Vorlesungen über Algebra

Mainz, Sommersemester 2008

Manfred Lehn

Korrekturstand: 23. November 2012.

Einleitung

Die Vorstellung von dem, was Algebra ist, hat sich im Laufe der Zeit sehr gewandelt. Im engsten Sinne ist Algebra die Lehre von der Auflösung von Gleichungen. Die dabei auftretenden Probleme und Phänomene haben aber die Fragestellungen und den Gegenstand der Untersuchung verschoben.

Die Feststellung, daß manche Gleichungen keine Lösungen besitzen, machte immer wieder die Erweiterung von Rechenbereichen notwendig. Um ungehindert subtrahieren zu können, muß man die Halbgruppe $\mathbb{N}$ zur Gruppe $\mathbb{Z}$ erweitern, um dividieren zu können, erweitert man den Ring $\mathbb{Z}$ zum Körper $\mathbb{Q}$. Die Messung von Streckenlängen und die Erfahrung der Pythagoräer, daß es inkommensurable Strecken gibt, führten zu der Erweiterung des Körpers $\mathbb{Q}$ zu dem vollständigen Körper $\mathbb{R}$. Und der Wunsch, auch für beliebige polynomiale Gleichungen Nullstellen zu haben, erzwang die Erweiterung von $\mathbb{R}$ zum algebraisch abgeschlossenen Körper $\mathbb{C}$.

Diese Entwicklung verlief aber historisch nicht in der systematischen Weise, wie sie diese einleitenden Sätze glauben machen könnten. Negative Zahlen wurden sehr viel später erfunden als Brüche oder selbst irrationale Zahlen. Die Theorie der reellen Zahlen als einem Körper, der durch Vervollständigung von $\mathbb{Q}$ bezüglich der Betragsbewertung konstruiert wird, ist viel jüngeren Datums als die Erfindung der komplexen Zahlen, auch wenn viele Grundideen für die Idee der Dedekindschen Schnitte sich schon in der Proportionentheorie von Eudoxos in den Elementen des Euklids finden.

Und die komplexen Zahlen kamen nicht auf die Welt, weil man unbedingt Wurzeln aus negativen Zahlen ziehen wollte – denn wozu wäre das gut? – , sondern weil Cardano Formeln zur Lösung kubischer Gleichungen vor sich hatte, die in gewissen Fällen zu Wurzelausdrücken mit negativen Radikanden führten, also anscheinend unlösbar waren, obwohl die Gleichungen selbst offensichtlich reelle Lösungen besaßen. Zur geschichtlichen Entwicklung speziell der Galoistheorie empfehle ich das eingehende Studium des Buches *Galois' theory of algebraic equations* von Jean-Pierre Tignol.

Seit dem 16. Jahrhundert wußte man, wie Gleichungen dritten und vierten Grades zu lösen sind. Das Problem, auch für Gleichungen höheren Grades Lösungsformeln zu finden, sei es für allgemeine Gleichungen, sei es für bestimmte Gleichungen, wie sie im Zusammenhang mit Einheitswurzeln und der Kreisteilung auftreten, erwies sich als schwierig. In den Arbeiten von Vandermonde, Lagrange und vor allem Galois kommt nun ein ganz neues Element ins Spiel: Der Zusammenhang zwischen der Auflösung von Gleichungen und den Symmetrien von polynomialen Ausdrücken in den Wurzeln der Gleichung unter Permutation dieser Wurzeln. Der Begriff der Gruppe war der erste in einer heute langen Liste von algebraischen Strukturen wie Körper, Ring, Vektorraum, Modul, Liealgebra, Schiefkörper, Operaden etc. Damit hat sich auch die Algebra selbst weg von einer Lehre, wie man Gleichungen löst, hin zur einer Wissenschaft von den Strukturen mathematischer Objekte gewandelt. Eine Vorlesung über Galoistheorie steht an der Schnittstelle zwischen der alten Lehre und der modernen Strukturwissenschaft. Das macht ihren Reiz aus.

Diese Vorlesungsnotizen sind nur für die Hörer meiner Vorlesung bestimmt und erheben keinen Anspruch auf Originalität. Eine Vorlesung kann immer nur einen Einblick in ein Gebiet geben, ohne Selbststudium geht es nicht. Dazu gehört die Lektüre der einschlägigen Literatur. Von den vielen existierenden Algebrabüchern (mit dem kanonischen Titel: Algebra) möchte ich besonders die von Bosch, M. Artin, und Lang nennen. Ich selbst habe die Galoistheorie aus dem Klassiker von van der Waerden gelernt. Zu den Klassikern zählt auch das kleine Buch mit dem eleganten Zugang von E. Artin. Und wer die Zeit hat, sollte noch eine Generation zurückgehen und einen Blick und einen zweiten in das interessante Algebrabuch von Weber werfen.

M.L.

Inhaltsverzeichnis

§1 Symmetrische Polynome

14. April 2008

Es sei A ein kommutativer Ring. Die Symmetrische Gruppe S_n wirkt auf dem Polynomring $A[X_1, \ldots, X_n]$ durch Vertauschung der Variablen: $\pi : X_i \mapsto X_{\pi(i)}$. Ein Polynom $f \in A[X_1, \ldots, X_n]$ heißt symmetrisch, wenn es invariant unter allen Permutation $\pi \in S_n$ ist. Das bedeutet, daß

$$f(X_1, \ldots, X_n) = f(X_{\pi(1)}, \ldots, X_{\pi(n)}) \tag{1.1}$$

für alle $\pi \in S_n$. Die Menge der symmetrischen Polynome bilden einen Unterring $A[X_1, \ldots, X_n]^{S_n}$ im Ring aller Polynome.

Die Potenzsummen $t_k := X_1^k + \ldots + X_n^k$, $k > 0$, sind symmetrisch. Ebenso die elementarsymmetrischen Polynome $s_k := \sum_{i_1 < \ldots < i_k} X_{i_1} \cdots X_{i_k}$, $0 < k \leq n$. Ausgeschrieben lauten die elementarsymmetrischen Polynome für $n = 4$:

$$\begin{aligned} s_1 &= X_1 + X_2 + X_3 + X_4 \\ s_2 &= X_1X_2 + X_1X_3 + X_1X_4 + X_2X_3 + X_2X_4 + X_3X_4 \\ s_3 &= X_1X_2X_3 + X_1X_2X_4 + X_1X_3X_4 + X_2X_3X_4 \\ s_4 &= X_1X_2X_3X_4 \end{aligned}$$

Die Bezeichnungen s_k sind nicht ganz befriedigend, weil man nur aus dem Kontext auf die Anzahl der relevanten Variablen schließen kann. Aber zusätzliche Indizierungen würden die Lesbarkeit unnötig erschweren.

Bemerkung 1.1 (Formeln von Girard[1] und Viète[2]) — In $A[X_1, \ldots, X_n, t]$ gilt die Beziehung

$$(t - X_1) \cdot \ldots \cdot (t - X_n) = t^n - s_1 t^{n-1} + s_2 t^{n-2} + \ldots + (-1)^n s_n. \tag{1.2}$$

Das sind die Formeln von Girard und Viète über den Zusammenhang zwischen den Koeffizienten eines Polynoms und seinen Nullstellen: Sind $\lambda_1, \ldots, \lambda_n \in A$ die Nullstellen eines Polynoms $f = X^n + f_1 X^{n-1} + f_2 X^{n-2} + \ldots + f_{n-1} X + f_n$, so gilt

$$f_k = (-1)^k s_k(\lambda_1, \ldots, \lambda_n).$$

Dabei sind die Nullstellen so häufig einzusetzen, wie es ihrer Vielfachheit entspricht.

Satz 1.2 *(Hauptsatz über symmetrische Polynome) — Es sei A ein kommutativer Ring. Der Ringhomomorphismus $\Phi : A[Y_1, \ldots, Y_n] \to A[X_1, \ldots, X_n]^{S_n}$, $Y_i \mapsto s_i$, ist ein Isomorphismus.*

[1] Albert Girard, ⋆1595 †8.12.1632
[2] François Viète, ⋆1540 †13.12.1603

In Worten ausgedrückt heißt das, daß sich jedes symmetrische Polynom als Polynom in den elementarsymmetrischen Polynomen ausdrücken läßt, und zwar auf eindeutige Weise.

Beweis. Zunächst erhält man durch die Zuordnung $Y_i \mapsto s_i$ wegen der universellen Eigenschaft des Polynomrings einen eindeutig bestimmten Ringhomomorphismus $A[Y_1, \ldots, Y_n] \to A[X_1, \ldots, X_n]$. Und da die Auswertung eines beliebigen Polynoms in beliebigen symmetrischen Polynomen wieder symmetrisch ist, liegt das Bild im Unterring der symmetrischen Polynome. Wir geben zwei Algorithmen an, die für jedes symmetrische Polynom eine Darstellung als Polynom in elementarsymmetrischen Polynomen liefern.

Algorithmus 1: Wir bezeichnen mit $q : A[X_1, \ldots, X_n] \to A[X_1, \ldots, X_{n-1}]$ den eindeutigen Homomorphismus mit $q(X_n) = 0$ und $q(X_i) = X_i$ für $i < n$. Unter q gehen symmetrische Polynome auf symmetrische Polynome, und zwar gilt $q(s_n) = 0$ und $q(s_i) = s'_i$, das i-te elementarsymmetrische Polynom in den Unbestimmten $X_1, \ldots, X_{n-1}$, für $i < n$. Es bezeichne $\Phi' : A[Y_1, \ldots, Y_{n-1}] \to A[X_1, \ldots, X_{n-1}]$ den Ringhomomorphismus $Y_i \mapsto s'_i$. Durch Induktion über die Anzahl der Variablen können wir als bekannt annehmen, daß Φ' ein Isomorphismus auf den Unterring der symmetrischen Polynome ist. Wir haben ein kommutatives Diagramm aus exakten Folgen

$$\begin{array}{ccccccccc} 0 & \longrightarrow & (X_n) & \longrightarrow & A[X_1, \ldots, X_n] & \xrightarrow{q} & A[X_1, \ldots, X_{n-1}] & \longrightarrow & 0 \\ & & \uparrow & & \uparrow{\scriptstyle \Phi} & & \uparrow{\scriptstyle \Phi'} & & \\ 0 & \longrightarrow & (Y_n) & \longrightarrow & A[Y_1, \ldots, Y_n] & \xrightarrow{q} & A[Y_1, \ldots, Y_{n-1}] & \longrightarrow & 0 \end{array} \tag{1.3}$$

Es sei nun $f \in A[X_1, \ldots, X_n]$ symmetrisch. Das Polynom $f' := q(f)$ ist symmetrisch in $X_1, \ldots, X_{n-1}$. Nach Induktion gibt es ein Polynom $g' \in A[Y_1, \ldots, Y_{n-1}]$ mit $\Phi'(g') = g'(s'_1, \ldots, s'_{n-1}) = f'$. Die Differenz $h := f - g'(s_1, \ldots, s_{k-1})$ ist dann ein symmetrisches Polynom mit $q(h) = 0$, d.h. $X_n | h$. Wegen der Symmetrie von h wird h auch von $X_2, \ldots, X_n$ geteilt, und somit auch von s_n. Wir setzen $\tilde{f} := h/s_n$. Nun hat $\tilde{f}$ einen kleineren Grad als f und ist symmetrisch. Wir können also induktiv annehmen, daß $\tilde{f}$ im Bild von Φ liegt. Es gibt also ein Polynom $\tilde{g} \in A[Y_1, \ldots, Y_n]$ mit $f = s_n \tilde{g}(s_1, \ldots, s_n) + g'(s_1, \ldots, s_{n-1})$.

Ebenso beweist man die Injektivität: Angenommen $g \in \ker(\Phi)$. Dann liegt $q(g)$ im Kern von Φ' und ist nach Induktion trivial. Daher gilt $g = s_n \tilde{g}$ für ein Polynom $\tilde{g}$ von kleinerem Grad. Aus $0 = \Phi(g) = X_1 \cdots X_n \cdot \Phi(\tilde{g})$ folgt, daß $\tilde{g} \in \ker(\Phi)$. Durch Induktion über den Grad von g folgt, daß $\tilde{g} = 0$ und damit auch, daß $g = s_n \tilde{g} = 0$.

Algorithmus 2: Dieser Algorithmus geht auf Waring[3] zurück, die Eindeutigkeit der Darstellung wurde ausdrücklich erst von Gauß[4] formuliert und bewiesen.

Wir ordnen die Monome $X^d = X_1^{d_1} \cdots X_n^{d_n}$ lexikographisch, d.h. wir setzen

[3] Edward Waring, $\star$1736 †15. August 1798

[4] Johann Carl Friedrich Gauß $\star$1777 †1855

$X^d > X^{d'}$ genau dann, wenn es ein i mit der folgenden Eigenschaft gibt: $d_j = d'_j$ für alle $j < i$ und $d_i > d'_i$.

Es sei nun $f = \sum f_t X^t$ ein symmetrisches Polynom. Für das Leitmonom X^d von f gilt wegen der Symmetrieannahme, daß $d_1 \geq d_2 \geq \ldots \geq d_n$. Das symmetrische Polynom

$$g := f_d s_1^{d_1-d_2} s_2^{d_2-d_3} \cdots s_{n-1}^{d_{n-1}-d_n} s_n^{d_n} \tag{1.4}$$

hat denselben Leitterm wie f. Die Differenz $f - g$ hat daher einen strikt kleineren Leitterm bezüglich der Monomordnung als f. Durch Induktion folgt nun die Behauptung. Ähnlich beweist sich die Injektivität: Das Polynom $s_1^{\nu_1} \cdots s_n^{\nu_n}$ hat das Leitmonom $x_1^{\nu_1+\ldots+\nu_n} x_2^{\nu_2+\ldots+\nu_n} \cdots x_n^{\nu_n}$. Die Bilder verschiedener Monome $Y_1^{\nu_1} \cdots Y_n^{\nu_n}$ unter Φ haben verschiedene Leitmonome. Deshalb kann es in $\Phi(\sum_\nu a_\nu Y^\nu)$ nicht zu einer vollständigen Auslöschung aller Monome in den Variablen X_i kommen. □

Eine fundamentale Konsequenz des Hauptsatzes, die wir in der Folge häufig anwenden werden, ist das folgende Prinzip:

Folgerung 1.3 *— Es seien $A \subset B$ Ringe und $f = X^n + a_1 X^{n-1} + \ldots + a_n \in A[X]$ ein Polynom, das über B in Linearfaktoren zerfällt:*

$$f(X) = (X - \lambda_1) \cdot \ldots \cdot (X - \lambda_n). \tag{1.5}$$

Dann liegt jedes Element $b \in B$, das sich symmetrisch und polynomiell in den Nullstellen $\lambda_1, \ldots, \lambda_n$ ausdrücken läßt, schon in A.

Beweis. Es sei $\Phi : A[X_1, \ldots, X_n] \to B$ der Ringhomomorphismus mit $\Phi : X_i \mapsto \lambda_i$. Die Annahme über b besagt, daß es ein symmetrisches Polynom f mit $\Phi(f) = b$ gibt. Nun gilt nach den Formeln von Girard und Viète, daß $\Phi(s_i) = (-1)^i a_i \in A$. Nach dem Hauptsatz gibt es ein Polynom $g \in A[Y_1, \ldots, Y_n]$ mit $f = g(s_1, \ldots, s_n)$. Es folgt $b = \Phi(f) = g(\Phi(s_1), \ldots, \Phi(s_n)) = g(-a_1, a_2, \ldots) \in A$. □

18. April 2008

Im Falle der Potenzsummen $t_k := x_1^k + \ldots + x_n^k$ findet man leicht die folgenden Umrechnungsformeln von Newton[5]:

$$\begin{aligned} t_1 &= s_1 \\ t_2 &= s_1^2 - 2s_2 \\ t_3 &= s_1^3 - 3s_1 s_2 + 3s_3 \end{aligned}$$

Hier und im folgenden setzen wir $s_k = 0$, wenn k größer als die Anzahl der betrachteten Variablen ist. Für größere k ist die Beschreibung der t_k als Polynome in den elementarsymmetrischen Polynomen weniger offensichtlich.

Lemma 1.4 *(Newton) — Es gilt*

$$t_n - s_1 t_{n-1} + s_2 t_{n-2} - \ldots + (-1)^n n s_n = 0. \tag{1.6}$$

[5] Sir Isaac Newton, ⋆1643 †1727

Beweis. Wertet man Gleichung (1.2) in X_i aus, erhält man

$$0 = X_i^n - s_1 X_i^{n-1} + \ldots + (-1)^n s_n. \tag{1.7}$$

Summation über alle $i = 1, \ldots, n$ liefert die Behauptung. □

Daraus lassen sich die t_n rekursiv durch die s_k, $k \leq n$, ausdrücken, ohne daß man auf den allgemeinen Algorithmus des Hauptsatzes 1.2 zurückgreifen muß. Man beachte den Vorfaktor n vor s_n in der Identität (1.6). Deshalb entstehen beim umgekehrten Auflösen nach den s_n Nenner. Die Formeln

$$\begin{aligned} s_1 &= t_1 \\ s_2 &= \frac{1}{2}(t_1^2 - t_2) \\ s_3 &= \frac{1}{6}t_1^3 - \frac{1}{2}t_1 t_2 + \frac{1}{3}t_3 \end{aligned}$$

gelten daher nur in $\mathbb{Q}$-Algebren.

Die Umrechnungsformeln zwischen elementarsymmetrischen Polynomen und Potenzsummen lassen sich einigermaßen geschlossen ausdrücken. Um solche Ausdrücke herzuleiten, verwenden wir erzeugende Funktionen.

1.5 Exkurs: Potenzreihenringe — Es sei A ein Ring. Wir versehen die Menge B aller Abbildungen $a : \mathbb{N}_0 \to A$, $n \mapsto a_n$, wie folgt mit der Struktur eines kommutativen Rings:

$$(a+b)_n := a_n + b_n, \quad (ab)_n := \sum_{k=0}^{n} a_k b_{n-k}.$$

Wir notieren eine Folge a wie folgt:

$$a = \sum_{n=0}^{\infty} a_n t^n.$$

Der Ring $A[[t]] := B$ heißt Ring der formalen Potenzreihen. Statt t kann natürlich eine beliebige andere Variable stehen. In $A[[t]]$ rechnet man, wie man es von Potenzreihen aus der Anaylsis gewohnt ist. Bezeichnet man mit $\mathbb{C}\{t\}$ den Ring der konvergenten Potenzreihen, d.h. der Potenzreihen mit positivem Konvergenzradius, so bestehen die Inklusionen

$$\mathbb{C}[t] \subset \mathbb{C}\{t\} \subset \mathbb{C}[[t]].$$

Allerdings können wir $A[[t]]$ für beliebige Ringe A bilden. Wir werden später Potenzreihenringe auf eine systematischere Weise als Vervollständigungen von Polynomringen konstruieren und dann selbst zum Gegenstand der Untersuchung machen. Für den Augenblick brauchen wir den Potenzreihenring lediglich als den Ring im Hintergrund, in dem sich die Rechnungen abspielen.

1.6 Exkurs: Erzeugende Funktionen — Kombinatorische Daten lassen sich häufig gut organisieren, wenn man sie als Koeffizienten einer Potenzreihe interpretiert. Wir

betrachten als Beispiel die Fibonacci-Zahlen

$$f_0 = 0, \quad f_1 = 1, \quad f_2 = 1, \quad f_3 = 2, \quad \ldots, \quad f_{n+1} = f_n + f_{n-1},$$

und bilden die Potenzreihe

$$f = \sum_{n=0}^{\infty} f_n t^n = t + t^2 + 2t^3 + 3t^4 + 5t^5 + \ldots \in \mathbb{Q}[[t]].$$

f heißt die erzeugende Funktion zur Folge (f_n). Die Umwandlung der Folge in eine Funktion ist rein formal. Sie wird erst dann nützlich, wenn es gelingt, die kombinatorischen Informationen über die Folge, also zum Beispiel Rekursionsrelationen, in eine algebraische Gleichung oder eine Differentialgleichung für f zu übersetzen. Im Beispiel der Fibonaccizahlen geht das so: Die Rekursionsrelationen zwischen den f_n lassen sich durch die eine Gleichung

$$f = tf + t^2 f + t$$

oder äquivalent

$$f = \frac{-t}{t^2 + t - 1}$$

ausdrücken. Damit ist viel gewonnen, denn die rechte Seite kann jetzt mit den Standardmethoden der Analysis untersucht werden. Wir machen eine Partialbruchzerlegung und entwickeln in eine geometrische Reihe. Dazu seien λ_1 und λ_2 die Nullstellen des Polynoms $t^2 + t - 1$:

$$\begin{aligned} f &= \frac{-t}{t^2 + t - 1} = \frac{1}{\lambda_2 - \lambda_1}\left(\frac{\lambda_1}{t - \lambda_1} - \frac{\lambda_2}{t - \lambda 2}\right) \\ &= \frac{1}{\lambda_1 - \lambda_2} \sum_{n=0}^{\infty} \left(\frac{1}{\lambda_1^n} - \frac{1}{\lambda_2^n}\right) t^n. \end{aligned}$$

Der Koeffizientenvergleich zeigt nun, daß

$$f_n = \frac{1}{\lambda_1 - \lambda_2}\left(\frac{1}{\lambda_1^n} - \frac{1}{\lambda_2^n}\right) = (-1)^{n-1} \frac{\lambda_1^n - \lambda_2^n}{\lambda_1 - \lambda_2}$$

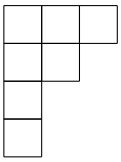
für alle $n \geq 0$, wobei im letzten Schritt die Relation $\lambda_1 \lambda_2 = -1$ verwendet wurde. Jetzt kann man die konkreten Werte

$$\lambda_1 = \frac{1}{2}\left(-1 + \sqrt{5}\right), \quad \lambda_2 = \frac{1}{2}\left(-1 - \sqrt{5}\right)$$

einsetzen und findet:

$$f_n = \frac{1}{\sqrt{5}}\left(\left(\frac{1 + \sqrt{5}}{2}\right)^n - \left(\frac{1 - \sqrt{5}}{2}\right)^n\right).$$

1.7 Exkurs: Partitionen — Eine Partition von $n \in \mathbb{N}_0$ ist eine monoton fallende Folge $\lambda = (\lambda_1, \lambda_2, \ldots)$ von Zahlen $\lambda_i \in \mathbb{N}_0$ mit $\sum_{i \geq 0} \lambda_i = n$. Die Anzahl der $\lambda_i \neq 0$ heißt die Länge der Partition. Ist ℓ die Länge von λ, so schreibt man meist $\lambda = [\lambda_1, \ldots, \lambda_\ell]$ und läßt die irrelevanten Nullen weg. Eine nützliche graphische Darstellungsmöglichkeit für Partitionen sind die sogenannten Young-Diagramme. Zum Beispiel ist



das Young-Diagramm zur Partition $[3,2,1,1]$ von 7. Für viele Zwecke ist eine andere exponentielle Notation von Partitionen angebracht: Wir fassen eine Abbildung $\alpha : \mathbb{N} \to \mathbb{N}_0$, $n \mapsto \alpha_n$, als die Partition auf, die die Zahl i genau α_i-mal enthält. Wir schreiben die Partition dann in der Form

$$\alpha = (1^{\alpha_1} 2^{\alpha_2} 3^{\alpha_3} \ldots),$$

also zum Beispiel

$$[4,4,2,1,1,1] = (1^3 2^1 3^0 4^2)$$

In dieser Notation ist die Länge der Partition α gegeben durch

$$|\alpha| = \sum_i \alpha_i$$

und α ist eine Partition von

$$\|\alpha\| = \sum_i \alpha_i i.$$

Mit diesen Begriffen greifen wir das Problem der Potenzsummen auf. Wir rechnen im Potenzreihenring $\mathbb{Q}[X_1, \ldots, X_n][[z]]$ und betrachten die logarithmische Ableitung des Ausdrucks

$$\prod_{i=1}^{n} (1 + zX_i) = \sum_{j=0}^{n} s_j z^j, \tag{1.8}$$

wobei $s_0 = 1$ und s_j wie früher das j elementarsymmetrische Polynom von $X_1, \ldots, X_n$ bezeichnet. Wir erhalten:

$$\begin{aligned} z\frac{\partial}{\partial z} \log\left(\sum_{j=0}^{n} s_j z^j\right) &= \sum_{i=1}^{n} \frac{zX_i}{1+zX_i} = \sum_{i=1}^{n}\sum_{m=1}^{\infty} (-1)^{m-1} z^m X_i^m \\ &= \sum_{m=1}^{\infty} (-1)^{m-1} t_m z^m = z\frac{\partial}{\partial z} \sum_{m=1}^{\infty} (-1)^{m-1} \frac{t_m}{m} z^m. \end{aligned}$$

Daraus ergibt sich

$$\log\left(1 + \sum_{j=1}^{n} s_j z^j\right) = \sum_{m=1}^{\infty} (-1)^{m-1} \frac{t_m}{m} z^m,$$

weil beide Seiten keine konstanten Terme in z haben. Das liefert einerseits

$$t_m = (-1)^{m-1} m \cdot \text{Coeff}\left(z^m, \log\left(1 + \sum_{j=1}^{n} s_j z^j\right)\right) \tag{1.9}$$

und andererseits

$$s_k = \mathrm{Coeff}\left(z^k, \exp\left(\sum_{m=1}^{\infty}(-1)^{m-1}\frac{t_m}{m}z^n\right)\right). \tag{1.10}$$

Beide Formeln kann man etwas expliziter machen, wenn man die Potenzreihenentwicklungen für $\log$ und $\exp$ und die Multinomialformel

$$(y_1 + \ldots + y_n)^m = \sum_{m_1+\ldots+m_n=m} \frac{m!}{m_1!\cdots m_n!} y_1^{m_1}\cdots y_n^{m_n} \tag{1.11}$$

verwendet. Mit den oben eingeführten Bezeichnungen für Partitionen in exponentieller Schreibweise gilt:

$$\frac{t_m}{m} = \sum_{\|\alpha\|=m} (-1)^{m+|\alpha|-1}\frac{(|\alpha|-1)!}{\alpha_1!\alpha_2!\cdots}\prod_i s_i^{\alpha_i}, \tag{1.12}$$

dabei läuft die Summe über alle Partitionen α von n. Und ganz analog findet mat

$$s_k = (-1)^k \sum_{\|\beta\|=k}\prod_j \frac{1}{\beta_j!}\left(\frac{-t_j}{j}\right)^{\beta_j}, \tag{1.13}$$

Aufgaben zu symmetrischen Polynomen

Aufgabe 1.1 — Programmieren Sie einen oder beide Algorithmen in Mupad (oder Maple oder ...). Präzisieren Sie zunächst die Aufgabenstellung: Sie übergeben eine beliebigen Ausdruck, in dem viele Bezeichner vorkommen können, eine Liste von Bezeichnern, die den Unbestimmten im Satz entsprechen, sowie eine Liste von Werten (!), die den elementarsymmetrischen Polynomen entsprechen. Da Sie nicht wissen, *welche* Werte übergeben werden, dürfen Sie nicht zu früh substituieren...

Aufgabe 1.2 — Drücken Sie die folgenden symmetrischen Polynome durch elementarsymmetrische Polynome aus:

1. $X_1^4 + X_2^4 + X_3^4 + X_4^4$.
2. Es sei $h_k \in A[X_1, \ldots, X_n]$ die Summe aller Monome vom Grad k. Die h_k heißen vollständige symmetrische Polynome. Schreiben Sie h_k für $n = 3$ und $k = 1, \ldots, 3$ als Polynom in den elementarsymmetrischen Polynomen.
3. $\Delta := \prod_{1\le i<j\le 3}(X_i - X_j)^2$.

Aufgabe 1.3 — Das Polynom $\Delta := \prod_{i<j}(X_i - X_j)^2 \in \mathbb{Z}[X_1, \ldots, X_n]$ ist symmetrisch. Deshalb gibt es ein Polynom disc_n, die sogenannte Diskriminante, mit $\Delta = \mathrm{disc}_n(s_1, \ldots, s_n)$, wobei $s_1, \ldots, s_n$ die elementarsymmetrischen Polynome in den X_i bezeichnen.

1. Bestimmen Sie disc_2 und disc_3.

2. Es sei $f = X^n - f_1 X^{n-1} + \ldots + (-1)^n f_n$. Zeigen Sie: f hat genau dann eine mehrfache Nullstelle, wenn $\mathrm{disc}(f_1, \ldots, f_n) = 0$.

3. Wir betrachten den Raum $V = \{f = X^3 - aX - b \mid a, b \in \mathbb{R}\} \cong \mathbb{R}^2$. Bestimmen Sie die Orte $V_1 \subset V$ aller Polynome mit mehrfacher Nullstelle und $V_0 \subset V_1$ aller Polynome mit dreifacher Nullstelle. (Zeichnung).

Aufgabe 1.4 — Betrachten Sie die letzte Frage aus Aufgabe 1.3 auch für Polynome vom Grad 4: Es sei $V = \{f = X^4 + aX^2 + bX + c \mid a, b, c \in \mathbb{R}\}$. Bestimmen Sie die Orte V_2 aller Polynome mit mindestens doppelter Nullstelle, V_{22} mit mindestens zwei doppelten Nullstellen, V_3 mit mindestens einer dreifachen Nullstelle und V_4 mit einer vierfachen Nullstelle.

Aufgabe 1.5 — Wir betrachten den Polynomring $S = \mathbb{C}[X_{ij}, 1 \leq i, j \leq n]$ in n^2 Unbestimmten. Das charakteristische Polynom $\chi_A(t) = t^n - \chi_1 t^{n-1} + \ldots + (-1)^n \chi_n$ der Matrix $A = (X_{ij}) \in M_n(\mathbb{C})$ hat Koeffizienten $\chi_k \in S$. Für jede Matrix $M \in M_n(\mathbb{C})$ sind $(-1)^i \chi_i(M)$ die Koeffizienten des charakteristischen Polynoms von M.

1. Es gibt ein Polynom $p \in S$ mit der Eigenschaft, daß jede Matrix $M \in M_n(\mathbb{C})$ genau dann paarweise verschiedene Eigenwerte hat, wenn $p(M) \neq 0$.

2. Finden Sie für $n = 4$ eine Formel, die die Koeffizienten $\chi_i(M)$, $i = 1, \ldots, n$ durch die Spuren $\mathrm{tr}(M^k)$, $k = 1 \ldots, n$, ausdrückt.

Hinweis zum zweiten Teil: Betrachten Sie zunächst diagonalisierbare Matrizen und verwenden Sie dann ein Stetigkeitsargument.

Aufgabe 1.6 (Invariante Polynome für die alternierende Gruppe) — Die Gruppe S_n operiert auf dem Polynomring $\mathbb{C}[X_1, \ldots, X_n]$ durch $\sigma(X_i) = X_{\sigma(i)}$. Ein Polynom f ist S_n-invariant (oder symmetrisch), wenn $\sigma(f) = f$ für alle $\pi \in S_n$. Ein Polynom f ist antisymmetrisch, wenn $\sigma(f) = \mathrm{sgn}(\sigma) f$ für alle $\pi \in S_n$. Schließlich ist f A_n-invariant, wenn $\sigma(f) = f$ für alle σ in der alternierenden Gruppe A_n. Zeigen Sie:

1. Das Polynom $\delta := \prod_{i<j}(X_i - X_j)$ ist antisymmetrisch.

2. Ist f antisymmetrisch, so gilt $\delta | f$, und f/δ ist symmetrisch.

3. f ist genau dann A_n-symmetrisch, wenn sich f als Summe eines symmetrischen und eines antisymmetrischen Polynoms schreiben läßt.

4. Die Menge A der A_n-invarianten Polynome ist ein Unterring in $\mathbb{C}[X_1, \ldots, X_n]$, der die Menge S der S_n-invarianten Polynome als Unterring enthält.

5. A wird als $\mathbb{C}$-Algebra von den elementarsymmetrischen Polynome s_1,..., s_n und δ erzeugt.

6. Der Kern des Homomorphismus $\Psi : \mathbb{C}[Y_1, \ldots, Y_n, Z] \to A$, $Y_i \mapsto s_i$, $Z \mapsto \delta$, wird von dem Element $Z^2 - \mathrm{disc}_n(Y_1, \ldots, Y_n)$ erzeugt (cf. Aufgabe 1.3).

Aufgaben zu erzeugenden Funktionen

Aufgabe 1.7 — Wir betrachten die Folgen (a_n) und (b_n), die durch die folgenden Rekursionsgleichungen definiert sind.

$$a_0 = 0, \quad a_{n+1} = 2a_n + 1, \text{ für } n \geq 0, \tag{1.14}$$

und

$$b_0 = 1, \quad b_{n+1} = 2b_n + n, \text{ für } n \geq 0. \tag{1.15}$$

Finden Sie explizite Formeln für die Folgen (a_n) und (b_n) mit Hilfe der erzeugenden Funktionen $a(z) := \sum_{n\geq 0} a_n z^n$ und $b(z) := \sum_{n\geq 0} b_n z^n$. Übersetzen Sie die Rekursionsgleichungen in Gleichungen für $a(z)$ bzw. $b(z)$. Lösen Sie nach $a(z)$ bzw. $b(z)$ auf und bestimmen Sie die a_n bzw. b_n.

Aufgabe 1.8 (Catalansche Zahlen) — Es sei X eine Menge mit einer nichtassoziativen Verknüpfung $\circ : X \times X \to X$. Für jedes n sei C_n die Anzahl der formal verschiedenen Möglichkeiten, n Elemente $x_1, \ldots, x_n$ in dieser Reihenfolge zu multiplizieren. Zum Beispiel ist $C_4 = 5$, denn es gibt die Möglichkeiten

$$x_1(x_2(x_3x_4)), \quad x_1((x_2x_3)x_4), \quad (x_1(x_2x_3))x_4, \quad ((x_1x_2)x_3)x_4, \quad (x_1x_2)(x_3x_4).$$

Genauso sieht man $C_1 = 1$, $C_2 = 1$ und $C_3 = 2$. Zeigen Sie:

1. Es gilt die Rekursionsgleichung $C_n = \sum_{k=1}^{n-1} C_k C_{n-k}$.

2. Für die erzeugende Funktion $C(t) = \sum_{n\geq 1} C_n t^n = t+t^2+2t^3+5t^4+14t^5+\ldots$ gilt: $C^2 - C = t$.

3. $C_n = \frac{1}{n}\binom{2n-2}{n-1}$.

C_n ist auch die Anzahl der Möglichkeiten, ein konvexes $(n+1)$-Eck durch Einziehen von sich nicht schneidenden Diagonalen in Dreiecke zu zerlegen.

Aufgabe 1.9 (Fibonaccizahlen II) — Eine andere nützliche Weise, eine erzeugende Funktion zu bilden, ist die folgende: Aus den Zahlen $f_0, f_1, \ldots$ bilden wir $f(t) := \sum_{n\geq 0} \frac{f_n}{n!} t^n$.

1. Die Rekursionsgleichung für die Fibonaccizahlen f_n übersetzt sich in die Differentialgleichung $f'' - f' - f = 0$ mit den Anfangswerten $f(0) = 0$, $f'(0) = 1$.

2. Man löse die Differentialgleichung und bestimme aus der Lösung die f_n.

§2 Gruppen und Symmetrien

Ich erinnere an einige Grundbegriffe aus der Gruppentheorie: Eine *Gruppe* ist eine Menge G zusammen mit einer assoziativen Verknüpfung $\circ : G \times G \to G$ und den folgenden Eigenschaften: Es gibt ein Neutralelement $e \in G$ mit $e \circ g = g = g \circ e$ für alle $g \in G$, und zu jedem Element $g \in G$ gibt es ein Inverses $h \in G$ mit $g \circ h = e = h \circ g$. Das Neutralelement ist eindeutig bestimmt, ebenso das Inverse jedes Elements, das wir meist mit g^{-1} bezeichnen.

Eine Gruppe ist *abelsch*[6], wenn $g \circ h = h \circ g$ für je zwei Elemente $g, h \in G$. Häufig wird die Verknüpfung in abelschen Gruppen additiv geschrieben, d.h. mit dem Symbol $+$. In diesem Falle wird das Neutralelement meist mit 0 bezeichnet und das Inverse zu g mit $-g$.

Eine Teilmenge $H \subset G$ ist eine *Untergruppe*, wenn H nicht leer ist, wenn $H \circ H \subset H$ und wenn H mit der Einschränkung der Verknüpfung wieder eine Gruppe ist. Damit eine nichtleere Teilmenge $H \subset G$ eine Untergruppe ist, genügt es, daß $gh^{-1} \in H$ für alle $g, h \in H$. Gelegentlich schreiben wir $H < G$, um auszudrücken, daß H eine Untergruppe von G ist. Eine Untergruppe $H < G$ ist *normal* oder ein *Normalteiler*, wenn $ghg^{-1} \in H$ für alle $h \in H$ und $g \in G$. Wir schreiben $H \lhd G$ um auszudrücken, daß H ein Normalteiler von G ist. Das *Zentrum* einer Gruppe ist der Normalteiler

$$Z(G) := \{g \in G \mid hg = gh \text{ für alle } h \in G\}.$$

Ein Gruppenhomomorphismus $\varphi : G \to G'$ ist eine Abbildung von Gruppen mit $\varphi(gh) = \varphi(g)\varphi(h)$. Ein Gruppenhomomorphismus φ ist ein Isomorphismus, wenn φ bijektiv ist. In diesem Falle ist die inverse Abbildung φ^{-1} automatisch ein Homomorphismus. Ein Isomorphismus $\varphi : G \to G$ ist ein Automorphismus von G. Wir bezeichnen einen trivialen Homomorphismus $\varphi : G \to G'$, der ganz G auf das Neutralelement $e' \in G'$ abbildet, durch $\varphi = e'$. Der Kern eines Homomorphismus $\varphi : G \to G'$ ist die Untergruppe $\varphi^{-1}(e') \subset G$, das Bild $\mathrm{im}(\varphi)$ die Untergruppe $\varphi(G) \subset G'$. Eine endliche oder unendliche Folge

$$\ldots \longrightarrow G_{n-1} \xrightarrow{\varphi} G_n \xrightarrow{\psi} G_{n+1} \ldots$$

heißt *exakt* an der Stelle G_n, wenn $\ker(\psi) = \mathrm{im}(\varphi)$.

Eine Gruppe ist *zyklisch*, wenn es ein Element $g \in G$ mit $G = \{g^n \mid n \in \mathbb{Z}\}$ gibt. Jede zyklische Gruppe ist isomorph zu $\mathbb{Z}$ oder $\mathbb{Z}/n$.

Für eine Untergruppe $H < G$ und ein Gruppenelement $a \in G$ bezeichnet $aH = \{ah \mid h \in H\}$ die durch a erzeugte *Linksnebenklasse* von H. Entsprechend ist $Ha = \{ha \mid h \in H\}$ die *Rechtsnebenklasse* zu H. Die Menge aller Linksnebenklassen wird mit G/H, die Menge aller Rechtsnebenklassen mit $H\backslash G$ bezeichnet. Offensichtlich haben alle Nebenklassen dieselbe Mächtigkeit wie H. Außerdem sind je zwei Links(oder Rechts)nebenklassen disjunkt oder gleich, d.h. G ist die disjunkte Vereinigung ihrer Links(oder Rechts)nebenklassen. Daraus ergibt sich:

[6] Niels Abel ⋆5. August 1802 †6. April 1829

Satz 2.1 *(Satz von Lagrange[7]) — Für jede Untergruppe H von G gilt*

$$|G| = |H| \cdot |G/H| = |H| \cdot |H\backslash G|.$$

Dabei spielt es keine Rolle, ob G oder H endliche oder unendliche Gruppen sind. □

Eine Untergruppe H ist genau dann ein Normalteiler, wenn $aH = Ha$ für alle $a \in G$. In diesem Falle sind die Mengen G/H und $H\backslash G$ gleich.

Satz 2.2 *— Es sei $N \lhd G$ ein Normalteiler. Es gibt genau eine Gruppenstruktur auf G/N, bezüglich der die kanonische Projektion $\pi : G \to G/N$ ein Gruppenhomomorphismus ist. G/N mit dieser Gruppenstruktur heißt Faktorgruppe zum Normalteiler N.*

Beweis. Da $\pi : G \to G/N$ surjektiv ist, ist die Gruppenstruktur durch die Forderung

$$g_1N \cdot g_2N = \pi(g_1) \cdot \pi(g_2) = \pi(g_1g_2) = g_1g_2N$$

eindeutig bestimmt. Definiert man umgekehrt die Verknüpfung auf die angegebene Weise, so ist zunächst zu zeigen, daß $\cdot$ wohldefiniert ist. In der Tat, falls $g_1N = g_1'N$ und $g_2N = g_2'N$, so gibt es $n_1, n_2 \in N$ mit $g_1' = g_1n_1$ und $g_2' = g_2n_2$. Daraus folgt

$$g_1'g_2' = g_1n_1g_2n_2 = g_1g_2(g_2^{-1}n_1g_2)n_2.$$

Weil N ein Normalteiler ist, gilt $(g_2^{-1}n_1g_2)n_2 \in N$, was zu zeigen war. Jetzt folgt leicht, daß $\cdot$ eine Gruppenstruktur und π ein Homomorphismus ist. □

Satz 2.3 *(Homomorphiesatz) — Es sei $\varphi : G \to G'$ ein Gruppenhomomorphismus. Dann induziert φ einen Isomorphismus $G/\ker(\varphi) \to \mathrm{im}(\varphi)$.*

Beweis. Indem wir G' durch $\varphi(G)$ ersetzen, können wir ohne Einschränkung annehmen, daß φ surjektiv ist. Es sei $N = \ker(\varphi)$. Nun folgt: $\varphi(g_1) = \varphi(g_2)$ genau dann, wenn $g_1^{-1}g_2 \in N$, d.h. wenn $g_1N = g_2N$. Deshalb ist $\bar{\varphi} : G/N \to G'$, $g_1N \mapsto \varphi(g_1)$, wohldefiniert, ein Gruppenhomomorphismus und bijektiv. □

Satz 2.4 *(Universelle Eigenschaft der Faktorgruppe) — Es sei G eine Gruppe, $N \lhd G$ ein Normalteiler und $\pi : G \to G/N$ die kanonische Projektion. Ein Gruppenhomomorphismus $\varphi : G \to G'$ faktorisiert genau dann über G/N, d.h. es gibt einen Homomorphismus $\bar{\varphi} : G/N \to G'$ mit $\varphi = \bar{\varphi} \circ \pi$, wenn $N \subset \ker(\varphi)$.*

Beweis. Wenn $\bar{\varphi}$ existiert, so gilt $\varphi(N) = \bar{\varphi}(\pi(N)) = \bar{\varphi}(\bar{e}) = e'$, d.h. $N \subset \ker(\varphi)$. Wir nehmen umgekehrt an, die Bedingung $N \subset \ker(\varphi)$ sei erfüllt. Dann gilt für zwei Repräsentanten g_1, g_2 derselben Nebenklasse $g_1N = g_2N \in G/N$, daß $g_1^{-1}g_2 \in$

[7] Lagrange ⋆25. Januar 1736 †10. April 1813

N, also $\varphi(g_1)^{-1}\varphi(g_2) = e'$ oder $\varphi(g_1) = \varphi(g_2)$. Das zeigt, daß $\bar{\varphi}(g_1 N) := \varphi(g_1)$ wohldefiniert ist. Es folgt dann sofort, daß $\bar{\varphi}$ ein Gruppenhomomorphismus ist, und nach Konstruktion gilt $\bar{\varphi} \circ \pi = \varphi$. □

2.1 Gruppenwirkungen

Eine *Linkswirkung* der Gruppe G auf der Menge X ist eine Abbildung

$$s : G \times X \to X$$

mit der Eigenschaft $s(e, x) = x$ und $s(g, s(h, x)) = s(gh, x)$ für alle $g, h \in G$, $x \in X$. Eine G-Menge ist eine Menge X mit einer G-Wirkung. Wenn die Wirkung aus dem Kontext klar ist, schreibt man kürzer $gx := s(g, x)$. Die Bedingung an die Wirkung liest sich dann wie eine klassische Assoziativitätsbedingung: $ex = x$, $g(hx) = (gh)x$ für $e, g, h \in G$ und $x \in X$. Analog definiert man eine Wirkung von rechts.

Es sei X eine G-Menge. Die *Bahn* (der Orbit) von $x \in X$ ist die Menge $Gx := \{gx \mid g \in G\}$. Die *Standgruppe* (Isotropie-, Stabilisatorgruppe) von $x \in X$ ist die Untergruppe $G_x := \mathrm{Stab}(x) := \{g \in G \mid gx = x\}$. Der Bahnenraum ist die Menge aller Bahnen und wird für eine Linkswirkung mit $G\backslash X$ und für eine Rechtswirkung mit X/G bezeichnet. Die kanonische Projektion $\pi : X \to G\backslash X$ bildet jedes $x \in X$ auf seine Bahn ab. Eine Wirkung ist *transitiv*, wenn alle Elemente von X in einer Bahn liegen. Die Wirkung ist *frei*, wenn alle Standgruppen trivial sind. Schließlich ist $x \in X$ ein *Fixpunkt*, wenn $Gx = \{x\}$, oder anders gesagt, wenn $G_x = G$. Die Menge aller Fixpunkte wird mit X^G bezeichnet.

Zwischen den Mächtigkeiten von X und seinen Bahnen und den Ordnungen von G und der Standgruppen bestehen Relationen, die durch die Bahnengleichungen präzisiert werden:

Satz 2.5 *(Bahnengleichungen) — Es sei G eine endliche Gruppe und $G \times X \to X$ eine Gruppenwirkung.*

1. *Es gilt $|X| = \sum_{B \in G\backslash X} |B|$.*
2. *Für jedes $x \in X$ gilt $|G| = |G_x| \cdot |Gx|$*

Beweis. Jedes Element von X liegt in genau einer Bahn, d.h. X ist die disjunkte Vereinigung aller Bahnen. Durch Übergang zu Mächtigkeiten folgt die erste Aussage. Es sei nun $x \in X$ beliebig. Wir betrachten die Abbildung $p : G \to Gx$, $g \mapsto gx$. Nach Konstruktion ist p surjektiv. Es sei $y \in Gx$ beliebig und $g_0 \in p^{-1}(y)$. Dann gilt $g \in p^{-1}(y)$ genau dann, wenn $gx = g_0 x$, d.h. $(g_0)^{-1}gx = x$, also $(g_0)^{-1}g \in G_x$ oder $g \in g_0 G_x$. Das bedeutet insbesondere, daß $|p^{-1}(y)| = |G_x|$ für alle $y \in Gx$. Es folgt $|G| = \sum_{y \in Gx} |p^{-1}(y)| = |Gx| \cdot |G_x|$. □

Beispiel 2.6 — Die Gruppe $G = \mathrm{SO}(2)$ wirkt auf der Einheitssphäre $S \subset \mathbb{R}^3$ durch Verdrehung der ersten beiden Koordinaten:

$$\left(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) , \begin{pmatrix} x \\ y \\ z \end{pmatrix} \right) \mapsto \begin{pmatrix} ax+by \\ cx+dy \\ z \end{pmatrix}.$$

Es gibt zwei Fixpunkte: die beiden Pole. Die Bahnen dieser Wirkung sind genau die Pole und die Breitenkreise. Die Standgruppe von $y \in S$ ist die volle Gruppe $\mathrm{SO}(2)$, wenn y ein Pol ist, und sonst die triviale Gruppe.

Beispiel 2.7 — Die Symmetrische Gruppe S_n wirkt auf der Menge $[n] = \{1, \ldots, n\}$ durch $(\pi, k) \mapsto \pi(k)$. Die Wirkung ist sicher transitiv: Sind $x, y \in [n]$ verschiedene Elemente, so bildet die Transposition $\tau = (x\, y)$ das Element x auf y ab, d.h. alle Elemente liegen in einer Bahn. Die Standgruppe jedes Elements ist isomorph zur symmetrischen Gruppe S_{n-1}.

Beispiel 2.8 — Es sei $H < G$ eine Untergruppe. Dann wirkt H durch Multiplikation von links und von rechts auf G. Die Bahnen sind genau die Rechts- bzw. Linksnebenklassen. Man beachte die Vertauschung von links und rechts: die Rechtsnebenklasse von H zu a ist die Menge $Ha = \{ha \mid h \in H\}$. Die Wirkung ist frei. Die Bahnengleichung führt auf den Satz von Lagrange.

2.2 Rechnen in der symmetrischen Gruppe

Ich setze die Grundregeln für das Rechnen in der symmetrischen Gruppe als bekannt voraus und wiederhole nur zum Zwecke der Referenz die Grundbegriffe.

Es sei $n \in \mathbb{N}$. Die symmetrische Gruppe S_n ist die Menge der Bijektionen der Menge $[n] = \{1, \ldots, n\}$ in sich mit der Komposition als Verknüpfung. Für jede Folge $(n_1, \ldots, n_k)$ von $k \geq 2$ paarweise verschiedenen Zahlen aus $[n]$ bezeichnet $\pi = (n_1 \ \ldots \ n_k) \in S_n$ die Permutation

$$\pi(i) = \begin{cases} n_{j+1} \\ n_1 \\ i \end{cases} \text{, falls } \begin{cases} i = n_j, j < k, \\ i = n_k, \\ \text{sonst.} \end{cases}$$

Permutationen dieser Form heißen k-Zykel oder Zykel der Länge k. Zykel der Länge 2 heißen Transpositionen. Es ist dann klar, daß $(n_1 \ldots n_k) = (n_k\, n_1 \ldots n_{k-1})$. Zwei Zykel $(n_1 \ \ldots \ n_k)$ und $(m_1 \ \ldots \ m_\ell)$ sind disjunkt, falls die Mengen $\{n_1, \ldots, n_k\}$ und $\{m_1, \ldots, m_\ell\}$ disjunkt sind. Schließlich bezeichnen wir gelegentlich die Identität auf $[n]$ mit dem 1-Zykel $(1) = (2) = \ldots$.

Es sei eine Permutation $\pi \in S_n$ gegeben. Die von π erzeugte zyklische Gruppe $\langle \pi \rangle$ operiert auf der Menge $[n]$, und unter dieser Wirkung zerfällt $[n]$ in Bahnen $B_1, \ldots, B_s$. Diese seien so numeriert, daß $|B_1| \geq |B_2| \geq \ldots$. Die Partition $Z(\pi) = [|B_1|, |B_2|, \ldots, |B_s|]$ von n heiße der Zykeltyp der Permutation π. Zum Beispiel ist

der Zykeltyp von $(145)(27) \in S_8$ die Partition $[3,2,1,1,1]$. Man sieht leicht, daß umgekehrt jede Partition von n wirklich als Zykeltyp einer Partition vorkommt.

Jede Bahn B der Länge ℓ bestimmt einen eindeutigen ℓ-Zykel ζ wie folgt: Es sei $x \in B$ beliebig gewählt. Wir setzen $\zeta = (x\,\pi(x)\,\pi^2(x)\ldots\pi^{\ell-1}(x))$. Eine Bahn der Länge 1, die also nur aus einem Fixpunkt unter $\langle\pi\rangle$ besteht, liefert natürlich die Identität. Definiert man auf diese Weise zu jeder Bahn B_i der Länge $\ell_i \geq 2$ einen Zykel ζ_i, so sind alle Zykel ζ_1, ζ_2,... paarweise disjunkt und es gilt $\pi = \zeta_1\zeta_2\ldots$. Nur im Falle $\pi = \mathrm{id}_{[n]}$ gibt es überhaupt keine Bahnen der Länge ≥ 2, und π ist das leere Produkt. Auf diese Weise läßt sich jede Permutation als Produkt von disjunkten Zykeln schreiben, und diese Darstellung ist eindeutig bis auf die Reihenfolge der Faktoren.

