Algebra

Thomas Markwig
Fachbereich Mathematik
Universität Tübingen

Vorlesungsskript

Sommersemester 2019

Inhaltsverzeichnis

Einleitung

Die vorliegende Ausarbeitung zur Vorlesung Algebra wird im Verlauf der Vorlesung des Sommersemesters 2019 mit Inhalten gefüllt, ergänzt und überarbeitet. Die jeweils aktualisierte Fassung wird auf der Webseite zur Vorlesung zur Verfügung gestellt. Sie wird im wesentlichen wiedergeben, was während der Vorlesung an die Tafel geschrieben wird. Die Ausarbeitung ersetzt in keiner Weise ein Lehrbuch und schon gar nicht den Besuch der Vorlesung.

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.

§ 1 Faktorielle Ringe und das Lemma von Gauß

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 seine Definition sowie die einiger weiterer grundlegender Begriffe der Vollständigkeit halber aber noch einmal wiederholen und erinnern an einige wichtige Eigenschaften in faktoriellen Ringen.

A) Faktorielle Ringe

Definition 1.1 (Primfaktorzerlegung)
Es sei R ein Integritätsbereich und R^* bezeichne die Gruppe der Einheiten in R.

a. Die Elemente $a, b \in R$ heißen *assoziiert*, wenn es ein $u \in R^*$ gibt mit $a = u \cdot b$.

b. Ein Element $0 \neq p \in R \setminus R^*$ heißt *irreduzibel*, falls aus $p = a \cdot b$ mit $a, b \in R$ schon $a \in R^*$ oder $b \in R^*$ folgt.

c. Ein Element $0 \neq p \in R \setminus R^*$ heißt *prim*, falls aus p teilt $a \cdot b$ mit $a, b \in R$ schon p teilt a oder p teilt b folgt.

d. 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.

e. 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 $0 \neq p \in R \setminus R^*$.

a. Genau dann ist p prim, wenn $u \cdot p$ prim ist.

b. Wenn p prim ist, dann ist p auch irreduzibel. Die Umkehrung gilt i. a. nicht. (Siehe [Mar08a, Satz 7.16-17])

Satz 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*

$$a = u \cdot \prod_{p \in \mathbb{P}_R} p^{n_p(a)} \tag{1}$$

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. *Mit den Bezeichnungen aus c. gilt für $a, b \in R \setminus \{0\}$:*

$$a \mid b \quad \Longleftrightarrow \quad n_p(a) \leq n_p(b) \;\; \forall p \in \mathbb{P}_R.$$

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 7.19].

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

d. Das folgt unmittelbar mit Hilfe der Darstellung (1) für a und b.

□

Beispiel 1.5

a. In $\mathbb{Z}$ ist die Menge $\mathbb{P}_{\mathbb{Z}} = \{p \in \mathbb{Z} \mid p > 0, p \text{ ist Primzahl}\}$ der positiven Primzahlen ein vollständiges Vertretersystem der Primzahlen und

$$-48 = (-1) \cdot 2^4 \cdot 3^1$$

ist die Primfaktorzerlegung von $z = -48$ aus Gleichung (1). Es gilt $n_2(-48) = 4$, $n_3(-48) = 1$ und $n_p(-48) = 0$ für $p \in \mathbb{P}_{\mathbb{Z}} \setminus \{2, 3\}$.

b. Ist K ein Körper, so ist die Menge

$$\mathbb{P}_{K[t]} = \{p \in K[t] \mid p \text{ ist irreduzibel und normiert}\}$$

der irreduziblen, normierten Polynome ein vollständiges Vertretersystem der Primelemente. Für $K = \mathbb{R}$ ist

$$2t^3 - 4t^2 + 2t - 4 = 2 \cdot (t^2 + 1) \cdot (t - 2)$$

die Primfaktorzerlegung von $f = 2t^3 - 4t^2 + 2t - 4$ aus Gleichung (1) und es gilt etwa $n_{t-2} = 1$.

Wir wollen nun den Begriff eines größten gemeinsamen Teilers und eines kleinsten gemeinsamen Vielfachen zweier Elemente etwas erweitern.

Definition 1.6 (Größte gemeinsame Teiler und kleinste gemeinsame Vielfache)
Sei R ein Integritätsbereich und seien $a_1, \ldots, a_n \in R$.

a. Ein Element $g \in R$ heißt *größter gemeinsamer Teiler* von $a_1, \ldots, a_n$, falls die folgenden beiden Eigenschaften erfüllt sind:

(i) $g \mid a_i$ für alle $i = 1, \ldots, n$.

(ii) Für alle $h \in R$ mit $h \mid a_i$ für alle $i = 1, \ldots, n$ gilt schon $h \mid g$.

Wir bezeichnen mit $\mathrm{ggT}(a_1, \ldots, a_n)$ die Menge der größten gemeinsamen Teiler von $a_1, \ldots, a_n$ in R.

b. Ein Element $k \in R$ heißt *kleinstes gemeinsames Vielfaches* von $a_1, \ldots, a_n$, falls die folgenden beiden Eigenschaften erfüllt sind:

(i) $a_i \mid k$ für alle $i = 1, \ldots, n$.

(ii) Für alle $l \in R$ mit $a_i \mid l$ für alle $i = 1, \ldots, n$ gilt schon $k \mid l$.

Wir bezeichnen mit $\mathrm{kgV}(a_1, \ldots, a_n)$ die Menge der kleinsten gemeinsamen Vielfachen von $a_1, \ldots, a_n$ in R.

Proposition 1.7 (Größte gemeinsame Teiler und kleinste gemeinsame Vielfache)
Es sei R *ein Integritätsbereich und seien* $a_1, \ldots, a_n \in R \setminus \{0\}$.

a. *Je zwei größte gemeinsame Teiler von* $a_1, \ldots, a_n$ *in* R *sind zueinander assoziiert, und ebenso sind je zwei kleinste gemeinsame Vielfache von* $a_1, \ldots, a_n$ *in* R *zueinander assoziiert.*

b. *Ist* R *ein faktorieller Ring und* $\mathbb{P}_R$ *ein vollständiges Vertretersystem für die Primelemente in* R*, dann ist*

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

ein größter gemeinsamer Teiler von $a_1, \ldots, a_n$ *in* R *und*

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

ein kleinstes gemeinsames Vielfaches von $a_1, \ldots, a_n$ *in* R.
Insbesondere existieren größte gemeinsame Teiler und kleinste gemeinsame Vielfache in faktoriellen Ringen stets.

Beweis:

a. Für $g, h \in \mathrm{ggT}(a_1, \ldots, a_n)$ gilt $g \mid h$ und $h \mid g$. Es gibt also $u, v \in R$ mit $h = u \cdot g$ und $g = v \cdot h$, woraus

$$1 \cdot h = h = u \cdot g = u \cdot v \cdot h \tag{2}$$

folgt. Da h ein Teiler der a_i ist und $a_i \neq 0$ gilt, ist h nicht 0 und wir können im Integritätsbereich R den Faktor h kürzen, womit wir

$$1 = u \cdot v$$

erhalten. Also sind u und v Einheiten, und g und h sind assoziiert.
Der Beweis für kleinste gemeinsame Vielfach geht analog.

b. Wegen Satz 1.4 d. ist g genau dann ein größter gemeinsamer Teiler von $a_1, \ldots, a_n$, wenn die folgenden beiden Eigenschaften erfüllt sind:
   (i) $n_p(g) \leq n_p(a_i)$ für alle $i = 1, \ldots, n$ und alle $p \in \mathbb{P}_R$ und
   (ii) wenn $n_p(h) \leq n_p(a_i)$ für alle $i = 1, \ldots, n$, dann ist $n_p(h) \leq n_p(g)$ für alle $p \in \mathbb{P}_R$.

   Mithin muß

$$n_p(g) = \min\{n_p(a_1), \ldots, n_p(a_n)\}$$

   für alle $p \in \mathbb{P}_R$ gelten. Mithin ist

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

   Die Aussage für kleinste gemeinsame Vielfache zeigt man analog.

□

B) Das Lemma von Gauß

Die zentrale Aussage, die wir in diesem Abschnitt beweisen wollen, ist Satz 1.18 und wird als Lemma von Gauß bezeichnet. Der Beweis erfordert, daß wir den Koeffizientenbereich R der betrachteten Polynome erweitern. Wir werden deshalb zunächst die für den Beweis benötigten Begriffe einführen und einige Hilfsaussagen herleiten, bevor wir den Abschnitt dem Satz und seinem Beweis abschließen.

Definition und Satz 1.8 (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 1.9 (Primitives Polynom und Inhalt eines Polynoms)
Es sei R ein Integritätsbereich und $0 \neq f = \sum_{i=0}^{n} a_i t^i \in R[t]$ ein Polynom.

a. Wir nennen f *primitiv*, wenn die Koeffizienten $a_0, \ldots, a_n$ teilerfremd sind, d.h.

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

b. 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 wegen Proposition 1.7 bis auf Multiplikation mit einer Einheit eindeutig bestimmt.

Bemerkung 1.10 (Der Inhalt eines Polynoms)
Es sei $0 \neq f \in R[t]$ ein Polynom.

a. Ist R ein faktorieller Ring, dann ist $\mathrm{cont}_R(f)$ nicht leer.

b. 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 1.11

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 $\mathbb{Q}[t]$. Es gilt $\mathrm{cont}_{\mathbb{Z}}(f) = \{2, -2\}$ und $\mathrm{cont}_{\mathbb{Q}}(f) = \mathbb{Q} \setminus \{0\}$, und $\frac{f}{2} = t + 1$ ist primitiv in $\mathbb{Z}[t]$.

Lemma 1.12
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

$$\frac{a \cdot a_i}{b} \in R \tag{3}$$

für alle $i = 0, \ldots, n$. Ist $p \in R$ ein Primteiler von b, so folgt aus Gleichung (3) 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

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

□

Beispiel 1.13
Für das Polynom

$$f = t^2 + 3t + \frac{1}{5} \in \mathbb{Q}[t]$$

ist $f = c \cdot g$ mit

$$g = 5t^2 + 15t + 1$$

und

$$c = \frac{1}{5} \in \mathbb{Q}$$

die Zerlegung aus Lemma 1.12.

Im weiteren Verlauf werden wir uns mit Eigenschaften wie prim und irreduzibel im Polynomring $R[t]$ über einem faktoriellen Ring R beschäftigen. Dazu wollen wir zuvor in Erinnerung rufen, daß wir die Einheiten in $R[t]$ kennen, wenn R ein Integritätsbereich ist.

Bemerkung 1.14 (Einheiten im Polynomring)
Ist R ein Integritätsbereich, dann gilt für Polynome $f, g \in R[t]$ die Gradformel

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

und

$$R[t]^* = R^*$$

ist die Menge der Einheiten im Polynomring $R[t]$ (siehe [Mar08a, Beispiel 7.2]).

Lemma 1.15
Ist R ein Integritätsbereich 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

$$c_k = \sum_{l=0}^{k} a_l \cdot b_{k-l} \tag{4}$$

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

$$a_{i_0} \cdot b_{j_0} \overset{(4)}{=} c_{i_0+j_0} - \sum_{l=0}^{i_0-1} a_l \cdot b_{i_0+j_0-l} - \sum_{l=i_0+1}^{i_0+j_0} a_l \cdot b_{i_0+j_0-l},$$

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 1.16 (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 1.15 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 1.17
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 Lemma 1.12 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 1.16 primitiv ist. Aus Lemma 1.12 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. □

Satz 1.18 (Lemma von Gauß)
Ist R ein faktorieller Ring, so ist auch $R[t]$ faktoriell.

Beweis: 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 1.15 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 Lemma 1.12 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 1.17 ist das primitive Polynom p_i dann auch prim in $R[t]$.

Zudem wissen wir aus Lemma 1.16, 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 Lemma 1.12

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

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 1.15 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 $R[t]$. □

Beispiel 1.19 (Faktorielle Polynomringe)

a. Der Polynomring $\mathbb{Z}[t]$ ist faktoriell.

b. Ist K ein Körper, dann ist der Polynomring $K[x_1, \ldots, x_n]$ in n Veränderlichen faktoriell. Dies folgt mittels Induktion aus dem Lemma von Gauß 1.18 wegen $K[x_1, \ldots, x_n] = K[x_1, \ldots, x_{n-1}][x_n]$.

C) Allgemeine Polynomringe

Im letzten Beispiel haben wir Polynomringe in endlich vielen Veränderlichen betrachtet und gesehen, wie man diese rekursiv definieren kann. Dies wollen wir im vorliegenden Abschnitt verallgemeinern auf eine beliebige Anzahl an Veränderlichen.

Definition und Bemerkung 1.20 (Allgemeine Polynomringe)
Sei R ein kommutativer Ring mit Eins und Λ sei eine beliebige Menge. Für jedes $\lambda \in \Lambda$ sei x_λ eine Veränderliche, und für eine endliche Teilmenge $\Omega = \{\lambda_1, \ldots, \lambda_k\} \subseteq \Lambda$ bezeichne

$$R[x_\lambda \mid \lambda \in \Omega] = \left\{ \sum_{\alpha=(\alpha_1,\ldots,\alpha_k)\in\mathbb{N}^k} a_\alpha \cdot x_{\lambda_1}^{\alpha_1} \cdot \ldots \cdot x_{\lambda_k}^{\alpha_k} \;\middle|\; a_\alpha \in R, \text{ nur endlich viele } a_\alpha \neq 0 \right\}$$

den Polynomring über R in den endlich vielen Veränderlichen x_λ mit $\lambda \in \Omega$. Die Addition und Multiplikation der Polynome sind dabei wie folgt gegeben

$$\left(\sum_\alpha a_\alpha \cdot x_{\lambda_1}^{\alpha_1} \cdot \ldots \cdot x_{\lambda_k}^{\alpha_k}\right) + \left(\sum_\alpha b_\alpha \cdot x_{\lambda_1}^{\alpha_1} \cdot \ldots \cdot x_{\lambda_k}^{\alpha_k}\right) = \sum_\alpha (a_\alpha + b_\alpha) \cdot x_{\lambda_1}^{\alpha_1} \cdot \ldots \cdot x_{\lambda_k}^{\alpha_k}$$

und

$$\left(\sum_\alpha a_\alpha \cdot x_{\lambda_1}^{\alpha_1} \cdot \ldots \cdot x_{\lambda_k}^{\alpha_k}\right) \cdot \left(\sum_\alpha b_\alpha \cdot x_{\lambda_1}^{\alpha_1} \cdot \ldots \cdot x_{\lambda_k}^{\alpha_k}\right) = \sum_\alpha \left(\sum_{\beta+\gamma=\alpha} a_\beta \cdot b_\gamma\right) \cdot x_{\lambda_1}^{\alpha_1} \cdot \ldots \cdot x_{\lambda_k}^{\alpha_k}.$$

Wir beachten, daß $R[x_\lambda \mid \lambda \in \Omega]$ für $\Omega \subseteq \Omega'$ ein Unterring von $R[x_\lambda \mid \lambda \in \Omega']$ ist. Daraus folgt unmittelbar, daß

$$R[\Lambda] := R[x_\lambda \mid \lambda \in \Lambda] := \bigcup_{\substack{\Omega \subset \Lambda \\ |\Omega| < \infty}} R[x_\lambda \mid \lambda \in \Omega]$$

ein kommutativer Ring mit Eins ist, den wir einen *(allgemeinen) Polynomring* nennen wollen. Wir werden die Kurznotation $R[\Lambda]$ nur verwenden, wenn wir die Indexmenge mit griechischen Großbuchstaben bezeichnet haben, um Verwechslungen mit anderen K-Algebren zu vermeiden, die analog bezeichnet werden (siehe Bemerkung 4.30).

Zunächst schauen wir uns die Einheitengruppe und die Primelemente in allgemeinen Polynomringen an, um dann zu zeigen, daß das Lemma von Gauß auch bei der Adjunktion von beliebig vielen Veränderlichen noch gilt.

Lemma 1.21 (Einheiten und Primelemente in allgemeinen Polynomringen)
Sei R ein Integritätsbereich, Λ eine Menge und $\Omega \subseteq \Lambda$ eine endliche Teilmenge.

a. Für die Einheitengruppe von $R[\Lambda]$ gilt $R[\Lambda]^* = R^*$.

b. Genau dann ist $0 \neq p \in R[\Omega]$ prim in $R[\Omega]$, wenn es prim in $R[\Lambda]$ ist.

Beweis: Im Beweis nutzen wir wesentlich aus, daß jedes Element in $R[\Lambda]$ nur von endlich vielen Veränderlichen abhängt.

a. Ist $f \in R[\Lambda]^*$, so gibt es ein $g \in R[\Lambda]$ mit $f \cdot g = 1$. Dann gibt es aber auch eine endliche Teilmenge $\Omega \subseteq \Lambda$ mit

$$f, g \in R[\Omega]$$

und somit

$$f \in R[\Omega]^*.$$

Aus Bemerkung 1.14 folgt mittels Induktion nach der Anzahl der Veränderlichen aber

$$R[\Omega]^* = R^*.$$

Also ist $f \in R^*$, und umgekehrt sind die Elemente in R^* offenbar Einheiten auch im allgemeinen Polynomring.

b. Wir setzen zunächst voraus, daß p prim in $R[\Omega]$ ist, und betrachten Polynome $f, g \in R[\Lambda]$ für die p ein Teiler des Produktes $f \cdot g$ in $R[\Lambda]$ ist, d.h. es gibt ein Polynom $a \in R[\Lambda]$ mit $a \cdot p = f \cdot g$. Es gibt dann aber eine endliche Obermenge $\Omega' \supseteq \Omega$, so daß

$$a, f, g \in R[\Omega'].$$

Da $R[\Omega']$ aus $R[\Omega]$ durch Adjunktion endlich vieler Veränderlicher entsteht, folgt aus Lemma 1.15 mit Induktion nach der Anzahl der adjungierten Veränderlichen, daß p auch prim in $R[\Omega']$ ist. Also teilt p einen der beiden Faktoren f oder g in $R[\Omega']$ und damit auch in $R[\Lambda]$. Somit ist p prim in $R[\Lambda]$.
Sei nun umgekehrt p prim in $R[\Lambda]$ und p teile ein Produkt $f \cdot g$ mit $f, g \in R[\Omega]$. Da p prim in $R[\Lambda]$ ist teilt p dann ohne Einschränkung f in $R[\Lambda]$, d.h. es gibt ein $a \in R[\Lambda]$ mit

$$p \cdot a = f.$$

Würde a eine Variable x_λ mit $\lambda \in \Lambda \setminus \Omega$ enthalten, so wäre der Grad von f in x_λ auf der linken Seite größer als 0, da R ein Integritätsbereich ist, und auf der rechten Seite gleich 0, was ein offensichtlicher Widerspruch ist. Also gilt schon $a \in R[\Omega]$ und p ist prim in $R[\Omega]$.

□

Proposition 1.22 (Allgemeine Polynomringe sind faktoriell.)
Ist R ein faktorieller Ring und ist Λ eine Menge, so ist $R[\Lambda]$ faktoriell.

Beweis: Sei $0 \neq f \in R[\Lambda]$ keine Einheit, so gibt es eine endliche Teilmenge $\Omega \subseteq \Lambda$ mit

$$0 \neq f \in R[\Omega] \setminus R^*.$$

Aus dem Lemma von Gauß 1.18 folgt mit Induktion, daß $R[\Omega]$ faktoriell ist. Mithin gibt es Primelemente $p_1, \ldots, p_k \in R[\Omega]$ so, daß

$$f = p_1 \cdot \ldots \cdot p_k.$$

Nach Lemma 1.21 sind die p_i auch prim in $R[\Lambda]$. Also ist $R[\Lambda]$ faktoriell. □

Wir wollen den Abschnitt abschließen, indem wir uns die universelle Eigenschaft von allgemeinen Polynomringen für den Fall anschauen, daß der Grundring ein Körper K ist.

Definition 1.23 (K-Algebra)
Es sei K ein Körper und $(R, +, \circ)$ ein (nicht notwendigerweise kommutativer) Ring mit Eins zusammen mit einer Skalarmultiplikation

$$\cdot : K \times R \longrightarrow R,$$

so daß $(R, +, \cdot)$ ein K-Vektorraum ist und die Multiplikation "$\circ$" und die Skalarmultiplikation "$\cdot$" wie folgt miteinander verträglich sind:

$$\lambda \cdot (x \circ y) = (\lambda \cdot x) \circ y = x \circ (\lambda \cdot y) \quad \forall\, \lambda \in K,\ \forall\, x, y \in R.$$

Dann heißt $(R, +, \circ, \cdot)$ eine K-Algebra.

Eine Abbildung zwischen K-Algebren heißt K-*Algebrenhomomorphismus*, wenn sie sowohl ein Ringhomomorphismus als auch K-linear ist, d.h. wenn sie mit allen drei Operationen verträglich ist und die Eins auf die Eins abbildet.

Beispiel 1.24

a. Ist K ein Teilkörper von L, so ist L eine kommutative K-Algebra, wobei die Multiplikation mit Skalaren in K mit der Multiplikation in L übereinstimmt.

b. Die Menge der $n \times n$-Matrizen $\mathrm{Mat}_n(K)$ über einem Körper K ist ein K-Vektorraum und ist zudem mit der Matrixmultiplikation ein Ring mit Eins $\mathbb{1}_n$. Für $n \geq 2$ ist $\mathrm{Mat}_n(K)$ dann eine nicht-kommutative K-Algebra.

c. Ist K ein Körper und Λ eine Menge, dann ist der allgemeine Polynomring $K[\Lambda]$ eine kommutative K-Algebra, wenn wir die Multiplikation mit den konstanten Polynomen als Skalarmultiplikation nehmen.

Satz 1.25 (Die universelle Eigenschaft von Polynomringen)
Es sei K ein Körper, Λ eine Menge und R eine beliebige kommutative K-Algebra. Ist $(r_\lambda \mid \lambda \in \Lambda)$ eine beliebige Familie in R, so gibt es genau einen K-Algebrenhomomorphismus

$$\varphi : K[\Lambda] \longrightarrow R$$

mit

$$\varphi(x_\lambda) = r_\lambda$$

für alle $\lambda \in \Lambda$.

Beweis: Wir definieren die Abbildung $\varphi : K[\Lambda] \longrightarrow R$ indem wir in einem Polynom $f \in K[\Lambda]$ jeweils für die Variable x_λ das Element r_λ einsetzen. Das geht, da in jedem Polynom nur endlich viele Summanden mit endlichen Produkten endlich vieler Variablen vorkommen, so daß das Ergebnis in R liegt. Die Formeln für die Addition und die Multiplikation in Definition 1.20 zusammen mit den Rechenregeln in dem kommutativen Ring R zeigen, daß φ dann ein Ringhomomorphismus ist.

Die Verträglichkeit mit der Skalarmultiplikation ist damit ebenfalls gewährleistet, da sie durch die Multiplikation mit konstanten Polynomen gegeben ist. Also ist φ ein K-Algebrenhomomorphismus.

Um die Eindeutigkeit zu zeigen, sei $\psi : K[\Lambda] \longrightarrow R$ ein zweiter K-Algebrenhomomorphismus mit $\psi(x_\lambda) = r_\lambda$ für alle $\lambda \in \Lambda$. Für ein beliebiges Polynom $f \in K[\Lambda]$ gibt es eine endliche Teilmenge

$$\Omega = \{\lambda_1, \ldots, \lambda_k\} \subseteq \Lambda$$

von Λ, so daß

$$f = \sum_{\alpha=(\alpha_1,\ldots,\alpha_k)\in\mathbb{N}^k} a_\alpha \cdot x_{\lambda_1}^{\alpha_1} \cdot \ldots \cdot x_{\lambda_k}^{\alpha_k}$$

mit $a_\alpha \in K$ und nur endlich viele der $a_\alpha \neq 0$. Dann gilt aber

$$\begin{aligned}
\psi(f) =& \psi\left(\sum_{\alpha=(\alpha_1,\ldots,\alpha_k)\in\mathbb{N}^k} a_\alpha \cdot x_{\lambda_1}^{\alpha_1} \cdot \ldots \cdot x_{\lambda_k}^{\alpha_k}\right) \\
=& \sum_{\alpha=(\alpha_1,\ldots,\alpha_k)\in\mathbb{N}^k} a_\alpha \cdot \psi(x_{\lambda_1})^{\alpha_1} \cdot \ldots \cdot \psi(x_{\lambda_k})^{\alpha_k} \\
=& \sum_{\alpha=(\alpha_1,\ldots,\alpha_k)\in\mathbb{N}^k} a_\alpha \cdot r_{\lambda_1}^{\alpha_1} \cdot \ldots \cdot r_{\lambda_k}^{\alpha_k} \\
=& \sum_{\alpha=(\alpha_1,\ldots,\alpha_k)\in\mathbb{N}^k} a_\alpha \cdot \varphi(x_{\lambda_1})^{\alpha_1} \cdot \ldots \cdot \varphi(x_{\lambda_k})^{\alpha_k} \\
=& \varphi\left(\sum_{\alpha=(\alpha_1,\ldots,\alpha_k)\in\mathbb{N}^k} a_\alpha \cdot x_{\lambda_1}^{\alpha_1} \cdot \ldots \cdot x_{\lambda_k}^{\alpha_k}\right) = \varphi(f).
\end{aligned}$$

Mithin stimmen ψ und φ überein und die Eindeutigkeit ist gezeigt. □

Bemerkung 1.26 (Freie K-Algebra)

a. Die universelle Eigenschaft des Polynomrings sagt, daß K-Algebrenhomomorphismen durch die Werte auf den Veränderlichen festgelegt sind, daß sie auf diesen aber beliebig vorgegeben werden können. Man nennt den Polynomring $K[\Lambda]$ deshalb auch *freie K-Algebra in den freien Erzeugern* $x_\lambda, \lambda \in \Lambda$.

b. Wenn man in der Definition von K-Algebra nur fordert, daß K ein kommutativer Ring mit Eins ist, und das Wort *Vektorraum* durch *Modul* ersetzt, erhält man Algebren über Ringen und Satz 1.25 bleibt inklusive des Beweises erhalten.

Aufgaben

Aufgabe 1.27

Zeige, ist R ein faktorieller Ring und $a \in \mathrm{Quot}(R)$ eine Nullstelle eines normierten Polynoms $0 \neq f \in R[t]$, dann gilt $a \in R$.

Aufgabe 1.28
Es sei R ein kommutativer Ring mit Eins.

Beweise die folgenden Aussagen:

a. Sind $0 \neq f, g \in R[t]$, so gibt es Polynome $q, r \in R[t]$ und eine natürliche Zahl $0 \leq k \leq \deg(g)$, so daß

$$\mathrm{lc}(f)^k \cdot g = q \cdot f + r$$

und

$$\deg(r) < \deg(f).$$

b. Ist $a \in R$ eine Nullstelle von g, so gibt es ein Polynom $q \in R[t]$ mit $g = q \cdot (t - a)$.

c. Ist R ein Integritätsbereich, so hat g höchstens $\deg(g)$ paarweise verschiedene Nullstellen in R.

d. Finde ein Beispiel für einen Ring R und ein Polynom $0 \neq g \in R[t]$ mit mehr als $\deg(g)$ Nullstellen.

Aufgabe 1.29
Es sei K ein Körper und $f \in K[t]$ ein Polynom vom Grad $2 \leq \deg(f) \leq 3$.

Zeige, f ist genau dann irreduzibel, wenn f in K keine Nullstelle hat.

Aufgabe 1.30
Sei K ein Körper. Zeige mit Hilfe von Aufgabe 1.27, daß der Unterring

$$R = \left\{ \sum_{i=0}^{n} a_i t^i \in K[t] \;\middle|\; n \in \mathbb{N}, a_1 = 0 \right\}$$

von $K[t]$ nicht faktoriell ist.

Aufgabe 1.31
Sei R ein Integritätsbereich. Beweise, dass folgende Aussagen äquivalent sind:

a. R ist faktoriell.

b. Der Schnitt zweier Hauptideale in R ist ein Hauptideal und für jede aufsteigende Kette

$$I_0 \subseteq I_1 \subseteq I_2 \subseteq \dots$$

von Hauptidealen in R existiert ein $n \in \mathbb{N}$ mit $I_k = I_n$ für alle $k \geq n$.

Aufgabe 1.32
Zeige, im Ring R aus Aufgabe 1.30 ist das Ideal

$$\langle t^2 \rangle \cap \langle t^3 \rangle = \langle t^5, t^6 \rangle$$

kein Hauptideal.

Aufgabe 1.33
Zeige, im Ring R aus Aufgabe 1.30 ist t^3 irreduzibel, aber nicht prim.

Aufgabe 1.34

Sei R ein Integritätsbereich, Λ eine Menge und $\Omega \subseteq \Lambda$ eine endliche Teilmenge. Zeige, genau dann ist $p \in R[\Omega]$ irreduzibel in $R[\Omega]$, wenn es irreduzibel in $R[\Lambda]$ ist.

§ 2 Das Lemma von Zorn und maximale Ideale

Im vorliegenden Abschnitt wollen wir uns mit maximalen Idealen in Ringen befassen und zeigen dazu zunächst das Lemma von Zorn als ein probates Mittel, die Existenz maximaler Objekte zu zeigen.

A) Das Lemma von Zorn

Das Lemma von Zorn stellt eine Technik für Beweise zur Verfügung, die in vielen Kontexten Anwendung findet, wenn ein Objekt gesucht wird, das bezüglich vorgegebener Kriterien eine Maximalitätseigenschaft erfüllen soll. In der Linearen Algebra zeigt man z.B. standardmäßig durch Anwendung des Lemmas von Zorn, daß jeder Vektorraum eine Basis besitzt, also eine maximal linear unabhängige Familie von Vektoren. Wir führen nun zunächst ein paar Begriffe ein, die notwendig sind, um das Lemma von Zorn zu formulieren und zu beweisen.

Definition 2.1 (Ordnungsrelationen)
Es sei M eine Menge.

a. Eine Relation $\leq$ auf M heißt eine *Ordnungsrelation* oder *Teilordnung* und das Tupel $(M, \leq)$ eine *teilgeordnete Menge*, wenn $\leq$ die folgenden Axiome erfüllt:
   (i) Für alle $x \in M$ gilt $x \leq x$. [Reflexivität]
   (ii) Wenn $x \leq y$ und $y \leq x$ für $x, y \in M$ gilt, so folgt $x = y$. [Antisymmetrie]
   (iii) Für $x, y, z \in M$ folgt aus $x \leq y$ und $y \leq z$ schon $x \leq z$. [Transitivität]

b. Eine Ordnungsrelation $\leq$ auf M heißt eine *Totalordnung*, wenn für je zwei $x, y \in M$ stets $x \leq y$ oder $y \leq x$ gilt.

c. Eine Totalordnung $\leq$ auf M heißt eine *Wohlordnung*, wenn jede nicht-leere Teilmenge von M ein minimales Element besitzt.

Definition 2.2 (Ketten)
Es sei $(M, \leq)$ eine teilgeordnete Menge.

a. Eine total geordnete Teilmenge K von M heißt eine *Kette* in M.

b. Ein Element $s \in M$ heißt *obere Schranke* einer Kette K, wenn $x \leq s$ für alle $x \in K$ gilt.

c. Ein Element $x \in M$ heißt *maximal* in M, wenn es kein $y \in M$ mit $x < y$ gibt.

d. Für eine Kette K und $x \in M$ definieren wir das *Initialsegment* von K unterhalb x durch

$$I(K, x) := \{y \in K \mid y < x\}.$$

Bemerkung 2.3
Man beachte, daß die leere Menge auch ein Kette ist und daß Initialsegmente von Ketten wieder Ketten sind. Zudem ist jedes $s \in M$ eine obere Schranke für die leere Kette.

Wir werden nun das Lemma von Zorn mit Hilfe des Auswahlaxioms beweisen.

Satz 2.4 (Lemma von Zorn)
Es sei $(M, \leq)$ *eine nicht-leere, teilgeordnete Menge. Wenn jede Kette in* M *eine obere Schranke in* M *besitzt, so besitzt* M *ein maximales Element.*

Beweis nach [Lew91]: Wir nehmen an, daß M kein maximales Element besitzt und wollen dies zum Widerspruch führen.

1. Schritt: Konstruiere eine Abbildung $f : \{K \subset M \mid K \text{ ist eine Kette}\} \longrightarrow M$ mit $f(K) > x$ für alle $x \in K$.

Ist K ein beliebige Kette in M, so ist die Menge

$$S_K := \{s \in M \mid s \text{ ist eine obere Schranke von } K\} \neq \emptyset$$

nicht leer, und mit Hilfe des Auswahlaxioms können wir für jede Kette K mithin eine obere Schranke $s_K \in S_K$ wählen. Für diese betrachten wir dann die Menge

$$T_K := \{x \in M \mid s_K < x\},$$

die nicht leer ist, weil sonst s_K ein maximales Element in M wäre. Wieder mit Hilfe des Auswahlaxioms können wir für jede Kette K in M nun ein $t_K \in M$ wählen und erhalten somit eine Abbildung

$$f : \{K \subset M \mid K \text{ ist eine Kette}\} \longrightarrow M : K \mapsto t_K,$$

für die

$$f(K) > x \tag{5}$$

für alle $x \in K$ gilt.

2. Schritt: Wir wollen eine *wohlgeordnete* Kette K *konform* zu f nennen, wenn für alle $x \in K$

$$x = f\big((I(K, x)\big) \tag{6}$$

gilt. Die leere Menge ist die einfachste zu f konforme Kette. Unser Ziel ist es, mit Hilfe der Vereinigung aller zu f konformen Ketten einen Widerspruch herzuleiten. Dazu müssen wir zu f konforme Ketten etwas genauer untersuchen.

3. Schritt: Wir zeigen zunächst die folgende Hilfsaussage: wenn A und B zwei zu f konforme Ketten sind mit $A \setminus B \neq \emptyset$, dann gibt es ein $x \in A$, so daß

$$B = I(A, x) \tag{7}$$

das Initialsegment von A unterhalb von x ist.

Um diese Aussage zu zeigen setzen wir zunächst

$$x := \min(A \setminus B) = \min\{\alpha \in A \mid \alpha \notin B\},$$

was möglich ist, da A wohlgeordnet ist. Wir erhalten dann

$$I(A, x) = \{\alpha \in A \mid \alpha < x\} \subseteq B,$$

da nach Definition von x alle kleineren Element in A schon in B liegen. Es bleibt noch zu zeigen, daß auch die umgekehrte Inklusion gilt.

Dazu nehmen wir an, es gelte

$$I(A,x) \subsetneqq B \tag{8}$$

und setzen dann

$$y := \min\big(B \setminus I(A,x)\big) = \min\{\beta \in B \mid \beta \notin I(A,x)\},$$

was möglich ist, da B wohlgeordnet ist. Wegen

$$A \setminus I(B,y) \supseteq A \setminus B \neq \emptyset \tag{9}$$

und weil A wohlgeordnet ist, existiert zudem

$$z := \min\big(A \setminus I(B,y)\big) = \min\{\alpha \in A \mid \alpha \notin I(B,y)\},$$

und aus der Inklusion (9) folgt zudem unmittelbar

$$x = \min(A \setminus B) \geq \min\big(A \setminus I(B,y)\big) = z. \tag{10}$$

Die Gleichung

$$I(A,z) = I(B,y) \tag{11}$$

ist nun leicht zu sehen. Denn für ein $\delta \in I(A,z)$ gilt $\delta \in A$ und $\delta < z$, so daß aus der Definition von z als Minimum unmittelbar $\delta \in I(B,y)$ folgt. Ist umgekehrt $\delta \in I(B,y)$, dann ist $\delta \in B$ und $\delta < y$, woraus mittels der Definition von y als Minimum dann schon mal

$$\delta \in I(A,x) \subseteq A \tag{12}$$

folgt. Wäre nun $z \leq \delta$, so würde aus (12)

$$z \leq \delta < x$$

folgen und aus der Definition von x als Minimum dann schon

$$z \in B.$$

Wegen $z \leq \delta < y$ würde dann aber auch

$$z \in I(B,y)$$

gelten, im Widerspruch zur Definition von z. Also gilt $\delta < z$ und somit $\delta \in I(A,z)$. Die Gleichung (11) ist also gezeigt.

Aus (10) und (11) folgt dann aber

$$x \geq z = f\big(I(A,z)\big) = f\big((I(B,y)\big) = y.$$

Würde in der Ungleichung $x = z$ gelten, so hätten wir

$$x = z = y \in B$$

im Widerspruch zur Definition von x, weshalb notwendigerweise

$$z < x$$

und damit wegen $z \in A$ auch

$$y = z \in I(A, x)$$

gelten muß. Das steht aber im Widerspruch Definition von y. Wir haben damit die Annahme in (8) widerlegt und die Hilfsaussage (7) gezeigt.

4. Schritt: Wir betrachten nun die Vereinigung

$$V := \bigcup_{\substack{A \subseteq M \\ A \text{ konform}}} A$$

aller zu f konformen Ketten und wollen für diese eine weitere Hilfsaussage beweisen: Ist A eine zu f konforme Kette und $x \in A$, so gilt

$$I(A, x) = I(V, x). \tag{13}$$

Die eine Inklusion

$$I(A, x) = \{y \in A \mid y < x\} \subseteq \{y \in V \mid y < x\} = I(V, x)$$

ist wegen $A \subseteq V$ offensichtlich. Für die andere Inklusion betrachten wir ein $y \in I(V, x)$ und müssen nur noch $y \in A$ zeigen. Für y gibt es eine zu f konforme Kette B mit $y \in B$. Ist $A = B$, so ist $y \in B = A$. Andernfalls erhalten wir aus (7)

$$A = I(B, u)$$

für ein $u \in B$ oder

$$B = I(A, v)$$

für ein $v \in A$. Im ersteren Fall ist $y < x < u$ und somit

$$y \in I(B, u) = A,$$

in letzterem Fall ist

$$y \in B = I(A, v) \subseteq A.$$

In jedem Fall gilt $y \in A$ und damit $y \in I(A, x)$. Damit ist (13) gezeigt.

5. Schritt: Wir wollen nun (13) nutzen, um zu zeigen, daß V in der Tat eine zu f konforme Kette ist.

Dazu zeigen wir zunächst, daß V eine Kette, also totalgeordnet, ist: Sind $x, y \in V$, so gibt es zwei zu f konforme Ketten A und B mit $x \in A$ und $y \in B$. Wegen (7) sind die beiden Ketten gleich oder eine der beiden ist ein Initialsegment der anderen, und wir können ohne Einschränkung $A \subseteq B$ annehmen. Da B als Kette totalgeordnet ist, gilt dann in B aber $x \leq y$ oder $y \leq x$. Also ist auch V total geordnet.

Dann müssen wir zeigen, daß V auch wohlgeordnet ist: Sei dazu $\emptyset \neq U \subseteq V$ eine nicht-leere Teilmenge von V, so müssen wir zeigen, daß U ein Minimum besitzt. Da U nicht leer ist, können wir ein $x \in U$ wählen und finden dazu eine zu f konforme Kette A mit $x \in A$. Ist nun $y \in U$ mit $y < x$, so gilt wegen (13) schon

$$y \in I(V, x) = I(A, x) \subseteq A,$$

und wir erhalten

$$\min(U) = \min\{y \in U \mid y \leq x\} = \min\{y \in U \cap A \mid y \leq x\} = \min(U \cap A),$$

wobei letzteres existiert, da A wohlgeordnet ist. Mithin ist V wohlgeordnet.

Schließlich müssen wir noch zeigen, daß V die Bedingung (6) erfüllt: Sei dazu $x \in V$ gegeben. Dann gibt es eine zu f konforme Kette A mit $x \in A$. Mit (13) gilt dann

$$I(A, x) = I(V, x),$$

und mit der Bedingung (6) für A erhalten wir die Bedingung (6)

$$x = f\big(I(A, x)\big) = f\big(I(V, x)\big)$$

auch für V. Damit ist gezeigt, daß V eine zu f konforme Kette ist.

6. Schritt: Setzen wir nun

$$x := f(V)$$

so sieht man leicht, daß auch $V \cup \{x\}$ eine zu f konforme Kette ist.

Da x nach Definition von f (siehe (5)) größer als alle Elemente von V ist, ist die Menge $V \cup \{x\}$ offenbar eine wohlgeordnete Kette. Es bleibt noch, die Bedingung (6) zu überprüfen. Für ein $y \in V \cup \{x\}$ unterscheiden wir zwei Fälle. Ist $y \in V$, so ist

$$I(V \cup \{x\}, y) = I(V, y)$$

und damit

$$y = f\big(I(V, y)\big) = f\big(I(V \cup \{x\}, y)\big).$$

Ist $y \notin V$, so ist $y = x$ und aus der Definition von x folgt

$$I(V \cup \{x\}, y) = I(V \cup \{x\}, x) = V$$

sowie

$$y = x = f(V) = f\big(I(V \cup \{x\}, y)\big).$$

Also ist auch $V \cup \{x\}$ ein zu f konforme Kette.

7. Schritt: Da aber V die Vereinigung aller zu f konformen Ketten ist, gilt dann

$$x \in V \cup \{x\} \subseteq V,$$

was im Widerspruch dazu steht, daß $x = f(V)$ echt größer als alle Elemente in V ist (siehe (5)). Dieser Widerspruch rührt von der Annahme her, daß M kein maximales Element beisitzt, womit die Existenz eines solchen bewiesen ist.

□

Bemerkung 2.5 (Lemma von Zorn, Auswahlaxiom und Wohlordnungssatz)
Wir haben das Lemma von Zorn mit Hilfe des Auswahlaxioms bewiesen. In der Tat kann man zeigen, daß das Auswahlaxiom auf der Basis der übrigen Axiome von Zermelo-Fraenkel auch aus dem Lemma von Zorn folgen würde. Die beiden sind also äquivalent zueinander. Sie sind ferner beide äquivalent zum Wohlordnungssatz, der

besagt, daß jede nicht-leere Menge eine Wohlordnung besitzt. Für weitere Details hierzu verweisen wir den Leser auf [**Moo82**, **Sze50**].

B) Maximale Ideale

Wir wollen nun den Begriff des maximalen Ideals einführen, weil maximale Ideale bei der Konstruktion von Körpern hilfreich sind.

Definition 2.6 (Maximales Ideal)
Es sei R ein kommutativer Ring mit Eins. Ein echtes Ideal $\mathfrak{m} \lhd R$ heißt *maximal*, wenn es kein Ideal $I \trianglelefteq R$ mit $\mathfrak{m} \subsetneqq I \subsetneqq R$ gibt. Wir schreiben dann: $\mathfrak{m} \lhd\cdot R$.

Beispiel 2.7

a. In einem Körper ist das Nullideal maximal, weil es das einzige echte Ideal ist.

b. In $\mathbb{Z}$ ist das Nullideal kein maximales Ideal wegen $\{0\} \subsetneqq 2\mathbb{Z} \subsetneqq \mathbb{Z}$.

Proposition 2.8 (Existenz maximaler Ideale)
Sei R ein kommutativer Ring mit Eins und $I \lhd R$ ein echtes Ideal in R. Dann gibt es ein maximales Ideal $\mathfrak{m} \lhd\cdot R$ mit $I \subseteq \mathfrak{m}$.

Beweis: Wir wollen den Beweis mit Hilfe des Lemmas von Zorn führen und betrachten dazu die Menge

$$M := \{J \lhd R \mid I \subseteq J\}$$

der echten Ideale, die I enthalten. Die Menge ist nicht leer, weil I in M enthalten ist. Zudem ist die Menge bezüglich der Inklusion "$\subseteq$" von Mengen teilgeordnet.

Sei nun K eine nicht-leere Kette in M, so setzen wir

$$S := \bigcup_{J \in K} J$$

als Vereinigung der Ideale in K. Wir wollen sehen, daß S ein echtes Ideal in R ist, welches I enthält.

Da die Kette nicht leer ist, gibt es ein Ideal $J \in K$ und somit gilt

$$I \subseteq J \subseteq S,$$

so daß S nicht leer ist und I enthält. Sind nun $x, x' \in S$ und $r \in R$. Dann gibt es zwei Ideale $J, J' \in S$ mit $x \in J$ und $x' \in J'$. Da K total geordnet ist bezüglich der Inklusion, gilt $J \subseteq J'$ oder $J' \subseteq J$. Im ersten Fall folgt

$$x + x' \in J' \subseteq S,$$

da J' ein Ideal ist, und im zweiten Fall folgt analog

$$x + x' \in J \subseteq S.$$

Außerdem gilt

$$r \cdot x \in J \subseteq S,$$

da J ein Ideal ist. Mithin ist auch S ein Ideal in R. Wäre

$$\bigcup_{J \in K} J = S \overset{!}{=} R \ni 1,$$

so würde es ein $J \in K$ mit $1 \in J$ geben, im Widerspruch dazu, daß die J echte Ideale sind. Also ist auch S ein echtes Ideal in R. Somit ist $S \in M$ und S ist eine obere Schranke von K, da $J \subseteq S$ für alle $J \in K$ gilt.

