Die Theorie der geometrischen Konstruktionen

Wolfgang Ströher

AKGEO Theorie der geometrischen Konstruktionen

Die Vorlesung behandelt das Problem, die Ausführbarkeit oder Nichtausführbarkeit einer vorgelegten geometrischen Konstruktion mit vorgeschriebenen Hilfsmitteln (Zeicheninstrumenten) zu untersuchen und die Leistungsfähigkeit der Zeichenhilfsmittel festzustellen.

Die Behandlung dieser Fragestellungern erfordert beträchtliche, oft tiefliegende, Kenntnisse aus Algebra und Zahlentheorie, die aber sämtlich in der Vorlesung hergeleitet werden, sodaß einschlägige Vorkenntnisse zum Besuch der Vorlesung nicht vorausgesetzt werden. Auch ist die Vorlesung völlig unabhängig vom Besuch der Vorlesung "AKGEO Praxis der geometrischen Konstruktionen".

Die Theorie der klassischen Konstruktionen
Polynome, die durch Quadratwurzelausdrücke lösbar sind
Polynome dritter Ordnung
Die GAUSSsche Zahlenebene
Die Kreisteilungsgleichung
Die klassischen regelmäßigen Vielecke
Hilfsmittel aus der Zahlentheorie
Die Theorie regelmäßiger Vielecke nach GAUSS
Das regelmäßige Siebzehneck
Gleichungen dritten Grades
Der „Casus irreducibilis"
Gleichungen vierten Grades
Gemeinsame Behandlung verschiedener Methoden zur Lösung biquadratischer Gleichungen
Die Transzendenz von e und π
Das Einschiebelineal
Die Dreiteilung des Winkels
Die Vervielfachung des Würfels
Einschiebungen nach BREIDENBACH
Konstruktion des regelmäßigen Sieben-, Neun- und Dreizehnecks
Behandlung der allgemeinen Gleichung 4.Ordnung nach BREIDENBACH

Theorie der geometrischen Konstruktionen

Vorbemerkungen

Geometrische Konstruktionen

Unter einer *geometrischen Konstruktion* versteht man die zeichnerische Darstellung eines geometrischen Objektes aus vorliegenden Angabestücken unter Einhaltung gegebener Bedingungen mit Hilfe vorgeschriebener Zeichengeräte

Ausführung geometrischer Konstruktionen

Die *Ausführung einer geometrischen Konstruktion* umfaßt folgende Punkte:

1. *Analyse* der Aufgabe (Aufsuchung der notwendigen Bedingungen für die Lösbarkeit
2. *Ausführung* der Konstruktion
3. Beweis der *Richtigkeit der Konstruktion*(Nachweis des Hinreichens der zu erfüllenden Bedingungen)
4. *Determination* (Anzahl der möglichen Lösungen und Sonderfälle)

Theorie geometrischer Konstruktionen

Unter der *Theorie geometrischer Konstruktionen* versteht man mehreres:

1. Angabe der *Lösungsmethoden*
2. Die Frage nach der Wirksamkeit und Reichweite der vorgeschriebenen Zeichengeräte
3. *Einteilung der Konstruktionsaufgaben* in Abhängigkeit von den Zeichengeräten (z.B. lineare, quadratische Aufgaben, Aufgaben höheren Grades, projektive und metrische Aufgaben)
4. Nachweis der eventuellen *Unmöglichkeit einer Lösung* von Aufgaben mit Hilfe der zulässigen Zeicheninstrumente
5. Untersuchung der Genauigkeit und Einfachheit einer Konstruktion (Geometrographie)

Wir beschäftigen uns hauptsächlich mit den Punkten 2, 3 und 4

Klassische Konstruktionen

Unter einer *klassischen Konstruktion* versteht man eine Konstruktion, bei der nur *Zirkel und Lineal* als Zeicheninstrumente zugelassen sind. Zirkel und Lineal dürfen *ausschließlich* auf folgende Weise verwendet werden:

1. Vorgabe beliebiger Punkte, Geraden und Kreisen als Angabe

2.a. Anlegen des Lineals an zwei gegebene oder bereits konstruierte Punkte, um deren Verbindungsgerade zu ziehen.

b. Zeichnen einer beliebigen (Hilfs-) Geraden

3.a. Einsetzen der beiden Zirkelspitzen in zwei gegebene oder bereits konstruierte Punkte

b. Zeichnen eines Kreises um einen gegebenen oder bereits konstruierten Punkt als Mittelpunkt mit dem durch zwei schon vorhandene Punkte bestimmten Radius

c. Zeichnen eines beliebigen (Hilfs-) Kreises mit beliebigem Mittelpunkt und Radius

4. Erzeugung neuer Punkte durch Schnitt von Geraden und Kreisen, die gemäß 2. und 3. gewonnen wurden.

5. Geraden und Kreise treten nur in *endlicher Anzahl* auf

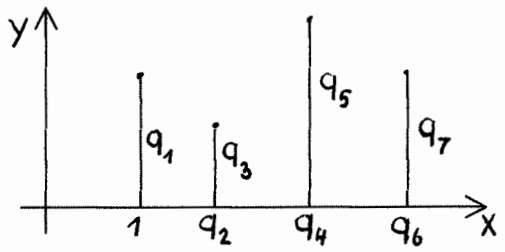
6. Vorgabe von gemäß 1.-5. konstruierten Punkten, Geraden und Kreisen als neue Angaben

Die Theorie der klassischen Konstruktionen

Grund- und Erweiterungskörper

Um wenigstens die notwendigen Bedingungen dafür aufzustellen, ob eine vorgelegte Konstruktion im klassischen Sinne zu bewältigen ist, bedienen wir uns der analytischen Geometrie, indem wir die Ebene in ein kartesisches Bezugssystem einbetten.

Da sich alle zulässigen Angabestücke durch Punkte festlegen lassen (Gerade durch zwei Punkte, Kreis durch Mittelpunkt und Punkt der Peripherie usw.) können wir alle Angaben durch Punkte definieren, deren Koordinaten als reelle Zahlen vorausgesetzt werden



Eine der gegeben Koordinaten können wir o.B.d.A. als Einheitsstrecke wählen.

Den Konstruktionen mit dem Lineal allein (Verbindung zweier Punkte, Schnitt zweier Geraden) entsprechen Operationen, die durch lineare Gleichungen beschrieben werden können, die sich durch rationale Ausdrücke lösen lassen.

Die Anwendung rationaler Operationen auf das Element 1 liefert den Körper $\mathbb{Q}$ der rationalen Zahlen, die Hinzufügung der anderen (endlich vielen) Angabekoordinaten $q_1, q_2, \ldots, q_r$ den Körper $\mathbb{K}_0$, der durch *Adjunktion* dieser Größen zu $\mathbb{Q}$ entsteht. Den durch die Angabewerte betimmten Körper $\mathbb{K}_0$ bezeichnen wir als *Grundkörper*.

$\mathbb{K}_0$ ist ein *Erweiterungskörper* von $\mathbb{Q}$ und ein *Unterkörper* des Körpers $\mathbb{R}$ der reellen Zahlen:

$$\mathbb{K}_0 := \mathbb{Q}[q_1, q_2, \ldots, q_r] \subset \mathbb{R}$$

Das allgemeine Element a von $\mathbb{K}_0$ hat daher die Bauart

$$a = \frac{p_1(q_1, q_2, \ldots, q_r)}{p_2(q_1, q_2, \ldots, q_r)}$$

worin $p_1(q_1, q_2, \ldots, q_r)$, $p_2(q_1, q_2, \ldots, q_r)$ Polynome in $q_1, \ldots, q_r$ mit Koeffizienten aus $\mathbb{Q}$ sind.

1. Alle rationalen Operationen in lassen sich durch klassische Operationen mit Zirkel und Lineal ausführen. Seien $a,b \in \mathbb{K}_0$, dann gilt:

Addition: $x = a + b$

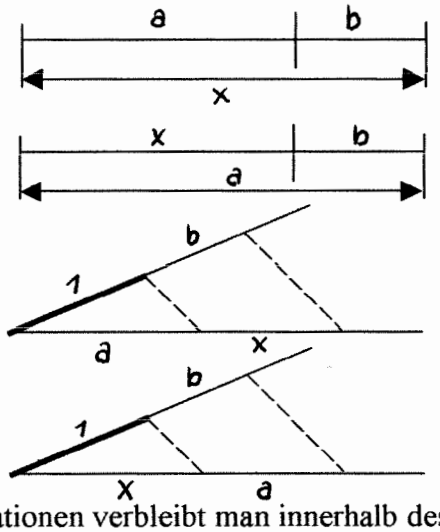
Subtraktion: $x = a - b$

Multiplikation: $x = a.b$

$a : 1 = x : b \ \ldots \ x = a.b$

Division: $x = a/b$

$x : 1 = a : b \quad x = a/b$

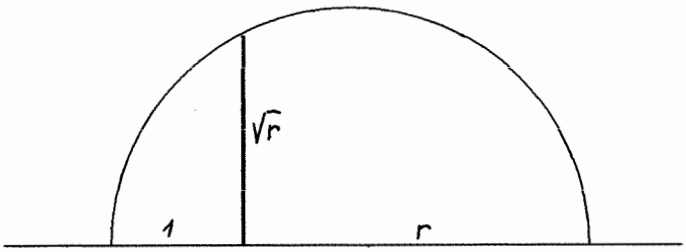


Durch Ausübung rationaler Operationen verbleibt man innerhalb des Grundkörpers $\mathbb{K}_0$

.2. Schnitte von Kreisen und Geraden sowie von Kreisen mit Kreisen führen auf quadratische Gleichungen mit Koeffizienten aus dem Grundkörper $\mathbb{K}_0$. Die Lösung einer quadratischen Gleichung hat die Gestalt

$$a + b.\sqrt{r} \qquad \text{mit } a,b,r \in \mathbb{K}_0$$

Die Wurzel $\sqrt{r}$ läßt sich nach dem Höhensatz für das rechtwinkelige Dreieck mit Zirkel und Lineal konstruieren:



Gehört $\sqrt{r}$ nicht dem Körper $\mathbb{K}_0$ an, so bilden wir einen *Erweiterungskörper* $\mathbb{K}_1$ von $\mathbb{K}_0$, indem wir $\sqrt{r}$ dem Körper $\mathbb{K}_0$ *adjungieren*:

$$\mathbb{K}_1 = \mathbb{K}_0[\sqrt{r}]$$

Sind $a,b,c,d,r \in \mathbb{K}_0$ so gilt

$$\left(a+b.\sqrt{r}\right)\pm\left(c+d.\sqrt{r}\right)=(a\pm c)+(b\pm d)\sqrt{r}$$

$$\left(a+b.\sqrt{r}\right).\left(c+d.\sqrt{r}\right)=(ac+bdr)+(ad+bc)\sqrt{r}$$

$$\frac{a+b.\sqrt{r}}{c+d.\sqrt{r}}=\frac{\left(a+b.\sqrt{r}\right).\left(c-d.\sqrt{r}\right)}{\left(c+d.\sqrt{r}\right).\left(c-d.\sqrt{r}\right)}=\frac{(ac-bdr)+(bc-ad)\sqrt{r}}{c^2-d^2.r}$$

Daher hat jedes Element von $\mathbb{K}_1$ die Gestalt

$$A + B.\sqrt{r} \quad \text{mit } A,B,r \in \mathbb{K}_0$$

Beispiel: $\mathbb{K}_0 = \mathbb{Q}$, $A = 3$, $B = 2$, $r = 5$

$$3 - 2.\sqrt{5} \in \mathbb{K}_1 = \mathbb{K}_0[\sqrt{5}]$$

3. Adjungiert man zu $\mathbb{K}_1$ die Quadratwurzel aus irgend einem Element $\rho \in \mathbb{K}_1$, etwa $\sqrt{A+B.\sqrt{r}} = \sqrt{\rho}$, so führt die Ausübung der rationalen Operationen zum *Erweiterungskörper*

$$\mathbb{K}_2 = \mathbb{K}_1[\sqrt{\rho}] \qquad \rho \in \mathbb{K}_1$$

dessen Elemente die Gestalt

$$\alpha + \beta.\sqrt{\rho} \qquad \alpha,\beta,\rho \in \mathbb{K}_1$$

haben

Beispiel(*):

$$1+2.\sqrt{5},\ 4-3.\sqrt{5},\ 7+6.\sqrt{5} \in \mathbb{K}_1$$

$$\left(1+2.\sqrt{5}\right)+\left(4-3.\sqrt{5}\right).\sqrt{7+6.\sqrt{5}} \in \mathbb{K}_2$$

4. Wenn man in dieser Weise fortfährt, erhält man einen Körper $\mathbb{K}_\mu$, dessen allgemeines Element die Bauart hat:

$$A + B.\sqrt{R} \quad \text{mit } A,B,R \in \mathbb{K}_{\mu-1}$$

Dabei stellt μ die Anzahl der übereinander geschachtelten Quadratwurzeln dar (*Ordnung* des Wurzelausdruckes)

2*. Man kann die Bildung des Körpers $\mathbb{K}_1$ verallgemeinern, indem man dem Körper $\mathbb{K}_0$ nicht nur eine, sondern mehrere Wurzeln adjungiert. Adjungiert man etwa $\sqrt{r}$ und $\sqrt{s}$, so hat das allgemeine Element von $\mathbb{K}_1$ die Gestalt

$$a + b.\sqrt{r} + c.\sqrt{s} + d.\sqrt{r}.\sqrt{s}$$

Hier darf man $\sqrt{r}.\sqrt{s}$ nicht etwa zu $\sqrt{(rs)}$ zusammenfassen, das sonst der Eindruck entstünde, man hätte drei Wurzeln adjungiert.

Ist m die Anzahl der voneinander unabhängigen Wurzeln, so gilt für Beispiel (*)

$$\mu = 2,\ m = 2$$

4*. Auch die Bildung von $\mathbb{K}_\mu$ kann verallgemeinert werden, indem man die Quadratwurzeln von m Elementen aus $\mathbb{K}_{\mu-1}$ adjungiert.

> Alle Ausdrücke, die dem Körper $\mathbb{K}_\mu$ angehören, lassen sich mit Zirkel und Lineal konstruieren.
>
> Umgekehrt führt jede mit Zirkel und Lineal ausführbare Konstruktion auf einen Ausdruck von $\mathbb{K}_\mu$.

Die Ausdrücke von $\mathbb{K}_1$ ergeben sich als Nullstellen von quadratischen Polynomen mit Koeffizienten aus $\mathbb{K}_0$.

Wir werden zeigen, daß sich die Elemente von $\mathbb{K}_\mu$ als Nullstellen eines gewissen Polynoms mit Koeffizienten aus $\mathbb{K}_0$ darstellen lassen.

Notwendigerweise ist eine Konstruktionsaufgabe genau dann mit Zirkel und Lineal lösbar, wenn sich ein Polynom der beschriebenen Art angeben läßt

Polynome

Polynomringe

Die Menge der Polynome in der Unbestimmten x über einem Körper $\mathbb{K}$ bildet den *Polynomring* $\mathbb{K}[x]$. Sei $f(x) \in \mathbb{K}[x]$, dann ist

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \quad (a_i \in \mathbb{K},\ a_n \neq 0)$$

ein *Polynom n-ten Grades*. Die Elemente $a \in \mathbb{K}$ bezeichnet man als *Polynome nullten Grades* (*konstante Polynome*), Dem *Nullpolynom* $f(x) \equiv 0$ schreiben wir *keinen Grad* zu. Ein Polynom halt also einen Grad ≥ 0 oder es ist das Nullpolynom.

Der EUKLIDische Algorithmus (Divisionsalgorithmus)[1]

Es seien $f(x)$ und $g(x)$ zwei Polynome aus $\mathbb{K}[x]$. Dann gilt

$f = g.q_0 + r_1$ $\qquad$ $grd\ r_1 < grd\ g$

$g = r_1.q_1 + r_2$ $\qquad$ $grd\ r_2 < grd\ r_1$

$r_1 = r_2.q_2 + r_3$ $\qquad$ $grd\ r_3 < grd\ r_2$

$\vdots$

$r_{k-2} = r_{k-1}.q_{k-1} + r_k$ $\qquad$ $grd\ r_k < grd\ r_{k-1}$

$r_{k-1} = r_k.q_k$

Setzt man $t := r_k$ und verfolgt man den Algorithmus von unten nach oben, so findet man

$$\uparrow\ t|r_{k-1} \Rightarrow t|r_{k-2} \Rightarrow \ldots \Rightarrow t|g \Rightarrow t|f$$

Das Polynom t ist also Teiler sowohl von f als auch von g

Ist umgekehrt das Polynom s ein Teiler sowohl von f als auch von g, so folgt bei Durchlaufung des Algorithmus von oben nach unten

$$\downarrow\ s|f \wedge s|g \Rightarrow s|r_1 \Rightarrow s|r_2 \Rightarrow \ldots \Rightarrow s|r_k = t$$

Das Polynom t ist also größter gemeinsamer Teiler von f und g [$ggT(f,g)$]

Ist $0 \neq t \in \mathbb{K}$ (also ein Polynom nullten Grades), so heißen f und g *teilerfremd*

Ist $t = ggT(f,g)$, so ist auch $\lambda.t$ ein ggT. Der ggT von Polynomen ist also nur bis auf einen skalaren Faktor bestimmt. Daher setzt man bei teilerfremden Polynomen $t := 1$.

> Ist $t = ggT(f,g)$, so gibt es Polynome p und q, sodaß gilt **(1)**
> $$t = p.f + q.g$$

BW: $\downarrow$ Elimination von $r_1, r_2, \ldots$ Es ergeben sich stets Linearkombinationen von f und g, deren letzte $t = r_k$ ist.

> f und g sind genau dann teilerfremd, wenn es Polynome p, q gibt, sodaß gilt **(2)**
> $$p.f + q.g = 1$$

BW: 1. f, g seien teilerfremd, Dann gilt nach (1)

$$p.f + q.g = 1 \in \mathbb{K}$$

2. Es gelte (2), f und g seien aber nicht teilerfremd, d.h.es gibt ein nichtkonstantes Polynom s mit

$$f = s.f_1, \quad g = s.g_1$$

Dann gilt wegen (2)

$$s(f_1.p + g_1.q) = 1$$

d.h. 1 wäre durch das nichtkonstante Polynom s teilbar Widerspruch!!

---

[1] EUKLID (ca. 300 v.Chr.) Elemente Buch VII, Satz 2

Obige Sätze gelten speziell für den Polynomring $\mathbb{Q}[x]$ und ebenso für den Ring $\mathbb{Z}$der ganzen Zahlen (Teilungsregeln)

Das Schema von RUFFINI - HORNER[1]

Es sei

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$$

ein Polynom über einem Körper $\mathbb{K}$. Der Wert $f(\lambda)$ des Polynoms an der Stelle $\lambda \in \mathbb{K}$ läßt sich vorteilhaft mit Hilfe des Schemas von RUFFINI - HORNER ermitteln:

	a_n	a_{n-1}	...	a_{i+1}	a_i	...	a_1	a_0
λ	*	$\lambda\, b_{n-1}$	...	$\lambda\, b_{i+1}$	$\lambda\, b_i$	...	$\lambda\, b_1$	λb_0
	b_{n-1}	b_{n-2}	...	b_i	b_{i-1}	...	b_0	$f(\lambda)$

1. Hier ist
   $b_{n-1} = a_n$
   $b_{n-2} = \lambda a_n + a_{n-1}$
   $b_{n-3} = \lambda^2 a_n + \lambda\, a_{n-1} + a_{n-2}$
   ...
   $b_0 = \lambda^{n-1}a_n + \lambda^{n-2}a_{n-1} + \lambda^{n-3}a_{n-2} + \ldots + \lambda\, a_2 + a_1$
   $f(\lambda) = \lambda^n a_n + \lambda^{n-1}a_{n-1} + \lambda^{n-2}a_{n-2} + \ldots + \lambda^2 a_2 + \lambda a_1 + a_0$
2. Wir definieren folgendes Polynom:
   $f_1(x) = b_{n-1}x^{n-1} + b_{n-2}x^{n-2} + \ldots + b_1 x + b_0$
   Dann gilt
   $$f(x) = f_1(x).(x - \lambda) + f(\lambda) \qquad (\bullet)$$
   d.h. $f_1(x)$ ist der Quotient, der sich bei Division von $f(x)$ durch $(x- \lambda)$ ergibt. Der Rest $f(\lambda)$ ist der Funktionswert von $f(x)$ an der Stelle λ.

   BW: $f_1(x).(x - \lambda) = (b_{n-1}x^{n-1} + b_{n-2}x^{n-2} + \ldots + b_1 x + b_0)(x- \lambda) =$
   $= b_{n-1}x^n + b_{n-2}x^{n-1} + b_{n-3}x^{n-2} + \ldots + b_1 x^2 + b_0 x -$
   $- b_{n-1}x^{n-1}\lambda - b_{n-2}x^{n-2}\lambda - \ldots - b_2 x^2 \lambda - b_1 x \lambda - b_0 \lambda =$
   $= b_{n-1}x^n + (b_{n-2} - b_{n-1}\lambda)x^{n-1} + (b_{n-3} - b_{n-2}\lambda)x^{n-2} + \ldots + (b_0 - b_1\lambda)x - b_0\lambda =$
   $= a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x - (f(\lambda) - a_0)$
   daher $f(x) = f_1(x).(x - \lambda) + f(\lambda)$

Verallgemeinerung des Schemas von RUFFINI - HORNER

Gegeben seien die beiden Polynome

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \text{ und } p(x) = x^2 - \lambda x - \mu$$

Die Division des Poynoms n-ten Grades $f(x)$ durch das Polxnom 2.Grades $p(x)$ ergibt als Quotienten ein Polynom (n-2)-ten Grades $f_1(x)$ und als Rest ein Polynom 1.Grades (welches sich auf eine Konstante oder das Nullpolynom reduzieren kann). Das Schema von RUFFINI-HORNER nimmt dann folgende Gestalt an

	a_n	a_{n-1}	a_{n-2}	a_{n-3}	...	a_3	a_2	a_1	a_0
λ	*	λb_{n-2}	λb_{n-3}	λb_{n-4}	...	λb_2	λb_1	λb_o	*
μ	*	*	μb_{n-2}	μb_{n-3}	...	μb_3	μb_2	μb_1	μb_0
	b_{n-2}	b_{n-3}	b_{n-4}	b_{n-5}	...	b_1	b_0	c_1	c_2

und es gilt
$b_{n-2} = a_n$
$b_{n-3} = a_{n-1} + \lambda\, b_{n-2}$
$b_{n-4} = a_{n-2} + \lambda\, b_{n-3} + \mu b_{n-2}$
$b_{n-5} = a_{n-3} + \lambda\, b_{n-4} + \mu b_{n-3}$
...

[1] Paolo RUFFINI (1765-1822) 1804, William HORNER (1786 -1837) 1819, das Verfahren findet sich bereits 1303 bei CHU SHIH-CHIEH (ca. 1270-ca.1330)

$b_2 = a_4 + \lambda\, b_3 + \mu b_4$
$b_1 = a_3 + \lambda\, b_2 + \mu b_3$
$b_0 = a_2 + \lambda\, b_1 + \mu b_1$
$c_1 = a_1 + \lambda\, b_0 + \mu b_1$
$c_0 = a_0 \quad + \mu b_0$

Das Ergebnis der Division lautet

$$f(x) = f_1(x).\, p(x) + r(x)$$

mit

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$$
$$p(x) = x^2 - \lambda x - \mu x$$
$$f_1(x) = b^{n-2}x^{n-2} + b_{n-3}x^{n-3} + \ldots + b_1 x + b_0$$
$$r(x) = c_1 x + c_0$$

Man beachte, daß das Quotientenpolynom $p(x)$ zur Anwendung des obigen Schemas normiert sein muß.
Die Verallgemeinerung bei Division durch Polynome beliebiger Ordnung liegt auf der Hand.

Entwicklung des Polynoms $f(x)$ als Potenzen von $y = x - \lambda$

Wendet man die Entwicklung (•) auch auf das Polynom $f_1(x)$ usw. an, so ergibt sich die Folge

$f(x) = f_1(x).(x - \lambda) + f(\lambda)$	
$f_1(x) = f_2(x).(x - \lambda) + f_1(\lambda)$	$(x - \lambda)$
$f_2(x) = f_3(x).(x - \lambda) + f_2(\lambda)$	$(x - \lambda)^2$
...	...
$f_{n-2}(x) = f_{n-1}(x).(x - \lambda) + f_{n-2}(\lambda)$	$(x - \lambda)^{n-2}$
$f_{n-1}(x) = a_n.(x - \lambda) + f_{n-1}(\lambda)$	$(x - \lambda)^{n-1}$

Multipliziert man jede Zeile mit dem angeführten Faktor und addiert alle Zeilen, so folgt

$$f(x) = f(\lambda) + f_1(\lambda)(x - \lambda) + f_2(\lambda)(x - \lambda)^2 + \ldots + f_{n-1}(\lambda)(x - \lambda)^{n-1} + a_n.(x - \lambda)^n$$

Setzt man

$$y := x - \lambda$$

so ergibt sich

$$f(x) = a_n y^n + f_{n-1}(\lambda).y^{n-1} + \ldots + f_1(\lambda).y + f(\lambda) =: g(y)$$

Irreduzible Polynome

Gilt für ein Polynom über dem Körper $\mathbb{K}$

$$a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 =$$
$$= (b^r x_r + b^{r-1}x_{r-1} + \ldots + b_1 x + b_0).(c_s x^s + c_{s-1}x^{s-1} + \ldots + c_1 x + c_0)$$
$$a_i, b_j, c_k \in \mathbb{K},\ r + s = n,\ r < n,\ s < n$$

so heißt das Polynom *reduzibel über* $\mathbb{K}$. Andernfalls heißt es *irreduzibel*

Da die Definition der Irreduzibilität fordert, daß jeder der beiden Faktoren einen echt kleineren Grad als das ursprüngliche Polynom hat, sind lineare Polynome und Polynome nullten Grades (Konstanten) stets irreduzibel.

Die Reduzibilität eines Polynoms hängt wesentlich vom Koeffizientenkörper $\mathbb{K}$ ab.

Beispiele:

$10x^2 - x - 21 = (2x - 3).(5x + 7)$ ... reduzibel über $\mathbb{Q}$

$25x^2 - 20x - 14 = [5x - (2 + 3\sqrt{2})].[5x - (2 - 3\sqrt{2})]$ ... irreduzibel über $\mathbb{Q}$, aber reduzibel über $\mathbb{Q}[\sqrt{2}]$

$f(x)$ und $g(x)$ seien Polynome über $\mathbb{K}$. Das Element λ eines Erweiterungskörpers $\mathbb{E}$ von $\mathbb{K}$ ist genau dann eine gemeinsame *Nullstelle* von $f(x)$ und $g(x)$, wenn λ Nullstelle des größten gemeinsamen Teilers $t(x)$ der Polynome $f(x)$ und $g(x)$ ist. Speziell gilt der Satz für gemeinsame Nullstellen über $\mathbb{K}$.

1. Es sei $\lambda \in \mathbb{E}$ und es gelte $f(\lambda) = 0$ und $g(\lambda) = 0$. Ferner sei $ggT(f,g) = t$
$(\exists p,q)\, t = p.f + q.g \Rightarrow t(\lambda) = p(\lambda) f(\lambda) + q(\lambda).g(\lambda) = 0$

2. Es sei $t(\lambda) = 0$. Dann gilt
$f(x) = t(x).f_1(x) \Rightarrow f(\lambda) = t(\lambda).f_1(\lambda) = 0$
$g(x) = t(x).g_1(x) \Rightarrow g(\lambda) = t(\lambda).g_1(\lambda) = 0$

Fundamentalsatz über irreduzible Polynome

> Es sei $f(x)$ ein irreduzibles und $g(x)$ ein beliebiges Polynom über $\mathbb{K}$. Haben $f(x)$ und $g(x)$ in einem Erweiterungkörper $\mathbb{E}$ von $\mathbb{K}$ eine gemeinsame Nullstelle λ, so ist $f(x)$ eine Teiler von $g(x)$

BW: Nach dem voranstehenden Satz müssen $f(x)$ und $g(x)$ einen größten gemeinsamen Teiler $t(x)$ mit der Nullstelle $\lambda \in \mathbb{E}$ haben. Da aber $f(x)$ irreduzibel ist, muß $t(x)$ (bis auf einen Faktor aus $\mathbb{K}$) mit $f(x)$ übereinstimmen.

Ist $\lambda \in \mathbb{K}$, so gilt bei Anwendung des Divisionsalgorithmus auf $f(x)$ und $g(x) := x - \lambda$

$$f(x) = (x - \lambda).q_0(x) + r_1(x)$$

Da $g(x)$ vom Grade 1 ist, muß $r_1(x)$ von Grade 0, also eine Konstante $r_1 \in \mathbb{K}$ sein. Daher gilt für den Wert von $f(x)$ an der Stelle λ

$$f(\lambda) = r_1$$

Ist λ eine Nullstelle von $f(x)$, so gilt

$$f(\lambda) = (\lambda - \lambda).q_0(\lambda) + r_1 \Rightarrow r_1 = f(\lambda) = 0$$

> Ist $\lambda \in \mathbb{K}$, so gilt
> $$f(x) = f_1(x).(x - \lambda) + f(\lambda)$$
> Ist $\lambda \in \mathbb{K}$ eine Nullstelle von $f(x)$, so wird $f(x)$ durch $(x-\lambda)$ geteilt

Rationale Nullstellen eines Polynoms über $\mathbb{Q}$

Es sei

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \qquad a_i \in \mathbb{Q},\ a_n \neq 0$$

ein Polynom über $\mathbb{Q}$. Ist $a_n = 1$, so heißt das Polynom *normiert*. Zur Berechnung der Nullstellen von $f(x) = 0$ kann man o.B.d.A. voraussetzen, daß alle a_i ganzzahlig sind, indem man $f(x)$ mit dem Generalnenner aller Koeffizienten multipliziert.

Den Bruch

$$\frac{\lambda}{\mu} \in \mathbb{Q} \text{ mit } \lambda, \mu \in \mathbb{Z} \text{ und } ggt(\lambda, \mu) = 1$$

nennen wir gleichfalls *normiert*.

> Ist der normierte Bruch $\frac{\lambda}{\mu}$ eine rationale Nullstelle des Polynoms
> $$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$$
> mit ganzzahligen Koeffizienten, so ist λ ein Teiler von a_0 und μ ein Teiler von a_n

BW:

$$a_n\left(\frac{\lambda}{\mu}\right)^n + a_{n-1}\left(\frac{\lambda}{\mu}\right)^{n-1} + \ldots + a_1\left(\frac{\lambda}{\mu}\right) + a_0 = 0 \Rightarrow$$

$$\Rightarrow a_n\lambda^n + a_{n-1}\lambda^{n-1}\mu + \ldots + a_1\lambda\mu^{n-1} + a_0\mu^n \Rightarrow$$

$$\Rightarrow \left\{\begin{array}{l} a_n\lambda^n = -\mu.\left[a_{n-1}\lambda^{n-1} + \ldots + a_1\lambda\mu^{n-2} + a_0\mu^{n-1}\right] \\ a_0\mu^n = -\lambda.\left[a_n\lambda^{n-1} + \ldots + a_1\mu^{n-1}\right] \end{array}\right\}$$

Da die rechte Seite der vorletzten bzw. letzten Zeile durch μ bzw. λ teilbar ist, muß es auch die linke Seite sein. Da λ, μ teilerfremd sind, sind es auch ihre n-ten Potenzen. Daraus folgt, daß a_n durch μ und a_0 durch λ teilbar sein muß. Daraus ergibt sich weiter

> Das normierte Polynom
> $$f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0$$
> mit ganzzahligen Koeffizienten besitzt als rationale Nullstellen nur ganze Zahlen, die Teiler von a_0 sein müssen

Ist nämlich der normierte Bruch λ/μ eine Nullstelle von $f(x)$, so müßte $\mu|1$ gelten, d.h. $\mu = \pm 1$

> Ist der normierte Bruch $\frac{\lambda}{\mu}$ eine rationale Nullstelle des Polynoms
> $$f(x) = a_nx^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0$$
> mit ganzzahligen Koeffizienten, so ist für jede ganze Zahl $(\lambda - \rho\mu) \neq 0$ $(\rho \in \mathbb{Z})$, der Wert $f(\rho)$ durch $(\lambda-\rho\mu)$ teilbar (notwendige Bedingung dafür daß $\frac{\lambda}{\mu}$ Nullstelle ist).

Obige Regel wurde von Jacob van WAESSENAER (Schüler von DESCARTES) erstmalig für $a_n = 1$, d.h. $\mu = 1$ angegeben

BW: Zunächst bilden wir mit beliebigem $\mu \neq 0$ $(\mu \in \mathbb{Z})$ den Ausdruck

$$\mu^n f(x) = a_n(\mu x)^n + \mu a_{n-1}(\mu x)^{n-1} + \ldots + \mu^{n-1}a_1(\mu x) + \mu^n a_0$$

Substituieren wir

$$y := \mu x$$

so erhalten wir

$$\mu^n f(x) = a_n y^n + \mu a_{n-1}y^{n-1} + \ldots + \mu^{n-1}a_1 y + \mu^n a_0 =: \Phi(y)$$

Ist $x = \frac{\lambda}{\mu}$ eine Nullstelle von $f(x)$, dann ist $y = \mu x = \mu.\frac{\lambda}{\mu} = \lambda$ eine Nullstelle von $\Phi(y)$.

Daher ist $\Phi(y)$ durch $(y - \lambda)$ teilbar, d.h.es gilt

$$\Phi(y) = \Phi_1(y).(y - \lambda) \qquad (\bullet)$$

worin sowohl $\Phi(y)$ als $\Phi_1(y)$ Polynome mit ganzzahligen Koeffizienten sind.
Wählen wir $0 \neq \rho \in \mathbb{Z}$ beliebig, aber $(\lambda-\rho\mu) \neq 0$. Setzen wir nun

$$y := \rho\mu = \mu x \Rightarrow x = \rho$$

so folgt wegen $(\bullet)$

$$\Phi(\rho\mu) = \Phi_1(\rho\mu).(\rho\mu - \lambda) = \mu^n f(\rho) \Rightarrow \frac{\Phi(\rho\mu)}{\lambda - \rho\mu} = \frac{\mu^n f(\rho)}{\lambda - \rho\mu} = -\Phi_1(\rho\mu) \in \mathbb{Z}$$

Da $\Phi_1(y)$ ganzzahlige Koeffizienten hat, ist auch $-\Phi_1(y)$ eine ganze Zahl, d.h.
$\mu^n.f(\rho)$ ist durch $(\lambda-\rho\mu)$ teilbar

BH: μ und $\lambda - \rho\mu$ sind teilerfremd

BW indirekt: Es sei $\lambda - \rho\mu = \lambda_1\sigma$, $\mu = \mu_1\sigma$ mit $0 < \mu_1 < \mu$. Dann wäre

$$\frac{\lambda-\rho\mu}{\mu} = \frac{\lambda_1\sigma}{\mu_1\sigma} = \frac{\lambda_1}{\mu_1} = \frac{\lambda}{\mu} - \rho \Rightarrow \frac{\lambda}{\mu} = \frac{\lambda_1+\rho\mu_1}{\mu_1}$$

Wegen $\mu_1 < \mu$ ließe sich $\frac{\lambda}{\mu}$ entgegen der Voraussetzung kürzen. Daher sind μ, $\lambda - \rho\mu$ teilerfremd, daher auch μ^n und $\lambda - \mu\rho$. Daher muß sich die ganze Zahl $f(\rho)$ durch $\lambda - \mu\rho$ teilen lassen.

Anwendung der Methode von WAESSENAER

Beispiel: Gesucht werden die rationalen Nullstellen des Polynoms

$$f(x) = 6x^3 + 7x^2 + 26x - 30$$

Man erkennt, daß es keine ganzzahligen Nullstellen gibt. Sei $x = \frac{\lambda}{\mu}$ (λ, μ teilerfremd) eine rationale Nullstelle:

λ muß Teiler von $|a_0| = 30$ sein, μ muß Teiler von $|a_3| = 6$ sein. Dann gibt es folgende Möglichkeiten:

$\lambda = \pm1, \pm2, \pm3, \pm5, \pm6, \pm10, \pm15, \pm 30$, $\mu = 1,2,3,6$

λ	μ	x	μ	x	μ	x	μ	x
1	1	1	2	1/2	3	1/3	6	1/6
-1	1	-1	2	-1/2	3	-1/3	6	-1/6
2	1	2	2	-	3	2/3	6	-
-2	1	-2	2	-	3	-2/3	6	-
3	1	3	2	3/2	3	-	6	-
-3	1	-3	2	-3/2	3	-	6	-
5	1	5	2	5/2	3	5/3	6	5/6
-5	1	-5	2	-5/2	3	-5/3	6	-5/6
6	1	6	2	-	3	-	6	-
-6	1	-6	2	-	3	-	6	-
10	1	10	2	-	3	10/3	6	-
-10	1	-10	2	-	3	-10/3	6	-
15	1	15	2	15/2	3	-	6	-
-15	1	-15	2	-15/2	3	-	6	-
30	1	30	2	-	3	-	6	-
-30	1	-30	2	-	3	-	6	-

Man müßte nun alle oben angeführten Möglichkeiten für $x = \frac{\lambda}{\mu}$ durchprobieren. Eine wesentliche Vereinfachung tritt ein, wenn man beachtet, daß λ, μ notwendigerweise nur dann zu einer Nullstelle gehören, wenn für eine beliebige ganze Zahl ρ mit $\lambda - \rho\mu \neq$ gilt

$$\lambda - \rho\mu \text{ teilt } f(\rho)$$

Wir wählen daher ρ so, daß $f(\rho)$ möglichst eine Primzahl wird oder wenigstens möglichst wenige Primfaktoren enthält.

Wir wählren $\rho = \pm 1, \pm 2$. Dann wird

$$f(1) = 9 = 3.3,\ f(-1) = -55 = -5.11,\ f(2) = 98 = 2.7.7,\ f(-2) = -102 = -2.3.17$$

λ	μ	$f(1) = 3.3$ λ -μ	$f(-1) = -5.11$ λ + μ	$f(2) = 2.7.7$ λ - 2μ	$f(-2) = -2.3.17$ λ + 2μ
1	2	**-1**	3	- 3	5
-1	2	**- 3**	**1**	- 5	**3**
2	1	**1**	3	0	4
2	3	**- 1**	**5**	- 4	10
-2	1	**- 3**	**-1**	- 4	0
3	2	**1**	**5**	**- 1**	7
5	2	**3**	7	**1**	9
5	6	**- 1**	**11**	**-7**	**17**
10	1	**9**	**11**	8	12

Man erkennt, daß höchstens x = 5/6 eine Nullstelle sein kann, was durch Einsetzen in die Gleichung $f(x)$ bestätigt wird.

Zwei Lemmata von GAUSS[1]

Definition: Ein Polynom mit ganzzahligen Koeffizienten heißt *primitiv*, wenn der größte gemeinsame Teiler aller Koeffizienten 1 ist.

1.Lemma von GAUSS: Das Produkt primitiver Polynome ist wieder ein primitives Polynom

BW: Es seien

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$$
$$g(x) = b_m x^m + b_{m-1}x^{m-1} + \ldots + b_1 x + b_0$$

primitive Polynome. Wir bilden das Produkt

$$f(x).g(x) := h(x) = c_{m+n}x^{m+n} + \ldots + c_1 x + c_0$$

Hier ist

$$c_0 = a_0 b_0$$
$$c_1 = a_0 b_1 + a_1 b_0$$
$$c_2 = a_0 b_2 + a_1 b_1 + a_0 b_2$$
$$\vdots$$
$$c_{i+j} = a_0 b_{i+j} + a_1 b_{i+j-1} + \ldots + a_{i-1} b_{j+1} + a_i b_j + a_{i+1} b_{j-1} + \ldots + a_{i+j} b_0$$
$$\vdots$$
$$c_{n+m} = a_n b_m$$

Wir nehmen an, daß das Produkt $h(x) = f(x).g(x)$ nicht primitiv sei, d.h. die c_i haben einen gemeinsamen $ggT(c_0, \ldots, c_{m+n}) = d \neq 1$. Ferner sei p eine in d enthaltene Primzahl. Da $f(x)$ und $g(x)$ beide primitiv sind, kann p nicht alle a_i bzw b_j teilen. Es sei also (beginnend mit a_0) a_i der erste Koeffizient von $f(x)$, und (beginnend mit b_0) b_j der erste Koeffizient von $g(x)$, der nicht durch p teilbar sei. Dann betrachten wir den Koeffizienten c_{i+j}. Alle seine Summanden, mit Ausnahme vom $a_i b_j$, sind durch p teilbar. Daher ist c_{i+j} nicht durch p teilbar, was der Annahme widerspricht.

2.Lemma von GAUSS: Jedes Polynom mit ganzzahligen Koeffizienten, das über $\mathbb{Q}$ reduzibel ist, läßt sich auch als Produkt von Polynomen niedrigeren Grades mit ganzzahligen Koeffizienten darstellen.

[1] Carl Friedrich GAUSS (1777-1855)

Beispiel: $6x^2 - 11x - 35 = \left(\frac{4}{3}x - \frac{14}{3}\right).\left(\frac{9}{2}x + \frac{15}{2}\right) = (2x - 7).(3x + 5)$

BW: Es sei das Polynom

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$$

über $\mathbb{Q}$ reduzibel.

$$f(x) = g(x).\ h(x)$$

Ferner sei m_1 der Hauptnenner der Koeffizienten von $g(x)$ und m_2 der Hauptnenner der Koeffizienten von $h(x)$. Dann gilt

$$g(x) = \frac{1}{m_1}.g_1(x) \quad \text{und} \quad h(x) = \frac{1}{m_2}.h_1(x)$$

wobei nunmehr $g_1(x)$ und $h_1(x)$ ganzzahlige Koeffizienten haben. Seien d_1 und d_2 die größten gemeinsamen Teiler der ganzzahligen Koeffizientenvon $g_1(x)$ und $h_1(x)$, so gilt

$$g(x) = \frac{1}{m_1}.g_1(x) = \frac{d_1}{m_1}.g_2(x)$$

$$h(x) = \frac{1}{m_2}.h_1(x) = \frac{d_2}{m_2}.h_2(x)$$

Hier sind g_2 und h_2 primitive Polynome mit ganzzahligen Koeffizienten. Dann ist

$$f(x) = \frac{d_1 d_2}{m_1 m_2}.g_2(x).h_2(x)$$

Setzen wir $\frac{d_1 d_2}{m_1 m_2} = \frac{r}{s}$, worin $\frac{r}{s}$ eine normierter Bruch ist, so gilt

$$f(x) = \frac{r}{s}.g_2(x).h_2(x) \qquad (\bullet)$$

Es sei

$$g_2(x).h_2(x) = c_n x^n + \text{---} + c_1 x + c_0, \qquad c_i \in \mathbb{Z}$$

Dann gilt wegen (•)

$$a_n = \frac{r}{s}.c_n, \ldots, a_1 = \frac{r}{s}.c_1, a_0 = \frac{r}{s}.c_0$$

Da die a_i nach Voraussetzung ganze Zahlen sind, muß $r.c_i$ duch s teilbar sein, wegen $ggT(r,s) = 1$ müssen alle c_i durch s teilbar sein.
Da g_2 und h_2 primitive Polynome sind, ist nach Lemma 1 auch $g_2.h_2$ primitiv, d.h. die c_i können keinen größten gemeinsamen Teiler $\neq 1$ besitzen, daher muß $s = 1$ sein und es gilt $f(x) = r.g_2(x).h_2(x)$, d.h. $f(x)$ wird in das Produkt ganzzahliger Faktoren zerlegt.

Zerlegung eines Polynoms über $\mathbb{Q}$ in irreduzible Faktoren über $\mathbb{Q}$ (Methode von KRONECKER[1])

O.B.d.A kann man voraussetzen, daß $f(x)$ ganzzahlige Koeffizienten besitzt.

1.Schritt: Untersuchung auf lineare Faktoren. Die Aufsuchung rationaler Nullstellen wurde bereits behandelt (Siehe Seite 8). Die gefundenen linearen Faktoren spalten wir ab.

2.Schritt: Aufsuchung von quadratischen Faktoren, die über $\mathbb{Q}$ irreduzibel sind.

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = g(x).\ h(x)$$

mit

$$g(x) = px^2 + qx + r$$

Nach dem 2.Lemma von GAUSS können wir voraussetzen, daß die Koeffizienten von

[1] Leopold KRONECKER (1821-1891)

$g(x)$ und $h(x)$ ganze Zahlen sind. Ist speziell $a_n = 1$, so müssen auch die führenden Koeffizienten von $g(x)$ und $h(x)$ gleich 1 sein, speziell also $p = 1$.
Wir wählen nun eine beliebige ganze Zahl x_0. Dann gilt

$$f(x_0) = g(x_0).h(x_0)$$

d.h. die ganze Zahl $f(x_0)$ muß durch die ganze Zahl $g(x_0)$ teilbar sein:

$$g(x_0) | f(x_0)$$

Dasselbe gilt für zwei beliebige andere ganze Zahlen x_1, x_2:

$$g(x_0) = px_0^2 + qx_0 + r = t_0 \ \ldots \ t_0 \mid f(x_0)$$
$$g(x_1) = px_1^2 + qx_1 + r = t_1 \ \ldots \ t_1 \mid f(x_1)$$
$$g(x_2) = px_2^2 + qx_2 + r = t_2 \ \ldots \ t_2 \mid f(x_2)$$

Aus diesen Beziehungen ermittelt man die ganzzahligen Unbekannten p, q, r.
Die ganzen Zahlen x_i ($i = 0,1,2$) wählt man durch Probieren möglichst so, daß die $f(x_i)$ Primzahlen sind oder möglichst wenig Primteiler auftreten, um die Anzahl der Rechenansätze zu minimieren.
Die gewonnenenLösungen für p,q,r müssen ganzzahlig sein. Das Polynom $g(x)$ muß zur Kontrolle $f(x)$ teilen.

Es sei $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ ein Polynom mit ganzzahligen Koeffizienten. Ist a_0 ungerade, so hat $f(x)$ keine ganzzahlige Nullstelle, wenn die Summe

$$a_n + a_{n-1} + \ldots + a_1$$

der restlichen Koeffizienten gerade ist

BW: Da a_0 nach Voraussetzung ungerade ist, kann eine ganzzahlige Nullstelle x als Teiler von a_0 nicht gerade sein. Dann ist auch jede Potenz von x ungerade:

$$x^i = 2s_i + 1$$

Dann gilt

$$f(x) = a_n(2s_n + 1) + \ldots + a_1(2s_1 + 1) + a_0 =$$
$$= \underbrace{2(a_n s_n + \ldots + a_1 s_1)}_{\text{gerade}} + (a_n + \ldots + a_1) + \underbrace{a_0}_{\text{unger.}}$$

Ist die Summe $a_n + a_{n-1} + \ldots + a_1$ gerade, so kann die Summe der geraden Summanden in $f(x)$ zusammen mit dem ungeraden Summanden a_0 nie verschwinden, d.h. die ganze Zahl x kann nicht Nullstelle sein

Irreduzibilitätskriterien

Ist das Polynom $f(x)$ über dem Körper $\mathbb{K}$ irreduzibel, so ist auch jenes Polynom $f_1(y)$ irreduzibel, welches aus $f(x)$ durch die Substitution $x = \lambda y + \mu$ ($\lambda, \mu \in \mathbb{K}$, $\lambda \neq 0$) hervorgeht, und umgekehrt.

$$f(x) = f(\lambda y + \mu) = f_1(y)$$

BW: Wäre $f(x) = g(x).h(x)$ über $\mathbb{K}$ reduzibel, so gälte auch
$f(x) = f(\lambda y + \mu) = g(\lambda y + \mu).h(\lambda y + \mu) = g_1(y).h_1(y) = f_1(y)$ und umgekehrt

Beispiel: $f(x) = x^4 + 4x^3 + 6x^2 + 4x + 2$ ($\mathbb{K} = \mathbb{Q}$)
Setzt man $y := x - 1$, so folgt
$f(x) = (x + 1)^4 + 1 = y^4 + 1$ . . . irreduzibel über $\mathbb{Q}$

Ist $f(x)$ ein normiertes Polynom mit ganzzahligen Koeffizienten, welches bei geeigneter Wahl einer Primzahl p über dem Restklassenkörper $\mathbb{Z}_p$ irreduzibel ist (d.h. $\mathbb{K} = \mathbb{Z}_p$), dann ist $f(x)$ auch über $\mathbb{Q}$ irreduzibel.

ACHTUNG: Die Umkehrung dieses Satzes gilt nicht! $f(x)$ kann sehr wohl über dem Restklassenkörper[1] $\mathbb{Z}_p$ reduzibel sein, obwohl $f(x)$ über $\mathbb{Q}$ irreduzibel ist

BW: Ist $f(x)$ normiert, so ist auch das modulo p reduzierte Polynom normiert und vom selben Grad.
Läßt sich $f(x) = g(x).h(x)$ nichttrivial zerlegen, so gäbe es für jede Primzahl p eine nichttriviale Zerlegung, da ja $g(x)$ und $h(x)$ ihre Grade behalten.
Findet sich bloß ein einziges p, für welches das ***mod*** p reduzierte Polynom irreduzibel ist, so ist auch $f(x)$ über $\mathbb{Q}$ irreduzibel.
Bei der Aufsuchung der Nullstellen hat man überhaupt nur die Elemente von $\mathbb{Z}_p$ auf das reduzierte Polynom anzuwenden.
Die Umkehrung gilt nicht. Ist nämlich das ***mod*** p reduzierte Polynom in zwei Faktoren $(x^r+...)(x^s+...)$ zerlegbar, so müssen deren führende Koeffizienten nicht von der rationalen Zahl 1 herrühren. Es gilt nämlich $i.p+1 \equiv 1$ (***mod*** p). Die Polynome der Umkehrung müssen also nicht mehr normiert sein

Beispiel: Hat das Polynom $f(x) = x^4 - 312x^3 + 2051x^2 - 3145x + 31752$ ganzzahlige Nullstellen?
Wegen $a_0 = 2^3.3^4.7^2$ gäbe es $(4.5.3).2 = 120$ Teiler von a_0, die man durchprobieren müßte.
Reduktion bezüglich einfacher Primzahlen:
$p = 2$ $f(x) \equiv x^4 + x^2 - x = 0 \quad \Rightarrow f(0) \equiv 0, f(1) \equiv 1$ (***mod*** 2)
$p = 3$ $f(x) \equiv x^4 + 2x^2 - x = 0 \quad \Rightarrow f(0) \equiv 0, f(1) \equiv 2, f(2) \equiv 1$ (***mod*** 3)
$p = 5$ $f(x) \equiv x^4 - 2x^3 + x^2 + 2 = 0 \Rightarrow$
$\Rightarrow f(0) \equiv 2, f(1) \equiv 2, f(2) \equiv 1, f(3) \equiv 3, f(4) \equiv 1$ (***mod*** 5)
Da es modulo 5 keine einzige Nullstelle gibt, hat die ursprüngliche Gleichung keine ganzzahlige Nullstelle, obwohl modulo 2 und 3 Nullstellen auftreten

Irreduzibilitätskriterium von EISENSTEIN: Ein Polynom

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$$

mit ganzzahligen Koeffizienten, dessen sämtliche Koeffizienten mit Ausnahme von a_n durch die Primzahl p teilbar sind, der Koeffizient a_0 wohl durch p, nicht aber durch p^2 teilbar ist, ist über $\mathbb{Q}$ irreduzibel

BW indirekt: Die Voraussetzung von EISENSTEIN[2] sei erfüllt und trotzdem sei $f(x)$ über $\mathbb{Q}$ reduzibel.
Dann läßt sich nach dem 2.GAUSSschen Lemma $f(x)$ sogar in Faktoren mit ganzzahligen Koeffizienten zerlegen

$$f(x) = g(x).h(x)$$

Es sei

$g(x) = b_k x^k + b_{k-1}x^{k-1} + \ldots + b_1 x + b_0 \qquad b_k \neq 0, \quad 0 < k < n$
$h(x) = c_l x^l + c_{l-1}x^{l-1} + \ldots + c_1 x + c_0 \qquad c_l \neq 0, \quad 0 < l < n$

Dann gilt

$a_0 = b_0 c_0$
$a_1 = c_0 b_1 + c_1 b_0$
:
$a_k = c_0 b_k + c_1 b_{k-1} + \ldots + c_k b_0$
:
$a_n = c_k b_l$

Nach Voraussetzung ist $a_0 = b_0 c_0$ durch p teilbar. Daher muß c_0 oder p_0 durch p teilbar sein. Da aber a_0 nicht durch p^2 teilbar ist, können nicht c_0 und b_0 durch p teilbar sein. Sei nun o.B.d.A.

$$p|b_0, \text{ aber } \neg(p|c_0)$$

Da nach Voraussetzung alle a_k bis auf a_n durch p teilbar sind, c_0 aber nicht durch p teilbar ist, ergibt sich der Reihe nach

$a_1 = c_0 b_1 + c_1 b_0 \Rightarrow p|b_1$

[1] Über den Begriff der Restklasse siehe Seite 38

[2] Gotthold EISENSTEIN (1832-1852)

$a_2 = c_0b_2 + c_1b_1 + c_2b_0 \Rightarrow p|b2$

$\vdots$

$a_k = c_0b_k + c_1b_{k-1} + \ldots + c_k b_0 \Rightarrow p|b_k$

Nun ist $a_n = b_kc_l$. Da b_k durch p teilbar ist, müßte a_n im Gegensatz zu Voraussetzung auch durch p teilbar sein. $f(x)$ ist daher irreduzibel

Polynome über $\mathbb{K}_0$, deren Nullstellen $\mathbb{K}_\mu$ angehören

Läßt sich eine Konstruktion, deren Angabewerte dem Körper $\mathbb{K}_0 := \mathbb{Q}[q_1, \ldots, q_r]$ angehören, mit Zirkel und Lineal bewältigen, so müssen die Koordinaten von Lösungspunkten notwendigerweise dem Körper $\mathbb{K}_\mu$ angehören, der durch Adjunktion von Quadratwurzelschachtelungen aus dem Körper $\mathbb{K}_0$ hervorgeht. Die Elemente von $\mathbb{K}_\mu$ müssen sich daher als Nullstellen von Polynomen berechnen lassen, deren Koeffizienten dem bekannten Angabekörper angehören.

Die Umkehrung gilt nicht, da sich keineswegs die Nullstellen jedes Polynoms über $\mathbb{K}_0$ durch Quadratwurzelschachtelungen darstellen lassen. Obige Bedingung ist also nicht hinreichend.

Es bedeute

μ . . . Anzahl der übereinandergeschachtelten Quadratwurzeln

m . . . Anzahl der voneinander unabhängigen Quadratwurzeln

Beispiel: Es sei $a,b,c,d,e,f,g,h \in \mathbb{K}_0$

$$x = \frac{\sqrt{a+b\sqrt{c+\sqrt{d}}}}{\sqrt{e+\sqrt{f}+g}} + \sqrt{h} \in \mathbb{K}_3 \qquad \mu = 3,\ m = 6$$

Wir betrachten nun ein Element $x \in \mathbb{K}_\mu$ mit m unabhängigen Wurzeln und bestimmen seine Normalform.

Enthält x im Nenner eines Bruches Wurzeln, so schaffen wir diese durch geeignete Erweiterungen weg, bis wir einen Ausdruck aus $\mathbb{K}_\mu$ erhalten, in welchem m unabhängige Wurzeln mit Koeffizienten aus $\mathbb{K}_0$ auftreten, von denen höchsten μ übereinander geschachtelt sind.
Jede der m Quadratwurzeln hat zwei Vorzeichen, sodaß bei m Wurzeln 2^m Werte

$$x_1, x_2, \ldots, x_{2^m}$$

möglich sind. Diese Werte nennt man *zueinander konjugiert*. Ist eines der x_i bekannt, so sind alle anderen mitbestimmt.

Beispiel: $\mu = 2$, $m = 3$, $2^3 = 8$ konjugierte Werte

$$x = x_1 = \sqrt{a}+\sqrt{b+\sqrt{c}} \qquad x_5 = -\sqrt{a}+\sqrt{b+\sqrt{c}}$$
$$x_2 = \sqrt{a}+\sqrt{b-\sqrt{c}} \qquad x_6 = -\sqrt{a}+\sqrt{b-\sqrt{c}}$$
$$x_3 = \sqrt{a}-\sqrt{b+\sqrt{c}} \qquad x_7 = -\sqrt{a}-\sqrt{b+\sqrt{c}}$$
$$x_4 = \sqrt{a}-\sqrt{b-\sqrt{c}} \qquad x_8 = -\sqrt{a}-\sqrt{b-\sqrt{c}}$$

Allerding müssen nicht alle 2^m konjugierten Werte verschieden sein

Beispiel: $\mu = 2$, $m = 3$

$$x_1 = \sqrt{a+\sqrt{b}}+\sqrt{a-\sqrt{b}}$$
$$x_2 = \sqrt{a-\sqrt{b}}+\sqrt{a+\sqrt{b}}$$

Der Ausdruck ändert sich nicht bei Vorzeichenwechsel von $\sqrt{b}$

Wir ermitteln nun das Polynom $F(x)$, welches alle 2^m Werte x^i (die nicht alle verschieden sein müssen) als Nullstellen enthält:

$$F(x) := (x - x_1)(x - x_2)\dots(x - x_{2^m}) \qquad \text{Polynom } 2^m\text{-ten Grades}$$

Die Koeffizienten von $F(x)$ sind eindeutig bestimmt. Wir behaupten

Die Koeffizienten von $F(x)$ gehören $\mathbb{K}_0$ an.

BW: Wir ändern das Vorzeichen einer der m Quadratwurzeln. Dadurch werden die x_i lediglich untereinander vertauscht, da die Nullstellen von $F(x)$ alle konjugierten Werte umfassen. Die Gleichung von $F(x)$ wird dadurch nicht verändert, da bloß eine Vertauschung der Faktoren eintritt.
Wenn das Polynom $F(x)$ sich bei Änderung des Vorzeichens einer Wurzel nicht ändert, kann in der Gleichung von $F(x)$ nur das Quadrat dieser Wurzel auftreten.
Daher können in den Koeffizienten von $F(x)$ keine Quadratwurzeln stehen. Die Koeffizienten von $F(x)$ müssen daher $\mathbb{K}_0$ angehören.

Wenn ein Wert $x \in \mathbb{K}_\mu$ Nullstelle eines Polynoms $f(x)$ über $\mathbb{K}_0$ ist, so sind auch alle konjugierten Werte Nullstellen desselben Polynomx $f(x)$

$f(x)$ muß keineswegs mit $F(x)$ übereinstimmen, denn es könnte ja noch andere Nullstellen enthalten.

