# Kapitel 4
# Nullstellen und Körpererweiterungen

## §1: Zerfällungskörper und der Fundamentalsatz der Algebra

Ist $k$ ein Körper und $f \in k[X]$ ein irreduzibles Polynom vom Grad mindestens zwei, so hat $f$ in $k$ keine Nullstelle. Wir kennen aber bereits viele Fälle, in denen es einen größeren Körper $K$ gibt, in dem $f$ eine oder mehrere Nullstellen hat. Solche Körper lassen sich auf verschiedene Weisen konstruieren: Ist etwa $k = \mathbb{Q}$ und $f = X^2 - 2$, so können wir bekanntlich mit dem Verfahren von HENON durch die Iteration

$$x_0 = 1, \qquad x_n = \frac{1}{2}\left(x_{n-1} + \frac{2}{x_{n-1}}\right) \quad \text{für alle } n \in \mathbb{N}$$

immer bessere Näherungslösungen konstruieren, und wenn wir die rationalen Zahlen durch Hinzunahme aller Grenzwerte von CAUCHY-Folgen (oder Intervallschachtelungen) zu den reellen Zahlen erweitern, ist dort der Grenzwert

$$x = \lim_{n\to\infty} x_n$$

dieser Folge eine Lösung.

Für die Nullstellen des Polynoms $X^2 + 1$ ist ein solcher Ansatz nicht möglich; hier müssen wir die „imaginäre Einheit“ $i$ einführen als „Symbol“ mit dem wir rechnen. Ähnlich hatten wir uns bereits gegen Ende des vorigen Kapitels überlegt, daß wir zu jedem Körper $k$ und jedem irreduziblen Polynom über $f$ einen größeren Körper finden können, in dem $f$ eine Nullstelle hat. Diesen Ansatz wollen wir nun systematisch ausbauen.

Beginnen wir mit Körpererweiterungen:

**Definition:** Sind $k \subseteq K$ zwei Körper, so bezeichnen wir $k$ als *Teilkörper* von $K$ und $K$ als *Erweiterungskörper* von $k$. Wir sagen auch, $K/k$, gesprochen $K$ über $k$, sei eine *Körpererweiterung*.

Ist $K/k$ eine Körpererweiterung, so ist $K$ ein $k$-Vektorraum, denn $K$ ist bezüglich seiner Addition eine abelsche Gruppe, und die Einschränkung der Multiplikation in $K$ auf $k \times K$ ist die Multiplikation der „Skalare“ aus $k$ mit den „Vektoren“ aus $K$. Klassisches Beispiel ist die Betrachtung des Körpers $\mathbb{C}$ der komplexen Zahlen als zweidimensionalen Vektorraum $\mathbb{R}^2$.

Im allgemeinen muß dieser Vektorraum nicht endlichdimensional sein: $\mathbb{R}$ kann beispielsweise unmöglich ein endlichdimensionaler $\mathbb{Q}$-Vektorraum sein, denn genau wie $\mathbb{Q}$ ist auch jeder Vektorraum $\mathbb{Q}^n$ abzählbar, aber $\mathbb{R}$ ist überabzählbar.

**Definition:** Ist $K$ ein endlichdimensionaler $k$-Vektorraum, sagen wir, die Körpererweiterung sei endlich, und wir bezeichnen die Dimension des $k$-Vektorraums $K$ als deren Grad $[K : k]$. Andernfalls sagen wir, sie sei unendlich und schreiben $[K : k] = \infty$.

Als Beispiel betrachten wir ein irreduzibles Polynom $f \in k[X]$ vom Grad $d$ und den Faktorring $K = k[X]/(f)$. Wie wir gegen Ende des vorigen Kapitels gesehen haben, ist er ein Körper, und als Vektorraum hat er beispielsweise die Basis $1, x, \ldots, x^{d-1}$, wobei $x = X + (f)$ die Restklasse von $X$ bezeichnet. Ist $f = a_d X^d + \cdots + a_0$ mit $a_d \neq 0$, so ist

$$X^d \equiv -\frac{a_{d-1}X^{d-1} + \cdots + a_1 X + a_0}{a_d} \bmod (f)$$

und damit

$$x^d = -\frac{a_{d-1}x^{d-1} + \cdots + a_1 x + a_0}{a_d} ,$$

so daß $x^d$ und die höheren Potenzen nicht zur Erzeugung gebraucht werden. Die genannten Elemente sind auch linear unabhängig über $k$, denn falls es Elemente $\lambda_i \in k$ gibt, so daß

$$\lambda_0 \cdot 1 + \lambda_1 \cdot x + \cdots + \lambda_{d-1} \cdot x^{d-1} = 0$$

ist, so muß das Polynom $\lambda_0 + \lambda_1 \cdot X + \cdots + \lambda_{d-1} \cdot X^{d-1}$ in $k[X]$ durch $f$ teilbar sein. Da sein Grad höchstens gleich $d-1$ sein kann, geht das nur, wenn es das Nullpolynom ist, wenn also alle $\lambda_i$ verschwinden.

Wir können dieses Ergebnis und die Diskussion im vorigen Kapitel zusammenfassen zum

**Lemma:** Ist $f \in k[X]$ ein irreduzibles Polynom vom Grad $d \geq 1$, so ist $K = k[X]/(f)$ ein Erweiterungskörper vom Grad $d$, in dem $f$ mindestens eine Nullstelle hat. ∎

Sind $L/K$ und $K/k$ zwei Körpererweiterungen, so ist auch $L/k$ eine; hier gilt:

**Lemma:** *a)* Sind $L/K$ und $K/k$ zwei endliche Körpererweiterungen, so ist auch $L/k$ eine endliche Körpererweiterung und

$$[L : k] = [L : K] \cdot [K : k] .$$

*b)* Ist $L/k$ eine endliche Körpererweiterung und ist $k \subseteq K \subseteq L$, so sind sowohl $L/K$ als auch $K/k$ endliche Körpererweiterungen. Ist $[L : k] = [K : k]$, so ist $K = L$.

*Beweis: a)* $b_1, \ldots, b_r$ seine eine Basis von $K$ als $k$-Vektorraum, und $c_1, \ldots, c_s$ sei eine Basis von $L$ als $K$-Vektorraum. Dann können wir in $L$ die $rs$-Produkte $b_i c_j$ bilden, und wollen uns überlegen, daß diese eine Basis des $k$-Vektorraums $L$ bilden.

Zunächst erzeugen sie diesen Vektorraum, denn jedes $v \in L$ läßt sich als Linearkombination

$$v = \lambda_1 c_1 + \cdots + \lambda_s c_s \quad \text{mit} \quad \lambda_j \in K$$

schreiben, und jedes $\lambda_j$ läßt sich schreiben als

$$\lambda_j = \mu_{1j} b_1 + \cdots + \mu_{rj} b_r \quad \text{mit} \quad \mu_{ij} \in k .$$

Setzt man dies in die darüberliegende Formelzeile ein, erhält man $v$ als Summe aller $\mu_{ij} b_i c_j$.

Zum Beweis der linearen Unabhängigkeit nehmen wir an,

$$\sum_{i=1}^{r}\sum_{j=1}^{s}\mu_{ij}b_ic_j = \sum_{j=1}^{s}\left(\sum_{i=1}^{r}\mu_{ij}b_i\right)c_j = 0$$

für irgendwelche Elemente $\mu_{ij} \in k$. Die Summen in der Klammer sind Elemente von $K$; wegen der linearen Unabhängigkeit der $c_j$ über $K$ müssen sie also alle verschwinden. Dann müssen aber auch alle $\mu_{ij}$ verschwinden, denn die $b_i$ sind linear unabhängig über $k$.

Somit ist $[L : k] = rs = [K : k] \cdot [L : K]$, wie behauptet.

*b)* Betrachten wir $K$ und $L$ als Vektorräume über $k$, so ist $K$ ein Untervektorraum von $L$, und natürlich sind Untervektorräume endlichdimensionaler Vektorräume selbst endlichdimensional. Wenn beide die gleiche Dimension haben, müssen sie sogar gleich sein. Als $K$-Vektorraum ist $L$ endlichdimensional, da eine $k$-Basis von $L$ insbesondere ein Erzeugendensystem von $L$ über dem größeren Körper $K$ ist.

■

Am einfachsten findet man die Nullstellen eines Polynoms, wenn das Polynom bereits als Produkt von Linearfaktoren gegeben ist. Wir wollen uns überlegen, daß es für jedes Polynom einen Körper gibt, über dem es so zerlegt werden kann:

**Definition:** $k$ sei ein Körper und $f \in k[X]$ sei ein Polynom. Ein Körper $K$ mit $k \subseteq K$ heißt *Zerfällungskörper* von $f$ über $k$, wenn gilt:

1.) Es gibt Elemente $z_1, \ldots, z_d \in K$ und $a \in k$, so daß im Polynomring $K[X]$ gilt $f = a(X - z_1) \cdots (X - z_n)$ .
2.) Ist $k \subseteq L \subseteq K$ und gibt es eine solche Zerlegung auch über $L$, so ist $L = K$.

In einem Zerfällungskörper *zerfällt* das Polynom also in ein Produkt von Linearfaktoren, und es gibt keinen echt kleineren Teilkörper, über dem dies bereits der Fall ist.

Für das Polynom $X^2 - 2 \in \mathbb{Q}[X]$ ist somit $\mathbb{Q} \oplus \mathbb{Q}\sqrt{2}$ ein Zerfällungskörper, denn $X^2 - 2 = (X + \sqrt{2})(X - \sqrt{2})$. Auch $\mathbb{Q}[X]/(X^2 - 2)$ ist ein Zerfällungskörper, denn bezeichnet $x$ die Restklasse von $X$, so ist auch $(X + x)(X - x) = X^2 - x^2 = X^2 - 2$.

**Satz:** $k$ sei ein Körper und $f \in k[X]$ ein Polynom. Dann gibt es einen Zerfällungskörper $K$ von $f$ über $k$.

*Beweis* durch Induktion nach $d = \deg f$: Für Polynome vom Grad Null gibt es nichts zu beweisen, für das Polynom $aX + b$ mit $a \neq 0$ ist $k$ selbst der Zerfällungskörper, denn

$$aX + b = a\left(X - \frac{(-b)}{a}\right) .$$

Sei nun $d > 1$ und $f \in k[X]$ ein Polynom vom Grad $d$. Weiter sei $g$ ein irreduzibler Faktor von $f$; für irreduzible $f$ setzen wir natürlich $g = f$. Wie wir aus dem Lemma zu Beginn dieses Paragraphen wissen, ist $k[X]/(g)$ ein Körper, in dem $g$ (mindestens) eine Nullstelle $z_1$ hat. Da es hierbei auf den Namen der Variablen nicht ankommt und wir $X$ im folgenden noch als Variable brauchen, betrachten wir stattdessen den Körper $k_1 = k[Y]/\big(g(Y)\big)$, wobei $g(Y)$ aus $g$ entsteht, indem wir $Y$ für die Variable $X$ einsetzen. Bezeichnet $z_1$ die Restklasse von $Y$ in $k_1$, ist also $g(z_1) = 0$ und damit auch $f(z_1) = 0$.

Nun betrachten wir $f$ und $g$ als Elemente des Polynomring $k_1[X]$; da $k$ ein Teilkörper von $k_1$ ist, geht das ohne Probleme. Da $f(z_1)$ verschwindet, ist $f$ dort ein Vielfaches von $(X - z_1)$. Sei etwa $f = (X - z_1) \cdot f_1$ mit einem Polynom $f_1 \in k_1[X]$ vom Grad $d - 1$. Nach Induktionsannahme gibt es einen Zerfällungskörper $K$ von $f_1$ über $k_1$. In diesem Körper läßt sich $f_1$ als Produkt von Linearfaktoren und einer Konstanten schreiben, also gibt es auch für $f = (X - z_1)f_1$ eine solche Darstellung

$$f = a(X - z_1)(X - z_2) \cdots (X - z_d) \quad \text{mit} \quad z_i \in K .$$

Der kleinste Teilkörper von $K$, der $k$ und alle $z_i$ enthält, ist somit ein Zerfällungskörper von $f$ über $k$.

∎

Für das Polynom $X^3 - 2$ über $\mathbb{Q}$ etwa konstruieren wir zunächst den Körper $k_1 = \mathbb{Q}[Y]/(Y^3 - 2)$; die Nebenklasse von $Y$ in $k_1$ bezeichnen wir als $z_1$. In $k_1$ ist dann $z_1^3 = 2$.

Nun dividieren wir $X^3 - 2 = X^3 - z_1^3$ in $k_1[X]$ durch $X - z_1$ und erhalten den Quotienten $f_1 = X^2 + z_1 X + z_1^2$. Mit einer neuen Variablen $Z$ bilden wir den neuen Faktorring $k_2 = k_1[Z]/(Z^2 + z_1 Z + z_1^2)$; die Restklasse

von $Z$ modulo $(f_1)$ sei $z_2$. In $k_2[X]$ ist $f_1$ durch $X - z_2$ teilbar, und da $f_2$ den Grad zwei hat, ist der Quotient linear. Somit liegen beide Nullstellen von $f_2$ in $k_2$; das Polynom $X^3 - 2$ zerfällt also über $k_2$ in Linearfaktoren.

$k_2$ ist ein zweidimensionaler $k_1$-Vektorraum mit Basis $1, z_2$, und $k_1$ ist ein dreidimensionaler $k_2$-Vektorraum mit Basis $1, z_1, z_1^2$. Als $k$-Vektorraum hat $k_2$ somit die Dimension sechs und die Basis $1, z_1, z_1^2, z_2, z_1 z_2, z_1^2 z_2$.

Wir können $k_1$ in $\mathbb{R}$ einbetten, indem wir $z_1$ auf $\sqrt[3]{2}$ abbilden. Dann haben wir für $z_2$ über $\mathbb{R}$ die quadratische Gleichung $z_2^2 + \sqrt[3]{2}\, z_2 \oplus \sqrt[3]{4} = 0$ mit Lösungen

$$\left(-\frac{1}{2} + \frac{1}{2}\sqrt{-3}\right) \sqrt[3]{2} \quad \text{und} \quad \left(-\frac{1}{2} - \frac{1}{2}\sqrt{-3}\right) \sqrt[3]{2}$$

in $\mathbb{C}$, wie erwartet. Wir hätten aber aber natürlich $k_1$ auch in $\mathbb{C}$ einbetten können, indem wir $z_1$ auf $\left(-\frac{1}{2} + \frac{1}{2}\sqrt{3}\right) \sqrt[3]{2}$ abbilden und hätten dann eine quadratische Gleichung mit komplexen Koeffizienten bekommen, die die konjugiert komplexe Zahl sowie $\sqrt[3]{2}$ als Lösungen hätte.

Es ist kein Wunder, daß die Gleichung in $\mathbb{C}$ drei Nullstellen hat; der sogenannte *Fundamentalsatz der Algebra* besagt, daß jedes Polynom mit komplexen Koeffizienten über $\mathbb{C}$ in Linearfaktoren zerfällt. Für diesen Satz gibt es mehrere Beweise, unter anderem über die Funktionentheorie oder mit Hilfe der algebraischen Topologie. Der folgende Beweis stammt aus dem Buch *Théorie algébrique des nombres* von PIERRE SAMUEL (Hermann, Paris, $^2$1971), und geht nach Angaben des Autors „im wesentlichen“ zurück auf LAGRANGE. Er verwendet nur elementare, aus der Analysisvorlesung bekannte Eigenschaften der reellen und komplexen Zahlen. Der wesentliche Beweisschritt ist der folgende

**Satz:** Jedes nichtkonstante Polynom $f \in \mathbb{R}[X]$ hat mindestens eine komplexe Nullstelle.

*Beweis:* Wir schreiben den Grad $d$ eines Polynoms in der Form $d = 2^n \cdot u$ mit $n \in \mathbb{N}_0$ und einer ungeraden Zahl $u$ und beweisen den Satz durch Induktion nach $n$.

Für den Induktionsanfang $n = 0$ müssen wir somit beweisen, daß jedes reelle Polynom ungeraden Grades mindestens eine komplexe Nullstelle hat. Da wir aus der Analysis wissen, daß es sogar eine reelle Nullstelle hat, ist das klar.

Nun sei $n > 0$; wir nehmen an, daß die Behauptung für alle Grade $d$, in deren Zerlegung ein kleineres $n$ auftaucht, bereits bewiesen sei, und betrachten ein Polynom $f \in \mathbb{R}[X]$ vom Grad $d = 2^n u$ mit irgendeinem ungeraden $u$. Wie wir wissen, gibt es einen Zerfällungskörper $K/\mathbb{R}$, über dem das Polynom in Linearfaktoren zerfällt. Die $d$ (nicht notwendigerweise verschiedenen) Nullstellen seien $z_1, \ldots, z_d$.

Mit diesen Nullstellen konstruieren wir nun neue Polynome, deren Grad zwar größer als $d$ ist, aber nur durch $2^{n-1}$ teilbar ist, so daß wir die Induktionsannahme anwenden können.

Zu jedem $\lambda \in \mathbb{R}$ betrachten wir für alle Paare $(i, j)$ mit $1 \leq i < j \leq d$ die Elemente

$$w_{ij}(\lambda) = z_i + z_j + \lambda z_i z_j \in K$$

sowie das Polynom

$$g_\lambda = \prod_{\substack{(i,j) \\ 1 \leq i < j \leq d}} \big(X - w_{ij}(\lambda)\big) \in K[X]\,.$$

Tatsächlich liegt $g_\lambda$ sogar in $\mathbb{R}[X]$, denn seine Koeffizienten sind nach dem Satz von VIÈTE (Kap. 1, §6) bis aufs Vorzeichen die elementarsymmetrischen Funktionen in den $w_{ij}(\lambda)$. Damit sind sie auch symmetrische Funktionen in den $z_i$, denn jede Permutation $z_i \mapsto z_{\pi(i)}$ führt zu einer Permutation $w_{ij}(\lambda) \mapsto w_{\pi(i)\pi(j)}(\lambda)$. Nach dem Hauptsatz über symmetrische Funktionen (Kap. 1, §7) lassen sie sich daher als Polynome in den elementarsymmetrischen Funktionen der $z_i$ schreiben, also, wieder nach VIÈTE, als Polynome in den Koeffizienten von $f$. Diese Koeffizienten sind reelle Zahlen; also sind auch die Koeffizienten aller $g_\lambda$ reelle Zahlen, d.h. $g_\lambda \in \mathbb{R}[X]$ für alle $\lambda$.

Da es $\frac{1}{2}d(d-1)$ Paare $(i, j)$ gibt, hat $g_\lambda$ den Grad

$$\frac{d(d-1)}{2} = \frac{2^n u(d-1)}{2} = 2^{n-1}u(d-1)\,.$$

Wegen $n \geq 1$ ist $d-1$ ungerade, also auch $u(d-1)$; die Grade der $g_\lambda$ sind daher nur durch $2^{n-1}$ teilbar, nicht aber durch $2^n$. Somit können wir die Induktionsvoraussetzung anwenden und folgern, daß jedes der Polynome $g_\lambda$ mindestens eine komplexe Nullstelle hat.

Die Nullstellen von $g_\lambda$ sind die $w_{ij}(\lambda) \in K$; damit wissen wir, daß es zu jedem $\lambda \in \mathbb{R}$ ein Paar $(i,j)$ gibt derart, daß $w_{ij}(\lambda)$ in $\mathbb{C}$ liegt.

Nun verwenden wir ein klassisches Beweisprinzip der Mathematik, das DIRICHLETsche Schubfachprinzip: Hat man $n$ Schubfächer und verteilt mehr als $n$ Objekte darauf, so müssen in mindestens einem dieser Schubfächer mindestens zwei Objekte liegen.

JOHANN PETER GUSTAV LEJEUNE DIRICHLET (1805 – 1859) wurde in der damals zu Frankreich gehörenden Stadt Düren geboren; er lehrte an den Universitäten Breslau, Berlin und Göttingen. 1828 gab er den ersten strengen Beweis für die Konvergenz von FOURIERreihen und untersuchte die Darstellbarkeit beliebiger Funktionen durch solche Reihen. Auch unser heutiger Funktionsbegriff geht auf DIRICHLET zurück. Sein wohl bekanntester Satz besagt, daß eine arithmetische Progression, deren Glieder keinen gemeinsamen Teiler haben, unendlich viele Primzahlen enthält.

Unsere Objekte sind die reellen Zahlen $\lambda$, die Schubfächer sind die Paare $(i,j)$. Es gibt $\frac{1}{2}d(d-1)$ Schubfächer, aber unendlich viele reelle Zahlen, also muß es zwei Werte $\lambda \neq \lambda'$ und ein Paar $(i,j)$ geben, so daß sowohl $w_{ij}(\lambda)$ als auch $w_{ij}(\lambda')$ in $\mathbb{C}$ liegen.

Gehen wir zurück zur Definition der $w_{ij}$, sehen wir, daß

$$z_i + z_j + \lambda z_i z_j = w_{ij}(\lambda) \quad \text{und} \quad z_i + z_j + \lambda' z_i z_j = w_{ij}(\lambda')$$

beides komplexe Zahlen sind, also auch

$$z_i z_j = \frac{w_{ij}(\lambda') - w_{ij}(\lambda)}{\lambda' - \lambda} \quad \text{und} \quad z_i + z_j = w_{ij}(\lambda) - \lambda z_i z_j \,.$$

Aus §2 von Kapitel 1 wissen wir, daß wir zwei Zahlen, deren Produkt $P$ und Summe $S$ wir kennen, als Lösungen der quadratischen Gleichung $x^2 - Sx + P = 0$ bestimmen können, und dort haben wir auch gesehen,

daß wir zu jeder komplexen Zahl eine komplexe Quadratwurzel finden können, so daß sich die Lösungsformel für quadratische Gleichungen auch im Komplexen anwenden läßt und komplexe Lösungen liefert. Somit sind $z_i$ und $z_j$ komplex, $f$ hat also in der Tat mindestens eine komplexe Nullstelle.

∎

**Korollar:** Jedes nichtkonstante Polynom $f \in \mathbb{C}[X]$ hat mindestens eine komplexe Nullstelle.

*Beweis:* Wir betrachten zu $f = a_d X^d + \cdots + a_0$ das Polynom

$$\overline{f} = \overline{a_d} X^d + \cdots + \overline{a_0}$$

mit den konjugiert komplexen Koeffizienten und multiplizieren die beiden miteinander. Der Koeffizient von $X^r$ in $f\overline{f}$ ist die Summe aller Produkte $a_i\overline{a_j}$ mit $i + j = r$. Ist $i \neq j$, kommt also in der Summe außer dem Summanden $a_i\overline{a_j}$ auch noch $a_j\overline{a_i}$ vor. Diese beiden Zahlen sind konjugiert komplex, so daß ihre Summe reell ist. Für gerade $r$ gibt es noch einen Term der Form $a_i\overline{a_i} = |a_i|^2$; auch der ist reell. Also ist die gesamte Summe reell, und damit ist $f\overline{f} \in \mathbb{R}[X]$. Nach dem gerade bewiesenen Satz hat $f\overline{f}$ mindestens eine komplexe Nullstelle $z$; es gibt also ein $z \in \mathbb{C}$, so daß $f(z)\overline{f}(z) = 0$ ist. Dann ist entweder $f(z) = 0$, und wir sind fertig, oder $\overline{f}(z) = 0$. In diesem Fall ist auch $\overline{\overline{f}(z)} = f(\overline{z}) = 0$, also ist $\overline{z}$ eine komplexe Nullstelle von $f$.

∎

Induktiv folgt sofort der

**Fundamentalsatz der Algebra:** Jedes Polynom $f \in \mathbb{C}[X]$ vom Grad $d \geq 1$ zerfällt vollständig in Linearfaktoren, läßt sich also schreiben als

$$f = a(X - z_1) \cdots (X - z_d) \quad \text{mit} \quad a, z_1, \ldots, z_d \in \mathbb{C}\,.$$

∎

Ist $k$ ein Teilkörper von $\mathbb{C}$ und $f \in k[X]$ ein irreduzibles Polynom über $k$, so zerfällt $f$ über $\mathbb{C}$ in Linearfaktoren:

$$f = a(X - z_1) \cdots (X - z_d) \quad \text{mit} \quad a \in k, \;\; z_1, \ldots, z_d \in \mathbb{C}\,.$$

Der kleinste Teilkörper von $\mathbb{C}$, der sowohl $k$ als auch die Elemente $z_1, \ldots, z_d$ enthält, ist daher ein Zerfällungskörper von $f$ über $k$.

**Definition:** Ist $K/k$ eine Körpererweiterung und sind $z_1, \ldots, z_r$ Elemente von $K$, so bezeichnen wir mit $k(z_1, \ldots, z_r)$ den kleinsten Teilkörper von $K$, der sowohl $k$ als auch die Elemente $z_1, \ldots, z_r$ enthält.

Dieser Körper existiert; er ist einfach der Durchschnitt aller Teilkörper von $K$, die sowohl $k$ als auch die sämtlichen $z_i$ enthalten. Wir sagen, $k(z_1, \ldots, z_r)$ entstehe aus $k$ durch *Adjunktion* der Elemente $z_1, \ldots, z_r$.

Beispielsweise ist $\mathbb{Q}\big(\sqrt{2}\big) = \mathbb{Q} \oplus \mathbb{Q}\sqrt{2}$ und $\mathbb{Q}\big(\sqrt[3]{2}\big) = \mathbb{Q} \oplus \mathbb{Q}\sqrt[3]{2} \oplus \mathbb{Q}\sqrt[3]{4}$ in $\mathbb{R}/\mathbb{Q}$; dabei bezeichnet $\oplus$ die direkte Summe von $\mathbb{Q}$-Vektorräumen.

Für ein irreduzibles Polynom über $\mathbb{Q}$ oder einem anderen Teilkörper von $\mathbb{C}$ haben wir somit zwei wesentlich verschiedene Zugänge zum Zerfällungskörper: Einmal durch Adjunktion der komplexen Nullstellen (wie immer wir die bekommen) oder rein formal durch die Restklassenkonstruktion, mit der wir oben die Existenz des Zerfällungskörpers allgemein bewiesen haben. Natürlich sollten wir uns fragen, was diese beiden Zerfällungskörper miteinander zu tun haben.

**Lemma:** $\varphi\colon k \to k'$ sei ein Isomorphismus von Körpern,

$$f = a_d X^d + \cdots + a_1 X + a_0 \in k[X]$$

sei ein Polynom über $k$ und

$$f' = \varphi(a_d) X^d + \cdots + \varphi(a_1) X + \varphi(a_0)$$

das entsprechende Polynom aus $k'[X]$. Weiter seien $K/k$ und $K'/k'$ Zerfällungskörper von $f$ *bzw.* $f'$. Dann gibt es einen Isomorphismus $\Phi\colon K \to K'$, der $\varphi$ fortsetzt.

*Beweis:* In $K[X]$ läßt sich das Polynom $f$ als Produkt von Linearfaktoren schreiben: $f = a_d(X - z_1) \cdots (X - z_d)$ mit $z_i \in K$. Wir beweisen den Satz durch Induktion nach der Anzahl $r$ jener $z_i$, die *nicht* in $k$ liegen.

Im Fall $r = 0$ zerfällt das Polynom bereits über $k$ in Linearfaktoren, d.h. $K = k$. Außerdem ist dann auch

$$f' = \varphi(a_d)\big(X - \varphi(z_1)\big) \cdots \big(X - \varphi(z_d)\big) \quad \text{mit} \quad \varphi(z_i) \in k' \,,$$

so daß auch $K' = k'$ ist und wir einfach $\Phi = \varphi$ setzen können.

Der Fall $r = 1$ tritt nicht auf, denn liegen etwa $z_2, \ldots, z_d$ in $k$, so muß auch $z_1$ in $k$ liegen, denn nach dem Wurzelsatz von VIÈTE ist

$$z_1 = -\frac{a_{d-1}}{a_d} - z_2 - \cdots - z_d \,.$$

Sei nun $r > 1$. Dann hat $f$ mindestens einen irreduziblen Faktor $g$ vom Grad größer eins. Durch Umnummerieren der Nullstellen können wir erreichen, daß $z_1$ eine Nullstelle von $g$ ist. Nun betrachten wir das Polynom $g' \in k'[X]$, das aus $g$ entsteht, indem wir alle Koeffizienten durch ihr Bild unter $\varphi$ ersetzen. Offensichtlich ist $g'$ ein irreduzibler Faktor von $f'$; das Element $z_1' \in K'$ sei eine Nullstelle von $g'$.

Im Körper $k(z_1)$ hat $g$ mindestens eine Nullstelle, nämlich $z_1$, und in $k'(z_1')$ hat $g'$ mindestens eine Nullstelle, nämlich $z_1'$. Außerdem ist

$$k(z_1) \cong k[X]/(g) \cong k'[X]/(g') \cong k'(z_1') \,.$$

Indem wir $\widetilde{\varphi}(z_1) = z_1'$ setzen, können wir $\varphi$ daher fortsetzen zu einen Isomorphismus $\widetilde{\varphi}\colon k(z_1) \to k'(z_1')$.

