Vorlesung Algebra I (neue Fassung)

Dirk Kussin

Institut für Mathematik, Uni Paderborn
Email address: dirk@math.uni-paderborn.de

Institut für Mathematik, TU Berlin
Email address: kussin@math.tu-berlin.de

Hinweis. Für Druckfehler wird keine Haftung übernommen.

Copyright © 2006 – 2025 by Dirk Kussin

Completely revised 2nd version 2021. Minor Update: Jan 22, 2025

Bisherige Verwendung in Vorlesungen des Autors:

- Uni Paderborn, Winter 2006/07 (Gruppen- und Ringtheorie) und Sommer 2007 (Körper- und Galoistheorie)
- TU Chemnitz, Sommer 2013 (komplett)
- Uni Stettin, Sommer 2015 (Körper- und Galoistheorie)
- Uni Münster, Sommer 2017 (Körper- und Galoistheorie)
- TU Berlin, Winter 2019/20 (komplett), Winter 2020/21
- TU Berlin, Winter 2021/22 (neue Fassung), Winter 2022/23, Winter 2023/24, Winter 2024/25

Gegenüber der früheren Fassung wird in dieser umgearbeiteten Version die Thematik des algebraischen Abschlusses eines Körper ganz an das (optionale) Ende verschoben. Bis dahin stehen endliche Körpererweiterung im Fokus, ohne auf mögliche Verallgemeinerungen auf beliebige algebraische Erweiterungen einzugehen. Diese Vorgehensweise in der Galoistheorie bis zum Hauptsatz (ohne algebraischen Abschluss, sowie ohne Satz vom primitiven Element) wurde durch Emil Artin und sein sehr einflussreiches Büchlein [1] popularisiert.

Änderung 9/2024: Die Definitionen von Links- und Rechtsnebenklassen getauscht. So stimmen sie jetzt überein z. B. mit denen in [9].

Inhaltsverzeichnis

KAPITEL I

Elementare Gruppentheorie

1. Der Gruppenbegriff

Aus der Linearen Algebra ist der Begriff einer Gruppe bekannt.

Definition 1.1

Eine Menge G mit einer Verknüpfung $\cdot\colon G \times G \to G$, $(x, y) \mapsto xy = x \cdot y$ heisst *Gruppe*, falls folgendes gilt:

(G1) die Verknüpfung ist assoziativ, d. h. $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ für alle $x, y, z \in G$;

(G2) es gibt ein neutrales Element e in G, d. h. für das gilt $x \cdot e = x = e \cdot x$ für alle $x \in G$;

(G3) zu jedem $x \in G$ gibt es ein inverses Element $y \in G$, d. h. für das gilt $x \cdot y = e = y \cdot x$.

Es ist leicht zu zeigen, dass es nur ein neutrales Element e geben kann, und dass ein inverses Element y zu x eindeutig bestimmt ist; man schreibt dann $y = x^{-1}$, und auch $e = e_G$, falls betont werden soll, dass es sich um das neutrale Element in G handelt.

Ist die Verknüpfung zusätzlich kommutativ, d. h. gilt $x \cdot y = y \cdot x$ für alle $x, y \in G$, so heisst die Gruppe G *abelsch*.

Der Gruppenbegriff ist zentral für die ganze Mathematik, nicht etwa nur von Bedeutung in der Algebra. Jedem mathematischen Objekt M (einer Menge, einem Vektorraum, einem topologischen Raum, einem geometrischen Objekt, einer Gruppe, einer geordneten Menge, etc.) kann man nämlich seine Symmetriegruppe $\mathbb{S}(M)$ zuordnen, gebildet aus allen die gegebene Struktur von M bewahrenden Isomorphismen $f\colon M \to M$. Je nach Kontext spricht man auch von der Automorphismengruppe $\mathrm{Aut}(M)$ von M.

Beispiele. (1) $\mathrm{GL}_n(K)$, die Menge der invertierbaren $n \times n$-Matrizen über dem Körper K.

(1') $\mathrm{Aut}_K(V)$, die Menge der K-linearen, bijektiven Abbildungen $f\colon V \to V$ des K-Vektorraums V in sich. (Automorphismengruppe von V.)

(2) $\mathbb{S}(M)$, die Menge der bijektiven Abbildungen $f\colon M \to M$ von der Menge M in sich. Speziell für $M = \{1, 2, \ldots, n\}$: die symmetrische Gruppe $\mathbb{S}_n = \mathbb{S}(M)$; dies ist die Menge der Permutationen der Zahlen $1, 2, \ldots, n$.

(3) $(\mathbb{Z}, +)$, die Menge der ganzen Zahlen mit der Addition als Verknüpfung. (Hier verwendet man eine *additive Schreibweise*: $x + y$ statt $x \cdot y = xy$, $-x$ statt x^{-1}, $x - y := x + (-y)$.) Das neutrale Element ist 0.

(4) Die Menge der komplexen Zahlen vom Betrag 1 bilden mit der Multiplikation in $\mathbb{C}$ eine Gruppe.

(5) Sei X ein topologischer Raum. Dann bildet die Menge der Homöomorphismen $f\colon X \to X$ von X auf sich (d. h. f ist stetig, bijektiv, und f^{-1} ist stetig) mit der Komposition von Abbildungen eine Gruppe. ("Symmetrie"- oder Automorphismengruppe von X.)

Die Anzahl der Elemente (bzw. die Kardinalität) einer Gruppe G heisst die *Ordnung* von G und bezeichnen wir mit $|G|$. Generell schreiben wir auch $|X|$ für die Kardinalität einer Menge X.

2. Untergruppen, Nebenklassenzerlegung

Definition 2.1

Eine Teilmenge U einer Gruppe G heisst *Untergruppe* von G (Schreibweise: $U < G$), falls gilt

(U1) $e_G \in U$
(U2) $U \cdot U \subseteq U$
(U3) $U^{-1} \subseteq U$.

Dabei ist $U \cdot U \stackrel{def}{=} \{u_1 u_2 \mid u_1,\, u_2 \in U\}$ und $U^{-1} \stackrel{def}{=} \{u^{-1} \mid u \in U\}$. Mit der von G induzierten Multiplikation

$$\cdot_U \colon U \times U \to U,\ (x, y) \mapsto x \cdot_G y$$

ist eine Untergruppe selbst eine Gruppe.

Beispiele. (a) Sei G eine Gruppe. Dann sind $\{e\}$ und G Untergruppen.
(b) Sei G eine Gruppe und $g \in G$ Dann ist

$$\langle g \rangle := \{g^n \mid n \in \mathbb{Z}\}$$

eine Untergruppe von G. Sie heisst die von g erzeugte (zyklische) Untergruppe.
(c) $\mathbb{A}_n$ (gerade Permutationen) ist Untergruppe von $\mathbb{S}_n$.
(d) $\mathrm{SL}_n(K) < \mathrm{GL}_n(K)$.

Definition 2.2

Eine Gruppe G heisst *zyklisch*, falls es ein $g \in G$ gibt mit $G = \langle g \rangle$.

Bemerkung. Jede zyklische Gruppe ist abelsch. Die Umkehrung gilt nicht.

Beispiele. (a) Die Permutation

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n-1 & n \\ 2 & 3 & \dots & n & 1 \end{pmatrix}$$

erzeugt eine zyklische Gruppe $\langle \sigma \rangle$, bestehend aus 1, σ, $\sigma^2, \dots, \sigma^{n-1}$, der Ordnung n.
(b) Sei $z_n = e^{2\pi i/n}$ betrachtet als Element von $(\mathbb{C}^\times, \cdot)$, wobei $\mathbb{C}^\times = \mathbb{C} \setminus \{0\}$. Dann besteht $U_n = \langle z_n \rangle$ aus den Elementen 1, z_n, ${z_n}^2, \dots, {z_n}^{n-1}$. Also $|U_n| = n$.
(c)* Jede endliche Untergruppe von $(\mathbb{C}^\times, \cdot)$ der Ordnung n stimmt mit U_n überein, ist also zyklisch.
(d)* Jede endliche Untergruppe der multiplikativen Gruppe $K^\times = K \setminus \{0\}$ eines Körpers K ist zyklisch.
(e) $(\mathbb{Z}, +)$ ist zyklisch (und unendlich).

Definition 2.3

Sei G eine Gruppe und U eine Untergruppe von G. Für $g \in G$ heisst

$$gU = \{gu \mid u \in U\}$$

die *Linksnebenklasse* von g nach U. Mit $G/U = \{gU \mid g \in G\}$ bezeichnen wir die Menge aller Linksnebenklassen von G nach U. Eine *Rechtsnebenklasse* ist analog definiert als Ug.

Lemma 2.4

Äquivalent sind:

(a) $gU = hU$
(b) $gU \cap hU \neq \emptyset$
(c) $h^{-1}g \in U$

Beweis. (Siehe Vorlesung.) ∎

Proposition 2.5

Sei U eine Untergruppe von G Dann ist

$$G = \coprod_{N \in G/U} N$$

eine disjunkte Zerlegung von G in Linksnebenklassen N, die alle zu U gleichmächtig sind.

Eine analoge Aussage gilt für Rechtsnebenklassen. Hierbei bezeichne $\coprod$ die disjunkte Vereinigung. Zwei Mengen M und N heissen gleichmächtig, wenn es eine bijektive Abbildung $f\colon M \to N$ gibt. Im Fall endlicher Mengen bedeutet dies, dass die Anzahlen der Elemente in M und in N übereinstimmen.

Beweis. Jedes $g \in G$ liegt in einer Nebenklasse, z. B. in gU. Verschiedene Nebenklassen sind nach Lemma 2.4 disjunkt. Dies zeigt den ersten Teil der Aussage. Für $g \in G$ ist die Abbildung

$$h\colon U \to gU,\ u \mapsto gu$$

bijektiv mit Umkehrabbildung $gU \to U$, $y \mapsto g^{-1}y$; daher sind U und gU gleichmächtig. ∎

Satz 2.6 (*Lagrange*)

Sei G eine endliche Gruppe und U eine Untergruppe. Dann gilt

$$|G| = |U| \cdot |G/U|.$$

Insbesondere sind daher die Ordnung $|U|$ von U und der Index $[G : U] \stackrel{def}{=} |G/U|$ *von G nach U Teiler der Ordnung $|G|$ von G.*

Folgerung 2.7

Jede Gruppe G von Primzahlordnung p ist zyklisch und hat $\{e\}$ und G als einzige Untergruppen.

Beweis. Ist U eine Untergruppe von G, so ist $|U|$ ein Teiler von p, also $|U| = 1$ oder $|U| = p$. Dies zeigt $U = \{e\}$ oder $U = G$. Wähle nun $e \neq g \in G$. Es folgt $\langle g\rangle \neq \{e\}$, also $\langle g\rangle = G$. ∎

Folgerung 2.8 (*"Kleiner Fermat"*)

Ist G eine Gruppe der Ordnung n und $g \in G$, so gilt $g^n = e$.

Beweis. Die von g erzeugte zyklische Untergruppe $U = \langle g\rangle$ hat als Ordnung einen Teiler m von n. Es reicht also folgende Aussage zu zeigen:

In einer zyklischen Gruppe $U = \langle g\rangle$ der Ordnung m gilt $g^m = e$; ferner ist m die kleinste natürliche Zahl ≥ 1 mit $g^m = e$.

Beweis hierfür: Man betrachte die Potenzen g, g^2, $g^3, \ldots$ von g. Da G, also insbesondere $\langle g\rangle$, nur aus endlich vielen Elementen besteht, muss es $j > i \geq 1$ geben mit $g^j = g^i$. Es gilt mit $r := j - i \geq 1$ dann $g^r = g^j(g^i)^{-1} = e$. Sei r die

kleinste natürliche Zahl ≥ 1 mit $g^r = e$. — Diese heisst auch die *Ordnung* von g; Schreibweise $r = \mathrm{ord}(g)$. — Dann sind die Elemente

$$e,\ g,\ g^2, \ldots,\ g^{r-1}$$

paarweise verschieden: sonst gilt für $0 \leq j < k \leq r-1$ $g^j = g^k$, also $g^{k-j} = e$, im Widerspruch zur Wahl von r. Ferner ist $\{e, g, \ldots, g^{r-1}\}$ gegen Multiplikation und Inverse abgeschlossen (beachte $g^r = e$, $g^{-1} = g^{r-1}$), also (leichte Übung) eine Untergruppe von G, die mit $\langle g \rangle$ übereinstimmt. Es folgt $|\langle g \rangle| = r$. ∎

Proposition und Definition 2.9

Sind G und H Gruppen, so ist $G \times H$ vermöge

$$(g, h) \cdot (g', h') = (gg', hh')$$

wieder eine Gruppe. $G \times H$ heisst direktes Produkt *von G und H.*

Satz 2.10

Jede Untergruppe einer zyklischen Gruppe ist zyklisch.

Beweis. Wesentliches Hilfsmittel ist die Division mit Rest in $\mathbb{Z}$: Seien m, n ganze Zahlen mit $n \neq 0$. Dann gibt es eindeutig bestimmte ganze Zahlen q, r mit

$$m = qn + r$$

und mit $0 \leq r < |n|$. (Beweis siehe Vorlesung.) Sei nun $(G, \cdot)$ ein zyklische Gruppe, etwa $G = \langle g \rangle$. Sei U eine Untergruppe von G, wobei wir $U \neq \{e\}$ annehmen. Sei $e \neq u \in U$. Es gibt dann ein $n \neq 0$ mit $u = g^n$. Da mit u auch u^{-1} in U ist, können wir $n > 0$ annehmen, und außerdem, dass $n > 0$ minimal ist mit $g^n \in U$. Wir zeigen $U = \langle u \rangle = \langle g^n \rangle$: Da $g^n = u \in U$ gilt, ist $\langle u \rangle \subseteq U$ klar. Sei $v \in U$ beliebig. Es gibt ein $m \in \mathbb{Z}$ mit $v = g^m$. Division mit Rest ergibt q, r mit $m = qn + r$ mit $0 \leq r < n$. Wegen g^m, $g^n \in U$ gilt auch $g^r = g^{m-qn} = g^m \cdot g^{-qn} \in U$. Wegen $r < n$ und der Minimalität von n folgt $r = 0$, also $v = g^m = g^{qn} = (g^n)^q = u^q \in \langle u \rangle$. ∎

Dies Argument mit der Division mit Rest wird uns später auch in anderen Situationen wieder begegnen.

Folgerung 2.11

Jede Untergruppe von $(\mathbb{Z}, +)$ ist zyklisch.

Proposition 2.12

Sei $G = \langle g \rangle$ eine zyklische Gruppe der Ordnung $n < \infty$. Sei d ein Teiler von n $(d > 0)$. Dann ist $U = \langle g^{n/d} \rangle$ eine Untergruppe der Ordnung d.

Beweis. Ersichtlich ist d der kleinste Exponent mit

$$(g^{n/d})^d = e.$$

∎

Für zyklische Gruppen lässt sich der Satz von Lagrange ($|U| \mid |G|$) also gewissermaßen "umkehren". Allerdings ist dies generell nicht der Fall:

Beispiel. Die alternierende Gruppe $\mathbb{A}_4$ hat die Ordnung 12, aber keine Untergruppe der Ordnung 6. (Werden wir später sehen.)

Aufgaben

Ü 2.1. Sei g ein Element in der Gruppe G mit $\mathrm{ord}(g) = n$. Für jedes $k \geq 1$ gilt $\mathrm{ord}(g^k) = n/\,\mathrm{ggT}(k, n)$.

Ü 2.2. Seien g, h Elemente in der Gruppe G. Dann gilt $\mathrm{ord}(gh) = \mathrm{ord}(hg)$.

Ü 2.3. Seien a, b Elemente in der Gruppe G, die (endliche) Ordnung $\mathrm{ord}(a) = m$ bzw. $\mathrm{ord}(b) = n$ haben. Es gelte außerdem $ab = ba$ und dass m und n teilerfremd sind. Dann hat ab die Ordnung mn.

Ü 2.4. Sei G eine endliche Gruppe der Ordnung ≥ 2 oder unendlich. Dann ist $G \times G$ nie zyklisch.

3. Homomorphismen und Kern

Definition 3.1

Seien G und H Gruppen. Eine Abbildung $f\colon G \to H$ heisst (Gruppen-) *Homomorphismus* (oder kürzer: *Morphismus*), wenn

$$f(x \cdot_G y) = f(x) \cdot_H f(y)$$

für alle x, $y \in G$ gilt. Ist f zusätzlich bijektiv, so nennen wir f *Isomorphismus*. Zwei Gruppen G und H heissen *isomorph* (Schreibweise: $G \simeq H$), falls es einen Isomorphismus $f\colon G \to H$ gibt. Isomorphismen $f\colon G \to H$ mit $G = H$ heißen auch *Automorphismen* (von G), und die Menge $\mathrm{Aut}(G)$ aller Automorphismen bildet eine Gruppe mit der Komposition von Abbildung als Verknüpfung.

Eigenschaften 3.2

$f\colon G \to H$ sei ein Gruppenhomomorphismus. Dann gilt

(a) $f(e_G) = e_H$
(b) $f(x^{-1}) = f(x)^{-1}$
(c) $U < G \Rightarrow f(U) < H$
(d) $V < H \Rightarrow f^{-1}(V) < G$.

Beweis. (Siehe Vorlesung.) ∎

Definition 3.3 (*Normalteiler*)

Eine Untergruppe N von G heisst *Normalteiler*, wenn für jedes $g \in G$

$$gNg^{-1} \subseteq N$$

gilt. Notation: $N \lhd G$.

Äquivalent sind:

- $gNg^{-1} \subseteq N$ für jedes $g \in G$.
- $gNg^{-1} = N$ für jedes $g \in G$.
- $gN \subseteq Ng$ für jedes $g \in G$.
- $gN = Ng$ für jedes $g \in G$.

Proposition 3.4

Sei $f\colon G \to H$ ein Gruppenhomomorphismus. Dann ist

$$N = \mathrm{Kern}(f) := \{x \in G \mid f(x) = e_H\} = f^{-1}(\{e_H\})$$

ein Normalteiler in G.

Beispiele. (1) $\det\colon \mathrm{GL}_n(K) \to K^\times$ hat Kern $\mathrm{SL}_n(K)$.
(2) $\mathrm{sgn}\colon \mathbb{S}_n \to \{\pm 1\}$ hat Kern $\mathbb{A}_n$.
(3) $\exp\colon (\mathbb{R}, +) \longrightarrow (\mathbb{R}^\times, \cdot)$ ist injektiver Gruppenhomomorphismus, also $\mathrm{Kern}(\exp) = \{0\}$.

Lemma 3.5 (*Injektivitätskriterium*)

Ein Gruppenhomomorphismus $f\colon G \to H$ ist genau dann injektiv, wenn $\mathrm{Kern}(f) = \{e_G\}$ gilt.

Beweis. (Siehe Vorlesung.) ∎

4. Der Satz von Cayley

Satz 4.1 (*Cayley*)

Sei G eine endliche Gruppe der Ordnung n. Dann ist G isomorph zu einer Untergruppe der symmetrischen Gruppe $\mathbb{S}_n$.

Beweis. Für jedes $g \in G$ ist die Abbildung

$$\varphi_g \colon G \to G,\ x \mapsto gx$$

eine bijektive Abbildung, somit ein Mitglied der symmetrischen Gruppe $\mathbb{S}(G) = \{f \colon G \to G \mid f \text{ bijektive Abbildung}\}$. Wir zeigen, dass

$$\varphi \colon G \to \mathbb{S}(G),\ g \mapsto \varphi_g$$

ein injektiver Gruppenhomomorphismus ist:

(a) φ ist Homomorphismus:

$$\varphi_{gh}(x) = (gh)x = g(hx) = \varphi_g(\varphi_h(x)) = \varphi_g \circ \varphi_h(x).$$

(b) φ ist injektiv: Ist $\varphi_g = 1_G$, so folgt

$$x = 1_G(x) = \varphi_g(x) = gx$$

für alle $x \in G$; insbesondere für $x = e$, und $g = e$ folgt.

Wegen $|G| = n$ gilt $\mathbb{S}(G) \simeq \mathbb{S}_n$, und die Behauptung folgt. ∎

5. Konjugation

Für jedes $g \in G$ ist $h_g \colon G \to G$, $x \mapsto gxg^{-1}$ ein Automorphismus von G.

Definition 5.1

Elemente x, $y \in G$ heißen *konjugiert*, falls es ein $g \in G$ gibt mit $y = gxg^{-1}$. Wir bezeichnen mit $C(x) = \{gxg^{-1} \mid g \in G\}$ die Menge aller zu x konjugierten Elemente. Diese heisst die *Konjugationsklasse* von x.

Ist U eine Untergruppe von G, so ist $h_g(U) = gUg^{-1}$ eine Untergruppe von G, die zu U *konjugiert* heisst. Genau die Normalteiler von G stimmen mit ihren konjugierten Untergruppen überein.

Definition 5.2

$Z(G) = \{x \in G \mid gx = xg \text{ für alle } g \in G\}$ heisst das *Zentrum* von G.

Proposition 5.3

$Z(G)$ ist Normalteiler in G.

Beweis. Trivial. Konjugation lässt $Z(G)$ sogar elementweise fest. ∎

Proposition 5.4

(a) $x \in C(x)$.
(b) $C(x) \cap C(y) \neq \emptyset \ \Rightarrow\ C(x) = C(y)$.
(c) $|C(x)| = 1 \ \Leftrightarrow\ C(x) = \{x\} \ \Leftrightarrow\ x \in Z(G)$.

Beweis. (Siehe Vorlesung.) ∎

Satz 5.5 (*Klassengleichung*)

Ist G eine endliche Gruppe, so gilt

$$|G| = |Z(G)| + \sum_{|C(x)|>1} |C(x)|.$$

Beweis. (Siehe Vorlesung.) ∎

Sei $Z(x) = \{g \in G \mid gxg^{-1} = x\}$ (der *Zentralisator* von x).

Lemma 5.6

$|C(x)| = |G|/|Z(x)|$.

Beweis. Durch $G/Z(x) \to C(x)$, $gZ(x) \mapsto gxg^{-1}$ ist eine (wohldefinierte!) Bijektion gegeben. ∎

Eine Gruppe der Ordnung p^n mit p prim und $n \geq 1$ nennt man auch eine *p-Gruppe*.

Proposition 5.7

Sei G eine p-Gruppe. Dann ist das Zentrum nicht trivial: $Z(G) \neq \{e\}$.

Beweis. Nach dem Lemma ist $|C(x)| = |G|/|Z(x)|$ ein Teiler von $|G| = p^n$. Ist $|C(x)| > 1$, so wird $|C(x)|$ also von p geteilt. Es folgt, dass auch $|Z(G)|$ von p geteilt wird. Also ist $Z(G)$ nicht trivial. ∎

Folgerung 5.8

Jede Gruppe der Ordnung p^2 (p prim) ist abelsch.

Beweis. Nach Proposition 5.7 sind nur

$$|Z(G)| = \begin{cases} p \\ p^2 \end{cases}$$

möglich. Falls $|Z(G)| = p^2$, so sind wir fertig. Nehme also $|Z(G)| = p$ an. Dann ist G nicht abelsch. Es gibt dann ein $x \in G$, dessen Zentralisator $Z(x)$ echt in G enthalten ist. Es folgt

$$Z(G) \subseteq Z(x) \subsetneq G$$

und damit (Lagrange) $Z(G) = Z(x)$. Aber $x \in Z(x)$ und $x \notin Z(G)$, Widerspruch. ∎

Aufgaben

Ü 5.1. Sei G eine Gruppe der Ordnung p prim. Dann gilt $|\operatorname{Aut}(G)| = p - 1$. (Wie sehen die Elemente von $\operatorname{Aut}(G)$ konkret aus?)

Ü 5.2. Sei $A \subseteq G$ eine Teilmenge der Gruppe G. Definiere $C(A) = C_G(A) = \{gAg^{-1} \mid g \in G\} \subseteq 2^G$ (Konjugationsklasse von A), $N(A) = N_G(A) = \{g \in G \mid gAg^{-1} = A\}$ (Normalisator) sowie $Z(A) = Z_G(A) = \{g \in G \mid gag^{-1} = a \text{ für alle } a \in A\}$ (Zentralisator von A in G). Dann gilt:

(1) $N(A)$ und $Z(A)$ sind Untergruppen von G mit $Z(A) \subseteq N(A)$.
(2) Im Fall $A = \{x\}$ gilt $N(x) := N(A) = Z(A) = Z(x)$.
(3) $|G| = |C(A)| \cdot |N(A)|$.
(4) Sei A ein Normalteiler von G. Dann ist $G \to \operatorname{Aut}(A)$, $g \mapsto h_{g|A}$ ($h_g(a) = gag^{-1}$) ein Gruppenmorphismus mit Kern $Z(A)$.
(5) Sei U eine Untergruppe von G. Dann gilt $U \lhd N_G(U)$, und $N_G(U)$ ist die größte Untergruppe von G, in der U ein Normalteiler ist. Es gilt $U \lhd G$ genau wenn $N_G(U) = G$.

KAPITEL II

Faktorstrukturen

1. Faktorgruppen

Ist N ein Normalteiler in einer Gruppe G, so gilt $gN = Ng$ für jedes $g \in G$; wir schreiben im folgenden $[g] := Ng$.

Satz und Definition 1.1

Sei G eine Gruppe und N ein Normalteiler in G. Dann bildet

$$G/N = \{[g] \mid g \in G\}$$

bezüglich der Verknüpfung

$$[x] \cdot [y] \overset{def}{=} [xy]$$

eine Gruppe. Dabei ist $[e_G]$ das neutrale Element und $[x^{-1}]$ zu $[x]$ invers.

G/N heißt die Faktorgruppe *von G* nach *N (oder auch Quotient von G nach N.)*

Beweis. (Siehe Vorlesung.) Hauptaugenmerk liegt hier darauf zu zeigen, dass die angegebene Verknüpfung wohldefiniert ist; dazu muss man die Normalteilereigenschaft verwenden. ∎

Zusatz 1.2

Die Abbildung

$$\nu \colon G \to G/N,\ x \mapsto [x]$$

ist ein surjektiver Gruppenhomomorphismus mit $\mathrm{Kern}(\nu) = N$.

$\nu = \nu_N \colon G \to G/N$ heißt der *natürliche Homomorphismus* (bzgl. N).

Bemerkung. (a) Jeder Kern eines Gruppenhomomorphismus $h \colon G \to H$ ist Normalteiler in G. Umgekehrt ist nach dem vorherigen jeder Normalteiler N in G Kern des natürlichen Homomorphismus

$$\nu_N \colon G \to G/N,\ x \mapsto [x]_N.$$

(b) Für $N = G$ ist $G/N = \{[e]\}$ die einelementige, triviale Gruppe.

(c) Für $N = \{e\}$ ist der natürliche Homomorphismus $\nu \colon G \to G/\{e\}$ surjektiv mit $\mathrm{Kern}(\nu) = \{e\}$, also ein Isomorphismus.

(d) Die allgemeine Situation liegt zwischen den beiden Extremfällen (b) und (c). Durch die Faktorkonstruktion wird beim Übergang von G nach G/N durch ν eine "Verkleinerung"von G erreicht, bei der N auf das neutrale Element $[e]$ von G/N und allgemein eine Nebenklasse $Nx \subseteq G$ auf das Element $[x]$ zusammenschrumpft.

Hinweis.

- Wenn G eine *abelsche* Gruppe und U in G eine Untergruppe ist, können wir somit stets die Faktorgruppe G/U bilden.
- Man mache sich klar, wo es mit der Faktorbildung im nicht-abelschen Fall schiefgeht, wenn U nur eine Untergruppe, aber kein Normalteiler von G ist!

Satz 1.3

Für jedes natürliche $n \geq 1$ ist

$$\mathbb{Z}_n := \mathbb{Z}/\mathbb{Z} \cdot n$$

eine zyklische Faktorgruppe von $(\mathbb{Z}, +)$ der Ordnung n, die gerade aus den Nebenklassen

$$[0],\ [1],\ [2], \ldots,\ [n-1]$$

besteht.

Beweis. Per Division mit Rest. (Vgl. Vorlesung.) ∎

Wie sieht *konkret* die Addition auf $\mathbb{Z}_n$ aus? Seien $0 \le x,\ y < n$ und

$$[x] + [y] = [x+y] = \begin{cases} [x+y] & \text{falls } x+y < n, \\ [x+y-n] & \text{sonst.} \end{cases}$$

Wir können daher auf $\{0, 1, \ldots, n-1\}$ eine Addition $+_n$ erklären durch

$$x +_n y = \begin{cases} x+y & \text{falls } x+y < n, \\ x+y-n & \text{sonst.} \end{cases} \tag{1.1}$$

Nimmt man dies als Startpunkt, müßte zunächst die Assoziativität der Verknüpfung gezeigt werden, was relativ aufwändig ist. Die Bildung der Faktorgruppe erledigt dies wesentlich eleganter.

Aufgaben

Ü 1.1. Man zeige (direkt), dass die Verknüpfung in (1.1) assoziativ ist.

Ü 1.2. Sei G eine Gruppe und U eine Untergruppe von G vom Index $[G : U] = 2$. Dann ist U ein Normalteiler in G.

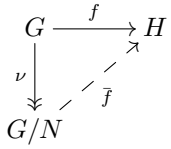
Ü 1.3. Sei G eine zyklische Gruppe. Dann ist auch jede Faktorgruppe von G zyklisch.

2. Der Homomorphiesatz

Das Konzept der Faktorgruppe entfaltet seine volle Wirksamkeit erst im Zusammenwirken mit dem Homomorphiesatz, der besagt, dass – bis auf eine nachfolgende Einbettung – jeder Homomorphismus so aussieht, wie ein natürlicher Homomorphismus $\nu\colon G \to G/N$.

Satz 2.1 (*Homomorphiesatz*)

Sei $f\colon G \to H$ ein Gruppenhomomorphismus und N ein Normalteiler in G mit $N \subseteq \mathrm{Kern}(f)$. Dann gibt es genau einen Homomorphismus $\bar{f}\colon G/N \to H$ mit $\bar{f} \circ \nu = f$; es gilt also $\bar{f}([x]) = f(x)$ für alle $x \in G$, d. h. das folgende Diagramm kommutiert:



Ferner gilt: $\bar{f}$ ist injektiv genau dann, wenn $N = \mathrm{Kern}(f)$ gilt. Außerdem ist $\mathrm{Bild}(\bar{f}) = \mathrm{Bild}(f)$.

Beweis. Definiere $\bar{f}([x]) = f(x)$ für alle $x \in G$. (Dies ist die einzige Möglichkeit, wenn die Aussage im Satz richtig sein soll.) Man muss zeigen, dass dies wohldefiniert ist. Seien also $x,\ y \in G$ mit $[x] = [y]$. Dies bedeutet $xy^{-1} \in N \subseteq \mathrm{Kern}(f)$, also folgt $f(x)f(y)^{-1} = f(xy^{-1}) = e_H$, was gleichbedeutend zu $f(x) = f(y)$ ist. — Man rechnet nun leicht nach, dass $\bar{f}$ ein Gruppenhomomorphismus ist, der das obige Diagramm kommutieren lässt. Ferner gilt dann offenbar $\mathrm{Kern}(\bar{f}) = \{[x] \mid x \in \mathrm{Kern}(f)\}$, und daher $\mathrm{Kern}(\bar{f}) = \{[e_G]\}$ genau dann, wenn für alle $x \in G$ gilt: $x \in \mathrm{Kern}(f) \Rightarrow x \in N$. ∎

Folgerung 2.2

Ist f surjektiv und $N = \mathrm{Kern}(f)$, so ist $\bar{f}$ ein Isomorphismus. ■

Wir erhalten eine vollständige Klassifikation zyklischer Gruppen:

Satz 2.3

Es gilt:

(a) *Jede unendliche zyklische Gruppe G ist isomorph zu $(\mathbb{Z}, +)$.*
(b) *Jede endliche zyklische Gruppe der Ordnung n ist isomorph zu $\mathbb{Z}_n$.*

Beweis. Sei $G = \langle g \rangle$. Die Abbildung $\phi\colon \mathbb{Z} \to G$, $i \mapsto g^i$ ist ein surjektiver Gruppenmorphismus mit $\mathrm{Kern}(\phi) = \{0\}$, falls $|G| = \infty$, und $\mathrm{Kern}(\phi) = n\mathbb{Z}$, falls $|G| = n$. ■

Aufgaben

Ü 2.1. Seien N, K Normalteiler in einer Gruppe G, und sei H eine Untergruppe von G.
(1) [1. Isomorphiesatz] Die kanonische Abbildung $H \to HN/N$, $x \mapsto [x]_N$ induziert einen Isomorphismus $H/H \cap N \simeq HN/N$.
(2) [2. Isomorphiesatz] Gilt $K \subseteq N$, so induziert die kanonische Abbildung $[x]_K \mapsto [x]_N$ einen Isomorphismus $(G/K)/(N/K) \simeq G/N$.
(3) Die Zuordnung $U \mapsto U/N$ induziert eine bijektive Abbildung von der Menge der Untergruppen (bzw. Normalteiler) U in G mit $N \subseteq U$ auf die Menge der Untergruppen (bzw. Normalteiler) der Faktorgruppe G/N.

Ü 2.2. Sei G eine p-Gruppe und A ein Normalteiler der Ordnung p. Dann gilt $A \subseteq Z(G)$. (Hinweis: Man zeige mit Hilfe von Ü 5.1 und Ü 5.2 aus dem vorigen Kapitel, dass $Z_G(A) = G$ gilt.)

Ü 2.3. Seien m und n zwei teilerfremde natürliche Zahlen. Dann ist die Produktgruppe $\mathbb{Z}_m \times \mathbb{Z}_n$ isomorph zur zyklischen Gruppe $\mathbb{Z}_{mn}$ ist.

3. Der Satz von Cauchy

Die behandelten Faktorgruppen sind außerordentlich nützlich. Sie ermöglichen z. B. für endliche Gruppen intelligente Induktionsargumente. Wir diskutieren hier als einen solchen Anwendungsfall den Satz von Cauchy.

Lemma 3.1

Sei G eine endliche abelsche Gruppe, deren Ordnung durch die Primzahl p geteilt wird. Dann enthält G ein Element der Ordnung p.

Beweis. Ist G zyklisch, so gibt es nach Proposition I.2.12 ein Element der Ordnung p. Andernfalls, sei $g \in G$ mit $\{e\} \subsetneq \langle g \rangle \subsetneq G$. Dann hat per Induktion wegen $|G| = |\langle g \rangle| \cdot |G/\langle g \rangle|$ nun $\langle g \rangle$ oder die (abelsche) Faktorgruppe $G/\langle g \rangle$ ein Element y der Ordnung p. Im ersten Fall ist man fertig. Im zweiten Fall sei $x \in G$ mit $y = [x]$, und sei $U = \langle x \rangle < G$. Ist $m = \mathrm{ord}(x) = |U|$, so gilt $y^m = [x^m] = [e]$. Also p teilt m, und daher enthält U (da zyklisch) ein Element der Ordnung p. ■

Satz 3.2 (*Cauchy (1845)*)

Es sei G eine endliche Gruppe, deren Ordnung durch die Primzahl p geteilt wird. Dann enthält G ein Element der Ordnung p.

Beweis. Das vorige Lemma zeigt die Richtigkeit des Satzes von Cauchy unter der Zusatzvoraussetzung, dass G abelsch ist. Den allgemeinen Fall führt man hierauf zurück: Induktion nach n mit $|G| = pn$. Für $n = 1$ ist die Aussage klar. Sei $n > 1$. Zwei Fälle sind möglich.

1. Fall. Es gibt eine echte Untergruppe U von G mit $p \mid |U|$. Dann enthält wegen $|U| < |G|$ nach Induktionsvoraussetzung U eine Element der Ordnung p, und dies gilt natürlich auch in G.

2. Fall. Es existiert keine echte Untergruppe U von G mit $p \mid |U|$. Wegen $n > 1$ ist G nach dem vorherigen Lemma nicht abelsch, d. h. es gilt $Z(G) \neq G$. Für jedes $x \in G$ mit $x \notin Z(G)$ (bzw. äquivalent $|C(x)| > 1$) ist der Zentralisator $Z(x)$ eine echte Untergruppe von G. Da dessen Ordnung nicht von p geteilt wird, teilt p den Index $[G : Z(x)] = |C(x)|$. Aus der Klassengleichung

$$|G| = |Z(G)| + \sum_{|C(x)|>1} |C(x)|$$

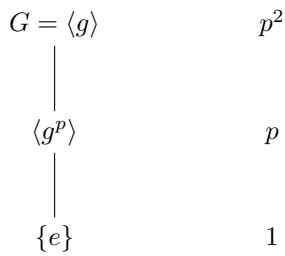
folgt $p \mid |Z(G)|$. Dies widerspricht aber der Aussage des 2. Falls, d. h. es kann nur der 1. Fall gelten (oder $n = 1$). ∎

4. Gruppen kleiner Ordnung

Mit Hilfe des Satzes von Cauchy können wir für eine ganze Reihe kleiner Ordnungen sämtliche Gruppen dieser Ordnung bestimmen. Wir wollen bis zur Ordnung 15 sehen, wie weit wir mit unseren jetzigen Fähigkeiten kommen. Sei also G eine endliche Gruppe der Ordnung n.

- $n = 1$ klar.
- $n = 2, 3, 5, 7, 11, 13$. Hier ist n eine Primzahl. Wir wissen, dass diese Gruppen zyklisch sind, isomorph zu $\mathbb{Z}_n$, und außer $\{e\}$ und G keine weiteren Untergruppen haben. $G = \langle g \rangle$, $g^n = e$. Wir haben also auch den sog. *Untergruppenverband* von G bestimmt (d. h. die Menge aller Untergruppen von G, geordnet mit der Inklusion.)

