Karlsruher Institut für Technologie

Lineare Algebra I
für die Fachrichtung Informatik
Wintersemester 2023/24

Lemma 3.4.13

(a) $g: \begin{pmatrix} \mathbb{Z} \longrightarrow \mathbb{Z}/0\mathbb{Z} \\ x \longmapsto [x]_0 \end{pmatrix}$ ist ein Ringisomorphismus

g surjektiv.

g Ringhomom.

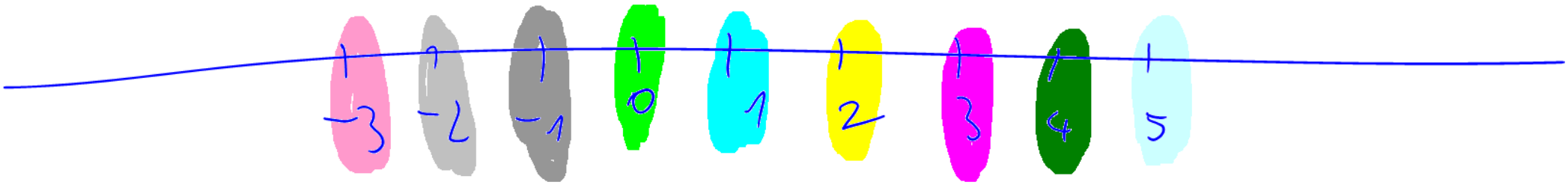
$g(x) = g(y)$ z.z: $x = y$

$\Rightarrow [x]_0 = [y]_0$

$\Rightarrow x \equiv_0 y$

$\Rightarrow x = y$

$\Rightarrow g$ injektiv.



Lemma 3.4.13

(b) Für $m \in \mathbb{N}$ gilt:

$$f: \left(\begin{array}{ccc} \{0, \dots, m-1\} & \longrightarrow & \mathbb{Z}/m\mathbb{Z} \\ r & \longmapsto & [r]_m \end{array} \right) \text{ ist bijektiv.}$$

Bw: f surjektiv.

Sei $w \in \mathbb{Z}/m\mathbb{Z}$. (z.z: $\exists r \in \{0, \dots, m-1\}$ $f(r) = w$.)

g surjektiv

$\Rightarrow \exists x \in \mathbb{Z}: g(x) = w$

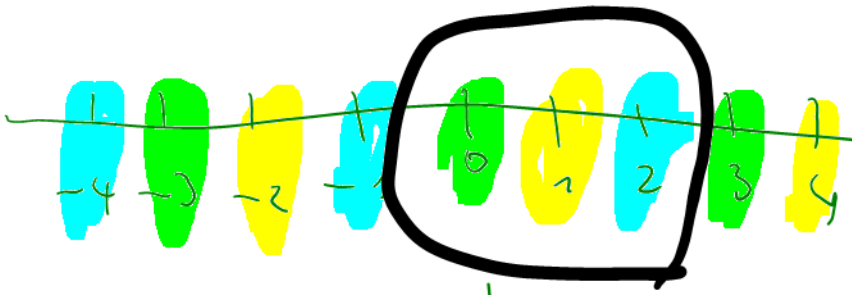
$[x]_m = w.$

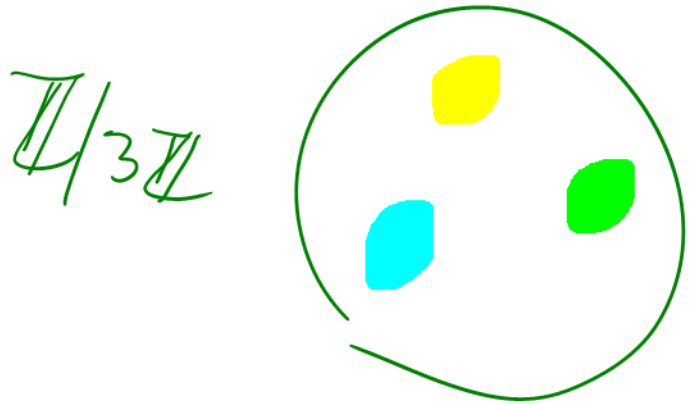
$x = km + r \qquad k \in \mathbb{Z}, r \in \{0, \dots, n-1\}$

$$[x]_m = [km + r]_m = [k]_m \cancel{[m]_m} + [r]_m = [r]_m$$

$= w$ ($[m]_m = 0$) $= f(r)$

z.B. $m = 3$





f injektiv $\qquad r, s \in \{0, \dots, m-1\}$

z.z.: $r = s$.