Da die leere Kette stets eine obere Schranke in M besitzt, sind die Voraussetzungen des Lemmas von Zorn erfüllt und wir erhalten ein maximales Element

$$\mathfrak{m} \in M.$$

Wir wollen nun zeigen, daß $\mathfrak{m}$ in der Tat ein maximales Ideal ist, das I enthält. Das ist aber offensichtlich, da jedes echte Ideal, das $\mathfrak{m}$ enthielte auch I enthalten würde und damit ein größeres Element als $\mathfrak{m}$ in M wäre, im Widerspruch zur Maximalität von $\mathfrak{m}$. □

Korollar 2.9 (Existenz maximaler Ideale)
Ist R ein kommutativer Ring mit Eins und nicht der Nullring, so enthält R ein maximales Ideal.

Beweis: Wir wenden Proposition 2.8 mit $I = \{0\}$ an. □

Bemerkung 2.10 (Existenz maximaler Ideale)
Die Aussagen von Proposition 2.8 und Korollar 2.9 sind reine Existenzaussagen. Der Beweis von Proposition 2.8 gibt keinerlei Auskunft darüber, wie man ein solches maximales Ideal im Falle eines konkret gegebenen Rings finden könnte. Das kann u.U. recht schwierig sein.

Der Zusammenhang zwischen maximalen Idealen und Körpern ergibt sich aus den folgenden beiden Propositionen.

Proposition 2.11 (Körper enthalten nur die trivialen Ideale.)
Ein kommutativer Ring R mit Eins ist genau dann ein Körper, wenn er nur die trivialen Ideale $\{0\}$ und R enthält und diese verschieden sind.

Beweis: Sei zunächst R ein Körper. Wegen $0 \neq 1$ muß $\{0\} \neq R$ gelten. Sei nun $\{0\} \neq I \trianglelefteq R$ ein Ideal. Dann enthält I ein Element $0 \neq a \in I$, und da R ein Körper ist, besitzt dieses in R ein multiplikatives Inverses. Wir erhalten für $r \in R$ beliebig damit

$$r = r \cdot 1 = r \cdot a^{-1} \cdot a \in I$$

und somit $I = R$. Der Ring R enthält also nur die trivialen Ideale.

Enthalte nun umgekehrt R nur die trivialen Ideale und diese seien verschieden. Aus $\{0\} \neq R$ folgt $0 \neq 1$. Es bleibt zu zeigen, daß jedes $0 \neq a \in R$ ein multiplikatives Inverses besitzt. Dazu betrachten wir das von a erzeugte Ideal

$$\{0\} \neq \langle a \rangle \trianglelefteq R.$$

Da R nur die trivialen Ideale besitzt, muß

$$\langle a \rangle = R \ni 1$$

gelten, so daß es ein $b \in R$ mit

$$1 = b \cdot a$$

gibt. Dieses b ist dann die gesuchte Inverse und R ist ein Körper. □

Proposition 2.12 (Maximale Ideale liefern Körper.)
Sei R ein kommutativer Ring mit Eins und $\mathfrak{m} \trianglelefteq R$ ein Ideal. Genau dann ist $\mathfrak{m}$ maximal, wenn $R/\mathfrak{m}$ ein Körper ist.

Beweis: Wir beachten, daß die Ideale des Faktorrings in folgender 1:1-Beziehung mit den Idealen in R stehen, die $\mathfrak{m}$ enthalten:

$$\{I \trianglelefteq R \mid \mathfrak{m} \subseteq I\} \longrightarrow \{\bar{I} \trianglelefteq R/\mathfrak{m}\} : I \mapsto I/\mathfrak{m}.$$

Dann ist $\mathfrak{m}$ genau dann ein maximales Ideal von R, wenn $R/\mathfrak{m}$ nur die trivialen Ideale $\mathfrak{m}/\mathfrak{m}$ und $R/\mathfrak{m}$ besitzt und diese verschieden sind. Dieses ist nach Proposition 2.11 aber genau dann der Fall, wenn $R/\mathfrak{m}$ ein Körper ist. □

Beispiel 2.13

a. Das Ideal $2\mathbb{Z}$ ist maximal in $\mathbb{Z}$, weil $\mathbb{Z}/2\mathbb{Z}$ ein Körper ist.

b. Ist K ein Körper und ist $a \in K$ dann ist $\langle t - a \rangle$ ein maximales Ideal in $K[t]$, da $K[t]/\langle t - a \rangle \cong K$ ein Körper ist.
Um dies zu sehen, betrachten wir den Ringhomomorphismus

$$\varphi : K[t] \longrightarrow K : f \mapsto f(a).$$

Offenbar ist φ surjektiv. Wir müssen nur noch zeigen, daß

$$\ker(\varphi) = \langle t - a \rangle$$

gilt, dann folgt die Behauptung aus dem Homomorphiesatz für Ringhomomorphismen. Die Inklusion $\langle t - a \rangle \subseteq \ker(\varphi)$ ist wieder offensichtich. Für die umgekehrte Inklusion betrachten wir ein Polynom $f \in \ker(\varphi)$ und zerlegen es mittels Division mit Rest als

$$f = (t - a) \cdot q + r$$

mit $q, r \in K[t]$ und $\deg(r) < \deg(t - a) = 1$. Also ist $r \in K$ ein konstantes Polynom und es folgt

$$0 = \varphi(f) = f(a) = (a - a) \cdot q(a) + r = r.$$

Damit haben wir $f = (t - a) \cdot q \in \langle t - a \rangle$ gezeigt.

c. Ist K ein Körper, so ist das Ideal $\langle x, y\rangle \lhd K[x, y]$ maximal, weil $K[x, y]/\langle x, y\rangle \cong K$ ein Körper ist.
Den Isomorphismus zeigt man wie in Teil b. mit Hilfe des surjektiven Ringhomomorphismus

$$\varphi : K[x, y] \longrightarrow K : f \mapsto f(0, 0)$$

dessen Kern

$$\ker(\varphi) = \langle x, y\rangle$$

erfüllt und mit Hilfe des Homomorphiesatzes für Ringhomomorphismen. Wieder ist die Inklusion $\langle x, y\rangle \subseteq \ker(\varphi)$ offensichtlich. Für die umgekehrte Inklusion betrachten wir ein Polynom $f \in \ker(\varphi)$. Dann ist $f(0, 0) \in K$ gerade der konstante Anteil von f und es gilt

$$f - f(0, 0) \in \langle x, y\rangle.$$

Da f im Kern von φ liegt gilt damit aber

$$f = f - 0 = f - \varphi(f) = f - f(0, 0) \in \langle x, y\rangle.$$

C) Maximale Ideale und Irreduzibilität in Hauptidealringen

Korollar 2.14 (Maximale Ideale in Hauptidealringen)
Sei R ein Hauptidealring R und $0 \neq p \in R$. Dann sind die folgenden Aussagen gleichwertig:

a. p ist irreduzibel.

b. $\langle p\rangle \lhd\cdot R$ ist ein maximales Ideal.

c. $R/\langle p\rangle$ ist ein Körper.

Insbesondere, ist K ein Körper und $f \in K[t]$ irreduzibel, so ist $K[t]/\langle f\rangle$ ein Körper.

Beweis: Aus Proposition 2.12 ist die Äquivalenz von b. und c. bereits bekannt.

Sei nun p irreduzibel in R und sei I ein Ideal in R mit

$$\langle p\rangle \subseteq I \subseteq R. \tag{14}$$

Da R ein Hauptidealring ist, gibt es ein $a \in R$ mit

$$I = \langle a\rangle,$$

und aus (14) folgt dann, daß es ein $b \in R$ gibt mit

$$p = a \cdot b.$$

Weil p irreduzibel ist, muß $a \in R^*$ oder $b \in R^*$ gelten. Im ersteren Fall ist $I = \langle a\rangle = R$ und im letzteren ist $\langle p\rangle = \langle a\rangle = I$, da p und a dann assoziiert sind. Also ist $\langle p\rangle$ ein maximales Ideal, und wir haben gezeigt, daß a. auch b. impliziert.

Setzen wir nun 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. Somit ist auch gezeigt, daß aus c. auch a. folgt, und die Äquivalenz der drei Aussagen ist bewiesen. □

Beispiel 2.15
Das Polynom $t^2 + 1 \in \mathbb{R}[t]$ ist irreduzibel, weil es in $\mathbb{R}$ keine Nullstelle hat. Mithin ist $\langle t^2 + 1\rangle \lhd \cdot\, \mathbb{R}[t]$ ein maximales Ideal. Es gilt in der Tat

$$\mathbb{R}[t]/\langle t^2 + 1\rangle \xrightarrow{\cong} \mathbb{C} : \overline{f} \mapsto f(i),$$

wie man sich leicht überzeugt.

Dazu betrachten wir zunächst den Ringhomomorphismus

$$\varphi : \mathbb{R}[t] \longrightarrow \mathbb{C} : f \mapsto f(i).$$

Die Abbildung φ ist offenbar surjektiv, da für eine beliebige komplexe Zahl $a+b\cdot i \in \mathbb{C}$ das Polynom

$$f = a + b \cdot t \in \mathbb{R}[t]$$

ein Urbild unter φ ist. Zudem wollen wir zeigen, daß

$$\ker(\varphi) = \left\langle t^2 + 1\right\rangle$$

gilt. Die Inklusion "$\supseteq$" ist dabei offensichtlich wegen $i^2 + 1 = 0$. Für die andere Inklusion betrachten wir ein Polynom $f \in \ker(\varphi)$ und finden wir mittels Division mit Rest zwei Polynome $q, r \in \mathbb{R}[t]$, so daß

$$f = q \cdot \left(t^2 + 1\right) + r$$

mit $\deg(r) < \deg(t^2 + 1) = 2$. Das Polynom r hat also die Form

$$r = a + b \cdot t$$

mit $a, b \in \mathbb{R}$ geeignet. Dann gilt

$$0 = \varphi(f) = f(i) = q(i) \cdot (i^2 + 1) + r(i) = q(i) \cdot 0 + r(i) = a + b \cdot i,$$

woraus $a = b = 0$ und damit

$$f = q \cdot \left(t^2 + 1\right) \in \left\langle t^2 + 1\right\rangle$$

folgt. Die Aussage über den Kern ist also bewiesen und der Rest folgt dann aus dem Homomorphiesatz für Ringhomomorphismen.

Aufgaben

Aufgabe 2.16 (Maximale Ideale im Polynomring über $\mathbb{Z}$)
Sei $p \in \mathbb{Z}$ eine Primzahl und $f \in \mathbb{Z}[t]$ ein Polynom, so daß die Reduktion $\bar{f}$ modulo p irreduzibel in $\mathbb{Z}/p\mathbb{Z}[t]$ ist. Zeige, dann ist das Ideal $\mathfrak{m} = \langle p, f\rangle$ in $\mathbb{Z}[t]$ ein maximales Ideal.[1]

Aufgabe 2.17
Sei K ein Körper und $f \in K[t] \setminus K$ habe die Primfaktorzerlegung

$$f = c \cdot p_1^{n_1} \cdot \ldots \cdot p_k^{n_k}$$

mit paarweise nicht assoziierten irreduziblen Polynomen p_i und mit $c \in K$.

Aufgabe 2.18 (Das Jacobsen Radikal)
Sei R ein kommutativer Ring und $J(R) = \bigcap_{\mathfrak{m} \lhd \cdot R} \mathfrak{m}$ der Durchschnitt aller maximalen Ideale. Zeige, $a \in J(R)$ genau dann, wenn $1 - a \cdot b \in R^*$ für alle $b \in R$.

Aufgabe 2.19 (Primideale)
Sei R ein kommutativer Ring mit Eins und sei $P \lhd R$ ein echtes Ideal. Zeige, daß die folgenden Aussagen gleichwertig sind:

a. Für $a, b \in R$ mit $a \cdot b \in P$ gilt schon $a \in P$ oder $b \in P$.

b. Für Ideale $I, J \trianglelefteq R$ mit $I \cdot J \subseteq P$ gilt schon $I \subseteq P$ oder $J \subseteq P$.

c. R/P ist ein Integritätsbereich.

Ein solches Ideal P heißt auch ein *Primideal* in R.

Aufgabe 2.20 (Primideale und Primelemente)
Sei R ein Integritätsbereich und $0 \neq p \in R$. Zeige, p ist genau dann ein Primelement, wenn $\langle p\rangle$ ein Primideal in R ist.

Aufgabe 2.21 (Existenz minimaler Primideale)
Zeige, jeder kommutative Ring mit Eins, der nicht der Nullring ist, enthält ein minimales Primideal, d.h. ein Primideal P, so daß es kein Primideal Q mit $Q \subsetneqq P$ gibt.

Aufgabe 2.22 (Lemma von Teichmüller-Tukey)
Sei M eine Menge und E sei eine Teilmenge der Potenzmenge von M mit $\emptyset \in E$. Zeige, die Menge

$$A = \{N \subseteq M \mid X \subseteq N \ \wedge\ |X| < \infty \implies X \in E\}$$

aller Teilmengen von M, deren endliche Teilmengen in E liegen enthält ein bezüglich der Inklusion maximales Element.

[1] In der Tat sind alle maximalen Ideale in $\mathbb{Z}[t]$ von dieser Form, aber das zu zeigen ist anspruchsvoller.

§ 3 Irreduzibilitätskriterien

Wir haben in Korollar 2.14 angedeutet, weshalb irreduziblen Polynomen für die Konstruktion von Körpern mit vorgegebenen Eigenschaften eine zentrale Rolle zukommt. Im Verlauf dieses Abschnitts wollen wir uns deshalb mit Methoden beschäftigen, mit Hilfe derer man in vielen Fällen entscheiden kann, ob ein Polynom irreduzibel ist.

A) Das Eisenstein-Kriterium

Satz 3.1 (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

$$a_k = \sum_{i+j=k} b_i \cdot c_j \tag{15}$$

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 (15) 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 3.2
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 Korollar 2.14 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 3.3
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 1.18 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 1.17 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 Lemma 1.12 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 1.16 auch $p \cdot q \in R[t]$ primitiv ist, folgt aus

$$f = (c \cdot d) \cdot p \cdot q \tag{16}$$

und Lemma 1.12, daß $c \cdot d \in R$. Da es sich bei Gleichung (16) 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 $e \in \mathrm{cont}_R(f)$

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

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

Beispiel 3.4
Wegen Satz 3.3 und Beispiel 3.2 ist das primitive Polynom $f = t^4 - 4t + 2 \in \mathbb{Z}[t]$ auch irreduzibel in $\mathbb{Q}[t]$.

B) Reduktion modulo p

Definition and Proposition 3.5 (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 3.6 (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 Korollar 2.14 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 3.7 (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 3.8
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.

C) Lineare Koordinatentransformationen

Proposition 3.9 (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 3.10 (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 3.1 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 3.3.

D) Primfaktorzerlegung

Bemerkung 3.11
Bei Polynomen kleinen Grades kann man die Irreduzibilität auch an der Nicht-Existenz von Nullstellen festmachen, 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 3.3 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 Vorlesungen zum symbolischen 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 3.12

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 3.13

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 $4 \cdot 4 \cdot 8 = 128$ Möglichkeiten streichen, da die Tupel, die sich nur um das Vorzeichen unterscheiden, bis auf Vorzeichen den gleichen Kandidaten für einen Teiler liefern.

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

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

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

$$g = b_2t^2 + b_1t + b_0 \in \mathbb{Q}[t]$$

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

$$g = b_2t^2 + b_1t + b_0 \in \mathbb{Q}[t]$$

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 3.10. 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 64 zu betrachtenden Tupel tatsächlich zu Faktoren von f gehören. Wenn die d_i mehr Teiler haben, erhöht sich die Anzahl der Tupel sehr schnell!

Aufgaben

Aufgabe 3.14
Zeige, daß $K := \mathbb{F}_2[t]/\langle t^2 + t + 1\rangle$ ein Körper mit 4 Elementen ist und bestimme die Additions- und Multiplikationstabelle von K.[2]

Aufgabe 3.15
Zeige, daß folgende Polynome irreduzibel sind:

a. $f = t^4 - 12t^2 - 8t + 9 \in \mathbb{Q}[t]$,

b. $f = t^5 - t^4 + t^3 - 2t^2 + 3t - 1 \in \mathbb{Q}[t]$,

c. $f = y^3 - x^2y^2 + x^2 - 3xy + 1 \in \mathbb{Z}[x, y]$.

Aufgabe 3.16
Seien $a_1, \ldots, a_n \in \mathbb{Z}$ paarweise verschieden und $k \in \mathbb{Z}[t]$ normiert mit $\deg(k) < \frac{n}{2}$. Zeige, daß das Polynom

$$f = (t - a_1) \cdot \ldots \cdot (t - a_n) \cdot k - 1$$

irreduzibel in $\mathbb{Z}[t]$ ist.

Hinweis: für eine Zerlegung $f = g \cdot h$ mit $g, h \in \mathbb{Z}[t]$ betrachte man die Zahlen $(g \cdot h)(a_i)$ und $(g + h)(a_i)$ in $\mathbb{Z}$, und man verwende Ergebnisse der Polynominterpolation, nämlich, daß ein Polynom vom Grad d durch seine Werte an $d + 1$ Stellen eindeutig festgelegt ist.

Aufgabe 3.17
Finde in Aufgabe 3.16 ein Beispiel mit $\deg(k) = \frac{n}{2}$, so daß das Polynom f nicht irreduzibel ist.

Aufgabe 3.18
Zeige für $m \geq 1$ die folgenden Aussagen:

a. Die Binomialkoeffizienten $\binom{2^m}{k}$ sind für $k = 1, \ldots, 2^m - 1$ durch 2 teilbar.

b. Das Polynom $f = t^{2^m} + 1$ ist irreduzibel in $\mathbb{Q}[t]$.

Hinweis: in Teil (a) betrachte man das Polynom $(x + y)^{2^m}$ in $\mathbb{Z}/2\mathbb{Z}[x, y]$, und in Teil (b) nutze man dann Teil (a).

[2] Für eine Primzahl p bezeichnet $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ den Körper der Restklassen ganzer Zahlen modulo p, siehe Beispiel 4.3.

Aufgabe 3.19

Berechne eine Primfaktorzerlegung der folgenden Polynome:

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

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

KAPITEL II

Galoistheorie

§ 4 Endliche Körpererweiterungen

A) Körpererweiterungen

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

Definition 4.1 (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 mit neutralem Element 0_{K}.
- $(\mathsf{K} \setminus \{0_{\mathsf{K}}\}, \cdot)$ ist eine abelsche Gruppe mit neutralem Element 1_{K}.
- 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 4.2

a. Wir haben in Definition 4.1 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 4.3

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 1.8 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 4.4 (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 4.5
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 für Ringe ist dann

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

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

B) Primkörper

Definition 4.6 (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 4.7 (Charakteristik)
Ist L ein Körper, so definieren wir

$$n \cdot \alpha = \underbrace{\alpha + \ldots + \alpha}_{n-\text{mal}}$$

für eine natürliche Zahl $n \geq 1$ und ein $\alpha \in L$. Die Abbildung

$$\varphi_L : \mathbb{Z} \longrightarrow L : n \mapsto \begin{cases} n \cdot 1_L, & n \geq 1, \\ 0_L, & n = 0, \\ -n \cdot (-1_L), & n \leq -1 \end{cases}$$

ist dann ein Ringhomomorphismus, wie man leicht nachrechnet. 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 der eindeutig bestimmte nicht-negative Erzeuger des Kerns von φ_L.

Satz 4.8
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 4.7.

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

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

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 $\mathrm{Im}(\varphi_L)$ ein Teilkörper von L. Da der Primkörper 1_L enthält und bezüglich Addition abgeschlossen ist, gilt zudem

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

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

Setzen wir nun $\mathrm{char}(L) = 0$ 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

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

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

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

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

Beispiel 4.9

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 4.10 (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 4.11

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 4.12 (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 4.13
Betrachten wir die Körpererweiterung $\mathbb{C}/\mathbb{R}$ und $\alpha = \mathfrak{i} \in \mathbb{C}$, so gilt

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

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

Bemerkung 4.14 (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]) sowie in Satz 1.25 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 4.15 (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

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

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

$$f = g \cdot \mu_\alpha, \tag{17}$$

und aus der Gradformel folgt

$$\deg(f) = \deg(g) + \deg(\mu_\alpha) \geq \deg(\mu_\alpha), \tag{18}$$

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 (18) sehen wir dann, daß der Faktor g in (17) 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 Korollar 2.14 ein Körper. Wegen des Homomorphiesatzes und Bemerkung 4.14 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 4.16 (Minimalpolynom der sechsten Einheitswurzel)

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

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

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

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

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 4.17 (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 4.18 (Einfache algebraische Körpererweiterungen)
Sei L/K *eine Körpererweiterung und* $\alpha \in L$ *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 $K(\alpha)/K$ *endlich.*

Beweis: Aus Satz 4.15 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 4.19
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.

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

Bemerkung 4.20 (Berechnung der Inversen von $f(\alpha)$)
Sei L/K ein Körpererweiterung und $\alpha \in L$ algebraisch über K mit Minimalpolynom $\mu_\alpha \in K[t]$ vom Grad n.

Aus dem Beweis von Korollar 4.18 ergibt sich unmittelbar, wie man für ein beliebiges Polynom $f \in K[t]$ den Repräsentanten von $f(\alpha)$ in $\mathrm{Lin}(1, \alpha, \ldots, \alpha^{n-1})$ findet. Division mit Rest liefert Polynome $q, r \in K[t]$, so daß

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

mit $\deg(r) \leq n - 1$, und es gilt

$$f(\alpha) = r(\alpha) \in \mathrm{Lin}(1, \alpha, \ldots, \alpha^{n-1}).$$

Zudem wissen wir, daß $f(\alpha)$ genau dann ungleich null und invertierbar ist, wenn μ_α kein Teiler von f ist. Aber wie finden wir in diesem Fall eine Darstellung von

$$\frac{1}{f(\alpha)} \in \mathrm{Lin}(1, \alpha, \ldots, \alpha^{n-1})$$

als Linearkombination von $1, \alpha, \ldots, \alpha^{n-1}$?

Da μ_α irreduzibel ist, folgt aus dem Umstand, daß μ_α kein Teiler von f ist, bereits, daß f und μ_α teilerfremd sind. Mit Hilfe des Euklidischen Algorithmus können wir dann Polynome $g, h \in K[t]$ bestimmen, so daß

$$1 = g \cdot f + h \cdot \mu_\alpha$$

gilt (siehe Bézout-Identität [Mar08a, Satz 7.54]), und erhalten

$$1 = g(\alpha) \cdot f(\alpha) + h(\alpha) \cdot \mu_\alpha(\alpha) = g(\alpha) \cdot f(\alpha)$$

wegen $\mu_\alpha(\alpha) = 0$. Bestimmen wir nun mittels Division mit Rest Polynome $q, r \in K[t]$ mit

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

und $\deg(r) \leq n - 1$, dann gilt

$$\frac{1}{f(\alpha)} = g(\alpha) = r(\alpha) \in \mathrm{Lin}(1, \alpha, \ldots, \alpha^{n-1}).$$

Beispiel 4.21
Aus dem Eisensteinkriterium folgt, daß das Polynom

$$t^3 + 2t + 2 \in \mathbb{Z}[t]$$

irreduzibel in $\mathbb{Z}[t]$ und mithin auch in $\mathbb{Q}[t]$ ist. Wegen des Fundamentalsatzes der Algebra 16.13 hat das Polynom eine Nullstelle α in $\mathbb{C}$ und

$$\mu_\alpha = t^3 + 2t + 2 \in \mathbb{Q}[t]$$

ist das Minimalpolynom von α. Da μ_α Grad 3 hat, gilt

$$\mathbb{Q}(\alpha) = \mathbb{Q}[\alpha] = \left\{ a + b \cdot \alpha + c \cdot \alpha^2 \;\middle|\; a, b \in \mathbb{Q} \right\}$$

und es gibt mithin $a, b, c \in \mathbb{Q}$ mit

$$\frac{1}{\alpha^3+\alpha+1} = a + b\cdot\alpha + c\cdot\alpha^2.$$

Um die Koeffizienten $a, b, c \in \mathbb{Q}$ zu bestimmen, wenden wir den Euklidischen Algorithmus an. Dividieren wir $r_0 = t^3+t+1$ mit Rest durch $r_1 = \mu_\alpha$, so erhalten wir

$$r_0 = t^3+t+1 = 1\cdot(t^3+2t+2)+(-t-1) = 1\cdot r_1 + r_2. \tag{19}$$

Im nächsten Schritt dividieren wir dann r_1 durch $r_2 = -t-1$ mit Rest und erhalten

$$r_1 = t^3+2t+2 = (-t^2+t-3)\cdot(-t-1)+(-1) = (-t^2+t-3)\cdot r_2 + r_3. \tag{20}$$

Da der Rest $r_3 = -1$ konstant ist, ist dies ein größter gemeinsamer Teiler von r_0 und r_1 und wir können danach auflösen und rückeinsetzen:

$$\begin{aligned}
-1 &\overset{(19)}{=} r_1 - \big(-t^2+t-3\big)\cdot r_2 \\
&\overset{(20)}{=} r_1 - \big(-t^2+t-3\big)\cdot(r_0 - 1\cdot r_1) \\
&= \big(-t^2+t-2\big)\cdot r_1 + \big(t^2-t+3\big)\cdot r_0 \\
&= \big(-t^2+t-2\big)\cdot \mu_\alpha + \big(t^2-t+3\big)\cdot\big(t^3+t+1\big).
\end{aligned}$$

Multiplizieren wir die Gleichung mit -1 und setzen α ein, so erhalten wir wegen $\mu_\alpha(\alpha) = 0$

$$1 = \big(-\alpha^2+\alpha-3\big)\cdot\big(\alpha^3+\alpha+1\big)$$

und mithin

$$\frac{1}{\alpha^3+\alpha+1} = -\alpha^2+\alpha-3.$$

Wir haben also das Inverse von $\alpha^3+\alpha+1$ als $\mathbb{Q}$-Linearkombination von $1, \alpha, \alpha^2$ dargestellt, ohne α genauer zu kennen.

D) Endliche Körpererweiterungen

Proposition 4.22 (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

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

für geeignete $\alpha_1, \ldots, \alpha_m \in L$ ist, wobei die Inklusion $\supseteq$ für jede Wahl der α_i ohnehin gilt. Wählen wir $m = n$ und $\alpha_1, \ldots, \alpha_n \in L$ als K-Vektorraumbasis von L, so ist jedes Element von L eine K-Linearkombination 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 4.23
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 4.24 (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 4.25
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 4.24 erhalten wir

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

□

Beispiel 4.26 (Erweiterungen von Primzahlgrad sind einfach.)
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 4.27
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.

Korollar 4.28
Ist L/K *eine Körpererweiterung und sind* $\alpha_1, \ldots, \alpha_n \in L$ *algebraisch über* K*, dann gilt*

$$K(\alpha_1, \ldots, \alpha_n) = K[\alpha_1, \ldots, \alpha_n]$$

und $K(\alpha_1, \ldots, \alpha_n)/K$ *ist endlich und damit algebraisch.*

Beweis: Wir führen den Beweis mit Induktion nach n, wobei der Fall $n = 1$ aus Satz 4.15, Korollar 4.18 und Proposition 4.22 folgt.

Sei also $n > 1$. Mittels Induktion wissen wir, daß

$$K(\alpha_1, \ldots, \alpha_{n-1}) = K[\alpha_1, \ldots, \alpha_{n-1}]$$

und daß $K(\alpha_1, \ldots, \alpha_{n-1})/K$ endlich ist. Wie im Fall $n = 1$ folgt dann

$$K(\alpha_1, \ldots, \alpha_n) = K(\alpha_1, \ldots, \alpha_{n-1})(\alpha_n) = K[\alpha_1, \ldots, \alpha_{n-1}](\alpha_n) = K[\alpha_1, \ldots, \alpha_n],$$

da α_n auch algebraisch über $K(\alpha_1, \ldots, \alpha_{n-1})$ ist, und $K(\alpha_1, \ldots, \alpha_n)/K(\alpha_1, \ldots, \alpha_{n-1})$ ist endlich. Aus Satz 4.24 folgt dann, daß auch $K(\alpha_1, \ldots, \alpha_n)/K$ eine endliche Körpererweiterung ist. □

Beispiel 4.29
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, das i als Nullstelle hat. Somit ist f das Minimalpolynom von i über $\mathbb{Q}(\sqrt{2})$, und wir erhalten für den Grad der Körpererweiterung $\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q}$

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

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

$$\alpha = 3 + \sqrt{2} + 2 \cdot i + 4 \cdot \sqrt{2} \cdot i \notin \mathbb{Q} \tag{21}$$

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

Man kann das Minimalpolynom auch berechnen:

$$\mu_\alpha = t^4 - 12t^3 + 122t^2 - 388t + 1241.$$

Daß α eine Nullstelle diese Polynoms ist, kann man leicht durch einsetzen nachrechnen. Mit Hilfe des Algorithmus 3.12 und etwas Ausdauer kann man auch nachprüfen, daß das Polynom irreduzibel und deshalb das Minimalpolynom ist.

Berechnet wurde das Minimalpolynom mit Hilfe des Open-Source Computeralgebrasystems SINGULAR:

```
                     SINGULAR                                 /Development
A Computer Algebra System for Polynomial Computations   / version 4.1.1
                                                       0<
by: W. Decker, G.-M. Greuel, G. Pfister, H. Schoenemann \ Feb 2018
FB Mathematik der Universitaet, D-67653 Kaiserslautern   \
> ring S=0,t,dp;
> ring R=0,(x,y),dp;
> qring Q=std(ideal(x2-2,y2+1));
> map F=S,ideal(3+x+2y+4xy);
> setring S;
> kernel(Q,F);
_[1]=t4-12t3+122t2-388t+1241
> factorize(t4-12t3+122t2-388t+1241);
[1]:
   _[1]=1
   _[2]=t4-12t3+122t2-388t+1241
[2]:
   1,1
```

Hier werden drei Ringe definiert $S = \mathbb{Q}[t]$, $R = \mathbb{Q}[x, y]$ und

$$Q = \mathbb{Q}[x, y]/\langle x^2 - 2, y^2 + 1\rangle \cong \mathbb{Q}[\sqrt{2}, i]$$

sowie der Ringhomomorphismus

$$F : \mathbb{Q}[t] \longrightarrow \mathbb{Q}[x, y]/\langle x^2 - 2, y^2 + 1\rangle : t \mapsto 3 + x + 2y + 4xy,$$

wobei x der Zahl $\sqrt{2}$ und y der Zahl i entspricht. Die Abbildung F ist also genau der Einsetzhomomorphismus ϕ_α aus Bemerkung 4.14. Sein Kern wird vom Minimalpolynom μ_α erzeugt und dieses wird mit dem Befehl `kernel(Q,F)` berechnet. Mit dem

Befehl `factorize` haben wir lediglich nochmals verifiziert, daß das Polynom auch irreduzibel ist. Unter der URL

`https://www.singular.uni-kl.de`

findet man das Programm SINGULAR zum Download und zur Online-Nutzung.

E) Das Turmgesetz

Bemerkung 4.30
Sei L/K eine Körpererweiterung und sei $N \subseteq L$ eine Teilmenge. Dann können wir den allgemeinen Polynomring $K[x_\alpha \mid \alpha \in N]$ betrachten, dessen Veränderliche durch die Elemente in der Menge N indiziert sind, und wir erhalten aus der universellen Eigenschaft des Polynomrings 1.25 einen K-Algebrenhomomorphismus

$$\varphi_N : K[x_\alpha \mid \alpha \in N] \longrightarrow L$$

mit

$$\varphi_N(x_\alpha) = \alpha,$$

indem in jedem Polynom die Variable x_α einfach durch α ersetzt wird. Es ist üblich, die K-Algebra Bild von φ_α mit

$$K[N] := \mathrm{Im}(\varphi_N)$$

zu bezeichnen, und wir werden das deshalb ebenfalls tun. Es muß aber darauf hingewiesen werden, daß das fahrlässig ist, da wir in Definition 1.20 diesselbe Notation verwendet haben, um den Polynomring $K[x_\alpha \mid \alpha \in N]$ zu bezeichnen, und φ_N ist in aller Regel *kein* Isomorphismus, so daß die beiden K-Algebren wesentlich verschieden sind! Siehe dazu den letzten Satz in Definition 1.20.

Korollar 4.31 (Das Turmgesetz)
Seien $K \leq L \leq M$ *Körper.*

a. *Sind* L/K *und* M/L *algebraisch, so ist* M/K *algebraisch.*

b. *Ist* $N \subseteq L$ *eine Teilmenge von Elementen von* L*, die algebraisch über* K *sind, dann ist*

$$K(N) = K[N]$$

und die Körpererweiterung $K(N)/K$ *ist algebraisch.*

Beweis:

a. Sei $\alpha \in M$ gegeben. Da α algebraisch über L ist, gibt es ein Polynom

$$f = t^n + \beta_{n-1} \cdot t^{n-1} + \ldots + \beta_0 \in L[t]$$

mit $f(\alpha) = 0$. Dann ist α aber schon algebraisch über $K(\beta_0, \ldots, \beta_{n-1})$ und die Körpererweiterung

$$K(\beta_0, \ldots, \beta_{n-1}, \alpha)/K(\beta_0, \ldots, \beta_{n-1})$$

ist nach Korollar 4.18 endlich. Da $\beta_0, \ldots, \beta_{n-1}$ algebraisch über K sind, ist die Körpererweiterung

$$K(\beta_0, \ldots, \beta_{n-1})/K$$

nach Korollar 4.28 endlich, und wegen der Gradformel 4.24 ist dann auch

$$K(\beta_0, \ldots, \beta_{n-1}, \alpha)/K$$

eine endliche Körpererweiterung. Aus Proposition 4.22 folgt schließlich, daß sie auch algebraisch ist. Insbesondere ist dann α algebraisch über K, und somit ist M/K algebraisch.

b. Die Inklusion $K[N] \subseteq K(N)$ ist offensichtlich, da der Körper $K(N)$ mit K und N auch jeden Polynomausdruck in Elementen aus N mit Koeffizienten aus K enthalten muß. Und da K und N in $K[N]$ enthalten sind, reicht es, zu zeigen, daß $K[N]$ ein Körper ist, um die Gleicheheit

$$K(N) = K[N]$$

zu verifizieren. $K[N]$ ist als Bild des Ringhomomorphismus φ_N ein kommutativer Ring mit Eins, und wir müssen nur zeigen, daß jedes $0 \neq f \in K[N]$ in $K[N]$ ein multiplikatives Inverses besitzt.
Sei dazu $0 \neq f \in K[N]$ gegeben. Dann ist f ein Polynom in endlich vielen $\alpha_1, \ldots, \alpha_n \in N$ mit Koeffizienten in K und die α_i sind algebraisch über K. Mithin gilt

$$f \in K[\alpha_1, \ldots, \alpha_n] = K(\alpha_1, \ldots, \alpha_n),$$

wobei die letzte Gleichheit aus Korollar 4.28 folgt. Damit besitzt f also ein multiplikatives Inverses in

$$K(\alpha_1, \ldots, \alpha_n) = K[\alpha_1, \ldots, \alpha_n] \subseteq K[N].$$

Aus Korollar 4.28 wissen wir zudem, daß $K(\alpha_1, \ldots, \alpha_n)$ algebraisch über K ist. Somit ist auch f und damit $K[N] = K(N)$ algebraisch über K.

□

Beispiel 4.32
Die Körpererweiterung

$$\mathbb{Q}(\sqrt{z} \mid z \in \mathbb{Z}_{>0})/\mathbb{Q}$$

ist algebraisch und es gilt

$$\mathbb{Q}(\sqrt{z} \mid z \in \mathbb{Z}_{>0}) = \mathbb{Q}[\sqrt{z} \mid z \in \mathbb{Z}_{>0}].$$

Aufgaben

Aufgabe 4.33
Für einen Körper L bezeichnet

$$\mathrm{Aut}(L) = \{\varphi : L \longrightarrow L \mid \varphi \text{ ist ein Körperautomorphismus}\}$$

die Automorphismengruppe von L. Zeige, ist P der Primkörper von L, so gilt

$$\varphi_{|P} = \mathrm{id}_P$$

für jedes $\varphi \in \mathrm{Aut}(L)$.

Aufgabe 4.34
Seien L/K eine Körpererweiterung und seien $f, g \in K[t]$. Gibt es ein $h \in L[t]$ mit $f = g \cdot h$, so gilt schon $h \in K[t]$

Aufgabe 4.35
Zeige, daß $f = t^3 + 3t + 1 \in \mathbb{Q}[t]$ irreduzibel ist und stelle für ein $\alpha \in \mathbb{C}$ mit $f(\alpha) = 0$ die Zahlen $\frac{1}{\alpha}$ und $\frac{1}{1+\alpha}$ als $\mathbb{Q}$-Linearkombination von $\{1, \alpha, \alpha^2\}$ dar.

Aufgabe 4.36
Zeige, ist p eine Primzahl und $n \geq 2$, dann ist $t^n - p \in \mathbb{Q}[t]$ das Minimalpolynom von $\sqrt[n]{p}$ über $\mathbb{Q}$.

Aufgabe 4.37
Bestimme für folgende $\alpha \in \mathbb{R}$ das Minimalpolynom von α über $\mathbb{Q}$ und den Grad der Körpererweiterung $\mathbb{Q}(\alpha)/\mathbb{Q}$:

a. $\alpha = \sqrt{3} + \sqrt[3]{5}$.

b. $\alpha = \sqrt[3]{\sqrt{5}+2} - \sqrt[3]{\sqrt{5}-2}$

Hinweis: in Teil b. berechne man den Wert zunächst näherungsweise mit einem Rechner.

Aufgabe 4.38 (Minimalpolynom der Körpererweiterung $\mathbb{Q}(\zeta_{11} + \zeta_{11}^{-1})/\mathbb{Q}$)
Sei $\zeta = e^{\frac{2\pi i}{11}} \in \mathbb{C}$ eine primitive elfte Einheitswurzel und sei $\alpha = \zeta + \zeta^{-1} \in \mathbb{C}$. Zeige,

$$f = t^5 + t^4 - 4 \cdot t^3 - 3 \cdot t^2 + 3 \cdot t + 1 \in \mathbb{Q}[t]$$

ist das Minimalpolynom von α über $\mathbb{Q}$.

Hinweis, betrachte bestimme die Potenzen α^i für $i = 0, \ldots, 5$ als Polynome in ζ und nutze ein Polynom aus Beispiel 3.10.

Aufgabe 4.39
Es sei L/K eine endliche Körpererweiterung und $\alpha \in L$ mit $|K(\alpha) : K| = n$.

a. Zeige, die Abbildung

$$f : L \longrightarrow L : x \mapsto \alpha \cdot x$$

ist K-linear und $K(\alpha)$ ist ein f-invarianter Unterraum von L.

b. Zeige, $f_{|K(\alpha)}$ hat bezüglich der Basis $B = (1, \alpha, \ldots, \alpha^{n-1})$ von $K(\alpha)$ die Matrixdarstellung

$$M_B^B(f_{|K(\alpha)}) = \begin{pmatrix} 0 & \ldots & \ldots & \ldots & \ldots & -a_0 \\ 1 & 0 & \ldots & \ldots & \ldots & -a_1 \\ 0 & 1 & 0 & \ldots & 0 & -a_2 \\ \vdots & \ddots & \ddots & \ddots & & \vdots \\ 0 & \ldots & 0 & 1 & 0 & \vdots \\ 0 & \ldots & \ldots & 0 & 1 & -a_{n-1} \end{pmatrix},$$

wenn $\mu_\alpha = t^n + a_{n-1} \cdot t^{n-1} + \ldots + a_0$ das Minimalpolynom von α über K ist.

c. Zeige, μ_α ist das charakteristische Polynom und zugleich das Minimalpolynom von $f_{|K(\alpha)}$ im Sinne der linearen Algebra, d.h.

$$\chi_{f_{|K(\alpha)}} = \det(t \cdot \mathrm{id}_{K(\alpha)} - f_{|K(\alpha)}) = \mu_{f_{|K(\alpha)}} = \mu_\alpha$$

d. Zeige, μ_α ist ein Teiler des charakteristischen Polynoms $\chi_f = \det(t \cdot \mathrm{id}_L - f) \in K[t]$ von f in $K[t]$.

e. Berechne das Minimalpolynom von $\alpha = \sqrt{2} + \sqrt{3} + \sqrt{5}$ über $\mathbb{Q}$.

Aufgabe 4.40
Zeige, eine Körpererweiterung L/K ist genau dann algebraisch, wenn jeder Ring R mit $K \leq R \leq L$ schon ein Körper ist.

Aufgabe 4.41 (Umkehrung von Lemma 13.4)
In der Aufgabe soll gezeigt werden, daß eine einfache, algebraische Körpererweiterung L/K nur endlich viele Zwischenkörper besitzt.

Sei dazu $L = K(\alpha)$ und α sei algebraisch über K mit Minimalpolynom $\mu_\alpha^K \in K[t]$. Ferner sei

$$\mathcal{Z}(L/K) = \{N \mid K \leq N \leq L\}$$

die Menge der Zwischenkörper von L/K und

$$P = \{f \in L[t] \mid f \text{ teilt } \mu_\alpha^K \text{ in } L[t] \text{ und } \mathrm{lc}(f) = 1\}$$

die Menge der normierten Teiler des Polynoms μ_α^K im Polynomring $L[t]$.

a. Zeige, die Abbildung

$$\varphi : \mathcal{Z}(L/K) \longrightarrow P : N \mapsto \mu_\alpha^N,$$

wobei $\mu_\alpha^N \in N[t]$ das Minimalpolynom von α über N bezeichnet, ist wohldefiniert und hat die Linksinverse

$$\psi : P \longrightarrow \mathcal{Z}(L/K) : t^n + a_{n-1}t^{n-1} + \ldots + a_0 \mapsto K(a_0, \ldots, a_{n-1}).$$

b. Zeige, L/K hat höchstens $2^{|L:K|-1}$ Zwischenkörper.

Aufgabe 4.42

Es sei p eine Primzahl, $L = \mathrm{Quot}(\mathbb{F}_p[x, y])$ und $K = \mathrm{Quot}(\mathbb{F}_p[x^p, y^p])$.
Zeige, die Körpererweiterung L/K ist endlich, aber nicht einfach.

Hinweis, betrachte $K(x + ay)$ für $a \in K$ und zeige u.a. $|L : K(y)| = |K(y) : K| = |K(x + ay) : K| = p$.

§ 5 Konstruktionen mit Zirkel und Lineal

A) Der Körper der konstruierbaren Zahlen

Definition und Bemerkung 5.1 (Konstruktionen mit Zirkel und Lineal)
Ziel einer Konstruktion mit Zirkel und Lineal ist es, aus einer gegebenen Menge M von Punkten in der Ebene $\mathbb{R}^2 = \mathbb{C}$ 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 5.2 ($\overline{z} \in \widetilde{M}$)
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 5.3 (Quadratisch abgeschlossen)
Ein Körper K heißt *quadratisch abgeschlossen*, wenn jedes Polynom der Form $t^2 - a \in K[t]$ über K zerfällt.

Satz 5.4 (Körper der konstruierbaren Zahlen)
Ist $0, 1 \in M \subseteq \mathbb{C}$, *so ist* $\widetilde{M}$ *ein quadratisch abgeschlossener Teilkörper von* $\mathbb{C}$.

[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.