BW: Nehmen wir an, x_1 habe die Bauart

$$x_1 = a + b\sqrt{r_1} + c\sqrt{r_2} + d\sqrt{r_1}\cdot\sqrt{r_2} \in \mathbb{K}_\mu \qquad a,b,c,d,r_1,r_2 \in \mathbb{K}_{\mu-1}$$

Ist x_1 Nullstelle von $f(x)$, so muß gelten

$$f(x_1) = A + B\sqrt{r_1} + C\sqrt{r_2} + D\sqrt{r_1}\cdot\sqrt{r_2} = 0, \quad A,B,C,D,r_1,r_2 \in \mathbb{K}_{\mu-1}$$

Dies ist aber nur möglich, wenn

$$A = B = C = D = 0$$

ist. Dann verschwindet $f(x)$ aber auch, wenn $\sqrt{r_1}$und $\sqrt{r_2}$ beliebig ihr Vorzeichen ändern. Die verschwindenden Werte A,B,C,D sind Elemente von $\mathbb{K}_{\mu-1}$ mit höchstens μ-1 übereinandergeschachtelten Wurzeln. Sei etwa

$$A = \alpha + \beta\sqrt{\rho_1} + \gamma\sqrt{\rho_2} + \delta\sqrt{\rho_1}\cdot\sqrt{\rho_2}, \qquad \alpha,\beta,\gamma,\delta,\rho_1,\rho_2 \in \mathbb{K}_{\mu-2}$$

Daraus folgt

$$\alpha = \beta = \gamma = \delta = 0$$

Daher verschwinden die A, ... auch, wenn sich die Vorzeichen von $\sqrt{\rho_1}$ und $\sqrt{\rho_2}$ ändern.
Fährt man so fort, so findet man, daß alle x_i, die aus x_1 durch beliebige Vorzeichenänderung der Wurzeln hervorgehen, Nullstellen von $f(x)$ sind.

Wir kennen nunmehr zwei Polynome mit Koeffizienten aus $\mathbb{K}_0$, die alle x_i als Nullstellen enthalten:

$F(x)$ . . . enthält eventuell mehrfache Nullstellen

$f(x)$ . . . enthält neben den x_i eventuell auch noch andere Nullstellen

Wir fragen nun nach dem Polynom $\Phi(x)$ niedrigsten Grades über $\mathbb{K}_0$, welches ein x_i (und damit auch alle konjugierten) als Nullstellen enthält

Eigenschaften von $\Phi(x)$

1. $\Phi(x)$ ist irreduzibel über $\mathbb{K}_0$

   BW indirekt: Wäre $\Phi(x)$ reduzibel, so gäbe es zwei Polynome mit

   $$\Phi(x) = \psi(x).\chi(x), \quad 0 < grd\,\psi < grd\,\Phi \;\wedge\; grd\,\chi < grd\,\Phi$$

   Dann gilt

   $$\Phi(x_1) = \psi(x_1).\chi(x_1) = 0$$

   d.h. einer der Faktoren $\psi(x_1)$ oder $\chi(x_1)$ muß verschwinden, was der Minimalität des Grades von $\Phi(x)$ widerspricht

2. $\Phi(x)$ hat keine mehrfachen Nullstellen

   BW indirekt: $\Phi(x)$ enthalte x_1 als α-fache Nullstelle. Die daraus folgende Darstellung

   $$\Phi(x) = (x - x_1)^{\alpha}.g(x)$$

   ist i.a. noch keine Zerlegung von $\Phi(x)$ über $\mathbb{K}_0$! Dann würde aber auch die 1.Ableitung

   $$\Phi(x)' = \alpha(x-x_1)^{\alpha-1}.g(x) + (x - x_1)^{\alpha}.g'(x)$$

   x_1 und damit auch alle konjugierten Elemente als Nullstellen enthalten. $\Phi'(x)$ wäre dann entgegen der Voraussetzung ein Polynom geringeren Grades über $\mathbb{K}_0$ als $\Phi(x)$. Widerspruch zur Voraussetzung.

3. $\Phi(x)$ hat keine anderen Nullstellen als die x_i

   BW indirekt: Gäbe es nämlich andere Nullstellen, hätte $\Phi(x)$ und $F(x)$ einen größten gemeinsamen Teiler, der natürlich ein Polynom über $\mathbb{K}_0$ ist. Dann könnte man $\Phi(x)$ über $\mathbb{K}_0$ in zwei Faktoren zerlegen. Widerspruch!

4. Es sei M die Anzahl der wesentlich verschiedenen Werte der x_i

   Dann gilt

   $$\Phi(x) = C(x - x_1)(x - x_2) \ldots (x - x_M), \quad C \in \mathbb{K}_0, \; grd\, \Phi(x) = M$$

5. $\Phi(x)$ ist das einzige irreduzible Polynom über $\mathbb{K}_0$, das von allen x_1 befriedigt wird

   BW indirekt: Wäre $f(x)$ ein Polynom über $\mathbb{K}_0$, das von allen x_i befriedigt wird, so wäre $f(x)$ durch $\Phi(x)$ teilbar und daher nicht irreduzibel

Wegen dieser fünf Eigenschaften kann man von dem irreduziblen Polynom über $\mathbb{K}_0$ sprechen, das von den x_i erfüllt wird.

Vergleichen wir nun $F(x)$ und $\Phi(x)$, so haben beide nur die x_i als Nullstellen, wobei $F(x)$ eventuell mehrfache Nullstellen hat. Dann ist $F(x)$ duch $\Phi(x)$ teilbar und es ist

$$F(x) = \Phi(x).F_1(x)$$

Wenn $F_1(x)$ keine Konstante ist, läßt es eine der mehrfachen Nullstellen von $F(x)$ zu und damit auch alle anderen. Demnach muß gelten

$$F_1(x) = \Phi(x).F_2(x)$$

So kann man fortfahren, wobei der Grad von $F_i(x)$ immer kleiner wird, bis sich $F_i(x)$ endlich auf eine Konstante reduziert:

$$\left.\begin{aligned} F(x) &= F_1(x).\Phi(x) \\ F_1(x) &= F_2(x).\Phi(x) \\ &\vdots \\ F_{\nu-2}(x) &= F_{\nu-1}(x).\Phi(x) \\ F_{\nu-1}(x) &= C.\Phi(x) \end{aligned}\right\} \begin{array}{l} \text{Produktbildung der} \\ \text{Gleichungen ergibt} \\ F(x) = C.[\Phi(x)]^{\nu} \end{array}$$

$F(x)$ ist bis auf einen konstanten Faktor aus $\mathbb{K}_0$ gleich einer Potenz von $\Phi(x)$

Nunmehr können wir auch eine Aussage über den Grad von $\Phi(x)$ machen:

$$grd\, F(x) = 2^m = \nu M$$

Daraus folgt, daß auch M eine Potenz von 2 ist.

> Der Grad eines über seinem Koeffizientenkörper irreduziblen Polynoms, dessen Nullstellen Quadratwurzelschachtelungen sind, ist stets notwendig eine Potenz von 2

Da es umgekehrt nur ein einziges irreduzibles Polynom $\Phi(x)$ gibt, das von allen x_i erfüllt wird, folgt

> Wenn ein irreduzibles Polynom nicht vom Grade 2^h ist, hat es keine Nullstellen, die durch Quadratwurzelschachtelungen über seinem Koeffizientenkörper gebildet werden

Dieser Satz besagt jedoch nicht, daß jedes irreduzible Polynom vom Grade 2^h Quadratwurzelschachtelungen als Nullstellen hat. Obige Bedingung ist nur notwenig, nicht aber hinreichend

Polynome dritter Ordnung

Die bisherigen Entwicklungen haben gezeigt, daß ein Problem, das auf eine irreduzible Gleichung dritten Grades über $\mathbb{K}_0$ führt, mit Zirkel und Lineal unlösbar ist. Zu diesen Problemen gehören die Würfelverdopplung und die Dreiteilung des Winkels.

Die Würfelverdopplung (das Delische Problem)

Nach Johannes PHILOPONOS (6.Jhd.n.Chr.) litten die Delier um etwa 430 v.Chr. an einer typhusartigen Krankheit. Das Orakel in Delphi verkündete, daß man den auf Delos befindlichen, Apollon gewidmeten, würfelförmigen Altar verdoppeln müsse. Die Delier erbauten daher einen würfelfömigen Altar von doppelter Kantenlänge, was jedoch die Seuche nicht verringerte. Das Orakel wurde dann so interpretiert, daß das Volumen des Altars zu verdoppeln sei. Da dies den Deliern nicht gelang, wandten sie sich an PLATON (427-347? v.Chr.) in Athen, der sie an HIPPOKATES von Chios (um 440 v.Chr.) verwies. Dieser reduzierte das Problem auf die Bestimmung zweier Strecken x, y mit der Eigenschaft (vgl. Seite 102)

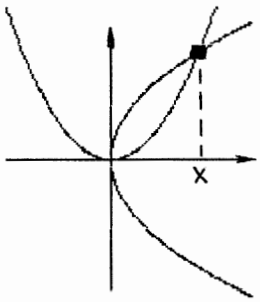
$$s : x = x : y = y : 2s \Rightarrow sy = x^2 \wedge y^2 = 2sx \Rightarrow y = \frac{x^2}{s}$$

daraus

$$\frac{x^4}{s^2} = 2sx \Rightarrow x^4 = 2s^3x \Rightarrow \underline{x^3 = 2s^3}$$

HIPPOKATES löste also das Problem durch den Schnitt der beiden Parabeln

$$x^2 = sy \quad \text{und} \quad y^2 = 2sx$$



Der Lösungsweg des HIPPOKATES verwendet allerdings im klassischen Sinne nicht zugelassene Kurven.

Der sich entwickelnden Korrespondenz zwischen Athen und Delos wegen, nannten die Athener um PLATON die Aufgabe das „Delische Problem".

Das zu lösende Problem lautet also:
Gegeben sei ein Würfel mit der Seitenkante s. Mit welchem Faktor x muß man s multiplizieren, um einen Würfel doppeltem Volumens zu erhalten?
Die neue Kante ist also sx und es soll gelten:

$$x^3s^3 = 2s^3 \Rightarrow \underline{x^3 = 2}$$

Wir haben also die Gleichung

$$x^3 = 2$$

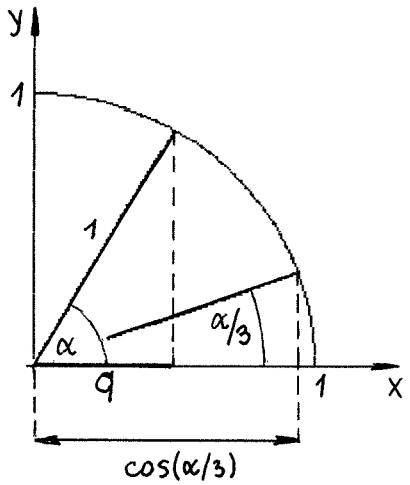
wenn möglich mit Zirkel und Lineal zu lösen. Wenn das kubische Polynom über dem Koeffizientenkörper $\mathbb{Q}$ irreduzibel ist, dann ist das Problem auf klassische Weise unlösbar.

Wir haben demnach die Reduziblität von $f(x) = x^3 - 2$ zu untersuchen. $f(x)$ könnte nur in einen quadratischen und in einen lineare Faktor oder in drei lineare Faktoren über $\mathbb{Q}$ zerlegt werden.

In jedem dieser Fälle müßte mindestens ein linearer Faktor über $\mathbb{Q}$ auftreten. Nach dem 2.Lemma von GAUSS (Seite 11) müßte diese Zerlegung mit ganzzahligen Koeffizienten möglich sein und als Nullstellen kommen nach Seite 9 nur die Werte $\pm 1, \pm 2$, als Teiler von $a_0 = 2$ in Frage. Man überzeugt sich leicht, daß keiner dieser Werte Nullstelle von $f(x)$ ist.

> Das Delische Problem ist, unabhängig von der Seitenlänge des gegebenen Würfels, mit Zirkel und Lineal nicht lösbar

Die Dreiteilung des Winkels



Es handelt sich darum, eine allgemeingültige Konstruktion zu finden, mit deren Hilfe man jeden Winkel mit Zirkel und Lineal dritteln kann

Der Winkel α ist bestimmt durch die Einkeitsstrecke 1 und die Strecke $q = \cos\alpha$

Die Angaben gehören also dem Körper $\mathbb{K}_0 = \mathbb{Q}[q]$ an. Unsere Aufgabe besteht darin, nach Möglichkeit mit Zirkel und Lineal die Strecke

$$\cos\frac{\alpha}{3}$$

zu konstruieren.

Mehrfache Anwendung des Additionstheorems ergibt

$$\cos\alpha = \cos\left(\frac{\alpha}{3}+\frac{2\alpha}{3}\right) = \cos\left(\frac{\alpha}{3}\right).\cos\left(\frac{2\alpha}{3}\right) - \sin\left(\frac{\alpha}{3}\right).\sin\left(\frac{2\alpha}{3}\right) =$$

$$= \cos\left(\frac{\alpha}{3}\right).\left(\cos^2\left(\frac{\alpha}{3}\right) - \sin^2\left(\frac{\alpha}{3}\right)\right) - \sin\left(\frac{\alpha}{3}\right).\left(2.\sin\left(\frac{\alpha}{3}\right).\cos\left(\frac{\alpha}{3}\right)\right) =$$

$$= \cos^3\left(\frac{\alpha}{3}\right) - 3.\cos\left(\frac{\alpha}{3}\right).\sin^2\left(\frac{\alpha}{3}\right) = \cos^3\left(\frac{\alpha}{3}\right) - 3.\cos\left(\frac{\alpha}{3}\right).\left(1-\cos^2\left(\frac{\alpha}{3}\right)\right) =$$

$$= 4.\cos^3\left(\frac{\alpha}{3}\right) - 3.\cos\left(\frac{\alpha}{3}\right) = \cos\alpha$$

Multiplikation mit 2 ergibt

$$2.\cos\alpha = \left(2.\cos\left(\frac{\alpha}{3}\right)\right)^3 - 3.\left(2.\cos\left(\frac{\alpha}{3}\right)\right)$$

Setzt man

$$x = 2.\cos\left(\frac{\alpha}{3}\right)$$

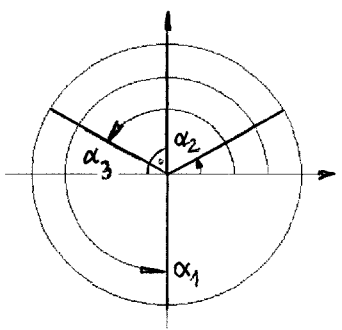
so erhält man als Gleichung für die Winkeldreiteilung

$$x^3 - 3x - 2.\cos\alpha = 0 \quad \text{bzw.} \quad x^3 - 3x - 2q = 0$$

Die Winkeldreiteilung mit Zirkel und Lineal ist möglich, wenn diese Gleichung 3.Grades über $\mathbb{Q}[q]$ reduzibel ist, ansonsten unmöglich.

Wir haben demnach zu untersuchen, ob sich mindestens ein Linearfaktor abspalten läßt, d.h. ob es eine Nullstelle über $\mathbb{Q}[q]$ gibt.

Bevor wir diese Frage in Angriff nehmen, entsinnen wir uns, daß es jedenfalls Winkel gibt, die sich mit Zirkel und Lineal dritteln lassen, z.B. die Winkel von 90° und 45°. Wir betrachten zunächst diese Sonderfälle.



$\boxed{\alpha = 90°}$ $\cos\alpha = \cos 90° = 0 = q$, $\mathbb{K}_0 = \mathbb{Q}$

Die Dreiteilungsgleichung lautet

$x^3 - 3x = (x^2 - 3)x = 0$

Über $\mathbb{K}_0$ existiert also die Nullstelle

$x_1 = 0 \in \mathbb{K}_0 = \mathbb{Q}$

Die beiden restlichen Nullstellen

$$x_2 = +\sqrt{3} \in \mathbb{K}_0\left[\sqrt{3}\right] = \mathbb{K}_1$$
$$x_2 = -\sqrt{3} \in \mathbb{K}_0\left[\sqrt{3}\right] = \mathbb{K}_1$$

sind Quadratwurzeln von Elementen aus $\mathbb{K}_1$ und daher konstruierbar. Wegen

$$\cos\left(\frac{\alpha}{3}\right) = \frac{x}{2}$$

ergibt sich

$$\cos\left(\frac{1}{3}.\alpha_1\right) = 0 \Rightarrow \frac{1}{3}.\alpha_1 = 270° \qquad (3.270 = 810 = 2.360 + 90)$$

$$\cos\left(\frac{1}{3}.\alpha_2\right) = +\frac{1}{2}.\sqrt{3} \Rightarrow \frac{1}{3}.\alpha_2 = 30°$$

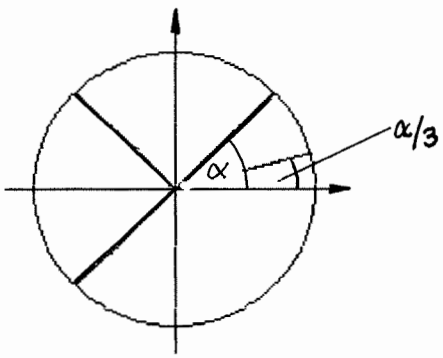
$$\cos\left(\frac{1}{3}.\alpha_3\right) = -\frac{1}{2}.\sqrt{3} \Rightarrow \frac{1}{3}.\alpha_3 = 150° \quad (3.150 = 450 = 360 + 90)$$

$\boxed{\alpha = 45°}$ $\quad \cos\alpha = \cos 45° = \frac{\sqrt{2}}{2} = q,\ \mathbb{K}_0 = \mathbb{Q}\left[\sqrt{2}\right]$

Die Dreiteilungsgleichung lautet

$$x^3 - 3x - \sqrt{2} = 0$$

Man erkennt sofort, daß $-\sqrt{2}$ eine Nullstelle aus $\mathbb{K}_0$ ist. Mit Hilfe des HORNER-Schemas (Seite 6) findet man



	1	0	-3	$-\sqrt{2}$
$-\sqrt{2}$		$-\sqrt{2}$	2	$+\sqrt{2}$
	1	$-\sqrt{2}$	-1	0

Daher gilt

$$x^3 - 3x - \sqrt{2} = \left(x^2 - x\sqrt{2} - 1\right)\left(x + \sqrt{2}\right)$$

Außer der Nullstelle

$$x_1 = -\sqrt{2}$$

gibt es noch die beiden Nullstellen

$$x_{2,3} = \frac{\sqrt{2} \pm \sqrt{6}}{2} = \frac{\sqrt{2} \pm \sqrt{2}.\sqrt{3}}{2} \in \mathbb{K}_1 = \mathbb{K}_0\left[\sqrt{3}\right] = \mathbb{Q}\left[\sqrt{2}, \sqrt{3}\right]$$

Daraus folgt

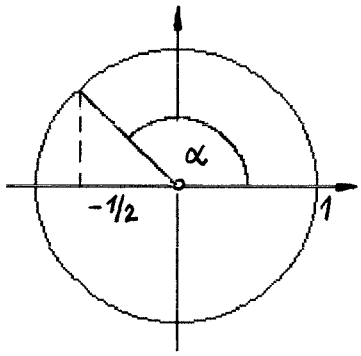
$$\cos\left(\frac{1}{3}.\alpha_1\right) = -\frac{\sqrt{2}}{2} \qquad \frac{1}{3}.\alpha_1 = 135°$$

$$\cos\left(\frac{1}{3}.\alpha_2\right) = \frac{\sqrt{2}}{4}.\left(1 + \sqrt{3}\right) \qquad \frac{1}{3}.\alpha_2 = 15°$$

$$\cos\left(\frac{1}{3}.\alpha_3\right) = \frac{\sqrt{2}}{4}.\left(1 - \sqrt{3}\right) \qquad \frac{1}{3}.\alpha_2 = 255°$$

Nach diesen Beispielen für drittelbare Winkel,ein Beispiel für einen Winkel, der sich nicht mit Zirkel und Lineal dritteln läßt

$\boxed{\alpha = 120°}$ $\quad \cos\alpha = \cos 120° = -\frac{1}{2} = q, \quad \mathbb{K}_0 = \mathbb{Q}$



Die Dreiteilungsgleichung lautet

$$x^3 - 3x + 1 = 0$$

Nach dem Seite 9 müßte es ganzzahlige Nullstellen geben, die (wegen $a_0 = 1$) nur die Werte ± 1 haben könnten. Man überzeugt sich leicht, daß keiner dieser Werte Nullstelle obiger Gleichung ist, diese ist daher irreduzibel.

Der Winkel von 120° kann mit Zirkel und Lineal nicht gedrittelt werden.
Diese Aussage ist äquivalent mit der Aussage, daß das regelmäßige Neuneck nicht mit Zirkel und Lineal konstruiert werden kann, da dessen Zentriwinkel
$40° = \frac{120°}{3}$ beträgt

Im Gegensatz dazu folgt aus den ersten beiden Beispielen, daß das Zwölfeck (Zentriwinkel 30°) und das Vierundzwanzigeck (Zentriwinkel 15°) mit Zirkel und Lineal konstruierbar sind.

Damit ist gezeigt, daß es Winkel gibt, die mit Zirkel und Lineal nicht drittelbar sind.

Wir wollen noch zeigen, daß ein gegebener Winkel im allgemeinen nicht drittelbar ist.. Wir nehmen an, daß $2q = 2\cos\alpha = t$ ein beliebig veränderlicher Parameter. Dann ist z.z., daß die Gleichung

$$x^3 - 3x - t = 0$$

für beliebiges t nicht reduzibel ist, d.h. über $\mathbb{Q}[t]$ keine Nullstelle besitzt. Gäbe es eine solche, so müßte

$$x = x(t)$$

eine rationale Funktion von t sein. x(t) müßte also die Gestalt

$$x = \frac{Z(t)}{N(t)} \in \mathbb{Q}[t] \qquad Z(t),\ N(t) \quad \text{teilerfremd}$$

aufweisen, worin Z(t), N(t) Polynome in t mit Koeffizienten aus $\mathbb{Q}$ sind.

Setzen wir in die Dreiteilungsgleichung ein, so müßte gelten

$$Z^3(t) - 3Z.(t).N(t)^2 - t.N(t)^3 = 0$$

daraus

$$Z^3(t) = N^2(t).[3.Z(t) + t.N(t)]$$

Hieraus würde folgen, daß Z(t) durch N(t) teilbar ist, was wegen der vorausgesetzten Teilerfremdheit nur eintreten kann, wenn N(t) eine Konstante ist, die wir in Z(t) aufgehen lassen können, d.h. es muß sein

$$x = Z(t)$$

woraus wiederum folgt

$$Z^3(t) - 3.Z(t) - t = 0 \Rightarrow t = Z(t).[Z^2(t) - 3]$$

d.h.t müßte durch das Polynom Z(t) teilbar sein. Das wiederum ist nur möglich, wenn

$$Z(t) = c.t, \qquad c \text{ Konstante aus } \mathbb{Q}$$

ist. Das würde bedeuten

$$c^3t^3 - 3ct - t = 0 \Rightarrow c^3t^2 - 3c - 1 = 0$$

was ein offenkundiger Widerspruch ist, da t eine beliebiger Parameter und c eine Konstante ist.

Diese Überlegungen zeigen, daß die Winkeldreiteilung im allgemeinen nicht möglich ist. Man entnimmt aber nicht, daß es doch gewisse dreiteilbare Winkel gibt. Jedoch erkennt man, daß es keine einheitliche Konstruktion zur Winkeldreiteilung geben kann. Jeder dreiteilbare Winkel erfordert seine eigene Konstruktion.

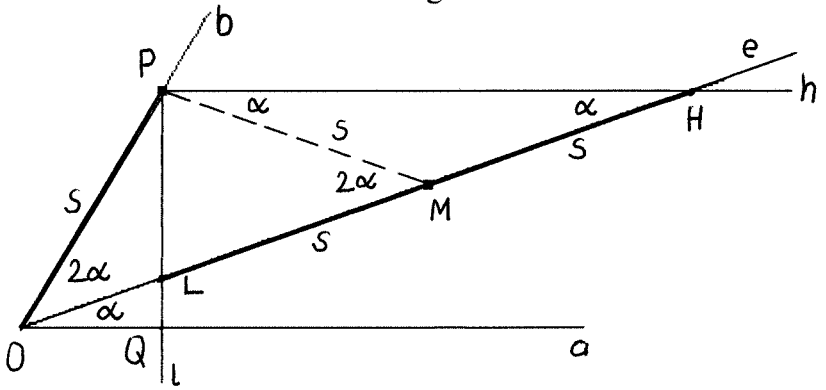
Anmerkung ohne Beweis: Die Menge der dreiteilbaren Winkel ist abzählbar, die der nicht dreiteilbaren ist nicht abzählbar.

Das erste Mal wurde die Unmöglichkeit der Winkeldreiteilung mit Zirkel und Lineal im Jahre 1837 bewiesen durch Pierre Laurent WANTZEL (1814-1848): „Recherches sur les moyens de reconnaître si un problème de géométrie se resoudre avec la règle et le compas". Journal de Mathématiques, 2.Bd (1837) 366-372.

Nichtklassische Lösung des Dreiteilungsproblems nach NIKOMEDES[1]

NIKOMEDES verwendet als nichtklassiches Zeicheninstrument das *Einschiebelineal*.. Genaueres im Kapitel „Das Einschiebelineal" Seite 97 ff.

Auf dem Schenkel b des dreizuteilenden Winkels tragen wir von Scheitel O die Strecke s =

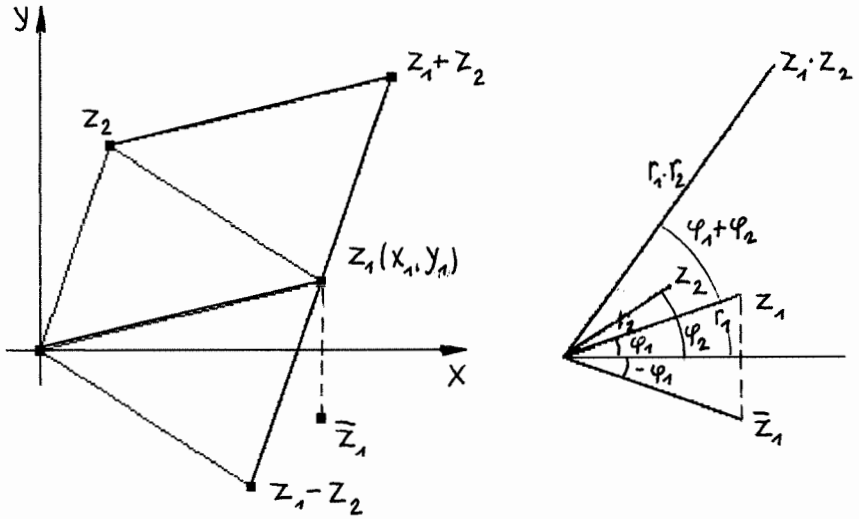


OP ab. Durch P ziehen wir die Parallele h und die Normale l zum Schenkel a. Die auf der Kante des Einschiebelineals e abgetragene Strecke 2s = LH schieben wir zwischen die Geraden l und h so ein, daß die Punkte H bzw. L auf den Geraden h bzw. l zu liegen kommen und die Verlängerung der Strecke LH durch O geht. Der Mittelpunkt M der Strecke LH ist auch Mittelpunkt des durch P gehenden THALESkreises über LH, daher ist MP = s. Im gleichschenkeligen Dreieck Δ HPM gilt: ∠ MHP = ∠ HPM = α. Der Außenwinkel von Δ HPM hat die Größe ∠ OMP = 2α. Im gleichschenkeligen Dreieck Δ OMP gilt ∠ OMP = ∠ MOP = 2α. Da die Winkel ∠ (he) = ∠ (ae) = α als Parallelwinkel gleich sind, wird der gegebene Winkel ∠ (ab) durch die Kante e des Einschiebelineals gedrittelt.

[1] NIKOMEDES (um 180 v.Chr.)

Die GAUSSsche Zahlenebene

Darstellung in kartesischen und in Polarkoordinaten



$z_1 = x_1 + \hat{\imath}.y_1$

$x_1 = \boldsymbol{Re}(z_1)$ Realteil von z_1

$y_1 = \boldsymbol{Im}(z_1)$ Imaginärteil von z_1

$\bar{z}_1 = x_1 - \hat{\imath}.y_1$ Konjugium

$z_2 = x_2 + \hat{\imath}.y_2$

$z_1 + z_2 = (x_1 + x_2) + (y_1 + y_2)$

$z_1 - z_2 = (x_1 - x_2) + (y_1 - y_2)$

$z_1 = r_1(\boldsymbol{cos}\,\varphi_1 + \hat{\imath}.\boldsymbol{sin}\,\varphi_1) \quad 0 \le r_1$

$r_1 = |z_1|$ Betrag von z_1

$\varphi_1 = \boldsymbol{arg}(z_1)$ Argument von z_1

$\bar{z}_1 = r_1(\boldsymbol{cos}\,\varphi_1 - \hat{\imath}.\boldsymbol{sin}\,\varphi_1)$ Konjugium

$z_2 = r_2(\boldsymbol{cos}\,\varphi_2 + \hat{\imath}.\boldsymbol{sin}\,\varphi_2)$

$$z_1 z_2 = r_1 r_2(\boldsymbol{cos}\,\varphi_1 + \hat{\imath}.\boldsymbol{sin}\,\varphi_1)(\boldsymbol{cos}\,\varphi_2 + \hat{\imath}.\boldsymbol{sin}\,\varphi_2) =$$
$$= r_1 r_2.\left[\begin{matrix}(\boldsymbol{cos}\,\varphi_1.\boldsymbol{cos}\,\varphi_2 - \boldsymbol{sin}\,\varphi_1.\boldsymbol{sin}\,\varphi_2) + \\ + \hat{\imath}.(\boldsymbol{cos}\,\varphi_1.\boldsymbol{sin}\,\varphi_2 + \boldsymbol{sin}\,\varphi_1.\boldsymbol{cos}\,\varphi_2)\end{matrix}\right] =$$
$$= r_1 r_2.[\boldsymbol{cos}(\varphi_1 + \varphi_2) + \hat{\imath}.\boldsymbol{sin}(\varphi_1 + \varphi_2)]$$

$$x = r.\boldsymbol{cos}\,\varphi, \quad y = r.\boldsymbol{sin}\,\varphi, \quad r = \sqrt{x^2 + y^2} = \sqrt{z.\bar{z}} = |z|$$

$$|z| = 0 \Leftrightarrow z = 0, \quad \boldsymbol{tan}\,\varphi = \frac{y}{x}$$

Die Formel von de MOIVRE[1]

$$z^n = r^n(\boldsymbol{cos}\,\varphi + \hat{\imath}.\boldsymbol{sin}\,\varphi)^n = r^n[\boldsymbol{cos}(n\varphi) + \hat{\imath}.\boldsymbol{sin}(n\varphi)], \quad n \in \mathbb{N}$$

BW: Folgt aus der oben angeführten Regel für das Produkt zweier in Polarkoordinaten gegebenen Zahlen

Aus der MOIVREschen Formel ergibt sich folgendes:

[1] Abraham de MOIVRE (1667-1754) 1730

$$(\cos\varphi+\hat{\imath}.\sin\varphi)^n=\cos^n\varphi+\hat{\imath}.\binom{n}{1}\cos^{n-1}\varphi.\sin\varphi-\binom{n}{2}\cos^{n-2}\varphi.\sin^2\varphi-\hat{\imath}.\binom{n}{3}\cos^{n-3}\varphi\sin^3\varphi+$$
$$+\binom{n}{4}\cos^{n-4}\varphi.\sin^4\varphi+\hat{\imath}.\binom{n}{5}\cos^{n-5}\varphi.\sin^5\varphi+\ldots=\cos(n\varphi)+\hat{\imath}.\sin(n\varphi)$$

Daraus die bekannten Formeln

$$\cos(n\varphi)=\binom{n}{0}\cos^n\varphi-\binom{n}{2}\cos^{n-2}\varphi.\sin^2\varphi+\binom{\nu}{4}\cos^{n-4}\varphi.\sin^4\varphi\mp\ldots$$

$$\sin(n\varphi)=\binom{n}{1}\sin\varphi.\cos^{n-1}\varphi-\binom{n}{3}\sin^3\varphi.\cos^{n-3}\varphi+\binom{n}{5}\sin^5\varphi.\cos^{n-5}\varphi\mp\ldots$$

bzw.

$$\cos(n\varphi)=\sum_{i=0}^{n}(-1)^i\binom{n}{2i}\cos^{n-2i}\varphi.\sin^{2i}\varphi$$

$$\sin(n\varphi)=\sum_{i=0}^{n}(-1)^i\binom{n}{2i+1}\cos^{2n-(2n+1)}\varphi.\sin^{2n+1}\varphi$$

Die Formel von MOIVRE gilt auch für negative ganzzahlige n, denn es ist

$$(\cos\varphi+\hat{\imath}.\sin\varphi)(\cos\varphi-\hat{\imath}.\sin\varphi)=\cos^2\varphi+\sin^2\varphi=1\Rightarrow$$

$$\frac{1}{(\cos\varphi+\hat{\imath}.\sin\varphi)}=(\cos\varphi+\hat{\imath}.\sin\varphi)^{-1}=(\cos\varphi-\hat{\imath}.\sin\varphi)\Rightarrow$$

$$(\cos\varphi+\hat{\imath}.\sin\varphi)^{-n}=(\cos\varphi-\hat{\imath}.\sin\varphi)^n=[\cos(-\varphi)+\hat{\imath}.\sin(-\varphi)]^n=$$
$$\cos(-n\varphi)+\hat{\imath}.\sin(-n\varphi)$$

also

$$(\cos\varphi+\hat{\imath}.\sin\varphi)^{-n}=\cos(-n\varphi)+\hat{\imath}.\sin(-n\varphi),\qquad n\in\mathbb{N}$$

Für die Division zweier Zahlen gilt daher

$$\frac{z_1}{z_2}=\frac{r_1}{r_2}.\frac{(\cos\varphi_1+\hat{\imath}\sin\varphi_1)}{(\cos\varphi_1+\hat{\imath}\sin\varphi_1)}=\frac{r_1}{r_2}.(\cos\varphi_1+\hat{\imath}\sin\varphi_1)(\cos\varphi_2+\hat{\imath}\sin\varphi_2)^{-1}=$$

$$=\frac{r_1}{r_2}.(\cos\varphi_1+\hat{\imath}\sin\varphi_1)(\cos(-\varphi_2)+\hat{\imath}\sin(-\varphi_2))=\frac{r_1}{r_2}.(\cos(\varphi_1-\varphi_2)+\hat{\imath}\sin(\varphi_1-\varphi_2))$$

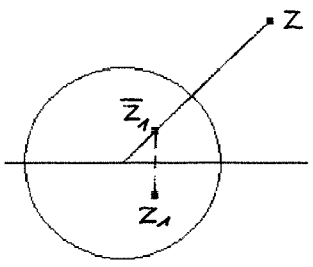
also

$$\frac{z_1}{z_2}=\frac{r_1}{r_2}.[\cos(\varphi_1-\varphi_2)+\hat{\imath}\sin(\varphi_1-\varphi_2)]$$

Speziell gilt

$$\frac{1}{z}=\frac{1}{r}.[\cos\varphi-\hat{\imath}.\sin\varphi]=z_1$$

$$\left.\begin{aligned}|z|&=r\\|z_1|&=\frac{1}{r}\end{aligned}\right\}\ |z|.|z_1|=1\quad\text{Inversion + Konjugium}$$



Da bei gegebenem z das Argument φ nur bis auf Vielfache von 2π bestimmt ist, gilt

$$z = r.[\cos(\varphi \pm 2\pi k) + \hat{\imath}.\sin(\varphi \pm 2\pi k)] \quad k = 0,1,2,...$$

Die Formel von MOIVRE gilt auch für rationale Exponenten. Es ist nämlich

$$(\cos\psi + \hat{\imath}.\sin\psi)^n = \cos(n\psi - 2\pi k) + \hat{\imath}.\sin(n\psi - 2\pi k)$$

Setzt man

$$\varphi := n\psi - 2\pi k \Rightarrow \psi = \frac{\varphi + 2\pi k}{n}$$

so folgt

$$\cos\varphi + \hat{\imath}.\sin\varphi = \left[\cos\left(\frac{\varphi + 2\pi k}{n}\right) + \hat{\imath}.\sin\left(\frac{\varphi + 2\pi k}{n}\right)\right]^n$$

also

$$\boxed{(\cos\varphi + \hat{\imath} + \sin\varphi)^{\frac{1}{n}} = \cos\left(\frac{\varphi}{n} + 2\pi\frac{k}{n}\right) + \sin\left(\frac{\varphi}{n} + 2\pi\frac{k}{n}\right) \qquad k = 0,1,2,\ldots,n-1}$$

Es gibt also n verschiedene Werte für die n-te Wurzel

Beispiel:

$$\sqrt[3]{1} = [\cos(0 + 2\pi k) + i.\sin(0 + 2\pi k)]^{\frac{1}{3}} = \cos\left(2\pi\frac{k}{3}\right) + \hat{\imath}.\sin\left(2\pi\frac{k}{3}\right)$$

$k = 0 \qquad \sqrt[3]{1} = \cos(0) + \hat{\imath}.\sin(0) = 1$

$k = 1 \qquad \sqrt[3]{1} = \cos\left(\frac{2\pi}{3}\right) + \hat{\imath}.\sin\left(\frac{2\pi}{3}\right) = -\frac{1}{2} + \hat{\imath}\frac{\sqrt{3}}{2}$

$k = 2 \qquad \sqrt[3]{1} = \cos\left(\frac{4\pi}{3}\right) + \hat{\imath}.\sin\left(\frac{4\pi}{3}\right) = -\frac{1}{2} - \hat{\imath}\frac{\sqrt{3}}{2}$

Die Gleichung
$z^n = a = r.(\cos\varphi + \hat{\imath}.\sin\varphi)$
hat über $\mathbb{C}$ die Nullstellen

$$z = \sqrt[n]{a} = \sqrt[n]{r}.\left[\cos\left(\frac{\varphi}{n} + 2\pi\frac{k}{n}\right) + \hat{\imath}.\sin\left(\frac{\varphi}{n} + 2\pi\frac{k}{n}\right)\right], \quad k = 0,1,\ldots,n-1$$

Es liegt hier ein Sonderfall des „Fundamentalsatzes der Algebra“ vor.

Die Darstellung komplexer Zahlen in der reellen Zahlenebene findet sich bereits 1797 bei Caspar WESSEL (1745-1818), 1806 bei Jean Robert ARGAND (1768-1822), 1831 bei Carl Friedrich GAUSS (1777-1855)

Die Kreisteilungsgleichung

Die Ecken des regelmäßigen n-Ecks, welches dem Einheitskreis eingeschrieben ist, erhält man durch Ausziehen der n-ten *Einheitswurzel*

$$z^n = 1$$

oder durch die Nullstellen der Gleichung

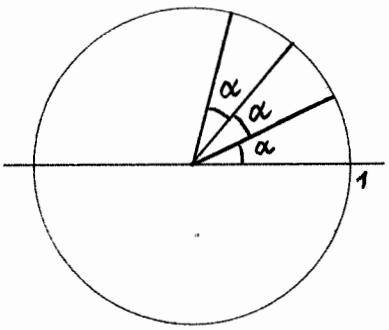
$$z^n - 1 = 0 \qquad (\bullet)$$

Die n-ten Einheitswurzeln lauten dann

$$\boxed{z = cos\left(\frac{2\pi k}{n}\right) + sin\left(\frac{2\pi k}{n}\right) \qquad k = 0,1,2,\ \ldots\ ,n-1}$$

Setzen wir

$$\alpha := \frac{2\pi}{n}$$



so lautet das Ergebnis ausführlich

$z_0 = 1$

$$z_1 = cos\left(\frac{2\pi}{n}\right) + \hat{\imath}.sin\left(\frac{2\pi}{n}\right) = cos\,\alpha + \hat{\imath}.sin\,\alpha$$

$$z_2 = cos\left(2\frac{2\pi}{n}\right) + \hat{\imath}.sin\left(2\frac{2\pi}{n}\right) = cos(2\alpha) + \hat{\imath}.sin(2\alpha)$$

$$\vdots$$

$$z_{n-1} = cos\left((n-1)\frac{2\pi}{n}\right) + \hat{\imath}.sin\left((n-1)\frac{2\pi}{n}\right) = cos[(n-1)\alpha] + \hat{\imath}.sin[(n-1)\alpha]$$

Da 1 für jedes n eine Nullstelle von (•) ist, ist z-1 ein Teiler von (•). Man nennt

$$f(z) = \frac{z^{n-1} - 1}{z - 1} = z^{n-1} + z^{n-2} + z^{n-3} + \ldots + z + 1$$

das *Kreisteilungspolynom* und $f(z) = 0$ die *Kreisteilungsgleichung*

Reziproke Gleichungen geraden Grades

Die Kreisteilungsgleichung ist ein Spezialfall einer *reziproken Gleichung*:

$$z^{2m} + az^{2m-1} + bz^{2m-2} + \ldots + rz^{m+1} \pm sz^m + rz^{m-1} + \ldots + bz^2 + az + 1 = 0$$

Die reziproken Gleichungen haben ihren Namen daher, daß mit jeder Nullstelle z auch $\frac{1}{z}$ eine Nullstelle ist, sodaß man mit jeder bekannten Nullstelle sofort eine weitere angeben kann.

Umformung ergibt

$$\left(z^{2m} + 1\right) + a\left(z^{2m-1} + z\right) + b\left(z^{2m-2} + z^2\right) + \ldots + r\left(z^{m+1} + z^{m-1}\right) \pm sz^m = 0$$

Division durch z^m ergibt

$$\left(z^m + \frac{1}{z^m}\right) + a\left(z^{m-1} + \frac{1}{z^{m-1}}\right) + b\left(z^{m-2} + \frac{1}{z^{m-2}}\right) + \ldots + r\left(z + \frac{1}{z}\right) \pm s = 0 \qquad (\blacklozenge)$$

Setzt man

$$t_k = z^k + \frac{1}{z^k}, \quad \text{speziell } t_0 = 2,\ t_1 = z + \frac{1}{z} =: x$$

so erhält man für die t_k die Rekursionsformel

$$t_k.x = \left(z^k + \frac{1}{z^k}\right).\left(z + \frac{1}{z}\right) = z^{k+1} + \frac{1}{z^{k-1}} + z^{k-1} + \frac{1}{z^{k+1}} = t_{k+1} + t_{k-1}$$

also

$$t_{k+1} = t_k.x - t_{k-1}$$

Daher

$t_0 = 2$

$t_1 = x$

$t_2 = t_1.x - t_o = x^2 - 2$

$t_3 = t_2.x - t_1 = x^3 - 2x - x = x^3 - 3x$

$t_4 = t_3.x - t_2 = x^4 - 3x^2 - x^2 + 2 = x^4 - 4x^2 + 2$

$t_5 = t_4.x - t_4 = x^5 - 4x^3 + 2x - x^3 + 3x = x^5 - 5x^3 + 5x$

$\vdots$

t_k ist also ein Polynom k-ten Grades in x. Setzt man in (♦) ein, so ergibt sich die *Resolvente*

$$t_m + at_{m-1} + bt_{m-2} + \ldots + rt_1 \pm 1 = 0$$

Die Resolvente ist also ein Polynom nur mehr m-ten Grades in x. Kennt man eine Nullstelle z der Resolvente, so folgt aus

$$x = z + \frac{1}{z} \Rightarrow z^2 - x.z + 1 = 0$$

Zur Ermittlung der z sind also nur mehr quadratische Gleichungen zu lösen

Die Lösung einer reziproken Gleichung 2m-ten Grades reduziert sich auf die Lösung der Resolvente m-ten Grades und quadratischer Gleichungen.

Reziproke Gleichungen ungeraden Grades

$$z^{2m+1} + az^{2m} + bz^{2m-1} + \ldots + rz^{m+2} + tz^{m+1} \pm tz^m \pm \ldots \pm bz^2 \pm az \pm 1 = 0$$

Es gelten stets nur die oberen oder nur die unteren Vorzeichen.

Umordnung ergibt

$$\left(z^{2m+1} \pm 1\right) + a\left(z^{2m} \pm z\right) + b\left(z^{2m-1} \pm z^2\right) + \ldots + t\left(z^{m+1} \pm z^m\right) = 0$$

Man erkennt: gelten die Vorzeichen

„+“ $\Rightarrow$ -1 ist Nullstelle $\Rightarrow$ Teilbarkeit durch z + 1

„-„ $\Rightarrow$ +1 ist Nullstelle $\Rightarrow$ Teilbarkeit durch z - 1

In beiden Fällen reduziert sich die Gleichung auf eine reziproke Gleichung geraden Grades.

Die klassischen regelmäßigen Vielecke

Das Problem der Konstruktion regelmäßiger Vielecke reduziert sich auf die Untersuchung der reziproken Kreisteilungsgleichung

$$z^n + z^{n-1} + z^{n-2} + \ldots + z + 1 = 0$$

Durch die Substitution

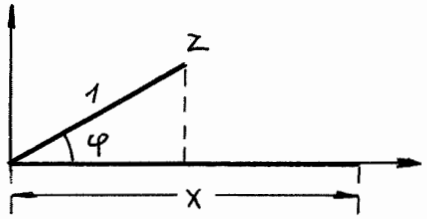
$$x = z + \frac{1}{z}$$

ergibt sich die Resolvente. Sei z eine Nullstelle der Kreisteilungsgleichung , so gilt

$$z = \cos\varphi + \hat{\imath}.\sin\varphi$$

$$\frac{1}{z} = \cos\varphi - \hat{\imath}.\sin\varphi$$

$$z + \frac{1}{z} = 2.\cos\varphi = x$$



Die Resolvente reduziert also das Problem auf das Aufsuchen reeller Zahlen

Es bleibt also noch zu untersuchen, ob die Nullstellen der Resolvente mit Zirkel und Lineal konstruierbar sind. Als bekannte Beispiele wählen wir die klassischen regelmäßigen Vielecke

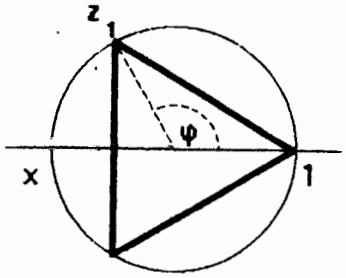
Das gleichseitige Dreieck

n = 3 $z^2 + z + 1 = 0 \mid :z$

$$\left(z + \frac{1}{z} + 1\right) = 0 \Rightarrow x + 1 = 0$$

$$x = -1 = 2\cos\varphi$$

$$\cos\varphi = -\frac{1}{2},\ \varphi = 120°$$



Das Quadrat

n = 4 $z^3 + z^2 + z + 1 = 0$

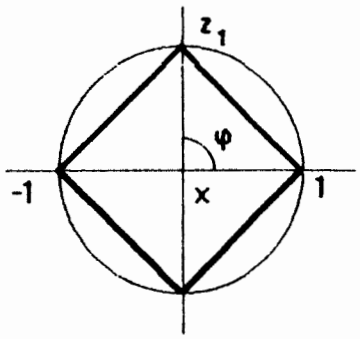
z = -1 ist Nullstelle, daher ist die Gleichung teilbar durch z + 1. Nach HORNER (Seite 6) gilt dann

	1	1	1	1
-1		-1	0	-1
	1	0	1	0

$z^2 + 1 = 0 \mid :z$

$$\left(z + \frac{1}{z}\right) = 0 \Rightarrow x = 0 = 2\cos\varphi$$

$$\cos\varphi = 0,\ \varphi = 90°$$



Das regelmäßige Fünf- und Zehneckeck

$\boxed{n=5}$ $z^4 + z^3 + z^2 + z + 1 = 0 \mid :z^2$

$$\left(z^2 + \frac{1}{z^2}\right) + \left(z + \frac{1}{z}\right) + 1 = 0$$

$$\left(x^2 - 2\right) + x + 1 = 0$$

$$\underline{x^2 + x + 1 = 0} \qquad (*)$$

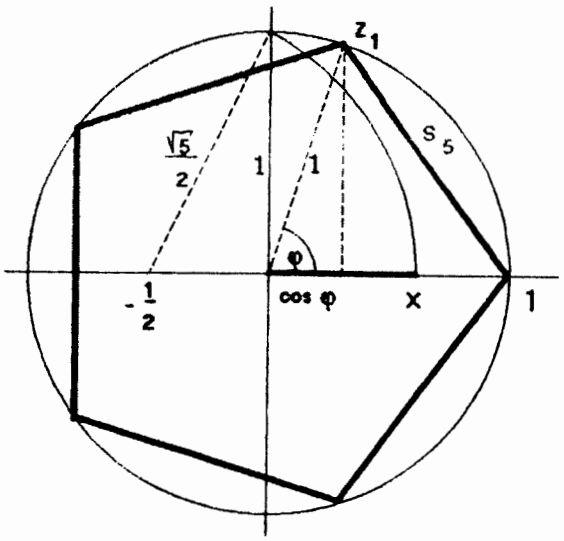
$$x = \frac{-1 \pm \sqrt{5}}{2}$$

$$x_1 = \frac{-1+\sqrt{5}}{2} = 2\cos\varphi_1$$

$$\cos\varphi_1 = \frac{\sqrt{5}-1}{4},\ \varphi_1 = 72°$$

$$x_2 = -\frac{1+\sqrt{5}}{2} = 2\cos\varphi_2$$

$$\cos\varphi_2 = --\frac{\sqrt{5}+1}{4},\ \varphi_2 = 144°$$

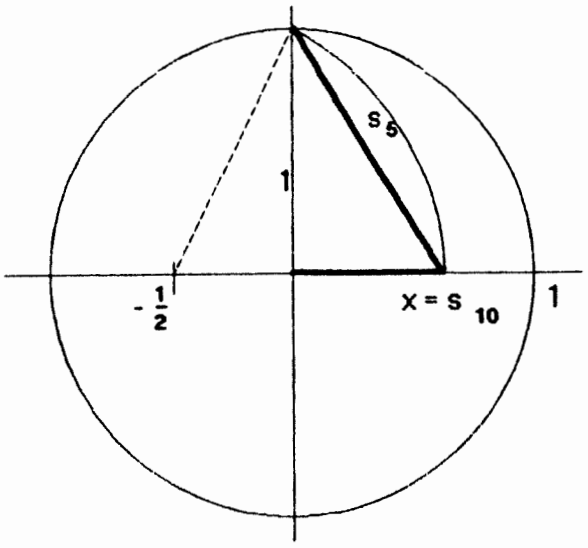


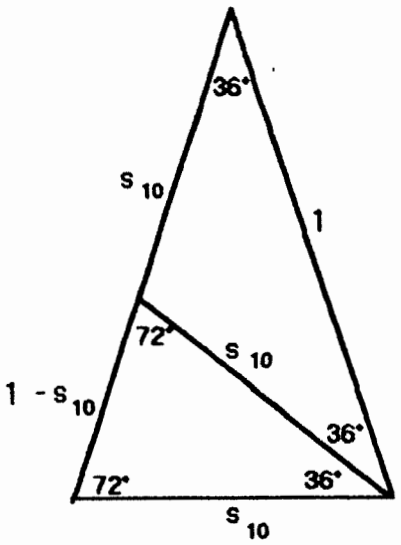
Für die Seite s_5 des regelmäßigen Fünfecks folgt

$$s_5^2 = \sin^2\varphi + (1-\cos\varphi)^2 = \sin^2\varphi + 1 + \cos^2\varphi - 2\cos\varphi = 2 - 2\cos\varphi$$

$$\underline{s_5^2 = 2 - \frac{\sqrt{5}-1}{2} = \frac{5-\sqrt{5}}{2}}$$

Konstruktion der Fünf- und Zehnecksseite





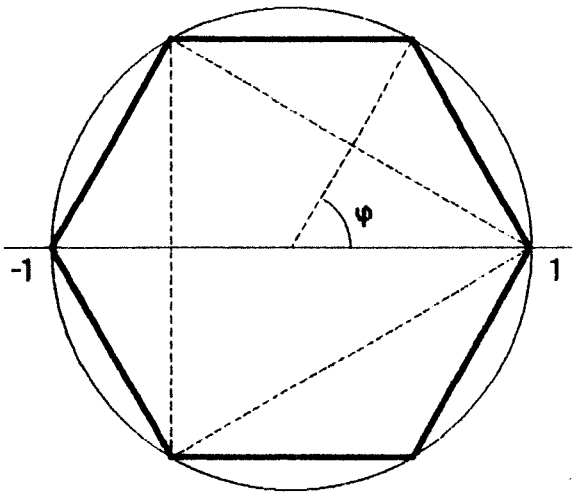
Für die Hypotenuse gilt $1 + x^2 = 1 + \frac{\left(\sqrt{5}-1\right)^2}{4} = 1 + \frac{6-2\sqrt{5}}{4} =$ $= \underline{\frac{10-2\sqrt{5}}{2} = s_5^2}$	$1 : s_{10} = s_{10} : (1 - s_{10})$ $s_{10}^2 = 1 - s_{10} \Rightarrow \underline{s_{10}^2 + s_{10} - 1}$ Das ist aber die Gleichung $(*)$ von $x \Rightarrow$ $\underline{x = s_{10}}$

Das regelmäßige Sechseck

n = 6 $z^5 + z^4 + z^3 + z^2 + z + 1 = 0$

Teilbar durch (z + 1).

	1	1	1	1	1	1
-1		-1	0	-1	0	-1
	1	0	1	0	1	0



$z^4 + z^2 + 1 = 0$

Unter den Ecken des Sechseckes sind die bereits bekannten Ecken des Dreieckes enthalten, die durch $z^2 + z + 1 = 0$ festgelegt sind. Nach HORNER (Seite 6)

	1	0	1	0	1
-1		-1	1	-1	
-1			-1	1	-1
	1	-1	1	0	0

Daher gilt die Zerlegung

$$z^5 + z^4 + z^3 + z^2 + z + 1 = (z+1)(z^2 + z + 1)(z^2 - z + 1)$$

Von Interesse sind nur noch die Nullstellen von

$$z^2 - z + 1 = 0 \mid :z \Rightarrow \left(z + \frac{1}{z}\right) - 1 = 0 \Rightarrow \underline{x - 1 = 0}$$

$$x = 1 = 2\cos\varphi \Rightarrow \cos\varphi = \frac{1}{2} \Rightarrow \underline{\varphi = 60°}$$

Das regelmäßige Siebeneck

n = 7 $z^6 + z^5 + z^4 + z^3 + z^2 + z + 1 = 0 \mid :z^3$

$$\left(z^3 + \frac{1}{z^3}\right) + \left(z^2 + \frac{1}{z^2}\right) + \left(z + \frac{1}{z}\right) + 1 = 0 \Rightarrow$$

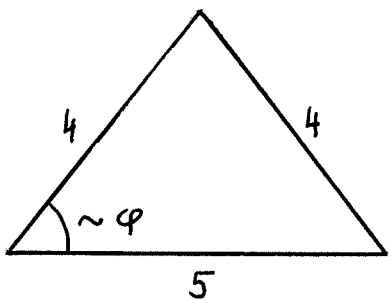
$$(x^3 - 3x) + (x^2 - 2) + x + 1 = 0 \Rightarrow \underline{x^3 + x^2 - 2x - 1 = 0}$$

Wenn diese Gleichung reduzibel wäre, müßte eine Nullstelle ± 1 sein. Da dies nicht der Fall ist, kann x nicht mit Zirkel und Lineal konstruiert werden

Näherungskonstruktion:

$$\varphi = \frac{360°}{7} = 51{,}4258°$$

$$\sim \varphi = 51{,}3178°$$



Anmerkung: Diese Näherungskonstruktion soll bei der Grundlegung der Kathedrale von Chartres verwendet worden sein[1]

[1] Luis CHARPENTIER: Die Geheimnisse der Kathedrale von Chartres, Gaia Verlag Köln 1997[14]

Das regelmäßige Neuneck

$\boxed{n=9}$ $z^8 + z^7 + z^6 + z^5 + z^4 + z^3 + z^2 + z + 1 = 0$

Jedenfalls ist im regelmäßigen Neuneck das regelmäßige Dreieck ($z^2 + z + 1 = 0$) enthalten. Daher muß obige Gleichung reduzibel sein.

	1	1	1	1	1	1	1	1	1
-1		-1	0	0	-1	0	0	-1	
-1			-1	0	0	-1	0	0	-1
	1	0	0	1	0	0	1	0	0

Es gilt also

$z^8 + z^7 + z^6 + z^5 + z^4 + z^3 + z^2 + z + 1 = (z^6 + z^3 + 1)(z^2 + z + 1)$

$$z^6 + z^3 + 1 = 0 \,|: z^3 \Rightarrow \left(z^3 + \frac{1}{z^3}\right) + 1 = 0 \Rightarrow \underline{x^3 - 3x + 1 = 0}$$

Das ist aber die Gleichung für die Dreiteilung des Winkels von 120°, die mit Zirkel und Lineal nicht möglich ist. Das regelmäßige Neuneck ist daher mit Zirkel und Lineal nicht konstruierbar.

Es gibt also mit Zirkel und Lineal konstruierbare und nicht konstruierbare regelmäßige Vielecke.

Es zeigt sich, daß man bei der Frage nach den konstruierbaren Vielecken sich auf Vielecke beschränken kann, deren Eckenanzahl eine Primzahl ist.

Seien nämlich p_1 und p_2 zwei verschiedene Primzahlen. Dann gibt es ganze Zahlen (siehe Seite 5) x und y, sodaß gilt

$$p_1x + p_2y = 1 \qquad (\bullet)$$

Die Zentriwinkel der zugehörigen Vielecke sind dann

$$\alpha_1 = \frac{360°}{p_1}, \quad \alpha_2 = \frac{360°}{p_2}$$

Das p_1p_2-Eck hat dann den Zentriwinkel

$$\alpha = \frac{360°}{p_1p_2}$$

Multipliziert man (•) mit $\frac{360°}{p_1p_2}$, so folgt

$$\frac{360°}{p_2}.x + \frac{306°}{p_1}.y = \frac{360°}{p_1p_2} \Rightarrow \underline{\alpha_2.x + \alpha_1.y = \alpha}$$

Beispiel: Das regelmäßige 15-Eck. $p_1 = 3$, $p_2 = 5$,

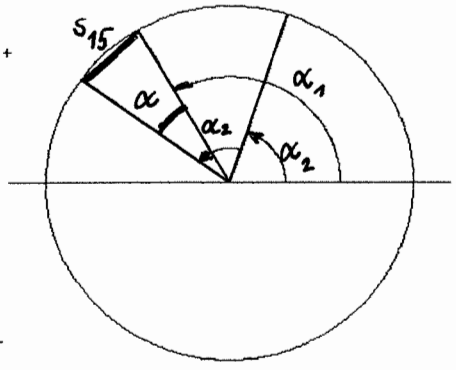
$\alpha_1 = 120°$, $\alpha_2 = 72°$

$3x + 5y = 1$

$x = 2$, $y = -1$

$2\alpha_2 - \alpha_1 = 144° - 120°$

$\underline{\alpha = 24°}$



Nach den bisherigen Ergebnissen lassen sich also Vielecke mit folgenden Eckenzahlen mit Zirkel und Lineal konstruieren:

3, 6, 12, 24, 48, 96, ... 5, 10, 20, 40, 80, ...
4, 8, 16, 32, 64, ... 15, 30, 60, ...