$$f(r) = f(s)$$

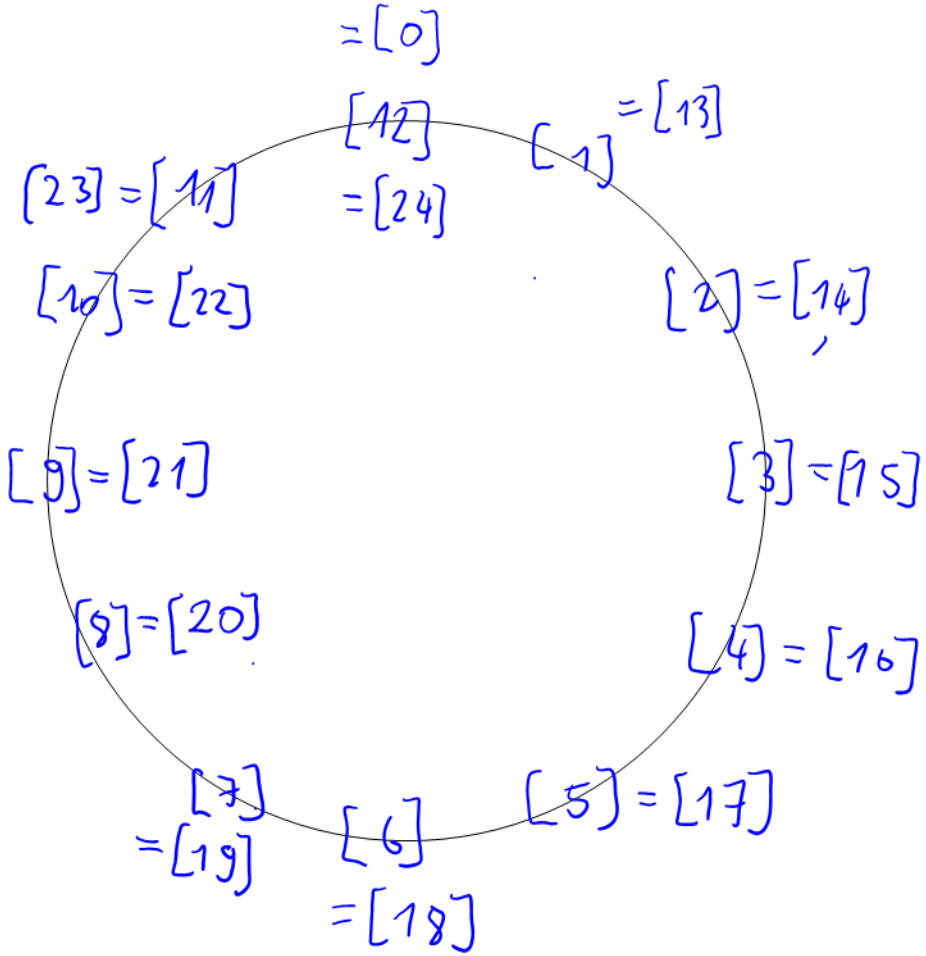
$$[r]_m = [s]_m$$

$$r \equiv_m s$$

$$m \mid (r - s) \dots$$

$$|r - s| \leq m - 1 \Rightarrow r - s = 0 \Rightarrow r = s.$$

z.B.: $\mathbb{Z}/12\mathbb{Z}$



$\mathbb{Z}/19\mathbb{Z}$

$$[17]_{19} \cdot [17]_{19} = [-2]_{19}\,[-2]_{19} = [4]_{19}.$$

z.B.: $\mathbb{Z}/5\mathbb{Z}$

+	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

·	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

Körper

$\mathbb{Z}/6\mathbb{Z}$

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

·	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Kein Körper

$[2]_6 \cdot [3]_6 = [6]_6 = [0]_6$ | $2 \cdot 3 = 6 = 0$

Lemma 3.4.15

Es sei $(R,+,\cdot)$ ein endliche kommutativer Ring und $0 \neq 1$.

