27.11.23

Homomorphismen: Ringe, Sei $m \in \mathbb{N}$, $n \in \mathbb{N}$

1. $f: (\mathbb{Z}, +, \cdot) \longrightarrow (\mathbb{Z}/m\mathbb{Z}, \oplus, \odot)$ / $f(a) = \bar{a}$
$a \longmapsto \bar{a}$ z.B. $f(2) = \bar{2}$

zu prüfen: $f(a+b) \overset{?}{=} f(a) \oplus f(b)$ $\quad f(a \cdot b) \overset{?}{=} f(a) \odot f(b)$ $\forall a, b \in \mathbb{Z}$

hierzu: • für $a, b \in \mathbb{Z}$ gilt:

$$\left.\begin{aligned} f(a+b) &= \overline{a+b} = \bar{a} \oplus \bar{b} \\ f(a) \oplus f(b) &= \bar{a} \oplus \bar{b} \checkmark \end{aligned}\right\} \Rightarrow f(a+b) = f(a) \oplus f(b).$$

• $f(a \cdot b) = \overline{a \cdot b} = \bar{a} \odot \bar{b} = f(a) \odot f(b)$ ✓

$\Rightarrow$ f ist ein Ringhomomorphismus.

2. $f: (\mathbb{Z}, +) \longrightarrow (n\mathbb{Z}, +)$ / $f(a) = n \cdot a$
$a \longmapsto n \cdot a$

• Gruppenhomomorphismus? $a, b \in \mathbb{Z}$:

$f(a+b) = n \cdot (a+b) = n \cdot a + n \cdot b = f(a) + f(b)$ ✓

• Ringhomomorphismus: $(\mathbb{Z}, +, \cdot) \to (n\mathbb{Z}, +, \cdot)$?

$f(a \cdot b) = n \cdot (a \cdot b)$

$f(a) \cdot f(b) = n \cdot a \cdot n \cdot b = n^2 \cdot (a \cdot b)$

$\Rightarrow$ für $n \neq 1$, ist f kein Ringhomomorphismus.

3. $f:$ ~~$\mathbb{Z}[X]$~~ $(\mathbb{Z}[X], +) \longrightarrow (\mathbb{Z}[X], +)$
$p \longmapsto p'$ (erste Ableitung z.B. $(x^2)' = 2 \cdot x$)
$f(p) = p'$ z.B. $f(x^2 + x) = 2x + 1$)

• Gruppenhomomorphismus? Seien $p, q \in \mathbb{Z}[X]$

$f(p+q) = (p+q)' = p' + q' = f(p) + f(q)$

· Ringhomomorphismus? Nein. z.B. für $p = 1+x$ und $q = 1-x$

$$f(p\cdot q) = f((1+x)(1-x)) = f(1-x^2) = -2x$$

$$f(p) = p' = (1+x)' = 1 \qquad f(q) = (1-x)' = -1$$

$$f(p)\cdot f(q) = 1\cdot(-1) = -1 \neq -2x$$

$\Rightarrow f(p\cdot q) \neq f(p)\cdot f(q) \Rightarrow$ <u>kein</u> Ringhomomorphismus

<u>Beispiele für Körper:</u>

- $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$,
- der "kleinste Körper" $= (\mathbb{Z}/2\mathbb{Z}, \oplus, \odot)$

ist ein Ring: bereits gesehen.

zu zeigen bleibt: $(\underbrace{\mathbb{Z}/2\mathbb{Z} \setminus \{\bar{0}\}}_{\{\bar{1}\}}, \odot)$ ist eine Gruppe,

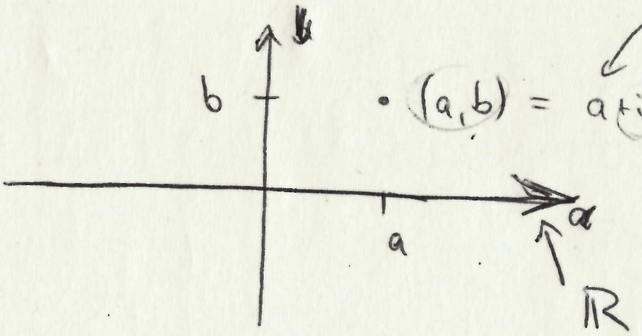
mit neutralem Element $\bar{1}$ und $(\bar{1})^{-1} = \bar{1}$.