Primitive Einheitswurzeln

Die von 1 verschiedenen Einheitswurzeln von

$$z^n - 1 = (z^{n-1} + z^{n-2} + \ldots + z + 1)(z - 1) = 0$$

haben die Gestalt

$$\varepsilon_0 = 1$$

$$\varepsilon_k = \cos\left(\frac{2\pi}{n}.k\right) + \hat{\imath}.\sin\left(\frac{2\pi}{n}.k\right) \qquad k = 1, \ldots, n-1$$

Jede beliebige Potenz einer beliebigen Einheitswurzel ist wieder eine Einheitswurzel

BW: Es sei ε_k^a die a-te Potenz einer n-ten Einheitswurzel ε_k. Nach EUKLID gilt (Seite 5)

$$a = nq + r$$

daher

$$\varepsilon_k^a = \varepsilon_k^{(nq+r)} = \varepsilon_k^{nq}.\varepsilon_k^r = \left(\varepsilon_k^n\right)^q.\varepsilon_k^r = 1^q.\varepsilon_k^r = \varepsilon_k^r \qquad r < n$$

Dann ist

$$\left(\varepsilon_k^r\right)^n = \left(\varepsilon_k^n\right)^r = 1^r = 1 \Rightarrow \varepsilon_k^r = \varepsilon_m \quad \text{mit geeignetem } m$$

Definition: Eine Einheitswurzel,deren Potenzen alle anderen Einheitswurzeln ergeben, heißt *primitive Einheitswurzel*

Beispiel: Das regelmäßige Sechseck, n = 6

Einheitswurzeln:	ε_1	ε_2	ε_3	ε_4	ε_5
Winkel:	60	120	180	240	300
	$\varepsilon_1^1 = \varepsilon_1$	$\varepsilon_2^1 = \varepsilon_2$	$\varepsilon_3^1 = \varepsilon_3$	$\varepsilon_4^1 = \varepsilon_4$	$\varepsilon_5^1 = \varepsilon_5$
	$\varepsilon_1^2 = \varepsilon_2$	$\varepsilon_2^2 = \varepsilon_4$	$\varepsilon_3^2 = \varepsilon_0$	$\varepsilon_4^2 = \varepsilon_2$	$\varepsilon_5^2 = \varepsilon_4$
	$\varepsilon_1^3 = \varepsilon_3$	$\varepsilon_2^3 = \varepsilon_0$	$\varepsilon_3^3 = \varepsilon_3$	$\varepsilon_4^3 = \varepsilon_0$	$\varepsilon_5^3 = \varepsilon_3$
	$\varepsilon_1^4 = \varepsilon_4$	$\varepsilon_2^4 = \varepsilon_2$	$\varepsilon_3^4 = \varepsilon_0$	$\varepsilon_4^4 = \varepsilon_4$	$\varepsilon_5^4 = \varepsilon_2$
	$\varepsilon_1^5 = \varepsilon_5$	$\varepsilon_2^5 = \varepsilon_4$	$\varepsilon_{31}^5 = \varepsilon_3$	$\varepsilon_4^5 = \varepsilon_2$	$\varepsilon_5^5 = \varepsilon_1$

ε_1 und ε_5 sind primitive Einheitswurzeln

Zu jedem Exponenten n gibt es primitive Einheitswurzeln

BW: Es sei n = st. Dann gilt $z^n - 1 = z^{st} - 1 = 0$. Setzt man $z^t := y$, so folgt

$$z^n - 1 = z^{st} - 1 = y^s - 1 = \left(y^{s-1} + y^{s-2} + \ldots + y + 1\right)(y - 1) = 0$$

d.h. jede Nullstelle von $y - 1 = z^t - 1 = 0$ ist auch Nullstelle von $z^{st} - 1 = z^n - 1 = 0$. Ist α eine Einheitswurzel von $z^t - 1 = 0$, dh. ist $\alpha^t = 1$, so ist zwar (wegen n = st) α auch eine Einheitswurzel von $z^n - 1 = 0$, aber Potenzierung ergibt immer wieder nur Einheitswurzeln von $z^t - 1 = 0$.

Keine Nullstelle von $z^n - 1 = 0$, die bereits einem Polynom geringeren Grades $z^t - 1 = 0$ $(z < n)$ genügt, kann primitive Einheitswurzel von $z^n - 1 = 0$ sein

Daher ist ε_1 sicher stets primitive Einheitswurzel, da sie keiner Gleichung geringeren

Grades genügt und es ist

$$\varepsilon_1^k = \varepsilon_k \quad k = 1, \ldots, n-1$$

Sei nun $\alpha = \varepsilon_1^m = \varepsilon_m$ n-te Einheitswurzel ($\alpha^n = 1$) mit $m < n$, wobei ***ggT***$(m,n) = g$ sei, d.h. es gilt $m = sg$, $n = tg$, wobei (wegen $m < n$) $s < t < n$ ist. Dann gilt

$$\alpha^t = \left(\varepsilon_1^{sg}\right)^t = \left(\varepsilon_1^{gt}\right)^s = \left(\varepsilon_1^n\right)^s = 1^s = 1$$

$\alpha = \varepsilon_1^m$ ist bereits Nullstelle des Polynoms $z^t - 1 = 0$ ($t < n$) niedrigeren Grades, kann daher keine primitive Einheitswurzel von $z^n - 1 = 0$ sein.

> Sind m, n teilerfremd (sonst aber beliebig), so ist
> $$\alpha := \varepsilon_1^m = \varepsilon_m$$
> primitive Einheitswurzel

BW: In der Folge

$$m, 2m, 3m, \ldots, (n-1)m \qquad (\bullet)$$

der Exponenten von α kommen alle Reste $1, 2, \ldots, n-1$ bei Division durch n vor. Wären nämlich für zwei verschiedene $k_1 \neq k_2$ (o.B.d.A. $k_1 < k_2 < n$) die Reste gleich

$$\left.\begin{array}{l} k_1 m = q_1 n + r \\ k_2 m = q_2 n + r \\ \hline (k_2 - k_1).m = (q_2 - q_1).n \end{array}\right\} \Rightarrow \frac{q_2 - q_1}{k_2 - k_1} = \frac{m}{n}$$

Wegen $k_2 - k_1 < n$ wäre der Bruch $\frac{m}{n}$ entgegen der Voraussetzung kürzbar. Die Division der Folge (•) durch n muß daher n -1verschiedene Reste hinterlassen und wegen $k = 1, \ldots, n-1$ sind dies alle möglichen Reste $1, \ldots, (n-1)$.

Es sei für ein beliebiges k: $km = qn + r$, daher

$$\alpha^k = \left(\varepsilon_1^m\right)^k = \varepsilon_1^{km} = \varepsilon_1^{qn+r} = \left(\varepsilon_1^n\right)^q . \varepsilon_1^r = 1^q . \varepsilon_1^r = \varepsilon_r \Rightarrow \underline{\alpha^k = \varepsilon_1^r = \varepsilon_r}$$

α^k durchläuft mit $k = 1, \ldots, (n-1)$ alle n-ten Einheitswurzeln ε_r (allerdings in anderer Reihenfolge). Alle $\alpha = \varepsilon_1^m = \varepsilon_m$ mit *ggT*$(m,n) = 1$ sind primitive Einheitswurzeln

> 1. Ist $n = p$ eine Primzahl, so ist jede von 1 verschiedene Nullstelle von $z^n - 1 = 0$ primitive Einheitswurzel
> 2. Ist $n = p^r$ eine Primzahlpotenz, so hat das Polynom
> $$\frac{z^{p^r} - 1}{z^{p^{r-1}} - 1} = z^{p^r(p-1)} + z^{p^{r-1}(p-2)} + \ldots + z^{p^{r-1}} + 1$$
> als Nullstellen nur primitive Einheitswurzel des Polynoms $z^{p^r} - 1$

BW: 1. Ist $n = p$ eine Primzahl und ε_1 Einheitswurzel von $z^p - 1 = 0$, so ist für jedes $m < p$ der ***ggT***$(m,p) = 1$, daher ist nach obiger Überlegung ε_1^m primitive Einheitswurzel

2. Ist $n = p^r$ Primzahlpotenz, so ist p^{r-1} der größte Teiler von p^r. Jene Nullstellen von $z^{p^r} - 1$, die bereits $z^{p^{r-1}} - 1$ genügen, können also keine primitiven Einheitswurzeln sein. Diese Nullstellen kürzen wir weg. Es verbleiben also nur jene Nullstellen, die nicht auch Nullstellen eines Polynoms geringeren Grades sind. Nun ist

$z^{p^r} = \left(z^{p^{r-1}}\right)^p$. Setzt man $x := z^{p^{r-1}}$, so folgt

$$\frac{z^{p^r}-1}{z^{p^{r-1}}-1} = \frac{x^p-1}{x-1} = x^{p-1}+x^{p-2}+\ldots+x+1 =$$

$$= z^{p^{r-1}(p-1)} + z^{p^{r-1}(p-2)} + \ldots + z^{p^{r-1}} + 1$$

Nachweis der Irreduzibilität der Kreisteilungsgleichung nach PLEMELJ[1]

Es wird sich zeigen, daß es genügt, die beiden Fälle $n = p$ und $n = p^2$ (p Primzahl) zu untersuchen.

Es sei

$$f(z) = \frac{z^p-1}{z-1} = z^{p-1}+z^{p-2}+\ldots+z+1 = 0$$

bzw.

$$f(z) = \frac{z^{p^2}-1}{z^p-1} = z^{p(p-1)} + z^{p(p-2)} + \ldots + z^p + 1 = 0$$

Jede Nullstelle der obigen Polynome ist eine primitive Einheitswurzel. In beiden Fällen gilt für $z = 1$

$$f(1) = p$$

Wäre $f(z)$ über $\mathbb{Q}$ reduzibel, so gäbe es nach dem 2.Lemma von GAUSS zwei Polynome, für die gilt

$$f(z) = g(z).h(z)$$

Für $z = 1$ müßte dann gelten

$$f(1) = g(1).h(1) = p \qquad (\blacklozenge)$$

Wir können o.B.d.A. annehmen, daß $g(z)$ jener irreduzible Teiler von $f(z)$ ist, für den gilt $g(1) = \pm p$. Dann muß $h(1) = \pm 1$ sein. Denn wegen ($\blacklozenge$) muß genau einer der Faktoren den Wert $\pm p$ haben.

Jede primitive Einheitswurzel ist Potenz irgend einer anderen primitiven Einheitswurzel. Seien etwa α und β primitive Einheitswurzeln von $f(z)$, so gibt es ein k mit

$$\beta = \alpha^k$$

Ferner muß gelten

$$f(\alpha) = g(\alpha).h(\alpha) = 0 \text{ und } f(\beta) = g(\beta).h(\beta) = 0$$

Ist etwa $g(\alpha) = 0$, $g(\beta) \neq 0$, so muß es ein geeignetes k geben, für welches $h(\alpha^k) = 0$ ist. Die beiden Polynome $g(z)$ und $h(z^k)$ haben daher eine gemeinsame Nullstelle. Da $g(z)$ irreduzibel ist, muß nach dem Hauptsatz für irreduzible Polynome gelten $h(z^k) = g(z).l(z)$. Für $z = 1$ würde dann folgen

$$\pm 1 = \pm p.l(1) \quad \text{Widerspruch!}$$

Der Kreisteilungskörper

Ist p eine Primzahl, so ist das Kreisteilungspolynom

$$f(z) = z^{p-1} + z^{p-2} + \ldots + z + 1$$

über $\mathbb{Q}$ irreduzibel. Sei ε eine beliebige Nullstelle von $f(z)$, dann gilt

$$\varepsilon^{p-1} + \varepsilon^{p-2} + \ldots + \varepsilon + 1 = 0 \qquad (*)$$

[1] Josip PLEMELJ (1873-1967) 1933

Durch Adjunktion von ε zu $\mathbb{Q}$ entsteht der Kreisteilungskörper

$$\mathbb{Q}[\varepsilon] \subset \mathbb{C}$$

Das allgemeine Element von $\mathbb{Q}[\varepsilon]$ hat dann die Bauart

$$\frac{g(\varepsilon)}{h(\varepsilon)} \qquad grd\ g,\ grd\ h < p-1$$

wobei $g(\varepsilon)$ und $h(\varepsilon)$ Polynome in ε mit Koeffizienten ausm $\mathbb{Q}$ sind, deren Grade kleiner als p-1 sind. Wegen (*) läßt sich nämlich jedes Polynom in ε auf ein Polynom höchstens (p-1)-ten Grades reduzieren. Ferner kann ε nicht Nullstelle von $h(z)$ sein. Wäre nämlich $h(\varepsilon) = 0$, so hätten $f(z)$ und $h(z)$ gemeinsame Nullstellen in $\mathbb{Q}[\varepsilon]$. Da $f(z)$ über irreduzibel ist, müßte nach dem Hauptsatz über irreduzible Polynome $f(z)$ ein Teiler von $h(z)$ sein. Da dies wegen $grd\ h < grd\ f$ unmöglich ist, sind $h(z)$ und $f(z)$ teilerfremd. Es gibt daher zwei Polynome $a(z)$ und $b(z)$, sodaß gilt (siehe Seite 5)

$$a(z).h(z) + b(z).f(z) = 1$$

daher

$$a(\varepsilon).h(\varepsilon) + b(\varepsilon).f(\varepsilon) = 1 \Rightarrow a(\varepsilon).h(\varepsilon) = 1 \Rightarrow \frac{1}{h(\varepsilon)} = a(\varepsilon)$$

Demnach läßt sich das allgemeine Element des Kreisteilungskörpers in der Gestalt

$$g(\varepsilon).a(\varepsilon) =: k(\varepsilon)$$

darstellen. Nach EUKLID (Seite 5) gilt nun für das Polynom $k(z)$

$$k(z) = q(z)f(z) + r(z) \qquad grd\ r < grd$$

demnach

$$k(\varepsilon) = q(\varepsilon).\underbrace{f(\varepsilon)}_{0} + r(\varepsilon)$$

> Jedes Element ≠ 0 des Kreisteilungskörpers hat die Gestalt
> $$r(\varepsilon) = \mu_0 + \mu_1\varepsilon + \mu_2\varepsilon^2 + \ldots + \mu_{p-2}\varepsilon^{p-2}$$
> mit einem geeignet gewählten Polynom r über $\mathbb{Q}$ mit $grd\ r < (p-1)$.
> Das Polynom $r(z)$ ist eindeutig bestimmt

BW indirekt: Es sei $r'(z)$ein zweites Polynom mit $grd\ r' < (p-1)$ und

$$r'(\varepsilon) = r(\varepsilon) \Rightarrow r'(\varepsilon) - r(\varepsilon) = 0$$

Für das Polynom $r''(z) := r'(z) - r(z)$ gilt dann gleichfalls $grd\ r'' < (p-1)$ und $r''(\varepsilon) = 0$. Da ε einem Polynom kleineren Grades als dem Kreisteilungspolynom nicht genügen kann, muß $r''(z)$ das Nullpolynom sein, woraus folgt $r'(z) = r(z)$.

Es gilt aber auch folgende Darstellung

> Jedes Element ≠ 0 des Kreisteilungskörpers läßt sich eindeutig in der Gestalt
> $$s(\varepsilon) = \lambda_1\varepsilon + \lambda_2\varepsilon^2 + \ldots + \lambda_{p-1}\varepsilon^{p-1}$$
> darstellen (kein absolutes Glied!)

BW: Es sei

$$\begin{array}{l} r(\varepsilon) = \mu_0 + \mu_1\varepsilon + \mu_2\varepsilon^2 + \ldots + \mu_{p-2}\varepsilon^{p-2} \\ \underline{f(\varepsilon) = 1 + \varepsilon + \varepsilon^2 + \ldots + \varepsilon^{p-2} + \varepsilon^{p-1} = 0 \quad \Big| -\mu_0} \\ s(\varepsilon) = r(\varepsilon) - \mu_0 f(\varepsilon) = \underbrace{(\mu_1 - \mu_0)}_{\lambda_1}\varepsilon + \underbrace{(\mu_2 - \mu_0)}_{\lambda_2}\varepsilon^2 + \ldots + \underbrace{(\mu_{p-2} - \mu_0)}_{\lambda_{p-2}}\varepsilon^{p-2} \underbrace{- \mu_0}_{\lambda_{p-1}}\varepsilon^{p-1} \end{array}$$

also

$$s(\varepsilon) = \lambda_1\varepsilon + \lambda_2\varepsilon^2 + \ldots + \lambda_{p-1}\varepsilon^{p-1}$$

Sei

$$s'(\varepsilon) = \lambda_1'\varepsilon + \lambda_2'\varepsilon^2 + \ldots + \lambda_{p-1}'\varepsilon^{p-1}$$

eine zweite Darstellung mit $s'(\varepsilon) = s(\varepsilon)$, so ist

$$s'(\varepsilon) - s(\varepsilon) = (\lambda_1' - \lambda_1)\varepsilon + \ldots + (\lambda_{p-1}' - \lambda_{p-1})\varepsilon^{p-1} = 0 \quad | : \varepsilon$$

$$= (\lambda_1' - \lambda_1) + \ldots + (\lambda_{p-1}' - \lambda_{p-1})\varepsilon^{p-2} = 0 = s''(\varepsilon)$$

d.h. ε wäre wieder Nullstelle eines Polynoms geringeren Grades als $f(z)$, was der Irreduzibilität von $f(z)$ widerspricht. Daher muß $s''(z)$das Nullpolynom sein und es ist $s'(z) = s(z)$.

Hilfsmittel aus der Zahlentheorie

Die Kongruenzrelation

Zwei ganze Zahlen heißen *kongruent bezüglich des Moduls* $m \in \mathbb{N}^*$, wenn ihre Differenz durch m teilbar ist.

$$a \equiv b \,(\textit{mod}\, m) \Leftrightarrow m|(a-b) \Leftrightarrow a = q_1 m + r \wedge b = q_2 m + r$$

Die Kongruenz ist eine Äquivalenzrelation über der Menge $\mathbb{Z}$ der ganzen Zahlen. Zwei Zahlen gehören derselben Äquivalenzklasse an, wenn sie bei Division durch den Modul m denselben Rest r hinterlassen. Da es bezüglich des Moduls m die Reste {0,1,2, ... , m-1} gibt, wird die Menge $\mathbb{Z}$ in m Äquivalenzklassen (Restklassen) eingeteilt.
Es gelten folgende Rechenregeln

$$\left.\begin{array}{l} a \equiv b(\textit{mod}\, m) \\ c \equiv d(\textit{mod}\, m) \end{array}\right\} \Rightarrow \left.\begin{array}{c} a \pm c \equiv b + d(\textit{mod}\, m) \\ ac \equiv bd(\textit{mod}\, m) \end{array}\right\}$$

BW: Nachrechnen

Es gilt aber speziell

$a \equiv b \,(\textit{mod}\, m) \Rightarrow ac \equiv bc \,(\textit{mod}\, m)$
Die Umkehrung gilt jedoch nicht
$[ac \equiv bc \,(\textit{mod}\, m) \Rightarrow a \equiv b \,(\textit{mod}\, m)] \Leftrightarrow \textit{ggT}(m,c) = 1$

BW: Es sei $ac \equiv bc \,(\textit{mod}\, m) \Rightarrow (a-b)c = \lambda m$

Daraus folgt m | (a - b) nur dann, wenn m und c teilerfremd sind. Wäre nämlich $\textit{ggT}(m,c) = t \neq 1$, sowäre m = m't, c = c't mit teilerfremden m' und c'. Dann folgt aus

$$(a-b)c = \lambda m \Rightarrow (a-b)c't = \lambda m't \Rightarrow (a-b)c' = \lambda m'$$

Aus der Teilerfremdheit von c' und m' folgt m' | (a-b). Daher

$$ac \equiv bc(\textit{mod}\, m) \wedge \textit{ggT}(c,m) = t \Rightarrow a \equiv b\left(\textit{mod}\, \frac{m}{t}\right)$$

Der „kleine" Satz von FERMAT[1]

Ist p eine Primzahl und $x \in \mathbb{N}^*$ mit $\textit{ggT}(p,x) = 1$, so gilt

$$x^{p-1} \equiv 1 \,(\textit{mod}\, p)$$

Allgemeiner gilt für beliebige $x \in \mathbb{N}$

$$x^p \equiv x \,(\textit{mod}\, p)$$

BW Des Satzes durch Induktion über x.

Induktionsannahme: Für jedes x ist $x^p - x$ durch p teilbar

Induktionsanfang: Die Behauptung gilt für x = 0 und x = 1

Induktionsbeweis: Es ist.z.z.: $p|\left((x+1)^p - (x+1)\right)$

Es gilt (Binomischer Lehrsatz):

$$(x+1)^p = x^p + px^{p-1} + \frac{p(p-1)}{2!}x^{p-2} + \ldots + \frac{p(p-1)\cdots 1}{(p-1)!}x + 1 \Rightarrow$$

$$\Rightarrow (x+1)^p - (x^p + 1) = px\left[x^{p-2} + \ldots + 1\right]$$

[1] Pierre FERMAT (1601-1655) 1640

Die letzte Differenz ist durch p teilbar. Da nach Induktionsannahme $x^p - x$ durch p teilbar ist, ist auch die Summe

$$(x+1)^p - (x^p + 1) + (x^p - x) = (x+1)^p - (x+1)$$

durch p teilbar, d.h

$$(x+1)^p \equiv (x+1) \ (mod\ p)$$

Es gilt also allgemein $x^p \equiv x \ (mod\ p)$. Ist nun $ggT(x,p) = 1$, so kann man durch x kürzen und erhält $x^{p-1} \equiv 1 \ (mod\ p)$

Kongruenzen mit Polynomen

Definition: Es seien $f(x)$ und $g(x)$ zwei Polynome mit ganzzahligen Koeffizienten. Man sagt

$$f(x) \equiv g(x) \ (mod\ p)$$

wenn alle Koeffizienten von $f(x) - g(x)$ durch p teilbar sind (p Primzahl). Ist

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 \qquad a_i \in \mathbb{Z}$$

so ist $grd\, f$ modulo p der höchste Exponent, dessen zugehöriger Koeffizient nicht durch p teilbar ist.

Beispiel: $f(x) = 15x^3 + 9x^2 + 16$

$grd\, f = 3 \ (mod\ 7)$ $\qquad f(x) \equiv x^3 + 2x^2 + 2 \ (mod\ 7)$

$grd\, f = 2 \ (mod\ 5)$ $\qquad f(x) \equiv 4x^2 + 1 \ (mod\ 5)$

$grd\, f = 0 \ (mod\ 3)$ $\qquad f(x) \equiv 1 \ (mod\ 3)$

Jedes $x \in \mathbb{Z}$, für welches gilt

$$f(x) \equiv 0 \ (mod\ p) \Leftrightarrow p \mid f(x)$$

heißt *Nullstelle modulo* p der gegebenen Kongruenz

Es gilt

x	0	1	2	3	4	5	6
$f(x)$	16	40	172	502	1120	2116	3580

In obigem Beispiel hat $f(x)$ daher folgende Nullstellen

$(mod\ 7)$ $\quad x = 4$ (wegen $1120 = 160.7$)

$(mod\ 5)$ $\quad x = 1, x = 4$

$(mod\ 3)$ $\quad$ keine Nullstelle

Hat die Kongruenz

$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 \ (mod\ p)$

mehr als n inkongruente Nullstellen, so sind alle Koeffizienten von $f(x)$ durch p teilbar.

BW: Es seien $n + 1$ Werte $x_1, x_2, \ldots, x_n, x_{n+1} \in \mathbb{Z}$ gegeben, deren Funktionswerte sämtlich durch p teilbar sind. Es ist z.z., daß dann alle a_i durch p teilbar sind.

Zum Nachweis stellen wir $f(x)$ in folgender Gestalt dar:

$$f(x) = b_0 + b_1(x - x_1) + b_2(x - x_1)(x - x_2) + b_3(x - x_1)(x - x_2)(x - x_3) + \ldots +$$
$$+ b_{n-2}(x - x_1)\cdots(x - x_{n-2}) + b_{n-1}(x - x_1)\cdots(x - x_{n-1}) + b_n(x - x_1)\cdots(x - x_{n-1})(x - x_n)$$

Die n+ 1 Größen lassen soch berechnen, da die n + 1 Funktionswerte $f(x_1), \ldots f(x_{n-1})$ bekannt sind. Es gilt nämlich

$f(x_1) = b_0 \qquad p \mid f(x_1) \Rightarrow \boxed{p \mid b_0}$

$f(x_2) = b_0 + b_1(x_2 - x_1)$ Es gilt $p \mid f(x_2)$ und $p \mid b_0$. Da wegen der Inkongruenz von x_1 und x_2 die Differenz $(x_2 - x_1)$ nicht durch p teilbar ist folgt $\boxed{p \mid b_1}$

$f(x_3) = b_0 + b_1(x_3 - x_1) + b_2(x_3 - x_1)(x_3 - x_2) \Rightarrow \boxed{p \mid b_2}$

:

$f(x_n) = b_0 + b_1(x_n - x_1) + \ldots + b_{n-1}(x_n - x_1)\ldots(x_n - x_{n-1}) \Rightarrow \boxed{p \mid b_{n-1}}$

$f(x_{n+1}) = b_0 + b_1(x_{n+1} - x_1) + \ldots + b_n(x_{n+1} - x_1)\ldots(x_{n+1} - x_n) \Rightarrow \boxed{p \mid b_n}$

Vergleichen wir nun die Koeffizienten von x^i in den beiden Darstellungen von $f(x)$

$a_n = b_n \quad p|b_n \Rightarrow \boxed{p|a_n}$

$a_{n-1} = b_{n-1} + b_n . h_n(x_i) \quad p|b_{n-1}, b_n \Rightarrow \boxed{p|a_{n-1}}$ Hier sind die $h_n(x_i)$ gewisse Funktionen der x_i

:

$$a_i \equiv 0 (mod\ p)$$

Korollar: Ein Polynom n-ten Grades modulo p, dessen Koeffizienten nicht alle durch p teilbar sind, hat höchstens n modulo p inkongruente Nullstellen.

Primitivreste einer Primzahl

Betrachet man die Reste 1,2, ... , p -1 einer Primzahl p, so gilt für jeden Rest x nach FERMAT

$$x^{p-1} \equiv 1 \ (mod\ p)$$

Man erkennt, daß für manche Reste x bereits ein kleinerer Exponent als p - 1 genügt, um eine zu 1 kongruente Potenz zu erhalten.

Definition: Es sei x einer der Reste 1, ... , p -1 der Primzahl p. Dann gilt $ggT(x,p) = 1$. Die kleinste natürliche Zahl a, für welche für ein gegebenes x gilt

$$x^a \equiv 1 \ (mod\ p)$$

heißt *Ordnung von* x (mod p)

$$a = ord\ x \ (mod\ p)$$

Jene Reste von x, deren Ordnun p -1 ist, heißen *Primitivreste* von p.

Zu jeder Primzahl gibt es Primitivreste. Zum Nachweis benötigen wie einige Hilfssätze

Hilfssatz 1: Ist $ord\ x = \delta \ (mod\ p)$ $(1 \le x \le p-1)$, so sind die Potenzen $x^1, x^2, \ldots, x^\delta \ (mod\ p)$ inkongruent

BW indirekt: Es sei $x^\alpha \equiv x^\beta \ (mod\ p)$, $\beta < \alpha \le \delta$. Dann gilt $x^{\alpha-\beta} \equiv 1 \ (mod\ p)$ mit $\alpha - \beta < \delta$. Dies ist ein Widerspruch, danach Voraussetzung δ der kleinste Exponent ist.

Hilfssatz 2: Ist $ord\ x = \delta \ (mod\ p)$, so gilt $x^\alpha \equiv x^\beta \ (mod\ p)$ genau dann, wenn $\alpha \equiv \beta \ (mod\ \delta)$

BW: 1.Es sei $\alpha = \delta q + r \qquad r < \delta$

$\beta = \delta q_1 + r_1 \qquad r_1 < \delta$

Dann folgt aus der Voraussetzung $x^\delta \equiv 1 \ (mod\ p)$

$$x^\alpha \equiv x^{\delta q + r} \equiv \left(x^\delta\right)^q . x^r \equiv x^r \ (mod\ p)$$

$$x^\beta \equiv x^{\delta q_1 + r_1} \equiv \left(x^\delta\right)^{q_1} . x^{r_1} \equiv x^{r_1} \ (mod\ p)$$

Daher

$$x^\alpha \equiv x^\beta \ (mod\ p) \Rightarrow x^r \equiv x^{r_1} \ (mod\ p)$$

Nach Hilfssatz 1 sind x^r und x^{r_1} für verschiedene Exponenten r und r_1 inkongruent (mod p). Daher muß $r = r_1$ sein, α und β hinterlasssen also bei Division durch δ gleiche Reste. Daher $\alpha \equiv \beta \ (mod\ \delta)$

2. Ist umgekehrt

$$\alpha \equiv \beta \ (mod\ \delta) \Rightarrow \alpha - \beta = c\delta \Rightarrow x^{\alpha-\beta} \equiv x^{c\delta} \equiv \left(x^\delta\right)^c \equiv 1 (mod\ p) \Rightarrow x^\alpha \equiv x^\beta \ (mod\ p)$$

Hilfssatz 3: Ist $ord\ x = \delta \ (mod\ p)$, so gilt $x^\alpha \equiv 1 \ (mod\ p)$ genau dann, wenn $\delta | \alpha$

BW: Ist $\beta = 0$, so folgt nach Hilfssatz 2:

$$\alpha \equiv 0 \ (mod\ \delta) \Leftrightarrow \delta | \alpha \wedge x^\alpha \equiv x^\beta \equiv x^0 \equiv 1 (mod\ p)$$

Hilfsatz 4: Ist δ die Ordnung eines Elements modulo p, so gilt $\delta | (p-1)$

BW: Ist $x^{\delta} \equiv 1 \equiv x^{p-1} \,(mod\, p)$, so folgt aus dem Hilfssatz 2:

$$p-1 \equiv \delta \,(mod\, \delta) \Rightarrow p-1 \equiv 0 \,(mod\, \delta) \Rightarrow \delta \mid (p-1)$$

Hilfssatz 5: Ist ***ord*** $x = \alpha.\beta$, so ist ***ord*** $x^{\alpha} \equiv \beta \,(mod\, p)$

BW: Es sei $ord\left(x^{\alpha}\right) =: \delta \,(mod\, p)$. Dann gilt $\left(x^{\alpha}\right)^{\delta} \equiv x^{\alpha\delta} \equiv 1 (mod\, p)$. Nach Hilfssatz 3 muß die Ordnung $\alpha.\beta$ von x den Exponenten $\alpha.\delta$ von x teilen:

$$\alpha.\beta \mid \alpha.\delta \Rightarrow \beta \mid \delta$$

Anderseits gilt auch

$$x^{\alpha\beta} = \left(x^{\alpha}\right)^{\beta} \equiv 1 (mod\, p)$$

Daher muß die Ordnung δ von x^{α} den Exponenten β von x^{α} teilen:

$$\delta \mid \beta \Rightarrow \underline{\delta = \beta}$$

Hilfssatz 6: Ist ***ord*** $x = \alpha$ (***mod*** p), und ***ord*** $y = \beta$ (***mod*** p) und sind α und β teilerfremd, so ist ***ord*** $(x.y) = \alpha.\beta$ (***mod*** p)

BW: Es sei ***ord*** $(x.y) =: \delta$ (***mod*** p) $\Rightarrow (x.y)^{\delta} \equiv 1 \,(mod\, p) \Rightarrow (x.y)^{\delta\beta} \equiv \underline{x^{\delta\beta}.y^{\delta\beta} \equiv 1 \,(mod\, p)}$

Definitionsgemäß gilt

$$y^{\beta} \equiv 1 (mod\, p) \Rightarrow y^{\delta\beta} \equiv 1 (mod\, p) \Rightarrow \underline{x^{\delta\beta} \equiv 1 (mod\, p)}$$

Ferner gilt nach Voraussetzung $x^{\alpha} \equiv 1$ (***mod*** p) , daher nach Hilfssatz 3:

$$\alpha \mid \delta.\beta \Rightarrow \underline{\alpha \mid \delta} \text{ (wegen } ggT(\alpha,\beta) = 1)$$

Analog

$$\underline{\beta \mid \delta}$$

Aus der Teilerfremdheit von α und β folgt weiter

$$\alpha.\beta \mid \delta$$

Anderseits gilt

$$\left.\begin{array}{l} x^{\alpha} \equiv 1 (mod\, p) \Rightarrow x^{\alpha\beta} \equiv 1 (mod\, p) \\ y^{\beta} \equiv 1 (mod\, p) \Rightarrow y^{\alpha\beta} \equiv 1 (mod\, p) \end{array}\right\} \Rightarrow (x.y)^{\alpha\beta} \equiv 1 \,(mod\, p)$$

Nach Hilfssatz 3 gilt weiter

$$\delta \mid \alpha.\beta \Rightarrow \underline{\delta = \alpha.\beta}$$

Wir können nun den Satz beweisen

Zu jeder Primzahl p existieren Primitivreste

BW:

$$\{\delta_1, \delta_2, \ldots, \delta_s\} \qquad (1)$$

sei die Menge der Ordnungen der modulo p auftretenden Reste 1,2, ... ,(p-1) und

$$\tau := kgV\left(\delta_{1,}, \delta_2, \ldots \delta_s\right) \qquad (2)$$

das *kleinste gemeinsame Vielfache* aller Ordnungen. Für jede Ordnung δ_j und die Anzahl s der Ordnungen gilt

$$\delta_j \leq (p-1) \text{ und } s \leq (p-1)$$

Zu jeder Ordnung δ_j gehört also mindestens ein Rest modulo p. Die Primzahlzerlegung von τ sei

$$\tau = q_1^{\alpha_1}.q_2^{\alpha_2} \ldots q_k^{\alpha_k} \qquad q_1, q_2, \ldots, q_k \text{ Primzahlen} \qquad (3)$$

Zu jedem Exponenten α_i $(1 \leq i \leq k)$ muß es dann ein δ_j aus der Menge (1) geben, das $q_i^{\alpha_i}$ als Faktor enthält und das demnach die Gestalt

$$\delta_j = q_i^{\alpha_i}.c_j$$

hat. Ist y_j ein Rest mit der Ordnung δ_j, dann gilt

$$y_j^{\delta_j} \equiv y_k^{q_i^{\alpha_i}.c_j} \equiv \left(y_j^{c_j}\right)^{q_i^{\alpha_i}} \equiv 1 \,(\mathit{mod}\, p)$$

Nach Hilfssatz 5 hat daher

$$x_j := y_j^{c_j} \quad \text{die Ordnung} \quad q_i^{\alpha_i}$$

Es seien nun $x_1, \ldots, x_k$ Elemente mit den Ordnungen $q_1^{\alpha_1}, \ldots, q_k^{\alpha_k}$ und g das Element

$$g := x_1.x_2 \ldots x_k$$

Dann hat g nach Hilfssatz 6

$$\mathit{ord}\, g = q_1^{\alpha_1} \ldots q_k^{\alpha_k} = \tau \Rightarrow g^{\tau} \equiv 1 (\mathit{mod}\, p)$$

da die $q_i^{\alpha_i}$ untereinander teilerfremd sind.

Nun hat jeder der Reste $x \in \{1, \ldots, p-1\}$ eine der Ordnungen δ_j von (1). Da alle δj Teiler von τ sind gilt $\tau = \gamma_j \delta_j$, daher

$$x^{\tau} = \left(x^{\delta_j}\right)^{\gamma_j} \equiv 1 (\mathit{mod}\, p)$$

wobei x ein beliebiger Rest ist. Daher hat die Polynomkongruenz

$$f(x) = x^{\tau} - 1 \equiv 0 \,(\mathit{mod}\, p) \qquad (4)$$

$(p - 1)$ inkongruente Nullstellen modulo p. Da die Koeffizienten von (4) nicht durch p teilbar sind, können höchstens τ inkongruente Nullstellen auftreten. es gilt daher

$$p - 1 \leq \tau \qquad (5)$$

Es war aber

$$\mathit{ord}\, g = \tau \,(\mathit{mod}\, p)$$

Anderseits gilt

$$g^{p-1} = (x_1 \ldots x_k)^{p-1} = x_1^{p-1} \ldots x_k^{p-1} \equiv 1 (\mathit{mod}\, p)$$

da die x_i Reste modulo p sind und daher dem Satz von FERMAT genügen. Daher gilt nach Hilfssatz 3

$$\tau | (p - 1)$$

Aus

$$\tau = p - 1 \Rightarrow \underline{g \text{ ist Primitivrest}}$$

Die Theorie regelmäßiger Vielecke nach GAUSS

FERMATsche Primzahlen[1]

Es genügt, regelmäßige Vielecke zu betrachten, deren Eckenzahl eine Primzahl p oder eine Primzahlpotenz p^α ist.

Es wird sich zeigen, daß für $p \neq 2$ ein p^2-Eck nicht konstruierbar ist, daher kann auch ein p^α-Eck nicht konstruierbar sein. Wäre namlich das p^α-Eck konstruierbar, dann wäre auch (durch Auslassung von jeweils $p^{\alpha-2}$ Ecken) das p^2-Eck konstruierbar.

Wie bereits gezeigt, sind für jede Primzahl p die Polynome

$$f(z) = \frac{z^p - 1}{z - 1} = z^{p-1} + z^{p-2} + \ldots + z + 1 = 0 \qquad (1)$$

bzw.

$$f(z) = \frac{z^{p^2} - 1}{z^p - 1} = z^{p(p-1)} + z^{p(p-2)} + \ldots + z^p + 1 = 0 \qquad (2)$$

über $\mathbb{Q}$ irreduzibel.

Zur Konstruierbarkeit der Nullstellen von $f(z)$ mit Zirkel und Lineal ist notwendig (aber nicht hinreichend), daß die Ordnung von $f(z)$ eine Potenz von 2 ist.

Wir betrachten zunächst Gleichung (2). Dann muß gelten

$$p(p - 1) = 2^h$$

Ist $p \neq 2$, so ist $p(p - 1)$ sicher keine Potenz von 2.

> p^α-Ecke sind mit Zirkel und Lineal nur konstruierbar, wenn $p = 2$ ist.

Wir betrachten nun Gleichung (1). Dann muß sein

$$p - 1 = 2^h \Rightarrow \underline{p = 2^h + 1}$$

<u>Ist $p = 2^h + 1$ eine Primzahl, so kann h keine ungerade Zahl als Teiler enthalten</u>

<u>BW indirekt:</u> Es sei $h = h_1(2r + 1)$. Dann gilt

$$p = 2^h + 1 = 2^{h_1(2r+1)} + 1$$

Setzt man $x := 2^{h_1}$, so folgt

$$p = x^{2r+1} + 1 = (x + 1)(x^{2r} - x^{2r-1} + x^{2r-2} \mp \ldots - x + 1)$$

p wäre dann keine Primzahl!

> Zu Konstrierbarkeit des regelmäßigen p-Ecks ist notwendig, daß p eine Primzahl der Gestalt
>
> $$p = 2^h + 1, \; h = 2^\mu$$
>
> ist (FERMATsche Zahl)

[1] FERMAT, Pierre (1601-1665)

μ	$2^{2^\mu}+1$	
0	3	Primzahlen
1	5	
2	17	
3	257	
4	65537	
5	4294967297 = 641.6700417	(EULER 1732)
6	18446744073709551617 = 274177.67280421310721	(LANDRY 1880)
⋮	⋮	??? Bisher keine weiteren Primzahlen gefunden
⋮	⋮	

Wir können nunmehr beweisen

> Notwendig und hinreichend für die Konstruierbarkeit eines regelmäßigen p-Ecks ist, daß p ein Primzahl der Gestalt
> $$p = 2^h + 1, \quad h = 2^\mu$$
> ist

Äquivalent dazu ist die Aussage

> Das irreduzible Polynom
> $$z^{p-1} + z^{p-2} + \ldots + z + 1 \quad (p = 2^h + 1, h = 2^\mu)$$
> ist durch Quadratwurzelausdrücke lösbar.

GAUSSsche Perioden

Die von 1 verschiedenen Einheitswurzeln lauten

$$\alpha := \frac{2\pi}{p}$$

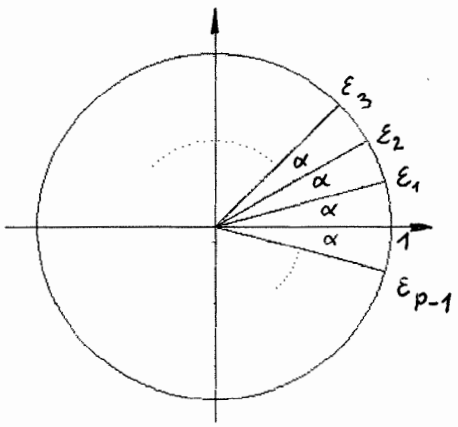
$$\varepsilon_1 = \cos\alpha + \hat{\imath}.\sin\alpha$$

$$\vdots$$

$$\varepsilon_r = \cos(r\alpha) + \hat{\imath}.\sin(r\alpha)$$

$$\vdots$$

$$\varepsilon_{p-1} = \cos[(p-1)\alpha] + \hat{\imath}.\sin[(p-1)\alpha]$$



Nach MOIVRE (Seite 24)gilt

$$\varepsilon_r = \varepsilon_1^r$$

Da ε_1 primitive Einheitswurzel ist, erhält man alle anderen Einheitswurzeln durch Potenzieren aus ε_1.

Wie gezeigt wurde, ist jede zu einer Primzahl p gehörige Einheitswurzel eine primitive Einheitswurzel (Seite 34). Daher kann man eine beliebige p-te Einheitswurzel ε auswählen. Die Potenzen

$$\varepsilon, \varepsilon^2, \ldots, \varepsilon^{p-1}$$

stellen die Einheitswurzeln

$$\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{p-1}$$

nur in anderer Reihenfolge dar. Wie gezeigt wurde, gilt für

$$k \neq l \wedge k,l, < p \text{ stets } \varepsilon^k \neq \varepsilon^l$$

Wie ferner gezeigt wurde (Seite 41), existiert unter den Resten einer Primzahl stets ein Primitivrest g, dessen Potenzen

$$g^1, g^2, g^3, \ldots g^{p-1}$$

kongruent zu den Resten 1, ... , p (*mod* p) sind, nur in anderer Reihenfolge.
Nach FERMAT gilt

$$g^p \equiv g \ (mod\ p)$$

Wir wählen nun eine beliebige Nullstelle ε von $f(z) = z^{p-1} + z^{p-2} + \ldots + z + 1$ und bilden die Potenzen

$$\varepsilon^{g^1}, \varepsilon^{g^2}, \varepsilon^{g^3}, \ldots, \varepsilon^{g^{p-1}}$$

Dies stellt bloß eine andere Reihenfolge von $\varepsilon, \varepsilon^2, \ldots, \varepsilon^{p-1}$ dar. Wir bilden nun den Ausdruck

$$\eta := \varepsilon^{g^1} + \varepsilon^{g^2} + \varepsilon^{g^3} + \ + \varepsilon^{g^{p-1}} = \varepsilon + \varepsilon^1 + \varepsilon^2 + \ldots + \varepsilon^{p-1} = -1$$

der den Wert -1 hat, da ε Nullstelle von $f(z)$ ist.

Wegen $p-1 = 2^h$ hat η eine gerade Anzahl von Summanden. Wir teilen sie in zwei Hälften

$$\left.\begin{aligned} \eta_1 &:= \varepsilon^{g^1} + \varepsilon^{g^3} + \varepsilon^{g^5} + \ldots + \varepsilon^{g^{p-2}} \\ \eta_2 &:= \varepsilon^{g^2} + \varepsilon^{g^4} + \varepsilon^{g^6} + \ldots + \varepsilon^{g^{p-1}} \end{aligned}\right\} \text{ je } \frac{p-1}{2} \text{ Summanden } \boxed{\eta = \eta_1 + \eta_2}$$

Jede dieser Größen unterteilen wir wieder in zwei gleiche Teile

$$\left.\begin{aligned} \eta_{11} &:= \varepsilon^{g^1} + \varepsilon^{g^5} + \varepsilon^{g^9} + \ldots + \varepsilon^{g^{p-4}} \\ \eta_{12} &:= \varepsilon^{g^3} + \varepsilon^{g^7} + \varepsilon^{g^{11}} + \ldots + \varepsilon^{g^{p-2}} \end{aligned}\right\} \text{ je } \frac{p-1}{4} \text{ Summanden } \boxed{\eta_1 = \eta_{11} + \eta_{12}}$$

$$\left.\begin{aligned} \eta_{21} &:= \varepsilon^{g^2} + \varepsilon^{g^6} + \varepsilon^{g^{10}} + \ldots + \varepsilon^{g^{p-3}} \\ \eta_{22} &:= \varepsilon^{g^4} + \varepsilon^{g^8} + \varepsilon^{g^{12}} + \ldots + \varepsilon^{g^{p-1}} \end{aligned}\right\} \text{ je } \frac{p-1}{4} \text{ Summanden } \boxed{\eta_2 = \eta_{21} + \eta_{22}}$$

So fortfahrend bilden wir Summen von

$$\frac{p-1}{8}, \frac{p-1}{16}, \ldots$$

Summanden, bis man schließlich zu Ausdrücken von je einem Summanden kommt, d.h. zu den Nullstellen von $f(z)$ selbst.

Die oben gebildeten Summen heißen *GAUSSsche Perioden*. Die GAUSSschen Perioden lassen sich durch Quadratwurzelausdrücke berechnen. Es ist

$$\boxed{\eta = \eta_1 + \eta_2 = -1}$$

Berechnen wir nun das Produkt $\eta_1 . \eta_2$. Bevor wir dies ausführen, ersetzen wir sowohl in η_1 als in η_2 die Größe ε durch ε^g.

$$\bar{\eta}_1 = \left(\varepsilon^g\right)^g + \left(\varepsilon^g\right)^{g^3} + \left(\varepsilon^g\right)^{g^5} + \ldots + \left(\varepsilon^g\right)^{g^{p-2}} = \varepsilon^{g^2} + \varepsilon^{g^4} + \varepsilon^{g^6} + \ldots + \varepsilon^{g^{p-1}} = \eta_2$$

$$\bar{\eta}_2 = \left(\varepsilon^g\right)^{g^2} + \left(\varepsilon^g\right)^{g^4} + \left(\varepsilon^g\right)^{g^6} + \ldots + \left(\varepsilon^g\right)^{g^{p-1}} = \varepsilon^{g^3} + \varepsilon^{g^5} + \varepsilon^{g^7} + \ldots + \underbrace{\varepsilon^{g^p}}_{g^p \equiv g\,(mod\ p)} = \eta_1$$

Durch den Ersatz von ε durch ε^g werden η_1 und η_2 vertauscht. Das Produkt $\eta_1 . \eta_2$ ist invariant gegenüber der Substitution von ε durch ε^g.

Das Produkt $\eta_1 . \eta_2 = \bar{\eta}_1 . \bar{\eta}_2 = \sum \varepsilon^{g^r} . \varepsilon^{g^s}$ besteht aus lauter Summanden der Gestalt

$$\varepsilon^{g^r}.\varepsilon^{g^s} = \varepsilon^{g^r+g^s} = \varepsilon^u$$

Nun gilt

$$u = q.p + t \Rightarrow \varepsilon^u = \varepsilon^{qp+t} = \left(\varepsilon^p\right)^q.\varepsilon^t = e^t \qquad t < p$$

also

$$\varepsilon^{g^r+g^s} = \varepsilon^t$$

Insgesamt treten $2^{h-1}.2^{h-1} = 2^{2h-2} = 2^h.2^{h-2}$ Summanden in $\eta_1.\eta_2$ auf. Nun gibt es aber nur $p - 1 = 2^h$ verschiedene Nullstellen von $f(z)$, daher müssen etliche Summanden mehrfach auftreten. Es gilt also

$$\eta_1.\eta_2 = \underline{\alpha.\varepsilon^g + \beta.\varepsilon^{g^2} + \ldots + \rho.\varepsilon^{g^{p-1}}} \overset{\varepsilon \to \varepsilon^g}{=} \alpha.\varepsilon^{g^2} + \beta.\varepsilon^{g^3} + \ldots + \rho.\underbrace{\varepsilon^{g^p}}_{\varepsilon^g} = \underline{\rho.\varepsilon^g + \alpha.\varepsilon^{g^2} + \beta.\varepsilon^{g^3} + \ldots}$$

Aus der Eindeutigkeit der Darstellung im Kreisteilungskörper (Seite 35) folgt

$$\alpha = \rho, \beta = \alpha, \gamma = \beta, \ldots \Rightarrow \alpha = \beta = \gamma = \ldots = \rho \in \mathbb{Z}$$

d.h.alle Koeffizienten sind gleich. Daraus folgt

$$\underline{\eta_1.\eta_2} = \rho.\left(\varepsilon^{g^1} + \varepsilon^{g^2} + \varepsilon^{g^3} + \ldots + \varepsilon^{g^{p-1}}\right) = \rho.\eta = \underline{-\rho}$$

Da aber insgesamt $2^h.2^{h-2}$ Summanden auftreten, muß $\underline{\rho = 2^{h-2}}$ sein. Daher

$$\boxed{\begin{aligned}\eta_1 + \eta_2 &= -1\\ \eta_1.\eta_2 &= -\rho\end{aligned}}$$

Ferner gilt $4.\rho = 2^2.2^{h-2} = 2^h = p-1 \Rightarrow$

$$\boxed{4\rho + 1 = p}$$

Nach VIETA[1]) sind η_1 und η_2 Nullstellen der quadratischen Gleichung

$$\underline{x^2 + x - \rho = 0} \Rightarrow \eta_{1,2} = \frac{-1 \pm \sqrt{1+4\rho}}{2} = \frac{-1 \pm \sqrt{p}}{2}$$

Wir berechnen nun die nächsten GAUSSschen Perioden

$$\eta_{11}, \eta_{12}; \eta_{21}.\eta_{22} \text{ von je } \frac{p-1}{2} = 2^{h-2} \text{ Summanden}$$

Zunächst gilt

$$\eta_{11} + \eta_{12} = \eta_1 \qquad \eta_{21} + \eta_{22} = \eta_2$$

Wir berechnen die Produkte

$$\eta_{11}.\eta_{12} \text{ und } \eta_{21}.\eta_{22}$$

Diesmal ist $\eta_{11}.\eta_{12}$ <u>invariant gegen die Substitution von ε gegen ε^{g^2}</u>

$$\bar{\eta}_{11} = \varepsilon^{g^3} + \varepsilon^{g^7} + \varepsilon^{g^{11}} + \ldots + \varepsilon^{g^{p-2}} = \eta_{12}$$

$$\bar{\eta}_{12} = \varepsilon^{g^5} + \varepsilon^{g^9} + \varepsilon^{g^{13}} + \ldots + \underbrace{\varepsilon^{g^p}}_{\varepsilon^g} = \eta_{11}$$

Nun ist

$$\eta_{11}.\eta_{12} = \sum \varepsilon^{g^r}.\varepsilon^{g^s} = \sum \varepsilon^{g^t}$$

in dieser Summe treten $2^{h-2}.2^{h-2} = 2^{2h-4} = 2^h.2^{h-4}$ Summanden auf. Es müssen wieder einige Summanden mehrfach auftreten, sodaß gilt

[1] VIÈTE, François (1540-1603

$$\eta_{11}.\eta_{12} = \left[\alpha_1.\varepsilon^g + \beta_1.\varepsilon^{g^3} + \ldots + \rho_1.\varepsilon^{g^{p-2}}\right] + \left[\alpha_2.\varepsilon^{g^2} + \beta_2.\varepsilon^{g^4} + \ldots + \rho_2.\varepsilon^{g^{p-1}}\right] =$$

$$\underset{=}{\overset{\varepsilon\to\varepsilon^{p^2}}{}} \left[\alpha_1.\varepsilon^{g^3} + \beta_1.\varepsilon^{g^5} + \ldots + \rho_1.\overbrace{\varepsilon^{g^p}}^{\varepsilon^g}\right] + \left[\alpha_2.\varepsilon^{g^4} + \beta_2\varepsilon^{g^6} + \ldots + \overbrace{\varepsilon^{g^{p+1}}}^{\left(\varepsilon^{g^p}\right)^g=\left(\varepsilon^g\right)^g=\varepsilon^{g^2}}\right]$$

Daraus folgt wieder wegen der Eindeutigkeit der Darstellung im Kreisteilungskörper (Seite 35)

$$\alpha_1 = \rho_1,\ \beta_1 = \alpha_1,\ \gamma_1 = \beta_1,\ \ldots\ ;\ \alpha_2 = \rho_2,\ \beta_2 = \alpha_2,\ \gamma_2 = \beta_2,\ \ldots$$

daher

$$\eta_{11}.\eta_{12} = \rho_1.\underbrace{\left(\varepsilon^g + \varepsilon^{g^3} + \varepsilon^{g^5} + \ldots + \varepsilon^{g^{p-2}}\right)}_{\eta_1} + \rho_2.\underbrace{\left(\varepsilon^{g^2} + \varepsilon^{g^4} + \varepsilon^{g^6} + \ldots + \varepsilon^{g^{p-1}}\right)}_{\eta_2}$$

Es ist also

$$\boxed{\eta_{11}.\eta_{12} = \rho_1.\eta_1 + \rho_2.\eta_2\,;\quad \eta_{11} + \eta_{12} = \eta_1}$$

Die η_{11}, η_{12} sind daher Nullstellen der quadratischen Gleichung

$$\underline{x^2 - \eta_1.x + \left(\rho_1.\eta_1 + \rho_2.\eta_2\right) = 0}$$

Die ganzen Zahlen ρ_i hängen von der speziellen Primzahl p ab und müssen gesondert berechnet werden.

Analog sind η_{21} und η_{22} Nullstellen einer von η_1 und η_2 abhängigen quadratischen Gleichung.

Zerlegt man $\eta_{11} = \eta_{111} + \eta_{112}$, so ist analog zu oben das Produkt $\eta_{111}.\eta_{112}$ invariant bezüglich der Substitution $\varepsilon \to \varepsilon^{g^3}$ und daher wieder eine Linearkombination von η_{11}, η_{12}, η_{21}, η_{22}. η_{111} und η_{112} sind daher wieder Nullstellen einer quadratischen Gleichung

Auf diese Weise berechnet man die Perioden mit

$$\frac{p-1}{16} = 2^{h-4},\ \frac{p-1}{32} = 2^{h-5},\ \ldots$$

Gliedern, bis man schließlich durch sukessives Auflösen von quadratischen Gleichungen (d.h. durch Konstruktion von Wurzelschachtelungen) auf jene Perioden kommt, die nur mehr aus einem Glied bestehen. Das sind aber die Nullstellen der Kreisteilungsgleichung.

> Jedes regelmäßige p-Eck, dessen Eckenzahl eine Primzahl der Bauart
> $$p = 2^h + 1,\ h = 2^\mu$$
> ist, läßt sich mit Zirkel und Lineal konstruieren.

Anmerkung: Im konkreten Fall hat man von jeder der zu ziehenden Quadratwurzeln noch das richtige Vorzeichen zu bestimmen.

