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 $f \in k[X]$ 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 λ_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 λ_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 μ_{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 es gibt 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 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 nehmen wir natürlich $g = f$. Wie wir aus dem Lemma zu Beginn dieses Paragraphen wissen, ist $k_1 = k[X]/(g)$ ein Körper, in dem g (mindestens) eine Nullstelle z_1 hat.

Nun vergessen wir, wie k_1 aus einem Polynomring über k entstanden ist, und betrachten k_1 einfach als einen Körper. Über diesem Körper können wir wieder den Polynomring $k_1[X]$ bilden. Dort ist $g(z_1) = 0$. also ist g ein Vielfaches von $(X - z_1)$. Damit ist auch f durch $(X - z_1)$ teilbar. 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 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 daher ein Zerfällungskörper von f über k.

■

Für das Polynom $X^3 - 2$ über $\mathbb{Q}$ etwa konstruieren wir zunächst den Körper $k_1 = \mathbb{Q}[X]/(X^3 - 2)$; die Nebenklasse von X 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 $f_1 = X^2 + z_1X + z_1^2$. Wir bilden den neuen Faktorring $k_2 = k_1[X]/(X^2 + z_1X + z_1^2)$; die Restklasse von X modulo (f_1) sei z_2. Wir können nun noch f_1 in $k_2[X]$ durch $X - z_2$ dividieren; aber da das Ergebnis linear ist, wissen wir auch so, daß auch die zweite Lösung der

quadratischen Gleichung in k_2 liegt; 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 $1, z_1, z_1^2, z_2, z_1z_2, z_1^2z_2$.

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 $z_2^3 + \sqrt[3]{2}z_2 + \sqrt[3]{4} = 0$ 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 $z_1, \ldots, z_d$.

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

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

Wir wollen uns überlegen, daß dieses Polynom tatsächlich sogar schon in $\mathbb{R}[X]$ liegt.

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_λ reelle Zahlen, d.h. $g_\lambda \in \mathbb{R}[X]$ für alle λ.

Da es $\frac{1}{2}d(d-1)$ Paare (i, j) gibt, hat g_λ 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_λ 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_λ mindestens eine komplexe Nullstelle hat.

Die Nullstellen von g_λ 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 λ, 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

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

Aus §2 von Kapitel 1 wissen wir, daß wir zwei Zahlen, deren Produkt P und Summe S wir kennen, als Lösung der quadratischen Gleichung $X^2 - SX + P = 0$ bestimmen können, und aus der Analysis wissen wir, 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 zueinander, 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

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

∎

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

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

Der kleinste Teilkörper von $\mathbb{C}$, der sowohl k als auch die Elemente $z_1, \ldots, z_d$ enthält, ist somit 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 $z_1, \ldots, z_r$.

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 φ fortsetzt.

Beweis: In $K[X]$ läßt sich das Polynom f als Produkt von Linearfaktoren schreiben:

$$f = a_d(X - z_1) \cdots (X - z_d) \quad \text{mit} \quad a_i \in K\,.$$

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

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

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 ist $f \in k[X]$ durch $a_d(X - z_2) \cdots (X - z_d)$ teilbar, und der Quotient $X - z_1$ liegt in $k[X]$, d.h. auch $z_1 \in k$.

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 φ 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

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

wir können also einen Isomorphismus $\widetilde{\varphi}\colon k(z_1) \to k'(z_1')$ finden, der φ fortsetzt.

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 $\widetilde{\varphi}$ anwenden. Da r dann um mindestens eins kleiner ist, gilt es nach Induktionsannahme für diese Situation und damit auch für die betrachtete. ∎

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 φ 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; wir brauchen die Induktionsannahme daher für die allgemeinere Situation.

§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 Δ 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 $X^3 - U$, und dort können wir die drei Lösungen berechnen. 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, und da sich dort alle Elemente durch Wurzelausdrücke darstellen lassen, gilt dasselbe auf jeden Fall auch für die Lösungen.