- $n = 4, 9$. Hier ist $n = p^2$ für eine Primzahl p, daher ist G abelsch (nach Folgerung I.5.8). Elemente $e \neq g \in G$ haben die Ordnung p oder p^2. Nur zwei Fälle sind möglich:
  (a) Es gibt ein $g \in G$ der Ordnung $n = p^2$. In diesem Fall ist G zyklisch, $G = \langle g \rangle$, $g^n = e$. Ferner ist der Untergruppenverband linear:

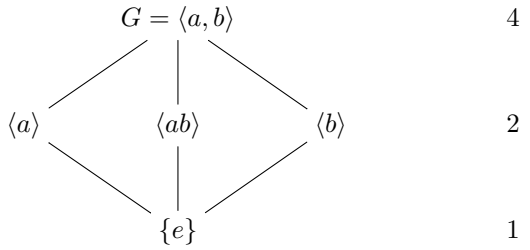


  Denn wegen $\operatorname{ord}(g) = p^2$ sieht man sofort, dass g^i für $1 \leq i \leq p-1$ eine Ordnung $> p$ haben muss und daher ein Erzeuger von G ist; daher ist $\langle g^p \rangle$ die einzige Untergruppe der Ordnung p.
  (b) Jedes $e \neq g \in G$ hat die Ordnung p. Jedes solche Element liegt daher in genau einer Untergruppe U der Ordnung p; denn zwei verschiedene Untergruppen der Ordnung p haben nur e im Durchschnitt. Abzählen

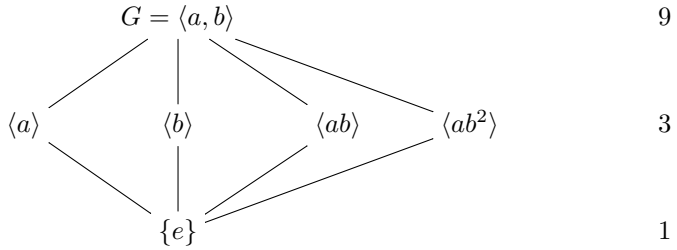
$$|G \setminus \{e\}| = p^2 - 1 = (p+1)(p-1) = (p+1)|U \setminus \{e\}|$$

zeigt, dass G genau $p+1$ Untergruppen der Ordnung p hat und dies alle echten Untergruppen von G sind.

(b1) $n = 4$ ($p = 2$). $G = \langle a, b\rangle$, $a^2 = b^2 = e$, $ab = ba$. G ist die sog. Kleinsche Vierergruppe, $G \simeq \mathbb{Z}_2 \times \mathbb{Z}_2 = \mathbb{V}_4$. Untergruppenverband:



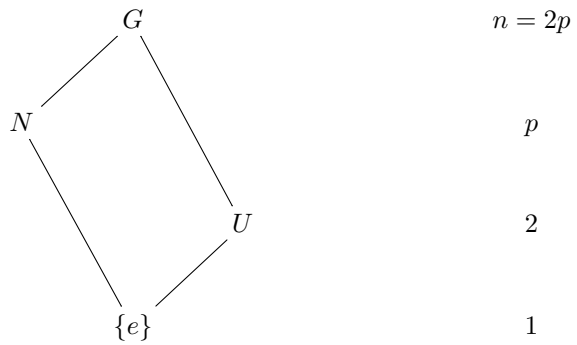
(b2) $n = 9$ ($p = 3$). $G = \langle a, b\rangle$, $a^3 = b^3 = e$, $ab = ba$. G ist isomorph zu $\mathbb{Z}_3 \times \mathbb{Z}_3$. Untergruppenverband:



Bemerkung: Mit ähnlicher Argumentation ist jede Gruppe der Ordnung $n = p^2$ entweder zu $\mathbb{Z}_n$ oder zu $\mathbb{Z}_p \times \mathbb{Z}_p$ isomorph. Diese Gruppen sind daher sämtlich direkte Produkte von zyklischen Gruppen. Der Hauptsatz über endliche abelsche Gruppen sagt, dass die letztgenannte Eigenschaft allgemeiner für alle endlichen abelschen Gruppen gilt.

- $n = 6, 10, 14$. Diese Ordnungen haben die Form $n = 2p$, wobei p eine ungerade Primzahl ist. Der Satz von Cauchy sagt uns, dass es sowohl ein Element g der Ordnung 2 als auch ein Element h der Ordnung p gibt. Es hat $N = \langle h\rangle$ als Untergruppe der Ordnung p den Index 2, ist also Normalteiler in G (vgl. Übungen). Folgende Fälle sind möglich (für Details vgl. Vorlesung):

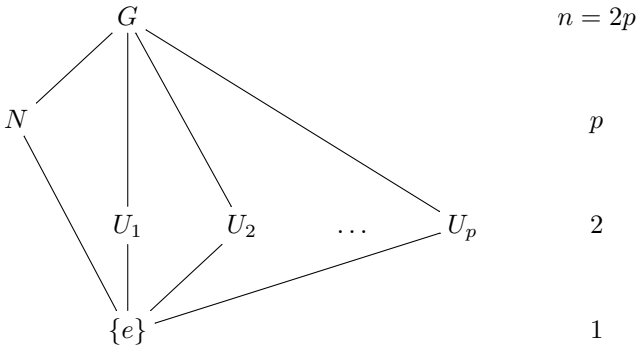
  (a) G hat ein Element der Ordnung $n = 2p$. Dann ist $G \simeq \mathbb{Z}_n$ zyklisch (insbesondere abelsch). Der Untergruppenverband von G ist



mit $U = \langle g\rangle$. (Man zeigt leicht, dass jedes Element außerhalb von N und U ein Erzeuger von G ist: $g^i h^j$ ($i = 0, 1$; $0 \le j \le p-1$) sind alle $2p$ Elemente, und nach ein vorherigen Übung gilt $\mathrm{ord}(gh^j) = 2p$.)

Präsentation durch Erzeugende und Relationen[1]: $G = \langle g, h\rangle$, $g^2 = e = h^p$, $hg = gh$, oder kürzer $G = \langle g, h \mid g^2, h^p, hgh^{-1}g^{-1}\rangle$. Man sieht, dass $G \simeq \mathbb{Z}_2 \times \mathbb{Z}_p$ ($\simeq \mathbb{Z}_{2p}$) gilt.

(b) Jedes $e \neq x \in G$ hat entweder die Ordnung 2 oder die Ordnung p. Man zeigt, dass N die einzige Untergruppe der Ordnung p ist. (Sonst gäbe es aus Elementanzahlsgründen nur eine weitere der Ordnung p und U wäre die einzige Untergruppe der Ordnung 2. Da aber alle Konjugierten von g die Ordnung 2 haben, muss g im Zentrum liegen; insbesondere $gh = hg$, und nach der schon genannten Übung hat dies Element die Ordnung $2p$, Widerspruch.) Somit haben alle Elemente aus $G \setminus N$ die Ordnung 2, bilden damit (zusammen mit e) p Untergruppen $U_1, \ldots, U_p$ der Ordnung 2. Wir haben den Untergruppenverband ermittelt:



Präsentation durch Erzeugende und Relationen: $N = \langle h\rangle$, $h^p = e$, $U_1 = \langle g\rangle$, $g^2 = e$. Man zeigt nun, dass

$$\varphi\colon N \times U_1 \to G,\ (n, u) \mapsto nu$$

bijektiv ist (wegen $N \cap U_1 = \{e\}$, und vgl. Elementanzahlen). Es lässt sich also jedes $x \in G$ eindeutig in der Form

$$x = h^i g^j \quad 0 \leq i \leq p-1,\ 0 \leq j \leq 1$$

schreiben. Wegen $\langle h\rangle = N \lhd G$ gilt

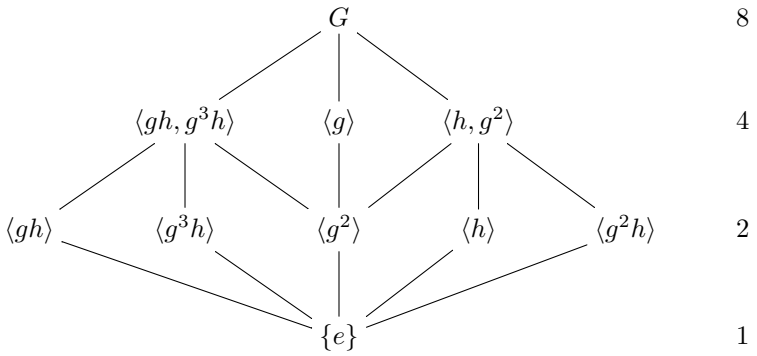
$$ghg^{-1} = h^i$$

für ein $1 \leq i \leq p-1$. Man sieht aber, dass nur $i = 1$ und $i = p-1$ möglich sind: denn wegen $g^2 = e$ und $ghg^{-1} = h^i$ folgt $h = g^2hg^{-2} = gh^ig^{-1} = (ghg^{-1})^i = h^{i^2}$, und deswegen $p \mid i^2 - 1 = (i-1)(i+1)$, d. h. aber $i = 1$ oder $i = p-1$. Im Fall $i = 1$ gilt $gh = hg$, und G ist abelsch, $G \simeq \mathbb{Z}_p \times \mathbb{Z}_2 \simeq \mathbb{Z}_{2p}$, also zyklisch. Dies ist aber Fall (a) und in (b) nicht möglich. Also bleibt nur $i = p-1$, und es gilt $G = \langle g, h\rangle$ mit Relationen $g^2 = e = h^p$, $ghg^{-1} = h^{p-1}$. Dies liefert die sog. Diedergruppe $\mathbb{D}_p$ (vom Grad p und der Ordnung $2p$).

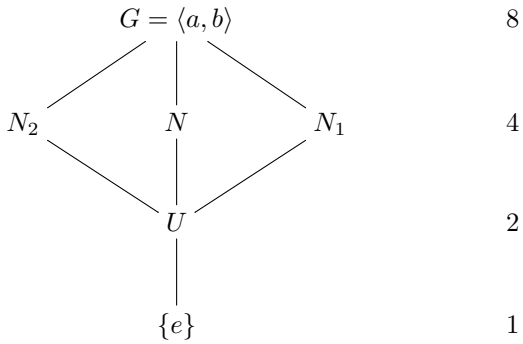
- $n = 8 = 2^3$. Die abelschen Fälle sind hier (isomorph zu) $\mathbb{Z}_8$, $\mathbb{Z}_2 \times \mathbb{Z}_4$ oder $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. Diese betrachten wir im folgenden nicht. Der interessante Fall ist dann, wenn G eine zyklische Untergruppe N der Ordnung 4 hat; diese ist dann automatisch ein Normalteiler von G. $N = \langle g\rangle$, $g^4 = e$. Es gibt dann zwei Fälle:

[1] Wir verwenden diese Sprechweise hier ad hoc. Für nähere Erläuterung vgl. unten stehende Bemerkung.

(a) In $G \setminus N$ gibt es ein Element h der Ordnung 2. Es folgt $G = \langle g, h\rangle$ mit $g^4 = e = h^2$, und ferner folgt $hgh^{-1} = g$ (und dann $G \simeq \mathbb{Z}_4 \times \mathbb{Z}_2$ abelsch) oder $hgh^{-1} = g^3$, womit es sich um die Diedergruppe $\mathbb{D}_4$ handelt. Der Untergruppenverband sieht wie folgt aus:



(b) In $G \setminus N$ hat jedes Element die Ordnung 4. Hier zeigt man, dass G die Quaternionengruppe ist:



$a^4 = e$, $b^2 = a^2$, $ba = a^{-1}b$. Hier sind alle Untergruppen Normalteiler.

- $n = 12 = 2^2 \cdot 3$. Hier gibt es als abelsche Gruppen

$$\mathbb{Z}_4 \times \mathbb{Z}_3 \simeq \mathbb{Z}_{12},\ \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \simeq \mathbb{Z}_2 \times \mathbb{Z}_6$$

und drei nichtabelsche. Siehe Übung 4.1.
  - $\mathbb{A}_4$ alternierende Gruppe;
  - $\mathbb{D}_6$ Diedergruppe;
  - sog. dizyklische Gruppe ($\langle a, b\rangle$, $a^6 = e$, $b^2 = a^3$, $ba = a^{-1}b$).
- $n = 15 = 3 \cdot 5$. Hier ist jede Gruppe zyklisch, siehe Übung 4.2.

Bemerkung. Sei $n \geq 1$. Die *Diedergruppe* $\mathbb{D}_n$ vom *Grad* n (der Ordnung $2n$; manche Autoren schreiben $\mathbb{D}_{2n}$ statt $\mathbb{D}_n$) ist definiert durch Erzeugende und Relationen,

$$\mathbb{D}_n = \langle r, s\rangle,\ r^n = e = s^2,\ srs^{-1} = r^{n-1}$$

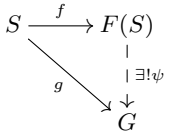
(beachte: $s^{-1} = s$ und $r^{-1} = r^{n-1}$), bzw.

$$\mathbb{D}_n = \langle r, s \mid r^n,\ s^2,\ srsr\rangle$$

und kann als Symmetriegruppe des regelmäßigen n-Ecks angesehen werden: r beschreibt eine Drehung um den Schwerpunkt des n-Ecks um den Winkel $2\pi/n$, und s eine Spiegelung an einer Geraden durch den Schwerpunkt, die Mittelsenkrechte einer Seite ist. [Vgl. den Fall $n = 4$ (Quadrat) in der Vorlesung.]

Bemerkung. Eine detaillierte Klassifizierung aller Gruppen der Ordnung ≤ 15 findet man in Abschnitt II.6 im Buch [6].

Bemerkung. * (1) [Freie Gruppe] Sei S eine Menge. Dann existiert eine Gruppe, bezeichnet mit $F(S)$, und eine Abbildung $f\colon S \to F(S)$, so dass folgende *universelle Eigenschaft* erfüllt ist. *Zu jeder Gruppe G und jeder Abbildung $g\colon S \to G$ gibt es genau einen Gruppenhomomorphismus $\psi\colon F(S) \to G$ mit $\psi \circ f = g$, d. h. das folgende Diagramm kommutiert:*



Ferner ist f injektiv und $F(S)$ wird erzeugt von den Elementen im Bild $f(S)$. Durch S ist die Gruppe dadurch bis auf Isomorphie eindeutig bestimmt. Man nennt sie *die durch S erzeugte freie Gruppe*. Die Elemente dieser Gruppe sind endliche (formale) Wörter $x_1 x_2 \dots x_n$ mit $x_i \in S \coprod S^{-1}$ (wobei S^{-1} disjunkt zu S ist und aus den Buchstaben x^{-1} für jedes $x \in S$ besteht, wobei die Wörter reduziert in dem Sinne sind, dass $x_i \neq {x_{i+1}}^{-1}$ für alle i gilt. Neutrales Elements ist das leere Wort. Die Verknüpfung ist durch (reduzierende) Konkatenation gegeben ist. Für Details verweisen wir auf die Bücher [9], I.12 oder [6], I.9. *Jede Gruppe G ist Faktorgruppe einer freien Gruppe* (man nehme für S eine Menge von Erzeugern von G, z. B. $S = G$). Ist G Faktorgruppe von $F(S)$, so nennt man G erzeugt von S (gemeint ist, von den Bildelementen $\pi(S)$ in G).

(2) [Präsentation durch Erzeuger und Relationen] Sei R eine Teilmenge reduzierter Wörter in $S \coprod S^{-1}$. Man sagt, dass eine Gruppe G erzeugt wird von S mit Relationen (in) R, falls $G \simeq F(S)/N$ gilt, wobei N der kleinste Normalteiler von $F(S)$ ist, der R enthält. (Dies ist der Durchschnitt aller Normalteiler in $F(S)$, die R enthalten.) Man schreibt $G = \langle S \mid R \rangle$ und nennt dies eine *Präsentation von G durch Erzeugende und Relationen*. Aus der universellen Eigenschaft von $F(S)$ folgt leicht folgende Eigenschaft, die man auch Satz von Van Dyck nennt. *Ist H eine von S erzeugte Gruppe, in der "alle Relationen aus R" gelten, dann gibt es einen surjektiven Gruppenhomomorphismus $\phi\colon \langle S \mid R \rangle \to H$.* Denn die Voraussetzung sagt mathematisch gerade aus, dass es einen surjektiven Morphismus $\psi\colon F(S) \to H$ gibt mit $R \subseteq \mathrm{Kern}(f)$. Ist N der kleinste Normalteiler, der R enthält, so folgt mit dem Homomorphiesatz die Existenz eines eindeutigen (surjektiven) Morphismus $\phi\colon F(S)/N \to H$ mit $\phi \circ \nu_N = \psi$.

Aufgaben

Ü 4.1. Man klassifiziere alle (nicht-abelschen) Gruppen der Ordnung $n = 12$.

Ü 4.2. Sei G eine Gruppe der Ordnung 15. Im folgenden soll gezeigt werden, dass G zyklisch ist.

(1) Es gibt eine Untergruppe U der Ordnung 3 und eine Untergruppe V der Ordnung 5. Die Abbildung $m\colon U \times V \longrightarrow G$, $(u, v) \mapsto u \cdot v$ ist bijektiv.
(2) Sei $\mathbb{S}(G/V)$ die Gruppe der bijektiven Abbildungen von der Menge der Linksnebenklassen von V in sich, also $\mathbb{S}(G/V) \simeq S_3$. Die Abbildung $\varphi\colon G \to \mathbb{S}(G/V)$, $g \mapsto \varphi_g$, wobei $\varphi_g(hV) = ghV$, ist ein Gruppenhomomorphismus.
(3) Das Bild von φ hat die Ordnung 3, also $\mathrm{Bild}\,\varphi \simeq \mathbb{Z}_3$.
(4) Es gibt einen Normalteiler N in G der Ordnung 5.
(5) Für jedes $g \in G$ ist die Abbildung $h_g\colon N \to N$, $h_g(n) = gng^{-1}$ ein Automorphismus. Die Abbildung $\psi\colon U \to \mathrm{Aut}(N)$, $u \mapsto h_u$ ist ein Gruppenhomomorphismus, der trivial ist. (Gibt es ein Element der Ordnung 3 in $\mathrm{Aut}(N) \simeq \mathrm{Aut}(\mathbb{Z}_5)$?)
(6) Für alle $u \in U$ und $n \in N$ gilt $un = nu$.
(7) Die Abbildung $m\colon U \times N \to G$, $(u, n) \mapsto u \cdot n$ ist ein Isomorphismus.
(8) $G \simeq \mathbb{Z}_{15}$.

Ü 4.3. $\mathbb{D}_n = \langle r, s \mid r^n,\ s^2,\ srsr \rangle$, die Diedergruppe vom Grad n präsentiert durch Erzeugende und Relationen, ist isomorph zur Symmetriegruppe $G = \langle R, S \rangle$ des regelmäßigen n-Ecks, (R $2\pi/n$-Drehung, S Spiegelung) und hat daher die Ordnung $2n$.

5. Ringe und Körper

Definition 5.1

Eine Menge R mit zwei Verknüpfungen

$$+\colon R \times R \to R \quad \text{und} \quad \cdot\colon R \times R \to R$$

heißt ein *Ring* (mit Eins 1_R), falls folgendes gilt:

(1) Es ist $(R, +)$ eine abelsche Gruppe. (Das neutrale Element bzgl. der Addition "+" heißt Null (-element) und wird mit $0 = 0_R$ bezeichnet.)
(2) Die Multiplikation "$\cdot$" ist assoziativ und hat ein neutrales Element (dieses heisst Eins (-element) und wird mit $1 = 1_R$ bezeichnet.)
(3) Es gelten zwischen "+" und "$\cdot$" die Distributivgesetze: für alle a, b, $c \in R$ ist

$$a \cdot (b + c) = a \cdot b + a \cdot c \text{ und } (a + b) \cdot c = a \cdot c + b \cdot c.$$

Ein *kommutativer Ring* R ist ein Ring, in dem die Multiplikation "$\cdot$" zusätzlich kommutativ ist.

Konvention: In der Notation nehmen wir immer die Regel "Punkt- vor Strichrechnung" an. Diese haben wir oben schon verwendet, denn statt $(a \cdot b) + (a \cdot c)$ haben wir einfach $a \cdot b + a \cdot c$ geschrieben. Desweiteren lässt man oft das "$\cdot$"-Zeichen weg und schreibt statt $a \cdot b$ einfach ab. Statt $a + (-b)$ schreibt man $a - b$.

Wir werden stets Ringe *mit* Eins betrachten.

Bemerkung. Sei R ein Ring. Für jedes $a \in R$ gilt $0 \cdot a = 0 = a \cdot 0$. (Denn $a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$, und Kürzen in $(R, +)$ liefert $a \cdot 0 = 0$. Die andere Gleichung ist analog.)

Die Nullring $R = \{0\}$ ist der einzige Ring (mit Eins), in dem $1 = 0$ gilt.

Beispiele. (a) $\mathbb{Z}$.

(b) Jeder Körper, insbesondere $\mathbb{Q}$, $\mathbb{R}$ und $\mathbb{C}$.
(c) $\mathrm{End}_K(V)$ für einen K-Vektorraum V.
(d) $\mathrm{M}_n(K)$. Für $n \geq 2$ nicht kommutativ.
$(e)^*$ $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} = \{[0], [1], \ldots, [n-1]\}$ mit

$$[x] \cdot [y] \stackrel{def}{=} [xy]$$

ist ein kommutativer Ring mit n Elementen.

$(f)^*$ K ein Körper, $K[T]$ der Ring der Polynome über K in der Unbestimmten T.

Definition 5.2

Ein Ring R, für den $R^\times = R \setminus \{0\}$ bzgl. Multiplikation eine Gruppe ist, heißt *Schiefkörper*. Ist R zusätzlich kommutativ, so heißt R ein *Körper*.

Beispiele. (1) $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ sind Körper. Weitere Körper wie

$$\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$$

und

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

erhält man als Teilkörper von $\mathbb{R}$ bzw. $\mathbb{C}$.

(2) Die Ringe $\mathbb{Z}$ und $\mathrm{M}_n(K)$ $(n \geq 2)$ sind keine (Schief-) Körper.
(3) Die Menge

$$\mathbb{H} = \left\{ \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} \mid a, b \in \mathbb{C} \right\}$$

bildet bzgl. Matrizenaddition und -multiplikation einen Schief-Körper, den Schiefkörper der (Hamiltonschen) *Quaternionen* . — Für $(a, b) \neq (0, 0)$ ist

$$\begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix}^{-1} = \frac{1}{|a|^2 + |b|^2} \begin{pmatrix} \bar{a} & -b \\ \bar{b} & a \end{pmatrix}.$$

(4)* Ist p eine Primzahl, so ist $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ ein Körper mit genau p Elementen.
(5)* Ist K ein endlicher Körper, so ist $|K| = p^n$ eine Primzahlpotenz.
(6)* Sind K und L endliche Körper mit $|K| = |L|$, so sind K und L isomorph.
(7)* Ist K ein Körper, so ist

$$K(T) = \left\{ \frac{f}{g} \mid f, g \in K[T],\ g \neq 0 \right\}$$

(formale Brüche) mit den üblichen Bruchrechenregeln ein Körper, der Körper der rationalen Funktionen über K in der Unbestimmten T. Es ist $K[T] \subset K(T)$ ein Unterring (identifiziere f mit $\frac{f}{1}$).

Proposition 5.3

Jeder Schiefkörper K ist nullteilerfrei, *d. h. $x \cdot y = 0$ impliziert $x = 0$ oder $y = 0$.*

Beweis. Ist $xy = 0$ und $x \neq 0$, so folgt

$$y = 1 \cdot y = (x^{-1}x)y = x^{-1}(xy) = 0.$$

■

Definition 5.4

Ein kommutativer Ring mit $0 \neq 1$ heißt *Integritätsring* (oder *Integritätsbereich*), wenn er nullteilerfrei ist.

Beispiele. (1) $\mathbb{Z}$.
(2) Allgemeiner ist (offenbar) jeder Unterring eines Körpers K nullteilerfrei.
(3)* Der Polynomring $K[T]$ ist nullteilerfrei (K ein Körper). (Beweis später.)
(4)* Jeder Integritätsbereich lässt sich in einen Körper einbetten, damit als Unterring eines Körpers auffassen. (Beweis später.)

Proposition 5.5

Jeder endliche Integritätsring R ist ein Körper.

Beweis. Sei $a \in R$, $a \neq 0$. Die Abbildung

$$\lambda_a \colon R \to R,\ x \mapsto ax$$

ist – da a kein Nullteiler ist – injektiv, und wegen der Endlichkeit von R auch surjektiv. Insbesondere gibt es ein $x \in R$ mit $1 = \lambda_a(x) = ax$. Also ist a invertierbar. ■

Definition 5.6

Sei $R = (R, +, \cdot)$ ein Ring mit Einselement. Sei K ein Körper (oder allgemeiner, ein kommutativer Ring). Dann heisst R eine *K-Algebra*, wenn R bzgl. einer Abbildung

$$K \times R \to R,\ (\alpha, r) \mapsto \alpha \cdot r = \alpha r$$

zusätzlich ein K-Vektorraum (bzw. K-Modul) ist, so dass gilt

$$\alpha(rs) = (\alpha r)s = r(\alpha s) \quad \text{für alle } \alpha \in K,\ r, s \in R.$$

Beispiele. Sei K ein Körper.

(1) $\mathrm{End}_K(V)$, für einen K-Vektorraum V, ist eine K-Algebra.

(2) $\mathrm{M}_n(K)$ ist eine K-Algebra der Dimension n^2.

(3)* $\mathcal{C}([0,1],\mathbb{R})$, stetige reelle Funktionen auf $[0,1]$, ist eine unendlichdimensionale $\mathbb{R}$-Algebra.

(4)* $K[T]$ ist eine unendlichdimensionale K-Algebra.

Proposition 5.7

Jede endlichdimensionale nullteilerfreie K-Algebra $R \neq 0$ (K ein Körper) ist ein Schiefkörper.

Beweis. Sei $a \in R$, $a \neq 0$. Die Abbildung

$$\lambda_a \colon R \to R,\ x \mapsto ax$$

ist K-linear und – da a kein Nullteiler ist – injektiv, und wegen der Endlichdimensionalität von R auch surjektiv. Insbesondere gibt es ein $x \in R$ mit $1 = \lambda_a(x) = ax$. Aus denselben Gründen gibt es ein $y \in R$ mit $1 = \lambda_x(y) = xy$. Es folgt

$$a = a \cdot 1 = a(xy) = (ax)y = 1 \cdot y = y,$$

d. h. $ax = 1 = xa$, und damit ist a invertierbar. ∎

Definition 5.8

Seien R und S Ringe. Eine Abbildung $f \colon R \to S$ heisst (Ring-) *Homomorphismus* (oder kürzer: *Morphismus*), falls

$$f(x+y) = f(x) + f(y) \quad \text{für alle } x, y \in R$$
$$f(x \cdot y) = f(x) \cdot f(y) \quad \text{für alle } x, y \in R$$
$$f(1_R) = 1_S$$

gilt. (Sind R, S zusätzlich K-Algebren und ist f zusätzlich K-linear, so heisst f ein *Algebrenhomomorphismus*.) Ist f zusätzlich bijektiv, so heisst f ein *Isomorphismus* (von Ringen). Zwei Ringe R und S heissen *isomorph* (Notation: $R \simeq S$), falls es einen Isomorphismus $f \colon R \to S$ gibt.

Definition 5.9

Eine Teilmenge S eines Ringes R heisst *Unterring* (oder *Teilring*), falls gilt

- S ist Untergruppe von $(R,+)$
- $S \cdot S \subseteq S$
- $1_R \in S$.

Dadurch wird S selbst mit den von R induzierten Verknüpfungen zu einem Ring (mit Eins $1_S = 1_R$). Ist zusätzlich R eine K-Algebra und S ein Unterraum, so heisst S *Unteralgebra* von R.

Ist der Unterring S von R ein Körper, so heisst S *Teilkörper* von R. Ist zusätzlich R selbst auch ein Körper, so nennt man R eine *Körpererweiterung* von S.

Beispiele. (1) $\mathbb{Z}$ ist Teilring von $\mathbb{Q}$. $\mathbb{Q}$ ist ein Teilkörper von $\mathbb{R}$.

(2) Sei $f \colon R \to S$ ein Ringhomomorphismus. Dann ist $\mathrm{Bild}(f)$ ein Unterring von S.

(3) Sei R ein Ring. Dann ist durch $h \colon \mathbb{Z} \to R$, $n \mapsto n \cdot 1 = \ldots$ ein Ringhomomorphismus gegeben, der einzige von $\mathbb{Z}$ nach R. Dessen Bild $\mathbb{Z} \cdot 1$ ist der kleinste Unterring von R. Außerdem wird auf diese Weise R zu einer $\mathbb{Z}$-Algebra. (Also ist jeder Ring in natürlicher Weise eine $\mathbb{Z}$-Algebra.)

(4) Ist S ein Unterring von R, so ist die Einbettung $j \colon S \to R$, $x \mapsto x$ ein Ringhomomorphismus.

(5) $A = \mathcal{C}([0,1], \mathbb{R})$. Sei $x \in [0,1]$. Dann ist $e_x \colon A \to \mathbb{R}$, $f \mapsto f(x)$ ein (surjektiver) Ringhomomorphismus.

Aufgaben

Ü 5.1. In jedem Ring gilt $(-1) \cdot (-1) = 1$.

Ü 5.2. [Binomialtheorem] Seien R ein Ring und a, $b \in R$, für die $ab = ba$ gilt. Für jedes $n \geq 0$ gilt

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}.$$

Ü 5.3. Sei $S := \begin{pmatrix} 0 & 0 & 2 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$. Sei K die Menge aller $A \in \mathrm{M}_3(\mathbb{Q})$, für die $AS = SA$ gilt.

(1) Es ist K ein $\mathbb{Q}$-Vektorraum mit Basis E, S, S^2. (E die Einheitsmatrix; was ist S^3?)

(2) Das charakteristische Polynom von S hat keine Nullstelle in $\mathbb{Q}$.

(3) Für jeden Vektor $x \in \mathbb{Q}^3$, $x \neq 0$, gilt, dass x, Sx, S^2x linear unabhängig sind. (Dazu verwende man Teil (2) um zu zeigen:

(i) $Sx \notin \langle x \rangle$; (ii) $S^2x \notin \langle x, Sx \rangle$.

Für (ii) ergänze man x, Sx mit einem y zu einer Basis von $\mathbb{Q}^3$ und betrachte die Darstellungsmatrix der linearen Abbildung $\mathbb{Q}^3 \longrightarrow \mathbb{Q}^3$, $v \mapsto Sv$ bzgl. *dieser* Basis; was folgt für das charakteristische Polynom von S falls (ii) nicht gilt?)

(4) Es ist K ein Integritätsring.

(Seien A und B Matrizen in K mit $AB = 0$. Man nehme an, $B \neq 0$. Dies führt zu $Ax = 0$ mit einem Vektor $x \in \mathbb{Q}^3$, $x \neq 0$. Man verwende Teil (3), um $A = 0$ zu schliessen.)

(5) Es ist K ein (kommutativer) Körper und $K/\mathbb{Q}$ eine Körpererweiterung vom Grad 3. (Wie wird hierbei $\mathbb{Q}$ als *Teil*körper von K aufgefasst?)

6. Ideale und Faktorringe

Proposition 6.1

Sei $f \colon R \to S$ ein Morphismus von Ringen. Dann hat

$$I = \mathrm{Kern}(f) = \{r \in R \mid f(r) = 0_s\}$$

folgende Eigenschaften:

(I1) *$(I, +)$ ist eine Untergruppe von $(R, +)$;*
(I2) *$R \cdot I \subseteq I$ und $I \cdot R \subseteq I$.*

Beweis. Klar. ∎

Definition 6.2

Eine Teilmenge $I \subseteq R$ eines Rings R heisst *Ideal*, falls sie obige Eigenschaften (I1) und (I2) erfüllt. Notation: $I \lhd R$.

Jeder Ring R hat die trivialen Ideale $\{0\}$ und R.

Lemma 6.3

Sei R ein kommutativer Ring und $a \in R$. Dann ist $I = Ra = \{ra \mid r \in R\}$ ein Ideal in R.

Ra heißt (das von a erzeugte) *Hauptideal*.

Satz 6.4

Im Ring $\mathbb{Z}$ ist jedes Ideal ein Hauptideal.

Beweis. Wir hatten schon gesehen, dass die abelsche Gruppe $(\mathbb{Z}, +)$ nur zyklische Untergruppen besitzt, allesamt von der Form $\mathbb{Z} \cdot n$ ($n \in \mathbb{Z}$). Da jedes Ideal in $\mathbb{Z}$ insbesondere eine Untergruppe von $\mathbb{Z}$ ist, folgt sofort die Behauptung. ■

Bemerkung. [Kongruenzen] Sei I ein Ideal in R, seien $a, b \in R$. Man schreibt $a \equiv b \mod I$, falls $a - b \in I$ gilt. ("a kongruent b modulo I") Im Fall $R = \mathbb{Z}$ und $I = \mathbb{Z}n$ schreibt man kürzer $\mod n$.

Definition 6.5

Ein Integritätsbereich, in welchem jedes Ideal ein Hauptideal ist, heißt *Hauptidealring* (oder *-bereich*).

Beispiele. Beispiele für Hauptidealringe:
(1) $\mathbb{Z}$
(2) Jeder Körper.
(3)* Der Polynomring $K[T]$ (K Körper). (Dies wird später gezeigt.)

Satz 6.6

Ein kommutativer Ring R ist genau dann ein Körper, wenn er genau zwei Ideale hat.

Beweis. (1) Seien $\{0\}$ und R die einzigen beiden Ideale in R (also insbesondere $R \neq \{0\}$). Sei $a \in R$ mit $a \neq 0$. Dann ist das von a erzeugte Hauptideal Ra ungleich $\{0\}$, also muss $Ra = R$ gelten. Insbesondere gibt es ein $r \in R$ mit $1 = ra$. Es folgt, dass a invertierbar ist.

(2) Sei R ein Körper. Dann sind die Ideale $\{0\}$ und R verschieden. Sei $I \neq \{0\}$ ein Ideal. Es gibt ein $a \in I$ mit $a \neq 0$. Da a invertierbar ist, gilt $1 = a^{-1}a \in Ra \subseteq I$. Ist nun $r \in R$ beliebig, so folgt $r = r \cdot 1 \in I$. Also gilt $I = R$. ■

Folgerung 6.7

Sei $f\colon K \to R$ ein Homomorphismus, wobei K ein Körper ist und R ein Ring mit $1 \neq 0$. Dann ist f injektiv.

Beweis. Wegen $f(1) = 1$ gilt $f \neq 0$. Also $\mathrm{Kern}(f) \neq K$ und somit $\mathrm{Kern}(f) = \{0\}$. ■

Satz und Definition 6.8

Sei R ein Ring und $I \subseteq R$ ein Ideal. Dann wird die Faktorgruppe R/I von $(R, +)$ nach I zu einem Ring vermöge der Multiplikation

$$[x] \cdot [y] \stackrel{def}{=} [xy],$$

wobei hier $[x]$ für $x \in R$ die Nebenklasse $x + I \in R/I$ bezeichnet. Es ist $1_{R/I} = [1_R]$. Der Ring R/I heisst der Faktorring *von R* nach *dem Ideal I (oder:* modulo *I).*

Beweis. Ähnlich wie im Gruppenfall ist hier der wesentliche Punkt zu zeigen, dass die Multiplikation wohldefiniert ist. Dazu verwendet man die Idealeigenschaft. (Details siehe Vorlesung.) ■

Satz 6.9 (*Homomorphiesatz für Ringe*)

Seien R und S Ringe, und sei $f\colon R \to S$ ein Ringhomomorphismus. Dann ist $I = \mathrm{Kern}(f)$ ein Ideal in R. Es gibt genau einen Ringhomomorphismus

$\bar{f}\colon R/I \to S$ mit $\bar{f} \circ \nu = f$, wobei $\nu\colon R \to R/I$, $a \mapsto [a]$ der natürliche surjektive Ringhomomorphismus ist. Ferner ist $\bar{f}$ injektiv.

Beweis. Der Homomorphiesatz für Gruppen liefert einen eindeutigen Gruppenhomomorphismus $\bar{f}\colon R/I \to S$, zwischen den additiven abelschen Gruppen $(R/I, +)$ und $(S, +)$, für den $\bar{f} \circ \nu = f$ gilt, und $\bar{f}$ ist injektiv. Es ist nur noch zu zeigen, dass ν und $\bar{f}$ auch *Ring*homomorphismen sind. Dies rechnet man leicht nach. (Siehe Vorlesung für Details.) ∎

Aufgaben

Ü 6.1. Sei V ein endlich-dimensionaler K-Vektorraum über dem Körper K der Dimension $n \geq 1$, sei R der Endomorphismenring $\mathrm{End}_K(V)$ ($\simeq \mathrm{M}_n(K)$). Man zeige, dass R nur die trivialen Ideale $\{0\}$ und R enthält. (Interessant hierbei ist u. a., dass R für $n \geq 2$ *kein* Schiefkörper ist, nicht einmal nullteilerfrei.)

Ü 6.2. Sei I ein Ideal in R. Dann ist Kongruenz $\equiv$ modulo I eine Äquivalenzrelation auf der Menge der Elemente von R, und es gilt:

- Aus $a \equiv b$ und $c \equiv d$ folgen $a + c \equiv b + d$, $a - c \equiv b - d$ und $ac \equiv bd$.

7. Der Faktorring $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$

Für eine natürliche Zahl $n \geq 1$ sei $\mathbb{Z}_n$ der Faktorring $\mathbb{Z}/n\mathbb{Z}$, auch der *Restklassenring modulo n* genannt.

Satz 7.1

Für $n \geq 1$ sind äquivalent:

(1) *$\mathbb{Z}_n$ ist ein Körper.*

(2) *$\mathbb{Z}_n$ ist ein Integritätsbereich.*

(3) *n ist eine Primzahl.*

Beweis. (1)⇔(2): Da $\mathbb{Z}_n$ endlich ist, folgt dies aus Proposition 5.5 und Proposition 5.3.

