

# Ziel: Satz 5 zu beweisen

**Satz 5** Sei  $f : V \rightarrow V$  ein Endomorphismus von  $n$ -dimensionalen  $\mathbb{R}$ -Vektorraum  $V$ . Angenommen, die komplexifizierung  $f_{\mathbb{C}}$  von  $f$  ist diagonalisierbar (als Endomorphismus von  $\mathbb{C}$ -Vektorraum  $V_{\mathbb{C}}$ .) Dann gibt es ein Basis  $B$  in  $V$  sodass die Matrix von  $f$  die folgende Form hat

$$\left( \begin{array}{c|c|c} \boxed{\begin{matrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_k \end{matrix}} & & \\ \hline & \boxed{\begin{matrix} \alpha_1 & \beta_1 \\ -\beta_1 & \alpha_1 \end{matrix}} & \\ \hline & & \ddots \\ \hline & & \boxed{\begin{matrix} \alpha_m & \beta_m \\ -\beta_m & \alpha_m \end{matrix}} \end{array} \right), \text{ wobei } \beta_j \neq 0 \text{ ist.}$$

( $k$  oder  $m$  können auch gleich 0 sein. Selbstverständlich gilt  $2 \cdot m + k = \dim(V)$ .)

**Bemerkung.** In LAAG I hatten wir zwei Diagonalisierbarkeitkriterien, Sätze 55, 58. Mit Hilfe von diesen Kriterien kann man entscheiden, ob eine Matrix  $A \in \text{Mat}(n, n, \mathbb{R}) \subseteq \text{Mat}(n, n, \mathbb{C})$  diagonalisierbar ist.

**Hauptsatz der Algebra (Beweis in Analysis – Vorlesungen oder in Funktionentheorie)** *Jedes  $P \in \mathbb{C}[x]$  mit  $\text{Grad}(P) \geq 1$  hat mind. eine Nullstelle*

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

**Folgerung B** *Jedes  $P \in \mathbb{R}[x]$ ,  $\text{Grad}(P) > 0$ , kann man in Produkt von lineare und quadratischen Faktoren  $g_i \in \mathbb{R}[x]$  zerlegen:  $P := g_1 g_2 \dots g_m$ , wobei  $\text{Grad}(g_i) \in \{1, 2\}$ .*

# Beweis von Folgerung B

**Hilfsaussage – letztes Mal bewiesen** Es sei

$P = \sum_{k=0}^n a_k x^k \in \mathbb{R}[x] \subseteq \mathbb{C}[x]$ . Dann gilt für jedes  $z \in \mathbb{C}$ :  $P(\bar{z}) = \overline{P(z)}$   
(wobei  $\bar{z}$  komplexe Konjugation ist)

Daraus folgt insbesondere, daß für ein  $P \in \mathbb{R}[x] \subseteq \mathbb{C}[x]$  zusammen mit  $P_n(c) = 0$  stets auch  $P_n(\bar{c}) = 0$  gilt. Damit ist eine Nullstelle von  $P_n$  entweder reell oder die zu ihr komplex konjugierte Zahl ist ebenfalls eine Nullstelle.

**Folgerung B** Jedes  $P \in \mathbb{R}[x]$ ,  $\text{Grad}(P) > 0$ , kann man in Produkt von lineare und quadratischen Faktoren  $g_i \in \mathbb{R}[x]$  zerlegen:  $P := g_1 g_2 \dots g_m$ , wobei  $\text{Grad}(g_i) \in \{1, 2\}$ .

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

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

mit  $A = -2\alpha \in \mathbb{R}$ ,  $B = \alpha^2 + \beta^2 \in \mathbb{R}$ . Wir dividieren  $P$  durch  $x - c$  und durch  $x - \bar{c}$ , und erhalten wegen  $(*)$  die Darstellung

$$P_n = (x - c)(x - \bar{c})Q_{n-2} = (x^2 + Ax + B)Q_{n-2}.$$

Da sowohl  $P_n$  als auch  $x^2 + Ax + B$  ausschließlich reelle Koeffizienten besitzen, hat auch  $Q_{n-2}$  nur reelle Koeffizienten. Also läßt sich die Prozedur wiederholen. Nach endlich viel Schritten bekommen wir

$P := g_1 g_2 \dots g_{m_1} Q_{n-2m_1}$ , wobei  $g_1, \dots, g_{m_1}$  quadratische Polynome  $\in \mathbb{R}[x]$  sind, und  $Q$  hat nur reelle Nullstelle. Nach Folgerung A kann man  $Q_{n-2m_1}$  in Form  $a(x - x_1) \dots (x - x_{n-2m_1})$  schreiben, wobei  $a, x_i \in \mathbb{R}$ .  $\square$

