Rostock. Math. Kolloq. **49**, 44–50 (1995)

Subject Classification (AMS)
51M15,12F05,00A35

Klaus–Dieter Drews

Eine vereinfachende Behandlung der Konstruierbarkeit von p^k– Ecken

Gewidmet den Herren Professoren
L. Berg, W. Engel, G. Pazderski *und* H.-W. Stolle.

Die Lösung des Konstruierbarkeitsproblem von regulären p^k–Ecken $-$ p hier stets ungerade Primzahl, $k = 1, 2, \dots$, Konstruktionen mit Lineal und Zirkel – läßt sich bekanntlich zusammenfassen in folgende drei Aussagen:

1. Ist ein p–Eck konstruierbar, so hat p die Form $2^m + 1$. Zur Primzahleigenschaft muß hierin $m = 2^n$, p eine FERMATsche Primzahl sein. (Bisher sind 5 solche bekannt: 3, 5, 17, 257, 65537.)

2. Hat p die Form $2^m + 1$, so ist das p–Eck konstruierbar.

3. Kein p^k–Eck mit $k > 1$ ist konstruierbar.

Eine Behandlung dieses Themas kann man nur auf der Basis gewisser Vorleistungen angehen, und es seien einige Begriffe und Tatsachen genannt, auf die wir uns berufen wollen:
Formulierung der Konstruierbarkeit mittels Einheitswurzeln; Körpererweiterungen durch irreduzible Polynome; Konstruierbarkeit genau aller Elemente aus Körpern über den rationalen Zahlen Q, die durch eine endliche Anzahl von Erweiterungen mit quadratischen Gleichungen entstehen (d. h., aller Qudratwurzelterme über Q); Zyklizität der primen Restklassengruppe mod p; EISENSTEINsches Irreduzibilitätskriterium.

Sehr sorgfältig widmen sich beispielweise [1] und [2] diesen Vorbereitungen, Bücher, die mit dem von uns beabsichtigten Abstraktionsniveau korrelieren; in [2] wird auch die obige Aussage 1 bewiesen, wir gehen auf sie hier nicht weiter ein. Bedauerlich fand ich es, als ich abseits einer Algebra–Vorlesung einen Zugang zu dem Problem benötigte, daß für die Aussagen 2 und 3 im dortigen Rahmen, unter Hinweis auf zusätzlich erforderliche Gruppen- und Körpertheorie, kein Weg angeboten wurde.

Alle mir bekannt gewordenen (modernen) Darstellungen ziehen – mit Ausnahme der ersten von zwei Varianten aus [3] - die GALOISsche Theorie zur Lösung heran. So ist es mein Bestreben, die gewünschten Aussagen auf eingangs abgesteckter Basis ohne wesentliche begriffliche Vertiefung zu erhalten. Moralische Unterstützung möchte ich mir z. B. aus [4] holen, wo es zu nahe verwandter Thematik heißt (S. 204): "Man soll ja nicht mit Kanonen nach Spatzen schießen."
Geniale Grundlagen zum Thema rühren bekanntlich von GAUSS [5] her, wir verwenden sie mit heutigen Werkzeugen. Wie in der erwähnten Variante aus [3] sind auch für nachfolgende Ausführungen die GAUSSschen Perioden wesentlich, dort in einer beanspruchenden Rechnung ("the proof is rather intricate", S. 104), wohingegen hier vergleichbare Argumente aus elememtaren Kenntnissen über Körper und Vektorräume gewonnen werden sollen.

Zu Aussage 2.

Wegen $x^p - 1 = (x-1)(x^{p-1} + x^{p-2} + \ldots + x + 1)$ enthält

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

alle p–ten Einheitswurzeln $\neq 1$ als Nullstellen; für $\varepsilon := e^{i\frac{2\pi}{p}}$ und jede Zahl g aus $\{1, \ldots, p-1\}$ gilt somit

$$\varepsilon^p = 1, \;\; f(\varepsilon) = 0, \quad f(\varepsilon^g) = 0.$$

Mittels des über Q irreduziblen $f(x)$ sei der Erweiterungskörper K von Q konstruiert:

$$K = Q(\varepsilon) = \{r(\varepsilon) \; : \; r(x) \in Q[x] \; \wedge \; \text{Grad } (r) \leq p-2\} \cup \{0\}.$$

K ist ein Vektorraum der Dimension $p-1$ über Q mit der Basis

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

Zu Polynomen $r_1(x), r_2(x)$ aus $Q[x]$ vom Grad $\leq p-2$ gibt es in $Q[x]$ eindeutig bestimmte Polynome $q(x), \; r_3(x)$ vom Grad $\leq p-2$ mit

$$r_1(x) \cdot r_2(x) \;\; = \;\; q(x) \cdot f(x) + r_3(x); \tag{2}$$

die Multiplikation im Körper K verläuft (für Elemente $\neq 0$) gemäß

$$r_1(\varepsilon) \cdot r_2(\varepsilon) = r_3(\varepsilon).$$

Wir behandeln nun unter

a) Die Existenz von Teilköpern des Körpers K, sodann unter
b) deren Vektorraum–Dimensionen, die erkennen lassen, daß ε Quadratwurzelterm über Q ist.

