Algebra

Stephan Ehlen

08. Oktober 2018

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät

Universität zu Köln

Organisatorisches

- Website der Veranstaltung: http://www.mi.uni-koeln.de:8917
- Meine Sprechstunde: Montags, 13:00-14:00 Uhr.
- Assistent: Alexandru Ciolan, Sprechstunde: Donnerstags, 13:00-14:00 Uhr.
- Anmeldung zu den Übungen bis **Mittwoch (10.10.), 18 Uhr**.
- Sie **müssen** 3 Prioritäten angeben.
- Bitte melden Sie sich *auch* an, wenn Sie *nicht* teilnehmen wollen (Gruppe: keine Teilnahme).
- Bitte geben Sie den korrekten Studiengang an (vor allem, Lehramt Master (6 CP)).
- Die Einteilung wird am Donnerstag (11.10.) auf der Website veröffentlicht.

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Übungen

- Übungsgruppen finden ab nächster Woche statt.
- 13 Übungsblatter mit je 40 Punkten, erstes Blatt ab Mittwoch online
- Abgabe immer Mittwochs bis 18 Uhr (Briefkasten in Raum 301)
- Abgaben zu zweit erlaubt (innerhalb einer Gruppe!)
- Klausurzulassung: 50%, wobei die Übung mit der niedrigsten erreichten Punktzahl nicht zählt.
- 40 Punkte pro Blatt, d.h. sie müssen mit 12 Abgaben auf mindestens 240 Punkte kommen.
- Bis zu 2 mal 5 Punkte Bonus für Vorrechnen.
- 6-CP: Stoff bis Weihnachten, die ersten 9 Übungsblätter, davon 160 Punkte mit 8 Abgaben.

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Literatur

1. Aktuelles Skript (auf Website verfügbar, wöchtenlich aktualisiert)
2. Skript von letztem Jahr (auf Website komplett verfügbar, aber es wird Abweichungen geben und das Skript enthält Tippfehler!)
3. Bücher (z.B.) mit dem Titel Algebra von: Bosch, Fischer, Jantzen und Schwermer, Artin (en), Lang (en).

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Inhalt

- Heute: Einführung (Motivation, Anwendungen, Grundstrukturen)
- Gruppen
- Ringe und Polynome
- Körpererweiterungen
- Galoistheorie und Anwendungen

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Algebraische Gleichungen

- „Algebra“stammt aus dem Arabischen („al-jabr“):
- *Rechnen mit Gleichungen* (wörtlicher: das Zusammenfügen gebrochener Teile).
- Der Begriff wurde im 9. Jhd. geprägt, basierend auf einem Rechenlehrbuch des persischen Mathematikers al-Chwarizmi.
- In der Algebra beschäftigen wir uns mit dem Lösen von *algebraischen*, d.h. polynomiellen Gleichungen.
- Erstes Studienjahr: **Lineare** Algebra, Systeme von linearen Gleichungen (Grad 1).

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Beispiel 1

$$1 \cdot x^2 + 2 \cdot x - 1 = 0$$

Hierbei ist x, die **Unbekannte** oder **Variable** von den bekannten Größen, auch *Koeffizienten* genannt, zu unterscheiden.

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Frage: Gibt es allgemeine Lösungsformeln?

Beispiel 2 (Lineare Gleichungen)

Seien a, b vorgegeben (zum Beispiel reelle Zahlen), mit $a \neq 0$. Betrachten wir die Gleichung

$$ax + b = 0.$$

Wir stellen fest, dass diese genau eine Lösung besitzt, nämlich

$$x = -\frac{b}{a}.$$

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Beispiel 3 (Quadratische Gleichungen)

Es seien a, b, c vorgegeben. Wir betrachten die quadratische Gleichung

$$ax^2 + bx + c = 0 \tag{1}$$

OBdA können wir $a \neq 0$ annehmen (falls $a = 0$, so sind wir in Beispiel 2). Wir erhalten die Lösungen von Gleichung (1) durch die Formel

$$x = \frac{-b \pm \sqrt{D}}{2a},$$

wobei $D = b^2 - 4ac$ ist. Wir sehen, dass es folgende Fälle gibt (falls $a, b, c \in \mathbb{R}$ sind):

1. Falls $D = 0$ ist, so gibt es genau eine reelle Lösung.
2. Falls $D > 0$ ist, so gibt es zwei verschiedene reelle Lösungen.
3. Und falls $D < 0$ ist, so gibt es keine reellen, aber zwei verschiedene komplexe Lösungen.

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Beispiel 4 (Kubische Gleichungen)

Wir betrachten nun eine Gleichung vom Grad 3 (einfache Form):

$$x^3 + ax + b = 0. \tag{2}$$

Allgemein kann man eine Gleichung 3. Grades durch Substitutionen in diese Form bringen.
Cardano(1545): 1515 von del Ferro (im Wesentlichen) gelöst.
Alle Lösungen sind gegeben durch

$$\underbrace{\sqrt[3]{-\frac{b}{2} + \sqrt{D}}}_{=u} + \underbrace{\sqrt[3]{-\frac{b}{2} - \sqrt{D}}}_{=v},$$

wobei

$$D = \left(\frac{a}{3}\right)^3 + \left(\frac{b}{2}\right)^2.$$

Die beiden dritten Wurzeln müssen so in $\mathbb{C}$ gewählt werden, dass $uv = -\frac{a}{3}$ gilt.

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

$$x^3 + ax + b = 0. \tag{2}$$

$$\underbrace{\sqrt[3]{-\frac{b}{2} + \sqrt{D}}}_{=u} + \underbrace{\sqrt[3]{-\frac{b}{2} - \sqrt{D}}}_{=v},$$

wobei

$$D = \left(\frac{a}{3}\right)^3 + \left(\frac{b}{2}\right)^2.$$

Beweis.

Nachrechnen:

$$\begin{aligned}
(u+v)^3 + a(u+v) + b &= u^3 + 3u^2v + 3uv^2 + v^3 + a(u+v) + b \\
&= -\frac{b}{2} + \sqrt{D} + 3uv(u+v) - \frac{b}{2} - \sqrt{D} + a(u+v) + b \\
&= -\frac{b}{2} + \sqrt{D} - a(u+v) - \frac{b}{2} - \sqrt{D} + a(u+v) + b \\
&= 0.
\end{aligned}$$

Insgesamt 3 Lösungen (ggf. mit Vielfachheiten gezählt) durch zugelassene Wahlen der Wurzeln. Also: dies ist eine allgemeine Lösungsformel. □

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Beispiel 5 (Quartische Gleichungen)

- Cardano (1545), Ferrari: explizite Lösungsformeln auch für polynomielle Gleichungen 4. Grades.
- Siehe zum Beispiel Abschnitt 6.2 im Buch von Bosch.

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Gleichungen vom Grad 5 (oder höher)

- Lange wurde nach weiteren Lösungsformeln gesucht.
- Satz von Abel-Ruffini (1799-1824): Die *allgemeine Gleichung* n-ten Grades ist für $n \geq 5$ **nicht** *durch Radikale auflösbar*.
- Durch Radikale auflösbar heißt: die Lösungen sind nur duch **Wurzelausdrücke** sowie **rationale Ausdrücke** in den Koeffizienten gegeben.
- Vorsicht: Der Satz besagt: es gibt keine *allgemeine* Lösungsformel. In Spezialfällen kann es solche Ausdrücke für eine spezielle Gleichung natürlich geben! (Und gibt es sie auch in vielen Fällen.)

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Galoistheorie

- Unser Held: Evariste Galois (1811 – 1832)

- Er lieferte eine differenziertere Antwort.
- Der Clou: Eine Beziehung zwischen algebraischen Gleichungen und Gruppentheorie.
- Z.B. gilt für eine Polynomfunktion $f : \mathbb{C} \to \mathbb{C}$, dass $f(x) = 0$ genau dann (durch Radikale) auflösbar ist, wenn die so genannte Galois-Gruppe von f auflösbar ist (wir lernen noch, was das heißt).

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Ein erstes Beispiel: DIe Galoisgruppe einer Gleichung

- Sei $\zeta_5 = e^{\frac{2\pi i}{5}} \in \mathbb{C}$.
- Die komplexe Zahl ζ_5 ist eine 5-te Einheitswurzel, d.h. Nullstelle des Polynoms
$$p(X) = X^5 - 1$$
vom Grade 5.
- Faktorisiere p:
$$p(X) = (X-1)q(X)$$
mit $q(X) = X^4 + X^3 + X^2 + X + 1$.
- Und da $\alpha_1 := \zeta_5 \neq 1$, ist ζ_5 bereits Nullstelle von q.
- Die 3 weiteren Nullstellen von q sind $\alpha_2 := \zeta_5^2, \alpha_3 := \zeta_5^3$ und $\alpha_4 := \zeta_5^4$.

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

- Ordne dem Polynom $q = X^4 + X^3 + X^2 + X + 1$ (oder der Körpererweiterung $\mathbb{Q} \subset \mathbb{Q}(\zeta_5)$) nun wie folgt eine Gruppe zu:
- Beobachtung: Relationen zwischen den Nullstellen von q:
  1. $\alpha_1^2 = \alpha_2$
  2. $\alpha_1^3 = \alpha_3$
  3. $\alpha_1^4 = \alpha_4$
  4. $\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 = -1$
- Definiere G als die Menge der Permutationen der Nullstellen $\alpha_1, \alpha_2, \alpha_3$ und α_4, so dass diese Relationen erhalten bleiben.
- Eine solche Permutation σ ist wegen der ersten 3 Relationen bereits durch das Bild $\sigma(\alpha_1)$ von α_1 bestimmt!
- Es gibt also 4 solche Permutationen und die Gruppe G kann man mit der additiven Gruppe $(\mathbb{Z}/4\mathbb{Z}, +)$ identifizieren:

$$G = \{\sigma_0 = \mathrm{id}, \sigma_1 : \zeta_5 \mapsto \zeta_5^2, \sigma_3 : \zeta_5 \mapsto \zeta_5^3, \sigma_2 : \zeta_5 \mapsto \zeta_5^4\} \cong \mathbb{Z}/4\mathbb{Z},$$

  wobei der Gruppenisomorphismus durch $\sigma_j \mapsto j$ gegeben ist.
- Wir schauen uns das später noch alles in Ruhe an.