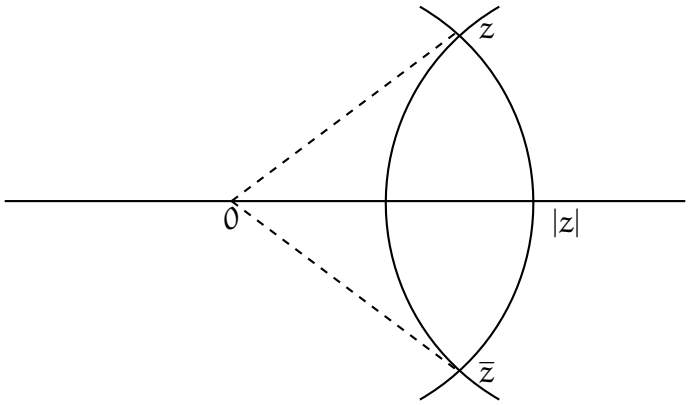

ABBILDUNG 1. Konstruktion von $\bar{z}$ durch Spiegeln

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 $u + v$ 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

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

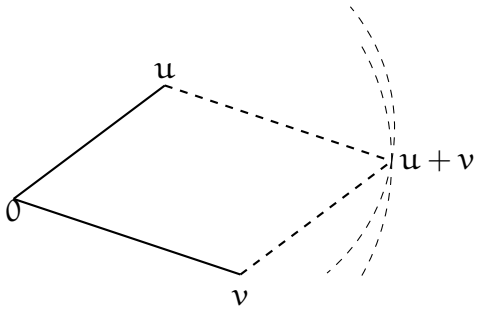

ABBILDUNG 2. Konstruktion der Summe zweier Zahlen

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

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

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 5.2 wissen wir, daß

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

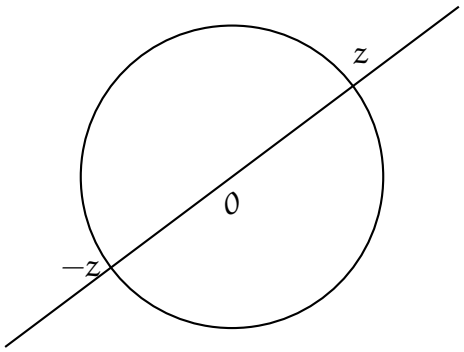

ABBILDUNG 3. Konstruktion des Negativen einer Zahl

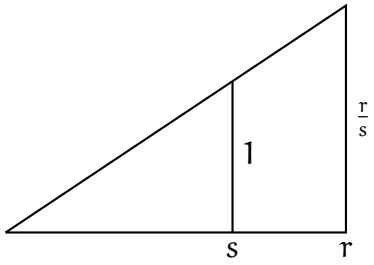

ABBILDUNG 4. Konstruktion von $\frac{r}{s}$

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

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

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 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 $0 \neq z = r \cdot e^{i\varphi} \in \widetilde{M}$ eine Quadratwurzel in $\widetilde{M}$ besitzt.

Aus Beispiel 5.2 wissen wir, daß $r \in \widetilde{M}$, und da $\widetilde{M}$ ein Körper ist, gilt dann auch

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

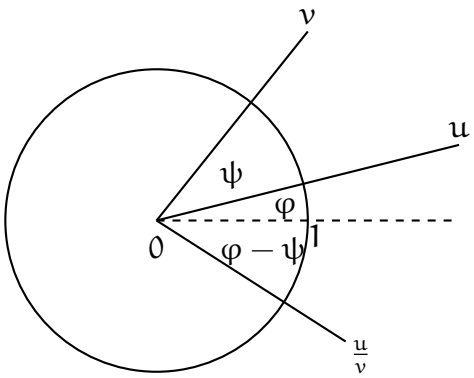

ABBILDUNG 5. Konstruktion von $e^{i\cdot(\varphi-\psi)}$

Schlagen wir um diesen Punkt einen Kreis vom Radius $\frac{r+1}{2} \in \widetilde{M}$ und schneiden diesen mit der mit Zirkel und Lineal konstruierbaren Lotgeraden auf die x-Achse durch 0, so erhalten wir die Figur in Abbildung 6. Aus dem Höhensatz[2] folgt dann,

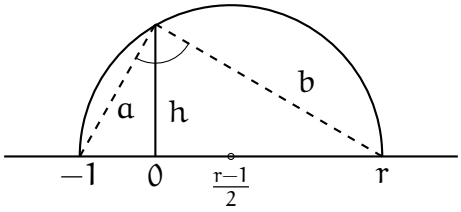

ABBILDUNG 6. Konstruktion der Quadratwurzel $\sqrt{r}$

daß die 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

[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 $r = h^2$.

Quadratwurzel

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

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

Bemerkung 5.5 (Klappzirkel und der Satz von Mohr-Mascheroni)

a. Wir haben in unseren Elementaroperationen einen Zirkel erlaubt, mit dem man die Distanz zwischen zwei Punkten abträgt und als Radius eines Kreises an einem anderen Punkt als Mittelpunkt nutzt. Man spricht dabei von einem festen Zirkel. Euklid nutzte in seinen Elementen [**Euk91**] für Konstruktionen mit Zirkel und Lineal hingegen einen sogenannten *Klappzirkel*. Mit diesem kann man zwar in einem Punkt einstechen, den Abstand zu einem anderen Punkt als Radius abtragen und um den ersten Punkt dann den Kreis mit diesem Radius schlagen, will man den Abstand aber zu einem anderen Punkt transferieren, so klappt der Zirkel beim Hochheben zusammen und man verliert den Radius wieder. Elementaroperationen mit Klappzirkel und Lineal sind auf den ersten Blick also restriktiver, als solche mit festem Zirkel und Lineal. Bei genauerem Hinsehen sieht man jedoch, daß dem nicht so ist. Schon Euklid selbst zeigt in Proposition 2 im ersten Buch der Elemente, daß sich der Abstand zweier Punkte allein mit Hilfe von Klappzirkel und Lineal an jeden anderen Punkt transferieren läßt, und in der Tat reicht sogar ein Klappzirkel alleine aus.

b. Der Satz von Mohr-Mascheroni sagt, daß man bei der Konstruktion mit Zirkel und Lineal sogar auf das Lineal verzichten kann und alleine mit dem Klappzirkel auskommt, ohne dabei konstruierbare Punkte in $\widetilde{M}$ zu verlieren.

B) Konstruierbarkeit und 2-Radikalerweiterungen

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

Bemerkung 5.6 (Körpererweiterungen für Elementaroperationen)
Es sei K ein Teilkörper von $\mathbb{C}$ mit $i \in K$ und 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

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

sowie

$$|z|^2 = z \cdot \overline{z} \in K.$$

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 sich der Schnittpunkt aus der Lösung eines linearen Gleichungssystems mit Koeffizienten in K ergibt. Genauer gilt für den Schnittpunkt

$$z = u_1 + \lambda \cdot (v_1 - u_1) = u_2 + \mu \cdot (v_2 - u_2)$$

zweier Geraden

$$g_1 = \{u_1 + \lambda \cdot (v_1 - u_1) \mid \lambda \in \mathbb{R}\}$$

und

$$g_2 = \{u_2 + \mu \cdot (v_2 - u_2) \mid \mu \in \mathbb{R}\}$$

durch Punkte $u_j = a_j + i \cdot b_j, v_j = c_j + i \cdot d_j \in \mathbb{R}$, daß die Koeffizienten λ und μ Lösungen des linearen Gleichungssystems

$$\begin{aligned} (a_1 - c_1) \cdot \lambda + (c_2 - a_2) \cdot \mu &= c_2 - c_1 \\ (b_1 - d_1) \cdot \lambda + (d_2 - b_2) \cdot \mu &= d_2 - d_1 \end{aligned} \tag{22}$$

sind. Da die Koeffizienten des Gleichungssystems in K liegen trifft das auch auf die Lösung $(\lambda, \mu)^t$ und mithin auf $z = u_1 + \lambda \cdot (v_1 - u_1)$ zu.

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

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

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 von $\omega^2 \in K$ adjungieren müssen, um die Gleichung in $K(\omega)$ lösen und die Schnittpunkte $u + \lambda \cdot (v - u)$ in $K(\omega)$ berechnen 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 $v = c + id \in K$ 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.

Bemerkung 5.7

a. Ist $M \subseteq \mathbb{C}$ eine Teilmenge von $\mathbb{C}$ und $\overline{M} = \{\overline{z} \mid z \in M\}$, so erfüllt der Körper $K = \mathbb{Q}(M \cup \overline{M})$ die Bedingung $\overline{z} \in K$ für alle $z \in K$.
Um dies zu sehen, beachten wir, daß die Komplexe Konjugation

$$\iota : \mathbb{C} \longrightarrow \mathbb{C} : z \mapsto \overline{z}$$

ein Körperisomorphismus ist. Für jeden Zwischenkörper L von $\mathbb{C}/\mathbb{Q}$ der $\mathbb{Q}$, M und $\overline{M}$ enthält, ist dann $\iota(L)$ ebenfalls ein Zwischenkörper von $\mathbb{C}/\mathbb{Q}$, der $\mathbb{Q} = \iota(\mathbb{Q})$, $\overline{M} = \iota(M)$ und $M = \iota(\overline{M})$ enthält. Mithin gilt

$$\mathbb{Q}(M \cup \overline{M}) = \bigcap_{\substack{\mathbb{Q} \le L \le \mathbb{C} \\ \mathbb{Q}, M, \overline{M} \subseteq L}} L = \bigcap_{\substack{\mathbb{Q} \le L \le \mathbb{C} \\ \mathbb{Q}, M, \overline{M} \subseteq L}} \iota(L) = \iota\big(\mathbb{Q}(M \cup \overline{M})\big).$$

b. Für den Körper K in Teil a. erfüllt auch $K(i)$ die Bedingung $\overline{z} \in K(i)$ für alle $z \in K(i)$, da mit i auch $-i = \overline{i} \in K(i)$ gilt und somit $K(i) = \mathbb{Q}(N \cup \overline{N})$ für $N = M \cup \{i\}$.

c. Die Aussagen in Teil b. und c. von Bemerkung 5.6 bleiben korrekt, wenn auf die Bedingung $i \in K$ verzichten.
In dem Fall folgt aus $u \in K$ nur noch $i \cdot \mathrm{Im}(u) \in K$ und nicht mehr, daß der Imaginärteil selbst in K enthalten ist. In Bemerkung 5.6 b. reicht das aber aus, da wir in Gleichung 22 dann die zweite Zeile einfach mit der imaginären Einheit i multiplizieren können. Für den Teil c. in der Bemerkung benötigen wir den Imaginärteil von Elementen in K gar nicht, so daß die Begründung hier unverändert bleiben kann.

d. Die Bedingung $\overline{z} \in K$ für alle $z \in K$ reicht nicht aus, um $\mathrm{Im}(z) \in K$ für alle $z \in K$ zu erhalten.
Um dies zu sehen, betrachten wir das Beispiel $K = \mathbb{Q}(\zeta)$ mit $\zeta = e^{\frac{2\pi i}{3}}$. Da ζ eine primitive dritte Einheitswurzel mit Minimalpolynom

$$\mu_\zeta = t^2 + t + 1 \in \mathbb{Q}[t]$$

ist, kennen wir den Körper K sehr genau:

$$K = \{a + b \cdot \zeta + c \cdot \zeta^2 \mid a, b, c \in \mathbb{Q}\} = \{a + b \cdot \zeta + c \cdot \overline{\zeta} \mid a, b, c \in \mathbb{Q}\}.$$

Also erfüllt K die Bedingung $\overline{z} \in K$ für $z \in K$. Würde zudem $\mathrm{Im}(\zeta) \in K$ gelten, so hätten wir auch wegen $i \cdot \mathrm{Im}(\zeta) \in K$ auch $e^{\frac{2\pi i}{4}} = i = \frac{i \cdot \mathrm{Im}(\zeta)}{\mathrm{Im}(\zeta)} \in K$. Mithin wäre aber auch die primitive 12-te Einheitswurzel

$$e^{\frac{2\pi i}{12}} = e^{(4+\frac{1}{12})\cdot 2\pi i} = e^{\frac{49}{12}\cdot 2\pi i} = \left(e^{\frac{7}{12}\cdot 2\pi i}\right)^7 = \left(e^{\frac{2\pi i}{4} + \frac{2\pi i}{3}}\right)^7 = (i \cdot \zeta)^7 \in K$$

in K. Aber in Satz 13.15 werden wir den Grad der zugehörigen Körpererweiterung als

$$|\mathbb{Q}(e^{\frac{2\pi i}{12}})/\mathbb{Q}| = |\mathbb{Z}_{12}^*| = 4$$

berechnen, was im Widerspruch dazu steht, daß es sich bei $\mathbb{Q}(e^{\frac{2\pi i}{12}})$ um einen Zwischenkörper von K handeln soll.

Definition 5.8 (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

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

und wegen der Gradformel dann

$$|L : K| = |K_n : K_{n-1}| \cdot \ldots \cdot |K_1 : K_0| = 2^n.$$

Korollar 5.9 (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. Es gibt eine 2-Radikalerweiterung L/K *mit* $z \in L$.

Insbesondere ist dann z *algebraisch über* K *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, wenn wir vorab zunächst die Quadratwurzel i aus -1 adjungieren, so folgt aus Bemerkung 5.6, daß in jedem Schritt höchstens eine Quadratwurzel adjungiert werden muß. Also gibt es eine 2-Radikalerweiterung L/K, so daß z in L enthalten ist.

Ist umgekehrt L/K eine 2-Radialerweiterung mit $z \in L$ und ist

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

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

Wir zeigen mit abbrechender Induktion nach j, daß

$$K_j \subseteq \widetilde{M}$$

gilt, wobei die Aussage für $n = 0$

$$K_0 = K = \mathbb{Q}\big(M \cup \overline{M}\big) \overset{5.4,5.2}{\subseteq} \widetilde{M}$$

aus Satz 5.4 und Beispiel 5.2 folgt. Sei nun bereits

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

gezeigt. Da $\widetilde{M}$ quadratisch abgeschlossen ist (siehe Satz 5.4), folgt

$$\omega_j \in \widetilde{M}$$

und mithin auch

$$K_j = K_{j-1}(\omega_j) \subseteq \widetilde{M}.$$

Für $j = n$ erhalten wir dann, daß

$$z \in L = K_n \subseteq \widetilde{M}$$

mit Zirkel und Lineal konstruierbar ist.

Die Aussage zum Grad der Körpererweiterung folgt aus der Gradformel 4.24 wegen

$$|K(z) : K| \,\Big|\, |L : K| = 2^n.$$

□

C) Anwendung auf klassische elementargeometrische Fragen

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

Bemerkung 5.10 (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 5.9 nicht mit Zirkel und Lineal konstruierbar. Das Delische Problem ist also nicht lösbar.

Bemerkung 5.11 (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 5.9). Die Quadratur des Kreises ist also nicht möglich.

Bemerkung 5.12 (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 3.1) und Satz 3.3, 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 5.9 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 5.13 (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 13.F)).

Aufgaben

Aufgabe 5.14
Zeige, daß man mit Hilfe von Klappzirkel und Lineal einen Kreis, dessen Radius dem Abstand zweier gegebener Punkte A und B entspricht, um einen beliebigen gegebenen dritten Punkt C schlagen kann.

[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 4.14). 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 3.3 anwendbar sind.

Aufgabe 5.15
Zeige, daß man alleine mit Hilfe eines Klappzirkels einen Kreis, dessen Radius dem Abstand zweier gegebener Punkte A und B entspricht, um einen beliebigen gegebenen dritten Punkt C schlagen kann.

Aufgabe 5.16
Beweise oder widerlege: man kann mit Zirkel und Lineal zu einem gegebenen Dreieck ein flächengleiches Quadrat konsturieren.

Aufgabe 5.17
Es sei K ein Teilkörper von $\mathbb{R}$ und $\alpha \in \mathbb{C}$ entstehe durch eine Elementaroperation wie in Definition 5.1, wobei die beteiligten Punkte Koordinaten in K haben. Dann gibt es ein $a \in K$ mit $a > 0$, so daß α Koordinaten in $K[\sqrt{a}]$ hat.

Aufgabe 5.18
Wir wollen einen Teilkörper K von $\mathbb{R}$ *positiv-quadratisch* abgeschlossen nennen, wenn für $a \in K$ und $a > 0$ stets auch $\sqrt{a} \in K$ gilt.

Zeige, für $M = \{0, 1\}$ ist der Teilkörper der konstruierbaren Zahlen $\mathbb{R} \cap \widetilde{M}$ in $\mathbb{R}$ der kleinste positiv-quadratisch abgeschlossene Teilkörper von $\mathbb{R}$.

Aufgabe 5.19 (Körpererweiterungen vom Grad 2)
Es sei L/K eine Körpererweiterung vom Grad $|L : K| = 2$.

a. Zeige, wenn $\mathrm{char}(K) \neq 2$, dann ist L/K eine 2-Radikalerweiterung.

b. Gilt die Aussage in a. auch noch, wenn $\mathrm{char}(K) = 2$?

§ 6 Zerfällungskörper

Im Abschnitt 4 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 Korollar 2.14 eine triviale Angelegenheit.

Definition 6.1 (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.

Beispiel 6.2 (Stammkörper)
Der Körper $\mathbb{C} = \mathbb{R}(i)$ der komplexen Zahlen ist ein Stammkörper des Polynoms $f = t^2 + 1$ als Polynom in $\mathbb{R}[t]$. Der Körper

$$\mathbb{Q}(i) = \mathbb{Q}[i] = \{a + b \cdot i \mid a, b \in \mathbb{Q}\}$$

der ganzen Gaußschen Zahlen ist ein Stammkörper desselben Polynoms als Polynom in $\mathbb{Q}[t]$. Der Begriff des Stammkörpers hängt also nicht alleine vom Polynom ab, sondern auch von dem Polynomring, in dem man es betrachtet.

Satz 6.3 (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 $\bar{t}$.

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

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

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 Körperhomomorphismus ist und somit K und $\varphi(K)$ nach Lemma 4.5 isomorph sind, ist das eine zulässige Identifizierung.

a. Aus Korollar 2.14 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

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

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

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

Da zudem $\overline{t}$ als Nullstelle des Polynoms f algebraisch ist, gilt nach Satz 4.15

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

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

□

Beispiel 6.4 (Stammkörper)

a. In Aufgabe 3.14 wurde der Stammkörper

$$L = \mathbb{F}_2[t]/\langle t^2 + t + 1\rangle = \{\overline{0}, \overline{1}, \overline{t}, \overline{t+1}\}$$

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

b. Das Polynom $f = t^2 + 1 \in \mathbb{F}_3[t]$ ist irreduzibel, weil es in $\mathbb{F}_3$ keine Nullstelle hat. Mithin ist dann

$$L = \mathbb{F}_3[t]/\langle t^2 + 1\rangle$$

ein Stammkörper von f, der genau $3^{\deg(f)} = 3^2 = 9$ Elemente besitzt.

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 6.5 (Erweiterung von Körperisomorphismen auf Polynomringe)
Ist die Abbildung

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

ein Körperisomorphismus, so ist die Abbildung

$$K[t] \longrightarrow K'[t] : \sum_{k=0}^{n} a_k t^k \mapsto \sum_{k=0}^{n} \varphi(a_k) t^k \tag{23}$$

ein Ringisomorphismus, den 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 6.6 (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 (23) in Bemerkung 6.5 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 4.15 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 6.3 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

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

und das Bild von α berechnet sich als

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

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

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

und es folgt $\Psi = \psi$. □

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

Korollar 6.7 (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 6.6 mit $\varphi = \mathrm{id}_K$. □

Beispiel 6.8 (Stammkörper)
Das Polynom $f = t^4 - 2 \in \mathbb{Q}[t]$ ist aufgrund des Eisenstein-Kriteriums 3.1 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) Existenz von Zerfällungskörpern

Definition 6.9 (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 6.10 (Zerfällungskörper)
Ein Zerfällungskörper L von f ist ein Erweiterungskörper von K, über dem f 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 6.11 (Zerfällungskörper)

a. Der Körper
$$\mathbb{C} = \mathbb{R}(i) = \mathbb{R}(i, -i)$$
ist der Zerfällungskörper des Polynoms
$$f = t^2 + 1 = (t - i) \cdot (t + i) \in \mathbb{R}[t].$$

b. In Beispiel 6.4 haben wir
$$L = \mathbb{F}_3[t]/\langle t^2 + 1\rangle$$
als Stammkörper des Polynoms $f = t^2 + 1$ über $\mathbb{F}_3$ kennengelernt und wir kennen die Nullstelle $\overline{t}$ von f in diesem Körper. Da f ein Polynom vom Grad 2 ist und wir den zu $\overline{t}$ gehörenden Linearfaktor abspalten können, muß auch die zweite Nullstelle von f in L liegen. Man sieht leicht
$$f(\overline{2t}) = \overline{2t}^2 + \overline{1}1 = \overline{t^2 + 1} = \overline{0}$$
und es folgt
$$f = \big(t - \overline{t}\big) \cdot \big(t - \overline{2t}\big).$$
Dann ist aber
$$L = \mathbb{F}_3[t]/\langle t^2 + 1\rangle = \mathbb{F}_3\big(\overline{t}\big) = \mathbb{F}_3\big(\overline{t}, \overline{2t}\big)$$
auch der Zerfällungskörper von f über $\mathbb{F}_3$.

Satz 6.12 (Existenz von Zerfällungskörpern)
Zu jedem Polynom $0 \neq f \in K[t]$ 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 6.13

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 6.8 und könnten den Zerfällungskörper also sofort angeben, wollen die Konstruktion im obigen Beweis aber nachverfolgen.

Da f irreduzibel ist, erhalten wir im ersten Schritt also den Erweiterungskörper

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

Über diesem faktorisiert f als

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

Das Polynom

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

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 $\mathbb{Q}$.

Da Zerfällungskörper im weiteren Verlauf der Vorlesung eine sehr wichtige Rolle spielen, wollen wir noch in einem weiteren Beispiel einen Zerfällungskörper berechnen.

Beispiel 6.14
Wir betrachten das Polynom

$$f = t^4 - 10t^2 + 18 \in \mathbb{Q}[t].$$

Eine Nullstelle $\alpha \in \mathbb{C}$ von f ist dann durch die Gleichung

$$\left(\alpha^2 - 5\right)^2 = 7$$

charakterisiert, und somit hat f die vier Nullstellen

$$\alpha_1 = \sqrt{5+\sqrt{7}},\ \ \alpha_2 = \sqrt{5-\sqrt{7}},\ \ \alpha_3 = -\sqrt{5+\sqrt{7}} \quad \text{und} \quad \alpha_4 = -\sqrt{5-\sqrt{7}}.$$

Der Zerfällungskörper von f über $\mathbb{Q}$ ist mithin

$$\mathrm{ZFK}_{\mathbb{Q}}(f) = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_2, \alpha_4) = \mathbb{Q}(\alpha_1, \alpha_2),$$

wobei die letzte Gleichheit aus $\alpha_3 = -\alpha_1$ und $\alpha_4 = -\alpha_2$ folgt.

C) Eindeutigkeit des Zerfällungskörpers

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 6.15 (Fortsetzbarkeit von Isomorphismen auf Zerfällungskörper)
Es sei $\varphi : K \longrightarrow K'$ ein Körperisomorphismus, L sei ein Zerfällungskörper von $0 \neq f \in K[t]$ 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 6.6 erhalten wir dann eine Fortsetzung

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

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 6.16 (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 6.15 mit $\varphi = \mathrm{id}_K$. □

Bemerkung 6.17 (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.

D) Gradabschätzung für Zerfällungskörper

Die folgende Proposition liefert uns eine Apriori-Abschätzung für den Grad eines Zerfällungskörpers.

Proposition 6.18 (Obere Schranke für den Grad des Zerfällungskörpers)
Ist $L = \mathrm{ZFK}_K(f)$ *der Zerfällungskörper eines Polynoms* $0 \neq f \in K[t]$ *vom Grad* $\deg(f) = n$, *so ist der Grad der Körpererweiterung* $|L : K|$ *ein Teiler von* $n!$ *und damit gilt insbesondere*

$$|\,\mathrm{ZFK}_K(f) : K| \leq n!.$$

Beweis: Wir führen den Beweis durch Induktion nach n, wobei für $n = 0$ wegen wegen $L = K$ nichts zu zeigen ist.

Sei nun $n > 0$ und sei g ein normierter irreduzibler Faktor von f, so daß

$$g = (t - \alpha_1) \cdot \ldots \cdot (t - \alpha_k)$$

und

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

gilt. Ist $f = \mathrm{lc}(f) \cdot g$ irreduzibel, so ist

$$L = K(\alpha_1)(\alpha_2, \ldots, \alpha_n) = \mathrm{ZFK}_{K(\alpha_1)}\left(\frac{f}{t - \alpha_1}\right),$$

so daß mit Induktion die Ungleichung

$$|L : K(\alpha_1)| \;\Big|\; (n-1)!$$

folgt. Zudem ist g dann das Minimalpolynom von α_1 über K und es gilt

$$|K(\alpha_1) : K| = \deg(g) = \deg(f) = n,$$

und wir erhalten insgesamt

$$|L : K| = |L : K(\alpha_1)| \cdot |K(\alpha_1) : K| \;\Big|\; (n-1)! \cdot n = n!.$$

Ist hingegen f nicht irreduzibel, so gilt $l = \deg(g) < n$ und $m = \deg(h) < n$. Nach Induktionsvoraussetzung gilt für den Zerfällungskörper

$$N = \mathrm{ZFK}_K(g) = K(\alpha_1, \ldots, \alpha_k) \subseteq L$$

dann

$$|N : K| \;\Big|\; l!.$$

Außerdem ist

$$L = N(\alpha_{k+1}, \ldots, \alpha_n) = \mathrm{ZFK}_N(h)$$

und nach Induktionsvoraussetzung gilt deshalb auch

$$|L : N| \;\Big|\; m!.$$

Wegen $\binom{l+m}{l} = \frac{(l+m)!}{l! \cdot m!}$ ist der Nenner ein Teiler des Zählers und wir erhalten

$$|L : K| = |L : N| \cdot |N : K| \;\Big|\; l! \cdot m! \;\Big|\; (l+m)! = n!.$$

□

Beispiel 6.19 (Zerfällungskörper)

a. Aus der Zerlegung $f = (t^2-2)\cdot(t^2+1) = (t-\sqrt{2})\cdot(t+\sqrt{2})\cdot(t+i)\cdot(t-i) \in \mathbb{Q}[t]$ folgt, daß

$$\mathrm{ZFK}_{\mathbb{Q}}(f) = \mathbb{Q}\big(\sqrt{2}, i\big)$$

der Zerfällungskörper von f über $\mathbb{Q}$ ist. Den Grad der Körpererweiterung

$$|\,\mathrm{ZFK}_{\mathbb{Q}}(f) : \mathbb{Q}| = 4$$

kennen wir aus Beispiel 4.29. Die in Proposition 6.18 angegebene obere Schranke $4! = 24$ ist erheblich größer als der tatsächliche Grad.

b. Betrachten wir das Polynom

$$f = t^3 - 2 = \big(t - \sqrt[3]{2}\big) \cdot \big(t - \sqrt[3]{2} \cdot \zeta\big) \cdot \big(t - \sqrt[3]{2} \cdot \zeta^2\big) \in \mathbb{Q}[t]$$

mit der dritten Einheitswurzel

$$\zeta = e^{\frac{2\pi i}{3}},$$

so erhalten wir aus der Zerlegung des Polynoms unmittelbar den Zerfällungskörper

$$\mathrm{ZFK}_{\mathbb{Q}}(f) = \mathbb{Q}\big(\sqrt[3]{2}, \sqrt[3]{2} \cdot \zeta, \sqrt[3]{2} \cdot \zeta^2\big) = \mathbb{Q}\big(\sqrt[3]{2}, \zeta\big),$$

wobei wir für die letzte Gleichheit die Gleichung

$$\zeta = \frac{\sqrt[3]{2} \cdot \zeta}{\sqrt[3]{2}} \in \mathrm{ZFK}_{\mathbb{Q}}(f)$$

beachten. Da f nach dem Eisensteinkriterium irreduzibel in $\mathbb{Q}[t]$ ist, ist f das Minimalpolynom von $\sqrt[3]{2}$ und wir haben

$$3 = \deg(f) = \left|\mathbb{Q}\left(\sqrt[3]{2}\right) : \mathbb{Q}\right| \;\Big|\; |\operatorname{ZFK}_{\mathbb{Q}}(f) : \mathbb{Q}|.$$

Zudem ist ζ eine Nullstelle des Polynoms

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

und keine Nullstelle von $t - 1$. Mithin ist das irreduzible (siehe Beispiel 3.10) Polynom

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

das Minimalpolynom von ζ und wir erhalten

$$2 = \deg(g) = \left|\mathbb{Q}(\zeta) : \mathbb{Q}\right| \;\Big|\; |\operatorname{ZFK}_{\mathbb{Q}}(f) : \mathbb{Q}|.$$

Dann gilt aber auch

$$6 = 2 \cdot 3 \;\Big|\; |\operatorname{ZFK}_{\mathbb{Q}}(f) : \mathbb{Q}|$$

und mit Proposition 6.18 gilt umgekehrt auch

$$|\operatorname{ZFK}_{\mathbb{Q}}(f) : \mathbb{Q}| \;\Big|\; 3! = 6.$$

Insgesamt erhalten wir damit

$$|\operatorname{ZFK}_{\mathbb{Q}}(f) : \mathbb{Q}| = 6 = 3!,$$

was zeigt, daß die obere Schranke für den Grad des Zerfällungskörpers in Proposition 6.18 auch angenommen werden kann.

Aufgaben

Aufgabe 6.20
Es sei $p \in \mathbb{Z}_{>0}$.

a. Bestimme zwei komplexe Zahlen $\alpha, \beta \in \mathbb{C}$, so daß $\operatorname{ZFK}_{\mathbb{Q}}(f) = \mathbb{Q}(\alpha, \beta)$ der Zerfällungskörper von $f = t^p - 2 \in \mathbb{Q}[t]$ über $\mathbb{Q}$ ist.

b. Berechne in Teil a. den Grad der Körpererweiterung $|\operatorname{ZFK}_{\mathbb{Q}}(f) : \mathbb{Q}|$, wenn p eine Primzahl ist.

Aufgabe 6.21
Es sei L/K ein Körpererweiterung, $f \in K[t]$ ein Polynom vom Grad 2 und $\alpha \in L$ eine Nullstelle von f. Zeige, dann ist ist $K(\alpha)$ der Zerfällungskörper von f über K.

Aufgabe 6.22
Bestimme den Zerfällungskörper $\operatorname{ZFK}_{\mathbb{F}_3}(f)$ von $f = t^3 - t + 1 \in \mathbb{F}_3[t]$.

Aufgabe 6.23
Sei L/K eine endliche Körpererweiterung vom Grad m und $f \in K[t]$ ein irreduzibles Polynom vom Grad n. Zeige, wenn m und n teilerfremd sind, so ist f auch irreduzibel in $L[t]$.

Hinweis, nutze aus, daß es eine Körpererweiterung von L gibt, in der f eine Nullstelle hat.

Aufgabe 6.24 (Zerfällungskriterium und Transitivität der Galoisgruppe)
Sei K ein Körper und $L = ZFK_K(f)$ der Zerfällungskörper eines Polynoms $f \in K[t]$. Ferner sei $g \in K[t]$ irreduzibel und $N = ZFK_K(g)$ sei der Zerfällungskörper von g über K.

a. Zeige, wenn $\alpha \in N$ und $\beta \in N$ zwei Nullstellen von g sind, dann gibt es einen Körperisomorphismus
$$\varphi : L(\alpha) \longrightarrow L(\beta)$$
mit $\varphi_{|K} = \mathrm{id}_K$ und $\varphi(\alpha) = \beta$.

b. Zeige, wenn g eine Nullstelle in L hat, so zerfällt g über L schon.

c. Zeige, ist f irreduzibel, dann gibt es einen Isomorphismus
$$\varphi : L \longrightarrow L$$
mit $\varphi_{|K} = \mathrm{id}_K$ und $\varphi(\alpha) = \beta$.

§ 7 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.

A) Endliche Körper und der Frobeniushomomorphismus

Proposition 7.1 (Endliche Körper haben Primzahlpotenzordnung.)
Ist K *ein endlicher Körper, so ist* $\operatorname{char}(K) = p \in \mathbb{P}$ *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 4.8 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 als P-Vektorraum isomorph zu P^n und seine Mächtigkeit ist

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

□

Beispiel 7.2 (Ein Körper mit vier Elementen.)
Der endliche Körper

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

aus Beispiel 6.4 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 7.3 (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, da 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 Potenzgesetze 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 4.5 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 7.4

Betrachten wir den Körper $K = \mathbb{F}_2[t]/\langle t^2+t+1\rangle$ aus Beispiel 7.2, 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 7.5 (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 7.3 ein Isomorphismus. □

B) Mehrfache Nullstellen

Definition 7.6 (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 7.7 (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

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

Lemma 7.8 (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

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

□

Beispiel 7.9
Betrachten wir das Polynom

$$f = t^5 + 3t^4 - 6t^3 + 14t^2 - 27t + 15 \in \mathbb{Q}[t],$$

so gilt

$$f(1) = 1 + 3 - 6 + 14 - 27 + 15 = 0$$

und mithin ist 1 eine Nullstelle von f. Für die Ableitung

$$f' = 5t^4 + 12t^3 - 18t^2 + 28t - 27 \in \mathbb{Q}[t]$$

gilt ebenfalls

$$f'(1) = 5 + 12 - 18 + 28 - 27 = 0.$$

Also ist 1 eine mehrfache Nullstelle von f, und in der Tat hat f die Primfaktorzerlegung

$$f = (t-1)^2 \cdot (t^2 + 3) \cdot (t + 5).$$

C) Existenz und Eindeutigkeit eines Körpers mit p^n Elementen

Satz 7.10 (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 und damit η_p^n 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

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

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

Korollar 7.11 (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 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 6.16 bis auf Isomorphie eindeutig bestimmt ist, ist K isomorph zu dem Körper in Satz 7.10. □

Beispiel 7.12

a. Der Körper $\mathbb{F}_2[x]/\langle x^2 + x + 1\rangle$ aus Beispiel 6.4 hat 2^2 Elemente und ist mithin der Zerfällungskörper des Polynoms

$$f = t^{2^2} - t = t^4 - t = t \cdot (t-1) \cdot \left(t^2 + t + 1\right) \in \mathbb{F}_2[t].$$

b. Die Polynome $x^3 + x + 1 \in \mathbb{F}_2[x]$ und $x^3 + x^2 + 1 \in \mathbb{F}_2[x]$ haben in $\mathbb{F}_2$ keine Nullstelle und sind als Polynome vom Grad 3 mithin irreduzibel. Die Körpererweiterung der zugehörigen Stammkörper

$$K = \mathbb{F}_2[x]/\langle x^3 + x + 1\rangle$$

und

$$L = \mathbb{F}_2[x]/\langle x^3 + x^2 + 1\rangle$$

über $\mathbb{F}_2$ hat jeweils den Grad

$$|K : \mathbb{F}_2| = \deg\left(x^3 + x + 1\right) = 3 = \deg\left(x^3 + x^2 + 1\right) = |L : \mathbb{F}_2|.$$

Mithin sind K und L jeweils Körper mit $2^3 = 8$ Elementen, weshalb

$$K \cong L \cong \mathrm{ZFK}_{\mathbb{F}_2}\left(t^{2^3} - t\right)$$

gilt und beides Zerfällungsköper des Polynoms

$$\left(t^{2^3} - t\right) = \left(t^8 - t\right) = t \cdot (t-1) \cdot \left(t^3 + t + 1\right) \cdot \left(t^3 + t^2 + 1\right) \in \mathbb{F}_2[t]$$

sind.

Bemerkung 7.13
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 13.1 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. In Korollar 13.3 zeigen wir schließlich, daß die Vereinigung aller $\mathrm{GF}(p^n)$ den algebraischen Abschluß von $\mathbb{F}_p$ im Sinne von Abschnitt 8 liefert. Dieser ist dann kein endlicher Körper mehr, sondern besitzt abzählbar unendlich viele Elemente.

Aufgaben

Aufgabe 7.14
Zeige, jeder endliche Integritätsbereich ist ein Körper.

Hinweis, für $0 \neq a \in R$ betrachte man die Abbildung $\varphi : R \longrightarrow R : x \mapsto a \cdot x$.

Aufgabe 7.15
Sei K ein Körper, $\alpha \in K$, $k \in \mathbb{Z}_{>0}$ und $f, g \in K[t]$. Beweise die folgenden Rechenregeln für formale Ableitungen:

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

b. $\left((t-\alpha)^k\right)' = k \cdot (t-\alpha)^{k-1}$.

Aufgabe 7.16 (n-te Einheitswurzeln)
Es sei K ein Körper mit $|K| = q$ Elementen und $n \in \mathbb{N}$ sei teilerfremd zu q. Ferner sei $m = \mathrm{ord}(\overline{q})$ die Ordnung von $\overline{q} \in (\mathbb{Z}/n\mathbb{Z})^*$ von $\overline{q}$ als Element der multiplikativen Gruppe $(\mathbb{Z}/n\mathbb{Z})^*$.

a. Zeige, der Zerfällungskörper $\mathrm{ZFK}_K(t^n - 1)$ ist in $\mathrm{ZFK}_K(t^{q^m} - t)$ enthalten und

$$|\mathrm{ZFK}_K(t^{q^m} - t)| = q^m.$$

Insbesondere, die n-ten Einheitswurzeln sind in $\mathrm{GF}(q^m)$ enthalten.

b. Bestimme den Grad der Körpererweiterung $\mathrm{ZFK}_{\mathbb{F}_2}(t^7 - 1)$ über $\mathbb{F}_2$.

Aufgabe 7.17

Sei K ein Körper mit $\mathrm{char}(K) = p > 0$ und sei $f = t^p - a \in K[t]$.

Zeige, f ist genau dann reduzibel in $K[t]$, wenn es ein $\alpha \in K$ mit $a = \alpha^p$ gibt.

Hinweis, für die Hinrichtung zeige und nutze man, daß aus $\alpha^p \in K$ und $\alpha^m \in K$ für ein $1 \leq m \leq p - 1$ schon $\alpha \in K$ folgt.

§ 8 Der algebraische Abschluß

In diesem Abschnitt führen wir den Begriff des algebraischen Abschlusses eines Körpers ein und zeigen, daß jeder Körper bis auf Isomorphie einen eindeutigen algebraischen Abschluß besitzt.

A) Einfache Eigenschaften des algebraischen Abschlusses

Definition 8.1 (Algebraischer Abschluß)
Sei K ein Körper.

a. Der Körper K heißt *algebraisch abgeschlossen*, wenn jedes nicht-konstante Polynom $f \in K[t]$ in K eine Nullstelle hat.

b. Ein Erweiterungskörper L von K heißt ein *algebraischer Abschluß* von K, wenn L/K algebraisch ist und L algebraisch abgeschlossen ist.

Es ist nicht ganz einfach, Beispiele für algebraisch abgeschlossene Körper zu geben, weil diese von Natur aus recht groß sind.

Beispiel 8.2 (Algebraischer Abschluß)
Der Fundamentalsatz der Algebra (siehe Satz 16.13) besagt, daß der Körper $\mathbb{C}$ der komplexen Zahlen algebraisch abgeschlossen ist. Damit ist $\mathbb{C}$ dann ein algebraischer Abschluß von $\mathbb{R}$, da $\mathbb{C}/\mathbb{R}$ algebraisch ist.

Wir wollen zunächst einige einfache, aber wichtige weitergehende Eigenschaften von algebraisch abgeschlossenen Körpern festhalten.

Proposition 8.3 (Algebraisch abgeschlossene Körper)
Es sei K ein algebraisch abgeschlossener Körper.

a. Ist $f \in K[t]$ ein nicht-konstantes Polynom, so zerfällt f in $K[t]$ in Linearfaktoren. Insbesondere enthält K alle Nullstellen von f in Erweiterungskörpern.

b. Ist L/K eine algebraische Körpererweiterung, so gilt schon $L = K$.

Beweis:

a. Den Beweis führen wir mit Induktion nach dem Grad n von f. Für $n = 1$ hat f nur eine Nullstelle und diese liegt nach Voraussetzung dann in K. Ist $n > 1$ so hat f in K eine Nullstelle α. Diese können wir als Linearfaktor abspalten und erhalten ein Polynom g vom Grad $n-1$ mit

$$f = (t - \alpha) \cdot g.$$

Nach Induktionsvoraussetzung zerfällt g über K in Linearfaktoren

$$g = c \cdot (t - \alpha_1) \cdot \ldots \cdot (t - \alpha_{n-1})$$

mit $c, \alpha_1, \ldots, \alpha_{n-1} \in K$ und somit zerfällt auch f über K in Linearfaktoren

$$f = c \cdot (t - \alpha) \cdot (t - \alpha_1) \cdot \ldots \cdot (t - \alpha_{n-1}).$$

Ist L/K eine Körpererweiterung und ist $\beta \in L$ eine Nullstelle von f, dann gilt

$$0 = f(\beta) = c \cdot (\beta - \alpha_1) \cdot \ldots \cdot (\beta - \alpha_n),$$

woraus $\beta = \alpha_i$ für ein $i \in \{1, \ldots, n\}$ und damit $\beta \in K$ folgt. Die Nullstellen von f in L sind also alle in K enthalten.

b. Sei $\alpha \in L$. Da α algebraisch über K ist, gibt es ein nicht-konstantes Polynom $f \in K[t]$, so daß α eine Nullstelle von f ist. Mit Teil a. liegt α dann schon in K.

□

B) Existenz eines algebraischen Abschlusses

Ein algebraischer Abschluß eines Körpers K wird die Eigenschaft des Körpers L im folgenden Lemma sicher erfüllen. Die Existenz des Körpers L im Lemma ist der erste Schritt im Beweis der Existenz eines algebraischen Abschlusses.

Lemma 8.4 (Konstruktionsschritt zum algebraischen Abschluß)
Es sei K ein Körper. Dann existiert eine algebraische Körpererweiterung L/K, so daß jedes nicht-konstante Polynom $f \in K[t] \setminus K$ eine Nullstelle in L hat.

Beweis nach Emil Artin: Wir betrachten die Menge

$$\Lambda = \{f \in K[t] \mid \deg(f) \geq 1\}$$

der nicht-konstanten Polynome und den zugehörigen allgemeinen Polynomring

$$K[\Lambda] = K[x_f \mid f \in \Lambda].$$

Ferner betrachten wir in diesem Polynomring das Ideal

$$I = \langle f(x_f) \mid f \in \Lambda \rangle \trianglelefteq K[\Lambda].$$

Man beachte, daß das Polynom $f(x_f)$ aus $f \in K[t]$ entsteht, indem man t durch die Veränderliche x_f ersetzt, und daß deshalb keine zwei der Erzeuger von I von derselben Veränderlichen abhängen.

Wir wollen nun zeigen, daß I ein echtes Ideal ist, und nehmen dafür das Gegenteil

$$I = K[\Lambda]$$

an. Dann gibt es Polynome $f_1, \ldots, f_k \in \Lambda$ und $g_1, \ldots, g_k \in K[\Lambda]$, so daß

$$1 = \sum_{i=1}^{k} g_i \cdot f_i(x_{f_i}). \tag{24}$$

Der Zerfällungskörper $ZFK_K(f)$ für $f = f_1 \cdot \ldots \cdot f_k \in K[t]$ ist eine K-Algebra, in der wir für jedes der f_i eine Nullstelle α_i wählen können. Aus der universellen Eigenschaft des Polynomrings 1.25 erhalten wir dann einen K-Algebrenhomomorphismus

$$\varphi : K[\Lambda] \longrightarrow ZFK_K(f)$$

mit

$$\varphi(x_{f_i}) = \alpha_i$$

für $i = 1, \ldots, k$ und

$$\varphi(x_f) = 0$$

für $f \in \Lambda \setminus \{f_1, \ldots, f_k\}$. Wenden wir diesen auf die Gleichung (24) an, so erhalten wir den Widerspruch

$$1 = \varphi(1) = \sum_{i=1}^{k} \varphi(g_i) \cdot f_i\big(\varphi(x_{f_i})\big) = \sum_{i=1}^{k} \varphi(g_i) \cdot f_i(\alpha_i) = \sum_{i=1}^{k} \varphi(g_i) \cdot 0 = 0.$$

Also muß

$$I \subsetneqq K[\Lambda]$$

gelten und I ist ein echtes Ideal in $K[\Lambda]$.

Proposition 2.8 liefert uns dann ein maximales Ideal

$$I \subseteq \mathfrak{m} \lhd \cdot\, K[\Lambda],$$

das I enthält, und wir setzen

$$L := K[\Lambda]/\mathfrak{m}.$$

Wegen Proposition 2.12 ist L dann ein Körper und

$$K \longrightarrow L : a \mapsto \overline{a}$$

ist ein Köpermonomorphismus, d.h. L enthält K als den Teilkörper der Restklassen der konstanten Polynome, und wir können L/K mit dieser Identifikation als Körpererweiterung betrachten.