a) Durch $\varphi_0(\varepsilon) := \varepsilon^g$, $\varphi_0(r(\varepsilon)) := r(\varphi_0(\varepsilon))$, $\varphi_0(0) := 0$ ($g \in \{1, \dots, p-1\}$, über g wird unten noch geeignet verfügt) ist eine Abbildung φ_0 von K in K definiert. Insbesondere gilt $\varphi_0(a) = a$ für die Elemente a aus Q und $\varphi_0(\varepsilon^\nu) = (\varphi_0(\varepsilon))^\nu$ $(\nu = 0, 1, \dots, p-2)$.

Die nachfolgenden Überlegungen (für Elemente $\neq 0$) zeigen, daß φ_0 einen *Automorphismus* von K bewirkt:

$\varphi_0(r_1(\varepsilon) + r_2(\varepsilon)) = \varphi_0(r_1(\varepsilon)) + \varphi_0(r_2(\varepsilon))$ ist klar;

$\varphi_0(r_1(\varepsilon) \cdot r_2(\varepsilon)) = \varphi_0(r_3(\varepsilon)) = r_3(\varphi_0(\varepsilon)) = r_1(\varphi_0(\varepsilon)) \cdot r_2(\varphi_0(\varepsilon)) = \varphi_0(r_1(\varepsilon)) \cdot \varphi_0(r_2(\varepsilon))$

gilt nach (2) wegen $f((\varphi_0(\varepsilon)) = f(\varepsilon^g) = 0$;

$\varphi_0(r(\varepsilon)) = r(\varphi_0(\varepsilon))$ verschwindet nicht, denn $\varphi_0(\varepsilon) = \varepsilon^g$ ist nicht Nullstelle eines Polynoms vom Grad $< p-1$.

Das Element 1 der Basis (1) werde nunmehr gegen das Element $-1-\varepsilon-\varepsilon^2-\dots-\varepsilon^{p-2} = \varepsilon^{p-1}$ ausgetauscht. Außerdem sei g ein erzeugendes Element der (zyklischen !) primen Restklassengruppe mod p, so daß die Potenzen $g^0, g^1, g^2, \dots, g^{p-2}$ mod p die Menge $\{1, 2, \dots, p-1\}$ durchlaufen, und wir notieren die neue Basis $\varepsilon, \varepsilon^2, \dots, \varepsilon^{p-1}$ in der Anordnung

$$\varepsilon^{g^0},\ \varepsilon^{g^1},\ \dots,\ \varepsilon^{g^{p-3}},\ \varepsilon^{g^{p-2}}. \tag{3}$$

Für die Darstellung

$$\alpha = \sum_{\nu=0}^{p-2} c_\nu \varepsilon^{g^\nu} \quad (c_\nu \in Q) \tag{4}$$

der Elemente aus K bez. dieser Basis gilt wegen $\varepsilon + \varepsilon^2 + \dots + \varepsilon^{p-1} = -1$ speziell:

$$\alpha \in Q \Longleftrightarrow c_0 = c_1 = \dots = c_{p-2}\ (= -\alpha). \tag{5}$$

Neben φ_0 betrachten wir weitere Automorphismen φ_i von K: Für $\alpha \in K$ sei

$$\varphi_i(\alpha) := \varphi_{i-1}(\varphi_{i-1}(\alpha)) \quad (i = 1, 2, \dots, m).$$

Wichtig sind im folgenden solche Elemente aus K, die bei φ_i auf sich abgebildet werden (*Fixelelemente*).

Für $i = 0, 1, \dots, m$ bilden die Fixelemente von φ_i jeweils einen Körper K_i.

Sind nämlich α und β bei φ_i invariant, so sind dies auch $\alpha+\beta, \alpha-\beta, \alpha\cdot\beta$ und α/β $(\beta \neq 0)$, weil φ_i ein Automorphismus ist.
Ersichtlich bestehen die Inklusionen $Q \subseteq K_{i-1} \subseteq K_i \subseteq K$ $(i \neq 0)$.

b) Bei der Anwendung von φ_0 gehen die Elemente (3) der Reihe nach über in

$$\varepsilon^{g^1},\ \varepsilon^{g^2},\ \dots,\ \varepsilon^{g^{p-2}},\ \varepsilon^{g^{p-1}} = \varepsilon^{g^0},$$

denn es ist $g^{p-1} = jp + 1$ und $\varepsilon^{jp} = (\varepsilon^p)^j = 1$ (j ganz), d.h., die Basiselemente (3) werden beim Automorphismus φ_0 zyklisch versetzt, und zwar um eine Position (um 2^0 Positionen). Dann gilt, wie man induktiv sofort sieht:

> Bei Anwendung von φ_i werden die $p-1$ Basiselemente (3) zyklisch um 2^i Positionen versetzt ($i \in \{0, 1, \dots, m\}$).

