Skript zur Vorlesung
Vertiefungsmodul Körpertheorie

Bachelor Mathematik und Lehramt,
Sommersemester 2014

Catherine Meusburger

Department Mathematik
Friedrich-Alexander-Universität Erlangen-Nürnberg

catherine.meusburger@math.uni-erlangen.de

(Stand: 18. Juli 2014)

Die Vorlesung orientiert sich an dem Lehrbuch *Christian Karpfinger, Kurt Meyberg, Algebra: Gruppen - Ringe - Körper (Springer Spektrum).*

Weitere Lehrbücher, die ich zur Vorbereitung der Vorlesung genutzt habe und auch als Literatur für Studierende empfehle, sind:

- Gerd Fischer, Lehrbuch der Algebra (Springer Spektrum),
- Siegfried Bosch, Algebra (Springer),
- Herold M. Edwards, Galois Theory (Springer Graduate Texts in Mathematics),
- Victor V. Prasolov, Polynomials (Algorithms and Computation in Mathematics 11, Springer),
- David J. Winter, The structure of Fields (Springer Graduate Texts in Mathematics).

Gelegentlich habe ich auch die Vorlesungsskripten von Herrn Prof. Christoph Schweigert (Universität Hamburg) von Herrn Prof. Wolfgang Soergl (Universität Freiburg) genutzt.

Danksagung: Ich bedanke mich bei Manuel Herbst und Dr. Yurii Savchuk für Kommentare, Hinweise und Ideen zum Skript und den Übungen. Bei Manuel Herbst bedanke ich mich ausserdem für seine sehr hilfreichen Verbesserungsvorschläge zu den Musterlösungen der Hausaufgaben und die Überarbeitung dieser Musterlösungen. Bei Prof. Friedrich Knop und Kay Paulus bedanke ich mich für Hinweise zur Vorlesung. Weiterhin bedanke ich mich bei allen Hörerinnen und Hörern der Vorlesung, die mir durch ihre Fragen, Kommentare und Hinweise geholfen haben, die Vorlesung und das Skript zu verbessern.

Bitte schicken Sie Korrekturen und Bemerkungen zu diesem Skript an
`catherine.meusburger@math.uni-erlangen.de`.

Inhaltsverzeichnis

1 Körpererweiterungen **4**

1.1 Grundlagen 5

1.2 Körpererweiterungen 13

1.3 Einfache und algebraische Körpererweiterungen 18

1.4 Algebraischer Abschluss und Zerfällungskörper 22

1.5 Normale und separable Körpererweiterungen 29

1.6 Endliche Körper 39

1.7 Übungen zu Kapitel 1 43

2 Galoistheorie **48**

2.1 Die Galois-Korrespondenz 48

2.2 Algebraische Galoiserweiterungen 53

2.3 Kreisteilungskörper 58

2.4 Übungen zu Kapitel 2 66

3 Anwendungen **71**

3.1 Konstruktionen mit Zirkel und Lineal 71

3.2 Auflösbarkeit algebraischer Gleichungen durch Radikale 80

3.3 Übungen zu Kapitel 3 86

A Übersichtstabellen **88**

B Kreisteilungspolynome **91**

1 Körpererweiterungen

Die Anfänge der Körpertheorie liegen im 19. Jahrhundert und gehen auf Nils Hendrik Abel und Évariste Galois zurück, die durch die Frage nach der **Auflösbarkeit von polynomialen Gleichungen** bzw. der Charakterisierung von **Nullstellen von Polynomen** motiviert waren. Diese arbeiteten jedoch nicht mit einer expliziten Definition eines Körpers oder einer Körpererweiterung. Der Begriff des Körpers wurde erst 1871 von Richard Dedekind und der Begriff der Körpererweiterung 1881 von Leopold Kronecker entwickelt. Diese beruhten vorwiegend auf den Körpern $\mathbb{R}, \mathbb{C}$ und $\mathbb{Q}$ und deren Erweiterungen. Das abstrakte Konzept eines Körpers wurde erst 1893 durch Heinrich Weber eingeführt.

Die zweite wichtige Motivation für die Entwicklung der Körpertheorie waren Fragen nach **geometrischen Konstruierbarkeit** von Größen **mit Zirkel und Lineal**. Diese wurden seit der Antike relativ erfolglos untersucht, und erst die Körpertheorie stellte den konzeptionellen Rahmen bereit, um diese Probleme zu lösen bzw. deren Unlösbarkeit zu beweisen. Die vier **klassischen geometrischen Probleme** dieser Art sind:

1. **Winkeldrittelung:** Ein gegebener Winkel soll mit Zirkel und Lineal in drei gleiche Teile zerlegt werden.
2. **Konstruktion eines regulären n-Ecks:** In einen vorgegebenen Kreis soll mit Zirkel und Lineal ein reguläres n-Eck ($n \geq 3$) einbeschrieben werden.
3. **Quadratur des Kreises:** Zu einem gegebenen Kreis soll mit Zirkel und Lineal ein Quadrat konstruiert werden, dessen Fächeninhalt gleich dem des Kreises ist.
4. **Würfelverdoppelung (Delisches Problem):** Aus einer Kante eines vorgegebenen Würfels soll mit Zirkel und Lineal die Kante eines Würfels doppelten Volumens konstruiert werden.

Der entscheidende Schritt zur Lösung dieser Probleme war ihre Zurückführung auf die Theorie von Zahlenkörpern. So konnte man dann beweisen, dass die Winkeldrittelung, die Quadratur des Kreises und die Würfelverdoppelung unmöglich sind. Die Konstruktion des regulären n-Ecks läßt sich mit Hilfe der Körpertheorie auf die Fermatschen Primzahlen zurückführen. Man konnte zeigen, dass ein reguläres n-Eck genau dann konstruierbar ist, wenn seine **Eulerzahl** $\varphi(n) = |\{a \in \{1, ..., n\} : \mathrm{ggT}(a, n) = 1\}|$ eine Zweierpotenz ist. Ist $n = p$ eine Primzahl, so ist $\varphi(p) = p - 1$, und die Frage reduziert sich auf die Suche nach Primzahlen der Form $F_k = 2^{2^k} + 1$ mit $k \in \mathbb{N}_0$, die **Fermatschen Primzahlen**. Von diesen sind nur fünf bekannt (3, 5, 17, 257, 65537), und für alle fünf wurde die Konstruktion explizit durchgeführt. Für 3 und 5 war die Konstruktion seit der Antike bekannt, der Beweis der Konstruierbarkeit des regulären 17-Ecks geht auf Gauss zurück (1706) aber die Konstruktion selbst wude erst 1825 von Johannes Erchinger durchgeführt. Das reguläre 257-gon wurde von Magnus Georg Paucker (1822) and Friedrich Julius Richelot (1832) konstruiert, und das reguläre 65537-gon 1894 von Johann Gustav Hermes durchgeführt, der eine Kurzversion[1] der Konstruktion veröffentlichte. Das Aufschreiben der vollständigen Konstruktion nahm ca. 10 Jahre in Anspruch, und die ca. 200 seitige Abhandlung lagert in der mathematischen Sammlung der Universität Göttingen.

[1] J. Hermes, Über die Teilung des Kreises in 65537 gleiche Teile, Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen, Mathematisch-Physikalische Klasse (in German) (Göttingen) 3: 170186.

1.1 Grundlagen

Um uns mit der Theorie von Körpern befassen zu können, wiederholen wir zunächst einige grundlegende Begriffe aus der Vorlesung Algebra. Für die Beweise der hier wiederholten Aussagen verweise ich auf die Vorlesung Algebra.

Definition 1.1.1: Ein **Körper** ist ein kommutativer Ring $K \neq \{0\}$ mit Eins, in dem jedes von Null verschiedene Element ein multiplikatives Inverses besitzt, d. h. eine Menge K mit zwei Verknüpfungen $+, \cdot : K \times K \to K$ so dass

(K1) $(K, +)$ eine abelsche Gruppe ist,

(K2) $(K^* = K \setminus \{0\}, \cdot)$ eine abelsche Gruppe ist,

(K3) das *Distributivgesetz* gilt: $k \cdot (l + m) = k \cdot l + k \cdot m$ für alle $k, l, m \in K$.

Die **Charakteristik** eines Körpers K ist

$$\operatorname{char}(K) = \begin{cases} 0 & n \cdot 1 \neq 0 \ \forall n \in \mathbb{N} \\ \min\left\{n \in \mathbb{N} : n \cdot 1 = 0\right\} \in \mathbb{N} & \text{sonst.} \end{cases}$$

$$\text{wobei } n \cdot 1 =: \underbrace{1 + \ldots + 1}_{n\times} \neq 0.$$

Aus der Definition eines Körpers ergeben sich direkt einige wichtige Eigenschaften.

Bemerkung 1.1.2:

1. Ein kommutativer Ring $R \neq \{0\}$ mit Eins ist genau dann ein Körper, wenn die Menge $R^\times = \{r \in R^* : \exists s \in R^* \text{ mit } r \cdot s = s \cdot r = 1\}$ der **Einheiten** in R und die Menge $R^* = R \setminus \{0\}$ zusammenfallen. Dies ist genau dann der Fall, wenn $I = \{0\}$ und $I = R$ die einzigen Ideale in R sind.
2. Die Charakteristik jedes nullteilerfreien Rings R und damit auch jedes eines Körpers K ist entweder null oder eine Primzahl.
3. Zu jedem Ring mit Eins und daher auch jedem Körper K existiert genau ein unitärer Ringhomomorphismus $\phi : \mathbb{Z} \to K$, nämlich

$$\phi(m) = \begin{cases} m \cdot 1 & m \in \mathbb{N} \\ 0 & m = 0 \\ -m \cdot 1 & -m \in \mathbb{N}, \end{cases}$$

   und es gilt $\ker(\phi) = \operatorname{char}(K)\mathbb{Z}$. Also ist $\operatorname{char}(K) = 0$ genau dann, wenn $\phi : Z \to K$ injektiv ist und $\operatorname{char}(K) = p \in \mathbb{N}$, p prim, genau dann, wenn $\ker(\phi) = p\mathbb{Z}$. Im zweiten Fall induziert ϕ einen unitären Ringhomomorphismus $\tilde{\phi} : Z/p\mathbb{Z} \to K$, $\overline{k} = [k] \mapsto \phi(k)$.
4. Für jeden Integritätbsbereich K mit $\operatorname{char}(K) = p \in \mathbb{N}$ prim, ist die **Frobeniusabbildung** $F_p : K \to K$, $x \mapsto x^p$ ein injektiver unitärer Ringhomomorphismus, und es gilt $(x + y)^p = x^p + y^p$ für alle $x, y \in K$.

5. Jede endliche Untergruppe der Gruppe der multiplikativen Gruppe $(K^*, \cdot)$ ist zyklisch. Dies folgt direkt aus dem Klassifikationssatz für endliche abelsche Gruppen. Denn jede endliche Untergruppe $G \subset K^*$ ist eine endliche abelsche Gruppe und somit nach dem Klassifikationssatz für abelsche Gruppen isomorph zu einer Gruppe $\mathbb{Z}/p_1^{n_1}\mathbb{Z} \times \ldots \times \mathbb{Z}/p_r^{n_r}\mathbb{Z}$ mit Primpotenzen $p_k^{n_k}$. Die Gruppe G ist zyklisch genau dann, wenn alle Primzahlen $p_1, ..., p_r$ paarweise verschieden sind. Dies ist der Fall genau dann, wenn $m := \min\{k \in \mathbb{N} : a^k = 0 \ \forall k \in G\} = |G| = p_1^{n_1} \cdots p_n^{r_n}$. (Allgemein gilt $m \leq |G|$). Ist $G \subset K^*$ so hat G maximal m Elemente, denn jedes Element von G ist eine Nullstelle des Polynoms $x^m - 1$ in K, das maximal m Nullstellen hat. Also ist G zyklisch.

Wichtige bekannte Beispiele für Körper sind der Körper $\mathbb{C}$ der *komplexen Zahlen*, der Körper $\mathbb{R}$ der *reellen Zahlen* und der Körper $\mathbb{Q}$ der *rationalen Zahlen* sowie die endlichen Körper $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ für Primzahlen $p \in \mathbb{N}$. Die Körper $\mathbb{F}_p$, $\mathbb{C}$ und $\mathbb{Q}$ sind Beispiele zweier allgemeiner Konstruktionen, die es einem erlauben, aus einem kommutativen, nullteilerfreien Ring R mit Eins bzw. einem Integritätsbereich R einen Körper zu konstruieren. Diese aus der Algebra bekannten Konstruktionen bezeichnet man als **Restklassenkörper** und **Quotientenkörper**.

Satz 1.1.3:

1. **Restklassenkörper:** Sei R ein kommutativer Ring mit Eins und $I \subset R$ ein Ideal. Dann ist der Restklassenring oder Faktorring R/I ein Körper genau dann, wenn I ein **maximales Ideal** ist, d. h. $I \subsetneq R$ und für jedes Ideal $J \subsetneq R$ mit $I \subset J$ gilt $I = J$.
2. **Quotientenkörper:** Sei R ein **Integritätsbereich**, d. h. ein kommutativer, nullteilerfreier Ring $R \neq \{0\}$ mit Eins, und $R^* = R \setminus \{0\}$. Dann definiert

$$(r, u) \sim (s, v) \quad \Leftrightarrow \quad r \cdot v = s \cdot u$$

eine Äquivalenzrelation auf $R \times R^*$, deren Äquivalenzklassen man mit mit $\frac{r}{u} = [(r, u)]$ bezeichnet. Die Menge $Q(R) = R \times R^* / \sim$ der Äquivalenzklassen mit den Verknüpfungen

$$\frac{r}{u} + \frac{s}{v} = \frac{rv + us}{uv} \qquad \frac{r}{u} \cdot \frac{s}{v} = \frac{rs}{uv}$$

ist ein Körper und wird als **Quotientenkörper** von R bezeichnet.

Bemerkung 1.1.4:

1. Jeder kommutative Ring $R \neq \{0\}$ mit Eins besitzt ein maximales Ideal, also auch stets Restklassenkörper.
2. Die Äquivalenzrelation in dem Quotientenkörper $Q(R)$ entspricht gerade dem bekannten "Kürzen von Brüchen". Ist $\frac{s}{v} \in Q(R)$ mit $s = rw$, $v = uw$ für ein $r \in R$ und $u, w \in R^*$, so folgt $s \cdot u = ruw = r \cdot v$ und somit $\frac{s}{v} = \frac{rw}{uw} = \frac{r}{u}$.
3. **Universelle Eigenschaft des Quotientenkörpers**: Jeder unitäre injektive Ringhomomorphismus $\phi : R \to K$ in einen Körper K läßt sich eindeutig zu einem injektiven unitären Ringhomomorphismus $\tilde{\phi} : Q(R) \to K$ fortsetzen, nämlich

$$\tilde{\phi}\left(\frac{r}{u}\right) = \phi(r) \cdot \phi(u)^{-1}.$$

Eine naheliegende Frage ist, was passiert, wenn man diese zwei Konstruktionen für Ringe durchführt, die zusätzliche Eigenschaften besitzen, also beispielsweise Hauptidealringe oder bereits Körper sind. Ebenso interessiert man sich dafür, was diese Konstruktionen für bekannte Beispiele von kommutativen Ringen wie den Ring $\mathbb{Z}$ der *ganzen Zahlen* oder den *Polynomring* $R[x]$ über einem kommutativen Ring R mit Eins ergeben.

Beispiel 1.1.5: (Restklassenkörper und Quotientenkörper)

1. Ist R ein Körper, so ist nach Bemerkung 1.1.2 das Ideal $I = \{0\}$ das einzige maximale Ideal in R und der zugehörige Restklassenkörper R/I ist isomorph zu R. Ebenso ist der Quotientenkörper $Q(R)$ isomorph zu R, denn es gilt $(r, u) \sim (ru^{-1}, 1)$ für alle $u \in R^*$, also $\frac{r}{u} = ru^{-1}$. Man erhält also durch Restklassenbildung in einem Körper oder Übergang zu dessen Quotientenkörper keine neuen Körper.
2. Sei R ein **Hauptidealring**, d. h. ein Integritätsbereich, in dem jedes Ideal von der Form $aR = \{a \cdot r : r \in R\}$ für ein $a \in R$ ist. Dann ist ein Ideal $I = aR$ maximal und der Restklassenring R/aR ein Körper genau dann, wenn $a \in R^*$ prim ist.
3. Für den Hauptidealring $R = \mathbb{Z}$ sind die maximalen Ideale gerade die Ideale der Form $I = p\mathbb{Z}$ für Primzahlen $p \in \mathbb{N}$, und der zugehörige Restklassenkörper ist der endliche Körper $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Der Quotientenkörper zu $\mathbb{Z}$ ist per Definition $Q(\mathbb{Z}) = \mathbb{Q}$.

Wir wollen nun weitere interessante Beispiele konstruieren, indem wir Rstklassenkörper und Quotientenkörper des *Polynomrings* $R[x]$ über einem kommutativen, nullteilerfreien Ring R betrachten. Dazu wiederholen wir zunächst die Definition und seine wichtigsten Eigenschaften.

Definition 1.1.6: Sei R ein kommutativer Ring mit Eins. Ein **Polynom** in R ist eine Folge $a_* = (a_0, a_1, \ldots)$ von Elementen $a_n \in R$, so dass fast alle (d. h. alle bis auf endlich viele) Elemente a_n verschwinden. Die Menge $R[x]$ aller Polynome in R bildet mit den Verknüpfungen

$$(a_* + b_*)_n = a_n + b_n \qquad (a_* \cdot b_*)_n = a_0 b_n + a_1 b_{n-1} + \ldots + a_{n-1} b_1 = a_n b_0$$

einen kommutativen Ring mit Eins $1_* = (1, 0, \ldots)$, den **Polynomring** über R. Man schreibt

$$x^n := (\underbrace{0, \ldots, 0}_{n\times}, 1, 0, \ldots) \quad \text{für } n \in \mathbb{N}_0, \qquad x := x^1.$$

Die Elemente der Form $rx^0 = (r, 0, ...)$ mit $r \in R$ bilden einen zu R isomorphen Unterring mit Eins, den wir mit R identifizieren. Wir schreiben also $x^0 = 1_* = 1$, und $a_* = \sum_{n=0}^{\infty} a_n x^n$. Der **Grad** eines Polynoms a_* ist

$$\deg(a_*) = \begin{cases} \max\{n \in \mathbb{N}_0 : a_n \neq 0\} & a_* \neq 0 \\ -\infty & a_* = 0, \end{cases}$$

Für $a_* \neq 0$ heißt der Koeffizient $a_{\deg(a_*)} \in R^*$ **Leitkoeffizient** von a_*. Ein Polynom a_* heißt **normiert**, wenn seit Leitkoeffizient gleich Eins ist.

Bemerkung 1.1.7:

1. Die **Auswertung** in einem Element $r \in R$ definiert einen Ringhomomorphismus
$$\mathrm{ev}_r : R[x] \to R, \quad \sum_{n=0}^{\infty} a_n x^n \mapsto a(r) = \sum_{n=0}^{\infty} a_n r^n.$$
2. Zu jedem Ringhomomorphismus $\varphi : R \to S$ zwischen kommutativen Ringen mit Eins erhält man durch Anwendung von φ auf die Koeffizienten einen Ringhomomorphismus
$$\varphi_* : R[x] \to S[x], \quad \sum_{n=0}^{\infty} a_n x^n \mapsto \sum_{n=0}^{\infty} \varphi(a_n) x^n.$$
3. Daraus ergibt sich, dass zu einem unitären Ringhomomorphismus $\varphi : R \to S$ und festem $s \in S$ genau ein Ringhomomorphismus $\Phi : R[x] \to S$ mit $\Phi(r) = \varphi(r)$ für alle $r \in R$ und $\Phi(x) = s$ existiert, nämlich $\Phi = \mathrm{ev}_s \circ \varphi_*$. Dies bezeichnet man als **universelle Eigenschaft des Polynomrings**.
4. Insbesondere erhält man für jeden kommutativen Ring R aus dem Ringhomomorphismus $\phi : \mathbb{Z} \to R$ (Bemerkung 1.1.2) genau einen Ringhomomorphismus $\Phi : \mathbb{Z}[x] \to R[x]$ mit $\Phi(nx^0) = nx^0$ und $\Phi(x) = x$.

Um aus Polynomringen Quotientenkörper konstruieren, müssen wir uns auf Polynomringe beschränken, die Integritätsbereiche sind. Für die Konstruktion von Restklassenkörpern wäre das im Prinzip nicht notwendig, aber in diesem Fall wünscht man sich, dass die Ideale in dem Polynomring von besonders einfacher Gestalt sind, also beispielsweise Hauptidealringe. Ausserdem sollten sich die Primelemente in diesem Polynomring auf möglichst einfach Weise beschreiben lassen. Um zu sehen, wann dies der Fall ist, erinnern wir an die folgenden zentralen Aussagen über Polynomringe aus der Vorlesung Algebra.

Satz 1.1.8: (Eigenschaften des Polynomrings)

1. Ist R ein Integritätsbereich, so ist auch der Polynomring $R[x]$ ein Integritätsbereich. Der zugehörige Quotientenkörper $Q(R[x])$ ist der Körper der **gebrochen rationalen Funktionen** über R, also Funktionen der Form
$$f(x) = \frac{\sum_{n=0}^{\infty} a_n x^n}{\sum_{m=0}^{\infty} b_m x^m} \qquad \text{mit } a_n, b_m \in R, a_n = 0, b_m = 0 \text{ für fast alle } n, m \in \mathbb{N}_0.$$
2. Ist K ein Körper, so ist der Polynomring $K[x]$ ein **euklidischer Ring** mit Höhenfunktion $h : K[x] \to \mathbb{N}_0$, $h(f) = \deg(f)$, d. h. zu jedem Paar von Polynomen $f, g \in R[x]$ mit $g \neq 0$ existieren Polynome $m, r \in R[x]$ mit $f = mg + r$ und $\deg(r) < \deg(g)$. Die Polynome m, r lassen sich mit dem euklidischen Algorithmus oder Polynomdivision bestimmen.
3. Ist K ein Körper, so ist der Polynomring $K[x]$ ein Hauptidealring, denn nach 2. ist $K[x]$ ein euklidischer Ring, und euklidische Ringe sind Hauptidealringe. Somit ist $K[x]$ insbesondere ein **faktorieller Ring**, d. h. ein Integritätsbereich, in dem sich jedes Element als Produkt von endlich vielen Primelementen schreiben läßt, denn Hauptidealringe, sind faktorielle Ringe. Die Primelemente sind damit genau die irreduziblen Elemente von $K[x]$.

4. Sei K ein Körper, $f \in K[x]^*$ und $(f) \subset K[x]$ das von f erzeugte Ideal in $K[x]$. Dann ist der Restklassenring $K[x]/(f)$ ein $\deg(f)$-dimensionaler Vektorraum über K, und die Restklassen $1, \overline{x}, ..., \overline{x}^{\deg(f)-1}$ der Polynome $1, x, ..., x^{\deg(f)-1}$ bilden eine Basis.
5. Der Restklassenring $K[x]/(f)$ ist genau dann ein Körper, wenn f **irreduzibel** ist, d. h. f ist nicht konstant und es existieren keine nicht-konstanten Polynome $g, h \in K[x]$ mit $f = g \cdot h$.

Mit Hilfe dieses Satzes lassen sich nun Quotientenkörper und Restklassenkörper von Polynomringen $K[x]$ über Körpern K konstruieren. Um die Restklassenkörper $K[x]/(f)$ zu verstehen, muss man sich genauer mit dem zugrundliegenden Körper K und dem Polynom f beschäftigen. Zunächst stellt man fest:

- Polynome vom Grad eins sind immer irreduzibel, was sich direkt aus der Gradformel $\deg(f \cdot g) = \deg(f) + \deg(g)$ für $f, g \in K[x]$ ergibt. Die zugehörigen Restklassenkörper sind isomorph zu K. Denn nach Satz 1.1.8 4. ist für $\deg(f) = 1$ das Polynom x eine Basis des Vektorraums $K[x]/(f)$ und damit der Körper $K[x]/(f)$ ein eindimensionaler Vektorraum über K.
- Um interessante Restklassenkörper zu erhalten, muss man also irreduzible Polynome höheren Grads betrachten, die nur dann existieren können, wenn K nicht algebraisch abgeschlossen ist. In einem algebraisch abgeschlossenen Körper wie beispielsweise $\mathbb{C}$ zerfällt jedes Polynom in Linearfaktoren, und ein Polynom vom Grad > 1 ist nie irreduzibel.
- Für ein Polynom $h \in K[x]$ vom Grad 2 oder 3 folgt aus der Gradformel $\deg(f \cdot g) = \deg(f) + \deg(g)$, dass h genau dann irreduzibel ist, wenn es keinen Linearfaktor besitzt. Also reduziert sich die Untersuchung der Irreduzibilität auf die Untersuchung der **Nullstellen** von h in K, die oft auch als **Wurzeln** von h bezeichnet werden.
- Für Polynome höheren Grades ist dies im allgemeinen komplizierter, da diese auch Produkte von irreduziblen Polynomen von Grad > 1 sein können. Ist $K = \mathbb{R}$, so ist jedes Polynom vom Grad > 2 reduzibel, und ein Polynom vom Grad 2 ist reduzibel genau dann, wenn es eine reelle Nullstelle besitzt. In $\mathbb{Q}[x]$ gibt es irreduzible Polynome beliebigen Grads.

Wir betrachten nun einige wichtige Beispiele für Restklassenkörper von Polynomringen.

Beispiel 1.1.9:

1. Das Polynom $f = 1 + x^2$ ist irreduzibel in $\mathbb{R}[x]$, denn es besitzt keine reelle Nullstelle. Der zugehörige Restklassenkörper $\mathbb{R}[x]/(f)$ ist nach Satz 1.1.8 4. ein zweidimensionaler Vektorraum über $\mathbb{R}$ mit Basis $1 + (f)$, $x + (f)$. Setzt man $1 = (f)$ und $\mathrm{i} = x + (f)$, so lässt sich jedes Element von $\mathbb{R}[x]/(f)$ eindeutig schreiben als Linearkombination $a + \mathrm{i}b$ mit $a, b \in \mathbb{R}$, und es gilt $\mathrm{i}^2 = x^2 + (f) = x^2 + 1 - 1 + (f) = -1 + (f) = -1$. Also erhält man das Multiplikationsgesetz in $\mathbb{C}$ und somit gilt $\mathbb{C} = \mathbb{R}[x]/(x^2 + 1)$.
2. Allgemeiner kann man zeigen, dass für *jedes* irreduzible Polynom $f \in \mathbb{R}[x]$ der Quotientenkörper $\mathbb{R}[x]/(f)$ entweder isomorph zu $\mathbb{R}$ oder isomorph zu $\mathbb{C}$ ist. Man erhält also durch die Betrachtung von Restklassen von Polynomen in $\mathbb{R}[x]$ keine weiteren Körper.
3. Das Polynom $g = x^2 - 2$ ist reduzibel in $\mathbb{R}[x]$, aber irreduzibel in $\mathbb{Q}[x]$, denn ansonsten hätte es eine Nullstelle in $\mathbb{Q}$.Die Nullstellen von g in $\mathbb{R}$ sind aber $x = \pm\sqrt{2} \notin \mathbb{Q}$. Der zugehörige Quotientenkörper $\mathbb{Q}[x]/(g)$ wird mit $\mathbb{Q}(\sqrt{2})$ bezeichnet. Er ist nach

Satz 1.1.8 4. ein zweidimensionaler Vektorraum über $\mathbb{Q}$ mit Basis $1+(f), x+(f)$. Schreibt man $1 = 1+(f)$, $\sqrt{2} = x+(f)$, so läßt sich jedes Element von $\mathbb{Q}[x]/(f)$ eindeutig als Linearkombination $a + b\sqrt{2}$ mit $a, b \in \mathbb{Q}$ darstellen, und man erhält $(\sqrt{2})^2 = (x+(f))^2 = x^2+(f) = x^2 - 2 + 2 + (f) = 2$.

In den endlichen Körpern $\mathbb{F}_p$ lassen sich die irreduziblen Polynome induktiv klassifizieren, da es insgesamt nur endlich viele Polynome eines gegebenen Grades gibt. Man muss also lediglich überprüfen, welche dieser Polynome sich als Produkt von Polynomen niedrigeren Grades schreiben lassen. Dabei kann man sich für $n > 1$ auf Polynome $f = a_0 + a_1 x + \ldots + a_n x^n$ mit $a_0 \neq 0$ beschränken, denn ein Polynom mit $a_0 = 0$ ist nie irreduzibel, da es durch x teilbar ist.

Beispiel 1.1.10: Irreduzible Polynome vom Grad ≤ 4 in $\mathbb{F}_2$

Wie in jedem Körper ist jedes lineare Polynom in $\mathbb{F}_2$ irreduzibel. Also erhält man zwei irreduzible Polynome vom Grad 1, nämlich x, $x+1$.

Ein Polynom vom Grad 2 ist irreduzibel genau, dann, wenn es sich nicht als Produkt zweier Polynome vom Grad 1 schreiben läßt. Dies ist gleichbedeutend dazu, dass es keine Nullstellen in $\mathbb{F}_2$ hat. Also muss für irreduzible Polynome insbesondere $a_0 = 1$ gelten, und es kommen nur die Polynome x^2+1, x^2+x+1 in Frage. Das erste hat eine Nullstelle, nämlich $1 \in \mathbb{F}_2$, das zweite nicht. Also ist x^2+x+1 das einzige irreduzible Polynom vom Grad 2.

Die Polynome vom Grad 3 in $\mathbb{F}_2[x]$ mit $a_0 \neq 0$ sind $x^3{+}1$, $x^3{+}x{+}1$, $x^3{+}x^2{+}1$, $x^3{+}x^2{+}x{+}1$, und ein Polynom vom Grad 3 in $\mathbb{F}_2[x]$ ist irreduzibel genau dann, wenn es sich nicht als Produkt eines Polynoms vom Grad 1 mit einem Polynom vom Grad 2 schreiben läßt. Dies ist gleichbedeutend dazu, dass es keine Nullstellen in $\mathbb{F}_2$ hat. Das erste und vierte haben eine Nullstelle in $\mathbb{F}_2$, das zweite und dritte nicht. Also sind die einzigen irreduziblen Polynome vom Grad 3 die Polynome x^3+x+1 und x^3+x^2+1.

Die Polynome vom Grad 4 mit $a_0 \neq 0$ sind $x^4{+}1$, $x^4{+}x{+}1$, $x^4{+}x^2{+}1$, $x^4{+}x^3{+}1$, $x^4{+}x^2{+}x{+}1$, x^4+x^3+x+1, $x^4+x^3+x^2+1$, $x^4+x^3+x^2+x+1$. Die Produkte der Polynome vom Grad 2 mit $a_0 \neq 0$ sind

$$(x^2+1)^2 = x^4+1, \quad (x^2+x+1)^2 = x^4+x^2+1, \quad (x^2+1)(x^2+x+1) = x^4+x^3+x+1$$

und die Produkte von Polynomen vom Grad 3 mit Polynomen vom Grad 1 mit $a_0 \neq 0$

$$(x+1)(x^3+1) = x^4+x^3+x+1, \quad (x+1)(x^3+x+1) = x^4+x^3+x^2+1$$
$$(x+1)(x^3+x^2+1) = x^4+x^2+x+1, \quad (x+1)(x^3+x^2+x+1) = x^4+1.$$

Also sind die irreduziblen Polynome in $\mathbb{F}_2[x]$ vom Grad 4 gerade die Polynome x^4+x+1, x^4+x^3+1, $x^4+x^3+x^2+x+1$.

	Grad 2	Grad 3	Grad 4
irreduzible Polynome in $\mathbb{F}_2[x]$	x^2+x+1	x^3+x+1	x^4+x+1
		x^3+x^2+1	x^4+x^3+1
			$x^4+x^3+x^2+x+1$

Die bisherigen Ergebnisse zur Konstruktion von Quotientenkörpern und Restklassenkörpern sind in Tabelle 1 zusammengefaßt. Die Fragezeichen in dieser Tabelle bedeuten dabei, dass es schwer ist, allgemeine Aussagen zu treffen bzw. diese Strukturen zu identifizieren.

Tabelle 1: Restklassenkörper und Quotientenkörper

kommutativer Ring mit Eins R	**maximale Ideale** I	**Körper** R/I	**Quotientenkörper**
Integritätsbereich R	maximale Ideale (?)	R/I	Q(R)
Hauptidealring R	aR, $a \in R$ prim	R/aR	Q(R)
ganze Zahlen $\mathbb{Z}$	$p\mathbb{Z}$, p prim	$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$	$\mathbb{Q}$
Körper K	$I = \{0\}$	K	K
Polynomring $K[x]$, K Körper	(f), f irreduzibel (i) $\deg(f) = 1$ (ii) $\deg(f) > 1$ (?)	$K[x]/(f)$ K ?	gebrochen rationale Funktionen in K
Polynomring $\mathbb{C}[x]$	(f), $\deg(f) = 1$	$\mathbb{C}$	gebrochen rationale Funktionen in $\mathbb{C}$
Polynomring $\mathbb{R}[x]$	(f), f irreduzibel $1 \leq \deg(f) \leq 2$ (i) $\deg(f) = 1$ (ii) $\deg(f) = 2$, ohne Nullstelle in $\mathbb{R}$	 $\mathbb{R}$ $\mathbb{C}$	gebrochen rationale Funktionen in $\mathbb{R}$
Polynomring $\mathbb{Q}[x]$	(f), f irreduzibel (i) $\deg(f) = 1$ (ii) $\deg(f) > 1$, f irreduzibel (?)	$\mathbb{Q}[x]/(f)$ $\mathbb{Q}$?	gebrochen rationale Funktionen in $\mathbb{Q}$
Polynomring $\mathbb{F}_p[x]$, $p \in \mathbb{N}$ prim	(f), f irreduzibel (i) $\deg(f) = 1$ (ii) $\deg(f) > 1$, f irreduzibel (?)	$\mathbb{F}_p[x]/(f)$ $\mathbb{F}_p$?	gebrochen rationale Funktionen in $\mathbb{F}_p$

Um die Fälle zu betrachten, die in Tabelle 1 mit Fragezeichen gekennzeichnet sind, benötigt man einfach handhabbare Kriterien, mit dem sich feststellen läßt ob ein Polynom in einem gegebenen Körper K irreduzibel ist. Dies sind die aus der Algebra bekannten Irreduzibilitätskriterien.

Satz 1.1.11: (**Irreduzibilitätskriterien**)

1. **Satz und Lemma von Gauß:** Sei R ein faktorieller Ring mit Quotientenkörper $K = Q(R)$. Dann ist auch der Polynomring $R[x]$ faktoriell und ein Polynom $f \in R[x]^*$ ist genau dann irreduzibel in $K[x]$, wenn es irreduzibel in $R[x]$ ist.

   Dieser Satz besagt, dass die Reduzibilität eines Polynoms in $R[x]$ über R äquivalent ist zu seiner Reduzibilität über K. Zur Untersuchung der Reduzibilität eines Polynoms mit ganzzahligen Koeffizienten über $K = \mathbb{Q}$ reicht es also aus, seine Faktorisierbarkeit in Polynome vom Grad > 1 mit *ganzzahligen Koeffizienten* zu untersuchen und umgekehrt. Hat das zu untersuchende Polynom Koeffizienten in $\mathbb{Q}$, kann man es durch Multiplikation mit einer geeigneten Zahl $n \in \mathbb{N}$ zunächst in ein Polynom mit ganzzahligen Koeffizienten umwandeln.

2. **Rationale Nullstellen:** Sei R ein faktorieller Ring mit Quotientenkörper $K = Q(R)$ und $f = a_0 + a_1x + \ldots + a_nx^n \in R[x]$. Ist $a = \frac{r}{u} \in K$ mit $r \in R$, $u \in R^*$ teilerfremd eine Nullstelle von f, so gilt $u|a_n$ und $r|a_0$.

Die möglichen Nullstellen eines Polynoms $f \in K[x]$ lassen sich also ermitteln, indem man f durch Multiplikation mit einem geeigneten Element $v \in R^*$ in ein Polynom $\tilde{f} = a_0 + a_1 x + \ldots + a_n x^n \in R[x]$ umwandelt und dann für alle Brüche $\pm\frac{r}{u}$ mit $u|a_n$ und $r|a_0$ überprüft, ob diese Nullstellen sind. Dabei wählt man $\tilde{f}$ aus Effizienzgründen **primitiv**, d. h. $\mathrm{ggT}(a_0, ..., a_n) = 1$, da man sonst unnötig viele Brüche überprüfen muss. Für Polynome vom Grad 2 oder 3 beantwortet dies die Frage nach Irreduzibilität in $K[x]$.

3. **Reduktion mod p:** Sei R ein Hauptidealring mit Quotientenkörper $K = Q(R)$ und $f = a_0 + a_1 x + \ldots + a_n x^n \in R[x]$ ein Polynom. Dann ist zu jedem Primelement $p \in R$ der Restklassenring $K_p = R/(p)$ ein Körper und man erhält ein Polynom

$$\pi_p(f) = \overline{a_0} + \overline{a_1} x + \ldots + \overline{a_n} x^n \in K_p[x],$$

wobei $\overline{a_k} = [a_k]$ die Restklasse von a_k in $R/(p)$ bezeichnet. Existiert ein Primelement $p \in R$, so dass der Leitkoeffizient von f nicht durch p teilbar ist und das Polynom $\pi_p(f) \in K_p[x]$ irreduzibel ist, so ist f auch irreduzibel in $K[x]$.

Dieses Kriterium ist nützlich, wenn man die Reduzibilität von Polynomen mit Koeffizienten in $\mathbb{Q} = Q(\mathbb{Z})$ untersuchen will. Denn in $K_p = \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ gibt es nur endlich viele irreduzible Polynome $f \in \mathbb{F}_p[x]$ mit gegebenem Grad $\deg(f) = n$, die sich induktiv leicht klassifizieren lassen. Hat man eine Liste solcher irreduziblen Polynome, so lassen sich daraus Aussagen über die Irreduzibilität eines Polynoms in $\mathbb{Q}[x]$ machen, indem man es zunächst durch Multiplikation mit einer geeigneten ganzen Zahl in ein Polynom in $\mathbb{Z}[x]$ umwandelt. Teilt p dessen Leitkoeffizienten nicht, so betrachtet man die Koeffizienten mod p und vergleicht das resultierende Polynom mit der Liste. Umgekehrt ist für ein über $\mathbb{Q}$ *reduzibles* Polynom $f \in \mathbb{Z}[x]$ immer auch das zugehörige Polynom $\pi_p(f)$ reduzibel, sofern p dessen Leitkoeffizienten nicht teilt.

4. **Eisensteinkriterium:** Sei R ein faktorieller Ring, $K = Q(R)$ sein Quotientenkörper und $f = a_0 + a_1 x + \ldots + a_n x^n \in R[x]$ ein Polynom mit Koeffizienten in R. Existiert ein Primelement $p \in R$ mit $p|a_{n-1}, ..., p|a_0$ und $p \nmid a_n, p^2 \nmid a_0$, so ist f irreduzibel in $K[x]$.

Dieses Kriterium ist besonders hilfreich, wenn man die Reduzibilität von Polynomen in $\mathbb{Q}[x]$ untersuchen möchte. Man wandelt dazu f durch Multiplikation mit einer geeigneten ganzen Zahl $a \in \mathbb{Z}$ in ein Polynom $f \in \mathbb{Z}[x]$ mit ganzzahligen Koeffizienten um. Existiert eine Primzahl, die alle Koeffizienten ausser dem Leitkoeffizienten teilt, und deren Quadrat den Koeffizienten a_0 nicht teilt, so ist f und damit auch das ursprüngliche Polynom irreduzibel. Oft lassen sich Polynome, auf die das Eisensteinkriterium nicht direkt anwendbar ist, durch geeignetes Translatieren $x \mapsto x + a$ mit $a \in R$ zu Polynomen machen, auf die das Eisensteinkriterium anwendbar ist.

Beispiel 1.1.12: (**Irreduzibilitätskriterien**)

1. Nach dem Kriterium der rationalen Nullstellen ist $\frac{1}{2}x^3 - \frac{7}{2}x^2 + 7x - 2$ irreduzibel in $\mathbb{Q}[x]$. Denn das zugehörige primitive Polynom $x^3 - 7x^2 + 14x - 4$ kann nach dem Kriterium der rationalen Nullstellen nur die Nullstellen $\frac{r}{u}$ mit $r|4$ und $u|1$ haben, also $\pm 1, \pm 2, \pm 4$. Man rechnet leicht nach, dass das keine Nullstellen sind.
2. Nach dem Kriterium der Reduktion mod 2 ist jedes Polynom $f = x^4 + nx + m$ mit $n, m \in \mathbb{Z}$ ungerade irreduzibel in $\mathbb{Q}[x]$, denn das zugehörige Polynom

$$\pi_2(f) = x^4 + \overline{n}x + \overline{m} = x^4 + x + 1$$

ist nach Beispiel 1.1.10 irreduzibel in $\mathbb{F}_2[x]$. Ebenso ist das Polynom $g = 7x^3 - 5x - 3$ irreduzibel in $\mathbb{Q}[x]$, denn $\pi_2(g) = x^3 + x + 1$ ist irreduzibel in $\mathbb{F}_2[x]$.

3. Es gibt irreduzible Polynome $f \in \mathbb{Q}[x]$, so dass für alle Primzahlen $p \in \mathbb{N}$ das zugehörige Polynom $\pi_p(f) \in \mathbb{F}_p[x]$ reduzibel ist. Ein Beispiel ist $f = x^4 - 10x^2 + 1$.
4. Das Polynom $f = 5x^7 + 3x^2 - 12x - 6$ ist irreduzibel in $\mathbb{Q}[x]$ nach dem Kriterium von Eisenstein mit $p = 3$.
5. Für $p \in \mathbb{N}$ prim ist das $p$te **Kreisteilungspolynom**

$$\Phi_p = \frac{x^p - 1}{x - 1} = \sum_{n=0}^{p-1} x^n = 1 + x + x^2 + \ldots + x^{p-1} \qquad \text{mit } p \text{ prim}$$

irreduzibel in $\mathbb{Q}[x]$. Hier kann man das Kriterium von Eisenstein nicht direkt anwenden, aber es ist möglich, Φ_p durch einen geeigneten Automorphismus $\psi : \mathbb{Q}[x] \to \mathbb{Q}[x]$ in ein Polynom umzuwandeln, für das das funktioniert. Ein solcher ist durch $\psi(q) = q$ für alle $q \in \mathbb{Q}$ und $\psi(x) = x + 1$ eindeutig bestimmt (siehe Bemerkung 1.1.7) und ändert nichts an der Irreduzibilität. Damit erhält man

$$\psi(\Phi_p) = \frac{(x+1)^p - 1}{x} = \sum_{n=1}^{p} \left(\begin{array}{c} p \\ n \end{array} \right) x^{n-1} = p + \frac{p(p-1)}{2} x + \ldots + p x^{p-2} + x^{p-1}.$$

Wegen

$$p \Big| \left(\begin{array}{c} p \\ n \end{array} \right) \ \forall n \in \{1, ..., p-1\}, \qquad p \nmid \left(\begin{array}{c} p \\ p \end{array} \right) = 1, \qquad p^2 \nmid \left(\begin{array}{c} p \\ 1 \end{array} \right) = p$$

folgt mit dem Kriterium von Eisenstein, dass $\psi(\Phi_p)$ und damit auch Φ_p irreduzibel ist.

Wir können Polynomringe benutzen, um endliche Körper mit einer vorgegebenen Anzahl n von Elementen zu konstruieren, sofern n eine Primpotenz ist. Ist $n = p$ eine Primzahl, so ist $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ ein endlicher Körper mit p Elementen. Ist $q \in \mathbb{F}_p[x]$ ein irreduzibles Polynom vom Grad $m \in \mathbb{N}$, so ist der Restklassenkörper $\mathbb{F}_p[x]/(q)$ ein m-dimensionaler Vektorraum über $\mathbb{F}_p$ und somit ein Körper mit p^m Elementen. Wir werden später zeigen, dass alle endlichen Körper von dieser Form sind.

Beispiel 1.1.13: Wir konstruieren einen Körper mit 4 Elementen. Das Polynom $f = x^2+x+1$ ist nach Beispiel 1.1.10 irreduzibel in $\mathbb{F}_2[x]$ und somit ist nach Satz 1.1.8 der Restklassenring $\mathbb{F}_2[x]/(f)$ ein Körper und ein zweidimensionaler Vektorraum über $\mathbb{F}_2$ mit Basis $\pi(1) = \overline{1}$, $\pi(x) = \overline{x}$. Also enthält der Körper K genau vier Elemente, nämlich $\overline{0}, \overline{1}, \overline{x}, \overline{1+x}$.

1.2 Körpererweiterungen

Nachdem eine mathematische Struktur definiert und Beispiele dieser Struktur betrachtet wurden, ist der nächste Schritt meist die Betrachtung *strukturerhaltender Abbildungen*, d. h. Abbildungen, die mit dieser Struktur kompatibel sind. Im Fall der Vektorräume sind dies lineare Abbildungen, für Gruppen, Ringe und Algebren, respektive, Gruppenhomomorphismen, Ringhomomorphismen und Algebrahomomorphismen und für topologische Räume sind es die stetigen Abbildungen. Im Fall von Körpern erhält man jedoch keinen neuen Begriff, da ein Körper nur ein unitärer Ring mit bestimmten Zusatzeigenschaften ist, aber keine zusätzlichen Strukturen aufweist.

Definition 1.2.1: Ein **Körperhomomorphismus** zwischen zwei Körpern K, L ist ein unitärer Ringhomomorphismus $\phi : K \to L$, d. h. eine Abbildung $\phi : K \to L$ mit

$$\phi(k+j) = \phi(k) + \phi(j)\ \forall k, j \in K \qquad \phi(k \cdot j) = \phi(k) \cdot \phi(j)\ \forall k, j \in K$$
$$\phi(0_K) = 0_L \qquad \phi(1_K) = 1_L.$$

Bemerkung 1.2.2:

1. Körperhomomorphismen sind injektiv und damit **Körpermonomorphismen**.

   Denn ist $\phi : K \to L$ ein Körperhomomorphismus, und $k \in K^*$ so hat k ein multiplikatives Inverses k^{-1}, und es folgt $\phi(k) \cdot \phi(k^{-1}) = \phi(k \cdot k^{-1}) = \phi(1_K) = 1_L$. Also gilt $\phi(k^{-1}) = \phi(k)^{-1}$ und damit insbesondere $\phi(k) \neq 0$ für alle $k \in K^*$.
2. Es folgt, dass jeder Körperhomomorphismus $\phi : K \to L$ ein **Körperisomorphismus** auf sein Bild $\phi(K) \subset L$ ist. Damit ist K isomorph zu einem Teilkörper von L, und die Untersuchung von Körperhomomorphismen in einen gegebenen Körper L reduziert sich auf die Untersuchung seiner Teilkörper.

Definition 1.2.3:

1. Ein **Teilkörper** eines Körpers L ist ein Teilring $K \subset L$, der (mit dieser Ringstruktur) ein Körper ist. Der Körper K heißt **Grundkörper** und der Körper L **Erweiterungskörper**. Das Paar (K, L) wird als **Körpererweiterung** und mit L/K bezeichnet.
2. Der Erweiterungskörper L ist auf kanonische Weise ein Vektorraum über dem Grundkörper K. Seine Dimension heißt **Grad** der Körpererweiterung und wird mit $[L : K] = \dim_K(L)$ bezeichnet.
3. Ist $[L : K]$ endlich, so heißt die Körpererweiterung L/K **endliche Körpererweiterung**, ansonsten **unendliche Körpererweiterung**. Ist $[L : K] = 2$, so spricht man von einer **quadratischen Körpererweiterung** .
4. Der **Primkörper** $P(L)$ eines Körpers L ist der kleinste Teilkörper von L

$$P(L) = \bigcap_{K \subset L \text{ Teilkörper}} K.$$

Bemerkung 1.2.4:

1. Eine Teilmenge $K \subset L$ eines Körpers L ist genau dann ein Teilkörper, wenn gilt:

$$a, b \in K \ \Rightarrow\ a - b \in K, a \cdot b \in K \quad \text{und} \quad c \in K^* \ \Rightarrow\ c^{-1} \in K.$$

2. Es gilt $[L : K] = 1$ genau dann, wenn $L \cong K$.
3. Ist $K \subset L$ eine Körpererweiterung, so haben K und L immer die gleiche Charakteristik, denn aus $a \in K^*$ folgt $a^{-1} \in K^*$ und damit $a \cdot a^{-1} = 1_L \in K^*$. Daraus ergibt sich $1_K = 1_L$ und damit $\text{char}(K) = \text{char}(L)$.
4. Man kann zeigen, dass $P(K) \cong \mathbb{Q}$ falls $\text{char}(K) = 0$ und $P(K) \cong \mathbb{F}_p$ falls $\text{char}(K) = p \in \mathbb{N}$ prim (Aufgabe 15).

Beispiel 1.2.5:

1. Für jeden Körper K und jedes nicht-konstante irreduzible Polynom $f \in K[x]^*$ ist nach Satz 1.1.8, 4. und 5. der Körper $K[x]/(f)$ eine Körpererweiterung von K vom Grad $\deg(f)$, denn die Restklassen der Polynome $1, x, \ldots, x^{\deg(f)-1}$ bilden eine Basis des K-Vektorraums $K[x]/(f)$.
2. Insbesondere ist nach Beispiel 1.1.9 die Körpererweiterung $\mathbb{C}/\mathbb{R}$ eine quadratische Körpererweiterung.
3. $\mathbb{R}/\mathbb{Q}$ ist eine unendliche Körpererweiterung, denn $\mathbb{Q}$ ist ein Teilkörper von $\mathbb{R}$ und $\mathbb{R}$ ist überabzählbar, während $\mathbb{Q}$ abzählbar ist. Wäre $[\mathbb{R} : \mathbb{Q}] = n \in \mathbb{N}$, so wäre R als $\mathbb{Q}$-Vektorraum isomorph zu $\mathbb{Q}^n$ und damit abzählbar.
4. Jeder Körper L ist eine Körpererweiterung über seinem Primkörper $P(L)$.

Im Folgenden werden wir Körper auch häufiger iterativ erweitern, d. h. Körpererweiterungen von Körpererweiterungen betrachten. Ein Beispiel sind die Körper $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$, da sowohl $\mathbb{R}/\mathbb{Q}$ als auch $\mathbb{C}/\mathbb{R}$ Körpererweiterungen sind.

Definition 1.2.6: Ein **Körperverband** oder **Körperturm** ist eine Familie von Körpern $K_0 \subset K_1 \subset \ldots \subset K_n$, so dass K_i/K_{i-1} eine Körpererweiterung ist für alle $i \in \{1, ..., n\}$. Die Körper $K_1, ..., K_{n-1}$ heißen **Zwischenkörper** von K_n/K_0.

Sind alle in einem Körperturm auftretenden Körpererweiterung endlich-dimensional, so lassen sich deren Grade leicht in Verbindung setzen. Dies führt auf den sogenannten Gradsatz, der eine der zentralsten und hilfreichsten Aussagen in der gesamten Körpertheorie ist.

