# Lernziele der 11. Woche

Die Studierenden sollen:

- Beweisen können, dass der kommutative Ring $\mathbb{Z}_q$ genau dann ein Körper ist, wenn $q$ eine Primzahl ist.
- Die (algebraische) Definition der komplexen Zahlen kennen sowie komplexe Zahlen multiplizieren, invertieren und konjugieren können.
- Die Definition eines Vektorraums über einem beliebigen Körper $\mathbb{K}^n$ verstehen.
- Den Hauptsatz der Algebra kennen und mithilfe dessen die Existenz von Eigenvektoren und Eigenwerten nachweisen können.

# Anwendung: Teilbarkeitsregeln im Dezimalsystem

Seien $\alpha_n, \alpha_{n-1}, ..., \alpha_0 \in \{0, ..., 9\}$.
$\alpha_n\alpha_{n-1}...\alpha_0$ sei die Zahl $\alpha_n \cdot 10^n + ... + \alpha_0$.
(Bsp. $237 = 2 \cdot 100 + 3 \cdot 10 + 7$).
**Frage:** $2 \mid \alpha_n\alpha_{n-1}...\alpha_0$*?* (In Worten: teilt 2 die Zahl $\alpha_n\alpha_{n-1}...\alpha_0$)?
Die Antwort wissen Sie seit der Schule (die Zahl ist gerade g.d.w. die letze Ziffer 0,2,4,6, oder 8 ist); jetzt werden wir diese Antwort beweisen; die Methode erlaubt es uns, Teilbarkeitsregeln für beliebige Zahl selber zu konstruieren.
**Frage umformulieren:** *Ist* $[\alpha_n\alpha_{n-1}...\alpha_0] = [0]$ *in* $\mathbb{Z}_2$*?*
Weil $[a] = [0]$ (in $\mathbb{Z}_2$) g.d.w. $2 \mid a - 0$.
**Frage umformulieren:** *Ist* $[\alpha_n \cdot 10^n + ... + \alpha_0 \cdot 1] = [0]$ *in* $\mathbb{Z}_2$*?*
Ausrechnen:

$$[\alpha_n \cdot 10^n + ... + \alpha_0 \cdot 1] = [\alpha_n \cdot 10^n] \overset{\text{mod } 2}{+} ... \overset{\text{mod } 2}{+} [\alpha_0 \cdot 1]$$
$$= [\alpha_n] \overset{\text{mod } 2}{\cdot} [10^n] \overset{\text{mod } 2}{+} ... \overset{\text{mod } 2}{+} [\alpha_1] \overset{\text{mod } 2}{\cdot} [10] \overset{\text{mod } 2}{+} [\alpha_0] \overset{\text{mod } 2}{\cdot} [1]$$
$$= [\alpha_n] \overset{\text{mod } 2}{\cdot} [0] \overset{\text{mod } 2}{+} ... \overset{\text{mod } 2}{+} [\alpha_1] \overset{\text{mod } 2}{\cdot} [0] \overset{\text{mod } 2}{+} [\alpha_0] \overset{\text{mod } 2}{\cdot} [1]$$
$$= [\alpha_n \cdot 0 + ... + \alpha_1 \cdot 0 + \alpha_0 \cdot 1] = [\alpha_0].$$

**Antwort:** $[\alpha_n\alpha_{n-1}...\alpha_0] = [0] \iff [\alpha_0] = [0]$ in $\mathbb{Z}_2$
**Antwort umformulieren:** $\alpha_n\alpha_{n-1}...\alpha_0$ ist g.d. durch 2 teilbar, wenn $\alpha_0$ durch 2 teilbar ist.

**Frage:** $3 \mid \alpha_n\alpha_{n-1}...\alpha_0$*?*

**Frage umformulieren:** *Ist* $[\alpha_n \cdot 10^n + ... + \alpha_0 \cdot 1] = [0]$ *in* $\mathbb{Z}_3$*?*

Wir rechnen $[10^k] = \underbrace{[10] \overset{\text{mod } 3}{\cdot} [10] \overset{\text{mod } 3}{\cdot} ... \overset{\text{mod } 3}{\cdot} [10]}_{k \text{ mal}}$ in $\mathbb{Z}_3$ aus:

| $k$ | $[10^k]$ in $\mathbb{Z}_3$ |
|---|---|
| 0 | $[1]$ |
| 1 | $[10] = [3 \cdot 3 + 1] = [1]$ |
| 2 | $[10^2] = [10] \cdot [10] = [1] \cdot [1] = [1]$ |
| 3 | $[10^3] = [10^2 \cdot 10] = [1] \cdot [1] = [1]$ |
| $\vdots$ | $\vdots$ |

Deswegen:

$$
\begin{aligned}
& [\alpha_n \cdot 10^n + ... + \alpha_1 \cdot 10 + \alpha_0 \cdot 1] \\
= & [\alpha_n] \overset{\text{mod } 3}{\cdot} [10^n] \overset{\text{mod } 3}{+} ... \overset{\text{mod } 3}{+} [\alpha_1] \overset{\text{mod } 3}{\cdot} [10] \overset{\text{mod } 3}{+} [\alpha_0] \overset{\text{mod } 3}{\cdot} [1] \\
= & [\alpha_n] \overset{\text{mod } 3}{\cdot} [1] \overset{\text{mod } 3}{+} ... \overset{\text{mod } 3}{+} [\alpha_1] \overset{\text{mod } 3}{\cdot} [1] \overset{\text{mod } 3}{+} [\alpha_0] \overset{\text{mod } 3}{\cdot} [1] \\
= & [\alpha_n + ... + \alpha_1 + \alpha_0].
\end{aligned}
$$

**Antwort:** $\alpha_n\alpha_{n-1}...\alpha_0$ *ist g.d. durch 3 teilbar, wenn* $\alpha_n + \alpha_{n-1} + ... + \alpha_0$ *durch 3 teilbar ist.*

**Frage:** $4 \mid \alpha_n\alpha_{n-1}...\alpha_0$? *Ist* $[\alpha_n\alpha_{n-1}...\alpha_0] = [0]$ *in* $\mathbb{Z}_4$?

Ausrechnen $10^k$ in $\mathbb{Z}_4$:

| $k$ | $[10^k]$ in $\mathbb{Z}_4$ |
|---|---|
| 0 | $[1]$ |
| 1 | $[2]$ |
| 2 | $[2] \overset{\text{mod } 4}{\cdot} [2] = [0]$ |
| 3 | $[2] \overset{\text{mod } 4}{\cdot} [0] = [0]$ |
| $\vdots$ | $\vdots$ |
| $n \geq 3$ | $[2] \overset{\text{mod } 4}{\cdot} [0] = 0$ |

**Antwort:** $\alpha_n\alpha_{n-1}...\alpha_0$ *ist g.d. durch 4 teilbar, wenn* $2 \cdot \alpha_1 + \alpha_0$ *durch 4 teilbar ist.*

**Bsp.** 16 *ist durch 4 teilbar, da* $2 \cdot 1 + 1 \cdot 6 = 8$ *durch 4 teilbar ist.*

$$
\begin{aligned}
&[\alpha_n \cdot 10^n + ... + \alpha_1 \cdot 10 \cdot \alpha_0 \cdot 1] \\
&= [\alpha_n] \overset{\text{mod } 4}{\cdot} [10^n] \overset{\text{mod } 4}{+} ... \overset{\text{mod } 4}{+} [\alpha_1] \overset{\text{mod } 4}{\cdot} [10] \overset{\text{mod } 4}{+} [\alpha_0] \overset{\text{mod } 4}{\cdot} [1] \\
&= [\alpha_n] \overset{\text{mod } 4}{\cdot} [0] \overset{\text{mod } 4}{+} ... \overset{\text{mod } 4}{+} [\alpha_1] \overset{\text{mod } 4}{\cdot} [2] \overset{\text{mod } 4}{+} \alpha_0 \overset{\text{mod } 4}{\cdot} [1] \\
&= [2 \cdot \alpha_1 + \alpha_0].
\end{aligned}
$$