Der folgende Satz ist nicht schwer zu beweisen: die erste Aussage ergibt sich durch direkte Rechnung, die zweite folgt dann mehr oder weniger direkt aus der ersten.

Satz 2.9 — *Für jede Permutation π und jeden k-Zykel $(n_1\ \ldots\ n_k)$ in S_n gilt*

$$\pi \cdot (n_1\ \ldots\ n_k) \cdot \pi^{-1} = (\pi(n_1)\ \ldots\ \pi(n_k)).$$

Zwei Permutationen $\pi, \pi' \in S_n$ sind genau dann konjugiert, wenn sie denselbe Zykeltyp haben. Insbesondere ist die Abbildung

$$\{\textit{Konjugationsklassen von } S_n\} \leftrightarrow \{\textit{Partitionen von } n\}, \pi \mapsto \textit{Zykeltyp von } \pi,$$

eine Bijektion.

2.3 Automorphismengruppen

Es sei G ein Gruppe. Die Menge $\mathrm{Aut}(G)$ aller Automorphismen von G ist eine Gruppe bezüglich Komposition und heißt Automorphismengruppe von G. Das Neutralelement von $\mathrm{Aut}(G)$ ist die identische Abbildung id_G, das gruppentheoretische Inverse von $\varphi \in \mathrm{Aut}(G)$ ist die inverse Abbildung φ^{-1}.

Beispiele 2.10 — 1. $\mathrm{Aut}(\mathbb{Z},+) \cong \mathbb{Z}/2$. Die Gruppe $\mathbb{Z}$ hat zwei Erzeuger: 1 und -1. Jeder Automorphismus muß 1 auf einen der beiden Erzeuger abbilden und ist durch diesen Wert auch schon eindeutig bestimmt. Deshalb ist $\mathrm{Aut}(\mathbb{Z}) = \{\mathrm{id}, -\mathrm{id}\}$.
2. $\mathrm{Aut}(\mathbb{Z}/2\times\mathbb{Z}/2) \cong S_3$. Die Gruppe $G = \mathbb{Z}/2\times\mathbb{Z}/2$ hat drei nichttriviale Elemente $(1,0)$, $(0,1)$, $(1,1)$. Diese haben die Eigenschaft, daß für je drei verschiedene Elemente g_1, g_2, g_3 gilt: $g_1g_2 = g_3$. Deshalb bestimmt jede Permutation der Menge $G \setminus \{0\}$ einen Automorphismus von G und umgekehrt.
3. $\mathrm{Aut}(\mathbb{Z}/n) \cong (\mathbb{Z}/n)^* = \{\bar{k} \mid 0 < k < n, k \text{ teilerfremd zu } n\}$. Jeder Automorphismus $\sigma : \mathbb{Z}/n \to \mathbb{Z}/n$ ist durch den Wert auf dem Erzeuger $\bar{1}$ eindeutig bestimmt, etwa $\sigma(\bar{1}) = \bar{k}$. Allgemein ist also $\sigma(\bar{i}) = \bar{k}\bar{i}$ für ein geeignetes $\bar{k}$. Und σ ist genau dann eine Bijektion, wenn $\bar{k}$ eine Einheit in $\mathbb{Z}/n$ ist, also zu n teilerfremd ist. Die Mächtigkeit der Einheitengruppe von $\mathbb{Z}/n$ ist per definitionem die Eulersche Phi-Funktion:

$\varphi(n) := |\{k \mid 0 < k < n, k \text{ teilerfremd zu } n\}|$. Es gilt

$$\frac{\varphi(n)}{n} = \prod_{p|n} \left(1 - \frac{1}{p}\right),$$

wo p durch die Primfaktoren von n läuft.

Es sei G eine (multiplikativ geschriebene) Gruppe. Für jedes Element $g \in G$ bezeichnet

$$c_g : G \to G, x \mapsto gxg^{-1},$$

die Konjugation mit g. Zwei Elemente $x, x' \in G$ sind konjugiert, wenn es ein $g \in G$ mit $gxg^{-1} = x'$ gibt. Konjugiert zu sein ist eine Äquivalenzrelation auf G. Die Äquivalenzklassen heißen Konjugationsklassen.

Denselben Sachverhalt kann man auch so sehen: Jede Gruppe G operiert auf sich vermöge der Wirkung $(g, x) \mapsto gxg^{-1}$. Die Konjugationsklasse von x ist genau die Bahn von x unter dieser Wirkung. Fixpunkte sind genau die Gruppenelemente, die mit allen anderen Gruppenelementen vertauschen.

Für jedes $g \in G$ ist c_g ein Automorphismus von G, denn

$$c_g(xy) = g(xy)g^{-1} = (gxg^{-1})(gyg^{-1}) = c_g(x)c_g(y).$$

Automorphismen dieses Typs heißen innere Automorphismen. Weiter ist die Abbildung $c : G \to \mathrm{Aut}(G)$ ein Gruppenhomomorphismus, denn

$$c_{gh}(x) = ghx(gh)^{-1} = g(hxh^{-1})g^{-1} = c_g(c_h(x)).$$

Der Kern von c ist $Z(G) = \{g \in G \mid xg = gx \text{ für alle } x \in G\}$, das Zentrum der Gruppe. Das Bild $\mathrm{Int}(G) := c(G) \subset \mathrm{Aut}(G)$ heißt Gruppe der inneren Automorphismen und ist nicht nur eine Untergruppe, sondern sogar ein Normalteiler. Es gilt nämlich $\varphi c_g \varphi^{-1} = c_{\varphi(g)}$. Die Faktorgruppe $\mathrm{Out}(G) := \mathrm{Aut}(G)/\mathrm{Int}(G)$ heißt Gruppe der äußeren Automorphismen. Wir können die Situation übersichtlich durch die folgende exakte Sequenz wiedergeben:

$$1 \longrightarrow Z(G) \longrightarrow G \longrightarrow \mathrm{Aut}(G) \longrightarrow \mathrm{Out}(G) \longrightarrow 1.$$

Der folgende Satz ist in gewissem Sinne kurios, weil es gar nicht einleuchten will, warum ausgerechnet die Gruppe S_6 anders sein soll als die anderen symmetrischen Gruppen.

Satz 2.11 *(O. Hölder[8]) — Die Abbildung $c : S_n \to \mathrm{Aut}(S_n)$ ist für alle $n \neq 2$ injektiv und für alle $n \neq 6$ surjektiv. In den beiden Ausnahmefällen ist $Z(S_2) = S_2$ und $\mathrm{Out}(S_6) \cong \mathbb{Z}/2$.*

[8] Otto Ludwig Hölder ⋆22. Dezember 1859 †29. August 1937

Beweis. 1. Schritt: Ein Element $\pi \in S_n$ liegt genau dann im Zentrum, wenn die Konjugationsklasse von π genau ein Element enthält. Aber dann kann π keinen Zykel der Länge $n \geq 3$ enthalten, sonst könnte man durch Umnumerieren eine andere Permutation mit demselben Zykeltyp erhalten. Ebensowenig darf π mehrere Zykel der Länge 2 enthalten oder gleichzeitig Fixpunkte haben und nichttriviale Zykel enthalten. Das läßt nur die Möglichkeiten $\pi = (1) = \mathrm{id}$ oder $\pi = (12)$, wenn $n = 2$. Das zeigt: $Z(S_n) = \{(1)\}$ für $n \neq 2$ und $Z(S_2) = S_2$.

2. Schritt: Es sei nun $\varphi : S_n \to S_n$ ein Automorphismus. Sind $g, g' \in S_n$ konjugiert, etwa $g' = xgx^{-1}$, so sind auch ihre Bilder konjugiert: $\varphi(g') = \varphi(x)\varphi(g)\varphi(x)^{-1}$. Mit demselben Argument sieht man, daß g und g' konjugiert sind, wenn ihre Bilder konjugiert sind. Das bedeutet: φ bildet Konjugationsklassen bijektiv auf Konjugationsklassen ab. Wir betrachten jetzt speziell die Konjugationsklasse T_1 aller Transpositionen. Das Bild einer Transposition hat die Ordnung 2, ist also das Produkt von k disjunkten Transpositionen. Es sei T_k die Menge aller Permutationen in S_n, die Produkte von k disjunkten Transpositionen sind, also den Zykeltyp $(1^{n-2k}2^k)$ haben. Es gibt also ein k derart, daß φ die Menge T_1 bijektiv auf T_k abbildet. Notwendigerweise müssen T_1 und T_k dazu dieselbe Mächtigkeit haben. Man sieht leicht, daß

$$|T_k| = \frac{n!}{2^k(n-2k)!k!}.$$

Das führt auf die Bedingung:

$$2^{k-1} = (k-2)!\binom{2k-2}{k}\binom{n-2}{2k-2}.$$

Eine triviale Lösung ist $k = 1$. Wir nehmen deshalb an, daß $k \geq 2$. Die linke Seite ist eine Potenz von 2. Das schließt wegen des Faktors $(k-2)!$ auf der rechten Seite alle $k \geq 5$ aus, und wegen des Faktors $\binom{2k-2}{k}$ auch $k = 4$. Im Falle $k = 2$ erhält man die Gleichung $2 = \binom{n-2}{2}$, die keine Lösung in n hat. Im Falle $k = 3$ reduziert sich die Gleichung auf $4 = \binom{4}{3}\binom{n-2}{4}$, was $n = 6$ impliziert. Damit haben wir alle möglichen Paare (n, k) gefunden, nämlich

$$(n \text{ beliebig}, k = 1) \qquad \text{oder} \qquad (n, k) = (6, 3).$$

3. Schritt. Es sei $\varphi \in \mathrm{Aut}(S_n)$ ein Automorphismus mit $\varphi(T_1) = T_1$. Allgemein gilt für Transpositionen $\tau = (ij)$ und $\tau' = (k\ell)$:

$$\mathrm{ord}(\tau\tau') = \begin{cases} 1 \\ 3 \\ 2 \end{cases}, \text{falls } |\{i,j\} \cap \{k,\ell\}| = \begin{cases} 2 \\ 1 \\ 0 \end{cases}$$

Das bedeutet, daß wir die 'Überlappung' des Wirkungsbereichs zweier Transpositionen an der Ordnung des Produkts ablesen können. Und diese Ordnung bleibt unter φ erhalten. Wir wenden diese Überlegung auf die Transpositionen $\tau_i = (i\, i+1)$, $i = 1, \ldots, n-1$, und ihre Bilder $\varphi(\tau_i)$ an. Bei geeigneter Numerierung folgt

$$\varphi(\tau_1) = (\sigma_1\sigma_2), \ldots, \varphi(\tau_{n-1}) = (\sigma_{n-1}\sigma_n)$$

eine gewisse Permutation σ. Es gilt nun: $\varphi(\tau_i) = \sigma\tau_i\sigma^{-1} = c_\sigma(\tau_i)$. Da die Gruppe S_n von $\tau_1,\ldots,\tau_{n-1}$ erzeugt wird, gilt $\varphi(\pi) = c_\sigma(\pi)$ für alle $\pi \in S_n$, also $\varphi = c_\sigma$. Damit ist gezeigt: *Jeder Automorphismus φ mit $\varphi(T_1) = T_1$ ist ein innerer Automorphismus.*

Insbesondere gilt dies für jeden Automorphismus von S_n, wenn $n \neq 6$. Damit ist gezeigt, daß $c : S_n \to \mathrm{Aut}(S_n)$ für $n \neq 6$ surjektiv ist.

4. Schritt: Es sei $n = 6$. Dann gilt $|T_1| = |T_3| = 15$ und $|T_2| = 45$. Sind $\varphi, \psi \in \mathrm{Aut}(S_6) \setminus \mathrm{Int}(S_6)$, so bilden φ und ψ die Menge T_1 bijektiv auf T_3 und umgekehrt T_3 bijektiv auf T_1 ab. Insbesondere gilt $\psi\varphi(T_1) = T_1$. Nach Schritt 3 ist $\psi\varphi$ ein innerer Automorphismus. Das bedeutet, daß $\mathrm{Out}(S_6)$ höchstens die Ordnung 2 hat. Zum Beweis der Behauptung genügt es also, einen Automorphismus anzugeben, der kein innerer Automorphismus ist.

5. Für die Konstruktion folgen wir einer Idee von Janusz und Rotman [*Outer Automorphisms of S_6, American Math. Monthly, 89,6 (1982), p. 407-410*]. Es sei Y die Menge aller 5-elementigen Untergruppen von S_5. Das sind genau die Untergruppen, die von einem 5-Zykel erzeugt werden. Je zwei solche Gruppen haben nur das Neutralelement gemeinsam. Da es genau 24 Elemente der Ordnung 5 in S_5 gibt, enthält die Menge Y genau $24/4 = 6$ Elemente. Die Gruppe S_5 operiert durch Konjugation auf Y:

$$S_5 \times Y \to Y, \quad (g, H) \mapsto gHg^{-1}.$$

Diese Wirkung ist transitiv, weil alle 5-Zykel konjugiert sind. Wenn wir die Elemente in Y willkürlich von 1 bis 6 durchnumerieren, liefert die Wirkung einen Homomorphismus $\varphi : S_5 \to S_6$. Wegen der Transitivität der Wirkung hat das Bild von φ mindestens sechs Elemente. Damit hat der Kern von φ einen Index ≥ 6. Aber die einzigen Normalteiler in S_5 sind die triviale Gruppe, A_5 und S_5 selbst. Deshalb ist φ injektiv. Das Bild $S_5' := \varphi(S_5) \subset S_6$ ist nicht zur Standardeinbettung $S_5 \subset S_6$ konjugiert: Die Wirkung von S_5 auf der Menge $\{1,\ldots,6\}$ hat 6 als Fixpunkt, und jede konjugierte Untergruppe aS_5a^{-1} hat $a(6)$ als Fixpunkt. Dagegen ist die Wirkung von S_5' transitiv und damit fixpunktfrei.

Die Gruppe S_6 operiert durch Linksmultiplikation auf der 6-elementigen Menge der Nebenklassen S_6/S_5', und zwar offensichtlich transitiv und mit Standgruppen der Form $aS_5'a^{-1}$. Wir wählen eine Numerierung S_6/S_5' mit der Eigenschaft, daß die Nebenklasse $[S_5']$ die Nummer 6 erhält. Dies liefert einen Homomorphismus $\psi : S_6 \to S_6$. Der Kern hat einen Index ≥ 6, und ist daher trivial, weil S_6 keine Normalteiler außer der trivialen Gruppe, A_6 und S_6 hat. Folglich ist ψ ein Automorphismus.

Wir zeigen, daß ψ kein innerer Automorphismus ist. Das Urbild $\psi^{-1}(S_5)$ ist nach Konstruktion der Stabilisator von $[S_5']$, also S_5'. Wäre ψ ein innerer Automorphismus, müßte das Urbild dagegen konjugiert zu S_5 sein. Nach Konstruktion von S_5' ist dies nicht der Fall. □

Bemerkung 2.12 — Das reguläre Dodekaeder enthält 5 den Ecken einbeschriebene Würfel und 6 Diagonalen durch die Eckpunkte. Diese werden von allen eigentlichen

Symmetrien des Dodekaeders permutiert. Dies führt zunächst zu einer Identifizierung der Symmetriegruppe des Dodekaeders mit der Gruppe A_5 und im nächsten Schritt zu einer Wirkung von A_5 auf der Menge der Diagonalen und somit zu einem 'exotischen' Homomorphismus $A_5 \to S_6$. Tatsächlich liegt das Bild schon in A_6, weil die Einschränkung der Signatur $S_6 \to \{\pm 1\}$ auf das Bild A_5' von A_5 trivial sein muß. Ähnlich wie oben liefert die Wirkung von A_6 auf A_6/A_5' einen äußeren Automorphismus $A_6 \to A_6$. Für die folgende Frage habe ich keine Lösung: Wie kann man diesen Automorphismus auf einfache (!) geometrische Weise zu einem Automorphismus von S_6 erweitern? Kurzum, kann man den äußeren Automorphismus von S_6 aus der Geometrie des Dodekaeders erklären?

Lektürehinweis: Howard, Millson, Snowden, Vakil: *A description of the outer automorphism of S_6 and the invariants of six points in projective space*.

2.4 Einfache Gruppen

Definition 2.13 — Eine Gruppe G ist einfach, wenn $G \neq \{e\}$ und wenn $\{e\}$ und G die einzigen Normalteiler in G sind.

Beispiel 2.14 — Eine abelsche Gruppe ist genau dann einfach, wenn sie zyklisch von Primzahlordnung ist. Denn ist G eine einfache abelsche Gruppe und $g \in G$ ein nichttriviales Element, dann erzeugt g einen Normalteiler in G, also ganz G. Hätte g unendliche Ordnung, so wäre $\langle g^2 \rangle$ ein echter Normalteiler. Folglich ist G endlich, $G \cong \mathbb{Z}/n$. Für jeden echten Teiler $d|n$ gibt es eine Untergruppe $H \subset \mathbb{Z}/n$, $H \cong \mathbb{Z}/d$. Wenn also G einfach sein soll, darf n keinen nichttrivialen Teiler haben. Ist umgekehrt p eine Primzahl, so ist jedes $x \neq 0$ im Körper $\mathbb{Z}/p$ invertierbar und erzeugt additiv die ganze Gruppe.

Satz 2.15 — *Für $n \geq 5$ ist A_n einfach.*

Beweis. Es sei $n \geq 5$ und $N \subset A_n$ ein Normalteiler $\neq \{(1)\}$. Unter allen Elementen in $N \setminus \{(1)\}$ besitze π die meisten Fixpunkte auf der Menge $\{1, \ldots, n\}$.

Angenommen, π enthält einen Zykel der Länge $m \geq 4$, ohne Einschränkung etwa den Zykel $z = (12 \cdots m)$. Dann enthält N auch das Element $(123)\pi(123)^{-1}\pi^{-1} = (124)$, im Widerspruch zur Maximalität von π.

Angenommen, π enthält einen Dreierzykel und einen dazu disjunkten Zykel der Länge ≥ 2 etwa $\pi = (123)(45\ldots)\ldots$. Dann enthält N auch $(124)\pi(421)\pi^{-1} = (12534)$. Wenn $\pi = (123)(456)\ldots$ oder $(123)(34)(56)\ldots$, so widerspricht (12534) der Maximalität von π. Falls $\pi = (123)(45)$, so ist (12534) selbst maximal, im Widerspruch zum vorigen Fall.

Angenommen, π enthält drei disjunkte Transpositionen, etwa $\pi = (12)(34)(56)\cdots$. Dann enthält N auch das Element $(123)\pi(321)\pi^{-1} = (13)(24)$, Widerspruch.

Angenommen, π enthält ein Produkt aus zwei disjunkten Transpositionen, etwa $\pi = (12)(34)$. Dann enthält N auch $(125)\pi(521)\pi^{-1} = (152)$, Widerspruch.

Es bleibt nur die Möglichkeit, daß π ein Dreierzykel ist, da N keine Transpositionen enthalten kann. Es sei ohne Einschränkung $\pi = (123)$. Ist nun π' irgendein Dreierzykel in A_n, so gibt es ein $\sigma \in S_n$ mit $\pi' = \sigma\pi\sigma^{-1}$. Es gilt dann aber auch $\pi' = (\sigma(45))\pi(\sigma(45))^{-1}$, und entweder σ oder $\sigma(45)$ liegt in A_n. Folglich enthält N mit π auch alle anderen Dreierzykel, und diese erzeugen A_n. □

Bemerkung 2.16 — Die endlichen einfachen Gruppen sind vollständig klassifiziert. Es gibt, wie wir gesehen haben,

- Die zyklischen Gruppen $\mathbb{Z}/p$, p prim.
- Die alternierenden Gruppen A_n, $n \geq 5$.

Darüberhinaus gibt es 16 Serien von Gruppen vom sogenannten Lie-Typ. Schließlich gibt es noch 26 endliche einfache Gruppen, die nicht in Serien auftreten und deshalb sporadische Gruppen genannt werden. Die größte unter den sporadischen Gruppen heißt Monstergruppe M. Sie wurde von Fischer und Griess 1973 vorausgesagt und 1982 von Griess konstruiert. Sie hat

$$|M| = 2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71 \tag{2.1}$$

$$= 808017424794512875886459904961710757005754368000000000 \tag{2.2}$$

Elemente. Es gibt merkwürdige Beziehungen zwischen der Monstergruppe und gewissen Funktionen, die in der Theorie der Modulformen auftauchen. Diese Beziehungen erschienen bei ihrem ersten Auftreten so verrückt, daß sie seither unter dem Schlagwort Mondschein (moonshine) bekannt sind. Für die Klärung vieler damit verbundener Fragen erhielt Borcherds 1998 die Fields-Medaille.

2.5 Auflösbare Gruppen

Definition 2.17 — Es sei G eine Gruppe. Eine Folge $(G_0, \ldots, G_n)$ von Untergruppen in G ist eine Normalreihe, wenn $G_0 = G$, $G_n = \{e\}$ und wenn für jedes $i = 1, \ldots, n$ die Gruppe G_i ein echter Normalteiler in G_{i-1} ist. Die Gruppen G_{i-1}/G_i, $i = 1, \ldots, n$, heißen die Faktoren der Normalreihe.

Wir notieren Normalreihen in der Form

$$\{e\} = G_n \lhd G_{n-1} \lhd \ldots \lhd G_0 = G.$$

Beispiele 2.18 — Es bezeichne S_n die symmetrische Gruppe. Die alternierende Gruppe A_n ist der Kern des alternierenden Charakters $\mathrm{sgn} : S_n \to \{\pm 1\}$ und deshalb ein Normalteiler. $\{(1)\} \lhd A_n \lhd S_n$ ist eine Normalreihe. Für $n = 4$ besitzt A_n den Normalteiler $V_4 = \{(1), (12)(34), (13)(24), (14)(23)\}$, und man erhält die Normalreihe $\{(1)\} \lhd V_4 \lhd A_4 \lhd S_4$. Daß V_4 ein Normalteiler ist, sieht man entweder durch direktes Nachrechnen, oder aus der folgenden Überlegung: Zwei Permutationen π und π'

sind genau in S_n konjugiert, wenn sie denselben Zykeltyp haben. Eine Untergruppe $H \subset S_n$ ist also genau dann ein Normalteiler, wenn H mit jeder Permutation π auch aller Permutationen desselben Zykeltyps enthält. Das ist bei $V_4 \subset S_4$ offensichtlich der Fall. Deshalb ist V_4 ein Normalteiler in S_4 und deshalb erst recht in A_4.

Definition 2.19 — Eine Gruppe heißt auflösbar, wenn es eine Normalreihe mit abelschen Faktoren gibt.

Es sei G eine Gruppe mit multiplikativ geschriebener Gruppenstruktur $(a, b) \mapsto ab$. Der Kommutator zweier Elemente $a, b \in G$ ist $[a, b] = aba^{-1}b^{-1}$. Aus der Definition folgt sofort:

$$[a, b]^{-1} = [b, a] \quad \text{und} \quad c[a, b]c^{-1} = [cac^{-1}, cbc^{-1}].$$

Deshalb ist die Menge $[G, G] \subset G$ aller endlichen Produkte von Kommutatoren eine Untergruppe von G und sogar ein Normalteiler. Der folgende Satz ist einfach zu beweisen:

Satz 2.20 — *Es sei G eine Gruppe. Die Faktorgruppe $G^{ab} = G/[G, G]$ ist abelsch. Jeder Gruppenhomomorphismus $f : G \to A$ in eine abelsche Gruppe A faktorisiert über $\pi : G \to G^{ab}$ und einen Homomorphismus $f^{ab} : G^{ab} \to A$.*

In diesem Sinne ist G^{ab} die größte abelsche Faktorgruppe von G.

Definition 2.21 — $\pi : G \to G/[G, G] = G^{ab}$ heißt Abelianisierung von G. Eine Gruppe G ist vollkommen oder perfekt, wenn $[G, G] = G$.

Zum Beispiel ist jede einfache Gruppe, die nicht abelsch ist, perfekt.

Es sei G eine beliebige Gruppe. Dann können wir rekursiv die folgenden Untergruppen definieren: $K^0(G) = G$, $K^1(G) = [G, G]$ und $K^{n+1}(G) = [K^n(G), K^n(G)]$. Nach Konstruktion ist $K^{n+1}(G)$ ein Normalteiler in $K^n(G)$, und die Faktoren der absteigenden Reihe

$$G = K^0(G) \rhd K^1(G) \rhd K^2(G) \rhd \dots$$

sind abelsch.

Satz 2.22 — *Eine Gruppe ist genau dann auflösbar, wenn $K^n G = \{e\}$ für ein $n \in \mathbb{N}$.*

Beweis. Wenn $K^n(G) = \{e\}$ für ein n, dann ist $K^0(G) \rhd \dots \rhd K^n(G)$ eine Normalreihe mit abelschen Faktoren, also G auflösbar. Wir betrachten die umgekehrte Richtung:

Angenommen, $G = G_0 \rhd G_1 \rhd G_2 \rhd \dots \rhd G_m = \{e\}$ ist eine Normalreihe mit abelschen Faktoren. Wir zeigen induktiv, daß $K^n(G) \subset G_n$ für alle $n = 0, \dots, m$. Für $n = 0$ ist nichts zu zeigen. Wenn die Behauptung für ein $n \geq 0$ schon gezeigt ist, schließen wir so: Das Bild der zusammengesetzten Abbildung $K^n(G) \to G_n \to G_n/G_{n+1}$ ist abelsch. Deshalb gilt $K^{n+1}(G) = [K^n(G), K^n(G)] \subset [G_n, G_n] \subset G_{n+1}$, was zu zeigen war. Insgesamt folgt $K^m(G) \subset G_m = \{e\}$. □

Folgerung 2.23 — *S_n ist auflösbar* $\Leftrightarrow$ $n \leq 4$.

Beweis. Wir haben für $n \leq 4$ Normalreihen mit abelschen Faktoren angegeben. Für $n \geq 5$ ist $[S_n, S_n] = A_n$, aber A_n ist perfekt. □

Lemma 2.24 — *Es sei $G = G_0 \rhd G_1 \rhd \ldots \rhd G_n = \{e\}$ eine Normalreihe. Ferner sei für einen index k ein Normalteiler $\bar{N} \lhd \bar{G} := G_k/G_{k+1}$ gegeben. Ist $p : G_k \to \bar{G}$ die kanonische Projektion, so ist $N := p^{-1}(\bar{N})$ ein Normalteiler in G_k und G_{k+1} ein Normalteiler in N. Insbesondere ist $G_0 \rhd \ldots \rhd G_k \rhd N \rhd G_{k+1} \rhd \ldots \rhd G_n = \{e\}$ eine Normalreihe. Die Faktoren dieser Reihe sind*

$$G_0/G_1, \ldots, G_k/N \cong \bar{G}/\bar{N}, N/G_{k+1} \cong \bar{N}, \ldots, G_{n-1}/G_n.$$

Beweis. Für $n \in N$ und $g \in G_k$ folgt: $p(gng^{-1}) = p(g)p(n)p(g)^{-1} = p(n) \in \bar{N}$, weil $\bar{N}$ ein Normalteiler ist. Insbesondere ist $gng^{-1} \in p^{-1}(\bar{N}) = N$, also N ein Normalteiler in G_k. Offensichtlich gilt $G_{k+1} = \ker(p|_N : N \to \bar{N})$. Mit dem Homomorphiesatz folgt $N/G_{k+1} \cong \bar{N}$. Ähnlich ist N der Kern des zusammengesetzten Homomorphismus $G_k \to \bar{G} \to \bar{G}/\bar{N}$. Wieder folgt mit dem Homomorphiesatz, daß $G_k/N \cong \bar{G}/\bar{N}$. □

Das Lemma erlaubt es, eine gegebene Normalreihe zu verfeinern, wenn man in einem der Faktoren einen Normalteiler findet. Zum Beispiel ist $S_4 \rhd V_4 \rhd \langle(1)\rangle$ eine Normalreihe mit den Faktoren S_3 bzw. V_4. in beiden Faktoren gibt es nichttriviale Normalteiler: $A_3 \subset S_3$ und $\langle(12)(34)\rangle V_4$. Das Urbild von A_3 unter $S_4 \to S_3$ ist A_4. Die an beiden Stellen verfeinerte Normalreihe ist die früher betrachtete Reihe.

$$S_4 \rhd A_4 \rhd V_4 \rhd \langle(12)(34)\rangle \rhd \langle(1)\rangle.$$

Folgerung 2.25 — *1. Jede endliche Gruppe besitzt eine Normalreihe, deren Faktoren einfache Gruppen sind.*
2. Eine endliche Gruppe ist genau dann auflösbar, wenn es eine Normalreihe gibt, deren Faktoren zyklische Gruppen von Primzahlordnung sind.

Beweis. 1. Es sei G eine endliche Gruppe. Eine Normalreihe ist höchstens so lang wie die Gruppenordnung von G. Insbesondere gibt es Normalreihen von maximaler Länge. Wäre in einer solchen Reihe ein Faktor nicht einfach, so könnte man mit dem Verfahren des Lemmas die gegebene Normalreihe um ein Glied verlängern, im Gegensatz zu ihrer angenommenen Maximalität.
2. Wenn es eine Normalreihe von G mit zyklischen Faktoren gibt, so ist G offensichtlich auflösbar. Ist G umgekehrt auflösbar, so gibt es eine Reihe mit abelschen Faktoren. Wir können wie im Teil 1 eine Normalreihe mit abelschen Faktoren von maximaler Länge wählen. Wäre einer der Faktoren H nicht zyklisch von Primzahlordnung, so

gäbe es einen echten Normalteiler in diesem Faktor. Die entsprechend verlängerte Normalreihe hätte immer noch abelsche Faktoren, denn die neu hinzugekommenen Faktoren sind eine Untergruppe bzw. eine Faktorgruppe von H und daher wieder abelsch. Wieder widerspricht dies der angenommenen Maximalität. □

Satz 2.26 — *Es sei G eine Gruppe und N ein Normalteiler. Dann gilt:*

$$G \text{ ist auflösbar} \quad \Leftrightarrow \quad N \text{ und } G/N \text{ sind auflösbar.}$$

Beweis. Es seien zunächst N und G/N auflösbar. Wir wählen Normalreihen mit abelschen Faktoren für beide Gruppen. Nach dem schon mehrfach benutzen Verfahren können wir anhand der Normalteiler in N und G/N die Normalreihe $G \rhd N \rhd \{e\}$ so verfeinern, daß die Faktoren der verfeinerten Reihe von G isomorph zu den Faktoren der Reihen von N bzw. G/N sind. Diese sind abelsch nach Voraussetzung. Damit haben wir eine Normalreihe für G mit abelschen Faktoren gefunden.

Es sei umgekehrt $G = G_0 \lhd \dots G_n = \{e\}$ eine Normalreihe von G mit abelschen Faktoren. Es sei $N_i = N \cap G_i$ und $\bar{G}_i$ das Bild von G_i in $\bar{G} = G/N$ unter der Projektion $\pi : G \to \bar{G}$. Dann gilt: N_{i+1} ist der Kern des zusammengesetzten Homomorphismus $N_i \to G_i \to G_i/G_{i+1}$ und deshalb ein Normalteiler. Außerdem ist N_i/N_{i+1} isomorph zum Bild von N_i in G_i/G_{i+1} und deshalb abelsch. Ähnlich ist $\bar{G}_{i+1}$ ein Normalteiler in $\bar{G}_i$. Nach Konstruktion ist die Komposition $G_{i+1} \to G_i \to \bar{G}_i \to \bar{G}_i/\bar{G}_{i+1}$ die triviale Abbildung. Nach dem Homomorphiesatz gibt es einen wohldefinierten Homomorphismus $G_i/G_{i+1} \to \bar{G}_i/\bar{G}_{i+1}$, und dieser ist surjektiv. Damit erweist sich auch $\bar{G}_i/\bar{G}_{i+1}$ als Faktorgruppe einer abelschen Gruppe als abelsch. Das zeigt: Die Normalreihen (N_i) von N und $(\bar{G}_i)$ von $\bar{G}$ haben abelsche Faktoren. □

2.6 p-Gruppen

Definition 2.27 — Es sei p eine Primzahl. Eine endliche Gruppe G ist eine p-Gruppe, wenn $|G| = p^n$ für ein $n \in \mathbb{N}$.

Die zentrale Beobachtung, die der Ausgangspunkt für viele Strukturaussagen über p-Gruppen ist, ist das folgende einfache Lemma:

Lemma 2.28 — *Es sei G eine p-Gruppe, die auf einer endlichen Menge X wirkt. Dann ist $|X| \equiv |X^G| \bmod p$, wenn X^G die Fixpunktemenge der Wirkung bezeichnet.*

Beweis. Es seien $B_i \subset X$, $i = 1, \dots, n$, die Bahnen der G-Wirkung und G_i die Standgruppen von ausgewählten Elementen $b_i \in B_i$. Dann gelten die Bahnengleichungen

$$|X| = \sum_i |B_i| \quad \text{und} \quad |B_i| = |G|/|G_i|.$$

Fixpunkte entsprechen bijektiv den Bahnen der Länge 1. Für alle anderen Bahnen ist $|B_i|$ ein nichttrivialer Teiler von $|G|$, also selbst durch p teilbar. Daraus folgt die Behauptung. □

Satz 2.29 — *Es sei G eine p-Gruppe. Dann ist das Zentrum von G nicht trivial. Insbesondere gibt es ein zentrales Element der Ordnung p.*

Beweis. Wir wenden Lemma 2.28 auf die folgende Situation an: Die Gruppe G wirke auf sich durch Konjugation. Ein Element $g \in G$ ist genau dann ein Fixpunkt, wenn es mit allen Elementen in G vertauscht, also im Zentrum liegt. Deshalb gilt $|Z(G)| \equiv |G| \equiv 0 \mod p$. Da das Zentrum aber mindestens das Neutralelement enthält, ist $|Z(G)| \geq p$. Ist $x \in Z(G)$ ein beliebiges nichttriviales Element, so ist seine Ordnung p^m für ein $m \geq 1$, und $y = x^{p^{m-1}}$ ist ein zentrales Element der Ordnung p. □

Satz 2.30 — *Es sei G eine p-Gruppe. Dann gibt es eine Folge von Untergruppen $G_0 = \{e\} < G_1 < \cdots < G_n = G$ der Ordnung $|G_i| = p^i$ mit der Eigenschaft, daß G_i ein Normalteiler in G ist. Insbesondere sind p-Gruppen auflösbar.*

Beweis. Es sei $x \in Z(G)$ ein Element der Ordnung p. Die von x erzeugte zyklische Untergruppe $G_1 = \langle x \rangle$ ist zentral und daher ein Normalteiler in G. Die Faktorgruppe G/G_1 ist ebenfalls eine p-Gruppe. Durch Induktion nach der Ordnung der Gruppe schließen wir auf die Existenz von Normalteilern $\{1\} < \overline{G}_2 < \ldots < \overline{G}_n = G/G_1$ mit $|\overline{G}_k| = p^{k-1}$. Es sei G_k das Urbild von $\overline{G}_k$ unter der Projektion $G \to G/G_1$. Als Urbilder von Normalteilern sind die G_k selbst Normalteiler, und ihre Ordnung ist $|G_k| = |G_1| \cdot |\overline{G}_k| = p^k$. Schließlich haben alle Faktoren G_k/G_{k+1} die Ordnung p und sind deshalb zyklisch. □

Definition 2.31 — Es sei G eine endliche Gruppe, p eine Primzahl und m die Multiplizität von p in der Ordnung von G. Eine p-Untergruppe $S \subset G$ ist eine p-Sylowuntergruppe, wenn $|S| = p^m$.

30.4.2008

Satz 2.32 *(Sylow[9])* — *Es sei G eine endliche Gruppe und p eine Primzahl.*

1. *G besitzt p-Sylowuntergruppen. Für ihre Anzahl s_p gelten die Beziehungen $s_p \mid |G|$ und $s_p \equiv 1 \mod p$.*
2. *Jede p-Untergruppe von G liegt in einer p-Sylowuntergruppe.*
3. *Alle p-Sylowuntergruppen von G sind konjugiert.*

[9] Ludwig Sylow ⋆1832 †1918

Beweis. 1. Wir variieren den Beweisgedanken von Lemma 2.28: Es sei $|G| = n = p^m u$ mit $p \nmid u$. Wir betrachten die Menge X aller p^n-elementigen Teilmengen von G. Die Gruppe G operiere auf X durch Linkstranslation, d.h. für $Y = \{y_1, \ldots, y_{p^m}\} \in X$ und $g \in G$ ist $gY = \{gy_1, \ldots, gy_{p^m}\}$.

Es sei nun $H = G_Y$ die Standgruppe von Y. Das bedeutet, daß $hY = Y$ für alle $h \in H$. Insbesondere erhalten wir eine neue Gruppenwirkung $H \times Y \to Y, (h, y) \mapsto hy$. Diese Wirkung ist mit der Wirkung von G auf X nicht zu verwechseln! Offensichtlich ist die Wirkung von H auf Y frei, und Y zerfällt in eine disjunkte Vereinigung von Rechtsnebenklassen von H. Aber das bedeutet insbesondere: Die Ordnung von H ist ein Teiler der Mächtigkeit von Y, d.h. H ist eine p-Gruppe der Ordnung $p^{m'}$ mit $m' \leq m$. Und H ist genau dann eine p-Sylowgruppe, wenn Y aus einer einzigen H-Bahn besteht, also die Form $Y = Hy$ hat.

Gehen wir wieder zur Wirkung von G auf X über, so bedeutet dies: Die Länge der Bahn von Y ist $|G|/|H| = up^{m-m'}$, also genau dann *nicht* durch p teilbar, wenn $Y = Hy$ für eine p-Sylowuntergruppe. Es sei $X_0 \subset X$ die Menge aller Teilmengen der Form $Y = Hy$ mit einer p-Sylowuntergruppe H und $y \in G$. Aus der Bahnengleichung folgt:

$$|X| \equiv |X_0| \bmod p.$$

Nun gilt:

$$|X| = \binom{p^n u}{p^n} \equiv u \not\equiv 0 \bmod p.$$

Da u teilerfremd zu p ist, ist X_0 nicht leer, d.h. es gibt p-Sylowuntergruppen. Weiter gibt es zu jeder p-Sylowuntergruppe H genau u verschiedene Nebenklassen Hy in X_0. Andererseits ist H als Standgruppe der Nebenklasse Hy eindeutig bestimmt, d.h. ein Elemente aus X_0 gehört immer nur zu genau einer p-Sylowuntergruppe. Das zeigt: $|X_0| = us_p$. Es folgt: $u \equiv us_p \bmod p$, also $s_p \equiv 1 \bmod p$.

2. Es sei $S < G$ eine p-Sylowuntergruppe und $H < G$ eine beliebige p-Untergruppe. Wir wenden Lemma 2.28 direkt auf die Wirkung von H auf der Menge G/S durch Linksmultiplikation an. Da

$$|G/S| = |G|/|S| = u \not\equiv 0 \bmod p,$$

gibt es einen Fixpunkt $yS \in G/S$, d.h. eine Nebenklasse yS mit $HyS = yS$. Aber das bedeutet, daß $y^{-1}Hy \subset S$ bzw. $H \subset ySy^{-1}$. Demnach liegt H in der p-Sylowuntergruppe ySy^{-1}, was zu zeigen war.

3. Dieses Argument liefert in dem Spezialfall, daß H selbst schon eine p-Sylowuntergruppe ist, eine Inklusion $H \subset ySy^{-1}$. Da beide Gruppen p-Sylowuntergruppen sind, sind sie gleichmächtig. Die Inklusionsbeziehung ist daher schon eine Gleichheit. Folglich sind je zwei p-Sylowuntergruppen konjugiert.

4. Schließlich betrachten wir die Wirkung von G auf der Menge X_1 der p-Sylowuntergruppen durch Konjugation: $(g, S) \mapsto gSg^{-1}$. Wir haben gerade gesehen, daß alle p-Sylowuntergruppen konjugiert sind. Es gibt deshalb nur eine Bahn. Bezeichnet

K die Standgruppe von $S \in X_1$, so folgt: $|G| = |K| \cdot |X_1|$, also ist $s_p = |X_1|$ ein Teiler von $|G|$. □

Im Beweis haben wir die folgende Kongruenz benutzt: Für jede Primzahl p und jede zu p teilerfremde natürliche Zahl u gilt

$$\binom{up^m}{p^m} \equiv u \bmod p.$$

Tatsächlich gilt eine allgemeinere Aussage:

Lemma 2.33 — *Es sei p eine Primzahl, $u \in \mathbb{N}$ und $0 \leq k \leq n$. Dann gilt:*

$$\binom{u}{k} \equiv \binom{up^m}{kp^m} \bmod p$$

Beweis. Im Polynomring $\mathbb{F}_p[x, y]$ gilt $(x + y)^p = x^p + y^p$. Induktiv folgt $(x + y)^{p^m} = x^{p^m} + y^{p^m}$ und schließlich

$$(x + y)^{up^m} = (x^{p^m} + y^{p^m})^u.$$

Indem man auf beiden Seiten nach der binomischen Formel expandiert und die Koeffizienten vergleicht, findet man die behauptete Formel. □

Aufgaben zur Gruppentheorie

Aufgabe 2.1 — Es sei G eine Gruppe und $S \subset G$ eine Teilmenge und X die Menge aller Untergruppen von G, die S enthalten. Zeigen Sie:

1. X ist nicht leer.
2. $\langle S \rangle := \bigcap_{H \in X} H$ ist ein Element in X.

$\langle S \rangle$ heißt die von S erzeugte Untergruppe von G, und G heißt von S erzeugt, wenn $G = \langle S \rangle$.

Aufgabe 2.2 — Es sei G eine Gruppe und $S \subset G$ eine Teilmenge. Es sei H die Menge aller Produkt $s_1 \cdots s_n$ mit $n \in \mathbb{N}_0$ und $s_i \in S$ oder $s_i^{-1} \in S$. Zeigen Sie, daß $H = \langle S \rangle$.

Aufgabe 2.3 — Es sei $n \in \mathbb{N}$ gegeben. Es bezeichne $s = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right) \in \mathrm{O}(2)$ die Spiegelung an der x-Achse und $d = \left(\begin{smallmatrix} \cos(2\pi/n) & -\sin(2\pi/n) \\ \sin(2\pi/n) & \cos(2\pi/n) \end{smallmatrix}\right) \in \mathrm{O}(2)$ die Drehung um den Winkel $2\pi/n$.

1. Die Untergruppe $C_n := \langle d \rangle$ in der orthogonalen Gruppe $\mathrm{O}(2)$ ist zyklisch mit Ordnung n, d.h. $C_n \cong \mathbb{Z}/n$.
2. Die Untergruppe $D_n := \langle s, d \rangle$ heißt Diedergruppe. Man zeige, daß $|D_n| = 2n$.

3. Man bestimme alle Konjugationsklassen von D_n. (Vorsicht: Unterscheide die Fälle n gerade und n ungerade.)

4. Man bestimme alle Untergruppen und Normalteiler in D_n.

Es sei $H < G$ eine Untergruppe. Das Verhältnis $[G : H] := |G/H| = |G|/|H|$ wird als Index von H in G bezeichnet.

Aufgabe 2.4 — Jede Untergruppe $H < G$ vom Index $[G : H] = 2$ ist ein Normalteiler.

Aufgabe 2.5 — Es sei G eine Gruppe, $N \lhd G$ ein Normalteiler und $H < G$ eine Untergruppe.

1. $N \cap H$ ist ein Normalteiler in H.

2. Die Menge $NH = \{nh \mid n \in N, h \in H\}$ ist eine Untergruppe in G.

3. N ist ein Normalteiler in NH.

4. Die Abbildung $NH \to NH/N$ hat den Kern $N \cap H$.

5. Die Abbildung $H/(N \cap H) \to NH/N$, $h \bmod (N \cap h) \mapsto h \bmod N$, ist ein Isomorphismus (Erster Isomorphiesatz).

6. Ist auch H ein Normalteiler, so ist $N \cap H$ ein Normalteiler in G.

Aufgabe 2.6 — Es sei $m : G \times X \to X$ eine Linkswirkung. Dann ist $q(x, g) := m(g^{-1}, x)$ eine Rechtwirkung von G auf X.

Aufgabe 2.7 — Es sei $G \times X \to X$ eine Gruppenwirkung. Liegen x und y in derselben Bahn, so sind ihre Standgruppen $G_x, G_y < G$ konjugierte Untergruppen. Wie hängen G_{gy} und G_y zusammen?

Aufgabe 2.8 — Es sei p eine Partition von n. Man bestimme die Mächtigkeit der Konjugationsklasse aller Permutationen vom Zykeltpy p.

Aufgabe 2.9 — Es sei G eine Gruppe und $g \in G$. Der Zentralisator von g in G ist die Menge $Z_G(g) = \{h \in G \mid hg = gh\}$. Man zeige:

1. $Z_G(g)$ ist eine Untergruppe von G.

2. $Z_G(x)$ ist die Standgruppe von x bezüglich der Wirkung $G \times G \to G$, $(g, x) \mapsto gxg^{-1}$.

3. Es sei speziell $G = S_n$ und $\pi \in S_n$ ein Permutation. Man drücke die Ordnung von $Z_{S_n}(\pi)$ durch den Zykeltyp von π aus.

Aufgabe 2.10 — Es seien N und H Gruppen und $\alpha : H \to \mathrm{Aut}(N)$ ein Gruppenhomomorphismus. Das semidirekte Produkt $N \rtimes_\alpha H$ ist die Menge $N \times H$ mit der folgenden Gruppenstruktur:

$$(n, h) \cdot (n', h') := (n\alpha(h)(n'), hh').$$

Zeigen Sie: 1. Die angegebene Verküpfung definiert tatsächlich eine Gruppenstruktur.
2. Die Abbildungen $N \to N \rtimes_\alpha H$, $n \mapsto (n, e)$, und $H \to N \rtimes_\alpha H$, $h \mapsto (e, h)$, sind injektive Gruppenhomomorphismen.
3. Identifiziert man N und H mit ihren Bildern in $N \rtimes H$, so gilt: N ist ein Normalteiler in $N \rtimes H$, und die Inklusion von H induziert einen Isomorphismus $H \cong (N \rtimes H)/N$.
4. Für $n \in N$ und $h \in H$ gilt: $hnh^{-1} = \alpha(h)(n)$.
5. Es sei $\alpha : \mathbb{Z}/2 \to \mathrm{Aut}(\mathbb{Z}/3)$ ein Homomophismus. Dann gilt $\mathbb{Z}/3 \rtimes_\alpha \mathbb{Z}/2 \cong \mathbb{Z}/6$ oder S_3 je nachdem, ob α die triviale Abbildung ist oder nicht.

Aufgabe 2.11 — Es seien $s_0, s_1 : \mathbb{R} \to \mathbb{R}$ die Punktspiegelungen an den Punkten 0 bzw. 1. Zeigen Sie: Die von s_0 und s_1 erzeugte Gruppe G ist isomorph zu $\mathbb{Z} \rtimes_\alpha \mathbb{Z}/2$, wobei $\alpha : \mathbb{Z}/2 \to \mathrm{Aut}(\mathbb{Z})$ den eindeutigen Gruppenisomorphismus bezeichne

Aufgabe 2.12 — Es sei V ein K-Vektorraum. Die Gruppe $\mathrm{GL}(V)$ der K-linearen Automorphismen von V ist eine Untergruppe in der Gruppe $\mathrm{Aut}(V)$ der Automorphismen von V als abelsche Gruppe. Es sei $\alpha : \mathrm{GL}(V) \to \mathrm{Aut}(V)$ die Inklusionsabbildung. Die Gruppe $\mathrm{Aff}(V) := V \rtimes_\alpha \mathrm{GL}(V)$ heißt *affine Gruppe* von V. Man zeige, daß $\mathrm{Aff}(V) \times V \to V$, $((b, A), v) \mapsto Av + b$, eine Gruppenwirkung von $\mathrm{Aff}(V)$ auf V ist.

Aufgabe 2.13 — Es sei K ein Körper und $G \subset \mathrm{GL}_n(K)$ die Untergruppe der oberen Dreiecksmatrizen. Zeigen Sie, daß G auflösbar ist.

Aufgabe 2.14 — 1. Für alle $n \geq 2$ gilt $[S_n, S_n] = A_n$.
2. $A_2 = \{(1)\}$, $A_3 \cong \mathbb{Z}/3$, also insbesondere $[A_3, A_3] = \{(1)\}$.
3. $[A_4, A_4] = V_4 := \{(12)(34), (13)(24), (14)(23)\}$, und $[V_4, V_4] = \{(1)\}$.
4. Für $n \geq 5$ ist $[A_n, A_n] = A_n$. [Ohne Rückgriff auf die in der Vorlesung bewiesene Einfachheit von A_n.]

Es sei K ein Körper. $\mathrm{GL}_n(K)$ bezeichnet die Gruppe der invertierbaren $n \times n$-Matrizen, $\mathrm{SL}_n(K)$ die Untergruppe der Matrizen mit Determinante 1, und Z_n die Untergruppe der Vielfachen der Einheitsmatrix. Man sieht leicht, daß Z_n ein Normalteiler ist. Wir definieren $\mathrm{PSL}_n(K) := \mathrm{SL}_n(K)/(Z_n \cap \mathrm{SL}_n(K))$ und $\mathrm{PGL}_n(K) := \mathrm{GL}_n(K)/Z_n$.

Aufgabe 2.15 — Es sei $\mathbb{F}_q$ ein[10] endlicher Körper mit q Elementen. Bestimmen Sie die Ordnungen der endlichen Gruppen $\mathrm{GL}_n(\mathbb{F}_q)$, $\mathrm{SL}_n(\mathbb{F}_q)$, $\mathrm{PGL}_n(\mathbb{F}_q)$ and $\mathrm{PSL}_n(\mathbb{F}_q)$.

[10] Wir werden im Laufe der Vorlesung sehen, daß es bis auf Isomorphie genau einen endlichen Körper mit q Elementen gibt, wenn q eine Primzahlpotenz ist.

Aufgabe 2.16 — Es sei K ein Körper und $n \in \mathbb{N}$.
1. Falls $(K, n) \neq (\mathbb{F}_2, 2)$, gilt $[\mathrm{GL}_n(K), \mathrm{GL}_n(K)] = \mathrm{SL}_n(K)$.
2. Falls $(K, n) \neq (\mathbb{F}_2, 2), (\mathbb{F}_2, 3)$, gilt $[\mathrm{SL}_n(K), \mathrm{SL}_n(K)] = \mathrm{SL}_n(K)$
[Elementarmatrizen $E_{ij}(\lambda)$ mit $E_{ij}(\lambda)_{mn} = \delta_{mn} + \lambda\delta_{im}\delta_{jn}$ betrachten.]
3. Was geschieht in den Ausnahmefällen?

Aufgabe 2.17 — Wir betrachten in $\mathrm{GL}_2(\mathbb{C})$ die Untergruppe Q_8, die von den Matrizen

$$I := \left(\begin{smallmatrix} i & 0 \\ 0 & -i \end{smallmatrix}\right) \quad \text{und} \quad J := \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$$

erzeugt wird. Zeigen Sie, daß Q_8 eine endliche Gruppe der Ordnung 8 ist. Q_8 heißt Quaternionengruppe. Bestimmen Sie alle Untergruppen und Normalteiler in Q_8.

Aufgabe 2.18 — Es gibt bis auf Isomorphie genau fünf Gruppen der Ordnung 8, nämlich

$$\mathbb{Z}/8, \quad \mathbb{Z}/4 \times \mathbb{Z}/2, \quad \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2, \quad D_4, \quad Q_8.$$

Dabei ist D_4 die Diedergruppe, die von der Spiegelung $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ und der Drehung $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ erzeugt wird, und Q_8 ist die Quaternionengruppe. Zu welcher dieser Gruppen ist die Gruppe

$$N = \left\{ \left(\begin{smallmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{smallmatrix}\right) \right\} \subset \mathrm{GL}_3(\mathbb{F}_2)$$

isomorph?