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 φ 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 den 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 $x \in k$, 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 $x \in k$. Nach Induktionsannahme müssen daher alle Koeffizienten in dieser Gleichung verschwinden, insbesondere der Koeffizient

$a_1\big(\sigma_1(y) - \sigma_r(y)\big)$ von $\sigma_1(x)$. Da σ_1 und σ_r verschiedenen Homomorphismen sind, können wir ein $y \in k$ finden, für das $\sigma_1(y) \neq \sigma_r(y)$ ist; 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 hier nur $r-1$ Automorphismen vorkommen, zeigt eine nochmalige Anwendung der Induktionsannahme, daß auch $a_2, \ldots, a_r$ verschwinden.

■

Definition: *a)* Ist K/k eine Körpererweiterung, so bezeichnen wir mit 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 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

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

denn da die Multiplikation mit σ 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 von 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 $[K : k] \geq |G|$.

Aus dem zweiten Lemma folgt das erste, indem wir letzteres anwenden auf den Fall $L = K$ und die Menge $G' = G \cup \{\mathrm{id}_K\}$: Dann ist $k = K^G$ und $[K : K^G] = [K : K^{G'}] = [K : k] \geq |G'| \geq |G|$.

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

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

mit $i = 1, \ldots, r$. 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 $\sigma_j(a_ib_i) = \sigma_1(a_i)\sigma_j(b_j)$ 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

$$\sigma_j(a_1b_1)+\sigma_j(a_2b_2)+\cdots+\sigma_j(a_nb_n) = \sigma_j(a_1b_1+a_2b_2+\cdots+a_nb_n) = \sigma_j(x) .$$

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 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; die i-te der n Gleichungen ist

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

Wieder muß es eine nichttriviale Lösung $(x_1, \ldots, x_{n+1})$ geben, denn wir haben nur n Gleichungen für $n + 1$ Unbekannte. Für jedes $\lambda \neq 0$ aus K ist dann auch $(\lambda x_1, \ldots, \lambda x_{n+1})$ eine nichttriviale Lösung; durch geeignete Wahl von λ können wir also x_1 zu einem beliebigen Element von K 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 σ_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

$$b_1S(x_1) + b_2S(x_2) + \cdots + b_{n+1}S(x_{n+1}) = 0\,,$$

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 σ von K, der nicht in G liegt. Wäre $K^G = K^H$, so müßte σ 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, 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 $\sqrt[2]{3}$ 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 φ 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 dann auch 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 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 ggT$(f, f') \neq 1$. Andererseits ist aber 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 das Nullpolynom sein kann, ist auch das unmöglich. Also gibt es in $\mathbb{R}[X]$ keine nichtseparablen Polynome.

Wir werden bald sehen, daß dies auch für alle anderen Körper gilt, die $\mathbb{Q}$ enthalten, sowie auch für alle endlichen Körper.

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 $k[X]$: Wie für jedes Polynom über einem Körper können wir auch hierzu einen Körper K/k finden, in dem f eine Nullstelle s hat. In $K[X]$ ist

$$(X - s)^p = \sum_{i=0}^{p} \binom{p}{i} X^{p-i} s^i = X^p - s^p = X^p - T \,,$$

da

$$\binom{p}{i} = \frac{p(p-1)\cdots\big(p-(i-1)\big)}{i!}$$

für $1 \leq i \leq p-1$ einen durch p teilbaren Zähler, aber keinen durch p teilbaren Nenner hat, modulo p also verschwindet. Die Zerlegung von f in irreduzible Faktoren im Zerfällungskörper ist also $(X - s)^p$, es gibt daher nur eine einzige p-fache Nullstelle.

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 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 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 $\sigma \in$ 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.

∎

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 $\sigma \in$ 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.

∎

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

Beweis: Aut(L/K) ist die Untergruppe jener Automorphismen aus 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 σ 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 haben wir alles zusammen, um den Hauptsatz der GALOIS-Theorie zu 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 Aut$(L/L^H) = H$ ist: H ist auf jeden Fall eine Untergruppe von Aut(L/L^H); wären die beiden verschieden, hätten sie nach obigem Korollar verschiedene Fixkörper. Da der Fixkörper von Aut(L/L^H) den Körper L^H enthält und $[L : L^H] = |H|$ ist, müssen die beiden Körper und somit auch die beiden Untergruppen übereinstimmen.

