universität
wien

DIPLOMARBEIT

Titel der Diplomarbeit

„Galoistheorie und Konstruktion mit Zirkel und Lineal“

Verfasser

Christian Dorner

angestrebter akademischer Grad

Magister der Naturwissenschaften (Mag.rer.nat)

Wien, im Februar 2012

Studienkennzahl lt. Studienblatt:	A 190 406 456
Studienrichtung lt. Studienblatt:	Mathematik und Geographie und Wirtschaftskunde
Betreuer:	ao. Univ.-Prof. Dr. Karl Auinger

Vorwort

So revolutionär der mathematische Inhalt der Galoistheorie war, so sagenumwoben ist auch die Person des Évariste Galois. Er war der Erste, der eine Sprache beherrschte, die bis heute verwendet wird. Nur zu seinen Lebzeiten wurde er für seine Entdeckung nicht gewürdigt. Allgemein hatte Galois kein Glück in seinem Leben. Hinzu kommt noch sein Charakter, der alles andere als angenehm beschrieben wird. Évariste wurde, bis er 12 Jahre alt war, von seiner Mutter unterrichtet und kam anschließend in das Lycée „Louis-le-Grand“. Seinen Lehrern fiel immer wieder die mathematische Begabung auf, jedoch auch sein bizarrer Charakter. Er beschloss, sich im Alter von 16 Jahren am „École Polytechnique“, eine der renommiertesten Hochschulen Europas, zu bewerben. Die Aufnahmeprüfung schaffte er jedoch nicht. Galois war aber davon überzeugt, dass er in einem zweiten und letzten Versuch die Examen bestehen werde. Kurz vor seinem letzten Antritt beging sein Vater Selbstmord, was ihn zu tiefst erschüttert hat. Bei der Prüfung verhielt er sich dermaßen respektlos gegenüber den beiden Professoren, die die Prüfung abnahmen, dass er abermals nicht aufgenommen wurde. Sein Traum, sich an der „École Polytechnique“ einzuschreiben, platzte und er musste sich mit der „École Préparatoire“ zufrieden geben.
Évariste Galois versuchte auch außerhalb der Schule auf sich aufmerksam zu machen und wollte Professor Chauchy ein Manuskript von ihm übergeben. Genau genommen war das eine ziemlich wagemutige Aktion, denn Chauchy hatte den Ruf, nur seine eigenen Arbeiten zu verbreiten, und für andere soll er nicht viel übrig gehabt haben. Doch irgendwie schien Chauchy an der Arbeit gefallen zu finden und wollte sie sogar präsentieren. Der berühmte Professor erkrankte am Tag der Präsentation und in der nächsten Sitzung erstatte er nur über seine Arbeit Bericht. Galois gab nicht auf und versuchte es erneut, diesmal gelangte sein Skript in die Hände von Fourier, der aber kurz nach Erhalt verstarb und das Manuskript verschwand erneut.
Geprägt von der politischen Ideologie seines Vaters begab er sich immer wieder in gefährliche Situationen, sodass er schlussendlich von der Hochschule „École Prépartoire“ verwiesen wurde und sogar im Gefängnis landete. Dort überarbeitete er seine Gedanken in Ruhe und ohne Ablenkung nochmals. Als Évariste wieder frei war, verliebte er sich in die Tochter eines Arztes. In den Geschichtsbüchern stirbt Galois aufgrund eines Duells mit dem Liebhaber seiner Geliebten. Jedoch bezweifeln einige, dass das der wahre Grund seines Todes ist. Eines steht jedoch fest: in einem Brief an seinen Freund versuchte er so nachvollziehbar wie möglich seine Entdeckung niederzuschreiben. Er beendete den Brief mit der Aufforderung diesen Inhalt Gauß oder Jacobi vorzulegen, diese sollten nicht die Richtigkeit sondern die Bedeutung seiner

Entdeckung beurteilen.
Aufgrund der faszinierenden Geschichte über das Leben von Évariste Galois aus dem Buch „Geheimnis der Symmetrie“ von Marcus du Sautoy (vgl. [10], S. 200ff) wollte ich mich näher dem mathematischen Inhalt seiner Entdeckung hingeben, wodurch diese Arbeit entstand.

Danksagung

An dieser Stelle möchte ich mich für die fachliche Betreuung bei ao.Univ.-Prof. Dr. Karl Auinger bedanken.
Der größte Dank gilt meinen Eltern, ohne deren finanzielle und mentale Unterstützung mein Studium nicht möglich gewesen wäre.

Inhaltsverzeichnis

1 Körpererweiterungen

Zu Beginn der Arbeit werden eine Fülle an Definitionen und Begrifflichkeiten eingeführt. Dabei werden vorerst allgemeine Körpererweiterungen behandelt. Gleich das erste Resultat, der Gradsatz, ist von zentraler Bedeutung für die ganze Arbeit, dadurch lassen sich Methoden der linearen Algebra verwenden. Anschließend werden besondere Körpererweiterungen betrachtet, im Fokus stehen dabei die algebraischen Körpererweiterungen. In diesem Kapitel richte ich mich nach den Büchern: „Algebra“ von M. Artin (Kapitel 13, [2]), „Galoissche Theorie“ von E. Artin (Kapitel 2, [1]), „Algebra“ von Jantzen und Schwermer (Kapitel V §1,2,3, [7]) sowie „Algebra“ von Karpfinger und Meyberg (Kapitel 19, 20, [9]).

Definition 1. Sei K ein Teilkörper des Köpers L, man nennt L einen *Erweiterungskörper* von K und spricht von der *Körpererweiterung* L/K.

Beispiel 1. Es ist $\mathbb{Q}$ ein Teilkörper von $\mathbb{R}$ und von $\mathbb{C}$, so sind $\mathbb{R}/\mathbb{Q}$ und $\mathbb{C}/\mathbb{Q}$ Körpererweiterungen.

Definition 2. Sei L/K eine Körpererweiterung und $M \subseteq L$, dann bezeichnet $K[M]$ den kleinsten Teilring von L, der K und M enthält.

Definition 3. Sei M eine Teilmenge des Köpers L, man nennt den kleinsten Teilkörper von L der M umfasst, *den von M erzeugten Teilkörper*. Bei einer gegebenen Köpererweiterung L/K wird der kleinste Teilkörper von L, der $K \cup M$ enthält mit $K(M)$ bezeichnet, man sagt: $K(M)$ ensteht durch *Adjunktion* von M aus K. Enthält M nur endlich viele Elemente $a_1, \ldots, a_n \in L$, so schreibt man $K(M) = K(a_1, \ldots, a_n)$. Die Körpererweiterung L/K wird *endlich erzeugbar* genannt, wenn es endlich viele Elmente $a_1, \ldots, a_n \in L$ gibt, sodass $L = K(a_1, \ldots, a_n)$ ist. Die Erweiterung L/K heißt *einfach*, falls es ein Element $a \in L$ existiert mit $L = K(a)$, das Element a wird *primitives Element* genannt.

Bemerkung. Im Zuge dieser Notation bezeichnet man für einen Körper K:

1. $K[X]$ den Ring der Polynome über K.
2. $K(X)$ den Quotientenkörper von $K[X]$ und man nennt ihn den Körper der rationalen Funktionen über K.

Beispiel 2. Sei K ein Körper, dann ist $K(X)/K$ eine Körpererweiterung.

Definition 4. Es heißt Z ein Zwischenkörper von L/K, wenn Z ein K umfassender Teilkörper von L ist, $K \subseteq Z \subseteq L$.

Beispiel 3.

Der Körper $\mathbb{R}$ ist ein Zwischenkörper von $\mathbb{C}/\mathbb{Q}$.

Sei K ein Körper und $n \in \mathbb{N}$, dann ist $K(X^n)$ ein Zwischenkörper von $K(X)/K$ für jedes beliebige $n \in \mathbb{N}$.

Aus folgender wichtiger Beobachtung lässt sich ein grundlegendes und äußerst wichtiges Resultat zeigen. Sei L/K eine Körpererweiterung, so kann man L als einen Vektorraum über dem Körper K auffassen. Als Addition wird die Addition in L benutzt. Die Skalare sind die Elemente c aus K und das Produkt ca mit $a \in L$ stellt die Skalarmultiplikation dar. Dadurch lassen sich Methoden der Linearen Algebra anwenden.

Definition 5. Sei L/K eine Körpererweiterung, dann heißt die Dimension $dim_K L$ dieses Vektorraums über K *der Grad der Körpererweiterung* L/K, man schreibt $[L : K] := dim_K L$. Die Erweiterung L/K wird endlich genannt, wenn $[L : K]$ endlich ist, also wenn $[L : K] \in \mathbb{N}$.

Beispiel 4.

Wir betrachten die Körpererweiterung $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$. Nach Definition 3 ist $\mathbb{Q}(\sqrt{2})$ der kleinste Körper der $\mathbb{Q} \cup \sqrt{2}$ enthält. Es lassen sich daher folgende Elemente bilden: ein einfaches Element a aus $\mathbb{Q}$ und ein Element b aus $\mathbb{Q}$ multipliziert mit $\sqrt{2}$, also $b\sqrt{2}$. Diese beiden kann man noch addieren und multiplizieren. Wir erhalten jedoch immer ein Element der Form $a + b\sqrt{2}$. Das Inverse Element bezüglich der Addition hat die Form $-a - b\sqrt{2}$ und das inverse Element bezüglich der Multiplikation hat die Form $c + d\sqrt{2}$, wobei $c = \frac{a}{a^2-2b^2} \in \mathbb{Q}$ und $d = \frac{-b}{a^2-2b^2} \in \mathbb{Q}$ (der Nenner ist verschieden von 0, denn $a^2 - 2b^2 = 0$ ist äquivalent zu $a = \pm b\sqrt{2} \notin \mathbb{Q}$ oder $b = \pm\frac{a\sqrt{2}}{2} \notin \mathbb{Q}$). Es gilt nun $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$. Wir zeigen nun, dass $\{1, \sqrt{2}\}$ eine Basis von $\mathbb{Q}(\sqrt{2})$ über $\mathbb{Q}$ ist. Sei c ein beliebiges Element aus $\mathbb{Q}(\sqrt{2})$. Wenn $c \in \mathbb{Q}$ liegt, dann gilt $c = c \cdot 1 + 0 \cdot \sqrt{2}$. Sei nun $c \in \mathbb{Q}(\sqrt{2}) \setminus \mathbb{Q}$, dann folgt. Nach Definition ist c der Form $c = a + b\sqrt{2}$ mit $a, b \in \mathbb{Q}$, daraus folgt $c = a \cdot 1 + b \cdot \sqrt{2}$. Also ist die Menge $\{1, \sqrt{2}\}$ ein Erzeugendensystem. Es bleibt noch die lineare Unabhängigkeit zu zeigen. Angenommen $\{1, \sqrt{2}\}$ sind linear abhängig, dann existieren $\lambda_1 \in \mathbb{Q}$ und $\lambda_2 \in \mathbb{Q}$ nicht beide verschieden Null, sodass $\lambda_1 \cdot 1 + \lambda_2 \cdot \sqrt{2} = 0$ folgt. Für ein $\lambda_2 \neq 0$, gilt dann $\frac{-\lambda_1}{\lambda_2} = \sqrt{2}$. Das ist ein Widerspruch zu $\lambda_1, \lambda_2 \in \mathbb{Q}$. Also ist $\{1, \sqrt{2}\}$ linear unabhängig und daher eine Basis. Aus den vorigen Überlegungen lässt sich der Grad der Körpererweiterung $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ bestimmen, es gilt $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$.

Satz 1.1 (Gradsatz)**.** Sei Z ein Zwischenkörper der Körpererweiterung L/K, dann gilt:

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

Beweis. Sei $(v_i)_{i\in I}$ eine Basis von L über Z und $(w_j)_{j\in J}$ eine Basis von Z über K, also ist $[L : Z] = |I|$ und $[Z : K] = |J|$. Zu zeigen ist, dass $(w_j v_i)_{(i,j)\in J\times I}$ eine Basis von L über K ist. Bei den im Beweis auftretenden Summen sind nur endlich viele Summanden verschieden von 0. Zuerst wird bewiesen, dass es sich dabei um ein Erzeugendensystem handelt. Sei $a \in L$ beliebig, dann lässt sich $a = \sum_{i\in I} z_i v_i$ mit $z_i \in Z$ darstellen, da $(v_i)_{i\in I}$ eine Basis von L über Z ist. Wir benützen jetzt die Basis $(w_j)_{j\in J}$, denn durch sie hat jedes z_i die Form $z_i = \sum_{j\in J} k_{ij} w_j$ mit $k_{ij} \in K$, daraus ergibt sich $a = \sum_{(i,j)\in I\times J} k_{ij} w_j v_i$. Es bleibt die lineare Unabhängigkeit zu beweisen:
Seien $k_{ij} \in K$ mit $\sum_{(i,j)\in I\times J} k_{ij} w_j v_i = 0$. Wir müssen zeigen, dass alle $k_{ij} = 0$ sind. Durch das Umschreiben der obigen Summe erhält man $\sum_{i\in I}(\sum_{j\in J} k_{ij} w_j) v_i = 0$. Da $(v_i)_{i\in I}$ eine Basis über L ist, folgt dass für jedes $i \in I$ die Summe $\sum_{j\in J} k_{ij} w_j = 0$ sein muss, es ist auch w_j eine Basis und daraus ergibt sich $k_{ij} = 0$ für alle $i \in I$ und $j \in J$. Es wurde nun gezeigt, dass $(w_j v_i)_{(i,j)\in J\times I}$ ein linear unabhängiges Erzeugendensystem von L über K ist und daher eine Basis von L über K und es gilt $|J \times I| = |J|\cdot|I| = [L : K]$. □

Korollar 1.2. Sei L/K eine endliche Körpererweiterung, dann gilt für einen Zwischenkörper Z von L/K, dass $[Z : K]$ ein Teiler von $[L : K]$ ist.

Beweis. Nach Satz 1.1 gilt $[L : K] = [L : Z] \cdot [Z : K]$, daraus folgt die Behauptung. □

Definition 6. Sei L/K eine Körpererweiterung, ein Element $a \in L$ heißt *algebraisch über* K, wenn a eine Nullstelle eines Polynoms $P \neq 0$ mit Koeffizienten in K ist, also $P \in K[X]$.

Beispiel 5.

Sei L/K eine Körpererweiterung, dann gilt für jedes Element $k \in K$, dass k algebraisch über K ist, da k immer Nullstelle des Polynoms $X - k \in K[X]$ ist.

Wir betrachten die Körpererweiterung $\mathbb{C}/\mathbb{Q}$, so ist i algebraisch über $\mathbb{Q}$, da das Polynom $P = X^2 + 1$ nur Koeffizienten aus $\mathbb{Q}$ hat, es gilt $P \in \mathbb{Q}[X]$.

Es ist die n-te Einheitswurzel $e^{\frac{2\pi i}{n}}$ algebraisch über $\mathbb{Q}$, da $X^n - 1 \in \mathbb{Q}[X]$.

Korollar 1.3. Sei L/K eine Körpererweiterung und $a \in L$ algebraisch über K, dann ist der Kern des Einsetzungshomomorphismus $\epsilon_a : K[X] \to L$, $P \mapsto P(a)$ nicht trivial.

Beweis. Da a algebraisch über K ist, existiert mindestens ein Polynom $P \in K[X]$, wobei $P \neq 0$, sodass $P(a) = 0$. □

Für die fortschreitenden Betrachtungen ist die Menge der Polynome, die bei dem obigen Einsetzhomomorphismus im Kern liegen, von großem Interesse. Aus allen im Kern liegenden Polynome wählen wir eines von kleinsten Grade aus und multiplizieren es mit einer Konstanten aus dem Körper K, sodass der höchste Koeffizient 1_K ist und nennen es vorerst P.

Lemma 1.4. Das oben beschriebene Polynom $P \in K[X]$ erfüllt folgende Eigenschaften

1. Für alle $G \in K[X]$ mit $G(a) = 0$ gilt $P \mid G$.
2. P ist irreduzibel.
3. P ist durch seine Konstruktion eindeutig bestimmt.

Beweis.

1. Sei $G \in K[X]$, dann lässt sich G folgendermaßen schreiben $G = P \cdot Q + R$, wobei der Grad von R kleiner ist als der Grad von P. Das Einsetzen von a führt dazu, dass $R(a) = 0$ sein muss, da $G(a) = 0$ ist. Nun hat das Polynom R die Nullstelle a, nach Konstruktion von P folgt, dass $R = 0$ ist, da P ja das Polynom kleinsten Grades mit Nullstelle a ist. Es gilt $G = P \cdot Q$, also $P \mid G$.
2. Angenommen P ist reduzibel, so zerfällt P in ein Produkt $P = Q \cdot G$ mit $Q, G \in K[X]$, wobei Q und G keine Einheiten von $K[X]$ sind. Aus $P = Q \cdot G$ folgt, dass Q oder G a als Nullstelle hat. $O.B.d.A$ sei $Q(a) = 0$ und Q hat kleineren Grad als P, das steht im Widerspruch zu der Konstruktion von P.
3. Angenommen es gibt ein $P_2 \in K[X]$ mit den selben Eigenschaften wie P. Insbesondere gilt auch Punkt 1 für P und P_2. Einerseits ist $P_2(a) = 0$ und daher $P \mid P_2$, andererseits gilt aber auch $P_2 \mid P$, da $P(a) = 0$. Daraus folgt $P = P_2$.

□

Definition 7. Das Polynom P nach der obigen Konstruktion heißt *Minimalpolynom von a über K* und wird mit $m_{a,K}$ bezeichnet.

Beispiel 6.

Gesucht ist das Minimalpolynom von $a = \frac{1+\sqrt{5}}{2}$ über $\mathbb{Q}$. Es gilt $a^2 = \frac{3+\sqrt{5}}{2}$, daraus folgt, dass $a^2 - a = \frac{3+\sqrt{5}}{2} - \frac{1+\sqrt{5}}{2} = 1$ ist. Also gilt $a^2 - a - 1 = 0$, darauf erstellen wir das Polynom $P = X^2 - X - 1$. Es ist normiert, nach

dem Kriterium von Eisenstein (mit einer Verschiebung $P(2X-1)$ und dann $p=3$) irreduzibel und hat a als Nullstelle. Aufgrund von Korollar 1.4 ist das Minimalpolynom eindeutig, dass bedeutet $P = m_{a,\mathbb{Q}}$.

Der Grad des Minimalpolynoms eines Elements über $\mathbb{Q}$ muss nicht immer zweiten Grades sein. Wir betrachten das Element $a = \sqrt{2}+\sqrt{3}$ und suchen das dazugehörige Minimalpolynom über $\mathbb{Q}$. In diesem Fall gilt $a^2 = 2\sqrt{6}+5$ und $a^4 = 20\sqrt{6}+49$, daraus ergibt sich $a^4-10a^2 = -1$, also $a^4-10a^2+1 = 0$. Wir erstellen auf diesem Ergebnis das Polynom $R = X^4-10X^2+1$, dann hat R folgende Eigenschaften. Es ist normiert, wiederum nach dem Kriterium von Eisenstein mit $p=2$ irreduzibel, hat a als Nullstelle und $R \in \mathbb{Q}[X]$. Somit ist $R = m_{a,\mathbb{Q}}$.

Satz 1.5. Sei L/K eine Körpererweiterung, $a \in L$ algebraisch über K und $m_{a,K}$ das zugehörige Minimalpolynom, so gilt $K[X]/(m_{a,K}) \cong K[a]$ und $K[a]$ ist ein Körper, daher gilt $K[a] = K(a)$.

Beweis. Wir verwenden zu diesem Beweis den Einsetzhomomorphismus aus 1.3. $K[X]$ ist ein Hauptidealring, da K ein Körper ist, aus diesem Grund wird der Kern der Abbildung ϵ_a, der ein Ideal von $K[X]$ ist, von nur einem einzigen Element erzeugt. Es gilt, $P \in K[X]$ ist irreduzibel genau dann wenn (P) maximal in der Menge der Hauptideale ist. Es liegt $m_{a,K} \in kern\ \epsilon_a$, nach Satz 1.4 ist $m_{a,K}$ irreduzibel und daher ist das von dem Minimalpolynom erzeugte Ideal maximal in $K[X]$, das heißt $(m_{a,K}) = kern\ \epsilon_a$. Der Kern von ϵ_a ist verschieden von $K[X]$, da die konstanten Polynome aus $K[X]$ nicht im Kern von ϵ_a liegen. Daraus folgt, dass $K[X]/(m_{a,K})$ ein Körper ist und nach dem Homomorphiesatz ismorph zum $im\ \epsilon_a$. Daraus ergibt sich, dass $K[a]$ ein Körper ist. Aus der Definition von $K(a)$ folgt, $K[a] = K(a)$. □

Satz 1.6. Sei L/K eine Körpererweiterung und $a \in L$ algebraisch über K mit dem Minimalpolynom $m_{a,K}$, dessen Grad n ist, so gilt $n = [K(a) : K]$.

Beweis. Die Aussage gilt, wenn gezeigt wird, dass $\{1, a, a^2, \ldots, a^{n-1}\}$ eine Basis von $K(a)$ ist. Es ist zu zeigen, dass die angebene Menge ein k-linear unabhängiges Erzeugendensystem von $K(a)$ darstellt. Seien $k_0, \ldots, k_{n-1} \in K$ mit $\sum_{i=0}^{n-1} k_i a^i = 0$, wir müssen zeigen, dass $k_0 = k_1 = \ldots = k_{n-1} = 0$. Wir betrachten das Polynom $Q = \sum_{i=0}^{n-1} k_i X^i$, dann gilt $degQ < n$ und $Q(a) = 0$. Nach Lemma 1.4 gilt $m_{a,K} \mid Q$ wegen $deg\ m_{a,K} = n$ folgt $Q = 0$, also ist Q das Nullpolynom. Aus diesem Grund sind $k_0 = k_1 = \ldots = k_{n-1} = 0$, das heißt $\{1, a, a^2, \ldots, a^{n-1}\}$ ist linear unabhängig.
Sei $v \in K(a)$ beliebig. Nach Satz 1.5 hat v die Form $v = P(a)$, für ein $P \in K[X]$. Wir dividieren P durch $m_{a,K}$ mit Rest und erhalten die Darstellung $P = S \cdot m_{a,K} + R$ für gewisse $S, R \in K[X]$ mit $degR < 0$. Das Einsetzen von

a führt zu $v = P(a) = S(a) \cdot 0 + R(a)$, wobei $R(a)$ die Form $\sum_{i=0}^{n-1} k_i a^i$ hat, mit $k_i \in K$ für $i \in \{0, \ldots, n-1\}$. Somit wurde gezeigt, dass $1, a, a^2, \ldots, a^{n-1}$ ein Erzeugendensystem und eine Basis ist. □

Beispiel 7.

Die Körpererweiterung $\mathbb{Q}(\frac{1+\sqrt{5}}{2})/\mathbb{Q}$ hat den Grad 2, denn in Beispiel 6 wurde gezeigt $deg\ m_{\frac{1+\sqrt{5}}{2},\mathbb{Q}} = 2$, also folgt nach Satz 1.6, dass $[\mathbb{Q}(\frac{1+\sqrt{5}}{2}) : \mathbb{Q}] = 2$.

Aufgrund von Beispiel 6 und Satz 1.6 hat die Körpererweiterung $\mathbb{Q}(\sqrt{2} + \sqrt{3})/\mathbb{Q}$ den Grad 4.

Definition 8. Eine Körpererweiterung L/K heißt algebraisch, wenn jedes $a \in L$ algebraisch über K ist.

Satz 1.7. Sei L/K eine Köpererweiterung, wenn L/K endlich ist, dann ist L/K auch algebraisch

Beweis. Sei L/K endlich, also $[L : K] = n$ für ein $n \in \mathbb{N}$. Sei $a \in L$ beliebig, dann sind die $n+1$ Elemente $1, a, \ldots, a^n$ linear abhängig. Es existieren daher $k_0, k_1, \ldots, k_n \in K$ nicht alle gleich 0, sodass $k_0 + k_1 a + \cdots + k_n a^n = 0$. Das Element a ist also eine Nullstelle des Polynoms $P = \sum_{i=0}^{n} k_i X^i$, wobei $P \neq 0$. Es ist a algebraisch über K. □

Bemerkung. Der Satz 1.7 stimmt nur in die eine Richtung, die Umkehrung gilt im Allgemeinen nicht. Für ein Gegenbeispiel greife ich jetzt etwas voraus. Wir verwenden dazu den erst in Lemma 7.2 eingeführten Teilkörper $\mathcal{K}(S)$ von $\mathbb{C}$, wobei $S = \{0, 1\}$. Man betrachte nun die Körpererweiterung $\mathcal{K}(S)/\mathbb{Q}$. Zu jedem $z \in \mathcal{K}(S)$ existiert eine Körperkette $\mathbb{Q} = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_n$ mit $[K_i : K_{i-1}] = 2$ und $z \in K_n$, daher ist die Körpererweiterung algebraisch. Zu jedem Element z in $\mathcal{K}(S)$ ist auch die Wurzel von z in $\mathcal{K}(S)$. Es liegen also $2, \sqrt{2}, \sqrt{\sqrt{2}}, \sqrt{\sqrt{\sqrt{2}}}, \ldots$ in $\mathcal{K}(S)$, dadurch ist die Körpererweiterung unendlich. Wir haben mit $\mathcal{K}(S)/\mathbb{Q}$ eine algebraische, aber unendliche Körpererweiterung gefunden.

Satz 1.8. Eine Körpererweiterung L/K ist genau dann endlich, wenn es endlich viele über K algebraische Elemente $a_1, \ldots, a_n \in L$ mit $L = K(a_1, \ldots, a_n)$ gibt.

Beweis. ($\Rightarrow$) Sei L/K endlich mit $n = [L : K]$. Nach der Definition 5 folgt, dass es eine K-Basis aus n Elementen von L geben muss. Sei nun $\{a_1, \ldots, a_n\}$ so eine Basis. Nach Satz 1.7 sind a_i mit $i \in \{1, \ldots, n\}$ algebraisch über K, daraus folgt $L = K(a_1, \ldots, a_n)$.
($\Leftarrow$) Sei $L = K(a_1, \ldots, a_n)$, wobei a_i mit $i \in \{1, \ldots, n\}$ algebraisch über K

ist. Der Beweis folgt mit Induktion nach n. Für den Induktionsanfang sei $n = 1$, dann gilt nach Satz 1.6 für $L = K(a_1)$, dass $[K(a_1) : K] = deg\ m_{a,K}$ ist. Also ist in diesem Fall L/K endlich. Für den Induktionsschritt soll die Aussage für $n-1$ gelten. Aus der Definition 3 folgt $L = K(a_1, \ldots, a_{n-1}, a_n) = K(a_1, \ldots, a_{n-1})(a_n)$ nach dem Satz 1.1 gilt:

$$[L : K] = [K(a_1, \ldots, a_{n-1})(a_n) : K] =$$

$$\underbrace{[K(a_1, \ldots, a_{n-1})(a_n) : K(a_1, \ldots, a_{n-1})]}_{wegen\ Satz\ 1.6\ endlich} \underbrace{[K(a_1, \ldots, a_{n-1}) : K]}_{nach\ Voraussetzung\ endlich}.$$

Die Aussage gilt nun auch für n Elemente und aus der Induktion folgt die Behauptung. □

Satz 1.9. Seien L/E und E/K algebraische Körpererweiterungen, $K \subseteq E \subseteq L$, dann ist auch L/K eine algebraische Körpererweiterung.

Beweis. Es genügt für ein beliebiges $a \in L$ zu zeigen: Wenn a über E algebraisch ist, dann ist a auch über K algebraisch. Nach Voraussetzung existiert ein Polynom $0 \neq P \in E[X]$ mit $P(a) = 0$, das heißt $P(a) = \sum_{i=0}^{n} e_i a^i = 0$ mit $e_i \in E$ für alle $i \in \{1, \ldots, n\}$. Nun gilt, dass a algebraisch über dem Körper $K(e_1, \ldots, e_n)$ ist. Die Elemente $e_1, \ldots, e_n$ sind algebraisch über K, da E/K eine algebraische Körpererweiterung ist. Aus dem Satz 1.1 folgt

$$\begin{aligned}[K(a) : K] &\leq [K(e_1, \ldots, e_n, a) : K] \\ &= \underbrace{[K(e_1, \ldots, e_n)(a) : K(e_1, \ldots, e_n)]}_{nach\ Satz\ 1.8\ endlich} \underbrace{[K(e_1, \ldots, e_n) : K]}_{nach\ Satz\ 1.8\ endlich} \in \mathbb{N}.\end{aligned}$$

Die Körpererweiterung $K(a)/K$ ist nun endlich und nach Satz 1.7 algebraisch, somit ist a algebraisch über K. Da a beliebig in L war, folgt die Aussage für die ganze Köpererweiterung L/K. □

2 Algebraischer Abschluss

Es stellt sich die Frage, ob man immer Erweiterungen zu einem Körper K finden kann, die Nullstellen von bestimmten Polynomen aus $K[X]$ enthalten. Wir betrachten das Polynom $X^2 + 1 \in \mathbb{Q}[X]$, so hat es in $\mathbb{Q}$ und $\mathbb{R}$ keine Nullstellen, jedoch in $\mathbb{C}$ erhält man i und $-i$. In diesem Beispiel erscheint es relativ einfach die richtige Körpererweiterung zu finden, im Allgemeinen muss das erst gezeigt werden. Das Ziel dieses Abschnitts ist es zu zeigen, dass es für jeden beliebigen Körper K einen Erweiterungskörper gibt, sodass jedes Polynom aus $K[X]$ in dieser Erweiterung in Linearfaktoren zerfällt. Dieses äußerst wichtige Resultat bedarf einiger Vorarbeit und Resultaten aus der Mengenlehre, wie das Lemma von Zorn. Letztere werden in dieser Arbeit ohne Beweis als Satz bzw. Lemma formuliert. Der Abschnitt beginnt mit der wichtigen Aussage, dass es zu jedem Polynom $P \in K[X]$ mit $degP \geq 1$ einen Erweiterungskörper L von K gibt, der eine Nullstelle von P enthält. In diesem Kapitel richte ich mich nach den Büchern „Algebra“ von Karpfinger und Meyberg (Kapitel 23, Anhang A, [9]), sowie „Algebra“ von Jantzen und Schwermer (Kapitel V §3,4, [7]).

Satz 2.1. Sei K ein Körper und $P \in K[X]$ ein irreduzibles Polynom mit $degP \geq 1$, dann existiert ein Erweiterungskörper L von K, der eine Nullstelle von P enthält. Es gilt $[L : K] = degP$.

Beweis. Sei $P \in K[X]$ irreduzibel, dann folgt, dass das von P erzeugte Ideal (P) ein maximales ist. Daraus ergibt sich, dass $L = K[X]/(P)$ ein Körper ist. Wir erstellen nun den Restklassenhomomorphismus $\pi : K[X] \to L$ mit $X \mapsto X+(P)$. Schränkt man π auf K ein, dann erhält man einen Homomorphismus $\pi_{|K} : K \to L$, also $k \mapsto k + (P)$. Dieser Homomorphismus $\pi_{|K}$ bildet K injektiv in L ab, da P nach Voraussetzung nicht konstant ist und daher 0_K das einzige Element in K ist, das auf $0_L = (P)$ abgebildet wird. Aus diesem Grund kann jedes Element $u \in K$ mit $\pi_{|K}(u) = u + (P)$ identifiziert werden. Mit dieser Sichtweise kann K als Teilkörper von L angesehen werden.
Sei nun $a := X + (P) \in L$ und $P = \sum_{i=0}^{n} k_i X^i \in K[X]$ mit $k_i \in K$ für alle $i \in \{0, \ldots, n\}$. Da K ein Teilkörper von L ist, gilt auch $k_i \in L$ für alle $i \in \{0, \ldots, n\}$, somit lässt sich P als Polynom über L auffassen und es gilt:

$$P(a) = \sum_{i=0}^{n} k_i (X + (P))^i = \sum_{i=0}^{n} k_i X^i + (P) = P + (P) = 0 + (P) = 0_L.$$

Somit ist a eine Nullstelle von P als Polynom über L. Es folgt aus der Irreduzibilität von P, dass es bis auf einen konstanten Faktor mit $m_{a,K}$ übereinstimmt. Da $\sum_{i=0}^{n} k_i X^i + (P) = \sum_{i=0}^{n} k_i a^i$ ist, gilt $L = K(a)$. Aus dem Satz 1.6 folgt dann $[L : K] = degP$. □

Die eben gezeigte Aussage lässt sich im nächsten Korrollar noch ein wenig verallgemeinern:

Korollar 2.2. Sei P ein beliebiges Polynom aus $K[X]$ mit $deg \geq 1$, dann existiert ein Erweiterungskörper L von K mit $[L : K] \leq degP$, der eine Nullstelle von P enthält.

Beweis. Sei $P \in K[X]$ ein beliebiges nichtkonstantes Polynom, so kann man P als Produkt von irreduzible Faktoren darstellen $P = G_1 \cdots G_n$ mit $G_i \in K[X]$ für alle $i \in \{1, \ldots, n\}$. Nun kann auf ein G_i der Satz 2.1 angewendet werden. Der liefert einen Erweiterungskörper von K, wo G_i und somit P eine Nullstelle haben. Es gilt $degP \geq degG_i = [L : K]$. □

Es folgt die grundlegende Definition für diesen Abschnitt und einige Eigenschaften, die später benötigt werden.

Definition 9. Ein Körper K heißt *algebraisch abgeschlossen*, falls jedes nichtkonstante Polynom $P \in K[X]$ eine Nullstelle in K hat.