(2)⇒(3): Sei n keine Primzahl. Dann gibt es $a, b \in \mathbb{Z}$ mit $1 < a, b < n$ mit $n = a \cdot b$. Für die Klassen in $\mathbb{Z}_n$ folgt dann $[a] \neq 0$, $[b] \neq 0$, aber $[a] \cdot [b] = [n] = [0]$, also ist $\mathbb{Z}_n$ nicht integer.

(3)⇒(2): Sei $n = p$ eine Primzahl. Wir verwenden folgende Eigenschaft einer Primzahl ("Euklids Lemma"): teilt p ein Produkt ab, so teilt p einen der Faktoren, a oder b. Seien nun $a, b \in \mathbb{Z}$ mit $[a] \cdot [b] = [0]$. Dann $[ab] = [a][b] = [0]$, also $ab \in \mathbb{Z} \cdot p$. Das bedeutet $p \mid ab$, also teilt p einen der Faktoren, was $[a] = 0$ oder $[b] = 0$ bedeutet. Also ist $\mathbb{Z}_p$ integer. ∎

Aufgaben

Ü 7.1. Sei $n \geq 1$. Für $a \in \mathbb{Z}$ ist $[a]$ genau dann eine Einheit im Restklassenring $\mathbb{Z}/n\mathbb{Z}$, wenn a und n teilerfremd sind, d. h. $\mathrm{ggT}(a, n) = 1$.

Ü 7.2. [Charakteristik und Primkörper eines Körpers] Sei K ein Körper mit Einselement 1_K. Für $n \in \mathbb{Z}$ sei

$$n \cdot 1_K := \begin{cases} \sum_{i=1}^{n} 1_K \in K & \text{falls } n \geq 0 \\ -\sum_{i=1}^{-n} 1_K \in K & \text{sonst.} \end{cases}$$

Sei $p := \min\{n \in \mathbb{N} \mid n \geq 1,\ n \cdot 1_K = 0\}$, falls das Minimum existiert; falls nicht, so sei $p := 0$. Man zeige:

(1) Für $n, m \in \mathbb{Z}$ ist $(n \cdot m) \cdot 1_K = (n \cdot 1_K) \cdot (m \cdot 1_K)$.

(2) Es gilt $p = 0$, oder p ist eine Primzahl. (Es heisst $\mathrm{Char}(K) := p$ die Charakteristik von K.)

(3) Es ist $\Pi(K) := \{\frac{n \cdot 1_K}{m \cdot 1_K} \mid n, m \in \mathbb{Z},\ m \cdot 1_K \neq 0\}$ ein Teilkörper von K.

(4) Es ist $\Pi(K)$ der *kleinste* Teilkörper von K. (Dieser heisst der Primkörper von K.)

(5) Ist $p = 0$, so ist $\Pi(K)$ isomorph zu $\mathbb{Q}$. Ist $p > 0$, so hat $\Pi(K)$ genau p Elemente und ist isomorph zum Körper $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$.

(6) Jeder endliche Körper K besteht aus p^n Elementen für eine Primzahl p und ein $n \geq 1$. Jeder solche enthält einen zu $\mathbb{F}_p$ isomorphen Teilkörper.

KAPITEL III

Gruppenaktionen

1. Grundlegende Eigenschaften und Beispiele

Definition 1.1

Sei G eine Gruppe und M eine Menge. Unter einer *Aktion* (oder auch: *Operation*) von G auf M verstehen wir eine Abbildung

$$G \times M \to M,\ (g, m) \mapsto g.m,$$

die den folgenden Bedingungen genügt:

(A1) $e.m = m$ für alle $m \in M$;
(A2) $g.(h.m) = (g \cdot h).m$ für alle g, $h \in G$, $m \in M$.

Beispiele. (1) $\mathrm{GL}_n(K)$ operiert auf K^n.
(2) Gruppe G operiert auf sich selbst durch (Links-) Multiplikation.
(3) Gruppe G operiert auf sich selbst durch Konjugation.

Definition 1.2

Sei $G \times M \to M$, $(g, m) \mapsto g.m$ eine Gruppenaktion und sei $m \in M$.

(a) $B = G.m = \{g.m \mid g \in G\}$ heißt die *G-Bahn* (auch: *Orbit*) von m (unter der Aktion von G).
(b) Mit $M/G = \{G.m \mid m \in M\}$ bezeichnen wir die Menge aller G-Bahnen von M, den sog. *Bahnenraum*.
(c) Die Menge $\mathrm{St}(m) = \mathrm{St}_G(m) = \{g \in G \mid g.m = m\}$ ist eine Untergruppe von G; sie heißt die *Standuntergruppe* (auch: *Isotropiegruppe*, oder *Stabilisator*) von m.

Lemma 1.3 (*Bahnenlemma*)

G operiere auf M. Sei $m \in M$.

(a) *Die Abbildung*

$$\varphi\colon G/\mathrm{St}(m) \to G.m,\ g \cdot \mathrm{St}(m) \mapsto g.m$$

ist eine Bijektion. Falls G endlich ist, ist also $|G.m| = [G : \mathrm{St}(m)]$ stets ein Teiler von $|G|$.

(b) *Ist $m' = g.m$, so ist*

$$\mathrm{St}(m') = g\,\mathrm{St}(m)g^{-1}.$$

Beweis. (Vgl. Vorlesung.) ∎

Satz 1.4 (*Bahnenzerlegung*)

(a) *Zwei Bahnen sind gleich oder disjunkt.*
(b) *Es gilt*

$$M = \coprod_{B \in M/G} B.$$

Beweis. (Vgl. Vorlesung.) ∎

Beispiele. (1) Die Gruppe $\mathbb{T} = \{z \in \mathbb{C} \mid |z| = 1\}$ operiert auf der Menge $\mathbb{C}$ der komplexen Zahlen durch Multiplikation

$$\mathbb{T} \times \mathbb{C} \to \mathbb{C},\ (t, x) \mapsto tx.$$

Die Bahnen sind Kreise um 0 mit einem Radius $r \geq 0$. Dieses Beispiel verdeutlicht besonders gut die Bahnenzerlegung. Wir sehen hier auch, dass die Bahnen unterschiedliche Mächtigkeiten haben können.

(2) Sei U eine Untergruppe der Gruppe G. Dies liefert die U-Aktion auf G,

$$U \times G \mapsto G,\ (u, g) \mapsto ug.$$

Die Bahnen sind hier die Rechtsnebenklassen Ug von U, die Standuntergruppen sind trivial. Alle Bahnen haben die gleich Mächtigkeit, da $U \to Ug$, $u \mapsto ug$ bijektiv. Falls G endlich ist, liefert die Bahnenzerlegung

$$|G| = |U| \cdot |G/U|,$$

den bekannten Satz von Lagrange.

(3) G operiert auf G durch Konjugation

$$(g, x) \mapsto gxg^{-1}.$$

Die Bahn zu $x \in G$ ist die Konjugationsklasse $C(x) = \{gxg^{-1} \mid g \in G\}$, die gleichmächtig ist zu $G/N(x)$, wobei $N(x)$ die Standuntergruppe $\{g \in G \mid gxg^{-1} = x\}$ ist, also der Zentralisator von x. Die Bahnenzerlegung führt – für endliches G – zur Klassengleichung.

(4) Sei σ eine Permutation von $1, \ldots, n$. Die zyklische Gruppe $G = \langle\sigma\rangle$ operiert auf $\{1, \ldots, n\}$. Die Bahn von i erhalten wir duch Bildung der Sequenz

$$\sigma(i),\ \sigma^2(i), \ldots,\ \sigma^j(i) = i \quad j > 0 \text{ minimal.}$$

Die Zahlen $1, \ldots, n$ werden dadurch in disjunkte Bahnen zerlegt. Dies korrespondiert zur sog. *Zykelzerlegung* von σ. *Jede Permutation zerlegt sich in paarweise disjunkte Zykel.*

2. Die Sylowsätze

Satz 2.1 (*1. Sylowscher Satz (1872)*)

Sei $|G| = p^n \cdot m$ mit p prim, m teilerfremd zu p, und $n \geq 1$. Dann besitzt G mindestens eine Untergruppe P der Ordnung p^n.

Jede solche Untergruppe heisst *p-Sylowgruppe* von G.

Beweis. Induktion nach $|G|$. Für $|G| = 1$ oder $|G| = p$ ist alles klar. Wir nehmen an, dass für Gruppen einer Ordnung $< |G|$ die Aussage gilt und zeigen sie für G. Sei $Z = Z(G)$ das Zentrum von G. Dann operiert G auf der Komplementmenge $G \setminus Z$ durch Konjugation

$$G \times \big(G \setminus Z\big) \to G \setminus Z,\ (g, x) \mapsto gxg^{-1}.$$

Die Bahnen der Operation sind die Konjugationsklassen $C(g)$ nichtzentraler Elemente g, deren Standuntergruppe $\mathrm{St}(g) = Z(g) = \{h \in G \mid hg = gh\}$ deren Zentralisator von g ist. Für nichtzentrales g gilt $Z(g) \neq G$. Zwei Fälle treten auf:

1. Fall: Es gibt ein $g \in G \setminus Z$, so dass p^n die Ordnung von $Z(g)$ teilt. Wegen $Z(g) \neq G$ lässt sich auf $Z(g)$ die Induktionsvoraussetzung anwenden: Es hat dann $Z(g)$, folglich auch G, eine Untergruppe der Ordnung p^n.

2. Fall: Für kein $g \in G \setminus Z$ ist p^n ein Teiler von $|Z(g)|$. Wegen (Bahnenlemma)

$$p^n \cdot m = |G| = |Z(g)| \cdot |C(g)|$$

muss dann p ein Teiler von $|C(g)|$ sein; dies für jedes $g \in G \setminus Z$. Da

$$G \setminus Z = \coprod_{|C(g)|>1} C(g)$$

(Bahnenzerlegung) ist dann p ein Teiler von $|G \setminus Z| = |G| - |Z|$ und p folglich ein Teiler von Z. Nach dem Satz von Cauchy (nur die kommutative Version benötigt) hat Z eine Untergruppe U der Ordnung p. Wegen $U < Z$ ist U ein Normalteiler in G, also können wir die Faktorgruppe G/U bilden und auf G/U die Induktionsvoraussetzung anwenden. Es gibt also eine Untergruppe $\overline{P}$ von G/U der Ordnung p^{n-1}. Definieren wir – mittels des natürlichen Homomorphismus $\nu\colon G \to G/U$ – die Untergruppe P von G als Urbild $P = \nu^{-1}(\overline{P})$, so folgt

$$P/U = \nu(P) = \overline{P},$$

also $|P| = |U| \cdot |\overline{P}| = p \cdot p^{n-1} = p^n$. ∎

Satz 2.2 (*2. Sylowscher Satz (1872)*)

Je zwei p-Sylowgruppen von G sind zueinander konjugiert.

Insbesondere sind alle p-Sylowgruppen von G zueinander isomorph.

Satz 2.3 (*3. Sylowscher Satz (1872)*)

Sei $|G| = p^n \cdot m$ mit p prim, m teilerfremd zu p, und $n \geq 1$. Die Anzahl $\alpha(p)$ der p-Sylowgruppen von G ist ein Teiler von m und von der Form $\alpha(p) = 1 + kp$ für ein $k \geq 0$.

Die Beweise des 2. und des 3. Sylowsatzes folgen mit dem folgenden Lemma.

Lemma 2.4

Seien P eine p-Sylowgruppe und U eine p-Untergruppe von G. Gilt $U \subseteq N(P) := \{g \in G \mid gPg^{-1} = P\}$, dem sog. Normalisator *von P, so gilt schon $U \subseteq P$.*

Beweis. Aus $U < N(P)$ folgt $UP < N(P)$, und P ist folglich normal in UP. Nach dem 1. Isomorphiesatz (Übung II.2.1) ist $[UP : P] = [U : P \cap U]$, und dies ist einerseits ein Teiler von $|U| = p^\ell$ (aus dem rechten Term), andererseits aber nicht durch p teilbar (aus dem linken Term). Es folgt $[UP : P] = 1$, d. h. $UP = P$, und damit $U \subseteq P$. ∎

Operiert die Gruppe G auf der Menge M, so ist

$$M^G := \{m \in M \mid g.m = m \text{ für alle } g \in G\}$$

die Menge der *Fixpunkte* dieser Aktion. Fixpunkte sind also gerade die Elemente mit einelementiger G-Bahn bzw. mit ganz G als Standuntergruppe. Die Bahnenzerlegung liefert (falls G, M endlich)

$$|M| = |M^G| + \sum_{|B|>1} |B|, \tag{2.1}$$

wobei über alle G-Bahnen B mit mehr als einem Element summiert wird; ist hierbei G eine p-Gruppe, so folgt aus dem Bahnenlemma $p \mid |B|$ und daher $p \mid |M| \Leftrightarrow p \mid |M^G|$.

Beweis vom 2. und 3. Sylowsatz. (2.) Sei U eine p-Untergruppe von G. Sei P eine beliebige p-Sylowgruppe von G. (Eine solche existiert nach dem 1. Sylowsatz.) Wir zeigen, dass es ein $g \in G$ gibt mit $U \subseteq gPg^{-1}$. (Daraus folgt dann mit $|U| = p^n$ insbesondere der 2. Sylowsatz.) Sei $M = \{gPg^{-1} \mid g \in G\}$ die Menge aller zu P konjugierten (Sylow-) Gruppen. Auf dieser Menge operiert G durch Konjugation mit einer Bahn, trivialerweise. Hier gilt $\mathrm{St}_G(P) = \{g \in G \mid$

$gPg^{-1} = P\} = N(P)$, und wegen $P < N(P)$ ist $|M| = |G.P| = [G : N(P)]$ (Bahnenlemma) ein Teiler von $[G : P] = m$, wird also nicht von p geteilt.

Die Untergruppe U operiert ebenfalls durch Konjugation auf M. Aus der Formel (2.1) (für U anstatt G) schließen wir, dass $M^U \neq \emptyset$ gilt. Sei $Q \in M$ ein Fixpunkt. Also $uQu^{-1} = Q$ für alle $u \in U$. Dies bedeutet $U \subseteq N(Q)$. Aus dem Lemma folgt $U \subseteq Q$. Wegen $Q \in M$ gibt es $g \in G$ mit $Q = gPg^{-1}$.

(3.) Sei $\mathscr{S}$ die Menge aller p-Sylowgruppen von G. Darauf operiert G durch Konjugation. Nach dem 2. Sylowschen Satz haben wir eine einzige G-Bahn und $\mathscr{S} = M$ wie oben. Nach dem vorherigen Beweisteil ist $\alpha(p) = [G : N(P)]$ ein Teiler von m.

Es operiert auch die Gruppe P auf $\mathscr{S}$ durch Konjugation. Sei $Q \in \mathscr{S}$ ein Element der Fixpunktmenge $\mathscr{S}^P$. Aus dem vorherigen Beweisteil (mit $U = P$) folgt $P \subseteq Q$, und wegen Anzahlsgleichheit sogar $P = Q$. Es ist also P der einzige Fixpunkt dieser P-Aktion. Aus der zu (2.1) analogen Formel ergibt sich $\alpha(p) = |\mathscr{S}| = 1 + kp$ für ein $k \geq 0$. ∎

3. Eine Anwendung: Gruppen der Ordnung 15 sind zyklisch

Sei G eine Gruppe der Ordnung $15 = 3 \cdot 5$. Für die Anzahlen $\alpha(3)$ bzw. $\alpha(5)$ der 3- bzw. 5-Sylowgruppen gilt nach dem dritten Sylowschen Satz $\alpha(3) \mid 5$, $\alpha(5) \mid 3$, und zusätzlich $\alpha(3) = 1 + \ell 3$ sowie $\alpha(5) = 1 + k5$ für $\ell, k \geq 0$. Also ist nur $\alpha(3) = 1 = \alpha(5)$ möglich. Das heisst, es gibt genau eine Untergruppe U der Ordnung 3 und genau eine Untergruppe V der Ordnung 5. Jedes Element in $G \setminus (U \cup V)$ hat die Ordnung 15, d. h. erzeugt G.

Allgemeiner:

Satz 3.1

Seien $p < q$ Primzahlen mit $p \nmid (q-1)$. Dann ist jede Gruppe der Ordnung $n = pq$ zyklisch, d. h. isomorph zu $\mathbb{Z}_{pq}$.

Beweis. Es gilt $\alpha(q) \in \{1, p\}$ sowie $\alpha(q) = 1 + \ell q$ für ein $\ell \geq 0$. Wegen $p < q$ kann nur $\alpha(q) = 1$ gelten. Weiter gilt $\alpha(p) \in \{1, q\}$ und $\alpha(p) = 1 + kp$ für ein $k \geq 0$. Wäre $\alpha(p) = q$, so folgte $kp = (q-1)$, Widerspruch zu der Annahme, dass $p \nmid (q-1)$ gilt. Also gibt es genau eine p- und genau eine q-Sylowgruppe von G. Jedes Element außerhalb dieser hat die Ordnung pq. Davon gibt es $pq - p - q + 1 = (p-1)(q-1) \geq q - 1 \geq 4$ viele. ∎

4. Die Anzahl der Bahnen

Die Gruppe G operiere auf der Menge M. Für $g \in G$ sei $\mathrm{Fix}(g) = \{m \in M \mid g.m = m\}$ die Menge aller *Fixpunkte* von g in M. (Es ist also $M^G = \bigcap_{g \in G} \mathrm{Fix}(g)$.)

Proposition 4.1 (*Fixpunktformel*)

Die endliche Gruppe G operiere auf der endlichen Menge M.

$$|M/G| = \frac{1}{|G|} \sum_{g \in G} |\,\mathrm{Fix}(g)|.$$

In Worten: Die Anzahl der Bahnen ist gleich dem Mittelwert der Anzahl der Fixpunkte.

Beweis. Sei

$$F = \{(g, m) \mid g \in G,\ m \in M,\ g.m = m\}.$$

Es gilt

$$F = \coprod_{g \in G} \{g\} \times \mathrm{Fix}(g) = \coprod_{m \in M} \mathrm{St}(m) \times \{m\},$$

also

$$|F| = \sum_{g \in G} |\operatorname{Fix}(g)| = \sum_{m \in M} |\operatorname{St}(m)|.$$

Seien $B_1, \ldots, B_r$ die verschiedenen Bahnen, $r = |M/G|$. Für alle Punkte einer Bahn B_i sind die Standuntergruppen konjugiert, haben also dieselbe Elementanzahl. Es folgt

$$|F| = \sum_{m \in M} |\operatorname{St}(m)| = \sum_{i=1}^{r} |B_i| \cdot |\operatorname{St}(m_i)| = r \cdot |G|$$

mit $m_i \in B_i$. Setzt man alles zusammen, folgt die Behauptung. ■

Beispiel. Die symmetrische Gruppe $\mathbb{S}_n$ operiert auf $\{1, \ldots, n\}$ mit nur einer Bahn. Folglich ist

$$1 = \frac{1}{n!} \sum_{\sigma \in \mathbb{S}_n} |\operatorname{Fix}(\sigma)|.$$

Daher hat eine Permutation "im Durchschnitt" einen Fixpunkt.

5. Einfache Gruppen

Definition 5.1

Eine Gruppe G heisst *einfach*, wenn $G \neq \{e\}$ gilt, und wenn G und $\{e\}$ die einzigen Normalteiler von G sind.

Proposition 5.2

Eine endliche abelsche Gruppe ist einfach genau dann, wenn sie von Primzahlordnung ist. ■

Dies folgt unmittelbar aus den Sätzen von Lagrange bzw. Cauchy. Wir konzentrieren uns bei der Untersuchung einfacher Gruppen daher auf den nicht-abelschen Fall.

Proposition 5.3

Es gibt keine einfache Gruppe der Ordnung p^2 bzw. pq (p, q prim).

Beweis. (a) Jede Gruppe der Ordnung p^2 ist abelsch. Eine abelsche Gruppe ist aber nur einfach, wenn $|G|$ ein Primzahl ist.

(b) Sei G von der Ordnung pq mit $p < q$ prim. Wir hatten weiter oben gesehen, dass $\alpha(q) = 1$ gilt; das bedeutet, dass es genau eine q-Sylowgruppe U von G gibt. Da alle Konjugierten einer q-Sylowgruppe wieder eine q-Sylowgruppe ist, folgt, dass U ein Normalteiler ist. Also ist G nicht einfach. ■

Als wichtiges Argument halten wir fest (die Umkehrung folgt aus dem zweiten Sylowschen Satz):

Lemma 5.4

Sei P eine p-Sylowgruppe der endlichen Gruppe G. Dann gilt

$$P \text{ ist Normalteiler} \;\Leftrightarrow\; \alpha(p) = 1.$$

Der Fall pq im obigen Resultat kann verallgemeinert werden:

Proposition 5.5

Es gibt keine einfache Gruppe der Ordnung ap (p prim, $1 < a \leq p$).

Beweis. Gelte $|G| = ap$. Wir können $a < p$ annehmen. Nach dem 3. Sylowsatz ist $\alpha(p)$ ein Teiler von a und von der Form $1 + kp$ für ein $k \geq 0$. Wegen $a < p$ folgt, dass nur $\alpha(p) = 1$ gelten kann. Somit ist nach dem Lemma *die* p-Sylowgruppe von G ein nicht-trivialer Normalteiler. ∎

Bemerkung. Es gilt der $p^\alpha q^\beta$-Satz von Burnside: *Es gibt keine einfache Gruppe der Ordnung* $p^\alpha q^\beta$ *(p, q prim, α, $\beta \geq 1$).*

Die Gruppe G operiere auf der Menge M. Wir sagen, dass diese Operation *transitiv* ist, wenn es genau eine G-Bahn von M gibt: $M = G.m$ (für ein, und damit alle, $m \in M$). Anders formuliert: Zu m, $m' \in M$ gibt es stets $g \in G$ mit $m' = g.m$.

Proposition 5.6 (*Poincaré*)

Sei G eine nicht-abelsche einfache Gruppe, die transitiv auf einer endlichen Menge M operiert, mit $n = |M| \geq 2$. Dann ist G isomorph zu einer Untergruppe der alternierenden Gruppe $\mathbb{A}_n$.

Beweis. Für jedes $g \in G$ bezeichne

$$g_M \colon M \to M,\ m \mapsto g.m$$

die Operation von g auf M. Wie im Beweis vom Satz von Cayley folgt, dass

$$\varphi \colon G \to \mathbb{S}(M),\ g \mapsto g_M$$

ein Gruppenhomomorphismus ist. Da $|M| \geq 2$ und G transitiv operiert, ist φ nicht trivial (d. h. $\mathrm{Kern}(\varphi) \neq G$). Da G einfach ist, folgt $\mathrm{Kern}(\varphi) = \{e\}$, also ist φ injektiv. Wegen $|M| = n$ können wir $\mathbb{S}(M)$ mit $\mathbb{S}_n$ identifizieren und erhalten somit eine Einbettung

$$\varphi \colon G \to \mathbb{S}_n.$$

Verkettung mit der Signatur $\mathrm{sgn} \colon \mathbb{S}_n \to \mathbb{Z}_2$ ergibt einen Homomorphismus $\mathrm{sgn} \circ \varphi \colon G \to \mathbb{Z}_2$, der wegen der Voraussetzung an G nicht surjektiv sein kann (andernfalls hätte G eine Untergruppe vom Index 2, die dann ein Normalteiler wäre). Also ist $\mathrm{sgn} \circ \varphi$ der triviale Homomorphismus und

$$G \simeq \varphi(G) < \mathbb{A}_n.$$

∎

Folgerung 5.7

Sei $n \geq 2$. Sei G eine nicht-abelsche einfache Gruppe. Es gelte eine der drei Bedingungen:

(i) *G hat eine Untergruppe U vom Index n; oder*
(ii) *G hat eine n-elementige Konjugationsklasse $C(g)$; oder*
(iii) *es gibt einen Primteiler p von $|G|$ mit $\alpha(p) = n$.*

Dann ist G zu einer Untergruppe von $\mathbb{A}_n$ isomorph.

Beweis. G operiert transitiv auf
(i) $G/U = \{gU \mid g \in G\}$ via Linksmultiplikation; bzw.
(ii) $C(g)$ via Konjugation; bzw.
(iii) der Menge der p-Sylowgruppen von G via Konjugation.
In jedem der drei Fälle folgt die Behauptung nun aus dem Satz von Poincaré. ∎

Satz 5.8

Es gibt keine nicht-abelsche einfache Gruppe G mit $1 \leq |G| < 60$.

Beweis. Wir können Primzahlpotenzen nach Proposition I.5.7 sowie Ordnungen ap (p prim, $1 < a < p$) ausschließen. Bleiben die Ordnungen

$$12,\ 18,\ 24,\ 30,\ 36,\ 40,\ 45,\ 48,\ 50,\ 54,\ 56.$$

(a) 18, 50, 54 haben die Form $2 \cdot p^k$ ($2 \neq p$ prim). Die p-Sylowgruppe hat Index 2, ist also Normalteiler.

(b) 12, 24, 48 haben die Form $3 \cdot p^k$ ($p = 2$ prim). Die p-Sylowgruppe hat Index 3, Widerspruch zu Poincaré (Folgerung 5.7).

(c) 40, 45 haben die Form $5 \cdot p^k$ (p prim). Die p-Sylowgruppe hat daher den Index 5. Somit ist G isomorph zu einer Untergruppe von $\mathbb{A}_5$, aber $|G| \nmid 60$, Widerspruch.

(d) 36. Hier hat eine 3-Sylowgruppe Index 4, also $G < \mathbb{A}_4$, Widerspruch.

(e) 30. Übung 7.1.

(f) 56. Übung 7.1. ■

Proposition 5.9

Jede einfache Gruppe der Ordnung 60 *ist isomorph zur alternierenden Gruppe* $\mathbb{A}_5$.

Beweis. Sei G einfach mit $|G| = 60$. Da 60 keine Primzahl ist, ist G nicht abelsch. Da $60 = 2^2 \cdot 3 \cdot 5$ folgt $\alpha(5) \in \{1, 6\}$. Wegen der Einfachheit von G scheidet $\alpha(5) = 1$ aus, somit gilt $\alpha(5) = 6$. Ferner ist $\alpha(2) \in \{3, 5, 15\}$ und $\alpha(3) \in \{4, 10\}$. Wegen des Satzes von Poincaré sind nur $\alpha(2) = 15$ und $\alpha(3) = 10$ von Interesse. (Im Falle $\alpha(2) = 5$ wäre $G < \mathbb{A}_5$, also $G \simeq \mathbb{A}_5$; im dem Fall wären wir also fertig. Der Fall $\alpha(3) = 4$ ist nicht möglich, da nach Poincaré $G < \mathbb{A}_4$ folgen würde.) Also:

$$\alpha(2) = 15,\ \alpha(3) = 10,\ \alpha(5) = 6.$$

Wir zeigen nun, dass G eine Untergruppe vom Index 5 besitzt. Dazu untersuchen wir die 15 2-Sylowgruppen von G, die je 4 Elemente haben. Falls je zwei verschiedene 2-Sylowgruppen $U \neq V$ einen trivialen Durchschnitt haben, folgt

$$|G| \geq 1 + 15 \cdot 3 + 10 \cdot 2 + 6 \cdot 4 = 90,$$

Widerspruch. Also gibt es zwei 2-Sylowgruppen $U \neq V$ mit $e \neq x \in U \cap V$. Als Untergruppen der Ordnung 4 sind U und V abelsch, somit umfasst der Zentralisator $Z(x)$ sowohl U als auch V, $[G : Z(x)]$ ist daher ein echter Teiler von $[G : U] = 3 \cdot 5$. Wegen des Satzes von Poincaré ist $[G : Z(x)] = 3$ nicht möglich. $[G : Z(x)] = 1$ ist ebenfalls nicht möglich, da dies sonst $e \neq x \in Z(G)$ impliziert und $Z(G)$ dann ein nichttrivialer Normalteiler von G wäre.

Also ist $[G : Z(x)] = 5$, und nach dem Satz von Poincaré G dann isomorph zu $\mathbb{A}_5$. ■

Bemerkung. *Es gibt keine nicht-abelsche einfache Gruppe G mit* $60 < |G| < 168$. Dies zeigt man (Übung 7.4) mit den gleichen Methoden (Sylow, Poincaré, ...) ähnlich wie oben.

6. Einfachheit der alternierenden Gruppe $\mathbb{A}_5$

Lemma 6.1

(a) *Für $n \geq 3$ wird $\mathbb{A}_n$ von 3-Zykeln erzeugt.*

(b) [Cauchy] *Für $n \geq 5$ sind je zwei 3-Zykeln in $\mathbb{A}_n$ zueinander konjugiert.*

Beweis. (a) Die Elemente aus $\mathbb{A}_n$ sind gerade die Produkte geradzahlig vieler Transpositionen. Es genügt daher zu zeigen, dass das Produkt zweier Transpositionen $(a\,b)$ und $(c\,d)$ ein Produkt von 3-Zykeln ist. Haben sie genau ein Element gemeinsam, etwa $b = c$, so gilt $(a\,b)(b\,d) = (d\,a\,b)$. Sind sie disjunkt, so gilt $(a\,b)(c\,d) = (c\,b\,a)(c\,d\,a)$.

(b) Ist σ in $\mathbb{S}_n$, so gilt offenbar $\sigma(a\,b\,c)\sigma^{-1} = (\sigma(a)\,\sigma(b)\,\sigma(c))$. Sind $(a\,b\,c)$ und $(a'\,b'\,c')$ zwei 3-Zykel, so gibt es $\sigma \in \mathbb{S}_n$ mit $\sigma(a) = a'$, $\sigma(b) = b'$, $\sigma(c) = c'$, was zeigt, dass die beiden 3-Zykel in $\mathbb{S}_n$ konjugiert sind. Ist dabei σ selbst noch

nicht in $\mathbb{A}_n$, so können wir σ mit $\tau = (d\,e)$ verknüpfen, wobei d und e verschieden sind von a, b, c; dies geht, weil $n \geq 5$ gilt. Es ist dann $\sigma\tau \in \mathbb{A}_n$. ∎

Satz 6.2 (*Jordan (1870)*)

Für $n \geq 5$ ist die alternierende Gruppe $\mathbb{A}_n$ einfach.

Beweis. Sei $N \neq \{e\}$ ein Normalteiler in $\mathbb{A}_n$. Wir zeigen, dass N einen 3-Zykel enthält. Aus Lemma 6.1 folgt dann $N = \mathbb{A}_n$.

Sei $1 \neq \sigma \in N$. Es gibt eine Darstellung

$$\sigma = \sigma_1 \circ \ldots \circ \sigma_r$$

von σ in disjunkte Zykeln (vgl. Bahnenzerlegung). Da disjunkte Zykeln miteinander kommutieren, können wir sie der Länge nach ordnen, also ohne Einschränkung gelte $\ell(\sigma_1) \geq \ell(\sigma_2) \geq \ldots \geq \ell(\sigma_r) \geq 2$, wobei $\ell(\sigma_i) = \ell_i$, wenn σ_i ein ℓ_i-Zykel ist.

1. Fall: $\ell_1 \geq 4$. Sei etwa $\sigma_1 = (a\ b\ c\ d \ldots)$. Mit $\tau = (a\ b\ c) \in \mathbb{A}_n$ gilt

$$(a\ d\ b) = (b\ c\ d)(c\ b\ a) = (\sigma\tau\sigma^{-1})\tau^{-1} = \sigma(\tau\sigma^{-1}\tau^{-1}) \in N.$$

2. Fall: $\ell_1 = 3$. Im Falle $\sigma = \sigma_1$ ist die Behauptung richtig. Sei also $r \geq 2$, seien $\sigma_1 = (a\ b\ c)$ und $\sigma_2 = (d\ e\ f)$ oder $\sigma_2 = (d\ e)$. Mit $\tau = (a\ b\ d) \in \mathbb{A}_n$ folgt

$$(a\ d\ c\ e\ b) = (b\ c\ e)(d\ b\ a) = (\sigma\tau\sigma^{-1})\tau^{-1} = \sigma(\tau\sigma^{-1}\tau^{-1}) \in N.$$

Nimmt man $(a\ d\ c\ e\ b)$ statt σ, so können wir den 1. Fall (mit $\sigma = \sigma_1$) anwenden.

3. Fall: $\ell_1 = 2$. Dann sind $\sigma_1, \ldots, \sigma_r$ disjunkte Transpositionen, und $r \geq 2$, etwa $\sigma_1 = (a\ b)$, $\sigma_2 = (c\ d)$. Sei $e \neq a, b, c, d$ (möglich wegen $n \geq 5$). Für $\tau = (a\ c\ e) \in \mathbb{A}_n$ folgt

$$(b\ d\ \sigma(e))(e\ c\ a) = (\sigma\tau\sigma^{-1})\tau^{-1} = \sigma(\tau\sigma^{-1}\tau^{-1}) \in N.$$

Gilt dabei $\sigma(e) = e$, so ist dies Element $(a\ b\ d\ e\ c)$, und wir können den 1. Fall anwenden. Gilt $\sigma(e) \neq e$, so sind $(b\ d\ \sigma(e))$ und $(e\ c\ a)$ disjunkt (denn $\sigma(e) \neq \sigma(d) = c$ und $\sigma(e) \neq \sigma(b) = a$). Nimmt man daher $(b\ d\ \sigma(e))(e\ c\ a)$ statt σ, so folgt die Behauptung aus dem 2. Fall. ∎

Bemerkung. Die $\mathrm{GL}_3(\mathbb{F}_2)$ ist einfach von der Ordnung 168. Bis zur Ordnung 1000 sind die Ordnungen 360, 504 und 660 die einzigen weiteren, zu denen nicht-abelsche einfache Gruppen existieren.

7. Auflösbare Gruppen

Definition 7.1

Sei G eine Gruppe. Eine Kette von Untergruppen

$$\{e\} = U_0 \subseteq U_1 \subseteq U_2 \subseteq \ldots \subseteq U_{n-1} \subseteq U_n = G$$

heißt eine *Normalreihe* für G, falls

- U_{i-1} ein Normalteiler in U_i ist für jedes $i = 1, \ldots, n$.

Wir drücken dies rein symbolisch auch so aus:

$$\{e\} = U_0 \lhd U_1 \lhd U_2 \lhd \ldots \lhd U_{n-1} \lhd U_n = G. \tag{7.1}$$

Die Faktorgruppen U_i/U_{i-1} $(i = 1, \ldots, n)$ heißen die *Faktoren* der Normalreihe. Die Normalreihe heißt *abelsch* (bzw. *zyklisch*, *prim-zyklisch*, *Kompositionsreihe*), falls alle Faktoren abelsch (bzw. zyklisch, zyklisch von Primzahlordnung, einfach) sind.

Offenbar ist G endlich genau dann, wenn in einer (bzw. jeder) Normalreihe für G alle Faktoren endlich sind. Jede prim-zyklische Normalreihe ist eine Kompositionsreihe. Es sei noch darauf hingewiesen, dass aus $V \lhd U \lhd G$ nicht notwendigerweise $V \lhd G$ folgt. (Man überlege sich ein Gegenbeispiel.)

Definition 7.2

Eine Gruppe G heißt *auflösbar*, falls es eine Normalreihe (7.1) für G gibt, die abelsch ist.

Satz 7.3

Es gelten folgende Aussagen.

(1) *Jede Untergruppe H einer auflösbaren Gruppe G ist auflösbar.*

(2) *Seien $\pi\colon G \to H$ ein surjektiver Gruppenhomomorphismus. Ist G auflösbar, so ist auch H auflösbar. Anders ausgedrückt: Faktorgruppen auflösbarer Gruppen modulo einem Normalteiler sind auflösbar.*

(3) *Sei N ein Normalteiler in der Gruppe G. Sind N und G/N auflösbar, so ist dies auch G.*

Beweis. (1) Sei (7.1) eine abelsche Normalreihe für G. Sei $V_i \stackrel{def}{=} U_i \cap H$. Dann ist offenbar V_{i-1} Normalteiler in V_i, und es ist (vgl. Übung II.2.1 (1))

$$\frac{V_i}{V_{i-1}} = \frac{U_i \cap H}{U_{i-1} \cap H} = \frac{U_i \cap H}{U_{i-1} \cap (U_i \cap H)} \simeq \frac{U_{i-1}(U_i \cap H)}{U_{i-1}} \subseteq \frac{U_i}{U_{i-1}}$$

als Untergruppe einer abelschen Gruppe abelsch.

(2) Sei (7.1) eine abelsche Normalreihe für G. Es ist dann $\{e\} = \pi(U_0) \subseteq \pi(U_1) \subseteq \pi(U_2) \subseteq \ldots \subseteq \pi(U_{n-1}) \subseteq \pi(U_n) = H$ eine Kette von Untergruppen. Sei $i \in \{1, \ldots, n\}$. Sei $h \in \pi(U_i)$. Es gibt ein $g \in U_i$ mit $\pi(g) = h$. Es folgt $h\pi(U_{i-1})h^{-1} = \pi(gU_{i-1}g^{-1}) = \pi(U_{i-1})$, also ist $\pi(U_{i-1})$ ein Normalteiler von $\pi(U_i)$. Ferner ist offenbar $\pi(U_i)/\pi(U_{i-1}) = \pi(U_i/U_{i-1})$ abelsch.

(3) Seien $N/N = U_0/N \lhd U_1/N \lhd U_2/N \lhd \ldots \lhd U_{n-1}/N \lhd U_n/N = G/N$ und $\{e\} = V_0 \lhd V_1 \lhd V_2 \lhd \ldots \lhd V_{m-1} \lhd V_m = N$ abelsche Normalreihen für G/N bzw. N (vgl. Übung II.2.1 (3)). Setzt man diese Ketten zusammen, so erhält man die Normalreihe

$$\{e\} = V_0 \lhd V_1 \lhd \ldots \lhd V_{m-1} \lhd V_m = N = U_0 \lhd U_1 \lhd \ldots \lhd U_{n-1} \lhd U_n = G,$$

wobei die Faktoren V_i/V_{i-1} und (vgl. Übung II.2.1 (2))

$$\frac{U_i}{U_{i-1}} \simeq \frac{U_i/N}{U_{i-1}/N}$$

abelsch sind. ∎

Beispiele. (1) Jede abelsche Gruppe ist auflösbar.