Umgekehrt sei K ein Zwischenkörper; wir müssen zeigen, daß K der Fixkörper von 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 muß also so viele Elemente haben, wie der Index von H in G angibt. 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 sonst wäre nach einem der obigen Lemmata $[K : k] < [G : H]$. Daher muß jeder dieser Isomorphismen ein Automorphismus von K sein, d.h. $\sigma(K) = K$.

Für einen beliebigen Automorphismus σ von L ist $\sigma(K)$ ein Teilkörper von L. Ein weiterer Automorphismus $\tau\colon L \to L$ läßt diesen Körper 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 τ 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 $\sigma \in$ 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 Aut(L/K) ein Normalteiler von Aut(L/k) ist, und 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 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 beweise 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, die 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 σ_i übereinstimmen.

Nun sei x ein beliebiges Element des Fixkörpers von 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 τ_i lassen k punktweise fest, und da x im Fixkörper von Aut(K/k) liegt, ist auch $\tau_i(x) = x$. Daher ist

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

Das Polynom

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

hat daher 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. ∎

§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 schon vom Beispiel der dritten Wurzel aus zwei 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 ζ eines Körpers k heißt n-te *Einheitswurzel*, wenn $\zeta^n = 1$ ist. Wenn es keinen Teiler $m|n$ gibt, für den bereits $\zeta^m = 1$ ist, bezeichnen wir ζ als eine *primitive* n-te Einheitswurzel.

Satz: Der Körper k enthalte eine primitive n-te Einheitswurzel ζ, 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.

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. Somit ist

$k(\sqrt[n]{a})/k$ GALOISsch. Jeder Automorphismus von $k(\sqrt[n]{a})$ muß $\sqrt[n]{a}$ mit einer der Potenzen ζ^i multiplizieren, und da die Potenzen von ζ 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. ∎

Wenn wir uns für eine allgemeine 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 interessieren, können wir uns beschränken auf den Fall $a_d = 1$, denn da a_d nicht verschwindet, können wir die Gleichung durch a_d dividieren. Die verbleibenden Koeffizienten $a_0, \ldots, a_{d-1}$ müssen wir als Unbestimmte betrachten, d.h. wir arbeiten über dem Körper

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

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

$$f = X^d + a_{d-1}X^{d-1} + \cdots + a_1 X + a_0 .$$

Er wird über K (sogar über k) erzeugt von d Elementen $z_1, \ldots, z_d$ derart, daß in $L[X]$ gilt

$$f = (X - z_1)(X - z_2)\cdots(X - z_d) .$$

Nach dem Wurzelsatz von VIÈTE ist dann

$$a_i = (-1)^{d-i}\varphi_{d-i}(z_1, \ldots, z_d) ,$$

wobei φ_i das i-te elementarsymmetrische Polynom in d Variablen bezeichnet.

Die Gruppe $\mathfrak{S}_d$ aller Permutationen der Menge $\{1, \ldots, d\}$ operiert auf L, indem die Wurzel z_i abgebildet wird auf $z_{\pi(i)}$ für jedes i und jede Permutation $\pi \in \mathfrak{S}_d$. Die a_i 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.

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 die rationalen Zahlen enthält, mit den Lösungsformeln

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

eine solche Darstellung; wenn wir über einem Körper k arbeiten, der $\mathbb{F}_2$ enthält, geht das allerdings zumindest so nicht, da wir in $\mathbb{F}_2$ nicht durch zwei dividieren können.

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 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 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 $G_i/G_{i+1} \cong \mathbb{Z}/n_i$. Im Hinblick auf die Auflösbarkeit von Gleichungen definieren wir:

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

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

von Untergruppe 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 $G \neq \{\mathrm{id}\}$ heißt *einfach*, wenn sie keinen Normalteiler außer sich selbst und $\{\mathrm{id}\}$ hat.

Die einfachsten Beispiele einfacher Gruppen sind die zyklischen Gruppen von Primzahlordnung; eine zyklische Gruppe $\mathbb{Z}/n$ mit zusammengesetztem n ist nicht einfach, denn ist r ein Teiler von n und g ein Erzeugendes der Gruppe, so erzeugt $g^{n/r}$ eine Untergruppe der Ordnung r, die natürlich ein Normalteiler ist, da jede Untergruppe einer abelschen Gruppe Normalteiler ist.

