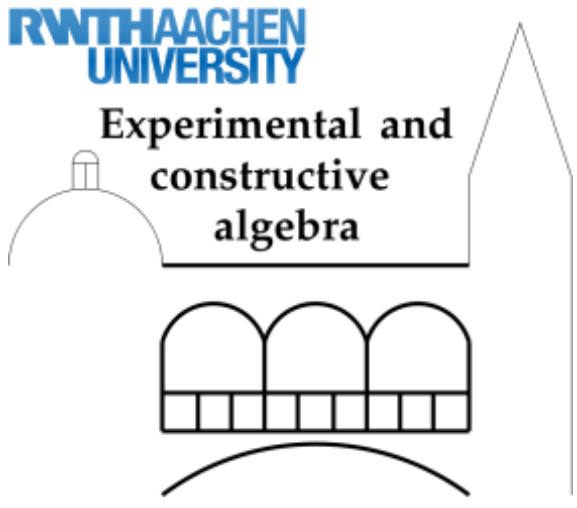
Gröbner basics

Daniel Andres



Codes und Systemtheorie

13. Mai 2011

Übersicht

Erinnerung und Notationen

- Sei K ein Körper.
- $K[x_1, \ldots, x_n] =: K[x]$ ist ein noetherscher Bereich.
- Multiindexnotation:

$$x^\alpha := x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdot \ldots \cdot x_n^{\alpha_n} \text{ mit } \alpha_i \in \mathbb{N}_0$$

- $\mathrm{Mon}(K[x]) := \{x^\alpha \mid \alpha \in \mathbb{N}_0^n\}$ Menge aller Monome
- $\mathrm{Mon}(K[x]) \cong \mathbb{N}_0^n$ als Monoid

Definition

Eine *Monomordnung* $\prec$ auf $K[x]$ ist eine Totalordnung mit $x^\alpha \prec x^\beta \implies x^{\alpha+\gamma} \prec x^{\beta+\gamma} \; \forall \; \alpha, \beta, \gamma \in \mathbb{N}_0^n$.
Eine Monomordnung auf $K[x]$ heißt *globale Ordnung*, wenn sie eine Wohlordnung ist.

Fakt: Eine Monomordnung $\prec$ auf $K[x]$ ist global $\iff 1 \prec x^\alpha \; \forall \; \alpha \in \mathbb{N}^n$.

Beispiel

Lexikographische Ordnung: $x^\alpha \prec_{\texttt{lp}} x^\beta$, falls

$$\exists \; 1 \leq i \leq n \text{ mit } \alpha_1 = \beta_1, \ldots, \alpha_{i-1} = \beta_{i-1} \text{ und } \alpha_i < \beta_i.$$

Graduiert-rückwärts-lexikographische Ordnung: $x^\alpha \prec_{\texttt{dp}} x^\beta$ falls

$$|\alpha| < |\beta| \text{ oder } \big(|\alpha| = |\beta| \text{ und}$$
$$\exists \; 1 \leq i \leq n \text{ mit } \alpha_n = \beta_n, \ldots, \alpha_{i+1} = \beta_{i+1} \text{ und } \alpha_i > \beta_i\big).$$

Ab jetzt: Fixiere globale Ordnung $\prec$ auf $K[x]$.

Definition

Sei $0 \neq f \in K[x]$. Man kann f eindeutig schreiben als

$$f = c_\alpha x^\alpha + \sum_{\beta \in \mathbb{N}_0^n} c_\beta x^\beta$$

mit $c_\alpha, c_\beta \in K, c_\alpha \neq 0$ und $x^\beta \prec x^\alpha$ für alle β mit $c_\beta \neq 0$. Dann heißen

$$\begin{aligned} \operatorname{lm}(f) &:= x^\alpha && \text{das } \textit{Leitmonom} \text{ von } f, \\ \operatorname{lc}(f) &:= c_\alpha && \text{der } \textit{Leitkoeffizient} \text{ von } f \text{ und} \\ \operatorname{lt}(f) &:= c_\alpha x^\alpha && \text{der } \textit{Leitterm} \text{ von } f. \end{aligned}$$

