n eine p-te Potenz in K ist und wenn zusätzlich im Falle $4 \mid n$ das Element c nicht von der Form $c = -4a^4$ mit $a \in K$ ist. Hinweis: Man studiere zunächst den Fall, daß n eine Primpotenz ist.

6.3 Konstruktionen mit Zirkel und Lineal

In diesem Abschnitt werden wir die Galois-Theorie auf geometrische Konstruktionsprobleme in der komplexen Zahlenebene $\mathbb{C}$ anwenden. Wir gehen von einer Teilmenge $M \subset \mathbb{C}$ aus (später setzt man meist $M = \{0, 1\}$) und sagen, ein Punkt $z \in \mathbb{C}$ *lasse sich mit Zirkel und Lineal aus M konstruieren*, wenn M sich durch endlich viele *elementare Konstruktionsschritte* zu einer Teilmenge $M' \subset \mathbb{C}$ mit $z \in M'$ vergrößern läßt. Dabei lassen wir folgende drei Typen von elementaren Konstruktionsschritten zu:

(1) Man betrachte zwei nicht-parallele Geraden g_1 und g_2 in $\mathbb{C}$, welche jeweils durch Punkte $z_1, z_2 \in M$ bzw. $z_3, z_4 \in M$ festgelegt sind, und füge zu M den Schnittpunkt von g_1 mit g_2 hinzu.

(2) Man betrachte eine Kreislinie K in $\mathbb{C}$ um einen Punkt $z_1 \in M$ mit einem Radius, der durch den Abstand $|z_3 - z_2|$ zweier Punkte $z_2, z_3 \in M$ gegeben wird, sowie eine Gerade g, die durch zwei Punkte z_4, $z_5 \in M$ definiert wird, und füge zu M alle Schnittpunkte von K mit g hinzu.

(3) Man betrachte zwei nicht-identische Kreislinien K_1 und K_2 in $\mathbb{C}$ mit Mittelpunkten $z_1, z_2 \in M$ sowie Radien $|z_4 - z_3|$ bzw. $|z_6 - z_5|$, die durch Abstände zwischen Punkten $z_3, z_4, z_5, z_6 \in M$ gegeben werden. Man füge die Schnittpunkte von K_1 mit K_2 zu M hinzu.

Wir bezeichnen mit $\mathfrak{K}(M)$ die Menge aller mit Zirkel und Lineal aus M konstruierbaren Punkte in $\mathbb{C}$, wobei wir stets $0, 1 \in M$ voraussetzen wollen. Ist dann $\overline{M}$ das Bild von M unter der komplexen Konjugation[1] $\mathbb{C} \longrightarrow \mathbb{C}$, $z \longmapsto \overline{z}$, so gilt offenbar $\mathfrak{K}(M) = \mathfrak{K}(M \cup \overline{M})$, da man zu jedem $z \in M$ den konjugierten Punkt $\overline{z}$ durch Spiegeln an der reellen Achse mit Zirkel und Lineal konstruieren kann.

Satz 1. *Sei $M \subset \mathbb{C}$ mit $0, 1 \in M$, und sei $z \in \mathbb{C}$. Dann ist äquivalent:*

(i) $z \in \mathfrak{K}(M)$.

(ii) *Es existiert eine Körperkette $\mathbb{Q}(M \cup \overline{M}) = L_0 \subset L_1 \subset \ldots \subset L_n \subset \mathbb{C}$ mit $z \in L_n$ und $[L_i : L_{i-1}] = 2$ für $i = 1, \ldots, n$.*

(iii) *z ist enthalten in einer Galois-Erweiterung L von $\mathbb{Q}(M \cup \overline{M})$, deren Grad $[L : \mathbb{Q}(M \cup \overline{M})]$ eine Potenz von 2 ist.*

Als direkte Folgerung ergibt sich hieraus:

[1] Wir verwenden in diesem Abschnitt die Notation $\overline{M}$ für das Bild von M unter der Konjugationsabbildung, auch wenn M ein Körper ist; ein algebraischer Abschluß eines solchen Körpers $M \subset \mathbb{C}$, üblicherweise mit $\overline{M}$ bezeichnet, wird nicht benötigt.