Wenn wir zeigen können, daß die alternierende Gruppe A_d für $d \geq 5$ einfach ist, kann $\mathfrak{S}_d$ für $d \geq 5$ nicht auflösbar sein, denn dann ist A_d der einzige Normalteiler und diese Gruppe hat selbst keinen nichttrivialen Normalteiler. Als nichtabelsche Gruppe ist sie selbstverständlich auch nicht zyklisch.

Satz: Für $d \geq 5$ ist die alternierende Gruppe A_d einfach.

Wir führen den *Beweis* in fünf Schritten:

1. Schritt: A_d wird von den Dreierzykeln erzeugt.

Beweis: Jedes Element von 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 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 π 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 π^{-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 π abgebildet auf ein $\pi(x) \notin \{a, b, c\}$, so daß $\pi(x)$ von $(a\ b\ c)$ festgelassen wird. Durch π^{-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 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 $\pi \in A_d$, sind wir fertig. Andernfalls existiert wegen $d \geq 5$ eine Transposition τ, 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 π eine ungerade Permutation ist, muß $\tau\pi$ gerade sein, also in A_d liegen.

4. Schritt: Für $d \geq 5$ ist jeder Normalteiler von A_d, der einen Dreierzyklus enthält, gleich A_d.

Beweis: Falls er einen Dreierzyklus enthält, muß er nach dem vorigen Schritt *alle* Dreierzykeln enthalten, ist also nach dem ersten Schritt gleich A_d.

Der Satz folgt nun aus

5. Schritt: Für $d \geq 5$ enthält jeder nichttriviale Normalteiler $N \trianglelefteq A_d$ einen Dreierzyklus.

Beweis: Ist π 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 π 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.

■

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 Mengen $\{P_0, \ldots, P_r\}$ 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 adjungieren die Koordinaten der Punkte P_i an $\mathbb{Q}$; der entstehende Körper sei k_0. Jede Gerade durch zwei der Punkte P_i läßt sich dann beschreiben als Nullstellenmenge einer linearen Gleichung mit Koeffizienten in k_0: Sind (x_i, y_i) und (x_j, y_j) die Koordinaten der beiden Punkte, so können wir beispielsweise die Gleichung

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

nehmen. 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 Geraden müssen wir ein System aus zwei linearen Gleichungen mit Koeffizienten aus k lösen; falls es eine Lösung gibt, d.h. wenn die Geraden nicht verschieden und parallel sind, liegt diese, wie aus der Linearen Algebra bekannt, wieder 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 konstruierte Punkte somit in einem Körper k, der aus k_0 durch schrittweise Körpererweiterungen vom Grad zwei entsteht:

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

Insbesondere ist $[k : k_0] = 2^r$ 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_r, P_s 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 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 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

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

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 ζ, 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 ζ 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 ζ^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 ξ von f und jede Primzahl p, die kein Teiler von n ist, auch ξ^p eine Nullstelle von f ist. Falls dies für irgendein ξ und irgendein p nicht der Fall ist, muß ξ^p Nullstelle eines weiteren irreduziblen Polynoms g sein. Da ξ^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 ξ 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 $G = g^p$. 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 ξ, 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 φ die aus dem zweiten Kapitel bekannte EULERsche φ-Funktion ist, die die Anzahl der primen Restklassen modulo n angibt.

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: $F_m = 2^{2^m} + 1$ heißt die m-te FERMAT-Zahl sein; 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 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, ist n das Produkt einer Zweierpotenz (die auch eins sein kann) mit verschiedenen FERMATschen Primzahlen. ∎

Tatsächlich gilt auch die Umkehrung dieses Satzes; wenn $n \geq 3$ also von der angegebenen Form ist, ist das regelmäßige n-Eck mit Zirkel und Lineal konstruierbar. 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 288) 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 nicht 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.

Ein weiteres klassisches Problem ist das der Dreiteilung des Winkels. Da die Konstruierbarkeit des regelmäßigen n-Ecks äquivalent ist zur Konstruierbarkeit des Winkels zwischen seinem Mittelpunkt und zwei benachbarten Ecken, also des Winkels $2\pi/n$, würde die Möglichkeit der Dreiteilung jedes Winkels mit Zirkel und Lineal zu einer Konstruktion des regelmäßigen 3^n-Ecks führen, denn das gleichseitige Dreieck ist natürlich konstruierbar, und mit dem Winkel $2\pi/3$ wäre auch jeder Winkel $2\pi/3^n$ konstruierbar.