Algorithmus (NFBuchberger)

Input: $f \in K[x], F \subset K[x]$ (endlich, nichtleer)
Output: $h \in K[x]$, eine *Normalform* von f bzgl. F

$h := f$
while $h \neq 0$ und es existiert $g \in F$ mit $\mathrm{lm}(g) \mid \mathrm{lm}(h)$ **do**
  wähle $g \in F$ mit $\mathrm{lm}(g) \mid \mathrm{lm}(h)$
  $h := h - \frac{\mathrm{lt}(h)}{\mathrm{lt}(g)} \cdot g$
return h

Definition

Sei $\varnothing \neq F \subset K[x]$ endlich. Eine endliche Teilmenge $G \subset I := \langle F \rangle$ heißt eine *Gröbnerbasis* von I bzgl. $\prec$, wenn

$$\forall\ f \in I\ \exists\ g \in G \text{ mit } \operatorname{lm}(g) \mid \operatorname{lm}(f).$$

Beispiel

$F := \{xy - 1, y^2 - 1\} \subset K[x, y]$ ist **keine** Gröbnerbasis vom $\langle F \rangle$ bzgl. $\prec_{\texttt{lp}}$ mit $y \prec_{\texttt{lp}} x$, denn

$$y \cdot (xy - 1) - x \cdot (y^2 - 1) = xy^2 - y - xy^2 + x = -x - y \in \langle F \rangle,$$

$$\text{und} \qquad xy \nmid x, \qquad y^2 \nmid x.$$

Definition

Seien $f, g \in K[x] \setminus \{0\}$ mit $\mathrm{lm}(f) = x^\alpha$ und $\mathrm{lm}(g) = x^\beta$. Sei weiter $x^\gamma = \mathrm{kgV}(x^\alpha, x^\beta)$, also $\gamma_i = \max(\alpha_i, \beta_i)$ für $1 \leq i \leq n$. Dann heißt

$$\mathrm{spoly}(f, g) = x^{\gamma-\alpha} \cdot f - \frac{\mathrm{lc}(f)}{\mathrm{lc}(g)} \cdot x^{\gamma-\beta} \cdot g$$

das *s-Polynom* von f und g.

Theorem

Sei $G \subset I := \langle F \rangle \subset K[x]$ endlich und nichtleer. Äquivalent sind:

- G ist Gröbnerbasis von I bzgl. $\prec$.
- $\forall\ f \in I\ \exists\ g \in G$ mit $\mathrm{lm}(g) \mid \mathrm{lm}(f)$.
- $\langle \mathrm{lm}(f) \mid f \in I \rangle = \langle \mathrm{lm}(g) \mid g \in G \rangle$.
- $\{\alpha \mid \mathrm{lm}(f) = x^\alpha, f \in I\}$
  $= \{\beta \mid \mathrm{lm}(g) = x^\beta, g \in G\} + \mathbb{N}_0^n$.
- $\texttt{NFBuchberger}(\mathrm{spoly}(g_1, g_2), G) = 0\ \forall\ g_1, g_2 \in G$.

Algorithmus (Buchberger)

Input: $F \subset K[x]$ endlich, nichtleer
Output: $G \subset K[x]$ eine Gröbnerbasis von $\langle F \rangle$ bzgl. $\prec$

$G := F$
$P := \{(f, g) \mid f, g \in G, f \neq g\}$
while $P \neq \varnothing$ **do**
  wähle $(f, g) \in P$
  $s :=$`NFBuchberger`$(\mathrm{spoly}(f, g), G)$
  if $s \neq 0$ **then**
    $P := P \cup \{(s, h) \mid h \in G\}$
    $G := G \cup \{s\}$
  $P := P \setminus \{(f, g)\}$
return G