(2) Jede endliche p-Gruppe ist auflösbar. (Übung 7.6.)

(3) Jede nicht-abelsche, einfache Gruppe ist nicht auflösbar.

(4) Satz von Feit-Thompson[1]: *Jede Gruppe ungerader Ordnung ist auflösbar.*

Satz 7.4

Für $n \geq 5$ ist die symmetrische Gruppe $\mathbb{S}_n$ nicht auflösbar.

Beweis. Mit $\mathbb{S}_n$ wäre auch die Untergruppe $\mathbb{A}_n$ auflösbar. Für $n \geq 5$ ist $\mathbb{A}_n$ aber einfach und nicht abelsch, also nicht auflösbar. (Für einen direkten Beweis vgl. das Lemma unten.) ∎

Satz 7.5

Sei G eine endliche Gruppe. Es ist G auflösbar genau dann, wenn es eine Normalreihe für G gibt, die prim-zyklisch ist.

[1] Walter Feit, John G. Thompson, *Solvability of groups of odd order*, Pacific J. Math. 13 (1963), 775-1029.

Beweis. Sei G auflösbar. Nach Definition gibt es eine abelsche Normalreihe (7.1). Es ist zu zeigen, dass wir durch "Verfeinerung" der Reihe (d. h. durch Einfügen von weiteren Untergruppen zwischen U_{i-1} und U_i erreichen können, dass die Faktoren sogar Primzahlordnung haben. Dies ist schon ohne Verfeinerung der Fall, wenn alle U_i/U_{i-1} einfach sind, denn eine (endliche) einfache, abelsche Gruppe ist zyklisch von Primordnung. Ist U_i/U_{i-1} nicht einfach, so gibt es ein $V \neq U_{i-1}$, U_i mit $U_{i-1} \lhd V \lhd U_i$, und es ist V/U_{i-1} als Untergruppe von U_i/U_{i-1} abelsch und U_i/V als Bild vom surjektiven Gruppenhomomorphismus $\pi\colon U_i/U_{i-1} \to U_i/V$, $[x]_{U_{i-1}} \mapsto [x]_V$ (vgl. Homomorphiesatz) ebenso. Dies setzt man induktiv fort bis alle sukzessiven Faktoren in der (verfeinerten) Kette einfach sind; da die Ordnungen der Faktoren immer kleiner werden, muss dies Verfahren nach endlich vielen Schritten abbrechen. — Die Umkehrung ist trivial. ∎

Bemerkung. Die endlichen einfachen Gruppen bilden die kleinsten Bausteine der endlichen Gruppen in folgendem Sinn: *Jede endliche Gruppe G besitzt eine Kompositionsreihe.* (Übung 7.5.) Es gilt dabei auch eine Eindeutigkeitsaussage, nämlich der Satz von Jordan-Hölder, der besagt, dass in einer Kompositionsreihe die einfachen Faktoren bis auf Reihenfolge und Isomorphie eindeutig durch G bestimmt sind. Insbesondere ist die natürliche Zahl n in jeder Kompositionsreihe (7.1) für G dieselbe; diese heißt die *Länge* der Gruppe G.

Sei $n \geq 5$. Die Nichtauflösbarkeit von $\mathbb{S}_n$ wird später noch wichtig sein. (Vgl. Satz VII.5.3.) Wir hatten Satz 7.4 aus der Einfachheit der $\mathbb{A}_n$ hergeleitet. Es gibt aber auch einen direkten (unabhängigen), einfachen Beweis, dass $\mathbb{S}_n$ nicht auflösbar ist. Dies folgt unmittelbar aus der folgenden Aussage.

Lemma 7.6

Sei $n \geq 5$ und G eine Untergruppe von $\mathbb{S}_n$, die alle 3-Zykel enthält. Ist N ein Normalteiler von G, so dass G/N abelsch ist, so enthält N alle 3-Zykel.

Beweis. Seien $x = (i\,j\,k)$ und $y = (k\,r\,s)$ zwei 3-Zykel in G, wobei i, j, k, r, s fünf verschiedene Zahlen in $\{1, \ldots, n\}$ sind. Seien $\bar{x}$, $\bar{y}$ die Klassen in G/N. Da G/N abelsch ist, folgt $\bar{x}\bar{y}\bar{x}^{-1}\bar{y}^{-1} = e$, also $xyx^{-1}y^{-1} \in N$. Nun gilt

$$N \ni xyx^{-1}y^{-1} = (i\,j\,k)(k\,r\,s)(k\,j\,i)(s\,r\,k) = (i\,r\,k).$$

Also ist der (beliebige) 3-Zykel $(i\,r\,k)$ in N. ∎

Bemerkung. Viele der bis hierhin vorgestellten gruppentheoretischen Hauptaussagen werden in ihrem historischen Kontext beleuchtet in dem sehr empfehlenswerten Artikel von Ian Stewart: *Galois and the simple group of order* 60. Archive for History of Exact Sciences 78 (2024), 1–28. https://doi.org/10.1007/s00407-023-00319-9

Aufgaben

Ü 7.1. Es gibt keine einfache Gruppe der Ordnung 30 oder 56.

Ü 7.2. Sei $n \geq 5$. Der einzige nicht-triviale Normalteiler von $\mathbb{S}_n$ ist $\mathbb{A}_n$.

Ü 7.3. $\mathbb{A}_4$ ist nicht einfach. $\mathbb{A}_4$ hat keine Untergruppe der Ordnung 6. $\mathbb{S}_4$ ist auflösbar.

Ü 7.4. Es gibt keine nicht-abelsche einfache Gruppe G der Ordnung $60 < |G| < 168$.

Ü 7.5. Jede endliche Gruppe besitzt eine Kompositionsreihe.

Ü 7.6. Jede endliche p-Gruppe ist auflösbar.

Ü 7.7. Seien p und q zwei verschiedene Primzahlen. Dann ist jede Gruppe der Ordnung pq auflösbar.

Ü 7.8. Jede Gruppe G der Ordnung $|G| < 60$ ist auflösbar.

Ü 7.9. Sei G eine endliche, nicht-abelsche einfache Gruppe, und sei p eine Primzahl. Man zeige mit der Klassengleichung, dass es eine echte Untergruppe $U < G$ (d. h. mit $U \neq G$) geben muss, so dass p nicht den Index $[G : U]$ teilt.

Ü 7.10. Sei G eine endliche, nicht-abelsche einfache Gruppe. Sei U eine echte Untergruppe der Ordnung $d > 1$. Dann gibt es (mindestens) eine weitere Untergruppe der Ordnung d. Was bedeutet das (anschaulich) für den Untergruppenverband von G?

Ü 7.11. Für Elemente g, h in einer Gruppe G wird der *Kommutator* definiert durch $[g,h] := ghg^{-1}h^{-1}$. Es gilt $gh = hg$ genau wenn $[g,h] = e$. Für Untergruppen U, V von G sei $[U,V] := \langle [u,v] \mid u \in U,\ v \in V \rangle$ die *gegenseitige Kommutatorgruppe* von U und V. Speziell sei $G' := G^{(1)} := [G,G]$ die *derivierte* Untergruppe von G.

(1) G ist abelsch genau wenn $G' = \{e\}$.
(2) Es gilt $G' \lhd G$.
(3) Die Faktorgruppe G/G' ist abelsch.
(4) Sei H eine abelsche Gruppe und $f\colon G \to H$ ein Morphismus. Dann gilt $G' \subseteq \mathrm{Kern}(f)$.
(5) G' ist der kleinste Normalteiler N in G, so dass G/N abelsch ist.

Ü 7.12. Für eine Gruppe G definiere die *derivierte* Normalreihe induktiv wie folgt: $G^{(0)} := G$, $G^{(1)} = [G,G]$, und $G^{(i+1)} = [G^{(i)}, G^{(i)}]$ für alle $i \geq 1$. Man hat dann die (evtl. unendlich lange) Kette

$$G = G^{(0)} \rhd G^{(1)} \rhd G^{(2)} \rhd \ldots \rhd G^{(n)} \rhd G^{(n+1)} \rhd \ldots$$

(1) Eine endliche Gruppe G ist auflösbar genau dann, wenn es ein $n \geq 0$ gibt mit $G^{(n)} = \{e\}$.

Ü 7.13. Sei $n \geq 5$. Dann gilt ${\mathbb{S}_n}' = {\mathbb{A}_n}' = \mathbb{A}_n$.

Ü 7.14. Sei G eine endliche Gruppe, in der *jede* Sylowgruppe ein Normalteiler ist. (Dies gilt z. B., wenn G abelsch ist.)

(1) Seien $p \neq q$ zwei Primteiler von $|G|$ und U bzw. V die p- bzw. q-Sylowgruppe von G. Dann gilt $uv = vu$ für alle $u \in U$, $v \in V$.
(2) G ist isomorph zum direkten Produkt aller ihrer p-Sylowgruppen (mit $p \mid |G|$).

Ü 7.15. Beschreibe (bis auf Isomorphie) alle Gruppen von der Ordnung 1225.

KAPITEL IV

Polynome und Ringe

1. Euklidische Ringe

In diesem Abschnitt werden wir nur *kommutative* Ringe R betrachten, d. h. es gilt stets $x \cdot y = y \cdot x$ für alle $x, y \in R$.

Definition 1.1

Ein Integritätsbereich R zusammen mit einer *Größenfunktion* $\sigma\colon R \setminus \{0\} \to \mathbb{N}_0$ heißt *euklidischer Ring*, wenn folgendes gilt: Zu allen Elementen $a, b \in R$ mit $b \neq 0$ gibt es $q, r \in R$ mit $a = qb + r$, mit $r = 0$ oder $\sigma(r) < \sigma(b)$.

Beispiel. $\mathbb{Z}$ ist ein euklidischer Ring mit Größenfunktion $\sigma = |-|$.

Satz 1.2

Jeder euklidische Ring R ist ein Hauptidealring.

Beweis. Sei $I \subseteq R$ ein Ideal. Ist $I = \{0\}$, so wird I von 0 erzeugt. Sei $I \neq \{0\}$. Wähle $a \in I$ mit $\sigma(a)$ minimal. Es gilt $Ra \subseteq I$. Sei umgekehrt $b \in I$. Dann gibt es q, $r \in R$ mit $b = qa + r$, wobei $r = 0$ oder $\sigma(r) < \sigma(a)$ gilt. Weil auch $r = b - qa \in I$ gilt, muss $r = 0$, gelten, also $b = qa \in Ra$. ∎

2. Teilbarkeit und Faktorisierung

Definition 2.1

Sei R ein Integritätsbereich.

(0) Seien $a, b \in R$. Wir sagen, dass a ein *Teiler* von b ist (oder a *teilt* b; a ist ein *Faktor* von b; b ist ein *Vielfaches* von a (Schreibweise: $a \mid b$), falls $b \in Ra$ gilt, falls es also ein $r \in R$ gibt mit $b = ra$.

(1) Ein $r \in R$ heißt *Einheit* (oder *invertierbar*), falls es ein $s \in R$ gibt mit $rs = 1$ $(= sr)$. Die Einheiten in R bilden eine (abelsche) Gruppe $E(R)$.

(2) Ein $u \in R$ heißt *irreduzibel*, falls $u \neq 0$ keine Einheit ist, und falls aus $u = ab$ folgt, dass a oder b eine Einheit ist.

(3) Ein $p \in R$ heißt *prim* (oder *Primelement*), falls $p \neq 0$ keine Einheit ist, und falls aus $ab \in Rp$ folgt, dass $a \in Rp$ oder $b \in Rp$ gilt. (Also: $p \mid ab \;\Rightarrow\; p \mid a$ oder $p \mid b$.)

(4) Gilt $Ra = Rb$, so heißen a und b *assoziiert* ($a \sim b$). Äquivalent dazu: Es gibt eine Einheit u mit $a = ub$.

Lemma 2.2

Jedes Primelement p in einem Integritätsbereich ist irreduzibel.

Beweis. Es gelte $p = ab$. Dann $ab \in Rp$. Es folgt etwa, dass $a \in Rp$ gilt, $a = rp$. Dann $p = rpb$, also $p(1 - rb) = 0$, und es folgt $1 - rb = 0$ bzw. $1 = rb$. Also ist b eine Einheit. ∎

Definition 2.3

Ein Integritätsbereich R heißt *faktoriell*, falls jede Nichteinheit $r \neq 0$ ein Produkt von Primelementen ist, $r = p_1 p_2 \dots p_n$ (p_i prim, $n \geq 1$).

Lemma 2.4

Sei R ein Integritätsbereich. Es gelte

$$p_1 p_2 \dots p_r = q_1 q_2 \dots q_s$$

mit Primelementen $p_1, \dots, p_r$ und $q_1, \dots, q_s$. Dann gilt $r = s$, und nach evtl. Umnummerierung $p_i \sim q_i$ für alle $i = 1, \dots, r$.

Beweis. p_1 teilt das Produkt $q_1 q_2 \dots q_s$, und da p_1 prim ist, einen dieser Faktoren (diese Eigenschaften von Primelementen gilt auch für mehr als zwei Faktoren per Induktion); nach Umnummerierung können wir $p_1 \mid q_1$ annehmen, etwa $a p_1 = q_1$. Da q_1 als Primelement irreduzibel ist und p_1 keine Einheit ist, muss a eine Einheit sein, d. h. $p_1 \sim q_1$. Kürzen (Nullteilerfreiheit!) von p_1 liefert $p_2 \dots p_r = (a q_2) q_3 \dots q_s$, und mit q_2 ist auch $a q_2$ prim. Die Aussage folgt nun per Induktion. ∎

Satz 2.5

Für einen Integritätsbereich R sind folgende Aussagen äquivalent:

(1) *R ist faktoriell.*

(2) *Jede Nichteinheit $\neq 0$ ist ein Produkt von irreduziblen Elementen, die bis auf Umnummerierung und Assoziiertheit eindeutig bestimmt sind.*

(3) *Jede Nichteinheit $\neq 0$ ist ein Produkt von irreduziblen Elementen, und jedes irreduzible Element in R ist prim.*

Beweis. (1)⇒(3) Nach 2.2 ist jede Nichteinheit $\neq 0$ ein Produkt von irreduziblen Elementen. Sei q irreduzibel. Dann ist $q = p_1 \dots p_r$ mit p_i prim. Da q irreduzibel folgt $q \sim p_i$ für ein i, und damit ist q prim.

(3)⇒(1) klar.

(2)⇒(3) Sei q irreduzibel. Gelte $ab \in Rq$, etwa $ab = cq$. Zerlegt man a, b und c in irreduzible Elemente und nutzt die Eindeutigkeit aus, so erhält man, dass $a \in Rq$ oder $b \in Rq$ gilt. Also ist q prim.

(3)⇒(2) Da jedes irreduzible Element prim ist, und Zerlegungen in Primelemente eindeutig sind (bis auf Assoziiertheit) nach 2.4, folgt auch die Eindeutigkeit der Zerlegung in irreduzible Elemente. ∎

Satz 2.6

Jeder Hauptidealring ist faktoriell.

Beweis. (1) ["Euklids Lemma"] *Jedes irreduzible Element ist prim.* Sei p irreduzibel. Gelte $ab \in Rp$ und $a \notin Rp$. Dann gilt $Rp \subsetneq Rp + Ra = Rc$ für ein $c \in R$, da R Hauptidealring. Dann $p \in Rc$, also $p = dc$. Fall d Einheit, nicht möglich wegen $Ra \neq Rc$. Also c Einheit, $Rc = R$. Also $1 = rp + sa$. Dann $b = rbp + sab \in Rp$.

(2) *Jede Nichteinheit $\neq 0$ ist ein Produkt von irreduziblen Elementen.* Sei $r \neq 0$ Nicheinheit. Angenommen, r ist nicht Produkt von irreduziblen Elementen. Dann ist r selbst nicht irreduzibel. Also gibt es Nichteinheiten a, b ($\neq 0$) mit $r = ab$. Dann ist a oder b nicht irreduzibel. Setzt man dies fort, so erhält man (!) eine unendliche, echt aufsteigende Kette

$$Ra_1 \subsetneq Ra_2 \subsetneq Ra_3 \subsetneq \dots \subsetneq Ra_n \subsetneq Ra_{n+1} \subsetneq \dots$$

Dann ist

$$I = \bigcup_{n \geq 1} Ra_n$$

ein Ideal, also ein Hauptideal, $I = Rc$. Es gibt ein n mit $c \in Ra_n$. Es folgt $Ra_n = Ra_{n+1}$, Widerspruch. ■

Wir haben also die Beziehungen

$$\text{euklidisch} \quad \Rightarrow \quad \text{Hauptidealring} \quad \Rightarrow \quad \text{faktoriell.}$$

Die Umkehrungen gelten i. a. nicht. Vgl. Ü 6.2. Ein Beispiel eines nicht-euklidischen Hauptidealrings ist angegeben in: Jack C. Wilson: *A principal ideal ring that is not a Euclidean ring.* Mathematics Magazine 46 (1973), 34–38. http://www.jstor.org/stable/2688577

Folgerung 2.7 (*Hauptsatz der Arithmetik*)

Der Ring $\mathbb{Z}$ ist faktoriell.

Aufgaben

Ü 2.1. Sei R ein Hauptidealring und $p \in R$ irreduzibel. Dann ist R/pR ein Körper.

3. Polynomringe

Definition von *Polynomen* über einem kommutativen Ring K als Funktionen (Folgen) $f = (f_n)_{n\geq 0} \colon \mathbb{N}_0 \to K$ mit endlichem Träger, d. h. $f_n = 0$ für "fast alle" (d. h. bis auf endliche viele) $n \geq 0$. Schreibe $0 = (0, 0, 0, \dots)$, $1 = (1, 0, 0, \dots)$.

Proposition 3.1

Die Menge aller Polynome über K wird zu einem kommutativen Ring mit 1 durch folgende Addition und Multiplikation

$$(f_n) + (g_n) = (f_n + g_n)$$

und

$$(f_n) \cdot (g_n) = (\sum_{i=0}^{n} f_i g_{n-i})_n.$$

Beweis. Nachrechnen. ■

Bemerkung. Sei R der Ring der Polynome über K. Dann ist $a \mapsto (a, 0, 0, \dots)$ ein injektiver Ringhomomorphismus $K \to R$. Identifiziere K als Teilring (-körper) von R vermöge dieses Homomorphismus'.

Schreibe $T := (0, 1, 0, 0, \dots) \in R$. Dann gilt $T^0 = 1 \in R$, $T^2 = (0, 0, 1, 0, 0, \dots)$, $T^3 = (0, 0, 0, 1, 0, \dots)$, usw.

Proposition 3.2

Jedes vom Nullpolynom verschiedene Polynom f über K hat eine Darstellung $f = a_0 + a_1 T + a_2 T^2 + \cdots + a_n T^n$ mit $n \geq 0$ und eindeutigen Koeffizienten $a_0, a_1, \dots, a_n \in K$, wobei $a_n \neq 0$.

Beweis. Klar. ■

Bezeichnung: $R = K[T]$ heisst der *Polynomring* über K in der Unbestimmten T. $n = \operatorname{grad} f$, *Leitkoeffizient* a_n.

Proposition 3.3

Sei K ein Integritätsbereich. Seien f, $g \in K[T]$ vom Nullpolynom verschieden. Dann gilt

(1) $\operatorname{grad}(f \cdot g) = \operatorname{grad}(f) + \operatorname{grad}(g)$. *(Insbesondere $fg \neq 0$.)*
(2) *$K[T]$ ist ein Integritätsbereich.*

Beweis. (1) Sei $f = a_m T^m + \cdots + a_1 T + a_0$ und $= b_n T^n + \cdots + b_1 T + b_0$ mit a_m, $b_n \neq 0$, also $\operatorname{grad}(f) = m$ und $\operatorname{grad}(g) = n$. Dann gilt $fg = a_m b_n T^{m+n} + \ldots$, wobei alle weiteren Summanden kleineren Grad als $m+n$ haben. Da K nullteilerfrei ist, gilt $a_m b_n \neq 0$, also ist $\operatorname{grad}(fg) = m + n = \operatorname{grad}(f) + \operatorname{grad}(g)$.
(2) folgt aus (1). ∎

Satz 3.4 (*Polynomdivision mit Rest*)

Sei K ein Körper. Seien f, $g \in K[T]$ mit $g \neq 0$. Dann gibt es eindeutig bestimmte q, $r \in K[T]$ mit

$$f = qg + r,$$

wobei $r = 0$ oder $r \neq 0$ und $\operatorname{grad}(r) < \operatorname{grad}(g)$.

Beweis. Existenz. Für $f = 0$ wähle $q = 0 = r$. Es gelte nun $f \neq 0$. Die Existenz wird durch Induktion nach $n = \operatorname{grad}(f)$ bewiesen. Falls $\operatorname{grad}(f) < \operatorname{grad}(g)$, wähle $q = 0$ und $r = f$. Gelte nun $n \geq m := \operatorname{grad}(g)$. Sei etwa $f = a_n T^n + \ldots$ und $g = b_m T^m + \ldots$, wobei die Leitkoeffizienten a_n, $b_m \neq 0$ sind. Dann ist $a_n {b_m}^{-1} T^{n-m} \cdot g = a_n T^n + \ldots$. Also ist $\tilde{f} := f - a_n {b_m}^{-1} T^{n-m} \cdot g$ entweder 0 oder vom Grad $\leq n-1$. Nach Induktionsvoraussetzung gibt es daher $\tilde{q}$, r mit $\tilde{f} = \tilde{q} g + r$, mit $r = 0$ oder $\operatorname{grad}(r) < \operatorname{grad}(g)$. Wir erhalten

$$f = \tilde{f} + a_n {b_m}^{-1} T^{n-m} \cdot g = \left(\tilde{q} + a_n {b_m}^{-1} T^{n-m}\right) \cdot g + r,$$

und mit $q = \tilde{q} + a_n {b_m}^{-1} T^{n-m}$ folgt $f = qg + r$.

Eindeutigkeit. Falls ebenfalls $f = q_1 g + r_1$ mit $r_1 = 0$ oder $\operatorname{grad}(r_1) < \operatorname{grad}(g)$, so erhält man $(q_1 - q)g = r - r_1$. Aus Gradgründen muss dann $r - r_1 = 0$ gelten, was auch $q_1 - q$ nach sich zieht. Also $q_1 = q$ und $r_1 = r$. ∎

Folgerung 3.5

Für jeden Körper K ist $K[T]$ ein euklidischer Ring mit Größenfunktion $\sigma = \operatorname{grad}$. Insbesondere ist $K[T]$ ein Hauptidealring und faktoriell.

Bemerkung. Der obige Beweis der Polynomdivision mit Rest funktioniert auch in beliebigen kommutativen Ringen mit 1, wenn man nur voraussetzt, dass der Leitkoeffizient von g eine Einheit ist.

Proposition 3.6 (*Universelle Eigenschaft des Polynomrings*)

Sei K ein kommutativer Ring. Der Polynomring $K[T]$ hat folgende universelle Eigenschaft*: Sei S ein Ring und $s \in S$. Sei $\varphi\colon K \to S$ ein Ringhomomorphismus. Dabei sei S ein kommutativer Ring, oder es gelte allgemeiner, dass $\varphi(a)s = s\varphi(a)$ gilt für alle $a \in K$. Dann gibt es genau einen Ringhomomorphismus $\overline{\varphi}\colon K[T] \to S$ mit $\overline{\varphi}_{|K} = \varphi$ und $\overline{\varphi}(T) = s$.*

Beweis. Definiere $\overline{\varphi}(\sum_{i=0}^n a_i T^i) = \sum_{i=0}^n \varphi(a_i) s^i$. ∎

Häufig ist $\varphi\colon K \longrightarrow S$ eine natürliche Einbettung $\iota\colon a \mapsto a$. Man schreibt dann: $\overline{\iota}(f) = f(s)$. In die Unbestimmte T wird das Element $s \in S$ *eingesetzt*. Ist s fest,

so ist $f \mapsto f(s)$, $K[T] \longrightarrow S$ ein Ringhomomorphismus, der sogenannte *Einsetzungshomomorphismus*. Ein $s \in S$ heißt *Nullstelle* von f (in S), falls $f(s) = 0$ gilt.

Bemerkung. Man denke etwa an den Satz von Cayley-Hamilton aus der Linearen Algebra: $A \in \mathrm{M}_n(K)$, $\chi_A \in K[T]$ das charakteristische Polynom, dann $\chi_A(A) = 0$. Die Matrix A ist also eine Nullstelle des Polynoms χ_A im Ring $S = \mathrm{M}_n(K)$.

Proposition 3.7

Sei K ein Körper, oder auch nur ein Integritätsbereich (vgl. obige Bemerkung). Sei $f \in K[T]$ ($f \neq 0$) ein Polynom vom Grad n. Sei $c \in K$ eine Nullstelle von f in K. Dann gilt

$$f = q \cdot (T - c),$$

mit $q \in K[T]$ vom Grad $n-1$. Insbesondere hat f in K höchstens n Nullstellen.

Beweis. Polynomdivision mit Rest liefert eindeutige q, $r \in K[T]$ mit $f = q(T-c)+r$ und $r = 0$ oder $\mathrm{grad}(r) < \mathrm{grad}(T-c) = 1$. In jedem Fall ist $r \in K$ konstant, und wegen $0 = f(c) = q(c)(c-c) + r(c) = r(c)$ folgt $r = 0$. ∎

Folgerung 3.8

Sei K ein unendlicher Körper. Dann ist $K[T]$ isomorph zum Ring $\mathrm{Pol}(K, K)$ *aller Polynom*funktionen $f\colon K \to K$, $c \mapsto a_0 + a_1 c + a_2 c^2 + \cdots + a_n c^n$ *mit Koeffizienten in K.*

Beweis. Jedes $f \in K[T]$ liefert eine eindeutige Polynomfunktion $c \mapsto f(c)$. Diese Zuordnung ist offenbar surjektiv und ein Homorphismus von Ringen. Weil K unendlich ist, ist diese Zuordnung auch injektiv nach dem vorherigen Satz. ∎

Beispiel. Sei $K = \mathbb{F}_2$ der Körper mit zwei Elementen 0 und 1. Das Polynom $f = T^2 + T \in K[T]$ ist verschieden vom Nullpolynom, aber die zugehörige Polynomfunktion $K \to K$, $a \mapsto f(a)$ ist die Nullfunktion, denn es gilt $f(0) = 0$ und $f(1) = 1 + 1 = 0$, also $f(a) = 0$ für alle $a \in K$.

4. Quotientenkörper

Bemerkung: Ist R Teilring eines Körpers K, so ist R ein Integritätsbereich. Es gilt auch die Umkehrung:

Satz 4.1

Sei R ein Integritätsbereich. Dann gibt es einen Körper K, so dass R mit einem Teilring von K identifiziert werden kann.

Beweis. Sei X die Menge aller Paare (a, b) mit a, $b \in R$, $b \neq 0$. Wir erklären eine Äquivalenzrelation $\sim$ auf X durch

$$(a, b) \sim (c, d) \quad \Leftrightarrow \quad ad = bc.$$

[Nachrechnen, dass dies eine Äquivalenzrelation ist.]

Sei $K = X/\sim$ die Menge der Äquivalenzklassen. Wir schreiben $\left[\frac{a}{b}\right]$ für die Klasse von (a, b).

Auf K wird nun eine Addition und eine Multiplikation wie folgt erklärt:

$$\left[\frac{a}{b}\right] + \left[\frac{c}{d}\right] \overset{def}{=} \left[\frac{ad + bc}{bd}\right]$$

und

$$\left[\frac{a}{b}\right] \cdot \left[\frac{c}{d}\right] \overset{def}{=} \left[\frac{ac}{bd}\right].$$

Man prüft nach, dass dies *wohldefiniert* ist, d. h. nicht von der Auswahl der Repräsentanten der Klasse abhängt. Wir zeigen dies nur für die (schwierigere)

Addition: Gilt $(a,b) \sim (a',b')$ und $(c,d) \sim (c',d')$, so folgt $(ad+bc, bd) \sim (a'd' + b'c', b'd')$ [kurz demonstrieren], und dies zeigt die Wohldefiniertheit.

Man sieht, dass diese "Bruchrechenregeln" K zu einem kommutativen Ring machen mit Nullelement $\left[\frac{0}{1}\right]$ und Einselement $\left[\frac{1}{1}\right]$. Es ist $\left[\frac{a}{b}\right] = 0$ genau dann, wenn $a = 0$ ist. Daher ist jedes $\left[\frac{a}{b}\right] \neq 0$ invertierbar mit Inversem $\left[\frac{b}{a}\right]$.

Es ist offenbar $\iota\colon R \to K$, $a \mapsto \left[\frac{a}{1}\right]$ ein injektiver Ringhomomorphismus. ∎

Bemerkung. Identifizieren wir R via ι mit einem Teilring des oben konstruierten Körpers K, so folgt, dass jedes Element von K von der Form ist $ab^{-1} = a/b$ mit a, $b \in R$, $b \neq 0$. In K gibt es dann keinen kleineren Körper, der R enthält. Man nennt K auch den *Quotientenkörper* oder den *Körper der Brüche* von R. Der bestimmte Artikel ist gerechtfertigt, denn ist L irgendein Körper, der aus den Elementen ("Brüchen") ab^{-1} mit a, $b \in R$, $b \neq 0$ besteht, so konstruiert man einen offensichtlichen Isomorphismus von K nach L, der alle Elemente aus R festlässt.

Beispiele. (1) $\mathbb{Q}$ ist Quotientenkörper von $\mathbb{Z}$.

(2) $K(T)$ sei der Körper der Brüche des Polynomrings $K[T]$. Er besteht aus allen (formalen) Brüchen von Polynomen $f(T)/g(T)$, wobei $g \neq 0$ ist. Dieser Körper heißt auch der *rationale Funktionenkörper* in einer Unbestimmten über K.

Aufgaben

Ü 4.1. Sei R faktoriell mit Quotientenkörper K. Sei $\{p_i \mid i \in I\}$ ein Repräsentantensystem der irreduziblen Elemente in R, d. h. jedes irreduzible Element in R ist assoziiert zu genau einem p_i. Jedes Element $x \in K$ mit $x \neq 0$ hat eine Darstellung

$$x = u \cdot \prod_{i \in I} {p_i}^{n_i}$$

mit eindeutigen $u \in E(R)$ und $n_i \in \mathbb{Z}$, wobei nur endlich viele der n_i ungleich null sind. Dabei gilt $x \in R$ genau dann, wenn alle $n_i \geq 0$ sind.

Ü 4.2. Sei R ein Integritätsbereich mit Quotientenkörper K und kanonischer Einbettung $\iota\colon R \to K$, $a \mapsto a/1$. Sei $f\colon R \to S$ ein Ringhomomorphismus, so dass $f(a)$ invertierbar in S ist für jedes $a \in R$, $a \neq 0$. Dann gibt es genau einen Ringhomomorphismus $h\colon K \to S$ mit $f = h \circ \iota$.

5. Faktorielle Ringe sind ganz abgeschlossen

Sei R ein Integritätsring mit Quotientenkörper K. Grundlegendes Beispiel ist hier $R = \mathbb{Z}$, $K = \mathbb{Q}$.

Proposition 5.1

Sei R ein faktorieller Ring mit Quotientenkörper K. Jedes Element $x \in K$, welches einer normierten Polynomgleichung

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0 \tag{5.1}$$

mit Koeffizienten $a_0, \ldots, a_{n-1} \in R$ genügt, ist notwendig in R gelegen. Ferner ist solch ein x ein Teiler von a_0.

Generell heisst ein Element x eines Oberrings S eines Rings R *ganz* über R, wenn eine Gleichung (5.1) gilt. (Wichtig dabei ist, dass sie normiert ist!) Der Satz besagt also, dass es im faktoriellen Fall in K keine über R ganzen Elemente gibt, die nicht schon selbst in R liegen. Man sagt dann, dass der (Integritäts-) Ring R *ganz abgeschlossen* (in K) ist.

Folgerung 5.2

Sei $f \in \mathbb{Z}[T]$ ein normiertes Polynom. Ist $x \in \mathbb{Q}$ mit $f(x) = 0$, so gilt $x \in \mathbb{Z}$ (und x ist sogar ein ganzzahliger Teiler des absoluten Glieds a_0 von f). ∎

Beispiel. Die Gleichung $x^{11} - 10x^6 + 3 = 0$ ist nicht in $\mathbb{Q}$ lösbar.

Folgerung 5.3

Sei $a \in \mathbb{Z}$ eine ganze Zahl, welche sich für gegebenes $n \geq 2$ in $\mathbb{Z}$ nicht als n-te Potenz schreiben lässt (d. h. wir nehmen $a \neq k^n$ für jedes $k \in \mathbb{Z}$ an). Dann ist die Gleichung

$$x^n - a = 0$$

nicht in $\mathbb{Q}$ lösbar. Anders formuliert: $\sqrt[n]{a} \notin \mathbb{Q}$. ■

Beweis von Proposition 5.1. Schreibe $x = a/b$ mit teilerfremden $a, b \in R$, $b \neq 0$. (In einem faktoriellen Ring ist dies möglich: man kürzt sukzessive gemeinsame irreduzible Faktoren heraus, bis keine mehr übrig bleiben.) Multiplikation von (5.1) mit b^n liefert

$$a^n + \sum_{i=1}^{n} a_{n-i} a^{n-i} b^i = 0,$$

also

$$a^n = -b \sum_{i=1}^{n} a_{n-i} a^{n-i} b^{i-1}.$$

Es folgt $b \mid a^n$. Wäre nun b keine Einheit in R, dann gäbe es einen Primfaktor p von b, und p wäre dann auch ein Primfaktor von a, Widerspruch. Also ist b eine Einheit in R, und damit $x = ab^{-1} \in R$. Ferner gilt

$$x \cdot \left(-x^{n-1} - a_{n-1} x^{n-2} - \cdots - a_2 x - a_1\right) = a_0,$$

also $x \mid a_0$. ■

Aufgaben

Ü 5.1. Das Polynom $T^3 + 9T - 2$ ist irreduzibel über $\mathbb{Q}$.

6. Faktorisierung von Polynomen: Der Satz von Gauß

Definition 6.1 (*ggT*)

Sei R Integritätsbereich. Seien a und $b \in R$. Ein $d \in R$ heißt ein *größter gemeinsamer Teiler* (ggT) von a und b, falls

(1) $d \mid a$ und $d \mid b$, und
(2) Ist $d' \in R$ mit $d' \mid a$ und $d' \mid b$, so folgt $d' \mid d$.

Die Definition wird in naheliegender Weise auf mehr als zwei Elemente erweitert. Analog ("dual") wird das *kleinste gemeinschaftliche Vielfache* (kgV) definiert.

Offenbar gilt: Sind d_1 und d_2 ggT's von a und b (falls existent), so gilt $d_1 \sim d_2$ (und umgekehrt). Ist $a \in R$ und $b = 0$, so ist a ein ggT von a und b. Ist 1 ein ggT von a und b, so heißen a und b auch *teilerfremd*.

Ü 6.1. Sei R ein Hauptidealring, und seien $a, b \in R$.
(1) ("Bézouts Lemma") Es gilt $Ra + Rb = Rd$ mit $d = \mathrm{ggT}(a, b)$.
(2) Es gilt $Ra \cap Rb = Rv$ mit $v = \mathrm{kgV}(a, b)$.

Auch in faktoriellen Ringen hat man die Existenz des ggT:

Lemma 6.2

Sei R faktoriell. Seien $a = u{p_1}^{m_1} \dots {p_r}^{m_r}$ und $b = v{p_1}^{n_1} \dots {p_r}^{n_r}$, mit $p_1, \dots, p_r$ paarweise nicht-assoziierte Primelemente und u, $v \in E(R)$, m_i, $n_j \geq 0$. (Alle Elemente $\neq 0$ lassen sich auf diese Weise schreiben.) Dann ist ein ggT von a und b gegeben durch ${p_1}^{k_1} \dots {p_r}^{k_r}$, wobei $k_i = \min(m_i, n_i)$.

Eine analoge Formel mit max statt min gilt für das kgV.

Beweis. Klar. ■

Lemma 6.3

Sei R faktoriell, und seien a, $b \in R$ nicht beide 0. Es sind a und b teilerfremd genau dann, wenn es kein *irreduzibles Element $p \in R$ gibt mit $p \mid a$ und $p \mid b$.*

Beweis. Klar. ∎

Definition 6.4

Sei R faktoriell. Der *Inhalt* $I(f)$ eines Polynoms $f = \sum_{i=0}^{n} a_i T^i \in R[T]$, $f \neq 0$ ist der ggT seiner Koeffizienten. (Dies ist nicht paarweise gemeint! Der ggT ist nur bis auf eine Einheit eindeutig definiert!) Ein Polynom f mit $\operatorname{grad}(f) \geq 1$ heißt *primitiv*, falls $I(f) = 1$ gilt.

Bemerkung: Ein Polynom $f \in R[T]$ mit $f \neq 0$ heisst *normiert*, falls der Leitkoeffizient $= 1$ ist. Ein normiertes Polynom vom Grad ≥ 1 ist immer primitiv.

Proposition 6.5 (*Gauß-Lemma*)

Sei R faktoriell. Seien f, $g \in R[T]$ ungleich null. Dann gilt (bis auf Einheiten) $I(fg) = I(f)I(g)$.