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

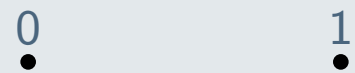
Konstruktionen mit Zirkel und Lineal

- Gegeben: $E \subset \mathbb{C} \cong \mathbb{R}^2$ Menge an Punkten im Raum.
- Identifiziere $\mathbb{R}^2 \cong \mathbb{C}$.
- **Elementare euklidische Figuren**:
  1. Konstruiere eine Gerade durch zwei verschiedene Punkte (Lineal) in E.
  2. Konstruiere einen Kreis, dessen Mittelpunkt in E liegt und der durch einen weiteren Punkt in E verläuft (Zirkel).
- E_1: Menge der Schnittpunkte elementarer euklidischer Figuren (die man aus $E = E_0$ erhält).
- E_2: Menge der Schnittpunkte elementarer euklidischer Figuren (die man aus E_1 erhält).
- $\hat{E} = \bigcup_{j=0}^{\infty} E_j =$ Menge der aus E konstruierbaren Punkte.
- Ein Punkt $p \in \mathbb{C}$ heißt *aus E (elementar) konstruierbar*, wenn er ein Schnittpunkt elementarer euklidischer Figuren ist (den man *induktiv* nach **endlich** vielen Konstruktionsschritten erhält). D.h.: $p \in \hat{E}$.

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Beispiel 6

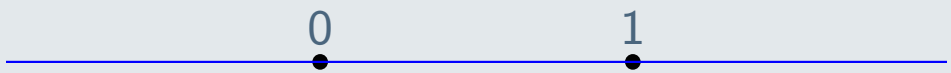
Sei $E = \{0, 1\}$ gegeben. Wir wollen $\frac{1}{2}$ konstruieren (oder allgemeiner den Mittelpunkt auf der Strecke zwischen zwei Punkten).



Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Beispiel 6

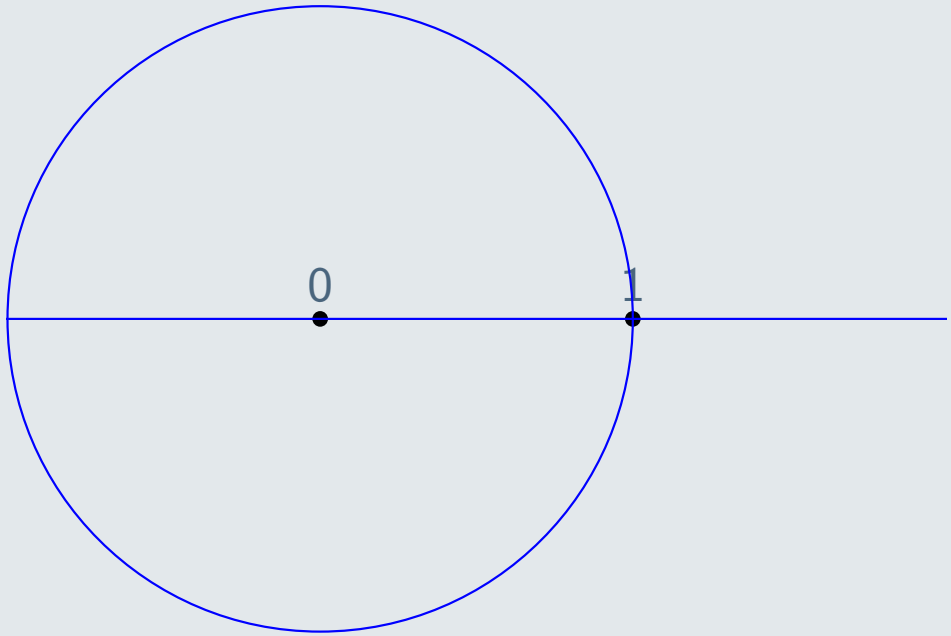
Sei $E = \{0, 1\}$ gegeben. Wir wollen $\frac{1}{2}$ konstruieren (oder allgemeiner den Mittelpunkt auf der Strecke zwischen zwei Punkten).



Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Beispiel 6

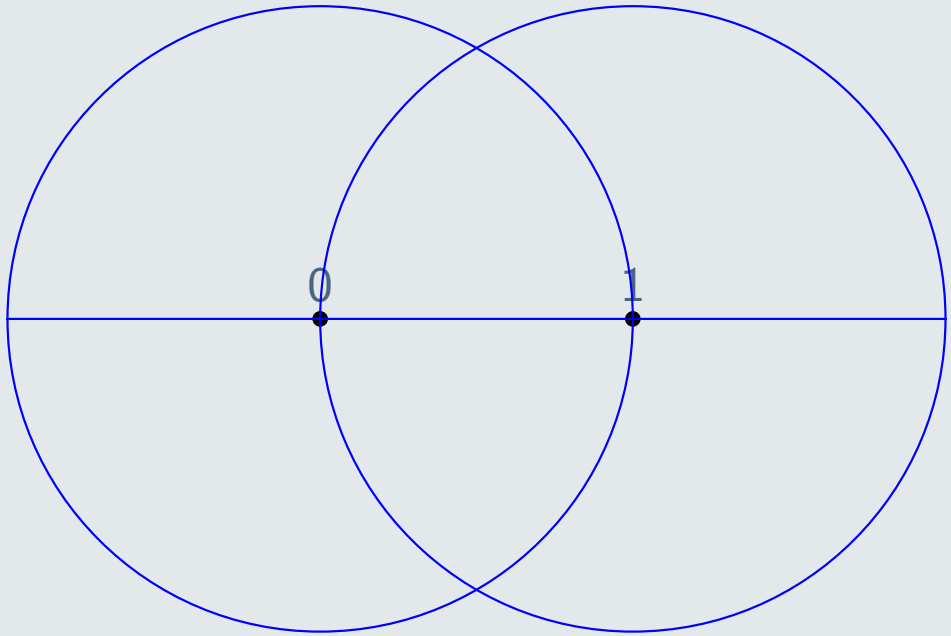
Sei $E = \{0, 1\}$ gegeben. Wir wollen $\frac{1}{2}$ konstruieren (oder allgemeiner den Mittelpunkt auf der Strecke zwischen zwei Punkten).



Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Beispiel 6

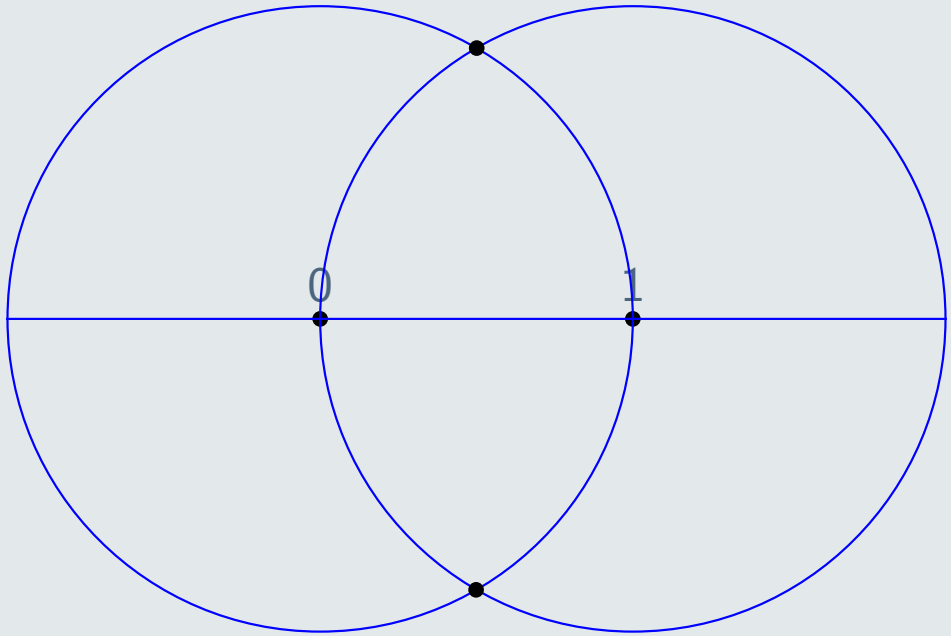
Sei $E = \{0, 1\}$ gegeben. Wir wollen $\frac{1}{2}$ konstruieren (oder allgemeiner den Mittelpunkt auf der Strecke zwischen zwei Punkten).



Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Beispiel 6

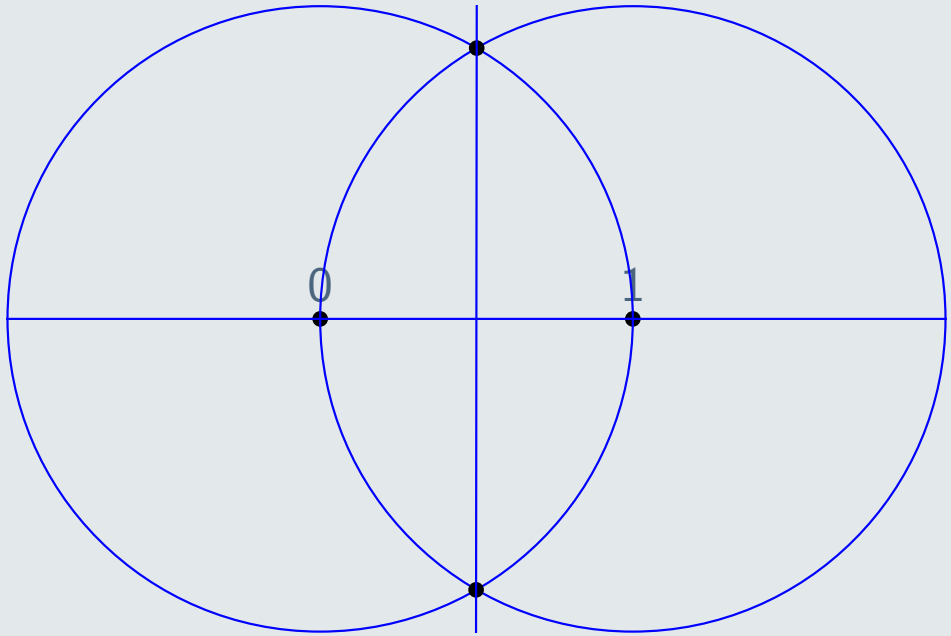
Sei $E = \{0, 1\}$ gegeben. Wir wollen $\frac{1}{2}$ konstruieren (oder allgemeiner den Mittelpunkt auf der Strecke zwischen zwei Punkten).



Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Beispiel 6

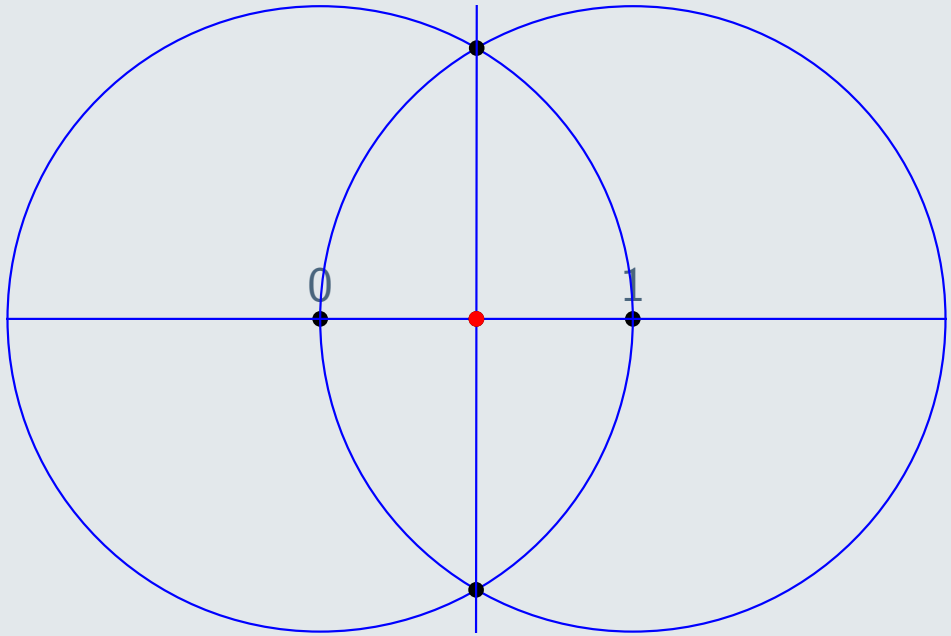
Sei $E = \{0, 1\}$ gegeben. Wir wollen $\frac{1}{2}$ konstruieren (oder allgemeiner den Mittelpunkt auf der Strecke zwischen zwei Punkten).



Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Beispiel 6

Sei $E = \{0, 1\}$ gegeben. Wir wollen $\frac{1}{2}$ konstruieren (oder allgemeiner den Mittelpunkt auf der Strecke zwischen zwei Punkten).



Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Klassische Konstruktionsprobleme

Aus der Antike sind folgende klassischen Konstruktionsprobleme überliefert.

1. **Winkeldreiteilung**: Gegeben einen Winkel α, unterteile ihn in 3 gleich große Winkel. Übersetzt: Ist für $E = \{0, 1, \cos(\alpha)\}$ auch $\cos(\alpha/3) \in \hat{E}$?
2. **Das Delische Problem der Würfelverdopplung**: Konstruiere zu einem gegebenen Würfel einen Würfel mit doppeltem Volumen. Äquivalent: $E = \{0, 1\}$; Ist $\sqrt[3]{2} \in \hat{E}$?
3. **Quadratur des Kreises**: Gegeben einen Kreis, konstruiere ein Quadrat mit dem gleichen Flächeninhalt. Äquivalent: $\sqrt{\pi} \in \hat{E}$ für $E = \{0, 1\}$.
4. **Konstruktion eines regelmäßigen n-Ecks**. Äquivalent: Ist für $E = \{0, 1\}$ der Punkt $e^{\frac{2\pi i}{n}} \in \hat{E}$?

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

- Mit algebraischen Methoden kann zeigen: die ersten drei Konstruktionsprobleme (Winkeldreiteilung, Würfelverdopplung, Quadratur des Kreises) sind im allgemeinen *unlösbar* (mit Zirkel und Lineal wie oben beschrieben)!
- Wir werden dies schon bald beweisen können, und dazu die Theorie der Körpererweiterungen benutzen.
- Für das regelmäßige n-Eck waren in der Antike beispielsweise Konstruktionen für $n \in \{2, 3, 4, 5, 6, 8\}$ bekannt.
- C. F. Gauß (1796): das regelmässige 17-Eck ist konstruierbar. Später im Semester: ein algebraisches Kriterium für die Konstruierbarkeit.

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

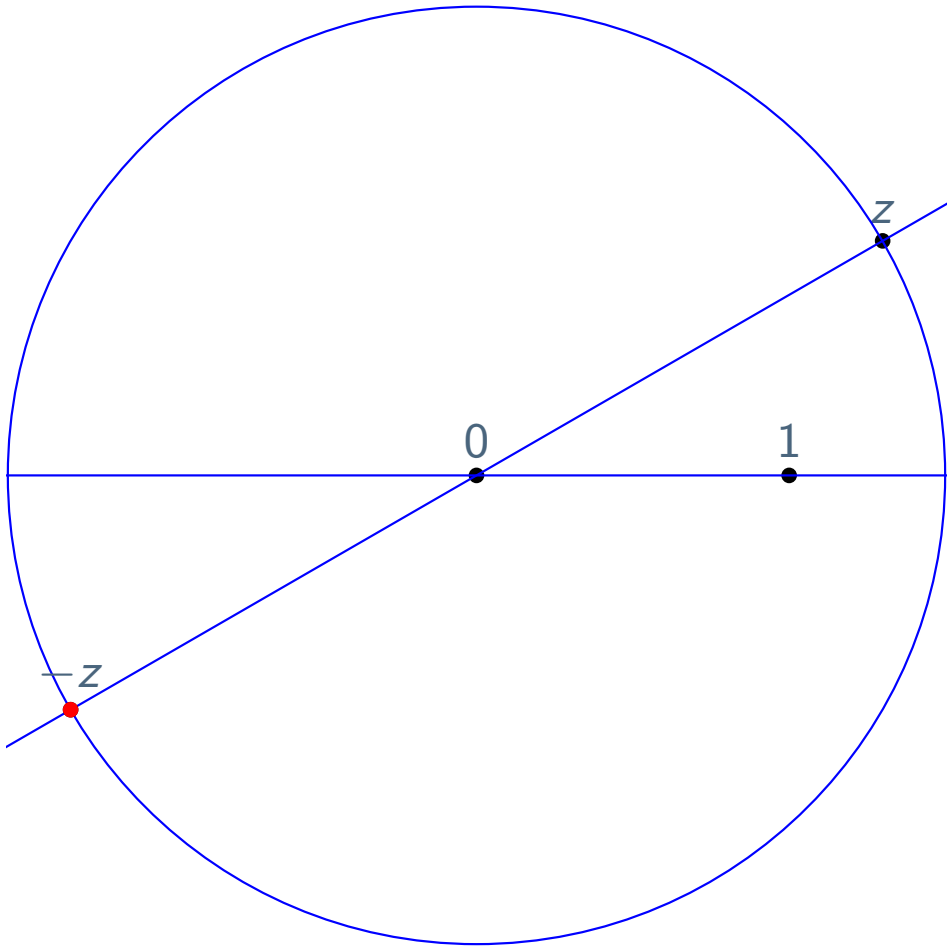
Der Körper der konstruierbaren Zahlen

- Wir wollen jetzt zeigen: Die Menge $\hat{E} \subset \mathbb{C}$ aller konstruierbarer Zahlen ist ein Teilkörper von $\mathbb{C}$.
- D.h.: im einzelnen:
- $0, 1 \in \hat{E}$ (Neutrale Elemente): klar.
- Mit $a \in E$ und $b \in E$ sind auch $ab, a + b \in \hat{E}$ (Abgeschlossenheit unter Multiplikation und Addition)
- Außerdem ist zu $a \in \hat{E}$ auch $-a \in \hat{E}$ und falls $a \neq 0$, so ist auch $a^{-1} \in \hat{E}$ (Existenz der Inversen).
- Wir führen beispielhaft die Addition vor, ein paar weitere Konstruktionen sind Übung.

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Additive Inverse

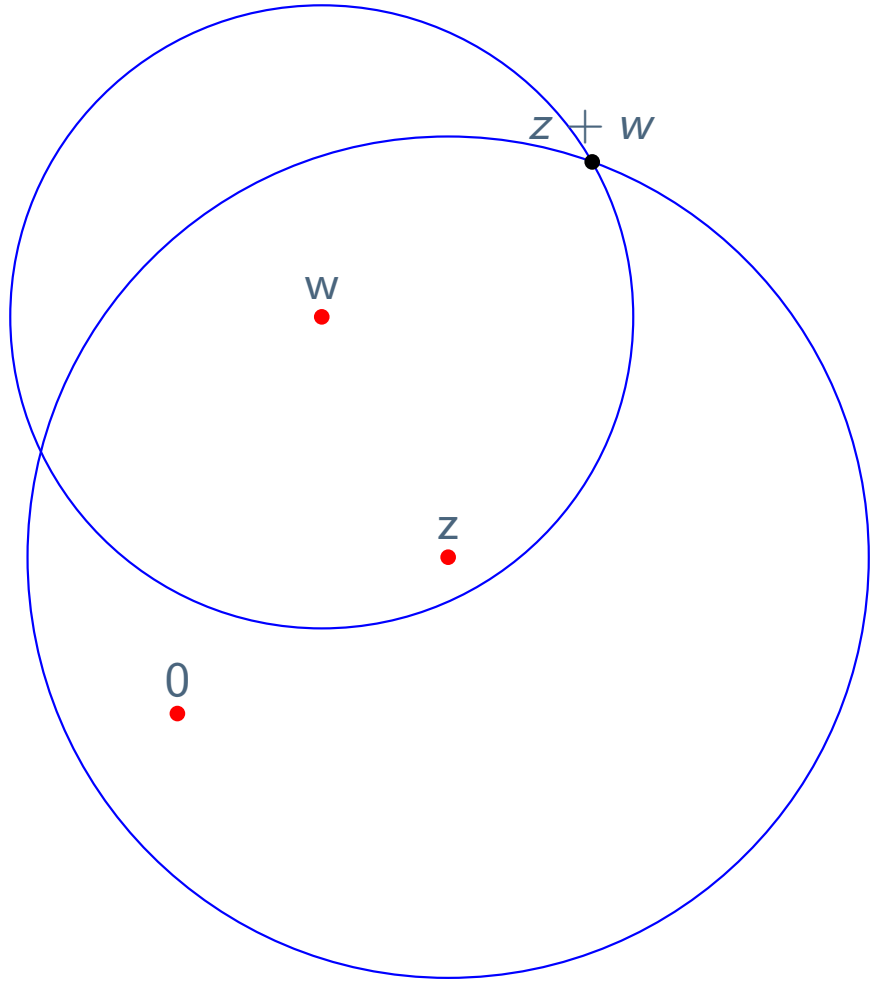
Gegeben $z \in \mathbb{C}$, konstruiere $-z$:



Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Addition

Gegeben $z, w \in \mathbb{C}$, konstruiere $z + w$ (Fall $z \neq w$). Die Idee: Konstruiere Kreis mit Radius $|z|$ um w und Kreis mit Radius $|w|$ um z. Der Schnittpunkt ist $z + w$.

