

1 Die Körperaxiome und ihre Folgen

“Die ganzen Zahlen hat Gott gemacht, alles übrige ist Menschenwerk”, Leopold Kronecker.

Definition: $\mathbb{N} := \{1, 2, 3, \dots\}$

$\mathbb{N}_0 := \{0, 1, 2, 3, \dots\}$

$\mathbb{Z} := \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$

Zunächst wollen wir uns überlegen was vernünftige “Zahlen” ausmachen soll. Wir möchten sicherlich, daß wir zwei Operationen unbeschränkt ausführen können: Eine Addition und eine Multiplikation.

+	·	
$A+ :$ $(a + b) + c =$ $a + (b + c)$	$A· :$ $a · (b · c) =$ $(a · b) · c$	Assoziativität
$N+ :$ $a + 0 = a$	$N· :$ $a · 1 = a$	Existenz des Neutral- elements
$K+ :$ $a + b = b + a$	$K· :$ $a · b = b · a$	Kommuta- tivität
$I+ :$ zu a gibt es $-a$, mit: $a + (-a) = 0$	$I· :$ zu $a \neq 0$ gibt es a^{-1} , mit: $a · a^{-1} = 1$	Existenz des Inversen

Des weiteren haben wir

$D : a · (b + c) = a · b + a · c$	Distributivität
$NT : 1 \neq 0$	Nichttrivialität

Bemerkung: Wir sind es gewohnt, Formeln von links nach rechts zu lesen.

Deshalb lesen wir $a + b + c$ als $(a + b) + c$. Die Kommutativität der Addition liefert dann:

$$a + b + c = b + c + a = (b + c) + a = a + (b + c).$$

Es sieht so aus, als benötige man die Assoziativität gar nicht. Beachten Sie aber bitte, daß wir $a + b + c$ noch gar nicht definiert haben. Tun wir das zum Beispiel durch

$$a + b + c := (a + b) + c,$$

so liefert uns die Kommutativität lediglich

$$a + b + c = (b + a) + c = c + (b + a) = c + (a + b),$$

aber nicht

$$a + b + c = a + (b + c).$$

Beispiele: 1) Die Menge $\mathbb{F}_2 = \{0, 1\}$

2) $\mathbb{Q} = \left\{ \frac{p}{q} \mid p \in \mathbb{Z} \text{ und } q \in \mathbb{N} \right\}$ mit der Multiplikation $\frac{p}{q} \cdot \frac{r}{s} = \frac{p \cdot r}{q \cdot s}$ und der Addition $\frac{p}{q} + \frac{r}{s} = \frac{p \cdot s + r \cdot q}{q \cdot s}$ (Genaueres dazu weiter unten).

Nichtbeispiele: 1) \mathbb{N}_0 (mit der gewöhnlichen Addition und Multiplikation) da es im allgemeinen keine additiven Inversen gibt.

2) \mathbb{Z} (mit der gewöhnlichen Addition und Multiplikation) da es im allgemeinen keine multiplikativen Inversen gibt.

1.1 Erste Folgerungen aus den Körperaxiomen

F1) Neutralelemente sind eindeutig bestimmt

denn: Seien $0'$ und $1'$ weitere Neutralelemente (NE). Dann ist

$$0 + 0' = 0', \text{ da } 0 \text{ Neutralelement ist, und}$$

$$0 + 0' = 0, \text{ da } 0' \text{ Neutralelement ist.}$$

Also ist $0 = 0 + 0' = 0'$. Analog sieht man, daß multiplikative Neutralelemente eindeutig sind.

F2) $a + 0 \cdot a = a$

Grund:

$$a + 0 \cdot a \stackrel{N \cdot}{=} 1 \cdot a + 0 \cdot a \stackrel{D}{=} (1 + 0) \cdot a \stackrel{N+}{=} 1 \cdot a \stackrel{N \cdot}{=} a$$

F3) $a \cdot 0 = 0$

Grund:

$$\begin{aligned} 0 &\stackrel{I+}{=} a + (-a) \stackrel{F2)}{=} (a + 0 \cdot a) + (-a) \stackrel{K+}{=} \\ &a + (-a) + 0 \cdot a \stackrel{I+}{=} 0 + 0 \cdot a \stackrel{N+}{=} 0 \cdot a \end{aligned}$$

F4) Ist $a \cdot b = 0$, so ist $a = 0$ oder $b = 0$ (oder beide).

denn: Ist $a \neq 0$ und $b \neq 0$, dann gibt es a^{-1} und b^{-1} , mit

$$(b^{-1} \cdot a^{-1}) \cdot (a \cdot b) = (b^{-1} \cdot a^{-1}) \cdot 0 \stackrel{F3)}{=} 0.$$

Aber auch:

$$\begin{aligned} (b^{-1} \cdot a^{-1}) \cdot (a \cdot b) &\stackrel{A \cdot}{=} b^{-1} \cdot (a^{-1} \cdot a) \cdot b \stackrel{I \cdot}{=} \\ &b^{-1} \cdot 1 \cdot b \stackrel{N \cdot}{=} b^{-1} \cdot b \stackrel{I \cdot}{=} 1. \end{aligned}$$

Also wäre $1 = 0$.

