Definition Körper: kommut. Ring $(\mathbb{K},+,\cdot)$ mit $1_{\mathbb{K}}$, sodass

$$1_{\mathbb{K}} \neq 0_{\mathbb{K}}, \qquad \mathbb{K}^* = \mathbb{K} \setminus \{0_{\mathbb{K}}\}.$$

Beispiel $(\mathbb{Q},+,\cdot)$ und $(\mathbb{R},+,\cdot)$ sind Körper. $(\mathbb{Z},+,\cdot)$ ist kein Körper.

Satz Es sei $n \in \mathbb{Z}_{\geq 2}$. Dann sind äquivalent:

(i) $(C_n,+,\cdot)$ ist Körper.

(ii) n ist Primzahl.

Beweis Es gilt:

$$C_n \text{ Körper} \iff \overline{1}, \ldots, \overline{n-1} \in C_n^*$$

$$\iff \operatorname{ggT}(a,n) = 1 \text{ für } a = 1, \ldots, n-1$$

$$\iff n \text{ Primzahl}. \qquad \square$$

Definition $\mathbb{K}, \mathbb{L}$ Körper. Eine Abb. $\varphi: \mathbb{K} \to \mathbb{L}$ heisst Körperhomomorphismus, falls

(i) φ Ringhom., d.h. stets

$$\varphi(a+b) = \varphi(a) + \varphi(b), \quad \varphi(a \cdot b) = \varphi(a)\varphi(b)$$

(ii) $\varphi(1_{\mathbb{K}}) = 1_{\mathbb{L}}$.

Satz Jeder körperhom. ist injektiv.

Lemma Es sei $\varphi : R \to S$ Ringhom. mit $\varphi(1_R) = 1_S$. Für jedes $r \in R^*$ gilt:

$$\varphi(r) \in S^*, \qquad \varphi(r)^{-1} = \varphi(r^{-1}).$$

Insbesondere: $\varphi(R^*) \subseteq S^*$.

Beweis. Es gilt:

$$\varphi(r) \cdot \varphi(r^{-1}) = \varphi(r \cdot r^{-1}) = \varphi(1_R) = 1_S,$$

$$\varphi(r^{-1}) \cdot \varphi(r) = \varphi(r^{-1} \cdot r) = \varphi(1_R) = 1_S.$$

Somit: $\varphi(r) \in S^*$ und $\varphi(r)^{-1} = \varphi(r^{-1})$. $\square$

Beweis Satz Es sei $\varphi : \mathbb{K} \to \mathbb{L}$ körperhom.

Zu zeigen: Sind $a, b \in \mathbb{K}$ mit $\varphi(a) = \varphi(b)$ gegeben, so gilt $a = b$. Wir haben:

$$\varphi(a-b) = \varphi(a) - \varphi(b) = 0_{\mathbb{K}}.$$

Lemma: $a - b \notin \mathbb{K}^*$. Wegen $\mathbb{K}^* = \mathbb{K} \setminus \{0_{\mathbb{K}}\}$:

$$a - b = 0_{\mathbb{K}}$$

D.h.: $a = b$. $\square$

Bemerkung Der Ringhom. $\pi : \mathbb{Z} \to C_n,\ a \mapsto \overline{r(a;n)}$ ist nicht injektiv!

Konstruktion (Körper der komplexen Zahlen). Wir setzen

$$\mathbb{C} := \mathbb{R} \times \mathbb{R} = \{(a_1, a_2);\ a_1, a_2 \in \mathbb{R}\}$$

Komponentenweise Addition auf $\mathbb{C}$:

$$(a_1, a_2) + (b_1, b_2) := (a_1 + b_1,\ a_2 + b_2)$$

Multiplikation auf $\mathbb{C}$:

$$(a_1, a_2) \cdot (b_1, b_2) := (a_1 b_1 - a_2 b_2,\ a_1 b_2 + a_2 b_1)$$

Satz $(\mathbb{C}, +, \cdot)$ ist Körper mit

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

Weiter:

$$-(a_1, a_2) = (-a_1, -a_2) \text{ f. alle } (a_1, a_2) \in \mathbb{C}$$

$$(a_1, a_2)^{-1} = \left(\frac{a_1}{a_1^2 + a_2^2},\ \frac{-a_2}{a_1^2 + a_2^2} \right) \text{ für alle } (a_1, a_2) \in \mathbb{C} \setminus \{0_{\mathbb{C}}\}.$$

Beweis. Exemplarisch: Kommutativität von "+":

$$\begin{aligned} (a_1, a_2) + (b_1, b_2) &= (a_1 + b_1,\ a_2 + b_2) \\ &= (b_1 + a_1,\ b_2 + a_2) \\ &= (b_1, b_2) + (a_1, a_2) \end{aligned}$$

Kommutativität von "$\cdot$":

$$\begin{aligned} (a_1, a_2) \cdot (b_1, b_2) &= (a_1 b_1 - a_2 b_2,\ a_1 b_2 + a_2 b_1) \\ &= (b_1 a_1 - b_2 a_2,\ b_1 a_2 + b_2 a_1) \\ &= (b_1, b_2) \cdot (a_1, a_2). \end{aligned}$$