Wir halten zunächst fest, daß jedes nicht-konstante Polynom $f \in K[t] \setminus K$ in L eine Nullstelle hat, da aus

$$f(x_f) \in I \subseteq \mathfrak{m}$$

unmittelbar

$$f\big(\overline{x_f}\big) = \overline{f(x_f)} = 0_L$$

folgt. Zugleich ist damit auch gezeigt, daß die Restklasse $\overline{x_f}$ der Veränderlichen x_f algebraisch über K ist. Aus Korollar 4.31 erhalten wir dann, daß

$$L = K[\Lambda]/\mathfrak{m} = K\big[\overline{x_\lambda} \;\big|\; \lambda \in \Lambda\big]$$

algebraisch über K ist. □

Satz 8.5 (Existenz eines algebraischen Abschlusses)
Jeder Körper K besitzt einen algebraischen Abschluß.

Beweis nach Emil Artin: Wir setzen $K_0 := K$ und konstruieren mit Hilfe von Lemma 8.4 eine algebraische Körpererweiterung K_1/K_0, so daß jedes nicht-konstante Polynom in $K_0[t]$ eine Nullstelle in K_1 hat. Dann fahren wir mit K_1 analog fort und konstruieren so rekursiv eine Kette von Körpern

$$K_0 \subseteq K_1 \subseteq K_2 \subseteq \ldots,$$

so daß jeweils K_{i+1}/K_i algebraisch ist und jedes Polynom in $K_i[t]$ eine Nullstelle in K_{i+1} besitzt. Schließlich definieren wir

$$\overline{K} := \bigcup_{i=0}^{\infty} K_i$$

und wollen zeigen, daß dies ein algebraischer Abschluß von K ist.

Sind $\alpha, \beta, \gamma \in \overline{K}$, dann gibt es ein K_i, das alle drei enthält, da die K_j eine aufsteigende Kette bilden. Wir können alle Körperaxiome mit diesen drei Elementen also in K_i nachprüfen, so daß sie erfüllt sind. $\overline{K}$ ist deshalb ein Körper und er enthält mit K_0 auch K.

Ist $\alpha \in \overline{K}$ gegeben, so gibt es ein $i \in \mathbb{N}$ mit $\alpha \in K_i$. Indem wir das Turmgesetz 4.31 endlich oft anwenden, erhalten wir zudem, daß K_i algebraisch über $K_0 = K$ ist. Somit ist insbesondere α algebraisch über K, und damit ist die Körpererweiterung $\overline{K}/K$ algebraisch.

Sei nun $f \in \overline{K}[t]$ ein nicht-konstantes Polynom. Dann hat f nur endlich viele Koeffizienten und mithin gibt es ein $i \in \mathbb{N}$, so daß $f \in K_i[t]$ liegt. Dann hat f nach Konstruktion aber eine Nullstelle in $K_{i+1} \subseteq \overline{K}$. Also ist $\overline{K}$ algebraisch abgeschlossen und damit ein algebraischer Abschluß von K. □

C) Einbettungssatz und Eindeutigkeit des algebraischen Abschlusses

Wir wollen nun noch die Eindeutigkeit des algebraischen Abschlusses eines Körpers K zeigen, und beweisen dafür zunächst den folgenden Fortsetzungssatz für algebraische Erweiterungen von K.

Satz 8.6 (Fortsetzungsssatz für algebraische Erweiterungen)
Sei L/K eine algebraische Körpererweiterung, $\overline{K}$ ein algebraischer Abschluß von K, Z ein Zwischenkörper von L/K und $\phi : Z \longrightarrow \overline{K}$ ein Körpermonomorphismus mit $\phi_{|K} = \mathrm{id}_K$. Dann gibt es einen Körpermonomorphismus

$$\varphi : L \longrightarrow \overline{K}$$

mit $\varphi_{|Z} = \phi$.

Beweis: Wir werden den Beweis mit Hilfe des Lemmas von Zorn führen. Dazu betrachten wir die Menge

$$M = \{(N, \varphi) \mid Z \leq N \leq L, \varphi : N \hookrightarrow \overline{K} \text{ ein Monomorphismus mit } \varphi_{|Z} = \phi\}$$

der Zwischenkörper von L/Z mit Einbettung in $\overline{K}$, die auf Z mit ϕ übereinstimmen. Die Menge ist nicht leer, da (Z, ϕ) in M liegt. Definieren wir

$$(N, \varphi) \leq (N', \varphi') \quad :\Longleftrightarrow \quad N \subseteq N' \text{ und } \varphi'_{|N} = \varphi$$

für $(N, \varphi), (N', \varphi') \in M$, dann sieht man leicht, daß M mit "$\leq$" teilgeordnet ist.

Sei nun C eine Kette in M. Dann setzen wir

$$N' := \bigcup_{(N,\varphi)\in C} N$$

und wir definieren eine Abbildung

$$\varphi' : N' \longrightarrow \overline{K}$$

durch

$$\varphi'(\alpha) = \varphi(\alpha),$$

wenn $\alpha \in N$ für ein $(N, \varphi) \in C$ gilt. Das für die Definition von $\varphi'(\alpha)$ gewählte (N, φ) mit $\alpha \in N$ muß nicht eindeutig sein, aber wenn $(\tilde{N}, \tilde{\varphi})$ ein zweites Element in der Kette C ist mit $\alpha \in \tilde{N}$, dann gilt $\varphi(\alpha) = \tilde{\varphi}(\alpha)$, so daß φ' wohldefiniert ist. Wir wollen nun zeigen, daß (N', φ') eine obere Schranke von C in M ist.

Dazu müssen wir zeigen, daß N' ein Zwischenkörper von L/Z ist und daß φ' ein Körpermonomorphismus ist, der auf Z mit ϕ übereinstimmt. Sind $\alpha, \beta \in N'$, so gibt es $(N_\alpha, \varphi_\alpha), (N_\beta, \varphi_\beta) \in C$ mit $\alpha \in N_\alpha$ und $\beta \in N_\beta$. Da C eine Kette ist, gilt ohne Einschränkung $N_\alpha \subseteq N_\beta$ und damit

$$\alpha \pm \beta \in N_\beta \subseteq N'$$

und

$$\alpha \cdot \beta \in N_\beta \subseteq N'$$

sowie für $\beta \neq 0$ auch

$$\frac{\alpha}{\beta} \in N_\beta \subseteq N'.$$

Ferner gilt

$$\varphi'(\alpha + \beta) = \varphi_\beta(\alpha + \beta) = \varphi_\beta(\alpha) + \varphi_\beta(\beta) = \varphi'(\alpha) + \varphi'(\beta)$$

und

$$\varphi'(\alpha \cdot \beta) = \varphi_\beta(\alpha \cdot \beta) = \varphi_\beta(\alpha) \cdot \varphi_\beta(\beta) = \varphi'(\alpha) \cdot \varphi'(\beta)$$

sowie für $x \in Z$

$$\varphi'(x) = \varphi_\beta(x) = \phi(x).$$

Beachten wir noch

$$Z \subseteq N',$$

so ist N' ein Teilkörper von L, der Z enthält, also ein Zwischenkörper von L/Z. Zudem ist φ' ein Körperhomomorphismus mit $\varphi'_{|Z} = \phi$, und als solcher ist φ' auch injektiv.

Damit ist $(N', \varphi') \in M$ gezeigt, und per Konstruktion ist (N', φ') eine obere Schranke für die Elemente von C. Wir können das Lemma von Zorn 2.4 also anwenden und erhalten ein maximales Element

$$(N, \varphi) \in M.$$

Es reicht zu zeigen, daß dann notwendigerweise

$$N = L$$

gelten muß. Dazu nehmen wir an, das sei nicht der Fall, und wählen ein Element $\alpha \in L \setminus N$. Nach Voraussetzung ist α algebraisch über K und somit auch über dem größeren Körper N. Sei nun

$$\mu_\alpha = t^n + a_{n-1}t^{n-1} + \ldots + a_0 \in N[t]$$

das Minimalpolynom von α über N. Mit der Fortsetzung von φ auf die Polynomringe über N aus Bemerkung 6.5 und

$$N' := \varphi(N)$$

ist dann

$$\varphi(\mu_\alpha) = t^n + \varphi(a_{n-1}) \cdot t^{n-1} + \ldots + \varphi(a_0) \in N'[t] \subseteq \overline{K}[t]$$

irreduzibel in $N'[t]$, da

$$\varphi : N \longrightarrow N'$$

ein Körperisomorphismus ist. Da $\overline{K}$ algebraisch abgeschlossen ist, besitzt f in $\overline{K}$ eine Nullstelle α'. Nun ist $N(\alpha)$ ein Stammkörper von μ_α und $N'(\alpha')$ ist ein Stammkörper von $\varphi(\mu_\alpha)$, und somit besitzt φ nach Proposition 6.6 eine Fortsetzung

$$\psi : N(\alpha) \xrightarrow{\cong} N'(\alpha') \subseteq \overline{K}$$

mit

$$\psi_{|N} = \varphi.$$

Dann wäre aber $(N(\alpha), \psi)$ ein Element von M, das echt größer wäre als (N, φ) im Widerspruch zur Maximalität von (N, φ). Also muß

$$N = L$$

gelten, und der Satz ist bewiesen. □

Korollar 8.7 (Einbettungssatz)
Sei L/K eine algebraische Körpererweiterung und sei $\overline{K}$ ein algebraischer Abschluß von K. Dann gibt es einen Körpermonomorphismus

$$\varphi : L \longrightarrow \overline{K}$$

mit $\varphi_{|K} = \mathrm{id}_K$.

Beweis: Dies folgt aus Satz 8.6 mit $N = K$ und $\phi = \mathrm{id}_K$. □

Korollar 8.8 (Eindeutigkeit des algebraischen Abschlusses)
Jeder Körper K besitzt bis auf Isomorphie genau einen algebraischen Abschluß, den wir mit $\overline{K}$ bezeichnen.

Beweis: Seien L und $\overline{K}$ zwei algebraische Abschlüsse von K. Dann ist L/K algebraisch und nach dem Einbettungssatz 8.7 gibt es einen Körpermonomorphismus

$$\varphi : L \longrightarrow \overline{K}.$$

Der Zwischenkörper $\varphi(L)$ von $\overline{K}/K$ ist als isomorphes Bild des algebraisch abgeschlossenen Körpers L algebraisch abgeschlossen. Zudem ist $\overline{K}$ algebraisch über $\varphi(L)$, da $\overline{K}$ schon algebraisch über K ist. Aus Proposition 8.3 wissen wir dann aber, daß schon

$$\varphi(L) = \overline{K}$$

gelten muß, und mithin ist φ ein Isomorphismus zwischen L und $\overline{K}$. □

Bemerkung 8.9 (Einbettungssatz)
Der Einbettungssatz besagt letztlich, daß wir jede algebraische Körpererweiterung eines Körpers K als Unterkörper seines eindeutigen algebraischen Abschlusses realisieren können.

Beispiel 8.10 (Der algebraische Abschluß der Primkörper)

a. Da der Körper $\mathbb{Q}$ im algebraisch abgeschlossenen Körper $\mathbb{C}$ enthalten ist, können wir den algebraischen Abschluß $\overline{\mathbb{Q}}$ des Primkörpers $\mathbb{Q}$ als Zwischenkörper von $\mathbb{C}/\mathbb{Q}$ realisieren. Er enthält aber nur abzählbar unendlich viele Elemente und ist somit erheblich kleiner als $\mathbb{C}$.
Um dies zu sehen, beachten wir zunächst, daß wir bei der Konstruktion des algebraischen Abschlusses im ersten Schritt gemäß Lemma 8.4 für jedes nichtkonstante Polynom $f \in \mathbb{Q}[t]$ eine Nullstelle von f an $\mathbb{Q}$ adjungiert haben. Da $\mathbb{Q}$ abzählbar ist, gibt es für jeden festen Grad n auch nur abzählbar viele Polynome vom Grad n und somit insgesamt nur abzählbar viele Polynome in $\mathbb{Q}[t]$. Mithin entsteht diese erste Körpererweiterung K_1 im Beweis von Satz 8.5 durch Adjunktion von abzählbar vielen komplexen Zahlen an $\mathbb{Q}$. Die Menge K_1 der Polynomausdrücke in diesen abzählbar vielen komplexen Zahlen mit Koeffizienten in einem abzählbaren Körper ist aber immer noch abzählbar. Mit demselben Argument sind dann alle K_i im Beweis von Satz 8.5 abzählbar und somit auch deren Vereinigung $\overline{\mathbb{Q}}$.

b. Ist p eine Primzahl, so bestimmen wir den algebraischen Abschluß $\overline{\mathbb{F}_p}$ des Primkörpers $\mathbb{F}_p$ in Korollar 13.3 als abzählbare Vereinigung endlicher Körper und sehen somit insbesondere, daß auch dieser abzählbar unendlich ist.

Aufgaben

Aufgabe 8.11
Zeige, daß die folgenden Aussagen für einen Körper K äquivalent sind:

a. K ist algebraisch abgeschlossen.

b. Jedes irreduzible Polynom in $\mathsf{K}[\mathsf{t}]$ hat Grad eins.

c. Ist L/K eine algebraische Körpererweiterung, so ist $\mathsf{L} = \mathsf{K}$.

d. Es gibt einen Teilkörper $\mathsf{N} \leq \mathsf{K}$ von K so, daß K/N algebraisch ist und daß jedes Polynom in $\mathsf{N}[\mathsf{t}] \setminus \mathsf{N}$ über K in Linearfaktoren zerfällt.

Aufgabe 8.12
Zeige, daß ein algebraisch abgeschlossener Körper niemals ein angeordneter Körper sein kann.

Aufgabe 8.13
Sei K ein Körper und $\mathsf{f} \in \mathsf{K}[\mathsf{t}] \setminus \mathsf{K}$ ein nicht-konstantes Polynom.

a. Zeige, genau dann hat f im algebraischen Abschluß $\overline{\mathsf{K}}$ von K eine mehrfache Nullstelle, wenn f und seine formale Ableitung f' in $\mathsf{K}[\mathsf{t}]$ nicht teilerfremd sind.

b. Sind f und f' teilerfremd in $\mathsf{K}[\mathsf{t}]$, so hat f keinen mehrfachen Primteiler in seiner Primfaktorzerlegung.

§ 9 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.

A) Charkterisierung normaler Körpererweiterungen

Definition 9.1 (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 oder ein *Automorphismus von* L/K, 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 9.2 (Automorphismen von $\mathbb{C}/\mathbb{R}$)
Da $\mathbb{C}$ algebraisch abgeschlossen ist (siehe Satz 16.13), 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 6 eingeführten Zerfällungskörpern.

Satz 9.3 (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 und* $\psi \in \mathrm{Gal}\,(M/K)$*, so gilt* $\psi(L) \subseteq L$.

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

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 6.16 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 als

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

für geeignete $\alpha_1, \ldots, \alpha_n \in L$ nach Proposition 4.22. 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 $K[t]$, das 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 6.7 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 6.15 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.: Da L/K endlich ist, haben wir wie im letzten Schritt

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

für geeignete $\alpha_i \in L$, die algebraisch über K sind (siehe Proposition 4.22). 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. □

Beispiel 9.4 (Normale Körpererweiterungen)

a. Die Körpererweiterung $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ ist nicht normal, weil nur eine der drei Nullstellen des Polynoms $t^3 - 2$ in $\mathbb{Q}(\sqrt[3]{2})$ enthalten ist.
Die Körpererweiterung
$$\mathbb{Q}\left(\sqrt[3]{2}, \zeta\right) \,/\, \mathbb{Q},$$
mit $\zeta = e^{\frac{2\pi i}{3}}$, ist hingegen normal, weil
$$\mathbb{Q}\left(\sqrt[3]{2}, \zeta\right) = \mathrm{ZFK}_{\mathbb{Q}}\left(t^3 - 2\right)$$
der Zerfällungskörper des Polynoms $t^3 - 2 \in \mathbb{Q}[t]$ ist, wie wir aus Beispiel 6.19 wissen.

b. Betrachten wir für eine Primzahl p den Körper $K = \mathbb{F}_p(x^p)$ als Teilkörper von $L = \mathbb{F}_p(x)$, so gilt
$$(t - x)^p = t^p - x^p \in K[t].$$
Mithin ist
$$L = K(x) = \mathrm{ZFK}_K(t^p - x^p)$$
und die Körpererweiterung L/K ist normal.

B) Folgerungen aus der Charakterisierung

Korollar 9.5 (Grad-2-Erweiterungen sind normal.)
Jede Körpererweiterung vom Grad 2 ist normal.

Beweis: Sei L/K eine Körpererweiterung vom Grad 2. Da 2 eine Primzahl ist, wissen wir aus Beispiel 4.26, daß dann $L = K(\alpha)$ für ein $\alpha \in L$ gilt. Ist $\mu_\alpha \in K[t]$ das Minimalpolynom von α über K, dann gilt

$$\deg(\mu_\alpha) = |L : K| = 2.$$

Wenn wir nun in L den Linearfaktor $t - \alpha$ abspalten, so finden wir ein $\beta \in L$ mit

$$\mu_\alpha = (t - \alpha) \cdot (t - \beta).$$

Aber dann ist

$$L = K(\alpha) = K(\alpha, \beta) = ZFK_K(\mu_\alpha)$$

Zerfällungskörper eines Polynoms in $K[t]$ und mithin ist L/K normal. □

Korollar 9.6
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

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

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

$$L = N(\alpha_1, \ldots, \alpha_n) = ZFK_N(f),$$

und somit ist L/N nach Satz 9.3 normal. □

Beispiel 9.7
Sei L der Zerfällungskörper des Polynoms

$$f = t^4 - 2 = \left(t - \sqrt[4]{2}\right) \cdot \left(t + \sqrt[4]{2}\right) \cdot \left(t - \sqrt[4]{2} \cdot i\right)\left(t + \sqrt[4]{2} \cdot i\right) \in \mathbb{Q}[t].$$

Wegen

$$i = \frac{\sqrt[4]{2} \cdot i}{\sqrt[4]{2}} \in L$$

folgt dann

$$L = \mathbb{Q}\left(\sqrt[4]{2}, i\right).$$

Dabei ist f das Minimalpolynom von $\sqrt[4]{2}$ über $\mathbb{Q}$, da es nach Eisenstein irreduzibel ist, und $t^2 + 1$ das Minimalpolynom von i über

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

da i nicht in diesem rein reellen Körper liegt und $t^2 + 1$ deshalb über selbigem irreduzibel sein muß. Damit erhalten wir

$$|M : \mathbb{Q}| = \left|\mathbb{Q}\left(\sqrt[4]{2}\right) : \mathbb{Q}\right| = \deg(t^4 - 2) = 4$$

und

$$|L : M| = \left|\mathbb{Q}\left(\sqrt[4]{2}, i\right) : \mathbb{Q}\left(\sqrt[4]{2}\right)\right| = \deg(t^2 + 1) = 2$$

sowie mit Hilfe der Gradformel

$$|L : \mathbb{Q}| = \left|L : \mathbb{Q}\left(\sqrt[4]{2}\right)\right| \cdot \left|\mathbb{Q}\left(\sqrt[4]{2}\right) : \mathbb{Q}\right| = 2 \cdot 4 = 8.$$

Wegen

$$\sqrt[4]{2}^2 = \sqrt{2}$$

ist

$$N := \mathbb{Q}(\sqrt{2})$$

ein echter Zwischenkörper von $M/\mathbb{Q} = \mathbb{Q}\left(\sqrt[4]{2}\right)/\mathbb{Q}$ und aus der Gradformel

$$2 \cdot 2 = 4 = |M : \mathbb{Q}| = |M : N| \cdot |N : \mathbb{Q}|$$

und der Eindeutigkeit der Primfaktorzerlegung folgt dann notwendigerweise

$$|M : N| = \left|\mathbb{Q}\left(\sqrt[4]{2}\right) : \mathbb{Q}(\sqrt{2})\right| = 2$$

und

$$|N : \mathbb{Q}| = \left|\mathbb{Q}\left(\sqrt{2}\right) : \mathbb{Q}\right| = 2.$$

Wir erhalten damit einen Turm von Zwischenkörpern von $L/\mathbb{Q}$, so daß alle sich daraus ergebenden Körpererweiterungen normal sind (siehe Abbildung 7), bis auf die Körperweiterung $M/\mathbb{Q} = \mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$, die nicht normal ist, da das Polynom $t^4 - 2$ nur zwei seiner vier Nullstellen in M hat.

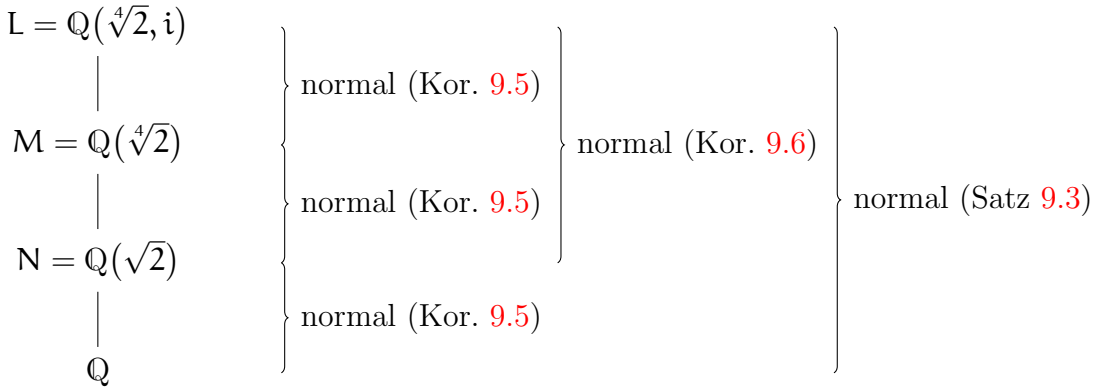

ABBILDUNG 7. Körperturm mit vielen normalen Erweiterungen

C) Die Galoisgruppe normaler Zwischenkörper

Wir wollen den Abschnitt mit einer Feststellung abschließen, die erklärt, weshalb normale Körpererweiterungen *normal* genannt werden. Dazu beweisen wir zunächst eine Hilfsaussage.

Lemma 9.8 (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

$$\varphi = \sigma \circ \psi \circ \sigma^{-1} \in \sigma \circ \mathrm{Gal}\,(L/N) \circ \sigma^{-1}.$$

□

Daraus leiten wir unmittelbar die folgende Eigenschaft von normalen Körpererweiterungen ab, die die Begriffsbildung erhellt.

Proposition 9.9 (N/K normal, dann $\mathrm{Gal}\,(L/N)$ Normalteiler in $\mathrm{Gal}\,(L/K)$)
Sei L/K *eine Körpererweiterung und sei* N *ein Zwischenkörper von* L/K*, so daß* N/K *endlich und normal ist, dann ist* $\mathrm{Gal}(L/N)$ *ein Normalteiler von* $\mathrm{Gal}(L/K)$.

Beweis: Wir beachten, daß jeder N-Automorphismus von L auch ein K-Automorphismus von L ist, so daß $\mathrm{Gal}\,(L/N)$ eine Teilmenge und damit eine Untergruppe von $\mathrm{Gal}\,(L/K)$ ist. Ist nun $\sigma \in \mathrm{Gal}\,(L/K)$ gegeben, so gilt wegen Satz 9.3

$$\sigma(N) = N,$$

weil N/K endlich und normal ist. Aus Lemma 9.8 folgt dann

$$\sigma \circ \mathrm{Gal}\,(L/N) \circ \sigma^{-1} = \mathrm{Gal}\,(L/\sigma(N)) = \mathrm{Gal}\,(L/N)\,.$$

Also ist $\mathrm{Gal}\,(L/N) \trianglelefteq \mathrm{Gal}\,(L/K)$ ein Normalteiler. □

Beispiel 9.10
In Beispiel 9.7 haben wir $L = \mathbb{Q}(\sqrt[4]{2}, i)$ als Körpererweiterung von $\mathbb{Q}$ sowie den Zwischenkörper $N = \mathbb{Q}(\sqrt{2})$ betrachtet. Weil $N/\mathbb{Q}$ normal ist, wissen wir, daß $\mathrm{Gal}\,(L/N)$ ein Normalteiler in $\mathrm{Gal}\,(L/\mathbb{Q})$ ist, obwohl wir die Galoisgruppen zum gegenwärtigen Zeitpunkt noch gar nicht kennen.

Aufgaben

Aufgabe 9.11
Überprüfe, ob die Körpererweiterung $\mathbb{Q}(\alpha)/\mathbb{Q}$ mit $\alpha = \sqrt{4+\sqrt{7}}$ normal ist und bestimme ihren Grad.

Aufgabe 9.12
Zeige, eine algebraische Körpererweiterung L/K ist genau dann normal, wenn es eine Teilmenge P von $K[t]$ gibt, so daß L die Menge der Nullstellen der Polynome in P ist.

Aufgabe 9.13
Sei L/K eine algebraische Körpererweiterung. Zeige, daß die folgenden Eigenschaften äquivalent sind:

a. L/K ist normal.

b. Es gibt eine Teilmenge P von $K[t]$, so daß L aus K durch die Adjunktion der Nullstellen in $\overline{L}$ der Polynome in P entsteht.

c. Für jeden Körpermonomorphismus $\varphi : L \longrightarrow \overline{L}$ mit $\varphi_{|K} = \mathrm{id}_K$ gilt $\varphi(L) = L$.

Aufgabe 9.14 (Die normale Hülle von L/K)
Es sei L/K ein algebraische Körpererweiterung.

a. Zeige, es gibt eine Körpererweiterung N/L, so daß N/K normal ist und so daß es keinen echten Zwischenkörper $L < M < N$ mit M/K normal gibt.

b. Zeige, daß der Körper N in Teil a. bis auf Isomorphie eindeutig bestimmt ist.

Aufgabe 9.15 (2-Radikalerweiterungen)
Beweise oder widerlege, daß jede 2-Radikalerweiterung normal ist.

§ 10 Separable Körpererweiterungen

Separabilität ist eine Eigenschaft, die in Charakteristik null stets gegeben ist, in positiver Charakteristik in vielen weitergehenden Kontexten aber zu Problemen führt. Es geht um die Frage, ob irreduzible Polynome mehrfache Nullstellen haben können. In dem Fall wird die Galois-Gruppe des zugehörigen Zerfällungskörpers kleiner ausfallen, als erwartet, wie wir genauer in Abschnitt 11 sehen werden.

A) Separable Polynome

Definition 10.1 (Separable Polynome)
Es sei K ein Körper.

a. Ein Polynom $f \in K[t]$ heißt *separabel* über K, wenn seine irreduziblen Faktoren in $K[t]$ keine mehrfachen Nullstellen in $\mathrm{ZFK}_K(f)$ haben.

b. Der Körper K heißt *vollkommen*, wenn jedes Polynom $f \in K[t]$ separabel ist.

Beispiel 10.2

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 10.3 (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 $\alpha \in \mathrm{ZFK}_K(f)$ eine Nullstelle von f. Da f irreduzibel ist, ist α keine mehrfache Nullstelle von f und somit ist $f'(\alpha) \neq 0$ nach Lemma 7.8, 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 7.8 folgt, daß α eine Nullstelle von f' ist, und wegen $\deg(f') < \deg(f)$ muß $f' = 0$ gelten. □

Beispiel 10.4 (Eine nicht separabele Körpererweiterung)
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 3.1 irreduzibel über $\mathbb{F}_p[x]$ und nach Satz 3.3 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 10.3 *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 10.5 (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 10.3. □

B) Separable Körpererweiterungen

Definition 10.6 (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 10.7

a. In Charakteristik 0 ist jede algebraische Körpererweiterung separabel.

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

Lemma 10.8
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

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

für geeignete $\alpha_1, \ldots, \alpha_n \in L$, die algebraisch über K sind. Ein Körpermonomorphismus $\varphi : L \hookrightarrow M$ mit $\varphi_{|K} = \mathrm{id}_K$ ist dann durch die Bilder der α_i eindeutig festgelegt.

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 $\mu_{\alpha_i} = \sum_{j=0}^{m} a_j t^j \in K_{i-1}[t]$ das Minimalpolynom von α_i über dem Körper K_{i-1}, so gilt

$$\varphi(\mu_{\alpha_i})\big(\varphi(\alpha_i)\big) = \sum_{j=0}^{m} \varphi(a_j) \cdot \varphi(\alpha_i)^j = \varphi\left(\sum_{j=0}^{m} a_j \cdot \alpha_i^j\right) = \varphi\big(\mu_{\alpha_i}(\alpha_i)\big) = \varphi(0) = 0,$$

d.h. φ bildet α_i auf eine Nullstelle von $\varphi(\mu_{\alpha_i})$ in M ab. Für α_i gibt es also höchstens

$$\deg\left(\varphi(\mu_{\alpha_i})\right) = \deg(\mu_{\alpha_i})$$

Möglichkeiten für $\varphi(\alpha_i)$.

Da φ durch die Bilder der α_i festgelegt ist, kann es höchstens

$$\deg(\mu_{\alpha_1}) \cdot \ldots \cdot \deg(\mu_{\alpha_n}) = |K_1 : K_0| \cdot |K_2 : K_1| \cdot \ldots \cdot |K_n : K_{n-1}| \overset{4.24}{=} |K_n : K_0| = |L : K|$$

Möglichkeiten für einen solchen Monomorphismus φ geben. □

Beispiel 10.9
Die Identität und die komplexe Konjugation sind zwei Automorphismen der Körpererweiterung $\mathbb{C}/\mathbb{R}$. Wegen $|\mathbb{C} : \mathbb{R}| = 2$ und Lemma 10.8 kann es auch keine weiteren geben (vgl. Beispiel 9.2).

C) Charakterisierung separabler Körpererweiterungen

Satz 10.10 (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 10.8 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 6.6 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 10.8 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 10.8 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 10.11
Für $p = 2$ ist die Körpererweiterung $\mathbb{F}_2(\sqrt{x})/\mathbb{F}_2(x)$ aus Beispiel 10.4 nicht separabel. Mithin gibt es nach Satz 10.10 keine Körpererweiterung $M/\mathbb{F}_2(\sqrt{x})$, so daß die Anzahl der Körpermonomorphismen

$$\varphi : \mathbb{F}_2(\sqrt{x}) \hookrightarrow M,$$

die auf $\mathbb{F}_2(x)$ eingeschränkt die Identität sind, genau $|\mathbb{F}_2(\sqrt{x}) : \mathbb{F}_2(x)| = 2$ beträgt. Wegen Lemma 10.8 muß die Anzahl also immer echt kleiner sein, so daß es stets nur einen einzigen solchen Körpermonomorphismus gibt. Das bedeutet insbesondere, daß die Identität der einzige $\mathbb{F}_2(x)$-Automorphismus von $\mathbb{F}_2(\sqrt{x})$ ist, d.h.

$$\mathrm{Gal}\left(\mathbb{F}_2(\sqrt{x})/\mathbb{F}_2(x)\right) = \{\mathrm{id}_{\mathbb{F}_2(\sqrt{x})}\}.$$

Beispiel 10.12 (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 10.13 (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 10.12 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. □

D) 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 13 C) aber noch einen zweiten Beweis des Satzes.

Satz 10.14 (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 Korollar 17.9 oder [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 im algebraischen Abschluß $\overline{K}$ von K haben, über dem die Polynome h, μ_{α_1} und μ_{α_2} in Linearfaktoren zerfallen. 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 10.15
Der Beweis des Satzes vom primitiven Element 10.14 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 einer Vorlesung zum symbolischen Rechnen erfahren.

Beispiel 10.16
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

$$\begin{aligned} a \notin & \left(\mathbb{Q} \cap \left\{ \frac{\alpha_j - \alpha_1}{\alpha_2 - \alpha_i} \;\middle|\; j = 2,3,4, i = 1,3,4 \right\} \right) \cup \{0\} \\ &= \mathbb{Q} \cap \left\{ \frac{2}{1-i}, \frac{2}{-1-i}, \frac{2}{-2i}, \frac{1-i}{1-i}, \frac{1-i}{-1-i}, \frac{1-i}{-2i}, \frac{1+i}{1-i}, \frac{1+i}{-1-i}, \frac{1+i}{-2i}, 0 \right\} \\ &= \{-1, 0, 1\}. \end{aligned}$$

Aufgaben

Aufgabe 10.17
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 10.18
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. $K(\alpha) = K(\alpha^p)$.

Aufgabe 10.19
Es sei K ein endlicher Körper der Charakteristik p mit $|K| = p^n$ Elementen und $f \in \mathbb{F}_p[t]$ sei ein irreduzibles Polynom vom Grad n.

a. Zeige, f zerfällt über K in Linearfaktoren.

b. Zeige, f ist ein Teiler von $t^{p^n} - t$ in $\mathbb{F}_p[t]$.

§ 11 Galoissche Körpererweiterungen

Wir haben in der Einleitung zu Abschnitt 10 angedeutet, daß das Vorhandensein von mehrfachen Nullstellen in irreduziblen Polynomen die Anzahl der K-Automorphismen in der Galoisgruppe des zugehörigen Zerfällungskörpers reduziert. Wir werden nun sehen, weshalb das so ist. Die K-Automorphismen des Zerfällungskörpers permutieren die Nullstellen des Polynoms. Fehlende Nullstellen reduzieren also die Anzahl möglicher Permutationen und damit der möglichen K-Automorphismen. Zerfällungskörper, bei denen die Anzahl an K-Automorphismen maximal ist, haben besonders interessante Eigenschaften. Dies führt zum Begriff der galoisschen Körpererweiterung.

A) K-Automorphismen als Permutationen der Nullstellen

Proposition 11.1 (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*
$$\mathrm{Gal}\,(L/K) \hookrightarrow \mathrm{Sym}(\{\alpha_1,\ldots,\alpha_n\}) : \tau \mapsto \tau_|$$
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*
$$\mathrm{Gal}\,(L/K) \longrightarrow Z_L(\mu_\alpha) = \{\alpha' \in L \mid \mu_\alpha(\alpha') = 0\} : \tau \mapsto \tau(\alpha)$$
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

$$\sigma(Z_L(f)) \subseteq Z_L(f).$$

Da die Menge Z endlich ist und σ injektiv ist, muß σ eingeschränkt auf Z dann eine Bijektion sein.

c. Nach Teil b. ist $\tau_|$ eine Permutation der Nullstellenmenge $Z_L(f) = \{\alpha_1, \ldots, \alpha_n\}$, also ein Element von $\mathrm{Sym}(\{\alpha_1, \ldots, \alpha_n\})$. Da τ 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 6.7, gibt es zu jeder Nullstelle α' von μ_α in L auch genau einen K-Automorphismus τ von $L = K(\alpha) = K(\alpha')$ mit $\tau(\alpha) = \alpha'$. Dies liefert die Surjektivität und die Injektivität der Abbildung. Um dabei die Gleichheit

$$K(\alpha) = K(\alpha')$$

zu sehen, beachten wir, daß nach Voraussetzung α' ein Element von $L = K(\alpha)$ ist und damit $K(\alpha') \subseteq K(\alpha)$ gilt und daß $K(\alpha)$ und $K(\alpha')$ als Stammkörper von μ_α denselben Grad über K haben.

□

Beispiel 11.2

a. Das Polynom

$$\mu_{\sqrt[3]{2}} = t^3 - 2 = \left(t - \sqrt[3]{2}\right) \cdot \left(t - \sqrt[3]{2} \cdot \zeta\right) \cdot \left(t - \sqrt[3]{2} \cdot \zeta^2\right) \in \mathbb{Q}[t],$$

mit $\zeta = e^{\frac{2\pi i}{3}}$, hat im Körper $\mathbb{Q}\left(\sqrt[3]{2}\right)$ nur die Nullstelle $\sqrt[3]{2}$. Aus Proposition 11.1 folgt dann, daß die Identität der einzige $\mathbb{Q}$-Automorphismus von $\mathbb{Q}\left(\sqrt[3]{2}\right)$ ist. Damit gilt dann

$$\left| \mathrm{Gal}\left(\mathbb{Q}\left(\sqrt[3]{2}\right)/\mathbb{Q}\right) \right| = 1 < 3 = \left|\mathbb{Q}\left(\sqrt[3]{2}\right) : \mathbb{Q}\right|.$$

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.

$$|\,\mathrm{Gal}\,(\mathbb{C}/\mathbb{R})\,| = 2 = |\mathbb{C} : \mathbb{R}|.$$

c. Das Polynom

$$f = (t^2 - 2) \cdot (t^2 - 7) \in \mathbb{Q}[t]$$

hat den Zerfällungskörper

$$L = \mathrm{ZFK}_{\mathbb{Q}}(f) = \mathbb{Q}\left(\sqrt{2}, -\sqrt{2}, \sqrt{7}, -\sqrt{7}\right) = \mathbb{Q}\left(\sqrt{2}, \sqrt{7}\right).$$

Wegen Proposition 11.1 muß ein $\mathbb{Q}$-Automorphismus von L die Nullstellen des irreduziblen Polynoms t^2-2 permutieren und die des irreduziblen Polynoms t^2-7. Beschreiben wir die $\mathbb{Q}$-Automorphismen von L als Permutationen der Menge

$$Z_L(f) = \left\{\sqrt{2}, -\sqrt{2}, \sqrt{7}, -\sqrt{7}\right\},$$

so kommen die folgenden vier Permutationen in Frage:

σ	$\sigma(\sqrt{2})$	$\sigma(-\sqrt{2})$	$\sigma(\sqrt{7})$	$\sigma(-\sqrt{7})$
id_L	$\sqrt{2}$	$-\sqrt{2}$	$\sqrt{7}$	$-\sqrt{7}$
σ_1	$-\sqrt{2}$	$\sqrt{2}$	$\sqrt{7}$	$-\sqrt{7}$
σ_2	$\sqrt{2}$	$-\sqrt{2}$	$-\sqrt{7}$	$\sqrt{7}$
$\sigma_1 \circ \sigma_2$	$-\sqrt{2}$	$\sqrt{2}$	$-\sqrt{7}$	$\sqrt{7}$

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:

$$\mathbb{Q} \leq \mathbb{Q}(\sqrt{2}) \leq \mathbb{Q}(\sqrt{2})(\sqrt{7}).$$

Wenden wir den Fortsetzungssatz 6.6 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 $\sqrt{7}$ festhält. Wir haben damit σ_1 als $\mathbb{Q}$-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

$$\mathrm{Gal}\left(\mathbb{Q}(\sqrt{2},\sqrt{7})/\mathbb{Q}\right) \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \cong \mathbb{K}_4 \leq \mathbb{S}_4$$

isomorph zur Kleinschen Vierergruppe, einer Untergruppe der $\mathbb{S}_4$ ist. Insbesondere gilt

$$\left|\mathrm{Gal}\left(\mathbb{Q}(\sqrt{2},\sqrt{7})/\mathbb{Q}\right)\right| = 4 = \left|\mathbb{Q}(\sqrt{2},\sqrt{7}) : \mathbb{Q}\right|.$$

Satz 11.3 zeigt, daß der Zusammenhang zwischen der Ordnung der Galoisgruppe und dem Grad der Körpererweiterung nicht zufällig ist.

Satz 11.3 (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 10.8 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) Charakterisierung galoisscher Körpererweiterungen

Körpererweiterungen, bei denen in Satz 11.3 die Gleichheit der beiden Zahlen gilt, haben besonders gute Eigenschaften und erhalten deshalb in der folgenden Definition einen eigenen Namen.

Definition 11.4 (Galoissche Körpererweiterungen)
Eine endliche Körpererweiterung L/K heißt *galoissch*, wenn $|\operatorname{Gal}(L/K)| = |L : K|$.

Beispiel 11.5
Aus Beispiel 11.2 folgt, daß die Körpererweiterungen $\mathbb{C}/\mathbb{R}$ und $\mathbb{Q}(\sqrt{2}, \sqrt{7})/\mathbb{Q}$ galoissch sind und daß $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ nicht galoissch ist.

Satz 11.6 (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 10.8 mit $M = L$ an, so sehen wir, daß es genau $|L : K|$ solche Monomorphismen gibt. Aus Satz 10.10 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 10.8 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 9.3 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 10.10 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 11.1 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. $\varphi \in \mathrm{Gal}\,(L/K)$ ist ein K-Automorphismus von L. Damit gilt dann

$$|\,\mathrm{Gal}\,(L/K)\,| = |L : K|$$

und L/K ist galoissch. □

Wir geben hier noch einen zweiten Beweis des Satzes 9.3, der den Satz vom primitiven Element verwendet.

Alternativer Beweis von 11.6: Wenn L/K separabel ist, dann gibt es nach dem Satz vom primitiven Element 10.14 ein notwendigerweise über K separables Element $\alpha \in L$ mit $L = K(\alpha)$.

a. $\Longrightarrow$ c.: Ist L/K galoissch, so ist $|\,\mathrm{Gal}\,(L/K)\,| = |L : K|$, so daß es mindestens $|L : K|$ Monomorphismen $\varphi : L \hookrightarrow L$ mit $\varphi_{|K} = \mathrm{id}_K$ gibt. Wenden wir Lemma 10.8 mit $M = L$ an, so sehen wir, daß es genau $|L : K|$ solche Monomorphismen gibt. Aus Satz 10.10 folgt dann, daß L/K separabel ist, und somit ist $L = K(\alpha)$ für ein separables $\alpha \in L$.

Nach Proposition 11.1 ist dann

$$\deg(\mu_\alpha) = |\,\mathrm{Gal}\,(K(\alpha)/K)\,| \overset{11.1}{=} |Z_L(\mu_\alpha)| \leq \deg(\mu_\alpha),$$

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 10.10 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 9.3 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 11.1

$$|\,\mathrm{Gal}\,(K(\alpha)/K)\,| \overset{11.1}{=} |Z_L(\mu_\alpha)| = \deg(\mu_\alpha) = |K(\alpha) : K|,$$

so daß $L = K(\alpha)$ galoissch über K ist. □

Korollar 11.7
Ist L/K *galoissch und* N *ein Zwischenkörper von* L/K*, so ist* L/N *galoissch.*

Beweis: Ist L/K galoissch, so ist $L = ZFK_K(f) = K(\alpha_1, \ldots, \alpha_n)$ nach Satz 11.6 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

$$L = N(\alpha_1, \ldots, \alpha_n) = ZFK_N(f)$$

ist der Zerfällungskörper von f über N. Also ist L/N nach Satz 11.6 galoissch. □

C) Erste Beispiele galoisscher Körpererweiterungen

Beispiel 11.8 ($\mathbb{S}_3$ als Galoisgruppe)
Das irreduzible Polynom

$$f = t^3 - 2 \in \mathbb{Q}[t]$$

aus Beispiel 6.19 und Beispiel 11.2 hat den Zerfällungskörper

$$L = ZFK_{\mathbb{Q}}(f) = \mathbb{Q}\left(\sqrt[3]{2}, \sqrt[3]{2} \cdot \zeta, \sqrt[3]{2} \cdot \zeta^2\right) = \mathbb{Q}\left(\sqrt[3]{2}, \zeta\right),$$

mit $\zeta = e^{\frac{2\pi i}{3}}$. Aus Beispiel 6.19 kennen wir auch den Grad

$$|L : \mathbb{Q}| = 6$$

der Körpererweiterung $L/\mathbb{Q}$. 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 11.1 wissen wir, daß $\operatorname{Gal}(L/\mathbb{Q})$ isomorph zu einer Untergruppe der $\mathbb{S}_3$ ist, und da diese nur sechs Elemente enthält, folgt

$$\operatorname{Gal}(L/\mathbb{Q}) \cong \mathbb{S}_3.$$

Beispiel 11.9 (Eine Körpererweiterung vom Grad 8)
In Beispiel 6.14 haben wir den Zerfällungskörper

$$ZFK_{\mathbb{Q}}(f) = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_2, \alpha_4) = \mathbb{Q}(\alpha_1, \alpha_2),$$

des Polynoms

$$f = t^4 - 10t^2 + 18 \in \mathbb{Q}[t]$$

mit den Nullstellen

$$\alpha_1 = \sqrt{5 + \sqrt{7}}, \quad \alpha_2 = \sqrt{5 - \sqrt{7}}, \quad \alpha_3 = -\sqrt{5 + \sqrt{7}} \quad \text{und} \quad \alpha_4 = -\sqrt{5 - \sqrt{7}}$$

kennengelernt.

Wir wollen nun zunächst den Grad $|ZFK_{\mathbb{Q}}(f) : \mathbb{Q}|$ bestimmen.

