22. Konstruktionen mit Zirkel und Lineal

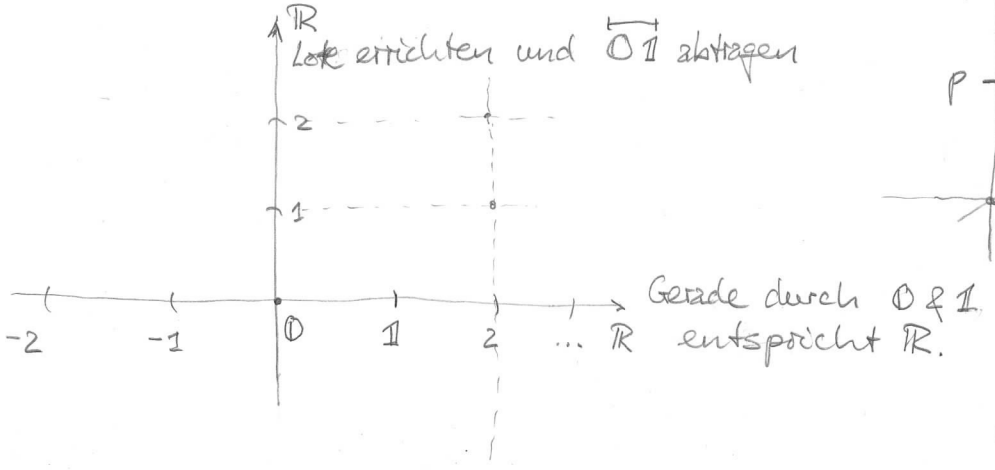
Wir untersuchen welche Punkte der reellen Ebene $\mathbb{R}^2$ sich, ausgehend von zwei fest gewählten Punkten, mit Hilfe von Zirkel und Lineal konstruieren lassen. Dazu müssen wir zuerst festlegen, was wir mit "konstruieren" meinen, und dann werden wir die Konstruktionen mit Körpererweiterungen in Verbindung bringen.

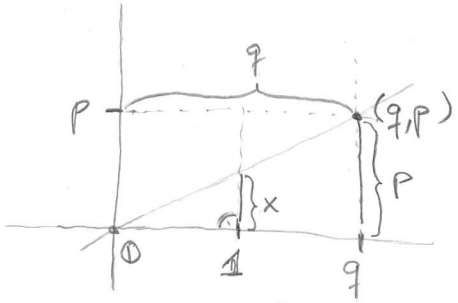
Mit Zirkel und Lineal sind folgende Punkte, Geraden und Kreise konstruierbar:

- Die beiden fest gewählten Punkte sind konstruierbar (kstb.), wobei wir ohne Einschränkung die mit $(0,0) =: \mathbb{0}$ und $(1,0) =: \mathbb{1}$ identifizieren.
- Sind $A \& B$ zwei versch. kstb. Punkte und M ein kstb. Punkt, so ist die Gerade $g = AB$ durch A und B, und der Kreis $k_{M,r}$ mit Mittelpunkt M und Radius $r = \overline{AB}$ (Länge der Strecke AB) konstruierbar.
- Sind $g_1 \& g_2$ kstb. Geraden und $k_{M_1,r_1} \& k_{M_2,r_2}$ kstb. Kreise (paarweise verschieden), so sind die Schnittpunkte (falls sie existieren) von g_1 und g_2, g_1 und k_{M_1,r_1}, und k_{M_1,r_1} und k_{M_2,r_2} konstruierbar.

<u>Bem.</u> Nicht jeder Punkt einer kstb. Geraden (kstb. Kreises) ist kstb.

Wir zeigen zuerst, dass alle rationalen Punkte $\mathbb{Q} \subseteq \mathbb{R}$ (bzw. $\mathbb{Q}^2 \subseteq \mathbb{R}^2$) kstb. sind: $\{\mathbb{0}, \mathbb{1}\} \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Z}^2 \longrightarrow \mathbb{Q}^2$





