② Körper + Ringe

Bisher: Gruppen

(z.B $(\mathbb{R}, +)$, $(\mathbb{R} - \{0\}, \cdot)$)

jetzt: Addition + Multiplikation gemischt.

Grundrechenarten

Ring R: $+, -, \cdot$ $\begin{cases} (R, +) \text{ ist Gruppe} \\ \text{Distributivgesetze} \end{cases}$

Körper K: $+, -, \cdot, :$ $\begin{cases} (K, +) \text{ ist Gruppe} \\ (K - \{0\}, \cdot) \text{ ist Gruppe} \\ \text{Distributivgesetze} \end{cases}$

Ringe

Def Sei R eine Menge und $+ : R \times R \to R$ und $\cdot : R \times R \to R$ zwei abgeschlossene Operat.

$(R, +, \cdot)$ heißt Ring wenn:

(i) $(R, +)$ ist kommutative Gruppe

(ii) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ für alle $a, b, c \in R$

(iii) $a \cdot (b + c) = a \cdot b + a \cdot c$

(iv) $(a + b) \cdot c = a \cdot c + b \cdot c$

- Achtung: $(R - \{0\}, \cdot)$ ist nicht notwendig Gruppe
- Ist $(R, \cdot)$ kommutativ so heißt $(R, +, \cdot)$ kommutativer Ring
- Gibt es ein $e \in R$ mit $a \cdot e = e \cdot a = a$ für alle $a \in R$
  Dann heißt $(R, +, \cdot)$ „Ring mit 1" $(1 := e)$

Notation

Sei $(R,+,\cdot)$ ein Ring

- Neutrales Element bzgl. $(R,+)$ heißt „0"
- Inverses zu a bzgl $(R,+)$ heißt „$-a$"
- Falls $(R,+,\cdot)$ Ring mit 1 dann heißt das neutrale E.e. bzgl $(R,\cdot)$ „1"

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

$(\mathbb{Z}_p,\oplus_p,\odot_p)$ ist Ring für alle $p\in\mathbb{N}$

$(p\mathbb{Z},+,\cdot)$

$\left(\left\{\frac{a}{2^i}\mid a\in\mathbb{Z}, i\in\mathbb{N}\right\},+,\cdot\right)$ ist Ring

Einige Rechenregeln:

Satz Sei $(R, +, \cdot)$ ein Ring mit 1 dann gilt:

(i) $0 \cdot x = 0 = x \cdot 0$ für alle $x \in R$

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

(iii) $(-1) \cdot (-1) = 1$

Bew (i) $0 \cdot x + x = 0 \cdot x + 1 \cdot x = (0+1) \cdot x = 1 \cdot x = x$

$\Rightarrow 0 \cdot x = 0$

(ii) $(-1) \cdot x + x = (-1) \cdot x + 1 \cdot x = (-1+1) \cdot x = 0 \cdot x = 0$

$\Rightarrow (-1) \cdot x = -x$

(iii) ... selber machen

Endliche Ringe

$(\mathbb{Z}_4, \oplus_4, \odot_4)$

$\oplus$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\odot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

- Ring mit 1
- $(\mathbb{Z}_4 - \{0\}, \odot_4)$ ist <u>keine</u> Gruppe
- 2 ist „Nullteiler"
  $2 \odot_4 2 = 0$
- 2 hat kein multiplikatives Inverses

$(\mathbb{Z}_5, \oplus_5, \odot_5)$

$\oplus_5$	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

$\odot_5$	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

- Ring mit 1
- $(\mathbb{Z}_5 - \{0\}, \odot_5)$ ist Gruppe
- $\mathbb{Z}_5 - \{0\}$ abgeschl. bzgl $\odot_5$
- keine Nullteiler
- jedes EL aus $\mathbb{Z}_5 - \{0\}$ hat multiplikatives Inverses

Körper

Beispiel $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$
$(\mathbb{C},+,\cdot)$

Def $(K,+,\cdot)$ heißt Körper wenn gilt:

(i) $(K,+,\cdot)$ ist Ring

(ii) $(K-\{0\},\cdot)$ ist kommutative Gruppe

Alternative Definition: $(K,+,\cdot)$ ist Körper

(i) $(K,+)$ ist komm. Gruppe

(ii) $(K-\{0\},\cdot)$ ist kommutative Gruppe

(iii) $a\cdot(b+c)=a\cdot b+a\cdot c$ für alle $a,b,c\in K$

Notation: Neutrale El in $(K,+)$ ist „0"