Satz 1.2.7: (**Gradsatz**)
Sei $K \subset E \subset L$ ein Körperturm mit Zwischenkörper E. Dann gilt $[L : K] = [L : E] \cdot [E : K]$.

Beweis:
Sei $[L : E] = n \in \mathbb{N}$ und $[E : K] = m \in \mathbb{N}$. Wir wählen eine eine Basis $\{l_1, ..., l_n\}$ von L als Vektorraum über E und eine Basis $\{e_1, ..., e_m\}$ von E als Vektorraum über K. Dann läßt sich jedes Element $l \in L$ eindeutig als Linarkombination $l = \sum_{i=1}^{n} \lambda_i l_i$ mit $\lambda_i \in E$ schreiben und jedes λ_i eindeutig als Linearkombination $\lambda_i = \sum_{j=1}^{m} \mu_{ij} e_j$ mit $\mu_{ij} \in K$. Man erhält also $l = \sum_{i=1}^{n} \sum_{j=1}^{m} \mu_{ij} e_j l_i$ mit $\mu_{ij} \in K$. Also erzeugt die Menge $\{e_j l_i\}_{1 \leq i \leq n, 1 \leq j \leq m}$ den K-Vektorraum L. Ausserdem ist sie linear unabhängig, denn ist $l = 0$, so folgt $\sum_{j=1}^{m} \mu_{ij} e_j = 0$ für alle $i = 1, ..., n$, da $\{l_1, ..., l_n\}$ eine E-Basis von L ist. Da aber auch $\{e_1, ..., e_m\}$ eine K-Basis von E ist, ergibt sich damit $\mu_{ij} = 0$ für alle $i = 1, ..., n$, $j = 1, ..., m$. □

Insbesondere lassen sich mit dem Gradsatz die möglichen Zwischenkörper E einer endlichen Körpererweiterung L/K stark einschränken, denn es kommen nur bestimme Grade in Frage. Ist $K \subset E \subset L$ ein Körperturm, so müssen nach dem Gradsatz $[L : E]$ und $[E : K]$ Teiler von $[L : K]$ sein, und aus $[L : E] = [L : K]$ folgt $E = K$. Eine endliche Körpererweiterung L/K kann also nur dann **echte Zwischenkörper**, d. h. Zwischenkörper $K \subsetneq E \subsetneq L$ haben, wenn ihr Grad $[L : K] \in \mathbb{N}$ weder Eins noch eine Primzahl ist.

Beispiel 1.2.8:

1. Die Körperwerweiterung $\mathbb{C}/\mathbb{R}$ hat keine keine echten Zwischenkörper, denn $[\mathbb{C} : \mathbb{R}] = 2$.
2. Ist K ein Körper, $f \in K[x]$ irreduzibel mit $\deg(f) \in \mathbb{N}$ prim und $L = K[x]/(f)$, so hat L/K keine echten Zwischenkörper.
3. $\mathbb{R}$ ist ein Zwischenkörper von $\mathbb{C}/\mathbb{Q}$, und es gilt $\infty = [\mathbb{C} : \mathbb{Q}] = [\mathbb{C} : \mathbb{R}] \cdot [\mathbb{R} : \mathbb{Q}] = 2 \cdot \infty$.

Im Folgenden möchten wir Zwischenkörper einer Körpererweiterung L/K konstruieren, indem wir ein oder mehrere Elemente von L zu K hinzufügen. Da das Ergebnis ein Körper sein soll, müssen stets alle Potenzen eines hinzugefügten Elements $\alpha \in L$, deren Inverse, deren Produkte mit Elementen aus K und Linearkombinationen solcher Elemente berücksichtigt werden. Die Liste der neu hinzukommenden Körperelemente ist offensichtlich kompliziert . Aus diesem Grund geht man Problem abstrakt an, und betrachtet stattdessen den kleinsten Teilkörper von L, der K und α enthält.

Definition 1.2.9: Sei L/K eine Körpererweiterung.

1. Für eine Teilmenge $S \subset L$ bezeichnet $K(S)$ den kleinsten Zwischenkörper von L/K, der S enthält, und $K[S]$ den kleinsten Teilring von L, der S enthält:

$$K(S) = \bigcap_{\substack{K \subset E \subset L \\ \text{Zwischenkörper,} \\ S \subset E}} E, \qquad K[S] = \bigcap_{\substack{R \subset L \text{ Teilring} \\ S \cup K \subset R}} R.$$

   Der Körper $K(S)$ heißt der von **von** S **erzeugte Teilkörper** von L und der Ring $K[S]$ der **von** S **erzeugte Teilring** von L. Man sagt $K(S)$ und $K[S]$ entstehen aus K durch **Adjunktion** von S.
2. Gilt $L = K(\alpha)$ für ein $\alpha \in L$, so nennt man die Körpererweiterung L/K eine **einfache Körpererweiterung** oder **primitive Körpererweiterung** und α ein **primitives Element** von L/K.
3. Für $S = \{s_1, ..., s_n\}$ schreibt man $K(s_1, ..., s_n)$ statt $K(\{s_1, ..., s_n\})$ und $K[s_1, ..., s_n]$ statt $K[\{s_1, ..., s_n\}]$.

Offensichtlich gilt $K(S) = K[S] = K$, falls die Teilmenge S in K enthalten ist. Ebenso sieht man direkt aus der Definition, dass für beliebige Teilmengen $S \subset L$ die Inklusion $K[S] \subset K(S)$ gelten muss, denn jeder Zwischenkörper von L/K, der S enthält, ist auch ein Teilring von L, der $K \cup S$ enthält. Im Allgemeinen ist es aber schwierig, aus der angegebenen Menge S abzulesen, wie der von S erzeugte Teilring oder Zwischenkörper aussieht. Insbesondere können verschiedene Mengen S, S' den gleichen Teilring oder Zwischenkörper erzeugen.

Beispiel 1.2.10: Es gilt $\mathbb{C} = \mathbb{R}[\mathrm{i}] = \mathbb{R}(\mathrm{i})$. Also ist $\mathbb{C}$ eine einfache Körpererweiterung und i ein primitives Element.

Dies folgt direkt aus der Tatsache, dass sich jedes Element von $\mathbb{C}$ eindeutig als Linearkombination $a + \mathrm{i}b$ mit $a, b \in \mathbb{R}$ schreiben läßt. Ist $\mathbb{R} \subset E \subset \mathbb{C}$ ein Zwischenkörper, der i enthält, so enthält E bereits alle Linearkombinationen $a + \mathrm{i}b$ mit $a, b \in \mathbb{R}$. Das Gleiche gilt für einen Teilring $R \subset \mathbb{C}$, der $\mathbb{R} \cup \{\mathrm{i}\}$ enthält.

Beispiel 1.2.11: Für beliebige $a, b \in \mathbb{Q}$ gilt $\mathbb{Q}(\sqrt{a}, \sqrt{b}) = \mathbb{Q}(\sqrt{a} + \sqrt{b})$. Also ist die Körpererweiterung $\mathbb{Q}(\sqrt{a}, \sqrt{b})/\mathbb{Q}$ primitiv und $\sqrt{a} + \sqrt{b}$ ein primitives Element.

Für $a = b$ ist dies trivial, denn $\mathbb{Q}(\sqrt{a}) = \mathbb{Q}(2\sqrt{a})$. Sei also $a \neq b$. Dann gilt offensichtlich $\mathbb{Q}(\sqrt{a} + \sqrt{b}) \subset \mathbb{Q}(\sqrt{a}, \sqrt{b})$, denn jeder Körper, der $\sqrt{a}$ und $\sqrt{b}$ enthält, enthält auch $\sqrt{a} + \sqrt{b}$.

Zu zeigen ist also, dass jeder Zwischenkörper $\mathbb{Q} \subset E \subset \mathbb{Q}(\sqrt{a}, \sqrt{b})$, der $\sqrt{a} + \sqrt{b}$ enthält, auch $\sqrt{a}$ und $\sqrt{b}$ enthält. Dazu berechnet man

$$(\sqrt{a} + \sqrt{b})^3 = a\sqrt{a} + 3a\sqrt{b} + 3b\sqrt{a} + b\sqrt{b} = (3b + a)(\sqrt{a} + \sqrt{b}) + 2(a - b)\sqrt{b}.$$

Also gilt

$$\sqrt{b} = \underbrace{\tfrac{1}{2}(a-b)^{-1}}_{\in\mathbb{Q}} \left(\underbrace{(\sqrt{a} + \sqrt{b})^3}_{\in\mathbb{Q}(\sqrt{a}+\sqrt{b})} - \underbrace{(3b + a)(\sqrt{a} + \sqrt{b})}_{\in\mathbb{Q}(\sqrt{a}+\sqrt{b})} \right)$$

$$\sqrt{a} = \underbrace{\sqrt{a} + \sqrt{b}}_{\in\mathbb{Q}(\sqrt{a}+\sqrt{b})} - \underbrace{\tfrac{1}{2}(a-b)^{-1}}_{\in\mathbb{Q}} \left(\underbrace{(\sqrt{a} + \sqrt{b})^3}_{\in\mathbb{Q}(\sqrt{a}+\sqrt{b})} - \underbrace{(3b + a)(\sqrt{a} + \sqrt{b})}_{\in\mathbb{Q}(\sqrt{a}+\sqrt{b})} \right).$$

Ist $\mathbb{Q} \subset E \subset \mathbb{Q}(\sqrt{a}, \sqrt{b})$ ein Zwischenkörper, der $\sqrt{a} + \sqrt{b}$ enthält, so enthält E auch die Terme auf den rechten Seiten dieser zwei Gleichungen und damit auch $\sqrt{a}$ und $\sqrt{b}$. Also ist $\mathbb{Q}(\sqrt{a}, \sqrt{b})/\mathbb{Q}$ einfach und $\sqrt{a} + \sqrt{b}$ primitiv.

Beispiel 1.2.12: Sei K ein Körper, $f \in K[x]$ irreduzibel und $L = K[x]/(f)$. Dann ist die Körpererweiterung L/K primitiv und $\overline{x}$ ist ein primitives Element.

Denn nach Satz 1.1.8, 4. und 5. ist $K[x]/(f)$ ein $\deg(f)$-dimensionaler Vektorraum über K mit Basis $\overline{1}, \overline{x}, \ldots, \overline{x}^{\deg(f)-1}$. Ist $K = K \cdot \overline{1} \subset E \subset K[x]/(f)$ ein Zwischenkörper, der $\overline{x}$ enthält, so enthält E auch die Restklassen $\overline{x}^k$ aller Monome x^k und deren Linearkombinationen über K. Also gilt $E = K[x]/(f) = K(\overline{x})$.

Beispiel 1.2.13: Für jeden Körper K ist der Körper $Q(K[x])$ der gebrochen rationalen Funktionen in K eine primitive Körpererweiterung von K, und das Polynom x ist ein primitives Element: $Q(K[x]) = K(x)$.

Das folgt, weil sich jedes Element von $Q(K[x])$ als Bruch $\frac{p}{q}$ mit $p, q \in K[x]$, $q \neq 0$ schreiben läßt und $K \subset Q(K[x])$ dabei den Brüchen $\frac{p}{q}$ mit konstanten Polynomen p, q entspricht. Ist nämlich $K \subset E \subset Q(K[x])$ ein Zwischenkörper, der das Polynom $x = \frac{x}{1}$ enthält, so enthält E auch alle Polynome $p \in K[x]$ und deren multiplikative Inverse $p^{-1} = \frac{1}{p}$. Also ist bereits ganz $Q(K[x])$ in E enthalten, und damit $E = Q(K[x]) = K(x)$.

Beispiel 1.2.14: Jede endliche Erweiterung L/K eines endlichen Körpers K ist primitiv.

Aus $[L : K] = n$ folgt $L \cong K^n$ als Vektorraum über K und damit $|L| = |K|^n$. Da nach Bemerkung 1.1.2, 5. jede endliche Untergruppe der Gruppe $(L^*, \cdot)$ zyklisch ist, ist $(L^*, \cdot)$ eine zyklische Gruppe der Ordnung $|K|^n - 1$. Somit existiert ein $l \in L$ mit $L^* = \{1, l, l^2, \ldots, l^{|K|^n-2}\}$. Jeder Zwischenkörper $K \subset E \subset L$, der l enthält, enthält auch alle Potenzen l^k und damit ganz K. Daraus folgt $E = L = K(l)$.

Die Beispiele zeigen, dass es hilfreich ist, die Eigenschaften der Adjunktion systematisch zu untersuchen. Insbesondere stellt sich dabei die Frage nach der Beziehung zwischen dem von $S \subset L$ erzeugten Teilkörper $K(S)$ und dem von S erzeugten Teilring $K[S]$. Ebenso erscheint es naheliegend, dass sich der von einer endlichen Menge $S = \{s_1, ..., s_n\}$ erzeugte Zwischenkörper $K(S)$ auch durch sukzessive Adjunktion der einzelnen Elemente s_i konstruieren lassen sollte, und für unendliche Mengen S erwartet man ein analoges Resultat.

Lemma 1.2.15: (**Eigenschaften der Adjunktion**)
Sei L/K eine Körpererweiterung. Dann gilt:

1. Für jede Teilmenge $S \subset L$ ist $K(S) \cong Q(K[S]) = \{ru^{-1} : r, u \in K[S], u \neq 0\}$.
2. Für beliebige Teilmengen $S, T \subset L$ ist $K(S \cup T) = (K(S))(T)$.
3. Für beliebige $s_1, ..., s_n \in L$ gilt $K[s_1, ..., s_n] = \{f(s_1, ..., s_n) : \ f \in K[x_1, ..., x_n]\}$.
4. Für jede Teilmenge $S \subset L$ ist

$$K[S] = \bigcup_{\substack{V \subset S \\ V \text{ endlich}}} K[V], \qquad K(S) = \bigcup_{\substack{V \subset S \\ V \text{ endlich}}} K(V).$$

Beweis:
1. Da jeder Zwischenkörper $K \subset E \subset L$ mit $S \subset E$ auch ein Teilring mit $K \cup S \subset E$ ist, gilt $K[S] \subset K(S)$. Wir können also den unitären injektiven Ringhomomorphismus $\iota : K[S] \to L$, $r \mapsto r$ betrachten, und aus der universellen Eigenschaft des Quotientenkörpers (Bemerkung 1.1.4) erhalten wir einen injektiven unitären Ringhomomorphismus $\tilde{\iota} : Q(K[S]) \to L$, $\frac{r}{u} \mapsto \iota(r)\iota(u)^{-1} = ru^{-1}$. Also ist $Q(K[S]) \cong \{ru^{-1} : r, u \in K[S], u \neq 0\}$ ein Teilkörper von L, der K und S enthält, und somit $K(S) \subset Q(K[S])$. Andererseits folgt aus $a, b \in K[S] \subset K(S)$ und $b \neq 0$ auch $ab^{-1} \in K(S)$, denn $K(S)$ ist ein Körper. Daraus ergibt sich $Q(K[S]) \subset K(S)$.

2. Folgt direkt aus der Definition.

3. Die Menge $M := \{f(s_1, ..., s_n) : f \in K[x_1, ..., x_n]\}$ ist ein Teilring von L, der $\{s_1, ..., s_n\}$ enthält. Also folgt $K[S] \subset M$. Andererseits folgt aus $s_1, ...s_n \in K[S]$ und der Tatsache, dass $K[S]$ ein Ring ist, dass für jedes Polynom $f \in K[x_1, ..., x_n]$ auch $f(s_1, ..., s_n) \in K[S]$ gilt, also $M \subset K[S]$.

4. Offensichtlich gilt

$$U := \bigcup_{\substack{V \subset S \\ V \text{ endlich}}} K[V] \subset K[S] \qquad W := \bigcup_{\substack{V \subset S \\ V \text{ endlich}}} K(V) \subset K(S),$$

denn für alle $V \subset S$ ist $K[V]$ ein Teilring von $K[S]$ und $K(V)$ ein Teilkörper von $K(S)$. Andererseits folgt aus $r, r' \in U$, dass endliche Mengen $V, V' \subset S$ existieren mit $r \in K[V]$, $r' \in K[V']$. Daraus ergibt sich $r, r' \in K[V \cup V']$ und, da $K[V \cup V']$ ein Ring ist, auch $r \pm r', r \cdot r' \in K[V \cup V'] \subset U$. Also ist U ein Ring, der K und S enthält und damit $K[S] \subset U$. Der Beweis für W ist analog. □

1.3 Einfache und algebraische Körpererweiterungen

Wie sich bereits an den Beispielen gezeigt hat, ist es sehr hilfreich eine Basis des Erweiterungskörpers als Vektorraum über dem Grundkörper zu kennen, um Aussagen über die durch

Adjunktion von Elementen erhaltenen Körpererweiterungen zu gewinnen. Dabei ist es essentiell, zwei Fälle zu unterscheiden, nämlich Elemente des Erweiterungskörpers, die Nullstellen von Polynomen mit Koeffizienten in K sind, und Elemente des Erweiterungskörpers, für die das nicht der Fall ist.

Definition 1.3.1: Sei L/K eine Körpererweiterung. Ein Element $\alpha \in L$ heißt **algebraisch** über K, wenn ein Polynom $p \in K[x]$ existiert mit $p(\alpha) = 0$. Ansonsten bezeichnet man a als **transzendent**. Die Körpererweiterung L/K heißt **algebraisch**, wenn alle Elemente von L algebraisch über K sind, und ansonsten **transzendent**.

Beispiel 1.3.2:

1. Ist $\alpha \in K$, so ist α algebraisch über K, denn $p(\alpha) = 0$ für $p = x - \alpha \in K[x]$.
2. $\mathrm{i} \in \mathbb{C}$ ist algebraisch über $\mathbb{R}$, denn $p(\mathrm{i}) = 0$ für $p = x^2 + 1 \in \mathbb{R}[x]$.
3. $\sqrt{2}$ ist algebraisch über $\mathbb{Q}$, denn $p(\sqrt{2}) = 0$ für $p = x^2 - 2 \in \mathbb{R}[x]$.
4. π und e sind transzendent über $\mathbb{Q}$. Ein Beweis findet sich z. B. im *Buch der Beweise* von Martin Aigner, Günter M. Ziegler.

Im Allgemeinen ist es schwierig, zu beweisen, dass ein gegebenes Element $\alpha \in L$ einer Körpererweiterung transzendent ist, während man zum Beweis, dass es algebraisch ist, nur ein Polynom $p \in K[x]$ mit $p(\alpha) = 0$ angeben muss. Dieses Polynom ist aber nicht eindeutig, denn ist p ein solches Polynom und $q \in K[x]$ beliebig, so ist auch $(pq)(\alpha) = p(\alpha)q(\alpha) = 0$. Die Polynome $p \in K[x]$ mit $p(\alpha) = 0$ bilden ein Ideal in $K[x]$, nämlich den Kern des unitären Ringhomomorphismus $\mathrm{ev}_\alpha : K[x] \to L$, $p \mapsto p(\alpha)$. Sucht man nun aber ein Polynom $p \in K[x]$ minimalen Grades mit $p(\alpha) = 0$ und fordert zusätzlich, dass dieses normiert ist, so ist dieses Polynom p eindeutig bestimmt, und man erhält das sogenannte **Minimalpolynom** von α.

Satz 1.3.3: Sei L/K eine Körpererweiterung und $\alpha \in L$ algebraisch. Dann gilt:

1. Es existiert genau ein normiertes Polynom $m_{\alpha,K} \in K[x]$ mit $m_{\alpha,K}(\alpha) = 0$ und $\deg(f) \geq \deg(m_{\alpha,K})$ für alle $f \in K[x]$ mit $f(\alpha) = 0$.
2. Das Polynom $m_{\alpha,K}$ ist irreduzibel in $K[x]$, und für $f \in K[x]$ gilt $f(\alpha) = 0 \Leftrightarrow m_{\alpha,K} | f$.
3. Der Auswertungshomomorphismus $\mathrm{ev}_\alpha : K[x] \to L$, $f \mapsto f(\alpha)$ induziert einen Körperisomorphismus $K[x]/(m_{\alpha,K}) \xrightarrow{\sim} K(\alpha)$.
4. Es gilt $[K(\alpha) : K] = \deg(m_{\alpha,K})$, und $\{1, \alpha, \ldots, \alpha^{\deg(m_{\alpha,K}-1)}\}$ ist eine Basis von $K(\alpha)$ als Vektorraum über K.

Das Polynom $m_{\alpha,K}$ heißt **Minimalpolynom** von α über K. Der Grad des Minimalpolynoms heißt der **Grad** von α über K, und man schreibt $\deg_K(\alpha) := \deg(m_{\alpha,K})$.

Beweis:
1. Da die Auswertungsabbildung $\mathrm{ev}_\alpha : K[x] \to L$ ein Ringhomomorphismus ist, ist ihr Kern $\ker(\mathrm{ev}_\alpha) = \{f \in K[x] : f(\alpha) = 0\}$ ein Ideal in $K[x]$. Da α algebraisch ist, gilt $\ker(\mathrm{ev}_\alpha) \neq \{0\}$. Da $K[x]$ ein Hauptidealring ist, existiert ein Polynom $g \in K[x]^*$, mit $\ker(\mathrm{ev}_\alpha) = (g)$, und man kann o.B.d.A. annehmen, dass dieses Polynom normiert ist. Dann gilt offensichtlich $f \in \ker(\mathrm{ev}_\alpha) \Leftrightarrow$

$g|f$ und somit folgt $\deg(f) \geq \deg(g)$ für alle $f \in K[x]$ mit $f(\alpha) = 0$. Wir können also $m_{\alpha,K} = g$ setzen, und die erste Aussage ist bewiesen.

2. Der unitäre Ringhomomorphismus $\mathrm{ev}_\alpha : K[x] \to L$ induziert einen injektiven unitären Ringhomomorphismus $K[x]/\ker(\mathrm{ev}_\alpha) \to L$. Da L nullteilerfrei ist, ist $K[x]/\ker(\mathrm{ev}_\alpha)$ ein Integritätsbereich. Damit ist $\ker(\mathrm{ev}_\alpha) = (m_{\alpha,K})$ ein Primideal und $m_{\alpha,K}$ ein Primelement, also irreduzibel. Dies beweist die zweite Aussage.

3. Mit Satz 1.1.8, 5. folgt , dass $K[x]/(m_{\alpha,K})$ ein Körper ist. Also ist der unitäre Ringhomomorphismus $K[x]/\ker(\mathrm{ev}_\alpha) \to L$ ein Körpermonomorphismus und somit ein Körperisomorphismus auf sein Bild $K(\alpha)$. Nach Satz 1.1.8 4. ist $\{1, \alpha, \ldots, \alpha^{\deg(m_{\alpha,K})-1}\}$ eine Basis von $K(\alpha)$ über K, also insbesondere $[K(\alpha) : K] = \deg(m_{\alpha,K})$. □

Beispiel 1.3.4:

1. Das Minimalpolynom von $a = \frac{1}{\sqrt{2}}(1 + \mathrm{i})$ über $\mathbb{Q}$ ist $p = x^4 + 1$. Denn wegen $(1 + \mathrm{i})^2 = 1 - 1 + 2\mathrm{i} = 2\mathrm{i}$, ist a ist eine Nullstelle von p und p ist normiert. Die Irreduzibilität von p über $\mathbb{Q}$ folgt mit dem Reduktionssatz (mod 3), denn p hat keine Nullstelle in $\mathbb{F}_3$, ist also irreduzibel über $\mathbb{F}_3$ und damit auch irreduzibel über $\mathbb{Q}$.

2. Ist K ein Körper und $f \in K[x]$ irreduzibel, so ist $K[x]/(f)$ eine algebraische Körpererweiterung über K und das Element $\overline{x}$ hat das Minimalpolynom f. Denn f ist normiert und $f(\overline{x}) = \overline{f(x)} = 0$. Da nach Satz 1.1.8 die Menge $\{1, \overline{x}, \ldots, \overline{x}^{\deg(f)-1}\}$ linear unabhängig über K ist, kann es kein Polynom $q \in K[x]$ mit $\deg(q) < \deg(f)$ und $q(\overline{x}) = 0$ geben.

3. Wir betrachten $L = \mathbb{Q}[x]/(f)$ mit $f = x^4 + 2x^2 + 2$.

   Nach dem Eisenstein-Kriterium ist f irreduzibel über $\mathbb{Q}$ und somit ist $L/\mathbb{Q}$ eine Körpererweiterung vom Grad 4. Nach 2. ist das Element $\overline{x}$ algebraisch über $\mathbb{Q}$ mit Minimalpolynom f. Das Element $\overline{x}^2$ ist algebraisch über $\mathbb{Q}$ mit Minimalpolynom $q = x^2 + 2x + 2$. Denn q ist normiert, $q(\overline{x}^2) = (\overline{x}^2)^2 + 2\overline{x}^2 + 2 = \overline{x^4 + 2x^2 + 2} = 0$, und da $\overline{x}^2 \notin \mathbb{Q}$, kann kann $\overline{x}^2$ nicht Nullstelle eines Polynoms vom Grad < 2 in $\mathbb{Q}[x]$ sein. Damit folgt insbesondere, dass f *reduzibel* über $\mathbb{Q}[x]/(f)$ ist, denn $f(\overline{x}^2) = 0 \Rightarrow q|f$.

Vergleicht man Beispiel 1.3.4, 2. mit mit Satz 1.3.3, 3. so sieht man, dass diese zwei Aussagen zusammen die Frage beantworten, welche Körpererweiterungen L/K sich als Restklassenkörper $K[x]/(f)$ realisieren lassen. Dies sind genau die primitiven algebraischen Körpererweiterungen L/K. Denn ist L primitiv und algebraisch, so existiert ein algebraisches Element $\alpha \in L$ mit $L = K(\alpha)$ und nach Satz 1.3.3, 3. ist $K(\alpha) \cong K[x]/(m_{\alpha,K})$. Umgekehrt ist jede Körpererweiterung $L = K[x]/(f)$ nach Beispiel 1.3.4, 2. algebraisch und primitiv.

Satz 1.3.3 erlaubt es einem, algebraische Elemente in Körpererweiterungen L/K mit Zwischenkörpern von L/K in Verbindung zu bringen und Aussagen über den Grad algebraischer Elemente in Körpererweiterungen L/K zu machen. Denn für jedes algebraische Element $\alpha \in L$ erhält man einen Zwischenkörper $K \subset K(\alpha) \subset L$, und es gilt $\deg_K(\alpha) = \deg(m_{\alpha,K}) = [K(\alpha) : K]$. Umgekehrt enthält jeder endliche Zwischenkörper $K \subset E \subset L$ ein über K algebraisches Element. So ergeben sich die folgenden zwei Korollare.

Korollar 1.3.5: Sei L/K eine Körpererweiterung und $\alpha \in L$. Dann sind äquivalent:

(i) α ist algebraisch über K.
(ii) $[K(\alpha) : K] < \infty$
(iii) Es existiert ein Zwischenkörper $K \subset E \subset L$ mit $[E : K] < \infty$ und $\alpha \in E$.

Beweis:
Offensichtlich gilt nach Satz 1.3.3 (i)⇒(ii) und (ii)⇒(iii), denn man kann $E = K(\alpha)$ wählen. (iii)⇒(i): Ist $K \subset E \subset L$ ein Zwischenkörper mit $\alpha \in E$ und $[E : K] < \infty$, so können die Potenzen $\alpha^m \in E$ mit $m \in \mathbb{N}_0$ nicht alle linear unabhängig sein. Somit existieren $\lambda_0, ..., \lambda_n \in K$ mit $\sum_{m=0}^{n} \lambda_m \alpha^m = 0$ und für $f = \sum_{m=0}^{n} \lambda_m x^m \in K[x]$ folgt $f(\alpha) = 0$, also α algebraisch. □

Korollar 1.3.6: Für eine endliche Körpererweiterung L/K ist jedes Element $\alpha \in L$ algebraisch über K und sein Grad teilt $[L : K]$.

Beweis:
Jedes Element $\alpha \in L$ ist algebraisch nach Korollar 1.3.5, denn man kann $E = L$ als Zwischenkörper wählen. Aus dem Gradsatz folgt dann die Behauptung. □

Satz 1.3.3 und Korollare 1.3.5 und 1.3.6 suggerieren, dass die Menge der algebraischen Elemente in einer gegebenen Körpererweiterung L/K einen Zwischenkörper der Körpererweiterung L/K bilden sollte. Um dies zu beweisen, zeigt man zunächst, dass jeder Zwischenkörper von L/K der durch die Adjunktion von endlich oder unendlich vielen über K algebraischen Elementen entsteht nur algebraische Elemente enthalten kann. Adjungiert man dann alle über K algebraischen Elemente, so erhält man den gesuchten Zwischenkörper, der auch als der *algebraische Abschluss* von K in L bezeichnet wird.

Lemma 1.3.7: Sei L/K eine Körpererweiterung. Dann gilt:

1. Ist $L = K(S)$ und jedes Element aus S algebraisch, so ist L/K algebraisch.
2. Der **algebraische Abschluss** $A(L/K) = \{\alpha \in L : \alpha \text{ algebraisch über } K\}$ **von** K **in** L ist ein Teilkörper von L.

Beweis:
1. Ist $V = \{s_1, ..., s_n\} \subset S$ endlich, so ist $K(V)/K$ endlich, denn $K(V) = K(s_1)(s_2)\cdots(s_n)$, und mit dem Gradsatz und Korollar 1.3.5 folgt

$$[K(V) : K] = [K(V) : K(s_2, ..., s_n)] \cdot [K(s_2, ..., s_n) : K(s_3, ..., s_n)] \cdots [K(s_n) : K] \in \mathbb{N}.$$

Also ist $K(V)$ nach Korollar 1.3.6 algebraisch über K und nach Lemma 1.2.15 auch $K(S)$.

2. Nach 1. ist $K(A(L/K)) \supset A(L/K)$ algebraisch über K. Also folgt $K(A(L/K)) \subset A(L/K)$ und damit $A(L/K) = K(A(L/K))$. Also ist $A(L/K)$ ein Teilkörper von L. □

Offensichtlich ist die erste Aussage nützlich, um zu untersuchen, ob eine durch Adjunktion gegebene Körpererweiterung algebraisch ist. Denn sie besagt, dass es ausreicht, dies für die Elemente der Menge S zu überprüfen. Die zweite Aussage besagt, dass die algebraischen Elemente einer gegebenen Körpererweiterung einen Zwischenkörper erzeugen. Interessiert man sich lediglich für die Nullstellen von Polynomen $p \in K[x]$ in L, so reicht es, statt L den Zwischenkörper $A(L/K)$ zu betrachten.

1.4 Algebraischer Abschluss und Zerfällungskörper

Im letzten Abschnitt wurde gezeigt, wie sich algebraische Elemente einer Körpererweiterung L/K durch Polynome $p \in K[x]$ charakterisieren lassen. Umgekehrt kann man natürlich auch von dem Polynomring $K[x]$ ausgehen und versuchen, gezielt Körpererweiterungen L/K zu konstruieren, in denen bestimmte Polynome in $K[x]$ Nullstellen besitzen. Ein Beispiel ist der Erweiterungskörper $\mathbb{C} = \mathbb{R}(\mathrm{i}) = \mathbb{R}[x]/(x^2+1)$, der historisch vor allem durch den Wunsch motiviert war, eine Nullstelle für das Polynom x^2+1 zu konstruieren. Nimmt man diesen Standpunkt ein, so ergeben sich direkt die folgenden Fragen:

- Existiert zu einem gegebenen Körper K und einem (nicht-konstanten) Polynom $p \in K[x]$ eine Körpererweiterung L/K, so dass das Polynom p eine Nullstelle in L besitzt bzw. über L in Linearfaktoren zerfällt?
- Wenn ja, gibt es eine kleinstmögliche Körpererweiterung L/K mit diesen Eigenschaften? In welchem Sinn ist diese eindeutig?
- Existiert zu einem gegebenen Körper K eine Körpererweiterung L/K, so dass in L *alle* Polynome $p \in K[x]$ eine Nullstelle besitzen bzw. in Linearfaktoren zerfallen?
- Wenn ja, ist diese eindeutig und in welchem Sinn?

Offensichtlich ist die erste Frage in dieser Liste am einfachsten zu beantworten. Um zu einem gegebenen nicht-konstanten Polynom $p \in K[x]$ einen Erweiterungskörper L von K zu konstruieren, in dem dieses Polynom eine Nullstelle besitzt, gehen wir von dem Beispiel $\mathbb{C} = \mathbb{R}(\mathrm{i}) = \mathbb{R}[x]/(x^2+1)$ und Beispiel 1.3.4 aus und konstruieren den Körper L durch Restklassenbildung im Polynomring $K[x]$.

Satz 1.4.1: (**Satz von Kronecker**)

Sei K ein Körper und $p \in K[x]$ ein nicht-konstantes Polynom. Dann existiert eine Körpererweiterung L/K mit $[L:K] \leq \deg(p)$, so dass p in L eine Nullstelle hat.

Beweis:
Ist $p \in K[x]$ irreduzibel, so können wir $L = K[x]/(p)$ wählen. Denn $L = K[x]/(p)$ ist ein Erweiterungskörper von K mit $[L:K] = \deg(p)$, und p ist nach Beispiel 1.3.4 2. das Minimalpolynom von $\overline{x} \in L$, also $p(\overline{x}) = 0$. Ist p reduzibel, so lässt sich p als endliches Produkt $p = f_1 \cdots f_n$ irreduzibler Polynome $f_1, ..., f_n \in K[x]$ schreiben, und man kann $L = K[x]/(f_i)$ für ein $i \in \{1, ..., n\}$ wählen. □

Statt eines einzelnen Polynoms kann man auch die Menge aller Polynome in $K[x]$ betrachten und versuchen, einen Erweiterungskörper L von K zu konstruieren, in dem jedes nicht-konstante Polynom in $K[x]$ eine Nullstelle hat. Dieses Problem ist offensichtlich gelöst, wenn man einen Erweiterungskörper L von K finden kann, in dem sogar jedes nicht-konstante Polynom in $L[x]$ eine Nullstelle hat. Solche Körper l bezeichnet man als algebraisch abgeschlossen. Ist ein algebraisch abgeschlossener Körper L zusätzlich ein algebraischer Erweiterungskörper eines Körpers K, so bezeichnet man ihn als algebraischen Abschluss von K.

Definition 1.4.2: Ein Körper L heißt **algebraisch abgeschlossen**, wenn jedes nicht-konstante Polynom $p \in L[x]$ eine Nullstelle in L hat. Ein algebraisch abgeschlossener Erweiterungskörper L eines Körpers K heißt **algebraischer Abschluss** von K, wenn L/K eine algebraische Körpererweiterung ist.

Bemerkung 1.4.3:

1. Ein Körper K ist algebraisch abgeschlossen genau dann, wenn jedes nicht-konstante Polynom $p \in K[x]$ in Linearfaktoren zerfällt oder, dazu äquivalent, jedes irreduzible Polynom $p \in K[x]$ linear ist (Aufgabe 18).
2. Man kann auch zeigen, dass ein Körper K genau dann algebraisch abgeschlossen ist, wenn er keinen echten algebraischen Erweiterungskörper L besitzt, oder, dazu äquivalent, keinen echten Erweiterungskörper L mit $[L : K] \in \mathbb{N}$. (Aufgabe 18).
3. Ist L/K algebraisch, so folgt mit Aufgabe 17, dass jeder algebraische Abschluss von L auch ein algebraischer Abschluss von K ist.
4. Der algebraische Abschluss $A(L/K) = \{\alpha \in L : \alpha \text{ algebraisch über } K\}$ eines Körpers K *in einem Erweiterungskörper* L aus Lemma 1.3.7 ist im allgemeinen *kein* algebraischer Abschluss von K. So hat z. B. das Polynom $x^2 + 1$ im algebraischen Abschluss $A(\mathbb{R}/\mathbb{Q})$ von $\mathbb{Q}$ in $\mathbb{R}$ keine Nullstelle.
5. Ist L ein algebraisch abgeschlossener Erweiterungskörper von K, so ist $A(L/K)$ ein algebraischer Abschluss von K. Denn jedes nicht-konstante Polynom $p \in A(L/K)[x] \subset L[x]$ hat dann eine Nullstelle $\alpha \in L$. Da diese algebraisch über $A(L/K)$ ist und $A(L/K)$ algebraisch über K, ist α nach 4. auch algebraisch über K und damit in $A(L/K)$ enthalten.

Beispiel 1.4.4:

1. Der Körper $\mathbb{C}$ ist algebraisch abgeschlossen, denn nach dem Fundamentalsatz der Algebra hat jedes nicht-konstante Polynom $p \in \mathbb{C}[x]$ eine Nullstelle in $\mathbb{C}$. Der Körper $\mathbb{C}$ ist ein algebraischer Abschluss von $\mathbb{R}$, denn wegen $\mathbb{C} = \mathbb{R}[x]/(x^2 + 1)$ ist $\mathbb{C}/\mathbb{R}$ algebraisch.
2. $\mathbb{C}$ ist kein algebraischer Abschluss von $\mathbb{Q}$, denn $\mathbb{C}/\mathbb{Q}$ ist keine algebraische Körpererweiterung. Schon der Zwischenkörper $\mathbb{R} \subset \mathbb{C}$ enthält die über $\mathbb{Q}$ transzendenten Elemente e, π.

Offensichtlich ergibt sich aus der Definition des algebraischen Abschlusses und den betrachteten Beispielen die Frage nach der Existenz eines algebraischen Abschlusses für einen gegebenen Körper. Dies ist die Aussage des Satzes von Steinitz, der allerdings eine reine Existenzaussage und keine explizite Beschreibung des algebraischen Abschlusses liefert.

Satz 1.4.5: (Satz von Steinitz) Jeder Körper K besitzt einen algebraischen Abschluss.

Beweis:
Die Beweisidee ist es, die Menge aller algebraischen Erweiterungskörper von K zu betrachten, und mit Hilfe des Zornschen Lemmas zu zeigen, dass diese ein maximales Element besitzt. Dann zeigt man, dass dieses maximale Element ein algebraischer Erweiterungskörper von K und ausserdem algebraisch abgeschlossen ist.

1. Wir zeigen: es existiert ein maximaler über K algebraischer Erweiterungskörper M von K.

Zunächst existiert eine überabzählbare Menge S mit $K \in S$ und $|K| < |S|$ [2]. Ist K unendlich, so kann man wegen $|K| < |\mathcal{P}(K)|$ nämlich die Potenzmenge $S = \mathcal{P}(K)$ wählen, ist K endlich,

[2]Die Schreibweise $|A| < |B|$, $|A| \leq |B|$ etc für Mengen A, B bezieht sich auf die Kardinalitäten. $|A| \leq |B|$ heisst, dass eine injektive Abbildung $f : A \to B$ existiert, $|A| < |B|$, dass eine injektive, aber keine surjektive Abbildung $f : A \to B$ existiert. Insbesondere ist die Abzählbarkeit einer Menge A äquivalent zu $|A| = |\mathbb{N}|$ und die Überabzählbarkeit zu $|\mathbb{N}| < |A|$

so kann man z. B. $S = K \cup \mathbb{R}$ wählen. Sei

$$\mathfrak{M} = \{L \in S : \, L \text{ Erweiterungskörper von } K,\, L/K \text{ algebraisch}\}.$$

Wegen $K \in \mathfrak{M}$ ist $\mathfrak{M} \neq \emptyset$, und $L \leq L' \;\Leftrightarrow\; L \subset L'$ Teilkörper definiert eine Ordnungsrelation auf $\mathfrak{M}$ (d. h. $\leq$ ist transitiv, reflexiv und antisymmetrisch).

Wir zeigen: Jede total geordnete Kette in M hat eine obere Schranke in $\mathfrak{M}$. Sei dazu $\mathfrak{k} \neq \emptyset$ eine total geordnete Kette in $(\mathfrak{M}, \leq)$ und $T := \bigcup_{L \in \mathfrak{k}} L$. Dann existiert zu $\alpha, \beta \in T$ ein algebraischer Erweiterungskörper $L \in \mathfrak{k}$ von K mit $\alpha, \beta \in L$. Durch $\alpha + \beta := \alpha +_L \beta$, $\alpha \cdot \beta := \alpha \cdot_L \beta$ erhält man zwei Verknüpfungen auf T, die unabhängig von der Wahl von L sind. Denn für jedes $L' \in \mathfrak{k}$ mit $\alpha, \beta \in L'$ gilt $L \leq L'$ oder $L' \leq L$ und somit stimmen die Addition und Multiplikation auf $L \cap L'$ überein. Durch direktes Nachrechnen der Axiome ergibt sich, dass T mit diesen Verknüpfungen ein Körper ist. Ausserdem ist $T \subset S$ per Definition ein Erweiterungskörper von L für jedes $L \in \mathfrak{k}$. Da alle $L \in \mathfrak{k}$ algebraisch sind, ist auch T/K algebraisch (Aufgabe 17) und damit $T \in \mathfrak{M}$. Also ist $T \in \mathfrak{M}$ eine obere Schranke von $\mathfrak{k}$, und mit dem Zornschen Lemma folgt, dass $(\mathfrak{M}, \leq)$ ein maximales Element M besitzt.

2. Wir zeigen: M ist algebraisch abgeschlossen.

Angenommen nicht. Dann existiert nach Bemerkung 1.4.3 ein algebraischer Erweiterungskörper $M \subsetneq M'$. Wir zeigen, dass dieser isomorph zu einem Element von S ist. Da nach Voraussetzung S überabzählbar und $|K| < |S|$ ist, muss für die Kardinalitäten gelten

$$|M' \setminus M| \leq |M'| < |S| = |S \setminus M|.$$

Die Ungleichung $|M'| < |S|$ folgt dabei aus den Tatsachen, dass S überabzählbar und M'/K eine algebraische Körpererweiterung ist. Denn für jede algebraische Körpererweiterung M'/K ist $|M'| = |K| < |S|$, falls K unendlich ist, und $|M'| \leq |\mathbb{N}| < |S|$ falls K endlich ist. Dies ergibt sich aus der Tatsache, dass die Menge $\mathfrak{P}$ aller normierten irreduziblen Polynome in $K[x]$ abzählbar ist, falls K endlich ist, und $|\mathfrak{P}| = |K|$ ist, falls K unendlich ist. Die Gleichung $|S| = |S \setminus M|$ folgt aus $|S| = |(S \setminus M) \cup M| = |S \setminus M| + |M| = \max\{|S \setminus M|, |M|\}$ zusammen mit der Aussage, dass für die algebraische Körpererweiterung M/K gilt $|M| = |K| < |S|$ oder $|M| = |\mathbb{N}| < |S|$.

Da $|M' \setminus M| < |S \setminus M|$ gilt, existiert eine injektive Abbildung $\phi : M' \to S$ mit $\phi|_M = \mathrm{id}_M$. Definiert man auf $\phi(M')$ die Verknüpfungen

$$\phi(\alpha) + \phi(\beta) := \phi(\alpha + \beta) \qquad \phi(\alpha) \cdot \phi(\beta) = \phi(\alpha \cdot \beta) \qquad \forall \alpha, \beta \in M',$$

so wird $\phi : M' \to \phi(M')$ ein Körperisomorphismus und $\phi(M')/M$ ein echter algebraischer Erweiterungskörper von M. Das ist ein Widerspruch zur Maximalität von M, und somit ist M algebraisch abgeschlossen. Da M/K ausserdem nach 1. algebraisch ist, ist M ein algebraischer Abschluss von K. □

Da der algebraische Abschluss eines gegebenen Körpers sehr kompliziert und schwer zu beschreiben sein kann, beschränkt man sich oft auf die Betrachtung von Körpererweiterungen L/K, in denen bestimmte Polynome in $K[x]$ in Linearfaktoren zerfallen. Diese Körpererweiterungen möchte man so effizient wie möglich wählen, d. h. den kleinsten Erweiterungskörper von K betrachten, für den dies der Fall ist. Dies führt auf das Konzept des Zerfällungskörpers.

Definition 1.4.6: Sei K ein Körper und $A \subset K[x]$. Ein Erweiterungskörper L von K heißt **Zerfällungkörper** von A über K, wenn:

1. Jedes Polynom $p \in A$ über L in Linearfaktoren zerfällt
2. L aus K durch Adjunktion von Nullstellen von Polynomen $p \in A$ entsteht.

Beispiel 1.4.7:

1. Das Polynom $f = x^3 - 2x \in \mathbb{Q}[x]$ hat in $\mathbb{R}$ die Nullstellen $\pm\sqrt{2}$, 0. Also ist $\mathbb{Q}(\sqrt{2}) \cong \mathbb{Q}[x]/(x^2 - 2)$ der Zerfällungskörper von p.
2. Ist L/K eine Körpererweiterung und $f = x^2 + bx + c \in K[x]$ irreduzibel mit einer Nullstelle $\alpha \in L$, so ist $K(\alpha) \subset L$ der Zerfällungskörper von f, denn in $K(\alpha)$ läßt sich der Linearfaktor $x - \alpha$ abspalten, also $f = q(x - \alpha)$ mit $q \in K(\alpha)[x]$ und q ist linear.
3. Wir betrachten $f = x^{2p} + 1 \in \mathbb{F}_p[x]$ für $p \in \mathbb{N}$ prim.

   Da $\mathbb{F}_p[x]$ ein Integritätsbereich mit $\mathrm{char}(\mathbb{F}_p[x]) = \mathrm{char}(\mathbb{F}_p) = p \neq 0$ ist, ist nach einem Ergebnis aus der Vorlesung Algebra die **Frobeniusabbildung** $F_p : \mathbb{F}_p[x] \to \mathbb{F}_p[x], x \mapsto x^p$ ein injektiver unitärer Ringhomomorphismus mit $(a + b)^p = a^p + b^p$ für alle $a, b \in \mathbb{F}_p[x]$. Also folgt $f = x^{2p} + 1 = (x^2 + 1)^p$, und der Zerfällungskörper von f ist isomorph zu $\mathbb{F}_p[x]/(x^2 + 1)$.

Direkt aus der Definition ergeben sich ausserdem die folgenden Aussagen über Zerfällungskörper, deren Beweis eine gute Übung ist.

Bemerkung 1.4.8: Ist L ein Zerfällungskörper von $A \subset K[x]$ über K, so gilt:

1. *Kein* echter Zwischenkörper $K \subsetneq E \subsetneq L$ ist ein Zerfällungskörper von A.
2. L/K ist algebraisch.
3. Ist $A = \{p_1, ..., p_n\}$ mit $p_i \in K[x]$, so ist L ein Zerfällungskörper von $q = p_1 \cdots p_n$ und jeder Zerfällungskörper von q ist ein Zerfällungskörper von A.
4. Für $A = \{p\}$ mit $\deg(p) = n$ folgt $[L : K] | n!$, insbesondere also $[L : K] \leq n!$.

Wie auch beim algebraischen Abschluss, stellt sich natürlich die Frage nach der Existenz eines Zerfällungskörpers für einen Körper K und eine Teilmenge $A \subset K[x]$. Dieser läßt sich mit Hilfe eines algebraischen Abschlusses $\overline{K}$ konstruieren, indem man in der Körpererweiterung $\overline{K}/K$ die Menge der Nullstellen von Polynomen in A zu K adjungiert.

Satz 1.4.9: Jede Teilmenge $A \subset K[x]$ hat einen Zerfällungskörper. Jeder Erweiterungskörper L von K, über dem jedes Polynom aus A zerfällt, enthält genau einen Zerfällungskörper von A.

Beweis:
Ist L/K eine Körpererweiterung, so dass jedes Polynom $p \in A$ über L zerfällt, so folgt $K(N_A) \subset L$, wobei $N_A = \{\alpha \in L : \exists p \in A : p(\alpha) = 0\}$ die Menge der Nullstellen von Polynomen $p \in A$ bezeichnet. Der Körper $K(N_A)$ ist dann ein in L enthaltener Zerfällungskörper von A. Nach den Satz von Steinitz (Satz 1.4.5) besitzt K einen algebraischen Abschluss $\overline{K}$, über

dem jedes Polynom $p \in A$ zerfällt. Also kann man $L = K$ wählen. Die Eindeutigkeit ergibt sich aus Bemerkung 1.4.8, 1. □

Insbesondere läßt sich mit Hilfe dieses Satzes der Zusammenhang zwischen Zerfällungskörpern und algebraischen Abschlüssen klären. Die Definitionen legen nahe, dass ein algebraischer Abschluss eines Körpers K ein Zerfällungskörper von $A = K[x]$ ist, und umgekehrt ein Zerfällungskörper von $K[x]$ auch ein algebraischer Abschluss von L ist. Dass dies tatsächlich zutrifft, zeigt das folgende Lemma.

Lemma 1.4.10: Ein Erweiterungskörper L von K ist ein algebraischer Abschluss von K genau dann, wenn er ein Zerfällungskörper von $K[x]$ ist.

Beweis:
Ist L ein algebraischer Abschluss von K, so enthält L nach Satz 1.4.9 genau einen Zerfällungskörper E von $K[x]$. Da für jedes $\alpha \in L$ das Minimalpolynom von α in K über E zerfällt, folgt $E = L$. Ist umgekehrt L ein Zerfällungskörper von $K[x]$, so ist nach Bemerkung 1.4.3 ein algebraischer Abschluss $\overline{L}$ von L auch ein algebraischer Abschluss von K und somit ein Zerfällungskörper von K. Damit folgt mit Satz 1.4.9 $L = \overline{L}$. □

Nachdem wir die Existenz von Zerfällungskörpern und ihren Zusammenhang mit dem Begriff des algebraischen Abschlusses geklärt haben, widmen wir uns nun der Frage nach der Eindeutigkeit von Zerfällungskörpern. Wie auch bei anderen Klassifikationsproblemen ist es hier sinnvoll, die Frage der Eindeutigkeit nur "bis auf Isomorphie" zu klären. Dazu benötigt man zunächst ein brauchbares Konzept von Isomorphismen von Körpererweiterungen.

Eine naheliegende Idee ist es, diese als Isomorphismen $\psi : L \to L'$ der Erweiterungskörper zu definieren, die den *Grundkörper K festlassen*. Analog definiert man auch Monomorphismen und Automorphismen von Körpererweiterungen. Zur Unterscheidung von allgemeinen Körperisomorphismen (Körpermonomorphismen, Körperautomorphismen), die die letzte Bedingung nicht erfüllen, bezeichnet man diese als K-Isomorphismen (K-Monomorphismen, K-Automorphismen).

Definition 1.4.11: Seien L/K, L'/K Körpererweiterungen. Ein Körpermonomorphismus (Körperisomorphismus, Körperautomorphismus) $\psi : L \to L'$ mit $\psi|_K = \mathrm{id}_K$ heißt **K-Monomorphismus** oder **K-Monomorphismus** (**K-Isomorphismus**, **K-Automorphismus**).

Bemerkung 1.4.12:

1. Sind L, L', L'' Erweiterungskörper eines Körpers K und $\phi : L \to L'$ und $\psi : L' \to L''$ K-Monomorphismen, so ist auch $\psi \circ \phi : L \to L''$ ein K-Monomorphismus.
2. Die K-Automorphismen einer Körpererweiterung L/K bilden eine Untergruppe der Automorphismen-Gruppe $\mathrm{Aut}(L)$, die sogenannte **Galois-Gruppe** $\Gamma(L/K)$ der Körpererweiterung L/K.