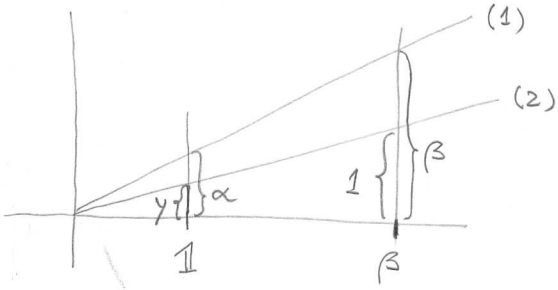
2. Strahlensatz:

$$\frac{p}{q} = \frac{x}{1} \Rightarrow x = \frac{p}{q}$$

Lemma 22.1 Sei C mit $\mathbb{Q} \subseteq C \subseteq \mathbb{R}$ eine Menge von kstb. Punkten. Dann sind mit $\alpha, \beta \in C$ auch $\alpha+\beta$, $-\beta$, $\alpha \cdot \beta$ und β^{-1} (für $\beta \neq 0$) kstb. Insbesondere lässt sich C zu einem Körper K erweitern mit $C \subseteq K \subseteq \mathbb{R}$, in welchem alle $\alpha \in K$ kstb. sind.

Def. Wir nennen den Zw.-Körper K mit $\mathbb{Q} \subseteq K \subseteq \mathbb{R}$ einen konstruierbaren Körper.

Beweis von Lem. 22.1: $\alpha \pm \beta$ klar.



Mit dem 2. Strahlensatz gilt:

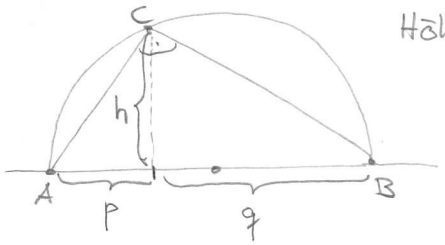
$$\frac{x}{\beta} = \frac{\alpha}{1} \Rightarrow x = \alpha \cdot \beta \quad (1)$$

$$\frac{1}{\beta} = \frac{y}{1} \Rightarrow y = \beta^{-1} \quad (2)$$

⊣

Lemma 22.2 Sei $\mathbb{Q} \subseteq K \subseteq \mathbb{R}$ ein Körper und $\alpha \in K$ kstb., so ist auch $\sqrt{\alpha}$ (für $\alpha \geq 0$) kstb.

Beweis:



Mit dem Satz von Thales ist $\triangle ABC$ rechtwinklig.

Höhensatz: $h^2 = p \cdot q$

Für $p=1$ und $q=\alpha$ erhalten wir $h^2 = 1 \cdot \alpha = \alpha$, also $h = \sqrt{\alpha}$

⊣

Lemma 22.3 Sei $K \subseteq \mathbb{R}$ ein kstb. Körper und seien $\alpha_i, \beta_i, \gamma_i, \rho_i \in K$ für $i \in \{1,2\}$, mit $\rho_i \neq 0$, $\lambda(\alpha_1, \beta_1, \gamma_1) \neq (\alpha_2, \beta_2, \gamma_2)$ für $\lambda \in \mathbb{R}$ und $(\alpha_1, \beta_1) = (\alpha_2, \beta_2)$.

Dann gilt:

(a) $g_i: \alpha_i x + \beta_i y + \gamma_i = 0$ für $i \in \{1,2\}$ sind kstb. Geraden.

(b) $k_i: k_{(\alpha_i, \beta_i), \rho_i}$ für $i \in \{1,2\}$ sind kstb. Kreise.

(c) Für den Schnittpunkt $S = (\varepsilon, \delta)$ von $g_1 \cap g_2$ (falls er ex.) gilt $\varepsilon, \delta \in K$.

(d) Für die Schnittpunkte $S_i = (\varepsilon_i, \delta_i)$ von g_1 und k_2 (falls sie ex.) gilt $K(\varepsilon_1, \varepsilon_2, \delta_1, \delta_2) = K(\sqrt{\omega})$ für ein $\omega \in K$ mit $\sqrt{\omega} \in \mathbb{R}$.

(e) Analog für die Schnittpunkte $S_i = (\varepsilon_i, \delta_i)$ von $k_1 \cap k_2$.

Beweis: (a) und (b) folgen direkt aus der Definition von kstb. Geraden und Kreisen.

(c) ε, δ sind die Lösungen eines lin. Gleichungssystems mit Koeff. in K. somit sind $\varepsilon, \delta \in K$.