$\mathbb{C}$: $\mathbb{R}$ & $\{i\}$ $\quad i^2 = -1$

$\underset{\mathbb{R}}{\overset{\cap}{a}} + i\cdot \underset{\mathbb{R}}{\overset{\cap}{b}}$ z.B. $2+5i$ $\quad \pi - 3{,}5i$

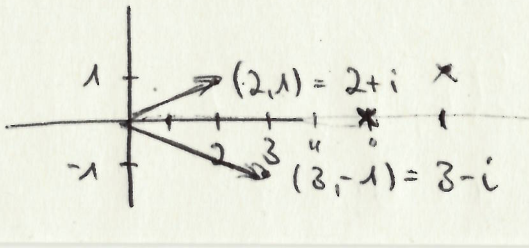
$(a,b) := a+ib$

$\underline{\underline{(a,0)}}$



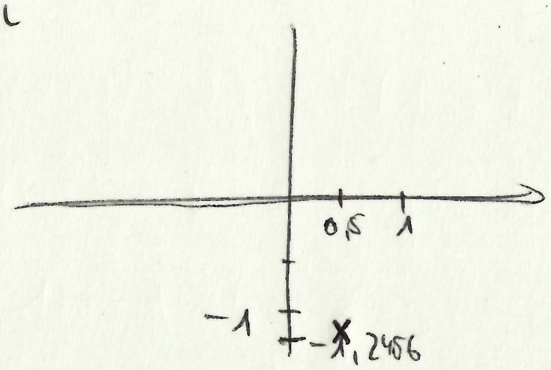
$$(2+i)+(3-i) = 5$$

$$(2+i)\cdot(3-i) = 2\cdot 3 - 2\cdot i + 3\cdot i - i^2 = 6+i-\underbrace{i^2}_{=-1}$$



$$= 6+i+1 = 7+i$$

$0{,}5 - 1{,}2456 \cdot i$



$(3,-8) \cdot (2,2) = (3\cdot 2 + 8\cdot 2,\ 3\cdot 2 - 8\cdot 2)$

$\cancel{(3,-}$

$$(3-8i)\cdot(2+2i) = 3\cdot 2 + 3\cdot 2i - 8i\cdot 2 - 8i\cdot 2i$$
$$= 3\cdot 2 + (3\cdot 2 - 8\cdot 2)\,i - 8\cdot 2\cdot \underbrace{i^2}_{=-1}$$
$$= (3\cdot 2 + 8\cdot 2) + (3\cdot 2 - 8\cdot 2)\,i$$

$$(x,y)\cdot(x',y') = (x+i\cdot y)\cdot(x'+iy')$$
$$= xx' + ixy' + iyx' + \underbrace{(i^2)}_{=-1}\cdot yy'$$
$$= (xx'-yy') + i(xy'+yx') = (xx'-yy',\ xy'+yx').$$

$\mathbb{C}$ ist ein Körper.

- $(\mathbb{C},+)$ ist eine Gruppe: $(0,0) = 0 + 0\cdot i$ ist das neutrale Element
  $-(x,y) = (-x,-y) = -x-y\cdot i.$
  Assoz. ✓
- $(\mathbb{C}\setminus\{(0,0)\}, \cdot)$ eine Gruppe: $(1,0) = 1 \in \mathbb{R}$,
  da: $(1,0)\cdot(x,y) = (1+\cancel{0i})\cdot(x+iy)$
  $= x+iy = (x,y).$

Inverses: Beispiel: Inv. vom $(1+i)$: $\dfrac{1}{1+i} = \dfrac{1\cdot(1-i)}{(1+i)(1-i)}$