Korollar 2. *Sei $M \subset \mathbb{C}$ mit $0, 1 \in M$. Es ist $\mathfrak{K}(M)$ ein algebraischer Erweiterungskörper von $\mathbb{Q}(M \cup \overline{M})$. Der Grad eines jeden Elementes $z \in \mathfrak{K}(M)$ über $\mathbb{Q}(M \cup \overline{M})$ ist eine Potenz von 2.*

Beweis von Satz 1. Wir beginnen mit der Implikation von (i) nach (ii). Wegen $\mathfrak{K}(M) \subset \mathfrak{K}(\mathbb{Q}(M \cup \overline{M}))$ dürfen wir M durch $\mathbb{Q}(M \cup \overline{M})$ ersetzen und somit annehmen, daß es sich bei M um einen *Körper* mit $M = \overline{M}$ handelt. Die Invarianz von M unter der komplexen Konjugation hat zur Folge, daß für einen Punkt $z \in M$ auch sein Realteil $\operatorname{Re} z$, sein Imaginärteil $\operatorname{Im} z$ sowie sein Betrag $|z|$ zu M gehören. Sei nun $z \in \mathfrak{K}(M)$. Es reicht, den Fall zu betrachten, wo z sich durch einen einzigen elementaren Konstruktionsschritt aus M gewinnen läßt, und zu zeigen, daß es zu z eine Körperkette $M \subset L' \subset L$ gibt mit $z \in L$ sowie $[L' : M] \leq 2$, $[L : L'] \leq 2$ und $L = \overline{L}$. Mit Induktion erhält man daraus den Allgemeinfall.

Wir betrachten zunächst einen Konstruktionsschritt des Typs (1). Dann ergibt sich z als Schnittpunkt zweier Geraden

$$g_1 = \{z_1 + t(z_2 - z_1), t \in \mathbb{R}\},$$
$$g_2 = \{z_3 + t'(z_4 - z_3), t' \in \mathbb{R}\},$$

mit $z_1, z_2, z_3, z_4 \in M$, d. h. wir haben die Gleichung

$$z_1 + t(z_2 - z_1) = z_3 + t'(z_4 - z_3)$$

nach den Parametern $t, t' \in \mathbb{R}$ aufzulösen. Eine Aufspaltung dieser Gleichung in Real- und Imaginärteil ergibt zwei lineare Gleichungen in den Unbekannten t, t' mit Koeffizienten in $\mathbb{R} \cap M$. Die Komponenten der Lösung (t_0, t_0') gehören dann ebenfalls zu $\mathbb{R} \cap M$, und wir erhalten

$$z = z_1 + t_0(z_2 - z_1) = z_3 + t_0'(z_4 - z_3) \in M,$$

so daß in diesem Falle keine (echte) Erweiterung von M notwendig ist; man setze $L = L' = M$.

Als nächstes nehmen wir an, daß z aus M durch einen Konstruktionsschritt des Typs (2) gewonnen wird. Es ist z also Schnittpunkt einer Kreislinie

$$K = \{\zeta \in \mathbb{C}, |\zeta - z_1|^2 = |z_3 - z_2|^2\}$$

mit einer Geraden

$$g = \{z_4 + t(z_5 - z_4), t \in \mathbb{R}\},$$

wobei $z_1, \ldots, z_5 \in M$. Um sämtliche Schnittpunkte von K mit g zu berechnen, ist die Gleichung

$$|z_4 + t(z_5 - z_4) - z_1|^2 = |z_3 - z_2|^2$$

nach t aufzulösen. Da es sich hierbei um eine quadratische Gleichung in t handelt mit Koeffizienten, die sich aus den Real- und Imaginärteilen von $z_1, \ldots, z_5$

mit rationalen Operationen berechnen lassen, also zu $\mathbb{R} \cap M$ gehören, hat jede Lösung und damit auch jeder Schnittpunkt von K mit g einen Grad ≤ 2 über M. Wir setzen nun $L' = M(z)$, $L = L'(\overline{z})$. Da M invariant unter der komplexen Konjugation ist, hat $\overline{z}$ über M denselben Grad wie z, also insbesondere einen Grad ≤ 2 über L', und die Kette $M \subset L' \subset L$ besitzt die gewünschten Eigenschaften.

Es bleibt noch ein Konstruktionsschritt des Typs (3) zu betrachten. Sei z also Schnittpunkt zweier nicht-identischer Kreise

$$K_1 = \{\zeta \in \mathbb{C}\,;\, |\zeta - z_1|^2 = r_1^2\},$$
$$K_2 = \{\zeta \in \mathbb{C}\,;\, |\zeta - z_2|^2 = r_2^2\},$$

wobei $r_1 = |z_4 - z_3|$, $r_2 = |z_6 - z_5|$, $z_1, \ldots, z_6 \in M$. Dann genügt z den Gleichungen

$$z\overline{z} - z\overline{z}_1 - \overline{z}z_1 + z_1\overline{z}_1 = r_1^2,$$
$$z\overline{z} - z\overline{z}_2 - \overline{z}z_2 + z_2\overline{z}_2 = r_2^2,$$

bzw., wenn man subtrahiert, einer Gleichung des Typs

$$az + \overline{a}\overline{z} + b = 0 \quad \text{bzw.} \quad 2\mathrm{Re}(az) + b = 0$$

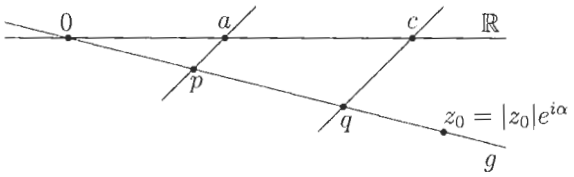
mit $a = \overline{z}_2 - \overline{z}_1 \in M$ und $b \in M \cap \mathbb{R}$. Da die Mittelpunkte von K_1 und K_2 verschieden sein müssen, handelt es sich bei der letzten Gleichung um eine Geradengleichung für z. Indem wir die zugehörige Gerade mit K_1 oder K_2 schneiden, können wir wie bei einem Konstruktionsschritt des Typs (2) weiterschließen. Der Beweis der Implikation (i) $\Longrightarrow$ (ii) ist damit abgeschlossen.

Zum Nachweis der umgekehrten Implikation genügt es zu zeigen, daß $\mathfrak{K}(M)$ (unter der Voraussetzung $0, 1 \in M$) ein Teilkörper von $\mathbb{C}$ ist und daß mit z auch jede der beiden Quadratwurzeln $\pm\sqrt{z}$ zu $\mathfrak{K}(M)$ gehört. Um dies einzusehen, zeigen wir nachfolgende Eigenschaften für $\mathfrak{K}(M)$, wobei wir einige dieser Eigenschaften nur aus beweistechnischen Gründen aufgelistet haben:

(a) $z_1, z_2 \in \mathfrak{K}(M) \Longrightarrow z_1 + z_2 \in \mathfrak{K}(M)$
(b) $z \in \mathfrak{K}(M) \Longrightarrow -z \in \mathfrak{K}(M)$
(c) $z \in \mathfrak{K}(M) \Longrightarrow |z| \in \mathfrak{K}(M)$
(d) $e^{\pi i/3} = \frac{1}{2} + \frac{1}{2} \cdot i\sqrt{3} \in \mathfrak{K}(M)$
(e) $z_1, z_2 \in \mathfrak{K}(M) \Longrightarrow |z_1||z_2| \in \mathfrak{K}(M)$
(f) $z \in \mathfrak{K}(M), z \neq 0 \Longrightarrow |z|^{-1} \in \mathfrak{K}(M)$
(g) $z_1, z_2 \in \mathfrak{K}(M) \Longrightarrow z_1 z_2 \in \mathfrak{K}(M)$
(h) $z \in \mathfrak{K}(M), z \neq 0 \Longrightarrow z^{-1} \in \mathfrak{K}(M)$
(i) $z \in \mathfrak{K}(M) \Longrightarrow \pm\sqrt{z} \in \mathfrak{K}(M)$

Jede der vorstehenden Implikationen kann man mit Hilfe einfacher geometrischer Konstruktionen verifizieren. Für (a) verwende man die Interpretation

der Addition komplexer Zahlen als Vektoraddition. Der "Vektor" $z_1 + z_2$ korrespondiert zu der Diagonalen des von den "Vektoren" z_1, z_2 aufgespannten Parallelogramms. Für (b) spiegele man z am Nullpunkt, es liegt $-z$ auf der Geraden durch 0 und z (man nehme $z \neq 0$ an) sowie auf der Kreislinie um 0 mit Radius $|z| = |z - 0|$. In (c) interpretiere man entsprechend $|z|$ als Schnittpunkt der reellen Achse mit der Kreislinie um 0 mit Radius $|z|$. Eigenschaft (d) benötigen wir zum Nachweis von (e) und (f), um zu sehen, daß $\mathfrak{K}(M)$ außer den Punkten $0, 1$ noch einen weiteren, nicht-reellen Punkt enthält; man errichte über der Strecke von 0 nach 1 ein gleichseitiges Dreieck der Seitenlänge 1. Die Spitze, als Schnittpunkt der Kreise um 0 bzw. 1 mit Radius 1, ist dann die primitive sechste Einheitswurzel $e^{\pi i/3} = \frac{1}{2} + \frac{1}{2} \cdot i\sqrt{3}$. In der Situation (e) und (f) schließlich nehme man $z_1 \neq 0 \neq z_2$ an und betrachte folgende Figur:



Um diese zu erhalten, wähle man einen Punkt $z_0 = |z_0|e^{i\alpha}$ in $M - \mathbb{R}$ mit $\operatorname{Re} z_0 > 0$, z. B. $z_0 = e^{\pi i/3}$, und betrachte die Gerade g durch 0 und z_0. Auf g kann man dann die Punkte $p = e^{i\alpha}$ und $q = |z_2|e^{i\alpha}$ betrachten, sowie auf der reellen Achse den Punkt $a = |z_1|$. Alle diese Punkte gehören zu $\mathfrak{K}(M)$, wie man leicht verifiziert. Auf der reellen Achse betrachte man noch den Punkt c, den man als Schnittpunkt von $\mathbb{R}$ mit der Parallelen zu $g_{a,p}$ durch q gewinnt; dabei sei $g_{a,p}$ die durch a und p festgelegte Gerade. Auch c gehört zu $\mathfrak{K}(M)$, wie man anhand elementarer Konstruktionen sofort nachprüft; man fälle etwa von q aus das Lot auf die Gerade durch a und p und errichte auf diesem Lot die Senkrechte in q. Dann gilt nach dem Strahlensatz

$$|q| \cdot |p|^{-1} = |c| \cdot |a|^{-1},$$

also wegen $|q| = |z_2|$, $|p| = 1$ und $|a| = |z_1|$

$$|c| = |a| \cdot |q| = |z_1| \cdot |z_2|$$

und somit $|z_1| \cdot |z_2| \in \mathfrak{K}(M)$. Indem man die Parallele zu $g_{a,p}$ durch $1 \in \mathbb{R}$ konstruiert, erhält man als Schnittpunkt mit g eine komplexe Zahl vom Betrag $|z_1|^{-1}$, wobei $|z_1|^{-1} \in \mathfrak{K}(M)$ gemäß (c). Da sich bei der Multiplikation komplexer Zahlen die Beträge multiplizieren und die Argumente addieren, hat man zum Nachweis von (g) bzw. (h) lediglich noch die Winkeladdition bzw. -negation elementargeometrisch durchzuführen, was aber ohne Probleme möglich ist. Da auch die Winkelhalbierung elementargeometrisch durchführbar ist, bleibt für (i) nur noch zu zeigen, daß für $z \in \mathfrak{K}(M) - \{0\}$ auch $\sqrt{|z|}$ konstruierbar ist. Hierzu betrachte man auf der reellen Achse die Strecke von $-|z|$ bis 1 und errichte hierüber den Halbkreis des Thales. Diesen schneide man mit der Senkrechten

auf der reellen Achse, die man in 0 errichtet. Als Schnittpunkt ergibt sich nach dem Höhensatz für rechtwinklige Dreiecke eine komplexe Zahl vom Betrag $\sqrt{|z|}$. Damit ist gezeigt, daß $\mathfrak{K}(M)$ ein Teilkörper von $\mathbb{C}$ ist und daß $\mathfrak{K}(M)$ abgeschlossen ist unter der Bildung von Quadratwurzeln. Die Äquivalenz der Bedingungen (i) und (ii) ist also bewiesen.

Es bleibt noch die Äquivalenz von (ii) und (iii) zu begründen; sei zunächst Bedingung (ii) gegeben. Zu der Erweiterung L_n von $K = \mathbb{Q}(M \cup \overline{M})$ läßt sich die normale Hülle L in $\mathbb{C}$ bilden; vgl. 3.5/7. Sind $\sigma_1, \ldots, \sigma_r$ die verschiedenen K-Homomorphismen von L_n nach $\mathbb{C}$, so ist L derjenige Körper, der über K von allen $\sigma_i(L_n)$, $i = 1, \ldots, r$, erzeugt wird. Da L_n aus K durch sukzessive Adjunktion von Quadratwurzeln entsteht, gilt dasselbe für jedes $\sigma_i(L_n)$ und daher auch für L. Somit ist L/K eine Galois-Erweiterung, deren Grad eine Potenz von 2 ist. Wegen $z \in L_n \subset L$ ist Bedingung (iii) erfüllt.

Ist umgekehrt Bedingung (iii) gegeben, so ist die Galois-Gruppe $\mathrm{Gal}(L/K)$ eine 2-Sylow-Gruppe und daher nach 5.4/9 auflösbar. Folglich besitzt $\mathrm{Gal}(L/K)$ eine Normalreihe, deren Faktoren zyklisch von der Ordnung 2 sind, vgl. 5.4/6. Zu einer solchen Kette korrespondiert dann aber aufgrund des Hauptsatzes der Galois-Theorie 4.1/6 eine Körperkette wie in Bedingung (ii) gefordert. □

Die Aussage des gerade bewiesenen Satzes ist oft nützlich, um zu zeigen, daß gewisse Größen bzw. Punkte der komplexen Zahlenebene nicht durch Konstruktion mit Zirkel und Lineal aus einer gegebenen Menge $M \subset \mathbb{C}$ erhalten werden können. Ein berühmtes Beispiel hierzu ist das Problem der *Quadratur des Kreises*, welches darin besteht, einen Kreis, gegeben durch Mittelpunkt und Radius, durch Konstruktion mit Zirkel und Lineal in ein flächengleiches Quadrat zu verwandeln. Man betrachte etwa den Kreis mit Radius 1 um 0. Sein Flächeninhalt wird durch die Zahl π gegeben. Ein flächengleiches Quadrat hat somit die Kantenlänge $\sqrt{\pi}$. Das Problem der Quadratur des Kreises besteht also darin, zu entscheiden, ob $\sqrt{\pi}$ zu $\mathfrak{K}(\{0,1\})$ gehört oder nicht. Gemäß Korollar 2 bildet $\mathfrak{K}(\{0,1\})$ einen algebraischen Erweiterungskörper von $\mathbb{Q}$, man weiß aber, wie F. Lindemann bereits 1882 in [11] gezeigt hat, daß die Zahlen π bzw. $\sqrt{\pi}$ transzendent über $\mathbb{Q}$ sind. Es ist also $\sqrt{\pi}$ nicht mit Zirkel und Lineal aus $\{0,1\}$ konstruierbar und somit die Quadratur des Kreises nicht lösbar. In der Vergangenheit sind durch Konstruktion mit Zirkel und Lineal oftmals sehr gute Näherungslösungen für π bzw. $\sqrt{\pi}$ gefunden worden, die dann in Unkenntnis der Sachlage verschiedentlich als Lösung des Problems der Quadratur des Kreises angesehen wurden.