Um Körpererweiterungen oder Zerfällungskörper L/K bis auf Isomorphie zu klassifizieren, müssen wir uns mit der Frage befassen, inwieweit ein K-Monomorphismus $\psi : L \to L'$ durch seine Werte auf $K \subset L$ bereits bestimmt ist bzw. auf wie viele verschiedene Weisen sich die Identitätsabbildung $\mathrm{id}_K : K \to K$ zu einem Körpermonomorphismus $L \to L'$ fortsetzen läßt. Hierzu betrachtet man einen etwas allgemeineren Fall, nämlich die Fortsetzung von Isomorphismen $\phi : K \to K'$ auf Körpererweiterungen L/K und L'/K'. Dies führt auf die sogenannten Fortsetzungssätze.

Satz 1.4.13: (**Fortsetzungssatz für primitive Körpererweiterungen**)

Seien L/K und L'/K' Körpererweiterungen, $\phi : K \to K'$ ein Körperisomorphismus und $\phi_* : K[x] \to K'[x]$, $\sum_{k=0}^n a_k x^k \mapsto \sum_{k=0}^n \phi(a_k)x^k$ der zugehörige Ringhomomorphismus aus Bemerkung 1.1.7. Sei $\alpha \in L$ algebraisch mit Minimalpolynom p.

1. Dann existiert zu jeder Nullstelle β von $\phi_*(p) \in K'[X]$ genau ein Körpermonomorphismus $\phi_\beta : K(\alpha) \to L'$ mit $\phi_\beta|_K = \phi$ und $\phi_\beta(\alpha) = \beta$, nämlich
$$\phi_\beta : \sum_{k=0}^n b_k\alpha^k \mapsto \sum_{k=0}^n \phi(b_k)\beta^k$$
2. Jeder Körpermonomorphismus $\psi : K(\alpha) \to L'$ mit $\psi|_K = \phi$ ist von dieser Form.

Beweis:
1. Nach Bemerkung 1.1.7 existiert zu $\beta \in L'$ genau ein Ringhomomorphismus $\Phi_\beta : K[x] \to L'$ mit $\Phi_\beta|_K = \phi$ und $\Phi_\beta(x) = \beta$, nämlich $\Phi_\beta = \mathrm{ev}_\beta \circ \phi_* : \sum_{k=0}^n b_k x^k \mapsto \sum_{k=0}^n \phi(b_k)\beta^k$. Ist β eine Nullstelle von $\phi_*(p)$, so gilt $\Phi_\beta(q) = 0$ für alle $q \in (p)$, und man erhält einen unitären Ringhomomorphismus $\tilde{\Phi}_\beta : K[x]/(p) \to L'$, $\sum_{k=0}^n b_k\overline{x}^k \mapsto \sum_{k=0}^n \phi(b_k)\beta^k$ mit $\tilde{\Phi}_\beta|_K = \phi$. Da nach Satz 1.3.3 die Evaluation in α einen Isomorphismus $\widetilde{\mathrm{ev}}_\alpha : K[x]/(p) \xrightarrow{\sim} K(\alpha), \sum_{k=0}^n b_k\overline{x}^k \to \sum_{k=0}^n b_k\alpha^k$ induziert, ist $\phi_\beta = \tilde{\Phi}_\beta \circ \widetilde{\mathrm{ev}}_\alpha^{-1} : K(\alpha) \to L'$ der gesuchte Körpermonomorphismus.

2. Ist umgekehrt $\psi : K(\alpha) \to L'$ ein Körpermonomorphismus mit $\psi|_K = \phi$, so folgt für alle Polynome $q = \sum_{k=0}^n b_k x^k \in K[x]$ die Identität $\psi(\sum_{k=0}^n b_k\alpha^k) = \sum_{k=0}^n \phi(b_k)\psi(\alpha)^k$. Der Körpermonomorphismus ψ ist also durch ϕ und $\beta = \psi(\alpha)$ eindeutig bestimmt. Ausserdem gilt $0 = \psi(0) = \psi(p(\alpha)) = \sum_{k=0}^n a_k\psi(\alpha)^k = \sum_{k=0}^n a_k\beta^k$, und somit ist β eine Nullstelle von $\phi_*(p)$. □

Im Fall von Erweiterungskörpern L, L', die Zerfällungskörper von Polynomen in $K[x]$ sind, läßt sich aus diesem Satz noch eine deutlich stärkere Aussage gewinnen, die es uns erlauben wird, die Eindeutigkeit von Zerfällungskörpern zu beweisen. Der Beweis benutzt das Zornsche Lemma.

Satz 1.4.14: (**Fortsetzungssatz für Zerfällungskörper**)

Sei $\phi : K \to K'$ ein Körperisomorphismus und $\phi_* : K[x] \to K'[x]$ der induzierte Ringhomomorphismus aus Bemerkung 1.1.7. Ist L ein Zerfällungskörper von $A \subset K[x]$ über K und L' ein Zerfällungskörper von $A' = \phi_*(A)$ über K', so kann ϕ zu einem Körperisomorphismus $\psi : L \to L'$ mit $\psi|_K = \phi$ fortgesetzt werden.

Beweis:
1. Sei $\mathfrak{M} = \{\text{Monomorphismen } \psi : F \to L' : \ K \subset F \subset L \text{ Zwischenkörper, } \psi|_K = \phi\}$. Für zwei Monomorphismen $\psi : F \to L'$, $\chi : G \to L'$ setzen wir $\chi \leq \psi$, wenn ψ eine Fortsetzung von χ

ist, d. h. $G \subset F$ und $\psi|_G = \chi$. Dies definiert eine Ordnungsrelation auf M, und wegen $\phi \in \mathfrak{M}$ ist $\mathfrak{M} \neq \emptyset$. Wir zeigen, dass jede total geordnete Kette $\mathfrak{k}$ in $(\mathfrak{M}, \leq)$ eine obere Schranke besitzt. Mit dem Zornschen Lemma folgt dann, dass $(\mathfrak{M}, \leq)$ ein maximales Element besitzt, also einen Monomorphismus $\psi : F \to L'$ für einen Zwischenkörper $K \subset F \subset L$ mit $\psi|_K = \phi$, so dass für jeden weiteren Monomorphismus $\chi : G \to L'$ mit $\chi|_K = \phi$ gilt $G \subset F$ und $\psi|_G = \chi$.

2. Jede total geordnete Kette $\mathfrak{k}$ in $(\mathfrak{M}, \leq)$ besitzt eine obere Schranke:

Dazu setzen wir $E := \bigcup_{\sigma \in \mathfrak{k}} \mathrm{Def}(\sigma)$, wobei $\mathrm{Def}(\sigma) = F$ den Definitionsbereich eines Körpermonomorphismus $\sigma : F \to L'$ bezeichnet. Dann ist E ein Zwischenkörper von L/K. Wir definieren nun eine Fortsetzung $\chi : E \to L'$ von ϕ durch die Vorschrift $\chi(\alpha) = \sigma(\alpha)$ für $\alpha \in F$ und $\sigma : F \to L'$. Dies ist unabhängig von der Wahl von σ, denn ist $\tau : G \to L'$ in $\mathfrak{k}$ ein weiterer Monomorphismus in $\mathfrak{k}$ mit $\alpha \in G$, so folgt $\sigma \leq \tau$ und damit $F \subset G$, $\tau|_F = \sigma$ oder $\tau \leq \sigma$ und damit $G \subset F$, $\sigma|_G = \tau$. Also erhalten wir eine injektive Abbildung $\chi : E \to L'$ mit $\chi|_K = \phi$. Wir zeigen, dass $\chi : E \to L'$ ein Körpermonomorphismus ist. Seien dazu $\alpha, \beta \in E$. Da $\mathfrak{k}$ eine Kette ist, existiert zu $\alpha, \beta \in E$ ein $\tau : G \to L'$ in $\mathfrak{k}$ mit $\alpha, \beta \in G$, und es folgt

$$\chi(\alpha+\beta) = \tau(\alpha+\beta) = \tau(\alpha)+\tau(\beta) = \chi(\alpha)+\chi(\beta), \quad \chi(\alpha\cdot\beta) = \tau(\alpha\cdot\beta) = \tau(\alpha)\cdot\tau(\beta) = \chi(\alpha)\cdot\chi(\beta).$$

Damit ist $\chi : E \to L'$ ein Körpermonomorphismus mit $\chi|_K = \phi$ und somit eine obere Schranke von $\mathfrak{k}$.

3. Mit dem Zornschen Lemma folgt, dass $(\mathfrak{M}, \leq)$ ein maximales Element $\psi : F \to L'$ besitzt. Es reicht dann, zu zeigen, dass $F = L$ und $\psi(L) = L'$ gilt:

Sei dazu $p \in A$ und $\alpha \in L$ mit $p(\alpha) = 0$. Dann zerfällt das Bild $\psi_*(m_{\alpha,K})$ des Minimalpolynoms von α in L' und somit hat $\psi_*(m_{\alpha,K})$ eine Nullstelle in L'. Mit Satz 1.4.13 folgt, dass sich ψ zu einem Monomorphismus $\psi : F(\alpha) \to L'$ fortsetzen läßt. Aus der Maximalität von ψ folgt dann direkt $F(\alpha) \subset F$, also $\alpha \in F$ und damit $F = L$.

Da p über L zerfällt, läßt es sich schreiben als $p = c(x - a_1) \cdots (x - a_n)$ mit $c, a_1, ..., a_n \in L$. Sein Bild ist gegeben durch $\psi_*(p) = \psi(c)(x - \psi(a_1)) \cdots (x - \psi(a_n))$. Also enthält $\psi(F) = \psi(L)$ einen Zerfällungskörper von $\psi_*(A)$ über K' und mit Satz 1.4.9 folgt $\psi(L) = L'$. □

Betrachtet man diesen Fortsetzungssatz nun für den Spezialfall $K = K'$ und $\phi = \mathrm{id}_K$, so erhält man direkt eine Eindeutigkeitsaussage für Zerfällungskörper und damit auch für algebraische Abschlüsse, die nach Lemma 1.4.10 ja gerade die Zerfällungskörper von $A = K[x]$ sind.

Korollar 1.4.15:

1. Zerfällungskörper sind eindeutig bis auf Isomorphie: Ist K ein Körper und sind L, L' Zerfällungskörper einer Menge $A \subset K[x]$, so existiert ein K-Isomorphismus $\psi : L \to L'$.
2. Zwei algebraische Abschlüsse L, L' von K sind K-isomorph, d. h. es existiert ein Körperisomorphismus $\psi : L \to L'$ mit $\psi|_K = \mathrm{id}_K$.

Ein weiterer wichtiger Spezialfall ergibt sich, wenn man in Satz 1.4.14 für den Körper L' einen algebraisch abgeschlossenen Körper wählt. Denn in diesem Fall enthält L' einen Zerfällungskörper von $\phi_*(K[x])$. Damit läßt sich dann ein Körperisomorphismus $\phi : K \to K'$ auf algebraischen Abschluss von L fortsetzen und damit insbesondere auf L selbst.

Satz 1.4.16: (**Fortsetzungssatz für K-Monomorphismen in algebraisch abgeschlossene Körper**)

Sei L/K eine algebraische Körpererweiterung. Dann ist jeder K-Monomorphismus $\phi : K \to M$ in einen algebraisch abgeschlossenen Erweiterungskörper M von K zu einem K-Monomorphismus $\tilde{\phi} : L \to M$ fortsetzbar.

Beweis:
Sei $\phi : K \to M$ ein K-Monomorphismus und $\overline{L}$ ein algebraischer Abschluss von L. Dann ist $\overline{L}$ nach Bemerkung 1.4.3 auch ein algebraischer Abschluss von K und nach Lemma 1.4.10 ein Zerfällungskörper von $K[x]$ über K. Nach Satz 1.4.9 enthält M einen Zerfällungskörper E von $\phi(K)[x]$ über $\phi(K)$. Mit Satz 1.4.14 zur Fortsetzung von Isomorphismen auf Zerfällungskörper folgt, dass sich ϕ zu einem K-Isomorphismus $\psi : \overline{L} \to E$ fortsetzen läßt, und $\psi|_L : L \to E \subset M$ ist der gesuchte K-Monomorphismus. □

1.5 Normale und separable Körpererweiterungen

Wie sich in der Vorlesung und in den Übungen bereits gezeigt hat, folgt für ein Polynom $p \in K[x]$, das eine Nullstelle in einem Erweiterungskörper L von K besitzt, nicht automatisch, dass es über L in Linearfaktoren zerfällt. Ist L ein Zerfällungskörper einer Teilmenge $A \subset K[x]$, so gilt dies sicherlich für alle Polynome $p \in A$, aber nicht jede algebraische Körpererweiterung L/K ist Zerfällungskörper einer Teilmenge $A \subset K[x]$. Körpererweiterungen dieser Art haben besonders schöne Eigenschaften und erhalten daher einen eigenen Namen. Sie heissen *normale Körpererweiterungen* und lassen sich auch über das Verhalten von K-Monomorphismen $L \to \overline{L}$ charakterisieren.

Satz 1.5.1: Sei L/K eine algebraische Körpererweiterung und $\overline{L}$ ein algebraischer Abschluss von L. Dann sind äquivalent:

(i) L ist Zerfällungskörper einer Teilmenge $A \subset K[x]$.

(ii) Jeder K-Monomorphismus $\phi : L \to \overline{L}$ erfüllt $\phi(L) = L$.

(iii) Jedes irreduzible Polynom $p \in K[x]$ mit einer Nullstelle in L zerfällt über L.

Eine algebraische Körpererweiterung L/K, die eine dieser Bedingungen erfüllt, heißt **normal**.

Beweis:
(i)⇒ (ii):
Sei $\phi : L \to \overline{L}$ ein K-Monomorphismus und $\alpha \in L$ eine Nullstelle von $p = \sum_{k=0}^{n} a_k x^k \in A$. Dann ist wegen $0 = \phi(0) = \phi(p(\alpha)) = \sum_{k=0}^{n} a_k \phi(\alpha)^k$ auch $\phi(\alpha)$ eine Nullstelle von p und liegt nach (i) in L. Also erhält ϕ die Nullstellenmenge $N_A = \{\alpha \in L : \exists p \in A \,\text{mit}\, p(\alpha) = 0\}$. Da nach (i) L ein Zerfällungskörper von A ist und somit $L = K(N_A)$, folgt $\phi(L) = L$.

(ii)⇒ (iii):
Sei $p \in K[x]$ ein irreduzibles Polynom mit einer Nullstelle $\alpha \in L$ und $\beta \in \overline{L}$ eine beliebige Nullstelle von p in $\overline{L}$. Dann existiert nach dem Fortsetzungssatz für primitive Körpererweiterungen (Satz 1.4.13) ein K-Monomorphismus $\phi : K(\alpha) \to \overline{L}$ mit $\phi(\alpha) = \beta$, und dieser ist nach Satz 1.4.16 zu einem K-Monomorphismus $\phi : L \to \overline{L}$ fortsetzbar. Nach Voraussetzung (ii) ist

$\beta = \phi(\alpha) \in \phi(L) = L$. Also liegen alle Nullstellen $\beta \in \overline{L}$ von p in L, und p zerfällt über L in Linearfaktoren.

(iii)⇒(i):
Nach (iii) zerfällt für jedes Element $\alpha \in L$ das Minimalpolynom $m_{\alpha,K}$ über L und somit ist L Zerfällungskörper von $A = \{m_{\alpha,K} : \alpha \in L\}$. □

Beispiel 1.5.2:

1. Quadratische Körpererweiterungen L/K sind normal. Denn jedes irreduzible Polynom $p \in K[x]$ mit einer Nullstelle $\alpha \in L$ hat den Grad $\deg(p) = 2$ und zerfällt somit über L in Linearfaktoren.
2. Ist $\overline{K}$ ein algebraischer Abschluss von K, so ist $\overline{K}/K$ normal, denn $\overline{K}$ ist nach Lemma 1.4.10 ein Zerfällungskörper von $K[x]$.
3. Die Körpererweiterung $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ ist nicht normal. Das Polynom $p = x^3 - 2$ hat die Nullstelle $\sqrt[3]{2}$ in L, zerfällt aber über $\mathbb{Q}(\sqrt[3]{2})$ nicht in Linearfaktoren, denn die anderen beiden komplexen Nullstellen $\sqrt[3]{2}e^{2\pi i/3}$ und $\sqrt[3]{2}e^{4\pi i/3}$ von p sind nicht in $\mathbb{Q}(\sqrt[3]{2})$ enthalten.

Durch Übergang zum algebraischen Abschluss einer algebraischen Körpererweiterung L/K erhält man also immer eine normale Körpererweiterung über K, die L als Zwischenkörper enthält. Im Allgemeinen möchte man dies aber nicht tun, sondern mit möglichst kleinen normalen Körpererweiterungen von K arbeiten, die L als Zwischenkörper enthalten. Eine offensichtliche Idee, um eine solche Körpererweiterung zu konstruieren, ist es, alle Nullstellen von Polynomen $p \in K[x]$ zu L zu adjungieren, die eine Nullstelle in L besitzen. Dies liefert die sogenannte *normale Hülle* von L/K.

Lemma 1.5.3: Zu jeder algebraischen Körpererweiterung L/K existiert ein Erweiterungskörper N von L, so dass N/K normal ist und kein echter Zwischenkörper $L \subset E \subsetneq N$ mit E/K normal existiert. Der Erweiterungskörper N ist eindeutig bis auf K-Isomorphie und heißt **normale Hülle** von L/K.

Beweis:
1. Existenz: Ist L/K eine algebraische Körpererweiterung, so ist für den Zerfällungskörper N der Menge $A = \{p \in K[x] : \exists \alpha \in L \,\text{mit}\, p(\alpha) = 0\}$ die Körpererweiterung N/K normal nach Satz 1.5.1 (i). Nach Satz 1.5.1 (iii) gilt für jeden Zwischenkörper $L \subset E \subset N$ mit E/K normal $E = N$. Also besitzt jede algebraische Körpererweiterung L/K eine normale Hülle N.

2. Eindeutigkeit: Sind N, N' zwei normale Hüllen von L/K, so folgt aus der Eindeutigkeit der Zerfällungskörper (Korollar 1.4.15), dass N und N' K-isomorph sind. □

Beispiel 1.5.4: Nach Beispiel 1.5.2, 3. ist die Körpererweiterung $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ nicht normal. Ihre normale Hülle ist $\mathbb{Q}(\sqrt{2}, e^{2\pi i/3})$, denn diese enthält alle Nullstellen des Minimalpolynoms $p = x^3 - 2$ von $\sqrt[3]{2}$ über $\mathbb{Q}$, und wegen $[\mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3}) : \mathbb{Q}(\sqrt[3]{2})] = 2$ existiert kein echter Zwischenkörper, über dem p in Linearfaktoren zerfällt.

Durch Übergang zur normalen Hülle können wir also zu jeder algebraischen Körperweiterung L/K eine normale Körpererweiterung N/K mit Zwischenkörper $K \subset L \subset N$ konstruieren. Hat ein über K irreduzibles Polynom $p \in K[x]$ dann eine Nullstelle in L, so zerfällt p über N bereits in Linearfaktoren, läßt sich als als

$$p = (x - \alpha_1)^{n_1} \cdots (x - \alpha_m)^{n_m} \qquad \text{mit } \alpha_1, ..., \alpha_m \in L \text{ paarweise verschieden, } n_1, ..., n_m \in \mathbb{N}$$

schreiben. Hierbei sind für jede Nullstelle α_k zwei Fälle zu unterscheiden, nämlich $n_k = 1$ (einfache Nullstelle) und $n_k > 1$ (mehrfache Nullstelle). Es wird sich zeigen, dass normale Körpererweiterungen besonders schöne Eigenschaften besitzen, wenn die Nullstellen der zugehörigen Polynome $p \in A \subset K[x]$ in L alle einfach sind. Wir werden sehen, dass dies für Körper der Charakteristik 0 stets der Fall ist, nicht aber für Körper der Charakteristik p mit $p \in \mathbb{N}$ prim. Wir müss en uns dazu zunächst genauer mit der Vielfachheit von Nullstellen von Polynomen $p \in K[x]$ beschäftigen.

Definition 1.5.5: Sei L/K eine Körpererweiterung und $p \in K[x]^*$. Ein Element $\alpha \in L$ heißt **m-fache Nullstelle** bzw. Nullstelle der **Vielfachheit** m von p, wenn ein Polynom $q \in K[x]$ mit $p = (x - \alpha)^m q$ und $q(\alpha) \neq 0$ existiert. Für $m = 1$ spricht man von einer **einfachen Nullstelle** für $m > 1$ von einer **mehrfachen Nullstelle**.

Der Nachteil dieser Definition ist, dass man das Polynom q etwa mit Hilfe des euklidischen Algorithmus oder mit Polynomdivision explizit bestimmen muss, um die Vielfachheit einer Nullstelle angeben zu können. Aus der Analysis ist ein nützliches Kriterium bekannt, die die Vielfachheit von Nullstellen einer stetig differenzierbaren Funktion $f : \mathbb{R} \to \mathbb{R}$ durch die Ableitung von f an der Nullstelle charakterisiert. Eine Nullstelle α einer solchen Funktion f ist nämlich genau dann einfach, wenn $f'(\alpha) \neq 0$. Die aus der Analysis bekannte Definition von Ableitungen über die Grenzwerte von Differenzenquotienten läßt sich natürlich nicht einfach auf beliebige Körper übertragen. Da wir aber nicht allgemeine Funktionen $f : K \to K$ sondern Polynome betrachten, können wir Ableitungen *formal*, über die aus der Analysis bekannten Formeln für die Ableitungen von Polynomen definieren.

Definition 1.5.6: Sei K ein Körper. Die **algebraische Ableitung** oder **formale Ableitung** eines Polynoms und $p = \sum_{k=0}^{n} a_k x^k \in K[x]$ ist das Polynom

$$p' = \sum_{k=1}^{n} k a_k x^{k-1}.$$

Bemerkung 1.5.7: Man zeigt leicht, dass für die formale Ableitung die üblichen Ableitungsregeln gelten. Alle Polynome $p, q \in K[x]$ erfüllen die:

1. **Summenregel:** $(p + q)'(x) = p'(x) + q'(x)$,
2. **Produktregel:** $(pq)'(x) = p'(x)q(x) + p(x)q'(x)$,
3. **Kettenregel:** $(p \circ q)'(x) = p'(q(x))q'(x)$.

Mit Hilfe der formalen Ableitung erhalten wir einfache Kriterien, um die Vielfachheit von Nullstellen von Polynomen $p \in K[x]$ zu charakterisieren.

Lemma 1.5.8: Sei L/K eine Körpererweiterung, so dass $p \in K[x]$ über L zerfällt. Dann gilt:

1. Ein Element $\alpha \in L$ ist genau dann eine mehrfache Nullstelle von p, wenn $p(\alpha) = p'(\alpha) = 0$.
2. Das Polynom $p \in K[x]$ hat genau dann mehrfache Nullstellen in L, wenn p und p' einen nicht-konstanten gemeinsamen Teiler in $K[x]$ haben.
3. Ist p irreduzibel über K, so hat p genau dann mehrfache Nullstellen in L, wenn $p' = 0$.

Beweis:
1. Ist $\alpha \in L$ eine mehrfache Nullstelle von p, so existiert ein $m \in \mathbb{N}$, $m > 1$ mit $p = (x-\alpha)^m q$ in $L[x]$. Mit der Produktregel folgt $p' = m(x-\alpha)^{m-1}q + (x-\alpha)^m q' = (x-\alpha)^{m-1}(mq + (x-\alpha)q')$ und damit $p'(\alpha) = 0$. Ist $\alpha \in L$ eine einfache Nullstelle von p in $L[x]$, so folgt $p = (x-\alpha)q$ mit $q(\alpha) \neq 0$ und damit $p'(\alpha) = q(\alpha) + (\alpha - \alpha)q' = q(\alpha) \neq 0$.

2. Sind p, p' teilerfremd in $K[x]$, so existieren Polynome $r, s \in K[x]$ mit $rp + sp' = 1$. Für alle $\alpha \in L$ mit $p(\alpha) = 0$ folgt $1 = r(\alpha)p(\alpha) + s(\alpha)p'(\alpha) = s(\alpha)p'(\alpha)$ und damit ist $p'(\alpha) \neq 0$. Nach 1. hat p somit keine mehrfache Nullstelle. Haben p, p' dagegen einen nicht-konstanten gemeinsamen Teiler $d \in K[x]$, so hat d eine Nullstelle $\alpha \in L$ und somit $(x-\alpha)|d$. Es folgt $(x-\alpha)|p, p'$ uns somit $p'(\alpha) = p(\alpha) = 0$. Nach 1. ist α dann eine mehrfache Nullstelle von p.

3. Sei p irreduzibel über K. Dann ist jeder nicht-konstante gemeinsame Teiler d von p, p' von der Form $d = cp$ mit $c \in K^*$. Daraus ergibt sich $\deg(d) = \deg(p) = \deg(p') + 1$, und aus $d|p'$ folgt $p' = 0$. Umgekehrt folgt aus $p' = 0$, dass jede Nullstelle $\alpha \in L$ einen nicht-konstanten Teiler d von p und p' liefert. Mit 2. folgt die Behauptung. □

Beispiel 1.5.9:

1. Das Polynom $p = x^3 - 3x + 2 \in \mathbb{Q}[x]$ hat wegen $p = (x-1)^2(x+2)$ die zweifache Nullstelle 1 und die einfache Nullstelle 2.

2. Das Polynom $p = x^3 + \overline{2}x^2 + x + \overline{2} = (x - \overline{1})(x^2 + \overline{1}) \in \mathbb{F}_3[x]$ hat eine einfache Nullstelle in $\overline{1}$, denn das Polynom $q = x^2 + \overline{1}$ hat keine Nullstelle in $\mathbb{F}_3$. Wegen $q' = \overline{2}x \neq 0$ und der Irreduzibilität von q folgt mit Lemma 1.5.8, dass p keine mehrfachen Nullstellen in seinem Zerfällungskörper haben kann.

3. Sei $K = Q(\mathbb{F}_p[x])$ der Körper der rationalen Funktionen über $\mathbb{F}_p$ mit $p \in \mathbb{N}$ prim. Dann ist das Polynom $q = y^p - x \in K[y]$ nach dem Eisenstein-Kriterium irreduzibel, denn das Polynom x ist ein Primelement in $\mathbb{F}_p[x]$. Das Polynom q hat wegen $q' = py^{p-1} = 0$ mehrfache Nullstellen in seinem Zerfällungskörper.

Hat ein Polynom $p \in K[x]$ nur einfache Nullstellen in einem Erweiterungskörper L von K, so liegen seine Nullstellen *separat*, d. h. verschiedene Nullstellen fallen nicht zusammen. Aus diesem Grund bezeichnet man ein solches Polynom als separabel. Ebenso erhalten wir über das Minimalpolynom ein Konzept von Separabilität für algebraische Elemente einer Körpererweiterung und ein Konzept von separablen Körpererweiterungen.

Definition 1.5.10:

1. Ein Polynom $p \in K[x]$ heißt **separabel** , wenn jeder irreduzible Faktor von p nur einfache Nullstellen in dem Zerfällungskörper von p über K hat, und ansonsten **inseparabel**.

2. Ein Element $\alpha \in L$ eines Erweiterungskörpers L von K heißt **separabel** (**inseparabel**) über K, wenn es algebraisch und sein Minimalpolynom $m_{\alpha,K}$ separabel (inseparabel) ist.
3. Eine Körpererweiterung L/K heißt **separabel** , wenn jedes Element aus L separabel über K ist. Eine nicht seperable algebraische Körpererweiterung nennt man **inseparabel**.
4. Ein Körper K heißt **vollkommen**, wenn jedes Polynom $p \in K[x]$ und damit jeder algebraische Erweiterungskörper von K separabel ist.

Beispiel 1.5.11:

1. Jedes Element $\alpha \in K$ ist separabel über K, da es algebraisch über K mit separablem Minimalpolynom $x - \alpha$ ist.
2. Eine algebraische Körpererweiterung ist genau dann separabel, wenn für alle $\alpha \in L$ das Minimalpolynom $m_{\alpha,K}$ in seinem Zerfällungskörper nur einfache Nullstellen hat.
3. Das Polynom $p = (x^2+1)^2(x-1)(x^4+x^3+x^2+x+1)$ ist separabel über $\mathbb{Q}$, denn seine irreduziblen Faktoren haben nur einfache Nullstellen. Diese sind $\pm$i für x^2+1, 1 für $x-1$ und $e^{2\pi ik/5}$, $k \in \{1,2,3,4\}$ für $x^4+x^3+x^2+x+1$.
4. Sind $p, q \in K[x]$ separabel über K, so auch $p \cdot q$.
5. Man kann zeigen, dass die Eigenschaft *separabel* transitiv ist: Sind E/K und L/E separable Körpererweiterungen, so ist auch L/K separabel (siehe Aufgabe 28).
6. Sei K ein Körper der Charakteristik $p \in \mathbb{N}$, $L = Q(K[x])$ und $E = Q(K[x^p]) \subset L$. Dann ist das Element $x \in L$ nicht separabel über K. Sein Minimalpolynom ist das Polynom $f = y^p - x^p \in E[y] \cong K[x,y]$, das nach dem Kriterium von Eisenstein irreduzibel über K ist und ausserdem $f(x) = x^p - x^p = 0$ erfüllt. Dieses Polynom läßt sich über L wegen des Frobeniusmonomorphismus in Charakteristik p aber auch als $f = (y-x)^p \in L[y] \cong K[x,y]$ schreiben und hat somit eine p-fache Nullstelle in L.

Versucht man naiv, inseparable Polynome oder Körpererweiterungen zu konstruieren, so stellt man fest, dass dies sehr schwierig ist. Das liegt daran, dass inseparable Körpererweiterungen eher selten sind und nur über Grundkörpern der Charakteristik $p \in \mathbb{N}$ mit p prim auftreten können, und - wie wir später sehen werden - auch dort nur, wenn der Grundkörper K bereits unendlich ist.

Lemma 1.5.12: Sei K ein Körper und L/K eine Körpererweiterung.

1. Ist $\mathrm{char}(K) = 0$, so ist jedes Polynom $q \in K[x]$ und damit jedes algebraische Element $\alpha \in L$ separabel über K.
2. Ist $\mathrm{char}(K) = p \in \mathbb{N}$ prim und $q \in K[x]$ irreduzibel, so ist q genau dann inseparabel über K, wenn ein $r \in K[x]$ mit $q(x) = r(x^p)$ existiert, d. h. q ist von der Form $q = \sum_{k=0}^{n} a_k x^{kp}$ mit $a_k \in K$.
3. Ist $\mathrm{char}(K) = p \in \mathbb{N}$ prim, so ist ein algebraisches Element $\alpha \in L$ genau dann separabel, wenn $K(\alpha^p) = K(\alpha)$.
4. Ist $\mathrm{char}(K) = p \in \mathbb{N}$ prim und $\alpha \in L$ algebraisch, so existiert ein $n \in \mathbb{N}_0$, so dass α^{p^n} separabel über K ist.

Beweis:
1. Ist $\mathrm{char}(K) = 0$ so hat jedes nicht-konstante Polynom $q \in K[x]$ eine nicht-verschwindende Ableitung $q' \neq 0$, und die Behauptung folgt aus Lemma 1.5.8, 3.

2. Nach Lemma 1.5.8, 3. ist ein irreduzibles Polynom $q = \sum_{k=0}^{n} a_k x^k \in K[x]$ genau dann inseparabel, wenn $q' = \sum_{k=1}^{n} k a_k x^{k-1} = 0$, d. h. $ka_k = 0$ für alle $k \in \{1, ..., n\}$. Es folgt $a_k = 0$ für alle $k \in \mathbb{N}$ mit $p \nmid k$.

3. Ist $\alpha \in L$ separabel über K, so ist α auch separabel über $K(\alpha^p) \subset K(\alpha)$, denn $m_{\alpha,K(\alpha^p)} | m_{\alpha,K}$. Da α eine Nullstelle von $q = x^p - \alpha^p = (x-\alpha)^p$ ist, folgt $m_{\alpha,K(\alpha^p)} = x - \alpha$ und somit $\alpha \in K(\alpha^p)$ und $K(\alpha^p) = K(\alpha)$. Ist $\alpha \in L$ dagegen inseparabel, so existiert nach 2. ein $q \in K[x]$ mit $m_{\alpha,K} = q(x^p)$ und damit $q(\alpha^p) = 0$. Mit dem Gradsatz folgt $[K(\alpha) : K] = \deg(m_{\alpha,K}) > \deg(q) \geq [K(\alpha^p) : K]$ und damit $K(\alpha^p) \neq K(\alpha)$.

4. Induktion über $\deg_K(\alpha)$. Die Aussage ist klar für $\deg_K(\alpha) = [K(\alpha) : K] = 1$, denn dann folgt $\alpha \in K$ und α separabel. Sei die Aussage bewiesen für alle Elemente $\beta \in L$ mit $\deg_K(\beta) \leq m - 1$, und sei $\alpha \in L$ mit $\deg_K(\alpha) = m$. Ist α separabel über K, so wählt man $n = 0$. Ist α inseparabel über K, so gilt nach 3. $\deg_K(\alpha^p) < \deg_K(\alpha)$, und nach Induktionsvoraussetzung existiert ein $r \in \mathbb{N}_0$ mit $(\alpha^p)^{p^r} = \alpha^{p \cdot p^r} = \alpha^{p^{r+1}}$ separabel über K. $\square$

Mit Hilfe dieses Lemmas können wir nun insbesondere die vollkommenen Körper K charakterisieren, für die jeder algebraische Erweiterungskörper separabel ist. Dabei stellt sich heraus, dass es nur sehr wenige unvollkommene Körper geben kann. Insbesondere zeigt der folgende Satz, dass die Körper $\mathbb{R}, \mathbb{C}, \mathbb{Q}$ sowie alle endlichen Körper $\mathbb{F}_p$ mit $p \in \mathbb{N}$ prim vollkommen sind.

Satz 1.5.13:

1. Jeder Körper der Charakteristik 0 ist vollkommen.
2. Ein Körper K der Charakteristik $p \in \mathbb{N}$ prim ist vollkommen genau dann, wenn die Frobeniusabbildung $F_p : K \to K$, $\alpha \mapsto \alpha^p$ surjektiv ist.
3. Jeder endliche Körper ist vollkommen.

Beweis:
1. Dies folgt direkt aus Lemma 1.5.12, 1.

2. Sei die Frobeniusabbildung $F_p : K \to K$ surjektiv. Wäre K nicht vollkommen, so gäbe es eine algebraische Körpererweiterung mit einem inseparablen Element und somit ein inseparables, irreduzibles Polynom $q \in K[x]$. Nach Lemma 1.5.12, 2. würde dann ein Polynom $r = \sum_{k=0}^{n} a_k x^k \in K[x]$ mit $q(x) = r(x^p)$ existieren. Wegen der Surjektivität der Frobeniusabbildung gäbe es $b_k \in K$ mit $a_k = F_p(b_k) = b_k^p$ und somit

$$q(x) = r(x^p) = \sum_{k=0}^{n} a_k x^{kp} = \sum_{k=0}^{n} b_k^p (x^k)^p = \left(\sum_{k=0}^{n} b_k x^k \right)^p ,$$

was ein Widerspruch zur Irreduzibilität von q ist.

Sei nun umgekehrt K vollkommmen. Dann gilt für jedes Element $\alpha \in K$ und jede Nullstelle $\beta \in L$ des Polynoms $q = x^p - \alpha \in K[x]$ in einem Zerfällungskörper L von q die Identität

$q = x^p - \beta^p = (x-\beta)^p$. Hätte $q \in K[x]$ einen irreduziblen Faktor in $K[x]$ vom Grad > 1, so hätte dieser also eine mehrfache Nullstelle in L und somit wäre q inseparabel. Also ist jeder irreduzible Faktor von q in $K[x]$ linear, und somit besitzt q eine Nullstelle in K. Also existiert zu jedem $\alpha \in K$ ein $\beta \in K$ mit $\beta^p = \alpha$ und somit ist die Frobeniusabbildung surjektiv.

3. Dies folgt aus 2., da für jeden endlichen Körper K die Frobeniusabbildung $F_p : K \to K$ injektiv und damit auch surjektiv ist. □

Aus diesem Satz ergibt sich direkt, dass ein nicht vollkommener Körper K die Charakteristik $\text{char}(K) = p \in \mathbb{N}$, p prim, haben und ausserdem unendlich sein muss. Damit ist er insbesondere eine unendliche Körpererweiterung über seinem Primkörper $P(K) = \mathbb{F}_p$. Ein natürlicher Kandidat für eine solche unendliche Körpererweiterung über $\mathbb{F}_p$ ist der Quotientenkörper des Polynomrings $\mathbb{F}_p[x]$, und es zeigt sich, dass dieser tatsächlich nicht separabel ist. Diese Aussage gilt allgemeiner für den Körper der gebrochen rationalen Funktionen über beliebigen Körpern der Charakteristik p.

Beispiel 1.5.14: (**Ein nicht vollkommener Körper**)

Sei K ein Körper mit $\text{char}(K) = p \in \mathbb{N}$ und $L = Q(K[x])$ der Körper der rationalen Funktionen über K. Dann liegt das Element x nicht im Bild der Frobeniusabbildung $F_p : L \to L$, denn aus $x = (r/q)^p$ mit $r = \sum_{k=0}^{n} a_k x^k \in K[x]$, $q = \sum_{k=0}^{m} b_k x^k \in K[x]^*$ folgt

$$\sum_{k=0}^{m} b_k^p x^{pk+1} = x \left(\sum_{k=0}^{m} b_k x^k \right)^p = xq^p = r^p = \left(\sum_{k=0}^{n} a_k x^k \right)^p = \sum_{k=0}^{n} a_k^p x^{kp},$$

und ein Koeffizientenvergleich zeigt, dass alle Koeffizienten a_k^p, b_k^p verschwinden. Da aber die Frobeniusabbildung $F_p : K \to K$ injektiv ist, folgt $p = q = 0$, was ein Widerspruch ist. Also kann x nicht im Bild der Frobeniusabbildung liegen. Somit ist $F_p : L \to L$ nicht surjektiv und nach Satz 1.5.13 L nicht vollkommen.

Wir lernen nun einen zentralen Satz kennen, der uns zeigen wird, warum Restklassenkörper $K[x]/(f)$ mit $f \in K[x]$ irreduzibel eine so wichtige Rolle in der Körpertheorie spielen. Es wurde bereits gezeigt, dass jede primitive algebraische Körpererweiterung von dieser Form ist, und ebenso ist klar, dass eine transzendente Körpererweiterung wegen $[K[x]/(f) : K] = \deg(f) \in \mathbb{N}$ nie von dieser Form sein kann. Es stellt sich also die Frage, wie sich die *primitiven* algebraischen Körpererweiterungen innerhalb der endlichen algebraischen Körpererweiterungen charakterisieren lassen. Mit Hilfe des folgenden Satzes werden wir beweisen, dass jede endliche algebraische Körpererweiterung von Körpern der Charakteristik null oder endlichen Körpern $\mathbb{F}_p$ mit $p \in \mathbb{N}$ prim primitiv ist.

Satz 1.5.15: (**Satz vom primitiven Element**)

Sei L/K eine Körpererweiterung mit $L = K(\alpha, \delta_1, ..., \delta_n)$, α algebraisch über K und $\delta_1, ..., \delta_n$ separabel. Dann ist L/K primitiv.

Beweis:
1. Ist K ein endlicher Körper, so ist wegen $[L : K] = [K(\alpha, \delta_1, ..., \delta_n) : K] \in \mathbb{N}$ auch L endlich,

und somit ist die multiplikative Gruppe $(L^*, \cdot)$ nach Bemerkung 1.1.2, 5. zyklisch. Also existiert ein $\gamma \in L$ mit $L = K(\gamma)$.

2. Sei nun K unendlich. Dann reicht es, den Fall $n = 1$ zu betrachten, und mit einem Induktionsargument folgt dann die Behauptung für allgemeines $n \in \mathbb{N}$. Denn nach Lemma 1.2.15 gilt $K(\alpha, \delta_1, ..., \delta_n) = K(\alpha, \delta_1, ..., \delta_{n-1})(\delta_n)$. Ist die Aussage bereits für $n-1$ bewiesen, so folgt, dass $K(\alpha, \delta_1, ..., \delta_{n-1})$ primitiv ist, d. h. ein algebraisches Element $\gamma \in L$ mit $K(\alpha, \delta_1, ..., \delta_{n-1}) = K(\gamma)$ existiert und somit $L = K(\gamma, \delta_n)$. Mit der Aussage für $n = 1$ folgt dann die Behauptung.

3. Sei also $n = 1$, $L = K(\alpha, \beta)$ mit α algebraisch, β separabel und $m_{\alpha,K}$, $m_{\beta,K}$ die Minimalpolynome von $\alpha, \beta \in L$ über K. Sei M der Zerfällungskörper von $q = m_{\alpha,K} \cdot m_{\beta,K}$, $\alpha = \alpha_1, ..., \alpha_r$ die verschiedenen Nullstellen von $m_{\alpha,K}$ und $\beta = \beta_1, ..., \beta_s$ die verschiedenen Nullstellen von $m_{\beta,K}$ in L. Ist $s = 1$, so folgt $\deg(m_{\beta,K}) = 1$, da β eine einfache Nullstelle von $m_{\beta,K}$ ist, und somit $\beta \in K(\alpha)$. Sei also $s \geq 2$.

Existiert ein algebraisches Element $\gamma \in L$ mit $L = K(\alpha, \beta) = K(\gamma)$, so ist dieses oBdA von der Form $\gamma = \alpha + b\beta$ mit $b \in K^*$, denn $\{\alpha, \beta\}$ ist eine K-Basis von L und $K(c\gamma) = K(\gamma)$ für alle $c \in K^*$. Wir wählen nun $b \in K \setminus M_{\alpha,\beta}$ mit

$$M_{\alpha,\beta} = \{(\alpha_j - \alpha)(\beta - \beta_i)^{-1} : \, j = 1, ..., r, i = 2, ..., s\},$$

was wegen K unendlich möglich ist. Dann folgt $\gamma = \alpha + b\beta \notin \{\alpha_j + b\beta_i : j = 1, ..., r, i = 2, ..., s\}$.

4. Wir zeigen: $\alpha, \beta \in K(\gamma)$ und somit $L = K(\gamma)$. Dazu betrachten wir das verschobene Minimalpolynom $m_{\alpha,K}(\gamma - bx) \in K(\gamma)[x]$. Dann existiert ein normiertes Polynom $d \in \mathrm{ggT}(m_{\beta,K}, m_{\alpha,K}(\gamma - bx)) \in K(\gamma)[x]$ und Polynome $f, g \in K(\gamma)[x]$ mit

$$f m_{\beta,K} + g m_{\alpha,K}(\gamma - bx) = d.$$

Aus $m_{\beta,K}(\beta) = m_{\alpha,K}(\gamma - b\beta) = m_{\alpha,K}(\alpha) = 0$ folgt dann $d(\beta) = 0$. Ausserdem sind wegen $d | m_{\beta,K}$ alle Nullstellen von d in M in der Menge $\{\beta, \beta_2, ..., \beta_s\} \subset M$ enthalten. Da aber für $i \geq 2$ gilt $\gamma - b\beta_i \notin \{\alpha, \alpha_2, ..., \alpha_r\}$ und somit $m_{\alpha,K}(\gamma - b\beta_i) \neq 0$, folgt mit $d | m_{\alpha,K}(\gamma - bx)$ auch $d(\beta_i) \neq 0$ für alle $i \geq 2$. Also ist β die einzige Nullstelle von d in M. Da $m_{\alpha,K}$ und $m_{\beta,K}$ über M zerfallen, zerfällt auch d über M und somit $d = (x - \beta)^m$ für ein $m \in \mathbb{N}$. Da aber $d | m_{\beta,K} \Rightarrow (x - \beta)^m | m_{\beta,K}$ und β eine einfache Nullstelle von $m_{\beta,K}$ ist, folgt $m = 1$. Also gilt $d = x - \beta \in K(\gamma)[x]$ und wegen $d | m_{\alpha,K}(\gamma - bx), m_{\beta,K}$ folgt $\beta \in K(\gamma)$ und $\alpha = \gamma - b\beta \in K(\gamma)[x]$. □

Da jede endliche Körpererweiterung nach Korollar 1.3.6 algebraisch ist, erfüllt insbesondere jede endliche separable Körpererweiterungen die Voraussetzungen von Satz 1.5.15. Dies gilt insbesondere für endliche Körpererweiterungen über einem Körper der Charakteristik null oder über einem Körper $\mathbb{F}_p$ mit $p \in \mathbb{N}$ prim, denn solche Körpererweiterungen sind nach Lemma 1.5.12 und Satz 1.5.13 stets separabel.

Korollar 1.5.16:

1. Jede endliche separable Körpererweiterung ist primitiv.
2. Jede endliche Erweiterung eines Körpers der Charakteristik null ist primitiv.
3. Jede endliche Erweiterung eines Körpers $\mathbb{F}_p$, p prim, ist primitiv.

Über unendlichen Körpern der Charakteristik $p \in \mathbb{N}$ existieren aber auch endliche Körpererweiterungen, die nicht primitiv sind. Dies zeigt das folgende Beispiel.

Beispiel 1.5.17: Sei E ein Körper mit $\mathrm{char}(E) = p \in \mathbb{N}$, $L = Q(E[x,y])$ der Körper der gebrochen rationalen Funktionen über E in den Unbestimmten x, y und $K = Q(E[x^p, y^p]) \subset L$.

Dann ist $\{x^m y^n : m, n \in \{0, ..., p-1\}\}$ eine K-Basis von L und somit $[L : K] = p^2$. Andererseits ist aber für jedes $z \in L$ das Element z^p in K enthalten, denn $z = \frac{r}{s}$ mit $r, s \in E[x,y]$. Ist $r = \sum_{n,m=0}^{p-1} a_{mn} x^m y^n$ mit $a_{mn} \in E$, so folgt

$$r^p = \left(\sum_{n,m=0}^{p-1} a_{mn} x^m y^n \right)^p = \sum_{n,m=0}^{p-1} a_{mn}^p x^{pm} y^{pn} \in E[x^p, y^p],$$

und somit $z^p \in K$ für alle $z \in L$. Daraus ergibt sich $[K(z) : K] \leq p < [K : L]$ für jedes $z \in L$, und somit kann L/K nicht primitiv sein.

Ein weiterer wichtiger Aspekt des Satzes über das primitive Element ist, dass sein Beweis konstruktiv ist und daher genutzt werden kann, um ein primitives Element für eine gegebene endliche, separable Körpererweiterung L/K zu bestimmen. Sind nämlich ein algebraisches Element $\alpha \in L$ und ein separables Element β mit $L = K(\alpha, \beta)$ bekannt, so besagt der Beweis von Satz 1.5.15, dass für jedes $b \in K \setminus M_{\alpha,\beta}$ das Element $\gamma = \alpha + b\beta$ primitiv ist. Um ein primitives Element γ zu bestimmen, reicht es also, die Nullstellen der Minimalpolynome von α und β zu berechnen und ein Element $b \in K^* \setminus M_{\alpha,\beta}$ zu wählen.

Beispiel 1.5.18: Wir betrachten die Körpererweiterung $\mathbb{Q}(\sqrt[3]{2}, \sqrt{2})/\mathbb{Q}$. Das Minimalpolynom über $\mathbb{Q}$ von $\alpha = \sqrt[3]{2}$ ist $m_{\alpha,\mathbb{Q}} = x^3 - 2$ und hat die Nullstellen $\alpha_1 = \alpha$, $\alpha_2 = \sqrt[3]{2} e^{2\pi \mathrm{i}/3}$, $\alpha_3 = \sqrt[3]{2} e^{4\pi \mathrm{i}/3}$. Das Minimalpolynom über $\mathbb{Q}$ von $\beta = \sqrt{2}$ ist $m_{\beta,\mathbb{Q}} = x^2 - 2$ mit Nullstellen $\beta_1 = -\beta_2 = \sqrt{2}$. Also gilt:

$$M_{\alpha,\beta} = \{(\alpha_j - \alpha)(\beta - \beta_i)^{-1} : j = 1, 2, 3, i = 2\} = \left\{ 0, -\frac{\sqrt[3]{2}(e^{2\pi \mathrm{i}/3} - 1)}{2\sqrt{2}}, -\frac{\sqrt[3]{2}(e^{4\pi \mathrm{i}/3} - 1)}{2\sqrt{2}} \right\},$$

und für jedes $b \in \mathbb{Q}^* \setminus M_{\alpha,\beta}$ ist $\sqrt[3]{2} + b\sqrt{2}$ primitiv. Insbesondere ist also $\sqrt[3]{2} + \sqrt{2}$ primitiv.

Wie die über K algebraischen Elemente eines Erweiterungskörpers L bilden auch die separablen Elemente von L einen Zwischenkörper der Körpererweiterung L/K, der als separabler Abschluss bezeichnet wird. Der Grad dieses Zwischenkörpers über dem Grundkörper wird als Separabilititätsgrad bezeichnet und wird uns später eine zentrale Aussage über die Anzahl der K-Automorphismen der Körpererweiterung liefern.

Lemma 1.5.19: Sei L/K eine Körpererweiterung.

1. Ist $L = K(S)$ und sind alle $\alpha \in S$ separabel über K, so ist L separabel über K.
2. Der **separable Abschluss** von K in L

$$S(L/K) = \{\alpha \in L : \alpha \,\text{separabel über}\, K\}$$

ist ein Teilkörper von L. Die Körpererweiterung $S(L/K)/K$ ist separabel und ihr Grad wird als **Separabilitätsgrad** von L/K und mit $[L : K]_s := [S(L/K) : K]$ bezeichnet.

Beweis:
1.1 Offensichtlich reicht es, denn Fall $\text{char}(K) = p \in \mathbb{N}$ zu betrachten. Da nach Lemma 1.2.15 $K(S) = \bigcup_{T \subset S \text{ endlich}} K(T)$, kann man sich ausserdem auf endliche Mengen $S = \{s_1, ..., s_m\}$ beschränken. Sind $s_1, .., s_m \in L$ separabel über K, so existiert nach Satz 1.5.15 ein Element $\gamma \in L$ mit $L = K(S) = K(\gamma)$ und $[K(\gamma) : K] = n \in \mathbb{N}$. Zu zeigen ist, dass jedes $\alpha \in K(\gamma) = K(S)$ separabel ist.