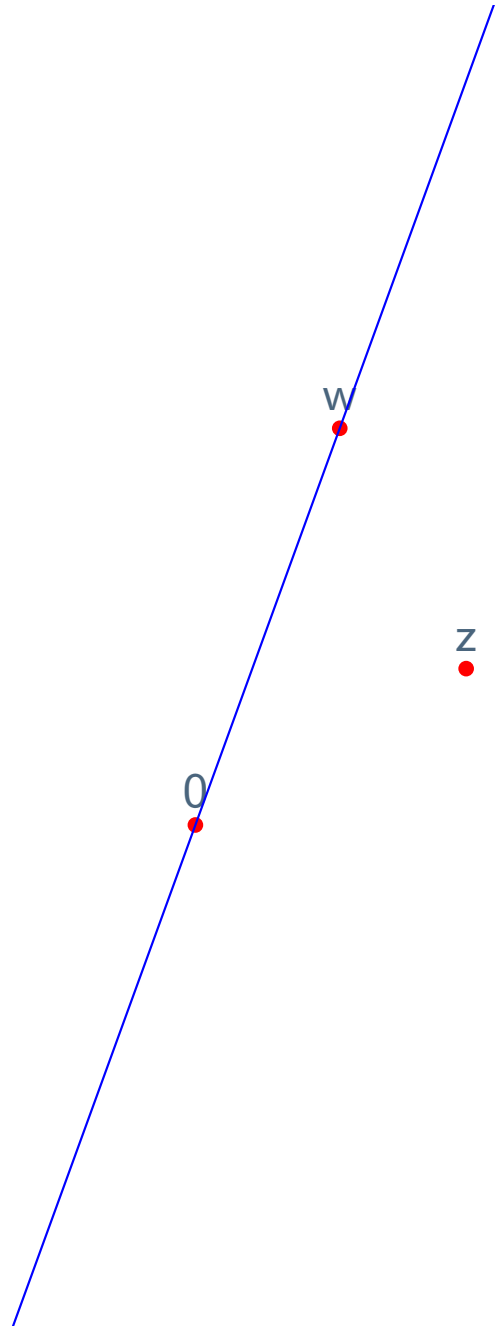


Addition

Gegeben $z, w \in \mathbb{C}$, konstruiere $z + w$ (Fall $z \neq w$):

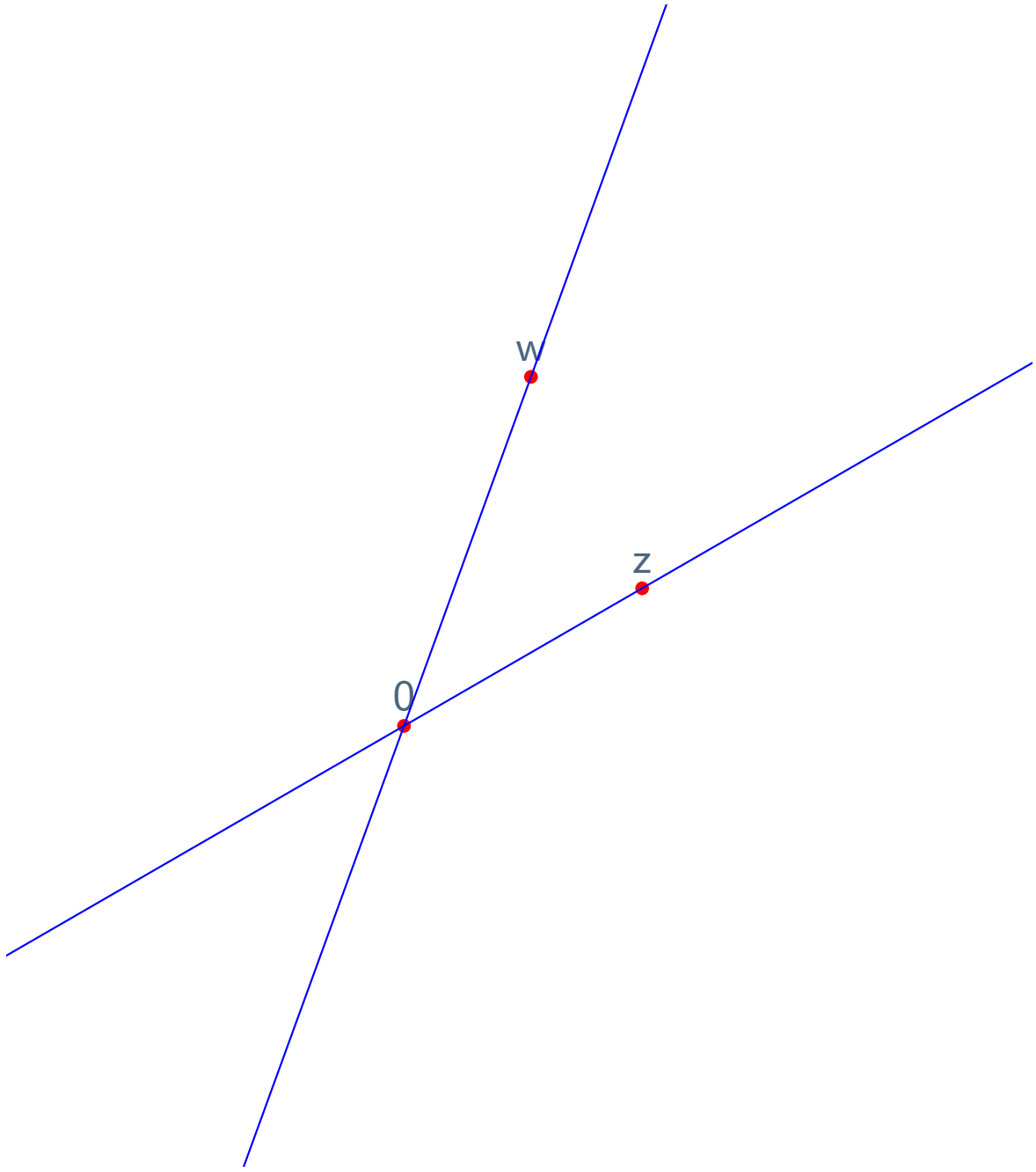
Addition

Gegeben $z, w \in \mathbb{C}$, konstruiere $z + w$ (Fall $z \neq w$):



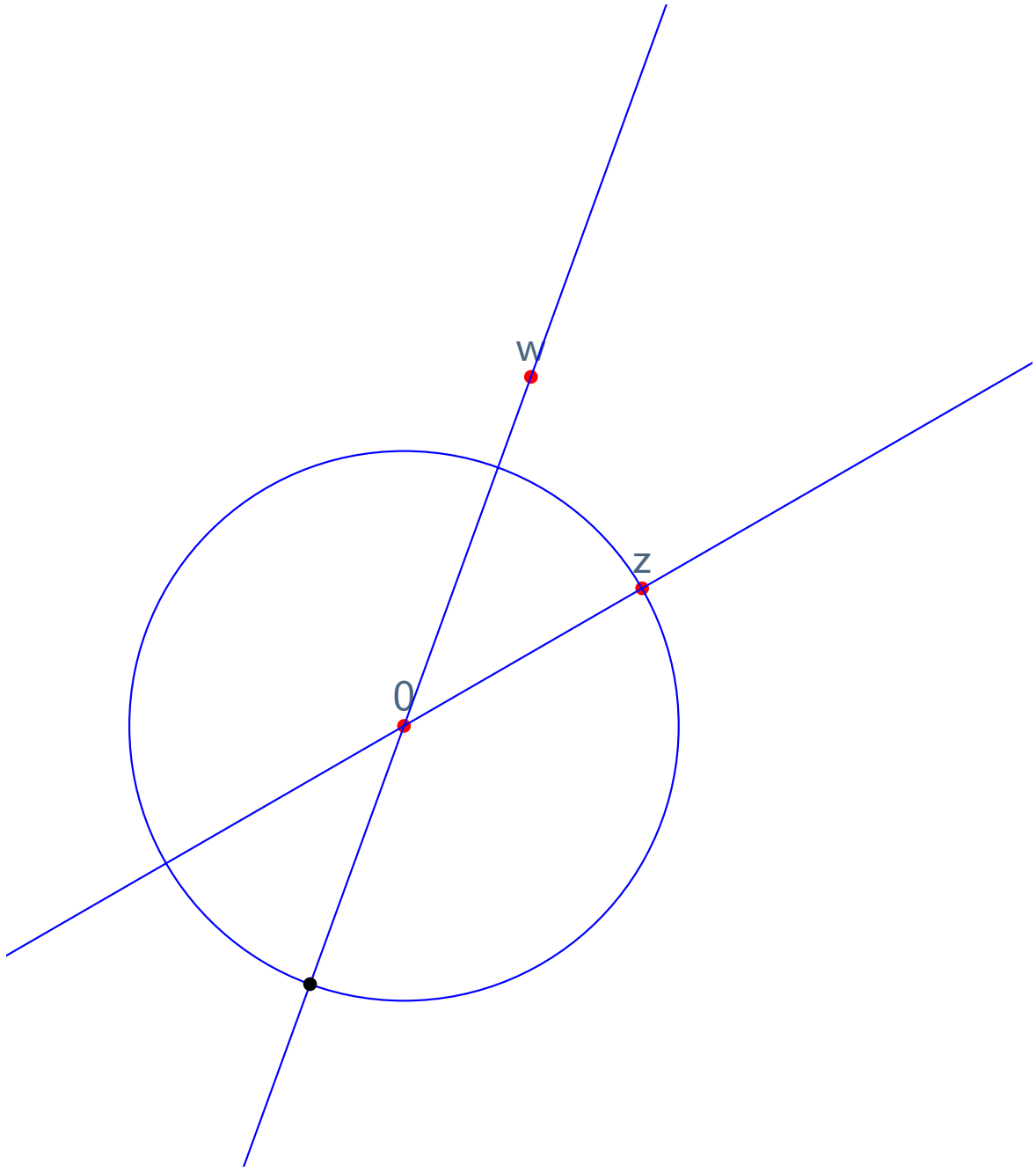
Addition

Gegeben $z, w \in \mathbb{C}$, konstruiere $z + w$ (Fall $z \neq w$):