Da $k(z_1)$ in $K$ liegt und $k'(z_1')$ in $K'$, können wir das zu beweisende Lemma auch für die Zerfällungskörper $K/k(z_1)$ und $K'/k'(z_1')$ und den Morphismus $\widetilde{\varphi}$ formulieren. Da $r$ dann um mindestens eins kleiner ist, gilt es hier nach Induktionsannahme, und damit gilt es auch für $K/k$ und $K'/k'$.

∎

**Korollar:** Je zwei Zerfällungskörper $K, K'$ eines Polynoms $f \in k[X]$ sind isomorph.

*Beweis:* Wir müssen nur das gerade bewiesene Lemma auf den Fall anwenden, daß $k' = k$ ist und $\varphi$ die Identität.

∎

Was uns wirklich interessiert ist natürlich dieses Korollar. Die allgemeinere Formulierung im Lemma war notwendig, da selbst im Fall $k = k'$ die Körper $k(z_1)$ und $k(z_1')$ im allgemeinen nicht gleich sind, sondern nur isomorph. Der Induktionsbeweis funktionierte daher nur, weil wir in der Formulierung des Lemmas von der allgemeineren Situation isomorpher Körper ausgegangen sind.

## §2: Automorphismen von Körpererweiterungen

Um die Nullstellenmenge eines Polynoms $f \in k[X]$ zu untersuchen, können wir den Zerfällungskörper $K$ von $f$ betrachten. Wenn wir den konstruieren können als eine Folge von Körpererweiterungen, die jeweils durch Adjunktion der Wurzel eines Elements entstehen, können wir alle Elemente von $K$ und damit insbesondere auch die Nullstellen von $f$ ausgehend von $k$ durch Wurzelausdrücke beschreiben.

Wenn wir etwa eine kubische Gleichung $x^3 + px + q = 0$ für zwei rationale Zahlen $p, q$ lösen wollen, betrachten wir nach der Lösungsformel zunächst die Zahl

$$U = -\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3},$$

sodann die dritten Wurzeln $u_1, u_2$ und $u_3$ von $U$, und erhalten schließlich die Lösungen

$$x_1 = u_1 - \frac{p}{3u_1}, \quad x_2 = u_2 - \frac{p}{3u_2} \quad \text{und} \quad x_3 = u_3 - \frac{p}{3u_3}.$$

Wir berechnen also zunächst in $\mathbb{Q}$ die Zahl $\Delta = \left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3$; falls sie in $\mathbb{Q}$ ein Quadrat ist, können wir $U$ als rationale Zahl berechnen. Im allgemeinen wird $\Delta$ kein Quadrat sein; dann gehen wir über zum Körper $k_1 = \mathbb{Q}(\sqrt{\Delta})$ mit $[k_1 : \mathbb{Q}] = 2$. Dort können wir das Element $U$ berechnen und müssen schauen, ob alle dritten Wurzeln von $U$ in $k_1$ liegen. Auch das wird im allgemeinen nicht der Fall sein; dann gehen wir weiter zum Zerfällungskörper $k_2$ des Polynoms $X^3 - U$. Dort liegen die drei Kubikwurzeln $u_1, u_2, u_3$ von $U$ und damit auch die drei Lösungen $x_1, x_2, x_3$ der Gleichung. Wie wir im ersten Kapitel gesehen haben, bedeutet das aber nicht unbedingt, daß $k_2/\mathbb{Q}$ der Zerfällungskörper des Polynoms $X^3 + pX + q$ sein muß: Selbst im Falle dreier ganzzahliger Lösungen sind für die Berechnung von $\sqrt{\Delta}$ und der dritten Wurzeln von $U$ Körpererweiterungen notwendig. Immerhin wissen wir, daß der Zerfällungskörper ein Teilkörper von $k_2$ ist.

In diesem Paragraphen wollen wir versuchen, die Struktur einer Körpererweiterung über ihre Zwischenkörper zu verstehen; diese Zwischenkörper wiederum wollen wir mit Hilfe von Automorphismen in den Griff bekommen.

Homomorphismen, Isomorphismen, Automorphismen, *usw.* von Körpern sind natürlich einfach Ringhomomorphismen, -isomorphismen, -automorphismen, *usw.;* bei Körpern sind diese allerdings automatisch injektiv:

**Lemma:** Ist $k$ ein Körper und $R$ ein Ring, so ist jeder Ringhomomorphismus $\varphi\colon k \to R$ injektiv.

*Beweis:* Kern $\varphi$ ist ein Ideal von $k$; falls es das Nullideal ist, sind wir fertig. Andernfalls gibt es mindestens ein Element $x \neq 0$, und wegen der Idealeigenschaft liegen auch alle Vielfachen von $x$ im Kern. Da in einem Körper alle Elemente außer der Null invertierbar sind, ist jedes $y \in k$ ein Vielfaches von $x$: $y = x \cdot (x^{-1}y)$, so daß Kern $\varphi = k$ wäre. Das ist aber nicht möglich, denn zumindest die Eins muß bei einem Ringhomomorphismus auf 1 abgebildet werden. ∎

Die folgende Diskussion des Zusammenhangs zwischen Automorphismen und Zwischenkörpern folgt im wesentlichen der besonders kompakten und einfachen Darstellung aus

EMIL ARTIN: Galoissche Theorie, *Leipzig 1959* (u.a.)

**Lemma:** $\sigma_1, \ldots, \sigma_r\colon k \to K$ seien paarweise verschiedene Homomorphismen des Körpers $k$ in einen Körper $K$. Dann sind $\sigma_1, \ldots, \sigma_r$ linear unabhängig im folgenden Sinne: Ist $a_1\sigma_1(x) + \cdots + a_r\sigma_r(x) = 0$ für alle $x \in k$ mit irgendwelchen Koeffizienten $a_i \in K$, so müssen alle $a_i$ verschwinden.

*Beweis* durch Induktion nach $r$. Im Falle $r = 1$ können wir einfach $x = 1$ einsetzen und erhalten $a_1 = a_1\sigma(1) = 0$; die Behauptung ist also richtig.

Nun sei $r > 1$ und $a_1\sigma_1(x) + \cdots + a_r\sigma_r(x) = 0$ für alle $x \in k$. Für jedes $y \in k$ gilt dann auch

$$a_1\sigma_1(xy) + \cdots + a_r\sigma_r(xy)$$
$$= a_1\sigma_1(x)\sigma_1(y) + \cdots + a_r\sigma_r(x)\sigma_r(y) = 0\,.$$

Wenn wir die ursprüngliche Gleichung mit $\sigma_r(y)$ multiplizieren, erhalten wir die weitere Gleichung

$$a_1\sigma_1(x)\sigma_r(y) + \cdots + a_r\sigma_r(x)\sigma_r(y) = 0\,.$$

Subtraktion der letzten beiden Gleichungen voneinander liefert die neue Gleichung

$$a_1\big(\sigma_1(y)-\sigma_r(y)\big)\sigma_1(x)+\cdots+a_{r-1}\big(\sigma_{r-1}(y)-\sigma_r(y)\big)\sigma_{r-1}(x)=0$$

für alle $x \in k$. Da diese nur $r-1$ Summanden enthält, verschwinden nach Induktionsannahme alle Koeffizienten, insbesondere der Koeffizient $a_1\big(\sigma_1(y)-\sigma_r(y)\big)$ von $\sigma_1(x)$. Da $\sigma_1$ und $\sigma_r$ verschiedenen Homomorphismen sind, können wir ein $y \in k$ finden, für das $\sigma_1(y) \neq \sigma_r(y)$ ist, und wenn wir mit diesem $y$ arbeiten, sehen wir, daß der Koeffizient $a_1$ verschwinden muß. Unsere Beziehung ist daher von der Form $a_2\sigma_2(x)+\cdots+a_r\sigma_r(x)=0$, und da auch hier nur $r-1$ Homomorphismen vorkommen, zeigt eine nochmalige Anwendung der Induktionsannahme das Verschwinden der restlichen Koeffizienten $a_2,\ldots,a_r$. ∎

**Definition:** *a)* Ist $K/k$ eine Körpererweiterung, so bezeichnen wir mit $\mathrm{Aut}(K/k)$ die Menge aller (Körper)-Automorphismen $\sigma\colon K \to K$, die auf $k$ die Identität sind, d.h. $\sigma(x)=x$ für alle $x \in k$.
*b)* Ist $G$ eine Menge von Automorphismen des Körpers $K$, so bezeichnen wir

$$K^G = \{x \in K \mid \sigma(x)=x \ \text{ für alle } \sigma \in G\}$$

als den Fixkörper von $G$.

Es ist klar, daß $\mathrm{Aut}(K/k)$ eine Gruppe ist und $K^G$ ein Teilkörper von $K$. Im Falle einer endlichen Gruppe $G=\{\sigma_1,\ldots,\sigma_n\}$ haben wir zwei Abbildungen von $K$ nach $K^G$, gegeben durch

$$S(x)=\sigma_1(x)+\cdots+\sigma_n(x) \quad \text{und} \quad N(x)=\sigma_1(x)\cdot\cdots\cdot\sigma_n(x)\,.$$

$S(x)$ heißt die *Spur* von $x$, $N(x)$ die *Norm.* Beide liegen in $K^G$, denn für jedes $\sigma \in G$ ist

$$\sigma\big(S(x)\big)=\sigma\big(\sigma_1(x)+\cdots+\sigma_n(x)\big)=\sigma\circ\sigma_1(x)+\cdots+\sigma\circ\sigma_n(x)=S(x)$$

und

$$\sigma\big(N(x)\big)=\sigma\big(\sigma_1(x)\cdot\cdots\cdot\sigma_n(x)\big)=\sigma\circ\sigma_1(x)\cdot\cdots\cdot\sigma\circ\sigma_n(x)=N(x)\,,$$

denn da die Multiplikation mit $\sigma$ eine bijektive Abbildung von $G$ nach $G$ definiert, ist auch die Menge aller $\sigma\circ\sigma_i$ gleich $G$. Natürlich ist weder

die Spur noch die Norm ein Ringhomomorphismus; immerhin ist die Spur ein Homomorphismus der additiven Gruppen und die Norm einer der multiplikativen Gruppen. Die Spurabbildung kann nicht gleich der Nullabbildung sein, denn wäre $\sigma_1(x) + \cdots + \sigma_n(x) = 0$ für alle $x \in K$, wären die Automorphismen $\sigma_1, \ldots, \sigma_n$ linear abhängig, im Widerspruch zum obigen Lemma.

**Lemma:** Ist $G$ eine endliche Menge von Automorphismen eines Körpers $K$, so ist $[K : K^G] \geq |G|$.

Wir beweisen dieses Lemma im Hinblick auf eine spätere Anwendung gleich etwas allgemeiner als

**Lemma:** Ist $G$ eine endliche Menge von Homomorphismen des Körpers $K$ in einen Körper $L$ und ist

$$k = \{x \in K \mid \sigma(x) = \tau(x) \text{ für alle } \sigma, \tau \in G\} ,$$

so ist $[K : k] \geq |G|$.

Daraus folgt das vorige Lemma, denn für $K = L$ und $G' = G \cup \{\mathrm{id}_K\}$ ist $k = K^{G'} = K^G$, und nach dem Lemma ist $[K : k] \geq |G'| \geq |G|$.

*Beweis* des zweiten Lemmas: Konkret sei $G = \{\sigma_1, \ldots, \sigma_n\}$. Wir nehmen an, daß der Grad $[K : k] = r < n$ sei, und wollen daraus einen Widerspruch ableiten.

Da $[K : k] = r$ ist, gibt es $r$ Elemente $b_1, \ldots, b_r \in K$, die eine $k$-Basis von $K$ bilden. Wir betrachten über $K$ das homogene lineare Gleichungssystem aus den $r$ Gleichungen

$$\sigma_1(b_i)x_1 + \sigma_2(b_i)x_2 + \cdots + \sigma_n(b_i)x_n = 0$$

für $i = 1, \ldots, r$. Da wir mehr Variablen als Gleichungen haben, muß es nichttriviale Lösungen geben; eine davon sei $(x_1, \ldots, x_n)$. Weiter sei $x$ ein beliebiges Element von $K$; wir schreiben es als $k$-Linearkombinationen $x = a_1b_1 + \cdots + a_rb_r$ der Basiselemente. Da die $a_i$ in $k$ liegen, ist $\sigma_j(a_i) = \sigma_1(a_i)$ und $\sigma_j(a_ib_i) = \sigma_1(a_i)\sigma_j(b_i)$ für alle $i, j$. Multiplizieren wir die $i$-te Gleichung des obigen Systems mit $\sigma_1(a_i)$, können wir das Ergebnis daher auch schreiben als

$$\sigma_1(a_ib_i)x_1 + \sigma_2(a_ib_i)x_2 + \cdots + \sigma_n(a_ib_i)x_n = 0 .$$

Addieren wir diese Gleichungen für $i = 1, \ldots, r$, hat $x_j$ in der Summe den Koeffizienten

$$\begin{aligned}&\sigma_j(a_1b_1) + \sigma_j(a_2b_2) + \cdots + \sigma_j(a_rb_r)\\ &= \sigma_j(a_1b_1 + a_2b_2 + \cdots + a_rb_r) = \sigma_j(x)\,.\end{aligned}$$

Die Summe der $r$ Gleichungen ist daher

$$x_1\sigma_1(x) + x_2\sigma_2(x) + \cdots + x_n\sigma_n(x) = 0\,.$$

Da $x$ als beliebiges Element von $K$ vorausgesetzt war, gilt dies für alle $x \in K$ und widerspricht somit der oben gezeigten linearen Unabhängigkeit von Körperhomomorphismen. Also kann $r$ nicht kleiner als $n$ sein, was das Lemma beweist. ∎

Für eine *Gruppe* $G$ von Automorphismen können wir das erste Lemma verschärfen zu

**Satz:** Ist $G$ eine endliche Gruppe von Automorphismen eines Körpers $K$, so ist $[K : K^G] = |G|$.

*Beweis:* Sei wieder $G = \{\sigma_1, \ldots, \sigma_n\}$. Da wir bereits wissen, daß $[K : K^G] \geq |G|$ ist, muß nur noch gezeigt werden, daß je $n + 1$ Elemente $b_1, \ldots, b_{n+1}$ von $K$ linear abhängig über $K^G$ sind. Auch dazu betrachten wir ein homogenes lineares Gleichungssystem mit weniger Gleichungen als Variablen; die $i$-te der $n$ Gleichungen sei

$$\sigma_i^{-1}(b_1)x_1 + \sigma_i^{-1}(b_2)x_2 + \cdots + \sigma_i^{-1}(b_{n+1})x_{n+1} = 0\,.$$

Wieder muß es eine nichttriviale Lösung $(x_1, \ldots, x_{n+1})$ geben; durch Umindizieren der $b_i$ können wir erreichen, daß $x_1 \neq 0$ ist. Für jedes $\lambda \neq 0$ aus $K$ ist auch $(\lambda x_1, \ldots, \lambda x_{n+1})$ eine nichttriviale Lösung; durch geeignete Wahl von $\lambda$ können wir also $x_1$ zu einem beliebigen Element von $K^\times$ machen. Wie wir wissen, ist die Spurabbildung nicht gleich der Nullabbildung; wir wählen $x_1$ so, daß $S(x_1) \neq 0$ ist.

Als nächstes wenden wir im obigen System auf die $i$-te Gleichung den Automorphismus $\sigma_i$ an und erhalten

$$b_1\sigma_i(x_1) + b_2\sigma_i(x_2) + \cdots + b_{n+1}\sigma_i(x_{n+1}) = 0\,.$$

Die Summe aller dieser Gleichungen ist

$$b_1 S(x_1) + b_2 S(x_2) + \cdots + b_{n+1} S(x_{n+1}) = 0\,,$$

wobei die Spuren $S(x_i)$ im Fixkörper $K^G$ liegen und nicht alle verschwinden, da zumindest $S(x_1) \neq 0$ ist. Somit sind $b_1, \ldots, b_{n+1}$ linear abhängig über $K^G$.

■

Als erstes Resultat über den Zusammenhang zwischen Automorphismengruppen und Teilkörpern erhalten sofort das folgende

**Korollar:** Sind $G$ und $H$ zwei verschiedene Gruppen von Automorphismen eines Körpers $K$, so sind $K^G$ und $K^H$ verschiedene Teilkörper.

*Beweis:* Von zwei verschiedenen Gruppen enthält mindestens eine ein Element, das nicht in der anderen enthalten ist. Nehmen wir an, $H$ enthalte einen Automorphismus $\sigma$ von $K$, der nicht in $G$ liegt. Wäre $K^G = K^H$, so müßte $\sigma$ den Körper $K^G$ punktweise festlassen, $K^G$ wäre also auch der Fixkörper der Menge $G \cup \{\sigma\}$. Nach dem Lemma vor dem gerade bewiesenen Satz wäre damit $[K : K^G] \geq |G| + 1$, aber nach dem Satz ist $[K : K^G] = |G|$.

■

Leider ist nicht jeder Teilkörper Fixkörper einer Automorphismengruppe: Für $\mathbb{Q}(\sqrt{2}/\mathbb{Q}$ haben wir zwar eine Automorphismengruppe der Ordnung zwei, bestehend aus der Identität und der Abbildung, die der Zahl $a + b\sqrt{2}$ deren konjugiertes Element $a - b\sqrt{2}$ zuordnet, doch schon für $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ gibt es aber nichts entsprechendes mehr: Jeder Automorphismus $\sigma \in \mathrm{Aut}\big(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}\big)$ muß $\sqrt[3]{2}$ auf eine Zahl $x$ mit $x^3 = 2$ abbilden, und da wir in einem Teilkörper der reellen Zahlen sind, läßt das nur die Möglichkeit $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$ zu. Also wird auch das Quadrat von $\sqrt[3]{2}$ auf sich selbst abgebildet und damit ganz $\mathbb{Q}(\sqrt[3]{2})$; es gibt also keinen Automorphismus außer der Identität.

Selbst $\mathrm{Aut}(\mathbb{R}/\mathbb{Q})$ besteht nur aus der Identität: Wir betrachten einen beliebigen Automorphismus $\varphi\colon \mathbb{R} \to \mathbb{R}$ der auf $\mathbb{Q}$ die Identität ist. (Wie man sich leicht überlegt, gilt das für jeden Automorphismus von $\mathbb{R}$ automatisch.) Da eine reelle Zahl $x$ genau dann größer oder gleich Null ist, wenn es ein $w \in \mathbb{R}$ gibt mit $w^2 = x$, muß $\varphi$ nichtnegative

Zahlen auf nichtnegative Zahlen abbilden, denn $\varphi(w^2) = \varphi(w)^2$. Wegen $\varphi(x) - \varphi(y) = \varphi(x - y)$ muß dann auch für alle $x \leq y$ gelten, daß $\varphi(x) \leq \varphi(y)$ ist. Nun kann man für jede reelle Zahl $x$ eine rationale Intervallschachtelung $\big([a_n, b_n]\big)_{n\in\mathbb{N}}$ angeben, d.h. eine Folge von Intervallen mit $a_n, b_n \in \mathbb{Q}$ derart, daß $x \in [a_n, b_n]$ für alle $n$ und $[a_{n+1}, b_{n+1}] \subseteq [a_n, b_n]$ für alle $n$ und $\lim_{n\to\infty}(b_n - a_n) = 0$. Da $\varphi(a_n) = a_n$ und $\varphi_n(b_n) = b_n$ ist, liegt auch $\varphi(x)$ in allen diesen Intervallen; also muß, wegen der letzten Bedingung, $\varphi(x) = x$ sein. Um solche Beispiele zumindest vorläufig auszuschließen definieren wir

**Definition:** Eine endliche Körpererweiterung $K/k$ heißt GALOISsch, wenn es eine Gruppe $G$ von Automorphismen von $K$ gibt, für die $k = K^G$ ist.

Natürlich muß dann nach obigem Korollar $G = \mathrm{Aut}(K/k)$ sein; wir bezeichnen diese Gruppe als die GALOIS-Gruppe von $K/k$.

ÉVARISTE GALOIS (1811 – 1832) wurde in Bourg La Reine in der Nähe von Paris geboren. Obwohl die französische Revolution zu seiner Zeit schon Jahrzehnte zurücklag, war er stark von ihr geprägt und überzeugter Republikaner, der deshalb immer wieder ins Gefängnis kam. In seiner Jugend wurde er nur von seiner Mutter unterrichtet; erst 1823 ging er auf eine Schule, und 1827 besuchte er erstmalig eine Mathematikklasse. Die Mathematik begeisterte ihn so sehr, daß er darüber alle anderen Fächer vernachlässigte. Trotzdem schaffte er 1828 nicht die Aufnahmeprüfung zur École polytechnique. 1829 veröffentlichte er seine erste mathematische Arbeit; sie handelte von Kettenbrüchen. 1830 folgte eine Arbeit über die Lösung algebraischer Gleichungen. Nachdem er eine posthum veröffentlichte Arbeit von ABEL über dieses Thema gelesen hatte, schrieb er, auf CAUCHYs Rat hin, eine Arbeit, die dessen Ergebnisse mit seinen kombinierte. Er reichte sie 1830 bei FOURIER, dem damaligen Sekretär der Akademie der Wissenschaften ein; nachdem dieser kurz darauf starb, ist diese Arbeit bis heute verschollen. Kurz vor einem Duell, dessen Hintergrund nicht ganz klar ist, schrieb er seine Resultate noch einmal kurz auf; am Tag nach dem Duell starb er an dessen Folgen.

Bevor wir uns überlegen, wie wir einer Körpererweiterung ansehen können, ob sie GALOISsch ist oder nicht, und ob diese Erweiterungen für uns nützlich sind, wollen wir uns zunächst überlegen, daß wir für

GALOISsche Erweiterungen in der Tat alles über die Zwischenkörper aus der Automorphismengruppe ablesen können.

Eine wesentliche Eigenschaft GALOISscher Erweiterungen ist die zunächst eher überflüssig erscheinende Bedingung der Separabilität:

**Definition:** Ein Polynom $f \in k[X]$ über einem Körper $k$ heißt *separabel,* wenn keiner seiner irreduziblen Faktoren im Zerfällungskörper von $f$ eine mehrfache Nullstelle hat. Für eine Körpererweiterung $K/k$ heißt ein Element $x \in K$ separabel, falls es Nullstelle eines separablen Polynoms aus $k[X]$ ist. $K/k$ heißt separabel, wenn jedes Element $x \in K$ separabel über $x$ ist.

Im Falle $k = \mathbb{R}$ ist offensichtlich jedes Polynom separabel: Hat nämlich ein irreduzibles Polynom $f \in \mathbb{R}[X]$ eine mehrfache Nullstelle, so ist diese auch eine Nullstelle der Ableitung $f'$. Damit ist $\mathrm{ggT}(f, f') \neq 1$. Andererseits ist aber $\mathrm{ggT}(f, f')$ ein Teiler von $f$, also entweder assoziiert zu eins oder zu $f$. Da $f'$ kleineren Grad als $f$ hat und im Falle eines Polynoms mit einer mehrfachen Nullstelle nicht konstant sein kann, ist auch das unmöglich. Also gibt es in $\mathbb{R}[X]$ keine nichtseparablen Polynome.

Für Polynome über einen beliebigen Körper $k$ können wir natürlich nicht von einer über Grenzwerte definierten Ableitung reden. Wir können sie aber trotzdem formal definieren:

**Definition:** $k$ sei ein Körper. Die (formale) Ableitung eines Polynoms $f = \sum_{i=0}^{d} a_i X^i \in k[X]$ ist das Polynom $f' = \sum_{i=1}^{d} i a_i X^{i-1}$.

Für $k = \mathbb{R}$ und $k = \mathbb{C}$ ist das natürlich die übliche Ableitung.

Aus der Definition folgt sofort, daß

$$\begin{cases} k[X] \to k[X] \\ \quad f \mapsto f' \end{cases}$$

eine $k$-lineare Abbildung ist. Um zu sehen, daß die formale Ableitung auch die Produktregel erfüllt, vergleichen wir die beiden Abbildungen

$$\begin{cases} k[X] \to k[X] \\ \quad f \mapsto (fg)' \end{cases} \quad \text{und} \quad \begin{cases} k[X] \to k[X] \\ \quad f \mapsto fg' + f'g \end{cases}.$$

Beide sind linear, und für $g = \sum_{j=0}^{e} b_j X^j$ wird das Basiselement $X^i$ für $i \geq 0$ von der ersten abgebildet auf $\sum_{j=0}^{e}(i+j)b_j X^{i+j-1}$, und von der zweiten auf

$$\sum_{j=1}^{e} j b_j X^{i+j-1} + \sum_{j=0}^{e} i b_j X^{i+j-1} = \sum_{j=0}^{e}(i+j)b_j X^{i+j-1} .$$

Somit stimmen beide Abbildungen überein, und die Produktregel ist bewiesen.

Wie in der Analysis gilt

**Lemma:** Die Nullstelle $z \in k$ des Polynoms $f \in k[X]$ hat genau dann eine Vielfachheit größer eins, wenn sie auch Nullstelle von $f'$ ist.

*Beweis:* Da $z$ Nullstelle von $f$ ist, gibt es ein Polynom $g \in k[X]$ derart, daß $f = (X - z)g$ ist. Nach der Produktregel ist $f' = (X - z)g' + g$, d.h. $f'(z)$ verschwindet genau dann, wenn $g(z)$ verschwindet, und das ist genau dann der Fall, wenn $z$ eine mehrfache Nullstelle von $f$ ist. ∎

Für ein Polynom aus $\mathbb{R}[X]$ (und für jede differenzierbare Funktion $f\colon \mathbb{R} \to \mathbb{R}$) ist $f'$ genau dann identisch Null, wenn $f$ konstant ist. Dies gilt nicht für Polynome über einem beliebigen Körper: Sei etwa $\mathbb{F}_p = \mathbb{Z}/p$ der Körper mit $p$ Elementen. (Wenn wir $\mathbb{Z}/p$ als Körper betrachten, schreiben wir meist $\mathbb{F}_p$; das $\mathbb{F}$ steht für *finit,* also endlich.) Dann hat das Polynom $f = X^p$ die Ableitung $f' = pX^{p-1} = 0$, denn in $\mathbb{F}_p$ ist $p = 0$. Trotzdem ist $f$ ein nichtkonstantes Polynom.

Um zu sehen, wann so etwas passieren kann, betrachten wir zu einem beliebigen Körper $k$ den einzig möglichen Ringhomomorphismus $\chi\colon \mathbb{Z} \to k$. Er bildet die Eins auf die Eins ab, und jede ganze Zahl $n$ auf das $n$-fache der Eins von $k$. Sein Kern ist ein Ideal von $\mathbb{Z}$, also ein Hauptideal $(m)$.

**Definition:** Die *Charakteristik* eines Körpers $k$ ist jene Zahl $m \in \mathbb{N}_0$, für die Kern $\chi = (m)$ ist. Wir schreiben $m = \operatorname{char} k$.

**Lemma:** Die Charakteristik eines Körpers ist entweder Null oder eine Primzahl.

*Beweis:* Wäre $\operatorname{char} k = ab$ eine zusammengesetzte Zahl mit $a, b > 1$, so wäre $\chi(a) \cdot \chi(b) = \chi(ab) = 0$, aber $\chi(a)$ und $\chi(b)$ beide von Null verschieden. Da Körper nullteilerfrei sind, ist das nicht möglich. ∎

Natürlich ist $\operatorname{char} \mathbb{Q} = \operatorname{char} \mathbb{R} = 0$ und $\operatorname{char} \mathbb{F}_p = p$ für jede Primzahl $p$. Über einem Körper der Charakteristik Null ist die Ableitung $iX^{i-1}$ von $X^i$ für $i \geq 1$ stets von Null verschieden; hier ist also $f' = 0$ genau dann, wenn $f$ konstant ist. Über einem Körper der Charakteristik $p > 0$ ist dagegen die Ableitung von $X^{np}$ für jedes $n \in \mathbb{N}_0$ gleich Null; die übrigen $X$-Potenzen haben nichtverschwindende Ableitungen. Die Ableitung eines Polynoms verschwindet daher genau dann, wenn alle Exponenten durch $p$ teilbar sind.

**Lemma:** Über einem Körper der Charakteristik Null sind alle Polynome separabel.

*Beweis:* Wir können genau so vorgehen, wie im Fall $k = \mathbb{R}$: Hat ein irreduzibles Polynom $f$ eine mehrfache Nullstelle, so ist diese auch eine Nullstelle von $f'$ und damit von $\operatorname{ggT}(f, f')$. Da $f$ eine Nullstelle hat, ist $f$ nicht konstant, so daß $f'$ nicht das Nullpolynom sein kann, sondern einen echt kleineren Grad als $f$ hat. Damit ist $\operatorname{ggT}(f, f')$ ein Faktor positiven Grades von $f$ mit echt kleinerem Grad als $f$. Dies widerspricht der Irreduzibilität von $f$. ∎

Auch über manchen Körpern positiver Charakteristik sind alle Polynome separabel, zum Beispiel über den Körpern $\mathbb{F}_p$. Um dies zu zeigen, betrachten wir zunächst einen speziellen Homomorphismus für Körper positiver Charakteristik und die Polynomringe darüber:

**Lemma:** Ist $R$ ein Körper mit Charakteristik $p > 0$ oder ein Polynomring über einem solchen Körper, so ist die Abbildung

$$\begin{cases} R \to R \\ x \mapsto x^p \end{cases}$$

ein Ringhomomorphismus.