1.2. Dazu beweisen wir eine Hilfsaussage: Es gilt $K(\gamma) = K(\gamma^p)$, also γ separabel.

Da $\{1, \ldots, \gamma^{n-1}\}$ eine K-Basis von L ist, läßt sich jedes Element $s_i \in S$, $i = 1, ..., m$, eindeutig schreiben als $s_i = \sum_{j=0}^{n-1} a_{ij}\gamma^j$ mit $a_{ij} \in K$. Mit der Identität $(a + b)^p = a^p + b^p$ für Körper der Charakteristik p (Frobeniusmonomorphismus) folgt $s_i^p = \sum_{j=0}^{n-1} a_{ij}^p \gamma^{pj}$, also $K(s_1^p, ..., s_m^p) \subset K(\gamma^p)$. Da die Elemente $s_i \in S$ separabel sind, folgt mit Lemma 1.5.12 die Identität $K(s_i^p) = K(s_i)$ und somit

$$K(\gamma) = K(s_1, ..., s_m) = K(s_1) \cdots K(s_m) = K(s_1^p) \cdots K(s_m^p) = K(s_1^p, ..., s_m^p) \subset K(\gamma^p) \subset K(\gamma).$$

1.3. Sei nun $\alpha \in K(\gamma) = K(S)$ mit $[K(\alpha) : K] = d$. Dann ist $\{1, \alpha, \ldots, \alpha^{d-1}\}$ eine K-Basis von $K(\alpha)$. Wir zeigen: die Menge $\{1, \alpha^p, \ldots \alpha^{p(d-1)}\}$ ist linear unabhängig über K. Dazu ergänzen wir $\{1, \alpha, \ldots, \alpha^{d-1}\}$ zu einer K-Basis $\{\beta_0, ..., \beta_{n-1}\}$ von $K(\gamma)$. Dann lässt sich jedes Element γ^m mit $m \in \{0, ..., n-1\}$ eindeutig schreiben als Linearkombination $\gamma^m = \sum_{j=0}^{n-1} b_{mj}\beta_n$ mit $b_{mj} \in K$ Mit dem Frobeniusmonomorphismus erhalten wir $\gamma^{mp} = \sum_{j=0}^{n-1} b_{mj}^p \beta_j^p$. Da $\{1, \gamma, ..., \gamma^{n-1}\}$ und nach 1.2. auch $\{1, \gamma^p, ..., \gamma^{p(n-1)}\}$ K-Basen von L sind, folgt, dass auch $\{\beta_0^p, ..., \beta_{n-1}^p\}$ den K-Vektorraum L erzeugt. Somit ist auch diese Menge und die Teilmenge $\{1, \alpha^p, ..., \alpha^{p(d-1)}\} \subset \{\beta_0^p, ..., \beta_{n-1}^p\}$ linear unabhängig. Daraus folgt $K(\alpha) = K(\alpha^p)$ und mit Lemma 1.5.12, 3. die Behauptung.

2. Nach 1. ist $K(S(L/K))$ ein seperabler Erweiterungskörper von K und somit ist $S(L/K) = K(S(L/K))$ ein Teilkörper von L. □

Offensichtlich stimmt für jede separable Körpererweiterung, insbesondere also für algebraische Körpererweiterungen über Körpern der Charakteristik null oder über Körpern $\mathbb{F}_p$, $p \in \mathbb{N}$ prim, der Separabilitätsgrad $[L : K]_s$ mit dem Grad $[L : K]$ der Körpererweiterung überein. Denn in diesem Fall ist der algebraische Abschluss $S(L/K) = L$. Allgemein folgt aus dem Gradsatz $[L : K] = [L : S(L/K)] \cdot [S(L/K) : K]$ und damit $[L : K]_s | [L : K]$.

Ein wichtiger Grund, sich mit dem Separabilitätsgrad zu beschäftigen, ist, dass sich damit die Zahl der K-Monomorphismen einer endlichen Körpererweiterung L/K in den algebraischen Abschluss von $\overline{K}$ bestimmen läßt und damit insbesondere die Zahl der K-Automorphismen von endlichen, normalen Körpererweiterungen.

Lemma 1.5.20: Sei L/K eine endliche Körpererweiterung und $\overline{K}$ ein algebraischer Abschluss von K. Dann gibt es genau $[L : K]_s$ verschiedene K-Monomorphismen $\phi : L \to \overline{K}$.

Beweis:
1. Wir zeigen: Jeder K-Monomorphismus $\sigma : S(L/K) \to \overline{K}$ Läßt sich zu einem K-Monomorphismus $\rho : L \to \overline{K}$ mit $\rho|_{S(L/K)} = \sigma$ fortsetzen, und jeder K-Monomorphismus $\tau : L \to \overline{K}$ ist durch seine Einschränkung $\tau|_{S(L/K)} : S(L/K) \to \overline{K}$ eindeutig bestimmt.

Die erste Aussage folgt direkt aus dem Fortsetzungssatz 1.4.16. Ist $\text{char}(K) = 0$, so gilt $S(L/K) = L$, und die zweite Aussage ist trivial. Sei also $\text{char}(K) = p$ und $\tau, \rho : L \to \overline{K}$ zwei K-Monomorphismen mit $\tau|_{S(L/K)} = \rho|_{S(L/K)}$. Nach Lemma 1.5.12, 4. existiert zu jedem $\alpha \in L$ ein $m \in \mathbb{N}_0$ mit α^{p^m} separabel und somit $\alpha^{p^m} \in S(L/K)$. Es folgt $\tau(\alpha)^{p^m} = \tau(\alpha^{p^m}) = \sigma(\alpha^{p^m}) = \sigma(\alpha)^{p^m}$. Mit der Identität $(a+b)^p = a^p + b^p$ in Körpern der Charakteristik p (Frobeniusmonomorphismus) folgt $(\sigma(\alpha) - \tau(\alpha))^{p^m} = 0$, also $\sigma(\alpha) = \tau(\alpha)$ für alle $\alpha \in L$.

2. Nach dem Satz vom primitiven Element 1.5.15 existiert ein $\gamma \in S(L/K)$ mit $S(L/K) = K(\gamma)$. Das Minimalpolynom $m_{\gamma,K} \in K[x]$ ist irreduzibel, separabel und vom Grad $n := [K(\gamma) : K] = [L : K]_s$, hat also genau n Nullstellen $\alpha_1, ..., \alpha_n \in \overline{K}$. Nach dem Fortsetzungssatz für primitive Körpererweiterungen (Satz 1.4.13) existiert zu jedem $i \in \{1, ..., n\}$ genau ein K-Monomorphismus $\tau_i : S(L/K) \to \overline{K}$ mit $\tau(\gamma) = \alpha_i$. Mit 1. folgt die Behauptung. □

Ein wichtiger Spezialfall dieses Satzes ergibt sich, wenn man die Gruppe $\Gamma(L/K)$ der K-Automorphismen einer normalen Körpererweiterung L/K betrachtet. In diesem Fall stimmen die algebraischen Abschlüsse von L und K überein ($\overline{L} = \overline{K}$), und nach Satz 1.5.1, 2. sind K-Monomorphismen $L \to \overline{L}$ nichts anderes als K-Automorphismen $L \to L$, denn für das Bild jedes K-Monomorphismus $\phi : L \to \overline{L}$ gilt $\phi(L) \subset L$. Also sind die Voraussetzungen von Lemma 1.5.20 erfüllt, und wir erhalten ein zentrales Korollar über die Anzahl der K-Automorphismen von L/K.

Korollar 1.5.21: Für jede endliche Körpererweiterung L/K gilt für die Anzahl $|\Gamma(L/K)|$ der K-Automorphismen von L:

1. $|\Gamma(L/K)| \leq [L : K]_s \leq [L : K]$.
2. $|\Gamma(L/K)| = [L : K]_s$ genau dann, wenn L/K normal ist.
3. $|\Gamma(L/K)| = [L : K]$ genau dann, wenn L/K normal und separabel ist.

1.6 Endliche Körper

Mit Hilfe der bisher erzielten Ergebnisse über algebraische Körpererweiterungen werden wir in diesem Abschnitt die endlichen Körper und deren Zwischenkörper vollständig klassifizieren und auch deren Automorphismengruppen bestimmen. Wir erinnern dazu zunächst an die bisher in der Vorlesung und in den Übungen bewiesenen Aussagen über endliche Körper.

Bemerkung 1.6.1: Sei K ein endlicher Körper mit $|K|$ Elementen. Dann gilt:

1. **Multiplikative Gruppe:** $(K^*, \cdot)$ ist nach Bemerkung 1.1.2, 5. eine zyklische Gruppe der Ordnung $|K| - 1$.
2. **Charakteristik und Primkörper:** es gilt $\text{char}(K) = p$ mit $p \in \mathbb{N}$ prim und $P(K) \cong \mathbb{F}_p$. Da jeder Körper eine Körpererweiterung über seinem Primkörper ist, ist $K/P(K)$ eine endliche Körpererweiterung.
3. **Anzahl der Elemente:** Ist $[K : P(K)] = n$, so hat K genau p^n Elemente, und es gilt $k^{p^n} = k$ für alle $k \in K$.

   Denn aus $[K : P(K)] = n$ folgt, dass K ein n-dimensionaler Vektorraum über $P(K) \cong \mathbb{F}_p$ ist und damit genau p^n Elemente enthält. Nach 1. ist damit $(K^*, \cdot)$ eine zyklische Gruppe der Ordnung $p^n - 1$, und mit dem kleinen Satz von Fermat folgt $k^{p^n - 1} = 1$ für alle $k \in K$.

4. **Vollkommenheit:** K ist vollkommen (Satz 1.5.13).

Nach Bemerkung 1.6.1, 3. muss also für einen endlichen Körper K die Anzahl der Elemente von K eine Primpotenz sein. Umgekehrt ergibt sich die Frage, ob zu jeder Primpotenz p^n ein endlicher Körper K mit p^n Elementen existiert und, wenn ja, wie viele nicht isomorphe solche Körper existieren. Die Antwort auf diese Frage entspricht einer vollständigen Klassifikation aller endlichen Körper. Um eine solche Klassifikation zu erhalten, nutzen wir aus, dass nach Bemerkung 1.6.1, 3. jedes Element eines endlichen Körpers mit p^n Elementen eine Nullstelle des Polynoms $x^{p^n} - x \in \mathbb{F}_p[x]$ ist. Da K p^n Elemente hat, hat das Polynom $x^{p^n} - x$ genau p^n verschiedene Nullstellen in K und zerfällt somit in Linearfaktoren der Vielfachheit eins. Dies legt es nahe, einen Körper mit p^n Elementen als Zerfällungskörper eines solchen Polynoms zu konstruieren.

Satz 1.6.2: (**Klassifikation endlicher Körper**)

Zu jeder Primzahl $p \in \mathbb{N}$ und jedem $n \in \mathbb{N}$ existiert (bis auf Isomorphie) genau ein Körper mit p^n Elementen, nämlich der Zerfällungskörper von $x^{p^n} - x \in \mathbb{F}_p[x]$ über $\mathbb{F}_p[x]$. Wir bezeichnen diesen mit $\mathbb{F}_{p^n}$.

Beweis:
1. **Existenz:** Sei K der Zerfällungskörper des Polynoms $f = x^{p^n} - x \in \mathbb{F}_p[x]$. Offensichtlich gilt nach Bemerkung 1.6.1, 3. für die Nullstellenmenge

$$N = \{\alpha \in K : f(\alpha) = 0\} = \{\alpha \in K : \alpha^{p^n} = \alpha\}$$

die Inklusion $\mathbb{F}_p \subset N \subset K$. Ausserdem folgt mit der Identität $(a+b)^p = a^p + b^p$ in Körpern der Charakteristik p (Frobeniusmonomorphismus)

$$(a-b)^{p^n} = a^{p^n} - b^{p^n} = a - b, \qquad (ab^{-1})^{p^n} = a^{p^n} b^{-p^n} = ab^{-1} \qquad \forall a, b \in N.$$

Also ist die Nullstellenmenge N ein Teilkörper von K, der $\mathbb{F}_p$ und alle Nullstellen von f in K enthält und somit der Zerfällungskörper von f über $\mathbb{F}_p$. Mit der Eindeutigkeit von Zerfällungskörpern folgt $K = N$. Es reicht also zu zeigen, dass f genau p^n verschiedene Nullstellen in K besitzt. Da $\deg(f) = p^n$ und f über K zerfällt, ist dies der Fall genau dann, wenn f keine mehrfachen Nullstellen in K besitzt. Dies folgt mit Lemma 1.5.8 aus der Identität $f' = p^n x^{p^n - 1} - 1 = -1 \neq 0$.

2. **Eindeutigkeit:** Ist umgekehrt K' ein endlicher Körper mit p^n Elementen, so ist ist nach Bemerkung 1.6.1 $P(K') \cong \mathbb{F}_p$ und K' ein Zerfällungskörper von $f = x^{p^n} - x \in P(K')[x]$. Da $P(K') \cong \mathbb{F}_p$ folgt mit Satz 1.4.14 $K' \cong K$. □

Beispiel 1.6.3:

1. Der Körper $\mathbb{F}_4$ ist der Zerfällungskörper von $f = x^4 - x$ über $\mathbb{F}_2$. Wegen $x^4 - x = x(x^3 - 1) = x(x - \overline{1})(\overline{1} + x + x^2)$ und der Irreduzibilität von $\overline{1} + x + x^2$ über $\mathbb{F}_2$ folgt, dass $g = \overline{1} + x + x^2$ das Minimalpolynom des primitiven Elements von $\mathbb{F}_4/\mathbb{F}_2$ sein muss. Also gilt $\mathbb{F}_4 \cong \mathbb{F}_2[x]/(\overline{1} + x + x^2)$.

2. Der Körper $\mathbb{F}_9$ ist Zerfällungskörper von

$$f = x^9 - x = x(x - \overline{1})(x + \overline{1})(x^2 + \overline{1})(x^2 + x - \overline{1})(x^2 - x - \overline{1}).$$

Die Polynome $x^2+\overline{1}, x^2+x-\overline{1}, x^2-x-\overline{1}$ sind irreduzibel in $\mathbb{F}_3[x]$, da sie keine Nullstellen in $\mathbb{F}_3$ besitzen. Offensichtlich entsteht $\mathbb{F}_9$ aus $\mathbb{F}_3$ durch Adjunktion der Nullstellen dieser Polynome. Diese aber explizit zu berechnen, ist unnötig.

Denn wegen $9 = 3^2$ gilt $\mathbb{F}_9/\mathbb{F}_3 = 2$ und somit ist $\mathbb{F}_9/\mathbb{F}_3$ primitiv mit einem quadratischen primitiven Element. Dieses muss Nullstelle eines über $\mathbb{F}_3$ irreduziblen quadratischen Polynoms q sein. Umgekehrt ist jede Nullstelle α eines solchen Polynoms ein primitives Element, denn es gilt $[\mathbb{F}_3(\alpha) : \mathbb{F}_3] = \deg(q) = 2 = [\mathbb{F}_9 : \mathbb{F}_3]$. Also folgt

$$\mathbb{F}_9 = \mathbb{F}_3[x]/(x^2 + \overline{1}) \cong \mathbb{F}_3[x]/(x^2 + x - \overline{1}) \cong \mathbb{F}_3[x]/(x^2 - x - \overline{1}).$$

Satz 1.6.2 liefert nicht nur eine vollständige Klassifikation endlicher Körper, sondern erlaubt es einem auch, die Teilkörper solcher endlichen Körper vollständig zu klassifizieren. Die Idee ist es dabei, mit dem Primkörper des endlichen Körpers zu arbeiten und dessen Teilkörper als Körpererweiterungen über dem Primkörper aufzufassen. Dann läßt sich Satz 1.6.2 auch auf die Teilkörper anwenden, und der Gradsatz liefert eine Klassifikation der Teilkörper.

Lemma 1.6.4: (**Teilkörper endlicher Körper**)

Zu jedem Teiler $d \in \mathbb{N}$ von $n \in \mathbb{N}$ besitzt der Körper $\mathbb{F}_{p^n}$ genau einen Teilkörper mit p^d Elementen, und jeder Teilkörper von $\mathbb{F}_{p^n}$ ist von dieser Form.

Beweis:
1. **Eindeutigkeit:** Für $\mathbb{F}_{p^n}$ gilt $P(\mathbb{F}_{p^n}) \cong \mathbb{F}_p$. Da jeder Teilkörper $E \subset \mathbb{F}_{p^n}$ den Primkörper $P(\mathbb{F}_{p^n}) \cong \mathbb{F}_p$ als Teilkörper enthält, folgt mit dem Gradsatz

$$n = [\mathbb{F}_{p^n} : P(\mathbb{F}_{p^n})] = [\mathbb{F}_{p^n} : E] \cdot [E : P(\mathbb{F}_{p^n})],$$

also $d := [E : P(\mathbb{F}_{p^n}])|n$. Nach Satz 1.6.2 ist damit ist E ein Körper mit p^d Elementen, und die Elemente von E sind Nullstellen von $g = x^{p^d} - x$. Da dieses Polynom maximal p^d Nullstellen in $\mathbb{F}_{p^n}$ hat, ist E der einzige Teilkörper von $\mathbb{F}_{p^n}$ mit p^d Elementen.

2. **Existenz:** Gilt $d|n$, so existiert ein $a \in \mathbb{N}$ mit $n = ad$, und mit der Formel für eine geometrische Summe

$$(x-1)\sum_{k=0}^{n} x^k = \sum_{k=1}^{n+1} x^k - \sum_{k=0}^{n} x^k = x^{n+1} - 1$$

folgt $p^n - 1 = p^{ad} - 1 = (p^d - 1)\sum_{k=0}^{a-1} p^{kd} =: (p^d - 1)m$, also $(p^d - 1)|(p^n - 1)$. Wiederum mit der Formel für die geometrische Summe erhält man $x^{(p^d-1)m} - 1 = (x^{p^d-1} - 1)\sum_{k=0}^{m-1} x^{k(p^d-1)}$. Also ist $g = x^{p^d} - x = x(x^{p^d-1} - 1)$ ein Teiler von $f = x^{p^n} - x = x(x^{p^n-1} - 1)$. Da f über $\mathbb{F}_{p^n}$ zerfällt, zerfällt auch g über $\mathbb{F}_{p^n}$, und der Zerfällungskörper von g ist nach Satz 1.6.2 ein Teilkörper von $\mathbb{F}_{p^n}$ mit p^d Elementen. □

Beispiel 1.6.5:

1. Der Körper $\mathbb{F}_8$ hat keinen Teilkörper mit vier Elementen. Denn $8 = 2^3$, $4 = 2^2$ und $2 \nmid 3$.

2. Der Körper $\mathbb{F}_{p^{12}}$ für $p \in \mathbb{N}$ prim enthält die echten Teilkörper $\mathbb{F}_p$, $\mathbb{F}_{p^2}$, $\mathbb{F}_{p^3}$, $\mathbb{F}_{p^4}$, $\mathbb{F}_{p^6}$. Der Teilkörper $\mathbb{F}_{p^6}$ enthält die Teilkörper $\mathbb{F}_p, \mathbb{F}_{p^2}$ und $\mathbb{F}_{p^3}$, der Teilkörper $\mathbb{F}_{p^4}$ die Teilkörper $\mathbb{F}_p, \mathbb{F}_{p^2}$ und die Teilkörper $\mathbb{F}_{p^2}$, $\mathbb{F}_{p^3}$ enthalten $\mathbb{F}_p$. Der Teilkörper $\mathbb{F}_{p^k}$ mit $k|12$ ist dabei die Teilmenge $\mathbb{F}_{p^k} = \{\alpha \in \mathbb{F}_{p^{12}} : \alpha^{p^k} = \alpha\}$.

Insbesondere ergibt sich aus Satz 1.6.2 und Lemma 1.6.4 die Aussage, dass jede endliche Erweiterung L/K eines endlichen Körpers bereits normal ist, denn sie ist Zerfällungskörper eines Polynoms $x^q - x$. Da nach Satz 1.5.13 jeder endliche Körper K vollkommen ist, ist L/K ausserdem separabel.

Korollar 1.6.6:
Jede endliche Erweiterung L/K eines endlichen Körpers K ist separabel und normal.

Dieses Korollar ermöglicht es uns insbesondere, die Gruppe $\Gamma(L/K)$ der K-Automorphismen von solchen endlichen Körpererweiterungen L/K zu bestimmen. Es stellt sich heraus, dass diese Gruppe zyklisch ist und von dem K-Monomorphismus $\phi : L \to L$, $\alpha \mapsto \alpha^{|K|}$ erzeugt wird.

Lemma 1.6.7: Sei L/K eine endliche Körpererweiterung eines endlichen Körpers K. Dann ist die Gruppe $\Gamma(L/K)$ der K-Automorphismen von L eine zyklische Gruppe der Ordnung $[L : K]$ und wird erzeugt von $\phi : L \to L$, $\alpha \mapsto \alpha^{|K|}$.

Beweis:
1. Nach Bemerkung 1.4.12 bilden die K-Automorphismen von L/K eine Gruppe $\Gamma(L/K)$. Da L/K nach Korollar 1.6.6 normal und separabel ist, besitzt L/K nach Korollar 1.5.21 genau $[L : K]$ verschiedene K-Automorphismen, also $|\Gamma(L/K)| = [L : K]$. Zu zeigen bleibt, dass $\Gamma(L/K)$ zyklisch ist und von dem K-Automorphismus $\phi : L \to L$, $\alpha \mapsto \alpha^{|K|}$ erzeugt wird.

2. Da $|K| = p^m$ mit $p = \mathrm{char}(K)$ und $m = [K : P(K)]$, gilt $\phi = (F_p)^m$, wobei $F_p : L \to L$, $\alpha \mapsto \alpha^p$ den Frobeniusmonomorphismus bezeichnet. Also ist ϕ ein Körpermonomorphismus und nach Bemerkung 1.6.1, 3 gilt $\phi(\alpha) = \alpha^{|K|} = \alpha$ für alle $\alpha \in K$. Damit ist ϕ ein K-Automorphismus und erzeugt eine Untergruppe $\langle\phi\rangle \subset \Gamma(L/K)$.

3. Wäre $|\langle\phi\rangle| < [L : K] =: n$, so würde ein $k \in \mathbb{N}$, $k < n$ mit $\phi^k = \mathrm{id}_L$ existieren, und das Polynom $x^{p^{mk}} - x$ hätte $|L|$ verschiedene Nullstellen in L - ein Widerspruch zu Satz 1.6.2, denn L ist der Zerfällungskörper von $x^{|L|} - x = x^{p^{mn}} - x$ Also muss $k \geq n$ und damit $\Gamma(L/K) = \langle\phi\rangle$ gelten. □

Insbesondere läßt sich mit Hilfe dieses Lemmas die Automorphismengruppe eines endlichen Körpers K bestimmen. Denn jeder endliche Körper K läßt sich als eine endliche Körpererweiterung seines Primkörpers $P(K) \cong \mathbb{F}_p$, $p \in \mathbb{N}$ prim, auffassen. Da jeder Körperautomorphismus von K den Primkörper erhält, sind Automorphismen $K \to K$ stets auch $P(K)$-Automorphismen von K und können mit Lemma 1.6.7 klassifiziert werden..

Korollar 1.6.8: Die Gruppe der Automorphismen des endlichen Körpers $\mathbb{F}_{p^n}$ ist eine zyklische Gruppe der Ordnung n und wird von dem Frobeniusautomorphismus $F_p : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$, $\alpha \mapsto \alpha^p$ erzeugt.

Beweis:
Der endliche Körper $\mathbb{F}_{p^n}$ ist eine Körpererweiterung vom Grad n über seinem Primkörper $\mathbb{F}_p$. Jeder Körperautomorphismus $\phi : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ läßt den Primkörper invariant, denn die Fixpunktmenge $\{\alpha \in \mathbb{F}_{p^n} : \phi(\alpha) = \alpha\}$ ist ein Teilkörper von $\mathbb{F}_{p^n}$ und enthält somit den Primkörper $\mathbb{F}_p$. Also ist jeder Körperautomorphismus $\phi : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ ein $\mathbb{F}_p$-Automorphismus. Mit Lemma 1.6.7 folgt die Behauptung. □

1.7 Übungen zu Kapitel 1

Aufgabe 1: Untersuchen Sie die folgenden Polynome auf Reduzibilität in $K[x]$.

(a) $3x^3 + 5x - 10$ für $K = \mathbb{Q}$,
(b) $x^4 + x^3 - x - 1$ für $K = \mathbb{Q}$,
(c) $x^2 + 3x - 1$ für $K = \mathbb{Q}, \mathbb{R}$,
(d) $x^2 + 3x - 1$ für $K = \mathbb{F}_2, \mathbb{F}_3$,
(e) $2x^7 + 5x^2 + 5x + 2$ für $K = \mathbb{Q}, \mathbb{F}_{17}$,
(f) $x^4 + 3x^3 + 9$ für $K = \mathbb{Q}$,
(g) $x^{14} + x^3 + x^2 + 4$ für $K = \mathbb{F}_5$.

Aufgabe 2: Wir betrachten das Polynom $f = x^2 + 2x + 5 \in \mathbb{Q}[x]$.

(a) Begründen Sie zunächst, dass dieses Polynom irreduzibel über $\mathbb{Q}$ und $\mathbb{R}$ ist.
(b) Geben Sie eine Basis des Restklassenkörpers $\mathbb{Q}[x]/(f)$ als Vektorraum über $\mathbb{Q}$ an.
(c) Berechnen Sie die multiplikativen Inversen der Elemente $\overline{x+1}$, $\overline{x-3}$ in $\mathbb{Q}[x]/(f)$.

Aufgabe 3: Wir betrachten den Restklassenring $K = \mathbb{Q}[x]/(f)$ mit $f = x^3 + 2x^2 - 2x + 3$ und bezeichnen die Restklasse eines Polynoms $p \in \mathbb{Q}[x]$ in K mit $\overline{p}$.

(a) Begründen Sie, dass dieser Restklassenring eine Körpererweiterung von $\mathbb{Q}$ ist, bestimmen Sie deren Grad und geben Sie eine $\mathbb{Q}$-Basis von K an.
(b) Schreiben Sie die Restklassen der folgenden Polynome als Linearkombination der Basisvektoren

$$f = x^3 + 2x^2 - 2x + 5, \qquad g = x^4 + 2x^3 - 2x^2, \qquad h = x^3 + 4x^2, \qquad k = x^6.$$

(c) Geben Sie die multiplikativen Inversen der Elemente $\overline{x}$, $\overline{x^2}$ als Linearkombination der Basiselemente an.

Aufgabe 4: Geben Sie für $n \in N$, $n \geq 2$ ein irreduzibles Polynom in $\mathbb{Q}[x]$ vom Grad n an.

Aufgabe 5: Wir betrachten den Polynomring $\mathbb{Q}[x]$ und das von den Polynomen

$$f = x^3 - x^2 \qquad g = x^5 + x^4 + 6x^3 + 6x^2 + 10x + 10$$

erzeugte Ideal in $\mathbb{Q}[x]$. Geben Sie ein Polynom $h \in \mathbb{Q}[x]$ an, das dieses Ideal erzeugt.

Aufgabe 6: Berechnen Sie den größten gemeinsamen Teiler der Polynome

$$f = 2x^5 + 10x^4 + x^3 - 14x^2 - x + 2, \qquad g = 2x^5 + 6x^4 - x^3 - 8x^2 + 1$$

in $\mathbb{Q}[x]$ und geben Sie Polynome $a, b \in \mathbb{Q}[x]$ an mit $\mathrm{ggT}(f, g) = af + bg$.

Aufgabe 7:

(a) Zeigen Sie, dass das Polynom $f = x^3 + 5x + 1$ genau eine Nullstelle $\alpha \in \mathbb{R}$ besitzt und dass diese nicht in $\mathbb{Q}$ enthalten ist.
(b) Geben Sie ein Polynom $q \in \mathbb{Q}[x]$ an, so dass

$$\frac{1-\alpha}{1+\alpha} = q(\alpha).$$

Aufgabe 8:

(a) Geben Sie die Polardarstellung $z = re^{\mathrm{i}\phi}$ mit $r \in (0, \infty)$, $\phi \in [0, 2\pi)$ für die folgenden komplexen Zahlen an und zeichnen Sie diese:

$$z_1 = 5\mathrm{i}, \qquad z_2 = 3 - 3\mathrm{i}, \qquad z_3 = \sqrt{3} + \mathrm{i}, \qquad z_4 = 2 - 2\mathrm{i}\sqrt{3}.$$

(b) Berechnen Sie z_k^{10}, $k = 1, 2, 3, 4$. Geben Sie die Lösung in der Form $a + \mathrm{i}b$ mit $a, b \in \mathbb{R}$ an.
(c) Schreiben Sie die folgenden komplexen Zahlen als $a + \mathrm{i}b$ mit $a, b \in \mathbb{R}$

$$w_1 = \exp(c + \mathrm{i}d),\ c, d \in \mathbb{R}, \qquad w_2 = -5e^{\mathrm{i}\pi}, \qquad w_3 = 3e^{5\pi\mathrm{i}/6}, \qquad w_4 = -e^{2\pi\mathrm{i}/3}.$$

(d) Bestimmen Sie alle komplexen Lösungen der folgenden Gleichung und zeichnen Sie diese:

$$(z - a - \mathrm{i}b)^n = c \qquad \text{für} \quad a, b, c \in \mathbb{R}, c \geq 0, n \in \mathbb{N}.$$

Aufgabe 9:

(a) Konstruieren Sie einen Körper $\mathbb{F}_9$ mit 9 Elementen.
(b) Untersuchen Sie das Polynom $p = x^3 + x^2 + 2$ auf Reduzibilität in $\mathbb{F}_9$.

Aufgabe 10: Sei $\phi : K \to K$ ein Körperautomorphismus eines Körpers K.

(a) Zeigen Sie, dass $F = \{a \in K : \phi(a) = a\}$ ein Teilkörper von K ist.
(b) Zeigen Sie, dass $\phi(a) = a$ für alle Elemente $a \in P(K)$, wobei $P(K)$ den Primkörper von K bezeichnet.

Aufgabe 11: Bestimmen Sie die Minimalpolynome der angegebenen Elemente $a \in L$ über den angegebenen Grundkörpern K und den Grad der Körpererweiterung L/K:

(a) $L = \mathbb{Q}[x]/(x^5 - 20x + 5)$, $K = \mathbb{Q}$, $a = 3, \overline{x}^3$.
(b) $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, $K = \mathbb{Q}(\sqrt{2})$, $a = \sqrt{3}$.
(c) $L = \mathbb{C}$, $K = \mathbb{Q}$, $a = \sqrt{3} + \mathrm{i}$
(d) $L = \mathbb{C}$, $K = \mathbb{Q}$, $a = e^{\mathrm{i}\pi/p}$ mit $p \in N$ prim.

Aufgabe 12: Zeigen Sie: Ist K ein Körper der Charakteristik $\mathrm{char}(K) \neq 2$ und L/K eine Körpererweiterung, so sind äquivalent:

(i) L/K ist eine quadratische Körpererweiterung.
(ii) L entsteht aus K durch Adjunktion einer Quadratwurzel, d. h. es existiert ein $\alpha \in L \setminus K$ mit $\alpha^2 \in K$ und $L = K(\alpha)$.

Aufgabe 13: Sei L/K eine Körpererweiterung, $a, b \in L^*$ und $n, m \in N$ teilerfremd mit $a^n, b^m \in K$.

(a) Beweisen Sie: $K(a, b) = K(ab)$.
(b) Zeigen Sie durch Angabe eines Gegenbeispiels, dass die Voraussetzung $\mathrm{ggT}(n, m) = 1$ notwendig ist.

Aufgabe 14: Sei L/K eine Körpererweiterung und $\alpha \in L$ transzendent über K. Zeigen Sie, dass dann gilt $K(\alpha) \cong Q(K[x])$.

Aufgabe 15: Sei L ein Körper und $P(L)$ sein Primkörper. Zeigen Sie:

(i) $\text{char}(L) = 0 \quad \Leftrightarrow \quad P(L) \cong \mathbb{Q}$.
(ii) $\text{char}(L) = p,\ p \in \mathbb{N}\,\text{prim} \quad \Leftrightarrow \quad P(L) \cong \mathbb{F}_p$

Aufgabe 16: Sei K ein endlicher Körper und $p = \text{char}(K)$. Zeigen Sie:

(a) $K/\mathbb{F}_p$ ist eine endliche Körpererweiterung.
(b) Ist $[K : \mathbb{F}_p] = n$, so hat K p^n Elemente und $k^{p^n} = k$ für alle $k \in K$.

Aufgabe 17: (**Transitivität der Eigenschaft "algebraisch"**)
Sei $K \subset E \subset L$ ein Körperturm, so dass E/K algebraisch ist. Beweisen Sie:

(a) Ist $\alpha \in L$ algebraisch über E, so ist α auch algebraisch über K.
(b) Ist L/E algebraisch, so ist auch L/K algebraisch.

Aufgabe 18: (Charakterisierung algebraisch abgeschlossener Körper)
Sei K ein Körper. Beweisen Sie, dass die folgenden Aussagen äquivalent sind:

(i) K ist algebraisch abgeschlossen.
(ii) Jedes Polynom aus $K[x]$ zerfällt in Linearfaktoren.
(iii) Jedes irreduzible Polynom in $K[x]$ hat Grad 1.
(iv) Es gibt keinen über K algebraischen echten Erweiterungskörper $K \subsetneq E$.
(v) Es gibt keine echte Körpererweiterung L/K mit $[L : K] \in \mathbb{N}$, $[L : K] \geq 2$.

Aufgabe 19: Beweisen Sie, dass der algebraische Abschluss des endlichen Körpers $\mathbb{F}_p$ mit $p \in \mathbb{N}$ prim unendlich ist.

Aufgabe 20: Sei L der Zerfällungskörper eines Polynoms $p \in K[x]$ über K.

(a) Beweisen Sie, dass $[L : K]$ ist ein Teiler von $\deg(p)!$ ist.
(b) Geben Sie ein Beispiel mit $\deg(p) \geq 3$ und $[L : K] = \deg(p)!$ an.
(c) Geben Sie ein Beispiel mit $\deg(p) < [L : K] < \deg(p)!$ an.

Aufgabe 21: Beweisen Sie: Zu jeder endlichen Körpererweiterung E/K existiert eine eine endliche Körpererweiterung L/E, so dass L/K normal ist.

Aufgabe 22: Bestimmen Sie die Gruppe der K-Automorphismen von L/K für $K = \mathbb{Q}$, $L = \mathbb{Q}[x]/(x^2 + x + 1)$.

Aufgabe 23: Untersuchen Sie, ob die folgenden Körpererweiterungen normal sind:

(a) $\mathbb{Q}(\mathrm{i}\sqrt{3})/\mathbb{Q}$,
(b) $\mathbb{Q}((1+\mathrm{i})\sqrt[4]{3})/\mathbb{Q}(\mathrm{i}\sqrt{3})$,
(c) $\mathbb{Q}((1+\mathrm{i})\sqrt[4]{3})/\mathbb{Q}$,
(d) $\mathbb{Q}(\sqrt{2+\sqrt{2}})/\mathbb{Q}$.

Aufgabe 24: Sei $\overline{K}$ ein algebraischer Abschluss des Körpers K, $E = Q(K[x])$ und $L = Q(\overline{K}[x])$ die Körper der gebrochen rationalen Funktionen über K und $\overline{K}$. Zeigen Sie, dass die Körpererweiterung L/E normal ist.

Aufgabe 25: Untersuchen Sie, ob die folgenden Polynome aus $K[x]$ mehrfache Nullstellen in Erweiterungskörpern L von K besitzen können und geben Sie deren Vielfachheit an:

(a) $p = x^3 + \overline{1}$, $K = \mathbb{F}_3$

(b) $q = x^4 - 5x^3 + 6x^2 + 4x - 8$, $K = \mathbb{Q}$
(c) $r = x^5 + 5x + 5$, $K = \mathbb{Q}$
(d) $s = x^4 + 3x^3 - 17x^2 + 9x - 5$, $K = \mathbb{Q}$

Aufgabe 26: Sei K ein Körper mit $\mathrm{char}(K) = 0$, $f \in K[x]$ nicht-konstant und L ein Erweiterungskörper von K, in dem f zerfällt:

$$f = c(x - \alpha_1)^{k_1} \cdots (x - \alpha_n)^{k_n}$$

mit $c, \alpha_1, ..., \alpha_n \in L$, $k_1, ..., k_n \in \mathbb{N}$ und $\alpha_i \neq \alpha_j$ für $i \neq j$. Zeigen Sie, dass das Polynom $q = (x - \alpha_1) \cdots (x - \alpha_n)$ in $K[x]$ liegt.

Aufgabe 27: Zeigen Sie, dass eine quadratische Körpererweiterung L/K genau dann inseparabel ist, wenn $\mathrm{char}(K) = 2$ und ein $\alpha \in L \setminus K$ mit $\alpha^2 \in K$ existiert.

Aufgabe 28: Zeigen Sie: sind L/E und E/K separable Körpererweiterungen, so ist auch L/K separabel.

Aufgabe 29: Sei L/K eine algebraische Körpererweiterung. Zeigen Sie:

(a) Ist K vollkommen, so ist auch L vollkommen.
(b) Ist L vollkommen und separabel über K, so ist auch K vollkommen.
(c) Die Voraussetzung der Separabilität von L/K ist notwendig.

Aufgabe 30: Sei K ein Körper, $K[x, y]$ der Polynomring über K in den zwei Variablen x, y und $Q(R)$ bezeichne den Quotientenkörper eines Integritätsbereichs R.

Untersuchen Sie, ob die Körpererweiterung $Q(K[x, y])/Q(K[x + y, xy])$ primitiv ist und geben Sie gegebenenfalls ein primitives Element an.

Aufgabe 31: Eine algebraische Körpererweiterung L/K heißt **rein inseparabel**, wenn jedes $\alpha \in L \setminus K$ inseparabel über K ist. Zeigen Sie:

(a) Für jede algebraische Körpererweiterung L/K ist $L/S(L/K)$ rein inseparabel.
(b) Ist L/K rein inseparabel, so existiert zu jedem Element $\alpha \in L$ ein $n \in \mathbb{N}_0$ mit $\alpha^{p^n} \in K$.
(c) Ist L/K rein inseparabel, so ist L/K normal.
(d) Ist L/K endlich und rein inseparabel, so gilt

$$\Gamma(L/K) = \{\sigma \in \mathrm{Aut}(L) : \sigma|_K = \mathrm{id}_K\} = \{\mathrm{id}_L\}.$$

Aufgabe 32: Untersuchen Sie, ob die folgenden Körpererweiterungen primitiv sind, und geben Sie in diesem Fall ein primitives Element an:

(a) $K(\alpha, \beta)/K$ mit β inseparabel und α separabel, K unendlich.
(b) $\mathbb{Q}(\sqrt{2}, \sqrt[3]{7})/\mathbb{Q}$
(c) $\mathbb{Q}(\mathrm{i}, \sqrt{2}\mathrm{i}, \sqrt{3}\mathrm{i})/\mathbb{Q}$

Aufgabe 33: Sei L/K eine algebraische Körpererweiterung und $\mathrm{char}(K) = p \in \mathbb{N}$. Zeigen Sie:

(a) Ist $\alpha \in L$ inseparabel über K, so ist der Grad von α durch p teilbar.
(b) Ist $[L : K]$ endlich und $p \nmid [L : K]$, so ist L/K separabel.

Aufgabe 34: Sei K ein Körper der Charakteristik $p \in \mathbb{N}$ und $L = K(\alpha)$ eine einfache transzendente Körpererweiterung. Beweisen Sie, dass das Polynom $f = x^p - \alpha$ irreduzibel und inseparabel über L ist.

Aufgabe 35: Sei K ein Körper der Charakteristik $p \in \mathbb{N}$ und $f \in K[x]$ irreduzibel. Zeigen Sie:

(a) Es existiert ein $n \in \mathbb{N}_0$ und ein separables Polynom $g \in K[x]$ mit $f(x) = g(x^{p^n})$.
(b) Jede Nullstelle von f in einem Zerfällungskörper L hat dann die Vielfachheit p^n.

Aufgabe 36: Zeigen Sie, dass jede Körpererweiterung L/K vom Grad 6 ein primitives Element besitzt.

Aufgabe 37: Geben Sie die Additionstabelle und die Multiplikationstabelle des Körpers mit 9 Elementen an.

Aufgabe 38: Sei $p \in \mathbb{N}$ eine Primzahl, $n \in \mathbb{N}$ und $f \in \mathbb{F}_p[x]$ irreduzibel. Zeigen Sie: f teilt $x^{p^n} - x$ genau dann, wenn $\deg(f)$ ein Teiler von n ist.

Aufgabe 39: Sei $\mathbb{F}$ ein algebraischer Abschluss des Körpers $\mathbb{F}_p$ mit $p \in \mathbb{N}$ prim und sei $q \neq p$ eine weitere Primzahl. Zeigen Sie:

(a) $\mathbb{F} = \bigcup_{n \in \mathbb{N}} \mathbb{F}_{p^{n!}}$. Wie sind die Multiplikation und Addition in $\mathbb{F}$ definiert?
(b) $\mathbb{F}_{q^\infty} = \bigcup_{n \in \mathbb{N}} \mathbb{F}_{p^{q^n}}$ ist ein echter, unendlicher Teilkörper von $\mathbb{F}$.
(c) Die von dem Frobeniusautomorphismus $F_p : \mathbb{F} \to \mathbb{F}$, $\alpha \mapsto \alpha^p$ erzeugte Untergruppe $\langle F_p \rangle \subset \mathrm{Aut}(\mathbb{F})$ ist unendlich.
(d) $\mathbb{F}_{q^\infty}$ ist vollkommen.
(e) Es gibt Automorphismen von $\mathbb{F}$, die nicht in $\langle F_p \rangle \subset \mathrm{Aut}(\mathbb{F})$ enthalten sind.

Aufgabe 40: Schreiben Sie alle über $\mathbb{F}_2$ irreduziblen Polynome vom Grad ≤ 3 explizit als Produkte irreduzibler Polynome in $\mathbb{F}_4[x]$.

Aufgabe 41: Sei K ein endlicher Körper.

(a) Zeigen Sie: für jedes $\alpha \in K^*$ und jeden Körperautomorphismus $\sigma : K \to K$ haben α und $\sigma(\alpha)$ die gleiche Ordnung in der multiplikativen Gruppe $(K^*, \cdot)$.
(b) Gibt es zu zwei Elementen $\alpha, \beta \in K^*$, die die gleiche Ordnung in $(K^*, \cdot)$ haben, immer einen Körperautomorphismus $\sigma : K \to K$ mit $\sigma(\alpha) = \beta$? Beweisen Sie dies, oder geben Sie ein Gegenbeispiel an.

Aufgabe 42: Sei $p > 2$ eine Primzahl. Zeigen Sie, dass es genau $\frac{1}{2}p(p-1)$ normierte, über $\mathbb{F}_p$ irreduzible quadratische Polynome gibt.

Aufgabe 43: Sei $\alpha \in L$ eine Nullstelle von $p = x^3 + x^2 + \overline{1} \in \mathbb{F}_2[x]$ in einem Zerfällungskörper L von p.

(a) Bestimmen Sie die Anzahl der Elemente in $\mathbb{F}_2(\alpha) \subset L$.
(b) Sind alle Elemente von $\mathbb{F}_2(\alpha)$ von der Form α^m, $m \in \mathbb{Z}$?
(c) Untersuchen Sie, ob das Polynom $q = x^3 + x + \overline{1} \in \mathbb{F}_2[x]$ über $\mathbb{F}_2(\alpha)$ irreduzibel ist.
(d) Zeigen Sie, dass jede Nullstelle von p und jede Nullstelle von q in $\mathbb{F}_2(\alpha)$ eine Potenz von α ist und geben Sie diese explizit an.

Aufgabe 44: Sei K der Körper K mit 2^{10} Elementen.

(a) Bestimmen Sie die Anzahl der Elemente in der multiplikativen Gruppe $(K^*, \cdot)$, die Erzeuger dieser Gruppe sind.
(b) Bestimmen Sie alle Teilkörper von K.
(c) Bestimmen Sie die Anzahl der über $P(K) = \mathbb{F}_2$ primitiven Elemente $\alpha \in K$.

2 Galoistheorie

2.1 Die Galois-Korrespondenz

Im Verlauf der Vorlesung wuerden Körpererweiterungen häufig mit Hilfe von Nullstellen von Polynomen konstruiert, und jedes algebraische Element einer Körpererweiterung läßt sich als Nullstelle seines Minimalpolynoms beschreiben. Eine zentrales Hilfsmittel in der Untersuchung von Auflösbarkeit von polynomialen Gleichungen, der Konstruierbarkeit mit Zirkel und Lineal und, allgemeiner, der Struktur von Körpererweiterungen und ihrer Zwischenkörper spielt die Galois-Theorie, die auf dem Zusammenspiel der folgenden drei Beobachtungen aufbaut.

Beobachtung 1: Automorphismengruppe Ist L ein Körper und $M \subset L$ eine Teilmenge, so bilden die Automorphismen in $\mathrm{Aut}(L)$, die alle Elemente von M erhalten, eine Untergruppe von $\mathrm{Aut}(L)$:

$$\mathcal{G}(M) = \{\phi \in \mathrm{Aut}(L) : \phi(m) = m \, \forall m \in M\}.$$

Dies zeigt man durch direktes Nachrechnen der Axiome. Offensichtlich gilt $\mathrm{id}_L \in \mathcal{G}(M)$. Für $\sigma, \tau \in \mathcal{G}(M)$ folgt $\sigma \circ \tau(m) = \sigma(\tau(m)) = \sigma(m) = m$ für alle $m \in M$, also auch $\sigma \circ \tau \in \mathcal{G}(M)$. Ist $\sigma \in \mathcal{G}(M)$, so folgt $\sigma^{-1}(m) = \sigma^{-1}(\sigma(m)) = m$ für alle $m \in M$, also auch $\sigma^{-1} \in \mathcal{G}(M)$.

Daraus ergibt sich insbesondere:

- Die K-Automorphismen einer Körpererweiterung L/K bilden eine Untergruppe $\Gamma(L/K) = \mathcal{G}(K) = \{\psi \in \mathrm{Aut}(L) : \psi|_K = \mathrm{id}_K\}$ der Automorphismengruppe $\mathrm{Aut}(L)$, die **Galoisgruppe**.
- Es gilt $\mathcal{G}(L) = \{\mathrm{id}_L\}$.
- Für jeden Zwischenkörper $K \subset E \subset L$ erhält man eine Untergruppe $\mathcal{G}(E) \subset \mathcal{G}(K)$, und es gilt $\mathcal{G}(E) = \Gamma(L/E)$.

Beobachtung 2: Fixkörper Ist L ein Körper und $\Omega \subset \mathrm{Aut}(L)$ eine Teilmenge der Automorphismengruppe von L, so ist die Fixpunktmenge ein Teilkörper von L:

$$\mathcal{F}(\Omega) = \{\alpha \in L : \phi(\alpha) = \alpha \, \forall \phi \in \Omega\}$$

Dies zeigt man durch direktes Nachrechnen der Körperaxiome. Offensichtlich gilt für $\alpha, \beta \in \mathcal{F}(\Omega)$ und Körperautomorphismen $\tau \in \Omega$ die Gleichungen $\tau(\alpha - \beta) = \tau(\alpha) - \tau(\beta) = \alpha - \beta$, $\tau(\alpha \cdot \beta) = \tau(\alpha) \cdot \tau(\beta) = \alpha \cdot \beta$, also $\alpha - \beta, \alpha \cdot \beta \in \mathcal{F}(\Omega)$. Ist $\alpha \in L^*$ folgt ausserdem $1 = \tau(1) = \tau(\alpha^{-1} \cdot \alpha) = \tau(\alpha) \cdot \tau(\alpha^{-1}) = \alpha \cdot \tau(\alpha^{-1})$, also $\tau(\alpha^{-1}) = \tau(\alpha)^{-1} = \alpha^{-1}$ und somit $\alpha^{-1} \in \mathcal{F}(\Omega)$.

Daraus ergibt sich insbesondere:

- Der Primkörper $P(L)$ ist in jedem Teilkörper von L und damit in jedem Fixpunktkörper $F(\Omega)$, $\Omega \subset \mathrm{Aut}(L)$ enthalten, also $P(L) \subset \mathcal{F}(\Omega) \subset L$.
- Ist L/K eine Körpererweiterung und $\Omega \subset \Gamma(L/K)$ eine Teilmenge der K-Monomorphismen von L, so erhält man einen Zwischenkörper $K \subset \mathcal{F}(\Omega) \subset L$.

Beobachtung 3: Nullstellen von Polynomen Sind L, L' Erweiterungskörper von K und $\sigma : L \to L'$ ein K-Monomorphismus, so ist für jede Nullstelle $\alpha \in L$ eines Polynoms $p \in K[x]$ auch $\sigma(\alpha)$ eine Nullstelle von p, denn dann gilt $p(\sigma(\alpha)) = \sigma(p(\alpha)) = \sigma(0) = 0$. K-Automorphismen einer Körpererweiterung L/K bilden Nullstellen von Polynomen mit Koeffizienten in K auf Nullstellen von Polynomen mit Koeffizienten in K ab.

Wir fixieren die Begriffe aus diesen Beobachtungen in der folgenden Definition, und untersuchen anschliessend die Galoisgruppe für einige wichtige Beispiele von Körpererweiterungen.

Definition 2.1.1:

1. Für einen Körper K und eine Teilmenge $M \subset \mathrm{Aut}(K)$ bezeichnet wir den Teilkörper $\mathcal{F}(M) = \{\alpha \in K : \phi(\alpha) = \alpha \, \forall \phi \in M\}$ als den **Fixkörper** von M.
2. Die **Galoisgruppe** $\Gamma(L/K)$ einer Körpererweiterung L/K ist die Gruppe der K-Automorphismen $\phi : L \to L$, $\phi|_K = \mathrm{id}_K$.
3. Die **Galoisgruppe** eines Polynoms $p \in K[x]$ über K ist die Galoisgruppe der Körpererweiterung L/K, wobei L der Zerfällungskörper von p über K ist.
4. Eine Körpererweiterung L/K heißt **galoissch** oder **Galoiserweiterung**, wenn $K = \mathcal{F}(\Gamma(L/K))$ gilt. Sie heisst **abelsch** bzw. **zyklisch**, wenn sie galoissch mit abelscher bzw. zyklischer Galoisgruppe ist.

Beispiel 2.1.2:

1. Es gilt $\Gamma(\mathbb{R}/\mathbb{Q}) = \{\mathrm{id}_\mathbb{R}\}$, also ist $\mathbb{R}/\mathbb{Q}$ nicht galoissch.

   Dies folgt aus der Anordenbarkeit von $\mathbb{R}$ und der Tatsache, dass $\mathbb{Q}$ dicht in $\mathbb{R}$ ist. Sind $a, b \in \mathbb{R}$ mit $a < b$ und $\tau \in \Gamma(\mathbb{R}/\mathbb{Q})$, so folgt $\tau(a) < \tau(b)$, denn dann existiert ein $y \in \mathbb{R}$ mit $b - a = y^2$ und somit $\tau(b) - \tau(a) = \tau(b - a) = \tau(y^2) = \tau(y)^2 > 0$. Gäbe es ein $x \in \mathbb{R}$ mit $\tau(x) \neq x$, so wäre wegen $\tau(-x) = -\tau(x)$ oBdA $x < \tau(x)$, und es gäbe ein $q \in \mathbb{Q}$ mit $x < q < \tau(x)$. Daraus folgt $\tau(x) < \tau(q) = q < \tau(x)$ - ein Widerspruch.
2. Es gilt $\Gamma(\mathbb{C}/\mathbb{R}) = \{\mathrm{id}_\mathbb{C}, \bar{}\} \cong \mathbb{Z}/2\mathbb{Z}$, wobei $\bar{} : \mathbb{C} \to \mathbb{C}$, $a + \mathrm{i}b \mapsto a - \mathrm{i}b$ für $a, b \in \mathbb{R}$ die komplexe Konjugation bezeichnet. Die Körpererweiterung $\mathbb{R}/\mathbb{C}$ ist also galoissch, abelsch und zyklisch.