Aufgabe 2.19 — Es sei G eine endliche Gruppe mit $|G| = pq$ mit Primzahlen $p > q$. Zeigen Sie:

1. Es gibt genau eine p-Sylowuntergruppe N.
2. Ist H eine q-Sylowuntergruppe, so ist G isomorph zu einem semidirekten Produkt $N \rtimes_\alpha H$.
3. Wenn q kein Teiler von $p - 1$ ist, ist G zyklisch.

Aufgabe 2.20 — Zeigen Sie:

1. Es sei G eine Gruppe mit Zentrum Z. Wenn G/Z zyklisch ist, so ist G abelsch.
2. Es sei p eine Primzahl. Jede Gruppe der Ordnung p^2 ist abelsch. Wie viele Gruppen der Ordnung p^2 gibt es?
3. Sei p eine Primzahl. Zeigen Sie: In einer nichtabelschen Gruppe der Ordnung p^3 hat das Zentrum die Ordnung p.

Wir wiederholen in den folgenden Aufgaben einige Ergebnisse aus der Vorlesung Elementare Algebra und Zahlentheorie. Es sei G eine abelsche Gruppe. Die Zahl $e(G) := \sup\{\mathrm{ord}(g) \mid g \in G\} \in \mathbb{N} \cup \{\infty\}$ heißt Exponent von G.

Aufgabe 2.21 — Es sei G eine Gruppe mit kommutierenden Elementen a und b von endlicher Ordnung $m = \mathrm{ord}(a)$ bzw. $n = \mathrm{ord}(b)$. Man zeige:

1. Sind m und n teilerfremd, so gibt es $k, \ell \in \mathbb{Z}$ mit $(ab)^k = a$ und $(ab)^\ell = b$, und das Element ab hat die Ordnung mn.
2. Es gibt ein Element $c \in \langle a, b\rangle < G$ mit $\mathrm{ord}(c) = \mathrm{kgV}(m, n)$.

Aufgabe 2.22 — Es sei G eine endliche abelsche Gruppe. Dann gilt $\mathrm{ord}(g)|e(G)$ für alle $g \in G$, und $e(G)$ teilt die Gruppenordnung. [Hinweis: Aufgabe 2.21.]

Aufgabe 2.23 — Es sei K ein Körper und $G < K^\times$ eine endliche Untergruppe der Einheitengruppe. Dann ist G zyklisch. Insbesondere ist für jeden endlichen Körper $\mathbb{F}$ die Einheitengruppe $\mathbb{F}^\times$ zyklisch. [Hinweis: Man zeige, daß alle $g \in G$ Nullstellen des Polynoms $X^{e(G)} - 1 \in K[X]$ sind.]

Die Bestimmung der Einheitengruppe $(\mathbb{Z}/n)^\times$ für eine beliebige natürliche Zahl zerfällt in zwei Teile. Zunächst zerlegt man $n = \prod_i p_i^{m_i}$ in seine Primfaktoren. Nach dem Chinesischen Restklassensatz gilt dann zunächst

$$\mathbb{Z}/n \cong \prod_i \mathbb{Z}/p_i^{m_i}$$

und damit auch

$$(\mathbb{Z}/n)^\times \cong \prod_i (\mathbb{Z}/p_i^{m_i})^\times.$$

Es bleibt das Problem, die Struktur von $(\mathbb{Z}/n)^\times$ für den Fall einer Primzahlpotenz $n = p^m$ zu bestimmen. Das geschieht in den folgenden Aufgaben.

Aufgabe 2.24 — Es sei p eine ungerade Primzahl. Für alle $m \geq 0$ gilt:

$$(1+p)^{p^m} \equiv 1 + p^{m+1} \ \equiv \ p^{m+2}.$$

Für alle $m \geq 0$ gilt

$$(1+2^2)^{2^m} \equiv 1 + 2^{m+2} \ \equiv \ 2^{m+3}.$$

Aufgabe 2.25 — Es sei p eine ungerade Primzahl und $m \geq 1$. Es sei U der Kern des Homomorphismus $\varphi : (\mathbb{Z}/p^m)^\times \to (\mathbb{Z}/p)^\times$.

1. U ist eine p-Gruppe.
2. U wird von $1 + p$ erzeugt.
3. $(\mathbb{Z}/p^m)^\times$ ist zyklisch der Ordnung $(p-1)p^{m-1}$.

Aufgabe 2.26 — Es sei $m \geq 2$ und U der Kern des Homomorphismus $\varphi : (\mathbb{Z}/2^m)^\times \to (\mathbb{Z}/4)^\times$.

1. U ist eine 2-Gruppe.
2. U wird von 5 erzeugt.
3. $(\mathbb{Z}/2^m)^\times \cong \mathbb{Z}/2 \times \mathbb{Z}/2^{m-2}$, wobei die Faktoren von -1 und 5 erzeugt werden.

§3 Körpererweiterungen

2. Mai 2008

3.1 Charakteristik und Grad

Wir kennen drei prinzipielle Methoden, um aus Ringen Körper zu konstruieren:

1. Ist A ein kommutativer Ring und $\mathfrak{m}$ ein maximales Ideal, dann ist der Restklassenring $A/\mathfrak{m}$ ein Körper, der *Restklassenkörper* von $\mathfrak{m}$. Aus $\mathbb{Z}$ gewinnt man so für jede Primzahl p den endlichen Körper $\mathbb{F}_p = \mathbb{Z}/p$.

2. Ist A ein Integritätsbereich, so ist der totale Quotientenring $Q(A)$ ein Körper, der *Quotientenkörper* von A. Das verallgemeinert den Übergang von den ganzen Zahlen $\mathbb{Z}$ zum Körper $\mathbb{Q} = Q(\mathbb{Z})$ der rationalen Zahlen.

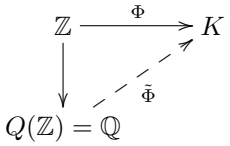
3. Es sei K ein Körper. Dann ist $K[X]$ ein Integritätsbereich. Sein Quotientenkörper ist der *Funktionenkörper*

$$F(X) := \left\{ \frac{f(X)}{g(X)} \;\middle|\; f, g \in K[X], g \neq 0 \right\}.$$

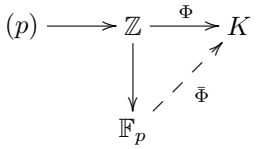
   Analog kann man mit einer beliebigen Anzahl von Unbestimmten verfahren.

Eine der wichtigsten Invarianten eines Körpers ist seine Charakteristik: Es sei K ein Körper und 1_K das Einselement. Für jedes $n \in \mathbb{N}$ bezeichne n_K die n-fache Summe von 1_K mit sich. Die Abbildung $\mathbb{N} \to K$, $n \to n_K$, setzt sich zu einem Ringhomomorphismus $\Phi : \mathbb{Z} \to K$ fort. Der Kern von Φ ist notwendigerweise ein Primideal. Die Charakteristik $\operatorname{char}(K)$ ist die Zahl 0 oder die Primzahl p je nachdem, ob $\ker(\Phi) = (0)$ oder $\ker(\Phi) = (p)$. Es gibt also zwei fundamental verschiedene Fälle:

1. $\operatorname{char}(K) = 0$. Dieser Fall tritt genau dann ein, wenn $n_K \neq 0$ für alle $n \in \mathbb{N}$. Der Ring $\mathbb{Z}$ wird durch Φ auf eindeutige Weise in K eingebettet. Jedes Element $\neq 0$ in $\mathbb{Z}$ ist in K invertierbar. Deshalb setzt sich die Abbildung Φ zu einem kanonischen injektiven Homomorphismus $\mathbb{Q} \to K$ des Quotientenkörpers fort.



2. $\operatorname{char}(K) = (p)$ für eine Primzahl p. Dabei ist p die kleinste natürliche Zahl n mit $n_K = 0$. Nach der universellen Eigenschaft des Restklassenrings induziert $\mathbb{Z} \to K$ einen kanonischen injektiven Homomorphismus $\mathbb{F}_p = \mathbb{Z}/(p) \to K$.



Ein *Unterkörper* in einem Körper K ist eine Teilmenge $k \subset K$, die unter Addition und Multiplikation abgeschlossen und mit diesen ererbten Verknüpfungen ein Körper ist. Der Durchschnitt aller Unterkörper in einem gegebenen Körper ist selbst ein Unterkörper, und zwar der kleinstmögliche. Er heißt der *Primkörper* von K. Offenbar ist der Primkörper eines Körpers auf kanonische Weise zu $\mathbb{Q}$ oder $\mathbb{F}_p$ isomorph je nachdem, ob $\mathrm{char}(K) = 0$ oder p.

Körper der Charakteristik $p > 0$ unterscheiden sich in zahlreichen Punkten von Körpern der Charakteristik 0. Alle endlichen Körper haben positive Charakteristik. Ein Beispiel für einen unendlichen Körper von positiver Charakteristik ist der Körper $\mathbb{F}_p(X)$ der rationalen Funktionen über $\mathbb{F}_p$.

Die Binomialkoeffizienten $\binom{p}{k}$ sind für $0 < k < p$ durch p teilbar. Deshalb gilt in den Körpern der Charakteristik $p > 0$ die Rechenregel

$$(a_1 + \ldots + a_n)^p = a_1^p + \ldots + a_n^p. \tag{3.1}$$

Daraus ergibt sich der Satz:

Satz 3.1 — *Es sei p eine Primzahl und K ein Körper der Charakteristik p. Die Abbildung $F : K \to K$, $a \mapsto a^p$, ist ein injektiver Ringhomomorphismus, der sogenannte* Frobeniushomomorphismus.

Definition 3.2 — Es sei K ein Körper. Eine K-Algebra ist ein Ring R zusammen mit einem Ringhomomorphismus $K \to R$.

Ein solcher Ringhomomorphismus $\varphi : K \to R$ ist immer injektiv. Außerdem wird R durch die skalare Multiplikation $\lambda \cdot x := \varphi(\lambda)x$ für $\lambda \in K$ und $x \in R$ zu einem K-Vektorraum. Wir können dann R mit den Mitteln der linearen Algebra untersuchen.

Definition 3.3 — Es sei K ein Körper. Ein Homomorphismus $K \to L$ in einen Körper L heißt Körpererweiterung von K. Die Dimension von L als K-Vektorraum heißt Grad der Erweiterung und wird mit $[L : K] := \dim_K(L)$ notiert. Eine Erweiterung $K \to L$ heißt endlich, wenn $[L : K] < \infty$.

Da jede Körpererweiterung notwendigerweise injektiv ist, identifizieren wir K häufig mit seinem Bild und betrachten K als einen Unterkörper von L, wenn es ohne Gefahr von Mißverständnissen möglich ist. Man spricht auch von einer Einbettung des Körpers K in den Körper L. Wenn man den Homomorphismus $K \to L$ nicht betonen will, schreibt man L/K für die Erweiterung.

Beispiele 3.4 — 1. Der Körper $K = \mathbb{Q}(\sqrt[3]{2})$ besitzt drei verschiedene Einbettungen in $\mathbb{C}$. Zunächst hat man mit der Abkürzung $\alpha = \sqrt[3]{2}$ die Darstellung

$$K = \{a + b\alpha + c\alpha^2 \mid a, b, c \in \mathbb{Q}\}. \tag{3.2}$$

Um K in $\mathbb{C}$ einzubetten, muß α auf eine komplexe Zahl abgebildet werden, deren dritte Potenz 2 ist. Dazu gibt es genau drei Möglichkeiten: α, $\alpha\rho$ und $\alpha\rho^2$ mit $\rho = \exp(2\pi i/3)$. Die Wahl von α liefert einfach die Standardinklusion $\varphi_1 = \mathrm{id} : K \to \mathbb{C}$, die beiden anderen Wahlen liefern Einbettungen $\varphi_2, \varphi_3 : K \to \mathbb{C}$, deren Bilder nicht einmal in $\mathbb{R}$ landen.

2. Etwas anders ist die Situation im folgenden Fall: Der Körper $\mathbb{Q}(\sqrt{2})$ besitzt zwei verschiedene Einbettungen in $\mathbb{C}$, nämlich $\varphi_1(a+b\sqrt{2}) = a+b\sqrt{2}$ und $\varphi_2(a+b\sqrt{2}) = a - b\sqrt{2}$. In diesem Falle sind die Bilder der beiden Abbildungen gleich, aber die Abbildungen selbst sind verschieden.

3. Die Erweiterungen $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ und $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ sind endlich vom Grad 3 bzw. 2. Ähnlich ist $[\mathbb{C} : \mathbb{R}] = 2$. Die Erweiterung $\mathbb{R}/\mathbb{Q}$ hat unendlichen Grad.

Satz 3.5 — *Es seien $K \to L \to M$ Körpererweiterungen. Dann gilt* 5. Mai 2008

$$[M : K] = [M : L] \cdot [L : K]. \tag{3.3}$$

Beweis. Es sei $\{x_i\}_{i\in I}$ eine K-Basis von L und $\{y_j\}_{j\in J}$ eine L-Basis von M. Wir betrachten die Menge $B := \{x_i y_j\}_{(i,j)\in I\times J}$. Es genügt zu zeigen, daß B eine Basis ist, denn $|B| = |I| \cdot |J|$.

Zunächst läßt sich jedes $m \in M$ als Linearkombination $m = \sum_j \ell_j y_j$ schreiben, wobei fast alle $\ell_j \in L$ verschwinden. Weiter läßt sich jedes $\ell_j \neq 0$ als Linearkombination $\ell_j = \sum_i a_{ij} x_i$ schreiben. Insgesamt sind nur endlich viele $a_{ij} \neq 0$. Nun gilt $m = \sum_{(i,j)} a_{ij} x_i y_j$. Folglich ist B ein Erzeugersystem.

Ist andererseits $0 = \sum_{(i,j)} a_{ij} x_i y_j = \sum_j \left(\sum_i a_{ij} x_i\right) y_j$, so folgt aus der linearen Unabhängigkeit der y_j zunächst, daß $\sum_i a_{ij} x_i = 0$ für alle j, und dann aus der linearen Unabhängigkeit der x_i, daß $a_{ij} = 0$ für alle (i, j). Folglich ist B eine Basis. □

Für den Satz und den Beweis ist es unerheblich, ob die Mengen I und J endlich sind oder nicht.

Satz 3.6 — *Es sei K ein Körper, A eine kommutative nullteilerfreie K-Algebra mit $\dim_K(A) < \infty$. Dann ist A ein Körper.*

Beweis. Der Beweis ist sehr leicht. Wir führen bei der Gelegenheit Bezeichnungen ein, die wir auch später gebrauchen können. Für jedes $a \in A$ ist die Linksmultiplikation

$$\ell_a : A \to A, \quad x \mapsto ax,$$

eine K-lineare Abbildung. Die Nullteilerfreiheit von A impliziert, daß ℓ_a injektiv ist, wenn $a \neq 0$. Da $\dim_K(A) < \infty$, ist jeder injektive Endomorphismus des K-Vektorraums A auch surjektiv. Es gibt also insbesondere zu jedem $a \in A \setminus \{0\}$ ein $b \in A$ mit $ab = \ell_a(b) = 1$. □

Es sei $K \to L$ eine Körpererweiterung und $S \subset L$ eine Menge. Es gibt Unterkörper von L, die das Bild von K und S enthalten, zum Beispiel L selbst. Der Durchschnitt

aller dieser Unterkörper hat dieselbe Eigenschaft und ist der kleinste Unterkörper mit dieser Eigenschaft. Er wird mit $K(S)$ bezeichnet und heißt der von S über K erzeugt Unterkörper von L. Er läßt sich auch folgendermaßen beschreiben:

$$K(S) := \left\{ \frac{p(s_1, \ldots, s_n)}{q(s_1, \ldots, s_n)} \;\middle|\; n \in \mathbb{N}_0, p, q \in K[X_1, \ldots, X_n], s_1, \ldots, s_n \in S, q(s) \neq 0. \right\}$$

Falls $S = \{a_1, \ldots, a_\ell\}$ schreiben wir kurz $K(a_1, \ldots, a_\ell)$ statt $K(\{a_1, \ldots, a_\ell\})$.

Definition 3.7 — Es sei L/K eine Körpererweiterung.

1. Eine Menge $S \subset L$ erzeugt die Erweiterung L/K, wenn $L = K(S)$.

2. Der Körper L heißt endlich erzeugt über K, wenn es eine endliche Menge $S \subset L$ mit $L = K(S)$ gibt.

3. Eine Erweiterung L/K heißt einfach, wenn es ein Element $a \in L$ mit $L = K(a)$ gibt.

Es ist klar, daß jede endliche Körpererweiterung auch endlich erzeugt ist, denn jede Basis ist erst recht ein Erzeugendensystem. Umgekehrt wird der Funktionenkörper $K(X)$ als Körpererweiterung von K allein von X erzeugt, d.h. $K(X)/K$ ist eine einfache Erweiterung, aber $[K(X) : K] = \infty$.

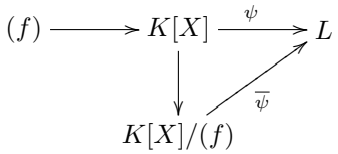
Man beachte auch, daß es zu jedem $a \in K(S)$ eine *endliche* Teilmenge $S_a \subset S$ mit $a \in K(S_a)$ gibt, weil sich jedes a als Quotient von zwei Polynomen mit Einträgen aus S ausdrücken läßt, die aber jeweils nur von endlich vielen Elementen aus S abhängen können.

3.2 Algebraische Erweiterungen

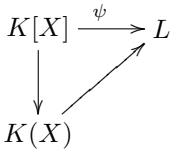
Es sei $i : K \to L$ eine Körpererweiterung und $a \in L$. Wegen der universellen Eigenschaft des Polynomrings gibt es genau einen Ringhomomorphismus $\psi : K[X] \to L$ mit $\psi|_K = i$ und $\psi(X) = a$. Wir schreiben kurz $\psi(f) =: f(a)$. Das Bild von ψ ist ein Unter*ring* von L und wird mit $K[a]$ bezeichnet. Weil jeder Unterring eines Körper nullteilerfrei ist, ist der Kern von ψ ein Primideal. Deshalb bestehen zwei Möglichkeiten:

1. $\ker(\psi) = (f)$ mit einem eindeutig bestimmten normierten irreduziblen Polynom f. Wegen der universellen Eigenschaft des Restklassenrings faktorisiert ψ über eine Einbettung $\overline{\psi} : K[X]/(f) \to L$. Es folgt, daß $K[X]/(f) \cong K(a)$ und $[K(a) : K] = [K[X]/(f) : K] = \mathrm{grad}(f) =: n$. Es gilt dann schon $K[a] = K(a)$. Wir nennen a in diesem Falle algebraisch vom Grad n über K. Das Polynom f ist das eindeutig bestimmte normierte Polynom kleinsten Grades mit $f(a) = 0$. Es heißt das Minimalpolynom von a und wird mit $\mathrm{minpol}_{a/K} := f$

bezeichnet.



2. $\ker(\psi) = (0)$. In diesem Falle wird $K[X]$ durch ψ in L eingebettet, und setzt sich gemäß der universellen Eigenschaft der Lokalisierung zu einer Einbettung des Körpers der rationalen Funktionen fort: $\Phi : K(X) \to L$. Es folgt, daß $K[X] \cong K[a]$ und $K(X) \cong K(a)$, und insbesondere ist $[K(a) : K] = \infty$. Wir nennen a in diesem Falle transzendent über K.



Definition 3.8 — Es sei L/K eine Körpererweiterung und $a \in L$ algebraisch über K. Ein Element $b \in L$ ist *konjugiert* zu a, wenn b Nullstelle des Minimalpolynoms von a ist.

Die Definition erweitert den Begriff der komplex konjugierten Zahl: In der Erweiterung $\mathbb{C}/\mathbb{R}$ ist jedes $z \in \mathbb{C}$ algebraisch über $\mathbb{R}$, und zwar vom Grad 1 oder 2 je nachdem ob z reell ist oder nicht. Die zu z konjugierten Zahlen sind z selbst und $\overline{z}$, die im üblichen Sinne konjugierte komplexe Zahl.

Beispiel 3.9 — Die komplexe Zahl $a = \sqrt{5}-2$ ist algebraisch über $\mathbb{Q}$: Da $\sqrt{5} = a+2$, folgt $5 = a^2 + 4a + 4$. Alternativ kann man $\sqrt{5}$ aus $a = \sqrt{5} - 2$ und $a^2 = 9 - 4\sqrt{5}$ eliminieren:

$$\sqrt{5} = a + 2 = \frac{1}{4}(9 - a^2). \tag{3.4}$$

Auch so ergibt sich $a^2 + 4a - 1 = 0$. Das Polynoms $x^2 + 4x - 1$ ist irreduzibel in $\mathbb{Q}[x]$, weil es keine Nullstellen in $\mathbb{Q}$ besitzt: Jede Nullstelle müßte schon ganzzahlig sein und außerdem ein Teiler des konstanten Terms. Die einzigen Teiler sind ± 1, und diese sind keine Nullstellen. Also ist $x^2 + 4x - 1$ das Minimalpolynom von a. Die zu a konjugierte Nullstelle ist $-\sqrt{5} - 2 = -a - 4 \in \mathbb{Q}(a)$.

Beispiel 3.10 — Es sei $a = \sqrt[3]{2} \in \mathbb{R}$. Dann ist $b = a^2 + a$ algebraisch über $\mathbb{Q}$: Wir finden $b^2 = (a^2+a)^2 = a^4+2a^3+a^2 = a^2+2a+4$ und $b^3 = a^6+3a^5+3a^4+a^3 = 6a^2 + 6a + 6$. Durch Elimination von a^2 und a aus diesen Gleichungen findet man $b^3 - 6b - 6 = 0$. Nach dem Eisensteinkriterium ist $x^3 - 6x - 6 \in \mathbb{Q}[X]$ irreduzibel und daher das Minimalpolynom von b. Die zu b konjugierten Elemente in $\mathbb{C}$ sind $\rho a^2 + \rho^2 a$ und $\rho^2 a^2 + \rho a$, wobei $\rho = \exp(2\pi i/3)$, wie man durch Ausmultiplizieren verifiziert:

$$(X - a^2 - a)(X - \rho a^2 - \rho a)(X - \rho^2 a^2 - \rho a) = \ldots = X^3 - 6X - 6. \tag{3.5}$$

Beachte: $a^3 = 2$, $\rho^2 + \rho + 1 = 0$. Die zu b konjugierten Zahlen sind nicht reell und liegen sicher nicht in $\mathbb{Q}(b)$.

9. Mai 2008

Beispiel 3.11 — Um das reguläre Siebeneck in den Einheitskreis zeichnen zu können, bräuchte man eine Strecke der Länge $u = \cos(\alpha)$, $\alpha = 2\pi/7$. Aus dem Additionstheorem für den Kosinus folgt für beliebige $a, b \in \mathbb{R}$:

$$\cos(a+b) + \cos(a-b) = 2\cos(a) \cdot \cos(b). \tag{3.6}$$

Daraus ergibt sich:

$$\cos(2\alpha) = 2u^2 - 1, \quad \cos(3\alpha) = 2u(2u^2-1) - u = 4u^3 - 3u \tag{3.7}$$

und

$$\cos(4\alpha) = 2(2u^2-1)^2 - 1 = 8u^4 - 8u^2 + 1. \tag{3.8}$$

Da $\cos(3\alpha) = \cos(4\alpha)$ für diese spezielle Wahl von α, liefert der Vergleich die Identität

$$8u^4 - 8u + 1 = 4u^3 - 3u \tag{3.9}$$

oder

$$8u^4 - 4u^3 - 8u^2 + 3u + 1 = 0. \tag{3.10}$$

Das Polynom $8x^4 - 4x^3 - 8x^2 + 3x + 1$ ist aber nicht irreduzibel, es hat die Nullstelle 1. Division durch $x - 1$ liefert das kubische Polynom:

$$8x^3 + 4x^2 - 4x - 1 \in \mathbb{Q}[x]. \tag{3.11}$$

Es liegt nahe, die Substitution $z = 2u = e^{i\alpha} + e^{-i\alpha}$ vorzunehmen. z ist dann Nullstelle des Polynoms $f = x^3 + x^2 - 2x - 1$. Da ± 1 keine Nullstellen von f sind, ist f irreduzibel. Also ist z algebraisch über $\mathbb{Q}$ mit Minimalpolynom f. Die zu $z = 2\cos(\alpha)$ konjugierten Elemente sind $2\cos(2\alpha) = z^2 - 2$ und $2\cos(3\alpha) = z^3 - 3z$ und liegen, wie die Formeln zeigen, in $\mathbb{Q}(z)$.

Man kann dasselbe Polynom f auch wie folgt herleiten: Es sei $\zeta = \exp(2\pi i/7)$. Dann genügt ζ der Gleichung

$$\zeta^6 + \zeta^5 + \zeta^4 + \zeta^3 + \zeta^2 + \zeta + 1 = 0. \tag{3.12}$$

Außerdem ist $z = \zeta + \zeta^{-1}$. Wir teilen (3.12) durch ζ^3 und entwickeln nach Potenzen von v:

$$\begin{aligned} \zeta^3 + \zeta^2 + \zeta + 1 + \zeta^{-1} + \zeta^{-2} + \zeta^{-3} &= z^3 + \zeta^2 + \zeta^{-2} - 2\zeta - 2\zeta^{-1} + 1 \\ &= z^3 + z^2 - 2\zeta - 2\zeta^{-1} - 1 \\ &= z^3 + z^2 - 2z - 1. \end{aligned}$$

Definition 3.12 — Eine Körpererweiterung $K \to L$ heißt algebraisch, wenn jedes $a \in L$ algebraisch über K ist, und andernfalls transzendent.

Satz 3.13 — *Die folgenden Aussagen über eine Körpererweiterung L/K sind äquivalent:*

1. *L/K ist endlich.*
2. *L/K ist algebraisch und endlich erzeugt.*
3. *L/K ist erzeugt von endlich vielen algebraischen Elementen.*

Beweis. $1 \Rightarrow 2$: Es sei L/K endlich vom Grad n. Jede Vektorraumbasis ist ein Erzeugersystem. Deshalb ist L/K sicher endlich erzeugt. Für jedes $a \in L$ sind die Elemente $1, a, \ldots, a^n$ linear abhängig über K. Es gelte etwa $f_0 + f_1 a + \ldots + f_n a^n = 0$. Dann ist a Nullstelle des Polynoms $f = \sum_k f_k X^k$ und deshalb algebraisch.
$2 \Rightarrow 3$: Trivial.
$3 \Rightarrow 1$: Es seien $s_1, \ldots, s_n \in L$ Elemente, die algebraisch über K sind und L erzeugen. Wir zeigen durch Induktion über n, daß der Körper $K_i = K(s_1, \ldots, s_i)$ endlich über K ist. Für $i = 1$ ist dies klar. Angenommen, $i > 1$ und $[K_{i-1} : K] < \infty$. Nach Annahme ist s_i algebraisch über K, also erst recht über K_{i-1}. Es folgt mit dem Gradsatz: $[K_i : K] = [K_i : K_{i-1}] \cdot [K_{i-1} : K] < \infty$. Mit $L = K_n$ hat man die Behauptung. □

Satz 3.14 — *Die folgenden Aussagen über eine Erweiterung L/K sind äquivalent:*

1. *L ist algebraisch über K.*
2. *L wird von Elementen erzeugt, die algebraisch über K sind.*
3. *Jede endliche Menge $S \subset L$ liegt in einem Zwischenkörper M von endlichem Grad über K.*

Beweis. $1 \Rightarrow 2$: Trivial.
$2 \Rightarrow 3$: Es sei T ein Erzeugendensystem von L über K aus algebraischen Elementen und $S \subset L$ eine endliche Teilmenge. Zu jedem Element $s \in S$ gibt es eine endliche Menge $T_s \subset T$ mit $s \in K(T_s)$. Es sei T' die Vereinigung aller T_s. Dann ist $M = K(T')$ ein von endlich vielen algebraischen Elementen erzeugter Zwischenkörper und nach Satz 3.13 algebraisch über K von endlichem Grad.
$3 \Rightarrow 1$: Jedes Element $a \in L$ liegt in einem Zwischenkörper von endlichem Grad über K und ist deshalb nach Satz 3.13 algebraisch über K.

□

Eine unmittelbare Folgerung des Satzes ist die folgende: Ist L/K eine Körpererweiterung, so ist die Menge aller Elemente in L, die algebraisch über K sind, ein Zwischenkörper.

Definition 3.15 — 1. Es sei L/K eine Körpererweiterung. Der Zwischenkörper aller Elemente in L, die algebraisch über K sind, heißt algebraischer Abschluß von K in L.

2. Der algebraische Abschluß von $\mathbb{Q}$ in $\mathbb{C}$ wird mit $\overline{\mathbb{Q}}$ bezeichnet und heißt der Körper der algebraischen Zahlen.

Satz 3.16 — *Es sei L/K eine algebraische und M/L eine beliebige Körpererweiterung. Ein Element $a \in M$ ist genau dann algebraisch über L, wenn a algebraisch über K ist.*

Beweis. Wenn a algebraisch über K ist, ist es trivialerweise auch algebraisch über L. Es sei also umgekehrt a algebraisch über L und $f = X^n + f_{n-1}X^{n-1} + \ldots + f_0$ das Minimalpolynom. Dann ist der von den Koeffizienten von f erzeugte Zwischenkörper $L' := K(f_0, \ldots, f_{n-1}) \subset L$ nach Satz 3.13 endlich über K, und nach Konstruktion ist a algebraisch über L'. Daher ist $[L'(a) : K] = [L'(a) : L'][L' : K] < \infty$ und somit a algebraisch über K. □

Man kann diesen Satz auch so ausdrücken, daß die Eigenschaft, eine algebraische Erweiterung zu sein, transitiv ist:

Folgerung 3.17 — *Sind $M/L/K$ Körpererweiterungen, so ist M/K genau dann algebraisch, wenn M/L und L/K algebraisch sind.* □

3.3 Nullstellen und algebraisch abgeschlossene Körper

Im letzten Abschnitt sind wir *analytisch* vorgegangen: Die Körpererweiterung $K \to L$ war gegeben, und zu einem algebraischen Element $a \in L$ haben wir das zugehörige Minimalpolynom betrachtet. In diesem Abschnitt gehen wir den umgekehrten *synthetischen* Weg: Wir starten mit einem Körper K und einem irreduziblen Polynom $f \in K[X]$ und konstruieren eine Erweiterung $K \to L$, in der f eine Nullstelle besitzt. Indem wir diesen Weg zu Ende gegen, können wir zu jedem Körper K eine algebraisch abgeschlossene Erweiterung $\overline{K}$ konstruieren.

Es sei $i : K \to L$ eine Körpererweiterung. Diese Abbildung erweitert sich zu einer Inklusion von Polynomringen $i' : K[X] \to L[X]$ durch $i'|_K = i$ und $i'(X) = X$. Solange keine Gefahr von Mehrdeutigkeiten besteht, schreiben wir wieder f statt $i'(f)$ für Polynome $f \in K[X]$. Ein Polynom $f \in K[X]$ kann in L Nullstellen bekommen oder über L in Faktoren zerfallen, die es über K noch nicht gab. Zum Beispiel ist $X^4 + 1 \in \mathbb{Q}[X]$ irreduzibel, besitzt aber über $\mathbb{R}$ bzw. $\mathbb{C}$ die Faktorisierungen

$$\begin{aligned} X^4 + 1 &= (X^2 + \sqrt{2}X + 1)(X^2 - \sqrt{2}X + 1) \\ &= (X - \varepsilon)(X - \varepsilon^3)(X - \varepsilon^5)(X - \varepsilon^7) \end{aligned}$$

mit der primitiven 8-ten Einheitswurzel $\varepsilon = \exp(2\pi i/8)$.

Satz 3.18 — *Es sei K ein Körper und $f \in K[X]$ ein irreduzibles normiertes Polynom vom Grad n. Dann ist $M := K[X]/(f)$ eine Körpererweiterung von K vom Grad n. Die Restklasse $\overline{X} \in M$ von X ist eine Nullstelle von f.*

Beweis. Angenommen, $\overline{a}, \overline{b} \in M$ sind Elemente mit $\overline{a}\overline{b} = 0$. Wir wählen Repräsentanten $a, b \in K[X]$. Die Annahme bedeutet, daß $f|ab$. Da f prim ist, folgt $f|a$ oder $f|b$, also $\overline{a} = 0$ oder $\overline{b} = 0$. Das zeigt, daß $K[X]/(f)$ ein Integritätsbereich ist. Durch Polynomdivision mit Rest folgt, daß jedes Polynom modulo f kongruent zu einem Polynom vom Grad $< n$ ist. Daher wird M als K-Vektorraum von den Restklassen von $1, X, \ldots, X^{n-1}$ aufgespannt. Nach Satz 3.6 ist M eine endliche Körpererweiterung von K. Wären die Restklassen von $1, \ldots, X^{n-1}$ nicht linearunabhängig, gäbe es $c_0, c_1, \ldots, c_{n-1} \in K$ derart, daß $c := c_0 + \ldots c_{n-1}X^{n-1}$ durch f teilbar wäre. Das ist absurd. Also ist $[M : K] = n$. Die letzte Aussage ist nach Konstruktion klar. □

Man beachte, daß man — mit den Bezeichnungen des Satzes — zu jedem Element $0 \neq \bar{g} = g_0 + g_1\overline{X} + \ldots + g_{n-1}\overline{X}^{n-1} \in M$ mit dem euklidischen Algorithmus ein Inverses explizit berechnen kann: Da f irreduzibel ist, sind f und $g = g_0 + g_1X + \ldots + g_{n-1}X^{n-1}$ in $K[X]$ teilerfremd. Man bestimmt dann mit dem euklidischen Algorithmus Polynome α und β mit $1 = \alpha f + \beta g$. Die Restklasse von β in M ist ein Inverses zu $\bar{g}$.

Folgerung 3.19 — *Es seien K ein Körper und $f_1, \ldots, f_n \in K[X] \setminus \{0\}$ Polynome. Dann gibt es eine Körpererweiterung L/K derart, daß alle f_i über L in Linearfaktoren zerfallen.*

Beweis. Man kann sich sofort auf den Fall $n = 1$ zurückziehen, indem man die Polynome durch ihr Produkt ersetzt. Es sei also f ein nichttriviales Polynom. Wir argumentieren mit Induktion über den Grad von f. Falls f den Grad 0 oder 1 hat, kann man $L = K$ wählen. Andernfalls sei $g|f$ ein irreduzibler normierter Faktor. Der Satz 3.18 garantiert die Existenz einer Erweiterung $K \to M$ und eines Elements $\beta_1 \in M$ mit $g(\beta_1) = 0$. Es sei $h := f/(X - \beta_1) \in M[X]$. Da $\operatorname{grad}(h) < \operatorname{grad}(f)$, folgt induktiv die Existenz einer Erweiterung $M \to L$ derart, daß h in $L[X]$ in Linearfaktoren zerfällt: $h = c(X - \beta_2) \cdots (X - \beta_\ell)$ mit $\beta_i \in M$ und $c \in K$ zerfällt. Damit hat man auch $f = c(X - \beta_1) \cdots (X - \beta_\ell)$. □

Definition 3.20 — Ein Körper K heißt algebraisch abgeschlossen, wenn die folgenden äquivalenten Bedingungen erfüllt sind:

1. Jedes nichtkonstante Polynome $f \in K[X]$ besitzt eine Nullstelle in K.
2. Jedes nichtkonstante Polynom $f \in K[X]$ zerfällt in ein Produkt aus Linearfaktoren.
3. Jedes irreduzible Polynom $f \in K[X]$ hat Grad 1.

Der Beweis der Äquivalenz der Bedingungen ist einfach.

Satz 3.21 — *Jeder Körper K besitzt eine Einbettung $K \to \tilde{K}$ in einen algebraisch abgeschlossenen Körper.*

Beweis. 1. Schritt: Wir imitieren die Konstruktion einer Nullstelle zu einem gegebenen Polynom, nur daß wir Nullstellen für alle Polynome auf einen Schlag konstruieren.

Es sei $F \subset K[X]$ die Menge aller normierten irreduziblen Polynome. Wir betrachten den Polynomring $R := K[\{X_f\}_{f\in F}]$ mit einer Unbestimmten X_f zu jedem $f \in F$. Es sei $I \subset R$ das Ideal, das von allen Elementen $f(X_f)$, $f \in F$, erzeugt wird. Da I die Konstanten nicht enthält, ist $I \neq R$. Es sei $\mathfrak{m} \subset R$ ein maximales Ideal, das I enthält. Der Restklassenring $L := R/\mathfrak{m}$ ist eine Körpererweiterung von K, und bezeichnet $\alpha_f \in L$ die Restklasse von X_f, so gilt $f(\alpha_f) = 0$, weil $f(X_f) \in I \subset \mathfrak{m}$. In L hat also jedes Polynom von K eine Nullstelle. Außerdem ist L algebraisch über K, weil L von den Restklassen der X_f erzeugt wird, die nach Konstruktion algebraisch über K sind.

Wir werden später sehen, daß L bereits algebraisch abgeschlossen ist. Bis dahin müssen wir anders argumentieren.

2. Schritt: Wir iterieren die Konstruktion und erhalten eine Folge von Körpererweiterungen

$$K_0 := K \to K_1 := L \to K_2 \to K_3 \to \dots \tag{3.13}$$

mit der Eigenschaft: Jedes irreduzible Polynom in $K_n[X]$ besitzt in K_{n+1} eine Nullstelle. Daraus folgt auch durch ein einfaches Gradargument: Jedes Polynom in $K_n[X]$ vom Grad $\leq m$ zerfällt in $K_{n+m}[X]$ in Linearfaktoren.

Wären die Abbildungen $K_n \to K_{n+1}$ Inklusionen im mengentheoretischen Sinne, so würden wir einfach $K_\infty := \bigcup K_n$ setzen. Jedes Polynom in $K_\infty[X]$ vom Grad ℓ hat nur endlich viele Koeffizienten und liegt daher schon in $K_N[X]$ für hinreichend groß gewähltes N und zerfällt in $K_{N+\ell}[X]$ in Linearfaktoren. Also ist K_∞ algebraisch abgeschlossen (und sicher auch algebraisch über K).

Da die iterativ konstruierten Erweiterungen $u_n : K_n \to K_{n+1}$ zwar injektiv, aber keine Inklusionen sind, müssen wir anders vorgehen: Es sei $A := \bigoplus_{n\geq 0} K_n$ mit komponentenweise definierten Verknüpfungen und $i_n : K_n \to A$ die Inklusionsabbildung. Dann ist A ein kommutativer Ring (ohne 1!). Es bezeichne $J \subset A$ das Ideal, das von allen Elementen der Form $i_{n+1}(u_n(x)) - i_n(x)$ erzeugt wird. Dann ist $K_\infty := A/I$ ein kommutativer Ring mit 1. Bezeichnet j_n die Komposition $K_n \to A \to K_\infty$, so gilt: $j_{n+1} \circ u_n = j_n$ für alle n und $\bigcup_{n\geq 0} j_n(K_n) = K_\infty$. Wie bereits ausgeführt ist K_∞ ein algebraisch abgeschlossener Körper. □

Die im zweiten Beweisschritt durchgeführte Konstruktion ist ein Spezialfall einer allgemeinen Konstruktion, die einem *direkten System* von Ringen einen *Kolimes* oder *direkten Limes* zuordnet.

16. Mai 2008

Definition 3.22 — Eine Erweiterung $K \to \overline{K}$ ist ein algebraischer Abschluß von K, wenn $\overline{K}$ algebraisch abgeschlossen und algebraisch über K ist.

Zum Beispiel ist $\mathbb{C}$ algebraisch abgeschlossen, aber nicht der algebraische Abschluß von $\mathbb{Q}$.

Satz 3.23 *(Fundamentalsatz der Algebra) — $\mathbb{C}$ ist algebraisch abgeschlossen.*

Wir beweisen den Satz nach der Methode von Lagrange. Gauß hat diesen Beweis wie auch andere frühere Beweise aus methodischen Gründen abgelehnt, weil diese Beweise die Existenz von Wurzeln einer vorgelegten Polynomgleichung in irgendeinem Rechenbereich voraussetzen (den Begriff Körper hier zu verwenden, wäre anachronistisch), vgl. die Einleitung der Dissertation von Gauß. Mit der Einführung des Begriffs der Körpererweiterung und dem abstrakten Nachweis, daß jedes Polynom $f \in K[X]$ über einer geeigneten Körpererweiterung $K \to K'$ zerfällt, fallen die Einwände von Gauß weg.

Da der Körper $\mathbb{C}$ als Erweiterung von $\mathbb{R}$ definiert ist und die Konstruktion von $\mathbb{R}$ analytische Elemente enthält, nämlich die Vervollständigung von $\mathbb{Q}$ bezüglich des Betrages, kommt man nicht ganz ohne analytische Hilfsaussagen aus. Man kann sie im Kern auf das folgende Lemma reduzieren:

Lemma 3.24 *— Jedes Polynom in $\mathbb{R}[X]$ von ungeradem Grad hat in $\mathbb{R}$ eine Nullstelle. Für jede positive reelle Zahl a hat $X^2 - a$ eine positive Nullstelle in $\mathbb{R}$.*

Beweis. Zwischenwertsatz. □

Aus der zweiten Aussage des Lemmas ergibt sich zunächst:

Lemma 3.25 *— Jedes quadratische Polynom in $\mathbb{C}[X]$ hat in $\mathbb{C}$ eine Nullstelle.*

Beweis. Durch quadratische Ergänzung führt man das Problem auf die Aussage zurück, daß jede komplexe Zahl eine komplexe Quadratwurzel besitzt. Ist nun $a + bi \neq 0$ vorgegeben, so führt der Ansatz $(x + iy)^2 = (a + bi)$ auf die Gleichungen

$$x^2 + y^2 = \sqrt{a^2 + b^2}, \quad x^2 - y^2 = a \tag{3.14}$$

mit den Lösungen

$$x = \pm\sqrt{\frac{1}{2}\left(a + \sqrt{a^2 + b^2}\right)}, \quad y = \pm\sqrt{\frac{1}{2}\left(-a + \sqrt{a^2 + b^2}\right)}. \tag{3.15}$$

Dabei sind die Vorzeichen so zu wählen, daß $2xy = b$. □

Beweis des Hauptsatzes der Algebra. Es genügt zu zeigen, daß jedes nichtkonstante reelle Polynom in $\mathbb{C}$ eine Nullstelle besitzt. Denn ist f ein beliebiges komplexes Polynom, so ist $g = f\overline{f}$ reell, und ist α eine Nullstelle von g, so ist entweder α oder $\overline{\alpha}$ eine Nullstelle von f.

Es sei nun ein normiertes Polynom $f \in \mathbb{R}[X]$ vom Grad n vorgelegt. Wir schreiben $n = 2^a u$ mit einer ungeraden Zahl u und einem Exponenten $a \in \mathbb{N}_0$. Wir führen den Beweis durch Induktion über a. Der Induktionsanfang $a = 0$ ist gerade der Fall eines Polynoms von ungeradem Grad $n = u$.

Es sei also $a \geq 1$ und die Behauptung für alle Polynome vom Grad $2^{a'}u'$ mit $a' < a$ schon gezeigt. Wir wählen eine algebraische Erweiterung $\mathbb{R} \subset \mathbb{C} \subset L$ so, daß f über L in Linearfaktoren zerfällt, $f = \prod_{i=1}^{n}(X - x_i)$. Wir betrachten für einen noch näher zu bestimmenden Parameter $t \in \mathbb{R}$ und für jedes Paar von Indizes $1 \leq i < j \leq n$ die Elemente $c_{ij} = x_i + x_j + tx_ix_j$, sowie das Polynom

$$f_t := \prod_{i<j}(X - c_{ij}). \tag{3.16}$$

Offensichtlich ist f_t symmetrisch unter Permutation der x_i. Die Koeffizienten von f_t lassen sich dann polynomiell durch t und die Koeffizienten von f ausdrücken, sind also insbesondere reell. Das Polynom $f_t \in \mathbb{R}[X]$ hat den Grad

$$\operatorname{grad}(f_t) = \binom{n}{2} = 2^{a-1}u(2^a u - 1) = 2^{a-1}u'. \tag{3.17}$$

Nach Induktionsannahme ist eine der Nullstellen c_{ij} von f_t komplex, d.h. es gibt ein Paar $(i(t), j(t))$ mit $u(t) := x_{i(t)} + x_{j(t)} + tx_{i(t)}x_{j(t)} \in \mathbb{C}$. Da es mehr reelle Zahlen als Paare (i, j) gibt, gibt es zwei verschiedene reelle Parameter s, t mit $(i(s), j(s)) = (i(t), j(t)) =: (i, j)$. Nun gilt:

$$(x_i + x_j) + sx_ix_j = u(s) \in \mathbb{C}, \quad (x_i + x_j) + tx_ix_j = u(t) \in \mathbb{C}. \tag{3.18}$$

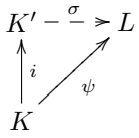
Dieses lineare Gleichungssystem für $x_i + x_j$ und x_ix_j hat eine eindeutige Lösung, weil die Determinante gleich $t - s \neq 0$ ist. Deshalb gilt

$$x_i + x_j, \quad x_ix_j \in \mathbb{C}. \tag{3.19}$$

Damit sind x_i und x_j die beiden Lösungen einer quadratischen Gleichung mit komplexen Koeffizienten. Wir wissen, daß diese quadratische Gleichung komplexe Lösungen besitzt. □

3.4 Fortsetzungen von Einbettungen

Es seien $i : K \to K'$ und $\psi : K \to L$ Körpererweiterungen. Eine Fortsetzung von ψ auf K' ist ein Homomorphismus $\sigma : K' \to L$ mit $\sigma \circ i = \psi$. Jede solche Fortsetzung ist K-linear. Umgekehrt ist jeder K-lineare Homomorphismus von Ringen $K' \to L$ eine Fortsetzung von ψ.



Satz 3.26 — *Es sei $K(a)/K$ eine einfache algebraische Erweiterung mit Minimalpolynom $f = \operatorname{minpol}_{a/K}$. Jede Fortsetzung einer gegebenen Einbettung $\psi : K \to L$ auf $K(a)$ bildet a auf eine Nullstelle von f in L ab. Umgekehrt gibt es zu jeder Nullstelle β*

von f in L genau eine Fortsetzung $\psi' : K(a) \to L$ mit $\psi'(a) = \beta$. Insbesondere ist die Anzahl der verschiedenen Fortsetzungen von ψ genau die Anzahl der verschiedenen Nullstellen von f in L.

Beweis. Da $f(a) = 0$, ist zunächst klar, daß jede Fortsetzung $\psi : K(a) \to L$ das Element a auf eine Nullstelle von f in L abbilden muß, und da $K(a)$ von a erzeugt ist, liegt ψ durch den Wert auf a fest.

Es sei nun umgekehrt eine Nullstelle $\beta \in L$ von f vorgegeben. Es ist $K(a) = K[X]/(f)$. Nach der universellen Eigenschaft des Polynomrings gibt es genau einen Homomorphismus $j : K[X] \to L$ mit $X \mapsto \beta$, der die Erweiterung $K \to L$ fortsetzt. Dabei geht f auf $f(\beta) = 0$. Insbesondere faktorisiert j nach der universellen Eigenschaft des Restklassenrings über einen Homomorphismus $\psi' : K(a) = K[X]/(f) \to L$. □

Satz 3.27 *(Existenz von Fortsetzungen) — Es sei L/K eine algebraische Erweiterung. Dann läßt sich jede Einbettung $j : K \to M$ in einen algebraisch abgeschlossenen Körper M zu einer Einbettung $i : L \to M$ fortsetzen.*

Beweis. Wir betrachten die Menge $X = \{(L', i')\}$ aller Paare aus einem Zwischenkörper L', $K \subset L' \subset L$, und einer Einbettung $i' : L' \to M$ mit $i'|_K = j$. Dann enthält X wenigstens das Element (K, j) und ist deshalb nicht leer. Die Menge X ist halbgeordnet durch die Relation

$$(L', i') \leq (L'', i'') :\Leftrightarrow L' \subset L'' \text{ und } i''|_{L'} = i'. \tag{3.20}$$

Ist nun $Y \subset X$ eine Kette, so setzen wir $L_Y := \bigcup_{L' \in Y} L'$ und definieren $i_Y : L_Y \to M$ durch $i_Y|_{L'} := i'$. Dann liegt das Paar (L_Y, i_Y) wieder in X und ist nach Konstruktion eine obere Schranke von Y. Mit anderen Worten: $(X, \leq)$ ist induktiv geordnet. Nach dem Zornschen Lemma existiert in X ein maximales Element (L_0, i_0).

Angenommen, die Inklusion $L_0 \subset L$ ist echt. Jedes Element $a \in L \setminus L_0$ ist algebraisch über K, also erst recht über L_0. Das Minimalpolynom g von a über L_0 besitzt in M eine Nullstelle, weil M algebraisch abgeschlossen ist. Folglich gibt es eine Fortsetzung $i_0' : L_0(a) \to M$ von i_0. Das Paar $(L_0(a), i_0')$ widerspräche der Maximalität von (L_0, i_0). Daher gilt in der Tat $L_0 = L$, und $i := i_0$ ist eine Fortsetzung von j, wie verlangt. □

Satz 3.28 *(Eindeutigkeit des algebraischen Abschlusses) — Es seien $i : K \to K'$ und $j : K \to K''$ algebraische Abschlüsse. Dann gibt es eine Fortsetzung $\psi : K' \to K''$ von j auf K', und jede solche Fortsetzung ist ein Isomorphismus.*

Beweis. Die Existenz von ψ ist eine Konsequenz des Satzes 3.27. Es sei nun $\psi : K' \to K''$ irgendeine Fortsetzung. Es ist nur zu zeigen, daß ψ surjektiv ist. Es sei $a \in K''$ vorgegeben mit Minimalpolynom h über K. Dann zerfällt h über K' vollständing in

Linearfaktoren $h = (X-a_1)\cdots(X-a_q)$. Es folgt $h = (X-\psi(a_1))\cdots(X-\psi(a_1))$ in $K''[X]$. Da a eine Nullstelle von h ist, gilt $a = \psi(a_i)$ für ein i. □

3.5 Endliche Körper

Satz 3.29 — *Es sei p eine Primzahl und $\overline{\mathbb{F}}_p$ ein algebraischer Abschluß von $\mathbb{F}_p$.*

1. *Für jedes $\ell \in \mathbb{N}$ gibt es in $\overline{\mathbb{F}}_p$ genau einen Unterkörper mit p^ℓ Elementen. Dieser wird mit $\mathbb{F}_{p^\ell}$ bezeichnet.*

2. *Ist K ein endlicher Körper der Charakteristik p und vom Grad ℓ über seinem Primkörper, so gilt $K \cong \mathbb{F}_{p^\ell}$.*

Beweis. Die Frobeniusabbildung $F : x \mapsto x^p$ ist ein Automorphismus von $\overline{\mathbb{F}}_p$. Dasselbe gilt dann für die ℓ-te Potenz F^ℓ. Wie wir wissen, ist die Menge $\mathbb{F}_{p^\ell}$ der Fixpunkte von F^ℓ ein Unterkörper von $\overline{\mathbb{F}}_p$. Nun besteht $\mathbb{F}_{p^\ell}$ genau aus den Elementen x mit der Eigenschaft $x^{p^\ell} = x$, also den Nullstellen des Polynoms $f = X^{p^\ell} - X$. Wegen $f' = -1$ hat f keine mehrfachen Nullstellen. Da $\overline{K}$ aber algebraisch abgeschlossen ist und f deshalb in Linearfaktoren zerfällt, hat f genau p^ℓ verschiedene Nullstellen. Folglich hat $\mathbb{F}_{p^\ell}$ genau p^ℓ Elemente.