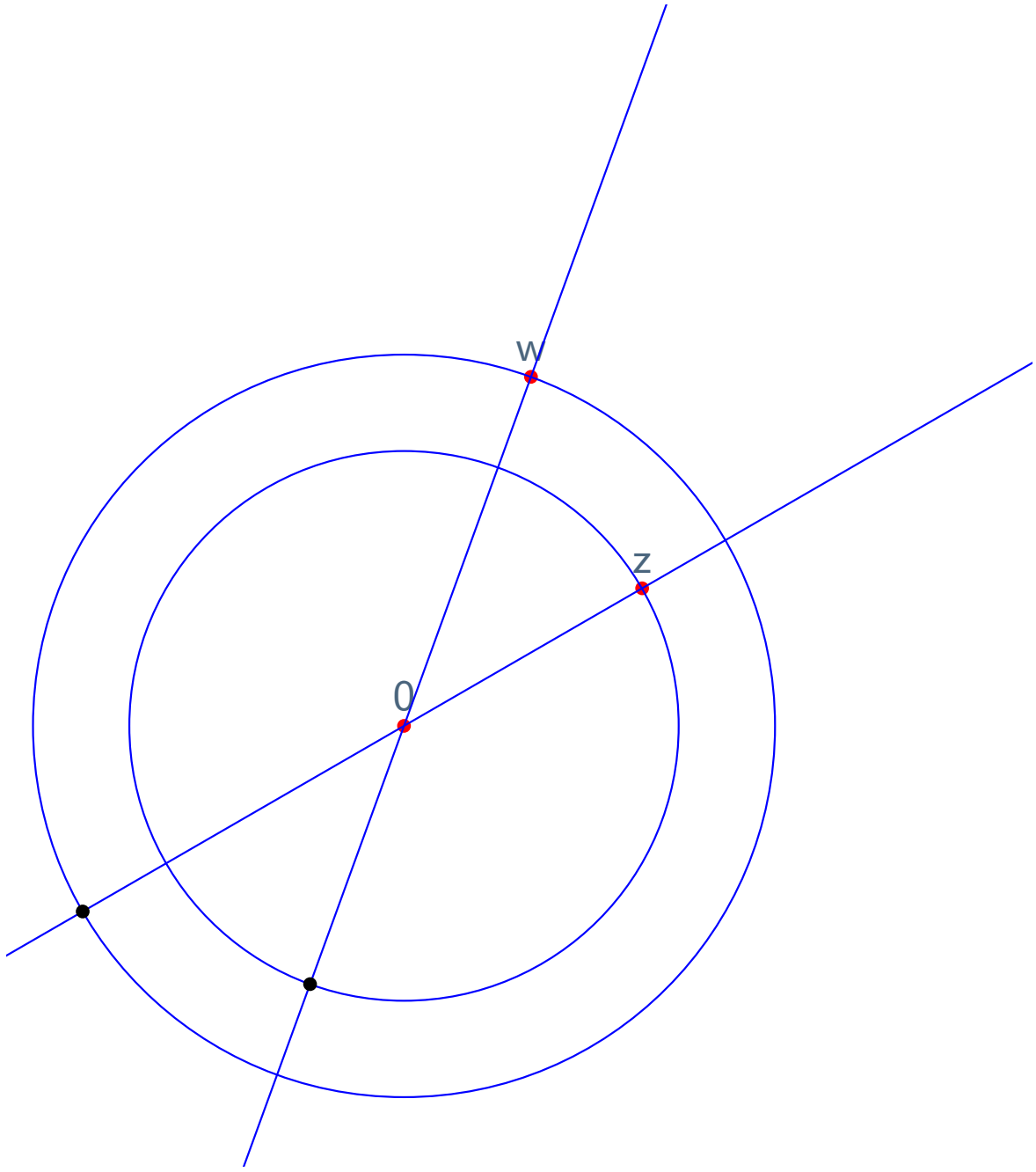
Addition

Gegeben $z, w \in \mathbb{C}$, konstruiere $z + w$ (Fall $z \neq w$):



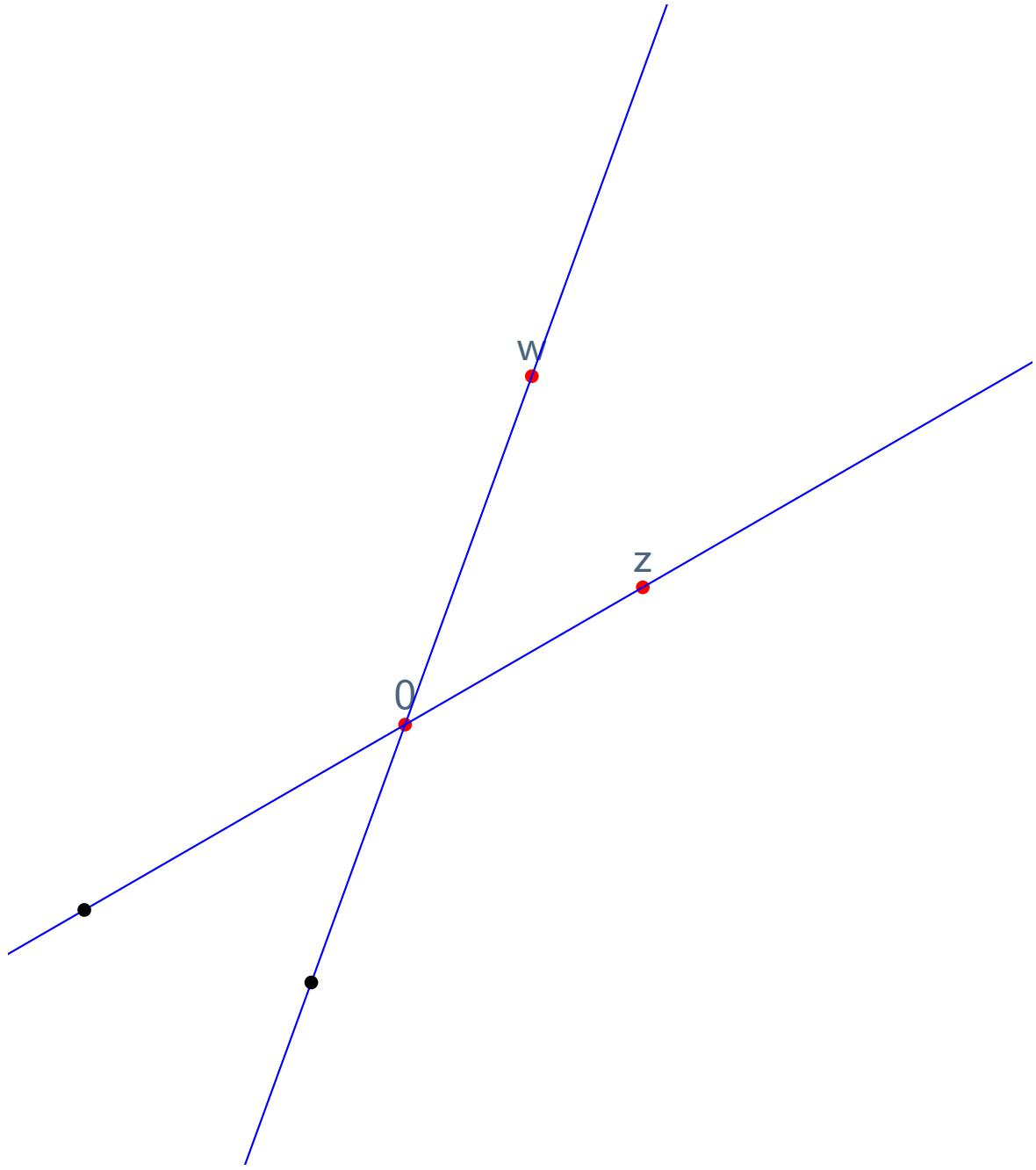
Addition

Gegeben $z, w \in \mathbb{C}$, konstruiere $z + w$ (Fall $z \neq w$):



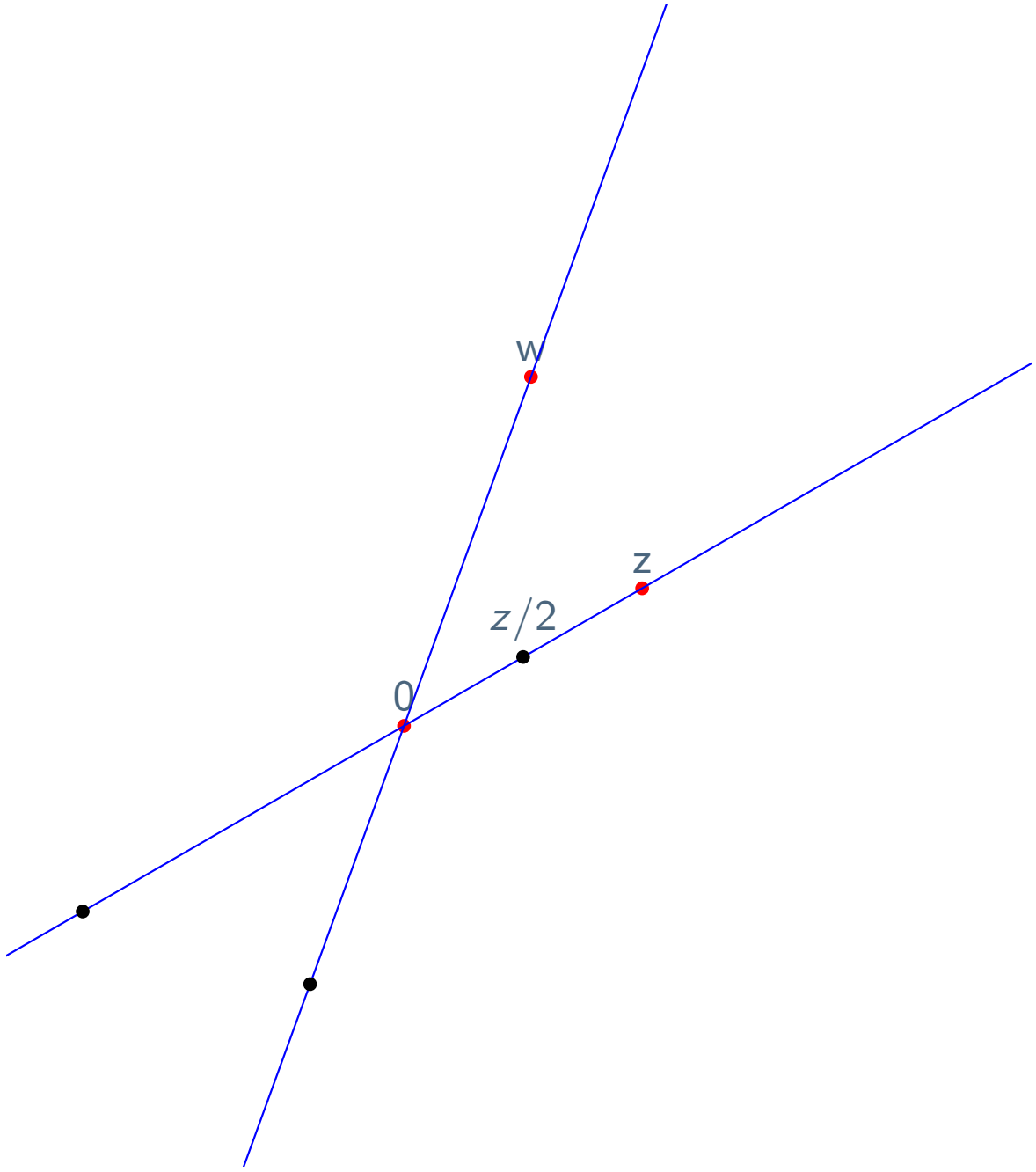
Addition

Gegeben $z, w \in \mathbb{C}$, konstruiere $z + w$ (Fall $z \neq w$):