   Denn offensichtlich ist wegen $\overline{z + w} = \overline{z} + \overline{w}$, $\overline{z \cdot w} = \overline{z} \cdot \overline{w}$ und $\overline{a} = a$ für $z, w \in \mathbb{C}$, $a \in \mathbb{R}$ die komplexe Konjugation ein $\mathbb{R}$-Automorphismus von $\mathbb{C}$. Andererseits ist aber jeder $\mathbb{R}$-Automorphismus $\tau \in \Gamma(\mathbb{C}/\mathbb{R})$ durch seinen Wert auf i eindeutig bestimmt, denn jedes $z \in \mathbb{C}$ läßt sich eindeutig schreiben als $z = a + \mathrm{i}b$ mit $a, b \in \mathbb{R}$. Aus $-1 = \tau(-1) = \tau(\mathrm{i}^2) = \tau(\mathrm{i})^2$ folgt $\tau(\mathrm{i}) = \mathrm{i}$ oder $\tau(\mathrm{i}) = -\mathrm{i}$, also $\tau = \mathrm{id}_\mathbb{C}$ oder $\tau = \bar{}$.
3. Die Körpererweiterung $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ ist nicht galoissch, denn $\Gamma(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \{\mathrm{id}_{\mathbb{Q}(\sqrt[3]{2})}\}$.

   Denn jeder $\mathbb{Q}$-Automorphismus $\tau \in \Gamma(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ ist durch $\tau(\sqrt[3]{2})$ eindeutig bestimmt. Wegen $2 = \tau(2) = \tau((\sqrt[3]{2})^3) = \tau(\sqrt[3]{2})^3$ muss $\tau(\sqrt[3]{2})$ eine Nullstelle von $x^3 - 2$ sein. Da aber die einzige in $\mathbb{Q}(\sqrt[3]{2})$ enthaltene Nullstelle von $x^3 - 2$ die Nullstelle $\sqrt[3]{2}$ ist, folgt $\tau(\sqrt[3]{2}) = \sqrt[3]{2}$ und somit $\tau = \mathrm{id}_{\mathbb{Q}(\sqrt[3]{2})}$.

4. Sei $L = Q(\mathbb{Q}[x])$ der Körper der gebrochen rationalen Funktionen mit Koeffizienten in $\mathbb{Q}$. Die Körpererweiterung $L/\mathbb{Q}$ ist galoissch, denn für jedes $a \in \mathbb{Q}$ ist

$$\tau_a : L \to L, \quad \frac{p}{q} \mapsto \frac{p(x+a)}{q(x+a)}$$

ein $\mathbb{Q}$-Automorphismus von L. Aus $p/q \in \mathcal{F}(\Gamma(L/\mathbb{Q}))$ mit $q \neq 0$ folgt $\tau_a(p/q) = p/q$ für alle $a \in \mathbb{Q}$ und somit $p(a)/q(a) = p(0)/q(0)$ für alle $a \in \mathbb{Q}$. Also ist $p/q = p(0)/q(0) \in \mathbb{Q}$, und es gilt $\mathcal{F}(\Gamma(L/Q)) = \mathbb{Q}$.

5. Jeder Körper L ist eine Erweiterungskörper über seinem Primkörper $P(L)$, und die Galoisgruppe dieser Körpererweiterung ist $\Gamma(L/P(L)) = \mathrm{Aut}(L)$. Denn offensichtlich gilt $\Gamma(L/P(L)) \subset \mathrm{Aut}(L)$, und $\mathcal{F}(\mathrm{Aut}(L)) \subset L$ ist ein Teilkörper von L. Da der Primkörper $P(L)$ in jedem Teilkörper von L enthalten ist, folgt $P(L) \subset \mathcal{F}(\mathrm{Aut}L) \subset L$. Also ist jeder Automorphismus von L bereits in $\Gamma(L/P(L))$ enthalten.

Wie auch schon im bisherigen Verlauf der Vorlesung interessiert man sich für Körpererweiterungen oft nur *bis auf K-Isomorphie*, d. h. man möchte Körpererweiterungen L/K, L'/K', zwischen denen ein somorphismus $\phi : L \to L'$ mit $\phi(K) = K'$ existiert, nicht unterscheiden. Daher stellt sich die Frage nach der Beziehung zwischen den Galoisgruppen solcher Körpererweiterungen, und man vermutet, dass diese isomorph sind. Eine offensichtliche Idee, um einen Gruppenisomorphismus zwischen den Galoisgruppen solcher Körpererweiterungen anzugeben, ist es, durch Verketten mit dem ϕ und seinem Inversen, Elementen aus $\Gamma(L/K)$ Elemente aus $\Gamma(L'/K')$ zuzuordnen.

Lemma 2.1.3: Seien L/K und L'/K' Körpererweiterungen mit Galoisgruppen $\Gamma = \Gamma(L/K)$, $\Gamma' = \Gamma(L'/K')$ und $\phi : L \to L'$ ein Körperisomorphismus mit $\phi(K) = K'$. Dann gilt:

1. Die Abbildung $F_\phi : \Gamma(L/K) \to \Gamma(L'/K')$, $\tau \mapsto \phi \circ \tau \circ \phi^{-1}$ ist ein Gruppenisomorphismus.
2. Die Körpererweiterung L/K ist galoissch genau dann, wenn L'/K' galoissch ist.

Beweis:
1. Offensichtlich ist für alle K-Automorphismen $\tau : L \to L$ die Abbildung $\phi \circ \tau \circ \phi^{-1} : L' \to L'$ ein K'-Automorphismus, denn die Verkettung von Körperisomorphismen ist ein Körperisomorphismus und wegen $\phi(K) = K'$ gilt $\phi \circ \tau \circ \phi^{-1}(k') = \phi \circ \phi^{-1}(k') = k'$ für alle $k' \in K'$. Also erhält man eine Abbildung $F_\phi : \Gamma \to \Gamma'$ mit Inversem $F_\phi^{-1} = F_{\phi^{-1}} : \Gamma' \to \Gamma$, $\sigma \mapsto \phi^{-1} \circ \sigma \circ \phi$. Diese ist ein Gruppenisomorphismus, denn

$$F_\phi(\mathrm{id}_L) = \phi \circ \mathrm{id}_L \circ \phi^{-1} = \phi \circ \phi^{-1} = \mathrm{id}_{L'}$$
$$F_\phi(\rho \circ \tau) = \phi \circ \rho \circ \tau \circ \phi^{-1} = \phi \circ \rho \circ \phi^{-1} \circ \phi \circ \tau \circ \phi^{-1} = F_\phi(\rho) \circ F_\phi(\tau) \quad \forall \rho, \tau \in \Gamma.$$

2. Es gilt $\phi(\mathcal{F}(\Gamma)) = \mathcal{F}(\Gamma')$. Denn für $\alpha \in \mathcal{F}(\Gamma)$ folgt

$$F_\phi(\tau)(\phi(\alpha)) = \phi \circ \tau \circ \phi^{-1} \circ \phi(\alpha) = \phi \circ \tau(\alpha) = \phi(\alpha) \quad \forall \tau \in \Gamma,$$

und mit der Surjektivität von F_ϕ ergibt sich $\phi(\alpha) \in \mathcal{F}(\Gamma')$, also $\phi(\mathcal{F}(\Gamma)) \subset \mathcal{F}(\Gamma')$. Analog erhält man $\phi^{-1}(\mathcal{F}(\Gamma')) \subset \mathcal{F}(\Gamma)$ und somit $\phi(\mathcal{F}(\Gamma)) = \mathcal{F}(\Gamma')$. Da $\phi(K) = K'$ gilt $\mathcal{F}(\Gamma) = K$ genau dann, wenn $\mathcal{F}(\Gamma') = K'$. □

Wir untersuchen nun einen weiteren zentralen Aspekt von Galoisgruppen und Fixkörpern, nämlich den Zusammenhang zwischen Zwischenkörpern einer Körpererweiterung L/K und Untergruppen ihrer Galoisgruppe $\Gamma(L/K)$. Sei dazu für eine beliebige Körpererweiterung L/K mit Galoisgruppe $\Gamma = \Gamma(L/K)$

$$\mathcal{U}(\Gamma) = \{\text{Untergruppen } G \subset \Gamma\} \qquad \mathcal{Z}(L/K) = \{\text{Zwischenkörper von } L/K\}.$$

Im Folgenden bezeichnen wir mit $\mathcal{F} : U(\Gamma) \to \mathcal{Z}(L/K)$ die Abbildung, die einer Untergruppe $G \subset \Gamma$ ihren Fixpunktkörper $\mathcal{F}(G)$ zuordnet, und mit $\mathcal{G} : \mathcal{Z}(L/K) \to \mathcal{U}(\Gamma)$ die Abbildung, die einem Zwischenkörper $K \subset E \subset L$ die Galoisgruppe $\mathcal{G}(E) = \Gamma(L/E)$ der Körpererweiterung L/E zuordnet.

Offensichtlich ist der Fixpunktkörper einer Untergruppe $G \subset \Gamma$ ein Zwischenkörper $K \subset E \subset L$ und wird um so grösser, je kleiner die Gruppe G ist. Umgekehrt ist die Galoisgruppe eines solchen Zwischenkörpers um so kleiner, je grösser der Zwischenkörper ist. Verkettet man die Abbildungen $\mathcal{F}$ und $\mathcal{G}$, so kann man ausserdem den Fixpunktkörper einer Galoisgruppe $\Gamma(L/E)$ mit dem Zwischenkörper E oder die Galoisgruppe einer Körpererweiterung $L/\mathcal{F}(G)$ mit G vergleichen. Offensichtlich gelten dann die Inklusionen $E \subset \mathcal{F}(\Gamma(L/E))$ und $G \subset \mathcal{G}(L/\mathcal{F}(G))$.

Lemma 2.1.4: Sei L/K eine Körpererweiterung mit Galoisgruppe $\Gamma(L/K) = \Gamma$. Dann gilt für beliebige Untergruppen $G, H \subset \Gamma$ und Zwischenkörper E, F von L/K:

1. $E \subset F \Rightarrow \mathcal{G}(F) \subset \mathcal{G}(E), \quad G \subset H \Rightarrow \mathcal{F}(H) \subset \mathcal{F}(G)$.
2. $E \subset \mathcal{F} \circ \mathcal{G}(E), \quad G \subset \mathcal{G} \circ \mathcal{F}(G)$.
3. $\mathcal{G} \circ \mathcal{F} \circ \mathcal{G}(E) = \mathcal{G}(E), \quad \mathcal{F} \circ \mathcal{G} \circ \mathcal{F}(G) = \mathcal{F}(G)$.

Untergruppen $G \subset \Gamma$ mit $\mathcal{G} \circ \mathcal{F}(G) = G$ und Zwischenkörper $K \subset E \subset L$ mit $\mathcal{F} \circ \mathcal{G}(E) = E$ bezeichnet man als **abgeschlossen**.

Beweis:
1. und 2. folgen direkt aus der Definition. Aus 2. folgt $\mathcal{G}(E) \subset \mathcal{G} \circ \mathcal{F}(\mathcal{G}(E)) = \mathcal{G} \circ \mathcal{F} \circ \mathcal{G}(E)$. Andererseits gilt nach 2. aber auch $E \subset \mathcal{F} \circ \mathcal{G}(E)$, und mit 1. folgt $\mathcal{G} \circ \mathcal{F} \circ \mathcal{G}(E) = \mathcal{G}(\mathcal{F} \circ \mathcal{G}(E)) \subset \mathcal{G}(E)$, also Gleichheit. Der Beweis von $\mathcal{F} \circ \mathcal{G} \circ \mathcal{F}(G) = \mathcal{F}(G)$ ist analog. □

Wir untersuchen den Zusammenhang zwischen Untergruppen der Galoisgruppe $\Gamma(L/K)$ einer Körpererweiterung L/K und Zwischenkörpern $K \subset E \subset L$ nun an einigen Beispielen. Dass bei den Inklusionen $E \subset \mathcal{F} \circ \mathcal{G}(E)$ und $G \subset \mathcal{G} \circ \mathcal{F}(G)$ in Lemma 2.1.4 auch bei galoisschen Körpererweiterungen echte Ungleichheit gelten kann, zeigt das folgende Beispiel.

Beispiel 2.1.5: Wir betrachten die galoissche Körpererweiterung $L/\mathbb{Q}$ mit $L = Q(\mathbb{Q}[x])$ aus Beispiel 2.1.2, den Zwischenkörper $E = Q(\mathbb{Q}[x^3])$ und die von dem $\mathbb{Q}$-Automorphismus

$$\sigma_a : L \to L, \quad \frac{p}{q} \mapsto \frac{p(ax)}{q(ax)}$$

für festes $a \in \mathbb{Q} \setminus \{0, 1, -1\}$ erzeugte Untergruppe $G = \langle \sigma_a \rangle \subset \Gamma(L/\mathbb{Q})$. Dann gilt:

1. $\mathcal{G}(E) = \{\mathrm{id}_L\}$ und somit $E \subsetneq \mathcal{F} \circ \mathcal{G}(E) = L$.
2. $\mathcal{F}(G) = \mathbb{Q}$ und somit $G \subsetneq \mathcal{G} \circ \mathcal{F}(G) = \Gamma(L/\mathbb{Q})$.

Denn aus $\rho \in \mathcal{G}(E)$ folgt $\rho(x)^3 = \rho(x^3) = x^3$ und somit $(\rho(x)/x)^3 - 1 = 0$. Also ist $\rho(x)/x$ algebraisch über $\mathbb{Q}$ und somit bereits in $\mathbb{Q}$ enthalten, denn jedes Element in $L \setminus \mathbb{Q}$ ist transzendent. Da $\rho(c) = c$ für alle $c \in \mathbb{Q}$, ergibt sich $\rho = \mathrm{id}_L$.

Ist $p/q \in \mathcal{F}(G)$ mit $\mathrm{ggT}(p, q) = 1$, so folgt $p(ax)q(x) = p(x)q(ax)$ für alle $x \in \mathbb{Q}$, und ein Koeffizientenvergleich liefert $\deg(p) = \deg(q)$. Aus $\mathrm{ggT}(p, q) = 1$ ergibt sich $\mathrm{ggT}(p(ax), q(ax)) = 1$, und somit muss eine Konstante $b \in \mathbb{Q}$ existieren mit $p(ax) = bp(x)$. Es folgt $p(x) = cx^{\deg(p)}$ und $q(x) = dx^{\deg(p)}$ mit $c, d \in \mathbb{Q}$. Aus $a \notin \{0, 1, -1\}$ und $\mathrm{ggT}(p, q) = 1$ ergibt sich $\deg(p) = \deg(q) = 0$ und $p/q \in \mathbb{Q}$.

Beispiel 2.1.6: Sei L/K eine Körpererweiterung mit Galoisgruppe Γ. Für Zwischenkörper E, F von L/K bezeichne $EF = E(F) = F(E)$ das **Kompositum** von E und F, d. h. den kleinsten Zwischenkörper von L/K, der E und F enthält, und für Untergruppen $G, H \subset \Gamma$ $\langle G \cup H \rangle$ die kleinste Untergruppe von Γ, die G und H enthält. Dann gilt:

$$\mathcal{G}(EF) = \mathcal{G}(E) \cap \mathcal{G}(F) \qquad \mathcal{F}(\langle G \cup H \rangle) = \mathcal{F}(G) \cap \mathcal{F}(H).$$

Denn nach Lemma 2.1.4, 1. gilt wegen $E, F \subset EF$ die Inklusion $\mathcal{G}(EF) \subset \mathcal{G}(E) \cap \mathcal{G}(F)$, und mit Lemma 2.1.4, 2. folgt $E \subset \mathcal{F} \circ \mathcal{G}(E) \subset \mathcal{F}(\mathcal{G}(E) \cap \mathcal{G}(F))$ und $F \subset \mathcal{F} \circ \mathcal{G}(F) \subset \mathcal{F}(\mathcal{G}(E) \cap \mathcal{G}(F))$. Also gilt $EF \subset \mathcal{F}(\mathcal{G}(E) \cap \mathcal{G}(F))$ und mit Lemma 2.1.4, 1. und 2. ergibt sich $\mathcal{G}(E) \cap \mathcal{G}(F) \subset \mathcal{G} \circ \mathcal{F}(\mathcal{G}(E) \cap \mathcal{G}(F)) \subset \mathcal{G}(EF)$, also $\mathcal{G}(EF) = \mathcal{G}(E) \cap \mathcal{G}(F)$. Die Aussagen für die Untergruppen folgen analog.

Wir wenden uns nun wieder unserer Ausgangsfrage zu, nämlich der Untersuchung des Zusammenhangs zwischen Untergruppen der Galoisgruppe einer Körpererweiterung L/K und ihren Zwischenkörpern. Dabei nehmen die abgeschlossenen Zwischenkörper eine Sonderrolle ein, denn sie entsprechen gerade den Zwischenkörpern $K \subset E \subset L$, für die die Körpererweiterung L/E galoissch ist. Ebenso können wir zeigen, dass die Galoisgruppen solcher Körpererweiterungen L/E stets abgeschlossene Untergruppen von $\Gamma(L/K)$ sind. Diesen Zusammenhang zwischen abgeschlossenen Untergruppen der Galoisgruppe $\Gamma(L/K)$ und abgeschlossenen Zwischenkörpern von L/K bezeichnet man als Galois-Korrespondenz.

Satz 2.1.7: (**Galois-Korrespondenz**)

Sei L/K eine Körpererweiterung mit Galoisgruppe Γ und $\mathcal{F} : \mathcal{U}(\Gamma) \to \mathcal{Z}(L/K)$, $\mathcal{G} : \mathcal{Z}(L/K) \to \mathcal{U}(\Gamma)$ wie in Lemma 2.1.4. Dann gilt:

1. Eine Untergruppe $G \subset \Gamma$ ist abgeschlossen genau dann, wenn ein Zwischenkörper E von L/K mit $G = \mathcal{G}(E)$ existiert.
2. Für einen Zwischenkörper $K \subset E \subset L$ sind äquivalent:
   (i) E abgeschlossen: $\mathcal{F} \circ \mathcal{G}(E) = E$.
   (ii) Es existiert eine Untergruppe $U \subset \Gamma$ mit $E = \mathcal{F}(U)$.
   (iii) Die Körpererweiterung L/E ist galoissch.
3. Die Abbildungen $\mathcal{F}$ und $\mathcal{G}$ induzieren zueinander inverse Bijektionen zwischen der Menge der abgeschlossenen Untergruppen von Γ und der Menge der abgeschlossenen Zwischenkörper von L/K.

Beweis:
1. Ist $G \subset \Gamma$ abgeschlossen, also $G = \mathcal{G} \circ \mathcal{F}(G)$, so gilt $G = \mathcal{G}(E)$ mit $E = \mathcal{F}(G)$. Ist umgekehrt $K \subset E \subset L$ ein Zwischenkörper mit $G = \mathcal{G}(E)$, so folgt mit Lemma 2.1.4, 3. $G = \mathcal{G}(E) = \mathcal{G} \circ \mathcal{F} \circ \mathcal{G}(E) = \mathcal{G} \circ \mathcal{F}(G)$.

2. (i) $\Leftrightarrow$ (iii): Wegen $\Gamma(L/E) = \mathcal{G}(E)$ ist L/E galoissch, $\mathcal{F}(\Gamma(L/E)) = E$, genau dann, wenn $E \subset \mathcal{Z}(L/K)$ abgeschlossen, $\mathcal{F} \circ \mathcal{G}(E) = E$.
(i) $\Leftrightarrow$(ii): Ist E abgeschlossen, so folgt $E = \mathcal{F}(U)$ mit $U = \mathcal{G}(E)$. Existiert umgekehrt eine Untergruppe $U \subset \Gamma$ mit $E = \mathcal{F}(U)$, so folgt mit Lemma 2.1.4, 3. die Gleichung $E = \mathcal{F}(U) = \mathcal{F} \circ \mathcal{G} \circ \mathcal{F}(U) = \mathcal{F} \circ \mathcal{G}(E)$, also E abgeschlossen.

3. Nach 1. ist für jeden abgeschlossenen Zwischenkörper $K \subset E \subset L$ die Gruppe $\mathcal{G}(E)$ abgeschlossen mit $\mathcal{F} \circ \mathcal{G}(E) = E$ und für jede abgeschlossene Untergruppe $G \subset \Gamma$ der Zwischenkörper $\mathcal{F}(G)$ abgeschlossen mit $\mathcal{G} \circ \mathcal{F}(G) = G$. □

2.2 Algebraische Galoiserweiterungen

Im Folgenden beschäftigen wir uns mit den Galoisgruppen *algebraischer*, galoisscher Körpererweiterungen und werden diese für viele Fälle explizit bestimmen. Als erstes wollen wir dazu den Begriff der Galoiserweiterung durch schon bekannte Eigenschaften von Körpererweiterungen charakterisieren.

Die in Beispiel 2.1.2 betrachteten Körpererweiterungen legen nahe, dass der Begriff der Galoiserweiterung etwas mit Normalität zu tun haben sollte. Denn ist L/K eine algebraische Körpererweiterung, so ist jeder K-Monomorphismus durch die Nullstellen der Minimalpolynome $m_{\alpha,K}$ von Elementen $\alpha \in L$ eindeutig bestimmt. Solche Nullstellen werden stets auf andere Nullstellen von $m_{\alpha,K}$ abgebildet, was bedeutet, dass es umso mehr K-Automorphismen gibt, je mehr Nullstellen von $m_{\alpha,K}$ in L ethalten sind. Je grösser die Zahl der K-Automorphismen, desto kleiner wird aber der zugehörige Fixpunktkörper, was es nahelegt, dass galoissche Körpererweiterungen Zerfällungskörpern entsprechen.

Ebenso ist offensichtlich, dass sich die Existenz von *mehrfachen* Nullstellen der Minimalpolynome im Körper L störend auf die K-Automorphismen auswirkt, da sich die Vielfachheit von Nullstellen unter einem K-Automorphismus nicht ändern sollte. Dies suggeriert, dass Körpererweiterungen, die normal und separabel sind, die größtmögliche Gruppe von K-Automorphismen und daher die kleinstmöglichen Fixpunktkörper der Galoisgruppe haben sollten und somit gute Kandidaten für Galoiserweiterungen sind.

Satz 2.2.1: (normal+separabel=galoissch)

Für eine algebraische Körpererweiterung L/K sind äquivalent:

(i) L/K ist galoissch.

(ii) L/K ist normal und separabel.

(iii) L ist Zerfällungskörper einer Familie separabler Polynome aus $K[x]$.

Beweis:
(i)⇒(ii): Sei L/K galoissch und $p \in K[x]$ ein irreduzibles normiertes Polynom mit einer

Nullstelle $\alpha \in L$. Dann ist für jeden K-Automorphismus $\tau \in \Gamma(L/K)$ auch $\tau(\alpha)$ eine Nullstelle von p, und somit ist die Menge $\{\tau(\alpha) : \tau \in \Gamma(L/K)\}$ endlich. Seien also $\alpha = \alpha_1$, α_2,...,$\alpha_r \in L$ die verschiedenen Bilder von α unter K-Automorphismen in $\Gamma(L/K)$ und $q := \prod_{i=1}^{r}(x - \alpha_i) = \sum_{i=0}^{r} a_i x^i \in L[x]$.

Wir zeigen $q = p$. Zunächst gilt für alle $\tau \in \Gamma(L/K)$

$$\tau_*(q) = \sum_{i=0}^{r} \tau(a_i)x^i = \prod_{i=1}^{r}(x - \tau(\alpha_i)) = \prod_{i=1}^{r}(x - \alpha_i) = \sum_{i=0}^{r} a_i x^i,$$

denn τ bildet Nullstellen von p auf Nullstellen von p ab und ist injektiv, permutiert also die Nullstellen von p. Aus dieser Gleichung ergibt sich $\tau(a_i) = a_i$ für alle $i = 0, ..., r$ und damit $q \in K[x]$. Da $q(\alpha) = 0$ folgt $p = m_{\alpha,K}|q$ und da $\alpha_1, ..., \alpha_r$ verschieden sind folgt $\deg(p) \geq \deg(q)$. Da ausserdem p und q normiert sind, muss $p = q$ gelten. Also zerfällt p über L und hat nur einfache Nullstellen, und somit ist L/K normal und separabel.

(ii)⇒(i): Wir zeigen: zu jedem $\alpha \in L \setminus K$ existiert ein K-Automorphismus $\tau_\alpha \in \Gamma(L/K)$ mit $\tau(\alpha) \neq \alpha$. Sei also $\alpha \in L \setminus K$. Da L/K separabel ist, ist hat $m_{\alpha,K}$ keine mehrfachen Nullstellen in dem algebraischen Abschluss $\overline{K}$ und wegen $\alpha \in L \setminus K$ gilt $\deg(m_{\alpha,K}) > 1$. Also muss $m_{\alpha,K}$ eine weitere Nullstelle $\beta \neq \alpha \in \overline{K}$ haben, und nach dem Fortsetzungssatz für primitive Körpererweiterungen (Satz 1.4.13) existiert ein K-Isomorphismus $\tau : K(\alpha) \to K(\beta) \subset \overline{K}$ mit $\tau(\alpha) = \beta$. Dieser läßt sich nach dem Fortsetzungssatz für K-Monomorphismen in algebraisch abgeschlossene Körper (Satz 1.4.16) zu einem K-Monomorphismus $\overline{\tau} : L \to \overline{K}$ fortsetzen, und da L/K normal ist folgt mit Satz 1.5.1 $\overline{\tau}(L) = L$. Also gilt $\tau_\alpha = \overline{\tau} \in \Gamma(L/K)$ und $\tau_\alpha(\alpha) = \tau(\alpha) = \beta \neq \alpha$. Also folgt $\mathcal{F}(L/K) = K$ und somit L/K galoissch.

(ii)⇔(iii): Dies folgt direkt aus Satz 1.5.1 und Lemma 1.5.19. □

Während viele Beispiele algebraischer Körpererweiterungen - insbesondere über Körpern der Charakteristik 0 oder endlichen Körpern - separabel sind, gibt es viele Beispiele nicht normaler und daher auch nicht galoisscher Körpererweiterungen. Ist eine solche Körpererweiterung ausserdem endlich, kann man daraus durch Hinzufügen von Nullstellen algebraischer Elemente eine galoissche Körpererweiterung konstruieren. Durch Übergang zu einem Erweiterungskörper, nämlich dem Zerfällungskörper des Minimalpolynoms eines primitiven Elements, erhält man dann eine Einbettung dieser Körpererweiterung in eine endliche, galoissche Körpererweiterung.

Korollar 2.2.2: (**Einbettung in Galoiserweiterungen**)

Zu jeder endlichen separablen Körpererweiterung L/K existiert eine endliche Galoiserweiterung M/K mit Zwischenkörper L.

Beweis:
Da L/K endlich und separabel ist, existiert nach dem Satz vom primitiven Element ein $\alpha \in L$ mit $L = K(\alpha)$. Das Minimalpolynom $m_{\alpha,K}$ ist separabel, und sein Zerfällungskörper M über L ist auch ein Zerfällungskörper von $m_{\alpha,K}$ über K. Also ist nach Satz 2.2.1 M/K galoissch. □

Wir untersuchen nun, unter welchen Bedingungen die Zwischenkörper einer algebraischen Körpererweiterung L/K galoissche Körpererweiterungen definieren. Ist L/K galoissch, so ist

nach Satz 2.2.1 L normal und separabel über K und somit auch normal und separabel über jedem Zwischenkörper $K \subset E \subset L$. Also ist die Körpererweiterung L/E galoissch für jeden Zwischenkörper E. Die Frage, ob auch die Körpererweiterung E/K galoissch ist, ist komplizierter. Denn aus L separabel über K folgt zwar, dass auch E separabel über K ist, aber aus L normal über K folgt nicht, dass auch E normal über K ist - ein Gegenbeispiel ist $L = \mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3})$, $E = \mathbb{Q}(\sqrt[3]{2})$, $K = \mathbb{Q}$. Ein Kriterium, wann auch die Körpererweiterung E/K galoissch ist liefert der Satz von Krull, der auch die Bezeichnung *normale* Körpererweiterung motiviert.

Satz 2.2.3: (Satz von Krull: Normalteiler und Zwischenkörper)

Sei L/K eine algebraische Galoiserweiterung mit Galoisgruppe Γ. Dann gilt für jeden Zwischenkörper E von L/K:

1. E ist abgeschlossen und L/E ist galoissch.
2. Jeder K-Monomorphismus $\phi : E \to \overline{L}$ in einen algebraischen Abschluss $\overline{L}$ von L kann zu einem K-Automorphismus $\phi \in \Gamma$ fortgesetzt werden.
3. E/K ist genau dann galoissch, wenn $\Gamma(L/E) \subset \Gamma$ eine normale Untergruppe ist, und in diesem Fall gilt $\Gamma(E/K) \cong \Gamma/\Gamma(L/E)$.

Beweis:
1. Da L/K algebraisch und galoissch ist, ist L nach Satz 2.2.1 normal über K und somit Zerfällungskörper einer Menge $A \subset K[x]$ über K separabler Polynome. Damit ist L auch Zerfällungskörper von $A \subset E[x]$ und alle Polynome in A sind separabel über E. Damit ist L normal und separabel über E. Also ist L/E nach Satz 2.2.1 galoissch, und nach Satz 2.1.7 ist E abgeschlossen.

2. Nach dem Fortsetzungssatz für K-Monomorphismen in algebraisch abgeschlossene Körper (Satz 1.4.16) kann jeder K-Monomorphismus $\phi : E \to \overline{L}$ zu einem K-Monomorphismus $\overline{\phi} : L \to \overline{L}$ fortgesetzt werden. Da L/K normal ist, gilt nach Satz 1.5.1 $\overline{\phi}(L) = L$ und somit $\overline{\phi} \in \Gamma$.

3. Sei E/K galoissch, also normal und separabel. Da aus L/K algebraisch auch E/K algebraisch folgt, ist E/K nach Satz 2.2.1 normal. Mit Satz 1.5.1 folgt $\tau(E) = E$ für alle $\tau \in \Gamma$ und somit $\tau|_E \in \Gamma(E/K)$. Also erhalten wir einen Gruppenhomomorphismus $\phi : \Gamma \to \Gamma(E/K)$, $\tau \mapsto \tau|_E$ mit $\ker(\phi) = \{\tau \in \Gamma : \tau|_E = \mathrm{id}_E\} = \Gamma(L/E)$. Da sich nach 2. jeder K-Automorphismus $\rho : E \to E \subset \overline{L}$ zu einem K-Automorphismus $\overline{\rho} \in \Gamma$ fortsetzen lässt, ist dieser Gruppenhomomorphismus surjektiv. Also ist $\Gamma(L/E) \subset \Gamma$ als Kern eines Gruppenhomomorphismus eine normale Untergruppe, und es gilt $\Gamma(E/K) \cong \Gamma/\Gamma(L/E)$.

Ist umgekehrt $\Gamma(L/E) \subset \Gamma$ eine normale Untergruppe, so gilt für alle $\sigma \in \Gamma$, $\rho \in \Gamma(L/E)$ $\sigma^{-1} \circ \rho \circ \sigma \in \Gamma(L/E)$. Damit gilt für alle $\alpha \in E$ die Identität $\rho(\sigma(\alpha)) = \sigma(\alpha)$, also $\sigma(\alpha) \in \mathcal{F}(\Gamma(L/E)) = E$. Damit ist gezeigt, dass für alle $\sigma \in \Gamma$ gilt $\sigma(E) \subset E$. Da auch $\sigma^{-1}(E) \subset E$, folgt $\sigma(E) = E$, also $\sigma|_E \in \Gamma(E/K)$ für alle $\sigma \in \Gamma$. Da L/K galoissch ist, existiert zu jedem $\alpha \in E \setminus K$ ein $\sigma \in \Gamma$ mit $\alpha \neq \sigma(\alpha) \in E$, und es folgt $\mathcal{F}(E) = \mathcal{F} \circ \mathcal{G}(\Gamma(E/K)) = K$, also E/K galoissch. □

Wir werden diesen Satz später benutzen, um zu beweisen, dass für eine endliche (also damit insbesondere algebraische) Galoiserweiterung L/K, die Zwischenkörper $K \subset E \subset L$ eins zu eins den Untergruppen der Galoisgruppe entsprechen.

Dazu müssen wir uns zunächst mit Körpererweiterungen beschäftigen, die man erhält, wenn man für einen gegebenen Körper L den Fixkörper $\mathcal{F}(\Gamma) \subset L$ einer Untergruppe $\Gamma \subset \mathrm{Aut}(L)$ betrachtet. Dies liefert offensichtlich eine Körpererweiterung $L/\mathcal{F}(\Gamma)$. Ist Γ eine endliche Untergruppe, so kann man aus der Ordnung von Γ direkt den Grad dieser Körpererweiterung ableiten, indem wir ähnlich wie im Beweis von Satz 2.2.1 ausnutzen, dass ein K-Isomorphismus einer Körpererweiterung L/K die Nullstellen von Polynomen in $K[x]$ aufeinander abbildet.

Satz 2.2.4: (Satz von Dedekind)

Sei L ein Körper und $\Gamma \subset \mathrm{Aut}(L)$ eine endliche Untergruppe mit Fixkörper $K = \mathcal{F}(\Gamma)$. Dann gilt $[L : K] = |\Gamma|$.

Beweis:
1. Wir zeigen zuerst, dass L/K separabel ist und $[K(\alpha) : K] \leq |\Gamma|$ für alle $\alpha \in L$ gilt.

Sei $\alpha \in L$ und $M = \{\tau(\alpha) : \tau \in \Gamma\}$ die (endliche) Bahn von α unter Γ. Dann gilt für das Polynom $q = \prod_{\beta \in M}(x - \beta) = \sum_{i=0}^{|M|} a_i x^i \in L[x]$ wegen $\tau(M) = M$ für alle $\tau \in \Gamma$

$$\tau_*(q) = \sum_{i=0}^{|M|} \tau(a_i)x^i = \prod_{\beta \in M}(x - \tau(\beta)) = \prod_{\beta \in M}(x - \beta) = \sum_{i=0}^{|M|} a_i x^i = q,$$

und somit $\tau(a_i) = a_i$ für alle $i = 0, ..., |M|$. Da per Definition $\mathcal{F}(\Gamma) = K$ gilt, folgt $a_i \in K$ für alle $i = 0, ..., |M|$, also $q \in K[x]$. Da q über L in Linearfaktoren zerfällt, nur einfache Nullstellen hat und $q(\alpha) = 0$ ist q separabel über K. Da das Minimalpolynom $m_{\alpha,K}$ wegen $q(\alpha) = 0$ das Polynom q teilt, gilt dies auch für das Minimalpolynom $m_{\alpha,K}$. Also ist L/K separabel mit $[K(\alpha) : K] = \deg(m_{\alpha,K}) \leq \deg(q) = |M| \leq |\Gamma|$ für alle $\alpha \in L$.

2. Da L/K algebraisch ist und nach 1. $[K(\alpha) : K] \leq |\Gamma|$ für alle $\alpha \in L$, existiert ein $\beta \in L$ mit $\deg_K(\beta) = [K(\beta) : K] = \max\{\deg_K(\alpha) : \alpha \in L\}$. Da L/K separabel ist, existiert dann zu jedem weiteren Element $\gamma \in L$ nach dem Satz vom primitiven Element ein $\delta \in L$ mit $K(\beta, \gamma) = K(\delta)$. Mit dem Gradsatz folgt

$$\deg_K(\delta) = [K(\delta) : K] = [K(\beta, \gamma) : K] = [K(\beta, \gamma) : K(\gamma)] \cdot [K(\gamma) : K] \geq \deg_K(\beta).$$

Da aber $\deg_K(\beta)$ als maximal angenommen war, impliziert das $\deg_K(\delta) = [K(\delta) : K] = [K(\gamma, \beta) : K] = [K(\beta) : K] = \deg_K(\beta)$ und damit $\delta \in K(\beta)$. Also gilt $L = K(\beta)$ und nach 1. $[L : K] = [K(\beta) : K] \leq |\Gamma|$. Nach Korollar 1.5.21 ist aber $|\Gamma| \leq |\Gamma(L/K)| \leq [L : K]$ und somit folgt Gleichheit. □

Indem wir diesen Satz mit dem Satz von Krull (Satz 2.2.3), mit Satz 2.1.7 und mit Korollar 1.5.21 kombinieren, erhalten wir, dass jeder Zwischenkörper einer *endlichen* Galoiserweiterung L/K und jede Untergruppe $U \subset \Gamma(L/K)$ abgeschlossen ist. Demnach ist für jeden Zwischenkörper $E \subset L$ die Körpererweiterung L/E galoissch, und ihre Galoisgruppe hat genau $[L : E]$ Elemente. Insbesondere erhält man für $E = L$, dass $[L : K] = |\Gamma(L/K)|$ gelten muss. Es ergibt sich ausserdem, dass die Abbildungen $\mathcal{G} : \mathcal{Z}(L/K) \to \mathcal{U}(\Gamma(L/K))$ und $\mathcal{F} : \mathcal{U}(\Gamma(L/K)) \to \mathcal{Z}(L/K)$ aus aus Lemma 2.1.4, die einem Zwischenkörper E die Galoisgruppe von L/E und einer Untergruppe $U \subset \Gamma(L/K)$ ihren Fixpunktkörper zuordnen bijektiv und zueinander invers sind. Dies ist ein zentrales Resultat der Galoistheorie, das unter dem Namen *Hauptsatz der endlichen Galoistheorie* bekannt ist.

Satz 2.2.5: (Hauptsatz der endlichen Galoistheorie)

Sei L/K eine endliche Galoiserweiterung mit Galoisgruppe Γ. Dann sind die Abbildungen $\mathcal{F} : \mathcal{U}(\Gamma) \to \mathcal{Z}(L/K)$, $G \mapsto \mathcal{F}(G)$ und $\mathcal{G} : \mathcal{Z}(L/K) \to \mathcal{U}(\Gamma)$, $E \mapsto \Gamma(L/E)$ aus Lemma 2.1.4 bijektiv und zueinander invers. Für jeden Zwischenkörper $K \subset E \subset L$ gilt:

1. $[L : E] = |\Gamma(L/E)|$.
2. E ist abgeschlossen und L/E galoissch.
3. Jeder K-Monomorphismus $\phi : E \to \overline{L}$ in einen algebraischen Abschluss $\overline{L}$ von L kann zu einem Element aus Γ fortgesetzt werden.
4. E/K ist genau dann galoissch, wenn $\Gamma(L/E)$ Normalteiler von Γ ist, und in diesem Fall gilt $\Gamma(E/K) \cong \Gamma/\Gamma(L/E)$.

Beweis:
1. Die Surjektivität von $\mathcal{F} : \mathcal{U}(\Gamma) \to \mathcal{Z}(L/K)$ ist nach Satz 2.1.7 äquivalent zu der Aussage, dass für jeden Zwischenkörper E von L/K die Körpererweiterung L/E galoissch ist, was direkt aus dem Satz von Krull (Satz 2.2.3) folgt. Die Gleichung $[L : E] = |\Gamma(L/E)|$ folgt aus dem Satz von Dedekind (Satz 2.2.4), und die letzten drei Aussagen wieder aus dem Satz von Krull. Also bleibt noch zu zeigen, dass jede Untergruppe $U \subset \Gamma$ abgeschlossen ist, denn dann ist auch $\mathcal{G} : \mathcal{U}(\Gamma) \to \mathcal{Z}(L/K)$ surjektiv, und die Aussage folgt mit Satz 2.1.7.

2. Nach Korollar 1.5.21 gilt $|\Gamma(L/K)| \leq [L : K]$. Somit ist jede Untergruppe $U \subset \Gamma$ endlich, und mit dem Satz von Dedekind folgt $[L : \mathcal{F}(U)] = |U|$. Wegen $\mathcal{F}(U) = \mathcal{F} \circ \mathcal{G} \circ \mathcal{F}(U)$ ist $\mathcal{F}(U)$ auch Fixkörper der Untergruppe $\mathcal{G} \circ \mathcal{F}(U) \subset \Gamma$, und mit dem Satz von Dedekind folgt $[L : \mathcal{F}(U)] = |\mathcal{G} \circ \mathcal{F}(U)| = |U|$. Also gilt $\mathcal{G} \circ \mathcal{F}(U) = U$, und U ist abgeschlossen. □

Korollar 2.2.6: Eine endliche, separable Körpererweiterung besitzt nur endlich viele Zwischenkörper.

Beweis:
Ist L/K endlich und separabel, so existiert nach Korollar 2.2.2 eine endliche Galoiserweiterung M/K mit $L \subset M$. Nach dem Hauptsatz (Satz 2.2.5) kann M/K nur endlich viele Zwischenkörper haben, denn diese sind in Bijektion mit den Untergruppen der endlichen Gruppe $\Gamma(L/K)$, und somit hat auch L/K nur endlich viele Zwischenkörper. □

Mit Hilfe des Hauptsatzes lassen sich in vielen Fällen die Galoisgruppe einer Körpererweiterung und ihre Untergruppen explizit bestimmen und dadurch auch alle Zwischenkörper klassifizieren. Allerdings wird dies mit zunehmendem Grad der Körpererweiterung immer schwieriger. Das einfachste, aber auch relativ uninteressante Beispiel sind galoissche Körpererweiterungen vom Grad zwei, deren Galoisgruppe stes isomorph zu $\mathbb{Z}/2\mathbb{Z}$ ist. Sie besteht aus der Identitätsabbildung und einem weiteren K-Isomorphismus, der die zwei Nullstellen des Minimalpolynoms eines primitiven Elements vertauscht. Interessantere Beispiele erhält man, wenn man Körpererweiterungen vom Grad drei oder vier betrachtet.

Beispiel 2.2.7: Wir betrachten die Körpererweiterung $\mathbb{Q}(\sqrt{2}, \mathrm{i})/\mathbb{Q}$ und bestimmen ihre Galoisgruppe Γ. Der Körper $L := \mathbb{Q}(\sqrt{2}, \mathrm{i})$ ist Zerfällungskörper des Polynoms

$$p = x^4 - x^2 - 2 = (x^2 + 1)(x^2 - 2).$$

Also ist $L/\mathbb{Q}$ normal und wegen $\mathrm{char}(\mathbb{Q}) = 0$ auch separabel, also galoissch. Die Polynome x^2+1 und x^2-2 sind irreduzibel über $\mathbb{Q}$ mit Nullstellen $\pm\mathrm{i}$ und $\pm\sqrt{2}$, und es folgt $[\mathbb{Q}(\sqrt{2},\mathrm{i}) : \mathbb{Q}] = 4$. Also hat die Galoisgruppe Γ vier Elemente, die jeweils durch ihren Wert auf $\sqrt{2}$ und i eindeutig bestimmt sind.

Nach dem Fortsetzungssatz für primitive Körpererweiterungen existieren ein $\mathbb{Q}(\sqrt{2})$-Automorphismus ϕ von L mit $\phi(\mathrm{i}) = -\mathrm{i}$ und ein $\mathbb{Q}(\mathrm{i})$-Automorphismus ψ von L mit $\psi(\sqrt{2}) = -\sqrt{2}$. Da $\phi \circ \phi = \psi \circ \psi = \mathrm{id}_L$ und $\phi \circ \psi = \psi \circ \phi \neq \mathrm{id}_L$ folgt

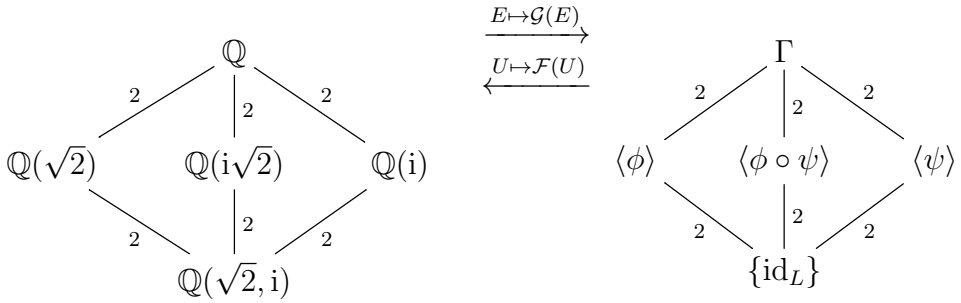
$$\Gamma = \langle \phi, \psi |\, \psi^2 = \phi^2 = \mathrm{id}_L, \phi \circ \psi = \psi \circ \phi \rangle \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Dies ist die Kleinsche Vierergruppe. Sie besitzt die Untergruppen $\{\mathrm{id}_L\}$, $\langle\phi\rangle \cong \mathbb{Z}/2\mathbb{Z}$, $\langle\psi\rangle \cong \mathbb{Z}/2\mathbb{Z}$, $\langle\phi\circ\psi\rangle \cong \mathbb{Z}/2\mathbb{Z}$ und Γ. Die zugehörigen Fixkörper sind

$$\mathcal{F}(\mathrm{id}_L) = L, \quad \mathcal{F}(\Gamma) = \mathbb{Q}, \quad \mathcal{F}(\langle\phi\rangle) = \mathbb{Q}(\sqrt{2}), \quad \mathcal{F}(\langle\psi\rangle) = \mathbb{Q}(\mathrm{i}), \quad \mathcal{F}(\langle\phi\circ\psi\rangle) = \mathbb{Q}(\mathrm{i}\sqrt{2}).$$

Da Γ abelsch ist, ist jede Untergruppe $U \subset \Gamma$ ein Normalteiler, und somit ist für alle Zwischenkörper E auch die Körpererweiterung $E/\mathbb{Q}$ galoissch.

Wir stellen die Zwischenkörper von $L/\mathbb{Q}$ und die Untergruppen von Γ schematisch in einem **Zwischenkörperdiagramm** bzw. **Untergruppendiagramm** dar:



Verbindungsstriche zwischen Teilkörpern bzw. Untergruppen bedeuten, dass der obere Körper ein Teilkörper des unteren Körpers bzw. die untere Gruppe eine Untergruppe der oberen Gruppe ist. Die Zahlen geben den Grad der Körpererweiterung an bzw. den Index der unteren in der oberen Gruppe an. Die Zwischenkörper E bzw. Untergruppen U an den gleichen Positionen im Diagramm stehen über die Relationen $E = \mathcal{F}(U)$ und $U = \mathcal{G}(E) = \Gamma(L/E)$ in Verbindung.

2.3 Kreisteilungskörper

In diesem Abschnitt befassen wir uns mit den Zerfällungskörpern von Polynomen der Form $x^n - 1$ über K. Diese bilden einerseits eine interessante Klasse von Körpererweiterungen, deren Galoisgruppe wir für beliebiges $n \in \mathbb{N}$ explizit berechnen können. Andererseits sind sie durch das Problem der Konstruktion regulärer n-Ecke mit Zirkel und Lineal motiviert. Die Gleichung $x^n = 1$ hat nämlich in $K = \mathbb{C}$ genau n Lösungen, die sogenannten $n$ten Einheitswurzeln. Diese entsprechen den Ecken eines in den Einheitskreis $E = \{z \in \mathbb{C} : |z| = 1\}$ einbeschriebenen regulären nEcks mit einer Ecke in 1.

Dies folgt direkt aus der Polardarstellung komplexer Zahlen. Jedes $z \in \mathbb{C}^*$ läßt sich nämlich eindeutig schreiben als $z = re^{\mathrm{i}\phi}$ mit $r = |z| \in \mathbb{R}^+$ und $\phi \in [0, 2\pi)$. Unter Benutzung der komplexen Exponentialfunktion $\exp : \mathbb{C} \to \mathbb{C}$, $z \mapsto e^z$ erhält man $z^n = r^n e^{\mathrm{i}n\phi}$. Da $e^{\mathrm{i}\phi} = \cos\phi + \mathrm{i}\sin\phi = 1$ genau dann, wenn $\phi \in 2\pi\mathbb{Z}$, folgt

$$z^n = r^n e^{\mathrm{i}n\phi} = 1 \quad \Leftrightarrow \quad r = 1,\ n\phi \in 2\pi\mathbb{Z}.$$

Wegen $\phi \in [0, 2\pi)$ ist dies äquivalent zu $r = 1$ und $\phi \in \{2\pi ik/n : k = 0, 1, ..., n-1\}$. Also ist die Menge der $n$ten Einheitswurzeln in $\mathbb{C}$ gegeben durch

$$W_n(\mathbb{C}) = \{z \in \mathbb{C} : z^n = 1\} = \{e^{2\pi ik/n} : k = 0, 1, ..., n-1\}.$$

Zeichnet man diese Zahlen, so sieht man, dass $e^{2\pi ik/n}$ einem Punkt auf dem Einheitskreis mit dem Winkel $2\pi k/n$ zur positiven reellen Achse entspricht. Die $n$ten Einheitswurzeln sind also genau die Punkte auf dem Einheitskreis, die man erhält, wenn man den Einheitskreis, ausgehend von der positiven rellen Achse, in n Segmente mit gleichem Winkel unterteilt. Die $n$ten Einheitswurzeln sind also die Ecken eines in E einbeschriebenen regulären n-Ecks.

Möchte man also die Konstruierbarkeit des regulären n-Ecks mit Zirkel und Lineal untersuchen, muss man sich genauer mit den Eigenschaften der $n$ten Einheitswurzeln bzw. mit dem Zerfällungskörper des Polynoms $x^n - 1$ befassen. Wir betrachten dieses Polynom nun über beliebigen Körpern K.

Definition 2.3.1: Sei K ein Körper.

1. Die Elemente $w \in K$ mit $w^n = 1$ bezeichnet man als $n$te **Einheitswurzeln** in K und schreibt $W_n(K) = \{w \in K : w^n = 1\}$ für die Menge der $n$ten Einheitswurzeln.
2. Den Zerfällungskörper $K_n \subset \overline{K}$ des Polynoms $x^n - 1 \in K[x]$ bezeichnet man als den $n$ten **Kreisteilungskörper** über K.

Beispiel 2.3.2:

1. Für beliebige Körper K gilt $W_1(K) = \{1\}$ und $K_1 = K$.
2. Es gilt $W_n(\mathbb{R}) = \{1\}$ falls n ungerade und $W_n(\mathbb{R}) = \{1, -1\}$ falls n gerade.
3. Aus $W_n(\mathbb{C}) = \{e^{2\pi ik/n} : k = 0, 1, ..., n-1\}$ erhält man die $n$ten Kreisteilungskörper $\mathbb{Q}_n = \mathbb{Q}(e^{2\pi i/n})$ und $\mathbb{R}_n = \mathbb{R}(e^{2\pi \imath/n})$. Diese sind offensichtlich primitive Körpererweiterungen über den Grundkörpern $\mathbb{Q}$ und $\mathbb{R}$. Es gilt $\mathbb{R}_n = \mathbb{R}$ falls $n \leq 2$ und $\mathbb{R}_n = \mathbb{C}$ für $n > 2$.
4. Es gilt $W_n(\mathbb{F}_2) = \{\overline{1}\}$, $W_n(\mathbb{F}_3) = \{\overline{1}\}$ falls n ungerade und $W_n(\mathbb{F}_3) = \{\overline{1}, \overline{2}\}$ falls n gerade.