*Beweis:* Da $R$ ein kommutativer Ring ist, muß natürlich $(xy)^p = x^p y^p$ sein. Bezüglich der Addition ist

$$(x+y)^p = x^p + \binom{p}{1} x^{p-1}y + \cdots + \binom{p}{p-1} xy^{p-1} + y^p \,,$$

und für alle $i$ mit $1 \leq i \leq p-1$ ist $\binom{p}{i} = \frac{p\cdots(p-(i-1))}{i!} \equiv 0 \bmod p$, da zwar der Zähler, nicht aber der Nenner durch $p$ teilbar ist. Somit ist $(x+y)^p = x^p + y^p$.

∎

**Definition:** Der Homomorphismus $x \mapsto x^p$ heißt FROBENIUS-Homomorphismus.

Damit können wir zeigen

**Lemma:** Jedes Polynom aus $\mathbb{F}_p[X]$ ist separabel.

*Beweis:* Wieder sei $f \in \mathbb{F}_p[X]$ ein irreduzibles Polynom. Falls $f'$ nicht das Nullpolynom ist, können wir genauso vorgehen wie beim Beweis des entsprechenden Lemmas für Körper der Charakteristik Null. Andernfalls hat $f$, wie wir oben gesehen haben, die Form $f = \sum_{i=0}^{d} a_i X^{ip}$ mit einem $d > 0$, da $f$ nicht konstant sein kann. Nach dem kleinen Satz von FERMAT ist in $\mathbb{F}_p$ jedes Element $a_i$ gleich seiner $p$-ten Potenz, und außerdem ist nach dem vorigen Lemma für zwei Polynome $g$ und $h$ stets $(g+h)^p = g^p + h^p$. Somit ist

$$\left(\sum_{i=0}^{d} a_i X^i\right)^p = \sum_{i=0}^{d} a_i^p X^{ip} = \sum_{i=0}^{d} a_i X^{ip} = f \,,$$

im Widerspruch zur Irreduzibilität von $f$.

∎

Betrachten wir aber den Körper $k = \mathbb{F}_p(T)$ aller rationaler Funktionen über $\mathbb{F}_p$, also den Quotientenkörper des Polynomrings $\mathbb{F}_p[T]$, so können wir inseparable Polynome finden, etwa das Polynom $f = X^p - T$ aus $k[X]$. Es ist irreduzibel in $\mathbb{F}_p[T][X] = \mathbb{F}_p[T, X]$, da es linear in $T$ ist, und nach dem Satz von GAUSS ist es somit auch irreduzibel in $k[X] = \mathbb{F}_p(T)[X]$.

Wie für jedes Polynom über einem Körper können wir dazu einen Körper $K/k$ finden, in dem $f$ eine Nullstelle $s$ hat. In $K[X]$ ist nach dem vorletzten Lemma $(X-s)^p = X^p - s^p = X^p - T$. Die Zerlegung von $f$ in irreduzible Faktoren im Zerfällungskörper ist also $(X-s)^p$; es gibt daher nur eine einzige Nullstelle, und die hat Vielfachheit $p$, so daß $f$ nicht separabel ist.

In einer GALOISschen Erweiterung kann so etwas nicht passieren; hier gilt

**Satz:** Jede GALOISsche Erweiterung $K/k$ ist separabel. Für ein Element $z \in K$ sei $M_z = \{\sigma(z) \mid \sigma \in \mathrm{Aut}(K/k)\}$; dann ist $z$ eine Nullstelle des über $k$ irreduziblen Polynoms

$$f = \prod_{w \in M_z} (X - w)\,.$$

*Beweis:* Da auch die Identität in $\mathrm{Aut}(K/k)$ liegt, ist $z \in M_z$ eine Nullstelle von $f$. Auch die Separabilität von $f$ ist klar, denn die Elemente von $M_z$ sind paarweise verschieden. Zu zeigen bleibt, daß $f$ in $k[X]$ liegt und irreduzibel ist. Die Koeffizienten von $f$ sind bis aufs Vorzeichen die elementarsymmetrischen Funktionen in den Nullstellen $w \in M_z$. Daher sind sie invariant unter $\mathrm{Aut}(K/k)$, liegen also, da $K/k$ eine GALOISsche Erweiterung ist, in $k$. Ist $f = gh$ eine Zerlegung von $f$ mit $g, h \in k[X]$, so muß mindestens einer der beiden Faktoren bei $z$ verschwinden; sei etwa $g(z) = 0$. Dann ist für jedes $\sigma \in \mathrm{Aut}(K/k)$ auch

$$g\big(\sigma(z)\big) = \sigma\big(g(z)\big) = \sigma(0) = 0\,,$$

so daß alle $w \in M_z$ Nullstellen von $g$ sind. Somit ist $g$ assoziiert zu $f$ und $h$ eine Einheit, $f$ also irreduzibel. Da alle Elemente von $M_z$ verschieden sind, ist $f$ auch separabel. ∎

**Korollar:** Ist $K/k$ eine GALOISsche Erweiterung und $f \in k[X]$ ein irreduzibles Polynom, das in $K$ eine Nullstelle $z$ hat, so zerfällt $f$ in $K[X]$ in Linearfaktoren.

*Beweis:* Wie wir am Ende des obigen Beweises gesehen haben, verschwindet ein Polynom mit Koeffizienten aus $k$, das bei einem $z \in K$

verschwindet, auch in allen $\sigma(z)$ mit $\sigma \in \mathrm{Aut}(K/k)$. Daher ist $f$ teilbar durch das im Satz angegebene Polynom zu $z$. Wegen der Irreduzibilität von $f$ unterscheiden sich die beiden höchstens um eine Einheit, also zerfällt auch $f$ in Linearfaktoren. ∎

Die Bedingung, daß $K/k$ eine GALOISsche Erweiterung sein soll, ist hier wesentlich: Beispielsweise zerfällt das Polynom $X^3 - 2$ über $\mathbb{Q}\big(\sqrt[3]{2}\big)$ nicht in Linearfaktoren, sondern nur in ein Produkt von $(X - \sqrt[3]{2})$ mit einem quadratischen Polynom.

**Satz:** $L/k$ sei eine GALOISsche Erweiterung, und $K$ sei ein Zwischenkörper. Dann ist auch $L/K$ GALOISsch.

*Beweis:* $\mathrm{Aut}(L/K)$ ist die Untergruppe jener Automorphismen aus $\mathrm{Aut}(L/k)$, die jedes Element von $K$ festlassen; ihre Gruppenordnung sei $r$ und ihr Fixkörper sei $K'$. Natürlich ist $K \leq K'$; wir müssen zeigen, daß die beiden Körper gleich sind. Da $[L : K'] = r$ ist, genügt dazu, daß auch $[L : K] = r$ ist.

Ein Automorphismus $\sigma \in \mathrm{Aut}(L/k)$ bildet $K$ ab auf einen Teilkörper $\sigma(K) \leq L$. Ein weiterer Automorphismus $\tau \in \mathrm{Aut}(L/k)$ stimmt genau dann auf $K$ mit $\sigma$ überein, wenn $\sigma^{-1}\tau$ die Identität auf $K$ ist, wenn also $\sigma^{-1}\tau$ in $\mathrm{Aut}(L/K)$ liegt. Dies wiederum ist äquivalent dazu, daß die beiden Nebenklassen $\sigma\,\mathrm{Aut}(L/K)$ und $\tau\,\mathrm{Aut}(L/K)$ übereinstimmen.

Zwei Automorphismen $\sigma, \tau\colon L \to L$ definieren bei Einschränkung auf $K$ somit genau dann die gleiche Abbildung, wenn sie in der gleichen Nebenklasse von $\mathrm{Aut}(L/k)$ modulo $\mathrm{Aut}(L/K)$ liegen. Die Anzahl dieser Nebenklassen ist der Index $s$ von $\mathrm{Aut}(L/K)$ in $\mathrm{Aut}(L/k)$. Nehmen wir aus jeder Nebenklasse einen Vertreter, erhalten wir somit $s$ verschiedene Homomorphismen von $K$ nach $L$. Da sie in $\mathrm{Aut}(L/k)$ liegen, induzieren sie allesamt die Identität auf $k$. Nach einem der oben bewiesenen Lemmata ist daher $[K : k] \geq s$. Außerdem wissen wir, daß $[L : K] \geq r$ ist, also ist $[L : k] = [L : K][K : k] \geq rs$. Da $L/k$ GALOISsch ist, ist $[L : k]$ die Ordnung von $\mathrm{Aut}(L/k)$. Die Ordnung dieser Gruppe ist nach LAGRANGE das Produkt der Ordnung der Untergruppe $\mathrm{Aut}(L/K)$ mit dem Index von $\mathrm{Aut}(L/K)$ in $\mathrm{Aut}(L/k)$, also $rs$. Damit ist einerseits

$[L : K][K : k] = rs$, andererseits $[L : K] \geq r$ und $[K : k] \geq s$. Das ist nur möglich, wenn $[L : K] = r$ und $[K : k] = s$ ist, und $[L : K] = r$ ist genau das, was wir beweisen wollten.

■

Damit können wir den Hauptsatz der GALOIS-Theorie beweisen:

**Satz:** $L/k$ sei eine GALOISsche Erweiterung und $G = \mathrm{Aut}(L/k)$. Dann gibt es eine Bijektion zwischen der Menge aller Untergruppen von $G$ und der Menge aller Körper $K$ mit $k \leq K \leq L$, die jeder Untergruppe $H \leq G$ deren Fixkörper $L^H$ zuordnet und jedem Zwischenkörper $K$ die Gruppe $\mathrm{Aut}(L/K)$. Ist $H \leq H' \leq G$, so ist $K^H \geq K^{H'}$. Außerdem ist $[L : L^H] = |H|$ und $[L^H : k] = [G : H]$.

*Beweis:* $\mathcal{U}$ sei die Menge aller Untergruppen von $G$ und $\mathcal{Z}$ die Menge aller Zwischenkörper $K$ mit $k \leq K \leq L$. Wir müssen zeigen, daß die beiden Abbildungen

$$\begin{cases} \mathcal{U} \to \mathcal{Z} \\ H \mapsto L^H \end{cases} \quad \text{und} \quad \begin{cases} \mathcal{Z} \to \mathcal{U} \\ K \mapsto \mathrm{Aut}(L/K) \end{cases}$$

zueinander invers sind. Ausgehend von einer Untergruppe $H \leq G$ müssen wir also zeigen, daß $\mathrm{Aut}(L/L^H) = H$ ist: $H$ ist auf jeden Fall eine Untergruppe von $\mathrm{Aut}(L/L^H)$; wären die beiden verschieden, hätten sie verschiedene Fixkörper, da der Grad eines Körpers über seinem Fixkörper nach einem früheren Lemma gleich der Ordnung der Automorphismengruppe ist. Der Fixkörper von $\mathrm{Aut}(L/L^H)$ enthält den Körper $L^H$, und $[L : L^H] = |H|$; daher müssen die beiden Körper und somit auch die beiden Untergruppen übereinstimmen.

Umgekehrt sei $K$ ein Zwischenkörper; wir müssen zeigen, daß $K$ der Fixkörper von $\mathrm{Aut}(L/K)$ ist. Da $L/K$ nach dem vorigen Satz GALOISsch ist, gilt dies in der Tat. Die restlichen Behauptungen sind klar.

■

Der Zwischenkörper $K = L^H$ ist genau dann GALOISsch über $k$, wenn $k$ der Fixkörper einer Gruppe von Automorphismen des Körpers $K$ ist. Da $[L : k] = |G|$ und $[L : K] = |H|$ ist, folgt $[K : k] = [G : H]$, die Gruppe hat also $[G : H]$ Elemente. Aus dem Beweis des vorletzten Satzes wissen

wir, daß die Automorphismen von $L/k$ genau $[G : H]$ verschiedene Isomorphismen von $K$ auf Teilkörper von $L$ induzieren, die $k$ festlassen. Mehr solche Isomorphismen kann es nicht geben, denn ist $G'$ eine Menge von Körperhomomorphismen $K \to L$, die $k$ festlassen und zu denen auch die Identität gehört, so wissen wir, daß der Körper

$$k' = \{x \in K \mid \sigma(x) = \tau(x) \text{ für alle } \sigma, \tau \in G'\},$$

einerseits den Körper $k$ enthält, andererseits aber ist nach einem der früheren Lemmata in diesem Paragraphen $[K : k'] \geq |G'|$. Gäbe es also mehr als $[G : H]$ Isomorphismen von $K$ auf Teilkörper von $L$, so wäre

$$[G : H] = [K : k] \geq [K : k'] \geq |G'| > [G : H]\,,$$

was nicht sein kann. Nun ist aber $K/k$ genau dann GALOISsch, wenn es eine Gruppe von $[G : H]$ Automorphismen von $K/k$ gibt, die $k$ als Fixkörper hat. Jeder solche Automorphismus ist natürlich insbesondere ein Isomorphismus von $K$ auf einen Teilkörper von $L$; da es insgesamt nur $[G : H]$ solche Isomorphismen gibt heißt dies, daß jeder dieser Isomorphismen ein Automorphismus von $K$ sein muß, d.h. $\sigma(K) = K$ für jeden Automorphismus $\sigma$ von $L$.

Für einen beliebigen Automorphismus $\sigma$ von $L$ und einen beliebigen Teilkörper $K = L^H$ ist $\sigma(K)$ ein Teilkörper von $L$. Ein weiterer Automorphismus $\tau\colon L \to L$ läßt $\sigma(K)$ genau dann punktweise fest, wenn für jedes $x \in K$ gilt $\tau\big(\sigma(x)\big) = \sigma(x)$ oder $\sigma^{-1}\tau\sigma(x) = x$. Somit muß $\sigma^{-1}\tau\sigma$ in $H$ liegen und $\tau$ in $\sigma H \sigma^{-1}$, d.h. $\sigma(K)$ ist der Zwischenkörper zur Untergruppe $\sigma H \sigma^{-1}$. Wenn $\sigma(K)$ gleich $K$ sein soll, muß dies gleich $H$ sein; daher ist $\sigma(K) = K$ für alle $\sigma \in \mathrm{Aut}(L/k)$ genau dann, wenn $H$ ein Normalteiler ist. In diesem Fall bilden die Nebenklassen von $H$ eine Gruppe, die Faktorgruppe $G/H$. Also gilt:

**Satz:** $L/k$ sei eine GALOISsche Erweiterung. Für einen Zwischenkörper $K$ ist $K/k$ genau dann GALOISsch, wenn $\mathrm{Aut}(L/K)$ ein Normalteiler von $\mathrm{Aut}(L/k)$ ist, und $\mathrm{Aut}(K/k)$ ist dann isomorph zur Faktorgruppe. ∎

Damit können wir die Zwischenkörper einer GALOISschen Erweiterung vollständig beschreiben durch die Untergruppen ihrer GALOIS-Gruppe. Das nützt uns allerdings nur dann etwas, wenn es interessante GALOISsche Erweiterungen gibt.

**Satz:** Eine endliche Körpererweiterung $K/k$ ist genau dann GALOISsch, wenn $K$ Zerfällungskörper eines über $k$ separablen Polynoms ist.

*Beweis:* Sei zunächst $K/k$ GALOISsch, und $b_1, \ldots, b_n$ sei eine Basis des $k$-Vektorraums $K$. Da dieser endlichdimensional ist, sind die verschiedenen Potenzen eines jeden $b_i$ linear abhängig. Es gibt daher zu jedem $b_i$ ein Polynom aus $k[X]$, das dort verschwindet; $f_i$ sei ein irreduzible Faktor davon, der $b_i$ als Nullstelle hat. Wie wir bereits gesehen haben, ist $f_i$ separabel und zerfällt über $K$ in Linearfaktoren. Damit ist auch das Produkt $f$ aller $f_i$ separabel, und $K$ ist der Zerfällungskörper von $f$ über $k$.

Umgekehrt sei $f$ ein separables Polynom, und $K/k$ sei der Zerfällungskörper von $f$ über $k$. Wir müssen zeigen, daß $K$ der Fixkörper von $G = \mathrm{Aut}(K/k)$ ist. Wir beweisen dies durch Induktion nach der Anzahl $r$ jener Nullstellen von $f$, die *nicht* in $k$ liegen. Im Falle $r = 0$ ist $K = k$, und die Behauptung ist trivialerweise richtig.

Für $r > 0$ betrachten wir eine nicht in $k$ liegende Nullstelle $z$ von $f$. Dann ist $K$ auch Zerfällungskörper von $f$ über $k(z)$, und da die Nullstelle $z$ in $k(z)$ liegt, ist die Anzahl der nicht in $k(z)$ liegenden Nullstellen von $f$ kleiner als $r$. Nach Induktionsannahme ist daher $K/k(z)$ GALOISsch, und $k(z)$ ist der Fixkörper von $\mathrm{Aut}\big(K/k(z)\big)$.

Als Nullstelle von $f$ ist $z$ auch Nullstelle eines irreduziblen Faktors $g$ von $f$, und mit $f$ ist auch $g$ separabel. Bezeichnet $d$ den Grad von $g$, hat $g$ daher $d$ verschiedene Nullstellen $z_1, \ldots, z_d$. Für jedes $i$ ist $k(z_i) \cong k[X]/(g)$, also gibt es Isomorphismen $\sigma_i \colon k(z) \to k(z_i)$. Beim Beweis der Tatsache, daß Zerfällungskörper isomorpher Körper isomorph sind, haben wir gesehen, daß sich jeder solche Isomorphismus fortsetzen läßt zu einem Isomorphismus der Zerfällungskörper. Da der Zerfällungskörper von $f$ über jedem der Körper $k(z_i)$ gleich $K$ ist, gibt es also $d$ Automorphismen $\tau_i \colon K \to K$, die auf $k(z)$ mit $\sigma_i$ übereinstimmen.

Nun sei $x$ ein beliebiges Element des Fixkörpers von $\mathrm{Aut}(K/k)$. Da $x$ dann insbesondere von allen Automorphismen von $K/k(z)$ festgelassen wird, ist auf jeden Fall $x \in k(z)$. Die Potenzen $1, z, \ldots, z^{d-1}$ bilden

eine Basis des Vektorraums $k(z)$ über $k$; daher können wir $x$ schreiben als

$$x = c_0 + c_1 z + \cdots + c_{d-1} z^{d-1} \quad \text{mit} \quad c_i \in k\,.$$

Die Automorphismen $\tau_i$ lassen $k$ punktweise fest, und da $x$ im Fixkörper von $\mathrm{Aut}(K/k)$ liegt, ist auch $\tau_i(x) = x$. Daher ist

$$\begin{aligned} x = \tau_i(x) &= c_0 + c_1 \tau_i(z) + \cdots + c_{d-1} \tau_i(z)^{d-1} \\ &= c_0 + c_1 z_i + \cdots c_{d-1} z_i^{d-1}\,. \end{aligned}$$

Das Polynom

$$c_{d-1} X^{d-1} + \cdots + c_1 X + (c_0 - x) \in K[X]$$

hat somit mindestens die $d$ verschiedenen Nullstellen $z_1, \ldots, z_d$. Da es höchstens den Grad $d-1$ hat, muß es gleich dem Nullpolynom sein. Insbesondere ist $c_0 - x = 0$, d.h. $x = c_0$ liegt in $k$. Damit ist die Behauptung bewiesen.

∎

**Korollar:** Ist $K/k$ eine separable endliche Körpererweiterung, so gibt es eine Körpererweiterung $L/K$ derart, daß $L/k$ GALOISsch ist.

*Beweis:* Nach Voraussetzung gibt es endich viele über $k$ separable Elemente $z_1, \ldots, z_r \in K$ derart, daß $K = k(z_1, \ldots, z_r)$ ist. Für jedes $z_i$ sei $f_i \in k[X]$ ein irreduzibles Polynom, das $z_i$ als Nullstelle hat. Dann ist der Zerfällungskörper des Produkts aller $f_i$ eine GALOISsche Erweiterung von $k$, die $K$ enthält.

∎

## §3: Lösbarkeit von Gleichungen durch Radikale

In diesem Paragraphen wollen wird uns überlegen, daß Polynomgleichungen vom Grad mindestens fünf *im allgemeinen* nicht durch Wurzelausdrücke lösbar sind. Dazu betrachten wir zunächst die Körpererweiterungen, die durch Adjunktion einer Wurzel entstehen. Wie wir vom Beispiel der dritten Wurzel aus zwei über $\mathbb{Q}$ wissen, sind diese im allgemeinen nicht GALOISsch; sie werden aber GALOISsch, wenn wir über einem Körper arbeiten, der genügend viele Einheitswurzeln enthält:

**Definition:** Ein Element $\zeta$ eines Körpers $k$ heißt $n$-te *Einheitswurzel,* wenn $\zeta^n = 1$ ist. Wenn es kein $m < n$ gibt, für das bereits $\zeta^m = 1$ ist, bezeichnen wir $\zeta$ als eine *primitive* $n$-te Einheitswurzel.

**Satz:** Der Körper $k$ enthalte eine primitive $n$-te Einheitswurzel $\zeta$, und $a \in k$ sei ein beliebiges Element von $k$. Dann ist $k(\sqrt[n]{a})/k$ eine GALOISsche Erweiterung mit einer zyklischen GALOIS-Gruppe.

Dabei bezeichnet $\sqrt[n]{a}$ ein festes Element $w$ eines Erweiterungskörpes von $k$ mit $w^n = a$. Beispielsweise können wir, falls das Polynom $W^n - a \in k[W]$ irreduzibel ist, die Restklasse von $W$ in $k[W]/(W^n - a)$ nehmen oder, falls $k$ ein Teilkörper von $\mathbb{C}$ ist, eine feste komplexe Zahl $w$ mit $w^n = a$.

*Beweis:* Das Polynom $X^n - a \in k[X]$ hat in $k(\sqrt[n]{a})$ die $n$ verschiedenen Nullstellen $\zeta^i \sqrt[n]{a}$ für $i = 0, \ldots, n-1$, ist also separabel. Außerdem ist $k(\sqrt[n]{a})/k$ Zerfällungskörper von $X^n - a$ über $k$; die Körpererweiterung ist also GALOISsch. Jeder Automorphismus von $k(\sqrt[n]{a})/k$ muß $\sqrt[n]{a}$ abbilden auf ein Element $x$ mit $x^n = a$, also auf eines der Elemente $\zeta^i \sqrt[n]{a}$. Durch dieses Element ist der Automorphismus eindeutig bestimmt, denn jedes Element von $k(\sqrt[n]{a})$ läßt sich als Polynom in $\sqrt[n]{a}$ mit Koeffizienten aus $k$ schreiben. Da die Potenzen von $\zeta$ eine zyklische Gruppe der Ordnung $n$ bilden, ist $\mathrm{Aut}\big(k(\sqrt[n]{a})/k\big)$ isomorph zu einer Untergruppe von $\mathbb{Z}/n$, also auch zyklisch. ∎

Auf der Suche nach einer allgemeinen Lösungsformel für Gleichungen $d$-ten Grades

$$a_d x^d + a_{d-1} x^{d-1} + \cdots + a_1 x + a_0$$

über einem Körper $k$ können wir uns beschränken auf den Fall $a_d = 1$, denn da $a_d$ nicht verschwindet, können wir die Gleichung durch $a_d$ dividieren. Wie wir in Kapitel 1 gesehen haben, könnten wir uns zusätzlich noch beschränken auf den Fall $a_{d-1} = 0$; da dies für die allgemeinen Betrachtungen hier keinen Vorteil bringt, wollen wir aber darauf verzichten. Wir betrachten die Koeffizienten $a_0, \ldots, a_{d-1}$ als Unbestimmte, d.h. wir arbeiten über dem Körper

$$K = k(a_0, \ldots, a_{d-1}) = \mathrm{Quot}\, k[a_0, \ldots, a_{d-1}]\,,$$

dessen Elemente rationale Funktionen (Quotienten von Polynomen) in den $d$ Variablen $a_0, \ldots, a_{d-1}$ sind. Über diesem Körper betrachten wir den Zerfällungskörper $L$ des Polynoms

$$f = X^d + a_{d-1}X^{d-1} + \cdots + a_1 X + a_0 \in K[X]\,.$$

In $L[X]$ ist $f = (X - z_1)\cdots(X - z_d)$ mit $z_1, \ldots, z_d \in L$, und natürlich ist $L = K(z_1, \ldots, z_d)$. Tatsächlich ist sogar $L = k(z_1, \ldots, z_d)$, denn nach dem Wurzelsatz von VIÈTE ist $a_j = (-1)^{d-j}\varphi_{d-j}(z_1, \ldots, z_d)$, wobei $\varphi_j$ das $j$-te elementarsymmetrische Polynom in $d$ Variablen bezeichnet, so daß alle $a_j$ und damit auch $K$ in $k(z_1, \ldots, z_d)$ liegen.

Die Gruppe $\mathfrak{S}_d$ aller Permutationen der Menge $\{1, \ldots, d\}$ operiert auf $L$, indem $z_i$ abgebildet wird auf $z_{\pi(i)}$ für jedes $i$ und jede Permutation $\pi \in \mathfrak{S}_d$. Die Koeffizienten $a_j$ als (bis aufs Vorzeichen) elementarsymmetrische Funktionen in den $z_i$ bleiben bei dieser Operation fix, also bleibt ganz $K$ fix. Wir wollen uns überlegen, daß *nur* $K$ fix bleibt, daß $K$ also der Fixkörper unter dieser Operation ist.

Da $L$ der Zerfällungskörper von $f$ über $K$ ist, läßt sich jedes Element $x \in L$ schreiben als Polynom in $z_1, \ldots, z_d$ mit Koeffizienten aus $K$. Da diese unter der Operation von $\mathfrak{S}_d$ fix bleiben, bleibt $x \in L$ genau dann fix, wenn es sich über $K$ als ein symmetrisches Polynom in den $z_i$ schreiben läßt. Nach dem Hauptsatz über symmetrische Polynome läßt sich jedes symmetrische Polynom schreiben als Polynom in den elementarsymmetrischen Polynomen, also läßt sich $x$ schreiben als Polynom in den $a_i$ und liegt somit in $K$. Somit ist $K$ der Fixkörper von $L$ unter der Operation der symmetrischen Gruppe $\mathfrak{S}_d$. Insbesondere ist $L/K$ eine GALOISsche Erweiterung mit $\mathrm{Aut}(L/K) \cong \mathfrak{S}_d$.

Wir sagen, die allgemeine Gleichung vom Grad $d$ lasse sich durch Radikale auflösen, wenn sich die $z_i$ schreiben lassen als Ausdrücke in den $a_j$, die nur Grundrechenarten und Wurzeln enthalten. Für $d = 2$ etwa haben wir im Falle eines Grundkörpers $k$ der Charakteristik 0 mit den Lösungsformeln

$$z_{1/2} = -\frac{a_1}{2} \pm \sqrt{\left(\frac{a_1}{2}\right)^2 - a_0}$$

eine solche Darstellung; tatsächlich gilt dies sogar über jedem Körper $k$ mit $\mathrm{char}\, k \neq 2$.

Falls sich die allgemeine Gleichung $d$-ten Grades durch Radikale auflösen läßt, gibt es zur obigen Körpererweiterung $L/K$ eine Folge von Zwischenkörpern

$$K = K_0 < K_1 < \cdots < K_r = L$$

derart, daß jeder Körper $K_{i+1}$ aus $K_i$ durch Adjunktion einer Wurzel entsteht. Dazu gibt es nach dem Hauptsatz der GALOIS-Theorie eine Folge von Gruppen

$$G_r = \{\mathrm{id}\} < G_{r-1} < \cdots G_1 < G_0 = \mathfrak{S}_d$$

derart, daß $K_i = L^{G_i}$ der Fixkörper von $G_i$ ist.

Für das Folgende wollen wir annehmen, daß der Grundkörper $k$ (und damit erst recht jeder Körper $K_i$) eine primitive $d!$-te Einheitswurzel enthält. Da der Grad jeder Körpererweiterung $K_i/K_{i-1}$ ein Teiler von $[L : K] = d!$ ist und $K_i$ aus $K_{i-1}$ durch Adjunktion einer $n$-ten Wurzel entsteht, wobei $n \leq d!$ sein muß, folgt aus dem zu Beginn dieses Paragraphen bewiesenen Satz, daß $K_{i+1}/K_i$ GALOISsch ist mit einer zyklischen GALOIS-Gruppe. Wir bezeichnen ihre Ordnung mit $n_i$.