Es sei nun K irgendein endlicher Körper der Charakteristik p und vom Grad ℓ über seinem Primkörper $\mathbb{F}_p$. Nach Satz 3.27 gibt es eine Einbettung $K \to \overline{\mathbb{F}}_p$. Die Einheitengruppe $K^\times$ hat die Ordnung $p^\ell - 1$. Für jedes Element $x \in K^\times$ gilt deshalb $x^{p^\ell-1} = 1$. Insbesondere gilt für jedes Element $x \in K$ die Gleichung $x^{p^\ell} = x$. Aber das bedeutet $K \subset \mathbb{F}_{p^\ell}$. Da die beiden Körper gleich viele Elemente enthalten, sind sie gleich. □

Satz 3.30 — *Es sei K ein Körper. Jede endliche Untergruppe $G \subset K^\times$ ist zyklisch.*

Beweis. Die Gruppe G ist offensichtlich abelsch. Der Exponent von G ist $e(G) = \max\{\mathrm{ord}(g) \mid g \in G\}$. Bekanntlich gilt für jede endliche abelsche Gruppe G' und jedes $g' \in G'$, daß $\mathrm{ord}(g') | e(G')$ (cf. Aufgabe 2.22). Für die Gruppe G heißt das, daß alle Gruppenelemente von G Nullstellen des Polynoms $X^{e(G)} - 1$ sind. Dieses Polynom hat höchstens $e(G)$ Nullstellen, d.h. $|G| \leq e(G)$. Da trivialerweise auch die umgekehrte Ungleichung besteht, gilt sogar Gleichheit. Folglich gibt es ein $g \in G$ mit $\mathrm{ord}(g) = |G|$, und dieses g erzeugt G. □

Folgerung 3.31 — *Ist K ein endlicher Körper, $|K| = p^\ell$, so ist $K^\times$ zyklisch von der Ordnung $p^\ell - 1$. Insbesondere gibt es ein Element $\theta \in K$ mit der Eigenschaft, daß $K = \mathbb{F}_p(\theta)$. Das Minimalpolynom von θ ist ein Teiler des Polynoms $x^{p^\ell-1} - 1$.*

Aufgaben zu den Grundbegriffen über Körper

Aufgabe 3.1 — Es sei K ein endlicher Körper. Dann hat ist $|K|$ eine Primzahlpotenz.

Aufgabe 3.2 — Es sei K ein Körper, G eine Gruppe und $G \times K \to K$ eine Gruppenwirkung mit der Eigenschaft, daß für jedes Gruppenelement $g \in G$ die Linksmultiplikation $\ell_g : K \to K$, $x \mapsto g.x$, ein Isomorphismus von Körpern ist. Man zeige, daß die Fixpunktmenge $K^G = \{x \in K \mid gx = x \text{ für alle } g \in G\}$ ein Unterkörper von K ist.

Aufgabe 3.3 — Die Gruppe $G = \mathbb{Z}/2 \times \mathbb{Z}/2$ operiert auf $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ durch

$$(\epsilon_1, \epsilon_2).(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) = a + (-1)^{\epsilon_1} b\sqrt{2} + (-1)^{\epsilon_2} c\sqrt{3} + (-1)^{\epsilon_1+\epsilon_2} d\sqrt{6}.$$

Bestimmen Sie die Fixkörper K^H für alle Untergruppen H von G.

Aufgabe 3.4 — Es sei K ein Körper. Die Körperautomorphismen $\varphi : K \to K$ bilden eine Gruppe $\mathrm{Aut}(K)$, die Automorphismengruppe von K. Man zeige:

1. $\mathrm{Aut}(\mathbb{Q}) = \{\mathrm{id}_{\mathbb{Q}}\}$.
2. $\mathrm{Aut}(\mathbb{R}) = \{\mathrm{id}_{\mathbb{R}}\}$.

Wir werden später sehen, daß $\mathrm{Aut}(\mathbb{C})$ überabzählbar ist.
[Hinweis für Teil 2.: Wie kann man die Eigenschaft $c > 0$ algebraisch charakterisieren? Zeige dann: Für reelle Zahlen $a > b$ gilt $\varphi(a) > \varphi(b)$. Insbesondere ist φ stetig.]

Aufgabe 3.5 — Es sei K ein Körper und $K(X)$ der Funktionenkörper in einer Unbestimmten. Zeigen Sie, daß für jede Matrix $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(K)$ die Abbildung $X \mapsto (aX + b)/(cX + d)$ einen eindeutig bestimmten K-linearen Automorphismus $\varphi_A \in \mathrm{Aut}(K(X))$ definiert und daß die Abbildung $\varphi : \mathrm{GL}_2(K) \to \mathrm{Aut}(K(X))$ ein Gruppenhomomorphismus ist.

Aufgaben zu algebraischen Erweiterungen

Aufgabe 3.6 — Bestimmen Sie die Minimalpolynome über $\mathbb{Q}$ der folgenden komplexen Zahlen $\sqrt{2} + 3$, $\sqrt{2} + \sqrt{3}$, $\sqrt[3]{5}^2 + \sqrt[3]{5} + 1$.

Es sei L/K eine endliche Körpererweiterung und $a \in L$. Dann definiert a durch Linksmultiplikation eine K-lineare Abbildung $\ell_a : L \to L$, $x \mapsto ax$. Wir bezeichnen mit $\chi_{a/L/K}$ das charakteristische Polynom von ℓ_a.

Aufgabe 3.7 — 1. Zeigen sie, daß $X^2 - 3 \in \mathbb{Q}(\sqrt{2})[X]$ irreduzibel ist. Insbesondere hat der Körper $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ den Grad 4 über $\mathbb{Q}$.
2. Berechnen Sie das charakteristische Polynom von $\ell_a : K \to K$ für $a = \sqrt{2}$ und $a = \sqrt{2} + \sqrt{3}$.

Aufgabe 3.8 — Es sei L/K eine endliche Erweiterung. Zeigen Sie: Das Minimalpolynom von $a \in L$ über K ist gleich dem Minimalpolynon von $\ell_a : L \to L$ im Sinne der linearen Algebra. Falls $L = K(a)$, gilt $\mathrm{minpol}_{a/K} = \chi_{a/K(a)/K}$.

Aus den beiden vorstehenden Aufgaben folgt, daß $\mathrm{minpol}_{a/K}$ ein Teiler von $\chi_{a/L/K}$ ist. Das läßt sich verschärfen.

Aufgabe 3.9 — Es seien $M/L/K$ endliche Erweiterungen und $a \in L$. Dann gilt $\chi_{a/M/K} = \chi_{a/L/K}^{[M:L]}$. Insbesondere gilt $\chi_{a/L/K} = \mathrm{minpol}_{a/K}^{[L:K(a)]}$.
[Hinweis: Wählen Sie zunächst eine K-Basis von L und dann eine L-Basis von M].

Eine komplexe Zahl heißt algebraisch oder transzendent, wenn sie algebraisch oder transzendent über $\mathbb{Q}$ ist. Die folgenden Aufgaben führen auf die Aussage, daß es ziemlich viele transzendente Zahlen gibt. Die Beweismethode geht auf Cantor zurück:

Aufgabe 3.10 (Euklid) — Es sei K ein Körper. Man zeige, daß es in $K[X]$ unendlich viele irreduzible normierte Polynome gibt.

Aufgabe 3.11 — Es sei K ein Körper und $\overline{K}$ ein algebraischer Abschluß von K. Man zeige:

1. Ist K endlich, so ist $\overline{K}$ abzählbar unendlich.
2. Ist K unendlich, so ist $|K| = |\overline{K}|$.
3. Es gibt reelle transzendente Zahlen.

Hinweis zu 1 und 2: Es sei $F \subset K[X]$ die Menge der normierten irreduziblen Polynome und $m : \overline{K} \to F$ die Abbildung $\alpha \mapsto \mathrm{minpol}_{\alpha/K}$.

Aufgaben zu endlichen Körpern

Aufgabe 3.12 — Die Inklusion $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^m}$ von Unterkörpern in $\overline{\mathbb{F}}_p$ besteht genau dann, wenn $n|m$.

Aufgabe 3.13 — Es sei p eine Primzahl, n teilerfremd zu p und $m = p^\ell n$.
1. Jede m-te Einheitswurzel in $\overline{\mathbb{F}}_p$ auch schon eine n-te Einheitswurzel.
2. Es gibt genau n verschiedene n-te Einheitswurzeln in $\overline{\mathbb{F}}_p$.
3. Es sei $\zeta \in \overline{\mathbb{F}}_p$ eine primitive n-te Einheitswurzel und $\mathbb{F}_p(\zeta) = \mathbb{F}_{p^\ell} \subset \overline{\mathbb{F}}_p$. Dann ist ℓ die Ordnung von p in $(\mathbb{Z}/n)^\times$.
4. Mit den Bezeichnungen aus 3: Das Kreisteilungspolynom Φ_n zerfällt in $\mathbb{F}_p[X]$ in ein Produkt von Polynomen vom Grad ℓ.
5. Zerlegen Sie $\Phi_7 \in \mathbb{F}_2[X]$ in irreduzible Faktoren.

§4 Galoistheorie

4.1 Separabilität

Definition 4.1 — Es sei K ein Körper. $f \in K[X]$ heißt separabel, wenn f in einem algebraischen Abschluß von K nur einfache Nullstellen hat. Andernfalls heißt f inseparabel.

Es sei L/K eine Körpererweiterung, in der das nichtkonstante Polynom $f \in K[X]$ eine Nullstelle α besitzt. Bekanntlich ist α genau dann eine mehrfache Nullstelle, wenn $f'(\alpha) = 0$ (Kriterium von Hudde[11]). In diesem Falle haben f und f' in $L[X]$ einen nichtkonstanten Faktor gemeinsamen. Aber der größte gemeinsame Teiler läßt sich mit dem euklidischen Algorithmus bereits in $K[X]$ berechnen. Damit erhält man das Kriterium:

Lemma 4.2 — *Ein Polynom $f \in K[X] \setminus \{0\}$ ist genau dann separabel, wenn der größte gemeinsame Teiler von f und f' konstant ist.* □

Satz 4.3 — *Es sei $f \in K[X]$ ein normiertes irreduzibles Polynom vom Grad $n > 0$.*

1. *Wenn $\mathrm{char}(K) = 0$, ist f separabel.*
2. *Wenn $\mathrm{char}(K) = p > 0$, so sei $e \in \mathbb{N}_0$ maximal mit der Eigenschaft, daß $f(X) = g(X^{p^e})$ für ein Polynom g. Dann ist g normiert, irreduzibel und separabel, und f ist genau dann separabel, wenn $e = 0$.*

Beweis. Es sei f ein normiertes irreduzibles Polynom von positivem Grad. Wenn f und f' über einem algebraischen Abschluß von K eine gemeinsame Nullstelle haben, müssen sie schon in $K[X]$ einen nicht konstanten gemeinsamen Teiler haben. Da $\mathrm{grad}(f') < \mathrm{grad}(f)$ und da f irreduzibel, ist dies nur möglich, wenn $f' = 0$. In Charakteristik 0 ist dies ausgeschlossen, weil f nicht konstant ist.

Es sei also $p = \mathrm{char}(K) > 0$. Mit dem Ansatz

$$f = X^n + f_{n-1}X^{n-1} + \ldots + f_1X + f_0$$

folgt aus der Annahme

$$0 = f' = nX^{n-1} + (n-1)f_{n-1}X^{n-2} + \ldots + f_1,$$

daß $p|k$ für alle k mit $f_k \neq 0$. Mit $m := n/p$ hat man daher

$$f = (X^p)^m + f_{(m-1)p}(X^p)^{m-1} + \ldots + f_pX^p + f_0.$$

Das bedeutet: $f(X) = h(X^p)$ für ein geeignetes Polynom h. Es ist klar, daß h irreduzibel und normiert ist. Ist h nicht separabel, hat man $h(X) = k(X^p)$ mit geeignetem

[11] Johan van Waveren Hudde ⋆23. April 1628 †15. April 1704

Polynom k und somit $f(X) = k(X^{p^2})$. Iteriert man das Argument, so kommt man nach endlich vielen Schritten zu $f(X) = g(X^{p^e})$ mit separablem $g \in K[X]$. $\square$

Beispiele 4.4 — 1. Es sei p eine Primzahl. Wir betrachten über dem Körper $\mathbb{F}_p(t)$ das Polynom $f = X^p - t$. Nach dem Eisensteinkriterium ist f irreduzibel, denn t ist ein Primelement im faktoriellen Ring $\mathbb{F}_p[t]$. Offensichtlich ist f inseparabel.
2. Das Polynom ist $X^7 - 3 \in \mathbb{F}_7[X]$ ist nicht einmal irreduzibel: Da $3^7 \equiv 3 \mod 7$, gilt $X^7 - 3 = X^7 - 3^7 = (X - 3)^7$.

Definition 4.5 — Es sei L/K eine algebraische Körpererweiterung und $\overline{L}/L$ ein algebraischer Abschluß.

1. $a \in L$ ist separabel über K, wenn das Minimalpolynom von a separabel ist, und andernfalls inseparabel. a ist rein inseparabel, wenn a die einzige Nullstelle von $\mathrm{minpol}_{a/K}$ in $\overline{L}$ ist.

2. L ist separabel über K, wenn alle Elemente von L separabel über K sind, und andernfalls inseparabel. L ist rein inseparabel über K, wenn alle Elemente von L rein inseparabel über K sind.

Bemerkung 4.6 — Die Definition bringt es sich mit sich, daß ein Element $a \in K$ zugleich separabel und rein inseparabel über K ist, denn das Minimalpolynom $X - a$ hat genau eine Nullstelle. Das klingt auf den ersten Blick etwas unangenehm, vermeidet aber Fallunterscheidungen in den Formulierungen späterer Sätze.

Definition 4.7 — Ein Körper K heißt vollkommen oder perfekt, wenn jedes normierte irreduzible Polynom über K separabel ist, oder dazu äquivalent, wenn jede algebraische Erweiterung von K separabel ist.

Satz 4.8 (Kriterien für Vollkommenheit) —

1. *Körper der Charakteristik 0 sind vollkommen.*

2. *Ein Körper K der Charakteristik $p > 0$ ist genau dann vollkommen, wenn die Frobeniusabbildung $F : K \to K, x \mapsto x^p$, surjektiv ist, d.h. wenn jedes Element $\alpha \in K$ eine p-te Wurzel in K besitzt.*

Insbesondere sind endliche Körper und algebraisch abgeschlossene Körper vollkommen.

Beweis. Die erste Aussage ist trivial. Zur zweiten: Wenn F nicht surjektiv ist und $a \in K \setminus K^p$, $K^p := F(K)$, dann ist $X^p - a$ ein inseparables irreduzibles Polynom. Es sei umgekehrt F surjektiv. Angenommen, f ist ein inseparables irreduzibles Polynom. Es gibt dann ein Polynom $g = g_m X^m + \ldots + g_1 X + g_0$ mit $f(X) = g(X^p)$. Es sei

$h_i := F^{-1}(g_i) = g_i^{1/p}$. Mit $h = X^m + \ldots + h_1 X + h_0$ folgt: $f(X) = g(X^p) = h(X)^p$, im Widerspruch zur Irreduzibilität von f. □

Satz 4.9 — *Es sei K ein endlicher Körper der Charakteristik p. Dann gilt $K = \mathbb{F}_p(a)$ mit einem separablen Element a.*

Beweis. Nach Satz 3.30 ist die Einheitengruppe eines endlichen Körpers zyklisch: $K^\times \cong \mathbb{Z}/(p^\ell - 1)$, $\ell = [K : \mathbb{F}_p]$. Ist a ein Gruppenerzeuger, so hat man $K = \{0\} \cup \{a^i \mid i = 1, \ldots, p^\ell - 1\}$. Außerdem ist a Nullstelle des Polynoms $f := X^{p^\ell} - X$. Da $f' = -1$, hat f keine mehrfache Nullstellen und somit das Minimalpolynom von a, das ein Teiler von f ist, auch nicht. □

Satz 4.10 (Satz vom primitiven Element) — *Es sei $L = K(a_1, a_2, \ldots, a_n)/K$ eine algebraische Erweiterung mit separablen Elementen $a_1, \ldots, a_{n-1}$. Dann ist L/K eine einfache Erweiterung, d.h. es gibt ein Element $c \in L$ mit $L = K(c)$. Sind alle Elemente $a_1, \ldots, a_n$ separabel, so kann auch c separabel gewählt werden.*

Beweis. Wenn K endlich ist, ist auch L endlich und wird von jedem Erzeuger θ der zyklischen Einheitengruppe $L^\times$ erzeugt. Wir können deshalb im Folgenden ohne Einschränkung annehmen, daß K unendlich viele Elemente hat. Außerdem genügt es, den Fall $n = 2$ zu betrachten, der allgemeine Fall folgt induktiv.

Wir betrachten also eine algebraische Erweiterung $L = K(a, b)/K$ und nehmen an, daß a separabel ist. Es sei $\overline{K}$ ein algebraischer Abschluß von $K(a, b)$. Wir bezeichnen mit $a_1 = a, a_2, \ldots, a_n$ und $b_1 = b, b_2, \ldots, b_\ell$ die paarweise verschiedenen Nullstellen der Minimalpolynome f von a bzw. g von b. Wir betrachten für ein noch näher zu bestimmendes Element $t \in K$ das Element $c := at + b \in K(a, b)$. Dann haben die Polynome $f(X)$ und $g(c - tX)$ die gemeinsame Nullstelle a. Die weiteren Nullstellen von $f(X)$ sind $a_2, \ldots, a_n$, die weiteren Nullstellen von $g(c - tX)$ die Elemente $a + (b - b_j)/t$. Wir wählen jetzt $t \neq 0$ so, daß $(a_i - a)t \neq b - b_j$ für alle $i > 1$ und alle j. Dies ist möglich, weil $|K| = \infty$ und weil durch diese Bedingung nur endlich viele Werte von t ausgeschlossen sind.

Nun ist der größte gemeinsame Teiler von $f(X)$ und $g(c - tX)$ in $K(c)[X]$ genau $X - a$. Deshalb läßt sich $X - a$ als Linearkombination von $f(X)$ und $g(c - tX)$ mit Koeffizienten in $K(c)[X]$ schreiben. Insbesondere liegt a in $K(c)$, und damit auch $b = c - at$. Das zeigt: $K(a, b) \subset K(c)$. Die umgekehrte Inklusion ist trivial.

Wir nehmen jetzt an, sowohl a als auch b seien separabel. Dann kann man t auch noch so wählen, daß $(a_i - a_{i'})t \neq b_j - b_{j'}$ falls $i \neq i'$ oder $j \neq j'$. Dann sind alle Elemente $c_{ij} = a_i + tb_j$ paarweise verschieden. Das Polynom

$$h(X) = \prod_i \prod_j (X - c_{ij})$$

ist symmetrisch unter Permutation der a_i untereinander und der b_j untereinander. Nach dem Hauptsatz über symmetrische Polynome lassen sich die Koeffizienten von h polynomiell durch die Koeffizienten von f und g ausdrücken und liegen deshalb in K. Deshalb ist das Minimalpolynom von c ein Teiler von h. Nach Konstruktion sind die Nullstellen von h paarweise verschieden. Deshalb ist das Minimalpolynom von c separabel. □

Definition 4.11 — Es sei L/K eine endliche Erweiterung und $K \to \overline{K}$ ein algebraischer Abschluß. Weil alle algebraischen Abschlüsse von K isomorph sind, hängt die Anzahl der Fortsetzungen $L \to \overline{K}$ nicht von der Wahl von $\overline{K}$ ab. Diese Zahl heißt der Separabilitätsgrad von L/K und wird mit $[L : K]_s$ bezeichnet.

Satz 4.12 — *Es sei $L = K(\alpha)/K$ eine einfache algebraische Erweiterung.*

1. *Wenn $\mathrm{char}(K) = 0$, ist $[L : K] = [L : K]_s$.*
2. *Wenn $\mathrm{char}(K) = p > 0$, so ist $[L : K] = p^e[L : K]_s$, wobei $e \in \mathbb{N}_0$ maximal mit der Eigenschaft ist, daß das Minimalpolynom von α die Form $g(X^{p^e})$ hat.*

Beweis. Es sei f das Minimalpolynom von α über K und $n = [L : K] = \mathrm{grad}(f)$. Wenn α separabel ist, hat das Minimalpolynom n verschiedene Nullstellen in $\overline{K}$. Deshalb gilt in diesem Falle $[L : K]_s = n$. Wenn α nicht separabel ist, hat K positive Charakteristik p. Mit e und g wie im Satz gilt also $f(X) = g(X^{p^e})$, und g ist das Minimalpolynom von α^{p^e}. Mit $m = \mathrm{grad}(g)$ gilt $n = mp^e$, und da g separabel ist, gibt es m verschiedene Fortsetzungen $\varphi_i : K(\alpha^{p^e}) \to \overline{K}$. Das Minimalpolynom von α über $K(\alpha^{p^e})$ ist $X^{p^e} - \alpha^{p^e}$. Es hat in $\overline{K}$ genau eine Nullstelle. Deshalb setzt sich jedes φ_i eindeutig auf $K(\alpha)$ fort. Darum ist $[L : K]_s = m = n/p^e$. □

23. Mai 2008

Satz 4.13 — *Es seien $M/L/K$ endliche Erweiterungen. Dann gilt*

$$[M : K]_s = [M : L]_s[L : K]_s.$$

Beweis. Es sei ein algebraischer Abschluß $K \to \overline{K}$ gewählt. Es bezeichne $F_{M/K}$ die Menge der Fortsetzungen auf M und $F_{L/K}$ die Menge der Fortsetzungen auf L. Die Einschränkung $\psi \mapsto \psi|_L$ definiert eine Abbildung $E : F_{M/K} \to F_{L/K}$. Da sich jede Fortsetzung auf L zu einer Fortsetzung auf M fortsetzen läßt, ist E surjektiv. Es sei sei nun eine Fortsetzung $\varphi : L \to \overline{K}$ fixiert. Alle Elemente in $\overline{K}$ sind algebraisch über K, also erst recht über L, und da $\overline{K}$ algebraisch abgeschlossen ist, ist $\overline{K}$ auch ein algebraischer Abschluß von L. Nach Definition gibt es genau $[M : L]_s$ verschiedene Fortsetzungen von φ auf M. Mit anderen Worten: $|E^{-1}(\varphi)| = [M : L]_s$. Es folgt: $[M : K]_s = |F_{M/K}| = \sum_{\varphi \in F_{L/K}} [M : L]_s = [M : L]_s[L : K]_s$. □

Satz 4.14 — *Für jede endliche Erweiterung L/K ist $[L:K]_s$ ein Teiler von $[L:K]$. Die folgenden Aussagen sind äquivalent:*

1. $[L:K]_s = [L:K]$.
2. *L/K ist separabel.*
3. *L wird von separablen Elementen erzeugt.*
4. *$L = K(a)$ für ein separables Element a.*

Beweis. Wir wählen $a \in L \setminus K$ und betrachten die Erweiterungen $K \to K(a) \to L$. Nach den Sätzen 4.12 und 4.13 und durch Induktion über den Grad ergibt sich zunächst die Teilbarkeitsrelation

$$[L:K]_s = [L:K(a)]_s[K(a):K]_s \mid [L:K(a)][K(a):K] = [L:K]$$

und damit die erste Behauptung.
$1 \Rightarrow 2$: Wenn die äußeren Terme gleich sind, so muß auch $[K(a):K]_s = [K(a):K]$ gelten, d.h. a ist separabel. Die Implikation $2 \Rightarrow 3$ ist trivial.
$3 \Rightarrow 4$: Es seien $a_1, \dots a_n$ separable Elemente mit $L = K(a_1, \dots, a_n)$. Gemäß dem Satz vom primitiven Element 4.10 gibt es ein separables $a \in L$ mit $L = K(a)$.
$4 \Rightarrow 1$: Ist schließlich $L = K(a)$ für ein separables Element, so gilt $[L:K]_s = [L:K]$ nach Satz 4.12. □

Satz 4.15 — *Es seien $M/L/K$ algebraische Erweiterungen.*

1. *L/K ist genau dann separabel, wenn L als K-Erweiterung von separablen Elementen erzeugt wird.*
2. *M/K ist genau dann separabel, wenn L/K und M/L separabel sind.*

Beweis. Es sei $S \subset L$ ein Erzeugendensystem aus separablen Elementen und $a \in L$ ein beliebiges Element. Dann gibt es eine endliche Teilmenge $S' \subset S$ mit $a \in K(S') \subset L$. Nach Konstruktion ist $[K(S'):K] < \infty$, und nach Satz 4.14 folgt, daß alle Elemente in $K(S')$ separabel über K sind. □

Satz 4.16 — *Es sei L/K eine algebraische Körpererweiterung. Die folgenden Aussagen sind äquivalent:*

1. *Jedes über K separable Element von L liegt in K.*
2. *L/K ist rein inseparabel.*
3. *L wird als Erweiterung von K von rein inseparablen Elementen erzeugt.*
4. $[L:K]_s = 1$.

Beweis. Falls $K = L$, ist der Satz aus trivialen Gründen richtig. Wir nehmen also an, daß $[L : K] > 1$. Zunächst gilt $1 \Rightarrow 2$: Es sei $a \in L \setminus K$ mit Minimalpolynom f. Nach Annahme ist a inseparabel über K. Deshalb ist $p = \mathrm{char}(K) > 0$ und es gibt ein $e > 0$ und ein separables Polynom g mit $f(X) = g(X^{p^e})$. Nun ist a^{p^e} separabel über K und liegt deshalb schon selbst in K, d.h. g ist linear und somit a rein inseparabel.
Die Implikation $2 \Rightarrow 3$ ist trivial.
$3 \Rightarrow 4$: Es sei $L = K(S)$ mit einer Menge S von rein inseparablen Elementen. Sind $f_1, f_2 : L \to \overline{K}$ verschiedene Einbettungen, so muß es ein $\alpha \in S$ mit $f_1(\alpha) \neq f_2(\alpha)$ geben. Aber $f_1(\alpha)$ und $f_2(\alpha)$ sind Nullstellen des Minimalpolynoms von α in $\overline{K}$, also gleich. Widerspruch.
$4 \Rightarrow 1$: Es sei $a \in L$ über K separabel. Da sich jede Einbettung $K(a) \to \overline{K}$ auf L fortsetzen läßt, hat man $[L : K]_s \geq [K(a) : K] > 1$, im Widerspruch zur Annahme. □

Satz 4.17 — *Es sei L/K eine algebraische Erweiterung. Dann gibt es genau einen Zwischenkörper $M \subset L$ mit der Eigenschaft, daß M/K separabel und L/M rein inseparabel ist.*

Beweis. Es sei $M \subset L$ die Menge aller über K separablen Elemente. Nach Satz 4.15 besteht $K(M)$ nur aus separablen Elementen, ist also gleich M. Es sei nun $a \in L \setminus M$ mit Minimalpolynom $f(X) = g(X^{p^e})$ und separablem g. Dann ist $b := a^{p^e}$ separabel über M und deshalb nach Satz 4.15 auch separabel über K. Nach Konstruktion liegt b schon in M, und f hat die Form $f(X) = X^{p^e} - b$. Das zeigt, daß a rein inseparabel über M ist. □

Definition 4.18 — Der Zwischenkörper M im vorstehenden Satz heißt die separable Hülle von K in L. Die separable Hülle von K in einem algebraischen Abschluß $\overline{K}$ heißt separabler Abschluß von K und wird mit K^s bezeichnet. In der üblichen Weise zeigt man, daß der separable Abschluß bis auf (nicht eindeutigen) Isomorphismus eindeutig ist.

4.2 Normale Erweiterungen und Zerfällungskörper

Definition 4.19 — Es sei L/K eine Körpererweiterung.

1. L/K ist normal, wenn jedes irreduzible Polynom $f \in K[X]$, das in L wenigstens eine Nullstelle besitzt, über L vollständig in Linearfaktoren zerfällt.
2. L/K ist Zerfällungskörper einer Menge $\mathcal{F} \subset K[X]$ von Polynomen, wenn jedes $f \in \mathcal{F}$ über L vollständig in Linearfaktoren zerfällt und wenn L von den Nullstellen der Polynome $f \in \mathcal{F}$ erzeugt wird.

26. Mai 2008

Satz 4.20 (Existenz und Eindeutigkeit des Zerfällungskörpers) — *Es sei $\mathcal{F} \subset K[X]$ eine Menge von Polynomen.*

1. *Es gibt einen Zerfällungskörper L/K von $\mathcal{F}$.*

2. *Zu je zwei Zerfällungskörpern $i_1 : K \to L_1$ und $i_2 : K \to L_2$ gibt es einen Homomorphismus $\varphi : L_1 \to L_2$ mit $\varphi \circ i_1 = i_2$, und jede solche Einbettung ist ein Isomorphismus.*

Beweis. 1. Es sei $i : K \to \overline{K}$ ein algebraischer Abschluß und $L \subset \overline{K}$ der Körper, der von den Nullstellen aller $f \in \mathcal{F}$ erzeugt wird. Offensichtlich ist L ein Zerfällungskörper von $\mathcal{F}$.
2. Zur Existenz von φ: Wir nehmen wieder mit transfiniter Induktion (= Zornsches Lemma) an, (L_0, φ_0) sei ein maximales Paar aus einem Zwischenkörper $L_0 \subset L_1$ mit einer Fortsetzung $\varphi_0 : L_0 \to L_2$ der Einbettung i_2. Falls $L_0 \neq L_1$, gibt es ein $f \in \mathcal{F}$ und eine Nullstelle $a \in L_1$ von f, die nicht in L_0 liegt. Dann ist minpol_{a/L_0} ein Teiler von f und hat deshalb in L_2 Nullstellen. Folglich läßt sich φ_0 zu einer Einbettung von $L_0(a)$ in L_1 fortsetzen, im Widerspruch zur Maximalität von (L_0, φ_0). Deshalb ist $L_0 = L_1$. Zur Surjektivität: Es sei $\varphi : L_1 \to L_2$ gegeben, $f \in \mathcal{F}$ und $b \in L_2$ eine Nullstelle von f. Nun zerfällt f über L_1 in Linearfaktoren: $f(X) = (X - a_1) \cdots (X - a_n) \in L_1[X]$. Es folgt: $f(X) = (X - \varphi(a_1)) \cdots (X - \varphi(a_n))$ Folglich ist $b \in \{\varphi(a_1), \ldots, \varphi(a_n)\}$. Da L_1 von allen Nullstellen der Polynome $f \in \mathcal{F}$ erzeugt wird, und diese, wie gerade gezeigt, im Bild von φ liegen, ist φ surjektiv. □

Beispiel 4.21 — Ist ein Polynom $f \in K[X]$ vorgegeben, läßt sich der Grad des Zerfällungskörpers nur durch eine Einzeluntersuchung angeben, wie die beiden folgenden Beispiele zeigen. Wir betrachten die ähnlich aussehenden Polynome $f = X^6 - 3$ und $g = X^6 + 3$ in $\mathbb{Q}[X]$. Nach dem Eisensteinkriterium sind beide irreduzibel.

1. Es sei $L = \mathbb{Q}(\alpha)$ mit $\alpha = \sqrt[6]{3}$. In $L[X]$ zerfällt f in vier Faktoren:

$$X^6 - 3 = (X - \alpha)(X + \alpha)(X^2 + \alpha X + \alpha^2)(X^2 - \alpha X + \alpha^2).$$

Die beiden quadratischen Faktoren können über L nicht weiter zerfallen, weil die Gleichung $f = 0$ die Lösungen $\alpha\rho^k$, $k = 0, \ldots, 5$ mit $\rho = \exp(2\pi i/6)$ hat, von denen nur α und $-\alpha = \alpha\rho^3$ reell sind. Adjungiert man an L eine Nullstelle β von $X^2 - \alpha X + \alpha^2$, etwa $M := L(\beta)$, so zerfällt dieses quadratische Polynom in die Faktoren $(X - \beta)(X - \alpha + \beta)$, aber auch das andere zerfällt und man erhält insgesamt die Zerlegung

$$X^6 - 3 = (X - \alpha)(X + \alpha)(X - \beta)(X + \beta)(X - \alpha + \beta)(X + \alpha - \beta)$$

über M. Es gilt $[M : \mathbb{Q}] = [M : L][L : \mathbb{Q}] = 2 \cdot 6 = 12$.

2. Völlig anders ist die Situation im Falle von g: Ist $\gamma \in \mathbb{C}$ eine Nullstelle von g, so gilt für $\omega := (\gamma^3 + 1)/2$, daß $\omega \neq -1$, aber

$$\omega^3 = \frac{1}{8}(\gamma^9 + 3\gamma^6 + 3\gamma^3 + 1) = \frac{1}{8}(-3\gamma^3 + 3 \cdot (-3) + 3\gamma^3 + 1) = -1.$$

Deshalb ist $\omega \in \mathbb{Q}(\gamma)$ eine primitive sechste Einheitswurzel, und g hat in $\mathbb{Q}(\gamma)$ sechs Nullstellen:

$$\gamma,\ \gamma\omega = \frac{\gamma^4+\gamma}{2},\ \gamma\omega^2 = \frac{-\gamma+\gamma^4}{2},\ \gamma\omega^3 = -\gamma,\ \gamma\omega^4 = -\frac{\gamma^4+\gamma}{2},\ \gamma\omega^5 = \frac{\gamma-\gamma^4}{2}.$$

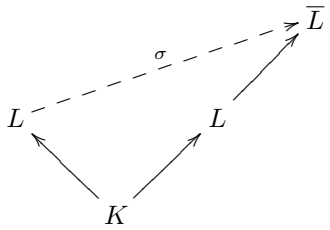
Deshalb ist $\mathbb{Q}(\gamma)$ schon der Zerfällungskörper von g, und $[\mathbb{Q}(\gamma) : \mathbb{Q}] = 6$.

Satz 4.22 (Normalitätskriterium) — *Die folgenden Aussagen über eine algebraische Erweiterung L/K sind äquivalent:*

1. *L/K ist normal.*
2. *L/K ist Zerfällungskörper einer Menge $\mathcal{F} \subset K[X]$.*
3. *Jede K-lineare Einbettung $\sigma : L \to \overline{L}$ in einen algebraischen Abschluß $\overline{L}$ von L bildet L in sich ab.*

In diesem Falle ist jede Abbildung $\sigma : L \to L$ wie in Aussage 3 ein Isomorphismus.

Beweis. $1 \Rightarrow 2$. Es sei $S \subset L$ ein Erzeugendensystem von L/K und $\mathcal{F}$ die Menge der Minimalpolynome der Elemente aus S. Dann hat jedes Polynom aus $\mathcal{F}$ nach Konstruktion eine Nullstelle in L und zerfällt nach Annahme über L vollständig in Linearfaktoren. Außerdem sind die Nullstellen der Polynome $f \in \mathcal{F}$ ein Erzeugendensystem. Nach Definition ist L/K ein Zerfällungskörper von $\mathcal{F}$.
$2 \Rightarrow 3$. Es sei ein algebraischer Abschluß $j : L \to \overline{L}$ gewählt und $\sigma : L \to \overline{L}$ eine K-lineare Fortsetzung:



Dann bildet σ jede Nullstelle eines Polynoms f in eine ebensolche Nullstelle ab. Alle diese Nullstellen liegen in L. Deshalb liegen die Bilder aller Nullstellen aller $f \in \mathcal{F}$ wieder in L. Da L außerdem von diesen Nullstellen erzeugt wird, gilt $\sigma(L) \subset L$.
$3 \Rightarrow 1$: Es sei $a \in L$ und $b \in \overline{L}$ eine Nullstelle des Minimalpolynoms von a. Dann gibt es eine K-lineare Einbettung $\psi : K(a) \to \overline{L}$ mit $\psi(a) = b$. Wir setzen diese zu einer Einbettung $\sigma : L \to \overline{L}$ fort. Nach Annahme gilt $\sigma(L) \subset L$, also erst recht $b = \sigma(a) \in L$. Das zeigt, daß L normal ist.

Die Schlußbehauptung folgt aus dem Eindeutigkeitssatz 4.20 für Zerfällungskörper. □

Satz 4.23 (Normale Hülle) — *Es sei L/K eine algebraische Erweiterung. Dann gibt es eine algebraische Erweiterung N/L mit der Eigenschaft, daß N/K normal ist und daß N der kleinste Zwischenkörper von $\overline{L}/L$ mit dieser Eigenschaft ist. Wenn L/K*

eine endliche Erweiterung ist, so ist auch N/K endlich. N/L heißt normale Hülle von L/K.

Beweis. Es sei $L \to \overline{L}$ ein algebraischer Abschluß, $S \subset L$ ein Erzeugendensystem von L/K und $\mathcal{F} = \{\mathrm{minpol}_{\alpha/K} \mid \alpha \in S\} \subset K[X]$. Es sei $N \subset \overline{L}$ der von allen Nullstellen der Polynome $f \in \mathcal{F}$ erzeugte Körper. Dann ist N normal über K und enthält L und ist der kleinste Unterkörper in $\overline{L}$ mit diesen beiden Eigenschaften. Wenn L/K eine endliche Erweiterung ist, kann S endlich gewählt werden. Es folgt $|\mathcal{F}| < \infty$ und $[N : K] < \infty$. □

Wie üblich zeigt man, daß die normale Hülle N/L einer algebraischen Erweiterung L/K bis auf (nicht eindeutigen) L-linearen Isomorphismus eindeutig ist.

4.3 Galoiserweiterungen

Definition 4.24 — Es sei L ein Körper. Die Menge der Automorphismen $\sigma : L \to L$ bildet mit der Komposition als Verknüpfung eine Gruppe $\mathrm{Aut}(L)$. Es sei $K \subset L$ ein Unterkörper. $\sigma : L \to L$ ist ein *relativer Automorphismus* von L/K, wenn $\sigma|_K = \mathrm{id}_K$. Die Menge der relativen Automorphismen ist eine Untergruppe $\mathrm{Aut}(L/K) < \mathrm{Aut}(L)$.

Lemma 4.25 (Dirichlet) — *Es seien $\sigma_1, \ldots, \sigma_n : \Gamma \to M^\times$ paarweise verschiedene Gruppenhomomorphismen von einer Gruppe Γ in die Einheitengruppe eines Körpers M. Dann sind $\sigma_1, \ldots, \sigma_n$ linear unabhängige Elemente im M-Vektorraum $\mathrm{Abb}(\Gamma, M)$ aller Abbildungen von Γ nach M. Mit anderen Worten: Sind $\mu_1, \ldots, \mu_n \in M$ mit der Eigenschaft, daß*

$$\mu_1\sigma_1(x) + \ldots + \mu_n\sigma_n(x) = 0$$

für alle $x \in \Gamma$, dann gilt $\mu_1 = \ldots = \mu_n = 0$.

Beweis. Es sei k minimal gewählt mit der Eigenschaft, daß (nach eventuell notwendigem Umnumerieren) die Homomorphismen $\sigma_1, \ldots, \sigma_k$ linear abhängig sind. Da alle $\sigma_i \neq 0$ sind, ist $k \geq 2$. Es gibt nun $\mu_1, \ldots, \mu_k \in M^\times$ mit $\sum_{i=1}^k \mu_i\sigma_i(x) = 0$ für alle $x \in \Gamma$. Da $\sigma_1 \neq \sigma_2$, gibt es ein $y \in \Gamma$ mit $\sigma_1(y) \neq \sigma_2(y)$. Nun bestehen die Relationen

$$0 = \sum_{i=1}^k \mu_i\sigma_i(yx) = \sum_{i=1}^k \sigma_i(y)\mu_i\sigma_i(x). \tag{4.1}$$

Durch Subtraktion der Relation

$$0 = \sigma_1(y)\sum_{i=1}^k \mu_i\sigma_i(x) \tag{4.2}$$

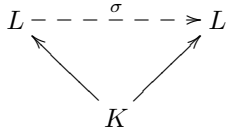
erhält man

$$0 = \sum_{i\geq 2}(\sigma_1(y) - \sigma_i(y))\mu_i\sigma_i(x) \quad \text{für alle } x \in K. \tag{4.3}$$

Da $\sigma_1(y) - \sigma_2(y) \neq 0$ ist dies eine nichttriviale Relation zwischen den Homomorphismen $\sigma_2 \ldots, \sigma_k$, im Widerspruch zur Minimalität von k. □

Im folgenden wollen wir das Lemma auf paarweise verschiedene Körperhomomorphismen $\sigma_1, \ldots, \sigma_n : K \to M$ anwenden: Die Einschränkungen der σ_i auf die Einheitengruppen sind Gruppenhomomorphismen. Deshalb ist das Lemma anwendbar und zeigt, daß die σ_i linear unabhängig sind.

Es sei $i : K \to L$ eine endliche Erweiterung. Jeder relative Automorphismus $\sigma \in \mathrm{Aut}(L/K)$ ist eine Fortsetzung von i.



Nach Satz 4.14 über die Anzahl von Fortsetzungen gilt $|\mathrm{Aut}(L/K)| \leq [L : K]$.

Definition 4.26 — Eine endliche Erweiterung L/K ist eine Galoiserweiterung[12], wenn $|\mathrm{Aut}(L/K)| = [L : K]$. In diesem Falle nennt man $\mathrm{Gal}(L/K) := \mathrm{Aut}(L/K)$ die Galoisgruppe der Erweiterung.

Beispiele 4.27 — 1. Es gibt zwei Automorphismen von $\mathbb{Q}(\sqrt{3})/\mathbb{Q}$, nämlich die Identität id und $\sigma : \sqrt{3} \mapsto -\sqrt{3}$. Also ist $\mathbb{Q}(\sqrt{3})/\mathbb{Q}$ eine Galoiserweiterung mit Galoisgruppe $\mathrm{Gal}(\mathbb{Q}(\sqrt{3})/\mathbb{Q}) \cong \mathbb{Z}/2$.
2. $\mathbb{C}/\mathbb{R}$ ist eine Galoiserweiterung: Die Galoisgruppe $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ ist isomorph zu $\mathbb{Z}/2$ und wird von der komplexen Konjugation $z \mapsto \overline{z}$ erzeugt.
3. Die Erweiterung $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ ist keine Galoiserweiterung. Es gibt drei $\mathbb{Q}$-lineare Einbettungen $\mathbb{Q}(\sqrt[3]{2}) \to \mathbb{C}$. Dabei wird $\alpha = \sqrt[3]{2}$ der Reihe nach auf α, $\rho\alpha$ und $\rho^2\alpha$ mit $\rho = \exp(2\pi i/3)$ abgebildet. Aber die beiden letzten Zahlen liegen nicht in $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ und liefern keine Automorphismen dieses Körpers.

Lemma 4.28 — *Es sei L/K eine endliche Galoiserweiterung mit Galoisgruppe G. Dann gilt $K = L^G$.*

Beweis. Nach Definition gilt sicher $K \subset M := L^G$ und $G \subset \mathrm{Aut}(L/M)$. Es folgt: $|G| \leq [L : M] \leq [L : K] = |G|$. Also besteht überall Gleichheit. Insbesondere ist $[L : M] = [L : K]$ und $M = K$. □

Beispiel 4.29 (Spurabbildung) — Es sei L ein Körper und $G \subset \mathrm{Aut}(L)$ eine endliche Untergruppe. Für jedes $x \in L$ ist $S(x) := \sum_{\sigma \in G} \sigma(x)$ invariant unter der Gruppe G, denn für $g \in G$ folgt nach Umindizierung:

$$g(S(x)) = \sum_{\sigma \in G} (g\sigma)(x) = \sum_{h \in G} h(x) = S(x).$$

[12] Évariste Galois ⋆25. Oktober 1811 †31. Mai 1832

Deshalb nimmt $S : L \to L$ Werte im Fixkörper $K := L^G$ an. Diese Abbildung $S : L \to K$ heißt Spurabbildung. Die Spur ist zunächst K-linear, denn für $\lambda \in K$ und $x \in L$ gilt

$$S(\lambda x) = \sum_{\sigma \in G} \sigma(\lambda x) = \sum_{\sigma \in G} \sigma(\lambda)\sigma(x) = \sigma(\lambda) \sum_{\sigma \in G} \sigma(x) = \lambda S(x),$$

weil $\sigma(\lambda) = \lambda$.

Die Spur ist aber vor allem nicht die Nullabbildung: Falls K die Charakteristik 0 hat, folgt dies sofort aus der einfachen Beobachtung, daß $S(1_L) = |G| \cdot 1_K$. Allgemeiner folgt die Behauptung für beliebige Charakteristik unmittelbar aus Lemma 4.25.

Lemma 4.30 — *Es sei L ein Körper und $G < \mathrm{Aut}(L)$ eine endliche Untergruppe. Dann ist L/L^G eine Galoiserweiterung mit $\mathrm{Aut}(L/L^G) = G$.*

Beweis. Es sei $G = \{\sigma_1, \ldots, \sigma_n\}$, $K = L^G$, und $x_1, \ldots, x_m \in L$ eine Basis von L als K–Vektorraum. Nach Konstruktion ist $G \subset \mathrm{Aut}(L/K)$, also $n = |G| \leq \mathrm{Aut}(L/K) \leq [L : K] = m$. Angenommen, $n < m$.

Die Matrix $(\sigma_i^{-1}(x_j))$ hat weniger Zeilen als Spalten. Deshalb gibt es einen nichttrivialen Vektor $y = (y_1, \ldots, y_m)^t \in L^m$ mit

$$\sum_{j=1}^{m} \sigma_i^{-1}(x_j) y_j = 0, \quad \text{für alle } i = 1, \ldots, n. \tag{4.4}$$

Nach eventuellem Umnumerieren kann man annehmen, daß $y_1 \neq 0$. Wir wissen, daß die Spurabbildung $S = \sum_i \sigma_i$ nicht identisch verschwindet. Es gibt also ein $u \in L$ mit $S(u) \neq 0$. Indem wir nötigenfalls alle y_j durch $y_j \frac{u}{y_1}$ ersetzen, können wir erreichen, daß neben den Gleichungen (4.4) zusätzlich $S(y_1) \neq 0$ gilt. Wir wenden auf die i-te Gleichung in (4.4) den Automorphismus σ_i an und summieren über alle $i = 1, \ldots, n$ auf:

$$\sum_{j=1}^{m} x_j S(y_j) = 0. \tag{4.5}$$

Die Koeffizienten $S(y_j)$ liegen alle in K. Deshalb beschreibt (4.5) eine K-lineare Abhängigkeit zwischen den Elementen $x_1, \ldots, x_m$, denn $S(y_1) \neq 0$. Dies widerspricht der Wahl der x_j als K-Basis von L. □

Lemma 4.31 — *Es sei L/K eine Galoiserweiterung mit Galoisgruppe $G = \mathrm{Gal}(L/K)$. Ist $\{a_1, \ldots, a_m\}$ die G-Bahn eines Elements $a \in L$, dann ist*

$$\mathrm{minpol}_{a/K} = (X - a_1) \cdot \ldots \cdot (X - a_m) \quad \in K[X].$$

Insbesondere ist a separabel.

Beweis. Es sei f das Minimalpolynom von a relativ K und $g = (X - a_1) \cdot \ldots \cdot (X - a_m)$. Zu jedem Element a_i in der G-Bahn von a gibt es nach Definition des Bahnbegriffs ein

$\sigma \in G$ mit $\sigma(a) = a_i$. Es folgt $0 = \sigma(f(a)) = f(\sigma(a)) = f(a_i)$. Demnach sind alle Bahnelemente Nullstellen von f, mit anderen Worten: $g|f$. Umgekehrt sind die Koeffizienten von g genau die elementarsymmetrischen Polynome der a_i und deshalb invariant unter allen Permutationen der a_i. Sie sind insbesondere invariant unter den Elementen der Galoisgruppe und liegen deshalb im Fixkörper $K = L^G$. Aus $g \in K[X]$ und $g(a) = 0$ folgt nach Definition des Minimalpolynoms die umgekehrte Teilbarkeitsrelation $f|g$. Da beide Polynome normiert sind, sind sie gleich. □

Satz 4.32 — *Die folgenden Aussagen über eine endliche Körpererweiterung sind äquivalent:*

1. *L/K ist eine Galoiserweiterung.*
2. *L/K ist separabel und normal.*
3. *L ist Zerfällungskörper eines irreduziblen separablen Polynoms aus $K[X]$.*
4. *L ist Zerfällungskörper eines separablen Polynoms aus $K[X]$.*

Beweis. $1 \Rightarrow 2$: Es sei $a \in L$ ein beliebiges Element. Nach Lemma 4.31 zerfällt das Minimalpolynom $\mathrm{minpol}_{a/K}$ über L in Linearfaktoren mit paarweise verschiedenen Nullstellen. Das zeigt, daß L separabel und normal über K ist.
$2 \Rightarrow 3$: Nach dem Satz vom primitiven Element existiert ein separables Element $a \in L$ mit $L = K(a)$. Das Minimalpolynom von a ist irreduzibel und separabel. Wegen der Normalität von L/K zerfällt es über L vollständig in Linearfaktoren. Nach Wahl von a wird L von a und a fortiori von den Nullstellen von $\mathrm{minpol}_{a/K}$ erzeugt und ist deshalb der Zerfällungskörper von f.
$3 \Rightarrow 4$: Trivial.
$4 \Rightarrow 1$: Es sei L der Zerfällungskörper eines separablen Polynoms $f \in K[X]$. Dann ist L normal und wird von separablen Elementen erzeugt. Wir wählen einen algebraischen Abschluß $L \to \overline{L}$. Es sei G die Menge der K-linearen Einbettungen $L \to \overline{L}$. Da L/K separabel ist, ist $|G| = [L : K]_s = [L : K]$. Für jedes $a \in L$ und jedes $\sigma \in G$ ist $\sigma(a)$ eine Nullstelle des Minimalpolynoms von a und liegt wegen der Normalität von f schon in L. Das bedeutet $\sigma(L) \subset L$, und aus Gradgründen muß sogar Gleichheit bestehen. Demnach ist jedes $\sigma \in G$ ein relativer Automorphismus von L/K. Da $|G| = [L : K]$, ist L/K eine Galoiserweiterung. □

Beispiel 4.33 — Es sei $L = Q(a, b)$ mit $a = \sqrt{2}, b = \sqrt{3} \in \mathbb{C}$. Als Zerfällungskörper des separablen Polynoms $(X^2 - 3)(X^2 - 2)$ ist $\mathbb{Q}(a, b)$ eine Galoiserweiterung von $\mathbb{Q}$ vom Grad 4. Jeder Automorphismus σ von $\mathbb{Q}(a, b)$ ist eindeutig durch die Wirkung auf

a und b bestimmt. Es gibt deshalb genau die vier Möglichkeiten:

$$\begin{aligned}
\sigma_0 : &\quad a \mapsto a, &\quad b \mapsto b \\
\sigma_1 : &\quad a \mapsto -a, &\quad b \mapsto b \\
\sigma_2 : &\quad a \mapsto a, &\quad b \mapsto -b \\
\sigma_3 : &\quad a \mapsto -a, &\quad b \mapsto -b
\end{aligned}$$

Die Elemente σ_1, σ_2 und σ_3 haben die Ordnung 2. Deshalb ist $\mathrm{Gal}(\mathbb{Q}(a,b)/\mathbb{Q}) \cong \mathbb{Z}/2 \times \mathbb{Z}/2$.

Beispiel 4.34 — Es sei $K = \mathbb{F}_p(t)$ und $L = \mathbb{F}_p(u)$. Die Abbildung $K \to L$, $t \mapsto u^p$, ist eine Körpererweiterung vom Grad p. Das Minimalpolynom von u über K ist $X^p - t \in K[X]$. Über L zerfällt $X^p - t$ in Linearfaktoren:

$$X^p - t = X^p - u^p = (X - u)^p.$$

Die Erweiterung ist normal, aber nicht separabel. Tatsächlich ist die Automorphismengruppe $\mathrm{Aut}(L/K) = \{id\}$ trivial, denn jeder relative Automorphismus von L/K ist bestimmt durch das Bild von u. Aber da u nur auf Nullstellen von $X^p - t$ abgebildet werden kann und u die einzige Nullstelle ist, ist die Identität der einzige relative Automorphismus.