Beweis. Zunächst kann man ohne Einschränkung annehmen, dass sowohl f wie auch g einen Grad ≥ 1 hat. Schreibt man $f = I(f)f'$ und $g = I(g)g'$, so sind f' und g' primitiv, es gilt $I(fg) = I(f)I(g)I(f'g')$, und es genügt daher zu zeigen:

(6.1) *Sind f und g primitiv, so ist auch fg primitiv.*

Seien $f = \sum_{i=0}^{m} a_i T^i$ und $g = \sum_{i=0}^{n} b_i T^i$ mit $a_m \neq 0$ und $b_n \neq 0$. Dann ist

$$fg = \sum_{i=0}^{m+n} (\sum_{j=0}^{i} a_j b_{i-j}) T^i.$$

Schreibe $c_i = \sum_{j=0}^{i} a_j b_{i-j}$ Sei p ein beliebiges Primelement. Sei r die größte ganze Zahl mit $0 \leq r \leq m$, $a_r \neq 0$ und p teilt nicht a_r. Ebenso sei s die größte ganze Zahl mit $0 \leq s \leq n$, $b_s \neq 0$ und p teilt nicht b_s. Es ist

$$c_{r+s} = a_r b_s + a_{r+1} b_{s-1} + \cdots + a_{r-1} b_{s+1} + \ldots$$

Da p das Produkt $a_r b_s$ nicht teilt, aber alle anderen Summanden auf der rechten Seite, teilt p nicht c_{r+s}. Es gibt also kein Primelement, welches alle Koeffizienten c_i gleichzeitig teilt, daher sind sie teilerfremd. ∎

Ist K ein Körper und $f \in K[T]$, so bedeutet f irreduzibel genau folgendes: (1) $\operatorname{grad}(f) \geq 1$, und (2) ist $f = gh$, so ist $\operatorname{grad}(g) = 0$ oder $\operatorname{grad}(h) = 0$. Ist R (nur) ein faktorieller Ring, so kann es auch irreduzible $f \in R[T]$ vom Grad 0 geben, nämlich gerade die irreduziblen Elemente in R.

Lemma 6.6 (*Gauß-Lemma*)

Sei R faktoriell und sei K der Quotientenkörper von R. Ist $f \in R[T]$ vom Grad ≥ 1 und irreduzibel, so ist f auch irreduzibel in $K[T]$.

Beweis. Sei f vom Grad ≥ 1 und irreduzibel über R, aber reduzibel über K. Man kann also schreiben $f = gh$ mit g, $h \in K[T]$, und mit $\operatorname{grad}(g)$, $\operatorname{grad}(h) \geq 1$. Multipliziert man mit dem Hauptnenner a der Koeffizienten von g und mit dem Hauptnenner b der Koeffizienten von h, so erhält man $abf = (ag)(bh)$ mit a, $b \in R$, $a \neq 0$, $b \neq 0$ und ag, $bh \in R[T]$. Schreibt man $ag = I(ag)g'$ und $bh = I(bh)h'$, so sind g' und h' primitiv, und $abf = I(ag)I(bh)g'h'$. Da f irreduzibel in $R[T]$ (und vom Grad ≥ 1), ist f primitiv. Vergleich der Inhalte beider Seiten liefert (bis auf Einheit) $ab = I(ag)I(bh)$. Kürzen liefert $f = g'h'$ mit g', $h' \in R[T]$ primitiv. Dies ergibt eine nicht-triviale Zerlegung von f in $R[T]$, Widerspruch.

Satz 6.7 (*Gauß*)

Ist R ein faktorieller Ring, so ist dies auch $R[T]$.

Sei K der Quotientenkörper von R. Die irreduziblen Polynome in $R[T]$ sind die irreduziblen Elemente in R und die primitiven Polynome in $R[T]$, die irreduzibel in $K[T]$ sind.

Beweis. Sei $f \in R[T]$, $f \neq 0$. Wir wissen, dass $K[T]$ als euklidischer Ring faktoriell ist. Es hat also f in $K[T]$ eine Zerlegung $f = q_1 q_2 \dots q_r$ mit Primelementen $q_i \in K[T]$. Zieht man Nenner und gemeinsame Teiler der Zähler heraus, so erhält man $f = cp_1 p_2 \dots p_r$ mit $c \in K$, $c \neq 0$, und primitiven, irreduziblen Polynomen $p_i \in R[T]$ (da irreduzibel in $K[T]$). Man kann schreiben $c = a/b$ mit teilerfremden a und b, und erhält $bf = ap_1 p_2 \dots p_r$. Der Inhalt der rechten Seite ist a (mit (6.1)), der der linken Seite wird von b geteilt. Also muss b eine Einheit in R sein, damit zerlegt sich f schon über R in irreduzible Elemente und Polynome. Ist $f = p'_1 p'_2 \dots p'_s$ eine weitere solche Darstellung, so sind die p'_j primitiv oder vom Grad 0. Die primitiven p'_j sind nach Lemma 6.6 auch irreduzibel über K, dort stimmen sie bis auf Einheiten in K (und Umnummerierung) mit den p_i überein, und obiges Argument zeigt nochmal, dass die p_i schon über R zu den p'_j assoziiert sind. ∎

Beispiel. $\mathbb{Z}[T]$ ist faktoriell.

Beispiel. Sei R faktoriell und $R[T_1, T_2] := R[T_1][T_2]$ der Polynomring in zwei Unbestimmten über R. Es ist $R[T_1, T_2]$ faktoriell. (Dies kann man induktiv auf endlich viele Unbestimmte erweitern.)

Aufgaben

Ü 6.2. $\mathbb{Z}[T]$ ist kein Hauptidealring.

Ü 6.3. Sei K ein Körper. Der Polynomring $K[T_1, T_2]$ in zwei Unbestimmten ist kein Hauptidealring.

Ü 6.4. Sei R faktoriell, und seien a, $b \in R$. Dann gilt (bis auf Assoziiertheit)

$$ab = \mathrm{ggT}(a, b) \cdot \mathrm{kgV}(a, b).$$

Ü 6.5. Sei R faktoriell, und seien a, b, $c \in R \setminus \{0\}$. Es gelte $a \mid bc$ und $\mathrm{ggT}(a, b) = 1$. Dann folgt $a \mid c$.

7. Ein Irreduzibilitätskriterium

Satz 7.1 (*Kriterium von Eisenstein*)

Sei R ein faktorieller Ring mit Quotientenkörper K. Sei $f \in R[T]$, $f = a_0 + a_1 T + \dots + a_n T^n$ vom Grad $n \geq 1$. Es gebe ein Primelement $p \in R$ mit

(1) $p \nmid a_n$. *(Etwa: f normiert.)*
(2) $p \mid a_i$ $(i = 0, \dots, n-1)$.
(3) $p^2 \nmid a_0$.

Dann ist f irreduzibel in $K[T]$.

Beweis. Schreibe $f = I(f) f'$ mit f' primitiv. Zu zeigen genügt, dass f' in $R[T]$ irreduzibel ist. Da $I(f)$ nicht von p geteilt wird, gelten bzgl. Teilbarkeit durch p für f' dieselben Bedingungen wie für f. Man kann also ohne Einschränkung annehmen, dass f selbst primitiv ist, und zu zeigen genügt (vgl. Lemma 6.6), dass f irreduzibel in $R[T]$ ist. Angenommen, dies ist falsch, also $f = gh$ in $R[T]$ mit $g = \sum_{i=0}^{r} b_i T^i$ und $h = \sum_{i=0}^{s} c_i T^i$ mit $b_r \neq 0$ und $c_s \neq 0$, wobei wir wegen der Primitivität zusätzlich r, $s \geq 1$ annehmen können. Dann ist

$$f = \sum_{i=0}^{r+s} \Big(\sum_{j=0}^{i} b_j c_{i-j} \Big) T^i.$$

Da $a_0 = b_0c_0$ durch p aber nicht durch p^2 teilbar ist, gilt etwa $p \mid b_0$ und $p \nmid c_0$. Da $a_n = b_rc_s$ nicht durch p teilbar ist, ist b_r nicht durch p teilbar. Sei k der kleinste Index mit $p \nmid b_k$. Da in

$$a_k = b_0c_k + b_1c_{k-1} + \cdots + b_{k-1}c_1 + b_kc_0$$

auf der rechten Seite nur der Summand b_kc_0 nicht durch p geteilt wird, folgt, dass a_k nicht durch p geteilt wird, Widerspruch zur Annahme $p \mid a_k$ $(k < n)$. ∎

Beispiel. Sei $f = 2T^5 + 15T^4 + 9T^3 + 6 \in \mathbb{Z}[T]$. Nach dem Kriterium von Eisenstein (mit $p = 3$) ist f irreduzibel in $\mathbb{Q}[T]$.

Aufgaben

Ü 7.1. Sei p eine Primzahl. Dann ist das Polynom

$$T^{p-1} + T^{p-2} + \ldots + T + 1$$

irreduzibel über $\mathbb{Q}$. (Hinweis: Eisenstein nach geeigneter Variablentransformation.)

Ü 7.2. In $\mathbb{Q}[T]$ gibt es zu jedem $n \geq 1$ unendlich viele normierte, irreduzible Polynome vom Grad n.

8. Anhang: Elementare Zahlentheorie und Kryptographie *

Wir haben gesehen, dass der Ring $\mathbb{Z}$ der ganzen Zahlen euklidisch ist, also insbesondere ein Hauptidealbereich und faktoriell ist. Die daraus resultierende Eigenschaft, dass sich jede natürliche Zahl $n \geq 1$ eindeutig als ein Produkt von (positiven) Primzahlen schreiben lässt, nennt man auch den *Hauptsatz der Arithmetik*. Im folgenden seien Primzahlen immer natürliche Zahlen, also positiv. Schon sehr lange ist bekannt:

Proposition 8.1 (*Euklid*)

Es gibt unendlich viele Primzahlen.

Beweis. Angenommen, es gäbe nur endlich viele; seien $p_1, \ldots, p_t \in \mathbb{N}$ alle Primzahlen. Setze $n := p_1 \cdot \ldots \cdot p_t + 1$. Als natürliche Zahl $n \geq 2$ hat n (nach dem Hauptsatz der Arithmetik) mindestens einen Primteiler p. Es muss dann $p = p_i$ für ein i gelten, aber offenbar teilt keines der p_i das n (es bleibt der Rest 1!). Widerspruch. ∎

Bemerkung. Es gilt der sehr viel stärkere sog. Primzahlsatz[1]: Für jede positive reelle Zahl x bezeichne $\pi(x)$ die Anzahl aller Primzahlen p mit $p \leq x$. Dann gilt

$$\pi(x) \sim \frac{x}{\ln x} \quad \text{für } x \to \infty.$$

Diese Asymptotik bedeutet $\lim_{x\to\infty} \pi(x)/(x/\ln x) = 1$.

Der erweiterte euklidische Algorithmus. Der euklidische Algorithmus berechnet bei Eingabe zwei natürlicher Zahlen a, b deren größten gemeinsamen Teiler $d = \mathrm{ggT}(a, b) \in \mathbb{N}$, und zwar durch sukzessive Division mit Rest. In der erweiterten Version werden zusätzlich ganze Zahlen x, y bestimmt mit $d = xa + yb$. (Vgl. auch Bézouts Lemma.)

Ist etwa $a \geq b > 0$, so liefert Division mit Rest $a = qb + r$ mit $0 \leq r < b$.

[1] Der Primzahlsatz wurde schon 1793 von Gauß und 1798 von Legendre vermutet, aber konnte erst 1896 unabhängig von Hadamard und de La Vallée Poussin bewiesen werden. Der Beweis verwendet tiefliegende analytische Methoden.

Lemma 8.2

(1) *Es gilt* $\mathrm{ggT}(a,b) = \mathrm{ggT}(b,r)$.
(2) *Ist* $r = 0$, *so ist* $b = \mathrm{ggT}(a,b)$.

Beweis. Unter Verwendung von $r = a - qb$ ist dies eine leichte Übungsaufgabe. ■

Wir wenden dies mehrfach an:

$$\begin{aligned} a &= q_1 b + r_1 \\ b &= q_2 r_1 + r_2 \\ r_1 &= q_3 r_2 + r_3 \\ &\dots \end{aligned}$$

Da $0 \leq \ldots < r_3 < r_2 < r_1$ muss dieses Verfahren nach endlich vielen Schritten den Rest 0 liefern, etwa $r_n > 0$ und $r_{n+1} = 0$. Es ist dann, nach dem Lemma, $\mathrm{ggT}(a,b) = r_n$.

Nun zur Berechnung von x und y. Aus $a = q_1 b + r_1$ folgt $r_1 = 1 \cdot a + (-q_1) \cdot b$. Also sei $x_1 = 1$ und $y_1 = -q_1$. Im nächsten Schritt, $b = q_2 r_1 + r_2$, und somit $r_2 = b - q_2 r_1 = b - q_2(a - bq_1) = (-q_2)a + (1 - y_1 q_2)b$. Also sei $x_2 = -q_2$ und $y_2 = 1 - y_1 q_2$. Angenommen, x_i, x_{i+1} und y_i, y_{i+1} sind bereits bestimmt, so dass

$$r_i = x_i a + y_i b$$
$$r_{i+1} = x_{i+1} a + y_{i+1} b$$

gilt. Der nächste Schritt im euklidischen Algorithmus liefert $r_i = q_{i+2} r_{i+1} + r_{i+2}$. Damit

$$\begin{aligned} r_{i+2} &= r_i - q_{i+2} r_{i+1} \\ &= x_i a + y_i b - q_{i+2}(x_{i+1} a + y_{i+1} b) \\ &= (x_i - q_{i+2} x_{i+1})a + (y_i - q_{i+2} y_{i+1})b. \end{aligned}$$

Sei also

$$x_{i+2} = x_i - q_{i+2} x_{i+1} \quad \text{und} \quad y_{i+2} = y_i - q_{i+2} y_{i+1}. \tag{8.1}$$

Dann gilt $r_{i+2} = a x_{i+2} + b y_{i+2}$. Insbesondere erhält man $d = \mathrm{ggT}(a,b) = r_n = x_n a + y_n b$.

Beispiel. Seien $a = 60972$ und $b = 19404$. Wir verwenden den erweiterten euklidischen Algorithmus in folgender, schematischen Weise (siehe Tabelle), wobei in der linken Spalte sukzessive Division mit Rest ausgeführt wird und die Faktoren auf der rechten Seite induktiv, ausgehend von $x_{-1} = 1$, $y_{-1} = 0$, $x_0 = 0$, $y_0 = 1$, mittels (8.1) berechnet werden. Der ggT ist 12. (Vgl. Lemma 8.2 (2).)

					60972	=	$1 \cdot 60972$	+	$0 \cdot 19404$
					19404	=	$0 \cdot 60972$	+	$1 \cdot 19404$
60972	=	$3 \cdot 19404$	+	2760	2760	=	$1 \cdot 60972$	+	$-3 \cdot 19404$
19404	=	$7 \cdot 2760$	+	84	84	=	$-7 \cdot 60972$	+	$22 \cdot 19404$
2760	=	$32 \cdot 84$	+	72	72	=	$225 \cdot 60972$	+	$-707 \cdot 19404$
84	=	$1 \cdot 72$	+	12	12	=	$-232 \cdot 60972$	+	$729 \cdot 19404$
72	=	$6 \cdot 12$	+	0					

Bemerkung. Der erweiterte euklidische Algorithmus lässt sich genauso in jedem euklidischen Ring durchführen. Insbesondere also auch im Polynomring $K[T]$ in einer Unbestimmten über einem Körper K. Im Gegensatz zu der durch Lemma 6.2 suggerierten Methode zur Berechnung des ggT, ist der euklidische Algorithmus sehr effizient.

Der Satz von Euler.

Bemerkung. Der (kleine) Satz von Fermat aus der Gruppentheorie lässt sich so ausdrücken: *Sei p eine Primzahl und a eine natürliche Zahl mit $p \nmid a$. Dann gilt $a^{p-1} \equiv 1 \bmod p$.*

Denn nach Voraussetzung ist die Restklasse von a modulo p nicht-null im Körper $\mathbb{Z}/p\mathbb{Z}$, dessen Einheitengruppe die Ordnung $p-1$ hat.

Satz 8.3 (*Euler*)

Sei $n \geq 1$ eine natürliche Zahl und $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a,n) = 1$. Dann gilt $a^{\varphi(n)} \equiv 1 \bmod n$.

Hierbei ist die Eulersche φ-Funktion definiert durch $\varphi(n) := |\{x \in \mathbb{N} \mid 1 \leq x \leq n,\ \mathrm{ggT}(x,n) = 1\}|$. Man beachte, dass im Falle $n = p$ prim $\varphi(p) = p-1$ gilt, der Satz von Fermat also ein Spezialfall ist.

Beweis. Man sieht leicht: die Klasse $[m]$ von $m \in \mathbb{Z}$ ist eine Einheit im Restklassenring $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$, genau wenn $\mathrm{ggT}(m,n) = 1$ gilt. (Man verwende Bézouts Lemma.) Also hat die Einheitengruppe von $\mathbb{Z}_n$ die Ordnung $\varphi(n)$. Nach dem kleinen Fermat ist deswegen $[a]^{\varphi(n)} = [1]$. ∎

Die folgende Aussage ist eine Variante des Satzes von Euler in einem Spezialfall:

Proposition 8.4

Sei $n = p \cdot q$ ein Produkt zweier verschiedener Primzahlen p und q. Für jede ganze Zahl $x \in \mathbb{Z}$ gilt $x \cdot x^{\varphi(n)} \equiv x \bmod n$.

Beweis. Es gilt $\varphi(n) = \varphi(p)\varphi(q) = (p-1)(q-1)$. Gelte zunächst $\mathrm{ggT}(x,n) = 1$. Dann gilt nach dem Satz von Euler $x^{\varphi(n)} \equiv 1 \bmod n$, und damit $x \cdot x^{\varphi(n)} \equiv x \bmod n$. Dies gilt offenbar auch für $x = 0$, oder allgemeiner, wenn $n \mid x$. Gelte nun $d = \mathrm{ggT}(x,n) > 1$ und $n \nmid x$. Dann kann nur $n = p$ oder $n = q$ gelten. Also etwa $x = q$ (der Fall $x = p$ geht analog). Dann gilt $p \nmid x$, und aus dem Satz von Fermat folgt $x^{p-1} \equiv 1 \bmod p$. Wegen $q \mid x$ ergibt sich $x \cdot x^{p-1} \equiv x \bmod pq$. Wiederholt man dies $(q-1)$-mal, so ergibt sich

$$x \equiv x \cdot x^{(p-1)} \equiv x \cdot x^{2(p-1)} \equiv \cdots \equiv x \cdot x^{(q-1)(p-1)} = x \cdot x^{\varphi(n)} \bmod n.$$

∎

Modulares Potenzieren. Im folgenden wird es wichtig sein, ℓ-te Potenzen einer natürlichen Zahl x modulo n zu berechnen, wobei hier typischerweise ℓ, x und n sehr große natürliche Zahlen sein werden. Wie dies relativ effizient geht, illustrieren wir im folgenden Beispiel.

Beispiel. Wir wollen $6^{1031} \bmod 789$ ausrechnen. Erst die Potenz 6^{1031} innerhalb $\mathbb{Z}$ berechnen und erst danach modulo 789 zu reduzieren würde riesige Zahlen produzieren. Stattdessen multiplizieren wir Schritt für Schritt und reduzieren jedesmal zwischendurch modulo 789 mittels Division mit Rest. Wir beschreiben das sog. wiederholte Quadrieren ("repeated squaring"):

Schreibe 1031 als Summe von Potenzen von 2:

$$1031 = 1024 + 4 + 2 + 1 = 2^{10} + 2^2 + 2^1 + 2^0.$$

Dann berechnen wir sukzessive $6^2 = 36$,

Es ergibt sich also $6^{1031} = 6^{1024} \cdot 6^4 \cdot 6^2 \cdot 6^1 \equiv 99 \cdot 507 \cdot 36 \cdot 6 \equiv \boxed{39} \bmod 789$.

Das RSA-Kryptoverfahren. Das RSA[2]-Verfahren ist ein sogenanntes asymmetrisches Verschlüsselungsverfahren. Alice möchte Bob eine chiffrierte Nachricht schicken. Dafür verwendet sie Bobs öffentlich bekannten Schlüssel (n,e) zum Chiffrieren, und Bob kann die Nachricht mit seinem dazu gehörigen geheimen Schlüssel

[2]Nach Ron Rivest, Adi Shamir, und Leonard Adleman vom Massachusetts Institute of Technology (1977).

$$\begin{array}{rcrcrcrcr}
6^4 & = & 36^2 & = & 1296 & \equiv & 507 & \mod & 789 \\
6^8 & = & 507^2 & = & 257049 & \equiv & 624 & \mod & 789 \\
6^{16} & = & 624^2 & = & 389376 & \equiv & 399 & \mod & 789 \\
6^{32} & \equiv & 399^2 & = & 159201 & \equiv & 612 & \mod & 789 \\
6^{64} & \equiv & 612^2 & = & 374544 & \equiv & 558 & \mod & 789 \\
6^{128} & \equiv & 558^2 & = & 311364 & \equiv & 498 & \mod & 789 \\
6^{256} & \equiv & 498^2 & = & 248004 & \equiv & 258 & \mod & 789 \\
6^{512} & \equiv & 258^2 & = & 66564 & \equiv & 288 & \mod & 789 \\
6^{1024} & \equiv & 288^2 & = & 82944 & \equiv & 99 & \mod & 789
\end{array}$$

(n, d) dechiffrieren. Hierbei ist n eine natürliche Zahl, die ein Produkt von zwei verschiedenen (großen) Primzahlen ist; die Zerlegung $n = p \cdot q$ ist nur Bob selbst bekannt[3]. Zudem wird diese Zerlegung nach Konstruktion der Schlüssel nicht mehr benötigt. Es gilt dann $\varphi(n) = (p-1)(q-1)$ (vgl. Übung 8.1). Bob wählt eine natürliche Zahl $1 < e < \varphi(n)$ mit $\mathrm{ggT}(e, \varphi(n)) = 1$. Aus n und e berechnet Bob (mit dem erweiterten euklidischen Algorithmus) die natürliche Zahl d mit $1 < d < \varphi(n)$ und der Eigenschaft $de \equiv 1 \bmod \varphi(n)$; es ist d also das multiplikative Inverse zu e modulo $\varphi(n)$. Die Zahlen p, q, d und $\varphi(n)$ müssen geheim bleiben. Veröffentlicht werden kann der öffentliche Schlüssel (n, e) jedem zugänglich z. B. auf Bobs Website. Dagegen ist (n, d) Bobs geheimer Schlüssel[4] nur ihm bekannt.

Ein Nachricht x kann man sich als natürliche Zahl $< n$ vorstellen. Alice chiffriert diese Nachricht als $y = x^e \bmod n$ und sendet y an Bob. Dieser bildet mit seinem geheimen Schlüssel $y^d \bmod n$ und erhält x zurück: denn mehrfache Anwendung obiger Proposition liefert

$$\begin{aligned}
y^d &\equiv x^{ed} = x^{1+k\varphi(n)} \\
&= x \cdot (x^{\varphi(n)})^k = x \cdot x^{\varphi(n)} \cdot (x^{\varphi(n)})^{k-1} \\
&\equiv x \cdot (x^{\varphi(n)})^{k-1} \equiv \cdots \equiv x \bmod n.
\end{aligned}$$

Beispiel. Ein Minibeispiel, um die Methode zu illustrieren. Seien $p = 11$, $q = 17$ und $n = pq = 187$. Es ist $\varphi(n) = 10 \cdot 16 = 160$. Wähle etwa $e = 7$. (Man sieht, dass $\mathrm{ggT}(7, 160) = 1$ gilt.) Wir verwenden den erweiterten euklidischen Algorithmus, um das Inverse d von 57 mod 352 zu berechnen. Wir erhalten $d = 23$. (Den behält Bob

$$\begin{array}{rcrcr|rcrcr}
 & & & & & 160 & = & 1 \cdot 160 & + & 0 \cdot 7 \\
 & & & & & 7 & = & 0 \cdot 160 & + & 1 \cdot 7 \\
\hline
160 & = & 22 \cdot 7 & + & 6 & 6 & = & 1 \cdot 160 & + & -22 \cdot 7 \\
7 & = & 1 \cdot 6 & + & 1 & 1 & = & -1 \cdot 160 & + & 23 \cdot 7
\end{array}$$

für sich.)

Es soll etwa die "Nachricht" $x = 12$ an Bob geschickt werden. Dazu bildet Alice mit Bobs öffentlichen Schlüssel $(187, 7)$

$$\begin{aligned}
y &= x^7 = 12^7 = (12^3)^2 \cdot 12 \equiv 45^2 \cdot 12 \equiv 155 \cdot 12 \\
&\equiv 177 \bmod 187
\end{aligned}$$

[3] Zur Konstruktion verwendet Bob Zufallszahlgeneratoren und probabilistische Primtests.

[4] Die Sicherheit des Geheimnisses beruht darauf, dass kein effizienter Algorithmus bekannt ist zum Faktorisieren (großer) natürlicher Zahlen in Primfaktoren, und damit weder $\varphi(n)$ noch d effizient berechnet werden kann. Man beachte aber, dass nicht bewiesen ist, dass es keinen effizienten Algorithmus geben kann. Und da Computer immer leistungsfähiger werden, müssen auch die Zahlen n (bzw. p und q) immer größer gewählt werden; zur Zeit wird empfohlen, dass n mindestens 600-stellig sein soll. Abgesehen davon werden noch weitere Anforderungen etwa an e gestellt, um gewissen bekannten Angriffen vorzubeugen. An dieser Stelle wird das Verfahren sozusagen nur in math. Reinkultur dargestellt.

und sendet also 177 an Bob. Dieser bildet mit seinem geheimen Schlüssel $y^d \bmod 187$, und erhält

$$\begin{aligned} 177^{23} &\equiv -10^{23} = -1000^7 \cdot 100 \equiv -65^7 \cdot 100 = -(65^2)^3 \cdot 6500 \\ &\equiv -111^3 \cdot 142 \equiv -111^2 \cdot 54 \equiv -166 \cdot 54 \equiv -175 \\ &= 12 \bmod 187, \end{aligned}$$

also die Originalnachricht.

Bemerkung. Man kann sich vorstellen, dass dieses modulare Potenzieren mit einem n, das mehrere hundert Stellen hat, relativ rechenaufwändig ist, insbesondere bei langen Nachrichten. Deshalb wird das RSA-Verfahren i.d.R. nur zum Austausch von Schlüsseln verwendet, die wiederum für andere, schnellere (symmetrische) Kryptoverfahren verwendet werden.

Aufgaben

Ü 8.1. (1) Sei p eine Primzahl und $k \geq 1$. Dann gilt $\varphi(p^k) = p^k - p^{k-1}$.
(2) Sind m, $n \in \mathbb{N}$ teilerfremd, so gilt $\varphi(mn) = \varphi(m)\varphi(n)$.
(3) Sei $n = p_1^{k_1} \dots p_t^{k_t}$ mit $k_i \geq 1$ und paarweise verschiedenen Primzahlen $p_1, \dots, p_t$. Dann gilt

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

Ü 8.2. [Chinesischer Restsatz] Sei R ein kommutativer Ring und seien $\mathfrak{m}_1, \dots, \mathfrak{m}_n$ Ideale in R, die paarweise coprim sind, d. h. für alle $i \neq j$ gilt $\mathfrak{m}_i + \mathfrak{m}_j = R$. Dann induziert der Ringmorphismus $R \to \prod_{i=1}^n R/\mathfrak{m}_i$, $r \mapsto (r + \mathfrak{m}_i)_{i=1}^n$ einen Isomorphismus

$$R/\bigcap_{i=1}^{n} \mathfrak{m}_i \simeq \prod_{i=1}^{n} R/\mathfrak{m}_i.$$

Ü 8.3. Sei $R = \mathbb{Z}$. Was bedeutet es für zwei Ideale $\mathbb{Z}n$ und $\mathbb{Z}m$ coprim zu sein? Was bedeutet der chinesische Restsatz für das Lösen eines Gleichungssystems linearer Kongruenzen

$$\begin{aligned} x &\equiv a_1 \bmod m_1 \\ x &\equiv a_2 \bmod m_2 \\ &\vdots \\ x &\equiv a_n \bmod m_n, \end{aligned}$$

wobei $a_1, \dots, a_n \in \mathbb{Z}$ und $m_1, \dots, m_n \in \mathbb{N}$ gegeben sind und $x \in \mathbb{Z}$ gefunden werden soll?

Ü 8.4. Seien $\mathfrak{a}$ und $\mathfrak{b}$ zwei Ideale in einem kommutativen Ring R. Das Produktideal $\mathfrak{a} \cdot \mathfrak{b}$ ist definiert als die Menge aller endlichen Summen $\sum_{i=1}^n a_i b_i$ mit $a_i \in \mathfrak{a}$, $b_i \in \mathfrak{b}$, $n \geq 0$. Es gilt stets $\mathfrak{a} \cdot \mathfrak{b} \subseteq \mathfrak{a} \cap \mathfrak{b}$. Sind $\mathfrak{a}$ und $\mathfrak{b}$ coprim ($\mathfrak{a} + \mathfrak{b} = R$), so gilt $\mathfrak{a} \cdot \mathfrak{b} = \mathfrak{a} \cap \mathfrak{b}$.

Ü 8.5. Für $f = T^5 - 6T + 1$ und $g = T^3 - 6T^2 + T + 4$ berechne einen größten gemeinsamen Teiler h von f und g in $\mathbb{Q}[T]$ und finde Polynome p und q in $\mathbb{Q}[T]$, so dass $h = pf + qg$ gilt.

Ü 8.6. Sei K ein beliebiger Körper. Dann gibt es im Polynomring $K[T]$ unendlich viele normierte irreduzible Polynome.

KAPITEL V

Endlich algebraische Körpererweiterungen

1. Algebraische und transzendente Elemente

Sei L/K ("L über K") eine *Körpererweiterung* , d. h. K ist ein Teilkörper von L, bzw. L ist ein Erweiterungskörper von K. (Man beachte, dass bei dieser Schreibweise L/K keine Faktorbildung gemeint ist!) Sei $x \in L$. Dann bezeichne $K[x]$ die Teilmenge von L bestehend aus den Elementen der Form

$$a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$$

mit $n \geq 0$ und $a_i \in K$. Es ist also $K[x] = \{f(x) \mid f \in K[T]\}$.

Proposition 1.1

$K[x]$ ist der bzgl. Inklusion $\subseteq$ kleinste Unterring von L, der K und x enthält. Die Abbildung $\phi_x \colon K[T] \to K[x]$, $f \mapsto f(x)$ ist ein surjektiver Ringhomomorphisms.

Beweis. Offensichtlich. ■

Definition 1.2

$K[x]$ entsteht aus K durch *Ringadjunktion* des Elementes $x \in L$. "K adjungiert x."

Statt ab^{-1} schreiben wir häufig auch a/b, oder $\frac{a}{b}$.

Analog: $K(x)$ die Menge aller in L gebildeten Quotienten

$$q = \frac{a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n}{b_0 + b_1 x + b_2 x^2 + \cdots + b_m x^m}$$

mit a_i, $b_j \in K$ und $b_0 + b_1 x + b_2 x^2 + \cdots + b_m x^m \neq 0$. Also besteht $K(x)$ aus den Elementen der Form a/b mit a, $b \in K[x]$, $b \neq 0$. Oder anders: $K(x) = \{f(x)/g(x) \mid f, g \in K[T],\ g(x) \neq 0\}$.

Proposition 1.3

$K(x)$ ist der bzgl. Inklusion kleinste Teilkörper von L, welcher K und x enthält.

Beweis. Offensichtlich. ■

Definition 1.4

$K(x)$ heißt der aus K durch Adjunktion des Elementes $x \in L$ gebildete Teilkörper von L.

Beispiel. (a) Die Zahlen $a + b\sqrt{2}$ mit a, $b \in \mathbb{Q}$ bilden einen Teilkörper K des Körpers $\mathbb{R}$. Es gilt $K = \mathbb{Q}[\sqrt{2}] = \mathbb{Q}(\sqrt{2})$.

(b) Im Körper $\mathbb{C}$ ist

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

(c)* Es lässt sich zeigen, dass $\mathbb{Q}[\pi] \subsetneq \mathbb{Q}(\pi)$ gilt. (π ist transzendent, Satz von Lindemann (1882).) Ähnliches gilt für die Eulersche Zahl e (Hermite (1873)). Die Beweise

hierfür sind sehr aufwändig und verlangen analytische Methoden. — Tatsächlich ist eine zufällig gegebene komplexe (oder reelle) Zahl mit 100%iger (!) Wahrscheinlichkeit transzendent. Dennoch ist es enorm schwierig, deren Transzendenz zu beweisen. Erst 1844 wurde von Liouville gezeigt, dass transzendente Zahlen überhaupt existieren.

Definition 1.5 (*Algebraische Elemente*)

Sei L/K eine Körpererweiterung. Ein $x \in L$ heisst *algebraisch über* K, wenn es ein normiertes Polynom

$$f = T^n + a_{n-1}T^{n-1} + \cdots + a_1T + a_0 \in K[T]$$

gibt, das x als Nullstelle hat, also $f(x) = 0$ gilt. Falls es ein solches Polynom nicht gibt, heisst x *transzendent über* K.

Eine Körpererweiterung L/K heisst *algebraisch*, falls jedes $x \in L$ algebraisch über K ist. Anderfalls heisst L/K *transzendente* Körpererweiterung.

Bemerkung. (1) Der Bezug ("über") zum Grundkörper K ist stets zu benennen. Nur wenn $K = \mathbb{Q}$ und $x \in \mathbb{C}$ nennt man x algebraisch bzw. transzendent (ohne weiteren Bezug).

(2) Ein normiertes Polynom f ist immer verschieden vom Nullpolynom. Ist umgekehrt $f \in K[T]$ mit $f \neq 0$ und K ein Körper, sowie x eine Nullstelle von f, so ist x auch Nullstelle eines normierten Polynoms $g \in K[T]$. Man wählt nämlich $g = {a_n}^{-1} \cdot f$, wenn a_n der Leitkoeffizient von f ist. Daher können wir in der Definition ohne Einschränkung annehmen, dass f normiert ist.

Definition 1.6 (*Minimalpolynom*)

Sei L/K eine Körpererweiterung, und sei $x \in L$ algebraisch über K. Es gibt dann, nach Definition, ein normiertes Polynom $f \in K[T]$, $f \neq 0$, mit $f(x) = 0$. Dann gibt es auch ein solches f minimalen Grades, und dies heisst das *Minimalpolynom* von x *über* K. (Dies ist offenbar eindeutig bestimmt.) Wir schreiben auch $f = \mathrm{MIPO}(x/K)$.

Satz 1.7 (*Charakterisierungen des Minimalpolynoms*)

Sei L/K eine Körpererweiterung, sei $x \in L$ und $f \in K[T]$ ein normiertes Polynom. Dann sind äquivalent:

(1) *f ist das Minimalpolynom von x über K, d. h. $0 \neq f \in K[T]$ ist minimalen Grades mit $f(x) = 0$.*

(2) *f ist irreduzibel über K und es gilt $f(x) = 0$.*

(3) *$f(x) = 0$, und f teilt jedes Polynom $g \in K[T]$ mit $g(x) = 0$.*

Beweis. (1)⇒(2) Ist f nicht irreduzibel, so gibt es $g, h \in K[T]$ mit $\mathrm{grad}(g), \mathrm{grad}(h) \geq 1$ mit $f = gh$. Es gilt dann $g(x) = 0$ oder $h(x) = 0$, wobei g und h kleineren Grad als f haben.

(2)⇒(1) Sei f irreduzibel, und sei $g \in K[T]$ minimalen Grades mit $g(x) = 0$. Schreibe $f = qg + r$ mit $r = 0$, oder $\mathrm{grad}(r) < \mathrm{grad}(g)$. Wegen $r(x) = 0$ ist nur $r = 0$ möglich, also $f = qg$. Da f irreduzibel ist, folgt, dass q ein konstantes Polynom $\neq 0$ ist, und auch f hat minimalen Grad.

(1)⇒(3) Folgt wie im vorherigen Beweisteil per Division (durch f) mit Rest.

(3)⇒(1) Klar. ∎

Bemerkung. Sei L/K eine Körpererweiterung. Dann ist L insbesondere ein K-Vektorraum, in natürlicher Weise. Damit steht das ganze Repertoire der Linearen Algebra (lineare Gleichungen, Matrizen, Basen, Dimension, etc.) zur Untersuchung von L/K bereit. Insbesondere ist $\dim_K L$ definiert (endlich oder unendlich).

Definition 1.8

Sei L/K eine Körpererweiterung. Die Dimension $\dim_K(L)$ heisst auch der *(Körper-) Grad* von L über K und wird mit $[L : K]$ bezeichnet. Eine Körpererweiterung L/K heisst *endlich*, falls $[L : K]$ endlich ist. Allgemeiner schreiben wir auch für einen kommutativen Ring R, der den Körper K als Teilring enthält, $[R : K] = \dim_K(R)$.

Satz 1.9

Sei L/K eine Körpererweiterung. Sei $x \in L$ algebraisch über K und $f = \mathrm{MIPO}(x/K)$ mit $n = \mathrm{grad}(f)$. Dann gilt:

(1) $fK[T] = \mathrm{Kern}(\phi_x)$.
(2) $K[x] \simeq K[T]/fK[T]$.
(3) *Eine Basis des K-Vektorraums $K[x]$ ist gegeben durch die Elemente $1, x, x^2, \ldots, x^{n-1}$. Insbesondere $[K[x] : K] = n = \mathrm{grad}(f)$.*
(4) *$K[x]$ ist ein Körper. Also $K[x] = K(x)$.*

Beweis. (1) folgt aus dem vorherigen Satz. (2) aus dem Homomorphiesatz.