Das regelmäßige Fünfeck

5-Eck $\quad \mu = 1,\ p = 5$

Ist ε eine Einheitswurzel, so gilt

$$\varepsilon^5 = 1,\ \varepsilon^4 + \varepsilon^3 + \varepsilon^2 + \varepsilon + 1 = 0$$

Da 2 ein Primitivrest von p = 5 ist, folgt

$2^1 \equiv 2,\ 2^2 \equiv 4,\ 2^3 \equiv 3,\ 2^4 \equiv 1$

Ersetzt man ε durch ε^2, so gilt

$$\varepsilon^{2^1}+\varepsilon^{2^2}+\varepsilon^{2^3}+\varepsilon^{2^4}+1=0$$

Dann gibt es folgende GAUSSschen Perioden

$$\eta=\varepsilon^{2^1}+\varepsilon^{2^2}+\varepsilon^{2^3}+\varepsilon^{2^4}=-1$$

$$\left.\begin{aligned}\eta_1&=\varepsilon^{2^1}+\varepsilon^{2^3}=\varepsilon^2+\varepsilon^3\\ \eta_2&=\varepsilon^{2^2}+\varepsilon^{2^4}=\varepsilon^4+\varepsilon^1\end{aligned}\right\}\ \eta=\eta_1+\eta_2$$

$$\eta_1.\eta_2=\varepsilon^6+\varepsilon^7+\varepsilon^3+\varepsilon^4=\varepsilon^4+\varepsilon^3+\varepsilon^2+\varepsilon=-1$$

Daher sind η_1 und η_2 Nullstellen der quadratischen Gleichung

$$\boxed{x^2+x-1=0}$$

$$\left.\begin{aligned}\eta_{11}&=\varepsilon^2\\ \eta_{12}&=\varepsilon^3\end{aligned}\right\}\ \eta_{11}+\eta_{12}=\eta_1$$

$$\eta_{11}.\eta_{12}=\varepsilon^5=1$$

Demnach sind η_{11} und η_{12} Nullstellen der quadratischen Gleichung

$$\boxed{x^2-\eta_1.x+1=0}$$

Setzt man, $\eta_{11}=\varepsilon^2=\boldsymbol{cos}\,\alpha+\hat{\imath}.\boldsymbol{sin}\,\alpha$, so folgt aus obiger Gleichung

$$\eta_{11}=\frac{1}{2}.\eta_1+\sqrt{\frac{1}{4}.\eta_1^2-1}=\left(\frac{1}{2}.\eta_1\right)+\hat{\imath}.\sqrt{1-\left(\frac{1}{2}.\eta_1\right)^2}=\boldsymbol{cos}\,\alpha+\hat{\imath}.\boldsymbol{sin}\,\alpha\Rightarrow \underline{\boldsymbol{cos}\,\alpha=\frac{1}{2}.\eta_1}$$

Aus der ersten Gleichung folgt

$$x^2+x-1=0\Rightarrow\eta_1=-\frac{1}{2}+\sqrt{\frac{1}{4}+1}\Rightarrow\eta_1=\frac{\sqrt{5}-1}{2}=2.\boldsymbol{cos}\,\alpha$$

$$\boxed{\boldsymbol{cos}\,\alpha=\boldsymbol{cos}\,72^\circ=\frac{\sqrt{5}-1}{4}=0{,}309017}$$

Das regelmäßige Siebzehneck

17-Eck $\quad \mu = 2,\ p = 17$

Ist ε eine Einheitswurzel so gilt

$$\varepsilon^{17}=1,\ \varepsilon^{16}+\varepsilon^{15}+\ldots+\varepsilon+1=0$$

Da 3 ein Primitivrest von 17 ist, gilt

$$3^1\equiv 3,\ 3^2\equiv 9,\ 3^3\equiv 10,\ 3^4\equiv 13,\ 3^5\equiv 5,\ 3^6\equiv 15,\ 3^7\equiv 11,\ 3^8\equiv 16,$$

$$3^9\equiv 14,\ 3^{10}\equiv 8,\ 3^{11}\equiv 7,\ 3^{12}\equiv 4,\ 3^{13}\equiv 12,\ 3^{14}\equiv 2,\ 3^{15}\equiv 6,\ 3^{16}\equiv 1$$

Nach Ersatz von ε durch ε^3 ergibt sich für die GAUSSschen Perioden

$$\eta=\varepsilon^{3^1}+\varepsilon^{3^2}+\varepsilon^{3^3}+\ldots+\varepsilon^{3^{16}}=-1$$

$$\left.\begin{aligned}\eta_1&=\varepsilon^{3^1}+\varepsilon^{3^3}+\varepsilon^{3^5}+\varepsilon^{3^7}+\varepsilon^{3^9}+\varepsilon^{3^{11}}+\varepsilon^{3^{13}}+\varepsilon^{3^{15}}\\ \eta_2&=\varepsilon^{3^2}+\varepsilon^{3^4}+\varepsilon^{3^6}+\varepsilon^{3^8}+\varepsilon^{e^{10}}+\varepsilon^{3^{12}}+\varepsilon^{3^{14}}+\varepsilon^{3^{16}}\end{aligned}\right\}\ \eta_1+\eta_2=\eta=-1$$

Da $\eta_1.\eta_2$ insgesamt 8.8 = 64 Summanden hat, muß jeder der 16 Summanden ε^{3^k} viermal auftreten. Daher gilt

$$\eta_1.\eta_2 = 4.\left(\varepsilon^{3^1} + \varepsilon^{3^2} + \varepsilon^{3^3} + ... + \varepsilon^{3^{16}}\right) = 4.\eta = -4$$

η_1 und η_2 genügen daher der quadratischen Gleichung

$$\boxed{x^2 + x - 4 = 0} \Rightarrow \eta_1, \eta_2$$

$$\left.\begin{aligned}\eta_{11} &= \varepsilon^{3^1} + \varepsilon^{3^5} + \varepsilon^{3^9} + \varepsilon^{3^{13}} \\ \eta_{12} &= \varepsilon^{3^3} + \varepsilon^{3^7} + \varepsilon^{3^{11}} + \varepsilon^{3^{15}}\end{aligned}\right\} \eta_{11} + \eta_{12} = \eta_1$$

Da $\eta_1.\eta_2$ 4.4 = 16 Summanden aufweist, tritt jeder Summand ε^{3^k} einmal auf und es gilt

$$\eta_{11}.\eta_{12} = \left(\varepsilon^{3^1} + \varepsilon^{3^2} + \varepsilon^{3^3} + ... + \varepsilon^{3^{16}}\right) = \eta = -1$$

η_{11}, η_{12} genügen daher der quadratischen Gleichung

$$\boxed{x^2 - \eta_1.x - 1 = 0} \Rightarrow \eta_{11}, \eta_{12}$$

Analog folgt

$$\left.\begin{aligned}\eta_{21} &= \varepsilon^{3^2} + \varepsilon^{3^6} + \varepsilon^{3^{10}} + \varepsilon^{3^{14}} \\ \eta_{22} &= \varepsilon^{3^4} + \varepsilon^{3^8} + \varepsilon^{3^{12}} + \varepsilon^{3^{16}}\end{aligned}\right\} \eta_{21} + \eta_{22} = \eta_2$$

$$\eta_{21}.\eta_{22} = \left(\varepsilon^{3^1} + \varepsilon^{3^2} + \varepsilon^{3^3} + ... + \varepsilon^{3^{16}}\right) = \eta = -1$$

$$\boxed{x^2 - \eta_2.x - 1 = 0} \Rightarrow \eta_{21}, \eta_{22}$$

$$\left.\begin{aligned}\eta_{111} &= \varepsilon^{3^1} + \varepsilon^{3^9} \\ \eta_{112} &= \varepsilon^{3^5} + \varepsilon^{3^{13}}\end{aligned}\right\} \eta_{111} + \eta_{112} = \eta_{11}$$

$$\eta_{111}.\eta_{112} = \varepsilon^{3^1+3^5} + \varepsilon^{3^1+3^{13}} + \varepsilon^{3^9+3^5} + \varepsilon^{3^9+3^{13}} = \varepsilon^{3^{10}} + \varepsilon^{3^6} + \varepsilon^{3^{14}} + \varepsilon^{3^2} = \eta_{21}$$

$$\boxed{x^2 - \eta_{11}.x + \eta_{21} = 0} \Rightarrow \eta_{111}, \eta_{112}$$

$$\left.\begin{aligned}\eta_{121} &= \varepsilon^{3^3} + \varepsilon^{3^{11}} \\ \eta_{122} &= \varepsilon^{3^7} + \varepsilon^{3^{15}}\end{aligned}\right\} \eta_{121} + \eta_{122} = \eta_{12}$$

$$\eta_{121}.\eta_{122} = \varepsilon^{3^3+3^7} + \varepsilon^{3^3+3^{15}} + \varepsilon^{3^{11}+3^7} + \varepsilon^{3^{11}+3^{15}} = \varepsilon^{3^8} + \varepsilon^{3^{12}} + \varepsilon^{3^{16}} + \varepsilon^{3^4} = \eta_{22}$$

$$\boxed{x^2 - \eta_{12}.x + \eta_{22} = 0} \Rightarrow \eta_{121}, \eta_{122}$$

$$\left.\begin{aligned}\eta_{211} &= \varepsilon^{3^2} + \varepsilon^{3^{10}} \\ \eta_{212} &= \varepsilon^{3^6} + \varepsilon^{3^{14}}\end{aligned}\right\} \eta_{211} + \eta_{212} = \eta_{21}$$

$$\eta_{211}.\eta_{212} = \varepsilon^{3^2+3^6} + \varepsilon^{3^2+3^{14}} + \varepsilon^{3^{10}+3^6} + \varepsilon^{3^{10}+3^{14}} = \varepsilon^{3^7} + \varepsilon^{3^{11}} + \varepsilon^{3^{15}} + \varepsilon^{3^3} = \eta_{12}$$

$$\boxed{x^2 - \eta_{21}.x + \eta_{12} = 0} \Rightarrow \eta_{211}, \eta_{212}$$

$$\left.\begin{aligned}\eta_{221} &= \varepsilon^{3^4} + \varepsilon^{3^{12}} \\ \eta_{222} &= \varepsilon^{3^8} + \varepsilon^{3^{16}}\end{aligned}\right\} \eta_{221} + \eta_{222} = \eta_{22}$$

$$\eta_{221\cdot 222} = \varepsilon^{3^4+3^8} + \varepsilon^{3^4+3^{16}} + \varepsilon^{3^{12}+3^8} + \varepsilon^{3^{12}3^{16}} = \varepsilon^{3^{13}} + \varepsilon^{3^9} + \varepsilon^{3^1} + \varepsilon^{3^5} = \eta_{11}$$

$$\boxed{x^2 - \eta_{22}.x + \eta_{11} = 0} \Rightarrow \eta_{221}, \eta_{222}$$

$$\left.\begin{aligned}\eta_{2221} &= \varepsilon^{3^8} = \varepsilon^{16}\\ \eta_{2222} &= \varepsilon^{3^{16}} = \varepsilon^{1}\end{aligned}\right\} \eta_{2221} + \eta_{2222} = \eta_{222}$$

$$\eta_{2221}.\eta_{2222} = \varepsilon^{16+1} = \varepsilon^{17} = 1$$

$$\boxed{x^2 - \eta_{222}.x + 1 = 0} \Rightarrow \eta_{2221},\ \eta_{2222}$$

Setzt man $\eta_{2222} = \varepsilon = \cos\alpha + \hat{\imath}.\sin\alpha$, so folgt aus der letzten Gleichung

$$\eta_{2222} = \frac{1}{2}\eta_{222} + \sqrt{\left(\frac{1}{2}\eta_{222}\right)^2 - 1} = \frac{1}{2}\eta_{222} + \hat{\imath}.\sqrt{1 - \sqrt{\left(\frac{1}{2}\eta_{222}\right)^2}} = \cos\alpha + \hat{\imath}.\sin\alpha$$

daher

$$\boxed{\cos\alpha = \frac{1}{2}\eta_{222}}$$

Es ist daher folgendes System von quadratischen Gleichungen zu lösen

$$\boxed{\begin{aligned} x^2 + x - 4 &= 0 && \Rightarrow \eta_1, \eta_2\\ x^2 - \eta_1.x - 1 &= 0 && \Rightarrow \eta_{11}\\ x^2 - \eta_2.x - 1 &= 0 && \Rightarrow \eta_{22}\\ x^2 - \eta_{22}.x + \eta_{11} &= 0 && \Rightarrow \eta_{222}\end{aligned}}$$

$$x^2 + x - 4 = 0 \Rightarrow \eta_1 = -\frac{1}{2}.\left[\sqrt{17} + 1\right],\ \eta_2 = \frac{1}{2}.\left[\sqrt{17} - 1\right]$$

$$x^2 - \eta_1.x - 1 = 0 \Rightarrow \eta_{11} = \frac{1}{4}.\left[\sqrt{34 + 2.\sqrt{17}} - \left(\sqrt{17} + 1\right)\right]$$

$$x^2 - \eta_2.x - 1 = 0 \Rightarrow \eta_{22} = \frac{1}{4}.\left[\sqrt{34 - 2.\sqrt{17}} + \left(\sqrt{17} - 1\right)\right]$$

$$x^2 - \eta_{22}.x + \eta_{11} = 0$$

Daraus

$$\eta_{222} == \frac{1}{8}\left\{\left(\sqrt{17} - 1\right) + \sqrt{34 - 2\sqrt{17}} + \sqrt{\left(12\sqrt{17} + 68\right) - \sqrt{2720 + 608\sqrt{17}}}\right\} = 2.\cos a$$

$$\boxed{\cos\alpha = \cos\left(\frac{360°}{17}\right) = \frac{1}{2}.\eta_{222} = 0{,}932472}$$

Zm Nachweis der Richtigkeit der folgenden Konstruktion, welche die 5.Ecke des Siebzehnecks liefert, hätte man analog zu obiger Rechnung die Größe

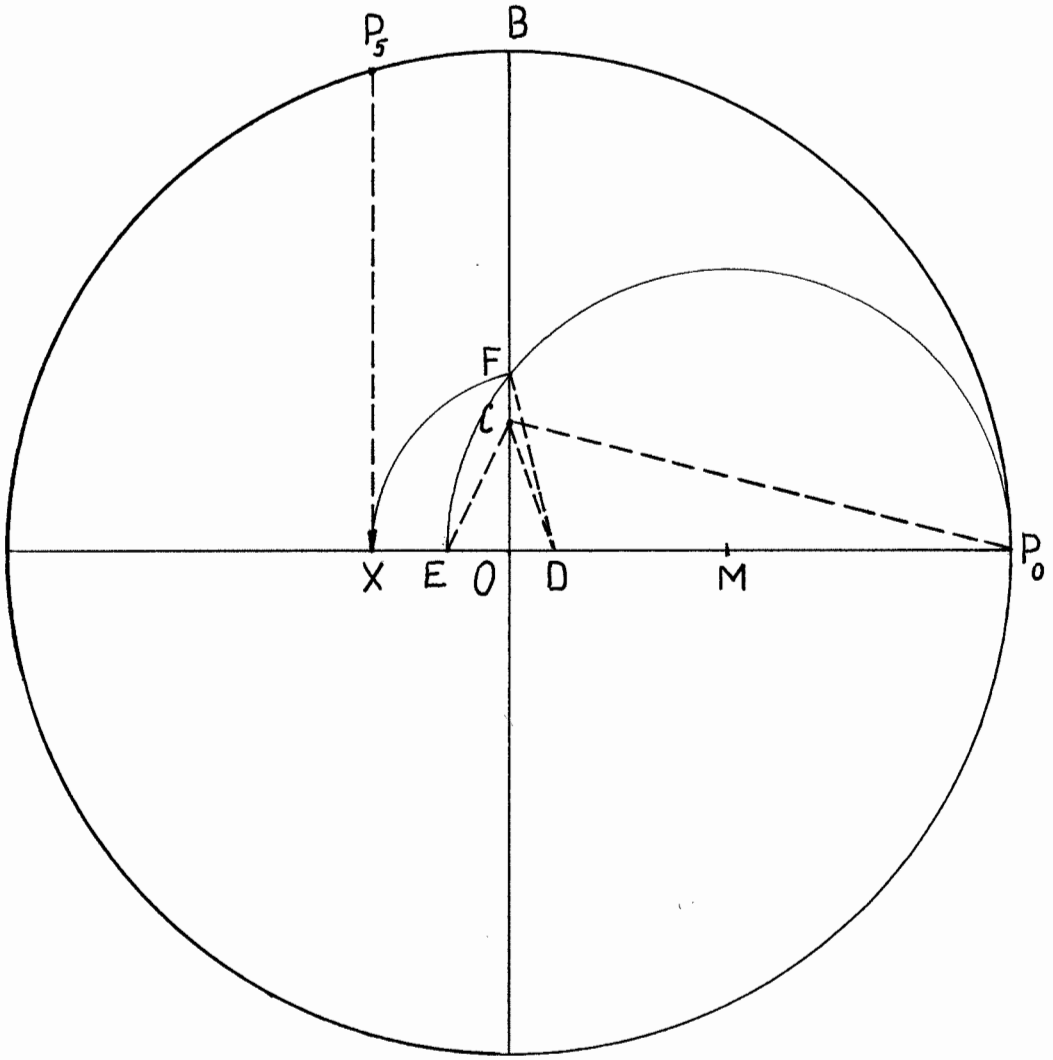
$$\varepsilon^5 = \varepsilon^{3^5} = \eta_{1121}$$

zu bestimmen

Konstruktion des regelmäßigen Siebzehnecks[1]

Konstruktionsanleitung:

1. OP_0 und OB sind orthogonale Durchmesser des Einheitskreises.
2. $OC = \frac{1}{4} OB$
3. $\angle OCP_0 := 4\varphi$
4. $\angle OCD = \varphi$
5. $\angle DCE = 45°$
6. F... Schnittpunkt des Thaleskreises über EP_0 mit OB
7. $XD = DF$
8. P_5 ist der 5.Eckpunkt des regelmäßigen Siebzehnecks



Der Beweis ergibt sich durch Nachrechnung der Konstruktion

[1] Diese hübsche Konstruktion findet sich in NEIDHARDT W. / WURM Ch.: Arbeitsbuch Thales. Dümmlers Verlag Bonn 1997.

Historische Bemerkungen

Die Konstruktion regelmäßiger Vielecke geht bis auf die vorgriechische Zeit zurück. Jedenfalls waren die Konstruktionen der klassischen Vielecke (Drei-, Vier-, Fünf-, Sechs- und Fünfzehneck) bereits den Pythagoreern bekannt (PYTHAGORAS (ca.580-500 v.Chr.)). Alle Konstruktionen finden sich in den „Elementen" von EUKLID (ca. 300 v.Chr.)

rgm. Dreieck	Buch I, Satz 1
rgm. Viereck	Buch IV, Satz 6-9
rgm. Fünfeck	Buch IV, Satz 10-14
rgm. Sechseck	Buch IV, Satz 15
rgm. 15-Eck	Buch IV, Satz 16

rgm. 17-Eck: Carl Friedich GAUSS (1777-1855)
29.März 1796 (Einteilung der Einheitswurzeln in zwei Gruppen)
Damit Beginn des wissenschaftlichen Tagebuchs (geführt bis 1814). Die erste Eintragung lautet:
1796 30.März: Principia quibus innititur sectio circuli ac divisibilitas eiusdem geometria in septemdecim partes etc.
Die Veröffentlichung erfolgte in:
Disquisitiones arithmeticae, Sectio prima, art.335. S.664, Leipzig 1801

rgm. 257-Eck: Friedrich Julius RICHELOT (1808-1875): De Resolutione algebraica aequationis $x^{257} = 1$, sive de divisione circuli per bisectionem anguli septies repetitam in partes 257 inter se aequales commentatio coronata
CRELLES Journal IX (1832) S 1-26, 146-161, 209-230, 337-356 (84 Seiten)

rgm. 65537-Eck: Johann Gustav HERMES (1846-1912). Seine Abhandlung ist aufbewahrt im Seminar zu Göttingen. Göttinter Nachrichten Nr.3 (1894)
HERMES benötigte für diese Arbeit 12 Jahre

Die Gleichung dritten Grades

Die reine Gleichung dritten Grades

Die reine Gleichung dritten Grades

$$x^3 = a^3$$

wird durch die Substitution $x = az$ auf die Kreisteilungsgleichung

$$z^3 = 1 \Rightarrow z^3 - 1 = (z-1)(z^2+z+1) = 0$$

zurückgeführt. Deren Nullstellen sind die 3.Einheitswurzeln. Sie lauten

$$1, \varepsilon = -\frac{1}{2} + \frac{\hat{\imath}}{2}\sqrt{3},\ \bar{\varepsilon} = -\frac{1}{2} - \frac{\hat{\imath}}{2}\sqrt{3}$$

wobei folgende Beziehungen gelten

$$\varepsilon + \bar{\varepsilon} = -1,\ \varepsilon + 1 = -\bar{\varepsilon}$$

$$\varepsilon.\bar{\varepsilon} = 1 = \varepsilon^3 = \varepsilon.\varepsilon^2 \Rightarrow \varepsilon^2 = \bar{\varepsilon} = \frac{1}{\varepsilon}$$

$$\varepsilon^2 + \varepsilon + 1 = 0$$

Daher lauten die Nullstellen der reinen Gleichung

$$\boxed{x^3 = a^3 \Rightarrow x_1 = a,\ x_2 = \varepsilon.a,\ x_3 = \bar{\varepsilon}.a = \varepsilon^2.a = \frac{a}{\varepsilon}}$$

Reduktion der allgemeinen Gleichung dritten Grades

Es seien z_1, z_2, z_3 die drei Nullstellen des Polynoms

$$z^3 + a_1 z^2 + a_2 z + a_3 = (z - z_1)(z - z_2)(z - z_3) \qquad a_i \in \mathbb{R}$$

Dann gilt

$$a_1 = -(z_1 + z_2 + z_3)$$
$$a_2 = (z_1 z_2 + z_1 z_3 + z_2 z_3)$$
$$a_3 = -(z_1 z_2 z_3)$$

Die Transformation

$$z = x + s \in \mathbb{R}$$

ergibt

$$z_1 + z_2 + z_3 = x_1 + x_2 + x_3 + 3s = -a_1$$

Wählt man s so, daß für die Nullstellen der Gleichung in x gilt

$$x_1 + x_2 + x_3 = 0$$

so folgt

$$s = -\frac{a_1}{3}$$

Dann ergibt sich die reduzierte Gleichung dritten Grades

$$\boxed{\begin{array}{c} x^3 + 3ax + 2b = 0 \\ x_1 + x_2 + x_3 = 0 \\ x_1 x_2 + x_1 x_3 + x_2 x_3 = 3a \\ x_1 x_2 x_3 = -2b \end{array}}$$

Die Formeln von CARDANO[1]

Zur Auflösung der reduzierten Gleichung

$$x^3 + 3ax + 2b = 0$$

setzen wir

$$x = u + v$$

dann folgt

$$\begin{aligned} x^3 + 3ax + 2b &= u^3 + 3u^2v + 3uv^2 + v^3 + 3a(u+v) + 2b = \\ &= u^3 + v^3 + 3uv(u+v) + 3a(u+v) + 2b = \\ &= \left[u^3 + v^3 + 2b\right] + \left[3uv + 3a\right](u+v) = 0 \end{aligned}$$

Die letzte Beziehung ist erfüllt, wenn folgende Bedingungen gelten

$$u^3 + v^3 = -2b$$

$$uv = -a$$

Nach Kubierung der 2.Gleichung folgt

$$\begin{aligned} u^3 + v^3 &= -2b \\ u^3v^3 &= -a^3 \end{aligned} \qquad (1)$$

Die Größen $y_1 := u^3, y_2 := v^3$ sind dann Nullstellen der *quadratischen Resolvente*

$$\boxed{y^2 + 2by - a^3 = 0}$$

Daher gilt

$$u^3 = -b + \sqrt{b^2 + a^3}, \quad v^3 = -b - \sqrt{b^2 + a^3}$$

Für die Größen u und v ergeben sich daher die Werte

$$\begin{aligned} u, \varepsilon u, \varepsilon^2 u &= \bar{\varepsilon} u \\ v, \varepsilon v, \varepsilon^2 v &= \bar{\varepsilon} u \end{aligned} \qquad (2)$$

also insgesamt neun Möglichkeiten, um die Nullstellen der reduzierten Gleichung zu bilden. Die Darstellungen (1) und (2) erhält man allerdings auch, wenn die reduzierte Gleichung die Gestalt

$$x^3 + 3\varepsilon ax + 2b = 0$$

oder

$$x^3 + 3\varepsilon^2 ax + 2b = 0$$

hätte. Die obigen neun Werte stellen also die Lösungstripel von drei Gleichungen dritten Grades dar. Um die für uns relevanten Gleichungen zu finden, müssen wir u und v so wählen, daß das Produkt uv = -a reell wird. Daher muß sein

$$\begin{aligned} x_1 &= u + v \\ x_2 &= \varepsilon u + \bar{\varepsilon} v \\ x_3 &= \bar{\varepsilon} u + \varepsilon v \end{aligned}$$

Demnach lautet die Formel von CARDANO

[1] Geronimo CARDANO (1501-1576) 1545
Herleitung der Formel nach Jan HUDDE (1628-1704)

$$x_1 = \sqrt[3]{-b+\sqrt{b^2+a^3}} + \sqrt[3]{-b-\sqrt{b^2+a^3}}$$
$$x_2 = \varepsilon.\sqrt[3]{-b+\sqrt{b^2+a^3}} + \bar{\varepsilon}.\sqrt[3]{-b-\sqrt{b^2+a^3}}$$
$$x_1 = \bar{\varepsilon}.\sqrt[3]{-b+\sqrt{b^2+a^3}} + \varepsilon.\sqrt[3]{-b-\sqrt{b^2+a^3}}$$

Diskussion der CARDANischen Formel

1.Fall $b^2+a^3 > 0$ Der Radikand ist reell, daher sind u,v beide reell, demnach ist x_1 reell und x_2, x_3 konjugiert komplex

$a > 0 \Rightarrow \left|\sqrt{b^2+a^3}\right| > |b| \Rightarrow u = \sqrt[3]{-b+\sqrt{b^2+a^3}} > 0$

$$v = \sqrt[3]{-b-\sqrt{b^2+a^3}} < 0$$

$b > 0 \Rightarrow (|v|>|u|),\ v < 0,\ u > 0 \Rightarrow u + v = x < 0$
$b < 0 \Rightarrow (|v|<|u|),\ v < 0,\ u > 0 \Rightarrow u + v = x > 0$

$a < 0 \Rightarrow \left|\sqrt{b^2+a^3}\right| < |b|$

$b > 0 \Rightarrow u < 0,\ v < 0, \Rightarrow u + v = x < 0$
$b < 0 \Rightarrow u > 0,\ v > 0, \Rightarrow u + v = x > 0$

Ist $b^2 + a^3 > 0$, so existieren eine reelle Nullstelle x und zwei konjugiert komplexe Nullstellen. Für die reelle Nullstelle gilt

$b > 0 \Rightarrow x < 0$
$b < 0 \Rightarrow x > 0$

2.Fall $b^2 + a^3 = 0 \Rightarrow a < 0$ Dann ist $u = v$, daher $x_1 = 2u$, $x_2 = x_3 = u\underbrace{(\varepsilon+\bar{\varepsilon})}_{-1} = -u$. Es gibt daher drei reelle Nullstellen, darunter zwei gleiche. Nach Voraussetzung gilt $b^2 = -a^3$ demnach

$$u = \sqrt[3]{-b} = \sqrt[3]{-\frac{b^3}{b^2}} = \sqrt[3]{\frac{b^3}{a^3}} = \frac{b}{a}$$

Daher $x_1 = \frac{2b}{a}$, $x_2 = x_3 = -\frac{b}{a}$, und wegen $a < 0$ folgt

$b < 0 \Rightarrow x_1 > 0,\ x_2 = x_3 < 0$
$b > 0 \Rightarrow x_1 < 0,\ x_2 = x_3 > 0$

Ist $b^2 + a^3 = 0$, so existieren drei reelle Nullstellen, von denen zwei zusammenfallen.Es gilt

$$x_1 = \frac{2b}{a},\ x_2 = x_3 = -\frac{b}{a}$$

$b < 0 \Rightarrow x_1 > 0,\ x_2 = x_3 < 0$
$b > 0 \Rightarrow x_1 < 0,\ x_2 = x_3 > 0$

$b^2 + a^3 = 0$ ist notwendig und hinreichend für das Auftreten einer doppelten Nullstelle

Es ist noch die Umkehrung des obigen Satzes zu zeigen. Die Gleichung habe zwei gleiche Nullstellen $x_2 = x_3$. Dann gilt nach VIETA

$$\left.\begin{array}{l} x_1 + 2x_2 = 0 \\ 2x_1x_2 + x_2^2 = 3a \\ x_1x_2^2 = -2b \end{array}\right| \begin{array}{l} x_1 = -2x_2 \\ -4x_2^2 + x_2^2 = -3x_2^2 = 3a \Rightarrow \underline{a = -x_2^2} \\ -2x_2^3 = -2b \Rightarrow b = x_2^3 \end{array}$$

Daher $\underline{b^2 + a^3} = x_2^6 - x_2^6 = \underline{0}$

3.Fall $\boxed{b^2 + a^3 < 0} \Rightarrow \boxed{a < 0}$ und $b^2 + a^3 = -c^2 \Rightarrow \sqrt{b^2 + a^3} = \hat{\imath}.c$

Dann gilt $u = \sqrt[3]{-b + \hat{\imath}.c}$, $v = \sqrt[3]{-b - \hat{\imath}.c} = \bar{u}$

Daher ist

$$\left.\begin{array}{l} x_1 = u + \bar{u} \\ x_2 = \varepsilon.u + \bar{\varepsilon}.\bar{u} \\ x_3 = \bar{\varepsilon}.u + \varepsilon.\bar{u} \end{array}\right\}$$ Drei reelle Nullstellen als Summe von jeweils zwei konjugiert komplexen Zahlen

Ist $b^2 + a^3 < 0$, so existieren drei reelle Nullstellen.Die reellen Nullstellen sind auf algebraischem Wege nur auf dem Umweg über das Komplexe zu ermitteln. Man nennt diesen Fall daher den „casus irreducibilis"

Die Unmöglichkeit, den Fall dreier reellen Nullstellen auf algebraischem Wege - d.h. bloß durch Schachtelungen von Quadrat- und Kubikwurzeln ohne Anwendung von Grenzbetrachtungen, unendlichen Reihen, transzendenten Funktionen u.ä. - ganz im Reellen, ohne Umweg über das Komplexe zu lösen, wurde erstmals von Otto HÖLDER (1859-1937) gezeigt: „Über den casus irreducibilis bei der Gleichung 3.Grades". Math. Annalen 38 (1891) S.307

Die Behandlung des „casus irreducibilis" mit Hilfe von Winkelfunktionen

Es sei

$$b^2 + a^3 < 0,\ a < 0,\ b^2 + a^3 = -c^2 \Rightarrow \sqrt{b^2 + a^3} = \hat{\imath}.c,\ u = \sqrt[3]{-b + \hat{\imath}.c} = \bar{v}$$

Wir gehen zur Darstellung in Polarkoordinaten über. Setzt man

$$|u| = \frac{r}{2},\ u^3 = -b + \hat{\imath}.c,\ |u^3| = \sqrt[+]{b^2 + c^2}$$

so gilt

$$u = |u|.(\cos\alpha + \hat{\imath}.\sin\alpha) = \frac{r}{2}.(\cos\alpha + \hat{\imath}.\sin\alpha)$$

$$v = \bar{u} = \frac{r}{2}.(\cos\alpha - \hat{\imath}.\sin\alpha)$$

$$x = u + \bar{u} = r.\cos\alpha$$

Die Nullstellen sind ermittelt, sobald $r = 2|u|$ und $\cos\alpha$ bekannt sind. Es gilt nach MOIVRE

$$u^3 = \frac{r^3}{8}.(\cos\alpha + \hat{\imath}.\sin\alpha)^3 = \frac{r^3}{8}.\left[\cos^3\alpha - 3\cos\alpha.\sin^2\alpha + \hat{\imath}.(3\cos^2\alpha.\sin\alpha - \sin^3\alpha)\right] =$$

$$= \frac{r^3}{8}.(\cos 3\alpha + \hat{\imath}.\sin 3\alpha) = -b + \hat{\imath}.c$$

Aus

$$|u^3| = \frac{r^3}{8} = \sqrt[+]{b^2 + c^2} = \sqrt[+]{b^2 - b^2 - a^3} = \sqrt[+]{-a^3}$$

folgt

$$|u| = \frac{r}{2} = \sqrt[+]{-a} \Rightarrow \boxed{r^2 = -4a}$$

$$-b = \frac{r^3}{8}.\cos 3\alpha \Rightarrow \boxed{\cos 3\alpha = -\frac{8b}{r^3}}$$

Berechnet man hieraus r und α, so folgt, da 3α nur bis auf Vielfache von 360° bestimmt ist, daß α nur bis auf Vielfache von 120° bestimmt ist. Es gilt daher

$$\begin{array}{l|l} r^2 = -4a & x_1 = r.\cos\alpha \\ \cos 3\alpha = -\dfrac{8b}{r^3} & \Rightarrow x_2 = r.\cos(\alpha + 120°) \\ & x_3 = r.\cos(\alpha + 240°) \end{array}$$

Zur Berechnung der obigen Größen ist also das Ausziehen eine Kubikwurzel (bei Berechnung von |u|) und die Dreiteilung desWinkels, (bei Berechnung von α) erforderlich. Es gilt daher

> Die Lösung einer Gleichung dritten Grades ist äquivalent der Beherrschung der Würfelvervielfachung und der Winkeldreiteilung

Die trigonometrische Behandlung der Gleichungen dritten Grades geht zurück auf
François VIÈTE (1540-1603), publiziert 1615
Albert GIRARD (1595-1632)
Frans van SCHOOTEN (1615-1660) 1646
Antonio CAGNOLI (1743-1816) 1786

Der „casus irreducibilis“

Symmetrische Polynome

Ein Polynom $f(x_1, \ldots, x_n)$ in den Unbestimmten $x_1, \ldots, x_n$ heißt *symmetrisch*, wenn es bei einer beliebigen Permutation der Unbestimmten seine Gestalt behält.

Man faßt die Glieder gleicher Ordnung r zu *homogenen symmetrischen Polynomen* S_r zusammen, sodaß ein symmetrisches Polynom folgende Bauart hat

$$f(x_1, \ldots, x_n) = S_r + S_{r-1} + \ldots + S_1 + S_0$$

Beispiel:

$$f(x_1,x_2)=(x_1^3x_2+x_2^3x_1)-(x_1^2+x_2^2)+4=S_4-S_2+S_0$$

$$f(x_1,x_2,x_3)=(x_1^2x_2+x_1^2x_3+x_2^2x_1+x_2^2x_3+x_3^2x_1+x_3^2x_2)+(x_1+x_2+x_3)=S_3+S_1$$

Oft ist es zweckmäßig, in jedem Term eines homogenene Polynoms sämtliche vorhandenen Unbestimmten in Evidenz zu setzen, also etwa in obigem Ausdruck in drei Unbestimmten zu schreiben

$$x_1^2x_2 = x_1^2x_2^1x_3^0 \quad \text{bzw.} \quad x_1 = x_1^1x_2^0x_3^0$$

Dann genügt es, sich auf die Betrachtung homogener symmetrischer Polynome zu beschränken.

Man bezeichnet den Term $x_1^{\nu_1}x_2^{\nu_2}\ldots x_n^{\nu_n}$ als *lexikographisch höher* als den Term $x_1^{\mu_1}x_2^{\mu_2}\ldots x_n^{\mu_n}$, wenn in der Folge der Differenzen

$$\nu_1-\mu_1, \nu_2-\mu_2, \ldots, \nu_n-\mu_n \qquad (\nu_1+\ldots+\nu_n)=(\mu_1+\ldots+\mu_n)$$

die erste nicht verschwindende Differenz positiv ist. Es ist z.B.

$$x_1^2x_3 = x_1^2x_2^0x_3^1 \text{ höher als } x_1x_3^2 = x_1^1x_2^0x_3^2 \text{ höher als } x_2^2x_3 = x_1^0x_2^2x_3^1$$

Da diese Beziehung transitiv ist, gibt es einen eindeutig bestimmten Term, der lexikographisch höher ist als alle anderen.

Für symmetrische homogene Polynome gilt: Der höchste Term hat die Eigenschaft

$$\nu_1 \geq \nu_2 \geq \ldots \geq \nu_n$$

Sonst gäbe es nämlich einen Exponenten ν_k mit $\nu_1 \geq \nu_2 \geq \ldots \geq \nu_k$, aber $\nu_k < \nu_{k+1}$. Wegen der Symmetrie gäbe es dann neben dem Term

$$x_1^{\nu_1}\ldots x_k^{\nu_k}.x_{k+1}^{\nu_{k+1}}\ldots x_n^{\nu_n}$$

auch noch den Term, der aus dem obigen durch Vertauschu ng von $x_k$und x_{k+1} entsteht:

$$x_1^{\nu_1}\ldots x_k^{\nu_k}.x_{k+1}^{\nu_{k+1}}\ldots x_n^{\nu_n} = x_1^{\nu_1}\ldots x_{k+1}^{\nu_{k+1}}.x_k^{\nu_k}\ldots x_n^{\nu_n}$$

Dieser Term wäre aber wegen $\nu_{k+1} - \nu_k > 0$ höher als der zuerst betrachtete.

Unmittelbar einsichtig sind die Sätze:

Produkt und Summe symmetrischer Polynome sind wieder symmetrische Polynome

Im Produkt zweier symmetrischen Polynome ist der höchste Term das Produkt der höchsten Terme der Faktoren

Schreibweise: Ist $x_1^{\nu_1}x_2^{\nu_2}\ldots x_n^{\nu_n}$ der höchste Term des symmetrischen Polynoms $f(x)$, so schreiben wir

$$H(f)=x_1^{\nu_1}x_2^{\nu_2}\ldots x_n^{\nu_n}$$

Für eine weiteres symmetrisches Polynom gilt dann

$$H(f.g) = H(f).H(g)$$

Elementarsymmetrische Funktionen

Seien x_1 , ... , x_n die Nullstellen des Polynoms

$$(x-x_1)(x-x_2)\cdots(x-x_n)=x^n-s_1x^{n-1}+s_2x^{n-2}-\ldots+(-1)^n s_n$$

dann sind

$$s_1=x_1+x_2+\ldots+x_n$$

$$s_2=x_1x_2+x_1x_3+\ldots+x_{n-1}x_n$$

$$s_3=x_1x_2x_3+x_1x_2x_4+\ldots+x_{n-2}x_{n-1}x_n$$

$$\vdots$$

$$s_n=x_1x_2x_3\cdots x_n$$

die *elementarsymmetrischen Funktionen* der Unbestimmten x_1, ..., x_n

Der Hauptsatz über symmetrische Funktionen

Jedes symmetrische Polynom läßt sich eindeutig als Polynom in den elementarsymmetrischen Funktionen darstellen

Es genügt, den Beweis für homogene Polynome zu führen. Es sei S ein homogenes symmetrisches Polynom mit

$$H(S)=x_1^{\nu_1}x_2^{\nu_2}\ldots x_n^{\nu_n}\qquad(\nu_1\geq\nu_2\geq\ldots\geq\nu_n)$$

Wir betrachten nun folgendes Polynom in den s_i.

$$P_0=s_1^{\nu_1-\nu_2}\cdot s_2^{\nu_2-\nu_3}\cdots s_{n-1}^{\nu_{n-1}-\nu_n}s_n^{\nu_n},\quad H(P_0)=H\left(s_1^{\nu_1-\nu_2}\right)\cdots H\left(s_n^{\nu_n}\right)$$

Da der höchste Term des Polynoms P_0 gleich dem Produkt der höchsten Terme der Faktoren ist, folgt für den höchsten Term von P_0

$$H(P_0)=(x_1)^{\nu_1-\nu_2}\cdot(x_1x_2)^{\nu_2-\nu_3}\cdot(x_1x_2x_3)^{\nu_3-\nu_4}\cdots(x_1\ldots x_{n-1})^{\nu_{n-1}-\nu_n}\cdot(x_1\ldots x_n)^{\nu_n}=x_1^{\nu_1}x_2^{\nu_2}\ldots x_n^{\nu_n}$$

d.h.

$$\underline{H(P_0)=H(S)}$$

P_0 ist also ein Polynom, welches in den x_i denselben Grad hat wie S und im höchsten Term mit S übereinstimmt. Das Polynom

$$S_1 := S - P_0$$

ist entweder das Nullpolynom, oder es ist vom selben Grad wie S, hat aber einen höchsten Term, der niedriger ist als der höchste Term von S. Analog definieren wir ein Polynom P_1 mit $H(P_1) = H(S_1)$ und erhalten

$$S_2 := S_1 - P_1$$

Auf diese Weise gelang man schließlich zu einem S_{k+1}, das verschwindet. Denn alle S_i haben denselben Grad, aber ständig abnehmende höchste Terme. Da die Höhe aber nicht beständig abnehmen kann, muß schließlich einmal der Fall eintreten, daß $S_{k+1} \equiv 0$ ist. Dann gilt

$$S = P_0 + P_1 + \ldots + P_k$$

Beispiel

$$S(x_1,x_2,x_3)=x_1^3x_2+x_1^3x_3+x_1x_2^3+x_1x_3^2+x_2^3x_3+x_2x_3^3$$

$$H(S)=x_1^3x_2x_3^0\quad\nu_1=3,\ \nu_2=1,\ \nu_3=0$$

$$P_0 := s_1^{\nu_1-\nu_2} s_2^{\nu_2-\nu_3} s_3^{\nu_3} = s_1^2 s_2^1 s_3^0 = (x_1+x_2+x_3)^2 (x_1x_2+x_1x_3+x_2x_3) =$$
$$= (x_1^3x_2 + x_1^3x_3 + x_1x_2^3 + x_1x_3^3 + x_2^3x_3 + x_2x_3^2) +$$
$$+ 2(x_1^2x_2^2 + x_1^2x_3^2 + x_2^2x_2^2) + 5(x_1^2x_2x_3 + x_1x_2^2x_3 + x_1x_2x_3^2)$$
$$S_1 = S - P_0 = -2(x_1^2x_2^2 + x_1^2x_3^2 + x_2^2x_2^2) - 5(x_1^2x_2x_3 + x_1x_2^2x_3 + x_1x_2x_3^2)$$
$$H(S_1) = -2x_1^2x_2^2 = -2x_1^2x_2^2x_3^0 \quad \nu_1 = 2,\ \nu_2 = 2,\ \nu_3 = 0$$
$$P_1 = -2s_1^{\nu_1-\nu_2} s_2^{\nu_2-\nu_3} s_3^{\nu_3} = -2s_2^2 = -2(x_1x_2 + x_1x_3 + x_2x_3)^2 =$$
$$= -2(x_1^2x_2^2 + x_1^2x_3^2 + x_2^2x_3^2) - 4(x_1^2x_2x_3 + x_1x_2^2x_3 + x_1x_2x_3^2)$$
$$S_2 = S_1 - P_1 = S - P_0 - P_1 = -(x_1^2x_2x_3 + x_1x_2^2x_3 + x_1x_2x_3^2)$$
$$H(S_2) = -x_1^2x_2x_3 \quad \nu_1 = 2,\ \nu_2 = 1,\ \nu_3 = 1$$
$$P_2 = -s_1^{\nu_1-\nu_2} s_2^{\nu_2-\nu_3} s_3^{\nu_3} = -s_1s_3 = -(x_1+x_2+x_3)(x_1x_2x_3) =$$
$$= -(x_1^2x_2x_3 + x_1x_2^2x_3 + x_1x_2x_3^2)$$
$$S_3 = S_2 - P_2 = S - P_0 - P_1 - P_2 = 0$$

Daher

$$\underline{S = P_0 + P_1 + P_2 = s_1^2s_2 - 2s_2^2 - s_1s_3}$$

Weitere Sätze über Polynome

Der Fundamentalsatz über irreduzible Polynome (Seite 8) lautete:

> Es sei $f(x)$ ein irreduzibles und $g(x)$ ein beliebiges Polynom über $\mathbb{K}$. Haben $f(x)$ und $g(x)$ in einem Erweiterungkörper $\mathbb{E}$ von $\mathbb{K}$ eine gemeinsame Nullstelle λ, so ist $f(x)$ eine Teiler von $g(x)$

Da $f(x)$ Teiler von $g(x)$ ist, folgt das Korollar

> Die Nullstellen von $f(x)$ in $\mathbb{E}$ sind auch Nullstellen von $g(x)$

Ferner gilt

> Die Nullstellen eines über $\mathbb{K}$ irreduziblen Polynoms in einem Erweiterungskörper $\mathbb{E}$ können nur einfach sein

BW indirekt: Sei λ eine mehrfache Nullstelle in einem Erweiterungskörper $\mathbb{E}$ von $\mathbb{K}$:

$f(x) = (x-\lambda)^k f_1(x) \quad k > 1$ die stellt keine Zerlegung über $\mathbb{K}$ dar, da $\lambda \notin \mathbb{K}$ ist

$f'(x) = k(x-\lambda)^{k-1} . f_1(x) + (x-\lambda)^k f_1'(x)$

Da $k > 1$ ist, ist λ auch Nullstelle von $f(x)$'. Da $f(x)$' aber ein Polynom über $\mathbb{K}$ ist, besitzt es mit $f(x)$ (Seite 7) einen *ggT* über $\mathbb{K}$, der nicht konstant ist. Daher kann $f(x)$ nicht irreduzibel über $\mathbb{K}$ sein. Widerspruch!

> Wenn ein irreduzibles Polynom $g(y)$ über $\mathbb{K}$ nach Adjunktion einer Nullstelle ξ des über $\mathbb{K}$ irreduziblen Polynoms $f(x)$ über $\mathbb{K}[\xi]$ reduzibel wird
>
> $$g(y) = h(y,\xi).h_1(y,\xi) \qquad (1)$$
>
> dann gilt dies für alle Nullstellen von $f(x)$

BW: Wir stellen beide Seiten von (1) explizit dar

$$g(y) = y^m + b_{m-1}y^{m-1} + \ldots + b_iy^i + \ldots + b_1y + b_0 =$$
$$= y^m + \varphi_{m-1}(\xi)y^{m-1} + \ldots + \varphi_i(\xi)y^i + \ldots + \varphi_1(\xi)y + \varphi_0(\xi)$$

Daraus ergibt sich durch Koeffizientenvergleich $\varphi_i(\xi) = b_i$, d.h. das Polynom $\varphi_i(\xi) - b_i = 0$ hat eine Nullstelle mit dem irreduziblen Polynom $f(x)$ gemeinsam, daher nach dem Korollar zum Fundamentalsatz alle Nullstellen.

Der Zerfällungssatz von KRONECKER

Seien $f(x)$ und $g(y)$ normierte irreduzible Polynome über $\mathbb{K}$, welche in einem geeigneten Erweiterungkörper $\mathbb{E}$ die Nullstellen

$$x_1, \ldots, x_n, y_1, \ldots, y_m$$

haben. Es sei $n = \textit{grd}\, f$, $m = \textit{grd}\, g$. Ferner sei η eine bestimmte Nullstelle von $g(y)$, die zu $\mathbb{K}$ adjungiert werde. Wir nehmen an, daß $f(x)$ im Körper $\mathbb{K}[\eta]$ reduzibel sei:

$$f(x) = \varphi(x,\eta).\varphi_1(x,\eta)$$

Dabei sei $\varphi(x,\eta)$ jener über $\mathbb{K}[\eta]$ irreduzible Faktor, für den für eine bestimmte Nullstelle $\xi \in \mathbb{K}[\eta]$ von $f(x)$ gilt

$$\varphi(\xi,\eta) = 0$$

Ist $k = \textit{grd}\, \varphi$, so folgt $k \le n$. Die Gleichheit gilt $k = n$ nur dann wenn $f(x)$ über $\mathbb{K}[\eta]$ irreduzibel ist.

Wird $f(x)$ durch die Adjunktion der speziellen Nullstelle η von $g(y)$ zu $\mathbb{K}$ reduzibel, dann auch bei Adjunktion einer beliebigen Nullstelle y_i von $g(y)$. Es gilt also

$$f(x) = \varphi(x,\eta).\varphi_1(x,\eta) \text{ für alle } \eta = y_1, \ldots, y_m$$

Multiplizieren wir alle diese Ausdrücke für $y_1, \ldots, y_m$, so erhält man

$$[f(x)]^m = \Phi(x).\Phi_1(x) \qquad (\bullet)$$

mit

$$\Phi = \prod_{j=1}^{m} \varphi(x,y_j) \qquad \Phi_1 = \prod_{j=1}^{m} \varphi_1(x,y_j)$$

$\Phi(x)$ und $\Phi_1(x)$ sind Polynome, deren Koeffizienten in den Nullstellen y_i von $g(y)$ symmetrisch sind, die daher Elemente von $\mathbb{K}$ sind.

Da $f(x)$ über $\mathbb{K}$ irreduzibel ist, folgt aus $(\bullet)$, daß sowohl $\Phi(x)$ als $\Phi_1(x)$ gewisse Potenzen von von $f(x)$ sein müssen, etwa

$$\Phi(x) = \varphi(x,y_1).\ \varphi(x,y_2)\ldots\ \varphi(x,y_m) = [f(x)]^{\mu}$$

Wegen $\textit{grd}\, \varphi = k$ gilt

$$mk = n\mu$$

Wegen $k \le n$ folgt $\dfrac{k}{n} = \dfrac{\mu}{m} \le 1 \Rightarrow \mu \le m$

Adjungieren wir umgekehrt eine Nullstelle ξ von $f(x)$ zu $\mathbb{K}$ und zerlegen $g(y)$ über $\mathbb{K}[\xi]$

$$g(y) = \psi(y,\xi).\psi_1(y,\xi)$$

Wieder sei $\psi(y,\xi)$ jener über $\mathbb{K}[\xi]$ irreduzible Faktor, der für eine bestimmte Nullstelle η von $g(y)$ verschwindet:

$$\psi(\eta,\xi) = 0$$

Es sei $l = \textit{grd}\, \psi \Rightarrow l \le m$. Wieder gilt $l = m$ nur dann, wenn $g(y)$ über irreduzibel ist. Wird $g(y)$ bei Adjunktion von ξ zu $\mathbb{K}$ über $\mathbb{K}[\xi]$ reduzibel, dann auch bei der Adjunktion einer beliebigen Nullstelle x_i von $f(x)$. Es gilt also

$$g(y) = \psi(y,\xi).\psi_1(y,\xi) \qquad \text{für alle } \xi = x_1, \ldots, x_n$$

Multiplikation aller dieser Ausdrücke ergibt

$$[g(y)]^n = \Psi(y).\Psi_1(y)$$

mit

$$\Psi(y) = \prod_{i=1}^{n} \psi(y, x_i)$$

Auch hier treten die Nullstellen von $f(x)$ symmetrisch auf, sodaß $\Psi(y)$ ein Polynom über $\mathbb{K}$ ist. Aus der Irreduzibilität von $g(y)$ folgt wie oben

$$\Psi(y) = [g(y)]^{\nu}$$

und wegen $grd\ \psi = l$ folgt $nl = m\nu$ und wegen $l \le m$ folgt

$$\frac{l}{m} = \frac{\nu}{n} \le 1 \Rightarrow \nu \le n$$

Wir betrachten nun die Polynome $\varphi(\xi,y)$ und $\psi(y,\xi)$. Hier ist $\psi(y,\xi)$ über $\mathbb{K}[\xi]$ irreduzibel, während wir über $\varphi(\xi,y)$ keine Aussage machen können.

Da $\varphi(\xi,y)$ und $\psi(y,\xi)$ die gemeinsame Nullstelle η haben

$$\varphi(\xi,\eta) = 0,\ \psi(\eta,\xi) = 0$$

sind wegen des Korollars (Seite 60) alle l Nullstellen von $\psi(y,\xi)$ auch Nullstellen von φ. Es gilt also

$$\varphi(\xi,\eta_r) = 0, \qquad r = 1, \ldots, l$$

Außer diesen l mit ψ gemeinsamen Nullstellen $\eta_1, \ldots, \eta_l$ kann $\varphi(\xi,y)$ auch noch andere Nullstellen η haben. Wir zeigen, daß es insgesamt μ solcher Werte η gibt. Es war

$$[f(x)]^{\mu} = \varphi(x,y_1)\ldots\varphi(x,y_m)$$

Nun ist, wegen $f(\xi) = 0$, der Wert ξ eine μ-fache Nullstelle der linken Seite. Wegen der Irreduzibilität von $\varphi(x,y_i)$ kann ξ nur eine einfache Nullstelle jedes Faktors der rechten Seite sein. Setzt man also $x = \xi$, so müssen genau μ Faktoren der rechten Seite verschwinden. Es gibt also insgesamt μ Werte η, für die $\varphi(\xi,\eta)$ verschwindet. Daher ist

$$\mu \le l \qquad (1)$$

Analog ergibt sich

$$\nu \le k \qquad (2)$$

Es gilt aber

$$\begin{aligned} mk = n\mu \ \wedge\ \nu \le k \ &\Rightarrow\ m\nu \le n\mu \Rightarrow nl \le n\mu \Rightarrow \underline{l \le \mu} \\ nl = m\nu \ \wedge\ \mu \le l \ &\Rightarrow\ n\mu \le m\nu \Rightarrow mk \le m\nu \Rightarrow \underline{k \le \nu} \end{aligned} \qquad (3)$$

Zusammen mit (1) und (2) ergibt das

$$\underline{l = \mu \text{ und } k = \nu \text{ und } mk = nl}$$

Zerfällungssatz von KRONECKER: Es seien $f(x)$ ($grd\ f = n$) und $g(y)$ ($grd\ g = m$) irreduzible normierte Polynome über dem Körper $\mathbb{K}$.. In einem geeignet gewählten Erweiterungskörper $\mathbb{E}$ von $\mathbb{K}$ seien

$x_1, \ldots, x_n$ die Nullstellen von $f(x)$

$y_1, \ldots, y_m$ die Nullstellen von $g(y)$

ξ, η sei ein beliebig ausgewähltes Paar dieser Nullstellen. Ferner sei $\varphi(x,\eta)$ ($grd\ \varphi = k$) jener irreduzible Faktor von $f(x)$ über $\mathbb{K}[\eta]$, der für $x = \xi$ verschwindet und $\psi(y, \xi)$

(*grd* $\psi = l$) jener irreduzible Faktor von $g(y)$ über $\mathbb{K}[\xi]$, der für $y = \eta$ verschwindet. Dann ist

$$\varphi(x,y_1) \dots \varphi(x,y_m) = [f(x)]^k$$
$$\psi(y,x_1) \dots \psi(y,x_n) = [g(y)]^l$$

und es gilt

$$mk = nl$$

Auch der folgende Satz stammt von KRONECKER

Ist das Binom

$$x^p - a, \quad a \in \mathbb{K}, \quad p \text{ Primzahl}$$

über dem Körper $\mathbb{K}$ reduzibel, so hat es eine Nullstelle, welche dem Körper $\mathbb{K}$ angehört

BW: Es sei

$$x^p - a = (c_0 + c_1x + \dots + c_{k-1}x^{k-1} + x^k)(d_0 + d_1x + \dots + d_{l-1}x^{l-1} + x^l)$$
$$k + l = p \Rightarrow k < p \quad (k \text{ gerade})$$

reduzibel über $\mathbb{K}$ und w sei jene Nullstelle $w^p = a$, für welche gilt

$$c_0 + c_1w + \dots + c_{k-1}w^{k-1} + w^k = 0 \qquad (\bullet)$$

Für alle Nullstellen $w_1, \dots, w_k$, welche $(\bullet)$ erfüllen, gilt

$$c_0 = w_1w_2 \dots w_k \text{ mit } w_i^p = a$$

Bildet man daher

$$c_0^p = w_1^p \dots w_k^p = a^k \Rightarrow c_0 = a^{\frac{k}{p}} \in \mathbb{K}$$

Das konstante Glied c_0 ist daher die k-te Potenz einer Nullstelle von $x^p - a$. Nun ist aber $k < p$, daher sind k und p teilerfremd und es gibt Elemente $r,s \in \mathbb{K}$, sodaß gilt (Seite 6)

$$rk + sp = 1 \Rightarrow \frac{r}{p}.k = \frac{1}{p} - s$$

also

$$c_0^r = \left(a^{\frac{k}{p}}\right)^r = a^{\frac{kr}{p}} = a^{\left(\frac{1}{p}-s\right)} = a^{\frac{1}{p}}.a^{-s} \Rightarrow \underline{a^{\frac{1}{p}} = c_0^r.a^s \in \mathbb{K}}$$

Es gibt also eine Nullstelle $w = a^{\frac{1}{p}}$, welche $\mathbb{K}$ angehört.

Kubische Gleichungen mit drei reellen Nullstellen

Das über seinem Koeffizientenkörper $\mathbb{K}_0 = \mathbb{Q}[a,b]$ irreduzible Polynom 3.Grades

$$x^3 + 3ax + 2b \qquad a,b \in \mathbb{R}$$

habe die Nullstellen x_1, x_2, x_3 mit den elementarsymmetrischen Funktionen

$$x_1 + x_2 + x_3 = 0$$
$$x_1x_2 + x_1x_3 + x_2x_3 = 3a$$
$$x_1x_2x_3 = -2b$$

Allgemein gilt nach CARDANO (Seite 54)

$$x_1 = u + v$$
$$x_2 = \varepsilon u + \bar{\varepsilon} v$$
$$x_3 = \bar{\varepsilon} u + \varepsilon v$$

$$u^3 = -b + \sqrt{b^2 + a^3}, \quad v^3 = -b - \sqrt{b^2 + a^3}$$

$$\varepsilon, \bar{\varepsilon} = \frac{-1 \pm i\sqrt{3}}{2}$$

$$\varepsilon + \bar{\varepsilon} = -1, \; \varepsilon + 1 = -\bar{\varepsilon}$$

$$\varepsilon.\bar{\varepsilon} = 1 = \varepsilon^3 = \varepsilon.\varepsilon^2 \Rightarrow \varepsilon^2 = \bar{\varepsilon} = \frac{1}{\varepsilon}$$

$$\varepsilon^2 + \varepsilon + 1 = 0$$

Wir setzen

$$\Delta = -(b^2 + a^3)$$

Ist

$$\Delta > 0 \Rightarrow a^3 + b^2 < 0 \Rightarrow u^3 = -b + i.\sqrt{\Delta}, \; v^3 = -b - i.\sqrt{\Delta}$$

so sind u und v konjugiert komplexe Größen. Daher sind alle drei Nullstellen reell. Allerdings kommen die reellen Nullstellen dadurch zustande, daß zunächst komplexe Wurzelausdrücke auftreten. Es erhebt sich die Frage, ob, von einer reellen Angabe ausgehend, das reelle Resultat nur über einen komplexen Umweg zu erreichen ist, oder ob die drei reellen Nullstellen einer Gleichung dritten Grades sich nicht durch reelle Wurzelausdrücke darstellen lassen.

Wir nehmen zunächst an, daß $\Delta > 0$ und daher x_1, x_2, x_3 reell sind. Wir berechnen

$$(x_1 - x_2)(x_2 - x_3)(x_3 - x_1) =$$
$$\left[(u+v) - (\varepsilon u + \varepsilon^2 v)\right].\left[(\varepsilon u + \varepsilon^2 v) - (\varepsilon^2 u + \varepsilon v)\right].\left[(\varepsilon^2 u + \varepsilon v) - (u+v)\right] =$$
$$\left[(1-\varepsilon)u + \underbrace{(1-\varepsilon^2)}_{\substack{(1+\varepsilon)(1-\varepsilon)= \\ -\varepsilon^2(1-\varepsilon)}} v\right].\left[\varepsilon(1-\varepsilon)u - \varepsilon(1-\varepsilon)v\right].\left[-\underbrace{(1-\varepsilon^2)}_{-\varepsilon^2(1-\varepsilon)} u - (1-\varepsilon)v\right] =$$
$$= -\varepsilon(1-\varepsilon)^3\left[u - \varepsilon^2 v\right].\left[u - v\right].\left[-\varepsilon^2 u + v\right] =$$
$$= -\varepsilon(1-\varepsilon)^3 (u-v)\left[-\varepsilon^2 u^2 + \underbrace{\varepsilon^4}_{\varepsilon} uv + uv - \varepsilon^2 v^2\right] =$$
$$= -\varepsilon(1-\varepsilon)^3 (u-v).\left[-\varepsilon^2(u^2 + v^2) + \underbrace{(1+\varepsilon)}_{-\varepsilon^2} uv\right] =$$
$$= \underbrace{\varepsilon^3}_{1}(1-\varepsilon)^3 (u-v).\left[u^2 + uv + v^2\right] = \underline{(1-\varepsilon)^3 (u^3 - v^3)}$$

Nun ist

$$\underline{(1-\varepsilon)^3} = 1 - 3\varepsilon + 3\varepsilon^2 - \underbrace{\varepsilon^3}_{1} = 3(\varepsilon^2 - \varepsilon) = \underline{3(\bar{\varepsilon} - \varepsilon)}$$

$$\underline{(\bar{\varepsilon} - \varepsilon)} = \frac{1}{2}\left[\left(-1 - i.\sqrt{3}\right) - \left(-1 + i.\sqrt{3}\right)\right] = \underline{-i.\sqrt{3}}$$

Wegen

$$u^3 - v^3 = 2i.\sqrt{\Delta}$$

ergibt sich

$$(x_1 - x_2)(x_2 - x_3)(x_3 - x_1) = 3.(-i.\sqrt{3}).2i.\sqrt{\Delta} = 6.\sqrt{3\Delta}$$

Daraus

$$x_1 - x_2 = \frac{6.\sqrt{3\Delta}}{(x_2 - x_3)(x_3 - x_1)} \qquad (\bullet)$$

Nun ist

$$(x_2 - x_3)(x_3 - x_1) = -x_3^2 - x_1x_2 + (x_2x_3 + x_1x_3)$$

Wegen

$$x_1x_2 + x_1x_3 + x_2x_3 = 3a \Rightarrow (x_1x_3 + x_2x_3) = 3a - x_1x_2$$

$$x_1x_2x_3 = -2b \Rightarrow x_1x_2 = -\frac{2b}{x_3}$$

Damit ergibt sich

$$(x_2 - x_3)(x_3 - x_1) = -x_3^2 + \frac{2b}{x_3} + 3a + \frac{2b}{x_3} = 3a + \frac{4b}{x_3} - x_3^2$$

Mit (•) folgt daraus

$$x_1 - x_2 = \frac{6.\sqrt{3\Delta}}{3a + \frac{4b}{x_3} - x_3^2}$$

$$x_1 + x_2 = -x_3$$

Hat eine über ihrem Koeffizientenkörper $\mathbb{K}_0$ irreduzible kubische Gleichung drei reelle Nullstellen , so läßt sich jede Nullstelle durch jede andere im Körper $\mathbb{K}_0\left(\sqrt{3\Delta}\right)$ rational darstellen

Ein Satz von HÖLDER

Es handelt sich also darum, wenigstens eine Nullstelle eines über dem Koeffizientenkörper irreduziblen Polynoms 3.Grades nur mit Hilfe reeller Wurzelausdrücke zu finden.