(d) Um $(\varepsilon_i, \delta_i)$ zu berechnen, müssen wir das Gleichungssystem

$$\alpha_1 X + \beta_1 Y + \gamma_1 = 0 \qquad (1)$$
$$(X-\alpha_2)^2 + (Y-\beta_2)^2 - \rho_2^2 = 0 \qquad (2)$$

lösen. Dazu ersetzen wir in (1) y durch einen linearen Ausdruck in x (oder umgekehrt) und setzen diesen in (2) ein. Für $S_i = (\varepsilon_i, \delta_i) \in \mathbb{R}^2$ erhalten wir:

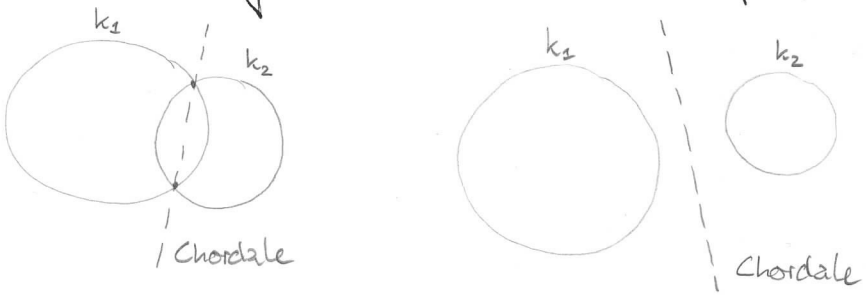
$$\varepsilon_{1,2} = \frac{a \pm \sqrt{\omega}}{2}, \quad \delta_{1,2} = \tilde{a} + \tilde{b}\sqrt{\omega} \quad \text{mit } a, \tilde{a}, \tilde{b}, \omega \in K.$$

D.h. $K(\varepsilon_i, \delta_i) = K(\sqrt{\omega})$ und die Schnittpunkte S_i sind in $K(\sqrt{\omega})$.

(e) Die Differenz der beiden Gleichungen

$$(X-\alpha_1)^2 + (Y-\beta_1)^2 + \rho_1^2 = 0 \quad \text{und} \quad (X-\alpha_2)^2 + (Y-\beta_2)^2 + \rho_2^2 = 0$$

gibt uns die Gleichung der Chordalen von k_1 & k_2:



Falls sich die Kreise k_1 & k_2 schneiden geht die Chordale durch die Schnittpunkte der Kreise und somit folgt (e) aus (d). ⊣

Korollar 22.4 Sei $K \subseteq \mathbb{R}$ ein kstb. Körper. Konstruieren wir mit Zirkel und Lineal aus den Punkten $K^2 \subseteq \mathbb{R}^2$ einen weiteren Punkt $(\alpha, \beta) \in \mathbb{R}^2 \setminus K^2$, so ex. $\omega \in K$ mit $\alpha, \beta \in K(\sqrt{\omega}) = K(\alpha, \beta)$.

Beweis: Folgt direkt aus Lem. 22.3 und der Definition von kstb. ⊣

Bem. Sei K mit $\mathbb{Q} \subseteq K \subseteq \mathbb{R}$ ein kstb. Körper.

- Mit Lemmata 22.1 & 22.3 und Kor. 22.4 entspricht jeder Konstruktion eines neuen Punktes $(\alpha, \beta) \in \mathbb{R}^2$ (aus Punkten von K^2) einer

Körpererw. $K(\sqrt{w}) \supseteq K$ mit $w \in K$ und $\sqrt{w} \notin K$; umgekehrt ist mit Lemmata 22.1 & 22.2 der Erweiterungskörper $K(\sqrt{w})$ für $w \in K$ ein kstb. Körper.

- Es genügt also kstb. Körper $K \subseteq \mathbb{R}$ zu betrachten, obwohl wir die Konstruktionen mit Zirkel und Lineal in $\mathbb{R}^2$ ausführen.

Zusammenfassung: Geometrisch ist eine reelle Zahl $\alpha \in \mathbb{R}$ genau dann konstruierbar, wenn es positive reelle Zahlen $w_0, \dots, w_n \in \mathbb{R}$ gibt, sodass $w_0 \in \mathbb{Q}$, $w_i \in \mathbb{Q}(\sqrt{w_0}, \dots, \sqrt{w_{i-1}})$ für $1 \le i \le n$, und $\alpha \in \mathbb{Q}(\sqrt{w_0}, \dots, \sqrt{w_n})$. Algebraisch ist eine reelle Zahl $\alpha \in \mathbb{R}$ genau dann konstruierbar, wenn es einen Körperturm $\mathbb{Q} = L_0 \subseteq \dots \subseteq L_n \subseteq \mathbb{R}$ gibt mit $\alpha \in L_n$ und $[L_i : L_{i-1}] = 2$ für $1 \le i \le n$. Insbesondere ist $[L_n : \mathbb{Q}] = 2^n$, wovon auch die Umkehrung gilt.