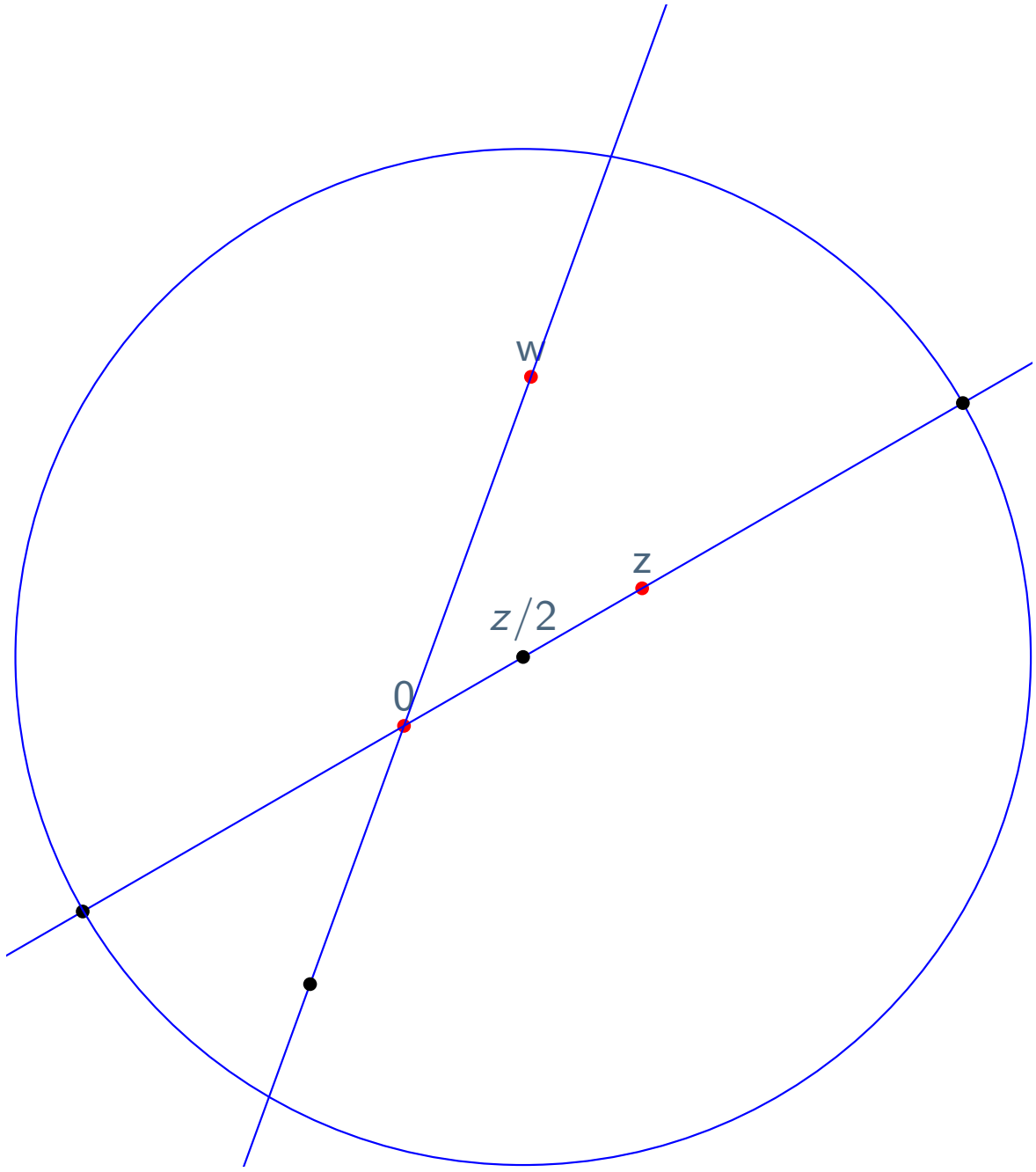
Addition

Gegeben $z, w \in \mathbb{C}$, konstruiere $z + w$ (Fall $z \neq w$):



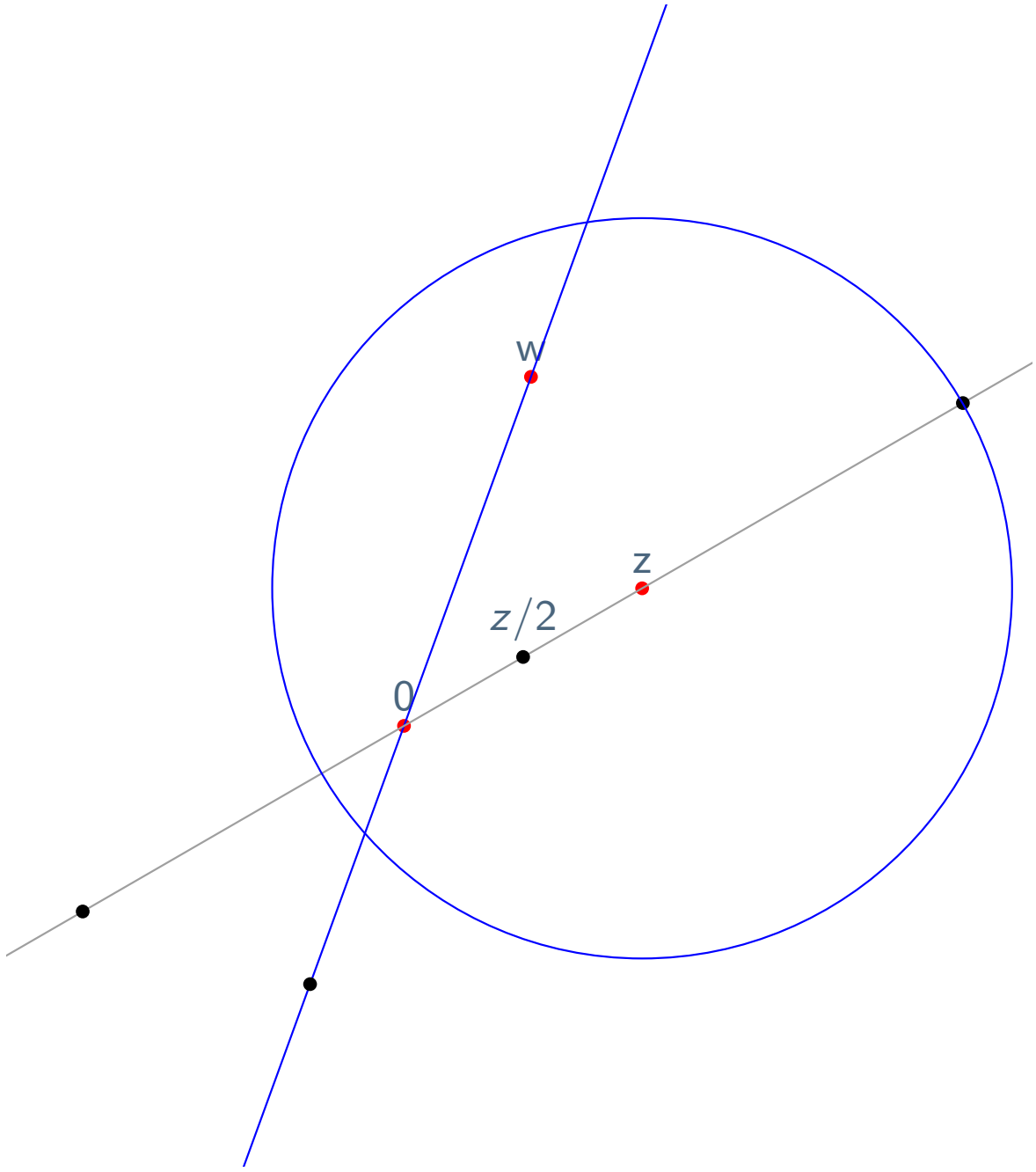
Addition

Gegeben $z, w \in \mathbb{C}$, konstruiere $z + w$ (Fall $z \neq w$):