Beispiel 8. Ein typisches Beispiel für einen algebraisch abgeschlossenen Körper ist $\mathbb{C}$. Die Eigenschaft geht aus dem Fundamentalsatz der Algebra hervor.

Definition 10. Ein Polynom $P \in K[X]$ *zerfällt* über dem Körper K, wenn sich P in ein Produkt von Linearfaktoren zerlegen lässt, das heißt wenn $c, a_1, \ldots, a_n \in K$ existieren, sodass $P = c(X - a_1) \ldots (X - a_n)$.

Beispiel 9.

Das Polynom $X^2 + 1$ aus der Einleitung zerfällt über $\mathbb{C}$ in das Polynom $(X + i)(X - i) \in \mathbb{C}[X]$.

Betrachte $X^2 - 2 \in \mathbb{Q}[X]$, so zerfällt dieses nicht über $\mathbb{Q}$. Durch die Adjunktion von $\sqrt{2}$ an $\mathbb{Q}$ erhält man den Körper $\mathbb{Q}(\sqrt{2})$, darüber zerfällt das Polynom P in $(X + \sqrt{2})(X - \sqrt{2})$.

Lemma 2.3. Sei K ein Körper und $P \in K[X]$ mit $degP = n > 1$, dann gilt: $P(a) = 0$ genau dann wenn $P = (X - a)Q$ für ein $Q \in K[X]$ mit $degQ = n - 1$.

Beweis. ($\Rightarrow$) Wenn $P(a) = 0$ gilt, können wir P schreiben als $P = (X - a)Q + R$ mit $Q, R \in K[X]$ und $degR < deg(X - a) = 1$. Wenn $R = c \neq 0$ wäre, würde $0 = P(a) = (a-a)Q+c = c$ folgen, also ein Widerspruch! Somit ist $R = 0$.
($\Leftarrow$) Sei P der Form $P = (X - a)Q$, dann gilt $P(a) = (a - a)Q = 0$. □

Bemerkung. Wegen der Eigenschaft der Gradfunktion $deg((X-a)Q) = deg(X-a) + degQ$ gilt $degQ = degP - 1$.

Lemma 2.4 (Charakterisierung algebraisch abgeschlossner Körper)**.** Ein Körper K ist algebraisch abgeschlossen, falls er eine der folgenden Bedingungen erfüllt:

1. Jedes Polynom $P \in K[X]$ zerfällt über K.
2. Wenn für jedes irreduzible Polynom $P \in K[X]$ gilt, $degP = 1$.
3. Für jede algebraische Erweiterung L/K gilt $L = K$.
4. Es existiert kein Erweiterungskörper $L \neq K$ von K mit $[L : K] \in \mathbb{N}$.

Beweis. Wir zeigen zuerst, dass ein algebraisch abgeschlossener Körper (1) erfüllt und anschließend, dass die Behauptungen äquivalent sind.
Sei K algebraisch abgeschlossen und $P \in K[X]$ ein nichtkonstantes Polynom mit $degP = n$ und *o.B.d.A.* sei $n > 1$. Nach Definition 9, gibt es eine Nullstelle $a \in K$, sodass $P(a) = 0$. Nach Satz 2.3 gilt, dass $P = (X-a)Q$ für ein $Q \in K[X]$ mit $degQ = n - 1$. Wiederhole nun das Argument mit dem Polynom Q und iteriere das Verfahren $n-2$-mal. Somit zerfällt P über K.
(1)⇒(2) Wenn P über K zerfällt, dann existieren nach Definition 10 Elemente $c, a_1, \ldots, a_n \in K$ sodass $P = c(X-a_1)\cdots(X-a_n)$. Jeder dieser Faktoren $(X-a_i)$ mit $i \in \{1, \ldots, n\}$ hat einen Grad von eins.
(2)⇒(3) Sei L eine algebraische Erweiterung von K und $a \in L$ beliebig. Da a algebraisch über K und das Minimalpolynom von a über K irreduzibel ist, gilt nach Voraussetzung $m_{a,K} = X - a$, daraus folgt aber, dass $a \in K$ ist. Aus der Beliebigkeit von a folgt die Behauptung $L = K$.
(3)⇒(4) Nach Voraussetzung gilt, dass es keinen über K algebraischen Erweiterungskörper $L \neq K$ gibt. Der Satz 1.7 besagt, dass jede endliche Erweiterung algebraisch ist. Aus der Verneinung dieser Implikation und aus der Voraussetzung folgen, dass es keinen Erweiterungskörper L mit $[L : K] \in \mathbb{N}$ gibt.
Um den Kreis zu schließen muss noch gezeigt werden, dass die Bedingung (4) impliziert, dass K algebraisch abgeschlossen ist.
Sei $P \in K[X]$ ein nichtkonstantes Polynom. Aufgrund von Korollar 2.2 existiert ein Erweiterungskörper von K, in dem P eine Nullstelle hat. Sei a eine solche Nullstelle. Nach Satz 1.6 ist die Körpererweiterung $K(a)/K$ endlich und nach der Voraussetzung gilt nun $K(a) = K$ und daher $a \in K$. Da das für jede Nullstelle von einem beliebigen Polynom P in $K[X]$ gilt, folgt die algebraische Abgeschlossenheit. □

Für den Satz von Steinitz, der besagt, dass jeder Körper einen algebraischen Abschluss besitzt, ist etwas Vorarbeit nötig. Dazu benötigt man eine Reihe von Definitionen und das Lemma von Zorn.

Definition 11. Sei M eine Menge und $\leq$ eine zweistellige Relation, $(M, \leq)$ heißt *geordnete Menge*, wenn folgende Eigenschaften erfüllt sind:

1. Für alle $x \in M : x \leq x$ (reflexiv).
2. Für alle $x, y, z \in M$ mit $x \leq y \wedge y \leq z \Rightarrow x \leq z$ (transitiv).
3. Für alle $x, y \in M$ mit $x \leq y \wedge y \leq x \Rightarrow x = y$ (antisymmetrisch).

Definition 12. Eine geordnete Menge $(M, \leq)$ mit der Eigenschaft: $\forall\, x, y \in M$ gilt: $x \leq y$ oder $y \leq x$ heißt *Kette*.

Definition 13. Sei $(M, \leq)$ eine geordnete Menge, man nennt sie *induktiv geordnet*, wenn für jede Kette $K \subseteq M$ ein $m \in M$ existiert mit $k \leq m$ für alle $k \in K$.

Definition 14. Sei $(M, \leq)$ eine geordente Menge, $m \in M$ heißt *maximales Element* von M, wenn für alle $l \in M$ mit $m \leq l$ folgt $m = l$.

Lemma 2.5 (Zorn'sches Lemma)**.** Jede induktiv geordnete nichtleere Menge $(M, \leq)$ besitzt ein maximales Element.

Definition 15. Seien A, B zwei Mengen, man sagt *A ist mindestens so mächtig wie B*, wenn eine injektive Abbildung von A nach B existiert und schreibt $|A| \leq |B|$. Wenn es eine bijeketive Abbildung von A auf B gibt, dann nennt man A und B gleichmächtig und schreibt $|A| = |B|$. $|A| < |B|$ bedeutet, dass es eine injektive Abbildung von A auf B gibt, aber es existiert keine bijektive Abbildung zwischen A und B.

Satz 2.6. Seien X, Y unendliche Mengen, dann gilt $|X \times Y| = max\{|X|, |Y|\}$.

Satz 2.7. Sei L/K eine algebraische Körpererweiterung, so gilt:

1. Wenn $|K| \notin \mathbb{N}$ ist, folgt $|L| = |K|$.
2. Wenn K endlich ist, folgt $|L| \leq |\mathbb{N}|$.

Beweis. Die Definition 8 besagt, dass sich jedes Element aus L als Nullstelle eines Polynoms aus $K[X]$ schreiben lässt. Sei nun U die Menge aller Polynome $\neq 0$. Definiere die Menge $N(P) = \{a \in L \mid P(a) = 0, P \in U\}$, dann kann man L schreiben als $L = \bigcup_{P \in U} N(P)$. Zeige zuerst den Fall $|K| \notin \mathbb{N}$. Es gilt $|K| \leq |U|$, da auch jedes konstante Polynom $P = c$ für alle $c \in K$ in U liegt. Als der schwierigere Schritt stellt sich die Ungleichung $|K| \geq |U|$ heraus. Im Anschluss wird durch eine Bijektion sofort die Gleichheit der Mächtigkeiten gezeigt. Sei nun P_n die Menge aller normierten irreduziblen Polynome mit Grad n. Es lässt sich eine Bijektion zwischen der Menge der Polynome n-ten Grades und der Menge aller $n+1$-Tupel, deren letzte Eintragung verschieden von 0 ist, finden. Diese sieht folgendermaßen aus:

$$a_0 + a_1 X + \cdots + a_{n-1} X^{n-1} + a_n X^n$$

$$\updownarrow$$

$$(\underbrace{a_0, a_1, \ldots, a_{n-1}}_{beliebig}, \underbrace{a_n}_{\neq 0}).$$

Dann kann die Mächtigkeit für die Menge P_n der Polynome n-ten Grades unter Verwendung von Satz 2.6 abgeschätzt werden:

$$|P_n| = \underbrace{|K| \times \cdots \times |K|}_{n-mal} \times \underbrace{|K \setminus \{0\}|}_{=|K|} = |K|.$$

Die Mächtigkeit der Menge U lässt sich aufgrund der Eigenschaft, dass U die disjunkte Vereinigung, über alle $n \in \mathbb{N}_0$, der Menge der Polynome n-ten Grades ist, so darstellen:

$$|U| = |P_0 \cup P_1 \cup P_2 \cup \cdots| = |P_0| + |P_1| + |P_2| + \cdots = |\mathbb{N}||K| = |K|.$$

Die Menge der Nullstellen eines Polynoms ist immer endlich, so lässt sich die Mächtigkeit von L, durch die zu Beginn erstellte Vereinigung $L = \bigcup_{P \in U} N(P)$ folgendermaßen abschätzen: $|L| \leq |\mathbb{N}| \cdot |K| = |K|$. Das gilt nach Satz 2.6. Da L/K eine Körpererweiterung ist, gilt die Ungleichung $|L| \geq |K|$ per Definition. Somit erhalten wir im Fall $|K| \notin \mathbb{N}$ die Gleichheit $|L| = |K|$.
Für den Fall (2), sei nun K endlich und P_n wie oben definiert. Wir betrachten abermals die Abbildung zwischen der Menge der Polynomen n-ten Grades und der aller $n+1$-Tupel, deren letzter Eintrag verschieden von 0 ist.

$$a_0 + a_1 X + \cdots + a_{n-1} X^{n-1} + a_n X^n$$

$$\updownarrow$$

$$(\underbrace{a_0, a_1, \ldots, a_{n-1}}_{beliebig}, \underbrace{a_n}_{\neq 0}).$$

Dadurch, dass für jeden Eintrag im $n+1$-Tupel nur endlich viele Element in Frage kommen, kann man die Mächtigkeit der Menge der Polynome n-ten Grades P_n abschätzen:

$$|P_n| \leq \underbrace{|\mathbb{N}| \times \cdots \times |\mathbb{N}|}_{n+1-mal} = |\mathbb{N}|.$$

Für die Mächtigkeit von U, diese Menge besteht aus der disjunkten Vereinigung der P_i für alle $i \in \mathbb{N}_0$ gilt:

$$|U| = |P_0 \cup P_1 \cup P_2 \cup \cdots| = |P_0| + |P_1| + |P_2| + \cdots \leq |\mathbb{N}| \cdot |\mathbb{N}| = |\mathbb{N}|.$$

Jedes Polynom hat endlich viele Nullstellen und es gilt $L = \bigcup_{P \in U} N(P)$, sodass sich $|L| \leq |\mathbb{N}| \cdot |\mathbb{N}| = |\mathbb{N}|$ ergibt. □

Satz 2.8. Für jede Menge X gilt $|X| < |2^X|$.

Dieser Satz besagt insbesondere, dass es zu jeder Menge X eine größere Menge gibt und wird im nächsten Satz verwendet. Dieses Resultat ist von theoretischer Art und ist wichtig um normale Körpererweiterungen zu behandeln, welcher ihrerseits für die Galoistheorie von großer Bedeutung sind. Nun ist die nötige Vorarbeit vollbracht und es kann folgendes wichitge Resultat bewiesen werden:

Satz 2.9 (E.Steinitz 1910)**.** Jeder Körper K besitzt einen algebraischen Abschluss.

Beweis. Sei K ein Körper, so existiert nach Satz 2.8 eine überabzählbare Menge S mit $K \subseteq S$ und $|K| < |S|$. Das Bilden von Allmengen führt zu mengentheoretischen Widersprüchen, um das zu vermeiden sei X die Menge aller algebraischen Erweiterungskörper L von K die in S liegen. Diese Menge ist nicht leer, da $K \in X$ liegt. Definiere nun folgende zweistellige Relation $\leq$ auf X,

$$L_1 \leq L_2 :\Leftrightarrow L_1 \text{ ist Teilkörper von } L_2.$$

Diese Relation ist

1. reflexiv, weil jeder Körper ein Teilkörper von sich selbst ist.

2. transitiv, denn seien $L_1, L_2, L_3 \in X$ Körper mit $L_1 \leq L_2 \wedge L_2 \leq L_3$ nach Definition von Teilkörper gilt für die Mengen $L_1 \subseteq L_2 \subseteq L_3$ und für alle $a, b, c \in L_1, c \neq 0$ folgt $a - b, ab, c^{-1} \in L_1$, da L_1 ein Körper ist, somit ist L_1 ein Teilkörper von L_3 und es gilt $L_1 \leq L_3$.

3. antisymmetrisch dadurch, dass für alle $L_1, L_2 \in X$ Körper mit $L_1 \leq L_2 \wedge L_2 \geq L_1$ die mengenmäßige Gleichheit $L_1 = L_2$ gilt. Sie haben durch die Teilkörpereigenschaft die gleichen Operationen, daher sind sich auch als Körper gleich und es gilt die Antisymmetrie.

$(X, \leq)$ ist also eine geordneten Menge.

- Wir zeigen $(X, \leq)$ ist induktiv geordnet:
  Sei κ eine Kette in $(X, \leq)$ und $T = \bigcup_{L \in \kappa} L$. Wir zeigen nun, dass T ein Körper ist. Dafür werden zwei Operationen benötigt, die wie folgt definiert werden. Seien $a, b \in T$, so gibt es ein $L \in \kappa$ mit $a, b \in L$. $(L, +, \cdot)$ ist ein Körper. Für T legen wir die Operationen mit $a \oplus b = a + b$ und $a \odot b = a \cdot b$ fest, da es sich bei den Elementen von κ um bestimmte Teilkörper handelt, ist die Definition von $\oplus$ und $\odot$ unabhängig von der Wahl von L. $(T, \oplus, \odot)$ ist tatsächlich ein Körper, da sich beispielsweise die Assoziativität durch, $\forall\ a, b, c \in T$ existiert ein L' mit $a, b, c \in L'$: $a \odot (b \odot c) = a \cdot (b \cdot c) = (a \cdot b) \cdot c = (a \odot b) \odot c$ ergibt. Der Nachweis der restlichen Köperaxiome erfolgt jeweils durch Zurückführung auf den jeweiligen Körper, der alle Elemente beinhaltet, dort können die geltenden Körperaxiome ausgenutzt werden.
  Alle Körper aus S liegen in S, das gilt somit insbesondere für alle Körper in κ, da κ eine Kette in $(X, \leq)$ ist. Aus dem vorigen Argument folgt, dass $T \subseteq S$ ein Erweiterungskörper für jedes $L \in \kappa$ ist. Die Vereinigungen T von algebraischen Erweiterungen $L \in \kappa$ ist wieder eine, also ist T/K algebraisch. Für jedes $L \in \kappa$ gilt daher $L \leq T$, somit ist T eine obere Schranke von κ, da κ beliebig war, ist $(X, \leq)$ induktiv geordnet.

- Aus dem Zorn'schen Lemma 2.5 folgt, dass $(X, \leq)$ ein maximales Element M besitzt.

- Wir zeigen, dass M algebraisch abgeschlossen ist. Der Beweis erfolgt indirekt:
  Angenommen M ist nicht algebraisch abgeschlossen. Nach den Äquivalenzen aus Lemma 2.4 folgt die Aussage (3) negiert, also existiert ein über M algebraischer Erweiterungskörper $M' \neq M$. Die Menge des Körper M' ist nicht notwendig eine Teilmenge von S, sodass M' nicht in X liegen muss. Es gilt nun ein isomorphes Bild von M' in S zu finden. Die Menge S ist nach Voraussetzung überabzählbar und es gilt $|K| < |S|$, es folgt:

$$|M' \setminus M| \leq |M'| \overset{(*)}{<} |S| \overset{(+)}{=} |S \setminus M|.$$

(*)M' ist ein algebraischer Erweiterunskörper von M und nach Satz 1.9 auch von K, da M/K algebraisch ist. Nach Satz 2.7 folgt für ein unendliches K, dass $|K| = |M'|$ ist und für ein endliches K gilt $|M'| \leq |\mathbb{N}|$. In beiden Fällen erhalten wir also die Ungleichung $|M'| < |S|$.
(+)Angenommen $|S| > |S \setminus M|$, dann folgt $|S| = |(S \setminus M) \cup M| = |S \setminus M| + |M| = max\{|S \setminus M|, |M|\} < |S|$.
Aufgrund dieser Ungleichung existiert eine injektive Abbildung φ nach Defnition 15, $\varphi : M' \to S$, wobei die Einschränkung von φ auf M der Identität entspricht, also $\varphi_{|M} = id_M$. Nun werden die Operationen $+', \cdot'$ von M' auf $\varphi(M')$ übertragen durch $\varphi(a) + \varphi(b) = \varphi(a +' b)$ und $\varphi(a) \cdot \varphi(b) = \varphi(a \cdot' b)$ für $a, b \in M'$, dann ist φ ein Isomorphismus von M' auf $\varphi(M')$. Bei $\varphi(M')$ handelt es sich um einen algebraischen Erweiterungskörper von M, wobei $\varphi(M') \neq M$. Sei $a \in M'$:

$$m_{a,M} = \sum_{i=0}^{n} m_i X^i \; m_i \in M \Rightarrow 0 = \varphi(\sum_{i=0}^{n} m_i a^i) = \sum_{i=0}^{n} m_i \varphi(a)^i$$

daher ist jedes Element aus $\varphi(M')$ algebraisch über M und nach Satz 1.9 auch über K. Aus diesem Grund ist $\varphi(M') \in X$ und $L \subseteq M \subseteq \varphi(M')$ für alle $L \in \kappa$. Das steht im Widerspruch zur Maximalität von M. Daher ist M algebraisch abgeschlossen. Es wurde also ein algebraischer Abschluss gefunden, das ist die Behauptung des Satzes.

□

Wie schon erwähnt spielt dieser Beweis in der Theorie eine wichtige Rolle. Es sei noch ein Beispiel zu algebraischen abgeschlossenen Körpern angeführt, das eigentlich den Status eines kleinen Satzes hat. Dieses ist keine direkte Folgerung aus dem Satz von Steinitz und stellt eine allgemeine Eigenschaft von algbraisch abgeschlossenen Körpern dar.

Beispiel 10. Ein algebraisch abgeschlossener Körper hat unendlich viele Elemente.

Beweis. Indirekt: Angenommen ein algebraisch abgeschlossener Körper K hat nur endlich viele Elemente $k_1, \ldots, k_n$. Erstelle nun das Polynom $P = (X - k_1) \cdot \ldots \cdot (X - k_n) + k$ mit $k \in K$, wobei $k \neq 0$. Dann hat P keine Nullstelle in K und das ist ein Widerspruch zur algebraischen Abgeschlossenheit. □

3 Zerfällungskörper

Mit der bloßen Existenz eines algebraischen Abschluss $\bar{K}$ eines Körpers K könnte man sich zufrieden geben. Es lässt sich noch genaueres darüber aussagen, denn in diesem Abschnitt wird gezeigt, dass der algebraische Abschluss bis auf K-Isomorphie eindeutig ist. Um dieses Resultat zu bekommen werden Zerfällungskörper eingeführt. Dabei handelt es sich um die kleinsten Körpererweiterungen über denen eine Menge von Polynomen zerfällt. Das Kapitel behandelt zu Beginn K-Homomorphismen und einige ihrer Eigenschaften. Diese spezielle Art von Homomorphismen sind für die Galoistheorie von größter Bedeutung, sodass diese Aussage auch in den nächsten Kapiteln ihre Anwendung finden. Anschließend werden, wie schon erwähnt, die Zerfällungskörper eingeführt und das wichtige Resultat, dass je zwei Zerfällungskörper einer Teilmenge K-isomorph sind, bewiesen. In diesen Kapitel richte ich mich nach den Büchern „Algebra“ von Jantzen und Schwermer (Kapitel V, §4, [7]), „Algebra“ von Karpfinger und Meyberg (Kapitel 23, [9]) und „Galois-Theorie“ von Staudner (Kapitel II, §4, [13]).

Definition 16. Seien L_1/K und L_2/K Erweiterungen desselben Körpers K, so wird eine Homomorphismus $\varphi : L_1 \to L_2$ mit der Bedingung $\varphi(k) = k$ für alle $k \in K$ ein *K-Homomorphismus* genannt. Ein bijektiver K-Homomorphismus heißt *K-Isomorphismus*. Einen K-Isomorphismus mit $\varphi : L_1 \to L_1$ nennt man *K-Automorphismus*.

Satz 3.1. Für jede Körpererweiterung L/K bildet die Menge der K-Automorphismen mit der Komposition als binäre Verknüpfung eine Gruppe und wird mit $Aut_K(L)$ bezeichnet.

Beweis. Die Komposition von K-Isomorphismen bleibt ein K-Isomorphismus, denn die Verknüpfung zweier Isomorphismen bleibt ein Isomorphismus und aus $\varphi_1, \varphi_2 \in Aut_K(L)$, $k \in K$ $\varphi_1(\varphi_2(k)) = \varphi_1(k) = k$ folgt das zweite Argument.

- Assoziativität: Für alle $\varphi_1, \varphi_2, \varphi_3 \in Aut_K(L)$, $a \in L$ gilt

$$\begin{aligned}\varphi_1 \circ (\varphi_2 \circ \varphi_3)_{(a)} &= \varphi_1 \circ (\varphi_2(\varphi_3(a))) = \varphi_1(\varphi_2(\varphi_3(a))) \\ &= (\varphi_1 \circ \varphi_2)_{\varphi_3(a)} = ((\varphi_1 \circ \varphi_2) \circ \varphi_3)_{(a)}\end{aligned}$$

- Neutrales Element ist die identische Abbildung $id(l) = l$ für alle $l \in L$.

- Inverses Element: da φ ein K-Isomorphismus ist, existiert auch eine bijektive Umkehrabbildung φ^{-1}. Die Funktion φ^{-1} ist auch ein K-Isomorphismus, denn für beliebige $x, y \in L$ existieren eindeutig bestimmte $a, b \in L$ mit $\varphi(a) = x$ und $\varphi(b) = y$. Es gilt $\varphi(a + b) = x + y$,

also auch $\varphi^{-1}(x+y) = a+b = \varphi^{-1}(x)+\varphi^{-1}(y)$. Weiters ist $\varphi(ab) = xy$, also ist $\varphi^{-1}(xy) = ab = \varphi^{-1}(x)\varphi^{-1}(y)$. Für beliebige Elemente k aus K gilt $\varphi(k) = k$, also auch $\varphi^{-1}(k) = k$. Somit ist φ^{-1} ein K-Isomorphismus. Es wurde daher das inverse Element gefunden.

Es wurden alle Eigenschaften einer Gruppe nachgewiesen. □

Um die Eindeutigkeit bis auf Isomorphie von Zerfällungskörpern einer Teilmenge von $K[X]$ zu zeigen, wobei K ein Körper ist, werden noch genauere Aussagen über Homomorphismen und K-Homomorphismen benötigt.

Lemma 3.2. Jeder K-Homomorphismus ist injektiv

Beweis. Seien L_1/K und L_2/K Erweiterungen des selben Körpers und φ ein K-Homomorphismus zwischen den beiden Körpern. Für alle $a \in L_1$, $a \neq 0$ folgt $1 = \varphi(1) = \varphi(aa^{-1}) = \varphi(a)\varphi(a)^{-1}$, daher ist $\varphi(a) \neq 0$. Das gilt für alle $a \in L_1$, $a \neq 0$. Also liegt nur $0 \in kern\ \varphi$, daraus folgt die Injektivität. □

Lemma 3.3. Sei $\varphi : L_1 \to L_2$ ein K-Homomorphismus, dann gilt: $a \in L_1$ ist genau dann algebraisch über K, wenn $\varphi(a)$ algebraisch über K ist.

Beweis. ($\Rightarrow$) Sei $a \in L_1$ algebraisch über K. Es existiert ein Polynom $P \in K[X]$ mit $P(a) = 0$ der Form $\sum_{i=0}^{n} k_i X^i$ mit $k_i \in K$ für alle $i \in \{0, 1, \ldots, n\}$. Wir wenden den K-Homomorphismus auf $0 = P(a)$ an und erhalten: $0 = \varphi(0) = \varphi(\sum_{i=0}^{n} k_i X^i) = \sum_{i=0}^{n} k_i \varphi(a)^i$. Es wurde also ein Polynom $P \in K[X]$ gefunden mit $P(\varphi(a)) = 0$. Also ist $\varphi(a)$ algebraisch über K.
($\Leftarrow$) Sei $\varphi(a) \in L_2$ algebraisch über K, so gibt es ein Polynom $P \in K[X]$ mit $P(\varphi(a)) = 0$. Das Polynom hat die Form $P = \sum_{i=0}^{n} k_i X^i$ mit $k_i \in K$ für alle $i \in \{0, 1 \ldots, n\}$. Es gilt daher:

$$
\begin{aligned}
0 &= \sum_{i=0}^{n} k_i \varphi(a)^i \\
0 &= \varphi(\sum_{i=0}^{n} k_i a^i) \\
0 &= \varphi(0) \quad \varphi \text{ ist injektiv} \\
0 &= \sum_{i=0}^{n} k_i a^i.
\end{aligned}
$$

Es wurde also ein Polynom aus $K[X]$ gefunden, von dem a eine Nullstelle ist. □

Definition 17. Seien K, K' zwei Körper, φ ein Isomorphismus von K nach K' und $P \in K[X]$ ein Polynom, dann bezeichnet man $\varphi^* : K[X] \to K'[X]$, definiert durch

$$\varphi^*(P) = \varphi^*(\sum_{i=0}^{n} k_i X^i) = \sum_{i=0}^{n} \varphi(k_i) X^i$$

als die *Fortsetzung des Isomorphismus* φ .

Satz 3.4. Seien $L/K, L'/K'$ zwei algebraische Körpererweiterungen und $\sigma : K \to K'$ ein Isomorphismus, $\sigma^* : K[X] \to K'[X]$ bezeichnet die Fortsetzung des Isomorphismus σ auf die Polynomringe. Dann gilt: für $a \in L$ und $a' \in L'$ mit $m_{a',K'} = \sigma^*(m_{a,K})$ gibt es genau einen Isomorphismus $\varphi : K(a) \to K'(a')$ mit $\varphi_{|K} = \sigma$ und $\varphi(a) = a'$.

Beweis. Nach Satz 1.5 ist $K[X]/(m_{a,K}) \cong K(a)$, daher können wir den kanonischen Isomorphismus $\pi : K[X]/(m_{a,K}) \to K(a)$ erstellen. Das gleiche Argument gilt für den Körper $K'[X]/(\sigma^* m_{a,K})$, sei also nun π' der kanonische Isomorphismus mit $\pi' : K'[X]/(m_{a',K'}) \to K(a')$. Der Isomorphismus $\sigma^* : K[X] \to K'[X]$ bildet das Hauptideal $(m_{a,K})$ auf $(m_{a',K'})$ ab, dadurch wird ein Isomorphismus Φ von $K[X]/(m_{a,K})$ auf $K'[X]/(m_{a',K'})$ induziert. Schränkt man Φ auf K ein, so gilt $\Phi_{|K} = \sigma$, da $m_{a,K}$ nicht konstant ist. Wir definieren nun $\varphi = \pi' \circ \Phi \circ \pi^{-1}$, so führt φ von $K(a)$ nach $K'(a')$ mit $\varphi_{|K} = \sigma$. Für das Bild $\varphi(a) = (\pi' \circ \Phi \circ \pi^{-1})_{(a)}$ gilt Folgendes, $\pi^{-1}(a)$ bildet a auf $X + (m_{a,K})$, Φ führt $X + (m_{a,K})$ zu $X + (m_{a',K'})$ über und $\pi'(X + m_{a',K'}) = a'$, somit gilt $\varphi(a) = a'$. □

Bemerkung. Erweitert man im Satz 3.4 den Bildbereich von $K(a')$ auf L' so verliert man im Allgemeinen die Surjektivität. Es bleibt also genau ein Monomorphismus φ übrig.

Korollar 3.5. Seien $L/K, L'/K'$ zwei algebraische Körpererweiterungen und $\sigma : K \to K'$ ein Isomorphismus, $\sigma^* : K[X] \to K'[X]$ bezeichnet die Fortsetzung des Isomorphismus σ auf die Polynomringe und sei $a \in L$. Dann ist die Anzahl der Homomorphismen φ von $K(a)$ nach L' mit $\varphi_{|K} = \sigma$ gleich der Anzahl der Nullstellen von $\sigma^*(m_{a,K})$ in L'

Beweis. Aus dem Satz 3.4 folgt, dass es für jede Nullstelle von $\sigma^*(m_{a,K})$ in L' genau einen Homomorphismus φ von $K(a)$ nach L' mit $\varphi_{|K} = \sigma$ und $\varphi(a) = a'$ gibt. Der Isomorphismus wird zum Homomorphismus, durch Vergrößerung des Bildraums von $K(a')$ auf L'. Es bleibt zu zeigen, dass das alle Homomorphismen sind. Das folgt aus: Sei $\tau : K(a) \to L'$ beliebiger Homomorphismus mit $\tau_{|K} = \sigma$, sei $P = \sum_{i=0}^{n} k_i X^i$ aus $K[X]$ beliebig. Es gilt: $\sigma^*(P)(\tau(a)) = \sum_{i=0}^{n} \sigma(k_i)\tau(a)^i = \sum_{i=0}^{n} \tau(k_i)\tau(a)^i = \tau(P(a))$. Wir

haben nun gezeigt, dass für alle Polynome $P \in K[X]$ die Gleichheit von $\sigma^*(P)(\tau(a)) = \tau(P(a))$ gilt. Somit erfüllt dies insbesondere das Minimalpolynom $m_{a,K}$. Also ist $\tau(a)$ eine Nullstelle von $\sigma^*(m_{a,K})$. Es wurde damit gezeigt, dass wir so alle Homomorphismen erhalten. □

Es wurde nun genug Vorarbeit geleistet um den Begriff Zerfällungskörper einzuführen und wichtige Resultate darüber zu beweisen.

Definition 18. Sei K ein Körper, ein Erweiterungskörper L von K wird *Zerfällungskörper von $A \subseteq K[X]$ über K* genannt, falls folgende Eigenschaften erfüllt sind:

- Jedes P aus A zerfällt über L.
- L wird von den Nullstellen der Polynome aus A erzeugt, also $L = K(\bigcup_{P \in A} W(P))$, wobei $W(P) := \{a \in L \mid P(a) = 0\}$.

Bemerkung. Wenn die Menge $A \subseteq K[X]$ endlich ist mit $A = \{P_1, \ldots, P_n\}$, dann kann A durch die Menge $\{P\}$ ersetzt werden, mit $P = P_1 \cdot \ldots \cdot P_n$. Es gilt dann $L = K(a_1, \ldots, a_n)$, wobei $P(a_i) = 0$ für ein $P \in A$ für alle $i \in \{1, \ldots, n\}$.