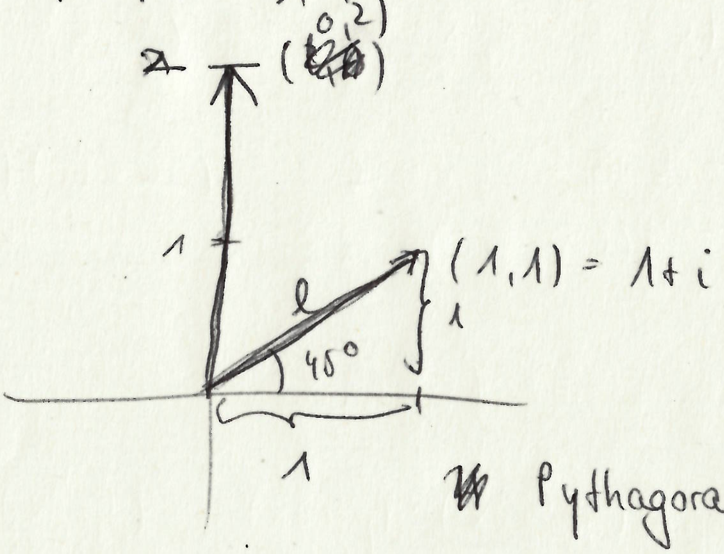
allg:

$$\left(\frac{x}{x^2+y^2},\ \frac{-y}{x^2+y^2}\right) \quad = \frac{1-i}{1-i^2} = \frac{1-i}{1+1} = \frac{1}{2}\cdot(1-i) = \frac{1}{2} - \frac{1}{2}\cdot i = \left(\frac{1}{2}, -\frac{1}{2}\right)$$

$$(1+i)\left(\tfrac{1}{2}-\tfrac{1}{2}i\right)=\tfrac{1}{2}-\tfrac{1}{2}i+\tfrac{1}{2}i-\tfrac{1}{2}(\underbrace{i^2}_{=-1})$$
$$=\tfrac{1}{2}+\tfrac{1}{2}=1.$$

<u>Allg.:</u> $$\underbrace{(x+iy)\cdot\left(\frac{x}{x^2+y^2}-i\cdot\frac{y}{x^2+y^2}\right)}$$

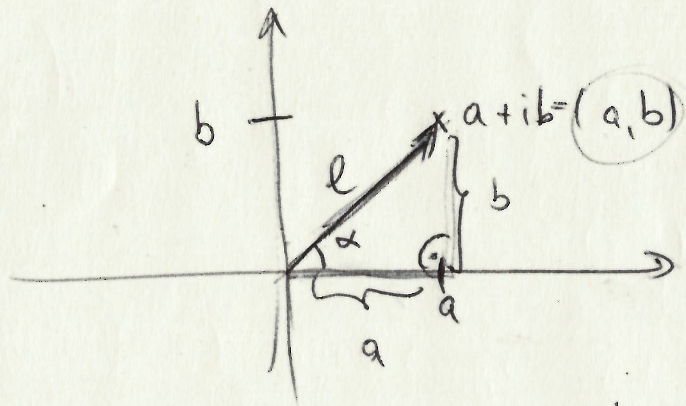
$$=\ \dots\ =1$$



Pythagoras: $l^2=1^2+1^2=2$
$\Rightarrow l=\sqrt{2}$

$(1+i)^2$ hat Länge $\sqrt{2}\cdot\sqrt{2}=2$.
und Winkel $45°+45°=90°$

$$(1+i)\cdot(1+i)=1+i+i+\underbrace{i^2}_{=-1}=\underbrace{2\cdot i}_{=0+2\cdot i}=(0,2)$$



$a=\mathrm{Re}(a+ib)$
$b=\mathrm{Im}(a+ib)$

$l=$ Länge$(a+ib)=$
$=\sqrt{a^2+b^2}$
$=$ "Betrag" von $a+ib$.
$|a+ib|$

$$\cos\alpha=\frac{a}{l}\Rightarrow \arccos\left(\frac{a}{l}\right)$$
$$\sin\alpha=\frac{b}{l}\qquad \arcsin\left(\frac{b}{l}\right)$$

$$\tan\alpha=\frac{\sin\alpha}{\cos\alpha}=\frac{b}{a}\Rightarrow\alpha=\arctan\left(\frac{b}{a}\right)$$