Wir adjungieren dem Körper $\mathbb{K}_0$ eine reelle Wurzel eines seiner Elemente mit beliebigem Primzahlexponenten. Ist das Polynom in diesem Erweiterungskörper nicht reduzibel, so adjungieren wir wiederum eine beliebige reelle Wurzel des Erweiterungkörpers. Sei $\mathbb{K} \subset \mathbb{R}$ der letzte Körper, über dem die Gleichung irreduzibel ist. Eine geeignet gewählte Wurzel aus einem Element von $\mathbb{K}$ mache aber die Gleichung reduzibel.

Es sei also das Polynom 3.Grades über $\mathbb{K}$ irreduzibel, werde aber reduzibel, wenn wir eine geeignete Wurzel eines Elementes aus $\mathbb{K}$ adjungieren.

Dann läge der Fall vor, daß über dem Körper $\mathbb{K}$ irreduzibles Polynom 3.Grades, bei dem jede Nullstelle reell und in jeder anderen rational ist, bei Adjunktion einer reellen Wurzel eines Elementes aus $\mathbb{K}$ reduzibel würde.

Daß dies nicht möglich ist, lehrt ein *Satz von HÖLDER*:

Ein in einem Körper $\mathbb{K}$ irreduzibles Polynom n-ten Grades mit einer reellen Nullstelle von der Eigenschaft, daß jede Nullstelle durch jede andere rational darstellbar ist, kann nicht durch Adjunktion einer reellen Wurzel mit Primzahlexponenten reduzibel werden, es sei denn, die adjungierte Wurzel ist eine Quadratwurzel; in diesem Falle muß aber n eine gerade Zahl sein.

BW: Es sei $f(x)$ das gegebene Polynom n-ten Grades mit einer reellen Nullstelle ξ, mit deren Hilfe man alle anderen Nullstellen in rationaler Weise darstellen kann.

Die zu adjungierende Wurzel sei Nullstelle des Polynoms

$$g(y) = y^p - a, \qquad a \in \mathbb{K}, \quad p \text{ Primzahl}$$

$g(y)$ ist gleichfalls über $\mathbb{K}$ irreduzibel. Wäre nämlich $g(y)$ über $\mathbb{K}$ reduzibel, so gäbe es nach KRONECKER eine Nullstelle $\eta \in \mathbb{K}$, und das müßte gerade die reelle p-te Wurzel aus a sein. Durch $\sqrt[p]{a} \in \mathbb{K}$ kann aber $f(x)$ nicht reduziert werden, da es nach Voraussetzung über $\mathbb{K}$ irreduzibel ist.

Wenden wir nun den Zerfällungssatz von KRONECKER auf die beiden über $\mathbb{K}_1$ irreduziblen Polynome an:

$$f(x) \Rightarrow \text{Nullstelle } \xi$$

$$g(y) \Rightarrow \text{Nullstelle } \eta$$

Es sei $f(x)$ reduzibel über $\mathbb{K}[\eta]$

$$f(x) = \varphi(x,\eta).\varphi_1(x,\eta) \text{ mit } \varphi(\xi,\eta) = 0, \; grd\, \varphi = k$$
$$\varphi(x,\eta) \text{ irreduzibel über } \mathbb{K}[\eta]$$

und $g(y)$ reduzibel über $\mathbb{K}[\xi]$

$$g(y) = \psi(y,\xi).\psi_1(y,\xi) \text{ mit } \psi(\eta,\xi) = 0 \; grd\, \psi = l$$
$$\psi(y,\xi) \text{ irreduzibel über } \mathbb{K}[\xi]$$

Dann gilt (hier ist $grd\, g = m = p$ Primzahl)

$$pk = nl$$

Wenn $k < n$ ist (d.h. wenn $f(x)$ über $\mathbb{K}[\eta]$ reduzibel ist), so gilt

$$\frac{k}{n} = \frac{l}{p} < 1 \Rightarrow l < p$$

Daher läßt sich wegen $k < n$ und $l < p$ der Bruch

$$\frac{n}{p} = \frac{k}{l}$$

kürzen. Da aber p eine Primzahl ist, muß p ein Teiler von n sein. Daraus entnehmen wir zunächst, daß ein Polynom 3.Grades (n = 3) durch Adjunktion einer Quadratwurzel nicht reduzibel ist, da 3 durch 2 nicht teilbar ist.

Wir nehmen nun wieder an, daß jede Nullstelle des Polynoms n-ten Grades reell und durch jede andere rational darstellbar sei. Ferner sei $f(x)$ bei Adjunktion von η über $\mathbb{K}[\eta]$ und $g(y)$ bei Adjunktion von ξ über $\mathbb{K}[\xi]$ reduzibel. Dann ist $k < n$ und $l < p$.

Unter den getroffenen Annahmen zerfällt $g(y)$ in irreduzible Faktoren desselben Grades

Es seien nämlich $x_1, \ldots, x_n$ die reellen, untereinander rational abhängigen Nullstellen von $f(x)$. Wir wählen eine dieser Nullstellen beliebig aus

$$\xi = x_1$$

Dann ist nach Voraussetzung

$$g(y) = \psi(y,\xi).\psi_1(y,\xi), \qquad \psi(y,\xi) \text{ irreduzibel über } \mathbb{K}[\xi]$$

Daraus folgt aber, daß $\psi(y,x_i)$ für alle Nullstellen $\xi = x_1, \ldots, x_n$ irreduzibel ist. Da nämlich die x_i rational zusammenhängen, gilt $\mathbb{K}[\xi] = \mathbb{K}[x_i]$ für beliebiges i. Ist aber $\psi(y,\xi)$ über $\mathbb{K}[\xi]$ irreduzibel, so bleibt es irreduzibel, wenn man ξ durch ein anderes Element desselben Körpers ersetzt.

Zwei irreduzible Polynome $\psi(y,x_i)$ und $\psi(y,x_j)$ stimmen überein oder sind teilerfremd.

Als irreduzibles Polynom über $\mathbb{K}[\xi]$ hat $\psi(y,x_i)$ keine mehrfachen Nullstellen (sonst wäre es reduzibel).

Jede Nullstelle der linken Seite von

$$g(y)^k = \psi(y,x_1)\dots \psi(y,x_n)$$

ist auch Nullstelle eines Faktors der rechten Seite. Da ber jedes $\psi(y,x_i)$ nur einfache Nullstellen hat, ist $g(y)$ das Produkt einer Teilmenge der Faktoren $\psi(y,x_1)$, ... , $\psi(y,x_n)$, zerfällt also in lauter Faktoren gleichen Grades $l = grd\ \psi$, ist demnach irgend ein Vielfaches α von l

$$grd\ g = p = \alpha.l$$

Da p eine Primzahl ist, muß $l = grd\ g = 1$ sein. $g(y)$ zerfällt daher in lauter Linearfaktoren.

Da nach Voraussetzung die Nullstellen x_1, ... , x_n alle reell sind, muß das über $\mathbb{K}[\xi]$ reduzible Polynom $g(y)$ lauter reelle Nullstellen haben. Daher muß

$$g(y) = y^p - a$$

lauter reelle Nullstellen aufweisen. Das ist abe nur bei p = 2 der Fall. Da, wie gezeigt, p und n einen gemeinsamen Teiler haben müssen, kann n keine ungerade Zahl (z.B n = 3) sein

Die Gleichung vierten Grades

Reduktion der allgemeinen Gleichung vierten Grades

Sind z_1, z_2, z_3, z_4 die Nullstellen des Polynoms vierten Grades

$$z^4 + a_1z^3 + a_2z^2 + a_1z + a_4 = 0 \qquad a_1 \in \mathbb{R}$$

so gilt

$$z^4 + a_1z^3 + a_2z^2 + a_1z + a_4 = (z - z_1)\,(z - z_2)\,(z - z_3)\,(z - z_4)$$

Daher ist

$$a_1 = -(z_1 + z_2 + z_3 + z_4)$$
$$a_2 = (z_1z_2 + z_1z_3 + z_1z_4 + z_2z_3 + z_2z_4 + z_3z_4)$$
$$a_3 = -(z_1z_2z_3 + z_1z_2z_4 + z_1z_3z_4 + z_2z_3z_4)$$
$$a_4 = (z_1z_2z_3z_4)$$

Führt man durch die Substitution

$$z = x + s$$

die neue Unbestimmte x ein, so gilt

$$z_1 + z_2 + z_3 + z_4 = x_1 + x_2 + x_3 + x_4 + 4s = -a_1$$

Fordert man, daß $x_1 + x_2 + x_3 + x_4 = 0$ sei, so muß

$$s = -\frac{a_1}{4}$$

sein und man erhält die *reduzierte Gleichung*

$$x^4 + ax^2 + bx + c = 0$$
$$x_1 + x_2 + x_3 + x_4 = 0$$
$$x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4 = a$$
$$x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4 = -b$$
$$x_1x_2x_3x_4 = c$$

Bestimmung der Nullstellen der reduzierten Gleichung nach DESCARTES[1]

Wir versuchen, die reduzierte biquadratische Gleichung in zwei quadratische Faktoren zu zerlegen

$$x^4 + ax^2 + bx + c = (x^2 - px + q)(x^2 + px + r) = x^4 + (q - p^2 + r)x^2 + p(q - r)x + qr$$

1. Sonderfall p =0. Der Ansatz reduziert sich auf $x^4 + (q + r)x^2 + qr = 0$. Die Gleichung nimmt mit $y := x^2$ die Gestalt $y^2 + (q + r)y + qr = 0$ (*quadratische Resolvente*) an und kann daher duch Quadratwurzelschachtelungen gelöst werden.

2. Allgemeiner Fall p ≠ 0. Dann ergibt der Koeffizientenvergleich

$$q + r - p^2 = a$$
$$p(q - r) = b$$
$$qr = c \qquad (*)$$

[1] René DESCARTES (Géométrie 1637) 1601-1665

$$\left.\begin{aligned} q+r &= a+p^2 \\ q-r &= \frac{b}{p} \end{aligned}\right\} +|-$$

$$\left.\begin{aligned} 2q &= \left(a+p^2\right)+\frac{b}{p} \\ 2r &= \left(a+p^2\right)-\frac{b}{p} \end{aligned}\right\} \bullet$$

$$4qr = \left(a+p^2\right)^2 - \frac{b^2}{p^2} \overset{(*)}{=} 4c \Rightarrow p^4 + 2ap^2 + a^2 - \frac{b^2}{p^2} = 4c$$

Daraus

$$p^6 + 2ap^4 + \left(a^2 - 4c\right)p^2 - b^2 = 0$$

Die Substitution

$$y := p^2$$

ergibt die *kubische Resolvente von DESCARTES*

$$\boxed{\begin{aligned} &y^3 + 2ay^2 + \left(a^2 - 4c\right)y - b^2 = 0 \\ &p = \sqrt{y} \\ &q = \frac{1}{2}\left(a+p^2\right)+\frac{b}{2p} \\ &r = \frac{1}{2}\left(a+p^2\right)-\frac{b}{2p} \end{aligned}}$$

Diskussion der Lösung nach DESCARTES

$x^2 - px + q = 0 \Rightarrow x_1, x_2 \qquad x_1 + x_2 = p$

$x^2 + px + q = 0 \Rightarrow x_3, x_4 \qquad x_3 + x_4 = -p$

Die Gleichung für p ist vom 6.Grad, da sich die Summe je zweier Nullstellen auf 6 Arten bilden läßt:

$$\pm p = \begin{cases} x_1 + x_2 \\ x_1 + x_3 \\ x_1 + x_4 \\ x_2 + x_3 \\ x_2 + x_4 \\ x_3 + x_4 \end{cases}$$

Da je zwei der 6 Möglichkeiten entgegengesetztes Vorzeichen haben, läßt sich der Grad auf drei reduzieren und man erhält die kubische Resolvente

Da in der kubischen Resolvente das konstante Glied stets negativ ist, gilt für deren Nullstellen

$$y_1 y_2 y_3 = b^2 > 0$$

Daher ist stets mindesten eine Nullstelle der Resolvente positiv und daher gibt es mindestens einen p-Wert, der reell und positiv ist $p := \sqrt{y}$. Dann gilt

$$x^2 - px + \left(\frac{1}{2}(a+p^2) + \frac{b}{2p}\right) = 0 \Rightarrow x_1, x_2$$

$$x^2 + px + \left(\frac{1}{2}(a+p^2) - \frac{b}{2p}\right) = 0 \Rightarrow x_3, x_4$$

$$x_{1,2} = \frac{p}{2} \pm \sqrt{\frac{p^2}{4} - \frac{1}{2}(a+p^2) - \frac{b}{2p}} = \frac{p}{2} \pm \sqrt{-\frac{b}{2p} - \frac{1}{2}\left(a + \frac{p^2}{2}\right)}$$

$$x_{3,4} = -\frac{p}{2} \pm \sqrt{+\frac{b}{2p} - \frac{1}{2}\left(a + \frac{p^2}{2}\right)}$$

Es genügt also die Kenntnis der positiven Nullstelle der Resolvente

Fallunterscheidungen

Untersuchung der Vorzeichen der Radikanden ergibt

$$\left.\begin{aligned} -\frac{b}{2p} - \frac{1}{2}\left(a + \frac{p^2}{2}\right) > 0 \Rightarrow -\frac{b}{p} > a + \frac{p^2}{2} \\ +\frac{b}{2p} - \frac{1}{2}\left(a + \frac{p^2}{2}\right) > 0 \Rightarrow +\frac{b}{p} > a + \frac{p^2}{2} \end{aligned}\right\} \Rightarrow \boxed{\left|\frac{b}{p}\right| > a + \frac{p^2}{2} \quad \text{4 getrennte reelle Nullstellen}}$$

$$\boxed{\left|\frac{b}{p}\right| < a + \frac{p^2}{2} \quad \text{2 Paare konjugiert komplexer Nullstellen}}$$

$$\left.\begin{aligned} -\frac{b}{p} > a + \frac{p^2}{2} \text{ und } \frac{b}{p} < a + \frac{p^2}{2} \\ \text{oder} \\ -\frac{b}{p} < a + \frac{p^2}{2} \text{ und } \frac{b}{p} < a + \frac{p^2}{2} \end{aligned}\right\} \text{2reelle und 2 konjugiert komplexe Nullstellen}$$

Ferner entnimmt man

> Hat die Resolvente eine rationale Nullstelle, so lassen sich die Nullstellen der biquadratischen Gleichung duch Quadratwurzelausdrücke darstellen

Es gilt aber auch die Umkehrung

> Ist die biquadratische Gleichung durch Quadratwurzelschachtelungen lösbar, so hat die kubische Resolvente eine rationale Nullstelle

Ist die vorliegende Gleichung biquadratisch, so können ihre Nullstellen höchstens zwei unabhängige Quadratwurzeln enthalten ($m = 2$) und höchstens zwei Quadratwurzeln übereinandergeschachtelt sein ($\mu = 2$). Es gibt demnach folgende Möglichkeiten für das Aussehen der Nullstellen

1.Fall:

$$x_1 = \alpha+\beta.\sqrt{\rho}+\gamma.\sqrt{\sigma}+\delta.\sqrt{\rho}.\sqrt{\sigma} = \left(\alpha+\beta.\sqrt{\rho}\right)+\sqrt{\sigma}\left(\gamma+\delta\sqrt{\rho}\right) = A+B\sqrt{\sigma}$$
$$x_2 = \alpha-\beta.\sqrt{\rho}+\gamma.\sqrt{\sigma}-\delta.\sqrt{\rho}.\sqrt{\sigma} = \left(\alpha-\beta.\sqrt{\rho}\right)+\sqrt{\sigma}\left(\gamma-\delta\sqrt{\rho}\right) = C+D\sqrt{\sigma}$$
$$x_3 = \alpha+\beta.\sqrt{\rho}-\gamma.\sqrt{\sigma}-\delta.\sqrt{\rho}.\sqrt{\sigma} = \left(\alpha+\beta.\sqrt{\rho}\right)-\sqrt{\sigma}\left(\gamma+\delta\sqrt{\rho}\right) = A-B\sqrt{\sigma}$$
$$x_4 = \alpha-\beta.\sqrt{\rho}-\gamma.\sqrt{\sigma}+\delta.\sqrt{\rho}.\sqrt{\sigma} = \left(\alpha-\beta.\sqrt{\rho}\right)-\sqrt{\sigma}\left(\gamma-\delta\sqrt{\rho}\right) = C-D\sqrt{\sigma} \qquad (\bullet)$$
$$\alpha,\beta,\gamma,\delta,\rho,\sigma \in \mathbb{Q}$$

$$(x-x_1)(x-x_3) = \left[x-\left(A+B\sqrt{\sigma}\right)\right]\left[x-\left(A-B\sqrt{\sigma}\right)\right] = x^2-2Ax+\left(A^2-\sigma B^2\right)$$
$$(x-x_2)(x-x_3) = \left[x-\left(C+D\sqrt{\sigma}\right)\right]\left[x-\left(C-D\sqrt{\sigma}\right)\right] = x^2-2Cx+\left(C^2-\sigma D^2\right)$$

Daraus

$$f(x) = (x-x_1)(x-x_3)(x-x_3)(x-x_4) = \left[x^2-2Ax+\left(A^2-\sigma B^2\right)\right]\left[x^2-2Cx+\left(C^2-\sigma D^2\right)\right]$$
$$= x^4-2(A+C)x^3+\left[(A+C)^2+2AC-\sigma\left(B^2+D^2\right)\right]x^2-2\left[AC(A+C)-\sigma\left(AD^2+B^2C\right)\right]x$$
$$+\left(A^2-\sigma B^2\right)\left(C^2-\sigma D^2\right)$$

Führt man hierin vermöge $(\bullet)$ die Größen $\alpha,\beta,\gamma,\delta,\rho,\sigma \in \mathbb{Q}$ ein, so ergibt sich die Darstellung

$$f(x) = x^4-4\alpha x^3+2\left(3\alpha^2-\beta^2\rho-\delta^2\rho\sigma-\gamma^2\sigma\right)x^2-4\left[\alpha^3-\alpha\left(\beta^2\rho+\delta^2\rho\sigma+\gamma^2\sigma\right)+2\beta\gamma\delta\rho\sigma\right]x+$$
$$\left[\left(\alpha^2-\gamma^2\sigma\right)^2+\rho^2\left(\beta^2-\delta^2\sigma\right)^2-2\rho(\alpha\beta-\gamma\delta\sigma)^2-2\rho\sigma(\alpha\delta-\beta\gamma)^2\right]$$

Mit Hilfe der Substitution

$$x = z+\alpha$$

erhält man die reduzierte Gleichung

$$z^4\underbrace{-2\left[\beta^2\rho+\sigma\left(\delta^2 r+g^2\right)\right]}_{a}z^2\underbrace{-8\beta\gamma\delta\rho\sigma}_{b}.z+\underbrace{\left[\left(\beta^2\rho-\delta^2\rho\sigma-\gamma^2\sigma\right)^2-4\delta^2\rho\sigma^2\gamma\right]}_{c}$$

Daher lautet die kubische Resolvente

$$y^3+2ay^2+\left(a^2-4c\right)y-b^2 =$$
$$y^3-4\left[\beta^2\rho+\sigma\left(\delta^2\rho+\gamma^2\right)\right]y^2+16\rho\sigma\left[\beta^2\left(\delta^2\rho+\gamma^2\right)+\gamma^2\delta^2\sigma\right]y-16\beta^2\gamma^2\delta^2\rho^2\sigma^2$$

Man erkennt, daß es drei rationale Nullstellen der Resolvente gibt, nämlich

$$y_1 = 4\beta^2\rho,\quad y_2 = 4\delta^2\rho\sigma,\quad y_3 = 4\gamma^2\delta$$

2.Fall:

$$x_1 = \alpha+\beta\sqrt{\rho}+\sqrt{\gamma+\delta\sqrt{\rho}}$$
$$x_2 = \alpha-\beta\sqrt{\rho}+\sqrt{\gamma-\delta\sqrt{\rho}}$$
$$x_3 = \alpha+\beta\sqrt{\rho}-\sqrt{\gamma+\delta\sqrt{\rho}}$$
$$x_4 = \alpha-\beta\sqrt{\rho}-\sqrt{\gamma-\delta\sqrt{\rho}}$$

Daraus

$$(x-x_1)(x-x_3) = x^2-2\left(\alpha+\beta\sqrt{\rho}\right)x+\left[\left(\alpha+\beta\sqrt{\rho}\right)^2-\left(\gamma+\delta\sqrt{\rho}\right)\right]$$
$$(x-x_2)(x-x_4) = x^2-2\left(\alpha-\beta\sqrt{\rho}\right)x+\left[\left(\alpha-\beta\sqrt{\rho}\right)^2-\left(\gamma-\delta\sqrt{\rho}\right)\right]$$

Also

$$f(x)=(x-x_1)(x-x_2)(x-x_3)(x-x_4)=$$
$$=\left\{x^2-2\left(\alpha+\beta\sqrt{\rho}\right)x+\left[\left(\alpha+b\sqrt{\rho}\right)^2-\left(\gamma+\delta\sqrt{\rho}\right)\right]\right\}\left\{x^2-2\left(\alpha-\beta\sqrt{\rho}\right)x+\left[\left(\alpha-\beta\sqrt{\rho}\right)^2-\left(\gamma-\delta\sqrt{\rho}\right)\right]\right\}$$
$$=x^4-4\alpha x^3+2\left[2\alpha^2+\left(\alpha^2-\beta^2\rho-\gamma\right)\right]x^2-4\left[\alpha\left(\alpha^2-\beta^2\rho-\gamma\right)+\beta\delta\rho\right]x$$
$$+\left[\left(\alpha^2-\beta^2\rho-\gamma\right)^2+4\beta\rho(\alpha\delta-\beta\gamma)-\delta^2\rho\right]=0$$

Die Substitution z := x - α ergibt die reduzierte Gleichung

$$z^4-2\left(\beta^2\rho+\gamma\right)z^2-4\beta\delta\rho.z+\left[\left(\beta^2\rho-\gamma\right)^2-\delta^2\rho\right]=0$$

deren Resolvente lautet

$$y^3-4\left(\beta^2\rho+\gamma\right)y^2+4\rho\left(4\beta^2\gamma+\delta^2\right)y-16\beta^2\delta^2\rho=0$$

Man erkennt sofort, daß $y = 4\beta^2\rho$ eine rationale Nullstelle der Resolvente ist. Die beiden restlichen Nullstellen ($y=2\gamma\pm2\sqrt{\gamma^2-\delta^2\rho}$) sind i.a nicht rational.

Methode von FERRARI[1]

FERRARI zerlegt die gegebene biquadratische Gleichung zunächst in die Differenz zweier Quadrate

$$x^4 + ax^2 + bx + c = (x^2 + q)^2 - (rx + s)^2 \qquad (1)$$

Sobald dies gelungen ist, kann man die biquadratische Gleichung in das Produkt zweier quadratischen Ausdrücke zerlegen

$$[(x^2 + q) + (rx + s)].[(x^2 + q) - (rx + s)]$$

Aus dem Ansatz (1) folgt

$$(x^2 + q)^2 - (x^4 + ax^2 + bx + c) = (rx + s)^2 \qquad (2)$$

Wir haben also die linke Seite zu einem Quadrat zumachen

$$x^4 + 2qx^2 + q^2 - x^4 - ax^2 - bx - c = (2q - a)x^2 - bx + (q^2 - c) \qquad (3)$$

Wegen

$$(ux \pm v)^2 = u^2.x^2 \pm 2uv.x + v^2 \Leftrightarrow (2uv)^2 = 4.u^2.v^2$$

muß gelten

$$b^2 = 4.(2q-a)\,(q^2 - c) = 8q^3 - 4aq^2 - 8cq + 4ac$$

Setzen wir

$$q=\frac{y}{2}$$

so erhalten wir die *Resolvente von FERRARI*

$$\boxed{y^3 - ay^2 - 4cy + 4ac - b^2 = 0}$$

als Bedingung dafür, daß (2) bzw. (3) zu einem Quadrat wird. Mit einer beliebigen Nullstelle der Resolvente gilt dann

$$(3)\Rightarrow(y-a)x^2-bx+\frac{y^2}{4}-c=(y-a)\left[x^2-\frac{b}{y-a}x+\frac{y^2-4c}{4(y-a)}\right]=\underline{(y-a)\left[x-\frac{b}{2(y-a)}\right]^2}$$

Daher gilt wegen (2)

[1] Ludovico FERRARI (1522-1565) 1545

$$\left(x^2+q\right)^2-\left(x^4+ax^2+bx+c\right)=\left(x^2+\frac{y}{2}\right)^2-\left(x^4+ax^2+bx+c\right)=(y-a)\left[x-\frac{b}{2(y-a)}\right]^2$$

Daher

$$\left(x^4+ax^2+bx+c\right)=\left(x^2+\frac{y}{2}\right)^2-(y-a)\left[x-\frac{b}{2(y-a)}\right]^2=$$
$$\left[\left(x^2+\frac{y}{2}\right)+\sqrt{y-a}\left(x-\frac{b}{2(y-a)}\right)\right]\cdot\left[\left(x^2+\frac{y}{2}\right)-\sqrt{y-a}\left(x-\frac{b}{2(y-a)}\right)\right]$$

Methode von EULER[1]

Zur Lösung der reduzierten biquadratischen Gleichung

$$x^4 + ax^2 + bx + c = 0$$

verallgemeinert EULER die Methode von HUDDE zur Herleitung der CARDANischen Formeln durch den Ansatz

$2x = u+v+w$

$4x^2 = (u^2 + v^2 + w^2) + 2(uv + uw + vw)$

$16x^4 = (u^2 +v^2 + w^2)^2 + 4(u^2 +v^2 + w^2)\,(uv + uw + vw) +$
$+ 4(u^2v^2 + u^2w^2+ v^2w^2) + 8uvw(u+v+w)$

Daraus folgt

$16(x^4 + ax^2 + bx + c) =$
$= [(u^2 +v^2 + w^2)^2 + 4(u^2v^2 + u^2w^2+ v^2w^2) + 4a(u^2 + v^2 + w^2)+16c] +$
$+[4(uv + uw + vw)(u^2 + v^2 + w^2 + 2a)] + [8(u+v+w)(uvw + b)]$

Um diesen Ausdruck zum Verschwinden zu bringen, setzen wir zunächst

$u^2 + v^2 + w^2+ 2a = 0 \Rightarrow u^2 + v^2 + w^2 = -2a$ (1)

$uvw + b = 0 \Rightarrow uvw = - b$ (2)

Dann bleibt nur noch die Erfüllung der Bedingung

$(u^2 +v^2 + w^2)^2 + 4(u^2v^2 + u^2w^2+ v^2w^2) + 4a(u^2 + v^2 + w^2)+16c = 0$

Mit (1) wird daraus

$4a^2 + 4(u^2v^2 + u^2w^2+ v^2w^2) + 4a(-2a) + 16c = 0$

daher

$u^2v^2 + u^2w^2+ v^2w^2 = a^2 -4c$ (3)

Setzen wir

$$y_1 := u^2,\ y_2 := v^2,\ y_3 = w^2$$

so stellen die Ausdrücke (1), (2) und (3) nach VIETA

$$y_1 + y_2 + y_3 = -2a$$
$$y_1y_2 + y_1y_3 + y_3y_2 = a_2 - 4c$$
$$y_1y_2y_3 = b^2$$

die Koeffizienten der Gleichung mit den Nullstellen y_1, y_2, y_3 dar. Es ergibt sich die *Resolvente von EULER*

$$y^3 +2ay^2 +(a^2 - 4c) -b^2 = 0$$

[1] Leonhard EULER (1707-1783) 1738

Sie ist identisch mit der Resolventevon DESCARTES. Die Resolvente von FERRARI ergibt sich daraus durch die Substituion $y \rightarrow y - a$

y sei eine Nullstelle der Resolvente. Dann gilt

$$2x = u + v + w = \sqrt{y1} + \sqrt{y2} + \sqrt{y_3}$$

Für die Quadratwurzeln gibt es folgende Vorzeichenkombinationen

$$\begin{array}{ll} +++ & -++ \\ ++- & -+- \\ +-+ & --+ \\ +-- & --- \end{array}$$

Nach (2) spielt das Vorzeichen nur bei

$$uvw = \sqrt{y_1 y_2 y_3} = -b$$

eine Rolle. Wir haben daher die Vorzeichen so zu wählen, daß gilt

$$\boxed{\sqrt{y_1} \cdot \sqrt{y_2} \cdot \sqrt{y_3} = -b}$$

Zwei Vorzeichen können also beliebig gewählt werden, das dritte ist dann bestimmt. Die zweite mögliche Vorzeichenwahl ergäbe dann eine Lösung der Gleichung

$$x^4 + ax^2 - bx + c = 0$$

Diskussion

Wegen $y_1 y_2 y_3 = b^2 > 0$ gibt es folgende Fälle zu unterscheiden

1.Fall: y_1, y_2, y_3 positiv, daher $\sqrt{y_1}, \sqrt{y_2}, \sqrt{y_3}$ reell

Daher gilt

b positiv (Schema 1)	b negativ (Schema 2)
$2x_1 = \sqrt{y_1} + \sqrt{y_2} + \sqrt{y_3}$	$2x_1 = \sqrt{y_1} - \sqrt{y_2} - \sqrt{y_3}$
$2x_2 = \sqrt{y_1} - \sqrt{y_2} + \sqrt{y_3}$	$2x_2 = -\sqrt{y_1} + \sqrt{y_2} - \sqrt{y_3}$
$2x_3 = -\sqrt{y_1} + \sqrt{y_2} + \sqrt{y_3}$	$2x_3 = -\sqrt{y_1} - \sqrt{y_2} + \sqrt{y_3}$
$2x_4 = -\sqrt{y_1} - \sqrt{y_2} - \sqrt{y_3}$	$2x_4 = -\sqrt{y_1} - \sqrt{y_2} - \sqrt{y_3}$

Alle vier Nullstellen x_i sind reell

2.Fall: $y_1 > 0$; y_2, $y_3 < 0$; $y_2 \neq y_3 \Rightarrow$ Daher $\sqrt{y_2} = \hat{\imath}.z_1$, $\sqrt{y_3} = \hat{\imath}.z_2$, rein imaginär $\Rightarrow$

Alle vier Nullstellen sind komplex. Ist b positiv, so gilt das 2.Schema von Fall 1, ist b negativ gilt das 1.Schema von Fall 1.

Ist $y_2 = y_3$, so treten eine doppelt zählende reelle, sowie zwei konjugiert komplexe Nullstellen auf. Ist b positiv, so gilt das 2.Schema von Fall 1, ist b negativ gilt das 1.Schema von Fall 1.

3.Fall: $y_1 > 0$, y_2, y_3 konjugiert komplex

Dann sind auch die Wurzeln $\sqrt{y_2} = \lambda + \hat{\imath}.\mu$, $\sqrt{y_3} = \lambda - \hat{\imath}.\mu$ konjugiert komplex. Zwei der vier Nullstellen sind reell, zwei konjugiert komplex. Ist b positiv, so gilt das 1.Schema von Fall 1, ist b negativ gilt das 2.Schema von Fall 1.

Gemeinsame Behandlung der verschiedenen Methoden zur Lösung von biquadratischen Gleichungen

Allen Auflösungsmethoden der Gleichungen 4.Grades liegt das Prinzip zu Grunde, Funktionen der Nullstellen zu bilden, welche bei beliebiger Vertauschung der Nullstellen nur drei Werte annehmen, nämlich die Nullstellen y_1, y_2, y_3 der kubischen Resolvente. Es gibt folgende Möglichkeiten

$$x_1x_2 + x_3 x_4$$
$$(x_1 + x_2)(x_3 + x_4)$$
$$(x_1x_2 - x_3 x_4)^2$$
$$(x_1 + x_2 - x_3 - x_4)^2$$

Wir betrachten als Beispiel nur den ersten Fall (LAGRANGE 1770 und WILSON 1792)

$y_1 = x_1 x_2 + x_3 x_4$

$y_2 = x_1 x_3 + x_2 x_4$

$y_3 = x_1 x_4 + x_2 x_3$

Wir bilden die elementarsymmetrischen Funktionen σ_i der Nullstellen y_i der kubischen Resolvente (siehe Seite 59) mit Hilfe der elementarsymmetrischen Funktionen s_j der x_i

$\underline{\sigma_1 = y_1 + y_2 + y_3} = x_1 x_2 + x_3 x_4 + x_1 x_3 + x_2 x_4 + = \underline{s_2}$

$\sigma_2 = y_1y_2 + y_1y_3 + y_2y_3 =$

$$= \left(x_1^2x_2x_3 + x_1x_2^2x_4 + x_1x_3^2x_4 + x_2x_3x_4^2\right) + y_1y_3 + y_2y_3 = S\left(x_1^2x_2x_3x_4^0\right)$$

$$H\left(x_1^2x_2x_3x_4^0\right)..P_0 = s_1s_3 = (x_1 + x_2 + x_3 + x_4)(x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4) = \ldots =$$

$$= S\left(x_1^2x_2x_3x_4^0\right) + 4s_4$$

Daher

$$S\left(x_1^2x_2x_3x_4^0\right) = s_1s_3 - 4s_4$$

Also

$\underline{\sigma_2 = y_1y_2 + y_1y_3 + y_2y_3 = s_1s_3 - 4s_4}$

$$\sigma_3 = y_1y_2y_3 = (x_1 x_2 + x_3 x_4)(x_1 x_3 + x_2 x_4)(x_1 x_4 + x_2 x_3) = \ldots = S\left(x_1^3x_2x_3x_4\right) + S\left(x_1^2x_2^2x_3^2x_4^0\right)$$

$$H\left(x_1^3x_2x_3x_4\right).P_0 = s_1^2s_4 = \left(x_1 + x_2 + x_3\right)^2\left(x_1x_2x_3x_4\right) = \ldots = S\left(x_1^3x_2x_3x_4\right) + 2s_2s_4$$

$$S\left(x_1^3x_2x_3x_4\right) = s_1^2 - 2s_2s_4$$

$$H\left(x_1^2x_2^2x_3^2x_4^0\right).P_0 = s_3^2 = \left(x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4\right)^2 = \ldots =$$

$$= S\left(x_1^2x_2^2x_3^2x_4^0\right) + 2S\left(x_1^2x_2^2x_3x_4\right)$$

$$H\left(x_1^2x_2^2x_3x_4\right).P_0 = s_2s_4 = \left(x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4\right)\left(x_1x_2x_3x_4\right) = S\left(x_1^2x_2^2x_3x_4\right)$$

Daher

$$S\left(x_1^2x_2^2x_3x_4\right) = s_2s_4$$

mithin

$$S\left(x_1^2x_2^2x_3^2x_4\right) = s_3^2 - 2s_2s_4$$

Daher

$$\underline{\sigma_3 = y_1y_2y_3} = \left(s_1^2s_4 - 2s_2s_4\right) + \left(s_3^2 - 2s_2s_4\right) = \underline{s_1^2s_4 + s_3^2 - 4s_2s_4}$$

Somit sind y_1, y_2, y_3 Nullstellen der *kubischen Resolvente*

$$y^3 - s_2 y^2 + (s_1 s_3 - 4s_4)y - (s_1^2 s_4 + s_3^2 - 4s_2 s_4) = 0$$

Liegt die gegebene biquadratische Gleichung in reduzierter Form vor

$$x^4 + ax^2 + bx + c = 0 \Rightarrow s_1 = 0,\ s_2 = a,\ s_3 = b,\ s_4 = c$$

Dann lautet die Resolvente

$$y^3 - ay^2 - 4cy + (4ac - b^2) = 0$$

Es ist dies die Resolvente von FERRARI

Berechnung der Nullstellen

$$x^4 + ax^2 + bx + c = 0$$

sei die reduzierte biquadratische Gleichung und

$$y^3 - ay^2 - 4cy + (4ac - b^2) = 0$$

die zugehörige kubische Resolvente, für deren Nullstellen gilt

$y_1 = x_1 x_2 + x_3 x_4$

$y_2 = x_1 x_3 + x_2 x_4$

$y_3 = x_1 x_4 + x_2 x_3$

Wir zeigen, daß mit Hilfe einer einzigen Nullstelle y der Resolvente alle Nullstellen x_i der biquadratischen Gleichung bestimmt werden können.

Es sei

$$y = x_1 x_2 + x_3 x_4 \qquad (1)$$

Ferner gilt

$$(x_1x_2)(x_3x_4) = c \Rightarrow x_3x_4 = \frac{c}{x_1x_2} \Rightarrow y = x_1x_2 + \frac{c}{x_1x_2} \Rightarrow \underline{(x_1x_2)^2 - y(x_1x_2) + c = 0}$$

Das Produkt $z_1 = (x_1x_2)$ ist also Nullstelle der quadratischen Gleichung

$$z^2 - yz + c = 0$$

Wegen $c = z_1z_2 = (x_1x_2)z_2$ sind $z_1 = x_1x_2$ und $z_2 = x_3x_4$, sodaß gilt

$$z_{1,2} = \frac{1}{2}\left[y \pm \sqrt{y^2 - 4c}\right]$$

Setzt man

$$w = \sqrt[+]{y^2 - 4c}$$

so folgt

$$x_1x_2 = \frac{1}{2}[y + w] \qquad (2)$$

$$x_3x_4 = \frac{1}{2}[y - w] \qquad (3)$$

Ferner gilt

$$(x_1x_2 + x_3x_4) + (x_1x_3 + x_2x_4 + x_1x_4 + x_2x_3) = a \Rightarrow \underline{y + (x_1 + x_2)(x_3 + x_4) = a} \qquad (4)$$

$$(x_1 + x_2) + (x_3 + x_4) = 0 \Rightarrow \underline{(x_1 + x_2) = -(x_3 + x_4)} \qquad (5)$$

Mit (4) und (5) ergibt sich daher

$$y - a = -(x_1 + x_2)(x_3 + x_4) = \underline{(x_1 + x_2)^2 = (x_3 + x_4)^2 = y - a} \qquad (6)$$

Zusammen mit (2), (3) und (6) folgt

$$x_1 + x_2 = \pm\sqrt{y-a} \qquad x_3 + x_4 = \mp\sqrt{y-a}$$
$$x_1x_2 = \frac{1}{2}[y+w] \qquad x_3x_4 = \frac{1}{2}[y+w] \tag{7}$$

Hier ist noch das Vorzeichen von $\sqrt{y-a}$ zu bestimmen. Nun ist

$$x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4 = -b$$

Multiplikation mit 2 und Umordnung ergibt

$$2x_1x_2(x_3 + x_4) + 2x_3x_4(x_1 + x_2) = -2b$$

Vermöge (2), (3) erhält man

$$(y+w)(x_3+x_4)+(y-w)(x_1+x_2) = -2b \Rightarrow$$
$$\Rightarrow \underbrace{y(x_1+x_2+x_3+x_4)}_{0} + w(x_3+x_4-x_1-x_2) = -2b$$

Mit (7) ergibt sich

$$w\left[\mp\sqrt{y-a} \mp \sqrt{y-a}\right] = \mp 2w\sqrt{y-a} = -2b \Rightarrow \underline{\pm w\sqrt{y-a} = 2b}$$

Da $w > 0$ ist, muß man $\sqrt{y-a}$ dasselbe Vorzeichen wie b erteilen

$$sgn\sqrt{y-a} = sgn\,b$$

Nach entsprechender Vorzeichenwahl sind dann nach (7) x_1, x_2 bzw. x_3, x_4 Nullstellen je einer quadratischen Gleichung und es gilt

$$x^4 + ax^2 + bx + c =$$
$$= \left[x^2 + x.\sqrt{y-a} + \frac{1}{2}(y+w)\right].\left[x^2 - x.\sqrt{y-a} + \frac{1}{2}(y-w)\right] \tag{8}$$
$$w = \sqrt{y^2-4c}, \qquad sgn\sqrt{y-a} = sgn\,b$$

Dieses Ergebnis entspricht der Zerlegung nach DESCARTES

$$x^4 + ax^2 + bx + c = (x^2 + px + q)(x^2 - px + r)$$

Umformung des 1.Faktors von (8) ergibt

$$x^2 + \frac{1}{2}y_1 + \sqrt{y-a}.\left(x + \frac{w}{2\sqrt{y-a}}\right)$$

Nun ist

$$\frac{w}{\sqrt{y-a}} = \frac{\sqrt{y^2-4c}}{\sqrt{y-a}} = \frac{\sqrt{(y^2-4c)(y-a)}}{y-a} = \frac{\sqrt{y^3-ay^3-4cy+4ac}}{y-a}$$

Da y eine Nullstelle der Resolvente

$$y^3 - ay^2 - 4cy + (4ac - b^2) = 0 \Rightarrow y^3 - ay^2 - 4cy + 4ac = b^2$$

ist gilt

$$\frac{w}{\sqrt{y-a}} = \frac{b}{y-a}$$

Daher erhält der 1.Faktor die Gestalt

$$x^2+\frac{1}{2}y_1+\sqrt{y-a}.\left(x+\frac{w}{2\sqrt{y-a}}\right)=\underline{\left(x^2+\frac{1}{2}y\right)+\sqrt{y-a}.\left(x+\frac{b}{2(y-a)}\right)}$$

Analog gilt für den 2.Faktor

$$\underline{\left(x^2+\frac{1}{2}y\right)-\sqrt{y-a}.\left(x+\frac{b}{2(y-a)}\right)}$$

Daher gilt

$$x^4+ax^2+bx+c=\underline{\left(x^2+\frac{1}{2}y\right)^2-(y-a).\left(x+\frac{b}{2(y-a)}\right)^2}$$

Das ist aber die Zerlegung nach FERRARI.

Sind $y_1 = y$, y_2, y_3 die Nullstellen der Resolvente, so folgt (zunächst ohne Rücksicht auf das Vorzeichen der Wurzeln) aus (7) und weiter zyklisch

$$x_1+x_2=\sqrt{y_1-a} \qquad x_3+x_4=-\sqrt{y_1-a}$$
$$x_1+x_3=\sqrt{y_2-a} \qquad x_2+x_4=-\sqrt{y_2-a}$$
$$x_1+x_4=\sqrt{y_3-a} \qquad x_2+x_3=-\sqrt{y_3-a}$$

Addition der 1.Kolonne ergibt

$$3x_1+x_2+x_3+x_4=2x_1+\underbrace{(x_1+x_2+x_3+x_4)}_{0}=\sqrt{y_1-a}+\sqrt{y_2-a}+\sqrt{y_3-a}$$

Daher

$$2x_1=\sqrt{y_1-a}+\sqrt{y_2-a}+\sqrt{y_3-a}$$
$$2x_2=\sqrt{y_1-a}-\sqrt{y_2-a}-\sqrt{y_3-a}$$
$$2x_3=-\sqrt{y_1-a}+\sqrt{y_2-a}-\sqrt{y_3-a}$$
$$2x_1=-\sqrt{y_1-a}-\sqrt{y_2-a}+\sqrt{y_3-a}$$

Die Vorzeichen der Wurzeln sind nicht unabhängig, denn es gilt

$$\sqrt{y_1-a}.\sqrt{y_2-a}.\sqrt{y_3-a}=(x_1+x_2)(x_1+x_3)(x_1+x_4)=\ldots=$$
$$=x_1^2\underbrace{(x_1+x_2+x_3+x_4)}_{0}+\underbrace{(x_1x_2x_3+x_1x_2x_4+x_1x_3x_4+x_2x_3x_4)}_{b}=-b$$

Die Vorzeichen sind also so zu wählen, daß gilt

$$\sqrt{y_1-a}.\sqrt{y_2-a}.\sqrt{y_3-a}=-b$$

Auf diese Weise gelangt man zu Methode von EULER

Zur Geschichte der algebraischen Gleichungen

Geometrische Methoden

Die rein kubischen Gleichungen wurden um 370 v.Chr. vom Erfinder der Kegelschnitte, dem Platoniker MENAICHMOS (um 350 v.Chr.) im Zusammenhang mit dem "Delischen Problem" gelöst.
Die allgemeinen kubischen Gleichungen soll nach dem Bericht von Omar ALKHAYYAMI (1044-1123/24) der Perser Abu Djafar gelöst haben. Die Griechen beherrschten die Auflösung gewisser spezieller Gleichungen bis zum 4.Grad auf geometrischem Wege unter Heranziehung von Kurven höherer Ordnung und unter Verwendung auch nicht-klassischer Zeicheninstrumente.
Die allgemeinen kubischen Gleichungen soll nach dem Bericht von Omar ALKHAYYAMI (1044-1123/24) der Perser Abu Djafar ALKHAZIN um 950 durch den Schnitt zweier Kegelschnitte gelöst haben.
Unser Interesse gilt jedoch der algebraischen Auflösung der Gleichungen.

Algebraische Methoden

Das Wort Algebra stammt von dem arabischen Wort al-djebr. Die Araber gebrauchten die beiden, wahrscheinlich aus dem Indischen stammenden, Worte aldjebr w'almokabala immer nur im Zusammenhang mit der von dem persischen Mathematiker Beha EDDIN (1547-1622) beschriebenen Vorgangsweise: "Die Seite, welche mit einer negativen Größe behaftet ist, wird ergänzt und etwas dieser negativen Größe Gleiches auf der anderen Seite addiert; das ist al-djebr. Die homogenen und gleichen Glieder werden weggestrichen und das ist almokabala.

Lineare Gleichungen

Die linearen Gleichungen wurden von den Arabern durch Anwendung der "regula falsi" gelöst, die jetzt nur mehr bei Gleichungen höheren Grades angewendet wird. Die schematische Behandlung der regula falsi wurde auch "Methode der Waagschalen" benannt.
Als hervorragende Mathematiker der arabischen Schule sind ABRAHAM ben ESRA (1130), Ibn ALBANNA (1222), ALKALZADI(+1486) und Beha EDDIN (1547-1622) zu nennen.

Quadratische Gleichungen

Es ist nicht ganz geklärt, ob die algebraische Lösung der vollständigen quadratischen Gleichung 2.Grades eine Leistung der Inder oder der griechisch-alexandrinischen Schule ist (DIOPHANT um 250 n.Chr). Eine den heutigen Anforderungen der elementaren Algebra entsprechende Methode findet sich bei dem indischen Astronomen BRAHMAGUPTA (um 630). Die Theorie dieser Methode wird auf den Mathematiker und Astronomen ARIABATTHIYA (geb.476) zurückgeführt. Das älteste arabische Werk über Algebra soll um 830 von MOHAMMED ben MUSA nach indischen Vorlagen verfaßt worden sein.
Obwohl die Inder auf dem Gebiet der Geometrie den Griechen weit unterlegen waren, übertrafen sie doch die letzteren auf dem Gebiet der Arithmethik und Algebra, da sie ein viel leistungsfähigeres Zahlensystem zur Verfügung hatten.

Kubische Gleichungen

Die algebraische Auflösung der reduzierten kubischen Gleichung wurde um 1500 (wahrscheinlich durch Probieren) zuerst von Scipione dal FERRO (ca.1465-1525), von 1496-1525 Professor der Mathematik in Bologna, entdeckt. FERRO veröffentlichte seine Formel nicht, sondern teilte sie unter dem Siegel der Verschwiegenheit einigen Freunden und Schülern mit, darunter dem Rechenmeister Antonio Maria FIOR und seinem Schwiegersohn Annibale della NAVE (1500?-1577). FIOR forderte den Mathematiker Nicolo FONTANO (1500-1557), der unter dem Namen TARTAGLIA (Stotterer) bekannt wurde, im Jahre 1535 zu einem öffentlichen Wettstreit in der Mathematik auf, in dessen Verlauf er TARTAGLIA 30 kubische Gleichungen zu Auflösung vorlegte. TARTAGLIA wurde Sieger und es gelang ihm, im Laufe des Streites selbständig die Formel des Gegners herauszufinden. TARTAGLIA teilte seine Formel 1539 unter eidlicher Verschwiegenheit Geronimo CARDANO (1501-1576) mit.
1542 stellte CARDANO bei einem Besuch, den er zusammen mit seinem Schüler Ludovico FERRARI (1522-1565) bei NAVE machte, fest, daß die Lösung von TARTAGLIA mit jener FERROs übereinstimmte. Er war daher der Meinung, daß TARTAGLIA auf unredlichem Weg in den Besitz dieser Formel gelangt sei, fühlte sich TARTAGLIA gegenüber nicht mehr an sein Schweigeversprechen gebunden und veröffentlichte diese Formel in seinem Werk „Ars magna“ (1545). Daher heißt diese Formel eigentlich zu Unrecht "CARDANIsche Formel". Der empörte Einspruch TARTAGLIAs führte zu äußerst heftigen öffentlichen Streitereien, an denen sich aber CARDANO nicht beteiligte.

Biquadratische Gleichungen

Die erste Methode zur Auflösung der allgemeinen Gleichung 4.Grades stammt von Ludovico FERRARI (1545). Andere Methoden stammen von René DESCARTES (1596-1650), Leonhard EULER (17071783) und vielen anderen.

Zusammenfassung

Alle Methoden zur Lösung der Gleichungen bis zum 4.Grad beruhen darauf, Ausdrücke aus den Nullstellen der Gleichungen zu bilden, die bei Permutation der Nullstellen ineinander übergehen und deren Berechnung sich auf eine Gleichung geringeren Grades als die gegebene zurückführen läßt. Daher lassen sich die Nullstellen der Gleichungen bis zum 4.Grad durch Wurzelschachtelungen darstellen.
Niels Henrik ABEL (1802-1829) und Evariste GALOIS (1811-1832) wiesen nach, daß dies für Gleichungen ab dem 5.Grad nicht mehr möglich ist. Der entscheidende Satz von GALOIS lautet: "Damit eine irreduzible Gleichung von Primzahlgrad durch Wurzelschachtelungen lösbar sei, ist notwendig und hinreichend, daß sich aus zwei beliebigen bekannten Nullstellen die restlichen rational darstellen lassen".

Literatur

MATTHIESSEN Ludwig: Grundzüge der antiken und modernen Algebra der litteralen Gleichungen. Leipzig, Teubner, 2.Aufl.1896, 1001 S.

HOFMANN Josef Ehrenfried: Geschichte der Mathematik. Erster Teil. Von den Anfängen bis zum Auftreten von Fermat und Descartes. Berlin, W.de Gruyter, Berlin 1953. (Sammlung Göschen Bd.226)

KOWALEWSKI Gerhard: Große Mathematiker. Eine Wanderung durch die Geschichte der Mathematik vom Altertum bis zur Neuzeit. J.F.Lehmanns Verlag, München/Berlin,2.Aufl. 1939

Die Transzendenz von ê und π

Algebraische und transzendente Zahlen

Ein Problem ist mit Zirkel und Lineal nur dann lösbar, wenn seine Behandlung auf eine algebraische Gleichung ganz bestimmter Bauart führt. Liegt diese Bauart nicht vor, so ist das Problem auf klassischem Wege nicht lösbar und man muß nichtklassische Hilfsmittel heranziehen, etwa Kegelschnitte oder algebraische Kurven höheren Grades.

A fortiori ist ein Problem mit Zirkel und Lineal nicht lösbar, wenn es gar keine algebraischen Kurven gibt, mit deren Verwendung man das Problem lösen könnten.

Zunächst werden wir jene reellen Zahlen ermitteln, welch überhaupt als Nullstellen algebraischer Gleichung auftreten können.

Eine reelle Zahl heißt *algebraische Zahl* (Bezeichnung von KRONECKER), wenn sie Nullstelle einer *algebraischen Gleichung* ist

$$a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n = 0$$
$$a_i \in \mathbb{Z},\ ggT(a_0, \ldots, a_n) = 1$$

Die Nullstellen können *reell* oder *komplex* sein. Uns interessieren in erster Linie die reellen Nullstellen. Später müssen wir aber auch komplexe Zahlen betrachten.

Ist eine Zahl nicht Nullstelle einer algebraischen Gleichung, so heißt sie *transzendent*.

Zunächst erkennt man, daß alle ganzen und rationalen Zahlen algebraisch sind, da sie den Gleichungen

$$x + a = 0,\ ax + b = 0,\quad a,b \in \mathbb{Z}$$

genügen. Ebenso sind alle Wurzeln aus rationalen Zahlen algebraisch:

$$ax^n + b = 0$$

Die Menge der algebraischen Zahlen ist abzählbar

Beweis 1873 von Georg CANTOR (1845-1918) in der Fassung von Felix KLEIN (1849-1925) 1895

Wir betrachten die ganzen Zahlen

$$N := n - 1 + |a_0| + |a_1| + \ldots + |a_n|$$

Einer gegebenen natürlichen Zahl N entspricht dann eine endliche Anzahl $\Phi(N)$ von algebraischen Gleichungen, da N nur auf endlich viele Arten als Summe von positiven ganzen Zahlen dargestellt werden kann. Wir können demnach folgende Tabelle anlegen (siehe Seite 82)

Die Ordnung erfolgt nach wachsendem N und nach wachsenden Werten der algebraischen Zahlen unter Weglassung der bereits früher aufgetretenen Zahlen. Keine dieser Zahlen enthält eine unendliche Folge von Neunen, da sich 0,099... = 0,1 stets als exakte Dezimale schreiben läßt. Da in obiger Liste jede algebraische Zahl an wohldefinierter Stelle steht, kann man sie durchnumerieren. Die Menge der algebraischen Zahlen ist daher abzählbar.

In jedem noch so kleinen Abschnitt der Zahlengeraden gibt es unendlich viele Punkte, die keine algebraische Abszisse haben

$N := n - 1 + |a_0| + |a_1| + \ldots + |a_n| \quad ggT(a_0, \ldots, a_n) = 1$

N	n	$\|a_0\|$	$\|a_1\|$	$\|a_2\|$	$\|a_3\|$	$\|a_4\|$	Gleichung	Φ(N)	Nullstellen
1	1	1					$x = 0$	1	0
2	1	2	0				$(2x = 0)$	2	-1
		1	1				$x \pm 1 = 0$		+1
	2	1	0	0			$(x^2 = 0)$		
3	1	3	0				$(3x = 0)$	4	-2
		2	1				$2x \pm 1 = 0$		-0,5
		1	2				$x \pm 2 = 0$		+0,5
	2	2	0	0			$(2x^2 = 0)$		+2
		1	1	0			$(x^2 + x = 0)$		
		1	0	1			$(x \pm 1 = 0)$		
	3	1	0	0	0		$(x^3 = 0)$		
4	1	4	0				$(4x = 0)$	12	-3
		3	1				$3x \pm 1 = 0$		-1,61803...
		2	2				$(2x \pm 2 = 0)$		-1,41421...
		1	3				$x \pm 3 = 0$		-0,70711...
	2	3	0	0			$(3x^2 = 0)$		-0,61803...
		2	1	0			$(2x^2 \pm x = 0)$		-0,33333...
		2	0	1			$2x^2 - 1 = 0$		+0,33333...
		1	2	0			$x^2 \pm 2x = 0$		+0,61803...
		1	1	1			$x^2 \pm x - 1 = 0$		+0,70711...
		1	0	2			$x^2 - 2 = 0$		+1,41421...
	3	2	0	0	0		$(2x^3 = 0)$		+1,61803...
		1	1	0	0		$(x^3 \pm x^2 = 0)$		+3
		1	0	1	0		$(x^3 \pm x = 0)$		
		1	0	0	1		$(x^3 \pm 1 = 0)$		
	4	1	0	0	0	0	$(x^4 = 0)$		
...	...	...	...	...	...	...	...	...	...

Das gegebene Intervall sei durch die ersten n Dezimalstellen festgelegt:

$$n,d_1d_2 \ldots d_s$$

$$n,d_1d_2 \ldots (d_s + 1)$$

Dann wählen wir als

(s+1)-te Dezimalstelle eine Zahl ≠ 9 und ungleich der (s+1)-ten Dezimalstelle der 1.algebraischen Zahl

(s+2)-te Dezimalstelle eine Zahl ≠ 9 und ungleich der (s+2)-ten Dezimalstelle der 2.algebraischen Zahl

.....

Auf diese Weise konstruieren wir einen Dezimalbruch, der sicher nicht in lauter Neunen ausläuft und sicher nicht in obiger Tabelle enthalten ist.

Es gibt daher mehr transzendente Zahlen als algebraische Zahlen, da man zur Besetzung jeder Dezimalstelle unter den Ziffern 0,1, ... ,8 auswählen kann, ohne daß eine algebraische Zahl entsteht.