Wir untersuchen nun systematisch die Eigenschaften der $n$ten Einheitswurzeln in Körpern K und deren algebraischen Abschlüssen $\overline{K}$. Dabei stellt sich heraus, dass wir die Fälle $\mathrm{char}(K)|n$ und $\mathrm{char}(K) \nmid n$ unterscheiden müssen[3].

Lemma 2.3.3: Sei K ein Körper. Dann gilt:

1. $(W_n(K), \cdot)$ ist eine endliche, zyklische Untergruppe von $(K^*, \cdot)$, und ihre Ordnung teilt n.
2. Gilt $\mathrm{char}(K) \nmid n$ und ist $\overline{K}$ der algebraische Abschluss von K, so gilt $|W_n(\overline{K})| = |K_n| = n$.
3. Ist $\mathrm{char}(K) = p \in \mathbb{N}$, so gilt $W_{p^r m}(K) = W_m(K)$ für alle $m, r \in \mathbb{N}$.

Gilt $\mathrm{char}(K) \nmid n$, so heisst ein Element $w \in W_n(\overline{K})$ **primitive** n**te Einheitswurzel**, wenn es die Ordnung $o(w) = n$ hat. Dies ist äquivalent dazu, dass es die Gruppe $(W_n(K), \cdot)$ erzeugt.

[3] Man beachte dabei, dass diese Unterscheidung nur für $\mathrm{char}(K) = p \in \mathbb{N}$ prim relevant ist. Denn da 0 kein Teiler irgendeiner natürlichen Zahl n ist, gilt für $\mathrm{char}(K) = 0$ immer $\mathrm{char}(K) \nmid n$

Beweis:
1. Offensichtlich ist 1 eine $n$te Einheitswurzel für alle $n \in \mathbb{N}$. Das Produkt zweier $n$ter Einheitswurzeln $a, b \in K$ ist wegen $(a \cdot b)^n = a^n \cdot b^n = 1 \cdot 1 = 1$ wieder eine $n$te Einheitswurzel. Für jede $n$te Einheitswurzel $a \in K$ gilt ausserdem $a \neq 0$ und somit existiert ein multiplikatives Inverses a^{-1}, das wegen $1 = 1^n = (a \cdot a^{-1})^n = (a^{-1})^n$ auch wieder eine $n$te Einheitswurzel ist. Somit ist $(W_n(K), \cdot)$ eine endliche Untergruppe von $(K^*, \cdot)$ und daher nach Bemerkung 1.1.2, 5. zyklisch, also $W_n(K) = \langle a \rangle$ für ein $a \in W_n(K)$. Da $a^n = 1$ muss die Ordnung $o(a) = |W_n(K)|$ ein Teiler von n sein.

2. Offensichtlich sind die $n$ten Einheitswurzeln genau die Nullstellen des Polynoms $p = x^n - 1 \in K[x]$. Gilt $\mathrm{char}(K) \nmid n$, so folgt $p'(w) = nw^{n-1} = nw^{-1} \neq 0$. Also besitzt p keine mehrfachen Nullstellen in $\overline{K}$ und die Anzahl der $n$ten Einheitswurzeln ist $\deg(p) = n$.

3. Mit dem Frobeniusmonomorphismus folgt für $a \in K$

$$a^{p^r m} = 1 \quad \Leftrightarrow \quad 0 = (a^m)^{p^r} - 1 = (a^m - 1)^{p^r} \quad \Leftrightarrow \quad a^m = 1$$

und somit $W_{p^r m}(K) = W_m(K)$. □

Die dritte Aussage des Lemmas besagt, dass es im Fall eines Körpers der Charakteristik $\mathrm{char}(K) = p \in \mathbb{N}$ unnötig ist, $n$te Einheitswurzeln mit $n = mp^r$ zu betrachten, und es ausreicht, sich mit $m$ten Einheitswurzeln für $p \nmid m$ zu beschäftigen.

Aus der ersten Aussage des Lemmas ergibt such direkt, dass für $n = p \neq \mathrm{char}(K)$, jede Einheitswurzel $w \in W_n(\overline{K})^\times = W_n(\overline{K}) \backslash \{1\}$ primitiv ist, denn die Ordnung jeder Einheitswurzel muss die Gruppenordnung $|W_n(\overline{K})| = p$ teilen. Ist n keine Primzahl, so ergibt sich analog, dass eine Einheitswurzel genau dann primitiv ist, wenn ihre Ordnung nicht eins und kein echter Teiler von n ist. Daraus lässt sich für vorgegebenes $n \in \mathbb{N}$ leicht die Anzahl der primitiven Einheitswurzeln bestimmen, und wir erhalten das folgende Lemma.

Lemma 2.3.4: Sei K ein Körper, $n \in \mathbb{N}$ mit $\mathrm{char}(K) \nmid n$ und $w \in \overline{K}$ eine primitive $n$te Einheitswurzel. Dann gilt:

1. Der $n$te Kreisteilungskörper K_n ist isomorph zu $K(w)$.
2. Die Menge der primitiven $n$ten Einheitswurzeln ist $W_n^*(\overline{K}) = \{w^k : \mathrm{ggT}(k, n) = 1\}$ und enthält genau $\varphi(n)$ Elemente.

Beweis:
1. Per Definition ist jede primitive $n$te Einheitswurzel $w \in \overline{K}$ ein Erzeuger der zyklischen Gruppe $W_n(\overline{K})$. Es folgt $K_n = K(W_n(\overline{K})) = K(w)$.

2. Offensichtlich gilt $\langle w^k \rangle = W_n(\overline{K})$ genau dann, wenn $\mathrm{ggT}(n, k) = 1$ ist. Also ist die Anzahl der primitiven $n$ten Einheitswurzeln durch die Eulersche φ-Funktion $\varphi : \mathbb{N} \to \mathbb{N}$, $n \mapsto \varphi(n) = |\{k \in \mathbb{N} : 1 \leq k \leq n, \mathrm{ggT}(k, n) = 1\}|$ gegeben. □

Existiert also eine primitive $n$te Einheitswurzel, so ist die Körpererweiterung K_n/K nach der Lemma 2.3.4 primitiv. Daher ist es naheliegend zu fragen, wie das Minimalpolynom $m_{w,K}$ einer

primitiven $n$ten Einheitswurzel $w \in K_n$ über K aussieht. Da K_n der Zerfällungskörper von $x^n - 1$ über K ist, muss $m_{w,K}$ das Polynom $x^n - 1$ teilen. Das Polynom $x^n - 1$ selbst kommt nicht in Frage, da es reduzibel ist: $x^n - 1 = (x-1)(1 + x + \ldots + x^{n-1})$ für alle $n \in \mathbb{N}$. Ist $n = p \in \mathbb{N}$ prim, so ist bekannt, dass das Kreisteilungspolynom $1 + x + \ldots + x^{p-1}$ irreduzibel ist, und ist daher das Minimalpolynom von w sein. Ist aber $n \in \mathbb{N}$ keine Primzahl, so kann das Polynom $1 + x + \ldots + x^{n-1}$ jedosch in weitere Linearfaktoren zerfallen. Beispielsweise gilt $1+x+x^2+x^3 = (x+1)(x^2+1)$ und $1+x+x^2+x^3+x^4+x^5 = (1+x)(1+x+x^2)(1-x+x^2)$.

Es liegt nahe, zu vermuten, dass Polynom $1 + x + \ldots + x^{n-1}$ reduzibel ist, genau dann, wenn n eine Primzahl ist, und dass die Teiler von n den Linearfaktoren in $x^n - 1$ entsprechen. Andererseits entsprechen Teiler d von n mit $1 < d < n$ nach Lemma 2.3.4 genau den nicht-primitiven $n$ten Einheitswurzeln, was suggeriert, dass das Minimalpolynom $m_{w,\mathbb{Q}}$ das Produkt der Linearfaktoren $(x - u)$ für primitive Einheitswurzeln $u \in W_n(\overline{K})$ sein sollte.

Definition 2.3.5: Sei K ein Körper und $n \in \mathbb{N}$ mit $\mathrm{char}(K) \nmid n$. Dann nennt man das Polynom

$$\Phi_{n,K} = \prod_{w \in W_n(\overline{K}) \text{primitiv}} (x - w) \in K_n[x]$$

das $n$te **Kreisteilungspolynom** über K. Für $K = \mathbb{Q}$ schreibt man auch Φ_n statt $\Phi_{n,\mathbb{Q}}$ und spricht vom $n$ten Kreisteilungspolynom.

Um zu zeigen, dass das Kreisteilungspolynom $\Phi_{n,K}$ ein Kandidat für das Minimalpolynom einer primitiven $n$ten Einheitswurzel w über K ist, müssen wir zeigen, dass es ein Polynom mit Koeffizienten in K ist und ausserdem seinen Zusammenhang mit dem Polynom $x^n - 1$ präzise formulieren können. Dies leistet das folgende Lemma.

Lemma 2.3.6: Sei K ein Körper.

1. Gilt $\mathrm{char}(K) \nmid n$ so ist $x^n - 1 = \prod_{0<d|n} \Phi_{d,K}$.
2. Das $n$te Kreisteilungspolynom $\Phi_n = \Phi_{n,\mathbb{Q}}$ ist normiert, vom Grad $\varphi(n)$ und $\Phi_n \in \mathbb{Z}[x]$.
3. Ist $\Phi_n = \sum_{j=0}^{\varphi(n)} k_j x^j$, so ist das $n$te Kreisteilungspolynom $\Phi_{n,K}$ über K gegeben durch $\Phi_{n,K} = \sum_{j=0}^{\varphi(n)} k_j x^j$, wobei $k_j = \underbrace{1 + \ldots + 1}_{k_j \times} \in P(K)$.

Beweis:
1. Das Polynom $x^n - 1$ zerfällt über $\overline{K}$ in Linearfaktoren, und hat nach Lemma 2.3.3 nur einfache Nullstellen in $\overline{K}$. Die Nullstellen sind gerade die $n$ten Einheitswurzeln. Ist $w \in W_n(\overline{K})$ eine Einheitswurzel der Ordnung $o(w) = d$, so muss gelten $d|n$, denn die Ordnung jedes Elements der Gruppe $W_n(\overline{K})$ teilt die Gruppenordnung. In diesem Fall ist und w dann eine primitive $d$te Einheitswurzel. Also gilt $W_n(\overline{K}) = \dot{\bigcup}_{0<d|n} \{w \in W_d(\overline{K}) : w \,\text{primitiv}\}$, und es folgt

$$x^n - 1 = \prod_{w \in W_n(\overline{K})} (x - w) = \prod_{0<d|n} \prod_{\substack{w \in W_d(\overline{K}) \\ \text{primitiv}}} (x - w) = \prod_{0<d|n} \Phi_{d,K}$$

2. Φ_d ist offensichtlich normiert und $\deg(\Phi_n) = |\{w \in W_n(\overline{K}) \,\text{primitiv}\}| = \varphi(n)$ nach Lemma 2.3.4. Wir beweisen die Aussagen 2. und 3. per Induktion über $n \in \mathbb{N}$.
$n = 1$**:** Ist $n = 1$, so gilt $\Phi_1(x) = x - 1 \in \mathbb{Z}[x]$ und $\Phi_{1,K} = x - 1_K \in P(K)[x]$.

$n \to n+1$**:** Seien die Aussagen 2.,3. bewiesen für alle Kreisteilungspolynome Φ_m und $\Phi_{m,K}$ mit $m \leq n$. Nach 1. gilt

$$x^{n+1} - 1 = \Phi_{n+1,K} \cdot \prod_{\substack{d|n+1,\\ 0<d<n+1}} \Phi_{d,K} = \Phi_{n+1,K} \cdot \Psi_{n+1,K}. \tag{1}$$

Nach Induktionsvoraussetzung ist $\Psi_{n+1} = \Psi_{n+1,\mathbb{Q}}$ normiert mit ganzzahligen Koeffizienten. Also existieren Polynome $q, r \in \mathbb{Z}[x]$ mit $x^{n+1} - 1 = q\Psi_{n+1} + r$ und $\deg(r) < \deg(\Psi_{n+1})$ oder $\deg(r) = 0$. Mit (1) folgt $(\Phi_{n+1} - q)\Psi_{n+1} = r$ und aus Gradgründen muss $r = 0$ und $\Phi_{n+1} = q \in \mathbb{Z}[x]$ gelten.

Für den Primkörper $P(K)$ gilt $P(K) = \mathbb{Q}$ oder $P(K) = \mathbb{F}_p$ mit $p \in \mathbb{N}$ prim. Im ersten Fall ist 3. bereits bewiesen. Im zweiten Fall betrachtet man den von der Projektion $\pi : \mathbb{Z} \to \mathbb{F}_p$, $k \mapsto \overline{k}$ induzierten Ringhomomorphismus $\pi_* : \mathbb{Z}[x] \to \mathbb{F}_p[x]$, $\sum_{j=0}^n k_j x^j \mapsto \sum_{j=0}^n \overline{k_j} x^j$. Dann gilt

$$\Phi_{n+1,K} \cdot \Psi_{n+1,K} = x^{n+1} - \overline{1} = \pi_*(x^{n+1} - 1) = \pi_*(\Phi_{n+1} \cdot \Psi_{n+1}) = \pi_*(\Phi_{n+1}) \cdot \pi_*(\Psi_{n+1})$$

Da nach Induktionsvoraussetzung $\Phi_{m,K} = \pi_*(\Phi_m)$ für alle $m \leq n$ folgt mit (1) dass $\Psi_{n+1,K} = \pi_*(\Psi_{n+1})$ gelten muss und somit $\Phi_{n+1,K} = \pi_*(\Phi_{n+1})$. □

Bemerkung 2.3.7:

1. Die dritte Aussage in Lemma 2.3.6 besagt, dass man das $n$te Kreisteilungspolynom für einen Körper der Charakteristik $p \in \mathbb{N}$ prim aus dem $n$ten Kreisteilungspolynom für $\mathbb{Q}$ berechnen kann, indem man die Koeffizienten modulo p reduziert.
2. Aus der im Beweis hergeleiteten Identität $W_n(\overline{K}) = \dot{\bigcup}_{0<d|n}\{w \in W_d(\overline{K}) : w \text{ primitiv}\}$ ergibt sich mit Lemma 2.3.3 für $\mathrm{char}(K) \nmid n$ die Identität
$$n = |W_n(\overline{K})| = \sum_{0<d|n} |\{w \in W_d(\overline{K}) : w \text{ primitiv}\}| = \sum_{0<d|n} \varphi(d).$$
3. Mit Hilfe von (1) lassen sich die Kreisteilungspolynome rekursiv berechnen und die Polynome $x^n - 1$ in Kreisteilungspolynome faktorisieren. Man erhält
$$\begin{aligned}
&x - 1 = \Phi_1 \\
&x^2 - 1 = (x+1)(x-1) = \Phi_2 \cdot \Phi_1 && \Rightarrow \quad \Phi_2 = x + 1 \\
&x^3 - 1 = (1 + x + x^2)(x-1) = \Phi_3 \cdot \Phi_1 && \Rightarrow \quad \Phi_3 = x^2 + x + 1 \\
&x^4 - 1 = (x^2+1)(x+1)(x-1) = \Phi_4 \cdot \Phi_2 \cdot \Phi_1 && \Rightarrow \quad \Phi_4 = 1 + x^2 \\
&x^5 - 1 = (1 + x + x^2 + x^3 + x^4)(x-1) = \Phi_5 \cdot \Phi_1 && \Rightarrow \quad \Phi_5 = x^4 + x^3 + x^2 + x + 1 \\
&x^6 - 1 = (x^2 - x + 1)(x^2 + x + 1)(x+1)(x-1) && \Rightarrow \quad \Phi_6 = x^2 - x + 1 \\
&\qquad = \Phi_6 \cdot \Phi_3 \cdot \Phi_2 \cdot \Phi_1
\end{aligned}$$
Für die Kreisteilungspolynome Φ_p mit $p \in \mathbb{N}$ prim ergibt sich dabei aus $x^p - 1 = \Phi_p \cdot \Phi_1$ die bekannte Formel $\Phi_p = 1 + x + x^2 + \ldots + x^{p-1}$.

Mit Hilfe der expliziten Beschreibung der Kreisteilungspolynome in Lemma 2.3.6 und ihrer Beziehung zu den Polynomen $x^n - 1$ können wir nun beweisen, dass die Kreisteilungspolynome $\Phi_n \in \mathbb{Z}[x]$ irreduzibel über $\mathbb{Q}$ sind. Da die Kreisteilungspolynome ausserdem normiert sind und per Definition $\Phi_n(w) = 0$ für jede primitive $n$te Einheitswurzel $w \in W_n(\mathbb{C})$, folgt daraus dann direkt, dass $\Phi_n(w)$ das Minimalpolynom jeder primitiven $n$ten Einheitswurzel ist.

Satz 2.3.8: Für jedes $n \in \mathbb{N}$ ist das $n$te Kreisteilungspolynom Φ_n irreduzibel über $\mathbb{Q}$.

Beweis:
1. Da Φ_n normiert ist, existiert ein normiertes irreduzibles Polynom $f \in \mathbb{Z}[x]$ mit $f|\Phi_n$. Zu zeigen ist, dass $f = \Phi_n$ gilt. Dazu benutzen wir die folgende Hilfsaussage:

(*) Für jede Nullstelle $w \in \mathbb{Q}_n$ von f und jede Primzahl $p \in \mathbb{N}$ mit $p \nmid n$ gilt $f(w^p) = 0$.

Ist $w \in \mathbb{Q}_n$ eine Nullstelle von f, so ist w auch eine Nullstelle von Φ_n und somit eine primitive $n$te Einheitswurzel. Mit (*) folgt $f(w^p) = 0$ für alle $p \in \mathbb{N}$ prim mit $\mathrm{ggT}(p, n) = 1$. Also ist auch w^p wieder eine Nullstelle von f und somit eine primitive $n$te Einheitswurzel. Ist $k \in \mathbb{N}$ mit $\mathrm{ggT}(k, n) = 1$, so existieren Primzahlen $p_1, ..., p_r$ mit $k = p_1 \cdots p_r$ und $\mathrm{ggT}(p_i, n) = 1$ für alle $i = 1, ..., r$. Durch wiederholtes Anwenden von (*) folgt $f(w^k) = 0$ und somit ist auch w^k eine primitive $n$te Einheitswurzel. Da $o(w) = n$ sind die Elemente $1, w, ..., w^{n-1}$ echt verschieden, und daher existieren mindestens $\varphi(n) = |\{k \in \mathbb{N} : k \leq n, \mathrm{ggT}(k, n) = 1\}|$ verschiedene Nullstellen von f. Also folgt $\deg(f) \geq \varphi(n) = \deg(\Phi_n)$ und $f = \Phi_n$.

2. Beweis der Hilfsaussage (*): Aus $f|\Phi_n$ und $\Phi_n|x^n - 1$ folgt $f|x^n - 1$ und somit existiert ein Polynom $g \in \mathbb{Z}[x]$ mit $x^n - 1 = f \cdot g$. Wir nehmen an, dass eine Nullstelle w von f existiert mit $f(w^p) \neq 0$ und führen dies zum Widerspruch.

Da w^p eine Nullstelle von $x^n - 1$ ist, folgt aus $f(w^p) \neq 0$ dass $g(w^p) = 0$ gelten muss, d. h. w ist eine Nullstelle des Polynoms $q = g(x^p)$. Andererseits ist aber das normierte irreduzible Polynom f das Minimalpolynom aller Nullstellen von $x^n - 1$, also $f = m_{w,\mathbb{Q}}$. Aus $g(w^p) = 0$ folgt dann $f|q$ in $\mathbb{Q}[x]$. Also existiert ein Polynom $r \in \mathbb{Q}[x]$ mit $q = g(x^p) = f \cdot r$. Da $f, q \in \mathbb{Z}[x]$ und f irreduzibel ist, folgt $r \in \mathbb{Z}[x]$.

Sei $\pi : \mathbb{Z} \to \mathbb{F}_p$, $k \mapsto \overline{k} = k + p\mathbb{Z}$ die Projektionsabbildung und $\pi_* : \mathbb{Z}[x] \to \mathbb{F}_p[x]$, $\sum_{j=0}^m k_j x^j \mapsto \sum_{j=0}^m \overline{k_j} x^j$ der induzierte Ringhomomorphismus. Mit dem Frobeniusmonomorphismus folgt für $g = \sum_{j=0}^m k_j x^j \in \mathbb{Z}[x]$

$$\pi_*(g)^p = \left(\sum_{j=0}^m \overline{k_j} x^j \right)^p = \sum_{j=0}^m \overline{k_j} x^{pj} = \pi_*(g(x^p)) = \pi_*(q) = \pi_*(f \cdot r) = \pi_*(f) \cdot \pi_*(r).$$

Ist nun $h \in \mathbb{F}_p[x]$ ein irreduzibler Faktor von $\pi_*(f)$, so folgt aus $\pi_*(f)\pi_*(r) = \pi_*(g(x^p)) = \pi_*(g)^p$ die Identität $h|\pi_*(g)$ und somit $h^2|\pi_*(f)\pi_*(g) = x^n - \overline{1}$. Also hat $x^n - \overline{1}$ eine mehrfache Nullstelle im algebraischen Abschluss $\overline{\mathbb{F}_p}$. Andererseits gilt aber $(x^n - 1)'(w) = \overline{n} w^{n-1}$ und $\overline{n}, w \neq 0$ - ein Widerspruch zu Lemma 1.5.8. Also muss $f(w^p) = 0$ gelten. □

Korollar 2.3.9: Das $n$te Kreisteilungspolynom Φ_n ist das Minimalpolynom jeder primitiven $n$ten Einheitswurzel $w \in W_n(\mathbb{C})$.

Bemerkung 2.3.10: Die Voraussetzung $K = \mathbb{Q}$ in Satz 2.3.8 ist notwendig. Aus

$$x^{12} - 1 = (x - 1)(x + 1)(1 + x + x^2)(1 + x^2)(x^2 - x + 1)(x^4 - x^2 + 1)$$

erhält man das 12te Kreisteilungspolynom $\Phi_{12} = x^4 - x^2 + 1$ über $\mathbb{Q}$ und das 12te Kreisteilungspolynom über $\mathbb{F}_5$, indem man seine Koeffizienten modulo 5 betrachtet. Dieses ist aber reduzibel, denn es gilt

$$x^4 - x^2 + \overline{1} = (x^2 - \overline{2}x - \overline{1}) \cdot (x^2 + \overline{2}x - \overline{1}).$$

Mit Hilfe der bewiesenen Aussagen über $n$te Einheitswurzeln und Kreisteilungspolynome können wir nun die Eigenschaften der Körpererweiterung K_n/K untersuchen und insbesondere ihre Galoisgruppe bestimmen.

Lemma 2.3.11: Sei K ein Körper und $n \in \mathbb{N}$ mit $\mathrm{char}(K) \nmid n$. Dann gilt:

1. Die Körpererweiterung K_n/K ist galoissch.
2. Die Galoisgruppe $\Gamma(K_n/K)$ ist isomorph zu einer Untergruppe der Gruppe $((\mathbb{Z}/n\mathbb{Z})^\times, \cdot)$.
3. Es gilt $\Gamma(K_n/K) \cong (\mathbb{Z}/n\mathbb{Z})^\times$ genau dann, wenn $\Phi_{n,K}$ irreduzibel über K ist.

Beweis:
1. Das Polynom $x^n - 1$ besitzt nach Lemma 2.3.3 genau n verschiedene Nullstellen in seinem Zerfällungskörper K_n und ist somit separabel über K. Da K_n Zerfällungskörper von $x^n - 1$ ist, ist die Körpererweiterung K_n/K ausserdem normal und somit nach Satz 2.2.1 galoissch.

2. Sei nun $w \in K_n$ eine primitive $n$te Einheitswurzel. Nach Lemma 2.3.4 gilt dann $K_n = K(w)$, und somit ist jeder K-Automorphismus $\tau \in \Gamma(K_n/K)$ durch $\tau(w)$ eindeutig bestimmt. Wegen $o(\tau(w)) = o(w)$ bildet τ primitive $n$te Einheitswurzeln auf primitive $n$te Einheitswurzeln ab. Also existiert ein $k \in \mathbb{Z}$ mit $\mathrm{ggT}(n,k) = 1$ und $\tau(w) = w^k$. Das zugehörige Element $\overline{k} = \pi(k) \in \mathbb{Z}/n\mathbb{Z}$ ist dadurch eindeutig bestimmt, und man erhält eine Abbildung

$$i : \Gamma(K_n/K) \to (\mathbb{Z}/n\mathbb{Z})^\times, \quad \tau \mapsto i(\tau) = \overline{k}$$

in die Menge der multiplikativen Einheiten $(\mathbb{Z}/n\mathbb{Z})^\times = \{\overline{k} \in \mathbb{Z}/n\mathbb{Z} : \mathrm{ggT}(n,k) = 1\}$. Da für $\sigma \in \Gamma(K_n/K)$ mit $i(\sigma) = \overline{k'}$ gilt $\sigma \circ \tau(w) = \tau(w)^{k'} = w^{kk'} = \sigma(w)^k = \tau \circ \sigma(w)$ folgt $i(\sigma \circ \tau) = i(\tau \circ \sigma) = i(\tau) \cdot i(\sigma)$. Somit ist i ein Gruppenhomomorphismus von $\Gamma(K_n/K)$ in die multiplikative Gruppe $((\mathbb{Z}/n\mathbb{Z})^\times, \cdot)$. Da aus $i(\tau) = 1$ folgt $\tau(w) = w$, ist i injektiv. Also ist $\Gamma(K_n/K) \cong i(\Gamma(K_n/K)) \subset (\mathbb{Z}/n\mathbb{Z})^\times$ isomorph zu einer Untergruppe von $((\mathbb{Z}/n\mathbb{Z})^\times, \cdot)$.

3. Da die Körpererweiterung K_n/K eine Galoiserweiterung ist, gilt nach dem Hauptsatz der endlichen Galoistheorie $[K_n : K] = |\Gamma(K_n/K)|$. Ist $\Phi_{n,K}$ irreduzibel, so folgt $|\Gamma(K_n/K)| = [K_n : K] = \deg(\Phi_{n,K}) = \varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$. Ist $\Phi_{n,K}$ reduzibel, so ergibt sich $|\Gamma(K_n/K)| = [K_n : K] < \deg(\Phi_{n,K}) = |(\mathbb{Z}/n\mathbb{Z})^\times|$. □

Beispiel 2.3.12:

1. Die Galoisgruppe der Körpererweiterung $\mathbb{Q}_n/\mathbb{Q}$ ist isomorph zu $((\mathbb{Z}/n\mathbb{Z})^\times, \cdot)$, denn nach Satz 2.3.8 ist das Kreisteilungspolynom Φ_n irreduzibel über $\mathbb{Q}$ für alle $n \in \mathbb{N}$.
2. Wir bestimmen die Zwischenkörper der Körpererweiterung $\mathbb{Q}_9/\mathbb{Q}$ und die Untergruppen der Galoisgruppe $\Gamma(\mathbb{Q}_9/\mathbb{Q}) \cong ((\mathbb{Z}/9\mathbb{Z})^\times, \cdot)$. Es gilt

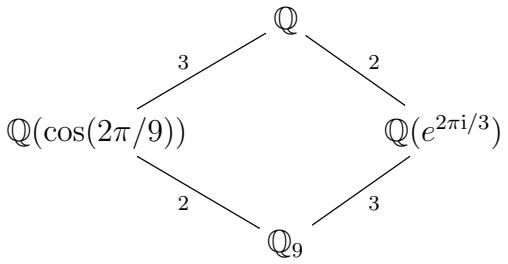
$$(\mathbb{Z}/9\mathbb{Z})^\times = \{\overline{k} : k \in \{1, ..., 8\}, \mathrm{ggT}(k,9) = 1\} = \{\overline{1}, \overline{2}, \overline{4}, \overline{5}, \overline{7}, \overline{8}\}.$$

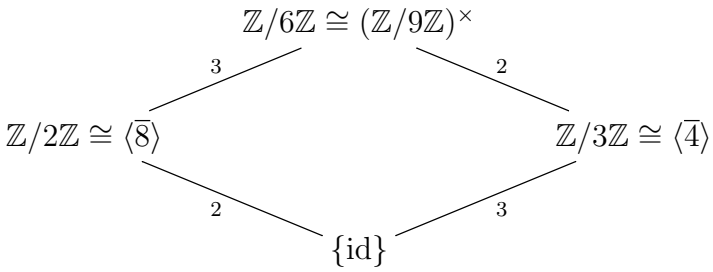
   Dies ist eine endliche abelsche Gruppe der Ordnung $\varphi(9) = 6$ und somit nach dem Klassifikationssatz für endliche abelsche Gruppen isomorph zu der Gruppe $\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. Neben der trivialen Gruppe und sich selbst hat $\mathbb{Z}/6\mathbb{Z}$ also die Untergruppen $\mathbb{Z}/2\mathbb{Z}$ und $\mathbb{Z}/3\mathbb{Z}$. Wegen $8^2 = 4^3 = 64 = 1 \bmod 9$ entspricht $\mathbb{Z}/2\mathbb{Z}$ der Untergruppe $\langle\overline{8}\rangle \subset (\mathbb{Z}/9\mathbb{Z})^\times$ und $\mathbb{Z}/3\mathbb{Z}$ der Untergruppe $\langle\overline{4}\rangle \subset (\mathbb{Z}/9\mathbb{Z})^\times$.

Für die zugehörigen Fixkörper gilt $[\mathcal{F}(\mathbb{Z}/2\mathbb{Z}) : \mathbb{Q}] = 3$, $[\mathcal{F}(\mathbb{Z}/3\mathbb{Z}) : \mathbb{Q}] = 3$, denn für jede Untergruppe $G \subset \Gamma(\mathbb{Q}_9/\mathbb{Q})$ folgt mit dem dem Gradsatz und dem Hauptsatz der endlichen Galoistheorie

$$6 = \varphi(9) = [\mathbb{Q}_9 : \mathbb{Q}] = [\mathbb{Q}_9 : \mathcal{F}(G)] \cdot [\mathcal{F}(G) : \mathbb{Q}] = |G| \cdot [\mathcal{F}(G) : \mathbb{Q}].$$

Wegen $e^{4\cdot 2\pi \mathrm{i}/3} = e^{2\pi \mathrm{i}/3}$ gilt $\mathbb{Q}(e^{2\pi \mathrm{i}/3}) \subset \mathcal{F}(\mathbb{Z}/3\mathbb{Z})$ und mit $[\mathcal{F}(\mathbb{Z}/3\mathbb{Z}) : \mathbb{Q}] = \deg_{\mathbb{Q}}(e^{2\pi \mathrm{i}}/3)$ folgt $\mathcal{F}(\mathbb{Z}/3\mathbb{Z}) = \mathbb{Q}(e^{2\pi \mathrm{i}/3}) = \mathbb{Q}(\frac{1}{2} + \frac{1}{2}\mathrm{i}\sqrt{3}) = \mathbb{Q}(\sqrt{3}\mathrm{i})$.
Wegen $e^{8\cdot 2\pi \mathrm{i}/9} = e^{-2\pi \mathrm{i}/9}$ und $e^{-8\cdot 2\pi \mathrm{i}/9} = e^{2\pi \mathrm{i}/9}$ gilt $\mathbb{Q}(\cos(2\pi/9)) \subset \mathcal{F}(\mathbb{Z}/2\mathbb{Z})$. Da $[\mathcal{F}(\mathbb{Z}/2\mathbb{Z}) : \mathbb{Q}] = 3$ eine Primzahl ist und $\cos(2\pi/9) \notin \mathbb{Q}$ folgt $\mathbb{Q}(\cos(2\pi/9)) = \mathcal{F}(\mathbb{Z}/2\mathbb{Z})$. Also erhält man die folgenden Zwischenkörper- und Untergruppendiagramme





Wir befassen uns nun noch mit den Kreisteilungskörpern für Körper der Charakteristik p. Um die Kreisteilungskörper K_n für $K = \mathbb{F}_q$ und ihre Galoisgruppen zu charakterisieren, beschränkt man sich auf den Fall $\mathrm{char}(k) \nmid n$. Da K_n ein endlicher Körper ist, gilt dann $K^n = \mathbb{F}_{q^s}$ mit $s \in \mathbb{N}$, und die Galoisgruppe $\Gamma(K_n/K)$ wird von $F_q : K_n \to K_n$, $\alpha \mapsto \alpha^q$ erzeugt. Dies erlaubt es einem, den Grad der Körpererweiterung K_n/K zur Ordnung von $\overline{p} \in \mathbb{Z}/n\mathbb{Z}$ in der Gruppe $((\mathbb{Z}/n\mathbb{Z})^\times, \cdot)$ in Beziehung zu setzen.

Lemma 2.3.13: Sei $K = \mathbb{F}_q$ mit einer Primpotenz $q = p^r \in \mathbb{N}$ und $n \in \mathbb{N}$ mit $p \nmid n$. Dann gilt $[K_n : K] = o(\overline{q})$ und $K_n \cong \mathbb{F}_{q^{o(\overline{q})}}$, wobei $o(\overline{q})$ die Ordnung der Restklasse von q in der Gruppe $((\mathbb{Z}/n\mathbb{Z})^\times, \cdot)$ bezeichnet.

Beweis:
Die Körpererweiterung K_n/K ist nach Lemma 2.3.11 galoissch und ausserdem endlich. Nach dem Hauptsatz der endlichen Galoistheorie gilt daher $|\Gamma(K_n/K)| = [K_n : K]$. Nach Lemma 1.6.7 ist $\Gamma(K_n/K)$ zyklisch und wird von $\psi : K_n \to K_n$, $\alpha \mapsto \alpha^q$ erzeugt. Also hat $\psi \in \Gamma(K_n/K)$ die Ordnung $[K_n : K]$. Da $K_n = K(w)$ für jede primitive Einheitswurzel $w \in K_n$, ist jedes Element von $\Gamma(K_n/K)$ durch seinen Wert auf w eindeutig bestimmt, und für $k \in \mathbb{N}$ gilt

$$\psi^k = \mathrm{id}_{K_n} \quad \Leftrightarrow \quad \psi^k(w) = w^{q^k} = w \quad \Leftrightarrow \quad n | q^k - 1 \quad \Leftrightarrow \quad \overline{q}^k = \overline{1}.$$

Also folgt $[K_n : K] = \min\{k \in \mathbb{N} : \psi^k = \mathrm{id}\} = \min\{k \in \mathbb{N} : \overline{q}^k = \overline{1}\} = o(\overline{q})$. □

Beispiel 2.3.14:

1. Für $n = 10$ sind die zu n teilerfremden Primpotenzen $q \in \{1, ..., n\}$ gerade $q = 3, 7, 9$. In der Gruppe $((\mathbb{Z}/10\mathbb{Z})^\times, \cdot)$ gilt $o(\overline{3}) = 4 = o(\overline{7})$ und $o(\overline{9}) = 2$, denn $3^2 = 9 = -1 \bmod 10$ und $7^2 = 49 = -1 \bmod 10$. Also folgt $(\mathbb{F}_3)_{10} \cong (\mathbb{F}_9)_{10} \cong \mathbb{F}_{81}$ und $(\mathbb{F}_7)_{10} \cong \mathbb{F}_{2401}$.
2. Für $n = 5$ sind die zu n teilerfremden Primpotenzen $q = 2, 3, 4$ und ihre Ordnungen in $\mathbb{Z}/5\mathbb{Z}$ sind $o(\overline{2}) = 4 = o(\overline{3})$, $o(\overline{4}) = 2$. Also folgt $(\mathbb{F}_2)_5 \cong (\mathbb{F}_4)_5 \cong \mathbb{F}_{16}$ und $(\mathbb{F}_3)_5 \cong \mathbb{F}_{81}$.

2.4 Übungen zu Kapitel 2

Aufgabe 1: Untersuchen Sie, welche der folgenden Körpererweiterungen galoissch sind:

(a) $\mathbb{Q}(\sqrt[5]{2})/\mathbb{Q}$.
(b) $\mathbb{Q}(\sqrt[6]{2}, \sqrt{3}\mathrm{i})/\mathbb{Q}$
(c) $\mathbb{Q}(t)/\mathbb{Q}(t^2)$ mit $t \in \mathbb{R}$ transzendent über $\mathbb{Q}$.
(d) $Q(\mathbb{F}_p[t])/Q(\mathbb{F}_p[t^p])$ mit $p \in \mathbb{N}$ prim.

Aufgabe 2: Sei $f \in \mathbb{Q}[x]$ ein Polynom mit einer Galoisgruppe ungerader Ordnung. Zeigen Sie, dass f dann nur reelle Nullstellen haben kann.

Aufgabe 3: Sei $K(S)/K$ eine Körpererweiterung, so dass jedes Element $s \in S$ Grad 2 über K hat. Zeigen Sie:

(a) Für alle $\sigma \in \Gamma(K(S)/K)$ gilt $\sigma^2 = \sigma \circ \sigma = \mathrm{id}_{K(S)}$.
(b) $\Gamma(K(S)/K)$ ist abelsch.
(c) Gilt $[K(S) : K] < \infty$, so ist $\Gamma(K(S)/K) \cong \mathbb{Z}/2\mathbb{Z} \times \ldots \times \mathbb{Z}/2\mathbb{Z}$.

Aufgabe 4: Wir betrachten den Körper $L = Q(\mathbb{C}[x])$ der gebrochen rationalen Funktionen mit Koeffizienten in $\mathbb{C}$.

(a) Zeigen Sie, dass durch $\sigma(x) = e^{2\pi\mathrm{i}/n} \cdot x$ mit $n \geq 3$ und $\tau(x) = 1/x$ $\mathbb{C}$-Isomorphismen von L definiert werden. Warum sind diese durch ihren Wert auf dem Polynom x eindeutig bestimmt?
(b) Bestimmen Sie die Ordnung der Elemente $\sigma, \tau \in \Gamma(L/\mathbb{Q})$ und zeigen Sie $\tau \circ \sigma \circ \tau^{-1} = \sigma^{-1}$.
(c) Folgern Sie, dass die von σ und τ erzeugte Untergruppe $G := \langle \sigma, \tau \rangle \subset \Gamma(L/\mathbb{C})$ isomorph zur Diedergruppe D_n ist.
(d) Berechnen Sie $\tau^i \circ \sigma^j(x^n + x^{-n})$ für $i \in \{0, 1\}$ und $j \in \{0, ..., n-1\}$ und folgern Sie $x^n + x^{-n} \in \mathcal{F}(G)$.
(e) Zeigen Sie: $\mathcal{F}(G) = Q(\mathbb{C}[x^n + x^{-n}])$.

Hinweis: Die Diedergruppe D_n ist die von der Spiegelung S an der reellen Achse und der Drehung D um $2\pi/n$ erzeugte Untergruppe der Symmetriegruppe eines regulären n-gons mit Ecken $e^{2\pi\mathrm{i}k/n}$, $k = 0, ..., n-1$ auf dem Einheitskreis. Sie ist gegeben durch die Erzeuger S, D und die Relationen $SDS^{-1} = D^{-1}$, $SD = D^{-1}S$, $DS = SD^{-1}$, und es gilt $D_n = \{S^i D^j : i = 0, 1, j =\in \mathbb{Z}\}$.

Aufgabe 5: Sei $\alpha = \sqrt{5 + 2\sqrt{5}}$.

(a) Bestimmen Sie das Minimalpolynom von α über $\mathbb{Q}$.
(b) Zeigen Sie, dass $\mathbb{Q}(\alpha)/\mathbb{Q}$ galoissch ist.
(c) Bestimmen Sie die Galoisgruppe von $\mathbb{Q}(\alpha)/\mathbb{Q}$.

Aufgabe 6: Sei K ein Körper, $f = a_n x^n + \ldots + a_1 x + a_0 \in K[x]$ ein nicht-konstantes Polynom mit $a_n a_0 \neq 0$ und $g = a_0 x^n + \ldots + a_{n-1} x + a_n \in K[x]$ (das *sogenannte zu f reziproke Polynom*). Zeigen Sie, dass f und g die selbe Galoisgruppe haben.

Aufgabe 7: Wir betrachten die Körpererweiterung $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$.

(a) Zeigen Sie, dass $\Gamma(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
(b) Berechnen Sie für alle Elemente $\sigma \in \Gamma(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$ das Bild des Elements $a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$ mit $a, b, c, d \in \mathbb{Q}$ unter σ.
(c) Bestimmen Sie für alle Untergruppen $U \subset \Gamma(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$ den zugehörigen Fixkörper.

Aufgabe 8: Sei $p \in \mathbb{N}$ prim, $n, m \in \mathbb{N}$ und $L/\mathbb{F}_{p^n}$ eine Körpererweiterung vom Grad $[L : \mathbb{F}_{p^n}] = m$. Bestimmen sie die Galoisgruppen $\Gamma(L/\mathbb{F}_p)$ und $\Gamma(L/\mathbb{F}_{p^n})$. Sind diese Körpererweiterungen galoissch?

Aufgabe 9: Sei K ein Körper, $f \in K[x]$, L der Zerfällungskörper von f und

$$N = \{\alpha \in L : f(\alpha) = 0\}$$

die Nullstellenmenge von f. Zeigen Sie:

(a) Für jedes Element $\tau \in \Gamma(L/K)$ ist $\tau|_N : N \to N$ eine Permutation.
(b) Die Grupppenordnung $|\Gamma(L/K)|$ ist ein Teiler von $|N|$!
(c) Ist $f \in K[x]$ irreduzibel, so operiert die Galoisgruppe $\Gamma(L/K)$ **transitiv** auf N, d. h. zu beliebigen Nullstellen $\alpha, \beta \in L$ von f existiert ein K-Automorphismus $\tau \in \Gamma(L/K)$ mit $\tau(\alpha) = \beta$.

Aufgabe 10: Zeigen Sie, dass für jedes irreduzible Polynom der Form $x^3 + ax + b \in \mathbb{Q}[x]$ mit $a > 0$ die Galoisgruppe von f isomorph zur Permutationsgruppe S_3 ist.

Aufgabe 11: Wir betrachten das Polynom $f = x^4 - 2 \in \mathbb{Q}[x]$.

(a) Bestimmen Sie den Zerfällungskörper L von $f = x^4 - 2$ über $\mathbb{Q}$.
(b) Bestimmen Sie die Galoisgruppe $\Gamma(L/\mathbb{Q})$.
(c) Bestimmen sie alle Untergruppen von $\Gamma(L/\mathbb{Q})$ und die zugehörigen Zwischenkörper. Stellen Sie Ihre Ergebnisse grafisch in Zwischenkörperdiagrammen und Untergruppendiagrammen dar.
(d) Untersuchen Sie, für welche Zwischenkörper $\mathbb{Q} \subset E \subset L$ die Körpererweiterung $E/\mathbb{Q}$ galoissch ist.

Aufgabe 12: Bestimmen Sie die Galoisgruppe des Polynoms $p = x^4 - 13x^2 + 1 \in \mathbb{Q}[x]$ über $\mathbb{Q}$ sowie alle Untergruppen der Galoisgruppe und die zugehörigen Fixkörper.

Aufgabe 13: Sei L/K eine algebraische Galoiserweiterung. Zeigen Sie:

(a) Ist $\alpha \in L$ mit $\tau(\alpha) \neq \alpha$ für alle $\tau \in \Gamma(L/K) \setminus \{\mathrm{id}_L\}$, so folgt $L = K(\alpha)$.
(b) Ist L/K endlich, so existiert für jede Untergruppe $G \subset \Gamma(L/K)$ ein Element $\alpha \in L$ mit $G = \mathcal{G}(\{\alpha\}) = \{\phi \in \Gamma(L/K) : \phi(\alpha) = \alpha\}$.

Aufgabe 14: Seien $\alpha_0, \alpha_1, ..., \alpha_4 \in \mathbb{C}$ die Ecken des regelmäßigen Fünfecks in der komplexen Ebene mit Mittelpunkt $0 \in \mathbb{C}$ und einer Ecke in $1 \in \mathbb{C}$.

(a) Zeigen Sie, dass die Ecken gegeben sind durch $\alpha_k = e^{2\pi \mathrm{i} k/5}$ für $k = 0, ..., 4$.
(b) Geben Sie die Ecken $\beta_0, ..., \beta_4$ eines regelmässigen Fünfecks an, das entsteht, wenn das Fünfeck in (a) um 30° gegen den Uhrzeigersinn gedreht wird und dann so verschoben wird, dass es den Mittelpunkt $1 + \mathrm{i}$ hat.

(c) Existiert ein normiertes Polynom $p \in \mathbb{Q}[x]$ fünften Grades mit Nullstellenmenge $\{\alpha_0, ..., \alpha_4\}$? Wenn ja, geben Sie es an und zerlegen Sie es in irreduzible Faktoren. Wenn nein, begründen Sie, warum es nicht existiert.
(d) Ist die Körpererweiterung $\mathbb{Q}(\alpha_0, ..., \alpha_4)/\mathbb{Q}$ normal?

Aufgabe 15: Wir betrachten ein Quadrat in der komplexen Ebene mit Mittelpunkt 0 und einer Ecke in $\frac{\sqrt{2}}{2}(1 + \mathrm{i})$.

(a) Bestimmen Sie die komplexe Zahlen $\alpha_0, ..., \alpha_3$, die den Ecken des Quadrats entsprechen. Geben Sie diese in der Form $a + \mathrm{i}b$ mit $a, b \in \mathbb{R}$ und in der Form $re^{\mathrm{i}\phi} = r\cos\phi + \mathrm{i}r\sin\phi$ mit $r \in \mathbb{R}^+$ und $\phi \in [0, 2\pi)$ an.
(b) Zeigen Sie, dass jede Ecke des Quadrats ein primitives Element von $\mathbb{Q}(\alpha_0, ..., \alpha_3)/\mathbb{Q}$ ist.
(c) Geben sie den Grad der Körpererweiterung $\mathbb{Q}(\alpha_0, ..., \alpha_3)/\mathbb{Q}$ an, indem Sie das Minimalpolynom eines primitiven Elements bestimmmen.
(d) Das Quadrat wird nun um $45° = \pi/4$ im Uhrzeigersinn gedreht. Geben Sie die Ecken $\beta_0, ..., \beta_3$ des gedrehten Quadrats in der Form $a + \mathrm{i}b$ mit $a, b \in \mathbb{R}$ und in der Form $re^{\mathrm{i}\phi} = r\cos\phi + \mathrm{i}r\sin\phi$ mit $r \in \mathbb{R}^+$ und $\phi \in [0, 2\pi)$ an.
(e) Geben Sie an, welche der Ecken $\beta_0, ..., \beta_3$ primitive Elemente der Körpererweiterung $\mathbb{Q}(\beta_0, ..., \beta_3)/\mathbb{Q}$ sind, und bestimmen Sie $[\mathbb{Q}(\beta_0, ..., \beta_3) : \mathbb{Q}]$.

Aufgabe 16: Geben Sie das Zwischenkörperdiagramm und das Untergruppendiagramm für die Körpererweiterung $\mathbb{F}_{5^{12}}/P(\mathbb{F}_{5^{12}})$ an, wobei $P(\mathbb{F}_{5^{12}})$ den Primkörper von $\mathbb{F}_{5^{12}}$ bezeichnet. Geben Sie dabei an, welche der darin auftretenden Körpererweiterungen galoissch und welche der darin auftretenden Untergruppen normal sind.

Aufgabe 17: Sei $S = \{\sqrt{2}, \sqrt[3]{3}, \sqrt[4]{4}, \ldots \sqrt[100]{100}\}$ und $L = \mathbb{Q}(S)$. Zeigen Sie, dass der Fixkörper der Galoisgruppe $\Gamma(L/\mathbb{Q})$ echt größer als $\mathbb{Q}$ ist.

Aufgabe 18: Sei $L/\mathbb{R}$ eine algebraische Körpererweiterung. Beweisen Sie:

(a) Es gilt: $L \cong \mathbb{R}$ oder $L \cong \mathbb{C}$
(b) $L/\mathbb{R}$ ist galoissch.
(c) Es gilt $\Gamma(L/\mathbb{R}) \cong \{\mathrm{id}_L\}$ oder $\Gamma(L/\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z}$.

Aufgabe 19: Sei L/K eine quadratische Körpererweiterung und $\mathrm{char}(K) = 0$. Beweisen Sie, dass L/K galoissch ist, und bestimmen Sie die Galoisgruppe von L/K.

Aufgabe 20: Sei L/K eine separable algebraische Körpererweiterung und $n \in \mathbb{N}$ fest mit $\deg_K(\alpha) = \deg(m_{\alpha,K}) \leq n$ für alle $\alpha \in L$. Ist die Körpererweiterung L/K endlich? Beweisen Sie die Aussage oder geben Sie ein Gegenbeispiel an.

Aufgabe 21: Sei $f = x^3 + x + 7 \in \mathbb{Q}[x]$ und L der Zerfällungskörper von f über $\mathbb{Q}$.

(a) Bestimmen Sie die Galoisgruppe $\Gamma(L/\mathbb{Q})$.
(b) Bestimmen Sie alle Untergruppen von $\Gamma(L/\mathbb{Q})$.
(c) Bestimmen Sie den Grad der Körpererweiterung $L/\mathbb{Q}$.

Aufgabe 22: Wir betrachten das Polynom $p = x^{12} - 1$ in $\mathbb{Q}[x]$.

(a) Bestimmen Sie den Zerfällungskörper L von p über $\mathbb{Q}$. Geben Sie alle Nullstellen von p in L in der Polardarstellung und in der Form $a + \mathrm{i}b$ mit $a, b \in \mathbb{R}$ an, und skizzieren Sie diese in der komplexen Ebene.
(b) Bestimmen Sie das Minimalpolynom $m_{\alpha,\mathbb{Q}}$ jeder Nullstelle von p in L und untersuchen Sie, welche der Nullstellen primitiv sind.

Aufgabe 23: Ist jeder Teilkörper eines Kreisteilungskörpers ein Kreisteilungskörper? Beweisen Sie die Aussage oder geben Sie ein Gegenbeispiel an.

Aufgabe 24: Wir betrachten die Körpererweiterung $\mathbb{Q}_n/\mathbb{Q}$. Bestimmen Sie alle Zwischenkörper von $\mathbb{Q}_n/\mathbb{Q}$ und alle Untergruppen der Galoisgruppe $\Gamma(\mathbb{Q}_n/\mathbb{Q})$ für:

(a) $n = 5$.
(b) $n = 11$.

