

Anderer Schreibweise:

• Statt  $x \sim y$  bezgl.  $m$  (d.h.  $x - y \in m\mathbb{Z}$ ) schreibt man auch  $x \equiv y$  ( $x$  ist kongruent  $y$  modulo  $m$ ),  $x, y \in \mathbb{Z}$ .

Weitere Darstellung von  $\mathbb{Z}_m$ :

• Ersetze  $\mathbb{Z}_m$  durch  $\mathbb{F}_m := \{0, 1, 2, \dots, m-1\}$ ,  $m$  prim.

Definition:

Seien  $(A, +, \cdot)$ ,  $(A', +', \cdot')$  zwei Körper und  $f: A \rightarrow A'$  Abb.  $f$  heißt (Körper-)Homomorphismus, wenn

$$\left. \begin{aligned} f(x+y) &= f(x) +' f(y) \\ f(x \cdot y) &= f(x) \cdot' f(y) \end{aligned} \right\} \forall x, y \in A \text{ [bei: } "A \setminus \{0\} \text{"]}$$

Ein bijektiver Homomorphismus heißt Isomorphismus, die Körper  $A$  und  $A'$  heißen dann isomorph.

Schreibweise:  $A \cong A'$ . Beispiel:  $\mathbb{F}_m \cong \mathbb{Z}_m$

Bemerkung (zur Definition):

In  $\mathbb{F}_p$  gilt  $\underbrace{1 + \dots + 1}_{p\text{-mal}} = 0$  und  $p$  ist die kleinste derartige Zahl.  $p$  heißt Charakteristik  $\text{char } \mathbb{F}_p$ .

Für beliebige Körper analoge Definition. Hierbei wird  $\text{char } K = 0$  gesetzt, wenn es kein  $m \in \mathbb{N}$  gibt mit  $\underbrace{1 + 1 + \dots + 1}_{m\text{-mal}} = 0$ .

Es gilt:

Für einen beliebigen Körper  $K$  ist  $\text{char } K$  entweder 0 oder eine Primzahl.

Beispiel für Körper:  $\mathbb{C}$

Betrachte  $(\mathbb{R}^2, +)$ :  $(x, y) + (x', y') = (x+x', y+y')$ ,  $(x, y) \in (\mathbb{C}, 0)$ .

Multiplikation auf  $\mathbb{R}^2$ :  $(a, b) \cdot (c, d) = (ac - bd, ad + bc)$

- kommutativ  $\checkmark$  (durch Hin- und Rückblicken...)
- assoziativ  $\checkmark$  (siehe Skript, Bew. lästig)
- distributiv:

$$(a, b) [(c, d) + (e, f)] = (a, b) [c+e, d+f]$$

$$= (ac+ae - bd+bf, ad+af + bc+be)$$

$$= (ac+ae - bd-bf, ad+af + bc+be)$$

$$(a, b)(c, d) + (a, b)(e, f) = (ac-bd, ad+bc) + (ae-bf, af+be)$$

$$= (ac-bd+ae-bf, ad+bc+af+be) \checkmark$$

- Neutralement ist  $(1, 0)$ :

$$(1, 0)(c, d) = (c, d) \checkmark$$

- Inversum ist  $\left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}\right)$ .

$$(a, b) \neq (0, 0)$$

$$\text{Denn: } (a, b) \left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}\right) = \left(\frac{a^2}{a^2+b^2} + \frac{b^2}{a^2+b^2}, -\frac{ab}{a^2+b^2} + \frac{ab}{a^2+b^2}\right)$$

$$= (1, 0) \checkmark$$

Ist „ $\cdot$ “ überhaupt eine Verknüpfung auf  $\mathbb{R}^2 \setminus \{0\}$ ?

$$(a, b), (c, d) \neq 0 \stackrel{?}{\Rightarrow} (ac-bd, ad+bc) \neq (0, 0)$$

$$\text{Angen. } (ac-bd, ad+bc) = (0, 0)$$

$$\Leftrightarrow (ac-bd)^2 + (ad+bc)^2 = 0$$

$$ac^2 + b^2d^2 + a^2d^2 + b^2c^2 = \underbrace{(a^2+b^2)}_{\neq 0} \underbrace{(c^2+d^2)}_{\neq 0} \neq 0 \checkmark$$

### Satz 10:

$(\mathbb{R}^2, +, \cdot)$  ist ein Körper.