**Bemerkung.** OBdA haben die quadratische Polynome aus Folgerung B keine reellen Nullstellen.

**Beweis.** Falls ein quadratisches Polynom  $g \in \mathbb{R}[x]$  aus der Zerlegung  $f = g_1 \dots g_m$  eine reelle Nullstelle  $c \in \mathbb{R}$  hat, dann ist nach Lemma 27 Vorl. Fricke LAAG I  $g = (x - c)f$ . Da  $\text{Grad}(g) = \text{Grad}(f) + 1 = 2$ , ist  $f$  jedenfalls ein lineares Polynom.  $\square$

**Folgerung C** Die Vielfachheit einer nichtreellen Nullstelle  $\alpha + \beta \cdot i$  eines Polynoms  $P \in \mathbb{R}[x]$  ist gleich die Vielfachheit der konjugierten Nullstelle  $\alpha - \beta \cdot i$ .

**Beweis.** Ist  $\alpha + \beta \cdot i$  eine Nullstelle eines quadratischen Polynoms  $g \in \mathbb{R}[x]$ , so ist  $\overline{\alpha + \beta \cdot i} = \alpha - \beta \cdot i$  die zweite Nullstelle von  $g$ . Also, jedes quadratische  $g$  aus der Zerlegung von  $P$  gibt uns zwei konjugierten Nullstellen. □

# Beweis von Satz 5

Zuerst als Beispiel führen wir Beweis in Dim 2 durch.

Wir betrachten das charakteristische Polynom  $\chi_{f_{\mathbb{C}}}$  vom Endomorphismus  $f_{\mathbb{C}}$ . Da die Matrix von  $f_{\mathbb{C}}$  gleich die Matrix von  $f$  ist, ist  $\chi_{f_{\mathbb{C}}} = \chi_f$ , und deswegen sind die Koeffizienten des charakteristisches Polynoms reell.

Deswegen sind alle Nullstellen von  $\chi_{f_{\mathbb{C}}}$  reell (in dem Fall ist  $f$  bereits über  $\mathbb{R}$  diagonalisierbar nach Satz 58 LAAG I), oder hat  $\chi_{f_{\mathbb{C}}}$  einen Eigenwert  $\alpha + \beta \cdot i$  mit  $\beta \neq 0$ .

Sei  $u + v \cdot i$  ein Eigenvektor zu  $\alpha + \beta \cdot i$ . Wir zeigen:  $u - v \cdot i$  ist auch ein Eigenvektor zu  $\alpha - \beta \cdot i$ .

In der Tat,

$$f_{\mathbb{C}}(u - v \cdot i) \stackrel{\text{Rechenregeln}}{=} \overline{f_{\mathbb{C}}(u + v \cdot i)} = \overline{(\alpha + \beta \cdot i)(u + v \cdot i)} \stackrel{\text{Rechenregeln}}{=} (\alpha - \beta \cdot i)(u - v \cdot i).$$

Da die Vektoren  $u - v \cdot i$  und  $u + v \cdot i$  Eigenvektoren mit verschiedenen Eigenwerten sind, sind sie linear unabhängig und bilden deswegen eine Basis.

Dann bilden die Vektoren  $u + \vec{0} \cdot i$  und  $v + \vec{0} \cdot i$  auch eine Basis in  $V_{\mathbb{C}}$  (weil Anzahl der Vektoren gleich die Dimension des Raums ist, und die Menge ist erzeugend). Dann ist  $(u, v)$  eine Basis in  $V$ .

Offensichtlich gilt:  $u + \vec{0} \cdot i = \frac{1}{2}(u + v \cdot i + u - v \cdot i)$ ,

$$v + \vec{0} \cdot i = -\frac{i}{2}(u + v \cdot i - (u - v \cdot i)),$$

Wir rechnen jetzt die Matrix der Abbildung  $f_{\mathbb{C}}$  in der Basis.

$$f_{\mathbb{C}}(u + \vec{0} \cdot i) = f_{\mathbb{C}}\left(\frac{1}{2}(u + v \cdot i + u - v \cdot i)\right) \stackrel{\text{Linearität}}{=} \frac{1}{2}f_{\mathbb{C}}(u + v \cdot i) + \frac{1}{2}f_{\mathbb{C}}(u - v \cdot i) \stackrel{\text{Weil Eigenvektoren}}{=} \frac{1}{2}(\alpha + \beta \cdot i)(u + v \cdot i) + \frac{1}{2}(\alpha - \beta \cdot i)(u - v \cdot i) = \alpha u - \beta v + \vec{0} \cdot i.$$

$$f_{\mathbb{C}}(u + \vec{0} \cdot i) \stackrel{\text{Analog}}{=} \alpha v + \beta u + \vec{0} \cdot i.$$

Dann ist die Matrix von  $f_{\mathbb{C}}$  gleich  $\begin{pmatrix} \alpha & \beta \\ -\beta & \alpha \end{pmatrix}$  wie im Satz 5.