Dann sind äquivalent:

(i) $(R,+,\cdot)$ ist ein Körper

(ii) $(R,+,\cdot)$ ist „nullteilerfrei", d.h.

$$\forall a,b \in R: \quad ab = 0 \implies a = 0 \text{ oder } b = 0$$

Achtung: Für unendliche Ringe sind (i) und (ii) NICHT äquivalent.

$(\mathbb{Z},+,\cdot)$ ist kein Körper, aber nullteilerfrei.

Bw: (i) $\Rightarrow$ (ii) gilt für alle Körper (auch unendliche).

(ii) $\Rightarrow$ (i): z.z: $R^\times = R \setminus \{0\}$.

„$\subseteq$": Sei $a \in R^\times$. $a a^{-1} = 1$

$\Rightarrow a \neq 0$, sonst: $0 \cdot a^{-1} = 1 \Rightarrow 0 = 1$ ↯.

„$\supseteq$": Sei $a \in R \setminus \{0\}$. z.z: $a \in R^\times$, d.h. $\exists x \in R \; ax = 1$

$$f : \begin{pmatrix} R \longrightarrow aR = \{ax \mid x \in R\} \\ x \longmapsto ax \end{pmatrix}$$ surjektiv.

Beh: f inj.

$f(x) = f(y) \Rightarrow ax = ay \Rightarrow ax - ay = 0$

$\Rightarrow a(x-y) = 0 \Rightarrow$ $a=0$ ↯ oder $x-y=0$

$\Rightarrow x = y$.

$f: R \longrightarrow aR$ bijektiv.

$|R| = n \longrightarrow |aR| = n.$ $aR \subseteq R.$

$\Rightarrow aR = R.$

$1 \in aR. \Rightarrow \exists x \quad f(x) = 1$

$ax = 1.$

∎

Satz 3.4.19

Für $m \in \mathbb{N}$ sind äquivalent:

(i) m ist eine Primzahl

(ii) $\mathbb{Z}/m\mathbb{Z}$ ist ein Körper

Bw: (i) $\Rightarrow$ (ii): m Primzahl $\Rightarrow m > 1$.

In $\mathbb{Z}/m\mathbb{Z}$ gilt $0 \neq 1$

$|\mathbb{Z}/m\mathbb{Z}| = m$.

Nach Lemma 3.4.15 reicht es zu zeigen, $\mathbb{Z}/m\mathbb{Z}$ nullteilerfrei.

Sei $a, b \in \mathbb{Z}/m\mathbb{Z}$. z.z: $a = 0$ oder $b = 0$.

$ab = 0$

$a = [x]_m \qquad b = [y]_m .$

$$[x]_m \cdot [y]_m = [0]_m$$

z.z.: $[x]_m = 0$ oder $[y]_m = 0$.

$$[x \cdot y]_m = [0]_m$$

$$x \cdot y \equiv_m 0$$

$$m \mid x \cdot y .$$

$\Longrightarrow$ $m \mid x$ oder $m \mid y$

Lemma von Euklid.

$[x]_m = 0$ oder $[y]_m = 0$.

(ii) $\Rightarrow$ (i). $\mathbb{Z}/m\mathbb{Z}$ Körper $\Rightarrow$ $m > 1$.

$k \in \mathbb{N}$

$k \mid m$ z.z.: $k = 1$ oder $k = m$.

Pf Widerspruch: $1 < k < m$.

