Konstruktionen mit Zirkel und Lineal

Wiland Schmale

mehrfach überarbeitetes Skript
zuletzt geringfügig geändert im Dezember 2008

Vorbemerkungen

Die klassischen Konstruktionsprobleme, um die es im Folgenden geht, sind:
Quadratur des Kreises, Rektifikation des Kreisumfanges, Würfelverdoppelung, Dreiteilung des Winkels und schließlich die Konstruktion eines regelmäßigen n-Eckes. Das Problem der Würfelverdoppelung wird oft auch Deli'sches Problem genannt.
"Konstruktion" heißt dabei stets Konstruktion mit Zirkel und Lineal. Alle aufgeführten Probleme sind zumindest teilweise unlösbar, wenn man sich strikt an gewisse Konstruktionsregeln (s. u.) hält. Innerhalb der nach diesen Regeln konstruierenden Geometrie wird die Unmöglichkeit gewisser Konstruktionsergebnisse nicht deutlich. Erst die analytisch-algebraische Interpretation der Konstruktion ebnete den Weg zu einer Klärung, indem sie die geometrischen Probleme in algebraische Probleme übersetzte, die im Laufe des 19. Jahrhunderts gelöst wurden. Ausnahme dabei ist die Konstruktion eines regelmäßigen n-Eckes, bei der das zugehörige algebraische Problem bis heute noch nicht vollständig gelöst ist (s. u.).
Die "Übersetzung" der Konstruktionsprobleme in algebraische Probleme ergibt sich mit elementaren Hilfsmitteln der analytischen Geometrie und der Körpertheorie. Der Schwierigkeitsgrad der entstehenden algebraischen Probleme ist recht unterschiedlich:

$$\left.\begin{array}{l}\text{Quadratur des Kreises}\\ \text{Rektifikation des Kreisumfanges}\end{array}\right\} \leftrightarrow \quad \text{Transzendenz von } \pi.$$

$$\text{Würfelverdoppelung} \leftrightarrow \ [\mathbb{Q}\left(\sqrt[3]{2}\right) : \mathbb{Q}] = ?$$

$$\text{Dreiteilung des Winkels } \varphi \leftrightarrow \ [\mathbb{Q}(\cos\varphi)(\cos(\varphi/3)) : \mathbb{Q}(\cos\varphi)] = ?$$

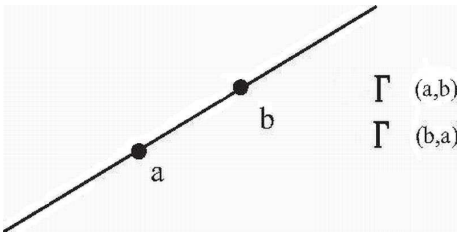
$$\left.\begin{array}{l}\text{Konstruktion eines regelmäßigen}\\ \text{n-Eckes}\end{array}\right\} \leftrightarrow \left\{\begin{array}{l}\text{Bestimme alle}\\ \text{Fermat-Primzahlen}\end{array}\right\}$$

Nur bei dem zuletzt aufgeführten "Übersetzungs"-Problem werden wir etwas Galoistheorie einsetzen.

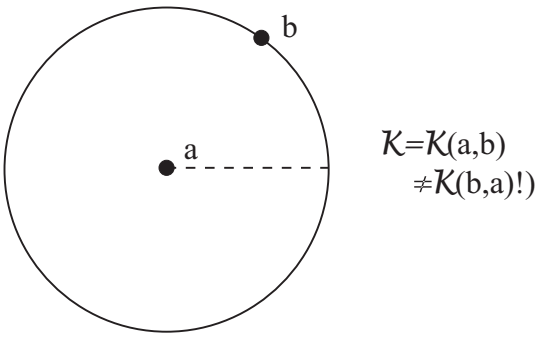
Am Ende des Textes folgen noch ein paar Hinweise zu erweiterten Konstruktionstechniken.

Die zulässigen Konstruktionsschritte

Es geht um Konstruktionen mit Zirkel und Lineal in der Ebene: Letztere fassen wir als $\mathbb{R}^2 = \mathbb{C}$ auf mit dem rechtwinkligen Koordinatensystem, das durch 1 und i vorgegeben ist Stets ist eine Punktmenge M vorgegeben, $(\varnothing \neq M \subset \mathbb{C})$ aus der heraus neue Punkte nach gewissen Regeln konstruiert werden können:
Mit dem Lineal können wir durch je zwei verschiedene Punkte $a, b \in M$ eine Gerade $\Gamma(a, b) = \Gamma(b, a)$ ziehen:



Mit dem Zirkel können wir zu zwei gegebenen Punkten $a \neq b$ aus M um a herum einen Kreis schlagen mit Radius $|b-a|$ der durch b geht.



Offensichtlich ist es dabei sinnvoll, stets vorauszusetzen, dass $\boxed{|M| \geq 2.}$
Außerdem wird **weiter unten** vorausgesetzt $\mathbf{0,1 \in M}$**.** Dies kann, wenn $|M| \geq 2$, notfalls durch affinen Koordinatenwechsel erreicht werden.