Satz 4.35 (Hauptsatz der Galoistheorie) — *Es sei L/K eine endliche Galoiserweiterung mit Galoisgruppe $G = \mathrm{Gal}(L/K)$.*

1. *Für jede Untergruppe $H < G$ ist $K \subset L^H \subset L$ ein Zwischenkörper.*
2. *Für jeden Zwischenkörper $K \subset M \subset L$ ist L/M eine endliche Galoiserweiterung, und $\mathrm{Gal}(L/M)$ ist eine Untergruppe in $\mathrm{Gal}(L/K)$.*
3. *Die Zuordnungen $\Phi : H \mapsto L^H$ und $\Psi : M \mapsto \mathrm{Gal}(L/M)$ definieren zueinander inverse Bijektionen zwischen den Mengen*

   $$\mathfrak{G} \;=\; \{H \mid H \text{ ist eine Untergruppe von } \mathrm{Gal}(L/K)\}$$

   und

   $$\mathfrak{Z} \;=\; \{M \mid M \text{ ist ein Zwischenkörper von } L/K\}.$$

   Die Abbildungen Φ und Ψ sind inklusionsumkehrend, d.h.

   $$H \subset H' \quad \Leftrightarrow \quad L^H \supset L^{H'}.$$

4. *Ein Zwischenkörper M ist genau dann eine Galoiserweiterung von K, wenn $\mathrm{Gal}(L/M)$ ein Normalteiler von $\mathrm{Gal}(L/K)$ ist. In diesem Falle ist die Folge von Gruppenhomomorphismen*

   $$1 \longrightarrow \mathrm{Gal}(L/M) \xrightarrow{i} \mathrm{Gal}(L/K) \xrightarrow{r} \mathrm{Gal}(M/K) \longrightarrow 1$$

exakt. Dabei bezeichnet i die Inklusion und $r : \mathrm{Gal}(L/K) \to \mathrm{Gal}(M/K)$ die Einschränkungsabbildung $\sigma \mapsto \sigma|_M$. Mit anderen Worten: $\mathrm{Gal}(M/K) \cong \mathrm{Gal}(L/K)/\mathrm{Gal}(L/M)$.

Beweis. 1. Die erste Aussage ist klar.
Zu 2: Es sei M ein Zwischenkörper. Für jedes $a \in L$ ist $\mathrm{minpol}_{a/M}$ ein Teiler von $\mathrm{minpol}_{a/K}$ in $M[X]$. Da $\mathrm{minpol}_{a/K}$ in $L[X]$ vollständig in Linearfaktoren zerfällt, die paarweise verschieden sind, gilt dasselbe für $\mathrm{minpol}_{a/M}$. Insbesondere ist L normal und separabel über M, also eine Galoiserweiterung. Jeder relative Automorphismus von L/M fixiert M, also erst recht K. Deshalb besteht eine Inklusion von Gruppen $\mathrm{Gal}(L/M) \subset \mathrm{Gal}(L/K)$.
Zu 3. Es sei zunächst $H \subset \mathrm{Gal}(L/K)$ eine Untergruppe. Dann ist $M := L^H$ ein Zwischenkörper, und nach Lemma 4.30 ist L/M eine Galoiserweiterung mit $\mathrm{Gal}(L/M) = H$. Das zeigt $\Psi \circ \Phi = \mathrm{id}_{\mathfrak{G}}$. Es sei nun umgekehrt M ein Zwischenkörper und $H = \mathrm{Gal}(L/M) < \mathrm{Gal}(L/K)$. Dann gilt $M = L^H$ nach Lemma 4.28. Das zeigt $\Phi \circ \Phi = \mathrm{id}_{\mathfrak{Z}}$. Daß Φ und Ψ inklusionsumkehrend sind, ist klar.
Zu 4. Es sei M ein Zwischenkörper, der normal über K ist. Als Zwischenkörper einer separablen Erweiterung ist M auch separabel über K. Nach dem Normalitätskriterium 4.22 bildet jedes $\sigma \in \mathrm{Gal}(L/K)$ den Körper M in sich ab. Dies definiert einen Homomorphismus

$$r : \mathrm{Gal}(L/K) \to \mathrm{Gal}(M/K), \quad \sigma \mapsto \sigma|_M.$$

Dieser ist surjektiv: Denn jeder Automorphismus $\sigma_0 \in \mathrm{Gal}(M/K)$ setzt sich zu einer Einbettung $\sigma : L \to \overline{L}$ in einen algebraischen Abschluß von L fort, und da L/K normal ist, gilt $\sigma(L) = L$. Somit ist $\sigma \in \mathrm{Gal}(L/K)$ und $r(\sigma) = \sigma_0$. Weiter besteht der Kern von r aus allen Automorphismen von L/K, die M festlassen, d.h. $\mathrm{Gal}(L/M)$. Deshalb ist $\mathrm{Gal}(L/M)$ ein Normalteiler mit Faktorgruppe $\mathrm{Gal}(M/K) = \mathrm{Gal}(L/K)/\mathrm{Gal}(L/M)$.

Es sei umgekehrt $\mathrm{Gal}(L/M)$ ein Normalteiler in $\mathrm{Gal}(L/K)$. Um zu zeigen, daß M/K normal ist, betrachten wir eine beliebige K-lineare Einbettung $\psi_0 : M \to \overline{L}$ von M in einen algebraischen Abschluß von L und wählen eine Fortsetzung $\psi : L \to \overline{L}$. Da L normal ist, gilt $\psi \in \mathrm{Gal}(L/K)$. Für ein beliebiges $\sigma \in \mathrm{Gal}(L/M)$ gilt nun nach Annahme, daß $\psi^{-1}\sigma\psi \in \mathrm{Gal}(L/M)$. Deshalb gilt für jedes $x \in M$:

$$\sigma(\psi(x)) = \psi((\psi^{-1}\sigma\psi)(x)) = \psi(x),$$

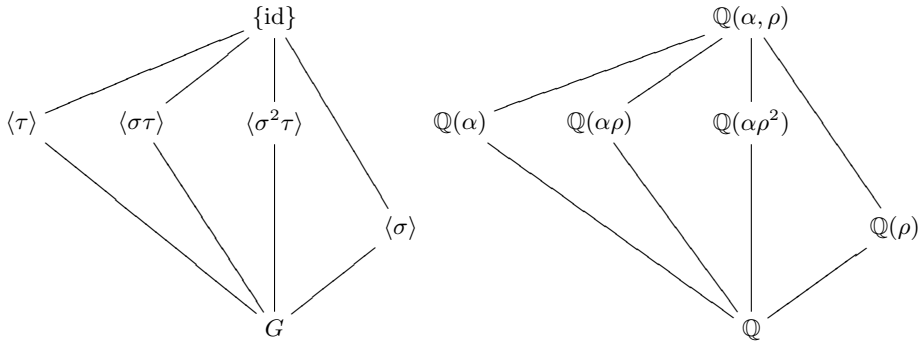
also $\psi(x) \in L^{\mathrm{Gal}(L/M)} = M$. Das zeigt $\psi(M) \subset M$. Mit dem Normalitätskriterium 4.22 folgt die Behauptung. □

Beispiel 4.36 — Es seien $\rho = \exp(2\pi i/3)$, $\alpha = \sqrt[3]{2}$ und $L = \mathbb{Q}(\alpha, \rho)$. Da ρ keine reelle Zahl ist, liegt ρ sicher nicht im Körper $\mathbb{Q}(\alpha)$. Da $\rho^2 + \rho + 1 = 0$, ist $L/\mathbb{Q}(\alpha)$ eine Erweiterung vom Grad 2 und $[L : \mathbb{Q}] = [L : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = 6$. Tatsächlich ist

$L/\mathbb{Q}$ eine Galoiserweiterung, denn L ist der Zerfällungskörper des Polynoms $X^3 - 2$. Jeder Automorphismus $L \to L$ muß α in α, $\alpha\rho$ oder $\alpha\rho^2$ abbilden und ρ in ρ oder $-\rho$. Damit sind alle sechs Möglichkeiten charakterisiert. Die Abbildungen

$$\sigma : \alpha \mapsto \alpha\rho, \quad \rho \mapsto \rho, \quad \text{und} \quad \tau : \alpha \mapsto \alpha, \quad \rho \mapsto -\rho.$$

erzeugen die Galoisgruppe. Es gelten die Relationen $\tau^2 = \mathrm{id}$, $\sigma^3 = \mathrm{id}$, $\tau\sigma\tau = \sigma^{-1}$. Man sieht, daß $G := \mathrm{Gal}(L/\mathbb{Q}) \cong S_3$. Es ergibt sich das folgende Schema von Untergruppen und zugehörigen Zwischenkörpern:

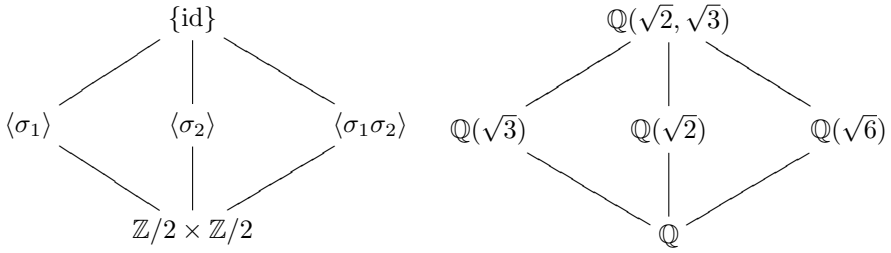


2. Juni 2008

Beispiel 4.37 — Wir wissen, daß die Galoisgruppe $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$ isomorph zu $\mathbb{Z}/2 \times \mathbb{Z}/2$ ist und von den Automorphismen

$$\sigma_1 : \sqrt{2} \mapsto -\sqrt{2}, \sqrt{3} \mapsto \sqrt{3}, \qquad \sigma_2 : \sqrt{2} \mapsto \sqrt{2}, \sqrt{3} \mapsto -\sqrt{3}$$

erzeugt wird. Die Korrespondenz zwischen Untergruppen und Zwischenkörpern sieht dann so aus:



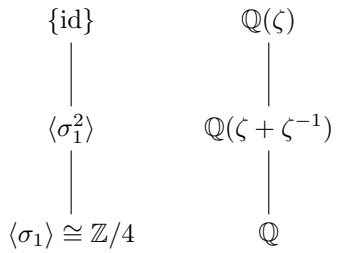
Beispiel 4.38 — Es sei $\zeta = \exp(2\pi i/5) \in \mathbb{C}$. Die Galoisgruppe $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ hat die Ordnung 4. Jeder Automorphismus muß ζ auf eine Potenz ζ^k abbilden, d.h. die Galoisgruppe $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ besteht aus den vier Automorphismen

$$\sigma_i : \zeta \mapsto \zeta^{2^i}, \quad i = 0, 1, 2, 3 \bmod 4,$$

die den Regeln $\sigma_i\sigma_j = \sigma_{i+j}$ genügen:

$$\sigma_i(\sigma_j(\zeta)) = \sigma_i(\zeta^{2^j}) = (\zeta^{2^i})^{2^j} = \zeta^{2^i \cdot 2^j} = \zeta^{2^{i+j}}.$$

Deshalb ist $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ zyklisch, erzeugt von σ_1, und es gibt nur eine Untergruppe, die von $\sigma_1^2 : \zeta \mapsto \zeta^4 = \zeta^{-1}$ erzeugt wird. Der zugehörige Zwischenkörper wird von $u = \zeta + \zeta^{-1} = 2\cos(\frac{2\pi}{5})$ erzeugt:



Ich schließe den Abschnitt mit einem Satz, der zusammen mit einem späteren Satz 7.12 über die Automorphismengruppe $\mathrm{Aut}(\mathbb{C})$ etwas Kurioses enthält. Beweis zur Übung.

Satz 4.39 — $\mathrm{Aut}(\mathbb{R}) = \{\mathrm{id}\}$.

Bemerkung und Satz aus Zeitgründen in der Vorlesung ausgelassen

Bemerkung 4.40 — In jeder algebraischen Erweiterung $K \subset L$ gibt es einen eindeutig bestimmten Zwischenkörper M, die separable Hülle von K in L, mit der Eigenschaft, daß M/K separabel und L/M rein inseparabel ist. Wenn L/K endlich und normal ist, kann man diese Reihenfolge auch umkehren: Wir betrachten die Gruppe $\mathrm{Aut}(L/K)$ der relativen Automorphismen. Da L/K normal ist, gilt $|\mathrm{Aut}(L/K)| = [L : K]_s$. Es sei $F := L^{\mathrm{Aut}(L/K)}$. Dann ist L/F eine endliche Galoiserweiterung vom Grad $[L : K]_s$. Aus dem Multiplikationssatz für den Separabilitätsgrad ergibt sich $[L : K]_s = [L : F]_s[F : K]_s$, also $[F : K]_s = 1$. Damit ist F/K rein inseparabel.

Wir benutzen diese Bemerkung, um den folgenden Satz zu beweisen. Er zeigt, daß wir in der Konstruktion des algebraischen Abschlusses in 3.21 bereits nach dem ersten Schritt fertig gewesen wären, daß also die Limeskonstruktion im zweiten Schritt überflüssig war.

Satz 4.41 — *Es sei L/K eine algebraische Körpererweiterung mit der Eigenschaft, daß jedes nichtkonstante Polynom $f \in K[X]$ eine Nullstelle in L hat. Dann ist L ein algebraischer Abschluß von K.*

Beweis. Es sei $f \in K[X]$ irreduzibel und $a_1, \ldots, a_n$ die Nullstellen von f in einem Zerfällungskörper L' von f über L. Nach Annahme liegt eine der Nullstellen, ohne Einschränkung a_1, in L. Es sei N die normale Hülle von $K(a_1)$ in L' und $F := N^{\mathrm{Aut}(L'/K)}$. Dann ist F/K rein inseparabel. Insbesondere hat das Minimalpolynom jedes Elements in F nur eine einzige Nullstelle, und diese liegt nach Voraussetzung in L. Das bedeutet, daß $F \subset L$. Die Galoiserweiterung N/F wird nach dem Satz vom primitiven Element von einem einzigen Element $b \in N$ erzeugt. Es seien $b = b_1, \ldots, b_\ell$ die Bilder von b unter der Galoisgruppe. Dann gilt $N = F(b_i)$ für jedes

$i = 1, \ldots, \ell$. Die Elemente $b_1, \ldots, b_\ell$ sind auch genau die Nullstellen des Minimalpolynoms von b über K. Nach Annahme liegt eine der Nullstellen, etwa b_j in L. Folglich hat man $N = F(b_j) \subset L$. Andererseits enthält N nach Konstruktion alle Nullstellen von f. Damit ist alles gezeigt. □

4.4 Einheitswurzeln und Kreisteilungskörper

Für einen kommutativen Ring R bezeichnet $R^\times$ die Gruppe der multiplikativen Einheiten. Bekanntlich bilden die Zahlen a, $0 < a < n$, die zu n teilerfremd sind, ein Repräsentantensystem für $(\mathbb{Z}/n)^\times$. Ihre Anzahl ist die Eulersche Phi-Funktion: $\varphi(n) = |(\mathbb{Z}/n)^\times|$. Gemäß dem chinesischen Restklassensatz gibt es für jede natürliche Zahl n mit der Primfaktorzerlegung $n = p_1^{a_1} \cdot \ldots \cdot p_\ell^{a_\ell}$ einen Ringisomorphismus

$$\mathbb{Z}/n \cong \prod_{i=1}^{\ell} \mathbb{Z}/p_i^{a_i}.$$

Durch Übergang zu den Einheiten entsteht daraus ein Gruppenisomorphismus

$$(\mathbb{Z}/n)^\times \cong \prod_{i=1}^{\ell} (\mathbb{Z}/p_i^{a_i})^\times,$$

und das bedeutet für die Gruppenordnungen:

$$\varphi(n) = \prod_{i=1}^{\ell} \varphi(p_i^{a_i}).$$

Andererseits sieht man direkt, daß die Anzahl der zu einer Primzahl p teilerfremden natürlichen Zahlen $< p^a$ durch $p^{a-1}(p-1)$ gegeben ist. Zusammengefaßt ergibt sich die bekannte Formel

$$\frac{\varphi(n)}{n} = \prod_{i=1}^{\ell} \frac{p_i - 1}{p_i}.$$

Es sei nun

$$\mu_n = \left\{ e^{\frac{2\pi i k}{n}} \;\middle|\; k = 0, \ldots, n-1 \right\} \subset \mathbb{C}^*$$

die Gruppe der n-ten Einheitswurzeln. Eine Einheitswurzel $\zeta \in \mu_n$ ist *primitiv*, wenn ζ die Ordnung n hat, also keine d-te Einheitswurzel für einen echten Teiler d von n ist. In analytischer Schreibweise sind die primitiven n-ten Einheitswurzeln durch die Ausdrücke $\exp(2\pi i k/n)$ mit zu n teilerfremden k gegeben. Mit anderen Worten: Unter dem Gruppenisomorphismus $\mathbb{Z}/n \mapsto \mu_n$, $k \mapsto \zeta^k$, mit $\zeta = \exp(2\pi i/n)$ gehen die zu n teilerfremden Restklassen bijektiv auf die primitiven n-ten Einheitswurzeln.

Definition 4.42 — Das Polynom

$$\Phi_n(X) := \prod_{\zeta \in \mu_n'} (X - \zeta), \tag{4.6}$$

wo ζ durch die Menge $\mu_n' \subset \mu_n$ der primitiven n-ten Einheitswurzeln läuft, heißt n-tes Kreisteilungspolynom.

Die ersten Kreisteilungspolynome sind

$$\begin{aligned}
\Phi_1 &= X - 1 \\
\Phi_2 &= X + 1 \\
\Phi_3 &= X^2 + X + 1 \\
\Phi_4 &= X^2 + 1 \\
\Phi_5 &= X^4 + X^3 + X^2 + X + 1 \\
\Phi_6 &= X^2 - X + 1
\end{aligned}$$

Nach Definition gilt $\operatorname{grad}(\Phi_n) = \varphi(n)$. Da jede n-te Einheitwurzel eine primitive d-te Einheitswurzel für genau einen Teiler d von n ist, bestehen die Beziehungen

$$X^n - 1 = \prod_{d|n} \Phi_d \qquad \text{und} \qquad n = \sum_{d|n} \varphi(d). \tag{4.7}$$

Bemerkung 4.43 — Mit der Möbiusfunktion μ und den Möbiusschen Umkehrformeln erhält man aus (4.7) die Beziehungen

$$\varphi_n = \sum_{d|n} \mu(n/d)d \tag{4.8}$$

und

$$\Phi_n = \prod_{d|n} (X^d - 1)^{(-1)^{\mu(n/d)}}. \tag{4.9}$$

Nach Konstruktion ist Φ_n ein Polynom mit komplexen Koeffizienten. Tatsächlich gilt:

Satz 4.44 — *Für alle $n \in \mathbb{N}$ ist $\Phi_n \in \mathbb{Z}[X]$.*

Beweis. Wir können induktiv annehmen, daß für alle echten Teiler d von n das Polynom Φ_d ganzzahlig und normiert ist. Es gilt nun

$$\Phi_n = \frac{X^n - 1}{\prod_{d|n,\, d<n} \Phi_d}. \tag{4.10}$$

Der Nenner ist ein ganzzahliges normiertes Polynom. Deshalb kann man Polynomdivision nicht nur in $\mathbb{C}[X]$ sondern auch in $\mathbb{Z}[X]$ ausführen. Das Ergebnis hängt nicht von einer möglichen Erweiterung des Koeffizientenrings ab, ist also über $\mathbb{Z}$ und $\mathbb{C}$ gleich. In $\mathbb{C}[X]$ geht die Division auf, also auch in $\mathbb{Z}[X]$. Daher ist Φ_n ganzzahlig und normiert. □

Satz 4.45 — *Die Kreisteilungspolynome Φ_n sind für alle $n \in \mathbb{N}$ in $\mathbb{Z}[X]$ irreduzibel.*

Beweis. Es sei ζ eine Wurzel von Φ_n und f ihr Minimalpolynom über $\mathbb{Q}$. Wir schreiben $\Phi_n = fg$ mit $g \in \mathbb{Q}[X]$. Nach dem Lemma von Gauß sind f und g ganzzahlig. Es sei p eine zu n teilerfremde Primzahl. Dann ist ζ^p ebenfalls eine primitive n-te Einheitswurzel und wegen der Zerlegung von Φ_n eine Nullstelle entweder von f oder von g. Angenommen, $g(\zeta^p) = 0$. Dann haben $f(X)$ und $g(X^p)$ einen gemeinsamen (normierten) Faktor $h(X) \in \mathbb{Z}[X]$. Wir reduzieren modulo p und erhalten in $\mathbb{F}_p[X]$ die Beziehungen

$$\bar{h}(X)|\bar{g}(X^p) = \bar{g}(X)^p, \quad \bar{h}(X)|\bar{f}(X).$$

Ein irreduzibler Faktor von $\bar{h}$ teilt somit sowohl $\bar{f}$ als auch $\bar{g}$. Er teilt deshalb $\overline{\Phi}_n$ und $\overline{X^n - 1}$ zweimal, obwohl $\overline{X^n - 1}$ sicher keine mehrfache Nullstellen hat, weil die Ableitung $n\overline{X}^{n-1}$ in keiner Nullstelle verschwindet: Widerspruch. Daher ist ζ^p eine Nullstelle von f.

Eine beliebige primitive n-te Einheitswurzel hat die Form ζ^m mit zu n teilerfremden Exponenten m. Zerlegt man $m = p_1 \cdots p_\ell$ in ein Produkt von Primzahlen, so zeigt das vorstehende Argument, daß

$$\zeta, \quad \zeta^{p_1}, \quad (\zeta^{p_1})^{p_2} = \zeta^{p_1 p_2}, \quad \ldots, \quad \zeta^{p_1 \cdots p_\ell} = \zeta^m$$

Nullstellen von f sind. Demnach ist jede Nullstelle von Φ_n auch eine Nullstelle von f. Das zeigt $\Phi_n = f$. □

Bemerkung 4.46 — Bei der Definition von Φ_n haben wir Einheitswurzeln in $\mathbb{C}$ verwendet. Aber da die Φ_n ganzzzahlige Koeffizienten haben und die Zerlegung

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

in $\mathbb{Z}[X]$ besteht, sind die Kreisteilungspolynome und diese Zerlegung über *jedem* Körper K definiert. Natürlich bleiben die Kreisteilungspolynome dabei nicht irreduzibel, sondern zerfallen je nach Körper auf sehr verschiedene Weise.

Ein Element $x \in K^\times$ ist eine n-te Einheitswurzel, wenn $x^n = 1$, und eine primitive Einheitswurzel, wenn $\mathrm{ord}(x) = n$ in $K^\times$.

Satz 4.47 — *Es sei K ein Körper, n eine natürliche Zahl und $\zeta \in \overline{K}$ eine primitive n-te Einheitswurzel. Die Erweiterung $K(\zeta)/K$ ist eine Galoiserweiterung. Jedes $\sigma \in \mathrm{Gal}(K(\zeta)/K)$ bestimmt ein eindeutiges Element $\phi(\sigma) \in (\mathbb{Z}/n)^\times$ mit der Eigenschaft $\sigma(\zeta) = \zeta^{\phi(\sigma)}$. Die Abbildung*

$$\phi : \mathrm{Gal}(K(\zeta)/K) \to (\mathbb{Z}/n)^\times$$

ist ein injektiver Gruppenhomomorphismus. Insbesondere ist die Erweiterung $K(\zeta)/K$ abelsch. ϕ ist genau dann ein Isomorphismus, wenn $\Phi_n \in K[X]$ irreduzibel ist.

Beweis. Nach Adjunktion von ζ zerfällt $X^n - 1$ in n verschiedene Linearfaktoren:

$$X^n - 1 = (X-1)(X-\zeta)(X-\zeta^2)\cdots(X-\zeta^{n-1}).$$

Insbesondere ist $K(\zeta)$ der Zerfällungskörper von $X^n - 1$ und separabel über K. Von den n Einheitswurzeln sind diejenigen, die nicht primitiv sind, Nullstellen von Φ_d für einen echten Teiler d von n. Deshalb ist ζ Nullstelle des Polynoms Φ_n, d.h. das Minimalpolynom von ζ ist Teiler von Φ_n. Jeder Automorphismus $\sigma \in \mathrm{Gal}(K(\zeta)/K)$ bildet ζ in eine primitive Einheitswurzel ab. Es gibt also genau ein $\phi(\sigma) \in (\mathbb{Z}/n)^\times$ mit $\sigma(\zeta) = \zeta^{\phi(\sigma)}$. Da ζ die Erweiterung erzeugt, ist σ durch $\phi(\sigma)$ eindeutig bestimmt. Deshalb ist ϕ eine injektive Abbildung. Für zwei Automorphismen σ und τ gilt:

$$\tau(\sigma(\zeta)) = \tau(\zeta^{\phi(\sigma)}) = (\tau(\zeta))^{\phi(\sigma)} = (\zeta^{\phi(\tau)})^{\phi(\sigma)} = \zeta^{\phi(\tau)\phi(\sigma)}.$$

Andererseits hat man

$$\tau(\sigma(\zeta)) = (\tau\circ\sigma)(\zeta) = \zeta^{\phi(\tau\circ\sigma)}.$$

Der Vergleich zeigt $\phi(\tau)\phi(\sigma) = \phi(\tau\circ\sigma)$. Damit ist ϕ ein Homomorphismus, wie behauptet. Die letzte Aussage ist klar. □

Das Kreisteilungspolynom $\Phi_n \in K[X]$ kann aus verschiedenen Gründen nicht irreduzibel sein:

1. Es kann sein, daß K eine m-te Einheitswurzel für ein $m|n$ enthält. Das schließt natürlich den Extremfall $m = n$ ein: Dann liegen alle n-ten Einheitswurzeln schon in K. Wir betrachten das Beispiel $n = 9$, $m = 3$ und $K = \mathbb{Q}(\rho)$, wo $\rho = \exp(2\pi i/3)$ eine dritte Einheitswurzel ist. Bezeichnet ζ eine primitive neunte Einheitswurzel, so hat ζ das Minimalpolynom $X^3 - \rho$ oder $X^3 - \rho^2$, und Φ_9 faktorisiert wie folgt:

$$\Phi_9 = X^6 + X^3 + 1 = (X^3 - \rho)(X^3 - \rho^2).$$

2. Das Minimalpolynom kann aber auch dann in kleinere Polynome zerfallen, wenn keine n-te Einheitswurzel in K liegt. Das zeigt das Beispiel $n = 5$ und $K = \mathbb{Q}(\sqrt{5})$: Es sei $\zeta \in \mathbb{C}$ eine primitive n-te Einheitswurzel und $\eta := \zeta + \zeta^{-1}$. Aus der Gleichung

$$\zeta^4 + \zeta^3 + \zeta^2 + \zeta + 1 = 0$$

gewinnt man

$$0 = \zeta^2 + \zeta + 1 + \zeta^{-1} + \zeta^{-2} = \eta^2 + \eta - 1.$$

Damit ist $\eta = (-1+\sqrt{5})/2$ oder $(-1-\sqrt{5})/2$ je nachdem, mit welcher Einheitswurzel ζ man anfängt. In jedem Falle zerfällt Φ_5 über $\mathbb{Q}(\sqrt{5})$ wie folgt:

$$\begin{aligned} X^4 + X^3 + X^2 + X + 1 &= (X-\zeta)(X-\zeta^4)(X-\zeta^2)(X-\zeta^3) \\ &= (X^2 - \eta X + 1)(X^2 - (-1-\eta)X + 1) \\ &= \left(X^2 + \frac{1+\sqrt{5}}{2}X + 1\right)\left(X^2 + \frac{1-\sqrt{5}}{2}X + 1\right). \end{aligned}$$

Beispiel 4.48 — Es sei $\zeta \in \mathbb{C}$ eine primitive 7. Einheitswurzel. Die Erweiterung $\mathbb{Q}(\zeta)/\mathbb{Q}$ ist eine Galoiserweiterung mit zyklischer Galoisgruppe

$$\begin{array}{ccccc} \mathbb{Z}/6 & \xrightarrow{\cong} & (\mathbb{Z}/7)^\times & \xrightarrow{\cong} & \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \\ k & \mapsto & 3^k, \quad j & \mapsto & (\sigma_j : \zeta \mapsto \zeta^j) \end{array}$$

Es gibt zwei Untergruppen der Ordnung 2 bzw. 3 in $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$, die von σ_6 bzw. σ_2 erzeugt werden. Wir betrachten die zugehörigen Zwischenkörper:

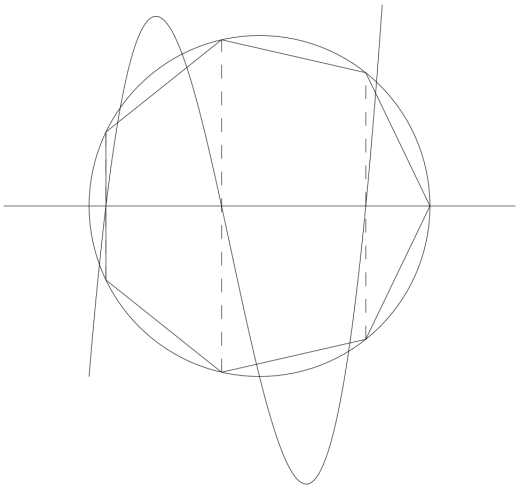
Es sei $H_1 = \{\sigma_1, \sigma_6\}$ und $K_1 = \mathbb{Q}(\zeta)^{H_1}$. Das Element $u = \zeta + \zeta^6 = 2\cos(2\pi/7)$ ist invariant unter H_1. Eine Gleichung für u findet man leicht aus

$$0 = \zeta^3 + \zeta^2 + \zeta + 1 + \zeta^{-1} + \zeta^{-2} + \zeta^{-3} = u^3 + u^2 - 2u - 1.$$

Dann ist $K_1 = \mathbb{Q}(u) = \mathbb{Q}(\cos(2\pi/7))$. Die Galoisgruppe von $K_1/\mathbb{Q}$ ist zyklisch von der Ordnung 3 und wird erzeugt von dem Element

$$u = \zeta + \zeta^{-1} \mapsto \zeta^2 + \zeta^{-2} = u^2 - 2.$$

Das regelmäßige Siebeneck mit dem Graphen des Polynoms $8x^3 + 4x^2 - 4x - 1$:

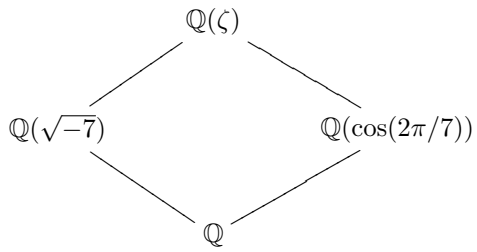


Nur zur Untergruppe $H_2 = \{\sigma_1, \sigma_2, \sigma_4\}$ und dem zugehörigen Zwischenkörper $K_2 = \mathbb{Q}(\zeta)^{H_2}$. Das Element $v = \zeta + \zeta^2 + \zeta^4$ ist invariant unter H_2. Es genügt der Gleichung

$$v^2 = \zeta^2 + \zeta^4 + \zeta + 2(\zeta^{1+2} + \zeta^{2+4} + \zeta^{4+1}) = -v - 2.$$

Insbesondere gilt $(2v + 1)^2 = -7$. Das zeigt: $K_2 = \mathbb{Q}(v) = \mathbb{Q}(\sqrt{-7})$.

Die Zwischenkörper von $\mathbb{Q}(\zeta)/\mathbb{Q}$ sind somit:



Satz 4.49 (Gauß – Die Konstruktion des regulären 17-Ecks) — *Es gilt*

$$\cos\frac{2\pi}{17} = \frac{1}{16}\left(-1+\sqrt{17}+\sqrt{34-2\sqrt{17}}+\sqrt{68+12\sqrt{17}-(6+2\sqrt{17})\sqrt{34-2\sqrt{17}}}\right)$$

Beweis. Die Konstruktion von Gauß funktioniert nicht nur für $p = 17$, sondern für alle Primzahlen der Form $p = 2^n + 1$, $n = 2^k$. Wir setzen entsprechend allgemein an und spezialisieren erst später.

Es sei ζ eine primitive p-te Einheitswurzel. Die Wahl einer Primitivwurzel w modulo p bestimmt einen Isomorphismus

$$\mathbb{Z}/2^n = \mathbb{Z}/(p-1) \to G := \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}), \quad j \mapsto (\sigma_j : \zeta \mapsto \zeta^{w^j}).$$

Für $\nu = 0, \ldots, n$ sei $G_\nu \subset G$ die von σ_{2^ν} erzeugte Untergruppe der Ordnung $2^{n-\nu}$. Wir erhalten die Kette von Untergruppen

$$\{\mathrm{id}\} = G_n < G_{n-1} < \ldots < G_1 < G_0 = G$$

und die zugehörige Kette von Zwischenkörpern

$$\mathbb{Q} = L_0 \subset L_1 \subset \ldots \subset L_{n-1} \subset L_n = \mathbb{Q}(\zeta), \qquad L_\nu = \mathbb{Q}(\zeta)^{G_\nu}.$$

Der Körper L_ν wird von

$$u_\nu := \sum_{g \in G_\nu} g(\zeta) = \sum_{k=0}^{2^{n-\nu}-1} \zeta^{w^{2^\nu k}}$$

erzeugt. Die Ausdrücke u_ν heißen Gaußsche Perioden.

Wir betrachten den Fall $p = 17$, also $n = 4$, und der Primitivwurzel $w = 3 \bmod 17$. (Um einzusehen, daß 3 eine Primitivwurzel modulo 17 ist, genügt es nachzurechnen, daß $3^8 \equiv -1 \bmod 17$). Dann lauten die Perioden:

$$\begin{aligned}
u_1 &= \zeta + \zeta^{-8} + \zeta^{-4} + \zeta^{-2} + \zeta^{-1} + \zeta^8 + \zeta^4 + \zeta^2 \\
u_2 &= \zeta + \zeta^{-4} + \zeta^{-1} + \zeta^4 \\
u_3 &= \zeta + \zeta^{-1} \\
u_4 &= \zeta
\end{aligned}$$

Diese genügen den folgenden quadratischen Gleichungen, wie man nachrechnen kann:

$$\begin{gathered} u_1^2 + u_1 - 4 = 0 \\ u_2^2 - u_1 u_2 - 1 = 0 \\ u_3^2 - u_2 u_3 + \tfrac{1}{2}(u_2 - 1)(u_1 + 1) - 1 = 0 \\ u_4^2 - u_4 + 1 = 0 \end{gathered}$$

Wenn man diese quadratischen Gleichungen auflöst, muß man vier Vorzeichenwahlen treffen, erhält also wie erwartet 16 verschiedene Einheitswurzeln. Für den gesuchten Kosinus kommt man mit $u_3/2$ aus. Über die richtigen Vorzeichenwahlen kann man numerisch entscheiden. Man findet:

$$u_1 = \frac{1}{2}\left(-1 + \sqrt{17}\right)$$

$$u_2 = \frac{1}{4}\left(-1 + \sqrt{17} + \sqrt{34 - 2\sqrt{17}}\right)$$

und schließlich

$$u_3 = \frac{1}{8}\left(-1 + \sqrt{17} + \sqrt{34 - 2\sqrt{17}} + \sqrt{68 + 12\sqrt{17} - (6 + 2\sqrt{17})\sqrt{34 - 2\sqrt{17}}}\right)$$

□

Aufgabe zu Kreisteilungspolynomen

Aufgabe 4.1 — Programmieren Sie die Berechnung des n-ten Kreisteilungspolynoms a) rekursiv aus der Formel (4.10) und b) direkt aus der Formel (4.9). Zum Vergleich: Die Kreisteilungspolynome sind in Mupad unter `polylib::cyclotomic` aufrufbar.

Aufgabe 4.2 — Wir verwenden die in Aufgabe 4.1 berechnete Tabelle für einige heuristische Überlegungen: Untersuchen Sie die Tabelle auf Regelmäßigkeiten, Stellen Sie Vermutungen an, Versuchen Sie diese zu beweisen. [z.B. Welcher Zusammenhang besteht zwischen Φ_n und Φ_{2n}, zwischen Φ_p und Φ_{p^ℓ}, p prim, etc. Die Tabelle zeigt, daß für $n \leq 100$ in Φ_n nur die Koeffizienten $-1, 0, 1$ vorkommen, warum? Was kann man allgemein erwarten? Beweis?]

§5 Konstruktionen mit Zirkel und Lineal

In diesem Abschnitt betrachten wir verschiedene Konstruktionsprobleme der klassischen Geometrie, die mit Zirkel und Lineal ausgeführt werden sollen. Die berühmtesten Konstruktionsprobleme sind die folgenden.

1. **Die Quadratur des Kreises.** *Gegeben ein Kreis mit Mittelpunkt p und Radius r. Man konstruiere ein Quadrat mit gleichem Flächeninhalt.*
   Wenn man durch Wahl einer Einheitsstrecke den Maßstab festlegt, ist das Problem dazu äquivalent, eine Strecke der Länge $\sqrt{\pi}$ zu konstruieren.

2. **Die Dreiteilung des Winkels.** *Man konstruiere zu einem gegebenen Winkel α den Winkel $\alpha/3$.*
   Die Aufgabe ist für gewisse spezielle Winkel, wie $\alpha = \pi/2$, leicht, es geht aber um einen allgemeinen Winkel.

3. **Das delische Problem: Die Verdopplung des Würfels.** *Man konstruiere zu einer gegebenen Strecke a eine Strecke b so, daß das Volumen eines Würfels der Kantenlänge b das Doppelte des Volumens eines Würfels der Kantenlänge a ist, d.h. $b^3 = 2a^3$.*
   Bei gewählter Einheitsstrecke ist das Problem dazu äquivalent, eine Strecke der Länge $\sqrt[3]{2}$ zu konstruieren.

Die ersten drei Aufgaben sind unlösbar. Der Unmöglichkeitsbeweis wird dadurch erbracht, daß man die Aufgaben algebraisiert und mit Körpertheorie zeigt, daß die entsprechenden algebraischen Probleme nicht lösbar sind. Für die Dreiteilung des Winkels und die Verdopplung des Würfels genügen dazu einfache Aussagen über Körpererweiterungen. Die Unmöglichkeit der Kreisquadratur ist sprichwörtlich. Der Beweis benötigt allerdings den Satz von Lindemann, daß π eine transzendente Zahl ist.

Diesen klassischen Problemen fügen wir das folgende hinzu:

4. **Regelmäßige n-Ecke.** Für welche natürlichen Zahlen n kann man ein reguläres n-Eck konstruieren?

Es war spätestens den Pythagoräern bekannt, daß man das Dreieck, das Viereck, das Fünfeck und das Fünfzehneck sowie alle regulären n-Ecke, die daraus durch wiederholte Verdopplung der Eckenzahl hervorgehen, konstruieren kann. In arabischen Quellen findet man eine Archimedes zugeschriebene Konstruktion des regelmäßigen Siebenecks durch eine sogenannte Neusis. Daß man auch mit Zirkel und Lineal etwas weiter kommt, war eine überraschende Entdeckung von Gauß.

Man beachte, daß die negativen Antworten für die oben genannten Probleme nur bei Beschränkung der gewählten Mittel Zirkel und Lineal Geltung haben. Läßt man andere Hilfsmittel, Maschinen oder Methoden zu, gibt es sehr wohl Lösungen.

Wir präzisieren den Begriff der Konstruktion mit Zirkel und Lineal wie folgt: In der euklidischen Ebene E sei eine Menge S mit mindestens zwei Punkten gegeben. Ein Punkt, eine Gerade bzw. ein Kreis sind S-konstruierbar (oder kurz: konstruierbar, wenn der Zusammenhang klar ist), wenn sie in endlich vielen Schritten auf die folgende Weise entstehen:

1. Alle Punkte in S sind konstruierbar.

2. Jede Gerade durch zwei verschiedene konstruierbare Punkte ist konstruierbar.

3. Jeder Kreis mit konstruierbarem Mittelpunkt und durch einen anderen konstruierbaren Punkt ist konstruierbar.

4. Jeder Schnittpunkt zweier konstruierbarer Geraden, einer konstruierbaren Geraden und eines konstruierbaren Kreises bzw. zweier konstruierbarer Kreise ist konstruierbar.

Um Fragen der Konstruierbarkeit zu algebraisieren, gehen wir wie folgt vor: Wir zeichnen zwei Punkte $P_0, P_1 \in S$ aus und betrachten den Abstand $|P_0P_1|$ als Längenmaßeinheit. Es gibt dann genau eine längentreue und orientierungserhaltende Identifizierung $E \to \mathbb{C}$ mit $P_0 \mapsto 0$ und $P_1 \mapsto 1$. In diesem Sinne betrachten wir von nun an S als eine Teilmenge von $\mathbb{C}$, die die Punkte 0 und 1 enthält, und sprechen von (aus S) konstruierbaren komplexen Zahlen.

Es seien p_1 und p_2 verschiedene komplexe Zahlen. Eine komplexe Zahl $z \neq p_1, p_2$ liegt auf der reellen Geraden durch p_1 und p_2, wenn das Verhältnis $(z - p_1)/(z - p_2)$ reell ist, d.h. wenn

$$\frac{z - p_1}{z - p_2} = \frac{\overline{z} - \overline{p}_1}{\overline{z} - \overline{p}_2}.$$

Multiplikation mit dem Hauptnenner und Kürzen aller doppelt vorkommenden Terme führt auf die folgende komplexe Form der Geradengleichung:

$$(\overline{p}_1 - \overline{p}_2)z + (p_2 - p_1)\overline{z} = \overline{p}_1 p_2 - p_1\overline{p}_2. \tag{5.1}$$

Ist $m \in \mathbb{C}$ und $r \in \mathbb{R}_{>0}$, so liegt z genau dann auf dem Kreis mit Mittelpunkt m durch den Punkt q, wenn

$$(z - m)(\overline{z} - \overline{m}) = (q - m)(\overline{q} - \overline{m}). \tag{5.2}$$

Die Berechnung der Schnittpunkte in den elementaren Konstruktionsschritten führt demnach auf die folgenden Gleichungssysteme:

1. Der Schnittpunkt zweier Geraden durch Punkte p_1, p_2 bzw. q_1, q_2 ist eine Lösung des *linearen* Gleichungssystems:

$$\begin{aligned}(\overline{p}_1 - \overline{p}_2)z + (p_2 - p_1)\overline{z} &= \overline{p}_1 p_2 - p_1\overline{p}_2\\ (\overline{q}_1 - \overline{q}_2)z + (q_2 - q_1)\overline{z} &= \overline{q}_1 q_2 - q_1\overline{q}_2.\end{aligned}$$

   Insbesondere liegt z in dem Körper $\mathbb{Q}(S \cup \overline{S})$, wenn $p_1, p_2, q_1, q_2 \in S$.

2. Jeder Schnittpunkt der Geraden durch Punkte p_1, p_2 mit dem Kreis um m durch q ist eine Lösung des Gleichungssystems

$$\begin{aligned}(\overline{p}_1 - \overline{p}_2)z + (p_2 - p_1)\overline{z} &= \overline{p}_1 p_2 - p_1\overline{p}_2\\ (z - m)(\overline{z} - \overline{m}) &= (q - m)(\overline{q} - \overline{m}).\end{aligned}$$

   Eliminiert man aus der zweiten Gleichung $\overline{z}$ mit Hilfe der ersten Gleichung, so bleibt eine quadratische Gleichung für z mit Koeffizienten in $\mathbb{Q}(S \cup \overline{S})$ übrig, wenn $p_1, p_2, m, q \in S$.

3. Jeder Schnittpunkt der beiden Kreise um m_1 durch q_1 bzw. um m_2 durch q_2 ist eine Lösung des Gleichungssystems

$$\begin{aligned}(z-m_1)(\overline{z}-\overline{m}_1) &= (q_1-m_1)(\overline{q}_1-\overline{m}_1)\\ (z-m_2)(\overline{z}-\overline{m}_2) &= (q_2-m_2)(\overline{q}_2-\overline{m}_2).\end{aligned}$$

Löst man beide Gleichungen nach $\overline{z}$ auf, erhält man die Bedingung

$$\overline{z} = m_1 + \frac{(q_1-m_1)(\overline{q}_1-\overline{m}_1)}{z-m_1} = m_2 + \frac{(q_2-m_2)(\overline{q}_2-\overline{m}_2)}{z-m_2} \tag{5.3}$$

Nach Multiplikation mit dem Hauptnenner ist dies eine quadratische Gleichung für z mit Koeffizienten in $\mathbb{Q}(S \cup \overline{S})$.

Satz 5.1 — *Es sei $S \subset \mathbb{C}$ eine Menge von Punkten mit $0, 1 \in S$. Ein Punkt $z \in \mathbb{C}$ ist genau dann in endlich vielen Schritten aus S konstruierbar, wenn es eine Folge von Körpererweiterungen $K_0 = \mathbb{Q}(S \cup \overline{S}) \subset K_1 \subset \ldots \subset K_n$ mit den folgenden Eigenschaften gibt: $[K_{i+1} : K_i] = 2$ für $i = 0, \ldots, n-1$, und $z \in K_n$.*

Beweis. Es sei zunächst z aus S konstruierbar. Dazu seien ℓ Schritte nötig, bei denen in elementaren Konstruktionsschritten der Reihe nach die Zahlen z_1, z_2,..., $z_\ell = z$ konstruiert werden. Wir setzen $S_k := S \cup \{z_1, \ldots, z_k\}$ und $L_k := \mathbb{Q}(S_k \cup \overline{S}_k)$ für $k = 0, \ldots, \ell$. Wir haben oben gesehen, daß z_k jeweils entweder in L_{k-1} oder in einer quadratischen Erweiterung davon liegt. Dasselbe gilt dann auch für $\overline{z}_k$. Wir erhalten eine Folge von Körpererweiterungen

$$L_0 \subset \ldots \subset L_{k-1} \subset L_{k-1}(z_k) \subset L_k = L_{k-1}(z_k, \overline{z}_k) \subset \ldots \subset L_\ell.$$

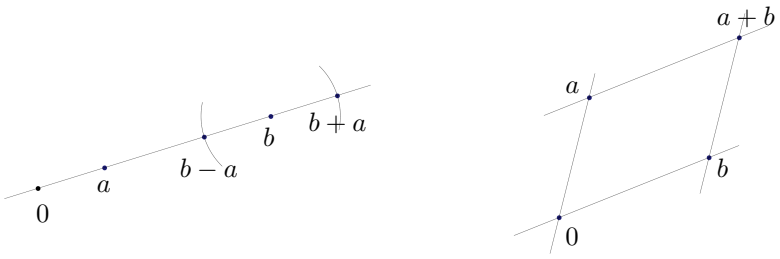
Der Körpergrad ist in jedem Schritt 1 oder 2, und nach Konstruktion ist $z \in L_\ell$. Das beweist die erste Richtung.

Für die umgekehrte Richtung halten wir zunächst fest: Durch Kombination von elementaren Konstruktionsschritten sind auch die folgenden Konstruktionen immer ausführbar:

1. Die Konstruktion der Parallelen zu einer konstruierten Geraden g durch einen konstruierten Punkt P.

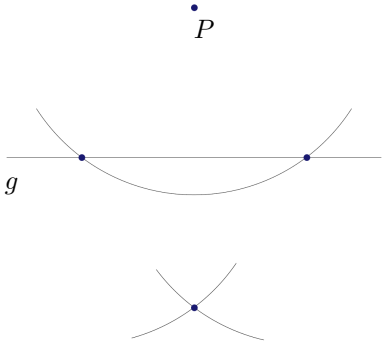
2. Die Konstruktion des Kreises um einen konstruierbaren Punkt m mit Radius $|Q_1Q_2|$, wobei Q_1 und Q_2 konstruierte Punkte sind.

Damit ist für je zwei konstruierbare Zahlen a und b auch ihre Summe und Differenz konstruierbar.



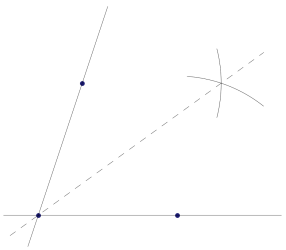
Die Konstruktion des Produktes oder Quotienten zweier Zahlen führt auf das Teilproblem, zwei Winkel zu addieren oder zu subtrahieren, und das Teilproblem, zwei Streckenlängen zu multiplizieren oder zu dividieren. Das erste Problem ist leicht, das zweite Problem wird durch die Strahlensätze gelöst:

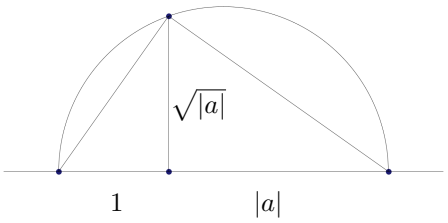
Schließlich kann man leicht jeden konstruierten Punkt P an einer konstruierten Geraden g spiegeln:



Insbesondere kann man zu jedem konstruierbaren Punkt z auch den komplex konjugierten Punkt $\overline{z}$ konstruieren. Damit ist gezeigt:

Ist $T \subset \mathbb{C}$ eine Menge von Punkten, die aus S konstruierbar ist, so sind alle Punkte im Körper $\mathbb{Q}(T \cup \overline{T})$ konstruierbar. Um die fehlende Richtung des Satzes zu beweisen, genügt es, die folgende Behauptung zu beweisen: Genügt $z \in \mathbb{C}$ einer quadratischen Gleichung, deren Koeffizienten konstruierbar sind, so gilt dies auch für z. Offensichtlich genügt es weiter zu zeigen: Ist a konstruierbar, so auch die beiden Quadratwurzeln aus a. Dazu wiederum genügt es, den von a mit der positiven reellen Achse gebildeten Winkel zu halbieren, und die Quadratwurzel aus $|a|$ zu ziehen. Letzteres kann man zum Beispiel mit dem Höhensatz erreichen:





Damit ist alles gezeigt. □

Satz 5.2 — *Die Würfelverdopplung ist nicht mit Zirkel und Lineal ausführbar.*

Beweis. In algebraischer Übersetzung lautet das Problem, die Zahl $z = \sqrt[3]{2}$ zu konstruieren. Dazu müßte es nach Satz 5.1 eine Körpererweiterung $L/\mathbb{Q}$ mit $z \in L$ und $[L : \mathbb{Q}] = 2^m$, $m \in \mathbb{N}$ geben. Das ist wegen $[\mathbb{Q}(z) : \mathbb{Q}] = 3$ und der Multiplikativität des Grads bei Körpererweiterungen unmöglich. Deshalb ist die Konstruktion nicht ausführbar. □

Satz 5.3 — *Die Winkeldreiteilung ist für einen allgemeinen Winkel nicht mit Zirkel und Lineal ausführbar.*

Beweis. Es sei der Winkel α gegeben und $a = 2\cos(\alpha)$. Einen Winkel β mit $\alpha = 3\beta$ zu konstruieren, ist äquivalent dazu, die reelle Zahl $x = 2\cos(\beta)$ aus a zu konstruieren. Nun gilt nach den Formeln von de Moivre:

$$\cos(\alpha) + \sin(\alpha)i = (\cos(\beta) + i\sin(\beta))^3$$

und somit

$$\cos(\alpha) = \cos(\beta)^3 - 3\cos(\beta)\sin(\beta)^2 = 4\cos(\beta)^3 - 3\cos(\beta).$$

Deshalb erfüllt x die kubischen Gleichung

$$x^3 - 3x - a = 0.$$

Es genügt, einen einzigen Winkel anzugeben, für den die Dreiteilung nicht möglich ist. Wir wählen dazu $\alpha = \pi/3$, also $a = 1$. Das Polynom $f = X^3 - X - 1$ ist irreduzibel. Deshalb ist $[\mathbb{Q}(x) : \mathbb{Q}] = 3$, und x kann nicht in einer Erweiterung $L/\mathbb{Q}$ liegen, deren Grad eine Potenz von 2 ist. Nach Satz 5.1 kann x nicht mit Zirkel und Lineal gelöst werden. □

Satz 5.4 — *Die Quadratur des Kreises ist nicht mit Zirkel und Lineal möglich.*

Beweis. In algebraischer Übersetzung besteht das Problem darin, eine Strecke der Länge $\sqrt{\pi}$ zu konstruieren. Nun hat Ferdinand von Lindemann gezeigt, daß π eine transzendente Zahl ist (Folgerung 7.6). Deshalb ist auch $\sqrt{\pi}$ nicht algebraisch und erst recht nicht konstruierbar. Die Hauptschwierigkeit liegt hier natürlich im Satz von Lindemann. □

Satz 5.5 — *Es sei $S \subset \mathbb{C}$ eine Menge von Punkten mit $0, 1 \in S$. Ein Punkt z ist genau dann aus S konstruierbar, wenn z algebraisch über $K = \mathbb{Q}(S \cup \overline{S})$ ist und wenn der Grad des Zerfällungskörpers von z über K eine Potenz von 2 ist.*

Beweis. Es sei zunächst z algebraisch über K und L der Zerfällungskörper von z. Weiter sei $[L : K] = 2^m$. Dann ist die Galoisgruppe $G := \mathrm{Gal}(L/K)$ eine 2-Gruppe. Wir haben gesehen, daß es eine Filtrierung von G durch Normalteiler

$$G_n = \{\mathrm{id}\} \subset G_{n-1} \subset \ldots \subset G_0 = G$$

mit der Eigenschaft gibt, daß $|G_i|/|G_{i+1}| = 2$. Dem entspricht eine Folge von Zwischenkörpern

$$K = K_0 \subset K_1 \subset \ldots \subset K_n = L, \qquad K_\nu = L^{G_\nu}$$

mit $[K_i : K_{i-1}] = 2$. Nach Satz 5.1 ist z mit Zirkel und Lineal aus S konstruierbar.