Erinnerung und Notationen

- Sei K ein Körper.
- $K[x_1, \ldots, x_n] =: K[x]$ ist ein noetherscher Bereich.
- Multiindexnotation:

$$x^\alpha := x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdot \ldots \cdot x_n^{\alpha_n} \text{ mit } \alpha_i \in \mathbb{N}_0$$

- Wir betrachten den freien $K[x]$-Modul vom Rang r mit Standardbasis $e_1, \ldots, e_r$.
- $\mathrm{Mon}(K[x]^r) := \{x^\alpha e_i \mid \alpha \in \mathbb{N}_0^n, 1 \leq i \leq r\}$ Menge aller Monome
- $\mathrm{Mon}(K[x]^r)$ steht in Bijektion zu $\mathbb{N}_0^n \times \{1, \ldots, r\}$

Definition

Sei $\prec_{K[x]}$ eine globale Ordnung auf $K[x]$.
Eine *Monomordnung* $\prec$ auf $K[x]^r$ ist eine Totalordnung mit

1. $x^\alpha e_i \prec x^\beta e_j \implies x^{\alpha+\gamma} e_i \prec x^{\beta+\gamma} e_j \ \forall\ \alpha, \beta, \gamma \in \mathbb{N}_0^n, 1 \leq i, j \leq r.$
2. $x^\alpha \prec_{K[x]} x^\beta \implies x^\alpha \cdot e_i \prec x^\beta \cdot e_i \ \forall\ \alpha, \beta, \in \mathbb{N}_0^n, 1 \leq i \leq r.$

Eine Monomordnung auf $K[x]^r$ heißt *globale Ordnung*, wenn sie eine Wohlordnung ist.

Fakt: Eine Monomordnung $\prec$ auf $K[x]^r$ ist global $\iff \prec_{K[x]}$ ist global.

Beispiel

Position over term-Ordnung (POT): $x^\alpha e_i \prec_{(\mathsf{c}, K[x])} x^\beta e_j$, falls

$$i < j \text{ oder } (i = j \text{ und } x^\alpha \prec_{K[x]} x^\beta).$$

Term over position-Ordnung (TOP): $x^\alpha e_i \prec_{(K[x], \mathsf{c})} x^\beta e_j$, falls

$$x^\alpha \prec_{K[x]} x^\beta \text{ oder } (x^\alpha = x^\beta \text{ und } i < j).$$

Ab jetzt: Fixiere globale Ordnung $\prec$ auf $K[x]^r$.

Definition

Sei $0 \neq f \in K[x]^r$. Man kann f eindeutig schreiben als

$$f = c_{\alpha,i} x^\alpha e_i + \sum_{\beta \in \mathbb{N}_0^n, j \in \mathbb{N}} c_{\beta,j} x^\beta e_j$$

mit $c_{\alpha,i}, c_{\beta,j} \in K, c_{\alpha,i} \neq 0$ und $x^\beta e_j \prec x^\alpha e_i$ für alle β, j mit $c_{\beta,j} \neq 0$.
Dann heißen

$$\begin{aligned} \mathrm{lm}(f) &:= x^\alpha e_i && \text{das } \textit{Leitmonom} \text{ von } f, \\ \mathrm{lc}(f) &:= c_{\alpha,i} && \text{der } \textit{Leitkoeffizient} \text{ von } f \text{ und} \\ \mathrm{lt}(f) &:= c_{\alpha,i} x^\alpha e_i && \text{der } \textit{Leitterm} \text{ von } f. \end{aligned}$$

Algorithmus (NFBuchberger)

Input: $f \in K[x]^r, F \subset K[x]^r$ (endlich, nichtleer)
Output: $h \in K[x]^r$, eine *Normalform* von f bzgl. F