**Frage:** $7 \mid \alpha_n\alpha_{n-1}...\alpha_0$?

Ausrechnen $10^k$ in $\mathbb{Z}_7$:

| $k$ | $[10^k]$ in $\mathbb{Z}_7$ |
|---|---|
| 0 | $[1]$ |
| 1 | $[3]$ |
| 2 | $[3] \overset{\text{mod } 7}{\cdot} [3] = [9] = [2]$ |
| 3 | $[3] \overset{\text{mod } 7}{\cdot} [2] = [6] = [-1]$ |
| 4 | $[3] \overset{\text{mod } 7}{\cdot} [-1] = [-3]$ |
| 5 | $[3] \overset{\text{mod } 7}{\cdot} [-3] = [-9] = [-2]$ |
| 6 | $[3] \overset{\text{mod } 7}{\cdot} [-2] = [-6] = [1]$ |
| $\vdots$ | $\vdots$ |
| $6k$ | $[1]$ |
| $6k+1$ | $[3]$ |
| $6k+2$ | $[2]$ |
| $6k+3$ | $[-1]$ |
| $6k+4$ | $[-3]$ |
| $6k+5$ | $[-2]$ |
| $\vdots$ | $\vdots$ |

**Bsp.** 938748033764775430564 9 ist durch 7 teilbar, weil

$$1 \cdot 9 + 3 \cdot 4 + 2 \cdot 6 - 1 \cdot 5 - 3 \cdot 0 - 2 \cdot 3$$
$$+1 \cdot 4 + 3 \cdot 5 + 2 \cdot 7 - 1 \cdot 7 - 3 \cdot 4 - 2 \cdot 6$$
$$+1 \cdot 7 + 3 \cdot 3 + 2 \cdot 3 - 1 \cdot 0 - 3 \cdot 8 - 2 \cdot 4$$
$$+1 \cdot 7 + 3 \cdot 8 + 2 \cdot 3 - 1 \cdot 9 - 3 \cdot 0 - 2 \cdot 0$$
$$= 42$$ durch 7 teilbar ist.

**Antwort:** $\alpha_n...\alpha_0$ *ist g.d. durch 7 teilbar,* wenn (in $\mathbb{Z}_7$)

$$10^0 \cdot \alpha_0 + 10^1 \cdot \alpha_1 + 10^2 \cdot \alpha_2 + 10^3 \cdot \alpha_3 + 10^4 \cdot \alpha_4 + 10^5 \cdot \alpha_5 + ... +$$
$$10^{6k} \cdot \alpha_{6k} + 10^{6k+1} \cdot \alpha_{6k+1} + 10^{6k+2} \cdot \alpha_{6k+2} + 10^{6k+3} \cdot \alpha_{6k+3} + 10^{6k+4} \cdot \alpha_{6k+4} +$$
$$10^{6k+5} \cdot \alpha_{6k+5} + ... \overset{\text{in } \mathbb{Z}_7}{=} \alpha_0 + 3\alpha_1 + 2\alpha_2 - \alpha_3 - 3\alpha_4 - 2\alpha_5$$
$$+ ... + \alpha_{6k} + 3\alpha_{6k+1} + 2\alpha_{6k+2} - \alpha_{6k+3} - 3\alpha_{6k+4} - 2\alpha_{6k+5} + ...$$

gleich Null (in $\mathbb{Z}_7$) ist; also wenn das, was rechts steht, durch 7 teilbar ist.

# Zu Hause:

Teilbarkeitsregel für 37. Hinweis: $37 \mid 999 = 1000 - 1$.

# Mit diesen Methoden kann man mehrere Zahlentheoretische Aufgaben lösen

**BspAufgabe:** Z.z.: $27 \mid 10^n + 18n - 1$. **Umformulieren:** Z.z.: $[10^n + 18n - 1] = [0]$ in $\mathbb{Z}_{27}$

Ausrechnen in $\mathbb{Z}_{27}$ :

| $k$ | $[10^k]$ in $\mathbb{Z}_{27}$ |
|---|---|
| 0 | $[1]$ |
| 1 | $[10]$ |
| 2 | $[100] = [4 \cdot 27 - 8] = [-8]$ |
| 3 | $[10] \cdot [-8] = [-81 + 1] = [1]$ |
| $\vdots$ | $\vdots$ |
| $3k$ | $[1]$ |
| $3k+1$ | $[10]$ |
| $3k+2$ | $[-8]$ |
| $\vdots$ | $\vdots$ |

Für $n = 3k$ ist $[10^{3k} + 18 \cdot 3 \cdot k - 1] = [1 + 0 - 1] = [0]$,

Für $n = 3k + 1$ ist

$[10^{3k+1} + 18 \cdot (3 \cdot k + 1) - 1] = [10 + 18 - 1] = [27] = [0]$,

Für $n = 3k + 2$ ist

$[10^{3k+2} + 18 \cdot (3 \cdot k + 2) - 1] = [-8 + 18 \cdot 2 - 1] = [27] = [0]$. □

**Def.** *Seien* $a, b \in \mathbb{Z}$. *Grösster gemeinsamer Teiler von* $a, b$ *(Bezeichnung:* $ggT(a,b)$ *) ist die grösste Zahl* $m \in \mathbb{N}$ *s.d.* $m \mid a$ *und* $m \mid b$. $ggT(a,b)$ *existiert g.d.w.* $(a,b) \neq (0,0)$. *Ist* $ggT(a,b) = 1$, *so heißen* $a$ *und* $b$ *teilerfremd.*

**Satz A5** *Seien* $a, b \in \mathbb{Z}$, $(a,b) \neq (0,0)$. *Dann gilt: Es gibt* $n, m \in \mathbb{Z}$ *s.d.* $na + mb = ggT(a,b)$.

Wir beweisen zuerst die folgende

**Hilfsaussage:** $ggT(a,b) = ggT(a-b,b)$. $\quad (*)$

Tatsächlich, $\begin{array}{l} x \mid a \\ k_1 x = a \end{array}$ und $\begin{array}{l} x \mid b \\ k_2 x = b \end{array} \Rightarrow \begin{array}{l} x \mid a-b \\ (k_1 - k_2)x = a - b, \end{array}$

also die Menge

$A := \{\text{alle gem. Teiler von } a, b\}$ ist eine Teilmenge von

$B := \{\text{alle gem. Teiler von } a-b, b\}$ (d.h., $A \subseteq B$).

Analog gilt:

$\begin{array}{l} x \mid a-b \\ k_1 x = a - b \end{array}$ und $\begin{array}{l} x \mid b \\ k_2 x = b \end{array} \Rightarrow \begin{array}{l} x \mid b \\ (k_1 + k_2)x = b, \end{array}$

also die Menge

$A := \{\text{alle gem. Teiler von } a, b\}$ enthält alle Elemente von

$B := \{\text{alle gem. Teiler von } a-b, b\}$ (d.h., $A \supseteq B$).

Also, $A = B$, und die grössten Elemente der Mengen sind ebenfalls gleich.

**Satz A5** *Seien $a, b \in \mathbb{Z}$, $(a, b) \neq (0, 0)$. Dann gilt: Es gibt $n, m \in \mathbb{Z}$ s.d. $na + mb = ggT(a, b)$.*

**Beweis des Satzes:** OBdA ist $a > 0$, $b > 0$. Induktion in $N := a + b$.

IA Falls $N = a + b = 2$, ist der Satz offensichtlich.