Der Körper der algebraischen Zahlen

> Jede Nullstelle eines Polynoms mit *algebraischen Koeffizienten* ist auch Nullstelle eines Polynoms mit *rationalen Koeffizienten* , d.h. sie ist selbst wieder eine algebraische Zahl

Es sei w eine Nullstelle des Polynoms

$$\rho x^n + \alpha x^{n-1} + \beta x^{n-2} + \ \dots \ + \gamma = 0$$

dessen Koeffizienten $\alpha, \beta, \dots, \gamma, \rho$ algebraische Zahlen sind, dh. Nullstellen der Polynome

$$\left.\begin{array}{l} \alpha \dots x^a + A_1 x^{a-1} + \dots + A_a = 0 \\ \beta \dots x^b + B_1 x^{b-1} + \dots + B_b = 0 \\ \vdots \\ \gamma \dots x^c + C_1 x^{c-1} + \dots + C_c = 0 \\ \rho \dots x^r + R_1 x^{r-1} + \dots + R_r = 0 \end{array}\right\} A_i, B_j, \dots, C_k, R_l \in \mathbb{Q}$$

Wir definieren nun reelle Zahlen der Form

$$w_i := w^{n'} \rho^{r'+1} \alpha^{a'} \beta^{b'} \dots \gamma^{c'} \quad \begin{cases} n' = 0,1, \ \dots \ , n-1 \\ a' = 0,1, \ \dots \ , a-1 \\ b' = 0,1, \ \dots \ , b-1 \\ \vdots \\ c' = 0,1, \ \dots \ , c-1 \\ r' = 0,1, \ \dots \ , r-1 \end{cases}$$

Es gibt also

$$m := n.a..b...c.r$$

Größen $w_{i'}$. Wir behaupten

> Die m Produkte
> $$ww_i \quad (i = 1, \dots, m)$$
> lassen sich in der Gestalt
> $$ww_i = k_{i1}w_1 + k_{i2}w_2 + \dots + k_{im}w_m$$
> mit rationalen k_{ij} darstellen

BW: Wir setzen

$$ww_i := w^{n'+1} \rho^{r'+1} \alpha^{a'} \beta^{b'} \dots \gamma^{c'}$$

1.Fall: $n' < n - 1 \Rightarrow n' + 1 < n$

a) $r' < r - 1 \Rightarrow r' + 1 < r$

In diese Falle ist ww_i gleich einem w_k mit geeignetem k , also eine rationale Linearkombination der w_i

$$ww_i = w_k$$

b) $r' = r - 1 \Rightarrow r' + 1 = r$

Der Definition von ρ entsprechend gilt

$$\rho^r = -R_1\rho^{r-1} - \dots - R_r$$

daher

$$ww_i = w^{n'+1}\left(-R_1\rho^{r-1} - \ldots - R_r\right)\alpha^{a'}\beta^{b'}\ldots\gamma^{c'} =$$
$$= -R_1\underbrace{w^{n'+1}\rho^{r-1}\alpha^{a'}\beta^{b'}\ldots\gamma^{c'}}_{w_j} - \ldots - R_r\underbrace{w^{n'+1}\alpha^{a'}\beta^{b'}\ldots\gamma^{c'}}_{w_k}$$

d.h. ww_i ist eine rationale Linearkombination mit den rationalen Koeffizienten R_i

2.Fall: $n' = n - 1 \Rightarrow n' + 1 = n$

Der Definition von w entsprechend gilt

$$\rho w^n = -\alpha w^{n-1} - \ldots - \gamma$$

daher

$$ww_i = \left(\rho w^n\right)\rho^{r'}\alpha^{a'}\beta^{b'}\ldots\gamma^{c'} = \left(-\alpha w^{n-1} - \ldots - \gamma\right)\rho^{r'}\alpha^{a'}\beta^{b'}\ldots\gamma^{c'} =$$
$$= -w^{n-1}\rho^{r'}\alpha^{a'+1}\beta^{b'}\ldots\gamma^{c'} - \ldots - \rho^{r'}\alpha^{a'}\beta^{b'}\ldots\gamma^{c'+1}$$

Wir betrachten den ersten Summanden des obigen Ausdrucks

a) $a' < a - 1 \Rightarrow a' + 1 < a$
dann ist, bei geeigneter Wahl von k, der erste Summand identisch mit einem w_k, daher ist der erste Summand eine rationale Linearkombination der w_i.

b) $a' = a - 1 \Rightarrow a' + 1 = a$
Entsprechend der Definition

$$\alpha^a = -A_1\alpha^{a-1} - \ldots - A_a$$

erhält der erste Summand die Gestalt

$$-w^{n-1}\rho^{r'}\left(-A_1\alpha^{a-1} - \ldots - A_a\right)\beta^{b'}\ldots\gamma^{c'} =$$
$$= A_1\underbrace{w^{n-1}\rho^{r'}\alpha^{a-1}\beta^{b'}\ldots\gamma^{c'}}_{w_j} + \ldots + A_a\underbrace{w^{w-1}\rho^{r'}\beta^{b'}\ldots\gamma^{c'}}_{w_k}$$

Es gilt daher

$$ww_i = k_{i1}w_1 + k_{i2}w_2 + \ldots + k_{im}w_m \qquad (i = 1,\ldots,m)$$

das kann man auch in der Gestalt schreiben

$$\begin{aligned}
(k_{11} - w)w_i + k_{12}w_2 + \ldots\ldots + k_{1m}w_m &= 0\\
k_{21}w_1 + (k_{22} - w)w_2 + \ldots\ldots + k_{2m}w_m &= 0\\
\vdots \qquad\quad \vdots \qquad\qquad\qquad \vdots \qquad\quad \vdots &\\
k_{m1}w_i + k_{m2}w_2 + \ldots\ldots + (k_{mm} - w)w_m &= 0
\end{aligned}$$

Es liegt also ein aus m Gleichungen bestehendes System fü die m unbekannten Größen w_i vor. Da nicht alle w_i verschwinden, muß die Determinante des Systems verschwinden, d.h. es muß gelten

$$\begin{vmatrix} k_{11} - w & k_{12} & \cdots & k_{1m} \\ k_{21} & k_{22} - w & \cdots & k_{2m} \\ \vdots & \vdots & & \vdots \\ k_{m1} & k_{m1} & \cdots & k_{mm} - w \end{vmatrix} = 0$$

Da die k_{ij} rational sind, genügt w also einer Gleichung m-ten Grades mit rationalen Koeffizienten .

Sind α und β algebraische Zahlen, so hat die Gleichung

$$\beta x - \alpha = 0$$

wie soeben bewiesen, die algebraische Zahl

$$x = \frac{\alpha}{\beta} \qquad (*)$$

als Nullstelle. Ist jedoch w algebraisch, so sind auch die Größen $-w$, $\frac{1}{w}$, $w+1$, $w-1$ algebraisch. Man hat bloß in der w definierenden algebraischen Gleichung an Stelle der Variablen x die neue Variable $x = -y$, $\frac{1}{y}$, $y-1$, $y+1$ zu substituieren. Ist daher β algebraisch, so ist auch $\frac{1}{\beta}$ algebraisch, daher wegen (*) auch

$$\alpha : \frac{1}{\beta} = \alpha\beta$$

algebraisch. Da mit $\frac{\alpha}{\beta}$ auch $\frac{\alpha}{\beta} \pm 1$ algebraisch sind, folgt auch daß

$$\left(\frac{\alpha}{\beta} \pm\right)\beta = \alpha \pm \beta$$

algebraisch sind.

Die Menge der algebraischen Zahlen bildet daher einen Zahlkörper.

Obige Sätze und ihre Beweise stammen von Richard DEDEKIND (1831-1916) 1894

Die Transzendenz von ê

Im Folgenden wird bewiesen, daß die Zahl ê nicht Nullstelle eines Polynoms mit rationalen Koeffizienten sein kann.

Der erste Beweis stammt von

Charles HERMITE 1873 (1822-1901)

Verbesserte Methoden von

Karl WEIERSTRASS 1885 (1815-1897)

David HILBERT 1893 (1862-1943)

Integralfreie Beweise stammen von

Adolf HURWITZ 1893 (1859-1919)

Paul GORDAN 1893 (1837-1912)

Der folgende Beweis geht im Wesentlichen auf GORDAN zurück.

Die Reihe für

$$\hat{e}^x = 1 + \frac{x}{1!} + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots$$

konvergiert für jedes x

$$(\forall x \in \mathbb{R}) \lim_{i \to \infty} \frac{x^i}{i!} = 0$$

Allgemeiner gilt

$$(\forall x \in \mathbb{C}) \lim_{i \to \infty} \frac{|x|^i}{i!} = 0$$

Wir zeigen

Die Zahl

$$\hat{e} = 1 + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \cdots$$

kann keine Beziehung der Gestalt

$$F(\hat{e}) = C_n\hat{e}^n + C_{n-1}\hat{e}^{n-1} + \ldots + C_1\hat{e} + C_0 = 0, \qquad C_i \in \mathbb{Z}$$

erfüllen, d.h. ê kann nicht Nullstelle einer algebraischen Gleichung $F(x) = 0$ sein, d.h. ê ist *transzendent*.

Beweis der Transzendenz von ê

Überblick über den Gang des Beweises

1. Wir nehmen an, es gäbe eine algebraische Gleichung, für die gilt

$$F(\hat{e}) = C_0 + C_1\hat{e} + C_2\hat{e}^2 + \ldots + C_{n-1}\hat{e}^{n-1} + C_n\hat{e}^n = 0 \qquad C_i \in \mathbb{Z}$$

2. Wir multiplizieren $F(\hat{e}) = 0$ mit einer geeignet gewählten ganzen Zahl $M \neq 0$

$$MF(\hat{e}) = MC_0 + MC_1\hat{e} + MC_2\hat{e}^2 + \ldots + MC_{n-1}\hat{e}^{n-1} + MC_n\hat{e}^n = 0, \qquad C_i \in \mathbb{Z}$$

3. Wir zerlegen jedes der Produkte $M\hat{e}^k$ $(k = 0,1, \ldots, n)$ in einen ganzzahligen M_k und einen echten Dezimalbruch $\varepsilon_k < 1$. Dann gilt

$$M\hat{e}^k = M_k + \varepsilon_k$$

daher weiter

$$MF(\hat{e}) = MC_0 + M_1C_1 + \ldots + M_nC_n + C_1\varepsilon_1 + \ldots + C_n\varepsilon_n = 0$$

4. Wir zeigen: Der ganzzahlige Teil

$$MC_0 + M_1C_1 + \ldots + M_nC_n \neq 0$$

verschwindet nicht.

5. Der Rest

$$C_1\varepsilon_1 + C_2\varepsilon_2 + \ldots + C_n\varepsilon_n$$

kann beliebig klein gemacht werden

Nach Durchführung dieser Schritte kann man die Unmöglichkeit von 1. beweisen, da die Summe einer nicht verschwindenden ganzen Zahl 4. und eines echten Bruches 5. nie Null sein kann.

Hilfsmittel zur Durchführung des Beweises

a) Wir führen folgende symbolische Schreibweise ein

$h^r := r!$ gilt nur für den Buchstaben h!

Dann können wir schreiben

$$\hat{e}^x = 1 + \frac{x}{h} + \frac{x^2}{h^2} + \frac{x^3}{h^3} + \cdots$$

Für ein Polynom

$$f(x) = \sum_{i=1}^{n} c_i x^i$$

würde gelten

$$f(h) = \sum_{i=1}^{n} c_i h^i = c_1 . 1! + c_2 . 2! + c_3 . 3! + \ldots + c_n . n!$$

Für eine beliebige ganze Zahl $k \in \mathbb{Z}$ ergibt sich, wenn man die auftretenden Potenzen formal nach dem binomischen Lehrsatz entwickelt

$$f(k+h) = \sum_{i=1}^{n} c_i (k+h)^i = \sum_{i=1}^{n} q_i . h^i = \sum q_i . i!$$

worin die $q_i = q_i(c_j,k)$ Polynome in k sind

b) Wir definieren ein Polynom

$$\Phi(x) := x^{p-1} \cdot \frac{[(1-x)(2-x)(3-x)\cdots(n-x)]^p}{(p-1)\ !}$$

Hierin bedeuten.

p ... beliebige (sehr große) Primzahl

n ... Grad der algebraischen Gleichung, der ê mutmaßlich genügt

Es ist

$grd\ \Phi(x) =: N = np + p - 1 = p(n+1) - 1$

n = 2m gerade ⇒ N = p(2m - 1) + 1 =2mp + (p - 1) ⇒ N gerade

n = 2m - 1 ungerade ⇒ N = p(2m - 1 + 1) - 1 = 2mp - 1 ⇒ N ungerade

Die Primzahl p werde so gewählt, daß gilt

$p > n > 0, \quad p > |C_0|$

Eigenschaften der Funktion Φ(x)

α) Für beliebiges, festgehaltenes x gilt

$$\lim_{p\to\infty} \Phi(x) = 0$$

Setzt man nämlich y := x(1 - x)(2 - x)...(n - x) so gilt

$$\Phi(x) = \frac{y^{p-1}}{(p-1)!} \cdot \frac{y}{x}$$

Da $\frac{y}{x}$ konstant ist und $\lim_{p\to\infty} \frac{y^{p-1}}{(p-1)!} = 0$, gilt die Behauptung

β) Φ(h) ist eine ganze Zahl, die nicht durch p teilbar ist, daher ist

$$0 \neq \Phi(h) \in Z$$

Zum Nachweis entwickeln wir Φ(x) nach Potenzen von x

$$\Phi(x) = \sum_{i=p-1}^{N} \frac{c_i x^i}{(p-1)!}$$

Man erkennt unmittelbar für die Randkoeffizienten

$c_{p-1} = (n!)^p$, $c_N = (-1)^p$, c_{p-1}, c_N ganze Zahlen

Daher

$$\Phi(x) = \frac{(n!)^p}{(p-1)!} \cdot x^{p-1} + \frac{c_p}{(p-1)!} \cdot x^p + \ \ldots\ + \frac{(-1)^p}{(p-1)!} x^N$$

Setzt man

x = h, so bedeutet $x^i = h^i = i!$

Dann ergibt sich

$$\Phi(h) = \frac{(n!)^p}{(p-1)!} \cdot (p-1)! - \frac{c_p}{(p-1)!} \cdot p! + \ \ldots (-1)^p \frac{1}{(p-1)!} \cdot N! = (n!)^p + p\left[-c_p + \cdots\cdots\right]$$

Der 2.Summand ist durch p teilbar. Da jedoch p > n gewählt wurde, ist (n!) , daher auch $(n!)^p$ nicht durch p teilbar. Demnach ist auch Φ(h) nicht durch p teilbar. Daraus folgt, daß die ganze (sehr große) Zahl Φ(h) ≠ 0 sein muß.

γ) $\Phi(k+h)$ ist eine ganze, durch p teilbare Zahl, wenn $k \in \{1,2,\ldots,n\}$ ist. Es gilt nämlich

$$\Phi(k+h) = (k+h)^{p-1} \cdot \frac{[(1-k-h)(2-h-k)\ldots(-h)\ldots(n-k-h)]^p}{(p-1)!}$$

Entwicklung dieses Ausdrucks nach Potenzen von h ergibt

$$\Phi(k+h) = \sum_{i=p}^{N} \frac{q_i h^i}{(p-1)!} = \sum_{i=p}^{N} \frac{q_i i!}{(p-1)!}$$

worin die $q_i(k)$ Polynome in k sind. Da $i \geq p$ ist, kann man aus jedem Summanden p herausheben, während sich die Nenner $(p-1)!$ wegkürzen. Die q_i haben natürlich ganzzahlige Werte

Beweis für die Transzendenz von ê

1. Es gelte die Annahme
   $F(\hat{e}) = C_0 + C_1\hat{e} + C_2\hat{e}^2 + \ldots + C_{n-1}\hat{e}^{n-1} + C_n\hat{e}^n = 0 \qquad C_i \in \mathbb{Z}$
2. Wir multiplizieren $F(\hat{e})$ mit der ganzen Zahl
   $$M = \Phi(h)$$
   Dann gilt
   $$\Phi(h)F(\hat{e}) = \Phi(h)C_0 + \Phi(h)C_1\hat{e} + \Phi(h)C_2\hat{e}^2 + \ldots + \Phi(h)\,C_n\hat{e}^n = \sum_{k=0}^{n} C_k.\Phi(h).\hat{e}^k$$
   Von dieser Summe untersuchen wir den Summanden
   $$\hat{e}^k\Phi(h) = \hat{e}^k.\sum_{i=p-1}^{N} \frac{c_i h^i}{(p-1)!} = \sum_{i=p-1}^{N} \frac{c_i \hat{e}^k h^i}{(p-1)!}$$
   Aus dieser Summe untersuchen wir den Summanden
   $$\hat{e}^k.h^i = \left(1 + \frac{k}{1!} + \frac{k^2}{2!} + \frac{k^3}{3!} + \ldots + \frac{k^i}{i!} + \frac{k^{i+1}}{(i+1)!} + \ldots\right).h^i =$$
   $$= h^i + \frac{h^i.k}{1!} + \frac{h^i.k^2}{2!} + \frac{h^i.k^3}{3!} + \ldots + \frac{h^i.k^i}{i!} + \left[\frac{h^i.k^{i+1}}{(i+1)!} + \ldots\right]$$
   Nun ist aber
   $$h^i = i! = i(i-1)! = i(i-1)(i-2)! = \cdots = i(i-1)\ldots3.2! = i(i-1)\ldots2.1!$$
   also
   $$h^i = ih^{i-1} = i(i-1)h^{i-2} = \cdots = i(i-1)\ldots3.h^2 = i(i-1)\ldots2.h = i!$$
   Daher
   $$\hat{e}^k.h^i = h^i + \frac{i}{1!}.h^{i-1}.k + \frac{i(i-1)}{2!}h^{i-2}.k^2 + \ldots + \frac{i!}{i!}.k^i +$$
   $$+k^i\left[0 + \frac{k}{i+1} + \frac{k^2}{(i+1)(i+2)} + \ldots\right]$$

$$\underline{\hat{e}^k.h^i} = h^i + \frac{i}{1!}.h^{i-1}.k + \frac{i(i-1)}{2!}h^{i-2}.k^2 + \ldots + \frac{i!}{i!}.k^i + k^i\left[0 + \frac{k}{i+1} + \frac{k^2}{(i+1)(i+2)} + \ldots\right] =$$

$$= h^i + \binom{i}{1}h^{i-1}.k + \binom{i}{2}h^{i-1}.k^2 + \ldots + \binom{i}{i}k^i + k^i\left[0 + \frac{k}{i+1} + \frac{k^2}{(i+1)(i+2)} + \ldots\right] =$$

$$= \underline{(h+k)^i + k^i\left[0 + \frac{k}{i+1} + \frac{k^2}{(i+1)(i+2)} + \ldots\right]}$$

Der Vergleich der Reihe

$$0 + \frac{k}{i+1} + \frac{k^2}{(i+1)(i+2)} + \ldots$$

mit der Reihe

$$\hat{e}^k = 1 + \frac{k}{1!} + \frac{k^2}{2!} + \cdots$$

lehrt, daß jeder Summand der oberen Reihe kleiner ist als jeder Summand der unteren Reihe. Man kann daher setzen

$$0 + \frac{k}{i+1} + \frac{k^2}{(i+1)(i+2)} + \ldots = q_{i,k}\hat{e}^k \qquad 0 < q_{i,k} < 1$$

daher

$$\hat{e}^k.h^i = (h+i)^i + q_{i,k}\hat{e}.k^i$$

3. Es gilt also

$$\hat{e}^k.\Phi(h) = \sum_{i=p-1}^{N}\frac{c_i\hat{e}^k h^i}{(p-1)!} = \sum_{i=p-1}^{N}\frac{c_i}{(p-1)!}\left[(h+k)^i + q_{i,k}\hat{e}^k.k^i\right] =$$

$$= \sum_{i=p-1}^{N}\frac{c_i}{(p-1)!}(h+k)^i + \hat{e}^k\sum_{i=p-1}^{N}q_{i,k}\frac{c_i}{(p-1)!}k^i$$

Für die erste Summe gilt

$$\sum_{i=p-1}^{N}\frac{c_i}{(p-1)!}(h+k)^i = \Phi(h+k) \quad \ldots \text{ ganze, sehr große Zahl}$$

Aus der Eigenschaft α) von Φ(x) folgt (Seite 87)

$$\lim_{p\to\infty}\sum\frac{c_i}{(p-1)!}(h+k)^i = \lim_{p\to\infty}\Phi(h+k) = 0$$

Umsomehr gilt für die zweite Summe wegen $q_{i,k} < 1$

$$\lim_{p\to\infty}\sum q_{i,k}\frac{c_i}{(p-1)!}k^i = 0$$

Da auch $\hat{e}^k$ eine endliche Größe ist, können wir

$$\varepsilon_k := \hat{e}^k\sum q_{i,k}\frac{c_i}{(p-1)!}k^i$$

durch Wahl einer entsprechend großen Primzahl p bliebig klein machen
Daher wird der Ausdruck

$$C_k\hat{e}^k\,\Phi(h) = C_k\,\Phi(h+k) + C_k\,\varepsilon_k$$

bei entsprechen großer Wahl von p sich immer mehr der ganzen Zahl $C_k\Phi(k)$ nähern, da $C_k\varepsilon_k$ beliebig klein wird.

4. Es gilt daher schließlich

$$F(\hat{e})\Phi(h) = C_0\Phi(h) + C_1\Phi(h+1) + C_2\Phi(h+2) + \ldots + C_n\Phi(h+n) + \\ + C_1\varepsilon_1 + C_2\varepsilon_2 + \ldots + C_n\varepsilon_n$$

Alle Summanden der ersten Zeile sind ganze Zahlen, die, mit Ausnahme von $C_0\Phi(h)$, alle durch p teilbar sind. $C_0\Phi(h)$ ist nicht durch p teilbar, da $p > C_0$ gewählt wurde und $\Phi(h)$ nicht durch p teilbar ist. Die erste Zeile stellt also eine ganze, nicht durch p teilbare Zahl dar, die nicht verschwinden kann

5 Da die Summe in der zweiten Zeile beliebig klein gemacht werden kann, kann der Ausdruck $F(\hat{e})\Phi(h)$ wegen $\Phi(h) \neq 0$ nicht verschwinden. Daher gilt $F(\hat{e}) \neq 0$. ê ist daher transzendent

Die Transzendenz von π

Den ersten Beweis erbrachte Ferdinand LINDEMANN (1852-1939) 1882. Beim folgenden Beweis ist es erforderlich, auch komplexe Nullstellen eine Polynoms zu berücksichtigen. Seien $x_1, \ldots, x_n$ die Nullstellen einer normierten Polynoms über $\mathbb{Q}$. Dann gilt

$$f(x) = (x-x_1)(x-x_2)\ldots(x-x_n) = x^n + \alpha_1 x^{n-1} + \alpha_2 x^{n-2} + \ldots + \alpha_n \qquad \alpha_i \in \mathbb{Q}$$

Die Größen

$$\begin{aligned} \alpha_1 &= -(x_1 + x_2 + \ldots + x_n) \\ \alpha_1 &= (x_1x_2 + x_1x_3 + \ldots + x_{n-1}x_n) \\ &\vdots \\ \alpha_n &= (-1)^n x_1x_2\cdots x_n \end{aligned}$$

sind die elementarsymmetrischen Funktionen der (nicht notwendig reellen) *assoziierten algebraischen Zahlen* x_i.

Betrachtet man algebraische Gleichungen mit ganzzahligen Koeffizienten, gilt also

$$f(x) = ax^n + a_1x^{n-1} + a_2x^{n-2} + \ldots + a_n \qquad a, a_i \in \mathbb{Z}$$

so stellen die Koeffizienten a_i, wenn $a \neq 1$ ist, nicht mehr die elemenarsymmetrischen Funktionen assoziierter algebraischer Zahlen dar. Setzt man jedoch

$$y := ax$$

Dann erhält man die neue Gleichung

$$y^n + a_1y^{n-1} + aa_2y^{n-2} + \ldots + a^{n-2}a_{n-1}y + a^{n-1}a_n$$

Die elementarsymmetrischen Funktionen dieser assoziierten algebraischen Zahlen sind ganzzahlig, wobei gilt

$$y_i = ax_i$$

HERMITE hat gezeigt, daß ê keiner Beziehung der Gestalt

$$F(\hat{e}) = C_0 + C_1\hat{e} + C_2\hat{e}^2 + \ldots + C_{n-1}\hat{e}^{n-1} + C_n\hat{e}^n = 0$$

mit ganzzahligen Koeffizienten genügen kann. LINDEMANN hat darüber hinaus folgendes gezeigt

Die Zahl ê kann keiner Beziehung der Gestalt $C_0 + C_1(\hat{e}^{k_1} + \hat{e}^{k_2} + \ldots + \hat{e}^{k_N}) + C_2(\hat{e}^{l_1} + \hat{e}^{l_2} + \ldots + \hat{e}^{l_{N'}}) + \ldots = 0$ genügen. Hierin sind die C_i ganze Zahlen und die k_i, l_j assoziierte algebraische Zahlen, die auch komplex sein können

Sind die k_i, l_j, ... Nullstellen der Gleichungen

$$k_i \;\ldots\; ax^N + a_1x^{N-1} + \ldots + a_N = \qquad a, a_i \in \mathbb{Z}$$
$$l_j \;\ldots\; bx^{N'} + b_1x^{N'-1} + \ldots + b_{N'} = 0 \qquad b, b_j \in \mathbb{Z}$$

. . . .

so sind die elementarsymmetrischen Funktionen i.a, keine ganzen Zahlen. Betrachten wir aber die elemtarsymmetrischen Funktionen der Größen

$$ak_i,\; bl_j$$

so sind deren elementarsymmetrische Funktionen ganzzahlig.

Der Beweis von LINDEMANN ist dem von HERMITE weitgehend nachgebildet. Der Beweis erfolgt wieder indirekt

Überblick über den Beweisgang von LINDEMANN

1. Wir nehmen an, es gäbe eine Beziehung
$$C_0 + C_1(\hat{e}^{k_1} + \hat{e}^{k_2} + \ldots + \hat{e}^{k_N}) + C_2(\hat{e}^{l_1} + \hat{e}^{l_2} + \ldots + \hat{e}^{l_{N'}}) + \ldots = 0$$
$$C_i \in \mathbb{Z},\; k_i,\; l_j, \text{ --- assoziierte algebraische Zahlen}$$

2 Wir multiplizieren 1. mit einer ganzen Zahl M und zerlegen jeden Summanden in einen ganzzahligen Anteil und einen Dezimalbruch < 1
$$\left.\begin{aligned} &M(\hat{e}^{k_1} + \hat{e}^{k_2} + \ldots + \hat{e}^{k_N}) = M_1 + \varepsilon_1 \\ &M(\hat{e}^{l_1} + \hat{e}^{l_2} + \ldots + \hat{e}^{l_{N'}}) = M_2 + \varepsilon_2 \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \end{aligned}\right\} M_i \in \mathbb{Z},\; \varepsilon_i < 1,\; \varepsilon_i \in \mathbb{R}$$

3. Die Beziehung 1. erhält dann die Gestalt
$$C_0M + C_1M_1 + C_2M_2 + \ldots$$
$$+ C_1\varepsilon_1 + C_2\varepsilon_2 + \ldots = 0$$

4. Die erste Zeile von 3 ist eine ganze Zahl, die sich nicht durch eine geeignete Primzahl teilen läßt, die daher auch nicht verschwinden kann

5. Die zweite Zeile von 3. kann beliebig klein gemacht werden. Da die Summe einer ganzen Zahl ≠ 0 und einer Zahl < 1 nicht verschwinden kann, ergibt sich ein Widerspruch zum Ansatz 1.

Wir benutzen wieder das Symbol

$$h^r := r! \qquad \underline{\text{gilt nur für den Buchstaben h!}}$$

und wählen als Faktor M die ganze Zahl M := Ψ(h), wobei gilt

$$\Psi(x) := \frac{x^{p-1}}{(p-1)!}.[(k_1 - x)(k_2 - x)\cdots(k_N - x)]^p.a^{Np}a^{N'p}a^{N''p}\ldots$$
$$.[(l_1 - x)(l_2 - x)\cdots(l_{N'} - x)]^p.b^{Np}b^{N'p}b^{N''p}\ldots$$

. . . .

Hier sind die k_i, l_j,... assoziierte algebraische Zahlen, und zwar sind

k_i ... Nullst. von $ax^N + a_1x^{N-1} + \ldots + a_N = 0$

l_j ... Nullst. von $bx^{N'} + b_1x^{N'-1} + \ldots + b_{N'} = 0$

.....

p ist eine beliebige (hinreichend große) Primzahl, für die gilt

$$p > |C_0|, |a|, |a_1|, \ldots, |a_N|$$
$$|b|, |b_1|, \ldots, |b_{N'}|$$
$$.....$$

Die in $\Psi(x)$ enthaltenen Faktoren a^{Np}, $a^{N'p}$,... wurden hinzugefügt, um sicherzustellen, daß die elementarsymmetrischen Funktionen von

$$ak_1, \ldots, ak_N$$
$$bl_1, \ldots, bl_{N'}$$

ganzzahlig sind. Der Grad von $\Psi(x)$ ist

$$grd\,\Psi = (p-1) + Np + N'p + \ldots\ldots := K$$

Daher können wir ansetzen

$$\Psi(x) = \sum_{i=p-1}^{K} \frac{c_i}{(p-1)!}.x^i$$

Eigenschaften von $\Psi(x)$

α) Für festgehaltenes x gilt

$$\lim_{p\to\infty} \Psi(x) = 0$$

Da x auch komplexe Werte annehmen kann, muß die absolute Konvergenz nachgewiesen werden. Dazu betrachten wir die Funktion

$$\Psi'(x) := \frac{|x|^{p-1}}{(p-1)!}.\underbrace{\left[a^{(N+N'+N''+\ldots)}.b^{(N+N'+N''+\ldots)}\cdots(|k_1|+|x|)\ldots(|l_1|+|x|)\ldots\right]^p}_{Z}$$

Für ein festes x ist der Wert der eckigen Klammer eine Konstante Z, sodaß gilt

$$\Psi'(x) = \frac{|x.Z|^{p-1}}{(p-1)!}.Z \Rightarrow \lim_{p\to\infty} \Psi'(x) = 0$$

umsomehr gilt dies für die viel schwächere Behauptung

$$\lim_{p\to\infty} \Psi(x) = 0$$

β) $\Psi(h)$ ist ganzzahlig, nicht durch p teilbar, daher ungleich Null. In

$$\Psi(h) = \sum_{i=p-1}^{K} \frac{c_i}{(p-1)!}.h^i$$

hat der erste Koeffizient c_{p-1} den Wert

$$c_{p-1} = [(ak_1)(ak_2)\ldots(ak_N)]^p.a^{N'p}a^{N'p}\ldots.$$
$$.[(bl_1)(bl_2)\ldots(bl_{N'})]^p.b^{Np}a^{N'p}\ldots.$$
$$.....$$

In den eckigen Klammern stehen dann die ganzzahligen elementarsymmetrischen Funktionen, d. h.es gilt

$$c_{p-1} = (-1)^{(Np+N'p+N''p+\dots)}\left[a_N a^{N-1}\right]^p . a^{N'p} a^{N''p} \dots$$
$$. \left[b_{N'} b^{N'-1}\right]^p . b^{Np} b^{N''p} \dots$$
$$\dots\dots\dots\dots\dots\dots$$

c_{p-1} ist der Koeffizient von h^{p-1} Da sich $(p-1)!$ wegkürzt und nach Voraussetzung $p > a$, a_N, ... ist, ist die ganze Zahl c_{p-1} nicht durch p teilbar.
Die restlichen Summanden sind auch ganzzahlig, da die Koeffizienten der Potenzen von x ja ganzzahlige elementarsymmetrische Funktionen sind und für $h^r = r!$ mit $r > p - 1$ sich alle Brüche mit dem Nenner $=(p-1)!$.kürzen lassen. Aus allen Summanden bis auf den ersten c_{p-1} läßt sich auch der Faktor p herausheben.
Da demnach alle Summanden von $\Psi(h)$ bis auf den ersten durch p teilbar sind, ist die ganz Zahl $\Psi(h)$ nicht durch p teilbar, daher von Null verschieden.

γ) $\sum \Psi(k_\nu + h)$ ist eine ganze, durch p teilbare Zahl, $k_1, \dots, k_N$ sind assoziierte algebraische Zahlen). Es ist

$$\Psi(k_\nu + h) = \frac{(k_\nu + h)^{p-1}}{(p-1)!} .$$
$$.\left[(k_1 - k_\nu - h)(k_2 - k_\nu - h)\dots(-h)\dots(k_N - k_\nu - h)\right]^p . a^{Np} a^{N'p} a^{N''} \dots$$
$$.\left[(l_1 - k_\nu - h)(l_2 - k_\nu - h)\dots\dots(l_{N'} - k_\nu - h)\right]^p . b^{Np} b^{N'p} b^{N''} \dots$$
$$\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots$$
$$= (-1)^p h^p a . \frac{a^{p-1}(k_\nu + h)^{p-1}}{(p-1)!} .$$
$$.\left[(k_1 - k_\nu - h)(k_2 - k_\nu - h)\dots\dots(k_N - k_\nu - h)\right]^p . a^{(N-1)p} a^{N''p} \dots$$
$$a^{N'p} .\left[(l_1 - k_\nu - h)(l_2 - k_\nu - h)\dots\dots(l_{N'} - k_\nu - h)\right]^p . b^{Np} b^{N'p} b^{N''} \dots$$
$$\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots$$

Hier treten alle l_j,... wieder symmetrisch auf, d.h. die symmetrischen Polynome in den l_j,.. lassen sich durch die ganzzahligen elementarsymmetrischen Funktionen der l_j,..darstellen, sind also ganzzahlig.
Da k_ν einzeln auftritt, ist $\Psi(k_\nu + h)$ keine symmetrische Funktion in den assoziierten algebraischen Zahlen k_i. Um Symmetrie zu erreichen bilden wir

$$\sum_{i=1}^{N} \Psi(k_i + h) = \sum (-1)^p . \frac{h^p a}{(p-1)!} .[\dots]$$

Nunmehr treten in der eckigen Klammer nur mehr symmetrische Funktionen aller assoziierten Zahlen k_i, l_j,... auf, deren Wert stets ganzzahlig ist. Wegen $h^p = p!$ ist also

$\sum_{i=1}^{N} \Psi(k_i + h)$ eine ganze, durch p teilbare Zahl.

Dasselbe gilt natürlich auch für alle Ausdrücke

$$\sum_{i=1}^{N} \Psi(k_i + h), \quad \sum_{j=1}^{N'} \Psi(l_j + h)$$

Beweis des Theorems von LINDEMANN

1. Wir nehmen an, es gäbe eine Beziehung der Gestalt

$$C_0 + C_1\left(\hat{e}^{k_1} + \hat{e}^{k_2} + \dots + \hat{e}^{k_N}\right) + C_2\left(\hat{e}^{l_1} + \hat{e}^{l_2} + \dots + \hat{e}^{l_{N'}}\right) + \dots = 0$$

2. Wir multiplizieren diese Beziehung mit der von Null verschiedenen ganzen Zahl
M := Ψ(h)

$$C_0\Psi(h)+C_1\left(\hat{e}^{k_1}\Psi(h)+\ldots+\hat{e}^{k_N}\Psi(h)\right)+C_2\left(\hat{e}^{l_1}\Psi(h)+\ldots+\hat{e}^{l_{N'}}\Psi(h)\right)+\ldots=0$$

Aus dieser Summe betrachten wir den Ausdruck

$$\hat{e}^k\Psi(h)=\hat{e}^k\sum\frac{c_i}{(p-1)!}.h^i=\sum\frac{c_i}{(p-1)!}.\hat{e}^k h^i$$

Wie bereits gezeigt, gilt

$$\hat{e}^k.h^i=(h+k)^i+k^i.\left[0+\frac{k}{i+1}+\frac{k^2}{(i+1)(i+2)}+\ldots\right]$$

Hier tritt allerdings die Schwierigkeit auf, daß die algebraische Zahl k auch <u>komplex</u> sein kann. Wir ersetzen daher k durch seinen Betrag |k|. Vergleicht man

$$0+\frac{|k|}{(i+1)}+\frac{|k|^2}{(i+1)(i+2)}+\ldots$$

mit

$$\hat{e}^{|k|}=1+\frac{|k|}{1!}+\frac{|k|^2}{2!}+\ldots$$

so findet man

$$\left|0+\frac{k}{i+1}+\frac{k^2}{(i+1)(i+2)}+\ldots\right|<0+\frac{|k|}{(i+1)}+\frac{|k|^2}{(i+1)(i+2)}+\ldots<\hat{e}^{|k|}$$

daher kann man setzen

$$\frac{k}{(i+k)}+\frac{k^2}{(i+1)(i+2)}+\ldots=q_{i,k}.\hat{e}^{|k|}$$

worin $q_{i,k}$ eine komplexe Größe mit $|q_{i,k}|<1$ ist

$$\hat{e}^k\Psi(h)=\sum_{i=p-1}^{K}\frac{c_i}{(p-1)!}.\hat{e}h^i=\sum_{i=p-1}^{K}\frac{c_i}{(p-1)!}.(h+k)^i+\hat{e}^{|k|}\sum_{i=p-1}^{K}\frac{c_i}{(p-1)!}.q_{i,k}k^i=$$

und

$$=\Psi(h+k)+\hat{e}^{|k|}\sum_{i=p-1}^{K}\frac{c_i}{(p-1)!}.q_{i,k}k^i$$

Summiert man über alle k, so gilt

$$\sum_{\nu=1}^{N}\hat{e}^{k_\nu}\Psi(h)=\sum_{\nu=1}^{N}\Psi(h+k_\nu)+\sum_{\nu=1}^{N}\left[\hat{e}^{|k_\nu|}.\sum_{i=p-1}^{K}\frac{c_i}{(p-1)!}.q_{i,k_\nu}k_\nu^i\right]$$

3. Führt man diese Schritte für alle assoziierten algebraischen Zahlen aus, so ergibt sich

$$C_0\Psi(h)+C_1.\sum_{\nu=1}^{N}\Psi(h+k_\nu)+C_2.\sum_{\mu=1}^{N'}\Psi(h+l_\mu)+\ldots\ldots$$

$$C_1.\sum_{\nu=1}^{N}\left[\hat{e}^{|k_\nu|}\sum_{i=p-1}^{K}\frac{c_i}{(p-1)!}.q_{i,k_\nu}k\right]+\ldots\ldots$$

4. In der ersten Zeile sind alle Summanden ganze Zahlen, von denen jeder, mit Ausnahme des ersten durch p teilbar ist. Die erste Zeile stellt also eine ganze Zahl dar, die nicht durch p teilbar ist, die daher <u>nicht Null sein kann</u>

5. Nach α) wissen wir, daß

$$\lim_{p\to\infty}\Psi(x)=\lim_{p\to\infty}\sum\frac{c_i}{(p-1)!}.x^i=0$$

ist, also auch dann, wenn wir $x := k_\nu$ setzen. Dies gilt umsomehr für

$$\sum_{i=p-1}^{K} \frac{c_i}{(p-1)!}.q_{i,k_\nu} k_\nu^i$$

und auch für

$$\hat{e}^{|k_\nu|} \sum_{i=p-1}^{K} \frac{c_i}{(p-1)!}.q_{i,k_\nu} k_\nu^i$$

da ja $\hat{e}^{|k_\nu|}$ nur eine konstanter Faktor ist. Daher kann die zweite Zeile von 3. bei geeignet großer Wahl von p beliebig klein gemacht werden. Der Ausdruck 1. ist daher die Summe einer nicht verschwindenden ganzen Zahl und eines beliebig kleinen Dezimalbruchs, kann daher nie verschwinden

Korollar zum Satz von Lindemann: Die Zahl ê kann keiner Gleichung der Gestalt

$$C'_0 + C'_1\hat{e}^{k_1} + C'_2\hat{e}^{l_1} + \ldots = 0$$

genügen, worin die C'_i ganze Zahlen und die k_1, l_1,... nichtassoziierte algebraische Zahlen sind.

Zum Beweis betrachten wir die jeweils ergänzenden assoziierten algebraischen Zahlen $k_2, \ldots, k_N; l_2, \ldots, l_{N'}, \ldots$, und bilden das Produkt

$$\prod_{\substack{\alpha=1\ldots N \\ \beta=1\ldots N'}} \left(C'_0 + C'_1.\hat{e}^{k_\alpha} + C'_2.\hat{e}^{l_\beta} + \ldots\right) =$$

$$= C_0 + C_1\left(\hat{e}^{k_1} + \hat{e}^{k_2} + \ldots + \hat{e}^{k_N}\right) + C_2\left(\hat{e}^{k_1+k_2} + \hat{e}^{k_1+k_3} + \ldots\right) + C_3\left(\hat{e}^{k_1+l_1} + \hat{e}^{k_1+l_2} + \ldots\right) + \ldots. =$$
$$= \sum C_i\left(\hat{e}^{w_1(k_\alpha, l_\beta, \ldots)} + \hat{e}^{w_2(k_\alpha, l_\beta, \ldots)} + \ldots\right) = 0$$

In jeder der Klammern stellen die Exponenten $w_i(k_\alpha, l_\beta, \ldots)$ lineare Ausdrücke in den assoziierten algebraischen Zahlen k_α, l_β,... dar. Die elementarsymmetrischen Funktionen der w_i sind infolge des Ansatzes symmetrische Polynome in den k_α, l_β,... und daher durch deren ganzzahlige elementarsymmetrische Funktionen darstellbar. Die Exponenten jeder Klammer sind daher Nullstellen einer algebraischen Gleichung mit ganzzahligen Koeffizienten , also assoziierte algebraische Zahlen.

Wir können daher den Satz von LINDEMANN auf das Produkt Π anwenden. Da dieses nie verschwinden kann, kann auch keiner der Faktoren verschwinden. Damit ist das Korollar bewiesen.

Es gilt aber weiter

Die Zahl ê kann keiner Bedingung der Bauart

$$C_0^{(1)} + C_1^{(1)}\hat{e}^k + C_2^{(1)}\hat{e}^l + \ldots = 0$$

genügen, in der sowohl die $C_i^{(1)}$ als auch die k,l, ... nichtassoziierte algebraische Zahlen sind.

Zum Beweis bilden wir das Produkt

$$\prod_{\substack{\alpha=1,\ldots,N_0 \\ \beta=1,\ldots N_1 \\ \gamma=1,\ldots N_2}} \left[C_0^{(\alpha)} + C_1^{(\beta)}\hat{e}^k + C_2^{(\gamma)}\hat{e}^l + \ldots\right] = C_0 + C_1\hat{e}^k + C_2\hat{e} + C_3\hat{e}^{2k} + C_4\hat{e}^{2l} + C_5\hat{e}^{k+l} + \ldots$$

Hiere sind die $C_0^{(\alpha)}$ die zu $C_0^{(1)}$ assoziierten algebraischen Zahlen, die $C_1^{(\beta)}$ die zu $C_1^{(1)}$ assoziierten algebraischen Zahlen usw. Die Koeffizienten des Produktes sind dann symmetrische Funktionen in den

$$C_0^{(1)}, C_0^{(2)}, \ldots, C_0^{(N_0)}$$
$$C_1^{(1)}, C_1^{(2)}, \ldots, C_1^{(N_1)}$$
$$\ldots\ldots\ldots$$

Diese symmetrischen Funktionen lassen sich durch die ganzzahligen elementarsymmetrischen Funktionen der $C_i^{(j)}$ ausdrücken, sind also selbst ganzzahlig. Damit gilt das Korollar. Demnach kann obiges Produkt nicht verschwinden, daher auch keiner seiner Faktoren. Es gilt also allgemein:

> Die Zahl ê kann keine Beziehung der Gestalt
> $$C_0 + C_1 ê^k + C_2 ê^l + \ldots = 0$$
> erfüllen, in der sowohl die Koeffizienten wie die Exponenten algebraische Zahlen sind

Umgekehrt kann man sagen

> Besteht die Beziehung
> $$C_0 + C_1 ê^k + C_2 ê^l + \ldots = 0$$
> so können nicht alle Koeffizienten oder Exponenten algebraisch sein

Aus diesem Satz können wir sofort auf die Transzendenz von π schließen. Es gilt nämlich nach EULER

$$1 + ê^{iπ} = 0$$

Nach obigem Satz kann π nicht algebraisch sein. Es ist also transzendent

Das Einschiebelineal

Als nichtklassisches Zeicheninstrument wollen wir das *Einschiebelineal* betrachten. Mit seiner Hilfe lassen sich (bis auf wenige Sonderfälle) alle Aufgaben 3. und 4. Grades lösen. Das Einschiebelineal besteht aus einem gewöhnlichen geradlinigen Lineal und einer ein für alle Mal darauf markierten Strecke s, der *Einschiebestrecke* (*Intervall*). Am einfachsten ist seine Verwendung als *Papierstreifen* oder als eine auf Transparentpapier aufgetragene Gerade als Trägerin der Strecke s.

Gebrauch des Einschiebelineals

1. Verwendung wie die erlaubte Anwendung eines normalen Lineals
2. Abtragen des Intervalls s auf eine vorhandene Gerade von einem darauf befindlichen Punkt nach beiden Seiten
3. Einschieben des Intervalls s zwischen zwei gegebene Gerade, wobei das Lineal durch einen vorgegebenen Punkt geht
4. Einschieben des Intervalls zwischen einer gegebenen Geraden und einem gegebenen Kreis, wobei das Lineal durch einen gegebenen Punkt geht.
5. Einschieben des Intervalls zwischen zwei gegebene Kreise, wobei die Gerade durch einen gegebenen Punkt geht.

Der Gebrauch des Zirkels in der üblichen Weise ist neben der Verwendung des Einschiebelineals gestattet.[1]

Wir zeigen nun die Verwendung des Einschiebelineals bei den klassischen, mit Zirkel und Lineal nicht lösbaren Problemen.

Die Dreiteilung des Winkels

Dreiteilung nach NIKOMEDES

Gegeben sei der Winkel mit den Schenkeln a und b. Auf b tragen wir die Strecke OP = r = s/2 ab. Dann schieben wir die Streck AB = s = 2r zwischen zwei Gerade l, h durch P, von denen h parallel, l normal zum Winkelschenkel a ist, so sein, daß das Lineal durch den Winkelscheitel O geht. ($3\alpha = 60°$, $r = 3/\sin 60°$, $s = 2r$)

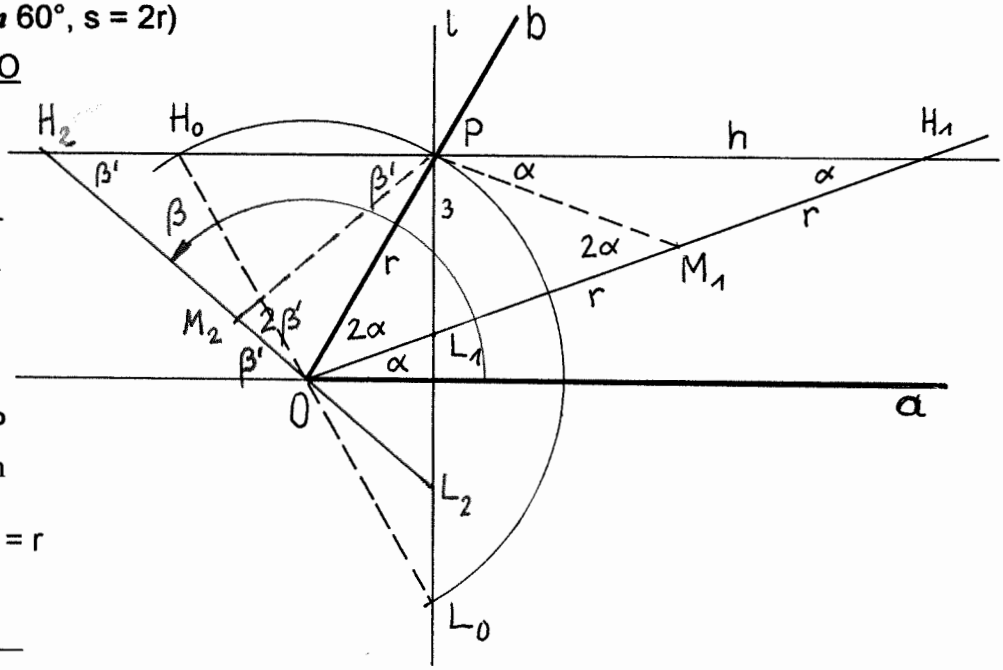
<u>Triviale Einschiebung H_0L_0O</u>

Sie läßt sich mit Zirkel und Lineal konstruieren, indem man den Kreis (O,r) mit h und l schneidet. Wegen der Konstruierbarkeit mit Zirkel und Lineal ist diese Einschiebung uninteressant.

<u>Erste Möglichkeit H_1L_1O</u>

Im rechtwinkeligen ΔL_1H_1P gilt nach THALES und nach Konstruktion

$L_1M_1 = M_1H_1 = M_1P = PO = r$



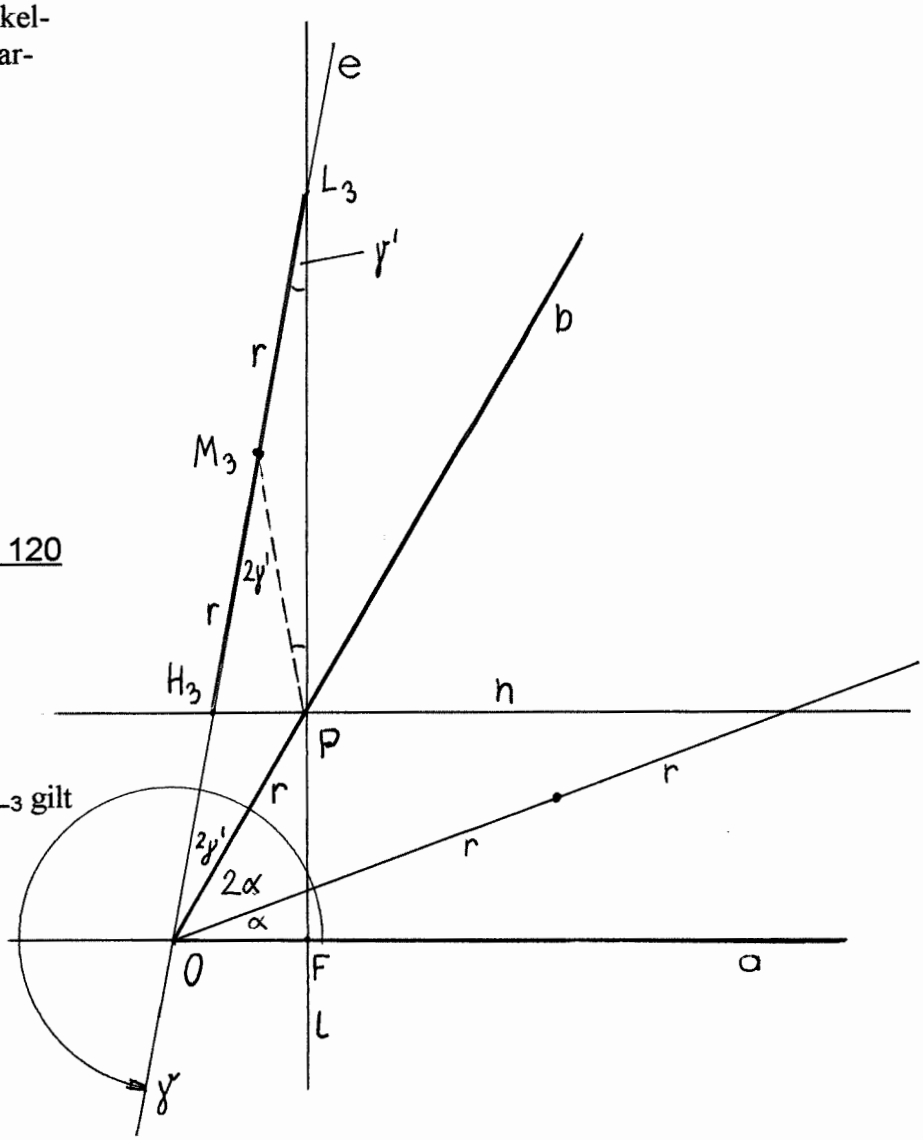
[1] Jakob STEINER (1796-1863) hat gezeigt, daß alle Konstruktionen, die mit Zirkel und Lineal ausführbar sind, auch mit dem Lineal allein bewerkstelligt werden können, wenn ein einziger Kreis mit Mittelpunkt gezeichnet vorliegt. Da man mit der Einschiebestrecke einen Kreis wenigstens punktweise darstellen kann, könnte man im Prinzip bei Verwendung des Einschiebelineals auf den Zirkel verzichten

Es seib $\alpha := \angle PH_1M_1$. Dann gilt wegen der auftretenden gleichschenkeligen Dreiecke und nach dem Außenwinkelsatz und wegen des auftretenden Parallelwinkels

$\angle PH_1M_1 = \angle M_1PH_1 = \alpha \Rightarrow$

$\angle OM_1P = 2\alpha = \angle POM_1 \Rightarrow$

$\angle (ab) = 3\alpha \Rightarrow \underline{\alpha = \frac{1}{3}\angle(ab)}$



Zweite Möglichkeit: H_2L_2O

$\angle PH_2M_2 = \angle M_2PH_2 = \beta' \Rightarrow$

$\angle OM_2P = 2\beta' = \angle POM_2 \Rightarrow$

$3\beta' + 3\alpha = 180 \Rightarrow \beta' = 60 - \alpha$

Wegen $\beta = 180 - \beta'$ folgt $\underline{\beta = \alpha + 120}$

Dritte Möglichkeit: H_3L_30

$\angle PL_3M_3 = \angle M_3PL_3 = \gamma' \Rightarrow$

$\angle PM_3O = 2\gamma' = \angle POM_3$

Im rechtwinkeligen Dreieck ΔFOL_3 gilt

$3\gamma' + 3\alpha = 90 \Rightarrow \gamma' = 30 - \alpha$

Weiters gilt

$\gamma = 2\gamma' + 3\alpha + 180 \Rightarrow$

$\gamma = 60 - 2\alpha + 3\alpha + 180$

also

$\underline{\gamma = \alpha + 240}$

Die Konchoide des NIKOMEDES[1]

Obige Konstruktionen können auch dargestellt werden als Schnitt der *Konchoide des* NIKOMEDES mit der Geraden h.

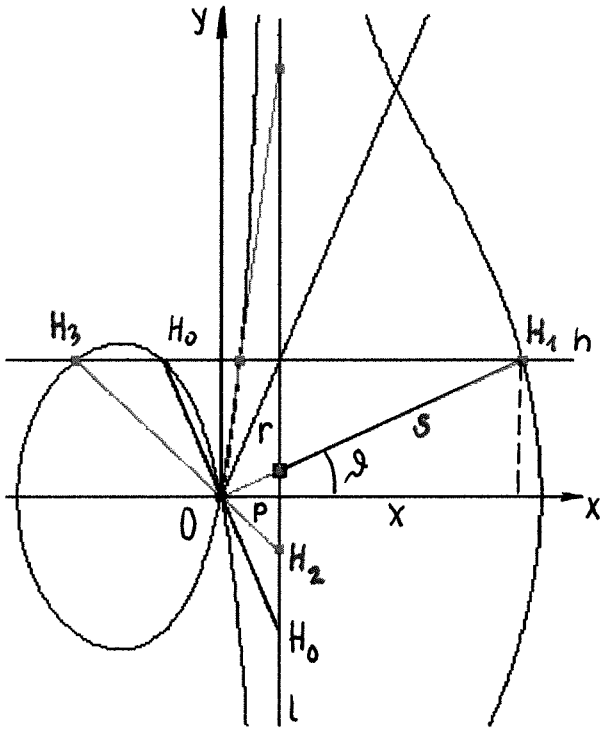
Wir wählen einen festen Punkt O, den *Pol*, eine feste Gerade l, die *Basislinie* oder *Leitlinie* und eine feste Strecke s, das *Intervall* der Konchoide. Der Abstand p von Pol und Baslisinie heißt *Poldistanz*.

Dann gilt

$$x = p + s.\cos\vartheta \Rightarrow \cos\vartheta = \frac{x-p}{s}$$

$$y = x.\tan\vartheta = x.\frac{\sin\vartheta}{\cos\vartheta} = \frac{xs}{x-p}.\sin\vartheta \Rightarrow \sin\vartheta = y.\frac{x-p}{xs}$$

[1] Die Konchoide („Muschelkurve") hat ihren Namen von der Gestalt einer ihrer Formen (siehe Seite 100) Die Erfindung der Konchoide wurde dem NIKOMEDES von PAPPOS zugeschrieben.



Daraus

$$\sin^2\vartheta+\cos^2\vartheta=1=y^2.\frac{(x-p)^2}{x^2s^2}+\frac{(x-p)^2}{s^2}\Rightarrow x^2s^2=(x-p)^2(x^2+y^2)$$

$$\boxed{(x^2+y^2)(x-p)^2-s^2x^2=0}$$

Konchoide des Nikomedes

Die Schnittpunkte dieser Kurve 4.Ordnung mit einer Geraden ergeben sich also als Nullstellen einer Gleichung 4.Grades. Geht die zu schneidende Gerade jedoch durch einen bereits bekannten Punkt der Konchoide, so reduziert sich die Aufsuchung der Schnittpunkte auf ein Problem 3.Grades.

Die oben durchgeführten Konstruktionen für die Winkeldreiteilung laufen auf den Schnitt der Geraden h mit einer Konchoide hinaus. Es gibt also vier Einschiebemöglichkeiten, von denen die triviale ausscheidet.

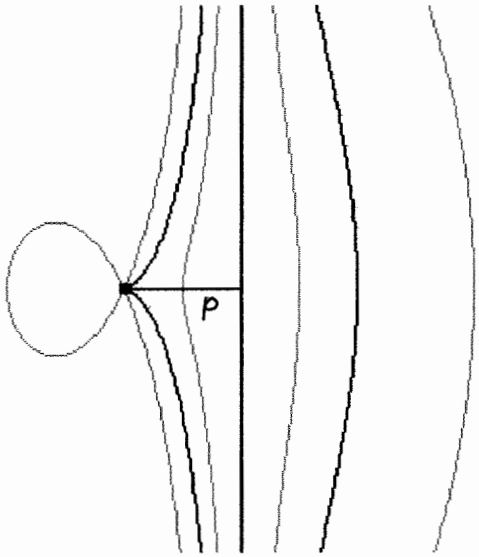
Wir bestimmen die vier Schnittpunkte der Konchoide mit der Geraden h mit der Gleichung $y=\sqrt{r^2-p^2}$. Einsetzen in obige Gleichung ergibt

$$(x^2+y^2)(x-p)^2-s^2x^2=0\wedge y=\sqrt{r^2-p^2}\wedge s=2r\Rightarrow$$
$$(x^2+r^2-p^2)(x-p)^2-4r^2x^2=\left[(x-p)(x+p)+r^2\right](x-p)^2-4r^2x^2=$$
$$=(x-p)^3(x+p)+r^2\left[(x-p)^2-4x^2\right]=$$
$$=(x-p)^3(x+p)+r^2\left[(x-p)-2x\right]\left[(x-p)+2x\right]=(x-p)^3(x+p)+r^2\left[3x-p\right]\left[-(p+x)\right]=$$
$$=\underline{(x+p)\left[(x-p)^3-r^2(3x-p)\right]=0}$$

Die Gleichung 4.Grades zerfällt also in den Linearfaktor (x + p), welcher dem trivialen Einschub entspricht und den irreduziblen Faktor 3.Ordnung $(x-p)^3-r^2(3x-p)$.