Definition 1:

Sei also $M \subset \mathbb{C}$ und $|M| \geq 2$

(a) $c \in \mathbb{C}$ heißt **(in einem Schritt) aus** M **konstruierbar,** wenn es $a, b, a'b' \in M$ gibt mit $a \neq b, a' \neq b'$, so dass mit $\Gamma = \Gamma(a,b), \Gamma' = \Gamma(a,' b'), \mathcal{K} = \mathcal{K}(a,b)$ und $\mathcal{K}' = \mathcal{K}(a',b')$ gilt:

(i) $c \in \Gamma \cap \Gamma'$ und $|\Gamma \cap \Gamma'| = 1$
oder (ii) $c \in \Gamma \cap \mathcal{K}'$ und $|\Gamma \cap \mathcal{K}'| = 2$
oder (iii) $c \in \mathcal{K} \cap \mathcal{K}'$ und $|\mathcal{K} \cap \mathcal{K}'| = 2$

(b) Seien $M^{(0)} := M$, $\boldsymbol{M^{(1)} := \{c \in \mathbb{C} : c \text{ aus } M \text{ in einem Schritt konstruierbar}\}}$ und für $r \geq 1$: $M^{(r)} = (M^{(r-1)})^{(1)}$ und schließlich

$$\boxed{\overset{\circ}{\overline{M}} := \bigcup_{r \geq 0} M^{(r)}}$$

c heiße **aus M in endlich vielen Schriften konstruierbar, wenn** $\boldsymbol{c \in \overset{\circ}{\overline{M}}}$**.**

Beachte dabei: Stets ist $M \subset M^{(1)}$:
und deswegen: $M \subset M^{(1)} \subset \ldots \subset M^{(r)} \subset \ldots \subset \overset{\circ}{\overline{M}}$
Beachte außerdem: $c \in \overset{\circ}{\overline{M}} \Leftrightarrow \exists r \in \mathbb{N} : c \in M^{(r)}$
und: Selbst wenn $|M| = 2$, ist $|\overset{\circ}{\overline{M}}| = \infty$!

Algebraische Beschreibung der Konstruktionsschritte und einige Folgerungen:

Die Auffassung der Konstruktionsebene als $\mathbb{R}^2$ oder $\mathbb{C}$ beinhaltet bereits die Zugrundelegung eines rechtwinkligen (cartesischen) Koordinatensystems. Dies ist die Grundlage für die algebraische Formulierung von Konstruktionsproblemen. Geraden und Kreise lassen sich durch Gleichungen beschreiben. Die Punkte in $M^{(1)}$ ergeben sich dann als Lösungen von Gleichungssystemen. Da wir (im Sinne der Algebraisierung) $\mathbb{C}$ dem $\mathbb{R}^2$ vorziehen, ist es dann auch zweckmäßig, **Geraden und Kreise im Komplexen** zu **beschreiben** ohne Rückgriff auf die reellen Koordinaten (Real- und Imaginärteil). Dies geschieht im Folgenden:

Hilfssatz 2: Seien $a, b \in \mathbb{C}$ und $a \neq b$.

(a) $\Gamma(a,b) = \{z \in \mathbb{C} : (b-a)\overline{(z-a)} = \overline{(b-a)}(z-a)\}$

(b) $\mathcal{K}(a,b) = \{z \in \mathbb{C} : (z-a)\overline{(z-a)} = (b-a)\overline{(b-a)}\}$
Dabei wurde wie üblich die zu $w \in \mathbb{C}$ konjungiert komplexe Zahl mit $\overline{w}$ bezeichnet.

Beweis:

(a) Sei Δ die rechtsstehende Menge. Man rechnet nach: $\Gamma = \{a + (b-a)t : t \in \mathbb{R}\} \subset \Delta$. Umgekehrt gilt für $z \in \Delta$:

$$(z-a)(b-a)^{-1} = \overline{(z-a)(b-a)^{-1}}.$$

Daher gibt es ein $t \in \mathbb{R}$ mit $(z-a) = (b-a)t$. Somit $z \in \Gamma$, bzw. $\Delta \subset \Gamma$.

(b) ist wohl allgemein bekannt. □

Sind in dem Hilfssatz $a, b \in M$, dann sind schon $b-a, \overline{b-a}$ nicht mehr notwendig in M. Bei der Bestimmung etwa von $\Gamma(a,b) \cap \mathcal{K}(a',b')$ und $a', b' \in M$ treten noch verwickeltere Ausdrücke in a, b, a', b' auf, die i. A. alle nicht mehr in M liegen. Allerdings liegen sie alle in $\mathbb{Q}(M \cup \overline{M})$ oder in einer Erweiterung vom Grad 2 von $\mathbb{Q}(M \cup \overline{M})$. Unter der zusätzlichen Vorraussetzung $0, 1 \in M$ wird sich später noch ergeben, dass $\mathbb{Q}(M \cup \overline{M}) \subset \overset{\circ}{\overline{M}}$ (folgt unmittelbar aus Satz 4, s. u.). Vorläufig spielt dies allerdings noch keine Rolle.

Satz 3: Sei $c \in M^{(1)}$, dann ist

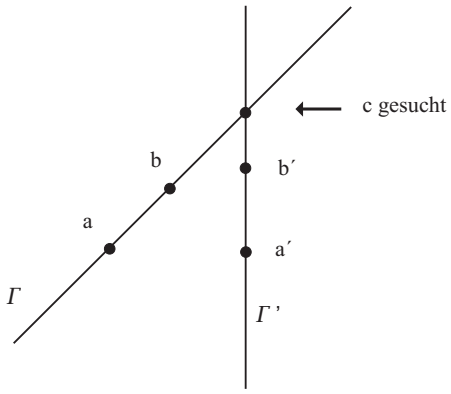
$$[\mathbb{Q}(M \cup \overline{M})(c) : \mathbb{Q}(M \cup \overline{M})] \leq 2.$$

Dabei ist $\overline{M} = \{\overline{z} : z \in M\}$.

