SoSe 2024

Universität Stuttgart
PD. Dr. P. H. Lesky

Konstruierbarkeit

Inhaltsverzeichnis

Hinweis:
Der Inhalt der Kapitel 1 – 4 ist ist nach geeigneter Aufbereitung für interessierte Schüler:innnen der Oberstufe verständlich. Es gibt hierzu im *Korrespondenzzirkel* des *Schülerzirkels Mathematik* zwei Einheiten, in denen diese Aufbereitung durchgeführt wurde. Bei Interesse kann man sich auf der Seite `https://www.f08.uni-stuttgart.de/schulen/schuelerzirkel-mathematik/` des Schülerzirkels Mathematik anmelden, um die Materialien des Korrespondenzzirkels herunterladen zu können.

1 Konstruktionen mit Zirkel und Lineal

1.1 Definition: Eine Zahl $\alpha \in \mathbb{R}$ heißt **konstruierbar**, wenn zu jeder beliebigen Strecke l eine Strecke a mit Zirkel und Lineal konstruiert werden kann, so dass für die Längen der beiden Strecken $|a| = |\alpha| \cdot |l|$ gilt.
Spezialisierung: Gilt $|l| = 1$, so ist eine Strecke der Länge $|\alpha|$ konstruierbar.

1.2 Satz: Sind $\alpha, \beta \in \mathbb{R}$ konstruierbar, dann sind auch

$$\alpha \pm \beta,\ \alpha \cdot \beta,\ \frac{\alpha}{\beta} \text{ (falls } \beta \neq 0),\ \sqrt{|\alpha|}$$

konstruierbar.

Beweis: Übungen

1.3 Folgerung: **1)** $\mathbb{Q}$ ist konstruierbar.

2) Sei $\beta \in \mathbb{Q}$, $\beta > 0$. Dann ist jede Zahl $z = x + y\sqrt{\beta}$ mit $x, y \in \mathbb{Q}$ konstruierbar.

1.4 Frage: Welche reellen Zahlen sind konstruierbar? Welche algebraischen Zahlen sind konstruierbar?

2 Körpererweiterungen

2.1 Definition: Sei $(K, +, \cdot)$ ein Körper. Eine Teilmenge $K' \subseteq K$ heißt**Unterkörper** von K, falls $(K', +, \cdot)$ ein Körper ist. Umgekehrt heißt K **Körpererweiterung** von K', geschrieben $K \mid K'$.

2.2 Satz (Unterkörperkriterium): Sei $(K, +, \cdot)$ ein Körper, $K' \subseteq K$. Dann ist K' genau dann ein Unterkörper, wenn

(U1) $0, 1 \in K'$ (Null- und Einselement) und

(U2) $\forall x, y \in K' : x + y \in K' \ \wedge \ x \cdot y \in K'$ und

(U3) $\forall x \in K' : -x \in K' \ \wedge \ \forall x \in K' \setminus \{0\} : \frac{1}{x} \in K'$.

2.3 Folgerung: **1)** K'' Unterkörper von K' und K' Unterkörper von $K \Rightarrow$ K'' Unterkörper von K.

2) K', K'' Unterkörper von $K \Rightarrow$ $K' \cap K''$ Unterkörper von K.

2.4 Beispiele: **1)** $\mathbb{R} \mid \mathbb{Q}$, $\mathbb{C} \mid \mathbb{R}$.

2) $K_1 := \{x + y\sqrt{3} : x, y \in \mathbb{Q}\}$ ist Unterkörper von $\mathbb{R}$, denn

(U1) $0, 1 \in K_1$,

(U2) $(x + y\sqrt{3}) + (x' + y'\sqrt{3}) = (x + x') + (y + y')\sqrt{3} \in K_1$,
$(x + y\sqrt{3}) \cdot (x' + y'\sqrt{3}) = (xx' + 3yy') + (xy' + yx')\sqrt{3} \in K_1$,

(U3) $(x + y\sqrt{3}) + (-x - y\sqrt{3}) = 0$ und
$(x + y\sqrt{3}) \cdot \dfrac{1}{x^2 - 3y^2}(x - y\sqrt{3}) = 1$.

2.5 Grundvoraussetzung: Wir betrachten Polynome als Funktionen $p : \mathbb{R} \to \mathbb{R}$, wobei die Koeffizienten aus einem Unterkörper von $\mathbb{R}$ sind. Im Folgenden wird immer vorausgesetzt:

K, K', K'' sind Unterkörper von $\mathbb{R}$ und Körpererweiterungen von $\mathbb{Q}$.

2.6 Definition: **1)** $K[x] = \{p : K \to K \mid p \text{ ist Polynom mit Koeffizienten aus } K\}$.

2) Sei K ein Körper und $K' \mid K$. Dann heißt $\alpha \in K'$ **algebraisch** über K, falls

$$\exists p \in K[x] : \big(p(\alpha) = 0 \wedge p \neq 0\big).$$

3) Eine **algebraische Körpererweiterung** von K ist eine Körpererweiterung, deren Elemente alle algebraisch über K sind.

2.7 Beispiele: $K_1 \mid \mathbb{Q}$ ist algebraische Körpererweiterung (K_1 definiert in 2.4)

$\mathbb{R} \mid \mathbb{Q}$ ist keine algebraische Körpererweiterung

2.8 Definition: $p \in K[x]$ heißt **reduzibel** über K, falls

$$\exists q, r \in K[x] : p = q \cdot r \ \wedge \ \deg(q) \geq 1 \ \wedge \ \deg(r) \geq 1.$$

Ist $p \in K[x]$ mit $\deg(p) \geq 1$ nicht reduzibel, so heißt p **irreduzibel**.
Achtung: Konstante Polynome sind weder reduzibel noch irreduzibel.

2.9 Beispiele: **1)** $p(x) = x^2 - 3$ ist irreduzibel über $\mathbb{Q}$, aber reduzibel über K_1 aus 2.4.

Denn $p(x) = (x - \sqrt{3})(x + \sqrt{3})$. Da $\pm\sqrt{3} \notin \mathbb{Q}$, ist p irreduzibel über $\mathbb{Q}$.

2) $p(x) = x^4 - 3$ ist irreduzibel über $\mathbb{Q}$, aber reduzibel über K_1, obwohl p keine Nullstelle in K_1 besitzt.

Denn $p(x) = (x^2 - \sqrt{3})(x^2 + \sqrt{3})$ in K_1, aber $\pm\sqrt[4]{3} \notin K_1, \notin \mathbb{Q}$.

2.10 Satz und Definition: Sei α algebraisch über K. Dann existiert genau ein $p \in K[x] \setminus \{0\}$ mit

(M1) p ist **normiert**, d.h. $p(x) = 1 \cdot x^{\deg(p)} + \ldots$ und

(M2) $p(\alpha) = 0$ und

(M3) $\forall q \in K[x] : \big(\deg(q) < \deg(p) \Rightarrow q(\alpha) \neq 0 \vee q = 0\big)$.

Dieses Polynom heißt **Minimalpolynom** von α über K. Wegen $p \neq 0$ und (M2) gilt $\deg(p) \geq 1$.

Beweis: **1)** Existenz: Setze $M := \big\{p \in K[x] : p(\alpha) = 0 \ \wedge \ p \neq 0\big\}$.
α algebraisch $\Rightarrow \ M \neq \emptyset \ \Rightarrow \ n := \min\big\{\deg(p) : p \in M\big\}$ existiert.
Wähle $p \in M$ mit $\deg(p) = n$. Sei $p(x) = a_n x^n + \ldots$.
Setze $p_0(x) := \frac{1}{a_n} p(x)$. Dann erfüllt p_0 (M1) und (M2).
Außerdem gilt für $q \in K[x]$: $\deg(q) < n \Rightarrow q \notin M \Rightarrow q(\alpha) \neq 0 \vee q = 0$.
Somit erfüllt p_0 auch (M3).