IV Angenommen für alle $a, b \in \mathbb{Z}$, $a > 0$, $b > 0$, $a + b \leq N$ gibt es $n, m$ s.d. $na + bm = ggT(a, b)$.

IS Z.z.: Für alle $a, b \in \mathbb{Z}$, $a > 0$ $b > 0$, $a + b = N + 1$ gibt es $n, m$ s.d. $na + bm = ggT(a, b)$.

Ist $a = b$, so ist die Aussage offensichtlich: $1 \cdot a + 0 \cdot b = ggT(a, b)$.

Angenommen, $a \neq b$, oBdA sei $a > b$. Nach (IV) und Hilfsaussage gibt es $n, m_1$ s.d. $n \cdot (a - b) + m_1 \cdot b = ggT(a - b, b) \overset{(*)}{=} ggT(a, b)$. Also,

$$na + \underbrace{(m_1 - n)}_{m} b = ggT(a, b),$$

□

**Def.** Ein kommutativer Ring $(\mathbb{K}, \cdot, +)$ heißt ein Körper, falls $(\mathbb{K} \setminus \{0\}, \cdot)$ eine Gruppe ist, wobei 0 das neutrale Element in $(\mathbb{K}, +)$ ist.

**Bemerkung.** Die Gruppe $(\mathbb{K} \setminus \{0\}, \cdot)$ ist automatische abel'sch, weil „$\cdot$“ kommutativ ist.

**Bsp.** $(\mathbb{Q}, \cdot, +)$, $(\mathbb{R}, \cdot, +)$, $(\mathbb{C}, \cdot, +)$ sind Körper.

**Sazt A6.** $(\mathbb{Z}_q, \overset{\text{mod } q}{\cdot}, \overset{\text{mod } q}{+})$ ist g.d. ein Körper, wenn $q$ eine Primzahl ist.

(R1) $(\mathbb{K}, +)$ ist eine abel'sche Gruppe, deren neutrales Element werden wir mit 0 bezeichen;

(R2) die Multiplikation „$\cdot$" ist assoziativ und kommutativ.

(R3) es gilt das Distributivgesetz, d. h. für alle $a, b, c \in \mathbb{K}$ ist $a \cdot (b + c) = a \cdot b + a \cdot c$.

**Beweis $\Longleftarrow$:** Angenommen: $q$ ist eine Primzahl. Z.z.: $(\mathbb{Z}_q, \overset{\text{mod } q}{\cdot}, \overset{\text{mod } q}{+})$ ist ein Körper. $(\mathbb{Z}_q, \overset{\text{mod } q}{\cdot}, \overset{\text{mod } q}{+})$ ist ein kommutativer Ring. Z.z.: $(\mathbb{Z}_q \setminus \{[0]\}, \overset{\text{mod } q}{\cdot})$ ist eine Gruppe.
(G1) ist nach Definition des Rings erfüllt, siehe (R2).
(G2) [1] ist ein neutrales Element bzgl. $\overset{\text{mod } q}{\cdot}$.
(G3) Z.z. Für jeden $[a] \neq [0]$ gibt es ein $n$ mit $[n \cdot a] = [1]$. Da $q$ eine Primzahl ist, ist $ggT(q, a) \in \{1, q\}$. Ist $ggT(q, a) = q$, so $q \vdots a$, also $[a] = [0]$. Ist $ggT(q, a) = 1$, so gibt es nach Satz A5 die Zahlen $n, m$ mit $1 = m \cdot q + n \cdot a$. Dann $[1] = [m \cdot q + n \cdot a] = [n \cdot a]$ (d.h., $n$ ist ein inverses Element zu $a$). Offensichtlich, ist $[n] \neq [0]$. (G3) ist bewiesen.
Daraus folgt auch, dass die Operation „$\cdot$" wohldefiniert ist: wenn $[a] \neq [0]$ und $[b] \neq [0]$ sind, ist $[a] \cdot [b]$ ebenfalls nicht 0. In der Tat, wir nehmen $n$ mit $[n] \cdot [a] = [0]$. Ist $[a] \cdot [b] = [0]$, so ist $\underbrace{[n] \cdot [a]}_{[1]} \cdot [b] = [n] \cdot [0]$;
daraus folgt dass $[b] = [0]$ was uns ein Widerspruch gibt. □

**Satz A6.** $(\mathbb{Z}_q, \overset{\text{mod } q}{\cdot}, \overset{\text{mod } q}{+})$ ist g.d. ein Körper, wenn $q$ eine Primzahl ist.

**Beweis $\Longrightarrow$.** Z.z.: ist $\mathbb{K}$ eine Körper, so ist $q$ eine Primzahl. Sei $q = m \cdot n$, wobei $n \neq q$,. Dann ist $[q] = [m \cdot n]$, also $[0] = [m] \overset{\text{mod } q}{\cdot} [n]$. Dann gilt: $[0] \overset{\text{Lemma A4}}{=} [0] \overset{\text{mod } q}{\cdot} ([n]^{-1}) = [m] \overset{\text{mod } q}{\cdot} [n] \overset{\text{mod } q}{\cdot} ([n]^{-1}) = [m]$, also $[m] = [0]$, also $m = q$. □

# Bitte üben

Was ist $[2]^{-1}$ in $\mathbb{Z}_5$?
Antwort: $[3]$, weil $[3] \cdot [2] = [6] = [1]$.

**Def.** *Sei* $(\mathbb{K}, \cdot, +)$ *ein Körper. Ein Unterkörper des Körpers* $\mathbb{K}$ *ist eine Teilmenge* $\mathbb{K}' \subseteq \mathbb{K}$, $\underbrace{\textit{die mind. aus zwei Elementen besteht}}_{\textit{wird besprochen, siehe } \textbf{Bemerkung} \textit{ unten}}$, *und die abgeschlossen bzgl. Addition, Multiplikation, und Invertieren in* $(\mathbb{K}, +)$ *und* $(\mathbb{K} \setminus \{0\}, \cdot)$ *ist.*

**Satz A7.** *Unterkörper ist ein Körper (bzgl. der induzierten Operationen.)*

**Beweis.** $\mathbb{K}'$ ist eine Untergruppe der Gruppe $(\mathbb{K}, +) \overset{\text{Satz A3}}{\Longrightarrow}$ ist eine Gruppe. Da die Gruppe $(\mathbb{K}, +)$ abe'sch ist, ist auch $\mathbb{K}'$ abel'sch.

$\mathbb{K}' \setminus \{0\}$ ist eine Untergruppe der Gruppe $(\mathbb{K} \setminus \{0\}, \cdot) \overset{\text{Satz A3}}{\Longrightarrow}$ ist eine abel'sche Gruppe. □

**Bemerkung.** Ohne der Bedingung, dass $\mathbb{K}'$ mind. aus 2 Elementen besteht, ist der Satz falsch – triviales Gegenbeispiel ist die 1-elementige Teilmenge $\{0\}$. In diesem Fall ist $\mathbb{K}' \setminus \{0\} = \emptyset$ KEINE Untergruppe, weil jede Untergruppe nach Definition nicht leer ist.