$h := f$
while $h \neq 0$ und es existiert $g \in F$ mit $\mathrm{lm}(g) \mid \mathrm{lm}(h)$ **do**
  wähle $g \in F$ mit $\mathrm{lm}(g) \mid \mathrm{lm}(h)$
  $h := h - \frac{\mathrm{lt}(h)}{\mathrm{lt}(g)} \cdot g$
return h

Hierbei:

$$x^\alpha e_i \mid x^\beta e_j \quad :\Longleftrightarrow \quad i = j \text{ und } x^\alpha \mid x^\beta$$

$$\frac{x^\alpha e_i}{x^\beta e_i} := \frac{x^\alpha}{x^\beta} e_i$$

Definition

Sei $\varnothing \neq F \subset K[x]^r$ endlich. Eine endliche Teilmenge $G \subset M := \langle F \rangle$ heißt eine *Gröbnerbasis* von M bzgl. $\prec$, wenn

$$\forall\ f \in M\ \exists\ g \in G \text{ mit } \operatorname{lm}(g) \mid \operatorname{lm}(f).$$

Definition

Seien $f, g \in K[x]^r \setminus \{0\}$ mit $\mathrm{lm}(f) = x^\alpha e_i$ und $\mathrm{lm}(g) = x^\beta e_j$. Sei weiter $x^\gamma = \mathrm{kgV}(x^\alpha, x^\beta)$, also $\gamma_i = \max(\alpha_i, \beta_i)$ für $1 \leq i \leq n$. Dann heißt

$$\mathrm{spoly}(f, g) = \delta_{i,j} \cdot \left(x^{\gamma-\alpha} \cdot f - \frac{\mathrm{lc}(f)}{\mathrm{lc}(g)} \cdot x^{\gamma-\beta} \cdot g\right)$$

das *s-Polynom* von f und g.

Theorem

Sei $G \subset I := \langle F \rangle \subset K[x]^r$ endlich und nichtleer. Äquivalent sind:

- G ist Gröbnerbasis von I bzgl. $\prec$.
- $\forall\ f \in I\ \exists\ g \in G$ mit $\mathrm{lm}(g) \mid \mathrm{lm}(f)$.
- $\langle \mathrm{lm}(f) \mid f \in I \rangle = \langle \mathrm{lm}(g) \mid g \in G \rangle$.
- $\{(\alpha, i) \mid \mathrm{lm}(f) = x^\alpha e_i, f \in I\}$
  $= \{(\beta, j) \mid \mathrm{lm}(g) = x^\beta e_j, g \in G\} + \mathbb{N}_0^n \times \{0\}$.
- $\mathtt{NFBuchberger}(\mathrm{spoly}(g_1, g_2), G) = 0\ \forall\ g_1, g_2 \in G$.

Algorithmus (Buchberger)

Input: $F \subset K[x]^r$ endlich, nichtleer
Output: $G \subset K[x]^r$ eine Gröbnerbasis von $\langle F \rangle$ bzgl. $\prec$

$G := F$
$P := \{(f, g) \mid f, g \in G, f \neq g\}$
while $P \neq \varnothing$ **do**
  wähle $(f, g) \in P$
  $s :=$`NFBuchberger`$(\mathrm{spoly}(f, g), G)$
  if $s \neq 0$ **then**
    $P := P \cup \{(s, h) \mid h \in G\}$
    $G := G \cup \{s\}$
  $P := P \setminus \{(f, g)\}$
return G

Beispiel

Betrachte das lineare Gleichungssystem

$$\begin{pmatrix} 3 & 1 & 1 & -1 \\ 13 & 8 & 6 & -7 \\ 14 & 10 & 6 & -7 \\ 7 & 4 & 3 & -3 \end{pmatrix} \cdot x = \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix}$$

über $\mathbb{Q}$ mit Parametern a, b, c, d.