2) Eindeutigkeit: Seien $p_1, p_2 \in K[x] \setminus \{0\}$, die (M1) – (M3) erfüllen.
(M2), (M3) $\Rightarrow \deg(p_1) = \deg(p_2)$
Setze $p := p_1 - p_2$.
(M1) $\Rightarrow \ \deg(p) \leq \deg(p_1) - 1 < \deg(p_1)$
$p(\alpha) = 0$ und (M3) $\Rightarrow \ p = 0$.

□

2.11 Satz: Ist α algebraisch über K, dann gelten die folgenden Aussagen.

1) Das Minimalpolynom von α ist irreduzibel.

2) Für alle $p \in K[x] \setminus \{0\}$ gilt

$$p \text{ erfüllt (M1) und (M2)} \wedge p \text{ ist irreduzibel} \Rightarrow p \text{ ist das Minimalpolynom von } \alpha.$$

Beweis: **1)** Sei p das Minimalpolynom von α und $p = q \cdot r$ mit $q, r \in K[x]$.
Dann $\deg(p) \geq 1$ und insbesondere $q, r \neq 0$
$p(\alpha) = 0 \Rightarrow q(\alpha) = 0 \vee r(\alpha) = 0$. O.B.d.A. $q(\alpha) = 0$.
$q(\alpha) = 0$, $q \neq 0$ und (M3) für $p \Rightarrow \deg(q) \geq \deg(p)$
$\overset{p=q\cdot r}{\Rightarrow} \deg(q) = \deg(p) \wedge \deg(r) = 0$
$\Rightarrow r$ ist ein konstantes Polynom,
$\Rightarrow \ p$ ist irreduzibel.

2) Sei $p \in K[x]$ irreduzibel mit $p(\alpha) = 0$, p normiert, und sei p_0 das Minimalpolynom von α.
(M3) $\Rightarrow \deg(p) \geq \deg(p_0)$
Teilen mit Rest: $p = q_1 \cdot p_0 + r_1$, $\deg(r_1) < \deg(p_0)$
$0 = p(\alpha) = q_1(\alpha) \underbrace{p_0(\alpha)}_{=0} + r_1(\alpha)$
$\Rightarrow r_1(\alpha) = 0 \ \wedge \ \deg(r_1) < \deg(p_0)$
(M3) $\Rightarrow r_1 = 0$, also $p = q_1 \cdot p_0$
p ist irreduzibel $\Rightarrow q_1 = \text{konst}$
p, p_0 normiert $\Rightarrow q_1 = 1$, also $p = p_0$.

□

2.12 Definition: Sei α algebraisch über K.

1) $\mathrm{Irr}(\alpha, K) :=$ Minimalpolynom von α über K.

2) α heißt **algebraisch vom Grad** $n := \deg\big(\mathrm{Irr}(\alpha, K)\big)$ über K.

2.13 Beispiele: **1)** $\sqrt{3}$ über $\mathbb{Q}$: $p(x) := x^2 - 3 \;\Rightarrow\; p$ erfüllt (M1) und (M2)
p irreduzibel $\Rightarrow\; \mathrm{Irr}(\sqrt{3}, \mathbb{Q}) = p \;\Rightarrow\; \sqrt{3}$ ist algebraisch über $\mathbb{Q}$ vom Grad 2.

2) $\sqrt{3}$ über K_1:
$\mathrm{Irr}(\sqrt{3}, K_1) = x - \sqrt{3} \;\Rightarrow\; \sqrt{3}$ ist algebraisch über K_1 vom Grad 1.

2.14 Satz und Definition: Seien $K' \mid K$, $\alpha \in K'$ und

$$K(\alpha) \;:=\; \bigcap \big\{K'' \subseteq K' : \alpha \in K'' \;\wedge\; K'' \mid K\big\}.$$

Dann ist $K(\alpha)$ der kleinste Erweiterungskörper von K, der α enthält und heißt von α **erzeugter Erweiterungskörper** von K (2.3: Schnitt von Unterkörpern ist Unterkörper).

2.15 Satz und Definition: Sei $K' \mid K$. Dann bildet K' einen Vektorraum über K, denn

$(K', +)$ ist kommutative Gruppe
Für $\lambda, \mu \in K$ und $v, w \in K'$ gilt $\lambda \cdot v \in K'$ und

$$\begin{aligned} (\lambda + \mu) \cdot v &= \lambda \cdot v + \mu \cdot v \\ \lambda \cdot (v + w) &= \lambda \cdot v + \lambda \cdot w \\ (\lambda \cdot \mu) \cdot v &= \lambda \cdot (\mu \cdot v) \\ 1 \cdot v &= v \end{aligned}$$

Die Dimension von K' als Vektorraum über K heißt **Körpergrad** von K' über K, geschrieben $[K' : K] := \dim(K')$.

2.16 Beispiel: $[K_1 : \mathbb{Q}] = 2$: Basis B von K_1 ist z.B. $B = \{1, \sqrt{3}\}$.

2.17 Satz: Ist α algebraisch über K vom Grad n, so gilt $\big[K(\alpha) : K\big] = n$.

Beweis: Für $n = 2$ vgl. Beispiel 2.4, für $\mathbb{Q}(\sqrt[3]{2})$ siehe Übungen.

2.18 Definition und Satz: Sei $K' \mid K$ und $[K' : K] < \infty$. Dann ist jedes Element $\beta \in K'$ algebraisch über K vom Grad $\leq n$. Sprechweise: K' ist **algebraisch vom Grad** $n := [K' : K]$ über K.

Beweis: Sei $n := [K' : K]$.
Für jedes $\beta \in K'$ ist $\{1, \beta, \beta^2, \ldots, \beta^n\}$ linear abhängig ($n + 1$ Vektoren)
$\Rightarrow\; \exists c_j \in K : \sum_{j=0}^{n} c_j \beta^j = 0$. Also ist β algebraisch höchstens vom Grad n.

□

2.19 Satz: Seien K', K'' Körpererweiterungen von K mit $K'' \mid K'$ und $[K'' : K'], [K' : K] < \infty$. Dann gilt die **Körpererweiterungsformel**

$$[K'' : K] \;=\; [K'' : K'] \cdot [K' : K].$$

Beweis: Seien $\{\alpha_1, \ldots, \alpha_n\}$ Basis von $K' \mid K$
$\{\beta_1, \ldots, \beta_m\}$ Basis von $K'' \mid K'$

1) Sei $x \in K'' \;\Rightarrow\; x \;=\; \sum_{j=1}^{m} c_j \beta_j$ mit $c_j \in K'$

$$= \sum_{j=1}^{m} \Big(\sum_{k=1}^{n} d_{jk} \alpha_k \Big) \beta_j \text{ mit } d_{jk} \in K$$

2) Behauptung: $B := \{\alpha_k \beta_j : k = 1, \ldots, n,\ j = 1, \ldots, m\}$ ist Basis von $K'' \mid K$.

a) B spannt K'' auf: Siehe 1)

b) B ist linear unabhängig: Seien $d_{jk} \in K$ mit

$$\sum_{j=1}^{m} \underbrace{\Big(\sum_{k=1}^{n} d_{jk} \alpha_k \Big)}_{\in K'} \beta_j \;=\; 0$$

$$\overset{\{\beta_1, \ldots, \beta_m\} \text{ lin. unabh.}}{\Rightarrow} \quad \sum_{k=1}^{n} d_{jk} \alpha_k = 0 \text{ für } j = 1, \ldots, m$$

$$\overset{\{\alpha_1, \ldots, \alpha_n\} \text{ lin. unabh.}}{\Rightarrow} \quad d_{jk} = 0 \text{ für } j = 1, \ldots, m,\ k = 1, \ldots, n.$$