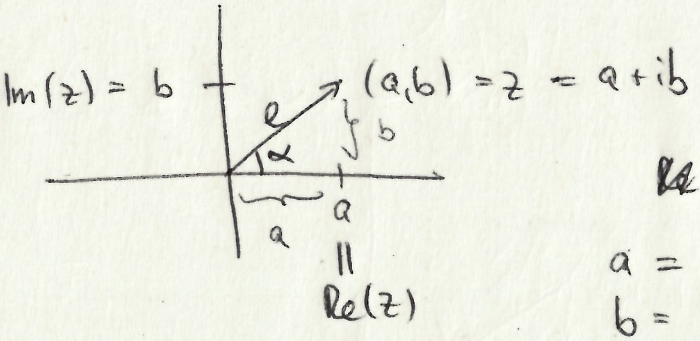
<u>komplex konjugierte</u> von $a+ib$: $a-ib$

$$(a+ib)\cdot\underset{\overline{a+ib}}{\underset{\shortparallel}{(a-ib)}} = a^2-(ib)^2 = a^2-\underset{-1}{\underset{\shortparallel}{i^2}}b^2 = a^2+b^2 = |a+ib|^2$$

$$= \text{Länge}^2$$

$$(a+\cancel{ib}) + (a-\cancel{ib}) = 2a = 2\cdot \mathrm{Re}(a+ib)$$

$$(\cancel{a}+ib) - (\cancel{a}-ib) = 2ib = 2i\cdot\underbrace{\mathrm{Im}(a+ib)}_{=b \text{ (reelle Zahl)}}$$



$$\cos\alpha = \frac{a}{l}$$

$$a = \cos\alpha\cdot l$$
$$b = \sin\alpha\cdot l$$

<u>Beispiele:</u>

- $(3+2i)(-1+i) = -3+3i-2i+2\underset{-1}{\underset{\shortparallel}{i^2}} = -3+i-2 = -5+i = (-5,1)$.
- $(-i)(-2+3i) = 2i-3i^2 = 2i+3 = (3,2)$
- $(5-i)(5+i) = 5^2+1^2 = 26$

  $5^2-\underset{-1}{\underset{\shortparallel}{i^2}} = 25+1$

- $\dfrac{3+2i}{5-3i} = \dfrac{(3+2i)(5+3i)}{(5-3i)(5+3i)} = \dfrac{15+9i+10i+6(\overset{-1}{\overset{\shortparallel}{i^2}})}{5^2+3^2} =$

  $= \dfrac{15+19i-6}{34} = \dfrac{9+19i}{34} = \dfrac{9}{34}+\dfrac{19}{34}\cdot i$

  $= \left(\dfrac{9}{34}, \dfrac{19}{34}\right)$.

- $\dfrac{1-i}{5-i} = \dfrac{(1-i)(5+i)}{(5-i)(5+i)} = \dfrac{5+i-5i-\overset{-1}{\overset{\shortparallel}{i^2}}}{5^2+1^2} = \dfrac{6-4i}{26} = \dfrac{3-2i}{13}$

  $= \left(\dfrac{3}{13}, -\dfrac{2}{13}\right)$.

~~(5−i)(5−i)~~

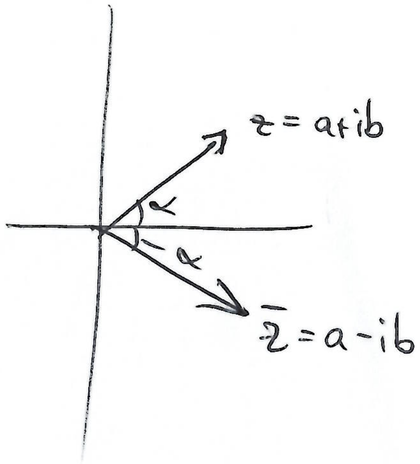
$$\underset{(x-2i)(x+2i)}{\underset{\shortparallel}{x^2+4}} = 0 \qquad x^2 = -4 = 4i^2 \iff x = \pm 2i$$

$$\overline{2i} = -2i$$

Beispiel:

$2\cdot x^4 - 8x^3 + 14x^2 - 24x + 24 = 0$ (*)

Angenommen $x \in \mathbb{C}$
ist eine komplexe Lösung
von (*)



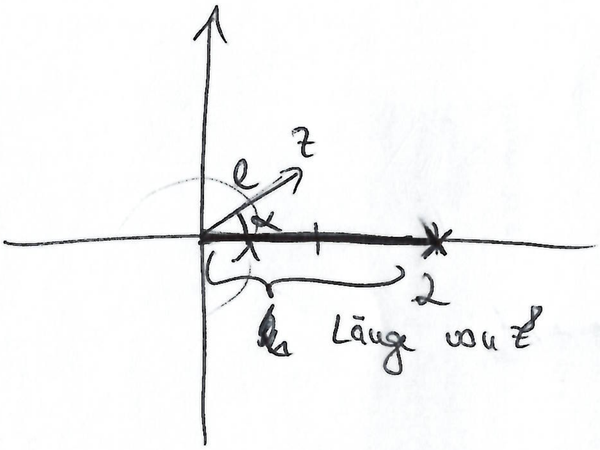
$\overline{2x^4 - 8x^3 + 14x^2 - 24x + 24} = \overline{0} = 0$