Weil aber 2^i ein Teiler von $p-1$ $(= 2^m)$ ist, geschieht diese Vertauschung auf 2^i elementefremden Zyklen (Orbits) mit jeweils 2^{m-i} Basiselementen. Die Summen der Elemente auf jedem dieser Orbits sind die GAUSS*schen Perioden*

$$\begin{array}{rcccccccl}
\eta_0 & := & \varepsilon^{g^0} & + & \varepsilon^{g^{2^i}} & + & \varepsilon^{g^{2\cdot 2^i}} & + & \dots, \\
\eta_1 & := & \varepsilon^{g^1} & + & \varepsilon^{g^{1+2^i}} & + & \varepsilon^{g^{1+2\cdot 2^i}} & + & \dots, \\
 & & \dots & & \dots & & \dots & & \\
\eta_{2^i-1} & := & \varepsilon^{g^{2^i-1}} & + & \varepsilon^{g^{2^i-1+2^i}} & + & \varepsilon^{g^{2^i-1+2\cdot 2^i}} & + & \dots
\end{array}$$

der Länge 2^{m-i}. Sie liegen (für jeweils festes i) im Körper K_i und sind offensichtlich linear unabhängig über Q.

Darüber hinaus aber gehört ein Element α genau dann zu K_i, bleibt es invariant bei φ_i, wenn es Linearkombination der η_ν ist, denn nach der oben angemerkten Wirkung von φ_i auf die Basis (3) muß für solches α in der eindeutigen Darstellung (4) immer $c_\nu = c_\mu$ sein, falls ν und μ um Vielfache von 2^i differieren, d.h.:

Für $i = 0, 1, \dots, m$ ist der Körper K_i ein Vektorraum der Dimension 2^i über Q.

Insbesondere gilt $K_0 = Q$ (vgl. auch (5)) und $K_m = K$.

Zusammen mit K_i betrachten wir jetzt K_{i-1} (für fixiertes $i > 0$). Eine Basis dieses Vektorraums der Dimension 2^{i-1} über Q bilden die 2^{i-1} GAUSSschen Perioden der Länge 2^{m-i+1}, sie seien mit

$$\zeta_0,\ \zeta_1,\ \dots,\ \zeta_l$$

bezeichnet (l steht für $2^{i-1}-1$). Zu K_{i-1} gehört η_0 ausdrücklich nicht, weil sich in der Darstellung (4) für η_0 die Koeffizienten erst nach 2^i und nicht nach 2^{i-1} Gliedern wiederholen. Andererseits liegen die 2^i Elemente

$$\zeta_o,\ \zeta_1,\ \dots,\ \zeta_l,\ \zeta_0\eta_0,\ \zeta_1\eta_0,\ \dots,\ \zeta_l\eta_0$$

in K_i, und überdies bilden sie eine Basis von K_i über Q, denn sie sind linear unabhängig über Q: Verschwindet nämlich die Linearkombination

$$\sum_{\nu=0}^{l} d'_\nu\zeta_\nu + \left(\sum_{\nu=0}^{l} d''_\nu\zeta_\nu\right)\eta_0 \quad (d'_\nu, d''_\nu \in Q), \tag{6}$$

so gilt $\sum\limits_{\nu=0}^{l} d''_\nu\zeta_\nu = 0$ (sonst folgte $\eta_0 \in K_{i-1}$) und dann müssen alle Koeffizienten d'_ν, d''_ν verschwinden.

Die Elemente aus K_i können deshalb in der Form (6), d. h. als $\beta' + \beta''\eta_0$ ($\beta', \beta'' \in K_{i-1}$) dargestellt werden, und dies besagt:

Für $i = 1, 2, \dots, m$ ist K_i ein Vektorraum der Dimension 2 über K_{i-1}.

Jedes Element α aus K_i genügt somit einer Gleichung höchstens zweiten Grades mit Koeffizienten aus K_{i-1}, denn $1, \alpha, \alpha^2$ sind linear abhängig über K_{i-1}. Wegen $K_0 = Q$ und $\varepsilon \in K_m = Q(\varepsilon)$ erhalten wir abschließend:

Für Primzahlen p von der Form $2^m + 1$ ist die p–te Einheitswurzel ε Quadratwurzelterm über Q und folglich konstruierbar.