Ein weiteres klassisches Problem, dessen Unlösbarkeit sich herausstellt, ist das Problem der *Würfelverdoppelung*: Kann man das Volumen eines Würfels durch Konstruktion mit Zirkel und Lineal verdoppeln? Man gehe etwa von einem Würfel der Kantenlänge 1 aus. Verdoppelung des Volumens führt zu einem Würfel der Kantenlänge $\sqrt[3]{2}$. Nach Korollar 2 gehört aber $\sqrt[3]{2}$ nicht zu $\mathfrak{K}(\{0,1\})$, da der Grad von $\sqrt[3]{2}$ über $\mathbb{Q}$ keine Potenz von 2 ist. In ähnlicher Weise behandelt man auch das Problem der Winkeldreiteilung; vgl. hierzu Aufgabe 2.

Wir wollen uns schließlich noch mit dem Problem der *Konstruktion regelmäßiger n-Ecke* beschäftigen. Wichtige Lösungsbeiträge hierzu gehen auf C. F. Gauß zurück. Das Problem besteht darin, zu entscheiden, ob für eine gegebene natürliche Zahl $n \geq 3$ die n-te primitive Einheitswurzel $e^{2\pi i/n}$ zu $\mathfrak{K}(\{0,1\})$ gehört oder nicht. Im Beweis zu Satz 1 hatten wir bereits $e^{\pi i/3} \in \mathfrak{K}(\{0,1\})$ gesehen. Das regelmäßige 6-Eck ist deshalb mit Zirkel und Lineal konstruierbar. Allgemeiner gilt:

Satz 3. *Sei $n \geq 3$ eine natürliche Zahl. Das regelmäßige n-Eck ist genau dann mit Zirkel und Lineal konstruierbar, wenn $\varphi(n)$ eine Potenz von 2 ist; dabei ist φ die Eulersche φ-Funktion (vgl. 4.5/3).*

Beweis. Es sei ζ_n eine primitive n-te Einheitswurzel über $\mathbb{Q}$. Dann ist $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ nach 4.5/7 bzw. 4.5/10 eine abelsche Galois-Erweiterung vom Grad $\varphi(n)$. Nehmen wir zunächst an, daß das regelmäßige n-Eck konstruierbar ist, also $\zeta_n \in \mathfrak{K}(\{0,1\})$ gilt, so ist nach Korollar 2 der Grad von ζ_n über $\mathbb{Q}$ und damit $\varphi(n)$ eine Potenz von 2. Weiß man umgekehrt, daß $\varphi(n) = [\mathbb{Q}(\zeta_n) : \mathbb{Q}]$ eine Potenz von 2 ist, ergibt sich $\zeta_n \in \mathfrak{K}(\{0,1\})$, indem man die Implikation von (iii) nach (i) in Satz 1 ausnutzt. □

Mit 4.5/4 berechnet man leicht folgende Werte der φ-Funktion:

n	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	...
$\varphi(n)$	2	2	4	2	*6*	4	*6*	4	*10*	4	*12*	*6*	8	8	16	...

Kursivdruck in der Zeile für $\varphi(n)$ deutet Nicht-Konstruierbarkeit des regelmäßigen n-Ecks an. Das regelmäßige 7-Eck ist das erste nicht-konstruierbare n-Eck in dieser Liste; der Beweis der Nicht-Konstruierbarkeit geht auf Gauß zurück. Gauß war es auch, der als erster ein Verfahren für die (recht aufwendige) Konstruktion des regelmäßigen 17-Ecks fand, man beachte $\varphi(17) = 16$.

Wir wollen abschließend noch auf den Zusammenhang zwischen der Konstruierbarkeit des regelmäßigen n-Ecks und der Zerlegung von n in Fermatsche Primzahlen eingehen.

