schreibweis $b = a^{-1}$

Bsp.:

$(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +)$ sind kommutative Gruppen mit $e = 0$ und $a^{-1} = -a$

$(a + 0 = a = 0 + a \ , \quad a + (-a) = 0 = (-a) + a.)$

$(\mathbb{R} \setminus \{0\}, \cdot)$ ist eine Gruppe mit $e = 1$ und $a^{-1} = \frac{1}{a}$

$(a \cdot 1 = a = 1 \cdot a \ , \quad a \cdot \frac{1}{a} = 1 = \frac{1}{a} \cdot a$

Satz (Wichtige Rechenregeln für Gruppen)

Sei $(G,\cdot)$ eine Gruppe. Dann gilt:

(i) $\forall a,b,c \in G: \quad a = b \Leftrightarrow a\cdot c = b\cdot c \quad \wedge \quad a = b \Leftrightarrow c\cdot a = c\cdot b$

(ii) $\forall a \in G: \quad a\cdot a^{-1} = e = a^{-1}\cdot a$

(iii) $\forall a,b \in G: \quad (a\cdot b)^{-1} = b^{-1}\cdot a^{-1}$

Def. (Potenzen in Gruppen)

Sei $(G,\cdot)$ eine Gruppe. Für alle $a \in G$ und $n \in \mathbb{N}$ def. man:

(i) $a^0 := e$

(ii) $a^n := \underbrace{a\cdot a\cdot \ldots \cdot a}_{n\text{-mal}}$

(iii) $a^{-n} := (a^n)^{-1}$

Satz (Potenzgesetze in Gruppen)

Sei $(G,\cdot)$ eine Gruppe.

Für alle $a \in G$ und alle $n,m \in \mathbb{Z}$ gilt:

(i) $a^n \cdot a^m = a^{n+m}$

(ii) $(a^n)^m = a^{n\cdot m} = (a^m)^n$

(iii) $a^{-n} = (a^{-1})^n$

Bem:

Die Regel $a^n \cdot b^n = (a\cdot b)^n$ für alle $a,b \in G$ und $n \in \mathbb{Z}$ gilt nur, falls G abelsch ist.

Satz:

Sei $(G, \cdot)$ eine Gruppe und sei $a \in G$. Dann gilt:

(i) $\varphi : G \to G$, $\varphi(x) = x \cdot a$ ist bijektiv

(ii) $\varphi : G \to G$, $\varphi(x) = a \cdot x$ ist bijektiv

Bew (nur für (ii)):

φ ist surjektiv:

Sei $b \in G$. Setze $x := b \cdot a^{-1} \in G$. Dann gilt:

$$\varphi(x) = x \cdot a = (b^{-1} \cdot a^{-1}) \cdot a = b \cdot (a^{-1} \cdot a) = b \cdot e = b \quad ✓$$

φ ist injektiv:

Seien $x_1, x_2 \in G$ und gelte $\varphi(x_1) = \varphi(x_2)$

$$\Rightarrow \quad x_1 \cdot a = x_2 \cdot a \quad \overset{| \cdot a^{-1}}{\Rightarrow} \quad x_1 = x_2 \quad ✓$$

$\square$

Bem.:

Ist G eine endliche Gruppe, $G = \{a_1, \dots, a_n\}$, so kann man alle Produkte $a_i \cdot a_j$ in einem quadratischen Schema aufschreiben. Dabei steht $a_i \cdot a_j$ in der i-ten Zeile und j-ten Spalte der Verknüpfungstafel:

$\cdot$	$\dots$ a_j $\dots$
$\vdots$	
a_i	$a_i \cdot a_j$
$\vdots$	

Der obige Satz besagt, dass in jeder Zeile und jeder Spalte jedes Element von G genau einmal vorkommt.

Def.:

Sei $(G, \cdot)$ eine Gruppe und sei $U \subseteq G$.

U heißt Untergruppe von G, falls gilt:

(i) $e \in U$

(ii) $\forall a, b \in U: \quad a \cdot b \in U$

(iii) $\forall a \in U: \quad a^{-1} \in U$.

$\Big\} \Leftrightarrow \forall a, b \in U: \quad a \cdot b^{-1} \in U$

Satz:

Sei $(G, \cdot)$ eine Gruppe und sei $U \subseteq G$.

Dann ist äquivalent:

(i) U ist eine Untergruppe von G

(ii) $(U, \cdot_{|U \times U})$ ist eine Gruppe.

Def.:

Seien $(G, \cdot_G)$ und $(H, \cdot_H)$ Gruppen.