$m = k \cdot l$ $1 < l < m$.

$[k \cdot l]_m = [m]_m$

$[k]_m \cdot [l]_m = [0]_m$ in $\mathbb{Z}/m\mathbb{Z}$.

$\Rightarrow$ $[k]_m = 0$ oder $[l]_m = 0$. ↯

□

Beispiele für Ringe und Körper

kein Körper

Körper

nicht kommutativ

$\mathbb{R}^{n \times n}$ $n \geq 2$

Kommutativ

$\hookrightarrow$ Unterring

$\cong$ isomorph

$\mathbb{C}$

$\mathbb{R}$

$\mathbb{Q}$

$\mathbb{Z}$

$\{0\}$ Nullring

$\mathbb{F}_4$

$\mathbb{F}_2$

$\cong$ $\mathbb{Z}/0\mathbb{Z}$ $\cong$ $\mathbb{Z}/1\mathbb{Z}$ $\mathbb{Z}/2\mathbb{Z}$ $\mathbb{Z}/3\mathbb{Z}$ $\mathbb{Z}/4\mathbb{Z}$ $\mathbb{Z}/5\mathbb{Z}$ $\mathbb{Z}/6\mathbb{Z}$ $\mathbb{Z}/7\mathbb{Z}$ ...

Alles in Kapitel 2 gilt, wenn $\mathbb{R}$ durch einen anderen Körper $\mathbb{K}$ ersetzt wird.

$x^2 = 3$ hat in $\mathbb{Q}$ keine Lösung

$x^2 = 3$ hat in $\mathbb{R}$ zwei Lösungen $\sqrt{3}, -\sqrt{3}$.

$x^2 = -1$ hat in $\mathbb{R}$ keine Lösung!

Komplexe Zahlen

La 3.5.1: In $\mathbb{R}$ hat $\boxed{x^2 = -1}$ keine Lösung.

Bw: $x > 0 \Rightarrow x^2 > 0 \quad x^2 \neq -1$

$x < 0 \Rightarrow -x > 0 \Rightarrow x^2 = (-x)^2 > 0 \quad x^2 \neq -1$

$x = 0 \Rightarrow x^2 = 0 \neq -1.$

Angenommen $\exists\, K$ Körpererweiterung von $\mathbb{R}$

mit $j \in K$ und $i^2 = -1$.

z.B.: $13 i^4 - 5i^3 + 12i^2 - 6i + 5 \in K$.

$= 13 + 5i - 12 - 6i + 5$

$6 - i$

$i^2 = -1$

$i^3 = -i$

$i^4 = (i^2)^2 = (-1)^2 = 1$.

Lemma 3.5.2

Wenn $z = a + ib$

und $z = x + iy$

Dann $a = x$ und $b = y$.

Bw: $a + ib = x + iy$

$a - x = iy - ib$

$a - x = i(y - b) \quad |()^2 \Rightarrow$ $\boxed{(a-x)^2 = (-1)(y-b)^2 \text{ in } \mathbb{R}}$

$(a-x)^2 \geq 0$, $(y-b)^2 \geq 0$, $(-1)(y-b)^2 \leq 0$

$\Rightarrow (a-x)^2 = 0 \Rightarrow a = x, \Rightarrow b = y$ ∎

Lemma 3.5.3:

$$(a_1 + b_1 i) + (a_2 + b_2 i) = (a_1 + a_2) + i(b_1 + b_2).$$

$$(a_1 + b_1 i) - (a_2 + b_2 i) = (a_1 - a_2) + i(b_1 - b_2).$$

$$(a_1 + b_1 i) \cdot (a_2 + b_2 i) = a_1 a_2 + a_1 b_2 i + b_1 a_2 i + b_1 b_2 i^2$$

$$= (a_1 a_2 - b_1 b_2) + i(a_1 b_2 + b_1 a_2).$$

$$\frac{a_1 + b_1 i}{a_2 + b_2 i} = \frac{(a_1 + b_1 i)(a_2 - b_2 i)}{(a_2 + b_2 i)(a_2 - b_2 i)} = \frac{(a_1 a_2 + b_1 b_2) + i(b_1 a_2 - a_1 b_2)}{a_2^2 + b_2^2}$$