**Def.** *Seien* $(\mathbb{K}_1, \cdot_1, +_1)$ und $(\mathbb{K}_2, \cdot_2, +_2)$ Körper. Eine Bijektion $\phi : \mathbb{K}_1 \to \mathbb{K}_2$ heißt ein Isomorphismus, falls für alle $a, b \in \mathbb{K}_1$ gilt:
$\phi(a \cdot_1 b) = \phi(a) \cdot_2 \phi(b)$, $(*)$
$\phi(a +_1 b) = \phi(a) +_2 \phi(b)$.
**Umgangssprachlich:** $\phi$ erhält die Operationen.
**Bemerkung** *Körperisomorphismus ist eine Äquivalenzrelation auf der Menge aller Körper.*
**Beweis.** Reflexivität und Symmetrie ist offensichtlich: ein Körper ist zu sich selbst isomorph, weil die Identitätsabbildung ein Isomorphismus ist. Wenn $(\mathbb{K}_1, \cdot_1, +_1)$ zu $(\mathbb{K}_2, \cdot_2, +_2)$ isomorph ist, also wenn es eine Bijektion $\phi : \mathbb{K}_1 \to \mathbb{K}_2$ existiert, die Operationen erhält, dann ist $(\mathbb{K}_2, \cdot_2, +_2)$ zu $(\mathbb{K}_1, \cdot_1, +_1)$ isomorph: die Abbildung $\phi^{-1}$, die nach Lemma 13 existiert, auch die Operationen erhält.
Um Transitivität zu zeigen, müssen wir zeigen, dass wenn $(\mathbb{K}_1, \cdot_1, +_1)$ zu $(\mathbb{K}_2, \cdot_2, +_2)$ isomorph ist, und $(\mathbb{K}_2, \cdot_2, +_2)$ zu $(\mathbb{K}_3, \cdot_3, +_3)$, so ist auch $(\mathbb{K}_1, \cdot_1, +_1)$ zu $(\mathbb{K}_3, \cdot_3, +_3)$ isomorph. Dazu "basteln" wir aus Isomorphismen $\phi_1 : \mathbb{K}_1 \to \mathbb{K}_2$ und $\phi_2 : \mathbb{K}_2 \to \mathbb{K}_3$ einen Isomorphismus $\phi : \mathbb{K}_1 \to \mathbb{K}_3$: wir setzten
$\phi = \phi_2 \circ \phi_1$. $\phi$ ist eine Bijektion als Verkettung von zwei Bijektionen. $\phi$ erhält die Operationen, weil z.B.
$\phi(a \cdot_1 b) = \phi_2(\phi_1(a \cdot_1 b)) \overset{(*)}{=} \phi_2(\phi_1(a) \cdot_2 \phi_1(b)) \overset{(*)}{=}$
$\phi_2(\phi_1(a)) \cdot_3 \phi_2(\phi_1(b)) = \phi_2 \circ \phi_1(a) \cdot_3 \phi_2 \circ \phi_1(b)$ □

**Def.** *Ein Körper* $(\mathbb{H}, \cdot, +)$ *heißt eine Körpererweiterung des Körpers* $(\mathbb{K}, \cdot, +)$*, falls* $\mathbb{H}$ *einen Unterkörper hat, der zu* $\mathbb{K}$ *isomorph ist.*

**Bsp.** Jede Körper ist eine Körpererweiterung von sich selbst.
$(\mathbb{R}, \cdot, +)$ ist eine Körpererweiterung von $(\mathbb{Q}, \cdot, +)$.
$(\mathbb{C}, \cdot, +)$ ist eine Körpererweiterung von $(\mathbb{R}, \cdot, +)$.
**Satz A8** *Jeder Körper ist eine Körpererweiterung von* $\mathbb{Z}_q$ *oder von* $\mathbb{Q}$
(Ohne Beweis; d.h., nur für die Information (wird auch nicht benutzt). Beweis für endliche Körper – Hausaufgabe).

# Körper von komplexen Zahlen.

**Informale Wiederholung der Definition.** Körper ist eine Menge $\mathbb{K}$ mit zwei Operationen, "+", und "$\cdot$", die bestimmte Eigenschaften erfüllen ( $\mathbb{K}$ ist Abelsche Gruppe bzgl. $+$ mit neutralem Element 0; $\mathbb{K}^* := \mathbb{K} \setminus \{0\}$ ist eine Abelsche Gruppe bzgl. $\cdot$; außerdem erfüllen die Operationen Distributivgesetz (R3)).

Der Körper von komplexen Zahlen, $\mathbb{C}$, ist als eine Menge die Menge $\mathbb{R}^2$. Die Elementen von $\mathbb{C}$ werden aber anders geschrieben: Element $\binom{a}{b}$ wird $a + ib$ geschrieben. Die Operationen $+$ und $\cdot$ sind wie folgt definiert:
$a + ib + x + iy = (a + x) + i(b + y)$ und
$(a + ib) \cdot (x + iy) = ax - by + i(ay + bx)$.
Mnemonische Regel für Produkt: man denke, dass $i = \sqrt{-1}$; d.h., man denke, dass $i^2 = -1$, und dann benutze Distributivgesetz:
$(a + \sqrt{-1}b) \cdot (x + \sqrt{-1}y) = ax + a\sqrt{-1}y + \sqrt{-1}bx + \sqrt{-1}b\sqrt{-1}y =$
$ax - by + \sqrt{-1}(ay + bx)$.
Wenn wir Elemente von $\mathbb{C}$ als Elemente von $\mathbb{R}^2$ schreiben, ist die Addition die übliche Addition in $\mathbb{R}^2$,

$$\binom{a}{b} + \binom{x}{y} = \binom{a + x}{b + y}.$$

Die Multiplikation ist in dieser Schreibweise wie folgt definiert:

$$\binom{a}{b} \cdot \binom{x}{y} = \binom{ax - by}{ay + bx}.$$

Wir zeigen jetzt, dass die Menge $\mathbb{C}$ mit den oben definierten Operationen ein Körper ist: wir müssen deswegen zeigen:
Dass $(\mathbb{C}, +)$ eine Abelsche Gruppe ist: dass ist aber offensichtlich, siehe ; neutrales element 0 ist $0 + i \cdot 0$.
Dass $(\mathbb{C} \setminus \{0\}, \cdot)$ eine Abelsche Gruppe ist:
(G1): mit Definition Assoziativität nachprüfen.
(G2): $1 + i \cdot 0$ ist ein neutrales Element.
(G3): Zum Element $a + ib \neq 0 + i \cdot 0$ ist das Element $\frac{a}{a^2+b^2} - i\frac{b}{a^2+b^2}$ ein inverses Element: nachrechnen:

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

$$= \left(a\frac{a}{a^2 + b^2} - b\frac{-b}{a^2 + b^2}\right) + i \cdot \left(\underbrace{b\frac{a}{a^2 + b^2} + a\frac{-b}{a^2 + b^2}}_{0}\right) = 1 + i \cdot 0.$$

Ausserdem soll ich Distributivgesetz beweisen: man kann dies direkt nachrechnen (werde aus Zeitgründen nicht machen).

**Wiederholung:** (Hauptdefinition aus Vorl. 3:) Vektorraum ist eine Menge $V$ mit zwei Abbildungen $+ : V \times V \to V$, $\circ : \mathbb{R} \times V \to V$ s.d. die folgende Eigenschaften erfüllt sind (für alle $u, v, w \in V$, $\lambda, \mu \in \mathbb{R}$).

I $(u + v) + w = u + (v + w)$

II $u + v = v + u$

III Es existiert ein $\vec{0} \in V$, s. d. $\vec{0} + v = v$

IV Es existiert ein $-v \in V$, s. d. $-v + v = \vec{0}$

V $(\lambda\mu)v = \lambda(\mu v)$

VI $(\lambda + \mu)v = (\lambda v + \mu v)$

VII $\lambda(u + v) = \lambda u + \lambda v$

VIII $1v = v$

**Def.** Sei $(\mathbb{K}, +, \cdot)$ ein Körper. Eine Menge $V$ mit Abbildungen
$+ : V \times V \to V$
$\circ : \mathbb{K} \times V \to V$
heißt ein Vektorraum über $\mathbb{K}$, falls die folgende Eigenschaften erfüllt sind (für alle $u, v, w \in V$, $\lambda, \mu \in \mathbb{K}$).