$\Rightarrow\; [K'' : K] = \#B = m \cdot n = [K'' : K'] \cdot [K' : K].$

□

2.20 Beispiel: $K_1 = \mathbb{Q}(\sqrt{3}) = \{x + y\sqrt{3} : x, y \in \mathbb{Q}\} \;\Rightarrow\; [K_1 : \mathbb{Q}] = 2$
Es gilt $\sqrt{5} \notin K_1$, denn

$$\begin{aligned} &\text{Annahme } \exists x, y \in \mathbb{Q} : \sqrt{5} = x + y\sqrt{3} \\ &\Leftrightarrow \quad 5 = x^2 + 2xy\sqrt{3} + 3y^2 \\ &\Leftrightarrow \quad \begin{cases} x = 0 \wedge 5 = 3y^2 & \lightning\ \sqrt{\frac{5}{3}} \notin \mathbb{Q} \\ y = 0 \wedge 5 = x^2 & \lightning\ \sqrt{5} \notin \mathbb{Q} \\ x \neq 0 \wedge y \neq 0 \wedge \sqrt{3} = \dfrac{1}{2xy}(5 - x^2 - 3y^2) \in \mathbb{Q} & \lightning \end{cases} \end{aligned}$$

$\Rightarrow\; \sqrt{5}$ ist algebraisch über K_1 vom Grad 2, denn

$$p(x) = x^2 - 5 \overset{\text{in } \mathbb{R}}{=} (x - \sqrt{5})(x + \sqrt{5}) \;\Rightarrow\; \mathrm{Irr}(\sqrt{5}, K_1) = p.$$

$K_2 := K_1(\sqrt{5}) \;\Rightarrow\; [K_2 : K_1] = 2$ (Basis $B = \{1, \sqrt{5}\}$)
$\Rightarrow\; [K_2 : \mathbb{Q}] = [K_2 : K_1] \cdot [K_1 : \mathbb{Q}] = 4.$
Nach Beweis des letzten Satzes: Basis $\{1 \cdot 1, 1 \cdot \sqrt{5}, \sqrt{3} \cdot 1, \sqrt{3} \cdot \sqrt{5}\}$.

2.21 Bemerkungen: **1)** $\alpha \in K \;\Rightarrow\; K(\alpha) = K \;\wedge\; \big[K(\alpha) : K\big] = 1.$

2) $K(-\alpha) = K(\alpha)$. Für $\alpha \neq 0$: $K\big(\frac{1}{\alpha}\big) = K(\alpha)$.

2.22 Satz: Sei $K'' \mid K' \mid K$. Dann

$$\alpha \in K'' \text{ algebraisch über } K \;\Rightarrow\; \alpha \text{ algebraisch über } K'.$$

Beweis: $\mathrm{Irr}(\alpha, K)(\alpha) = 0$ und $\mathrm{Irr}(\alpha, K) \in K[x] \subseteq K'[x]$. □

2.23 Satz: Seien $K'' \mid K' \mid K$ und K' algebraisch über K. Dann

$$\alpha \in K'' \text{ algebraisch über } K' \;\Rightarrow\; \alpha \text{ algebraisch über } K.$$

Beweis: $\mathrm{Irr}(\alpha, K')(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0$ mit $a_j \in K'$.

Betrachte $K_0 := K(a_0)$, $K_1 := K_0(a_1)$, …, $K_{n-1} := K_{n-2}(a_{n-1})$.

$$\begin{array}{l} a_0 \text{ algebraisch über } K \overset{2.17}{\Rightarrow} [K_0 : K] < \infty \\ a_1 \text{ algebraisch über } K \overset{2.22}{\Rightarrow} a_1 \text{ algebraisch über } K_0 \overset{2.17}{\Rightarrow} [K_1 : K_0] < \infty \\ \qquad\qquad \vdots \end{array}$$

$\Rightarrow\; [K_{n-1} : K] = [K_{n-1} : K_{n-2}] \cdots [K_0 : K] < \infty$
$\overset{2.18}{\Rightarrow}\; K_{n-1}$ algebraisch über K

$\mathrm{Irr}(\alpha, K') \in K_{n-1}[x] \;\Rightarrow\; \alpha$ algebraisch über K_{n-1}
$\Rightarrow\; \alpha \in K_{n-1}(\alpha) \;\wedge\; [K_{n-1}(\alpha) : K] = \underbrace{[K_{n-1}(\alpha) : K_{n-1}]}_{<\infty \text{ nach } 2.17} \cdot [K_{n-1}, K] < \infty$

$\overset{2.18}{\Rightarrow}\; \alpha$ algebraisch über K. □

2.24 Folgerung: Seien $K' \mid K$ und $n := [K' : K] < \infty$ und $\alpha \in K'$. Dann ist α algebraisch über K. Bezeichnet m den algebraischen Grad von m über K, so gelten

1) m teilt n.

2) $m = n \;\Leftrightarrow\; K(\alpha) = K'$.

Beweis: Nach 2.18 ist K' algebraisch über K, also auch $\alpha \in K'$ algebraisch über K..

1) $\alpha \in K' \;\wedge\; K' \mid K \;\Rightarrow\; K' \mid K(\alpha)$
Es gilt $\big[K(\alpha) : K\big] = m$ (2.17)
2.22 $\Rightarrow$ K' algebraisch über $K(\alpha)$
Multiplikationsformel: $n = [K' : K] = \big[K' : K(\alpha)\big] \cdot m$.

2) Aus letzter Formel: $n = m \;\Leftrightarrow\; \big[K' : K(\alpha)\big] = 1 \;\Leftrightarrow\; K' = K(\alpha)$.

□

2.25 Bemerkung: Sei $n = [K' : K] < \infty$. Man kann sich nun die Frage stellen, ob es dann ein $\alpha \in K$ geben muss, das algebraisch über K vom Grad n ist. Gibt es ein solches α, so gilt $K' = K(\alpha)$, und man nennt α ein *primitives Element* von K'. Eine hinreichende Bedingung für die Existenz eines solchen α gibt der *Satz vom primitiven Element*.

3 Konstruierbarkeit von Zahlen

3.1 Satz: Seien $n \in \mathbb{N}$ und

$$\begin{array}{rcl} \alpha_1 \in \mathbb{Q},\, \alpha_1 > 0,\, K_1 & := & \mathbb{Q}(\sqrt{\alpha_1}), \\ \alpha_2 \in K_1,\, \alpha_2 > 0,\, K_2 & := & K_1(\sqrt{\alpha_2}), \\ \alpha_3 \in K_2,\, \alpha_3 > 0,\, K_3 & := & K_2(\sqrt{\alpha_3}), \\ & \vdots & \\ \alpha_n \in K_{n-1},\, \alpha_n > 0,\, K_n & := & K_{n-1}(\sqrt{\alpha_n}). \end{array}$$

Dann sind alle Element von K_n konstruierbar.

Beweis: Induktionsanfang siehe 1.3.

Induktionsschritt siehe 1.2. □

3.2 Bemerkung: Sei K ein Körper und $\alpha \in K$. Dann ist $\sqrt{\alpha}$ algebraisch vom Grad 1 oder 2 über K. Mit Satz 2.17 folgt $\big[K(\sqrt{\alpha}) : K\big] = 1$ oder $\big[K(\sqrt{\alpha}) : K\big] = 2$.
Somit gilt in 3.1 $\big[K_j(\sqrt{\alpha_{j+1}}) : K_{j-1}(\sqrt{\alpha_j})\big] \in \{1, 2\}$.
$\Rightarrow$ in 3.1 gilt $[K_n : \mathbb{Q}] = 2^k$ für ein $k \in \mathbb{N}_0$.

3.3 Hilfssatz: Sei K ein Unterkörper von $\mathbb{R}$. In einem kartesischen Korrdinatensystem seien Punkte $P_j(x_j, y_j)$ mit $x_j, y_j \in K$ gegeben. Seien weiter g_j Geraden durch je zwei dieser Punkte und k_j Kreise um diese Punkte, die als Radius den Abstand zweier Punkte $|P_jP_k|$ haben. Dann:

1) Der Schnittpunkt $P(x, y)$ zweier Geraden besitzt Koordinaten $x, y \in K$ (falls existent).

2) Die Schnittpunkte eines Kreises mit einer Geraden oder einem anderen Kreis besitzen Koordinaten in $K(\sqrt{\alpha})$ mit jeweils geeignet gewähltem $\alpha \in K$ (falls existent).