Eindeutigkeiten

Sei $M \subset K[x]^r$ ein Modul. Dann besitzt M eine Gröbnerbasis G bzgl. $\prec$.
Fakt:

- $\langle G \rangle = M$.
- $\texttt{NFBuchberger}(f, G)$ ist eindeutig bestimmt $\forall\ f \in K[x]^r$.

Definition

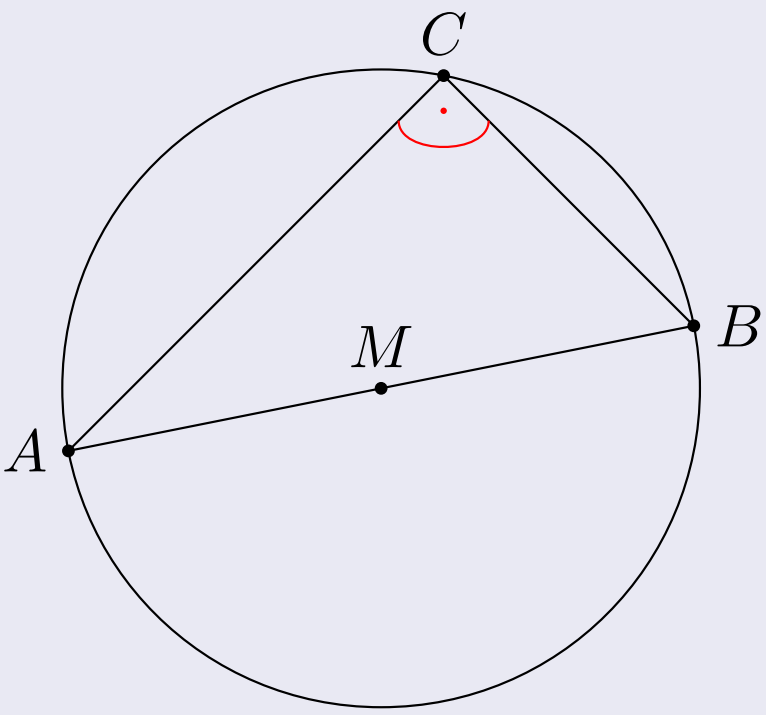
- Eine Gröbnerbasis G heißt *minimal* (oder *interreduziert*), wenn $0 \notin G$ und $\mathrm{lm}(g) \nmid \mathrm{lm}(g')\ \forall\ g \neq g' \in G$.
  (D.h. $G \setminus \{g\}$ ist keine Gröbnerbasis $\forall\ g \in G$.)
- G heißt *reduziert*, wenn G minimal ist, $\mathrm{lc}(g) = 1$ und $\mathrm{lm}(g)$ kein Monom von $g'\ \forall\ g \neq g' \in G$ teilt.

Fakt: Reduzierte Gröbnerbasen sind eindeutig bestimmt.

