# 3. Irreduzible Polynome und Kreisteilungspolynome

Aus dem letzten Kapitel wissen wir, dass wir zur Berechnung des Grades einer algebraischen Körpererweiterung Minimalpolynome benötigen: ist $L/K$ mit $L = K(a)$ für ein $a \in L$ eine einfache algebraische Körpererweiterung, so ist ihr Grad $[L : K]$ nach Satz 2.14 (a) gleich dem Grad des Minimalpolynoms $m_a$ von $a$ über $K$. Außerdem haben wir in Lemma 2.6 bereits gesehen, dass $m_a$ dadurch charakterisiert werden kann, dass es ein irreduzibles normiertes Polynom über $K$ mit Nullstelle $a$ ist. Während man normierte Polynome mit Nullstelle $a$ in der Regel leicht finden kann, ist es jedoch in der Praxis oft schwierig zu entscheiden, ob diese Polynome auch irreduzibel sind — dies haben wir in Beispiel 2.9 (d) bereits gesehen. Das einzige Irreduzibilitätskriterium, das wir bisher kennen, ist das Ergebnis aus Aufgabe 2.7 (a), dass ein Polynom vom Grad 2 oder 3 genau dann irreduzibel ist, wenn es keine Nullstellen besitzt.

Dass diese Untersuchung der Irreduzibilität von Polynomen im Allgemeinen ein schwieriges Problem ist, kann man leicht verstehen, wenn man die analoge Situation im Ring $\mathbb{Z}$ der ganzen Zahlen betrachtet. Ihr wisst ja vermutlich, dass es sehr aufwändig ist, von einer (großen) Zahl herauszufinden, ob sie irreduzibel, also eine Primzahl ist. Die Primfaktorzerlegung einer solchen Zahl zu bestimmen ist sogar noch einmal ein ganzes Stück komplizierter; in der Tat ist es die Grundlage vieler moderner Kryptographieverfahren, dass es hierfür kaum effektivere Methoden gibt als ein zeitaufwändiges Durchprobieren aller denkbaren Teiler. Im strukturell noch komplizierteren Polynomring $K[t]$ über einem Körper $K$ wird diese Situation natürlich in der Regel nicht besser. Wir müssen uns daher damit begnügen, in diesem Kapitel ein paar Irreduzibilitätskriterien anzugeben, die zwar in den für uns interessanten Beispielen, insgesamt jedoch nur für „relativ wenige“ Polynome funktionieren. Wir beschränken uns dabei hier auf Polynome über dem Körper $K = \mathbb{Q}$, da dies der für unsere Anwendungen relevante Fall ist.

**Bemerkung 3.1.** Die meisten Strategien, um die Irreduzibilität eines Polynoms in $\mathbb{Q}[t]$ zu zeigen, verfahren in zwei Schritten:

(a) zunächst führt man die Frage nach der Irreduzibilität in $\mathbb{Q}[t]$ durch geeignetes „Wegkürzen der Nenner“ auf die Irreduzibilität in $\mathbb{Z}[t]$ zurück;

(b) die Irreduzibilität in $\mathbb{Z}[t]$ zeigt man dann, indem man die Koeffizienten des Polynoms modulo einer Primzahl $p$ reduziert und so zum oft einfacher zu behandelnden Polynomring $\mathbb{Z}_p[t]$ über dem Körper $\mathbb{Z}_p$ übergeht.

Beachte, dass der erste Teil (a) dabei nicht nur bedeutet, dass man das betrachtete Polynom $f$ mit einer geeigneten Zahl multipliziert, so dass es in $\mathbb{Z}[t]$ liegt: auch bei einem Polynom in $\mathbb{Z}[t]$ ist es natürlich noch etwas anderes, ob man nach der Irreduzibilität in $\mathbb{Q}[t]$ oder in $\mathbb{Z}[t]$ fragt — denn es wäre ja prinzipiell denkbar, dass man zwar eine nicht-triviale Zerlegung $f = g \cdot h$ mit rationalen, aber nicht mit ganzzahligen Polynomen $g$ und $h$ findet, so dass $f$ dann zwar irreduzibel in $\mathbb{Z}[t]$, aber nicht in $\mathbb{Q}[t]$ wäre.

Es stellt sich jedoch heraus, dass die Situation hier besonders schön ist und ein derartiger Fall nicht auftreten kann: eine Zerlegungsmöglichkeit eines ganzzahligen Polynoms über $\mathbb{Q}$ führt immer auch schon zu einer Zerlegungsmöglichkeit über $\mathbb{Z}$. Dies zeigt der folgende Satz, der damit den Punkt (a) der oben beschriebenen Strategie bereits klärt.

**Satz 3.2 (Lemma von Gauß).** *Ist ein nicht-konstantes Polynom $f \in \mathbb{Z}[t]$ irreduzibel in $\mathbb{Z}[t]$, so auch in $\mathbb{Q}[t]$.*

*Beweis.* Angenommen, $f$ wäre reduzibel in $\mathbb{Q}[t]$. Wir zeigen in zwei Schritten, dass $f$ dann auch reduzibel in $\mathbb{Z}[t]$ ist.

1. Behauptung: ist $f$ reduzibel in $\mathbb{Q}[t]$, so gibt es ein $\lambda \in \mathbb{N}_{>0}$, so dass sich $\lambda f$ als Produkt nicht-konstanter Polynome in $\mathbb{Z}[t]$ schreiben lässt. Dies sieht man sofort ein: haben wir eine Zerlegung $f = g \cdot h$ mit nicht-konstanten Polynomen $g, h \in \mathbb{Q}[t]$, so gibt es natürlich $\mu, \nu \in \mathbb{N}_{>0}$, so dass $\mu g, \nu h \in \mathbb{Z}[t]$ gilt (man wähle z. B. für $\mu$ und $\nu$ das kleinste gemeinsame Vielfache der in den Koeffizienten von $g$ bzw. $h$ auftretenden Nenner). Mit $\lambda := \mu\nu$ erhalten wir dann die gewünschte Zerlegung $\lambda f = (\mu g)(\nu h)$ in $\mathbb{Z}[t]$.

2. Behauptung: lässt sich $\lambda f$ für ein $\lambda \in \mathbb{N}_{>1}$ als Produkt nicht-konstanter Polynome in $\mathbb{Z}[t]$ schreiben, so gilt dies auch für $\lambda' f$ für ein geeignetes $\lambda' < \lambda$ in $\mathbb{N}_{>0}$. Für den Beweis dieser Behauptung sei also $\lambda f = g \cdot h$ für nicht-konstante $g, h \in \mathbb{Z}[t]$. Wegen $\lambda > 1$ können wir einen Primfaktor $p$ von $\lambda$ wählen und $\lambda' := \frac{\lambda}{p} \in \mathbb{N}_{>0}$ setzen, so dass wir die Zerlegung $p\lambda' f = gh$ in $\mathbb{Z}[t]$ erhalten. Wir betrachten diese Gleichung nun in $\mathbb{Z}_p[t]$, d. h. reduzieren alle Koeffizienten der Polynome modulo $p$. Bezeichnet $\overline{f} \in \mathbb{Z}_p[t]$ das Polynom, das man aus $f \in \mathbb{Z}[t]$ erhält, indem man alle Koeffizienten durch ihre Restklassen in $\mathbb{Z}_p$ ersetzt (und analog für die anderen auftretenden Polynome), so bekommen wir also die Zerlegung

$$\overline{p} \cdot \overline{\lambda'} \cdot \overline{f} = \overline{g} \cdot \overline{h} \quad \in \mathbb{Z}_p[t].$$

Aber natürlich ist $\overline{p} = \overline{0}$ in $\mathbb{Z}_p[t]$, und damit erhalten wir $\overline{g} \cdot \overline{h} = \overline{0}$ in $\mathbb{Z}_p[t]$. Da $\mathbb{Z}_p[t]$ nach [G, Lemma 9.9 (b)] als Polynomring über einem Körper ein Integritätsring ist, ist dies nur möglich, wenn bereits einer der Faktoren gleich Null ist. Es sei also ohne Beschränkung der Allgemeinheit $\overline{g} = \overline{0}$ in $\mathbb{Z}_p[t]$. Dies bedeutet aber gerade, dass alle Koeffizienten von $g$ durch $p$ teilbar sind. Das Polynom $g' := \frac{g}{p}$ liegt damit ebenfalls in $\mathbb{Z}[t]$, und wir erhalten aus $\lambda f = g \cdot h$ nach Division durch $p$ wie gewünscht die Zerlegung $\lambda' f = g' \cdot h$ in $\mathbb{Z}[t]$ mit $\lambda' < \lambda$. Dies zeigt auch die 2. Behauptung.

Die Aussage des Satzes ergibt sich nun offensichtlich aus der Kombination der beiden Schritte: nach der 1. Behauptung gibt es zunächst ein $\lambda \in \mathbb{N}_{>0}$, so dass $\lambda f$ ein Produkt nicht-konstanter Polynome in $\mathbb{Z}[t]$ ist, und durch fortgesetzte Anwendung der 2. Behauptung können wir diese Zahl $\lambda$ dann so lange reduzieren, bis sie gleich 1 ist. □

**Bemerkung 3.3.** Der Beweis von Satz 3.2 zeigt sogar noch etwas mehr: ist $f \in \mathbb{Z}[t]$ reduzibel in $\mathbb{Q}[t]$, d. h. können wir $f = g \cdot h$ für gewisse nicht-konstante Polynome $g, h \in \mathbb{Q}[t]$ schreiben, so gibt es auch eine Zerlegung $f = g' \cdot h'$ mit $g', h' \in \mathbb{Z}[t]$, *wobei $g'$ und $h'$ aus $g$ bzw. $h$ durch Multiplikation mit einer rationalen Zahl entstehen.* In den beiden Schritten des Beweises werden die beiden Polynome der ursprünglichen Zerlegung über $\mathbb{Q}$ nämlich lediglich mit konstanten Faktoren multipliziert, um die letztendlich gewünschte Zerlegung über $\mathbb{Z}$ zu erhalten. Aus dieser Beobachtung erhalten wir das folgende nützliche Resultat.

**Folgerung 3.4.** *Es seien $f, g, h \in \mathbb{Q}[t]$ normierte Polynome mit $f = g \cdot h$. Gilt dann $f \in \mathbb{Z}[t]$, so liegen auch $g$ und $h$ bereits in $\mathbb{Z}[t]$.*

*Beweis.* Nach Bemerkung 3.3 gibt es $g', h' \in \mathbb{Z}[t]$, die sich von $g$ bzw. $h$ nur um einen konstanten Faktor unterscheiden und für die $f = g' \cdot h'$ gilt. Da der Leitkoeffizient 1 von $f$ dabei gleich dem Produkt der ganzzahligen Leitkoeffizienten von $g'$ und $h'$ ist, können die Leitkoeffizienten von $g'$ und $h'$ außerdem nur 1 oder $-1$ sein. Weil $g$ und $h$ aber nach Voraussetzung den Leitkoeffizienten 1 haben, bedeutet dies gerade, dass $g' = \pm g$ und $h' = \pm h$ gelten muss. Mit $g', h' \in \mathbb{Z}[t]$ ergibt sich damit auch wie behauptet $g, h \in \mathbb{Z}[t]$. □

Insbesondere erhalten wir damit das folgende Kriterium, das oft bei der Suche von Nullstellen ganzzahliger Polynome hilft und das euch vielleicht in der einen oder anderen Form schon aus der Schule bekannt war.

**Folgerung 3.5** (Ganzzahligkeit von Nullstellen)**.** *Es sei $f = t^n + a_{n-1}t^{n-1} + \cdots + a_0 \in \mathbb{Z}[t]$ ein normiertes Polynom. Ist $x \in \mathbb{Q}$ eine Nullstelle von $f$, so gilt bereits $x \in \mathbb{Z}$, und $x$ ist ein Teiler von $a_0$.*

*Beweis.* Ist $x \in \mathbb{Q}$ eine Nullstelle von $f$, so können wir diese bekanntlich abspalten [G, Lemma 11.15] und $f = (t - x)\, g$ für ein normiertes Polynom $g = t^m + b_{m-1}t^{m-1} + \cdots + b_0 \in \mathbb{Q}[t]$ schreiben. Nach Folgerung 3.4 folgt dann $t - x, g \in \mathbb{Z}[t]$ und damit insbesondere $x \in \mathbb{Z}$. Vergleichen wir schließlich noch die konstanten Koeffizienten, so sehen wir außerdem $a_0 = -x\, b_0$ und damit $x \,|\, a_0$. □

**Bemerkung 3.6.** Aufgrund von Satz 3.2 können wir uns für den Nachweis der Irreduzibilität ganzzahliger Polynome über $\mathbb{Q}[t]$ also vollständig auf den Ring $\mathbb{Z}[t]$ zurückziehen, d. h. die Irreduzibilität lediglich in $\mathbb{Z}[t]$ überprüfen. Beachte jedoch, dass in $\mathbb{Z}[t]$ nicht alle konstanten Polynome, sondern nur die Polynome $\pm 1$ Einheiten sind. So ist also z. B. das Polynom $2t \in \mathbb{Z}[t]$ reduzibel, da es das Produkt der Nichteinheiten 2 und $t$ ist. Reduzibilität in $\mathbb{Z}[t]$ bedeutet also nicht notwendigerweise, dass sich das Polynom als Produkt zweier *nicht-konstanter* Polynome schreiben lässt. Um derartige Probleme zu umgehen, wollen wir uns im Folgenden auf normierte Polynome beschränken. Normierte Polynome über $\mathbb{Z}[t]$ können offensichtlich keine Konstante ungleich $\pm 1$ als Teiler haben, so dass in diesem Fall die Reduzibilität über $\mathbb{Z}[t]$ wirklich äquivalent dazu ist, dass sich das Polynom als Produkt von nicht-konstanten Polynomen schreiben lässt.

Wir wollen im Folgenden nun zwei einfache Irreduzibilitätskriterien angeben. Wie schon in Bemerkung 3.1 (b) angekündigt ergeben sich beide (analog zum Beweis von Satz 3.2) durch Reduktion modulo einer Primzahl.

**Lemma 3.7** (Irreduzibilität durch Reduktion modulo $p$)**.** *Es sei $f \in \mathbb{Z}[t]$ ein normiertes Polynom. Gibt es eine Primzahl $p$, so dass das Polynom $\overline{f} \in \mathbb{Z}_p[t]$ irreduzibel in $\mathbb{Z}_p[t]$ ist, so ist bereits $f$ irreduzibel in $\mathbb{Z}[t]$ (und damit nach Satz 3.2 auch in $\mathbb{Q}[t]$).*

*Beweis.* Wäre $f$ reduzibel in $\mathbb{Z}[t]$, nach Bemerkung 3.6 also $f = g \cdot h$ für nicht-konstante $g, h \in \mathbb{Z}[t]$, so wäre natürlich auch $\overline{f} = \overline{g} \cdot \overline{h}$ reduzibel in $\mathbb{Z}_p[t]$. □

**Beispiel 3.8.** Man prüft leicht nach, dass das Polynom $f = t^4 + t^3 + t^2 + t + 1 \in \mathbb{Z}_2[t]$ irreduzibel ist [G, Aufgabe 11.8 (a)] — z. B. indem man explizit nachrechnet, dass die Polynome in $\mathbb{Z}_2[t]$ vom Grad 1 und 2 (von denen es ja nur sehr wenige gibt) alle keine Teiler von $f$ sind. Also ist nach Lemma 3.7 jedes normierte ganzzahlige Polynom, dessen Reduktion modulo 2 gleich $f$ ist (d. h. jedes Polynom $t^4 + a_3t^3 + a_2t^2 + a_1t + a_0 \in \mathbb{Z}[t]$ mit ungeraden $a_0, \ldots, a_3$) irreduzibel in $\mathbb{Z}[t]$ und auch in $\mathbb{Q}[t]$.

**Satz 3.9 (Irreduzibilitätskriterium von Eisenstein).** *Es sei $f = t^n + a_{n-1}t^{n-1} + \cdots + a_1t + a_0 \in \mathbb{Z}[t]$ ein normiertes Polynom. Gibt es eine Primzahl $p$, so dass $p \mid a_i$ für alle $i = 0, \ldots, n-1$ sowie $p^2 \nmid a_0$ gilt, so ist $f$ irreduzibel in $\mathbb{Z}[t]$ (und damit nach Satz 3.2 auch in $\mathbb{Q}[t]$).*

*Beweis.* Angenommen, $f$ wäre reduzibel in $\mathbb{Z}[t]$, nach Bemerkung 3.6 also von der Form $f = g \cdot h$ für gewisse nicht-konstante $g, h \in \mathbb{Z}[t]$. Ein Vergleich der Leitkoeffizienten liefert sofort, dass $g$ und $h$ dann Leitkoeffizient $\pm 1$ haben müssen und damit ohne Beschränkung der Allgemeinheit als normiert vorausgesetzt werden können.

Wir reduzieren die Gleichung $f = g \cdot h$ nun wieder modulo $p$. Da $p$ nach Voraussetzung alle Koeffizienten $a_0, \ldots, a_{n-1}$ von $f$ teilt, folgt $\overline{f} = t^n$ und damit $\overline{g} \cdot \overline{h} = t^n$ in $\mathbb{Z}_p[t]$. Weil es in $\mathbb{Z}_p[t]$ nach [G, Satz 11.9] eine eindeutige Primfaktorzerlegung gibt und $t$ in $\mathbb{Z}_p[t]$ als irreduzibles Polynom natürlich prim ist [G, Bemerkung 11.6], ist $t$ demnach der einzige Primfaktor, der in $\overline{g}$ und $\overline{h}$ auftreten kann, d. h. es ist $\overline{g} = t^k$ und $\overline{h} = t^l$ für gewisse $k, l \geq 1$.

Insbesondere bedeutet dies nun, dass die konstanten Koeffizienten von $g$ und $h$ gleich 0 modulo $p$, also durch $p$ teilbar sein müssen. Damit ist dann der konstante Koeffizient von $f$, der ja wegen $f = g \cdot h$ das Produkt der konstanten Koeffizienten von $g$ und $h$ ist, aber durch $p^2$ teilbar, was ein Widerspruch zur Voraussetzung ist. □

**Beispiel 3.10.** Es seien $p$ eine Primzahl und $n \in \mathbb{N}_{>0}$. Dann ist das normierte Polynom $t^n - p$ nach dem Kriterium von Eisenstein aus Satz 3.9 sowohl in $\mathbb{Z}[t]$ als auch in $\mathbb{Q}[t]$ irreduzibel. Da es außerdem $\sqrt[n]{p}$ als Nullstelle hat, ist es nach Lemma 2.6 das Minimalpolynom von $\sqrt[n]{p}$ über $\mathbb{Q}$. Also gilt stets $[\sqrt[n]{p} : \mathbb{Q}] = n$. Dies verallgemeinert die Ergebnisse von Beispiel 2.9 (b) und (c).

**Aufgabe 3.11.** Zu einer Körpererweiterung $L/K$ bezeichne $\overline{K}^L \subset L$ die Menge aller Elemente von $L$, die über $K$ algebraisch sind. Man zeige:

(a) $\overline{K}^L$ ist ein Körper.

(b) Die Körpererweiterung $\overline{\mathbb{Q}}^{\mathbb{R}}/\mathbb{Q}$ ist algebraisch, aber nicht endlich.

**Aufgabe 3.12** (Varianten des Irreduzibilitätskriteriums von Eisenstein)**.** Es sei $f = t^n + a_{n-1}t^{n-1} + \cdots + a_0 \in \mathbb{Z}[t]$ ein ganzzahliges normiertes Polynom vom Grad $n \geq 2$, so dass kein Teiler von $a_0$ eine Nullstelle von $f$ ist. Man zeige, dass $f$ dann irreduzibel in $\mathbb{Z}[t]$ und damit auch in $\mathbb{Q}[t]$ ist, wenn eine der folgenden beiden Bedingungen gilt:

(a) $p \,|\, a_i$ für alle $i = 0, \ldots, n-2$ sowie $p^2 \nmid a_0$;

(b) $p \,|\, a_i$ für alle $i = 0, \ldots, n-1$ sowie $p^2 \nmid a_1$.

04

Für den Rest dieses Kapitels wollen wir nun mit Hilfe der bisherigen Resultate die Minimalpolynome und Grade der Zahlen $e^{\frac{2\pi i}{n}}$ über $\mathbb{Q}$ bestimmen. Damit kommen wir dann auch bei unserer Frage nach der Konstruierbarkeit mit Zirkel und Lineal weiter — da wir ja aus Beispiel 1.23 (C) schon wissen, dass das regelmäßige $n$-Eck genau dann mit Zirkel und Lineal konstruierbar ist, wenn $e^{\frac{2\pi i}{n}}$ in einer 2-Radikalerweiterung liegt, und dies nach Folgerung 2.22 (b) höchstens dann möglich ist, wenn $[e^{\frac{2\pi i}{n}} : \mathbb{Q}]$ eine Zweierpotenz ist.

Da die komplexen Zahlen der Form $e^{\frac{2\pi i}{n}}$, oder allgemeiner die Lösungen der Gleichung $t^n - 1 = 0$, in der Praxis eine wichtige Rolle spielen, werden wir ihnen zunächst einen speziellen Namen geben.

**Definition 3.13** (Einheitswurzeln)**.** Es sei $n \in \mathbb{N}_{>0}$. Wir setzen

$$E_n := \{z \in \mathbb{C} : z^n = 1\} = \left\{e^{\frac{2\pi i k}{n}} : k \in \mathbb{Z}\right\} = \left\{e^{\frac{2\pi i k}{n}} : k = 0, \ldots, n-1\right\}$$

und nennen die Elemente von $E_n$ die **$n$-ten Einheitswurzeln**. Die Elemente der Teilmenge

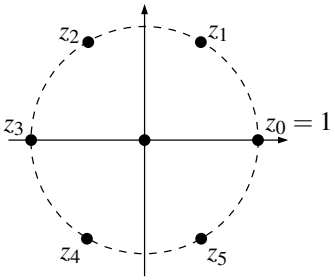
$$E_n' := \{z \in E_n : z^k \neq 1 \text{ für alle } k \text{ mit } 1 \leq k < n\},$$

also die $n$-ten Einheitswurzeln, für die $n$ auch die kleinste Potenz ist, bei der wieder 1 herauskommt, werden **primitive $n$-te Einheitswurzeln** genannt.

**Beispiel 3.14.**

(a) Für $n = 1$ ist offensichtlich ist $E_1 = E_1' = \{1\}$. Für $n = 2$ ergibt sich $E_2 = \{1, -1\}$ sowie $E_2' = \{-1\}$.

(b) Das Bild rechts zeigt die sechs 6-ten Einheitswurzeln $z_k := e^{\frac{2\pi i k}{6}}$ für $k = 0, \ldots, 5$. Von ihnen sind genau $z_1$ und $z_5$ primitiv — denn es ist ja $z_0^1 = z_2^3 = z_3^2 = z_4^3 = 1$, wohingegen alle Potenzen $z_1^m$ und $z_5^m$ für $m = 1, \ldots, 5$ ungleich 1 sind.




**Bemerkung 3.15.**

(a) Offensichtlich ist $E_n$ zusammen mit der Multiplikation eine Untergruppe von $(\mathbb{C}^*, \cdot) = (\mathbb{C}\backslash\{0\}, \cdot)$. In der Tat ist sie genau das Bild des Gruppenhomomorphismus

$$f : (\mathbb{Z}, +) \to (\mathbb{C}^*, \cdot), \quad k \mapsto e^{\frac{2\pi i k}{n}}.$$

Da der Kern von $f$ genau $n\mathbb{Z}$ ist, folgt aus dem Homomorphiesatz [G, Satz 6.17], dass die Abbildung

$$g : (\mathbb{Z}_n, +) \to (E_n, \cdot), \quad \overline{k} \mapsto e^{\frac{2\pi i k}{n}}$$

ein Gruppenisomorphismus ist: die Gruppe $E_n$ der $n$-ten Einheitswurzeln ist isomorph zu $\mathbb{Z}_n$.

(b) Man kann leicht sehen, welche Einheitswurzeln primitiv sind: es sei dazu $z = e^{\frac{2\pi ik}{n}} \in E_n$. Dann gilt

$$\begin{aligned}
z \in E_n' &\Leftrightarrow \text{die Ordnung von } z \text{ in } \mathbb{C}^* \text{ ist } n && \text{(Definition 3.13)}\\
&\Leftrightarrow \text{die Ordnung von } \overline{k} \text{ in } \mathbb{Z}_n \text{ ist } n && \text{((a))}\\
&\Leftrightarrow \langle \overline{k} \rangle = \mathbb{Z}_n && \text{([G, Lemma 5.14])}\\
&\Leftrightarrow \overline{1} \in \langle \overline{k} \rangle = \{\overline{ak} : a \in \mathbb{Z}\}\\
&\Leftrightarrow \overline{k} \text{ ist eine Einheit in } \mathbb{Z}_n\\
&\Leftrightarrow \operatorname{ggt}(k,n) = 1 && \text{([G, Folgerung 10.31]).}
\end{aligned}$$

Unter dem Isomorphismus aus (a) entsprechen die primitiven $n$-ten Einheitswurzeln $E_n' \subset E_n$ also genau den Einheiten $\mathbb{Z}_n^* \subset \mathbb{Z}_n$; insbesondere ist damit $|E_n'| = |\mathbb{Z}_n^*|$. In Beispiel 3.14 (b) für $n = 6$ waren dies genau $e^{1 \cdot \frac{2\pi i}{6}}$ und $e^{5 \cdot \frac{2\pi i}{6}}$, entsprechend den Einheiten $\overline{1}$ und $\overline{5}$ in $\mathbb{Z}_6$, bzw. entsprechend den zu 6 teilerfremden Zahlen 1 und 5 in $\{0,\dots,5\}$.

Mit Hilfe der primitiven Einheitswurzeln können wir nun bereits die Polynome definieren, die sich später als die Minimalpolynome von $e^{\frac{2\pi i}{n}}$ herausstellen werden:

**Definition 3.16** (Kreisteilungspolynome)**.** Für $n \in \mathbb{N}_{>0}$ heißt

$$\Phi_n := \prod_{z \in E_n'} (t - z) \quad \in \mathbb{C}[t]$$

das **$n$-te Kreisteilungspolynom**.

**Beispiel 3.17.** Aus Beispiel 3.14 erhalten wir z. B.

$$\begin{aligned}
\Phi_1 &= t - 1,\\
\Phi_2 &= t + 1,\\
\Phi_6 &= \left(t - e^{\frac{2\pi i}{6}}\right)\left(t - e^{5 \cdot \frac{2\pi i}{6}}\right) = t^2 - t + 1.
\end{aligned}$$

Für größere $n$ ist die Berechnung von $\Phi_n$ direkt nach Definition 3.16 oft recht umständlich. Die folgende rekursive Formel ist hier in der Regel nützlicher.

**Lemma 3.18** (Rekursive Formel für die Kreisteilungspolynome)**.** *Für alle $n \in \mathbb{N}_{>0}$ ist $E_n$ die disjunkte Vereinigung aller $E_d'$ mit $d \mid n$. Insbesondere gilt also*

$$t^n - 1 \;= \prod_{d \mid n} \Phi_d \quad \in \mathbb{C}[t].$$

*Beweis.* Nach Bemerkung 3.15 (b) ist $E_d'$ genau die Menge aller Elemente der Ordnung $d$ in $\mathbb{C}^*$. Insbesondere ist die Vereinigung aller $E_d'$ also disjunkt.

Ist nun $z \in E_n$, so ist die Ordnung $d$ von $z$ nach [G, Folgerung 5.15 (a)] ein Teiler von $|E_n| = n$, also ist dann auch $z \in E_d'$ für ein $d \mid n$. Ist umgekehrt $z \in E_d'$ für ein $d \mid n$, so folgt mit $z^d = 1$ natürlich auch $z^n = 1$ und damit $z \in E_n$. Insgesamt zeigt dies, dass $E_n$ die disjunkte Vereinigung aller $E_d'$ mit $d \mid n$ ist.

Die behauptete Gleichheit von Polynomen folgt nun unmittelbar, da auf beiden Seiten offensichtlich das (eindeutig bestimmte) normierte Polynom vom Grad $n$ mit den Nullstellen $E_n$ steht. □

**Beispiel 3.19.**

(a) Für $n = 6$ liefert Lemma 3.18 die disjunkte Zerlegung $E_6 = E_6' \cup E_3' \cup E_2' \cup E_1'$. Dies hatten wir in Beispiel 3.14 (b) auch schon direkt gesehen: mit der dortigen Bezeichnung $z_k = e^{\frac{2\pi ik}{6}}$ für $k = 0,\dots,5$ ist $E_6 = \{z_0,\dots,z_5\}$, $E_6' = \{z_1, z_5\}$, $E_3' = \{z_2, z_4\}$, $E_2' = \{z_3\}$ und $E_1' = \{z_0\}$.

(b) Ist $p$ eine Primzahl, so liefert die Formel aus Lemma 3.18

$$t^p - 1 = \Phi_p \cdot \Phi_1 = \Phi_p \cdot (t-1)$$

und damit nach der endlichen geometrischen Reihe

$$\Phi_p = \frac{t^p - 1}{t-1} = t^{p-1} + t^{p-2} + \cdots + t + 1.$$

(c) Allgemeiner kann man für alle $n \in \mathbb{N}_{>0}$ die Formel aus Lemma 3.18 zu der Gleichung

$$\Phi_n = (t^n - 1) \Big/ \prod_{\substack{d \mid n \\ d < n}} \Phi_d$$

umstellen, mit der man alle $\Phi_n$ leicht durch rekursive Polynomdivision berechnen kann.

**Aufgabe 3.20.** Man zeige:

(a) $\Phi_{p^r}(t) = \Phi_p(t^{p^{r-1}})$ für jede Primzahl $p$ und alle $r \geq 1$;

(b) $\Phi_{2n}(t) = \Phi_n(-t)$ für alle ungeraden $n > 1$.

Obwohl Definition 3.16 komplexe Zahlen benutzt und damit a priori komplexe Polynome liefert, haben sich alle unsere bisher berechneten Kreisteilungspolynome in den Beispielen 3.17 und 3.19 (b) als ganzzahlig herausgestellt. Dies ist kein Zufall, wie der folgende Satz zeigt.

**Satz 3.21** (Ganzzahligkeit der Kreisteilungspolynome)**.** *Für alle $n \in \mathbb{N}_{>0}$ gilt $\Phi_n \in \mathbb{Z}[t]$.*

*Beweis.* Wir zeigen die Behauptung mit Induktion über $n$; der Induktionsanfang für $n = 1$ ist klar wegen $\Phi_1 = t - 1$.

Für den Induktionsschritt sei nun $n \in \mathbb{N}_{>1}$. Nach Induktionsvoraussetzung ist dann

$$f_n := \prod_{\substack{d \mid n \\ d < n}} \Phi_d \quad \in \mathbb{Z}[t]$$

ein normiertes ganzzahliges Polynom. Wir können nun $t^n - 1$ in $\mathbb{Q}[t]$ mit Rest durch $f_n$ dividieren und erhalten

$$t^n - 1 = q f_n + r \quad \in \mathbb{Q}[t]$$

für gewisse $q, r \in \mathbb{Q}[t]$ mit $\deg r < \deg f_n$. Außerdem ergibt Lemma 3.18

$$t^n - 1 = \Phi_n f_n \quad \in \mathbb{C}[t].$$

Subtraktion dieser beiden Gleichungen voneinander liefert nun

$$(\Phi_n - q) f_n = r \quad \in \mathbb{C}[t],$$

nach der Gradformel [G, Lemma 9.9 (a)] also $\deg(\Phi_n - q) + \deg f_n = \deg r$. Wegen $\deg r < \deg f_n$ ist dies aber nur dann möglich, wenn $\deg(\Phi_n - q) = \deg r = -\infty$, also $\Phi_n - q = r = 0$ ist. Insbesondere ist damit $\Phi_n = q \in \mathbb{Q}[t]$. Aus der Gleichung $t^n - 1 = \Phi_n f_n$ in $\mathbb{Q}[t]$ ergibt sich dann mit Folgerung 3.4 auch sofort $\Phi_n \in \mathbb{Z}[t]$. □

**Bemerkung 3.22.** Berechnet man z. B. mit Hilfe der Rekursionsformel aus Lemma 3.18 einmal einige Kreisteilungspolynome, so stellt man schnell fest, dass die Koeffizienten dieser Polynome nicht nur ganzzahlig, sondern „sehr oft“ sogar nur 0, 1 oder $-1$ sind — allerdings mit einer kaum zu durchschauenden Verteilung. So ist z. B.

$$\Phi_{42} = t^{12} + t^{11} - t^9 - t^8 + t^6 - t^4 - t^3 + t + 1.$$

In der Tat ist das erste(!) Kreisteilungspolynom, das überhaupt einen Koeffizienten vom Betrag größer als 1 besitzt,

$$\begin{aligned}\Phi_{105} = {} & t^{48} + t^{47} + t^{46} - t^{43} - t^{42} - 2t^{41} - t^{40} - t^{39} + t^{36} + t^{35} + t^{34} + t^{33} + t^{32} + t^{31} - t^{28} - t^{26} \\ & - t^{24} - t^{22} - t^{20} + t^{17} + t^{16} + t^{15} + t^{14} + t^{13} + t^{12} - t^9 - t^8 - 2t^7 - t^6 - t^5 + t^2 + t + 1.\end{aligned}$$

Dennoch kann man ebenfalls zeigen, dass die Menge aller in den Kreisteilungspolynomen auftretenden Koeffizienten unbeschränkt ist.

Fassen wir unsere bisherigen Ergebnisse zu den Kreisteilungspolynomen zusammen, so wissen wir also, dass $\Phi_n$ ein normiertes, ganzzahliges (und damit insbesondere rationales) Polynom mit Nullstelle $e^{\frac{2\pi i}{n}}$ ist. Um zu zeigen, dass $\Phi_n$ wirklich das Minimalpolynom von $e^{\frac{2\pi i}{n}}$ ist, bleibt also nach Lemma 2.6 nur noch seine Irreduzibilität zu zeigen. Allerdings ist leider keines unserer bisherigen Irreduzibilitätskriterien auf die Kreisteilungspolynome anwendbar; wir müssen hierfür also einen neuen Beweis angeben. Wie unsere bisherigen Kriterien benutzt auch dieser (nicht ganz einfache) Beweis Reduktion modulo einer Primzahl. Er verwendet die folgenden beiden Hilfsaussagen, die wir beide später in dieser Vorlesung noch einmal wiedersehen werden.

**Lemma 3.23** (Rechenregeln für Potenzen in $\mathbb{Z}_p$)**.** *Für $a \in \mathbb{Z}_p$ und $f, g \in \mathbb{Z}_p[t]$ gelten die folgenden einfachen Rechenregeln:*

(a) $(f+g)^p = f^p + g^p$;

(b) $a^p = a$;

(c) $f(t^p) = f(t)^p$.

*Beweis.*

(a) Nach der binomischen Formel gilt zunächst natürlich

$$(f+g)^p = \sum_{i=0}^{p} \binom{p}{i} f^i g^{p-i} = f^p + g^p + \sum_{i=1}^{p-1} \binom{p}{i} f^i g^{p-i}.$$

Nun ist $p$ aber für $i = 1, \ldots, p-1$ ein Teiler des Binomialkoeffizienten

$$\binom{p}{i} = \frac{p \cdot (p-1) \cdot \cdots \cdot (p-i+1)}{1 \cdot 2 \cdot \cdots \cdot i},$$

da $p$ zwar im Zähler, aber nicht im Nenner dieses Bruches auftritt. Also ist dieser Binomialkoeffizient gleich Null in $\mathbb{Z}_p$, woraus die Behauptung folgt.

(b) Für $a = 0$ ist die Aussage natürlich klar. Andernfalls ist $a \in \mathbb{Z}_p^*$ eine Einheit, da $\mathbb{Z}_p$ ein Körper ist. Wegen $|\mathbb{Z}_p^*| = |p-1|$ folgt aus dem kleinen Satz von Fermat [G, Folgerung 5.15 (b)] also $a^{p-1} = 1$ und damit $a^p = a$.

(c) Ist $f = \sum_n a_n t^n$, so folgt

$$f(t)^p = \Big(\sum_n a_n t^n\Big)^p \overset{(a)}{=} \sum_n a_n^p t^{pn} \overset{(b)}{=} \sum_n a_n t^{pn} = f(t^p). \qquad \square$$

**Lemma 3.24** (Formale Ableitungen)**.** *Für ein Polynom $f = \sum_n a_n t^n \in K[t]$ über einem Körper $K$ betrachten wir die **formale Ableitung** $f' := \sum_n n a_n t^{n-1}$. Für diese gilt:*

(a) *Für alle $f, g \in K[t]$ ist $(f+g)' = f' + g'$ und $(fg)' = f'g + fg'$.*

(b) *Ist $f \in K[t]$ ein Polynom, das teilerfremd zu seiner formalen Ableitung $f'$ ist, so hat $f$ keine mehrfachen Faktoren in seiner Primfaktorzerlegung (und damit insbesondere keine mehrfachen Nullstellen).*

*Beweis.*

(a) Dies ergibt sich durch einfaches Nachrechnen, siehe z. B. [G, Aufgabe 9.10].

(b) Angenommen, $f$ hätte einen mehrfachen Faktor in seiner Primfaktorzerlegung, d. h. es wäre $f = g^2 h$ für $g, h \in K[t]$ mit $\deg g > 0$. Anwenden der Differentiationsregeln aus (a) ergibt dann

$$f' = 2gg'h + g^2 h' = g(2g'h + gh'),$$

woraus wir sehen, dass $f$ und $f'$ im Widerspruch zur Annahme den gemeinsamen Teiler $g$ haben. $\square$

**Bemerkung 3.25.** Die Rechenregeln aus Lemma 3.24 (a) sind euch für reelle Polynome und die in der Analysis definierte Ableitung natürlich bereits aus der Schule bzw. aus den „Grundlagen der Mathematik“ bekannt. Auch die Aussage aus Teil (b) habt ihr dort vielleicht schon einmal gesehen — zumindest wohl in der Form, dass mehrfache Nullstellen eines Polynoms auch Nullstellen seiner Ableitung sind. Die besondere Aussage in Lemma 3.24 ist, dass dies nicht nur über $\mathbb{R}$, sondern für die nun rein formal definierte Ableitung auch über jedem beliebigen Körper gilt. In der Tat werden wir dieses Resultat im Beweis der Irreduzibilität der Kreisteilungspolynome für die endlichen Körper $\mathbb{Z}_p$ anwenden, und zwar für das folgende Beispiel.

**Beispiel 3.26.** Wir betrachten das Polynom $f = t^n - 1$ über einem Körper $K$. Offensichtlich ist $f' = nt^{n-1}$.

(a) Ist $\operatorname{char} K$ kein Teiler von $n$ (z. B. im Fall $\operatorname{char} K = 0$), so ist $n \neq 0$ in $K$ und damit $f' \neq 0$. Da die Primfaktorzerlegung von $f'$ dann $t$ als einzigen Primfaktor enthält und dieser offensichtlich kein Teiler von $f$ ist, sind $f$ und $f'$ teilerfremd. Nach Lemma 3.24 (b) hat $f$ in diesem Fall also keine mehrfachen Faktoren. Für $K = \mathbb{C}$ wussten wir dies bereits, denn da hat $t^n - 1$ ja genau die $n$ verschiedenen Linearfaktoren $t - z$ für $z \in E_n$.

(b) Ist $\operatorname{char} K = p > 0$ ein Teiler von $n$, so ist $f' = 0$ das Nullpolynom. Damit sind $f$ und $f'$ nicht teilerfremd (jeder Teiler von $f$ ist ja auch einer von $f'$), d. h. Lemma 3.24 (b) ist nicht anwendbar. In der Tat kann es dann auch passieren, dass $f$ mehrfache Faktoren besitzt: für $n = p > 2$ und $K = \mathbb{Z}_p$ zum Beispiel ist $f = t^p - 1 = (t-1)^p$ nach Lemma 3.23 (a).

Mit diesen beiden Hilfsaussagen können wir nun wie angekündigt zeigen, dass $\Phi_n$ das Minimalpolynom von $e^{\frac{2\pi i}{n}}$ ist.

**Satz 3.27** (Irreduzibilität der Kreisteilungspolynome)**.** *Es sei $n \in \mathbb{N}_{>0}$. Dann gilt:*

(a) *Ist $z \in E_n$ eine $n$-te Einheitswurzel und $m \in \mathbb{N}_{>0}$ mit $\operatorname{ggt}(m,n) = 1$, so haben $z$ und $z^m$ dasselbe Minimalpolynom über $\mathbb{Q}$.*

(b) *$e^{\frac{2\pi i}{n}}$ hat das Minimalpolynom $\Phi_n$ über $\mathbb{Q}$. Insbesondere ist $\Phi_n$ also irreduzibel in $\mathbb{Q}[t]$.*

*Beweis.*

(a) Wir betrachten zunächst den Spezialfall, dass $m = p$ eine Primzahl ist. Es seien $f$ und $g$ die Minimalpolynome von $z$ bzw. $z^p$ in $\mathbb{Q}[t]$. Wir machen einen Widerspruchsbeweis und nehmen also an, dass $f \neq g$.

(1) Natürlich ist $t^n - 1 \in \mathbb{Z}[t]$ ein normiertes Polynom mit Nullstellen $z$ und $z^p$. Nach Bemerkung 2.5 sind die Minimalpolynome $f$ und $g$ dann Teiler von $t^n - 1$. Da sie irreduzibel sind und wir sie als verschieden angenommen haben, gilt also $t^n - 1 = f \cdot g \cdot h$ für ein (ebenfalls normiertes) Polynom $h \in \mathbb{Q}[t]$. Mit Folgerung 3.4 sehen wir, dass dann sogar $f, g, h \in \mathbb{Z}[t]$ gelten muss. Wir können die Gleichung also modulo $p$ reduzieren und erhalten $t^n - 1 = \overline{f} \cdot \overline{g} \cdot \overline{h}$ in $\mathbb{Z}_p[t]$. Da nach Voraussetzung $p \nmid n$ gilt, hat nun $t^n - 1$ nach Beispiel 3.26 (a) keine mehrfachen Nullstellen in $\mathbb{Z}_p[t]$. Damit müssen $\overline{f}$ und $\overline{g}$ in $\mathbb{Z}_p[t]$ offensichtlich teilerfremd sein, denn ein gemeinsamer Teiler von ihnen wäre ja ein quadratischer Teiler von $t^n - 1 \in \mathbb{Z}_p[t]$.

(2) Andererseits ist $z$ nach Konstruktion von $g$ auch eine Nullstelle von $g(t^p)$. Also muss das Minimalpolynom $f$ von $z$ nach Bemerkung 2.5 ein Teiler von $g(t^p)$ sein, d. h. es gibt ein Polynom $k \in \mathbb{Q}[t]$ mit $g(t^p) = f \cdot k$. Wir haben $f$ und $g$ (und damit auch $g(t^p)$) aber oben schon als ganzzahlige Polynome erkannt, und damit ist nach Folgerung 3.4 auch $k \in \mathbb{Z}[t]$. Wir können unsere Gleichung also wieder modulo $p$ reduzieren und erhalten nach Lemma 3.23 (c)

$$\overline{f} \cdot \overline{k} = \overline{g(t^p)} = \overline{g}^p \quad \in \mathbb{Z}_p[t].$$

Dies ist aber nur möglich, wenn jeder Primfaktor von $\overline{f}$ auch einer von $\overline{g}$ ist — im Widerspruch zum Resultat von (1). Dies zeigt die Behauptung (a) für den Fall, dass $m = p$ eine Primzahl ist.

Fortgesetzte Anwendung dieses Ergebnisses liefert nun sofort, dass auch die Zahlen $z$ und $z^{p_1 \cdots p_r} = ((z^{p_1}) \cdots)^{p_r}$ das gleiche Minimalpolynom haben, sofern die Primzahlen $p_1, \ldots, p_r$ keine Teiler von $n$ sind. Da sich jede Zahl $m$ mit $\operatorname{ggt}(m,n) = 1$ als Produkt derartiger Primzahlen schreiben lässt, folgt damit die Behauptung (a).

(b) Das Minimalpolynom von $z = e^{\frac{2\pi i}{n}}$ muss nach (a) auch alle $z^m$ mit $\operatorname{ggt}(m,n) = 1$ als Nullstellen haben. Dies sind nach Bemerkung 3.15 (b) aber genau die primitiven Einheitswurzeln. Damit kann der Grad des Minimalpolynoms von $z$ nicht kleiner als $|E_n'|$ sein. Da dies nach Definition 3.16 aber genau der Grad von $\Phi_n$ ist, sehen wir, dass $\Phi_n$ wirklich das normierte Polynom minimalen Grades mit Nullstelle $z$, also das Minimalpolynom von $z$ ist. Insbesondere ist $\Phi_n$ nach Lemma 2.6 damit irreduzibel in $\mathbb{Q}[t]$. □

**Bemerkung 3.28.** Da $\Phi_n$ die primitiven $n$-ten Einheitswurzeln als Nullstellen hat, normiert und nach Satz 3.27 (b) auch irreduzibel in $\mathbb{Q}[t]$ ist, sehen wir als leichte Verallgemeinerung von Satz 3.27 (b), dass $\Phi_n$ nicht nur das Minimalpolynom von $e^{\frac{2\pi i}{n}}$, sondern sogar von jeder primitiven $n$-ten Einheitswurzel ist.

Nachdem wir nun die Minimalpolynome $\Phi_n$ der Einheitswurzeln $e^{\frac{2\pi i}{n}}$ kennen, wollen wir natürlich auch noch den Grad dieser Polynome bestimmen. Dieser ist nach Konstruktion genau $|E_n'|$, also $|\mathbb{Z}_n^*|$ nach Bemerkung 3.15 (b). Wenn ihr die Vorlesung „Elementare Zahlentheorie“ schon gehört habt, wisst ihr bereits, was hierbei herauskommt:

**Satz 3.29** (Grad der Kreisteilungspolynome)**.** *Es sei $n \in \mathbb{N}_{>0}$ eine natürliche Zahl mit Primfaktorzerlegung $n = p_1^{k_1} \cdot \cdots \cdot p_r^{k_r}$ (für verschiedene Primzahlen $p_1, \ldots, p_r$). Dann gilt für jede primitive $n$-te Einheitswurzel $z$*

$$[z : \mathbb{Q}] = \deg \Phi_n = |E_n'| = |\mathbb{Z}_n^*| = \varphi(n),$$

*wobei $\varphi$ die **Eulersche $\varphi$-Funktion***

$$\varphi(n) := \prod_{i=1}^{r} (p_i - 1)\, p_i^{k_i - 1}$$

*ist.*

*Beweis.* Die erste Gleichheit ist Bemerkung 3.28, die zweite folgt aus Definition 3.16, und die dritte aus Bemerkung 3.15 (b). Es bleibt also nur noch die letzte Gleichheit, d. h. die Anzahl der Einheiten in $\mathbb{Z}_n$ zu berechnen. Wir tun dies in zwei Schritten:

1. Fall: $n = p^k$ ist eine Primzahlpotenz. Die *Nichteinheiten* von $\mathbb{Z}_n$ sind dann genau $\overline{m}$ für alle $m = 0, \ldots, p^k - 1$, die einen gemeinsamen Teiler mit $p^k$ haben [G, Folgerung 10.31]. Dies sind genau die Vielfachen von $p$, also die $p^{k-1}$ Zahlen $m = i\,p$ mit $i = 0, \ldots, p^{k-1} - 1$. Damit folgt $|\mathbb{Z}_{p^k}^*| = n - p^{k-1} = (p-1)\,p^{k-1}$.