Beispiel 11. Gesucht ist ein Zerfällungskörper in $\mathbb{C}$ des Polynoms $X^4 - 7 \in \mathbb{Q}[X]$, sowie dessen Grad über $\mathbb{Q}$. Aufgrund von $X^4 - 7 = (X + \sqrt[4]{7})(X - \sqrt[4]{7})(X + i\sqrt[4]{7})(X - i\sqrt[4]{7})$ ergibt sich $\mathbb{Q}(i, \sqrt[4]{7})$ als ein Zerfällungskörper. Weiters ist $X^2 + 1$ das Minimalpolynom von i über $\mathbb{Q}(\sqrt[4]{7})$, so gilt $[\mathbb{Q}(i, \sqrt[4]{7}) : \mathbb{Q}(\sqrt[4]{7})] = 2$. Das Polynom $X^4 - 7$ ist normiert, irreduzibel nach Eisenstein und hat $\sqrt[4]{7}$ als Nullstelle und stellt aus diesen Gründen das Minimalpolynom $m_{\sqrt[4]{7},\mathbb{Q}}$ dar. Für den Grad ergibt sich:

$$[\mathbb{Q}(i, \sqrt[4]{7}) : \mathbb{Q}] = [\mathbb{Q}(i, \sqrt[4]{7}) : \mathbb{Q}(\sqrt[4]{7})] \cdot [\mathbb{Q}(\sqrt[4]{7}) : \mathbb{Q}] = 2 \cdot 4 = 8$$

Lemma 3.6. Sei L ein Zerfällungskörper eines nichtkonstanten Polynoms P über K mit $deg P = n$, dann gilt $[L : K] \leq n!$

Beweis. Die Körpererweiterung L/K ist nach Satz 1.8 endlich. Der Beweis erfolgt mittels Induktion nach dem Grad von P:
Induktionsanfang: für $n = 1$.
Der Grad von P ist 1, dadurch hat P genau eine Nullstelle a im Zerfällungskörper L. Nach Definition 18 ist $L = K(a)$. Es gilt weiters, dass $m_{a,K} \mid P$, daraus folgt nach Satz 1.6, $[L : K] = [K(a) : K] = deg\, m_{a,K} \leq deg P = 1 = 1!$
Induktionsschritt: von $n - 1$ auf n:
Seien nun $a_1, \ldots, a_n \in L$ die Nullstellen des Polynoms P, es gilt nach Definition 18 $L = K(a_1, \ldots, a_n)$. Nach Lemma 1.4 gilt $m_{a_1,K} \mid P$ und aus

Satz 1.6 folgt $[K(a_1) : K] = deg\ m_{a_1,K} \leq degP = n$. Spalte die Nullstelle a_1 von P ab, dann ist $L = K(a_1)(a_2, \ldots, a_n)$ ein Zerfällungskörper von $P/(X - a_1)$ über $K(a_1)$. Es folgt nun $deg(P/(X - a_1)) = degP - 1 = n - 1$, dafür gilt nun die Induktionsvoraussetzung $[L : K(a_1)] \leq (n - 1)!$. Durch $[L : K] = [L : K(a_1)][K(a_1) : K] \leq (n - 1)!n = n!$ wird die Behauptung gezeigt. □

Die Einschränkung $n!$ kann nicht kleiner gemacht werden, das verdeutlicht folgendes Beispiel:

Beispiel 12. Gesucht ist der Grad des Zerfällungskörpers über $\mathbb{Q}$ des Polynoms $X^3 + 3 \in \mathbb{Q}[X]$. Die Nullstellen des Polynoms sind: $\sqrt[3]{3}, \zeta\sqrt[3]{3}, \zeta^2\sqrt[3]{3}$ wobei $\zeta = e^{\frac{2\pi i}{3}} = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$. Der Zerfällungskörper des Polynoms ist also $\mathbb{Q}(\sqrt[3]{3}, \zeta)$. Das Minimalpolynom $m_{\sqrt[3]{3},\mathbb{Q}} = X^3 - 2$ ist vom Grad 3 und $m_{\zeta,\mathbb{Q}(\sqrt[3]{3})} = X^2 + X + 1$ ist vom Grad 2. Für den Grad der Körpererweiterung ergibt sich:

$$[\mathbb{Q}(\sqrt[3]{3}, \zeta) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{3}, \zeta) : \mathbb{Q}(\sqrt[3]{3})][\mathbb{Q}(\sqrt[3]{3}) : \mathbb{Q}] = 2 \cdot 3 = 6 = 3!$$

Da die Erweiterung $\mathbb{Q}(\sqrt[3]{3}, \zeta)$ den Grad 6 hat, kann die obere Schranke nicht kleiner gemacht werden.

Lemma 3.7. Sei K ein Körper und $A \subseteq K[X]$, dann existiert zu A ein Zefällungskörper über K.

Beweis. Nach Satz 2.9 besitzt jeder Körper und somit auch K einen algebraischen Abschluss $\bar{K}$, nach Definition 9 zerfällt jedes nicht konstante Polynom von A über $\bar{K}$. Sei nun W die Menge aller Nullstellen der Polynome $P \in A$, wobei $W \subseteq \bar{K}$. Dann gilt, dass der Köperer $K(W)$ ein Teilkörper von $\bar{K}$ ist. Somit wurde der Zerfällungskörper von A über K gefunden. □

Satz 3.8. Je zwei Zerfällungskörper einer Teilmenge von $K[X]$ über K sind K-isomorph.

Beweis. Diese Behauptung wird allgemeiner bewiesen: Seien K und K' Körper und φ ein Isomorphismus von K nach K', $A \subseteq K[X]$ und A' die Menge von Polynomen die durch Fortsetzung des Isomorphismus φ ensteht. Wenn L ein Zerfällungskörper von A über K und L' ein solcher von A' über K', dann kann φ zu einem Isomorphismus von L auf L' fortgesetzt werden.
Sei U die Menge aller Fortsetzungen von φ zu Monomorphismen von Zwischenkörpern von L/K in L'. Sei E_σ der Definitionsbereich der Funktion $\sigma \in U$. Der Monomorphismus φ liegt in U, also gilt $U \neq \emptyset$. Auf diser Menge U wird eine zweistellige Relation definiert:

$$\sigma \leq \tau \Leftrightarrow \ \tau \text{ ist eine Fortsetzung von } \sigma\ .$$

Bei $(U, \leq)$ handelt es sich um eine geordnete Menge, da sie:

1. reflexiv ist: σ ist eine Fortsetzung von sich selbst, da die Einschränkung $\sigma_{|E_\sigma} = \sigma$ ist.

2. transitiv ist: Seien $\sigma, \tau, \rho \in U$ mit $\sigma \leq \tau$ und $\tau \leq \rho$, dann gilt $\rho_{|E_\tau} = \tau$ und $\tau_{|E_\sigma} = \sigma$, also ist $\rho_{|E_\sigma} = \sigma$ damit gilt die Transitivität.

3. antisymmetrisch ist: Seien $\sigma, \tau \in U$ mit $\sigma \leq \tau$ und $\tau \leq \sigma$, so führt $\sigma : E_\sigma \to L'$ und $\tau : E_\tau \to L'$, aus der Voraussetzung folgt, dass für die Definitionsmengen gilt $E_\sigma \subseteq E_\tau$ und $E_\tau \subseteq E_\sigma$, somit ergibt sich $E_\sigma = E_\tau$, also ist $\sigma = \tau$.

- Zeige nun, dass $(U, \leq)$ induktiv geordnet ist.
  Seien κ eine Kette in $(U, \leq)$ und $E = \bigcup_{\sigma \in \kappa} E_\sigma$. Alle E_σ erfüllen $K \subseteq E_\sigma \subseteq L$, somit gilt auch für $K \subseteq E \subseteq L$. Die Vereinigung der ineinandergeschachtelten Körper ergibt wieder einen Körper, da für jeweils zwei Elemente $a, b \in E$ gilt, es existiert ein E_σ mit $a \in E_\sigma$ und es existiert ein E_τ mit $b \in E_\tau$. Dann gilt *o.B.d.A.* $E_\sigma \subseteq E_\tau$ und daher ist a auch ein Element von E_τ. Der Körper E_τ ist bezüglich beider Operationen und der Inversenbildung abgeschlossen. Somit ist E ein Zwischenkörper von L/K. Sei χ die Abbildung von E nach L', die die Elemente folgendermaßen zuordnet: Für ein $a \in E$ gibt es ein $\sigma \in \kappa$ mit $a \in E_\sigma$, wir setzen $\chi(a) = \sigma(a)$. Jetzt ist, aber χ nicht abhängig von der Abbildung σ, da für alle τ mit $\sigma \leq \tau$ gilt $\sigma(a) = \tau(a)$, weil es sich dabei um Fortsetzungen von Funktionen handelt, die bei Einschränkungen auf den kleineren Körper gleich sind.
  Für alle $a, b \in E$ existiert ein σ, sodass $a, b \in E_\sigma$ sind, das gilt wegen der Ketteneigenschaft von κ. Daraus folgt:

$$\chi(a+b) = \sigma(a+b) = \sigma(a) + \sigma(b) = \chi(a) + \chi(b)$$
$$\chi(ab) = \sigma(ab) = \sigma(a)\sigma(b) = \chi(a)\chi(b).$$

  Da für alle $a \in E_\sigma, a \neq 0$ gilt: $1 = \chi(1) = \chi(aa^{-1}) = \chi(a)\chi(a)^{-1}$ ist χ injektiv, also ein Monomorphismus. Die Konstruktion von χ zeigt, dass es jedes $\sigma \in \kappa$ fortsetzt. Es gilt nun für alle $\sigma \in \kappa$, dass $\sigma \leq \chi$ ist. Da κ beliebig war, wurde gezeigt, dass $(U, \leq)$ induktiv geordnet ist.

- Nach dem Lemma 2.5 besitzt $(U, \leq)$ ein maximales Element $\psi : F \to L'$, wobei F ein Zwischenkörper von L/K.

- Zeige $F = L$
  Sei ein $P = \sum_{i=0}^{n} k_i X^i \in A$ und $a \in L$ mit $P(a) = 0$, so ist $P_2 =$

$\sum_{i=0}^{n} \varphi(k_i)X^i \in A'$ und es zerfällt über L'. Also hat L' eine Nullstelle von P_2. Dann existiert nach Satz 3.4 ein Isomorphismus $\bar{\psi}$ von $F(a)$ nach $F(\bar{\psi}(a))$. Dieser lässt sich als Monomorphismus von $F(a)$ nach L' auffassen, da $F(\bar{\psi}(a)) \subseteq L'$ ist. Die Abbildung ψ liegt maximal in $(U, \leq)$ und $\bar{\psi}$ ist eine Fortsetzung von ψ, also $\psi \leq \bar{\psi}$. Nach der Definition 14 des maximalen Elements folgt $\psi = \bar{\psi}$ und daraus $F(a) = F$. Also ist $a \in F$. Da a beliebig in L war gilt $F = L$

- Sei $Q = \sum_{i=0}^{n} k_i X^i \in A$ und $a \in L$, sodass $Q(a) = 0$ ist. Dann folgt wegen Satz 3.3, dass $\psi(a_i)$ eine Nullstelle von $\sum_{i=0}^{n} \psi(k_i)X^i = \sum_{i=0}^{n} \varphi(k_i)X^i$ ist, aufgrund der Fortsetzungseigenschaft von ψ. Es gilt $\psi(F)$ enthält alle Nullstellen der Polynome aus A', das Bild von F enthält damit einen Zerfällungskörper von A'. Wenn L' Zerfällungskörper von A' ist, existiert kein Zwischenkörper $\neq L'$ von L'/K' Zerfällungskörper von A', also $L' = \psi(F)$.

- Es wurde nun die verallgemeinerte Aussage gezeigt.

- Aus dem Sonderfall $K = K'$ und $\varphi = id_K$ folgt die Behauptung: Je zwei Zerfällungskörper einer Teilmenge von $K[X]$ über K sind K-isomorph.

□

Lemma 3.9. Sei L ein Erweiterungskörper von K, dann gilt: L ist ein algebraischer Abschluss von K genau dann, wenn L ein Zerfällungskörper von $K[X]$ über K ist.

Beweis. ($\Rightarrow$) Sei L ein algebraischer Abschluss von K. Wir konstruieren nun einen Zerfällungskörper von $K[X]$ in L. Sei W die Menge aller Nullstellen aller Polynome aus $K[X]$. So ist $W \subseteq L$. Daraus folgt, dass $K(W) \subseteq L$ ist. Sei $b \in L$ beliebig, dann zerfällt das Minimalpolynom $m_{b,K}$ über $K(W)$. Also ist $b \in K(W)$, da b beliebig war gilt $L = K(W)$
($\Leftarrow$) Sei L der Zerfällungskörper von $K[X]$. Nach Satz 2.9 hat L einen algebraischen Abschluss $\bar{L}$. Es gilt also $L \subseteq \bar{L}$. Aufgrund der Transitivität der Eigenschaft algebraisch gilt, $\bar{L}$ ist auch algebraischer Abschluss von K. Nach der Hinrichtung ist $\bar{L}$ auch ein Zerfällungskörper von $K[X]$ über K. Nach Satz 3.8 sind Zerfällungskörper von $K[X]$ über K bis auf K-Isomorphie eindeutig. Da $L \subseteq \bar{L}$ gilt, folgt also $\bar{L} = L$. □

Korollar 3.10. Je zwei algebraische Abschlüsse von K sind K-isomorph.

Beweis. Sei L ein algebraischer Abschluss von K, so gilt nach Satz 3.9, dass L ein Zerfällungskörper von $K[X]$ über K ist und aus dem Satz 3.8 folgt die Eindeutigkeit bis auf Isomorphie. □

Korollar 3.11. Jeder Körper besitzt bis auf K-Isomorphie genau einen algebraischen Abschluss.

Beweis. Die Existenz ergibt sich aus Satz 2.9 und die Eindeutigkeit bis auf K-Isomorphie aus Korollar 3.10 □

Die letzten Sätze und Korollare ergeben, dass algebraische Abschlüsse eines Körpers, sowie Zerfällungskörper gewisser Mengen vom algebraischen Standpunkt her nicht unterscheidbar sind.

Korollar 3.12. Sei L/K eine Körpererweiterung und φ ein K-Homomorphismus von L nach $\bar{K}$, dann lässt sich φ zu einem K-Automorphismus in $\bar{K}$ erweitern.

Beweis. Wir wählen einen algebraischen Abschluss $\bar{K}$ so, dass $L \subseteq \bar{K}$ und $\varphi(L) \subseteq \bar{K}$ ist. Wir betrachten φ als Isomorphismus von L nach $\varphi(L)$. Nach Lemma 3.9 ist $\bar{K}$ ein Zerfällungskörper von $K[X]$ und ebenfalls von $\varphi(K)[X] = K[X]$. Nach Satz 3.8 lässt sich φ zu einem K-Isomorphismus von $\bar{K}$ nach $\bar{K}$ erweitern. Die Fortsetzung ist also ein K-Automorphismus in $\bar{K}$. □

4 Normale Körpererweiterungen

In diesem Kapitel werden spezielle algebraische Körpererweiterungen behandelt, nämlich die normalen Körpererweiterungen. Diese sind für die später behandelten Galoiserweiterungen maßgebend. Der erste Satz behandelt Fortsetzungen von Monomorphismen und wird für den Beweis der Eigenschaften von normalen Körpererweiterungen gebraucht. Der Satz über die Äquivalenzen von normalen Körpererweiterungen wird in den folgenden Kapiteln verwendet. Abschließend werden noch Beispiele für normale und nichtnormale Erweiterungen angegeben, sowie ein Gegenbeispiel für die Transitivität der Eigenschaft normal. In diesem Kapitel wurden die Bücher „Algebra“ von Jantzen und Schwermer (Kapitel V, §4, [7]), „Algebra“ von Karpfinger und Meyberg (Kapitel 23, [9]), sowie „Körper-Ringe-Gleichungen“ von Cigler (Kapitel VIII, §1, [5]) verwendet.

Satz 4.1. Wenn L/K eine algebraische Körpererweiterung ist, dann lässt sich jeder Monomorphismus von K in einen über K algebraischen abgeschlossenen Körper M zu einem Monomorphismus von L nach M fortsetzen.

Beweis. Sei φ ein Monomorphismus von K nach M. Weiters sei $\bar{L}$ der algebraische Abschluss von L, somit ist $\bar{L}$ auch der algebraische Abschluss von K. Nach Lemma 3.9 ist $\bar{L}$ auch der Zerfällungskörper von $K[X]$ über K. Der algebraisch abgeschlossene Körper M enthält einen Zerfällungskörper von $\varphi(K)[X]$ über $\varphi(K)$. Sei dieser E. Der Monomorphismus φ kann als Isomorphismus von K nach $\varphi(K)$ gesehen werden. Nach Satz 3.8 existiert ein Isomorphismus ψ zwischen $\bar{L}$ und E, der φ fortsetzt. Die Einschränkung im Definitionsbereich der Funktion ψ von $\bar{L}$ auf L liefert einen φ fortsetzenden Monomorphismus nach M. □

Nun beginnen wir mit den speziellen algebraischen Erweiterungen, den normalen Körpererweiterungen.

Definition 19. Eine algebraische Körpererweiterung L/K heißt *normal*, wenn jedes irreduzible Polynom aus $K[X]$, das in L eine Nullstelle besitzt, über L in Linearfaktoren zerfällt.

Bemerkung. Die Definition besagt, dass jedes irreduzible Polynom aus $K[X]$ mit einer Nullstelle in L bereits alle Nullstellen in L hat. In verschiedenen Büchern wird normal verschieden definiert, das liegt an den Äquivalenzen im folgenden Satz. Es wird meist eine der drei Äquivalenzen als Definition gewählt. Aufgrund des Satzes 4.2 ist das eben möglich.

Satz 4.2 (Äquivalenzen normaler Körpererweiterungen)**.** Sei L/K eine algebraische Körpererweiterung und $\bar{L}$ der algebraische Abschluss von L. Dann sind folgende Aussagen äquivalent:

1. L/K ist normal.
2. Für eine Menge nichtkonstanter Polynome $A \subseteq K[X]$ ist L der Zerfällungskörper von A über K ist.
3. Für jeden K-Homomorphismus $\varphi : L \to \bar{L}$ gilt $\varphi(L) = L$.

Beweis. (1)⇒(2) Sei $a \in L$. Wir betrachten das Minimalpolynom $m_{a,K}$, so zerfällt dieses nach Voraussetzung über L. Also zerfällt für jedes beliebige $b \in L$ das Minimalpolynom $m_{b,K}$ über L. Wir bilden die Menge $A = \{m_{a,K} \mid a \in L\}$, dann ist A eine Teilmenge von $K[X]$. Somit ist L der Zerfällungskörper von A.
(2)⇒(3) Sei L ein Zerfällungskörper einer Teilmenge A von $K[X]$ über K. Sei $\varphi : L \to \bar{L}$ ein K-Homomorphismus, nach Lemma 3.2 ist φ injektiv und nach Lemma 3.3 gilt die Aussage, wenn $a \in L$ eine Nullstelle eines Polynoms $P \in A$ ist, dann ist auch $\varphi(a)$ Nullstelle des Polynoms, das durch Fortsetzung von φ auf $K[X]$ entsteht. Denn sei $P = \sum_{i=0}^{n} k_i X^i$, dann gilt $\varphi^*(P) = \sum_{i=0}^{n} \varphi(k_i) X^i = \sum_{i=0}^{n} k_i X^i = P$, da φ ein K-Homomorphismus ist. Alle $P \in A$ zerfallen nach Voraussetzung über L und für alle Nullstellen a eines Polynoms $P \in A$ gilt, dass $\varphi(a)$ ebenfalls eine Nullstelle eines Polynoms $P \in A$ ist. Sei W die Menge aller Nullstellen von Elementen aus A, dann folgt aus dem Gezeigten, dass $\varphi(W) = W$ ist. Die Abbildung φ permutiert die Nullstellen. Seien $a_1, \ldots, a_n$ alle Nullstellen aus W, dann gilt nach Definition 18, $L = K(W)$. Nun folgt $\varphi(L) = \varphi(K(W)) = K(\varphi(W)) = K(W) = L$
(3)⇒(1) Seien $a \in L$ und $b \in \bar{L}$ Nullstellen eines irreduziblen Polynom $P \in K[X]$. Die Körpererweiterungen $\bar{L}/K$ und L/K sind algebraisch, für $\sigma = id_K$ existiert ein K-Homomorphismus φ von $K(a)$ nach $K(b)$ mit $\varphi_{|K} = \sigma$ und $\varphi(a) = b$. Nach Satz 4.1 lässt sich φ zu einem $\psi : L \to \bar{L}$ fortsetzen. Die Voraussetzung besagt, dass $\psi(L) = L$ ist, daher gilt $b = \psi(a) \in \psi(L) = L$ da a, b beliebig waren zerfällt jedes irreduzible Polynom über L in Linearfaktoren. □

Korollar 4.3. Jede Körpererweiterung vom Grad 2 ist normal.

Beweis. Sei L/K eine Erweiterung vom Grad 2 und $a \in L \setminus K$. Sei P ein irreduzibles Polynom aus $K[X]$ mit $P(a) = 0$. Das Polynom P muss nicht normiert sein, hat aber den gleichen Grad, wie das Minimalpolynom $m_{a,K}$. Also ist P vom Grad 2 und kann daher nur in L in ein Produkt zweier Linearfaktoren zerfallen. Also enthält L alle Wurzeln des beliebigen Polynoms P. L/K ist nach Definition 19 eine normale Körpererweiterung. □

Beispiel 13.

Wir betrachten die Körpererweiterung $\mathbb{Q}(i\sqrt{5})/\mathbb{Q}$. So ist X^2+5 das Minimalpolynom von $i\sqrt{5}$ über $\mathbb{Q}$. Es gilt daher $[\mathbb{Q}(i\sqrt{5}) : \mathbb{Q}] = 2$. Aus dem Korollar 4.3 folgt, dass die Körpererweiterung normal ist.

Wir zeigen nun, dass die Körpererweiterungen $\mathbb{Q}(\sqrt{7})/\mathbb{Q}$ und $\mathbb{Q}(i\sqrt[4]{7})/\mathbb{Q}(\sqrt{7})$ normal sind und die Körpererweiterung $\mathbb{Q}(i\sqrt[4]{7})/\mathbb{Q}$ nicht normal ist.
Es gilt $m_{\sqrt{7},\mathbb{Q}} = X^2 - 7$, daher ist $\mathbb{Q}(\sqrt{7})/\mathbb{Q}$ eine Erweiterung vom Grad 2 und nach Korollar 4.3 normal. Wir betrachten die nächste Körpererweiterung $\mathbb{Q}(i\sqrt[4]{7})/\mathbb{Q}$. Das Minimalpolynom von $i\sqrt[4]{7}$ über $\mathbb{Q}$ ist $X^4 - 7$. Daher hat die Körpererweiterung $\mathbb{Q}(i\sqrt[4]{7})/\mathbb{Q}$ den Grad 4. Der Körper $\mathbb{Q}(i\sqrt[4]{7})$ kann aber nicht der Zerfällungskörper des Polynom $X^4 - 7$ sein, da dieser nach Beispiel 11 Grad 8 über $\mathbb{Q}$ hat. Die Nullstellen $\sqrt[4]{7}$ und $-\sqrt[4]{7}$ liegen nicht in $\mathbb{Q}(i\sqrt[4]{7})$. Es existiert also ein irreduzibles Polynom mit einer Nullstelle in $\mathbb{Q}(i\sqrt[4]{7})$, jedoch sind nicht alle anderen Nullstellen in $\mathbb{Q}(i\sqrt[4]{7})$, daher ist nach dem Satz 4.2 die Erweiterung $\mathbb{Q}(i\sqrt[4]{7})/\mathbb{Q}$ nicht normal. Für die Erweiterung $\mathbb{Q}(i\sqrt[4]{7})/\mathbb{Q}(\sqrt{7})$ gilt nach Gradsatz 1.1 und dem oben Gezeigten:

$$4 = [\mathbb{Q}(i\sqrt[4]{7}) : \mathbb{Q}] = [\mathbb{Q}(i\sqrt[4]{7}) : \mathbb{Q}(\sqrt{7})][\mathbb{Q}(\sqrt{7}) : \mathbb{Q}] = 2 \cdot 2.$$

Somit ist auch $\mathbb{Q}(i\sqrt[4]{7})/\mathbb{Q}(\sqrt{7})$ normal. Die Eigenschaft „normal“ ist daher im Allgemeinen nicht transitiv. Seien die Körpererweiterungen L/Z und Z/K normal, dann muss L/K nicht normal sein.

5 Separable Körpererweiterungen

Einfache Körpererweiterungen sind leichter zu handhaben, so lässt sich zum Beispiel der Grad solcher Körpererweiterungen schnell bestimmen. In diesem Kapitel wird gezeigt, dass eine Vielzahl von endlichen algebraischen Körpererweiterung einfach sind. Dazu wird der bislang neue Begriff der Separabilität benötigt. Dabei betrachtet man, ob die Nullstellen eines Polynoms getrennt voneinander in einem Zerfällungskörper liegen. Um das Ziel, den Satz vom primitiven Element, zu beweisen wird neben der Separabilität, die Charakteristik und auch der aus der Analysis bekannte Begriff der Ableitung eingeführt. Dabei werden einige Eigenschaften der beiden gezeigt bis der zuvor erwähnte Satz bewiesen werden kann. Die verwendete Literatur umfasst die Werke „Algebra“ von Artin (Kapitel 13.6, [2]), „Algebra“ von Bosch (Kapitel 3.4, [4]), „Algebra“ von Jantzen und Schwermer (Kapitel V §5, [7]) und „Algebra“ von Karpfinger und Meyberg (Kapitel 24, [9]), „Galoissche Theorie“ von Artin (Kapitel II, [1]) und „Körper Ringe Gleichungen“ von Cigler (Kapitel VII 3 und VIII 1, [5]).

Definition 20. Sei $P = \sum_{i=0}^{n} k_i X^i \in K[X]$ dann definiert man die *Ableitung von P* folgendermaßen:

$$P' = \sum_{i=0}^{n} i k_i X^{i-1}.$$

Die Ableitung wurde hier also wie aus der Analysis bekannt, für Polynome definiert.

Beispiel 14. Wir bilden die Ableitung des Polynoms $P = 7X^3+5X^2+3X+1$. Es gilt nach Definition $P' = 21X^2 + 10X + 3$.

Für die Ableitung von Polynomprodukten benötigt man die "Produktregel".

Lemma 5.1. Seien P und Q Polynome über einen Körper K, dann gilt:

$$(P \cdot Q)' = P'Q + PQ'.$$

Beweis. Sei $P = \sum_{i=0}^{n} a_i X^i$ und $Q = \sum_{j=0}^{m} b_j X^j$. Wir berechnen zuerst die linke Seite:

$$\begin{aligned}
&(P \cdot Q)' = \\
&= ((a_0 + a_1X + \cdots + a_nX^n)(b_0 + b_1X + \cdots + b_mX^m))' \\
&= (a_0b_0 + (a_1b_0 + a_0b_1)X + (a_0b_2 + a_1b_1 + a_2b_0)X^2 + \cdots + a_nb_mX^{m+n})' \\
&= (a_1b_0 + a_0b_1) + 2(a_0b_2 + a_1b_1 + a_2b_0)X + \cdots + (n+m)(a_nb_m)X^{n+m-1}.
\end{aligned}$$

Die rechte Seite berechnen wir in mehreren Schritten:

$$
\begin{aligned}
&(P'Q) = \\
&= (a_1 + 2a_2X + \cdots + na_nX^{n-1})(b_0 + b_1X + b_2X^2 + \cdots + b_mX^m) \\
&= a_1b_0 + 2a_2b_0X + a_1b_1X + \cdots + na_nb_mX^{n+m-1} \\
&(PQ') = \\
&= (a_0 + a_1X + a_2X^2 + \cdots + a_nX^n)(b_1 + 2b_2X + \cdots + mb_mX^{m-1} \\
&= a_0b_1 + a_1b_1X + 2a_0b_2X + \cdots + ma_nb_mX^{n+m-1} \\
&P'Q + PQ' = \\
&= (a_0b_1 + a_1b_0) + 2(a_0b_2 + a_1b_1 + a_2b_0)X + \cdots + (m+n)a_nb_mX^{m+n-1}
\end{aligned}
$$

□

Definition 21. Sei L/K eine Körpererweiterung, dann heißt $a \in L$ *r-fache Wurzel* oder *Wurzel der Vielfachheit* r von $P \in K[X]$, wenn

$$P = (X-a)^r Q \text{ mit } Q(a) \neq 0.$$

Wenn $r = 1$ so heißt a einfache Wurzel, sonst ($r > 1$) mehrfache Wurzel.

Beispiel 15. Wir betrachten das Polynom $P = X^3 - 4X^2 - 3X + 18 \in \mathbb{Q}[X]$, so lässt sich P in der Form $P = (X-3)^2(X+2)$ darstellen. Also hat P die zweifache Wurzel 3 und die einfache Wurzel -2.

Lemma 5.2. Ein Polynom $P \in K[X]$ hat genau dann eine mehrfache Wurzel, wenn im Zerfällungskörper L die Polynome P und P' eine gemeinsame Wurzel haben.

Beweis. ($\Rightarrow$)Sei a eine r-fache Wurzel von P, so lässt sich P nach Definition 21 schreiben als:

$$P = (X-a)^r Q \text{ mit } Q(a) \neq 0 \text{ und } r > 1.$$

Die Ableitung von P sieht so aus:

$$P' = r(X-a)^{r-1}Q + (X-a)^r Q' = (X-a)^{r-1}(rQ + (X-a)Q').$$

So haben P und P' eine gemeinsame Wurzel.
($\Leftarrow$) Angenommen a ist eine einfache Wurzel von P, dann lässt sich P der Form $P = (X-a)Q$ mit $Q(a) \neq 0$ darstellen. Die Ableitung von P ist $P' = (X-a)Q' + Q$. Daraus folgt $P'(a) \neq 0$. Das ist ein Widerspruch zu P und P' haben eine gemeinsame Wurzel. □

Lemma 5.3. Sei L ein Zerfällungskörper von $P \in K[X]$ und P irreduzibel über K, dann gilt: P hat genau dann mehrfache Wurzeln in L, wenn $P' = 0$

Beweis. ($\Rightarrow$)Indirekt: Angenommen P' ist nicht das Nullpolynom, so hat es nach Definition einen kleineren Grad als P. Ein gemeinsamer Teiler $D \in K[X]$ von P und P' hat also auch kleineren Grad als P. Da aber P irreduzibel über K ist, kann D nur eine Konstante sein. Also kann P nach Lemma 5.2 keine mehrfachen Wurzeln haben.
($\Leftarrow$) Sei P' das Nullpolynom, so ist P selbst gemeinsamer Teiler von P und P', also hat P mehrfache Wurzeln. □

Beispiel 16. Wir betrachten das Polynom $P = X^5 + 5X + 5 \in \mathbb{Q}[X]$. Nach dem Eisensteinkriterium mit $p = 5$ ist P irreduzibel. Aufgrund von Satz 5.3 hat P nur einfache Wurzeln, da die Ableitung $P' \neq 0$.

Definition 22. Ein Polynom $P \in K[X]$ nennt man *separabel*, wenn jeder irreduzible Faktor von P in einem Zerfällungskörper von P über K nur einfache Wurzeln hat. Sei L/K eine Körpererweiterung, ein Element $a \in L$ heißt *separabel* über K, wenn a über K algebraisch ist und sein Minimalpolynom $m_{a,K}$ separabel ist. L/K heißt *separabel*, wenn jedes Element aus L seperabel über K ist. Eine nichtseperables Polynom bzw. eine nichtsperable Körpererweiterung heißt auch *inseperabel*.

Bemerkung. Der Zerfällungskörper ist bis auf K-Isomorphie eindeutig, also hängt die Definition nicht von der Wahl des Zerfällungskörper ab.

Korollar 5.4. Seien $P, Q \in K[X]$ separabel, dann ist auch $P \cdot Q$ separabel.

Beweis. Jeder der irreduziblen Faktoren der Polynome P und Q haben in ihrem jeweiligen Zerfällungskörper nur einfache Nullstellen. Wir betrachten das Polynom $P \cdot Q$ und zerlegen es in irreduzible Faktoren. Der Zerfällungskörper von $P \cdot Q$ erweitert den jeweiligen von P und von Q. Also hat das Polynom $P \cdot Q$ in seinem Zerfällungskörper nur einfache Wurzeln und ist nach Definition separabel. □

Für die weiteren Betrachtungen spielt die Charakteristik eine große Rolle, die wie folgt definiert ist:

Definition 23. Sei K ein Körper und $M = \{k \in \mathbb{N} \mid k1 = 0\}$. Falls $M \neq \emptyset$, sagt man der Körper K hat die Charakteristik $CharK = minM$. Im Fall $M = \emptyset$ hat der Körper K die Charakteristik $CharK = 0$.

Lemma 5.5. Sei K ein Körper und $charK \neq 0$, dann ist $charK = p$ eine Primzahl.

Beweis. Sei $p > 0$ die Charakteristik von K und $p = rs$, wobei $r, s \in \mathbb{N}$. Wir betrachten die Elemente $r1_K \in K$ und $s1_K \in K$ so gilt $0_K = p1 = (r1)(s1)$. Da K als Körper keine Nullteiler besitzt, folgt, dass $r1 = 0$ oder $s1 = 0$. Da $r \leq p$ und $s \leq p$ gilt, $r = p$ oder $s = p$. □

Definition 24. Sei K ein Körper und $p = charK$ eine Primzahl dann heißt $\Psi : K \to K$ mit $a \mapsto a^p$ *Frobeniusabbildung.*

Lemma 5.6. Sei K ein Körper und $charK = p > 0$, dann ist die Frobeniusabbildung ein Homomorphismus.

Beweis. Seien $x, y \in K$. Es gilt $\binom{p}{i} \equiv 0(p)$ für alle $i \in \{1, \cdots, p-1\}$, denn $\binom{p}{i} = \frac{p!}{i!(p-i)!}$ und der Faktor p kommt im Nenner nicht vor.
Für die Addition gilt:

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

Für die Multiplikation gilt:

$$\Psi(xy) = (xy)^p = x^p y^p = \Psi(x)\Psi(y).$$

□

Bemerkung. Nach Lemma 3.2 ist jeder Homomorphismus zwischen zwei Körpern injektiv, so auch die Frobeniusabbildung.

Lemma 5.7. Sei K ein Körper, wenn K die Charakterisitk 0 hat, so ist jedes nichtkonstante Polynom separabel.

Beweis. Die einzigen Polynome P mit Ableitung $P' = 0$ sind in diesem Fall die konstanten Polynome $P = c$ mit $c \in K$. Nach Satz 5.3 hat also dann jedes irreduzible Polynom nur einfache Wurzeln. Das gilt auch für die irreduziblen Faktoren eines beliebigen nichtkonstanten Polynom. □

Bemerkung. Bei einem Körper K mit $charK = 0$ ist jede algebraische Körpererweiterung separabel.

Satz 5.8. Sei K ein Körper und $charK = p > 0$, dann gilt, ein irreduzibles Polynom $P \in K[X]$ ist genau dann inseparabel, wenn ein $Q \in K[X]$ mit $P(X) = Q(X^p)$ existiert, das bedeutet $P(X) = \sum_{i=0}^{d} c_i X^{ip}$ mit $c_0, \ldots, c_d \in K$.