Anwendungen

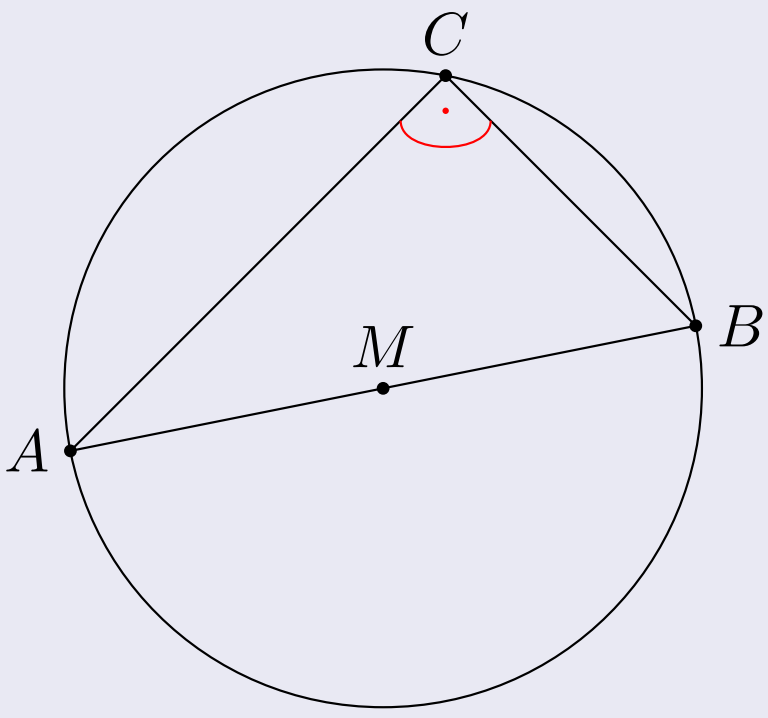
- Schnitte von Idealen/ Untermoduln
- Schnitte von Ideal und Unteralgebra
- Lösbarkeit bzw. Lösen von polynomiellen Gleichungssystemen
- Radikalmitgliedschaft
- Urbilder unter Ring-/Modulhomomorphismen
- Algebraische Abhängigkeiten und Unteralgebramitgliedschaft
- Annihilatorberechnung
- Syzygienberechnung
- Automatisches Beweisen
- Ideal-/ Modulmitgliedschaft: $\texttt{NFBuchberger}(f, G) = 0 \iff f \in M$.
- ...

Beispiel (Satz des Thales)



Liegt der Punkt C eines Dreiecks ABC auf einem Halbkreis ?ber der Strecke AB, dann hat das Dreieck bei C einen rechten Winkel.

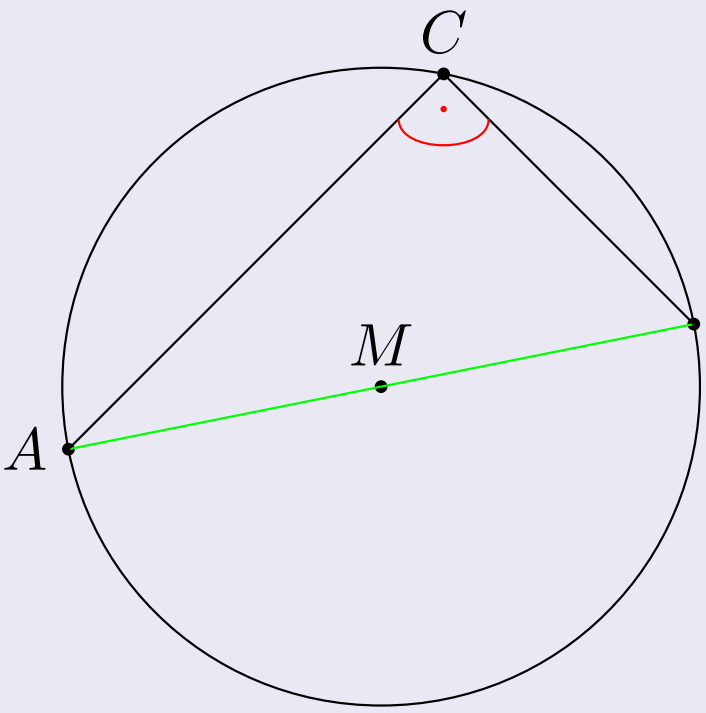
Beispiel (Satz des Thales)



Liegt der Punkt C eines Dreiecks ABC auf einem Halbkreis ?ber der Strecke AB, dann hat das Dreieck bei C einen rechten Winkel.

Anders gesagt: Seien $r := AM = BM$, $A := (0, 0), B := (b_1, b_2), C := (c_1, c_2)$.