Satz 22.5 Sei $L : \mathbb{Q}$ eine normale Körpererw. mit $L \subseteq \mathbb{R}$ und $[L : \mathbb{Q}] = 2^k$ (für ein $k \in \mathbb{N}$). Dann ist der Körper L konstruierbar, d.h. jedes $\alpha \in L$ ist kstb.

Beweis: Der Beweis ist mit Induktion über k, wobei für $k = 0$ nichts zu beweisen ist (bzw. die Aussage folgt aus $\mathbb{Q}$ kstb.).

- Da $L : \mathbb{Q}$ galoissch ist, ist $|\mathrm{Gal}(L:\mathbb{Q})| = [L : \mathbb{Q}] = 2^k$. Sei $G := \mathrm{Gal}(L:\mathbb{Q})$.
- Da G auf G durch Konjugation operiert, gilt:

$$|G| = \underbrace{|Z(G)|}_{\text{1-elem. Konj.-Kl.}} + \sum_{x \in G} \underbrace{[G : St_G(x)]}_{=: n_x}$$

$|[x]| > 1$

Weil $n_x > 1$ und $n_x \mid 2^k$, ist n_x gerade für alle x mit $|[x]| > 1$. Somit ist $|Z(G)| \ge 2$, und weil $|Z(G)| \mid |G|$ und $|G| = 2^k$, ist $|Z(G)| = 2^\ell$ für ein $1 \le \ell \le k$.

- Mit dem Satz von Cauchy ex. ein $\sigma \in Z(G)$ mit $\mathrm{ord}(\sigma) = 2$. Damit ist, weil $\sigma\tau = \tau\sigma$ (bzw. $\tau\sigma\tau^{-1} = \sigma$) für alle $\tau \in G$, $\langle \sigma \rangle \trianglelefteq G$. Sei $N := \langle \sigma \rangle$, d.h. $N \trianglelefteq G$ mit $|N| = 2$.

- Zum Normalteiler N gehört ein Zwischenkörper $L^N \subseteq L$ mit $[L^N : \mathbb{Q}] = 2^{k-1}$. Da $N \trianglelefteq G$, ist die Körpererw. $L^N : \mathbb{Q}$ normal, und mit der Induktionsvoraussetzung ist L^N kstb.
- Weiter ist $[L : L^N] = 2$. Sei nun $\alpha \in L \setminus L^N$ und $X^2 + bX + c$ das Minimalpolynom von α über L^N. Dann ist $\alpha = \frac{b \pm \sqrt{b^2 - 4c}}{2}$, $b^2 - 4c =: \omega \in L^N$, und $\alpha \in L^N(\sqrt{\omega})$. Also ist α kstb.

⊣

Zur Konstruktion von regelmässigen n-Ecken

Zuerst ein paar Bemerkungen und Definitionen:

- Die Lösungen in $\mathbb{C}$ von $X^n - 1 = 0$ heissen n-te Einheitswurzeln.
- Es ex. genau n paarweise versch. n-te Einheitswurzeln, nämlich $\xi_k := e^{k \cdot \frac{2\pi i}{n}}$ für $0 \leq k < n$.
- Die n-ten Einheitswurzeln bilden eine multiplikative zyklische Untergruppe E_n von $(\mathbb{C}^*, \cdot)$.
- Eine n-te Einheitswurzel ξ_k heisst primitiv, falls $\langle \xi_k \rangle = E_n$.
- Es ex. genau $\varphi(n)$ primitive n-te Einheitswurzeln, nämlich ξ_k mit $(n,k) = 1$.
- Ist ξ_k eine n-te primitive Einheitswurzel, so ist $\operatorname{ord}(\xi_k) = n$. Allgemein: Ist $\operatorname{ord}(\xi_k) = d$ (für $d \mid n$), so ist ξ_k eine d-te primitive Einheitswurzel.

Satz 22.6 Das reguläre n-Eck ist genau dann konstruierbar (in $\mathbb{R}^2$), wenn $\varphi(n) = 2^\ell$ (für ein $\ell \in \mathbb{N}$).