F5) Inverse sind eindeutig und es gilt: $-(-a) = a$ und $(a^{-1})^{-1} = a$ für $a \neq 0$.

Grund:

$$a + (-a) = 0, \text{ also ist } a \text{ additives Inverses zu } (-a),$$

$$\text{daher } a = -(-a).$$

Den zweiten Teil sieht man analog.

$$\mathbf{F6)} \quad (-1) \cdot a = -a$$

Grund:

$$a + (-1) \cdot a \stackrel{N.}{=} 1 \cdot a + (-1) \cdot a \stackrel{D}{=} (1 + (-1)) \cdot a \stackrel{I+}{=} 0 \cdot a \stackrel{F3)}{=} 0$$

also mit F5 die Behauptung.

$$\mathbf{F7)} \quad (-1) \cdot (-1) = 1$$

Grund:

$$\begin{aligned} (-1) \cdot (-1) + (-1) &= (-1) \cdot (-1) + 1 \cdot (-1) = \\ ((-1) + 1) \cdot (-1) &= 0 \cdot (-1) = 0 \end{aligned}$$

Damit ist $(-1) \cdot (-1)$ das additive Inverse von (-1) , also $(-1) \cdot (-1) = -(-1) = 1$ (nach F5).

$$\mathbf{F8)} \quad (-a) \cdot (-a) = a \cdot a =: a^2$$

Grund:

$$\begin{aligned} (-a) \cdot (-a) &= (-1) \cdot a \cdot (-1) \cdot a = (-1) \cdot (-1) \cdot a \cdot a = \\ 1 \cdot a \cdot a &= a \cdot a = a^2 \end{aligned}$$

$$\mathbf{F9)} \quad -(a + b) = (-a) + (-b) \text{ und } (a \cdot b)^{-1} = a^{-1} \cdot b^{-1}$$

Grund:

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

und

$$a^{-1} \cdot b^{-1} \cdot a \cdot b = a^{-1} \cdot a \cdot b^{-1} \cdot b = 1 \cdot 1 = 1$$

Einschub: Warum gibt es kein multiplikatives Inverses von 0?

Wir hätten: $0 \cdot 0^{-1} = 1$ nach Definition des multiplikativen Inversen und $0^{-1} \cdot 0 = 0$ nach F3.

Definition:

$$a - b := a + (-b)$$

$$\frac{a}{b} = a \cdot b^{-1} \text{ falls, } b \neq 0$$

1.2 Die binomischen Formeln

$$B1) (a+b)^2 = (a+b) \cdot (a+b) \stackrel{D}{=} a \cdot (a+b) + b \cdot (a+b) \stackrel{D}{=} a^2 + a \cdot b + b \cdot a + b^2 \stackrel{K+}{=} a^2 + 2 \cdot a \cdot b + b^2$$

$$B2) (a-b)^2 = (a+(-b))^2 \stackrel{B1}{=} a^2 + 2 \cdot a \cdot (-b) + (-b)^2 = a^2 + 2 \cdot a \cdot (-1) \cdot b + b^2 = a^2 - 2 \cdot a \cdot b + b^2$$

$$B3) (a-b) \cdot (a+b) = (a+(-b)) \cdot (a+b) = a \cdot (a+b) + (-b) \cdot (a+b) = a^2 + a \cdot b + (-1) \cdot b \cdot a + (-1) \cdot b^2 = a^2 - b^2$$

1.3 Die Regeln der Bruchrechnung

Im folgenden seien alle auftretenden Nenner $\neq 0$.

Br1) $\frac{a}{b} = \frac{a}{b} \cdot \frac{d}{d}$, speziell: $\frac{d}{d} = 1$

Grund:

$$\frac{a}{b} \cdot \frac{d}{d} \stackrel{Def.}{=} (a \cdot b^{-1}) \cdot (d \cdot d^{-1}) = a \cdot b^{-1} \cdot 1 = a \cdot b^{-1} = \frac{a}{b}$$

Br2) $\frac{a}{b} \cdot \frac{c}{d} = \frac{a \cdot c}{b \cdot d}$

Grund:

$$\frac{a}{b} \cdot \frac{c}{d} \stackrel{Def.}{=} (a \cdot b^{-1}) \cdot (c \cdot d^{-1}) = (a \cdot c) \cdot (b \cdot d)^{-1} = \frac{a \cdot c}{b \cdot d}$$