Zur Umkehrung: Es sei z aus S konstruierbar. Dann gibt es nach Satz 5.1 eine Folge von Körpererweiterungen

$$K = K_0 \subset K_1 \subset \ldots \subset K_\ell$$

mit $[K_i : K_{i-1}] = 2$ und $z \in K_\ell$. Wir setzen $L_0 = K_0$ und konstruieren induktiv eine Folge von Körpererweiterungen

$$K = L_0 \subset L_1 \subset \ldots \subset L_\ell$$

mit den folgenden Eigenschaften:

1. $K_i \subset L_i$.
2. L_i ist normal über K.
3. $[L_{i+1} : L_i]$ ist eine Potenz von 2.

Es sei k ein Index mit $0 \leq k < \ell$ und L_k mit den verlangten Eigenschaften schon konstruiert. Es gibt nun ein $a \in K_{k+1}$ mit $K_{k+1} = K_k(a)$, und dieses a ist eine Nullstelle eines quadratischen Polynoms $f \in K_k[X]$. Es seien weiter $a = a_1, \ldots, a_m \in \mathbb{C}$ die Nullstellen von $\mathrm{minpol}_{a/K}$. Wir setzen $L_{k+1} := L_k(a_1, \ldots, a_m)$. Dann gilt nach Konstruktion sicher $L_k \subset L_{k+1}$ und $K_{k+1} \subset L_{k+1}$, und L_{k+1}/K ist normal. Zu jedem a_i gibt es einen Automorphismus $\sigma_i \in \mathrm{Gal}(L_{k+1}/K)$ mit $\sigma_i(a) = a_i$. Der Automorphismus σ_i transformiert $f \in K_k[X] \subset L_k[X]$ in ein Polynom $f_i \in L_k[X]$, weil L_k

normal ist. Aus $f(a) = 0$ folgt $f_i(a_i) = 0$. Insbesondere ist a_i quadratisch über L_k, also erst recht höchstens quadratisch über $L_k(a_1, \ldots, a_{i-1})$. Die Körpererweiterungen

$$L_k \subset L_k(a_1) \subset \ldots \subset L_k(a_1, a_2, \ldots, a_m) = L_{k+1}$$

haben also jeweils den Grad 1 oder 2. Damit ist die Induktion abgeschlossen.

Insgesamt erhalten wir so eine normale Erweiterung L_ℓ/K von 2-Potenzgrad mit $z \in L_\ell$. Dann enthält L_ℓ einen Zerfällungskörper von z über K, und dessen Grad über K ist notwendigerweise ebenfalls eine Potenz von 2. □

Lemma 5.6 — *Eine Zahl der Form $2^n + 1$ ist höchstens dann eine Primzahl, wenn $n = 2^k$ für ein $k \in \mathbb{N}_0$.*

Beweis. Angenommen, $n = mq$ mit einer ungeraden Zahl q, $1 < q \leq n$. Dann gilt

$$2^n + 1 = (2^m + 1)\left((2^m)^{q-1} - (2^m)^{q-2} + \ldots - 2^m + 1\right).$$

Wenn also $2^n + 1$ eine Primzahl sein soll, darf n keinen nichttrivialen ungeraden Faktor enthalten. □

Definition 5.7 — Zahlen der Form $F_k = 2^{2^k} + 1$ heißen Fermatzahlen.

Die ersten Fermatzahlen sind wirklich Primzahlen:

$$F_0 = 3, \quad F_1 = 5, \quad F_2 = 17, \quad F_3 = 257, \quad F_4 = 65537.$$

Aber schon die nächste Fermatzahl faktorisiert (Euler): $2^{32} + 1 = 641 \cdot 6700417$. Es sind keine weiteren Fermatzahlen bekannt, die Primzahlen sind. Die Faktorisierung von Fermatzahlen ist ein beliebter Test für die Qualität von neuen Faktorisierungsalgorithmen. Den jeweils aktuellen Stand der Bemühungen findet man wohl am schnellsten durch eine Suche im Internet.

Satz 5.8 (Gauß) — *Ein reguläres n-Eck ist genau dann mit Zirkel und Lineal konstruierbar, wenn n die Form*

$$n = 2^m p_1 \cdots p_\ell$$

hat, wobei $m, \ell \in \mathbb{N}_0$ und $p_1, \ldots, p_\ell$ paarweise verschiedene Fermat-Primzahlen sind.

Beweis. Es sei $n = 2^m p_1^{\nu_1} \cdots p_\ell^{\nu_\ell}$ die Primfaktorzerlegung von n. Der Zerfällungskörper des Kreisteilungspolynoms Φ_n hat den Grad

$$\varphi(n) = 2^{m-1} p_1^{\nu_1 - 1} \cdots p_\ell^{\nu_\ell - 1}(p_1 - 1) \cdots (p_\ell - 1).$$

Nach Satz 5.5 ist das reguläre n-Eck genau dann mit Zirkel und Lineal konstruierbar, wenn $\varphi(n)$ eine Zweierpotenz ist. Dies ist genau dann der Fall, wenn jede ungerade

Primzahl $p = p_1, \ldots, p_\ell$ höchstens mit Vielfachheit 1 vorkommt und wenn in diesem Falle $p - 1$ eine Potenz von 2, also p eine Fermat-Primzahl ist. □

Was die tatsächliche Konstruktion angeht, so genügt es offensichtlich, für jede Fermat-Primzahl p eine Konstruktion des regulären p-Ecks anzugeben. Wie das geht, haben wir schon gesehen (siehe Satz 4.49). Für zusammengesetzte Zahlen n ergibt sich die Konstruktion dann leicht.

§6 Auflösbarkeit von Gleichungen

6.1 Spur und Norm

Es sei L/K eine endliche Körpererweiterung und $a \in L$. Die Linksmultiplikation

$$\ell_a : L \to L, \quad x \mapsto ax$$

ist eine K-lineare Abbildung, und wir hatten bereits das charakteristische Polynom

$$\mathrm{charpol}_{a/L/K}(X) := \det(X\mathrm{id}_L - \ell_a)$$

betrachtet.

Lemma 6.1 — *Es seien $K \subset L \subset M$ Körpererweiterungen und $a \in L$.*

1. $\mathrm{charpol}_{a/K(a)/K} = \mathrm{minpol}_{a/K}$.
2. $\mathrm{charpol}_{a/M/K} = \mathrm{charpol}_{a/L/K}^{[M:L]}$.
3. $\mathrm{charpol}_{a/L/K} = \mathrm{minpol}_{a/K}^{[L:K(a)]}$.

Beweis. Zu 1: Das Minimalpolynom $\mathrm{minpol}_{a/K}$ ist ein Teiler des charakteristischen Polynoms $\mathrm{charpol}_{a/K(a)/K}$. Da beide denselben Grad $[K(a) : K]$ haben und normiert sind, sind sie gleich.
Zu 2: Es sei $x_1, \ldots, x_n$ eine K-Basis von L und $y_1, \ldots, y_m$ eine L-Basis von M. Es sei B die Matrix zu ℓ_a bezüglich der Basis $x_1, \ldots, x_n$. Dann ist

$$x_1y_1, \ldots, x_ny_1, x_1y_2, \ldots, x_ny_m$$

eine K-Basis von M, und zu $\ell_a : M \to M$ gehört bezüglich dieser Basis die Matrix

$$\begin{pmatrix} B & & & \\ & B & & \\ & & \ddots & \\ & & & B \end{pmatrix}$$

mit $m = [L : M]$ Blockmatrizen entlang der Hauptdiagonalen. Aus der Multiplikativität des charakteristischen Polynoms für Blockmatrizen folgt $\mathrm{charpol}_{a/M/K} = \mathrm{charpol}_{a/L/K}^m$, wie behauptet.
Zu 3: Die Behauptung ist eine Konsequenz aus 1. und 2. □

Definition 6.2 — Es sei L/K eine endliche Körpererweiterung. Die Abbildungen

$$\mathrm{Sp}_{L/K} : L \to K, \quad a \mapsto \mathrm{Sp}_{L/K}(a) := \mathrm{tr}(\ell_a)$$

und

$$\mathrm{Nm}_{L/K} : L \to K, \quad a \mapsto \mathrm{Nm}_{L/K}(a) := \det(\ell_a)$$

heißen Spur und Norm von L/K.

Nach Definition gilt

$$\mathrm{charpol}_{a/L/K}(X) = X^n - \mathrm{Sp}_{L/K}(a)X^{n-1} + \ldots + (-1)^n \mathrm{Nm}_{L/K}(a),$$

mit $n = [L : K]$, d.h. bis auf Vorzeichen sind Spur und Norm genau der $n-1$-te und der 0-te Koeffizient des charakteristischen Polynoms. Aus Lemma 6.1 ergeben sich leicht eine Reihe von Eigenschaften von Spur und Norm:

Lemma 6.3 — *Es sei L/K eine endliche Körpererweiterung. Für alle $a, b \in L$ gilt*

$$\begin{aligned} \mathrm{Sp}_{L/K}(a+b) &= \mathrm{Sp}_{L/K}(a) + \mathrm{Sp}_{L/K}(b), \\ \mathrm{Nm}_{L/K}(ab) &= \mathrm{Nm}_{L/K}(a) \cdot \mathrm{Nm}_{L/K}(b). \end{aligned}$$

Insbesondere ist $\mathrm{Nm}_{L/K} : L^* \to K^*$ ein Gruppenhomomorphismus. Außerdem gilt $\mathrm{Sp}_{L/K}(a) = [L : K] \cdot a$ und $\mathrm{Nm}_{L/K}(a) = a^{[L:K]}$ für $a \in K$.

Beweis. Die erste Behauptung folgt sofort aus der Additivität der Spur bzw. der Multiplikativität der Determinante von Matrizen. Die zweite Aussage ergibt sich daraus, daß ℓ_a für $a \in K$ bezüglich jeder K-Basis von L die Matrix $aI_{[L:K]}$ hat. □

Lemma 6.4 — *Es sei L/K eine endliche Galoiserweiterung mit Galoisgruppe G. Es sei ferner $a \in L$ und $\{a_1, \ldots, a_n\}$ die G-Bahn von a. Dann gilt:*

$$\mathrm{minpol}_{a/K} = \prod_{i=1}^{n} (X - a_i)$$

und

$$\mathrm{charpol}_{a/K/L} = \prod_{\sigma \in G} (X - \sigma(a)).$$

Bezeichnet H die Standgruppe von a, so ist $K(a) = L^H$ und $H = \mathrm{Gal}(L/K(a))$.

Beweis. Die Gruppe G permutiert die Elemente der Bahn $B := \{a_1, \ldots, a_n\}$. Deshalb sind die Koeffizienten des Polynoms $f := (X - a_1) \cdot \ldots \cdot (X - a_n)$ invariant unter G und liegen in $L^G = K$. Insbesondere ist das Minimalpolynom von a ein Teiler von f. Umgekehrt ist klar, daß f ein Teiler des Minimalpolynoms ist. Da beide normiert sind, sind sie gleich.

Weiter ist klar, daß $K(a) \subset L^H$. Andererseits ist nach der Bahnengleichung

$$[K(a) : K] = \deg(\mathrm{minpol}_{a/K}) = |B| = |G|/|H| = [L : K]/[L : L^H] = [L^H : K].$$

Das impliziert $K(a) = L^H$ und $H = \mathrm{Gal}(L/K(a))$. Wir betrachten die Abbildung $\pi : G \to B, \sigma \mapsto \sigma(a)$. Dann ist $\pi^{-1}(a_i) = \sigma_i H$. Insbesondere kommt jedes a_i in der endlichen Folge $(\sigma(a))_{\sigma \in G}$ genau $|H|$ mal vor. D.h.

$$\prod_{\sigma \in G} (X - \sigma(a)) = \Big(\prod_{i=1}^{n} (X - a_i) \Big)^{|H|} = \mathrm{minpol}_{a/K}^{[L:K(a)]} = \mathrm{charpol}_{a/L/K}\,.$$

□

6.2 Zyklische Erweiterungen

Definition 6.5 — Eine endliche Galoiserweiterung L/K heißt zyklisch, wenn die Galoisgruppe $\mathrm{Gal}(L/K)$ eine zyklische Gruppe ist.

Der merkwürdige Name des folgenden berühmten Satzes rührt daher, daß er als "Satz 90" in Hilberts *Zahlbericht* für die Deutsche Mathematikervereinigung erscheint.

Satz 6.6 (Hilbert 90) — *Es sei L/K eine zyklische Galoiserweiterung und σ ein Erzeuger der Galoisgruppe. Die folgenden Aussagen sind für ein $a \in L$ äquivalent:*

$$\mathrm{Nm}_{L/K}(a) = 1 \qquad \Leftrightarrow \qquad a = \frac{b}{\sigma(b)} \text{ für ein } b \in L^\times.$$

Beweis. Es sei $n = [L : K]$. Da die Galoisgruppe zyklisch ist, gilt $\mathrm{Nm}_{L/K}(a) = \prod_{i=0}^{n-1} \sigma^i(a)$. Falls $a = b/\sigma(b)$ für ein $b \in L^\times$, so hat man

$$\mathrm{Nm}_{L/K}(a) = \frac{b}{\sigma(b)} \cdot \frac{\sigma(b)}{\sigma^2(b)} \cdot \ldots \cdot \frac{\sigma^{n-1}(b)}{\sigma^n(b)} = \frac{b}{\sigma^n(b)} = 1.$$

Zur Umkehrung: Es sei a mit $\mathrm{Nm}_{L/K}(a) = 1$ gegeben. Wegen der linearen Unabhängigkeit von $\mathrm{id}, \sigma, \ldots, \sigma^{n-1}$ ist die Abbildung $u : L \to L$ mit

$$u(x) = x + a\sigma(x) + a\sigma(a)\sigma^2(x) + \ldots + a\sigma(a)\sigma^2(a)\cdots\sigma^{n-2}(a)\sigma^{n-1}(x)$$

nicht die Nullabbildung. Wir wählen $y \in L$ mit $b := u(y) \neq 0$. Dann gilt:

$$\begin{aligned} a\sigma(b) &= a\sigma(u(y)) \\ &= a\sigma(y) + a\sigma(a\sigma(y)) + \ldots + a\sigma(a\sigma(a)\sigma^2(a)\cdots\sigma^{n-2}(a)\sigma^{n-1}(y)) \\ &= a\sigma(y) + a\sigma(a)\sigma^2(y) + \ldots + a\sigma(a)\sigma^2(a)\cdots\sigma^{n-2}(a)\sigma^{n-1}(y) \\ &\quad + \mathrm{Nm}_{L/K}(a)\sigma^n(y) \\ &= b, \end{aligned}$$

weil $\sigma^n(y) = y$ und $\mathrm{Nm}_{L/K}(a) = 1$ nach Voraussetzung. Damit ist $a = b/\sigma(b)$ wie verlangt. □

Satz 6.7 (Die reine Gleichung) — *Es sei $n \in \mathbb{N}$ und K ein Körper, der eine primitive n-te Einheitswurzel ζ enthält.*

1. *Ist L/K eine zyklische Erweiterung vom Grad n, dann ist $L = K(a)$ für ein Element a mit einem Minimalpolynom der Form $X^n - c \in K[X]$.*
2. *Ist umgekehrt $a \in \overline{K}$ eine Nullstelle eines Polynoms $X^n - c \in K[X]$, so ist $\mathrm{minpol}_{a/K} = X^d - b$ für einen Teiler d von n, $K(a)/K$ ist eine zyklische Erweiterung vom Grad d, und die Abbildung*

$$\mathbb{Z}/d \longrightarrow \mathrm{Gal}(K(a)/K), \quad k \mapsto (a \mapsto \zeta^{kn/d}a)$$

ist ein Gruppenisomorphismus. Ferner zerfällt $X^n - c$ zerfällt über $K(a)$ in Linearfaktoren und über K wie folgt: $X^n - c = \prod_{i=1}^{n/d}(X^d - \zeta^{di}b)$.

Beweis. 1. Es gilt $\mathrm{Nm}_{L/K}(\zeta) = \zeta^{[L:K]} = \zeta^n = 1$. Insbesondere gibt es nach Satz 90 von Hilbert ein $a \in L$ mit $\zeta\sigma(a) = a$. Es folgt induktiv:

$$\sigma^k(a) = a\zeta^{-k}$$

für $k = 0, \ldots, n-1$. Diese Werte sind paarweise verschieden, weil ζ eine primitive n-te Einheitswurzel ist. Insbesondere ist

$$(X-a)\cdot(X-a\zeta^{-1})\cdot\ldots\cdot(X-a\zeta^{n-1}) = X^n - a^n$$

das Minimalpolynom von a. Mit $c = a^n \in K$ folgt die Behauptung.
Zu 2. Ist a eine Nullstelle von $X^n - c$ in einem algebraischen Abschluß von K, so sind alle anderen von der Form $a\zeta^k$, $k = 0, \ldots, n-1$. Insbesondere ist $K(a)$ der Zerfällungskörper von $X^n - c$. Es sei $d := [K(a) : K]$. Für jedes $\sigma \in \mathrm{Gal}(K(a)/K)$ gibt es genau ein $\varphi(\sigma) \in \mathbb{Z}/n$ mit $\sigma(a) = a\zeta^{\varphi(\sigma)}$. Dies definiert eine injektive Abbildung

$$\varphi : \mathrm{Gal}(K(a)/K) \to \mathbb{Z}/n.$$

Außerdem gilt

$$\zeta^{\varphi(\tau\sigma)}a = \tau(\sigma(a)) = \tau(\zeta^{\varphi(\sigma)}a) = \zeta^{\varphi(\sigma)}\tau(a) = \zeta^{\varphi(\sigma)}\zeta^{\varphi(\tau)}a = \zeta^{\varphi(\sigma)+\varphi(\tau)}a.$$

Der Vergleich zeigt, daß $\varphi(\tau\sigma) = \varphi(\sigma) + \varphi(\tau)$, mit anderen Worten, φ ist ein Gruppenhomomorphismus. Notwendigerweise ist das Bild von φ die zu $\mathbb{Z}/d$ isomorphe Untergruppe, die von der Restklasse $\overline{n/d}$ erzeugt wird. Deshalb wird die Galoisgruppe von der Abbildung $a \mapsto a\zeta^{n/d}$ erzeugt. Bezeichnet $\xi := \zeta^{n/d}$ diese primitive d-te Einheitswurzel, so ist das Minimalpolynom von a durch

$$(X-a)(X-\xi a)\cdots(X-\xi^{d-1}a) = X^d - a^d =: X^d - b$$

gegeben. Schließlich gilt:

$$X^n - c = \prod_{i=0}^{n-1}(X-\zeta^i a) = \prod_{j=0}^{n/d-1}\prod_{i=0}^{d-1}(X-\xi^i\zeta^j a) = \prod_{j=0}^{n/d-1}(X^d - (\zeta^j a)^d).$$

□

Satz 6.8 (Hilbert 90, additive Variante) — *Es sei L/K eine zyklische Galoiserweiterung und σ ein Erzeuger der Galoisgruppe. Die folgenden Aussagen sind für ein $a \in L$ äquivalent:*

$$\mathrm{Sp}_{L/K}(a) = 0 \qquad \Leftrightarrow \qquad a = b - \sigma(b) \text{ für ein } b \in L.$$

Beweis. Die Richtung $\Leftarrow$ ist wieder einfach. Für die umgekehrte Richtung sei $a \in L$ mit $\mathrm{Sp}_{L/K}(a) = 0$ vorgegeben. Wir wählen ein $y \in L$ mit $\mathrm{Sp}_{L/K}(y) \neq 0$ und bilden

$$c = a\sigma(y) + (a+\sigma(a))\sigma^2(y) + \ldots + (a+\sigma(a)+\ldots+\sigma^{n-2}(a))\sigma^{n-1}(y).$$

Für dieses Element gilt

$$c - \sigma(c) = a\Big(\sigma(y) + \sigma^2(y) + \ldots + \sigma^{n-1}(y)\Big) - \Big(\sigma(a) + \sigma^2(a) + \ldots + \sigma^{n-1}(a)\Big)y.$$

Da $\mathrm{Sp}_{L/K}(a) = 0$, ist der Koeffizient von y in $c - \sigma(c)$ genau a. Deshalb hat man weiter

$$c - \sigma(c) = a(y + \sigma(y) + \ldots + \sigma^{n-1}(y)) = a\ \mathrm{Sp}_{L/K}(y).$$

Nach Wahl von y ist das Element $\mathrm{Sp}_{L/K}(y) \in K^\times$. Mit $b := c/\mathrm{Sp}_{L/K}(y)$ folgt die Behauptung. □

In einem Körper der Charakteristik p hat das Polynom $X^p - X$ nach dem kleinen Fermatschen Satze die p-Nullstellen $0, 1, \ldots, (p-1)$. Deshalb besteht die Faktorisierung

$$X^p - X = X \cdot (X-1) \cdot \ldots \cdot (X-(p-1)).$$

Substitutiert man X durch $X - a$ mit einem beliebigen Element a erhält man

$$X^p - X - (a^p - a) = (X-a)(X-a-1) \cdot \ldots \cdot (X-a-p+1).$$

Diese kleine Rechnung wird im Beweis des folgenden Satzes benutzt:

Satz 6.9 (Artin – Schreier) — *Es sei K ein Körper der Charakteristik $p > 0$ und L/K eine endliche Erweiterung.*

1. *Ist L/K eine zyklische Galoiserweiterung vom Grad p, dann ist $L = K(a)$ für ein a mit einem Minimalpolynom der Form $X^p - X - c \in K[X]$.*
2. *Umgekehrt zerfällt jedes Polynom $X^p - X - c \in K[X]$ entweder schon in K vollständig in Linearfaktoren oder ist irreduzibel. Ist im zweiten Falle a eine Nullstelle in einem algebraischen Abschluß, so ist $K(a)/K$ eine zyklische Galoiserweiterung, und die Abbildung*

$$\mathbb{Z}/p \to \mathrm{Gal}(K(a)/K), \quad k \mapsto (a \mapsto a + k),$$

ist ein Gruppenisomorphismus.

Beweis. Es sei zunächst L/K zyklisch vom Grad p. Es gilt $\mathrm{Sp}_{L/K}(-1) = -p = 0$. Deshalb gibt es nach der additiven Variante des Satzes von Hilbert ein $a \in L$ mit $-1 = a - \sigma(a)$, oder $\sigma(a) = a + 1$. Dann kann a nicht in K liegen. Nach dem Gradsatz ist $[K(a) : K]$ ein Teiler von $[L : K] = p$. Deshalb ist $K(a) = L$. Das Minimalpolynom bestimmt sich so: Induktiv gilt $\sigma^k(a) = a + k$ für alle $k = 0, \ldots, p-1$. Also ist

$$\begin{aligned} \mathrm{minpol}_{a/K} &= \prod_{k=0}^{p-1} (X - \sigma^k(a)) \\ &= (X-a)(X-a-1)\cdots(X-a-p+1) = X^p - X - (a^p - a). \end{aligned}$$

Das war zu zeigen.

Ist umgekehrt das Polynoms $X^p - X - c \in K[X]$ vorgegeben und a eine Nullstelle in einer Erweiterung von K, so gilt für $i = 0, \ldots, p-1$, daß $(a+i)^p - (a+i) - c = (a^p - a - c) + (i^p - i) = 0$. Enthält also eine Erweiterung von K eine Nullstelle, so enthält sie alle. Folglich zerfällt $X^p - X - c$ entweder in $K[X]$ vollständig in Linearfaktoren oder ist irreduzibel. Im zweiten Falle hat der Zerfällungskörper den Grad p und ist separabel, weil das Polynom p verschiedene Nullstellen hat. Ist a eine Nullstelle, so wird die Galoisgruppe offensichtlich durch $a \mapsto a+1$ erzeugt, und diese Abbildung hat die Ordnung p. □

6.3 Auflösbare Gleichungen

Es sei K ein Körper und $f \in K[X]$ ein separables Polynom vom Grad n. Wir wollen in diesem Abschnitt die Frage betrachten, unter welchen Bedingungen sich die Nullstellen von f durch Wurzelausdrücke in den Koeffizienten von f beschreiben lassen. Wir wollen die folgende Sprechweise verwenden: Es sei L ein Zerfällungskörper von f. Wir bezeichnen die Galoisgruppe $\mathrm{Gal}(L/K)$ kurz als Gruppe der Gleichung $f = 0$.

Definition 6.10 — Eine Erweiterung M/K ist eine Radikalerweiterung, wenn M/K eine zyklische Erweiterung vom Grad m ist, wobei m entweder die Charakteristik von K ist oder m zur Charakteristik prim ist und K eine primitive m-te Einheitswurzel enthält.

Definition 6.11 — Es sei K ein Körper und $f \in K[X]$ ein irreduzibles Polynom. f heißt durch Radikale auflösbar, wenn es eine Kette von Körpererweiterungen $K = K_0 \subset K_1 \subset \ldots \subset K_n$ mit den folgenden Eigenschaften gibt: K_n enthält eine Nullstelle von f und für jedes $i = 1, \ldots, n$ ist K_i/K_{i-1} eine Radikalerweiterung.

Definition 6.12 — Eine Galoiserweiterung L/K heißt auflösbar, wenn die Galoisgruppe $\mathrm{Gal}(L/K)$ auflösbar ist.

Satz 6.13 — *Die folgenden Aussagen sind für ein irreduzibles Polynom $f \in K[X]$ äquivalent:*

1. *f ist durch Radikale auflösbar.*
2. *Die Gruppe der Gleichung $f = 0$ ist auflösbar.*

Beweis. $1 \Rightarrow 2$: Es sei $K = K_0 \subset \ldots \subset K_n$ eine Kette von Erweiterungen mit den Eigenschaften der Definition 6.11. Wir konstruieren induktiv Körper $L_k \subset \overline{K}_n$, $k = 0, \ldots, n$ mit

1. $K_0 = L_0$ und $K_i \subset L_i$ für alle $i = 1, \ldots, n$.
2. L_i/K ist eine Galoiserweiterung.

3. $\mathrm{Gal}(L_i/L_{i-1})$ ist auflösbar.

Es sei $0 < i \leq n$ gegeben und L_{i-1} bereits konstruiert. Wir betrachten das Kompositum $K_i' = K_i L_{i-1}$. Dann ist K_i'/L_{i-1} eine Galoiserweiterung, und es gibt eine kanonische Injektion $\mathrm{Gal}(K_i'/L_{i-1}) \to \mathrm{Gal}(K_i/K_{i-1})$. Insbesondere ist $\mathrm{Gal}(K_i'/L_{i-1})$ zyklisch von einer Ordnung m, wobei entweder $m = \mathrm{char}(K) > 0$ oder m prim zur Charakteristik ist und K_{i-1}, also auch L_{i-1}, eine primitive m-te Einheitswurzel enthält, d.h. K_i'/L_{i-1} ist eine Radikalerweiterung. Also ist L'/L_{i-1} eine einfache Erweiterung, $L_i' = L_{i-1}(a)$, wobei das Minimalpolynom von a die Form $X^m - X - c$ oder $X^m - c$ für ein $c \in L_{i-1}$ hat. Die Erweiterung L_{i-1}/K ist nach Induktionsannahme normal. Es seien $c = c_1, \ldots, c_\ell \in L_{i-1}$ die zu c konjugierten Elemente, ferner $a_j \in \overline{K}_n$ eine Nullstelle des Polynoms $X^m - X - c_j$ bzw. $X^m - c_j$ für $j = 1, \ldots, \ell$. Die Erweiterungen $L_{i-1}(a_j)/L_{i-1}$ sind zyklisch der Ordnung m. Wir betrachten die Erweiterungen

$$L_{i-1} \subset L_{i-1}(a_1) \subset L_{i-1}(a_1, a_2) \subset \ldots \subset L_{i-1}(a_1, a_2, \ldots, a_\ell) =: L_i.$$

Dann ist L_i/K normal, und jede Erweiterung $L_{i-1}(a_1, \ldots, a_j)/L_{i-1}(a_1, \ldots, a_{j-1})$ ist eine Galoiserweiterung, deren Galoisgruppe isomorph zu einer Untergruppe von $\mathrm{Gal}(L_{i-1}(a_j)/L_{i-1})$ und daher zyklisch ist. Für die Galoisgruppe $\mathrm{Gal}(L_i/L_{i-1})$ heißt das, daß es eine Filtrierung durch Normalteiler gibt, deren Faktorgruppen zyklisch sind. Das bedeutet: $\mathrm{Gal}(L_i/L_{i-1})$ ist auflösbar. Das beendet den Induktionsschritt.

Insgesamt erhält man einen Körper L_n, der K_n und damit eine Wurzel von f enthält, der eine Galoiserweiterung von K ist, und der eine Kette von Zwischenkörpern mit auflösbaren Galoisgruppen enthält. Demnach hat $\mathrm{Gal}(L_n/K)$ eine Filtrierung durch Normalteiler mit auflösbaren Faktorgruppen und ist damit selbst auflösbar. Der Zerfällungskörper F von f ist nach Konstruktion ein Zwischenkörper von L_n/K, und die Galoisgruppe $\mathrm{Gal}(F/K)$ folglich eine Faktorgruppe von $\mathrm{Gal}(L_n/K)$. Da Faktorgruppen von auflösbaren Gruppen wieder auflösbar sind, ist $\mathrm{Gal}(F/K)$ auflösbar. Das war zu zeigen.

$2 \Rightarrow 1$: Es sei F ein Zerfällungskörper von f. Nach Annahme ist die Galoisgruppe $G = \mathrm{Gal}(L/K)$ auflösbar. Es sei $N = |G|$. Es seien $q_1, \ldots, q_\ell$ alle Primzahlen $\leq N$ und $\neq \mathrm{char}(K)$, und der Größe nach aufsteigend sortiert. Wir konstruieren rekursiv Körpererweiterungen $K = K_0 \subset K_1 \subset \ldots \subset K_\ell$ mit der Eigenschaft, daß K_j alle primitiven Einheitswurzeln der Ordnungen $q_1, \ldots, q_j$ enthält. Es sei dazu $k > 0$ und K_{k-1} schon konstruiert und ζ eine primitive q_k-te Einheitswurzel. Nach Wahl der q_i's ist q_k prim zur Charakteristik, falls diese endlich ist. Die Galoisgruppe $\mathrm{Gal}(K_{k-1}(\zeta)/K_{k-1})$ ist isomorph zu einer Untergruppe von $\mathbb{Z}/(q_k - 1)$ und daher abelsch und hat eine Ordnung, deren sämtliche Primfaktoren kleiner als q_k sind. Es gibt daher eine Filtrierung der Galoisgruppe durch Untergruppen mit zyklischen Faktoren derselben Primzahlordnungen und dazugehörig eine Kette von zyklischen Körpererweiterungen

$$K_{k-1} = K_{k-1,0} \subset K_{k-1,1} \subset K_{k-1,2} \subset \ldots \subset K_{k-1,s} = K_{k-1}(\zeta) =: K_k,$$

wobei der Körpergrad $[K_{i-1,t} : K_{i-1,t-1}]$ an jeder Stelle entweder eine der Primzahlen $q_1, \ldots, q_{k-1}$ oder die Charakteristik von K ist. Insbesondere sind alle Erweiterungen $K_{i-1,t}/K_{i-1,t-1}$ Radikalerweiterungen. Nach Induktionsannahme enthält K_{i-1} die q_i-ten Einheitswurzeln für alle $i \leq k-1$.

Es sei nun L das Kompositum von K_ℓ und F in einem gemeinsamen algebraischen Abschluß. Dann ist $\mathrm{Gal}(L/K_\ell)$ eine Untergruppe von $\mathrm{Gal}(F/K)$ und nach Annahme auflösbar und hat eine Ordnung $\leq N$. Folglich gibt es eine Filtrierung von $\mathrm{Gal}(L/K_\ell)$ durch Normalteiler mit zyklischen Faktoren von Primzahlordnung $\leq N$. Dazu gehört eine Kette von zyklischen Körpererweiterungen

$$K_\ell = K_{\ell,0} \subset K_{\ell,1} \subset K_{\ell,2} \subset \ldots \subset K_{\ell,u} = L,$$

wobei der Körpergrad $[K_{\ell,t} : K_{\ell,t-1}]$ an jeder Stelle entweder eine der Primzahlen $q_1, \ldots, q_\ell$ oder die Charakteristik von K ist, d.h. alle Erweiterungen $K_{\ell-1,t}/K_{\ell-1,t-1}$ sind Radikalerweiterungen.

Nach Konstruktion hat f eine Nullstelle in L. Zusammengenommen heißt das, daß f eine Auflösung durch Radikale besitzt. □

Es sei wieder allgemein K ein Körper, $f \in K[X]$ ein separables Polynom. Es seien $\alpha_1, \alpha_2, \ldots, \alpha_n \in L$ die Nullstellen von f im Zerfällungskörper L von f. Jedes Element $g \in \mathrm{Gal}(L/K)$ permutiert die Nullstellen, d.h. es gibt eine eindeutige Permutation $\overline{g} \in S_n$ mit der Eigenschaft, daß

$$g(\alpha_i) = \alpha_{\overline{g}(i)} \quad \text{für alle } i = 1, \ldots, n.$$

Dies definiert einen Gruppenhomomorphismus

$$\varphi : \mathrm{Gal}(L/K) \to S_n, \quad g \mapsto \overline{g}.$$

Da L von den Nullstellen von f erzeugt wird, ist jedes $g \in G$ vollständig durch die Wirkung auf den Nullstellen bestimmt. Insbesondere ist der Homomorphismus φ injektiv, und wir können $\mathrm{Gal}(L/K)$ als Untergruppe von S_n auffassen.

Allerdings hängt φ von der Numerierung der Nullstellen ab. Je zwei Numerierungen

$$\{\alpha_1, \ldots, \alpha_n\} = \{\alpha'_1, \ldots, \alpha'_n\}$$

unterscheiden sich um eine Permutation π mit $\alpha'_i = \alpha_{\pi(i)}$. Bezeichnet $\varphi' : \mathrm{Gal}(L/K) \to S_n$ die Einbettung zur zweiten Numerierung, so gilt:

$$\alpha_{\pi(\varphi'(g)(i))} = \alpha'_{\varphi'(g)(i)} = g(\alpha'_i) = g(\alpha_{\pi(i)}) = \alpha_{\varphi(g)(\pi(i))},$$

d.h.

$$\varphi'(g) = \pi^{-1} \circ \varphi(g) \circ \pi.$$

Die Einbettungen zu verschiedenen Numerierungen sind also konjugiert.

Lemma 6.14 — *Mit diesen Bezeichnungen gilt:*

1. *Die Ordnung von* $\mathrm{Gal}(L/K)$ *ist ein Teiler von* $n!$.
2. *Wenn* f *irreduzibel ist, operiert* $\mathrm{Gal}(L/K)$ *transitiv auf den Nullstellen von* f. *In diesem Falle ist* n *ein Teiler von* $|\mathrm{Gal}(L/K)|$.

Beweis. Die erste Behauptung folgt einfach daraus, daß $\mathrm{Gal}(L/K)$ eine Untergruppe von S_n ist. Es ist weiter klar, daß für ein irreduzibles Polynom alle Nullstellen von f in einer Bahn unter der Galoisgruppe liegen. Die Teilbarkeitsrelation ist eine Konsequenz der Bahnengleichung: Die Länge jeder Bahn ist ein Teiler der Gruppenordnung. □

Folgerung 6.15 — *Es sei* $f \in K[X]$ *ein Polynom vom Grad* ≤ 4. *Dann ist die Gleichung* $f = 0$ *durch Radikale auflösbar.*

Beweis. Die Gruppe der Gleichung $f = 0$ ist eine Untergruppe von S_4 und deshalb auflösbar. □

Bemerkung 6.16 — Es sei K ein Körper. Die symmetrische Gruppe S_n wirkt auf dem rationalen Funktionenkörper $M := K(X_1, \ldots, X_n)$ durch Vertauschung der Unbestimmten. Die Erweiterung M/M^{S_n} ist eine Galoiserweiterung mit Galoisgruppe S_n. Dies ist einfach ein Spezialfall von Lemma 4.30. Mit Hilfe des Hauptsatzes über symmetrische Polynome können wir aber mehr sagen: Zunächst gibt es einen Ringisomorphismus

$$K[Y_1, \ldots, Y_n] \longrightarrow K[X_1, \ldots, X_n]^{S_n}$$

der die Unbestimmte Y_i mit dem i-ten elementarsymmetrischen Polynom in den Unbestimmten X_j identifiziert. Dieser Isomorphismus induziert eine Abbildung der Funktionenkörper:

$$K(Y_1, \ldots, Y_n) \xrightarrow{\psi} K(X_1, \ldots, X_n)^{S_n} \subset K(X_1, \ldots, X_n).$$

Wir wollen zeigen, daß ψ ein Isomorphismus ist. Dazu ist zu zeigen, daß jede symmetrische rationale Funktion $f \in K(X_1, \ldots, X_n)$ sich als Quotient zweier symmetrischer Polynome $p, q \in K[X_1, \ldots, X_n]$ schreiben läßt. Das ist leicht: Es sei $f = p/q$ irgendeine Darstellung von f als Quotient zweier Polynome p, q. Wir bilden

$$f = \frac{p}{q} = \frac{p \cdot \prod_{\sigma \in S_n \setminus \{\mathrm{id}\}} \sigma(q)}{\prod_{\sigma \in S_n} \sigma(q)}.$$

Der Nenner $\tilde{q} = \prod_{\sigma \in S_n} \sigma(q)$ ist invariant. Der Zähler $\tilde{p} = p \cdot \prod_{\sigma \in S_n \setminus \{\mathrm{id}\}} \sigma(q)$ aber auch, denn er läßt sich als Produkt der symmetrischen Funktionen f und $\tilde{q}$ schreiben.

Das zeigt, daß $K(X_1, \ldots, X_n)/K(Y_1, \ldots, Y_n)$ eine Galoiserweiterung mit Galoisgruppe S_n ist. Die Unbestimmten X_i sind Nullstellen der Gleichung

$$X^n - Y_1 X^n + Y_2 X^{n-2} + \ldots + (-1)^n Y_n = 0.$$

Diese Gleichung läßt sich als die allgemeine Gleichung vom Grad n über dem Körper K auffassen. Für $n \geq 5$ ist die Galoisgruppe S_n nicht auflösbar. In diesem Sinne gibt es keine Lösungs*formeln* für die Nullstellen, die sich durch Radikale in den Unbestimmten Y_i ausdrücken lassen.

Trotzdem gibt es ja Gleichungen vom Grad $n \geq 5$, die sich durch Radikale lösen lassen. Das einfachste Beispiel liefern die 11.ten Einheitswurzeln: Das Minimalpolynom von $\cos(2\pi/11)$ hat Grad 5, und der Zerfällungskörper ist zyklisch vom Grad 5. Die Auflösbarkeit wurde für dieses Beispiel zuerst von Vandermonde beschrieben. (Vgl. das lesenswerte Buch von Tignol).

Im Prinzip könnte es nun sein, daß sich jede Gleichung durch Radikale lösen läßt, auch wenn es keine allgemeine Lösungsformel gibt. Wir werden gleich sehen, daß dies nicht der Fall ist, indem wir Körpererweiterungen von $\mathbb{Q}$ mit Galoisgruppe S_n konstruieren.

Von einem etwas allgemeineren Standpunkt aus könnte man die Frage auch so angehen: Gegeben ein Körper K und ein endliche Gruppe G; gibt es eine Galoiserweiterung L/K mit Galoisgruppe $\mathrm{Gal}(L/K) = G$? Dies ist das 'inverse Galoisproblem'. Invers deshalb, weil wir nicht den Körper vorgeben und die Galoisgruppe suchen, sondern umgekehrt die Gruppe vorgeben. Für endliche Körper ist die Antwort leicht: Genau die zyklischen Gruppen kommen als Galoisgruppen vor. Für $K = \mathbb{Q}$ ist noch immer unklar, ob sich jede endliche Gruppe als Galoisgruppe einer Erweiterung von $\mathbb{Q}$ realisiern läßt. Für die symmetrischen Gruppen ist dies tatsächlich der Fall, wie wir zeigen werden.

Wir betrachten zunächst ein einfaches Beispiel:

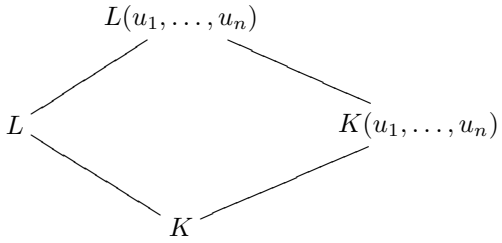
Beispiel 6.17 — Es sei $L/\mathbb{Q}$ der Zerfällungskörper des Polynoms $f = X^5 - 4X - 2$. Mit dem Eisensteinkriterium folgt sofort, daß f irreduzibel ist. Als Funktion auf $\mathbb{R}$ hat f genau zwei Extremstellen und deshalb genau drei reelle Nullstellen. Die beiden übrigen Nullstellen sind komplex konjugiert. Die komplexe Konjugation ist daher ein Element der Galoisgruppe $G = \mathrm{Gal}(L/\mathbb{Q})$ und entspricht unter der Einbettung $G \subset S_5$ einer Transposition. Da 5 ein Teiler der Ordnung von G und eine Primzahl ist, enthält G ein Element der Ordnung 5. Unter der Einbettung $G \subset S_5$ muß dieses Element einem 5-Zykel entsprechen. Die Galoisgruppe G ist also eine Untergruppe von S_5, die einen 5-Zykel und eine Transposition enthält. Man kann zeigen (Übung), daß G dann schon mit S_5 übereinstimmen muß.

23. Juni 2008

Wir folgen van der Waerden in der Beschreibung eines Verfahrens, die Galoisgruppe zu bestimmen.

Wir gehen von der folgenden Situation aus: K ist ein Körper, L/K der Zerfällungskörper eines separablen normierten Polynom $f \in K[X]$ vom Grad n. Wir betrachten die Funktionenkörper $K(u_1, \ldots, u_n)$ und $L(u_1, \ldots, u_n)$ mit Unbestimmten

$u_1, \ldots, u_n$.



Zur Erinnerung: Der Funktionenkörper $K(u_1, \ldots, u_n)$ ist der Quotientenkörper des Polynomrings $K[u_1, \ldots, u_n]$. Wir lassen die Galoisgruppe $G = \mathrm{Gal}(L/K)$ auf dem Körper $L(u_1, \ldots, u_n)$ wirken, indem jedes $g \in G$ nur auf den Koeffizienten einer rationalen Funktion $f \in L(u_1, \ldots, u_n)$ wirkt, aber die Unbestimmten fest läßt, d.h. $g(u_i) = u_i$ für alle $i = 1, \ldots, n$.

Lemma 6.18 — $L(u_1, \ldots, u_n)^G = K(u_1, \ldots, u_n)$. *Insbesondere ist die Inklusion* $K(u_1, \ldots, u_n) \to L(u_1, \ldots, u_n)$ *eine Galoiserweiterung mit Galoisgruppe* G.

Beweis. Es genügt, die erste Behauptung zu beweisen. Dabei ist die Inklusionsbeziehung "$\supset$" klar. Es sei umgekehrt $z \in L(u_1, \ldots, u_n)^G$, und zwar gegeben als Quotient $z = a/b$ mit $a, b \in L[u_1, \ldots, u_n]$. Wir betrachten

$$\tilde{b} = \prod_{g \in G} g(b), \quad \tilde{a} = a \cdot \prod_{g \in G \setminus \{\mathrm{id}\}} g(b).$$

Dann ist $\tilde{b} \in L[u_1, \ldots, u_n]^G = K[u_1, \ldots, u_n]$. Folglich ist auch $\tilde{a} = z\tilde{b}$ einerseits invariant, andererseits ein Polynom, und liegt deshalb in $K[u_1, \ldots, u_n]$. Das zeigt, daß $z = \tilde{a}/\tilde{b} \in K(u_1, \ldots, u_n)$. □

Wir betrachen nun das Element

$$\theta := u_1\alpha_1 + \ldots + u_n\alpha_n = \sum_{i=1}^{n} u_i\alpha_i \in L[u_1, \ldots, u_n],$$

wo α_1,..., α_n die Nullstellen von f sind. Man kann θ als eine universelle Linearkombination der Nullstellen von f auffassen. Die Bilder von θ unter G sind offenbar paarweise verschieden. Deshalb ist

$$T := \prod_{g \in G} (X - g(\theta)) \in K(u_1, \ldots, u_n)[X]$$

das Minimalpolynom von θ bezüglich $K(u_1, \ldots, u_n)$. Aus der Konstruktion geht sogar genauer hervor, daß

$$T \in K[u_1, \ldots, u_n][X].$$

Wir betrachten nun neben der Wirkung von G auf $L(u_1, \ldots, u_n)$ eine andere Wirkung der Gruppe S_n auf $L(u_1, \ldots, u_n)$ und $K(u_1, \ldots, u_n)$, die dazu in dem folgenden Sinne komplementär ist: Wir setzen für $\pi \in S_n$ die Wirkung durch

$$\pi|_L = \mathrm{id}_L, \quad \text{und} \quad \pi(u_i) = u_{\pi(i)} \text{ für } i = 1, \ldots, n.$$

fest. Damit bilden wir das Polynom

$$F = \prod_{\pi \in S_n} (X - \pi(\theta)) \qquad \in L(u_1, \ldots, u_n)[X].$$

Die Koeffizienten von F (als Polynom in X) sind Polynome in den u_i und α_i mit Koeffizienten in K. Sie sind genauer symmetrische Polynome in α_1,..., α_n und lassen sich nach dem Hauptsatz über symmetrische Polynome durch die Koeffizienten von f ausdrücken. Es folgt:

$$F \in K[u_1, \ldots, u_n][X].$$

Die Gruppe G besitzt nun eine Einbettung $\varphi : G \to S_n$, $g \mapsto \overline{g}$, mit der Eigenschaft

$$g(\alpha_i) = \alpha_{\overline{g}(i)}.$$

Man beachte, daß für ein $g \in G$ und $z \in L(u_1, \ldots, u_n)$ die Elemente $g(z)$ und $\overline{g}(z)$ verschieden sind: Bei der Berechnung von $g(z)$ geht die Wirkung von g auf den Skalaren in L ein, bei $\overline{g}(z)$ die Wirkung der Permutation $\overline{g}$ auf den Unbestimmten u_i. Speziell beim Element θ hängen die Ergebnisse aber eng zusammen:

$$g(\theta) = \sum_{i=1}^{n} u_i g(\alpha_i) = \sum_{i=1}^{n} u_i \alpha_{\overline{g}(i)} = \sum_{j=1}^{n} u_{\overline{g}^{-1}(j)} \alpha_j = \overline{g}^{-1}(\sum_j u_j \alpha_j) = \overline{g}^{-1}(\theta).$$

Es seien nun $\pi_1, \ldots, \pi_\ell \in S_n$ Vertreter für die Nebenklassen $S_n/\varphi(G)$. Dann gilt:

$$\begin{aligned} F &= \prod_{\pi \in S_n} (X - \pi(\theta)) = \prod_{j=1}^{\ell} \prod_{g \in G} (X - \pi_j \overline{g}(\theta)) \\ &= \prod_{j=1}^{\ell} \pi_j \left(\prod_{g \in G} (X - g^{-1}(\theta)) \right) = \prod_{j=1}^{\ell} \pi_j(T). \end{aligned}$$

Wir wissen, daß T irreduzibel in $K[u_1, \ldots, u_n][X]$ ist. Dasselbe gilt dann auch für die Bilder $\pi_j(T)$. Damit erweist sich

$$F = \pi_1(T) \cdot \ldots \pi_\ell(T).$$

als die Zerlegung vn F in irreduzible Faktoren im faktoriellen Ring $K[u_1, \ldots, u_n]$.

Lemma 6.19 — *1. Die Permutationen $\pi \in S_n$ vertauschen die irreduziblen Faktoren von F transitiv.*
2. Es sei $G_j := \{g \in S_n \mid \pi(\pi_j(T)) = \pi_j(T)\}$. Es gilt $g \in G_j$ genau dann, wenn g einen Linearfaktor von $\pi_j(T)$ in einen Linearfaktor von $\pi_j(T)$ abbildet.
3. Es gilt $G_j = \pi_j \varphi(G) \pi_j^{-1}$.

Beweis. Die Bilder $\pi(\theta)$, $\pi \in S_n$, sind paarweise verschieden, weil die Elemente $\alpha_1, \ldots, \alpha_n$ paarweise verschieden sind. Die Gruppe S_n operiert transitiv auf den Linearfaktoren $(X - \pi(\theta))$ von F. Da die Primfaktorzerlegung von F in $A[u_1, \ldots, u_n][X]$

eindeutig ist (durch die Normierung der Leitkoeffizienten bzgl. X), vertauscht $\pi \in S_n$ die Primfaktoren von F. Wegen der Transitivität auf den Linearfaktoren muß auch diese Wirkung auf den Linearfaktoren transitiv sein. Das beweist Aussage 1.