Aufgabe 25: Beweisen Sie, dass die Polynome x^4+1 und x^4-x^2+1 irreduzibel über $\mathbb{Q}$ aber reduzibel über $\mathbb{F}_p$ für alle Primzahlen $p \in \mathbb{N}$ sind.
Hinweis: Betrachten Sie die Galoisgruppe des $n$ten Kreisteilungskörpers über $\mathbb{F}_p$.

Aufgabe 26: Beweisen Sie:

(a) Ist $n \geq 3$, so hat das $n$te Kreisteilungspolynom Φ_n geraden Grad.
(b) Ist $n \in \mathbb{N}$ ungerade mit $n \geq 3$, so gilt $\Phi_{2n}(x) = \Phi_n(-x)$
(c) Für alle $n \in \mathbb{N}$ und $p \in \mathbb{N}$ prim ist

$$\Phi_{np}(x) = \begin{cases} \Phi_n(x^p) & \text{falls } p|n \\ \Phi_n(x^p)/\Phi_n(x) & \text{falls } p \nmid n. \end{cases}$$

Aufgabe 27: Berechnen Sie alle Kreisteilungspolynome Φ_n mit $n \leq 24$. Geben Sie die Polynome in einer Tabelle an.

Aufgabe 28:

(a) Zerlegen Sie das 12te Kreisteilungspolynom $\Phi_{12,\mathbb{F}_{11}}$ über $\mathbb{F}_{11}$ in irreduzible Faktoren.
(b) Geben Sie die Minimalpolynome aller primitiven siebten Einheitswurzeln in $(\mathbb{F}_2)_{17}$ an.

Aufgabe 29: Sei $z \in \mathbb{C} \setminus \mathbb{Z}$ mit $z^2 \in \mathbb{Z}$. Bestimmen Sie alle $n$ten Einheitswurzeln im Körper $L = \mathbb{Q}(z)$ für alle $n \in \mathbb{N}$.

Aufgabe 30: Wahr oder falsch? Geben Sie eine kurze Begründung oder ein Gegenbeispiel an.

(a) Jeder Körper ist ein Erweiterungskörper von $\mathbb{Q}$ oder einem Körper $\mathbb{F}_p$ mit $p \in \mathbb{N}$ prim.
(b) Ist eine Körpererweiterung L/K primitiv mit $L = K(S)$, so ist die Teilmenge $S \subset L$ endlich.
(c) Eine Körpererweiterung der Form $\mathbb{Q}(\sqrt[n]{p})$ mit $p \in \mathbb{N}$ prim und $n > 2$ ist nie normal.
(d) Jede Körpererweiterung vom Grad 2 ist separabel.
(e) Jede Körpererweiterung vom Grad 2 ist normal.
(f) Jede echte Körpererweiterung von $\mathbb{R}$ ist isomorph zu $\mathbb{C}$.
(g) Ein Polynom der Form $1 + x + x^2 + \ldots + x^n$ ist irreduzibel über $\mathbb{Q}$ für alle $n \in \mathbb{N}$.
(h) Ist L/K eine algebraische Galoiserweiterung mit abelscher Galoisgruppe, so ist E/K galoissch für jeden Zwischenkörper $K \subset E \subset L$.
(i) Jede endliche Galoiserweiterung L/K ist primitiv.
(j) Ist $L/\mathbb{Q}$ eine normale Körpererweiterung, so existiert zu jedem $\alpha \in L \setminus \mathbb{Q}$ ein Element $\phi \in \Gamma(L/K)$ mit $\phi(\alpha) \neq \alpha$.
(k) Ist L/K eine algebraische Galoiserweiterung mit zyklischer Galoisgruppe, so gilt $L = \mathbb{F}_{p^r}$ und $K = \mathbb{F}_{p^s}$ für ein $p \in \mathbb{N}$ prim, $r, s \in \mathbb{N}$ und $s|r$.
(l) Jede Körpererweiterung der Form $\mathbb{F}_{p^r}/\mathbb{F}_{p^s}$ mit $p \in \mathbb{N}$ prim, $r, s \in \mathbb{N}$ und $s|r$ ist galoissch.

Aufgabe 31: Bestimmen Sie die Galoisgruppe von $p = x^5 - 5$ über $\mathbb{Q}$.

Aufgabe 32: Bestimmen Sie den Zerfällungskörper L des Polynoms x^6+3 über $\mathbb{Q}$, den Grad der Körpererweiterung $L/\mathbb{Q}$ und die Galoisgruppe $\Gamma(L/\mathbb{Q})$.

Aufgabe 33: Wahr oder falsch? Begründen Sie die Aussagen oder widerlegen Sie sie mit einem Gegenbeispiel.

(a) Die Gruppe $((\mathbb{Z}/n\mathbb{Z})^\times, \cdot)$ ist zyklisch für alle $n \in \mathbb{N}$.
(b) Die Eigenschaft "normal" ist transitiv: sind E/K und L/E normale Körpererweiterungen, so ist auch L/K normal.
(c) Die Eigenschaft "galoissch" ist transitiv: sind E/K und L/E Galoiserweiterungen, so ist auch L/K eine Galoiserweiterung.
(d) Ist L/K eine Galoiserweiterung vom Grad 4, so ist die Galoisgruppe $\Gamma(L/K)$ zyklisch.
(e) Jeder Kreisteilungskörper über einem endlichen Körper ist von der Form $\mathbb{F}_{p^r}$ für $p, r \in \mathbb{N}$, p prim.
(f) Ist $p \in \mathbb{Q}[x]$ ein irreduzibles Polynom vom Grad 3, so ist seine Galoisgruppe entweder isomorph zu S_3 oder zu A_3.
(g) Jede algebraische Körpererweiterung $L/\mathbb{Q}$ ist primitiv.

3 Anwendungen

3.1 Konstruktionen mit Zirkel und Lineal

Wir widmen und nun einer wichtigen Anwendung der Körpertheorie, nämlich Fragen der Konstruierbarkeit mit Hilfe von Zirkel und Lineal. Dazu betrachten wir eine Menge S von Punkten in der euklidischen Ebene $\mathbb{R}^2$ und untersuchen, welche Punkte sich aus Punkten in S mit Hilfe eines Zirkels und eines Lineals (ohne Längenmarkierungen) konstruieren lassen.

Dazu bezeichnen wir im Folgenden mit $[p, q]$ die Gerade durch zwei verschiedener Punkte $p, q \in S$, mit $K(p, r)$ den Kreis mit Mittelpunkt $p \in S$ und Radius $r \in \mathbb{R}^+$ und mit $|p - q| \in \mathbb{R}^+$ den Abstand zweier Punkte $p, q \in S$. Wir betrachten die drei grundlegende Konstruktionsschritte in Abbildung 1, mit denen wir die Menge S erweitern können:

- **Schritt a): Schnitt zweier Geraden.**
  Für Punkte $p, p', q, q' \in S$ mit $p \neq p'$, $q \neq q'$ und $[p, p'] \neq [q, q']$, ist auch der Schnittpunkt der Geraden $[p, p']$ und $[q, q']$ konstruierbar, falls er existiert.
- **Schritt b): Schnitt von Gerad und Kreis**
  Sind $p, q, q', t, t' \in S$ mit $t \neq t'$, $q \neq q'$, so sind alle Schnittpunkte der Geraden $[q, q']$ mit dem Kreis $K(p, |t - t'|)$ konstruierbar.
- **Schritt c): Schnitt zweier Kreise**
  Für Punkte $p, p', t, t', s, s' \in S$ mit $t \neq t'$, $s \neq s'$ und $p \neq p'$ sind alle Schnittpunkte der Kreise $K(p, |s - s'|)$ und $K(p', |t - t'|)$ konstruierbar.

Durch Kombinieren dieser drei elementaren Konstruktionsschritte erhält man, wie in Abbildung 2 gezeigt wird, die aus der Schule bekannten Konstruktionen mit Zirkel und Lineal:

- **Ganzzahlige Vielfache von Abständen konstruieren:** Abbildung 2 a).
- **Das Lot fällen:** Abbildung 2 b) und c).
- **Parallele zu einer Geraden durch einen Punkt konstruieren:** Abbildung 2 d).
- **Den Mittelpunkt einer Strecke konstruieren:** Abbildung 2 e).
- **Winkelhalbierende konstruieren:** Abbildung 2 f).
- **Winkel addieren:** Abbildung 2 g).

Wir betrachten nun die Menge der Punkte im $\mathbb{R}^2$, die sich durch Ausführen von endlich vielen elementaren Konstruktionsschritten konstruieren lassen.

Definition 3.1.1: Sei $S \subset \mathbb{R}^2$. Ein Punkt $p \in \mathbb{R}^2$ heißt aus S mit Zirkel und Lineal **konstruierbar**, wenn es ein $n \in \mathbb{N}$ und eine Kette $S = S_0 \subset S_1 \subset \ldots \subset S_n \subset \mathbb{R}^2$ von Teilmengen $S_i \subset \mathbb{R}^2$ gibt, so dass $p \in S_n$ und S_i aus S_{i-1} durch Hinzufügen der in einem der drei elementaren Konstruktionsschritt entstehenden Punkte hervorgeht. Wir bezeichnen die **Menge der konstruierbaren Punkte** mit $\mathrm{Kon}(S) \subset \mathbb{R}^2$.

Die zentrale Idee, die es ermöglicht, Probleme der Konstruierbarkeit zu lösen oder zu zeigen, dass diese unlösbar sind, ist es diese Probleme mit Hilfe von Zahlenkörpern zu beschreiben. Dazu

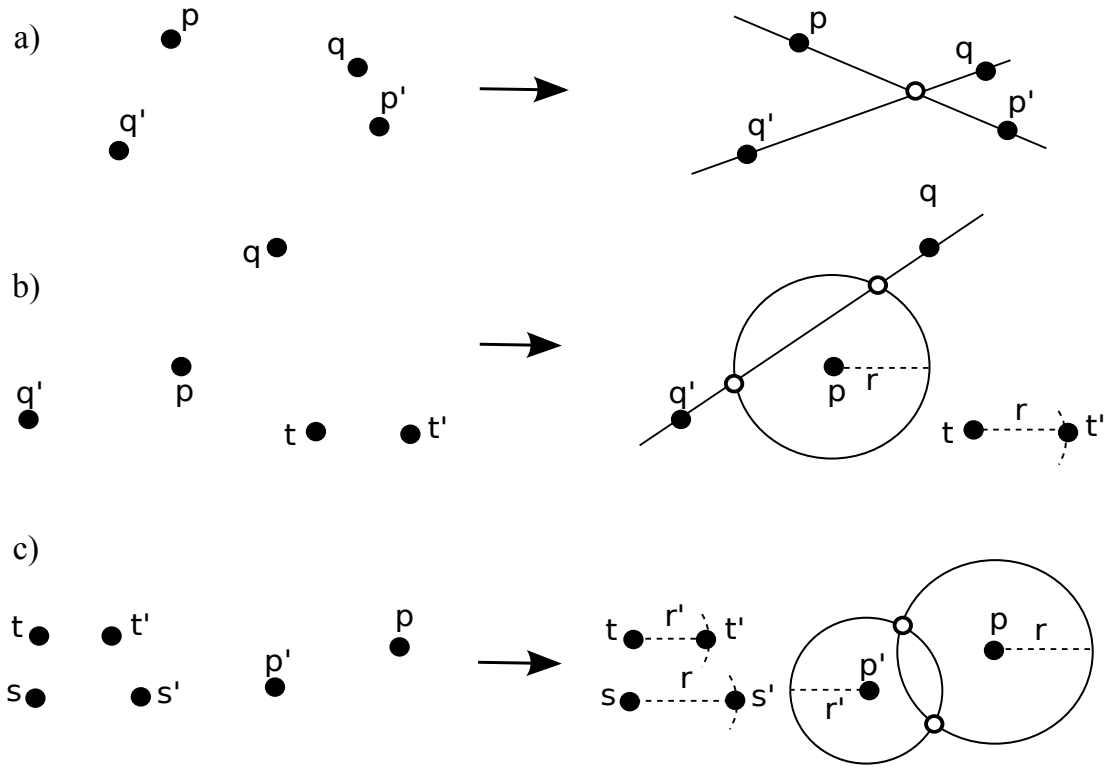


Abbildung 1: Die drei elementaren Konstruktionsschritte. Schwarze Punkte bezeichnen gegebene Punkte aus S, weisse Punkte die konstruierten Punkte.

identifizieren wir die euklidische Ebene mit dem Körper $\mathbb{C}$ der komplexen Zahlen und zeigen, dass die aus einer Menge $S \subset \mathbb{C}$ mit $0, 1 \in S$ konstruierbaren Zahlen einen Zwischenkörper $\mathbb{Q} \subset \mathrm{Kon}(S) \subset \mathbb{C}$ bilden.

Satz 3.1.2: Sei $S \subset \mathbb{C}$ eine Teilmenge mit $0, 1 \in S$. Dann gilt:

1. Die Menge $\mathrm{Kon}(S)$ der aus mit Zirkel und Lineal konstruierbaren Punkte ist ein Zwischenkörper[4] $\mathbb{Q}(S \cup \overline{S}) \subset \mathrm{Kon}(S) \subset \mathbb{C}$.
2. Ist $z \in \mathbb{C}$ mit $z^2 \in \mathrm{Kon}(S)$, so ist auch $z \in \mathrm{Kon}(S)$.
3. Für alle $z \in \mathrm{Kon}(S)$ ist auch $\overline{z} \in \mathrm{Kon}(S)$.

Beweis:
1. Wir zeigen zunächst, dass $\mathbb{Q} \subset \mathrm{Kon}(S)$. Da $0, 1 \in S$ erhält man durch Zeichnen der Gerade $[0, 1] = \mathbb{R} \subset \mathbb{C}$ und wiederholtem Abtragen der Länge $1 = |1 - 0|$ direkt $\mathbb{Z} \subset \mathrm{Kon}(S)$. Indem man die Mittelsenkrechte der Punkte $1, -1 \in \mathbb{C}$ konstruiert und wiederum Abstände abträgt, erhält man $\mathrm{i}\mathbb{Z} \in \mathrm{Kon}(S)$. Zu $n \in \mathbb{N}$ kann man unter Benutzung des Strahlensatzes dann den Punkt $1/n$ konstruieren, indem man die Gerade $[n, \mathrm{i}]$ und die dazu parallele Gerade g durch 1 zeichnet. Dann gilt nach dem Strahlensatz $g \cap \mathrm{i}\mathbb{R} = \{\mathrm{i}/n\}$, und der Schnittpunkt von $K(0, 1/n)$ mit $\mathbb{R}$ ist $1/n$. Also ist $\mathbb{Q} \subset \mathrm{Kon}(S)$.

[4]Achtung: $\overline{S} = \{\overline{z} : z \in S\}$ bezeichnet hier die Menge der zu Punkten in S komplex konjugierten Punkte und hat nichts mit einem algebraischen Abschluss zu tun.

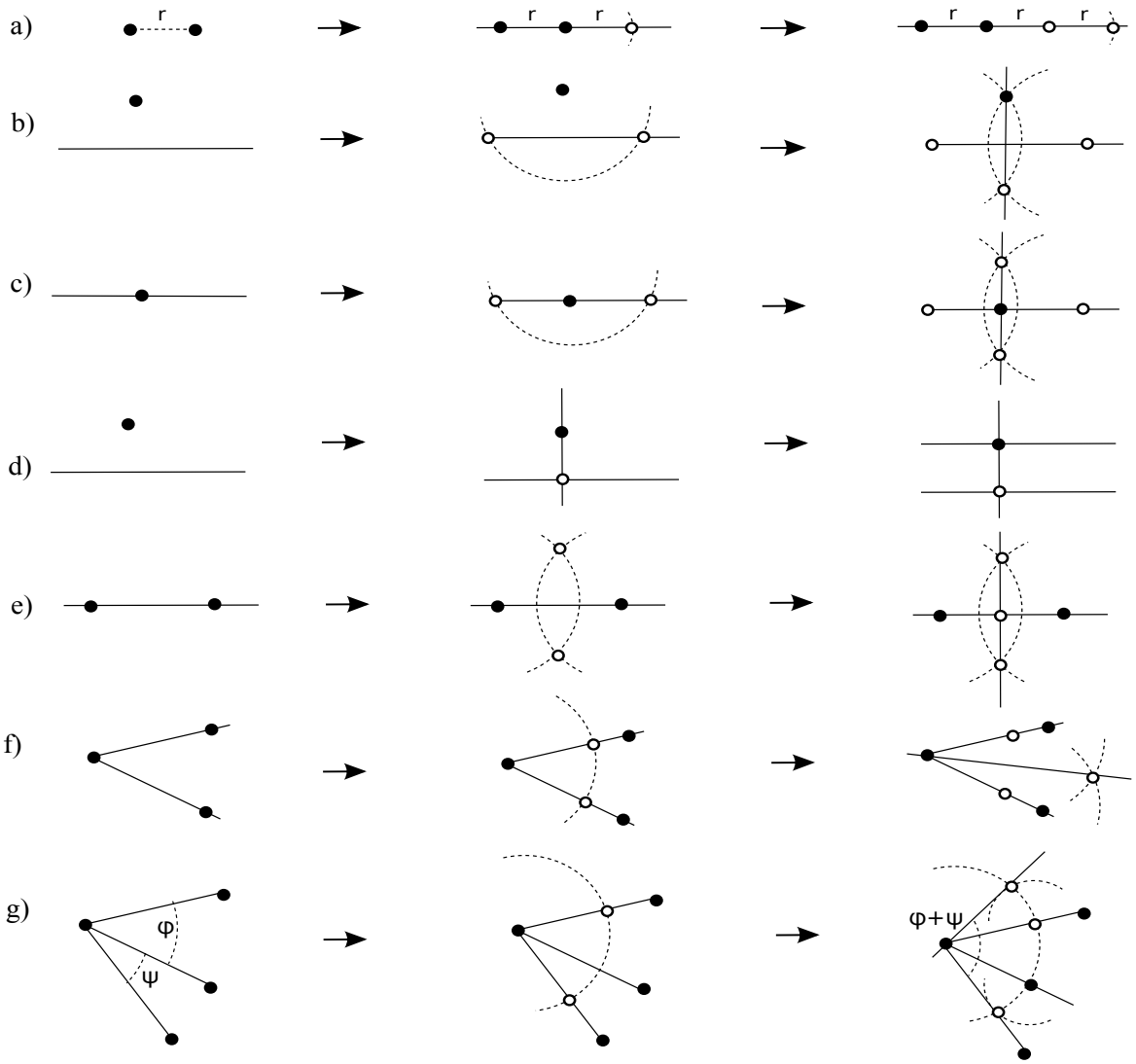
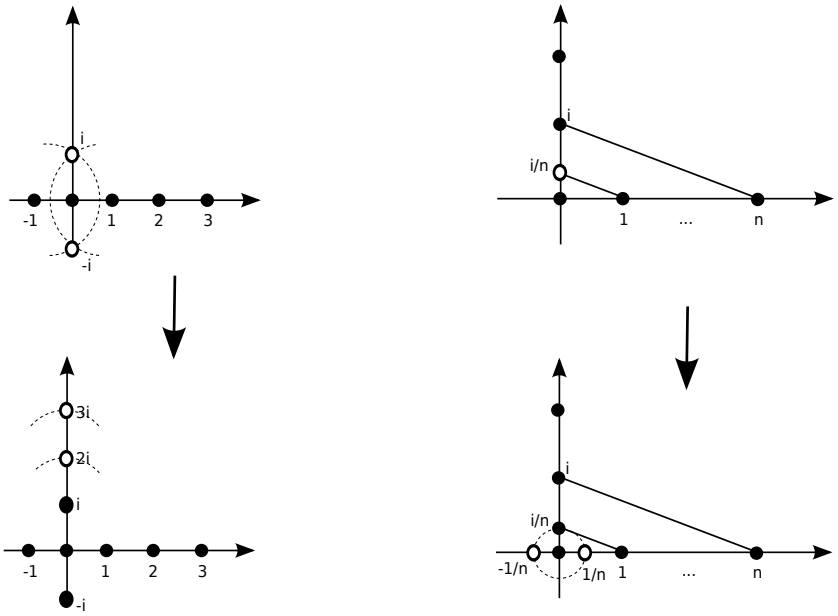
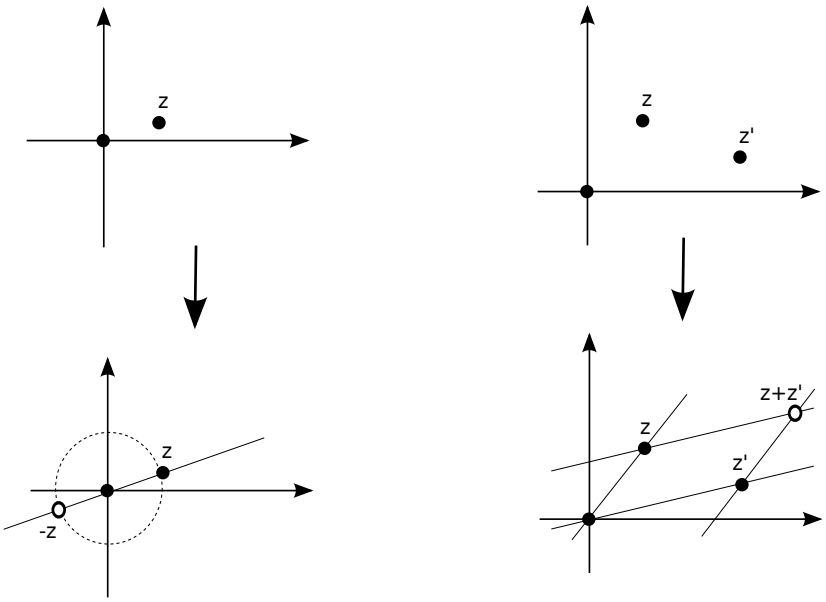


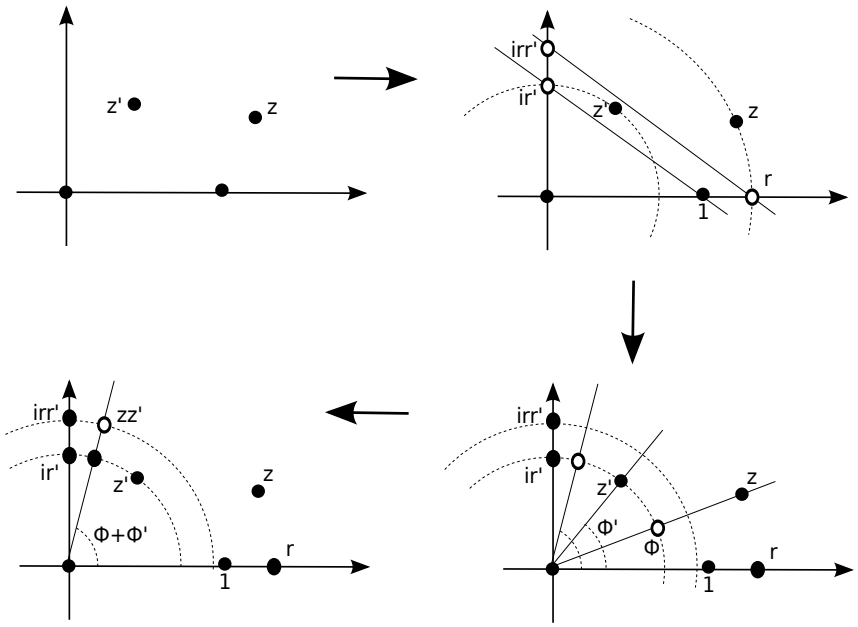
Abbildung 2: Bekannte Konstruktionen als Folge elementarer Konstruktionsschritte. Schwarze Punkte bezeichnen gegebene Punkte aus S, weisse Punkte die konstruierten Punkte.



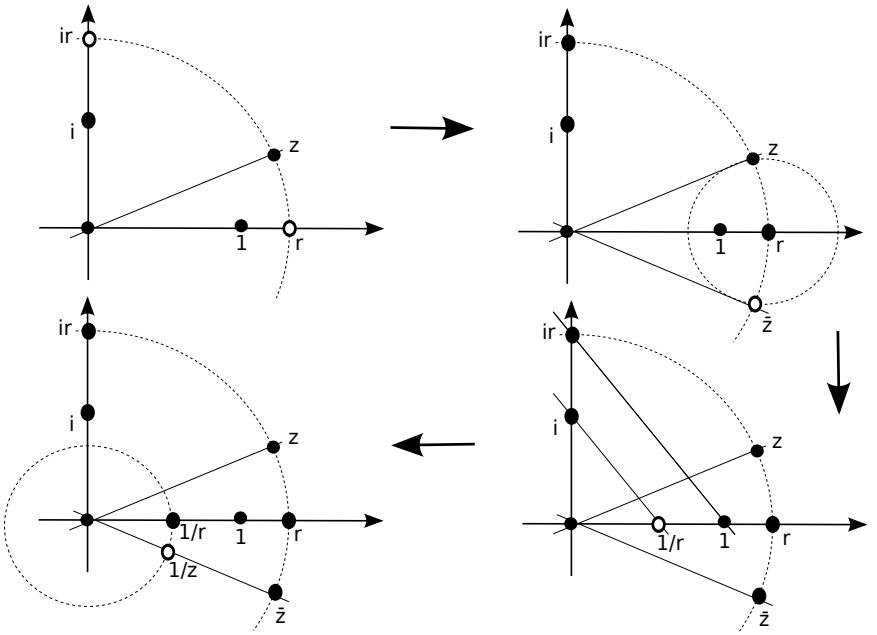
2. Wir zeigen, dass $\mathrm{Kon}(S)$ ein Körper ist. Sind $z, z' \in \mathrm{Kon}(S)$, so ist $z + z' \in \mathrm{Kon}(S)$, denn $z + z'$ ist der Schnittpunkt der zu $[0, z]$ parallelen Geraden durch z' mit der zu $[0, z']$ parallelen Geraden durch z. Durch Abtragen der Länge $|z| = |z - 0|$ auf der Geraden $[0, z]$ erhält man, dass für $z \in \mathrm{Kon}(S)$ auch $-z \in \mathrm{Kon}(S)$ gilt.



3. Sind $z = re^{\mathrm{i}\phi}, z' = r'e^{\mathrm{i}\phi'} \in \mathrm{Kon}(S)$ so erhält man den Punkt $\mathrm{i}r'$ als Schnittpunkt des Kreises $K(0, r')$ mit der imaginären Achse $[0, i]$ und den Punkt r als Schnittpunkt des Kreises $K(0, r)$ mit der reellen Achse $\mathbb{R} = [0, 1]$. Zeichnet man die Parallele zu der Geraden $[1, \mathrm{i}r']$ durch r, so schneidet diese nach dem Strahlensatz die imaginäre Achse in $\mathrm{i}rr'$. Konstruiert man nun den Schnittpunkt $K(0, r') \cap [0, z]$ und addiert auf $K(0, r)$ in z' den Winkel ϕ, so erhält man den Punkt $w = r'e^{\mathrm{i}(\phi+\phi')}$, und es folgt $zz' = [0, w] \cap K(0, rr')$. Also gilt $zz' \in \mathrm{Kon}(S)$.

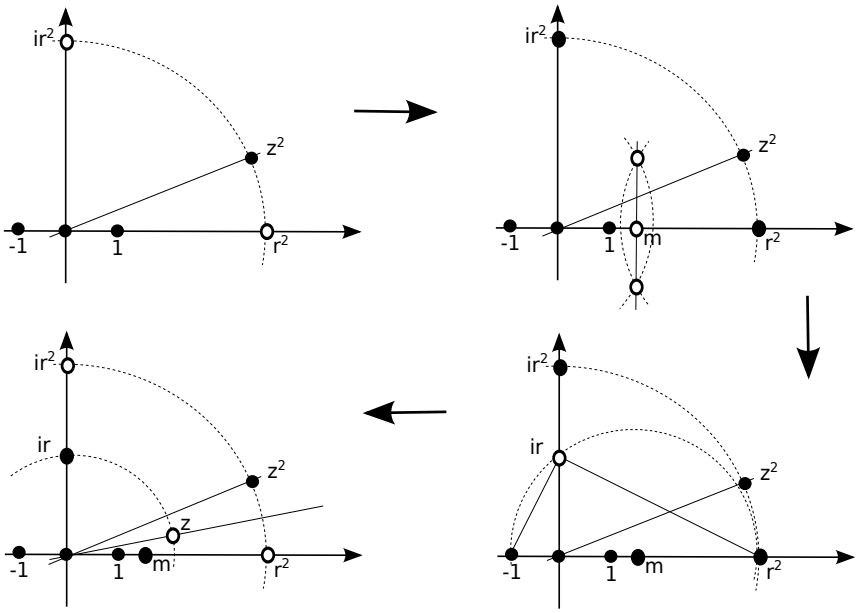


4. Ähnlich ergibt sich, dass für $z = re^{\mathrm{i}\phi} \in \mathrm{Kon}(S)$ auch $1/z = e^{-\mathrm{i}\phi}/r$ und $\overline{z} = re^{-\mathrm{i}\phi}$ in $\mathrm{Kon}(S)$ enthalten sind. Dazu zeichnet man den Kreis $K(0,r)$, der $\mathrm{i}\mathbb{R} = [0,\mathrm{i}]$ in $\mathrm{i}r$ und $\mathbb{R} = [0,1]$ in r schneidet. Dann schneidet man diesen Kreis mit dem Kreis $K(r,|z-r|)$ und erhält den Punkt $\overline{z} = re^{-\mathrm{i}\phi} = K(0,r) \cap K(r,|z-r|)$. Um $1/z$ zu konstruieren zeichnet man die Gerade $[\mathrm{i}r,1]$ und die dazu parallele Gerade durch i. Letztere schneidet die reelle Achse in $1/r$. Der Punkt $1/z$ ist der Schnittpunkt des Kreises $K(0,1/r)$ mit der Geraden $[0,\overline{z}]$. Damit ist gezeigt, dass $\mathrm{Kon}(S)$ ein Körper ist und für alle $z \in \mathrm{Kon}(S)$ auch $\overline{z} \in \mathrm{Kon}(S)$ gilt. Da $\mathbb{Q} \subset \mathrm{Kon}(S)$ und $S \cup \overline{S} \subset \mathrm{Kon}(S)$ folgt $\mathbb{Q}(S \cup \overline{S}) \subset \mathrm{Kon}(S) \subset \mathbb{C}$.



5. Wir zeigen noch, dass für $z \in \mathbb{C}$ mit $z^2 \in \mathrm{Kon}(S)$ folgt, dass $z \in \mathrm{Kon}(S)$. Sei also $z = re^{\mathrm{i}\phi}$ mit $z^2 = r^2 e^{2\mathrm{i}\phi} \in \mathrm{Kon}(S)$. Dazu zeichnet man den Kreis $K(0,r^2)$, der die reelle Achse in r^2 schneidet, und konstruiert den Mittelpunkt $m = \frac{1}{2}(r^2-1)$ der Strecke mit Endpunkten $-1, r^2$. Der Kreis $K(m, \frac{1}{2}(r^2+1))$ um m ist ein Thaleskreis und schneidet die imaginäre Achse in $\mathrm{i}s$.

Nach dem Satz des Pythagoras gilt $s^2+1 = |\mathrm{i}s+1|^2$, $r^4+s^2 = |\mathrm{i}s-r|^2$ und $|\mathrm{i}s+1|^2+|\mathrm{i}s-r|^2 = (1+r^2)^2$. Durch Auflösen dieser Gleichungen findet man $s = r$. Schneidet man den Kreis $K(0,r)$ mit der Winkelhalbierenden zwischen den Geraden $\mathbb{R}$ und $[0,z^2]$, so erhält man z.



□

Um die Körpererweiterungen $\mathrm{Kon}(S)/\mathbb{Q}(S \cup \overline{S})$ besser zu verstehen, ist es naheliegend, sich zunächst mit der Frage zu beschäftigen, ob diese algebraisch oder transzendent ist und die Grade der darin auftretenden algebraischen Elemente zu bestimmen. Dazu betrachtet man zunächst die Körpererweiterungen, die enstehen, wenn man zu einem Körper L mit $\mathrm{i} \in L$ und $\overline{L} = L$ einen aus L elementar konstruierbaren Punkt adjungiert.

Lemma 3.1.3: Sei $L \subset \mathbb{C}$ ein Teilkörper mit $\mathrm{i} \in L$ und[5] $\overline{L} = L$. Sind $z, z' \in \mathbb{C}$ aus Punkten in L durch einen elementaren Konstruktionsschritt konstruierbar, so existiert ein $w \in \mathbb{R}$ mit $w^2 \in L$ und $z, z' \in L(w)$. Insbesondere gilt: $\overline{L(w)} = L(w)$ und $[L(w) : L] \leq 2$.

Beweis:
Wegen $\overline{L} = L$ und $\mathrm{i} \in L$, liegt ein Punkt $z \in \mathbb{C}$ in L genau dann, wenn $\mathrm{Re}\,(z) = \frac{1}{2}(z+\overline{z}) \in L$ und $\mathrm{Im}\,(z) = -\frac{\mathrm{i}}{2}(z-\overline{z}) \in L$. Wir betrachten nun die drei elementaren Konstruktionsschritte.

Schritt (a): Ist z Schnittpunkt zweier Geraden durch Punkte in S, so existierten $p, p', q, q' \in S$ und $\lambda, \mu \in \mathbb{R}$ mit $z = p + \lambda(p'-p) = q + \mu(q'-q)$ Durch Zerlegen in Real- und Imaginärteil erhält man zwei inhomogene lineare Gleichungen für λ, μ mit Koeffizienten in $L \cap \mathbb{R}$. Also sind $\lambda, \mu \in L \cap \mathbb{R}$ damit $z \in L$.

Schritt (b): Sind z, z' Schnittpunkte einer Geraden durch zwei Punkte $q \neq q' \in L$ mit einem Kreis $K(p,r)$, wobei $p \in S$ und $r \in L \cap \mathbb{R}$, so existiert ein $\lambda \in \mathbb{R}$ mit $z = q + \lambda(q'-q)$, und es

[5] Achtung: $\overline{L} = \{\overline{z} : z \in L\}$ bezeichnet hier die Menge der zu Punkten in L komplex konjugierten Punkte und hat nichts mit einem algebraischen Abschluss zu tun.

gilt $|z-p|^2 = r^2$ Dies liefert eine quadratische Gleichung in λ mit Koeffizienten $\alpha, \beta, \gamma \in L \cap \mathbb{R}$

$$r^2 = |q+\lambda(q'-q)-p|^2 = \lambda^2 \underbrace{|q-q'|^2}_{=:\alpha} + 2\lambda \underbrace{(\mathrm{Re}\,(q'-q)\mathrm{Re}\,(q-p) + \mathrm{Im}\,(q'-q)\mathrm{Im}\,(q-p))}_{=:\beta} + \underbrace{|p-q|^2}_{=:\gamma}.$$

Wegen $q \neq q'$ impliziert die Existenz einer Lösung $\beta^2 - 4\alpha\gamma > 0$, und $w := \sqrt{\beta^2 - 4\alpha\gamma} \in \mathbb{R}$ ist die gesuchte Wurzel.

Schritt (c): Sind z, z' Schnittpunkte zweier Kreise $K(p,r)$ und $K(p',r')$ mit $p \neq p' \in L$ und $r, r' \in L \cap \mathbb{R}$, so erfüllt z die Gleichungen $|z-p|^2 = r^2$ und $|z-p'|^2 = r'^2$. Subtrahiert man diese Gleichungen voneinander, so erhält man ein lineares inhomogenes Gleichungssystem in den Variablen $\mathrm{Re}\,(z)$, $\mathrm{Im}\,(z)$ mit Koeffizienten in $L \cap \mathbb{R}$

$$\underbrace{(\mathrm{Re}\,(p) - \mathrm{Re}\,(p'))}_{\in L\cap\mathbb{R}} \mathrm{Re}\,(z) + \underbrace{(\mathrm{Im}\,(p) - \mathrm{Im}\,(p'))}_{\in L\cap\mathbb{R}} \mathrm{Im}\,(z) = \underbrace{r^2 - r'^2 + |p'|^2 - |p|^2}_{\in L\cap\mathbb{R}}.$$

Also folgt $\mathrm{Re}\,(z), \mathrm{Im}\,(z) \in L \cap \mathbb{R}$ und somit $z \in L$. □

Lemma 3.1.3 besagt, dass die Körpererweiterungen, die entsehen, wenn man zu L einen aus L elementar konstruierbaren Punkt adjungiert, trivial oder quadratisch sind. Der geometrische Grund dafür ist, dass sich zwei Geraden oder Kreise in maximal zwei Punkten schneiden, die Lösungen einer linearen oder quadratischen Gleichung sind.

Unter Benutzung dieses Lemmas können wir nun zeigen, dass die Körpererweiterung $\mathrm{Kon}(\{0,1\})/\mathbb{Q}$ eine unendliche algebraische Körpererweiterung ist und nur Elemente enthält, deren Grad über $\mathbb{Q}$ eine Zweierpotenz ist. Dies ist die Aussage, mit der wir später beweisen werden, dass bestimmte Konstruktionsprobleme unlösbar sind.

Satz 3.1.4: Sei $S \subset \mathbb{C}$ mit $0, 1 \in S$. Dann gilt:

1. Die Körpererweiterung $\mathrm{Kon}(S)/\mathbb{Q}(S \cup \overline{S})$ ist algebraisch.
2. $[\mathrm{Kon}(\{0,1\}) : \mathbb{Q}] = \infty$
3. Es gilt $z \in \mathrm{Kon}(S)$ genau dann, wenn es einen endlichen Körperturm

$$\mathbb{Q}(S \cup \overline{S}) = L_0 \subset L_1 \subset \ldots \subset L_r \subset \mathbb{C}$$

mit $z \in L_r$ und $[L_k : L_{k-1}] \leq 2$ für alle $k \in \{1, ..., r\}$ gibt.

Beweis:
1. Offensichtlich folgt Aussage 1 aus Aussage 3. Zu Aussage 2 überlegt man sich, dass man aus -1 durch $n$faches Winkelhalbieren alle Elemente $z_n = e^{\pi \mathrm{i}/2^n}$ mit $n \in \mathbb{N}$ konstruieren kann. Das Minimalpolynom von $e^{\mathrm{i}\pi/2^n} = e^{2\pi\mathrm{i}/2^{n+1}}$ über $\mathbb{Q}$ ist $\Phi_{2^{n+1}} = x^{2^n} + 1$, denn

$$x^{2^{n+1}} - 1 = (x^{2^n} + 1) \cdot (x^{2^n} - 1) = \prod_{0<d|2^{n+1}} \Phi_d = \Phi_{2^{n+1}} \cdot \prod_{0<d|2^n} \Phi_d = \Phi_{2^{n+1}} \cdot (x^{2^n} - 1).$$

Also folgt $\deg_{\mathbb{Q}}(z_n) = 2^n$ und $[\mathrm{Kon}(\{0,1\}) : \mathbb{Q}] \geq \deg_{\mathbb{Q}}(z_n) = 2^n$ für alle $n \in \mathbb{N}$.

3. Sei $\mathbb{Q}(S \cup \overline{S}) = L_0 \subset L_1 \subset \ldots \subset L_r$ ein Körperturm mit $[L_k : L_{k-1}] \leq 2$ für alle $k \in \{1, ..., r\}$. Wir zeigen per Induktion über r, dass L_r konstruierbar ist. Für $r = 0$ ist dies offensichtlich. Sei die Aussage nun bewiesen für $r \leq k-1$. Gilt $[L_k : L_{k-1}] = 1$, so ist $L_k = L_{k-1}$ und somit sind

alle Elemente in L_k konstruierbar. Ansonsten ist $[L_k : L_{k-1}]$ quadratisch und $L_k = L_{k-1}(w)$, wobei w eine Nullstelle eines über L_{k-1} irreduziblen Polynoms $p = x^2 + \beta x + \gamma$ mit $\beta, \gamma \in L_{k-1}$ ist. Dann gilt aber auch $L_k = L_{k-1}(w')$ für $w' \in \mathbb{C}$ mit $w'^2 = \beta^2 - 4\gamma \in L_{k-1}$. Da nach Satz 3.1.2 w' konstruierbar ist, sind alle Elemente in L_k konstruierbar.

Sei nun $z \in \mathrm{Kon}(S)$. Nach Voraussetzung existiert dann eine Kette $S = S_0 \subset S_1 \subset \ldots \subset S_r$ von Teilmengen $S_i \subset \mathbb{C}$, so dass S_k aus S_{k-1} durch eine elementare Konstruktion entsteht, also $S_k = S_{k-1} \cup \{z_k, z_k'\}$ mit (nicht notwendigerweise verschiedenen) $z, z' \in \mathbb{C}$. Sei $L_0 = \mathbb{Q}(S \cup \overline{S})$, $L_1 = L_0(\mathrm{i})$. Dann gilt $\overline{L_0} = L_0$, $\overline{L_1} = L_1$ und $[L_1 : L_0] \leq 2$. Nach Lemma 3.1.3 existiert zu $z_1, z_1' \in S_1$ ein $w_1 \in \mathbb{R}$ mit $z_1, z_1' \in L_1(w_1) =: L_2$ und $[L_2 : L_1] \leq 2$. Durch Iteration dieses Verfahrens erhält man den gesuchten Körperturm $L_0 \subset L_1 \subset \ldots \subset L_r$ mit $z \in L_r$. □

Korollar 3.1.5: Sei $S \subset \mathbb{C}$ mit $0, 1 \in S$, $z \in \mathrm{Kon}(S)$ und $L = \mathbb{Q}(S \cup \overline{S})$. Dann ist $[L(z) : L]$ eine Zweierpotenz.

Wir beweisen nun mit Hilfe dieser Korollars, dass die folgenden klassischen Konstruktionssprobleme unlösbar sind:

1. **Quadratur des Kreises:** Zu einem gegebenen Kreis soll mit Zirkel und Lineal ein Quadrat konstruiert werden, dessen Fächeninhalt gleich dem des Kreises ist.
2. **Würfelverdoppelung (Delisches Problem):** Aus einer Kante eines vorgegebenen Würfels soll mit Zirkel und Lineal die Kante eines Würfels doppelten Volumens konstruiert werden.
3. **Winkeldrittelung:** Ein beliebiger Winkel soll mit Zirkel und Lineal in drei gleiche Teile zerlegt werden.

Nach Korollar 3.1.5 reicht es dafür aus, zu zeigen, dass die Konstruktionsprobleme die geometrische Konstruktion einer Zahl $z \in \mathbb{C}$ erfordern, die entweder transzendent über $\mathbb{Q}$ ist oder algebraisch über $\mathbb{Q}$ mit Grad $\deg_{\mathbb{Q}}(z) \neq 2^n$ für alle $n \in \mathbb{N}$.

Satz 3.1.6:

1. Die Quadratur des Kreises ist unmöglich.
2. Die Würfelverdoppelung ist unmöglich.
3. Die Drittelung eines Winkels $\alpha \in [0, 2\pi)$ ist im Allgemeinen unmöglich.

Beweis:
1. **Quadratur des Kreises:** Der Flächeninhalt eines Kreises vom Radius 1 ist π. Die Quadratur des Kreises entspräche also der Konstruktion eines Quadrats mit Seitenlänge $\sqrt{\pi}$ aus der Startmenge $S = \{0, 1\}$. Da π und somit auch $\sqrt{\pi}$ transzendent über $\mathbb{Q}$ ist, kann $\sqrt{\pi}$ nicht in dem algebraischen Erweiterungskörper $\mathrm{Kon}(\{0, 1\})$ enthalten sein.

2. **Würfelverdoppelung:** Die Würfelverdoppelung eines vorgegebenen Würfels mit Kandenlänge 1 entspricht der Konstruktion eines Würfels mit Seitenlänge $d = \sqrt[3]{2}$ aus $S = \{0, 1\}$. Die Zahl $d = \sqrt[3]{2}$ ist algebraisch über $\mathbb{Q}$ vom Grad $\deg_{\mathbb{Q}}(d) = 3$, was keine Zweierpotenz ist.

3. **Winkeldrittelung:** Ein vorgegebener Winkel $\alpha \in [0, 2\pi)$ entspricht einer komplexen Zahl $z = e^{\mathrm{i}\alpha}$ auf dem Einheitskreis, und die Winkeldrittelung der Konstruktion der komplexen

Zahl $w = e^{\mathrm{i}\alpha/3}$ aus $S = \{0, 1, z\}$. Da $\overline{z} = z^{-1}$ gilt $\mathbb{Q}(S \cup \overline{S}) = \mathbb{Q}(z)$. Da $w^3 = z$ teilt das Minimalpolynom von w über $\mathbb{Q}(z)$ das Polynom $x^3 - z$. Da das Polynom z ein Primelement im Quotientenkörper $Q(\mathbb{Q}[z])$ ist, ist das Polynom $x^3 - z \in Q(\mathbb{Q}[z])[x]$ irreduzibel nach Eisenstein, und somit gilt $[Q(\mathbb{Q}[z])(x)]) : Q(\mathbb{Q}[z])] = 3 \neq 2^n$. Also ist eine Winkeldrittelung im allgemeinen unmöglich. □

Bemerkung 3.1.7: Ähnlich wie im Beweis von Satz 3.1.8 zeigt man auch, dass konkrete Winkel nicht drittelbar sind. Ist $\alpha = 2\pi/3$, so ist das Minimalpolynom von $z = e^{\mathrm{i}\alpha/3} = e^{2\pi\mathrm{i}/9}$ über $\mathbb{Q}$ das Kreisteilungspolynom $\Phi_9 = x^6 + x^3 + 1$ und das Miimalpolynom von $e^{2\pi\mathrm{i}/3}$ das Kreisteilungspolynom $\Phi_3 = 1 + x + x^2$. Also gilt

$$6 = [\mathbb{Q}(e^{2\pi\mathrm{i}/9}) : \mathbb{Q}] = [\mathbb{Q}(e^{2\pi\mathrm{i}/3}) : \mathbb{Q}(e^{2\pi\mathrm{i}/3})] \cdot [\mathbb{Q}(e^{2\pi\mathrm{i}/3}) : \mathbb{Q}] = 2 \cdot [\mathbb{Q}(e^{2\pi\mathrm{i}/9}) : \mathbb{Q}(e^{2\pi\mathrm{i}/3})]$$

und somit $[\mathbb{Q}(e^{2\pi\mathrm{i}/9}) : \mathbb{Q}(e^{2\pi\mathrm{i}/3})] = 3 \neq 2^n$. Es gibt aber auch Winkel, die sich dritteln lassen, beispielsweise $\alpha = 270° = 3\pi/2$. In diesem Fall ist $e^{\mathrm{i}\alpha/3} = e^{\mathrm{i}\pi/2} = \mathrm{i}$ und $e^{\mathrm{i}\alpha} = e^{3\pi\mathrm{i}/2} = -\mathrm{i}$, also $e^{\mathrm{i}\alpha/3} \in \mathbb{Q}(e^{\mathrm{i}\alpha})$.

Wir betrachten nun das vierte klassische Problem, nämlich die **Konstruktion eines regulären n-Ecks**. In einen vorgegebenen Kreis soll mit Zirkel und Lineal ein reguläres n-Eck ($n \geq 3$) einbeschrieben werden. Dies entspricht offensichtlich für den Kreis $K(0, 1)$ der geometrischen Konstruktion des $n$ten Kreisteilungskörpers $\mathbb{Q}_n$ aus $S = \{0, 1\}$ oder, dazu äquivalent, der Konstruktion einer primitiven $n$ten Einheitswurzel.

Das Minimalpolynom einer primitiven $n$ten Einheitswurzel $w \in \mathbb{Q}_n$ ist das $n$te Kreisteilungspolynom Φ_n und hat nach Lemma 2.3.6 Grad $\varphi(n)$. Also ist eine primitive $n$te Einheitswurzel genau dann konstruierbar aus $S = \{0, 1\}$, wenn $\deg_{\mathbb{Q}}(w) = \varphi(n)$ eine Zweierpotenz ist. Nun stellt sich die Frage für welche $n \in \mathbb{N}$ dies zutrifft. Der folgende Satz zeigt, dass dieses Problem mit **Fermatschen Primzahlen** zusammenhängt, also Primzahlen der Form $p = 2^{2^k} + 1$ mit $k \in \mathbb{N}_0$. Bis heute sind nur fünf Fermatsche Primzahlen bekannt, nämlich $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65\,537$.

Satz 3.1.8: Ein reguläres n-Eck ist genau dann konstruierbar, wenn $\varphi(n)$ eine Zweierpotenz ist. Dies ist der Fall genau dann, wenn $n = 2^m$ oder $n = 2^m p_1 \cdots p_r$ mit $m, r \in \mathbb{N}$ und paarweise verschiedenen Fermatschen Primzahlen $p_1, ..., p_r$.

Beweis:
Ist $n = p_1^{n_1} \cdots p_r^{n_r}$ die Primfaktorzerlegung von n, so gilt

$$\varphi(n) = p_1^{n_1 - 1} \cdots p_r^{n_r - 1} \cdot (p_1 - 1) \cdots (p_r - 1).$$

Also ist $\varphi(n)$ eine Zweierpotenz genau dann, wenn für alle $p_j \neq 2$ gilt $n_j = 1$ und $p_j = 1 + 2^{m_j}$ für ein $m_j \in \mathbb{N}$. Eine Zahl der Form $2^m + 1$ kann aber nur dann eine Primzahl sein, wenn $m = 2^k$ für ein $k \in \mathbb{N}$. Denn hätte m einen ungeraden Teiler, so wäre $2^m = 2^{d \cdot l}$ mit $d, l \in \mathbb{N}$ ungerade und somit $2^m + 1 = 2^{d \cdot l} + 1 = (2^l + 1)(1 - 2^l + 2^{2l} - \ldots + 2^{(k-1)l})$. Also müssen alle Primfaktoren $p_j \neq 2$ Fermatsche Primzahlen sein. □

3.2 Auflösbarkeit algebraischer Gleichungen durch Radikale

In diesem Abschnitt werden wir eine weitere wichtige Anwendung der Galoistheorie betrachten, nämlich die Auflösbarkeit von algebraischen Gleichungen. Eine algebraische Gleichung über einem Körper K ist eine Gleichung der Form $p(x) = 0$ mit einem Polynom $p \in K[x]$. Unter Auflösbarkeit versteht man grob gesprochen, die Möglichkeit eine Formel für die Nullstellen zu finden, die diese als verschachtelte Wurzeln von Elementen in K beschreibt, also etwa für $K = \mathbb{Q}$ Ausdrücke der Form

$$\sqrt[n]{\sqrt{3}a + b + (\sqrt[3]{c^3 + 2d + 1})^2} \qquad a, b, c, d \in \mathbb{Q}.$$

Um diese Frage mit Hilfe der Galoistheorie zu behandeln, benötigt man zunächst ein mathematisches Konzept, dass diesen intuitiven Begriff der Auflösbarkeit erfaßt und mit Körpererweiterungen in Verbindung bringt. Hierbei ist es naheliegend, $n$te Wurzeln als Nullstellen von Polynomen der Form $x^n - a$ mit $a \in K$ aufzufassen. Da Produkte, Summen und Linearkombinationen solcher Wurzeln in den Formeln auftauchen können, ist es naheliegend, Körpererweiterungen zu betrachten, die durch Adjunktion solcher Nullstellen enstehen - die sogenannten *einfachen Radikalerweiterungen*.