Da $L/K$ GALOISsch ist, sind auch alle Erweiterungen $L/K_i$ GALOISsch und $\mathrm{Aut}(L/K_i) = G_i$. Der Körper $K_{i+1}$ ist ein Zwischenkörper dieser Erweiterung, und da er GALOISsch über $K_i$ ist, muß $G_{i+1}$ ein Normalteiler von $G_i$ sein mit einer zyklischen Faktorgruppe $G_i/G_{i+1} \cong \mathbb{Z}/n_i$.

Für $d = 3$ etwa haben wir die Folge $\{\mathrm{id}\} < \mathfrak{A}_3 < \mathfrak{S}_3$. Die Körpererweiterung $L/K$ hat als Grad die Gruppenordnung sechs der $\mathfrak{S}_3$, und der Fixkörper $K_1$ von $\mathfrak{A}_3$ ist eine quadratische Erweiterung von $K$. Sie kommt zustande durch das Ziehen der Quadratwurzel aus der Diskriminante in der Lösungsformel. $L/K_1$ hat Grad drei; dies entspricht dem Ziehen der Kubikwurzel. Da $K$ nach Voraussetzung eine primitive dritte Einheitswurzel enthält, enthält diese Erweiterung alle dritten Wurzeln des Radikanden, ist also GALOISsch.

Mit der Frage, wann wir in $\mathfrak{S}_d$ eine solche Folge von Untergruppen finden können, wollen wir uns als nächstes beschäftigen.

Im Hinblick auf die Auflösbarkeit von Gleichungen definieren wir:

**Definition:** Eine endliche Gruppe $G$ heißt *auflösbar,* wenn es eine Folge

$$G_r = \{\mathrm{id}\} \lhd G_{r-1} \lhd \cdots G_1 \lhd G_0 = G$$

von Untergruppen gibt derart, daß $G_{i+1}$ stets ein Normalteiler von $G_i$ mit zyklischer Faktorgruppe $G_i/G_{i+1}$ ist.

Falls sich die allgemeine Gleichung $d$-ten Grades durch Radikale lösen läßt, muß die Permutationsgruppe $\mathfrak{S}_d$ also auflösbar sein. Wir wollen uns überlegen, daß dies für $d \geq 5$ nicht der Fall ist. Dazu führen wir zunächst einen weiteren Begriff ein:

**Definition:** Eine endliche Gruppe $G$ heißt *einfach,* wenn sie nicht nur aus dem Neutralelement $e$ besteht und keine Normalteiler außer sich selbst und $\{e\}$ hat.

Die einfachsten Beispiele einfacher Gruppen sind die zyklischen Gruppen von Primzahlordnung, die ja überhaupt keine echten Untergruppen haben. Eine zyklische Gruppe $\mathbb{Z}/n$ mit zusammengesetztem $n$ ist nicht einfach, denn ist $r$ ein echter Teiler von $n$ und $g$ ein Erzeugendes der Gruppe, so erzeugt $g^{n/r}$ eine Untergruppe der Ordnung $r$, die natürlich wie jede Untergruppe einer abelschen Gruppe ein Normalteiler ist. Auch die symmetrische Gruppe $\mathfrak{S}_d$ ist für $d > 2$ nicht einfach, da sie die alternierende Gruppe $\mathfrak{A}_d$ als Normalteiler enthält. Wir wollen uns aber überlegen, daß $\mathfrak{A}_d$ für $d \geq 5$ einfach ist. Daraus wird dann insbesondere folgen, daß $\mathfrak{S}_d$ für $d \geq 5$ nicht auflösbar ist und es somit keine allgemeine Lösungsformel für Gleichungen vom Grad größer vier geben kann, die mit Grundrechenarten und Wurzeln auskommt:

**Lemma:** Ist $\mathfrak{A}_d$ einfach und nicht zyklisch, so ist $\mathfrak{S}_d$ nicht auflösbar.

*Beweis:* Falls $\mathfrak{A}_d$ einfach ist, kann es in $\mathfrak{S}_d$ außer $\mathfrak{A}_d$ keinen nichttrivialen Normalteiler $N$ geben, denn für den wäre $N' = N \cap \mathfrak{A}_d$ ein Normalteiler von $\mathfrak{A}_d$, müßte also entweder gleich $\mathfrak{A}_d$ sein oder nur aus der Identität bestehen. $N' = \mathfrak{A}_d$ ist äquivalent zu $N = \mathfrak{S}_d$ oder $N = \mathfrak{A}_\mathfrak{d}$, und wenn $N'$ nur aus der Identität besteht, kann $N$ außer der Identität keine gerade Permutation enthalten. Da das Produkt zweier ungerader Permutationen gerade ist, besteht daher $N$ entweder nur aus der Identität oder ist die von einer ungeraden Permutation $\omega$ der Ordnung zwei erzeugte zyklische

Untergruppe der Ordnung zwei. Letztere kann aber für $d \geq 3$ kein Normalteiler sein, da es immer eine Permutation $\pi \in \mathfrak{S}_d$ gibt, für die $\pi^{-1}\omega\pi$ eine von $\omega$ verschiedene ungerade Permutation ist. (Für $d \leq 2$ besteht $\mathfrak{A}_d$ nur aus der Identität, ist also nicht einfach.)

Falls $\mathfrak{S}_d$ auflösbar wäre, gäbe es für die Untergruppenfolge aus der obigen Definition daher nur die beiden Möglichkeiten $\{e\} \lhd \mathfrak{S}_d$ und $\{e\} \lhd \mathfrak{A}_d \lhd \mathfrak{S}_d$. Im ersten Fall müßte $\mathfrak{S}_d$ zyklisch sein; dies ist nur für $d = 2$ erfüllt, und dann ist $\mathfrak{A}_d$ nicht einfach. Im zweiten Fall müßte $\mathfrak{A}_d$ zyklisch sein, was wir ausgeschlossen haben (und was im übrigen genau für $d = 3$ erfüllt ist, wo diese Folge von Inklusionen die Auflösbarkeit der $\mathfrak{S}_3$ zeigt). Somit kann $\mathfrak{S}_d$ im Falle einer nichtzyklischen einfachen alternierenden Gruppe $\mathfrak{A}_d$ nicht auflösbar sein.

**Satz:** Für $d \geq 5$ ist die alternierende Gruppe $\mathfrak{A}_d$ einfach.

Wir führen den *Beweis* in fünf Schritten:

**1. Schritt:** $\mathfrak{A}_d$ wird von den Dreierzykeln erzeugt.

*Beweis:* Jedes Element von $\mathfrak{A}_d$ ist ein Produkt einer geraden Anzahl von Transpositionen. Falls zwei aufeinanderfolgende Transpositionen ein gemeinsames Element haben, ist $(a\ b)(b\ c) = (a\ b\ c)$ ein Dreierzyklus; andernfalls ist

$$(a\ b)(c\ d) = (a\ b)(b\ c)(b\ c)(c\ d) = (a\ b\ c)(b\ c\ d)$$

Produkt zweier Dreierzykeln. Somit läßt sich jedes Element von $\mathfrak{A}_d$ als Produkt von Dreierzykeln schreiben.

**2. Schritt:** Alle Dreierzykeln in $\mathfrak{S}_d$ sind zueinander konjugiert.

*Beweis:* $(a\ b\ c)$ und $(a'\ b'\ c')$ seien zwei Dreierzykeln und $\pi$ eine Permutation, die $a'$ auf $a$, $b'$ auf $b$ und $c'$ auf $c$ abbildet. Dann bildet $\pi^{-1}(a\ b\ c)\pi$ das Element $a'$ zunächst ab auf $a$, dann via $(a\ b\ c)$ auf $b$, und weiter via $\pi^{-1}$ auf $b'$. Genauso überlegt man sich, daß $b'$ auf $c'$ und $c'$ auf $a'$ abgebildet wird.

Ein $x \notin \{a', b', c'\}$ wird von $\pi$ abgebildet auf ein $\pi(x) \notin \{a, b, c\}$, so daß $\pi(x)$ von $(a\ b\ c)$ festgelassen wird. Durch $\pi^{-1}$ wird es wieder zurück auf $x$ abgebildet. Somit ist $\pi^{-1}(a\ b\ c\ )\pi = (a'\ b'\ c')$.

**3. Schritt:** Für $d \geq 5$ sind je zwei Dreierzykel sogar bereits in $\mathfrak{A}_d$ zueinander konjugiert.

*Beweis:* $(a\ b\ c)$ und $(a'\ b'\ c')$ seien zwei Dreierzykeln und $\pi \in \mathfrak{S}_d$ eine Permutation, für die $\pi^{-1}(a\ b\ c)\pi = (a'\ b'\ c')$ ist. Falls $\pi$ in $\mathfrak{A}_d$ liegt, sind wir fertig. Andernfalls existiert wegen $d \geq 5$ eine Transposition $\tau$, die jedes der drei Elemente $a, b, c$ festläßt. Somit ist $\tau^{-1}(a\ b\ c)\tau = (a\ b\ c)$ und damit $(\tau\pi)^{-1}(a\ b\ c)(\tau\pi) = \pi^{-1}(a\ b\ c\ )\pi = (a'\ b'\ c')$. Da $\pi$ eine ungerade Permutation ist, muß $\tau\pi$ gerade sein, also in $\mathfrak{A}_d$ liegen.

**4. Schritt:** Für $d \geq 5$ ist jeder Normalteiler von $\mathfrak{A}_d$, der einen Dreierzyklus enthält, gleich $\mathfrak{A}_d$.

*Beweis:* Falls er einen Dreierzyklus enthält, muß er nach dem vorigen Schritt *alle* Dreierzykeln enthalten, ist also nach dem ersten Schritt gleich $\mathfrak{A}_d$.

Der Satz folgt nun aus

**5. Schritt:** Für $d \geq 5$ enthält jeder nichttriviale Normalteiler $N \trianglelefteq \mathfrak{A}_d$ einen Dreierzyklus.

*Beweis:* Ist $\pi$ irgendein Element von $N$, so ist auch $\pi^{-1} \in N$, und für jedes $\omega \in N$ liegt auch $\omega^{-1}\pi^{-1}\omega$ in $N$, und damit auch $\pi\omega^{-1}\pi^{-1}\omega$.

Jedes Element $\pi \in N$ läßt sich schreiben als Produkt elementfremder Zykeln. Wir betrachten ein Element, das einen Zyklus der maximal vorkommenden Länge enthält.

Ist diese Länge mindestens gleich vier, ist $\pi$ Produkt eines Zykels $(a\ b\ c\ d\ \ldots)$ der Länge mindestens vier und eventuell weiterer Zykeln. Wir setzen $x = \pi^{-1}(a)$ und betrachten $\omega = (c\ a\ b)$. Das Produkt $\pi\omega^{-1}\pi^{-1}\omega$ bildet $a$ über die Zwischenergebnisse $a \mapsto c \mapsto b \mapsto c \mapsto d$ ab auf $d$, welches via $d \mapsto d \mapsto c \mapsto a \mapsto b$ auf $b$ geht. Dieses wiederum wird via $b \mapsto a \mapsto x \mapsto x \mapsto a$ auf $a$ abgebildet. Bei den übrigen Elementen überzeugt man sich leicht, daß sie auf sich selbst abgebildet werden; somit ist $\pi\omega^{-1}\pi^{-1}\omega = (a\ d\ b)$ ein Dreierzyklus aus $N$.

Falls die maximale Länge gleich drei ist und wir keinen Dreierzyklus haben, gibt es eine Permutation $\pi \in N$, die das Produkt eines Dreierzyklus mit Dreier- und Zweierzykeln ist. Der Dreierzyklus sei

$(a\ b\ c)$, der nächste nichttriviale Faktor sei entweder ein Dreierzyklus $(d\ e\ f)$ oder eine Transposition $(d\ e)$. Wir betrachten wieder die Permutation $\pi\omega^{-1}\pi^{-1}\omega$, dieses Mal für $\omega = (d\ b\ a)$. Nun geht $a$ via $a \mapsto d \mapsto x \mapsto x \mapsto d$ auf $d$, welches via $d \mapsto b \mapsto a \mapsto b \mapsto c$ auf $c$ geht, welches wiederum via $c \mapsto c \mapsto b \mapsto d \mapsto e$ auf $e$ geht. Damit enthält $\pi\omega^{-1}\pi^{-1}\omega$ einen Zyklus der Länge mindestens vier, im Widerspruch zu unserer Annahme, der längste Zyklus eines jeden Elements sei höchstens ein Dreierzyklus.

Bleibt noch der Fall, daß sich jedes Element von $N$ als Produkt elementfremder Transpositionen schreiben läßt. Deren Anzahl muß gerade sein, es gibt also ein Element, das einen Faktor $(a\ b)(c\ d)$ enthält mit vier verschiedenen Zahlen $a, b, c, d$, und es gibt noch mindestens eine weitere Zahl $e$, die von diesen vier Zahlen verschieden ist. Wir setzen $x = \pi^{-1}(e)$ und betrachten $\pi\omega^{-1}\pi^{-1}\omega$ für $\omega = (e\ c\ a)$. Hier zeigen die Abbildungsketten $a \mapsto e \mapsto x \mapsto x \mapsto e$, $e \mapsto c \mapsto d \mapsto d \mapsto c$ und $c \mapsto a \mapsto b \mapsto b \mapsto a$, daß $\pi\omega^{-1}\pi^{-1}\omega$ den Dreierzyklus $(a\ e\ c)$ enthält, im Widerspruch zur Annahme, daß alle Elemente von $N$ Produkte elementfremder Transpositionen sind. Also tritt auch dieser Fall nicht auf, und wir haben gezeigt, daß $N$ auf jeden Fall einen Dreierzyklus enthalten muß. ∎

Da die Gruppe $\mathfrak{A}_d$ für $d \geq 4$ nicht abelsch ist, ist sie erst recht nicht zyklisch; daher zeigt der gerade bewiesenen Satz zusammen mit dem davor bewiesenen Lemma, daß die Gruppe $\mathfrak{S}_d$ für $d \geq 5$ nicht auflösbar ist. Als Korollar folgt sofort der

**Satz von Abel:** Für $d \geq 5$ ist die allgemeine Gleichung $d$-ten Grades nicht durch Radikale auflösbar. ∎

## §4: Konstruktionen mit Zirkel und Lineal

In der klassischen EUKLIDischen Geometrie geht man aus von einer Menge $\{P_0, \ldots, P_r\}$ von Punkten der Ebene und konstruiert daraus „mit Zirkel und Lineal“ weitere Punkte. Dabei sind folgende Operationen erlaubt:

- Durch zwei der vorhandenen Punkte wird eine Gerade gezeichnet (mit dem Lineal)
- Um einen der vorhandenen Punkte wird eine Kreislinie gezeichnet, die einen anderen der vorhandenen Punkte enthält (mit dem Zirkel)
- Schnittpunkte der gezeichneten Geraden und/oder Kreise werden zu den vorhandenen Punkten dazugenommen.

Diese Operationen können beliebig oft wiederholt werden.

Um solche Konstruktionen mit Körpererweiterungen in Verbindung zu bringen, wählen wir ein kartesisches Koordinatensystem und haben nun zwei Möglichkeiten: Entweder wir adjungieren für jeden Punkt $P_j = (x_j, y_j)$ die Koordinaten $x_j, y_j \in \mathbb{R}$ an $\mathbb{Q}$ und erhalten so einen Körper $k_0 < \mathbb{R}$, oder wir adjungieren stattdessen die komplexe Zahl $x_j + iy_j$ an $\mathbb{Q}$ und erhalten einen Körper $k_0' < \mathbb{C}$. Da wir in der Geometrie eher an reelle Koordinaten gewohnt sind, ist der erste Zuganng anschaulicher, so daß wir zunächst diesen benutzen werden. Bei der Frage nach der Konstruierbarkeit regelmäßiger $n$-Ecke werden sich allerdings die komplexen Zahlen als nützlicher erweisen.

Die Gerade durch zwei Punkte $P_i = (x_i, y_i)$ und $P_j = (x_j, y_j)$ ist die Lösungsmenge der Gleichung

$$(x - x_i)(y_j - y_i) + (y - y_i)(x_j - x_i) = 0 \,,$$

deren sämtliche Koeffizienten in $k_0$ liegen. Die Kreislinie um $P_i$, auf der $P_j$ liegt, wird entsprechend beschrieben durch die quadratische Gleichung

$$(x - x_i)^2 + (y - y_i)^2 = (x_j - x_i)^2 + (y_j - y_i)^2 \,,$$

deren Koeffizienten ebenfalls in $k_0$ liegen.

Zur Berechnung des Schnittpunkts zweier verschiedener Geraden müssen wir ein lineares Gleichungssystem mit Koeffizienten aus $k_0$ lösen; falls es eine Lösung gibt, d.h. wenn die Geraden nicht parallel sind, ist diese ein Punkt mit Koordinaten in $k_0$.

Beim Schnitt einer Geraden $ax + by = c$ mit einem Kreis beachten wir zunächst, daß $a$ und $b$ nicht beide verschwinden können. Wir können die Gleichung also nach mindestens einer der beiden Variablen auflösen.

Das Ergebnis setzen wir ein in die Kreisgleichung und erhalten eine quadratische Gleichung in der anderen Variablen. Wenn es Schnittpunkte gibt, hat diese reelle Lösungen, die entweder in $k_0$ liegen oder in einem Körper $k_1/k_0$, der aus $k_0$ entsteht durch Adjunktion der Quadratwurzel eines Elements von $k_0$. Im letzteren Fall ist $k_1/k$ eine Erweiterung vom Grad zwei.

Ähnlich ist die Situation beim Schnitt von zwei Kreisen: Die Differenz der beiden Gleichungen

$$(x-a)^2 + (y-b)^2 = r^2 \quad \text{und} \quad (x-c)^2 + (y-d)^2 = s^2$$

ist eine lineare Gleichung in $x$ und $y$ (es sei denn, die beiden Kreise wären konzentrisch), definiert also eine Gerade, und die Schnittmenge der beiden Kreislinien ist gleich der Schnittmenge dieser Geraden mit einer der beiden Kreislinien.

Falls wir eine Konstruktion mit Zirkel und Lineal durchführen können, liegen die Koordinaten aller konstruierter Punkte somit in einem Körper $k$, der aus $k_0$ durch schrittweise Körpererweiterungen vom Grad zwei entsteht:

$$k_0 < k_1 < \cdots < k_n = k \quad \text{und} \quad [k_i : k_{i-1}] = 2 \quad \forall i = 1, \ldots, n\,.$$

Insbesondere ist $[k : k_0] = 2^n$ eine Zweierpotenz.

Betrachten wir einige klassische mathematische Konstruktionsprobleme unter diesem Gesichtspunkt! Am einfachsten geht das beim sogenannten Delischen Problem: Der Legende nach fragten die Einwohner der griechischen Insel Delos (eine der kleinsten der Kykladen im Ägäischen Meer) anläßlich einer Pestepedemie ihr Orakel um Rat. Dieses verlangte, daß sie den würfelförmigen Altar im Tempel des Apollon durch einen Würfel mit doppeltem Volumen ersetzen sollten. Natürlich mußte dessen Kantenlänge aus der des alten Würfels mit Zirkel und Lineal konstruiert werden.

Wir haben also zwei Ausgangspunkte $P_0$ und $P_1$ derart, daß die Strecke $\overline{P_0P_1}$ der Kantenlänge des alten Würfels entspricht. Da wir das Koordinatensystem und die Einheit frei wählen können, sei etwa $P_0 = (0,0)$ und $P_1 = (1,0)$. Wir müssen zwei Punkte $P_i, P_j$ konstruieren, deren

Verbindungsstrecke die Länge $\sqrt[3]{2}$ hat. Wenn wir das können, können wir diese Strecke von $P_1$ aus auf der $x$-Achse abtragen und erhalten den Punkt $(\sqrt[3]{2}, 0)$; der Körper $k$, in dem nach Ende der Konstruktion alle Koordinaten liegen, muß also die dritte Wurzel aus zwei enthalten und hat somit $\mathbb{Q}(\sqrt[3]{2})$ als Teilkörper. Damit muß $[k : \mathbb{Q}]$ durch drei teilbar sein, ist also keine Zweierpotenz. Daher ist das Delische Problem nicht mit Zirkel und Lineal lösbar.

Als nächstes betrachten wir das Problem der Konstruktion des regelmäßigen $n$-Ecks mit Zirkel und Lineal. Die griechischen Mathematiker konnten natürlich gleichseitige Dreiecke und Quadrate konstruieren, ebenso das regelmäßige Fünfeck, das Fünfzehneck, und über die Halbierung des Innenwinkeld damit auch jedes $n$-Eck, dessen Eckenanzahl eine der genannten Zahlen mal einer Zweierpotenz ist. Erst rund zwei Tausend Jahre später gelang 1796 dem damals 19-jährigen GAUSS die Konstruktion eines weiteren regelmäßigen $n$-Ecks, des Siebzehnecks. In seinem 1798 geschriebenen und 1801 erschienenen Buch *Disquisitiones Arithmeticae* bewies er allgemein, welche regelmäßigen $n$-Ecke sich mit Zirkel und Lineal konstruieren lassen und welche nicht.

Um sein Ergebnis zu verstehen, empfiehlt es sich, die Ebene mit der komplexen Zahlenebene zu identifizieren und das Problem so in Algebra zu übersetzen, daß wir nach der Konstruktion eines Punktes $P$ mit Koordinaten $(x, y)$ die komplexe Zahl $x + iy$ adjungieren.

Wenn wir ausgehen vom Mittelpunkt $P_0 = (0, 0)$ des regelmäßigen $n$-Ecks und einer Ecke $P_1 = (1, 0)$, haben die weiteren Ecken die Koordinaten $(\cos \frac{2\pi j}{n}, \sin \frac{2\pi j}{n})$ für $j = 1, \ldots, n-1$. Diese Punkte werden identifiziert mit den komplexen Zahlen

$$\cos \frac{2\pi j}{n} + i \sin \frac{2\pi j}{n} = e^{2\pi i j/n} = \left(e^{2\pi i/n}\right)^j ;$$

falls das regelmäßige $n$-Eck mit Zirkel und Lineal konstruierbar ist, muß also die primitive $n$-te Einheitswurzel $\zeta = e^{2\pi i/n}$ in einem Erweiterungskörper von Zweipotenzordnung über $\mathbb{Q}$ liegen.

Der Körper $\mathbb{Q}(\zeta)$ enthält natürlich auch alle Potenzen von $\zeta$, ist also ein Zerfällungskörper des Polynoms $X^n - 1$. Dieses ist aber nicht irreduzibel, beispielsweise ist $X - 1$ ein Teiler, da die Eins eine Nullstelle ist.

Allgemeiner: Ist $n = mq$, so ist $X-1$ auch ein Teiler von $X^q-1$; ersetzen wir hier $X$ durch $X^m$, folgt, daß $X^m-1$ Teiler von $X^{mq}-1 = X^n-1$ ist. Bezeichnet also $f$ den irreduziblen Faktor von $X^n-1$, der $\zeta$ als Nullstelle hat, so hat $f$ nur primitive $n$-te Einheitswurzeln als Nullstellen, denn ist $x$ bereits eine $m$-te Einheitswurzel für einen echten Teiler $m$ von $n$, so ist $x$ Nullstelle von $X^m-1$. Wäre sie auch eine Nullstelle von $f$, so wäre $x$ eine mehrfache Nullstelle des Polynoms $X^n-1$. Da dessen Ableitung $nX^{n-1}$ nur bei der Null verschwindet, ist das nicht möglich.

Die primitiven $n$-ten Einheitswurzel allerdings müssen allesamt Nullstellen von $f$ sein nach dem folgenden Argument von DEDEKIND: Da die primitiven $n$-ten Einheitswurzeln genau die Potenzen $\zeta^j$ sind, für die $j$ teilerfremd zu $n$ sind, läßt sich $j$ schreiben als Produkt von Primzahlen, die keine Teiler von $n$ sind. Daher reicht es zu zeigen, daß für jede Nullstelle $\xi$ von $f$ und jede Primzahl $p$, die kein Teiler von $n$ ist, auch $\xi^p$ eine Nullstelle von $f$ ist. Falls dies für irgendein $\xi$ und irgendein $p$ nicht der Fall ist, muß $\xi^p$ Nullstelle eines weiteren irreduziblen Polynoms $g$ sein. Da $\xi^p$ eine primitive $n$-te Einheitswurzel ist, muß auch $g$ ein Teiler von $X^n-1$ sein. Betrachten wir das Polynom $G = g(X^p) \in \mathbb{Q}[X]$. Da $g(\xi^p)$ verschwindet, ist $\xi$ eine Nullstelle von $G$.

Nach dem Lemma von GAUSS können wir bei der Zerlegung des Polynoms $X^n-1$ in $\mathbb{Q}[X]$ annehmen, daß alle Faktoren ganzzahlige Koeffizienten haben, daß also $f, g$ und damit auch $G$ in $\mathbb{Z}[X]$ liegen. Wenn wir alle Koeffizienten modulo $p$ reduzieren, erhalten wir Polynome $\overline{f}, \overline{g}$ und $\overline{G}$ aus $\mathbb{F}_p[X]$, wobei $\overline{f}$ und $\overline{g}$ zwei verschiedene (nicht notwendigerweise irreduzible) Faktoren von $X^n-1$ in $\mathbb{F}_p[X]$ sind. Da in $\mathbb{F}_p$ jedes Element gleich seiner $p$-ten Potenz ist, ist $\overline{G} = g^p$. Somit sind alle Nullstellen von $\overline{G}$ auch Nullstellen von $\overline{g}$. Die Polynome $f$ und $G$ aus $\mathbb{Z}[X]$ haben in $\mathbb{Q}(\zeta)$ die gemeinsame Nullstelle $\xi$, also hat der ggT $h$ der beiden Polynome positiven Grad. Betrachten wir ihn modulo $p$, erhalten wir ein Polynom $\overline{h}$, das sowohl $\overline{f}$ als auch $\overline{G}$ teilt. Wegen $\overline{G} = \overline{g}^p$ folgt, daß auch der ggT von $\overline{f}$ und $\overline{g}$ positiven Grad hat. Somit hat das Polynom $X^n-1 \in \mathbb{F}_p[X]$ in seinem Zerfällungskörper mindestens eine mehrfache Nullstelle. Das ist aber nicht möglich, denn seine (formale) Ableitung $nX^{n-1}$ ist nicht das Nullpolynom, da

$p$ kein Teiler von $n$ ist, und es hat nur die Null als Nullstelle, die aber keine Nullstelle von $X^n - 1$ ist. Daher hat $X^n - 1$ auch als Polynom über $\mathbb{F}_p$ keine mehrfache Nullstelle, so daß die Annahme $f(\xi^p) \neq 0$ zu einem Widerspruch führt. Dies zeigt, daß $f$ genau die primitiven $n$-ten Einheitswurzeln als Nullstellen hat.

Somit hat das irreduzible Polynom $f \in \mathbb{Q}[X]$ mit $f(\zeta) = 0$ den Grad $\varphi(n)$, wobei $\varphi$ die aus dem zweiten Kapitel bekannte EULERsche $\varphi$-Funktion ist, die die Anzahl der primen Restklassen modulo $n$ angibt. Da alle Nullstellen von $f$ Potenzen von $\zeta$ sind, ist $\mathbb{Q}(\zeta)$ ein Zerfällungskörper von $f$ über $\mathbb{Q}$; insbesondere ist die Körpererweiterung $\mathbb{Q}(\zeta)/\mathbb{Q}$ GALOISsch und hat den Grad $\varphi(n)$.

Dies zeigt, daß das regelmäßige $n$-Eck nur dann mit Zirkel und Lineal konstruierbar sein kann, wenn $\varphi(n)$ eine Zweierpotenz ist. Wie wir uns in Kapitel zwei überlegt haben, läßt sich $\varphi(n)$ anhand der Primzerlegung von $n$ bestimmen: Für

$$n = \prod_{i=1}^{r} p_i^{e_i} \qquad \text{ist} \quad \varphi(n) = \prod_{i=1}^{r} \left( p_i^{e_i - 1} \cdot (p_i - 1) \right) .$$

Somit müssen alle Faktoren in diesem Produkt Zweierpotenzen sein.

Im Falle $p_i = 2$ ist das automatisch erfüllt; alle anderen möglichen $p_i$ sind ungerade, so daß $e_i = 1$ sein muß und $p_i - 1$ eine Zweierpotenz.

Primzahlen der Form $2^r + 1$ heißen FERMATsche Primzahlen. $2^r + 1$ kann nur dann prim sein, wenn $r$ eine Zweierpotenz ist, denn ist $r$ ungerade, so ist $2^r + 1 \equiv (-1)^r + 1 = 0 \bmod 3$ durch drei teilbar, und ist $r = 2^s u$ mit einer ungeraden Zahl $u > 1$, so ist $2^r + 1 \equiv (-1)^u + 1 \equiv 0 \bmod 2^s + 1$ durch $2^s + 1$ teilbar.

**Definition:** Die $m$-te FERMAT-Zahl ist $F_m = 2^{2^m} + 1$; falls $F_m$ prim ist, heißt $F_m$ eine FERMATsche Primzahl.