Das wohl berühmteste Problem für Konstruktionen mit Zirkel und Lineal ist die Quadratur des Kreises. Wenn sie möglich ist, muß $\mathbb{Q}(\pi)/\mathbb{Q}$ eine Körpererweiterung von Zweierpotenzordnung sein. Tatsächlich aber bewies FERDINAND VON LINDEMANN 1882, daß $\mathbb{Q}(\pi)/\mathbb{Q}$ eine unendliche Körpererweiterung ist, was man auch so ausdrückt, daß π eines *transzendente* Zahl ist. Damit war auch bewiesen, daß die Quadratur des Kreises mit Zirkel und Lineal nicht möglich ist.

§5: Endliche Körper

Für jeden Körper k gibt es genau einen (Ring-)homomorphismus $\varphi: \mathbb{Z} \to k$, denn durch die Homomorphieeigenschaft und die Bedingungen $\varphi(0) = 0$ und $\varphi(1) = 1$ ist φ vollständig festgelegt. Der Kern von φ ist ein Ideal von $\mathbb{Z}$, also ein Hauptideal (n). Dabei muß $n = 0$ oder eine Primzahl sein, denn wäre $n = rs$ ein Produkt zweier Zahlen vom Betrag größer eins, so wäre $\varphi(r)\varphi(s) = \varphi(n) = 0$, im Widerspruch zur Nullteilerfreiheit eines Körpers.

Definition: Die Zahl $p \geq 0$, für die Kern $\varphi = (p)$ ist, heißt die *Charakteristik* char k des Körpers k.

Für einen Körper der Charakteristik Null ist φ injektiv, der Körper enthält also einen zu $\mathbb{Z}$ isomorphen Ring und damit einen zu $\mathbb{Q}$ isomorphen Körper. Im Falle positiver Charakteristik $p > 0$ ist $\varphi(\mathbb{Z})$ isomorph zu $\mathbb{Z}/p = \mathbb{F}_p$, der Körper enthält also einen zu $\mathbb{F}_p$ isomorphen Körper. Diesen zu $\mathbb{Q}$ oder $\mathbb{F}_p$ isomorphen Körper bezeichnen wir als den *Primkörper* des Körpers k. Wir identifizieren ihn meist mit $\mathbb{Q}$ beziehungsweise $\mathbb{F}_p$.

Der Primkörper eines endlichen Körpers k muß natürlich einer der Körper $\mathbb{F}_p$ sein; k ist dann ein endlichdimensionaler $\mathbb{F}_p$-Vektorraum, so daß die Elementanzahl eines endlichen Körpers immer eine Primzahlpotenz sein muß.

In einem Körper k der positiven Charakteristik $p > 0$ führt die Multiplikation eines Elements mit einem Vielfachen von p stets auf das Ergebnis Null. Da der Binomialkoeffizient $\binom{p}{i}$ für $0 < i < p$ einen durch p teilbaren Zähler, aber einen nicht durch p teilbaren Nenner hat, ist er ein Vielfaches von p; daher ist für zwei beliebige Elemente x, y eines solchen Körpers

$$(x + y)^p = \sum_{i=0}^{p} \binom{p}{i} x^i y^{p-i} = x^p + y^p \ .$$

Somit ist die Abbildung

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

ein Homomorphismus. Er heißt 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.

Wie wir wissen, ist jeder Homomorphismus eines Körpers in einen Körper injektiv; das gilt insbesondere 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.

Wie wir aus §3 des vorigen Kapitels wissen, ist die multiplikative Gruppe eines endlichen Körpers stets zyklisch; 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 Logarithmus 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 $\mathbb{F}_2$ 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 eines wählen, das das Rechnen modulo diesem Polynom möglichst einfach macht; insbesondere sollte das verwendete Polynom möglichst wenige Terme habe.

Wie sich zeigt, bestehen dreizehn der dreißig Polynome aus sieben nichtverschwindenden Termen, die restlichen siebzehn aus 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 bei zwei Polynomen 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.