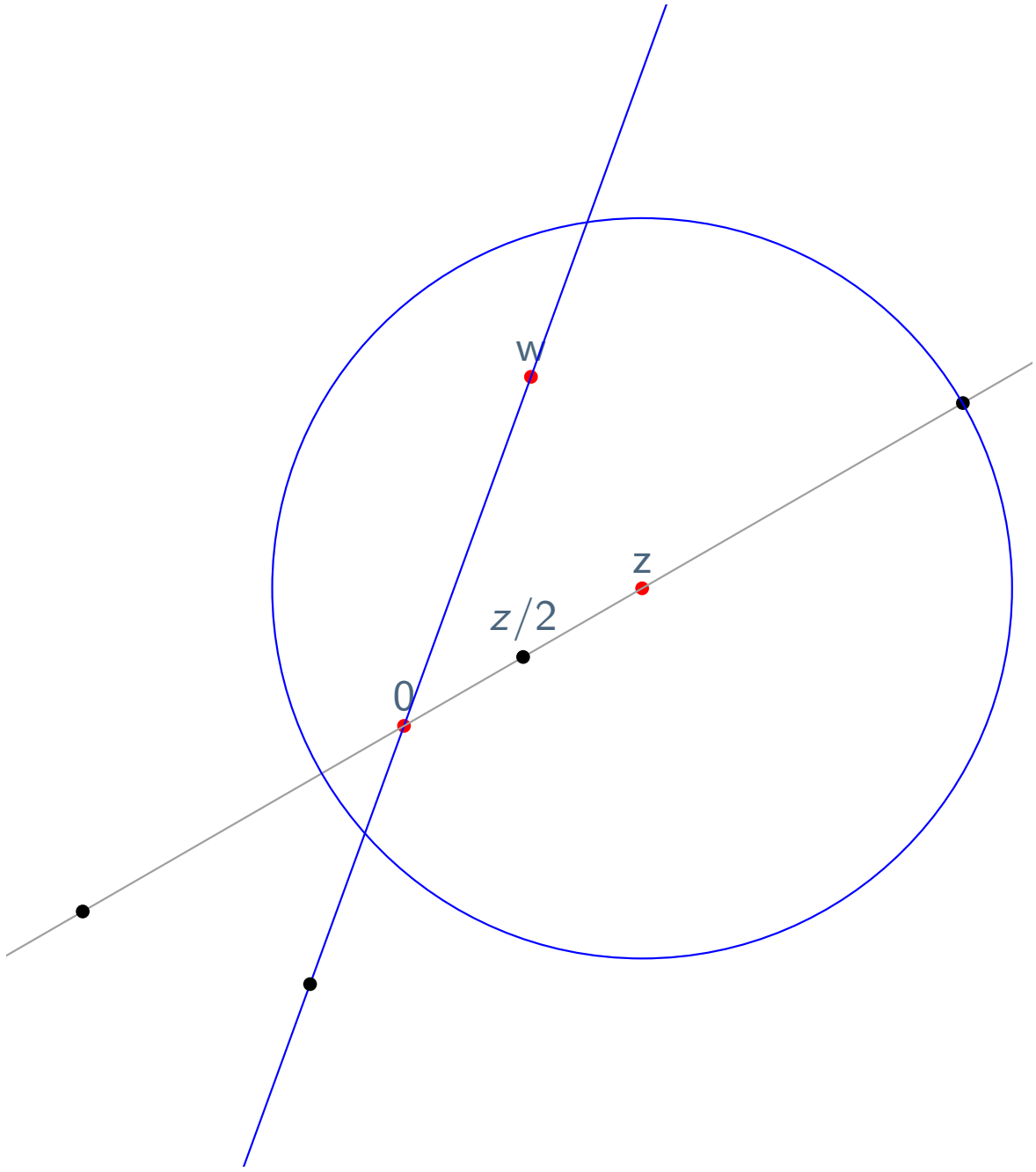
Addition

Gegeben $z, w \in \mathbb{C}$, konstruiere $z + w$ (Fall $z \neq w$):



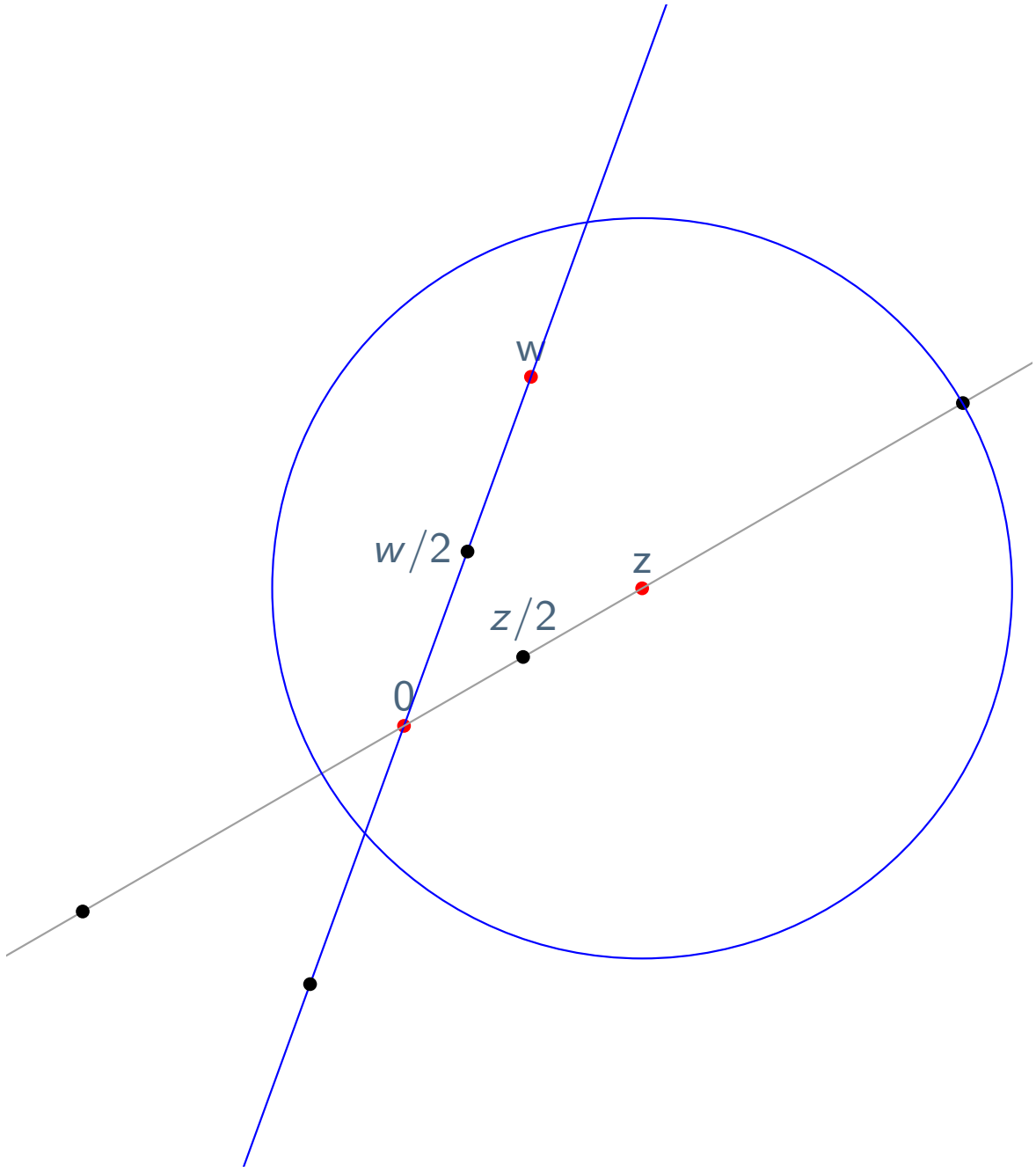
Addition

Gegeben $z, w \in \mathbb{C}$, konstruiere $z + w$ (Fall $z \neq w$):



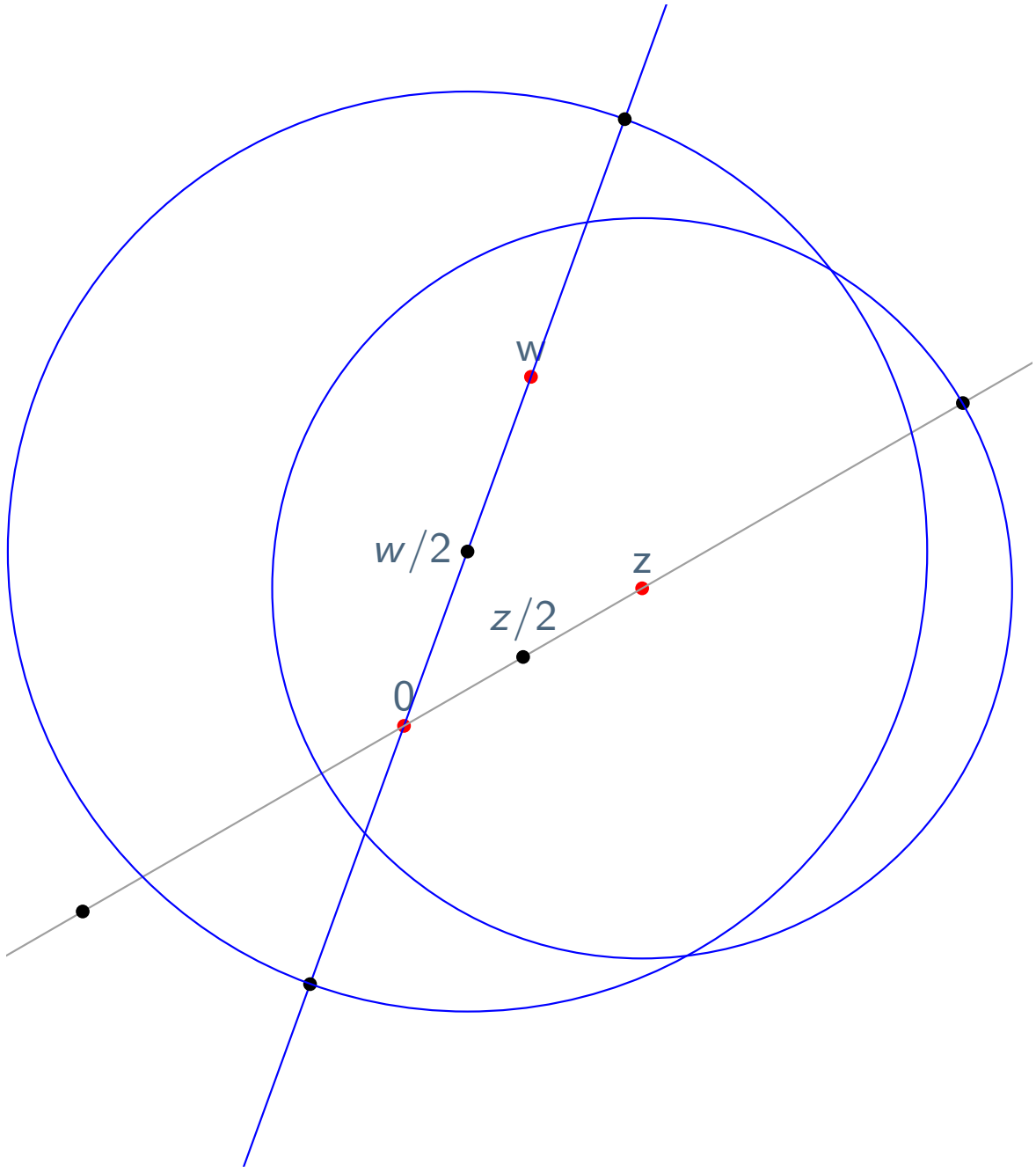
Addition

Gegeben $z, w \in \mathbb{C}$, konstruiere $z + w$ (Fall $z \neq w$):