# Beweis für eine beliebige Dimension $n$

Wir suchen eine Basis sodass die Matrix von  $f$  wie im Satz 5 ist.

Wiederholung: Satz 54 LAAG I: Eine Matrix ist diagonalisierbar  $\iff$  es gibt eine Basis, die nur aus Eigenvektoren besteht.

Angenommen ist  $f_{\mathbb{C}}$  diagonalisierbar. Seien  $\lambda_1, \dots, \lambda_s$  die reelle Eigenwerten von  $f_{\mathbb{C}}$ .

Wir zeigen:  $geo_{f_{\mathbb{C}}}(\lambda_i) = geo_f(\lambda_i)$ . Sei  $A$  die Matrix von  $f$  (und deswegen auch von  $f_{\mathbb{C}}$ ).

$$\begin{aligned} geo_f(\lambda_i) &\stackrel{\text{Definition}}{=} \dim(\text{Kern}_{f-\lambda_i \cdot Id}) \stackrel{\text{1ste Dimensionsformel}}{=} \\ & n - \dim(\text{Bild}_{f-\lambda_i \cdot Id}) = n - rk(A - \lambda_i \cdot I) \stackrel{\text{Weil die Matrix von } f_{\mathbb{C}} \text{ auch } A \text{ ist}}{=} \\ & geo_{f_{\mathbb{C}}}(\lambda_i). \end{aligned}$$

Dann gibt es **reelle** linear unabhängige Eigenvektoren  $b_1^i, \dots, b_{alg_f(\lambda_i)}^i$  zu  $\lambda_i$ . (Offensichtlich ist  $alg_f(\lambda_i) = alg_{f_{\mathbb{C}}}(\lambda_i)$ ).

Jetzt betrachten wir die komplexen Eigenwerte von  $f_{\mathbb{C}}$ . Da das Polynom  $\mathfrak{N}_{f_{\mathbb{C}}} = \mathfrak{N}_f \in \mathbb{R}[x]$ , gilt:

Für jeden Eigenwert  $\alpha + \beta \cdot i$  ist  $\overline{\alpha + \beta \cdot i} = \alpha - \beta \cdot i$  auch ein Eigenwert (Hilfsaussage zu Folgerung B).

Angenommen,  $\alpha_1 + \beta_1 \cdot i, \alpha_1 - \beta_1 \cdot i, \dots, \alpha_m + \beta_m \cdot i, \alpha_m - \beta_m \cdot i$  sind die komplexe Eigenwerten. Hier stets  $\beta_j \neq 0$ .

Seien  $u_1 + v_1 \cdot i, \dots, u_{\text{alg}_{f_{\mathbb{C}}}(\alpha + \beta \cdot i)} + v_{\text{alg}_{f_{\mathbb{C}}}(\alpha + \beta \cdot i)} \cdot i$  linear unabhängige Eigenvektoren zum Eigenwert  $\alpha + \beta \cdot i$ . Dann gilt:

(i) die Vektoren

$\overline{u_1 + v_1 \cdot i} = u_1 - v_1 \cdot i, \dots,$   
 $\overline{u_{\text{alg}_{f_{\mathbb{C}}}(\alpha + \beta \cdot i)} + v_{\text{alg}_{f_{\mathbb{C}}}(\alpha + \beta \cdot i)} \cdot i} = u_{\text{alg}_{f_{\mathbb{C}}}(\alpha + \beta \cdot i)} - v_{\text{alg}_{f_{\mathbb{C}}}(\alpha + \beta \cdot i)} \cdot i$  sind  
Eigenvektoren zu  $\alpha - \beta \cdot i = \overline{\alpha + \beta \cdot i}$ .

(ii) Diese Eigenvektoren sind ebenfalls linear unabhängig (und deswegen bilden eine Basis in  $\text{Eig}_{\alpha - \beta \cdot i}$ ).

$$(i): \text{ wie in Dim 2: } f_{\mathbb{C}}(u - v \cdot i) \stackrel{\text{Rechenregeln}}{=} \overline{f_{\mathbb{C}}(u + v \cdot i)} = \overline{(\alpha + \beta \cdot i)(u + v \cdot i)} \stackrel{\text{Rechenregeln}}{=} (\alpha - \beta \cdot i)(u - v \cdot i).$$

(ii): Angenommen,

$(\gamma_1 + \delta_1 \cdot i)(u_1 - v_1 \cdot i) + \dots + (\gamma_k + \delta_k \cdot i)(u_k - v_k \cdot i) = \vec{0} + \vec{0} \cdot i$ . Wir konjugieren die beiden Seiten:

$$\overline{(\gamma_1 + \delta_1 \cdot i)(u_1 - v_1 \cdot i) + \dots + (\gamma_k + \delta_k \cdot i)(u_k - v_k \cdot i)} \stackrel{\text{Rechenregeln}}{=} \overline{(\gamma_1 - \delta_1 \cdot i)(u_1 + v_1 \cdot i) + \dots + (\gamma_k - \delta_k \cdot i)(u_k + v_k \cdot i)} = \vec{0} + \vec{0} \cdot i = \vec{0} + \vec{0} \cdot i.$$

Da die Vektoren  $u_j + v_j \cdot i$  linear unabhängig sind, sind die Koeffiziente  $\gamma_j - \delta_j \cdot i = 0$  folglich  $\gamma_j + \delta_j \cdot i = 0$ .

Jetzt betrachten wir das Tupel

$$\underbrace{(b_1^1 + \vec{0} \cdot i, \dots, b_{\text{alg}_f(\lambda_j)}^1 + \vec{0} \cdot i, \dots, b_1^s + \vec{0} \cdot i, \dots, b_{\text{alg}_f(\lambda_i)}^s + \vec{0} \cdot i)}_{\text{Basis in } \text{Eig}_{\lambda_1}(f)} \quad \underbrace{\dots}_{\text{Basis in } \text{Eig}_{\lambda_s}(f)} \quad \underbrace{(u_1^1 + v_1^1 \cdot i, \dots, u_{\text{alg}_f(\alpha_1 + \beta_1 \cdot i)}^1 + v_{\text{alg}_f(\alpha_1 + \beta_1 \cdot i)}^1 \cdot i)}_{\text{Basis in } \text{Eig}_f(\alpha_1 + \beta_1 \cdot i)},$$

$$\underbrace{(u_1^1 - v_1^1 \cdot i, \dots, u_{\text{alg}_f(\alpha_1 + \beta_1 \cdot i)}^1 - v_{\text{alg}_f(\alpha_1 + \beta_1 \cdot i)}^1 \cdot i, \dots)}_{\text{Basis in } \text{Eig}_{\alpha_1 - \beta_1 \cdot i}(f)}.$$

Die Vektoren sind linear unabhängig, weil die Vektoren aus verschiedenen Eigenräumen nach Satz 53 LAAG I linear unabhängig sind, und weil sie in jedem Eigenraum eine Basis bilden und deswegen auch linear unabhängig sind. Dann bilden sie eine Basis in  $V_{\mathbb{C}}$ .

Jetzt können wir die Basis konstruieren, sodass die Matrix von  $A$  wie im Satz 5 ist: wir betrachten das Tupel

$$\left( \underbrace{b_1^1, \dots, b_{\text{alg}_f(\lambda_1)}^1}_{\text{Basis in } \text{Eig}_{\lambda_1}(f)}, \dots, \underbrace{b_1^s, \dots, b_{\text{alg}_f(\lambda_s)}^s}_{\text{Basis in } \text{Eig}_{\lambda_s}(f)}, \dots, \right. \\ \left. \underbrace{u_1^1, v_1^1, \dots, u_{\text{alg}_{\alpha_1+\beta_1} \cdot i}^1, v_{\text{alg}_{\alpha_1+\beta_1} \cdot i}^1}_{\text{reelle und imaginäre Anteil von Basisvektoren in } \text{Eig}_{\alpha_1+\beta_1 \cdot i}}, \dots, \right.$$

reelle und imaginäre Anteil von Basisvektoren in  $\text{Eig}_{\alpha_1+\beta_1 \cdot i}$

$$u_1^m, v_1^m, \dots, u_{\text{alg}_{\alpha_m+\beta_m} \cdot i}^m, v_{\text{alg}_{\alpha_m+\beta_m} \cdot i}^m).$$

Anzahl Elementen im Tupel ist gleich

$$\text{alg}_{\lambda_1} + \dots + \text{alg}_{\lambda_s} + 2\text{alg}_{\alpha_1+\beta_1 \cdot i} + \dots + 2\text{alg}_{\alpha_m+\beta_m \cdot i} \stackrel{\text{Folgerung A}}{=} n.$$

Die (komplexifizierung) von Vektoren sind erzeugen in  $V_{\mathbb{C}}$ : man kann mit deren Hilfe die Basiselemente von komplexen Basis erzeugen:

$$u_i + \vec{0} \cdot i + i \cdot (v_i + \vec{0} \cdot i) = u_i + v_i \cdot i,$$

und deswegen auch alle Vektoren von  $V_{\mathbb{C}}$ .

Dann ist das Tupel eine Basis in  $V$ .