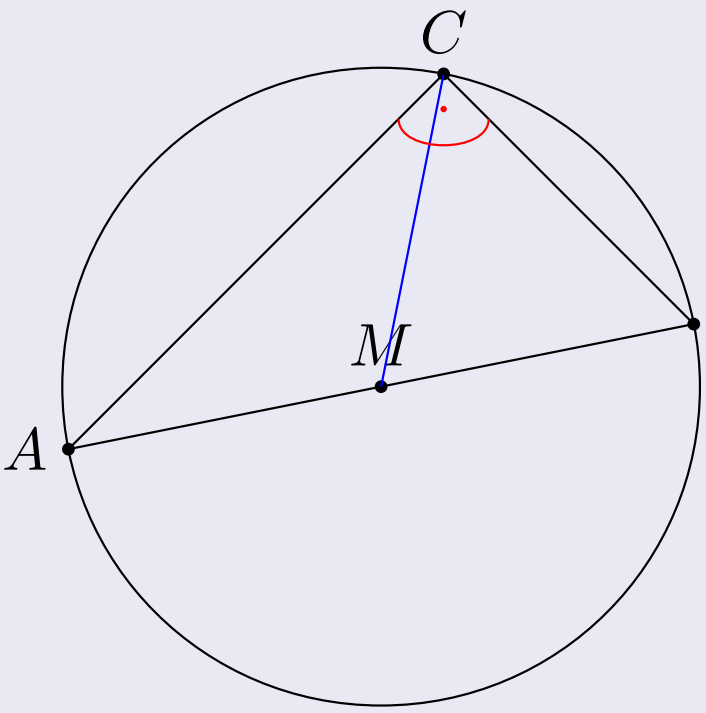
Beispiel (Satz des Thales)



Liegt der Punkt C eines Dreiecks ABC auf einem Halbkreis ?ber der Strecke AB, dann hat das Dreieck bei C einen rechten Winkel.

Anders gesagt: Seien $r := AM = BM$, $A := (0,0), B := (b_1, b_2), C := (c_1, c_2)$. Es gelte $4r^2 = \langle AB, AB \rangle = b_1^2 + b_2^2$

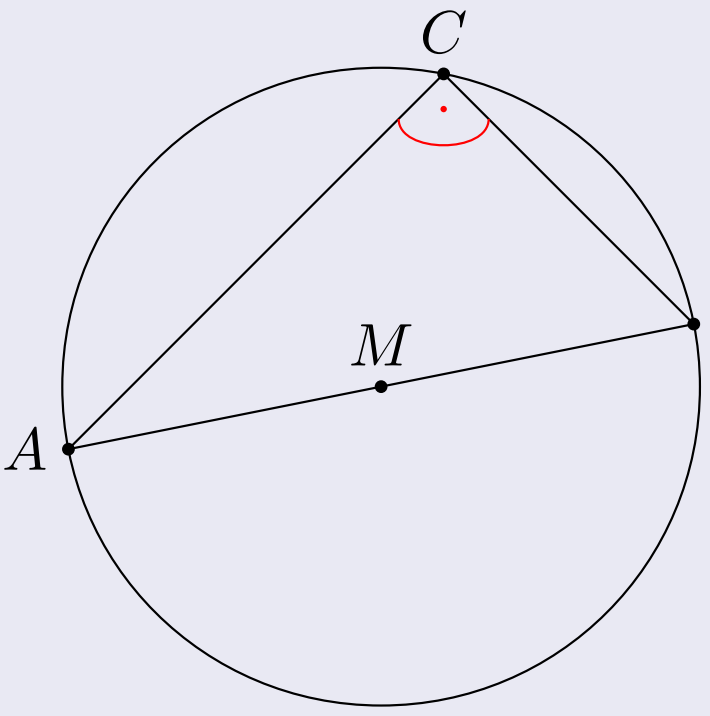
Beispiel (Satz des Thales)



Liegt der Punkt C eines Dreiecks ABC auf einem Halbkreis ?ber der Strecke AB, dann hat das Dreieck bei C einen rechten Winkel.

Anders gesagt: Seien $r := AM = BM$, $A := (0,0), B := (b_1, b_2), C := (c_1, c_2)$. Es gelte $4r^2 = \langle AB, AB\rangle = b_1^2 + b_2^2$ und $r^2 = \langle MC, MC\rangle = (c_1 - \frac{1}{2}b_1)^2 + (c_2 - \frac{1}{2}b_2)^2$.