Beweis. Sei also $charK = p > 0$, weiters sei

$$P = \sum_{i=0}^{n} k_i X^i \text{ und } P' = \sum_{i=1}^{n} i k_i X^{i-1}.$$

Für das Polynom P, welches nach Voraussetzung irreduzibel ist, gilt: P ist genau dann inseparabel, wenn $P' = 0$. Das ist gleichbedeutend mit $ik_i = 0$ für alle $i \in \{1, \cdots, n\}$. Die Koeffizienten ik_i verschwinden genau dann, wenn $p \mid i$ oder $k_i = 0$. Wenn die k_i für jedes nicht durch p teilbare i verschwinden, also wenn in diesem Fall $k_i = 0$ gilt, dann ist P' das Nullpolynom. P' ist genau dann das Nullpolynom, wenn ein $Q \in K[X]$ existiert mit $P(X) = Q(X^p)$. Wenn P' das Nullpolynom ist, dann muss wegen dem zuvor Erwähnten so ein Polynom Q existieren. Wenn es nun so ein besagtes Q gibt, dann ist $P' = \sum_{i=1}^{d} ipc_i X^{ip-1}$ und das ist das Nullpolynom. □

Satz 5.9. Seien L/K eine Körpererweiterung, a algebraisch über K und $charK = p > 0$. Das Element a ist genau dann separabel über K wenn $K(a^p) = K(a)$ ist.

Beweis. ($\Rightarrow$) Sei a separabel über K, dann ist a auch separabel über $K(a^p)$, da $m_{a,K(a^p)} \mid m_{a,K}$. Das folgt aus $K \subseteq K(a^p)$. Wegen $a^p \in K(a)$ gilt $K(a^p) \subseteq K(a)$. Wenn wir zeigen, dass $a \in K(a^p)$ liegt, dann folgt die Gleichheit. Das Element a ist eine Wurzel von $(X-a)^p \overset{Lemma\ 5.6}{=} X^p - a^p \in K(a^p)[X]$ wegen der Separabilität von a und aufgrund der Eigenschaften des Minimalpolynoms gilt $m_{a,K(a^p)} = X - a$. Somit ist $a \in K(a^p)$, also $K(a) = K(a^p)$
($\Leftarrow$) Indirekt: Angenommen a ist inseparabel über K. Nach dem Satz 5.8 existiert für das nach Lemma 1.4 irreduzible Minimalpolynom $m_{a,K}$ ein $Q \in K[X]$ mit $m_{a,K}(X) = Q(X^p)$. Für das Element a^p gilt $Q(a^p) = 0$. Das Minimalpolynom $m_{a^p,K}$ hat also kleineren oder gleichen Grad wie Q. Es gilt da p eine Primzahl ist:

$$[K(a) : K] = deg\ m_{a,K} > deg Q \geq [K(a^p) : K].$$

Daraus folgt $K(a) \neq K(a^p)$. Das steht im Widerspruch zur Voraussetzung. □

Definition 25. Einen Körper K nennt man *vollkommen*, wenn jedes Polynom aus $K[X]$ separabel ist.

Satz 5.10. Ein Körper K ist genau dann vollkommen, wenn $charK = 0$ oder $charK = p > 0$ mit der Eigenschaft, dass die Frobeniusabbildung ein Automorphismus ist.

Beweis. Im Fall $charK = 0$ ist nichts mehr zu zeigen, da jedes Element ein separables Minimalpolynom besitzt, weil nach Satz 5.7 jedes Polynom separabel ist. Also ist nur der Fall mit $charK = p$ zu zeigen.
($\Rightarrow$) Indirekt: Angenommen die Frobeniusabbildung ist nicht surjektiv. So existiert ein $a \in K \setminus \Psi(K)$. Wir zeigen, dass $X^p - a$ ein irreduzibles Polynom in $K[X]$ mit p-facher Nullstelle ist.
Es existiert kein $k \in K$, sodass $\Psi(k) = k^p = a$. Also sei b eine Wurzel in einem Erweiterungskörper, bzw. in dem Zerfällungskörper, der ja existiert. Dann ist $b^p = a$ und daher $(X-b)^p = \sum_{i=0}^{p} \binom{p}{i} X^i b^{p-i} = X^p - b^p = X^p - a$. Wäre nun das Polynom nicht irreduzibel, so gäbe es einen reduziblen Faktor der Gestalt $(X-b)^j$ für ein $j \in \{1, \cdots, p-1\}$. Insbesondere wäre $b^j \in K$, da das der konstante Term des Polynoms wäre. Da p eine Primzahl ist, sind j und p relativ prim, daher existieren m, l mit $1 = jm + lp$. Dann gilt $b = b^{jm+lp} = (b^j)^m (b^l)^p = (b^j)^m a^l \in K$. Daher ist dann auch $a = b^p \in \Psi(K)$. Das steht im Widerspruch zur Wahl von a, daher ist $X^p - a$ irreduzibel in $K[X]$. Es wurde also ein irreduzibles Polynom mit p-facher Nullstelle in einem Zerfällungskörper gefunden, das ist ein Widerspruch zu der Voraussetzung, dass K vollkommen ist.
($\Leftarrow$) Indirekt: Sei Ψ surjektiv und $P \in K[X]$ ein irreduzibles Polynom. Angenommen P ist inseparabel. Dann gibt es nach Satz 5.8 ein Polynom $Q(X) = \sum_{i=0}^{n} a_i X^i \in K[X]$ mit $P(X) = Q(X^p)$. Für die Koeffizienten gilt aufgrund der Surjektivität $a_i = \Psi(b_i) = b_i^p$ mit $b_i \in K$ für alle $i \in \{1, \cdots, n\}$. Aufgrund der Eigenschaft des Binomialkoeffizienten $\binom{p}{i} \equiv 0(p)$ für $i \notin \{0, p\}$ in einem Körper mit $charK = p$ kann man folgern:

$$P(X) = \sum_{i=0}^{n} b_i^p X^{ip} = (\sum_{i=0}^{n} b_i X^i)^p.$$

Das steht im Widerspruch mit der Irreduzibilität von P, da es nun zerlegbar ist. □

Für den Satz vom primitiven Element benötigen wir noch eine Aussage über Untergruppen der multiplikativen Gruppe eines Körpers K.

Hilfssatz 5.11. Sei K ein Körper und U eine endliche Untergruppe der Ordnung $n \in \mathbb{N}$ der multiplikativen Gruppe K^*, dann ist U eine zyklische Gruppe.

Beweis. Wir verwenden dafür den Satz (vgl. [5], S. 131), dass jede endliche abelsche Gruppe isomorph zu dem direkten Produkt zyklischer Untergruppen ist. Genauer gilt

$$U \cong \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_k\mathbb{Z}$$

für ein eindeutig bestimmtes $k \in \mathbb{N}$ und $d_1|d_2|\cdots|d_k$, wobei $n = d_1 \cdot \ldots \cdot d_k$. Wir betrachten nun ein Element des Produktes so gilt, dass die Ordnung dieses Elements d_k teilt. Denn alle d_i mit $i \in \{1, \ldots, k\}$ teilen d_k. Daraus folgt, dass jedes Element aus U eine Nullstelle des Polynoms $X^{d_k} - 1$ ist. Diese Polynom hat aber höchstens d_k verschiedene Nullstellen in K. Die Untergruppe U besteht aber aus n Elementen mit $n = d_1 \cdot \ldots \cdot d_k$, dann gilt $n = d_k$ und $k = 1$. Also ist U zyklisch. □

In der klassichen Formulierung lautet der Satz vom primitiven Element folgendermaßen:

Satz 5.12 (Satz vom primitiven Element)**.** Sei L/K eine endliche separable Körpererweiterung, dann existiert ein primitives Element $a \in L$ mit $L = K(a)$.

Dieser folgt als Korollar aus diesem Satz:

Satz 5.13. Sei L/K eine Körpererweiterung der Form $L = K(a, c_1, \ldots, c_n)$, wobei a algebraisch über K ist und $c_1, \ldots, c_n$ separabel über K sind. Dann existiert ein Element $e \in L$ mit $L = K(e)$, sodass die Erweiterung einfach ist.

Beweis. Dieser Satz bedarf einer Fallunterscheidung, denn K kann eine endliche Mächtigkeit haben oder nicht:
1. Fall: $|K| \in \mathbb{N}$, der Körper L kann, wie am Beginn der Arbeit erwähnt, auch als Vektorraum über K betrachtet werden. Da nur endlich viele Elemente hinzugefügt werden und K endlich ist, ist auch L als endlich dimensionaler Vektorraum über dem Körper K selbst endlich. Der Hilfssatz 5.11 besagt, dass die multiplikative Gruppe L^* zyklisch ist, das heißt, es existiert ein Element $a \in L$, sodass $L^* = \langle a \rangle$. Daher folgt $L = K(a)$ und das primitive Element wurde im endlichen Fall gefunden.
2. Fall: $|K| \notin \mathbb{N}$, es genügt die Aussage für eine Körpererweiterung $K(a, c)$ mit c separabel zu zeigen. Denn es gilt $L = K(a, c_1, \ldots, c_{n-1})(c_n)$, mittels Induktion kann dann im Induktionsschritt die Behauptung für $n-1$ Elemente vorausgesetzt werden, für die gibt es also dann ein Element e_{n-1}. Man erhält $K(e_{n-1})(c_n) = K(e_{n-1}, c_n)$. Sei nun $n = 1$ und $b := c_1$. Es gilt nun ein Element e zu finden, sodass $K(a, b) = K(e)$ ist. Sei $P = m_{a,K}$ und $Q = m_{b,K}$ die jeweiligen Minimalpolynome über K. Sei M der Zerfällungskörper von PQ über $K(a, b)$. Seien $a = a_1, \ldots, a_r$ und $b = b_1, \ldots, b_s$ die Wurzeln der Minimalpoylnome in M. Falls $s = 1$, ist b die einzige Wurzel von $m_{b,K}$ und b ist nach Voraussetzung separabel. Daher hat das Minimalpolynom nur einfache Wurzeln und nur eine Nullstelle. In diesem Fall gibt es nur eine Wurzel, das führt zu $degQ = 1$. Aus dem Erwähnten folgt, dass $b \in K$ ist.

Für die folgenden Überlegungen sei $s \geq 2$. Es gilt $K(a,b) = K(e)$ zu zeigen. Jedes $e \in K(a,b)$ ist von der Form $e = ca + db$ mit $c, d \in K^*$. Wenn man durch c durchdividiert, erhält man $\alpha e = a + \gamma' b$ mit $\frac{1}{c} = \alpha$ und $\gamma' = \frac{d}{c}$. Da $K(\alpha e) = K(e)$ für alle $\alpha \in K$, betrachtet man $e = a + \gamma' b$ mit $\gamma' \in K$. Es existiert ein $\gamma \in K \setminus \{(a_j - a)(b - b_i)^{-1} \mid 1 \leq j \leq r, 2 \leq i \leq s\}$ da $|K| \notin \mathbb{N}$. Es gilt:

$$\begin{aligned} a + \gamma b = a_j + \gamma b_i &\Leftrightarrow a_j - a = \gamma(b - b_i) \\ &\Leftrightarrow \gamma = \frac{a_j - a}{b - b_i} \end{aligned}$$

daraus folgt nach der Wahl von γ:

$$e = a + \gamma b \notin \{a_j + \gamma b_i \mid 1 \leq j \leq r, 2 \leq i \leq s\}.$$

Das Polynom $P(e - \gamma X)$ liegt in $K(e)[X]$, da $e \in K(e)$ und $\gamma \in K \subseteq K(e)$ ist. $K(e)$ ist ein Körper, daher ist $K(e)[X]$ ein Hauptidealring mit Gradfunktion als Normfunktion. Dadurch lässt sich der ggT betrachten. Es existiert ein normiertes Polynom $D = ggT(Q, P(e - \gamma X))$. Da wir uns eben in einem Hauptidealbereich befinden, existieren Polynome $F, G \in K(e)[X]$ mit $D = FQ + GP(e - \gamma X)$. Da $Q = m_{b,K}$ ist, gilt $Q(b) = 0$ und $P(e - \gamma b) = P(a) = 0$, da $P = m_{a,K}$ ist, so erhalten wir b als Nullstelle von D. Alle Wurzeln von D liegen in der Menge $\{b_1, \ldots, b_s\}$, da $D \mid Q$. Für jedes $j \in \{1, \ldots, r\}$ und $i \geq 2$ gilt $e - \gamma b_i \neq a_j$ aufgrund des Argumentes weiter oben. Dadurch hat $P(e - \gamma X)$ nach b keine weitere Nullstelle. Da $D \mid P(e - \gamma X)$ gilt auch $D(b_i) \neq 0$ für $2 \leq i \leq s$. Also ist b die einzige Wurzel von D in M. Das Polynom D hat eine Form $D = (X - b)^t$ für ein $t \geq 1$. Da D ja der ggT der beiden Polynome ist, gilt $(X - b)^t \mid Q$. Da Q das Minimalpolynom eines separablen Elementes ist, hat Q nur einfache Wurzeln, somit ist $t = 1$. Also ist aber $X - b = D \in K(e)[X]$ und dadurch ist $b \in K(e)$, sowie $a = e - \gamma b \in K(e)$. Es wurde nun gezeigt, dass $a, b \in K(e)$ liegen, es gilt also $K(e) = K(a,b)$. Daraus folgt Satz 5.12 in seiner üblichen Form. □

Beispiel 17. Besitzt die Körpererweiterung $\mathbb{Q}(\sqrt[3]{3}, \sqrt{2})/\mathbb{Q}$ ein primitives Element? Ja, da die Charakteristik von $\mathbb{Q}$ gleich 0 ist und nach Lemma 5.7 ist jedes Polynom separabel über $\mathbb{Q}$. Das gilt insbesondere für die Minimalpolynome der Elemente $\sqrt[3]{3}$ und $\sqrt{2}$. Es kann der Satz vom primitven Element 5.12 angewandt werden. Wir versuchen ein solches Element wie im obigen Beweis zu konstruieren. Wir betrachten die Minimalpolynome $P = X^3 - 3$ für $\sqrt[3]{3}$ und $Q = X^2 - 2$ für $\sqrt{2}$ beide über $\mathbb{Q}$. Die Nullstellen von P sind $a = a_1 = \sqrt[3]{3}, a_2 = \zeta\sqrt[3]{3}, a_3 = \zeta\sqrt[3]{3}$ wobei $\zeta = e^{\frac{2\pi i}{3}} = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$. Für Q ergibt sich $b = b_1 = \sqrt{2}, b_2 = -\sqrt{2}$. Erstelle nun die Menge aus der γ nicht gewählt

werden darf:

$$R = \{(a_j - a)(b - b_i)^{-1} | 1 \leq j \leq 3, i = 2\} = \left\{0, \frac{a_2 - a}{b - b_2}, \frac{a_3 - a}{b - b_2}\right\} =$$

$$\left\{0, \frac{\zeta\sqrt[3]{3} - \sqrt[3]{3}}{\sqrt{2} + \sqrt{2}}, \frac{\zeta^2\sqrt[3]{3} - \sqrt[3]{3}}{\sqrt{2} + \sqrt{2}}\right\}.$$

Wir wählen nun ein $\gamma \in \mathbb{Q} \setminus R$, wie zum Beispiel 1. Nach dem Satz 5.12 kann $c = a + b = \sqrt[3]{3} + \sqrt{2}$ als primitives Element gewählt werden. Die Körpererweiterung $\mathbb{Q}(\sqrt[3]{3}, \sqrt{2})/\mathbb{Q}$ kann geschrieben werden als $\mathbb{Q}(\sqrt[3]{3}+\sqrt{2})/\mathbb{Q}$.

Für das nächste Kapitel werden noch Eigenschaften von separablen Erweiterungen, sowie der Begriff des Separabilitätsgrad benötigt.

Satz 5.14. Jede einfache algebraische Erweiterung $K(a)$ von K ist genau dann separabel, wenn a separabel ist.

Beweis. ($\Rightarrow$) Sei $K(a)/K$ separabel, so folgt per Definition, dass alle $x \in K(a)$ separabel über K sind, insbesondere auch a.
($\Leftarrow$) Sei a separabel über K. Im Fall $charK = 0$ gilt nach Satz 5.10, dass K vollkommen ist und daher ist jede algebraische Erweiterung separabel über K. Wir betrachten nun den Fall $charK = p > 0$. Es gilt nach Satz 5.9, dass $K(a) = K(a^p)$, da a separabel ist. Sei nun $b \in K(a)$ beliebig mit $n = [K(a) : K]$ und $d = [K(b) : K]$. Dann sind $\{1, a, \ldots, a^{n-1}\}$ und $\{1, a^p, \ldots, (a^p)^{n-1}\}$ K-Basen von $K(a)$. Eine K-Basis von $K(b)$ stellt $B = \{1, b \ldots, b^{d-1}\}$ dar. Man kann B nun zu einer K-Basis von $K(a)$ erweitern, $\{u_1, \ldots, u_n\}$. Dann gilt, dass jedes a^i die Form:

$$a^i = \sum_{i=0}^{n} k_i u_i \text{ mit } k_i \in K$$

hat. Mit Hilfe des Frobeniushomomorphismus lassen sich die $(a^p)^i$ so darstellen: $a^{ip} = \sum_{i=0}^{n} k_i^p u_i^p$. Aus diesem Grund ist nun $\{u_1^p, \ldots, u_n^p\}$ ein K-Erzeugendensystem bestehend aus n Elementen, daher eine K-Basis von $K(a)$ und daher linear unabhängig. Daraus lässt sich die K-lineare Unabhängigkeit von $\{1, b^p, \ldots, (b^p)^{d-1}\}$ folgern. Aus $K(b^p) \subseteq K(b)$ folgt $[K(b^p) : K] \leq d$, da $\{1, b^p, \ldots, (b^p)^{d-1}\}$ linear unabhängig sind folgt $d \leq [K(b^p) : K]$. Wir erhalten also $[K(a^p) : K] = d$ und daraus die Gleichheit von $K(b) = K(b^p)$. Nach Satz 5.9 ist b separabel. □

Bemerkung. Ist L/K eine Körpererweiterung und $M \subseteq L$ eine Menge von separablen Elementen über K, so ist die Körpererweiterung $K(M)/K$ separabel: denn $K(M) = \bigcup_{N \subseteq M,\, N\, endlich} K(N)$ und jedes $K(N)$ ist separabel.

Definition 26. Sei L/K eine algebraische Körpererweiterung und $\bar{K}$ ein algebraischer Abschluss von K, dann ist der Separabilitätsgrad $[L:K]_s$ von L/K definiert als die Anzahl der verschiedenen K-Homomorphismen von L nach $\bar{K}$.

Die Definition hängt nicht von der Wahl des algebraischen Abschlusses $\bar{K}$ von K ab.

Satz 5.15. Sei L/K eine endliche Körpererweiterung, dann gilt für jeden Zwischenkörper Z:

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

Beweis. Sei $(\varphi_i)_{i\in I}$ die Familie paarweise verschiedener K-Homomorphismen von Z nach $\bar{K}$ mit $|I| = [Z:K]_s$. Sei $(\tau_j)_{j\in J}$ die Familie paarweise verschiedener Z-Homomorphismen von L nach $\bar{Z}$ wobei $|J| = [L:M]_s$ ist. Wir wählen einen algebraischen Abschluss $\bar{K}$ von K mit $K \subseteq Z \subseteq L \subseteq \bar{K}$. Dieser Abschluss ist nun auch algebrasicher Abschluss von Z und L. Also lässt sich τ_i als K-Homomorphismus von L nach $\bar{K}$ betrachten. Wir wollen nun die K-Homomorphismen φ_i erweitern. Nach Korollar 3.12 können wir jedes φ_i zu einem K-Automorphismus $\bar{\varphi_i}$ von $\bar{K}$ nach $\bar{K}$ erweitern. Wir betrachten nun die zusammengesetzten K-Homomorphismen $\bar{\varphi_i} \circ \tau_j$ mit $i \in I$ und $j \in J$ von L nach $\bar{K}$. Als nächstes wird gezeigt: Wenn $\bar{\varphi_{i_1}} \circ \tau_{j_1} = \bar{\varphi_{i_2}} \circ \tau_{j_2}$ gilt, dann ist $\varphi_{i_1} = \varphi_{i_2}$ und $\tau_{j_1} = \tau_{j_2}$. Sei also $\bar{\varphi_{i_1}} \circ \tau_{j_1} = \bar{\varphi_{i_2}} \circ \tau_{j_2}$. Wir beschränken die Abbildungen auf Z, dann sind τ_{i_1} und τ_{i_2} gleich der Identität, da sie Z-Homomorphismen sind. Daraus folgt aber, dass $\varphi_{i_1} = \varphi_{i_2}$ ist. Dann gilt auch für die Erweiterungen die Gleichheit $\bar{\varphi_{i_1}} = \bar{\varphi_{i_2}}$. Es folgt $\tau_{j_1} = \tau_{j_2}$. Die Abbildungen $\bar{\varphi_i} \circ \tau_j$ mit $i \in I$ und $j \in J$ sind also paarweise verschieden. Es bleibt noch zu zeigen, dass wir so alle K-Homomorphismen erhalten. Sei also σ ein beliebiger K-Homomorphismus von L nach $\bar{K}$. Wir schränken σ auf Z ein, so ist $\sigma_{|Z}$ ein K-Homomorphismus Z nach K. Es existiert ein $i \in I$ mit $\sigma_{|Z} = \varphi_i$. Die Abbildung $\bar{\varphi_i}^{-1} \circ \sigma$ ist also ein Z-Homomorphismus von L nach $\bar{K}$. Es existiert ein $j \in J$, sodass $\bar{\varphi_i}^{-1} \circ \sigma = \tau_j$ ist. Wir erhalten $\sigma = \bar{\varphi_i} \circ \tau$. Somit hat jeder beliebige K-Homomorphismus die Form $\bar{\varphi_i} \circ \tau_j$. Es folgt die Behauptung. □

6 Galoistheorie

Wie viele Zwischenkörper hat eine Körpererweiterung L/K? Eigentlich kann bis jetzt keine exakte Antwort auf diese Frage gegeben werden. Mit Hilfe der entwickelten Begrifflichkeiten aus den vorigen Kapiteln und neuen aus dem folgenden Abschnitt ist man in der Lage diese ganz genau zu beantworten. Jedoch bedarf es spezieller Körpererweiterungen, nämlich endlicher Galoiserweiterungen. Die Faszination liegt darin, dass die Zwischenkörperproblematik auf das Finden von Untergruppen der Galoisgruppe reduziert werden kann. Das Auffinden von Untergruppen ist vergleichsweise wesentlich einfacher. Als nützlich erweist sich die Galoistheorie zu Beantwortung der Frage, welche regelmäßigen n-Ecke konstruierbar sind. Diese Anwendung wird in einem späteren Kapitel behandelt. Um das Ziel, den Hauptsatz der endlichen Galoistheorie zu beweisen, werden zuvor Galoisgruppen, Fixkörper, Galoiserweiterungen und deren Eigenschaften behandelt. Abschließend wird anhand eines Beispiels das Auffinden der Zwischenkörper einer gegebenen Körpererweiterung mit Hilfe des Hauptsatzes illustriert. Die verwendete Literatur umfasst die Werke „Algebra“ von Artin (Kapitel 14.1, [2]), „Algebra“ von Bosch (Kapitel 3.4, [4]), „Algebra“ von Jantzen und Schwermer (Kapitel V §5, [7]), „Algebra“ von Karpfinger und Meyberg (Kapitel 24, [9]) und „Galois-Theorie“ von Staudner (Kapitel V und VI, [13]).

Definition 27. Sei L/K eine Körpererweiterung. Nach Satz 3.1 bildet die Menge $Aut_K(L)$ eine Gruppe. Diese Gruppe heißt nun *Galoisgruppe* und wird mit $\Gamma(L/K)$ bezeichnet.

Beispiel 18. Wir betrachten die Körpererweiterung $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$. Welche Elemente enthält $\Gamma(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$? Das Minimalpolynom $m_{\sqrt{2},\mathbb{Q}} = X^2-2$ hat neben $\sqrt{2}$ eine zweite Nullstelle $-\sqrt{2}$. Nach Satz 3.4 existiert ein Isomorphismus:

$$\varphi : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(-\sqrt{2})$$

mit $\varphi(\sqrt{2}) = -\sqrt{2}$, der $\mathbb{Q}$ fix lässt. Die Körper $\mathbb{Q}(\sqrt{2})$ und $\mathbb{Q}(-\sqrt{2})$ sind identisch, also ist φ ein Automorphismus. Weiters gilt $\varphi(-\sqrt{2}) = \sqrt{2}$, also bildet φ^2 das Element $\sqrt{2}$ auf sich selbst ab. Da $\sqrt{2}$ den Körper $\mathbb{Q}(\sqrt{2})$ über $\mathbb{Q}$ erzeugt, ist φ selbstinvers. Also sind φ und die Identitätsabbildung Id Elemente der Galoisgruppe der betrachteten Körpererweiterung. Es könnte jedoch sein, dass eine weitere Abbildung existiert!
Sei $\tau \in \Gamma(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$. Wir betrachten das Element $\sqrt{2}$ als Nullstelle von $m_{\sqrt{2},\mathbb{Q}}$, so muss $\tau(\sqrt{2})$ auch eine Nullstelle von $m_{\sqrt{2},\mathbb{Q}}$, siehe Beweis von Lemma 3.3. Es kann $\sqrt{2}$ nur auf sich selbst oder $-\sqrt{2}$ abgebildet werden, dann ist aber $\tau = id$ oder $\tau = \varphi$. Also waren $\{Id, \varphi\}$ alle Elemente der Galoisgruppe $\Gamma(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$.

Lemma 6.1. Für jede Menge Δ von Automorphismen eines Körpers L gilt, dass

$$\mathcal{F}(\Delta) = \{a \in L \mid \delta(a) = a, \forall \delta \in \Delta\}$$

ein Teilkörper von L ist.

Beweis. Sei $\delta \in \Delta$ beliebig und $a, b, c \in \mathcal{F}(\Delta)$, wobei $c \neq 0$, dann gilt durch

- $\delta(a - b) = \delta(a) - \delta(b) = a - b$
- $\delta(ab) = \delta(a)\delta(b) = ab$
- $\delta(c^{-1}) = \delta(c)^{-1} = c^{-1}$

dass $a - b, ab, c^{-1} \in \mathcal{F}(\Delta)$ sind. □

Definition 28. Der Körper $\mathcal{F}(\Delta)$ in Lemma 6.1 heißt *Fixkörper* von Δ.

Definition 29. Eine Körpererweiterung L/K wird *galoissch* genannt, wenn der Fixkörper der Galoisgruppe $\Gamma(L/K)$ gleich K ist, also

$$\mathcal{F}(\Gamma(L/K)) = \{a \in L \mid \delta(a) = a, \forall \delta \in \Gamma(L/K)\} = K.$$

Lemma 6.2. Sei L/K eine endliche Körpererweiterung, dann gilt folgende Ordnungsabschätzung

$$|\Gamma(L/K)| \leq [L : K]_s \leq [L : K].$$

Beweis. Es sind zwei Ungleichungen zu zeigen:

- $|\Gamma(L/K)| \leq [L : K]_s$
  Nach Definition bezeichnet $[L : K]_s$ die Anzahl der verschiedenen K-Homomorphismen von L nach $\bar{K}$ und $|\Gamma(L/K)|$ die Anzahl der verschieden K-Automorphismen von L nach L. Es gilt für die Körper, dass $K \subseteq L \subseteq \bar{K}$. Somit ist jeder K-Automorphismus von L auch ein K-Homomorphismus von L nach $\bar{K}$. Die Umkehrung gilt im Allgemeinen nicht, daraus resultiert die Ungleichung.

- $[L : K]_s \leq [L : K]$
  Wir beweisen die Aussage mittels Induktion nach der minimalen Anzahl der algebraischen Erweiterungselemente $K(a_1, \ldots, a_n)$
  Für den Induktionsanfang: Sei $n = 1$, $L = K(a_1)$
  Der Separabilitätsgrad $[L : K]_s$ ist gleich der Anzahl der verschiedenen Nullstellen des Minimalpolynoms $m_{a_1,K}$, denn aufgrund von Lemma 3.5

gibt es für jede Nullstelle von $m_{a_1,K}$ genau einen Homomorphismus. In diesem Fall entspricht $L = K(a_1)$. Nur wenn a_1 seperabel ist, also $m_{a_1,K}$ keine mehrfachen Nullstellen hat, folgt dass $[L : K]_s = [L : K]$ ist, da nach Satz 1.6 für den Grad $deg\ m_{a_1,K} = [L : K]$ gilt. Wenn $m_{a_1,K}$ mehrfache Nullstellen besitzt, ergibt sich die Ungleichung $[L : K]_s \leq [L : K]$. Denn die Anzahl der unterschiedlichen Nullstellen wird kleiner und somit die der Homomorphismen, aber der Grad des Minimalpolynoms bleibt unverändert.
Für den Induktionsschritt von $n-1$ auf n ist aufgrund von Satz 5.15 und der Eigenschaft $K(a_1, \ldots, a_{n-1}, a_n) = K(a_1, \ldots, a_{n-1})(a_n)$ nochmals genau das gleiche Argument zu verwenden.

□

Korollar 6.3. Sei $K(a)/K$ eine einfache algebraische Körpererweiterung und sei a nicht separabel über K, dann gilt:

$$[K(a) : K]_s < [K(a) : K].$$

Beweis. Sei a nicht separabel über K, dann hat das Minimalpolynom $m_{a,K}$ eine mehrfache Nullstelle in einem Zerfällungskörper. Sei weiters $deg\ m_{a,K} = n$. Nach Satz 3.5 gibt es genau so viele Homomorphismen von $K(a)$ nach $\bar{K}$, wie $m_{a,K}$ Nullstellen in $\bar{K}$ hat. Es gilt nun nach Satz 1.6, dass $[K(a) : K] = n$. Das Minimalpolynom $m_{a,K}$ hat mindestens eine Nullstelle der Vielfachheit $r > 1$ in $\bar{K}$ hat, das bedeutet, dass es $n - r < n$ Homomorphismen von $K(a)$ nach $\bar{K}$ gibt. Also ist $[K(a) : K]_s < [K(a) : K]$. □

Lemma 6.4. Sei L/K eine endliche Körpererweiterung, dann ist $|\Gamma(L/K)| = [L : K]_s$ genau dann, wenn L/K normal ist.

Beweis. ($\Rightarrow$) Es gilt $|\Gamma(L/K)| = [L : K]_s$, dann ist die Anzahl der K-Automorphismen von L genauso groß wie die Anzahl der K-Homomorphismen von L nach $\bar{K}$. Jeder K-Automorphismus von L ist auch ein K-Homomorphismus von L nach $\bar{K}$ bzw. $\bar{L}$. Daher folgt für jeden K-Homomorphismus φ von L nach $\bar{L}$, dass $\varphi(L) = L$. Nach Satz 4.2 ist die Körpererweiterung nun normal.
($\Leftarrow$) Sei L/K normal, dann gilt nach Satz 4.2 für jeden K-Homomorphismus φ von L nach $\bar{L}$, dass $\varphi(L) = L$ ist. Die Tatsache $K \subseteq L \subseteq \bar{L}$ impliziert, dass $\bar{L}$ auch ein algebraischer Abschluss von K ist und dieser ist bis auf K-Isomorphie eindeutig. Die Anzahl der verschiedenen K-Homomorphismen von L nach $\bar{K}$ sind somit gleich der Anzahl der K-Automorphismen von L, daher gilt $|\Gamma(L/K)| = [L : K]_s$. □

Lemma 6.5. Für jede endliche Körpererweiterung L/K gilt $|\Gamma(L/K)| = [L : K]$ genau dann, wenn L/K normal und separabel ist.

Beweis. ($\Rightarrow$) Sei $|\Gamma(L/K)| = [L : K]$: nach Lemma 6.2 gilt für jede endliche Körpererweiterung die Ordnungsabschätzung

$$|\Gamma(L/K)| \leq [L : K]_s \leq [L : K].$$

Nach Verwendung der Voraussetzung folgt in diesem Fall

$$|\Gamma(L/K)| = [L : K]_s = [L : K].$$

Nach Aussage von Lemma 6.4 ist die Körpererweiterung normal, da die Gleichheit von $|\Gamma(L/K)| = [L : K]_s$ gilt. Es bleibt zu zeigen, dass aus $[L : K]_s = [L : K]$ die Separabilität von L/K folgt. Angenommen L/K ist nicht separabel, dann existiert ein Element $a \in L$, sodass $m_{a,K}$ mehrfache Nullstellen besitzt. Betrachte die Erweiterung $K(a)/K$, dann gilt nach Korollar 6.3, dass $[K(a) : K]_s < [K(a) : K]$. Daraus folgt mit Hilfe von Satz 1.1 und Satz 5.15:

$$[L : K] = [L : K(a)][K(a) : K] > [L : K(a)]_s[K(a) : K]_s = [L : K]_s = [L : K]$$

ein Widerspruch.
($\Leftarrow$) Die Umkehrung folgt ebenfalls aus Lemma 6.2 und 6.4. Denn aus der Eigenschaft normal folgt $|\Gamma(L/K)| = [L : K]_s$. Wenn L/K endlich und separabel ist, dann existiert nach Satz 5.12 ein Element $a \in L$, sodass $L = K(a)$. Die Erweiterung ist separabel, dadurch hat das Minimalpolynom von a über K nur einfache Nullstellen. Die Anzahl der verschiedenen K-Homomorphismen von L nach $\bar{K}$ ist dadurch gleich dem Grad von $m_{a,K}$. Also gilt $[L : K]_s = [L : K]$ und daher $|\Gamma(L/K)| = [L : K]$. □

Beispiel 19.

Wie sieht die Galoisgruppe $\Gamma(\mathbb{C}/\mathbb{R})$ aus? Es gilt $[\mathbb{C} : \mathbb{R}] = 2$. Nach Korollar 4.3 ist diese Körpererweiterung normal. Die Körpererweiterung $\mathbb{C}/\mathbb{R}$ ist algebraisch und $\mathbb{R}$ hat die Charakteristik 0. Es lässt sich Satz 6.5 anwenden, nach dem die Gleichheit von $|\Gamma(\mathbb{C}/\mathbb{R})| = [\mathbb{C} : \mathbb{R}]$ gilt. Nun ist die komplexe Konjugation $k : z \to \bar{z}$ ein Automorphimus in $\mathbb{C}$, der $\mathbb{R}$ fix lässt. Klarerweise hat diese Eigenschaften auch die Identitätsabbildung. Es wurden zwei Automorphismen mit Fixkörper $\mathbb{R}$ gefunden, es ergibt sich diese Galoisgruppe: $\Gamma(\mathbb{C}/\mathbb{R}) = \{Id, k\}$.

Wir betrachten nochmals die Körpererweiterung $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$, dessen Galoisgruppe wir schon im Beispiel 18 gefunden haben. Der Satz 6.5 bestätigt das

zuvor erhaltene Ergebnis, denn $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ ist normal, da sie nach Beispiel 4 den Grad 2 hat und sie ist separabel da es sich um eine algebraische Erweiterung handelt und $char\mathbb{Q} = 0$ gilt. Das heißt $\Gamma(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = 2$. Also sind die beiden, im Beispiel 18 gefunden Abbildungen die einzigen.

Definition 30. Sei L/K eine galoissche Körpererweiterung und a in L, dann nennt man die Elemente $\sigma(a)$ mit $\sigma \in \Gamma(L/K)$ *Konjungierte* von a.

Bei der folgenden Behauptung muss die Erweiterung nicht zwingend endlich sein, jedoch wird die Eigenschaft algebraisch vorausgesetzt.

Satz 6.6. Eine algebraische Körpererweiterung L/K ist genau dann galoissch, wenn L/K normal und separabel ist.

Beweis. ($\Rightarrow$) Sei L/K eine algebraische Galoiserweiterung und sei a in L. Betrachte nun die Menge aller Konjungierten von a:

$$N = \{\sigma(a) \mid \sigma \in \Gamma(L/K)\}.$$

Nach Lemma 3.3 ist jedes Element dieser Menge auch eine Nullstelle von $m_{a,K}$. Die Nullstellenmenge eines Polynoms ist endlich, so auch die Menge N. Daraus folgt, dass ein $\tau \in \Gamma(L/K)$ eine Permutation der Nullstellen von $m_{a,K}$ bewirkt. Seien $a_1, \ldots, a_n$ die Elemente aus N. Das Polynom

$$Q = \prod_{i=1}^{n}(X - a_i) \in L[X]$$

besitzt ausschließlich Koeffizienten aus K. Denn ein $\sigma \in \Gamma(L/K)$ bewirkt wie erwähnt nur eine Permutation der Elemente $a_1, \ldots, a_n$ somit gilt $\sigma(Q) = Q$. Aus diesem Grund liegen die Koeffizienten im Fixkörper $\mathcal{F}(\Gamma(L/K))$, der ist nach Voraussetzung gleich K. Das bedeutet, dass $Q \in K[X]$ ist. Wegen $Q(a) = 0$ ist $m_{a,K}$ ein Teiler von Q. Das Minimalpolynom $m_{a,K}$ ist also separabel. Das Element $a \in L$ wurde beliebig gewählt. Daher ist die Erweiterung separabel und normal.
($\Leftarrow$) Sei L/K normal und separabel und $a \in L \setminus K$. Das Element a ist nun per Definition auch separabel und da $a \notin K$ hat das Minimalpolynom $m_{a,K}$ eine weitere Wurzel $b \neq a$, welche in einem algebraischen Abschluss von K liegt. Nach Satz 3.4 gibt es genau einen Isomorphismus φ von $K(a)$ nach $K(b)$ mit $\varphi(a) = b$. Aus Satz 4.1 lässt sich dieser zu einen K-Monomorphismus $\bar{\varphi}$ von L nach $\bar{K}$ fortsetzen. Nach Voraussetzung ist L/K eine normale Körpererweiterung. Der Satz 4.2 besagt, dass für jeden K-Homomorphismus $\tau : L \to \bar{L}$ gilt $\tau(L) = L$, das folgt insbesondere für $\bar{\varphi}$. Daher ist $\bar{\varphi} \in \Gamma(L/K)$; da a beliebig aus $L \setminus K$ war und $\bar{\varphi}$ ein K-Automorphismus von L mit der Eigenschaft $\varphi(a) = b \neq a$ existiert, ist L/K galoissch. □

Bemerkung. In dem Beweis des Satzes 6.6 wird verwendet, dass die Definition 29 eine äquivalente Formulierung der Form besitzt: Die Körpererweiterung L/K ist galoissch, wenn für jedes $a \in L \setminus K$ ein $\delta \in \Gamma(L/K)$ existiert mit $\delta(a) \neq a$.

Beispiel 20.

Die Körpererweiterung $\mathbb{C}/\mathbb{R}$ ist nach Beispiel 19 normal und separabel und nach Satz 6.6 galoissch. Diese Aussage wäre auch ohne den Satz 6.6 möglich, da durch Beispiel 19 die Elemente der Galoisgruppe und deren Fixkörper bekannt sind. Die Menge, die beide Abbildungen unverändert lassen, ist genau $\mathbb{R}$.

Das gilt auch für die Körpererweiterung $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$, denn auch sie ist nach Beispiel 19 normal und separabel und nach Satz 6.6 galoissch.

Allgemein gilt, dass jede Körpererweiterung L/K vom Grad 2 und $charK = 0$, galoissch ist. Denn sie ist normal aufgrund des Korollars 4.3 und separabel aufgrund von Lemma 5.7. Durch Anwendung von Satz 6.6 folgt die Behauptung.

Für die kommenden Überlegungen sei L/K eine beliebige Körpererweiterung. Es werden einige neue Notationen eingeführt, die das Handhaben der folgenden Sätze erleichtern. Wir beginnen mit einer Auflistung dieser:

1. $\Gamma := \Gamma(L/K)$.
2. $\mathcal{Z}(L/K)$ bezeichnet die Menge aller Zwischenkörper von L/K.
3. $\mathcal{U}(L/K)$ oder $\mathcal{U}(\Gamma)$ bezeichnet die Menge aller Untergruppen von Γ.
4. Für jedes $\Delta \in \mathcal{U}(L/K)$ bezeichnet $\Delta^+ := \mathcal{F}(\Delta) = \{a \in L \mid \delta(a) = a \; \forall \delta \in \Delta\}$.
5. Für jedes $E \in \mathcal{Z}(L/K)$ bezeichnet $E^- := \Gamma(L/E) = \{\sigma \in \Gamma(L/K) \mid \sigma(a) = a \; \forall a \in E\}$.

Bemerkung. Δ^+ liegt in $\mathcal{Z}(L/K)$ und E^- liegt in $\mathcal{U}(\Gamma)$.

Definition 31. Die *+Abbildung* wird definiert: $+ : \mathcal{U}(\Gamma) \to \mathcal{Z}(L/K)$, die Zuordnung der Elemente sieht folgendermaßen aus: $\Delta \mapsto \Delta^+$. Die *-Abbildung* wird folgendermaßen festgelegt: $- : \mathcal{Z}(L/K) \to \mathcal{U}(\Gamma)$, die Elemente werden, wie folgt zugeordnet: $E \mapsto E^-$.

Bemerkung. Seien $\Delta \in \mathcal{U}(\Gamma)$ und $E \in \mathcal{Z}(L/K)$, dann versteht man unter: $\Delta^{+-} := (\Delta^+)^-$ bzw. $E^{-+} := (E^-)^+$ und $\Delta^{+-+} = (\Delta^{+-})^+$ bzw. $E^{-+-} = (E^{-+})^-$.

Lemma 6.7. Seien $\Delta, \Delta_1, \Delta_2 \in \mathcal{U}(\Gamma)$ und $E, E_1, E_2 \in \mathcal{Z}(L/K)$ beliebig, dann gilt:

1. $\Delta_1 \subseteq \Delta_2 \Rightarrow \Delta_1^+ \supseteq \Delta_2^+$; $E_1 \subseteq E_2 \Rightarrow E_1^- \supseteq E_2^-$.
2. $\Delta \subseteq \Delta^{+-}$; $E \subseteq E^{-+}$.
3. $\Delta^{+-+} = \Delta^+$; $E^{-+-} = E^+$.

Beweis. (1) Seien $\Delta_1, \Delta_2 \in \mathcal{U}(\Gamma)$ und $\Delta_1 \subseteq \Delta_2$, Δ_1 ist also eine Untergruppe von Δ_2, dadurch hat Δ_2 genau die gleichen Elemente, also K-Automorphismen, wie Δ_1. Wenn Δ_2 echt größer ist, besitzt sie noch mehr K-Automorphismen, die eventuell den Fixkörper verkleinern, daher gilt $\Delta_1^+ \supseteq \Delta_2^+$.
Seien E_1 und E_2 aus $\mathcal{Z}(L/K)$ mit $E_1 \subseteq E_2$, dann gibt es für Automorphismen, die E_1 fix lassen gleich viele oder mehr Möglichkeiten als für Automorphismen bei denen E_2 den Fixkörper bildet. Daraus folgt $E_1^+ \supseteq E_2^+$.
(2) Sei $\Delta \in \mathcal{U}(\Gamma)$ und $\delta \in \Delta$ beliebig. Wir betrachten die Menge aller Elemente in L, die δ alleine fix lässt $\mathcal{F}(\delta)$. Dann gilt $\mathcal{F}(\delta) \supseteq \Delta^+ = \mathcal{F}(\Delta)$, wobei $\mathcal{F}(\delta)$ nach Lemma 6.1 ein Körper sein muss. Aus (a) folgt $\delta \in \mathcal{F}(\delta)^- \subseteq \mathcal{F}(\Delta)^- = \Delta^{+-}$. Jeder Automorphismus aus Δ ist auch in Δ^{+-}.
Sei $E \in \mathcal{Z}(L/K)$ und $a \in E$. Wir betrachten $K(a)$, das ist der kleinste Körper der a und K enthält. Es gilt also $K(a) \subseteq E$ aus (a) folgt $K(a)^- \supseteq E^-$. In $K(a)^-$ sind alle Automorphismen, die $K(a)$ fix lassen. Wir wenden darauf nochmals (a) an. Man erhält $a \in K(a)^{-+} \subseteq E^{-+}$. Es wurde gezeigt, dass jedes a aus E auch in E^{-+} enthalten ist.
(3) Nach (2) gilt $\Delta \subseteq \Delta^{+-}$ so folgt aus (1) $\Delta^+ \supseteq (\Delta^{+-})^+ = \Delta^{+-+}$. Andererseits lässt sich aus (2) $\Delta^+ \subseteq (\Delta^+)^{-+} = \Delta^{+-+}$ folgern. Also stimmt die Behauptung $\Delta^+ = \Delta^{+-+}$.
Für E folgt aus (2) $E \subseteq E^{-+}$ nach Anwendung von (1) erhält man $E^- \supseteq (E^{-+})^- = E^{-+-}$. Genauso lässt sich aus (2) $E^- \subseteq (E^-)^{+-} = E^{-+-}$ folgern. Es gilt somit $E^- = E^{-+-}$. □

Bemerkung. Die +Abbildung bzw. die -Abbildung sind im Allgemeinen weder injektiv noch surjektiv.

Definition 32. Die Untergruppe $\Delta \in \mathcal{U}(\Gamma)$ heißt *abgeschlossen*, wenn $\Delta = \Delta^{+-}$. Analog dazu definiert man: Ein Körper $E \in \mathcal{Z}(L/K)$ wird als *abgeschlossen* bezeichnet, wenn gilt $E = E^{-+}$. Die Mengen der eben definierten abgeschlossenen Elemente werden mit $\mathcal{U}_a(\Gamma)$ bzw. mit $\mathcal{Z}_a(L/K)$ bezeichnet.

Lemma 6.8. Sei $E \in \mathcal{Z}(L/K)$ dann sind die folgende Punkte äquivalent:

1. E ist abgeschlossen.

2. Es existiert ein $\Delta \in \mathcal{U}(\Gamma)$, sodass $E = \Delta^+$.

3. L/E ist galoissch.

Beweis. (1)⇒(2) Sei $E \in \mathcal{Z}(L/K)$ abgeschlossen, also gilt $E = E^{-+}$, dann existiert ein $\Delta \in \mathcal{U}(\Gamma)$ mit $\Delta = E^-$, da nach Bemerkung E^- ein Element von $\mathcal{U}(\Gamma)$ ist. Durch das Einsetzen von dem gefundenen Δ ergibt sich $E = \Delta^+$.
(2)⇒(3) Sei $\Delta \in \mathcal{U}(\Gamma)$ mit $E = \Delta^+$. Es ist $E = \Gamma(L/E)^+$ zu zeigen. Wegen $E = \Delta^+$ gilt $\Delta \subseteq \Gamma(L/E)$, daher ist $E = \Delta^+ \supseteq \Gamma(L/E)^+$. Daraus folgt also $E \supseteq \Gamma(L/E)$. Die Inklusion $E \subseteq \Gamma(L/E)^+$ ist trivial. Es gilt nun $E = \Gamma(L/E)^+$
(3)⇒(1) Sei die Körpererweiterung L/E galoissch, dann gilt per Definition $E = \Delta^+$ für $\Delta := \Gamma(L/E) = E^-$. Nach Einsetzen von E^- für Δ, folgt $E = (E^-)^+ = E^{-+}$, also ist E abgeschlossen. □

Lemma 6.9. Sei $\Delta \in \mathcal{U}(\Gamma)$, dann gilt: Δ ist genau dann abgeschlossen, wenn ein $E \in \mathcal{Z}(L/K)$ existiert, sodass $\Delta = E^-$.

Beweis. (⇒) Sei $\Delta \in \mathcal{U}(\Gamma)$ abgeschlossen, dann gilt per Definition $\Delta^{+-} = \Delta$. Es existiert ein $E \in \mathcal{Z}(L/K)$ mit $E = \Delta^+$, da Δ durch die +Abbildung immer zu einem Körper wird, siehe Lemma 6.1. Durch das Einsetzen erhält man $E^- = \Delta$.
(⇐) Sei $\Delta \in \mathcal{U}(\Gamma)$, mit $\Delta = E^-$ für ein $E \in \mathcal{Z}(L/K)$. Aus der Gleichheit und Lemma 6.7(c) folgt $\Delta^{+-} = E^{-+-} = E^- = \Delta$. □

Lemma 6.10. Die +Abbildung eingeschränkt auf abgeschlossene Untergruppen, also $\mathcal{F} : \mathcal{U}_a(\Gamma) \to \mathcal{Z}_a(L/K)$ mit $\Delta \mapsto \Delta^+$ ist bijektiv. Die Umkehrabbildung ist $\mathcal{G} : E \mapsto E^-$.

Beweis. Allgemein gilt für jedes $\Delta \in \mathcal{U}(\Gamma)$, dass $\Delta^+ \in \mathcal{Z}_a(L/K)$ ist. Aufgrund von Lemma 6.7 gilt $(\Delta^+)^{-+} = \Delta^{+-+} = \Delta^+$. Insbesondere erfüllt das auch jedes $\Delta \in \mathcal{U}_a(\Gamma)$. Analog betrachtet man $E \in \mathcal{Z}_a(L/K)$ für die gilt $E^- \in \mathcal{U}_a(\Gamma)$, das erfüllen wiederum alle $E \in \mathcal{Z}(L/K)$, wegen Lemma 6.7 mit $(E^-)^{+-} = E^-$. Die Abgeschlossenheit von Δ und E wird erst jetzt gebraucht. Aus $\mathcal{G}(\mathcal{F}(\Delta)) = \Delta^{+-} = \Delta$ für ein beliebiges $\Delta \in \mathcal{U}_a(\Gamma)$ und $\mathcal{F}(\mathcal{G}(E)) = E^{-+} = E$ für ein beliebiges $E \in \mathcal{Z}_a(L/K)$ zeigt sich, dass $\mathcal{G} \circ \mathcal{F} = Id_{\mathcal{U}_a(\Gamma)}$ und $\mathcal{F} \circ \mathcal{G} = Id_{\mathcal{Z}_a(L/K)}$ ist. Also sind $\mathcal{F}$ und $\mathcal{G}$ bijektive Funktionen und $\mathcal{G}$ ist die Umkehrfunktion von $\mathcal{F}$. □

Satz 6.11. Eine Körpererweiterung L/K ist genau dann galoissch, wenn L Zerfällungskörper einer Familie separabler Polynome aus $K[X]$ ist.

Beweis. ($\Rightarrow$) Sei L/K eine galoissche Körpererweiterung, dann ist nach Satz 6.6 L/K normal und separabel. Nach Satz 4.2 gilt, dass L der Zerfällungskörper einer Menge A von Polynomen aus $K[X]$ ist. Da L/K separabel ist, ist A eine Menge von separablen Polynomen.
($\Leftarrow$) Sei L der Zerfällungskörper einer Menge $A \subseteq K[X]$ separabler Polynome. Es fehlt noch die Separabilität von L/K zu zeigen. Sei nun $N = \{a \in L \mid \exists P \in A \text{ mit } P(a) = 0\}$. Da L der Zerfällungskörper von A ist, gilt $L = K(N)$. Die Menge N besteht nur aus separablen Elementen, denn die Minimalpolynome der Elemente aus N teilen die separablen Polynome aus A. Nach Satz 5.14 und anschließender Bemerkung ist die Körpererweiterung L/K auch separabel. Es gilt wegen dem Satz 4.2, dass L/K normal ist. Nach Satz 6.6 ist L/K galoissch. □

Satz 6.12 (Krull)**.** Sei L/K eine algebraische Körpererweiterung und $\Gamma = \Gamma(L/K)$ die dazugehörige Galoisgruppe. Unter diesen Voraussetzungen erfüllt jeder Zwischenkörper E von L/K:

1. Jede Körpererweiterung L/E ist galoissch und jeder Zwischenkörper E ist abgeschlossen.

2. Jeder K-Homomorphismus von E in einen algebraischen Abschluss $\bar{L}$ von L ist zu einem Element aus Γ fortsetzbar.

3. Die Körpererweiterung E/K ist genau dann galoissch, wenn $\Gamma(L/E)$ ein Normalteiler von Γ ist.

Beweis. (1) Nach Voraussetzung ist L/K galoissch, aufgrund von Satz 6.11 ist L Zerfällungskörper einer Menge separabler Polynome $A \subseteq K[X]$. Wir betrachten nun die Polynome aus A über dem Körper E, dann bleiben die Elemente aus A separabel über L. Durch erneute Anwendung des Satz 6.11 ist L/E galoissch. Nach Lemma 6.8 gilt für eine galoissche Körpererweiterung L/E, dass E abgeschlossen ist.
(2) Aufgrund des Satzes 4.1 kann man einen beliebigen K-Homomorphismus τ von E nach $\bar{L}$, der ja immer injektiv ist, zu einem Monomorphismus $\bar{\tau}$ von L nach $\bar{L}$ erweitern, sofern L/K algebraisch ist. Das trifft in diesem Fall zu. Bei L/K handelt es sich um eine galoissche Erweiterung daher gilt nach Satz 6.6, dass L/K normal ist. Aus Satz 4.2 lässt sich für die nun normale Körpererweiterung L/K folgern, dass $\bar{\tau}(L) = L$ ist, daher gilt $\bar{\tau} \in \Gamma$
(3) ($\Rightarrow$) Sei E/K galoissch, dann ist nach Satz 6.6 E/K normal. Aus dem Satz 4.2 gilt für jedes $\tau \in \Gamma$, dass $\tau(E) = E$. Schränkt man nun τ auf E ein, dann ist $\tau_{|E} \in \Gamma(E/K)$, da alle τ den Körper K fix lassen. Die Aussage im Punkt (2) impliziert, dass die Abbildung $\varphi : \tau \to \tau_{|E}$ surjektiv ist. Die Abbildung

φ stellt einen Epimorphismus von Γ auf $\Gamma(E/K)$ dar. Wir untersuchen nun den Kern der Abbildung genauer:

$$\tau \in kern\ \varphi \Leftrightarrow \tau_{|E} = id_E \Leftrightarrow \tau \in \Gamma(L/E).$$

Es gilt $\Gamma(L/E) = kern\ \varphi$ und der $kern\ \varphi$ ist ein Normalteiler der Urbildgruppe, also von $\Gamma(L/K)$.
($\Leftarrow$) Sei $\Gamma(L/E) = E^-$ ein Normalteiler von Γ. Seien $\sigma \in \Gamma$, $\tau \in E^-$ und $a \in E$ beliebig, dann gilt $\sigma^{-1}\tau\sigma(a) = \tau(a) = a$ oder $\tau\sigma(a) = \sigma(a)$. Daraus folgt, dass $\sigma(a)$ ein Element des Fixkörpers von E^- ist, also $\sigma(a) \in E^{-+}$. Aufgrund der Aussage (1) ist jeder Zwischenkörper von L/K abgeschlossen, dann ist $\sigma(a) \in E^{-+} = E$. Daraus begründet sich $\sigma(E) \subseteq E$. Es gilt auch $\sigma(E) \supseteq E$, denn sei $\sigma^{-1} \in \Gamma$, dann folgt $\sigma\tau\sigma^{-1}(a) = a$. Es gilt aufgrund des vorigen Arguments $\sigma^{-1}(a) \in E$ und daraus folgt $\sigma^{-1}(E) \subseteq E$, das bedeutet $E \subseteq \sigma(E)$. Die nun erhaltene Gleichheit $\sigma(E) = E$, ergibt $\sigma_{|E} \in \Gamma(E/K)$. Sei $b \in E \setminus K$ so existiert ein $\sigma \in \Gamma$ mit $\sigma(b) \neq b$, da ja L/K galoissch ist und der Fixkörper genau K sein muss. Es folgt $\sigma_{|E}(b) \neq b$, daher ist E/K galoissch. □

Der wichtige Satz von Dedekind wird in zwei Schritten bewiesen und gliedert sich hier in einen Satz und einen Hilfssatz.

Satz 6.13 (Dedekind)**.** Sei L ein Körper und Γ eine endliche Untergruppe von $AutL$ mit Fixkörper K, dann gilt $[L : K] = |\Gamma|$.

Hilfssatz 6.14. Unter den obigen Voraussetzungen ist L/K separabel und für jedes $a \in L$ gilt $[K(a) : K] \leq |\Gamma|$.

Beweis. Sei $a \in L$ und $M = \{\varphi(a) \mid \varphi \in \Gamma\}$ die Menge der Konjungierten von a. Bilde das Polynom $Q = \prod_{b\in M}(X - b)$. Dieses lässt sich auch schreiben als $Q = \sum_{i=0}^{|M|} a_i X^i \in L[X]$. Es gilt auch $\gamma(M) = M$ für alle $\gamma \in \Gamma$, so folgt nun mit dem selben Argument, wie im Beweis von Satz 6.6, dass $Q \in K[X]$ ist. Das Polynom Q hat nur einfache Wurzeln, da in der Menge M jedes $\varphi(a)$ nur einmal vorkommt und a ist Nullstelle von Q, also ist a separabel über K. Das Element ist also auch algebraisch, dann gilt aufgrund von Satz 1.6, dass $[K(a) : K] = deg\ m_{a,K} \leq degQ = |M| \leq |\Gamma|$. □

Beweis. Aufgrund des Hilfssatz 6.14 gilt $[K(a) : K] \leq |\Gamma|$ für alle $a \in L$. Daraus folgt es existiert ein $c \in L$ mit $[K(c) : K] \geq [K(a) : K]$ für alle $a \in L$. Es lässt sich die Behauptung $L = K(c)$ folgern. Angenommen $L \neq K(c)$, dann existiert ein $b \in L \setminus K(c)$. Wir betrachten nun $K(c)(b) \supset K(c)$, dann gilt nach Satz 1.1:

$$[K(c)(b) : K] = \underbrace{[K(c)(b) : K(c)]}_{>1}[K(c) : K] > [K(c) : K].$$

Nach dem Satz 5.12 vom primitiven Element existiert ein Element d, sodass $K(a)(b) = K(d)$, daraus folgt $[K(d) : K] > [K(c) : K]$, das steht im Widerspruch zum maximalen Element. Also gilt $L = K(c)$. Aus der Abschätzung des Hilfssatz 6.14 gilt nun $[L : K] = [K(c) : K] \leq |\Gamma|$. Andererseits folgt aus Lemma 6.2 die Abschätzung für endliche Erweiterungen L/K durch $|\Gamma| \leq |\Gamma(L/K)| \leq [L : K]$. Daher gilt $|\Gamma| = [L : K]$. □

Satz 6.15 (Hauptsatz der endlichen Galoistheorie)**.** Für jede endliche Galoiserweiterung L/K mit Galoisgruppe Γ sind alle Zwischenkörper von L/K und alle Untergruppen von Γ abgeschlossen. Die Abbildungen $\mathcal{F}$ und $\mathcal{G}$ sind bijektiv und invers zueinander, sie sind folgendermaßen definiert:

$$\mathcal{F} : \mathcal{U}(\Gamma) \to \mathcal{Z}(L/K),\ \Delta \mapsto \mathcal{F}(\Delta)$$
$$\mathcal{G} : \mathcal{Z}(L/K) \to \mathcal{U}(\Gamma),\ E \mapsto \Gamma(L/E).$$

Zusätzlich gelten für $E \in \mathcal{Z}(L/K)$ folgende Aussagen:

1. Jedes E erfüllt $|\Gamma(L/E)| = [L : E]$.
2. Die Körpererweiterung L/E ist galoissch und E ist abgeschlossen.
3. Jeder K-Homomorphismus φ von E in einen algebraischen Abschluss $\bar{L}$ von L ist zu $\bar{\varphi}$ fortsetzbar, sodass $\bar{\varphi} \in \Gamma$.
4. Die Körpererweiterung E/K ist genau dann galoissch, wenn $\Gamma(L/E)$ Normalteiler von Γ ist.

Beweis. Da L/K endlich ist, folgt nach Lemma 6.2 auch, dass Γ endlich ist und daher auch die Untergruppe $\Gamma(L/E)$, wo alle Automorphismen Fixkörper E haben. Es lässt sich dadurch Satz 6.13 anwenden, nachdem die Behauptung $[L : E] = |\Gamma(L/E)|$ für beliebiges $E \in \mathcal{Z}(L/K)$ ihre Gültigkeit erlangt. Aufgrund von Satz 6.12 folgen die Aussagen (2)-(4). Um aus dem Lemma 6.10 die Bijektivität von $\mathcal{F}$ und $\mathcal{G}$ folgern zu können, muss man zeigen, dass jedes $\Delta \in \mathcal{U}(\Gamma)$ abgeschlossen ist, also $\Delta^{+-} = \Delta$. Für die Zwischenkörper $E \in \mathcal{Z}(L/K)$ erweist sich die Aussage (1) aus Satz 6.12 als hilfreich. Sei nun $\Delta \in \mathcal{U}(\Gamma)$ beliebig. Es ist ja Γ endlich und Δ eine endliche Untergruppe von Γ, dann gilt nach Satz 6.13, dass $[L : \Delta^+] = |\Delta|$. Es existiert ein $E \in \mathcal{Z}(L/K)$ mit $E := \Delta^+$. Nach Lemma 6.7 gilt $\Delta \subseteq \Delta^{+-}$ und $E = \Delta^+ = \Delta^{+-+}$. Daher ist E auch Fixkörper von $E^- = \Delta^{+-}$. Aus Satz 6.13 folgt $[L : \Delta^+] = |\Delta^{+-}|$. Also wird durch $|\Delta| = [L : \Delta^+] = |\Delta^{+-}|$ die Eigenschaft abgeschlossen, $\Delta = \Delta^{+-}$, erfüllt. Es handelt sich jetzt bei $\mathcal{F}$ und $\mathcal{G}$ um Abbildungen, wie im Lemma 6.10 beschrieben, also sind $\mathcal{F}$ und $\mathcal{G}$ bijektiv und invers zueinander. □

Korollar 6.16. Sei L/K eine endliche Körpererweiterung, dann gelten folgende Äquivalenzen:

1. L/K ist galoissch.
2. L/K ist normal und separabel.
3. L ist Zerfällungskörper eines separablen Polynoms $P \in K[X]$.
4. L ist Zerfällungskörper eines irreduziblen und separablen Polynoms $P \in K[X]$.
5. Für den Grad der Körpererweiterung gilt $[L : K] = |\Gamma(L/K)|$.

Beweis. Im Wesentlichen sind das alles Folgerungen aus den vorangegangen Sätzen, im Detail:
(1)⇔(2) Diese Äquivalenz folgt aus Satz 6.6.
(1)⇔(3) Folgt aus Satz 6.11.
(1)⇔(5) Nach dem Haupsatz der endlichen Galoistheorie gilt für jeden Zwischenkörper E von L/K die Gleichung $[L : E] = |\Gamma(L/E)|$, also auch für K, dass $[L : K] = |\Gamma(L/K)|$.
(3)⇒(4) Diese Implikation trifft zu, da die Menge der irreduziblen und separablen Polynome eine Teilmenge der separablen Polynome ist.
(4)⇒(2) Folgt aus Satz 6.11. □

Die Galoisgruppe einer endlichen Körpererweiterung ist aufgrund des Korollars 6.16 immer endlich, deswegen hat sie auch nur endlich viele Untergruppen. Der Hauptsatz der endlichen Galoistheorie 6.15 besagt dann, dass diese Körpererweiterung auch nur endliche viele Zwischenkörper hat. Für Erweiterungen von Körpern mit Charakteristik 0 ist das ein erstaunliches Ergebnis. Intuitiv möchte man glauben, dass die Adjunktionen zwei verschiedener Elemente auch verschiedene Zwischenkörper erzeugen. Jedoch ist das nur bei einigen wenigen der Fall, die meisten erzugen bei der Adjunktion sogar den ganzen Körper.

Beispiel 21. Wir suchen alle Zwischenkörper der Erweiterung $\mathbb{Q}(\sqrt{2}, \sqrt{5})/\mathbb{Q}$. Der Körper $\mathbb{Q}(\sqrt{2}, \sqrt{5})$ ist Zerfällungskörper des separablen Polynoms $(X^2 - 2)(X^2 - 5) = X^4 - 7X^2 + 10$. Nach Korollar 6.16 ist die Körpererweiterung $\mathbb{Q}(\sqrt{2}, \sqrt{5})/\mathbb{Q}$ galoissch. Mit den Minmalpolynome $m_{\sqrt{2},\mathbb{Q}} = X^2 - 2$ und $m_{\sqrt{5},\mathbb{Q}(\sqrt{2})} = X^2 - 5$ lässt sich der Grad der Körpererweiterung bestimmen:

$$[\mathbb{Q}(\sqrt{2}, \sqrt{5}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{5}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \cdot 2 = 4.$$

Also hat nach dem Korollar 6.16 die Galoisgruppe der hier behandelten Körpererweiterung eine Mächtigkeit von 4. Wir betrachten nun die Körpererweiterung $\mathbb{Q}(\sqrt{2},\sqrt{5})/\mathbb{Q}(\sqrt{2})$. So gibt es nach Satz 3.4 einen Isomorphismus σ von $\mathbb{Q}(\sqrt{2})(\sqrt{5})$ nach $\mathbb{Q}(\sqrt{2})(-\sqrt{5})$. Beide Wurzeln erzeugen denselben Körper $\mathbb{Q}(\sqrt{2},\sqrt{5})$ und σ ist ein selbstinverser $\mathbb{Q}(\sqrt{2})$-Automorphismus, der $\sqrt{5}$ auf $-\sqrt{5}$ abbildet, vergleiche dazu das Beispiel 18. Auf die gleich Art und Weise lässt sich ein selbstinverser $\mathbb{Q}(\sqrt{5})$-Automorphismus τ erzeugen, der $\sqrt{2}$ auf $-\sqrt{2}$ abbildet. Das Element $\tau \circ \sigma \neq Id$ es vertauscht die Vorzeichen beider Elemente $\sqrt{2}$ und $\sqrt{5}$. Es wurden also vier verschiedene Automorphismen gefunden, die Galoisgruppe ist komplett:

$$\Gamma(\mathbb{Q}(\sqrt{2},\sqrt{5})/\mathbb{Q} = \{Id, \sigma, \tau, \sigma\tau\}.$$

Wir untersuchen nun die Fixkörper der Untergruppen der Galoisgruppe. Die Galoisgruppe hat auf alle Fälle die trivialen Untergruppen, die Identität und sich selbst. Es muss mindestens eine Untergruppe der Ordnung 2 existieren, so erzeugen σ und τ eine Untergruppe, da sie selbstinvers sind. Weiters erzeugt das Element $\sigma\tau$ ebenfalls eine Untergruppe der Ordnung 2, da es auch selbstinvers ist. Es ist also jedes Element der Galoisgruppe selbstinvers, es kann also keine weitere Untergruppen der Ordnung 2 geben. Also hat die Körpererweiterung drei echte Zwischenkörper. Wie oben schon erwähnt lässt die Abbildung σ den Körper $\mathbb{Q}(\sqrt{2})$ fest, bei τ wird $\mathbb{Q}(\sqrt{5})$ nicht verändert. Wir betrachten $\sigma\tau(\sqrt{2}\sqrt{5}) = \sqrt{2}\sqrt{5} = \sqrt{10}$, also ist der Fixkörper $\mathcal{F}(\langle\sigma\tau\rangle) = \mathbb{Q}(\sqrt{10})$. Es wurden alle drei Zwischenkörper von $\mathbb{Q}(\sqrt{2},\sqrt{5})/\mathbb{Q}$ gefunden.

7 Konstruktion mit Zirkel und Lineal

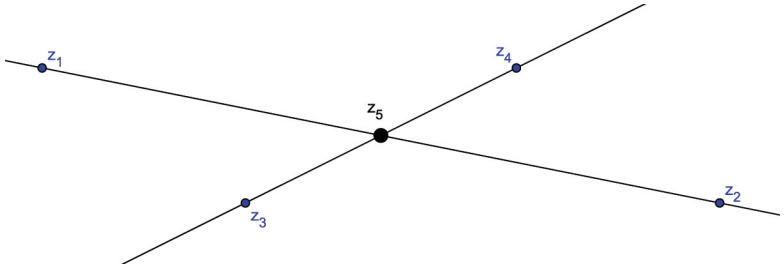
7.1 Konstruierbarkeit

In diesem Kapitel findet die Galoistheorie Anwendung auf geometrische Konstruktionen. Zuerst bedarf es jedoch einer Einführung in diese Thematik, die vorerst den Hauptsatz der endlichen Galoistheorie nicht verwendet. Zu Beginn dieses Abschnitts muss geklärt werden, was es bedeutet, Konstruktionen mit Zirkel und Lineal durchzuführen. Aufgrund der besseren Begrifflichkeit verwende ich für die Konstruktionsprobleme, die komplexe Zahlenebene $\mathbb{C}$. Es wäre genau so möglich, siehe im Buch „Algebra“ von Artin. M (Kapitel 13.4, [2]), diese Thematik in $\mathbb{R}$ aufzufassen. In diesem Buch ist ein Punkt in der Ebene nur dann konstruierbar, wenn seine kartesischen Koordinaten konstruierbar sind. Das fällt in der komplexen Zahlenebene weg, denn ein Punkt $(x|y) \in \mathbb{R}^2$ wird mit $z = x + iy \in \mathbb{C}$ identifiziert. Jede Konstruktion beginnt mit einer Startmenge, in der alle Punkte als bereits konstruiert gelten. Mit Hilfe dreier elementaren Konstruktionen können aus der Startmenge gewisse Punkte konstruiert werden. Das interessante an diesem Kapitel ist, dass diese Konstruktionsprobleme in die Sprache der Körpererweiterungen übersetzt werden. In diesem Kapitel richte ich mich nach den Büchern: „Algebra“ von Bosch (Kapitel 6.4, [4]) und „Algebra“ von Karpfinger und Meyberg (Kapitel 21, [9]). Alle Skizzen wurden mit der Software „GeoGebra“ erstellt.

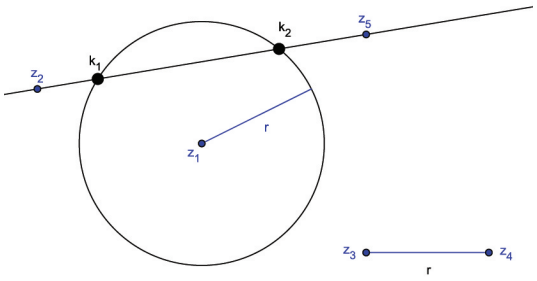
Definition 33. Sei $S \subset \mathbb{C}$, $|S| \geq 2$ die Startmenge, ein Punkt $z \in \mathbb{C}$ *lässt sich mit Zirkel und Lineal konstruieren*, wenn M sich durch endlich viele elementare Konstruktionsschritte zu einer Teilemenge $S' \subset \mathbb{C}$ mit $z \in S'$ vergrößern lässt.

Definition 34. Es werden folgende drei Typen von elementaren Konstruktionen zugelassen.

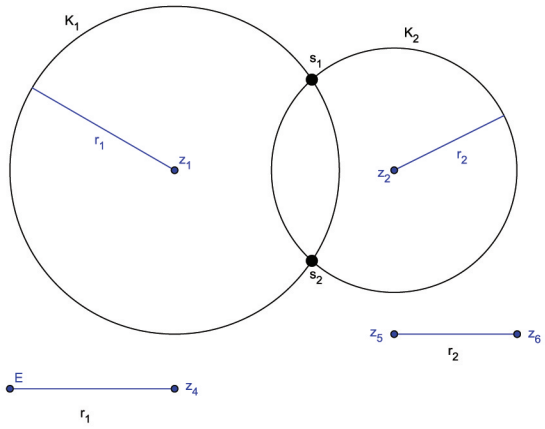
1. Seien g_1 und g_2 zwei nichtparallele Geraden in $\mathbb{C}$, wobei die Gerade g_1 durch die Punkte $z_1, z_2 \in S$ und g_2 durch die Punkte $z_3, z_4 \in S$ festgelegt wird. Dann gilt der Schnittpunkt z_5 der beiden Geraden als konstruiert und der Punkt z_5 liegt nun in S'.



2. Sei K eine Kreislinie in $\mathbb{C}$ um den Mittelpunkt $z_1 \in S$ mit einem Radius, der durch den Abstand $|z_3 - z_2|$ zweier Punkte $z_2, z_3 \in S$ gegeben wird. Sei weiters g eine Gerade gegeben durch die Punkte $z_4, z_5 \in S$. Dann betrachtet man die Menge der Schnittpunkte zwischen Kreis und Geraden als konstruiert und erweitert die Menge S zu S'.



3. Seien K_1 und K_2 zwei nicht identische Kreise in $\mathbb{C}$ mit den Mittelpunkten $z_1, z_2 \in \mathbb{C}$ und den Radien $|z_4 - z_3|$ und $|z_6 - z_5|$. Dann gilt die Menge der Schnittpunkte von K_1 und K_2 als konstruiert und erweitert damit S auf S'.



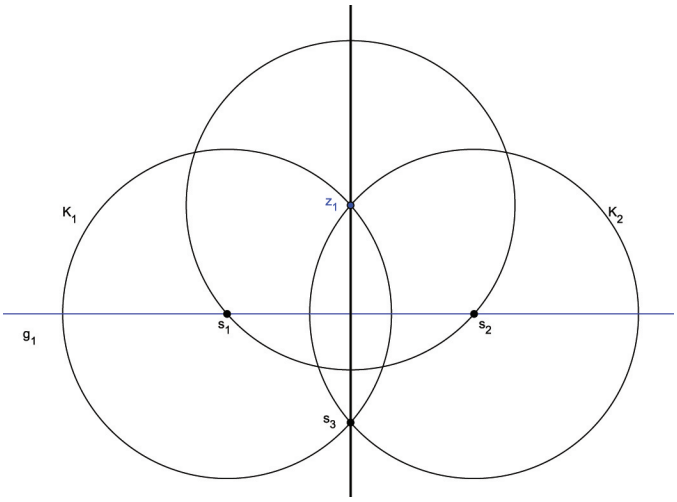
Die Menge aller mit Zirkel und Lineal aus S konstruierbaren Punkte in $\mathbb{C}$ wird mit $\mathcal{K}(S)$ bezeichnet.

Aus den elementaren Konstruktionen lassen sich unmittelbar folgende fünf Konstruktionen ableiten, die später benötigt werden.

Korollar 7.1. Seien die Punkte $0, 1, z_1, z_2, z_3 \in \mathbb{C}$ und eine Gerade g in $\mathbb{C}$ gegeben, dann lassen sich folgende Konstruktionen durchführen:

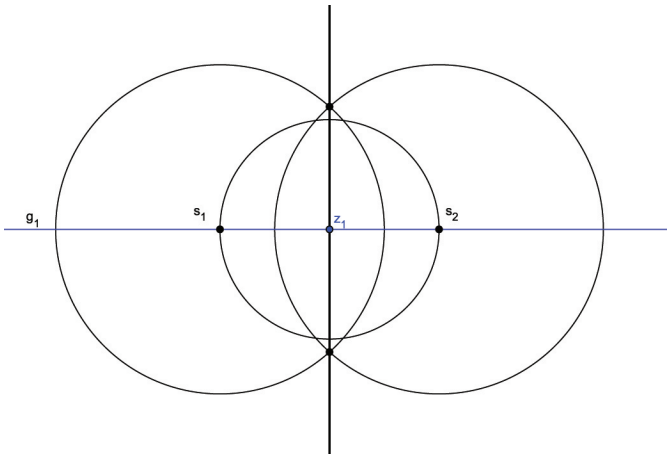
1. Es lassen sich beliebig große Abstände erzeugen.
2. Das Lot von z_1 auf g und die Senkrechte von z_2 auf g lassen sich konstruieren.
3. Der Mittelpunkt zweier Punkte z_1 und z_2 kann konstruiert werden.
4. Es kann eine Parallele zu g durch einen Punkt z_1 erzeugt werden.
5. Die winkelhalbierende Gerade kann konstruiert werden.

Beweis. Die Beweise der einzelenen Punkte erfolgen durch Verwendung der elementaren Konstruktionen:
(1) Durch Verwendung der Elementarkonstruktion (2) lassen sich beliebige Abstände konstruieren.
(2) Seien der Punkt z_1 und die Gerade g gegeben, wobei $z_1 \notin g$. Dann erfolgt im ersten Schritt durch Anwendung der Elementarkonstruktion (2), die Konstruktion eines Kreises mit dem Mittelpunkt z_1 und einem Radius, sodass sich zwei Schnittpunkte $s_1, s_2 \in g$ mit dem Kreis und der Gerade ergeben. Verwende nun einen dieser Schnittpunkte, $o.B.d.A$ s_1 als Mittelpunkt eines Kreises K_1 mit dem Radius $|s_1 - z_1|$. Anschließend erstellt man einen zweiten Kreis K_2 mit dem Mittelpunkt s_2 und dem Radius $|s_2 - z_1|$. Durch Verwendung der Elementarkonstruktion (3) schneidet man K_1 und K_2, sodass sich zwei Schnittpunkte z_1 und s_3 ergeben. Als letzten Schritt wird das Lot gezogen, das entspricht der Gerade, die durch die Punkte z_1 und s_3 geht.

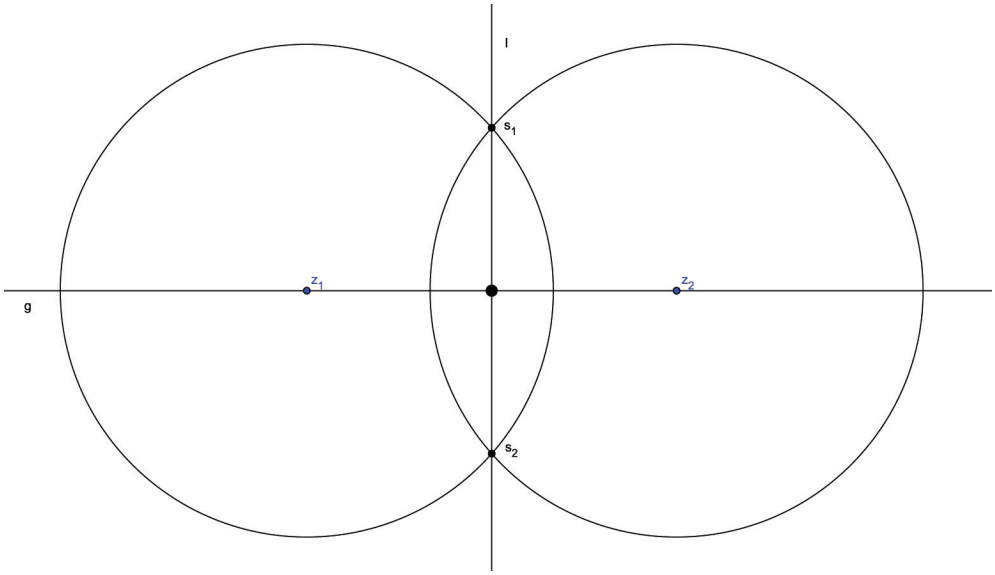


Seien z_1 und g eine Gerade mit $z_1 \in g$. Wir erstellen einen Kreis mit Mittelpunkt z_1 und einen beliebigen Radius $|r| > 0$. Durch das Schneiden des

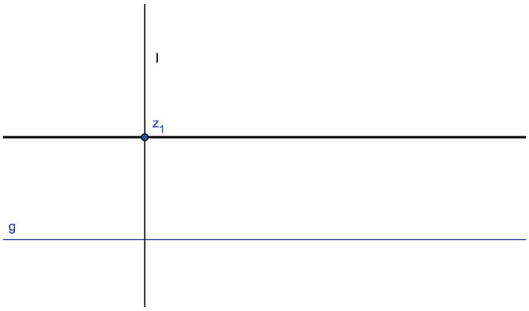
Kreises und der Gerade g enstehen zwei Schnittpunkte s_1 und s_2. Wir konstruieren nun zwei Kreise mit gleichen Radien $|r_2| > |r|$, einen mit Mittelpunkt s_1 und den anderen mit Mittelpunkt s_2. Die Schnittpunkte dieser zuvor erstellten Kreise, definieren die Senkrechte auf g durch z_1.



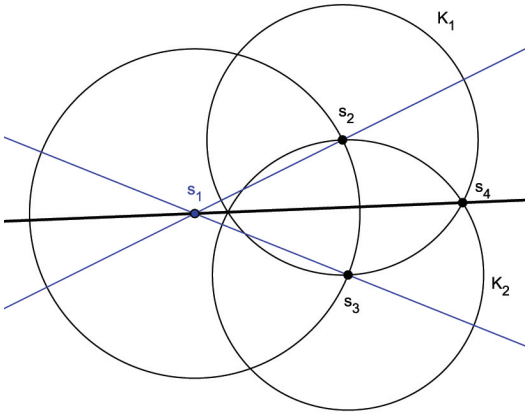
(3) Seien z_1 und z_2 gegeben. Wir ziehen eine Gerade g durch beide gegebenen Punkte und erstellen zwei Kreise mit gleichen Radien $|r| > \frac{1}{2}|z_1 - z_2|$, wobei einmal z_1 und das andere Mal z_2 der Mittelpunkt ist. Durch den Schnitt der beiden soeben erstellten Kreise, erhält man zwei Schnittpunkte s_1 und s_2, durch diese wird eine Gerade l gezogen. Der Schnitt von l mit g ergibt den Mittelpunkt von z_1 und z_2.



(4) Sei eine Gerade g und Punkt z_1 gegeben. Wir konstruieren das Lot l von z_1 auf g nach Punkt (2) und anschließend die Senkrechte in z_1 auf l.



(5) Seien zwei nicht parallele Geraden g und l mit einem Schnittpunkt s_1 gegeben. Wir konstruieren einen Kreis mit Mittelpunkt s_1 und Radius $|r| > 0$. Durch den Schnitt von dem Kreis mit g und l erhält man zwei Punkte s_2, s_3. Wir erstellen zwei neue Kreise K_1, K_2 mit den Mittelpunkten s_2 und s_3 und mit gleichen Radien von $|r| > \frac{1}{2}|s_2 - s_3|$. Im Schnitt von K_1 und K_2 liegt ein neuer Punkt s_4. Die Gerade, die durch die Punkte s_1 und s_4 verläuft ist die Winkelhalbierende.



□

Im folgende Satz wird die Wurzel aus einem komplexen Element z benötigt, $\sqrt{z}$ ist so zu verstehen, dass $(\sqrt{z})^2 = z$ ist. Wir benötigen einen Hilfssatz um im Anschluss das Lemma 7.3 zu beweisen.

Hilfssatz 7.2. Die Menge aller konstruierbaren Punkte $\mathcal{K}(S)$ mit $0, 1 \in S$ ist ein Teilkörper von $\mathbb{C}$ mit den Eigenschaften:

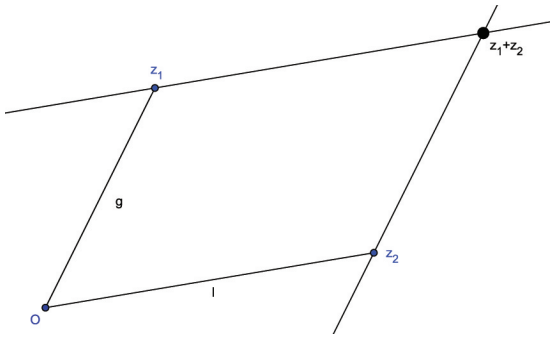
1. $z \in \mathcal{K}(S) \Rightarrow \sqrt{z} \in \mathcal{K}(S)$.
2. $z \in \mathcal{K}(S) \Rightarrow \bar{z} \in \mathcal{K}(S)$.

Beweis. Um zu zeigen, dass $\mathcal{K}(S)$ ein Teilkörper von $\mathbb{C}$ mit den oben angeführten Eigenschaften ist, müssen folgende Implikationen nachgewiesen werden.

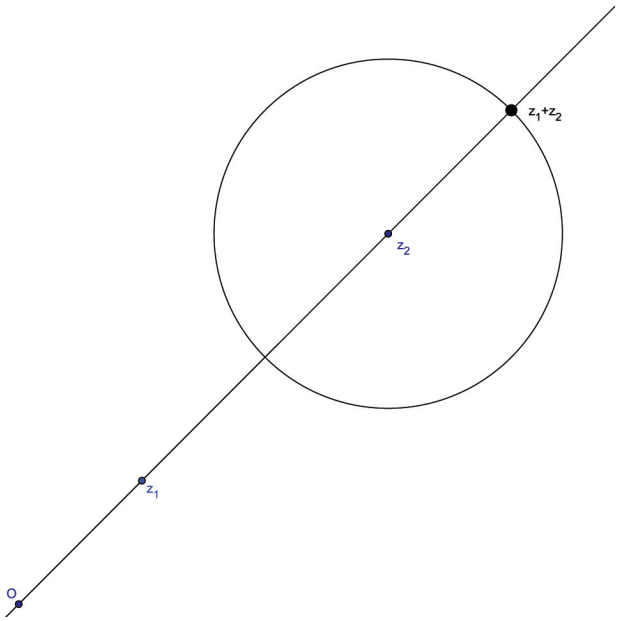
1. $z_1, z_2 \in \mathcal{K}(S) \Rightarrow z_1 + z_2 \in \mathcal{K}(S)$.
2. $z \in \mathcal{K}(S) \Rightarrow -z \in \mathcal{K}(S)$.
3. $z_1, z_2 \in \mathcal{K}(S) \Rightarrow z_1 z_2 \in \mathcal{K}(S)$.
4. $z \in \mathcal{K}(S) \Rightarrow z^{-1} \in \mathcal{K}(S)$.
5. Für die Eigenschaft (1) $z \in \mathcal{K}(S) \Rightarrow \sqrt{z} \in \mathcal{K}(S)$.
6. Für die Eigenschaft (2) $z \in \mathcal{K}(S) \Rightarrow \bar{z} \in \mathcal{K}(S)$.

Die einzelnen Punkt werden mittels geometrischer Konstruktion gezeigt:

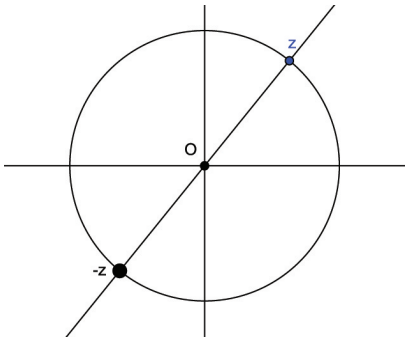
1. Seien z_1 und z_2 gegeben. Es bedarf einer Fallunterscheidung.
   1.Fall: Die Punkte $0, z_1, z_2$ liegen nicht auf einer Geraden. Wir erstellen zwei Geraden g und l, g durchläuft die Punkte 0 und z_1 und l wird durch 0 und z_2 gelegt. Nach Korollar 7.1 ist das Parallelverschieben konstruierbar, verschiebe g parallel durch z_2 und l durch z_1. Die beiden neu konstruierten parallelen Geraden bilden einen Schnittpunkt, das ist $z_1 + z_2$.



   2.Fall: Die Punkte $0, z_1, z_2$ liegen auf einer Geraden. Wir erstellen die Gerade, die durch die drei Punkte verläuft und einen Kreis mit dem Punkt als Mittelpunkt, dessen Betrag größer ist. Das sei *o.B.d.A.* z_2 mit dem Radius $r = |z_1 - 0| = |z_1|$. Aus dem Schnitt zwischen Kreis und Gerade ergibt sich $z_1 + z_2$.

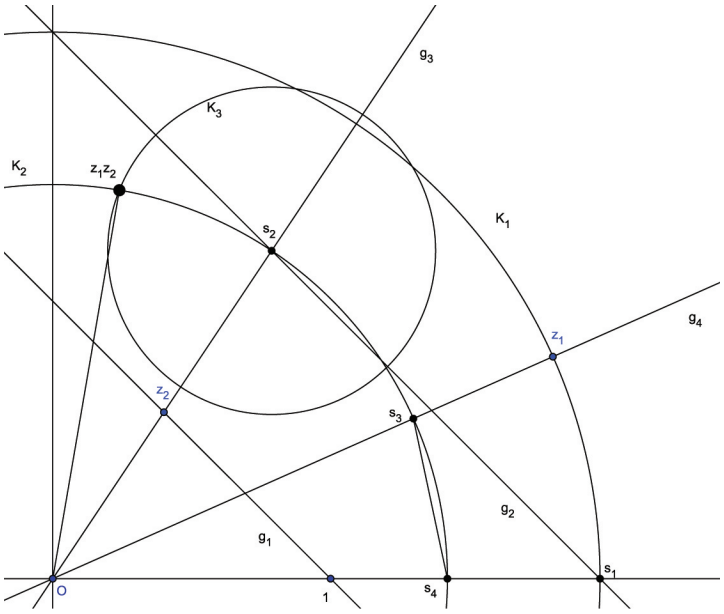


2. Sei $z \in \mathcal{K}(S)$. Wir legen eine Gerade durch die Punkte 0 und z und erstellen einen Kreis mit Mittelpunkt 0 und Radius $r = |z - 0| = |z|$. Der Schnittpunkt des Kreises mit der Gerade ergibt $-z$.



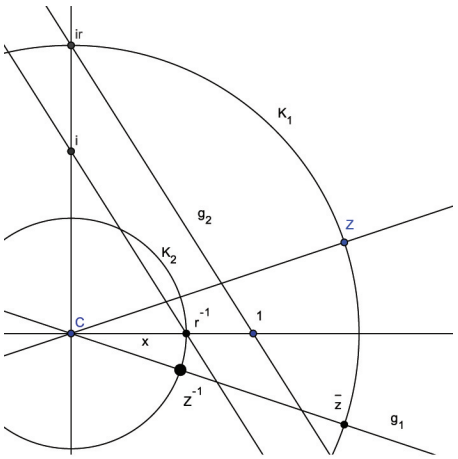
3. Seien z_1 und z_2 gegeben. Die Punkte lassen sich schreiben als $z_1 = r_1 e^{i\varphi_1}$ und $z_2 = r_2 e^{i\varphi_2}$. Wir erstellen eine Gerade, die Koordinatenachse, durch die Punkte 0 und 1, sowie eine Gerade g_1 durch die Punkte z_2 und 1. Wir konstruieren anschließend einen Kreis K_1 mit Mittelpunkt 0 und Radius r_1. Der Schnittpunkt s_1 zwischen der Koordinatenachse und dem Kreis K_1 hat die Entfernung $|r_1|$ zu dem Ursprung. Wir erstellen eine Parallele g_2 zu g_1 durch s_1 und eine weitere Gerade g_3 durch 0 und z_2. Durch den Schnitt von g_2 und g_3 erhält man s_2. Der Abstand $|s_2 - 0| = |s_2| = r_1 r_2$, das gilt aufgrund des Strahlensatzes, denn

$\frac{r_1}{1} = \frac{|s_2|}{r_2}$. Die Länge ist konstruiert, es fehlt noch der Winkel von $z_1 z_2$. Dazu müssen φ_1 und φ_2 addiert werden. Sei *o.B.d.A.* $|z_2| < |z_1|$, wir konstruieren einen Kreis K_2 mit dem Mittelpunkt 0 und Radius der Länge $|s_2|$ und eine Gerade g_4 durch die Punkte 0 und z_1. Durch den Schnitt von K_2 mit g_4 erhalten wir s_3 und s_4 entsteht beim Schnitt mit der Koordinatenachse. Anschließend erstellen wir einen Kreis K_3 mit dem Mittelpunkt in s_2 und Radius $r_3 = |s_4 - s_3|$. Durch das Schneiden von K_2 mit K_3 erhält man $z_1 z_2$.

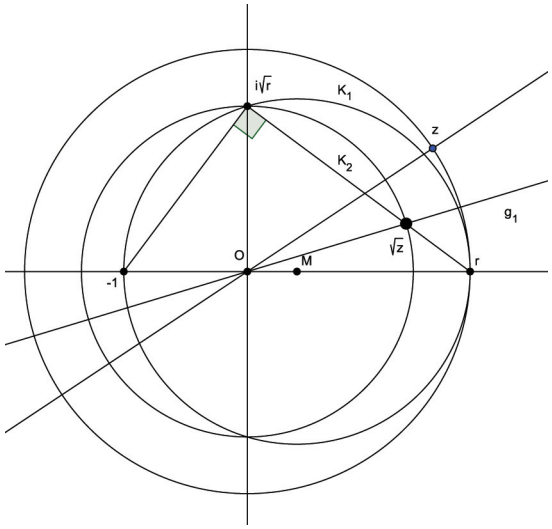


4. Sei $z = re^{i\varphi}$ gegeben, gesucht ist die Konstruktion von $z^{-1} = \frac{1}{r}e^{-i\varphi}$. Es lässt sich $\bar{z}$ konstruieren, siehe Punkt 7, ohne dass Punkt 4 dazu verwendet wird, es ergibt sich damit kein Zirkelschluss. Der Punkt $\bar{z} = re^{-i\varphi}$ hat den Winkel $-\varphi$. Das gesuchte Inverse liegt auf der Gerade g_1, die durch 0 und $\bar{z}$ verläuft. Es fehlt noch, die Länge $\frac{1}{r}$ zu konstruieren. Der Punkt i kann durch den Schnitt des Kreises mit Mittelpunkt 0 und Radius $r_1 = |1 - 0| = |1|$ und der y-Achse konstruiert werden. Wir erstellen anschließend einen Kreis K_1 mit dem Mittelpunkt in 0 und dem Radius r. Im Schnitt von K_1 und der y-Achse liegt der Punkt ir. Wir ziehen eine Gerade g_2 von ir nach 1 und verschieben diese parallel durch den Punkt i. Durch den Schnitt der soeben konstruierten Parallelen und der waagrechten Koordinatenachse ergibt sich der Punkt r^{-1}. Die Begründung, dass es sich bei diesem Punkt um r^{-1} handelt liegt im Strahlensatz: Sei x die unbekannte Länge auf der x-Achse $x = \frac{x}{1} = \frac{i}{ir} = \frac{1}{r} = r^{-1}$. Schlussendlich muss noch ein Kreis K_2 mit dem

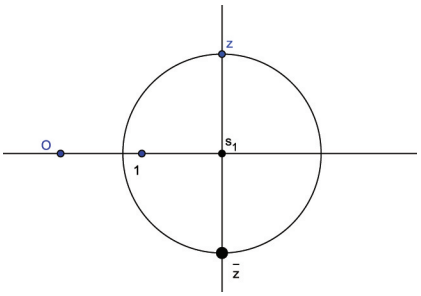
Mittelpunkt 0 und dem Radius $r_2 = |r^{-1} - 0| = |r^{-1}|$ mit g_1 geschnitten werden, um den Punkt $z^{-1} = \frac{1}{r}e^{-i\varphi}$ zu erhalten.



5. Sei $z = re^{i\varphi}$ gegeben, gesucht ist $\sqrt{z} = \sqrt{r}e^{i\frac{\varphi}{2}}$. Die Konstruktion der Koordinatenachsen aus den Punkten 0 und 1 wurde in den zuvor erwähnten Punkten gezeigt. Es kann nach Korollar 7.1 (5) die Winkelhalbierende g_1 von der waagrechten Koordinatenachse und der Geraden durch die Punkte 0 und z konstruiert werden. Wir schneiden nun den Kreis mit Mittelpunkt 0 und der waagrechten Koordinatenachse, so erhält man den Punkt r. Wir erstellen nun den Mittelpunkt M der Punkte r und -1. Der Punkt -1 kann auf die gleiche Art konstruiert werden, wie i zuvor. Wir ziehen nun einen Kreis K_1 mit Mittelpunkt M und Radius $r_1 = |M - r|$. Wir schneiden K_1 mit der senkrechten Koordinatenachse und erhalten den Punkt x. Nach dem Satz von Thales ist das Dreieck durch die Punkte $-1, r, x$ ein rechtwinkeliges Dreieck. Nun lässt sich der Höhensatz anwenden, dadurch erhält man $1 \cdot r = |x|^2$. Es gilt also $\sqrt{r} = |x|$, dadurch ergibt sich $x = i\sqrt{r}$. Wir erstellen einen Kreis K_2 mit Mittelpunkt in 0 und Radius $r_2 = |i\sqrt{r} - 0|$. Wir schneiden nun K_2 mit g_1 und erhalten $\sqrt{z} = \sqrt{r}e^{i\frac{\varphi}{2}}$.



6. Sei ein Punkt z gegeben. Wir erstellen das Lot durch den Punkt z auf die Gerade, die durch 0 und 1 läuft. Durch den Schnitt der Normalen und der Geraden ensteht ein Schnittpunkt s_1, wir verwenden diesen als Mittelpunkt eines Kreises mit Radius $r = |z - s_1|$. Aus dem Schnitt von Gerade und Kreis resultiert $\bar{z}$.



Es wurden alle Punkte für einen Teilkörper gezeigt. □

Definition 35. Sei S die Menge der gegebenen Punkte, dann versteht man unter $\bar{S} = \{\bar{s} \mid s \in S\}$.

Lemma 7.3. Sei $S \subset \mathbb{C}$ mit $0, 1 \in S$ und sei $z \in \mathbb{C}$, dann ist äquivalent:

1. $z \in \mathcal{K}(S)$.
2. Es existiert eine Körperkette $\mathbb{Q}(S \cup \bar{S}) = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_n \subseteq \mathbb{C}$ mit $z \in K_n$ und $[K_i : K_{i-1}] = 2$ für alle $i \in \{1, \ldots, n\}$.

Beweis. (1)⇒(2) Sei $z \in \mathcal{K}(S)$, also ist z mit Zirkel und Lineal konstruierbar. Es genügt die Fälle zu betrachten, wo z aus einem einzigen elementaren Konstruktionsschritt konstruierbar ist. Also müssen nach Definition 34 drei Fälle unterschieden werden. Dabei muss dann gezeigt werden, dass zu z eine Körperkette $S \subseteq K_1 \subseteq K_2$ existiert (eigentlich ist S kein Körper, wir begründen gleich darunter warum wir S als Körper annehmen können) mit $z \in K_2$, sodass gilt $[K_1 : S] \leq 2$ und $[K_2 : K_1] \leq 2$. Der Fall das z mehrere Konstruktionsschritte benötigt, setzt sich wiederum aus mehreren elementaren Konstruktionsschritten zusammen und folgt mit Induktion aus dem Spezialfall. Bevor die einzelnen Schritte gezeigt werden, können noch ein paar Annahmen gemacht werden. An sich ist S kein Körper, da $\mathcal{K}(S) \subseteq \mathcal{K}(\mathbb{Q}(S \cup \bar{S}))$, kann man S durch $\mathbb{Q}(S \cup \bar{S})$ ersetzen, oder aber S gleich als einen Körper annehmen, der unter der komplexen Konjugation invariant bleibt. Weiters darf angenommen werden, dass $i \in S$ ist, andernfalls ersetzt man S durch $S(i)$. Diese Adjunktion entspricht einer Erweiterung zweiten Grades.
1. Fall: Wir untersuchen diejenige Elementarkonstruktion für z, die sich als Schnitt zweier nichtparallelen Geraden ergibt. Sei z der Schnittpunkt zweier solcher Geraden g_1 und g_2

$$g_1 = \{z_1 + t(z_2 - z_1) \mid t \in \mathbb{R}\}$$

$$g_2 = \{z_3 + u(z_4 - z_3) \mid u \in \mathbb{R}\}$$

wobei $z_1, z_2, z_3, z_4 \in S$. Man erhält die Gleichung:

$$z_1 + t(z_2 - z_1) = z_3 + u(z_4 - z_3).$$

Aus der einen Gleichung lassen sich zwei Gleichungen erstellen, indem man in Realteil und Imaginärteil aufspaltet. Die Koeffizienten dieser linearen Gleichungen sind aus S, aus diesem Grund sind die Lösungen t_0, u_0 in S. Der Schnittpunkt z liegt ebenfalls in S, denn z ergibt sich aus:

$$z = z_1 + t_0(z_2 - z_1) = z_3 + u_0(z_4 - z_3).$$

Dieser Fall stellt also gar keine echte Körpererweiterung dar.
2. Fall: Wir betrachten nun z also Lösung des elementaren Konstruktionsschritt, der sich durch den Schnitt von Kreis K und Geraden g ergibt.

$$K = \{k \in \mathbb{C} \mid |k - z_1|^2 = |z_3 - z_4|^2\}$$

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

wobei $z_1, z_2, z_3, z_4, z_5 \in S$. Der Schnittpunkt z ergibt sich als Lösung der Gleichung:

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

Es handelt sich hierbei um eine quadratische Gleichung in t, die Lösungen dieser lassen sich aus dem Realteil und Imaginärteilen von z_1, z_2, z_3, z_4, z_5 berechnen. Die Lösung z ist eine Nullstelle des Polynoms, das sich aus der obigen Gleichung durch Umformen ergibt. Also ist das Minimalpolynom von z über S ein Teiler von diesem eben erwähnten Polynom und hat daher einen Grad kleiner gleich 2. Daraus ergibt sich für die Körpererweiterung $S(z)/S$, wobei $K_2 = S(z)$ ein Grad $[K_2 : S] \leq 2$.
3. Fall: Wir behandeln jetzt den Fall, bei dem z im Schnitt zweier nichtidentischer Kreise K_1, K_2 liegt.

$$K_1 = \{k \in \mathbb{C} \mid |k - z_1|^2 = |z_3 - z_2|^2\}$$

$$K_2 = \{k \in \mathbb{C} \mid |k - z_4|^2 = |z_6 - z_5|^2\}$$

wobei $z_1, z_2, z_3, z_4, z_5, z_6 \in S$. Sei $r_1 = |z_3 - z_2|$ und $r_2 = |z_6 - z_5|$. Unter Verwendung der Eigenschaft $|c|^2 = c\bar{c}$ für alle $c \in \mathbb{C}$ ergeben sich zwei Gleichungen der Form, die z erfüllt:

$$z\bar{z} - z_1\bar{z} - z\bar{z_1} + z_1\bar{z_1} = r_1^2$$

$$z\bar{z} - z_2\bar{z} - z\bar{z_2} + z_2\bar{z_2} = r_2^2.$$

Durch Subtraktion erhält man eine Gleichung:

$$z(\bar{z_2} - \bar{z_1}) + \bar{z}(z_2 - z_1) + |z_1|^2 - |z_2|^2 = r_1^2 - r_2^2.$$

Sei nun $a = \bar{z_2} - \bar{z_1}$ und $b = |z_1|^2 - |z_2|^2 - r_1^2 + r_2^2$, die beide in S liegen. Die Mittelpunkte z_1 und z_2 sind verschieden, also handelt es sich dabei um eine Gerade. Dadurch kann man diesen Fall auf den vorigen Fall zurückführen.
(2)$\Leftarrow$(1) Es reicht zu beweisen, dass $\mathcal{K}(S)$ ein Teilkörper von $\mathbb{C}$ ist, der abgeschlossen unter Quadratwurzelbidlung ist. Das zeigt der Hilfsatz 7.2. □

Korollar 7.4. Sei $S \subseteq \mathbb{C}$ mit $0, 1 \in S$ und $K_0 := \mathbb{Q}(S \cup \bar{S})$. Wenn $a \in \mathbb{C}$ aus S mit Zirkel und Lineal konstruierbar ist, dann ist $[K_0(a) : K_0]$ eine Potenz von 2.