Wenden wir das Eisensteinkriterium mit $p = 2$ an, so erhalten wir, daß f irreduzibel ist und $\mathbb{Q}(\alpha_1)/\mathbb{Q}$ hat den Grad

$$|\mathbb{Q}(\alpha_1) : \mathbb{Q}| = \deg(f) = 4.$$

Dabei gilt

$$\sqrt{7} = \alpha_1^2 - 5 \in \mathbb{Q}(\alpha_1).$$

Nehmen wir an, es würde

$$\alpha_2 \in \mathbb{Q}(\alpha_1)$$

gelten. Dann würde

$$\sqrt{2} = \frac{\sqrt{5+\sqrt{7}} \cdot \sqrt{5-\sqrt{7}}}{3} = \frac{\alpha_1 \cdot \alpha_2}{3} \in \mathbb{Q}(\alpha_1)$$

folgen. Dann würde aber

$$\mathbb{Q}(\sqrt{2}, \sqrt{7}) \subseteq \mathbb{Q}(\alpha_1)$$

gelten, und da beide Körper Grad 4 über $\mathbb{Q}$ haben, würde schon

$$\mathbb{Q}(\alpha_1) = \mathbb{Q}(\sqrt{2}, \sqrt{7})$$

folgen. Aus Beispiel 11.2 würden wir dann auch die Galoisgruppe $\mathrm{Gal}\,(\mathbb{Q}(\alpha_1)/\mathbb{Q})$ kennen und hätten ein

$$\sigma \in \mathrm{Gal}\,(\mathbb{Q}(\alpha_1)/\mathbb{Q})$$

mit $\sigma^2 = \mathrm{id}_{\mathbb{Q}(\alpha_1)}$ sowie

$$\sigma(\sqrt{2}) = -\sqrt{2}$$

und

$$\sigma(\sqrt{7}) = -\sqrt{7}.$$

Damit erhielten wir dann

$$\sigma(\alpha_1^2) = \sigma(5+\sqrt{7}) = 5 - \sqrt{7}$$

und somit

$$\sigma(\alpha_1) = \pm\alpha_2.$$

Zugleich müßte aber

$$\sigma(\alpha_1) \cdot \sigma(\alpha_2) = \sigma(\alpha_1 \cdot \alpha_2) = \sigma(3 \cdot \sqrt{2}) = -3 \cdot \sqrt{2} = -\alpha_1 \cdot \alpha_2$$

gelten, woraus wir

$$\sigma(\alpha_2) = \mp\alpha_1$$

schließen müßten. Da die Bilder von α_1 und α_2 unterschiedliche Vorzeichen hätten, würden wir dann

$$\sigma^2(\alpha_1) = \pm\sigma(\alpha_2) = -\alpha_1$$

erhalten, im Widerspruch zu $\sigma^2 = \mathrm{id}_{\mathbb{Q}(\alpha_1)}$. Also muß

$$\alpha_2 \notin \mathbb{Q}(\alpha_1)$$

gelten.

Aber wegen $\sqrt{7} \in \mathbb{Q}(\alpha_1)$ ist dann

$$t^2 - \alpha_2^2 = t^2 - (5 - \sqrt{7}) \in \mathbb{Q}(\alpha_1)[t]$$

das Minimalpolynom von α_2 über $\mathbb{Q}(\alpha_1)$, und wir haben

$$|\mathbb{Q}(\alpha_1, \alpha_2) : \mathbb{Q}(\alpha_1)| = 2.$$

Aus der Gradformel folgt dann

$$|\operatorname{ZFK}_{\mathbb{Q}}(f) : \mathbb{Q}| = |\mathbb{Q}(\alpha_1, \alpha_2) : \mathbb{Q}| = |\mathbb{Q}(\alpha_1) : \mathbb{Q}| \cdot |\mathbb{Q}(\alpha_1, \alpha_2) : \mathbb{Q}(\alpha_1)| = 4 \cdot 2 = 8.$$

Als Zerfällungskörper eines separablen Polynoms ist die Körpererweiterung auch galoissch, und wir erhalten

$$|\operatorname{Gal}(\operatorname{ZFK}_{\mathbb{Q}}(f)/\mathbb{Q})| = |\operatorname{Gal}(\mathbb{Q}(\alpha_1, \alpha_2)/\mathbb{Q})| = |\operatorname{ZFK}_{\mathbb{Q}}(f) : \mathbb{Q}| = 8.$$

Wir werden später zeigen, daß die Galoisgruppe eine Diëdergruppe der Ordnung 8 ist.

Aufgaben

Aufgabe 11.10
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 $L = K(\alpha)$.

Aufgabe 11.11
Betrachte den Zerfällungskörper $L = \operatorname{ZFK}_{\mathbb{Q}}(f)$ des Polynoms $f = t^4 - 8t^2 + 9 \in \mathbb{Q}[t]$ und zeige

$$\operatorname{Gal}(L/\mathbb{Q}) \cong \{\mathrm{id}, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}.$$

Aufgabe 11.12 (Galoisgruppe eines Polynoms vom Grad 3)
Es sei K ein Körper und $L = \operatorname{ZFK}_K(f)$ der Zerfällungskörper eines irreduziblen, separablen Polynoms $f = t^3 + a_2 \cdot t^2 + a_1 \cdot t + a_0 \in K[t]$ vom Grad drei.

a. Zeige, ist $f = (t - \alpha_1) \cdot (t - \alpha_2) \cdot (t - \alpha_3)$ eine Faktorisierung von f über dem Zerfällungskörper L, dann gilt

$$\begin{aligned}\Delta(f) :=& a_1^2 \cdot a_2^2 - 4 \cdot a_1^3 - 4 \cdot a_0 \cdot a_2^3 + 18 \cdot a_0 \cdot a_1 \cdot a_2 - 27 \cdot a_0^2 \\ \stackrel{!}{=}& (\alpha_1 - \alpha_2)^2 \cdot (\alpha_1 - \alpha_3)^2 \cdot (\alpha_2 - \alpha_3)^2 \in K.\end{aligned}$$

   Man nennt $\Delta(f)$ die *Diskriminante* von f.

b. Zeige, ist $\Delta(f) \in \{q^2 \mid q \in K\}$ eine Quadratzahl in K, so gilt $\operatorname{Gal}(L/K) \cong \mathbb{A}_3$.

c. Zeige, ist $\Delta(f) \notin \{q^2 \mid q \in K\}$ keine Quadratzahl in K, so gilt $\operatorname{Gal}(L/K) \cong \mathbb{S}_3$.

d. Bestimme die Galoisgruppe von $f = t^3 - 3t + 1 \in \mathbb{Q}[t]$.

Aufgabe 11.13 ($\mathbb{S}_n$ als Galoisgruppe)
Sei $L = \mathbb{Q}(x_1, \ldots, x_n)$ der Körper der rationalen Funktionen über $\mathbb{Q}$ in den Veränderlichen $x_1, \ldots, x_n$ und sei

$$f_n = (t - x_1) \cdot \ldots \cdot (t - x_n) = t^n + s_{n-1}^n \cdot t^{n-1} + \ldots + s_1^n \cdot t + s_0^n.$$

Man nennt $s_0^n, \ldots, s_{n-1}^n$ die *elementarsymmetrischen Polynome* in den Veränderlichen $x_1, \ldots, x_n$.

a. Berechne die Polynome s_0^3, s_1^3, s_2^3 explizit.

b. Zeige, $s_i^n \in \mathbb{Z}[x_1, \ldots, x_n]$ für alle $i = 0, \ldots, n-1$.

c. Zeige, L ist galoissch über $K = \mathbb{Q}(s_0^n, \ldots, s_{n-1}^n)$ mit Galoisgruppe

$$\mathrm{Gal}\,(L/K) \cong \mathbb{S}_n.$$

§ 12 Hauptsatz der Galoistheorie

Ziel dieses Abschnittes ist es, den Zusammenhang zwischen der Struktur einer endlichen Körpererweiterung L/K und der 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 12.9).

A) Fixkörper und die Galoiskorrespondenz

Definition und Bemerkung 12.1
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 im Falle $\beta \neq 0$ auch

$$\sigma(\alpha \cdot \beta^{-1}) = \sigma(\alpha) \cdot \sigma(\beta^{-1}) = \alpha \cdot \beta^{-1}$$

für alle $\sigma \in U$ gilt.

b. Ist N ein Zwischenkörper der Körpererweiterung L/K, 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 (siehe auch Proposition 9.9),

$$\mathrm{Gal}(L/N) \leq \mathrm{Gal}(L/K)\,.$$

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 12.2

Betrachten wir noch einmal Beispiel 11.2 c., d.h.

$$L = \mathrm{ZFK}_{\mathbb{Q}}\left((t^2-2)\cdot(t^2-7)\right) = \mathbb{Q}\left(\sqrt{2},\sqrt{7}\right)$$

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	$\sigma(\sqrt{2})$	$\sigma(\sqrt{-2})$	$\sigma(\sqrt{7})$	$\sigma(\sqrt{-7})$
id_L	$\sqrt{2}$	$-\sqrt{2}$	$\sqrt{7}$	$-\sqrt{7}$
σ_1	$-\sqrt{2}$	$\sqrt{2}$	$\sqrt{7}$	$-\sqrt{7}$
σ_2	$\sqrt{2}$	$-\sqrt{2}$	$-\sqrt{7}$	$\sqrt{7}$
$\sigma_1\circ\sigma_2$	$-\sqrt{2}$	$\sqrt{2}$	$-\sqrt{7}$	$\sqrt{7}$

Die Untergruppe

$$U = \langle\sigma_1\rangle = \{\mathrm{id}_L, \sigma_1\} \leq \mathrm{Gal}\,(L/\mathbb{Q})$$

der Galoisgruppe hat den Fixkörper

$$\mathrm{Fix}\,(L,U) = \mathbb{Q}\left(\sqrt{7}\right).$$

Umgekehrt ist auch

$$\mathrm{Gal}\left(L/\mathbb{Q}\left(\sqrt{7}\right)\right) = U$$

die Galoisgruppe der Körpererweiterung $L/\mathbb{Q}\left(\sqrt{7}\right)$, da die Identität und σ_1 die einzigen Elemente von $\mathrm{Gal}\,(L/\mathbb{Q})$ sind, die den Körper $\mathbb{Q}\left(\sqrt{7}\right)$ invariant lassen.

Hier gilt also

$$\mathrm{Gal}\,(L/\mathrm{Fix}\,(L,U)) = U$$

und

$$\mathrm{Fix}\left(L, \mathrm{Gal}\left(L/\mathbb{Q}\left(\sqrt{7}\right)\right)\right) = \mathbb{Q}\left(\sqrt{7}\right),$$

d.h. die Abbildungen Gal und Fix aus Definition 12.1 kehren ihre Wirkungen auf U und $\mathbb{Q}\left(\sqrt{7}\right)$ 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 12.1 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 12.3

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* L^L *aller Abbildungen von* 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 also $n \geq 2$ 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

$$\lambda_1 \cdot \sigma_1 + \ldots + \lambda_n \cdot \sigma_n = 0 \tag{25}$$

die Nullabbildung ist. Wegen $\sigma_1 \neq \sigma_n$ finden wir ein $\beta \in L$ mit

$$\sigma_1(\beta) \neq \sigma_n(\beta). \tag{26}$$

Setzen wir in Gleichung (25) den Wert $\alpha \cdot \beta$ ein, so erhalten wir

$$\begin{aligned} 0 =& \lambda_1 \cdot \sigma_1(\alpha \cdot \beta) + \ldots + \lambda_n \cdot \sigma_n(\alpha \cdot \beta) \\ =& \lambda_1 \cdot \sigma_1(\alpha) \cdot \sigma_1(\beta) + \ldots + \lambda_n \cdot \sigma_n(\alpha) \cdot \sigma_n(\beta). \end{aligned} \tag{27}$$

für alle $\alpha \in L$. Setzen wir nun in Gleichung (25) α ein, multiplizieren die Gleichung mit $\sigma_n(\beta)$ und subtrahieren das Ergebnis von Gleichung (27), 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 (26) dann

$$\lambda_1 = 0.$$

Setzen wir dies in Gleichung (25) 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 12.2 haben wir ein Beispiel für die Aussage des folgenden Satzes von Artin gesehen.

Satz 12.4 (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

$$\mathrm{Gal}(L/\mathrm{Fix}(L, U)) = U.$$

Insbesondere ist die Körpererweiterung $L/\mathrm{Fix}(L, U)$ *also galoissch.*

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 12.3.

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, d.h.

$$\mathrm{Ker}(A) \neq \{(0, \ldots, 0)^t\}. \tag{28}$$

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

$$U = \{\sigma_1, \ldots, \sigma_n\} = \{\sigma_i \circ \sigma_1, \ldots, \sigma_i \circ \sigma_n\}, \tag{29}$$

so erhalten wir für $\alpha \in L$ die Gleichung

$$\sigma_i\big(\varphi(\alpha)\big) = \sigma_i \left(\sum_{j=1}^{n} \sigma_j(\alpha) \right) = \sum_{j=1}^{n} \sigma_i \circ \sigma_j(\alpha) \overset{(29)}{=} \sum_{k=1}^{n} \sigma_k(\alpha) = \varphi(\alpha)$$

und damit

$$\varphi(\alpha) \in \mathrm{Fix}\,(L, U)\,.$$

Sei nun

$$(\lambda_1, \ldots, \lambda_m)^t \in \mathrm{Ker}(A)$$

beliebig. Da das Produkt aus den Zeilen der Matrix A mit dem Vektor $(\lambda_1, \ldots, \lambda_m)^t$ null ergibt, erhalten wir

$$0 = \sum_{i=1}^{n} \sigma_i(0) \overset{(28)}{=} \sum_{i=1}^{n} \sigma_i \left(\sum_{j=1}^{m} \lambda_j \cdot \sigma_i^{-1}(\alpha_j) \right) = \sum_{i=1}^{n} \sum_{j=1}^{m} \sigma_i(\lambda_j) \cdot \alpha_j$$
$$= \sum_{j=1}^{m} \sum_{i=1}^{n} \sigma_i(\lambda_j) \cdot \alpha_j = \sum_{j=1}^{m} \varphi(\lambda_j) \cdot \alpha_j.$$

Aus der linearen Unabhängigkeit der Familie B über $\mathrm{Fix}\,(L, U)$ folgt dann

$$\varphi(\lambda_1) = \ldots = \varphi(\lambda_n) = 0.$$

Wir können nun einen solchen Vektor $(\lambda_1, \ldots, \lambda_m)^t \neq (0, \ldots, 0)^t$ wählen, und dann muß $\lambda_k \neq 0$ für ein $k \in \{1, \ldots, m\}$ gelten. Für $\alpha \in L$ ist dann auch der Vektor

$$\frac{\alpha}{\lambda_k} \cdot (\lambda_1, \ldots, \lambda_m)^t \in \mathrm{Ker}(A)$$

im Kern von A und seine k-te Komponente hat den Wert α. Damit erhalten wir dann aber

$$0 = \varphi(\alpha) = \sigma_1(\alpha) + \ldots + \sigma_n(\alpha)$$

für alle $\alpha \in L$. Dies steht aber im Widerspruch zu Lemma 12.3.

Damit haben wir die erste Gleichung gezeigt,

$$|L : \mathrm{Fix}\,(L, U)\,| = n = |U|. \tag{30}$$

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 11.3

$$|U| \leq |\,\mathrm{Gal}\,(L/\mathrm{Fix}\,(L, U))\,| \overset{11.3}{\leq} |L : \mathrm{Fix}\,(L, U)\,| \overset{(30)}{=} |U|,$$

woraus die fehlende Gleichheit folgt,

$$U = \mathrm{Gal}\,(L/\mathrm{Fix}\,(L, U))\,.$$

□

Beispiel 12.5

In Beispiel 12.2 haben wir den Körper

$$L = \mathbb{Q}(\sqrt{2}, \sqrt{7})$$

betrachtet sowie eine Untergruppe

$$U = \langle \sigma_1 \rangle = \{\mathrm{id}_L, \sigma_1\} = \mathrm{Gal}\left(L/\mathbb{Q}(\sqrt{7})\right) \leq \mathrm{Gal}\,(L/\mathbb{Q}) = \mathrm{Aut}(L),$$

wobei die letzte Gleichheit aus Aufgabe 4.33 folgt. Zudem haben wir dort die aus dem Satz von Artin folgende Gleichheit

$$\mathrm{Gal}\,(L/\mathrm{Fix}\,(L,U)) = U$$

nachgeprüft.

Korollar 12.6
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 12.4, da $\mathrm{Gal}\,(L/K)$ nach Satz 11.3 eine endliche Untergruppe von $\mathrm{Aut}(L)$ ist. □

C) Kiterium für galoissche Körpererweiterungen

Korollar 12.7 (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. Da $\mathrm{Gal}\,(L/K)$ nach Satz 11.3 eine endliche Gruppe ist, ist auch U endlich. Aus dem Satz von Artin folgt dann, daß $L/K = L/\mathrm{Fix}\,(L,U)$ galoissch ist sowie die Gleichung

$$\mathrm{Gal}\,(L/K) = \mathrm{Gal}\,(L/\mathrm{Fix}\,(L,U)) = U.$$

□

Schauen wir uns diese Folgerungen aus dem Satz von Artin nun in zwei konkreten Beispielen an.

Beispiel 12.8

a. Wir wollen zunächst daran erinnern, daß jeder Automorphismus eines Körpers automatisch den Primkörper invariant läßt (siehe Aufgabe 4.33). Deshalb gilt für den Körper $L = \mathbb{Q}(\alpha)$ mit $\alpha = \sqrt[3]{2}$ auch

$$\mathrm{Aut}(L) = \mathrm{Gal}(L/\mathbb{Q}) = \{\mathrm{id}_L\},$$

wobei wir die letzte Gleichung in Beispiel 11.2 gezeigt haben. Damit besitzt $\mathrm{Aut}(L)$ nur die triviale Untergruppe $\mathrm{Aut}(L)$ und es gilt

$$\mathrm{Fix}\,(L, \mathrm{Aut}(L)) = L \neq \mathbb{Q},$$

woraus wir mittels Korollar 12.7 noch mal die bereits bekannte Tatsache ableiten können, daß $L/\mathbb{Q}$ nicht galoissch ist, weil $\mathbb{Q}$ nicht Fixkörper einer Untergruppe von $\mathrm{Aut}(L)$ sein kann.

b. In Beispiel 12.2 haben wir nachgeprüft, daß für den Körper $L = \mathbb{Q}(\sqrt{2}, \sqrt{7})$ und den Teilkörper $Q(\sqrt{7})$ die Gleichheit

$$\mathrm{Fix}\left(L, \mathrm{Gal}\left(L/\mathbb{Q}(\sqrt{7})\right)\right) = \mathbb{Q}(\sqrt{7})$$

gilt. Aus Korollar 12.7 folgt dann, daß die Körpererweiterung $L/\mathbb{Q}(\sqrt{7})$ galoissch ist. Das hätten wir aber auch daraus schließen können, daß sie als Körpererweiterung vom Grad 2 normal und wegen $\mathrm{char}(L) = 0$ auch separabel ist.

D) Der Hauptsatz der Galoistheorie

Im Satz von Artin haben wir gesehen, daß Gal für endliche Körpererweiterungen eine Linksinverse von Fix ist. Wir werden nun zeigen, daß Gal für endliche galoissche Körpererweiterungen auch eine Rechtsinverse von Fix ist.

Satz 12.9 (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.

Beweis des Hauptsatzes der Galoistheorie 12.9:

a. Aus Korollar 12.6 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

$$\mathrm{Fix}(L, \mathrm{Gal}(L/N)) = N \tag{31}$$

zu zeigen, wobei N ein beliebiger Zwischenkörper von L/K ist. Nach Korollar 11.7 ist L/N galoissch und aus Korollar 12.7 folgt dann (31).

b. Sei N ein Zwischenkörper von L/K. Nach Korollar 11.7 ist L/N galoissch und wir erhalten die erste Gleichung

$$|L : N| = |\mathrm{Gal}(L/N)|.$$

Für die zweite Gleichung verwenden wir die Gradformel

$$|L : K| = |L : N| \cdot |N : K| \tag{32}$$

sowie den Satz von Lagrange

$$|\mathrm{Gal}(L/K)| = |\mathrm{Gal}(L/N)| \cdot |\mathrm{Gal}(L/K) : \mathrm{Gal}(L/N)| \tag{33}$$

Da L/K und L/N galoissch sind, folgt daraus

$$|N : K| \overset{(32)}{=} \frac{|L : K|}{|L : N|} = \frac{|\mathrm{Gal}(L/K)|}{|\mathrm{Gal}(L/N)|} \overset{(33)}{=} |\mathrm{Gal}(L/K) : \mathrm{Gal}(L/N)|.$$

c. Setzen wir zunächst voraus, daß N/K galoissch ist. Dann ist N/K insbesondere endlich und normal nach Proposition 9.9 ist dann $\mathrm{Gal}(L/N) \trianglelefteq \mathrm{Gal}(L/K)$ ein Normalteiler.
Sei nun $\mathrm{Gal}(L/N) \trianglelefteq \mathrm{Gal}(L/K)$ vorausgesetzt, dann folgt für $\sigma \in \mathrm{Gal}(L/K)$ mit Lemma 9.8

$$\mathrm{Gal}(L/N) = \sigma \circ \mathrm{Gal}(L/N) \circ \sigma^{-1} = \mathrm{Gal}(L/\sigma(N)).$$

Aus Teil a. leiten wir dann

$$N \overset{\text{a.}}{=} \mathrm{Fix}(L, \mathrm{Gal}(L/N)) = \mathrm{Fix}(L, \mathrm{Gal}(L/\sigma(N))) \overset{\text{a.}}{=} \sigma(N)$$

ab. Das heißt, jeder K-Automorphismus von L induziert einen K-Automorphismus von N.
Damit ist die Einschränkung

$$\varepsilon : \mathrm{Gal}(L/K) \longrightarrow \mathrm{Gal}(N/K) : \sigma \mapsto \sigma_{|N}$$

wohldefiniert, und wir wollen nun zeigen, daß sie ein Gruppenepimorphismus mit

$$\mathrm{Ker}(\varepsilon) = \mathrm{Gal}\,(L/N)$$

ist. Wenn uns dies gelingt, so erhalten wir

$$\mathrm{Gal}\,(L/K)\,/\,\mathrm{Gal}\,(L/N) \cong \mathrm{Gal}\,(N/K)$$

und damit

$$|\,\mathrm{Gal}\,(N/K)\,| = \frac{|\,\mathrm{Gal}\,(L/K)\,|}{|\,\mathrm{Gal}\,(L/N)\,|} = |\,\mathrm{Gal}\,(L/K) : \mathrm{Gal}\,(L/N)\,| \overset{\text{b.}}{=} |N : K|,$$

so daß N/K galoissch ist.
Es ist klar, daß ε ein Gruppenhomomorphismus mit dem angegebenen Kern

$$\mathrm{Ker}(\varepsilon) = \{\sigma \in \mathrm{Gal}\,(L/K) \mid \sigma_{|N} = \mathrm{id}_N\} = \mathrm{Gal}\,(L/N)$$

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

$$\begin{aligned}\mathrm{Fix}\,(N, \mathrm{Im}(\varepsilon)) &= \left\{\alpha \in N \;\middle|\; \sigma(\alpha) = \alpha \;\forall\; \sigma \in \mathrm{Gal}\,(L/K)\right\} \\ &= N \cap \mathrm{Fix}\,(L, \mathrm{Gal}\,(L/K)) \overset{12.7}{=} N \cap K = K.\end{aligned}$$

Aufgrund des Satzes von Artin 12.4 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.

□

E) Erste Beispiele für den Hauptsatz der Galoistheorie

Beispiel 12.10 ($\mathbb{S}_3$ als Galoisgruppe)
In Beispiel 11.8 haben wir die Galoisgruppe des Zerfällungskörpers

$$L = \mathrm{ZFK}_{\mathbb{Q}}(f) = \mathbb{Q}\big(\sqrt[3]{2}, \zeta\big),$$

mit $\zeta = e^{\frac{2\pi i}{3}}$, 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

$$\alpha_1 = \sqrt[3]{2}, \alpha_2 = \sqrt[3]{2} \cdot \zeta, \alpha_3 = \sqrt[3]{2} \cdot \zeta^2 \in \mathbb{C}$$

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 8). Bei

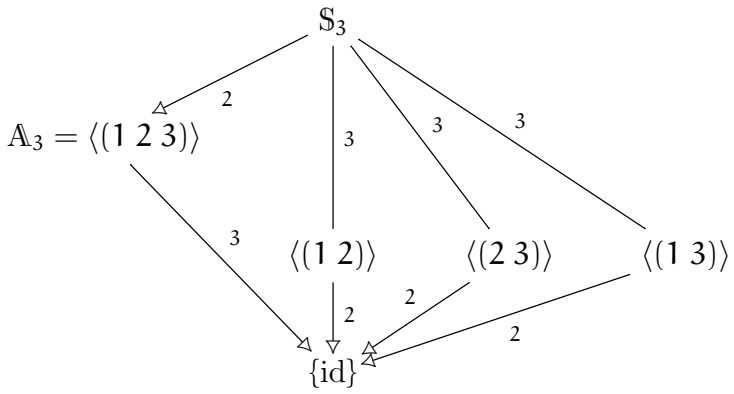

Abbildung 8. Der Untergruppenverband von $\mathbb{S}_3$

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 9). Aufgrund des Hauptsatzes der Galoistheorie entspricht diesem der duale Zwi-

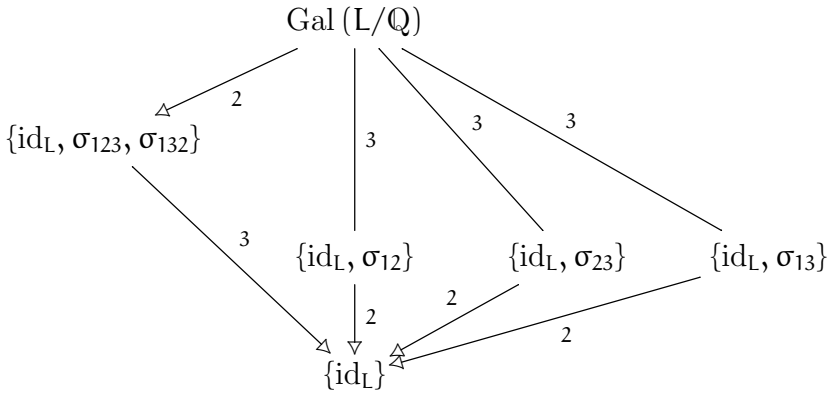

Abbildung 9. Der Untergruppenverband von $\mathrm{Gal}\left(\mathrm{ZFK}_{\mathbb{Q}}(t^3-2)/\mathbb{Q}\right)$

schenkörperverband der Körpererweiterung $L/\mathbb{Q}$ (siehe Abbildung 10). Bei der gra-

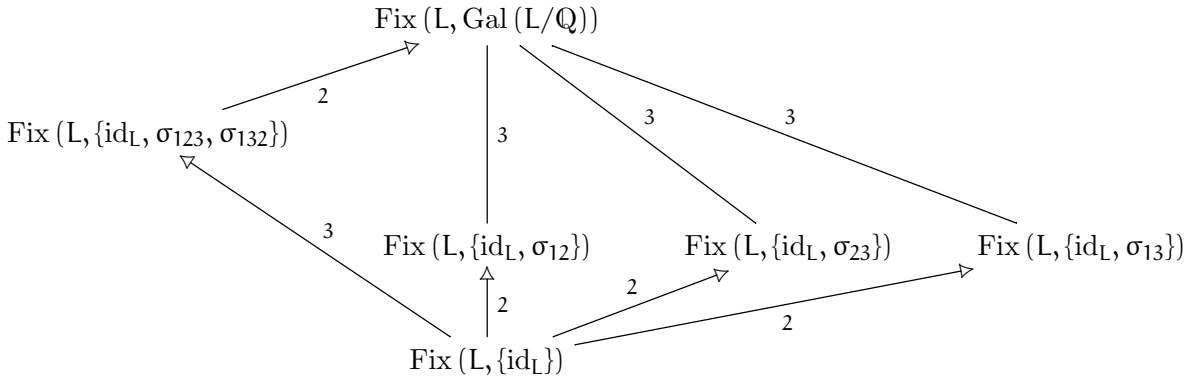

ABBILDUNG 10. Der Zwischenkörperverband von $\mathrm{ZFK}_{\mathbb{Q}}(t^3-2)/\mathbb{Q}$

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 11. Dabei ist die Gleichung

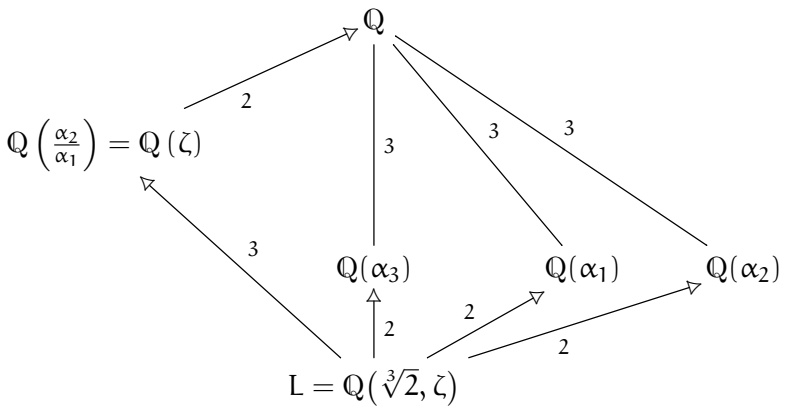

ABBILDUNG 11. Der Zwischenkörperverband von $\mathrm{ZFK}_{\mathbb{Q}}(t^3-2)/\mathbb{Q}$

$$\mathrm{Fix}\,(L,\{\mathrm{id}_L,\sigma_{12}\}) = \mathbb{Q}(\alpha_3)$$

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

$$\operatorname{Fix}(L, \{\mathrm{id}_L, \sigma_{123}, \sigma_{132}\}) = \mathbb{Q}\left(\frac{\alpha_2}{\alpha_1}\right) = \mathbb{Q}(\zeta)$$

zu sehen, betrachten wir

$$\frac{\alpha_2}{\alpha_1} = \zeta$$

und berechnen

$$\sigma_{123}\left(\frac{\alpha_2}{\alpha_1}\right) = \frac{\alpha_3}{\alpha_2} = \zeta = \frac{\alpha_2}{\alpha_1}.$$

Also läßt σ_{123} die Zahl invariant und damit auch $\sigma_{123}^{-1} = \sigma_{132}$, so daß ζ und damit $\mathbb{Q}(\zeta)$ im Fixkörper enthalten sind. Wegen

$$|\operatorname{Fix}(L, \{\mathrm{id}_L, \sigma_{123}, \sigma_{132}\}) : \mathbb{Q}| = 2 = \deg(t^2 + t + 1) = |\mathbb{Q}(\zeta) : \mathbb{Q}|$$

folgt dann wieder die Gleichheit. Hierbei haben wir ausgenutzt, daß $g = t^2 + t + 1$ nach Beispiel 3.10 irreduzibel über $\mathbb{Q}$ und damit das Minimalpolynom von ζ über $\mathbb{Q}$ ist.

Beispiel 12.11
In Beispiel 9.7 haben wir $L = \mathbb{Q}(\sqrt[4]{2}, i)$ als Körpererweiterung von $\mathbb{Q}$ sowie den Zwischenkörper $M = \mathbb{Q}(\sqrt[4]{2})$ betrachtet. Weil die Körpererweiterung $M/\mathbb{Q}$ nicht normal ist, ist $\operatorname{Gal}(L/M)$ kein Normalteiler von $\operatorname{Gal}(L/\mathbb{Q})$, und mithin ist letztere Gruppe nicht abelsch. Also muß $\operatorname{Gal}(L/\mathbb{Q})$ eine nicht-abelsche Gruppe der Ordnung

$$|\operatorname{Gal}(L/\mathbb{Q})| = |L : \mathbb{Q}| = 8$$

sein. Mit etwas Kenntnis in Gruppentheorie kann man zeigen, daß es bis auf Isomorphie davon genau zwei solche Gruppen gibt, die Diëdergruppe der Ordnung 8 und die Quaterionengruppe der Ordnung 8. Um welche von beiden es sich handelt, wollen wir an dieser Stelle offen lassen.

Aufgaben

Aufgabe 12.12
Sei $K = \mathbb{Q}(\sqrt{2}, \sqrt{7})$. Bestimme den Zwischenkörperverband von $K/\mathbb{Q}$ unter Verwendung der Ergebnisse aus Beispiel 11.2.

Aufgabe 12.13 ($\mathbb{D}_8$ als Galoisgruppe)
Es seien $L = \mathrm{ZFK}_{\mathbb{Q}}(t^4 - 2)$ der Zerfällungskörper von $t^4 - 2$ über $\mathbb{Q}$ und $\mathbb{D}_8 := \langle \pi, \tau \rangle \leq \mathbb{S}_4$ mit $\pi = (1\,2\,3\,4)$ und $\tau = (2\,4)$.

a. Zeige, $\pi^4 = \tau^2 = \mathrm{id}$ und $\tau \circ \pi = \pi^3 \circ \tau$ und leite daraus ab, daß

$$\mathbb{D}_8 = \{\pi^m \circ \tau^n \mid 0 \leq m \leq 3, 0 \leq n \leq 1\}$$

Ordnung 8 hat.

b. Bestimme den Untergruppenverband von $\mathbb{D}_8$.

c. Zeige, die Galoisgruppe $\mathrm{Gal}(L/\mathbb{Q})$ enthält zwei $\mathbb{Q}$-Automorphismen σ und ω mit

$$\langle \sigma, \omega \rangle \cong \mathbb{D}_8.$$

d. Bestimme den Zwischenkörperverband von $L/\mathbb{Q}$.

Hinweis: in Teil c. nutze man, daß ein $\mathbb{Q}$-Automorphismus von $L/\mathbb{Q}$ die Nullstellen von $t^4 - 2$ und von $t^2 + 1$ permutiert und dadurch festgelegt ist.

Aufgabe 12.14 ($\mathbb{D}_8$ 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 12.15
Zeige, es gibt einen Isomorphismus von $\mathbb{Q}[\sqrt{2}, \sqrt{7}]$ nach $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$ und schließe daraus, daß die Galoisgruppen der beiden Körper über $\mathbb{Q}$ isomorph sind.

Aufgabe 12.16 (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 Beispiel 11.2 (unter Berücksichtigung von Aufgabe 12.15), 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 $L/\mathbb{Q}$.

Die Galoisgruppe von $L/\mathbb{Q}$ wird auch Quaterionengruppe genannt (siehe auch Aufgabe 14.25).

Aufgabe 12.17

a. Zeige, eine Gruppe der Ordnung 4 ist isomorph zu $\mathbb{Z}/4\mathbb{Z}$ oder zu $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$.

b. Zeige, die Galoisgruppe der Körpererweiterung $\mathbb{Q}(\alpha)/\mathbb{Q}$ mit $\alpha = \sqrt{4+\sqrt{7}}$ aus Aufgabe 9.11 ist isomorph zu $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

c. Bestimme den Zwischenkörperverband von $\mathbb{Q}(\alpha)/\mathbb{Q}$ in Teil b.

§ 13 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 13.1 (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 7.10 ist $\mathrm{GF}(p^n)$ der Zerfällungskörper des Polynoms

$$f = t^{p^n} - t \in \mathbb{F}_p[t]$$

und dieses ist nach Beispiel 10.12 separabel über $\mathbb{F}_p$. Also ist $\mathrm{GF}(p^n)/\mathbb{F}_p$ nach Satz 11.6 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 7.5 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 12.9, 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] oder Korollar 17.5). Deren Fixkörper hat dann die Ordnung p^m.

□

B) Der algebraische Abschluß von $\mathbb{F}_p$

Bemerkung 13.2 (Endliche Körper)
Ist p eine Primzahl und sind m und n zwei beliebige positive ganze Zahlen, dann können wir wegen Korollar 13.1 $GF(p^m)$ und $GF(p^n)$ als Zwischenkörper von $GF(p^{kgv(m,n)})$ auffassen.

Korollar 13.3 (Der algebraische Abschluß von $\mathbb{F}_p$)
Ist p ein Primzahl, so ist der algebraische Abschluß von $\mathbb{F}_p$ der Körper

$$\overline{\mathbb{F}_p} = \bigcup_{n\in\mathbb{Z}_{>0}} GF(p^n).$$

Beweis: Wir müssen zunächst zeigen, daß die Vereinigung

$$L := \bigcup_{n\in\mathbb{Z}_{>0}} GF(p^n)$$

der endlichen Körper $GF(p^n)$ wieder ein Körper ist. Seien dazu $\alpha, \beta, \gamma \in L$, so gibt es positive ganze Zahlen l, m, n, so daß $\alpha \in GF(p^l)$, $\beta \in GF(p^m)$ und $\beta \in GF(p^n)$ gilt. Nach Bemerkung 13.2 gilt dann aber schon

$$\alpha, \beta, \gamma \in GF\left(p^{kgv(l,m,n)}\right).$$

Wir können die Körperaxiome für die drei Elemente also in diesem Körper nachprüfen und sie sind erfüllt. Somit erhalten wir, daß L ein Körper ist.

Zudem ist L algebraisch über $\mathbb{F}_p$, da jedes Element von L schon in einem $GF(p^n)$ liegt und dieser algebraisch über $\mathbb{F}_p$ ist.

Um zu sehen, daß L auch algebraisch abgeschlossen ist, betrachten wir ein beliebiges nicht-konstantes Polynom $f \in L[t]$. Da f nur endlich viele Koeffizienten hat, gibt es ein $n > 0$ mit

$$f \in GF(p^n)[t].$$

Betrachten wir nun den Zerfällungskörper von f über $GF(p^n)$, so ist

$$m := |\,ZFK_{GF(p^n)}(f) : GF(p^n)| < \infty,$$

und mithin ist $ZFK_{GF(p^n)}(f)$ ein endlicher Körper mit p^{mn} Elementen, also

$$ZFK_{GF(p^n)}(f) = GF(p^{mn}) \subset L.$$

Insbesondere hat f also in L eine Nullstelle und somit ist L algebraisch abgeschlossen.

□

C) Der Satz vom primitiven Element

Wir wollen hier einen zweiten Beweis des Satzes vom primitiven Element geben, der den Hauptsatz der Galoistheorie verwendet.

Lemma 13.4 (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] und Korollar 17.9), 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 4.22 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 13.5
Bemerkung 10.15 gilt hier analog. Zudem beachte man, daß auch die Umkehrung von Lemma 13.4 gilt: eine endliche, einfache Körpererweiterung hat nur endlich viele Zwischenkörper (siehe Aufgabe 4.41).

Satz 13.6 (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 11.6 ist $ZFK_K(f)/K$ galoissch. Aus dem Hauptsatz der Galoistheorie 12.9 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 13.4 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/K endlich und nach Satz 10.10 auch separabel über K. □

Korollar 13.7 (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 10.14, weil L/K dann nach Korollar 10.13 oder nach Korollar 10.5 separabel ist. □

Beispiel 13.8
Die Körpererweiterung $\mathbb{Q}(\sqrt{2}, \sqrt{7})/\mathbb{Q}$ aus Beispiel 11.2 hat Grad 4 und ist nach Korollar 13.7 einfach. Wir wollen zeigen, daß

$$\alpha = \sqrt{2} + \sqrt{7}$$

ein erzeugendes Element ist. Dazu beachten wir, daß

$$\beta := \sqrt{2} - \sqrt{7} = -\frac{5}{\sqrt{2} + \sqrt{7}} = -\frac{5}{\alpha} \in \mathbb{Q}(\alpha)$$

gilt. Damit gilt dann aber auch

$$\sqrt{2} = \frac{\alpha + \beta}{2}, \sqrt{7} = \frac{\alpha - \beta}{2} \in \mathbb{Q}(\alpha),$$

woraus die Behauptung folgt.

Alternativ hätte man hier mit Aufgabe 11.10 argumentieren können. Aus Beispiel 11.2 kennen wir die Elemente der Galoisgruppe der Körpererweiterung, und keiner der Automorphismen, außer der Identität, läßt α fest. Also muß α ein primitives Element der Körpererweiterung sein.

D) Kreisteilungspolynome

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 von Bemerkung 13.10 verweisen wir auf die Vorlesungen Elementare Zahlentheorie (siehe [Mar08b, S. 57]) und Algebraische Strukturen (siehe [Mar08a, Kor. 4.61,4.62]) sowie auf das folgende Lemma.

Lemma 13.9 (Ordnung von Potenzen)
Sei $(G,\cdot)$ *eine Gruppe und* $g \in G$ *ein Element von Ordnung* $o(g) = n < \infty$*, dann gilt für* $d \in \mathbb{Z}_{>0}$

$$o(g^d) = \frac{n}{\operatorname{ggt}(d,n)}.$$

Beweis: Die Ordnung von g^d ist die Zahl

$$\begin{aligned} m &:= \min\{k > 0 \mid e = (g^d)^k = g^{d\cdot k}\} \\ &= \min\{k > 0 \mid n \text{ teilt } d\cdot k\} \\ &= \min\{k > 0 \mid \operatorname{kgv}(d,n) \text{ teilt } d\cdot k\}, \end{aligned}$$

wobei für die letzte Gleichheit zu beachten ist, daß die Zahl $d\cdot k$ bereits durch $\operatorname{kgv}(d,n)$ geteilt wird, wenn sie nur durch n geteilt wird. Aus der Gleichheit

$$\operatorname{ggt}(d,n)\cdot\operatorname{kgv}(d,n) = d\cdot n$$

folgt dann aber unmittelbar, daß

$$k = \frac{n}{\operatorname{ggt}(d,n)}$$

eine solche Zahl ist und daß es keine kleinere geben kann. □

Bemerkung 13.10 (n-te Einheitswurzeln)
Ist $n \in \mathbb{Z}_{>0}$ und $\zeta_n := e^{\frac{2\pi i}{n}}$, so heißen die Elemente in

$$E_n := \left\{z \in \mathbb{C} \;\middle|\; z^n = 1\right\} = \left\{z \in \mathbb{C}^* \;\middle|\; o(z) \text{ teilt } n\right\} = \left\{\zeta_n^d \;\middle|\; d = 1,\dots,n\right\}$$

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:

$$\zeta_n^d \text{ primitiv} \quad\Longleftrightarrow\quad o(\zeta_n^d) = n \quad\overset{13.9}{\Longleftrightarrow}\quad \operatorname{ggt}(d,n) = 1. \tag{34}$$

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 13.11 (Das n-te Kreisteilungspolynom über $\mathbb{Q}$)
Das Polynom

$$\phi_n:=\prod_{\zeta\in E_n \text{ primitiv}}(t-\zeta)=\prod_{\substack{1\le d\le n\\ ggt(d,n)=1}}\left(t-\zeta_n^d\right)=\prod_{\substack{\zeta\in\mathbb{C}^*\\ o(\zeta)=n}}(t-\zeta)\in\mathbb{C}[t]$$

heißt das n-*te Kreisteilungspolynom* über $\mathbb{Q}$.

Beispiel 13.12

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 $\frac{n}{ggt(n,k)}$ 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 13.15 zeigt.

Im Beweis des Hauptergebnisses des nächsten Unterabschnitts werden wir die folgende einfache Eigenschaft des Polynomrings $\mathbb{Z}[t]$ mehrfach verwenden.

Lemma 13.13
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. □

Damit sind wir in der Lage, zu zeigen, daß die Kreisteilungspolynome ganzzahlige Koeffizienten haben und in $\mathbb{Z}[t]$ sogar irreduzibel sind.

Proposition 13.14
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: 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 13.17 folgt aber auch

$$t^n - 1 = \Phi_n \cdot g$$

und aus Lemma 13.13 folgt dann

$$\Phi_n \in \mathbb{Z}[t].$$

Wegen Satz 3.3 reicht es nun, zu zeigen, daß Φ_n irreduzibel in $\mathbb{Z}[t]$ ist, die Irreduzibilität in $\mathbb{Q}[t]$ folgt dann. Da $\mathbb{Z}[t]$ nach dem Lemma von Gauß 1.18 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

$$\Phi_n = \mu_\zeta \cdot \mu_{\zeta^p} \cdot g. \tag{35}$$

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 13.13 gilt dabei sogar

$$h \in \mathbb{Z}[t].$$

Mittels Reduktion mod p (siehe Definition 3.5)

$$\rho_p : \mathbb{Z}[t] \longrightarrow \mathbb{F}_p[t]$$

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 7.3). 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 (35)

$$d^2 \,\Big|\, \overline{\mu_\zeta} \cdot \overline{\mu_{\zeta^p}} \cdot \overline{g} = \overline{\phi_n} \mid t^n - \overline{1}$$

in $\mathbb{F}_p[t]$. Also hat $t^n - \overline{1}$ eine mehrfache Nullstelle α in seinem Zerfällungskörper über $\mathbb{F}_p$ und diese ist wegen Lemma 7.8 auch eine Nullstelle von

$$\left(t^n - \overline{1}\right)' = n \cdot t^{n-1} \neq 0,$$

wobei die letzte Ungleichung aus $p \not| n$ folgt. Dann müßte aber $\alpha = \overline{0}$ gelten im Widerspruch dazu, daß 0 keine Nullstelle von $t^n - \overline{1}$ ist. Also gilt $\mu_\zeta = \mu_{\zeta^p}$ und die Aussage des Lemmas ist bewiesen. □

E) Kreisteilungskörper

Wir wollen nun die Zerfällungskörper der Kreisteilungspolynome untersuchen.

Satz 13.15 (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: Aus Proposition 13.14 wissen wir schon, daß ϕ_n in $\mathbb{Z}[t]$ liegt und dort irreduzibel ist. Der Grad von ϕ_n ist nach Definition gleich der Anzahl der primitiven n-ten Einheitswurzeln in E_n und dies ist nach (34) in Bemerkung 13.10 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]).

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.

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 $1 \le d \le n$ mit $\mathrm{ggt}(d, n) = 1$, da σ die Nullstellen des Polynoms $\phi_n \in \mathbb{Q}[t]$ permutiert. 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 der Definitions- und der Zielbereich von τ aber gleichmächtig sind, folgt daraus auch die Surjektivität von τ, so daß τ ein Gruppenisomorphismus ist. □

Bemerkung 13.16 (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 13.15 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 13.17
Ist $p \in \mathbb{P}$ eine Primzahl, so haben wir in Beispiel 3.10 gesehen, daß das Polynom

$$\frac{t^p - 1}{t - 1} = t^{p-1} + t^{p-2} + \ldots + t + 1 \in \mathbb{Z}[t] \tag{36}$$

in $\mathbb{Z}[t]$ irreduzibel ist. Damit muß

$$\phi_p = t^{p-1} + t^{p-2} + \ldots + t + 1 \tag{37}$$

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 13.15 können wir die Gleichung (37) und die Irreduzibilität des Polynoms (36) aber auch anders sehen. Wir wissen ja, daß ϕ_p ein Teiler des Polynoms (36) ist und daß

$$\deg(\phi_p) = |\mathbb{Z}_p^*| = p - 1$$

gilt. Damit erhalten wir die Gleichung (37) und die Irreduzibilität des Polynoms.

Der Satz von Lambert–Euler–Gauß (siehe [**Mar08b**, Satz 6.7] oder Korollar 17.9) 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] oder Korollar 17.5), 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 12 (siehe auch Beispiel 17.4). Um die Untergruppen von $\mathbb{Z}_{13}^*$ explizit anzugeben, haben wir die Primitivwurzel $\overline{7}$ von $\mathbb{Z}_{13}^*$ verwendet (siehe [**Mar08b**, § 7]).

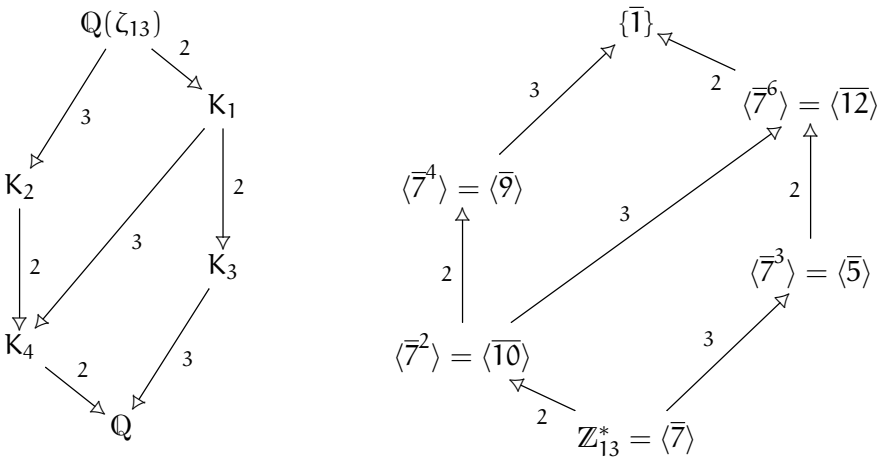

ABBILDUNG 12. Das Zwischenkörperdiagramm von $\mathbb{Q}(\zeta_{13})/\mathbb{Q}$

Bemerkung 13.18 (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 13.15 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.

F) Konstruierbarkeit des regelmäßigen n-Ecks

Bemerkung 13.19 (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

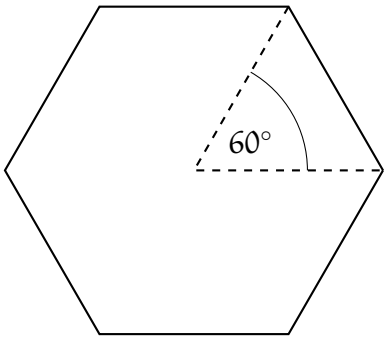

ABBILDUNG 13. Ein regelmäßiges 6-Eck

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

$$\zeta_n = e^{\frac{2\pi i}{n}}$$

zu konstruieren. Aus Satz 13.15 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 5.9 wissen wir, wenn ζ_n konstruierbar ist, dann muß diese Zahl eine 2-Potenz sein. Aber für welche n ist das der Fall und reicht das auch immer aus?

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. In der Tat gilt auch, 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.

Wir wollen nun zunächst zeigen, daß $|\mathbb{Z}_n^*| = 2^k$ für ein geeignetes k auch hinreichend ist, damit die Zahl ζ_n konstruierbar ist.

Proposition 13.20 (Galoissche 2-Radikalerweiterungen)
Sei L/K *eine galoissche Körpererweiterung vom Grad* $|L : K| = 2^n$ *mit abelscher Galoisgruppe und* $\mathrm{char}(K) \neq 2$*, dann ist* L/K *eine 2-Radikalerweiterung.*

Beweis: Wir zeigen die Aussage mit Induktion nach n, wobei die Aussage für $n = 1$ aus Aufgabe 5.19 folgt. Sei also $n \geq 1$.

Da L/K galoissch ist, gilt

$$|\operatorname{Gal}(L/K)| = |L : K| = 2^n$$

und wir können ein $\mathrm{id}_L \neq \sigma \in \operatorname{Gal}(L/K)$ wählen. Wegen des Satzes von Lagrange wissen wir

$$o(\sigma) = 2^k$$

für ein $1 \leq k \leq n$. Die Untergruppe

$$U = \langle \sigma^{2^{k-1}} \rangle$$

von $\operatorname{Gal}(L/K)$ hat dann die Ordnung 2. Da $\operatorname{Gal}(L/K)$ abelsch ist, ist U zudem ein Normalteiler von $\operatorname{Gal}(L/K)$. Aus dem Hauptsatz der Galoistheorie wissen wir dann, daß

$$N := \operatorname{Fix}(L, U)$$

galoissch über K ist mit Galoisgruppe

$$\mathrm{Gal}\,(N/K) \cong \mathrm{Gal}\,(L/K) \,/\, \mathrm{Gal}\,(L/N)\,.$$

Insbesondere ist $\mathrm{Gal}\,(N/K)$ als Faktorgruppe einer abelschen Gruppe also abelsch. Wegen

$$|N : K| = |\,\mathrm{Gal}\,(L/K) : U| = 2^{n-1}$$

können wir dann Induktion auf N/K anwenden und erhalten, daß N/K eine 2-Radikalerweiterung ist. L/N hat aber den Grad $|U| = 2$, so daß L aus N wegen des Falls $n = 1$ ebenfalls durch die Adjunktion einer Quadratwurzel entsteht, und wir erhalten insgesamt, daß L/K eine 2-Radikalerweiterung ist. □

Korollar 13.21 (Konstruierbarkeit von ζ_n)
Für $n \geq 3$ sind die folgenden Aussagen gleichwertig:

a. $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ *ist eine 2-Radikalerweiterung.*

b. $|\mathbb{Z}_n^*| = |\mathbb{Q}(\zeta_n) : \mathbb{Q}$ *ist eine Zweierpotenz.*

c. ζ_n *ist aus* $M = \{0, 1\}$ *mit Zirkel und Lineal konstruierbar.*

Beweis: Wenn $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ eine 2-Radikalerweiterung ist, dann ist der Grad der Körpererweiterung auch eine Zweierpotenz (siehe Korollar 5.9). Ist der Grad eine Zweierpotenz, dann ist nach Proposition 13.20 die Köpererweiterung $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ auch eine 2-Radikalerweiterung, weil sie galoissch mit abelscher Galoisgruppe ist (siehe Satz 13.15). Die Äquivalenz von a. und c. folgt aus Korollar 5.9. □

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 13.22 (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

$$|\mathbb{Z}_{q_i^{n_i}}^*| = \varphi\big(q_i^{n_i}\big) = q_i^{n_i-1} \cdot (q_i - 1)$$

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 13.23
Die Zahl

$$n = 17 = 2^{2^2} + 1$$

ist eine Fermatsche Primzahl und somit ist das reguläre 17-Eck wegen Satz 13.22 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.

Aufgaben

Aufgabe 13.24
Zeige, daß das Polynom $f = t^4 + t^3 + t^2 + t + 1$ irreduzibel in $\mathbb{F}_2[t]$ ist und bestimme ein primitives Element α für die Körpererweiterung $\mathbb{F}_2[t]/\langle f\rangle$ über $\mathbb{F}_2$.

Aufgabe 13.25
Zeige, $\alpha = \sqrt[3]{2} + \zeta$ mit $\zeta = e^{\frac{2\pi i}{3}}$ ist ein primitives Element des Zerfällungskörpers $\mathrm{ZFK}_{\mathbb{Q}}(t^3 - 2)$ über $\mathbb{Q}$.

Hinweis: man kann Aufgabe 11.10 verwenden.

Aufgabe 13.26
Die Eulersche φ-Funktion

$$\varphi : \mathbb{Z}_{>0} \longrightarrow \mathbb{Z} : n \mapsto |\mathbb{Z}_n^*|$$

ordnet einer positiven ganzen Zahl n die Anzahl der Einheiten im Ring $\mathbb{Z}_n$ zu.

a. Zeige, wenn $n, m \in \mathbb{Z}_{>0}$ teilerfremd sind, dann gilt $\varphi(n \cdot m) = \varphi(n) \cdot \varphi(m)$.

b. Zeige, ist $p \in \mathbb{P}$ eine Primzahl, dann gilt $\varphi(p^k) = p^{k-1} \cdot (p - 1)$.

c. Zeige, mit der Notation aus Satz 1.4 gilt

$$\varphi(n) = \prod_{\substack{p \in \mathbb{P} \\ p|n}} \left(p^{n_p(n)} - p^{n_p(n)-1}\right) = n \cdot \prod_{\substack{p \in \mathbb{P} \\ p|n}} \left(1 - \frac{1}{p}\right).$$

Hinweis: in Teil (a) darf man den Chinesischen Restsatz anwenden.

Aufgabe 13.27

Bestimme eine Körpererweiterung $L/\mathbb{Q}$ mit $\mathrm{Gal}(L/\mathbb{Q}) \cong \mathbb{Z}_4 \times \mathbb{Z}_2$.

Aufgabe 13.28

Bestimme eine Körpererweiterung L/K mit $\mathrm{Gal}(L/K) \cong \mathbb{Z}_8$.

Aufgabe 13.29

Bestimme den Zwischenkörperverband von $\mathbb{Q}(\zeta_{25})/\mathbb{Q}$ mit $\zeta_{25} = e^{\frac{2\pi i}{25}}$ wie in Beispiel 13.17, d.h. es müssen keine Erzeuger für die Zwischenkörper ausgerechnet werden.

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 16.13) und der Zusammenhang der Auflösbarkeit von Gleichungen durch Radikale und der Auflösbarkeit der zugehörigen Galoisgruppe (siehe Satz 19.6).

§ 14 Gruppenoperationen

Gruppen, die auf Mengen operieren, tauchen in vielen Bereichen der Mathematik in ganz natürlicher Weise auf. Ein Beispiel dafür wäre die Galoisgruppe des Zerfällungskörpers eines Polynoms, die die Nullstellen des Polynoms permutiert (siehe auch Beispiel 14.3 und Aufgabe 14.17). Wir wollen in diesem Abschnitt den Begriff einführen und erste interessante Eigenschaften herleiten.

A) Gruppenoperationen und der Satz von Cayley

Operationen von Gruppen auf Mengen induzieren in natürlicher Weise eine Äquivalenzrelation auf der Menge 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 14.1 (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 14.2 (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 14.3

a. Die Gruppe $(\mathbb{R}, +)$ operiert auf der Menge $\Omega = \mathbb{C}$ durch

$$\mathbb{R} \times \mathbb{C} \longrightarrow \mathbb{C} : (t, \omega) \mapsto t * \omega = e^{2\cdot\pi\cdot i\cdot t} \cdot \omega,$$

wie man aus den Potenzgesetzen ableitet. Die Bahn $\omega^{\mathbb{R}}$ von $0 \neq \omega \in \mathbb{C}$ ist der Kreis vom Radius $|\omega|$ um den Ursprung, und der Stabilisator $\mathbb{R}_\omega$ von ω ist die Untergruppe $\mathbb{Z}$ von $\mathbb{R}$.

b. 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 14.2 ist dabei die Identität.

c. 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

$$\pi^k * (g_1, \ldots, g_n) := (g_{k+1}, g_{k+2}, \ldots, g_n, g_1, g_2, \ldots, g_k).$$

Dazu beachten wir zunächst, daß für $(g_1, \ldots, g_n) \in \Omega$

$$g_2 \cdot g_3 \cdot \ldots \cdot g_n \cdot g_1 = g_1^{-1} \cdot g_1 \cdot g_2 \cdot \ldots \cdot g_n \cdot g_1 = g_1^{-1} \cdot e_H \cdot g_1 = e_H$$

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

$$\begin{aligned}
\pi^k * \left(\pi^l * (g_1, \ldots, g_n)\right) &= \pi^k * (g_{l+1}, \ldots, g_n, g_1, \ldots, g_l) \\
&= (g_{m+1}, \ldots, g_n, g_1 \ldots, g_m) \\
&= \pi^m * (g_1, \ldots, g_n) \\
&= \pi^{k+l} * (g_1, \ldots, g_n) \\
&= (\pi^k \circ \pi^l) * (g_1, \ldots, g_n)
\end{aligned}$$

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 $G_\omega = G$.

d. Ist L/K eine Körpererweiterung und ist $f \in K[t]$ ein Polynom, dann operiert die Galoisgruppe $\mathrm{Gal}(L/K)$ von L/K nach Proposition 11.1 auf der Menge $Z_L(f)$ der Nullstellen von f in L durch

$$\mathrm{Gal}(L/K) \times Z_L(f) \longrightarrow Z_L(f) : (\sigma, \alpha) \mapsto \sigma(\alpha).$$

Ist $L = \mathrm{ZFK}_K(f)$ und ist f irreduzibel in $K[t]$, dann ist die Operation wegen Aufgabe 6.24 transitiv.

Satz 14.4 (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 14.2 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 $\mathbb{S}_{|G|}$. □

B) Die Bahnbilanzgleichung

Wir wollen die Bahnblianzgleichung herleiten, die zeigt, daß die Mächtigkeit der Menge Ω in natürlicher als Summe von Indizes von Untergruppen von G geschrieben werden kann.

Lemma 14.5 (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 14.6 (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 14.7 (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 eine Bijektion und die behauptete Gleichheit der Mächtigkeiten

$$|G : G_\omega| = |\omega^G|$$

folgt. Wegen Lemma 14.5 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 14.8 (Bahnbilanzgleichung)
Betrachten wir noch einmal $G = \mathbb{S}_n$ und $\Omega = \{1, \ldots, n\}$ aus Beispiel 14.3. 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

$$|G : G_\omega| = \frac{|\mathbb{S}_n|}{|\mathbb{S}_{n-1}|} = \frac{n!}{(n-1)!} = n = |\Omega| = |\omega^G|.$$

C) Das Zentrum einer Gruppe

Definition 14.9 (Zentrum)
Ist G eine Gruppe, so nennen wir

$$Z(G) := \{g \in G \mid g \cdot h = h \cdot g \ \ \forall\, h \in G\}$$

das *Zentrum* von G. Das Zentrum besteht also genau aus den Elementen, die mit allen anderen kommutieren.

Proposition 14.10 (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.

c. G *ist genau dann abelsch, wenn* $Z(G) = G$.

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.

Die Aussage in Teil c. ist offensichtlich korrekt, da das Zentrum genau aus den Elementen besteht, die mit allen anderen vertauschen. □

Beispiel 14.11 (Zentrum)

a. Das Zentrum von $\mathbb{S}_3$ ist $Z(\mathbb{S}_3) = \{\mathrm{id}\}$.

b. 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.

D) Die Klassengleichung

Korollar 14.12 (Klassengleichung)
Ist G *eine endliche Gruppe, so 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 14.7 auf die Konjugation als Operation von G auf G an, so erhalten wir für $g \in G$ unter Berücksichtigung von Beispiel 14.6

$$|g^G| = |G : G_g| = |G : C_G(g)|.$$

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 ein 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 14.7 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 14.13 (Klassengleichung)
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

$$\rho^{\mathbb{D}_8} = \{\rho, \rho^\pi\} = \{(2\,3), (1\,4)\}.$$

Damit ist π, σ, ρ das in der Klassengleichung erwähnte Repräsentantensystem.

E) Das Zentrum einer p-Gruppe

Definition 14.14 (p-Gruppe)
Für eine Primzahl p ist eine Gruppe G ein p-*Gruppe*, wenn $|G|$ eine p-Potenz ist.

Korollar 14.15 (p-Gruppen haben ein nicht-triviales Zentrum.)
Ist G *eine nicht-triviale* p*-Gruppe, so ist* $|Z(G)| > 1$.

Beweis: Wir beachten, daß ein Element $g \in G$ 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 14.12

$$p \,\Big|\, |G : C_G(g_i)|.$$

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. □

Beispiel 14.16
Die Diëdergruppe $\mathbb{D}_8$ ist eine 2-Gruppe mit Zentrum $|Z(\mathbb{D}_8)| = 2$, siehe Beispiel 14.11.

Aufgaben

Aufgabe 14.17 (Irreduzibilitätskriterium mittels Transitivität)
Sei L/K eine Körpererweiterung und sei $f \in K[t]$ ein Polynom ohne mehrfache Nullstelle, das in L zerfällt. Zeige, wenn die Galoisgruppe $\mathrm{Gal}\,(L/K)$ (gemäß Beispiel 14.3) transitiv auf der Nullstellenmenge $Z_L(f)$ operiert, dann ist f irreduzibel in $K[t]$.

Aufgabe 14.18 (Artin-Schreier-Polynome)
Sei K ein Körper der Charkteristik $p > 0$ mit Primkörper $P \cong \mathbb{F}_p$, $f = t^p - t - a \in K[t]$ und $\alpha \in \overline{K}$ eine Nullstelle von f. Zeige die folgenden Aussagen:

a. $Z_{\overline{K}}(f) = \{\alpha + b \mid b \in P\}$ ist die Menge der Nullstellen von f in $\overline{K}$.

b. $K(\alpha) = \mathrm{ZFK}_K(f)$ ist galoissch über K.

c. Genau dann ist f irreduzibel, wenn $\alpha \notin K$.

d. Ist $\alpha \notin K$, dann ist $\mathrm{Gal}(K(\alpha)/K) \cong \mathbb{Z}_p$ zyklisch der Ordnung p.

Aufgabe 14.19 (Ordnung eines Produktes)
Seien $(G, \cdot)$ eine Gruppe und $g, h \in G$ Elemente endlicher Ordnung mit $g \cdot h = h \cdot g$.

a. Wenn $\langle g \rangle \cap \langle h \rangle = \{e_G\}$ gilt, dann gilt $o(g \cdot h) = \mathrm{kgv}(o(g), o(h))$.

b. Wenn $\mathrm{ggt}(o(g), o(h)) = 1$ gilt, dann gilt $o(g \cdot h) = o(g) \cdot o(h)$.

Aufgabe 14.20
Sei G eine einfache Gruppe und $U \leq G$ mit $1 < n = |G : U| < \infty$. Zeige, G ist isomorph zu einer Untergruppe der $\mathbb{S}_n$.

Aufgabe 14.21
Die endliche Gruppe G operiere transitiv auf der endlichen Menge Ω mit $|\Omega| \geq 2$. Zeige, es gibt ein $g \in G$ ohne Fixpunkt, d.h. $g * \omega \neq \omega$ für alle $\omega \in \Omega$ gilt.

Aufgabe 14.22 (Zykeltyp einer Permutation)
Ist eine Permutation

$$\pi = \sigma_1 \circ \ldots \circ \sigma_m \in \mathbb{S}_n$$

als Produkt von paarweise disjunkten Zyklen σ_i der Länge k_i mit $k_1 \geq k_2 \geq \ldots \geq k_m$ gegeben, dann nennt man $(k_1, \ldots, k_m)$ den *Zykeltyp* der Permutation π.[1]

a. Zeige, ist $\pi \in \mathbb{S}_n$ ein k-Zykel und $\sigma \in \mathbb{S}_n$, dann ist $\pi^\sigma = \sigma \circ \pi \circ \sigma^{-1}$ ein k-Zykel.

b. Zeige, der Zykeltyp einer Permutation bleibt unter Konjugation erhalten.

c. Zeige, hat $\pi \in \mathbb{S}_n$ den Zykeltyp $(k_1, \ldots, k_m)$, dann gilt $o(\pi) = \mathrm{kgv}(k_1, \ldots, k_m)$.

Aufgabe 14.23 (Produktformel für Untergruppen)
Es seien $U, V \leq G$ Untergruppen der Gruppe $(G, \cdot)$.

a. Zeige, daß durch

$$(u, v) \sim (u', v') \iff u \cdot v = u' \cdot v'$$

eine Äquivalenzrelation auf der Menge $U \times V$ definiert wird.

b. Zeige, daß die Äquivalenzklasse von $(u, v) \in U \times V$ die Gestalt

$$\overline{(u, v)} = \left\{ (u \cdot y, y^{-1} \cdot v) \mid y \in U \cap V \right\}$$

besitzt und die Mächtigkeit $|U \cap V|$ hat.

c. Beweise, wenn U und V endlich sind, so genügt die Mächtigkeit der Menge

$$U \cdot V := \{u \cdot v \mid u \in U, v \in V\}$$

der Produktformel

$$|U \cdot V| = \frac{|U| \cdot |V|}{|U \cap V|}.$$

[1] Da die Zerlegung bis auf die Reihenfolge der Zykel eindeutig ist, ist der Zykeltyp eindeutig.

Aufgabe 14.24
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.

Aufgabe 14.25 (Quaterionengruppe)
Wir betrachten die Untergruppe $Q_8 = \langle I, J\rangle \leq Gl_2(\mathbb{C})$ der Gruppe der invertierbaren 2×2-Matrizen über $\mathbb{C}$, die von den beiden Matrizen

$$I = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \text{und} \quad J = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$$

erzeugt wird. Zeige die folgenden Aussagen:

a. $I^2 = J^2 = (I \circ J)^2 = -\mathbb{1}_2$ und $I \circ J = J^3 \circ I$.

b. Q_8 ist eine nicht-abelsche Gruppe der Ordnung $|Q_8| = 8$.

c. $Z(Q_8) = \{\mathbb{1}_2, -\mathbb{1}_2\}$.

d. Bestimme damit den Untergruppenverband von Q_8, und zeige dazu, daß Q_8 genau eine Untergruppe der Ordnung 2 und drei Untergruppen der Ordnung 4 enthält.

e. Alle Untergruppe der Q_8 sind Normalteiler.

f. Q_8 ist nicht isomorph zur Diëdergruppe $\mathbb{D}_8$.

Die Gruppe Q_8 wird auch *Quaterionengruppe* genannt (siehe auch Aufgabe 12.16).

Aufgabe 14.26 (Galoissche 2-Radikalerweiterungen)
Sei L/K eine galoissche Körpererweiterung vom Grad $|L : K| = 2^n$ für ein $n \geq 1$ und $\mathrm{char}(K) \neq 2$. Zeige, dann ist L eine 2-Radikalerweiterung von K.

§ 15 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 16.7 oder Korollar 18.4).

A) Der Satz von Cauchy

Wir wissen, daß die Ordnung eines Elementes stets ein Teiler der Gruppenordnung ist. Gibt es auch Teiler der Gruppenordnung, die definitiv als Ordnungen von Elementen auftauchen?

Satz 15.1 (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 14.3. 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 14.3 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

$$(g_{k+1}, \ldots, g_p, g_1, \ldots, g_k) = \pi^k * \omega = \omega = (g_1, \ldots, g_p)$$

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. □

Beispiel 15.2 (Der Satz von Cauchy)

a. Die symmetrische Gruppe $\mathbb{S}_3$ hat die Ordnung $6 = 2 \cdot 3$ und sie enthält Elemente der Ordnung 2, z.B. $(1\ 2)$, und der Ordnung 3, z.B. $(1\ 2\ 3)$. Sie enthält aber kein Element der Ordnung 6. Der Satz von Cauchy gilt also nicht für beliebige Teiler der Gruppenordnung.

b. Die Kleinsche Vierergruppe

$$\mathbb{K}_4 = \{\mathrm{id}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$$

hat die Ordnung $4 = 2^2$, enthält aber kein Element der Ordnung 2^2. Der Satz von Cauchy ist also nicht mal richtig für Primzahlpotenzen, die die Gruppenordnung teilen.

B) Der erste Sylowsatz

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. Er verallgemeinert damit den Satz von Cauchy.

Satz 15.3 (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 14.12 wissen wir

$$|G| = |Z(G)| + \sum_{j=1}^{k} |G : C_G(g_j)|$$

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_j geben, so daß p kein Teiler von $|G : C_G(g_j)|$ ist. Aus dem Satz von Lagrange wissen wir dann

$$p^i \Big| \frac{|G|}{|G : C_G(g_j)|} = |C_G(g_j)|.$$

Da g_j nicht im Zentrum von G liegt, ist

$$|C_G(g_j)| < |G|$$

und nach Induktionsvoraussetzung hat $C_G(g_j)$ 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 15.1 ein Element $g \in Z(G)$ der Ordnung p. Die Untergruppe

$$N = \langle g \rangle \leq G$$

ist nach Proposition 14.10 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 15.4

a. 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:

$$|\langle (1\ 2) \rangle| = 2, |\langle (1\ 2\ 3\ 4) \rangle| = 4, |\mathbb{D}_8| = 8, |\langle (1\ 2\ 3) \rangle| = 3.$$

b. Die alternierende Gruppe $\mathbb{A}_4$ hat Ordnung 12, besitzt aber keine Untergruppe der Ordnung 6. Im Ersten Sylowsatz ist es also wichtig, daß der Teiler eine Primzahlpotenz ist (siehe auch Korollar 16.8).
Um die Aussage zu zeigen, betrachten wir die alternierende Gruppe etwas genauer

$$\mathbb{A}_4 = \big\{(1), (a\ b)(c\ d), (a\ b\ c) \;\big|\; \{a,b,c,d\} = \{1,2,3,4\}\big\}.$$

Wir sehen, daß die $\mathbb{A}_4$ den Normalteiler

$$K = \{(1), (12)(34), (13)(24), (14)(23)\}$$

enthält.
Angenommen, $\mathbb{A}_4$ würde zudem eine Untergruppe V mit $|V| = 6$ enthalten. Die Produktformel für Untergruppen (siehe Aufgabe 14.23) impliziert dann

$$|V \cap K| = \frac{|V| \cdot |K|}{|V \cdot K|} \geq \frac{24}{12} = 2$$

und aus dem Satz von Lagrange folgt dann wegen $V \cap K \leq V$ und $V \cap K \leq K$ schon

$$|V \cap K| = 2.$$

Also enthält V ein Element der Form $(a\ b)(c\ d)$ sowie vier 3-Zyklen. Wir unterscheiden folgende Fälle:

- Sind $(a\ b\ c), (a\ c\ b) \in V$, dann erhalten wir den Widerspruch
$$(a\ c)(b\ d) = (a\ c\ b)(a\ b)(c\ d)(a\ b\ c) \in V.$$
- Sind $(a\ b\ d), (a\ d\ b) \in V$, dann erhalten wir den Widerspruch
$$(a\ d)(b\ c) = (a\ d\ b)(a\ b)(c\ d)(a\ b\ d) \in V.$$
- Sind $(a\ c\ d), (a\ d\ c) \in V$, dann erhalten wir den Widerspruch
$$(a\ c)(b\ d) = (a\ d\ c)(a\ b)(c\ d)(a\ c\ d) \in V.$$

Aber eines der drei Paare müßte in V sein. Also haben wir insgesamt einen Widerspruch hergeleitet.

C) Der zweite Sylowsatz

Wir wollen nun sehen, was wir über die 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 15.5 (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

$$\operatorname{Syl}_p(G) = \big\{U \leq G \;\big|\; |U| = p^n\big\}$$

die p-*Sylowgruppen* von G.

Beispiel 15.6
Die $\mathbb{D}_8$ ist eine 2-Sylowgruppe von $\mathbb{S}_4$.

Satz 15.7 (Zweiter Sylowsatz)
Es sei G *eine endliche Gruppe und* p *eine Primzahl mit* $|G| = p^n \cdot m$ *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* $P, Q \in \mathrm{Syl}_p(G)$ *gibt es ein* $g \in G$ *mit* $Q = P^g$.

Beweis:

a. Wir wählen ein $P \in \mathrm{Syl}_p(G)$ 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 14.7 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 15.8 (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 15.11 bestimmen können.

D) Der dritte Sylowsatz

Der dritte Sylowsatz macht Aussagen zur Anzahl der p-Sylowgruppen einer endlichen Gruppe und kann in interessanten Fällen damit auch genutzt werden, um zu zeigen, daß bestimmte Sylowgruppen Normalteiler sind.

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 15.9 (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 14.6 sieht man, daß U auf Ω durch Konjugation operiert,

$$U \times \Omega \longrightarrow \Omega : \left(u, P^g\right) \mapsto (P^g)^u = ugPg^{-1}u^{-1} = ug \cdot P \cdot (ug)^{-1} = P^{ug}.$$

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 15.7 das folgende Lemma, das im Beweis des Dritten Sylowsatzes eingeht.

Lemma 15.10
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 15.9 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 15.7 folgt. □

Wir sind nun in der Lage, den Dritten Sylowsatz zu formulieren und zu beweisen.

Satz 15.11 (Dritter Sylowsatz)
Ist G *eine endliche Gruppe und* p *eine Primzahl, die* $|G|$ *teilt, so gilt*

$$|\mathrm{Syl}_p(G)| \equiv 1 \pmod{p}$$

und für alle $P \in \mathrm{Syl}_p(G)$ *gilt zudem*

$$|\mathrm{Syl}_p(G)| = |G : N_G(P)| \;\Big|\; \frac{|G|}{|P|}.$$

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 15.7 folgt. Aus Bemerkung 15.9 mit $U = G$ wissen wir, daß G auf Ω durch Konjugation operiert und aus dem Zweiten Sylowsatz 15.7 wissen wir, daß diese Operation transitiv ist. Mit der Bahnbilanzgleichung 14.7 und Bemerkung 15.9 folgt dann

$$|\mathrm{Syl}_p(G)| = |\Omega| = |P^G| = |G : G_P| = |G : N_G(P)|.$$

Da P eine Untergruppe von $N_G(P)$ ist, teilt die Ordnung P die von $N_G(P)$ und wir erhalten

$$|\operatorname{Syl}_p(G)| = |G : N_G(P)| = \frac{|G|}{|N_G(P)|} \mid \frac{|G|}{|P|}.$$

Es bleibt noch

$$|\operatorname{Syl}_p(G)| \equiv 1 (\operatorname{mod} p)$$

zu zeigen. Dazu lassen wir mit Hilfe von Bemerkung 15.9 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

$$P^P = \left\{P^g \mid g \in P\right\} = \{P\}$$

von P. Sei dazu $Q \in \Omega = \operatorname{Syl}_p(G)$ eine p-Sylowgruppe mit

$$Q^P = \left\{Q^g \mid g \in P\right\} = \{Q\},$$

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

$$P \in \operatorname{Syl}_p(N_G(Q)) = \{Q\}.$$

Also gibt es genau eine Bahn der Länge eins unter der Operation von P auf Ω.

Wenden wir nun die Bahnbilanzgleichung 14.7 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

$$|\operatorname{Syl}_p(G)| = 1 + \sum_{i=1}^{k} |P : P_{Q_i}| \equiv 1 (\operatorname{mod} p).$$

□

Beispiel 15.12

Die Anzahl der 2-Sylowgruppen in $\mathbb{S}_4$ ist nach Beispiel 15.8 mindestens 2. Zudem ist sie ein Teiler von $\frac{24}{8} = 3$. Also gibt es genau drei 2-Sylowgruppen in $\mathbb{S}_4$.

Bemerkung 15.13
Aus dem dritten Sylowsatz folgt unmittelbar, daß eine p-Sylowgruppe P einer Gruppe G genau dann ein Normalteiler von G ist, wenn G nur eine p-Sylowgruppe besitzt.

Denn P ist genau dann ein Normalteiler von G, wenn $G = N_G(P)$ gilt; was genau dann der Fall ist, wenn $|\mathrm{Syl}_p(G)| = |G : N_G(P)| = 1$ gilt.

Dies ist allerdings nur ein Spezialfall der folgenden allgemeineren Aussage.

Lemma 15.14 (Normalteilerkriterium)
Ist G eine endliche Gruppe und ist $U \leq G$ die einzige Untergruppe von G der Ordnung d, so gilt $U \trianglelefteq G$.

Beweis: Für $g \in G$ ist die Konjugation

$$\alpha_g : G \longrightarrow G : h \mapsto h^g$$

ein Gruppenisomorphismus. Deshalb ist $U^g = \alpha_g(U)$ eine Untergruppe von G der Ordnung $|U^g| = |U| = d$. Nach Voraussetzung ist U aber die einzige solche Untergruppe, woraus

$$U = U^g$$

folgt. Also ist U ein Normalteiler von G. □

Beispiel 15.15 (Kleinsche Vierergruppe als Normalteiler in $\mathbb{A}_4$)
Die Alternierende Gruppe

$$\mathbb{A}_4 = \big\{(1), (a\ b)(c\ d), (a\ b\ c) \;\big|\; \{a, b, c, d\} = \{1, 2, 3, 4\}\big\}.$$

enthält nur eine Untergruppe der Ordnung 4, nämlich die Kleinsche Vierergruppe

$$K_4 = \{(1), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}.$$

Diese muß also ein Normalteiler in der $\mathbb{A}_4$ sein. In der Tat ist sie sogar ein Normalteiler in der größeren Gruppe $\mathbb{S}_4$, obwohl diese weitere Untergruppen der Ordnung 4 hat.

Aufgaben

Aufgabe 15.16
Zeige, in einer Gruppe der Ordnung 45 sind die Sylowgruppen Normalteiler, und folgere daraus, daß die Gruppe abelsch ist.

Aufgabe 15.17
Zeige, ist G eine endliche Gruppe, N ein Normalteiler in G und $P \in \mathrm{Syl}_p(G)$, dann gilt $P \cap N \in \mathrm{Syl}_p(N)$.

Aufgabe 15.18
Finde ein Beispiel für eine endliche Gruppe G mit Untergruppe U und p-Sylowgruppe P, so daß $U \cap P$ keine p-Sylowgruppe in U ist.

§ 16 Anwendungen der Sylowsätze

In diesem Abschnitt wollen wir uns ein paar Anwendungen der Sylowsätze anschauen, zunächst innerhalb der Gruppentheorie, aber dann auch mit Blick auf Körpererweiterungen und die Galoistheorie. Insbesondere wollen wir einen algebraischen Beweis des Hauptsatzes der Algebra geben.

A) Direkte Produkte

Eine besondere Situation liegt vor, wenn alle Sylowgruppen in G Normalteiler sind. Dann ist G das direkte Produkt der Sylowgruppen (siehe Korollar 16.6). Das spielt unter anderem bei der Klassifikation der endlichen abelschen Gruppen eine wichtige Rolle (siehe Satz 17.13).

Bemerkung 16.1 (Äußere direkte Produkte)
Sind $(G, \cdot)$ und $(H, *)$ zwei Gruppen, so wird auch das kartesische Produkt $G \times H$ durch die komponentenweise Operation

$$(g, h) \circ (g', h') := (g \cdot g', h * h')$$

für $(g, h), (g', h') \in G \times H$ zu einer Gruppe, die man das *(äußere) direkte Produkt* der beiden Gruppen nennt. Analog gilt dies für das kartesische Produkt von beliebig vielen Gruppen.

Wir wollen in diesem Abschnitt direkte Produkte als Produkte bestimmter Normalteiler wiederfinden.

Lemma 16.2 (Produkt von Untergruppe und Normalteiler)
Ist $(G, \cdot)$ eine Gruppe, $U \leq G$ eine Untergruppe von G und $N \trianglelefteq G$ ein Normalteiler von G, dann ist

$$U \cdot N = \{u \cdot n \mid u \in U, n \in N\}$$

eine Untergruppe von G. Ist $U \trianglelefteq G$ sogar ein Normalteiler, dann ist auch $U \cdot N \trianglelefteq G$ ein Normalteiler von G.

Beweis: Die Aussage wurde bereits in der Vorlesung Algebraische Strukturen bewiesen (siehe [Mar08a, Lemma 4.29]). Wir führen den Beweis nur der Vollständigkeit halber noch mal an.

Wegen $e_G = e_G \cdot e_G \in U \cdot N$ ist $U \cdot N$ eine nicht-leere Teilmenge von G. Seien nun $u \cdot n, u' \cdot n' \in U \cdot N$ zwei beliebige Elemente mit $u, u' \in U$ und $n, n' \in N$. Da N ein Normalteiler ist, gilt

$$n'' := u^{-1} \cdot n' \cdot u = (n')^{(u^{-1})} \in N$$

und somit

$$(u' \cdot n') \cdot (u \cdot n) = u' \cdot u \cdot u^{-1} \cdot n' \cdot u \cdot n = (u' \cdot u) \cdot (n'' \cdot n) \in U \cdot N.$$

Außerdem gilt

$$n''' := u \cdot n^{-1} \cdot u^{-1} = (n^{-1})^u \in N$$

und damit

$$(u \cdot n)^{-1} = n^{-1} \cdot u^{-1} = u^{-1} \cdot u \cdot n^{-1} \cdot u^{-1} = u^{-1} \cdot n''' \in U \cdot N.$$

Also ist $U \cdot N$ eine Untergruppe von G.

Sei nun U gar ein Normalteiler, dann gilt für $u \in U$, $n \in N$ und $g \in G$ zudem

$$g \cdot (u \cdot n) \cdot g^{-1} = (g \cdot u \cdot g^{-1}) \cdot (g \cdot n \cdot g^{-1}) \in U \cdot N,$$

da U und N Normalteiler sind. Also ist die Untergruppe $U \cdot N$ ein Normalteiler in G. □

Beispiel 16.3
In der symmetrischen Gruppe $\mathbb{S}_4$ ist die Kleinsche Vierergruppe

$$K_4 = \{(1), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}.$$

ein Normalteiler und das Erzeugnis eines Vierzykels $U = \langle(1\ 2\ 3\ 4)\rangle$ eine Untergruppe der Ordnung 4. Das Produkt $U \cdot K_4$ ist dann eine Untergruppe der $\mathbb{S}_4$, deren Ordnung wegen der Produktformel (siehe Aufgabe 14.23) Ordnung

$$|U \cdot K_4| = \frac{|U| \cdot |K_4|}{|U \cap K_4|} = \frac{4 \cdot 4}{2} = 8$$

ist. Es handelt sich dabei um die Diëdergruppe $\mathbb{D}_8$ aus Beispiel 14.11.

Proposition 16.4 (Inneres direktes Produkt)
Sei $(G, \cdot)$ *eine Gruppe und seien* $M, N \trianglelefteq G$ *zwei Normalteiler in* G *mit* $M \cap N = \{e_G\}$.

a. Dann gilt $m \cdot n = n \cdot m$ *für alle* $m \in M$ *und* $n \in N$.

b. Die Abbildung

$$\alpha : M \times N \longrightarrow M \cdot N : (m, n) \mapsto m \cdot n$$

ist ein Gruppenisomorphismus.

Wir nennen $M \cdot N$ *das* innere direkte Produkt *von* M *und* N.

Beweis:

a. Für $m \in M$ und $n \in N$ gilt

$$m \cdot n \cdot m^{-1} = n^m \in N^m = N,$$

da M ein Normalteiler ist, und somit

$$m \cdot n \cdot m^{-1} \cdot n^{-1} \in N.$$

Analog gilt

$$n \cdot m^{-1} \cdot n^{-1} = (m^{-1})^n \in M^n = M,$$

da N ein Normalteiler ist, und somit

$$m \cdot n \cdot m^{-1} \cdot n^{-1} \in M.$$

Also gilt

$$m \cdot n \cdot m^{-1} \cdot n^{-1} \in M \cap N = \{e_G\}$$

und damit

$$m \cdot n \cdot m^{-1} \cdot n^{-1} = e_G.$$

Multipliziert man die Gleichung von rechts zunächst mit n und dann mit m, erhält man wie gewünscht

$$m \cdot n = m \cdot n \cdot m^{-1} \cdot n^{-1} \cdot n \cdot m = e_G \cdot n \cdot m = n \cdot m.$$

b. Wir beachten zunächst, daß $M \cdot N$ nach Lemma 16.2 eine Untergruppe von G ist. Für $(m,n),(m',n') \in M \times N$ gilt dann

$$\begin{aligned}\alpha\big((m,n)\cdot(m',n')\big) &= \alpha\big((m\cdot m', n\cdot n')\big) = m\cdot m'\cdot n\cdot n' \\ &\overset{a.}{=} m\cdot n\cdot m'\cdot n' = \alpha\big((m,n)\big)\cdot\alpha\big((m',n')\big).\end{aligned}$$

Also ist α ein Gruppenhomomorphismus. α ist zudem surjektiv wegen

$$M \cdot N = \{m \cdot n \mid m \in M, n \in N\} = \{\alpha((m,n)) \mid (m,n) \in M \times N\} = \alpha(M \times N).$$

Sei ferner $(m,n) \in \mathrm{Ker}(\alpha)$, dann gilt

$$e_G = \alpha\big((m,n)\big) = m \cdot n$$

und somit

$$m = n^{-1} \in M \cap N = \{e_G\}.$$

Also folgt $m = n = e_G$ und $(m,n) = (e_G, e_G)$ ist das neutrale Element von $M \times N$. Damit ist α dann auch injektiv und somit ein Gruppenisomorphismus.

□

Bevor wir nun G als Produkt seiner Sylowgruppen schreiben, wollen wir noch eine kleine Hilfsaussage beweisen, die wir immer wieder verwenden werden, auch im Beweis der Produktzerlegung.

Lemma 16.5
Sei G eine Gruppe und seien $U, V \leq G$ endliche Untergruppen teilerfremder Ordnung. Dann gilt $U \cap V = \{e_G\}$.

Beweis: Weil $U \cap V$ eine Untergruppe von U und von V ist, muß die Ordnung $|U \cap V|$ ein Teiler von $|U|$ und von $|V|$ sein. Da die beiden Zahlen teilerfremd sind, gilt also

$$|U \cap V| = 1$$

und somit $U \cap V = \{e_G\}$. □

Korollar 16.6 (G als direktes Produkt seiner Sylowgruppen)
Sei $(G,\cdot)$ *eine endliche Gruppe,* $|G| = p_1^{n_1} \cdot \ldots \cdot p_k^{n_k}$ *die Primfaktorzerlegung von* $|G|$ *und sei* $N_i \in \mathrm{Syl}_{p_i}(G)$ *für* $i = 1, \ldots, k$.

Wenn alle $N_i \trianglelefteq G$ *Normalteiler in* G *sind, dann ist*

$$\alpha : N_1 \times \ldots \times N_k \longrightarrow G = N_1 \cdot \ldots \cdot N_k : (g_1, \ldots, g_k) \mapsto g_1 \cdot \ldots \cdot g_k$$

ein Isomorphismus.

