$\mathbb{N}$ ~~$(\mathbb{N}, +)$~~ ~~keine Gruppe~~

~~$(\mathbb{N}, +, \cdot)$~~

$\mathbb{Z}$ $(\mathbb{Z}, +)$ abelsche Gruppe

$(\mathbb{Z}, +, \cdot)$ komm. Ring mit Eins

$\mathbb{Q}$ $(\mathbb{Q}, +, \cdot)$

$\mathbb{R}$ $(\mathbb{R}, +, \cdot)$ } kommutativer Ring mit Eins

$\mathbb{C}$ $(\mathbb{C}, +, \cdot)$

X Menge

$$(\mathrm{Abb}(X, \mathbb{R}), \oplus, \odot)$$

$$f \oplus g := \begin{pmatrix} X & \longrightarrow & \mathbb{R} \\ x & \longmapsto & f(x) + g(x) \end{pmatrix}$$

$$f \odot g := \begin{pmatrix} X & \longrightarrow & \mathbb{R} \\ x & \longmapsto & f(x) \cdot g(x) \end{pmatrix}$$

Beweis

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

$\overset{(R1)}{=} 0 \cdot a + 0 \cdot a \quad | -(0 \cdot a)$

$\overset{(R3)}{=}$

$0 = 0 \cdot a + \underbrace{0 \cdot a - (0 \cdot a)}_{0}$

$0 = 0 \cdot a$

(ii) $(-a) \cdot b + a \cdot b = \underbrace{(-a+a)}_{(R3)} \cdot b$

$\| \qquad = 0 \cdot b$

$-(a \cdot b) \qquad \overset{(i)}{=} 0$

(iii) $(-a) \cdot (-b) = \underbrace{-(-a) \cdot b}_{(ii)}$

$= a \cdot b$

□

z.B.: $\mathbb{Z} \subset (\mathbb{R}, +, \cdot)$ Unterring mit Eins

$$\begin{array}{ccc} (\mathbb{Z}, +, \cdot) & \longrightarrow & (\mathbb{R}, +, \cdot) \\ \| & \longmapsto & \| \\ z & & z \end{array}$$

Homomorphismus von Ringen mit Eins.

z.B. $5 \cdot \mathbb{Z} \subset (\mathbb{Z}, +, \cdot)$ Unterring (ohne Eins)

$(\mathbb{Z}/m\mathbb{Z}, +, \odot)$ $\quad [x]+[y] := [x+y]$

$[x] \odot [y] := [x \cdot y]$

(wohldef.: Sei $[x'] = [x]$
$[y'] = [y]$

Dann ist $x' - x = p \cdot m$ für ein $p \in \mathbb{Z}$
$y' - y = q \cdot m$ " " $q \in \mathbb{Z}$

Somit ist

$$\begin{aligned} x'y' - xy &= x'y' - x'y + x'y - xy \\ &= x'(y'-y) + (x'-x)\cdot y \\ &= x' \cdot q \cdot m + p \cdot m \cdot y \\ &= m \cdot (x'q + p \cdot y) \end{aligned}$$

also $[x'y'] = [xy]$ ✓)

... ist ein Kommutativer Ring mit 1

und $(\mathbb{Z}, +, \cdot) \longrightarrow (\mathbb{Z}/m\mathbb{Z}, +, \cdot)$ ist

$x \longmapsto [x]$

ein Homomorphismus von Ringen mit 1.

$(\mathbb{Z}/2\mathbb{Z}, +, \cdot)$

$+$	0	1
$[0] = 0$	0	1
$[1] = 1$	1	0

$\cdot$	0	1
0	0	0
1	0	1

$(\mathbb{Z}/3\mathbb{Z}, +, \cdot)$

$+$	0	1	$[2]$
0	0	1	$[2]$
1	1	$[2]$	0
$[2]$	$[2]$	0	1

$\cdot$	0	1	$[2]$
0	0	0	0
1	0	1	$[2]$
$[2]$	0	$[2]$	1

$= [1]$
$= [4]$

$(\mathbb{Z}/4, +, \cdot)$

$+$	0	1	$[2]$	$[3]$
$[0] = 0$	0	1	$[2]$	$[3]$
$[1] = 1$	1	$[2]$	$[3]$	0
$[2]$	$[2]$	$[3]$	0	1
$[3]$	$[3]$	0	1	$[2]$

$\cdot$	0	1	$[2]$	$[3]$
0	0	0	0	0
1	0	1	$[2]$	$[3]$
$[2]$	0	$[2]$	0	$[2]$
$[3]$	0	$[3]$	$[2]$	1

$[2] \cdot [2] = [4]$
$= [0]$
$= 0$

Bsp: $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$

nullteilerfrei

$\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$ "

$\mathbb{Z}/4\mathbb{Z}$ hat Nullteiler

Beweis: $a \cdot b = a \cdot c \quad | -(a \cdot c)$

$a \cdot b - (a \cdot c) = 0$

$(a \cdot b + (-a) \cdot c = 0)$

$a \cdot b + a \cdot (-c) = 0$

$a \cdot (b + (-c)) = 0$

Da $a \neq 0$, folgt $b + (-c) = 0 \quad | +c$

$b = c$. □

Ein Körper ist ein kommutativer Ring mit Eins, in dem jedes Element außer 0 ein multiplikatives Inverses besitzt.