Schreibweise:  $\mathbb{C}$  Körper der komplexen Zahlen,  $z = (a, b) \in \mathbb{C}$ ,  
 $a$  heißt Realteil von  $z$ ,  $b$  Imaginärteil.

Andere übliche Schreibweise:  $z = a+ib$

Zusammenhang: Die Menge  $\{(a, 0) \in \mathbb{C} \mid a \in \mathbb{R}\}$  ist  
mit den eingeschränkten Verknüpfungen ein  
Körper (Unterkörper von  $\mathbb{C}$ ), der zu  $\mathbb{R}$  isomorph ist.

Isomorphismus  $f: \mathbb{R} \rightarrow \tilde{\mathbb{R}}$  bettet  $\mathbb{R}$  in  $\mathbb{C}$  ein.

Nun gilt  $z = (a, b) = (a, 0) + (0, 1)(b, 0) \Rightarrow i^2 = (-1, 0)$   
 $\begin{matrix} & x \mapsto (x, 0) \\ & \nearrow & \searrow \\ a & & b \\ & i & \end{matrix}$  kurz:  $i^2 = -1$

$\Rightarrow z = a + ib$  mit  $i^2 = -1$ .

Mit dieser Schreibweise kann man wie in  $\mathbb{R}$  rechnen:

$$(a + ib)(c + id) = (ac + ibc + aid + i^2 bd) = (ac - bd + i(bc + ad))$$

~~XX~~  $z \neq 0 \Rightarrow \frac{1}{z} = \frac{1}{a + ib} = \frac{a + ib - 1}{(a + ib)(a - ib)} = \frac{a - ib}{a^2 - i^2 b^2} = \frac{a - ib}{a^2 + b^2}$   
 $= \frac{a}{a^2 + b^2} + i \frac{-b}{a^2 + b^2}$ .

Zu  $z = a + ib$  sei  $\bar{z} = a - ib$  die konjugiert komplexe Zahl.

Regeln:

$$\left. \begin{aligned} (a) \quad \overline{z + w} &= \bar{z} + \bar{w} \\ \overline{z \cdot w} &= \bar{z} \cdot \bar{w} \end{aligned} \right\} z, w \in \mathbb{C}$$

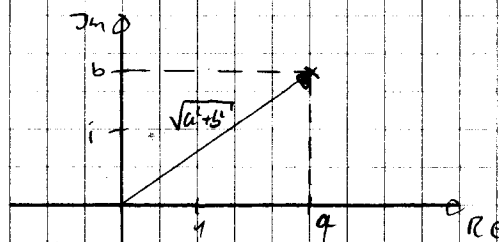
(b)  $\overline{\bar{z}} = z, z \in \mathbb{C}$

(c)  $\bar{z} = z \Leftrightarrow z \in \mathbb{R}$

(d)  $z \cdot \bar{z}$  ist reell und  $\geq 0$  und  $[z \cdot \bar{z} = 0 \Leftrightarrow z = 0]$

$|z| := \sqrt{z \cdot \bar{z}}$  heißt Betrag von  $z$ .

Demnach:  $z \cdot \bar{z} = a^2 + i^2 b^2 = a^2 + b^2$



Bemerkung:

Die Abb.  $z \mapsto \bar{z}$  ist ein Körperisomorphismus, der  $\mathbb{R}$  festhält. (Automorphismus) Außer der Identität ist dies der einzige derartige Automorphismus.