Bemerkung 4: Wenn Char(K)$\neq$ 2 und $[F : K] = 2$, dann gibt es $\alpha \in F$, $d \in K$ mit $F = K(\alpha)$ und $\alpha^2 = d$ (oder: $\alpha = „\sqrt{d}$). Körpererweiterungen der Dimension ≤ 2, wie sie in Satz 1 auftreten, sind also stets Quadratwurzelerweiterungen (QWE).

Beweis von Satz 3:

(a)



$$\begin{aligned} a &\neq b \\ a' &\neq b' \\ a, a',\, b, b' &\in M \end{aligned}$$

Nach Hilfssatz 2(a):

$$\Gamma = \{z \in \mathbb{C} : (b-a)\overline{(z-a)} = \overline{(b-a)}(z-a)\}$$

$$\Gamma' = \{z \in \mathbb{C} : (b'-a')\overline{(z-a')} = \overline{(b'-a')}(z-a')\}$$

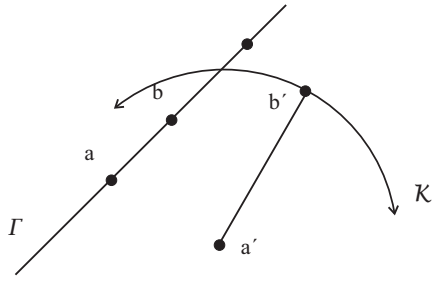
Für $z \in \Gamma \cap \Gamma'$ gilt dann:

$$\overline{z} = \tfrac{\overline{(b-a)}}{b-a}(z-a) + \overline{a} \text{ und } \overline{z} = \tfrac{\overline{(b'-a')}}{(b'-a')}(z-a') + \overline{a'}$$

also $z \cdot u = v \quad u, v \in \mathbb{Q}(M \cup \overline{M})$

Man sieht: Falls $\Gamma \cap \Gamma' \neq \varnothing$ und $\Gamma \neq \Gamma'$ ist $z \in \mathbb{Q}(M \cup \overline{M})$.

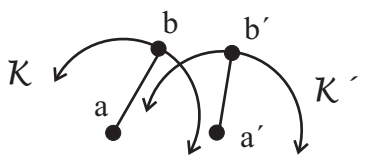
(b) Mit Hilfssatz 2(a) und (b) erhält man:



$$\left.\begin{aligned} \Gamma &= \{z \in \mathbb{C} : (b-a)\overline{(z-a)} = \overline{(b-a)}(z-a)\} \\ \mathcal{K} &= \{z \in \mathbb{C} : (z-a')\overline{(z-a')} = \overline{(b'-a')}(b'-a')\} \end{aligned}\right\} \quad \circledast$$

Für $z \in \Gamma \cap \mathcal{K}$ gilt zunächst wieder $\overline{z} = \frac{\overline{(b-a)}}{b-a}(z-a) + \overline{a}$. Damit kann $\overline{z}$ in $\circledast$ eliminiert werden und es ergibt sich eine quadratische Gleichung für z über $\mathbb{Q}(M \cup \overline{M})$. Da $b \neq a$ hat diese zwar stets Lösungen, aber die Lösungen führen nicht immer zu Punkten in $\Gamma \cap \mathcal{K}$.

(c) Hier gilt noch Hilfssatz 2(b):



Für $z \in \mathcal{K} \cap \mathcal{K}'$ muss gelten $\overline{z} = \frac{(b-a)\overline{(b-a)}}{(z-a)} + \overline{a}$ und $\overline{z} = \frac{(b'-a')\overline{(b'-a')}}{(z-a')} + \overline{a'}$.

Es resultiert wieder eine quadratische Gleichung für z mit Koeffizienten aus $\mathbb{Q}(M \cup \overline{M})$. □

Beispiel zum Beweisteil (b): $a = 0$, $b = i$, $a' = 2$, $b' = 3$ dann ist $\Gamma = \{z \in \mathbb{C} : \overline{z} = -z\}$ und $\mathcal{K} = \{z \in \mathbb{C}(z-2)(\overline{z}-2) = 1\}$ und die resultierende quadratische Gleichung lautet $z^2 = 3$.

Bemerkung 5: Sei K ein Unterkörper von $\mathbb{C}$ mit $\overline{K} = K$ und sei $c \in \mathbb{C}$. Dann gilt:

$$[K(c) : K] = [K(\overline{c}) : K]$$

denn "–" ist ein Automorphismus von $\mathbb{C}$.

Definition 6:

Sei $K = F_o \subset F_1 \subset \ldots \subset F_r = F$ ein Körperturm und gelte: $[F_i : F_{i-1}] \leq 2$ für $1 \leq i \leq r$, dan heißt F iterierte Quadratwurzelerweiterung (kurz: **iQWE**) von K.

Als Motivation für diese Definition dient die Bemerkung

Satz 7: Sei $K = \mathbb{Q}(M \cup \overline{M})$.

(a) Ist $c \in \mathbb{C}$ konstruierbar aus M, dann liegt $K(c)$ in einer iQWE innerhalb $\mathbb{C}$ von K.

(b) Insbesondere ist $[K(c) : K] = 2^m$, m geeignet.

Für (a) gibt es eine Umkehrung, siehe Satz 10. Aus $[K(c) : K] = 2^m$ folgt i.A. **nicht** die Konstruierbarkeit von c. Für ein **Gegenbeispiel** siehe J. Rotmann: Galois Theory; Remark p. 90.