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

Notizen: $\forall a, b \in K$:

(i) $0 \neq 1$

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

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

(iv) $(-a)(-b) = a \cdot b$

(v) Körper sind nullteilerfrei.

Beweis: (i) $1 \in K^*$ ✓

(ii – iv) gilt für Ringe ✓

(v) für $a, b \in K^*$
ist $a \cdot b \in K^*$ ✓ □

$(\mathbb{Z}/2\mathbb{Z}, +, \cdot) = K$

$+$	0	1
$[0] = 0$	0	1
$[1] = 1$	1	0

$\cdot$	0	1
0	0	0
1	0	1

$K^\times$ ✓

$(\mathbb{Z}/3\mathbb{Z}, +, \cdot) = K$

$+$	0	1	$[2]$
0	0	1	$[2]$
1	1	$[2]$	0
$[2]$	$[2]$	0	1

$\cdot$	0	1	$[2]$
0	0	0	0
1	0	1	$[2]$
$[2]$	0	$[2]$	1

$K^\times$ ✓

~~$(\mathbb{Z}/4, +, \cdot)$~~

$+$	0	1	$[2]$	$[3]$
0	0	1	$[2]$	$[3]$
1	1	$[2]$	$[3]$	0
$[2]$	$[2]$	$[3]$	0	1
$[3]$	$[3]$	0	1	$[2]$

$\cdot$	0	1	$[2]$	$[3]$
0	0	0	0	0
1	0	1	$[2]$	$[3]$
$[2]$	0	$[2]$	0	$[2]$
$[3]$	0	$[3]$	$[2]$	1

Beweis

$(A \Rightarrow B)$ ✓ s.o.

$(A \Leftarrow B)$ Sei $R := \mathbb{Z}/m\mathbb{Z}$ nullteilerfrei

$$a \in R \setminus \{0\}$$

$$\tau_a : R \setminus \{0\} \longrightarrow R \setminus \{0\}$$
$$x \longmapsto x \cdot a$$

wohldef. und injektiv ($0 \neq m$)

($\tau_a(x) = \tau_a(y)$ dann $x \cdot a = y \cdot a$,

daher $x = y$.)

Da $R \setminus \{0\}$ endlich ist, ist

τ_a auch surjektiv ($\rightarrow$ 2.1.4).

$R \setminus \{0\} \neq \emptyset$, $\cdot$ assoziativ,

τ_a surjektiv $\Rightarrow$ $(R \setminus \{0\}, \cdot)$ Gruppe.

(Lemma 2.2.4) Δ

$(B \Rightarrow C)$ $(\neg B \Leftarrow \neg C)$

Ist $m = a \cdot b$ mit $1 < \underbrace{a, b}_{\in \mathbb{Z}} < m$

so ist $[m] = [a] \cdot [b]$ in $\mathbb{Z}/m\mathbb{Z}$

$[m] = 0$ $\quad [a] \neq 0$ $\quad [b] \neq 0$

$(B \Leftarrow C)$ Sei m Primzahl, und

$[a] \cdot [b] = [0]$ in $\mathbb{Z}/m\mathbb{Z}$,

also $[a \cdot b] = [0]$.

Dann $m \mid a \cdot b$,

somit $m \mid a$ oder $m \mid b$

(m prim),

also $[a] = [0]$ oder $[b] = [0]$

□

$(\mathbb{Q}, +, \cdot)$

$(\mathbb{R}, +, \cdot)$ $\quad \mathbb{Z}/2\mathbb{Z}$ $\quad \mathbb{Z}/5\mathbb{Z}$ $\quad \mathbb{Z}/7\mathbb{Z}$ ...

$(\mathbb{C}, +, \cdot)$

Beweis: Nachrechnen!

$$0_{\mathbb{C}} = (0,0)$$

$$-(a,b) = (-a,-b)$$

$$1_{\mathbb{C}} = (1,0)$$

$$(a,b)^{-1} = \left(\frac{a}{\underbrace{a^2+b^2}_{\neq 0}}, \frac{-b}{a^2+b^2}\right)$$

$(a,b) \neq 0_{\mathbb{C}}$

[...] □

Notation:

$$a := (a,0)$$

$$i := (0,1)$$ "imaginäre Einheit"

$$ib := (0,b)$$

$$\boxed{a + ib := (a,b)}$$

Es ist $i^2 = (0,1) \cdot (0,1)$

$$= (-1,0) = -1$$

$$\underbrace{(a,b) \cdot (a',b')}_{(a+ib)\cdot(a'+ib')}$$

$$= aa' + a\bar{z}b' + \bar{z}ba' + \bar{z}b\bar{z}b'$$

$$= aa' + iab' + iba' + i^2bb'$$

$$= (aa' - bb') + i(ab' + ba')$$

$i^2 = -1$

$$(aa' - bb',\ ab' + ba')$$

$\mathbb{C}$