$$= \frac{a_1 a_2 + b_1 b_2}{a_2^2 + b_2^2} + i \frac{b_1 a_2 - a_1 b_2}{a_2^2 + b_2^2}.$$

$$\frac{1}{a + bi} = \frac{a - bi}{a^2 + b^2} = \frac{a}{a^2 + b^2} + i\left(-\frac{b}{a^2 + b^2}\right)$$

Angenommen $\exists K \supseteq \mathbb{R}$ und $i \in K$

$i^2 = -1$

$\Rightarrow \mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}$ Unterkörper von K,
Körperem. von $\mathbb{R}$

K
|
$\mathbb{C}$
|
$\mathbb{R}$

Satz 3.5.4 Existenz der komplexen Zahlen

Es gibt eine Körpererweiterung

$\mathbb{C}$ von $\mathbb{R}$, mit $i \in \mathbb{C}$ mit $i^2 = -1$,

mit der Eigenschaft, dass sich jedes $z \in \mathbb{C}$ eindeutig

als $a + ib$ mit $a, b \in \mathbb{R}$ schreiben lässt.

$\mathbb{C}$ ist der Körper der komplexen Zahlen.

Bw: $\mathbb{C} := \mathbb{R}^2$

$(\mathbb{R}^2, +)$ abelsche Gruppe

$0_{\mathbb{C}} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$.

Definiere $\cdot : \mathbb{R}^2 \times \mathbb{R}^2 \longrightarrow \mathbb{R}^2$

$$\left(\begin{pmatrix} a_1 \\ b_1 \end{pmatrix}, \begin{pmatrix} a_2 \\ b_2 \end{pmatrix} \right) \longmapsto \begin{pmatrix} a_1 a_2 - b_1 b_2 \\ a_1 b_2 + b_1 a_2 \end{pmatrix}$$

- assoziativ
- $1_{\mathbb{C}} := \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ ist Neutralelement bzgl. $\cdot$
- kommutativ

Distributivgesetz

Jedes $\begin{pmatrix} a \\ b \end{pmatrix} \neq \begin{pmatrix} 0 \\ 0 \end{pmatrix}$ hat ein Inverses bzgl. $\cdot$

$$\begin{pmatrix} a \\ b \end{pmatrix} \cdot \frac{1}{a^2+b^2} \begin{pmatrix} a \\ -b \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = 1_{\mathbb{C}}.$$

Das muss man nachrechnen

$$i_{\mathbb{C}} := \begin{pmatrix} 0 \\ 1 \end{pmatrix} \qquad i_{\mathbb{C}} \cdot i_{\mathbb{C}} = -1_{\mathbb{C}}.$$

Das muss man nachrechnen!

$$\varphi : \left(\begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{C} \\ x & \longmapsto & \begin{pmatrix} x \\ 0 \end{pmatrix} \end{array} \right) \quad \text{inj. Körperhomomorphismus.}$$

$$\begin{pmatrix} x \\ 0 \end{pmatrix} \cdot \begin{pmatrix} y \\ 0 \end{pmatrix} = \begin{pmatrix} xy \\ 0 \end{pmatrix}.$$

Alternativ:

$$C := \left\{ \begin{pmatrix} \alpha & -\beta \\ \beta & \alpha \end{pmatrix} \mid \alpha, \beta \in \mathbb{R} \right\} \subseteq \mathbb{R}^{2\times 2}.$$