Lass uns die Matrix von  $f$  in der Basis ausrechnen:

$f(b_j) = \lambda_j b_j$ , da die Vektoren  $b_j$  aus der Basis Eigenvektoren sind, folglich ist der Koordinatenvektor von  $f(b_j) = e_j \lambda_j$ , folglich ist die  $j$ -te Spalten der Matrix wie im Satz.

$$f(u_i) = \frac{1}{2} f_{\mathbb{C}}(u_i + v_i \cdot i + u_i - v_i \cdot i) = \frac{1}{2} (f_{\mathbb{C}}(u_i + v_i \cdot i) + f_{\mathbb{C}}(u_i - v_i \cdot i)) =$$

$$\frac{1}{2} ((\alpha_i + \beta_i \cdot i)(u_i + v_i \cdot i) + (\alpha_i - \beta_i \cdot i)(u_i - v_i \cdot i)) \stackrel{\text{Ausrechnen}}{=} \alpha_i u_i - \beta_i v_i.$$

Dann ist die entsprechende Spalte der Matrix wie im Satz. Analog:

$$f(v_i) = -\frac{i}{2} f_{\mathbb{C}}(u_i + v_i \cdot i - (u_i - v_i \cdot i)) = -\frac{i}{2} (f_{\mathbb{C}}(u_i + v_i \cdot i) - f_{\mathbb{C}}(u_i - v_i \cdot i)) =$$

$$-\frac{i}{2} ((\alpha_i + \beta_i \cdot i)(u_i + v_i \cdot i) - (\alpha_i - \beta_i \cdot i)(u_i - v_i \cdot i)) \stackrel{\text{Ausrechnen}}{=} \alpha_i v_i + \beta_i u_i.$$

Dann ist die entsprechende Spalte der Matrix wie im Satz. □

# Anwendung von Körpererweiterung: Konstruktionen mit Zirkel und Lineal:

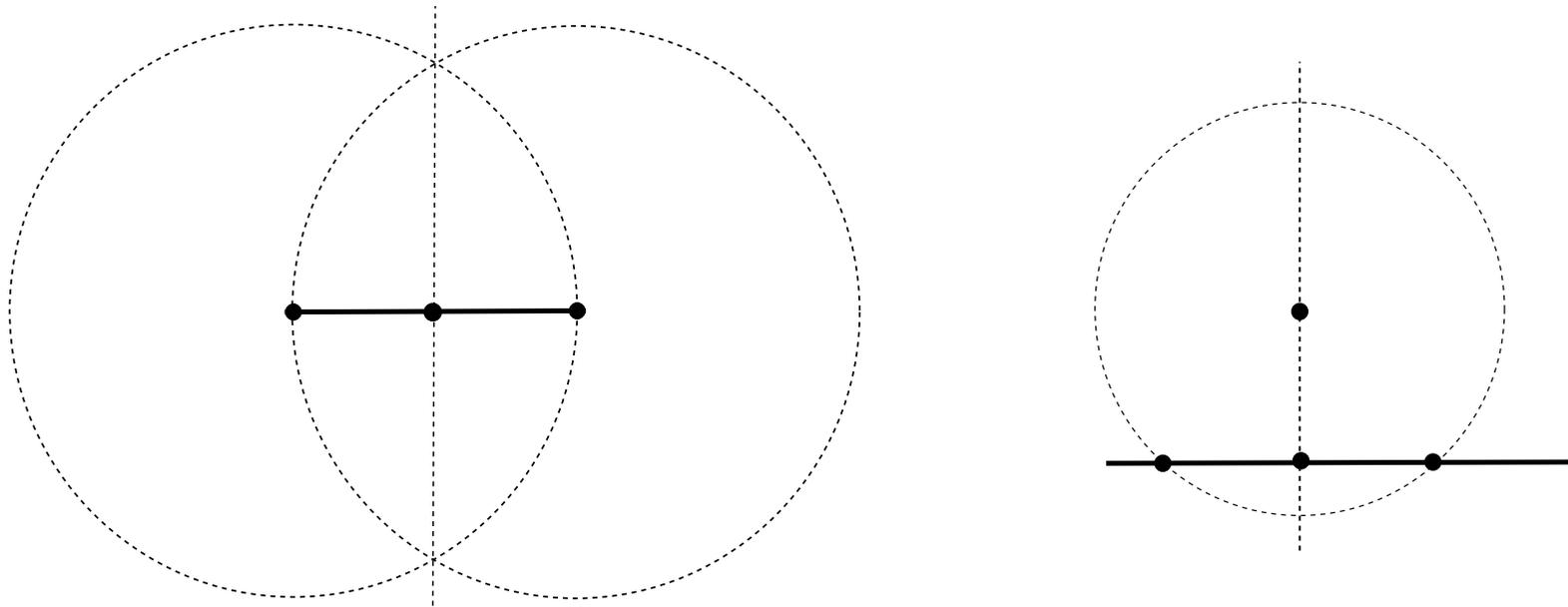
**Frage: (Euklid)** Welche geometrischen Objekten sind allein mit Zirkel und Lineal konstruierbar?