Beweis. Nach Lemma 7.3 liegt a in einem Erweiterungskörper von K_0, wobei eine Körperkette $K_0 \subseteq K_1 \subseteq K_2 \subseteq \ldots \subseteq K_n = L$ existiert mit $[K_i : K_{i-1}] = 2$ für alle $i \in \{1, \ldots, n\}$. Nach dem Gradsatz 1.1 gilt dann $[L : K_0] = 2^n$. Der Grad des Zwischenkörpers $K_0(a)$ von L/K_0 muss nach Korollar 1.2 ein Teiler von 2^n sein. Daraus ergibt sich, dass $[K_0(a) : K_0]$ eine Potenz von 2 ist.

□

Bemerkung. Mit Hilfe des Korollars 7.4 lässt sich die Unmöglichkeit gewisser geometrischer Konstruktionen beweisen.

7.2 Kreisteilungskörper

In diesem Kapitel wird das Polynom $X^n - 1$ genauer untersucht. Es hat trotz seiner Einfachheit eine äußerst wichtige Rolle in der Algebra. Vor allem die Nullstellen des Polynoms, die Einheitswurzeln werden hier behandelt. Für die Arbeit sind sie im nächsten Abschnitt von Bedeutung, denn anhand der Einheitswurzeln lassen sich Konstruierbarkeitsfragen von regelmäßigen n-Ecken beantworten. Weiters werden der Zerfällungskörper des Polynom $X^n - 1$ und seine Eigenschaften in diesem Kapitel besprochen. In den Mittelpunkt des Interesse rückt dabei immer wieder der Körper $\mathbb{Q}$ und die Kreisteilungspolynome, denn diese werden dann für das konkrete Angeben eines Körperturms bei der Vieleckkonstruktion im darauffolgenden Kapitel benötigt. In diesem Kapitel werden nur Körper K mit $charK = 0$ betrachtet. Ich habe folgende Literatur verwendete: „Algebra“ von Bosch (Kapitel 4.5, [4]), „Algebra“ von Jantzen und Schwermer (Kapitel VI §2, [7]), „Algebra“ von Karpfinger und Meyberg (Kapitel 28, [9]) und „Galois Theory“ von Edwards (Kaptiel §69, [6]).

Definition 36. Sei K ein Körper und $n \in \mathbb{N}$, dann heißt $\zeta \in K$ mit $\zeta^n = 1$ *n-te Einheitswurzel*. Von nun an bezeichne $E_n(K) := \{\zeta \in K | \zeta^n = 1\}$ die Menge der n-ten Einheitswurzeln aus K.

Beispiel 22. Wir betrachten den Körper $\mathbb{C}$, dann ist die Menge der 4-ten Einheitswurzeln gegeben durch $E_4(\mathbb{C}) = \{e^{\frac{0}{4}}, e^{\frac{2\pi i}{4}}, e^{\frac{4\pi i}{4}}, e^{\frac{6\pi i}{4}}\} = \{1, i, -1, -i\}$.

Lemma 7.5. Sei K ein Körper, dann ist $E_n(K)$ eine Untergruppe der multiplikativen Einheitengruppe $(K^*, \cdot)$

Beweis. Seien $g, h \in E_n(K)$, dann gilt für $(gh^{-1})^n = g^n(h^n)^{-1} = 1$, somit gilt $gh^{-1} \in E_n(K)$. □

Wir betrachten nun das Polynom $P = X^n - 1 \in K[X]$, so hat P in $\bar{K}$ n verschieden Nullstellen. Im Fall $p = charK \neq 0$ kann P auch weniger Nullstellen in $\bar{K}$ haben, nämlich dann wenn p ein Teiler von n ist. Für $charK = 0$ gilt aber, wie schon erwähnt folgendes:

Lemma 7.6. Sei K ein Körper und $\bar{K}$ der dazugehörige algebraische Abschluss, so gilt $|E_n(\bar{K})| = n$

Beweis. Wir betrachten das Polynom $P = X^n - 1 \in K[X]$, dann ist $P' = nX^{n-1} \neq 0$. Nach Lemma 5.3 hat P nur einfache Nullstellen, daraus folgt die Behauptung. □

Satz 7.7. Die Menge der n-ten Einheitswurzeln $E_n(K)$ ist eine endliche und zyklische Gruppe.

Beweis. Nach Lemma 7.6 ist $E_n(K)$ endlich und nach 7.5 stellt sie eine endliche Untergruppe der multiplikativen Einheitengruppe dar. Jede endliche Untergruppe der Einheitengruppe ist nach Hilfssatz 5.11 zyklisch. Daraus folgt die Behauptung. □

Beispiel 23. Jede n-te Einheitswurzel ζ ist eine Nullstelle des Polynoms $X^n - 1 \in K[X]$. Es gilt:

$$X^n - 1 = (X - 1)(X^{n-1} + X^{n-2} + \ldots + X + 1)$$

Daraus ergibt sich für eine n-te Einheitswurzel $\zeta \neq 1$:

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

Definition 37. Sei K ein Körper. Eine n-te Einheitswurzel ζ aus $\bar{K}$ wird *primitive n-te Einheitswurzel* genannt, wenn $n = ord(\zeta)$ und $E_n^*(\bar{K}) := \{\zeta \in K \mid ord(\zeta) = n\}$ bezeichnet die Menge der primitiven n-ten Einheitswurzeln.

Beispiel 24. Wir betrachten wieder den Körper $\mathbb{C}$, dann gilt $E_4^*(\mathbb{C}) = \{e^{\frac{2\pi i}{4}}, e^{\frac{6\pi i}{4}}\} = \{i, -i\}$

Um die primitiven n-ten Einheitswurzeln genauer zu untersuchen, benötigt man die Eulersche φ-Funktion

Definition 38. Für $n \in \mathbb{N}$ wird die *Eulersche φ-Funktion* definiert durch

$$\varphi(n) = |\{i \in \mathbb{Z} | 0 \leq i \leq n - 1, ggT(i, n) = 1\}|$$

Beispiel 25. $\varphi(10) = |\{1, 3, 7, 9\}| = 4$

Lemma 7.8. Sei K ein Körper, dann gilt $|E_n^*(\bar{K})| = \varphi(n)$.

Beweis. Die Gruppe $E_n(\bar{K})$ ist zyklisch von der Ordnung n. Sie enthält genau $\varphi(n)$ erzeugende Elemente. Nach Definition erzeugen die n-ten Einheitswurzeln die Gruppe $E_n(\bar{K})$, daraus folgt die Behauptung. □

Definition 39. Sei K ein Körper. Den Zerfällungskörper K_n des Polynoms $X^n - 1 \in K[X]$ nennt man *n-ten Kreisteilungskörper* über K.

Der Kreisteilungskörper K_n wird durch Adjunktion einer primitiven n-ten Einheitswurzel erzeugt. Denn eine primitive n-te Einheitswurzel erzeugt $E_n(\bar{K})$ und K_n ist der kleinste Körper, der K und $E_n(\bar{K})$ enthält. Also gilt $K_n = K(\zeta)$ mit $\zeta \in E_n^*(\bar{K})$.

Definition 40. Sei K ein Körper. Das Polynom

$$\Phi_{n,K} = \prod_{\zeta \in E_n^*(\bar{K})} (X - \zeta) \in K_n[X]$$

heißt *n-tes Kreisteilungspolynom über K*. Betrachtet man das n-te Kreisteilungspolynom über $\mathbb{Q}$ so schreibt man $\Phi_n := \Phi_{n,\mathbb{Q}}$ und nennt es nur *n-tes Kreisteilungspolynom*.

Beispiel 26. Es können sofort einige Beispiele angegeben werden: Sei $n = 1$, dann ist $e^0 = 1$ die einzige primitive Einheitswurzel und es gilt $\Phi_1 = X - 1$. Im Fall $n = 2$ ist $E_n^*(\bar{\mathbb{Q}}) = \{e^{\frac{2\pi i}{2}}\} = \{-1\}$ aus der Definition folgt $\Phi_2 = X+1$. Betrachte nun $n = 4$ aus Beispiel 24 hat das 4-te Kreisteilungspolynom die Form $\Phi_4 = (X - i)(X + i) = X^2 + 1$.

Korollar 7.9. Das n-te Kreisteilungspolynom hat Grad $\varphi(n)$.

Beweis. Nach Definition hat das n-te Kreisteilungspolynom genau die primitiven n-ten Einheitswurzeln als Nullstellen. Nach Lemma 7.8 sind das genau $\varphi(n)$, also hat das Polynom den Grad $\varphi(n)$. □

Satz 7.10. Sei K ein Körper, dann gilt $X^n - 1 = \prod_{0<d|n} \Phi_{d,K}$ für den Fall $K = \mathbb{Q}$ folgt $X^n - 1 = \prod_{0<d|n} \Phi_d$.

Beweis. Die Ordnung einer n-ten Einheitswurzel ist ein Teiler von n. Aus dieser Eigenschaft lässt sich die Menge der n-ten Einheitswurzeln $E_n(\bar{K})$ als diskjunkte Vereinigung schreiben: $E_n(\bar{K}) = \bigcup_{d|n} E_d^*(\bar{K})$. Dadurch hat $X^n - 1_K$ genau die gleichen Nullstellen in dem algebraischen Abschluss von K wie $\prod_{0<d|n} \Phi_{d,K}$. Das gilt auch für den Spezialfall der Kreisteilungspolynome über $\mathbb{Q}$. □

Satz 7.11. Das n-te Kreisteilungspolynom Φ_n ist normiert und hat ganzzahlige Koeffizienten, also $\Phi_n \in \mathbb{Z}[X]$.

Beweis. Das n-te Kreisteilungspolynom ist normiert, da aufgrund der Definition des Polynoms der höchste Koeffizient nur eins sein kann. Die zweite Behauptung erfolgt mit Induktion nach n. Der Induktionsanfang stimmt durch $\Phi_1 = X + 1 \in \mathbb{Z}[X]$. Sei nun die Behauptung für $n - 1$ richtig, dann ist $P = \prod_{d|n,d\neq n} \Phi_d$ ein Element aus $\mathbb{Z}[X]$. Wir benutzen nun die Tatsache, dass eindeutig bestimmte Polynome $Q, R \in \mathbb{Z}[X]$ existieren mit $X^n - 1 = QP + R$, wobei $degP > degR$. Andererseites gilt nach Satz 7.10 auch $X^n - 1 = \Phi_n P \in \bar{\mathbb{Q}}[X]$. Daraus folgt $QP + R = \Phi_n P$ und damit $R = P(\Phi_n - Q)$. Da für R gilt $degR < degP$, dann muss $\Phi_n = Q \in \mathbb{Z}[X]$ sein. □

Beispiel 27. Durch Satz 7.10 lassen sich die einzelnen Kreisteilungspolynome rekursiv berechnen. Um Φ_n zu erhalten, muss $X^n - 1$ durch die d-ten Kreisteilungspolynome durchdividiert werden, wo d ein Teiler von n ist.

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

Diese Beispiele lassen vermuten, dass diese Polynome als Koeffizienten nur 1 und -1 haben. Nach Bosch (vgl. [4], S. 190) stimmt diese Vermutung aber nicht, denn:

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

Um zu zeigen, dass das n-te Kreisteilungspolynom irreduzibel ist, benötigt man vorerst einen Hilfssatz:

Hilfssatz 7.12. Sei $\zeta \in K_n$ eine primitive Einheitswurzel und p eine Primzahl, die n nicht teilt, dann sind die Minimalpolynome $m_{\zeta,\mathbb{Q}}$ und $m_{\zeta^p,\mathbb{Q}}$ gleich.

Beweis. Sei $\zeta \in K_n$ eine primitive n-te Einheitswurzel. Im ersten Schritt müssen wir zeigen, dass die Minimalpolynome $m_{\zeta,\mathbb{Q}}$ und $m_{\zeta^p,\mathbb{Q}}$ ganzzahlige Koeffizienten haben. Nach Satz 7.11 ist Φ_n aus $\mathbb{Z}[X]$. Das n-te Kreisteilungspolynom zerlegt sich in $\mathbb{Z}[X]$ der Form $\Phi_n = \prod_{i=1}^{k} f_i$ wobei $f_i \in \mathbb{Z}[X]$ irreduzibel sind. Da Φ_n normiert ist haben die f_i als höchsten Koeffizient 1 oder -1. Damit sind die f_i auch über $\mathbb{Q}[X]$ irreduzibel. Ersetzt man zusätzlich einige f_i durch $-f_i$, so kann man annehmen, dass alle f_i normiert sind. Es existiert ein f_i mit $1 \leq i \leq k$ das ζ als Nullstelle hat, dann ist $f_i = m_{\zeta,\mathbb{Q}}$, da f_i irreduzibel und normiert ist. Analog lässt sich ein j finden mit $m_{\zeta^p,\mathbb{Q}} = f_j$. Sei ab jetzt $f = f_i$ und $g = f_j$. Um die Gültigkeit der Aussage zu beweisen, genügt es zu zeigen, dass $i = j$ ist. Ist das nicht der Fall, so muss fg ein Teiler von Φ_n in $\mathbb{Z}[X]$ sein und daher auch von $X^n - 1$.
Indirekt: Angenommen $fg \mid X^n - 1$ in $\mathbb{Z}[X]$. Nach der Definition von g

gilt $g(\zeta^p) = 0$, daraus lässt sich folgern, dass ζ eine Nullstelle des Polynoms $g(X^p)$ ist. Das Polynom f als Minimalpolynom von ζ teilt das Polynom $g(X^p)$ in $\mathbb{Q}[X]$. Es wurde gezeigt, dass $g \in \mathbb{Z}[X]$ ist, dann ist auch $g(X^p) \in \mathbb{Z}[X]$. Also existiert ein $h \in \mathbb{Z}[X]$, sodass $g(X^p) = fh$ ist. Wir betrachten nun den Homomorphismus $\pi : \mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ und die zugehörige Fortsetzung $\pi^* : \mathbb{Z}[X] \to \mathbb{Z}/p\mathbb{Z}[X]$. Sei nun g der Form $g = \sum_{j=0}^{m} a_j X^j$ mit $a_j \in \mathbb{Z}$, dann gilt für die Koeffizienten nach dem kleinen Fermat, dass $\pi(a_j) = \pi(a_j)^p$ in $\mathbb{Z}/p\mathbb{Z}$. Es folgt:

$$\pi^*(g)^p = (\sum_{j=0}^{m} \pi(a_j)X^j)^p = \sum_{j=0}^{m} \pi(a_j)X^{jp} = \pi^*(g(X^p)) = \pi^*(f)\pi^*(h)$$

Also teilt $\pi^*(f)$ das Polynom $\pi^*(g)^p$ in $\mathbb{Z}/p\mathbb{Z}[X]$. Sei $q \in \mathbb{Z}/p\mathbb{Z}[X]$ ein irreduzibler Faktor von $\pi^*(f)$, so teilt dieser auch $\pi^*(g)$. Es teilt daher q^2 das Produkt $\pi^*(f)\pi^*(g)$. Nach Annahme des indirekten Beweises gilt $fg \mid X^n - 1$, dadurch teilt q^2 auch $X^n - 1 = \pi^*(X^n - 1)$. Es existiert also ein s in $\mathbb{Z}/p\mathbb{Z}$, sodass gilt $X^n - 1 = q^2 s$. Wir bilden nun die Ableitung:

$$D(X^n - 1) = nX^{n-1} = 2qD(q)s + q^2 D(s)$$

Nach Voraussetzung ist p eine Primzahl die n nicht teilt, also ist $nX^{n-1} \neq 0$. Das heißt q teilt das Polynom nX^{n-1}, da q irreduzibel ist, stimmt es bis auf einen Faktor verschieden von Null mit X überein. Das ist ein Widerspruch da q das Polynom $X^n - 1$ teilt, aber X nicht. □

Satz 7.13. Das n-te Kreisteilungspolynom Φ_n ist für jedes $n \in \mathbb{N}$ irreduzibel über $\mathbb{Q}$ und $\mathbb{Z}$.

Beweis. Das Polynom Φ_n ist ein Element aus $\mathbb{Z}[X]$ und normiert, siehe Satz 7.11. Also ist Φ_n genau dann über $\mathbb{Q}$ irreduzibel, wenn Φ_n über $\mathbb{Z}$ irreduzibel ist.
Sei nun K_n der Zerfällungskörper von Φ_n über $\mathbb{Q}$. Wir wählen eine feste primitive n-te Einheitswurzel $\zeta \in K_n$. Eine beliebige primitive Einheitswurzel besitzt die Form $\zeta^m \in K_n$ mit $ggT(m, n) = 1$. Wir betrachten nun die Primfaktorenzerlegung von $m = p_1 \cdot \ldots \cdot p_k$. Dann gilt $p_i \nmid n$ für alle $i \in \{1, \ldots, k\}$, somit ist auch jedes $\zeta^{p_1 \cdot \ldots \cdot p_j}$ mit $1 \leq j \leq k$ eine primitive n-te Einheitswurzel. Durch den Hilfsatz 7.12 und Induktion folgt, dass alle $\zeta^{p_1 \cdot \ldots \cdot p_j}$ dasselbe Minimalpolynom wie ζ haben. Daher gilt auch $m_{\zeta,\mathbb{Q}}(\zeta^m) = 0$. Dieses Minimalpolynom hat also jede n-te primitive Einheitswurzel als Nullstelle, nach Satz 7.8 sind das genau $\varphi(n)$. Da ζ eine Nullstelle von Φ_n ist, gilt $m_{\zeta,\mathbb{Q}} \mid \Phi_n$. Das n-te Kreisteilungspolynom ist normiert und hat Grad $\varphi(n)$, also ist $m_{\zeta,\mathbb{Q}} = \Phi_n$ und daher ist Φ_n irreduzibel. □

Das n-te Kreisteilungspolynom Φ_n ist normiert, irreduzibel über $\mathbb{Q}$ und hat die primitiven n-ten Einheitswurzeln als Nullstelle. Es stellt somit das Minmimalpolynom einer jeden primitiven n-ten Einheitswurzel über $\mathbb{Q}$ dar. Es lässt sich damit der Grad der Körpererweiterung $\mathbb{Q}(\zeta)/\mathbb{Q}$ über den Grad des Kreisteilungspolynom Φ_n bestimmen.

Beispiel 28. Sei p eine Primzahl und ζ eine primitive p-te Einheitswurzel, dann ist

$$m_{\zeta,\mathbb{Q}} = X^{p-1} + X^p + \ldots + X + 1$$

das Minimalpolynom von ζ über $\mathbb{Q}$. Das ergibt sich aus dem Beispiel 23 und dem Satz 7.10

Satz 7.14. Sei K ein Körper und $n \in \mathbb{N}$, dann ist K_n eine endliche Galoiserweiterung von K.

Beweis. Sei $P = X^n - 1 \in K[X]$, dann ist nach Voraussetzung des Kapitels ($charK = 0$) die Ableitung $P' = nX^{n-1} \neq 0$. Nach Lemma 5.3 hat P keine mehrfachen Wurzeln in K_n. Damit ist P separabel über K. Der Kreisteilungskörper K_n ist Zerfällungskörper eines Polynoms $P \in K[X]$ und nach dem Korollar 6.16 ist die Körpererweiterung K_n/K galoissch. □

Satz 7.15. Sei $\mathbb{Q}_n/\mathbb{Q}$ eine Körpererweiterung, dann ist die Galoisgruppe $\Gamma(\mathbb{Q}_n/\mathbb{Q})$ isomorph zu der primen Restklassengruppe $\mathbb{Z}_n^*$.

Beweis. Sei $\Gamma := \Gamma(\mathbb{Q}_n/\mathbb{Q})$, $\zeta \in \mathbb{Q}_n$ eine primitive n-te Einheitswurzel und $\tau \in \Gamma$. Für jedes τ gilt $ord(\zeta) = ord(\tau(\zeta))$. Denn angenommen es existiert ein $k \in \mathbb{N}$ mit $k < n$, sodass $(\tau(\zeta))^k = 1$, dann gilt aufgrund der Eigenschaften eines Automorphismus, dass $(\tau(\zeta))^k = \tau(\zeta^k) = 1$ ist und daher $\zeta^k = 1$, das ist ein Widerspruch zu $ord(\zeta) = n$.
Also ist das Bild $\tau(\zeta)$ ebenfalls eine primitive n-te Einheitswurzel mit $\tau(\zeta) = \zeta^r$ wobei $r \in \mathbb{Z}$ und $ggT(r, n) = 1$. Die Verbindung zur primen Restklassengruppe liegt im folgenden Argument, sei $k \in \mathbb{Z}$:

$$\tau(\zeta) = \zeta^k \Leftrightarrow \zeta^r = \zeta^k \Leftrightarrow n \mid r - k \Leftrightarrow \bar{k} = \bar{r} \in \mathbb{Z}/n\mathbb{Z}$$

Sei nun $i(\tau) := \bar{r}$, dann ist diese Definition durch τ und $\tau(\zeta) = \zeta^r$ eindeutig festgelegt. Ich möchte nun einen Homomorphismus $\pi : \Gamma \to (\mathbb{Z}/n\mathbb{Z})^* = \mathbb{Z}_n^*$ aufstellen. Die Elmente sollen folgende Zuordnung besitzen: $\pi : \tau \mapsto i(\tau)$. Es bleibt nachzuweisen, dass es sich dabei um einen Homomorphismus handelt, also $\pi(\sigma\tau) = \pi(\sigma)\pi(\tau)$, wobei $\sigma, \tau \in \Gamma$. Seien $k \in i(\sigma)$ und $k' \in i(\tau)$, dann gilt:

$$\sigma(\tau(\zeta)) = \sigma(\zeta^{k'}) = (\sigma(\zeta))^{k'} = \zeta^{kk'}.$$

Daher ist $kk' \in i(\sigma\tau)$. Seien nun $i(\sigma) = \bar{m}$ und $i(\tau) = \bar{n}$, dann gilt:

$$\pi(\sigma)\pi(\tau) = \bar{m}\bar{n} = \overline{mn} = \pi(\sigma\tau).$$

Die Abbildung π ist nun ein Homomorphismus. Der Kern von π besteht nur aus dem Einselement, weil aus $i(\tau) = \bar{1}$ folgt $\tau(\zeta) = \zeta^1 = \zeta$. Da $\mathbb{Q}_n = \mathbb{Q}(\zeta)$ kann τ nur die Identität $Id_{\mathbb{Q}_n}$ sein. Wir betrachten nun die Mächtigkeiten der Bild und Urbildmenge von π:

$$|\Gamma| = [\mathbb{Q}_n : \mathbb{Q}] = [\mathbb{Q}(\zeta) : \mathbb{Q}] = deg\Phi_n = \varphi(n) = |\mathbb{Z}_n^*|.$$

Daher handelt es sich bei π um eine injektive Abbildung zwischen zwei gleichmächtigen Mengen, also ist π auch bijektiv. □

7.3 Konstruktion regelmäßiger Vielecke

Ausgerüstet mit dem Hauptsatz der endlichen Galoistheorie und den zuvor behandelten Kreisteilungskörpern kann nun eine Antwort auf die Frage gegeben werden: Welche n-Ecke sind mit Zirkel und Lineal konstruierbar? Schon die alten Griechen wussten wie 3-Ecke, 5-Ecke und 15-Ecke konstruiert werden. Weiters konnten sie ein $2n$-Eck konstruieren, wenn ein n-Eck gegeben war. Über viele Jahrhunderte, ja fast zwei Jahrtausende, tat sich nichts auf diesem Gebiet, bis der damals achtzehnjährige Gauß herausfand, wie man mit Zirkel und Lineal ein 17-Eck konstruiert. Mit Hilfe der Galoistheorie lässt sich exakt sagen, welche n-Ecke konstruierbar sind und welche nicht! Wesentlich für die Konstruktion eines regelmäßigen Vielecks sind die n-ten Einheitswurzeln über $\mathbb{Q}$. Denn sie stellen die Eckpunkte eines regelmäßigen Vielecks dar und teilen den Einheitskreis in n gleiche Sektoren. Eine weitere wichtige Rolle bei der Konstruierbarkeitsfrage eines n-Ecks spielen, wie so oft, die Primzahlen, genauer die fermatschen Primzahlen. In diesem Abschnitt richte ich mich nach den Büchern: „Algebra“ von Bosch (Kapitel 6.4, [4]), „Algebra“ von Karpfinger und Meyberg (Kapitel 28, [9]), „Die Kreisteilung und die Konstruierbarkeit regelmäßiger N-Ecke“ von Katrin Seyr (Kapitel 2.4, [12]), „Galois Theory“ von Stewart (Kapitel 17, [14]) und „Regelmäßige Körper im $\mathbb{R}_n$, $n = 2, 3, 4, 5$“ von Irmgard Kager (Kapitel 1.3.3., [8]). Für die Konstruktion des 17-Ecks habe ich die Artikel „Constructing the 17-gon“ von Artin ([3]) und „Eine Konstruktion des regelmäßigen 17-Ecks“ von Schmidt ([11]) verwendet. Alle Skizzen wurden mit der Software „GeoGebra“ erstellt.

Definition 41. Eine Primzahl der Gestalt $f_k = 2^{2^k} + 1$ mit $k \in N_0$ heißt fermatsche Primzahl.

Bemerkung. Es ist noch unbekannt, ob es unendlich viele fermatsche Primzahlen gibt. Für $0 \leq k \leq 4$ sind f_k Primzahlen:

$$f_0 = 3,\ f_1 = 5,\ f_2 = 17,\ f_3 = 257,\ f_4 = 65537$$

Für $k = 5$ erhält man keine Primzahl, denn $2^{2^5} + 1 = 4294967297 = 641 \cdot 6700417$.

Satz 7.16. Sei $3 \leq n \in \mathbb{N}$. Ein regelmäßiges n-Eck ist genau dann mit Zirkel und Lineal konstruierbar, wenn $\varphi(n)$ eine Potenz von 2 ist.

Beweis. ($\Rightarrow$) Sei ζ eine primitive n-te Einheitswurzel, die aus $0, 1$ konstruierbar ist. Betrachte die Körpererweiterung $\mathbb{Q}(\zeta)/\mathbb{Q}$, so ist nach Satz 1.6 der Grad der Köpererweiterung gleich dem Grad des Minimalpolynoms von ζ

über $\mathbb{Q}$. Es gilt $m_{\zeta,\mathbb{Q}} = \Phi_n$. Verwende nun das Korollar 7.4 und es ergibt sich für ein $k \in \mathbb{N}$:

$$\varphi(n) = [\mathbb{Q}(\zeta) : \mathbb{Q}] = 2^k.$$

($\Leftarrow$) Sei $\varphi(n)$ eine Potenz von 2. Es ist $\mathbb{Q}_n = \mathbb{Q}(\zeta)$. Nach Satz 7.15 und der Voraussetzung gilt für ein $k \in \mathbb{N}$ folgendes:

$$[\mathbb{Q}(\zeta) : \mathbb{Q}] = |\Gamma(\mathbb{Q}(\zeta)/\mathbb{Q})| = |\mathbb{Z}_n^*| = \varphi(n) = 2^k.$$

Nach dem Hauptsatz für endlich erzeugte abelsche Gruppen ist jede endlich erzeugte abelsche Gruppe das direkte Produkt ihrer zyklischen Untergruppen. Es liegt eine Gruppe $\Gamma(\mathbb{Q}(\zeta)/\mathbb{Q})$ der Ordnung 2^k vor. Man erhält also einen „Gruppenturm“ der folgenden Form:

$$\Gamma(\mathbb{Q}(\zeta)/\mathbb{Q}) = \Delta_0 \supseteq \Delta_1 \ldots \supseteq \Delta_k = \{Id\}$$

mit den Eigenschaften, $|\Delta_i| = 2^{k-i}$ und daher ist der Index jeweils $[\Delta_i : \Delta_{i-1}] = 2$ für $1 \leq i \leq k$. Da es dabei um eine endliche Galoiserweiterung handelt kann der Hauptsatz der endlichen Galoistheorie 6.15 angewendet werden. Jede Gruppe Δ_i entspricht einem Zwischenkörper $E_i := \mathcal{F}(\Delta_i)$ für $1 \leq i \leq k$. Es folgt:

$$\mathbb{Q} = E_0 \subseteq E_1 \subseteq \cdots \subseteq E_k = \mathbb{Q}(\zeta)$$

mit $[E_i : E_{i-1}] = 2$ für $1 \leq i \leq k$. Nach Satz 7.3 ist die primitive n-te Einheitswurzel ζ aus $0, 1$ konstruierbar. □

Satz 7.17. Sei $n \in \mathbb{N}$ und $2 \leq n$. Es ist $\varphi(n)$ genau dann eine Potenz von 2, wenn verschiedene Fermatsche Primzahlen $p_2, \ldots, p_k$ und eine natürliche Zahl m existieren mit $n = 2^m p_2 \cdot \ldots \cdot p_k$.