Hierbei sind Konstruktionen (z. B. v. d. WAERDEN [6]) als solche in der *komplexen Ebene* aufgefaßt. Aus $g^{\frac{p-1}{2}} \equiv -1 \pmod p$ (für das erzeugende Element g der primen Restklassengruppe mod p) folgt jedoch

$$\varphi_{m-1}(\varepsilon) = \varepsilon^{g^{2^{m-1}}} = \varepsilon^{g^{\frac{p-1}{2}}} = \varepsilon^{-1} = \overline{\varepsilon},$$

so daß φ_{m-1} jedes Element aus K in sein konjugiert komplexes abbildet. Die Fixelemente hiervon, der Körper K_{m-1} und seine Teilkörper, sind somit *reell*: In $K_{m-1}(= K_i)$ liegt

$$\eta_0 = \varepsilon^{g^0} + \varepsilon^{g^{2^{m-1}}} = \varepsilon + \overline{\varepsilon} = 2\cos\frac{2\pi}{p}$$

als reell aufgebauter Quadratwurzelterm über Q.

Zu Aussage 3.

Es genügt zu zeigen, daß p^2–Ecke nicht konstruierbar sind. Wegen

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

ist eine primitive p^2–te Einheitswurzel γ Nullstelle von

$$f_1(x) := (x^p)^{p-1} + (x^p)^{p-2} + \ldots + x^p + 1.$$

Wir werden $f_1(x)$ als über Q irreduzibel nachweisen. Demnach hat der kleinste Körper $Q(\gamma)$, in dem γ liegt, die Vektorraumdimension $p(p-1)$ über Q; dies ist keine Potenz von 2 und folglich γ nicht konstruierbar.
Vorausgeschickt sei, daß für $\mu = 1, \ldots, p-1$ und $\kappa = 1, \ldots, \mu$ stets

$$\binom{p \cdot \mu}{p \cdot \kappa} \equiv \binom{\mu}{\kappa} \pmod p$$

gilt; denn in

$$\binom{p\mu}{p\kappa} = \frac{p\mu(p\mu-1)\ldots(p\mu-p+1)\ \ p(\mu-1)\ldots\ \ p(\mu-\kappa+1)\ldots(p\mu-p\kappa+1)}{p\kappa(p\kappa-1)\ldots(p\kappa-p+1)\ \ p(\kappa-1)\ldots\ \ p\qquad\qquad\ldots 1}$$

kürze man alle Faktoren p sowie mudolo p die zwischen den Vielfachen von p stehenden Reste $p-1, p-2, \ldots, 1$.

Sei nun

$$f_1(x+1) = (x+1)^{p(p-1)} + (x+1)^{p(p-2)} + \ldots + (x+1)^p + 1 =: \sum_{\nu=0}^{p(p-1)} b_\nu x^\nu.$$

Man sieht $b_{p(p-1)} = 1$, $b_0 = p$ und für die übrigen Koeffizienten

$$b_\nu = \binom{p(p-1)}{\nu} + \binom{p(p-2)}{\nu} + \ldots + \binom{p}{\nu}.$$

Gilt $\nu = p\kappa$ $(\kappa = 1, \ldots, p-2)$, so folgt mit der Vorbemerkung

$$b_\nu \equiv \binom{p-1}{\kappa} + \binom{p-2}{\kappa} + \ldots + \binom{\kappa}{\kappa} = \binom{p}{\kappa+1} \equiv 0 \pmod p;$$

ist ν dagegen kein Vielfaches von p, so teilt p schon jeden Summanden von b_ν. Nach dem EISENSTEINschen Kriterium ist hiernach $f_1(x+1)$ und dann auch $f_1(x)$ irreduzibel über Q.

Literatur

[1] **Jones, A., Morris, S. A.** und **Pearson, K. A.** : *Abstract Algebra and Famous Impossibilities.* New York 1991

[2] **Gilbert, W. J.** : *Modern Algebra with Applications.* New York 1976

[3] **Hadlock, C. R.** : *Field Theory and its Classical Problems.* Washington, D.C. 1978

[4] **Laugwitz, D.** : *Unlösbarkeit geometrischer Konstruktionsaufgaben - Braucht man dazu moderne Algebra ?* In: Fuchssteiner, B. u. a. (Eds.) : *Jahrbuch Überblicke Mathematik 1976.* S. 201–204, Mannheim 1976

[5] **Gauss, C. F.** : *Disquisitiones Arithmeticae (1801).* Werke Bd.1, 2. Abdruck, Göttingen 1870

[6] **van der Waerden, B. L.** : *Algebra I.* 4. Aufl., Berlin 1955

eingegangen: 29. August 1995

Autor:

Dr. K.-D. Drews
Universität Rostock
Fachbereich Mathematik
Universitätsplatz 1
18051 Rostock
Deutschland