Wir definieren den Begriff „**konstruierbar**“ durch die folgenden Festlegungen: (Was darf man machen?)

(a) Die Gerade durch zwei gegebene verschiedene Punkte ist konstruierbar. (b) Der Kreis um einen gegebenen Punkt dessen Radius gleich Abstand zwischen zwei gegebenen Punkten ist konstruierbar. (c) Der Schnittpunkt von zwei sich schneidenden Geraden, (d) die Schnittpunkte eines gegebenen Kreises und einer den Kreis schneidenden gegebenen Geraden, (e) Die Schnittpunkte von zwei sich schneidenden gegebenen Kreisen sind konstruierbar.

Geometrische Gebilde (wie z.B. Punkte, Geraden, Strecken, Kreise, Dreiecke, Polygone,) die jeweils durch eine endliche Punktmenge festgelegt werden können, wollen wir vorübergehend als „**Objekte**“ bezeichnen. Wir sagen dann, das Objekt  $a$  sei bei Vorgabe der Objekte  $a_1, \dots, a_k$  **konstruierbar**, wenn es Objekte  $a_{k+1}, \dots, a_n = a$  gibt, so dass  $a_j$  bei Vorgabe der Objekte  $a_1, \dots, a_{j-1}$  konstruierbar ist für  $j = k + 1, \dots, n$ .

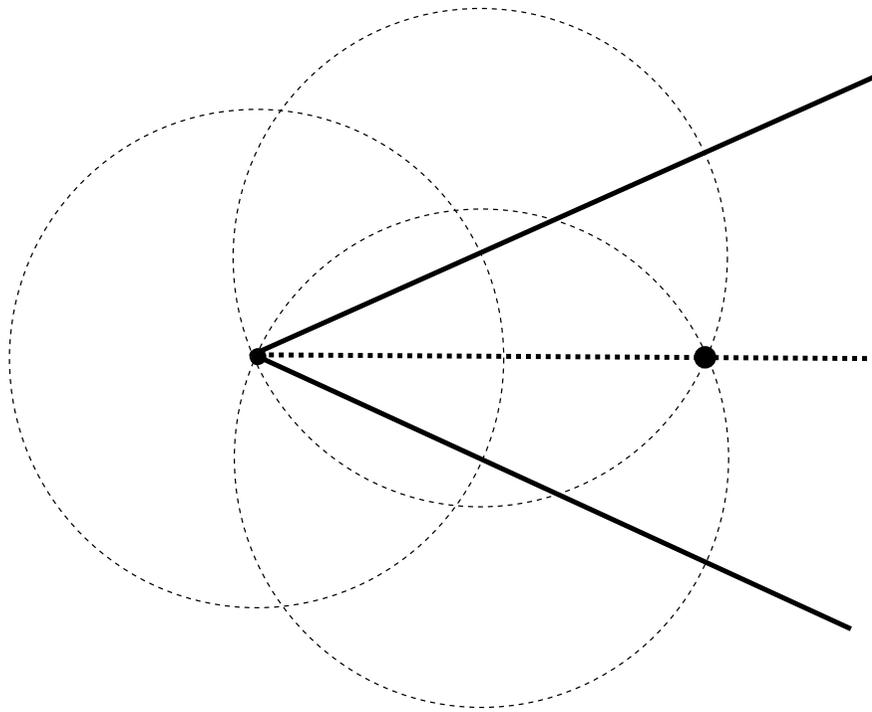
# Grundkonstruktionen aus der Schule: Mittelpunkt einer gegebenen Strecke ist konstruierbar.