Beweis: Vorüberlegungen:

a) Ist g Gerade durch $P_1(x_1, y_1)$ und $P_2(x_2, y_2)$, so gilt

$$g \;=\; \big\{(x, y) \in K^2 : ax + by = c\big\}$$

mit $a = y_2 - y_1 \in K$, $b = x_1 - x_2 \in K$, $c = y_2x_1 - y_1x_2 \in K$.

b) Ist k Kreis um $P_1(x_1, y_1)$ mit $r = |P_2P_3|$, so gilt

$$k \;=\; \big\{(x, y) \in K^2 : (x - x_1)^2 + (y - y_1)^2 = d\big\}$$

mit $d = (x_3 - x_2)^2 + (y_3 - y_2)^2 \in K$.

1) Schnitt von g_1 und g_2:

$$\begin{array}{rcl} a_1x + b_1y & = & c_1 \\ a_2x + b_2y & = & c_2 \end{array} \quad \text{mit } a_j, b_j, c_j \in K$$

liefert Lösungen $(x, y) \in K^2$ (falls existent).

2) Schnitt von g und k:

$$\begin{aligned} ax+by &= c \\ (x-x_0)^2+(y-y_0)^2 &= d \end{aligned} \text{ mit } a,b,c,d \in K.$$

Z.B. $b \neq 0$: $y = \frac{1}{b}(c-ax)$ in Kreisgleichung

$$\begin{aligned} (x-x_0)^2 + \Big(\frac{c}{b} - \frac{a}{b}x - y_0\Big)^2 &= d \\ \Leftrightarrow\ a_1x^2 + a_2x + a_3 &= 0 \text{ mit } a_1,a_2,a_3 \in K \\ \Leftrightarrow\ x_{1,2} &= \frac{-a_2 \pm \sqrt{a_2^2-4a_1a_3}}{2a_1} \in K\big(\sqrt{a_2^2-4a_1a_3}\big) = K(\sqrt{\alpha}) \end{aligned}$$

falls $\alpha = a_2^2 - 4a_1a_3 \geq 0$. Aus Geradengleichung: $y_{1,2} = \frac{1}{b}(c-ax_{1,2}) \in K(\sqrt{\alpha})$.

3) Schnitt von k_1 und k_2:

$$(x-x_0)^2+(y-y_0)^2 = d_0 \quad (1)$$
$$(x-x_1)^2+(y-y_1)^2 = d_1 \quad (2)$$

Bilde (1)−(2):

$$2x(x_1-x_0)+2y(y_1-y_0) = d_0-d_1+x_1^2-x_0^2+y_1^2-y_0^2 \in K. \quad (3)$$

(1) und (3) ist Schnitt Gerade-Kreis, liefert Schnittpunktkoordinaten in $K(\sqrt{\alpha})$.

□

3.4 Satz: Eine Zahl $\alpha \in \mathbb{R}$ ist genau dann in endlich vielen Schritten mit Zirkel und Lineal konstruierbar, wenn es eine endliche Kette von Erweiterungskörpern wie in 3.1 gibt, so dass $\alpha \in K_n$.

Beweis: Rückrichtung: 3.1

Hinrichtung: Es gebe n Konstruktionsschritte, mit denen aus einer Strecke l eine Strecke der Länge $|\alpha| \cdot |l|$ konstruiert wird. In jedem Schritt soll eine der Schnittkonstruktionen aus 3.3 ausgeführt werden.
Lege in die Ebene ein kartesisches Koordinatensystem, so dass l = Strecke von $P(0,0)$ nach $Q(1,0)$.

P, Q haben rationale Koordinaten
$\overset{3.3}{\Rightarrow}$ $\exists \alpha_1 \in \mathbb{Q}$: Für alle im 1. Schritt konstr. Punkte $(x_j^{(1)}, y_j^{(1)})$ gilt $x_j^{(1)}, y_j^{(1)} \in \mathbb{Q}(\sqrt{\alpha_1}) =: K_1$
$\overset{3.3}{\Rightarrow}$ $\exists \alpha_2 \in K_1$: Für alle im 2. Schritt konstr. Punkte $(x_j^{(2)}, y_j^{(2)})$ gilt $x_j^{(2)}, y_j^{(2)} \in K_1(\sqrt{\alpha_2}) =: K_2$
$\vdots$
$\overset{3.3}{\Rightarrow}$ $\exists \alpha_n \in K_{n-1}$: Für alle im n-ten Schr. konstr. Pkte $(x_j^{(n)}, y_j^{(n)})$ gilt $x_j^{(n)}, y_j^{(n)} \in K_{n-1}(\sqrt{\alpha_n}) =: K_n$

Für die Länge $|\alpha|$ gilt nun

$$|\alpha| = \sqrt{(x_j^{(n)}-x_k^{(n)})^2+(y_j^{(n)}-y_k^{(n)})^2} \in K_n(\sqrt{\alpha_{n+1}}) =: K_{n+1}.$$

□

3.5 Folgerung: Ist $\alpha \in \mathbb{R}$ konstruierbar, so folgt:

$$\exists n \in \mathbb{N}_0 : \alpha \text{ ist algebraisch über } \mathbb{Q} \text{ vom Grad } 2^n.$$

Beweis: Letzter Satz: Es gilt $\alpha \in K_{n+1}$ für ein $n \in \mathbb{N}$.
Multiplikationsformel und 3.2: $[K_{n+1} : \mathbb{Q}] = [K_{n+1} : K_n] \cdots [K_1 : \mathbb{Q}] = 2^k$ mit $k \leq n+1$
2.24 $\Rightarrow$ α ist algebraisch über $\mathbb{Q}$ vom Grad m und m teilt 2^k.

□

4 Die klassischen Probleme der konstruktiven Geometrie

4.1 Satz (Würfelverdopplung): Gegeben sei ein Würfel. Es ist nicht möglich, die Kantenlänge eines Würfels, der das doppelte Volumen besitzt, mit Zirkel und Lineal aus der Kantenlänge des gegebenen Würfels zu konstruieren.

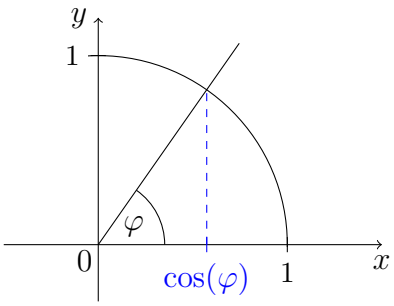
Beweis: $V_{\text{Würfel}} = d^3$, $V' = d'^3 \stackrel{!}{=} 2d^3$
$\Rightarrow \quad \dfrac{d'}{d} = \sqrt[3]{2}$ muss konstruiert werden
$\sqrt[3]{2}$ ist algebraisch über $\mathbb{Q}$ vom Grad 3, denn $\mathrm{Irr}(\sqrt[3]{2}, \mathbb{Q})(x) = x^3 - 2$, siehe Übungen.
$3 \notin \{2^n : n \in \mathbb{N}_0\} \stackrel{\text{letzte Folgerung}}{\Rightarrow} \sqrt[3]{2}$ ist nicht konstruierbar. □

4.2 Satz (Quadratur des Kreises): Gegeben sei ein Kreis mit Radius r. Es ist nicht möglich, aus r mit Zirkel und Lineal die Seitenlänge eines Quadrates zu konstruieren, das den selben Flächeninhalt wie der Kreis besitzt.

Beweis: Sei r der Kreisradius.
$F_{\text{Kreis}} = \pi r^2$, $F_{\text{Quadrat}} = a^2 \stackrel{!}{=} \pi r^2 \;\Rightarrow\; \dfrac{a}{r} = \sqrt{\pi}$ muss konstruiert werden
$\sqrt{\pi}$ ist transzendent (andernfalls wäre π algebraisch)
$\stackrel{3.5}{\Rightarrow}$ $\sqrt{\pi}$ ist nicht konstruierbar. □

4.3 Satz (Dreiteilung des Winkels): Es gibt keine Konstruktion mit Zirkel und Lineal, mit der jeder Winkel in drei gleich große Winkel aufgeteilt werden kann.

Beweis: **1)** Ein Winkel φ ist genau dann konstruierbar, wenn $\cos(\varphi)$ konstruierbar ist.