Haben insbesondere $\pi_j(T)$ und $\pi\pi_j(T)$ auch nur einen einzigen Linearfaktor gemeinsam, so müssen sie schon gleich sein. Das zeigt Aussage 2. Für jedes $g \in G$ gilt

$$\pi_j \overline{g} \pi_j^{-1}(\pi(T)) = \pi_j(\overline{g}(T)) = \pi_j(g^{-1}(T)) = \pi_j(T).$$

Das bedeutet, daß $\pi_j \varphi(G) \pi_j^{-1} \subset G_j$. Andererseits ist $|G| = |S_n|/\ell = |G_j|$ wegen der transitiven Wirkung von S_n auf gleichmächtigen Mengen der Restklassen S_n/G bzw. der Faktoren von F. Aus der Inklusion der Gruppen folgt wegen der Gleichmächtigkeit die behauptete Gleichheit $G_j = \pi_j \varphi(G) \pi_j^{-1}$. □

Das Lemma kann man so lesen: Seiner Definition nach hängt das Polynom T von der Kenntnis der Galoisgruppe G und der Wahl einer Numerierung der Nullstellen ab. Aber man kann allein aus der Kenntnis von f das Polynom F vom Grad $n!$ bestimmen. Wenn wir weiter davon ausgehen, daß wir die Primfaktorzerlegung von F im Ring $K[u_1, \ldots, u_n]$ ausführen können, diese sei $F = F_1 \cdot \ldots \cdot F_\ell$, dann können wir auch die Standgruppen

$$G_j = \{\pi \in S_n \mid \pi(F_j) = F_j\}$$

bestimmen. Das Lemma sagt nun, daß alle Gruppen G_j, $j = 1, \ldots, n$ untereinander und zur Galoisgruppe G konjugiert sind.

Mit Hilfe des Lemmas können wir nun den folgenden Satz von van der Waerden beweisen.

Satz 6.20 — *Es sei A ein faktorieller Ring mit Quotientenkörper K, ferner $\mathfrak{p} \subset A$ ein Primideal, $\overline{A} := A/\mathfrak{p}$ der Restklassenring und $\overline{K}$ dessen Quotientenkörper. Es sei $f \in A$ ein normiertes Polynom vom Grad n mit der Eigenschaft, daß f und die Reduktion $\overline{f} = f \bmod \mathfrak{p} \in \overline{A}[X]$ separabel sind. Es seien G bzw. $\overline{G}$ die Galoisgruppen von f und $\overline{f}$. Dann ist $\overline{G}$, aufgefaßt als Untergruppe von S_n, konjugiert zu einer Untergruppe von $G \subset S_n$.*

Beweis. Wir konstruieren nach dem oben beschriebenen Verfahren zu f das Polynom $F \in K[u_1, \ldots, u_n][X]$, seine Primfaktorzerlegung $F = F_1 \cdot \ldots \cdot F_\ell$ und die Standgruppen G_j zu den Faktoren F_j. Gemäß den besonderen Annahmen des Satzes hat f aber schon Koeffizienten im Ring A. Entsprechend dem Hauptsatz über symmetrische Polynome kann man das obige Argument dahingehend verschärfen, daß F dann auch ein Polynom in $A[u_1, \ldots, u_n][X]$ ist. Wegen des Satzes von Gauß liegen auch die irreduziblen Faktoren F_j von F schon in $A[u_1, \ldots, u_n][X]$.

Konstruiert man nun in analoger Weise zu $\overline{f} \in \overline{A}[X] \subset \overline{K}[X]$ das Polynom $\overline{F} \in \overline{K}[u_1, \ldots, u_n][X]$, so ist aus der Konstruktion klar, daß $\overline{F}$ das Bild von F unter der Reduktionsabbildung

$$A[u_1, \ldots, u_n][X] \to \overline{A}[u_1, \ldots, u_n][X] \to \overline{K}[u_1, \ldots, u_n][X]$$

ist. Bezeichnen weiter $\overline{F}_1, \ldots, \overline{F}_\ell$ die Bilder der Faktoren $F_1, \ldots, F_\ell$, so hat man in $\overline{K}[u_1, \ldots, u_n][X]$ die Faktorzerlegung $\overline{F} = \overline{F}_1 \cdot \ldots, \cdot \overline{F}_\ell$. Aber natürlich brauchen die Polynome $\overline{F}_j$ nicht irreduzibel zu sein, sondern können (und werden in der Regel) weiter zerfallen, etwa wie folgt:

$$\overline{F}_j = F_{j_1} \cdot \ldots \cdot F_{js_j}, \quad j = 1, \ldots, \ell.$$

Nun gilt für jede Permutation $\pi \in S_n$: Wenn $\pi(F_{11}) = F_{11}$, dann bildet π einen Linearfaktor von F_{11}, also insbesondere von $\overline{F}_1$, auf einen Linearfaktor von F_{11} und damit von $\overline{F}_1$ ab. Aber wegen Aussage 2 des Lemmas 6.19 heißt das, daß $\pi(F_1) = F_1$. Kurzum: Die Standgruppe von F_{11} ist eine Untergruppe der Standgruppe von F_1. Wegen Aussage 3 von Lemma 6.19 folgt die Behauptung des Satzes. □

Um den Beweisgang des folgenden Satzes nicht zu unterbrechen, erinnere ich vorweg daran, daß jede endliche Körpererweiterung eines endlichen Körpers $\mathbb{F}_q$ bereits eine Galoiserweiterung ist, und zwar mit zyklischer Galoisgruppe. Insbesondere hat der Zerfällungskörper eines irreduziblen Polynoms $f \in \mathbb{F}_p[X]$ vom Grad n ebenfalls den Grad n.

Satz 6.21 — *Für jedes $n \in \mathbb{N}$ existiert ein irreduzibles normiertes Polynom $f \in \mathbb{Z}[X]$, dessen Zerfällungskörper $L/\mathbb{Q}$ eine zu S_n isomorphe Galoisgruppe hat.*

Beweis. Für $n = 2$ oder $n = 3$ leisten $f = X^2 - 2$ bzw. $X^3 - 2$ alles Gewünschte. Es sei also im folgenden $n \geq 4$.

1. Wähle ein irreduzibles Polynom $f_2 \in \mathbb{F}_2[X]$ vom Grad n. Der Zerfällungskörper von f ist $\mathbb{F}_{2^n}$. Die Galoisgruppe $G_2 = \mathrm{Gal}(\mathbb{F}_{2^n}/\mathbb{F}_2)$ ist zyklisch von der Ordnung n und wird als Untergruppe in S_n von einem n-Zykel erzeugt.

2. Wähle ein irreduzibles Polynom $f_3' \in \mathbb{F}_3[X]$ vom Grad $n-1$. Setze $f_3 = X \cdot f_3'$. Der Zerfällungskörper von f_3 ist $\mathbb{F}_{3^{n-1}}$. Die Galoisgruppe $G_3 = \mathrm{Gal}(\mathbb{F}_{3^{n-1}}/\mathbb{F}_3)$ ist zyklisch von der Ordnung $n-1$ und wird als Untergruppe von S_n von einem n–Zykel erzeugt.

3. Das Polynom $f_5' = X^2 + 2 \in \mathbb{F}_5$ ist irreduzibel. Wähle weiter ein irreduzibles Polynom f_5'' vom Grad $n-2$ bzw. $n-3$ je nachdem, ob n ungerade oder gerade ist, und setze $f_5 = f_5' f_f''$ bzw. $f_5 = f_5' f_5'' X$. Es sei L der Zerfällungskörper von f, und es seien α_1, α_2 die Nullstellen von f_5' und $\alpha_3, \ldots, \alpha_n$ die übrigen Nullstellen von f. Es sei $g \in G_5 = \mathrm{Gal}(L/\mathbb{F}_5)$ ein Element mit $g(\alpha_1) = \alpha_2$. Die Einschränkung von g auf $K(\alpha_3, \ldots, \alpha_n)$ hat ungerade Ordnung m. Dann wirkt g^m auf $\alpha_3, \ldots, \alpha_n$ trivial und auf α_1, α_2 als Transposition. Das zeigt: Als Untergruppe in S_n enthält G_5 eine Transposition.

4. Mit Hilfe des Chinesischen Restklassensatzes findet man ein normiertes Polynom $f \in \mathbb{Z}[X]$ vom Grad n, das die simultanen Kongruenzen

$$f \equiv f_2 \bmod 2, \quad f \equiv f_3 \bmod 3, \quad f \equiv f_5 \bmod 5$$

erfüllt. Da f_2 irreduzibel ist, muß auch f irreduzibel sein. Die Galoisgruppe G von f enthält als Untergruppe von S_n gemäß Satz 6.20 Gruppen, die zu G_2, G_3 und G_5 isomorph sind. Insbesondere enthält G einen n–Zykel, einen $n-1$–Zykel und eine Transposition. Wir schließen mit dem folgenden Lemma, daß $G = S_n$. □

Lemma 6.22 — *Es sei $G \subset S_n$ eine Untergruppe, die einen n–Zykel, einen $n-1$–Zykel und eine Transposition enthält. Dann ist $G = S_n$.*

Beweis. Ohne Einschränkung sei $\pi = (12\ldots(n-1))$ ein $n-1$–Zykel in G, ferner (ij) eine Transposition in G. Da G einen n–Zykel enthält, operiert G transitiv auf den Elementen $\{1,\ldots,n\}$. Wähle $g \in G$ mit $g(j) = n$. Es sei $k = g(i)$. Dann gilt $G \ni g(ij)g^{-1} = (kn)$. Es folgt weiter $G \ni \pi^{\ell-k}(kn)\pi^{k-\ell} = (\ell n)$ für alle $\ell < n$. Schließlich enthält G auch das Element $(h\ell) = (hn)(\ell n)(hn)^{-1}$ für alle $h < \ell < n$. Damit enthält G alle Transpositionen. Da S_n von den Transpositionen erzeugt wird, ist $G = S_n$. □

Das Beispiel wurde aus Zeitgründen ausgelassen

Beispiel 6.23 — Wir illustrieren das Verfahren für $n = 5$: Das Polynom $X^{2^5-1} - 1 = X^{31} - 1 \in \mathbb{F}_2[X]$ zerfällt wie folgt in Linearfaktoren:

$$\begin{aligned} X^{31}-1 &= (X-1)(X^5+X^2+1)(X^5+X^3+1) \\ &\quad \cdot(X^5+X^3+X^2+X+1)(X^5+X^4+X^2+X+1) \\ &\quad \cdot(X^5+X^4+X^3+X+1)(X^5+X^4+X^3+X^2+1). \end{aligned}$$

Wir wählen als irreduzibles Polynom

$$f_2 = X^5 + X^2 + 1 \in \mathbb{F}_2[X].$$

Von den 8 verschiedenen irreduziblen Faktoren vom Grad 4 des Polynoms

$$\begin{aligned} \Phi_{80} &= \Phi_{3^4-1} = X^{32} - X^{24} + X^{16} - X^8 - 1 \\ &= (X^4+X^3-1)(X^4+X-1)(X^4-X^3-1)(X^4-X-1) \\ &\quad \cdot(X^4+X^3+X^2-X-1)(X^4-X^3+X^2+X-1) \\ &\quad \cdot(X^4+X^3-X^2-X-1)(X^4-X^3-X^2+X-1) \end{aligned}$$

wählen wir $X^4 - X - 1$ und setzen

$$f_3 = X^5 - X^2 - X \in \mathbb{F}_3[X].$$

Schließlich sei (mit einer kleinen Abweichung vom Algorithmus des Beweises)

$$f_5 = (X^2+2)X(X-1)(X-2) = X^5 + 2X^4 + 4X^3 + 4X^2 + 4X \in \mathbb{F}_5[X].$$

Ein Polynom, das die simultane Kongruenz löst, ist

$$f = X^5 + 12X^4 - 6X^3 - X^2 + 14X + 15.$$

Nach dem Satz ist die Galoisgruppe von f isomorph zu S_5.

§7 Transzendenzfragen

7.1 Transzendente Zahlen

Ein Element $a \in L$ ist transzendent über dem Unterkörper $K \subset L$, wenn es kein nichtkonstantes Polynom $f \in K[X]$ mit $f(a) = 0$ gibt. Eine komplexe Zahl a ist transzendent, wenn sie transzendent über $\mathbb{Q}$ ist. Ein Abzählargument liefert:

Satz 7.1 (Cantor) — *Der algebraische Abschluß $\overline{\mathbb{Q}}$ von $\mathbb{Q}$ in $\mathbb{C}$ ist abzählbar. Insbesondere gibt es überabzählbar viele transzendente Zahlen in $\mathbb{C}$.*

Beweis. Es gibt für festes $n \in \mathbb{N}$ nur abzählbare viele Polynome in $\mathbb{Q}[X]$ vom Grad n. Jedes von diesen hat höchstes endlich viele Nullstellen in $\mathbb{C}$. Der Körper $\overline{\mathbb{Q}} \subset \mathbb{C}$ aller über $\mathbb{Q}$ algebraischen Zahlen ist also die abzählbare Vereinigung von abzählbaren Mengen und damit selbst abzählbar. Da $\mathbb{C}$ überabzählbar ist, ist auch $\mathbb{C} \setminus \overline{\mathbb{Q}}$ überabzählbar. □

Der Beweis zeigt eigentlich allgemeiner:

Folgerung 7.2 — *Ist K endlich, so ist der algebraische Abschluß $\overline{K}$ abzählbar. Ist K unendlich, so sind K und $\overline{K}$ gleichmächtig.*

Streng genommen ist dieser Beweis von Cantor sogar konstruktiv: man kann die algebraischen Zahlen explizit abzählen, und das Diagonalverfahren liefert eine transzendente Dezimalzahl.

Der folgende ältere Beweis ist in anderer Weise konstruktiv: Er beruht auf der Beobachtung, daß sich nichtrationale algebraische Zahlen schlecht (!) durch rationale Zahlen approximieren lassen.

Satz 7.3 (Liouville) — *Es sei $a \in \mathbb{C}$ eine algebraische Zahl vom Grad $n \geq 2$ über $\mathbb{Q}$. Dann gibt es $\varepsilon > 0$ derart, daß für jede rationale Zahl p/q, $q \in \mathbb{N}$, gilt*

$$\left| a - \frac{p}{q} \right| \geq \frac{\varepsilon}{q^n}. \tag{7.1}$$

Beweis. Es sei $f \in \mathbb{Q}[X]$ das Minimalpolynom von a. Ferner sei P der Hauptnenner aller Koeffizienten von f, und schließlich sei $C = 1 + P \cdot \sum_{k=1}^{n} |f^{(k)}(a)/k!|$. Da f irreduzibel ist und keine mehrfache Nullstelle besitzt, ist $f'(\alpha) \neq 0$, also $C > 1$. Es sei $0 < \varepsilon < 1/C$.

Wir schließen dann wie folgt: Für jede rationale Zahl $p/q \in \mathbb{Q}$ ist einerseits $f(p/q)$ eine rationale Zahl, die nicht 0 sein kann. Da der Nenner von $f(p/q)$ höchstens Pq^n ist, gilt

$$|f(p/q)| \geq \frac{1}{Pq^n} \tag{7.2}$$

Andererseits folgt mit $\delta := a - p/q$ unter der Annahme $|\delta| < \varepsilon/q^n < 1$, daß

$$|f(p/q)| = |f(a-\delta)| = \left| f(a) + \sum_{k=1}^{n} (-1)^k \frac{f^{(k)}(a)}{k!} \delta^k \right| < \frac{\varepsilon}{q^n} \sum_{k=1}^{n} \frac{|f^{(k)}(a)|}{k!} < \frac{\varepsilon C}{Pq^n}. \tag{7.3}$$

Zusammengenommen hat man den Widerspruch

$$\frac{1}{Pq^n} \leq f(p/q) \leq \frac{\varepsilon C}{Pq^n} < \frac{1}{Pq^n}. \tag{7.4}$$

□

Mit diesem Satz findet man sofort viele transzendente Zahlen, zum Beispiel läßt sich die Zahl

$$\alpha := \sum_{n=0}^{\infty} \frac{1}{2^{n!}} \tag{7.5}$$

viel zu gut approximieren. Das ist natürlich ein künstliches Beispiel. Interessanter ist die Tatsache, daß e und π transzendente Zahlen sind. Wir führen den Beweis im folgenden Abschnitt.

7.2 Die Transzendenz von e und π

Satz 7.4 (Lindemann) — *Es seien $\alpha_1, \ldots, \alpha_n$ paarweise verschiedene algebraische Zahlen und $A_1, \ldots, A_n$ beliebige nichtverschwindende algebraische Zahlen. Dann ist $A_1 e^{\alpha_1} + \ldots + A_n e^{\alpha_n} \neq 0$.*

Unmittelbare Konsequenzen davon sind:

Folgerung 7.5 (Hermite) — *e ist transzendent.*

Beweis. Andernfalls gäbe es ganze Zahlen $A_0, \ldots, A_n$, die nicht alle verschwinden, mit $A_0 + A_1 e + \ldots + A_n e^n = 0$, im Widerspruch zum Satz von Lindemann. □

Folgerung 7.6 (Lindemann) — *π ist transzendent.*

Beweis. Wäre π algebraisch, so wäre auch πi algebraisch, und die Eulersche Identität $1 + e^{i\pi} = 0$ stünde im Widerspruch zu Satz 7.4. □

Hermite hat die Transzendenz von e im Jahre 1873 bewiesen, also lange vor Lindemann. Vielmehr baute Lindemann auf den Ideen von Hermite auf und bewies 1882 seinen Satz über die Exponentialfunktion. Der Beweis, den ich im Folgenden gebe, stammt von Hilbert (1893, vgl. Ges. Werke Bd. 1, Seite 1). Hilbert beweist direkt die beiden Folgerungen und überläßt dem Leser die Ausarbeitung des allgemeinen Falls zur Übung. Der folgende Beweis ist die Bearbeitung der Übungsaufgabe.

Wir nehmen also an, es seien paarweise verschiedene $\alpha_i \in \overline{\mathbb{Q}}$, $1 \leq i \leq n$, und beliebige $A_i \in \overline{\mathbb{Q}} \setminus \{0\}$ mit der Eigenschaft

$$A_1 e^{\alpha_1} + \ldots + A_n e^{\alpha_n} = 0. \tag{7.6}$$

gegeben. Notwendigerweise ist $n \geq 2$.

Der Beweis besteht aus zwei Teilen: Im ersten Teil reduzieren wir den allgemeinen Fall auf die Betrachtung des folgenden Spezialfalls

$$A_0 e^0 + A_1(e^{\alpha_{11}} + \ldots + e^{\alpha_{1\ell_1}}) + \ldots + A_m(e^{\alpha_{m1}} + \ldots + e^{\alpha_{m\ell_m}}) = 0, \tag{7.7}$$

wobei A_i ganze Zahlen $\neq 0$ und für jedes $j = 1, \ldots, m$ die Exponenten $\alpha_{j1}, \ldots, \alpha_{j\ell_j}$ die Nullstellen eines irreduziblen Polynoms $g_j \in \mathbb{Q}[X]$ vom Grad ℓ_j sind. Diese Reduktion geschieht in vier Schritten:

1. Schritt: Wir können ohne Einschränkung annehmen, daß in (7.6) alle Koeffizienten A_i ganze Zahlen sind.

Andernfalls sei G die Galoisgruppe der normalen Hülle von $\mathbb{Q}(A_1, \ldots, A_n) \subset \mathbb{C}$ über $\mathbb{Q}$. Die Exponenten β auf der rechten Seite der Identität

$$0 = \prod_{\sigma \in G} (\sigma(A_1)e^{\alpha_1} + \ldots + \sigma(A_n)e^{\alpha_n}) = \sum_j B_j e^{\beta_j} \tag{7.8}$$

haben die Form $\beta_j = \sum_i m_i \alpha_i$ mit ganzzahligen Koeffizienten m_i mit $\sum_i m_i = |G|$ und sind daher algebraische Zahlen. Die Koeffizienten B_j sind invariant unter der Galoisgruppe G und deshalb rationale Zahlen. Nach Multiplikation mit dem Hauptnenner werden sie ganzzahlig.

Allerdings werden nach dem Ausmultiplizieren Terme zusammengefaßt und könnten sich gegebenseitig auslöschen. Wir müssen also noch verifizieren, daß wenigstens ein Term e^{β_j} mit einem Koeffizienten $\neq 0$ übrig bleibt. Das ist sicher dann der Fall, wenn β_j nur auf eine Weise als Summe von Exponenten α_i geschrieben werden kann. Denn dann ist der Koeffizient B_j ein Produkt der zugehörigen Koeffizienten A_i und somit $\neq 0$. Dazu genügt das Lemma:

Lemma 7.7 — *Es seien $S_1, \ldots, S_\ell \subset \mathbb{C}$ nichtleere endliche Mengen. Dann gibt es in der Menge $S_1 + \ldots + S_n$ eine Zahl β, die sich nur auf eine Weise als Summe $\beta = s_1 + \ldots + s_n$ mit $s_i \in S_i$ schreiben läßt. Falls $|S_j| \geq 2$ für wenigstens einen Index, so gibt es wenigstens zwei verschiedene β mit der verlangten Eigenschaft.*

Beweis. Es sei $T = S_1 \cup \ldots \cup S_n$. Wir wählen $x \in \mathbb{C}$ so, daß x auf keinem Vektor $y - y' \neq 0$, $y, y' \in T$, senkrecht steht. Dann gibt es in jeder Menge S_i genau ein s_i derart, daß $\langle s_i, x\rangle = \max\{\langle s, x\rangle \mid s \in S_i\}$, und $\beta_+ := s_1 + \ldots + s_n$ hat die verlangte Eigenschaft. Dasselbe Argument mit $\min$ statt $\max$ liefert ein Element β_-, das von β_+ verschieden ist, sobald eine Menge S_j wenigstens zwei Elemente hat. □

2. Schritt: Es bestehe also die Identität (7.6) mit ganzen Zahlen A_j. Es sei S die Menge der Exponenten. Dann kann man ohne Einschränkung annehmen, daß S mit

α_j auch alle Konjugierten von α_j enthält, und zwar jeweils mit demselben ganzen Koeffizienten:

Diesmal bezeichne G die Galoisgruppe der normalen Hülle von $\mathbb{Q}(\alpha_1, \ldots, \alpha_n) \subset \mathbb{C}$ über $\mathbb{Q}$. Wir entwickeln wieder das folgende Produkt nach formalen Potenzen von e:

$$0 = \prod_{\sigma \in G} \left(A_1 e^{\sigma(\alpha_1)} + \cdots + A_n e^{\sigma(\alpha_n)} \right) = \sum_j B_j e^{\beta_j}. \tag{7.9}$$

Zunächst sieht man mit Hilfe des Lemmas, diesmal angewandt auf die Mengen $\sigma(S)$, $\sigma \in G$, daß die Summe auf der rechten Seite wenigstens zwei nichttriviale Summanden hat. Außerdem sind die Exponenten algebraische Zahlen, die Menge der Exponenten ist abgeschlossen unter Konjugation, und konjugierte Exponenten haben denselben Koeffizienten. Faßt man die Terme mit konjugierten Exponenten zusammen, so erhält man eine Identität:

$$0 = B_1(e^{\beta_{11}} + \ldots + e^{\beta_{1\ell_1}}) + \ldots + B_m(e^{\beta_{m1}} + \ldots + e^{\beta_{m\ell_m}}) \tag{7.10}$$

mit ganzen Zahlen $B_j \in \mathbb{Z} \setminus \{0\}$ und paarweise verschiedenen algebraischen Zahlen β_{ji} derart, daß für jedes j die Zahlen $\beta_{j1}, \ldots, \beta_{j\ell_j}$ die Nullstellen eines irreduziblen Polynoms $g_j \in \mathbb{Q}[X]$ sind.

3. Schritt: Man kann ohnen Einschränkung annehmen, daß eine Identität der Form (7.7) besteht.

Dazu gehen wir von einer Identität der Form (7.10) aus und multiplizieren mit $(e^{-\beta_{11}} + \ldots + e^{-\beta_{1\ell_1}})$. Man erhält nach erneutem Umsortieren eine Identität der Form (7.10) mit neuen Exponenten und neuen Koeffizienten, wobei diesmal aber insbesondere der Term $\ell_1 B_1 e^0$ vorkommt.

Das beendet den ersten Teil. Bevor wir zum zweiten Teil übergehen, will ich die Reduktionsschritte kurz an einem Beispiel illustrieren. Starten wir mit einem Ausdruck

$$\sqrt{2}e^3 + \sqrt{5}e^{\sqrt{7}},$$

so erhält man im ersten Schritt

$$\begin{aligned}(\sqrt{2}e^3 + \sqrt{5}e^{\sqrt{7}})(-\sqrt{2}e^3 + \sqrt{5}e^{\sqrt{7}})(\sqrt{2}e^3 - \sqrt{5}e^{\sqrt{7}})(-\sqrt{2}e^3 - \sqrt{5}e^{\sqrt{7}}) \\ = \quad 4e^{12} - 20e^{6+2\sqrt{7}} + 25e^{4\sqrt{7}}.\end{aligned}$$

Im zweiten Schritt wird hieraus:

$$\begin{aligned}&(4e^{12} - 20e^{6+2\sqrt{7}} + 25e^{4\sqrt{7}})(4e^{12} - 20e^{6-2\sqrt{7}} + 25e^{-4\sqrt{7}}) \\ &\quad = \quad -500\big(e^{6+2\sqrt{7}} + e^{6-2\sqrt{7}}\big) + 100\big(e^{12+4\sqrt{7}} + e^{12-4\sqrt{7}}\big) \\ &\qquad\quad -80\big(e^{18+2\sqrt{7}} + e^{18-2\sqrt{7}}\big) + 400e^{12} + 16e^{24} + 625e^0.\end{aligned}$$

Der dritte Schritt ist hier unnötig, weil e^0 mit Koeffizient 625 vorkommt.

Damit kommen wir zum zweiten, eigentlichen Teil des Beweises. Wir können vom folgenden Datum ausgehen: Es besteht eine Identität

$$0 = A_0 e^0 + A_1(e^{\alpha_{11}} + \ldots + e^{\alpha_{1\ell_1}}) + \ldots + A_m(e^{\alpha_{m1}} + \ldots + e^{\alpha_{m\ell_m}}) \tag{7.11}$$

mit ganzen Zahlen $A_j \in \mathbb{Z}\setminus\{0\}$ und paarweise und von 0 verschiedenen algebraischen Exponenten α_{jk}. Dabei sind für jedes j die Exponenten $\alpha_{j1}, \ldots, \alpha_{j\ell_j}$ die Nullstellen eines irreduziblen normierten Polynoms $g_j(X) \in \mathbb{Q}[X]$ vom Grad ℓ_j. Es gibt dann ein $c \in \mathbb{N}$ mit der Eigenschaft, daß $cg_j(X) \in \mathbb{Z}[X]$ für jedes j. Wir definieren

$$g := \prod_j g_j, \qquad \ell := \sum_j \ell_j. \tag{7.12}$$

Wir wählen nun eine natürliche Zahl $n \in \mathbb{N}$, die im Laufe des Beweises genauer spezifiziert wird, und multiplizieren die Identität (7.7) mit dem Integral

$$c^L \int_0^\infty z^n g(z)^{n+1} e^{-z} dz, \tag{7.13}$$

wo L eine hinreichend große natürliche Zahl ist, über die wir später verfügen. Wir erhalten die Identität

$$0 = A_0 I_0 + \sum_{j=1}^m A_j I_j + I_\varepsilon, \tag{7.14}$$

wobei die einzelnen Terme für die folgenden Integrale stehen:

$$I_0 = c^L \int_0^\infty z^n g(z)^{n+1} e^{-z} dz, \tag{7.15}$$

$$\begin{aligned} I_j &= c^L \sum_{k=1}^{\ell_j} \int_{\alpha_{jk}}^\infty z^n g(z)^{n+1} e^{\alpha_{jk}-z} dz \\ &= c^L \sum_{k=1}^{\ell_j} \int_0^\infty (t+\alpha_{jk})^n g(t+\alpha_{jk})^{n+1} e^{-t} dt. \end{aligned} \tag{7.16}$$

$$I_\varepsilon = c^L \sum_{j=1}^m A_j \sum_{k=1}^{\ell_j} e^{\alpha_{jk}} \int_0^{\alpha_{jk}} z^n h(z)^{n+1} e^{-z} dz \tag{7.17}$$

Wir berechnen nun die einzelnen Integrale oder geben wenigstens eine Abschätzung.

i) Zunächst überzeugt man sich leicht von der Richtigkeit der Gleichung

$$\int_0^\infty z^N e^{-z} dz = N!, \qquad N \in \mathbb{N}_0. \tag{7.18}$$

Der Term kleinsten Grades des z-Polynoms $c^L z^n g(z)^{n+1}$ ist $z^n h(0)^{n+1}$. Sein Beitrag zum Integral I_0 ist $n! c^L g(0)^{n+1}$. Wenn $L \geq \ell(n+1)$, steuern alle anderen Terme zum Integral I_0 ganzzahlige Beiträge bei, die durch $(n+1)!$ teilbar sind. Insbesondere ist in diesem Falle $I_0/n!$ ist ganzzahlig, und

$$I_0/n! \equiv c^L g(0)^{n+1} \mod n+1. \tag{7.19}$$

ii) Für festes j und $k = 1, \ldots, \ell_j$ ist α_{jk} eine Nullstelle von g. Deshalb hat

$$C^{\ell(n+1)} (t+\alpha_{jk})^n g(t+\alpha_{jk})^{n+1}$$

bei $t = 0$ eine Nullstelle der Ordnung $\geq (n+1)$ und die Koeffizienten bezüglich t sind ganzzahlige Polynom in α_{jk} vom Grad $\leq n + (n+1)\deg(g) < \ell(n+1)$. Wenn $L \geq 2\ell(n+1)$, folgt

$$c^L(t+\alpha_{jk})^n g(t+\alpha_{jk})^{n+1} \in t^{n+1}\mathbb{Z}[c\alpha_{jk}][t]. \tag{7.20}$$

Mittelung über alle Nullstellen liefert deshalb

$$c^L \sum_{k=1}^{\ell_j} (t+\alpha_{jk})^n g(t+\alpha_{jk})^{n+1} \in t^{n+1}\mathbb{Z}[t]. \tag{7.21}$$

Jetzt liefert die Integration einen Wert $I_j \in (n+1)!\,\mathbb{Z}$. Insbesondere gilt

$$I_j/n! \equiv 0 \mod (n+1), \tag{7.22}$$

sobald $L \geq 2\ell(n+1)$.

iii) Das verbliebene Integral schätzen wir ab: Die Vereinigung K der Strecken $[0, \alpha_{jk}]$ ist eine kompakte Teilmenge in $\mathbb{C}$. Deshalb sind die Funktionen $zg(z)$ und $g(z)e^{-z}$ auf K beschränkt, etwa durch $\gamma > 0$. Dann gilt:

$$|I_\epsilon| \leq c^{2\ell(n+1)}\gamma^{n+1} \sum_j |A_j| \sum_k |\alpha_{jk}e^{\alpha_{jk}}| =: (c^{2\ell}\gamma)^{n+1}c'. \tag{7.23}$$

Damit ist mit der Wahl $L = 2\ell(n+1)$ einerseits die linke Seite der Identität

$$(A_0 I_0 + \sum_j A_j I_j)/n! = -I_\epsilon/n! \tag{7.24}$$

eine ganze Zahl mit Rest $A_0(c^{2\ell}g(0))^{n+1} \mod n+1$ ist, während andererseits die rechte Seite dem Betrage nach durch $c'(\gamma c^{2\ell})^{n+1}/n!$ beschränkt ist. Wir wählen nun n so groß, daß $c'c^{n+1}/n! < 1$, und zugleich als Vielfaches von $A_0 c^{2\ell} g(0)$. Da n und $n+1$ teilerfremd sind, ist die linke Seite von (7.24) eine von 0 verschiedene ganze Zahl, während die rechte Seite dem Betrage nach kleiner 1 ist. Mit diesem Widerspruch ist Satz 7.4 bewiesen.

7.3 Transzendenzbasen

Definition 7.8 — Es sei L/K eine Körpererweiterung.

1. Eine Teilmenge $S \subset L$ heißt algebraisch unabhängig über K, wenn der kanonische Ringhomomorphismus $\Phi : K[\{X_s\}_{s\in S}] \to L$, $X_s \mapsto s$, injektiv ist. In diesem Falle setzt sich Φ zu einer kanonischen Einbettung $\tilde{\Phi} : K(\{X_s\}_{s\in S}) \to L$ des Funktionenkörpers fort, dessen Bild $K(S)$ ist.

2. Eine algebraisch unabhängige Teilmenge $S \subset L$ ist eine Transzendenzbasis der Erweiterung L/K, wenn L algebraisch über $K(S)$ ist.

3. Die Erweiterung L/K heißt rein transzendent, wenn es ein algebraisch unabhängiges Erzeugendensystem S von L gibt.

Satz 7.9 (Steinitz) — *1. Jede Körpererweiterung L/K hat eine Transzendenzbasis. 2. Alle Transzendenzbasen einer Körpererweiterung haben dieselbe Mächtigkeit.*

Beweis. 1. Wir nehmen zunächst allgemeiner an, S sei eine endliche, algebraisch unabhängige Teilmenge und L sei algebraisch über $K(T)$, und zeigen unter diesen Voraussetzungen, daß $|S| \leq |T|$. Offenbar können wir ohne Einschränkung annehmen, daß S nicht leer ist.

Angenommen, $S_0 = S \cap T$ und $s \in S \setminus S_0$. Nach Voraussetzung ist s algebraisch über $K(T)$, ist also Nullstelle eines nichtkonstanten Polynoms $f \in K(T)[X]$. Nach Multiplikation mit dem Hauptnenner kann man ohne Einschränkung annehmen, daß $f \in K[T][X]$. Es gibt also endlich viele Koeffizienten f_{nm}, so daß

$$0 = \sum_{n,m} f_{n,m} t_1 n_1 \cdots t_\ell^{n_\ell} s^m \tag{7.25}$$

mit $t_1, \ldots, t_\ell \in T$. Wir können annehmen, daß f so gewählt ist, daß ℓ minimal ist. Lägen alle t_i in S_0, wäre $S_0 \cup \{s\}$ nicht algebraisch unabhängig, im Widerspruch zur Annahme über S. Ohne Einschränkung ist t_ℓ kein Element von S_0. Bezeichnet d den Grad von f bezüglich t_ℓ, so ist der Koeffizient von t_ℓ^d nicht 0, sonst würde er der Minimalität von f widersprechen. Das zeigt, daß t_ℓ algebraisch über $K(T')$ ist, wobei $T' := S_0 \cup \{s\} \cup T \setminus \{t_\ell\}$ ist. Jedes Element in L, das algebraisch über $K(T)$ ist, ist daher auch algebraisch über $K(T')$.

Die neue Menge T' hat dieselbe Mächtigkeit wie T, und $S_0' = T' \cap S = S_0 \cup \{s\}$. In endlich vielen Schritten kann man also T durch eine Menge $\tilde{T}$ gleicher Mächtigkeit ersetzen, die S enthält. Insbesondere ist dann $|T| \geq |S|$.

2. Es seien nun S und T zwei Transzendenzbasen. Jedes $s \in S$ ist algebraisch über $K(T)$. Es gibt dann aber auch schon eine endliche Teilmenge $T_s \subset T$ derart, daß s algebraisch über $K(T_s)$ ist. Insbesondere ist S algebraisch über $K(T_S)$ mit $T_S := \bigcup T_s$. Andererseits ist T algebraisch über $K(S)$, also auch über $K(T_S)$. Da T nach Voraussetzung algebraisch unabhängig ist, folgt $T = T_S$.

Daraus schließen wir: Ist S endlich, so ist $T = T_S$ als Vereinigung von endlich vielen endlichen Mengen ebenfalls endlich. Mit Schritt 1 folgt nun $|S| \leq |T|$ und $|T| \leq |S|$, also Gleichheit. Ist umgekehrt S unendlich, so hat $T = T_S$ als Vereinigung einer von S parametrisierten Familie endlicher Mengen höchstens die Mächtigkeit $|S|$. Aus der Symmetrie des Arguments folgt auch jetzt $|S| = |T|$.

3. Das beweist die Gleichmächtigkeit beliebiger Transzendenzbasen. Es bliebt zu zeigen, daß es Transzendenzbasen gibt.

Dazu betrachten wir die Menge $X \subset L$ aller algebraisch unabhängigen Teilmengen und die durch Inklusion definierte Halbordnung auf X. Die Menge X ist nicht leer,

denn X enthält die leere Menge. Es sei weiter K eine Kette in X und $T := \bigcup_{S\in K} S$. Wäre T nicht algebraisch unabhängig, so gäbe es eine endliche Teilmenge $T' \subset T$, die Nullstelle eines nichtkonstanten Polynoms wäre. Jedes Element $t'_i \in T$ stammt aus einer Menge $S_i \in K$. Da K eine Kette ist, gibt es eine Menge $S \in K$ mit $S_i \subset S$ für alle i, insbesondere also auch $T' \subset S$. Aber da S algebraisch unabhängig ist, muß dies auch für T' gelten. Damit liegt T in K und ist eine obere Schranke von K. Nach dem Zornschen Lemma gibt es ein maximales Element T in X. Es genügt zu zeigen, daß L algebraisch über $K(T)$ ist. Andernfalls gibt es ein Element $a \in L$, das transzendent über $K(T)$ ist. Aber dann ist $T \cup \{a\}$ algebraisch unabhängig, im Widerspruch zur Maximalität von T. □

Definition 7.10 — Es sei $K \to L$ eine Körpererweiterung mit Transzendenzbasis S. Die Zahl $\mathrm{trdeg}(L/K) := |S|$ heißt Transzendenzgrad von L über K.

Offenbar ist $K \to L$ genau dann algebraisch, wenn $\mathrm{trdeg}(L/K) = 0$.

Satz 7.11 — *Es seien $K \to M \to L$ Körpererweiterungen. Dann gilt*

$$\mathrm{trdeg}(L/K) = \mathrm{trdeg}(L/M) + \mathrm{trdeg}(M/K). \tag{7.26}$$

Beweis. Übung. □

Aus der Eindeutigkeit der Mächtigkeit einer Transzendenzbasis für L/K folgt nicht, daß die rein transzendenten Zwischenkörper, die von zwei Transzendenzbasen erzeugt werden, gleich sind. Ein einfaches Beispiel bietet der Funktionenkörper $K(X)/K$. Sowohl $\{X\}$ also auch $\{X^2\}$ sind Transzendenbasen. Aber $K(X^2) \subset K(X)$ ist ein echter Unterkörper.

Satz 7.12 — $\mathrm{Aut}(\mathbb{C})$ *ist eine überabzählbare Gruppe.*

Beweis. Es sei $S \subset \mathbb{C}$ eine Transzendenzbasis. Da $\mathbb{C}$ der algebraische Abschluß von $\mathbb{Q}(S)$ und überabzählbar ist, muß auch S überabzählbar sein. Es sei $\pi : S \to S$ eine beliebige Bijektion und $\varphi : \mathbb{Q}(S) \to \mathbb{Q}(S)$ der zugehörige Körperisomorphismus mit $\varphi|_S = \pi$. Dann existiert ein Isomorphismus $\psi : \mathbb{C} \to \mathbb{C}$ mit $\psi|_{\mathbb{Q}(S)} = \varphi$. □

Aufgaben zu transzendenten Erweiterungen

Aufgabe 7.1 — Zeigen Sie, daß $\sum_{n=0}^{\infty} \frac{1}{2^{n!}}$ eine transzendente Zahl ist.

Aufgabe 7.2 — Beweisen Sie den folgenden Satz: *Es seien $L/M/K$ Körpererweiterungen. Dann gilt:* $\mathrm{trdeg}(L/K) = \mathrm{trdeg}(L/M) + \mathrm{trdeg}(M/K)$.

A Ringtheorie

Der Inhalt dieses Anhangs ist Gegenstand der früheren Vorlesungen 'Elementare Algebra und Zahlentheorie', 'Lineare Algebra' und 'Computeralgebra'. Zum bequemeren Verweis habe ich die wichtigsten Begriffe, Methoden und Ergebnisse noch einmal zusammengestellt.

A.1 Grundbegriffe

Definition A.1 — Ein *Ring* ist eine Menge A mit zwei Verknüpfungen $+$ und $\cdot$ mit den folgenden Eigenschaften:

1. $(A, +)$ ist eine kommutative Gruppe. Das Neutralelement der Addition wird mit 0 bezeichnet, das additive Inverse zu a mit $-a$.
2. Die Multiplikation $\cdot$ ist assoziativ, und es gibt ein Neutralelement 1 der Multiplikation.
3. Es gilt das Distributivgesetz: $(a+b)c = ac+bc$ und $a(b+c) = ab+ac$ für alle $a, b, c \in A$.

Ein Ring A heißt *kommutativ*, wenn $\cdot$ kommutativ ist. Ein kommutativer Ring ist ein *Körper*, wenn $0 \neq 1$ und wenn jedes Element $a \in K \setminus \{0\}$ ein multiplikatives Inverses besitzt. Eine Abbildung $f : A \to B$ zwischen Ringen ist ein Ringhomomorphismus, wenn $f(a+b) = f(a)+f(b)$, $f(ab) = f(a)f(b)$ für alle $a, b \in A$ und wenn $f(1) = 1$.

Der Nullring 0 ist die Menge $\{0\}$ mit den trivialen Verknüpfungen $0+0 = 0\cdot 0 = 0$. Im Nullring ist 0 zugleich Null- und Einselement. In jedem Ring $A \ncong 0$ sind Null- und Einselement verschieden.

Definition A.2 — Es sei A ein kommutativer Ring.

1. Ein Element $a \in A$ ist invertierbar oder eine *Einheit*, wenn es ein $b \in A$ mit $ab = 1$ gibt. Die Einheiten in A bilden eine Gruppe mit der Ringmultiplikation als Verknüpfung, die *Einheitengruppe* von A, und wird mit $A^\times$ bezeichnet.
2. $a \in A$ ist ein *Nullteiler*, wenn es ein $b \in A \setminus \{0\}$ mit $ab = 0$ gibt. Ein kommutativer Ring ist nullteilerfrei oder ein *Integritätsbereich*, wenn $A \neq 0$ und wenn 0 der einzige Nullteiler in A ist. In einem Integritätsbereich gilt für $a, b, c \in A$ die Kürzungsregel: $\quad ac = bc \quad \Rightarrow \quad a = b$.
3. $a \in A$ ist *nilpotent*, falls $a^n = 0$ für ein $n \in \mathbb{N}$.

Definition A.3 — Es sei A ein kommutativer Ring und $S \subset A$ eine Teilmenge.

1. $a \in A$ ist ein Teiler von $b \in A$, wenn es ein $c \in A$ mit $b = ac$ gibt. In Zeichen: $a|b$. Falls a kein Teiler von b ist, schreibt man $a \nmid b$.

2. $d \in A$ ist ein gemeinsamer Teiler von S, wenn $d|a$ für alle $a \in S$, und d ist ein größter gemeinsamer Teiler von S, wenn d ein gemeinsamer Teiler ist und wenn für jeden anderen gemeinsamen Teiler x von S gilt $x|d$.

3. $a, b \in A$ sind assoziiert, in Zeichen: $a \sim b$, wenn $a = ub$ für eine Einheit u.

4. $v \in A$ ist ein gemeinsames Vielfaches von S, wenn $a|v$ für alle $a \in S$, und v ist ein kleinstes gemeinsames Vielfaches von S, wenn v ein gemeinsames Vielfaches ist und wenn für jedes andere gemeinsame Vielfache y gilt $v|y$.

Lemma A.4 — *Es sei A ein Integritätsbereich.*

1. *Für $a, b \in A$ gilt $a \sim b$ genau dann, wenn $a|b$ und $b|a$.*

2. *Falls ein größter gemeinsamer Teiler für $S \subset A$ existiert, ist er eindeutig bis auf Einheiten.*

3. *Falls ein kleinstes gemeinsames Vielfaches für $S \subset A$ existiert, ist es eindeutig bis auf Einheiten.*

A.2 Polynomringe

Es sei A ein kommutativer Ring und $f = \sum_{k=0}^{n} f_k X^k \in A[X]$ ein Polynom. Der Grad von f ist

$$\deg(f) = \begin{cases} -\infty, & \text{falls } f = 0 \\ \max\{k \mid f_k \neq 0\} & \text{sonst.} \end{cases}$$

Ist $f \in A[X]$ ein Polynom vom Grad $d = \deg(f) \geq 0$, dann ist $Lt(f) := f_d X^d$ der Leitterm von f, $Lc(f) := f_d$ der Leitkoeffizient und $Lm(f) := X^d$ das Leitmonom. Bei Polynomringen in mehreren Variablen, etwa $A[X_1, \ldots, X_\ell]$, verwenden wir häufig Multiindexbezeichnungen: Für $n = (n_1, \ldots, n_\ell) \in \mathbb{N}_0^\ell$ ist

$$X^n := X_1^{n_1} \cdot \ldots \cdot X_\ell^{n_\ell}.$$

Jedes $f \in A[X_1, \ldots, X_\ell]$ schreibt sich dann in der Form

$$f = \sum_{n \in \mathbb{N}_0^\ell} f_n X^n,$$

wobei für fast alle $n \in \mathbb{N}_0^\ell$ der Koeffizient f_n verschwindet.

Auf analoge Weise können wir den Polynomring mit beliebig vielen Unbestimmten einführen: Es bezeichne S eine beliebige Indexmenge, im endlichen Falle etwa die Menge $\{1, \ldots, \ell\}$. Dann sei $\mathbb{N}_0^S$ die Menge aller Folgen $(n_s)_{s \in S}$ mit $n_s \in \mathbb{N}_0$ und $n_s = 0$ für fast alle $s \in S$. Durch die Verknüpfung

$$(n + n')_s := n_s + n'_s$$

wird $\mathbb{N}_0^S$ zu einem abelschen Monoid mit dem Nullelement $0 = (0)_{s\in S}$. Bezeichnet $e_s \in \mathbb{N}_0^S$, $s \in S$, die Folge $(e_s)_{s'} = \delta_{s,s'}$, so kann man jedes Element $n \in \mathbb{N}_0^S$ in der Form $n = \sum_{s\in S} n_s e_s$ schreiben; in der formal unendlichen Summe sind nur endlich viele Elemente ungleich Null. Wir definieren auf

$$B := \{f : \mathbb{N}_0^S \to A \mid f_n = 0 \text{ für fast alle } n \in \mathbb{N}_0^S\}$$

wie folgt zwei Verknüpfungen:

$$(f+g)_n := f_n + g_n, \qquad (f\cdot g)_n = \sum_{n'+n''=n} f_{n'} \cdot g_{n''}.$$

Man rechnet sofort nach, daß $(B, +, \cdot)$ ein kommutativer Ring ist. Speziell können wir für jedes $s \in S$ die Abbildung $X_s : \mathbb{N}_0^S \to A$ mit der Eigenschaft $(X_s)_n = \delta_{e_s,n}$ betrachten, und für jedes $n \in \mathbb{N}_0^S$ das Monom $X^n := \prod_{s\in S} X_s^{n_s}$. Mit diesen Bezeichnungen gilt nun

$$f = \sum_{n\in\mathbb{N}_0^S} f_n X^n \quad \text{für jedes } f \in B.$$

Außerdem ist die Abbildung $A \to B$, $a \mapsto aX^0$, ein injektiver Ringhomomorphismus. Wir identifizieren A mit dem Bild in B und bezeichnen mit $A[\{X_s\}_{s\in S}] := B$ den Polynomring in den Unbestimmten X_s, $s \in S$.

Satz A.5 *(Universelle Eigenschaft des Polynomrings) — Es sei $\varphi : A \to R$ ein Ringhomomorphismus in einen kommutativern Ring R und $r = (r_s)_{s\in S}$ eine Folge von Elementen in R. Dann gibt es genau einen Ringhomomorphismus*

$$\Phi : A[\{X_s\}_{s\in S}] \longrightarrow R$$

mit $\Phi|_A = \varphi$ und $\Phi(X_s) = r_s$.

Beweis. Falls Φ existiert, muß Φ jedenfalls auf einem Polynom $f = \sum_n f_n X^n$ folgendermaßen aussehen:

$$\Phi(f) = \sum_n \varphi(f_n) \prod_s \Phi(X_s)^{n_s} = \sum_n \varphi(f_n) \prod_x r_s^{n_s}.$$

Definiert man umgekehrt eine Abbildung Φ auf diese Weise, so hat Φ alle gewünschten Eigenschaften. □

Der Ringhomomorphismus Φ heißt Auswertungsabbildung in b. Wir schreiben kurz $f(r) := \Phi(f)$. Die Aussage bleibt auch für nichtkommutative Ringe R mit Eins richtig, solange alle Elemente in $\varphi(A) \cup \{r_s \mid s \in S\}$ miteinander kommutieren.

A.3 Ideale und Restklassenringe

Definition A.6 — Es sei A ein kommutativer Ring.

1. Eine nichtleere Teilmenge $I \subset A$ ist ein *Ideal*, wenn für alle $x, x' \in I$ und alle $a \in A$ gilt: $x + x' \in I$ und $ax \in I$.

2. Für jedes $a \in A$ ist die Menge $(a) = \{ra \mid r \in A\}$ ein Ideal, das von a erzeugte *Hauptideal*. In jedem Ring gibt es das Nullideal $(0) = \{0\}$ und das Einsideal $(1) = A$. Schließlich ist A ein *Hauptidealring*, wenn jedes Ideal in A ein Hauptideal ist.

3. Für $S \subset A$ ist $(S) := \{a_1 s_1 + \ldots + a_n s_n \mid n \in \mathbb{N}_0,\ a_i \in A,\ s_i \in S\}$ das von S erzeugte Ideal. (S) ist auch der Durchschnitt aller Ideale in A, die S enthalten. Ist $S = \{s_1, \ldots, s_n\}$, schreibt man $(s_1, \ldots, s_n) := (S)$. Ein Ideal I ist *endlich erzeugt*, wenn es $s_1, \ldots, s_n \in A$ mit $I = (s_1, \ldots, s_n)$ gibt. Der Ring A ist noethersch, wenn jedes Ideal endlich erzeugt ist.

Beispiele A.7 — Es sei A ein kommutativer Ring.
1. Für jeden Ringhomomorphismus $\varphi : A \to A'$ ist der Kern $\ker(\varphi) = \varphi^{-1}(0)$ ein Ideal in A.
2. Es sei $\{I_s\}_{s \in S}$ eine Familie von Ideal in A. Dann sind $\bigcap_{s \in S} I_s$ und $\sum_{s \in S} I_s := \left(\cup_{s \in S} I_s \right)$ Ideale in A.
3. Sind I_1 und I_2 Ideale in A, so ist auch $I_1 I_2 := \left(\{x_1 x_2 \mid x_i \in I_i\} \right)$ ein Ideal in A.

Beweis. Übung □

Es sei nun A ein kommutativer Ring mit einem Ideal I. Wir schreiben:

$$a \equiv b \bmod I \quad :\Leftrightarrow \quad a + I = b + I \quad \Leftrightarrow \quad a - b \in I.$$

Für jedes $a \in A$ bezeichne $\overline{a} := a + I$ die Restklasse von a modulo I, und A/I bezeichne die Menge aller Restklassen. Die Abbildung $\pi : A \to A/I$, die jedes $a \in A$ auf seine Restklasse $\overline{a} = a + I$ schickt, heißt kanonische Projektion.

Lemma A.8 — *Es gibt genau eine Ringstruktur auf A/I, bezüglich der π ein Ringhomomorphismus wird, nämlich*

$$\overline{a} + \overline{b} := \overline{a + b}, \quad \overline{a} \cdot \overline{b} := \overline{ab}.$$

Beweis. Es ist klar, daß die Verknüpfungen nur so definiert werden können, weil π surjektiv ist. Man zeigt dann, daß die so definierten Verknüpfungen wohldefiniert sind. Für die Wohldefiniertheit der Addition wird nur benutzt, daß I eine additive Untergruppe ist. Für die Wohldefiniertheit der Multiplikation wird die Idealeigenschaft gebraucht: Es seien a, a' und b, b' Elemente aus A mit $a + I = a' + I$ und $b + I = b' + I$, also $a' = a + x$ und $b' = b + y$ mit $x, y \in I$. Dann hat man

$$a'b' = (a + x)(b + y) = ab + (ay + xb + xy) \in ab + I.$$

Daß die Ringaxiome in A/I erfüllt sind, folgt dann automatisch, weil π surjektiv ist und die Verknüpfungen erhält und weil A ein Ring ist. □

Definition A.9 — Es sei A ein kommutativer Ring und $I \subset A$ ein Ideal. Der Ring A/I heißt Restklassenring von A bezüglich I.