Inverse zu a in $(K,+)$ ist „$-a$"

Neutrale in $(K-\{0\},\cdot)$ ist „1"

Inverse in $(K-\{0\},\cdot)$ zu a ist „a^{-1}" bzw $\frac{1}{a}$

Der kleinste Körper

$(\{0,1\}, +, \cdot) \approx (\mathbb{Z}_2, \oplus_2, \odot_2)$

$+$	0	1
0	0	1
1	1	0

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

Allgemein $(\mathbb{Z}_p, \oplus_p, \odot_p)$ ist

Körper g.d.w p ist Primzahl

Zur Erinnerung $(\mathbb{R}^2, +)$ ist Gruppe $\begin{cases} (a_1, b_1) + (a_2, b_2) \\ = (a_1 + a_2, b_1 + b_2) \end{cases}$

Kann man $(\mathbb{R}^2, +, \cdot)$ zu einem Körper machen?

↑ Was kann das sein

Was wir wissen:

Neutrales El bzgl. $(\mathbb{R}^2, +)$ ist $(0,0)$

Inverses zu (a,b) bzgl $(\mathbb{R}^2, +)$ ist $(-a, -b)$

Es sei $(a,b)\cdot(c,d)=(ac-bd\ ,ad+bc)$

Satz: $(\mathbb{R}^2,+,\cdot)$ ist Körper

Beweis: • $(\mathbb{R}^2,+)$ ist Gruppe (hatten wir schon)

• $(\mathbb{R}^2,+,\cdot)$ ist Distributiv ← Nachrechnen

$(a,b)\cdot((c,d)+(e,f))=$

$(a,b)\cdot(c,d)+(a,b)\cdot(e,f)$

• $(\mathbb{R}^2-\{(0,0)\},\cdot)$ ist kommutative Gruppe

• Assoziativ, kommutativ ← Nachrechnen

• Neutrales EL: $(1,0)\cdot(c,d)=(c,d)$

• Inverses EL: $\left(\frac{a}{a^2+b^2}\ ,\frac{-b}{a^2+b^2}\right)\cdot(a,b)=\left(\frac{a^2}{a^2+b^2}+\frac{b^2}{a^2+b^2}\ \frac{ab}{a^2+b^2}-\frac{ba}{a^2+b^2}\right)$

$=(1,0)$

Einige Eigenschaften von $(a,b)\cdot(c,d)=(ac-bd,ad+bc)$

$(1,0)$ „=" „1":
$$(1,0)\cdot(a,b)=(a,b)$$

$$(a,0)\cdot(c,0)=(a\cdot c,0)$$

Erste Komponente verhält sich wie „·" in $\mathbb{R}$

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

Es gibt mindestens ein Element das mit sich selbst multipliziert „-1" ergibt

$$=-(1,0)$$

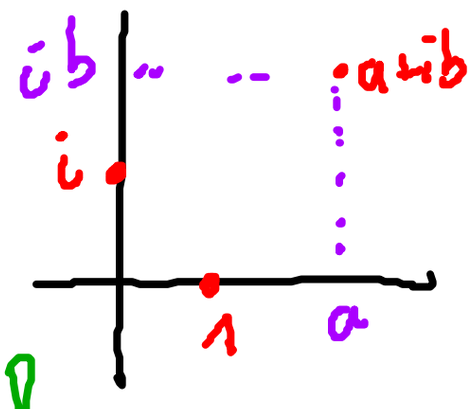
Wir führen ein:

$(a,0) =: a$

$(1,0) =: 1$

$(0,1) =: i$ mit $i^2=-1$

$(a,b) =: a+ib$ $\Leftarrow$ komplexe Zahlen!



Objekte	Addition	Multiplikation
$(a,b) \in \mathbb{R}^2$	$(a,b)+(c,d) = (a+c, b+d)$	$(a,b)\cdot(c,d) = (ac-bd, ad+bc)$
$a+ib$ $i^2=-1$	$(a+\bar{i}b)+(c+\bar{i}d)$ $a+c+\bar{i}(b+d)$	$(a+\bar{i}b)\cdot(c+\bar{i}d)$ $= ac+a\bar{i}d+\bar{i}bc+\bar{i}b\bar{i}d$ $= ac+\bar{i}^2bd+\bar{i}ad+\bar{i}bc$ $= ac-bd+\bar{i}(ad+bc)$

$$\mathbb{C} = \mathbb{R} + i\mathbb{R}$$