(3) Schreibe $f = T^n + \sum_{i=0}^{n-1} a_i T^i$, mit $a_i \in K$. Wegen $f(x) = 0$ ist

$$x^n = -a_0 - a_1 x - \cdots - a_{n-1} x^{n-1},$$

und mit Induktion folgt, dass $K[x]$ über K erzeugt wird von den Elementen $1, x, x^2, \ldots, x^{n-1}$. Da f minimalen Grades mit $f(x) = 0$ ist, folgt, dass diese Elemente auch linear unabhängig über K sind.

(4) Da $K[x]$ als Teilring des Körpers L nullteilerfrei ist, folgt dies aus Proposition II.5.7. ∎

Satz 1.10

Jede endliche Körpererweiterung L/K ist algebraisch.

Genauer gilt: Ist $[L : K] = n$, so gibt es zu jedem $x \in L$ ein normiertes Polynom $f \in K[T]$ vom Grad $\leq n$ mit $f(x) = 0$.

Beweis. Sei $x \in L$. Wegen $[L : K] = n$ sind die $n+1$ Elemente 1, x, $x^2, \ldots,$ x^n linear abhängig über K. Es gibt also $b_0, \ldots, b_n \in K$ nicht alle null mit

$$b_0 + b_1 x + \cdots + b_n x^n = 0.$$

Daraus folgt die Behauptung. ∎

Satz 1.11 (*Charakterisierungen algebraischer Elemente*)

Sei L/K eine Körpererweiterung, und sei $x \in L$. Dann sind äquivalent:

(1) *x ist algebraisch über K.*
(2) *$[K[x] : K]$ ist endlich.*
(3) *$K(x) = K[x]$.*
(4) *$K[x]$ ist ein Teilkörper von L.*

Beweis. (1)⇔(2) und (2)⇒(3) folgt aus den vorherigen Argumenten. (3)⇔(4) ist klar.

(3)⇒(1): Gilt $K(x) = K[x]$, so ist $K[x]$ ein Körper, und insbesondere ist x invertierbar in $K[x]$ (der Fall $x = 0$ ist uninteressant). Es gibt also eine natürliche Zahl n und Elemente $b_0, \ldots, b_{n-1} \in K$ mit

$$x^{-1} = b_0 + b_1 x + \cdots + b_{n-1} x^{n-1}.$$

Multiplikation der Gleichung mit x zeigt dann, dass x einer Polynomgleichung über K genügt, x ist also algebraisch über K. ∎

Folgerung 1.12

Sei L/K eine Körpererweiterung und $x \in L$ algebraisch über K. Dann ist die Körpererweiterung $K(x)/K$ algebraisch.

Beweis. Für alle $y \in K(x)$ gilt $[K(y) : K] \leq [K(x) : K] < \infty$. ∎

Ist x algebraisch über K, so heisst der Körpergrad $[K(x) : K]$ auch der Grad des Elements x über K.

Definition 1.13

Eine Körpererweiterung L/K heisst *einfach*, falls es ein $x \in L$ gibt mit $L = K(x)$. Ist in diesem Fall x algebraisch über K, so heisst sie *einfach algebraisch*, und x ein *primitives* (=erzeugendes) Element von L/K; andernfalls heisst L/K *einfach transzendent*.

Beispiel. $\mathbb{C}/\mathbb{R}$ ist wegen $\mathbb{C} = \mathbb{R}[i]$ einfach algebraisch. $\mathbb{Q}(\pi)/\mathbb{Q}$ ist einfach transzendent.*

Proposition 1.14 (*Einfach transzendente Erweiterungen; Kronecker (1882)*)

Sei L/K eine Körpererweiterung und $\alpha \in L$ transzendent über K. Dann ist $K(\alpha) \simeq K(T)$; genauer: Es gibt einen Isomorphismus $K(T) \xrightarrow{\sim} K(\alpha)$, der T auf α schickt und auf K wie die Identität wirkt.

Beweis. Definiere $K(T) \to K(\alpha)$, $f(T)/g(T) \mapsto f(\alpha)/g(\alpha)$, wobei $g(T) \neq 0$ gilt. Da α transzendent über K ist, folgt dann auch $g(\alpha) \neq 0$. Man prüft unmittelbar nach, dass dies wohldefiniert ist (unabhängig von der Darstellung des Bruches), ein Homomorphismus von Ringen, und nach Definition von $K(\alpha)$ ist die Abbildung auch surjektiv. Weil $K(T)$ ein Körper ist, ist sie offenbar auch injektiv. ∎

Anmerkung*: Es folgt etwa, dass $\mathbb{Q}(\pi) \simeq \mathbb{Q}(T) \simeq \mathbb{Q}(e)$ (mit $\pi \leftrightarrow T \leftrightarrow e$) gilt.

Bemerkung. [Allgemeinere Adjunktionen] Sind $x_1, x_2, \ldots$ Elemente in L so definiert man $K[x_1, x_2] \stackrel{def}{=} (K[x_1])[x_2]$ und $K(x_1, x_2) \stackrel{def}{=} (K(x_1))(x_2)$. Induktiv werden der Ring $K[x_1, \ldots, x_n]$ und der Körper $K(x_1, \ldots, x_n)$ definiert. Dies ist der kleinste Teilring (bzw. -körper) von L, der K und $\{x_1, \ldots, x_n\}$ enthält.

2. Einfach algebraische Körpererweiterungen

In Satz 1.9 hatten wir ein algebaisches Element $x \in L$ und dessen Minimalpolynom über K betrachtet, wobei L/K eine schon gegebene Körpererweiterung war. Der folgende wichtige Satz ist gewissermaßen eine Umkehrung davon, der uns zeigt, wie man einfach algebraische Körpererweiterungen "abstrakt" konstruieren kann, d. h. *ohne* in einem evtl. schon gegebenen Oberkörper zu argumentieren.

Satz 2.1 (*Satz von Kronecker (1887)*)

Sei K ein Körper. Sei $f \in K[T]$ normiert und irreduzibel vom Grad n. Dann ist $L = K[T]/fK[T]$ eine Körpererweiterung von K vom Grad $[L : K] = n$. Die Klasse $t = [T]$ von T in L ist eine Nullstelle von f in L, und es gilt $L = K(t)$. Ferner ist f das Minimalpolynom von t über K.

Beweis. Weil f ein Primelement in $K[T]$ ist, folgt unmittelbar, dass der Faktorring $K[T]/fK[T]$ ein Integritätsbereich ist. Offenbar ist $a \mapsto [a] = a + fK[T]$ ein injektiver Ringhomomorphismus $K \to K[T]/fK[T]$, womit K als Teilkörper von L identifiziert wird. (Vgl. auch nachfolgende Übung.)

Die Klassen $[1], [T], \ldots, [T^{n-1}]$ bilden eine K-Basis von L: Denn ist $[g] = g + fK[T] \in L$, so zeigt Division mit Rest, $g = qf + r$, dass $[g] = [r]$, und $r = 0$ oder $\operatorname{grad}(r) < n$, d. h. r wird von $1, T, \ldots, T^{n-1}$ erzeugt. Ist $\sum_{i=0}^{n-1} a_i[T^i] = 0$,

so ist $\sum_{i=0}^{n-1} a_i T^i \in fK[T]$, aber aus Gradgründen geht nur $\sum_{i=0}^{n-1} a_i T^i = 0$, also alle $a_i = 0$.

Weil nun L eine endlichdimensionale nullteilerfreie K-Algebra ist, folgt aus Proposition II.5.7, dass L ein Körper ist.

Ist $t = [T]$, so ist dann $L = K(t)$ unmittelbar klar. Einsetzen ergibt $f(t) = f([T]) = [f] = [0]$. Da f irreduzibel über K ist, ist f das Minimalpolynom von t über K (vgl. 1.7). ■

Beispiel. [Cauchy (1847)] $\mathbb{R}[T]/(T^2+1) \simeq \mathbb{R}[i] = \mathbb{C}$.

Ü 2.1. Seien K, L Körper und $j\colon K \to L$ ein Monomorphismus. Dann gibt es eine Körpererweiterung L'/K und einen Isomorphismus $\sigma\colon L' \to L$ mit $\sigma_{|K} = j$.

Definition 2.2

(1) Seien L/K und L'/K Körpererweiterungen. Ein Isomorphismus $\sigma\colon L \to L'$ heißt ein *K-Isomorphismus*, wenn $\sigma_{|K} = 1_K$ gilt. (Äquivalent: σ ist K-linear.)

(2) Ist dabei $L = L'$, so heißt σ ein *K-Automorphismus*.

(3) Allgemeiner: Ist $i\colon K \to K'$ ein Isomorphismus (bzw. ein Monomorphismus; vgl. anschließende Bemerkung) von Körpern, und sind L/K und L'/K' Körpererweiterungen, so nennen wir einen Isomorphismus (Monomorphismus) $\sigma\colon L \to L'$ *Isomorphismus (Monomorphismus) von Körpererweiterungen*, falls $\sigma_{|K} = i$ gilt.

(4) Im Falle $K = K'$ und $i = 1_K$ nennen wir einen Monomorphismus $\sigma\colon L \to L'$ mit $\sigma_{|K} = 1_K$ einen *K-Monomorphismus*.

(5) Ist $i\colon K \to K'$ ein Monomorphismus und $L' = K'$, so nennen wir einen Monomorphismus $\sigma\colon L \to K'$ mit $\sigma_{|K} = i$ eine *Fortsetzung* von i (auf L).

Bemerkung. Sei L ein Körper und R ein Ring, $R \neq \{0\}$, und sei $\sigma\colon L \to R$ ein Homomorphismus von Ringen. Dann ist offenbar σ injektiv. (Beachte $\sigma(1) = 1 \neq 0$.) Wir nennen dann σ auch einen Monomorphismus. Auch wenn dies automatisch der Fall ist, sprechen wir meist lieber von Monomorphismus als von Homomorphismus, besonders, wenn $R = L'$ ebenfalls ein Körper ist. Offenbar gilt: Sind L/K und L'/K Körpererweiterungen, so ist σ ein K-Monomorphismus genau dann, wenn σ K-linear ist.

Für einen Ringmorphismus $\sigma\colon R \to S$ definiere den Morphismus $\sigma^*\colon R[T] \to S[T]$ durch

$$\sigma^*(\sum_{i=0}^{n} a_i T^i) = \sum_{i=0}^{n} \sigma(a_i) T^i.$$

Für $f \in R[T]$ schreiben wir auch $f^\sigma = \sigma^*(f)$.

Lemma 2.3

Sei L/K und L'/K' Körpererweiterungen und $i\colon K \to K'$ ein Isomorphismus. Sei $\sigma\colon L/K \to L'/K'$ ein Isomorphismus von Erweiterungen. Ist $f \in K[T]$ und $x \in L$ eine Nullstelle von f, so ist $\sigma(x)$ eine Nullstelle von $i^*(f)$ in L'.

Beweis. Sei $f = \sum_{j=0}^{n} a_j T^j$. Dann gilt

$$i^*(f)(\sigma(x)) = \sum_{j=0}^{n} i(a_j)(\sigma(x))^j = \sum_{j=0}^{n} \sigma(a_j)\sigma(x^j) = \sigma(\sum_{j=0}^{n} a_j x^j) = \sigma(f(x)) = \sigma(0) = 0.$$ ■

Satz 2.4

Seien $K(\alpha)/K$ und $K(\beta)/K$ einfach algebraische Körpererweiterungen. Äquivalent sind:

(1) *Es gibt einen K-Isomorphismus $\sigma\colon K(\alpha) \xrightarrow{\sim} K(\beta)$ mit $\sigma(\alpha) = \beta$.*
(2) *α und β haben dasselbe Minimalpolynom $f \in K[T]$.*

Beweis. (2)⇒(1) Nach Satz 1.9 haben wir Isomorphismen $\sigma_\alpha\colon K[T]/(f) \to K(\alpha)$ und $\sigma_\beta\colon K[T]/(f) \to K(\beta)$, die die Elemente aus K festlassen und T auf α bzw. β schicken. Dann hat $\sigma := \sigma_\beta \circ {\sigma_\alpha}^{-1}$ die behauptete Eigenschaft in (1).

(1)⇒(2) Sei $f = \mathrm{MIPO}(\alpha/K)$. Aus dem Lemma folgt $f(\beta) = f(\sigma(\alpha)) = 0$. Da f irreduzibel ist, folgt $f = \mathrm{MIPO}(\beta/K)$. ∎

Oft ist es nützlich, vorstehende Aussage (2)⇒(1) allgemeiner zu haben:

Satz 2.5

Seien K und L Körper und $i\colon K \to L$ ein Isomorphismus. Seien $K(\alpha)/K$ und $L(\beta)/L$ einfach algebraische Körpererweiterungen. Sei $f \in K[T]$ das Minimalpolynom von α über K und $g \in L[T]$ das Minimalpolynom von β über L. Gilt $i^*(f) = g$, so gibt es einen Isomorphismus von Erweiterungen $j\colon K(\alpha)/K \to L(\beta)/L$ mit $j(\alpha) = \beta$.

Beweis. Wie oben, nur dass man noch den von $i^*\colon K[T] \to L[T]$ induzierten Isomorphismus $K[T]/(f) \to L[T]/(i^*(f))$ (Homomorphiesatz!) zwischenschaltet. Konkret wird hier also für $x = a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-1}\alpha^{n-1} \in K(\alpha)$ definiert

$$j(x) := i(a_0) + i(a_1)\beta + i(a_2)\beta^2 + \cdots + i(a_{n-1})\beta^{n-1} \in L(\beta). \tag{2.1}$$

∎

3. Der Gradsatz

Der folgende Satz ist von ähnlich grundlegender Bedeutung wie der Satz von Lagrange in der Gruppentheorie:

Satz 3.1 (*Gradsatz*)

Sei $K \subseteq L \subseteq M$ ein Körperturm. $[M : K]$ ist genau dann endlich, wenn $[M : L]$ und $[L : K]$ endlich sind. In dem Fall gilt

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

Man beweist dazu die folgende stärkere Aussage, die auch selbst sehr nützlich und wichtig ist.

Zusatz 3.2

Sei $K \subseteq L \subseteq M$ ein Körperturm. Ist $\ell_1, \ldots, \ell_p$ eine K-Basis von L und $m_1, \ldots, m_q$ eine L-Basis von M, so ist die pq-elementige Menge

$$\{\ell_i m_j \mid i = 1, \ldots, p,\ j = 1, \ldots, q\}$$

eine K-Basis von M.

Beweis. Man zeigt leicht die lineare Unabhängigkeit und die Erzeugendeneigenschaft für die $\ell_i m_j$ über K, indem man sie mittels

$$\sum_{i,\,j} \alpha_{ij}\ell_i m_j = \sum_{j=1}^{q}\Big(\sum_{i=1}^{p} \alpha_{ij}\ell_i\Big)m_j$$

auf die entsprechenden Eigenschaften der ℓ_i über L und der m_j über K zurückführt. ∎

Beispiel. $x = \sqrt{i}$ ist Nullstelle des Polynoms $T^4 + 1$. Es gilt $\sqrt{i} = \frac{1}{2}(\sqrt{2} + i\sqrt{2})$. Schauen wir uns die Körpererweiterung $\mathbb{Q}(i, \sqrt{2})/\mathbb{Q}$ an. Es gilt $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$. Weil $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{R}$ und $i \notin \mathbb{R}$, gilt auch $[\mathbb{Q}(i, \sqrt{2}) : \mathbb{Q}(\sqrt{2})] = 2$, und damit nach dem Gradsatz

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

Es ist 1, $\sqrt{2}$ eine $\mathbb{Q}$-Basis von $\mathbb{Q}(\sqrt{2})$ und 1, i eine $\mathbb{Q}(\sqrt{2})$-Basis von $\mathbb{Q}(i,\sqrt{2})$. Nach dem Zusatz ist deswegen

$$1,\ i,\ \sqrt{2},\ i\sqrt{2}$$

eine $\mathbb{Q}$-Basis von $\mathbb{Q}(i,\sqrt{2})$. Außerdem gilt $\mathbb{Q}(\sqrt{i}) = \mathbb{Q}(i,\sqrt{2})$: Wegen $\sqrt{i} = \frac{1}{2}(\sqrt{2} + i\sqrt{2}) \in \mathbb{Q}(i,\sqrt{2})$, also $\mathbb{Q}(\sqrt{i}) \subseteq \mathbb{Q}(i,\sqrt{2})$. Sollte diese Inklusion echt sein, so muss $[\mathbb{Q}(\sqrt{i}) : \mathbb{Q}] < 4$ ein Teiler von 4 sein, also $= 1$ oder $= 2$. Offenbar kann er nicht $= 1$ sein. Er kann aber auch nicht $= 2$ sein, denn sonst müsste $i = \sqrt{i}^2$ sich als LKB über $\mathbb{Q}$ in 1, $\sqrt{i} = \frac{1}{2}(\sqrt{2} + i\sqrt{2})$ darstellen lassen. Da aber 1, i, $\sqrt{2}$, $i\sqrt{2}$ linear unabhängig über $\mathbb{Q}$ sind, ist dies nicht möglich. Es folgt $[\mathbb{Q}(\sqrt{i} : \mathbb{Q}] = 4$, und da mit $f = T^4 + 1 \in \mathbb{Q}[T]$ ein normiertes Polynom vom Grad 4 ist mit $f(x) = 0$, gilt $\mathrm{MIPO}(x/\mathbb{Q}) = T^4 + 1$.

Folgerung 3.3

Sei L/K eine Körpererweiterung. Sind $x_1, \ldots, x_n \in L$ sämtlich algebraisch über K, so gilt

$$K(x_1, \ldots, x_n) = K[x_1, \ldots, x_n],$$

und dies ist eine endliche Körpererweiterung von K.

Beweis. Induktion nach n. Für $n = 1$ wissen wir die Aussage schon. Es ist

$$\begin{aligned} K[x_1, \ldots, x_n] &= K[x_1, \ldots, x_{n-1}][x_n] \\ &\overset{IV}{=} K(x_1, \ldots, x_{n-1})[x_n] \\ &\overset{1.11}{=} K(x_1, \ldots, x_{n-1})(x_n) \\ &= K(x_1, \ldots, x_n). \end{aligned}$$

■

Satz 3.4 (*Charakterisierung endlicher Körpererweiterungen*)

Sei L/K eine Körpererweiterung. Äquivalent sind:

(1) *L/K ist endlich.*
(2) *Es gibt endlich viele über K algebraische Elemente $x_1, \ldots, x_n \in L$ mit $L = K(x_1, \ldots, x_n)$.*

Beweis. (2)⇒(1) Nach der vorstehenden Folgerung.

(1)⇒(2) Ist L/K endlich, so gibt es eine endliche K-Basis $y_1, \ldots, y_m \in L$. Damit gilt insbesondere $L = K(y_1, \ldots, y_m)$, und wegen $[K(y_i) : K] \leq [L : K] < \infty$ sind alle y_i algebraisch über K. ■

Bemerkung. Aufgrund des Satzes nennt man eine endliche Körpererweiterung auch manchmal *endlich algebraisch*.

Proposition 3.5 (*Interner algebraischer Abschluss*)

L/K sei Körpererweiterung. Es gilt

(1) *Die über K algebraischen Elemente in L bilden einen Teilkörper L_a von L.*
(2) *L_a ist der größte Teilkörper von L, der über K algebraisch ist.*
(3) *Jedes Element aus L, welches über L_a algebraisch ist, liegt schon in L_a.*

Beweis. (1) Seien $x, y \in L$ algebraisch über K. Dann gilt $x + y \in K(x, y)$, also $[K(x + y) : K] \leq [K(x, y) : K] < \infty$, und analoges gilt für $x \cdot y$. Ist $x \neq 0$, so gilt $x^{-1} \in K(x)$, also auch $[K(x^{-1}) : K] \leq [K(x) : K] < \infty$. Also sind $x + y$, xy und x^{-1} algebraisch über K, und es folgt, dass L_a ein Körper ist.

(2) ist trivial.

(3) Sei $x \in L$ algebraisch über L_a. Dann gibt es ein normiertes $f \in L_a[T]$ mit $f(x) = 0$. Sei etwa $f = T^n + a_{n-1}T^{n-1} + \cdots + a_1T + a_0$, wobei $a_0, \ldots, a_{n-1}$ algebraisch über K sind. Dann ist offenbar x algebraisch über $M = K(a_0, \ldots, a_{n-1})$. Es folgt

$$[K(x) : K] \leq [M(x) : K] = [M(x) : M] \cdot [M : K] < \infty,$$

weil beide Faktoren endlich sind. Also ist x algebraisch über K, d. h. $x \in L_a$. ∎

Bemerkung. Man schreibt auch $L_a = \overline{K}$, wobei bei dieser Notation aber zu betonen ist, dass es relativ L gemeint ist. Dann besagt (3) symbolisch ausgedrückt $\overline{\overline{K}} = \overline{K}$.

Beispiel. $\overline{\mathbb{Q}}$ in $\mathbb{C}$ ist die Menge der algebraischen Zahlen.

Folgerung 3.6 (*Transitivität algebraischer Erweiterungen*)

Es sei $K \subseteq L \subseteq M$ ein Körperturm. Die Erweiterung M/K ist genau dann algebraisch, wenn die beiden Erweiterungen M/L und L/K beide algebraisch sind.

Beweis. (1) [Transitivität] Seien M/L und L/K algebraisch. Dann gilt $L \subseteq \overline{K}$, dem algebraischen Abschluss von K in M. Sei $x \in M$. Dies ist algebraisch über L, also erst recht über $\overline{K}$. Nach dem Resultat zuvor gilt dann $x \in \overline{K}$, also ist x algebraisch über K. Es folgt, dass M/K algebraisch ist.

(2) Die andere Richtung ist trivial: Sei M/K algebraisch. Jedes $x \in M$ ist über K, also erst recht über L algebraisch. Also ist M/L algebraisch. Da jedes Element von M algebraisch über K ist, ist insbesondere jedes Element von L algebraisch über K. Also ist auch L/K algebraisch. ∎

Aufgaben

Ü 3.1. Für eine Körpererweiterung L/K sind äquivalent:
(1) L/K ist algebraisch.
(2) Jeder Ring R mit $K \subseteq R \subseteq L$ (Teilringe) ist ein Körper.

Ü 3.2. Sei L/K eine Körpererweiterung, und sei $0 \neq x \in L$ algebraisch über K. Dann haben MIPO(x/K) und MIPO(x^{-1}/K) denselben Grad.

Ü 3.3. Seien $a, b \in \mathbb{R}$ und $z = a + ib \in \mathbb{C}$. Dann: z ist algebraisch $\Leftrightarrow$ a und b sind algebraisch.

Ü 3.4. Für den Körper $\overline{\mathbb{Q}}$ der komplexen algebraischen Zahlen gilt: $\overline{\mathbb{Q}}/\mathbb{Q}$ ist algebraisch und $[\overline{\mathbb{Q}} : \mathbb{Q}] = \infty$, genauer: abzählbar unendlich.

4. Berechnung von Minimalpolynomen

Beispiel. Betrachte $L = \mathbb{Q}(\sqrt{i})/\mathbb{Q}$. Wir haben schon gesehen, dass 1, i, $\sqrt{2}$, $i\sqrt{2}$ eine $\mathbb{Q}$-Basis von L ist.

(1) Sei $x = 2i + \sqrt{2}$. Wir wollen das Minimalpolynom von x über $\mathbb{Q}$ berechnen. Dazu stellen wir die Elemente 1, x, $x^2, \ldots$ als Linearkombination in der oben gegebenen Basis dar. Die Koeffizienten schreiben wir als Spalten einer Matrix:

1	x	x^2	x^3	x^4
1	0	-2	0	-28
0	2	0	4	0
0	1	0	-10	0
0	0	4	0	-16

Da nach dem Gradsatz $[L : \mathbb{Q}] = 4$, müssen wir hier maximal bis x^4 gehen und stellen x^4 (sofern dies nicht schon vorher möglich ist), als Linearkombination in den vorherigen Potenzen von x dar. Hier sehen wir, dass die ersten vier Spaltenvektoren linear unabhängig sind, also 1, x, x^2, x^3 sind linear unabhängig. Daher muss MIPO$(x/\mathbb{Q})$ den Grad 4 haben, und man sieht, indem man die letzte Spalte als LKB der vorderen Spalten darstellt, $x^4 = -4x^2 - 36$, und damit MIPO$(x/\mathbb{Q}) = T^4 + 4T^2 + 36$.

(2) $x = 1 + \sqrt{2} + i$.

1	x	x^2	x^3	x^4
1	1	2	4	0
0	1	2	8	24
0	1	2	2	0
0	0	2	6	16

Man sieht $x^4 = 4x^3 - 4x^2 - 8$, also $\mathrm{MIPO}(x/\mathbb{Q}) = T^4 - 4T^3 + 4T^2 + 8$.

Bemerkung. Es sei L/K eine Körpererweiterung und $0 \neq x \in L$. Dann haben die Elemente x und $1/x$ denselben Grad über K. Denn es gilt $K(x) = K(1/x)$.

Beispiel. Minimalpolynom von $x = 1 + i + \sqrt{2}$ über $\mathbb{Q}$ ist $T^4 - 4T^3 + 4T^2 + 8$, das von $1/x$ ist $T^4 + 1/2T^2 - 1/2T + 1/8$.

5. Konstruktionen mit Zirkel und Lineal

- Dreiteilung des Winkels.
- Verdoppelung des Würfels (Delisches Problem).
- Quadratur des Kreises.
- Konstruktion des regelmäßigen n-Ecks.

Definition 5.1

Es sei M eine Teilmenge von $\mathbb{C}$, welche die Punkte 0 und 1 enthält.

(1) Eine Gerade G heisst *unmittelbar* aus M *konstruierbar*, wenn es Elemente z_1, $z_2 \in M$ mit $z_1 \neq z_2$ so gibt, dass z_1, $z_2 \in G$.

(2) Ein Kreis heisst *unmittelbar* aus M *konstruierbar*, wenn es Elemente z_0, z_1, z_2 in M so gibt, dass K der Kreis um z_0 mit Radius $|z_1 - z_2|$ ist.

(3) Ein Punkt $z \in \mathbb{C}$ heisst *unmittelbar* aus M *konstruierbar*, wenn es A und B mit $A \neq B$ und $z \in A \cap B$ so gibt, dass A und B jeweils eine unmittelbar aus M konstruierbare Gerade oder einen unmittelbar aus M konstruierbaren Kreis bedeuten.

Definition 5.2

Wir setzen $M^{(0)} = M$ und erklären rekursiv $M^{(n+1)}$ als die Menge der unmittelbar aus $M^{(n)}$ konstruierbaren Punkte aus $\mathbb{C}$. Definitionsgemäß heißt dann

$$K(M) = \bigcup_{n \in \mathbb{N}} M^{(n)}$$

die Menge der ausgehend von M *mit Zirkel und Lineal konstruierbaren Punkte*.

Wir nennen ein $z \in \mathbb{C}$ (schlechthin) (mit Zirkel und Lineal) *konstruierbar*, wenn z ausgehend von der Menge $\{0, 1\}$ konstruierbar ist. Wir nehmen im folgenden immer $M = \{0, 1\}$ an.

Satz 5.3

Sei $M = \{0, 1\}$. Dann ist $K(M)$ der kleinste Teilkörper K von $\mathbb{C}$ mit folgenden Eigenschaften (1) und (2):

(1) *$z \in K \Rightarrow \overline{z} \in K$;*

(2) *Ist $z \in \mathbb{C}$ Lösung einer quadratischen Gleichung $z^2 + az + b = 0$ mit Koeffizienten $a, b \in K$, so folgt $z \in K$. (Oder kürzer: $z \in K \Rightarrow \sqrt{z} \in K$.)*

Kurz: $K(M)$ ist der kleinste Teilkörper von $\mathbb{C}$, der unter komplexer Konjugation[1] und Quadratwurzelziehen abgeschlossen ist[2].

[1] Anmerkung: Auf diese Eigenschaft (1) kann verzichtet werden, vgl. Lemma 5.9 unten; aus beweistechnischen Gründen fordern wie sie hier mit.

[2] Man nennt $K(M)$ (für $M = \{0, 1\}$) auch den pythagoräischen Abschluss von $\mathbb{Q}$.

Beweis. (0) $K(M)$ ist ein Teilkörper von $\mathbb{C}$: Sind z und w in $K(M)$, so erhält man $z-w$ als Schnittpunkt des Kreises um z mit Radius $|w|$ und des Kreises um $-w$ mit Radius $|z|$. Sei $z \in \mathbb{C}$, $z \neq 0$. In Polarkoordinaten, $z = re^{i\alpha}$. Dann gilt offenbar

$$z \in K(M) \quad \Leftrightarrow \quad r,\, e^{i\alpha} \in K(M).$$

Seien nun $z = re^{i\alpha}$ und $w = se^{i\beta}$ in $K(M) \setminus \{0\}$. Wir wollen zeigen, dass dann auch $z/w \in K(M)$ gilt. Dazu genügt es zu zeigen, dass r/s und $e^{i(\alpha-\beta)}$ in $K(M)$ sind.

(a) Für r/s können wir $r \neq s$ annehmen. Es ist $i \in K(M)$, und dann $1+i \in K(M)$. Sei A die Gerade durch 0 und $1+i$. Sei $a \in A$ Schnittpunkt des Kreises um 0 mit Radius r mit A, und b der Schnittpunkt mit dem Kreis um 0 mit Radius s. Wir können annehmen, dass a und b im ersten Quadranten liegen. Sei B die Gerade durch 1 und b. Wir können dann eine Parallele B' konstruieren, die durch den Punkt a geht. Der Schnittpunkt von B' mit der reellen Achse heiße c. Der Strahlensatz sagt uns nun

$$\frac{r}{s} = \frac{|a|}{|b|} = \frac{c}{1}.$$

Der konstruierte Punkt $c \in K(M)$ ist also r/s.

(b) Mit $w = e^{i\beta}$ ist auch $\overline{w} = e^{i(-\beta)}$ in $K(M)$. Wir müssen also nur eine Winkeladdition konstruieren. Das ist einfach.

Es folgt, dass $K(M)$ ein Teilkörper von $\mathbb{C}$ ist. (Insbesondere enthält $K(M)$ als Teilkörper $\mathbb{Q}$.) Wir zeigen die Eigenschaften (1) und (2):

(1) Die einfache Konstruktion haben wir eben schon verwendet.

(2) Sei $z \in K(M) \setminus \{0\}$. Wir zeigen $\sqrt{z} \in K(M)$. Schreibe $z = re^{i\alpha}$. Es ist $\sqrt{z} = \sqrt{r}e^{i\alpha/2}$. Die Winkelhalbierung ist einfach zu konstruieren. Es sind r, 0 und -1 in $K(M)$. Der Mittelpunkt der Strecke zwischen -1 und r ist $\frac{r-1}{2}$. Wir schlagen einen Kreis B um diesen Punkt, so dass -1 und r die Schnittpunkte von B mit der reellen Achse sind. Der Schnittpunkt von B mit der imaginären Achse heiße a. Die Punkte -1, r und a bilden die Ecken des rechtwinkligen Dreiecks im Thaleskreis, die Länge der Verbindung zwischen 0 und a bildet die Höhe h des Dreiecks. Der Höhensatz (mehrfache Anwendung des Satzes von Pythagoras) sagt $h^2 = |-1| \cdot r$. Es ist also $h = |a| \in K(M)$ Quadratwurzel von r.

Gilt $z^2 + az + b = 0$ mit $a, b \in K(M)$, so gilt $z = -\frac{a}{2} \pm \sqrt{\frac{a^2}{4} - b}$, also $z \in K(M)$ nach dem vorherigen Argument.

(3) Sei nun K ein Teilkörper von $\mathbb{C}$, der die Eigenschaft (1) und (2) erfüllt. Wir haben $K(M) \subseteq K$ zu zeigen. Dazu zeigen wir per Induktion, dass $M^{(n)} \subseteq K$ gilt für jedes $n \geq 0$: Es gilt $M^{(0)} = M = \{0, 1\} \subseteq K$ trivialerweise. Sei $n \geq 0$, und wir nehmen an, wir hätten bereits $M^{(n)} \subseteq K$ gezeigt. Wir zeigen $M^{(n+1)} \subseteq K$: Sei $z \in M^{(n+1)}$, also $z \in A \cap B$, $A \neq B$, mit drei möglichen Fällen:

(a) A und B sind Geraden; $a_1, a_2 \in A$, $a_1 \neq a_2$, $b_1, b_2 \in B$, $b_1 \neq b_2$, und $a_1, a_2, b_1, b_2 \in M^{(n)} \subseteq K$. Es gilt

$$A = \{a + tc \mid t \in \mathbb{R}\}, \quad B = \{b + sd \mid s \in \mathbb{R}\},$$

mit $a = a_1$, $c = a_2 - a_1$, $b = b_1$, $d = b_2 - b_1 \in K$. Man kann dies auch so schreiben:

$$A = \{w \in \mathbb{C} \mid \overline{c}(w-a) = c(\overline{w-a})\},\ B = \{w \in \mathbb{C} \mid \overline{d}(w-b) = d(\overline{w-b})\},$$

denn ist $\overline{c}(w-a)$ reell, so erhält man mit $t := \overline{c}(w-a)/\overline{c}c \in \mathbb{R}$, dass $w = a + tc$ gilt; umgekehrt folgt aus $w = a + tc$, dass $\overline{c}(w-a) = tc\overline{c}$ reell ist. Es ist also $(z, \overline{z})^t$ eine Lösung des linearen Gleichungssystems

$$\begin{pmatrix} \overline{c} & -c \\ \overline{d} & -d \end{pmatrix} \begin{pmatrix} z \\ \overline{z} \end{pmatrix} = \begin{pmatrix} -c\overline{a} + \overline{c}a \\ -d\overline{b} + \overline{d}b \end{pmatrix}.$$

Diese ist eindeutig, denn z ist der einzige Schnittpunkt zweier ungleicher Geraden; gleichbedeutend: die Richtungsvektoren c und d sind nicht reell-proportional, was äquivalent ist dazu, dass die Determinante $-\overline{c}d + c\overline{d} \neq 0$ ist. Da alle Koeffizienten

in K sind, gilt $z, \overline{z} \in K$, denn

$$\begin{pmatrix} z \\ \overline{z} \end{pmatrix} = \begin{pmatrix} \overline{c} & -c \\ \overline{d} & -d \end{pmatrix}^{-1} \cdot \begin{pmatrix} -c\overline{a} + \overline{c}a \\ -d\overline{b} + \overline{d}b \end{pmatrix}.$$

(b) A ist Gerade und B ein Kreis. Konkret:

$$\begin{aligned} A: &\quad \overline{b}(w-a) - b(\overline{w-a}) = 0 \\ B: &\quad (w-c)(\overline{w-c}) = s^2 \quad (= |w-c|^2), \end{aligned}$$

mit $a, b \in M^{(n)} \subseteq K$, $b \neq 0$ (wie oben) und $c \in M^{(n)} \subseteq K$ und $s = |p-q|$, $p, q \in M^{(n)} \subseteq K$. Nutzt man nun $z \in A \cap B$, so sieht man, dass z Nullstelle eines quadratischen Polynoms $f \in K[T]$ ist, also wegen (2) folgt $z \in K$.

(c) A und B sind Kreise. Konkret:

$$\begin{aligned} A: &\quad (w-a)(\overline{w-a}) = r^2 \\ B: &\quad (w-b)(\overline{w-b}) = s^2, \end{aligned}$$

mit $a, b, r, s \in M^{(n)} \subseteq K$ mit $a \neq b$ (und r, s Beträge von Differenzen von Elementen in $M^{(n)}$). Nutzt man $z \in A \cap B$, zieht die erste Gleichung von der zweiten ab, so erhält man mit $c := s^2 - r^2 + a\overline{a} - b\overline{b} \in K \cap \mathbb{R}$, dass z den Gleichungen B und

$$A': \quad (\overline{a-b})w + (a-b)\overline{w} + c = 0$$

genügt. Multipliziert man die letzte Gleichung mit i, setzt $e := i \cdot (b-a) \in K$ und dann $f := c/2\,\mathrm{Im}(e) \in K \cap \mathbb{R}$, so erfüllt z die Gleichung $\overline{e}w - e\overline{w} + ic = 0$, und wegen $ic = 2if\,\mathrm{Im}(e) = 2i\,\mathrm{Im}(e\overline{f}) = e\overline{f} - \overline{e}f$ die Geradengleichung

$$A'': \quad \overline{e}(w-f) - e(\overline{w-f}) = 0.$$

Wir können nun den Fall (b) anwenden.

In jedem Fall ergibt sich also $z \in K$. Damit $M^{(n+1)} \subseteq K$, und schließlich $K(M) \subseteq M$. ■

Satz 5.4

Für eine komplexe Zahl z sind äquivalent:

(1) *z ist konstruierbar, d. h. $z \in K(\{0,1\})$.*

(2) *Es gibt einen Körperturm*

$$\mathbb{Q} = K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_{n-1} \subset K_n$$

mit Schritten vom Grad $[K_i : K_{i-1}] = 2$ (für alle $1 \leq i \leq n$), welcher z erreicht, d. h. $z \in K_n$.

Der Beweis wird weiter unten geführt.

Folgerung 5.5 (*Notwendiges Kriterium für Konstruierbarkeit*)

Jede konstruierbare komplexe Zahl z ist algebraisch über $\mathbb{Q}$ und der Grad $[\mathbb{Q}(z) : \mathbb{Q}]$ ist eine Potenz von 2. ■

Bemerkung. Die Umkehrung der Folgerung gilt nur in modifizierter Form, die wir auch erst mit mehr Theorie (Galoistheorie) beweisen können. Vgl. Satz VII.8.1.

Folgerung 5.6

Die Zahl π ist nicht konstruierbar. Damit ist die Quadratur des Kreises nicht lösbar.

Beweis. π ist nicht algebraisch. (Satz von Lindemann[3] (1882).)

[3]Auf den nicht-trivialen Beweis, der analytische Methoden verwendet, können wir hier nicht eingehen. Wir verweisen auf die Bücher von Lang oder Morandi oder Stewart im Literaturverzeichnis.