Br3) $\frac{a}{c} + \frac{b}{c} = \frac{a+b}{c}$

Grund:

$$\frac{a}{c} + \frac{b}{c} = (a \cdot c^{-1}) + (b \cdot c^{-1}) \stackrel{D}{=} (a+b) \cdot c^{-1} = \frac{a+b}{c}$$

Br4) $\frac{a}{c} + \frac{b}{d} = \frac{a \cdot d + b \cdot c}{c \cdot d}$

Grund:

$$\frac{a}{c} + \frac{b}{d} \stackrel{Br1}{=} \frac{a}{c} \cdot \frac{d}{d} + \frac{b}{d} \cdot \frac{c}{c} \stackrel{Br2}{=} \frac{a \cdot d}{c \cdot d} + \frac{b \cdot c}{c \cdot d} \stackrel{Br3}{=} \frac{a \cdot d + b \cdot c}{c \cdot d}$$

Br5) $\frac{\frac{a}{b}}{\frac{c}{d}} = \frac{a \cdot d}{b \cdot c}$

Grund:

$$\begin{aligned} \frac{\frac{a}{b}}{\frac{c}{d}} &= \frac{a}{b} \cdot \left(\frac{c}{d}\right)^{-1} = (a \cdot b^{-1}) \cdot (c \cdot d^{-1})^{-1} = a \cdot b^{-1} \cdot c^{-1} \cdot d = \\ &= (a \cdot d) \cdot (b \cdot c)^{-1} = \frac{a \cdot d}{b \cdot c} \end{aligned}$$

1.4 Umformungen von Gleichungen

Klar ist: Gilt $a = b$, so auch $a + c = b + c$

Ist umgekehrt: $a + c = b + c$, so können wir auf beiden Seiten $(-c)$ addieren und erhalten: $a + c + (-c) = b + c + (-c)$, also $a = b$.

Für die Multiplikation gilt klarerweise: Ist $a = b$, so auch $a \cdot c = b \cdot c$. Ist umgekehrt $a \cdot c = b \cdot c$, so ist $a \cdot c \cdot c^{-1} = b \cdot c \cdot c^{-1}$ und mithin $a = b$, falls c^{-1} existiert, falls also $c \neq 0$ ist.

1.5 Potenzen in Körpern

Definition: Potenzen

Sei n eine natürliche Zahl. Wir definieren für $n \in \mathbb{N}$:

$$a^n := \underbrace{a \cdot \dots \cdot a}_{n\text{-mal}}, a^0 = 1 \text{ und für } a \neq 0, a^{-n} := (a^{-1})^n$$

0^0 lassen wir undefiniert.

Aus der Definition sieht man sofort die Potenzrechenregeln für $n, m \in \mathbb{Z}$:

$$a^n \cdot a^m = a^{n+m}$$

und

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

Satz (endliche geometrische Reihe):

$$x^n - 1 = (x - 1) \cdot (1 + x + \dots + x^{n-1}) = (x - 1) \sum_{k=0}^{n-1} x^k$$

Grund: Die rechte Seite ergibt ausmultipliziert

$$x \sum_{k=0}^{n-1} x^k - \sum_{k=0}^{n-1} x^k = \sum_{k=0}^{n-1} x^{k+1} - x^k = x^n - 1$$

Folgerung:

$$x^n - y^n = (x - y) \sum_{k=0}^{n-1} x^k y^{n-k-1}$$

Grund: Ist $y \neq 0$ so folgt mit der endlichen geometrischen Reihe

$$x^n - y^n = y^n \left(\left(\frac{x}{y} \right)^n - 1 \right) = y \left(\frac{x}{y} - 1 \right) y^{n-1} \sum_{k=0}^{n-1} \left(\frac{x}{y} \right)^k =$$

$$(x - y) \cdot \sum_{k=0}^{n-1} x^k y^{n-k-1}$$

Anwendung: Seien p, q Körperelemente und $\frac{p^2}{4} - q = a^2$ für ein a . Dann ist:

$$\begin{aligned} x^2 + p \cdot x + q &= x^2 + p \cdot x + \frac{p^2}{4} - \frac{p^2}{4} + q \\ &= \left(x + \frac{p}{2}\right)^2 - \frac{p^2}{4} + q \end{aligned}$$

Für welche x wird der letzte Ausdruck 0? Offenbar genau dann, wenn gilt:

$$\left(x + \frac{p}{2}\right)^2 = \frac{p^2}{4} - q = a^2$$

Erinnerung (p,q-Formel):

$$x_{1,2} = -\frac{p}{2} \pm \sqrt{\frac{p^2}{4} - q}$$