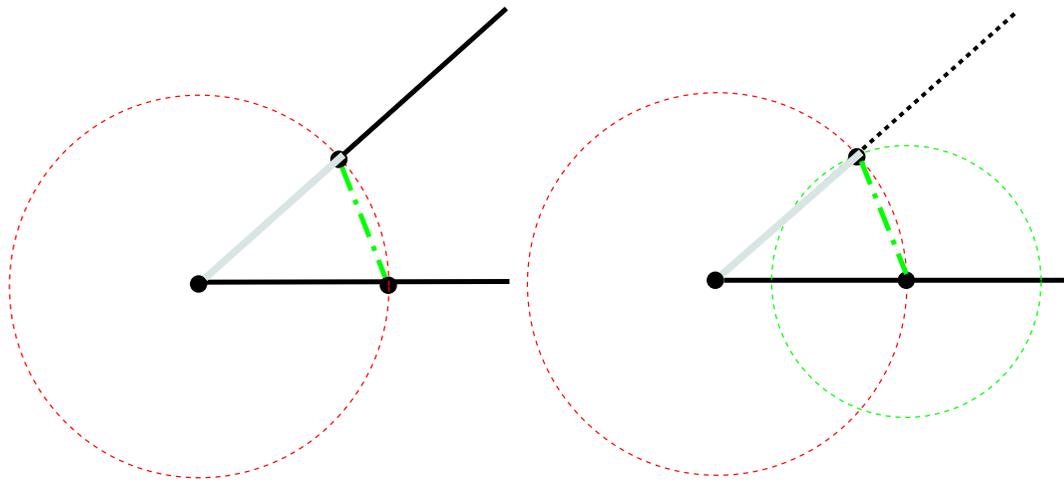
Wir haben mehr gemacht: wir haben die Gerade konstruiert, die zur gegebenen Strecke orthogonal ist. Deswegen ist

- ▶ die Senkrechte in einem gegebenen Punkt einer gegebenen Geraden konstruierbar.
- ▶ Projektion eines Punktes auf einer Gerade ist konstruierbar.

Winkelhalbierende eines gegebenen Winkels ist konstruierbar.

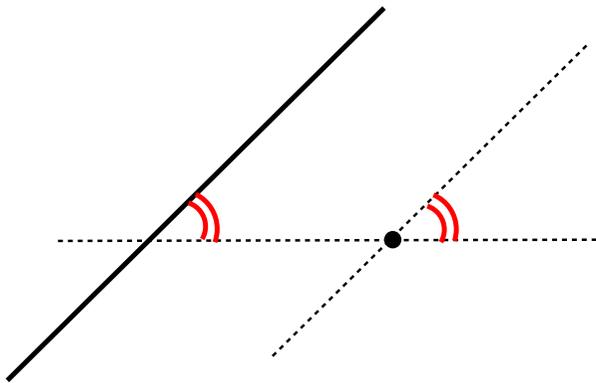


An einem gegebenen Strahl ist vom Anfangspunkt aus der Winkel abzutragen, der die gleiche Größe hat wie ein gegebener Winkel.



Ähnlich, eine Gerade durch einen gegebenen Punkt, die zu einer gegebenen Geraden parallel ist, ist konstruierbar.

An einem gegebenen Strahl ist vom Anfangspunkt aus der Winkel abzutragen, der die gleiche Größe hat wie ein gegebener Winkel.



Ähnlich, eine Gerade durch einen gegebenen Punkt, die zu einer gegebenen Geraden parallel ist, ist konstruierbar.

# Konstruierbare Zahlen

**Def. 4** Die Zahl  $a \in \mathbb{R}$  heißt *konstruierbar*, wenn bei gegebener Strecke der Länge 1 eine Strecke der Länge  $|a|$  konstruierbar ist.

**Satz 6.** Sind die Zahlen  $a, b \in \mathbb{R}$  konstruierbar, so auch die Zahlen  $a + b, a - b, ab, a/b$  (falls  $b \neq 0$ ),  $\sqrt{a}$  (falls  $a > 0$ ).

**Beweis.** Seien Strecken der Längen 1,  $a, b$  gegeben. Die Konstruktion von Strecken der Längen  $a + b$  und  $a - b$  ist trivial. Die Konstruktion von Strecken der Längen  $a/b$  und  $ab$  läßt sich an den folgenden ähnlichen Dreiecken ablesen:



Solches ähnliches Dreieck ist konstruierbar, weil eine Gerade durch einen gegebenen Punkt, die zu einer gegebenen Geraden parallel ist, konstruierbar ist.

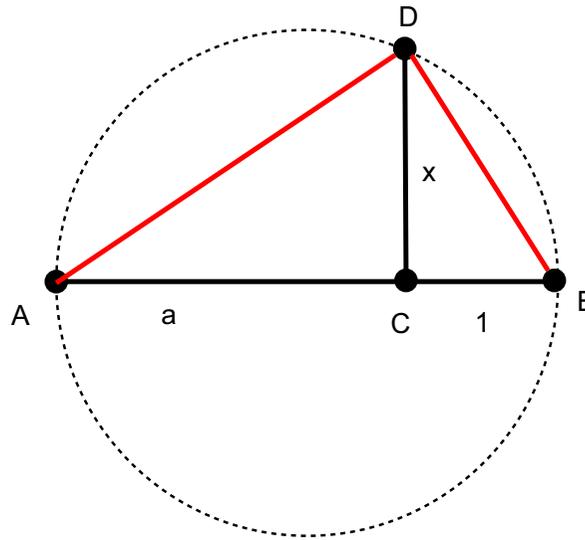
# Konstruktion von $\sqrt{a}$

Konstruiere die Strecke  $AB$  der Länge  $a + 1$ .