Inversenbildung bez. "$\cdot$":

$$\begin{aligned} &\left(\frac{a_1}{a_1^2 + a_2^2},\ \frac{-a_2}{a_1^2 + a_2^2} \right) \cdot (a_1, a_2) \\ &= \left(\frac{a_1^2}{a_1^2 + a_2^2} - \frac{-a_2^2}{a_1^2 + a_2^2},\ \frac{a_1 a_2}{a_1^2 + a_2^2} + \frac{-a_1 a_2}{a_1^2 + a_2^2} \right) \\ &= (1, 0). \end{aligned}$$

$\square$

Bemerkung Ist $a \in \mathbb{R}$ gegeben, so schreiben wir abkürzend

$$a \text{ für } (a,0) \in \mathbb{C}.$$

Weiter setzen wir

$$I := (0,1) \in \mathbb{C}.$$

Es gilt:

$$\begin{aligned} I^2 = I \cdot I &= (0,1)\cdot(0,1) \\ &= (0\cdot 0 - 1\cdot 1,\ 0\cdot 1 + 1\cdot 0) \\ &= (-1,0) \\ &= -1_{\mathbb{C}}. \end{aligned}$$

Für jedes $(a_1,a_2) \in \mathbb{C}$:

$$\begin{aligned} (a_1,a_2) &= (a_1,0)\cdot(1,0) + (a_2,0)\cdot(0,1) \\ &= a_1 \cdot 1_{\mathbb{C}} + a_2 \cdot I \\ &= a_1 + a_2 \cdot I. \end{aligned}$$

Bequemes Rechnen in $\mathbb{C}$:

$$\begin{aligned} (a_1,a_2)\cdot(b_1,b_2) &= (a_1 + a_2 \cdot I)\cdot(b_1 + b_2 \cdot I) \\ &\overset{\text{Ausmult.}}{=} a_1 b_1 + a_2 b_2 I^2 + a_1 b_2 I + a_2 b_1 \cdot I \\ &= a_1 b_1 - a_2 b_2 + (a_1 b_2 + a_2 b_1)\cdot I \end{aligned}$$

Man nennt $I = (0,1) \in \mathbb{C}$ auch die imaginäre Einheit (auch i, $\sqrt{-1}$).

Beispiel. Ab jetzt kurz 1 für $1_{\mathbb{C}}$.

$$(1+I)(1-I) = 1 - I^2 = 2,$$

$$(2-3I)^{-1} = \frac{2}{2^2+3^2} - \frac{-3}{2^2+3^2}\cdot I = \frac{2}{13} + \frac{3}{13}\cdot I$$

Bemerkung Es sei $\mathbb{K}$ Körper. Lineares Gleichungssystem über $\mathbb{K}$:

$$(*)\quad \begin{array}{rcl} a_{11}x_1 + \dots + a_{1n}x_n &=& b_1 \\ \vdots && \vdots \\ a_{m1}x_1 + \dots a_{mn}x_n &=& b_m \end{array}$$

m Gleichungen

n Unbekannte

wobei $a_{ij}, b_k \in \mathbb{K}$. Lösung von $(*)$: Tupel $(x_1, \dots, x_n) \in \mathbb{K}^n$, das alle Glg. erfüllt.

Frage: Wie löst man $(*)$ systematisch?

Antwort: "Gauß-Verfahren". Bsp.: $\mathbb{K} = \mathbb{Q}$ und

$$\begin{aligned} x_1 - x_2 + x_3 &= 1 \\ x_1 + x_2 - 3x_3 &= -1 \\ -x_2 + 2x_3 &= 1 \end{aligned}$$

Wir bringen das System durch systematische Variablenelimination auf "Zeilenstufenform":

① $-1 \cdot$ Glg. 1 zu Glg. 2 addieren:

$$\begin{aligned} x_1 - x_2 + x_3 &= -1 \\ 2x_2 - 4x_3 &= -2 \\ -x_2 + 2x_3 &= 1 \end{aligned}$$

② $\frac{1}{2} \cdot$ Glg. 2:

$$\begin{aligned} x_1 - x_2 + x_3 &= 1 \\ x_2 - 2x_3 &= -1 \\ -x_2 + 2x_3 &= 1 \end{aligned}$$

③ Glg. 2 zu Glg. 3 addieren:

$$\begin{aligned} x_1 - x_2 + x_3 &= 1 \\ x_2 - 2x_3 &= -1 \\ 0 \cdot x_3 &= 0 \end{aligned}$$

Jetzt kann man die Lösungen bestimmen

* x_3 frei wählbar
* $x_2 = 2x_3 - 1$
* $x_1 = x_2 - x_3 + 1 = 2x_3 - 1 - x_3 + 1 = x_3$

Lösungsmenge:

$$\{(x_3, 2x_3 - 1, x_3);\ x_3 \in \mathbb{Q}\}$$