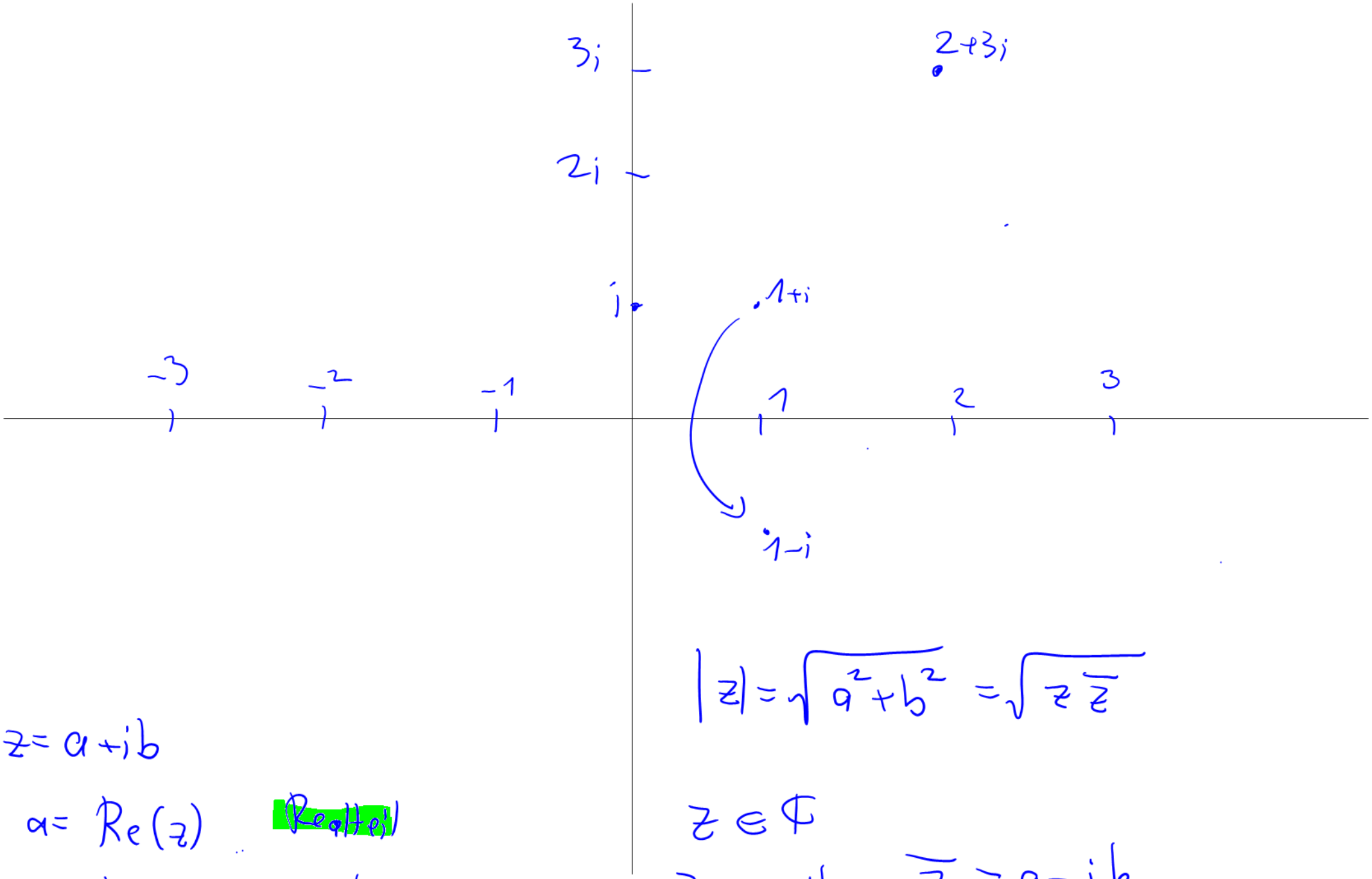
Zeige: C Unterring von $\mathbb{R}^{2\times 2}$.