Beweis: Seien $c_1, \ldots, c_s = c$ die Punkte, die sich jeweils bei den endlich vielen Konstruktionsschritten ergeben: und zwar c_1 aus $M^{(1)}$ und c_i aus $(M \cup \{c_1, \ldots, c_{i-1}\})^{(1)}$ für $2 \leq i \leq s$. Wir betrachten folgenden Körperturm:
$K \subset K(c_1) \subset K(c_1, \overline{c}_1) =: K_1 \subset K_1(c_2) \subset K_1(c_2, \overline{c}_2) =: K_2 \subset \ldots \subset K_{s-1}(c_s) \subset K_{s-1}(c_s, \overline{c}_s) =: K_s =: F$.
Wegen Satz 3 und der nachfolgenden Bemerkung 5 ist F eine iQWE von K. Beachte dabei, dass $K_\nu = \mathbb{Q}(M \cup \{c_1, \ldots, c_\nu\} \cup \overline{M \cup \{c_1, \ldots, c_\nu\}})$. □

Der in den Vorbemerkungen angesprochene "Übersetzungsvorgang" wird durch Satz 7(a) und seine spätere Umkehrung Satz 10 geleistet:

$$\left\{ \begin{array}{l} c \text{ aus } M \\ \text{konstruierbar ?} \end{array} \right\} \longleftrightarrow \left\{ (\mathbb{Q}(M \cup \overline{M}))(c) \subset \text{iQWE von } \mathbb{Q}(M \cup \overline{M}) \,? \right\}$$

Will man darauf hinaus, dass c nicht konstruierbar ist, genügt schon Satz 7(a): Man versucht zu zeigen, dass c nicht in einem Quadratwurzelturm über $\mathbb{Q}(M \cup \overline{M})$ liegen kann. Auch ohne die Umkehrung von Satz 7(a) lassen sich daher die o. a. klassischen Konstruktionsprobleme schon weitgehend klären.

(a) **Quadratur des Kreises:** Gegeben $M = \{0, 1\} = \overline{M}$, also $\mathbb{Q}(M \cup \overline{M}) = \mathbb{Q}$.
Zu konstruieren: $c = \frac{\sqrt{\pi}}{2}$.
Da $[\mathbb{Q}(\sqrt{\pi}) : \mathbb{Q}(\pi)] = 2$ und $[\mathbb{Q}(\pi) : \mathbb{Q}] = \infty$ wegen der **Transzendenz von** π (Satz von Lindemann (1882) zitiert nach Ebbinghaus e. a. "Zahlen" 2. Auflage(1988). S.

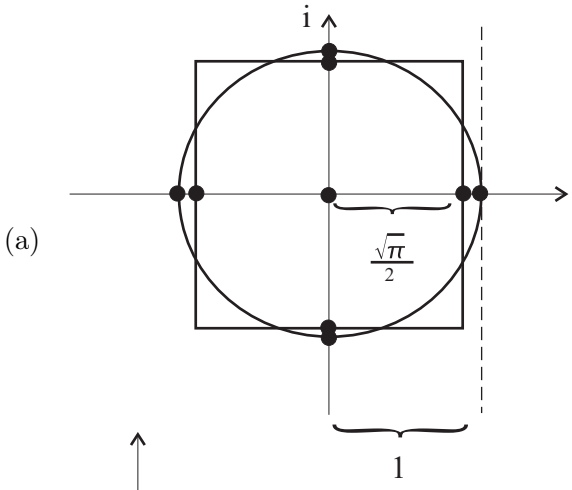
124), ist $[\mathbb{Q}(\sqrt{\pi}) : \mathbb{Q}] = \infty$. $\mathbb{Q}(c)$ kann daher nicht in einer iQWE von $\mathbb{Q}$ liegen. Wegen Satz 7 ist c nicht konstruierbar.

(b) **Rektifikation des Kreisumfangs:** Gegeben $M = \{0, i\}$, zu konstruieren $c = 2\pi$. Vorgehen analog zu (a). Ergebnis: c ist nicht konstruierbar.

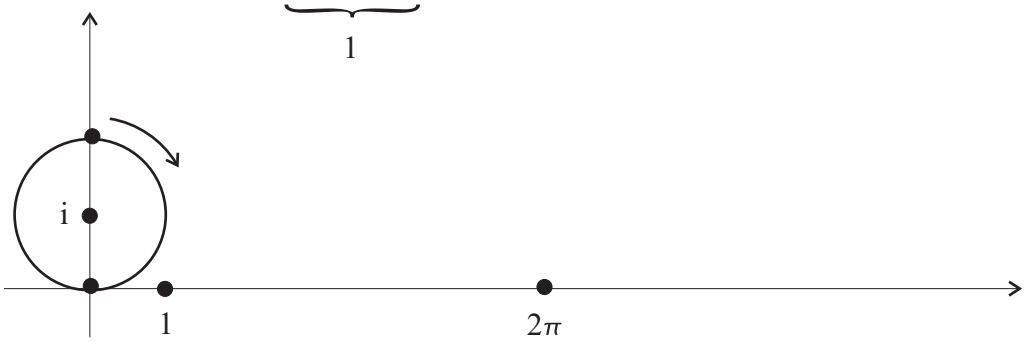
(c) **Würfelverdoppelung:** Gegeben $M = \{0, 1\}$, zu konstruieren $c = \sqrt[3]{2}$.
Da $[\mathbb{Q}(c) : \mathbb{Q}] = 3$, ist c nach Satz 7 nicht konstruierbar.