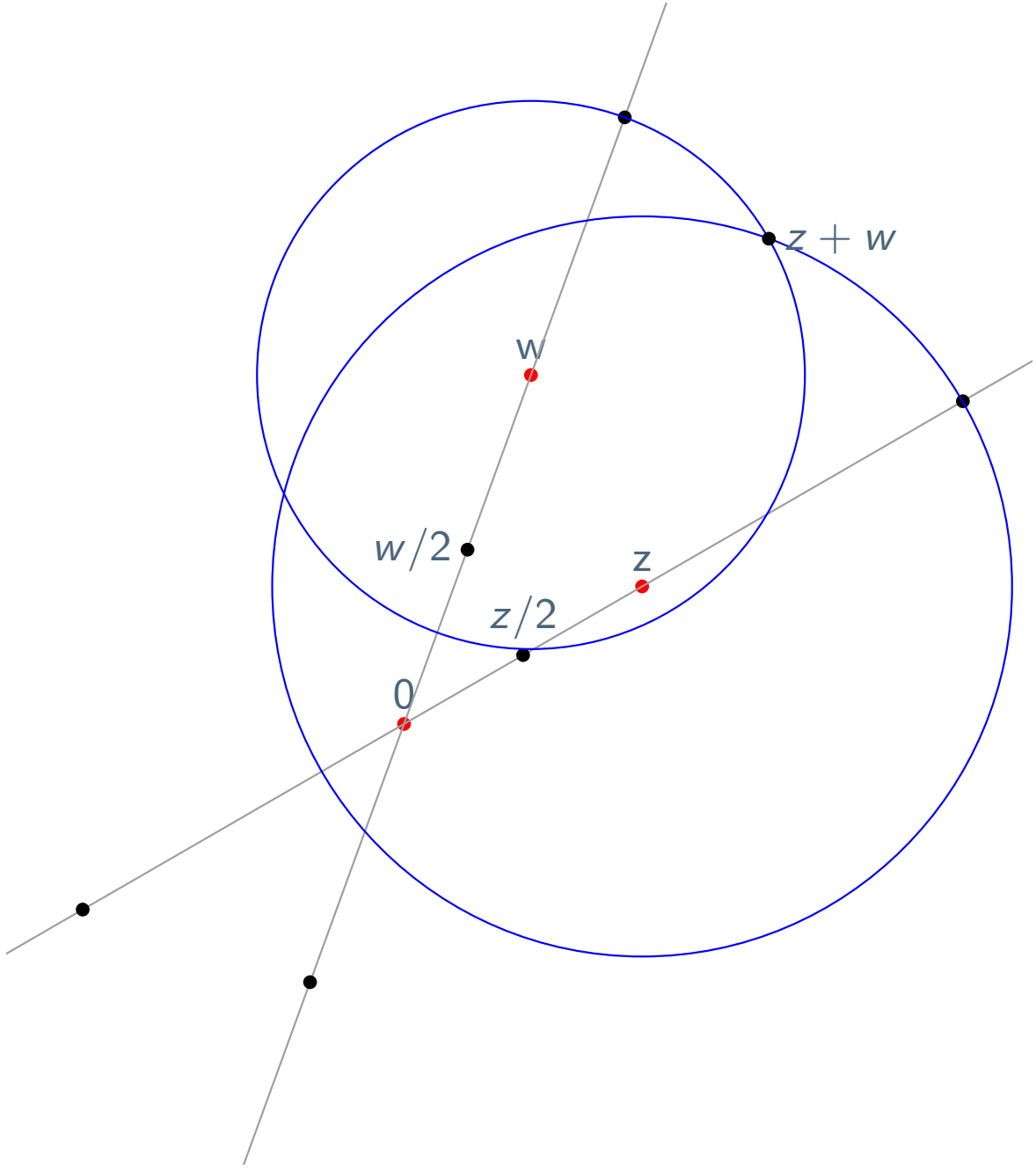
Addition

Gegeben $z, w \in \mathbb{C}$, konstruiere $z + w$ (Fall $z \neq w$):



Addition

Gegeben $z, w \in \mathbb{C}$, konstruiere $z + w$ (Fall $z \neq w$):



App-Tipps

- Euclidea App (Android/iOS): https://www.euclidea.xyz
- Geogebra https://www.geogebra.org

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Die Grundstrukturen

Die wichtigsten mathematischen Strukturen für diese Vorlesung sind:

1. Gruppen
2. Ringe
3. Körper
4. (Moduln)

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Gruppen

Definition 7 (Halbgruppe, Monoid, Gruppe)

1. Eine *Halbgruppe* ist ein Paar $(G, \circ)$ gegeben durch eine nicht-leere Menge G mit einer (inneren) Verknüpfung $\circ : G \times G \to G$, die assoziativ ist, d.h. es gilt für alle $a, b, c \in G$, dass $(a \circ b) \circ c = a \circ (b \circ c)$.
2. Ein Element $e \in G$ in einer Halbgruppe wird *neutrales Element* (oder *Einselement*) genannt, falls für alle $g \in G$ gilt: $e \circ g = g \circ e = g$.
3. Eine Halbgruppe $(G, \circ)$ mit neutralem Element e wird *Monoid* genannt.
4. Ein Element $h \in G$ in einem Monoiden heißt zu $g \in G$ *invers*, falls $h \circ g = g \circ h = e$ gilt.
5. Eine *Gruppe* ist ein Monoid $(G, \circ)$, in dem jedes Element ein Inverses besitzt.
6. Gruppen, Halbgruppen und Monoiden heißen *abelsch* oder *kommutativ*, falls $g \circ h = h \circ g$ für alle $g, h \in G$ gilt.

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Verknüpfungstafeln/Gruppentafeln

- Ist G eine endliche Menge und $\circ$ eine Verknüpfung auf G, so kann man eine *Verknüpfungstafel* aufstellen.
- Beispiel: Sei $G = \{a, b\}$.

$\circ$	a	b
a	$a \circ a$	$a \circ b$
b	$b \circ a$	$b \circ b$

- Nur praktikabel für Mengen mit wenigen Elementen.
- An der Verknüpfungstafel kann man viele Eigenschaften ablesen.
- Z.B.: Ist a neutrales Element, so füllt sich die Tabelle bereits so:

$\circ$	a	b
a	a	b
b	b	$b \circ b$

- Kommutativität: Verknüpfungstabelle symmetrisch. (Man sieht: Jede Gruppe mit 2 Elementen ist kommutativ)
- Die Verknüpfungstabelle einer Gruppe ist ein *lateinisches Quadrat* (wie auch bei Sudoku).
- Frage: Wie wird $G = \{a, b\}$ zur Gruppe?

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Verknüpfungstafeln/Gruppentafeln

- Ist G eine endliche Menge und $\circ$ eine Verknüpfung auf G, so kann man eine *Verknüpfungstafel* aufstellen.
- Beispiel: Sei $G = \{a, b\}$.

$\circ$	a	b
a	$a \circ a$	$a \circ b$
b	$b \circ a$	$b \circ b$

- Nur praktikabel für Mengen mit wenigen Elementen.
- An der Verknüpfungstafel kann man viele Eigenschaften ablesen.
- Kommutativität: Verknüpfungstabelle symmetrisch. (Man sieht: Jede Gruppe mit 2 Elementen ist kommutativ)
- Die Verknüpfungstabelle einer Gruppe ist ein *lateinisches Quadrat* (wie auch bei Sudoku).
- Frage: Wie wird $G = \{a, b\}$ zur Gruppe?

$\circ$	a	b
a	a	b
b	b	a

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Beispiele

Beispiel 8

1. $(\mathbb{N}, +)$ ist eine abelsche Halbgruppe (aber kein Monoid)
2. $(\mathbb{N}_0, +)$ ist ein abelscher Monoid.
3. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ sind, zusammen mit der gewöhnlichen Addition, abelsche Gruppen.
4. $\mathbb{Q} \setminus \{0\}, \mathbb{R} \setminus \{0\}, \mathbb{C} \setminus \{0\}$ sind, zusammen mit der gewöhnlichen Multiplikation, abelsche Gruppen (wir schreiben auch $\mathbb{Q}^\times, \mathbb{R}^\times$ und $\mathbb{C}^\times$)
5. Genauso sind $\mathbb{Q}^+ := \{x \in \mathbb{Q} \mid x > 0\}$ und analog $\mathbb{R}^+$ abelsche Gruppen mit der Multiplikation.

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Beispiele

Beispiel 9 (Symmetrische Gruppe)

- M: Menge
- $S(M) :=$ Menge der bijektiven Abbildungen $M \to M$
- Dies ist eine Gruppe mit der Komposition von Abbildungen
- Für $M = \{1, 2, \ldots, n\}$ heißt $S_n := S(M)$ die *symmetrische Gruppe* (von n Elementen).

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Beispiele

Beispiel 10

- $(G, \circ)$: Gruppe, M irgendeine Menge
- $G^M := \mathrm{Abb}(M, G) =$ Menge der Abbildungen von M nach G
- Dies ist eine Gruppe mit der *punktweisen Multiplikation*:
- Für $f, g \in G^M$ definiert man $(f \cdot g)(x) := f(x) \circ g(x)$.

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Beispiele

Beispiel 11

- Sei K ein Körper und V ein K-Vektorraum.
- Dann bildet die Menge $\mathrm{GL}(V)$ der bijektiven linearen Abbildungen auf V eine Gruppe mit der Komposition von Abbildungen als Verknüpfung.
- Für $V = K^n$ ist $\mathrm{GL}(V) \cong \mathrm{GL}_n(K) =$ invertierbare $n \times n$-Matrizen (Verknüpfung: Multiplikation von Matrizen).

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Multiplikative und additive Notation

- Man verwendet bei abstrakten Gruppen häufig die *multiplikative Notation*:
  - Ist $(G, \circ)$ eine Gruppe, schreibe einfach ab für $a \circ b$.
  - Übliche Notation für neutrales Element: $1 \in G$
  - Inverses Element zu $a \in G$ wird dann mit a^{-1} bezeichnet.
  - Vorsicht: Es kann durchaus $ab \neq ba$ sein (falls G nicht kommutativ ist).
- Oftmals kommt auch die *additive Notation* zur Anwendung
  - Besonders bei abelschen Gruppen
  - Schreibe die Verknüpfung dann als $+$
  - Neutrales Element: $0 \in G$
  - $-a$ für das zu a inverse Element.
  - Schreibe außerdem einfach $a - b$ für $a + (-b)$.

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln