Einführung in die Algebra

Thomas Markwig
Fachbereich Mathematik
Technische Universität Kaiserslautern

Vorlesungsskript

Wintersemester 2014/15

Inhaltsverzeichnis

KAPITEL I

Faktorielle Ringe und Irreduzibilität

In diesem Kapitel wollen wir einige Eigenschaften von Ringen, insbesondere von Polynomringen, herleiten, die in Kapitel II bei der Konstruktion von Beispielen für Körpererweiterungen nützlich sein werden. Alle in diesem Kapitel betrachteten Ringe sollen kommutative Ringe mit Eins sein, wie sie in der Vorlesung Algebraische Strukturen eingeführt wurden (siehe [**Mar08a**, §6]). Wir werden zudem die dort eingeführten Grundbegriffe der Ringtheorie verwenden wie Einheit, assoziierte Elemente, Integritätsbereich, prim, irreduzibel (siehe [**Mar08a**, §§6-7]). Ferner werden die dort bewiesenen grundlegenden Aussage als bekannt vorausgesetzt, wie etwa, daß jedes Primelement irreduzibel ist und daß in einem Hauptidealring auch die Umkehrung gilt (siehe [**Mar08a**, §7]).

§ 1 Faktorielle Ringe

Der zentrale Begriff dieses Abschnitts ist der des faktoriellen Rings, der bereits in der Vorlesung Algebraische Strukturen eingeführt wurde (siehe [**Mar08a**, Def. 7.14]). Wir wollen die Definition der Vollständigkeit halber noch einmal wiederholen und erinnern an einige wichtige Eigenschaften in faktoriellen Ringen.

Definition 1.1 (Primfaktorzerlegung)
Es sei R ein Integritätsbereich.

a. Für $0 \neq a \in R \setminus R^*$ heißt eine Darstellung

$$a = p_1 \cdot \ldots \cdot p_k$$

von a als Produkt endlich vieler Primelemente $p_1, \ldots, p_k \in R$ eine *Primfaktorzerlegung* von a.

b. Ein Ring R heißt *faktoriell* oder ein *ZPE-Ring*, wenn jedes $0 \neq a \in R \setminus R^*$ eine Primfaktorzerlegung besitzt.

Beispiel 1.2
Hauptidealringe sind faktoriell (siehe [**Mar08a**, Satz 7.60]).
Insbesondere sind $\mathbb{Z}$ und der Polynomring $K[t]$ über einem Körper K faktoriell.

Bemerkung 1.3
Es sei R ein Integritätsbereich, $u \in R^*$ und $0 \neq p \in R \setminus R^*$.
Genau dann ist p prim, wenn $u \cdot p$ prim ist.

Proposition 1.4 (Eigenschaften faktorieller Ringe)
Es sei R *ein faktorieller Ring.*

a. *Genau dann ist* $p \in R$ *irreduzibel, wenn* p *prim ist.*

b. *Primfaktorzerlegungen sind bis auf die Reihenfolge und die Assoziiertheit eindeutig. Genauer gilt, wenn* $a = p_1 \cdot \ldots \cdot p_k = q_1 \cdot \ldots \cdot q_l$ *zwei Primfaktorzerlegungen von* a *sind, so gilt*

$$k = l$$

und es gibt eine Permutation $\sigma \in \mathbb{S}_k$ *mit*

$$\langle p_i \rangle = \langle q_{\sigma(i)} \rangle$$

für $i = 1, \ldots, k$*, d.h.* p_i *ist zu* $q_{\sigma(i)}$ *assoziiert.*

c. *Eine Teilmenge* $\mathbb{P}_R$ *von* R *heißt ein* vollständiges Vertretersystem für die Primelemente *in* R*, wenn jedes Primelement in* R *zu genau einem Element in* $\mathbb{P}_R$ *assoziiert ist.*
Ist $\mathbb{P}_R$ *ein vollständiges Vertretersystem für die Primelemente in* R*, so besitzt jedes* $0 \neq a \in R$ *eine* eindeutige *Darstellung der Form*

$$a = u \cdot \prod_{p \in \mathbb{P}_R} p^{n_p(a)}$$

mit $u \in R^*$ *und*

$$n_p(a) = \max\left\{ n \in \mathbb{N} \;\middle|\; p^n \mid a \right\}$$

für $p \in \mathbb{P}_R$.

d. *Je zwei Elemente in* R *haben einen größten gemeinsamen Teiler und ein kleinstes gemeinsames Vielfaches.*

Beweis:

a. Ist $p \in R$ irreduzibel und ist $p = q_1 \cdot \ldots \cdot q_k$ eine Primfaktorzerlegung von p, so folgt $k = 1$, da ansonsten q_1 und $q_2 \cdot \ldots \cdot q_k$ keine Einheiten sind und p sich somit als Produkt zweier Nicht-Einheiten schreiben ließe im Widerspruch zur Irreduzibilität von p. Also ist $p = q_1$ prim.
Umgekehrt wissen wir schon, daß jedes Primelement irreduzibel ist (siehe [**Mar08a**, Lemma 7.16]).

b. Siehe [**Mar08a**, Bemerkung 7.14].

c. Dies folgt aus Teil b. unter Beachtung von Bemerkung 1.3 durch Zusammenfassung von assoziierten Primelementen.

d. Sind $0 \neq a, b \in R$ gegeben, so gilt

$$\prod_{p \in \mathbb{P}_R} p^{\min\{n_p(a), n_p(b)\}} \in \mathrm{ggT}(a, b)$$

und

$$\prod_{p\in\mathbb{P}_R} p^{\max\{n_p(a),n_p(b)\}} \in \mathrm{kgV}(a,b),$$

wie man mit Hilfe der Primfaktorzerlegung leicht nachprüft, wenn man folgende offensichtliche Äquivalenz beachtet:

$$c \mid d \quad\Longleftrightarrow\quad n_p(c) \le n_p(d) \;\; \forall\, p \in \mathbb{P}_R.$$

□

Bemerkung 1.5
Es sei R ein Integritätsbereich.

a. Die Begriffe größter gemeinsamer Teiler und kleinstes gemeinsames Vielfaches lassen sich für mehr als zwei Elemente definieren, und in faktoriellen Ringen existieren sie ebenfalls stets mit der offensichtlichen Verallgemeinerung der Formeln im Beweis von Proposition 1.4:

$$\prod_{p\in\mathbb{P}_R} p^{\min\{n_p(a_1),\ldots,n_p(a_n)\}} \in \mathrm{ggT}(a_1,\ldots,a_n)$$

und

$$\prod_{p\in\mathbb{P}_R} p^{\max\{n_p(a_1),\ldots,n_p(a_n)\}} \in \mathrm{kgV}(a_1,\ldots,a_n)$$

für $0 \neq a_1,\ldots,a_n \in R$. Für größte gemeinsame Teiler siehe etwa [**Mar08b**, Definition 2.1 und Proposition 2.2].

b. Größte gemeinsame Teiler und kleinste gemeinsame Vielfache sind stets bis auf Assoziiertheit eindeutig bestimmt.

Die zentrale Aussage, die wir in diesem Abschnitt beweisen wollen, ist der folgende Satz, der auch als Lemma von Gauß bezeichnet wird. Sein Beweis erfordert, daß wir den Koeffizientenbereich R der betrachteten Polynome erweitern. Nachdem wir den Satz formuliert haben, werden wir deshalb zunächst die für den Beweis benötigten Begriffe einführen und einige Hilfsaussagen herleiten, bevor wir den Abschnitt mit dem Beweis des Satzes abschließen.

Satz 1.6 (Lemma von Gauß)
Ist R *ein faktorieller Ring, so ist auch* $R[t]$ *faktoriell.*

Definition und Satz 1.7 (Der Quotientenkörper)
Es sei R ein Integritätsbereich und $S = R \setminus \{0\}$.

Auf der Menge $R \times S$ wird durch

$$(r,s) \sim (r',s') \quad :\Longleftrightarrow\quad r\cdot s' = r'\cdot s$$

für $(r,s),(r',s') \in R \times S$ eine Äquivalenzrelation definiert. Wir bezeichnen die Äquivalenzklasse von $(r,s) \in R \times S$ mit

$$\frac{r}{s} := \{(r',s') \in R \times S \mid (r',s') \sim (r,s)\}$$

und nennen die Menge der Äquivalenzklassen

$$\mathrm{Quot}(R) := Q(R) := \left\{ \frac{r}{s} \;\middle|\; (r,s) \in R \times S \right\}$$

den *Quotientenkörper* von R.

Die Operationen

$$\frac{r}{s} + \frac{r'}{s'} := \frac{r \cdot s' + r' \cdot s}{s \cdot s'}$$

und

$$\frac{r}{s} \cdot \frac{r'}{s'} := \frac{r \cdot r'}{s \cdot s'}$$

sind wohldefiniert und $(\mathrm{Quot}(R), +, \cdot)$ ist ein Körper. Zudem ist die Abbildung

$$i : R \longrightarrow \mathrm{Quot}(R) : r \mapsto \frac{r}{1}$$

ein Ringmonomorphismus.

Beweis: Der Beweis der Aussagen ist dem Leser als Übungsaufgabe überlassen. □

Definition 1.8 (Primitives Polynom)
Es sei R ein Integritätsbereich und $0 \neq f = \sum_{i=0}^{n} a_i t^i \in R[t]$ ein Polynom. Wir nennen f *primitiv*, wenn die Koeffizienten $a_0, \ldots, a_n$ teilerfremd sind, d.h.

$$1 \in \mathrm{ggT}(a_0, \ldots, a_n).$$

Definition und Bemerkung 1.9 (Der Inhalt eines Polynoms)
Es sei R ein faktorieller Ring und $0 \neq f = \sum_{i=0}^{n} a_i t^i \in R[t]$ ein Polynom.

Wir nennen die Menge

$$\begin{aligned} \mathrm{cont}_R(f) &:= \mathrm{ggT}(a_0, \ldots, a_n) \\ &= \{g \in R \mid g \text{ ist ein größter gemeinsamer Teiler von } a_0, \ldots, a_n\} \end{aligned}$$

den *Inhalt* von f. Die Elemente in $\mathrm{cont}_R(f)$ sind bis auf Multiplikation mit einer Einheit eindeutig bestimmt.

Man beachte, daß f genau dann primitiv ist, wenn $\mathrm{cont}_R(f) = R^*$ die Menge der Einheiten in R ist. Ferner ist f/c für jedes $c \in \mathrm{cont}_R(f)$ primitiv.

Beispiel 1.10

a. Ist K ein Körper, so ist jedes Polynom $0 \neq f \in K[t]$ primitiv.

b. Das Polynom $f = 2t + 2 \in \mathbb{Z}[t]$ ist nicht primitiv in $\mathbb{Z}[t]$, wohl aber in $\mathbb{Q}[t]$.

Bemerkung 1.11
Es sei R ein faktorieller Ring.

a. Ist $f \in R[t]$ primitiv und $c \in \mathrm{Quot}(R)$ mit $c \cdot f \in R[t]$, so ist $c \in R$.

b. Ist $0 \neq f \in \mathrm{Quot}(R)[t]$, so gibt es ein $0 \neq c \in \mathrm{Quot}(R)$ und ein $g \in R[t]$ primitiv, so daß $f = c \cdot g$.

Beweis: Für den Beweis von Teil a. betrachten wir das primitive Polynom

$$f = \sum_{i=0}^{n} a_i t^i \in R[t]$$

und wir schreiben

$$c = \frac{a}{b}$$

mit $a, b \in R$ so, daß a und b teilerfremd sind. Wegen $c \cdot f \in R[t]$ gilt dann

$$\frac{a \cdot a_i}{b} \in R \tag{1}$$

für alle $i = 0, \ldots, n$. Ist $p \in R$ ein Primteiler von b, so folgt aus Gleichung (1) und weil p kein Teiler von a ist, daß p ein Teiler von a_i für alle $i = 0, \ldots, n$ ist. Da f nach Voraussetzung primitiv ist und die a_i somit keinen gemeinsamen Primteiler haben, hat auch b keinen Primteiler, d.h. $b \in R^*$ und

$$c = \frac{a}{b} \in R.$$

Für den Teil b. betrachten wir das Polynom

$$0 \neq f = \sum_{i=0}^{n} \frac{a_i}{b_i} \cdot t^i \in \mathrm{Quot}(R)[t]$$

mit $a_i \in R$ und $b_i \in R \setminus \{0\}$. Dann ist

$$b_0 \cdot \ldots \cdot b_n \cdot f \in R[t]$$

und für

$$d \in \mathrm{cont}_R(b_0 \cdot \ldots \cdot b_n \cdot f)$$

gilt dann

$$g := \frac{b_0 \cdot \ldots \cdot b_n \cdot f}{d} \in R[t]$$

ist primitiv und

$$c \cdot g = f$$

für

$$0 \neq c = \frac{d}{b_0 \cdot \ldots \cdot b_n} \in \mathrm{Quot}(R).$$

□

Lemma 1.12
Ist R ein faktorieller Ring und $p \in R$ prim in R, dann ist p auch prim in $R[t]$.

Beweis: Seien $f = \sum_{i=0}^{n} a_i t^i$ und $g = \sum_{j=0}^{m} b_j t^j$ zwei Polynome in $R[t]$, so daß p das Produkt

$$f \cdot g = \sum_{k=0}^{m+n} c_k t^k$$

mit

$$c_k = \sum_{l=0}^{k} a_l \cdot b_{k-l} \tag{2}$$

in $R[t]$ teilt. Dann teilt p jeden der Koeffizienten c_k in R.

Nehmen wir nun an, daß p weder f noch g in $R[t]$ teilt, dann gibt es Indizes i_0 und j_0, so daß p kein Teiler von a_{i_0} und kein Teiler von b_{j_0} in R ist. Wir wählen i_0 und j_0 minimal mit dieser Eigenschaft. Wegen der Minimalität der Indizes und weil p ein Teiler von $c_{i_0+j_0}$ ist, teilt dann p in R jeden Summanden der rechten Seite der Gleichung

$$a_{i_0} \cdot b_{j_0} \overset{(2)}{=} c_{i_0+j_0} - \sum_{l=0}^{i_0-1} a_l \cdot b_{i_0+j_0-l} - \sum_{l=i_0+1}^{i_0+j_0} a_l \cdot b_{i_0+j_0-l},$$

also auch die linke Seite. Da p in R prim ist, teilt p dann aber schon a_{i_0} oder b_{j_0} im Widerspruch zur Wahl von i_0 und j_0. Also ist die Annahme falsch und p teilt f oder g in $R[t]$. □

Lemma 1.13 (Gauß)
Ist R ein faktorieller Ring und sind $f, g \in R[t]$ primitiv, so ist auch $f \cdot g$ primitiv.

Beweis: Nehmen wir an, daß $f \cdot g$ nicht primitiv ist. Dann gibt es ein Primelement $p \in R$, das jeden Koeffizienten von $f \cdot g$ in R teilt und damit in $R[t]$ ein Teiler des Produktes $f \cdot g$ ist. Wegen Lemma 1.12 ist dann p ein Teiler von f oder g in $R[t]$ und damit ein Teiler von jedem Koeffizienten des Polynoms in R. Das widerspricht der Annahme, daß beide Polynome primitiv sind. □

Lemma 1.14
Sei R ein faktorieller Ring und $f \in R[t]$ sei primitiv in $R[t]$ und prim in $\mathrm{Quot}(R)[t]$. Dann ist f prim in $R[t]$.

Beweis: Wir beachten zunächst, daß f als primitives Polynom in $R[t]$ nicht das Nullpolynom ist und daß f als Primelement von $\mathrm{Quot}(R)[t]$ keine Einheit in $R[t]$ sein kann.

Seien nun $g, h \in R[t]$ zwei Polynome, so daß f das Produkt $g \cdot h$ in $R[t]$ teilt. Wir müssen zeigen, daß f dann in $R[t]$ ein Teiler von g oder von h ist.

Da f in $\mathrm{Quot}(R)[t]$ prim ist, teilt f eines der Polynome g oder h in $\mathrm{Quot}(R)[t]$ und wir können ohne Einschränkung annehmen, daß dies für g der Fall ist. Es gibt also ein Polynom $k \in \mathrm{Quot}(R)[t]$, so daß

$$g = f \cdot k.$$

Wir wollen nun zeigen, daß k bereits in $R[t]$ liegt. Dazu schreiben wir das Polynom k wie in Bemerkung 1.11 als

$$k = c \cdot q$$

für ein primitives Polynom $q \in R[t]$ und ein $0 \neq c \in \mathrm{Quot}(R)$. Dann gilt

$$g = f \cdot k = c \cdot f \cdot q,$$

wobei das Polynom $f \cdot q$ nach Lemma 1.13 primitiv ist. Aus Bemerkung 1.11 folgt dann aber, daß c ein Element in R ist. Somit ist

$$k = c \cdot q \in R[t]$$

gezeigt und f ist ein Teiler von g in $R[t]$. Damit haben wir gezeigt, daß f ein Primelement in $R[t]$ ist. □

Beweis des Lemmas von Gauß 1.6: Es sei $0 \neq f \in R[t] \setminus R^*$ eine Nicht-Einheit und nicht Null. Wir müssen zeigen, daß sich f als Produkt von endlich vielen Primelementen schreiben läßt.

Ist f ein konstantes Polynom, so besitzt f in R eine Primfaktorzerlegung, da R faktoriell ist, und diese ist nach Lemma 1.12 auch eine Primfaktorzerlegung in $R[t]$.

Wir können also annehmen, daß f mindestens Grad 1 hat. Da $\mathrm{Quot}(R)$ ein Körper ist, ist der Polynomring $\mathrm{Quot}(R)[t]$ faktoriell und f läßt sich schreiben als

$$f = q_1 \cdot \ldots \cdot q_k$$

mit $q_i \in \mathrm{Quot}(R)[t]$ prim. Gemäß Bemerkung 1.11 schreiben wir q_i als

$$q_i = c_i \cdot p_i$$

mit $p_i \in R[t]$ primitiv und $0 \neq c_i \in \mathrm{Quot}(R)$. Die Polynome q_i und p_i sind assoziiert in $\mathrm{Quot}(R)[t]$, so daß mit q_i auch p_i ein Primelement in $\mathrm{Quot}(R)[t]$ ist. Wegen Lemma 1.14 ist das primitive Polynom p_i dann auch prim in $R[t]$.

Zudem wissen wir aus Lemma 1.13, daß das Polynom

$$p := p_1 \cdot \ldots \cdot p_k \in R[t]$$

primitiv ist, so daß wir wegen

$$f = c_1 \cdot \ldots \cdot c_k \cdot p \in R[t]$$

aus Bemerkung 1.11

$$c := c_1 \cdot \ldots \cdot c_k \in R$$

erhalten. Da R faktoriell ist, besitzt c in R eine Primfaktorzerlegung

$$c = a_1 \cdot \ldots \cdot a_m$$

und die a_i sind mit Lemma 1.12 auch prim in $R[t]$. Damit ist

$$f = a_1 \cdot \ldots \cdot a_m \cdot p_1 \cdot \ldots \cdot p_k$$

eine Zerlegung von f in Primpolynome in $R[t]$. □

§ 2 Irreduzibilitätskriterien

Wir werden in Kapitel II Körpererweiterungen untersuchen. Dabei wird eine zentrale Frage sein, wie man zu einem gegebenen Körper K einen größeren Körper mit vorgegebenen Eigenschaften konstruieren kann. Die folgende Proposition zeigt, weshalb irreduziblen Polynomen dabei eine zentrale Rolle zukommt.

Proposition 2.1
In einem Hauptidealring R ist p genau dann irreduzibel, wenn $R/\langle p\rangle$ ein Körper ist. Insbesondere, ist K ein Körper und $f \in K[t]$ irreduzibel, so ist $K[t]/\langle f\rangle$ ein Körper.

Beweis: Setzen wir zunächst voraus, daß p irreduzibel ist. Da R ein Hauptidealring ist, ist p dann auch ein Primelement in R. Betrachten wir nun eine Restklasse $\overline{0} \neq \overline{a} \in R/\langle p\rangle$, so müssen wir zeigen, daß $\overline{a}$ in $R/\langle p\rangle$ ein multiplikatives Inverses besitzt. Aus $\overline{a} \neq \overline{0}$ folgt, daß p kein Teiler von a ist. Da p prim ist, sind p und a mithin teilerfremd und aus der Bézout-Identität (siehe [**Mar08a**, Satz 7.54]) folgt dann die Existenz von $b, c \in R$ mit

$$1 = b \cdot a + c \cdot p.$$

Modulo p liest die Gleichung sich als

$$\overline{1} = \overline{b} \cdot \overline{a} + \overline{c} \cdot \overline{p} = \overline{b} \cdot \overline{a} + \overline{c} \cdot \overline{0} = \overline{b} \cdot \overline{a}$$

und $\overline{b}$ ist das gesuchte Inverse zu $\overline{a}$.

Setzen wir nun umgekehrt voraus, daß $R/\langle p\rangle$ ein Körper ist und betrachten wir ein Produkt $a \cdot b$ in R, das von p geteilt wird. Dann gilt für die Restklassen

$$\overline{a} \cdot \overline{b} = \overline{a \cdot b} = \overline{0} \in R/\langle p\rangle.$$

In einem Körper erzwingt das $\overline{a} = \overline{0}$ oder $\overline{b} = \overline{0}$, was sich zu $p \mid a$ oder $p \mid b$ übersetzt. Also ist p prim und damit auch irreduzibel. □

Im weiteren Verlauf des Abschnitts wollen wir Methoden kennen lernen, mit Hilfe derer man in vielen Fällen entscheiden kann, ob ein Polynom irreduzibel ist.

Satz 2.2 (Das Eisenstein-Kriterium)
Es sei R ein faktorieller Ring und $f = \sum_{i=0}^{n} a_i t^i \in R[t] \setminus R^*$ ein primitives Polynom. Wenn es ein Primelement $p \in R$ gibt, so daß p ein Teiler von $a_0, \ldots, a_{n-1}$ ist und p^2 kein Teiler von a_0 ist, dann ist f irreduzibel in $R[t]$.

Beweis: Als primitives Polynom ist f nicht 0 und nach Voraussetzung ist f auch keine Einheit in $R[t]$. Wir müssen also zeigen, daß aus $f = g \cdot h$ für $g, h \in R[t]$ folgt, daß g oder h eine Einheit in $R[t]$ ist.

Nehmen wir stattdessen an, $f = g \cdot h$ mit $g = \sum_{i=0}^{k} b_i t^i \in R[t]$ vom Grad k und $h = \sum_{j=0}^{l} c_j t^j \in R[t]$ vom Grad l.

Wenn $k = 0$ gilt, so ist $g \in R$ ein Teiler aller Koeffizienten von f und mithin eine Einheit, da f primitiv ist. Analog ist h eine Einheit, wenn $l = 0$ gilt.

Es bleibt also nur der Fall $k, l > 0$ und damit zugleich $k, l < n$ zu betrachten. Aus $f = g \cdot h$ folgt

$$a_k = \sum_{i+j=k} b_i \cdot c_j \tag{3}$$

für $k = 0, \ldots, n$. Nach Voraussetzung gilt

$$p \mid a_0 = b_0 \cdot c_0,$$

und da p prim ist, können wir ohne Einschränkung

$$p \mid b_0$$

annehmen. Da p^2 kein Teiler von a_0 ist, folgt zugleich

$$p \nmid c_0.$$

Wir zeigen nun mit Induktion nach i, daß

$$p \mid b_i$$

für alle $i = 0, \ldots, k$ gelten muß. Für den Induktionsschritt setzen wir voraus, daß die Eigenschaft für alle Indizes von 0 bis $i - 1$ bereits gezeigt ist. Aus (3) folgt

$$b_i \cdot c_0 = a_i - b_{i-1} \cdot c_1 - b_{i-2} \cdot c_2 - \ldots - b_0 \cdot c_i$$

und die rechte Seite ist wegen der Voraussetzung $p \mid a_i$ (für $i < n$) und wegen der Induktionsvoraussetzung durch p teilbar. Also haben wir

$$p \mid b_i \cdot c_0$$

gezeigt. Da p prim ist und c_0 nicht teilt, muß p also b_i teilen. Wir haben also mit Induktion gezeigt, daß p jeden Koeffizienten von g teilt, dann gilt aber auch

$$p \mid b_k \cdot c_l = a_n$$

im Widerspruch dazu, daß f primitiv ist und p deshalb nicht alle Koeffizienten von f teilen kann. □

Beispiel 2.3
Das Polynom

$$f = t^5 - 4t + 2 \in \mathbb{Z}[t]$$

ist als normiertes Polynom primitiv. Zudem teilt die Primzahl 2 alle Koeffizienten außer dem Leitkoeffizienten und $2^2 = 4$ ist kein Teiler des konstanten Anteils von f. Also ist f nach dem Eisensteinkriterium irreduzibel in $\mathbb{Z}[t]$.

In Proposition 2.1 haben wir gezeigt, weshalb irreduzible Polynome über Körpern interessant sind. Das Eisensteinkriterium ist aber nur dann anwendbar, wenn es im Koeffizientenbereich des Polynoms Primelemente gibt, was für einen Körper ganz sicher nicht der Fall ist. Wieso kann man das Eisensteinkriterium dennoch auch in Polynomringen über Körpern gewinnbringend einsetzen?

Satz 2.4
Sei R *ein faktorieller Ring. Ein Polynom* $f \in R[t] \setminus R$ *ist genau dann irreduzibel in* $R[t]$*, wenn* f *primitiv in* $R[t]$ *und irreduzibel in* $\mathrm{Quot}(R)[t]$ *ist.*

Beweis: Man beachte, daß wegen des Lemmas von Gauß 1.6 die Ringe $R[t]$ und $\mathrm{Quot}(R)[t]$ faktoriell sind und daß deshalb die Begriffe prim und irreduzibel zusammenfallen.

Ist f also primitiv und irreduzibel in $\mathrm{Quot}(R)[t]$, so ist f nach Lemma 1.14 auch irreduzibel in $R[t]$.

Ist umgekehrt f irreduzibel in $R[t]$ und ist $f = g \cdot h$ mit $g, h \in \mathrm{Quot}(R)[t]$, so können wir g und h gemäß Bemerkung 1.11 schreiben als

$$g = c \cdot p$$

und

$$h = d \cdot q$$

mit $p, q \in R[t]$ primitiv und $0 \neq c, d \in \mathrm{Quot}(R)$. Da nach Lemma 1.13 auch $p \cdot q \in R[t]$ primitiv ist, folgt aus

$$f = (c \cdot d) \cdot p \cdot q \tag{4}$$

und Bemerkung 1.11, daß $c \cdot d \in R$. Da es sich bei Gleichung (4) mithin um eine Gleichung in $R[t]$ handelt, folgt dann aus der Irreduzibilität von f, daß zwei der drei Faktoren cd, p und q Einheiten in $R[t]$ sein müssen. Dann ist aber $g = c \cdot p$ oder $h = d \cdot q$ eine Einheit in $\mathrm{Quot}(R)[t]$ und somit ist f irreduzibel in $\mathrm{Quot}(R)[t]$. Zudem muß f primitiv sein, da für $c \in \mathrm{cont}_R(f)$

$$f = c \cdot \frac{f}{c}$$

sonst eine Zerlegung von f in zwei Nicht-Einheiten wäre, weil $\frac{f}{c}$ mindestens Grad 1 hat. □

Beispiel 2.5
Wegen Satz 2.4 und Beispiel 2.3 ist das primitive Polynom $f = t^4 - 4t + 2 \in \mathbb{Z}[t]$ auch irreduzibel in $\mathbb{Q}[t]$.

Definition and Proposition 2.6 (Reduktion mod p)
Es sei R ein Ring und $p \in R$. Die Restklassenabbildung

$$R \longrightarrow R/\langle p \rangle : a \mapsto \overline{a}$$

induziert einen Ringepimorphismus

$$\rho_p : R[t] \longrightarrow R/\langle p \rangle[t] : \sum_{i=0}^{n} a_i t^i \mapsto \sum_{i=0}^{n} \overline{a_i} \cdot t^i,$$

den wir die *Reduktion mod* p nennen. Wenn der Kontext klar ist, schreiben wir auch einfach $\overline{f}$ statt $\rho_p(f)$ für ein Polynom $f \in R[t]$.

Beweis: Daß es sich um einen Ringepimorphismus handelt ist offensichtlich (siehe auch [**Mar08a**, S. 131f.]). □

Bemerkung 2.7 (Reduktion mod p)
Ist R ein Integritätsbereich und $p \in R$ prim, so ist auch $R/\langle p\rangle$ ein Integritätsbereich.

Beweis: Den Beweis der Aussage haben wir im Prinzip schon im Beweis von Proposition 2.1 gesehen. Aus

$$\overline{0} = \overline{a} \cdot \overline{b} = \overline{a \cdot b}$$

folgt, daß p ein Teiler von $a \cdot b$ ist. Ist p prim, so teilt p mithin a oder b, und das heißt, daß $\overline{a}$ oder $\overline{b}$ null sein muß. Damit haben wir gezeigt, daß $R/\langle p\rangle$ ein Integritätsbereich ist. □

Proposition 2.8 (Reduktion mod p)
Sei R ein Integritätsbereich, $p \in R$ prim, $f = \sum_{i=0}^{n} a_i t^i \in R[t]$ primitiv mit $p \nmid a_n$. Ist die Reduktion $\overline{f} = \rho_p(f)$ mod p irreduzibel in $R/\langle p\rangle[t]$, so ist f irreduzibel in $R[t]$.

Beweis: Da ein Ringhomomorphismus Einheiten auf Einheiten abbildet und $\overline{f}$ keine Einheit ist, kann f auch keine Einheit sein. Zudem ist f als primitives Polynom nicht das Nullpolynom.

Ist $f = g \cdot h$ mit $g, h \in R[t]$, so müssen wir zeigen, daß g oder h eine Einheit in $R[t]$ ist. Nach Voraussetzung teilt p den Leitkoeffizienten von f nicht, und da dieser das Produkt der Leitkoeffizienten von g und h ist, werden auch deren Leitkoeffizienten nicht von p geteilt. Damit gilt dann aber unmittelbar

$$\deg(f) = \deg(\overline{f}), \quad \deg(g) = \deg(\overline{g}) \quad \text{und} \quad \deg(h) = \deg(\overline{h}).$$

Da $\overline{f}$ irreduzibel ist, können wir ohne Einschränkung annehmen, daß $\overline{g}$ eine Einheit in $R/\langle p\rangle[t]$ ist. Damit gilt dann insbesondere

$$\deg(g) = \deg(\overline{g}) = 0.$$

Mithin ist $g \in R$ ein Teiler von jedem Koeffizienten von f, und da f primitiv ist, folgt, daß $g \in R^* = R[t]^*$ eine Einheit ist. Damit haben wir gezeigt, daß f irreduzibel ist. □

Beispiel 2.9
Das primitive Polynom

$$f = t^4 + t^3 + t^2 + t + 1 \in \mathbb{Z}[t]$$

ist irreduzibel in $\mathbb{Z}[t]$ und mithin auch in $\mathbb{Q}[t]$.

Um dies zu sehen, betrachten wir die Reduktion mod 2 und erhalten das Polynom

$$\overline{f} = t^4 + t^3 + t^2 + t + \overline{1} \in \mathbb{Z}_2[t].$$

Wäre dieses reduzibel, müßte es einen irreduziblen Faktor vom Grad 1 oder 2 haben. Diese können wir leicht bestimmen:

$$t, t + \overline{1}, t^2 + t + \overline{1}.$$

Die ersten beiden Polynome scheiden als Faktoren aus, weil weder $\overline{0}$ noch $\overline{1}$ Nullstellen von $\overline{f}$ sind. Das dritte Polynom schließt man mittels einer einfachen Polynomdivision als Faktor aus.

Proposition 2.10 (Lineare Koordinatentransformationen $t \mapsto at + b$)
Es sei R *ein Integritätsbereich,* $a \in R^*$ *und* $b \in R$*. Dann ist die lineare Koordinatentransformation*

$$\Phi_{a,b} : R[t] \longrightarrow R[t] : f \mapsto f(at + b)$$

ein Ringisomorphismus.
Insbesondere gilt, $f \in R[t]$ *ist genau dann irreduzibel, wenn* $\Phi_{a,b}(f)$ *irreduzibel ist.*

Beweis: Offenbar ist der Einsetzhomomorphismus $\Phi_{a,b}$ ein Ringhomomorphismus (siehe auch [**Mar08a**, Lemma 7.36]) und $\Phi_{\frac{1}{a},-\frac{b}{a}}$ ist die Umkehrabbildung von $\Phi_{a,b}$. □

Beispiel 2.11 (Kreisteilungspolynome)
Wir wollen nun zeigen, daß das Polynom

$$f = t^{p-1} + t^{p-2} + \ldots + t + 1 \in \mathbb{Z}[t]$$

für jede Primzahl $p \in \mathbb{P}$ irreduzibel in $\mathbb{Z}[t]$ und in $\mathbb{Q}[t]$ ist.

Dazu beachten wir zunächst, daß sich f schreiben läßt als

$$f = \frac{t^p - 1}{t - 1}.$$

Wenn wir nun die lineare Koordinatentransformation

$$\Phi_{1,1} : \mathbb{Z}[t] \longrightarrow \mathbb{Z}[t] : f \mapsto f(t + 1)$$

auf f anwenden, so erhalten wir

$$\Phi_{1,1}(f) = \frac{(t+1)^p - 1}{(t+1) - 1} = \frac{\sum_{k=0}^{p} \binom{p}{k} \cdot t^k - 1}{t} = \sum_{k=1}^{p} \binom{p}{k} \cdot t^{k-1}.$$

Es handelt sich bei $\Phi_{1,1}(f)$ also um ein normiertes Polynom in $\mathbb{Z}[t]$, so daß p jeden Koeffizienten außer dem Leitkoeffizienten teilt, aber p^2 teilt den konstanten Anteil $\binom{p}{1} = p$ nicht. Das Eisenstein-Kriterium 2.2 sagt uns dann, daß $\Phi_{1,1}(f)$ irreduzibel in $\mathbb{Z}[t]$ ist. Dann ist aber auch f irreduzibel in $\mathbb{Z}[t]$ und mithin in $\mathbb{Q}[t]$ nach Satz 2.4.

Bemerkung 2.12
Bei Polynomen kleinen Grades kann man die Irreduzibilität auch an der Nicht-Existenz von Nullstellen fest machen, da Nullstellen Linearfaktoren des Polynoms entsprechen. Genauer gilt, ein Polynom vom Grad 2 oder 3 über einem Körper ist genau dann irreduzibel, wenn es keine Nullstelle hat. (Siehe auch [**Mar08a**, Korollar 7.40].)

Wir werden in der Vorlesung im wesentlichen an Polynomen in $\mathbb{Q}[t]$ interessiert sein. Wegen Satz 2.4 reduziert sich die Berechnung einer Primfaktorzerlegung in $\mathbb{Q}[t]$ auf die Berechnung einer solchen in $\mathbb{Z}[t]$. Wir wollen nun einen naiven Algorithmus dafür angeben, wie man eine solche berechnen kann. Für effizientere Algorithmen sei auf die Vorlesung Einführung in das symbolische Rechnen verwiesen.

Die Grundidee des Algorithmus beruht darauf, daß für einen Teiler g eines Polynoms f und für eine ganze Zahl a gilt, daß die ganze Zahl $g(a)$ ein Teiler von $f(a)$ ist, und daß $f(a)$ nur endlich viele Teiler hat, so daß für die Zahl $g(a)$ nur endlich viele Werte in Frage kommen. Ein Polynom ist aber durch die Werte an endlich vielen Stellen bestimmt, so daß man leicht alle möglichen Kandidaten für einen Teiler g auflisten kann. Zudem reicht es Teiler vom Grad kleiner oder gleich $\frac{\deg(f)}{2}$ zu testen, da ein reduzibles Polynom zwangsläufig einen solchen Teiler haben muß.

Algorithmus 2.13

INPUT: $f \in \mathbb{Z}[t]$ primitiv mit $\deg(f) = n \geq 2$.

OUTPUT: Eine Primfaktorzerlegung von f.

1. Schritt: Setze $r = \left\lfloor \frac{n}{2} \right\rfloor$.

2. Schritt: Bestimme die Zahlen $d_i := f(i)$ für $i = 0, \ldots, r$.

3. Schritt: Wenn eine der Zahlen $d_i = 0$ ist, starte den Algorithmus erneut mit $\frac{f}{t-i} \in \mathbb{Z}[t]$ und gib das Ergebnis zusammen mit dem Faktor $t - i$ zurück.

4. Schritt: Wenn die d_i, $i = 0, \ldots, r$, alle ungleich 0 sind, gehe wie folgt vor:

- Bestimme alle Teiler $c_{i,1}, \ldots, c_{i,k_i} \in \mathbb{Z}$ von d_i.
- Wähle ein Tupel

  $$(a_1, \ldots, a_r) \in \{(c_{0,j_0}, \ldots, c_{r,j_r}) \mid 1 \leq j_i \leq k_i, i = 0, \ldots, r\}$$

  und berechne das eindeutige Interpolationspolynom $g \in \mathbb{Q}[t]$ vom Grad höchstens r mit $g(i) = a_i$ für $i = 0, \ldots, r$ (z.B. mit Hilfe der Lagrange-Interpolationspolynome).
- Wenn dieses in $\mathbb{Z}[t]$ von positivem Grad ist und in $\mathbb{Z}[t]$ das Polynom f teilt, dann starte den Algorithmus erneut mit g und mit $\frac{f}{g}$ als Input und gib das Gesamtergebnis zurück.
- Andernfalls wähle ein neues Tupel, solange bis ein Teiler gefunden wurde oder die Menge leer ist.
- Wenn die Menge leer wird, ohne daß ein Teiler gefunden wurde, dann ist f irreduzibel, weil dann offenbar kein Faktor vom Grad höchstens r in $\mathbb{Z}[t]$ existiert, und man gibt einfach f zurück.

Beispiel 2.14

Wir wollen mit dem obigen Ansatz das primitive Polynom

$$f = t^4 + t^3 - t^2 - 2t - 2 \in \mathbb{Z}[t]$$

faktorisieren.

Wir starten also mit $r = 2$ und berechnen das Tupel

$$(d_0, d_1, d_2) = \big(f(0), f(1), f(2)\big) = (-2, -3, 14).$$

Die Teilertupel listen wir in Tabelle 1 auf. In der Tat kann man die Hälfte der

$(1,1,1)$,	$(1,1,-1)$,	$(1,1,2)$,	$(1,1,-2)$,	$(1,1,7)$,	$(1,1,-7)$,	$(1,1,14)$,	$(1,1,-14)$
$(1,-1,1)$,	$(1,-1,-1)$,	$(1,-1,2)$,	$(1,-1,-2)$,	$(1,-1,7)$,	$(1,-1,-7)$,	$(1,-1,14)$,	$(1,-1,-14)$
$(1,3,1)$,	$(1,3,-1)$,	$(1,3,2)$,	$(1,3,-2)$,	$(1,3,7)$,	$(1,3,-7)$,	$(1,3,14)$,	$(1,3,-14)$
$(1,-3,1)$,	$(1,-3,-1)$,	$(1,-3,2)$,	$(1,-3,-2)$,	$(1,-3,7)$,	$(1,-3,-7)$,	$(1,-3,14)$,	$(1,-3,-14)$
$(-1,1,1)$,	$(-1,1,-1)$,	$(-1,1,2)$,	$(-1,1,-2)$,	$(-1,1,7)$,	$(-1,1,-7)$,	$(-1,1,14)$,	$(-1,1,-14)$
$(-1,-1,1)$,	$(-1,-1,-1)$,	$(-1,-1,2)$,	$(-1,-1,-2)$,	$(-1,-1,7)$,	$(-1,-1,-7)$,	$(-1,-1,14)$,	$(-1,-1,-14)$
$(-1,3,1)$,	$(-1,3,-1)$,	$(-1,3,2)$,	$(-1,3,-2)$,	$(-1,3,7)$,	$(-1,3,-7)$,	$(-1,3,14)$,	$(-1,3,-14)$
$(-1,-3,1)$,	$(-1,-3,-1)$,	$(-1,-3,2)$,	$(-1,-3,-2)$,	$(-1,-3,7)$,	$(-1,-3,-7)$,	$(-1,-3,14)$,	$(-1,-3,-14)$
$(2,1,1)$,	$(2,1,-1)$,	$(2,1,2)$,	$(2,1,-2)$,	$(2,1,7)$,	$(2,1,-7)$,	$(2,1,14)$,	$(2,1,-14)$
$(2,-1,1)$,	$(2,-1,-1)$,	$(2,-1,2)$,	$(2,-1,-2)$,	$(2,-1,7)$,	$(2,-1,-7)$,	$(2,-1,14)$,	$(2,-1,-14)$
$(2,3,1)$,	$(2,3,-1)$,	$(2,3,2)$,	$(2,3,-2)$,	$(2,3,7)$,	$(2,3,-7)$,	$(2,3,14)$,	$(2,3,-14)$
$(2,-3,1)$,	$(2,-3,-1)$,	$(2,-3,2)$,	$(2,-3,-2)$,	$(2,-3,7)$,	$(2,-3,-7)$,	$(2,-3,14)$,	$(2,-3,-14)$
$(-2,1,1)$,	$(-2,1,-1)$,	$(-2,1,2)$,	$(-2,1,-2)$,	$(-2,1,7)$,	$(-2,1,-7)$,	$(-2,1,14)$,	$(-2,1,-14)$
$(-2,-1,1)$,	$(-2,-1,-1)$,	$(-2,-1,2)$,	$(-2,-1,-2)$,	$(-2,-1,7)$,	$(-2,-1,-7)$,	$(-2,-1,14)$,	$(-2,-1,-14)$
$(-2,3,1)$,	$(-2,3,-1)$,	$(-2,3,2)$,	$(-2,3,-2)$,	$(-2,3,7)$,	$(-2,3,-7)$,	$(-2,3,14)$,	$(-2,3,-14)$
$(-2,-3,1)$,	$(-2,-3,-1)$,	$(-2,-3,2)$,	$(-2,-3,-2)$,	$(-2,-3,7)$,	$(-2,-3,-7)$,	$(-2,-3,14)$,	$(-2,-3,-14)$

TABELLE 1. Liste der Teilertupel für $(-2,-3,14)$

$4 \cdot 4 \cdot 8 = 256$ Möglichkeiten streichen, da die Tupel, die sich nur um das Vorzeichen unterscheiden, bis auf Vorzeichen den gleichen Kandidaten für einen Teiler liefern.

Wählt man aus dieser Menge nun das Tupel $(a_0, a_1, a_2) = (1, 1, -1)$, so sucht man ein Polynom

$$g = b_2 t^2 + b_1 t + b_0 \in \mathbb{Q}[t]$$

vom Grad höchstens zwei, für das

$$1 = g(0) = b_0, \quad 1 = g(1) = b_2 + b_1 + b_0 \quad \text{und} \quad -1 = g(2) = 4b_2 + 2b_1 + b_0$$

gilt, und man rechnet leicht nach, daß $b_0 = 1$, $b_1 = 1$ und $b_2 = -1$ die eindeutige Lösung ist, d.h.

$$g = -t^2 + t + 1 \in \mathbb{Z}[t]$$

ist unser Kandidat. Aber Polynomdivision

$$f = (-t^2 - 2t - 2) \cdot g + 2t$$

zeigt, daß g kein Teiler von f ist. Der Punkt (a_0, a_1, a_2) war also nicht passend.

Wählen wir stattdessen den Punkt $(a_0, a_1, a_2) = (1, 3, 7)$, so suchen wir ein Polynom mit

$$g = b_2 t^2 + b_1 t + b_0 \in \mathbb{Q}[t]$$

vom Grad höchstens zwei, für das

$$1 = g(0) = b_0, \quad 3 = g(1) = b_2 + b_1 + b_0 \quad \text{und} \quad 7 = g(2) = 4b_2 + 2b_1 + b_0$$

gilt. Die eindeutige Lösung des Gleichungssystems ist $b_0 = 1$, $b_1 = 1$ und $b_2 = 1$, so daß wir

$$g = t^2 + t + 1 \in \mathbb{Z}[t]$$

als Kandidaten erhalten. Man berechnet mittels Polynomdivision nun

$$f = (t^2 - 2) \cdot (t^2 + t + 1)$$

und könnte die beiden Faktoren als neuen Input für den Algorithmus nehmen. In der Tat wissen wir für das Polynom $t^2 - 2$ aber nach Eisenstein bereits, daß es irreduzibel ist, und für $t^2 + t + 1$ wissen wir es aus Beispiel 2.11. Wir haben also eine Primfaktorzerlegung von f in $\mathbb{Z}[t]$ und damit in $\mathbb{Q}[t]$ berechnet.

Wie ineffizient dieser naive Ansatz ist, sieht man an der Tatsache, daß nur 2 der 128 zu betrachtenden Tupel tatsächlich zu Faktoren von f gehören. Wenn die d_i mehr Teiler haben, erhöht sich die Anzahl der Tupel sehr schnell!

KAPITEL II

Galoistheorie

§ 3 Endliche Körpererweiterungen

A) Körpererweiterungen

In der Vorlesung Algebraische Strukturen (siehe [**Mar08a**, Def. 6.1 und Def. 6.11]) wurden den die Begriffe *Körper* und *Teilkörper* eingeführt. Da sie für die Vorlesung von zentraler Bedeutung sind, wiederholen wir die Definitionen hier noch einmal.

Definition 3.1 (Körpererweiterung)

a. Eine nicht-leere Menge K mit zwei zweistelligen Operationen

$$+ : \mathsf{K} \times \mathsf{K} \longrightarrow \mathsf{K}$$

und

$$\cdot : \mathsf{K} \times \mathsf{K} \longrightarrow \mathsf{K}$$

heißt *Körper*, wenn die folgenden Axiome erfüllt sind:

- $(\mathsf{K}, +)$ ist eine abelsche Gruppe.
- $(\mathsf{K} \setminus \{0\}, \cdot)$ ist eine abelsche Gruppe.
- Die Distributivgesetze sind erfüllt.

b. Eine nicht-leere Teilmenge K eines Körpers L heißt ein *Teilkörper* von L, wenn K mit den Einschränkungen der Addition und der Multiplikation selbst wieder ein Körper ist. Wir schreiben dann $\mathsf{K} \leq \mathsf{L}$.

c. Ist K ein Teilkörper von L, so nennen wir L auch einen *Erweiterungskörper* von K und wir sprechen von der *Körpererweiterung* L über K. Es ist in der Algebra üblich, diese mit dem Symbol L/K zu bezeichnen.

d. Ist L/K ein Körpererweiterung und $\mathsf{N} \leq \mathsf{L}$ ein Teilkörper von L, der K enthält, so nennen wir N einen *Zwischenkörper* von L/K.

Bemerkung 3.2

a. Wir haben in Definition 3.1 zwei Bezeichungen für dasselbe Objekt eingeführt. Einmal sprechen wir von einem Teilkörper K von L (in Symbolen $\mathsf{K} \leq \mathsf{L}$), dann von einem Erweiterungskörper L über K (in Symbolen L/K). Verschoben hat sich dabei allein der Blickwinkel.
Studiert man die Teilkörper eines gegebenen Körpers L, so will man in aller Regel L besser verstehen, indem man seine Teilstrukturen untersucht. Interessiert man sich für Körpererweiterungen von K, so ist der kleinere Körper

K der Ausgangspunkt und man versucht Probleme zu lösen, die sich in K nicht lösen lassen, indem man zu einem geeigneten größeren Körper übergeht. Für unsere Vorlesung wird dies von primärem Interesse sein, so daß wir von Körpererweiterungen sprechen wollen.

b. Man sollte beachten, daß die Schreibweise L/K rein symbolisch zu verstehen ist und keine Faktorstruktur bezeichnet!

Beispiel 3.3

a. $\mathbb{Q}$, $\mathbb{R}$ und $\mathbb{C}$ sind Beispiele für Körper; $\mathbb{C}/\mathbb{R}$ und $\mathbb{C}/\mathbb{Q}$ und $\mathbb{R}/\mathbb{Q}$ sind Körpererweiterungen.

b. Ist $p \in \mathbb{P}$ eine Primzahl, so ist $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ ein Körper mit p Elementen (siehe [**Mar08a**, Kor. 7.18]).

c. Ist K ein Körper, so ist der Quotientenkörper

$$K(t) := \mathrm{Quot}(K[t]) = \left\{ \frac{f}{g} \;\middle|\; f, g \in K[t], g \neq 0 \right\}$$

aus Definition 1.7 ein Körper, der *Körper der rationalen Funktionen* über K.

Wann immer man algebraische Strukturen betrachtet, führt man auch strukturerhaltende Abbildungen ein. Für Körper sind das letztlich einfach die Ringhomomorphismen.

Definition 3.4 (Körperhomomorphismus)
Eine Abbildung $\varphi : K \longrightarrow L$ zwischen zwei Körpern heißt ein *Körperhomomorphismus*, wenn sie ein Ringhomomorphismus ist, d.h. wenn folgende Axiome gelten:

- $\varphi(a + b) = \varphi(a) + \varphi(b)$ für $a, b \in K$,
- $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$ für $a, b \in K$,
- $\varphi(1_K) = 1_L$.

Die Körper K und L heißen *isomorph*, wenn es einen Körperisomorphismus, d.h. einen bijektiven Körperhomomorphismus, von K nach L gibt. Wir schreiben dann $K \cong L$.

Lemma 3.5
Ist $\varphi : K \longrightarrow L$ *ein Körperhomomorphismus, so ist* φ *injektiv.*
Insbesondere ist $L/\varphi(K)$ *eine Körpererweiterung mit* $\varphi(K) \cong K$.

Beweis: Wir müssen zeigen, daß der Kern von φ nur die Null enthält. Sei also $a \in \mathrm{Ker}(\varphi)$ und nehmen wir $a \neq 0$ an. Dann besitzt a im Körper K ein Inverses und wir erhalten

$$0_L = 0_L \cdot \varphi(a^{-1}) = \varphi(a) \cdot \varphi(a^{-1}) = \varphi(a \cdot a^{-1}) = \varphi(1_K) = 1_L.$$

Das ist ein Widerspruch dazu, daß in einem Körper 0_L und 1_L verschieden sein müssen.

Also haben wir gezeigt, daß φ injektiv ist. Wegen des Homomorphiesatzes ist dann

$$K \cong \varphi(K) \leq L$$

und $\varphi(K)$ ist ein Teilkörper von L. □

B) Primkörper

Definition 3.6 (Primkörper und Charakteristik)
Es sei L ein Körper.

a. Wir nennen den Durchschnitt

$$P := \bigcap_{K \leq L} K$$

aller Teilkörper von L den *Primkörper* von L.

b. Gibt es eine natürliche Zahl $n \geq 1$ mit

$$\underbrace{1_L + \ldots + 1_L}_{n-\text{mal}} = 0_L,$$

so nennen wir die kleinste solche Zahl die *Charakteristik* von L. Gibt es keine solche Zahl, so sagen wir L habe die *Charakteristik* 0. Wir bezeichnen die Charakteristik des Körpers mit $\mathrm{char}(L)$.

Bemerkung 3.7 (Charakteristik)
Ist L ein Körper, so ist die Abbildung

$$\varphi_L : \mathbb{Z} \longrightarrow L : n \mapsto n \cdot 1_L = \underbrace{1_L + \ldots + 1_L}_{n-\text{mal}}$$

ein Ringhomomorphismus. Mithin ist der Kern von φ_L als Ideal in $\mathbb{Z}$ ein Hauptideal und aus der Definition der Charakteristik von L folgt unmittelbar

$$\mathrm{Ker}(\varphi_L) = \langle \mathrm{char}(L) \rangle_{\mathbb{Z}} = \mathrm{char}(L) \cdot \mathbb{Z}.$$

Die Charakteristik von L ist also die kleinste natürliche Zahl, die den Kern von φ_L erzeugt.

Satz 3.8
Es sei L ein Körper und P sei der Primkörper von L.

a. P ist der kleinste Teilkörper von L.

b. Ist $\mathrm{char}(L) \neq 0$, so ist $\mathrm{char}(L) = p$ eine Primzahl und $P \cong \mathbb{F}_p$.

c. Ist $\mathrm{char}(L) = 0$, so ist $P \cong \mathbb{Q}$.

Beweis: Daß der Durchschnitt von Teilkörpern wieder ein Teilkörper ist, folgt unmittelbar aus der Definition. Insbesondere ist also der Primkörper ein Teilkörper von L und aufgrund seiner Definition in jedem anderen Teilkörper von L enthalten. Damit ist a. gezeigt.

Für den Beweis von Teil b. und c. betrachten wir den Ringhomomorphismus

$$\varphi_L : \mathbb{Z} \longrightarrow L : n \mapsto n \cdot 1_L = \underbrace{1_L + \ldots + 1_L}_{n-\text{mal}}$$

aus Bemerkung 3.7.

Setzen wir zunächst $p := \operatorname{char}(L) \neq 0$ voraus, so gilt $\operatorname{Ker}(\varphi_L) = p\mathbb{Z}$ und aus dem Homomorphiesatz erhalten wir

$$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} = \mathbb{Z}/\operatorname{Ker}(\varphi_L) \cong \operatorname{Im}(\varphi_L) \leq L$$

ist ein Unterring von L. Da L als Körper nullteilerfrei ist, trifft dies auch auf $\mathbb{F}_p$ zu und p muß eine Primzahl sein (siehe [**Mar08a**, Kor. 7.18]). Damit ist $\mathbb{F}_p$ dann ein Körper und $\operatorname{Im}(\varphi_L)$ ein Teilkörper von L. Da der Primkörper 1_L enthält und bezüglich Addition abgeschlossen ist, gilt zudem

$$\operatorname{Im}(\varphi_L) \subseteq P.$$

Aufgrund der Definition von P als Durchschnitt aller Teilkörper von L gilt dann aber schon $P = \operatorname{Im}(\varphi_L)$.

Setzen wir nun $\operatorname{char}(L) = 0$ voraus, so ist φ_L injektiv und wir können φ_L auf $\mathbb{Q}$ fortsetzen durch

$$\psi : \mathbb{Q} \longrightarrow L : \frac{a}{b} \mapsto \varphi_L(a) \cdot \varphi_L(b)^{-1}.$$

Man beachte dabei, daß aus

$$\frac{a}{b} = \frac{c}{d}$$

die Gleichung

$$a \cdot d = c \cdot b$$

und mithin

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

sowie

$$\varphi_L(a) \cdot \varphi_L(b)^{-1} = \varphi_L(c) \cdot \varphi_L(d)^{-1}$$

folgt, was die Wohldefiniertheit der Abbildung ψ sicherstellt. Offenbar ist ψ ein Körperhomomorphismus und mithin injektiv, so daß mit dem Homomorphiesatz

$$\mathbb{Q} \cong \operatorname{Im}(\psi) \leq L$$

gilt und $\operatorname{Im}(\psi)$ ein Teilkörper von L ist. Zudem gilt wie oben

$$\operatorname{Im}(\psi) \subseteq P,$$

weil $1_L \in P$ und P bezüglich Addition und Division abgeschlossen ist. Wir erhalten dann aber auch hier $\operatorname{Im}(\psi) = P$, weil P der kleinste Teilkörper von L ist. □

Beispiel 3.9

a. Die Körper $\mathbb{Q}$, $\mathbb{R}$ und $\mathbb{C}$ haben Charakteristik 0 und den Primkörper $\mathbb{Q}$.

b. Der Körper $\mathbb{F}_p$, $p \in \mathbb{P}$, hat die Charakteristik p und ist selbst sein Primkörper.

C) Einfache algebraische Körpererweiterungen

Definition 3.10 (Algebraisch und transzendent)
Es sei L/K ein Körpererweiterung.

a. Ein Element $\alpha \in L$ heißt *algebraisch über* K, wenn ein Polynom $0 \neq f \in K[t]$ existiert mit $f(\alpha) = 0$.

b. Ein Element $\alpha \in L$ heißt *transzendent über* K, wenn es nicht algebraisch ist.

c. Die Körpererweiterung L/K heißt *algebraisch*, wenn jedes $\alpha \in L$ algebraisch über K ist.

Beispiel 3.11

a. Die Zahl $\alpha = \sqrt{2} \in \mathbb{R}$ ist algebraisch über $\mathbb{Q}$, da sie Nullstelle des Polynoms $f = t^2 - 2 \in \mathbb{Q}[t]$ ist.

b. Die Körpererweiterung $\mathbb{C}/\mathbb{R}$ ist algebraisch, da $\alpha = a + ib \in \mathbb{C}$ Nullstelle des Polynoms $f = (t - a)^2 + b^2 \in \mathbb{R}[t]$ ist.

c. $\mathbb{R}/\mathbb{Q}$ ist nicht algebraisch.
Um das einzusehen, beachte man, daß mit $\mathbb{Q}$ auch $\mathbb{Q}[t]$ abzählbar ist. Da jedes Polynom nur endlich viele Nullstellen hat, kann es in $\mathbb{R}$ nur abzählbar viele Zahlen geben, die Nullstelle eines Polynoms mit rationalen Koeffizienten sind. Also muß es auch reelle Zahlen geben, die nicht algebraisch über $\mathbb{Q}$ sind.

d. Ist L/K eine Körpererweiterung, so ist jedes Element $\alpha \in K$ algebraisch über K, da es Nullstelle des Polynoms $t - \alpha \in K[t]$ ist.

Definition 3.12 (K adjungiert M)
Es sei L/K eine Körpererweiterung und $M \subseteq L$.

a. Wir nennen den Durchschnitt

$$K(M) := \bigcap_{M \cup K \subseteq N \leq L} N$$

aller Zwischenkörper von L/K, die die Menge M enthalten, K *adjungiert* M. Es ist der kleinste Zwischenkörper von L/K, der M enthält.

b. Ist $M = \{\alpha_1, \ldots, \alpha_n\}$ endlich, so schreiben wir auch $K(\alpha_1, \ldots, \alpha_n)$ statt $K(M)$.

c. Eine Körpererweiterung der Form $K(\alpha)/K$ nennen wir eine *einfache Körpererweiterung*, und α nennen wir ein *primitives Element* der Erweiterung.

Beispiel 3.13
Betrachten wir die Körpererweiterung $\mathbb{C}/\mathbb{R}$ und $\alpha = i \in \mathbb{C}$, so gilt

$$\mathbb{R}(i) = \mathbb{C},$$

da jeder Körper, der $\mathbb{R}$ und i enthält auch alle Ausdrücke der Form $a + ib$ mit $a, b \in \mathbb{R}$ enthält. Also ist $\mathbb{C}/\mathbb{R}$ eine einfache Körpererweiterung.

Bemerkung 3.14 (Der Einsetzhomomorphismus)
Sei L/K eine Körpererweiterung und $\alpha \in L$. Wir haben den *Einsetzhomomorphismus*

$$\phi_\alpha : K[t] \longrightarrow L : f \mapsto f(\alpha)$$

bereits in den Algebraischen Strukturen (siehe [**Mar08a**, Lem. 7.36]) und den Grundlagen der Mathematik (siehe [**Mar11**, Prop. 31.11]) kennengelernt. Das Bild des Einsetzhomomorphismus ist der Unterring

$$K[\alpha] := \mathrm{Im}(\phi_\alpha) = \{f(\alpha) \mid f \in K[t]\} \subseteq K(\alpha)$$

von $K(\alpha)$. Um die Inklusion zu sehen, beachtet man, daß der Körper $K(\alpha)$ mit K und α auch jeden Polynomausdruck in α mit Koeffizienten in K enthält.

Ist α transzendent über K, so enthält der Kern von ϕ_α nur das Nullpolynom und ϕ_α ist injektiv und induziert den Isomorphismus

$$K[\alpha] \cong K[t].$$

Zudem sieht man leicht, daß in diesem Fall

$$K(\alpha) = \left\{ \frac{f(\alpha)}{g(\alpha)} \;\middle|\; f, g \in K[t], g \neq 0 \right\} \cong K(t)$$

der Quotientenkörper von $K[\alpha]$ ist, da jeder Körper, der K und α enthält auch die rationalen Funktionen in α mit Koeffizienten aus K enthalten muß.

Im folgenden Satz untersuchen wir mit Hilfe des Einsetzhomomorphismus die einfache Körpererweiterung $K(\alpha)/K$ auch für algebraische α.

Satz 3.15 (Das Minimalpolynom)
Es sei L/K *ein Körpererweiterung und* $\alpha \in L$ *sei algebraisch über* K*.*

a. *Es gibt ein eindeutig bestimmtes normiertes Polynom* $0 \neq \mu_\alpha \in K[t]$ *kleinsten Grades, das* α *als Nullstelle hat, das* Minimalpolynom *von* α *über* K*.*
b. *Das Minimalpolynom* μ_α *erzeugt den Kern des Einsetzhomomorphismus* ϕ_α*.*
c. *Das Minimalpolynom* μ_α *ist irreduzibel und* ϕ_α *induziert einen Isomorphismus*

$$K[t]/\langle \mu_\alpha \rangle \cong K[\alpha] = K(\alpha).$$

Beweis: Der Kern von ϕ_α wird als Ideal im Hauptidealring $K[t]$ von einem Polynom μ_α erzeugt. Indem wir durch den Leitkoeffizienten teilen, können wir ohne Einschränkung annehmen, daß μ_α normiert ist. Ist $0 \neq f \in K[t]$ irgendein Polynom, das α als Nullstelle hat, so gilt

$$f \in \mathrm{Ker}(\phi_\alpha) = \langle \mu_\alpha \rangle.$$

Mithin gibt es ein $g \in K[t]$ mit

$$f = g \cdot \mu_\alpha, \tag{5}$$

und aus der Gradformel folgt

$$\deg(f) = \deg(g) + \deg(\mu_\alpha) \geq \deg(\mu_\alpha), \tag{6}$$

so daß μ_α in der Tat ein Nicht-Null-Polynom kleinsten Grades ist, das α als Nullstelle besitzt. Um die Eindeutigkeit von μ_α zu sehen, können wir annehmen, daß f ein zweites normiertes Polynom kleinsten Grades mit α als Nullstelle ist. Aus (6) sehen wir dann, daß der Faktor g in (5) konstant sein muß, und da f und μ_α beide normiert sind, muß in der Tat $g = 1$ und damit $f = \mu_\alpha$ gelten. Damit sind Teil a. und Teil b. gezeigt.

Wäre μ_α nicht irreduzibel, so gäbe es eine Faktorisierung

$$\mu_\alpha = f \cdot g$$

von μ_α in zwei Nicht-Einheiten und f und g hätten beide einen Grad, der echt kleiner als der Grad von μ_α wäre. Zugleich müßte wegen

$$0 = \mu_\alpha(\alpha) = f(\alpha) \cdot g(\alpha)$$

aber α Nullstelle von f oder g sein, im Widerspruch zur Minimalität des Grades von μ_α in Teil a.. Also ist μ_α irreduzibel.

Aber dann ist $K[t]/\langle\mu_\alpha\rangle$ nach Proposition 2.1 ein Körper. Wegen des Homomorphiesatzes und Bemerkung 3.14 gilt zudem

$$K[t]/\langle\mu_\alpha\rangle = K[t]/\operatorname{Ker}(\phi_\alpha) \cong \operatorname{Im}(\phi_\alpha) = K[\alpha] \subseteq K(\alpha),$$

so daß $K[\alpha]$ ein Zwischenkörper von L/K ist, der α enthält, womit auch

$$K(\alpha) \subseteq K[\alpha]$$

folgt. Damit ist auch c. gezeigt. □

Beispiel 3.16

a. Das Minimalpolynom von $\alpha = \sqrt{2}$ über $\mathbb{Q}$ ist

$$\mu_{\sqrt{2}} = t^2 - 2 \in \mathbb{Q}[t],$$

da es wegen $\sqrt{2} \notin \mathbb{Q}$ kein Polynom vom Grad 1 mit $\sqrt{2}$ als Nullstelle geben kann. Mithin gilt

$$\mathbb{Q}(\sqrt{2}) = \mathbb{Q}[\sqrt{2}] = \{f(\sqrt{2}) \mid f \in \mathbb{Q}[t]\}.$$

b. Die komplexe Zahl

$$\alpha = e^{\frac{2\pi i}{6}} \in \mathbb{C}$$

ist eine sechste Einheitswurzel und ist deshalb Nullstelle des Polynoms

$$f = t^6 - 1 \in \mathbb{Q}[t].$$

Da f nicht irreduzibel ist, kann f aber nicht das Minimalpolynom sein. In der Tat sieht man leicht die folgende Faktorisierung

$$f = (t^3 - 1) \cdot (t^3 + 1).$$

von f über $\mathbb{Q}$. Aus $\alpha^3 = -1$ folgt, daß α eine Nullstelle des Faktors

$$g = t^3 + 1 = (t + 1) \cdot (t^2 - t + 1)$$

ist, und somit eine Nullstelle von

$$h = t^2 - t + 1.$$

Da h ein Polynom mit reellen Koeffizienten ist, muß mit α auch das komplex Konjugierte $\overline{\alpha}$ von α eine Nullstelle von h sein. Damit hat

$$h = (t - \alpha) \cdot \left(t - \overline{\alpha}\right)$$

in $\mathbb{Q}$ keine Nullstelle und ist somit irreduzibel in $\mathbb{Q}[t]$. Das Minimalpolynom von α über $\mathbb{Q}$ ist dann als normierter, nicht-konstanter Faktor von h mit h identisch, d. h.

$$\mu_\alpha = t^2 - t + 1.$$

Das Beispiel soll zeigen, daß es nicht unbedingt einfach ist, das Minimalpolynom zu berechnen, auch wenn wir evt. leicht ein Polynom mit α als Nullstelle finden.

Definition 3.17 (Grad einer Körpererweiterung)
Ist L/K eine Körpererweiterung, so ist L ein K-Vektorraum und wir nennen die Dimension

$$|L : K| := \dim_K(L) \in \mathbb{N} \cup \{\infty\}$$

von L als K-Vektorraum den *Grad* der Körpererweiterung L/K.
Die Körpererweiterung L/K heißt *endlich*, wenn sie einen endlichen Grad hat.

Korollar 3.18 (Einfache algebraische Körpererweiterungen)
Sei L/K *eine Körpererweiterung und* $\alpha \in K$ *sei algebraisch über* K *mit* $n = \deg(\mu_\alpha)$.

Dann ist die Menge

$$B = \{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$$

eine Basis von $K(\alpha)$ *als* K*-Vektorraum und*

$$|K(\alpha) : K| = \deg(\mu_\alpha) = n.$$

Insbesondere ist die einfache Körpererweiterung $K(\alpha)$ *endlich.*

Beweis: Aus Satz 3.15 wissen wir, daß

$$K(\alpha) = K[\alpha] = \{f(\alpha) \mid f \in K[t]\}$$

gilt. Damit enthält $K(\alpha)$ die lineare Hülle

$$\begin{aligned} \mathrm{Lin}(1, \alpha, \ldots, \alpha^{n-1}) &= \left\{ a_0 \cdot 1 + a_1 \cdot \alpha + \ldots + a_{n-1} \cdot \alpha^{n-1} \;\middle|\; a_0, \ldots, a_{n-1} \in K \right\} \\ &= \left\{ f(\alpha) \;\middle|\; f \in K[t], \deg(f) \leq n - 1 \right\}. \end{aligned}$$

Wir müssen noch die umgekehrte Inklusion zeigen. Sei dazu $f \in K[t]$ beliebig gegeben. Division mit Rest liefert uns zwei Polynome $q, r \in K[t]$, so daß

$$f = q \cdot \mu_\alpha + r$$

mit $\deg(r) < \deg(\mu_\alpha) = n$. Damit gilt dann aber

$$f(\alpha) = q(\alpha) \cdot \mu_\alpha(\alpha) + r(\alpha) = r(\alpha) \in \mathrm{Lin}(1, \alpha, \ldots, \alpha^{n-1})$$

und die fehlende Inklusion

$$K(\alpha) \subseteq \mathrm{Lin}(1, \alpha, \ldots, \alpha^{n-1})$$

ist gezeigt. Also ist B ein Erzeugendensystem von $K(\alpha)$ als K-Vektorraum.

Es bleibt zu zeigen, daß B linear unabhängig ist. Sei dazu eine beliebige Linearkombination

$$a_0 \cdot 1 + a_1 \cdot \alpha + \ldots + a_{n-1} \cdot \alpha^{n-1} = 0$$

der Null mit Koeffizienten $a_0, \ldots, a_{n-1} \in K$ gegeben. Dann ist

$$f = a_0 \cdot 1 + a_1 \cdot t + \ldots + a_{n-1} \cdot t^{n-1} \in K[t]$$

mit

$$f(\alpha) = 0$$

und

$$\deg(f) \leq n - 1 < \deg(\mu_\alpha).$$

Da der Kern des Einsetzhomomorphismus von μ_α erzeugt wird und f enthält, muß f das Nullpolynom sein und mithin gilt

$$a_0 = \ldots = a_{n-1} = 0.$$

Somit ist B auch linear unabhängig. □

Beispiel 3.19
Der Grad der Körpererweiterung $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ ist

$$\left|\mathbb{Q}(\sqrt{2}) : \mathbb{Q}\right| = \deg(t^2 - 2) = 2$$

und $\{1, \sqrt{2}\}$ ist eine $\mathbb{Q}$-Vektorraumbasis von $\mathbb{Q}(\sqrt{2})$ als $\mathbb{Q}$-Vektorraum, d.h.

$$\mathbb{Q}(\sqrt{2}) = \left\{a + b \cdot \sqrt{2} \;\middle|\; a, b \in \mathbb{Q}\right\}.$$

D) Endliche Körpererweiterungen

Proposition 3.20 (Endliche Körpererweiterungen sind algebraisch.)
Ist L/K *eine endliche Körpererweiterung, so ist* L/K *algebraisch und es gilt*

$$L = K(\alpha_1, \ldots, \alpha_n)$$

für geeignete $\alpha_1, \ldots, \alpha_n \in L$.

Beweis: Es sei

$$n := |L : K|$$

der Grad der Körpererweiterung L/K und es sei $\alpha \in L$ beliebig. Die $n + 1$ Elemente

$$1, \alpha, \alpha^2, \ldots, \alpha^n \in L$$

müssen linear abhängig über K sein. Also gibt es eine nicht-triviale Linearkombination

$$a_0 \cdot 1 + a_1 \cdot \alpha + \ldots + a_n \cdot \alpha^n = 0$$

und somit ist

$$0 \neq f = a_0 + a_1 \cdot t + \ldots + a_n \cdot t^n \in K[t]$$

ein Nicht-Null-Polynom in $K[t]$ mit $f(\alpha) = 0$. Also ist α algebraisch über K.

Es bleibt zu zeigen, daß

$$L = K(\alpha_1, \ldots, \alpha_n)$$

für geeignete $\alpha_1, \ldots, \alpha_n \in L$ ist, wobei die Inklusion $\supseteq$ für jede Wahl der α_i ohnehin gilt. Wählen wir $\alpha_1, \ldots, \alpha_n \in L$ als K-Vektorraumbasis von L, so ist jedes Element von L eine K-Linearkombination von der α_i und mithin auch im kleinsten Teilkörper $K(\alpha_1, \ldots, \alpha_n)$ von L enthalten, der K und die α_i enthält. Das zeigt die fehlende Inklusion $\subseteq$. □

Beispiel 3.21
Die einfache Körpererweiterung $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ ist algebraisch über $\mathbb{Q}$ und somit ist jede Zahl der Form

$$\alpha = a + b \cdot \sqrt{2}$$

mit $a, b \in \mathbb{Q}$ Nullstelle eines Polynoms mit rationalen Koeffizienten. In der Tat ist α Nullstelle des Polynoms

$$f = (t - a)^2 - 2b^2 \in \mathbb{Q}[t].$$

Satz 3.22 (Gradformel)
Sind $K \leq L \leq M$ *Körper, so gilt die Gradformel*

$$|M : K| = |M : L| \cdot |L : K|.$$

Insbesondere, sind M/L *und* L/K *endlich, so ist auch* M/K *endlich und algebraisch.*

Beweis: Ist M als L-Vektorraum unendlich-dimensional, so ist M als K-Vektorraum erst recht unendlich-dimensional. Ebenso gilt, wenn L als K-Vektorraum unendlich-dimensional ist, dann ist M als K-Vektorraum erst recht unendlich dimensional. Die Gradformel gilt also, wenn einer der beiden Faktoren auf der rechten Seite unendlich ist.

Wir können deshalb annehmen, daß

$$|L : K| = n < \infty$$

und

$$|M : L| = m < \infty$$

gilt. Sind nun

$$\{\alpha_1, \ldots, \alpha_n\} \subset L$$

eine Basis von L als K-Vektorraum und

$$\{\beta_1, \ldots, \beta_m\} \subset M$$

eine Basis von M als L-Vektorraum, reicht es, zu zeigen, daß

$$B = \{\alpha_i \cdot \beta_j \mid i = 1, \ldots, n,\ j = 1, \ldots, m\}$$

eine Basis von M als K-Vektorraum ist.

Sei dazu $\gamma \in M$ beliebig gegeben. So können wir γ als Linearkombination

$$\gamma = b_1 \cdot \beta_1 + \ldots + b_m \cdot \beta_m$$

mit $b_1, \ldots, b_m \in L$ schreiben. Jedes b_j läßt sich wiederum als Linearkombination

$$b_j = a_{1j} \cdot \alpha_1 + \ldots + a_{nj} \cdot \alpha_n$$

mit Koeffizienten $a_{1j}, \ldots, a_{nj} \in K$ schreiben. Insgesamt erhalten wir also

$$\gamma = \sum_{j=1}^{m} b_j \cdot \beta_j = \sum_{j=1}^{m} \sum_{i=1}^{n} a_{ij} \cdot \alpha_i \cdot \beta_j \in \mathrm{Lin}_K(B)$$

und B ist ein Erzeugendensystem von M als K-Vektorraum.

Um zu zeigen, daß B linear unabhängig ist, betrachten wir eine Linearkombination

$$0 = \sum_{j=1}^{m} \sum_{i=1}^{n} a_{ij} \cdot \alpha_i \cdot \beta_j = \sum_{j=1}^{m} \left(\sum_{i=1}^{n} a_{ij} \cdot \alpha_i \right) \cdot \beta_j$$

der Null mit Koeffizienten in K. Wegen der linearen Unabhängigkeit von $\{\beta_1, \ldots, \beta_m\}$ über L folgt, daß für alle $j = 1, \ldots, m$

$$\sum_{i=1}^{n} a_{ij} \cdot \alpha_i = 0$$

gilt. Die lineare Unabhängigkeit von $\{\alpha_1, \ldots, \alpha_n\}$ über K impliziert dann aber, daß

$$a_{ij} = 0$$

für alle $i = 1, \ldots, n$ und für alle $j = 1, \ldots, m$ gelten muß. Damit ist die lineare Unabhängigkeit von B bewiesen. □

Korollar 3.23
Ist L/K *eine endliche Körpererweiterung und ist* $\alpha \in L$*, so ist*

$$\deg(\mu_\alpha) = |K(\alpha) : K| \leq |L : K|$$

ein Teiler von $|L : K|$*.*

Beweis: Aus der Gradformel 3.22 erhalten wir

$$|K(\alpha) : K| \;\Big|\; |K(\alpha) : K| \cdot |L : K(\alpha)| = |L : K|.$$

□

Beispiel 3.24
Ist L/K eine endliche Erweiterung mit Primzahlgrad $|L : K| = p \in \mathbb{P}$, so gilt $L = K(\alpha)$ für jedes $\alpha \in L \setminus K$.

Dazu beachte man nur, daß für $\alpha \in L \setminus K$ der Grad $|K(\alpha) : K|$ nicht eins sein kann, so daß aus

$$p = |L : K| = |L : K(\alpha)| \cdot |K(\alpha) : K|$$

dann unmittelbar

$$|K(\alpha) : K| = p$$

und

$$|L : K(\alpha)| = 1$$

folgt. Letzteres bedeutet aber $L = K(\alpha)$.

Bemerkung 3.25
Ist L/K eine Körpererweiterung und sind $M, N \subseteq L$, so gilt offenbar

$$K(M \cup N) = K(M)(N) = K(N)(M)$$

ist der kleinste Zwischenkörper von L/K, der M und N enthält.

Beispiel 3.26
Wir betrachten die Körper $\mathbb{Q} \leq \mathbb{Q}(\sqrt{2}) \leq \mathbb{Q}(\sqrt{2}, i)$. Die Zahl i ist Nullstelle des Polynoms

$$f = t^2 + 1 \in \mathbb{Q}[t] \subset \mathbb{Q}(\sqrt{2})[t]$$

und wegen $i \notin \mathbb{Q}(\sqrt{2})$ kann es auch kein Polynom kleineren Grades in $\mathbb{Q}(\sqrt{2})[t]$ geben, daß i als Nullstelle hat. Somit ist f das Minimalpolynom von i über $\mathbb{Q}(\sqrt{2})$, und wir erhalten für den Grad der Körpererweiterung $\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q}$

$$\left|Q(\sqrt{2}, i) : \mathbb{Q}\right| = \left|Q(\sqrt{2}, i) : Q(\sqrt{2})\right| \cdot \left|Q(\sqrt{2}) : \mathbb{Q}\right| = 2 \cdot 2 = 4$$

und

$$\left\{1, \sqrt{2}, i, \sqrt{2} \cdot i\right\}$$

ist eine $\mathbb{Q}$-Vektorraumbasis von $\mathbb{Q}(\sqrt{2}, i)$. Aus dem Grad der Körpererweiterung können wir dann ableiten, daß die Zahl

$$\alpha = 3 + \sqrt{2} + 2 \cdot i + 4 \cdot \sqrt{2} \cdot i \notin \mathbb{Q}$$

Nullstelle eines Polynoms vom Grad 2 oder 4 in $\mathbb{Q}[t]$ ist.

§ 4 Konstruktionen mit Zirkel und Lineal

Definition und Bemerkung 4.1 (Konstruktionen mit Zirkel und Lineal)
Ziel einer Konstruktion mit Zirkel und Lineal ist es, aus einer gegebenen Menge M von Punkten in der Ebene $\mathbb{R}^2$ neue Punkte durch elementargeometrische Operationen zu erzeugen. Dabei sollen folgende Elementaroperationen erlaubt sein:

- Der Schnitt zweier verschiedener Geraden durch Punkte in M.
- Der Schnitt zweier verschiedener Kreise mit Mittelpunkt in M, deren Radius der Abstand zweier Punkte in M ist.
- Der Schnitt einer Geraden durch zwei Punkte in M mit einem Kreis mit Mittelpunkt in M, dessen Radius der Abstand zweier Punkte in M ist.

Damit diese Elementaroperationen möglich sind, muß M mindestens zwei Punkte enthalten, und bei geeigneter Normierung kann man davon ausgehen, daß dies die komplexen Zahlen 0 und 1 sind.

Wir bezeichnen nun mit M' die Menge der Punkte, die sich aus M durch Elementaroperationen der obigen Form als Schnittpunkte gewinnen lassen. Setzen wir nun $M_0 = M$ und rekursiv $M_n = M'_{n-1}$, so ist

$$\widetilde{M} = \bigcup_{n \geq 0} M_n$$

die *Menge der aus* M *mit Zirkel und Lineal konstruierbaren Punkte.*[1]

Beispiel 4.2 ($\overline{z} \in \widetilde{M}$)
Aus $0, 1 \in M$ und $0 \neq z \in M$ können wir mit Zirkel und Lineal leicht den Betrag $|z|$ und das komplex Konjugierte $\overline{z}$ von z konstruieren und erhalten so

$$|z|, \overline{z} \in \widetilde{M}.$$

Dazu spiegeln wir z an der Geraden durch 0 und 1 wie in Abbildung 1 und erhalten $\overline{z}$ als das Spiegelbild und $|z|$ als den Schnittpunkt des Kreises um 0 mit dem Radius $|z - 0|$.

Definition 4.3 (Quadratisch abgeschlossen)
Ein Körper K heißt *quadratisch abgeschlossen*, wenn jedes Polynom der Form $t^2 - a \in K[t]$ über K zerfällt.

Satz 4.4 (Körper der konstruierbaren Zahlen)
Ist $0, 1 \in M \subseteq \mathbb{C}$*, so ist* $\widetilde{M}$ *ein quadratisch abgeschlossener Teilkörper von* $\mathbb{C}$*.*

Beweis: Seien $u, v \in \widetilde{M}$ gegeben. Liegen u und v auf derselben Geraden durch 0, so ist $u + v$ einer der Schnittpunkte des Kreises um u mit Radius $|v - 0|$ mit der Geraden durch 0 und u. Sind die beiden hingegen $\mathbb{R}$-linear unabhängig, so ist $u + v$

[1] Man beachte, daß $\widetilde{M}' = \widetilde{M}$ gilt, weil für die Elementaroperationen jeweils nur drei Punkte benötigt werden. Mit demselben Argument sieht man, daß jeder Punkt in $\widetilde{M}$ mittels endlich vieler Elementaroperationen aus M gewonnen werden kann.

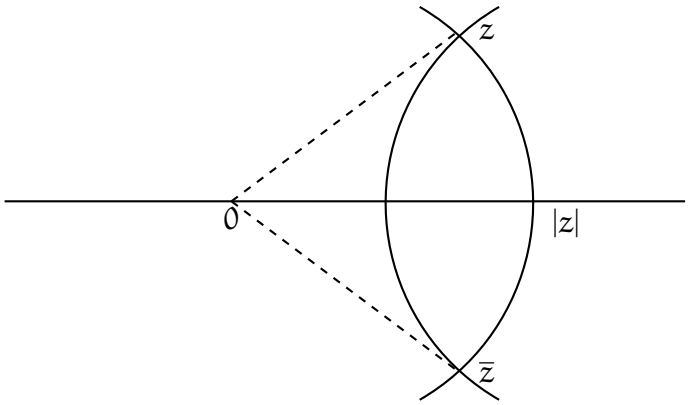

Abbildung 1. Konstruktion von $\bar{z}$ durch Spiegeln

einer der Schnittpunkte der Kreise um u mit Radius $|v - 0|$ und um v mit Radius $|u - 0|$, siehe Abbildung 2. In jedem der Fälle erhalten wir

$$u + v \in \widetilde{M}.$$

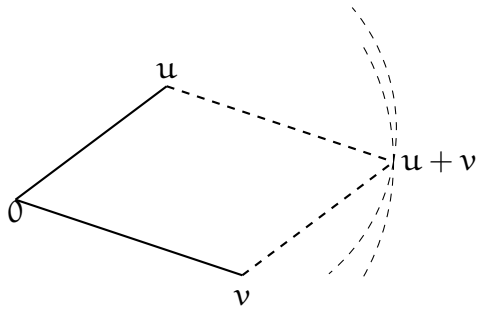

Abbildung 2. Konstruktion der Summe zweier Zahlen

Ist $0 \neq z \in \widetilde{M}$, so ist $-z$ Schnittpunkt der Geraden durch 0 und z mit dem Kreis um 0 mit dem Radius $r = |z - 0|$ (siehe Abbildung 3) und es folgt

$$-z \in \widetilde{M}.$$

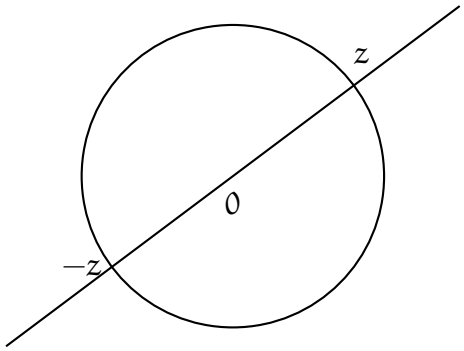

Abbildung 3. Konstruktion des Negativen einer Zahl

Sind $0 \neq u = r \cdot e^{i\varphi}, v = s \cdot e^{i\psi} \in \widetilde{M}$ gegeben, so gilt

$$\frac{u}{v} = \frac{r}{s} \cdot e^{i\cdot(\varphi-\psi)}.$$

Aus Beispiel 4.2 wissen wir, daß

$$r = |u|, s = |v| \in \widetilde{M},$$

und da mit Zirkel und Lineal Lote gefällt werden können, ist die Figur in Abbildung 4 mit Zirkel und Lineal konstruierbar. Aus einem der Strahlensätze folgt dann

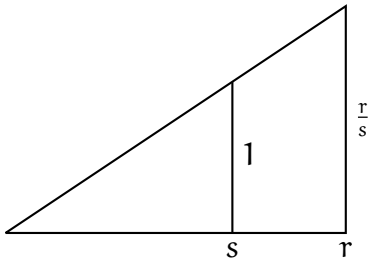

ABBILDUNG 4. Konstruktion von $\frac{r}{s}$

$$\frac{r}{s} \in \widetilde{M}.$$

Wir erhalten zudem die Zahlen

$$e^{i\varphi}, e^{i\psi} \in \widetilde{M}$$

als Schnitt der Geraden durch u bzw. durch v mit dem Kreis um 0 von Radius $1 = |1-0|$. Schlagen wir nun um $e^{i\varphi}$ einen Kreis mit Radius $|e^{i\psi}-1|$, so ist einer der Schnittpunkte mit dem Kreis um 0 vom Radius 1 der Punkt (siehe Abbildung 5)

$$e^{i\cdot(\varphi-\psi)} \in \widetilde{M}.$$

Legen wir durch diesen und 0 eine Gerade, so schneidet sie den Kreis um 0 mit

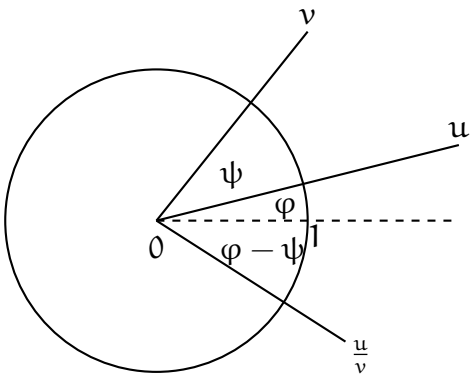

ABBILDUNG 5. Konstruktion von $e^{i\cdot(\varphi-\psi)}$

Radius $\frac{r}{s} = |\frac{r}{s} - 0|$ im Punkt

$$\frac{u}{v} = \frac{r}{s} \cdot e^{i\cdot(\varphi-\psi)} \in \widetilde{M},$$

so daß der Quotient in $\widetilde{M}$ liegt.

Damit haben wir gezeigt, daß $\widetilde{M}$ ein Teilkörper von $\mathbb{C}$ ist, und es bleibt zu zeigen, daß jedes $0 \neq z = r \cdot e^{i\varphi} \in \widetilde{M}$ ein Quadratwurzel in $\widetilde{M}$ besitzt.

Aus Beispiel 4.2 wissen wir, daß $r \in \widetilde{M}$, und da $\widetilde{M}$ ein Körper ist, gilt dann auch

$$\frac{r-1}{2} \in \widetilde{M}.$$

Schlagen wir um diesen Punkt einen Kreis vom Radius r und schneiden diesen mit der mit Zirkel und Lineal konstruierbaren Lotgeraden auf die x-Achse durch 0, so erhalten wir die Figur in Abbildung . Aus dem Höhensatz[2] folgt dann, daß die

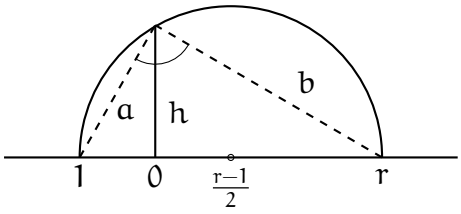

Abbildung 6. Konstruktion der Quadratwurzel $\sqrt{r}$

eingezeichnete Höhe h genau den Wert

$$\sqrt{r} = h \in \widetilde{M}$$

hat, so daß die positive Quadratwurzel von r in $\widetilde{M}$ liegt. Mit $1 \in \widetilde{M}$ und $e^{i\varphi} = \frac{z}{r} \in \widetilde{M}$ liegt auch

$$w = 1 + e^{i\varphi} = |1 + e^{i\varphi}| \cdot e^{\frac{i\varphi}{2}} \in \widetilde{M}$$

in $\widetilde{M}$ (das entspricht der Halbierung des Winkels φ mit Zirkel und Lineal). Die Gerade durch w und 0 schneidet dann den Kreis um 0 mit Radius $\sqrt{r}$ in einer Quadratwurzel

$$\sqrt{z} = \sqrt{r} \cdot e^{\frac{i\varphi}{2}} \in \widetilde{M}$$

von z, die somit in $\widetilde{M}$ liegt. □

[2]Wer den Höhensatz nicht mehr kennt, kann ihn auch unmittelbar aus dem Satz des Pythagoras und dem Satz des Thales ableiten. In Figur 6 sind wegen des Satzes von Thales drei rechtwinklige Dreiecke eingezeichnet, für die nach dem Satz des Pythagoras

$$a^2 = 1^2 + h^2$$

sowie

$$b^2 = r^2 + h^2$$

und

$$(1 + r)^2 = a^2 + b^2$$

gilt. Setzen wir die ersten beiden Gleichungen in der dritten ein, so erhalten wir

$$1 + 2r + r^2 = (1 + r)^2 = 1^2 + h^2 + r^2 + h^2 = 1 + 2h^2 + r^2$$

und damit $r = h^2$.

Unser nächstes Ziel ist es, zu zeigen, daß konstruierbare Zahlen algebraische Zahlen mit sehr speziellen Eigenschaften sind.

Bemerkung 4.5 (Körpererweiterungen für Elementaroperationen)
Es sei K ein Teilkörper von $\mathbb{C}$, so daß aus $z \in K$ auch $\overline{z} \in K$ folgt.

Ist $z \in K'$ aus K mit einer Elementaroperation konstruierbar, so gilt

$$z \in K(\omega)$$

für ein $\omega \in \mathbb{C}$ mit $\omega^2 \in K$. Dies folgt aus den folgenden vier Anmerkungen.

a. Für $z \in K$ gilt auch

$$\mathrm{Re}(z) = \frac{z + \overline{z}}{2} \in K$$

und

$$\mathrm{Im}(z) = \frac{z - \overline{z}}{2} \in K.$$

b. Sind g und h zwei verschiedene Geraden in der Ebene durch jeweils zwei Punkte in K, die sich in der Ebene schneiden, so liegt der Schnittpunkt wieder in K. Das liegt daran, daß g und h jeweils Lösungsmenge einer linearen Gleichung mit Koeffizienten in K sind und der Schnittpunkt somit die Lösungsmenge eines linearen Gleichungssystems mit Koeffizienten in K ist.

c. Ist

$$g = \{u + \lambda \cdot (v - u) \mid \lambda \in \mathbb{R}\}$$

eine Gerade durch zwei Punkte $u, v \in K$ und ist

$$k = \left\{z \in \mathbb{C} \;\middle|\; |z - w|^2 = r^2\right\} = \left\{z \in \mathbb{C} \;\middle|\; (z - w) \cdot (\overline{z - w}) = r^2\right\}$$

ein Kreis um $w \in K$ mit Radius $r \in K$, erhält man die Schnittpunkte, sofern sich g und k schneiden, indem man die Gleichung

$$\begin{aligned} r^2 =& (u + \lambda \cdot (v - u) - w) \cdot (\overline{u} + \lambda \cdot (\overline{v - u}) - \overline{w}) \\ =& |v - u|^2 \cdot \lambda^2 + 2\,\mathrm{Re}\left((u - w) \cdot (\overline{u - v})\right) \cdot \lambda + |u - w|^2 \end{aligned}$$

nach λ in $\mathbb{R}$ auflöst. Da dies eine quadratische Gleichung mit Koeffizienten in K ist, wird man an K also höchstens eine Quadratwurzel ω aus $\omega^2 \in K$ adjungieren müssen, um die Gleichung in $K(\omega)$ lösen zu können.

d. Betrachten wir nun den Schnitt zweier Kreise

$$k = \left\{z \in \mathbb{C} \;\middle|\; |z - u|^2 = r^2\right\} = \left\{x + iy \in \mathbb{C} \;\middle|\; (x - a)^2 + (y - b)^2 = r^2\right\}$$

um $u = a + ib \in K$ mit Radius $r \in K$ und

$$l = \left\{z \in \mathbb{C} \;\middle|\; |z - v|^2 = s^2\right\} = \left\{x + iy \in \mathbb{C} \;\middle|\; (x - c)^2 + (y - d)^2 = s^2\right\}$$

um $\nu = c + id \in K$ mit Radius $s \in K$. Ein Punkt $z = x + iy$ im Schnitt von k und l genügt also der Gleichung

$$\begin{aligned} r^2 - s^2 =& (x-a)^2 + (y-b)^2 - (x-c)^2 - (y-d)^2 \\ =& 2\cdot(c-a)\cdot x + 2\cdot(d-b)\cdot y + a^2 + b^2 - c^2 - d^2. \end{aligned}$$

Dies ist eine lineare Gleichung in x und y mit Koeffizienten in K und die Lösungsmenge ist somit eine Gerade durch zwei Punkte in K. Die Schnittpunkte von k und l sind also die Schnittpunkte dieser Geraden mit k, so daß wir aus c. ableiten, daß die Adjunktion von höchstens einer Quadratwurzel ω mit $\omega^2 \in K$ ausreicht, um die Schnittpunkte in $K(\omega)$ wiederzufinden.

Definition 4.6 (2-Radikalerweiterung)
Eine Körpererweiterung L/K heißt eine 2-*Radikalerweiterung*, wenn es eine Kette

$$K = K_0 < K_1 < \ldots < K_n = L$$

von Zwischenkörper mit $K_i = K_{i-1}(\omega_i)$ für ein $\omega_i \notin K_{i-1}$ mit $\omega_i^2 \in K_{i-1}$ gibt.

Man beachte, daß dann $t^2 - \omega_i^2 \in K_{i-1}[t]$ das Minimalpolynom von ω_i über K_{i-1} ist und daß somit

$$|K_i : K_{i-1}| = 2.$$

Korollar 4.7 (Konstruierbarkeit und 2-Radikalerweiterungen)
Sei $0, 1 \in M \subseteq \mathbb{C}$ *eine Teilmenge von* $\mathbb{C}$, $K = \mathbb{Q}(M \cup \overline{M})$ *und* $z \in \mathbb{C}$.
Dann sind die folgenden Aussagen gleichwertig:

a. z *ist aus* M *mit Zirkel und Lineal konstruierbar, d. h.* $z \in \widetilde{M}$.

b. $K(z)/K$ *ist eine* 2*-Radikalerweiterung.*

Insbesondere ist dann z *algebraisch mit* $|K(z) : K| = 2^n$ *für ein* $n \in \mathbb{N}$.

Beweis: Ist z aus M mit Zirkel und Lineal konstruierbar, so sind hierfür nur endlich viele Elementaroperationen notwendig und aus Bemerkung 4.5 folgt, daß in jedem Schritt höchstens eine Quadratwurzel adjungiert werden muß. Also ist $K(z)/K$ eine 2-Radikalerweiterung.

Ist umgekehrt $K(z)/K$ eine 2-Radialerweiterung und ist

$$K = K_0 < K_1 < \ldots < K_n = K(z)$$

die zugehörige Zwischenkörperkette mit $K_i = K_{i-1}(\omega_i)$, $\omega_i^2 \in K_{i-1}$ und $\omega_i \notin K_{i-1}$ für $i = 1, \ldots, n$.

Wir zeigen mit abbrechender Induktion nach i, daß

$$K_i \subseteq \widetilde{M}$$

gilt, wobei die Aussage für $n = 0$

$$K_0 = K = \mathbb{Q}\big(M \cup \overline{M}\big) \overset{4.4,4.2}{\subseteq} \widetilde{M}$$

aus Satz 4.4 und Beispiel 4.2 folgt. Sei nun bereits

$$K_{i-1} \subseteq \widetilde{M}$$

gezeigt. Da $\widetilde{M}$ quadratisch abgeschlossen ist (siehe Satz 4.4), folgt

$$\omega_i \in \widetilde{M}$$

und mithin auch

$$K_i = K_{i-1}(\omega_{i-1}) \subseteq \widetilde{M}.$$

Für $i = n$ erhalten wir dann, daß

$$z \in K(z) = K_n \subseteq \widetilde{M}$$

mit Zirkel und Lineal konstruierbar ist.

Die Aussage zum Grad der Körpererweiterung folgt aus der Gradformel 3.22. □

Wir sind nun in der Lage, einige klassische Probleme zur Konstruierbarkeit mit Zirkel und Lineal zu stellen und zu beantworten.

Bemerkung 4.8 (Das Delische Problem)
Dabei geht es um die Frage, ob wir in der Lage sind, aus einem gegebenen Würfel mit Zirkel und Lineal einen Würfel von doppeltem Volumen zu konstruieren.

Wir können hierfür annehmen, daß die Seitenlänge des Würfels und damit auch sein Volumen 1 ist, so daß sich die Aufgabe darauf reduziert, mit Zirkel und Lineal aus der Menge $M = \{0, 1\}$ die Zahl

$$z = \sqrt[3]{2}$$

zu konstruieren, da dies die Seitenlänge eines Würfels mit doppeltem Volumen sein wird. Da aber z das Minimalpolynom

$$\mu_z = t^3 - 2 \in \mathbb{Q}\big(M \cup \overline{M}\big)[t] = \mathbb{Q}[t]$$

vom Grad 3 hat und somit

$$|\mathbb{Q}(z) : \mathbb{Q}| = 3$$

gilt, ist $z = \sqrt[3]{2}$ nach Korollar 4.7 nicht mit Zirkel und Lineal konstruierbar. Das Delische Problem ist also nicht lösbar.

Bemerkung 4.9 (Quadratur des Kreises)
Hierbei geht es um die Aufgabe, zu einem gegebenen Kreis mit Zirkel und Lineal ein Quadrat mit demselben Flächeninhalt zu konstruieren.

Wir können hierfür annehmen, daß der Kreis den Mittelpunkt 0 und den Radius 1 hat, so daß sein Flächenhinhalt den Wert π hat. Unsere Aufgabe besteht dann darin, die Zahl $z = \sqrt{\pi}$ aus der Menge $M = \{0, 1\}$ zu konstruieren. Man kann nun aber zeigen, daß $\sqrt{\pi}$ nicht algebraisch über $\mathbb{Q} = \mathbb{Q}(M \cup \overline{M})$ ist, so daß $\sqrt{\pi}$ auch nicht mit Zirkel und Lineal konstruierbar ist (siehe Korollar 4.7). Die Quadratur des Kreises ist also nicht möglich.

Bemerkung 4.10 (Winkeldreiteilung)
Bei dem Problem geht es darum, zu einem beliebigen Winkel φ mit Zirkel und Lineal den Winkel $\frac{\varphi}{3}$ zu konstruieren.

Dieses Problem können wir normieren zu der Aufgabe, aus der Menge

$$M = \{0, 1, e^{i\varphi}\}$$

die Zahl

$$z = e^{\frac{i\varphi}{3}}$$

zu konstruieren. Es gibt Winkel φ, für die das möglich ist. Ist etwa $\varphi = \frac{3\pi}{2}$, so ist

$$z = i \in \widetilde{M}.$$

Die Aufgabe ist aber nicht für alle Winkel lösbar. Ist nämlich $e^{i\varphi}$ transzendent über $\mathbb{Q}$, so ist das Polynom

$$t^3 - e^{i\varphi} \in \mathbb{Q}(e^{i\varphi})[t]$$

irreduzibel nach dem Eisensteinkriterium[3] (Satz 2.2) und Satz 2.4, so daß die Körpererweiterung

$$\mathbb{Q}(e^{\frac{i\varphi}{3}})/\mathbb{Q}(e^{i\varphi}) = \mathbb{Q}(e^{i\varphi})(e^{\frac{i\varphi}{3}})/\mathbb{Q}(e^{i\varphi})$$

den Grad

$$|\mathbb{Q}(e^{\frac{i\varphi}{3}}) : \mathbb{Q}(e^{i\varphi})| = 3$$

hat. Aus Korollar 4.7 folgt dann, daß $z = e^{\frac{i\varphi}{3}}$ nicht konstruierbar ist. Da die Zahl der über $\mathbb{Q}$ algebraischen Zahlen aber abzählbar ist und da der Kreis vom Radius 1 um 0 überabzählbar viele Zahlen enthält, muß es solche transzendenten $e^{i\varphi}$ geben. Die Winkeldreiteilung ist also im allgemeinen nicht möglich.

Bemerkung 4.11 (Konstruierbarkeit des regelmäßigen n-Ecks)
Mit Hilfe der Galoistheorie, die wir im weiteren Verlauf der Vorlesung entwickeln werden, können wir auch entscheiden, welche regelmäßigen n-Ecke mit Zirkel nun Lineal konstruierbar sind (siehe Abschnitt 11.D)).

[3]Ist $e^{i\varphi}$ transzendent über $\mathbb{Q}$, so gilt $\mathbb{Q}[e^{i\varphi}] \cong \mathbb{Q}[x]$ und $\mathbb{Q}(e^{i\varphi}) \cong \mathbb{Q}(x)$, wobei die Isomorphismen $e^{i\varphi}$ und x identifizieren (siehe Bemerkung 3.14). Der Ring $\mathbb{Q}[e^{i\varphi}]$ ist also faktoriell und $e^{i\varphi}$ ist in dem Ring ein Primelement, so daß das Eisensteinkriterium und Satz 2.4 anwendbar sind.

§ 5 Zerfällungskörper

Im Abschnitt 3 haben wir uns mit der Frage beschäftigt, ob bestimmte Elemente eines gegebenen Erweiterungskörpers L von K Nullstelle eines Polynoms mit Koeffizienten in K sind. In diesem Abschnitt wollen wir zu einem gegebenen Polynom f mit Koeffizienten in K einen Erweiterungskörper suchen, in dem das Polynom dann Nullstellen besitzt. Den kleinsten Erweiterungskörper, in dem f in Linearfaktoren zerfällt, werden wir seinen Zerfällungskörper nennen.

Aufgrund des Fundamentalsatzes der Algebra wissen wir, daß ein Polynom f mit rationalen Koeffizienten in $\mathbb{C}$ zerfällt, so daß man leicht sieht, daß f einen Zerfällungskörper besitzt und daß dieser ein Teilkörper von $\mathbb{C}$ sein muß. Für beliebige Körper, etwa $K = \mathbb{F}_p$ oder $K = \mathbb{Q}(t)$, ist die Existenz eines solchen Körpers a priori nicht klar. Wir werden ihn in diesem Abschnitt konstruieren und dabei sehen, daß er bis auf Isomorphie eindeutig bestimmt ist.

A) Stammkörper

Ein irreduzibles Polynom $f \in K[t]$ vom Grad $\deg(f) \geq 2$ hat in K keine Nullstelle. Wir wollen zunächst einen Erweiterungskörper von K konstruieren, in dem f eine Nullstelle besitzt. In der Tat ist dies unter Berücksichtigung von Proposition 2.1 eine triviale Angelegenheit.

Definition 5.1 (Stammkörper)
Es sei $f \in K[t]$ irreduzibel und L/K eine Körpererweiterung.
Ist $L = K(\alpha)$ für ein $\alpha \in L$ mit $f(\alpha) = 0$, so heißt L ein *Stammkörper* von f.

Satz 5.2 (Existenz von Stammkörpern)
Es sei K ein Körper und $f \in K[t]$ ein irreduzibles Polynom.

a. $K[t]/\langle f\rangle$ ist ein Erweiterungskörper von K und das Polynom f hat in $K[t]/\langle f\rangle$ die Nullstelle $\overline{t}$.

b. Das Polynom $f/_{lc(f)}$ ist das Minimalpolynom von $\overline{t} \in K[t]/\langle f\rangle$ über K und

$$K[t]/\langle f\rangle = K\big(\overline{t}\big).$$

Insbesondere ist $K[t]/\langle f\rangle$ ein Stammkörper von f.

Beweis: Wir identifizieren die Elemente a von K mit den Restklassen $\overline{a}$ in $K[t]/\langle f\rangle$. Da die Abbildung

$$\varphi : K \hookrightarrow K[t]/\langle f\rangle : a \mapsto \overline{a}.$$

ein Körpermonomorphismus ist und somit K und $\varphi(K)$ nach Lemma 3.5 isomorph sind, ist das eine zulässige Identifizierung.

a. Aus Proposition 2.1 wissen wir, daß $L = K[t]/\langle f\rangle$ ein Körper ist, weil f irreduzibel ist. Außerdem gilt für $f = \sum_{k=0}^{n} a_k t^k$ mittels der obigen Identifizierung in

$K[t]/\langle f\rangle$ dann

$$f(\bar{t}) = \sum_{k=0}^{n} \overline{a_k} \cdot \bar{t}^k = \overline{\sum_{k=0}^{n} a_k t^k} = \bar{f} = \bar{0}.$$

b. Da jedes Element in $K[t]/\langle f\rangle$ ein Polynom in $\bar{t}$ ist, gilt

$$K[t]/\langle f\rangle = K\big[\bar{t}\big].$$

Da zudem $\bar{t}$ als Nullstelle des Polynoms f algebraisch ist, gilt nach Satz 3.15

$$K\big[\bar{t}\big] = K(\bar{t}).$$

Aus demselben Satz folgt, daß das Minimalpolynom $\mu_{\bar{t}}$ von t über K ein normierter, nicht-konstanter Teiler des normierten irreduziblen Polynoms $f/_{lc(f)}$ sein muß, so daß beide übereinstimmen müssen.

□

Aufgabe 5.3
Beschreibe den Stammkörper

$$L = \mathbb{F}_2[t]/\langle t^2 + t + 1\rangle$$

des irreduziblen Polynoms $f = t^2 + t + 1 \in \mathbb{F}_2[t]$ mittels einer Additions- und Multiplikationstabelle.

Wir wollen nun noch zeigen, daß der Stammkörper bis auf eindeutige Isomorphie eindeutig bestimmt ist. Dazu sind zunächst ein paar Vorbemerkungen zur Fortsetzung von Körperisomorphismen notwendig.

Bemerkung 5.4 (Erweiterung von Körperisomorphismen auf Polynomringe)
Ist die Abbildung

$$\varphi : K \longrightarrow K'$$

ein Körperisomorphismus, so ist die Abbildung

$$K[t] \longrightarrow K'[t] : \sum_{k=0}^{n} a_k t^k \mapsto \sum_{k=0}^{n} \varphi(a_k) t^k \tag{7}$$

ein Ringisomorphismus, die wir der Einfachheit halber wieder mit φ bezeichnen.

Insbesondere ist f genau dann irreduzibel in $K[t]$, wenn $\varphi(f)$ irreduzibel in $K'[t]$ ist.

Proposition 5.5 (Fortsetzbarkeit von Isomorphismen auf Stammkörper)
Es sei $\varphi : K \longrightarrow K'$ *ein Körperisomorphismus,* $f \in K[t]$ *sei irreduzibel,* $L = K(\alpha)$ *mit* $f(\alpha) = 0$ *sei ein Stammkörper von* f *und* $L' = K'(\alpha')$ *mit* $\varphi(f)(\alpha') = 0$ *sei ein Stammkörper von* $\varphi(f)$.
Dann gibt es genau einen Körperisomorphismus $\psi : L \longrightarrow L'$ *mit* $\psi_{|K} = \varphi$ *und*

$$\psi(\alpha) = \alpha'.$$

Man kann die Aussage durch folgendes kommutatives Diagramm veranschaulichen:

$$\begin{array}{ccc} K & \xrightarrow[\varphi]{\cong} & K' \\ \downarrow & & \downarrow \\ K(\alpha) & \xrightarrow[\exists_1 \psi]{\cong} & K'(\alpha') \\ \alpha & \longmapsto & \alpha' \end{array}$$

Beweis: Der Ringisomorphismus φ aus Gleichung (7) in Bemerkung 5.4 induziert einen Ringisomorphismus

$$\overline{\varphi} : K[t]/\langle f\rangle \xrightarrow{\cong} K'[t]/\langle \varphi(f)\rangle : \overline{g} \mapsto \overline{\varphi(g)},$$

da

$$\varphi\left(\langle f\rangle\right) = \langle \varphi(f)\rangle.$$

Satz 3.15 liefert uns zwei Isomorphismen

$$\overline{\phi_\alpha} : K[t]/\langle \mu_\alpha\rangle \longrightarrow K(\alpha) : \overline{g} \mapsto g(\alpha)$$

und

$$\overline{\phi_{\alpha'}} : K'[t]/\langle \mu_{\alpha'}\rangle \longrightarrow K'(\alpha) : \overline{h} \mapsto h(\alpha'),$$

die von den Einsetzhomomorphismen ϕ_α und $\phi_{\alpha'}$ induziert wurden. Nun beachten wir noch, daß aus Satz 5.2 die Gleichheit

$$\langle \mu_\alpha\rangle = \langle f\rangle$$

und

$$\langle \mu_{\alpha'}\rangle = \langle \varphi(f)\rangle$$

folgt. Damit können wir $\psi = \overline{\phi_{\alpha'}} \circ \overline{\varphi} \circ \overline{\phi_\alpha^{-1}}$ nun als Komposition

$$\psi : K(\alpha) \xrightarrow{\overline{\phi_\alpha^{-1}}} K[t]/\langle f\rangle \xrightarrow{\overline{\varphi}} K'[t]/\langle \varphi(f)\rangle \xrightarrow{\overline{\phi_{\alpha'}}} K'(\alpha')$$

dreier Isomorphismen definieren und erhalten somit einen Isomorphismus ψ. Für $a \in K$ gilt dann

$$\psi(a) = \overline{\phi_{\alpha'}} \circ \overline{\varphi} \circ \overline{\phi_\alpha^{-1}}(a) = \overline{\phi_{\alpha'}} \circ \overline{\varphi}\big(\overline{a}\big) = \overline{\phi_{\alpha'}}\big(\overline{\varphi(a)}\big) = \varphi(a)$$

und das Bild von α berechnet sich als

$$\psi(\alpha) = \overline{\phi_{\alpha'}} \circ \overline{\varphi} \circ \overline{\phi_\alpha^{-1}}(\alpha) = \overline{\phi_{\alpha'}} \circ \overline{\varphi}\big(\overline{t}\big) = \overline{\phi_{\alpha'}}\big(\overline{t}\big) = \alpha'.$$

Es bleibt noch die Eindeutigkeit des Isomorphismus zu zeigen. Sei dazu

$$\Psi : K(\alpha) \longrightarrow K'(\alpha')$$

ein zweiter Körperisomorphismus mit $\Psi_{|K} = \varphi$ und $\Psi(\alpha) = \alpha'$. Jedes Element β in $K(\alpha)$ ist ein Polynom in α mit Koeffizienten in K, ist also von der Form

$$\beta = \sum_{k=0}^{n} a_k \alpha^k.$$

Dann gilt aber

$$\Psi(\beta) = \sum_{k=0}^{n} \Psi(a_k)\Psi(\alpha)^k = \sum_{k=0}^{n} \varphi(a_k)(\alpha')^k = \sum_{k=0}^{n} \psi(a_k)\psi(\alpha)^k = \psi(\beta),$$

und es folgt $\Psi = \psi$. □

Wendet man die Proposition auf die Identität von K an, so erhält man die folgende Eindeutigkeitsaussage für Stammkörper.

Korollar 5.6 (Eindeutigkeit des Stammkörpers)
Sind $K(\alpha)$ *und* $K(\alpha')$ *zwei Stammkörper des irreduziblen Polynoms* $f \in K[t]$ *mit* $f(\alpha) = f(\alpha') = 0$*, so gibt es genau einen Isomorphismus*

$$\psi : K(\alpha) \longrightarrow K(\alpha')$$

mit $\psi_{|K} = \mathrm{id}_K$ *und* $\psi(\alpha) = \alpha'$*.*
Insbesondere ist der Stammkörper von f *bis auf Isomorphie eindeutig bestimmt.*

Beweis: Die Aussage folgt aus Proposition 5.5 mit $\varphi = \mathrm{id}_K$. □

Beispiel 5.7 (Stammkörper)
Das Polynom $f = t^4 - 2 \in \mathbb{Q}[t]$ ist aufgrund des Eisenstein-Kriteriums 2.2 irreduzibel und hat in $\mathbb{C}$ die Nullstellen

$$\alpha_1 = \sqrt[4]{2}, \quad \alpha_2 = \sqrt[4]{2} \cdot i, \quad \alpha_3 = -\sqrt[4]{2}, \quad \alpha_4 = -\sqrt[4]{2} \cdot i.$$

Die folgenden Erweiterungskörper von $\mathbb{Q}$ sind somit als Stammkörper von f isomorph zueinander:

$$\mathbb{Q}\big(\sqrt[4]{2}\big) \cong \mathbb{Q}\big(\sqrt[4]{2} \cdot i\big) \cong \mathbb{Q}[t]/\langle t^4 - 2\rangle.$$

B) Zerfällungskörper

Definition 5.8 (Zerfällungskörper)
Es sei K ein Körper und $f \in K[t]$ ein Polynom vom Grad $\deg(f) = n$.
Ein Erweiterungskörper L von K heißt ein *Zerfällungskörper* von f über K, wenn

$$L = K(\alpha_1, \ldots, \alpha_n)$$

und

$$f = \mathrm{lc}(f) \cdot (t - \alpha_1) \cdot \ldots \cdot (t - \alpha_n).$$

Bemerkung 5.9 (Zerfällungskörper)
Ein Zerfällungskörper L von f ist ein Erweiterungskörper von K, über dem L in Linearfaktoren zerfällt. Die Tatsache, daß L zudem aus K durch Adjunktion der Nullstellen von f entsteht, bedeutet, daß L minimal mit dieser Eigenschaft ist. Man hat K also gerade nur um soviel erweitert, wie nötig ist, um das Zerfallen von f zu gewährleisten.

Beispiel 5.10
Der Körper

$$\mathbb{C} = \mathbb{R}(i) = \mathbb{R}(i, -i)$$

ist der Zerfällungskörper des Polynoms

$$f = t^2 + 1 = (t - i) \cdot (t + i) \in \mathbb{R}[t].$$

Also gilt auch

$$\mathbb{C} \cong \mathbb{R}[t]/\langle t^2 + 1 \rangle.$$

Satz 5.11 (Existenz von Zerfällungskörpern)
Zu jedem Polynom $f \in K[t]$ *gibt es einen Zerfällungskörper von* f *über* K.

Beweis: Wir beweisen die Aussage mittels Induktion nach $n = \deg(f)$. Ist $n = 0$, so ist $L = K$ ein Zerfällungskörper von f und der Induktionsanfang ist gezeigt.

Für $n > 0$ besitzt f aufgrund der Primfaktorzerlegung einen irreduziblen Faktor g und zu diesem gibt es einen Stammkörper $L_1 = K(\alpha_1)$ mit $g(\alpha_1) = 0$. Wegen $f = g \cdot h$ ist dann aber auch

$$f(\alpha_1) = g(\alpha_1) \cdot h(\alpha_1) = 0,$$

und α_1 ist eine Nullstelle von f in L_1. Wir können in $L_1[t]$ also den Linearfaktor $t - \alpha_1$ von f abspalten und erhalten

$$f = (t - \alpha_1) \cdot f_1$$

für ein $f_1 \in L_1[t]$ vom Grad $n - 1$. Wenden wir Induktion auf f_1 an, so finden wir einen Erweiterungskörper

$$L = L_1(\alpha_2, \ldots, \alpha_n) = K(\alpha_1, \ldots, \alpha_n)$$

von L_1, so daß

$$f_1 = \mathrm{lc}(f_1) \cdot (t - \alpha_2) \cdot \ldots \cdot (t - \alpha_n).$$

Wegen $\mathrm{lc}(f) = \mathrm{lc}(f_1)$ erhalten wir dann aber auch

$$f = (t - \alpha_1) \cdot f_1 = \mathrm{lc}(f_1) \cdot (t - \alpha_1) \cdot \ldots \cdot (t - \alpha_n),$$

und L ist ein Zerfällungskörper von f. □

Beispiel 5.12
Der Beweis des Satzes ist konstruktiv und zeigt, daß wir einen Zerfällungskörper berechnen können, indem wir sukzessive Stammkörper berechnen. Wir wollen das am Beispiel von

$$f = t^4 - 2 \in \mathbb{Q}[t]$$

vorführen. Wir kennen die Nullstellen

$$\alpha_1 = \sqrt[4]{2}, \quad \alpha_2 = \sqrt[4]{2} \cdot i, \quad \alpha_3 = -\sqrt[4]{2}, \quad \alpha_4 = -\sqrt[4]{2} \cdot i.$$

von f bereits aus Beispiel 5.7. Da f irreduzibel ist, erhalten wir im ersten Schritt also die Körpererweiterung

$$L_1 = \mathbb{Q}(\alpha_1) = \mathbb{Q}\big(\sqrt[4]{2}\big).$$

Über dieser faktorisiert f als

$$f = (t-\alpha_1)\cdot(t-\alpha_3)\cdot(t+\alpha_1^2) = \big(t-\sqrt[4]{2}\big)\cdot\big(t+\sqrt[4]{2}\big)\cdot\big(t^2+\sqrt{2}\big).$$

Das Polynom

$$f_1 = t+\alpha_1^2 = t^2+\sqrt{2} \in \mathbb{Q}(\alpha_1)[t]$$

ist wiederum irreduzibel, da seine Nullstellen rein imaginär sind und deshalb nicht in dem rein reellen Körper $\mathbb{Q}(\alpha_1)$ liegen können. α_2 ist eine der Nullstellen, so daß wir im zweiten Schritt den Körper

$$L_2 = L_1(\alpha_2) = \mathbb{Q}(\alpha_1,\alpha_2)$$

erhalten, über dem f_1 und damit auch f dann in Linearfaktoren zerfällt:

$$f = (t-\alpha_1)\cdot(t+\alpha_1)\cdot(t-\alpha_2)\cdot(t+\alpha_2).$$

Wegen $\alpha_3 = -\alpha_1 \in L_2$ und $\alpha_4 = -\alpha_2 \in L_2$ gilt dann auch

$$L_2 = \mathbb{Q}(\alpha_1,\alpha_2) = \mathbb{Q}(\alpha_1,\alpha_2,\alpha_3,\alpha_4)$$

und L_2 ist ein Zerfällungskörper von f über $\mathbb{Q}$. Ersetzen wir bei der Adjunktion α_2 durch $\frac{\alpha_2}{\alpha_1} = i$, so erhalten wir denselben Körper in anderer Darstellung. Es gilt also

$$L_2 = \mathbb{Q}\big(\sqrt[4]{2}, i\big)$$

ist ein Zerfällungskörper von $f = t^4-2$ über $\mathbb{Q}$.

Wie beim Stammkörper eines irreduziblen Polynoms wollen wir zeigen, daß der Zerfällungskörper bis auf Isomorphie eindeutig bestimmt ist. Der wesentliche Schritt dazu ist die folgende Proposition.

Proposition 5.13 (Fortsetzbarkeit von Isomorphismen auf Zerfällungskörper)
Es sei $\varphi : K \longrightarrow K'$ ein Körperisomorphismus, L sei ein Zerfällungskörper von $f \in K[t]$ und L' sei ein Zerfällungskörper von $\varphi(f) \in K'[t]$.

a. *Ist $\psi : L \longrightarrow L'$ ein Körperisomorphismus mit $\psi_{|K} = \varphi$, so bildet ψ die Nullstellen von f bijektiv auf die Nullstellen von $\varphi(f)$ ab.*

b. *Es gibt einen Körperisomorphismus $\psi : L \longrightarrow L'$ mit $\psi_{|K} = \varphi$.*

Man kann die Aussage durch folgendes kommutatives Diagramm veranschaulichen:

$$\begin{array}{ccc} K & \xrightarrow[\varphi]{\cong} & K' \\ \big\downarrow & & \big\downarrow \\ L & \xrightarrow[\exists\psi]{\cong} & L' \end{array}$$

Beweis: a. Ist $\alpha \in L$ eine Nullstelle von $f = \sum_{k=0}^{n} a_k t^k$, so gilt

$$\varphi(f)\big(\psi(\alpha)\big) = \sum_{k=0}^{n} \varphi(a_k) \cdot \psi(\alpha)^k = \sum_{k=0}^{n} \psi(a_k) \cdot \psi(\alpha)^k = \psi\big(f(\alpha)\big) = \psi(0) = 0.$$

Also werden die Nullstellen von f auf Nullstellen von $\varphi(f)$ abgebildet. Da wir mit Hilfe von φ^{-1} und ψ^{-1} die Rollen von f und $\varphi(f)$ vertauschen können, sehen wir auch, daß wir auf diesem Wege genau die Nullstellen von $\varphi(f)$ erhalten.

b. Wir beweisen die Aussage mit Induktion nach $n = \deg(f)$, wobei für $n = 0$ nichts zu zeigen ist, da dann $K = L$ und $K' = L'$, so daß $\psi = \varphi$ die gewünschte Fortsetzung ist.
Für $n > 0$ können wir einen irreduziblen Faktor g von f wählen. Dann ist auch $\varphi(g)$ ein irreduzibler Faktor von $\varphi(f)$. Zudem gibt es ein $\alpha_1 \in L$, das Nullstelle von g ist, da f über L in Linearfaktoren zerfällt, und

$$L_1 = K(\alpha_1)$$

ist ein Stammkörper von g über K. Analog besitzt $\varphi(g)$ eine Nullstelle $\alpha_1' \in L'$ und

$$L_1' = K'(\alpha_1')$$

ist ein Stammkörper von $\varphi(g)$ über K'. Aus Proposition 5.5 erhalten wir dann eine Fortsetzung

$$\begin{array}{ccc} K & \xrightarrow[\varphi]{\cong} & K' \\ \big\downarrow & & \big\downarrow \\ L_1 & \xrightarrow[\exists\phi]{\cong} & L_1' \end{array}$$

von φ auf die beiden Stammkörper mit $\phi(\alpha_1) = \alpha_1'$. Dann gilt aber

$$f = (t - \alpha_1) \cdot f_1$$

mit $f_1 \in L_1[t]$ vom Grad $n - 1$ und

$$\varphi(f) = (t - \alpha_1') \cdot \phi(f_1)$$

mit $\phi(f_1) \in L_1'[t]$. Man beachte, daß L ein Zerfällungskörper von f_1 über L_1 ist und daß L' ein Zerfällungskörper von $\phi(f_1)$ über L_1' ist. Wenden wir Induktion auf f_1 an, so erhalten wir einen Körperisomorphismus

$$\psi : L \longrightarrow L'$$

mit $\psi_{|L_1} = \phi$. Insbesondere gilt dann aber

$$\psi_{|K} = \phi_{|K} = \varphi.$$

□

Aus der Proposition leiten wir sofort die Eindeutigkeit des Zerfällungskörpers bis auf Isomorphie ab.

Korollar 5.14 (Eindeutigkeit des Zerfällungskörpers)
Sind L *und* L' *zwei Zerfällungskörper des Polynoms* $f \in K[t]$*, so gibt es einen Isomorphismus*

$$\psi : L \longrightarrow L'$$

mit $\psi_{|K} = \mathrm{id}_K$*. Zerfällt zudem* f *über* L *als*

$$f = \mathrm{lc}(f) \cdot (t - \alpha_1) \cdot \ldots \cdot (t - \alpha_n)$$

und über L' *als*

$$f = \mathrm{lc}(f) \cdot (t - \alpha'_1) \cdot \ldots \cdot (t - \alpha'_n),$$

so gibt es eine Permutation $\sigma \in \mathbb{S}_n$ *mit*

$$\psi(\alpha_i) = \alpha'_{\sigma(i)}$$

für $i = 1, \ldots, n$*.*

Beweis: Dies folgt aus Proposition 5.13 mit $\varphi = \mathrm{id}_K$. □

Bemerkung 5.15 (Der Zerfällungskörper)
Da der Zerfällungskörper eines Polynoms $f \in K[t]$ bis auf Isomorphie eindeutig bestimmt ist, können wir von *dem* Zerfällungskörper $\mathrm{ZFK}_K(f)$ von f über K sprechen.

Aufgabe 5.16
Ist $L = \mathrm{ZFK}_K(f)$ der Zerfällungskörper eines Polynoms $f \in K[t]$ vom Grad n, so ist der Grad der Körpererweiterung $|L : K|$ ein Teiler von $n!$.

§ 6 Endliche Körper

Wir wollen in diesem Abschnitt die endlichen Körper vollständig klassifizieren. Wir werden zeigen, daß die Mächtigkeit eines endlichen Körpers immer eine Primzahlpotenz ist und daß es zu jeder Primzahlpotenz p^n bis auf Isomorphie nur einen Körper mit p^n Elementen gibt.

Proposition 6.1 (Endliche Körper haben Primzahlpotenzordnung.)
Ist K *ein endlicher Körper, so ist* $\mathrm{char}(K) = p \in \mathbb{P}$ *eine Primzahl und*

$$|K| = p^n$$

für $n = |K : P|$*, wenn* $P \cong \mathbb{F}_p$ *der Primkörper von* K *ist.*

Beweis: Wenn K nur endlich viele Elemente besitzt, so ist die additive Ordnung von 1_K endlich, aber diese ist gerade die Charakteristik des Körpers und mit Satz 3.8 ist sie dann eine Primzahl.

Der Primkörper P von K ist ein Teilkörper von K, so daß K ein P-Vektorraum der Dimension $n = |K : P|$ ist. Mithin ist K also P-Vektorraum isomorph zu P^n und seine Mächtigkeit ist

$$|K| = |P|^n = |\mathbb{F}_p|^n = p^n.$$

□

Beispiel 6.2 (Ein Körper mit vier Elementen.)
Der endliche Körper

$$K = \mathbb{F}_2[t]/\langle t^2 + t + 1\rangle$$

aus Aufgabe 3.5 hat Charakteristik zwei und hat genau vier Elemente,

$$K = \left\{\overline{0}, \overline{1}, \overline{t}, \overline{t+1}\right\}.$$

In einem Körper der Charakteristik p vereinfacht sich der binomische Lehrsatz für das Potenzieren mit p enorm. Man erhält die Rechenregel, die in der Schule über den reellen Zahlen oft fälschlicherweise angewendet wird.

Proposition 6.3 (Der Frobeniushomomorphismus)
Es sei K *ein Körper der Charakteristik* p*. Für* $a, b \in K$ *gilt dann*

$$(a + b)^p = a^p + b^p.$$

Insbesondere ist die Abbildung

$$\eta_p : K \longrightarrow K : a \mapsto a^p$$

ein Körpermonomorphismus, der Frobeniushomomorphismus *von* K*, und* η_p *operiert auf dem Primkörper von* K *als Identität.*

Beweis: Der Binomialkoeffizient

$$\binom{p}{k} = \frac{p \cdot (p-1) \cdot \ldots (p-k+1)}{k \cdot (k-1) \cdot \ldots \cdot 1} \in \mathbb{N}$$

ist für $1 \leq k \leq p-1$ durch p teilbar, die Primzahl p im Zähler vorkommt, im Nenner aber nicht. Damit gilt aber

$$\binom{p}{k} \cdot c = 0$$

für jedes $c \in K$ und jedes $1 \leq k \leq p-1$. Der binomische Lehrsatz liefert also

$$(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} \cdot a^k \cdot b^{p-k} = a^p + b^p,$$

weil die mittleren Summanden alle 0 sind. Für die Abbildung η_p ergibt sich daraus

$$\eta_p(a+b) = (a+b)^p = a^p + b^p = \eta_p(a) + \eta_p(b).$$

Aufgrund der Potenzgesetzte gilt zudem

$$\eta_p(a \cdot b) = (a \cdot b)^p = a^p \cdot b^p = \eta_p(a) \cdot \eta_p(b),$$

und für die Eins gilt ohnehin

$$\eta_p(1) = 1^p = 1.$$

Also ist η_p ein Körperhomomorphismus und nach Lemma 3.5 auch ein Monomorphismus. Beachte auch, daß $\eta_p(1) = 1$ gilt, so daß

$$\eta_p(\underbrace{1+\ldots+1}_{k}) = \underbrace{\eta_p(1)+\ldots+\eta_p(1)}_{k} = \underbrace{1+\ldots+1}_{k}$$

gilt, was zur Folge hat, daß η_p auf den Primkörper eingeschränkt die Identität ist. □

Beispiel 6.4
Betrachten wir den Körper $K = \mathbb{F}_2[t]/\langle t^2+t+1\rangle$ aus Aufgabe 6.2, gilt:

$\overline{a}$	$\eta_2(\overline{a})$
$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{1}$
$\overline{t}$	$\overline{t^2} = \overline{t+1}$
$\overline{t+1}$	$\overline{t^2+2t+1} = \overline{t}$

Der Frobeniushomomorphismus ist also ein Isomorphismus. Insbesondere besitzt jedes Element in K eine eindeutig bestimmte Quadratwurzel in K.

Es ist kein Zufall, daß der Frobeniushomomorphismus in diesem Fall ein Isomorphismus ist.

Korollar 6.5 (Der Frobeniushomomorphismus für endliche Körper)
Ist K ein endlicher Körper der Charakteristik p, so ist der Frobeniushomomorphismus

$$\eta_p : K \longrightarrow K : a \mapsto a^p$$

ein Isomorphismus. Insbesondere besitzt jedes $a \in K$ genau eine p-te Wurzel in K.

Beweis: Ist K endlich, so ist jede injektive Abbildung von K nach K automatisch auch surjektiv. Also ist η_p wegen Proposition 6.3 ein Isomorphismus. □

Definition 6.6 (Vielfachheit einer Nullstelle)
Eine Nullstelle $\alpha \in L$ eines Polynoms $f \in L[t]$ hat die *Vielfachheit* k, wenn es ein Polynom $g \in L[t]$ gibt, so daß

$$f = (t - \alpha)^k \cdot g$$

und $g(\alpha) \neq 0$. Eine *mehrfache Nullstelle* von f ist eine Nullstelle von f von Vielfachheit mindestens zwei.

Bemerkung 6.7 (Formale Ableitung)
Für ein Polynom $f = \sum_{i=0}^{n} a_i t^i$ können wir die *formale Ableitung* als

$$f' = \sum_{i=1}^{n} i a_i t^{i-1}$$

definieren. Man zeigt dann sehr leicht, daß die formale Ableitung den üblichen Rechenregeln für Ableitungen genügt. Es gilt etwa die *Produktregel*

$$(f \cdot g)' = f' \cdot g + f \cdot g'$$

sowie

$$(t - \alpha)^k = k \cdot (t - \alpha)^{k-1}.$$

Lemma 6.8 (Kriterium für mehrfache Nullstellen)
Eine Nullstelle $\alpha \in L$ von $f \in L[t]$ ist genau dann eine mehrfache Nullstelle, wenn α eine Nullstelle der formalen Ableitung f' ist.

Beweis: Bezeichnen wir die Vielfachheit von α als Nullstelle von f mit k, so gilt

$$f = (t - \alpha)^k \cdot g$$

mit $g(\alpha) \neq 0$ und $k \geq 1$. Für die formale Ableitung von f erhalten wir also

$$f' = k \cdot (t - \alpha)^{k-1} \cdot g + (t - \alpha)^k \cdot g'.$$

Ist nun $k = 1$, so folgt

$$f'(\alpha) = 1 \cdot (\alpha - \alpha)^0 \cdot g(\alpha) + (\alpha - \alpha) \cdot g'(\alpha) = g(\alpha) \neq 0.$$

Ist umgekehrt $k \geq 2$, so gilt

$$f'(\alpha) = k \cdot (\alpha - \alpha)^{k-1} \cdot g(\alpha) + (\alpha - \alpha)^k \cdot g'(\alpha) = 0 + 0 = 0.$$

□

Satz 6.9 (Existenz eines Körpers mit p^n Elementen.)
Der Zerfällungskörper des Polynoms $f = t^{p^n} - t \in \mathbb{F}_p[t]$ hat genau p^n Elemente.

Beweis: Für den Zerfällungskörper $\mathrm{ZFK}_{\mathbb{F}_p}(f)$ von f über $\mathbb{F}_p$ gilt

$$\mathrm{ZFK}_{\mathbb{F}_p}(f) = \mathbb{F}_p(\alpha_1, \ldots, \alpha_{p^n})$$

mit

$$f = (t - \alpha_1) \cdot \ldots \cdot (t - \alpha_{p^n}).$$

Wir zeigen zunächst, daß die Menge

$$N = \{\alpha_1, \ldots, \alpha_{p^n}\}$$

der Nullstellen von f ein Teilkörper von $\mathrm{ZFK}_{\mathbb{F}_p}(f)$ ist.

Dazu beachten wir, daß die Nullstellen α von f durch die Bedingung

$$\eta_p^n(\alpha) = \alpha^{p^n} = \alpha$$

charakterisiert sind, daß sie also unter n-facher Anwendung des Frobeniushomomorphismus η_p invariant bleiben. Da η_p ein Homomorphismus ist gilt dann für zwei Nullstellen α und β von f aber auch

$$\eta_p^n(\alpha \pm \beta) = \eta_p^n(\alpha) \pm \eta_p^n(\beta) = \alpha \pm \beta$$

und

$$\eta_p^n(\alpha \cdot \beta) = \eta_p^n(\alpha) \cdot \eta_p^n(\beta) = \alpha \cdot \beta$$

sowie

$$\eta_p^n(\alpha^{-1}) = \eta_p^n(\alpha)^{-1} = \alpha^{-1},$$

wenn $\alpha \neq 0$. Daraus folgt aber, daß N ein Teilkörper von $\mathrm{ZFK}_{\mathbb{F}_p}(f)$ ist, wenn wir noch beachten, daß 0 und 1 offensichtlich Nullstellen von f sind.

Der Teilkörper N von $\mathrm{ZFK}_{\mathbb{F}_p}(f)$ muß den Primkörper $\mathbb{F}_p$ von $\mathrm{ZFK}_{\mathbb{F}_p}(f)$ enthalten und er enthält die Nullstellen von f, also gilt

$$\mathrm{ZFK}_{\mathbb{F}_p}(f) = \mathbb{F}_p(\alpha_1, \ldots, \alpha_{p^n}) \subseteq N \subseteq \mathrm{ZFK}_{\mathbb{F}_p}(f)$$

und damit die Gleichheit der Mengen.

Um zu sehen, daß $\mathrm{ZFK}_{\mathbb{F}_p}(f) = N$ genau p^n Elemente hat, reicht es also, zu zeigen, daß die p^n Nullstellen von f paarweise verschieden sind, daß f also keine mehrfache Nullstelle hat. Dazu betrachten wir die formale Ableitung

$$f' = p \cdot t^{p^n - 1} - 1 = -1 \in \mathbb{F}_p[t].$$

Als konstantes Polynom hat f' keine Nullstelle und somit hat f keine mehrfache Nullstelle. □

Korollar 6.10 (Eindeutigkeit des Körpers mit p^n Elementen.)
Je zwei Körper mit p^n Elementen sind isomorph zueinander.

Beweis: Sei K ein Körper mit p^n Elementen.

Wir werden zeigen zunächst, daß K ein Zerfällungskörper von $f = t^{p^n} - t$ über dem Primkörper $P \cong \mathbb{F}_p$ von K ist.

Ist K ein Körper mit p^n Elementen, so hat die multiplikative Gruppe $(K^*, \cdot)$ von K genau $p^n - 1$ Elemente. Aus dem Satz von Lagrange folgern wir also

$$a^{p^n-1} = 1$$

für alle $a \in K^* = K \setminus \{0\}$ und somit

$$a^{p^n} = a$$

für alle Elemente $a \in K$, da offenbar auch auch $0^{p^n} = 0$ gilt. Mithin sind alle Elemente von K Nullstellen von f, und da f als Polynom vom Grad p^n höchstens p^n Nullstellen haben kann, sind die p^n Elemente von K also genau die Nullstellen von f. Damit zerfällt f über K in Linearfaktoren und K entsteht offenbar aus P durch Adjunktion der Nullstellen

$$P(K) = K.$$

Also ist K ein Zerfällungskörper von f.

Da der Zerfällungskörper von f über $P \cong \mathbb{F}_p$ wegen Korollar 5.14 bis auf Isomorphie eindeutig bestimmt ist, ist K isomorph zu dem Körper in Satz 6.9. □

Bemerkung 6.11
Den bis auf Isomorphie eindeutig bestimmten endlichen Körper mit p^n Elementen bezeichnen wir mit $\mathrm{GF}(p^n)$, dabei steht GF für *Galois field*. In Korollar 11.1 werden wir die Galoisgruppe von $\mathrm{GF}(p^n)$ bestimmen und wir werden sehen, für welche m der endliche Körper $\mathrm{GF}(p^m)$ als Teilkörper von $\mathrm{GF}(p^n)$ gefunden werden kann.

§ 7 Normale Körpererweiterungen

Hat ein Polynom $f \in K[t]$ vom Grad zwei eine Nullstelle α in einem Erweiterungskörper L von K, so zerfällt es dort schon in Linearfaktoren, da sich $t - \alpha$ mittels Polynomdivision abspalten läßt. Für Polynome von höherem Grad gilt dies nicht mehr notwendigerweise. Wir wollen nun Körpererweiterungen L/K betrachten, die diese Eigenschaft für alle irreduziblen Polynome in $K[t]$ haben.

Definition 7.1 (Normale Körpererweiterungen)
Es sei L/K ein Körpererweiterung.

a. L/K heißt *normal*, wenn jedes irreduzible Polynom $f \in K[t]$ mit einer Nullstelle in L über L schon in Linearfaktoren zerfällt.

b. Ein Körperisomorphismus $\sigma : L \longrightarrow L$ mit $\sigma_{|K} = \mathrm{id}_K$ heißt ein K-*Automorphismus* von L, und die Menge

$$\mathrm{Gal}\,(L/K) := \{\sigma : L \to L \mid \sigma \text{ ist ein Körperisomorphismus mit } \sigma_{|K} = \mathrm{id}_K\}$$

heißt die *Galoisgruppe* oder die *Automorphismengruppe* der Körpererweiterung L/K. Sie ist ein Untergruppe von $(\mathrm{Aut}(L), \circ)$.

Beispiel 7.2
Da $\mathbb{C}$ algebraisch abgeschlossen ist (siehe Fundamentalsatz der Algebra 12.34), ist die Körpererweiterung $\mathbb{C}/\mathbb{R}$ normal. Sie besitzt nur zwei Automorphismen, d. h. es gibt nur zwei Körperautomorphismen von $\mathbb{C}$ die $\mathbb{R}$ fest lassen, die Identität $\mathrm{id}_{\mathbb{C}}$ und die komplexe Konjugation $\bar{\cdot}$. Es gilt also

$$\mathrm{Gal}\,(\mathbb{C}/\mathbb{R}) = \{\mathrm{id}_{\mathbb{C}}, \bar{\cdot}\}.$$

Um dies zu sehen, betrachten wir einen beliebigen $\mathbb{R}$-Automorphismus σ von $\mathbb{C}$. Dann gilt

$$\sigma(i)^2 = \sigma(i^2) = \sigma(-1) = -1.$$

Mithin muß $\sigma(i) \in \{i, -i\}$ gelten und somit

$$\sigma(a + ib) = \sigma(a) + \sigma(i) \cdot \sigma(b) = a \pm ib.$$

Wir wollen nun endliche normale Körpererweiterungen charakterisieren und setzen sie in Zusammenhang mit den in Abschnitt 5 eingeführten Zerfällungskörpern.

Satz 7.3 (Charakterisierung normaler Körpererweiterungen)
Für eine endliche Körpererweiterung L/K *sind die folgenden Aussagen äquivalent:*

a. L/K *ist normal.*

b. Ist M/L *eine Körpererweiterung, so gilt* $\psi(L) \subseteq L$ *für alle* $\psi \in \mathrm{Gal}\,(M/K)$.

c. Ist M/L *eine Körpererweiterung, so gilt* $\psi(L) = L$ *für alle* $\psi \in \mathrm{Gal}\,(M/K)$.

d. L *ist der Zerfällungskörper eines Polynoms* $f \in K[t]$.

Beweis:

d. $\Longrightarrow$ c.: Ist $L = \mathrm{ZFK}_K(f)$ mit $f = \sum_{k=0}^{n} a_k t^k \in K[t]$ vom Grad $n = \deg(f)$, so ist

$$L = K(\alpha_1, \ldots, \alpha_n),$$

wenn $\alpha_1, \ldots, \alpha_n \in L$ die Nullstellen von f sind. Für $\sigma \in \mathrm{Gal}\,(M/K)$ ist dann aber $\sigma(L)$ ein Zerfällungskörper von

$$\sigma(f) = \sum_{k=0}^{n} \sigma(a_k) t^k = \sum_{k=0}^{n} a_k t^k = f,$$

weil

$$\sigma(L) = K\big(\sigma(\alpha_1), \ldots, \sigma(\alpha_n)\big)$$

und

$$\sigma(f) = \mathrm{lc}(f) \cdot \big(t - \sigma(\alpha_1)\big) \cdot \ldots \big(t - \sigma(\alpha_n)\big).$$

Aus Korollar 5.14 folgt dann, daß σ die Nullstellen von f nur permutiert hat, daß also

$$\sigma(L) = K\big(\sigma(\alpha_1), \ldots, \sigma(\alpha_n)\big) = K(\alpha_1, \ldots, \alpha_n) = L.$$

c. $\Longrightarrow$ b.: Klar.

b. $\Longrightarrow$ a.: Es sei $g \in K[t]$ irreduzibel mit einer Nullstelle $\alpha \in L$. Nach Voraussetzung ist L/K eine endliche Körpererweiterung, so daß wir L schreiben können also

$$L = K(\alpha_1, \ldots, \alpha_n) = K(\alpha, \alpha_1, \ldots, \alpha_n)$$

für geeignete $\alpha_1, \ldots, \alpha_n \in L$ nach Proposition 3.20. Aus der gleichen Proposition erhalten wir, daß die α_i algebraisch über K sind und wir können ihr Minimalpolynom $\mu_{\alpha_i} \in K[t]$ betrachten. Dann ist

$$f = g \cdot \mu_{\alpha_1} \cdot \ldots \cdot \mu_{\alpha_n} \in K[t]$$

ein Polynom in $K[t]$, daß α und die α_i als Nullstellen hat. Der Zerfällungskörper

$$M = \mathrm{ZFK}_K(f)$$

von f über K enthält dann L als Teilkörper und g zerfällt über M in Linearfaktoren.

Sei nun $\beta \in M$ eine beliebige Nullstelle von g, so gibt es nach Korollar 5.6 einen K-Isomorphismus

$$\phi : K(\alpha) \longrightarrow K(\beta).$$

Als Zerfällungskörper von f über K ist M auch der Zerfällungskörper von f über jedem Zwischenkörper von M/K, also insbesondere von f über $K(\alpha)$ und über $K(\beta)$. Wegen Proposition 5.13 läßt sich ϕ dann zu einem Isomorphismus

$$\sigma : M \longrightarrow M$$

fortsetzen und σ ist damit insbesondere ein K-Automorphismus von M. Nach Voraussetzung gilt dann

$$\beta = \sigma(\alpha) \in \sigma(L) \subseteq L.$$

Also enthält L alle Nullstellen von g und somit zerfällt g über L.

a. $\Longrightarrow$ d.: Wie im letzten Schritt haben wir

$$L = K(\alpha_1, \ldots, \alpha_n)$$

für geeignete $\alpha_i \in L$, die algebraisch über K sind (siehe Proposition 3.20). Die irreduziblen Faktoren μ_{α_i} des Polynoms

$$f = \mu_{\alpha_1} \cdot \ldots \cdot \mu_{\alpha_n} \in K[t]$$

haben in L jeweils mindestens eine Nullstelle und zerfallen wegen a. somit vollständig über L. Damit ist

$$L = \mathrm{ZFK}_K(f)$$

der Zerfällungskörper von f über K. □

Korollar 7.4
Ist L/K *endlich und normal und* N *ein Zwischenkörper von* L/K*, so ist* L/N *normal.*

Beweis: Es gibt ein Polynom $f \in K[t]$ mit

$$L = \mathrm{ZFK}_K(f) = K(\alpha_1, \ldots, \alpha_n)$$

und $f = (t - \alpha_1) \cdot \ldots \cdot (t - \alpha_n)$. Aber dann gilt auch

$$L = N(\alpha_1, \ldots, \alpha_n) = \mathrm{ZFK}_N(f),$$

und somit ist L/N nach Satz 7.3 normal. □

§ 8 Separable Körpererweiterungen

A) Separable Polynome

Definition 8.1 (Separable Polynome)
Ein Polynom $f \in K[t]$ heißt *separabel* über K, wenn seine irreduziblen Faktoren in $K[t]$ keine mehrfachen Nullstellen in $ZFK_K(f)$ haben.

Beispiel 8.2

a. Das Polynom $f = t^2 - 2 = \left(t - \sqrt{2}\right) \cdot \left(t + \sqrt{2}\right) \in \mathbb{Q}[t]$ ist separabel über $\mathbb{Q}$.

b. Das Polynom $f = t^2 - 2t + 1 = (t-1)^2 \in \mathbb{Q}[t]$ ist separabel über $\mathbb{Q}$, weil sein einziger irreduzibler Faktor $t - 1$ keine mehrfache Nullstelle hat.

Proposition 8.3 (Kriterium für Separabilität)
Ein irreduzibles Polynom $f \in K[t]$ *ist genau dann separabel über* K*, wenn* $f' \neq 0$

Beweis: Sei zunächst f separabel und $\alpha \in ZFK_K(f)$ eine Nullstelle von f. Da f irreduzibel ist, ist α keine mehrfache Nullstelle von f und somit ist $f'(\alpha) \neq 0$ nach Lemma 6.8, was $f' \neq 0$ impliziert.

Setzen wir umgekehrt voraus, daß f nicht separabel ist, dann besitzt f eine mehrfache Nullstelle α. Da f irreduzibel ist, unterscheidet sich f vom Minimalpolynom von α über K nur um einen konstanten Faktor und ist somit von minimalem Grad unter den Nicht-Null-Polynomen mit α als Nullstelle. Aus Lemma 6.8 folgt, daß α eine Nullstelle von f' ist, und wegen $\deg(f') < \deg(f)$ muß $f' = 0$ gelten. □

Beispiel 8.4
Das Polynom $f = t^p - x \in \mathbb{F}_p(x)[t]$ über dem Körper $\mathbb{F}_p(x)$ der rationalen Funktionen über $\mathbb{F}_p$ ist nach dem Kriterium von Eisenstein 2.2 irreduzibel über $\mathbb{F}_p[x][t]$ und nach Satz 2.4 somit auch irreduzibel über $\mathbb{F}_p(x)$. Für die Ableitung von f gilt

$$f' = p \cdot t^{p-1} = 0,$$

so daß f wegen Proposition 8.3 *nicht* separabel über $\mathbb{F}_p(x)$ ist.

Man kann dies auch unmittelbar aus der Definition sehen. Der Zerfällungskörper von f ist sein Stammkörper

$$\mathbb{F}_p(x)[t]/\langle t^p - x\rangle \cong \mathbb{F}_p\left(\sqrt[p]{x}\right)$$

und über diesem zerfällt f als

$$f = t^p - x = \left(t - \sqrt[p]{x}\right)^p,$$

so daß f eine p-fache Nullstelle hat.

Korollar 8.5 (Körper der Charakteristik 0 sind vollkommen.)
Ist K *ein Körper der Charakteristik* 0*, so ist jedes Polynom in* $K[t]$ *separabel über* K.

Beweis: Ist $f \in K[t]$ ein irreduzibles Polynom, so ist $\deg(f) \geq 1$ und damit $\deg(f') \geq 0$, so daß $f' \neq 0$ gilt. Die Behauptung folgt also aus Proposition 8.3. □

B) Separable Körpererweiterungen

Definition 8.6 (Separable Körpererweiterungen)
Es sei L/K eine Körpererweiterung und $\alpha \in L$ algebraisch über K.

a. α heißt *separabel* über K, wenn das Minimalpolynom μ_α über K separabel ist.

b. L/K heißt *separabel*, wenn jedes Element aus L separabel über K ist.

Beispiel 8.7

a. In Charakteristik 0 ist jede Körpererweiterung separabel, z.B. $\mathbb{C}/\mathbb{R}$.

b. Die Körpererweiterung $\mathbb{F}_p(\sqrt[p]{x})/\mathbb{F}_p(x)$ für $p \in \mathbb{P}$ ist nicht separabel.

Lemma 8.8
Es sei L/K *eine endliche Körpererweiterung und* M/L *sei eine Körpererweiterung. Dann gibt es höchstens* $|L : K|$ *Körpermonomorphismen* $\varphi : L \hookrightarrow M$ *mit* $\varphi_{|K} = \mathrm{id}_K$.

Beweis: Da L/K endlich ist, gilt $L = K(\alpha_1, \ldots, \alpha_n)$ für geeignete $\alpha_1, \ldots, \alpha_n \in L$, die algebraisch über K sind. Wir setzen

$$K_i := K(\alpha_1, \ldots, \alpha_i)$$

und erhalten so eine Kette von Zwischenkörpern von L/K

$$K := K_0 \leq K_1 \leq K_2 \leq \ldots \leq K_n = L.$$

Sei nun $\mu_{\alpha_i} = \sum_{j=0}^{n} a_j t^j \in K_{i-1}[t]$ das Minimalpolynom von α_i über dem Körper K_{i-1}, so gilt

$$\varphi(\mu_{\alpha_i})\big(\varphi(\alpha_i)\big) = \sum_{j=0}^{n} \varphi(a_j) \cdot \varphi(\alpha_i)^j = \varphi\left(\sum_{j=0}^{n} a_j \cdot \alpha_i^j\right) = \varphi\big(\mu_{\alpha_i}(\alpha_i)\big) = \varphi(0) = 0,$$

d.h. φ bildet α_i auf eine Nullstelle von $\varphi(\mu_{\alpha_i})$ in M ab. Für α_i gibt es also höchstens

$$\deg\big(\varphi(\mu_{\alpha_i})\big) = \deg(\mu_{\alpha_i})$$

Möglichkeiten für $\varphi(\alpha_i)$.

Wegen $L = K(\alpha_1, \ldots, \alpha_n)$ ist φ durch die Bilder der α_i festgelegt, so daß es höchstens

$$\deg(\mu_{\alpha_1}) \cdot \ldots \cdot \deg(\mu_{\alpha_n}) = |K_1 : K_0| \cdot |K_2 : K_1| \cdot \ldots \cdot |K_n : K_{n-1}| \overset{3.22}{=} |K_n : K_0| = |L : K|$$

Möglichkeiten für einen solchen Monomorphismus φ. □

Satz 8.9 (Kriterien für Separabilität)
Für eine endliche Körpererweiterung L/K *sind die folgenden Aussagen gleichwertig:*

a. L/K *ist separabel.*

b. $L = K(\alpha_1, \ldots, \alpha_n)$ *für über* K *separable Elemente* $\alpha_1, \ldots, \alpha_n \in L$.

c. Es gibt eine Körpererweiterung M/L *mit genau* $|L : K|$ *Körpermonomorphismen* $\varphi : L \longrightarrow M$ *mit* $\varphi_{|K} = \mathrm{id}_K$.

Insbesondere, ist $f \in K[t]$ *separabel über* K*, so ist* $\mathrm{ZFK}_K(f)/K$ *separabel.*

Beweis:

a. $\Longrightarrow$ b.: Als endliche Körpererweiterung ist $L = K(\alpha_1, \ldots, \alpha_n)$ für geeignete $\alpha_1, \ldots, \alpha_n \in L$, die nach Voraussetzung dann separabel über K sind, weil L/K separabel ist.

b. $\Longrightarrow$ c.: Um den Körper M zu wählen, schauen wir noch mal in den Beweis von Lemma 8.8 und wählen

$$M = \mathrm{ZFK}_L(f) = \mathrm{ZFK}_L(\mu_{\alpha_1} \cdot \ldots \mu_{\alpha_n})$$

als Zerfällungskörper des Polynoms

$$f = \mu_{\alpha_1} \cdot \ldots \mu_{\alpha_n} \in L[t].$$

Dann zerfällt jedes der Polynome μ_{α_i} über M vollständig.

Setzen wir nun voraus, daß die α_i separabel über K sind, so hat das Minimalpolynom μ_{α_i} von α_i über K_{i-1} als Teiler des Minimalpolynoms von α_i über K keine mehrfache Nullstelle und hat mithin genau $\deg(\mu_{\alpha_i})$ Nullstellen. Mithilfe von Proposition 5.5 können wir dann Monomorphismen $\varphi : L \longrightarrow M$ ausgehend von

$$\varphi_0 = \mathrm{id}_K : K_0 = K \hookrightarrow M$$

sukzessive konstruieren, wobei wir bei der Fortsetzung im i-ten Schritt von

$$\varphi_{i-1} : K_{i-1} \hookrightarrow M$$

nach

$$\varphi_i : K_i = K_{i-1}(\alpha_i) \hookrightarrow M$$

genau $\deg(\mu_{\alpha_i}) = |K_i : K_{i-1}|$ Möglichkeiten haben. Auf diese Weise konstruieren wir

$$|L : K| = |K_1 : K_0| \cdot |K_2 : K_1| \cdot \ldots \cdot |K_n : K_{n-1}|$$

verschiedene Monomorphismen $\varphi : L \longrightarrow M$ mit $\varphi_{|K} = \mathrm{id}_K$, und wegen Lemma 8.8 gibt es auch nicht mehr.

c. $\Longrightarrow$ a.: Angenommen, es gibt ein $\alpha_1 \in L$, das nicht separabel über K ist. Dann ist $\alpha_1 \notin K$ und das Minimalpolynom μ_{α_1} von α_1 über K hat eine mehrfache Nullstelle. Wir können L nun als

$$L = K(\alpha_1, \ldots, \alpha_n)$$

schreiben. Im Beweis von Lemma 8.8 gibt es dann im ersten Schritt echt weniger als

$$\deg(\mu_{\alpha_1}) = |K_1 : K|$$

Möglichkeiten für den Monomorphismus φ, so daß wir insgesamt im Widerspruch zur Voraussetzung echt weniger als $|L : K|$ Monomorphismen erhalten. □

Beispiel 8.10 (Endliche Körper sind separabel über ihrem Primkörper.)
Das Polynom $f = t^{p^n} - t \in \mathbb{F}_p$ hat in seinem Zerfällungskörper

$$\mathrm{GF}(p^n) = \mathrm{ZFK}_{\mathbb{F}_p}(f)$$

genau p^n paarweise verschiedene Nullstellen, nämlich die p^n Elemente von $\mathrm{GF}(p^n)$. Mithin ist f separabel über $\mathbb{F}_p$ und somit ist auch $\mathrm{GF}(p^n)/\mathbb{F}_p$ separabel.

Endliche Körper sind also separabel über ihrem Primkörper und damit auch über jedem Zwischenkörper.

Korollar 8.11 (Endliche Körper sind vollkommen.)
Ist K *ein endlicher Körper und* $f \in K[t]$*, so ist* f *separabel über* K*.*

Beweis: Der Zerfällungskörper von f ist ein endlicher Körper und ist wegen Beispiel 8.10 dann auch separabel über K. Die irreduziblen Faktoren von f sind aber die Minimalpolynome über K der Nullstellen von f und haben deshalb keine mehrfachen Nullstellen, so daß f separabel über K ist. □

C) Der Satz vom primitiven Element

Wir geben hier einen ersten Beweis des Satzes vom primitiven Element, der ohne den Hauptsatz der Galoistheorie auskommt und Auskunft darüber gibt, wie das primitive Element gewählt werden kann. Wir geben im Unterabschnitt 11 B) aber noch einen zweiten Beweis des Satzes.

Satz 8.12 (Der Satz vom primitiven Element)
Sei $L = K(\alpha_1, \ldots, \alpha_n)$ *endlich über* K *und seien* $\alpha_2, \ldots, \alpha_n$ *separabel über* K*, dann gibt es ein* $\alpha \in L$ *mit* $L = K(\alpha)$ *und* L/K *ist einfach.*

Beweis: Wir betrachten zunächst den Fall, daß K ein endlicher Körper ist. Da L als K-Vektorraum isomorph zu $K^{|L:K|}$ ist, ist dann auch L endlich. Aus dem Satz von Lambert-Euler-Gauß (siehe [**Mar08b**, Satz 6.7]) folgt deshalb, daß die multiplikative Gruppe

$$L^* = \langle \alpha \rangle$$

zyklisch ist, d.h. jedes Nicht-Null-Element von L ist eine Potenz von α. Insbesondere ist dann

$$L = K[\alpha] = K(\alpha).$$

Sei nun K ein unendlicher Körper. Wir können ohne Einschränkung annehmen, daß die Anzahl der Erzeuger minimal mit der Eigenschaft gewählt wurde, daß die letzten $n-1$ separabel über K sind, und wollen zeigen, daß dann $n = 1$ gilt.

Nehmen wir $n \geq 2$ an, so können wir für $0 \neq a \in K$ die Zahl

$$\beta_a := \alpha_1 + a \cdot \alpha_2 \in L$$

und den Körper

$$K_a := K(\alpha_1 + a \cdot \alpha_2) = K(\beta_a)$$

betrachten. Da L/K endlich ist, sind α_1 und α_2 algebraisch über K und wir können ihre Minimalpolynome μ_{α_1} und μ_{α_2} über K betrachten. Für das Polynom

$$h := \mu_{\alpha_1}(\beta_a - a \cdot t) \in K(\beta_a)[t]$$

gilt dann

$$h(\alpha_2) = \mu_{\alpha_1}(\alpha_1) = 0$$

und α_2 ist eine gemeinsame Nullstelle von μ_{α_2} und h.

Wir zeigen nun, daß für alle bis auf endlich viele $a \in K$ die beiden Polynome keine weitere gemeinsame Nullstelle in $M = \mathrm{ZFK}_K(\mu_{\alpha_1} \cdot \mu_{\alpha_2} \cdot h)$ haben. Sind

$$\alpha_1, \beta_1, \ldots, \beta_k \in M$$

die paarweise verschiedenen Nullstellen von μ_{α_1} und

$$\alpha_2, \gamma_1, \ldots, \gamma_l \in M$$

die paarweise verschiedenen Nullstellen von μ_{α_2} und ist

$$a \notin \left\{ \frac{\beta_j - \alpha_1}{\alpha_2 - \gamma_i} \;\middle|\; i = 1, \ldots, l, j = 1, \ldots, k \right\},$$

so gilt

$$a \cdot (\alpha_2 - \gamma_i) \neq \beta_j - \alpha_1$$

und

$$\beta_a - a \cdot \gamma_i = \alpha_1 + a \cdot (\alpha_2 - \gamma_i) \neq \alpha_1 + \beta_j - \alpha_1 = \beta_j$$

für alle i, j. Also ist keine der weiteren Nullstellen $\gamma_1, \ldots, \gamma_l$ von μ_{α_2} eine Nullstelle von h.

Da K unendlich ist, können wir ein solches $a \in K$ wählen. Dann hat aber der normierte größte gemeinsame Teiler $d \in K(\beta_a)[t]$ von μ_{α_2} und h über $K(\beta_a)$ in M nur die Nullstelle α_2 und ist von der Form

$$d = (t - \alpha_2)^m$$

für ein geeignetes m. Da μ_{α_2} separabel über K ist, hat es keine mehrfachen Nullstellen, und mithin gilt $m = 1$, so daß

$$t - \alpha_2 = d \in K(\beta_a)[t]$$

gilt. Insbesondere ist dann

$$\alpha_2 \in K(\beta_a)$$

und damit auch

$$\alpha_1 = \beta_a - a \cdot \alpha_2 \in K(\beta_a).$$

Damit folgt unmittelbar

$$K(\alpha_1, \alpha_2) \subseteq K(\beta_a) = K(\alpha_1 + a \cdot \alpha_2) \subseteq K(\alpha_1, \alpha_2)$$

und deshalben

$$L = K(\alpha_1, \ldots, \alpha_n) = K(\beta_a, \alpha_3, \ldots, \alpha_n)$$

im Widerspruch zur Minimalität des Erzeugendensystems. □

Bemerkung 8.13
Der Beweis des Satzes vom primitiven Element 8.12 liefert mehr als nur die Existenz eines primitiven Elementes.

Wenn der Körper K *unendlich* viele Elemente hat, dann erhalten wir, daß *fast jede* K*-Linearkombination*

$$\alpha = \lambda_1 \cdot \alpha_1 + \ldots \lambda_n \cdot \alpha_n$$

der Erzeuger von $L = K(\alpha_1, \ldots, \alpha_n)$ ein primitives Element sein wird. Dabei meint *fast jede*, daß die auszuschließende Menge der $(\lambda_1, \ldots, \lambda_n)^t \in K^n$ von Dimension kleiner n ist. Wählt man die λ_i zufällig, so trifft man mit Wahrscheinlichkeit 1 ein zulässiges Tupel.

Ist der Körper K *endlich*, so reduziert sich die Suche nach einem primitiven Element auf die Suche nach einem Erzeuger der Einheitengruppe von L. Das ist i.a. jedoch ein schwieriges Problem (siehe [**Mar08b**, Bem. 6.8]), so daß sich primitive Elemente über endlichen Körpern nicht so leicht bestimmen lassen wie über unendlichen. Will man endliche Körper effizient in Computern repräsentieren, dann benötigt man diese jedoch. Mehr dazu kann man in der Vorlesung Einführung in das symbolische Rechnen erfahren.

Beispiel 8.14
Schauen wir uns den Zerfällungskörper

$$L = \mathrm{ZFK}_{\mathbb{Q}}(f) = \mathbb{Q}[\alpha_1, \alpha_2, \alpha_3, \alpha_4] = \mathbb{Q}[\alpha_1, \alpha_2]$$

mit

$$\alpha_1 = \sqrt[4]{2}, \quad \alpha_2 = i \cdot \sqrt[4]{2}, \quad \alpha_3 = -\sqrt[4]{2}, \quad \alpha_4 = -i \cdot \sqrt[4]{2}$$

des irreduziblen Polynoms

$$f = t^4 - 2 \in \mathbb{Q}[t]$$

an. Dann ist

$$\alpha = \alpha_1 + a \cdot \alpha_2 = \sqrt[4]{2} + a \cdot i \cdot \sqrt[4]{2}$$

ein primitives Element von L sobald

$$\begin{aligned} a \notin & \left(\mathbb{Q} \cap \left\{ \frac{\alpha_j - \alpha_1}{\alpha_2 - \alpha_i} \;\middle|\; j = 2,3,4, i = 1,3,4 \right\} \right) \cup \{0\} \\ &= \mathbb{Q} \cap \left\{ \frac{2}{1-i}, \frac{2}{-1-i}, \frac{2}{-2i}, \frac{1-i}{1-i}, \frac{1-i}{-1-i}, \frac{1-i}{-2i}, \frac{1+i}{1-i}, \frac{1+i}{-1-i}, \frac{1+i}{-2i}, 0 \right\} \\ &= \{-1, 0, 1\}. \end{aligned}$$

Aufgabe 8.15
Es sei K ein Körper mit $\mathrm{char}(K) = p > 0$ und $f \in K[t]$ irreduzibel.
Zeige, f ist genau dann nicht separabel, wenn es ein $g \in K[t]$ gibt mit $f = g(t^p)$.

Aufgabe 8.16

Es sei L/K eine Körpererweiterung mit $\mathrm{char}(K) = p > 0$ und $\alpha \in L$.
Zeige, daß die folgenden Aussagen gleichwertig sind:

a. α ist separabel über K.

b. $K(\alpha)/K(\alpha^p)$ ist separabel.

c. $K(\alpha) = K(\alpha^p)$.

§ 9 Galoissche Körpererweiterungen

A) K-Automorphismen als Permutationen der Nullstellen

Proposition 9.1 (K-Automorphismen als Permutationen der Nullstellen)
Sei L/K *eine Körpererweiterung,* $f \in K[t]$ *und* $\sigma \in \mathrm{Gal}(L/K)$.

a. *Für* $\alpha \in L$ *gilt*
$$f\big(\sigma(\alpha)\big) = \sigma\big(f(\alpha)\big).$$

b. *Ist* $Z_L(f) = \{\alpha \in L \mid f(\alpha) = 0\}$ *die Menge der Nullstellen von* f *in* L*, so ist*
$$\sigma_| : Z_L(f) \xrightarrow{1:1} Z_L(f) : \alpha \mapsto \sigma(\alpha)$$
eine Permutation der Nullstellen von f.

c. *Ist* $L = \mathrm{ZFK}_K(f)$ *mit* $f = (t-\alpha_1)\cdot\ldots\cdot(t-\alpha_n)$*, so ist die Abbildung*
$$\mathrm{Gal}(L/K) \hookrightarrow \mathrm{Sym}(\{\alpha_1,\ldots,\alpha_n\}) : \sigma \mapsto \sigma_|$$
ein Gruppenmonomorphismus. Insbesondere können wir $\mathrm{Gal}(L/K)$ *also als Untergruppe der symmetrischen Gruppe* $\mathbb{S}_m$ *mit* $m = |\{\alpha_1,\ldots,\alpha_n\}|$ *auffassen.*

d. *Ist* $L = K(\alpha)$ *und ist* α *algebraisch über* K*, so ist die Abbildung*
$$\mathrm{Gal}(L/K) \longrightarrow Z_L(\mu_\alpha) = \{\alpha' \in L \mid \mu_\alpha(\alpha') = 0\} : \sigma \mapsto \sigma(\alpha)$$
eine Bijektion.

Beweis:

a. Ist $f = \sum_{i=0}^{n} a_i t^i$, so gilt
$$\begin{aligned} f\big(\sigma(\alpha)\big) &= \sum_{i=0}^{n} a_i \sigma(\alpha)^i = \sum_{i=0}^{n} \sigma(a_i)\sigma(\alpha)^i \\ &= \sum_{i=0}^{n} \sigma(a_i\alpha^i) = \sigma\left(\sum_{i=0}^{n} a_i\alpha^i\right) = \sigma\big(f(\alpha)\big), \end{aligned}$$
wegen $\sigma(a_i) = a_i$.

b. Aus a. folgt mit $f(\alpha) = 0$ auch $f(\sigma(\alpha)) = 0$ und damit
$$\sigma(Z) \subseteq Z.$$
Da die Menge Z endlich ist und σ injektiv ist, muß σ eingeschränkt auf Z dann eine Bijektion sein.

c. Nach Teil b. ist $\sigma_|$ eine Permutation der Nullstellenmenge $Z_L(f) = \{\alpha_1,\ldots,\alpha_n\}$, also ein Element von $\mathrm{Sym}(\{\alpha_1,\ldots,\alpha_n\})$. Da σ wegen $L = K(\alpha_1,\ldots,\alpha_n)$ durch die Werte von $\alpha_1,\ldots,\alpha_n$ eindeutig bestimmt ist, ist die Abbildung injektiv, und da die Operation auf beiden Seiten die Komposition ist, ist sie auch ein Gruppenhomomorphismus. Man beachte noch, daß
$$\mathrm{Sym}(\{\alpha_1,\ldots,\alpha_n\}) \cong \mathbb{S}_m$$

gilt für $m = |\{\alpha_1, \ldots, \alpha_n\}|$.

d. Wegen b. liegt das Bild der Abbildung in $Z_L(\mu_\alpha)$, und wegen der Eindeutigkeit des Stammkörpers, Korollar 5.6, gibt es zu jeder Nullstelle α' von μ_α in L auch genau einen K-Automorphismus σ von $L = K(\alpha) = K(\alpha')$ mit $\sigma(\alpha) = \alpha'$. Dies liefert die Surjektivität und die Injektivität der Abbildung.

□

Beispiel 9.2

a. Das Polynom

$$\mu_{\sqrt[3]{2}} = t^3 - 2 = \left(t - \sqrt[3]{2}\right) \cdot \left(t - \sqrt[3]{2} \cdot e^{\frac{2\pi i}{3}}\right) \cdot \left(t - \sqrt[3]{2} \cdot e^{\frac{4\pi i}{3}}\right) \in \mathbb{Q}[t]$$

hat im Körper $\mathbb{Q}\left(\sqrt[3]{2}\right)$ nur die Nullstelle $\sqrt[3]{2}$. Aus Proposition 9.1 folgt dann, daß die Identität der einzige $\mathbb{Q}$-Automorphismus von $\mathbb{Q}\left(\sqrt[3]{2}\right)$ ist. Damit gilt dann

$$\left| \operatorname{Gal}\left(\mathbb{Q}\left(\sqrt[3]{2}\right)/\mathbb{Q}\right) \right| = 1 < 3 = \left|\mathbb{Q}\left(\sqrt[3]{2}\right) : \mathbb{Q}\right|.$$

b. Die Körpererweiterung $\mathbb{C}/\mathbb{R}$ hat den Grad $|\mathbb{C} : \mathbb{R}| = 2$ und es gibt genau zwei $\mathbb{R}$-Automorphismen von $\mathbb{C}$, d.h.

$$|\operatorname{Gal}(\mathbb{C}/\mathbb{R})| = 2 = |\mathbb{C} : \mathbb{R}|.$$

c. Das Polynom

$$f = (t^2 - 2) \cdot (t^2 - 3) \in \mathbb{Q}[t]$$

hat den Zerfällungskörper

$$L = \mathrm{ZFK}_{\mathbb{Q}}(f) = \mathbb{Q}\left[\sqrt{2}, -\sqrt{2}, \sqrt{3}, -\sqrt{3}\right] = \mathbb{Q}\left[\sqrt{2}, \sqrt{3}\right].$$

Wegen Proposition 9.1 muß ein $\mathbb{Q}$-Automorphismus von L die Nullstellen des irreduziblen Polynoms $t^2 - 2$ permutieren und die des irreduziblen Polynoms $t^2 - 3$. Beschreiben wir die $\mathbb{Q}$-Automorphismen von L als Permutationen der Menge

$$Z_L(f) = \left\{\sqrt{2}, -\sqrt{2}, \sqrt{3}, -\sqrt{3}\right\},$$

so kommen die folgenden vier Permutationen in Frage:

σ	$\sigma(\sqrt{2})$	$\sigma(\sqrt{-2})$	$\sigma(\sqrt{3})$	$\sigma(\sqrt{-3})$
id_L	$\sqrt{2}$	$-\sqrt{2}$	$\sqrt{3}$	$-\sqrt{3}$
σ_1	$-\sqrt{2}$	$\sqrt{2}$	$\sqrt{3}$	$-\sqrt{3}$
σ_2	$\sqrt{2}$	$-\sqrt{2}$	$-\sqrt{3}$	$\sqrt{3}$
$\sigma_1 \circ \sigma_2$	$-\sqrt{2}$	$\sqrt{2}$	$-\sqrt{3}$	$\sqrt{3}$

Um zu sehen, daß σ_1 von einem $\mathbb{Q}$-Automorphismus von L durch Einschränkung herkommt, beachten wir, daß L aus $\mathbb{Q}$ durch doppelte Stammkörperbildung entsteht:

$$\mathbb{Q} \leq \mathbb{Q}\left[\sqrt{2}\right] \leq \mathbb{Q}\left[\sqrt{2}\right]\left[\sqrt{3}\right].$$

Wenden wir den Fortsetzungssatz 5.5 für die erste Erweiterung an, so erhalten wir einen $\mathbb{Q}$-Isomorphismus von $\mathbb{Q}[\sqrt{2}]$, der $\sqrt{2}$ auf $-\sqrt{2}$ abbildet. Wenden wir denselben Satz anschließend auf die zweite Erweiterung an, so können wir den eben gewonnenen $\mathbb{Q}$-Automorphismus zu einem $\mathbb{Q}$-Automorphismus von L fortsetzen, der $\sqrt{3}$ festhält. Wir haben damit σ_1 also $\mathbb{Q}$-Automorphismus von L realisiert.

Analog zeigt man, daß σ_2 ein Element der Galoisgruppe festlegt, und damit dann auch die Komposition $\sigma_1 \circ \sigma_2$. Wir haben damit gezeigt, daß

$$\mathrm{Gal}\left(\mathbb{Q}[\sqrt{2},\sqrt{3}]/\mathbb{Q}\right) \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \cong \mathbb{K}_4 \leq \mathbb{S}_4$$

isomorph zur Kleinschen Vierergruppe, einer Untergruppe der $\mathbb{S}_4$ ist. Insbesondere gilt

$$\left|\mathrm{Gal}\left(\mathbb{Q}[\sqrt{2},\sqrt{3}]/\mathbb{Q}\right)\right| = 4 = \left|\mathbb{Q}[\sqrt{2},\sqrt{3}] : \mathbb{Q}\right|.$$

Satz 9.3 zeigt, daß in der Zusammenhang zwischen der Ordnung der Galoisgruppe und dem Grad der Körpererweiterung nicht zufällig ist.

Satz 9.3 (Ordnung der Galoisgruppe)
Ist L/K *eine endliche Körpererweiterung, so gilt*

$$|\,\mathrm{Gal}\,(L/K)\,| \leq |L : K|,$$

d.h. der Grad der Körpererweiterung beschränkt die Ordnung der Galoisgruppe.

Beweis: Wenden wir Lemma 8.8 mit $M = L$ an, so erhalten wir, daß es höchstens $|L : K|$ Körpermonomorphismen $\varphi : L \hookrightarrow L$ mit $\varphi_{|K} = \mathrm{id}_K$ gibt. Da jeder K-Isomorphismus von L ein solcher ist, folgt die Behauptung. □

B) Galoissche Körpererweiterungen

Körpererweiterungen, bei denen in Satz 9.3 die Gleichheit der beiden Zahlen gilt, haben besonders gute Eigenschaften und erhalten deshalb in der folgenden Definition einen eigenen Namen.

Definition 9.4 (Galoissche Körpererweiterungen)
Eine endliche Körpererweiterung L/K heißt *galoissch*, wenn $|\,\mathrm{Gal}\,(L/K)\,| = |L : K|$.

Beispiel 9.5
Aus Beispiel 9.2 folgt, daß die Körpererweiterungen $\mathbb{C}/\mathbb{R}$ und $\mathbb{Q}[\sqrt{2},\sqrt{3}]/\mathbb{Q}$ galoissch sind und daß $\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q}$ nicht galoissch ist.

Satz 9.6 (Kriterien für die Eigenschaft galoissch)
Für eine endliche Körpererweiterung L/K *sind die folgenden Aussagen gleichwertig:*

a. L/K *ist galoissch.*

b. L/K *ist normal und separabel.*

c. L *ist der Zerfällungskörper eines über* K *separablen Polynoms* $f \in K[t]$.

Beweis:

a. $\Longrightarrow$ b.: Ist L/K galoissch, so ist $|\operatorname{Gal}(L/K)| = |L : K|$, so daß es mindestens $|L : K|$ Monomorphismen $\varphi : L \hookrightarrow L$ mit $\varphi_{|K} = \mathrm{id}_K$ gibt. Wenden wir Lemma 8.8 mit $M = L$ an, so sehen wir, daß es genau $|L : K|$ solche Monomorphismen gibt. Aus Satz 8.9 folgt dann, daß L/K separabel ist.

Um zu zeigen, daß L/K auch normal ist, betrachten wir eine beliebige Körpererweiterung M/L und einen beliebigen K-Automorphismus ψ von M. Dieser induziert einen Körpermonomorphismus

$$\psi_{|L} : L \hookrightarrow M$$

mit $\psi_{|K} = \mathrm{id}_K$. Nach Lemma 8.8 gibt höchstens $|L : K|$ solcher Monomorphismen, aber jeder der $|L : K| = |\operatorname{Gal}(L/K)|$ K-Automorphismen von L ist ein solcher K-Monomorphismus. Also muß $\psi_{|L}$ einer der K-Automorphismen von L sein. Insbesondere gilt also $\psi(L) = L$, und aus Satz 7.3 folgt dann, daß L/K normal ist.

b. $\Longrightarrow$ c.: Ist L/K normal, so ist L der Zerfällungskörper eines Polynoms $f \in K[t]$. Da L/K separabel ist und L alle Nullstellen von f enthält, ist auch f über K separabel, denn die irreduziblen Faktoren von f sind die Minimalpolynome über K der Nullstellen von f und haben somit keine mehrfachen Nullstellen.

c. $\Longrightarrow$ a.: Nach Voraussetzung ist

$$L = \mathrm{ZFK}_K(f) = K(\alpha_1, \ldots, \alpha_n)$$

mit

$$f = (t - \alpha_1) \cdot \ldots \cdot (t - \alpha_n) \in K[t]$$

separabel über K. Nach Satz 8.9 ist dann L/K separabel und es gibt eine Körpererweiterung M/L mit genau $|L : K|$ Körpermonomorphismen

$$\varphi : L \hookrightarrow M$$

und $\varphi_{|K} = \mathrm{id}_K$. Wie in Proposition 9.1 sieht man, daß φ die Nullstellen von f permutiert, so daß

$$\varphi(L) = \varphi\big(K(\alpha_1, \ldots, \alpha_n)\big) = K(\alpha_1, \ldots, \alpha_n) = L$$

folgt, d.h. $\varphi \in \operatorname{Gal}(L/K)$ ist ein K-Automorphismus von L. Damit gilt dann

$$|\operatorname{Gal}(L/K)| = |L : K|$$

und L/K ist galoissch. □

Wir geben hier noch einen zweiten Beweis des Satzes 7.3, der den Satz vom primitiven Element verwendet.

Alternativer Beweis von 9.6: Wenn L/K separabel ist, dann gibt es nach dem Satz vom primitiven Element 8.12 ein notwendigerweise über K separables Element $\alpha \in L$ mit $L = K(\alpha)$.

a. $\Longrightarrow$ c.: Ist L/K galoissch, so ist $|\operatorname{Gal}(L/K)| = |L : K|$, so daß es mindestens $|L : K|$ Monomorphismen $\varphi : L \hookrightarrow L$ mit $\varphi_{|K} = \mathrm{id}_K$ gibt. Wenden wir Lemma 8.8 mit $M = L$ an, so sehen wir, daß es genau $|L : K|$ solche Monomorphismen gibt. Aus Satz 8.9 folgt dann, daß L/K separabel ist, und somit ist $L = K(\alpha)$ für ein separables $\alpha \in L$.

Nach Proposition 9.1 ist dann

$$\deg(\mu_\alpha) = |\operatorname{Gal}(K(\alpha)/K)| \overset{9.1}{=} |Z_L(\mu_\alpha)| \leq \deg(\mu_\alpha),$$

und mithin müssen die Nullstellen von f alle in $L = K(\alpha)$ liegen, so daß $L = \mathrm{ZFK}_K(\mu_\alpha)$ der Zerfällungskörper eines separablen Polynoms ist.

c. $\Longrightarrow$ b.: Nach Satz 8.9 ist L als Zerfällungskörper eines separabelen Polynoms separabel über K und als Zerfällungskörper ist es normal.

b. $\Longrightarrow$ a.: Da L/K separabel ist, ist $L = K(\alpha)$ für ein separables $\alpha \in L$. Da L/K normal ist, zerfällt μ_α nach Satz 7.3 über L in Linearfaktoren, weil es eine Nullstelle α in L hat. Diese sind paarweise verschieden, weil μ_α separabel ist. Dann gilt aber mit Proposition 9.1

$$|\operatorname{Gal}(K(\alpha)/K)| \overset{9.1}{=} |Z_L(\mu_\alpha)| = \deg(\mu_\alpha) = |K(\alpha) : K|,$$

so daß $L = K(\alpha)$ galoisch über K ist. □

Korollar 9.7
Ist L/K *galoissch und* N *ein Zwischenkörper von* L/K*, so ist* L/N *galoissch.*

Beweis: Ist L galoissch, so ist $L = \mathrm{ZFK}_K(f) = K(\alpha_1, \ldots, \alpha_n)$ nach Satz 9.6 der Zerfällungskörper eines über K separablen Polynoms

$$f = (t - \alpha_1) \cdot \ldots \cdot (t - \alpha_n) \in K[t].$$

Aber dann ist f auch separabel über N und es gilt

$$L = N(\alpha_1, \ldots, \alpha_n) = \mathrm{ZFK}_N(f)$$

ist der Zerfällungskörper von f über N. Also ist L/N nach Satz 9.6 galoissch. □

Beispiel 9.8
Das irreduzible Polynom

$$f = t^3 - 2 \in \mathbb{Q}[t]$$

aus Beispiel 9.2 hat die Nullstellen

$$\sqrt[3]{2},\ \sqrt[3]{2} \cdot e^{\frac{2\pi i}{3}},\ \sqrt[3]{2} \cdot e^{\frac{4\pi i}{3}} \in \mathbb{C}.$$

Der Zerfällungskörper ist

$$L = \mathrm{ZFK}_{\mathbb{Q}}(f) = \mathbb{Q}\Big[\sqrt[3]{2},\ \sqrt[3]{2} \cdot e^{\frac{2\pi i}{3}},\ \sqrt[3]{2} \cdot e^{\frac{4\pi i}{3}}\Big] = \mathbb{Q}\big[\sqrt[3]{2}, e^{\frac{2\pi i}{3}}\big],$$

und die Körpererweiterung $L/\mathbb{Q}$ hat die Zwischenkörper $\mathbb{Q}\big[\sqrt[3]{2}\big]$ und $\mathbb{Q}[e^{\frac{2\pi i}{3}}]$ vom Grad

$$\big|\mathbb{Q}\big[\sqrt[3]{2}\big] : \mathbb{Q}\big| = 3$$

sowie

$$|\mathbb{Q}[e^{\frac{2\pi i}{3}}] : \mathbb{Q}| = \deg(t^2 + t + 1) = 2.$$

Da beide ein Teiler vom Grad $|L : K|$ sind, ist dieser mindestens 6, aber aus Aufgabe 5.16 wissen wir auch, daß $6 = 3! = \deg(f)!$ eine obere Schranke für den Grad von L über K ist, woraus

$$|L : \mathbb{Q}| = 6$$

folgt. Als Zerfällungskörper des separablen Polynoms f ist L aber galoissch über $\mathbb{Q}$, so daß auch

$$|\operatorname{Gal}(L/\mathbb{Q})| = |L : \mathbb{Q}| = 6$$

gelten muß. Aus Proposition 9.1 wissen wir, daß $\operatorname{Gal}(L/\mathbb{Q})$ isomorph zu einer Untergruppe der $\mathbb{S}_3$ ist, und diese nur sechs Elemente enthält, folgt

$$\operatorname{Gal}(L/\mathbb{Q}) \cong \mathbb{S}_3.$$

Aufgabe 9.9

Es sei L/K eine galoissche Körpererweiterung und es gebe ein $\alpha \in L$, so daß $\sigma(\alpha) \neq \alpha$ für alle $\mathrm{id}_L \neq \sigma \in \operatorname{Gal}(L/K)$. Zeige, dann ist $L = K(\alpha)$.

§ 10 Hauptsatz der Galoistheorie

Ziel dieses Abschnittes ist es, den Zusammenhang zwischen der Struktur einer endlichen Körpererweiterung L/K und ihrer Galoisgruppe $\mathrm{Gal}(L/K)$ zu untersuchen. Wir werden sehen, daß im Falle einer galoisschen Körpererweiterung eine Dualität zwischen beiden besteht (siehe Hauptsatz der Galoistheorie 10.7).

A) Fixkörper und die Galoiskorrespondenz

Definition und Bemerkung 10.1
Sei L/K eine Körpererweiterung.

a. Ist $U \leq \mathrm{Aut}(L)$ eine Untergruppe der Automorphismengruppe von L, so heißt

$$\mathrm{Fix}(L,U) := \{\alpha \in L \mid \sigma(\alpha) = \alpha \ \forall\ \sigma \in U\}$$

der *Fixkörper* von U in L und ist ein Teilkörper von L, da für $\alpha, \beta \in \mathrm{Fix}(L,U)$

$$\sigma(\alpha \pm \beta) = \sigma(\alpha) \pm \sigma(\beta) = \alpha \pm \beta$$

und

$$\sigma(\alpha \cdot \beta) = \sigma(\alpha) \cdot \sigma(\beta) = \alpha \cdot \beta$$

gilt.

b. Ist N ein Zwischenkörper der Körpererweiterung L/K eine Körpererweiterung, dann ist jeder N-Automorphismus von L offenbar auch ein K-Automorphismus von L, so daß $\mathrm{Gal}(L/N)$ eine Untergruppe von $\mathrm{Gal}(L/K)$ ist,

$$\mathrm{Gal}(L/N) \leq \mathrm{Gal}(L/K)\,.$$

c. Bezeichnen wir mit

$$\mathcal{U}(L/K) := \{U \mid U \leq \mathrm{Gal}(L/K)\}$$

die Menge der Untergruppen der Galoisgruppe von L/K und mit

$$\mathcal{Z}(L/K) := \{N \mid K \leq N \leq L\}$$

die Menge der Zwischenkörper von L/K, so erhalten wir die Abbildungen

$$\mathrm{Gal} : \mathcal{Z}(L/K) \longrightarrow \mathcal{U}(L/K) : N \mapsto \mathrm{Gal}(L/N)$$

und

$$\mathrm{Fix} : \mathcal{U}(L/K) \longrightarrow \mathcal{Z}(L/K) : U \mapsto \mathrm{Fix}(L,U)\,.$$

Diese sind offenbar inklusionsumkehrend, d.h.

$$U \leq V \leq \mathrm{Gal}(L/K) \quad\Longrightarrow\quad \mathrm{Fix}(L,V) \leq \mathrm{Fix}(L,U)$$

und

$$K \leq N \leq M \leq L \quad\Longrightarrow\quad \mathrm{Gal}(L/M) \leq \mathrm{Gal}(L/N)\,.$$

Wir wollen im weiteren Verlauf u.a. zeigen, daß unter guten Voraussetzungen an L/K, die beiden Abbildungen invers zueinander sind.

Beispiel 10.2

Betrachten wir noch einmal Beispiel 9.2 c., d.h.

$$L = \mathrm{ZFK}_{\mathbb{Q}}\left((t^2-2)\cdot(t^2-3)\right) = \mathbb{Q}\big[\sqrt{2},\sqrt{3}\big]$$

mit

$$\mathrm{Gal}\,(L/\mathbb{Q}) = \{\mathrm{id}_L, \sigma_1, \sigma_2, \sigma_1\circ\sigma_2\} \cong \mathbb{Z}_2\times\mathbb{Z}_2$$

und

σ	$\sigma(\sqrt{2})$	$\sigma(\sqrt{-2})$	$\sigma(\sqrt{3})$	$\sigma(\sqrt{-3})$
id_L	$\sqrt{2}$	$-\sqrt{2}$	$\sqrt{3}$	$-\sqrt{3}$
σ_1	$-\sqrt{2}$	$\sqrt{2}$	$\sqrt{3}$	$-\sqrt{3}$
σ_2	$\sqrt{2}$	$-\sqrt{2}$	$-\sqrt{3}$	$\sqrt{3}$
$\sigma_1\circ\sigma_2$	$-\sqrt{2}$	$\sqrt{2}$	$-\sqrt{3}$	$\sqrt{3}$

Die Untergruppe

$$U = \langle\sigma_1\rangle = \{\mathrm{id}_L, \sigma_1\} \leq \mathrm{Gal}\,(L/\mathbb{Q})$$

der Galoisgruppe hat den Fixkörper

$$\mathrm{Fix}\,(L,U) = \mathbb{Q}\big[\sqrt{3}\big].$$

Umgekehrt ist auch

$$\mathrm{Gal}\left(L/\mathbb{Q}\big[\sqrt{3}\big]\right) = U$$

die Galoisgruppe der Körpererweiterung $L/\mathbb{Q}\big[\sqrt{3}\big]$, da die Identität und σ_1 die einzigen Elemente von $\mathrm{Gal}\,(L/\mathbb{Q})$ sind, die den Körper $\mathbb{Q}\big[\sqrt{3}\big]$ invariant lassen.

Hier gilt also

$$\mathrm{Gal}\,(L/\mathrm{Fix}\,(L,U)) = U$$

und

$$\mathrm{Fix}\left(L, \mathrm{Gal}\left(L/\mathbb{Q}\big[\sqrt{3}\big]\right)\right) = \mathbb{Q}\big[\sqrt{3}\big],$$

d.h. die Abbildungen Gal und Fix aus Definition 10.1 kehren ihre Wirkungen auf U und $\mathbb{Q}\big[\sqrt{3}\big]$ um, wie wir uns das wünschen.

B) Der Satz von Artin

In diesem Abschnitt wollen wir den Satz von Artin zeigen, aus dem folgt, daß die Abbildung Gal in Definition 10.1 stets eine Linksinverse zu Fix ist. Das folgende Lemma ist ein wichtiges technisches Hilfsmittel dazu. Es besagt, daß paarweise verschiedene Automorphismen von L im L-Vektorraum aller Selbstabbildungen von L linear unabhängig sind.

Lemma 10.3

Sind $\sigma_1,\ldots,\sigma_n \in \mathrm{Aut}(L)$ *paarweise verschieden, so ist die Familie* $\{\sigma_1,\ldots,\sigma_n\}$ *linear unabhängig im* L*-Vektorraum aller Abbildungen* L *nach* L.

Beweis: Wir führen den Beweis durch Induktion nach n, wobei die Aussage für $n = 1$ offenbar richtig ist, weil σ_1 nicht die Nullabbildung ist.

Sei als $n \geq 2$ und es sei schon bewiesen, daß $n-1$-elementige Teilfamilien von $\mathrm{Aut}(L)$ linear unabhängig sind. Ferner seien $\lambda_1, \ldots, \lambda_n \in L$ gegeben, so daß

$$\lambda_1 \cdot \sigma_1 + \ldots + \lambda_n \cdot \sigma_n = 0 \tag{8}$$

die Nullabbildung ist. Wegen $\sigma_1 \neq \sigma_2$ finden wir ein $\beta \in L$ mit

$$\sigma_1(\beta) \neq \sigma_n(\beta). \tag{9}$$

Setzen wir in Gleichung (8) den Wert $\alpha \cdot \beta$ ein, so erhalten wir

$$\begin{aligned} 0 =& \lambda_1 \cdot \sigma_1(\alpha \cdot \beta) + \ldots + \lambda_n \cdot \sigma_n(\alpha \cdot \beta) \\ =& \lambda_1 \cdot \sigma_1(\alpha) \cdot \sigma_1(\beta) + \ldots + \lambda_n \cdot \sigma_n(\alpha) \cdot \sigma_n(\beta). \end{aligned} \tag{10}$$

für alle $\alpha \in L$. Setzen wir nun Gleichung (8) α ein, multiplizieren die Gleichung mit $\sigma_n(\beta)$ und subtrahieren das Ergebnis von Gleichung (10), so erhalten wir

$$\begin{aligned} 0 &= \sum_{i=1}^{n} \lambda_i \cdot \sigma_i(\alpha) \cdot \sigma_i(\beta) - \sum_{i=1}^{n} \lambda_i \cdot \sigma_i(\alpha) \cdot \sigma_n(\beta) \\ &= \sum_{i=1}^{n-1} \lambda_i \cdot \big(\sigma_i(\beta) - \sigma_n(\beta)\big) \cdot \sigma_i(\alpha) \end{aligned}$$

für alle $\alpha \in L$. Mittels Induktion folgt dann

$$\lambda_i \cdot \big(\sigma_i(\beta) - \sigma_n(\beta)\big) = 0$$

für alle $i = 1, \ldots, n-1$. Für $i = 1$ folgt wegen (9) dann

$$\lambda_1 = 0.$$

Setzen wir dies in Gleichung (8) ein, so erhalten wir

$$\lambda_2 \cdot \sigma_2 + \ldots + \lambda_n \cdot \sigma_n = 0,$$

und mit Induktion gilt deshalb auch

$$\lambda_2 = \ldots = \lambda_n = 0.$$

□

In Beispiel 10.2 haben wir ein Beispiel für die Aussage des folgenden Satzes von Artin gesehen.

Satz 10.4 (Satz von Artin)
Ist $U \leq \mathrm{Aut}(L)$ *eine endliche Untergruppe der Automorphismengruppe von* L*, so gelten*

$$|L : \mathrm{Fix}(L, U)| = |U|$$

und

$$\mathrm{Gal}(L/\mathrm{Fix}(L, U)) = U.$$

Beweis: Da $n := |U| < \infty$ ist, hat U die Form $U = \{\sigma_1, \ldots, \sigma_n\}$ mit paarweise verschiedenen σ_i.

Wir wollen zunächst zeigen, daß $|L : \mathrm{Fix}(L, U)| \geq n$ gilt, und nehmen dazu das Gegenteil an. Dann besitzt L eine $\mathrm{Fix}(L, U)$-Basis

$$B = \{\alpha_1, \ldots, \alpha_m\}$$

mit $m < n$. Die Matrix

$$A = (\sigma_j(\alpha_i))_{\substack{i=1,\ldots,m \\ j=1,\ldots,n}} \in \mathrm{Mat}(m \times n, L)$$

hat also höchstens den Rang m und mithin enthält ihr Kern einen nicht-trivialen Vektor

$$(0, \ldots, 0) \neq (\lambda_1, \ldots, \lambda_n)^t \in \mathrm{Ker}(A).$$

Ist nun $\alpha \in L$ beliebig gegeben, so läßt sich α als Linearkombination

$$\alpha = a_1 \cdot \alpha_1 + \ldots + a_m \cdot \alpha_m$$

mit $a_1, \ldots, a_n \in \mathrm{Fix}(L, U)$ schreiben. Wir erhalten dann

$$\begin{aligned} \sum_{i=1}^{n} \lambda_i \cdot \sigma_i(\alpha) &= \sum_{i=1}^{n} \lambda_i \cdot \sigma_i \left(\sum_{j=1}^{m} a_j \cdot \alpha_j \right) = \sum_{i=1}^{n} \sum_{j=1}^{m} \lambda_i \cdot a_j \cdot \sigma_i(\alpha_j) \\ &= \sum_{j=1}^{m} a_j \cdot \sum_{i=1}^{n} \lambda_i \cdot \sigma_i(\alpha_j) = (a_1, \ldots, a_m) \circ A \circ (\lambda_1, \ldots, \lambda_n)^t = 0 \end{aligned}$$

im Widerspruch zu Lemma 10.3.

Analog wollen wir nun zeigen, daß $|L : \mathrm{Fix}(L, U)| \leq n$ gilt, und nehmen auch dazu das Gegenteil an. Dann gibt es in L eine linear unabhängige Familie

$$B = \{\alpha_1, \ldots, \alpha_m\}$$

mit $m > n$. Die Matrix

$$A = \left(\sigma_i^{-1}(\alpha_j)\right)_{\substack{i=1,\ldots,n \\ j=1,\ldots,m}} \in \mathrm{Mat}(n \times m, L)$$

hat höchstens den Rang n und ihr Kern ist nicht null,

$$\mathrm{Ker}(A) \neq \{(0, \ldots, 0)^t\}.$$

Wir betrachten nun die Abbildung

$$\varphi : L \longrightarrow L : \alpha \mapsto \sigma_1(\alpha) + \ldots + \sigma_n(\alpha).$$

Beachten wir, daß für $i \in \{1, \ldots, n\}$ die Gruppe U sich schreiben läßt als

$$U = \{\sigma_1, \ldots, \sigma_n\} = \{\sigma_i \circ \sigma_1, \ldots, \sigma_i \circ \sigma_n\}, \tag{11}$$

so erhalten wir für $\alpha \in L$ die Gleichung

$$\sigma_i\big(\varphi(\alpha)\big) = \sigma_i \left(\sum_{j=1}^{n} \sigma_j(\alpha) \right) = \sum_{j=1}^{n} \sigma_i \circ \sigma_j(\alpha) \overset{(11)}{=} \sum_{k=1}^{n} \sigma_k(\alpha) = \varphi(\alpha)$$

und damit

$$\varphi(\alpha) \in \mathrm{Fix}\,(L, U)\,.$$

Ist nun

$$(\lambda_1, \ldots, \lambda_m)^t \in \mathrm{Ker}(A) \tag{12}$$

beliebig, so erhalten wir

$$0 = \sum_{i=1}^{n} \sigma_i(0) \overset{(12)}{=} \sum_{i=1}^{n} \sigma_i \left(\sum_{j=1}^{m} \lambda_j \cdot \sigma_i^{-1}(\alpha_j) \right) = \sum_{i=1}^{n} \sum_{j=1}^{m} \sigma_i(\lambda_j) \cdot \alpha_j$$
$$= \sum_{j=1}^{m} \sum_{i=1}^{n} \sigma_i(\lambda_j) \cdot \alpha_j = \sum_{j=1}^{m} \varphi(\lambda_j) \cdot \alpha_j.$$

Da die Familie B linear unabhängig über $\mathrm{Fix}\,(L, U)$ ist, folgt daraus

$$\varphi(\lambda_1) = \ldots = \varphi(\lambda_n) = 0$$

für alle $\nu = (\lambda_1, \ldots, \lambda_n)^t \in \mathrm{Ker}(A)$. Da der Kern von A nicht-trivial ist, gibt es einen solchen Vektor mit einer Komponente $\lambda_k \neq 0$, und da mit ν auch $\lambda \cdot \nu \in \mathrm{Ker}(A)$ für alle $\lambda \in L$ gilt, so folgt unmittelbar

$$\varphi(\lambda \cdot \lambda_k) = 0$$

für alle $\lambda \in L$ und damit

$$\sigma_1(\alpha) + \ldots + \sigma_n(\alpha) = \varphi(\alpha) = 0$$

für alle $\alpha \in L$, da $L = \{\lambda \cdot \lambda_k \mid \lambda \in L\}$. Dies steht aber im Widerspruch zu Lemma 10.3.

Damit haben wir die erste Gleichung gezeigt,

$$|L : \mathrm{Fix}\,(L, U)\,| = n = |U|. \tag{13}$$

Für die zweite Gleichung beachten wir, daß offenbar

$$U \leq \mathrm{Gal}\,(L/\mathrm{Fix}\,(L, U))$$

gilt, da die Automorphismen in U nach Definition des Fixkörpers $\mathrm{Fix}\,(L, U)$ diesen punktweise invariant lassen. Außerdem wissen wir aus Satz 9.3

$$|U| \leq |\,\mathrm{Gal}\,(L/\mathrm{Fix}\,(L, U))\,| \overset{9.3}{\leq} |L : \mathrm{Fix}\,(L, U)\,| \overset{(13)}{=} |U|,$$

woraus die fehlende Gleichheit folgt,

$$U = \mathrm{Gal}\,(L/\mathrm{Fix}\,(L, U))\,.$$

□

Korollar 10.5

Ist L/K *eine endliche Körpererweiterung, so gilt*

$$\mathrm{Gal} \circ \mathrm{Fix} = \mathrm{id}_{\mathcal{U}(L/K)},$$

d.h. für $U \leq \mathrm{Gal}\,(L/K)$ *gilt*

$$\mathrm{Gal}\,(L/\mathrm{Fix}\,(L, U)) = U.$$

Beweis: Dies folgt aus dem Satz von Artin 10.4, da $\mathrm{Gal}\,(L/K)$ nach Satz 9.3 eine endliche Untergruppe von $\mathrm{Aut}(L)$ ist. □

Korollar 10.6 (Kriterium für die Eigenschaft galoissch)
Eine endliche Körpererweiterung L/K *ist genau dann galoissch, wenn*

$$\mathrm{Fix}\,(L, U) = K$$

für eine Untergruppe $U \leq \mathrm{Aut}(L)$ *ist. In diesem Fall ist* $U = \mathrm{Gal}\,(L/K)$.

Beweis: Ist L/K galoissch, so folgt aus dem Satz von Artin

$$|L : \mathrm{Fix}\,(L, \mathrm{Gal}\,(L/K))\,| = |\,\mathrm{Gal}\,(L/K)\,| = |L : K|$$

und mithin $\mathrm{Fix}\,(L, \mathrm{Gal}\,(L/K)) = K$, da K ein Teilkörper von $\mathrm{Fix}\,(L, \mathrm{Gal}\,(L/K))$ ist.

Ist umgekehrt $\mathrm{Fix}\,(L, U) = K$ für $U \leq \mathrm{Aut}(L)$, so folgt zunächst, daß

$$U \subseteq \mathrm{Gal}\,(L/K)\,,$$

weil U den Körper K fest läßt. Mit dem Satz von Artin folgt dann

$$|\,\mathrm{Gal}\,(L/K)\,| \geq |U| = |L : \mathrm{Fix}\,(L, U)\,| = |L : K| \overset{9.3}{\geq} |\,\mathrm{Gal}\,(L/K)\,|$$

und L/K ist galoissch. Außerdem muß aus Ordnungsgründen $U = \mathrm{Gal}\,(L/K)$ gelten. □

C) Der Hauptsatz der Galoistheorie

Satz 10.7 (Hauptsatz der Galoistheorie)
Es sei L/K *eine endliche galoissche Körpererweiterung.*

a. Die Abbildungen Gal *und* Fix *sind bijektiv und invers zueinander, d.h. für* $K \leq N \leq L$ *gilt*

$$\mathrm{Fix}\,(L, \mathrm{Gal}\,(L/N)) = N$$

und für $U \leq \mathrm{Gal}\,(L/K)$ *gilt*

$$\mathrm{Gal}\,(L/\mathrm{Fix}\,(L, U)) = U.$$

Insbesondere besitzt L/K *nur endlich viele Zwischenkörper.*

b. Für alle Zwischenkörper N *von* L/K *gilt*

$$|L : N| = |\,\mathrm{Gal}\,(L/N)\,|$$

und

$$|N : K| = |\,\mathrm{Gal}\,(L/K) : \mathrm{Gal}\,(L/N)\,|.$$

Insbesondere ist L/N *galoissch.*

c. *Für einen Zwischenkörper* N *von* L/K *ist die Erweiterung* N/K *genau dann galoissch, wenn* $\mathrm{Gal}(L/N) \trianglelefteq \mathrm{Gal}(L/K)$ *ein Normalteiler von* $\mathrm{Gal}(L/K)$ *ist. In diesem Fall ist*

$$\mathrm{Gal}(L/K) \,/\, \mathrm{Gal}(L/N) \xrightarrow{\cong} \mathrm{Gal}(N/K) : \overline{\sigma} \mapsto \sigma_{|N}$$

ein Gruppenisomorphismus.

Für den Beweis benötigen wir die folgende Hilfsaussage.

Lemma 10.8 (Konjugation in Galoisgruppen)
Sei N *ein Zwischenkörper der Körpererweiterung* L/K *und* $\sigma \in \mathrm{Gal}(L/K)$. *Dann gilt*

$$\sigma \circ \mathrm{Gal}(L/N) \circ \sigma^{-1} = \mathrm{Gal}(L/\sigma(N)).$$

Beweis: Ist $\varphi \in \mathrm{Gal}(L/N)$ ein N-Automorphismus von L, so ist

$$\sigma \circ \varphi \circ \sigma^{-1} : L \longrightarrow L$$

ein Automorphismus von L und für $\beta = \sigma(\alpha) \in \sigma(N)$ gilt

$$\sigma \circ \varphi \circ \sigma^{-1}(\beta) = \sigma \circ \varphi(\alpha) = \sigma(\alpha) = \beta,$$

so daß $\sigma \circ \varphi \circ \sigma^{-1} \in \mathrm{Gal}(L/\sigma(N))$ folgt.

Ist umgekehrt $\varphi \in \mathrm{Gal}(L/\sigma(N))$ und

$$\psi = \sigma^{-1} \circ \varphi \circ \sigma : L \longrightarrow L,$$

so sieht man wie oben, daß $\psi \in \mathrm{Gal}(L/N)$ gilt, und damit ist

$$\varphi = \sigma \circ \psi \circ \sigma^{-1} \in \sigma \circ \mathrm{Gal}(L/N) \circ \sigma^{-1}.$$

□

Beweis des Hauptsatzes der Galoistheorie 10.7:

a. Aus Korollar 10.5 wissen wir schon, daß

$$\mathrm{Gal} \circ \mathrm{Fix} = \mathrm{id}_{\mathcal{U}(L/K)}$$

gilt, d.h. daß Gal linksinvers zu Fix ist. Es bleibt also

$$\mathrm{Fix}(L, \mathrm{Gal}(L/N)) = N \tag{14}$$

zu zeigen, wobei N ein beliebiger Zwischenkörper von L/K ist. Nach Korollar 9.7 ist L/N galoissch und aus Korollar 10.6 folgt dann (14).

b. Sei N ein Zwischenkörper von L/K. Nach Korollar 9.7 ist L/N galoissch und wir erhalten die erste Gleichung

$$|L : N| = |\,\mathrm{Gal}(L/N)\,|.$$

Für die zweite Gleichung verwenden wir die Gradformel

$$|L : K| = |L : N| \cdot |N : K| \tag{15}$$

sowie den Satz von Lagrange

$$|\operatorname{Gal}(L/K)| = |\operatorname{Gal}(L/N)| \cdot |\operatorname{Gal}(L/K) : \operatorname{Gal}(L/N)| \tag{16}$$

Da L/K und L/N galoissch sind, folgt daraus

$$|N : K| \overset{(15)}{=} \frac{|L : K|}{|L : N|} = \frac{|\operatorname{Gal}(L/K)|}{|\operatorname{Gal}(L/N)|} \overset{(16)}{=} |\operatorname{Gal}(L/K) : \operatorname{Gal}(L/N)|.$$

c. Setzen wir zunächst voraus, daß N/K galoissch ist. Dann ist N/K insbesondere normal nach Satz 9.6. Ist nun $\sigma \in \operatorname{Gal}(L/K)$ gegeben, so gilt

$$\sigma(N) = N$$

wegen Satz 7.3. Aus Lemma 10.8 folgt dann

$$\sigma \circ \operatorname{Gal}(L/N) \circ \sigma^{-1} = \operatorname{Gal}(L/\sigma(N)) = \operatorname{Gal}(L/N).$$

Also ist $\operatorname{Gal}(L/N) \trianglelefteq \operatorname{Gal}(L/K)$ ein Normalteiler.
Sei nun $\operatorname{Gal}(L/N) \trianglelefteq \operatorname{Gal}(L/K)$ vorausgesetzt, dann folgt für $\sigma \in \operatorname{Gal}(L/K)$ mit Lemma 10.8

$$\operatorname{Gal}(L/N) = \sigma \circ \operatorname{Gal}(L/N) \circ \sigma^{-1} = \operatorname{Gal}(L/\sigma(N)).$$

Aus dem Satz von Artin 10.4 leiten wir dann

$$N = \operatorname{Fix}(L, \operatorname{Gal}(L/N)) = \operatorname{Fix}(L, \operatorname{Gal}(L/\sigma(N))) = \sigma(N)$$

ab. Das heißt, jeder K-Automorphismus von L induziert einen K-Automorphismus von N.
Damit ist die Einschränkung

$$\varepsilon : \operatorname{Gal}(L/K) \longrightarrow \operatorname{Gal}(N/K) : \sigma \mapsto \sigma_{|N}$$

wohldefiniert, und wir wollen nun zeigen, daß sie ein Gruppenepimorphismus mit

$$\operatorname{Ker}(\varepsilon) = \operatorname{Gal}(L/N)$$

ist. Wenn uns dies gelingt, so erhalten wir

$$\operatorname{Gal}(L/K) / \operatorname{Gal}(L/N) \cong \operatorname{Gal}(N/K)$$

und damit

$$|\operatorname{Gal}(N/K)| = \frac{|\operatorname{Gal}(L/K)|}{|\operatorname{Gal}(L/N)|} = |\operatorname{Gal}(L/K) : \operatorname{Gal}(L/N)| \overset{\text{b.}}{=} |N : K|,$$

so daß N/K galoissch ist.
Es ist klar, daß ε ein Gruppenhomomorphismus mit dem angegebenen Kern

$$\operatorname{Ker}(\varepsilon) = \{\sigma \in \operatorname{Gal}(L/N) \mid \sigma_{|N} = \mathrm{id}_N\} = \operatorname{Gal}(L/N)$$

ist. Für die Surjektivität beachten wir, daß $\mathrm{Im}(\varepsilon) \leq \mathrm{Gal}(N/K)$ eine Untergruppe von $\mathrm{Gal}(N/K)$ ist, und wir erhalten dann

$$\begin{aligned}\mathrm{Fix}(N, \mathrm{Im}(\varepsilon)) &= \left\{ \alpha \in N \;\middle|\; \sigma(\alpha) = \alpha \; \forall\, \sigma \in \mathrm{Gal}(L/K) \right\} \\ &= N \cap \mathrm{Fix}(L, \mathrm{Gal}(L/K)) \overset{10.6}{=} N \cap K = K.\end{aligned}$$

Aufgrund des Satzes von Artin 10.4 ist dann

$$\mathrm{Gal}(N/K) = \mathrm{Gal}(N/\mathrm{Fix}(N, \mathrm{Im}(\varepsilon))) = \mathrm{Im}(\varepsilon)$$

und ε ist surjektiv.
Aus dem Homomorphiesatz folgt dann auch, daß die Abbildung

$$\mathrm{Gal}(L/K) \,/\, \mathrm{Gal}(L/N) \longrightarrow \mathrm{Gal}(N/K) : \overline{\sigma} \mapsto \sigma_{|N}$$

ein Gruppenisomorphismus ist.

□

Beispiel 10.9
In Beispiel 9.8 haben wir die Galoisgruppe des Zerfällungskörpers

$$L = \mathrm{ZFK}_{\mathbb{Q}}(f) = \mathbb{Q}\big[\sqrt[3]{2}, e^{\frac{2\pi i}{3}}\big]$$

des irreduziblen Polynoms

$$f = t^3 - 2 \in \mathbb{Q}[t]$$

über $\mathbb{Q}$ bestimmt und haben

$$\mathrm{Gal}(L/\mathbb{Q}) \cong \mathbb{S}_3$$

erhalten. Damit gehört also zu jeder Permutation der drei Nullstellen

$$\alpha_1 = \sqrt[3]{2}, \alpha_2 = \sqrt[3]{2} \cdot e^{\frac{2\pi i}{3}}, \alpha_3 = \sqrt[3]{2} \cdot e^{\frac{4\pi i}{3}} \in \mathbb{C}$$

von f genau ein $\mathbb{Q}$-Automorphismus von L:

σ	$\sigma(\alpha_1)$	$\sigma(\alpha_2)$	$\sigma(\alpha_3)$	σ als Element von $\mathbb{S}_3$
id_L	α_1	α_2	α_3	id
σ_{12}	α_2	α_1	α_3	(1 2)
σ_{23}	α_1	α_3	α_2	(2 3)
σ_{13}	α_3	α_2	α_1	(1 3)
σ_{123}	α_2	α_3	α_1	(1 2 3)
σ_{132}	α_3	α_1	α_2	(1 3 2)

Den Untergruppenverband von $\mathbb{S}_3$ kennen wir sehr genau (siehe Abbildung 7). Bei der graphischen Darstellung geben die Striche an, daß die tiefer gelegene Gruppe U eine Untergruppe der höher gelegenen Gruppe V ist, und die Zahlen geben den Index $|V : U|$ an. Ist der Strich ein Pfeil, so bedeutet dies, daß U ein Normalteiler in V ist.

Damit kennen wir auch den Untergruppenverband von $\mathrm{Gal}(L/\mathbb{Q})$ (Abbildung 8). Aufgrund des Hauptsatzes der Galoistheorie entspricht diesem der duale Zwi-

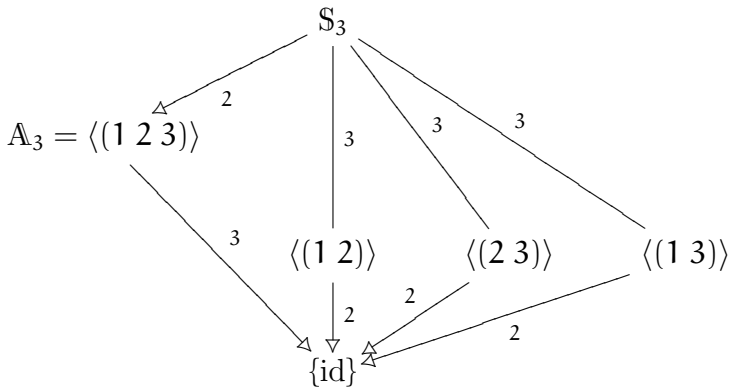

ABBILDUNG 7. Der Untergruppenverband von $\mathbb{S}_3$

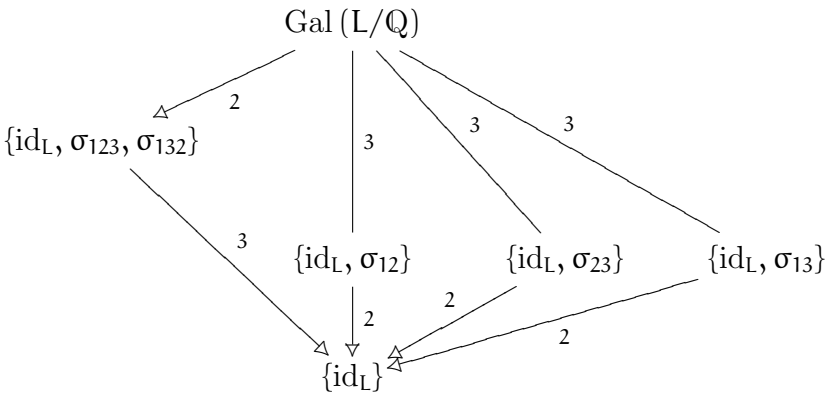

ABBILDUNG 8. Der Untergruppenverband von $\mathrm{Gal}\left(\mathrm{ZFK}_{\mathbb{Q}}(t^3-2)/\mathbb{Q}\right)$

schenkörperverband der Körpererweiterung $L/\mathbb{Q}$ (siehe Abbildung 9). Bei der gra-

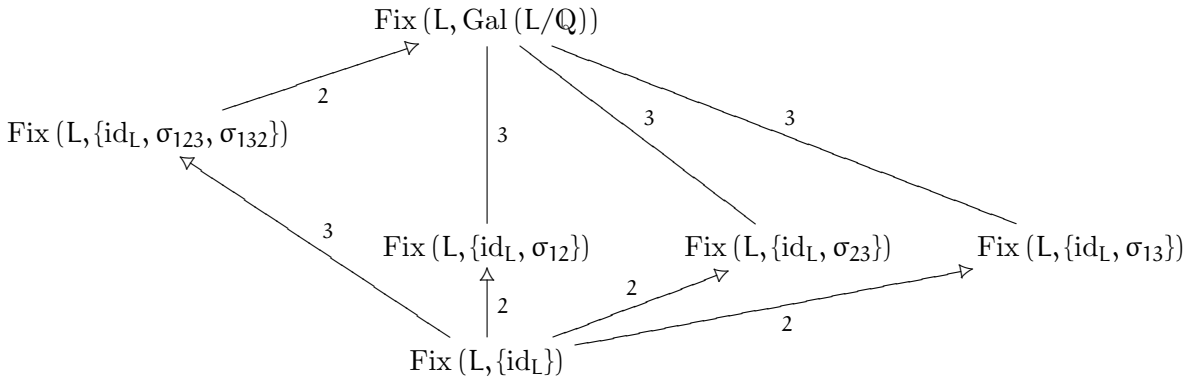

ABBILDUNG 9. Der Untergruppenverband von $\mathrm{Gal}\left(\mathrm{ZFK}_{\mathbb{Q}}(t^3-2)/\mathbb{Q}\right)$

phischen Darstellung bedeutet ein Strich, daß der höher gelegene Körper N ein Teilkörper des tiefer gelegenen Körpers M ist, und die Zahl am Strich gibt den Grad

$|M : N|$ der Körpererweiterung an. Ein Pfeil bedeutet, daß die Körpererweiterung M/N galoissch ist.

Berechnen wir die Fixkörper konkret, so erhalten wir das Diagramm in Abbildung 10. Dabei ist die Gleichung

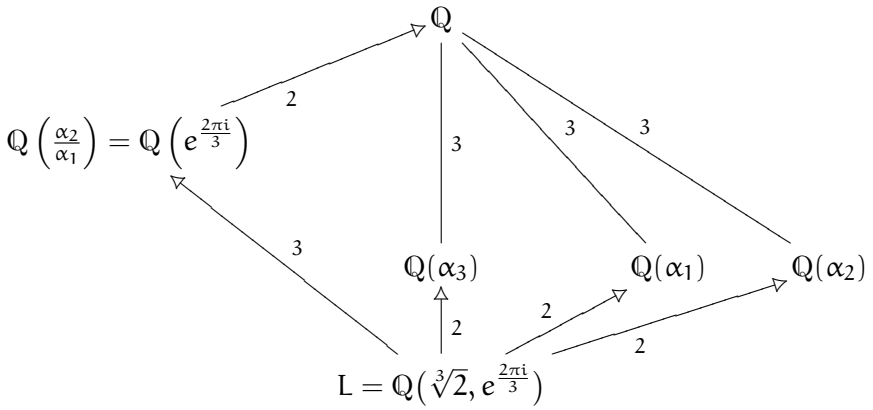

Abbildung 10. Der Untergruppenverband von $\mathrm{Gal}\left(\mathrm{ZFK}_{\mathbb{Q}}(t^3-2)/\mathbb{Q}\right)$

$$\mathrm{Fix}\,(L, \{\mathrm{id}_L, \sigma_{12}\}) = \mathbb{Q}(\alpha_3)$$

offensichtlich, da α_3 von σ_{12} festgelassen wird und $|\mathbb{Q}(\alpha_3) : \mathbb{Q}| = \deg(t^3-2) = 3 = |\mathrm{Fix}\,(L, \{\mathrm{id}_L, \sigma_{12}\}) : \mathbb{Q}|$. Analog sieht man

$$\mathrm{Fix}\,(L, \{\mathrm{id}_L, \sigma_{23}\}) = \mathbb{Q}(\alpha_1)$$

und

$$\mathrm{Fix}\,(L, \{\mathrm{id}_L, \sigma_{13}\}) = \mathbb{Q}(\alpha_2).$$

Um die Gleichung

$$\mathrm{Fix}\,(L, \{\mathrm{id}_L, \sigma_{123}, \sigma_{132}\}) = \mathbb{Q}\left(\frac{\alpha_2}{\alpha_1}\right) = \mathbb{Q}\left(e^{\frac{2\pi i}{3}}\right)$$

zu sehen, betrachten wir

$$\frac{\alpha_2}{\alpha_1} = e^{\frac{2\pi i}{3}}$$

und berechnen

$$\sigma_{123}\left(\frac{\alpha_2}{\alpha_1}\right) = \frac{\alpha_3}{\alpha_2} = e^{\frac{2\pi i}{3}} = \frac{\alpha_2}{\alpha_1}.$$

Also läßt σ_{123} die Zahl invariant und damit auch $\sigma_{123}^{-1} = \sigma_{132}$, so daß $e^{\frac{2\pi i}{3}}$ und damit $\mathbb{Q}\left(e^{\frac{2\pi i}{3}}\right)$ im Fixkörper enthalten sind. Wegen

$$|\mathrm{Fix}\,(L, \{\mathrm{id}_L, \sigma_{123}, \sigma_{132}\}) : \mathbb{Q}| = 2 = \deg(t^2+t+1) = |\mathbb{Q}\left(e^{\frac{2\pi i}{3}}\right) : \mathbb{Q}|$$

folgt dann wieder die Gleichheit. Hierbei haben wir ausgenutzt, daß $g = t^2+t+1$ nach Beispiel 2.11 irreduzibel über $\mathbb{Q}$ und damit das Minimalpolynom von $e^{\frac{2\pi i}{3}}$ über $\mathbb{Q}$ ist.

Aufgaben

Aufgabe 10.10 ($\mathbb{D}_8$ als Galoisgruppe)
Gegeben seien das Polynom $f = t^4 - 10t^2 + 18 \in \mathbb{Q}[t]$ und sein Zerfällungskörper $L = \mathrm{ZFK}_{\mathbb{Q}}(f) \leq \mathbb{C}$.

a. Zeige, daß die Galoisgruppe $\mathrm{Gal}(L/\mathbb{Q})$ isomorph zur Diedergruppe

$$\mathbb{D}_8 = \langle (1\,2\,3\,4), (1\,4)(2\,3) \rangle \leq \mathbb{S}_4$$

der Ordnung 8 ist.

b. Bestimme den Untergruppenverband von $\mathbb{D}_8$ und den Zwischenkörperverband von $\mathrm{Gal}(L/\mathbb{Q})$.

Aufgabe 10.11 (Quaternionengruppe $\mathbb{Q}_8$ als Galoisgruppe)
Sei $K = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$, $\alpha = (2 + \sqrt{2}) \cdot (3 + \sqrt{3}) \in K$ und $L = \mathbb{Q}[\sqrt{\alpha}]$.

a. Zeige, daß α ein primitives Element von K ist.

b. Berechne das Minimalpolynom von α und von $\sqrt{\alpha}$ über $\mathbb{Q}$.

c. Zeige, sind $\sigma_1, \sigma_2 \in \mathrm{Gal}(K/\mathbb{Q})$ wie in Aufgabe 9.2, dann gibt es Zahlen $0 \neq \lambda_1, \lambda_2 \in K$ mit

$$\sigma_i(\alpha) = \lambda_i^2 \cdot \alpha$$

für $i = 1, 2$. Leite daraus ab, daß es für $i = 1, 2$ je einen $\mathbb{Q}$-Automorphismus $\tau_i \in \mathrm{Gal}(L/\mathbb{Q})$ gibt, der auf K mit σ_i übereinstimmt.

d. Zeige, $\tau_1^2 = \tau_2^2 \neq \mathrm{id}_L$, $\tau_1^4 = \mathrm{id}_L$ und $\tau_1 \circ \tau_2 \circ \tau_1^{-1} = \tau_2^{-1}$.

e. Zeige, $\mathrm{Gal}(L/\mathbb{Q}) = \langle \tau_1, \tau_2 \rangle$ hat die Ordnung

$$|\,\mathrm{Gal}(L/\mathbb{Q})\,| = |L : \mathbb{Q}| = 8$$

und $L/\mathbb{Q}$ ist galoissch.

f. Bestimme den Untergruppenverband von $\mathrm{Gal}(L/\mathbb{Q})$ und den Zwischenkörperverband von $L/\mathbb{Q}$.

§ 11 Anwendungen des Hauptsatzes der Galoistheorie

Wir wollen in diesem Abschnitt einige einfache Anwendungen des Hauptsatzes der Galoistheorie zusammenstellen.

A) Die Automorphismengruppen endlicher Körper

In diesem Unterabschnitt bestimmen wir die Struktur der Automorphismengruppe $\mathrm{Aut}(\mathrm{GF}(p^n)) = \mathrm{Gal}\,(\mathrm{GF}(p^n)/\mathbb{F}_p)$ vollständig.

Korollar 11.1 (Die Automorphismengruppe endlicher Körper)
Sei $p \in \mathbb{P}$ *eine Primzahl und seien* $n, m \in \mathbb{Z}_{>0}$ *mit* $m \leq n$.

a. $\mathrm{GF}(p^n)/\mathbb{F}_p$ *ist galoissch und die Galoisgruppe* $\mathrm{Gal}\,(\mathrm{GF}(p^n)/\mathbb{F}_p)$ *ist zyklisch von Ordnung* n *mit dem Frobeniushomomorphismus*

$$\eta_p : \mathrm{GF}(p^n) \longrightarrow \mathrm{GF}(p^n) : \alpha \mapsto \alpha^p$$

als Erzeuger.

b. Ist K *ein Teilkörper von* $\mathrm{GF}(p^n)$*, so ist* $|K| = p^m$ *für einen Teiler* m *von* n.

c. Für jeden Teiler m *von* n *hat* $\mathrm{GF}(p^n)$ *genau einen Teilkörper der Ordnung* p^m.

Genau dann ist $\mathrm{GF}(p^m)$ *ein Teilkörper von* $\mathrm{GF}(p^n)$*, wenn* m *ein Teiler von* n *ist.*

Beweis:

a. Nach Satz 6.9 ist $\mathrm{GF}(p^n)$ der Zerfällungskörper des Polynoms

$$f = t^{p^n} - t \in \mathbb{F}_p[t]$$

und dieses ist nach Beispiel 8.10 separabel über $\mathbb{F}_p$. Also ist $\mathrm{GF}(p^n)/\mathbb{F}_p$ nach Satz 9.6 galoissch und somit gilt

$$|\,\mathrm{Gal}\,(\mathrm{GF}(p^n)/\mathbb{F}_p)\,| = |\,\mathrm{GF}(p^n) : \mathbb{F}_p| = n.$$

Wir wollen nun zeigen, daß der Frobeniushomomorphismus, der wegen Korollar 6.5 ein $\mathbb{F}_p$-Automorphismus von $\mathrm{GF}(p^n)$ ist, die Ordnung n hat, denn dann erzeugt er die Galoisgruppe und diese ist zyklisch. Nehmen wir dazu an, die Ordnung

$$k = \mathrm{ord}(\eta_p) < n$$

sei echt kleiner als n. Dann gilt

$$\alpha = \mathrm{id}_{\mathrm{GF}(p^n)}(\alpha) = \eta_p^k(\alpha) = \alpha^{p^k}$$

für alle $\alpha \in \mathrm{GF}(p^n)$ und das Polynom

$$g = t^{p^k} - t \in \mathbb{F}_p[t]$$

hätte $p^n > p^k = \deg(g)$ Nullstellen in $\mathrm{GF}(p^n)$, was nicht sein kann.

b./c. Dies folgt aus dem Hauptsatz der Galoistheorie 10.7, da eine zyklische Untergruppe der Ordnung n nur für die Teiler von n eine Untergruppe besitzen kann und für jeden Teiler m von n auch genau eine Untergruppe der Ordnung $\frac{n}{m}$ hat (siehe [**Mar08a**, Kor. 4.62]). Deren Fixkörper hat dann die Ordnung p^m.

□

B) Der Satz vom primitiven Element

Wir wollen hier einen zweiten Beweis des Satzes vom primitiven Element geben, der den Hauptsatz der Galoistheorie verwendet.

Lemma 11.2 (Kriterium für Einfachheit)
Hat eine endliche Körpererweiterung L/K *nur endlich viele Zwischenkörper, so ist sie einfach, d.h. es gibt ein* $\alpha \in L$ *mit* $L = K(\alpha) = K[\alpha]$.

Beweis: Wir betrachten zunächst den Fall, daß L ein endlicher Körper ist. Dann folgt aus dem Satz von Lambert-Euler-Gauß (siehe [**Mar08b**, Satz 6.7]), daß die multiplikative Gruppe

$$L^* = \langle \alpha \rangle$$

zyklisch ist, d.h. jedes Nicht-Null-Element von L ist eine Potenz von α. Insbesondere ist dann

$$L = K[\alpha] = K(\alpha).$$

Sei nun $|L| = \infty$, dann muß auch $|K| = \infty$ gelten, da L als K-Vektorraum isomorph zu $K^{|L:K|}$ ist. Da L/K endlich ist, ist L nach Proposition 3.20 von der Form

$$L = K(\alpha_1, \ldots, \alpha_n),$$

wobei wir die Anzahl der Erzeuger $\alpha_1, \ldots, \alpha_n$ minimal wählen können.

Nehmen wir $n \geq 2$ an, so können wir für $a \in K$ den Körper

$$K_a := K(\alpha_1 + a \cdot \alpha_2)$$

betrachten. Da L/K nur endlich viele Zwischenkörper hat, aber K unendlich ist, muß es zwei Element $a, b \in K$ geben mit $a \neq b$ und

$$K_a = K_b.$$

Wir erhalten dann

$$(a - b) \cdot \alpha_2 = (\alpha_1 + a \cdot \alpha_2) - (\alpha_1 + b \cdot \alpha_2) \in K_a = K_b,$$

und wegen $0 \neq a - b \in K \subseteq K_a$ folgt somit

$$\alpha_2 \in K_a.$$

Aber dann gilt auch

$$\alpha_1 = (\alpha_1 + a \cdot \alpha_2) - a \cdot \alpha_2 \in K_a,$$

woraus unmittelbar

$$K(\alpha_1, \alpha_2) \subseteq K_a = K(\alpha_1 + a \cdot \alpha_2) \subseteq K(\alpha_1, \alpha_2)$$

und damit

$$K(\alpha_1, \alpha_2) = K(\alpha_1 + a \cdot \alpha_2)$$

folgt. Aber dann gilt

$$L = K(\alpha_1, \ldots, \alpha_n) = K(\alpha_1 + a \cdot \alpha_2, \alpha_3, \ldots, \alpha_n)$$

im Widerspruch dazu, daß die Anzahl der Erzeuger minimal gewählt war. Also ist $n = 1$ und $L = K(\alpha_1) = K[\alpha_1]$ ist einfach. □

Bemerkung 11.3
Bemerkung 8.13 gilt hier analog.

Satz 11.4 (Der Satz vom primitiven Element)
Genau dann ist L/K *endlich und separabel, wenn* $L = K(\alpha)$ *für ein separables* $\alpha \in L$.

Beweis: Ist $L = K(\alpha_1, \ldots, \alpha_n)$ endlich und separabel über K und ist

$$f = \mu_{\alpha_1} \cdot \ldots \cdot \mu_{\alpha_n} \in K[t],$$

so ist f separabel über K als Produkt separabler Polynome und nach Satz 9.6 ist $ZFK_K(f)/K$ galoissch. Aus dem Hauptsatz der Galoistheorie 10.7 folgt dann, daß $ZFK_K(f)/K$ nur endlich viele Zwischenkörper hat. Aber wegen $L \subseteq ZFK_K(f)$ hat dann auch L/K nur endlich viele Zwischenkörper und $L = K(\alpha)$ ist nach Lemma 11.2 einfach über K. Wegen $\alpha \in L$ ist α zudem separabel über K.

Ist umgekehrt $L = K(\alpha)$ für ein über K separables Element α, so ist L endlich und nach Satz 8.9 auch separabel über K. □

Korollar 11.5 (Satz vom primitiven Element)
Ist L/K *eine endliche Körpererweiterung und ist* K *endlich oder hat* K *die Charakteristik* $\mathrm{char}(K) = 0$*, so ist* L/K *einfach.*

Beweis: Die Aussage folgt aus Satz 8.12, weil L/K dann nach Korollar 8.11 oder nach Korollar 8.5 separabel ist. □

C) Kreisteilungspolynome und Kreisteilungskörper

Wir wollen uns darauf beschränken, Kreisteilungspolynome und -körper über $\mathbb{Q}$ zu betrachten. Einige der Aussagen kann man mit etwas mehr Aufwand auch über beliebigen Körpern zeigen. Für die Ergebnisse der folgenden Bemerkung verweisen wir auf die Vorlesungen Elementare Zahlentheorie (siehe [**Mar08b**, S. 57]) und Algebraische Strukturen (siehe [**Mar08a**, Kor. 4.61,4.62]).

Bemerkung 11.6 (n-te Einheitswurzeln)
Ist $n \in \mathbb{Z}_{>0}$ und $\zeta_n := e^{\frac{2\pi i}{n}}$, so heißen die Elemente in

$$E_n := \{z \in \mathbb{C} \mid z^n = 1\} = \{z \in \mathbb{C}^* \mid o(z) \text{ teilt } n\} = \{\zeta_n^d \mid d = 1, \ldots, n\}$$

die n-*ten Einheitswurzeln* in $\mathbb{C}$. E_n ist eine zyklische Untergruppe der multiplikativen Gruppe $\mathbb{C}^*$ des Körpers $\mathbb{C}$,

$$E_n = \langle \zeta_n \rangle.$$

Die Erzeuger von E_n heißen die primitiven n-ten Einheitswurzeln und es gilt:

$$\zeta_n^d \text{ primitiv} \quad \Longleftrightarrow \quad o(\zeta_n^d) = n \quad \Longleftrightarrow \quad \operatorname{ggt}(d, n) = 1. \tag{17}$$

Man beachte, daß E_n nach Definition genau aus den Nullstellen des Polynoms

$$f = t^n - 1 = (t - \zeta_n) \cdot (t - \zeta_n^2) \cdot \ldots \cdot (t - \zeta_n^n) \in \mathbb{Q}[t]$$

besteht und daß mithin

$$\mathrm{ZFK}_{\mathbb{Q}}\left(t^n - 1\right) = \mathbb{Q}\left(\zeta_n^1, \ldots, \zeta_n^n\right) = \mathbb{Q}\left(\zeta_n\right)$$

gilt.

Definition 11.7 (Das n-te Kreisteilungspolynom über $\mathbb{Q}$)
Das Polynom

$$\phi_n := \prod_{\zeta \in E_n \text{ primitiv}} (t - \zeta) = \prod_{\substack{1 \le d \le n \\ \operatorname{ggt}(d,n)=1}} \left(t - \zeta_n^d\right) = \prod_{\substack{\zeta \in \mathbb{C}^* \\ o(\zeta)=n}} (t - \zeta) \in \mathbb{C}[t]$$

heißt das n-*te Kreisteilungspolynom* über $\mathbb{Q}$.

Beispiel 11.8

a. $\phi_1 = t - 1$.

b. $\phi_2 = t + 1$.

c. $\phi_3 = (t - \zeta_3) \cdot (t - \zeta_3^2) = t^2 - (\zeta_3 + \zeta_3^2) \cdot t + \zeta_3^3 = \frac{t^3 - 1}{t - 1} = t^2 + t + 1$.

d. $\phi_4 = (t - i) \cdot (t + i) = t^2 + 1$.

e. Aus der Definition der Kreisteilungspolynome folgt unmittelbar

$$\prod_{\substack{1 \le d \le n \\ d \mid n}} \phi_d = \prod_{\substack{1 \le d \le n \\ o(\zeta) = d \mid n}} (t - \zeta) = \prod_{k=1}^{n} (t - \zeta_n^k) = t^n - 1,$$

weil $\frac{n}{\operatorname{ggt}(n,k)}$ die Ordnung von ζ_n^k ist und sich somit E_n genau aus den primitiven d-ten Einheitswurzeln der Teiler d von n zusammensetzt.

f. Aus Teil e. folgt

$$\phi_8 = \frac{t^8 - 1}{\phi_1 \cdot \phi_2 \cdot \phi_4} = \frac{t^8 - 1}{(t - 1) \cdot (t + 1) \cdot (t^2 + 1)} = t^4 + 1.$$

Alle betrachteten Beispiele für Kreisteilungspolynome sind in der Tat Polynome in $\mathbb{Z}[t]$. Das ist kein Zufall, wie Satz 11.10 zeigt.

Im Beweis des Hauptergebnisses dieses Unterabschnitts werden wir die folgende einfache Eigenschaft des Polynomrings $\mathbb{Z}[t]$ mehrfach verwenden.

Lemma 11.9
Seien $f, g \in \mathbb{Z}[t]$ *und* $h \in \mathbb{C}[t]$ *normiert mit* $f = g \cdot h$*, so ist* $h \in \mathbb{Z}[t]$.

Beweis: Division mit Rest (siehe [**Mar08a**, Prop. 7.27]) von f durch das normierte Polynom g liefert uns Polynome $q, r \in \mathbb{Z}[t]$ mit

$$f = q \cdot g + r$$

und $\deg(r) < \deg(g)$. Aus $f = g \cdot h$ erhalten wir dann

$$(h - q) \cdot g = r,$$

was wegen der Gradbeschränkung von r nur für $r = 0$ und

$$h = q \in \mathbb{Z}[t]$$

möglich ist. □

Satz 11.10 (Die Galoisgruppe von $\mathbb{Q}(\zeta_n)/\mathbb{Q}$)
Das n*-te Kreisteilungspolynom* ϕ_n *ist ein irreduzibles ganzzahliges Polynom,*

$$\phi_n \in \mathbb{Z}[t],$$

vom Grad

$$\deg(\phi_n) = |\mathbb{Q}(\zeta_n) : \mathbb{Q}| = |\mathbb{Z}_n^*| = \varphi(n),$$

wobei φ *die Eulersche* φ*-Funktion ist, und*

$$\mathbb{Q}(\zeta_n) = \mathrm{ZFK}_{\mathbb{Q}}(\phi_n)$$

ist galoissch über $\mathbb{Q}$ *mit der abelschen Galoisgruppe*

$$\mathrm{Gal}\,(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong \mathbb{Z}_n^*,$$

so daß alle Zwischenkörper von $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ *galoissch über* $\mathbb{Q}$ *sind.*

Wir nennen $\mathbb{Q}(\zeta_n)$ *den* n-ten Kreisteilungskörper *über* $\mathbb{Q}$.

Beweis: Wir wollen zunächst mit Induktion nach n

$$\phi_n \in \mathbb{Z}[t]$$

zeigen. Für $n = 1$ gilt $\phi_n = t - 1 \in \mathbb{Z}[t]$. Für $n > 1$ ist das Polynom

$$g := \prod_{\substack{1 \le d < n \\ d \mid n}} \phi_d \in \mathbb{Z}[t]$$

per Induktion in $\mathbb{Z}[t]$. Aus Beispiel 11.13 folgt aber auch

$$t^n - 1 = \phi_n \cdot g$$

und mit aus Lemma 11.9 folgt dann

$$\phi_n \in \mathbb{Z}[t].$$

Den Beweis der Irreduzibilität lagern wir nach Lemma 11.11 aus, da er recht technisch ist.

Der Grad von ϕ_n ist nach Definition gleich der Anzahl der primitiven n-ten Einheitswurzeln in E_n und dies ist nach (17) gleich der Anzahl der zu n teilerfremden Zahlen zwischen 1 und n und diese liefern genau die Einheiten in $\mathbb{Z}_n$, woraus

$$\deg(\phi_n) = |\mathbb{Z}_n^*| = \varphi(n)$$

folgt (siehe auch [**Mar08a**, Prop. 7.56] und [**Mar08b**, Def. 3.15]).

Als nächstes wollen wir einen Gruppenhomomorphismus

$$\tau : \mathrm{Gal}\,(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \longrightarrow \mathbb{Z}_n^*$$

definieren. Ist $\sigma \in \mathrm{Gal}\,(\mathbb{Q}(\zeta_n)/\mathbb{Q})$, dann gilt

$$\sigma(\zeta_n) = \zeta_n^d$$

für ein $1 \leq d \leq n$, da σ die Nullstellen des Polynoms $t^n - 1$ permutiert. Da $\sigma_{|E_n}$ ein Automorphismus ist (siehe Proposition 9.1), muß $\sigma(\zeta_n)$ wieder ein Erzeuger der Gruppe E_n, also eine primitive n-te Einheitswurzel sein, so daß $\mathrm{ggt}(d, n) = 1$ gilt. Wir setzen nun

$$\tau(\sigma) := \overline{d} \in \mathbb{Z}_n^*.$$

Man beachte, daß der $\mathbb{Q}$-Automorphismus σ von $\mathbb{Q}(\zeta_n)$ durch das Bild von ζ_n eindeutig festgelegt ist, so daß die Abbildung τ injektiv ist. Sind $\sigma, \pi \in \mathrm{Gal}\,(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ mit $\sigma(\zeta_n) = \zeta_n^d$ und $\pi(\zeta_n) = \zeta_n^e$, so gilt

$$\sigma \circ \pi(\zeta_n) = \sigma(\zeta_n^e) = \sigma(\zeta_n)^e = (\zeta_n^d)^e = \zeta_n^{d \cdot e}$$

und damit

$$\tau(\sigma \circ \pi) = \overline{d \cdot e} = \overline{d} \cdot \overline{e} = \tau(\sigma) \cdot \tau(\pi),$$

so daß τ ein Gruppenmonomorphismus ist.

Da $\mathbb{Q}(\zeta_n)$ alle Nullstellen von ϕ_n enthält, ist

$$\mathbb{Q}(\zeta_n) = \mathrm{ZFK}_{\mathbb{Q}}(\phi_n)$$

als Zerfällungskörper des separablen Polynoms $\phi_n \in \mathbb{Q}[t]$ galoissch über $\mathbb{Q}$, und es gilt

$$|\,\mathrm{Gal}\,(\mathbb{Q}(\zeta_n)/\mathbb{Q})\,| = |\mathbb{Q}(\zeta_n) : \mathbb{Q}| = \deg(\phi_n) = |\mathbb{Z}_n^*|,$$

wobei wir verwenden, daß ϕ_n als irreduzibles Polynom das Minimalpolynom von ζ_n über $\mathbb{Q}$ ist. Daraus folgt insbesondere die Surjektivität von τ, so daß τ ein Gruppenisomorphismus ist. □

Lemma 11.11
Das Kreisteilungspolynom $\phi_n \in \mathbb{Z}[t]$ ist irreduzibel *über $\mathbb{Z}$ und über $\mathbb{Q}$, und es ist damit das Minimalpolynom von ζ_n über $\mathbb{Q}$. Insbesondere gilt also*

$$\mathbb{Q}(\zeta_n) \cong \mathbb{Q}[t]/\langle \phi_n \rangle.$$

Beweis: Wegen Satz 2.4 reicht es, zu zeigen, daß f irreduzibel in $\mathbb{Z}[t]$ ist. Da $\mathbb{Z}[t]$ nach dem Lemma von Gauß 1.6 faktoriell ist, können wir die Zerlegung

$$\phi_n = f_1 \cdot \ldots \cdot f_k$$

des normierten Polynoms ϕ_n in normierte irreduzible Faktoren in $\mathbb{Z}[t]$ betrachten.

Wir wollen zeigen, daß einer der irreduziblen Faktoren alle primitiven n-ten Einheitswurzeln als Nullstelle hat, so daß er mit ϕ_n übereinstimmen muß. Dazu reicht es, zu zeigen, daß für jede primitive n-te Einheitswurzel $\zeta \in E_n$ und jede Primzahl $p \in \mathbb{P}$ mit $p \nmid n$ die Zahlen ζ und ζ^p Nullstellen desselben irreduziblen Faktors sind. Denn die primitiven n-ten Einheitswurzeln entstehen aus ζ_n durch Potenzieren mit einer zu n teilerfremden Zahl, d.h. durch sukzessives Potenzieren mit Primzahlen, die keine Teiler von n sind.

Sei also $\zeta \in E_n$ und sei $p \in \mathbb{P}$ mit $p \nmid n$. Die irreduziblen Faktoren von ϕ_n, die ζ bzw. ζ^p als Nullstelle haben, sind auch irreduzibel über $\mathbb{Q}$ und mithin deren Minimalpolynome. Wir bezeichnen sie deshalb mit μ_ζ bzw. μ_{ζ^p}

Wir nehmen

$$\mu_\zeta \neq \mu_{\zeta^p}$$

an. Dann gibt es ein normiertes Polynom $g \in \mathbb{Z}[t]$ mit

$$\phi_n = \mu_\zeta \cdot \mu_{\zeta^p} \cdot g. \tag{18}$$

Betrachten wir das Polynom

$$f = \mu_{\zeta^p}(t^p) \in \mathbb{Z}[t],$$

so gilt

$$f(\zeta) = \mu_{\zeta^p}(\zeta^p) = 0.$$

Also ist μ_ζ als Minimalpolynom von ζ in $\mathbb{Q}[t]$ ein Teiler von f in $\mathbb{Q}[t]$, d.h. es gibt ein $h \in \mathbb{Q}[t]$ mit

$$\mu_{\zeta^p}(t^p) = f = \mu_\zeta \cdot h,$$

und aus Lemma 11.9 gilt dabei sogar

$$h \in \mathbb{Z}[t].$$

Mittels Reduktion mod p (siehe Definition 2.6)

$$\rho_p : \mathbb{Z}[t] \longrightarrow \mathbb{F}_p[t]$$

erhalten wir in $\mathbb{F}_p[t]$ die Gleichung

$$\overline{\mu_\zeta} \cdot \overline{h} = \overline{\mu_{\zeta^p}(t^p)} = \eta_p(\overline{\mu_{\zeta^p}}) = \overline{\mu_{\zeta^p}}^p,$$

da der Frobeniushomomorphismus

$$\eta_p : \mathbb{F}_p(t) \longrightarrow \mathbb{F}_p(t) : a \mapsto a^p$$

auf $\mathbb{F}_p$ die Identität ist (siehe Proposition 6.3). Ist nun d ein irreduzible Faktor von $\overline{\mu_\zeta}$ in $\mathbb{F}_p[t]$ so ist d auch ein Faktor von $\overline{\mu_{\zeta^p}}$ und wir erhalten aus (18)

$$d^2 \,\Big|\, \overline{\mu_\zeta} \cdot \overline{\mu_{\zeta^p}} \cdot \overline{g} = \overline{\phi_n} \mid t^n - 1$$

in $\mathbb{F}_p[t]$. Also hat $t^n - 1$ eine mehrfache Nullstelle in seinem Zerfällungskörper über $\mathbb{F}_p$, was wegen Lemma 6.8 im Widerspruch zu

$$\left(t^n - 1\right)' = n \cdot t^{n-1} \neq 0$$

steht, wenn $p \not| n$. Also gilt $\mu_\zeta = \mu_{\zeta^p}$ und die Aussage des Lemmas ist bewiesen. □

Bemerkung 11.12 (Galoisgruppen von Kreisteilungskörpern)
Ist K ein beliebiger Körper mit $\mathrm{char}(K) = 0$, so ist

$$K(\zeta_n) = \mathrm{ZFK}_K(t^n - 1)$$

galoissch über K und man kann wie im Beweis von Satz 11.10 einen Gruppenmonomorphismus

$$\tau : \mathrm{Gal}\,(K(\zeta_n)/K) \hookrightarrow \mathbb{Z}_n^*$$

definieren. Damit sieht man, daß die Galoisgruppe $\mathrm{Gal}\,(K(\zeta_n)/K)$ abelsch ist.

Beispiel 11.13
Ist $p \in \mathbb{P}$ eine Primzahl, so haben wir in Beispiel 2.11 gesehen, daß das Polynom

$$\frac{t^p - 1}{t - 1} = t^{p-1} + t^{p-2} + \ldots + t + 1 \in \mathbb{Z}[t] \tag{19}$$

in $\mathbb{Z}[t]$ irreduzibel ist. Damit muß

$$\phi_p = t^{p-1} + t^{p-2} + \ldots + t + 1 \tag{20}$$

gelten, da ϕ_p ein Teiler dieses Polynoms in $\mathbb{Z}[t]$ ist. Es gilt also insbesondere

$$|\mathbb{Q}(\zeta_p) : \mathbb{Q}| = \deg(\phi_p) = p - 1.$$

Mit Hilfe des Satzes 11.10 können wir die Gleichung (20) und die Irreduzibilität des Polynoms (19) aber auch anders sehen. Wir wissen ja, daß ϕ_p ein Teiler des Polynoms (19) ist und daß

$$\deg(\phi_p) = |\mathbb{Z}_p^*| = p - 1$$

gilt. Damit erhalten wir die Gleichung (20) und aus Lemma 11.9 dann auch die Irreduzibilität des Polynoms.

Der Satz von Lambert-Euler-Gauß (siehe [**Mar08b**, Satz 6.7]) garantiert uns, daß $\mathbb{Z}_p^*$ eine zyklische Gruppe ist und somit für jeden Teiler der Gruppenordnung genau eine Untergruppe hat (siehe [**Mar08a**, Kor. 4.62]), und die Untergruppe der Ordnung d ist in der der Ordnung e genau dann enthalten, wenn d ein Teiler von e ist. Also hat $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ für jeden Teiler d von $p - 1$ genau einen Zwischenkörper N vom Grad

$$|N : \mathbb{Q}| = \frac{p - 1}{d}$$

und wenn N und M Zwischenkörper mit $|N : \mathbb{Q}| = \frac{p-1}{d}$, $|M : \mathbb{Q}| = \frac{p-1}{e}$ und $d \mid e$ sind, dann ist M ein Teilkörper von N. Man beachte auch, daß $\mathbb{Z}_p^*$ abelsch ist, so daß alle Untergruppen Normalteiler sind.

Für $p = 13$ erhalten wir also das Zwischenkörperdiagramm in Abbildung 11. Um

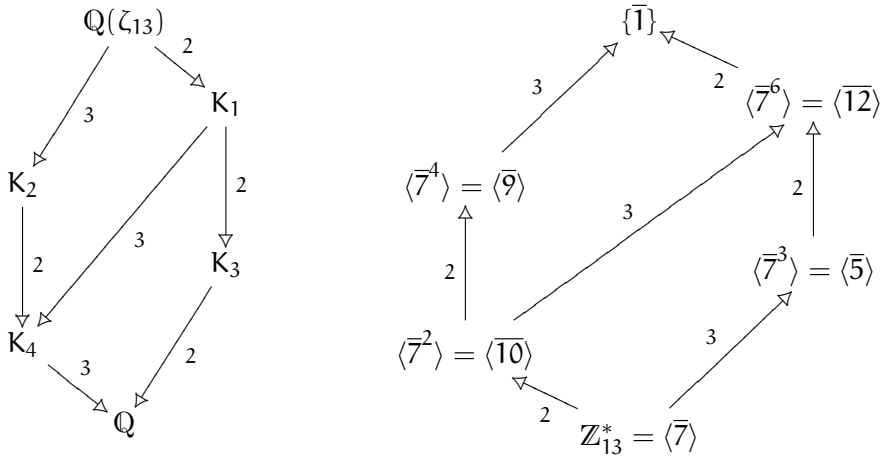

Abbildung 11. Das Zwischenkörperdiagramm von $\mathbb{Q}(\zeta_{13})/\mathbb{Q}$

die Untergruppen von $\mathbb{Z}_{13}^*$ explizit anzugeben, haben wir die Primitivwurzel $\overline{7}$ von $\mathbb{Z}_{13}^*$ verwendet (siehe [**Mar08b**, § 7]).

Bemerkung 11.14 (Verbindung zur Elementaren Zahlentheorie)
In der Vorlesung Elementare Zahlentheorie wird ein ganzer Abschnitt (siehe [**Mar08b**, § 7]) der Untersuchung der Struktur von $\mathbb{Z}_n^*$ gewidmet, insbesondere der Frage, wann diese Gruppe zyklisch ist. In Satz 11.10 haben wir gesehen, daß die Einheitengruppen $\mathbb{Z}_n^*$ als Galoisgruppen der Kreisteilungskörper über $\mathbb{Q}$ auftauchen. Sie spielen also eine wichtige Rolle in der Galoistheorie und ihre Struktur gibt Auskunft über die Struktur und insbesondere den Zwischenkörperverband von $\mathbb{Q}(\zeta_n)/\mathbb{Q}$. Dies erläutert vielleicht das Interesse an der Fragestellung in der Elementaren Zahlentheorie.

D) Konstruierbarkeit des regelmäßigen n-Ecks

Bemerkung 11.15 (Konstruierbarkeit des regelmäßigen n-Ecks)
Kann man zu $n \geq 3$ mit Zirkel und Lineal ein regelmäßiges n-Eck konstruieren? Denken wir uns das n-Eck so in die Ebene eingebettet, daß sein Mittelpunkt bei 0 und eine seiner Ecken bei 1 liegt, so sind die Ecken des regulären n-Ecks genau die n-ten Einheitswurzeln

$$E_n = \left\{ e^{\frac{2\pi i k}{n}} \;\middle|\; k = 0, \ldots, n-1 \right\}.$$

Die Aufgabe lautet also, aus aus der Menge $M = \{0, 1\}$ die Zahl

$$\zeta_n = e^{\frac{2\pi i}{n}}$$

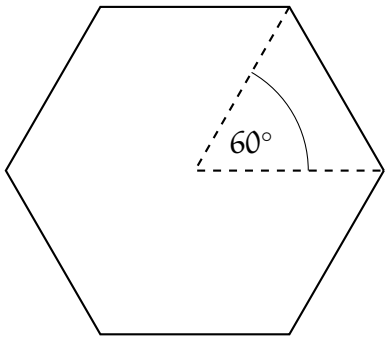

ABBILDUNG 12. Ein regelmäßiges 6-Eck

zu konstruieren. Aus Satz 11.10 kennen wir eine Formel für den Grad von $\mathbb{Q}(\zeta_n)/\mathbb{Q}$, nämlich

$$|\mathbb{Q}(\zeta_n) : \mathbb{Q}| = \deg(\phi_n) = |\mathbb{Z}_n^*|,$$

und wegen Korollar 4.7 ist ζ_n genau dann konstruierbar, wenn diese Zahl eine 2-Potenz ist. Aber für welche n ist das der Fall?

Beim regulären 6-Eck ist die Konstruktion einfach. Der Einheitskreis um 1 schneidet den Einheitskreis um 0 in ζ_6. Also gilt

$$\zeta_6 \in \widetilde{M}$$

und das reguläre 6-Eck ist somit konstruierbar. Das hätten wir auch daran ablesen können, daß

$$\phi_6 = t^2 - t - 1,$$

wegen

$$t^6 - 1 = \phi_6 \cdot \phi_3 \cdot \phi_2 \cdot \phi_1 = \phi_6 \cdot (t^2 + t + 1) \cdot (t + 1) \cdot (t - 1),$$

ein Polynom vom Grad 2 ist.

Machen wir uns nun Ergebnisse zunutze, die in der Vorlesung Elementare Zahlen gezeigt werden, so können wir die regulären n-Ecke, die konstruierbar sind, vollständig klassifizieren.

Satz 11.16 (Konstruierbarkeit des regulären n-Ecks)
Das reguläre n-Eck ist genau dann mit Zirkel und Lineal konstruierbar, wenn

$$n = 2^k \cdot p_1 \cdot \ldots \cdot p_l$$

für paarweise verschiedene Fermatsche Primzahlen

$$p_i = 2^{2^{m_i}} + 1.$$

Beweis: Die Zahl n habe die Primfaktorzerlegung

$$n = q_1^{n_1} \cdot \ldots \cdot q_m^{n_m}.$$

In der Vorlesung Elementare Zahlentheorie zeigt man, daß

$$\mathbb{Z}_n^* \cong \mathbb{Z}_{q_1^{n_1}}^* \times \ldots \times \mathbb{Z}_{q_m^{n_m}}^*$$

gilt (siehe [**Mar08b**, Satz 6.18]) und daß

$$|\mathbb{Z}^*_{q_i^{n_i}}| = \varphi\left(q_i^{n_i}\right) = q_i^{n_i-1} \cdot (q_i - 1)$$

gilt (siehe [**Mar08b**, Kor. 3.7]). Wir erhalten damit

$$|\mathbb{Z}^*_n| = \prod_{i=1}^{m} |\mathbb{Z}_{q_i^{n_i}}| = \prod_{i=1}^{m} q_i^{n_i-1} \cdot (q_i - 1).$$

Dies ist nun genau dann eine Zweierpotenz, wenn die ungeraden Primzahlen q_i nur mit Vielfachheit $n_i = 1$ vorkommen und zudem

$$q_i - 1 = 2^{k_i}$$

eine Zweierpotenz ist, was aber notwendigerweise zur Folge hat, daß

$$k_i = 2^{m_i}$$

selbst eine Zweierpotenz ist (siehe [**Mar08b**, Bem. 1.24]). □

Beispiel 11.17
Die Zahl

$$n = 17 = 2^{2^2} + 1$$

ist eine Fermatsche Primzahl und somit ist das reguläre 17-Eck wegen Satz 11.16 mit Zirkel und Lineal konstruierbar. Die Konstruktion aber tatsächlich durchzuführen ist ein ziemliches Problem, und unser Satz gibt uns dazu auch keinerlei Hinweis.

Das reguläre 7-Eck ist hingegen nicht konstruierbar, da 7 keine Fermatsche Primzahl ist.

KAPITEL III

Endliche Gruppen in der Galoistheorie

In diesem Teil der Vorlesung wollen wir grundlegende Methoden aus der Theorie der endlichen Gruppen kennenlernen, die einerseits für die Untersuchung konkreter Beispiele von Galoisgruppen wichtig sind und mit deren Hilfe andererseits interessante theoretische Ergebnisse in der Galoistheorie erzielt werden können. Dazu zählen ein Beweis des Fundamentalsatzes der Algebra (siehe Satz 12.34) und der Zusammenhang der Auflösbarkeit von Gleichungen durch Radikale und der Auflösbarkeit der zugehörigen Galoisgruppe (siehe Satz 13.20).

§ 12 Gruppenoperationen und die Sylowsätze

Ein sehr nützliches Ergebnis zu endlichen Gruppen in der Vorlesung Algebraische Strukturen war der Satz von Lagrange, daß die Ordnung einer Untergruppe ein Teiler der Ordnung der Gesamtgruppe ist. Die Sylowsätze, die wir in diesem Abschnitt beweisen wollen, zeigen, daß es für bestimmte Teiler der Gruppenordnung auch sicher Untergruppen der entsprechenden Ordnung gibt, und geben uns zu diesen weitere nützliche Hinweise. Aus ihnen kann man sehr viel über die Struktur einer endlichen Gruppe ableiten (siehe etwa Korollar 12.27 oder Korollar 13.4).

A) Gruppenoperationen

Operationen von Gruppen auf Mengen induzieren in natürlicher Weise eine Äquivalenzrelation auf Mengen und liefern auf diese Weise eine disjunkte Zerlegung der Menge in Äquivalenzklassen, die Bahnen der Gruppenoperation. Sie tauchen in nahezu allen Bereichen der Mathematik auf. In unserer Vorlesung sind sie das zentrale Mittel, um die Sylowsätze zu beweisen.

Definition 12.1 (Operation einer Gruppe auf einer Menge)
Es sei $(G, \cdot)$ eine Gruppe und Ω eine Menge.

a. Eine Abbildung

$$* : G \times \Omega \longrightarrow \Omega : (g, \omega) \mapsto g * \omega$$

heißt eine *Operation* von G auf Ω, wenn für alle $g, h \in G$ und für alle $\omega \in \Omega$

$$g * (h * \omega) = (g \cdot h) * \omega$$

und

$$e_G * \omega = \omega$$

gilt. Man sagt dann auch, die *Gruppe* G *operiert auf der Menge* Ω.

b. Für $\omega \in \Omega$ heißt
$$\omega^G := \{g * \omega \mid g \in G\} \subseteq \Omega$$
die *Bahn* von ω unter G und
$$G_\omega := \{g \in G \mid g * \omega = \omega\} \leq G$$
der *Stabilisator* von ω in G.

c. Eine Operation von G auf Ω heißt *treu*, wenn $\bigcap_{\omega\in\Omega} G_\omega = \{e_G\}$ gilt. Sie heißt *transitiv*, wenn $\Omega = \omega^G$ für ein $\omega \in \Omega$ gilt.

Bemerkung 12.2 (Operationen als Gruppenhomomorphismen)
Es sei $* : G \times \Omega \longrightarrow \Omega$ eine Operation der Gruppe G auf der Menge Ω.

Für ein $g \in G$ ist die Abbildung
$$\alpha_g : \Omega \longrightarrow \Omega : \omega \mapsto g * \omega$$
bijektiv mit der Inversen
$$\alpha_{g^{-1}}\Omega \longrightarrow \Omega : \omega \mapsto g^{-1} * \omega,$$
wegen
$$(\alpha_{g^{-1}} \circ \alpha_g)(\omega) = \alpha_{g^{-1}}(\alpha_g(\omega)) = g^{-1} * (g * \omega) = (g^{-1} \cdot g) * \omega = e_G * \omega = \omega.$$
Zudem ist die Abbildung
$$\alpha : G \longrightarrow \mathrm{Sym}(\Omega) : g \mapsto \alpha_g$$
ein Gruppenhomomorphismus, wegen
$$\alpha(g \cdot h)(\omega) = (g \cdot h) * \omega = g * (h * \omega) = \alpha_g(\alpha_h(\omega)) = (\alpha_g \circ \alpha_h)(\omega).$$
Eine Operation von G auf Ω induziert also einen Gruppenhomomorphismus von G nach $\mathrm{Sym}(\Omega)$, und umgekehrt induziert jeder solche Gruppenhomomorphismus eine Operation von G auf Ω. Man beachte auch, daß die Operation genau dann treu ist, wenn α injektiv ist.

Beispiel 12.3

a. Die Gruppe $G = \mathbb{S}_n$ operiert auf der Menge $\Omega = \{1, \ldots, n\}$ durch
$$\pi * k := \pi(k)$$
für $\pi \in \mathbb{S}_n$ und $k \in \Omega$. Die Operation ist treu und transitiv, und die Abbildung α in Bemerkung 12.2 ist dabei die Identität.

b. Es sei H eine Gruppe,
$$\Omega = \{(g_1, \ldots, g_n) \in H^n \mid g_1 \cdot \ldots \cdot g_n = e_H\}$$
und
$$G = \langle (1\ 2\ \ldots\ n) \rangle = \{\mathrm{id}, \pi, \pi^2, \ldots, \pi^{n-1}\} \leq \mathbb{S}_n$$

die Untergruppe der symmetrischen Gruppe $\mathbb{S}_n$, die vom n-Zykel

$$\pi = (1\ 2\ \ldots\ n)$$

erzeugt wird. Die Gruppe G operiert dann auf Ω durch

$$\pi^k * (g_1, \ldots, g_n) := (g_k, g_{k+1}, \ldots, g_n, g_1, g_2, \ldots, g_{k-1}).$$

Dazu beachten wir zunächst, daß

$$g_2 \cdot g_3 \cdot \ldots \cdot g_n \cdot g_1 = g_1^{-1} \cdot g_1 \cdot g_2 \cdot \ldots \cdot g_n \cdot g_1 = g_1^{-1} \cdot e_H \cdot g_1 = e_H$$

gilt, woraus

$$\pi * (g_1, \ldots, g_n) \in \Omega$$

folgt. Iterative Anwendung von π zeigt

$$\pi^k * (g_1, \ldots, g_n) \in \Omega$$

für alle $k \in \{0, \ldots, n-1\}$. Ferner gilt

$$\mathrm{id} * (g_1, \ldots, g_n) = (g_1, \ldots, g_n)$$

und

$$\begin{aligned}
\pi^k * \left(\pi^l * (g_1, \ldots, g_n)\right) =& \pi^k * (g_l, \ldots, g_n, g_1, \ldots, g_{l-1}) \\
=& (g_m, \ldots, g_n, g_1 \ldots, g_{m-1}) \\
=& \pi^m * (g_1, \ldots, g_n) \\
=& \pi^{k+l} * (g_1, \ldots, g_n) \\
=& (\pi^k \circ \pi^l) * (g_1, \ldots, g_n)
\end{aligned}$$

für alle $(g_1, \ldots, g_n) \in \Omega$ und für alle $k, l, m \in \{0, \ldots, n-1\}$ mit m kongruent zu $k + l$ modulo n. Damit haben wir gezeigt, daß G auf Ω operiert.
Ist $\omega = (g, \ldots, g) \in \Omega$, was z. B. für $g = e_H$ der Fall ist, so enthält die Bahn

$$\omega^G = \{(g, \ldots, g)\}$$

von ω nur ein Element und der Stabilisator von ω ist $G_\omega = G$.

Satz 12.4 (Cayley)
Ist $(G, \cdot)$ *eine endliche Gruppe, so ist* G *isomorph zu einer Untergruppe von* $\mathbb{S}_{|G|}$.

Beweis: Die Multiplikation "$\cdot$" der Gruppe ist offensichtlich eine Operation der Gruppe G auf der Menge G. Diese ist treu, weil aus $g \cdot \omega = \omega$ wegen der Kürzungsregel schon $g = e_G$ folgt und somit der Stabilisator von jedem $\omega \in G$ die Menge $\{e_G\}$ ist. Also definiert die Abbildung α aus Bemerkung 12.2 in diesem Fall einen Gruppenmonomorphismus

$$\alpha : G \longrightarrow \mathrm{Sym}(G) \cong \mathbb{S}_{|G|}$$

und G ist isomorph zum Bild von α als Untergruppe von $\mathbb{S}_{|G|}$. □

Lemma 12.5 (Gruppenoperationen als Äquivalenzrelationen)
Die Gruppe G *operiere auf der Menge* Ω*.*

a. Für $\omega \in \Omega$ *ist der Stabilisator* G_ω *eine Untergruppe von* G*.*

b. Je zwei Bahnen der Operation sind entweder identisch oder disjunkt, und Ω *ist die disjunkte Vereinigung der Bahnen unter* G*.*

Beweis:

a. Sind $g, h \in G_\omega$, so gilt

$$(g \cdot h) * \omega = g * (h * \omega) = g * \omega = \omega$$

und

$$g^{-1} * \omega = g^{-1} * (g * \omega) = (g^{-1} \cdot g) * \omega = e_G * \omega = \omega,$$

woraus $g \cdot h \in G_\omega$ und $g^{-1} \in G_\omega$ folgt. Da G_ω wegen $e_G \in G_\omega$ zudem nicht leer ist, ist G_ω eine Untergruppe von G.

b. Für $\omega, \omega' \in \Omega$ definieren wir $\omega \sim \omega'$, wenn es ein $g \in G$ gibt mit $g * \omega = \omega'$. Wir zeigen zunächst, daß $\sim$ eine Äquivalenzrelation auf Ω ist.
Für $\omega \in \Omega$ gilt $e_G * \omega = \omega$, woraus die Reflexivität der Relation folgt. Ist $g * \omega = \omega'$, so ist

$$g^{-1} * \omega' = g^{-1} * (g * \omega) = (g^{-1} \cdot g) * \omega = e_G * \omega = \omega,$$

woraus die Symmetrie der Relation folgt. Für die Transitivität betrachten wir $g * \omega = \omega'$ und $h * \omega' = \omega''$ und erhalten mit

$$(h \cdot g) * \omega = h * (g * \omega) = h * \omega' = \omega''$$

dann die Transitivität der Relation. Also ist $\sim$ eine Äquivalenzrelation auf Ω. Dabei ist die Bahn

$$\omega^G = \{g * \omega \mid g \in G\} = \{\omega' \in \Omega \mid \omega \sim \omega'\}$$

von ω unter G gerade die Äquivalenzklasse von ω bezüglich der Äquivalenzrelation. Insbesondere sind die Bahnen zweier Elemente ω und ω' also entweder disjunkt oder identisch und Ω ist die disjunkte Vereinigung der Bahnen.

□

Beispiel 12.6 (Konjugation)
Ist G eine Gruppe, so definiert

$$G \times G \longrightarrow G : (g, \omega) \mapsto \omega^g = g \cdot \omega \cdot g^{-1}$$

eine Operation von G auf G, die wir die *Konjugation* nennen. Um zu sehen, daß die Konjugation eine Operation ist, beachten wir, daß für $g, h, \omega \in G$ stets

$$\omega^{e_G} = e_G \cdot \omega \cdot e_G^{-1} = \omega$$

und

$$\omega^{g\cdot h} = (g\cdot h)\cdot\omega\cdot(g\cdot h)^{-1} = g\cdot(h\cdot\omega\cdot h^{-1})\cdot g^{-1} = \left(\omega^{h}\right)^{g}$$

gilt. Der Stabilisator

$$C_G(\omega) := G_\omega = \{g\in G \mid g\cdot\omega\cdot g^{-1} = \omega\} = \{g\in G \mid g\cdot\omega = \omega\cdot g\} \leq G$$

von $\omega\in G$ heißt auch der *Zentralisator* von ω in G. Die Bahn

$$\omega^G = \left\{\omega^g \;\middle|\; g\in G\right\}$$

heißt die *Konjugationsklasse* von ω unter G.

Satz 12.7 (Bahnbilanzgleichung)
Die Gruppe G operiere auf der endlichen Menge Ω. Dann gilt für $\omega\in\Omega$.

$$|G : G_\omega| = |\omega^G|$$

und es gibt ein Vertretersystem $\omega_1,\ldots,\omega_n\in\Omega$, so daß

$$|\Omega| = \sum_{i=1}^{n}|\omega_i^G| = \sum_{i=1}^{n}|G : G_{\omega_i}|.$$

Beweis: Wir beachten für $g,h\in G$ zunächst, daß die Bedingung

$$g*\omega = h*\omega$$

äquivalent zu

$$\left(h^{-1}\cdot g\right)*\omega = h^{-1}*(g*\omega) = h^{-1}*(h*\omega) = (h^{-1}\cdot h)*\omega = e_G*\omega = \omega$$

ist und damit äquivalent zu

$$h^{-1}\cdot g\in G_\omega,$$

was wiederum gleichwertig zur Gleichheit

$$g\cdot G_\omega = h\cdot G_\omega$$

der beiden Linksnebenklassen von G_ω bezüglich g und h ist.

Daraus leiten wir zunächst ab, daß die Abbildung

$$\beta : G/G_\omega \longrightarrow \omega^G : g\cdot G_\omega \mapsto g*\omega$$

nicht von der Wahl des Repräsentanten g der Linksnebenklasse $g\cdot G_\omega$ abhängt und somit wohldefiniert ist. Ferner folgt daraus, daß β injektiv ist. Zudem ist β offensichtlich surjektiv, da die Nebenklasse $g\cdot G_\omega$ ein Urbild von $g*\omega\in\omega^G$ unter β ist. Also ist β ein Isomorphismus und die behauptete Gleichheit der Mächtigkeiten

$$|G : G_\omega| = |\omega^G|$$

folgt. Wegen Lemma 12.5 ist Ω die disjunkte Vereinigung der Bahnen unter G. Wählen wir ein Vertretersystem $\omega_1,\ldots,\omega_n$ für die Bahnen, so gilt also

$$\Omega = \dot{\bigcup_{i=1}^{n}}\omega_i^G,$$

woraus sich unmittelbar die Gleichheit

$$|\Omega| = \sum_{i=1}^{n} |\omega_i^G| = \sum_{i=1}^{n} |G : G_{\omega_i}|$$

ergibt. □

Beispiel 12.8
Betrachten wir noch einmal $G = \mathbb{S}_n$ und $\Omega = \{1, \ldots, n\}$ aus Beispiel 12.3. Für $\omega = n \in \Omega$ ist der Stabilisator

$$G_\omega = \{\pi \in \mathbb{S}_n \mid \pi(n) = n\} \cong \mathbb{S}_{n-1}$$

eine Untergruppe, die isomorph zur $\mathbb{S}_{n-1}$ ist. Zugleich ist die Bahn

$$\omega^G = \{1, \ldots, n\} = \Omega$$

offenbar ganz Ω, und wir erhalten

$$|G : G_\omega| = \frac{|\mathbb{S}_n|}{|\mathbb{S}_{n-1}|} = \frac{n!}{(n-1)!} = n = |\Omega| = |\omega^G|.$$

Definition 12.9
Ist G eine Gruppe, so nennen wir

$$Z(G) := \{g \in G \mid g \cdot h = h \cdot g\}$$

das *Zentrum* von G. Das Zentrum besteht also genau aus den Elementen, die mit allen anderen kommutieren.

Proposition 12.10 (Das Zentrum von G)
Es sei G eine Gruppe.

a. $Z(G)$ ist ein Normalteiler von G.

b. Jede Untergruppe von $Z(G)$ ist ein Normalteiler von G.

Beweis: Sind $g, g' \in Z(G)$, so gilt für alle $h \in G$

$$(g \cdot g') \cdot h = g \cdot (g' \cdot h) = g \cdot (h \cdot g') = (g \cdot h) \cdot g' = (h \cdot g) \cdot g' = h \cdot (g \cdot g')$$

und aus

$$g \cdot h = h \cdot g$$

folgt

$$h \cdot g^{-1} = g^{-1} \cdot (g \cdot h) \cdot g^{-1} = g^{-1} \cdot (h \cdot g) \cdot g^{-1} = g^{-1} \cdot h.$$

Damit ist $g \cdot g' \in Z(G)$ und $g^{-1} \in Z(G)$ gezeigt. Da zudem offensichtlich $e_G \in Z(G)$ gilt, ist $Z(G)$ eine Untergruppe von G.

Sei nun $U \leq Z(G)$ eine Untergruppe von $Z(G)$, dann ist U auch eine Untergruppe von G. Für $h \in G$ beliebig gilt zudem

$$h \cdot U = \{h \cdot g \mid g \in U\} = \{g \cdot h \mid g \in U\} = U \cdot h,$$

woraus schließlich folgt, daß U ein Normalteiler von G ist. Insbesondere ist also $Z(G)$ ein Normalteiler von G. □

Beispiel 12.11

a. G ist genau dann abelsch, wenn $Z(G) = G$.

b. Das Zentrum von $\mathbb{S}_3$ ist $Z(\mathbb{S}_3) = \{\mathrm{id}\}$.

c. Das Zentrum der Diëdergruppe

$$\mathbb{D}_8 = \langle (1\,2\,3\,4), (2\,4) \rangle$$

der Ordnung 8 ist

$$Z(\mathbb{D}_8) = \{\mathrm{id}, (1\,3)(2\,4)\}.$$

Dies kann man einfach nachrechnen. Alternativ kann man sich an die Identifikation der $\mathbb{D}_8$ mit der Symmetriegruppe des Quadrates erinnern. Die Elemente der $\mathbb{D}_8$ sind also die vier Drehungen um $0°$, $90°$, $180°$ und $270°$, sowie die Spiegelungen an den vier Symmetrieachsen des Quadrates. Elementargeometrische Überlegungen zeigen dann, daß neben der Identität die Drehung um $180°$ die einzige Symmetrieabbildung ist, die mit allen anderen vertauscht.

Korollar 12.12 (Klassengleichung)
Ist G eine endliche Gruppe, so gilt enthält die Konjugationsklasse von $g \in G$ genau

$$|g^G| = |G : C_G(g)|$$

Elemente und es gilt die Klassengleichung

$$|G| = |Z(G)| + \sum_{i=1}^{k} |G : C_G(g_i)|,$$

wobei $g_1, \ldots, g_k \in G \setminus Z(G)$ ein Repräsentantensystem der Konjugationsklassen mit mehr als einem Element ist.

Beweis: Wenden wir die Bahnbilanzgleichung 12.7 auf die Konjugation als Operation von G auf G an, so erhalten wir für $g \in G$ unter Berücksichtigung von Beispiel 12.6

$$|g^G| = |G : G_g| = |G : C_G(g)|.$$

Damit gilt insbesondere, daß die Bahn von g unter G genau dann nur ein Element enthält, wenn

$$G = C_G(g) = \{h \in G \mid g \cdot h = h \cdot g\},$$

d. h. genau dann, wenn $g \in Z(G)$.

Wir wählen ein Vertretersystem $g_1, \ldots, g_n$ für die Bahnen von G unter Konjugation, wobei die g_i so sortiert seien, daß die Bahnen von $g_1, \ldots, g_k$ mehr als Element enthalten und die Bahnen von $g_{k+1}, \ldots, g_n$ genau ein Element enthalten. Damit gilt dann

$$Z(G) = \{g_{k+1}, \ldots, g_n\}$$

und aus der Bahnbilanzgleichung 12.7 folgt

$$|G| = \sum_{i=1}^{n} |g_i^G| = |Z(G)| + \sum_{i=1}^{k} |g_i^G| = |Z(G)| + \sum_{i=1}^{k} |G : C_G(g_i)|.$$

□

Beispiel 12.13
Wir wollen uns die Klassengleichung am Beispiel der $\mathbb{D}_8$ veranschaulichen. Wir wissen bereits, daß

$$Z(\mathbb{D}_8) = \{\mathrm{id}, (1\ 3)(2\ 4)\}.$$

Zudem enthält die $\mathbb{D}_8$ genau zwei Vierzykel, $\pi = (1\ 2\ 3\ 4)$ und $\pi^{-1} = (1\ 4\ 3\ 2)$. Da π nicht im Zentrum liegt, muß die Konjugationsklasse von π ein weiteres Element enthalten, und da der Zykeltyp unter Konjugation erhalten bleibt, muß

$$\pi^{\mathbb{D}_8} = \left\{\pi, \pi^{-1}\right\}$$

gelten. Es bleiben die Elemente

$$(1\ 4)(2\ 3), (1\ 2)(3\ 4), (2\ 3), (1\ 4).$$

Deren Konjugationsklassen müssen jeweils wieder mindestens zwei Elemente enthalten, da sie nicht im Zentrum sind, und sie können nur Elemente desselben Zykeltyps enthalten. Es folgt mit $\sigma = (1\ 4)(2\ 3)$ und $\rho = (2\ 3)$ also

$$\sigma^{\mathbb{D}_8} = \{\sigma, \sigma^{\pi}\} = \{(1\ 4)(2\ 3), (1\ 2)(3\ 4)\}$$

und

$$\rho^{\mathbb{D}_8} = \{\rho, \rho^{\pi}\} = \{(2\ 3), (1\ 4)\}$$

für $\rho = (2\ 3)$ gilt. Damit ist π, σ, ρ das in der Klassengleichung erwähnte Repräsentantensystem.

Definition 12.14 (p-Gruppe)
Für eine Primzahl p ist eine Gruppe G ein p-*Gruppe*, wenn $|G|$ eine p-Potenz ist.

Korollar 12.15 (p-Gruppen haben ein nicht-triviales Zentrum.)
Ist G *eine* p-*Gruppe, so ist* $|Z(G)| > 1$.

Beweis: Wir beachten, daß ein Elemente $g \in G$ genau dann im Zentrum von G liegt, wenn $G = C_G(g)$ gilt, d. h. wenn $|G : C_G(g)| = 1$. Da der Index $|G : C_G(g)|$ nach dem Satz von Lagrange ein Teiler der p-Potenz $|G|$ ist, gilt für die Elemente $g_1, \ldots, g_k \in G \setminus Z(G)$ aus der Klassengleichung 12.12

$$p \,\Big|\, |G : C_G(g_i)|.$$

Damit ist dann p aber ein Teiler von

$$|G| - \sum_{i=1}^{k} |G : C_G(g_i)| = |Z(G)|,$$

und diese Zahl kann insbesondere nicht eins sein. □

B) Die Sylowsätze

Das zentrale Ziel dieses Abschnittes ist es, den Satz von Lagrange teilweise umzukehren. Der Satz von Lagrange sagt, daß die Ordnung einer Untergruppe immer ein Teiler der Ordnung der Gruppe ist. Es bleibt die Frage, für welche Teiler der Gruppenordnung es Untergruppen der entsprechenden Ordnung gibt. Der Erste Sylowsatz wird zeigen, daß wir dies zumindest für Primzahlpotenzen sicher stellen können. Ein erster Schritt in die Richtung ist, der Satz von Cauchy, die Aussage für Primteiler zeigt.

Satz 12.16 (Cauchy)
Ist G *eine endliche Gruppe und* $p \in \mathbb{P}$ *eine Primzahl die die Ordnung* $|G|$ *von* G *teilt, so besitzt* G *ein Element der Ordnung* p.

Beweis: Wir setzen

$$\Omega = \{(g_1, \ldots, g_p) \mid g_1 \cdot \ldots \cdot g_p = e_G\}$$

wie in Beispiel 12.3. Man beachte, daß es zu jedem Tupel $(g_1, \ldots, g_{p-1}) \in G^{p-1}$ genau ein $g_p \in G$ mit

$$(g_1, \ldots, g_p) \in \Omega$$

gibt, nämlich $g_p = (g_1 \cdot \ldots \cdot g_{p-1})^{-1}$. Es gilt also

$$|\Omega| = |G^{p-1}| = |G|^{p-1}.$$

Aus Beispiel 12.3 wissen wir, daß die von

$$\pi = (1\ 2\ \ldots\ p) \in \mathbb{S}_p$$

erzeugte Untergruppe U von $\mathbb{S}_p$ auf Ω operiert.

Ist $\omega = (g_1, \ldots, g_p) \in \Omega$, so ist

$$|\omega^U| = |U : U_\omega| \in \{1, p\},$$

da der Index nach dem Satz von Lagrange ein Teiler von $|U| = p$ sein muß. Dabei gilt offenbar $|\omega^U| = 1$ genau dann, wenn

$$(g_k, \ldots, g_p, g_1, \ldots, g_{k-1}) = \pi^k * \omega = \omega = (g_1, \ldots, g_p)$$

für alle $k = 1, \ldots, p$ gilt, d. h. wenn

$$g_1 = \ldots = g_p.$$

Wir wissen, daß

$$\Omega = \dot{\bigcup_{i=1}^{n}} \omega_i^U$$

die disjunkte Vereinigung der Bahnen ist, wobei $\omega_1, \ldots, \omega_n$ ein Vertretersystem für die Bahnen ist. Wir können davon ausgehen, daß die ω_i so sortiert sind, daß die

Bahnen von $\omega_1, \ldots, \omega_k$ genau p Elemente haben und die Bahnen von $\omega_{k+1}, \ldots, \omega_n$ jeweils nur ein Element haben. Dann gilt

$$n - k = |\{\omega_{k+1}, \ldots, \omega_n\}| = |\Omega| - \sum_{i=1}^{k} |\omega_i^U| = |G|^{p-1} - k \cdot p$$

und die rechte Seite ist nach Voraussetzung durch p teilbar, weil $|G|$ durch p teilbar ist. Da die Bahn von $(e_G, \ldots, e_G)$ sicher nur ein Element enthält, gilt $n - k \geq 1$, und da p ein Teiler von $n-k$ ist muß $n-k \geq p$ gelten. Es gibt also mindestens ein weiteres Element $(g, \ldots, g) \in \Omega$ mit $g \neq e_G$, und aus

$$g^p = g \cdot \ldots \cdot g = e_G$$

folgt dann, daß g die Ordnung p hat, da p eine Primzahl ist. □

Satz 12.17 (Erster Sylowsatz)
Ist G eine endliche Gruppe, $p \in \mathbb{P}$ eine Primzahl und p^i ein Teiler der Ordnung $|G|$ von G, so besitzt G eine Untergruppe U der Ordnung $|U| = p^i$.

Beweis: Wir führen den Beweis durch Induktion nach $n = |G|$, wobei für $n = 1$ nichts zu zeigen ist. Sei also $n > 1$ und $i > 0$, da für $i = 0$ die gesuchte Untergruppe $\{e_G\}$ ist. Aus der Klassengleichung 12.12 wissen wir

$$|G| = |Z(G)| + \sum_{i=1}^{k} |G : C_G(g_i)|$$

für gewisse $g_1, \ldots, g_k \in G \setminus Z(G)$. Wir unterscheiden nun zwei Fälle.

Ist p kein Teiler von $|Z(G)|$, so muß es ein g_i geben, so daß p kein Teiler von $|G : C_G(g_i)|$ ist. Aus dem Satz von Lagrange wissen wir dann

$$p^i \Big| \frac{|G|}{|G : C_G(g_i)|} = |C_G(g_i)|.$$

Da g_i nicht im Zentrum von G liegt, ist

$$|C_G(g_i)| < |G|$$

und nach Induktionsvoraussetzung hat $C_G(g_i)$ eine Untergruppe U der Ordnung p^i, die dann auch eine Untergruppe von G ist.

Ist p ein Teiler von $|Z(G)|$, so gibt es nach dem Satz von Cauchy 12.16 ein Element $g \in Z(G)$ der Ordnung p. Die Untergruppe

$$N = \langle g \rangle \leq G$$

ist nach Proposition 12.10 ein Normalteiler von G und hat Ordnung p. Die Faktorgruppe G/N hat dann die Ordnung

$$|G/N| = \frac{|G|}{p} < |G|$$

und p^{i-1} ist ein Teiler von $|G/N|$. Nach Induktionsvoraussetzung besitzt G/N dann eine Untergruppe V der Ordnung $|V| = p^{i-1}$. Die Untergruppe V der Faktorgruppe ist aber von der Form $V = U/N$ für eine Untergruppe U von G und es gilt

$$|U| = |U/N| \cdot |N| = p^{i-1} \cdot p = p^i.$$

Damit ist die Aussage des Satzes in beiden Fällen bewiesen. □

Beispiel 12.18
Die symmetrische Gruppe $\mathbb{S}_4$ hat die Ordnung

$$|\mathbb{S}_4| = 4! = 24 = 2^3 \cdot 3.$$

Sie besitzt also sicher Untergruppen der Ordnung 2, 4, 8 und 3. Beispiele dafür kennen wir auch:

$$|\langle(1\ 2)\rangle| = 2, |\langle(1\ 2\ 3\ 4)\rangle| = 4, |\mathbb{D}_8| = 8, |\langle(1\ 2\ 3)\rangle| = 3.$$

Man kann übrigens mit etwas Rechnen zeigen, daß $\mathbb{A}_4$ keine Untergruppe der Ordnung 6 besitzt, obwohl sie Ordnung 12 hat. Im Ersten Sylowsatz ist es also wichtig, daß der Teiler eine Primzahlpotenz ist (siehe auch Korollar 12.28).

Wir wollen nun sehen, was wir über maximalen p-Untergruppen einer Gruppe G sagen können. Daraus ergibt sich der Zweite Sylowsatz, ein wichtiges Mittel, um die Struktur endlicher Gruppen zu untersuchen.

Definition 12.19 (p-Sylowgruppen)
Ist G eine endliche Gruppe, $p \in \mathbb{P}$ eine Primzahl und $|G| = p^n \cdot m$ mit $\operatorname{ggt}(m, p) = 1$, so heißen die Elemente von

$$\operatorname{Syl}_p(G) = \left\{U \leq G \;\middle|\; |U| = p^n\right\}$$

die p-*Sylowgruppen* von G.

Beispiel 12.20
Die $\mathbb{D}_8$ ist eine 2-Sylowgruppe von $\mathbb{S}_4$.

Satz 12.21 (Zweiter Sylowsatz)
Es sei G eine endliche Gruppe und p eine Primzahl mit $|G| = p^n m$ und $p \nmid m$.

a. *Jede p-Untergruppe von G ist in einer p-Sylowgruppe enthalten.*
b. *Die p-Sylowgruppen von G sind zueinander konjugiert in G, d. h. für je zwei p-Sylowgruppen $P, Q \in \operatorname{Syl}_p(G)$ gibt es ein $g \in G$ mit $Q = P^g$.*

Beweis:

a. Wir wählen ein $P \in \operatorname{Syl}_p(G)$ und betrachten die Menge

$$\Omega = G/P = \{gP \mid g \in G\}$$

der Linksnebenklassen von P. Ist nun $U \leq G$ eine beliebige p-Untergruppe von G der Ordnung $|U| = p^l$, so operiert U offensichtlich auf Ω durch Multiplikation

von links,

$$U \times \Omega \longrightarrow \Omega : (u, gP) \mapsto ugP,$$

und die Bahn von $\omega = gP$ ist

$$\omega^U = \{ugP \mid u \in U\}.$$

Aus dem Satz von Lagrange und der Bahnbilanzgleichung erhalten wir dann

$$m = \frac{|G|}{|P|} = |\Omega| = \sum_{i=1}^{k} |\omega_i^U|,$$

wenn $\omega_1 = g_1P, \ldots, \omega_k = g_kP$ ein Vertretersystem für die Bahnen unter U ist. Da die linke Seite nicht durch p teilbar ist, muß mindestens ein Summand auf der rechten Seite teilerfremd zu p sein. Es gibt also ein $\omega = gP$ mit

$$p \nmid |\omega^U| = |U : U_\omega| \;\Big|\; |U| = p^l,$$

wobei die Gleichung in der Mitte aus der Bahnbilanzgleichung 12.7 folgt und die Teilereigenschaft am Ende aus dem Satz von Lagrange. Dies ist aber nur für

$$|\omega^U| = 1$$

möglich, woraus sich

$$\{gP\} = \omega^U = \{ugP \mid u \in U\}$$

ableitet. Damit gilt aber

$$g^{-1}ug = g^{-1}uge_G \in g^{-1}ugP = g^{-1}gP = P$$

oder alternativ

$$u = gg^{-1}ugg^{-1} \in gPg^{-1} = P^g$$

für alle $u \in U$, also

$$U \subseteq P^g.$$

Da die Konjugation mit g

$$G \longrightarrow G : h \mapsto h^g$$

ein Gruppenisomorphismus ist, ist P^g eine Untergruppe von G der Ordnung $|P^g| = |P| = p^n$, ist also auch eine p-Sylowgruppe. Damit ist die Aussage in Teil a. gezeigt.

b. Setzen wir im Beweis von Teil a. $U = Q$, so erhalten wir dort

$$Q \subseteq P^g,$$

und da beide Gruppen p^n Elemente enthalten, gilt die Gleichheit.

□

Beispiel 12.22 (2-Sylowgruppen der $\mathbb{S}_4$)
Die 2-Sylowgruppen von $\mathbb{S}_4$ sind konjugiert, also insbesondere isomorph. Damit ist jede Untergruppe der $\mathbb{S}_4$ mit 8 Elementen isomorph zur $\mathbb{D}_8$. Da zudem die $\mathbb{D}_8$ die vom Vierzykel $(1\ 3\ 2\ 4)$ erzeugte Untergruppe nicht enthält, gibt es mindestens zwei 2-Sylowgruppen in der $\mathbb{S}_4$. Wir werden sehen, daß wir die Anzahl auch ohne Rechnen mit den Permutationen in $\mathbb{S}_4$ mit Hilfe des Dritten Sylowsatzes 12.25 bestimmen können.

Im Beweis des Dritten Sylowsatzes spielt die in der folgenden Bemerkung eingeführte Konjugation einer Gruppe auf der Menge der Konjugationsklassen einer anderen Gruppe eine wichtige Rolle.

Bemerkung 12.23 (Konjugation)
Es seien $P, U \leq G$ zwei Untergruppen von G und

$$\Omega = \left\{ P^g = gPg^{-1} \;\middle|\; g \in G \right\}$$

die Menge der Konjugationsklassen von P unter G. Wie in Beispiel 12.6 sieht man, daß U auf Ω durch Konjugation operiert,

$$U \times \Omega \longrightarrow \Omega : \left(u, P^g\right) \mapsto (P^g)^u = ugPg^{-1}u^{-1} = ug \cdot P \cdot (ug)^{-1} = P^{gu}.$$

Die Bahn von P unter U ist die *Menge der Konjugationsklassen von* P *unter* U

$$P^U = \left\{ P^u \;\middle|\; u \in U \right\}$$

und der Stabilisator von P unter U

$$N_U(P) := U_P = \{u \in U \mid uPu^{-1} = P\} \leq U$$

wird der *Normalisator von* P *in* U genannt. Offensichtlich gilt

$$P \cap U \trianglelefteq N_U(P).$$

Aus der Bemerkung ergibt sich mit Hilfe des Zweiten Sylowsatzes 12.21 das folgende Lemma, das im Beweis des Dritten Sylowsatzes eingeht.

Lemma 12.24
Es sei G *eine endliche Gruppe,* p *eine Primzahl und* $P \in \mathrm{Syl}_p(G)$*. Dann gilt*

$$\mathrm{Syl}_p(N_G(P)) = \{P\}.$$

Beweis: Da die Ordnung von P die maximale p-Potenz in $|G|$ ist und da wegen des Satzes von Lagrange $|N_G(P)|$ ein Teiler von $|G|$ ist, ist P eine p-Sylowgruppe von $N_G(P)$, d. h.

$$P \in \mathrm{Syl}_p(N_G(P)).$$

Aus Bemerkung 12.23 wissen wir, daß

$$P = P \cap G \trianglelefteq N_G(P)$$

ein Normalteiler im Normalisator ist. Damit erhalten wir

$$\{P\} = \left\{P^g \;\middle|\; g \in N_G(P)\right\} = \mathrm{Syl}_p(N_G(P)),$$

wobei die letzte Gleichheit aus dem Zweiten Sylowsatz 12.21 folgt. □

Wir sind nun in der Lage, den Dritten Sylowsatz zu formulieren und zu beweisen.

Satz 12.25 (Dritter Sylowsatz)
Ist G *eine endliche Gruppe und* p *eine Primzahl, die* $|G|$ *teilt, so gilt*

$$|\mathrm{Syl}_p(G)| \equiv 1 (\mathrm{mod}\ p)$$

und für alle $P \in \mathrm{Syl}_p(G)$ *gilt zudem*

$$|\mathrm{Syl}_p(G)| = |G : N_G(P)|.$$

Insbesondere ist $|\mathrm{Syl}_p(G)|$ *ein Teiler der Ordnung von* G.

Beweis: Wir wählen nun eine p-Sylowgruppe P und setzen

$$\Omega = \mathrm{Syl}_p(G) = \left\{P^g \;\middle|\; g \in G\right\},$$

wobei die letzte Gleichheit aus dem Zweiten Sylowsatz 12.21 folgt. Aus Bemerkung 12.23 mit $U = G$ wissen wir, daß G auf Ω durch Konjugation operiert und aus dem Zweiten Sylowsatz 12.21 wissen wir, daß diese Operation transitiv ist. Mit der Bahnbilanzgleichung 12.7 und Bemerkung 12.23 folgt dann

$$|\mathrm{Syl}_p(G)| = |\Omega| = |P^G| = |G : G_P| = |G : N_G(P)|.$$

Es bleibt noch

$$|\mathrm{Syl}_p(G)| \equiv 1 (\mathrm{mod}\ p)$$

zu zeigen. Dazu lassen wir mit Hilfe von Bemerkung 12.23 mit $U = P$ die p-Sylowgruppe P auf Ω durch Konjugation operieren.

Wir wollen zunächst sehen, daß es unter dieser Operation nur eine Bahn der Länge eins gibt, nämlich die Bahn

$$P^P = \left\{P^g \;\middle|\; g \in P\right\} = \{P\}$$

von P. Sei dazu $Q \in \Omega = \mathrm{Syl}_p(G)$ eine p-Sylowgruppe mit

$$Q^P = \left\{Q^g \;\middle|\; g \in P\right\} = \{Q\},$$

dann gilt

$$Q^g = Q$$

für alle $g \in P$ und somit ist

$$P \subseteq N_G(Q)$$

im Normalisator von Q in G enthalten. Aus Ordnungsgründen folgt dann

$$P \in \mathrm{Syl}_p(N_G(Q)) = \{Q\}.$$

Also gibt es genau eine Bahn der Länge eins unter der Operation von P auf Ω.

Wenden wir nun die Bahnbilanzgleichung 12.7 an, so erhalten wir

$$|\operatorname{Syl}_p(G)| = |\Omega| = |\{P\}| + \sum_{i=1}^{k} |Q_i^P| = 1 + \sum_{i=1}^{k} |P : P_{Q_i}|,$$

wenn $P, Q_1, \ldots, Q_k$ ein Vertretersystem der Bahnen unter der Operation von P ist. Da die Länge der Bahnen von $Q_1, \ldots, Q_k$ ein Teiler der Ordnung der p-Gruppe P ist, der nicht eins ist, ist jede dieser Längen durch p teilbar. Wir erhalten deshalb

$$|\operatorname{Syl}_p(G)| = 1 + \sum_{i=1}^{k} |P : P_{Q_i}| \equiv 1 (\text{mod } p).$$

□

Beispiel 12.26
Die Anzahl der 2-Sylowgruppen in $\mathbb{S}_4$ ist nach Beispiel 12.22 mindestens 2. Zudem ist sie ein Teiler von 24, der Teilerfremd zu 2 ist. Also gibt es genau drei 2-Sylowgruppen in $\mathbb{S}_4$.

Als einfache Anwendung der Sylowsätze wollen wir nun Gruppen der Ordnung 15 klassifizieren.

Korollar 12.27
Eine Gruppe G *der Ordnung* 15 *ist zyklisch.*

Beweis: Wir wissen, daß G eine 3-Sylowgruppe P und eine 5-Sylowgruppe Q besitzt, die als Gruppen von Primzahlordnung zyklisch sind.

Die Anzahl der 5-Sylowgruppen ist ein Teiler von 15, der kongruent zu 1 modulo 5 ist. Also ist gibt es nur eine 5-Sylowgruppe, und da alle eine solche unter Konjugation wieder auf eine 5-Sylowgruppe abgebildet wird, muß diese ein Normalteiler sein. Analog sieht man, daß es nur eine 3-Sylowgruppe gibt und daß diese ein Normalteiler von G ist.

Ist nun $g \in P$ ein Element der Ordnung 3 und $h \in Q$ ein Element der Ordnung 5, dann gilt

$$ghg^{-1}h^{-1} \in P \cap Q = \{e_G\},$$

da beide Untergruppen Normalteiler sind und teilerfremde Ordnung haben. Also gilt

$$gh = hg,$$

damit ist die Abbildung

$$\alpha : P \times Q \longrightarrow G : (g^k, h^l) \mapsto g^k \cdot h^l$$

ein Gruppenhomomorphismus. Ferner gilt $(g^k, h^l) \in \operatorname{Ker}(\alpha)$ genau dann, wenn

$$g^k \cdot h^l = e_G,$$

d. h. wenn

$$g^k = h^{-l} \in P \cap Q = \{e_G\}.$$

Der Kern von α enthält also nur das neutrale Element und α ist injektiv. Wegen $|P \times Q| = |G|$ folgt dann, daß α auch surjektiv und damit ein Isomorphismus ist. Wir erhalten insgesamt

$$G \cong P \times Q \cong \mathbb{Z}_3 \times \mathbb{Z}_5 \cong \mathbb{Z}_{15},$$

und die Gruppe G wird von $g \cdot h$ erzeugt. □

Als unmittelbare Folgerung erhalten wir ein Beispiel dafür, daß eine Gruppe nicht zu jedem Teiler der Gruppenordnung ein Untergruppe der entsprechenden Ordnung enthält.

Korollar 12.28 (Der Satz von Lagrange ist nicht umkehrbar.)
$\mathbb{S}_5$ *enthält keine Untergruppe der Ordnung* 15*, obwohl* 15 *ein Teiler von* $|\mathbb{S}_5|$ *ist.*

Beweis: Die $\mathbb{S}_5$ enthält nur Elemente der Ordnungen $1, \ldots, 5$. Das folgt unmittelbar aus der Tatsache, daß eine Permutation mit Zykeltyp $(k_1, \ldots, k_n)$ die Ordnung $\mathrm{kgv}(k_1, \ldots, k_n)$ hat, wie man leicht nachrechnet. □

Beispiel 12.29 (Galoisgruppen der Ordnung 15)
Es sei $L = \mathrm{ZFK}_{\mathbb{Q}}(f)$ der Zerfällungskörper eines Polynoms mit Galoisgruppe der Ordnung 15. Wir wollen zeigen, daß dann

$$\deg(f) \geq 8$$

gelten muß.

Aus Korollar 12.27 wissen wir, daß

$$\mathrm{Gal}\,(L/\mathbb{Q}) \cong \mathbb{Z}_{15}$$

gilt. Außerdem gilt mit $n = \deg(f)$ auch

$$\mathrm{Gal}\,(L/\mathbb{Q}) \leq \mathbb{S}_n.$$

Aber die kleinste Zahl n, für die $\mathbb{S}_n$ ein Element der Ordnung 15 besitzt, ist $n = 8$; dann hat

$$\pi = (1\ 2\ 3\ 4\ 5)(6\ 7\ 8)$$

die Ordnung 15. Also muß $\deg(f) = n \geq 8$ gelten.

Beispiel 12.30 (Eine Galoisgruppe der Ordnung 15)
Es sei $K = \mathbb{Q}(\zeta_{15})$ der 15-te Kreisteilungskörper und

$$L = \mathrm{ZFK}_K(t^{15} - 2) = \mathbb{Q}(\zeta_{15}, \alpha) = K(\alpha),$$

mit

$$\alpha = \sqrt[15]{2},$$

der Zerfällungskörper von $f = t^{15} - 2$ über K. Mit Hilfe des Eisensteinkriteriums 2.2 und Satz 2.4 wissen wir, daß f irreduzibel über $\mathbb{Q}$ ist. Daraus folgt dann

$$\left|\mathbb{Q}(\alpha) : \mathbb{Q}\right| = 15.$$

Außerdem wissen wir, daß

$$|K : \mathbb{Q}| = |\mathbb{Q}(\zeta_{15}) : \mathbb{Q}| = \varphi(15) = 8$$

gilt. Da $L/\mathbb{Q}$ die Zwischenkörper $\mathbb{Q}(\alpha)$ und K hat, sind sowohl 15, als auch 8 Teiler von $|L : \mathbb{Q}|$, und da beide teilerfremd sind und $L = K(\alpha)$, folgt dann

$$|L : \mathbb{Q}| = 15 \cdot 8$$

und

$$|L : K| = 15.$$

Damit ist insbesondere gezeigt, daß f irreduzibel über K ist.

Als Zerfällungskörper eines separablen Polynoms über K liefert L eine galoissche Körpererweiterung L/K, und es gilt

$$|\operatorname{Gal}(L/K)| = |L : K| = 15.$$

Aus Korollar 12.27 folgt dann

$$\operatorname{Gal}(L/K) \cong \mathbb{Z}_{15},$$

und als zyklische Gruppe der Ordnung 15 mit den Teilern $1, 3, 5, 15$ hat $\operatorname{Gal}(L/K)$ genau vier Untergruppen. Aufgrund des Hauptsatzes der Galoistheorie hat L/K dann genau vier Zwischenkörper. Man sieht leicht, daß dies neben L und K die beiden Körper

$$K(\alpha^3) = K\big(\sqrt[5]{2}\big)$$

und

$$K(\alpha^5) = K\big(\sqrt[3]{2}\big)$$

mit den Minimalpolynomen

$$\mu_{\alpha^5} = t^3 - 2$$

und

$$\mu_{\alpha^3} = t^5 - 2.$$

Man beachte dabei, daß man wie für f zeigen kann, daß die beiden Polynome irreduzibel über K sind.

C) Der Fundamentalsatz der Algebra

Wir werden nun mit Hilfe des Ersten Sylowsatzes und des Hauptsatzes der Galoistheorie den Fundamentalsatz der Algebra beweisen.

Definition 12.31 (Algebraisch abgeschlossen)
Ein Körper K heißt *algebraisch abgeschlossen*, wenn jedes nicht-konstante Polynom in $K[t]$ über K in Linearfaktoren zerfällt, d.h. wenn K keine echte algebraische Körpererweiterung besitzt.

Lemma 12.32

a. $\mathbb{R}$ *besitzt keine echte Körpererweiterung von ungeradem Grad.*

b. $\mathbb{C}$ *besitzt keine Körpererweiterung vom Grad* 2*.*

Beweis:

a. Sei $L/\mathbb{R}$ eine Körpererweiterung von ungeradem Grad $n = |L : \mathbb{R}|$. Aus dem Satz vom primitiven Element 11.5 folgt dann, daß

$$L = \mathbb{R}(a),$$

und das Minimalpolynom μ_α von α über $\mathbb{R}$ ist irreduzibel von ungeradem Grad

$$\deg(\mu_\alpha) = |\mathbb{R}(\alpha) : \mathbb{R}| = n.$$

Aus dem Zwischenwertsatz (siehe [**Mar11**, Satz 14.12, Bsp. 14.13]) folgt dann, daß μ_α eine Nullstelle in $\mathbb{R}$ hat. Also muß

$$\mu_\alpha = t - \alpha$$

und somit $L = \mathbb{R}$ gelten.

b. Wäre $L/\mathbb{C}$ eine Körpererweiterung vom Grad zwei, so wäre

$$L = \mathbb{C}(\alpha)$$

mit Minimalpolynom $\mu_\alpha = t^2 + pt + q \in \mathbb{C}[t]$ irreduzibel nach dem Satz vom primitiven Element 11.5. Aber dann hat μ_α die Nullstelle

$$\beta = -\frac{p}{2} + \sqrt{\frac{p^2}{4} - q} \in \mathbb{C},$$

weil jede komplexe Zahl eine Quadratwurzel besitzt, im Widerspruch zur Irreduzibilität von μ_α.

□

Lemma 12.33
Ist L/K *eine galoissche Körpererweiterung und* p^k *ein Teiler von* $|L : K|$ *für eine Primzahl* $p \in \mathbb{P}$*, dann gibt es einen Zwischenkörper* N *von* L/K *mit* $|L : N| = p^k$*.*

Beweis: Da L/K galoissch ist, gilt

$$p^k \,\Big|\, |L : K| = |\operatorname{Gal}(L/K)|.$$

Nach dem Ersten Sylowsatz 12.17 gibt es dann eine Untergruppe $U \leq \operatorname{Gal}(L/K)$ von Ordnung $|U| = p^k$. Aus dem Hauptsatz der Galoistheorie folgt dann die Existenz eines Zwischenkörpers $N = \operatorname{Fix}(L, U)$ von L/K mit

$$\operatorname{Gal}(L/N) = U$$

und somit

$$|L : N| = |\operatorname{Gal}(L/N)| = p^k.$$

□

Satz 12.34 (Fundamentalsatz der Algebra)
Der Körper $\mathbb{C}$ *ist algebraisch abgeschlossen.*

Beweis: Es sei $f \in \mathbb{C}[t]$ ein nicht-konstantes Polynom und $L = \mathrm{ZFK}_{\mathbb{C}}(f)$ sei der Zerfällungskörper von f über $\mathbb{C}$. Wir wollen zeigen, daß $L = \mathbb{C}$ gilt, dann zerfällt f über $\mathbb{C}$ in Linearfaktoren und somit ist $\mathbb{C}$ algebraisch abgeschlossen.

Nach dem Satz vom primitiven Element 11.5 ist L als endliche Erweiterung von $\mathbb{R}$ einfach über $\mathbb{R}$, ist also von der Form

$$L = \mathbb{R}(\alpha)$$

für ein $\alpha \in L$. Ist M der Zerfällungskörper des Minimalpolynoms von α über $\mathbb{R}$, dann ist $M/\mathbb{R}$ nach Satz 9.6 galoissch und

$$\mathbb{R} \subset \mathbb{C} \subseteq L = \mathbb{R}(\alpha) \subseteq M$$

mit

$$2 = |\mathbb{C} : \mathbb{R}| \,\Big|\, |M : \mathbb{R}| = |\operatorname{Gal}(M/\mathbb{R})|.$$

Ist $U \in \mathrm{Syl}_2(\operatorname{Gal}(M/\mathbb{R}))$ eine 2-Sylowgruppe und ist $N = \operatorname{Fix}(M, U)$, so folgt mit dem Hauptsatz der Galoistheorie, daß

$$|N : \mathbb{R}| \overset{10.7}{=} |\operatorname{Gal}(M/\mathbb{R}) : \operatorname{Gal}(M/N)|$$

eine ungerade Zahl ist. Nach Lemma 12.32 impliziert das

$$N = \mathbb{R}$$

und

$$U = \operatorname{Gal}(M/\mathbb{R}).$$

Aber dann sind

$$|M : \mathbb{R}| = |U| = 2^k$$

und dann auch

$$|M : \mathbb{C}| = 2^{k-1}$$

Potenzen der Zahl 2.

Nehmen wir $k \geq 2$ an, so besitzt die galoissche Körpererweiterung $M/\mathbb{C}$ nach Lemma 12.33 einen Zwischenkörper Z mit $|M : Z| = 2^{k-2}$ und es folgt

$$|Z : \mathbb{C}| = \frac{|M : \mathbb{C}|}{|M : Z|} = \frac{2^{k-1}}{2^{k-2}} = 2$$

im Widerspruch zu Lemma 12.32. Also ist $k = 1$ und damit $M = L = \mathbb{C}$. □

Aufgaben

Aufgabe 12.35

Es sei G eine endliche Gruppe. Zeige die folgenden Aussagen:

a. Ist $G/Z(G)$ zyklisch, so ist G abelsch.

b. Ist $|G| = p^2$ für eine Primzahl p, so ist G abelsch.

§ 13 Auflösbare Gruppen und Auflösbarkeit durch Radikale

In diesem Abschnitt wollen wir mit Hilfe des Hauptsatzes eine weitere interessante Brücke zwischen der Gruppentheorie und der Körpertheorie schlagen. Wir wenden uns den Lösungsformeln für die Nullstellen von Polynomen mit Hilfe von Wurzelausdrücken zu und wollen zeigen, daß Polynome nur dann durch Radikale auflösbar sind, wenn die Galoisgruppe ihres Zerfällungskörpers im Sinne der Gruppentheorie auflösbar ist. Die notwendigen Begriffe führen wir im folgenden ein.

A) Einfache Gruppen

Definition 13.1 (Einfache Gruppen)
Eine Gruppe G heißt *einfach*, wenn sie nur die Normalteiler G und $\{e_G\}$ besitzt.

Proposition 13.2 (Einfache abelsche Gruppen)
Eine abelsche Gruppe ist genau dann einfach, wenn sie zyklisch von Primzahlordnung ist.

Beweis: Ist G zyklisch von Primzahlordnung, so hat G aufgrund des Satzes von Lagrange nur die trivialen Untergruppen $\{e_G\}$ und G und ist somit einfach.

Ist G abelsch und ist die Ordnung $|G|$ keine Primzahl, so hat die Ordnung einen Primteiler p mit $1 < p < |G|$. Aus dem Satz von Cauchy 12.16 folgt dann, daß G eine Untergruppe N der Ordnung p besitzt. Da G abelsch ist, ist N ein Normalteiler, so daß G nicht einfach ist. □

Bemerkung 13.3 (Klassifikation einfacher Gruppen)
Will man eine endliche Gruppe G untersuchen und kennt einen nicht-trivialen Normalteiler $N \lhd G$, dann kann verrät die Struktur der kleineren Gruppen N und G/N eine Menge über G und kann G aus diesen beiden rekonstruieren. In diesem Sinne bilden die Gruppen, die keine nicht-trivialen Normalteiler besitzen, die Elementarbausteine zur Konstruktion aller anderen Gruppen. Es war eines der ganz großen Projekte der sechziger und siebziger Jahre des zwanzigsten Jahrhunderts, die einfachen Gruppen zu klassifizieren, d. h. für jede Isomorphieklasse von einfachen Gruppen einen Vertreter anzugeben. An dem Projekt haben viele Mathematiker mitgewirkt und der Beweis der Klassifikation umfaßt mehr als 15.000 Seiten, die in mehr als 500 Artikeln veröffentlicht wurden (siehe [**Gor82, Gor83, Gor96**]). Das Ergebnis besagt, daß es drei klar beschriebene, unendliche Serien von einfachen Gruppen gibt und zusätzlich noch 26 weitere einfache Gruppen, die sogenannten sporadischen einfachen Gruppen, die sich nicht in diese Serien einordnen lassen. Die größte der sporadischen einfachen Gruppen hat, die *Monstergruppe*, hat

808.017.424.794.512.875.886.459.904.961.710.757.005.754.368.000.000.000

Elemente. Es versteht sich, daß die Klassifikation oder eine ausführliche Betrachtung der sporadischen einfachen Gruppen den Rahmen der Vorlesung sprengen würde.

Wir wollen hier ein erstes nicht-abelsches Beispiel für eine einfache Gruppe geben. Mit etwas mehr Aufwand kann man zeigen, daß es das kleinste Beispiel einer nicht-abelschen einfachen Gruppe ist.

Korollar 13.4 ($\mathbb{A}_5$ ist einfach.)
Die alternierende Gruppe $\mathbb{A}_5$ vom Grad 5 ist einfach.

Beweis: Durch einfaches Auflisten und Zählen der Elemente, stellt man fest, daß die $\mathbb{A}_5$ genau 24 Fünfzykel und genau 20 Dreizykel enthält. Da jede 5-Sylowgruppe der $\mathbb{A}_5$ genau vier Fünfzykel enthält und je zwei 5-Sylowgruppen aufgrund des Satzes von Lagrange nur das neutrale Element gemeinsam haben können, muß es genau sechs 5-Sylowgruppen in der $\mathbb{A}_5$ geben. Analog sieht man, daß es genau zehn 3-Sylowgruppen gibt.

Sei nun $\{e_G\} \subsetneqq N \trianglelefteq \mathbb{A}_5$ ein Normalteiler in der $\mathbb{A}_5$. Wir wollen zeigen, daß $N = \mathbb{A}_5$ gilt, und betrachten dazu verschiedene Fälle.

Wenn 5 ein Teiler von $|N|$ ist, dann enthält N eine 5-Sylowgruppe von $\mathbb{A}_5$. Da N als Normalteiler aber invariant unter Konjugation mit Elementen aus G ist und die 5-Sylowgruppen alle konjugiert sind, muß N dann alle 5-Sylowgruppen enthalten, woraus

$$|N| \geq 1 + 24 = 25$$

folgt. Aufgrund des Satzes von Lagrange gilt dann schon

$$|N| \in \{30, 60\}.$$

Also enthält N auch eine 3-Sylowgruppe von G und damit alle, woraus

$$|N| \geq 1 + 24 + 20 = 45$$

folgt, also $|N| = 60$ und $N = \mathbb{A}_5$.

Ist 3 ein Teiler von $|N|$, so zeigt man analog, daß $N = \mathbb{A}_5$ gilt.

Ist $|N| = 4$, so ist N eine N eine 2-Sylowgruppe von $\mathbb{A}_5$ und da die 2-Sylowgruppen konjugiert sind, müßte N als Normalteiler die einzige 2-Sylowgruppe von $\mathbb{A}_5$ sein, im Gegensatz dazu, daß es $60 - 24 - 20 - 1 = 15$ Elemente der Ordnung 2 gibt, die alle in 2-Sylowgruppen liegen müssen.

Es bleibt der Fall $|N| = 2$ zu betrachten. In diesem Fall ist $N = \langle n \rangle$ für ein Element n der Ordnung 2. Da N ein Normalteiler ist, muß

$$n^g = n$$

für alle $g \in \mathbb{A}_5$ gelten. Eine leichte Rechnung zeigt, daß das für keine der 15 Doppeltranspositionen in $\mathbb{A}_5$ gelten kann:

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

□

B) Auflösbare Gruppen

Eine der wichtigsten und am besten untersuchten Klassen endlicher Gruppen sind die die auflösbaren Gruppen (siehe [**DH92**]). Sofern sie nicht-abelsch sind, sind sie weit davon entfernt, einfach zu sein. Sie lassen sich mit Hilfe sukzessiver Normalteilerbildung auf Bausteine reduzieren, die zyklisch von Primzahlordnung sind, wie wir weiter unten zeigen werden.

Definition 13.5 (Auflösbare Gruppen)
Eine Gruppe G heißt *auflösbar*, wenn es eine Kette

$$\{e_G\} = G_k \leq G_{n-1} \leq \ldots \leq G_1 \leq G_0 = G$$

gibt, so daß $G_i \trianglelefteq G_{i-1}$ und G_{i-1}/G_i abelsch für alle $i = 1, \ldots, k$ gilt.
Wir nennen eine solche Kette eine *Subnormalteilerkette* mit abelschen Faktoren.

Beispiel 13.6 (Auflösbare Gruppen)

a. Abelsche Gruppen G sind auflösbar mit der Subnormalteilerkette $\{e_G\} \leq G$.

b. Die Gruppe $\mathbb{S}_4$ ist auflösbar mit der Subnormalteilerkette

$$\{\mathrm{id}\} < \mathbb{K}_4 < \mathbb{A}_4 < \mathbb{S}_4,$$

wobei

$$\mathbb{K}_4 = \{\mathrm{id}, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$$

die Kleinsche Vierergruppe ist. Man beachte, daß in diesem Fall alle Gruppen in der Subnormalteilerkette sogar Normalteiler von $\mathbb{S}_4$ sind; das ist mehr als gefordert ist. Die Faktorgruppen $\mathbb{S}_4/\mathbb{A}_4$ und $\mathbb{A}_4/\mathbb{K}_4$ sind von Primzahlordnung und deshalb abelsch, die Gruppe $\mathbb{K}_4/\{\mathrm{id}\}$ ist bekanntermaßen abelsch.

c. Die Gruppe $\mathbb{A}_5$ ist nach Korollar 13.4 einfach und nicht-abelsch. Mithin kann sie keinen Normalteiler G_1 besitzen, so daß $\mathbb{A}_5/G_1 = G_0/G_1$ abelsch ist. Also ist $\mathbb{A}_5$ nicht auflösbar.

Proposition 13.7 (Untergruppen und Faktorgruppen auflösbarer Gruppen)
Sei G eine endliche Gruppe, $U \leq G$ eine Untergruppe und $N \trianglelefteq G$ ein Normalteiler.

a. Ist G auflösbar, so ist U auflösbar.

b. Genau dann ist G auflösbar, wenn N und G/N auflösbar sind.

Beweis:

a. Ist G auflösbar und ist

$$\{e_G\} = G_k \leq G_{n-1} \leq \ldots \leq G_1 \leq G_0 = G$$

eine Subnormalteilerkette wie in Definition 13.5, so setzen wir

$$U_i := G_i \cap U \leq U.$$

Damit erhalten wir eine Kette

$$\{e_U\} = U_k \leq U_{n-1} \leq \ldots \leq U_1 \leq U_0 = U$$

von Untergruppen von U. Dabei gilt

$$U_i = G_i \cap U = G_i \cap G_{i-1} \cap U = G_i \cap U_{i-1},$$

so daß U_i als Schnitt der Untergruppe U_{i-1} von G_{i-1} mit dem Normalteiler G_i von G_{i-1} ein Normalteiler von U_{i-1} ist (siehe [**Mar08a**, Lemma 4.29]). Aus dem Ersten Isomorphiesatz (siehe [**Mar08a**, Satz 4.54]) erhalten wir dann

$$U_{i-1}/U_i = U_{i-1}/G_i \cap U_{i-1} \cong U_{i-1} \cdot G_i/G_i \leq G_{i-1}/G_i,$$

so daß U_{i-1}/U_i isomorph zu einer Untergruppe der abelschen Gruppe G_{i-1}/G_i ist und damit selbst abelsch sein muß.

b. Sei zunächst G auflösbar und

$$\{e_G\} = G_k \leq G_{n-1} \leq \ldots \leq G_1 \leq G_0 = G$$

eine Subnormalteilerkette wie in Definition 13.5. Da N ein Normalteiler ist, erhalten wir durch Multiplikation mit N eine Kette

$$N = G_kN \leq G_{n-1}N \leq \ldots \leq G_1N \leq G_0N = G \tag{21}$$

von Untergruppen in G, die alle N enthalten. Ist nun $n \in N$ und $g \in G_{i-1}$, dann gilt

$$gnG_iN = gnG_iNn = gnNG_in = gNG_in = NgG_in = NG_ign = G_iNgn,$$

wobei N mit g und G_i vertauscht, weil N ein Normalteiler in G ist, und G_i mit g vertauscht, weil G_i ein Normalteiler in G_{i-1} ist. Damit haben wir gezeigt, daß

$$NG_i \trianglelefteq NG_{i-1}$$

gilt für $i = 1, \ldots, k$. Wenden wir nun den Ersten und den Zweiten Isomorphiesatz (siehe [**Mar08a**, Satz 4.54,4.55]) an, so erhalten wir

$$\begin{aligned} G_{i-1}N/G_iN =& G_{i-1}G_iN/G_iN \cong G_{i-1}/G_{i-1} \cap G_iN \\ \cong& (G_{i-1}/G_i)/((G_{i-1} \cap G_iN)/G_i), \end{aligned}$$

so daß $G_{i-1}N/G_iN$ isomorph zu einer Faktorgruppe der abelschen Gruppe G_{i-1}/G_i und damit selbst abelsch ist. Also ist mit (21)

$$\{e_{G/N}\} = G_kN/N \leq G_{k-1}N/N \leq \ldots \leq G_1N/N \leq G_0N/N = G/N$$

eine Subnormalteilerkette wie in Definition 13.5 mit abelschen Faktoren

$$(G_{i-1}N/N)/(G_iN/N) \cong G_{i-1}N/G_iN.$$

Damit ist gezeigt, daß G/N auflösbar ist. Aus Teil a. wissen wir zudem, daß N auflösbar ist.
Seien nun umgekehrt N und G/N auflösbar, so gibt es Subnormalteilerketten

$$\{e_G\} = N_k \leq N_{k-1} \leq \ldots \leq N_1 \leq N_0 = N$$

und

$$\{e_{G/N}\} = G_l/N \leq G_{l-1}/N \leq \ldots \leq G_1/N \leq G_0/N = G/N$$

wie in Definition 13.5 mit abelschen Faktoren, und dann ist

$$\{e_G\} = N_k \leq N_{k-1} \leq \ldots \leq N_0 = N = G_l \leq G_{l-1} \leq \ldots \leq G_0 = G$$

eine Subnormalteilerkette wie in Definition 13.5 mit abelschen Faktoren, wobei wir aufgrund des Zweiten Isomorphiesatzes wieder

$$G_{i-1}/G_i \cong (G_{i-1}/N)/(G_i/N)$$

beachten. Also ist G auflösbar

□

Korollar 13.8 (Auflösbarkeit von $\mathbb{S}_n$)
$\mathbb{S}_n$ und $\mathbb{A}_n$ sind für $n \geq 5$ nicht auflösbar.

Beweis: Die Gruppen enthalten jeweils eine Untergruppe, die isomorph zur $\mathbb{A}_5$ ist. Da diese nach Beispiel 13.6 nicht auflösbar ist, sind die Gruppen selbst nach Proposition 13.7 nicht auflösbar. □

Korollar 13.9 (p-Gruppen sind auflösbar)
Ist G eine p-Gruppe, so ist G auflösbar.

Beweis: Die Ordnung von G sei $|G| = p^n$ mit $p \in \mathbb{P}$. Wir führen den Beweis durch Induktion nach n, wobei für $n = 0$ nichts zu zeigen ist. Ist $n \geq 1$, so besitzt G nach Korollar 12.15 ein nicht-triviales Zentrum $Z(G)$. Falls $Z(G) = G$ gilt, so ist G abelsch und damit auflösbar. Falls $Z(G) \neq G$, so haben wir einen Normalteiler von G mit

$$1 < |Z(G)| < |G|$$

gefunden. Die p-Gruppen $Z(G)$ und $G/Z(G)$ sind dann per Induktion auflösbar, und aus Proposition 13.7 leiten wir dann ab, daß auch G auflösbar ist. □

Beispiel 13.10 (Quaterionengruppe)
In Aufgabe 10.11 war eine Galoisgruppe der Ordnung 8 zu berechnen, die sogenannte Quaterionengruppe. Diese ist als 2-Gruppe auflösbar.

In den Anwendungen, die wir im Blick haben, benötigen wir, daß sich eine Subnormalteilerkette wie in Definition 13.5 zu einer Subnormalteilerkette verfeinern läßt, in der die Faktoren alle Primzahlordnung haben und damit insbesondere zyklisch sind.

Satz 13.11 (Auflösbare Gruppen haben Hauptreihen mit zyklischen Faktoren)
Eine endliche Gruppe G ist genau auflösbar, wenn es eine Kette von Untergruppen

$$\{e_G\} = G_k < G_{n-1} < \ldots < G_1 < G_0 = G$$

gibt mit $G_i \lhd G_{i-1}$ *und* G_{i-1}/G_i *zyklisch von Primzahlordnung für* $i = 1, \ldots, k$. *Eine solche Kette wird dann auch eine* Hauptreihe *von* G *genannt.*

Beweis: Da die Faktoren der obigen Hauptreihe als zyklische Gruppen abelsch sind, folgt aus der Existenz einer Hauptreihe mit zyklischen Faktoren die Auflösbarkeit von G.

Ist umgekehrt eine Subnormalteilerkette wie in Definition 13.5 mit abelschen Faktoren gegeben, so müssen wir zeigen, daß wir diese zu einer Hauptreihe verfeinern können. Beachte dabei, daß ein abelscher Faktor G_{i-1}/G_i, der nicht von Primzahlordnung ist, nach Proposition 13.2 auch nicht einfach ist. Also gibt es einen Normalteiler echt zwischen G_i und G_{i-1}, der die Subnormalteilerkette verfeinert. Da die Ordnung der Faktoren dabei kleiner wird, können wir das nur endlich oft machen und erhalten schließlich eine Hauptreihe. □

Beispiel 13.12
Die auflösbare Gruppe $\mathbb{S}_4$ hat die Hauptreihe

$$\{\mathrm{id}\} < \langle (1\,2)(3\,4) \rangle < \mathbb{K}_4 < \mathbb{A}_4 < \mathbb{S}_4.$$

Korollar 13.13
Gruppen der Ordnung pq *mit* $p, q \in \mathbb{P}$ *sind auflösbar.*

Beweis: Ist $p = q$, so ist G nach Korollar 13.9 abelsch und damit auflösbar.

Andernfalls können wir $p > q$ annehmen. Aus dem Dritten Sylowsatz 12.25 wissen wir, daß $|\mathrm{Syl}_p(G)|$ ein Teiler von q ist, der modulo p den Rest 1 hat. Also gilt

$$|\mathrm{Syl}_p(G)| = 1.$$

Damit muß die einzige p-Sylowgruppe P von G dann ein Normalteiler sein, da unter Konjugation p-Sylowgruppen aus Ordnungsgründen auf p-Sylowgruppen abgebildet werden. Wegen $|G/P| = q$ und $|P| = p$ sind zudem G/P und P zyklisch, so daß

$$\{e_G\} < P < G$$

eine Hauptreihe mit zyklischen Faktoren ist. Also ist G abelsch. □

Beispiel 13.14
Gruppen der Ordnung 6, 9, 10, 14, 21, 22, 25 und 26 sind auflösbar, ebenso eine Gruppe der Ordnung

$$52.8907.979 = 22993 \cdot 23003.$$

Mit ähnlichen einfachen Mitteln kann man zeigen, daß jede Gruppe von einer Ordnung echt kleiner als 60 auflösbar ist.

Bemerkung 13.15 (Satz von Burnside (1911) / Satz von Feit-Thompson (1963))

a. Der Satz von Burnside besagt, daß jede Gruppe, deren Ordnung höchstens höchstens zwei Primteiler hat, auflösbar ist.

b. Der Satz von Feit-Thompson besagt, daß jede Gruppe ungerader Ordnung auflösbar ist. Der Beweis dieses Satzes ist etwa 300 Seiten lang (siehe [**FT63**]) und stellt den Auftakt zur Klassifikation der endlichen einfachen Gruppen dar.

C) Auflösung polynomialer Gleichungen

Bemerkung 13.16 (Lösungsformeln zum Bestimmen von Nullstellen)
Betrachten wir ein Polynom der Form

$$f = t^n + a_{n-1}t^{n-1} + \ldots + a_0 \in \mathbb{C}[t],$$

so wissen wir, daß f über $\mathbb{C}$ in Linearfaktoren zerfällt

$$f = (t - \alpha_1) \cdot \ldots \cdot (t - \alpha_n),$$

wobei die α_i genau die Nullstellen von f sind. Wir interessieren uns nun für geschlossene Formeln zur Bestimmung der Nullstellen aus den Koeffizienten. Dabei sollen möglichst nur einfach Operationen benötigt werden.

$\underline{n = 1}$**:** Dann ist $f = t - a_1$ und wir sind fertig.

$\underline{n = 2}$**:** Die Formel

$$\alpha = -\frac{a_1}{2} \pm \sqrt{\frac{a_1^2}{4} - a_2}$$

zur Bestimmung der Nullstellen ist aus der Schule bekannt.

$\underline{n = 3}$**:** Wir unterwerfen das Polynom f zunächst der Tschirnhausen-Transformation

$$\Phi_{1,-\frac{a_2}{3}} : \mathbb{C}[t] \xrightarrow{\cong} \mathbb{C}[t] : h \mapsto h\left(t - \tfrac{a_2}{3}\right),$$

und erhalten so ein neues Polynom

$$g = f\left(t - \frac{a_2}{3}\right) = t^3 + pt + q \tag{22}$$

mit

$$p = a_1 - \frac{a_2^2}{3}$$

und

$$q = a_0 - \frac{a_1 a_2}{3} + \frac{2a_2^3}{27}.$$

Ist $p = 0$, so sind die dritten Wurzeln aus q die Nullstellen von g und deren Urbild unter $\Phi_{1,-\frac{a_2}{3}}$ sind die Nullstellen von f.
Wir nehmen nun also $p \neq 0$ an und folgen dem Ansatz

$$t = u + v$$

von Gerolamo Cardano (1545). Aus der Gleichung $g = 0$ wird dann

$$\left(u^3 + v^3 + 3uv \cdot (u + v)\right) + p \cdot (u + v) + q = 0 \tag{23}$$

Wir wählen nun v so, daß

$$3uv = -p \tag{24}$$

gilt, d.h. $u \neq 0$ und

$$v = -\frac{p}{3u}. \tag{25}$$

Aus Gleichung (23) wird dann

$$0 \overset{(23),(24)}{=} u^3 + v^3 + q \overset{(25)}{=} u^3 + q - \frac{p^3}{27u^3}. \tag{26}$$

Multipliziert man diese Gleichung mit u^3, so erhält man

$$(u^3)^2 + qu^3 - \frac{p^3}{27} = 0.$$

Wenden wir hierauf die Lösungsformel für Polynome zweiten Grades an, so erhalten wir

$$u^3 = -\frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}. \tag{27}$$

Ist nun $u \in \mathbb{C}$ eine dritte Wurzel aus der rechten Seite,

$$u = \sqrt[3]{-\frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}},$$

und ist $\zeta_3 = e^{\frac{2\pi i}{3}}$, so gilt mit $v = -\frac{p}{3u}$, daß

$$\beta_1 = u + v, \quad \beta_2 = \zeta_3 \cdot u + \zeta_3^2 \cdot v, \quad \beta_3 = \zeta_3^2 \cdot u + \zeta_3 \cdot v$$

die Nullstellen von g sind. Dabei beachte man, daß wegen (26)

$$u^3 = -\frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$$

genau dann gilt, wenn

$$v^3 = -\frac{q}{2} \mp \sqrt{\frac{q^2}{4} + \frac{p^3}{27}},$$

so daß es in der Formel für die Nullstellen keine Rolle spielt, ob man in (27) das $\pm$-Zeichen durch Plus oder Minus ersetzt hat.

Aus den Nullstellen von g lassen sich die Nullstellen von f dann wieder leicht ablesen, und wir könnten dies als länglichen verschachtelten Ausdruck in den Koeffizienten von f darstellen.

$\underline{n = 4}$**:** Ein ähnlicher Ansatz von Cardanos Schüler Lodovico Ferrari führte 1545 auch zu einer Lösungsformel für Polynome vierten Grades. Dazu wendet man die Tschirnhausen-Transformation

$$\Phi_{1,-\frac{a_3}{4}} : \mathbb{C}[t] \longrightarrow \mathbb{C}[t] : h \mapsto h\left(t - \frac{a_3}{4}\right)$$

auf f an und erhält ein Polynom der Form

$$g = t^4 + pt^2 + qt + r.$$

Sind nun $\beta_1, \beta_2, \beta_3 \in \mathbb{C}$ die Nullstellen des Polynoms

$$h = t^3 - 2pt^2 + (p^2 - 4r) \cdot t + q^2 = 0,$$

so sind die vier Zahlen

$$\gamma = \frac{\pm\sqrt{-\beta_1} \pm \sqrt{-\beta_2} \pm \sqrt{-\beta_3}}{2},$$

wobei eine ungerade Anzahl der $\pm$-Zeichen ein Plus ist, und

$$\sqrt{-\beta_1} \cdot \sqrt{-\beta_2} \cdot \sqrt{-\beta_3} = -q$$

gelten muß, genau die Nullstellen von g.

In allen vier Fällen ($n = 1, 2, 3, 4$) erhält man eine Formel zur Bestimmung der Nullstellen von f aus den Koeffizienten von f allein unter Verwendung der Körperoperationen und des Wurzelziehens. Auch wenn die Formeln zunehmend komplizierter werden, liegt die Frage nahe, ob dies auch für Polynome höheren Grades möglich ist.

Beispiel 13.17 (Die Formel von Cardano)
Wir wollen die Nullstellen von

$$f = t^3 + 3t - 4 \in \mathbb{C}[t]$$

mit Hilfe des Verfahrens von Cardano bestimmen. Da das Polynom schon in der Normalform (22) gegeben ist, brauchen wir keine Tschirnhausen-Transformation anzuwenden. Mit $p = 3$ und $q = -4$ ergibt sich aus

$$u = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} = \sqrt[3]{2 + \sqrt{5}} = \sqrt[3]{\sqrt{5} + 2} \in \mathbb{R}$$

und

$$\begin{aligned} -\sqrt[3]{\sqrt{5} - 2} \cdot u &= -\sqrt[3]{\sqrt{5} - 2} \cdot \sqrt[3]{\sqrt{5} + 2} \\ &= -\sqrt[3]{(\sqrt{5} - 2) \cdot (\sqrt{5} + 2)} = -\sqrt[3]{5 - 4} = -1 = -\frac{p}{3} = vu \end{aligned}$$

die Gleichung

$$v = -\frac{3}{3u} = -\frac{1}{\sqrt[3]{\sqrt{5} + 2}} = -\sqrt[3]{\sqrt{5} - 2} \in \mathbb{R}$$

Die Nullstellen von f berechnen sich also als

$$\beta_1 = \sqrt[3]{\sqrt{5} + 2} - \sqrt[3]{\sqrt{5} - 2}.$$

sowie

$$\beta_2 = \sqrt[3]{\sqrt{5} + 2} \cdot e^{\frac{2\pi i}{3}} - \sqrt[3]{\sqrt{5} - 2} \cdot e^{\frac{4\pi i}{3}}$$

und

$$\beta_3 = \sqrt[3]{\sqrt{5} + 2} \cdot e^{\frac{4\pi i}{3}} - \sqrt[3]{\sqrt{5} - 2} \cdot e^{\frac{2\pi i}{3}}.$$

Die erste der beiden Nullstellen ist reell, die anderen beiden sind es nicht. Aus

$$f(1) = 1^3 + 3 \cdot 1 - 4 = 0$$

folgt aber auch, daß 1 eine reelle Nullstelle von f ist, und wir erhalten die nicht offensichtliche Gleichung

$$\beta_1 = \sqrt[3]{\sqrt{5}+2} - \sqrt[3]{\sqrt{5}-2} = 1.$$

Die Formeln von Cardano liefern uns also nicht unbedingt eine einfache Darstellung der Nullstellen.

Definition 13.18 (Radikalerweiterung)

a. Eine Körpererweiterung L/K heißt *Radikalerweiterung*, wenn

$$L = K(\alpha_1, \ldots, \alpha_n)$$

mit

$$\alpha_i^{k_i} \in K(\alpha_1, \ldots, \alpha_{i-1})$$

für ein geeignetes $k_i \in \mathbb{Z}_{>}0$, $i = 1, \ldots, n$, d. h. L entsteht aus K durch sukzessive Adjunktion von Wurzeln.

b. Ein Polynom $f \in K[t]$ heißt *durch Radikale auflösbar* über K, wenn es eine Radikalerweiterung in L/K gibt, so daß f in L in Linearfaktoren zerfällt.

Bemerkung 13.19 (Auflösbarkeit durch Radikale)

a. Die Frage am Ende von Bemerkung 13.16 können wir nun wie folgt konkretisieren. Sei

$$f = a_n t^n + a_{n-1} t^{n-1} + \ldots + a_0 \in \mathbb{C}[t]$$

gegeben und ist

$$K = \mathbb{Q}(a_0, \ldots, a_n),$$

ist dann $f \in K[t]$ über K durch Radikale auflösbar?

b. Ist K ein Teilkörper von $\mathbb{C}$ und $f \in K[t]$ ein Polynom vom Grad

$$\deg(f) \leq 4,$$

so zeigen die Lösungsformeln in Bemerkung 13.16, daß f durch Radikale auflösbar ist.

Für die Klärung der Frage ist der folgende Satz von zentraler Bedeutung, der zudem erläutert, weshalb auflösbare Gruppen auflösbar heißen.

Satz 13.20 (Auflösbarkeit durch Radikale)
Für ein Polynom $f \in K[t]$ *mit* $\mathrm{char}(K) = 0$ *sind die folgenden Aussagen gleichwertig:*

a. f *ist über* K *durch Radikale auflösbar.*

b. Die Galoisgruppe $\mathrm{Gal}\,(\mathrm{ZFK}_K(f)/K)$ *ist auflösbar.*

Für den Beweis des Satzes benötigen wir zwei Hilfsaussagen.

Lemma 13.21 (Der Zerfällungskörper von $t^n - \alpha^n$)
Es sei K *ein Körper mit* $\mathrm{char}(K) = 0$ *und* $\zeta_n = e^{\frac{2\pi i}{n}} \in K$.

a. Ist $L = K(\alpha)$ *mit* $\alpha^n \in K$*, dann ist* $L = \mathrm{ZFK}_K(t^n - \alpha^n)$ *galoissch über* K *und*

$$\mathrm{Gal}\,(L/K) \leq \mathbb{Z}_n$$

ist eine zyklische Gruppe deren Ordnung n *teilt.*

b. Ist L/K *galoissch mit* $\mathrm{Gal}\,(L/K) \cong \mathbb{Z}_n$ *und* n *prim, so ist* $L = K(\alpha)$ *mit* $\alpha^n \in K$.

Beweis:

a. Das Polynom $f = t^n - \alpha^n \in \mathbb{K}[t]$ faktorisiert als

$$f = \big(t - \zeta_n^0\alpha\big) \cdot \big(t - \zeta_n^1\alpha\big) \cdot \ldots \cdot \big(t - \zeta_n^{n-1}\alpha\big).$$

Da mit ζ_n auch die Potenzen von ζ_n in K und damit in L liegen, zerfällt f über L und

$$L = K(\alpha) = K\big(\alpha, \zeta_n\alpha, \ldots, \zeta_n^{n-1}\alpha\big) = \mathrm{ZFK}_K(f)$$

ist der Zerfällungskörper von f über K. Da f wegen $\mathrm{char}(K) = 0$ auch separabel ist, ist L/K nach Satz 9.6 galoissch.
Nach Proposition 9.1 permutiert ein Element $\sigma \in \mathrm{Gal}\,(L/K)$ die Nullstellen f und wir können die folgende Abbildung definieren

$$\tau : \mathrm{Gal}\,(L/K) \longrightarrow \mathbb{Z}_n : \sigma \mapsto \overline{k},$$

wenn

$$\sigma(\alpha) = \zeta_n^k\alpha,$$

wobei wir beachten, daß dabei die Restklasse von k in $\mathbb{Z}_n$ eindeutig festgelegt ist. Wegen

$$\zeta_n^i \in K = \mathrm{Fix}\,(L, \mathrm{Gal}\,(L/K))$$

für $i = 1, \ldots, n$ gilt dann für $\sigma, \pi \in \mathrm{Gal}\,(L/K)$ mit $\sigma(\alpha) = \zeta_n^k\alpha$ und $\pi(\alpha) = \zeta_n^l$ auch

$$\sigma \circ \pi(\alpha) = \sigma(\zeta_n^l\alpha) = \zeta_n^l\sigma(\alpha) = \zeta_n^l\zeta_n^k\alpha = \zeta_n^{l+k}\alpha$$

und damit

$$\tau(\sigma \circ \pi) = \overline{l + k} = \overline{k} + \overline{l} = \tau(\sigma) + \tau(\pi),$$

d. h. τ ist ein Gruppenhomomorphismus. Ferner ist σ durch das Bild von α festgelegt, so daß τ auch injektiv ist. Damit ist $\mathrm{Gal}\,(L/K)$ isomorph zu einer Untergruppe der zyklischen Gruppe $\mathbb{Z}_n$ und ist als solche selbst wieder zyklisch mit einer Ordnung, die $|\mathbb{Z}_n| = n$ teilt (siehe [**Mar08a**, Kor. 4.62]).

b. Nach Voraussetzung ist die Galoisgruppe

$$\mathrm{Gal}\,(L/K) = \langle\sigma\rangle$$

von einem Element σ der Ordnung n erzeugt. Als K-Automorphismus von L ist

$$\sigma : L \longrightarrow L$$

insbesondere ein K-Vektorraumisomorphismus und aus

$$\sigma^n = \mathrm{id}_L$$

folgt, daß das Minimalpolynom μ_σ von σ ein Teiler des Polynoms

$$t^n - 1 = \left(t - \zeta_n^0\right) \cdot \left(t - \zeta_n^1\right) \cdot \ldots \cdot \left(t - \zeta_n^n\right) \in K[t]$$

ist. Dieses zerfällt über K in paarweise verschiedene Linearfaktoren, so daß σ als K-lineare Abbildung diagonalisierbar ist (siehe [**Mar11**, Satz 33.21]). Da n die Ordnung von σ und eine Primzahl ist und da alle Eigenwerte von σ n-te Einheitswurzeln sind, muß einer der Eigenwerte eine primitive n-te Einheitswurzel $\zeta \in K$ sein.
Sei nun $0 \neq \alpha \in L$ ein Eigenvektor von σ zum Eigenwert $\zeta \in K$, so gilt

$$\sigma(\alpha) = \zeta\alpha$$

und somit

$$\sigma(\alpha^n) = \sigma(\alpha)^n = \zeta^n\alpha^n = \alpha^n.$$

Da die Galoisgruppe von L/K von σ erzeugt wird, folgt damit

$$\alpha^n \in \mathrm{Fix}\left(L, \mathrm{Gal}\left(L/K\right)\right) = K,$$

wobei wir für die letzte Gleichheit ausnutzen, daß L/K galoissch ist (siehe Korollar 10.6).
Wir wollen nun zeigen, daß

$$L = K(\alpha)$$

gilt, wobei die Inklusion $\supseteq$ klar ist. Außerdem gilt

$$|K(\alpha) : K| \;\Big|\; |L : K| = |\,\mathrm{Gal}\,(L/K)\,| = n,$$

woraus

$$|K(\alpha) : K| \in \{1, n\}$$

folgt, da wir n als Primzahl vorausgesetzt haben. Wäre der Grad der Körpererweiterung 1, so müßte $\alpha \in K$ gelten, so daß 1 der Eigenwert von α wäre. Also gilt

$$|K(\alpha) : K| = n = |L : K|,$$

woraus die Gleichheit $L = K(\alpha)$ folgt.

□

Bemerkung 13.22
Die Bedingung n prim in Teil b. von Lemma 13.21 ist überflüssig. Mit etwas Aufwand kann man zeigen, daß das Polynom

$$f = t^n - \alpha^n \in K[t]$$

irreduzibel über K ist. Dann ist f aber das Minimalpolynom von α über K und die Gleichheit der Grade im Beweis folgt wiederum.

Lemma 13.23 (Translationssatz)
Es seien L *und* N *Zwischenkörper von* M/K *und es sei* N/K *galoissch. Dann sind auch* $N/L \cap N$ *und* $L(N)/L$ *galoissch mit*

$$\mathrm{Gal}\,(L(N)/L) \cong \mathrm{Gal}\,(N/L \cap N)$$

Das Diagramm in Abbildung 1 veranschaulicht die Lage der Körper zueinander.

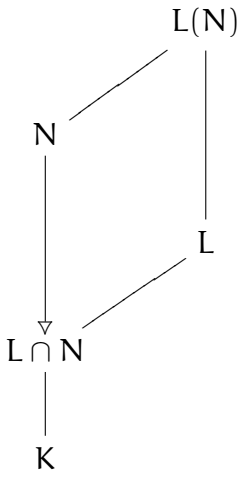

Abbildung 1. Körperdiagramm im Translationssatz

Beweis: Da N/K galoissch ist, ist $N/L \cap N$ nach dem Hauptsatz der Galoistheorie 10.7 ebenfalls galoissch und es gibt nach Satz 9.6 ein separables Polynom

$$f = (t - \alpha_1) \cdot \ldots \cdot (t - \alpha_n) \in K[t],$$

so daß

$$N = \mathrm{ZFK}_K(f) = K(\alpha_1, \ldots, \alpha_n)$$

der Zerfällungskörper von f über K ist. Dann ist aber

$$L(N) = L(\alpha_1, \ldots, \alpha_n) = \mathrm{ZFK}_L(f)$$

der Zerfällungskörper von f über L, und nach Satz 9.6 ist $L(N)/L$ mithin auch galoissch.

Ist $\sigma \in \mathrm{Gal}\,(L(N)/L) \leq \mathrm{Gal}\,(L(N)/K)$, so gilt mit Satz 7.3

$$\sigma(N) = N,$$

da N/K normal ist. Dies erlaubt es uns, den folgenden Gruppenhomomorphismus

$$\tau : \mathrm{Gal}\,(L(N)/L) \longrightarrow \mathrm{Gal}\,(N/K) : \sigma \mapsto \sigma_{|N}$$

zu definieren. Da σ durch die Bilder der Nullstellen von f festgelegt ist und diese alle in N liegen, ist die Abbildung τ injektiv und somit ist $\mathrm{Gal}\,(L(N)/L)$ isomorph zu einer Untergruppe

$$\mathrm{Gal}\,(L(N)/L) \cong U \leq \mathrm{Gal}\,(N/K)$$

von $\mathrm{Gal}\,(N/K)$. Unter Berücksichtigung des Hauptsatzes der Galoistheorie 10.7 und weil $L(N)/L$ galoissch ist gilt dabei

$$\begin{aligned}\mathrm{Fix}\,(N,U) =&\{\alpha \in N \mid \sigma(\alpha) = \alpha \ \ \forall\, \sigma \in \mathrm{Gal}\,(L(N)/L)\\ =&N \cap \mathrm{Fix}\,(L(N), \mathrm{Gal}\,(L(N)/L)) = N \cap L,\end{aligned}$$

woraus wegen des Hauptsatzes der Galoistheorie unmittelbar

$$U = \mathrm{Gal}\,(N/\mathrm{Fix}\,(N,U)) = \mathrm{Gal}\,(N/L \cap N)$$

folgt. □

Beweis von Satz 13.20: Für den Beweis sei $L = \mathrm{ZFK}_K(f)$ und $n = |L : K|$.

1. Fall: $\zeta_n \in K$: "$\Longrightarrow$": Wenn f durch Radikale auflösbar ist, so ist L Zwischenkörper einer Radikalerweiterung

$$M = K(\alpha_1, \ldots, \alpha_m)$$

von K mit

$$\alpha_i^{k_i} \in K(\alpha_1, \ldots, \alpha_{i-1})$$

für $i = 1, \ldots, m$, k_i minimal. Wir setzen nun

$$K_i := K(\alpha_1, \ldots, \alpha_i)$$

für $i = 0, \ldots, m$ und zeigen durch Induktion nach m, daß $\mathrm{Gal}\,(L/K)$ auflösbar ist.
Für $m = 0$ folgt die Behauptung aus $K = L = M$ und $\mathrm{Gal}\,(L/K) = \{\mathrm{id}_K\}$.
Ist $m > 0$, so hat der Körper

$$L(K_1) = \mathrm{ZFK}_{K_1}(f)$$

als Zwischenkörper der Radikalerweiterung M/K_1 nach Induktion eine auflösbare Galoisgruppe

$$\mathrm{Gal}\,(L(K_1)/K_1) \overset{13.23}{\cong} \mathrm{Gal}\,(L/L \cap K_1)\,,$$

so daß wegen des Translationssatzes 13.23 $\mathrm{Gal}\,(L/L \cap K_1)$ auflösbar ist.
Weil $k_i = \deg(t^{k_i} - \alpha_i^{k_i}) = |K_1 : K|$ ein Teiler von $n = |L : K|$ ist, liegt mit ζ_n auch $\zeta_{k_i} = \zeta_n^{\frac{n}{k_i}} \in K$ in K und wir können Lemma 13.21 anwenden und erhalten, daß die Galoisgruppe $\mathrm{Gal}\,(K_1/K)$ zyklisch ist. Dann ist die Untergruppe $\mathrm{Gal}\,(K_1/L \cap K_1)$ aber ein Normalteiler und aus dem Hauptsatz der Galoistheorie folgt, daß

$$\mathrm{Gal}\,(L \cap K_1/K) \cong \mathrm{Gal}\,(K_1/K) \,/\, \mathrm{Gal}\,(K_1/L \cap K_1)$$

als Faktorgruppe einer zyklischen Gruppe ebenfalls zyklisch ist und daß $L \cap K_1/K$ galoissch ist. Dann ist wegen des Hauptsatzes der Galoistheorie 10.7 aber auch

$$\mathrm{Gal}\,(L/K) \,/\, \mathrm{Gal}\,(L/L \cap K_1) \cong \mathrm{Gal}\,(L \cap K_1/K)\,,$$

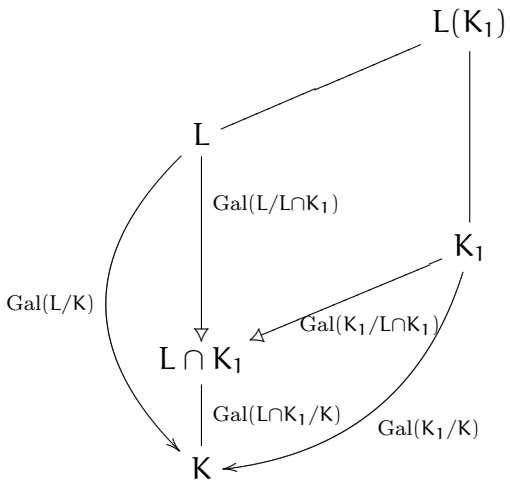

ABBILDUNG 2. Körperdiagramm mit Galoisgruppen, Beweis von 13.20

und diese Gruppe ist somit zyklisch und damit auflösbar.
Wir haben also gezeigt, daß die Gruppe $\mathrm{Gal}\,(L/K)$ einen Normalteiler besitzt, der auflösbar ist und dessen Faktorgruppe auflösbar ist. Nach Proposition 13.7 ist dann die Gruppe $\mathrm{Gal}\,(L/K)$ aber auch selbst auflösbar.
"$\Longleftarrow$": Wir wollen nun umgekehrt voraussetzen, daß $G_0 := \mathrm{Gal}\,(L/K)$ galoissch ist. Dann gibt es nach Satz13.11 eine Subnormalteilerkette

$$\mathbb{1} = G_m \trianglelefteq G_{m-1} \trianglelefteq \ldots \trianglelefteq G_0,$$

so daß G_{i-1}/G_i zyklisch von Primzahlordnung $p_i \in \mathbb{P}$ ist für $i = 1, \ldots, m$. Wir definieren dann Zwischenkörper

$$K_i := \mathrm{Fix}\,(L, G_i) \leq L$$

von L/K und erhalten wegen Korollar 10.6

$$K = K_0 \leq K_1 \leq \ldots \leq K_m = L.$$

Aus dem Hauptsatz der Galoistheorie 10.7 wissen wir, daß L/K_{i-1} galoissch ist mit Galoisgruppe

$$\mathrm{Gal}\,(L/K_{i-1}) = \mathrm{Gal}\,(L/\mathrm{Fix}\,(L, G_{i-1})) = G_{i-1}.$$

Da G_i ein Normalteiler dieser Gruppe ist, ist mithin

$$K_i = \mathrm{Fix}\,(L, G_i)$$

galoissch über K_{i-1} mit zyklischer Galoisgruppe

$$\mathrm{Gal}\,(K_i/K_{i-1}) \cong \mathrm{Gal}\,(L/K_{i-1}) \,/\, \mathrm{Gal}\,(L/K_i) = G_{i-1}/G_i.$$

Die Primzahl $p_i = |G_{i-1}/G_i|$ ist nach dem Satz von Lagrange ein Teiler von

$$n = |L : K| = |\,\mathrm{Gal}\,(L/K)\,| = |G_0|,$$

so daß mit ζ_n auch $\zeta_{p_i} = \zeta_n^{\frac{n}{p_i}} \in K$ in K liegt, und aus Lemma 13.21 folgt dann, daß

$$K_i = K_{i-1}(\alpha_i)$$

mit

$$\alpha_i^{p_i} \in K_{i-1}$$

für ein geeignetes $\alpha_i \in K_i$. Damit ist dann

$$L = K(\alpha_1, \ldots, \alpha_m)$$

eine Radikalerweiterung von K.

2. Fall: $\zeta_n \notin K$**:** Wir betrachten nun das Körperdiagramm in Abbildung 3.

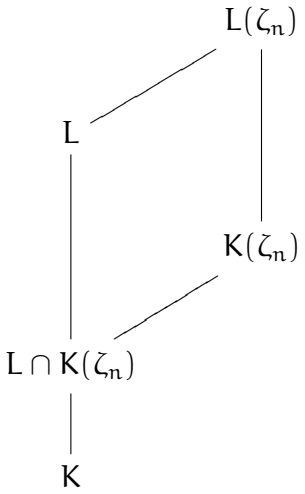

ABBILDUNG 3. Körperdiagramm zu L/K und $L(\zeta_n)/K(\zeta_n)$

"$\Longrightarrow$": Ist L in einer Radikalerweiterung

$$M = K(\alpha_1, \ldots, \alpha_m)$$

von K mit

$$\alpha_i^{k_i} \in K(\alpha_1, \ldots, \alpha_{i-1}$$

enthalten, so ist

$$M(\zeta_n) = K(\zeta_n)(\alpha_1, \ldots, \alpha_m)$$

eine Radikalerweiterung von $K(\zeta_n)$, die $L(\zeta_n)$ enthält. Diese erfüllt die Voraussetzungen des 1. Falls, so daß

$$\mathrm{Gal}\,(L(\zeta_n)/K(\zeta_n)) \overset{13.23}{\cong} \mathrm{Gal}\,(L/L \cap K(\zeta_n))$$

auflösbar ist.
Nach Bemerkung 11.12 ist $K(\zeta_n)/K$ galoissch mit abelscher Galoisgruppe $\mathrm{Gal}\,(K(\zeta_n)/K)$. Also ist die Untergruppe

$$\mathrm{Gal}\,(K(\zeta_n)/L \cap K(\zeta_n)) \trianglelefteq \mathrm{Gal}\,(K(\zeta_n)/K)$$

ein Normalteiler, so daß

$$L \cap K(\zeta_n)/K$$

nach dem Hauptsatz der Galoistheorie 10.7 galoissch ist und

$$\mathrm{Gal}\,(L \cap K(\zeta_n)/K) \cong \mathrm{Gal}\,(K(\zeta_n)/K) \,/\, \mathrm{Gal}\,(K(\zeta_n)/L \cap K(\zeta_n))$$

abelsch und damit nach Beispiel 13.6 auflösbar ist. Daraus folgt mit demselben Argument dann wiederum, daß

$$\mathrm{Gal}\,(L/L \cap K(\zeta_n)) \trianglelefteq \mathrm{Gal}\,(L/K)$$

ein Normalteiler ist und daß

$$\mathrm{Gal}\,(L \cap K(\zeta_n)/K) \cong \mathrm{Gal}\,(L/K) \,/\, \mathrm{Gal}\,(L/L \cap K(\zeta_n))$$

gilt. Also ist $\mathrm{Gal}\,(L/K)$ als Gruppe mit auflösbarem Normalteiler $\mathrm{Gal}\,(L/L \cap K(\zeta_n))$ und auflösbarer zugehöriger Faktorgruppe selbst auflösbar ist, siehe Proposition 13.7.
"$\Longleftarrow$": Ist $\mathrm{Gal}\,(L/K)$ auflösbar, so ist die Untergruppe

$$\mathrm{Gal}\,(L/L \cap K(\zeta_n)) \leq \mathrm{Gal}\,(L/K)$$

nach Proposition 13.7 auflösbar und nach dem Translationssatz 13.23 ist dann auch

$$\mathrm{Gal}\,(L(\zeta_n)/K(\zeta_n)) \cong \mathrm{Gal}\,(L/L \cap K(\zeta_n))$$

auflösbar. Auf diese Körpererweiterung ist der 1. Fall anwendbar und wir erhalten, daß $L(\zeta_n)$ in einer Radikalerweiterung

$$M = K(\zeta_n)(\alpha_1, \ldots, \alpha_m)$$

von $K(\zeta_n)$ mit

$$\alpha_i^{k_i} \in K(\zeta_n, \alpha_1, \ldots, \alpha_{i-1})$$

für $i = 1, \ldots, m$ enthalten ist. Aber dann ist M wegen

$$\zeta_n^n = 1 \in K$$

auch eine Radikalerweiterung von K, so daß L in einer Radikalerweiterung von K enthalten ist.

□

Bemerkung 13.24 (Gleichungen vom Grad höchstens 4 sind auflösbar.)
Satz 13.20 ist ein zu Bemerkung 13.16 alternatives Argument, um zu sehen, daß jedes Polynom $f \in K[t]$ vom Grad höchstens 4 über einem Teilkörper von $\mathbb{C}$ durch Radikale auflösbar ist, da die Galoisgruppe des Zerfällungskörpers über K als Untergruppe der symmetrischen Gruppe $\mathbb{S}_4$ (siehe Proposition 9.1) auflösbar ist (siehe Beispiel 13.6 und Proposition 13.7).

Satz 13.25 (Abel-Ruffini)
Das Polynom $f = t^5 - 4t + 2 \in \mathbb{Q}[t]$ *ist über* $\mathbb{Q}$ *nicht durch Radikale auflösbar, weil*

$$\mathrm{Gal}\,(\mathrm{ZFK}_{\mathbb{Q}}(f)/\mathbb{Q}) \cong \mathbb{S}_5.$$

Beweis: Aus dem Eisensteinkriterium 2.2 folgt, daß f irreduzibel über $\mathbb{Z}$ und damit auch über $\mathbb{Q}$ ist (siehe Satz 2.4). Wir betrachten die folgende Wertetabelle:

t	-2	-1	1	2
$f(t)$	-22	5	-1	26

Aus dem Zwischenwertsatz (siehe [**Mar11**, Satz 14.12]) folgt dann, daß f mindestens drei reelle Nullstellen besitzt. Die Ableitung

$$f' = 5t^4 - 4$$

hat nur zwei reelle Nullstelle

$$t = \pm\sqrt[4]{\frac{4}{5}},$$

so daß f wegen des Satzes von Rolle (siehe [**Mar11**, Satz 18.5]) auch nicht mehr als drei reelle Nullstellen haben kann. Aufgabe 13.27 liefert dann

$$\mathrm{Gal}\,(L/\mathbb{Q}) = \mathbb{S}_5.$$

Mithin ist die Galoisgruppe nach Korollar 13.8 nicht auflösbar, und wegen Satz 13.20 ist dann f nicht durch Radikale auflösbar. □

Bemerkung 13.26 (Lösungsformeln für Grad 5?)
Nachdem Cardano und Ferrari erfolgreich Lösungsformeln für Polynome vom Grad 3 und 4 angegeben hatten, haben die Mathematiker lange vergebens nach vergleichbaren Formeln für Polynome vom Grad 5 oder höher gesucht. Satz 13.25 zeigt, weshalb. Eine solche allgemeine Formel kann es nicht geben.

Aufgaben

Aufgabe 13.27 (Satz von Abel-Ruffini)

a. Sind $\tau \in \mathbb{S}_p$ eine Transposition und $\pi \in \mathbb{S}_p$ ein p-Zykel mit $p \in \mathbb{P}$, so gilt

$$\langle \tau, \pi \rangle = \mathbb{S}_p.$$

b. Ist $f \in \mathbb{Q}[t]$ ein irreduzibles Polynom von ungeradem Primzahlgrad p mit genau zwei nicht-reellen Nullstellen und $L = \mathrm{ZFK}_{\mathbb{Q}}(f)$. Zeige,

$$\mathrm{Gal}\,(L/\mathbb{Q}) \cong \mathbb{S}_p.$$

Literaturverzeichnis

[Dec14] Wolfram Decker, *Einführung in die Algebra*, Vorlesungsskript, TU Kaiserslautern, 2014.

[DH92] Klaus Doerk and Trevor Hawkes, *Finite soluble groups*, De Gruyter Expositions in Mathematics, no. 4, De Gruyter, 1992.

[FT63] Walter Feit and John G. Thompson, *Solvability of groups of odd order*, Pacific Journal of Mathematics **13** (1963), 755–1029.

[Gar86] D. J. H. Garling, *A course in Galois theory*, Cambridge University Press, 1986.

[Gat10] Andreas Gathmann, *Einführung in die Algebra*, Vorlesungsskript, TU Kaiserslautern, 2010.

[Gor82] Daniel Gorenstein, *Finite simple groups*, Plenum Print, New York, 1982.

[Gor83] ———, *The classification of finite simple groups*, vol. 1, Plenum Print, New York, 1983.

[Gor96] ———, *The classification of finite simple groups*, vol. 2, Plenum Print, New York, 1996.

[Hup67] Bertram Huppert, *Endliche Gruppen*, vol. 1, Die Grundlehren der mathematischen Wissenschaften, no. 134, Springer, Berlin, 1967.

[Kur77] Hans Kurzweil, *Endliche Gruppen*, Springer Hochschultext, Springer, 1977.

[Lei96] Felix Leinen, *Algebra I & II*, Vorlesungsausarbeitung, Johannes Gutenberg-Universität Mainz, 1995/96.

[Mal11] Gunter Malle, *Einführung in die Algebra*, Vorlesungsausarbeitung, 2011.

[Mar08a] Thomas Markwig, *Algebraische Strukturen*, Vorlesungsskript, TU Kaiserslautern, 2008.

[Mar08b] ———, *Elementarmathematik vom höheren Standpunkt aus*, Vorlesungsskript, TU Kaiserslautern, 2008.

[Mar11] ———, *Grundlagen der Mathematik*, Vorlesungsskript, TU Kaiserslautern, 2011.

[PS10] Gerhard Pfister and Stefan Steidel, *Einführung in die Algebra*, Vorlesungsskript WS 2009/10, TU Kaiserslautern, 2010.