Abbildungen zu (a) - (d)

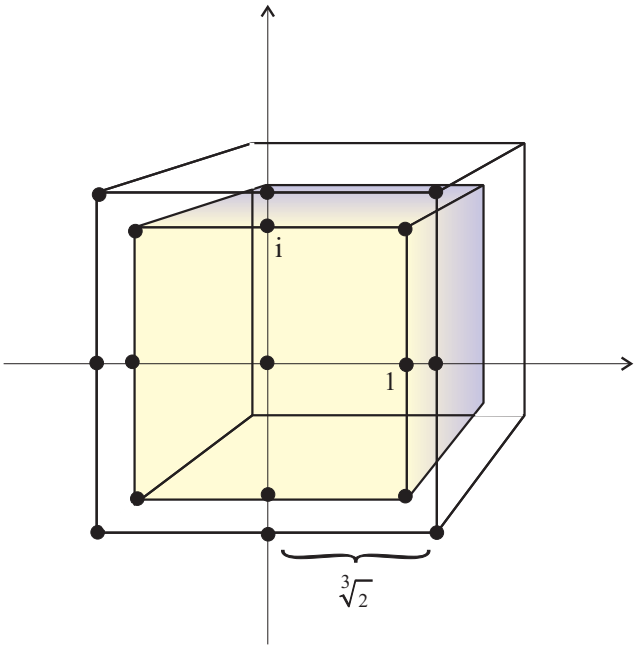
(a)

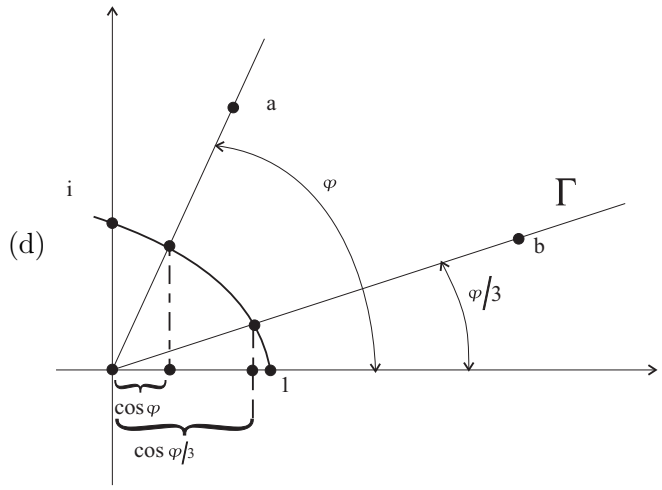


(b)



(c)





(d) **Dreiteilung des Winkels φ:**

Gegeben ist $\{0, 1, a\}$; zu konstruieren ist irgend ein Punkt $b \neq 0$ auf Γ(siehe Abbildung zu (d). Offensichtlich ist ein solcher Punkt b genau dann konstruierbar aus $\{0, 1, a\}$, wenn $(\cos \varphi/3)$ aus $M = \{0, 1, \cos \varphi\}$ konstruierbar ist.

Für gewisse φ ist eine Konstruktion möglich: z. B. $\varphi = 90°$. Wegen Satz 7 untersuchen wir an Stelle des geometrischen Problems die Körpererweiterung $F = K(\cos \varphi)$ mit $K = \mathbb{Q}(\cos \varphi)$. Ist $[F : K]$ ungerade, ergibt sich die Unmöglichkeit einer Konstruktion für den gegebenen Winkel φ.

Aus der Beziehung

$$\cos \varphi + i \sin \varphi = e^{i\varphi} = \left(e^{i\varphi/3}\right)^3 = (\cos(\varphi/3)) + i \sin(\varphi/3)^3$$

erhält man eine Gleichung für $\alpha = 2 \cos(\varphi/3)$ über K :

$$(2 \cos(\varphi/3))^3 - 3(2 \cos(\varphi/3)) - 2 \cos \varphi = 0$$

bzw. $\alpha^3 - 3\alpha - 2 \cos \varphi = 0$.

Behauptung: Für $\varphi = 60°$ ist $\cos \varphi/3 = \cos 20°$ nicht konstruierbar.

Beweis: Dann ist $\cos \varphi = \frac{1}{2}$ und $f = x^3 - 3x - 1$ hat $2\alpha = 2 \cos 20°$ als Nullstelle. $f \in \mathbb{Z}[x]$ mit höchsten Koeffizienten 1. Dann müssen alle rationalen Nullstellen ganz sein und den konstanten Term -1 teilen. Da $f(1) \neq 0$ und $f(-1) \neq 0$, hat f keine rationalen Nullstellen und ist somit als Polynom vom Grad 3 unzerlegbar über $K = \mathbb{Q}(\cos 60°) = \mathbb{Q}(1/2) = \mathbb{Q}$. Es folgt $[F : K] = 3$. □

Wie wir gesehen haben führt die Einführung von Koordinaten und die algebraische Beschreibung (analytische Geometrie) zu einer "Trivalisierung" der betrachteten Konstruktionsprobleme.
Das folgende Konstruktionsproblem ist auch auf der algebraischen Seite noch nicht gelöst.

Für welche n ist die Konstruktion der Eckpunkte eines regelmäßigen n-Ecks aus $M = \{0, 1\}$ mit Zirkel und Linear möglich?

Unser bisheriger Wissenstand erlaubt immerhin schon folgende Teilaussage:

Satz 8: Sei $n \geq 3$. Wenn das regelmäßige $n-$Eck (aus $\{0,1\}$) konstruierbar ist, dann ist entweder $n = 2^k$ mit $k \geq 2$ oder $n = 2^k \cdot p_1 \dots p_r$ mit paarweise verschiedenen Fermat-Primzahlen $p_1, \dots, p_r$ und $k \geq 0$.

Definition: Eine Primzahl p heißt **Fermat-Primzahl,** wenn $p = 2^{2^t} + 1$.
Einzige bisher bekannte Beispiele: $t = 0, \dots, 4$ bzw. : $p = 3, 5, 17, 257, 65.537$.

Beweis von Satz 8:

(a) Das regelmäßige $n-$Eck ist konstruierbar genau dann, wenn $\zeta_n := e^{\frac{2\pi i}{n}}$ konstruierbar ist (jeweils aus $\{0,1\}$).

(b) Wenn ζ_n konstruierbar ist, dann auch ζ_m für alle Teiler m von n, denn $\zeta_n^{\frac{n}{m}} = \zeta_m$.

(c) Wenn ζ_n konstruierbar, p prim, $p \neq 2$ und $\boldsymbol{p|n}$, dann ist $p = 2^{2^t} + 1$:
Da $M = \{0,1\}$ ist hier $\mathbb{Q}(M \cup \overline{M}) = \mathbb{Q}$.
Das Minimalpolynom von ζ_p über $\mathbb{Q}$ ist $x^{p-1}+\ldots+x+1$. Daher ist $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p-1$.
Wegen Satz 7(b) muss dann gelten: $p-1 = 2^m$, m geeignet. Erstaunlicherweise muss nun zwangsläufig auch m eine $2-$er Potenz sein. Denn wäre $q > 2$ ein ungerader Teiler von m mit $m = rq$, dann würde gelten:

$$-p = -2^m - 1 = -(2^r)^q - 1 \underset{\text{da } q \text{ ungerade}}{=} (-2^r)^q - 1 = \underbrace{((-2^r) - 1)}_{\substack{\neq \pm 1 \\ < p}} \underbrace{((-2^r)^{q-1} + \ldots + (-2^r) + 1)}_{\neq \pm 1}$$

(d) Ist p eine ungerade Primzahl mit $p|n$ und ist ζ_n konstruierbar, dann gilt **nicht** $p^2|n$:

Annahme, es würde gelten: $p^2|n$. Wegen (b) ist dann ζ_{p^2} konstruierbar.

ζ_{p^2} ist Nullstelle von $\frac{x^{p^2}-1}{x^p-1} = \frac{(x^p)^p-1}{x^p-1}$

$$= (x^p)^{p-1} + \ldots + (x^p) + 1 = f$$

f ist unzerlegbar in $\mathbb{Q}[x][x := u + 1$; Eisenstein; ausgeführt z. B. bei Hadlock; siehe auch bei Stewart p. 181]. Da $\deg f = p(p-1)$ folgt: $p|[\mathbb{Q}(\zeta_{p^2}) : \mathbb{Q}]$ im Widerspruch zu Satz 7(b). □

Nun möchte man natürlich gerne noch wissen, ob zumindest für die oben angegebenen Fermat-Primzahlen ζ_p auch wirklich konstruierbar ist. Die Vorgabe einer Konstruktion ist eine Möglichkeit, das Problem zu lösen.[Bis $n = 17$ schon Gauß bekannt; interessante historische Hinweise für $n = 257$ und $n = 65.537$ bei Fischer/Sacher: Einführung in die Algebra S. 211 und bei Hadlock p. 119]. Auf Gauß geht auch die Umkehrung von Satz 8 zurück. Zu ihrer Herleitung benötigen wir eine Umkehrung von Satz 7(a). Diese wird sich unmittelbar aus folgender dataillierten Beschreibung von $\overline{\overline{M}}^{\circ}$ ergeben, die auch für sich interessant ist.

Satz 9: Seien $0, 1 \in M$.

(a) $\overline{\overline{M}}^{\circ}$ ist ein Unterkörper von $\mathbb{C}$.

(b) Mit dem Körper $W = \overline{\overline{M}}^{\circ} \cap \mathbb{R}$ gilt: $\overline{\overline{M}}^{\circ} = W + iW$.

(c) $\overline{\overline{M}}^{\circ}$ ist algebraisch über $\mathbb{Q}(M)$.

(d) $\overline{\overline{M}}^{\circ}$ besitzt keine Körpererweiterung der Dimension 2 kurz: $\overline{\overline{M}}^{\circ}$ ist quadratisch abgeschlossen.

(e) $\overline{\overline{M}}^{\circ}$ ist der kleinste Unterkörper von $\mathbb{C}$, der M enthält und quadratisch abgeschlossen ist.

(f) $\overline{\overline{M}}^{\circ} = \bigcup\{F : F \text{ ist iQWE von } \mathbb{Q}(M) \text{ in } \mathbb{C}\}$

Der **Beweis** folgt am Ende des §.

Die angekündigte **Umkehrung von Satz 7(a)** ergibt sich nun unmittelbar aus Satz 9(a) und (d) oder (f):

Satz 10: Ist F eine iQWE von $\mathbb{Q}(M)$ innerhalb $\mathbb{C}$ und $c \in F$, dann ist $c \in \overline{\overline{M}}^{\circ}$ (d. h. c ist konstruierbar).

Beweis: Da $M \subset \overline{\overline{M}}^{\circ}$ und da $\overline{\overline{M}}^{\circ}$ Unterkörper von $\mathbb{C}$ (Satz 9(a)) ist, gilt $\mathbb{Q}(M) \subset \overline{\overline{M}}^{\circ}$. Wegen Satz 9(d) oder (f) folgt nun sofort: $F \subset \overline{\overline{M}}^{\circ}$. □

Bemerkung: Satz 9(b) besagt insbesondere $i \in \overline{\overline{M}}^{\circ}$ und $\overline{c}$, Re(c), Im (c) $\in \overline{\overline{M}}^{\circ}$, falls $c \in \overline{\overline{M}}^{\circ}$.

Mit Hilfe von Satz 10 erhalten wir die **Umkehrung von Satz 8:**

Satz 11: Sei $n = 2^k$ mit $k \geq 2$ oder $n = 2^k p_1 \dots p_r$ mit $k \geq 0$ und mit paarweise verschiedenen Fermatprimzahlen $p_1, \dots, p_r$. Dann ist ζ_n konstruierbar.

Bemerkung: Die Sätze 8 und 11 liefern eine vollständige Charakterisierung derjenigen n für die ζ_n konstruierbar ist. Zugleich entsteht aber ein neues, zahlentheoretisches Problem: "Bestimme **alle** Fermatprimzahlen". Letzteres ist bislang ungelöst. Immerhin wissen wir genau für welche $n \leq 65537$ (=letzte bekannte Fermatprimzahl) ζ_n konstruierbar ist, nämlich für:

$$n = 3, 4, 5, 6, 8, 10, 12, 15, 16, 17, 20, 24, 30, 32, 34, \dots$$

Beweis von Satz 11:

(a) $\boldsymbol{n = 2^k}$, dann ist ζ_n offensichtlich konstruierbar.

(b) $\boldsymbol{n = p}$, $\boldsymbol{p}$ **Fermat-Primzahl:** Das Minimalpolynom von ζ_p über $\mathbb{Q}$ ist $x^{p-1}+\ldots+x+1$. Daher ist $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p-1 = 2^{2^t}$, $t \geq 0$ geeignet. Da $x^{p-1}+\ldots+x+1 = \prod_{i=1}^{p-1}(x-\zeta_p^i)$, ist $\mathbb{Q}(\zeta_p)$ ein Zerfällungskörper über K, also galois´sch über K, da ja $\text{char}(\mathbb{Q}) = 0$. Sei $G = \text{Aut}_{\mathbb{Q}}(\mathbb{Q}(\zeta_p))$. Dann ist $|G| = p - 1 = 2^{2^t}$.

Der erste Sylow´sche Satz (siehe Jacobson Basic Algebra I p.78) besagt insbesondere, dass eine Gruppe der Ordnung 2^m stets eine Untergruppe der Ordnung 2^{m-1} enthält. Diese ist zwangsläufig ein Normalteiler! (Ü)

Mit Induktion ergibt sich daher, dass **G auflösbar** ist, und zwar genauer, dass es eine Nomalteilerkette gibt.

$< 1 >= G_r \lhd \ldots \lhd G_o = G$ und $|G_i/G_{i+1}| = 2$

Dem entspricht ein Körperturm:

$$\mathbb{Q} \subset F_o \subset \ldots \subset F_r = \mathbb{Q}(\zeta_p) \text{ mit } [F_{i+1} : F_i] = 2.$$

Nach Satz 10 ist daher $\zeta_p \in \overline{\overset{\circ}{\{0,1\}}}$, bzw. konstruierbar aus $\{0,1\}$.

(c) **Seien $u, v \in \mathbb{N}_+, ggT(u,v) = 1$ und seien ζ_u und ζ_v konstruierbar, dann ist auch $\zeta_{u \cdot v}$ konstruierbar:**

Es gibt u', v' derart, dass $uv' + u'v = 1$ und es ist dann

$$(\zeta_u)^{u'} \cdot (\zeta_v)^{v'} = e^{(\frac{u'}{u} + \frac{v'}{v})2\pi i} = e^{\frac{2\pi i}{uv}} = \zeta_{uv}$$

Da ζ_u, $\zeta_v \in \overline{\overset{\circ}{\{0,1\}}}$ ist nun nach Satz 9(a) auch $\zeta_{uv} \in \overline{\overset{\circ}{\{0,1\}}}$... oder, wenn man Satz 9 nicht benutzen will:
Nach Satz 7(a) sind $\mathbb{Q}(\zeta_u)$ und $\mathbb{Q}(\zeta_v)$ jeweils in einer iQWE von $\mathbb{Q}$ innerhalb $\mathbb{C}$ enthalten, daher auch $\mathbb{Q}(\zeta_u) \vee \mathbb{Q}(\zeta_v)$ (Übung). □

Literaturhinweis: Ein Quadratwurzelausdruck für ζ_{17} wird ausführlich bei F. Bachmann Algebra (1990) hergeleitet. S. 186 ff. Dort gibt es weitere Hinweise auf S. 189. Die folgende **Formel für ζ_{17}** ist diesem Buch entnommen:

$$\zeta_{17} = \frac{1}{2}S + i\sqrt{1 - (\frac{1}{2}S)^2}$$

mit $S = (\zeta_{17} + \zeta_{17}^{-1}) = \frac{-1+\sqrt{17}}{8} + \frac{-1+\sqrt{17}}{16}\sqrt{\frac{17+\sqrt{17}}{2}} + \frac{1}{4}\sqrt{17 + 3\sqrt{17} - \frac{7+\sqrt{17}}{2}\sqrt{\frac{17+\sqrt{17}}{2}}}$

offensichtlich ist $0 \leq S \leq 2$, da $|\zeta_{17}| = 1$.

Es bleibt noch der Beweis von Satz 9 nachzutragen:
Die folgenden 9 Aussagen lassen sich alle durch Angabe einfacher Konstruktionen beweisen. Sofern diese nicht offensichtlich sind werden sie kurz angedeutet. Satz 9 ergibt sich dann unmittelbar aus (1)-(9).

(1) $i \in \overline{\overset{\circ}{M}}$

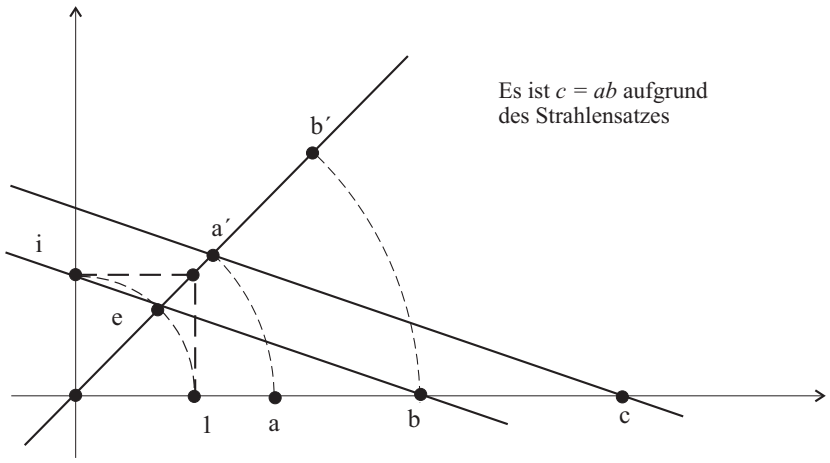
(2) $a_1 + ia_2 \in \overline{\overset{\circ}{M}} \quad \Rightarrow \quad a_1,\, ia_2 \in \overline{\overset{\circ}{M}}$

(3) $a_1 + ia_2 \in \overline{\overset{\circ}{M}} \quad \Rightarrow \quad a_2 + ia_1 \in \overline{\overset{\circ}{M}}$ und $a_1 - ia_2 \in \overline{\overset{\circ}{M}}$

(4) $a_1,\, a_2 \in \overline{\overset{\circ}{M}} \cap \mathbb{R} \quad \Rightarrow \quad a_1 + ia_1 \in \overline{\overset{\circ}{M}}$

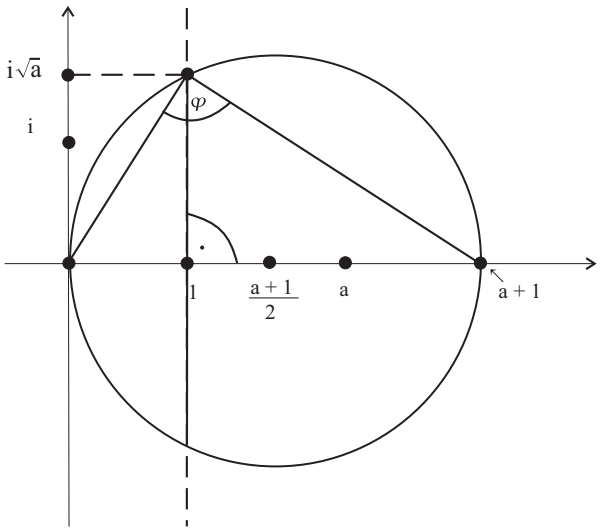
(5) $a,\, b \in \overline{\overset{\circ}{M}} \cap \mathbb{R} \quad \Rightarrow \quad a + v \in \overline{\overset{\circ}{M}} \cap \mathbb{R}$

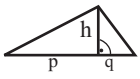
(6) $a,\, b \in \overline{\overset{\circ}{M}} \cap \mathbb{R} \quad \Rightarrow \quad a \cdot b \in \overline{\overset{\circ}{M}} \cap \mathbb{R}$



(7) $0 \neq a \in \overset{\circ}{\overline{M}} \cap \mathbb{R} \Rightarrow a^{-1} \in \overset{\circ}{\overline{M}} \cap \mathbb{R}$.
Ziehe in obiger Figur die Graden $\Gamma(1, a')$ und konstruiere dann die Parallele durch e. Diese schneidet die reelle Achse in a^{-1} (Strahlensatz).

(8) $0 < a \in \overset{\circ}{\overline{M}} \cap \mathbb{R} \Rightarrow \sqrt{a} \in \overset{\circ}{\overline{M}} \cap \mathbb{R}$



Aufgrund des Höhensatzes [$h^2 = pq$: ] ist $i\sqrt{a}$ konstruierbar und damit auch $\sqrt{a}$.

(9) $a, b \in \overset{\circ}{\overline{M}} \Rightarrow a + b,\ a \cdot b \in \overset{\circ}{\overline{M}}$
$0 \neq a \in \overset{\circ}{\overline{M}} \Rightarrow a^{-1},\ \sqrt{a} \in \overset{\circ}{\overline{M}}$
Beachte dabei: mit $a = \mathrm{re}^{i\varphi}$, $b = \mathrm{se}^{i\psi}$ ist $ab = \mathrm{rse}^{i(\varphi+\psi)}$ und $\sqrt{a} = \sqrt{r}e^{i\varphi/2}$, außerdem: $a^{-1} = \frac{\overline{a}}{a\overline{a}}$. □

Schlussbemerkungen: Das klassische Thema 'Konstruierbarkeit mit Zirkel und Lineal' kann man als abgeschlossen ansehen. Allerdings stellt Satz 11 einen Zusammenhang her zu einem bisher ungelösten Problem der Zahlentheorie. Ganz anders sieht es aus, wenn man andere Konstruktionstechniken zulässt. Ein Beispiel hierfür ist die gut lesbare Arbeit: 'Constructions Using Conics' von Eric Bainville und Bernard Genèves im Mathematical Intelligencer Heft 3, 2000, S. 59-72. Dort werden unter anderem schöne Konstruktionen für regelmäßige n-Ecke angegeben. Dabei wird sowohl MAPLE als auch Cabri-Geometrie-Software benutzt. Ein weiteres aktuelles ergibt sich im Rahmen der so genannten 'Origamics'. Ein gut lesbarer Artikel zu Letzterem ist
`http://www.mathematik.uni-dortmund.de/didaktik/_personelles/people/henn/origa_hd.pdf`