I $(u + v) + w = u + (v + w)$

II $u + v = v + u$

III Es existiert ein $\vec{0} \in V$, s. d. $\vec{0} + v = v$

IV Für jedes $v \in V$ es existiert ein $-v \in V$, s. d. $-v + v = \vec{0}$

V $(\lambda\mu)v = \lambda(\mu v)$

VI $(\lambda + \mu)v = (\lambda v + \mu v)$

VII $\lambda(u + v) = \lambda u + \lambda v$

VIII $1v = v$ (Wobei 1 das neutrale Element in $(\mathbb{K}, \cdot)$ ist.)

Vor Weihnachten haben wir in Beweisen nur Eigenschaften I–VIII benutzt. Deswegen sind alle Aussagen, die wir in diesen Vorlesungen bewiesen haben, auch für Vektorräume über beliebigen Körpern gültig (und die Beweise für beliebige Körper wiederholen buchstäblich die Beweise für $\mathbb{K} = \mathbb{R}$). Das war auch ein Grund, warum ich das Wort „Skalare“ statt „reelle Zahlen“ benutzt habe – der einzige Unterschied ist jetzt, dass skalare Elemente aus $\mathbb{K}$ sind.
Das betrifft u.a.: Allgemeine Theorie von Vektorräumen, Untervektorräumen, Basis, Dimension, lineare Abbildungen, Matrizen, Determinante, Behandlung linearer Gleichungssysteme, Eigenwerte, Eigenvektoren, Diagonalisierbarkeit.
Es gibt auch Aussagen, die tatsächlich einige Eigenschaften von $\mathbb{R}$ verwenden und deswegen nicht über einem beliebigen Körper richtig sind (wir haben aber diese Aussagen noch nicht gehabt:
**Bsp.** In jedem Vektorraum über $\mathbb{R}$ gilt: Ist $v \neq \vec{0}$, so ist $v + v \neq \vec{0}$.
Diese Aussage ist aber falsch in den Vektorräumen über $\mathbb{Z}_2$:
In der Tat: $v + v \overset{VI}{=} (1 + 1)v = 2v = 0v = \vec{0}$.

# $\mathbb{K}-$Vektorraum $\mathbb{K}^n$

**Bsp.** Sei $(\mathbb{K}, \cdot, +)$ ein Körper. $\mathbb{K}^n = \underbrace{\mathbb{K} \times ... \times \mathbb{K}}_{n \quad \text{Stuck}}$ ist die Menge von $n-$Tupeln $\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ mit den Operationen $\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} + \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = \begin{pmatrix} x_1 + y_1 \\ \vdots \\ x_n + y_n \end{pmatrix}$,

$\lambda \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} \lambda x_1 \\ \vdots \\ \lambda x_n \end{pmatrix}$ – dasselbe wir früher; die Elemente $x_i, y_i$ und $\lambda$ liegen jetzt in $\mathbb{K}$.

# Rechnen Sie bitte selbst

- In $(\mathbb{Z}_5)^3$ addieren Sie $\begin{pmatrix}1\\2\\3\end{pmatrix}$ und $\begin{pmatrix}4\\4\\2\end{pmatrix}$.

  **Antwort:** $\begin{pmatrix}1\\2\\3\end{pmatrix} + \begin{pmatrix}4\\4\\2\end{pmatrix} = \begin{pmatrix}5\\6\\5\end{pmatrix} \overset{\text{in } \mathbb{Z}_5}{=} \begin{pmatrix}0\\1\\0\end{pmatrix}$.

- Berechnen Sie $\det \begin{pmatrix}4 & 3\\3 & 1\end{pmatrix} \in Mat(2,2,\mathbb{Z}_5)$.

  **Antwort:** $\det \begin{pmatrix}4 & 3\\3 & 1\end{pmatrix} = 4 - 9 \overset{\text{in } \mathbb{Z}_5}{=} 4 + 1 = 5 = 0$.

- Finden Sie den Eigenvektor zum Eigenwert 0 von $\begin{pmatrix}4 & 3\\3 & 1\end{pmatrix} \in Mat(2,2,\mathbb{Z}_5)$.

  **Antwort:** Dazu müssen wir das System $\begin{pmatrix}4 & 3\\3 & 1\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix} = \begin{pmatrix}4x & +3y\\3x & +\ y\end{pmatrix} = \begin{pmatrix}0\\0\end{pmatrix}$ lösen, z.B. mit Gauss-Algorithmus. Substrahiere $\text{Zeile}_1$ von $\text{Zeile}_2$ und ersetze 4 mit $-1$ und 3 mit $-2$ in $\text{Zeile}_1$ ergibt $\begin{pmatrix}-x & -2y\\-x & -2y\end{pmatrix} = \begin{pmatrix}0\\0\end{pmatrix}$. Dann ist jeder Vektor $\begin{pmatrix}x\\y\end{pmatrix}$ mit $x = -2y$ eine Lösung. Also ist $\begin{pmatrix}-2\\1\end{pmatrix}$ ein Eigenvektor. Um sicher zu gehen kann man nachrechnen: $\begin{pmatrix}4 & 3\\3 & 1\end{pmatrix}\begin{pmatrix}-2\\1\end{pmatrix} = \begin{pmatrix}-8+3\\-6+1\end{pmatrix} \overset{\text{in } \mathbb{Z}_5}{=} \begin{pmatrix}0\\0\end{pmatrix}$

**Satz 11 (Hauptsatz der linearen Algebra)** *Zwei endlichdimensionale Vektorräume über einem Körper sind genau dann isomorph, wenn sie gleiche Dimension haben.*

# Bitte üben

**Satz 11 (Hauptsatz der linearen Algebra)** *Zwei endlichdimensionale Vektorräume über einem Körper sind genau dann isomorph, wenn sie gleiche Dimension haben.*

**Frage:** Gibt es einen Vektorraum, der aus 2 Punkten besteht? JA! Für $\mathbb{K} = \mathbb{Z}_2$ ist $\mathbb{K}^1$ ein Vektorraum; Anzahl von Punkten in $\mathbb{K}^1$ ist 2.

**Frage.** Gibt es einen Vektorraum, der aus 4 Punkten besteht? JA! Für $\mathbb{K} = \mathbb{Z}_2$ ist $\mathbb{K}^2 = (\mathbb{Z}_2)^2$ ein Vektorraum; Anzahl von Punkten in $\mathbb{K}^2$ ist die Anzahl von $2-$Zeiligen Vektoren mit sodass Einträge in der 2-Elemetiger Menge $\mathbb{Z}_2$ ist, also 4.

**Noch eine Frage für Sie:** Gibt es einen Vektorraum, der aus 6 Punkten besteht? Nein; ist aber nicht trivial (in dem Fall muss $\mathbb{K}$ endlich sein; in Hausaufgabe 4 mussen Sie zeigen, dass $\#\,\mathbb{K}$ ein Primzahlpotenz ist; und deswegen muss die Anzahl von Elementen in einem endlichen Vektorraum Primzahlpotenz sein und kann deswegen nicht 6 sein.