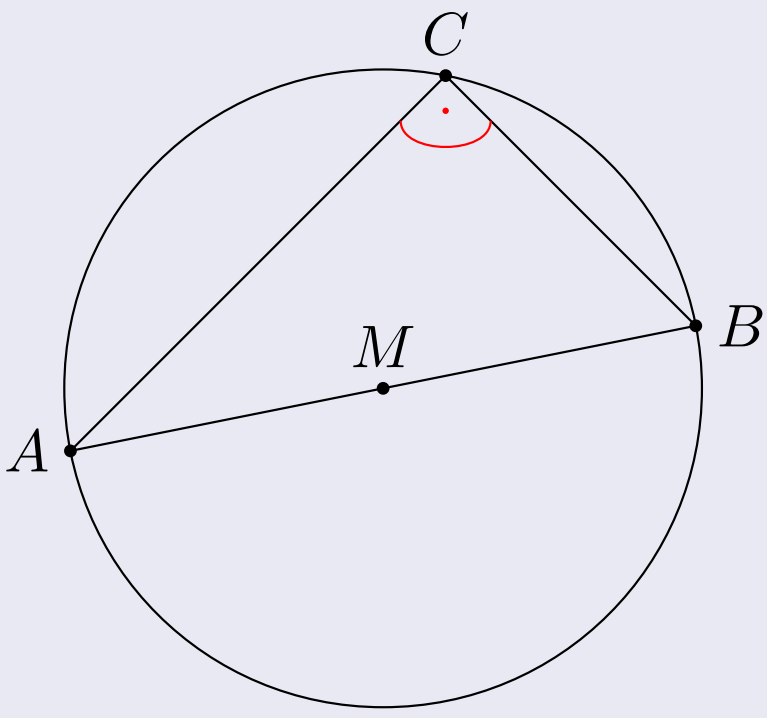
Beispiel (Satz des Thales)



Liegt der Punkt C eines Dreiecks ABC auf einem Halbkreis ?ber der Strecke AB, dann hat das Dreieck bei C einen rechten Winkel.

Anders gesagt: Seien $r := AM = BM$, $A := (0,0), B := (b_1, b_2), C := (c_1, c_2)$.
Es gelte $4r^2 = \langle AB, AB\rangle = b_1^2 + b_2^2$ und $r^2 = \langle MC, MC\rangle = (c_1 - \frac{1}{2}b_1)^2 + (c_2 - \frac{1}{2}b_2)^2$.
Dann folgt
$0 = \langle CA, CB\rangle = c_1(c_1 - b_1) + c_2(c_2 - b_2)$.

Beispiel (Satz des Thales)



Liegt der Punkt C eines Dreiecks ABC auf einem Halbkreis ?ber der Strecke AB, dann hat das Dreieck bei C einen rechten Winkel.

Anders gesagt: Seien $r := AM = BM$, $A := (0,0), B := (b_1, b_2), C := (c_1, c_2)$.
Es gelte $4r^2 = \langle AB, AB\rangle = b_1^2 + b_2^2$ und $r^2 = \langle MC, MC\rangle = (c_1 - \frac{1}{2}b_1)^2 + (c_2 - \frac{1}{2}b_2)^2$.
Dann folgt
$0 = \langle CA, CB\rangle = c_1(c_1 - b_1) + c_2(c_2 - b_2)$.

Also:

$$\left.\begin{aligned} b_1^2 + b_2^2 - 4r^2 &= 0, \\ (c_1 - \frac{1}{2}b_1)^2 + (c_2 - \frac{1}{2}b_2)^2 - r^2 &= 0 \end{aligned}\right\} \implies c_1(c_1 - b_1) + c_2(c_2 - b_2) = 0.$$