2) Aus den Additionstheremen: $\cos(3\alpha) = 4\cos^3(\alpha) - 3\cos(\alpha)$.

3) Sei $\varphi = 3\alpha$ gegeben. Zur Bestimmung von $x = \cos\left(\frac{\varphi}{3}\right) = \cos(\alpha)$ muss

$$4x^3 - 3x - \cos(\varphi) \;=\; 0$$

gelöst werden.
Behauptung: Für $\varphi = \frac{\pi}{3}$ ist x nicht konstruierbar, d.h. der Winkel $\alpha = \frac{\pi}{9}$ ist nicht konstruierbar.
$\varphi = \frac{\pi}{3} \;\Rightarrow\; \cos(\varphi) = \frac{1}{2} \;\Rightarrow$ gesucht ist x als Lösung von

$$p(x) \;:=\; 8x^3 - 6x - 1 \;=\; 0.$$

p ist irreduzibel (Übungen). Also ist x algebraisch vom Grad 3.
$3 \notin \{2^n : n \in \mathbb{N}_0\} \stackrel{3.5}{\Rightarrow} x = \cos\left(\frac{\pi}{9}\right)$ ist nicht konstruierbar. □

4.4 Bemerkung: Der Winkel $\varphi = \frac{\pi}{2}$ kann gedrittelt werden, denn $\frac{\varphi}{3} = \frac{\pi}{6}$ ist konstruierbar. Was ändert sich im Beweis?

$\varphi = \frac{\pi}{2} \Rightarrow \cos(\varphi) = 0 \Rightarrow$ Löse $4x^3 - 3x = 0$

$x(4x^2 - 3) = 0 \Leftrightarrow x = 0 \vee x = \pm\frac{\sqrt{3}}{2} \in \mathbb{Q}(\sqrt{3})$

In diesem Fall ist $x = \cos\left(\frac{\varphi}{3}\right)$ algebraisch vom Grad 2 über $\mathbb{Q}$, also konstruierbar.

5 Konstruierbarkeit regelmäßiger Vielecke, Winkelteilung

5.1 Definition: Seien eine Strecke AB und ein Punkt C auf AB gegeben. Dann teilt C die Strecke AB im Verhältnis des **goldenen Schnitts**, falls

$$\frac{|AC|}{|CB|} = \frac{|AB|}{|AC|} =: \Phi.$$

5.2 Satz: **1)** $\Phi = \frac{1}{2}\left(1 + \sqrt{5}\right)$. Insbesondere ist Φ konstruierbar.

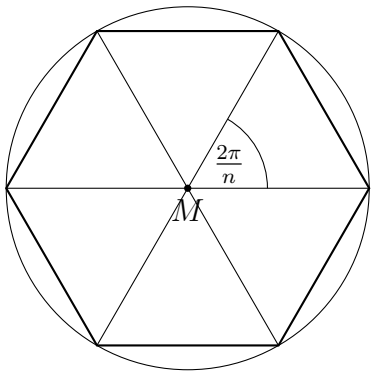
2) $\cos\left(\frac{\pi}{5}\right) = \frac{1}{2}\Phi$, also sind auch die Winkel $\frac{\pi}{5}$ und $\frac{2\pi}{5}$ konstruierbar.

Beweis: **1)** $a := |AC|$, $b := |CB|$

$$\Rightarrow \Phi = \frac{a}{b} = \frac{a+b}{a} = 1 + \frac{b}{a} = 1 + \frac{1}{\Phi}$$
$$\Rightarrow \Phi^2 - \Phi - 1 = 0$$
$$\Leftrightarrow \Phi_{1,2} = \frac{1}{2} \pm \sqrt{\frac{1}{4} + 1} = \frac{1}{2} \pm \frac{\sqrt{5}}{2}$$
$$\overset{\Phi > 0}{\Rightarrow} \Phi = \tfrac{1}{2} + \tfrac{\sqrt{5}}{2}.$$

2) Übungen □

5.3 Bemerkung: Das regelmäßige n-Eck ist genau dann konstruierbar, wenn der Winkel $\frac{2\pi}{n}$ bzw. $\cos\left(\frac{2\pi}{n}\right)$ konstruierbar ist.



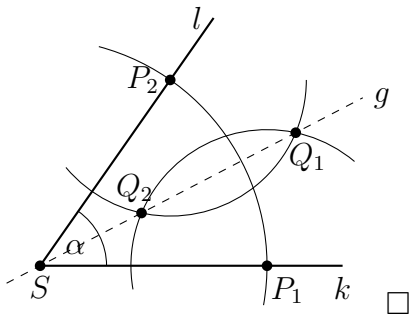
5.4 Satz: Regelmäßige n-Ecke sind für $n = 3, 4, 5, 6$ konstruierbar, für $n = 18$ nicht.

Beweis: $n = 3, 4, 6$ klar, $n = 5$ letzter Satz.
$n = 18$: $\varphi = \frac{2\pi}{18} = \frac{\pi}{9}$ ist nicht konstruierbar (siehe Beweis 4.3). □

5.5 Satz: Halbierung von Winkeln ist konstruierbar.

Beweis: Gegeben ist der Winkel α mit Scheitel S und Schenkeln k, l.

Zeichne Kreis mit beliebigem Radius um S.
Schnitt mit den Schenkeln ergibt die Punkte P_1 und P_2.
Zeichne Kreise mit übereinstimmendem Radius um P_1 und P_2.
Schnitt dieser Kreise ergibt die Punkte Q_1 und Q_2.
Die Punkte S, Q_1 und Q_2 liegen auf einer Geraden g.
g ist die Mittelsenkrechte der Strecke P_1P_2 und halbiert deshalb den Winkel α.



□

5.6 Satz: **1)** Ist das regelmäßige n-Eck konstruierbar, so sind alle $2^m \cdot n$-Ecke mit $m \in \mathbb{N}$ konstruierbar.

2) Ist das regelmäßige n-Eck konstruierbar und gilt $n = k \cdot l$ mit $k, l \in \mathbb{N}$, dann sind auch die regelmäßigen k- und l-Ecke konstruierbar.

3) Sind das regelmäßige m-Eck und n-Eck konstruierbar und gilt $\mathrm{ggT}(m, n) = 1$, dann ist auch das regelmäßige $m \cdot n$-Eck konstruierbar.

Beweis: **1)** $\frac{2\pi}{n}$ konstruierbar $\overset{5.5}{\Rightarrow}$ $\frac{2\pi}{2n}$ konstruierbar $\overset{5.5}{\Rightarrow}$ $\frac{2\pi}{4n}$ konstruierbar ...

2) Konstruiere ein $n = k \cdot l$-Eck. Überspringe jeweils l Ecken. Die verbleibenden Ecken sind Ecken eines regelmäßigen k-Ecks.

3) Erweiterter euklidischer Algorithmus: $\exists k, l \in \mathbb{Z} : k \cdot n + l \cdot m = 1$.
Nach Voraussetzung: $\alpha = \frac{2\pi}{n}$, $\beta = \frac{2\pi}{m}$ konstruierbar.
$\Rightarrow\ l \cdot \alpha + k \cdot \beta = \frac{2\pi}{n} l + \frac{2\pi}{m} k = \frac{2\pi}{n \cdot m}(lm + kn) = \frac{2\pi}{n \cdot m}$ konstruierbar.
(Addition/Subtraktion/Vielfachenbildung von Winkeln durch Aneinandersetzen)

□

5.7 Bemerkung: Unser Kenntnisstand: Welche n-Ecke sind konstruierbar, welche nicht?

$n =$	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
konstruierbar	✓	✓	✓	✓	?	✓	–	✓	?	✓	?	?	✓	✓	?	–	?	✓

5.8 Satz: Seien $P, Q \in \mathbb{Q}[x]$, P irreduzibel, und P, Q haben eine gemeinsame Nullstelle. Dann ist P Teiler von Q.