Beweis: Wir zeigen nun per Induktion nach m, daß $N_1 \cdot \ldots \cdot N_m$ ein Normalteiler in G von Ordnung

$$|N_1 \cdot \ldots \cdot N_m| = p_1^{n_1} \cdot \ldots \cdot p_m^{n_m}$$

ist und daß die Abbildung

$$\alpha_m : N_1 \times \ldots \times N_m \longrightarrow N_1 \cdot \ldots \cdot N_m : (g_1, \ldots, g_m) \mapsto g_1 \cdot \ldots \cdot g_m$$

ein Gruppenisomorphismus ist. Für $m = 1$ ist die Aussage offensichtlich. Sei also $m > 1$. Nach Induktionsvoraussetzung ist dann

$$\alpha_{m-1} : N_1 \times \ldots \times N_{m-1} \longrightarrow N_1 \cdot \ldots \cdot N_{m-1} : (g_1, \ldots, g_{m-1}) \mapsto g_1 \cdot \ldots \cdot g_{m-1}$$

ein Isomorphismus und $N_1 \cdot \ldots \cdot N_{m-1}$ ein Normalteiler von G der Ordnung

$$|N_1 \cdot \ldots \cdot N_{m-1}| = p_1^{n_1} \cdot \ldots \cdot p_{m-1}^{n_{m-1}}.$$

Nach Lemma 16.2 ist dann

$$N_1 \cdot \ldots \cdot N_m = (N_1 \cdot \ldots \cdot N_{m-1}) \cdot N_m$$

als Produkt von zwei Normalteilern selbst ein Normalteiler von G und da die Ordnungen von $N_1 \cdot \ldots \cdot N_{m-1}$ und von N_m teilerfremd sind, ist der Schnitt nach Lemma 16.5 auch trivial. Wir können also Proposition 16.4 anwenden und erhalten einen Isomorphismus

$$\beta : N_1 \cdot \ldots \cdot N_{m-1} \times N_m \longrightarrow N_1 \cdot \ldots \cdot N_m : (g, h) \mapsto g \cdot h.$$

Dann ist aber α_m als Verkettung von β mit dem Isomorphismus

$$\alpha_{m-1} \times \mathrm{id}_{N_m} : (N_1 \times \ldots \times N_{m-1}) \times N_m \longrightarrow (N_1 \cdot \ldots \cdot N_{m-1}) \times N_m$$

ebenfalls ein Isomorphismus. Für die Ordnung der Gruppe ergibt sich daraus

$$|N_1 \cdot \ldots \cdot N_m| = |N_1 \times \ldots \times N_m| = |N_1| \cdot \ldots \cdot |N_m| = p_1^{n_1} \cdot \ldots \cdot p_m^{n_m}.$$

Wenden wir die bewiesene Aussage mit $m = k$ an, so gilt

$$G = N_1 \cdot \ldots \cdot N_k$$

aus Ordnungsgründen, und $\alpha = \alpha_m$ liefert den gesuchten Isomorphismus. □

B) Gruppen der Ordnung 15

Als einfache Anwendung der Sylowsätze und von Korollar 16.6 wollen wir nun Gruppen der Ordnung 15 klassifizieren.

Korollar 16.7 (Klassifikation von Gruppen der Ordnung 15)
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 (siehe etwa Korollar 17.8).

Die Anzahl der 5-Sylowgruppen ist ein Teiler von $\frac{15}{5} = 3$, der kongruent zu 1 modulo 5 ist. Also ist gibt es nur eine 5-Sylowgruppe und diese muß wegen Bemerkung 15.13 ein Normalteiler sein. Analog sieht man, daß es nur eine 3-Sylowgruppe gibt und daß diese ein Normalteiler von G ist.

Wegen Korollar 16.6 gilt dann

$$G = P \cdot Q \cong P \times Q \cong \mathbb{Z}_5 \times \mathbb{Z}_3.$$

Der Chinesische Restsatz liefert einen Ringisomorphismus

$$\mathbb{Z}_{15} \longrightarrow \mathbb{Z}_5 \times \mathbb{Z}_3,$$

der insbesondere ein Isomorphismus der additiven Gruppen ist. Also ist

$$G \cong \mathbb{Z}_{15}$$

eine zyklische Gruppe der Ordnung 15.

□

Als unmittelbare Folgerung erhalten wir ein Beispiel dafür, daß eine Gruppe nicht zu jedem Teiler der Gruppenordnung eine Untergruppe der entsprechenden Ordnung enthält.

Korollar 16.8 (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 (siehe auch Aufgabe 14.22). □

Beispiel 16.9 (Galoisgruppen der Ordnung 15)
Es sei $L = \mathrm{ZFK}_K(f)$ der Zerfällungskörper eines separablen Polynoms mit Galoisgruppe der Ordnung 15. Wir wollen zeigen, daß dann

$$\deg(f) \geq 8$$

gelten muß.

Aus Korollar 16.7 wissen wir, daß

$$\mathrm{Gal}\,(L/K) \cong \mathbb{Z}_{15}$$

gilt. Außerdem gilt mit $n = \deg(f)$ auch

$$\mathrm{Gal}\,(L/K) \leq \mathbb{S}_n.$$

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 16.10 (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 3.1 und Satz 3.3 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

$$|\,\mathrm{Gal}\,(L/K)\,| = |L : K| = 15.$$

Aus Korollar 16.7 folgt dann

$$\mathrm{Gal}\,(L/K) \cong \mathbb{Z}_{15},$$

und als zyklische Gruppe der Ordnung 15 mit den Teilern $1, 3, 5, 15$ hat $\mathrm{Gal}\,(L/K)$ genau vier Untergruppen (siehe Korollar 17.5). Aufgrund des Hauptsatzes der Galoistheorie hat L/K dann genau vier Zwischenkörper. Man sieht leicht, daß dies neben L und K die beiden Körper

$$K(\alpha^3) = K\left(\sqrt[5]{2}\right)$$

und

$$K(\alpha^5) = K\left(\sqrt[3]{2}\right)$$

mit den Minimalpolynomen

$$\mu_{\alpha^5} = t^3 - 2$$

und

$$\mu_{\alpha^3} = t^5 - 2$$

sind. 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.

Lemma 16.11

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 13.7 folgt dann, daß

$$L = \mathbb{R}(\alpha),$$

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 13.7. 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 16.12

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 15.3 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 16.13 (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 13.7 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 11.6 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

$$|N : \mathbb{R}| \overset{12.9}{=} |\operatorname{Gal}(M/\mathbb{R}) : \operatorname{Gal}(M/N)| = |\operatorname{Gal}(M/\mathbb{R}) : U|$$

eine ungerade Zahl ist. Nach Lemma 16.11 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 16.12 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 16.11. Also ist $k = 1$ und damit $M = L = \mathbb{C}$. □

Aufgaben

Aufgabe 16.14 (Äußeres semidirektes Produkt)
Seien $(U, \cdot)$ und $(N, \cdot)$ zwei Gruppen und sei

$$\varphi : U \longrightarrow \mathrm{Aut}(N)$$

ein Gruppenhomomorphismus. Wir definieren für $(n, u), (m, v) \in G := N \times U$

$$(n, u) \cdot (m, v) := (n \cdot \varphi(u)(m), u \cdot v)\,.$$

a. Zeige, $(G, \cdot)$ ist eine Gruppe.

b. Zeige, $N' := \{(n, e_U) \mid n \in N\}$ ist ein Normalteiler von G.

c. Zeige, $U' := \{(e_N, u) \mid u \in U\}$ ist eine Untergruppe von G.

d. Ziege, $N' \cap U' = \{e_G\}$ und $N' \cdot U' = G$.

Wir schreiben in dem Fall $G = N \ltimes_\varphi U$ und nennen G das *äußere semidirekte Produkt* von U und V.

Aufgabe 16.15 (Inneres semidirektes Produkt)
Sei $(G, \cdot)$ eine Gruppe, $U \leq G$ und $N \trianglelefteq G$ mit $U \cap N = \{e_G\}$ und $U \cdot N = G$. Zeige, dann ist

$$\varphi : U \longrightarrow \mathrm{Aut}(N) : g \mapsto (\alpha_g : N \longrightarrow N : n \mapsto n^g)$$

ein Gruppenhomomorphismus und die Abbildung

$$\beta : N \ltimes_\varphi U \longrightarrow G : (n, u) \mapsto n \cdot u$$

ist ein Gruppenisomorphismus.

§ 17 Klassifikation zyklischer und abelscher Gruppen

Wir wollen in diesem Abschnitt zyklische und abelsche Gruppen bis auf Isomorphie vollständig klassifizieren.

A) Klassifikation Zyklischer Gruppen

In den folgenden beiden Abschnitten wiederholen wir die Ergebnisse zur Klassifikation und zum Untergruppenverband zyklischer Gruppen, die aus der Vorlesung Algebraische Strukturen bereits bekannt sind (siehe [Mar08a, Satz 4.60, Korollar 4.43, Satz 4.62, Lemma 7.7, Korollar 7.50]).

Definition 17.1
Eine Gruppe $(G, \cdot)$ heißt *zyklisch*, wenn sie von einem Element erzeugt wird, d.h. wenn es ein $g \in G$ gibt, so daß $G = \langle g \rangle$.

Satz 17.2 (Klassifikation zyklischer Gruppen, [Mar08a] Satz 4.60)
Es sei $G = \langle g \rangle$ *eine zyklische Gruppe.*

a. Ist $|G| = \infty$*, so haben wir den Gruppenisomorphismus*

$$\alpha : \mathbb{Z} \xrightarrow{\cong} G : z \mapsto g^z.$$

b. Ist $|G| = n < \infty$*, so haben wir den Gruppenisomorphismus*

$$\overline{\alpha} : \mathbb{Z}_n \xrightarrow{\cong} G : \overline{z} \mapsto g^z.$$

Beweis: Für die Abbildung

$$\alpha : \mathbb{Z} \xrightarrow{\cong} G : z \mapsto g^z$$

und zwei ganze Zahlen $x, y \in \mathbb{Z}$ gilt

$$\alpha(x + y) = g^{x+y} = g^x \cdot g^y = \alpha(x) \cdot \alpha(y).$$

α ist also ein Gruppenhomomorphismus, und es gilt

$$\mathrm{Im}(\alpha) = \{g^z \mid z \in \mathbb{Z}\} = \langle g \rangle = G,$$

d.h. α ist surjektiv.

Ist $|G| = o(g) = \infty$, so ist

$$\{0\} = \{z \in \mathbb{Z} \mid g^z = e_G\} = \mathrm{Ker}(\alpha),$$

d.h. α ist in diesem Fall auch injektiv.

Ist $|G| = o(g) = n < \infty$, so ist

$$\mathrm{Ker}(\alpha) = \{z \in \mathbb{Z} \mid g^z = e_G\} = n\mathbb{Z}.$$

Aus dem Homomorphiesatz folgt mithin, daß die Abbildung $\overline{\alpha}$ ein Gruppenisomorphismus ist. □

B) Untergruppenverband einer endlichen zyklischen Gruppe

Will man nun den Untergruppenverband endlicher zyklischer Gruppen verstehen, so reicht es, die Untergruppen von $\mathbb{Z}_n$ und dazu die von $\mathbb{Z}$ kennenzulernen.

Lemma 17.3 (Untergruppenverband von $\mathbb{Z}_n$)

a. *Die Untergruppen der additiven Gruppe* $(\mathbb{Z}, +)$ *sind genau die Ideale im Ring* $(\mathbb{Z}, +, \cdot)$*, d.h. die Mengen der Form*

$$m\mathbb{Z} = \{m \cdot z \mid z \in \mathbb{Z}\}$$

mit $m \in \mathbb{N}$.

b. *Ist* $n \in \mathbb{Z}_{>0}$ *eine positive ganze Zahl, so gilt*

$$\overline{U} \leq \mathbb{Z}_n \iff \exists\, m \in \{1, \ldots, n\} \text{ mit } m \text{ teilt } n \,:\, \overline{U} = m\mathbb{Z}/n\mathbb{Z} = \langle \overline{m}_n \rangle.$$

Insbesondere ist jede Untergruppe von $\mathbb{Z}_n$ *zyklisch.*

c. *Sind* k *und* m *zwei Teiler von* $n \in \mathbb{Z}_{>0}$*, dann gilt* $\langle \overline{k}_n \rangle \subseteq \langle \overline{m}_n \rangle$ *genau dann, wenn* m *ein Teiler von* k *ist.*

Beweis:

a. Da jedes Ideal bezüglich der Addition eine Untergruppe ist, reicht es zu zeigen, daß jede Untergruppe U von $(\mathbb{Z}, +)$ auch ein Ideal ist. Seien dazu $u \in U$ und $z \in \mathbb{Z}$ gegeben, dann gilt

$$z \cdot u = \begin{cases} \sum_{i=1}^{z} u, & \text{falls } z > 0, \\ 0, & \text{falls } z = 0, \\ \sum_{i=1}^{-z} (-u), & \text{falls } z < 0. \end{cases}$$

Da U als Untergruppe mit u auch $-u$ und endliche Summen seiner Elemente enthält, gilt jeweils $z \cdot u \in U$. Als Untergruppe ist U zudem bezüglich der Addition abgeschlossen und nicht-leer. Mithin ist U ein Ideal in $\mathbb{Z}$.
Daß die Ideale alle von der Form $m\mathbb{Z}$ sind, gilt, weil $\mathbb{Z}$ ein Hauptidealring ist.

b. Die Aussage folgt aus der Tatsache, daß jede Untergruppe $\overline{U}$ der Faktorgruppe $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ von der Form $U/n\mathbb{Z}$ für die eindeutig bestimmte Untergruppe

$$U = \{z \in \mathbb{Z} \mid \overline{z} \in \overline{U}\}$$

mit $n\mathbb{Z} \subseteq U$ ist, sowie aus der Tatsache, daß das Ideal $U = m\mathbb{Z}$ das Ideal $n\mathbb{Z}$ genau dann enthält, wenn m ein Teiler von n ist.

c. Es gilt

$$k\mathbb{Z}/n\mathbb{Z} = \langle \overline{k}_n \rangle \subseteq \langle \overline{m}_n \rangle = m\mathbb{Z}/n\mathbb{Z}$$

genau dann, wenn

$$k\mathbb{Z} \subseteq m\mathbb{Z}.$$

Letzteres ist aber gleichwertig dazu, daß m ein Teiler von k ist.

□

Beispiel 17.4 (Untergruppenverband von $\mathbb{Z}_{12}$)
Aus dem Teilerverband der Zahl 12 mit den Teilern $1, 2, 3, 4, 6, 12$ ergibt sich gemäß Lemma 17.3 der Untergruppenverband der $\mathbb{Z}_{12}$ wie in Abbildung 1 dargestellt.

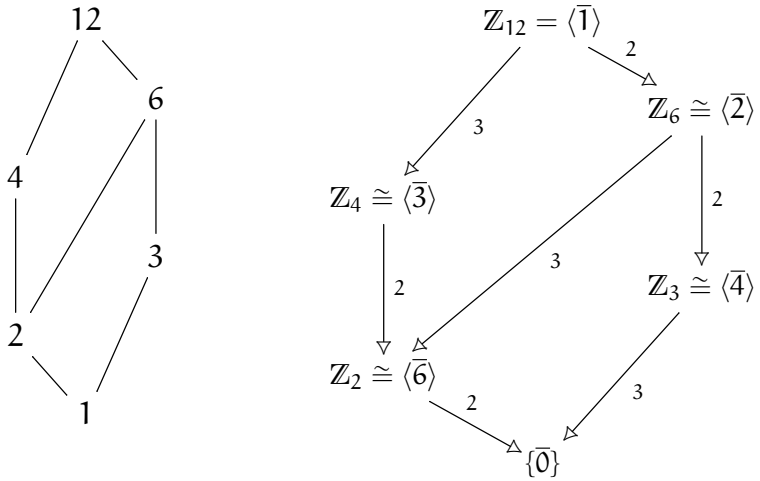

ABBILDUNG 1. Teilerverband von 12 und Untergruppenverband von $\mathbb{Z}_{12}$

Korollar 17.5 (Untergruppenverband einer endlichen zyklischen Gruppe)
Ist $G = \langle g\rangle$ *eine zyklische Gruppe der Ordnung* $|G| = n < \infty$*, dann gilt*

$$U \leq G \iff \exists\, m \in \{1, \dots, n\} \text{ mit } m \text{ teilt } n \,:\, U = \langle g^m\rangle.$$

Für eine solche Untergruppe gilt zudem

$$\left|\langle g^m\rangle\right| = \frac{n}{m}.$$

Insbesondere hat G *für jeden Teiler von* n *genau eine Untergruppe dieser Ordnung.*

Schließlich gilt für zwei Teiler k, m *von* n*:*

$$\langle g^k\rangle \subseteq \langle g^m\rangle \iff m \mid k.$$

Beweis: Nach Satz 17.2 ist die Abbildung

$$\overline{\alpha} : \mathbb{Z}_n \longrightarrow G : \overline{z} \mapsto g^z$$

ein Gruppenisomorphismus mit $\alpha(\overline{m}_n) = g^m$, so daß die erste und die letzte Aussage aus Lemma 17.3 folgen. Die Aussage zur Ordnung erhalten wir aus Lemma 13.9, da $\operatorname{ggt}(m, n) = m$. Schließlich beachte man noch, daß mit m auch $\frac{n}{m}$ alle Teiler von n durchläuft. □

Da die Untergruppen von $\mathbb{Z}$ zyklisch sind nach Lemma 17.3 erhalten wir mit Satz 17.2 und Korollar 17.5 folgende Aussage.

Korollar 17.6
Jede Untergruppe einer zyklischen Gruppe ist zyklisch.

C) Der Satz von Lambert–Euler–Gauß

Wir haben eben gesehen, daß zyklische Gruppen zu jedem Teiler der Gruppenordnung genau eine Untergruppe dieser Ordnung besitzen. Wir wollen nun zeigen, daß dies auch nur in zyklischen Gruppen der Fall ist.

Satz 17.7 (Charakterisierung zyklischer Gruppen)
Für eine endliche Gruppe $(G, \cdot)$ *sind die folgenden Aussagen äquivalent:*

a. G *ist zyklisch.*

b. G *hat für jeden Teiler* d *von* $|G|$ *genau eine Untergruppe der Ordnung* d.

c. G *hat für jeden Teiler* d *von* $|G|$ *höchstens eine Untergruppe der Ordnung* d.

Beweis: Es sei $n = |G|$ die Ordnung von G.

a. $\Longrightarrow$ b.: Diese Aussage wurde bereits in der Vorlesung algebraische Strukturen bewiesen, siehe Korollar 17.5.

b. $\Longrightarrow$ c.: Dies gilt offenbar.

c. $\Longrightarrow$ a.: Wir führen den Beweis mittels Induktion nach $|G|$, wobei für $|G| = 1$ nichts zu zeigen ist.

Sei also $|G| > 1$. Wir halten zunächst fest, daß jede echte Untergruppe von G ebenfalls für jeden Teiler d der Gruppenordnung höchstens eine Untergruppe der Ordnung d besitzt und mithin nach Induktionsvoraussetzung zyklisch ist.

Wir betrachten zunächst den Fall, daß

$$|G| = p^n$$

nur einen Primfaktor $p \in \mathbb{P}$ besitzt. Nach dem Ersten Sylowsatz 15.3 hat G eine Untergruppe U der Ordnung

$$|U| = p^{n-1},$$

die dann zyklisch ist. Aus Korollar 17.5 wissen wir deshalb, daß U für jedes p^k mit $1 \leq k \leq n-1$ eine Untergruppe der Ordnung p^k enthält.

Sei nun $h \in G \setminus U$, dann gilt

$$o(h) = p^k$$

für ein $1 \leq k \leq n$ wegen des Satzes von Lagrange. Wäre $k < n$, so wäre $\langle h \rangle$ eine Untergruppe von G von Ordnung p^k, und weil G höchstens eine solche besitzt und eine solche schon in U enthalten ist, müßte

$$\langle h \rangle \subseteq U$$

gelten, im Widerspruch zu $h \notin U$. Also ist $k = n$ und somit aus Ordnungsgründen

$$\langle h \rangle = G.$$

Es bleibt noch, den Fall zu betrachten, daß

$$|G| = p_1^{n_1} \cdot \ldots \cdot p_k^{n_k}$$

mindestens zwei verschiedene Primfaktoren hat. Wir können zu jedem Primfaktor p_i von $|G|$ eine p_i-Sylowgruppe N_i wählen. Nach Voraussetzung ist N_i die einzige Untergruppe von G der Ordnung $p_i^{n_i}$ und ist deshalb nach Lemma 15.14 ein Normalteiler in G. Als echte Untergruppe von G ist N_i zudem zyklisch und nach Satz 17.2 gilt deshalb

$$N_i \cong \mathbb{Z}_{p_i^{n_i}}.$$

Wenden wir nun Korollar 16.6 an, so erhalten wir

$$G \cong N_1 \times \ldots \times N_k \cong \mathbb{Z}_{p_1^{n_1}} \times \ldots \times \mathbb{Z}_{p_k^{n_k}} \cong \mathbb{Z}_{|G|},$$

wobei der letzte Isomorphismus aus dem Chinesischen Restsatz folgt. Damit ist G insbesondere zyklisch. □

Mit der Charakterisierung entdecken wir die folgende Aussage aus den Algebraischen Strukturen nochmals.

Korollar 17.8 (Gruppen von Primzahlordnung sind zyklisch.)
Ist G eine Gruppe von Primzahlordnung, so ist G zyklisch.

Beweis: Da die Ordnung einer Untergruppe ein Teiler der Ordnung von G ist, hat G nur die trivialen Untergruppen und hat mithin zu jedem Teiler der Gruppenordnung genau eine Gruppe dieser Ordnung. Also ist G zyklisch nach Satz 17.7. □

Korollar 17.9 (Lambert–Euler–Gauß)
Endliche Untergruppen der multiplikativen Gruppe eines Körpers sind zyklisch.

Beweis: Sei $(G, \cdot)$ eine endliche Untergruppe der multiplikativen Gruppe eines Körpers K. Ist $U \leq G$ eine Untergruppe von G der Ordnung d, wobei d ein Teiler von $|G|$ ist, so gilt nach dem Satz von Lagrange

$$u^d = u^{|U|} = 1$$

für jedes $u \in U$. Damit sind die d Elemente von U Nullstellen des Polynoms

$$t^d - 1 \in K[t].$$

Da dieses Polynom höchstens d Nullstellen besitzt, kann es keine zweite Untergruppe von G der Ordnung d geben. Damit ist G aufgrund von Satz 17.7 zyklisch. □

D) Charakterisierung zyklischer p-Gruppen

Wir wollen nun ein Kriterium formulieren, mit Hilfe dessen wir bei einer p-Gruppe feststellen können, ob sie zyklisch ist.

Proposition 17.10 (Charakterisierung zyklischer p-Gruppen)
Eine nicht-triviale abelsche p-Gruppe ist genau dann zyklisch, wenn sie nur eine Untergruppe der Ordnung p besitzt.

Beweis: Ist G eine nicht-triviale zyklische p-Gruppe, so besitzt G nach Korollar 17.5 genau eine Untergruppe der Ordnung p.

Sei nun umgekehrt G eine nicht-triviale abelsche Gruppe mit genau eine Untergruppe der Ordnung p und $|G| = p^n$. Wir zeigen mittels Induktion nach n, daß G zyklisch ist. Für $n = 1$ ist G dabei als Gruppe von Primzahlordnung nach Korollar 17.8 zyklisch. Sei also $n > 1$. Die Abbildung

$$\alpha : G \longrightarrow G : g \mapsto g^p$$

ist ein Gruppenhomomorphismus,

$$\alpha(g \cdot h) = (g \cdot h)^p = g^p \cdot h^p = \alpha(g) \cdot \alpha(h),$$

da G abelsch ist. Der Kern

$$\mathrm{Ker}(\alpha) = \{g \in G \mid \alpha(g) = e_G\} = \{g \in G \mid g^p = e_G\}$$

enthält alle Elemente der Ordnung p von G. Da jedes von diesen eine Untergruppe der Ordnung p erzeugt und es nur eine solche gibt, muß $\mathrm{Ker}(\alpha)$ die eindeutig bestimmte Untergruppe der Ordnung p von G sein. Aus dem Homomorphiesatz erhalten wir

$$|\mathrm{Im}(\alpha)| = \frac{|G|}{|\mathrm{Ker}(\alpha)} = \frac{p^n}{p} = p^{n-1} > 1.$$

Als Untergruppe von G kann $\mathrm{Im}(\alpha)$ höchstens eine Untergruppe der Ordnung p enthalten und wegen des Ersten Sylowsatzes muß $\mathrm{Im}(\alpha)$ auch eine Untergruppe der Ordnung p enthalten. Mittels Induktion ist dann

$$\mathrm{Im}(\alpha) = \langle h \rangle$$

zyklisch, und wir können ein $g \in G$ wählen mit

$$h = \alpha(g) = g^p.$$

Aus Lemma 13.9 wissen wir dabei

$$o(g) = o(h) \cdot \mathrm{ggt}(o(g), p) = |\mathrm{Im}(\alpha)| \cdot p = p^{n-1} \cdot p = p^n,$$

so daß aus Ordnungsgründen

$$G = \langle g \rangle$$

gelten muß. □

Bemerkung 17.11 (Quaterionengruppe)
Die Voraussetzung abelsch in Proposition 17.10 ist essentiell, wie das Beispiel der Quaterionengruppe in Aufgabe 14.25 zeigt. Diese ist eine nicht-abelsche 2-Gruppe der Ordnung 8, die genau eine Untergruppe der Ordnung 2 besitzt. Als nicht-abelsche Gruppe ist sie erst recht nicht zyklisch.

E) Klassifikation endlicher abelscher Gruppen

Wir wollen in diesem Abschnitt die endlichen abelschen Gruppen bis auf Isomorphie klassifizieren, indem wir zeigen, daß sie in bis auf die Reihenfolge eindeutiger Art und Weise als direktes Produkt zyklischer Gruppen von Primzahlpotenzordnung geschrieben werden können. Dazu beweisen wir zunächst eine Hilfsaussage.

Lemma 17.12 (Produktzerlegung von abelschen p-Gruppen)
Sei G eine abelsche p-Gruppe und $g \in G$ ein Element von maximaler Ordnung, dann gibt es eine Untergruppe $U \leq G$, so daß $G = \langle g \rangle \cdot U$ das innere direkte Produkt von U und $\langle g \rangle$ ist. Insbesondere gilt dann

$$G \cong \langle g \rangle \times U.$$

Beweis: Wir führen den Beweis mit Induktion nach $n = |G|$, wobei wir $g = e_G$ und $U = \{e_G\}$ für $n = 1$ wählen können. Sei also $n > 1$.

Wenn G zyklisch ist, muß zwangsläufig

$$G = \langle g \rangle$$

gelten und wir können $U = \{e_G\}$ wählen. Andernfalls besitzt G nach Proposition 17.10 mehr als eine Untergruppe der Ordnung p, und da $\langle g \rangle$ als zyklische Gruppe nur eine Untergruppe der Ordnung p hat, muß es eine Untergruppe $N \leq G$ mit

$$|N| = p$$

und

$$N \cap \langle g \rangle = \{e_G\}$$

geben. Da G abelsch ist, ist N sogar ein Normalteiler von G und die Faktorgruppe G/N hat die Ordnung

$$|G/N| = \frac{|G|}{|N|} = \frac{|G|}{p} < |G|.$$

Zudem gilt für die Restklasse $\overline{g} = gN \in G/N$ genau dann

$$g^k N = \overline{g}^k = \overline{e_G} = N$$

wenn

$$g^k \in N \cap \langle g \rangle = \{e_G\}$$

gilt, was genau dann der Fall ist, wenn

$$g^k = e_G$$

gilt. Dies impliziert die Gleichheit der Ordnungen

$$o(\overline{g}) = o(g)$$

von g und $\overline{g}$. Da die Elemente in G/N keine größere Ordnung als die in G haben können, ist $\overline{g}$ also ein Element maximaler Ordnung in G/N. Wenden wir nun Induktion auf G/N an, so finden wir eine Untergruppe $\overline{U} \leq G/N$, so daß G/N das innere direkte Produkt von $\overline{U}$ und $\langle\overline{g}\rangle$ ist. Sei nun $U \leq$ die eindeutig bestimmte Untergruppe von G mit

$$\overline{U} = U/N,$$

dann gilt einerseits

$$(U \cdot \langle g\rangle)/N = \overline{U} \cdot \langle\overline{g}\rangle = G/N$$

und somit

$$G = U \cdot \langle g\rangle.$$

Andererseits gilt für $h \in U \cap \langle g\rangle$, daß es ein $k \in \mathbb{N}$ mit

$$h = g^k$$

gibt und daß damit

$$\overline{h} = \overline{g}^k \in \overline{U} \cap \langle\overline{g}\rangle = \{\overline{e_G}\} = \{N\}$$

gilt. Das bedeutet

$$hN = \overline{h} = \overline{e_G} = N$$

und deshalb

$$g^k = h \in N \cap \langle g\rangle = \{e_G\}.$$

Also gilt auch

$$U \cap \langle g\rangle = \{e_G\},$$

und G ist das innere direkte Produkt der beiden Gruppen. Aus Proposition16.4 folgt dann auch

$$G \cong \langle g\rangle \times U.$$

□

Satz 17.13 (Klassifikation endlicher abelscher Gruppen)
Ist G *eine endliche abelsche Gruppe und ist* $|G| = p_1^{n_1} \cdot \ldots p_k^{n_k}$ *die Primfaktorzerlegung von* $|G|$*, dann gibt es eindeutig bestimmte Zahlen*

$$n_{i1} \geq n_{i2} \geq \ldots \geq n_{ij_i} \geq 1$$

für $i = 1, \ldots, k$*, so daß*

$$G \cong N_1 \times \ldots \times N_k$$

und

$$N_i \cong \mathbb{Z}_{p_i^{n_{i1}}} \times \ldots \times \mathbb{Z}_{p_i^{n_{ij_i}}}$$

sowie

$$n_i = n_{i1} + \ldots + n_{ij_i}$$

gilt, wobei die N_i *gerade die* p_i*-Sylowgruppen von* G *sind. Wir nennen die Menge der Tupel* $(n_{i1}, \ldots, n_{ij_i})_{p_i}$ *den* Typ *der abelschen Gruppe* G*.*

Beweis: Da G abelsch ist, sind die p_i-Sylowgruppen von G Normalteiler und aus Korollar 16.6 folgt, daß

$$G \cong N_1 \times \ldots \times N_k$$

isomorph zum direkten Produkt seiner p_i-Sylowgruppen N_i ist.

Die N_i sind p_i-Gruppen und wenden wir Lemma 17.12 wiederholt an, finden wir $g_1, \ldots, g_{j_i} \in N_i$, so daß

$$N_i \cong \langle g_1 \rangle \times \ldots \times \langle g_{j_i} \rangle$$

und die Ordnungen der g_l sind dabei der Größe nach geordnet. Es gibt also natürliche Zahlen

$$n_{i1} \geq \ldots \geq n_{ij_i} \geq 1,$$

so daß

$$o(g_l) = p_i^{n_{il}}$$

und

$$\langle g_l \rangle \cong \mathbb{Z}_{p_i^{n_{il}}}.$$

Dabei gilt zudem

$$p_i^{n_i} = |N_i| = |\mathbb{Z}_{p_i^{n_{i1}}} \times \ldots \times \mathbb{Z}_{p_i^{n_{ij_i}}}| = \prod_{l=1}^{j_i} |\mathbb{Z}_{p_i^{n_{il}}}| = \prod_{l=1}^{n_i} p_i^{n_{il}} = p_i^{n_{i1}+\ldots+n_{ij_i}}$$

und deshalb

$$n_i = n_{i1} + \ldots + n_{ij_i}.$$

Dies zeigt die Existenz der obigen Zerlegung. Die Eindeutigkeit der Zahlen zeigen wir erst in Korollar 17.16 und verwenden bis dahin nur deren Existenz. □

Aus Satz 17.13 folgt unmittelbar das folgende Korollar.

Korollar 17.14 (Produktzerlegung endlicher abelscher Gruppen)
Endliche abelsche Gruppen sind isomorph zu direkten Produkten zyklischer Gruppen.

Eine weitere Folgerung aus der Klassifikation endlicher abelscher Gruppen ist ein alternativer Beweis für den Satz von Lambert–Euler–Gauß.

Alternativer Beweis des Satzes von Lambert–Euler–Gauß 17.9: Sei K ein Körper und G eine endliche Untergruppe der multiplikativen Gruppe $(K^*, \cdot)$ von K. Dann ist G eine abelsche Gruppe und aus dem Klassifikationssatz 17.13 wissen wir, daß

$$G \cong N_1 \times \ldots \times N_k$$

isomorph zum direkten Produkt seiner p_i-Sylowgruppen N_i ist.

Dabei ist N_i eine abelsche p_i-Gruppe. Ist $U \leq N_i$ eine Untergruppe von N_i der Ordnung p_i, dann gilt wegen des Satzes von Lagrange

$$u^{p_i} = 1$$

für jedes $u \in U$, d.h. die Elemente von U sind Nullstellen des Polynoms

$$t^{p_i} - 1 \in K[t].$$

Da das Polynom höchstens p_i Nullstellen hat, hat N_i höchstens eine Untergruppe der Ordnung p_i. Wegen des Ersten Sylowsatzes 15.3 hat N_i auch eine solche Untergruppe, so daß die Voraussetzungen von Lemma 17.10 erfüllt sind. Mithin ist

$$N_i \cong \mathbb{Z}_{p_i^{n_i}}$$

eine zyklische p_i-Gruppe. Der Chinesische Restsatz impliziert dann

$$G \cong N_1 \times \ldots \times N_k \cong \mathbb{Z}_{p_1^{n_1}} \times \ldots \times \mathbb{Z}_{p_k^{n_k}} \cong \mathbb{Z}_m$$

mit $m = p_1^{n_1} \cdot \ldots \cdot p_k^{n_k}$. Damit ist G eine zyklische Gruppe. □

F) Eindeutigkeit des Typs einer abelschen Gruppe

Wir müssen noch zeigen, daß der Typ der abelschen Gruppe durch diese eindeutig festgelegt ist. Da die Zerlegung als direktes Produkt der Sylowgruppen eindeutig ist, reicht es, dies für eine abelsche p-Gruppe zu zeigen. Die folgende Proposition ist der Schlüssel dazu.

Proposition 17.15 (G_p und G^p)
Es sei $(n_1, \ldots, n_j)_p$ *Typ einer abelschen* p*-Gruppe* G *mit* $n_r > n_{r+1} = 1$.

a. Die Menge $G_p = \{g \in G \mid g^p = e_G\}$ *ist ein Untergruppe von* G *der Ordnung* p^j.

b. Die Menge $G^p = \{g^p \mid g \in G\}$ *ist eine Untergruppe von* G *vom Typ*

$$(n_1 - 1, \ldots, n_r - 1)_p.$$

Beweis: Wir betrachten zunächst noch mal den Gruppenhomomorphismus

$$\alpha : G \longrightarrow G : g \mapsto g^p$$

aus dem Beweis von Proposition 17.10. Dann gilt

$$G_p = \mathrm{Ker}(\alpha) \leq G$$

und

$$G^p = \mathrm{Im}(\alpha) \leq G.$$

Da G den Typ $(n_1, \ldots, n_j)_p$ hat, gibt es Elemente $g_1, \ldots, g_j \in G$, so daß

$$\varphi : \langle g_1 \rangle \times \ldots \times \langle g_j \rangle \xrightarrow{\cong} G : (h_1, \ldots, h_j) \mapsto h_1 \cdot \ldots \cdot h_j$$

ein Isomorphismus ist und $o(g_i) = p^{n_i}$ gilt. Dann wird G von $g_1, \ldots, g_j$ erzeugt und damit wird G^p von $g_1^p, \ldots, g_j^p$ erzeugt, da G abelsch ist, so daß wir

$$\varphi^{-1}(G^p) = \langle g_1^p \rangle \times \ldots \times \langle g_j^p \rangle.$$

erhalten. Mit Lemma 13.9 gilt dabei

$$o(g_l^p) = \frac{o(g)}{ggt(o(g), p)} = \frac{p^{n_l}}{p} = p^{n_l - 1},$$

woraus sich einerseits die Aussage zum Typ von G^p ergibt und andererseits die Ordnung

$$|G^p| = o(g_1^p) \cdot \ldots \cdot o(g_j^p) = p^{n_1 - 1} \cdot \ldots \cdot p^{n_j - 1} = p^{n-j}.$$

Aus dem Homomorphiesatz erhalten wir damit

$$|G_p| = |\operatorname{Ker}(\alpha)| = \frac{|G|}{|\operatorname{Im}(\alpha)|} = \frac{|G|}{|G^p|} = \frac{p^n}{p^{n-j}} = p^j.$$

□

Korollar 17.16 (Eindeutigkeit der Produktzerlegung)
Der Typ einer endlichen abelschen p-Gruppe ist eindeutig bestimmt.

Beweis: Wir beweisen die Aussage mit Induktion nach n für $|G| = p^n$. Ist $n = 1$, so ist $G \cong \mathbb{Z}_p$ und der Typ von G ist notwendigerweise $(1)_p$. Sei also $n > 1$.

Wir beachten, daß die Untergruppen G_p und G^p nur von G und nicht von der Zerlegung in Satz 17.13 abhängt. Seien $(n_1, \ldots, n_j)_p$ und $(m_1, \ldots, m_k)_p$ zwei Typen von G. Aus Proposition 17.15 folgt dann

$$p^j = |G_p| = p^k$$

und somit

$$j = k.$$

Seien ferner r und s so gewählt, daß

$$n_r > n_{r+1} = 1 = m_{s+1} < m_s,$$

dann hat G^p nach Proposition 17.15 die beiden Typen

$$(n_1 - 1, \ldots, n_r - 1)_p$$

und

$$(m_1 - 1, \ldots, m_s - 1)_p.$$

Da die Ordnung von G^p echt kleiner als die von G ist, ist der Typ von G^p durch G^p und damit durch G nach Induktionsvoraussetzung eindeutig festgelegt. Es gilt also

$$r = s$$

sowie

$$n_l = m_l$$

für $l = 1, \ldots, r$. Aber für $l = r + 1, \ldots, j$ gilt ohnehin

$$n_l = m_l = 1.$$

Damit haben wir die Aussage bewiesen. □

Beispiel 17.17

Wir geben ein Beispiel für zwei Körpererweiterungen mit isomorphen Galoisgruppen.

a. Die multiplikative Gruppe $(\mathbb{Z}_{16}^*, \cdot)$ des Rings $\mathbb{Z}_{16}$ ist eine abelsche Gruppe der Ordnung

$$|\mathbb{Z}_{16}^*| = \varphi(16) = \varphi(2^4) = 2^4 - 2^3 = 8,$$

wobei φ die Eulersche φ-Funktion bezeichnet (siehe Aufgabe 13.26). Eine kurze Rechnung zeigt

$$\overline{5}^2 = \overline{25} = \overline{9}, \overline{5}^3 = \overline{45} = \overline{13}, \overline{5}^4 = \overline{65} = \overline{1}$$

und

$$\overline{15}^2 = (-\overline{1})^2 = \overline{1}.$$

Also sind $M = \langle\overline{5}\rangle$ und $N = \langle-\overline{1}\rangle$ zwei Normalteiler in $\mathbb{Z}_{16}^*$ mit

$$M \cap N = \{\overline{1}\}.$$

Zudem ist $M \cdot N$ eine Untergruppe von $\mathbb{Z}_{16}^*$, die mehr als die 4 Elemente von M enthält, und aus Ordnungsgründen folgt deshalb

$$M \cdot N = \mathbb{Z}_{16}^*.$$

Damit ist dann $\mathbb{Z}_{16}^*$ das innere direkte Produkt von M und N und wir erhalten

$$\mathbb{Z}_{16}^* = M \cdot N \cong M \times N \cong \mathbb{Z}_4 \times \mathbb{Z}_2.$$

Die Gruppe ist isomorph nach Satz 13.15 zur Galoisgruppe

$$\mathrm{Gal}\,(\mathbb{Q}(\zeta_{16})/\mathbb{Q}) \cong \mathbb{Z}_{16}^*$$

des 16-ten Kreisteilungskörpers

$$\mathbb{Q}(\zeta_{16}) = \mathrm{ZFK}_{\mathbb{Q}}(t^{16} - 1) = \mathrm{ZFK}_{\mathbb{Q}}(\Phi_{16}).$$

b. Der Chinesische Restsatz liefert uns die Zerlegung

$$\mathbb{Z}_{20}^* \cong \mathbb{Z}_5^* \times \mathbb{Z}_4^* = \langle\overline{2}_5\rangle \times \langle\overline{3}_4\rangle \cong \mathbb{Z}_4 \times \mathbb{Z}_2.$$

Diese Gruppe ist isomorph nach Satz 13.15 zur Galoisgruppe

$$\mathrm{Gal}\,(\mathbb{Q}(\zeta_{20})/\mathbb{Q}) \cong \mathbb{Z}_{20}^*$$

des 20-ten Kreisteilungskörpers

$$\mathbb{Q}(\zeta_{20}) = \mathrm{ZFK}_{\mathbb{Q}}(t^{20} - 1) = \mathrm{ZFK}_{\mathbb{Q}}(\Phi_{20}).$$

Die beiden Körpererweiterungen $\mathbb{Q}(\zeta_{16})/\mathbb{Q}$ und $\mathbb{Q}(\zeta_{20})/\mathbb{Q}$ haben also Zwischenkörperverbände der gleichen Struktur, auch wenn die Körper verschieden sind.

Aufgaben

Aufgabe 17.18
Berechne den Untergruppenverband der zyklischen Gruppen $\mathbb{Z}_{40}$ und $\mathbb{Z}_{60}$.

Aufgabe 17.19
Es sei $(G, \cdot)$ eine Gruppe, $g \in G$ und $n \in \mathbb{Z}_{>0}$. Zeige, genau dann gibt es einen Gruppenhomomorphismus $\alpha : \mathbb{Z}_n \longrightarrow G$ mit $\alpha(\overline{1}) = g$, wenn die Ordnung von g ein Teiler von n ist.

Aufgabe 17.20
Zeige, eine nicht-triviale abelsche Gruppe G ist genau dann einfach, wenn $|G|$ eine Primzahl ist.

Aufgabe 17.21
Man finde je einen Erzeuger der zyklischen Gruppen $(\mathbb{Z}_3^*, \cdot)$, $(\mathbb{Z}_5^*, \cdot)$ und $(\mathbb{Z}_{17}^*, \cdot)$.

Aufgabe 17.22 (Die Automorphismengruppe einer endlichen zyklischen Gruppe)
Die Menge

$$\mathrm{Aut}(\mathbb{Z}_n) = \{\alpha : \mathbb{Z}_n \longrightarrow \mathbb{Z}_n \mid \alpha \text{ ist ein Gruppenautomorphismus}\}$$

ist eine Untergruppe der symmetrischen Gruppe $(\mathrm{Sym}(\mathbb{Z}_n), \circ)$. Zeige, die Abbildung

$$\varphi : \mathrm{Aut}(\mathbb{Z}_n) \longrightarrow \mathbb{Z}_n^* : \alpha \mapsto \alpha(\overline{1})$$

ist ein Gruppenisomorphismus.

Aufgabe 17.23
Bestimme die Struktur des Zwischenkörperverbands von $\mathbb{Q}(\zeta_{15})/\mathbb{Q}$.

Aufgabe 17.24
Bestimme bis auf Isomorphie alle Gruppen der Ordnung 10201.

Aufgabe 17.25
Wir betrachten die Untergruppe $G = \langle A, B\rangle \leq \mathrm{Gl}_2(\mathbb{C})$ der Gruppe der invertierbaren 2×2-Matrizen über $\mathbb{C}$, die von den beiden Matrizen

$$A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \text{und} \quad B = \begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix}$$

erzeugt wird. Zeige die folgenden Aussagen:

a. $A^2 = B^2 = (I \circ J)^2 = -\mathbb{1}_2$ und $A \circ B = B \circ Y$.

b. G ist eine abelsche Gruppe der Ordnung $|G| = 8$.

c. Bestimme den Isomorphietyp von G sowie den Untergruppenverband

Vergleiche die Gruppe auch mit der Quaterionengruppe aus Aufgabe 14.25).

§ 18 Auflösbare Gruppen

In diesem Abschnitt wollen wir die Klasse der abelschen Gruppen erweitern, indem wir eine Bedingung einführen, die schwächer als die Kommutativität der Multiplikation ist, die aber stark genug ist, die Gruppe in abelsche Teile zu zerlegen. Die notwendigen Begriffe führen wir im folgenden ein.

A) Einfache Gruppen

Definition 18.1 (Einfache Gruppen)
Eine Gruppe G heißt *einfach*, wenn sie nur die Normalteiler G und $\{e_G\}$ besitzt.

Proposition 18.2 (Einfache abelsche Gruppen)
Eine nicht-triviale 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 15.1 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 18.3 (Klassifikation einfacher Gruppen)
Will man eine endliche Gruppe G untersuchen und kennt einen nicht-trivialen Normalteiler $N \lhd G$, dann verrät die Struktur der kleineren Gruppen N und G/N eine Menge über G und man kann G aus diesen beiden rekonstruieren. In diesem Sinne bilden die Gruppen, die keine nicht-trivialen Normalteiler besitzen, die Elementarbausteine, in die sich alle anderen Gruppen zerlegen lassen (Satz von Jordan-Hölder). 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 18.4 ($\mathbb{A}_5$ 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 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 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 18.5 (Auflösbare Gruppen)
Eine Gruppe G heißt *auflösbar*, wenn es eine Kette

$$\{e_G\} = G_k \leq G_{k-1} \leq \ldots \leq G_1 \leq G_0 = G$$

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 18.6 (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. 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 18.4 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.

Bemerkung 18.7 (Abgeleitete Reihe)
Man beachte, daß in Beispiel 18.6 b. alle Gruppen in der Subnormalteilerkette sogar Normalteiler von $\mathbb{S}_4$ sind; das ist mehr als gefordert ist, aber eine solche Normalteilerkette, die sogenannte abgeleitete Reihe, gibt es bei auflösbaren Gruppen immer (siehe Aufgabe 18.19).

Proposition 18.8 (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

$$\{e_G\} = G_k \leq G_{k-1} \leq \ldots \leq G_1 \leq G_0 = G$$

eine Subnormalteilerkette wie in Definition 18.5, so setzen wir

$$U_i := G_i \cap U \leq U.$$

Damit erhalten wir eine Kette

$$\{e_U\} = U_k \leq U_{k-1} \leq \ldots \leq U_1 \leq U_0 = U$$

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

$$\{e_G\} = G_k \leq G_{k-1} \leq \ldots \leq G_1 \leq G_0 = G$$

eine Subnormalteilerkette wie in Definition 18.5. Da N ein Normalteiler ist, erhalten wir durch Multiplikation mit N eine Kette

$$N = G_kN \leq G_{k-1}N \leq \ldots \leq G_1N \leq G_0N = G \tag{38}$$

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 (38)

$$\{e_{G/N}\} = G_kN/N \leq G_{k-1}N/N \leq \ldots \leq G_1N/N \leq G_0N/N = G/N$$

eine Subnormalteilerkette wie in Definition 18.5 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 18.5 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 18.5 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 18.9 (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 18.6 nicht auflösbar ist, sind die Gruppen selbst nach Proposition 18.8 nicht auflösbar. □

Korollar 18.10 (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 14.15 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 18.8 leiten wir dann ab, daß auch G auflösbar ist. □

Beispiel 18.11 (Quaternionengruppe)
In Aufgabe 14.25 haben wir die Quaternionengruppe Q_8 der Ordnung 8 betrachtet. Diese ist als 2-Gruppe auflösbar.

C) Kompositionsreihen mit zyklischen Faktoren

In den Anwendungen, die wir im Blick haben, benötigen wir, daß sich eine Subnormalteilerkette wie in Definition 18.5 zu einer Subnormalteilerkette verfeinern läßt, in der die Faktoren alle Primzahlordnung haben und damit insbesondere zyklisch sind.

Satz 18.12 (Auflösbarkeit = Kompositionsreihen mit zyklischen Faktoren)
Eine endliche Gruppe G *ist genau auflösbar, wenn es eine Kette von Untergruppen*

$$\{e_G\} = G_k < G_{k-1} < \ldots < G_1 < G_0 = G$$

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 Kompositionsreihe *von* G *genannt.*

Beweis: Da die Faktoren der obigen Kompositionsreihe als zyklische Gruppen abelsch sind, folgt aus der Existenz einer Kompositionsreihe mit zyklischen Faktoren die Auflösbarkeit von G.

Ist umgekehrt eine Subnormalteilerkette wie in Definition 18.5 mit abelschen Faktoren gegeben, so müssen wir zeigen, daß wir diese zu einer Kompositionsreihe verfeinern können. Beachte dabei, daß ein abelscher Faktor G_{i-1}/G_i, der nicht von Primzahlordnung ist, nach Proposition 18.2 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 Kompositionsreihe. □

Beispiel 18.13
Die auflösbare Gruppe $\mathbb{S}_4$ hat die Kompositionsreihe

$$\{\mathrm{id}\} < \langle (1\,2)(3\,4) \rangle < \mathbb{K}_4 < \mathbb{A}_4 < \mathbb{S}_4.$$

Korollar 18.14
Gruppen der Ordnung pq *mit* $p, q \in \mathbb{P}$ *sind auflösbar.*

Beweis: Ist $p = q$, so ist G nach Korollar 18.10 auflösbar.

Andernfalls können wir $p > q$ annehmen. Aus dem Dritten Sylowsatz 15.11 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 Kompositionsreihe mit zyklischen Faktoren ist. Also ist G auflösbar. □

Beispiel 18.15
Gruppen der Ordnung 6, 9, 10, 14, 21, 22, 25 und 26 sind auflösbar, ebenso eine Gruppe der Ordnung

$$528.907.979 = 22993 \cdot 23003.$$

Mit ähnlich einfachen Mitteln kann man zeigen, daß jede Gruppe von einer Ordnung echt kleiner als 60 auflösbar ist.

Bemerkung 18.16 (Satz von Burnside (1911) / Satz von Feit-Thompson (1963))

a. Der Satz von Burnside besagt, daß jede Gruppe, deren Ordnung 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.

Aufgaben

Aufgabe 18.17 (Charakteristische Untergruppen)
Sei G eine Gruppe mit Normalteiler $N \trianglelefteq G$ und $M \leq N$ eine Untergruppe von N. Zeige, wenn $\varphi(M) \subseteq M$ für alle Automorphismen $\varphi \in \mathrm{Aut}(N)$ von N gilt, dann ist M ein Normalteiler von G.

Aufgabe 18.18 (Kommutatorgruppen)
Es sei G eine Gruppe und für $g, h \in G$ bezeichne

$$[g, h] := g \cdot h \cdot g^{-1} \cdot h^{-1}$$

den *Kommutator* von g und h. Ferner definieren wir $G^{(0)} := G$ sowie rekursiv

$$G^{(n)} := [G^{(n-1)}, G^{(n-1)}] := \langle [g, h] \mid g, h \in G^{(n-1)} \rangle$$

für $n \geq 1$. Zeige, für alle $n \in \mathbb{N}$ ist $G^{(n)}$ ein Normalteiler von G.

Aufgabe 18.19 (Abgeleitete Reihe)
Sei G eine endliche Gruppe. Zeige, die folgenden Aussagen sind äquivalent:

a. G ist auflösbar.

b. Es gibt ein $n \in \mathbb{N}$ mit $G^{(n)} = \{e_G\}$.

c. Es gibt eine Kette

$$\{e_G\} = G_k \leq G_{k-1} \leq \ldots \leq G_1 \leq G_0 = G$$

von Normalteilern von G mit G_{i-1}/G_i abelsch für $i = 1, \ldots, k$.

Aufgabe 18.20
Zeige, ist G eine auflösbare Gruppe, dann besitzt G eine maximale Untergruppe, die ein Normalteiler ist, d.h. es gibt einen Normalteiler $N \trianglelefteq G$, so daß keine Untergruppe U von G mit $N \subsetneqq U \subsetneqq G$ gibt.

Aufgabe 18.21

Zeige, besitzt eine Gruppe G zwei abelsche Untergruppen U und V, so daß $\mathsf{G} = \mathsf{U} \cdot \mathsf{V}$ gilt, dann ist G auflösbar.

§ 19 Auflösbarkeit durch Radikale

In diesem Abschnitt wollen wir mit Hilfe des Hauptsatzes der Galoistheorie 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.

A) Auflösung polynomialer Gleichungen

Bemerkung 19.1 (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 einfache Operationen benötigt werden.

$\underline{n = 1}$**:** Dann ist $f = t - a_1$ und wir sind fertig.

$\underline{n = 2}$**:** Die Formel

$$\alpha = -\frac{a_1}{2} \pm \sqrt{\frac{a_1^2}{4} - a_0}$$

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

$$g = f\left(t - \frac{a_2}{3}\right) = t^3 + pt + q \tag{39}$$

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

$$\left(u^3 + v^3 + 3uv \cdot (u + v)\right) + p \cdot (u + v) + q = 0 \tag{40}$$

Wir wählen nun v so, daß

$$3uv = -p \tag{41}$$

gilt, d.h. $u \neq 0$ und

$$v = -\frac{p}{3u}. \tag{42}$$

Aus Gleichung (40) wird dann

$$0 \overset{(40),(41)}{=} u^3 + v^3 + q \overset{(42)}{=} u^3 + q - \frac{p^3}{27u^3}. \tag{43}$$

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

$$u^3 = -\frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}. \tag{44}$$

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 (43)

$$u^3 = -\frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$$

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 (44) 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 19.2 (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 (39) 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.

B) Radikalerweiterungen und Auflösbarkeit durch Radikale

Definition 19.3 (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 $k_i \in \mathbb{Z}_{\geq 2}$, $i = 1, \ldots, n$, d. h. L entsteht aus K durch sukzessive Adjunktion von Wurzeln.

b. Wir nennen eine Radikalerweiterung wie in a. *abelsch*, wenn die Körpererweiterung $K(\alpha_1, \ldots, \alpha_i)/K(\alpha_1, \ldots, \alpha_{i-1})$ für alle $i = 1, \ldots, m$ galoissch mit abelscher Galoisgruppe ist.

c. Ein Polynom $f \in K[t]$ heißt *durch Radikale auflösbar* über K, wenn es eine Radikalerweiterung in L/K gibt, so daß f über L in Linearfaktoren zerfällt.

Bemerkung 19.4 (Auflösbarkeit durch Radikale)

a. Die Frage am Ende von Bemerkung 19.1 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 19.1, daß f durch Radikale auflösbar ist.
Die Galoisgruppe des Zerfällungskörpers $ZFK_K(f)$ über K für ein solches Polynom ist isomorph zu einer Untergruppe der $\mathbb{S}_4$ und ist damit ebenfalls auflösbar. Wir werden in Satz 19.6 sehen, daß das kein Zufall ist.

c. Auch wenn ein Polynom $f \in K[t]$ durch Radikale auflösbar ist, wird der Zerfällungskörper $\mathrm{ZFK}_K(f)$ selbst in aller Regel keine Radikalerweiterung von K sein, wie Beispiel 19.5 zeigt.

d. Auch wenn die Nullstellen eines durch Radikale auflösbaren Polynoms alle reelle Zahlen sind, wie in Beispiel 19.5, kann man in aller Regel keine rein reelle Radikalerweiterung finden, die den Zerfällungskörper des Polynoms enthält. In Aufgabe 19.25 ist zu zeigen, daß dies für irreduzible Polynome vom Grad 3 in $\mathbb{Q}[t]$ nie der Fall ist.

e. Man kann in der Definition des Begriffs Radikalerweiterung die k_i minimal mit der Eigenschaft $\alpha_i^{k_i} \in K_{i-1}$ wählen und kann dabei erreichen, daß die k_i Primzahlen sind (siehe Aufgabe 19.21). Das bedeutet jedoch nicht, daß der Grad $|K_i : K_{i-1}|$ dann gleich der Primzahl k_i sein muß. Man denke z.B. an die primitive dritte Einheitswurzel ζ_3 für die $k = 3$ minimal mit $\zeta_3^k \in \mathbb{Q}$ ist, während

$$|\mathbb{Q}(\zeta_3) : \mathbb{Q}| = \det(t^2 + t + 1) = 2$$

gilt.

Beispiel 19.5 (Zerfällungskörper, der keine Radikalerweiterung ist)
Aus Aufgabe 11.12 wissen wir, daß die Galoisgruppe des Polynoms

$$f = t^3 - 3t + 1 \in \mathbb{Q}[t]$$

isomorph zur $\mathbb{A}_3$ ist, weil die Diskriminante

$$D(f) = -4 \cdot (-3)^3 - 27 \cdot 1^2 = 81 = 9^2$$

eine Quadratzahl in $\mathbb{Q}$ ist. Mithin ist der Grad

$$|\,\mathrm{ZFK}_{\mathbb{Q}}(f) : \mathbb{Q}| = |\mathbb{A}_3| = 3$$

eine Primzahl und die Körpererweiterung $\mathrm{ZFK}_{\mathbb{Q}}(f)/\mathbb{Q}$ hat keine echten Zwischenkörper. Wäre nun $\mathrm{ZFK}_{\mathbb{Q}}(f)$ eine Radikalerweiterung, so müßte

$$\mathrm{ZFK}_{\mathbb{Q}}(f) = \mathbb{Q}(\alpha)$$

für ein $\alpha \in \mathbb{C} \setminus \mathbb{Q}$ mit $\alpha^3 \in \mathbb{Q}$ gelten. Da $\mathrm{ZFK}_{\mathbb{Q}}(f)/\mathbb{Q}$ galoissch ist, müßten dann alle drei Nullstellen des Minimalpolynoms

$$\mu_\alpha = t^3 - \alpha^3 = (t - \alpha) \cdot (t - \zeta_3 \cdot \alpha) \cdot (t - \zeta_3^2 \cdot \alpha)$$

in $\mathrm{ZFK}_{\mathbb{Q}}(f)$ liegen, woraus unmittelbar

$$\zeta_3 = \frac{\zeta_3 \cdot \alpha}{\alpha} \in \mathrm{ZFK}_{\mathbb{Q}}(f)$$

folgen würde. Dann hätte aber $\mathrm{ZFK}_{\mathbb{Q}}(f)/\mathbb{Q}$ den Zwischenkörper $\mathbb{Q}(\zeta_3)$ vom Grad 2, was nicht sein kann.

Die drei Nullstellen von f sind übrigens reelle Zahlen. Um dies zu sehen, schauen wir uns einige Werte von f an:

x	-2	0	1	2
$f(x)$	-1	1	-1	3

Aus dem Zwischenwertsatz folgt dann, daß f in $\mathbb{R}$ drei Nullstellen besitzt. Mit Hilfe der Formeln von Cardano können wir die Nullstellen von f auch bestimmen als

$$\alpha_j = \zeta_3^j \cdot \sqrt[3]{\frac{-1+i\cdot\sqrt{3}}{2}} + \zeta_3^{-j} \cdot \sqrt[3]{\frac{-1-i\cdot\sqrt{3}}{2}}$$

für $j = 0, 1, 2$. Mithin ist der Zerfällungskörper von f über $\mathbb{Q}$ in der Radikalerweiterung

$$\mathbb{Q}\left(\zeta_3, \sqrt{-3}, \sqrt[3]{\frac{-1+i\cdot\sqrt{3}}{2}}\right)/\mathbb{Q}$$

enthalten. Obwohl alle Nullstellen von f reell sind, ist diese Radikalerweiterung nicht rein reell.

Man sieht aber leicht, daß es sich um eine abelsche Radikalerweiterung handelt. Dazu betrachten wir die Kette

$$\mathbb{Q} \leq \mathbb{Q}(\zeta_3) \leq \mathbb{Q}\big(\zeta_3, \sqrt{-3}\big) \leq \mathbb{Q}\left(\zeta_3, \sqrt{-3}, \sqrt[3]{\frac{-1+i\cdot\sqrt{3}}{2}}\right)$$

von Zwischenkörpern. Die erste Erweiterung in der Kette ist als Kreisteilungskörpererweiterung galoissch mit abelscher Galoisgruppe; die zweite Erweiterung hat Grad 2 und ist somit galoissch mit zyklischer Galoisgruppe $\mathbb{Z}_2$; für die dritte Körpererweiterung werden wir schließlich Lemma 19.9 zeigen, daß auch sie galoissch mit zyklischer Galoisgruppe ist.

Für die Klärung der Frage in Bemerkung 19.4 a. ist der folgende Satz von zentraler Bedeutung, der zudem erläutert, weshalb auflösbare Gruppen auflösbar heißen.

Satz 19.6 (Auflösbarkeit durch Radikale)
Für ein Polynom $f \in K[t]$ *mit* $\operatorname{char}(K) = 0$ *sind die folgenden Aussagen gleichwertig:*

a. f *ist über* K *durch Radikale auflösbar.*

b. Die Galoisgruppe $\operatorname{Gal}(\mathrm{ZFK}_K(f)/K)$ *ist auflösbar.*

Bemerkung 19.7 (Gleichungen vom Grad höchstens 4 sind auflösbar.)
Satz 19.6 ist ein zu Bemerkung 19.1 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 11.1) auflösbar ist (siehe Beispiel 18.6 und Proposition 18.8).

Beispiel 19.8 (Das Minimalpolynom von $\zeta_{11} + \zeta_{11}^{-1}$ ist durch Radikale auflösbar.)
Das Polynom

$$f = t^5 + t^4 - 4 \cdot t^3 - 3 \cdot t^2 + 3 \cdot t + 1 \in \mathbb{Q}[t]$$

aus Aufgabe 4.38 ist das Minimalpolynom von $\alpha = \zeta_{11} + \zeta_{11}^{-1}$. Mithin ist $\mathbb{Q}(\alpha)$ ein Zwischenkörper von $\mathbb{Q}(\zeta_{11})/\mathbb{Q}$ vom Grad

$$|\mathbb{Q}(\alpha) : \mathbb{Q}| = \deg(f) = 5.$$

Da die Galoisgruppe

$$\mathrm{Gal}\,(\mathbb{Q}(\zeta_{11})/\mathbb{Q}) \cong \mathbb{Z}_{11}^* \cong \mathbb{Z}_{10}$$

zyklisch ist, ist jede Untergruppe ein Normalteiler und somit ist mit dem Hauptsatz der Galoistheorie insbesondere die Körpererweiterung $\mathbb{Q}(\alpha)/\mathbb{Q}$ galoissch. Dann ist aber $\mathrm{Gal}\,(\mathbb{Q}(\alpha)/\mathbb{Q})$ als Faktorgruppe einer zyklischen Gruppe selbst zyklisch, und wegen

$$|\,\mathrm{Gal}\,(\mathbb{Q}(\alpha)/\mathbb{Q})\,| = |\mathbb{Q}(\alpha) : \mathbb{Q}| = 5$$

ist sie isomorph zu $\mathbb{Z}_5$. Insbesondere ist die Gruppe dann aber auflösbar und somit ist f auflösbar durch Radikale. Das allein hilft uns aber leider nicht dabei, die Nullstellen von f als Radikalausdrücke zu bestimmen.

Für den Beweis des Satzes benötigen wir drei Hilfsaussagen.

C) Vorbereitung des Beweises – 1) Reine Körpererweiterungen

Lemma 19.9 (Reine Körpererweiterungen: 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: Für den Beweis beachten wir, daß die primitive n-te Einheitswurzel ζ_n im Körper K enthalten ist.

a. Das Polynom $f = t^n - \alpha^n \in K[t]$ faktorisiert als

$$f = \left(t - \zeta_n^0 \alpha\right) \cdot \left(t - \zeta_n^1 \alpha\right) \cdot \ldots \cdot \left(t - \zeta_n^{n-1} \alpha\right).$$

Da mit ζ_n auch die Potenzen von ζ_n in K und damit in L liegen, zerfällt f über L und

$$L = K(\alpha) = K\left(\alpha, \zeta_n\alpha, \ldots, \zeta_n^{n-1}\alpha\right) = \mathrm{ZFK}_K(f)$$

ist der Zerfällungskörper von f über K. Da f wegen $\mathrm{char}(K) = 0$ auch separabel ist, ist L/K nach Satz 11.6 galoissch.

Nach Proposition 11.1 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] oder Korollar 17.6).

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

$$t^n - 1 = (t - \zeta_n^0) \cdot (t - \zeta_n^1) \cdot \ldots \cdot (t - \zeta_n^{n-1}) \in K[t]$$

ist. Dieses zerfällt über K in paarweise verschiedene Linearfaktoren, so daß σ als K-lineare Abbildung diagonalisierbar ist (siehe [Mar11, Satz 33.21]) und alle Eigenwerte von σ n-te Einheitswurzeln sind. Wäre 1 der einzige Eigenwert von σ, so wäre σ als diagonalisierbarer Endomorphismus die Identität, im Widerspruch dazu, daß σ die Ordnung n hat. Also hat σ eine n-te Einheitswurzel $1 \neq \zeta \in K$ als Eigenwert.
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

$$\alpha^n \in \mathrm{Fix}\,(L, \mathrm{Gal}\,(L/K)) = K,$$

wobei wir für die letzte Gleichheit ausnutzen, daß L/K galoissch ist (siehe Korollar 12.7).
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 zum Eigenvektor α wäre. Also gilt

$$|K(\alpha) : K| = n = |L : K|,$$

woraus die Gleichheit $L = K(\alpha)$ folgt.

□

Bemerkung 19.10
Die Bedingung n prim in Teil b. von Lemma 19.9 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 (siehe Aufgabe 19.22 und Aufgabe 19.23).

Beispiel 19.11 (Der Zerfällungskörper von $t^{15} - 2$)
In Beispiel 16.10 haben wir die Körpererweiterung L/K betrachtet mit $K = \mathbb{Q}(\zeta_{15})$ und $L = \mathrm{ZFK}_K(t^{15} - 2) = K(\alpha)$ sowie $\alpha = \sqrt[15]{2}$. Wir haben dort die Isomorphie $\mathrm{Gal}\,(L/K) \cong \mathbb{Z}_{15}$ gezeigt.

D) Vorbereitung des Beweises – 2) abelsche Radikalerweiterungen

Eine unmittelbar Folgerung aus Lemma 19.9 ist die Existenz abelscher Radikalerweiterungen für Zerfällungskörper durch Radikale auflösbarer Polynome.

Korollar 19.12 (Existenz abelscher Radikalerweiterungen)
Ist L Zwischenkörper einer Radikalerweiterung mit $\mathrm{char}(L) = 0$, dann ist L auch Zwischenkörper einer abelschen Radikalerweiterung.

Beweis: Nach Voraussetzung 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 $i = 1, \ldots, m$. Für $i = 0, \ldots, m$ setzen wir nun

$$K_i = K(\alpha_1, \ldots, \alpha_i)$$

und schließlich

$$n = k_1 \cdot \ldots \cdot k_m.$$

Dann betrachten wir die Körpererweiterung $M(\zeta_n)$, wobei

$$\zeta_n = e^{\frac{2\pi i}{n}} \in \mathbb{C}$$

eine primitive n-te Einheitswurzel ist. Damit erhalten wir eine Kette von Körpererweiterungen

$$K = K_0 \leq K_0(\zeta_n) \leq K_1(\zeta_n) \leq \ldots \leq K_m(\zeta_n) = M(\zeta_n)$$

mit

$$K_i(\zeta_n) = K(\zeta_n, \alpha_1, \ldots, \alpha_i) = K_{i-1}(\zeta_n)(\alpha_i)$$

sowie

$$\alpha_i^{k_i} \in K_{i-1} \subseteq K_{i-1}(\zeta_n).$$

Da für $i = 1, \ldots, m$ mit ζ_n auch die primitive k_i-te Einheitswurzel

$$\zeta_{k_i} = \zeta_n^{\frac{n}{k_i}} \in K_0(\zeta_n) \subseteq K_{i-1}(\zeta_n)$$

in $K_{i-1}(\zeta_n)$ enthalten ist, können wir Lemma 19.9 auf die Körpererweiterung $K_i(\zeta_n)/K_{i-1}(\zeta_n)$ anwenden und erhalten, daß diese galoissch mit zyklischer und mithin abelscher Galoisgruppe ist. Zudem ist auch $K_0(\zeta_n)/K_0$ nach Bemerkung 13.16 galoissch mit abelscher Galoisgruppe und wegen $\zeta_n^n = 1 \in K_0$ ist dann $M(\zeta_n)/K$ eine abelsche Radikalerweiterung, die L als Zwischenkörper enthält. □

E) Vorbereitung des Beweises – 3) der Translationssatz

Lemma 19.13 (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 2 veranschaulicht die Lage der Körper zueinander.

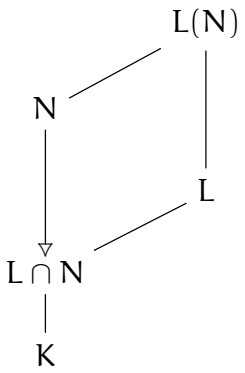

ABBILDUNG 2. Körperdiagramm im Translationssatz

Beweis: Da N/K galoissch ist, ist $N/L \cap N$ nach dem Hauptsatz der Galoistheorie 12.9 ebenfalls galoissch und es gibt nach Satz 11.6 ein separables Polynom

$$f = (t - \alpha_1) \cdot \ldots \cdot (t - \alpha_n) \in K[t],$$

so daß

$$N = ZFK_K(f) = K(\alpha_1, \ldots, \alpha_n)$$

der Zerfällungskörper von f über K ist. Dann ist aber

$$L(N) = L(\alpha_1, \ldots, \alpha_n) = ZFK_L(f)$$

der Zerfällungskörper von f über L, und nach Satz 11.6 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 9.3

$$\sigma(N) = N,$$

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 12.9 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. □

F) Der Beweis der Auflösbarkeit durch Radikale

Beweis von Satz 19.6: Für den Beweis sei $L = ZFK_K(f)$.

"$\Longrightarrow$": Wenn f durch Radikale auflösbar ist, so ist L wegen Korollar 19.12 Zwischenkörper einer abelschen Radikalerweiterung

$$M = K(\alpha_1, \ldots, \alpha_m)$$

von K mit

$$\alpha_i^{k_i} \in K(\alpha_1, \ldots, \alpha_{i-1})$$

für $i = 1, \ldots, m$. 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 $\mathrm{Gal}\,(L/K) = \{\mathrm{id}_K\}$.

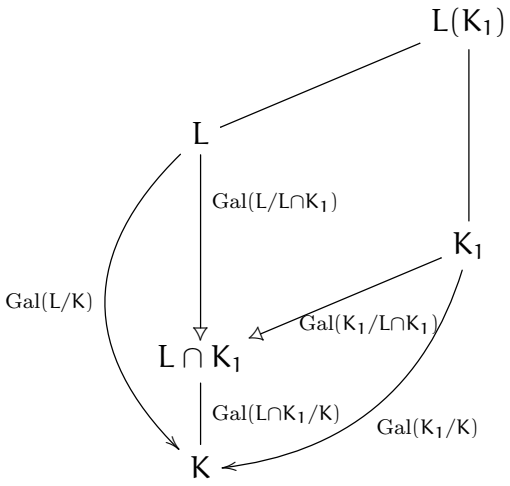

Abbildung 3. Körperdiagramm mit Galoisgruppen, Beweis von 19.6

Ist $m > 0$, so hat der Körper (siehe auch Abbildung 3)

$$L(K_1) = ZFK_{K_1}(f)$$

als Zwischenkörper der abelschen Radikalerweiterung M/K_1 nach Induktion eine auflösbare Galoisgruppe

$$\mathrm{Gal}\,(L(K_1)/K_1) \overset{19.13}{\cong} \mathrm{Gal}\,(L/L \cap K_1)\,,$$

so daß wegen des Translationssatzes 19.13 $\mathrm{Gal}\,(L/L \cap K_1)$ auflösbar ist.

Da die Radikalerweiterung M/K abelsch ist, ist insbesondere K_1/K galoissch und $\mathrm{Gal}\,(K_1/K)$ ist abelsch. 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 abelschen Gruppe ebenfalls abelsch ist und daß $L \cap K_1/K$ galoissch ist. Dann ist wegen des Hauptsatzes der Galoistheorie 12.9 aber auch

$$\operatorname{Gal}(L/K) \,/\, \operatorname{Gal}(L/L \cap K_1) \cong \operatorname{Gal}(L \cap K_1/K),$$

und diese Gruppe ist somit ebenfalls abelsch und damit auflösbar.

Wir haben also gezeigt, daß die Gruppe $\operatorname{Gal}(L/K)$ einen Normalteiler besitzt, der auflösbar ist und dessen Faktorgruppe auflösbar ist. Nach Proposition 18.8 ist dann die Gruppe $\operatorname{Gal}(L/K)$ aber auch selbst auflösbar.

"$\Longleftarrow$": Für die umgekehrte Richtung setzen wir voraus, daß $\operatorname{Gal}(L/K)$ auflösbar ist, setzen $n = |L : K|$ und unterscheiden zwei Fälle.

1. Fall: $\zeta_n \in K$**:** Da $\operatorname{Gal}(L/K)$ auflösbar ist, gibt es nach Satz 18.12 eine Subnormalteilerkette

$$\{e_G\} = G_m \trianglelefteq G_{m-1} \trianglelefteq \ldots \trianglelefteq G_0 = \operatorname{Gal}(L/K),$$

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

$$K_i := \operatorname{Fix}(L, G_i) \leq L$$

von L/K und erhalten wegen Korollar 12.7

$$K = K_0 \leq K_1 \leq \ldots \leq K_m = L.$$

Aus dem Hauptsatz der Galoistheorie 12.9 wissen wir, daß L/K_{i-1} galoissch ist mit Galoisgruppe

$$\operatorname{Gal}(L/K_{i-1}) = \operatorname{Gal}(L/\operatorname{Fix}(L, G_{i-1})) = G_{i-1}.$$

Da $G_i = \operatorname{Gal}(L/K_i)$ ein Normalteiler dieser Gruppe ist, ist mithin

$$K_i = \operatorname{Fix}(L, G_i)$$

galoissch über K_{i-1} mit zyklischer Galoisgruppe

$$\operatorname{Gal}(K_i/K_{i-1}) \cong \operatorname{Gal}(L/K_{i-1}) \,/\, \operatorname{Gal}(L/K_i) = G_{i-1}/G_i.$$

Die Primzahl $p_i = |G_{i-1}/G_i|$ ist nach dem Satz von Lagrange ein Teiler von

$$n = |L : K| = |\operatorname{Gal}(L/K)| = |G_0|,$$

so daß mit ζ_n auch $\zeta_{p_i} = \zeta_n^{\frac{n}{p_i}} \in K$ in K liegt, und aus Lemma 19.9 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 4. Da L/K

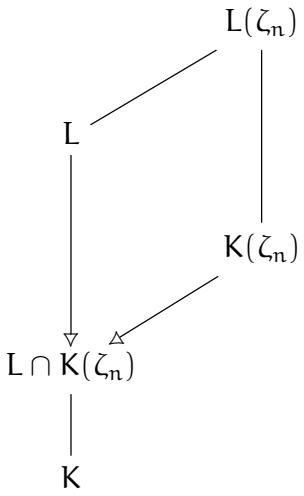

ABBILDUNG 4. Körperdiagramm zu L/K und $L(\zeta_n)/K(\zeta_n)$

galoissch ist, können wir den Translationssatz 19.13 anwenden und erhalten, daß $L(\zeta_n)/K(\zeta_n)$ und $L/L \cap K(\zeta_n)$ galoissch sind mit Galoisgruppe

$$\operatorname{Gal}(L(\zeta_n)/K(\zeta_n)) \cong \operatorname{Gal}(L/L \cap K(\zeta_n)).$$

Insbesondere ist dann aber

$$\begin{aligned} k :=& |L(\zeta_n) : K(\zeta_n)| = |\operatorname{Gal}(L(\zeta_n)/K(\zeta_n))| \\ =& |\operatorname{Gal}(L/L \cap K(\zeta_n))| = |L : L \cap K(\zeta_n)| \;\Big|\; |L : K| = n \end{aligned}$$

ein Teiler von n und somit gilt

$$\zeta_k = \zeta_n^{\frac{n}{k}} \in K(\zeta_n). \tag{45}$$

Also erfüllt $L(\zeta_n)/K(\zeta_n)$ die Voraussetzungen des 1. Falls.
Da $\operatorname{Gal}(L/K)$ auflösbar, ist nach Proposition 18.8 auch die Untergruppe

$$\operatorname{Gal}(L/L \cap K(\zeta_n)) \leq \operatorname{Gal}(L/K)$$

auflösbar und nach dem Translationssatz 19.13 ist dann auch

$$\operatorname{Gal}(L(\zeta_n)/K(\zeta_n)) \cong \operatorname{Gal}(L/L \cap K(\zeta_n))$$

auflösbar. Mit Hilfe des 1. Falls erhalten wir dann, daß $L(\zeta_n) = \mathrm{ZFK}_{K(\zeta_n)}(f)$ 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 19.14 (Zwischenkörperketten bei auflösbarer Galoisgruppe)
Aus dem Beweis von Satz 19.6 folgt im Fall $\zeta_n \in K$ für $n = |\mathrm{ZFK}_K(f) : K|$ und $\mathrm{Gal}(\mathrm{ZFK}_K(f)/K)$ auflösbar, daß der Zerfällungskörper $\mathrm{ZFK}_K(f)$ selbst eine Radikalerweiterung von K ist und daß es eine Zwischenkörperkette

$$K = K_0 \leq K_1 \leq \ldots \leq K_m = \mathrm{ZFK}_K(f)$$

gibt, so daß $K_i = K_{i-1}(\alpha_i)$ mit $\alpha_i^{p_i} \in K_{i-1}$ eine einfache galoissche Radikalerweiterung vom Primzahlgrad

$$|K_i : K_{i-1}| = p_i$$

ist. Wenn $\zeta_n \notin K$ nicht in K enthalten ist, dann ist der Zerfällungskörper nur in einer Radikalerweiterung M/K enthalten, für die es eine Zwischenkörperkette wie oben gibt, wobei man $M = \mathrm{ZFK}_{K(\zeta_n)}(f)$ nehmen kann (siehe auch Bemerkung 19.4).

G) Der Satz von Abel-Ruffini

Wir wollen den Abschnitt mit dem Satz von Abel-Ruffini abschließen, der zeigt, daß auch nicht-auflösbare Gruppen als Galoisgruppen von galoisschen Körpererweiterungen auftreten können. Damit beantworten wir dann insbesondere die Frage, wie es um die Existenz von allgemeinen Lösungsformeln für Polynome vom Grad 5 oder mehr bestellt ist.

Proposition 19.15 (Erzeuger für $\mathbb{S}_p$)
Sind $\tau \in \mathbb{S}_p$ eine Transposition und $\pi \in \mathbb{S}_p$ ein p-Zykel mit $p \in \mathbb{P}$, so gilt

$$\langle \tau, \pi \rangle = \mathbb{S}_p.$$

Beweis: Wir können ohne Einschränkung $\tau = (1\ 2)$ annehmen.

Zunächst betrachten wir den Fall

$$\pi = (1\ 2\ 3\ \ldots\ p).$$

Dann gilt

$$(i\quad i+1) = (\pi^{i-1}(1)\ \ \pi^{i-1}(2)) = \pi^{i-1} \circ \tau \circ \pi^{-(i-1)} \in \langle \tau, \pi \rangle$$

für alle $i = 1, \ldots, p-1$, und da $\mathbb{S}_p$ von diesen Transpositionen erzeugt wird (siehe [Mar08a, Kor. 3.14]), folgt die Behauptung.

Sei nun π ein beliebiger p-Zyklus. Da p eine Primzahl ist, sind auch die Potenzen π^i für $i = 1, \ldots, p-1$ von π wieder p-Zykel und es gibt ein i mit $\pi^i(1) = 2$, so daß

$$\pi^i = (1\ 2\ a_3\ \ldots\ a_p).$$

Für

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & p \\ 1 & 2 & a_3 & a_4 & \dots & a_p \end{pmatrix} \in \mathbb{S}_p$$

gilt

$$\sigma^{-1} \circ \tau \circ \sigma = \tau$$

und

$$\sigma^{-1} \circ \pi^i \circ \sigma = (1\,2\,3\,\dots\,p),$$

so daß wir für $U = \langle \pi, \tau \rangle$

$$\mathbb{S}_p = \langle (1\,2\,3\,\dots\,p), \tau \rangle \subseteq \sigma^{-1} \circ U \circ \sigma = U^{\sigma^{-1}}$$

und damit

$$\mathbb{S}_p = \mathbb{S}_p^\sigma \subseteq U \subseteq \mathbb{S}_p$$

erhalten. □

Satz 19.16 (Abel-Ruffini)
Ist $f \in \mathbb{Q}[t]$ *ein irreduzibles Polynom von ungeradem Primzahlgrad* p *mit genau zwei nicht-reellen Nullstellen und* $L = \mathrm{ZFK}_{\mathbb{Q}}(f)$*, so gilt*

$$\mathrm{Gal}\,(L/\mathbb{Q}) \cong \mathbb{S}_p.$$

Beweis: Ist $\lambda \in \mathbb{C}$ eine Nullstelle von f, so gilt

$$f\big(\overline{\lambda}\big) = \overline{f(\lambda)} = \overline{0} = 0.$$

Also permutiert die komplexe Konjugation die Nullstellen von f, woraus zunächst

$$\bar{\cdot} \in \mathrm{Gal}\,(\mathrm{ZFK}_{\mathbb{Q}}(f)/\mathbb{Q})$$

folgt, und da f genau $p-2$ reelle Nullstellen hat folgt zudem, daß die komplexe Konjugation eine Transposition ist.

Außerdem gilt für eine Nullstelle α von f

$$p = |\mathbb{Q}(\alpha) : \mathbb{Q}| \;\Big|\; |\,\mathrm{ZFK}_{\mathbb{Q}}(f) : \mathbb{Q}| = |\,\mathrm{Gal}\,(\mathrm{ZFK}_{\mathbb{Q}}(f)/\mathbb{Q})\,|,$$

so daß $\mathrm{Gal}\,(\mathrm{ZFK}_{\mathbb{Q}}(f)/\mathbb{Q})$ auch einen p-Zykel enthält. Nach Teil a. gilt dann

$$\mathrm{Gal}\,(\mathrm{ZFK}_{\mathbb{Q}}(f)/\mathbb{Q}) \cong \mathbb{S}_p.$$

□

Korollar 19.17 (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 3.1 folgt, daß f irreduzibel über $\mathbb{Z}$ und damit auch über $\mathbb{Q}$ ist (siehe Satz 3.3). 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. Aus dem Satz von Abel-Ruffini 19.16 folgt dann

$$\mathrm{Gal}\,(L/\mathbb{Q}) \cong \mathbb{S}_5.$$

Mithin ist die Galoisgruppe nach Korollar 18.9 nicht auflösbar, und wegen Satz 19.6 ist dann f nicht durch Radikale auflösbar. □

Bemerkung 19.18 (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. Korollar 19.17 zeigt, weshalb. Eine solche allgemeine Formel kann es nicht geben, auch wenn für ausgewählte Polynome (wie in Beispiel 19.8) die Nullstellen durch Radikalausdrücke darstellbar sind.

Aufgaben

Aufgabe 19.19
Zeige, ist $K = \mathbb{Q}(\zeta_8)$ der achte Kreisteilungskörper über $\mathbb{Q}$ und $L = \mathrm{ZFK}_K(t^8 - 2)$ der Zerfällungskörper von $t^8 - 2$ über K, dann gilt $\mathrm{Gal}\,(L/K) \cong \mathbb{Z}_4$.

Aufgabe 19.20
Es sei $L = \mathrm{ZFK}_{\mathbb{Q}}(t^3 - 3t + 1)$.

a. Berechne die Nullstellen von f mit der Formel von Cardano und zeige, daß alle Nullstellen reell sind.

b. Finde einen Erweiterungskörper M von L, so daß $M/\mathbb{Q}$ eine Radikalerweiterung ist.

c. Zeige, $L/\mathbb{Q}$ ist galoissch und $|\,\mathrm{Gal}\,(L/\mathbb{Q})\,| = 3$.

d. Zeige, $L/\mathbb{Q}$ ist keine Radikalerweiterung.

Aufgabe 19.21 (Zwischenkörperkette einer Radikalerweiterung)
Zeige, ist L/K eine Radikalerweiterung, dann gibt es eine Kette von Zwischenkörpern

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

mit

$$K_i = K_{i-1}(\alpha_i)$$

und $p_i \in \mathbb{P}$ ist minimal, so daß

$$\alpha_i^{p_i} \in K_{i-1},$$

für $i = 1, \ldots, n$.

Aufgabe 19.22 (Minimalpolynom einer reinen Körpererweiterung)
Es sei K ein Körper mit $\operatorname{char}(K) = 0$, $\zeta_n = e^{\frac{2\pi i}{n}} \in K$ und $0 \neq \alpha \in \overline{K}$ mit $\alpha^n \in K$.

a. Zeige, $d = |\operatorname{Gal}(K(\alpha)/K)|$ ist ein Teiler von n und minimal mit $\alpha^d \in K$.

b. Zeige, $t^d - \alpha^d \in K[t]$ ist irreduzibel und das Minimalpolynom von α über K.

Aufgabe 19.23 (Reine Körpererweiterungen, Verallgemeinerung von Lemma 19.9)
Zeige, ist L/K eine galoissche Körpererweiterung in Charakteristik 0 mit zyklischer Galoisgruppe $\operatorname{Gal}(L/K) \cong \mathbb{Z}_n$ und ist $\zeta_n \in K$, dann gilt $L = K(\alpha)$ mit $\alpha^n \in K$.

Aufgabe 19.24
Sei K ein Körper mit $\operatorname{char}(K) = 0$, $p \in \mathbb{P}$ eine Primzahl und $\alpha \in K$, so daß $t^p - \alpha$ keine Nullstelle in K hat. Zeige, dann ist $t^p - \alpha$ irreduzibel in K.

Aufgabe 19.25 (Radikalerweiterung bei Polynomen mit rein reellen Nullstellen)
Zeige, ist $f \in \mathbb{Q}[t]$ ein irreduzibles Polynom vom Grad 3 mit drei reellen Nullstellen, dann ist der Zerfällungskörper von f über $\mathbb{Q}$ trotzdem in keiner rein reellen Radikalerweiterung enthalten.

Literaturverzeichnis

[DGPS19] Wolfram Decker, Gert-Martin Greuel, Gerhard Pfister, and Hans Schönemann, SINGULAR *4-1-2 — A computer algebra system for polynomial computations*, Tech. report, Centre for Computer Algebra, University of Kaiserslautern, 2019, `http://www.singular.uni-kl.de`.

[DH92] Klaus Doerk and Trevor Hawkes, *Finite soluble groups*, De Gruyter Expositions in Mathematics, no. 4, De Gruyter, 1992.

[Euk91] Euklid, *Die Elemente*, 8 ed., Bibliothek klassischer Texte, Wissenschaftliche Buchgesellschaft, 1991.

[Fis08] Gerd Fischer, *Lehrbuch der Algebra*, Vieweg, 2008.

[FT63] Walter Feit and John G. Thompson, *Solvability of groups of odd order*, Pacific Journal of Mathematics **13** (1963), 755–1029.

[Gar86] David John Haldane 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.

[Hum96] John F. Humphreys, *A course in group theory*, OUP, Oxford, 1996.

[Kur77] Hans Kurzweil, *Endliche Gruppen*, Springer Hochschultext, Springer, 1977.

[Lei96] Felix Leinen, *Algebra I & II*, Vorlesungsausarbeitung, Johannes Gutenberg-Universität Mainz, 1995/96.

[Lew91] Jonathan Lewin, *A simple proof of Zorn's lemma*, Amer. Math. Monthly **98** (1991), no. 4, 353–354.

[Mal11] Gunter Malle, *Einführung in die Algebra*, Vorlesungsausarbeitung, 2011.

[Mar08a] Thomas Markwig, *Algebraische Strukturen*, Vorlesungsskript, TU Kaiserslautern, 2008.

[Mar08b] ———, *Elementare Zahlentheorie*, Vorlesungsskript, TU Kaiserslautern, 2008.

[Mar11] ———, *Grundlagen der Mathematik*, Vorlesungsskript, TU Kaiserslautern, 2011.

[Moo82] Gregory H. Moore, *Zermelo's axiom of choice: Its origins, development and influence*, Studies in the History of Mathematics and Physical Sciences, no. 8, Springer, 1982.

[PS10] Gerhard Pfister and Stefan Steidel, *Einführung in die Algebra*, Vorlesungsskript WS 2009/10, TU Kaiserslautern, 2010.

[SS78] Günter Scheja and Uwe Storch, *Lehrbuch der Algebra*, Mathematische Leitfäden, vol. I, Teubner, 1978.

[SS81] ———, *Lehrbuch der Algebra*, Mathematische Leitfäden, vol. III, Teubner, 1981.

[SS88] ———, *Lehrbuch der Algebra*, Mathematische Leitfäden, vol. II, Teubner, 1988.

[Sze50] Tibor Szele, *On Zorn's lemma*, Publicationes Mathematicae Debreccen **1** (1949/50), 254–57.