Eine Abbildung $\varphi: G \to H$ heißt Gruppenhomomorphismus, falls gilt:

$\forall a, b \in G: \quad \varphi(a \cdot_G b) = \varphi(a) \cdot_H \varphi(b)$

Ist φ zusätzlich bijektiv, so heißt φ Gruppenisomorphismus.

Satz

Seien $(G, \cdot_G)$ und $(H, \cdot_H)$ Gruppen und sei $\varphi: G \to H$ ein Gruppenhom.

Dann gilt:

(i) $\varphi(e_G) = e_H$,

(ii) $\forall a \in G: \quad \varphi(a^{-1}) = (\varphi(a))^{-1}$

(iii) $\forall a \in G \ \forall n \in \mathbb{Z}: \quad \varphi(a^n) = (\varphi(a))^n$

Def.:

Seien $(G, \cdot_G)$ und $(H, \cdot_H)$ Gruppen und sei $\varphi: G \to H$ ein Gruppenhom.

Dann heißt: $\mathrm{Kern}(\varphi) := \{ a \in G \mid \varphi(a) = e_H \}$ der Kern von φ

Satz

Seien $(G, \cdot_G)$ und $(H, \cdot_H)$ Gruppen und sei $\varphi: G \to H$ ein Gruppenhom.

Dann gilt: $\mathrm{Kern}(\varphi)$ ist eine Untergruppe von G.

Def.:

Ein Ring $(R, +, \cdot)$ ist eine Menge R zusammen mit 2 Verknüpfungen

$+ : R \times R \to R$

$\cdot : R \times R \to R$

so dass die folgenden Eigenschaften erfüllt sind:

(1) $(R, +)$ ist eine kommutative Gruppe, d.h.:

(i) $\forall a, b, c \in R: \ (a+b)+c = a+(b+c)$

(Assoziativität)

(ii) $\exists 0 \in R \ \forall a \in R: \ a+0 = a = 0+a$

(Existenz des neutralen Elements bzgl +)

(iii) $\forall a \in R \ \exists -a \in R: \ a+(-a) = 0 = (-a)+a$

(Existenz des inversen Elements bzgl +)

(iv) $\forall a, b \in R: \ a+b = b+a$

(Kommutativität)

(2) $\forall a, b, c \in R: \ (a \cdot b) \cdot c = a \cdot (b \cdot c)$

(Assoziativität)

(3) $\exists 1 \in R \ \forall a \in R: \ a \cdot 1 = a = 1 \cdot a$

(Existenz des neutralen Elements bzg $\cdot$)

(4) $\forall a, b, c \in R: \ a \cdot (b+c) = a \cdot b + a \cdot c \ , \ (a+b) \cdot c = a \cdot c + b \cdot c$

(Distributivgesetze)

Gilt zusätzlich:

(5) $\forall a, b \in R: \ a \cdot b = b \cdot a$

so heißt R kommutativ

Gilt zusätzlich:

(6) $1 \neq 0$ und

(7) $\forall a \in R \setminus \{0\} \; \exists b \in R: \; a \cdot b = 1 = b \cdot a$

(Existenz des inversen Elements bzgl. $\cdot$)

so heißt R Körper.

Satz:

Sei K eine Menge mit 2 Verknüpfungen $+: K \times K \to K$ und $\cdot: K \times K \to K$.

Dann ist äquivalent:

(i) $(K, +, \cdot)$ ist ein Körper

(ii) $(K, +)$ ist eine abelsche Gruppe, $(K \setminus \{0\}, \cdot)$ ist eine abelsche Gruppe und es gelten die Distributivgesetze aus obiger Def.

Bsp.:

$(\mathbb{Z}, +, \cdot)$ ist ein kommutativer Ring, aber kein Körper.

$(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ sind Körper

$(\mathbb{Z}_n, +, \cdot)$ ist ein kommutativer Ring

$(\mathbb{Z}_n, +, \cdot)$ ist ein Körper $\Leftrightarrow$ n ist eine Primzahl

$(K^{n \times n}, +, \cdot)$ ist ein Ring, aber kein Körper (für $n \geq 2$)

Satz (Rechenregeln für Körper)

Sei K ein Körper. Dann gilt für alle $a, b \in K$:

(i) $0 \cdot a = a \cdot 0 = 0$

(ii) $(-1) \cdot a = -a$

(iii) $(-a) \cdot b = a \cdot (-b) = -ab$ und $(-a) \cdot (-b) = a \cdot b$

(iv) $a \cdot b = 0 \Leftrightarrow a = 0$ oder $b = 0$.