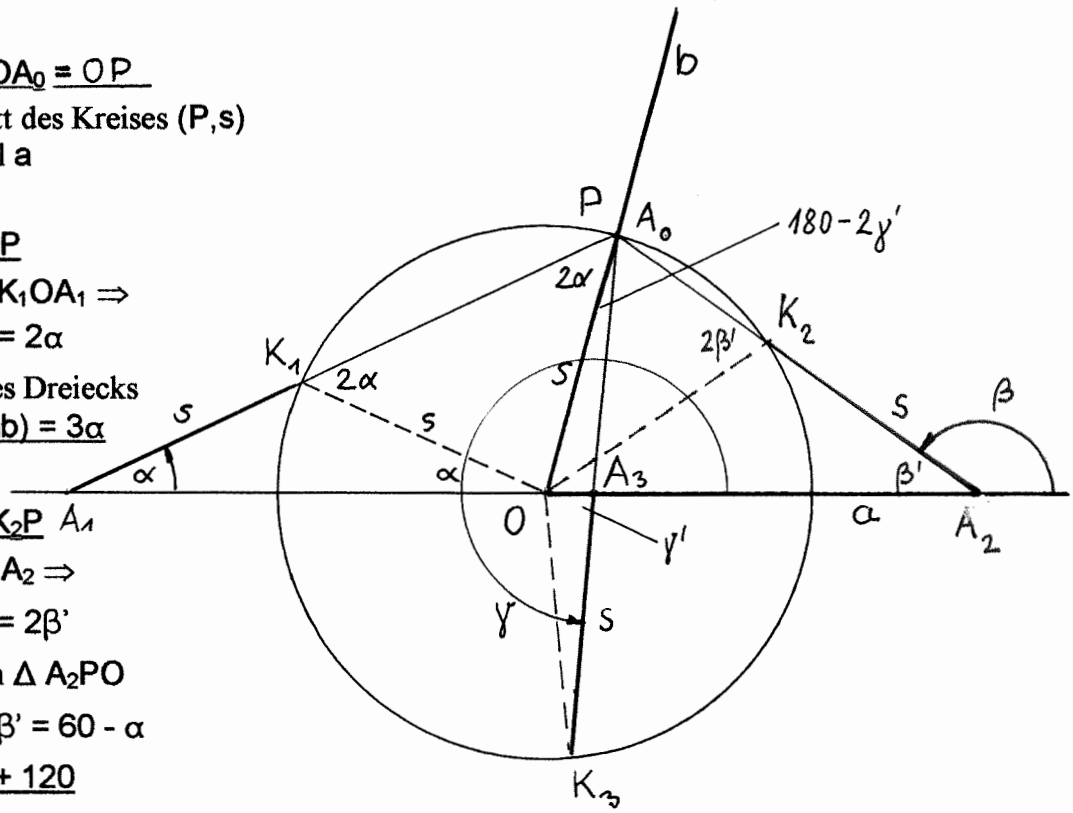
Die Gestalt der Konchoide hängt vom Verhältnis des Intervalles s und der Poldistanz p ab. Es ergibt sich eine der folgenden Möglichkeiten

s < p Muschelform, **s = p gespitze Form,** s > p Doppelpunkt



Winkeldreiteilung nach ARCHIMEDES[1]

Zur Drittelung des Winkels $\angle (ab) = 3\alpha$ mit dem Scheitel O wählen wir auf dem Winkelschenkel b den Punkt P, dessen Abstand von O gleich der Einschiebestrecke s ist. s ist zwischen den Winkelschenkel a und dem Kreis k(O,s) so einzuschieben, daß das Einschiebelineal durch den Punkt P auf dem Schenkel b geht. ($3\alpha = 75°$, $s = 3{,}5$)



Triviale Einschiebung: $\underline{OA_0 = OP}$

Sie ergibt sich als Schnitt des Kreises (P,s) mit dem Winkelschenkel a

Erste Möglichkeit: $\underline{A_1K_1P}$

Sei $\alpha := \angle K_1A_1O = \angle K_1OA_1 \Rightarrow$

$\Rightarrow \angle OK_1P = \angle K_1PO = 2\alpha$

Für den Außenwinkel des Dreiecks ΔA_1OP gilt daher $\underline{\angle (ab) = 3\alpha}$

Zweite Möglichkeit: $\underline{A_2K_2P}$

$\beta' = \angle K_2A_2O = \angle K_2OA_2 \Rightarrow$

$\Rightarrow \angle OK_2P = \angle OPK_2 = 2\beta'$

Für die Winkelsumme in ΔA_2PO

gilt $3\beta' + 3\alpha = 180 \Rightarrow \beta' = 60 - \alpha$

Daher $\underline{\beta = 180 - \beta' = \alpha + 120}$

Dritte Möglichkeit: $\underline{A_3K_3P}$

$\gamma' = \angle K_3OA_3 = \angle K_3A_3O \Rightarrow$

[1] ARCHIMEDES (287?-212 v. Chr.)

$\Rightarrow \angle OK_3A_3 = 180 - 2\gamma' = \angle OPK_3$

Für den Außenwinkel von ΔA_1A_3P

gilt daher

$\alpha + 2\alpha + 180 - 2\gamma' = \gamma' \Rightarrow \gamma' = \alpha + 60$

Wegen $\gamma = \gamma' + 180$ folgt $\underline{\gamma = \alpha + 240}$

Obige Konstruktion gestattet zwei Auffassungen:

1. Schnitt des Kreises k mit der durch den Pol P, der Leitlinie a und dem Intervall s fesgelegten Konchoide des NIKOMEDES
2. Schnitt der Geraden a mit der *Kreiskonchoide* , welche durch den Kreis k als Leitkurve, den Punkt P als Pol und das Intervall s bestimmt ist. Diese Kurve heißt auch PASCALschnecke, benannt nach Étienne PASCAL (1588-1651), den Vater von Blaise PASCAL (1623-1662)

Gleichung der PASCALschnecke

Sei d der Durchmesser des *Basiskreises* k und O der auf k liegende *Pol* der PASCALschnecke

$$x = \cos(\vartheta).(d.\cos(\vartheta) + s)$$
$$y = \sin(\vartheta).(d.\cos(\vartheta) + s)$$

Daraus folgt wegen

$$\cos(\vartheta) = \frac{x}{\sqrt{x^2 + y^2}} \Rightarrow$$

$$x^2 + y^2 = \left(d.\frac{x}{\sqrt{x^2 + y^2}} + s \right)^2 =$$

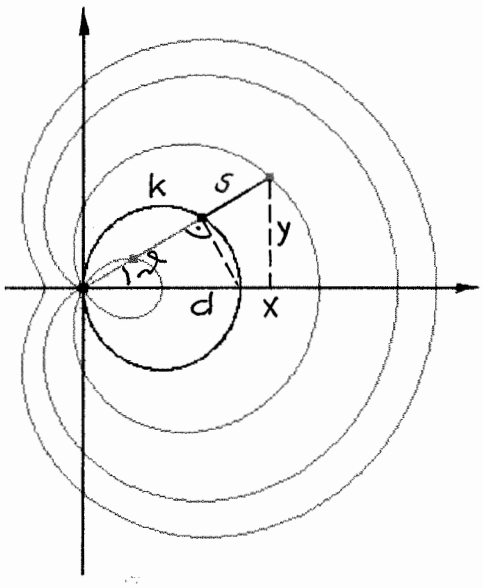
$$= \frac{\left(d.x + s.\sqrt{x^2 + y^2}\right)^2}{x^2 + y^2} \Rightarrow$$

$$\Rightarrow \left(x^2 + y^2\right)^2 = \left(d.x + s.\sqrt{x^2 + y^2}\right)^2 \Rightarrow$$

$$\Rightarrow \left(x^2 + y^2\right) = \left(d.x + s.\sqrt{x^2 + y^2}\right) \Rightarrow$$

$$\Rightarrow \left(x^2 + y^2\right) - d.x = s.\sqrt{x^2 + y^2} \Rightarrow$$

$$\Rightarrow \left(x^2 + y^2 - d.x\right)^2 = s^2\left(x^2 + y^2\right)$$



Daher

$$\boxed{\left(x^2 + y^2 - d.x\right)^2 - s^2\left(x^2 + y^2\right) = 0}$$

Allgemeine Gleichung der PASCALschnecke

Die PASCALschnecke als Trisektrix

Im Falle der Winkeldreiteilung haben wir zu setzen

$$d = 2s$$

Dann gilt

$$\left(x^2+y^2-2sx\right)^2-s^2\left(x^2+y^2\right)=0$$ **PASCALschnecke als Trisektrix**

Setzen wir k = - *tan*(3α), so haben wir die Trisektrix mit der Geraden y = k(x-s) zu schneiden.

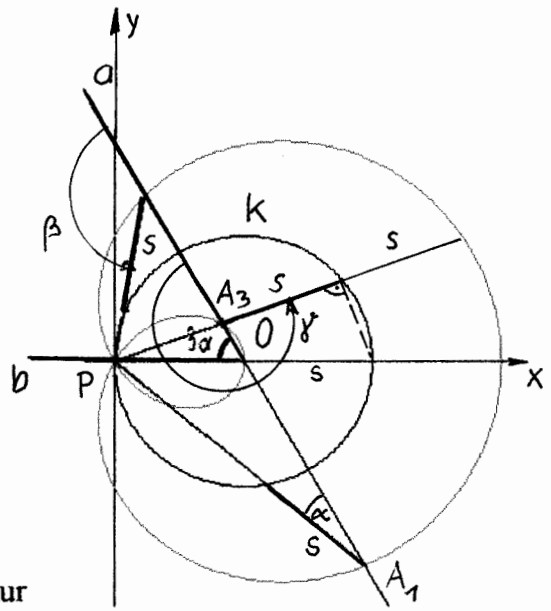
$$\left(x^2+k^2(x-s)^2-2sx\right)^2-s^2\left(x^2+k^2(x-s)^2\right)=0$$

Umformung und Ausquadrieren ergibt

$$\left[k^2(x-s)^2+x(x-s)-sx\right]^2-s^2\left(x^2+k^2(x-s)^2\right)=0$$

$$\left[\left(k^2(x-s)+x\right)(x-s)-sx\right]^2-s^2x^2-s^2k^2(x-s)^2=0$$

$$\left(k^2(x-s)+x\right)^2(x-s)^2-2sx\left(k^2(x-s)+x\right)(x-s)+$$
$$+s^2x^2-s^2x^2-s^2k^2(x-s)^2=0$$



Daher gilt

$$(x-s)\left[\begin{matrix}\left(k^2(x-s)+x\right)^2(x-s)-2sx\left(k^2(x-s)+x\right)\\-s^2k^2(x-s)\end{matrix}\right]=0$$

Es spaltet sich also der Linearfaktor (x - s) ab, sodaß nur mehr eine irreduzible Gleichung 3.Grades

$$\left(k^2(x-s)+x\right)^2(x-s)-2sx\left(k^2(x-s)+x\right)-s^2k^2(x-s)^2=0$$

zu lösen ist.

Die Vervielfachung des Würfels (Kubikwurzelziehen)

Gegeben sei ein Würfel von der Kantenlänge a. Gesucht werde ein Würfel, dessen Volumen das λ - fache des Volumens des gegebenen Würfels beträgt.

Sei x die Seitenlänge des gesuchten Würfels. Dann muß gelten

$$x^3=\lambda a^3 \Rightarrow x=a.\sqrt[3]{\lambda}$$

Die Vervielfachung des Würfels läuft also auf das Ausziehen der Kubikwurzel aus λ hinaus.

Lösung nach HIPPOKRATES VON Chios[1]

HIPPOKRATES erkannte, daß das Ausziehen der n-ten Wurzel mit der Einschaltung von (n-1) *mittleren Proportionalen* zwischen zwei gegebene Größen a und b äquivalent ist.

$$a : x_1 = x_1 : x_2 = x_2 : x_3 = \ldots = x_{n-2} : x_{n-1} = x_{n-1} : b$$

Das bedeutet

$$\frac{a}{x_1}=\frac{x_1}{x_2}=\frac{x_2}{x_3}=\cdots=\frac{x_{n-2}}{x_{n-1}}=\frac{x_{n-1}}{b}=\frac{1}{q}$$ ... konstanter Quotient

Daher

[1] HIPPOKRATES von Chios (um 440 v.Chr.). Nicht zu verwechseln mit dem berühmten Arzt HIPPOKRATES von Kos (ca. 460-ca.370 v.Chr.)

$$\left.\begin{array}{l} aq = x_1 \\ x_1 q = x_2 \\ x_2 q = x_3 \\ \vdots \\ x_{n-2} q = x_{n-1} \\ x_{n-1} q = b \end{array}\right\} \bullet \text{ Produktbildung dieser Ausdrücke ergibt } \underline{b = aq^n}$$

Setzt man $b = a\lambda \Rightarrow \frac{b}{a} = \lambda = q^n \Rightarrow \underline{q = \sqrt[n]{\lambda}}$

Die Strecken $a, x_1, \ldots, x_{n-1}, b$ bilden daher die Glieder einer geometrischen Reihe mit dem Faktor

$$\underline{q = \sqrt[n]{\frac{b}{a}} = \sqrt[n]{\lambda}}$$

$$x_1^n = a^n q^n = a^n . \frac{b}{a} = a^{n-1} b, \quad x_2^n = x_1^n q^n = a^{n-1} b . \frac{b}{a} = a^{n-2} b^2, \cdots$$

Zusammengefaßt ergibt sich also

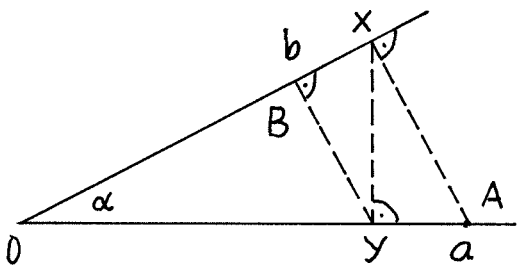
$$\boxed{\begin{array}{l} x_1^n = a^{n-1} b \\ x_2^n = a^{n-2} b^2 \\ \vdots \\ x_{n-2}^n = a^2 b^{n-2} \\ x_{n-1}^n = a b^{n-1} \end{array}}$$

Sonderfälle

$n = 2 \quad a : x = x : b, \quad x^2 = ab, \quad q = \sqrt{\lambda}, \; x = a\sqrt{\lambda}$

$n = 3 \quad a : x = x : y = y : b, \quad q = \sqrt[3]{\lambda}, \; \underline{x = a.\sqrt[3]{\lambda}}, \; b = y.\sqrt[3]{\lambda}, \; y = \frac{b}{\sqrt[3]{\lambda}}$

<u>Konstruktion für n = 3</u> Auf dem Schenkel a des Winkels $\alpha = \angle(ab)$ tragen wir die Strecke $OA = a$ auf. Durch sukzessive Normalprojektion jeweils auf den anderen Winkelschenkel ergeben sich der Reihe nach die Strecken $OA = a \rightarrow x \rightarrow y \rightarrow OB = b$



$$\frac{1}{\cos\alpha} = \frac{1}{q} = \frac{1}{\sqrt[3]{\lambda}} = \frac{a}{x} = \frac{x}{y} = \frac{y}{b} \Rightarrow a : x = x : y = y : b$$

HIPPOKRATES löste dieses Problem mit Parabeln (siehe Seite 19)

Lösung nach NEWTON[1]

Das Volumen des Würfels mit der Seitenkante a soll mit $\lambda < 1$ multipliziert werden[2]. Der gesuchte Würfel hat dann die Seitenlänge $x = a.\sqrt[3]{\lambda}$. Dazu bestimmen wir zunächst die Hilfsstrecke $b := \lambda a$, sowie auf dem Einschiebelineal e die Einschiebestrecke $s = \frac{a}{2}$. Im Kreis k(O,s) verlängern wir den den Radius OP = s nochmals um die Strecke PL = s und schlagen die Strecke $b = \lambda a = PM$ von P aus auf dem Kreis k(O,s) ab. Das Einschiebelineal e ist dann zwischen die beiden Geraden l = (LM) und h = (PM) mit dem Pol O einzuschieben. Der triviale Einschub (OPL) ist uninteressant. Es ist zu zeigen, daß für den nichttrivialen Einschub (ONX) gilt MX = x (Für den trivialen Einschub würde gelten x = MP = b)

Mit y:= XQ = ON gilt für die Potenz von X bezüglich k

$$y(y + 2s) = x(x + b) \Rightarrow y(y + a) = x(x + b) \qquad (1)$$

Anwendung des Satzes von MENELAOS[3] auf das Dreieck Δ OPX und die Gerade l ergibt

$$\frac{OL}{PL}.\frac{PM}{XM}.\frac{XN}{ON} = \frac{\overbrace{2s}^{a}}{s}.\frac{b}{x}.\frac{s}{y} = \frac{a.b}{x.y} = 1 \Rightarrow a = \frac{xy}{b} \Rightarrow \frac{a}{x} = \frac{y}{b} \qquad (2)$$

Einsetzen in (1) ergibt

$$y\left(y + \frac{xy}{b}\right) = x(x+b) \Rightarrow \frac{y^2}{b}(x+b) = x(x+b) \Rightarrow (x+b)\left(\frac{y^2}{b} - x\right) = 0$$

Dem Faktor (x + b) entspricht der triviale Einschub. Für den nichttrivialen Einschub gilt dann $\frac{x}{y} = \frac{y}{b}$. Zusammen mit (2) gilt daher $\underline{a : x = x : y = y = b}$. Zwischen die bekannten Strecken a und b werden also zwei mittlere Proportionalen eingeschaltet. Nach HIPPOKRATES folgt daraus

$$\underline{y^3 = a^3.\lambda} \Rightarrow \underline{y^3 = \frac{b^3}{\lambda}}$$

Beispiel: (a = 10, s = ½ a = 5, λ = ½)

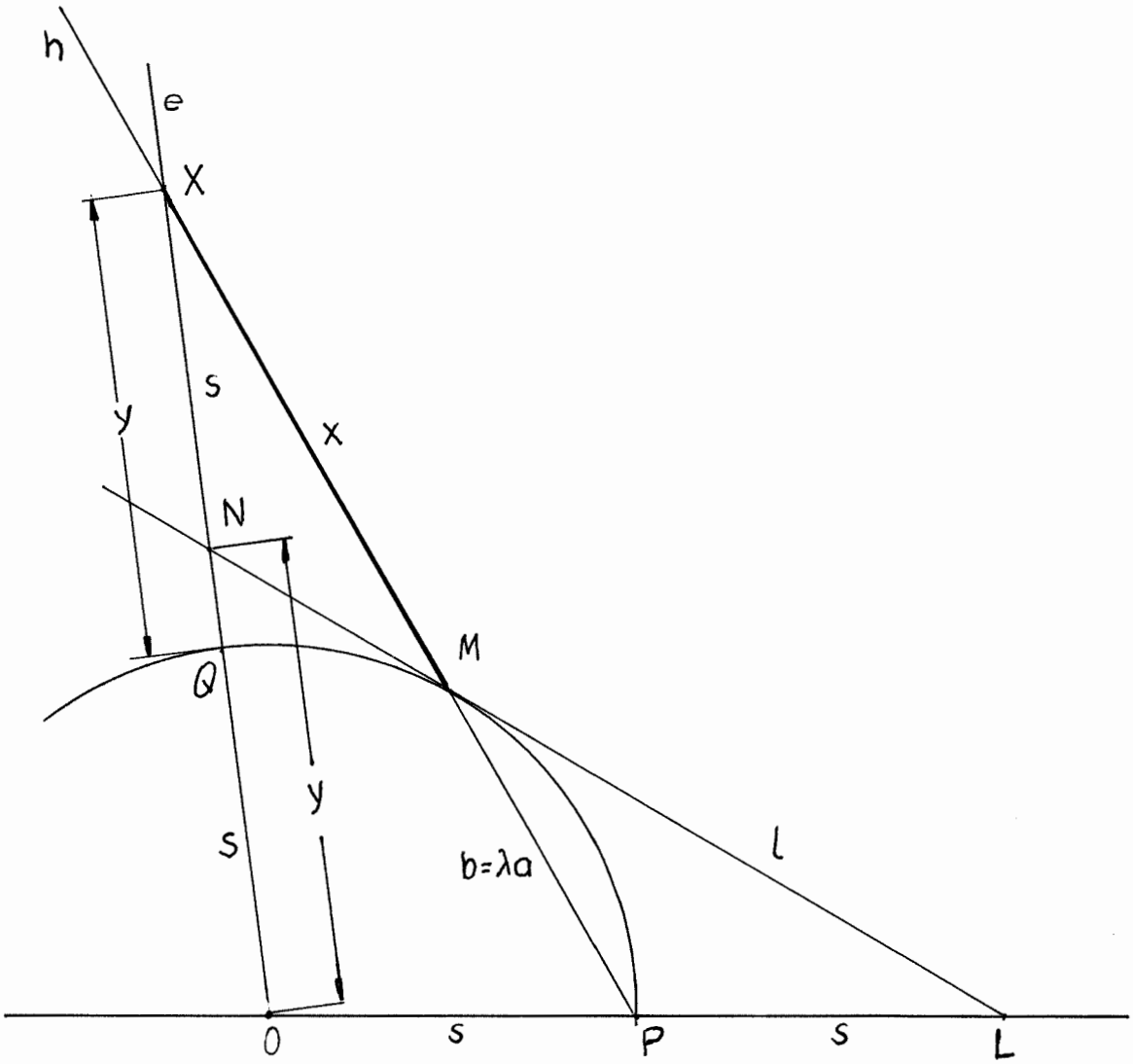
---

[1] Isaak NEWTON (1642-1727)

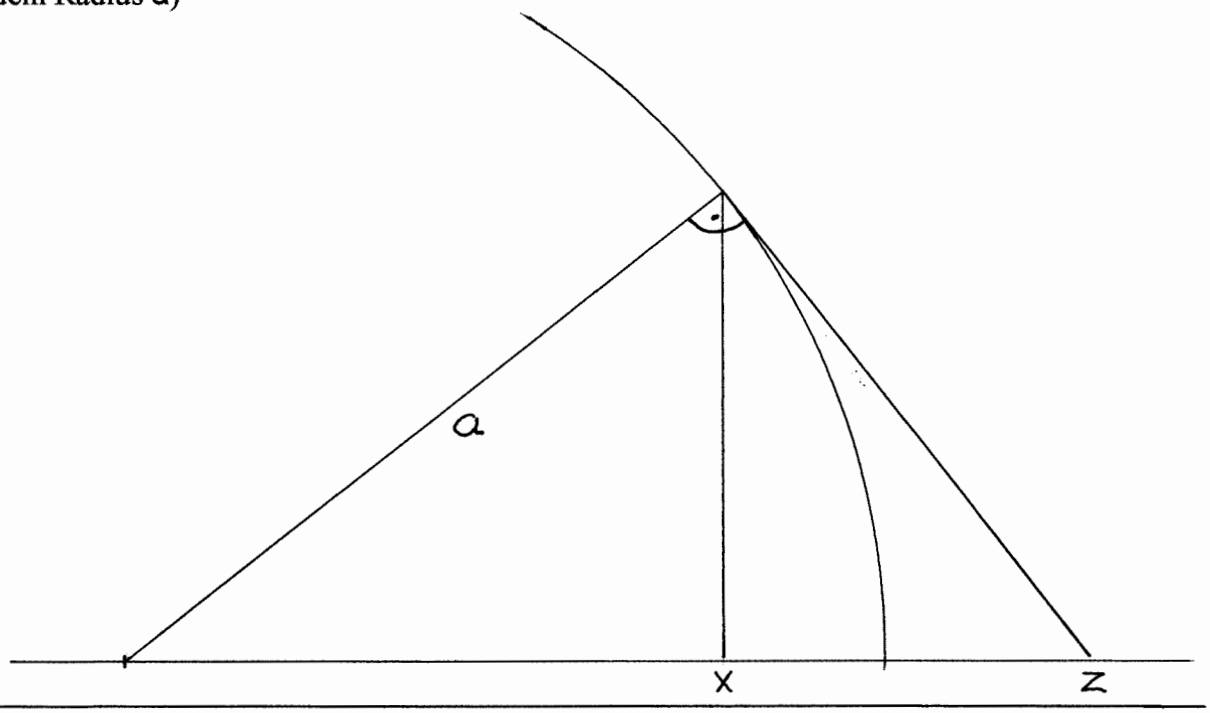
[2] Die Voraussetzung $\lambda < 1$ bedeutet keine Einschränkung. Denn sei etwa $\mu > 1$ und $z = a.\sqrt[3]{\mu}$ gesucht. Wir setzen dann $\lambda = \frac{1}{\mu}$ und konstruieren die Strecke $x = a.\sqrt[3]{\lambda}$. Mit Hilfe des Kathetensatzes ergibt sich dann

$$xz = a^2 \Rightarrow z = \frac{a^2}{x} = \frac{a^2}{a.\sqrt[3]{\lambda}} = a.\sqrt[3]{\mu}$$

[3] MENELAOS von Alexandria (um 100 n.Chr.)



Ist eine Verdopplung des Würfels gefordert, so ergäbe sich die Würfelkante $z = a.\sqrt[3]{2}$ aus $xz = a^2$, etwa durch Anwendung des Kathetensatzes (oder der Inversion an einem Kreis, mit dem Radius a)



Einschiebungen nach Walter BREIDENBACH[1]

Die bisherigen Anwendungen des Einschiebelineals wurden durch geschickte Überlegungen jeweil speziell dem vorliegenden Problem angepaßt. Ein gemeinsamer Grundgedanke liegt den behandelten Lösungen nicht zugrunde.

Wenn man auf analytischem Wege festgestellt hat, daß ein geometrisches Problem auf eine irreduzible Gleichung dritten oder vierten Grades führt, so stellt sich die Frage, wie man die zeichnerische Lösung mit einem geeigneten Zeicheninstrument, bei uns stets das Einschiebelineal, bewerkstelligen kann.

Es handelt sich also darum, die *Leitlinien* g und h, die *Einschiebestrecke* s sowie den *Pol* P der Einschiebung in geeigneter Weise festzulegen.

Ist $f(x) = 0$ die Gleichung 4.Grades, so ist es zweckmäßig, die gesuchte Nullstelle $x = \lambda$ als Punkt auf der Abszissenachse eines kartesischen Bezugssystems abzulesen.

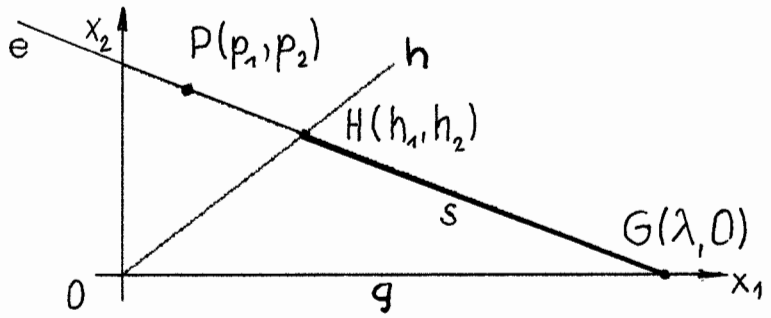
Es empfiehlt sich daher, eine der beiden Leitlinien, etwa g, in die x-Achse des Koordinatensystems, die andere, h, durch den Ursprung zu legen. Dann bleibt noch der Pol P, die zweite Leitlinie h sowie die Einschiebestrecke zu bestimmen.

Es sei

$$P(p_1, p_2) \qquad (1)$$

der Pol einer Einschiebung der Strecke s zwischen die beiden Leitlinien

$$g \ldots x_2 = 0, \quad h \ldots x_2 = k.x_1 \qquad (2),(3)$$



Ist $G(\lambda,0)$ der Schnittpunkt der Einschiebegeraden e mit der Leitlinie g, dann lautet die Gleichung der Einschiebegeraden

$$x_2 = \frac{p_2}{p_1 - \lambda}(x_1 - \lambda) \qquad (4)$$

Der Schnittpunkt H der Einschiebegeraden mit der Leitlinie h (3) ergibt sich dann mit

$$x_2 = \frac{p_2}{p_1 - \lambda}(x_1 - \lambda) = k.x_1 \Rightarrow \left(\frac{p_2}{p_1 - \lambda} - k\right)x_1 = \frac{\lambda p_2}{p_1 - \lambda} \Rightarrow \left(\frac{\lambda k + (p_2 - kp_1)}{p_1 - \lambda}\right)x_1 = \frac{\lambda p_2}{p_1 - \lambda} \Rightarrow$$

$$x_1 = \frac{\lambda p_2}{\lambda k + (p_2 - kp_1)} \text{ und } x_2 = \frac{\lambda k p_2}{\lambda k + (p_2 - kp_1)}$$

also

$$H\left(\frac{\lambda p_2}{\lambda k + (p_2 - kp_1)}, \frac{\lambda k p_2}{\lambda k + (p_2 - kp_1)}\right) \qquad (5)$$

Für die Länge der Einschiebestrecke s = GH ergibt sich

[1] BREIDENBACH W.: Der Rechte Winkel und das Einschiebelineal. Zeitschrift für mathematischen und naturwissenschaftlichen Unterricht, 56 , 4-13

$$s^2=\left[\lambda-\frac{\lambda p_2}{\lambda k+(p_2-kp_1)}\right]^2+\left[\frac{\lambda kp_2}{\lambda k+(p_2-kp_1)}\right]^2=\frac{\lambda^2[\lambda k+(p_2-kp_1)-p_2]^2+\lambda^2k^2p_2^2}{[\lambda k+(p_2-kp_1)]^2}=$$
$$=\frac{\lambda^2k^2\left[(\lambda-p_1)^2+p_2^2\right]}{[\lambda k+(p_2-kp_1)]^2}$$

somit

$$s^2=\frac{\lambda^2k^2\left[(\lambda-p_1)^2+p_2^2\right]}{[\lambda k+(p_2-kp_1)]^2} \tag{6}$$

Stellt λ die durch Einschiebung zu ermittelnde Größe dar, so wird sie durch folgende Gleichung 4.Grades dargestellt:

$$s^2[\lambda k+(p_2-kp_1)]^2=\lambda^2k^2\left[(\lambda-p_1)^2+p_2^2\right]\Rightarrow$$
$$s^2\left[\lambda^2k^2+2\lambda k(p_2-kp_1)+(p_2-kp_1)^2\right]=\lambda^2k^2\left[\lambda^2-2\lambda p_1+\left(p_1^2+p_2^2\right)\right]\Rightarrow$$
$$k^2\lambda^4-2k^2p_1\lambda^3+k^2\left[\left(p_1^2+p_2^2\right)-s^2\right]\lambda^2-2s^2k(p_2-kp_1)\lambda-s^2(p_2-kp_1)^2=0$$

Kürzung durch k^2 ergibt die Gleichung 4.Grades

$$\boxed{\lambda^4-2p_1\lambda^3+\left[\left(p_1^2+p_2^2\right)-s^2\right]\lambda^2-\frac{2s^2}{k}(p_2-kp_1)\lambda-\frac{s^2}{k^2}(p_2-kp_1)^2=0} \tag{7}$$

Vergleicht man die Gestalt von (7) mit einer allgemeinen Gleichung 4.Grades

$$\boxed{x^4+c_3x^3+c_2x^2+c_1x-c_0^2=0} \tag{8}$$

so ist ein Vergleich von (8) mit (7) ist nur möglich, wenn das konstante Glied von (8) negativ ist. (Siehe aber später die Diskussion Seite 117). Dann ergibt sich

$$c_3=-2p_1 \tag{9}$$

$$c_2=\left(p_1^2+p_2^2\right)-s^2 \tag{10}$$

$$c_1=-\frac{2s^2}{k}(p_2-kp_1) \tag{11}$$

$$c_0^2=\frac{s^2}{k^2}(p_2-kp_1)^2 \tag{12}$$

Daraus folgt

$$(9)\Rightarrow \underline{p_1=-\frac{c_3}{2}} \tag{13}$$

$$(11)\wedge(12)=\frac{c_0^2}{c_1}=-\frac{p_2-kp_1}{2k}=-\frac{p_2}{2k}+\frac{p_1}{2}\overset{(13)}{=}-\frac{p_2}{2k}-\frac{c_3}{4}\Rightarrow \underline{\frac{p_2}{2k}=-\frac{c_0^2}{c_1}-\frac{c_3}{4}} \tag{14}$$

$$(11)\Rightarrow c_1=-\frac{2s^2}{k}(p_2-kp_1)=-2s^2\left(\frac{p_2}{k}-p_1\right)\overset{(14)(13)}{=}-2s^2\left(-2\frac{c_0^2}{c_1}-\frac{c_3}{2}+\frac{c_3}{2}\right)=\frac{4s^2c_0^2}{c_1}\Rightarrow$$

$$\underline{s^2=\frac{c_1^2}{4c_0^2}} \tag{15}$$

$$(11)\wedge(15)\Rightarrow c_1=-\frac{2s^2}{k}(p_2-kp_1)=-\frac{c_1^2}{2kc_0^2}(p_2-kp_1)\Rightarrow 2kc_0^2=-c_1p_2+c_1kp_1\Rightarrow$$

$$k(2c_0^2-c_1p_1)=-c_1p_2\Rightarrow \underline{k=\frac{c_1p_2}{c_1p_1-2c_0^2}} \qquad (16)$$

$$(10)\wedge(9)\wedge(15)\Rightarrow c_2=(p_1^2+p_2^2)-s^2=\left(\frac{c_3^2}{4}+p_2^2\right)-\frac{c_1^2}{4c_0^2}\Rightarrow$$

$$\underline{p_2^2=c_2-\frac{c_3^2}{4}-\frac{c_1^2}{4c_0^2}} \qquad (17)$$

Es gilt also

$$\boxed{\begin{aligned} p_1&=-\frac{c_3}{2}\\ p_2^2&=c_2-\frac{c_3^2}{4}+\frac{c_1^2}{4c_0^2}\\ s^2&=\frac{c_1^2}{4c_0^2}\\ k&=\frac{c_1p_2}{c_1p_1-2c_0^2}\end{aligned}} \qquad (18)$$

Die Winkeldreiteilung

Setzt man $q:=\cos\alpha$ und $x:=2\cos\frac{\alpha}{3}$, so lautet die Gleichung für die Dreiteilung des Winkels (Seite 20)

$$x^3 - 3x - 2q = 0$$

Multiplikation mit $(x + \rho)$ ergibt die Gleichung 4.Grades

$$(x^3 - 3x - 2q)(x + \rho) = x^4 + \rho x^3 - 3x^2 - (2q + 3\rho)x - 2q\rho = 0$$

$x = -\rho$ entspricht dem trivialen Einschub. Setzt man zweckmäßigerweise $\rho = 2q$, so folgt

$$x^4 + 2qx^3 - 3x^2 - 8qx - 4q^2 = 0$$

Vergleich mit der allgemeinen Gleichung (18) ergibt

$$c_3 = 2q,\ c_2 = -3,\ c_1 = -8q,\ c_0^2 = 4q^2$$

Daraus ergeben sich die Koeffizienten der Einschiebegleichung

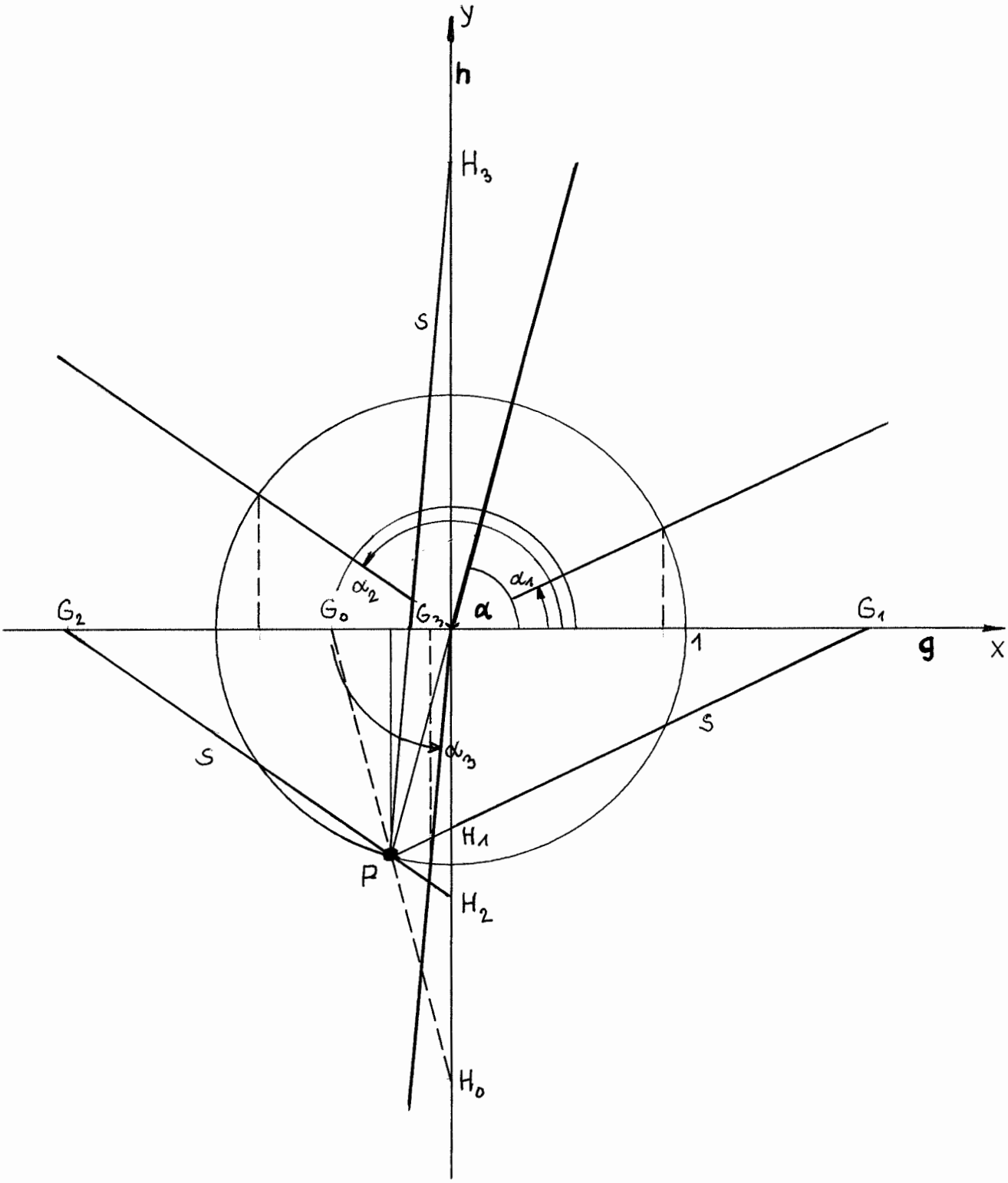
$$p_1=-\frac{c_3}{2}=-q \qquad \underline{\underline{p_1=-q=-\cos\alpha}}$$

$$p_2^2=c_2-\frac{c_3^2}{4}+\frac{c_1^2}{4c_0^2}=-3-\frac{4q^2}{4}+\frac{64q^2}{16q^2}=1-q^2 \qquad \underline{\underline{p_2=-\sqrt{1-q^2}=-\sin\alpha}}$$

$$s^2=\frac{c_1^2}{4c_0^2}=\frac{64q^2}{16q^2}=4 \qquad \underline{\underline{s=2}}$$

$$k=\frac{c_1p_2}{c_1p_1-2c_{0\,1}^2}=\frac{8q\sqrt{1-q^2}}{8q^2-8q^2}=\infty \qquad \underline{\underline{k=\infty}}$$

Beispiel: α = 75°, Einheit E = 4 cm



Das Ausziehen der 3.Wurzel

Die zu lösende Gleichung lautet

$$x^3 - \lambda = 0 \qquad 0 < \lambda < 1$$

Als trivialen Einschub wählen wir $x = -\lambda$. Dann gilt

$$(x^3 - \lambda)(x+\lambda) = x^4 + \lambda x^3 - \lambda x - \lambda^2 = 0$$

Vergleich mit (8) ergibt

$$c_3 = \lambda,\ c_2 = 0,\ c_1 = -\lambda,\ c_0^2 = \lambda^2$$

Daraus folgt für die Einschiebegleichung

$$p_1 = -\frac{c_3}{2} = -\frac{\lambda}{2} \qquad \underline{\underline{p_1 = -\frac{\lambda}{2}}}$$

$$p_2^2 = c_2 - \frac{c_3^2}{4} + \frac{c_1^2}{4c_0^2} = 0 - \frac{\lambda^2}{2} + \frac{\lambda^2}{4} + \frac{\lambda^2}{4\lambda^2} = \frac{1-\lambda^2}{4} \qquad \underline{\underline{p_2 = \frac{1}{2}\sqrt{1-\lambda^2}}}$$

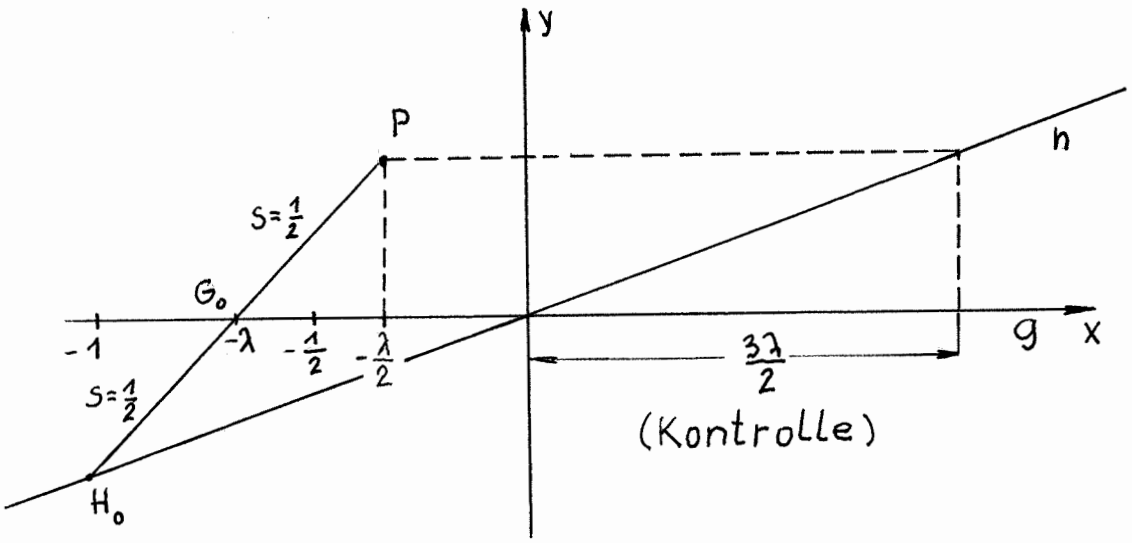
$$s^2 = \frac{c_1^2}{4c_0^2} = \frac{\lambda^2}{4\lambda^2} = \frac{1}{4} \qquad \underline{\underline{s = \frac{1}{2}}}$$

$$k = \frac{c_1 p_2}{c_1 p_1 - 2c_0^2} = \frac{(-\lambda)p_2}{(-\lambda)\left(-\frac{\lambda}{2}\right) - 2\lambda^2} = \frac{-\lambda p_2}{\frac{\lambda^2}{2} - 2\lambda^2} \qquad \underline{\underline{k = \frac{2p_2}{3\lambda}}}$$

Bei gegebener Einheitsstrecke 1 und gegebenem $\lambda < 1$ ermittelt man $P(p_1,p_2)$ und h folgendermaßen[1]: Da der triviale Einschub $x = -\lambda$ bekannt ist, kann man p_1 und p_2 auf folgende Weise konstruieren

$$p_1 = -\frac{\lambda}{2},\ p_2^2 = \frac{1}{4} - \left(\frac{\lambda}{2}\right)^2 = s^2 - \left(\frac{\lambda}{2}\right)^2,\ s = \frac{1}{2}$$

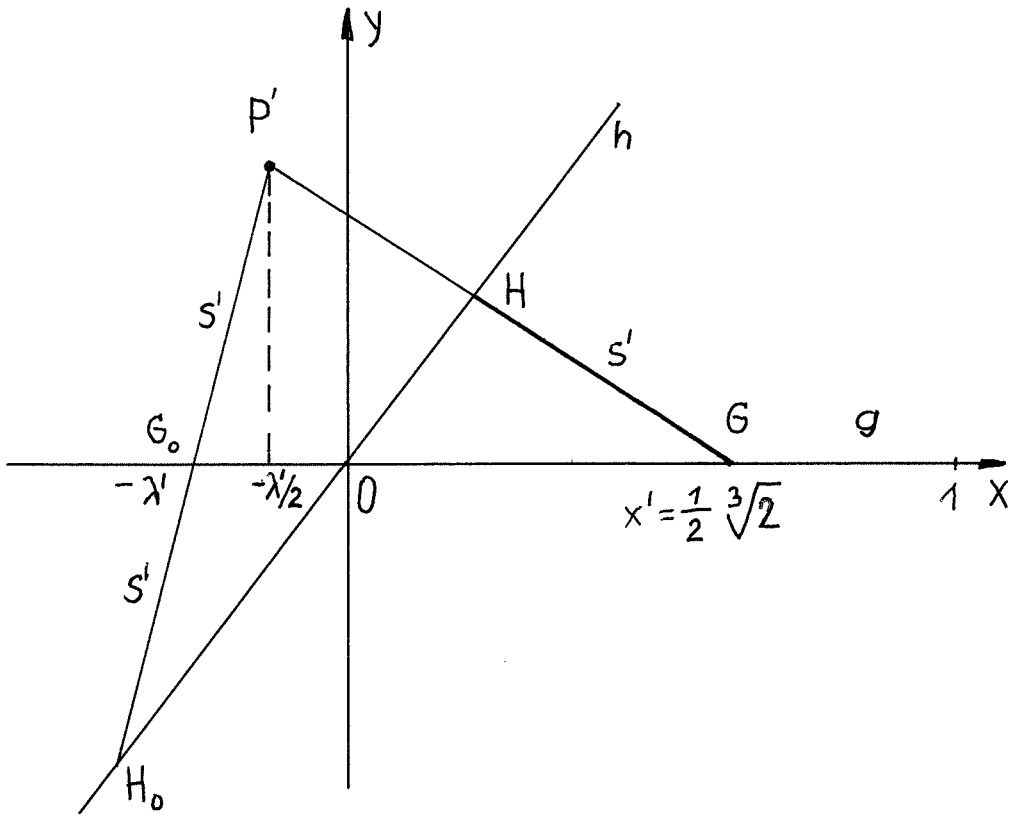
Ist P bekannt, dann kann man mit Hilfe des trivialen Einschubs einen Hilfspunkt H_0 von h konstruieren



[1] Nach George E. MARTIN: Geometric constructions, Springer, Undergraduate Texts in Mathematics, 1998, Seite 128, tritt diese Konstruktion bereits bei NIKOMEDES auf.

Beispiel: $x^3 = 2$, $\lambda = 2$. Wir setzen: (Einheit E = 8 cm)

$$x = \lambda x' \Rightarrow \lambda^3 x'^3 = 2 \Rightarrow x'^3 = \frac{2}{\lambda^3} = \frac{1}{4} =: \lambda' \Rightarrow p_1' = -\frac{\lambda'}{2} = -\frac{1}{8} \Rightarrow x = 2x'$$



Konstruktion des regelmäßigen Siebenecks

Die Kreisteilungsgleichung des Siebenecks (Seite 31)

$$z^6 + z^5 + z^4 + z^3 + z^2 + z + 1 = 0$$

reduziert sich durch die Substitution

$$x := z + \frac{1}{z} = 2\cos\alpha \qquad \alpha \text{ ist der Zentriwinkel einer Sehne des Siebenecks}$$

auf die kubische Gleichung

$$x^3 + x^2 - 2x - 1 = 0$$

Als trivialen Einschub wählen wir den Faktor (x+1), sodaß die zu lösende Gleichung die Gestalt

$$(x+1)(x^3 + x^2 - 2x - 1) = x^4 + 2x^3 - x^2 - 3x - 1 = 0$$

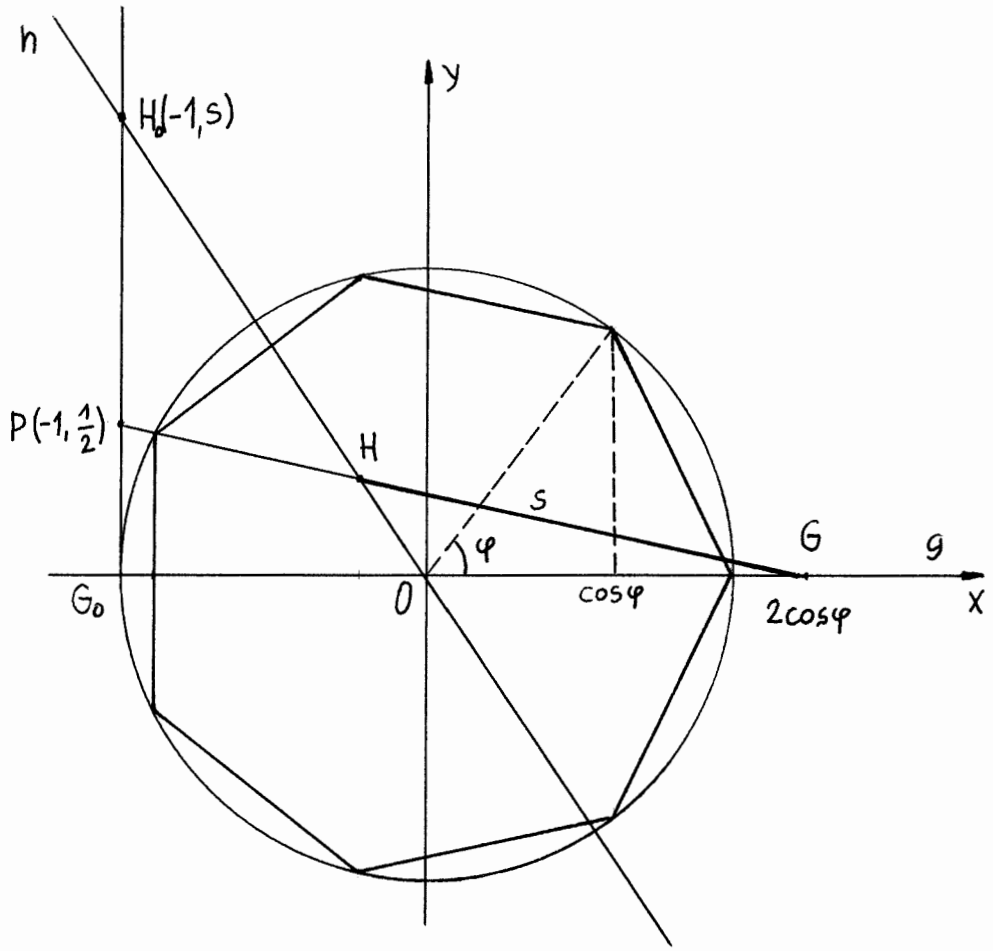
annimmt. Dann gilt

$$c_3 = 2,\ c_2 = -1,\ c_1 = -3,\ c_0^2 = 1$$

Aus (18) folgt dann

$$p_1 = -1,\ p_2 = \frac{1}{2},\ s = \frac{3}{2},\ k = -\frac{3}{2}$$

Beipiel: Einheit = 4 cm



Die Konstruktion des regelmäßigen Neunecks

Die Kreisteilungsgleichung des regelmäßigen Neunecks lautet (Seite 32)

$$z^8+z^7+z^6+z^5+z^4+z^3+z^2+z+1=(z^6+z^3+1)(z^2+z+1)$$

Der Faktor (z^2+z+1) entspricht dem im Neuneck enthaltenen gleichseitigen Dreieck. Die Substitution

$$x := z+\frac{1}{z}=2\cos\alpha$$ α ist der Zentriwinkel einer Sehne des Neunecks

führt $(z^6+z^3+1)=0$ in die kubische Gleichung

$$x^3-3x+1=0$$

über. Wählen wir $(x-1)$ als Faktor für den trivialen Einschub, so ergibt sich die Gleichung 4.Grades

$$(x^3-3x+1)(x-1)=x^4-x^3-3x^2+4x-1=0$$

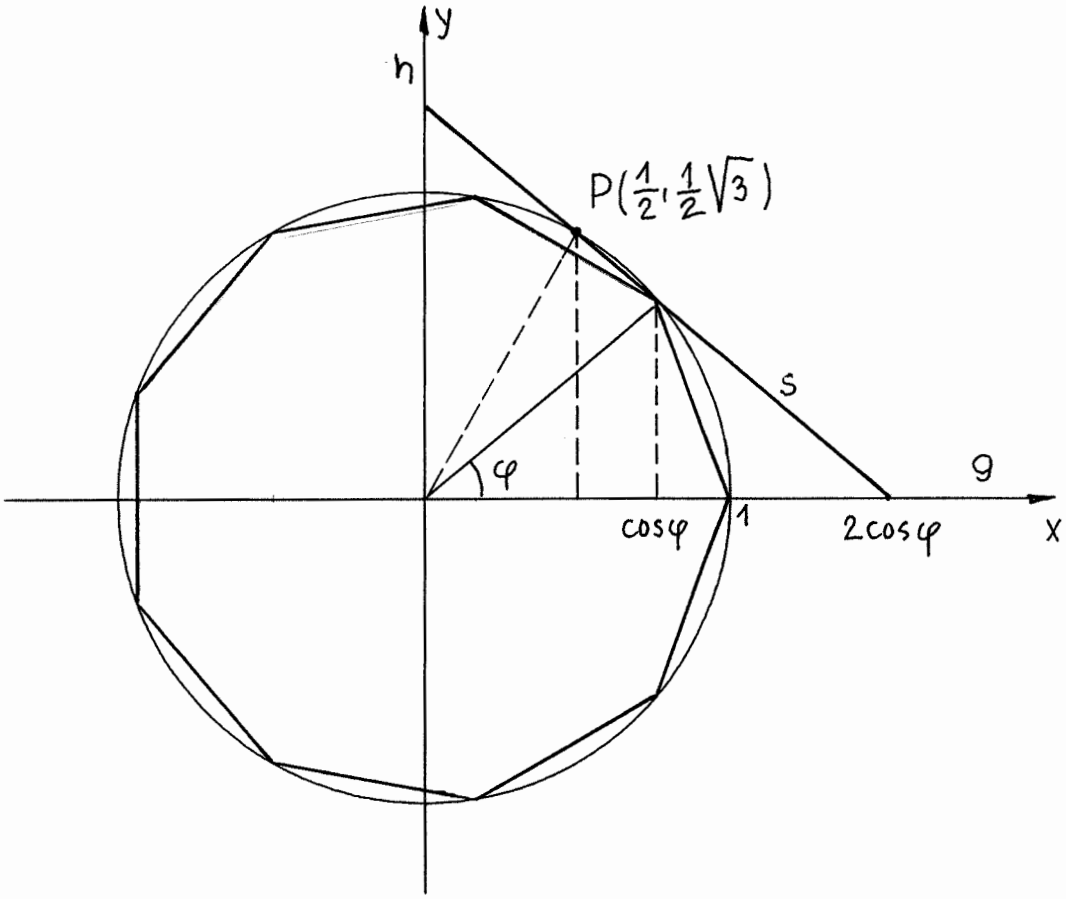
Hier ist

$$c_3=-1,\ c_2=-3,\ c_1=4,\ c_0=1$$

Daraus ergibt sich aus (18)

$$p_1=\frac{1}{2},\quad p_2=\frac{1}{2}.\sqrt{3},\quad s=2,\quad k=\infty$$

Beispiel: Einheit E = 4 cm



Konstruktion des regelmäßigen Dreizehnecks

Analytische Grundlagen

Die Kreisteilungsgleichung für das Dreizehneck lautet

$$z^{12} + z^{11} + z^{10} + z^9 + z^8 + z^7 + z^6 + z^5 + z^4 + z^3 + z^2 + z + 1 = 0$$

Ist ε eine 13.Einheitswurzel, so gilt

$$\varepsilon^{12} + \varepsilon^{11} + \ldots + \varepsilon^2 + \varepsilon + 1 = 0$$

Ist g ein Primitivrest (Seite 41) von 13, so sind auch ε^{g^i} Nullstellen der Kreisteilungsgleichung.

Nun ist g = 2 ein Primitivrest modulo 13, denn es gilt

$2^1 \equiv 2, 2^2 \equiv 4, 2^3 \equiv 8, 2^4 \equiv 3, 2^5 \equiv 6, 2^6 \equiv 12, 2^7 \equiv 11, 2^8 \equiv 9, 2^9 \equiv 5, 2^{10} \equiv 10, 2^{11} \equiv 7, 2^{12} \equiv 1$ (•)

Daher stellen die Ausdrücke ε^{g^i} nur eine andere Reihenfolge der Nullstellen ε^i dar. Somit gilt

$$\eta = \varepsilon^{2^1} + \varepsilon^{2^2} + \varepsilon^{2^3} + \varepsilon^{2^4} + \varepsilon^{2^5} + \varepsilon^{2^6} + \varepsilon^{2^7} + \varepsilon^{2^8} + \varepsilon^{2^9} + \varepsilon^{2^{10}} + \varepsilon^{2^{11}} + \varepsilon^{2^{12}} = -1$$

Wir unterteilen η in drei Summanden η_1, η_2, η_3, indem wir jeden dritten Summanden von η herausgreifen

$$\eta_1 = \varepsilon^{2^1} + \varepsilon^{2^4} + \varepsilon^{2^7} + \varepsilon^{2^{10}}$$
$$\eta_2 = \varepsilon^{2^2} + \varepsilon^{2^5} + \varepsilon^{2^8} + \varepsilon^{2^{11}}$$
$$\eta_3 = \varepsilon^{2^3} + \varepsilon^{2^6} + \varepsilon^{2^9} + \varepsilon^{2^{12}}$$

Es ist also

$$\eta = \eta_1 + \eta_2 + \eta_3 = -1$$

Weiters gilt

$$\eta_1.\eta_2 + \eta_2.\eta_3 + \eta_3.\eta_1 = \left(\varepsilon^{2^1} + \varepsilon^{2^4} + \varepsilon^{2^7} + \varepsilon^{2^{10}}\right)\left(\varepsilon^{2^2} + \varepsilon^{2^5} + \varepsilon^{2^8} + \varepsilon^{2^{11}}\right) +$$
$$+ \left(\varepsilon^{2^2} + \varepsilon^{2^5} + \varepsilon^{2^8} + \varepsilon^{2^{11}}\right)\left(\varepsilon^{2^3} + \varepsilon^{2^6} + \varepsilon^{2^9} + \varepsilon^{2^{12}}\right) +$$
$$+ \left(\varepsilon^{2^3} + \varepsilon^{2^6} + \varepsilon^{2^9} + \varepsilon^{2^{12}}\right)\left(\varepsilon^{2^1} + \varepsilon^{2^4} + \varepsilon^{2^7} + \varepsilon^{2^{10}}\right)$$

Jeder Summand besteht aus dem Produkt je zweier viergliedriger Terme, daher aus je 16 Produkten, die gesamte Summe daher aus 48 Summanden. Da es insgesamt nur zwölf ε-Potenzen gibt, muß jede Potenz viermal vorkommen, demnach

$$\eta_1.\eta_2 + \eta_2.\eta_3 + \eta_3.\eta_1 = 4.\eta = -4$$

Ferner gilt

$$\eta_1.\eta_2.\eta_3 = \left(\varepsilon^{2^1} + \varepsilon^{2^4} + \varepsilon^{2^7} + \varepsilon^{2^{10}}\right)\left(\varepsilon^{2^2} + \varepsilon^{2^5} + \varepsilon^{2^8} + \varepsilon^{2^{11}}\right)\left(\varepsilon^{2^3} + \varepsilon^{2^6} + \varepsilon^{2^9} + \varepsilon^{2^{12}}\right)$$

Da hier 3 Faktoren zu je vier Summanden auftreten, hat das Produkt 64 Summanden. Die Summe η ist daher fünfmal enthalten. Für die restlichen vier Summanden gilt wegen (•)

$$\varepsilon^{\left(2^1+2^5+2^9\right)} + \varepsilon^{\left(2^2+2^6+2^{10}\right)} + \varepsilon^{\left(2^3+2^7+2^{11}\right)} + \varepsilon^{\left(2^4+2^8+2^{12}\right)} = \varepsilon^{(2+6+5)} + \varepsilon^{(4+12+10)} + \varepsilon^{(8+11+7)} + \varepsilon^{(3+9+1)} = \varepsilon^{13} + \varepsilon^{2.13} + \varepsilon^{2.13} + \varepsilon^{13}$$

Wegen $13 \equiv 0$ (***mod*** 13) ergeben diese vier Summanden die Summe 4, sodaß gilt

$$\eta_1.\eta_2.\eta_3 = 5.\eta + 4 = -5 + 4 = -1$$

Die Größen η_1, η_2, η_3 sind daher die Nullstellen der kubischen Gleichung

$$x^3 + x^2 - 4x + 1 = 0$$

Diese Gleichung hat drei reelle Nullstellen, von denen zwei positiv und eine negativ ist.