Um diesen Satz mit der Galoistheorie zu verknüpfen, beweisen wir zuerst folgendes

Theorem 22.7 Alle primitiven Einheitswurzeln in $\mathbb{C}$ haben jeweils dasselbe Minimalpolynom über $\mathbb{Q}$.

Beweis: Sei $\mathcal{J}$ die Menge aller n-ten Einheitswurzeln in $\mathbb{C}$ (primitiv oder nicht-primitiv). Wir definieren die Relation $\sim$ auf $\mathcal{J}$ durch

$$\varepsilon \sim \delta :\Leftrightarrow m_\varepsilon = m_\delta \text{, wobei } m_\varepsilon (m_\delta) \text{ das Min.-Poly. von } \varepsilon (\delta) \text{ über } \mathbb{Q} \text{ ist.}$$

- Offensichtlich ist $\sim$ eine Äquivalenzrelation auf $\mathcal{J}$ und für $\varepsilon \in \mathcal{J}$ sei $[\varepsilon]$ die Äquivalenzklasse von ε und $m_{[\varepsilon]}$ das zugehörige Min.-Poly.
- Über $\mathbb{C}$ ist $X^n - 1 = \prod_{\delta \in \mathcal{J}} (X - \delta)$ und weil für $\varepsilon \in \mathcal{J}$, $m_\varepsilon \mid X^n - 1$ und m_ε normiert ist gilt $m_{[\varepsilon]} = \prod_{\delta \in [\varepsilon]} (X - \delta)$ und $X^n - 1 = \prod_{\substack{[\varepsilon] \\ \varepsilon \in \mathcal{J}}} m_{[\varepsilon]}$.
- Das gibt uns eine Faktorisierung von $X^n - 1 \in \mathbb{Z}[X]$ in normierte irred. Faktoren über $\mathbb{Q}$. D.h. $X^n - 1$ ist reduzibel über $\mathbb{Q}$ und mit dem Lemma von Gauss ist, weil $X^n - 1 \in \mathbb{Z}[X]$ primitiv ist, $X^n - 1$ auch reduzibel über $\mathbb{Z}$ und die Polynome $m_{[\varepsilon]}$ sind in $\mathbb{Z}[X]$, haben also ganzzahlige Koeffizienten.

Beh. Ist p eine Primzahl mit $p \nmid n$, dann ist (für $\varepsilon \in \mathcal{J}$): $\varepsilon \sim \varepsilon^p$.

Bew. Für einen Widerspruch nehmen wir an, $m_{[\varepsilon]} \neq m_{[\varepsilon^p]}$, d.h. $\varepsilon \not\sim \varepsilon^p$.

- Wir definieren das Polynom $k \in \mathbb{Z}[X]$ durch

$$k := m_{[\varepsilon^p]}(X^p).$$

D.h. ist $m_{[\varepsilon^p]} = a_0 + a_1 X^1 + a_2 X^2 + \ldots + \underbrace{a_\ell}_{=1} X^\ell$ das Min.-Poly. von ε^p, so ist $m_{[\varepsilon^p]}(X^p) = a_0 + a_1 X^p + a_2 \underbrace{(X^p)^2}_{X^{2p}} + \ldots + \underbrace{(X^p)^\ell}_{X^{\ell p}} = k$.

Insbesondere ist k normiert.

- Somit ist $k(\varepsilon) = a_0 + a_1 \varepsilon^p + a_2 (\varepsilon^p)^2 + \ldots + (\varepsilon^p)^\ell = m_{[\varepsilon^p]}(\varepsilon^p) = 0$, und ε ist eine Nullstelle von k, woraus $m_{[\varepsilon]} \mid k$ folgt.
- Wir finden somit ein $q \in \mathbb{Z}[X]$ mit $m_{[\varepsilon]} \cdot q = k = m_{[\varepsilon^p]}(X^p)$.

[Um zu sehen, dass $q \in \mathbb{Z}[X]$, beachte dass k und $m_{[\varepsilon]}$ normiert sind. Deshalb muss auch q normiert sein. Ist $q = b_0 + b_1 X^1 + \ldots + X^{(\ell-1)p}$ so lässt sich mit Induktion zeigen, dass $b_{(\ell-1)p-1}, b_{(\ell-1)p-2}, \ldots, b_0 \in \mathbb{Z}$ sind.]