$2\cdot\bar{x}^4 - 8\cdot\bar{x}^3 + 14\bar{x}^2 - 24\bar{x} + 24 = 0$

d.h. wenn x eine Lösung ist, dann auch $\bar{x}$.

für $x \in \mathbb{R}$ ist $\bar{x} = x$

in $\mathbb{R}$ hat $z^8 = 2$ die 2 Lösungen $\pm\sqrt[8]{2}$



$z\cdot z\cdot z\cdot z \dots$

(1) der Winkel von z^8 mit der x-Achse $8\cdot\alpha = k\cdot 360°$.

(2) und die Länge von z^8 gleich ℓ^8, also 2

$\Rightarrow \ell = \sqrt[8]{2} \in \mathbb{R}$.

Endliche Körper: $\mathbb{Z}/_p\mathbb{Z}$ für eine Primzahl p.

- $\mathbb{Z}/_p\mathbb{Z}$: Ringe laut Vorlesung mit $\oplus, \odot$ und neutralem Element $\bar{0}$ (bzgl. $\oplus$) und das inverse Element bzgl. $\oplus$ von $\bar{a}$ ist $\overline{p-a}$ $\left(\overline{p-a} \oplus \bar{a} = \overline{p-a+a} = \bar{p} = \bar{0}\right)$
- $(\mathbb{Z}/_p\mathbb{Z} \setminus \{\bar{0}\}, \odot)$ ist eine Gruppe, denn: neutrales Element bzgl $\odot$ ist: $\bar{1}$

  Sei $\bar{a} \in \mathbb{Z}/_p\mathbb{Z} \setminus \{\bar{0}\}$.

  Suche $\bar{b} \in \mathbb{Z}/_p\mathbb{Z}$ s.d. $\bar{a} \odot \bar{b} = \bar{1}$.

  $\uparrow$ inverses Element.

$ggT(p, a) = 1$ $\quad\left(\begin{smallmatrix} p = 11 \\ 3 \end{smallmatrix}\right)$

$\Downarrow$

es gibt $s, t \in \mathbb{Z}$ s.d. $s p + a \cdot t = 1$
(erweiteter Euklid. Algorithmus)

$\overline{\cancel{s \cdot p} + a \cdot t} = \bar{1}$

$\Leftrightarrow$ $\overline{a \cdot t} = \bar{1}$

$\bar{a} \odot \bar{t}$ $\Rightarrow$ $\bar{t}$ ist das multiplikative Inverse von $\bar{a}$!

$\Rightarrow$ $\mathbb{Z}/_p\mathbb{Z}$ ist ein <u>Körper</u>!

Was ist für andere Restklassenringe, z.B. $\mathbb{Z}/_{12}\mathbb{Z}$

$\bar{9}$ $\quad (ggT(9, 12) = 3 \neq 1)$

$\bar{5}$ hat ein Inverses bzgl $\odot$

- Alle Elemente $\bar{a}$ in $\mathbb{Z}/_m\mathbb{Z}$ mit $ggT(a, m) = 1$ sind invertierbar, d.h. es gibt ein $\bar{b}$ mit $\bar{a} \odot \bar{b} = \bar{1}$
- Alle Elemente $\bar{a}$ ~~ ~~ in $\mathbb{Z}/_m\mathbb{Z}$ mit $ggT(a, m) \neq 1$ sind nicht invertierbar

$\Rightarrow$ $\mathbb{Z}/m\mathbb{Z}$ ist ein Körper wenn:

alle Elemente $\bar{a}$ außer $\bar{0}$ ein mult. Inverses haben.

$\Leftrightarrow$ für alle Elemente $\bar{a}$ gilt: $ggT(a, m) = 1$.

$\Leftrightarrow$ m ist eine Primzahl.

$\Rightarrow$ Satz: $\mathbb{Z}/_{m}\mathbb{Z}$ ist genau dann ein Körper, wenn $m = p$ eine Primzahl ist.