Konstruiere den Kreis von Radius  $(a+1)/2$  um dem Mittelpunkt der Strecke.

Konstruiere die Gerade durch  $C$ , die orthogonal zu  $AB$  ist. Sei  $D$  ein Schnittpunkt der Geraden mit dem Kreis

Die Länge von  $CD$  ist  $\sqrt{a}$ . Tatsächlich, der Winkel  $ADB$  ist  $\frac{\pi}{2}$ . (Wird auf der nächsten Folie erklärt)



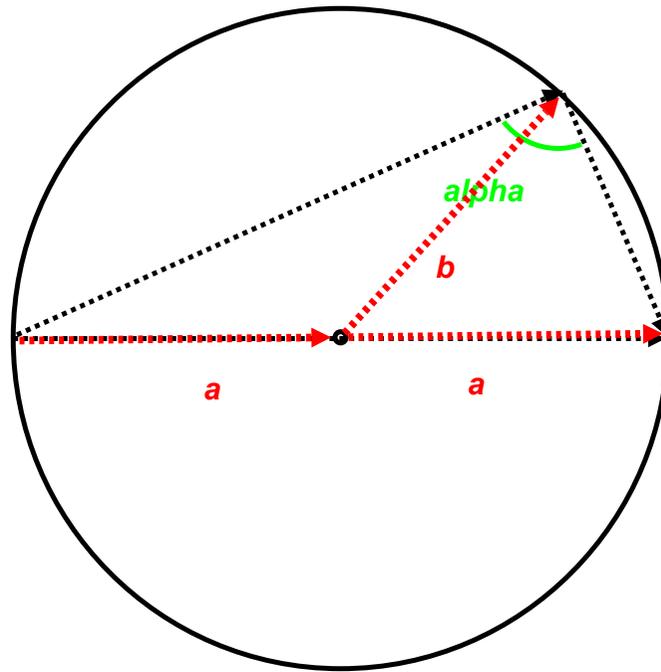
Nach Pythagoras ist

$$\begin{aligned} |AD|^2 + |BD|^2 &= |AB|^2 \\ x^2 + a^2 + x^2 + 1 &= (a + 1)^2. \end{aligned}$$

Dann  $x^2 = a$ , also  $x = \sqrt{a}$



**Z.Z.** Im Dreieck auf dem Bild ist der Winkel *alpha* gleich  $\pi/2$ .



**Beweis.** Betrachte die Vektoren  $\vec{a}, \vec{b}$  wie auf dem Bild. Wir zeigen, dass  $\langle \vec{a} + \vec{b}, \vec{a} - \vec{b} \rangle = 0$ . Wegen Bilinearität und Symmetrie, ist

$$\underbrace{\langle \vec{a} + \vec{b}, \vec{a} - \vec{b} \rangle}_{\vec{u}, \vec{v}} = \langle \vec{a}, \vec{a} \rangle + \underbrace{\langle \vec{b}, \vec{a} \rangle - \langle \vec{a}, \vec{b} \rangle}_{=0, \text{ Symmetrie}} - \langle \vec{b}, \vec{b} \rangle = \langle \vec{a}, \vec{a} \rangle - \langle \vec{b}, \vec{b} \rangle =$$

$$|a|^2 - |b|^2 = 0. \text{ Dann ist } \arccos\left(\frac{\langle \vec{u}, \vec{v} \rangle}{|\vec{u}| |\vec{v}|}\right) = \arccos(0) = \frac{\pi}{2}. \quad \square$$

**Def. 5** Wir sagen, dass ein Unterkörper  $\mathbb{K} \subseteq \mathbb{R}$  eine **iterierte quadratische Erweiterung** von  $\mathbb{Q}$  ist, falls es eine endliche Folge von quadratischen Erweiterungen

$\mathbb{K}_0, \mathbb{K}_1 = \mathbb{K}_0(\sqrt{s_1}), \mathbb{K}_2 = \mathbb{K}_1(\sqrt{s_2}), \dots, \mathbb{K}_k = \mathbb{K}_{k-1}(\sqrt{s_k}) \subseteq \mathbb{R}$  gibt, sodass  $\mathbb{K}_0 = \mathbb{Q}$  und  $\mathbb{K}_k = \mathbb{K}$ .

**Folgerung** *Liegt  $a \in \mathbb{R}$  in einer iterierten quadratischen Erweiterung von  $\mathbb{Q}$ , so ist  $a$  konstruierbar.*

**Beweis: Hausaufgabe.**