[Da k normiert ist, ist k auch primitiv und wir können auch nochmals mit dem Lemma von Gauss argumentieren.]

- Wir betrachten nun die Polynome $m_{[\varepsilon]}$, q, k, und X^n-1 über dem Körper $\mathbb{F}_p$, d.h. wir rechnen modulo p.
  - Zuerst betrachten wir die formale Ableitung $D(\overline{X^n-1}) = \bar{n}X^{n-1}$: Da $p \nmid n$ ist $\bar{n} \neq \bar{0}$ und $\frac{X}{\bar{n}} \cdot D(\overline{X^n-1}) = X^n$. Somit ist $\frac{X}{\bar{n}} \cdot D(\overline{X^n-1}) - (\overline{X^n-1}) = \bar{1}$, d.h. $D(\overline{X^n-1})$ und $\overline{X^n-1}$ sind teilerfremd, und mit Prp. 18.2 folgt:

    $\overline{X^n-1} \in \mathbb{F}_p[X]$ besitzt keine mehrfache Nullstellen in einem Zerf.-Körper $L \supseteq \mathbb{F}_p$. (*)

  - Andererseits ist $\bar{k} = \overline{m_{[\varepsilon]}} \cdot \overline{q} = \overline{m_{[\varepsilon^p]}(X^p)} = \overline{(m_{[\varepsilon^p]})^p}$.
    (mit Aufg. 97 (Serie 18))

    Somit haben $\overline{m_{[\varepsilon]}}$ und $\overline{m_{[\varepsilon^p]}}$ eine gemeinsame Nullstelle in einer Körpererw. von $\mathbb{F}_p$, und damit hat, weil $m_{[\varepsilon]} \neq m_{[\varepsilon^p]}$,

$$\overline{X^n-1} = \prod_{\substack{[\varepsilon] \\ \varepsilon \in J}} \overline{m_{[\varepsilon]}}$$

    eine mehrfache Nullstelle in einem Erweiterungskörper von $\mathbb{F}_p$. Dies widerspricht aber (*), womit die Behauptung bewiesen ist. Beh.!

- Es gilt somit, dass für alle $\varepsilon \in J$ und alle Primzahlen p mit $p \nmid n$, $\varepsilon^p \sim \varepsilon$. Da für p, q gilt $(\varepsilon^p)^q = \varepsilon^{p \cdot q}$, gilt für alle $u = p_1 \cdot \ldots \cdot p_e$ mit p_i Primzahl und $p_i \nmid n$, $u \in (\mathbb{Z}/n\mathbb{Z})^*$ und $\varepsilon^u \sim \varepsilon$; und weiter gilt, dass alle $u \in (\mathbb{Z}/n\mathbb{Z})^*$ von dieser Form sind.
- Für jeden Teiler $d \mid n$ sei $J_d \subseteq J$ die Menge aller d-ten primitiven Einheitswurzeln. Dann ist $J = \dot{\bigcup}_{d \mid n} J_d$ (disj. Vereinigung). Um dies zu sehen, beachte dass für jedes $\varepsilon \in J_d$, $J_d = \{\varepsilon^u : u \in (\mathbb{Z}/d\mathbb{Z})^*\}$.
- Somit ist für $d \mid n$, $\Phi_d := \prod_{\delta \in J_d} (X - \delta)$ das Min.-Poly. von jeder der d primitiven d-ten Einheitswurzeln und $\Phi_d \in \mathbb{Z}[X]$.

Korollar 22.8 Für $n \in \mathbb{N}$ ist $X^n - 1 = \prod_{d \mid n} \Phi_d$ mit $\Phi_d \in \mathbb{Z}[X]$.

Beweis von Satz 22.6: ($\Rightarrow$) Ist das reguläre n-Eck konstruierbar, so folgt dass für $\xi = (\underbrace{\cos(\frac{2\pi}{n})}_{=:\varepsilon}, i\cdot\underbrace{\sin(\frac{2\pi}{n})}_{=:\delta}) \in \mathbb{C}$ gilt: $\varepsilon, \delta \in L \subseteq \mathbb{R}$

L ist ein kstb. Körper, und $[L:\mathbb{Q}] = 2^k$. Weiter gilt $\xi \in L(i)$ mit $[L(i):L] = 2$, d.h. $[L(i):\mathbb{Q}] = 2^{k+1}$.