FERMAT vermutete, daß alle $F_m$ prim seien; das ist eine der sehr wenigen seiner Vermutungen, die sich als falsch herausstellten. $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ und $F_4 = 65\,537$ sind in der Tat allesamt prim (was auch FERMAT wußte), aber wie EULER 1732 zeigte, ist

$$F_5 = 4\,294\,967\,297 = 641 \cdot 6\,700\,417 .$$

Auch alle anderen $F_m$ mit $m \geq 5$, die bislang getestet wurden, sind keine Primzahlen; es ist also nicht bekannt, ob es ein $m \geq 5$ gibt, für das $F_m$ prim ist.

Für die Konstruierbarkeit des regelmäßigen $n$-Ecks folgt:

**Satz:** Falls das regelmäßige $n$-Eck mit Zirkel und Lineal konstruierbar ist, läßt sich $n$ als Produkt einer Zweierpotenz (die auch eins sein kann) mit verschiedenen FERMATschen Primzahlen schreiben. ∎

Als Korollar zu diesem Satz können wir sofort auch die Unlösbarkeit eines anderen klassischen geometrischen Problems zeigen:

**Korollar:** Es ist nicht möglich, einen beliebigen Winkel mit Zirkel und Lineal in drei gleiche Teile zu zerlegen.

*Beweis:* Falls es ein solches Verfahren gäbe, könnte man insbesondere den Innenwinkel eines gleichseitigen Dreiecks dreiteilen. Damit wäre der Innenwinkel des regelmäßigen Neunecks und damit dieses selbst mit Zirkel und Lineal konstruierbar, im Widerspruch zum gerade gezeigten Resultat von GAUSS. ∎

GAUSS bewies auch die Umkehrung des obigen Satzes; bevor wir uns damit beschäftigen, wollen wir uns aber davon überzeugen, daß zumindest in vielen Fällen klassische Konstruktionsverfahren ausreichen. Beginnen wir mit den einzelnen Faktoren:

Die Konstruierbarkeit des regelmäßigen Dreiecks ist aus der Schule bekannt, das $2^m$-Eck für $m \geq 2$ kann aus dem Quadrat durch Winkelhalbierungen konstruiert werde. Die Konstruktion des regelmäßigen Fünfecks wird in der Schule üblicherweise nicht behandelt, war aber bereits den Pythagoräern bekannt: Diese brauchten sie für ihr Symbol, den fünfzackigen Stern, bestehend aus den sämtlichen Diagonalen eines regelmäßigen Fünfecks. Die Konstruktion des regelmäßigen Siebzehnecks geht, wie erwähnt, zurück auf GAUSS, der auch den obigen Satz (einschließlich seiner Umkehrung) bewies. Das grundsätzliche Verfahren, wie er aus der Struktur der GALOIS-Gruppe eine Konstruktion des

Siebzehnecks herleitete, führte später auch zur Konstruktion des 257-Ecks durch

MAGNUS GEORG PAUCKER: Geometrische Verzeichnung des regelmäßigen Siebzehn-Ecks und des regelmäßige Zweyhundersiebenundfunfzig-Ecks in den Kreis, *Jahresverhandlungen der Kurländischen Gesellschaft für Literatur und Kunst* **2**, 1822, S. 160–219

(die Konstruktion des 257-Ecks beginnt Seite 188) und

FRIEDRICH JULIUS RICHELOT: De resolutione algebraica aequationis $x^{257} = 1$, sive de divisione circuli per bisectionem anguli septies repetitam in partes 257 inter se aequales commentatio coronata, *Journal für die reine und angewandte Mathematik* **9**, 1832, S. 1–26, 146–161, 209–230, 337–358.

Das regelmäßige 65 537-Eck konstruierte JOHANN GUSTAV HERMES in über zehnjähriger Arbeit; er hinterlegte das aus mehr als zweihundert großformatigen Seiten bestehende Manuskript 1889 in einem Handkoffer im mathematischen Institut der Universität Göttingen, wo es immer noch zu finden ist. 1894 veröffentlichte er eine siebzehnseitige Zusammenfassung

J. HERMES: Ueber die Teilung des Kreises in 65537 gleiche Teile, *Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen, Mathematisch-Physikalische Klasse,* 1894, S. 170–186.

Da er als Königsberger kein Mitglied der Göttinger Gesellschaft der Wissenschaften war, wurde das Manuskript dort von FELIX KLEIN vorgelegt.

Falls es ein $m \geq 5$ geben sollte, für das $F_m$ prim ist, folgt aus dem Satz von GAUSS, daß auch das regelmäßige $F_m$-Eck mit Zirkel und Lineal konstruierbar ist; eine entsprechende Konstruktion konnte natürlich bislang noch niemand vorlegen, und auch in Zukunft wird das nur schwer möglich sein: Die kleinste FERMAT-Zahl, von der nicht bekannt ist, ob sie prim ist oder nicht, ist $F_{33}$, und diese Zahl hat über fünf Milliarden Dezimalstellen.

Beschäftigen wir uns als nächstes mit den Produkten aus Zweierpotenzen und verschiedenen FERMATschen Primzahlen. Wir müssen zeigen:

Sind $n$ und $m$ zwei zueinander teilerfremde Zahlen derart, daß das regelmäßige $n$-Eck und das regelmäßige $m$-Eck beide mit Zirkel und Lineal konstruierbar sind, so läßt sich auch das regelmäßige $nm$-Eck konstruieren. Allgemein läßt sich das regelmäßige $r$-Eck genau dann mit Zirkel und Lineal konstruieren, wenn der Winkel beim Mittelpunkt zwischen zwei benachbarten Ecken konstruierbar ist. Beim $n$-Eck und beim $m$-Eck ist er $2\pi/n$ *bzw.* $2\pi/m$; wir müssen zeigen, daß sich daraus der Winkel $2\pi/nm$ konstruieren läßt. Da $n$ und $m$ teilerfremd sind, gibt es ganze Zahlen $a, b$, so daß $am + bn = 1$ ist. Multiplikation mit $2\pi/nm$ macht daraus

$$a \cdot \frac{2\pi}{n} + b \cdot \frac{2\pi}{m} = \frac{2\pi}{nm} \, .$$

Ganzzahlige Vielfache eines Winkels und Summen und Differenzen von Winkeln lassen sich problemlos mit Zirkel und Lineal konstruieren; somit ist auch der Winkel $2\pi/nm$ und damit das regelmäßige $nm$-Eck mit Zirkel und Lineal konstruierbar.

Für einen vollständigen Beweis der Umkehrung können wir beispielsweise zeigen, daß jeder Punkt mit Koordinaten in einer GALOISschen Körpererweiterung vom Grad $2^m$ mit Zirkel und Lineal konstruiert werden kann. Wir beginnen mit den Punkten, deren Koordinaten im Grundkörper selbst liegen.

**Lemma:** $P_0, \ldots, P_r$ seien Punkte der Ebene $\mathbb{R}^2$ mit $P_0 = (0,0)$ und $P_1 = (1,0)$, und $K/\mathbb{Q}$ entstehe aus $\mathbb{Q}$ durch Adjunktion der Koordinaten der $P_i$. Dann kann jeder Punkt $P$ mit Koordinaten in $K$ aus den Punkten $P_i$ mit Zirkel und Lineal konstruiert werden.

*Beweis:* $P$ habe die Koordinaten $(x, y)$ mit $x, y \in K$, und die Koordinaten der $P_i$ seien $(x_i, y_i)$. Dann ist

$$K = \mathbb{Q}(x_0, \ldots, x_r, y_0, \ldots, y_r) \, ,$$

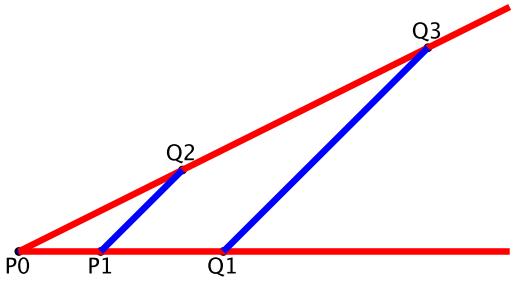
und $x, y$ lassen sich als rationale Funktionen in den $x_i$ und $y_i$ schreiben. Da wir $P$ konstruieren können, sobald wir Strecken der Längen $x$ und $y$ konstruiert haben, reicht es, daß wir aus gegebenen Streckenlängen auch alle Streckenlängen konstruieren können, die sich als rationale Funktionen in den gegebenen ausdrücken lassen. Dies folgt induktiv, sobald

wir wissen, daß wir aus gegebenen Längen auch deren Summen, Differenzen, Produkte und Quotienten konstruieren lassen. Für Summen und Differenzen ist dies trivial: Wir können die beiden Strecken einfach mit dem Zirkel auf einer festen Geraden abtragen.

Für Produkte und Quotienten können wir o.B.d.A. annehmen, daß beide Strecken positive Längen haben. Für das Produkt tragen wir auf dem von $P_0$ ausgehenden Strahl durch $P_1$ eine Strecke $\overline{P_0Q_1}$ der Länge $a$ ab, auf einem anderen Strahl durch $P_0$ eine Strecke $\overline{P_0Q_2}$ der Länge $b$. Sodann konstruieren wir die Parallele zur Geraden $P_1Q_2$ durch $Q_1$; sie schneide die Gerade $P_0Q_2$ im Punkt $Q_3$. Nach dem Strahlensatz ist dann

$$\left|\overline{P_0Q_3}\right| : \left|\overline{P_0Q_2}\right| = \left|\overline{P_0Q_1}\right| : \left|\overline{P_0P_1}\right| = a : 1 \,.$$

Da die Strecke $\overline{P_0Q_2}$ die Länge $b$ hat, muß daher $\overline{P_0Q_3}$ die Länge $ab$ haben.




Um für den Quotienten $a/b$ die gleiche Zeichnung verwenden zu können, tragen wir auf einen Strahl durch $P_0$ die Strecke $\overline{P_0Q_3}$ der Länge $a$ ab und auf dem Strahl von $P_0$ durch $P_1$ die Strecke $\overline{P_0Q_1}$ der Länge $b$. $Q_2$ sei der Schnittpunkt der Parallelen zu $Q_1Q_3$ durch $P_1$ mit dem Strahl durch $Q_3$. Nach dem Strahlensatz ist dann

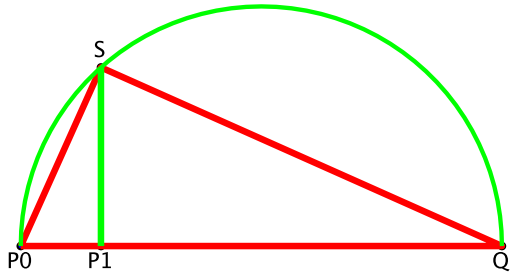
$$\left|\overline{P_0Q_3}\right| : \left|\overline{P_0Q_2}\right| = \left|\overline{P_0Q_1}\right| : \left|\overline{P_0P_1}\right| = a : 1 \,,$$

und da $\overline{P_0Q_3}$ die Länge $b$ hat, erfüllt die Länge $x$ von $\overline{P_0Q_2}$ die Relation $b : x = a : 1$, d.h. $x = b/a$.

■

**Lemma:** $P_0, \ldots, P_r$ seien Punkte der Ebene $\mathbb{R}^2$ mit $P_0 = (0,0)$ und $P_1 = (1,0)$, und $K/\mathbb{Q}$ entstehe aus $\mathbb{Q}$ durch Adjunktion der Koordinaten der $P_i$. Dann kann jeder Punkt $P$ mit Koordinaten in einem Erweiterungskörper $L/K$ vom Grad zwei aus den Punkten $P_i$ mit Zirkel und Lineal konstruiert werden.

*Beweis:* Jedes Element von $L$ liegt entweder bereits in $K$ oder ist Lösung einer quadratischen Gleichung mit Koeffizienten in $K$. Wir müssen uns also zusätzlich zum bereits im Beweis des vorigen Lemmas gezeigten überlegen, daß sich jede quadratische Gleichung mit Koeffizienten aus $K$ mit Zirkel und Lineal lösen läßt. Da wir alle Grundrechenarten ausführen können, müssen wir dazu nur noch zeigen, daß wir zu einer Strecke der Länge $a > 0$ auch eine Strecke der Länge $\sqrt{a}$ konstruieren können.




Dazu können wir beispielsweise auf der Geraden $P_0P_1$ die Strecke $a$ von $P_1$ aus als $\overline{P_1Q}$ in die von $P_0$ abgewandte Richtung abtragen. Über der Strecke $\overline{P_0Q}$ (mit Länge $a+1$) konstruieren wir den THALES-Kreis, d.h. wir konstruieren zunächst die Mittelsenkrechte zu $\overline{P_0Q}$, die diese im Punkt $M$ schneide; dann zeichnen wir den Kreis um $M$ durch $Q$ (und damit auch $P_0$). Mit diesem Kreis schneiden wir die Senkrechte zur Strecke $\overline{P_0Q}$ durch den Punkt $P_1$; einer der beiden Schnittpunkte sei $S$. Nach dem Satz des THALES ist $\Delta P_0QS$ ein rechtwinkliges Dreieck. Seine Hypothenuse $\overline{P_0Q}$ wird durch den Fußpunkt $P_1$ der Höhe $\overline{P_1S}$ in die Teilstrecken $\overline{P_0P_1}$ der Länge eins und $\overline{P_1Q}$ der Länge $a$ aufgeteilt. Nach dem Höhensatz ist das Quadrat der Höhe $h = \left|\overline{P_1S}\right|$ gleich dem Produkt $1 \cdot a$, d.h. $h = \sqrt{a}$.

■

**Korollar:** $P_0, \ldots, P_r$ seien Punkte der Ebene $\mathbb{R}^2$ mit $P_0 = (0,0)$ und $P_1 = (0,1)$, und $K/\mathbb{Q}$ entstehe aus $\mathbb{Q}$ durch Adjunktion der Koordinaten der $P_i$. Zum Körper $L/K$ gebe es eine Folge von Zwischenkörpern

$$K = L_0 < L_1 < \cdots < L_r = L$$

derart, daß $[L_i : L_{i-1}] = 2$ ist für $i = 1, \ldots, r$. Dann kann jeder Punkt $P$ mit Koordinaten in $L$ aus den Punkten $P_i$ mit Zirkel und Lineal konstruiert werden.

*Beweis* durch Induktion nach $r$: Für $r = 1$ ist das gerade das obige Lemma, und für $r > 1$ wissen wir nach der Induktionsvoraussetzung, daß sich jeder Punkt mit Koordinaten aus $L_{r-1}$ aus den $P_i$ konstruieren läßt. Da $L_r/L_{r-1}$ eine quadratische Erweiterung ist, gibt es ein $w \in L_{r-1}$, so daß sich jedes Element von $L_r$ in der Form $a + b\sqrt{w}$ mit $a, b \in L_{r-1}$ schreiben läßt. Da wir Strecken der Längen $a, b$ und $w$ nach Induktionsannahme konstruieren können und nach obigem Lemma zu $w$ auch $\sqrt{w}$, folgt die Behauptung. ∎

Die Voraussetzung dieses Korollars an der Körper $L$ ist schwer nachzuweisen; wir wollen uns überlegen, daß wir sie ersetzen können durch die einfachere Voraussetzung, daß $L/K$ GALOISsch ist und $[L : K]$ eine Zweierpotenz. $\mathrm{Aut}(L/K)$ ist dann eine Gruppe von Zweipotenzordnung; als erstes soll gezeigt werden, daß jede solche Gruppe auflösbar ist. Für die vorbereitenden Lemmata brauchen wir die Voraussetzung über die Gruppenordnung noch nicht und können sie daher etwas allgemeiner formulieren:

**Lemma:** Die Gruppe $G$ habe einen Normalteiler $N$ derart, daß sowohl $N$ als auch $G/N$ auflösbar sind. Dann ist auch $G$ auflösbar.

*Beweis:* Wegen der Auflösbarkeit von $N$ gibt es eine Folge von Untergruppen $N_0, \ldots, N_r$ von $N$ mit

$$\{1\} = N_r \trianglelefteq N_{r-1} \trianglelefteq \cdots \trianglelefteq N_1 \trianglelefteq N_0 = N$$

derart, daß alle Faktorgruppen $N_{j-1}/N_j$ zyklisch sind. Entsprechend gibt es eine Folge von Untergruppen

$$\{1\} = N/N = \overline{G}_s \trianglelefteq \overline{G}_{s-1} \trianglelefteq \cdots \trianglelefteq \overline{G}_1 \trianglelefteq \overline{G}_0 = G/N$$

derart, daß alle Faktorgruppen $\overline{G}_{j-1}/\overline{G}_j$ zyklisch sind. Die Abbildung $\varphi\colon G \to G/N$, die jedes $g \in G$ auf seine Restklasse module $N$ abbildet, ist ein Homomorphismus; daher sind die Urbilder $G_i = \varphi^{-1}(\overline{G}_i)$ der $\overline{G}_i$ Untergruppen von $G$ und

$$N = G_s \trianglelefteq G_{s-1} \trianglelefteq \cdots \trianglelefteq G_1 \trianglelefteq G_0 = G\,.$$

Da $N$ ein Normalteiler sowohl von $G_{j-1}$ als auch von $G_j$ ist, können wir $G_{j-1}/N$ abbilden nach $G_{j-1}/G_j$, indem wir die Nebenklasse $gN$

abbilden auf $gG_j$. Diese Abbildung ist offensichtlich surjektiv und hat den Kern $G_j/N$; nach dem Homomorphiesatz ist also

$$\overline{G}_{j-1}/\overline{G}_j = (G_{j-1}/N)/(G_j/N) \cong G_{j-1}/G_j$$

für alle $j$. Daher sind auch die Faktorgruppen $G_{j-1}/G_j$ zyklisch. Setzen wir die beiden Reihen hintereinander, sehen wir, daß $G$ auflösbar ist. ∎

**Lemma:** Jede endliche abelsche Gruppe $G$ ist auflösbar. Ist ihre Ordnung $m$ das Produkt der Primzahlpotenzen $p_i^{e_i}$ und $e$ die Summe der Exponenten $e_i$, so gibt es Untergruppen $G_0, \ldots, G_e$ von $G$ derart daß

$$\{1\} = G_e \trianglelefteq G_{e-1} \trianglelefteq \cdots G_1 \trianglelefteq G_0 = G$$

ist und jeweils $e_i$ der Faktorgruppen $G_{j-1}/G_j$ isomorph zu $\mathbb{Z}/p_i$ sind.

*Beweis* durch Induktion nach $e$: Für $e = 1$ ist $G$ eine zyklische Gruppe von Primzahlordnung; mit $G_1 = \{1\}$ und $G_0 = G$ ist die Behauptung trivialerweise erfüllt.

Nun sei $e > 1$ und $g \neq 1$ ein Element von $g$. Seine Ordnung sei $r$, und $p$ sei ein Primteiler von $r$. Dann ist $h = g^{r/p}$ ein Element der Ordnung $p$, erzeugt also eine zyklische Untergruppe $N$ der Ordnung $p$ in $G$. Wegen der Kommutativität von $G$ ist $N$ ein Normalteiler, und $G/N$ ist eine abelsche Gruppe der Ordnung $|G|/p$. Somit ist die Exponentensumme $e$ für $G/N$ um eins kleiner als für $G$; nach Induktionsvoraussetzung gilt die Behauptung also für $G/N$, und sie gilt natürlich auch für $N \cong \mathbb{Z}/p$. Nach dem vorigen Lemma ist $G$ daher auflösbar, und da die Faktorgruppen sowohl für $N$ als auch für $G/N$ zyklisch von Primzahlordnung sind, gilt dies auch für die von $G$.

∎

**Satz:** Jede Gruppe $G$ von Primzahlpotenzordnung $p^n$ ist auflösbar. Es gibt eine Folge von Untergruppen $G_0, \ldots, G_n$ von $G$ derart, daß

$$\{1\} = G_n \trianglelefteq G_{n-1} \trianglelefteq \cdots \trianglelefteq G_1 \trianglelefteq G_0 = G$$

ist und $G_{i-1}/G_i \cong \mathbb{Z}/p$ für $i = 1, \ldots n$.

*Beweis* durch Induktion nach $n$: Für $n = 0$ gibt es nichts zu beweisen; im Falle $n = 1$ ist $G$ isomorph zu $\mathbb{Z}/p$, denn jedes Element außer dem

Neutralelement muß nach LAGRANGE die Ordnung $p$ haben. Sei also $n \geq 2$.

Wir definieren das *Zentrum* einer Gruppe $G$ als

$$Z(G) = \{x \in G \mid xg = gx \text{ für alle } g \in G\} .$$

es ist eine Untergruppe, denn es enthält offensichtlich das Neutralelement, und für zwei Elemente $x, y \in Z(G)$ ist

$$(xy)g = x(yg) = x(gy) = (xg)y = (gx)y = g(xy)$$

und

$$x^{-1}g = (g^{-1}x)^{-1} = (xg^{-1})^{-1} = gx^{-1}$$

für alle $g \in G$. Tatsächlich ist $Z(G)$ sogar ein Normalteiler von $G$, denn durch Multiplikation von links mit $g^{-1}$ wird die Gleichung $xg = gx$ zu $g^{-1}xg = g^{-1}gx = x$; ein Element $x \in G$ liegt also genau dann im Zentrum von $G$, wenn $x^g = x$ ist für alle $g \in G$.

Wir wollen uns als nächstes überlegen, daß $Z(G)$ für eine Gruppe der Ordnung $p^n$ mit $n \geq 1$ nicht nur aus dem Neutralelement bestehen kann: Dazu lassen wir $G$ durch Konjugation auf sich selbst operieren, betrachten also die Operation

$$\begin{cases} G \times G \to G \\ \quad (g, x) \mapsto x^g = g^{-1}xg \end{cases} .$$

Die Bahn eines Elements $x \in G$ besteht aus allen Konjugierten von $x$. Genau dann, wenn $x$ im Zentrum liegt, sind alle Konjugierten von $x$ gleich $x$, die Bahn von $x$ besteht also nur aus $x$ selbst. Für alle anderen Elemente von $G$ enthält sie mindestens ein weiteres Element. Nach der Bahnbilanzgleichung ist ihre Elementanzahl der Quotient aus der Gruppenordnung durch die Ordnung des Stabilisators; für eine Gruppe von $p$-Potenzordnung ist das eine $p$-Potenz ungleich eins, also eine durch $p$ teilbare Zahl.

Somit enthält die Bahn eines Elements aus dem Zentrum genau ein Element; jede andere Bahn enthält eine durch $p$ teilbare Anzahl von Elementen. Da jedes Element von $G$ in genau einer Bahn liegt, ist die Summe der Mächtigkeiten gleich der Gruppenordnung $p^n$. Diese

Summe ist gleich der Ordnung des Zentrums, die wegen $e \in Z(G)$ mindestens eins sein muß, plus einer durch $p$ teilbaren Zahl. Somit muß auch die Ordnung des Zentrums durch $p$ teilbar und damit mindestens $p$ sein.

Haben wir also eine Gruppe $G$ der Ordnung $p^n$ mit $n > 1$, so hat $Z(G)$ mindestens die Ordnung $p$. Das Zentrum ist Normalteiler und als abelsche Gruppe auch auflösbar; nach einem der obigen Lemmata sind alle Faktorgruppen zyklisch von Primzahlordnung, also isomorph zu $\mathbb{Z}/p$, da die Ordnung von $Z(G)$ eine $p$-Potenz ist. Die Faktorgruppe $G/Z(G)$ hat höchstens Ordnung $p^{n-1}$, ist also nach Induktionsvoraussetzung auflösbar mit allen Faktorgruppen isomorph zu $\mathbb{Z}/p$, und damit ist auch $G$ aufllösbar mit allen Faktorgruppen isomorph zu $\mathbb{Z}/p$. ∎

Uns interessiert hier vor allem der Fall $p = 2$; hier sind also alle Faktorgruppen isomorph zu $\mathbb{Z}/2$, d.h. für eine GALOISsche Erweiterung $L/K$, deren Grad eine Zweierpotenz ist, gibt es eine Folge von ZwKn, von denen jeder eine quadratische Erweiterung seines Vorgängers ist. Daraus folgt insbesondere, daß das regelmäßige $n$-Eck mit Zirkel und Lineal konstruiert werden kann, wenn $n$ das Produkt einer Zweierpotenz mit verschiedenen FERMATschen Primzahlen ist.

## §5: Transzendente Zahlen und die Quadratur des Kreises

Eines der berühmtesten Probleme der klassischen Geometrie, das es sogar in die Umgangssprache geschafft hat, ist die Quadratur des Kreises, d.h. die Konstruktion eines Quadrats, das den gleichen Flächeninhalt hat wie ein vorgegebener Kreis. Wie wir in diesem Paragraphen sehen werden, kann diese Konstruktion nicht mit Zirkel und Lineal ausgeführt werden, da beispielsweise für den Kreis mit Radius eins die Seitenlänge des Quadrats in keiner endlichen Körpererweiterung von $\mathbb{Q}$ liegt.

**Definition:** $K/\mathbb{Q}$ sei eine Körpererweiterung. Ein Element $x \in K$ heißt *algebraisch,* wenn es ein Polynom $f \in \mathbb{Z}[X]$ gibt, das an der Stelle $x$ verschwindet. Andernfalls heißt $x$ *transzendent.*

Natürlich ist jede rationale Zahl algebraisch, denn der Bruch $p/q$ ist eine Nullstelle des linearen Polynoms $qX - p$. Auch Wurzeln, egal

ob reell oder nicht aus ganzen Zahlen, sind algebraisch als Nullstellen von Polynomen $X^n - a$. Allgemeiner ist sogar jeder Ausdruck, der nur rationale Zahlen, Grundrechenarten und Wurzeln enthält, algebraisch, denn die so konstruierte Zahl liegt in einer Körpererweiterung endlichen Grades $K/\mathbb{Q}$, und jedes Element $x$ eines solchen Körpers ist algebraisch: Da $K$ als $\mathbb{Q}$-Vektorraum endliche Dimension hat, können die Potenzen $x^n$ nicht alle linear unabhängig sein; wir erhalten also eine lineare Abhängigkeit, d.h. ein Polynom aus $\mathbb{Q}[X]$, das für $x$ verschwindet. Multiplikation mit dem Hauptnenner der Koeffizienten macht daraus ein Polynom aus $\mathbb{Z}[X]$, das bei $x$ verschwindet.

Die Idee, daß es nichtalgebraische Zahlen geben könne, kam erst im Laufe des achtzehnten Jahrhunderts auf, unter anderem bei GOTTFRIED WILHELM LEIBNIZ (1646–1716), der von ihnen sagte: Omnem rationem trancendunt. (Sie übersteigen jede Vernunft.) 1844 konnte JOSEPH LIOUVILLE (1809–1882) als erster von einer reellen Zahl beweisen, daß sie transzendent ist; es handelte sich um die ansonsten völlig uninteressante Zahl $\sum 10^{-i!}$, wobei über alle $i \in \mathbb{N}$ summiert wird. 1874 zeigte GEORG CANTOR (1845–1918) durch eine Variante seines ersten Diagonalverfahrens, daß es nur abzählbar viele algebraische (reelle oder komplexe) Zahlen gibt, während er mit seinem zweiten Diagonalverfahren die Überabzählbarkeit von $\mathbb{R}$ und $\mathbb{C}$ bewies und daraus folgerte, daß es überabzählbar viele transzendente Zahlen gibt. Trotzdem ist es im Einzelfall meist sehr schwer, die Transzendenz einer Zahl zu beweisen; es gibt hier noch viele offene Probleme.

Wenn wir ausgehen von Punkten mit rationalen Koordinaten, hat jeder Punkt, den wir daraus mit Zirkel und Lineal konstruieren können, algebraische Zahlen als Koordinaten, und auch die Länge jeder konstruierten Strecke ist algebraisch. Zur Quadratur eines Kreises mit gegebenem (und daher algebraischem) Radius $r$ müssen wir ein Quadrat mit Seitenlänge $r\sqrt{\pi}$ konstruieren. Falls dies mit Zirkel und Lineal möglich wäre, müßte $r\sqrt{\pi}$ und damit auch $\sqrt{\pi}$ und schließlich auch $\pi$ selbst algebraisch sein. Aus der Transzendenz von $\pi$ folgt somit die Unmöglichkeit der Quadratur des Kreises mit Zirkel und Lineal.

Ein erstes Problem beim Nachweis der Transzendenz von $\pi$ ist eine geeignete Definition von $\pi$. Klassisch war $\pi$ definiert als das Verhältnis des Kreisumfangs zu seinem Durchmesser, aber es gibt bislang keinen Transzendenzbeweis, der damit auskommt. Alle bekannten Beweise gehen aus von der Beziehung $e^{\pi i} = -1$.

1873 bewies CHARLES HERMITE die Transzendenz von $e$, danach erst

1882 CARL LOUIS FERDINAND VON LINDEMANN die von $\pi$. Für dessen Beweis wird die Transzendenz von $e$ nicht wirklich benötigt, allerdings verwendete und erweiterte er HERMITEs Methoden, so daß sein Beweis besser verständlich wird, wenn wir zunächst den von HERMITE betrachten.

CHARLES HERMITE (1822–1901) war einer der bedeutendsten Mathematiker des neunzehnten Jahrhunderts. Zu seinen Resultaten zählen eine Vereinfachung des ABELschen Beweises, daß Gleichungen fünften Grades im allgemeinen nicht durch Wurzelausdrücke gelöst werden können, die explizite Lösung solcher Gleichungen durch elliptische Funktionen, die er sodann auf zahlentheoretische Probleme anwendete, der Nachweis, daß $e$ eine transzendente Zahl ist, eine Interpolationsformel und vieles mehr. HERMITE galt als ein sehr guter akademischer Lehrer; er unterrichtete an der École Polytechnique, dem Collège de France, der École Normale Supérieure und der Sorbonne.

CARL LOUIS FERDINAND VON LINDEMANN (1852–1939) wurde in Hannover geboren und studierte in Göttingen, Erlangen, wo er bei FELIX KLEIN promovierte, und München. Danach besuchte er Universitäten in Oxford, Cambridge, London und Paris, wo er unter anderem mit HERMITE über dessen Transzendenzbeweis für $e$ und seine Versuche, diesen auf $\pi$ auszudehnen diskutierte. Während HERMITE damit erfolglos blieb, fand LINDEMANN 1882 den Trick, der HERMITE noch gefehlt hatte und konnte so mit dessen Methoden die Transzendenz von $\pi$ beweisen. Zunächst aber habilitierte er sich 1877 in Würzburg und wurde daraufhin Professor zunächst in Freiburg, dann 1883 in Königsberg und schließlich 1893 in München. Er hatte über sechzig Doktoranden, darunter als wohl berühmtesten DAVID HILBERT (1862–1943). Auch mathematische Seminare in ihrer heutigen Form gehen im wesentlichen auf ihn zurück.

Die folgende Darstellung ist eine Vereinfachung der Beweise von HERMITE und LINDEMANN; sie folgt im wesentlichen dem Anhang zu Kapitel 1 aus dem Buch

ANTOINE CHAMBERT-LOIR: Algèbre corporelle, *Les éditions de l'École Polytechnique, Palaiseau,* 2005.

Ausgangspunkt ist, für ein zunächst beliebiges Polynom $f \in \mathbb{R}[X]$ und eine komplexe Zahl $z$, das Integral

$$I(f,z) = \int_0^1 z e^{z(1-u)} f(zu)\, du\,.$$

Sein Wert kann über Funktionswerte von $f$ und seinen Ableitungen $f^{(j)}$ berechnet werden:

**Lemma:** Für ein Polynom $f \in \mathbb{R}[X]$ vom Grad $d$ ist

$$I(f,z) = e^z \sum_{j=0}^{d} f^{(j)}(0) - \sum_{j=0}^{d} f^{(j)}(z)\,.$$

*Beweis* durch Induktion nach $d$: Für $d = 0$ ist $f$ konstant; es gibt also ein $c \in \mathbb{R}$ mit $f(z) = c$ für alle $z \in \mathbb{R}$. Dann ist

$$I(f,z) = \int_0^1 cze^{z(1-u)}\, du = ce^z \int_0^1 ze^{-zu}\, du = ce^z \left( -e^{-zu}\Big|_0^1 \right)$$
$$= ce^z(-e^{-z}+1) = -c + ce^z = e^z f(0) - f(z)\,,$$

wie behauptet.

Für $d > 0$ führen wir das Integral durch partielle Integration auf $I(f',z)$ zurück: Der Integrand ist das Produkt von $f(zu)$ mit $ze^{z(1-u)}$, und wie wir beim Fall $d = 0$ gesehen haben, ist $ze^{z(1-u)}$ die Ableitung von $-e^{z(1-u)}$ nach $u$. Somit ist

$$I(f,z) = -e^{z(1-u)} f(zu)\Big|_0^1 + \int_0^1 ze^{z(1-u)} \cdot f'(zu)\, du$$
$$= -f(z) + e^z f(0) + I(f',z)\,.$$

$f'$ ist ein Polynom vom Grad $d-1$; nach Induktionsannahme ist daher

$$I(f',z) = e^z \sum_{j=0}^{d-1} f^{(j+1)}(0) - \sum_{j=0}^{d-1} f^{(j+1)}(z) = e^z \sum_{j=1}^{d} f^{(j)}(0) - \sum_{j=1}^{d} f^{(j)}(z)\,.$$

Um $I(f,z)$ zu bekommen, müssen wir nach der vorangehenden Formel noch $-f(z)+e^z f(0)$ addieren; dadurch bekommen die beiden Summen rechts noch ihren Term zum Index $j = 0$, was die behauptete Formel beweist.

∎

Die grundsätzliche Strategie bei den Transzendenzbeweisen für $e$ und $\pi$ besteht darin, daß uns die Annahme, eine Zahl sei algebraisch, für geeignete Polynome $f$ und geeignete Zahlen $z$ untere Schranken für den gerade hergeleiteten Ausdruck liefert. Diese können wir dann vergleichen mit oberen Schranken für geeignete Summen solcher Integrale und dabei auf einen Widerspruch hoffen.

Für die Konstruktion unterer Schranken im Falle der Ableitungen in obiger Formel ist vor allem die folgende elementare Aussage nützlich:

**Lemma:** Für ein Polynom $f \in \mathbb{Z}[X]$ sind alle Koeffizienten der $r$-ten Ableitung durch $r!$ teilbar. Insbesondere sind damit auch alle Werte von $f^{(r)}(x)$ an ganzzahligen Stellen $x$ durch $r!$ teilbar.

*Beweis:* Durch $r$-malige Ableitung wird der Summand $a_j X^j$ von $f$ im Falle $r > 0$ zu Null, ansonsten zu

$$\big(j-(r-1)\big)\big(j-(r-2)\big)\cdots(j-1)j\cdot a_j X^{j-r} = r!\binom{j}{r}\cdot a_j X^{j-r}\ .$$

Da sowohl die Binomialkoeffizienten als auch alle $a_j$ ganze Zahlen sind, sind alle Koeffizienten von $f^{(r)}$ durch $r!$ teilbar.

∎

Eine obere Schranke für $I(f,z)$ ist leicht zu finden: Der Betrag des Faktors $ze^{z(1-u)}$ ist für alle $u \in [0,\ 1]$ kleiner oder gleich $|z|\cdot e^{|z|}$, also ist der Betrag des Integranden höchstens gleich dieser Zahl mal dem Supremum von $|f(zu)|$ im Intervall $[0,\ 1]$. Um eine Schranke für das Integral zu bekommen, müssen wir nur noch mit der Länge eins des Integrationsintervalls multiplizieren und erhalten

**Lemma:** $|I(f,z)| \le |z|\cdot e^{|z|}\cdot \sup_{u\in[0,\,1]}|f(zu)|\ .$

∎

Damit haben wir im wesentlichen alles beisammen, um die Transzendenz von $e$ zu beweisen:

**Satz von** HERMITE**:** $e$ ist transzendent.

*Beweis:* Andernfalls müßte $e$ Nullstelle eines Polynoms $f \in \mathbb{Z}[X]$ sein, also etwa

$$f(e) = a_d e^d + a_{d-1} e^{d-1} + \cdots + a_1 e + a_0 = 0 \quad \text{mit} \quad a_j \in \mathbb{Z}\,.$$

Dabei können wir annehmen, daß $a_0$ nicht verschwindet, denn andernfalls können wir so lange durch $e$ dividieren, bis wir ein Polynom mit $a_0 \neq 0$ erhalten. Wir wollen uns überlegen, daß die Annahme $f(e) = 0$ auf einen Widerspruch führt.

Dazu betrachten wir für jede Primzahl $p$ das Polynom

$$f_p = X^{p-1}(X-1)^p \cdots (X-d)^p$$

vom Grad $(d+1)p - 1$ und die Zahl

$$J_p = a_0 I(f_p, 0) + a_1 I(f_p, 1) + \cdots + a_d I(f_p, d)\,.$$

Wie wir oben nachgerechnet haben, ist für $z = k$

$$I(f_p, k) = e^k \sum_{j=0}^{(d+1)p-1} f_p^{(j)}(0) - \sum_{j=0}^{(d+1)p-1} f_p^{(j)}(k)\,.$$

Die erste Summe ist unabhängig von $k$; wenn wir also über $k$ summieren, um $J_p$ zu bestimmen, können wir diese Summe ausklammern und erhalten

$$\begin{aligned} J_p &= \sum_{j=0}^{(d+1)p-1} f_p^{(j)}(0) \cdot \sum_{k=0}^{d} a_k e^k - \sum_{k=0}^{d} a_k \sum_{j=0}^{(d+1)p-1} f_p^{(j)}(k) \\ &= -\sum_{k=0}^{d} a_k \sum_{j=0}^{(d+1)p-1} f_p^{(j)}(k)\,, \end{aligned}$$

denn nach unserer Annahme verschwindet $f(e) = \sum_{k=0}^{d} a_k e^k$.

Nach Konstruktion von $f_p$ verschwinden auch alle $f_p^{(j)}(k)$ für $1 \leq k \leq d$ und $j = 0, \ldots, p-1$, denn $k$ ist ja eine $p$-fache Nullstelle von $f_p$. Für $j \geq p$ wissen wir immerhin nach dem obigen Lemma, daß alle Funktionswerte von $f^{(j)}$ an ganzzahligen Stellen Vielfache von $j!$ und damit insbesondere auch von $p!$ sind.

Da die Null nur eine $(p-1)$-fache Nullstelle von $f_p$ ist, verschwinden nur die Werte $f_p^{(j)}(0)$ mit $j < p-1$, und nach obigem Argument sind die mit $j \geq p$ durch $p!$ teilbar. Über $f_p^{(p-1)}(0)$ wissen wir noch nichts. Hier hilft uns die Verallgemeinerung der LEIBNIZ-Regel auf höhere Ableitungen, die man entweder aus der Analysis kennt oder durch Induktion mit Hilfe der klassischen Produktregel beweist: Für $r \geq 1$ und zwei mindestens $r$ mal differenzierbare Funktionen $u, v$ ist

$$(uv)^{(r)} = \sum_{j=0}^{r} \binom{r}{j} u^{(r-j)} v^{(j)} .$$

Dies wenden wir an auf $u = X^{p-1}$ und $v = (X-1)^p \cdots (X-d)^p$ und $r = p-1$. Alle Ableitungen von $u$ außer der $(p-1)$-ten verschwinden an der Stelle Null; daher ist

$$f_p^{(p-1)}(0) = (uv)^{(p-1)}(0) = \sum_{j=0}^{p-1} \binom{p-1}{j} u^{(p-1-j)}(0) v^{(j)}(0)$$

$$= u^{(p-1)}(0) v(0) = (p-1)!(-1)^p \cdots (-d)^p = (p-1)! \cdot (-1)^{dp} d!^p ,$$

und das ist für $p > d$ eine nicht durch $p$ teilbare Zahl. In der Summe

$$J_p = -\sum_{k=0}^{d} a_k \sum_{j=0}^{(d+1)p-1} f_p^{(j)}(k)$$

ist dann also jeder nichtverschwindende Summand durch $p!$ teilbar mit der einzigen möglichen Ausnahme von $a_0 f_p^{(p-1)}(0)$, der genau dann durch $p!$ teilbar ist, wenn $a_0$ Vielfaches von $p$ ist. Für $p > |a_0|$ ist das nicht der Fall; daher ist für alle hinreichend großen Primzahlen $p$

$$J_p \equiv (-1)^{dp+1} a_0 (p-1)! d!^p \not\equiv 0 \bmod p! .$$

Kürzen durch $(p-1)!$, was nach obiger Rechnung auch $f_p^{(p-1)}(0)$ teilt, macht daraus

$$\frac{J_p}{(p-1)!} \equiv (-1)^{dp-1} a_0 d!^p \not\equiv 0 \bmod p .$$

Insbesondere ist $J_p/(p-1)!$ damit auch selbst ungleich Null. Da es eine ganze Zahl ist, muß es mindestens Betrag eins haben, d.h. $(p-1)! \leq \left|J_p\right|$.

Um dies zu einem Widerspruch zu führen, verwenden wir das Lemma vom Beginn des Paragraphen über eine obere Abschätzung für die Integrale $I(f, z)$: Danach ist

$$\left|I(f_p, k)\right| \le k \cdot e^k \cdot \sup_{u \in [0,\,1]} \left|f_p(ku)\right| = k \cdot e^k \cdot \sup_{x \in [0,\,k]} \left|f_p(x)\right| \ .$$

Die Schranke auf der rechten Seite ist offensichtlich monoton wachsend in $k$; daher ist

$$\left|I(f_p, k)\right| \le d \cdot e^d \cdot \sup_{x \in [0,\,d]} \left|f_p(x)\right|$$

für $k = 1, \ldots, d$ und

$$|J|_p \le \|f\|_1 \cdot d \cdot e^d \cdot \sup_{x \in [0,\,d]} \left|f_p(x)\right| \ ,$$

wobei $\|f\|_1 = |a_0| + \cdots + |a_d|$ die $\mathrm{L}^1$-Norm jenes hypothetischen Polynoms $f$ ist, das in $e$ verschwindet.

Bleibt noch die Abschätzung der rechten Seite durch eine Funktion von $p$. Dazu zerlegen wir $f_p$ wieder in ein Produkt

$$f_p = X^{p-1} \cdot g^p \quad \text{mit} \quad g = (X-1)(X-2)\cdots(X-d) \, .$$

Im Intervall $[0,\, d]$ ist $|x| \le d$, und $|g(x)|$ nimmt irgendwo sein Maximum $M$ an. Somit ist

$$\sup_{x \in [0,\,d]} \left|f_p(x)\right| \le d^{p-1} M^p$$

für alle $p$ und

$$\left|J_p\right| \le \|f\|_1 \cdot d \cdot e^d \cdot d^{p-1} M^p = \|f\|_1 e^d (dM)^p < \left(\|f\|_1 d e^d M\right)^p$$

für alle Primzahlen $p$. Zusammen mit der obigen Abschätzung zeigt dies, daß für $c = \|f\|_1 d e^d M$ und alle hinreichend großen Primzahlen $p$ gilt

$$(p-1)! \le \left|J_p\right| \le c^p \, .$$

Das kann aber nicht sein, da $(p-1)!$ schneller wächst als jede $p$-te Potenz. Genauer ist nach der STIRLINGschen Formel

$$(p-1)! \sim \left(\frac{p-1}{e}\right)^{p-1} \sqrt{2\pi} \, ;$$

sobald $(p-1)/e$ hinreichend viel größer als $c$ ist, kann die Ungleichung also unmöglich richtig sein. Damit führt die Annahme, $e$ sei Nullstelle eines Polynoms mit ganzen Koeffizienten, zu einem Widerspruch, und die Transzendenz von $e$ ist bewiesen. ∎

Der Beweis für die Transzendenz von $\pi$ ist aufwendiger. Wie man heute weiß, bilden Funktionen wie die Exponentialfunktion algebraische Zahlen, abgesehen von offensichtlichen Ausnahmefällen wie $e^0 = 1$, nie auf algebraische Zahlen ab. Da $e^{\pi i} = -1$ algebraisch ist, kann daher $\pi i$ und damit auch $\pi$ nicht algebraisch sein. Der ursprüngliche Beweis von LINDEMANN konnte nicht auf solche allgemeinen Resultate zurückgreifen, verwendete aber auch die Beziehung $e^{\pi i} = -1$.

Wie HERMITE arbeitete er mit Integralen der Form $I(f, z)$, aber er definierte die Summen $J_p$ nicht wie HERMITE, indem er die Koeffizienten eines hypothetischen Polynoms mit Nullstelle $e$ *bzw.* $\pi$ verwendete, sondern er arbeitete mit den sämtlichen Nullstellen eines solchen Polynoms. Um Summen über die Nullstellen eines Polynoms typographisch einfach darstellen zu können, definieren wir

**Definition:** $f \in \mathbb{C}[X]$ sei ein Polynom vom Grad $d$ mit den (nicht notwendigerweise verschiedenen) Nullstellen $z_1, \ldots, z_d$, und $g\colon \mathbb{C} \to \mathbb{C}$ sei eine beliebige Funktion. Dann setzen wir

$$\sum_{f(z)=0} g(z) \underset{\text{def}}{=} \sum_{j=1}^{d} g(z_j) \quad \text{und} \quad \prod_{f(z)=0} g(z) \underset{\text{def}}{=} \prod_{j=1}^{d} g(z_j)\,.$$

Wenn $f$ ein Polynom mit ganzzahligen Koeffizienten ist, sind die Nullstellen $z_j$ algebraische Zahlen, und die Werte $g(z_j)$ werden im allgemeinen keine ganze Zahlen sein. Trotzdem gilt

**Lemma:** Für $f = a_d X^d + a_{d-1} X^{d-1} + \cdots + a_1 X + a_0$ mit $a_i \in \mathbb{Z}$ und ein weiteres Polynom $g \in \mathbb{Z}[X]$ vom Grad $n$ ist $a_d^n \sum_{f(z)=0} g(z)$ eine ganze Zahl.

*Beweis:* Unter einer Permutation der Nullstellen von $f$ ändert sich in der Summe nur die Reihenfolge der Summanden; $\sum_{f(z)=0} g(z)$ ist also ein

symmetrisches Polynom in den Nullstellen von $f$. Nach dem Hauptsatz über symmetrische Funktionen läßt sich dieses schreiben als Polynom mit ganzzahligen Koeffizienten in den elementarsymmetrischen Funktionen der Nullstellen und damit nach dem Wurzelsatz von VIÈTE als Polynom mit ganzzahligen Koeffizienten in den Koeffizienten des Polynoms $f/a_d$. (Der Wurzelsatz von VIÈTE gilt nur für Polynome mit höchstem Koeffizient eins.) Da $\sum_{f(z)=0} g(z)$ als Polynom in den Nullstellen $z_j$ von $f$ höchstens den Grad $n$ hat, hat auch dieses Polynom in den Koeffizienten $a_i/a_d$ von $f/a_d$ höchstens den Grad $n$. Durch Multiplikation mit $a_d^n$ erhalten wir daher ein Polynom mit ganzzahligen Koeffizienten in $a_0, \ldots, a_d$ und damit eine ganze Zahl. ∎

Der erste Schritt im Beweis der Transzendenz von $\pi$ zeigt, daß die entsprechende Aussage für eine Summe von Exponentialfunktionen höchstens dann gelten kann, wenn die Summe verschwindet:

**Lemma:** Für ein Polynom $f \in \mathbb{Z}[X]$ mit $f(0) \neq 0$ kann

$$\sum_{f(z)=0} e^z$$

keine von Null verschiedene ganze Zahl sein.

*Beweis:* Angenommen, die Summe wäre $N \in \mathbb{Z} \setminus \{0\}$. Wir wählen eine (beliebige) Primzahl $p$ und betrachten das Polynom $g = X^{p-1} f^p$ aus $\mathbb{Z}[X]$. Wenn wir den Grad von $f$ mit $d$ bezeichnen, hat es den Grad $m = p - 1 + pd = p(d+1) - 1$. Wir verwenden wieder eine Summe gewisser der von HERMITE eingeführten Integrale, hier

$$J_p \underset{\text{def}}{=} \sum_{f(z)=0} I(g, z) \, .$$

Nach der oben bewiesenen Abschätzung ist

$$|I(g,z)| \leq |z| \, e^{|z|} \sup_{u \in [0,1]} |g(zu)| \, .$$

Da $f$ ein Polynom ist, ist $|f(zu)|$ eine stetige Funktion von $u$ und nimmt daher auf dem kompakten Intervall [0, 1] ein Maximum $M_1$ an. Der Betrag von $uz$ ist dort kleiner oder gleich $|z|$. $M_2$ bezeichne das

Maximum der Beträge sämtlicher Nullstellen von $f$, falls dieses größer oder gleich eins ist, und eins sonst. Entsprechend sei $M_3$ das Maximum der $e^{|z|}$, mindestens aber eins. Dann ist

$$|I(g,z)| \leq M_2 \cdot M_3 \cdot M_2^{p-1} \cdot M_1^p \leq (M_1 M_2 M_3)^p$$

und $\left|J_p\right| \leq d(M_1 M_2 M_3)^p \leq (dM_1 M_2 M_3)^p$. Es gibt daher eine reelle Zahl $M$, für die gilt

$$\left|J_p\right| \leq M^p \,.$$

Um auch eine untere Schranke zu bekommen, beginnen wir wieder mit der expliziten Formel für den Wert von $I(g,z)$:

$$I(g,z) = e^z \sum_{j=0}^{m} g^{(j)}(0) - \sum_{j=0}^{m} g^{(j)}(z) \,.$$

Summation über alle Nullstellen von $f$ führt auf

$$\begin{aligned} J_p &= \sum_{f(z)=0} I(g,z) = \left( \sum_{f(z)=0} e^z \right) \sum_{j=0}^{m} g^{(j)}(0) - \sum_{f(z)=0} \sum_{j=0}^{m} g^{(j)}(z) \\ &= N \sum_{j=0}^{m} g^{(j)}(0) - \sum_{j=0}^{m} \sum_{f(z)=0} g^{(j)}(z) \,, \end{aligned}$$

wobei $N$ nach unserer Annahme eine von Null verschiedene ganze Zahl ist. Da Null eine $(p-1)$-fache Nullstelle von $g$ ist, verschwindet $g^{(j)}(0)$ für $j < p-1$. Für $j = p-1$ wenden wir wieder die verallgemeinerte LEIBNIZ-Regel

$$(uv)^{(r)} = \sum_{k=0}^{r} \binom{r}{k} u^{(k)} v^{(r-k)}$$

an; hier für $u = X^{p-1}, v = f^p$ und $uv = g$. Da $u^{(j)}(0)$ für $j < p-1$ verschwindet und $u^{(p-1)}(0) = (p-1)!$ ist, folgt

$$g^{(p-1)}(0) = (p-1)! f(0)^p \,.$$

Für $j \geq p$ schließlich wissen wir, daß $g^{(j)}(0)$ durch $j!$ teilbar ist, also insbesondere durch $p!$. Es gibt daher eine ganze Zahl $A_p$, so daß gilt

$$\sum_{j=0}^{m} g^{(j)}(0) = (p-1)! f(0)^p + p! A_p \,.$$

Zur Untersuchung der Doppelsumme im Ausdruck für $J_p$ beachten wir, daß jede Nullstelle $z$ von $f$ eine $p$-fache Nullstelle von $g$ ist. Daher verschwindet $g^{(j)}(z)$ für $j < p$. Für $j \geq p$ sind alle Koeffizienten von $g^{(j)}$ durch $j!$ teilbar, also insbesondere durch $p!$. Es gibt daher Polynome $g_j \in \mathbb{Z}[X]$, so daß $g^{(j)} = p!g_j$ ist. Wie $g^{(j)}$ hat auch $g_j$ dem Grad $m-j$. Nach dem vorigen Lemma ist daher $a_d^{m-j} \sum_{f(z)=0} g_j(z)$ eine ganze Zahl, und

$$a_d^{m-j} \sum_{f(z)=0} g^{(j)}(z) = a_d^{m-j} p! \sum_{f(z)=0} g_j(z)$$

ist eine durch $p!$ teilbare ganze Zahl. Für $j \geq p$ ist $a_d^{m-j}$ ein Teiler von $a_d^{m-p}$; daher ist $a_d^{m-p} \sum_{f(z)=0} g^{(j)}(z)$ für alle $j \geq p$ eine durch $p!$ teilbare ganze Zahl. Es gibt somit eine ganze Zahl $B_p$ derart, daß

$$-a_d^{m-p} \sum_{j=0}^{m} \sum_{f(z)=0} g^{(j)}(z) = -a_d^{m-p} \sum_{j=p}^{m} \sum_{f(z)=0} g^{(j)}(z) = p!B_p$$

ist. Insgesamt erhalten wir so die Formel

$$\begin{aligned} J_p &= N\big((p-1)!f(0)^p + p!A_p\big) + p!\frac{B_p}{a_d^{m-p}} \\ &= N(p-1)!f(0)^p + p!\left(NA_p + \frac{B_p}{a_d^{m-p}}\right) . \end{aligned}$$

Multiplikation mit $a_d^{m-p}$ und Division durch $(p-1)!$ führt auf

$$\frac{a_d^{m-p}}{(p-1)!} J_p = N a_d^{m-p} f(0) + p(N a_d^{m-p} A_p + B_p) ,$$

und das ist eine ganze Zahl. Der Grad $m$ von $g$ ist $(d+1)p-1$, also ist $m-p = dp-1$

Nach unseren Annahmen sind $N, a_d$ und $f(0)$ allesamt von Null verschieden; es gibt daher höchstens endlich viele Primzahlen, die eine dieser drei Zahlen teilen. Für jede andere Primzahl $p$ ist diese ganze Zahl nicht durch $p$ teilbar und damit insbesondere von Null verschieden. Sie hat daher mindestens den Betrag eins, was auf die Abschätzung

$$\big|J_p\big| \geq \frac{(p-1)!}{a_d^{m-p}} = \frac{(p-1)!}{a_d^{dp-1}}$$

führt, denn der Grad $m$ von $g$ ist $(p+1)d-1$. Wie wir bereits gezeigt haben, ist andererseits $\left|J_p\right| \leq M^p$ für eine geeignete Konstante $M$; daher ist

$$\frac{(p-1)!}{a_d^{dp-1}} \leq M^p \quad \text{und} \quad (p-1)! \leq \frac{(a_d M)^p}{a_d}$$

für jede hinreichend große Primzahl $p$. Da $(p-1)!$ schneller wächst als jede $p$-te Potenz, führt das auf den gesuchten Widerspruch. ∎

Nach diesen Vorbereitungen folgt nun recht schnell der Satz von LINDEMANN:

**Satz:** $\pi$ ist transzendent.

*Beweis:* Wäre $\pi$ algebraisch, so wäre auch $\pi i$ algebraisch; es gäbe also ein irreduzibles Polynom $f \in \mathbb{Z}[X]$, das $\pi i$ als Nullstelle hätte. Sein Grad sei $d$, und die (komplexen) Nullstellen von $f$ seien $z_1, \ldots, z_d$. Da $\pi i$ zu diesen Nullstellen gehört, ist

$$\prod_{f(z)=0} (1+e^z) = \prod_{j=1}^{d} (1+e^{z_j}) = 0\,.$$

Ausmultipliziert wird das zu

$$\sum_{\varepsilon \in \{0,1\}^d} e^{\sum_{j=1}^{d} \varepsilon_j z_j} = 0\,.$$

Die $2^d$ Summen $\sum \varepsilon_j z_j$ sind die Nullstellen des Polynoms

$$P_0 = \prod_{\varepsilon \in \{0,1\}^d} \left( X - \sum_{j=1}^{d} \varepsilon_j z_j \right)\,,$$

dessen Koeffizienten nach VIÈTE die elementarsymmetrischen Funktionen in diesen Summen sind.

Eine Permutation der Nullstellen $z_1, \ldots, z_d$ von $f$ permutiert auch die Nullstellen $\sum \varepsilon_j z_j$ von $P_0$; daher lassen sich die Koeffizienten von $P_0$ nach dem Hauptsatz über symmetrische Polynome als Polynome in den

elementarsymmetrischen Funktionen in den $z_j$ schreiben, also als Polynome in den Koeffizienten jenes normierten Polynoms, das die $z_j$ als Nullstellen hat. Da $f$ nicht als normiert vorausgesetzt war, sind dies nicht die Koeffizienten von $f$, sondern die von $f/a_d$, wobei $a_d$ den führenden Koeffizienten von $f$ bezeichnet. Die Koeffizienten von $P_0$ sind somit rationale Funktionen der Koeffizienten von $f$, und da letztere ganzzahlig sind, folgt, daß alle Koeffizienten von $P_0$ in $\mathbb{Q}$ liegen. Multiplizieren wir $P_0$ mit deren Hauptnenner und dividieren wir durch die größtmögliche $X$-Potenz $X^q$, erhalten wir ein Polynom $P \in \mathbb{Z}[X]$ mit $P(0) \neq 0$, das alle nichtverschwindenden Summen $\sum \varepsilon_j z_j$ als Nullstellen hat.

Nun ist einerseits

$$\sum_{\varepsilon \in \{0,1\}^d} e^{\sum_{j=1}^d \varepsilon_j z_j} = \prod_{f(z)=0} (1 + e^z) = 0 \,,$$

andererseits ist

$$\sum_{\varepsilon \in \{0,1\}^d} e^{\sum_{j=1}^d \varepsilon_j z_j} = \sum_{P_0(z)=0} e^z = qe^0 + \sum_{P(z)=0} e^z = q + \sum_{P(z)=0} e^z \,.$$

Wenn alle $\varepsilon_j$ verschwinden, ist die Summe der $\varepsilon_j z_j$ gleich Null; daher ist $q \geq 1$. Zusammen mit den beiden letzten Formelzeilen folgt

$$\sum_{P(z)=0} e^z = -q \in \mathbb{Z} \setminus \{0\} \,,$$

was nach dem vorigen Lemma unmöglich ist. Die Annahme, $\pi$ sei algebraisch, führt daher zu einem Widerspruch, d.h. $\pi$ ist transzendent. ∎

## §6: Endliche Körper

Da jeder Körper der Charakteristik Null den Körper der rationalen Zahlen enthält, haben endliche Körper $k$ notwendigerweise positive Charakteristik. Ist $\operatorname{char} k = p$, so enthält $k$ einen zu $\mathbb{F}_p$ isomorphen Teilkörper, das Bild des kononischen Homomorphismus $\mathbb{Z} \to k$, und ist somit isomorph zu einem $\mathbb{F}_p$-Vektorraum. Die Elementanzahl eines endlichen Körpers ist somit stets eine Primzahlpotenz.