# Wiederholung Analysis I

Für $\mu = \underbrace{\alpha}_{\in\mathbb{R}} + i \cdot \underbrace{\beta}_{\in\mathbb{R}} \in \mathbb{C}$ ist $\bar{\mu} := \alpha - i \cdot \beta$. (Heißt $\mu-$konjugiert)

Nach Definition gilt: $\bar{\mu} = \mu \Longleftrightarrow \mu \in \mathbb{R}$, $\bar{\bar{\mu}} = \mu$. Außerdem gilt:

$\overline{\mu_1 \cdot \mu_2} = \overline{\mu_1} \cdot \overline{\mu_2}$ $(*)$

$\overline{\mu_1 + \mu_2} = \overline{\mu_1} + \overline{\mu_2}$, $(**)$

$\overline{\mu} \cdot \mu = |\mu|^2 = \alpha^2 + \beta^2$. $(***)$

**Beweis:** Ausrechnen. z.B. für $(*)$:

$\overline{(\alpha_1 + i \cdot \beta_1)(\alpha_2 + i \cdot \beta_2)} = \alpha_1\alpha_2 - \beta_1\beta_2 + i \cdot (\alpha_1\beta_2 + \alpha_2\beta_1)$;

$\overline{(\alpha_1 + i \cdot \beta_1) \cdot (\alpha_2 + i \cdot \beta_2)} = (\alpha_1 - i \cdot \beta_1)(\alpha_2 - i \cdot \beta_2) =$

$\alpha_1\alpha_2 - \beta_1\beta_2 - i \cdot (\alpha_1\beta_2 + \alpha_2\beta_1) = \overline{\alpha_1\alpha_2 - \beta_1\beta_2 + i \cdot (\alpha_1\beta_2 + \alpha_2\beta_1)}$ .

Man kann die Konjugation auch komponentenweise auf Vektoren und Matrizen anwenden, z.B.

$$\overline{\begin{pmatrix} \alpha_1 + i \cdot \beta_1 \\ \alpha_2 + i \cdot \beta_2 \\ \alpha_3 + i \cdot \beta_3 \end{pmatrix}} = \begin{pmatrix} \alpha_1 - i \cdot \beta_1 \\ \alpha_2 - i \cdot \beta_2 \\ \alpha_3 - i \cdot \beta_3 \end{pmatrix}.$$

**Rechnen Sie bitte selbst:**

$$\overline{\begin{pmatrix} 1+2i & 2-i \\ 2+i & i \end{pmatrix}} = \begin{pmatrix} 1-2i & 2+i \\ 2-i & -i \end{pmatrix}$$

Wegen $(*)$, $(**)$ und Rechenregeln für Matrizen ist dann $\overline{Av} = \overline{A}\overline{v}$.

In der Tat, die $i-$te Komponente von $Av$ ist $\sum_j a_{ij} v_j$. Konjugation davon ist $\overline{\sum_j a_{ij} v_j} \overset{(**)}{=} \sum_j \overline{a_{ij} v_j} \overset{(*)}{=} \sum_j \overline{a_{ij}}\ \overline{v_j}$, und dies ist die $i-$te Komponente von $\overline{A}\overline{v}$. Ferner gilt: Ist $A$ eine reelle Matrix, so ist $\overline{A} = A$, und deswegen $\overline{Av} = A\overline{v}$.

**Hauptsatz der Algebra (wird in der Analysis – Vorlesungen bewiesen)** *Jedes Polynom $P$ über $\mathbb{C}$ (d.h. mit komplexen Koeffizienten) mit Grad$(P) \geq 1$ hat mind. eine Nullstelle*

**Bsp.** Polynom $x^2 + 1$ hat keine Nullstelle in $\mathbb{R}$. Das Polynom kann man aber auch als Polynom über $\mathbb{C}$ auffassen, weil $\mathbb{R} \subseteq \mathbb{C}$. Das Polynom soll dann nach dem Hauptsatz der Algebra Nullstellen haben. Es hat sie: $x_1 = i$ , $x_2 = -i$ sind die Nullstellen.

**Folgerung A.** Jede Matrix über $\mathbb{C}$ hat mind. einen Eigenwert und Eigenvektor.

**Beweis.** Nach Satz 29 sind die Eigenwerte von $A$ genau die Nullstellen von $\aleph_A$. Da, nach Lemma 25 , $\aleph_A$ ein Polynom vom Grad $n \geq 1$ ist, hat $A$ mind. einen Eigenwert und deswegen auch mind. einen Eigenvektor. □

# Philosophische Frage:

*Wozu braucht man komplexe Zahlen? In der Natur gibt es doch keine komplexen Zahlen?*
**Antwort:** Mit Hilfe von komplexen Zahlen kann man auch einige Aussagen über reelle Zahlen (und deswegen auch über die Natur) beweisen/besser verstehen.
**Die folgende philosophische Frage ist ähnlich, klingt jetzt unnatürlich, war aber vor 150 Jahren aktiv vertreten und ist genauso berechtigt:** *Wozu braucht man negative Zahlen? In der Natur gibt es doch keine negativen Zahlen? (Im Bus sind -2 Leute; das bedeutet, wenn noch 2 dazu kommen ist der Bus leer.)*

Ich zeige noch zwei weitere Anwendungen des Hauptsatzes der Algebra; eine jetzt und eine in der nächste Vorlesung; mit gleichen Beweisideen

# Bezeichnung:

Für den Körper $\mathbb{K}$ bezeichne ich mit $\mathbb{K}[x]$ die Menge aller Polynome mit Koeffizienten in $\mathbb{K}$. Z.B. ist $\mathbb{R}[x]$ die Menge aller Polynome mit reellen Koeffizienten, und $\mathbb{C}[x]$ die Menge aller Polynome mit komplexen Koeffizienten.

**Wiederholung – Lemma 27; jetzt für beliebige Körper.** *Sei $P \in \mathbb{K}[x]$ ein Polynom. Ist $\lambda \in \mathbb{K}$ eine Nullstelle von $P$, so existiert genau ein Polynom $Q \in \mathbb{K}[x]$ mit $P = (x - \lambda)Q$.*
*Ferner gilt $Grad(Q) = Grad(P) - 1$.*

**Folgerung B.** *Jedes $P \in \mathbb{C}[x]$, $P \neq 0$,kann man in lineare Faktoren zerlegen (d.h. in der Form $P = a(x - x_1)(x - x_2)...(x - x_n)$ schreiben,wobei $a, x_i \in \mathbb{C}$ sind). Diese Zerlegung ist eindeutig bis auf das Umstellen von Faktoren.*

**Beweis:** Existenz: Sei $P$ ein Polynom des Grades $n \geq 1$. Nach Hauptsatz der Algebra hat es eine Nullstelle $x_1$. Nach Lemma 27 ist dann $P = (x - x_1)g$, wobei $Grad(g) = Grad(P) - 1$.Ist $Grad(g) = 0$, so ist $g = a \in \mathbb{C}$,und wir sind fertig. Sonst hat $g$ eine Nulstelle $x_2$, und deswegen (Lemma 27) ist $g = (x - x_2)h$, wobei $Grad(h) = Grad(g) - 1 = Grad(P) - 2$,also $P = (x - x_1)(x - x_2)h$, U.S.W. Nach $n$ Schritten bekommen wir $P = a(x - x_1)...(x - x_n)$.
Eindeutigkeit: Induktion nach $n$. I.A. ist trivial: hat $P$ Grad 0, so ist $P = a = b$,also $a = b$. I.V.: Angenommen, jedes Polynom des Grades $n - 1$ kann man EINDEUTIG in der Form $P = a(x - x_1)(x - x_2)...(x - x_{n-1})$ darstellen. I.S. Z.z.: Die Eindeutigkeit gilt auch für Polynome des Grades $n$. Sei $P = a(x - x_1)...(x - x_n) = b(x - y_1)...(x - y_n)$, wobei $a \neq 0 \neq b$. Da $x_1$ eine Nullstelle des Polynoms $a(x - x_1)...(x - x_n) = b(x - y_1)...(x - y_n)$ ist,ist $b(x_1 - y_1)(x_1 - y_2)...(x_1 - y_n) = 0$, und deswegen ist eines der $y_i$ gleich $x_1$. OBdA ist $y_1 = x_1$. Dividieren des Polynoms durch $(x - x_1)$ gibt $a(x - x_2)...(x - x_n) = b(x - y_2)...(x - y_n)$. Nach I.V. ist $a = b$ und die Faktoren $(x - x_i)$ sind die Faktoren $(x - y_i)$ $(i \geq 2)$, möglicherweise in anderer Reihenfolge. □