- Weil ξ eine primitive n-te Einheitswurzel ist, ist $\mathbb{Q}(\xi)$ ein Zerf.-Körper von $X^n - 1$ über $\mathbb{Q}$ und die Körpererw. $\mathbb{Q}(\xi):\mathbb{Q}$ ist galoissch. Insbesondere ist für $G := \mathrm{Gal}(\mathbb{Q}(\xi):\mathbb{Q})$, $|G| = [\mathbb{Q}(\xi):\mathbb{Q}]$.
- Weil mit Thm. 22.7 alle primitiven n-ten Einheitswurzeln dasselbe Min.-Poly. haben und jeder $\mathbb{Q}$-Autom. $\sigma \in G$ durch $\sigma(\xi)$ bestimmt ist, gibt es genau $\varphi(n)$ $\mathbb{Q}$-Autom. von $\mathbb{Q}(\xi)$, denn $\varphi(n)$ ist die Anzahl der primitiven n-ten Einheitswurzeln. Somit ist $[\mathbb{Q}(\xi):\mathbb{Q}] = \varphi(n)$. $= 2^{k+1}$ $= \varphi(n)$
- Wir haben also $[L(i):\mathbb{Q}] = [L(i):\mathbb{Q}(\xi)]\cdot[\mathbb{Q}(\xi):\mathbb{Q}]$, d.h. $\varphi(n) = 2^\ell$ für $\ell \in \mathbb{N}$.

($\Leftarrow$) Da für $\varepsilon := \cos(\frac{2\pi}{n}) = \frac{1}{2}(\xi + \xi^{-1})$, ξ eine Nullstelle von $X^2 - 2\varepsilon X + 1$ ist, ist $[\mathbb{Q}(\xi):\mathbb{Q}(\varepsilon)]$ entweder 1 oder 2. Da weiter $\mathbb{Q}(\xi):\mathbb{Q}$ normal ist und $G \cong (\mathbb{Z}/n\mathbb{Z})^*$ abelsch ist, ist $\mathrm{Gal}(\mathbb{Q}(\xi):\mathbb{Q}(\varepsilon)) \trianglelefteq G$ und $\mathbb{Q}(\varepsilon):\mathbb{Q}$ ist ebenfalls normal. Weiter gilt:

$$\underbrace{[\mathbb{Q}(\xi):\mathbb{Q}]}_{=2^\ell} = \underbrace{[\mathbb{Q}(\xi):\mathbb{Q}(\varepsilon)]}_{=1 \text{ oder } 2}\cdot[\mathbb{Q}(\varepsilon):\mathbb{Q}] \Rightarrow [\mathbb{Q}(\varepsilon):\mathbb{Q}] = 2^m \text{ für } m \le \ell.$$

Somit ist $\mathbb{Q}(\varepsilon) \subseteq \mathbb{R}$ kstb., und mit ε ist auch das n-Eck kstb. ⊣

Korollar 22.9 Das reguläre n-Eck ist genau dann konstruierbar, wenn $n = 2^s \cdot p_1 \cdot \ldots \cdot p_k$ für $s, k \in \mathbb{N}$ und die p_i's paarweise versch. Fermatprimzahlen sind, d.h. Primzahlen der Form $2^{2^m}+1$ für $m \in \mathbb{N}$.

Beweis: Ist $n = \prod_i p_i^{\ell_i}$ (p_i prim, paarw. versch., $\ell_i \ge 1$), so ist mit Aufg. 51.(b)ff(e):
$\varphi(n) = \prod_i p_i^{\ell_i - 1}(p_i - 1)$. Ist nun $\varphi(n) = 2^t$, so muss gelten $\ell_i = 1$ für alle i mit $p_i \neq 2$, und damit ist $n = 2^s \cdot p_1 \cdot \ldots \cdot p_k$ mit $p_i = 2^{t_i}+1$.
Sei u ungerade. Dann gilt allg. $(x^u+1) = (x+1)(x^{u-1} - x^{u-2} + - \ldots + 1)$ für alle x. Für $x = 2^a$ erhalten wir somit $(2^a+1) \mid 2^{a\cdot u}+1$.
Ist also $p_i = 2^{t_i}+1$ prim, so kann t_i keinen ung. Faktor enthalten, d.h. $t_i = 2^m$ für $m \in \mathbb{N}$. ⊣