■

Folgerung 5.7

Die Zahl $\sqrt[3]{2}$ ist nicht konstruierbar. Damit ist die Verdoppelung des Würfels (das Delische Problem) nicht lösbar.

Beweis. Für $\alpha = \sqrt[3]{2}$ gilt (vgl. Kriterium von Eisenstein) $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$. ■

Folgerung 5.8

$\zeta = e^{2\pi i/9}$ (= 40°-Winkel) ist nicht konstruierbar, dagegen ζ^3 (= 120°-Winkel) aber schon. Damit ist die Dreiteilung des Winkels nicht lösbar.

Beweis. Es ist $\omega := \zeta^3 = \frac{-1+i\sqrt{3}}{2}$. Diese Zahl ist konstruierbar. Angenommen, auch ζ selbst wäre konstruierbar. Dann auch $\zeta^{-1} = \bar{\zeta}$ und $\alpha := \zeta + \zeta^{-1}$. Offenbar gilt $\omega^3 = 1$ und $\omega^2 + \omega + 1 = 0$. Damit $\zeta^6 + \zeta^3 = -1$. Es folgt $\alpha^3 = (\zeta + \zeta^{-1})^3 = \zeta^3 + 3\zeta + 3\zeta^{-1} + \zeta^{-3} = 3\alpha - 1$ (beachte $\zeta^{-3} = \zeta^6$). Das Polynom $T^3 - 3T + 1$ ist irreduzibel über $\mathbb{Q}$, weil es keine rationale Nullstelle hat. Also $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$, was keine Zweierpotenz ist, Widerspruch. ■

Die Nichtlösbarkeit der Verdoppelung des Würfels und der Dreiteilung des Winkels wurde zuerst von L. P. Wantzel 1837 gezeigt.

Bemerkung. Wir werden später sehen, dass das reguläre n-Eck genau dann konstruierbar ist, wenn $\varphi(n)$ eine Potenz von 2 ist. Hier ist φ die Eulersche φ-Funktion, welche bei gegebener Primzahlfaktorisierung

$$n = p_1^{r_1} \cdots p_t^{r_t}$$

durch

$$\varphi(n) = \left(p_1^{r_1} - p_1^{r_1-1}\right) \cdots \left(p_t^{r_t} - p_t^{r_t-1}\right)$$

erklärt ist. Wir werden den Nachweis dieses Satzes an späterer Stelle führen, wenn uns stärkere Hilfsmittel der Galoistheorie zur Verfügung stehen.

Beweis von Satz 5.4. Wir nehmen ab jetzt $M = \{0, 1\}$ an. Dann ist die Eigenschaft (1), Abgeschlossenheit gegenüber komplexer Konjugation, in Satz 5.3 nicht nötig, sondern automatisch erfüllt. Dies folgt aus dem folgenden allgemeineren Lemma.

Lemma 5.9

Sei $\tau\colon \mathbb{C} \to \mathbb{C}$ ein Ringautomorphismus des Körpers $\mathbb{C}$. Sei $K \subseteq \mathbb{C}$ der kleinste Teilkörper von $\mathbb{C}$, der abgeschlossen ist unter Lösungen von quadratischen Gleichungen. Dann gilt $\tau(K) \subseteq K$.

Beweis. Setze $K' = \tau^{-1}(K)$. Seien $f' = T^2 + a'T + b' \in K'[T]$ und $x \in \mathbb{C}$ mit $f'(x) = 0$. Dann gilt mit $a = \tau(a')$, $b = \tau(b')$, $y = \tau(x)$ und $f = T^2 + aT + b \in K[T]$:

$$f(y) = \tau(f'(x)) = \tau(0) = 0.$$

Wegen der Abgeschlossenheit von K folgt $y \in K$ und damit $x = \tau^{-1}(y) \in K'$. Also ist auch K' abgeschlossen unter Lösungen von quadratischen Gleichungen, und wegen der Minimalitätseigenschaft von K folgt $K \subseteq K'$. Sei nun $x \in K$. Dann gilt $x \in K'$, also $x = \tau^{-1}(y)$ für ein $y \in K$. Es folgt $\tau(x) = y \in K$. Es folgt $\tau(K) \subseteq K$. ■

$z \in \mathbb{C}$ heisst *erreichbar*, wenn es einen Körperturm

$$\mathbb{Q} = K_0 \subset K_1 \subset \cdots \subset K_n$$

in $\mathbb{C}$ gibt, so dass alle $[K_i : K_{i-1}] = 2$ gilt $(1 \leq i \leq n)$, welcher z erreicht, d. h. $z \in K_n$. Mit $\widehat{\mathbb{Q}}$ bezeichnen wir die Menge aller erreichbaren $z \in \mathbb{C}$.

Proposition 5.10

$\widehat{\mathbb{Q}}$ ist ein Teilkörper von $\mathbb{C}$ mit folgender Eigenschaft:

- *Genügt $z \in \mathbb{C}$ einer quadratischen Gleichung über $\widehat{\mathbb{Q}}$, so gilt schon $z \in \widehat{\mathbb{Q}}$.*

Beweis. Seien $z, w \in \widehat{\mathbb{Q}}$. Es gibt Körpertürme

$$\mathbb{Q} = K_0 \subset K_1 \subset \cdots \subset K_n$$

und

$$\mathbb{Q} = L_0 \subset L_1 \subset \cdots \subset L_m$$

mit $[K_i : K_{i-1}] = 2$ und $[L_j : L_{j-1}] = 2$, mit $z \in K_n$ und $w \in L_m$. Es gibt α_i vom Grad 2 über K_{i-1} mit $K_i = K_{i-1}(\alpha_i)$ und β_j vom Grad 2 über L_{j-1} mit $L_i = L_{j-1}(\beta_j)$. Es ist dann $K_i = \mathbb{Q}(\alpha_1, \ldots, \alpha_i)$ und $L_j = \mathbb{Q}(\beta_1, \ldots, \beta_j)$. Man betrachtet nun den Körperturm

$$\mathbb{Q} \subset \mathbb{Q}(\alpha_1) \subset \cdots \subset \mathbb{Q}(\alpha_1, \ldots, \alpha_n) \subseteq \mathbb{Q}(\alpha_1, \ldots, \alpha_n, \beta_1) \subseteq \cdots \subseteq \mathbb{Q}(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m),$$

wobei in dem größten der Körper die Elemente z und w, und somit auch $z - w$ und z/w (sofern $w \neq 0$) liegen. Jedes β_j hat den Grad 2 über L_{j-1}, also einen Grad ≤ 2 über $K_n(\beta_1, \ldots, \beta_{j-1})$. Lässt man Indizes j mit $L_j = L_{j-1}$ aus, so erhält man einen Körperturm mit Gradschritten 2, der $z - w$ und z/w erreicht.

Sei nun $z \in \mathbb{C}$ eine Lösung von $z^2 + az + b = 0$, wobei $a, b \in \widehat{\mathbb{Q}}$ gilt. Dann werden a und b von einem gemeinsamen Körperturm der obigen Form erreicht, etwa $a, b \in K_n$. Es ist dann $z \in K_{n+1} := K_n(\sqrt{a^2/4 - b})$ und $[K_{n+1} : K_n] \leq 2$. ∎

Proposition 5.11

Für $M = (\{0, 1\})$ gilt $K(M) = \widehat{\mathbb{Q}}$.

Beweis. "$\subseteq$" Beide Teilkörper, $K(M)$ und $\widehat{\mathbb{Q}}$, sind abgeschlossen bzgl. Lösungen von quadratischen Gleichungen, und nach Satz 5.3 (und Lemma 5.9) ist $K(M)$ der kleinste solche. Also folgt $K(M) \subseteq \widehat{\mathbb{Q}}$.

"$\supseteq$" Sei

$$\mathbb{Q} = K_0 \subset K_1 \subset \cdots \subset K_n$$

ein Körperturm in $\mathbb{C}$ mit $[K_i : K_{i-1}] = 2$ für $1 \leq i \leq n$. Man zeigt induktiv für $i = 0, \ldots, n$, dass $K_i \subseteq K(M)$ gilt. Für $i = 0$ ist dies wegen $K_0 = \mathbb{Q}$ klar. Es sei bereits gezeigt, dass $K_{i-1} \subseteq K(M)$ gilt. Sei $z \in K_i$. Wir können $z \notin K_{i-1}$ annehmen. Dann erfüllt z wegen $[K_i : K_{i-1}] = 2$ eine quadratische Gleichung $z^2 + az + b = 0$ mit $a, b \in K_{i-1}$. Es folgt $a, b \in K(M)$, und nach Satz 5.3 folgt $z \in K(M)$. ∎

Aufgaben

Ü 5.1. Das reguläre 5-Eck ist mit Zirkel und Lineal konstruierbar. Man beschreibe explizit eine Konstruktionsanleitung.

Ü 5.2. Das reguläre 7-Eck ist *nicht* konstruierbar.

Ü 5.3. Sei $z := e^{2\pi i/18} \in \mathbb{C}$, und sei α der Realteil von z.

(1) Es gilt $8\alpha^3 = 6\alpha + 1$. (Hinweis: $1/2 = \cos(3 \cdot 2\pi/18) = \mathrm{Re}(e^{3 \cdot 2\pi i/18})$ und $\alpha = \cos(2\pi/18)$.)
(2) Man bestimme das Minimalpolynom von α über $\mathbb{Q}$. (Hinweis: Betrachte $\beta := 2\alpha$ statt α.)
(3) $\mathbb{Q}(z)$ ist abgeschlossen gegen Konjugation, d. h. ist $w \in \mathbb{Q}(z)$, so gilt auch für die konjugierte komplexe Zahl $\overline{w} \in \mathbb{Q}(z)$.
(4) Man bestimme $[\mathbb{Q}(z) : \mathbb{Q}]$.
(5) Man bestimme das Minimalpolynom von z über $\mathbb{Q}$. (Hinweis: Betrachte z^3 auf dem Einheitskreis.)
(6) Ist das reguläre 18-Eck konstruierbar?

Ü 5.4. Sei $L \supset K \supseteq \mathbb{Q}$ ein Körperturm mit $[L : K] = 2$. Dann gibt es $b \in L$ mit $L = K(b)$ und $b^2 \in K$. (Es ist also $L = K(\sqrt{a})$ mit $a = b^2 \in K$.)

KAPITEL VI

Galoistheorie

1. Die Galoisgruppe einer Körpererweiterung und Fixkörper

Definition 1.1 (*Galoisgruppe*)

Sei L/K eine Körpererweiterung. Die Menge aller K-Automorphismen $\sigma\colon L \to L$ ist ein Gruppe, wobei die Verknüpfung durch Komposition von Abbildungen gegeben ist. Diese Gruppe heisst die *Galoisgruppe* der Körpererweiterung L/K und wird mit $\mathrm{Gal}(L/K)$ bezeichnet.

Proposition 1.2

Sei L/K eine endliche Körpererweiterung. Dann hat die Galoisgruppe $\mathrm{Gal}(L/K)$ endliche Ordnung.

Beweis. Sei etwa $L = K(\alpha_1, \ldots, \alpha_n)$ mit über K algebraischen α_i, vgl. Satz V.3.4. Indem man nun das Produkt $f = f_1 \cdot \ldots \cdot f_n$ der Minimalpolynome der α_i und die Nullstellenmenge von f in L betrachtet, folgt die Behauptung leicht aus Lemma V.2.3, denn jeder K-Automorphismus von L ist durch sein Wirken auf $\alpha_1, \ldots, \alpha_n$ schon eindeutig bestimmt. (Die Vervollständigung der Details sei als einfache Übung empfohlen.) ∎

Satz 1.3 (*Isomorphismen-Erweiterungs-Lemma*)

Seien $K(x)/K$ und $K'(x')/K'$ einfache algebraische Körpererweiterungen und $i\colon K \to K'$ ein Isomorphismus. Sei $f \in K[T]$ das Minimalpolynom von x über K, und es gelte, dass $i^*(f)$ das Minimalpolynom von x' über K' ist. Dann ist die Anzahl der Erweiterungen $\sigma\colon K(x) \to K'(x')$ von i gleich der Anzahl der verschiedenen Nullstellen von f in $K(x)$. Es gibt genau eine solche Erweiterung σ mit $\sigma(x) = x'$.

Beweis. Seien $x = x_1, x_2, \ldots, x_s$ die verschiedenen Nullstellen von f in $L = K(x)$. Nach Satz V.2.5 gibt es einen Isomorphismus $\sigma\colon K(x) \to K'(x')$, der i fortsetzt und mit $\sigma(x) = x'$. Nach Lemma V.2.3 überführt σ die verschiedenen Nullstellen $x_1, \ldots, x_s$ von f in $K(x)$ in die verschiedenen Nullstellen $\sigma(x_1), \ldots, \sigma(x_s)$ von $i^*(f)$ in $K'(x')$. Ist nun $\tau\colon K(x) \to K'(x')$ ein beliebiger Isomorphismus, der i fortsetzt, so gibt es ein j mit $\tau(x) = \sigma(x_j)$. Da $1, x, \ldots, x^{n-1}$ eine K-Basis von $K(x)$ ist und τ eine Fortsetzung von $i\colon K \to K'$, ist τ durch das Bild $\tau(x)$ schon eindeutig festgelegt. Es gibt für τ also genau s Möglichkeiten. ∎

Spezialisiert man auf $K = K'$, $x = x'$ und $i = 1_K$, so erhält man:

Folgerung 1.4

Sei $K(x)/K$ eine einfach algebraische Körpererweiterung, und sei $f \in K[T]$ das Minimalpolynom von x über K. Dann ist die Ordnung von $\mathrm{Gal}(K(x)/K)$ gleich der Anzahl der verschiedenen Nullstellen von f in $K(x)$. Insbesondere gilt

$$|\mathrm{Gal}(K(x)/K)| \leq \mathrm{grad}(f) = [K(x) : K].$$

Es wird ein wichtiges Ziel sein, diese Aussage auf beliebige endliche Körpererweiterungen zu verallgemeinern.

Bemerkung. Die vorherige Aussage (und ihr Beweis) liefert ein Konstruktionsverfahren für $\mathrm{Gal}(K(x)/K)$; die Elemente von $\mathrm{Gal}(K(x)/K)$ korrespondieren mit den (verschiedenen) Nullstellen von f in $K(x)$; sind $x_1, \dots, x_s \in K(x)$ die verschiedenen Nullstellen von f in $K(x)$, so induziert die Festsetzung $\sigma_i(x) = x_i$ ein eindeutig bestimmtes Element von $\mathrm{Gal}(K(x)/K)$.

Beispiele. (1) Betrachte $\mathbb{C}/\mathbb{R}$. Es ist $\mathbb{C} = \mathbb{R}(i)$. Das Minimalpolynom $f = T^2 + 1$ von i über $\mathbb{R}$ hat die Nullstellen i und $-i$ (die beide in $\mathbb{R}(i)$ liegen). Es gibt also die Möglichkeiten $i \mapsto i$ und $i \mapsto -i$. Dies liefert die $\mathbb{R}$-Automorphismen $1_{\mathbb{C}}$ (die Identität) und τ definiert durch $\tau(a + bi) = a - bi$ (es ist also τ die komplexe Konjugation). $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \{1, \tau\} = \langle\tau\rangle$.

(2) Betrachte $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$. Hierbei bezeichnet $\sqrt[3]{2}$ die eindeutig bestimmte positive reelle dritte Wurzel aus 2. Die komplexen Nullstellen des Minimalpolynoms $T^3 - 2$ von $\alpha = \sqrt[3]{2}$ über $\mathbb{Q}$ sind $\alpha, e^{2\pi i/3}\alpha, e^{4\pi i/3}\alpha$. Wegen $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$ liegt davon nur α in $\mathbb{Q}(\sqrt[3]{2})$. Also besteht $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ nur aus dem neutralen Element.

(3) Betrachte $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$. Die komplexen Nullstellen des Minimalpolynoms $T^4 - 2$ von $\alpha = \sqrt[4]{2}$ über $\mathbb{Q}$ sind $\alpha, i\alpha, -\alpha, -i\alpha$. Davon sind nur α und $-\alpha$ in $\mathbb{Q}(\sqrt[4]{2})$. Also besteht $\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q})$ aus dem neutralen Element und dem $\mathbb{Q}$-Automorphismus σ der α auf $-\alpha$ schickt; dieser ist auf beliebigen Elementen von $\mathbb{Q}(\sqrt[4]{2})$ definiert durch

$$\sigma(a + b\alpha + c\alpha^2 + d\alpha^3) = a - b\alpha + c\alpha^2 - d\alpha^3.$$

(4) Betrachte $\mathbb{Q}(i, \sqrt[4]{2})/\mathbb{Q}(i)$. Es ist $f = T^4 - 2$ ein Polynom über $\mathbb{Q}(i)$, welches $\sqrt[4]{2}$ als Nullstelle hat. Wegen

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

folgt $[\mathbb{Q}(i, \sqrt[4]{2}) : \mathbb{Q}(i)] = 4$, und damit ist f auch das Minimalpolynom von $\sqrt[4]{2}$ über $\mathbb{Q}(i)$. Alle Nullstellen $\alpha, i\alpha, -\alpha, -i\alpha$ (mit $\alpha = \sqrt[4]{2}$) liegen in $\mathbb{Q}(i, \sqrt[4]{2})$. Sei σ der $\mathbb{Q}(i)$-Automorphismus von $\mathbb{Q}(i, \sqrt[4]{2})$, der durch $\sigma\colon \alpha \mapsto i\alpha$ bestimmt ist. Dann gilt $\sigma^2\colon \alpha \mapsto -\alpha$, $\sigma^3\colon \alpha \mapsto -i\alpha$ und $\sigma^4 = 1_L$. Es ist also $\mathrm{Gal}(\mathbb{Q}(i, \sqrt[4]{2})/\mathbb{Q}(i))$ zyklisch von der Ordnung 4, erzeugt von σ.

Definition 1.5 (*Fixkörper*)

Sei L ein Körper und G eine Gruppe von Automorphismen $\sigma\colon L \to L$. Dann ist $L^G = \{x \in L \mid \sigma(x) = x \text{ für alle } \sigma \in G\}$ ein Teilkörper von L, der *Fixkörper* von G.

Insbesondere: Ist L/K eine Körpererweiterung und $U \subseteq \mathrm{Gal}(L/K)$ eine Untergruppe der Galoisgruppe, so ist der Fixkörper L^U ein Zwischenkörper von L/K.

Bemerkung. Sei L/K eine Körpererweiterung mit Galoisgruppe $G = \mathrm{Gal}(L/K)$. Es gilt $L^G \supseteq K$ und $\mathrm{Gal}(L/L^G) = \mathrm{Gal}(L/K)$, wie man leicht nachrechnet.

Definition 1.6 (*Galoiserweiterung*)

Eine algebraische Körpererweiterung L/K heisst *galoissch*, oder *Galoiserweiterung*, falls $L^{\mathrm{Gal}(L/K)} = K$ gilt.

Beispiele. (1) $\mathbb{C}/\mathbb{R}$. Sei $G = \mathrm{Gal}(\mathbb{C}/\mathbb{R})$. Es ist $\mathbb{C}^G = \{z \in \mathbb{C} \mid z = \bar{z}\} = \mathbb{R}$. Also ist $\mathbb{C}/\mathbb{R}$ galoissch.

(2) Es ist $G = \{1\}$ die Galoisgruppe von $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$. Also gilt $\mathbb{Q}(\sqrt[3]{2})^G = \mathbb{Q}(\sqrt[3]{2}) \neq \mathbb{Q}$, d. h. diese Körpererweiterung ist nicht galoissch.

(3) Es ist $G = \{1, \sigma\}$ (wie oben beschrieben) die Galoisgruppe von $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$. Es ist dann

$$\mathbb{Q}(\sqrt[4]{2})^G = \{x \mid \sigma(x) = x\} = \{a + c\sqrt{2} \mid a, c \in \mathbb{Q}\} = \mathbb{Q}(\sqrt{2}),$$

also ist diese Körpererweiterung nicht galoissch.

(4) $\mathbb{Q}(i, \sqrt[4]{2})/\mathbb{Q}(i)$ ist galoissch. Wir haben eben schon gezeigt, dass die Galoisgruppe G zyklisch ist mit Erzeuger $\sigma\colon \alpha \mapsto i\alpha$. Es folgt weiter:

$$L^G = \{x \in \mathbb{Q}(i, \sqrt[4]{2}) \mid \sigma(x) = x\}.$$

Jedes Element $x \in \mathbb{Q}(i, \sqrt[4]{2})$ lässt sich schreiben als

$$x = x_0 + x_1\alpha + x_2\alpha^2 + x_3\alpha^3$$

mit eindeutige x_0, x_1, x_2, $x_3 \in \mathbb{Q}(i)$. Damit ist

$$\sigma(x) = x_0 + x_1 i\alpha - x_2\alpha^2 - x_3 i\alpha^3.$$

Es folgt damit $x \in L^G$ genau dann, wenn $x_1 = ix_1$, $x_2 = -x_2$ und $x_3 = -ix_3$, also, wenn $x = x_0 \in \mathbb{Q}(i)$ gilt. Also $L^G = \mathbb{Q}(i)$. Damit ist die Körpererweiterung $\mathbb{Q}(i, \sqrt[4]{2})/\mathbb{Q}(i)$ galoissch.

2. Zerfällungskörper

Definition 2.1 (*Zerfällungskörper*)

Sei K ein Körper und $f \in K[T]$ mit $f \neq 0$. Ein Erweiterungskörper L von K heißt ein *Zerfällungskörper* von f über K, falls

- f zerfällt über L in Linearfaktoren, d. h. $f = c \cdot (T - a_1) \cdot \ldots \cdot (T - a_n)$ mit $c \in K^\times$ und $a_1, \ldots, a_n \in L$; und
- es gilt $L = K(a_1, \ldots, a_n)$.

Die zweite Bedingung ist offenbar gleichwertig dazu, dass es in L keinen kleineren Körper gibt, über dem f zerfällt. Außerdem gilt ersichtlich $[L : K] < \infty$.

Beispiel. Sei $f = T^3 - 2 \in \mathbb{Q}[T]$. Die komplexen Nullstellen von f sind $\sqrt[3]{2}$, $\sqrt[3]{2}e^{2\pi i/3}$, $\sqrt[3]{2}e^{4\pi i/3}$. Ein Zerfällungskörper von f über $\mathbb{Q}$ ist gegeben durch

$$L = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}e^{2\pi i/3}, \sqrt[3]{2}e^{4\pi i/3}) = \mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3}).$$

Satz 2.2 (*Existenz von Zerfällungskörpern; Kronecker (1887)*)

Sei K ein Körper und $f \in K[T]$ mit $f \neq 0$. Dann gibt es einen Zerfällungskörper L von f über K.

Beweis. Wir beweisen die Aussage per Induktion nach $n = \operatorname{grad}(f)$ unter Verwendung des Satzes von Kronecker. Für $n = 1$ ist nichts zu zeigen. Sei $n > 1$. Es hat f einen irreduziblen Faktor $f_1 \in K[T]$. Nach Satz V.2.1 gibt es einen Erweiterungskörper $L_1 = K(a_1)$ von K mit $f_1(a_1) = 0$. In $L_1[T]$ gilt dann $f = (T - a_1)g$. Nach Induktionsvoraussetzung hat g einen Zerfällungskörper L/L_1. Dann ist offenbar L ein Zerfällungskörper von f über K. ∎

Satz 2.3 (*Isomorphismen-Erweiterungs-Theorem*)

Sei $i\colon K \to K'$ ein Körperisomorphismus, sei $0 \neq f \in K[T]$. Sei L ein Zerfällungskörper von f über K, sei L' ein Zerfällungskörper von $f' = i^*(f)$ über K'. Dann gibt es einen Isomorphismus von Erweiterungen $\sigma\colon L/K \to L'/K'$ mit $\sigma_{|K} = i$. Es gibt $\leq [L : K]$ solche Isomorphismen. Die Anzahl ist $= [L : K]$ genau dann, wenn jeder irreduzible Faktor von f über L in paarweise verschiedene Linearfaktoren zerfällt.

Beweis. Induktion nach $n = \operatorname{grad}(f)$. Das folgende Diagramm veranschaulicht die Vorgehensweise im Beweis.

(2.1)
$$\begin{array}{ccc} L & \overset{\sigma}{-\!\!-\!\!\to} & L' \\ | & & | \\ K(x) & \overset{j}{-\!\!\to} & K'(x') \\ | & & | \\ K & \xrightarrow{\quad i \quad} & K' \end{array}$$

Man geht von unten nach oben vor. Zunächst erweitert man i durch j auf einen Zwischenkörper $K(x)$, wobei x eine Nullstelle von f in L ist, indem man Satz 1.3 (Isomorphismen-Erweiterungs-Lemma) anwendet. Dann wird j per Induktionsvoraussetzung auf L erweitert. Die Details:

Existenz. Für $n = 0$ ist nichts zu zeigen. Sei $n \geq 1$. Es gibt einen irreduziblen Faktor f_1 von f in $K[T]$. Dann ist $f_1' = i^*(f_1)$ ein irreduzibler Faktor von f'. Sei x eine Nullstelle von f_1 in L und x' eine Nullstelle von $i^*(f_1)$ in L'. Nach Satz 1.3 gibt es einen Isomorphismus $j\colon K(x) \to K'(x')$, der i erweitert und x auf x' abbildet. Schreibe $f = (T-x)g$ und $f' = (T-x')g'$ mit $f \in K(x)[T]$ und $f' \in K'(x')[T]$. Dann gilt $f' = i^*(f) = j^*(f) = j^*(T-x)j^*(g) = (T-x')j^*(g)$, also $g' = j^*(g)$. Offenbar ist L Zerfällungskörper von g über $K(x)$ und L' Zerfällungskörper von g' über $K'(x')$. Man wendet nun die Induktionsvoraussetzung auf g an.

Anzahl. Auch dies beweist man per Induktion, mit Lemma V.2.3 und Satz 1.3, indem man $L/K(x)$ und $K(x)/K$ betrachtet. Der obige irreduzible Faktor f_1' hat in L' höchstens $\operatorname{grad}(f_1') = \operatorname{grad}(f_1) = [K(x) : K]$ verschiedene Nullstellen $x' = x_1', \ldots, x_m'$, wobei $m = [K(x) : K]$ genau dann, wenn f_1 über L in paarweise verschiedene Linearfaktoren zerfällt. Es definiert jedes $j_\ell\colon K(x) \to K'(x_\ell') \subseteq L'$ durch $x \mapsto x_\ell'$ eine Erweiterung von i. Für $L/K(x)$ wendet man dann die Induktionsannahme auf jedes j_ℓ an, denn die irreduziblen Faktoren von $g = f/(T-x) \in K(x)[T]$ zerfallen über L in paarweise verschiedene Linearfaktoren, wenn dies für f gilt; gilt dies für f nicht, dann macht man den Induktionsanfang mit einem irreduziblen Faktor $f_1 \in K[T]$ von f, bei dem Linearfaktoren mehrfach vorkommen, erhält nur $m < [K(x) : K]$ Erweiterungen von i auf $K(x)$ nach $K(x_\ell')$, und nach Induktionsannahme kann jede dieser m Erweiterungen höchstens $[L : K(x)]$-mal auf L nach L' erweitert werden, d. h. es gibt höchstens $m \cdot [L : K(x)] < [L : K]$ Erweiterungen von i auf L. ∎

Spezialisiert[1] man auf $K = K'$ und $i = 1_K$, so erhält man:

Folgerung 2.4 (*Eindeutigkeit des Zerfällungskörpers*)

Seien L und L' Zerfällungskörper des Polynoms $f \neq 0$ über K. Dann gibt es einen K-Isomorphismus $\sigma\colon L \to L'$. ∎

Beispiel. Wir veranschaulichen obigen Induktionsbeweis an einem Beispiel (mit $i = 1_K$). Zum konkreten Berechnen aller Erweiterungen ist er nicht unbedingt so praktisch, wie er zunächst aussieht. Seien $K = \mathbb{Q}$, $f = T^3 - 2 \in K[T]$ und L der Zerfällungskörper von f wie im vorigen Beispiel. Seien $\alpha = \sqrt[3]{2}$, $\omega = e^{2\pi i/3}$. Die Nullstellen von f sind $\alpha_1 = \alpha$, $\alpha_2 = \omega\alpha$, $\alpha_3 = \omega^2\alpha$. Es ist f das Minimalpolynom von α über K. Es gibt also drei K-Isomorphismen $j_\ell\colon K(\alpha) \to K(\alpha_\ell)$ (mit $\ell = 1, 2, 3$). (Man beachte dagegen, dass $\operatorname{Gal}(K(\alpha)/K) = \{1\}$.) Alle $K(\alpha_\ell)$ sind Zwischenkörper von L/K. Diese K-Isomorphismen sind jetzt auf eine einfache Erweiterung von $K(\alpha)$ zu erweitern. Gemäß dem Induktionsbeweis betrachtet man $K(\alpha)(\alpha_2)$ (was hier schon $= L$ ist) und $g = f/(T-\alpha) = (T-\alpha_2)(T-\alpha_3) = T^2 + \alpha T + \alpha^2$. Dies ist auch das Minimalpolynom

[1] Man beachte aber, dass für obigen Induktionsbeweis die allgemeinere Situation notwendig war.

von α_2 über $K(\alpha)$. Es sind dann (jeweils) die Polynome $j_\ell^*(g)$ zu betrachten. Offenbar $j_1^*(g) = g$, und eine kleine Rechnung ergibt ($1 + \omega + \omega^2 = 0$ verwendend)

$$j_2^*(g) = T^2 + \alpha_2 T + \alpha_2^2 = (T - \alpha)(T - \alpha_3), \quad j_3^*(g) = T^2 + \alpha_3 T + \alpha_3^2 = (T - \alpha)(T - \alpha_2),$$

und damit $j_2^*(g) = \mathrm{MIPO}(\alpha/K(\alpha_2))$, $j_3^*(g) = \mathrm{MIPO}(\alpha/K(\alpha_3))$. Gemäß der Formel (2.1) im Beweis von Satz V.2.5 kann jedes j_ℓ auf genau zwei Weisen zu einem Automorphismus von L erweitert werden, nämlich indem für ein Element $x = a_0 + a_1\alpha_2$ mit $a_0, a_1 \in K(\alpha)$ das primitive Element α_2 jeweils auf eine der beiden Nullstellen von $j_\ell^*(g)$ geschickt und auf die "Koeffizienten" a_k der Isomorphismus j_ℓ angewendet wird. Dies ergibt dann 6 verschiedene K-Automorphismen von L/K, und wegen $[L : K] = 6$ damit die Elemente der Galoisgruppe von L/K. Statt diese 6 Elemente konkret aufzulisten (was nach obiger Herleitung nun zwar einfach ist, aber etwas lästig hinzuschreiben), beschreiben wir stattdessen eine Variante (in diesem konkreten Fall), die j_ℓ zu erweitern, und die die Auflistung der 6 Elemente der Galoisgruppe übersichtlicher gestaltet.

Statt α_2 nehmen wir ω als primitives Element, denn es ist auch $L = K(\alpha)(\omega)$. Das Minimalpolynom von ω über $K(\alpha)$ ist $h = (T^3 - 1)/(T - 1) = T^2 + T + 1$, wie man leicht nachrechnet. (Verwende $\omega \notin \mathbb{R} \supseteq K(\alpha)$.) Wegen $j_\ell(1) = 1$ gilt $j_\ell^*(h) = h$ für *alle* ℓ. (Dies vereinfacht die Sache!) Die beiden Nullstellen davon sind ω und ω^2. Jedes $x \in L$ hat eine eindeutige Darstellung $x = a_0 + a_1\omega$ mit $a_0, a_1 \in K(\alpha)$. Jedes j_ℓ lässt sich dann auf genau zwei Weisen zu einem Automorphismus $\sigma_{\ell,t} \colon L \to L$, $t = 1, 2$, gemäß der Formel (2.1) im Beweis von V.2.5 erweitern:

$$\sigma_{\ell,t}(x) := j_\ell(a_0) + j_\ell(a_1)\omega^t.$$

Wir erhalten somit

$$\mathrm{Gal}(L/K) = \{\sigma_{\ell,t} \mid \ell = 1, 2, 3;\ t = 1, 2\}.$$

Aufgaben

Ü 2.1. Untersuchung wie im vorstehenden Beispiel, aber für den Zerfällungskörper von $f = T^4 - 2 \in \mathbb{Q}[T]$.

Ü 2.2. Sei L der Zerfällungskörper eines Polynoms $f \in K[T]$ vom Grad n. Dann gilt $[L : K] \leq n!$.

Ü 2.3. Sei L Zerfällungskörper eines Polynoms $f \in K[T]$ vom Grad $n \geq 1$. Wenn $[L : K] = n!$ gilt, dann ist f irreduzibel.

Ü 2.4. Sei $f \in K[T]$ mit Primfaktorzerlegung $f = a \cdot p_1^{m_1} \cdot \ldots \cdot p_t^{m_t}$, mit $a \in K^\times$ und paarweise verschiedenen normierten und irreduziblen Polynomen p_i. Der Zerfällungskörper von f ist identisch mit dem des Polynoms $p_1 \cdot \ldots \cdot p_t$.

Ü 2.5. Seien L und L' Zerfällungskörper eines Polynoms $0 \neq f \in K[T]$. Liegen L und L' in einem gemeinsamen Oberkörper Ω, so gilt $L = L'$.

3. Charakteristik und Primkörper eines Körpers

Definition 3.1

(Erinnerung: Ü II.7.2.) Sei K ein Körper. Gibt es keine ganze Zahl $n \geq 1$ mit $n \cdot 1_K = 0$, so ist die *Charakteristik* von K gleich 0, also $\mathrm{Char}(K) = 0$. Gibt es eine solche Zahl n, so ist die kleinste solche Zahl eine Primzahl p, und diese ist dann die *Charakteristik* von K.

Der *Primkörper* $\Pi(K)$ von K ist der kleinste in K enthaltene Teilkörper, d. h. der Durchschnitt aller Teilkörper von K.

Proposition 3.2

Sei K ein Körper.

(1) *Im Fall* $\mathrm{Char}(K) = 0$ *ist* $\Pi(K) = \{\frac{m \cdot 1_K}{n \cdot 1_K} \mid m, n \in \mathbb{Z},\ n > 0\} \simeq \mathbb{Q}$.

(2) *Im Fall* $\mathrm{Char}(K) = p > 0$ *ist* $\Pi(K)$ *zum Restklassenkörper* $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ *isomorph.*

Beweis. Die Abbildung $\mu\colon \mathbb{Z} \to K$, $n \mapsto n \cdot 1_K$ ist ein Ringhomomorphismus, der genau dann injektiv ist, wenn $\mathrm{Char}(K) = 0$ gilt. In dem Fall ist das Bild $\{n \cdot 1_K \mid n \in \mathbb{Z}\}$ ein zu $\mathbb{Z}$ isomorpher Teilring von K, und es folgt, dass $\Pi(K) \simeq \mathbb{Q}$ ist. Wenn dagegen $\mathrm{Char}(K) = p > 0$ gilt, so ist $\mathrm{Kern}(\mu) = p\mathbb{Z}$. Der Homomorphiesatz liefert: Es ist $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} \xrightarrow{\sim} \mathrm{Bild}(\mu) \subseteq \Pi(K) \subseteq K$. Da $\mathbb{F}_p$ ein Körper ist, gilt dies auch für $\mathrm{Bild}(\mu)$, und es folgt $\Pi(K) = \mathrm{Bild}(\mu)$. ∎

Aufgaben

Ü 3.1. Sei K ein Körper mit $\mathrm{Char}(K) = p > 0$. Dann ist die Abbildung $\sigma_p\colon K \to K$, $x \mapsto x^p$ ein Ringmorphismus. (Dieser heisst der Frobenius-Endomorphismus.)

Ü 3.2. Sei K ein Körper mit $\mathrm{Char}(K) = p > 0$. Für jedes $a \in K$ gilt $T^p - a^p = (T - a)^p$.

4. Vielfachheit von Nullstellen

Definition 4.1

Sei L/K eine Körpererweiterung und $0 \neq f \in K[T]$. Sei $a \in L$ eine Nullstelle von f. Die *Vielfachheit* e von a in L ist die natürliche Zahl $e \geq 1$ mit $f = (T - a)^e \cdot g$, wobei $g \in L[T]$ gilt mit $g(a) \neq 0$. Die Nullstelle a heisst einfach, falls $e = 1$ gilt, sonst mehrfach (doppelt, dreifach, etc.). — Dies gilt auch für $e = 0$: Ist a keine Nullstelle, so sei die Vielfachheit 0.

Definition 4.2

Sei K ein Körper. Definiere die (formale) *Derivation* $D\colon K[T] \to K[T]$ durch

$$f = \sum_{i=0}^{n} a_i T^i \ \mapsto\ \sum_{i=1}^{n} i a_i T^{i-1} =: D(f).$$

Es heisst $D(f)$ die (formale) Derivierte von f.

Folgende Eigenschaften sind leicht nachzurechnen:

- D ist K-linear.
- (Produktregel) $D(fg) = fD(g) + D(f)g$ für alle f, $g \in K[T]$.

Satz 4.3 (*Derivationskriterium für Einfachheit von Nullstellen*)

Sei K ein Körper und $0 \neq f \in K[T]$ ein Polynom.

(1) *Sei a eine Nullstelle von f. Es ist a eine einfache Nullstelle genau dann, wenn $D(f)(a) \neq 0$ gilt.*

(2) *f hat in beliebigen Erweiterungskörpern von K nur einfache Nullstellen genau dann, wenn $\mathrm{ggT}(f, D(f)) = 1$ gilt.*

(3) *Sei f zusätzlich irreduzibel. Genau dann hat f in jedem Erweiterungskörper von K nur einfache Nullstellen, wenn $D(f) \neq 0$ gilt.*

Beweis. Für (1) wendet man die Produktregel an auf $f = (T-a)^e \cdot g$, wobei $e \geq 1$ und $g(a) \neq 0$ gilt. Ist $e = 1$, so folgt $D(f) = g + (T-a)D(g)$, also $D(f)(a) = g(a) \neq 0$. Ist $e \geq 2$, so folgt $D(f)(a) = 0$ aus $D(f) = e(T-a)^{e-1}g + (T-a)^e D(g)$.