Ist $P \in \mathbb{R}[x]$, so ist $P \in \mathbb{C}[x]$, weil $\mathbb{R} \subseteq \mathbb{C}$.
**Folgerung C.** Jedes $P \in \mathbb{R}[x]$, $Grad(P) > 0$, kann man in Produkt von linearen und quadratischen Faktoren zerlegen: $P := g_1 g_2 ... g_m$, wobei $Grad(g_i) \in \{1, 2\}$.
Hilfsaussage Es sei $P = \sum_{k=0}^{n} a_k x^k \in \mathbb{R}[x] \subseteq \mathbb{C}[x]$. Dann gilt für jedes $z \in \mathbb{C}$: $P(\overline{z}) = \overline{P(z)}$ (wobei $\bar{z}$ komplexe Konjugation ist)
**Wiederholung:** Für $z = a + ib$ ist $\bar{z} = a - ib$.
Wir wiederholen (noch einmal Heute) die folgenden Eigenschaften komplexer Zahlen: $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$, $\overline{z_1 \cdot z_2} = \overline{z_1} \cdot \overline{z_2}$.
Deswegen ist $\overline{z^k} = \overline{z}^k$ für alle $k \in \mathbb{N}$. Damit erhalten wir wegen $a_k \in \mathbb{R}$
$\overline{P_n(z)} = \overline{a_n z^n + a_{n-1} z^{n-1} + \cdots + a_1 z + a_0} =$
$\overline{a_n z^n} + \overline{a_{n-1} z^{n-1}} + \cdots + \overline{a_1 z} + \overline{a_0} = a_n \overline{z}^n + a_{n-1} \overline{z}^{n-1} + \cdots + a_1 \overline{z} + a_0$.
Hilfsaussage ist bewiesen. Daraus folgt insbesondere, daß für ein $P \in \mathbb{R}[x] \subseteq \mathbb{C}[x]$ zusammen mit $P_n(c) = 0$ stets auch $P_n(\overline{c}) = 0$ gilt: Konjugieren der Gleichung $P_n(c) = 0$ ergibt $P_n(\overline{c}) = 0$. Damit ist eine Nullstelle von $P_n$ entweder reell oder die zu ihr komplex konjugierte Zahl ist ebenfalls eine Nullstelle.

Es sei nun $c = \alpha + i\beta$ mit $\alpha, \beta \in \mathbb{R}$ eine Nullstelle von $P_n$. Dann ist

$$(x-c)(x-\overline{c}) = (x-\alpha-i\beta)(x-\alpha+i\beta) = (x-\alpha)^2+\beta^2 = x^2+Ax+B \qquad (*)$$

mit $A = -2\alpha \in \mathbb{R}$, $B = \alpha^2 + \beta^2 \in \mathbb{R}$. Wir dividieren $P$ durch $x - c$ und durch $x - \overline{c}$, und erhalten wegen $(*)$ die Darstellung $P_n = (x-c)(x-\overline{c})Q_{n-2} = (x^2+Ax+B)Q_{n-2}$.
Da sowohl $P_n(x)$ als auch $x^2 + Ax + B$ ausschließlich reelle Koeffizienten besitzen, hat auch $Q_{n-2}(x)$ nur reelle Koeffizienten. Also läßt sich die Prozedur wiederholen. Nach endlich vielen Schritten bekommen wir $P := g_1 g_2 ... g_{m_1} Q_{n-2m_1}$, wobei $g_1, ..., g_{m_1}$ quadratische Polynome sind, und $Q$ hat nur reelle (d.h., keine komplexe) Nullstellen. Nach Folgerung B kann man $Q_{n-2m_1}$ in Form $a(x - x_1)...(x - x_{n-2m_1})$ schreiben, wobei $a, x_i \in \mathbb{R}$.Dann ist unser Polynom $P_n$ in Produkt von quadratischen und linearen Polynomen zerlegt:
$P_n(x) = a \cdot g_1 \cdot g_2 ... g_{m_1} \cdot (x - x_1)...(x - x_{n-2m_1})$ (das Koeffizient $a$ kann man noch in einem $g_j$ oder $(x - x_j)$ verstecken). □

**Folgerung D („Beste“ Form einer reellen $n \times n$ Matrix sodass $\aleph_A$ $n$ verschiedene (möglicherweise komplexe) Nullstellen hat)** *Sei $A \in Mat(n, n, \mathbb{R}) \subseteq Mat(n, n, \mathbb{C})$ eine Matrix, die über $\mathbb{C}$ $n$ verschiedene Eigenwerte hat. Dann gibt es eine Matrix $B \in GL_n(\mathbb{R})$ sodass die Matrix $B^{-1}AB$ die Block-diagonale Form*

$$\begin{pmatrix} \boxed{A_1} & & \\ & \ddots & \\ & & \boxed{A_m} \end{pmatrix}$$

*hat, wobei jedes $A_j$ eine $(1 \times 1)-$Matrix $(\lambda_j)$, oder eine $(2 \times 2)-$Matrix der Form $\begin{pmatrix} \alpha_j & \beta_j \\ -\beta_j & \alpha_j \end{pmatrix}$, wobei $\beta \neq 0$ ist, und alle $\lambda_k$ sowie alle $\mu_j := \alpha_j + i \cdot \beta_j$ paarweise verschieden sind. Die Einträge der $(1 \times 1)$-Blöcken sind dann die (reelle) Eigenwerte $\lambda_k$, und die $2 \times 2$-Blöcke $\begin{pmatrix} \alpha_j & \beta_j \\ -\beta_j & \alpha_j \end{pmatrix}$, entsprechen dann den Paaren von komplexwertigen Eigenwerten $\mu_j := \alpha_j + i \cdot \beta_j$ und $\bar{\mu}_j := \alpha_j - i \cdot \beta_j$*

# Beweisstrategie: (nicht nur für Folgerung D)

Wir steigen von $\mathbb{R}$ nach $\mathbb{C}$ auf: Man kann $A$ als eine Matrix über $\mathbb{C}$ auffassen (deren Einträge reell sind).
Nach Voraussetzung kann man dann eine Basis $(b_1, ..., b_n)$ in $\mathbb{C}^n$ finden (die zugehörige Transformationsmatrix bezeichnen wir mit $B$; die Spalten von $B$ sind die Basisvektoren), s.d. die Matrix von $B^{-1}AB$ Diagonalform hat. Dann steigen wir von $\mathbb{C}$ nach $\mathbb{R}$ ab: Mit Hilfe von Basisvektoren $b_i$ konstruieren wir die REELLEN Basisvektoren und bekommen die Aussage.

**Analogie: Folgerung B aus Hauptsatz der Algebra** *Jedes* $P \in \mathbb{R}[x]$, *Grad*$(P) > 0$, *kann man in Produkt von linearen und quadratrischen Faktoren zerlegen.*

**Beweis wiederholen:**

1. Man kann $P$ als Polynom über $\mathbb{C}$ auffassen und dann in Produkt von linearen Faktoren zerlegen: $P = (\lambda_1 - x)...(\lambda_n - x)a$.
2. Ist $\lambda_1$ eine nicht reelle Nullstelle, so ist $\bar{\lambda}_1$ auch eine Nullstelle (Weil $\overline{P(\lambda_1)} = P(\bar{\lambda}_1)$). Da $Q_2 := (\lambda_1 - x)(\bar{\lambda}_1 - x)$ ein (quadratisches) Polynom über $\mathbb{R}$ ist, ist $P = Q_2 P_{n-2}$, wobei $P_{n-2} \in \mathbb{R}[x]$ mit *Grad*$(P_{n-2}) = n - 2$.