Beweis: Sei $P(x_0) = Q(x_0) = 0$. OBdA sei P normiert. Dann $P = \mathrm{Irr}(x_0, \mathbb{Q})$.
$Q(x_0) = 0\ \Rightarrow \deg(Q) \geq \deg(P)$.
Teilen mit Rest: $Q = S \cdot P + R$ mit $S, R \in \mathbb{Q}[x]$ und $\deg(R) < \deg(P)$.
$\Rightarrow\ 0 = Q(x_0) = S(x_0) \cdot 0 + R(x_0)$, also $R(x_0) = 0$.
$\deg(R) < \deg(P) \overset{P = \mathrm{Irr}(x_0, \mathbb{Q})}{\Rightarrow} R = 0$.

□

5.9 Satz (Gauß): Sind $P, Q \in \mathbb{Q}[x]$ normierte Polynome, so gilt

$$P \cdot Q \in \mathbb{Z}[x] \;\Rightarrow\; P, Q \in \mathbb{Z}[x].$$

Beweis: Seien $P(x) = x^n + \sum_{j=0}^{n-1} \frac{p_j}{q_j} x^j$, $Q(x) = x^m + \sum_{j=0}^{m-1} \frac{r_j}{s_j} x^j$, wobei p_j, q_j bzw. r_j, s_j jeweils teilerfremd.

Setze $a := \mathrm{kgV}(q_0, \ldots, q_{n-1})$, $b := \mathrm{kgV}(s_0, \ldots, s_{n-1})$ und

$$\begin{aligned} a \cdot P(x) &=: \sum_{j=0}^{n} a_j x^j, \quad a_j \in \mathbb{Z}, \\ b \cdot Q(x) &=: \sum_{j=0}^{m} b_j x^j, \quad b_j \in \mathbb{Z}. \end{aligned}$$

1) Beachte, dass für jede Primzahl p gilt: Nicht alle $a_0, \ldots, a_n$ sind durch p teilbar. Andernfalls wäre $\frac{a}{p} \cdot P \in \mathbb{Z}[x]$ $\lightning$ $a = \mathrm{kgV}(q_0, \ldots, q_{n-1})$
Genauso für $b \cdot Q$.

2) Betrachte $a \cdot b \cdot Q(x) \cdot P(x) =: \sum_{j=0}^{n+m} c_j x^j$ mit $c_j \in \mathbb{Z}$.

Zeige: Es gibt keine Primzahl, die alle der Koeffizienten $c_0, \ldots, c_{n+m}$ teilt.
Sei p eine Primzahl. Setze

$$\begin{aligned} j_0 &:= \min\{j = 0, \ldots, n : p \text{ ist kein Teiler von } a_j\} \\ k_0 &:= \min \underbrace{\{k = 0, \ldots, m : p \text{ ist kein Teiler von } b_k\}}_{\neq \emptyset \text{ wegen 1)}} \end{aligned}$$

$\Rightarrow\; c_{j_0+k_0} = \sum_{j=0}^{j_0+k_0} \underbrace{a_j b_{j_0+k_0-j}}_{(*)}$ ist nicht durch p teilbar,

denn $(*)$ ist durch p teilbar, falls $j \leq j_0 - 1$ oder $j_0 + k_0 - j \leq k_0 - 1 \Leftrightarrow j \geq j_0 + 1$,
$(*)$ ist nicht durch p teilbar für $j = j_0$.

3) Sei nun $P \cdot Q \in \mathbb{Z}[x]$, $P \cdot Q$ normiert
$\Rightarrow\; a \cdot b$ teilt alle Koeffizienten von $a \cdot b \cdot P \cdot Q$
$\overset{2)}{\Rightarrow}\; a \cdot b = 1$
$\Rightarrow\; \mathrm{kgV}(q_0, \ldots, q_{n-1}) = 1$ und $\mathrm{kgV}(s_0, \ldots, s_{m-1}) = 1$
$\Rightarrow\; q_0 = \ldots = q_{n-1} = s_0 = \ldots = s_{m-1} = 0$
$\Rightarrow\; P, Q \in \mathbb{Z}[x]$.

□

5.10 Beispiel: Sei $P(x) = x^5 - 2x^4 - 4x^3 + 2x^2 + 11x + 4$. Ist P reduzibel in $\mathbb{Q}[x]$?

1) Mögliche rationale Nullstellen $x = \pm 1, \pm 2, \pm 4$.

2) Ansatz: $P(x) = (x^2 + ax + b)\big(x^3 - (a+2)x^2 + cx + \frac{4}{b}\big)$
$\overset{5.9}{\Rightarrow}\; a, c, \frac{4}{b} \in \mathbb{Z}$, somit $b \in \{\pm 1, \pm 2, \pm 4\}$

3) Probieren $\Rightarrow\; P(x) = (x^2 - 2x - 1)(x^3 - 3x - 4)$.

5.11 Satz (Eisenstein-Kriterium für normierte Polynome): Sei $P \in \mathbb{Z}[x]$ normiert,

$$P(x) \;=\; x^n + \sum_{j=0}^{n-1} a_j x^j,$$

und es gebe eine Primzahl p, so dass p Teiler von $a_0, \ldots, a_{n-1}$ und p^2 kein Teiler von a_0 ist. Dann ist P über $\mathbb{Q}$ irreduzibel, d.h. in $\mathbb{Q}[x]$ nicht in Faktoren zerlegbar.

Beweis: Annahme $P = Q \cdot R$ mit $Q, R \in \mathbb{Q}[x]$, $\deg(Q), \deg(R) \geq 1$.
Seien $Q(x) = \sum_{j=0}^{m} b_j x^j$, $R(x) = \sum_{j=0}^{k} c_j x^j \;\Rightarrow\; b_m \cdot c_k = 1$ und $m, k \leq n-1$
$b_m \cdot c_k = 1 \;\Rightarrow\; Q, R$ normiert wählbar (betrachte $\frac{1}{b_m} Q$ und $\frac{1}{c_k} R = b_m R$).
Q, R normiert $\overset{5.9}{\Rightarrow}\; Q, R \in \mathbb{Z}[x]$
$a_0 = c_0 \cdot b_0$ durch p teilbar, nicht durch $p^2 \;\Rightarrow$ Entweder b_0 durch p teilbar oder c_0.
OBdA b_0 durch p teilbar und c_0 nicht durch p teilbar.

Setze $j_0 := \min\{j = 0, \ldots, m : b_j \text{ nicht durch } p \text{ teilbar}\} \geq 1$
Beachte: $b_m = 1 \;\Rightarrow\; j_0 \leq m \leq n-1$

$$\Rightarrow\; a_{j_0} = \sum_{j=0}^{j_0} \underbrace{b_{j_0 - j} c_j}_{\substack{\text{Für } j=0\text{: } b_{j_0}\cdot c_0 \text{ nicht durch } p \text{ teilbar} \\ \text{Für } j \geq 1\text{: } b_{j_0-j} \text{ durch } p \text{ teilbar}}} \quad \text{ist nicht durch } p \text{ teilbar } \lightning$$

□

5.12 Satz: Es seien $p \in \mathbb{N}$ eine Primzahl und

$$\Phi_1(x) \;:=\; \frac{x^p - 1}{x - 1} \;=\; \sum_{k=0}^{p-1} x^k,$$
$$\Phi_2(x) \;:=\; \frac{x^{p^2} - 1}{x^p - 1} \;=\; \sum_{k=0}^{p-1} x^{kp} \;=\; \Phi_1(x^p)$$

die **Kreisteilungspolynome**. Dann sind Φ_1, Φ_2 irreduzibel über $\mathbb{Q}$.