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^2 = -\mathbb{1}.$$

$\mathbb{C}$ kommutativ. $\quad I = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$

$\forall z \in \mathbb{C} \quad z = \alpha \mathbb{1} + \beta I.$

. . .



$$|z| = \sqrt{a^2+b^2} = \sqrt{z\,\overline{z}}$$

$z = a + ib$

$a = Re(z)$ Realteil

$b = Im(z)$ Imaginärteil

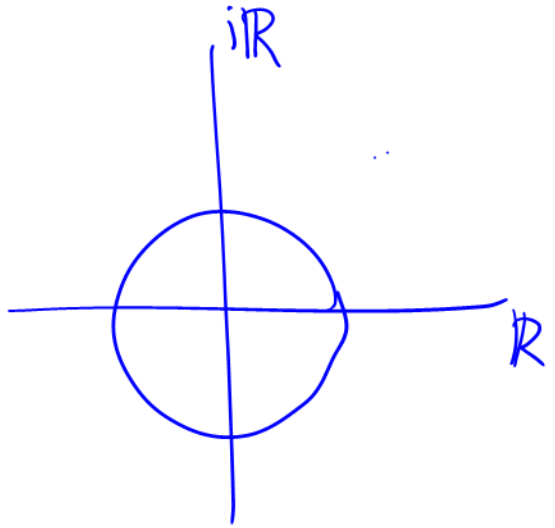
$z \in \mathbb{C}$

$z = a + ib \quad \overline{z} = a - ib$

komplex konjugierte Zahl

$$S^1 = \{ z \in \mathbb{C} \mid |z| = 1 \} \subseteq \mathbb{C}$$

Einheitskreis.



Lemma 3.5.7

(a) $\left.\begin{matrix} \mathrm{Re}: \mathbb{C} \to \mathbb{R} \\ \mathrm{Im}: \mathbb{C} \to \mathbb{R} \end{matrix}\right\}$ ist ein Gruppenhomo bzgl. $(\mathbb{C},+) \to (\mathbb{R},+)$.

Achtung: Kein Ring/Körperhomo.

(b) $i\mathbb{R} = \{ ib \mid b \in \mathbb{R} \} = \ker(\mathrm{Re})$ Untergruppe von $(\mathbb{C},+)$

(c) $\begin{pmatrix} \mathbb{C} \to \mathbb{C} \\ z \mapsto \overline{z} \end{pmatrix}$ ist ein Körperautomorphismus.

$\overline{z+w} = \overline{z} + \overline{w}$

$\overline{zw} = \overline{z} \cdot \overline{w}$

$\overline{1} = 1$

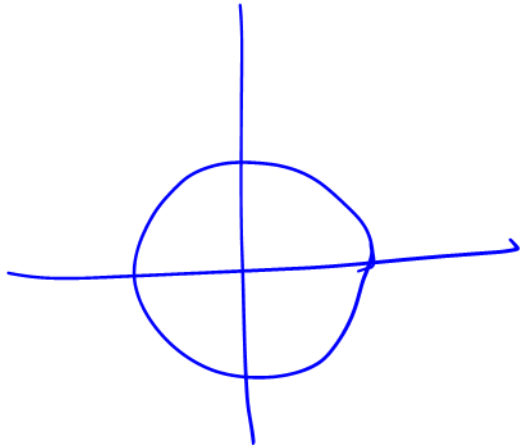
$\overline{0} = 0$.

(d) $|\cdot| : \mathbb{C} \longrightarrow [0,\infty)$ ist multiplikativ.

$|\cdot| : (\mathbb{C}^\times, \cdot) \longrightarrow ((0,\infty), \cdot)$ ist Gruppenhomomorph.

$\ker(|\cdot|) = S^1$

$(S^1, \cdot)$ Untergruppe von $\mathbb{C}^\times$.



Notation 3.6.8

$$\exp : \left(\begin{array}{ccc} (\mathbb{C}, +) & \longrightarrow & \mathbb{C}^\times = (\mathbb{C}\setminus\{0\}, \cdot) \\ z & \longmapsto & e^z = \exp(z) = \sum_{k=0}^{\infty} \frac{z^k}{k!} \end{array} \right)$$

komplexe Exp ist Gruppenhomo

$e^{z+w} = e^z \cdot e^w$