Wie wir in §2 gesehen haben, ist die Abbildung

$$F\colon \begin{cases} k \to k \\ x \mapsto x^p \end{cases}$$

für jeden Körper der Charakteristik $p$ ein Homomorphismus, der sogenannte FROBENIUS-Homomorphismus. Wenn wir ihn $r$ mal hintereinander ausführen, erhalten wir die Abbildung, die jedes Element $x \in k$ auf $x^{p^r}$ abbildet; auch sie ist natürlich ein Homomorphismus, den wir mit $F^r$ bezeichnen.

Ein Homomorphismus eines Körpers in einen Körper ist stets injektiv. Das gilt natürlich auch für die Homomorphismen $F^r\colon k \to k$. Im Falle eines endlichen Körpers $k$ folgt aus der Injektivität die Surjektivität, in diesem Fall ist $F^r$ also ein Automorphismus von $k$. Für die Körper $\mathbb{F}_p$ können wir den kleinen Satz von FERMAT auch so formulieren, daß $F$ (und damit auch jedes $F^r$) die identische Abbildung ist.

Aus §3 des vorigen Kapitels wissen wir, daß die multiplikative Gruppe eines endlichen Körpers stets zyklisch ist. In einem Körper $k$ mit $p^n$ Elementen hat sie die Ordnung $p^n - 1$, so daß es ein Element $x$ der Ordnung $p^n - 1$ geben muß. Dieses ist natürlich, genau wie alle seine Potenzen, eine Nullstelle des Polynoms $X^{p^n-1} - 1$; da dessen Grad gleich der Elementanzahl der multiplikativen Gruppe von $k$ ist, besteht diese somit genau aus den Nullstellen dieses Polynoms. Insbesondere ist $k$ ein Zerfällungskörper von $X^{p^n-1} - 1$, und da alle Zerfällungskörper eines festen Polynoms zueinander isomorph sind, sind auch alle Körper mit $p^n$ Elementen zueinander isomorph.

Da das Polynom $X^{p^n-1} - 1$ alle Elemente außer der Null als Nullstellen hat, hat $X^{p^n} - X$ *alle* Elemente eines Körpers mit $p^n$ Elementen als Nullstelle; somit ist die $n$-te Potenz $F^n$ des FROBENIUS-Automorphismus gleich der Identität auf $k$.

Mit dieser Bemerkung können wir auch leicht einsehen, daß es zu jeder Primzahlpotenz $p^n$ einen Körper mit $p^n$ Elementen gibt: Wir bilden zunächst über $\mathbb{F}_p$ den Zerfällungskörper des Polynoms $X^{p^n-1} - 1$; er enthält alle Nullstellen dieses Polynoms und natürlich auch die Null. Diese Elemente bilden zusammen einen Teilkörper, nämlich den

Fixkörper von $F^n$. Da der Zerfällungskörper der kleinste Körper ist, der alle Nullstellen enthält, ist er gleich dieser Menge aus $p^n$ Elementen.

Zusammenfassend können wir festhalten

**Satz:** Für jede Primzahlpotenz $p^n$ gibt es Körper mit $p^n$ Elementen; sie sind alle zueinander isomorph. Für jedes Element $x$ eines solchen Körpers ist $x^{p^n} = x$, die $n$-te Potenz des FROBENIUS-Automorphismus ist also die Identität. ∎

Wir bezeichnen „den“ Körper mit $p^n$ Elementen mit $\mathbb{F}_{p^n}$.

Falls der Körper $\mathbb{F}_{p^n}$ einen der Körper $\mathbb{F}_{p^m}$ enthält, ist er ein $\mathbb{F}_{p^m}$-Vektorraum; daher ist $p^n$ eine Potenz von $p^m$, d.h. $m$ muß ein Teiler von $n$ sein. Ist umgekehrt $m$ ein Teiler von $n$, so folgt aus $x^m = 1$, daß auch $x^n = 1$ ist, d.h. jede Nullstelle von $X^m - 1$ (im Zerfällungskörper $\mathbb{F}_{p^m}$) ist auch eine Nullstelle von $X^n - 1$, so daß $X^m - 1$ ein Teiler von $X^n - 1$ ist und der Zerfällungskörper von $X^n - 1$ einen Zerfällungskörper von $X^m - 1$ enthält, d.h. $\mathbb{F}_{p^m}$ ist in $\mathbb{F}_{p^n}$ enthalten.

$\mathbb{F}_{p^m}$ ist der Fixkörper unter $F^m$; daher ist die Erweiterung $\mathbb{F}_{p^n}/\mathbb{F}_{p^m}$ GALOISsch. Die GALOIS-Gruppe wird erzeugt von $F^m$; da $F^n$ die Identität auf $\mathbb{F}_{p^n}$ ist, ist diese eine zyklische Gruppe mit $n/m$ Elementen.

Zum expliziten Rechnen in einem Körper $\mathbb{F}_{p^n}$ muß dieser zunächst irgendwie konkret als Vektorraum über $\mathbb{F}_p$ dargestellt werden; in $\mathbb{F}_p$ können wir schließlich rechnen. Wir wissen, daß $\mathbb{F}_{p^n}$ aus $\mathbb{F}_p$ entsteht durch Adjunktion eines erzeugenden Elements $x$ der Gruppe $\mathbb{F}_{p^n}^\times$; da die Körpererweiterung den Grad $n$ hat, ist $x$ Nullstelle eines irreduziblen Polynoms vom Grad $n$ über $\mathbb{F}_p$. Ist umgekehrt $f$ ein irreduzibles Polynom vom Grad $n$, so ist $\mathbb{F}_p[X]/(f)$ über $\mathbb{F}_p$ eine Körpererweiterung vom Grad $n$, hat also $p^n$ Elemente und ist somit isomorph zu $\mathbb{F}_{p^n}$.

Wenn wir also ein irreduzibles Polynom $f \in \mathbb{F}_p[X]$ vom Grad $n$ gefunden haben, können wir $\mathbb{F}_{p^n}$ identifizieren mit $\mathbb{F}_p[X]/(f)$, und dort können wir die Elemente identifizieren mit den Polynomen aus $\mathbb{F}_p[X]$ vom Grad kleiner $n$. Die Addition und Subtraktion sind problemlos, bei der Multiplikation erhalten wir im allgemeinen allerdings ein Polynom

vom Grad $n$ oder größer. Dieses muß dann ersetzt werden durch seinen Rest bei der Division durch $f$. Multiplikative Inverse schließlich lassen sich mit Hilfe des erweiterten EUKLIDischen Algorithmus bestimmen: Ist das Element $x \neq 0$ aus $\mathbb{F}_{p^n}$ gegeben durch das Polynom $g \in \mathbb{F}_p[X]$ vom Grad kleiner $n$, so sind $f$ und $g$ teilerfremd, da $g \neq 0$ und $f$ irreduzibel ist. Daher gibt es Polynome $g^*, f^*$ mit $\deg g^* < \deg f = n$ und $\deg f^* < \deg g$, so daß $gg^* + ff^* = 1$ ist. Modulo $f$ ist somit $gg^* = 1$.

Die Computeralgebra kennt, insbesondere für Polynome aus $\mathbb{F}_p[X]$, effiziente Faktorisierungsverfahren; man kann sich daher irreduzible Polynome vom Grad $n$ über $\mathbb{F}_p$ verschaffen, indem man das Polynom $X^{p^n-1} - 1 \in \mathbb{F}_p[X]$ in seine irreduziblen Faktoren zerlegt und einen der Faktoren vom Grad $n$ auswählt. Wegen der Existenz des Körpers $\mathbb{F}_{p^n}$ muß es mindestens einen solchen Faktor geben, oft gibt es aber mehrere, die aber alle zu zueinander isomorphen Körpern führen.

Im Falle des Körpers $\mathbb{F}_{256}$, der sowohl für den *Advanced Encryption Standard* AES als auch für die Fehlerkorrektur auf CDs und DVDs verwendet wird, lassen sich die Faktoren von $X^{255} - 1$ über $\mathbb{F}_2$ per Computer leicht bestimmen. Wie sich zeigt, haben dreißig davon den Grad acht, den wir für einen Körper mit $256 = 2^8$ Elementen brauchen. Zweckmäßigerweise sollten wir einen wählen, der das Rechnen modulo diesem Polynom möglichst einfach macht; insbesondere sollte das verwendete Polynom möglichst wenige Terme habe.

Dreizehn der dreißig Polynome haben sieben nichtverschwindende Terme, die restlichen siebzehn nur fünf. Wir wählen natürlich eines der letzteren. Alle diese Polynome haben, wie jedes Polynom vom Grad acht über $\mathbb{F}_2$, den führenden Term $X^8$; danach folgen vier weitere Terme. Bei der Reduktion modulo einem solchen Polynom $P = X^8 + \mathit{Rest}$ benutzt man, daß dann

$$X^8 \equiv \mathit{Rest}, \qquad X^9 \equiv X \cdot \mathit{Rest}, \quad \ldots$$

ist; dies wird umso häufiger mehrfach angewandt werden müssen, je höheren Grad das Polynom *Rest* hat. Am effizientesten kann man also rechnen, wenn das Polynom *Rest* den kleinstmöglichen Grad hat. Bei unseren siebzehn Kandidaten ist dies der Grad vier; er kommt zweimal

vor, nämlich bei

$$X^8 + X^4 + X^3 + X + 1 \quad \text{und} \quad X^8 + X^4 + X^3 + X^2 + 1\,.$$

Das erste dieser Polynome wird für AES verwendet, das zweite bei der Fehlerkorrektur auf CDs.

Die genaue Festlegung für das Rechnen in $\mathbb{F}_{256} = \mathbb{F}_2^8$ für die Zwecke von AES ist folgende: Wir schreiben ein Byte als $(a_7, a_6, \ldots, a_0)$ und identifizieren es mit dem Polynom

$$a_7X^7 + a_6X^6 + \cdots + a_1X + a_0\,;$$

das Byte 0000 0010 entspricht also $X$.

Der Einfachheit halber schreiben wir Bytes meist als zweiziffrige Hexadezimalzahlen: Im betrachteten Beispiel wäre das $02_{\text{hex}}$, und das Byte $\text{A5}_{\text{hex}} = 1010\,0101$ entspricht dem Polynom $X^7 + X^5 + X^2 + 1$.

Man beachte, daß trotz dieser Schreibweise die Addition und Multiplikation in $\mathbb{F}_{256}$ natürlich nichts mit der Addition und Multiplikation von Hexadezimalzahlen zu tun haben. Zwar ist $01_{\text{hex}} + 02_{\text{hex}} = 03_{\text{hex}}$, aber $01_{\text{hex}} + 01_{\text{hex}} = 00_{\text{hex}}$ und $05_{\text{hex}} + 04_{\text{hex}} = 01_{\text{hex}}$.

Zur Berechnung von $\text{A5}_{\text{hex}} \cdot 01_{\text{hex}}$ müssen wir das Polynom

$$(X^7 + X^5 + X^2 + 1) \cdot X = X^8 + X^6 + X^3 + X$$

berechnen und modulo $m(X) = X^8 + X^4 + X^3 + X + 1$ reduzieren. Da

$$X^8 \bmod m(X) = X^4 + X^3 + X^2 + 1$$

ist (in $\mathbb{F}_2$ ist $-1 = 1$), ist dies

$$(X^4 + X^3 + X^2 + 1) + (X^6 + X^3 + X) = X^6 + X^4 + X^2 + X + 1\,.$$

Somit ist $\text{A5}_{\text{hex}} \cdot 01_{\text{hex}} = 56_{\text{hex}}$.

Trotz der Wahl des optimalen Polynoms ist die Multiplikation also immer noch erheblich aufwendiger als die Addition.

## §7: Mehr über Einheitswurzeln

Die $n$-ten Einheitswurzeln spielen eine wesentliche Rolle bei der Konstruktion des regelmäßigen $n$-Ecks mit Zirkel und Lineal, und wir wir gerade gesehen haben, sind auch alle Elemente außer der Null im Körper mit $p^n$ Elementen $(p^n - 1)$-te Einheitswurzeln. Es liegt daher nahe, Einheitswurzeln etwas genauer zu betrachten.

**Definition:** Für einen Körper $k$ bezeichnen wir

$$\mu_n(k) = \left\{ x \in k \;\middle|\; x^n = 1 \right\}$$

als die Gruppe der $n$-ten Einheitswurzeln von $k$. Der Zerfällungskörper des Polynoms $X^n - 1$ über $k$ heißt der $n$-te *Kreisteilungskörper* über $k$ und wird mit $k_n$ bezeichnet.

$\mu_n(k)$ ist in der Tat eine Gruppe, denn natürlich enthält sie die Eins, und ist $x^n = y^n = 1$, so ist auch $(xy)^n = x^n y^n = 1$. Auch das inverse Element $x^{-1}$ liegt in $\mu_n(k)$, denn $\left(x^{-1}\right)^n = x^{-n} = \left(x^n\right)^{-1} = 1$.

Für $k = \mathbb{Q}$ und $k = \mathbb{R}$ beispielsweise haben wir

$$\mu_n(\mathbb{Q}) = \mu_n(\mathbb{R}) = \begin{cases} \{1\} & \text{für ungerade } n \\ \{1, -1\} & \text{für gerade } n \end{cases} .$$

Deutlich größer ist

$$\mu_n(\mathbb{C}) = \left\{ e^{2\pi i j/n} \;\middle|\; j = 0, \ldots, n-1 \right\} .$$

Für endliche Körper ist $\mu_{p-1}(\mathbb{F}_p) = \mathbb{F}_p^\times$ nach dem kleinen Satz von FERMAT. Da die multiplikative Gruppe eines endlichen Körpers zyklisch ist, gilt allgemeiner auch $\mu_{p^n-1}(\mathbb{F}_{p^n}) = \mathbb{F}_{p^n}^\times$, aber $\mu_{p^m}(\mathbb{F}_{p^n}) = \{1\}$ für alle $m$, denn $x^{p^n} = x$ für alle $x$, so daß für $x \neq 1$ auch $x^{p^m}$ nicht gleich eins sein kann.

**Lemma:** Falls die Charakteristik von $k$ kein Teiler von $n$ ist, ist $\mu_n(k_n)$ eine Gruppe der Ordnung $n$. Ist $n = p^r m$ mit einer zu $p = \operatorname{char} k$ teilerfremden Zahl $m$, so ist $\mu_n(k_n) = \mu_m(k_n)$ eine Gruppe der Ordnung $m$.

*Beweis:* Falls $n$ kein Vielfaches der Charakteristik ist, ist die Ableitung $nX^{n-1}$ des Polynoms $X^n - 1$ nicht das Nullpolynom. Da $nX^{n-1}$ nur für $x = 0$ verschwindet, $X^n - 1$ dort aber den Wert $-1$ annimmt, gibt es keine gemeinsame Nullstelle des Polynoms mit seiner Ableitung, so daß alle Nullstellen von $X^n - 1$ einfach sind. Da $k_n$ der Zerfällungskörper dieses Polynoms ist, hat es dort also $n$ verschiedene Nullstellen.

Ist $n = p^r m$ und $\operatorname{char} k = p$, so ist $(X^m - 1)^{p^r} = X^{mp^r} - 1^{p^m} = X^n - 1$, und $X^m - 1$ hat, da $p$ kein Teiler von $m$ ist, $m$ verschiedene Nullstellen. Jede dieser Nullstellen ist eine $p^r$-fache Nullstelle von $X^n - 1$. ∎

Als nächstes wollen wir uns überlegen, daß $\mu_n(k)$ stets eine zyklische Gruppe ist. Wir betrachten zunächst Körper $k$ der Charakteristik Null. Da diese $\mathbb{Q}$ als Teilkörper enthalten, ist auch $\mathbb{Q}_n$ ein Teilkörper von $k_n$. Da sowohl $\mu(\mathbb{Q}_n)$ als auch $\mu(k_n)$ die Ordnung $n$ hat, ist $\mu_n(k_n) = \mu_n(\mathbb{Q}_n)$. Somit ist $\mu_n(k_n)$ genau dann zyklisch, wenn $\mu_n(\mathbb{Q}_n)$ zyklisch ist. Da $\mathbb{C}$ algebraisch abgeschlossen ist und $\mathbb{Q}_n$ enthält, ist auch $\mu_n(\mathbb{Q}_n) = \mu_n(\mathbb{C})$, und letzteres ist eine zyklische Gruppe, die von $e^{2\pi i/n}$ erzeugt wird. Somit ist $\mu_n(k_n)$ in Charakteristik Null stets zyklisch. $\mu_n(k)$ als Untergruppe davon ist ebenfalls zyklisch nach dem folgenden

**Lemma:** Jede Untergruppe einer zyklischen Gruppe ist zyklisch.

*Beweis:* Die zyklische Gruppe $G$ sei erzeugt vom Element $g \in G$, und $U$ sei eine Untergruppe. Falls $U$ nur aus dem Neutralelement besteht, ist $U$ zyklisch. Andernfalls enthält $U$ Potenzen $g^n$ mit $n > 0$; der kleinste vorkommende positive Exponent sei $s$. Für jedes Element $g^m$ von $U$ können wir $m$ mit Rest durch $s$ dividieren und erhalten eine Gleichung $m = qs + r$ mit $0 \leq r < s$. Mit $g^m$ und $g^{qs} = \left(g^s\right)^q$ liegt auch $g^r = g^m g^{-qs}$ in $U$; wegen der Minimalität von $s$ muß daher $r = 0$ sein. Somit ist $g^m$ eine Potenz von $g^s$, d.h. $g^s$ erzeugt die Untergruppe $U$. ∎

Ist $\operatorname{char} k = p > 0$, so enthält $k$ den Körper $\mathbb{F}_p$ als Teilkörper und $k_n$ damit den Körper $\left(\mathbb{F}_p\right)_n$. Dieser ist ein endlicher Körper, und wie wir aus Kapitel 3, §3, wissen, ist die multiplikative Gruppe eines endlichen Körpers stets zyklisch. Damit ist auch $\mu_n\left(\left(\mathbb{F}_p\right)_n\right)$ als Untergruppe dieser multiplikativen Gruppe zyklisch, und da $\mu_n(k_n)$ nach dem Lemma die gleiche Ordnung wie $\mu_n\left(\left(\mathbb{F}_p\right)_n\right)$ hat, ist auch $\mu_n(k_n)$ zyklisch. $\mu_n(k)$ schließlich ist zyklisch als Untergruppe davon.

**Definition:** Eine $n$-te Einheitswurzel $\zeta \in \mu_n(k)$ heißt *primitive $n$-te Einheitswurzel,* wenn es keine natürliche Zahl $d < n$ gibt, für die bereits $\zeta^d = 1$ ist. Die Menge der primitiven $n$-ten Einheitswurzeln wird mit $\mu_n^*(k)$ bezeichnet. Falls $\mu_n^*(k_n)$ nicht leer ist, bezeichnen wir

$$\Phi_n = \prod_{\zeta \in \mu_n^*(k_n)} (X - \zeta)$$

als das $n$-te *Kreisteilungspolynom* über $k$.

Beispielsweise ist also $\mu_4(\mathbb{R}) = \emptyset$, aber $\mu_4^*(\mathbb{C}) = \{i, -i\}$. Da $\mathbb{C}$ der Zerfällungskörper von $X^4 - 1$ über $\mathbb{R}$ ist, ist $(X + i)(X - i) = X^2 + 1$ das vierte Kreisteilungspolynom sowohl über $\mathbb{R}$ als auch über $\mathbb{C}$.

Zumindest für $k = \mathbb{Q}$ sind wir dem $n$-ten Kreisteilungspolynom in einem anderen Zusammenhang bereits begegnet: Für den Satz von GAUSS, wonach das regelmäßige $n$-Eck genau dann mit Zirkel und Lineal konstruiert werden kann, wenn $\varphi(n)$ eine Zweierpotenz ist, betrachteten wir einen irreduziblen Faktor des Polynoms $X^n - 1$, der eine primitive $n$-te Einheitswurzel als Nullstelle hat, und zeigten dann mit einem Argument von DEDEKIND, daß dieser Faktor genau die primitiven $n$-ten Einheitswurzeln als Nullstellen hat. Somit ist dieser Faktor, wenn wir ihn auf führenden Koeffizienten eins normieren, gerade das $n$-te Kreisteilungspolynom $\Phi_n$. Insbesonder folgt:

**Satz:** Das $n$-te Kreisteilungspolynom $\Phi_n$ über $\mathbb{Q}$ ist irreduzibel. ∎

Sobald wir eine primitive $n$-te Einheitswurzel kennen, können wir leicht auch alle anderen bestimmen nach dem folgenden

**Lemma:** Ist $G$ eine zyklische Gruppe der Ordnung $n$ und ist $g$ ein Erzeugendes von $G$, so ist $g^r$ genau dann ebenfalls ein Erzeugendes, wenn $r$ teilerfremd zu $n$ ist. Ist also $\zeta$ eine primitive $n$-te Einheitswurzel, so besteht $\mu_n^*(k)$ genau aus den Elementen $\zeta^r$ mit $0 \leq r < n$ und $\mathrm{ggT}(n, r) = 1$.

*Beweis:* Ist $r$ teilerfremd zu $n$, liefert uns der erweiterte EUKLIDische Algorithmus ganze Zahlen $\alpha, \beta$, für die $\alpha r + \beta n = 1$ ist. Damit ist

$$g = g^{\alpha r + \beta n} = \left(g^r\right)^{\alpha} \left(g^n\right)^{\beta} = \left(g^r\right)^{\alpha}$$

eine Potenz von $g^r$, so daß sich jede Potenz von $g$ auch als eine Potenz von $g^r$ schreiben läßt. Ist dagegen $d$ ein positiver gemeinsamer Teiler von $r$ und $n$, so ist $\alpha r \bmod n$ für jedes $\alpha \in \mathbb{Z}$ durch $d$ teilbar, so daß das Erzeugnis von $g^r$ keine Potenzen $g^e$ enthalten kann, für die $e$ kein Vielfaches von $d$ ist; insbesondere ist $g$ keine Potenz von $g^r$. ∎

**Korollar:** Falls char $k$ kein Teiler von $n$ ist, enthält $\mu_n^*(k_n)$ genau $\varphi(n)$ Elemente.

*Beweis:* Nach Kapitel 2 haben genau die zu $n$ teilerfremden Elemente von $\mathbb{Z}/n$ ein multiplikatives Inverses, und die EULERsche $\varphi$-Funktion gibt die Elementanzahl der primen Restklassengruppe $\left(\mathbb{Z}/n\right)^\times$ an. ∎

**Lemma:** Ist char $k = 0$, so ist $\Phi_n$ ein Polynom mit ganzzahligen Koeffizienten vom Grad $\varphi(n)$.

*Beweis* durch Induktion nach $n$.

Für $n = 1$ hat $\Phi_1 = X - 1$ offensichtlich ganzzahlige Koeffizienten.

Nun sei $n > 1$; wir nehmen an, daß $\Phi_d$ für $d < n$ in $\mathbb{Z}[X]$ liegt. Ist $\zeta \in \mu_n(k_n)$ keine primitive $n$-te Einheitswurzel, so gibt es einen echten Teiler $d$ von $n$ derart, daß $\zeta$ eine primitive $d$-te Einheitswurzel ist. Deshalb ist

$$X^n - 1 = \prod_{d|n} \Phi_d \,.$$

Nach Induktionsvoraussetzung sind die $\Phi_d$ mit $d < n$ Polynome mit ganzzahligen Koeffizienten; daher liegt auch

$$\Psi_n = \prod_{\substack{d|n \\ d<n}} \Phi_d$$

in $\mathbb{Z}[X]$. In $\mathbb{Q}[X]$ haben wir eine Polynomdivision mit Rest; dort dividieren wir $X^n - 1$ durch $\Psi_n$. Der Quotient sei $Q$, und der Rest $R$ ist entweder das Nullpolynom oder ein Polynom, dessen Grad kleiner als der von $\Psi_n$ ist. Da der führende Koeffizient eines Kreisteilungspolynoms nach Konstruktion stets eins ist, hat auch $\Psi_n$ den führenden Koeffizienten eins, so daß bei der Polynomdivision keine Nenner entstehen. Daher liegen sowohl $Q$ als auch $R$ in $\mathbb{Z}[X]$, und sie sind die einzigen Polynome aus $\mathbb{Q}[X]$ mit $\deg R < \deg \Psi_n$, für die $X^n - 1 = Q\Psi_n + R$ ist. In $\mathbb{Q}[X]$ ist aber auch $X^n - 1 = \Phi_n \Psi_n$, also muß $R = 0$ sein und $\Phi_n = Q$ liegt in $\mathbb{Z}[X]$. ∎

Da $\Phi_d$ den Grad $\varphi(d)$ hat, folgt aus der Formel $X^n - 1 = \prod_{d|n} \Phi_d$ durch Gradvergleich, daß

$$n = \sum_{d|n} \varphi(d)$$

sein muß, beispielsweise ist also

$$6 = \varphi(6) + \varphi(3) + \varphi(2) + \varphi(1) = 2 + 2 + 1 + 1 \, .$$

Die Formel erlaubt auch die rekursive Berechnung der Polynome $\Phi_n$:

$$\Phi_1 = X - 1$$

$$\Phi_2 = \frac{X^2 - 1}{\Phi_1} = \frac{X^2 - 1}{X - 1} = X + 1$$

$$\Phi_3 = \frac{X^3 - 1}{\Phi_1} = \frac{X^3 - 1}{X - 1} = X^2 + X + 1$$

$$\Phi_4 = \frac{X^4 - 1}{\Phi_1\Phi_2} = \frac{X^4 - 1}{(X - 1)(X + 1)} = X^2 + 1$$

$$\Phi_5 = \frac{X^5 - 1}{\Phi_1} = \frac{X^5 - 1}{X - 1} = X^4 + X^3 + X^2 + X + 1$$

$$\Phi_6 = \frac{X^6 - 1}{\Phi_1\Phi_2\Phi_3} = \frac{X^6 - 1}{(X - 1)(X + 1)(X^2 + X + 1)} = X^2 - X + 1$$

$$\Phi_7 = \frac{X^7 - 1}{\Phi_1} = \frac{X^7 - 1}{X - 1} = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$$

$$\Phi_8 = \frac{X^8 - 1}{\Phi_1\Phi_2\Phi_4} = \frac{X^8 - 1}{(X - 1)(X + 1)(X^2 + 1)} = X^4 + 1 \, ,$$

und so weiter. Nach dem obigen Satz sind sie allesamt irreduzibel in $\mathbb{Q}[X]$ und damit wegen ihrer Primitivität auch in $\mathbb{Z}[X]$. Wenn wir diese Polynome allerdings über einen Körper positiver Charakteristik betrachten, müssen sie dort nicht irreduzibel sei: Über $\mathbb{F}_3$ ist beispielsweise $(X + 2)^2 = X^2 + 4X + 1 = X^2 + X + 1$ eine Zerlegung von $\Phi_3$, und über $\mathbb{F}_7$ ist $\Phi_3 = (X + 3)(X + 5)$.

Auch über Erweiterungskörpern von $\mathbb{Q}$ müssen die Kreisteilungspolynome natürlich nicht irreduzibel sei; über $\mathbb{C}$ etwa zerfallen sie trivialer-

weise in ein Produkt von Linearfaktoren. Die Irreduzibilität von $\Phi_n$ über einem Körper $k$ hängt eng mit der GALOIS-Gruppe von $k_n/k$ zusammen:

**Lemma:** Falls $n$ kein Vielfaches von $\operatorname{char} k$ ist, ist $k_n/k$ eine GALOISsche Erweiterung von $k$, und ihre GALOIS-Gruppe ist isomorph zu einer Untergruppe von $\left(\mathbb{Z}/n\right)^\times$. Sie ist genau dann gleich $\left(\mathbb{Z}/n\right)^\times$, wenn $\Phi_n$ in $k[X]$ irreduzibel ist.