Dann liefert Induktion nach $n$ die Aussage.

# Hilfsaussage vor Beweis von Folgerung D

Wir zeigen zuerst die folgende Aussage:
Sei $A \in Mat(n, n, \mathbb{R})$ und $V \in \mathbb{C}^n$ ein Eigenvektor zum Eigenwert $\mu = \alpha + i \cdot \beta$. Dann ist auch $\bar{V}$ (= „$V$ konjugiert“) ein Eigenvektor zum Eigenwert $\bar{\mu}(=\alpha - i \cdot \beta)$.

**Beweis.** Wir konjugieren die Gleichung $AV = \mu V$: Wir bekommen

$$\overline{AV} = \overline{\mu V} \overset{\text{Rechnenregeln}}{\Longrightarrow} \bar{A}\bar{V} = \bar{\mu}\bar{V} \overset{\text{Weil } A \text{ reell ist}}{\Longrightarrow} A\bar{V} = \bar{\mu}\bar{V}.$$

□

**Beweis von Folgerung D.** Wir konstruieren eine Basis von $\mathbb{R}^n$. Die Anzahl von reellen Eigenwerten sei $m \in \{0, ..., n\}$. Die ersten $m$ Vektoren $b_1, ..., b_m$ von unserer Basis seien die zugehörigen Eigenvektoren.
Für jedes Paar von komplex-konjugierten nichtreellen Eigenwerten $\mu_j = \alpha_j + i \cdot \beta_j$, $\bar{\mu}_j = \alpha_j - i \cdot \beta_j$ (wobei $\beta_j \neq 0$) betrachten wir den Eigenvektor $V_j = v_j + i \cdot u_j \in \mathbb{C}^n$ zu $\mu_j$ (wobei $v_j, u_j \in \mathbb{R}^n$ sind); und auch den konjugierten Vektor $\bar{V}_j = v_j - i \cdot u_j$. Nach Hilfsaussage ist $\bar{V}_j$ ein Eigenvektor zu $\bar{\mu}_j = \alpha_j - i \cdot \beta_j$. Wir nehmen dann die Vektoren $v_j, u_j$ in unser Tupel auf.

Wir bekommen dann ein $n-$Tupel von Vektoren: Die ersten $m-$Vektoren sind Eigenvektoren zu reellen Eigenwerten; dann kommen die Paare $v_{m+1}, u_{m+1}, ..., v_{m+\frac{n-m}{2}}, u_{m+\frac{n-m}{2}}$. Die Anzahl von Vektoren in unserem Tupel ist $n$, weil wir $n$ Eigenwerte haben, und von jedem reellen Eigenwert ein Vektor in unser Tupel kommt und von jedem Paar von komplex-konjugierten Eigenwerten $\mu, \bar{\mu}$ zwei Vektoren in unser Tupel kommen.
Das Tupel ist eine Basis: Wir müssen nur Linearunabhängigkeit zeigen.
Sei $k_1 b_1 + ... + k_m b_m + r_{m+1} v_{m+1} - s_{m+1} u_{m+1} + ... = \vec{0}$. $\quad (*)$
Wir bemerken, dass jedes
$rv - su = \text{Reelle Anteil von} \big((r + i \cdot s)(v + i \cdot u)\big)$; wir rechnen es aus:

$$((r + i \cdot s)(v + i \cdot u)) = rv - su + i \cdot (ru + sv).$$

Außerdem ist es klar, und kann rechnerisch gezeigt werden, dass

$$\text{Reelle Anteil von}\big((r + i \cdot s)(v + i \cdot u)\big) = \tfrac{1}{2}\left((r + i \cdot s)(v + i \cdot u) + \overline{(r + i \cdot s)}\,\overline{(v + i \cdot u)}\right)$$

Also, $(*)$ ist gleich

$$(k_1 b_1 + ... + k_m b_m + \tfrac{1}{2}(r_{m+1} + i \cdot s_{m+1})(v_{m+1} + i \cdot u_{m+1}) + \tfrac{1}{2}\overline{(r_{m+1} + i \cdot s_{m+1})}\,\overline{(v_{m+1} + i \cdot u_{m+1})} + ...).$$

Das ist aber eine Linearkombination über $\mathbb{C}$ von Basisvektoren von $\mathbb{C}^n$. Dann ist sie trivial, und schließlich $k_j = 0$, $s_j = 0$, $r_j = 0$ womit das Tupel $(b_1, ..., b_m, v_{m+1}, u_{m+1}, ..., v_{m+\frac{n-m}{2}}, u_{m+\frac{n-m}{2}})$ eine Basis ist.

Wie sieht die Matrix von $f_A$ in dieser Basis aus? Um es herauszufinden, müssen wir laut Vorl. 16 $Ab_j$ bzw. $Av_j$ und $Au_j$ als Linearkombination von $(b_1, ..., b_m, v_{m+1}, u_{m+1}, ..., v_{m+\frac{n-m}{2}}, u_{m+\frac{n-m}{2}})$ darstellen; die Koeffizienten sind dann die Einträge der entsprechenden Spalte.
Da $Ab_j = \lambda_j b_j$, sind die ersten $m$ Spalten gleich $\lambda_j e_j$ wie wir es wollen.
Wir werden jetzt $Av_j$ und $Au_j$ betrachten.

Dazu benutzen wir, dass $v = \frac{1}{2}\left((v + i \cdot u) + (v - i \cdot u)\right) = \frac{1}{2}(V + \bar{V})$ und $u = \frac{1}{2i}\left((v + i \cdot u) - (v - i \cdot u)\right) = \frac{1}{2i}(V - \bar{V})$.
Dann ist
$Av = \frac{1}{2}A\left((v + i \cdot u) + (v - i \cdot u)\right) \overset{\text{Weil Eigenvektoren nach Konstruction}}{=}$
$\frac{1}{2}\left((\alpha + i \cdot \beta)(v + i \cdot u) + (\alpha - i \cdot \beta)(v - i \cdot u)\right) = \alpha v - \beta u$. Also ist die entsprechende Spalte der Matrix von $f_A$ in der Basis

$(b_1, ..., b_m, v_{m+1}, u_{m+1}, ..., v_{m+\frac{n-m}{2}}, u_{m+\frac{n-m}{2}})$ gleich $\begin{pmatrix} 0 \\ \vdots \\ \alpha \\ -\beta \\ \vdots \\ 0 \end{pmatrix}$ wie wir es

wollen.
Analog gilt: $Au = \frac{1}{2i}A\left((v + i \cdot u) - (v - i \cdot u)\right) \overset{\text{Weil Eigenvektoren}}{=}$
$\frac{1}{2i}\left((\alpha + i \cdot \beta)(v + i \cdot u) - (\alpha - i \cdot \beta)(v - i \cdot u)\right) = \beta v + \alpha u$. Also ist die entsprechende Spalte der Matrix von $f_A$ in der Basis

$(b_1, ..., b_m, v_{m+1}, u_{m+1}, ..., v_{m+\frac{n-m}{2}}, u_{m+\frac{n-m}{2}})$ gleich $\begin{pmatrix} 0 \\ \vdots \\ \beta \\ \alpha \\ \vdots \\ 0 \end{pmatrix}$ wie wir es

wollen. □