Weiter Zerlegung der Größen η_1, η_2, η_3 ergibt

$$\eta_{11} = \varepsilon^{2^1} + \varepsilon^{2^7} \qquad \eta_{12} = \varepsilon^{2^4} + \varepsilon^{2^{10}}$$
$$\eta_{21} = \varepsilon^{2^2} + \varepsilon^{2^8} \qquad \eta_{22} = \varepsilon^{2^5} + \varepsilon^{2^{11}}$$
$$\eta_{31} = \varepsilon^{2^3} + \varepsilon^{2^9} \qquad \eta_{32} = \varepsilon^{2^6} + \varepsilon^{2^{12}}$$

Einfache Zwischenrechnungen ergeben

$$\eta_{11}\eta_{12} = \left(\varepsilon^{2^1} + \varepsilon^{2^7}\right)\left(\varepsilon^{2^4} + \varepsilon^{2^{10}}\right) = \varepsilon^{2^9} + \varepsilon^{2^6} + \varepsilon^{2^{12}} + \varepsilon^{2^3} = \eta_3$$
$$\eta_{21}\eta_{22} = \left(\varepsilon^{2^2} + \varepsilon^{2^8}\right)\left(\varepsilon^{2^5} + \varepsilon^{2^{11}}\right) = \varepsilon^{2^{10}} + \varepsilon^{2^7} + \varepsilon^{2^1} + \varepsilon^{2^4} = \eta_1$$
$$\eta_{31}\eta_{32} = \left(\varepsilon^{2^3} + \varepsilon^{2^9}\right)\left(\varepsilon^{2^6} + \varepsilon^{2^{12}}\right) = \varepsilon^{2^{11}} + \varepsilon^{2^8} + \varepsilon^{2^2} + \varepsilon^{2^5} = \eta_2$$

Daraus folgt

$$x^2 - \eta_1.x + \eta_3 \Rightarrow \eta_{11}, \eta_{12}$$
$$x^2 - \eta_2.x + \eta_1 \Rightarrow \eta_{21}, \eta_{22} \qquad (\blacklozenge)$$
$$x^2 - \eta_3.x + \eta_2 \Rightarrow \eta_{31}, \eta_{32}$$

Weitere Zerlegung ergibt

$$\eta_{111} = \varepsilon^{2^1} \quad \eta_{112} = \varepsilon^{2^7} \quad \eta_{121} = \varepsilon^{2^4} \quad \eta_{122} = \varepsilon^{2^{10}}$$
$$\eta_{211} = \varepsilon^{2^2} \quad \eta_{212} = \varepsilon^{2^8} \quad \eta_{221} = \varepsilon^{2^5} \quad \eta_{222} = \varepsilon^{2^{11}}$$
$$\eta_{311} = \varepsilon^{2^3} \quad \eta_{312} = \varepsilon^{2^9} \quad \eta_{321} = \varepsilon^{2^6} \quad \eta_{322} = \varepsilon^{2^{12}}$$

Die η_{ijk} stellen demnach die Eckpunkte des Dreizehnecks dar. Wegen

$\eta_{111} + \eta_{112} = \eta_{11}$
$\eta_{121} + \eta_{122} = \eta_{12}$
$\eta_{211} + \eta_{212} = \eta_{21}$
$\eta_{221} + \eta_{222} = \eta_{22}$
$\eta_{311} + \eta_{312} = \eta_{31}$
$\eta_{321} + \eta_{322} = \eta_{31}$

und $\eta_{111}.\eta_{112} = \eta_{121}.\eta_{122} = \eta_{211}.\eta_{212} = \eta_{221}.\eta_{222} = \eta_{311}.\eta_{312} = \eta_{321}.\eta_{322} = 1$

sind die Eckpunkte η_{ijk} (i = 1,2,3, j,k = 12) des Dreizehnecks Nullstellen der Gleichungen

$$x^2 - \eta_{ij}.x + 1 = 0$$

Sei

$$\eta_{ij1} = \boldsymbol{cos}\,(\alpha_{ij}) + \hat{\imath}.\boldsymbol{sin}(\alpha_{ij}), \quad \eta_{ij2} = \boldsymbol{cos}\,(\alpha_{ij}) - \hat{\imath}.\boldsymbol{sin}(\alpha_{ij})$$

so folgt

$$\eta_{ij1} + \eta_{ij2} = 2.\,\boldsymbol{cos}\,(\alpha_{ij}) = \eta_{ij} \Rightarrow \boldsymbol{cos}(\alpha_{ij}) = \frac{\eta_{ij}}{2}$$

Mit $x := \frac{\eta_{ij}}{2}$ ergibt sich demnach die Abszisse je zweier zur x-Achse symmetrisch liegenden Punkte des Dreizehnecks.

Ausführung der Konstruktion

Um nach BREIDENBACH die Nullstellen der Gleichung $x^3 + x^2 - 4x + 1 = 0$ zu ermitteln, führen wir (x-1) als trivialen Einschub ein. Dann gilt

$$(x^3 + x^2 - 4x + 1)\,(x - 1) = x^4 - 5x^2 + 5x - 1 = 0$$

In Formel (18) haben wir zu setzen

$$c_3 = 0,\ c_2 = -5,\ c_1 = 5,\ c_0^2 = 1$$

dann ergibt sich

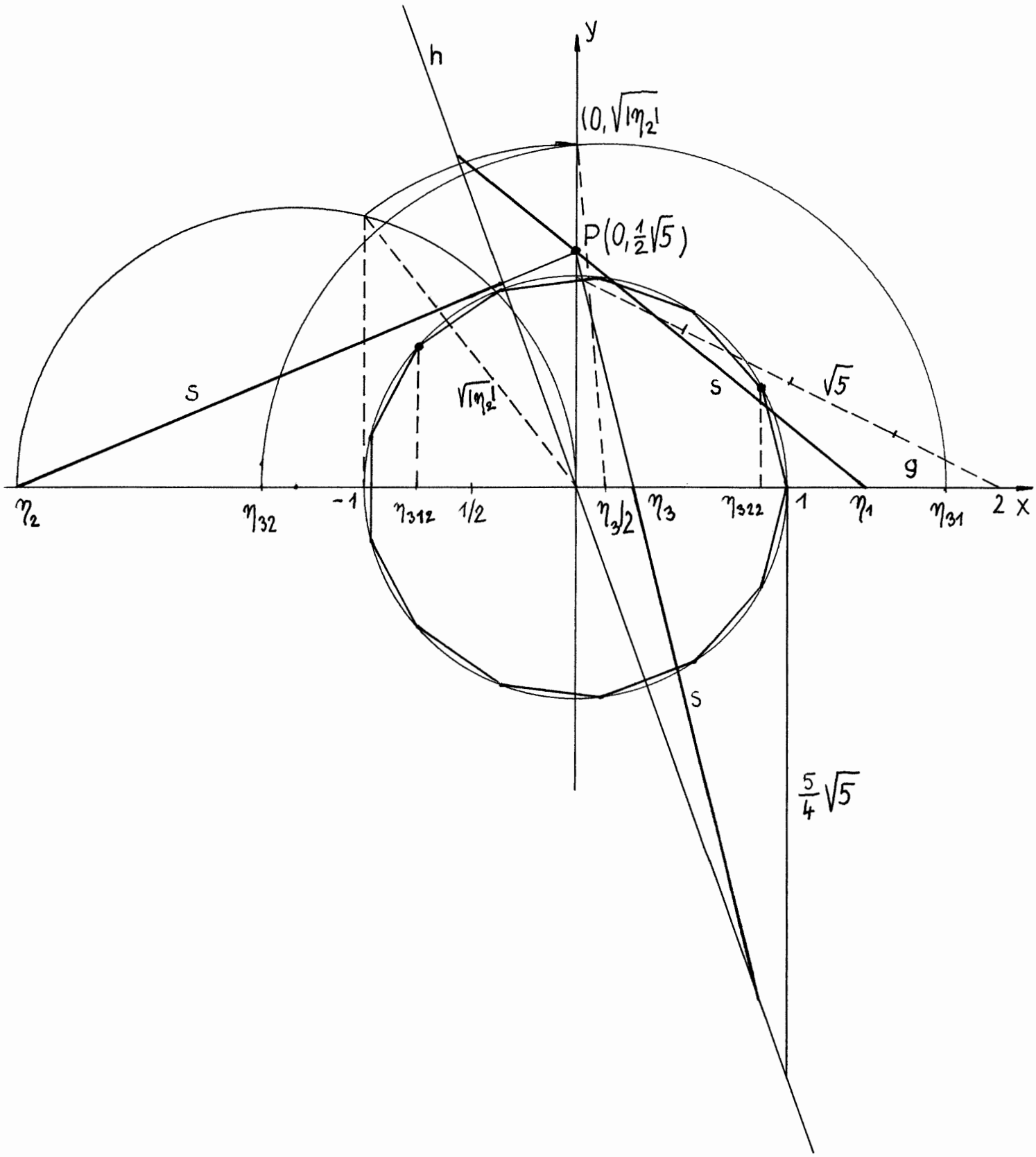
$$p_1 = 0,\ p_2 = \frac{\sqrt{5}}{2},\ s = \frac{5}{2},\ k = -\frac{5}{4}\sqrt{5}$$

Sobald die Werte $\eta_1 > 0$, $\eta_2 < 0$, $\eta_3 > 0$ durch Einschiebung ermittelt sind, können die Größen η_{ij} als Nullstellen quadratischer Gleichungen gefunden werden, wobei man unter Beachtung von (♦) je zwei η_i paaren kann.

Wir wählen (Einheit E = 4cm) η_2 und η_3 zur Konstruktion von η_{31} und η_{32}. Dann gilt

$x^2 - \eta_3.x + \eta_2 = 0 \Rightarrow x^2 - \eta_3.x - |\eta_2| = 0 \Rightarrow$

$$\eta_{31} = \frac{\eta_3}{2} + \sqrt{\left(\frac{\eta_3}{2}\right)^2 + |\eta_2|},\quad \eta_{32} = \left|\sqrt{\left(\frac{\eta_3}{2}\right)^2 + |\eta_2|} - \frac{\eta_3}{2}\right|$$


h
y
$(0, \sqrt{|\eta_2|})$
$P(0, \frac{1}{2}\sqrt{5})$
s
$\sqrt{|\eta_2|}$
s
$\sqrt{5}$
g
η_2
η_{32}
-1
η_{312}
1/2
$\eta_{3/2}$
η_3
η_{322}
1
η_1
η_{31}
2
X
s
$\frac{5}{4}\sqrt{5}$

Nach James PIERPONT läßt sich jedes regelmäßige n - Eck mit Hilfe des Einschiebelineals konstruieren, wenn $n > 2$die Gestalt

$$n = 2^i 3^j . p_1 p_2 ... p_k$$

aufweist, wobei i, j, k nichtnegative ganze Zahlen und die $p_1, \ldots, p_k$ voneinander verschiedene Primzahlen der Gestalt $2^r 3^s + 1$ sind. Primzahlen dieser Gestalt nennt man PIERPONT - Primzahlen[1]

Erweiterung der Konstruktion von BREIDENBACH zur Behandlung der allgemeinen Gleichung 4.Ordnung

Beim Versuch, die Gleichungen (18) zur graphischen Lösung *beliebiger* Gleichungen 4.Grades zu verwenden, hat man Folgendes zu beachten: Die Lösungspunkte werden als Schnittpunkte der durch die Leitlinie h, den Pol P und die Distanz s bestimmten Konchoide des NIKOMEDES mit der Geraden g gefunden. Die vier möglichen reellen Schnittpunkte der Konchoide mit g können getrennt oder zu zweien oder dreien zusammengerückt sein. In den beiden letzten Fällen ist g eine gewöhnliche oder eine Wendetangente der Konchoide (Siehe Figur auf Seite 99)

In folgenden Fällen ist die BREIDENBACHsche Konstruktion nicht anwendbar:

1. Es gibt überhaupt keine reellen Nullstellen
2. Die Gleichung hat eine vierfach zählende Nullstelle. Da die Konchoide keinen Flachpunkt besitzt, ist dieser Fall nicht behandelbar.
3. Der Fall einer doppelt zählenden und zweier konjugiert komplexen Nullstellen
4. Je zwei der vier reellen Nullstellen sind zusammengerückt

Die Fälle 2, 3 und 4 folgen aus den geometrischen Eigenschaften der Konchoide.

Ferner scheint zunächst die BREIDENBACHsche Methode nicht anwendbar, wenn das lineare Glied der Gleichung verschwindet. In diesem Falle wäre $c_1 = 0$ und nach (18) wäre $s = k = 0$ und die Geraden h und g fielen zusammen.

Natürlich entzieht sich auch der Fall eines negativen konstanten Gliedes ein reellen Konstruktion, da in diesem Falle $c_0 = i.\sqrt{c_0^2}$ zu setzen wäre, ebenso wenn die Koordinate p_2 des Poles imaginär würde.

Die letztgenannten Fälle können aber durch eine geeignete Parallelverschiebung in Richtung der x - Achse vermieden werden.

Verschiebt man nämlich die gegebene Kurve $y = x^4 + c_3 x^3 + c_2 x^2 + c_1 x - c_0^2$ (8) in x - Richtung, so muß, sofern die gegebenen Funktion überhaupt reelle Nullstellen besitzt, bei entsprechender Wahl der Schiebstrecke t ein negativer Abschnitt auf der y-Achse zu erzielen sein. Durch die Parallelverschiebung um t nimmt die Gleichung der Kurve die Gestalt an:

$$f(x-t) = (x-t)^4 + c_3(x-t)^3 + c_2(x-t)^2 + c_1(x-t) - c_0^2 =$$
$$= x^4 + (c_3 - 4t)x^3 + (c_2 - 3c_3 t + 6t^2)x^2 + (c_1 - 2c_2 t + 3c_3 t^2 - 4t^3)x - (c_0^2 + c_1 t - c_2 t^2 + c_3 t^3) =$$
$$= x^4 + a_3 x^3 + a_2 x^2 + a_1 x - a_0^2 \qquad (19)$$

und die Bestimmungsstücke der Einschiebung erhalten die Form

$$p_1 = \frac{4t - c_3}{2} \qquad (20)$$

[1] James PIERPOINT: American Mathematical Society Bulletin 2.Bd. (1895)

$$p_2 = \frac{1}{2}\sqrt{\frac{\left(\begin{array}{l}8t^6 - 12c_3t^5 + 2\left(2c_2 + 3c_3^2\right)t^4 - c3\left(4c_2 + c_3^2\right)t^3 + \left(8c_0^2 + 2c_1c_3 + c_2c_3^2\right)t^2 - \\ - c_3\left(4c_0^2 + c_1c_3\right)t + + c_0^2\left(4c_2 - c_3^2\right) + c_1^2\end{array}\right)}{-t^4 + c_3t^3 - c_2t^2 + c_1t + c_0^2}} \qquad (21)$$

$$s = \sqrt{\frac{\left(c_1 - 2c_2t + 3c_3t^2 - 4t^3\right)^2}{4\left(c_0^2 + c_1t - c_2t^2 + c_3t^3 - t^4\right)}} \qquad (22)$$

$$k(t) = \frac{4t^3 - 3c_3t^2 + 2c_2t - c_1}{12t^4 - 12c_3t^3 + \left(4c_2 + 3c_3^2\right)t^2 - 2c_2c_3t + 4c_0^2 + c_1c_3}\cdot$$

$$\cdot\sqrt{\frac{\left(\begin{array}{l}8t^6 - 12c_3t^5 + 2\left(2c_2 + 3c_3^2\right)t^4 - c3\left(4c_2 + c_3^2\right)t^3 + \left(8c_0^2 + 2c_1c_3 + c_2c_3^2\right)t^2 - \\ - c_3\left(4c_0^2 + c_1c_3\right)t + c_0^2\left(4c_2 - c_3^2\right) + c_1^2\end{array}\right)}{-t^4 + c_3t^3 - c_2t^2 + c_1t + c_0^2}} \qquad (23)$$

Elimination des Parameters t aus (21) mit Hilfe von (20) ergibt die kartesische Gleichung des *Ortes der Pole*

$$p_2(x) = \frac{3363}{9512}\sqrt{\frac{\left(\begin{array}{l}64x^6 + 16\left(8c_2 - 3c_3^2\right)x^4 + 4\left(256c_0^2 + c_3\left(64c_1 - c_3\left(16c_2 - 3c_3^2\right)\right)\right)x^2 + \\ + 256c_0^2\left(8c_2 - 3c_3^2\right) + 512c_1^2 - 64c_1c_3^2 + c_3^4\left(8c_2 - c_3^2\right)\end{array}\right)}{16x^4 + 8\left(8c_2 - 3c_3^2\right)x^2 + 16\left(c_3\left(4c_2 - c_3^2\right) - 8c_1\right) - 256c_0^2 - c_3\left(64c_1 - c_3\left(16c_2 - 3c_3^2\right)\right)}} \qquad (24)$$

Die reellen Werte für die Pole liegen zwischen den Schnittpunkten von (24) mit der x-Achse und den Asymptoten an diese Kurve.

Um die reellen Werte für die Länge der Einschiebestrecke s zu erhalten, hat man mit (20) aus (22) t zu eliminieren und findet

$$s(x) = \sqrt{-\frac{\left(4x^3 + \left(8c_2 - 3c_3^2\right)x - 8c_1 + c_3\left(4c_2 - c_3^2\right)\right)^2}{16x^4 + 8\left(8c_2 3c_3^2\right)x^2 + 16\left(c_3\left(4c_2 - c_3^2\right) - 8c_1\right)x - 256c_0^2 - c_3\left(64c_1 - c_3\left(16c_2 - 3c_3^2\right)\right)}} \qquad (25)$$

(24) und (25) lassen zusammen jenen Bereich erkennen, in welchem man auf reelle Weise den Pol P und den Anstieg k wählen kann. Nach Wahl von $x = p_1$ wird mit Hilfe von (20) die Größe der vorgenommenen Parallelverschiebung ermittelt. Die Nullstelle der ürsprünglich gegebenen Funktion hat dann den Wert x - t.

In der Praxis wird man natürlich die obigen Rechnungen nicht ausführen, sondern die Größe der Parallelverschiebung zu erraten versuchen

Beispiel:

$$f(x) = x^4 + 4x^3 + 4.8x^2 + 5.6x + 3,$$

Verschiebung um die Strecke t = 2 in x-Richtung ergibt

$$f(x-t) = x^4 - 4x^3 + 4.8x^2 + 2.4x - 5$$

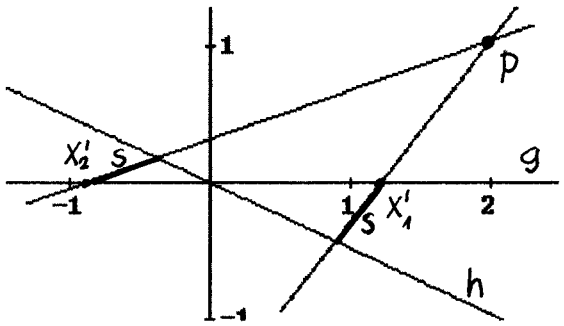
Für die verschobene Kurve gilt

$$c^3 = -4,\ c_2 = 4.8,\ c_1 = 2.4,\ c_0 = \sqrt{5}$$

Daraus folgt nach Formel (18) von Seite 108

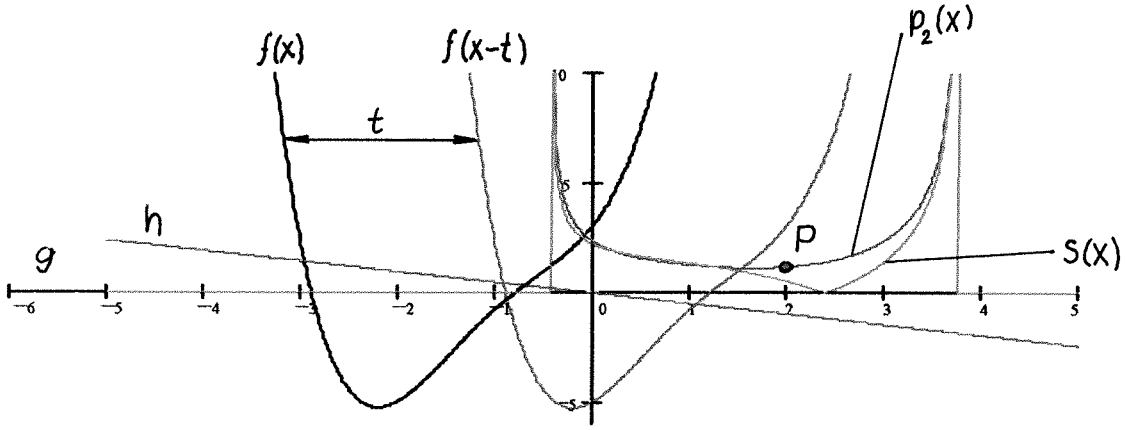
$$p_1 = 2,\ p_2 = \frac{2\sqrt{170}}{25} = 1.044,\ s = \frac{6\sqrt{5}}{25} = 0.537,\ k = -\frac{12\sqrt{170}}{325} = -0.481$$

Alle diese Werte sind im Prinzip mit Zirkel und Lineal konstruierbar.



$$x_1' = 1.21,\ x_2' = -0.88 \Rightarrow x_1 = x_1' - 2 = -0.79,\ x_2 = x_2' - 2 = -2.88$$

Die tatsächliche Anwendung obiger Rechnungen ergäbe folgendes Bild



Literatur

ADLER A: Theorie der geometrischen Konstruktionen, Göschen Leipzig, 1906

BACHMANN P.: Die Lehre von der Kreisteilung und ihre Beziehung zur Zahlentheorie. Teubner, Leipzig, 1913

BESKIN N.M - BOLTJANSKI W.G - MASLOWA G.G. - TSCHETWERUCHIN N.F. - JAGLOM I.G.: Allgemeine Prinzipien geometrischer Konstruktionen. In „Enzyklopädie der Elementarmathematik", Bd.IV: Geometrie, VEB D.Verl.d.Wiss., Berlin 1969

BEUTEL E.: Die Quadratur des Kreises. Teubner. Leipzig, 1933

BIEBERBACH L.: Theorie der geometrischen Konstruktionen. Birkhäuser, Basel 1952

BREIDENBACH W.: Die Dreitielung des Winkels, Teubner Leipzig, 1933

ENRIQUES F.: Fragen der Elementargeometrie, 2 Bde., Teubner Leipzig, 1.Bd. 1911, 2.Bd. 1907

HERRMANN A.: Das Delische Problem, Teubner Leipzig, 1927

HERTERICH K.: Dreieckskonstruktionen. Klett, Stuttgart, 1961

KLEIN F.: Vorträge über ausgewählte Fragen der Elementargeometrie. Teubner, Leipzig 1895

LEBESQUE H.: Leçons sur les constructions géométriques. Gautier-Villars, Paris 1950

MANIN J.L.: Über die Lösbarkeit von Konstruktionsaufgaben mit Zirkel und Lineal. In „Enzyklopädie der Elementarmathematik ", Bd.IV: Geometrie, VEB D.Verl.d.Wiss., Berlin 1969

MITZSCHERLING A.: Das Problem der Kreisteilung, Teubner, Leipzig, 1913

MOLENBROEK P.: Leerboek der vlakke meetkunde, Noordhoff, Groningen, 1955

PETERSEN J (= HJELMSLEV J.H.): Methoden und Theorien zuir Auflösung geometrischer Construktionsaufgaben. Host, Kopenhaben, 1879

VAHLEN Th.: Konstruktionen und Approximationen, Teubner Leipzig, 1911

Ergänzende Literatur aus Algebra und Zahlentheorie

BIEBERBACH L. - BAUER G.: Vorlesungen über Algebra. Teubner, Leipzig, 1928

CHINTSCHIN A.J.: Die Elemente der Zahlentheorie. In „Enzyklopädie der Elementarmathematik", Bd.I: Arithmetik, VEB D.Verl.d.Wiss., Berlin 1969

HLAWKA E. - SCHOISSENGEIER J.: Zahlentheorie. Manz, Wien, 1979

LUGOWSKI H. - WEINERT H.J.: Grundzüge der Algebra, 3Bde. Mathematisch - Naturwissenschaftliche Bebliothek, Bd. 9-11, Teubner, Leipzig, 1.Bd. 1966^2, 2.Bd. 1965^2, 3.Bd. 1960

MATTHIESSEN L.: Grundzüge der antiken und modernen Algebra der litteralen Gleichungen. Teubner Leipzig, 1896

NEVANLINNA F.: Einführung in die Algebra und die Theorie der algebraischen Gelcihungen. Birkhäuser, Basel, 1965

SCHOLZ A. - SCHÖNBERG B.: Einführung in die Zahlentheorie, Sammlung Göschen Bd.1131, W.d.Gruyter, Berlin 1935

STRUBECKER K.: Einführung in die höhere Mathematik. Bd.I. Grundlagen S.222-266, Oldenburg München Wien 1966^2

WINOGRADOW I.M.: Elemente der Zahlentheorie, München, 1956

Stichwortverzeichnis

Inhaltsverzeichnis

Beispiele zum Schema von Ruffini - Horner

Bestimmung des Funktionswertes eines Polynoms

$f(x) = 2x^6 - 7x^5 + 8x^4 - 17x^3 + 15x + 13$ $\quad f(3) = ?$

	2	-7	8	-17	0(!)	15	13
3		6	-3	15	-6	-18	-9
	2	-1	5	-2	-6	-3	4

$\underline{f(3) = 4}$

Division eines Polynomes durch einen linearen Ausdruck

$$\frac{f(x)}{g(x)} = \frac{5x^4 - 3x^3 + 2x^2 - 8x + 30}{x + 2}$$

	5	-3	2	-8	30
-2		-10	26	-56	128
	5	-13	28	-64	158

$$\frac{f(x)}{g(x)} = 5x^3 - 13x^2 + 28x - 64 + \frac{158}{x+2} \Rightarrow$$

$$f(x) = (5x^3 - 13x^2 + 28x - 64)(x+2) + 158$$

Nullstellen eines Polynoms

$f(x) = x^3 + 5x^2 + 8x + 6$

Als ganzzahlige Nullstellen kommen nur $\pm 1, \pm 2, \pm 3, \pm 6$ in Frage

	1	5	8	6
-3		-3	-6	-6
	1	2	2	0

Eine Nullstelle ist $\underline{x_1 = -3}$

$f(x) = (x^2 + 2x + 2)(x+3)$

Für die restlichen Nullstellen gilt

$x^2 + 2x + 2 = 0 \Rightarrow \underline{x_{2,3} = -1 \pm \sqrt{1-2} = -1 \pm i}$ . . . nicht reell

Division eines Polynoms 8.Ordnung durch ein normiertes Polynom 3.Ordnung

$$\frac{f(x)}{g(x)} = \frac{3x^8 + 2x^7 - 10x^6 + 8x^5 - 24x^4 + 8x^3 + 10x - 4}{x^3 + 2x^2 - x + 3}$$

	3	2	-10	8	-24	8	0(!)	10	-4
-2		-6	8	-2	14	-6	16		
1			3	-4	1	-7	3	-8	
-3				-9	12	-3	21	-9	24
	3	-4	1	-7	3	-8	40	-7	20

$\underline{f(x) = (3x^5 - 4x^4 + x^3 - 7x^2 + 3x - 8).\, g(x) + (40x^2 - 7x + 20)}$

Entwicklung eines Polynoms an einer gegebenen Stelle

$f(x) = x^4 - 3x^2 + x - 10$ an der Stelle $x = -1$ $(y = x + 1)$ entwickeln!

$f(x) = c_4(x+1)^4 + c_3(x+1)^3 + c_2(x+1)^2 + c_1(x+1) + c_0 = c_4y^4 + c_3y^3 + c_2y^2 + c_1y + c_0$

	1	0(!)	-3	1	-10
-1		-1	1	2	-3
	1	-1	-2	3	$-13 = c_0$
-1		-1	2	0	
	1	-2	0	$3 = c_1$	
-1		-1	3		
	1	-3	$3 = c_2$		
-1		-1 0			
	$1 = c_4$	$-4 = c_4$			

$f(x) = (x+1)^4 - 4(x+1)^3 + 3(x+1)^2 + 3(x+1) - 13 = y^4 - 4y^3 + 3y^2 + 3y - 1$

Division von Polynomen, wenn der Divisor nicht normiert ist

$$\frac{f(x)}{g(x)} = \frac{6x^5 + 13x^4 + 6x^3 - 4x^2 + 8x + 5}{3x^2 - x + 1}$$

$$f(x) = g(x).q(x) + r(x) = \left(\frac{1}{3}.g(x)\right).(3q(x)) + r(x) = \left(x^2 - \frac{1}{3}x + \frac{1}{3}\right).(3q(x)) + r(x)$$

	6	13	6	-4	8	5
1/3		2	5	3	-2	
-1/3			-2	-5	-3	2
	6	15	9	-6	3	7

$3q(x) = 6x^3 + 15x^2 + 9x - 6 \Rightarrow q(x) = 2x^3 + 5x^2 + 3x - 2$

$f(x) = g(x).(2x^3 + 5x^2 + 3x - 2) + (3x + 7)$

Darstellung eines gegebenen Polynoms n-ten Grades $f(x) = \sum_{j=0}^{n} a_j x^j$ in der Gestalt

$$f(x) = c_0 + \sum_{i=1}^{n} \prod_{k=1}^{i} c_i(x - x_k)$$

Beispiel:

$f(x) = 3x_3 - 4x_2 + 5x - 8 = c_0 + c_1(x-2) + c_2(x-2)(x+3) + c_3(x.-2)(x+3)(x+5)$

	3	-4	5	-8
2		6	4	18
	3	2	9	$10 = c_0$
-3		-9	21	
	3	-7	$30 = c_1$	
-5		-15		
	$3 = c_3$	$-22 = c_2$		

$$f(x) = f_1(x)(x-2) + c_0$$
$$f_1(x) = f_2(x)(x+3) + c_1 \mid (x-2)$$
$$f_2(x) = \underbrace{f_3(x)}_{c_3}(x+5) + c_2 \mid (x-2)(x-3)$$

$$f(x) = c_0 + c_1(x-2) + c_2(x-2)(x+3) + c_3(x-2)(x+3)(x+5)$$

$f(x) = 10 + 30.(x - 2) - 22.(x-2)(x-3) + 3(x-2)(x-3)(x-5)$

Bestimmung eines Polynoms n-ter Ordnung durch n+1 Punkte

Ein Polynom 4.Ordnung soll durch die fünf Punkte (-2|4), (-1|2), (0|-1), (2|3), (5|5) festgelegt werden. Ansatz:

$f(x) = c_4(x+2)(x+1)x(x-2) + c_3(x+2)(x+1)x + c_2(x+2)(x+1) + c_1(x+2) + c_0$

Wir setzen der Reihe nach die gegebenen Punkte ein

$f(-2) = 4 = c_0$

$f(-1) = 2 = c_1(-1+2) + c_0 = c_1 + c_0$

$f(0) = -1 = c_2(2)(1) + c(2) + c_0 = 2c_2 + 2c_1 + c_0$

$f(2) = 3 = c_3(2+2)(2+1)2 + c_2(2+2)(2+1) + c_1(2+2) + c_0 = 24c_3 + 12c_2 + 4c_1 + c_0$

$f(5) = 5 = c_4((5+2)(5+1)(5)(5-2) + c_3(5+2)(5+1)(5) + c_2(5+2)(5+1) + c_1(5+2) + c_0 =$

$= 630c_4 + 210c_3 + 42c_2 + 7c_1 + c_0$

$c_0 = 4$

$c_1 = -2$

$c_2 = -1/2$

$c_3 = 13/24$

$c_4 = -311/2520$

Daher

$$f(x) = -\frac{311}{2520}(x+2)(x+1)x(x-2) + \frac{13}{24}(x+2)(x+1)x - \frac{1}{2}(x+2)(x+1) - 2(x+2) + 4 =$$

$$= -\frac{311x^4 - 1054x^3 - 4079x^2 + 4846x + 2520}{2520}$$

Anwendung des Schemas von Ruffini - Horner zur Darstellung von Zahlen in einer gegebenen Basis

q ... gegebene Basis, z ... darzustellende Zahl,

R ... Ziffernvorrat des betrachteten Zahlsystems

$R = \{r_0 = 0, r_1 = 1, \ldots r_9 = 9, r_{10}, r_{11}, \ldots, r_{q-1}\}$

Speziell gilt für das

Zehnersystem ... R{0,1,2,3,4,5,6,7,8,9}

Binärsystem ... R{0,1}

Hexadezimalsystem ... R{0,1,2,3,4,5,6,7,8,9,A,B,C,D,E,F}

Die Darstellung der Zahl z in der Basis q lautet dann

$z = a_n q^n + a_{n-1} q^{n-1} + a_{n-2} q^{n-2} \ldots + a_1 q + a_0, \quad a_i \in R$

$z_q = a_n a_{n-1} a_{n-2} \ldots a_1 a_0$

Umrechung von $z_q = a_n a_{n-1} a_{n-2} \ldots a_1 a_0$ in die dekadische Darstellung $z_{10} := z$

	a_n	a_{n-1}	a_{n-2}	...	a_2	a_1	a_0
q		$q.b_{n-1}$	$q.b_{n-2}$	...	$q.b_2$	$q.b_1$	$q.b_0$
	b_{n-1}	b_{n-2}	b_{n-3}	...	b_1	b_0	z

☞

Umrechnung der Dezimalzahl z in die Zahl $z_q = a_n a_{n-1} a_{n-2} \ldots a_1 a_0$ mit der Basis q

In diesem Falle kennt man von obigem Schema nur die Werte z und q. Die Größen a_i sind zu bestimmen. Nun gilt

$z = q.b_0 + a_0$

$b_0 = q.b_1 + a_1$

$b_1 = q.b_2 + a_2$

.....

dh.die Größen a_i sind die sukzessiven Reste der Divisionen z:q, b_0:q, b_1:q, ... wobei für die b_i gilt

$$b_i = \left[\frac{b_{i-1}}{q}\right] \qquad (\bullet)$$

Zweckmäßigerweise stellt man das folgende Schema daher folgender-maßen dar

	a_n	a_{n-1}	a_{n-2}	...	a_2	a_1	a_0
q		$q.b_{n-1}$	$q.b_{n-2}$	...	$q.b_2$	$q.b_1$	$q.b_0$
	b_{n-1}	b_{n-2}	b_{n-3}	...	b_1	b_0	z

☜

Man bestimmt zunächst $b_0 = \left[\frac{z}{q}\right]$ und dann in der letzten Zeile sukzessiv die Größen b_i gemäß (•). Anschließend bestimmt man die a_i als Differenzen $ai = b_{i-1} - q.b_i$

Beispiele:

Binäre Zahlen

% 1100111 = z

	1	1	0	0	1	1	1
2		2	6	12	24	50	102
	1	3	6	12	25	51	z = 103

☞

215 = % z

	1	1	0	1	0	1	1	1
2		2	6	12	26	52	106	214
	1	3	6	13	26	53	107	215

☞

215 = % 11010111

Hexadezimalzahlen

$ 2B3E = z

	2	B = 11	3	E = 14
16		31	672	10800
	2	42	675	10814 =z

☞

23009 = $ z

	5	9	14 = E	11 = C
16		80	1424	23020
	5	89	1438	23009 = z

☞

23009 = § 59EC

Beipiele für Gleichungen 3.Grades

$\boxed{x^3 - 10x^2 + 35x - 44 = 0}$

$$x = y + \frac{10}{3} \Rightarrow y = x - \frac{10}{3}$$

	1	-10	35	-44
$\frac{10}{3}$		$\frac{10}{3}$	$\frac{-200}{9}$	$\frac{1150}{27}$
	1	$\frac{-20}{3}$	$\frac{115}{9}$	$\frac{-38}{27}$
$\frac{10}{3}$		$\frac{10}{3}$	$\frac{-100}{9}$	
	1	$\frac{-10}{3}$	$\frac{15}{9}$	
$\frac{10}{3}$		$\frac{10}{3}$		
	1	0		

$$y^3 + \frac{5}{3}.y - \frac{38}{27} = 0$$

Nach CARDANO gilt daher

$$x = \sqrt[3]{-b + \sqrt{b^2 + a^3}} + \sqrt[3]{-b - \sqrt{b^2 + a^3}}$$

$$a = \frac{5}{9}, \quad b = -\frac{19}{27} \Rightarrow b^2 + a^3 = \frac{361}{729} + \frac{125}{729} = \frac{486}{729} = \frac{2}{3} > 0$$

$\Rightarrow$ eine reelle, zwei k.k Nullstellen

$$y_1 = \sqrt[3]{\frac{19}{27} + \sqrt{\frac{2}{3}}} + \sqrt[3]{\frac{19}{27} - \sqrt{\frac{2}{3}}}$$

Wir untersuchen, ob sich die 3.Wurzeln algebraisch ausziehen lassen (i.a. ist dies nicht möglich). Wir treffen den Ansatz:

$$\sqrt[3]{\frac{19}{27} + \sqrt{\frac{2}{3}}} = u + \sqrt{\frac{2}{3}} \Rightarrow \frac{19}{27} + \sqrt{\frac{2}{3}} = u^3 + 3.u^2.\sqrt{\frac{2}{3}} + 3.u.\frac{2}{3} + \frac{2}{3}.\sqrt{\frac{2}{3}} = \left(u^3 + 2u\right) + \sqrt{\frac{2}{3}}.\left(3u^2 + \frac{2}{3}\right)$$

Vergleich der rationalen und irrationalen Bestandteilen auf beiden Seiten ergibt

$$1 = 3u^2 + \frac{2}{3} \Rightarrow 3u^2 = \frac{1}{3} \Rightarrow u^2 = \frac{1}{9} \Rightarrow u = \lambda.\frac{1}{3} \qquad \left(\lambda^2 = 1\right)$$

Probe:

$$\frac{19}{27} = \lambda.\left(\frac{1}{27} + \frac{2}{3}\right) = \lambda.\frac{19}{27} \Rightarrow \lambda = 1 \Rightarrow u = \frac{1}{3}$$

Also

$$\sqrt[3]{\frac{19}{27} + \sqrt{\frac{2}{3}}} = \frac{1}{3} + \sqrt{\frac{2}{3}}$$

Da sich bei der zweiten Kubikwurzel nur das Vorzeichen der Quadratwurzel ändert, gilt

Da sich bei der zweiten Kubikwurzel nur das Vorzeichen der Quadratwurzel ändert, gilt

$$\sqrt[3]{\frac{19}{27}-\sqrt{\frac{2}{3}}}=\frac{1}{3}-\sqrt{\frac{2}{3}}$$

Daher

$$y_1=\left(\frac{1}{3}+\sqrt{\frac{2}{3}}\right)+\left(\frac{1}{3}-\sqrt{\frac{2}{3}}\right)=\frac{2}{3}\Rightarrow x_1=y_1+\frac{10}{3}=\frac{2}{3}+\frac{10}{3}=\frac{12}{3}=\underline{\underline{4=x_1}}$$

Die beiden restlichem k.k. Nullstellen sind Lösungen eine quadratischen Gleichung, die sich nach Horner ergibt

	1	-10	35	-44
4		4	-14	44
	1	-6	11	0

$$x^2-6x+11=0\Rightarrow \underline{\underline{x_{2,3}=3\pm\sqrt{9-11}=3\pm i.\sqrt{2}}}$$

$\boxed{x^3+6x^2-x-30=0}$

$x=y-2\Rightarrow y=x+2$

	1	6	-1	-30
-2		-2	-8	18
	1	4	-9	-12
-2		-2	-4	
	1	2	-13	
-2		-2		
	1	0		

$\underline{y^3-13y-12=0}$

$$a=-\frac{13}{3},\quad b=-6\Rightarrow a^3+b^2=-\frac{2197}{27}+36=-\frac{1225}{27}<0\Rightarrow 3 \text{ relle Nullstellen}$$

Wir wenden daher die trigonometrische Auflösung an

$$r^2=-4a=26\Rightarrow r=\sqrt{26}$$

$$cos(3\alpha)=-\frac{8b}{r^3}=\frac{18\sqrt{39}}{169}\Rightarrow 3\alpha=48{,}3063\Rightarrow \alpha=16{,}1021$$

$$y_1=r.cos(\alpha)=4$$

$$y_2=r.cos(\alpha+120)=-3$$

$$y_3=r.cos(\alpha+240)=-1$$

Daher

$\underline{x_1=y_1-2=2,\ x_2=y_2-2=-5,\ x_3=y_3-2=-3}$

BEISPIEL zum SATZ von F E R M A T für p = 13

es muß für $1 \leq x \leq 12$ gelten

$$x^{12} \equiv 1 \pmod{13}$$

Ordnung	
1	$1^1 \equiv 1$
(12)	$\underline{2}^1 \equiv 2,\ 2^2 \equiv 4,\ 2^3 \equiv 8,\ 2^4 \equiv 3,\ 2^5 \equiv 6,\ 2^6 \equiv 12,\ 2^8 \equiv 9,$ $2^9 \equiv 5,\ 2^{10} \equiv 10,\ 2^{11} \equiv 7,\ 2^{12} \equiv 1$
3	$3^1 \equiv 3,\ 3^2 \equiv 9,\ 3^3 \equiv 1$
6	$4^1 \equiv 4,\ 4^1 \equiv 3,\ 4^3 \equiv 12,\ 4^4 \equiv 9,\ 4^5 \equiv 10,\ 4^6 \equiv 1$
4	$5^1 \equiv 5,\ 5^2 \equiv 12,\ 5^3 \equiv 8,\ 5^4 \equiv 1$
(12)	$\underline{6}^1 \equiv 6,\ 6^2 \equiv 10,\ 6^3 \equiv 8,\ 6,^4 \equiv 9,\ 6^5 \equiv 2,\ 6^6 \equiv 7,\ 6^8 \equiv 3,$ $6^9 \equiv 5,\ 6^{10} \equiv 4,\ 6^{11} \equiv 11,\ 6^{12} \equiv 1$
(12)	$7^1 \equiv 7,\ 7^2 \equiv 10,\ 7^3 \equiv 5,\ 7^4 \equiv 9,\ 7^5 \equiv 11,\ 7^6 \equiv 12,\ 7^7 \equiv 6,$ $7^8 \equiv 3,\ 7^9 \equiv 8,\ 7^{10} \equiv 4,\ 7^{11} \equiv 2,\ 7^{12} \equiv 1$
4	$8^1 \equiv 8,\ 8^2 \equiv 12,\ 8^3 \equiv 5,\ 8^4 \equiv 1$
3	$9^1 \equiv 9,\ 9^2 \equiv 3,\ 9^3 \equiv 1$
6	$10^1 \equiv 10,\ 10^2 \equiv 9,\ 10^3 \equiv 12,\ 10^4 \equiv 3,\ 10^5 \equiv 4,\ 10^6 \equiv 1$
(12)	$\underline{11}^1 \equiv 11,\ 11^2 \equiv 4,\ 11^3 \equiv 5,\ 11^4 \equiv 3,\ 11^5 \equiv 7,\ 11^8 \equiv 2.$ $11^9 \equiv 8,\ 11^{10} \equiv 10,\ 11^{11} \equiv 6,\ 11^{12} \equiv 1$
2	$12^1 \equiv 12,\ 12^2 \equiv 1$

BEISPIEL zum SATZ von F E R M A T für p = 17

Es muß für $1 \leq x \leq 16$ gelten

$$x^{16} \equiv 1 \pmod{17}$$

Ordnung	
1	$1^1 \equiv 1$
8	$2^1 \equiv 2,\ 2^2 \equiv 4,\ 2^3 \equiv 8,\ 2^4 \equiv 16,\ 2^5 \equiv 15,\ 2^6 \equiv 13,\ 2^7 \equiv 9,$ $2^8 \equiv 1,$
(16)	$\underline{3}^1 \equiv 3,\ 3^2 \equiv 9,\ 3^3 \equiv 10,\ 3^4 \equiv 13,\ 3^5 \equiv 5,\ 3^6 \equiv 15,\ 3^7 \equiv 11,$ $3^8 \equiv 16,\ 3^9 \equiv 14,\ 3^{10} \equiv 8,\ 3^{11} \equiv 7,\ 3^{12} \equiv 4,\ 3^{13} \equiv 12,$ $3^{14} \equiv 2,\ 3^{15} \equiv 6,\ 3^{16} \equiv 1$
4	$4^1 \equiv 4,\ 4^2 \equiv 16,\ 4^3 \equiv 13,\ 4^4 \equiv 1$
(16)	$\underline{5}^1 \equiv 5,\ 5^2 \equiv 8,\ 5^3 \equiv 6,\ 5^4 \equiv 13,\ 5^5 \equiv 14,\ 5^6 \equiv 2,\ 5^7 \equiv 10,$ $5^8 \equiv 16,\ 5^9 \equiv 12,\ 5^{10} \equiv 9,\ 5^{11} \equiv 11,\ 5^{12} \equiv 4,\ 5^{13} \equiv 3,$ $5^{14} \equiv 15,\ 5^{15} \equiv 7,\ 5^{16} \equiv 1$
(16)	$\underline{6}^1 \equiv 6,\ 6^2 \equiv 2,\ 6^3 \equiv 12,\ 6^4 \equiv 4,\ 6^5 \equiv 7,\ 6^6 \equiv 8,\ 6^7 \equiv 14,$ $6^8 \equiv 16,\ 6^9 \equiv 11,\ 6^{10} \equiv 15,\ 6^{11} \equiv 5,\ 6^{12} \equiv 13,\ 6^{13} \equiv 10,$ $6^{14} \equiv 9,\ 6^{15} \equiv 3,\ 6^{16} \equiv 1$
(16)	$\underline{7}^1 \equiv 7,\ 7^2 \equiv 15,\ 7^3 \equiv 3,\ 7^4 \equiv 4,\ 7^5 \equiv 11,\ 7^6 \equiv 9,\ 7^7 \equiv 12,$ $7^8 \equiv 16,\ 7^9 \equiv 9,\ 7^{10} \equiv 2,\ 7^{11} \equiv 14,\ 7^{12} \equiv 13,\ 7^{13} \equiv 6,$ $7^{14} \equiv 8,\ 7^{15} \equiv 5,\ 7^{16} \equiv 1$
8	$8^1 \equiv 8,\ 8^2 \equiv 13,\ 8^3 \equiv 2,\ 8^4 \equiv 16,\ 8^5 \equiv 9,\ 8^6 \equiv 4,\ 8^7 \equiv 15,$ $8^8 \equiv 1$
8	$9^1 \equiv 9,\ 9^2 \equiv 13,\ 9^3 \equiv 15,\ 9^4 \equiv 16,\ 9^5 \equiv 8,\ 9^6 \equiv 4,\ 9^7 \equiv 2,$ $9^8 \equiv 1$
(16)	$10^1 \equiv 10,\ 10^2 \equiv 15,\ 10^3 \equiv 14,\ 10^4 \equiv 4,\ 10^5 \equiv 6,\ 10^6 \equiv 9,$ $10^7 \equiv 5,\ 10^8 \equiv 16,\ 10^9 \equiv 7,\ 10^{10} \equiv 2,\ 10^{11} \equiv 3,\ 10^{12} \equiv 13,$ $10^{13} \equiv 11,\ 10^{14} \equiv 8,\ 10^{15} \equiv 12,\ 10^{16} \equiv 1$
(16)	$\underline{11}^1 \equiv 11,\ 11^2 \equiv 2,\ 11^3 \equiv 5,\ 11^4 \equiv 4,\ 11^5 \equiv 10,\ 11^6 \equiv 8,$ $11^7 \equiv 3,\ 11^8 \equiv 16,\ 11^9 \equiv 6,\ 11^{10} \equiv 15,\ 11^{11} \equiv 12,\ 11^{12} \equiv 13,$ $11^{13} \equiv 7,\ 11^{14} \equiv 9,\ 11^{15} \equiv 14,\ 11^{16} \equiv 1$

Ordnung

⑯ $\underline{12}^1 \equiv 12,\ 12^2 \equiv 8,\ 12^3 \equiv 11,\ 12^4 \equiv 13,\ 12^5 \equiv 3,\ 12^6 \equiv 2,$
$12^7 \equiv 7,\ 12^8 \equiv 16,\ 12^9 \equiv 5,\ 12^{10} \equiv 9,\ 12^{11} \equiv 6,\ 12^{12} \equiv 4,$
$12^{13} \equiv 14,\ 12^{14} \equiv 15,\ 12^{15} \equiv 10,\ 12^{16} \equiv 1$

4 $13^1 \equiv 13,\ 13^2 \equiv 16,\ 13^3 \equiv 4,\ 13^4 \equiv 1$

⑯ $\underline{14}^1 \equiv 14,\ 14^2 \equiv 9,\ 14^3 \equiv 7,\ 14^4 \equiv 13,\ 14^5 \equiv 12,\ 14^6 \equiv 15,$
$14^7 \equiv 6,\ 14^8 \equiv 16,\ 14^9 \equiv 3,\ 14^{10} \equiv 8,\ 14^{11} \equiv 10,\ 14^{12} \equiv 4,$
$14^{13} \equiv 5,\ 14^{14} \equiv 2,\ 14^{15} \equiv 11,\ 14^{16} \equiv 1$

8 $15^1 \equiv 15,\ 15^2 \equiv 4,\ 15^3 \equiv 9,\ 15^4 \equiv 16,\ 15^5 \equiv 2,\ 15^6 \equiv 13,$
$15^7 \equiv 8,\ 15^8 \equiv 1$

2 $16^1 \equiv 16,\ 16^2 \equiv 1$

Anwendung der Methode von KRONECKER

Beispiel: Das Polynom

$$f(x) = 2x^5 + x^4 - 4x^3 - x^2 + 1 = (px^2 + qx + r).h(x)$$

soll auf irreduzible quadratische Faktoren über $\mathbb{Q}$ untersucht werden. Man überzeugt sich leicht, daß f(x) keine rationalen NSTen hat.

Wir berechnen die Werte von $f(x_0)$, $f(x_1)$, $f(x_2)$ für $x_0 = 0$, $x_1 = 1$, $x_2 = -1$. Es gilt

$f(0) = 1$ Teiler $g(0) = \pm 1$

$f(1) = -1$ Teiler $g(1) = \pm 1$

$f(-1) = 3$ Teiler $g(-1) = \pm 1, \pm 3$

Wir haben also die ganzzahligen Lösungen des Gleichungssystems

$x_0 = 0$ $\quad r = \pm 1$

$x_1 = 1$ $\quad p + q + r = \pm 1$

$x_2 = -1$ $\quad p - q + r = \pm 1, \pm 3$

zu suchen. Das GAUSSsche Schema lautet

	p	q	r									
⇒	0	0	1	1	1	1	1	1	1	1	-1	Dieser Teil kann
	1	1	1	1	1	1	1	-1	-1	-1	-1	1	weggelassen werden,
	1	-1	1	1	-1	3	-3	1	-1	3	-3	1	da mit ihm nur die
	1	1	0	0	0	0	0	-2	-2	-2	-2		Größen -p, -q, -r
⇒	1	-1	0	0	-2	2	-4	0	-2	2	-4		berechnet würden.
	0	0	1	1	1	1	1	1	1	1	1		
:2	2	0	0	0	-2	2	-4	-2	-4	0	-6		
	1	-1	0	0	-2	2	-4	0	-2	2	-4		
	0	0	1	1	1	1	1	1	1	1	1		
⇒	1	0	0	0	-1	1	-2	-1	-2	0	-3		
	1	-1	0	0	-2	2	-4	0	-2	2	-4		
	0	0	1	1	1	1	1	1	1	1	1		
	1	0	0	0	-1	1	-2	-1	-2	0	-3		
	0	+1	0	0	+1	-1	+2	-1	0	-2	+1		
	0	0	1	1	1	1	1	1	1	1	1		

Es gibt also folgende Möglichkeiten

$g(x) =$ $\quad 1$ . . . unbrauchbar (Konstante!)

$-x^2 + x + 1$

$x^2 - x + 1$

$-2x^2 + 2x + 1$

$-x^2 - x + 1$

$-2x + 1$ . . . unbrauchbar (Linearfaktor!)

"Die Theorie der geometrischen Konstruktionen" (Prof.W.STRÖHER)
Einlageblatt Nr.6

LITERATUR ZUR THEORIE DER GEOMETRISCHEN KONSTRUKTIONEN

A.ADLER: Theorie der geometrischen Konstruktionen,
Göschen, Leipzig, 1906

P.BACHMANN: Die Lehre von der Kreisteilung und ihre Beziehung zur Zahlentheorie,
Teubner, Leipzig, 1872

E.BEUTEL: Die Quadratur des Kreises,
Teubner, Leipzig, 1913

L.BIEBERBACHER: Theorie der geometrischen Konstruktionen,
Birkhäuser, Basel, 1952

W.BREIDENBACH: Die Dreiteilung des Winkels,
Teubner, Leipzig, 1933

F.ENRIQUES: Fragen der Elementargeometrie 2 Bde.
Teubner, Leipzig, 1 Bd.1911, 2 Bd.1907

A.HERRMANN. Das Delische Problem,
Teubner, Leipzig, 1927

F.KLEIN: Vorträge über ausgewählte Fragen der Elementargeometrie,
Teubner, Leipzig, 1895

H.LEBESGUE: Lecons sur les constructions géométriques,
Gauthier-Villars, Paris, 1950

A.MITZSCHERLING: Das Problem der Kreisteilung,
Teubner, Leipzig, 1913

P.MOLENBROEK: Leerboek der vlakke meetkunde,
Noordhoff, Groningen, 1955

J.PETERSEN: Methoden und Theorien zur Auflösung geometrischer Construktionsaufgaben,
Høst, Kopenhagen, 1879

A.QUEMPER DE LANASCOL: Géométrie du compas,
Beauchard, Paris, 1925

Th.VAHLEN: Konstruktionen und Approcimationen,
Teubner, Leipzig, 1911

S.C.van VEEN: Passermeetkunde,
Noorduijn, Groningen, 1951

K.HERTERICH: Dreieckskonstruktionen,
Klett, Stuttgart, 1961

M.CLEYET-MICHAUD: Le nombre d'or(Sammlung Que sais-je?)
Presses Universitaires de France 1975

Literaturliste zur Vorlesung

"Theorie der geometrischen Konstruktionen"

Prof.W.STRÖHER

ADLER A: Theorie der geometrischen Konstruktionen, Göschen, Leipzig , 1906

BACHMANN P.: Die Lehre von der Kreisteilung und ihre Beziehung zur Zahlentheorie. Teubner, Leipzig, 1872

BESKIN N.M.-BOLTJANSKI W.G.-MASLOWA G.G.-TSCHETWERUCHIN N.F.-JAGLOM I.G.: Allgemeine Prinzipien geometrischer Konstruktionen. in "Enzyklopädie der Elementarmathematik", Bd.IV: Geometrie, VEB D.Verl.d.Wiss. Berlin, 1969

BEUTEL E. : Die Quadratur des Kreises. Teubner, Leipzig, 1913

BIEBERBACH L.: Theorie der geometrischen Konstruktionen. Birkhäuser, Basel, 1952

BREIDENBACH W.: Die Dreiteilung des Winkels, Teubner Leipzig, 1933

ENRIQUES F.: Fragen der Elementargeometrie, 2 Bde., Teubner, Leipzig, 1.Bd. 1911, 2.Bd. 1907

HERRMANN A.: Das Delische Problem, Teubner, Leipzig, 1927

HERTERICH K. Dreieckskonstruktionen, Klett, Stuttgart, 1961

KLEIN F.: Vorträge über ausgewählte Fragen der Elementargeometrie, Teubner Leipzig, 1895

LEBESGUE H.: Leçons sur les constructions géométriques, Gauthier-Villars, Paris, 1950

MANIN J.L.: Über die Lösbarkeit von Konstruktionsaufgaben mit Zirkel und Lineal. In "Enzyklopädie der Elementarmathematik2, Bd.IV: Geometrie, VEB D.Verl.d.Wiss., Berlin, 1969

MASCHERONI L.: Geometria del compasso, Pavia, 1797

MASCHERONI L.: Gebrauch des Zirkels (Übersetzung ins Deutsche), Schlesinger, Berlin, 1825

MITZSCHERLING A.: Das Problem der Kreisteilung. Teubner, Leipzig, 1913

MOHR G.: Euclides Danicus, Amsterdam, 1672, Herausgegeben von J. HJELMSLEV, Kopenhagen, 1928

MOLENBROEK P.: Leerboek der vlakke meetkunde, Noordhoff, Groningen, 1955

PETERSEN J. (= J.HJELMSLEV): Methoden und Theorien zur Auflösung geometrischer Construktionsaufgaben. Host, Kopenhagen, 1879

QUEMPER de LANASCOL A.: Géométrie du compas, Beauchard, Paris, 1925

VAHLEN Th.: Konstruktionen und Approximationen, Teubner, Leipzig, 1911

VEEN van S.C.: Passermeetkunde. Noorduijn, Groningen, 1951

Ergänzende Literatur aus Algebra und Zahlentheorie

BIEBERBACH L.-BAUER G.: Vorlesungen über Algebra, Teubner, Leipzig, 1928

CHINTSCHIN A.J.: Die Elemente der Zahlentheorie. In "Enzyklopädie der Elementarmathematik", Bd.I: Arithmetik, VEB D.Verl.d.Wiss., Berlin, 1967

HLAWKA E.-SCHOISSENGEIER J.: Zahlentheorie, Manz, Wien, 1979

LUGOWSKI H.-WEINERT H.J.: Grundzüge der Algebra, 3 Bde., Mathematisch-Naturwissenschaftliche Bibliothek, Bd.p-11, Teubner, Leipzig, 1.Bd.(3.Aufl.) 1966, ".Bd.(2.Aufl.) 1965, 3.Bd. 1960

MATTHIESSEN L.: Grundzüge der antiken und modernen Algebra der litteralen Gleichungen, Teubner, Leipzig, 1896

NEVANLINNA F.: Einführung in die Algebra und die Theorie der algebraischen Gleichungen. Birkhäuser, Basel, 1965

SCHOLZ A.-SCHÖNEBERG B.: Einführung in die Zahlentheorie, Sammlung Göschen Bd.1131, W.d.Gruyter, Berlin, 1935

STRUBECKER K:: Einführung in die höhere Mathematik. Band I: Grundlagen S 222-266, Oldenbourg München Wien 2.Aufl. 1966

WINOGRADOW I.M.: Elemente der Zahlentheorie, München, 1956