Da auch ineinander verschachtelte Wurzeln auftreten können - etwa in den Cardanoschen Formeln, die die Lösungen einer Polynomgleichung dritten Grades angeben - müssen wir dann auch Körpertürme $K \subset K_1 \subset \ldots \subset K_r = L$ betrachten, in denen der Teilkörper K_i durch Adjunktion von Nullstellen eines reinen Polynoms aus K_{i-1} hervorgeht - die sogenannten *Radikalerweiterungen*. Dies führt auf die folgende Definition.

Definition 3.2.1: Sei K ein Körper.

1. Ein Polynom der Form $x^n - a$ mit $a \in K$, $n \in \mathbb{N}$ heißt **reines Polynom** über K und eine Gleichung der Form $x^n - a = 0$ eine **reine Gleichung** über K.
2. Eine Nullstelle $\alpha \in \overline{K}$ eines reinen Polynoms bezeichnet man als **Radikal** über K und eine Körpererweiterung der Form $K(\alpha)/K$ als **einfache Radikalerweiterung** von K.
3. Eine Körpererweiterung L/K heisst **Radikalerweiterung**, wenn es einen Körperturm $K = K_0 \subset K_1 \subset \ldots \subset K_r = L$ gibt, so dass K_i/K_{i-1} für alle $i \in \{1, ..., r\}$ eine einfache Radikalerweiterung ist.
4. E/K heisst **durch Radikale auflösbar**, wenn es eine Radikalenerweiterung L/K mit $K \subset E \subset L$ gibt.
5. Ein Polynom $p \in K[x]$ heißt **durch Radikale auflösbar**, wenn sein Zerfällungskörper auflösbar durch Radikale ist.

Wir möchten nun die Auflösbarkeit von Körpererweiterungen bzw. Polynomen durch deren Galoisgruppen charakterisieren. Da die Auflösbarkeit in beiden Fällen durch eine Folge von Zwischenkörpern charakterisiert ist, die einfache Radikalerweiterungen sind, bietet es sich an, zunächst die Galoisgruppen von einfachen Radikalerweiterungen zu betrachten.

Solche Körpererweiterungen sind offenbar eng verwandt mit Kreisteilungskörpern. Da für jede Nullstelle α eines reinen Polynoms $p = x^n - a \in K[x]$ und jede $n$te Einheitswurzel ϵ auch $\alpha\epsilon^k$ wieder eine Nullstelle von p ist, bietet es sich an, zunächst eine primitive $n$te Einheitswurzel ϵ zum Grundkörper K zu adjungieren und anschliessend eine Nullstelle des reinen Polynoms p zu

$K(\epsilon)$. Die im zweiten Schritt entstehende Körpererweiterung hat dann eine besonders einfache Form und besitzt eine zyklische Galoisgruppe.

Lemma 3.2.2: Sei K ein Körper. Enthält K eine primitive $n$te Einheitswurzel, so gilt für jedes reine Polynom $p \in K[x]$ mit $\deg(p) = n$ und beliebige Nullstellen $\alpha, \beta \in \overline{K}$ von p:

1. $K(\alpha) = K(\beta)$.
2. $K(\alpha)/K$ ist zyklisch mit $d := [K(\alpha) : K] | n$ und $\alpha^d \in K$.

Beweis:
1. Sei $p = x^n - a$ mit $a \in K$, α eine Nullstelle von p in $\overline{K}$ und $\epsilon \in K$ eine primitive $n$te Einheitswurzel. Dann gilt $(\epsilon^k \alpha)^n = \epsilon^{nk} \alpha^n = \alpha^n = a$ für alle $k \in \mathbb{N}$. Also sind α, $\epsilon\alpha$, $\epsilon^2\alpha$,..., $\epsilon^{n-1}\alpha$ n verschiedene Nullstellen von p in $\in K(\alpha)$. Damit zerfällt p über $K(\alpha)$, ist separabel über K, und für jede Nullstelle β von p gilt $K(\beta) = K(\alpha)$.

2. Da p separabel über K ist und über $K(\alpha)$ zerfällt, ist $K(\alpha)/K$ normal und separabel und somit galoissch. Jeder K-Automorphismus $\tau \in \Gamma(K(\alpha)/K)$ ist durch seinen Wert auf α eindeutig bestimmt, und es gilt $\tau(\alpha) = \epsilon^k \alpha$ für ein $k \in \mathbb{N}$. Wegen $n = \min\{k \in \mathbb{N} : \epsilon^k = 1\}$ ist die zugehörige Restklasse $\overline{k}$ in $\mathbb{Z}/n\mathbb{Z}$ dadurch eindeutig bestimmt, und man erhält eine Abbildung

$$\phi : \Gamma(K(\alpha)/K) \to \mathbb{Z}/n\mathbb{Z}, \quad \tau \mapsto \phi(\tau) = \overline{k}.$$

Diese Abbildung ist ein Gruppenhomomorphismus von $\Gamma(K(\alpha)/K)$ in $(\mathbb{Z}/n\mathbb{Z}, +)$. Denn für $\tau, \sigma \in \Gamma(K(\alpha)/K)$ mit $\tau(\alpha) = \epsilon^k \alpha$ und $\sigma(\alpha) = \epsilon^{k'} \alpha$ folgt $\sigma \circ \tau(\alpha) = \tau \circ \sigma(\alpha) = \epsilon^{k+k'} \alpha$ und somit $\phi(\sigma \circ \tau) = \phi(\tau \circ \sigma) = \overline{k + k'} = \phi(\tau) + \phi(\sigma)$. Ausserdem ist ϕ injektiv, denn aus $\phi(\tau) = 0$ folgt $\tau(\alpha) = \epsilon^{kn} \alpha = \alpha$ und somit $\tau = \mathrm{id}$.

3. Also gilt $\Gamma(K(\alpha)/K) \cong \phi(\Gamma(K(\alpha)/K)) \subset (\mathbb{Z}/n\mathbb{Z}, +)$. Insbesondere ist $\Gamma(K(\alpha)/K)$ zyklisch und $d := |\Gamma(K(\alpha)/K)| = [K(\alpha) : K] | n = |\mathbb{Z}/n\mathbb{Z}|$. Daraus folgt $\tau^d(\alpha) = \epsilon^{kd} \alpha = \mathrm{id}(\alpha) = \alpha$ und damit $\tau(\alpha^d) = (\epsilon^k \alpha)^d = \epsilon^{kd} \alpha^d = \alpha^d$ für alle $\tau \in \Gamma(K(\alpha)/K)$. Da $K(\alpha)/K$ galoissch ist, impliziert das $\alpha^d \in K$. □

Bemerkung 3.2.3: Auf die Voraussetzung, dass K eine primitive $n$te Einheitswurzel enthält, kann nicht verzichtet werden. Betrachtet man das Polynom $p = x^4 - 4 \in \mathbb{Q}[x]$ so sieht man, dass sein Zerfällungskörper $\mathbb{Q}(\sqrt{2}, \mathrm{i})$ ist, denn seine Nullstellen sind $\pm\sqrt{2}, \pm\sqrt{2}\mathrm{i}$. Nach Beispiel 2.2.7 ist aber die Galoisgruppe $\Gamma(\mathbb{Q}(\sqrt{2}, \mathrm{i})/\mathbb{Q})$ isomorph zur Diedergruppe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ und damit nicht zyklisch.

Lemma 3.2.2 besagt, dass die Zyklizität der Galoisgruppe $\Gamma(L/K)$ eine notwendige Bedingung dafür ist, dass eine Körpererweiterung L/K über einem Körper K, der eine primitive $n$te Einheitswurzel enthält, eine einfache Radikalerweiterung ist. Das folgende Lemma zeigt, dass diese Bedingung auch hinreichend ist.

Lemma 3.2.4: Sei L/K eine zyklische Körpererweiterung vom Grad n. Enthält K eine primitive $n$te Einheitswurzel, so ist L der Zerfällungskörper eines reinen Polynoms $p \in K[x]$ vom Grad n, i. e. eine einfache Radikalerweiterung, und für jede Nullstelle α von p gilt $L = K(\alpha)$.

Beweis:
1. Wir beweisen zunächst eine Hilfsaussage, das sogenannte **Dedekindsche Lemma**: Sind K, L Körper, $\alpha_1, ..., \alpha_n \in L$ und $\tau_1, ..., \tau_n : K \to L$ verschiedene Körpermonomorphismen mit $\sum_{k=1}^{n} \alpha_k \tau_k(\beta) = 0$ für alle $\beta \in K$, so folgt $\alpha_1 = \ldots = \alpha_n = 0$.

Dies beweist man durch Induktion über n. Für $n = 1$ ist die Aussage klar. Sei die Aussage nun bewiesen für alle $n \leq m-1$. Seien $\alpha_1, ..., \alpha_m \in L$ und $\tau_1, ..., \tau_m : K \to L$ verschiedene Monomorphismen mit $\sum_{k=1}^{m} \alpha_k \tau_k(\beta) = 0$ für alle $\beta \in K$. Dann existiert ein $\gamma \in K$ mit $\tau_1(\gamma) \neq \tau_m(\gamma)$, und es folgt für alle $\beta \in K$

$$0 = \tau_m(\gamma) \cdot \sum_{k=1}^{m} \alpha_k \tau_k(\beta) = \sum_{k=1}^{m} \alpha_k \tau_k(\gamma\beta) = \sum_{k=1}^{m} \alpha_k \tau_k(\gamma)\tau_k(\beta) \quad \Rightarrow \sum_{k=1}^{m-1} (\tau_k(\gamma) - \tau_m(\gamma)) \alpha_k \tau_k(\beta) = 0.$$

Mit der Induktionsvoraussetzung folgt $\alpha_k(\tau_k(\gamma) - \tau_m(\gamma)) = 0$ für alle $k \in \{1, ..., m-1\}$ und aus $\tau_m(\gamma) \neq \tau_1(\gamma)$ ergibt sich $\alpha_1 = 0$. Also gilt $\sum_{k=2}^{m} \alpha_k \tau_k(\beta) = 0$ für alle $\beta \in L$, und mit der Induktionsvoraussetzung folgt die Behauptung.

2. Sei $\Gamma(L/K) \cong \langle \sigma \rangle$ und $\epsilon \in K$ eine primitive $n$te Einheitswurzel. Dann existiert wegen $\epsilon^k \neq 0$ für alle $k \in \{0, ..., n-1\}$ nach 1. ein $\gamma \in L$ mit $\alpha := \gamma + \epsilon\sigma(\gamma) + \ldots + \epsilon^{n-1}\sigma^{n-1}(\gamma) \neq 0$. Wegen $\epsilon^n = 1$ und $\sigma^n = \mathrm{id}_L$ folgt

$$\sigma(\alpha) = \sigma(\gamma) + \epsilon\sigma^2(\gamma) + \ldots + \epsilon^{n-1}\sigma^n(\gamma) = \epsilon^{-1}\gamma + \sigma(\gamma) + \epsilon\sigma^2(\gamma) + \ldots + \epsilon^{n-2}\sigma^{n-1}(\gamma) = \epsilon^{-1}\alpha,$$

und somit $\sigma(\alpha^n) = \sigma(\alpha)^n = \epsilon^{-n}\alpha^n = \alpha^n$. Also gilt $\alpha^n \in K$, und wegen $\sigma^k(\alpha) = \epsilon^{-k}\alpha$ sind $\alpha, \sigma(\alpha) = \epsilon^{-1}\alpha, ..., \sigma^{n-1}(\alpha) = \epsilon^{-(n-1)}\alpha$ verschiedene Nullstellen des Minimalpolynoms $m_{\alpha,K}$. Es folgt $\deg(p) \geq n = [L : K]$, also $L = K(\alpha)$. □

Lemma 3.2.2 und 3.2.4 zeigen, dass eine Körpererweiterung vom Grad n über einem Körper K, der eine $n$te Einheitswurzel enthält, genau dann eine einfache Radikalerweiterung ist, wenn ihre Galoisgruppe zyklisch ist. Endliche Galoiserweiterungen mit zyklischen Galoisgruppen entsprechen also einfachen Radikalerweiterungen.

Wir möchten dieses Ergebnis nun verallgemeinern, und die Galoisgruppen von allgemeinen Radikalerweiterungen oder durch Radikale auflösbaren Körpererweiterungen charakterisieren. Dies sind Körpererweiterungen L/K, die sich durch Körpertürme $K = K_0 \subset K_1 \subset \ldots \subset K_r = L$ von einfachen Radikalerweiterungen K_i/K_{i-1} beschreiben lassen.

Die Korrespondenz zwischen Untergruppen der Galoisgruppe $\Gamma(L/K)$ und Zwischenkörpern $K \subset E \subset L$ suggeriert, dass die Galoisgruppen solcher Körpererweiterungen Gruppentürmen $\{e\} = G_0 \subset G_1 \subset \ldots \subset G_r = \Gamma(L/K)$ mit normalen Untergruppen $G_{i-1} \subset G_i$ und G_i/G_{i-1} zyklisch, also insbesondere abelsch, entsprechen sollten. Solche Gruppen sind aus der Vorlesung Algebra bereits bekannt - es sind die sogenannten auflösbaren Gruppen. Wir wiederholen die Definition und die wichtigsten Eigenschaften von auflösbaren Gruppen.

Definition 3.2.5:

1. Die **Kommutatorgruppe** einer Gruppe G ist die von den Gruppenkommutatoren von Elementen in G erzeugte Untergruppe $[G, G] = \langle \{[g, h] = ghg^{-1}h^{-1} : g, h \in G\} \rangle$.

2. Interativ definiert man die **nte Kommutatorgruppe** von G durch $G^{(0)} = G$ und $G^{(n)} = [G^{(n-1)}, G^{(n-1)}]$ für alle $n \in \mathbb{N}$.
3. Eine Gruppe G heißt **auflösbar**, wenn ein $n \in \mathbb{N}$ mit $G^{(n)} = \{e\}$ existiert.

Bemerkung 3.2.6:

1. Die Kommutatorgruppe $[G, G]$ ist ein Normalteiler von G.
2. Für einen Normalteiler $N \subset G$ ist die Faktorgruppe G/N genau dann abelsch, wenn $[G, G] \subset N$ gilt. Insbesondere sind für jede Gruppe G die Faktorgruppen $G^{(n-1)}/G^{(n)}$ abelsch.
3. Jede Untergruppe und jede Faktorgruppe einer auflösbaren Gruppe ist auflösbar.
4. Das direkte Produkt von auflösbaren Gruppen ist auflösbar.
5. Ist $N \subset G$ ein Normalteiler und sind N und G/N auflösbar, so ist auch G auflösbar.
6. Eine Gruppe G ist genau dann auflösbar, wenn sie eine abelsche Normalreihe hat, d. h. eine Folge normaler Untergruppen $\{e\} = G_0 \subset G_1 \subset \ldots \subset G_r = G$ mit G_i/G_{i-1} abelsch existiert.
7. Jede endliche auflösbare Gruppe besitzt eine Normalreihe $\{e\} = G_0 \subset G_1 \subset \ldots \subset G_r = G$ mit G_i/G_{i-1} zyklisch.

Beispiel 3.2.7:

1. Jede abelsche und damit insbesondere jede zyklische Gruppe ist auflösbar.
2. Die Gruppe S_n ist auflösbar genau dann, wenn $n < 5$.
3. Jede Gruppe ungerader Ordnung ist auflösbar (Satz von Feit-Thompson).

Mit Hilfe dieser Definitionen und Aussagen können wir nun zeigen, dass die Auflösbarkeit der Galoisgruppe ein hinreichendes Kriterium für die Auflösbarkeit eines separablen Polynoms ist, falls die Charakteristik des Körpers die Ordnung der Galoisgruppe nicht teilt.

Satz 3.2.8: Sei $p \in K[x]$ separabel über K. Ist die Galoisgruppe Γ von p auflösbar über K und $\mathrm{char}(K) \nmid |\Gamma|$, so ist p auflösbar durch Radikale.

Beweis:
1. Gilt $\mathrm{char}(K) \nmid n$, so enthält der $n$te Kreisteilungskörper $K_n \subset \overline{K}$ über K nach Lemma 2.3.4 eine primitive $n$te Einheitswurzel ϵ, und es gilt $K_n = K(\epsilon)$. Damit ist $K(\epsilon)/K$ eine einfache Radikalerweiterung, denn ϵ ist eine Nullstelle des reinen Polynoms $x^n - 1 \in K[x]$.

Sei $L \subset \overline{K}$ der Zerfällungskörper von p über K und $|\Gamma| = |\Gamma(L/K)| = n$. Da p separabel und L/K normal ist, ist die Körpererweiterung L/K eine endliche Galoiserweiterung. Dies gilt auch für die Körpererweiterung M/K_n mit $M = L(\epsilon) = K_n(L)$, denn da M der Zerfällungskörper von $p \in K[x] \subset K_n[x]$ ist, ist M/K_n normal und wegen p separabel über K ist auch M/K_n separabel, also galoissch.

2. Da L/K normal ist, gilt $\tau(L) \subset L$ für jedes $\tau \in \Gamma(M/K_n)$, und wir erhalten einen Gruppenhomomorphismus $\phi : \Gamma(M/K_n) \to \Gamma$, $\tau \mapsto \tau|_L$. Dieser ist injektiv, denn aus $\tau|_L = \mathrm{id}_L$ folgt

wegen $\tau|_{K_n} = \mathrm{id}_{K_n}$ auch $\tau|_M = \mathrm{id}_M$. Somit ist die Galoisgruppe $\Gamma(M/K_n)$ isomorph zu einer Untergruppe von Γ und damit auflösbar als Untergruppe einer auflösbaren Gruppe.

3. Da $\Gamma(M/K)$ eine endliche auflösbare Gruppe ist, existiert nach Bemerkung 3.2.6 7. eine Folge von normalen Untergruppen $\{e\} = G_0 \subset G_1 \subset \ldots \subset G_s = \Gamma(M/K_n)$ mit G_i/G_{i-1} zyklisch für alle $i \in \{1, ..., s\}$. Nach dem Hauptsatz der endlichen Galoistheorie bilden die Fixkörper dieser Untergruppen einen Körperturm $K_n = \mathcal{F}(G_s) \subset \mathcal{F}(G_{n-1}) \subset \ldots \subset \mathcal{F}(G_1) \subset \mathcal{F}(\{e\}) = M$. Ausserdem sind nach dem Hauptsatz der endlichen Galoistheorie alle Körpererweiterungen $M/\mathcal{F}(G_i)$ galoissch mit Galoisgruppe G_i. Da $G_{i-1} \subset G_i$ eine normale Untergruppe ist, sind nach dem Hauptsatz auch alle Körpererweiterungen $\mathcal{F}(G_{i-1})/\mathcal{F}(G_i)$ galoissch mit Galoisgruppe G_i/G_{i-1}. Somit sind alle Körpererweiterungen $\mathcal{F}(G_{i-1})/\mathcal{F}(G_i)$ zyklisch und $[\mathcal{F}(G_i) : K_n] \,|\, [M : K_n] \,|\, n$. Da $K_n \subset \mathcal{F}(G_i)$ eine $n$te Einheitswurzel enthält ist $\mathcal{F}(G_{i-1})/\mathcal{F}(G_i)$ nach Lemma 3.2.4 eine einfache Radikalerweiterung. Also ist M/K eine Radikalerweiterung mit $L \subset M$. □

Beispiel 3.2.9:

1. Ist K ein Körper der Charakteristik $\mathrm{char}(K) = 0$, so ist die Bedingung $\mathrm{char}(K) \nmid |\Gamma|$ in Satz 3.2.8 immer erfüllt, und jedes Polynom $p \in K[x]$ mit auflösbarer Galoisgruppe ist auflösbar durch Radikale.
2. Insbesondere ist also jedes Polynom $p \in K[x]$ mit zyklischer oder abelscher Galoisgruppe mit Koeffizienten in einem Körper der Charakteristik 0 auflösbar durch Radikale, denn zyklische und abelsche Gruppen sind auflösbar.
3. Jedes Polynom vom Grad ≤ 4 über einem Körper der Charakteristik $\neq 2, 3$ ist auflösbar. Denn wegen $\mathrm{char}(K) \nmid 4$ ist p separabel und $\mathrm{char}(K) \nmid |\Gamma(p)|$. Da ein solches Polynom maximal vier verschiedene Nullstellen in seinem Zerfällungskörper hat und die Galoisgruppe die Nullstellen von p permutiert, kommen nur Untergruppen von S_2, S_3, S_4 als Galoisgruppen in Frage. Die Gruppen S_2, S_3, S_4 und somit auch all ihre Untergruppen sind auflösbar.

Satz 3.2.8 liefert ein hinreichendes Kriterium für die Auflösbarkeit einer algebraischen Gleichung durch Radikale, nämlich die Auflösbarkeit der zugehörigen Galoisgruppe. Wir werden nun zeigen, dass die Auflösbarkeit der Galoisgruppe unter bestimmten Voraussetzungen auch ein notwendiges Kriterium für die Auflösbarkeit ist. Mit dieser Aussage könenn wir dann beweisen, dass bestimmte algebraische Gleichungen nicht auflösbar sind.

Dazu müssen wir einerseits Zerfällungskörper von Polynomen betrachten, also normale Körpererweiterungen. Andererseits müssen wir durch Adjunktion von primitiven Einheitswurzeln dafür sorgen, dass die relevanten Körper solche Einheitswurzeln enthalten. Dies zwingt uns dazu, ineinander verschachtelte normale Körpererweiterungen zu betrachten, die durch Adjunktion von Nullstellen und Einheitswurzeln entstehen. Dazu benötigen wir zunächst noch zwei Lemmata um die Galoisgruppen von normalen Körpertürmen zu charakterisieren und zu untersuchen, wie sich die Eigenschaft, eine Radikalerweiterung zu sein, unter dem Übergang zur normalen Hülle einer Körpererweiterung verhält.

Lemma 3.2.10: Sei $K \subset E \subset L$ ein Zwischenkörper und seien die Körpererweiterungen L/K und E/K normal. Dann ist $\phi : \Gamma(L/K) \to \Gamma(E/K)$, $\tau \mapsto \tau|_E$ ein Epimorphismus, $\Gamma(L/E) \subset \Gamma(L/K)$ eine normale Untergruppe und $\Gamma(E/K) \cong \Gamma(L/K)/\Gamma(L/E)$.

Beweis:
Da E/K normal ist, gilt $\tau(E) \subset E$ für jeden K-Automorphismus $\tau \in \Gamma(L/K)$, und somit $\tau|_E \in \Gamma(E/K)$. Da L/K algebraisch ist, kann umgekehrt jedes $\sigma \in \Gamma(E/K)$ nach den Fortsetzungssätzen 1.4.13 bis 1.4.16 zu einem K-Automorphismus $\sigma \in \Gamma(L/K)$ fortgesetzt werden. Also ist ϕ surjektiv, und es gilt $\tau \in \ker(\phi)$ genau dann, wenn $\tau|_E = \mathrm{id}_E$ also $\ker(\phi) = \Gamma(L/E)$. Damit ist $\Gamma(L/E) \subset \Gamma(L/K)$ eine normale Untergruppe und $\Gamma(E/K) \cong \Gamma(L/K)/\Gamma(L/E)$. □

In dem wir dieses Lemma mit Bemerkung 3.2.6 kombinieren, werden wir später die Auflösbarkeit der Galoisgruppen $\Gamma(L/K)$, $\Gamma(L/E)$ und $\Gamma(E/K)$ für Körpertürme $K \subset E \subset L$ mit L/K, E/K normal in Beziehung setzen können. Das folgende Lemma zeigt, dass sich an der Eigenschaft eine Radikalerweiterung zu sein, durch Übergang zur normalen Hülle nichts ändert. Wir können also im Folgenden mit Zerfällungskörpern arbeiten.

Lemma 3.2.11: Ist L/K eine Radikalerweiterung und N die normale Hülle von L/K, so ist auch N/K eine Radikalerweiterung.

Beweis:
1. Sei N die normale Hülle von L/K in $\overline{K}$ und $\mathrm{id}_N = \sigma_0, ..., \sigma_r$ die verschiedenen K-Automorphismen von N. Wir setzen $F_i = \sigma_i(L)$ und $E = F_1 \dots F_r = F_1(F_2 \dots F_r) = (F_1(F_2))(F_3 \dots F_r) = F_1(\dots F_{r-1}(F_r) \dots) \subset N$. Dann läßt sich jeder K-Monomorphismus $\sigma : E \to \overline{K}$ nach den Fortsetzungssätzen 1.4.13 bis 1.4.16 zu einem K-Automorphismus $\tilde{\sigma} : N \to N$ fortsetzen. Es folgt $\tilde{\sigma} = \sigma_i$ für ein $i \in \{1, ..., r\}$ und somit $\sigma(E) = E$. Also ist E/K normal und somit wegen der Eindeutigkeit der normalen Hülle $N = E = (F_1(F_2))(F_3 \dots F_r) = F_1(\dots F_{r-1}(F_r) \dots)$.

2. Es reicht also zu zeigen, dass für zwei Radikalerweiterungen F_1/K und F_2/K mit $F_1, F_2 \subset \overline{K}$ auch das Kompositum F/K mit $F = F_1F_2 = F_1(F_2) = F_2(F_1)$ eine Radikalerweiterung ist. Da $F = F_2(F_1)$ aus F_2 durch sukzessive Adjunktion von Radikalen entseht, ist F/F_2 eine Radikalerweiterung und somit auch F/K. □

Mit Hilfe dieser zwei Lemmata können wir nun beweisen, dass die Auflösbarkeit ihrer Galoisgruppe auch ein notwendiges Kriterium dafür ist, dass eine gegebene endliche Körperperweiterung durch Radikale auflösbar ist.

Satz 3.2.12: Sei L/K eine endliche durch Radikale auflösbare Körpererweiterung mit $L \subset \overline{K}$ und N die normale Hülle von L/K in $\overline{K}$. Dann ist $\Gamma(N/K)$ auflösbar.

Beweis:
1. Nach Voraussetzung existiert eine Radikalerweiterung M/K mit $L \subset M$. Nach Lemma 3.2.11 ist die normale Hülle $N' \subset \overline{K}$ von M/K in $\overline{K}$ eine Radikalerweiterung über K. Da $N \subset N'$ und N/K, N'/K normal sind, ist Lemma 3.2.10 der Gruppenhomomorphismus $\phi : \Gamma(N'/K) \to \Gamma(N/K)$, $\tau \mapsto \tau|_N$ ein Epimorphismus und $\Gamma(N'/K) \cong \Gamma(N/K)/\ker(\phi)$. Ist also $\Gamma(N'/K)$ auflösbar, so folgt mit Bemerkung 3.2.6, 3. dass auch $\Gamma(N/K)$ auflösbar ist. Es reicht also, die Aussage für $\Gamma(N'/K)$ zu beweisen.

2. Da N'/K eine normale Radikalerweiterung ist, existiert ein Körperturm $K = K_0 \subset K_1 \subset \dots \subset K_r = L$ mit $K_i = K_{i-1}(\alpha_i)$ und $\alpha_i^{p_i} \in K_{i-1}$. Durch Einfügen weiterer Zwischenkörper kann

man wegen $(\alpha^s)^r = \alpha^{r \cdot s}$ o. B. d. A. annehmen, dass $p_i \in \mathbb{N}$ prim für alle $i \in \{1, ..., r\}$ gilt. Sei n das Produkt der p_i mit $p_i \neq \text{char}(K)$. Dann enthält $\overline{K}$ eine primitive $n$te Einheitswurzel ϵ. Da N'/K eine normale Radikalerweiterung ist, ist $N'(\epsilon)$ Zerfällungskörper einer Familie separabler Polynome aus $K[x]$ und somit $N'(\epsilon)/K$ normal. Man erhält einen Körperturm $K(\epsilon) = K_0(\epsilon) \subset K_1(\epsilon) \subset \ldots \subset K_r(\epsilon) = N'(\epsilon)$ mit $K_i(\epsilon) = K_{i-1}(\epsilon)(\alpha_i)$ und $\alpha_i^{p_i} \in K_{i-1}(\epsilon)$.

3. Wir zeigen mit vollständiger Induktion über r, dass $\Gamma(N'(\epsilon)/K(\epsilon))$ auflösbar ist. Für $r = 1$ gilt entweder $p_1 = \text{char}(K)$ oder $p_1 \neq \text{char}(K)$. Im ersten Fall ist die Körpererweiterung $K_1(\epsilon)/K(\epsilon)$ wegen $(x^{p_1} - \alpha_1)' = p_1 x^{p_1 - 1} = 0$ rein inseparabel und $|\Gamma(K_1(\epsilon)/K_0(\epsilon)| = [K_1(\epsilon) : K_0(\epsilon)]_s = 1$. Gilt $p_1 \neq \text{char}(K)$, so ist nach Lemma 3.2.2 die Galoisgruppe $\Gamma(K_1(\epsilon)/K(\epsilon))$ zyklisch. In beiden Fällen ist $K_1(\epsilon)/K_0(\epsilon)$ normal und $\Gamma(K_1(\epsilon)/K(\epsilon))$ auflösbar. Durch Anwendung der Induktionsvoraussetzung auf die normale Radikalerweiterung $N'(\epsilon)/K_1(\epsilon)$ folgt, dass $\Gamma(N'(\epsilon)/K_1(\epsilon))$ auflösbar ist. Mit Lemma 3.2.10 und Bemerkung 3.2.6 folgt die Auflösbarkeit von $\Gamma(N'(\epsilon)/K(\epsilon))$, denn $\Gamma(N'(\epsilon)/K(\epsilon)) \subset \Gamma(N'(\epsilon)/K(\epsilon))$ ist eine auflösbare normale Untergruppe und $\Gamma(K_1(\epsilon)/K(\epsilon)) \cong \Gamma(N'(\epsilon)/K(\epsilon))/\Gamma(N'(\epsilon)/K_1(\epsilon))$ ist auflösbar.

4. Wir zeigen, dass $\Gamma(N'/K)$ auflösbar ist. Die Gruppe $\Gamma(N'(\epsilon)/K(\epsilon)$ ist auflösbar nach 3. Die Galoisgruppe $\Gamma(K(\epsilon)/K)$ ist abelsch, da $K(\epsilon) \cong K_n$ ein Kreisteilungskörper ist, und somit ebenfalls auflösbar. Nach Lemma 3.2.10 gilt ausserdem $\Gamma(K(\epsilon)/K) \cong \Gamma(N'(\epsilon)/K)/\Gamma(N'(\epsilon)/K(\epsilon))$ und somit ist nach Bemerkung 3.2.6 auch $\Gamma(N'(\epsilon)/K)$ auflösbar. Wiederum nach Lemma 3.2.10 ist $\Gamma(N'/K) \cong \Gamma(N'(\epsilon)/K)/\Gamma(N'(\epsilon)/N)$ und nach Bemerkung 3.2.6 ist damit auch $\Gamma(N'/K)$ auflösbar. □

Da die Galoisgruppe eines Polynoms $p \in K[x]$ die Galoisgruppe seines Zerfällungskörpers L über K ist, erhalten wir aus diesem Satz eine notwendige Bedingung für die Auflösbarkeit von algebraischen Gleichungen durch Radikale. Im Fall $\text{chark}(K) = 0$ liefert dies zusammen mit Satz 3.2.8 eine notwendige und hinreichende Bedingung.

Korollar 3.2.13: Sei K ein Körper.

1. Ist ein Polynom $p \in K[x]$ durch Radikale auflösbar, so ist seine Galoisgruppe auflösbar.
2. Gilt $\text{char}(K) = 0$, so ist ein Polynom $p \in K[x]$ genau dann durch Radikale auflösbar, wenn seine Galoisgruppe auflösbar ist.

Beispiel 3.2.14: Ist $q \in \mathbb{Q}[x]$ ein irreduzibles Polynom mit $\deg_{\mathbb{Q}}(q) = p \in \mathbb{N}$ prim und genau zwei Nullstellen in $\mathbb{C} \setminus \mathbb{R}$, so kann man zeigen, dass die Galoisgruppe von q die gesamte symmetrische Gruppe S_p ist. Die symmetrische Gruppe S_n ist auflösbar genau dann, wenn $n \leq 4$ gilt. Also kann es für $p \in \mathbb{N}$ prim, $p \geq 5$ keine allgemeine Lösungsformel geben, die die Nullstellen eines Polynoms $q \in \mathbb{Q}[x]$ durch seine Koeffizienten ausdrückt.

3.3 Übungen zu Kapitel 3

Aufgabe 1:
Bestimmen Sie die Zahlen $n \in \{1, 2, ..., 100\}$, für die das reguläre n-Eck konstruierbar ist.

Aufgabe 2: Zeigen Sie:

(a) Ein Winkel $\alpha \in [0, 2\pi)$ kann genau dann mit Zirkel und Lineal gedrittelt werden, wenn das Polynom $4x^3 - 3x - \cos(\alpha)$ reduzibel über $\mathbb{Q}(\cos\alpha)$ ist.
(b) Für jedes $n \in \mathbb{N}$ mit $3 \nmid n$ kann $\alpha = 2\pi/n$ mit Zirkel und Lineal gedrittelt werden.

A Übersichtstabellen

Eigenschaften von Elementen in Körpererweiterungen

Sei L/K eine Körpererweiterung, $f, g \in K[x]$ irrduzibel, $\alpha \in L$, $n \in \mathbb{N}$, $p \in \mathbb{N}$ prim, $q \in \mathbb{Q}$.

Eigenschaft	**Definition**	**Beispiele**	**Bemerkungen**
$\alpha \in L$ algebraisch über K	Nullstelle von Polynom mit Koeffizienten in K $\exists p \in K[x] : \ p(\alpha) = 0$	• i in $\mathbb{C}/\mathbb{R}$, $\mathbb{C}/\mathbb{Q}$, • $\sqrt[p]{q}$ in $\mathbb{R}/\mathbb{Q}$ für $q \in \mathbb{Q}$, • $\overline{x}$ in $K[x]/(g)$, • $\alpha \in K$	• $K(\alpha) \cong K[x]/(m_{\alpha,K})$ • $[K(\alpha) : K] = \deg_K(\alpha)$ • Zwischenkörper $K \subset E \subset L$: $\alpha \in L$ algebraisch über E, E/K algebraisch $\Rightarrow \alpha$ algebraisch über K
• Minimalpolynom von α über K	eindeutiges normiertes Polynom $m_{\alpha,K} \in K[x]$ von minimalem Grad mit $m_{\alpha,K}(\alpha) = 0$	• $m_{\mathrm{i},\mathbb{Q}} = x^2 + 1$, • $m_{\sqrt[p]{q},\mathbb{Q}} = 1 + ... + x^{p-1}$, • $m_{\overline{x},K[x]/(g)} = g$, • $\alpha \in K \Rightarrow m_{\alpha,K} = x - \alpha$	• $m_{\alpha,K}$ ist irreduzibel • $f \in K[x]$ mit $f(\alpha) = 0$ $\Rightarrow m_{\alpha,K} \mid f$ • Zwischenkörper $K \subset E \subset L$: $\Rightarrow m_{\alpha,E} \mid m_{\alpha,K}$ in $E[x]$
• Grad von α über K	Grad des Minimalpolynoms von α über K $\deg_K(\alpha) = \deg(m_{\alpha,K})$	• $\deg_{\mathbb{Q}}(\mathrm{i}) = \deg_{\mathbb{R}}(\mathrm{i}) = 2$, • $\deg_{\mathbb{Q}}(\sqrt[p]{q}) = p - 1$, • $\alpha \in K \Rightarrow \deg_K(\alpha) = 1$	• Zwischenkörper $K \subset E \subset L$: $\Rightarrow \deg_E(\alpha) \mid \deg_K(\alpha)$
$\alpha \in L$ transzendent über K	nicht algebraisch über K	• e, π in $\mathbb{R}/\mathbb{Q}$	• $K(\alpha) \cong Q(K[x])$
$\alpha \in L$ primitiv	$L = K(\alpha)$	• primitiv: i in $\mathbb{C}/\mathbb{R}$, π in $\mathbb{Q}(\pi)/\mathbb{Q}$, $\overline{x}$ in $K[x]/(g)$, • nicht primitiv: i in $\mathbb{C}/\mathbb{Q}$, π in $\mathbb{R}/\mathbb{Q}$	α primitiv $\not\Rightarrow \alpha$ algebraisch α algebraisch $\not\Rightarrow \alpha$ primitiv α primitiv $\not\Rightarrow \alpha$ transz. α transz. $\not\Rightarrow \alpha$ primitiv
$\alpha \in L$ separabel über K	α algebraisch und $m_{\alpha,K}$ hat nur einfache Nullstellen in Zerfällungskörper	• $K = \mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{F}_{p^n}$ und $\alpha \in L$ algebraisch, • $\alpha \in K$	• $\mathrm{char}(K) = 0 \vee \lvert K \rvert < \infty$: $\alpha \in L$ alg. $\Rightarrow \alpha$ separabel
$\alpha \in L$ inseparabel	α algebraisch und nicht separabel	• $K = Q(\mathbb{F}_p[x^p])$, $L = Q(\mathbb{F}_p[x])$, $\alpha = x \in L$	• α insep. $\Rightarrow \lvert K \rvert = \infty$, $p = \mathrm{char}(K) \mid \deg_K(\alpha)$

Eigenschaften von Körpererweiterungen

Sei L/K eine Körpererweiterung, $\alpha \in L$, $f, g \in K[x]$ irreduzibel, $n \in \mathbb{N}$, $p \in \mathbb{N}$ prim.

Eigenschaft	**Definition**	**Beispiele**	**Bemerkungen**
Grad $[L:K]$	Dimension von L als Vektorraum über K	•$[K[x]/(f):K] = \deg(f)$, •$[\mathbb{Q}(e^{2\pi i/p}):\mathbb{Q}] = p-1$, • $[\mathbb{F}_{p^n}:\mathbb{F}_p] = n$	• Zwischenkörper $K \subset E \subset L$: $[L:K] = [L:E] \cdot [E:K]$
• L/K endlich	$[L:K] \in \mathbb{N}$	• $K[x]/(f)$, $\mathbb{F}_{p^n}/\mathbb{F}_p$, • $K(\alpha)$ für α alg.	• endlich $\Rightarrow$ algebraisch • algebraisch $\not\Rightarrow$ endlich
• L/K quadratisch	$[L:K] = 2$	• $\mathbb{C}/\mathbb{R}$, $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$	• quadratisch $\Rightarrow$ normal
• L/K unendlich	$[L:K] = \infty$	• $\mathbb{R}/\mathbb{Q}$, $\mathbb{Q}(\pi)/\mathbb{Q}$, $Q(K[x])/K$, $\overline{\mathbb{F}_p}$	
L/K primitiv	$\exists \alpha \in L:\ L = K(\alpha)$	• $K[x]/(f)$, • $Q(K[x])/K$, • $K = \mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{F}_{p^n}$ für L/K endlich, • L/K alg.,$[L:K]=6$	• primitiv $\not\Rightarrow$ algebraisch • primitiv $\not\Rightarrow$ endlich • endlich+sep. $\Rightarrow$ primitiv
L/K algebraisch	alle $\alpha \in L$ sind algebraisch über K	• $K[x]/(f)$, • L/K endlich, • algebraischer Abschluss $L = \overline{K}$	• endlich $\Rightarrow$ algebraisch, • normal $\Rightarrow$ algebraisch, • (in)sep. $\Rightarrow$ algebraisch • Zwischenkörper $K \subset E \subset L$: L/E,E/K alg. $\Rightarrow$ L/K alg.
L/K normal	L/K algebraisch und L Zerfällungskörper von $A \subset K[x]$	• L/K quadratisch, • $\overline{K}/K$, • $\mathbb{Q}(e^{2\pi i/p})$, • nicht normal: $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$,	• L/K normal $\Leftrightarrow \forall K$-Mono $\phi: L \to \overline{L}$ gilt $\phi(L) = L$. • L/K normal $\Leftrightarrow$ jd. irred. $p \in K[x]$ mit Nullstelle in L. zerfällt über L
L/K separabel	alle $\alpha \in L$ sind separabel über K	• $K = \mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{F}_{p^n}$ für L/K algebraisch,	• K vollkommen, L/K alg. $\Rightarrow$ L/K separabel • Zwischenkörper $K \subset E \subset L$: L/E,E/K sep. $\Rightarrow$ L/K sep. • $p = \mathrm{char}(K) \nmid [L:K] < \infty$ $\Rightarrow$ L/K sep.
L/K inseparabel	L/K algebraisch und nicht separabel über K	• $K = Q(\mathbb{F}_p[x^p])$, $L = Q(\mathbb{F}_p[x])$	• L/K inseparabel $\Rightarrow \mathrm{char}(K) \neq 0$, $\lvert K \rvert = \infty$
L/K transzendent	$\exists \alpha \in L$ transzendent über K	• $Q(K[x])/K$, • $\mathbb{R}/\mathbb{Q}$, $\mathbb{C}/\mathbb{Q}$, $\mathbb{Q}(\pi)/\mathbb{Q}$	• transzendent $\Rightarrow$ unendlich
L/K galoissch	$K = \mathcal{F}(\Gamma(L/K))$	• $\mathbb{F}_{p^n}/\mathbb{F}_p$, $\mathbb{C}/\mathbb{R}$ • $\mathbb{Q}(e^{2\pi i/n})$, • $\overline{\mathbb{F}}_p/\mathbb{F}_p$	• L/K algebraisch: galoissch$\Leftrightarrow$normal+separabel • galoissch $\not\Rightarrow$ algebraisch

Wichtige Galoisgruppen

Sei $p \in \mathbb{N}$ prim, $n, r, s \in \mathbb{N}$.

Körpererweiterung	**Galoisgruppe**	**Bemerkungen**
endliche Körper $\mathbb{F}_{q^s}/\mathbb{F}_q$ mit $q = p^r$	zyklisch, erzeugt von $\psi : \alpha \mapsto \alpha^q$, Ordnung $[\mathbb{F}_{q^s} : \mathbb{F}_q] = s$	• jede endliche Körpererweiterung eines endlichen Körpers ist von dieser Form
Kreisteilungskörper • K_n/K mit $\mathrm{char}(K) \nmid n$ • $\mathbb{Q}_n/\mathbb{Q}$	• Untergruppe von $(\mathbb{Z}/n\mathbb{Z})^\times$ • $(\mathbb{Z}/n\mathbb{Z})^\times \Leftrightarrow \Phi_{n,K}$ irreduzibel • $(\mathbb{Z}/n\mathbb{Z})^\times$	• $\mathrm{char}(K) = 0 \Rightarrow \mathrm{char}(K) \nmid n$ • $n = p$ prim $\Rightarrow \mathbb{Z}/(p-1)\mathbb{Z}$
einfache Radikalerweiterung von Grad n, Grundkörper enthält $n$te Einheitswurzel	zyklisch	• zyklisch $\Rightarrow$ abelsch
Zerfällungskörper von $q \in K[x]$, q auflösbar	auflösbar	• $\mathrm{char}(K) = 0$: p auflösbar $\Leftrightarrow$ Galoisgruppe von p auflösbar, • $p \in \mathbb{Q}[x]$, $\deg(p) \leq 4$ $\Rightarrow$ p auflösbar
$\mathbb{Q}(\sqrt{2}, \mathrm{i})$	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	
quadratisch+separabel	$\mathbb{Z}/2\mathbb{Z}$	
Zerfällungskörper von irred. Polynom $q \in \mathbb{Q}[x]$, Grad p, genau 2 Nullst. in $\mathbb{C} \setminus \mathbb{R}$	symmetrische Gruppe S_p	• auflösbar $\Leftrightarrow p \leq 4$

B Kreisteilungspolynome

Die Kreisteilungspolynome Φ_n für $n \leq 30$.

$$\Phi_1(x) = x - 1$$
$$\Phi_2(x) = x + 1$$
$$\Phi_3(x) = x^2 + x + 1$$
$$\Phi_4(x) = x^2 + 1$$
$$\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$$
$$\Phi_6(x) = x^2 - x + 1$$
$$\Phi_7(x) = x^6 + x^5 + x^4 + x^3 + x^2 + 1$$
$$\Phi_8(x) = \Phi_4(x^2) = x^4 + 1$$
$$\Phi_9(x) = \Phi_3(x^3) = x^6 + x^3 + 1$$
$$\Phi_{10}(x) = \Phi_5(-x) = x^4 - x^3 + x^2 - x + 1$$
$$\Phi_{11}(x) = x^{10} + x^9 + \ldots + x^2 + x + 1$$
$$\Phi_{12}(x) = \Phi_6(x^2) = x^4 - x^2 + 1$$
$$\Phi_{13}(x) = x^{12} + x^{11} + \ldots + x^2 + x + 1$$
$$\Phi_{14}(x) = \Phi_7(-x) = x^6 - x^5 + x^4 - x^3 + x^2 - x + 1$$
$$\Phi_{15}(x) = \Phi_3(x^5)/\Phi_3(x) = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1$$
$$\Phi_{16}(x) = \Phi_8(x^2) = x^8 + 1$$
$$\Phi_{17}(x) = x^{16} + x^{15} + \ldots + x^2 + x + 1$$
$$\Phi_{18}(x) = \Phi_9(-x) = x^6 - x^3 + 1$$
$$\Phi_{19}(x) = x^{18} + x^{17} + \ldots + x^2 + x + 1$$
$$\Phi_{20}(x) = \Phi_{10}(x^2) = x^8 - x^6 + x^4 - x^2 + 1$$
$$\Phi_{21}(x) = \Phi_3(x^7)/\Phi_3(x) = x^{12} - x^{11} + x^9 - x^8 + x^6 - x^4 + x^3 - x + 1$$
$$\Phi_{22}(x) = \Phi_{11}(-x) = x^{10} - x^9 + x^8 - x^7 + x^6 - x^5 + x^4 - x^3 + x^2 - x + 1$$
$$\Phi_{23}(x) = x^{22} + x^{21} + \ldots + x^2 + x + 1$$
$$\Phi_{24}(x) = \Phi_{12}(x^2) = x^8 - x^4 + 1$$
$$\Phi_{25}(x) = \Phi_5(x^5) = x^{20} + x^{15} + x^{10} + x^5 + 1$$
$$\Phi_{26}(x) = \Phi_{13}(-x) = x^{12} - x^{11} + x^{10} - x^9 + x^8 - x^7 + x^6 - x^5 + x^4 - x^3 + x^2 - x + 1$$
$$\Phi_{27}(x) = \Phi_9(x^3) = x^{18} + x^9 + 1$$
$$\Phi_{28}(x) = \Phi_{14}(x^2) = x^{12} - x^{10} + x^8 - x^6 + x^4 - x^2 + 1$$
$$\Phi_{29}(x) = x^{28} + x^{27} + \ldots + x^2 + x + 1$$
$$\Phi_{30}(x) = \Phi_{15}(-x) = x^8 + x^7 - x^5 - x^4 - x^3 + x + 1.$$

Index

K-Automorphismus, 26
K-Isomorphismus, 26
K-Monomorphismus, 26
K-Monomorphismus, 26
m-fache Nullstelle, 31

abelsche Körpererweiterung, 49
abgeschlossene Untergruppe der Galoisgruppe, 51
abgeschlossener Zwischenkörper, 51
Adjunktion, 16
algebraisch abgeschlossen, 23
algebraische Ableitung, 31
algebraische Körpererweiterung, 19
algebraischer Abschluss, 23
algebraischer Abschluss (in einem Erweiterungskörper), 21
algebraisches Element, Körpererweiterung, 19
auflösbar durch Radikale, Körpererweiterung, 80
auflösbar durch Radikale, Polynom, 80
auflösbar, Gruppe, 83
Auswertung, 7

Charakteristik, 5

Dedekinsches Lemma, 82

echte Zwischenkörper, 15
Einbettung in Galoiserweiterungen, 54
einfache Körpererweiterung, 16
einfache Nullstelle bzw. Wurzel, 31
einfache Radikalerweiterung, 80
Einheiten, 5
Einheitswurzeln, 59
Eisensteinkriterium, 12
endliche Körpererweiterung, 14
Erweiterungskörper, 14
euklidischer Ring, 8

faktorieller Ring, 8
Fermatschen Primzahlen, 79
Fixkörper, 49
formale Ableitung, 31
Fortsetzungssatz für K-Monomorphismen in algebraisch abgeschlossene Körper, 29
Fortsetzungssatz für primitive Körpererweiterungen, 27
Fortsetzungssatz für Zerfällungskörper, 27
Frobeniusabbildung, 5, 25
Frobeniusmonomorphismus, 5

Galois-Gruppe, 27
Galois-Korrespondenz, 52
Galoiserweiterung, 49
Galoisgruppe, 48, 49
Galoisgruppe, Polynom, 49
galoissch, 49
gebrochen rationalen Funktionen, 8
Grad, algebraisches Element, 19
Grad, Körpererweiterung, 14
Grad, Polynom, 7
Gradsatz, 15
Grundkörper, 14

Hauptidealring, 7
Hauptsatz der endlichen Galoistheorie, 57

Ideal, maximales, 6
Integritätsbereich, 6
irreduzibel, Polynom, 8
Irreduzibilitätskriterien, 11

Körper, 5
Körpererweiterung, 14
Körperhomomorphismus, 14
Körperisomorphismus, 14
Körpermonomorphismus, 14
Körperverband, 15
Klassifikation endlicher Körper, 40
Kommutatorgruppe, 82
Kompositum, 52
konstruierbar, 71
Kreisteilungskörper, 59
Kreisteilungspolynom, 13, 61

Leitkoeffizient, 7

mehrfache Nullstelle bzw. Wurzel, 31
Menge der konstruierbaren Punkte, 71
Minimalpolynom, 19

normal+separabel=galoissch, 53
normale Hülle, 30
normale Körpererweiterung, 29
normiert, 7
nte Kommutatorgruppe, 83

Nullstelle, 9

Polynom, 7
Polynomring, 7
primitive $n$te Einheitswurzel, 59
primitive Körpererweiterung, 16
primitives Element, 16
primitives Polynom, 12
Primkörper, 14

quadratische Körpererweiterung, 14
Quotientenkörper, 6

Radikal, 80
Radikalerweiterung, 80
Rationale Nullstellen, 11
Reduktion mod p, 12
reine Gleichung, 80
reines Polynom, 80
Restklassenkörper, 6

Satz und Lemma von Gauß, 11
Satz vom primitiven Element, 35
Satz von Dedekind, 56
Satz von Kronecker, 22
Satz von Krull, 55
Satz von Steinitz, 23
separabel, Element in Erweiterungskörper, 33
separabel, Körpererweiterung, 33
separabel, Polynom, 32
Separabilitätsgrad, 37
separabler Abschluss, 37

Teilkörper, 14
Teilkörper endlicher Körper, 41
transzendente Körpererweiterung, 19
transzendentes Element, Körpererweiterung, 19

unendliche Körpererweiterung, 14
universelle Eigenschaft des Polynomrings, 8
Universelle Eigenschaft des Quotientenkörpers, 6

Vielfachheit, 31
vollkommen, 33

Wurzel, Polynom, 9

Zerfällungkörper, 25
Zwischenkörper, 15
Zwischenkörperdiagramm, 58
zyklische Körpererweiterung, 49