Beweis. Aus der Zahlentheorie ist bekannt: Wenn die Primfaktorzerlegung für ein $m \in \mathbb{N}$ folgendermaßen aussieht $m = p_1^{a_1} \cdot \ldots \cdot p_k^{a_k}$, dann ist $\varphi(m)$ gleich

$$\varphi(m) = p_1^{a_1-1} \cdot \ldots \cdot p_k^{a_k-1}(p_1 - 1) \cdot \ldots \cdot (p_k - 1)$$

($\Rightarrow$) Sei $\varphi(n)$ eine Potenz von 2 und $n = p_1^{a_1} \cdot \ldots \cdot p_k^{a_k}$ die Primfaktorenzerlegung von n, dann gilt wegen der obigen Bemerkung:

$$\varphi(n) = p_1^{a_1-1} \cdot \ldots \cdot p_k^{a_k-1}(p_1 - 1) \cdot \ldots \cdot (p_k - 1)$$

Daraus ergibt sich, dass $\varphi(n)$ genau dann eine Potenz von 2 ist, wenn $p_1 = 2$ (und damit $p_1 - 1 = 1$) ist und für $2 \leq i \leq k$ $a_i = 1$ und $(p_i - 1)$ eine Potenz von 2 ist. Das bedeutet, dass p_i eine fermatsche Primzahl für $2 \leq i \leq k$ ist. Die Primfaktorenzerlegung erhält die Form $n = 2^m p_2 \cdot \ldots \cdot p_k$, wobei p_i mit

$2 \leq i \leq k$ fermatische Primzahlen sind.
($\Leftarrow$) Sei nun $n = 2^m p_2 \cdot \ldots \cdot p_k$, dann gilt nach der obigen Bemerkung, dass

$$\varphi(n) = 2^{m-1}(p_2 - 1) \cdot \ldots \cdot (p_k - 1)$$

Da p_i für $2 \leq i \leq k$ eine fermatsche Primzahl ist, ergibt sich eine Potenz von 2 für $(p_i - 1)$. Daraus folgt die Behauptung. □

Beispiel 29 (Konstruktion eines 5-Ecks)**.** Um ein Konstruktionsverfahren für das 5-Eck anzugeben, muss ein entsprechender Körperturm gefunden werden. Sei nun $\zeta = e^{\frac{2\pi i}{5}}$. Wir betrachten die Körpererweiterung $\mathbb{Q}_5/\mathbb{Q}$, mit $\mathbb{Q}_5$ ist der 5-te Kreisteilungskörper über $\mathbb{Q}$ gemeint, so wie er in Definition 39 festgelegt wurde. Wir untersuchen die Galoisgruppe der zuvor erwähnten Körpererweiterung, so gilt nach Satz 7.15:

$$\Gamma(\mathbb{Q}_5/\mathbb{Q}) \cong \mathbb{Z}_5^* \cong (\mathbb{Z}_4, +).$$

Die Galoisgruppe hat Ordnung 4 und ist zyklisch, sie wird also von einem $\mathbb{Q}$-Automorphismus erzeugt. Wir nutzen jetzt die Isomorphie der Galoisgruppe aus. Die multiplikative Gruppe $\mathbb{Z}_5^*$ wird von den Potenzen von 2 modulo 5 erzeugt, so gilt:

$$2^0 = 1,\ 2^1 = 2,\ 2^2 = 4,\ 2^3 = 3.$$

Die primitiven Einheitswurzeln werden dementsprechend aufgelistet:

$$\zeta^1,\ \zeta^2,\ \zeta^4,\ \zeta^3.$$

Das Minimalpolynom von ζ der primitiven 5-Einheitswurzel über $\mathbb{Q}$ ist schon bekannt, es das 5-Kreisteilungspolynom Φ_5 und hat nach Beispiel 28 die Form:

$$m_{\zeta,\mathbb{Q}} = X^4 + X^3 + X^2 + X + 1.$$

Da das Minimalpolynom alle primitiven 5-ten Einheitswurzeln als Nullstelle hat, existiert nach Satz 3.4 ein $\mathbb{Q}$-Automorphismus $\tau \in \Gamma(\mathbb{Q}_5/\mathbb{Q})$ mit $\tau(\zeta) = \zeta^2$ und $\tau(\zeta^i) = \zeta^{2i}$. Dieser Automorphismus permutiert die Hochzahlen zyklisch:

$$\zeta^1 \to \zeta^2 \to \zeta^4 \to \zeta^3 (\to \zeta^1).$$

Dieser Automorphimus erzeugt $\Gamma(\mathbb{Q}_5/\mathbb{Q})$, mit Hilfe von τ kann jeder andere Automorphismus aus $\Gamma(\mathbb{Q}_5/\mathbb{Q})$ dargestellt werden. Untersuche nun die Untergruppen von $\Gamma(\mathbb{Q}_5/\mathbb{Q})$, die ebenfalls zyklisch sind. Die Galoisgruppe hat eine interessante und zwei triviale Untergruppen:

$$\langle \tau^0 \rangle = \{Id\} = \Delta_2,\ \langle \tau^2 \rangle = \{Id, \tau^2\} = \Delta_1,\ \langle \tau^1 \rangle = \langle \tau^3 \rangle = \Gamma(\mathbb{Q}_5/\mathbb{Q}) = \Delta_0$$

mit $[\Delta_{i-1} : \Delta_i] = 2$ für $i = 1, 2$. Es handelt sich hier um eine endliche Galoiserweiterung, also lässt sich der Hauptsatz der endlichen Galoistheorie 6.15 anwenden. Sei nun $E_i := \mathcal{F}(\Delta_i)$. Es ergibt sich eine Zwischenkörperstruktur

$$\mathbb{Q} = E_0 \subseteq E_1 \subseteq E_2 = \mathbb{Q}_5$$

mit $[E_i : E_{i-1}] = 2$ für $i = 1, 2$. Die Körpererweiterung hat also nur einen echten Zwischenkörper E_1. Suche nun ein w_1, für das gilt $E_1 = \mathbb{Q}(w_1)$. Es kann $w_1 = \zeta + \zeta^4$ gewählt werden, da $w_1 \notin \mathbb{Q}$ und w_1 liegt aufgrund von $\tau^2(w_1) = \tau^2(\zeta) + \tau^2(\zeta^4) = \zeta^4 + \zeta = w_1$ in E_1. Da es sich um eine Körpererweiterung zweiten Grades handelt, wird E_1 durch die Adjunktion von w_1 an $\mathbb{Q}$ erzeugt. Wir bestimmen nun das Minimalpolynom $m_{w_1,\mathbb{Q}}$. Da w_1 eine Nullstelle $m_{w_1,\mathbb{Q}}$ ist muss auch $w_2 = \tau(w_1) = \zeta^2 + \zeta^3$ eine sein, daraus ergibt sich folgender Ansatz:

$$(X - w_1)(X - w_2) = X^2 - (w_1 + w_2)X + w_1 w_2.$$

Aufgrund der Identität $\Phi_5(\zeta) = \zeta^4 + \zeta^3 + \zeta^2 + \zeta + 1 = 0$ gilt:

$$\begin{aligned} w_1 + w_2 &= \zeta^4 + \zeta^3 + \zeta^2 + \zeta = -1 \\ w_1 w_2 &= \zeta^4 + \zeta^3 + \zeta^2 + \zeta = -1. \end{aligned}$$

Also hat das Minimalpolynom die Form:

$$m_{w_1,\mathbb{Q}} = X^2 + X - 1.$$

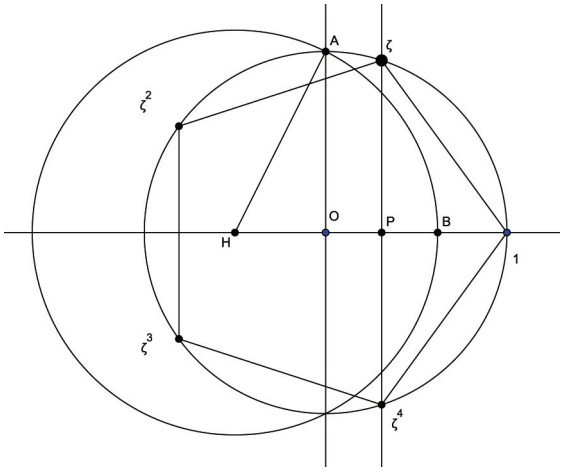
Es gilt $\zeta + \zeta^{-1} = 2cos(\frac{2\pi}{5})$ und $(\zeta + \zeta^{-1})^2 = 1 - \zeta - \zeta^{-1}$. Dadurch ist $2cos(\frac{2\pi}{5})$ auch Lösung des Minimalpolynoms. Um die Nullstellen des Minimalpolynoms zu erhalten, verwenden wir die quadratische Lösungsformel, dann ergibt sich für die Lösung $w_1 > 0$ folgendes:

$$2cos(\frac{2\pi}{5}) = w = \frac{1}{2}(\sqrt{5} - 1).$$

Schon jetzt lässt sich das 5-Eck konstruieren, da $cos(\frac{2\pi}{5}) = \frac{1}{4}(\sqrt{5} - 1)$ der Realteil der primitven Einheitswurzel ζ ist. Der Erweiterungskörper E_1 hat also die Form $\mathbb{Q}(\sqrt{5})$.
Die Zeichnung lässt sich wie folgt erstellen:

- Wir beginnen mit dem Einheitskreis.
- Wir halbieren den Radius auf der x-Achse und erhalten H.
- Aufgrund des Satzes von Pythagoras hat Strecke $\overline{HA}$ die Länge $\frac{\sqrt{5}}{2}$.

- Wir zeichenen einen Kreis mit Mittelpunkt H und Radius $\overline{HA}$ und durch den Schnitt mir der x-Achse erhalten wir den Punkt B.
- Die Strecke $\overline{OB}$ hat die Länge $\frac{\sqrt{5}}{2} - \frac{1}{2}$.
- Durch das Halbieren der Strecke $\overline{OB}$ erhält man die gesuchte Länge $\frac{1}{4}(\sqrt{5} - 1)$.
- Wir konstruieren das Lot von B auf die x-Achse. Der Schnitt des Lots mit dem Einheitskreis liefert ζ.
- Durch das Abschlagen der Länge $|\zeta - 1|$ erhält man die restlichen Eckpunkte des 5-Ecks. Dieses Vorgehen entspricht dem Schnitt zweier Kreise (diese wurden zur besseren Übersichtlichkeit in der Zeichnung weggelassen).



Beispiel 30 (7-Eck)**.**

Es gilt $\varphi(7) = 6$ und 6 ist keine Potenz von 2. Nach Satz 7.16 ist das 7-Eck nicht konstruierbar!

Durch Satz 7.16 kann man leicht zeigen, dass das 7-Eck nicht konstruierbar ist. Diese Aussage lässt jedoch auch ohne den besagten Satz zeigen: Wenn die primitive 7-te Einheitswurzel $z = e^{\frac{2\pi i}{7}}$ konstrierbar ist, so ist auch $a = 2\cos(\frac{2\pi}{7})$ konstruierbar, denn

$$z + \bar{z} = \cos(\frac{2\pi}{7}) + i\sin(\frac{2\pi}{7}) + \cos(\frac{2\pi}{7}) - i\sin(\frac{2\pi}{7}) = 2\cos(\frac{2\pi}{7}) = a$$

Das Minimalpolynom von z ist Φ_7, daraus und aus $z\bar{z} = 1$ bzw. $\bar{z} = z^{-1}$ folgt:

$$\begin{aligned}
&z^6 + z^5 + z^4 + z^3 + z^2 + z + 1 = 0\\
&\bar{z} + \bar{z}^2 + \bar{z}^3 + z^3 + z^2 + z + 1 = 0\\
&z^3 + z + \bar{z} + \bar{z}^3 + z^2 + \bar{z}^2 + 1 = 0\\
&z^3 + 3z + 3\bar{z} + \bar{z}^3 + z^2 + 2 + \bar{z}^2 - 2z - 2\bar{z} - 1 = 0\\
&z^3 + 3z^2\bar{z} + 3z\bar{z}^2 + \bar{z}^3 + z^2 + 2\bar{z}z + \bar{z}^2 - 2z - 2\bar{z} - 1 = 0\\
&(z + \bar{z})^3 + (z + \bar{z})^2 - 2(z + \bar{z}) - 1 = 0\\
&a^3 + a^2 - 2a - 1 = 0.
\end{aligned}$$

Wir betrachten nun das Polynom $P = X^3 + X^2 - 2X - 1$. Für a ergibt sich dadurch das Minimalpolynom

$$m_{a,\mathbb{Q}} = X^3 + X^2 - 2X - 1 \in \mathbb{Q}[X]$$

denn a ist eine Nullstelle, es ist normiert und irreduzibel, verwende das Eisensteinkriterium mit $p = 2$ bei einer Verschiebung $m_{a,\mathbb{Q}}(2X + 2)$. Damit hat die Körpererweiterung $\mathbb{Q}(a)/\mathbb{Q}$ den Grad $[\mathbb{Q}(a) : \mathbb{Q}] = 3$. Nach Satz 7.4 ist a und daher das 7-Eck nicht mit Zirkel und Lineal konstruierbar.

Beispiel 31 (Konstruktion eines 17-Ecks)**.** Wiederum muss ein entsprechender Körperturm gefunden werden. Sei diesmal $\zeta = e^{\frac{2\pi i}{17}}$ und wir betrachten die Körpererweiterung $\mathbb{Q}_{17}/\mathbb{Q}$, dann gilt nach Satz 7.15 für die Galoisgruppe:

$$\Gamma(\mathbb{Q}_{17}/\mathbb{Q}) \cong \mathbb{Z}_{17}^* \cong (\mathbb{Z}_{16}, +).$$

Die Galoisgruppe hat die Ordnung 16 und ist wieder zyklisch. Die multiplikative Gruppe $\mathbb{Z}_{17}^*$ wird von der Potenz 3 modulo 17 erzeugt, so gilt:

$$3^0 = 1,\ 3^1 = 3,\ 3^2 = 9,\ 3^3 = 10,\ 3^4 = 13, \ldots$$

Dementsprechend listen wir die primitiven Einheitswurzeln

$$\zeta^1\ \zeta^3\ \zeta^9\ \zeta^{10}\ \zeta^{13}\ \zeta^5\ \zeta^{15}\ \zeta^{11}\ \zeta^{16}\ \zeta^{14}\ \zeta^8\ \zeta^7\ \zeta^4\ \zeta^{12}\ \zeta^2\ \zeta^6.$$

Es existiert wieder nach Satz 3.4 ein $\mathbb{Q}$-Automorphismus $\tau \in \Gamma(\mathbb{Q}_{17}/\mathbb{Q})$ mit $\tau(\zeta) = \zeta^3$ und $\tau(\zeta^i) = \zeta^{3i}$. Dieser Automorphismus permutiert die Einheitswurzeln folgendermaßen:

$$\begin{aligned}
&\zeta^1 \to \zeta^3 \to \zeta^9 \to \zeta^{10} \to \zeta^{13} \to \zeta^5 \to \zeta^{15} \to \zeta^{11} \to\\
&\zeta^{16} \to \zeta^{14} \to \zeta^8 \to \zeta^7 \to \zeta^4 \to \zeta^{12} \to \zeta^2 \to \zeta^6.
\end{aligned}$$

Dadurch ergeben sich folgende Untergruppen von $\Gamma(\mathbb{Q}_{17}/\mathbb{Q})$:

$$\langle\tau^0\rangle = \{Id\} = \Delta_4,\ \langle\tau^8\rangle = \Delta_3,\ \langle\tau^4\rangle = \Delta_2,\ \langle\tau^2\rangle = \Delta_1,\ \langle\tau\rangle = \Gamma(\mathbb{Q}_{17}/\mathbb{Q}) = \Delta_0$$

mit $[\Delta_{i-1} : \Delta_i] = 2$ für alle $i = 1, 2, 3, 4$. Die hier behandelte Körpererweiterung ist eine endliche Galoiserweiterung. Durch Anwendung des Hauptsatzes der endlichen Galoistheorie 6.15 ergibt sich die Zwischenkörperstruktur, sei wiederum $E_i = \mathcal{F}(\Delta_i)$:

$$\mathbb{Q} = E_0 \subseteq E_1 \subseteq E_2 \subseteq E_3 \subseteq E_4 = \mathbb{Q}_{17}$$

mit $[E_i : E_{i-1}] = 2$ für $i = 1, 2, 3, 4$. Die Körpererweiterung hat also drei echte Zwischenkörper. Es werden jetzt primitive Elemente w_1, w_2 und w_3 gesucht, sodass $E_1 = \mathbb{Q}(w_1), E_2 = E_1(w_2), E_3 = E_2(w_3)$ erfüllt ist.
Für w_1 kann gewählt werden $w_1 = \zeta + \zeta^9 + \zeta^{13} + \zeta^{15} + \zeta^{16} + \zeta^8 + \zeta^4 + \zeta^2$, da $w_1 \notin \mathbb{Q}$ und w_1 liegt im Fixkörper E_1, weil $\tau^2(w_1) = w_1$. Da die Körpererweiterung zweiten Grades ist, wird E_1 durch Adjunktion von w_1 an $\mathbb{Q}$ erzeugt. Wir bestimmen nun das Minimalpolynom $m_{w_1,\mathbb{Q}}$, das als Nullstelle auch $v_1 = \tau(w_1) = \zeta^3 + \zeta^{10} + \zeta^5 + \zeta^{11} + \zeta^{14} + \zeta^7 + \zeta^{12} + \zeta^6$ haben muss. Da es sich um eine Körpererweiterung zweiten Grades handelt, ergibt sich der Ansatz mittels einem Minimalpolynom zweiten Grades:

$$(X - w_1)(X - v_1) = X^2 - (w_1 + v_1)X + w_1v_1.$$

Das Ergebnis der Summe $w_1 + w_2 = -1$ ergibt sich aus dem Kreisteilungspolynom, da $\Phi_{17}(\zeta) = 0$. Das Produkt w_1v_1 wird zu einer Summe aus 64 Summanden mit dem Ergebnis $w_1v_1 = -4$. Das ergibt das Minimalpolynom:

$$m_{w_1,\mathbb{Q}} = X^2 + X - 4.$$

Das Element w_1 lässt sich umschreiben zu $w_1 = (\zeta + \zeta^{-1}) + (\zeta^2 + \zeta^{-2}) + (\zeta^4 + \zeta^{-4}) + (\zeta^8 + \zeta^{-8})$, da $\zeta^i + \zeta^{i-1} > 0$ gilt, ist auch $w_1 > 0$. Nun lassen sich die Lösungen des Minimalpolynoms wie folgt zuordnen:

$$w_1 = \frac{1}{2}(\sqrt{17} - 1),\ v_1 = -\frac{1}{2}(\sqrt{17} + 1).$$

Als nächstes wird E_2 untersucht, dabei gilt es ein w_2 zu finden, das durch Adjunktion an E_1 den Körper E_2 erzeugt. Es stellt sich heraus, dass $w_2 = \zeta + \zeta^{13} + \zeta^{16} + \zeta^4$ gewählt werden kann, denn $\tau^4(w_2) = w_2$ und $w_2 \notin E_1$, da $\tau^2(w_2) = \zeta^2 + \zeta^9 + \zeta^{15} + \zeta^8 \neq w_2$, also liegt w_2 nicht im Fixkörper von $\langle\tau^2\rangle$. Verwende den gleichen Ansatz für das Minimalpolynom wie zuvor, mit $v_2 = \tau^2(w_2) = \zeta^9 + \zeta^{15} + \zeta^8 + \zeta^2$.

$$m_{w_2,E_1} = (X - w_2)(X - v_2) = X^2 - (w_2 + v_2)X + w_2v_2.$$

Die Summe w_2+v_2 hat das Ergebnis $\zeta+\zeta^9+\zeta^{13}+\zeta^{15}+\zeta^{16}+\zeta^8+\zeta^4+\zeta^2 = w_1$ und das Produkt liefert aufgrund von $\Phi_{17}(\zeta) = 0$ das Ergebnis $w_2v_2 = \zeta + \zeta^2 + \zeta^3 + \ldots + \zeta^{15} + \zeta^{16} = -1$. Wir erhalten das Minimalpolynom

$$m_{w_2,E_1} = X^2 - w_1X - 1.$$

Dadurch, dass $w_2 = (\zeta + \zeta^{-1}) + (\zeta^4 + \zeta^{-4}) > 0$ ist, lassen sich die Lösungen von m_{w_2,E_1} wie folgt zuordnen:

$$w_2 = \frac{1}{2}(\sqrt{w_1^2+4} + w_1),\ v_2 = -\frac{1}{2}(\sqrt{w_1^2+4} - w_1).$$

Es fehlt noch w_3 mit $E_3 = E_2(w_2)$. Wir wählen $w_3 = \zeta + \zeta^{16}$, als ein Element von E_3, da $\tau^8(w_3) = w_3$. Weiters ist $w_3 \notin E_2$ da $\tau^4(w_3) = \zeta^{13} + \zeta^4 \neq w_3$. Wir wählen $v_3 = \zeta^{13} + \zeta^4$. Der Ansatz für das Minimalpolynom m_{w_3,E_2} ist analog zu den vorigen. Es werden die Berechnungen $w_3+v_3 = \zeta+\zeta^{13}+\zeta^{16}+\zeta^4 = w_2$ und $w_3v_3 = \zeta^{14} + \zeta^{12} + \zeta^5 + \zeta^3 = \frac{1}{2}(w_2^2 - v_2 - 4) =: a$ benötigt. Das ergibt das Minimalpolynom:

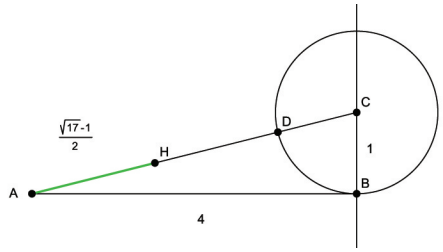
$$m_{w_3,E_2} = X^2 - w_2X + a$$

Sowohl das Element $w_3 = \zeta + \zeta^{-1} > 0$, also auch $v_3 = \zeta^4 + \zeta^{-4} > 0$. Da $\zeta^k + \zeta^{-k} = 2cos(\frac{2k\pi}{17})$ ist, sind beide Lösungen reell. Es ist $v_3 = 2cos(\frac{8\pi}{17}) < 2cos(\frac{2\pi}{17}) = w_3$. Es gilt also $0 < v_3 < w_3$ und deswegen lassen sich die Lösungen der quadratischen Gleichung zuordnen und ergeben:

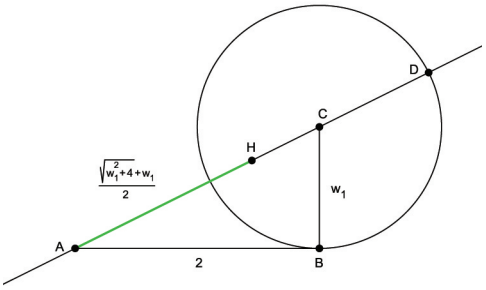
$$w_3 = \frac{1}{2}(\sqrt{w_2^2 - 4a}+w_2) = \frac{\sqrt{-w_2^2 + 2v_2 + 8} + w_2}{2},\ v_3 = -\frac{1}{2}(\sqrt{w_2^2 - 4a}-w_2).$$

Daraus lässt sich bereits das 17-Eck konstruieren, da $w_3 = \zeta+\zeta^{-1} = 2cos(\frac{2\pi}{17})$ und $cos(\frac{2\pi}{17})$ ist der Realteil von ζ. Wir werden nun Schritt für Schritt die primitiven Element konstruieren, bis wir bei w_3 angekommen sind. Es gibt sehr schöne Verfahren zur Konstruktion eines 17-Ecks, wie etwa von Hardy und Wright (vgl. [14], S.170ff). Ich werde kein direktes Verfahren angeben, sondern die einzelnen Schritte, die benötigt werden um den Realteil $cos(\frac{2\pi}{17})$ mit Zirkel und Lineal zu zeichnen. Die Konstruktion lässt sich folgendermaßen erstellen:

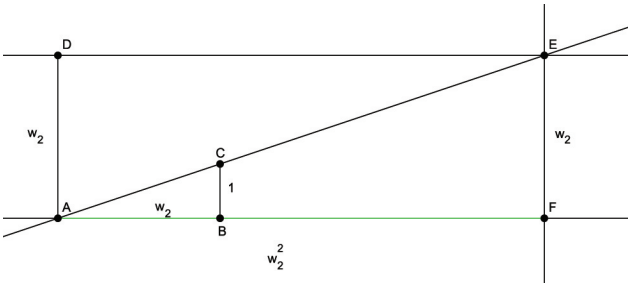
- Die Wurzel aus 17 lässt sich mit Hilfe des Satzes von Pythagoras zeichnen. Wir erstellen dazu ein rechtwinkeliges Dreieck ABC mit den Katheten der Länge 4 und der Länge 1. Anschließend wird durch den Schnitt eines Kreises der Länge 1 mit der Hypothenuse die Länge $\sqrt{17}$ um eins vermindert, das entspricht der Strecke $\overline{AD}$. Das Halbieren liefert die Strecke $\overline{AH}$, welche die Länge w_1 hat.



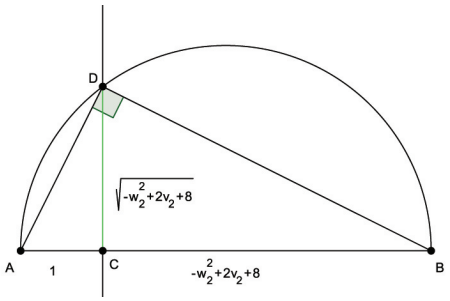
- Wir erstellen ein rechtwinkeliges Dreieck ABC mit den Längen 2 und w_1. Die Hypothenuse hat nun die Länge $\sqrt{w_1^2 + 2^2}$. Wiederum konstruieren wir einen Kreis mit Radius w_1, sodass wir die Hypothenuse um a verlängern. Das Halbieren der Strecke liefert den Wert $w_2 = \frac{\sqrt{w_1^2+4}+w_1}{2}$. Analog wird $v_2 = \frac{\sqrt{w_1^2+4}-w_1}{2}$ konstruiert, nur das die Hypothenuse um a verkürzt wird. Die Länge v_2 bnötigt man für die weitern Schritte.



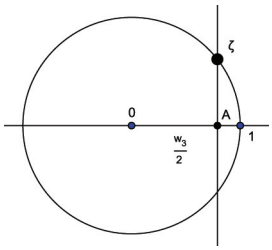
- Für die Konstruktion von $w_3 = \frac{\sqrt{-w_2^2+2v_2+8}+w_2}{2}$ betrachten wir zunächst, wie wir w_2^2 mit Zirkel und Lineal konstruieren können. Wir zeichnen zunächst eine Gerade, auf der wie die Länge w_2 auftragen, das entspricht der Strecke $\overline{AB}$. Danach konstruieren wir eine Parallele dazu mit dem Abstand w_2. Normal auf die Gerade und durch den Punkt B tragen wir die Strecke der Länge 1 auf und erhalten den Endpunkt C. Wir konstruieren nun eine Gerade durch die Punkte A und C. Im Schnittpunkt von dieser eben konstruierten Geraden und der Parallelen liegt E. Wir zeichnen das Lot von E auf die erste konstruierte Gerade und erhalten F. Nach dem Strahlensatz gilt $\overline{AF} : \overline{AB} = \overline{EF} : \overline{BC}$ und das ist $\frac{|\overline{AF}|}{w_2} = \frac{w_2}{1}$. Also hat $\overline{AF}$ die Länge w_2^2.



Die Konstruktion der Länge $-w_2^2 + 2v_2 + 8$, welche aufgrund $w_3 \in \mathbb{R}$ größer 0 ist, wird durch Anhängen der bereits bekannten Längen erreicht. Der Satz von Thales und der Höhensatz liefern $\sqrt{-w_2^2 + 2v_2 + 8}$.



Wir hängen die Länge w_2 an $\sqrt{-w_2^2 + 2v_2 + 8}$ an und das Halbieren liefert w_3. Wir konstruieren eine Strecke der Länge $\frac{w_3}{2}$ entlang der x-Achse ausgehend vom Ursprung. Wir erstellen das Lot, normal auf die x-Achse und durch den Endpunkt der Strecke. Der erste Eckpunkt entsteht durch den Schnitt von Lot und Einheitskreis.



Literatur

[1] Artin E., (1973) *Galoissche Theorie*, Frankfurt am Main.

[2] Artin M., (1998) *Algebra*, Basel.

[3] Artin M., (2011) *Constructing the 17-gon*, URL: `http://math.mit.edu/classes/18.702/seventeengon5.pdf`, 14.01.2012.

[4] Bosch S., (2001) *Algebra*, Berlin.

[5] Cigler J., (1995) *Körper Ringe Gleichungen*, Heidelberg[u.a].

[6] Edwards H.M., (1984) *Galois Theory*, New York.

[7] Jantzen J.C. und Schwermer J. (2006) *Algebra*, Berlin.

[8] Kager I., (1992) *Regelmäßige Körper im* $\mathbb{R}_n$, Wien.

[9] Karpfinger C. und Meyberg K.,(2010) *Algebra Gruppen-Ringe-Körper*, Heidelberg.

[10] Sautoy M., (2008) *Das Geheimnis der Symmetrie*, München.

[11] Schmidt C., (2004) *Eine Konstruktion des regelmäßigen 17-Ecks*, URL: `http://www.math.kit.edu/user/mi2/schmidt/WS04/skVl/siebzehneck.pdf`, 14.01.2012.

[12] Seyr K., (1992) *Die Kreisteilung und die Konstruierbarkeit regelmäßiger N-Ecke*, Wien.

[13] Staudner O., (1998) *Galois-Theorie*, Wien.

[14] Steward I., (1989) *Galois Theory*, London.

Zusammenfassung

Diese Diplomarbeit beschäftigt sich mit Galoistheorie und ihrer Anwendung auf die Konstruktion von regelmäßigen Vielecken mit Zirkel und Lineal. In den ersten sechs Kapiteln wird der Hauptsatz der endlichen Galoistheorie erarbeitet. Die Arbeit beginnt mit der Betrachtung von einfachen und algebraischen Körpererweiterungen. Im Anschluss wird bewiesen, dass jeder Körper K einen algebraischen Abschluss besitzt. Über die Einführung von Zerfällungskörper zeigen wir, dass je zwei algebraische Abschlüsse von K bis auf K-Isomorphie eindeutig sind. Weiters werden normale und separable Körpererweiterungen und ihre Eigenschaften untersucht. Diese sind für die Behandlung von galoisschen Erweiterungen besonders wichtig. Wir beantworten im Anschluss die Fragestellung, wie viele Zwischenkörper eine endliche, normale Körpererweiterung L/K hat. Mit Hilfe der Galoiskorrespondenz können wir die Zwischenkörper eindeutig Untergruppen der Galoisgruppe zuordnen. Das Auffinden von Zwischenkörper wird auf das Auffinden von Untergruppen reduziert. Ausgerüstet mit dem Hauptsatz der endlichen Galoistheorie werden im siebenten Kapitel Konstruierbarkeitsfragen behandelt. Dabei verwenden wir die erarbeitete Sprache der Körpererweiterungen und wenden diese auf Konstruktionsprobleme an. Es wird gezeigt, dass die Menge aller konstruierbaren Punkte $\mathcal{K}(S)$ ausgehend von einer Startmenge S mit $0, 1 \in S$ ein Teilkörper von $\mathbb{C}$ ist. Im Abschnitt Kreisteilungskörper behandeln wir die Einheitswurzeln, diese sind der Schlüssel zur Konstruktion von regelmäßigen Vielecken, da sie als die Eckpunkte von regelmäßigen Eckpunkten betrachtet werden können. Schlussendlich wird genau angegeben, welches n-Eck mit Zirkel und Lineal konstruierbar ist und welches nicht. Wir erstellen einen Zusammenhang zwischen den fermatschen Primzahlen und der Konstruierbarkeit von regelmäßigen n-Ecken. Ein regelmäßiges n-Eck ist genau dann konstruierbar, wenn $\varphi(n)$ eine Potenz von 2 ist. Abschließend werden wir mit Hilfe der Galoistheorie das 5-Eck und das 17-Eck konstruieren. Dabei geben wir jeweils einen entsprechenden Körperturm an, dieser liefert uns ein Konstruktionsverfahren der beiden Vielecke.

Summary

This diploma thesis deals with Galois theory and its application to constructions with compass and ruler. The first six chapters are a preparation of the fundamental theorem of Galois theory. At first we analyze field extensions, in particular algebraic and simple extensions. Furthermore we prove an important theorem, which is known as "tower law". Then we show that every field K has an algebraic closure. With the help of the theory of splitting fields, we prove that an algebraic closure is unique up to an isomorphism, which fixes K. Afterwards normal and separable field extensions are introduced. These special extensions are important for Galois theory. In the sixth chapter we set up a bijection between the set of intermediate fields of a finite Galois extension and the set of subgroups of the Galois group. This function is called the Galois correspondence. The determination of intermediate fields of a Galois extension is reduced to the determination of the subgroups of the Galois group. The next chapter gives an application of the Galois theory. At first we consider simple constructions with compass and ruler and connect the language of field extensions to constructions with ruler and compass. In the next chapter cyclotomic fields are introduced, where we consider primitive roots. The complex primitive roots of unity are the key to construct regular polygons. We prove that the regular n-gon is constructible if and only if $\varphi(n)$ is a power of 2, where $\varphi(n)$ is Euler's totient function. Furthermore we reduce the problem to number theory, by giving a connection to the Fermat primes. At the end the fundamental theorem of Galois theory is used to construct the 5-gon and the 17-gon, by finding an explicit tower of fields.

Curriculum Vitae

Persönliche Daten

Name:	Christian Dorner
Geburtstag:	31. August 1987
Geburtsort:	Baden
Staatsbürgerschaft:	Österreich

Schulbildung

1994-1998	Volksschule in Bad Vöslau
1998-2006	Realgymnasium mit Darstellender Geometrie
26. Juni 2006	Matura mit gutem Erfolg bestanden
WS 2006/07	Beginn des Studiums Lehramt Mathematik und Geographie und Wirtschaftskunde an der Universität Wien
4. Juni 2009	Erste Diplomprüfung bestanden
19. Jänner 2011	Erhalt des Leistungsstipendiums nach dem Studienförderungsgesetz der Universität Wien
SS 2011	Beginn des Bachelorstudiums Mathematik an der Universität Wien
20. Jänner 2012	Erhalt des Leistungsstipendiums nach dem Studienförderungsgesetz der Universität Wien

Praktische Erfahrung

August 2004	Vereinigte Volksbanken Baden-Mödling-Liesing tätig als Ferialpraktikant in der Abteilung Marktfolge Passiv Dienstleistungen
Juli 2005	Vereinigte Volksbanken Baden-Mödling-Liesing tätig als Ferialpraktikant in der Abteilung Marktfolge Passiv Dienstleistungen
August 2006	Vereinigte Volksbanken Baden-Mödling-Liesing tätig als Ferialpraktikant in der Abteilung Marktfolge Passiv Dienstleistungen

August 2007	Volksbank Baden e. Gen. tätig als Ferialpraktikant in der Abteilung Marktfolge Passiv Dienstleistungen
August 2008	Volksbank Baden e. Gen. tätig als Ferialpraktikant in der Abteilung Marktfolge Passiv Dienstleistungen
August 2009	Volksbank Baden e. Gen. tätig als Ferialpraktikant in der Abteilung Private Banking
Okt. 09-Sept. 10	Teilzeitbeschäftigter bei Volksbank Baden e. Gen. in der Abteilung Marktfolge Passiv Dienstleistungen
Seit Jänner 2011	Freier Dienstnehmer bei der Firma learning4life, zur Abhaltung von Trainings und Nachhilfe
WS 2011/12	Tutor für Unterrichtsplanung am Institut für Geographie und Regionalforschung der Universität Wien

Bad Vöslau, 15. Februar 2012