Beweis: **1)** $x^p = 1 \;\Leftrightarrow\; x_k = \mathrm{e}^{\mathrm{i}\frac{2\pi}{p}k}$, $k = 0, 1, \ldots, p-1$
$\Rightarrow\; \Phi_1$ hat die Nullstellen $x_1, \ldots, x_{p-1}$.
Beachte: $x_1, \ldots, x_{p-1}$ sind primitive Einheitswurzeln, d.h. für jedes feste k gilt

$$\{x_k^n : n = 0, \ldots, p-1\} \;=\; \{\mathrm{e}^{\mathrm{i}\frac{2\pi}{p}n} : n = 0, \ldots, p-1\} \;=\; \{\text{alle Lösungen von } x^p - 1 = 0\}.$$

2) Annahme: $\Phi_1(x) = Q(x)R(x)$ mit $Q, R \in \mathbb{Q}[x]$, $\deg(Q), \deg(R) \geq 1$
Φ_1 normiert $\;\Rightarrow\; Q, R$ normiert wählbar
$\Phi_1 \in \mathbb{Z}[x] \;\overset{\text{Gauß}}{\Rightarrow}\; Q, R \in \mathbb{Z}[x]$
$\Phi_1(1) = p \;\Rightarrow$ OBdA $Q(1) \in \{\pm p\}$, $R(1) \in \{\pm 1\}$
OBdA kann Q als irreduzibel angenommen werden. Andernfalls:
Zerlege $Q = Q_1 \cdot Q_2$, $Q_1, Q_2 \in \mathbb{Q}[x]$ sind normiert wählbar und nach Gauß folgt $Q_1, Q_2 \in \mathbb{Z}[x]$.

Führe diese Zerlegung so lange fort, bis Q als Produkt von lauter irreduziblen, normierten Polynomen in $\mathbb{Z}[x]$ dargestellt wird. Ersetze Q durch den irreduziblen Teiler $\tilde{Q}$ von Q mit $\tilde{Q}(1) \in \{\pm p\}$, alle anderen Teiler können bei $x = 1$ nur die Werte ± 1 besitzen, schiebe diese Teiler zu R.

Wähle $k, l \in \{1, \ldots, p-1\}$ mit $Q(x_k) = 0$ und $R(x_l) = 0$ (Q, R müssen mindestens eine Nullstelle in $\mathbb{C}$ besitzen, die dann auch Nullstelle von Φ_1 ist).

Nach 1): $\exists n \in \{1, \ldots, p-1\} : x_l = x_k^n$. Setze $\tilde{R}(x) := R(x^n)$
$\Rightarrow$ $\tilde{R} \in \mathbb{Z}[x]$, $\tilde{R}$ ist normiert, $\tilde{R}$ und Q besitzen die Nullstelle $x = x_k$.
Q irreduzibel $\overset{5.8}{\Rightarrow}$ $\tilde{R} = \tilde{Q} \cdot Q$ mit $\tilde{Q} \in \mathbb{Q}[x]$
Gauß $\Rightarrow$ $\tilde{Q} \in \mathbb{Z}[x]$
$\Rightarrow$ $\underbrace{R(1)}_{\in\{\pm 1\}} = \tilde{R}(1) = \underbrace{\tilde{Q}(1)}_{\in\mathbb{Z}} \cdot \underbrace{Q(1)}_{\in\{\pm p\}}$ ↯

Also war die Annahme falsch, Φ_1 ist somit irreduzibel.

3) Was ändert sich bei Φ_2? Die Nullstellen von Φ_2 sind

$$x_k = \mathrm{e}^{\frac{2\pi}{p^2}k} \text{ mit } k \in \{1, \ldots, p^2 - 1\} \setminus \{p, 2p, \ldots, (p-1)p\}.$$

Sonst bleibt alles im Beweis gleich. □

5.13 Hilfsatz: Eine Zahl $n = 2^m + 1$ mit $m \in \mathbb{N}_0$ kann nur dann Prinzahl sein, wenn $m = 2^k$ für geeignetes $k \in \mathbb{N}_0$.

Beweis: Annahme: $m = a \cdot b$ mit $a \geq 3$, a ungerade

$$\Rightarrow\ 2^m + 1 = 2^{ab} + 1 = 1 - (-2^b)^a = \underbrace{\left(1 - (-2^b)\right)}_{\in\mathbb{Z}} \underbrace{\sum_{k=0}^{a-1} \left((-2)^b\right)^k}_{\in\mathbb{Z}}$$

$\Rightarrow$ $2^m + 1$ ist keine Primzahl. □

5.14 Definition: Die Zahlen $F_n = 2^{2^n} + 1$ mit $n = 0, 1, \ldots$ heißen **Fermat-Zahlen**. Es gilt

$$F_0 = 3,\ F_1 = 5,\ F_2 = 17,\ F_3 = 257,\ F_4 = 65\,537.$$

$F_1, \ldots, F_4$ sind Primzahlen, F_5 ist keine Primzahl. Es ist nicht bekannt, ob weitere F_n Primzahlen sind.

5.15 Satz: **1)** Ist $p \in \mathbb{N}$ Primzahl, $p \geq 3$, dann ist das regelmäßige p^2-Eck nicht konstruierbar.

2) Ist $p \in \mathbb{N}$ Primzahl und das regelmäßige p-Eck konstruierbar, dann ist p eine Fermat-Zahl.

Beweis: Sei das regelmäßige m-Eck konstruierbar und $p \geq 3$ Primzahl.
Zeige: $m = p^2 \Rightarrow$ ↯ und $m = p \Rightarrow p$ ist Fermat-Zahl.

1) m-Eck konstruierbar $\Rightarrow \cos\left(\frac{2\pi}{m}\right)$ und $\sin\left(\frac{2\pi}{m}\right)$ konstruierbar
$\overset{3.5}{\Rightarrow}$ $\cos\left(\frac{2\pi}{m}\right), \sin\left(\frac{2\pi}{m}\right)$ sind von algebraischem Grad 2^n über $\mathbb{Q}$ mit passendem $n \in \mathbb{N}_0$
Setze $K' := \mathbb{Q}\big((\cos\left(\frac{2\pi}{m}\right)\big)$, $K := K'\big(\sin\left(\frac{2\pi}{m}\right)\big)$
$\overset{2.24,\ 2.19}{\Rightarrow}$ $[K : \mathbb{Q}] = 2^k$ mit geeignetem $k \in \mathbb{N}_0$
$\Rightarrow$ $\mathrm{e}^{\mathrm{i}\frac{2\pi}{m}} \in K(\mathrm{i})$ und $\big[K(\mathrm{i}) : \mathbb{Q}\big\}\big] = 2^{k+1}$
$\overset{2.24}{\Rightarrow}$ $\mathrm{e}^{\mathrm{i}\frac{2\pi}{m}}$ ist algebraisch über $\mathbb{Q}$ mit Grad l, wobei l Teiler von 2^{k+1}.

2) Sei $m = p^2$. Setze $z := \mathrm{e}^{\mathrm{i}\frac{2\pi}{p^2}}$. z ist Nullstelle von Φ_2
Letzter Satz $\Rightarrow$ $\Phi_2 = \mathrm{Irr}(z, \mathbb{Q})$
$\Rightarrow$ $\mathrm{e}^{\mathrm{i}\frac{2\pi}{p^2}}$ ist algebraisch über $\mathbb{Q}$ vom Grad $\deg(\Phi_2) = p(p-1)$.
$p \geq 3 \Rightarrow p(p-1)$ ist kein Teiler von 2^{k+1} für $k \in \mathbb{N}_0$ ↯

3) Sei $m = p$. $z := \mathrm{e}^{\mathrm{i}\frac{2\pi}{p}}$ ist algebraisch über $\mathbb{Q}$ vom Grad $\deg(\Phi_1) = p - 1$
1) $\Rightarrow \exists l \in \mathbb{N}_0 : p - 1 = 2^l$ bzw. $p = 2^l + 1$
$\overset{5.13}{\Rightarrow}$ p ist eine Fermat-Zahl.

□

5.16 Folgerung: Sei $n \in \mathbb{N}$, $n \geq 3$. Ist das regelmäßige n-Eck konstruierbar, so folgt

$$n \in \{2^j : j \in \mathbb{N},\ j \geq 2\} \cup \{2^j \cdot p_1 \cdots p_k : j \in \mathbb{N}_0,\ k \in \mathbb{N},\ p_1, \ldots, p_k \geq 3 \text{ paarweise verschiedene Fermat-Zahlen, die Primzahlen sind}\}. \quad (*)$$

Beweis: Primfaktorzerlegung $n = 2^j \cdot p_1^{l_1} \cdots p_k^{l_k}$
$\overset{5.6}{\Rightarrow}$ $p_i^{l_i}$-Eck konstruierbar
$\overset{5.15}{\Rightarrow}$ $l_i = 1$ und p_i sind Fermat-Zahlen.