Satz A.10 *(Universelle Eigenschaft des Restklassenrings) — Es sei A ein kommutativer Ring, $I \subset A$ ein Ideal und $\pi : A \to A/I$ die kanonische Projektion. Zu einem Ringhomomorphismus $\varphi : A \to B$ gibt es genau dann einen Ringhomomorphismus $\overline{\varphi} : A/I \to B$ mit $\varphi = \overline{\varphi} \circ \pi$, wenn $I \subset \ker(\varphi)$. In diesem Falle ist $\overline{\varphi}$ eindeutig bestimmt.*

Beweis. Falls ein solches $\overline{\varphi}$ existiert, so ist es offensichtlich eindeutig bestimmt, weil π surjektiv ist. Außerdem gilt in diesem Falle für jedes $x \in I$, daß $\varphi(x) = \overline{\varphi}(\pi(x)) = \overline{\varphi}(0) = 0$, also $I \subset \ker(\varphi)$. Es gelte nun umgekehrt $I \subset \ker(\varphi)$. Wir definieren $\overline{\varphi}(\pi(a)) := \varphi(a)$. Es genügt zu zeigen, daß $\overline{\varphi}$ wohldefiniert ist. Für $a, b \in A$ mit $\pi(a) = \pi(b)$ folgt $a - b \in I \subset \ker(\varphi)$, also $\varphi(a) - \varphi(b) = \varphi(a - b) = 0$. □

Definition A.11 — Es sei A ein kommutativer Ring.

1. Ein Ideal $\mathfrak{p} \subset A$ ist ein *Primideal*, wenn $\mathfrak{p} \neq A$, und wenn für beliebige Ringelemente $a, b \in A$ aus $ab \in \mathfrak{p}$ folgt: $a \in \mathfrak{p}$ oder $b \in \mathfrak{p}$.

2. Die Menge $\mathrm{Spec}(A) := \{\mathfrak{p} \mid \mathfrak{p} \text{ ist ein Primideal}\}$ heißt das Primspektrum oder kurz das *Spektrum* von A.

3. Ein Ideal $\mathfrak{m} \subset A$ ist ein *maximales Ideal*, wenn $\mathfrak{m} \neq A$, und wenn für jedes Ideal I mit $\mathfrak{m} \subset I$ gilt $\mathfrak{m} = I$ oder $I = A$.

Lemma A.12 — *Es sei A ein kommutativer Ring und $\mathfrak{p} \subset A$ ein Ideal.*

1. *$\mathfrak{p}$ ist ein Primideal $\Leftrightarrow$ $A/\mathfrak{p}$ ist ein Integritätsbereich.*

2. *$\mathfrak{p}$ ist ein maximales Ideal $\Leftrightarrow$ $A/\mathfrak{p}$ ist ein Körper.*

Beweis. Übung □

Im Beweis des folgenden Satzes verwenden wir das Zornsche Lemma[13].

[13] Eine Relation $\leq$ auf einer Menge X ist eine Halbordnung (oder partielle Ordnung), wenn (1) für alle $a \in A$ gilt $a \leq a$, wenn (2) aus $a \leq b$ und $b \leq a$ folgt, daß $a = b$, und wenn (3) aus $a \leq b$ und $b \leq c$ folgt, daß $a \leq c$. Eine halbgeordnete Menge ist eine Menge mit einer Halbordnung. Eine Ordnung (oder Totalordnung) auf X ist eine Halbordnung mit der zusätzlichen Eigenschaft, daß für je zwei Elemente $a, b \in X$ einer der beiden Fällen $a \leq b$ oder $b \leq a$ eintritt. Ein typisches Beispiel einer halbgeordneten Menge ist die Potenzmenge $X = P(Y)$ einer Menge Y mit der Inklusionsrelation. Diese Menge ist nicht geordnet, sobald Y mehr als ein Element enthält. Es sei X eine halbgeordnete Menge: jede Teilmenge $K \subset X$ erbt eine Halbordnung. K ist eine Kette, wenn diese Halbordnung sogar eine Ordnung ist. $s \in X$ ist eine obere Schranke von $A \subset X$, wenn $a \leq s$ für alle $a \in A$. Schließlich ist $a \in A$ ein maximales Element von A, wenn aus $b \in A$ und $a \leq b$ folgt, daß $a = b$. Eine halbgeordnete Menge X ist induktiv geordnet, wenn jede Kette $K \subset X$ eine obere Schranke besitzt. Das Lemma von Zorn besagt: Jede nichtleere, induktiv geordnete Menge besitzt ein maximales Element.

Satz A.13 — *Zu jedem Ideal $I \subsetneq A$ gibt es ein maximales Ideal $\mathfrak{m} \subset A$ mit $I \subset \mathfrak{m}$.*

Beweis. Es sei X die Menge aller Ideale $J \subsetneq A$ mit $I \subset J$. Da X das Ideal I enthält, ist X nicht leer. Die Inklusionsordnung ist eine Halbordnung auf X. Jede Kette $K \subset X$ besitzt die obere Schranke $J_K := \bigcup_{J \in K} J$. Nach dem Zornschen Lemma gibt es ein maximales Element $\mathfrak{m} \in X$. Für jedes $a \in A$ folgt nun: $\mathfrak{m}+(a) = A$ oder $\mathfrak{m}+(a) \in X$. Wegen der Maximalität von $\mathfrak{m}$ muß im zweiten Fall $\mathfrak{m} = \mathfrak{m} + (a)$ gelten. Es gibt also keine Ideale, die echt zwischen $\mathfrak{m}$ und A liegen. □

Eine unmittelbare Folgerung daraus ist, daß jeder Ring $A \neq 0$ wenigstens ein maximales Ideal und damit wenigstens ein Primideal besitzt, d.h. $\mathrm{Spec}(A) = \emptyset$ genau dann, wenn $A = 0$.

A.4 Euklidische Ringe

Definition A.14 — Ein *euklidischer Ring* ist ein Integritätsbereich A zusammen mit einer Gradfunktion $\delta : A \setminus \{0\} \to \mathbb{N}_0$ und der Eigenschaft, daß es für alle $a \in A$ und $b \in A \setminus \{0\}$ Elemente $q, r \in A$ mit $a = qb + r$ und $r = 0$ oder $\delta(r) < \delta(b)$ gibt.

Häufig spricht vom Rest r der Division von a durch b. Dabei muß man allerdings daran denken, daß das Paar (q, r) im allgemeinen durch (a, b) nicht (!) eindeutig bestimmt ist. Dies ist nicht einmal im Ring $\mathbb{Z}$ der ganzen Zahlen mit $\delta(a) := |a|$ der Fall.

Beispiele A.15 — 1. $\mathbb{Z}$ ist ein euklidischer Ring mit Gradfunktion $\delta(a) := |a|$.
2. $\mathbb{Z}[i]$ ist ein euklidischer Ring mit Gradfunktion $\delta(z) = |z|^2$.
3. Für jeden Körper K ist der Polynomring $K[X]$ euklidisch mit Gradunktion $\delta(f) = \deg(f)$.

Satz A.16 — *Euklidische Ringe sind Hauptidealringe.*

Beweis. Es sei (A, δ) ein euklidischer Ring und $I \subset A$ ein Ideal. Falls $I = 0$, ist nichts zu zeigen. Es sei also $I \neq 0$ und $b \in I \setminus \{0\}$ ein Element mit $\delta(b) = \min\{\delta(c) \mid c \in I \setminus \{0\}\}$. Offensichtlich ist $(b) \subset I$. Falls keine Gleichheit gilt, sei $a \in I \setminus (b)$ beliebig und $r = a - qb$ ein Rest bei Division von a durch b, so daß also $r = 0$ oder $\delta(r) < \delta(b)$. Da $r = a - qb \in I$, ist die zweite Möglichkeit wegen der Minimalitätsbedingung an b ausgeschlossen, aber auch die Möglichkeit $r = 0$ führt auf den Widerspruch $a = qb \in (b)$. □

Satz A.17 — *Es sei A ein Hauptidealring. Dann besitzt jede endliche Menge $S \subset A$ einen größten gemeinsamen Teiler d. Außerdem gibt es Elemente $s_i \in S$ und $a_i \in A$ für $i = 1, \ldots, n$ mit*

$$d = a_1 s_1 + \ldots + a_n s_n.$$

Beweis. Das von S erzeugte Ideal ist ein Hauptideal, etwa $S = (d)$. Dann besitzt d wegen $d \in (S)$ eine Darstellung wie angegeben. Wegen $s \in S \subset (S) = (d)$ gilt $d|s$ für alle $s \in S$. Schließlich folgt aus $x|s$ für alle $s \in S$ auch $x|\sum_i a_i s_i = d$. Damit ist d ein größter gemeinsamer Teiler. □

Bemerkung A.18 — In Euklidischen Ringen A gibt es ein Verfahren, die additive Darstellung eines größten gemeinsamen Teilers zu berechnen, den euklidischen Algorithmus. Es seien a und b in A gegeben. Man setzt $a_0 = a$ und $a_1 = b$. Solange $a_i \neq 0$ berechnet man iterativ $a_{i-1} = q_{i-1}a_i + a_{i+1}$ mit $a_{i+1} = 0$ oder $\delta(a_{i+1}) < \delta(a_i)$. Da die Folge $\delta(a_i)$ für $i \geq 1$ monoton fällt, bricht das Verfahren nach endlich vielen Schritten ab. Wurde im n-ten Schritt $a_{n+1} = 0$ gefunden, so ist a_n ein größter gemeinsamer Teiler von a und b. Durch Auflösen der Gleichungen $a_{i-1} = q_{i-1}a_i + a_{i+1}$, $i = 1, \ldots, n$, nach a_0 und a_1 findet man Koeffizienten A_k und B_k mit $a_k = A_k a + B_k b$.

A.5 Lokalisierung und Quotientenringe

Weil in den ganzen Zahlen die multiplikativen Inversen fehlen, geht man zum Körper der rationalen Zahlen über. Allgemeiner konstruiert man zu einem Integritätsbereich A seinen Quotientenkörper $Q(A)$, in dem alle Elemente aus $A \setminus \{0\}$ invertierbar sind. Lokalisierung ist ein Verfahren, zu einem gegebenen kommutativen Ring A einen neuen Ring zu konstruieren, in dem eine vorgegebene Menge von Elementen invertierbar wird.

Definition A.19 — Es sei A ein kommutativer Ring. Eine Teilmenge $S \subset A$ ist multiplikativ abgeschlossen, wenn $1 \in S$ und wenn $f_1 f_2 \in S$ für alle $f_1, f_2 \in S$.

Wir betrachten auf der Menge $A \times S$ die folgende Relation:

$$(a, s) \sim (a', s') \quad :\Leftrightarrow \quad \text{es gibt ein } t \in S \text{ mit } tas' = ta's.$$

Dies ist eine Äquivalenzrelation (!). Wenn A ein Integritätsbereich ist, kann wegen der Gültigkeit der Kürzungsregel in der Definition der Relation stets $t = 1$ gewählt werden. Wir bezeichnen mit $S^{-1}A := A \times S/\sim$ den Quotienten nach der Relation $\sim$ und mit a/s die Klasse von (a, s).

Lemma A.20 — *Auf $S^{-1}A$ wird durch*

$$\frac{a}{s} + \frac{a'}{s'} := \frac{as' + a's}{ss'} \quad \textit{und} \quad \frac{a}{s} \cdot \frac{a'}{s'} := \frac{aa'}{ss'}$$

eine Ringstruktur definiert. Die Abbildung $i : A \to S^{-1}A, a \mapsto a/1$, ist ein Ringhomomorphismus.

Beweis. Übung □

Der Ring $S^{-1}A$ oder genauer: die Abbildung $i : A \to S^{-1}A$ heißt Lokalisierung von A nach der Menge S.

Satz A.21 *(Universelle Eigenschaft der Lokalisierung) — Es sei A ein kommutativer Ring, $S \subset A$ eine multiplikativ abgeschlossene Menge und $i : A \to S^{-1}A$ die zugehörige Lokalisierung. Ist $\varphi : A \to B$ ein Ringhomomorphismus in einen kommutativen Ring B mit $\varphi(S) \subset B^\times$, dann gibt es einen eindeutig bestimmten Ringhomomorphismus $\psi : S^{-1}A \to B$ mit $\varphi = \psi \circ i$.*

Beweis. Falls ψ existiert, muß wegen $\varphi(a) = \psi(a/1) = \psi(a/s)\psi(s/1) = \psi(a/s)\varphi(s)$ gelten: $\psi(a/s) = \varphi(a)\varphi(s)^{-1}$. Daher ist ψ jedenfalls eindeutig. Definiert man umgekehrt ψ auf diese Weise, dann ist ψ wohldefiniert und ein Homomorphismus. □

In den folgenden Fällen werden spezielle Bezeichnungen verwendet: A sei ein kommutativer Ring.

1. Für $f \in A$ setzt man $A_f := \{f^n \mid n \in \mathbb{N}_0\}^{-1}A$.
2. Für ein Primideal $\mathfrak{p} \subset A$ setzt man $A_\mathfrak{p} := (A \setminus \mathfrak{p})^{-1}A$.
3. Die Menge $NNT(A)$ der Nichtnullteiler von A ist multiplikativ abgeschlossen. $Q(A) := \mathrm{NNT}(A)^{-1}A$ heißt der totale Quotientenring von A. Wenn A ein Integritätsbereich ist, ist $Q(A)$ der Quotientenkörper von A.

Beispiele A.22 — 1. $Q(\mathbb{Z}) = \mathbb{Q}$.
2. Es sei K ein Körper. Der Polynomring $K[X]$ ist ein Integritätsbereich. Der Körper

$$K(X) := Q(K[X])$$

heißt Körper der rationalen Funktionen (mit Koeffizienten in K).
3. Es sei $p \in \mathbb{N}$ eine Primzahl und $(p) \subset \mathbb{Z}$ das zugehörige Primideal. Man unterscheide die Lokalisierungen:

$$\mathbb{Z}_p := \left\{ \frac{a}{s} \in \mathbb{Q} \;\middle|\; \text{der einzige Primfaktor von } s \text{ ist } p. \right\}$$

und

$$\mathbb{Z}_{(p)} := \left\{ \frac{a}{s} \in \mathbb{Q} \;\middle|\; \text{kein Primfaktor von } s \text{ ist } p. \right\}$$

Insbesondere ist $\mathbb{Z}_p \cap \mathbb{Z}_{(p)} = \mathbb{Z}$. Der Umgang mit diesen Bezeichnungen wird dadurch erschwert, daß in vielen mathematischen Texten $\mathbb{Z}_p$ für den Restklassenring $\mathbb{Z}/p$ verwendet wird, und in wieder anderen Texten $\mathbb{Z}_p$ den Ring der ganzen p-adischen Zahlen bezeichnet. Da hilft nur: Augen auf!

A.6 Faktorielle Ringe

Definition A.23 — Es sei A ein Integritätsbereich.

1. $f \in A$ ist irreduzibel, wenn $f \neq 0$ und $f \notin A^\times$ und wenn aus $f = ab$ folgt: $f \sim a$ oder $f \sim b$.

2. $f \in A$ ist prim, wenn $f \neq 0$ und $f \notin A^\times$ und wenn aus $f|ab$ folgt: $f|a$ oder $f|b$.

Lemma A.24 — *Jedes Primelement ist irreduzibel.*

Beweis. Es sei f prim und $f = ab$. Dann gilt ohne Einschränkung $f|a$, also $a = fc$. Daraus folgt $f = fbc$, also $f(1 - bc) = 0$, so daß b und c Einheiten sein müssen und $f \sim a$. □

Definition A.25 — Ein kommutativer Ring A heißt *faktoriell*, wenn A nullteilerfrei ist und wenn jedes Element $a \in A \setminus \{0\}$ eine Produktdarstellung $a = \epsilon \cdot p_1 \cdot \ldots \cdot p_\ell$ mit einer Einheit $\epsilon \in A^\times$ und primen Elementen p_i, $i = 1, \ldots, \ell$, $\ell \in \mathbb{N}_0$, besitzt.

Lemma A.26 — *Es sei A ein faktorieller Ring und $a \in A \setminus \{0\}$. Die Primfaktorzerlegung $a = \epsilon \cdot p_1 \cdot \ldots \cdot p_\ell$ ist eindeutig bis auf Einheiten und die Reihenfolge der Faktoren, d.h. sind $a = \epsilon \cdot p_1 \cdot \ldots \cdot p_\ell$ und $a = \epsilon' \cdot p'_1 \cdot \ldots \cdot p'_n$ zwei Primfaktorzerlegungen, dann gilt $\ell = n$, und es gibt eine Permutation $\pi \in S_n$ mit der Eigenschaft, daß $p_i \sim p'_{\pi(i)}$ für $i = 1, \ldots, \ell$.*

Beweis. Ohne Einschränkung ist $\ell \leq n$. Wenn $\ell = 0$, ist $a = \varepsilon$ eine Einheit. Dann sind auch alle Faktoren ε' und p'_i Einheiten. Das geht nur, wenn auch $n = 0$.

Es sei also $\ell > 0$. Dann teilt p_1 das Element $a = \varepsilon' p'_1 \cdots p'_n$, also auch einen der Faktoren p'_i. Nach Umordnung kann man annehmen, daß es p'_1 ist. Es gilt nun $p'_1 = p_1 x$ mit einem $x \in A$. Da p'_1 irreduzibel ist und p_1 keine Einheit, ist x eine Einheit, d.h. $p_1 \sim p'_1$. Nach Kürzen von p_1 hat man Zerlegungen

$$\varepsilon p_2 \cdots p_\ell = (\varepsilon' x) p'_2 \cdots p'_n.$$

Induktion nach ℓ zeigt $n = \ell$ und $p'_i \sim p_i$ für $i = 2, \ldots, n$, nach passender Umordnung. □

Satz A.27 — *Es sei A ein Integritätsbereich. A ist genau dann faktoriell, wenn gilt*

1. *Jedes irreduzible Element in A ist prim.*
2. *Jede aufsteigenden Kette von Hauptidealen in A wird stationär.*

Beweis. Es sei zunächst A faktoriell und f ein irreduzibles Element. Nach Voraussetzung gibt es eine Primfaktorzerlegung $f = \varepsilon p_1 \cdots p_\ell$. Da f irreduzibel ist, gilt $f|p_i$ für ein i. Weil p_i auch irreduzibel ist, hat man $f \sim p_i$ für ein i. Insbesondere ist f prim. Weiter sei $(a_1) \subset (a_2) \subset (a_3) \subset \ldots$ eine aufsteigende Kette von Hauptidealen. Das ist äquivalent dazu, daß $a_2|a_1$, $a_3|a_2$, etc. Aus der Eindeutigkeit der Primfaktorzerlegung folgt, daß die Primfaktoren von a_2 bis auf Assoziation eine Teilmenge der Primfaktoren von a_1 sind. Sind die Primfaktoren einschließlich Vielfachheit gleich, unterscheiden sich a_1 und a_2 höchstens um eine Einheit, was $(a_1) = (a_2)$ impliziert.

Ist also die Inklusion $(a_2) \subset (a_1)$ echt, so hat a_2 weniger Primfaktoren als a_1. In der Idealkette kann echte Inklusion demnach nur endlich oft vorkommen.

Es gelte umgekehrt die Bedingung 2. Ein Element $a \in A \setminus \{0\}$ heiße zerlegbar, wenn sich a als Produkt aus Einheiten und irreduziblen Elementen darstellen läßt. Offenbar sind alle Einheiten und alle irreduziblen Elemente zerlegbar, ebenso alle Produkte aus zerlegbaren Elementen. Angenommen, es gibt ein unzerlegbares Element $a \in A \setminus \{0\}$. Dann ist a nicht irreduzibel und besitzt eine Zerlegung $a = a'a''$ in Faktoren, die beide keine Einheit sind. Wenigstens einer der Faktoren ist ebenfalls unzerlegbar, etwa a'. Wir setzen $a_1 = a$ und $a_2 = a'$ und verfahren mit a' analog. Dies führt auf eine Idealkette $(a_1) \subset (a_2) \subset \ldots$, in der alle Inklusionen echt sind, im Widerspruch zur Annahme. Demnach besitzen alle nichttrivialen Elemente in A eine multiplikative Zerlegung in irreduzible Elemente und Einheiten. Gilt zusätzlich die Bedingung 1, so besitzt jedes nichttriviale Element eine Primfaktorzerlegung. □

Satz A.28 — *Nullteilerfreie Hauptidealringe sind faktoriell.*

Beweis. Es sei A ein nullteilerfreier Hauptidealring. Nach Satz A.27 genügt es zu zeigen, daß jedes irreduzible Element f prim ist. Es gelte dazu $f|ab$ und $f \nmid a$. Das Ideal (f, a) ist ein Hauptideal, etwa $(f, a) = (c)$. Es bestehen dann Gleichungen

$$f = mc, \quad a = nc, \quad c = pf + qa, \quad ab = fr$$

mit geeigneten Koeffizienten $m, n, p, q, r \in A$. Da f irreduzibel ist, ist entweder $c \sim f$ oder $c \sim 1$. Der erste Fall ist wegen $c|a$ und $f \nmid a$ ausgeschlossen. Im zweiten Falle folgt $b = (bc^{-1})c = (bc^{-1})(pf + qa) = c^{-1}(bpf + qfr)$, also $f|b$. □

Es sei A ein faktorieller Ring und $D \subset A$ ein Vertretersystem für die Klassen assoziierter Primelemente, d.h. jedes Primelement ist zu genau einem Primelement in D assoziiert. In manchen Ringen läßt sich ein solches Vertretersystem durch eine einfache Konvention auszeichnen: In $\mathbb{Z}$ unterscheiden sich assoziierte Primelemente höchsten um ein Vorzeichen und wir können $D = \{p \in \mathbb{N} \mid p \text{ Primzahl}\}$ wählen. Im Polynomring $K[X]$ über einem Körper X unterscheiden sich assoziierte Primelemente höchstens um eine nichttriviale Konstante. In jeder Klasse gibt es also genau ein normiertes Polynom, d.h. ein Polynom mit Leitkoeffizienten 1, und wir können $D = \{f \mid f \text{ ist normiert und irreduzibel}\}$ setzen.

Mit einem solchen Vertretersystem D können wir jedes Element $a \in A \setminus \{0\}$ auf eindeutige Weise in der Form

$$a = u \prod_{p \in D} p^{\nu_p}$$

schreiben, wobei $\nu_p = 0$ für fast alle $p \in D$. Man nennt $\mathrm{ord}_p(a) := \nu_p$ die Ordnung von a bezüglich p. Allgemeiner definieren wir für jedes $a = b/c \in Q(A)^\times$ mit $b, c \in A$ und $p \in D$ die Ordnung

$$\mathrm{ord}_p(a) := \mathrm{ord}_p(b) - \mathrm{ord}_p(c) \in \mathbb{Z}.$$

Aus der Eindeutigkeit der Primfaktorzerlegung folgt, daß die Ordnung

$$\mathrm{ord}_p : Q(A)^\times \to \mathbb{Z}$$

wohldefiniert und ein Gruppenhomomorphismus ist. Wir erweitern die Abbildung noch, indem wir formal $\mathrm{ord}_p(0) := \infty$ setzen. Mit diesen Bezeichnungen haben wir dann für jedes $a \in Q(A)^\times$ eine eindeutige Zerlegung

$$a = u \prod_{p \in D} p^{\mathrm{ord}_p(a)}$$

mit einer Einheit $u \in A$.

Definition A.29 — Es sei A ein faktorieller Ring, $D \subset A$ ein Repräsentantensystem der Klassen assoziierter Primelemente.

1. Für ein Tupel $\{a_0, \ldots, a_n\}$ von Elementen in $Q(A)$, die nicht alle gleichzeitig verschwinden, heißt

   $$\mathrm{Inh}(a_0, \ldots, a_n) = \prod_{p \in D} p^{\min\{\mathrm{ord}_p(a_i) | i=0,\ldots,n\}} \in Q(A)$$

   der Inhalt des Tupels.

2. Für $f = \sum_{i=0}^n f_n X^n \in Q(A)[X] \setminus \{0\}$ heißt $\mathrm{Inh}(f) = \mathrm{Inh}(f_0, \ldots, f_n)$ der Inhalt des Polynoms f.

3. Ein Polynom $f \in Q(A)[X] \setminus \{0\}$ heißt primitiv, wenn $\mathrm{Inh}(f) = 1$.

Im Folgenden gehen wir, wenn von einem faktoriellen Ring A die Rede ist, immer davon aus, daß ein Vertretersystem $D \subset A$ für Primelemente gewählt ist, und die Begriffe 'Inhalt' und 'primitiv' beziehen sich stets auf dieses fest gewählte System. Man verifiziert leicht die folgenden Aussagen:

1. Für jedes $a \in Q(A)^\times$ ist $a/\mathrm{Inh}(a)$ eine Einheit in A.

2. Für $a \in Q(A)^\times$ und $f \in Q(A)[X] \setminus \{0\}$ gilt $\mathrm{Inh}(af) = \mathrm{Inh}(a)\,\mathrm{Inh}(f)$.

3. Ein nichttriviales Polynom $f \in Q(A)[X]$ ist genau dann primitiv, wenn $f \in A[X]$ und wenn die Koeffizienten von f teilerfremd sind.

4. Für $f \in Q(A)[X] \setminus \{0\}$ ist $f/\mathrm{Inh}(f)$ primitiv.

Es folgen eine Reihe von Sätzen, die in der Regel nach Gauß benannt werden. Gauß beweist in Disq. Arith. Art. 42 eigentlich den folgenden Satz: *Sind $f, g \in \mathbb{Q}[X]$ normierte Polynome von positivem Grad und ist $fg \in \mathbb{Z}[X]$, dann haben auch f und g ganzzahlige Koeffizienten.* Die Beweismethode verallgemeinert sich auf faktorielle Ringe und führt zu den folgenden Aussagen:

Lemma A.30 — *Es sei A ein faktorieller Ring. Sind $f, g \in A[X]$ nichttriviale primitive Polynome, so ist auch $fg \in A[X]$ primitiv.*

Beweis. Wir machen den Ansatz

$$f = f_0 + f_1 X + \ldots + f_n X^n, \quad g = g_0 + g_1 X + \ldots + g_m X^m,$$

und $fg =: h = h_0 + h_1 X + \ldots + h_{n+m} X^{n+m}$. Es sei ein Primelement $p \in D$ fixiert. Da f und g primitiv sind, gibt es Indizes i und j mit $\operatorname{ord}_p(f_i) = 0$ und $\operatorname{ord}_p(g_j) = 0$. Es seien i_0 bzw. j_0 die größten Indizes mit dieser Eigenschaft. Dann ist in dem Ausdruck

$$h_{i_0+j_0} = f_{i_0} g_{j_0} + \sum_{i>i_0} f_i g_{k_0-i} + \sum_{j>j_0} f_{k_0-j} g_j.$$

im zweiten Summanden jeweils der erste Faktor durch p teilbar, und im dritten Summanden jeweils der zweite Faktor. Andererseits ist $f_{i_0} g_{i_0}$ nicht durch p teilbar. Folglich ist $h_{i_0+j_0}$ nicht durch p teilbar und somit p kein Faktor des Inhalts von h. Da dies für alle $p \in D$ gilt, ist h primitiv. □

Lemma A.31 — *Es sei A ein faktorieller Ring. Für nichttriviale Polynome $f, g \in Q(A)[X]$ gilt:* $\operatorname{Inh}(fg) = \operatorname{Inh}(f) \operatorname{Inh}(g)$.

Beweis. Die Polynome $f/\operatorname{Inh}(f)$ und $g/\operatorname{Inh}(g)$ sind primitiv, nach Lemma A.30 also auch $fg/(\operatorname{Inh}(f)\operatorname{Inh}(g))$. Daraus folgt

$$1 = \operatorname{Inh}\left(\frac{fg}{\operatorname{Inh}(f)\operatorname{Inh}(g)}\right) = \frac{\operatorname{Inh}(fg)}{\operatorname{Inh}(f)\operatorname{Inh}(g)}.$$

□

Satz A.32 — *Es sei A ein faktorieller Ring. Ein nichtkonstantes Polynom $f \in A[X]$, das in $A[X]$ irreduzibel ist, ist auch in $Q(A)[X]$ irreduzibel.*

Beweis. Es sei $f \in A[X]$ ein nichtkonstantes irreduzibles Polynom. Dann ist f insbesondere primitiv und $\operatorname{Inh}(f) = 1$. Angenommen, es gibt eine Zerlegung $f = gh$ mit nichtkonstanten Polynomen $g, h \in Q(A)[X]$. Dann gilt $1 = \operatorname{Inh}(f) = \operatorname{Inh}(g)\operatorname{Inh}(h)$ und somit

$$f = \frac{g}{\operatorname{Inh}(g)} \frac{h}{\operatorname{Inh}(h)}.$$

Auf der rechten Seite stehen zwei nichtkonstante Polynome in $A[X]$ im Widerspruch zur Irreduzibilität von f. □

Satz A.33 (Satz von Gauß) — *A faktoriell $\Rightarrow$ $A[X]$ faktoriell.*

Beweis. $A[X]$ genügt der Kettenbedingung für Hauptideale: Hat man $(f_1) \subset (f_2) \subset \ldots$, so fällt der Grad der Polynome f_n monoton und muß konstant werden, etwa für alle $n \geq n_0$. Dann ist $f_n/f_{n_0} =: a_n \in A$ für $n \geq n_0$ eine Folge von Ringelementen mit $(a_n) \subset (a_{n+1}) \subset \ldots$. Weil A der Kettenbedingung für Hauptideale genügt, wird auch diese Kette stationär.

Nach Satz A.27 genügt es zu zeigen, daß jedes in $A[X]$ irreduzible Element f prim ist. Wenn f konstant ist, ist dies klar. Es sei also f ein nicht konstantes, irreduzibles Polynom, und es gelte $f|ab$ für Polynome $a, b \in A[X]$. Nach Satz A.32 ist f in $Q(A)[X]$ irreduzibel, und weil $Q(A)[X]$ ein Hauptidealring ist, auch prim. Ohne Einschränkung können wir daher annehmen, daß $f|a$ in $Q(A)[X]$, etwa $a = fc$ mit $c \in Q(A)[X]$. Gemäß Lemma A.31 hat man

$$\mathrm{Inh}(a) = \mathrm{Inh}(f)\,\mathrm{Inh}(c) = \mathrm{Inh}(c) \in A.$$

Aber dann ist auch $c \in A[X]$. Deshalb ist f schon in $A[X]$ ein Teiler von a. Zusammengenommen zeigt dies, daß f prim ist. □

Durch Induktion über die Anzahl der Variablen erhält man:

Folgerung A.34 — *A faktoriell $\Rightarrow$ $A[X_1, \ldots, X_\ell]$ faktoriell.*
Insbesondere ist für jeden Körper K der Polynomring $K[X_1, \ldots, X_\ell]$ faktoriell. □

Die folgenden Kriterien erweisen sich als außerordentlich nützlich, wenn man die Irreduzibilität eines Polynoms testen will.

Satz A.35 *(Eisensteinkriterium) — Es sei A ein faktorieller Ring und p ein Primelement in A. Gilt für das nichtkonstante primitive Polynom $f = f_0 + \ldots + f_n X^n$, daß*

$$p \not| f_n, \quad p|f_{n-1}, \quad \ldots, \quad p|f_0, \quad p^2 \not| f_0,$$

so ist f in $A[X]$ irreduzibel.

Beweis. Es sei $f = gh$ eine Zerlegung mit Polynomen $g = g_0 + \ldots + g_m X^m$, $h = h_0 + \ldots + h_\ell X^\ell \in A[X]$, die keine Einheiten sind. Da f primtiv ist, sind g und h auch nicht konstant. Wir betrachten die kanonische Projektion $A[X] \to A/(p)[X]$ und schreiben $\overline{f}$ für das Bild von f etc. Nach Annahme ist $\overline{g}\overline{h} = \overline{f} = X^n$. Notwendigerweise ist dann $\overline{g} = \overline{g}_m X^m$ und $\overline{h} = \overline{h}_\ell X^\ell$. Das bedeutet, daß p ein Teiler von g_0 und von h_0 ist. Aber dann teilt p^2 das Produkt $g_0 h_0 = f_0$, im Widerspruch zur Annahme. □

Satz A.36 *(Reduktionskriterium) — Es sei A ein faktorieller Ring und $\mathfrak{p} \subset A$ ein Primideal mit Restklassenring $\overline{A}$. Es sei $f \in A[X]$ ein nichtkonstantes primitives Polynom mit $Lc(f) \notin \mathfrak{p}$. Ist die Reduktion $\overline{f} \in \overline{A}[X]$ irreduzibel, so ist auch f irreduzibel.*

Beweis. Angenommen, f ist nicht irreduzibel und besitzt eine Zerlegung $f = gh$, in der g und h keine Einheiten sind. Da f primitiv ist, können g und h keine Konstanten sein. Die Annahme $Lc(f) \notin \mathfrak{p}$ bedeutet, daß $\overline{f}$ und f denselben Grad haben. Wegen $\overline{f} = \overline{g}\overline{h}$ haben daher auch $\overline{g}$ und $\overline{h}$ denselben Grad wie g bzw. h und sind nichtkonstante Polynome. Das Widerspricht der Annahme, daß $\overline{f}$ irreduzibel ist. □

A.7 Möbiussche Umkehrformeln

Die Abbildung $\mu : \mathbb{N} \to \mathbb{Z}$ mit $\mu(n) = (-1)^r$, falls $n = p_1 \cdots p_r$ mit r paarweise verschiedenen Primfaktoren, und $\mu(n) = 0$ sonst, heißt Möbiusfunktion. Es gilt also zum Beispiel

n	1	2	3	4	5	6	7
$\mu(n)$	1	-1	-1	0	-1	1	-1

Die Möbiusfunktion hat die fundamentale Eigenschaft

$$\sum_{d|n} \mu(d) = \begin{cases} 1, \text{ falls } n = 0, \text{ und} \\ 0 \text{ sonst.} \end{cases}$$

Lemma A.37 *(Möbiussche Umkehrformeln) — Es sei A ein kommutativer Ring. Für zwei Folgen $a, b : \mathbb{N} \to A$ sind die folgenden Aussagen äquivalent:*

1. $a_n = \sum_{d|n} b_d$ *für alle* $n \in \mathbb{N}$.
2. $b_n = \sum_{d|n} \mu(n/d) a_d$ *für alle* $n \in \mathbb{N}$.

Beweis. Man kommt von der einen Formel zur anderen durch ein einfaches Doppelsummenargument, oder etwas strukturierter wie folgt: Auf der Menge R aller Folgen $a : \mathbb{N} \to A$ ist durch $(a + b)_n = a_n + b_n$ und $(a * b)_n = \sum_{d|n} a_d b_{n/d}$ die Struktur eines kommutativen Rings gegeben. Das Neutralelement für das sogenannte Faltungsprodukt $*$ ist die Abbildung ε mit $\varepsilon_n = \delta_{n,0}$. Bezeichnet 1 die konstante Abbildung $1_n = 1$, so übersetzt sich die fundamentale Eigenschaft der Möbiusfunktion in die Aussage $1 * \mu = \varepsilon$. Die zu vergleichenden Ausagen lassen sich mit dem Faltungsprodukt so schreiben: $a = b * 1$ und $b = a * \mu$. Die Äquivalenz der Aussagen folgt also unmittelbar daraus, daß μ und 1 bezüglich $*$ invers zueinander sind. □

A.8 Aufgaben

Aufgabe A.1 — Was kann man über kommutative Ringe A mit $A^\times \cong 0$ sagen?

Aufgabe A.2 — Es sei A ein kommutativer Ring. Man zeige:

1. A nullteilerfrei $\Rightarrow A[X]$ nullteilerfrei.
2. A nullteilerfrei $\Rightarrow A[X]^\times = A^\times$.

Aufgabe A.3 — Bestimmen Sie alle Einheiten, alle Nullteiler und alle nilpotenten Elemente in $\mathbb{Z}/24$ und in $\mathbb{Z}/4[X]$.

Aufgabe A.4 — Es seien $a, b \in A$ nilpotent, $u \in A$ beliebig.

1. $a + b$ und ua sind nilpotent.
2. $u + aX \in A[X]$ ist genau dann eine Einheit, wenn $u \in A$ eine Einheit ist. Was ist in diesem Falle das Inverse von $u + aX$?

Aufgabe A.5 — Beweisen Sie die Aussagen aus Beispiel A.7. Geben Sie Beispiele für Ideale I und J mit $IJ = I \cap J$ bzw. mit $IJ \neq I \cap J$.

Zu maximalen Idealen und Primidealen:

Aufgabe A.6 — Es sei A ein kommutativer Ring.
1. Jedes maximale Ideal ist ein Primideal.
2. Ein Hauptideal (a) ist genau dann ein Primideal, wenn a ein Primelement ist.
3. Ein Ideal $\mathfrak{p}$ ist genau dann ein Primideal, wenn $\mathfrak{p} \neq A$ und wenn für alle Ideale $\mathfrak{a}$ und $\mathfrak{b}$ aus $\mathfrak{ab} \subset \mathfrak{p}$ folgt: $\mathfrak{a} \subset \mathfrak{p}$ oder $\mathfrak{b} \subset \mathfrak{p}$.
4. $\mathfrak{p}$ ist genau dann ein Primideal, wenn $A/\mathfrak{p}$ ein Integritätsbereich ist.
5. $\mathfrak{m}$ ist genau dann ein maximales Ideal, wenn $A/\mathfrak{m}$ ein Körper ist.

Aufgabe A.7 — Zeigen Sie, indem Sie den Existenzbeweis für maximale Ideale imitieren: Ist A ein kommutativer Ring, $I \subset A$ ein Ideal und $f \in A$ ein Element mit $f^n \notin I$ für alle $n > 0$. Dann gibt es ein Primideal $\mathfrak{p}$ mit $I \subset \mathfrak{p}$ und $f \notin \mathfrak{p}$.

Aufgabe A.8 — Es sei $f : A \to B$ ein Homomorphismus von kommutativen Ringen. Für jedes Primideal $\mathfrak{p} \subset B$ ist $f^{-1}(\mathfrak{p})$ ein Primideal in A. Dies definiert eine Abbildung $\tilde{f} : \operatorname{Spec}(B) \to \operatorname{Spec}(A)$.

Aufgabe A.9 — Es sei A ein kommutativer Ring. Für jedes Ideal I in A sei $V(I) := \{\mathfrak{p} \in \operatorname{Spec}(A) \mid I \subset \mathfrak{p}\}$. Eine Menge $V \subset \operatorname{Spec}(A)$ heißt Zariski-abgeschlossen, wenn es ein Ideal I mit $V = V(I)$ gibt. Zeigen Sie, daß die Zariski-abgeschlossenen Teilmengen von $\operatorname{Spec}(A)$ die abgeschlossenen Mengen einer Topologie auf $\operatorname{Spec}(A)$ sind. (Diese Topologie heißt Zariski-Topologie.) Zeigen Sie, daß für jeden Ringhomomorphismus $f : A \to B$ die Abbildung $\tilde{f} : \operatorname{Spec}(B) \to \operatorname{Spec}(A)$ stetig ist.

Zu Lokalisierungen:

Aufgabe A.10 — Man zeige:
1. Für jedes $f \in A$ ist $\{f^n \mid n \in \mathbb{N}_0\}$ multiplikativ abgeschlossen.
2. $\mathfrak{p} \subset A$ ist genau dann ein Primideal, wenn $A \setminus \mathfrak{p}$ multiplikativ abgeschossen ist.
3. Die Menge $\operatorname{NNT}(A) := \{a \in A \mid a \text{ ist kein Nullteiler}\}$ der Nichtnullteiler von A ist multiplikativ abgeschlossen.

Aufgabe A.11 — Zeigen Sie, daß die im Abschnitt A.5 definierte Relation $\sim$ auf $A \times S$ eine Äquivalenzrelation ist. Wozu wurde das Element t in der Definition der Relation gebraucht? Unter welchen Bedingungen kann man auf t verzichten und die Definition der Relation vereinfachen? Beweisen Sie Lemma A.20 und die fehlenden Teile in Satz A.21.

Aufgabe A.12 — Es sei A ein kommutativer Ring und $i : A \to S^{-1}A$ die Lokalisierung von A nach der multiplikativ abgeschlossenen Teilmenge $S \subset A$. Zeigen Sie:
1. $S^{-1}A$ ist genau dann der Nullring, wenn $0 \in S$. Insbesondere ist A_f genau dann der Nullring, wenn f nilpotent ist.
2. $i : A \to S^{-1}A$ ist genau dann injektiv, wenn S keine Nullteiler enthält. Insbesondere ist $i : A \to Q(A)$ injektiv.
3. Wenn A ein Integritätsbereich ist, ist $Q(A)$ ein Körper. In welchem Sinne ist $Q(A)$ der kleinste Körper, der A enthält?

Aufgabe A.13 — Wir schreiben $K(X_1, \ldots, X_\ell) := Q(K[X_1, \ldots, X_\ell])$. Was ist der Unterschied zwischen den Körpern $K(X_1, X_2)$ und $K(X_1)(X_2)$ der Definition und ihrer Bedeutung nach? Formulieren und beweisen Sie einen Zusammenhang.

Zu faktoriellen Ringen:

Aufgabe A.14 — Jeder faktorielle Ring besitzt unendlich viele paarweise nichtassoziierte Primelemente. [Hinweis: Das wußte schon Euklid.]

Aufgabe A.15 — Es sei A ein kommutativer Ring zusammen mit einer Abbildung $\delta : A \setminus \{0\} \to \mathbb{N}_0$ mit den Eigenschaften

$$\delta(a) = 0 \Leftrightarrow a \in A^\times, \quad \text{und} \quad \delta(ab) = \delta(a) + \delta(b) \text{ für alle } a, b \in A \setminus \{0\}.$$

Zeigen Sie, daß jedes Element $a \in A \setminus \{0\}$ eine Produktzerlegung in irreduzible Elemente und Einheiten besitzt.

Aufgabe A.16 — Es sei K ein Körper und $A = K[\{X_s\}_{s_S}]$ der Polynomring mit Unbestimmten X_s, $s \in S$, für eine beliebige Indexmenge. Man zeige:
1. A ist genau dann noethersch, wenn S endlich ist.
2. A ist faktoriell.

Aufgabe A.17 — Es sei A faktoriell und $D \subset A$ ein Vertretersystem. Man zeige, daß für zwei Elemente $a, b \in A \setminus \{0\}$ genau dann $a|b$ gilt, wenn $\mathrm{ord}_p(a) \leq \mathrm{ord}_p(b)$ für alle $p \in D$. Formulieren Sie Existenzaussagen und Charakterisierungen für größte gemeinsame Teiler und kleinste gemeinsame Vielfache.

Aufgabe A.18 — Verallgemeinern Sie Folgerung A.34 auf Polynomringe mit beliebig vielen Unbestimmten.

Zur Möbiusfunktion:

Aufgabe A.19 — Es sei φ die Eulersche Phi-Funktion, d.h. $\varphi(n)$ ist die Anzahl der zu n teilerfremden ganzen Zahlen zwischen 0 und n. Für jede natürliche Zahl n gilt $\sum_{d|n} \varphi(d) = n$, indem wir für jedes $d|n$ die natürlichen Zahlen $x < n$ mit $\mathrm{ggT}(x, n) = d$ zusammenfassen und zählen. Wenden Sie hierauf die Möbiussche Umkehrformel an und zeigen Sie, daß $\frac{\varphi(n)}{n} = \prod_{p|n} \left(1 - \frac{1}{p}\right)$, wobei p durch die Primteiler von n läuft.

B Die Quatenionengruppe als Galoisgruppe

Das *inverse Galoisproblem* lautet: *Läßt sich jede endliche Gruppe als Galoisgruppe einer Erweiterung von $\mathbb{Q}$ erhalten*? Diese Frage ist offen. Wir haben in der Vorlesung gesehen, dass alle abelschen Gruppen, sowie die alternierenden und die symmetrischen Gruppen realisiert werden. Shafarevich hat gezeigt, dass jede auflösbare Gruppe realisiert wird. Zu den Gruppen, für die die Frage offen ist, gehört die Mathieugruppe M_{24}, das ist eine der einfachen sporadischen Gruppen mit der Ordnung $48 \cdot 24 \cdot 23 \cdot 22 \cdot 21 \cdot 20$, aber auch schon gewissermaßen einfachere Gruppen der Form $\mathrm{SL}(2, \mathbb{F}_q)$ für gewisse Primzahlen q.

An dieser Stelle soll uns die nächst schwierigere Gruppe nach der symmetrischen Gruppe S_3 genügen. Ich kann mich nicht erinnern, von wem ich das folgende Beispiel kennengelernt habe.

Satz B.1 — *Die Gruppe der Gleichung $X^8 - 72X^6 + 180X^4 - 144X^2 + 36 = 0$ über $\mathbb{Q}$ ist die Quaternionengruppe Q_8.*

Beweis. Es sei $f(X) := X^8 - 72X^6 + 180X^4 - 144X^2 + 36$. Ist $\alpha \in \overline{\mathbb{Q}}$ eine Nullstelle von f, so auch $-\alpha$. In der Zerlegung von f in irreduzible Faktoren muss daher jeder Faktor selbst ein Polynom in X^2 sein, da f keine Lösungen in $\mathbb{Q}$ hat. Es genügt also, sich von der Irreduzibilität des Polynoms

$$g(X) := X^4 - 72X^3 + 180X^2 - 144X + 36$$

zu überzeugen. Das sieht man aus der folgenden expliziten Lösung der Gleichung $g(X) = 0$. Die Substitution $X = z + 18$ führt auf das Polynom

$$h(z) = g(z + 18) = z^4 - 1764z^2 - 40320z - 259164.$$

Die Gleichung $h(z) = 0$ wird mit dem Ansatz

$$z^4 + 2dz^2 + d^2 = (1764 + 2d)z^2 + 40320z + (259164 + d^2) \tag{B.1}$$

gelöst: Bezeichnet man die rechte Seite mit $Az^2 + Bz + C$, so läßt sie sich genau dann als Quadrat einer Linearform $(\sqrt{A}z + \sqrt{C})$ schreiben, wenn $4AC = B^2$. Dies führt in der gegeben Situation auf die Bedingung

$$4(1764 + 2d)(259164 + d^2) = 40320^2,$$

also die Gleichung

$$d^3 + 882d^2 + 259164d + 25369848 = 0$$

für d. Diese Gleichung zerfällt in Linearfaktoren

$$(d + 282)(d + 294)(d + 306) = 0.$$

Setzt man $d = -306$ in die Gleichung (B.1) ein, so erhält man:

$$z^2 - 306 = \pm 12\sqrt{2}(2z + 35)$$

oder umgeformt:

$$(z \mp 12\sqrt{2})^2 = 594 \pm 420\sqrt{2} = 3(198 \pm 140\sqrt{2}) = 3(10 \pm 7\sqrt{2})^2.$$

Das führt auf die vier folgenden Lösungen für $g(x) = 0$:

$$\begin{aligned} x_1 &= 18 + 12\sqrt{2} + 10\sqrt{3} + 7\sqrt{6} \\ x_2 &= 18 - 12\sqrt{2} + 10\sqrt{3} - 7\sqrt{6} \\ x_3 &= 18 + 12\sqrt{2} - 10\sqrt{3} - 7\sqrt{6} \\ x_4 &= 18 - 12\sqrt{2} - 10\sqrt{3} + 7\sqrt{6} \end{aligned}$$

Offenbar ist der Zerfällungskörper von $g(X)$ der Körper

$$M := \mathbb{Q}(x_1) = \mathbb{Q}(\sqrt{2}, \sqrt{3}).$$

Dessen Galoisgruppe ist

$$\mathrm{Gal}(M/\mathbb{Q}) = \mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}) \cong \mathbb{Z}/2 \times \mathbb{Z}/2 = \langle \bar{I}, \bar{J} \rangle$$

mit Erzeugern

$$\begin{aligned} \bar{I} &: \sqrt{2} \mapsto -\sqrt{2}, \sqrt{3} \mapsto \sqrt{3}, \\ \bar{J} &: \sqrt{2} \mapsto \sqrt{2}, \sqrt{3} \mapsto -\sqrt{3}, \end{aligned}$$

und den Relationen $\bar{I}^2 = 1, \bar{J}^2 = 1, \bar{I}\bar{J} = \bar{J}\bar{I}$.

Es sei jetzt α eine Wurzel der Gleichung $T^2 - x_1 = 0$, und $L = M(\alpha)$. Die Galoisgruppe $\mathrm{Gal}(L/M) \cong \mathbb{Z}/2$ wird erzeugt von einer Involution $\iota : \alpha \mapsto -\alpha$. Wir zeigen zunächst, dass das Polynom f über L in Linearfaktoren zerfällt. Dazu müssen wir Wurzeln α_i der Gleichungen $T^2 - x_i = 0$ finden. Nun gilt:

$$(\alpha\alpha_i)^2 = \alpha^2\alpha_i^2 = x_1x_i.$$

Für $i = 2, 3, 4$ findet man:

$$\begin{aligned} x_1x_2 &= 42 + 24\sqrt{3} = [\sqrt{2}(3 + 2\sqrt{3})]^2 \\ x_1x_3 &= 18 + 12\sqrt{2} = [\sqrt{3}(2 + 1\sqrt{2})]^2 \\ x_1x_4 &= 30 + 12\sqrt{6} = [\sqrt{3}(2 + \sqrt{6})]^2. \end{aligned}$$

Demnach sind die acht Wurzeln von $f(X)$ gegeben durch:

$$\pm\alpha, \quad \pm\frac{3\sqrt{2}+2\sqrt{6}}{\alpha}, \quad \pm\frac{2\sqrt{3}+\sqrt{6}}{\alpha}, \quad \pm\frac{2\sqrt{3}+3\sqrt{2}}{\alpha}.$$

Es bleibt die Galoisgruppe zu bestimmen. Dazu seien I und J die Fortsetzungen von $\bar{I}$ und $\bar{J}$, die durch

$$I(\alpha) = \frac{3\sqrt{2}+2\sqrt{6}}{\alpha} \quad \text{bzw.} \quad J(\alpha) = \frac{2\sqrt{3}+\sqrt{6}}{\alpha}$$

charakterisiert sind. Man findet, dass I^2 und J^2 den Körper M festlassen und α auf $-\alpha$ abbilden. Insbesondere gilt $I^2 = J^2 = \iota$, und I und J haben die Ordnung 4. Betrachte die beiden Kompositionen IJ und JI. Man findet:

$$IJ(\alpha) = I\left(\frac{2\sqrt{3}+\sqrt{6}}{\alpha}\right) = \frac{2\sqrt{3}-\sqrt{6}}{3\sqrt{2}+2\sqrt{6}}\alpha = -(\sqrt{2}-1)(\sqrt{3}-2)\alpha$$

und

$$JI(\alpha) = J\left(\frac{3\sqrt{2}+2\sqrt{6}}{\alpha}\right) = \frac{3\sqrt{2}-2\sqrt{6}}{2\sqrt{3}+\sqrt{6}}\alpha = (\sqrt{2}-1)(\sqrt{3}-2)\alpha.$$

Das zeigt $IJ = \iota JI$. Da ι mit I und J vertauscht, lauten die vollen Relationen für die Automorphismen I, J und $K := IJ$:

$$I^2 = J^2 = K^2 = IJK = \iota, \iota^2 = \mathrm{id}.$$

Die von I und J erzeugte Gruppe ist daher die Quaternionengruppe Q_8, die wegen ihrer Mächtigkeit bereits mit $\mathrm{Gal}(L/\mathbb{Q})$ übereinstimmen muss. □