*Beweis:* Falls $n$ kein Vielfaches von $\operatorname{char} k$ ist, können wir wie im Fall $k = \mathbb{Q}$ argumentieren: Die Ableitung $nX^{n-1}$ von $X^n - 1$ ist dann nicht das Nullpolynom und hat keine gemeinsame Nullstelle mit $X^n - 1$; daher ist $X^n - 1$ separabel und $k_n/k$ als Zerfällungskörper eines separablen Polynoms GALOISsch. Für jede primitive $n$-te Einheitswurzel $\zeta$ ist $k_n = k(\zeta)$, und jeder Automorphismus von $k_n/k$ muß $\zeta$ wieder auf eine primitive $n$-te Einheitswurzel abbilden. Da sich diese als Potenz von $\zeta$ schreiben läßt mit einem zu $n$ teilerfremden Exponenten, muß $\operatorname{Aut}(k_n/k)$ eine Untergruppe von $\left(\mathbb{Z}/n\right)^\times$ sein. Genau dann, wenn $\Phi_n$ in $k[X]$ irreduzibel ist, ist $k_n \cong k[X]/(\Phi_n)$ und hat somit den Grad $\varphi(n)$ über $k$, so daß die GALOIS-Gruppe in diesem Fall $\varphi(n)$ Elemente hat und damit ganz $\left(\mathbb{Z}/n\right)^\times$ sein muß.

∎

Speziell für einen endlichen Körper $k = \mathbb{F}_q$ können wir die GALOIS-Gruppe explizit angeben:

**Lemma:** Ist $k = \mathbb{F}_q$ mit $q = p^r$, und ist $p$ kein Teiler von $n$, so ist $\operatorname{Aut}(k_n/k)$ isomorph zur von $q$ mod $n$ in $\left(\mathbb{Z}/n\right)^\times$ erzeugten zyklischen Untergruppe.

*Beweis:* Nach dem vorigen Lemma ist die Erweiterung GALOISsch. Die GALOIS-Gruppe einer endlichen Erweiterung von $\mathbb{F}_q$ ist zyklisch und wird erzeugt von der $r$-ten Potenz des FROBENIUS-Automorphismus $F$. Für jede primitive $n$-te Einheitswurzel $\zeta$ ist $k_n = \mathbb{F}_q(\zeta)$, und ist dies der Körper mit $p^s$ Elementen, so ist $F^s(\zeta) = \zeta^{p^s} = \zeta$ für jede primitive $n$-te Einheitswurzel $\zeta$. Also ist $\zeta^{p^s-1} = 1$, so daß $n$ ein Teiler von $p^s - 1$ sein muß. Ist $s = ar$, so ist $p^s - 1 = q^a - 1$, d.h. in $\left(\mathbb{Z}/n\right)^\times$ hat $q$ die Ordnung $a$. Da $\mathbb{F}_{p^s}$ als $\mathbb{F}_{p^r}$-Vektorraum die Dimension $a$ hat, ist

dies auch die Ordnung der GALOIS-Gruppe, die somit isomorph ist zur von $q$ mod $n$ erzeugten Untergruppe der primen Restklassengruppe. ∎

Um zu sehen, wie wir anhand der GALOIS-Gruppe die Zwischenkörper von $k_n/k$ explizit bestimmen können, brauchen wir zunächst ein allgemeines Lemma über GALOISsche Erweiterungen. Ziemlich am Anfang von §2 hatten wir für eine GALOISsche Erweiterung $K/k$ die Spur $S(x)$ eines Elements $x \in K$ definiert als die Summe aller Bilder von $x$ unter den Elementen der GALOIS-Gruppe. Jetzt definieren wir etwas allgemeiner

**Definition:** Für eine Untergruppe $H$ der GALOIS-Gruppe $G$ der Körpererweiterung $K/k$ setzen wir

$$S_H(x) \underset{\text{def}}{=} \sum_{\sigma \in H} \sigma(x) \, .$$

Für $H = G$ ist das gerade die Spur, und wie wir wissen, liegt $S(x)$ stets in $k$. Völlig analog können wir zeigen, daß $S_H(x)$ im Fixkörper $K^H$ liegen muß, denn für jedes Element $\tau \in H$ ist

$$\tau\big(S_H(x)\big) = \tau\left(\sum_{\sigma \in H} \sigma(x)\right) = \sum_{\sigma \in H} (\tau \circ \sigma)(x) = S_H(x) \, ,$$

da die Multiplikation mit $\tau$ eine bijektive Abbildung von $H$ nach $H$ ist. Offensichtlich ist $S_H \colon K \to K^H$ die Spurabbildung der GALOISschen Erweiterung $K/K^H$. Insbesondere ist daher, wie wir in §2 gleich nach der Definition der Spur gesehen haben, $S_H$ nicht die Nullabbildung; es gibt also Elemente $x \in K$, für die $S_H(x)$ nicht verschwindet. Außerdem ist $S_H$ eine $K^H$-lineare Abbildung, denn für $x \in K$ und $y \in K^H$ ist

$$S_H(xy) = \sum_{\sigma \in H} \sigma(xy) = \sum_{\sigma \in H} \sigma(x)\sigma(y) = \sum_{\sigma \in H} \sigma(x)y = yS_H(x) \, ,$$

und als Spurabbildung ist $S_H$ natürlich ein Homomorphismus bezüglich der Addition. Schließlich ist $S_H$ surjektiv, denn ist $x \in K$ ein Element mit $S_H(x) \neq 0$, so ist für jedes $y \in K^H$

$$S_H\left(\frac{y}{S_H(x)}x\right) = \frac{y}{S_H(x)} S_H(x) = y \, .$$

Daraus wiederum folgt

**Lemma:** $K/k$ sei eine GALOISsche Erweiterung mit GALOIS-Gruppe $G$, und $H$ sei eine Untergruppe von $G$. Weiter sei $\{x_1, \ldots, x_n\}$ ein Erzeugendensystem von $K$ als $k$-Vektorraum. Dann erzeugen die Elemente $S_H(x_i)$ den Fixkörper $K^H$ als $k$-Vektorraum.

*Beweis:* Wegen der Surjektivität von $S_H$ gibt es zu jedem $y \in K^H$ ein $x \in K$ mit $S_H(x) = y$. Als Element des $k$-Vektorraums $K$ läßt sich $x$ schreiben als $x = \sum_{i=1}^n c_i x_i$ mit $c_i \in k$. Als $K^H$-lineare Abbildung ist $S_H$ erst recht $k$-linear; somit ist

$$y = S_H(x) = S_H\left(\sum_{i=1}^n c_i x_i\right) = \sum_{i=1}^n c_i S_H(x_i)\,.$$

Damit läßt sich jedes Element von $K^H$ als $k$-Linearkombination der Elemente $S_H(x_i)$ darstellen, was die Behauptung beweist. ∎

Für die Körpererweiterung $k_n/k$ bilden die $n$-ten Einheitswurzeln ein solches Erzeugendensystem, aber für $n \neq 1$ natürlich keine Basis, denn es gibt ja $n$ verschiedene $n$-te Einheitswurzeln, aber der Grad von $k_n/k$ ist höchstens gleich $\varphi(n)$. In der Tat ist für jede $n$-te Einheitswurzel $\zeta \neq 1$ beispielsweise

$$1 + \zeta + \zeta^2 + \cdots + \zeta^{n-1} = 0\,,$$

denn multipliziert man diese Summe mit $\zeta$, so erhält man bis auf die Reihenfolge der Summanden die gleiche Summe, d.h. das Produkt dieser Summe mit $1 - \zeta$ ist Null. Im Falle $\zeta \neq 1$ folgt daraus, daß die Summe verschwinden muß. Weitere lineare Abhängigkeiten können sich etwa auch dadurch ergeben, daß außer der Eins noch weitere Einheitswurzeln bereits in $k$ liegen.

Die GALOIS-Gruppe von $k_n/k$ ist eine Untergruppe von $\left(\mathbb{Z}/n\right)^\times$. Ist etwa $k = \mathbb{Q}$ und $n = 5$, so ist $\mathbb{Z}/5 = \mathbb{F}_5$ ein Körper; die prime Restklassengruppe ist also zyklisch von der Ordnung vier. Sie wird erzeugt von der Zwei, denn $2^2 = 4$, $2^3 = 3$ und $2^4 = 1$. Die GALOIS-Gruppe ist wegen der Irreduzibilität von $\Phi_5$ über $\mathbb{Q}$ die gesamte Gruppe $\left(\mathbb{Z}/5\right)^\times$. Schreiben wir $k_5 = \mathbb{Q}(\zeta)$ mit einer primitiven fünften Einheitswurzel $\zeta$, entspricht das Element $j \in \left(\mathbb{Z}/5\right)^\times$ dem Automorphismus von $k_5/\mathbb{Q}$,

der $\zeta$ auf $\zeta^j$ abbildet. Die einzige echte Untergruppe $H$ der GALOIS-Gruppe hat die Ordnung zwei und wird erzeugt vom Quadrat dieses Automorphismus, also der Abbildung, die $\zeta$ auf $\zeta^4 = \zeta^{-1}$ abbildet. Sie bildet auch jede Potenz $\zeta^r$ ab auf $\zeta^{-r}$; der Zwischenkörper $L$ vom Grad zwei wird also erzeugt von den Elementen

$$S_H(\zeta^r) = \zeta^r + \zeta^{-r} \quad \text{für } r = 0, \ldots, 4 \,.$$

Man beachte, daß diese Zahlen allesamt reell sind, denn für jede komplexe Zahl $z$ vom Betrag eins ist $z\bar{z} = |z|^2 = 1$. Somit ist $z + z^{-1} = z + \bar{z} = 2\,\mathfrak{Re}\, z$. Tatsächlich erhalten wir nur drei verschiedene Werte, denn wegen $\zeta^5 = 1$ ist $S_H(\zeta^3) = S_H(\zeta^2)$ und $S_H(\zeta^4) = S_H(\zeta)$. Somit wird $L$ als $\mathbb{Q}$-Vektorraum erzeugt von den drei Zahlen $1, \zeta + \zeta^{-1}$ und $\zeta^2 + \zeta^{-2}$. Da $L/\mathbb{Q}$ nur den Grad zwei hat, können diese allerdings nicht linear unabhängig über $\mathbb{Q}$ sein, und in der Tat folgt aus dem Verschwinden von $1 + \zeta + \zeta^2 + \zeta^3 + \zeta^4$ nach Division durch $\zeta^2$, daß

$$\zeta^{-2} + \zeta^{-1} + 1 + \zeta + \zeta^2 = 1 + \left(\zeta + \zeta^{-1}\right) + \left(\zeta^2 + \zeta^{-2}\right) = 0$$

ist. Somit hat $L$ als $\mathbb{Q}$-Vektorraum beispielsweise die Basis bestehend aus der Eins und aus $\zeta + \zeta^{-1}$.

Da $L/\mathbb{Q}$ eine quadratische Körpererweiterung ist, muß $\zeta + \zeta^{-1}$ einer quadratischen Gleichung über $\mathbb{Q}$ genügen. $\left(\zeta + \zeta^{-1}\right)^2 = \zeta^2 + \zeta^{-2} + 2$, und wie wir gerade gesehen haben, ist $\left(\zeta^2 + \zeta^{-2}\right) + 1 = -\left(\zeta + \zeta^{-1}\right)$. Somit ist

$$(\zeta + \zeta^{-1})^2 + (\zeta + \zeta^{-1}) = 1 \,.$$

$\zeta + \zeta^{-1}$ ist also eine Nullstelle des Polynoms $X^2 + X - 1$, d.h. einer der beiden Werte $-\frac{1}{2} \pm \frac{1}{2}\sqrt{5}$, Für $\zeta = e^{2\pi i/5}$ haben $\zeta$ und $\zeta^{-1} = \bar{\zeta}$ positiven Realteil, so daß $\zeta + \zeta^{-1}$ gleich $\frac{1}{2}\left(\sqrt{5} - 1\right)$ sein muß; für $\zeta = e^{2\cdot 2\pi i/5}$ etwa wäre $\zeta + \zeta^{-1} = -\frac{1}{2}\left(\sqrt{5} + 1\right)$. In beiden Fällen ist $L = \mathbb{Q}\left(\zeta + \zeta^{-1}\right) = \mathbb{Q}\left(\sqrt{5}\right)$.

$k_5/L$ ist ebenfalls eine quadratische Erweiterung. Wenn wir von der Einheitswurzel $\zeta = e^{2\pi i/5}$ ausgehen, ist sie wegen $\zeta + \zeta^{-1} = \frac{1}{2}\left(\sqrt{5} - 1\right)$ gegeben durch die quadratische Gleichung $\zeta^2 - \frac{1}{2}\left(\sqrt{5} - 1\right)\zeta + 1 = 0$. Deren Lösungen sind

$$\frac{1 - \sqrt{5}}{4} \pm i\frac{\sqrt{2}\,\sqrt{5 + \sqrt{5}}}{4} \,,$$

wobei $\zeta$ die Lösung mit positivem Imaginärteil ist und $\zeta^{-1}$ die mit dem negativen. Der Körper $k_5$ entsteht also aus $L$ durch Adjunktion von $\sqrt{-2}\cdot\sqrt{5+\sqrt{5}}$.

Für $\zeta = e^{4\pi i/5}$ erhalten wir $\zeta$ und $\zeta^{-1}$ entsprechend als Lösungen der quadratischen Gleichung $\zeta^2 + \frac{1}{2}\big(\sqrt{5}+1\big)\zeta + 1 = 0$, also

$$\frac{1+\sqrt{5}}{4} \pm i\frac{\sqrt{2}\,\sqrt{5-\sqrt{5}}}{4}\,.$$

$k_5$ ist also auch gleich $L\Big(\sqrt{-2}\cdot\sqrt{5-\sqrt{5}}\Big)$.

Zusammenfassend können wir sagen, daß wir für alle primitiven fünften Einheitswurzeln sowohl den Realteil als auch den Imaginärteil explizit durch Wurzelausdrücke dargestellt haben. Da wir mit Quadratwurzeln ausgekommen sind, können wir an diesen Ausdrücken auch leicht eine Vorschrift zur Konstruktion des regelmäßigen Fünfecks ablesen.

Für $n = 7$ wird die Situation schon deutlich komplexer: Die GALOIS-Gruppe von $k_7/k = \mathbb{Q}$ ist wieder wegen der Irreduzibilität von $\Phi_7$ über $\mathbb{Q}$ die gesamte prime Restklassengruppe. $\big(\mathbb{Z}/7\big)^\times$ wird aber nicht von der Zwei erzeugt, denn $2^3 \equiv 1 \bmod 7$. Die Drei ist allerdings eine primitive Wurzel modulo sieben, denn in $\big(\mathbb{Z}/7\big)^\times$ ist $3^2 = 2$, $3^3 = 6$, $3^4 = 4$, $3^5 = 5$ und $3^6 = 1$. Die GALOIS-Gruppe wird somit erzeugt vom Automorphismus $\tau$, der jede siebte Einheitswurzel $\zeta$ auf $\zeta^3$ abbildet, und sie ist isomorph zur zyklischen Gruppe $\mathbb{Z}/6$. Damit gibt es genau zwei nichttriviale Untergruppen, eine der Ordnung drei und eine der Ordnung zwei.

Die Untergruppe $H$ der Ordnung drei wird erzeugt von $\tau^2$ und enthält auch $\tau^4$. Wegen $\tau^2(\zeta) = \zeta^9 = \zeta^2$ und $\tau^4(\zeta) = \tau^2\big(\tau^2(\zeta)\big) = \tau^2(\zeta^2) = \zeta^4$ ist $S_H(\zeta) = \zeta + \zeta^2 + \zeta^4$. Dieses Element liegt im Fixkörper $L = K^H$ von $H$, aber nicht in $\mathbb{Q}$, denn wäre es gleich einer rationalen Zahl $q$, so wäre $\zeta$ Nullstelle des Polynoms $X^4 + X^2 + X - q \in \mathbb{Q}[X]$, im Widerspruch zur Irreduzibilität von $\Phi_7$ über $\mathbb{Q}$. Daher bildet $\zeta + \zeta^2 + \zeta^4$ zusammen mit der Eins eine $\mathbb{Q}$-Basis von $L$ und muß Nullstelle eines quadratischen Polynoms aus $\mathbb{Q}[X]$ sein. Dieses Polynom hat auch $\tau\big(\zeta + \zeta^2 + \zeta^4\big)$ als

Lösung, ist also nach VIÈTE

$$\left(X-\zeta-\zeta^2-\zeta^4\right)\left(X-\zeta^3-\zeta^5-\zeta^6\right)=X^2-aX+b$$

mit $a=(\zeta+\zeta^2+\zeta^4)+(\zeta^3+\zeta^5+\zeta^6)=-1$ und

$$b=(\zeta+\zeta^2+\zeta^4)(\zeta^3+\zeta^5+\zeta^6)=\zeta^4+\zeta^6+1+\zeta^5+1+\zeta+1+\zeta^2+\zeta^3=2\,.$$

Somit ist $\zeta+\zeta^2+\zeta^4$ eine Nullstelle des Polynoms $X^2+X+2$, also eine der beiden Zahlen $-\frac{1}{2}\pm\frac{1}{2}\sqrt{-7}$. Insbesondere ist $L=K^H=\mathbb{Q}\left(\sqrt{-7}\right)$,

Für jede primitive siebte Einheitswurzel $\zeta$ ist

$$\zeta^2+\left(\zeta^2\right)^2+\left(\zeta^2\right)^4=\zeta^2+\zeta^4+\zeta$$

und

$$\zeta^4+\left(\zeta^4\right)^2+\left(\zeta^4\right)^4=\zeta^4+\zeta+\zeta^2\,,$$

so daß $S_H(\zeta)=S_H(\zeta^2)=S_H(\zeta^4)$ ist. Dieser gemeinsame Wert ist eine der beiden Zahlen $-\frac{1}{2}\pm\frac{1}{2}\sqrt{-7}$, die andere ist gleich $S_H(\zeta^3)$, $S_H(\zeta^5)$ und $S_H(\zeta^6)$. Man beachte, daß $\zeta^3,\zeta^5$ und $\zeta^6$ die Inversen von $\zeta^4,\zeta^2$ und $\zeta$ sind und damit konjugiert komplex zu diesen Zahlen.

Für $\zeta=e^{2\pi i/7}$ ist der Imaginärteil von $\zeta+\zeta^2+\zeta^4$ gleich

$$\sin(2\pi/7)+\sin(4\pi/7)+\sin(8\pi/7)\approx 1{,}322875656\approx\tfrac{1}{2}\sqrt{7}\,,$$

so daß $S_H(\zeta)=-\frac{1}{2}+\frac{1}{2}\sqrt{-7}$ ist. $\zeta$ ist daher eine Nullstelle des Polynoms $X^4+X^2+X+\frac{1}{2}-\frac{1}{2}\sqrt{-7}$ über $\mathbb{Q}\left(\sqrt{-7}\right)$. Dieses Polynom kann allerdings unmöglich irreduzibel über $\mathbb{Q}\left(\sqrt{-7}\right)$ sein, denn $\left[\mathbb{Q}\left(\sqrt{-7}\right):\mathbb{Q}\right]=2$ und $\left[k_7:\mathbb{Q}\right]=6$, so daß $\left[k_7:\mathbb{Q}\left(\sqrt{-7}\right)\right]=3$ ist.

Die Computeralgebra kennt Algorithmen, mit denen man auch Polynome über endlichen Erweiterungen von $\mathbb{Q}$ in ihre irreduziblen Faktoren zerlegen kann; für obiges Polynom liefern sie die beiden Faktoren

$$X-\frac{1}{2}+\frac{\sqrt{-7}}{2}\quad\text{und}\quad X^3+\frac{1-\sqrt{-7}}{2}X^2-\frac{1+\sqrt{-7}}{2}X-1\,.$$

Der erste hat die Nullstelle $\frac{1}{2}-\frac{1}{2}\sqrt{-7}$, der zweite hat $\zeta,\zeta^2$ und $\zeta^4$ als Nullstellen. $\mathbb{Q}(\zeta)$ ist somit der Zerfällungskörper dieses kubischen

Polynoms über $\mathbb{Q}\big(\sqrt{-7}\big)$. Anwendung der Formel von CARDANO führt beispielsweise auf die Nullstelle

$$\frac{\sqrt[3]{56+12\sqrt{21}-4\sqrt{-7}}}{6}+\frac{2\sqrt{-7}}{3\sqrt[3]{56+12\sqrt{21}-4\sqrt{-7}}}-\frac{1-\sqrt{-7}}{6}\,,$$

von der die numerische Auswertung (nach Regeln von Maple für die Werte von Kubikwurzeln komplexer Zahlen) zeigt, daß sie gleich $e^{2\pi i/7}$ ist.

Real- und Imaginärteil kann man aus dieser Darstellung nur schlecht ablesen, höchstens über die allgemeinen Formeln

$$\mathfrak{Re}\,z=\frac{z+\bar z}{2}\quad\text{und}\quad\mathfrak{Im}\,z=\frac{z-\bar z}{2i}\,.$$

In einem beliebigen Erweiterungskörper $K/\mathbb{Q}$ müssen allerdings zu einem Element $z\in K$ weder Realteil noch Imaginärteil in $K$ liegen, denn weder muß $\bar z$ in $K$ liegen noch $i$. In unserem Fall, für $K=k_7$, liegt aber zu jedem Element $z$ auch $\bar z$ in $K$, denn $\tau^3$ bildet $\zeta$ aus auf $\zeta^{27}=\zeta^{-1}$. Damit wird jede siebte Einheitswurzel auf ihr Inverses abgebildet, das komplex konjugiert zu ihr ist. Da die siebten Einheitswurzeln (ohne die Eins) eine $\mathbb{Q}$-Vektorraumbasis von $k_7$ bilden und $\tau^3$ auf dieser Basis mit der komplexen Konjugation übereinstimmt, ist $\tau^3$ auf $k_7$ die komplexe Konjugation. Damit liegt für jedes $z\in k_7$ auch der Realteil in $k_7$. Ein nichtverschwinder Imaginärteil kann aber nicht in $k_7$ liegen, denn sonst wäre $i\in\mathbb{Q}(\zeta)$, und $\mathbb{Q}(i)$ wäre ein Teilkörper vom Grad zwei. Da die GALOIS-Gruppe nur eine Untergruppe der Ordnung drei hat, gibt es aber nur einen Teilkörper vom Grad zwei, und das ist $L=\mathbb{Q}\big(\sqrt{-7}\big)$.

Die Gleichung

$$\zeta^4+\zeta^2+\zeta+\frac12\pm\frac12\sqrt{-7}=0$$

zeigt, daß für $x=\mathfrak{Re}\,\zeta=\cos\alpha$ gilt

$$\cos 4\alpha+\cos 2\alpha+\cos\alpha+\tfrac12=0\,.$$

Da $\zeta$ eine siebte Einheitswurzel ist, sind $\zeta^4$ und $\zeta^3$ invers zueinander, also komplex konjugiert, und haben daher denselben Realteil. Somit ist $\cos 4\alpha=\cos 3\alpha$ und damit auch

$$\cos 3\alpha+\cos 2\alpha+\cos\alpha+\tfrac12=0\,.$$

Aus der Gleichung

$$(\cos\alpha + i\sin\alpha)^2 = \left(e^{i\alpha}\right)^2 = e^{i\cdot 2\alpha} = \cos 2\alpha + i\sin 2\alpha$$

folgt, daß

$$\cos 2\alpha = \cos^2\alpha - \sin^2\alpha = \cos^2\alpha - (1-\cos^2\alpha) = 2\cos^2\alpha - 1$$

ist. Entsprechend führt die Gleichung

$$(\cos\alpha + i\sin\alpha)^3 = \left(e^{i\alpha}\right)^3 = e^{i\cdot 3\alpha} = \cos 3\alpha + i\sin 3\alpha$$

auf die Formel

$$\begin{aligned}\cos 3\alpha &= \cos^3\alpha - 3\cos\alpha\,\sin^2\alpha = \cos^3\alpha - 3\cos\alpha\,(1-\cos^2\alpha)\\ &= 4\cos^3\alpha - 3\cos\alpha\,.\end{aligned}$$

Speziell für $\alpha = 2\pi/7$ genügt $x = \cos\alpha$ somit der Gleichung

$$(4x^3 - 3x) + (2x^2 - 1) + x + \frac{1}{2} = 4x^3 + 2x^2 - 2x - \frac{1}{2} = 0\,.$$

Diese kubische Gleichung hat die drei verschiedenen Lösungen $\cos\alpha$, $\cos 2\alpha$ und $\cos 3\alpha$; wir sind also im *casus irreducibilis* mit drei verschiedenen reellen Lösungen, die bei Anwendung der Formel von CARDANO aber als Ausdrücke mit Wurzeln aus nichtreellen Zahlen erscheinen. Eine der Lösungen ist beispielsweise

$$x = \frac{\sqrt[3]{28 + 84\sqrt{-3}}}{28} + \frac{7}{3\sqrt[3]{28 + 84\sqrt{-3}}} - \frac{1}{6}\,,$$

was Maple numerisch mit $\cos\alpha$ identifiziert.

Es gibt auch einen Zwischenkörper $L'$ vom Grad drei über $\mathbb{Q}$; er ist der Fixkörper von $k_7$ bezüglich der Untergruppe $H = \{1, \tau^3\}$. Wie wir gerade gesehen haben, ist der Automorphismus $\tau^3$ die komplexe Konjugation, bildet also $\zeta$ ab auf $\bar{\zeta} = \zeta^{-1}$. Somit ist $S_{H'}(\zeta) = \zeta + \zeta^{-1}$.

Der Zwischenkörper $L'$ wird als $\mathbb{Q}$-Vektorraum nach dem obigen Lemma erzeugt von den Elementen $S_{H'}(\zeta^j)$, also von den drei Zahlen $S_{H'}(\zeta) = \zeta + \zeta^{-1} = \zeta + \zeta^6$, $S_{H'}(\zeta^2) = \zeta^2 + \zeta^{-2} = \zeta^2 + \zeta^5$ und

$S_{H'}(\zeta^3) = \zeta^3 + \zeta^{-2} = \zeta^3 + \zeta^4$. Das Polynom $X^3 + aX^2 + bX + c$ mit diesen drei Nullstellen hat nach dem Satz von VIÈTE die Koeffizieten

$$\begin{aligned}
a &= -(\zeta + \zeta^6 + \zeta^2 + \zeta^5 + \zeta^3 + \zeta^4) = 1 \\
b &= (\zeta + \zeta^6)(\zeta^2 + \zeta^5) + (\zeta + \zeta^6)(\zeta^3 + \zeta^4) + (\zeta^2 + \zeta^5)(\zeta^3 + \zeta^4) \\
&= \zeta^{11} + \zeta^{10} + 2\zeta^9 + 2\zeta^8 + 2\zeta^6 + 2\zeta^5 + \zeta^4 + \zeta^3 \\
&= 2\zeta^6 + 2\zeta^5 + 2\zeta^4 + 2\zeta^3 + 2\zeta^2 + 2\zeta = -2 \\
c &= -(\zeta + \zeta^6)(\zeta^2 + \zeta^5)(\zeta^3 + \zeta^4) \\
&= -(\zeta^{15} + \zeta^{14} + \zeta^{12} + \zeta^{11} + \zeta^{10} + \zeta^9 + \zeta^7 + \zeta^6) \\
&= -(\zeta^6 + \zeta^5 + \zeta^4 + \zeta^3 + \zeta^2 + \zeta + 2) = -1\,.
\end{aligned}$$

$\zeta+\zeta^{-1}$ ist also eine Nullstelle des kubischen Polynoms $X^3+X^2-2X-1$. Auch hier haben wir drei verschiedene reelle Nullstellen, denn

$$\zeta^j + \zeta^{-j} = \zeta^j + \overline{\zeta^j} = 2\,\mathfrak{Re}\,\zeta^j = 2\cos j\alpha\,.$$

Wieder sind wir also im *casus irreducibilis* mit drei reellen Lösungen, die aber in der Lösungsformel von CARDANO als Kombinationen komplizierter komplexer Wurzelausdrücke dargestellt werden. In der Tat haben wir fast die gleiche kubische Gleichung wie eben, denn ist $x$ eine Nullstelle von $X^3 + X^2 - 2X - 1$, so ist

$$4\left(\frac{x}{2}\right)^3 + 2\left(\frac{x}{2}\right)^2 - 2\frac{x}{2} - \frac{1}{2} = \frac{x^3 + x^2 - 2x - 1}{2} = 0\,,$$

d.h. $\frac{x}{2}$ ist eine Nullstelle von $4X^3 + 2X^2 - 2X - \frac{1}{2}$. Der Körper $L'$ ist somit der Zerfällungskörper über $\mathbb{Q}$ für jedes der beiden Polynome $X^3 + X^2 - 2X - 1$ und $4X^3 + 2X^2 - 2X - \frac{1}{2}$.

$\mathbb{Q}(\zeta)/L'$ ist eine quadratische Erweiterung; da

$$\zeta + \zeta^{-1} = u$$

eine Nullstelle des Polynoms $X^3 + X^2 - 2X - 1$ ist, können wir wie beim Fall der fünften Einheitswurzeln vorgehen und sehen nach Multiplikation obiger Gleichung mit $\zeta$, daß $\mathbb{Q}(\zeta)$ der Zerfällungskörper des Polynoms $X^2 - uX + 1$ über $L'$ ist. Damit sind alle Zwischenkörper mehr oder weniger explizit bestimmt.