□

5.17 Bemerkungen: **1)** Es gilt auch die Umkehrung: Gilt $(*)$, dann ist das regelmäßige n-Eck konstruierbar (Gauß 1801).
Konstruktionen: 17-Eck Gauß 1796, 257-Eck Richelot 1832, 65 537-Eck Hermes 1889.

2) Welche n-Ecke sind konstruierbar, welche nicht?

$n =$	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
konstruierbar	✓	✓	✓	✓	–	✓	–	✓	–	✓	–	–	✓	✓	✓	–	–	✓

5.18 Hilfssatz: Für $n \in \mathbb{N}$ gilt

$$\cos(nx) \ = \ T_n\big(\cos(x)\big),$$

wobei $T_n \in \mathbb{Z}[x]$ mit $\deg(T_n) = n$ (**Tschebyscheff-Polynome**). Weiter gelten:

1) $T_{n+1}(x) = 2xT_n(x) - T_{n-1}(x)$.

2) Ist $T_n(x) = \sum_{k=0}^{n} a_k x^k$, so gelten

a) $a_n = 2^{n-1}$ und $\forall k \in \{1, \dots, n-1\} : 2^{k-1}$ teilt a_k.

b) n ungerade $\Rightarrow$ $a_0 = 0$,

c) $n = p$ Primzahl $\Rightarrow$ $\forall k \in \{1, \dots, n-1\} : p$ teilt a_k.

Beweis: **0)**
$$\begin{aligned} \cos(nx) + \mathrm{i}\sin(nx) &= \mathrm{e}^{\mathrm{i}nx} = (\mathrm{e}^{\mathrm{i}x})^n \\ &= \big(\cos(nx) + \mathrm{i}\sin(nx)\big)^n \\ &= \sum_{k=0}^{n} \binom{n}{k} \cos^{n-k}(x)\mathrm{i}^k \sin^k(x) \end{aligned}$$

Bilde Realteil:
$$\begin{aligned} \cos(nx) &= \sum_{k=0,\ k \text{ gerade}}^{n} \binom{n}{k} \cos^{n-k}(x)(-1)^{k/2}\sin^k(x) \\ &= \sum_{l=0}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{2l} \cos^{n-2l}(x)(-1)^l \sin^{2l}(x) \\ \Rightarrow\ T_n(y) &= \sum_{l=0}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{2l} y^{n-2l}(-1)^l(1-y^2)^l \end{aligned}$$

$\Rightarrow$ $T_n(x) \in \mathbb{Z}[x]$, $\deg(T) = n$.

1)
$$\begin{array}{lcll} \cos\big((n+1)x\big) & \overset{\text{Add. Theoreme}}{=} & \cos(x)\cos(nx) - \sin(x)\sin(nx) & = T_{n+1}\big(\cos(x)\big) \\ \cos\big((n-1)x\big) & = & \underbrace{\cos(-x)}_{=\cos(x)}\ \underbrace{\cos(nx)}_{=T_n(\cos(x))} - \underbrace{\sin(-x)}_{=-\sin(x)}\sin(nx) & = T_{n-1}\big(\cos(x)\big) \end{array}$$

$\Rightarrow$ $T_{n+1}\big(\cos(x)\big) + T_{n-1}\big(\cos(x)\big) = 2\cos(x)T_n\big(\cos(x)\big)$
$\overset{y:=\cos(x)}{\Rightarrow}$ $T_{n+1}(y) + T_{n-1}(y) = 2yT_n(y)$.

2) **a)** Induktionsanfang $T_1(x) = x$, $T_2(x) = 2x^2 - 1$
$\Rightarrow$ $a_n = 2^{n-2}$, a_k durch 2^{k-1} teilbar für $1 \le k \le n$
Induktionsschritt:

$$T_{n+1}(x) = 2x \underbrace{T_n(x)}_{\substack{a_n = 2^{n-1} \\ a_k \text{ durch } 2^{k-1} \text{ teilbar}}} - \underbrace{T_{n-1}(x)}_{\tilde{a}_k \text{ durch } 2^{k-1} \text{ teilbar}}$$

$\Rightarrow$ $T_{n+1} = 2^n x^{n+1} + \sum_{k=0}^{n} b_k x^k$, wobei b_k durch 2^{k-1} teilbar ist.

Induktionsschluss: Für alle T_n gilt $a_n = 2^{n-1}$ und a_k ist durch 2^{k-1} teilbar für $1 \le k \le n$.

b) n ungerade $\Rightarrow$ x^{n-2l} sind nur ungerade x-Potenzen
$(1-x^2)^l$ liefert nur gerade x-Potenzen
$\Rightarrow$ T_n enthält nur ungerade x-Potenzen, insbesondere $a_0 = 0$.

c) $n = p$ Primzahl $\Rightarrow$ $\binom{p}{k} = \frac{p(p-1)\cdots(p-k+1)}{k!}$ ist durch p teilbar.

□

5.19 Satz: Ist $n \in \mathbb{N} \setminus \{2^j : j \in \mathbb{N}_0\}$, so gibt es keine Konstruktion mit Zirkel und Lineal zur Teilung beliebiger Winkel in n gleiche Teile.

Beweis: **1)** Fall $n = p$ Primzahl. Zeige, dass es einen konstruierbaren Winkel φ gibt, so dass $\frac{\varphi}{p}$ nicht konstruierbar ist.

Sei $\cos(\varphi)$ konstruierbar. Zur Konstruktion von $\frac{\varphi}{p}$ muss $x_0 = \cos\left(\frac{\varphi}{n}\right)$ konstruiert werden, x_0 ist Lösung von

$$T_p(x_0) \;=\; \cos(\varphi).$$

Wähle φ so, dass $\cos(\varphi) = \frac{p}{2(p+1)}$. Offensichtlich ist φ konstruierbar. Dann ist x_0 Lösung der Gleichung

$$T_p(x) - \frac{p}{2(p+1)} \;=\; 0. \qquad (*)$$

Multiplikation mit $2(p+1)^p$ ergibt

$$2(p+1)^p T_p(x) - p(p+1)^{p-1} \;=\; 0.$$

Letzter Satz $\Rightarrow$ Jeder Koeffizient b_k von $2(p+1)^p T_p(x)$ ist durch $2^{k-1} \cdot p \cdot 2 \cdot (p+1)^p$ teilbar für $1 \le k \le p-1$, und es gilt $b_p = 2^p(p+1)^p$, $b_0 = 0$.

Substituiere $y := 2(p+1)x$

$$\Rightarrow \begin{cases} Q(y) := 2(p+1)^p T_p\Big(\dfrac{y}{2(p+1)}\Big) \text{ ist Polynom, } Q \in \mathbb{Z}[x] \\ Q \text{ ist normiert mit } b_0 = 0 \\ \forall k \in \{1, \ldots, p-1\} : b_k \text{ ist durch } p \text{ teilbar} \end{cases}$$

Wende Eisenstein auf $\tilde{Q}(y) := Q(y) - p(p+1)^{p-1}$ an $\Rightarrow$ $\tilde{Q}$ ist irreduzibel über $\mathbb{Q}$
$\Rightarrow$ $y_0 = 2(p+1)x_0$ ist algebraisch über $\mathbb{Q}$ vom Grad p, also auch x_0
$\overset{3.5}{\Rightarrow}$ x_0 ist nicht konstruierbar.

2) Allgemeiner Fall: Sei $n \in \mathbb{N} \setminus \{2^j : j \in \mathbb{N}_0\}$
Primfaktorzerlegung $n = 2^j p_1^{l_1} \cdots p_k^{l_k}$ mit $k \ge 1$, $l_1 \ge 1$

Annahme: n-Teilung konstruierbar $\overset{5.6}{\Rightarrow}$ p_1-Teilung konstruierbar $\quad \lightning$ (Fall 1).

□