Bernold Fiedler 11.5.2009

Notiz: Konstruktion regulärer n-Ecke

Aufgabe: Konstruiere die Eckpunkte z des regulären n-Ecks auf dem Einheitskreis, mit Zirkel & Lineal.

Kepler (1619): n-Eck konstruierbar $\Leftrightarrow$
(ein wenig falsch) $n = 2^m p, \quad p \in \{1, 3, 5, 15\}$.

Gauss (1796): $n = 17$ konstruierbar.

(1801): $n = 2^m p_1 \cdot \ldots \cdot p_r$ konstruierbar, falls p_i verschiedene Fermat-Primzahlen sind.

Def.: Fermat-Primzahlen sind Primzahlen F_k der Form

(1) $$F_k := 2^{(2^k)} + 1, \qquad k = 0, 1, 2, \ldots.$$

Bem.: $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65537$ sind die einzigen heute bekannten Fermat-Primzahlen F_k. ~~die prim sind~~ Die Zahlen $F_5, \ldots, F_{11}$ sind nicht prim. Es ist nicht bekannt, ob es weitere Fermat-Primzahlen gibt.

Satz [Gauss (1801), Wantzel (1837)]

n-Eck konstruierbar $\Longleftrightarrow$

$n = 2^m p_1 \cdot \ldots \cdot p_r$ mit verschiedenen Fermat-Primzahlen p_i.

Beweis:

Der Beweis benutzt Galois-Theorie, wie sie in Büchern mit dem Titel "Algebra" steht. Idee: Ecken (z) des n-Ecks lösen

(2) $$0 = z^n - 1 = \prod_{d \text{ teilt } n} Q_d(z)$$

mit $z \in \mathbb{C}$. Die (über $\mathbb{Q}$) irreduziblen Polynome $Q_d = z^{\varphi(d)} + \ldots$ vom Grad $\varphi(d)$ heißen ganzzahlige Koeffizienten und Kreisteilungs-Polynome; sie haben Grade

(3) $\varphi(d)$ = Anzahl der zu d teilerfremden (kleiner als) natürlichen Zahlen $\leq d$ =

= "Eulersche φ-Funktion" =

= "Euler totient function" =

$= 2^{\alpha_0 - 1} q_1^{\alpha_1 - 1} \cdot \ldots \cdot q_\ell^{\alpha_\ell - 1} \cdot (q_1 - 1) \cdot \ldots \cdot (q_\ell - 1)$, wenn

$d = 2^{\alpha_0} q_1^{\alpha_1} \cdot \ldots \cdot q_\ell^{\alpha_\ell}$ die Primfaktor-Zerlegung von d ist; Faktoren mit $\alpha_i = 0$ werden weggelassen, q_i ungerade.

[Beispiel: $\varphi(p) = p-1$ für p prim.
$Q_d(z) = \prod (z - \zeta^k)$, $\zeta := \exp(2\pi i/d)$, k teilerfremd zu d]

Galois-Theorie besagt, dass Nullstellen z der $\mathbb{Q}$-irreduziblen Polynome $Q_d(z)$ aus der gegebenen Strecke 1 (hier: Radius des umbeschriebenen Einheitskreises) konstruierbar sind, genau dann, wenn der Grad von Q_d eine Potenz von 2 ist.(*)$_1$ Dabei ist die Grundidee, dass per Lineal Operationen zum Körper $\mathbb{Q}$ ausgeführt werden können. Der Zirkel aber kann quadratische Gleichungen lösen, weil mit a auch $\sqrt{a}$ als Diagonale des Quadrats mit Seite a konstruierbar ist. Sukzessive "Quadraturen" dieser Art erlauben die Auflösung irreduzibler Polynome vom Grad $2 \cdot 2 \cdot \ldots \cdot 2$.(*)$_2$

(*)$_1$ Die Galois-Gruppen der Q_d sind zyklisch.

(*)$_2$ Die Lösungen von $Q_d(z) = 0$ werden durch sukzessive Wurzelbildungen $\pm\sqrt{a}$ konstruiert, die jeweils nichts weiter als eine Verdopplung des Polynomgrades erlauben.

Also ist die Gleichung $z^n - 1 = 0$ per Zirkel und Lineal auflösbar genau dann, wenn

(4) $\varphi(d) = \mathrm{Grad}(Q_d) = 2^\mu$

für alle d und geeignete μ gilt. Sei

(5) $$n = 2^m p_1^{m_1} \cdot \ldots \cdot p_\ell^{m_\ell}$$

die Primfaktorzerlegung von n, und

(6) $$d = 2^{\alpha_0} q_1^{\alpha_1} \cdot \ldots \cdot q_\ell^{\alpha_\ell}$$

die ~~von~~ des Teilers d von n. Dann gilt $q_i = p_i$ und $\alpha_i \leq m_i$. Wir sind also fertig, wenn ~~aus~~ wir zeigen

(7) $\varphi(n) = 2^\mu$ ist Potenz von 2

$\Longleftrightarrow$ $m_1 = \ldots = m_\ell = 1$ und die p_i sind Fermat-Primzahlen.

Wir können ja (7) ebenso auf n selbst wie auf seine Teiler d anwenden.

Die Rück-Richtung "$\Leftarrow$" folgt (von (7)) sofort aus unserer Formel (3) für $\varphi(n)$ und der Definition (1) der Fermat-Primzahlen.

Die Hin-Richtung "$\Rightarrow$" (aus (3) mit $d=r$ und aus (5)) folgt ebenso, leicht, mit einem kleinen Lemma.

<u>Lemma</u>: Sei $p = 2^\mu + 1$ prim. Dann ist $\mu = 2^k$, also p eine Fermat-Primzahl.