2. Fall: $n = p_1^{k_1} \cdot \cdots \cdot p_r^{k_r}$ ist eine beliebige natürliche Zahl. Nach dem chinesischen Restsatz [G, Satz 11.22] gilt dann

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{k_1}} \times \cdots \times \mathbb{Z}_{p_r^{k_r}}.$$

Da ein Element in einem Produktring nach Definition der Ringstruktur offensichtlich genau dann eine Einheit ist, wenn jede Komponente eine Einheit ist, folgt daraus auch

$$\mathbb{Z}_n^* \cong \left(\mathbb{Z}_{p_1^{k_1}}\right)^* \times \cdots \times \left(\mathbb{Z}_{p_r^{k_r}}\right)^*$$

Nach dem 1. Fall ergibt sich hieraus sofort die behauptete Formel $|\mathbb{Z}_n^*| = \varphi(n)$. □

05

**Aufgabe 3.30.** Man zeige: ist $n > 2$, so gilt $\left[z + \frac{1}{z} : \mathbb{Q}\right] = \frac{1}{2}\varphi(n)$ für jede primitive $n$-te Einheitswurzel $z$.

Wie bereits angekündigt hat Satz 3.29 natürlich eine unmittelbare Anwendung auf die Frage nach der Konstruierbarkeit des regelmäßigen $n$-Ecks mit Zirkel und Lineal. Dazu müssen wir nach Beispiel 2.23 (C) herausfinden, wann $[e^{\frac{2\pi i}{n}} : \mathbb{Q}] = \varphi(n)$ eine Zweierpotenz ist.

**Lemma 3.31.** *Es sei $n \in \mathbb{N}_{>0}$. Dann ist $\varphi(n)$ genau dann eine Zweierpotenz, wenn $n$ von der Form*

$$n = 2^m \cdot p_1 \cdot \cdots \cdot p_r$$

*ist, wobei $r, m \geq 0$ gilt und $p_1, \ldots, p_r$ verschiedene Primzahlen der Form $p_i = 2^{2^{a_i}} + 1$ mit $a_1, \ldots, a_r \in \mathbb{N}$ sind.*

*Beweis.* Hat $n$ die angegebene Form, so ist nach Satz 3.29

$$\varphi(n) = \begin{cases} \prod_{i=1}^r 2^{2^{a_i}} & \text{für } m = 0, \\ 2^{m-1} \cdot \prod_{i=1}^r 2^{2^{a_i}} & \text{für } m > 0 \end{cases}$$

eine Zweierpotenz. Hat umgekehrt $n$ die allgemeine Primfaktorzerlegung $n = p_1^{k_1} \cdot \cdots \cdot p_r^{k_r}$ und ist

$$\varphi(n) = \prod_{i=1}^r (p_i - 1)\, p_i^{k_i - 1}$$

eine Zweierpotenz, so können ungerade Primfaktoren wegen des Faktors $p_i^{k_i-1}$ in $\varphi(n)$ offensichtlich nur einfach auftreten, und wegen des Faktors $p_i - 1$ müssen sie von der Form $p_i = 2^{b_i} + 1$ für gewisse $b_i \in \mathbb{N}_{>0}$ sein.

Es bleibt also nur noch zu zeigen, dass eine Zahl der Form $2^b + 1$ nur dann eine Primzahl sein kann, wenn $b$ selbst eine Zweierpotenz ist. Nehmen wir also an, $b$ wäre keine Zweierpotenz. Dann könnten wir $b$ als $b = qc$ mit ungeradem $q > 1$ und geeignetem $c < b$ schreiben. Setzen wir in der Identität

$$x^q - y^q = (x - y) \cdot (x^{q-1} + x^{q-2}y + \cdots + xy^{q-2} + y^{q-1})$$

dann $x = 2^c$ und $y = -1$ ein, so ist die linke Seite gleich $2^b + 1$, und auf der rechten Seite haben wir den nicht-trivialen Faktor $x - y = 2^c + 1$. Also kann $2^b + 1$ dann nicht prim sein, was zu zeigen war. □

**Bemerkung 3.32** (Fermatsche Primzahlen)**.** Die in Lemma 3.31 auftretenden Primzahlen der Form $2^{2^a} + 1$ für $a \in \mathbb{N}$ nennt man **Fermatsche Primzahlen**. Die ersten Zahlen dieser Form sind

| $a$ | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| $2^{2^a} + 1$ | 3 | 5 | 17 | 257 | 65537 |

und dies sind in der Tat alles Primzahlen. Als man die Zahlen der Form $2^{2^a} + 1$ zuerst untersucht hat (und numerisch nicht weiter als bis $a = 4$ gekommen ist, weil es Taschenrechner ja noch nicht gab), hat man mit „naiver Induktion“ aus der obigen Tabelle vermutet, dass alle Zahlen dieser Form Primzahlen sind. Heute wissen wir es jedoch besser: schon $2^{2^5} + 1 = 4294967297 = 641 \cdot 6700417$ ist zusammengesetzt, und in der Tat hat man bisher noch *gar keine* weitere Primzahl der Form $2^{2^a} + 1$ für $a > 4$ gefunden.

**Folgerung 3.33** (Notwendige Bedingung für die Konstruierbarkeit des $n$-Ecks)**.** *Das regelmäßige $n$-Eck ist höchstens dann mit Zirkel und Lineal konstruierbar, wenn $n$ von der Form*

$$n = 2^m \cdot p_1 \cdot \cdots \cdot p_r$$

*für ein $m \geq 0$ und verschiedene Fermatsche Primzahlen $p_1, \ldots, p_r$ ist.*

*Beweis.* Nach Beispiel 1.23 (C) ist das regelmäßige $n$-Eck genau dann mit Zirkel und Lineal konstruierbar, wenn $e^{\frac{2\pi i}{n}}$ in einer 2-Radikalerweiterung von $\mathbb{Q}$ liegt. Dies ist nach Folgerung 2.22 (b) aber höchstens dann möglich, wenn der Grad $[e^{\frac{2\pi i}{n}} : \mathbb{Q}]$ eine Zweierpotenz ist. Da dieser Grad nach Satz 3.29 gleich $\varphi(n)$ ist, folgt die Behauptung also aus Lemma 3.31. □

**Bemerkung 3.34.** Die ersten $n$-Ecke, die nach dem Kriterium aus Folgerung 3.33 nicht mit Zirkel und Lineal konstruierbar sind, sind $n = 7$, 9, 11, 13 und 14. In allen anderen Fällen mit $n \leq 17$ ist $\varphi(n)$ nach Lemma 3.31 eine Zweierpotenz — was bedeutet, dass wir dann mit unseren bisherigen Ergebnissen noch keine Aussage über die Konstruierbarkeit machen können. Erst in Folgerung 7.8 werden wir mit Hilfe der Galoistheorie sehen, dass die Bedingung in Folgerung 3.33 in der Tat auch

hinreichend ist und alle $n$-Ecke, für die $\varphi(n)$ eine Zweierpotenz ist, auch wirklich mit Zirkel und Lineal konstruiert werden können.