Definition 4. *Für $\ell \in \mathbb{N}$ heißt $F_\ell = 2^{2^\ell} + 1$ die ℓ-te* Fermatsche Zahl. *Eine* Fermatsche Primzahl *ist eine Primzahl, die zugleich eine Fermatsche Zahl ist, also eine Primzahl der Form $2^{2^\ell} + 1$.*

Es sind $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65537$ Primzahlen, also Fermatsche Primzahlen. Dies sind die einzigen Fermatschen Zahlen, von denen man bisher weiß, daß sie prim sind.

Satz 5. *Sei $n \geq 2$. Dann ist äquivalent:*

(i) $\varphi(n)$ *ist eine Potenz von* 2.

(ii) *Es existieren verschiedene Fermatsche Primzahlen* $p_1, \ldots, p_r$ *sowie eine natürliche Zahl* $m \in \mathbb{N}$ *mit* $n = 2^m p_1 \ldots p_r$.

Beweis. Für eine Primzahl p ist $\varphi(p^m) = (p-1)p^{m-1}$ genau dann eine Potenz von 2, wenn $p \neq 2$ gilt oder wenn $p^{m-1} = 1$, also $m = 1$ gilt und $p-1$ eine Potenz von 2 ist. Somit folgt die Aussage des Satzes aufgrund der Multiplikativität der φ-Funktion mit folgendem Lemma:

Lemma 6. *Eine Primzahl* $p \geq 3$ *ist genau dann eine Fermatsche Zahl, wenn* $p-1$ *eine Potenz von* 2 *ist.*

Beweis. Für jede Fermatsche Zahl p ist nach Definition $p-1$ eine Potenz von 2. Sei umgekehrt $p-1$ eine Potenz von 2, etwa $p = (2^{2^\ell})^r + 1$ mit ungeradem r. Gilt dann $r > 1$, so können wir p aufgrund der Formel

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

echt zerlegen in der Form

$$(2^{2^\ell})^r + 1 = (2^{2^\ell} + 1)((2^{2^\ell})^{r-1} - \ldots + 1).$$

Da aber p eine Primzahl ist, ergibt sich $r = 1$. □

Zusammenfassend stellt sich heraus, daß das regelmäßige n-Eck genau dann mit Zirkel und Lineal konstruierbar ist, wenn n von der Form $n = 2^m p_1 \ldots p_r$ mit paarweise verschiedenen Fermatschen Primzahlen $p_1, \ldots, p_r$ sowie einer natürlichen Zahl m ist.

Aufgaben

1. *Es sei* $M \subset \mathbb{C}$ *eine Teilmenge mit* $0, 1 \in M$. *Man diskutiere die Frage, ob ein Element* $z \in \mathbb{C}$ *bereits dann zu* $\mathfrak{K}(M)$ *gehört, wenn sein Grad über* $\mathbb{Q}(M \cup \overline{M})$ *eine Potenz von* 2 *ist. Insbesondere betrachte man für* $M = \{0, 1\}$ *den Fall, wo* z *vom Grad* 4 *über* $\mathbb{Q}$ *ist.*

2. *Man überlege, ob das Problem der Winkeldreiteilung mit Zirkel und Lineal lösbar ist.*

3. Für $M = \{0, 1\}$ betrachte man die Erweiterung $\mathfrak{K}(M)/\mathbb{Q}$. Man zeige:
   (i) $\mathfrak{K}(M)/\mathbb{Q}$ ist eine unendliche Galois-Erweiterung.
   (ii) $\mathfrak{K}(M)$ ist darstellbar als Vereinigung einer aufsteigenden Kette von Galois-Erweiterungen von $\mathbb{Q}$, deren Grad jeweils eine Potenz von 2 ist.
   (iii) Man beschreibe die Gruppe $\mathrm{Gal}(\mathfrak{K}(M)/\mathbb{Q})$, indem man die Notation des projektiven Limes benutzt, vgl. Abschnitt 4.2.

4. Man beschreibe die Konstruktion mit Zirkel und Lineal für das regelmäßige 5-Eck.