<u>Bem</u>: Dieses Lemma ist zugleich der direkte Beweis unseres Satzes für $n=p$ prim: denn ist ja

$$z^n - 1 = z^p - 1 = \underbrace{(z-1)}_{Q_1(z)}\underbrace{(1+z+\dots+z^{p-1})}_{Q_p(z)} \tag{8}$$

und $\varphi(n) = \varphi(p) = p-1 = 2^\mu$. Bis heute hatte also Kepler im Fall der regulären p-Ecke mit p prim nur für $p = F_2$, F_3, F_4 nachweislich unrecht!

<u>Beweis (Lemma):</u>

Der kleine Satz von Fermat sagt, dass es einen Teiler ϱ von $p-1$ gibt, so dass

(9) $$2^{\varrho} \equiv 1 \pmod{p};$$

wähle ϱ (>0) minimal. Nach Voraussetzung ist

(10) $$2^{\mu} \equiv -1 \pmod{p},$$

und sicherlich ist auch μ minimal mit dieser Eigenschaft. Notfalls nach Division $\mu = a\varrho + b$ mit Rest b sehen wir $0 < \mu < \varrho$, wegen der Minimalität von μ. Andrerseits ~~folgt ϱ~~ teilt ϱ auch 2μ, wegen der Minimalität von ϱ und weil auch $2^{2\mu} = (2^{\mu})^2 \equiv 1 \pmod{p}$. Also folgt:

(11) $$2\mu = \varrho \text{ teilt } p-1 = 2^{\mu}.$$

Also ist $\mu = 2^k$ selbst eine Potenz von 2. Damit sind Lemma und Satz bewiesen.

$\square$

<u>Beispiel:</u> das Pentagon $n=5$, $\omega := \exp(2\pi i/5)$.

$$(12)\quad z^5-1 = \prod_{k=0}^{4}(z-\omega^k) = \underbrace{(z-1)}_{Q_1(z)}\cdot\underbrace{\prod_{k=1}^{4}(z-\omega^k)}_{Q_5(z)} = (z-1)\underbrace{(z^4+z^3+z^2+z+1)}_{Q_5(z)}$$

Wir haben also die Lösungen $z=\omega^k$, $k=1,\dots,4$, als sukzessive Lösungen quadratischer (von $Q_5(z)=0$) Gleichungen (14, 15) zu konstruieren. Mit $\varphi := 2\pi/5$ betrachten wir die Hilfsvariablen

$$(13)\quad \zeta := \tfrac{1}{2}(\omega+\omega^4) = \tfrac{1}{2}(\omega+\bar\omega) = \cos\varphi \quad \text{und}$$

$$\tfrac{1}{2}(\omega^2+\omega^3) = \tfrac{1}{2}(\omega^2+\bar\omega^2) = \cos 2\varphi$$

$$= 2\cos^2\varphi - 1 = 2\zeta^2-1. \quad (*)$$

Dann folgt

$$(14)\quad 0 = \tfrac{1}{2}Q_5(\omega) = \tfrac{1}{2}(1+\omega+\omega^2+\omega^3+\omega^4) = 2\zeta^2+\zeta-\tfrac{1}{2},$$

also $0 < \zeta = \frac{1}{4}(\sqrt{5}-1) = \frac{1}{2}\cdot$(goldener Schnitt).

Nach Konstruktion von $\zeta = \cos\varphi$ folgt $\omega = \cos\varphi + i\sin\varphi$ durch $\sin\varphi = \sqrt{1-\zeta^2}$ leicht am Einheitskreis, oder algebraisch per quadratischer Gleichung

$$(15)\quad \omega^2 - 2\zeta\omega + 1 = \omega^2 - \omega^2 - \omega^5 + 1 = 0.$$

(*) (Galois: ζ ist invariant unter dem Automorphismus $z \mapsto \bar z$ des Körpers $\mathbb{Q}(\omega)$.)

Anmerkungen zu Kepler:

Ganz recht behauptet Kepler, dass die Seitenlängen $s_p = |\exp(2\pi i/p) - 1|$ des regulären p-Ecks zu $p=7$ und 11 nicht konstruierbar sind. Er weist folgende Näherungen $\tilde{s}_p$ als "offensichtlich falsch" zurück:

Autor	Näherung	Relativer Fehler
Albrecht Dürer	$\tilde{s}_7 = \frac{1}{2} s_3$	$-2.0\,‰$
von Malaspina	$\tilde{s}_{14/3} = 5/4$	$+2.4\,‰$
"verbreitet"	$\tilde{s}_{11} = \frac{1}{13}\sqrt{\frac{1}{3}(88+43\sqrt{3})}$	$+4.7\,‰$

Dabei führt die Sehnenlänge $|\exp(2\pi i/(14/3)) - 1| =$ $= s_{14/3}$ des 3/14 Kreisbogens fortgesetzt zum $12/14 \equiv -2/14 \equiv -1/7$ und zum $15/14 \equiv 1/14$ Kreisbogen.

Dezimale Näherungen:

$$s_3 = \sqrt{3} = 1.7320508076\ldots$$
$$s_7 = 0.8677674782\ldots$$
$$s_{11} = 0.5634651137\ldots$$
$$s_{14/3} = 1.2469796037\ldots$$

Literatur z.B.:

[Courant, Robbins (Stewart)]
"Was ist Mathematik"

[Lang] "Algebra"

[van der Waerden] "Algebra"

[Kepler] "Harmonices Mundi", Liber I (1619)

[Gauss] "Disquisitiones Arithmeticae" (1801)

[Wantzel] "Recherches sur les moyens de reconnaitre si un problème de géométrie peut se résoudre avec la règle et le compas" (1837)