(2) Zunächst eine Vorüberlegung: Sei L/K eine Körpererweiterung. Dann gilt die Aussage $\mathrm{ggT}(f, D(f)) = 1$ in $L[T]$ genau dann, wenn sie in $K[T]$ gilt. Denn gilt dies in $K[T]$, so gibt es g, $h \in K[T]$ mit $1 = gf + hD(f)$. Dies ist auch

eine Gleichung in $L[T]$, woraus sofort die Teilerfremdheit von f und $D(f)$ auch in $L[T]$ folgt. Haben umgekehrt f und $D(f)$ in $L[T]$ keine gemeinsamen Teiler, dann trivialweise auch in $K[T]$ nicht.

Es genügt die Aussage in (2) zu zeigen für den Fall, dass L Zerfällungskörper von f über K ist. Sind f und $D(f)$ teilerfremd in $L[T]$, so können sie auch keine gemeinsame Nullstelle in L haben, und aus (1) folgt, dass alle Nullstellen von f in L einfach sein müssen. Haben dagegen f und $D(f)$ einen gemeinsamen Teiler $g \in L[T]$ vom Grad ≥ 1, so zerfällt g (wie f) in $L[T]$ komplett in Linearfaktoren, und es folgt, dass f und $D(f)$ eine gemeinsame Nullstelle in L haben. Aus (1) folgt dann die Mehrfachheit dieser Nullstelle von f.

(3) Gilt $D(f) \neq 0$, muss wegen $\operatorname{grad}(D(f)) \leq \operatorname{grad}(f) - 1$ der ggT von f und $D(f)$ eine Einheit sein. Nach (2) hat f in jedem Erweiterungskörper von K nur einfache Nullstellen. Ist dies umgekehrt der Fall, so ist ebenfalls nach (2) der ggT von f und $D(f)$ eine Einheit, also muss $D(f) \neq 0$ gelten. ∎

Bemerkung. Man beachte, dass man mit dem nützlichen Kriterium (2) bzw. (3) sehr effizient Einfachheit aller Nullstellen von f prüfen kann, ohne diese Nullstellen bzw. den Zerfällungskörper von f überhaupt zu kennen.

Bemerkung. Sei $f \in K[T]$. Gelte $\operatorname{Char}(K) = p > 0$. Genau dann gilt $D(f) = 0$, wenn $f = g(T^p)$ für ein $g \in K[T]$ gilt. Dagegen ist im Fall $\operatorname{Char}(K) = 0$ immer $D(f) \neq 0$, sofern f nicht konstant ist.

Aufgaben

Ü 4.1. Sei $f = (T-a)^m \cdot g$. Dann ist $D^m(f)(a) = m!g(a)$. (Wobei $D^m = D \circ \ldots \circ D$ die m-fache Komposition von D ist, also die m-te Derivation.)

Ü 4.2. Es gelte $\operatorname{Char}(K) = 0$. Sei $0 \neq f \in K[T]$ und L ein Zerfällungskörper von f. Die Vielfachheit einer Nullstelle $a \in L$ von f ist dann die kleinste natürliche Zahl e mit $D^e(f)(a) \neq 0$.

5. Separabilität

Definition 5.1

Ein irreduzibles Polynom $f \in K[T]$ heißt *separabel*, falls es in einem Zerfällungskörper nur einfache Nullstellen hat. Ein beliebiges Polynom $0 \neq f \in K[T]$ heißt *separabel*, wenn jeder seiner irreduziblen Faktoren separabel ist.

Bemerkung. Nach Satz 4.3 (3) ist ein irreduzibles Polynom $f \in K[T]$ separabel genau dann, wenn $D(f) \neq 0$ gilt.

Satz 5.2 (*Charakterisierung der Separabilität von Polynomen*)

Sei $f \in K[T]$ ein nicht-konstantes Polynom und L ein Zerfällungskörper von f über K. Dann sind äquivalent:

(1) *f ist ein separables Polynom.*

(2) *Für jeden Isomorphismus $i\colon K \to K'$ und jeden Zerfällungskörper L' von $f' = i^*(f)$ über K' ist die Anzahl der Erweiterungen $\sigma\colon L \to L'$ von i gleich dem Körpergrad $[L:K]$.*

(3) *Die Anzahl der K-Automorphismen $\sigma\colon L \to L$ ist gleich dem Körpergrad $[L:K]$. Mit anderen Worten: $|\operatorname{Gal}(L/K)| = [L:K]$.*

Beweis. (1)⇔(2) Folgt aus dem Isomorphismen-Erweiterungs-Theorem. — Man sieht auch, dass es in (2)⇒(1) reicht anzunehmen, dass $K' = K$, $i = 1_K$ und $L' = L$ gilt, was sofort auch die Äquivalenz zu (3) zeigt. ∎

Definition 5.3

Sei L/K eine Körpererweiterung, sei $x \in L$ algebraisch über K. Dann heißt x *separabel* über K, falls das Minimalpolynom von x über K separabel ist.

Eine algebraische Körpererweiterung L/K heißt *separabel*, falls jedes $x \in L$ separabel über K ist.

Satz 5.4

Jede endliche Erweiterung L/K von einem Körper K der Charakteristik 0 ist separabel.

Beweis. Sei $x \in L$ und $f = T^n + \sum_{i=0}^{n-1} a_i T^i$ das Minimalpolynom von x über K. Dann ist $D(f) = n \cdot T^{n-1} + \ldots \neq 0$. Also ist x separabel über K. ∎

Proposition 5.5

Sei $K \subseteq F \subseteq L$ ein Körperturm. Ist L/K separabel, so sind auch L/F und F/K separabel.

Beweis. Sei L/K separabel. Sei $x \in L$. Das Minimalpolynom g von x über F ist (in $F[T]$) ein Teiler des Minimalpolynoms f von x über K. Mit f hat dann aber erst recht g nur einfache Nullstellen. Trivialerweise ist F/K separabel. ∎

Bemerkung. Es gilt auch die Umkehrung, d. h. die Transitivität separabler Erweiterungen. Der Beweis ist nicht ganz einfach, selbst im endlichen Fall. Vgl. Übung 8.5. Wir werden die Aussage aber nicht verwenden.

Aufgaben

Ü 5.1. Sei K ein Körper mit $\mathrm{Char}(K) = p > 0$. Sei L/K eine endliche Körpererweiterung, deren Grad $n = [L : K]$ nicht von p geteilt wird. Dann ist L/K separabel.

Ü 5.2. Sei K ein Körper mit $\mathrm{Char}(K) = p > 0$. Sei $f \in K[T]$ irreduzibel. Dann gibt es ein $n \geq 0$ und ein separables $g \in K[T]$ mit $f = g(T^{p^n})$. Ist a in einem Erweiterungskörper L eine Nullstelle von f, so hat a die Vielfachheit p^n, und a^{p^n} ist separabel über K.

Ü 5.3. Sei $f \in K[T]$ irreduzibel. Es ist f separabel genau dann, wenn es eine Körpererweiterung L/K und eine einfache Nullstelle x von f in L gibt.

6. Normalität

Definition 6.1

Eine algebraische Körpererweiterung L/K heißt *normal*, falls für jedes (normierte) irreduzible Polynom $f \in K[T]$ gilt: Hat f eine Nullstelle $\alpha \in L$, so zerfällt f über L vollständig in Linearfaktoren.

Satz 6.2

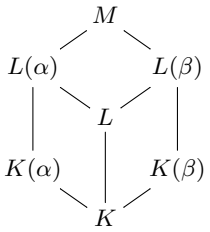
Sei L/K eine endliche Körpererweiterung. Die folgenden Aussagen sind äquivalent:

(1) *L/K ist normal.*
(2) *L/K ist Zerfällungskörper eines Polynoms in $K[T]$.*

Beweis. (1)⇒(2) Sei L/K normal. Schreibe $L = K(\alpha_1, \ldots, \alpha_n)$. Für jedes $i = 1, \ldots, n$ sei f_i das Minimalpolynom von α_i über K. Sei $f = f_1 \ldots f_n$. Jedes f_i ist irreduzibel und zerfällt über L in Linearfaktoren, da L/K normal. Da L von den Nullstellen von f über K erzeugt wird, ist L ein Zerfällungskörper von f über K.

(2)⇒(1) Es sei L Zerfällungskörper eines Polynoms $f \in K[T]$. Sei $g \in K[T]$ irreduzibel, ohne Einschränkung normiert. Es habe g eine Nullstelle $\alpha \in L$. Sei

$M \supseteq L$ ein Zerfällungskörper von fg über K. Sei β eine weitere Nullstelle von g in M.



Sei $\gamma = \alpha$ oder $\gamma = \beta$. Dann gilt

$$[L(\gamma) : L] \cdot [L : K] = [L(\gamma) : K] = [L(\gamma) : K(\gamma)] \cdot [K(\gamma) : K].$$

Nun sind $K(\alpha)$ und $K(\beta)$ nach Satz V.2.4 K-isomorph, mit $\alpha \mapsto \beta$. Außerdem ist $L(\gamma)$ offenbar ein Zerfällungskörper von f über $K(\gamma)$. Daher gibt es nach Satz 2.3 einen Isomorphismus von $L(\alpha)$ nach $L(\beta)$, der obigen K-Isomorphismus fortsetzt. Man bekommt $[L(\alpha) : K(\alpha)] = [L(\beta) : K(\beta)]$, was zusammen $[L(\alpha) : K] = [L(\beta) : K]$ und schließlich durch Kürzen $[L(\alpha) : L] = [L(\beta) : L]$ ergibt. Da $\alpha \in L$, folgt $1 = [L(\alpha) : L] = [L(\beta) : L]$, was aber $\beta \in L$ bedeutet. Also liegen alle Nullstellen von g in L. ■

Folgerung 6.3

Sei L/K eine endliche Körpererweiterung. Ist L/K normal und separabel, so ist L Zerfällungskörper eines separablen Polynoms über K.

Beweis. Ergibt sich sofort aus dem vorherigen Satz und aus der Definition eines separablen Polynoms. ■

Wir zeigen später auch die Umkehrung; vgl. Satz 8.1.

Normaler Abschluss. Sei L/K eine endliche Körpererweiterung. Eine Körpererweiterung N/L heisst *normaler Abschluss* von L/K, falls

(i) N/K eine endliche, normale Körpererweiterung ist, und
(ii) für jeden Zwischenkörper M von N/L gilt: ist M/K normal, so gilt $M = N$.

Proposition 6.4

Jede endliche Körpererweiterung L/K besitzt einen normalen Abschluss.

Beweis. Sei etwa $L = K(\alpha_1, \ldots, \alpha_n)$ mit algebraischen Elementen α_i und $f_i = \mathrm{MIPO}(\alpha_i/K)$. Setze $f = f_1 \cdot \ldots \cdot f_n$. Sei N Zerfällungskörper von f über K, wobei wir ohne Einschränkung $N \supseteq L$ annehmen können. Dann ist N/K endlich und normal. Über einem echt kleineren Zwischenkörper M von L/K zerfällt mindestens eines der irreduziblen Polynome f_i noch nicht, also ist M/K nicht normal. ■

Satz 6.5 (*Einschränkungssatz*)

Sei L/K eine endliche Körpererweiterung. Äquivalent sind:

(1) *L/K ist normal.*
(2) *Für jede Körpererweiterung F/L und für jeden K-Automorphismus $\sigma\colon F \to F$ gilt $\sigma(L) \subseteq L$.*
(3) *Es gibt eine endliche normale Körpererweiterung F/K, die L enthält, so dass für jeden K-Automorphismus $\sigma\colon F \to F$ gilt $\sigma(L) \subseteq L$.*

Beweis. (1)⇒(2) Sei L/K normal, F/L eine Körpererweiterung und $\sigma \in \mathrm{Gal}(F/K)$. Sei $\alpha \in L$. Das Minimalpolynom f von α über K zerfällt über L in Linearfaktoren. Da $\beta = \sigma(\alpha)$ auch eine Nullstelle von f ist, folgt $\sigma(\alpha) \in L$.

(2)⇒(3) Sei F/K ein normaler Abschluss von L/K. Dann ist F/K eine endliche normale Körpererweiterung, mit der sich (3) aus (2) ergibt.

(3)⇒(1) Es ist F Zerfällungskörper eines Polynoms $f \in K[T]$. Sei $g \in K[T]$ irreduzibel, und es habe g eine Nullstelle α in L. Da F/K normal ist, zerfällt g über F in Linearfaktoren. Sei $\beta \in F$ eine weitere Nullstelle von g. Nach Satz V.2.4 gibt es einen K-Isomorphismus $i\colon K(\alpha) \to K(\beta)$ mit $i(\alpha) = \beta$. Da offenbar F auch Zerfällungskörper von f über $K(\alpha)$ und über $K(\beta)$ ist, gibt es nach Satz 2.3 einen (K-) Automorphismus $\sigma\colon F \to F$, der i fortsetzt. Nach Voraussetzung gilt dann $\sigma(L) \subseteq L$. Es folgt $\beta = i(\alpha) = \sigma(\alpha) \in L$, d. h. alle Nullstellen von g liegen schon in L. ∎

Bemerkung. Aus (2) bzw. (3) im Einschränkungssatz folgt trivialerweise jeweils sogar $\sigma(L) = L$. — Sei L/K eine Körpererweiterung. Zwischenkörper M und M' heißen *konjugiert* (in L), falls es $\sigma \in \mathrm{Gal}(L/K)$ gibt mit $\sigma(M) = M'$. Sei M/K eine endliche Erweiterung. Es ist also M/K normal genau dann, wenn M in jeder Körpererweiterung mit all seinen Konjugierten übereinstimmt, und genau dann, wenn es in einer endlichen normalen Erweiterung von K mit all seinen Konjugierten übereinstimmt. — Daher ist der Begriff einer *normalen* (Zwischen-) Körpererweiterung in Analogie zur *Normal*teilereigenschaft einer Untergruppe.

Ist M/K eine (endliche) Körpererweiterung und sind $L_1, \ldots, L_t$ Zwischenkörper, so dass kein echter Teilkörper von M die Vereinigung aller L_i enthält, so heisst M das *Kompositum* der L_i. Man schreibt auch $M = L_1 L_2 \ldots L_t$.

Proposition 6.6

Sei L/K eine endliche Körpererweiterung und N ein normaler Abschluss. Dann ist N das Kompositum aller Konjugierten von L in N.

Beweis. Wir übernehmen die Bezeichnungen aus dem Beweis von Proposition 6.4. Sei β_i irgendeine Nullstelle von f_i in N. Dann gibt es $\sigma \in \mathrm{Gal}(N/K)$ mit $\beta_i = \sigma(\alpha_i) \in \sigma(L)$. ∎

Aufgaben

Ü 6.1. In Definition 6.1 kann man auf die Irreduzibilität nicht verzichten: man gebe ein Beispiel einer endlichen, normalen Erweiterung L/K an und ein (nicht-irreduzibles) Polynom $f \in K[T]$, welches eine Nullstelle in L hat, aber über L nicht in Linearfaktoren zerfällt.

Ü 6.2. Jede Körpererweiterung L/K mit $[L : K] = 2$ ist normal.

Ü 6.3. Sei L/K eine algebraische Körpererweiterung. Äquivalent sind:
(1) L/K ist normal.
(2) Jedes $x \in L$ ist Nullstelle eines irreduziblen Polynoms $f \in K[T]$, welches über L in Linearfaktoren zerfällt.

Ü 6.4. Sei L/K eine endliche Körpererweiterung und N ein normaler Abschluss davon. Sei N'/K eine normale Erweiterung, die L enthält.
(1) Es gibt einen L-Monomorphismus $N \to N'$.
(2) Liegen N und N' in einem gemeinsamen Körper Ω, so gilt $N \subseteq N'$.

Ü 6.5. Zwei normale Abschlüsse N und N' einer endlichen Erweiterung L/K sind L-isomorph.

Ü 6.6. Sei $L \supseteq M \supseteq K$ ein Körperturm, so dass L/K und M/K endlich und normal sind. Dann induziert Einschränkung $\sigma \mapsto \sigma_{|M}$ einen surjektiven Morphismus $\mathrm{Gal}(L/K) \to \mathrm{Gal}(M/K)$.

Ü 6.7. Sei L/K eine endliche normale Körpererweiterung, und sei M ein Zwischenkörper. Jeder K-Monomorphismus $\tau\colon M \to L$ lässt sich fortsetzen zu einem K-Automorphismus $\sigma\colon L \to L$ (d. h. mit $\sigma_{|M} = \tau$).

Ü 6.8. Sei L/K eine endliche normale Erweiterung. Sei $f \in K[T]$ irreduzibel, und seien $\alpha, \beta \in L$ Nullstellen von f. Dann gibt es einen K-Automorphismus von L mit $\sigma(\alpha) = \beta$.

Ü 6.9. [Anzahl der Fortsetzungen] Sei L/K eine endliche Körpererweiterung, und sei N ein normaler Abschluss von L/K (oder allgemeiner, irgendeine endliche normale Erweiterung von K, die L enthält). Es gibt mindestens einen und höchstens $[L : K]$ verschiedene K-Monomorphismen $\sigma\colon L \to N$. Es gibt exakt $[L : K]$ solche K-Monomorphismen genau dann, wenn L/K separabel ist.

(Hinweis: Per Induktion nach $n = [L : K]$: ist L/K separabel, so ist die Anzahl $= [L : K]$, ist L/K nicht separabel, so ist die Anzahl $< [L : K]$.)

Ü 6.10. Sei L/K eine endliche Körpererweiterung und M ein Zwischenkörper. Dann gibt es höchstens $[M : K]$ viele K-Monomorphismen $\sigma\colon M \to L$. Ist M/K nicht separabel, so ist die Anzahl echt kleiner als $[M : K]$.

7. Der Satz von Artin

Satz 7.1 (*Emil Artin*)

Sei L ein Körper und G eine endliche Gruppe von Automorphismen von L, der Ordnung n. Sei $K = L^G$ der Fixkörper. Dann ist L/K eine normale und separable Körpererweiterung vom Grad $[L : K] = n$ und mit Galoisgruppe $\mathrm{Gal}(L/K) = G$.

Beweis. Sei $\alpha \in L$. Sei $\sigma_1, \dots, \sigma_r \in G$ ein maximales System, so dass $\sigma_1(\alpha), \dots, \sigma_r(\alpha)$ verschieden sind. Sei

$$f = \prod_{i=1}^{r} \big(T - \sigma_i(\alpha)\big) \in L[T].$$

Sei $\sigma \in G$. Dann permutiert σ die Elemente $\sigma_1(\alpha), \dots, \sigma_r(\alpha)$, und daher gilt $\sigma^*(f) = f$. Die Koeffizienten von f bleiben also fix unter allen $\sigma \in G$, und daher liegen die Koeffizienten in $K = L^G$, d. h. $f \in K[T]$. Ferner gilt $f(\alpha) = 0$. Da f nur einfache Nullstellen hat, folgt, dass α separabel über K ist.

Ist $\alpha \in L$ Nullstelle eines irreduziblen Polynoms $g \in K[T]$, so ist dieses (bis auf Normierung) das Minimalpolynom von α über K und daher ein Teiler von obigem Polynom f, und zerfällt daher in $L[T]$ (wie f) komplett in Linearfaktoren. Daher ist L/K auch normal.

Es ist L/K auch endlich; genauer gilt: $[L : K] \le |G| = n$. Denn: Angenommen, $[L : K] \le n$ gilt nicht. Dann gibt es (mindestens) $n + 1$ Elemente $y_1, \dots, y_n, y_{n+1} \in L$, die linear unabhängig über K sind. Seien $\sigma_1 = 1_L$, $\sigma_2, \dots, \sigma_n$ die Elemente von G. Diese sind K-Automorphismen (also K-linear). Wir betrachten die Matrix

$$A = \big(\sigma_i(y_j)\big) \in \mathrm{M}_{n\times n+1}(L).$$

Da A höchstens den Rang n haben kann, sind die Spalten von A linear abhängig über L. Es gibt also $c_1, \dots, c_{n+1} \in L$, nicht alle $= 0$, so dass $\sum_{j=1}^{n+1} c_j\sigma_i(y_j) = 0$ für $i = 1, \dots, n$. In so einer Darstellung können nicht alle c_j in K liegen, denn sonst würde aus $\sigma_1 = 1_L$ eine lineare Abhängigkeit von $y_1, \dots, y_{n+1}$ über K folgen. Sei $\ell \ge 1$ minimal, so dass die ersten ℓ Spalten von A (nach evtl. Umnummerierung) linear abhängig über L sind. Es gibt also $c_1, \dots, c_\ell \in L$, nicht alle $= 0$, mit

$$\sum_{j=1}^{\ell} c_j\sigma_i(y_j) = 0 \qquad i = 1, \dots, n. \tag{7.1}$$

Wegen der Minimalität von ℓ müssen dann sogar alle $c_j \ne 0$ sein ($j = 1, \dots, \ell$), und außerdem gilt $\ell \ge 2$. Wir können (nach Division durch c_1) ohne Einschränkung $c_1 = 1$ annehmen. Sei $\sigma \in G$. Wenden wir σ auf (7.1) an, so werden dabei

die σ_i permutiert, und wir erhalten

$$\sum_{j=1}^{\ell} \sigma(c_j)\sigma_i(y_j) = 0 \qquad i = 1, \dots, n.$$

Bilden wir die Differenz der beiden Gleichungen, so bekommen wir (wegen $c_1 = 1$)

$$\sum_{j=2}^{\ell} \big(c_j - \sigma(c_j)\big)\sigma_i(y_j) = 0 \qquad i = 1, \dots, n.$$

Wegen der Minimalität von ℓ folgt dann aber $c_j - \sigma(c_j) = 0$ für $j = 2, \dots, \ell$. Wegen $c_1 = 1_L$ gilt dies auch für $j = 1$. Es folgt $c_1, \dots, c_\ell \in L^G = K$. Das ist aber ein Widerspruch, wie oben schon gezeigt wurde.

Wir haben also bis jetzt: L/K ist eine endliche, normale und separable Erweiterung mit $[L : K] \leq |G|$. Nach Folgerung 6.3 ist L Zerfällungskörper eines separablen $f \in K[T]$. Aus Satz 5.2 ergibt sich $[L : K] = |\operatorname{Gal}(L/K)|$. Trivial gilt $G \subseteq \operatorname{Gal}(L/K)$. Wir erhalten also insgesamt $[L : K] = |G| = |\operatorname{Gal}(L/K)|$ und $G = \operatorname{Gal}(L/K)$. Damit ist der Satz von Artin bewiesen. ∎

Folgerung 7.2

Sei L/K eine endliche Körpererweiterung. Dann gilt $|\operatorname{Gal}(L/K)| \leq [L : K]$. Genauer ist $|\operatorname{Gal}(L/K)|$ ein Teiler von $[L : K]$. Es gilt Gleichheit genau dann, wenn L/K eine Galoiserweiterung ist.

Beweis. Sei $G = \operatorname{Gal}(L/K)$ und L^G der Fixkörper. Zunächst ist festzuhalten, dass G endlich ist, nach Proposition 1.2. Nach dem vorherigen Satz und dem Gradsatz gilt $|G| = [L : L^G] \mid [L : K]$. Wiederum mit dem Gradsatz folgt

$$|G| = [L : K] \quad \Leftrightarrow \quad [L^G : K] = 1 \quad \Leftrightarrow \quad L^G = K \quad \Leftrightarrow \quad L/K \text{ galoissch.}$$

∎

Folgerung 7.3

Sei L/K eine endliche Galoiserweiterung. Dann ist L/K separabel und normal.

Beweis. Für $G = \operatorname{Gal}(L/K)$ gilt $L^G = K$, und die Behauptung folgt unmittelbar aus dem Satz von Artin. ∎

8. Charakterisierungen von Galoiserweiterungen

Satz 8.1

Sei L/K eine endliche Körpererweiterung. Dann sind äquivalent:

(1) *L/K ist galoissch.*
(2) *L/K ist normal und separabel.*
(3) *L ist Zerfällungskörper eines separablen Polynoms in $K[T]$.*
(4) *Es gilt $|\operatorname{Gal}(L/K)| = [L : K]$.*

Beweis. Folgerung 7.2 zeigt die Äquivalenz von (1) und (4). Folgerung 7.3 zeigt die Implikation (1)⇒(2). Die Implikation (2)⇒(3) ist Folgerung 6.3, während (3)⇒(4) aus Satz 5.2 folgt. ∎

Folgerung 8.2

Sei L/K endlich galoissch und M ein Zwischenkörper. Dann ist L/M galoissch.

Beweis. Es ist L/K normal und separabel. Dann ist L/M nach Proposition 5.5 separabel, und offenbar ist L als Zerfällungskörper eines Polynoms f über K auch Zerfällungskörper von f über M, also ist L/M auch normal. ■

Folgerung 8.3

Sei L/K eine endliche Erweiterung. Ist L/K separabel, oder ist genauer $L = K(\alpha_1, \ldots, \alpha_n)$ mit allen α_i separabel über K, so ist der normale Abschluss N/K von L/K galoissch.

In dem Fall nennt man N auch einen *Galois-Abschluss* von L/K.

Beweis. Das Polynom $f = f_1 \cdot \ldots \cdot f_n$ im Beweis von Proposition 6.4 ist unter diesen Voraussetzungen separabel, also ist N/K separabel. ■

Aufgaben

Ü 8.1. Es gelte $\mathrm{Char}(K) \neq 2$. Jede Körpererweiterung L/K mit $[L : K] = 2$ ist galoissch. (Gilt dies auch, wenn $\mathrm{Char}(K) = 2$? Vgl. spätere Abschnitte.)

Ü 8.2. Sei $L = K(\alpha_1, \ldots, \alpha_n)$ mit allen α_i algebraisch und separabel über K. Dann ist die Körpererweiterung L/K separabel.

Ü 8.3. [Interner separabler Abschluss] Sei L/K eine endliche Erweiterung. Die Teilmenge $L_s \subseteq L$ aller über K separablen Elemente in L ist ein Zwischenkörper von L/K. Mit $[L : K]_s := [L_s : K]$ folgt

$$L/K \text{ separabel} \quad \Leftrightarrow \quad [L : K]_s = [L : K].$$

Ü 8.4. Sei L/K eine endliche Körpererweiterung mit $\mathrm{Char}(K) = p > 0$. Sei $\alpha \in L \setminus L_s$. Dann gibt es $n > 0$ mit $\alpha^{p^n} \in L_s$, und $\mathrm{MIPO}(\alpha/L_s)$ hat α als einzige (mehrfache) Nullstelle.

Ü 8.5. [Transitivität endlicher separabler Erweiterungen] Sei L/K eine endliche Erweiterung und M ein Zwischenkörper. Sind L/M und M/K separabel, so ist auch L/K separabel.

Skizze: Angenommen, L/K ist nicht separabel. Dann gilt $\mathrm{Char}(K) = p > 0$. Sei L_s der interne separable Abschluss über K. Dann gibt es $\alpha \in L \setminus L_s$. Es gilt $M \subseteq L_s$ und L/L_s ist separabel. Es gibt $n > 0$ mit $\alpha^{p^n} \in L_s$, und $g = (T - \alpha)^{p^n}$ liegt in $L_s[T]$. Ferner ist $\mathrm{MIPO}(\alpha/L_s)$ ein Teiler von g. Da aber α separabel über L_s ist, folgt $\alpha \in L_s$, Widerspruch.

(Ein methodisch anderer Beweis wird später mit Proposition IX.2.2 geführt.)

9. Der Hauptsatz der Galoistheorie

Lemma 9.1

Sei L/K eine Körpererweiterung und M ein Zwischenkörper. Ist $\sigma \in \mathrm{Gal}(L/K)$, so ist

$$\mathrm{Gal}(L/\sigma(M)) = \sigma \,\mathrm{Gal}(L/M)\sigma^{-1}. \tag{9.1}$$

Beweis. Ist τ ein M-Automorphismus von L, so ist $\sigma\tau\sigma^{-1}$ offenbar ein $\sigma(M)$-Automorphismus von L, und jeder solche ist von dieser Form. ■

Bemerkung. Ist M/K endlich und normal, so folgt $\mathrm{Gal}(L/M) \lhd \mathrm{Gal}(L/K)$, weil M in L nach Satz 6.5 mit all seinen Konjugierten $\sigma(M)$ übereinstimmt.

Sei L/K eine Körpererweiterung mit Galoisgruppe $G = \mathrm{Gal}(L/K)$. Bezeichne mit $\mathcal{Z}$ die Menge aller Zwischenkörper M von L/K, also so, dass $K \subseteq M \subseteq L$ ein Körperturm ist. Bezeichne mit $\mathcal{U}$ die Menge aller Untergruppen von G. Beides sind geordnete Mengen bzgl. der Inklusion.

Satz 9.2 (*Hauptsatz der Galoistheorie*)

Sei L/K eine endliche Galoiserweiterung mit Galoisgruppe $G = \mathrm{Gal}(L/K)$. Dann gilt:

(1) *Die Abbildungen*

$$\Phi\colon \mathcal{Z} \to \mathcal{U},\ M \mapsto \mathrm{Gal}(L/M)$$

und

$$\Psi\colon \mathcal{U} \to \mathcal{Z},\ U \mapsto L^U$$

sind ordnungs-umkehrend und zueinander invers.

(2) *Für jeden Zwischenkörper M von L/K ist die Körpererweiterung L/M galoissch; dagegen ist M/K galoissch (äquivalent: normal) genau dann, wenn $\Phi(M) = \mathrm{Gal}(L/M) \subseteq G$ ein Normalteiler ist. In diesem Fall hat man eine kanonische Isomorphie von Gruppen*

$$\mathrm{Gal}(M/K) \simeq \frac{\mathrm{Gal}(L/K)}{\mathrm{Gal}(L/M)}.$$

Beweis. (1) Sei M ein Zwischenkörper, also $M \in \mathcal{Z}$. Es ist L/M galoissch nach Folgerung 8.2. Mit $U = \mathrm{Gal}(L/M) \in \mathcal{U}$ folgt also $L^U = M$. Mit anderen Worten, es gilt $\Psi\Phi(M) = M$, also $\Psi \circ \Phi = 1_{\mathcal{Z}}$.

Sei umgekehrt U eine Untergruppe von G. Dann gilt nach dem Satz von Artin $\mathrm{Gal}(L/L^U) = U$, mit anderen Worten $\Phi\Psi(U) = U$. Damit gilt auch $\Phi \circ \Psi = 1_{\mathcal{U}}$.

(2) Der erste Teil wurde schon gezeigt. Sei M/K normal. Nach der Bemerkung zum Lemma ist dann $\mathrm{Gal}(L/M)$ ein Normalteiler in G.

Ist umgekehrt $\mathrm{Gal}(L/M)$ ein Normalteiler in G, so folgt aus (9.1) für jedes $\sigma \in G$ die Gleichheit $\mathrm{Gal}(L/\sigma(M)) = \mathrm{Gal}(L/M)$, also $\Phi(\sigma(M)) = \Phi(M)$. Aus Teil (1) folgt $\sigma(M) = M$ für jedes $\sigma \in G$, also ist M/K normal (also galoissch) nach Satz 6.5 (3)⇒(1).

Sind diese Bedingungen nun erfüllt, so ist die Einschränkung $\sigma \mapsto \sigma_{|M}$ ein Gruppenhomomorphismus $\rho\colon G = \mathrm{Gal}(L/K) \to \mathrm{Gal}(M/K)$, nach dem Einschränkungssatz 6.5. Dessen Kern ist offenbar gerade durch $\mathrm{Gal}(L/M)$ gegeben. Ferner ist ρ surjektiv aufgrund des Isomorphismen-Erweiterungs-Theorems 2.3. Also induziert ρ einen Isomorphismus $\mathrm{Gal}(L/K)/\mathrm{Gal}(L/M) \xrightarrow{\sim} \mathrm{Gal}(M/K)$, nach dem Homomorphiesatz. ∎

Aufgaben

Ü 9.1. Für die Bijektion in (1) im Hauptsatz ist die Voraussetzung "L/K galoissch" notwendig.

Ü 9.2. Sei L/K eine endliche normale Erweiterung. Sei L_s der separable Abschluss von K in L. Dann gilt: L_s/K ist galoissch, $\mathrm{Gal}(L/L_s) = \{1\}$ und $|\mathrm{Gal}(L/K)| = [L : K]_s$. (Hinweis: Vgl. Ü 8.4.)

Ü 9.3. Sei L/K endlich galoissch. Sei M ein Zwischenkörper und $K_0 = M^{\mathrm{Gal}(M/K)}$. Dann ist $\mathrm{Gal}(L/K_0)$ der Normalisator von $\mathrm{Gal}(L/M)$ in $\mathrm{Gal}(L/K)$, und es gilt

$$\mathrm{Gal}(M/K) \simeq \frac{\mathrm{Gal}(L/K_0)}{\mathrm{Gal}(L/M)}.$$

10. Ein Beispiel

Beispiel. Wir betrachten die Körpererweiterung $L = \mathbb{Q}(i, \sqrt[4]{2})$ über $K = \mathbb{Q}$.

(1) Offenbar ist L der Zerfällungskörper des separablen Polynoms $f = T^4 - 2$ über $\mathbb{Q}$, denn die komplexen Nullstellen von f sind $\alpha = \sqrt[4]{2}$, $i\alpha$, $-\alpha$, $-i\alpha$, und es ist $L = \mathbb{Q}(\alpha, i\alpha, -\alpha, -i\alpha)$. Daher ist L/K galoissch.

(2) Es gilt $[\mathbb{Q}(\alpha):\mathbb{Q}]=4$, denn T^4-2 ist nach Eisenstein das Minimalpolynom von α über $\mathbb{Q}$. Es ist $\mathbb{Q}(\alpha)\subseteq\mathbb{R}$, also $i\notin\mathbb{Q}(\alpha)$. Andererseits ist i Nullstelle des Polynoms $T^2+1\in\mathbb{Q}(\alpha)[T]$, und daher gilt $[\mathbb{Q}(\alpha,i):\mathbb{Q}(\alpha)]=2$. Es folgt daher

$$[L:K]=[\mathbb{Q}(\alpha,i):\mathbb{Q}(\alpha)]\cdot[\mathbb{Q}(\alpha):\mathbb{Q}]=2\cdot 4=8.$$

(3) Betrachte die Zwischenkörper $\mathbb{Q}(\alpha)$ und $\mathbb{Q}(i)$. Über diesen ist L jeweils einfach, erzeugt von i bzw. von α mit Minimalpolynomen T^2+1 über $\mathbb{Q}(\alpha)$ bzw. T^4-2 über $\mathbb{Q}(i)$. Nach Satz V.2.4 gibt es einen $\mathbb{Q}(i)$-Automorphismus σ von L mit $\sigma(\alpha)=i\alpha$ und einen $\mathbb{Q}(\alpha)$-Automorphismus τ von L mit $\tau(i)=-i$. Insbesondere sind dies K-Automorphismen, also $\sigma,\tau\in\mathrm{Gal}(L/K)$.

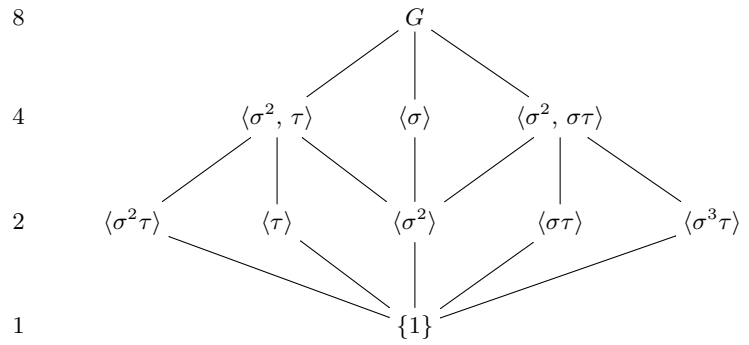
Automorphismus	Wirkung auf α	Wirkung auf i
1	α	i
σ	$i\alpha$	i
σ^2	$-\alpha$	i
σ^3	$-i\alpha$	i
τ	α	$-i$
$\sigma\tau$	$i\alpha$	$-i$
$\sigma^2\tau$	$-\alpha$	$-i$
$\sigma^3\tau$	$-i\alpha$	$-i$

Da dies 8 verschiedene K-Automorphismen sind, sind dies auch schon alle Elemente von $G=\mathrm{Gal}(L/K)$. Die abstrakte Beschreibung von G ist

$$G=\langle\sigma,\tau\mid\sigma^4=1=\tau^2,\ \tau\sigma=\sigma^3\tau\rangle.$$

Dies ergibt also die Diedergruppe $\mathbb{D}_4$ vom Grad 4.

(4) Wir haben den folgenden Untergruppenverband von G:



(5) Wir berechnen die Fixkörper der Untergruppen. Es ist $L^G=\mathbb{Q}$ und $L^{\{1\}}=L$. Schreibe jedes $x\in L$ in der Form

$$x=x_0+x_1\alpha+x_2\alpha^2+x_3\alpha^3+x_4i+x_5i\alpha+x_6i\alpha^2+x_7i\alpha^3$$

mit rationalen Koeffizienten.

Es ist

$$\begin{aligned}L^{\langle\sigma^2,\tau\rangle}&=\{x\in L\mid\sigma^2(x)=x=\tau(x)\}\\&=\{x\in L\mid x_1=x_3=x_5=x_7=0,\ x_4=x_6=0\}\\&=\{x=x_0+x_2\sqrt{2}\}\\&=\mathbb{Q}(\sqrt{2}).\end{aligned}$$

Ebenso

$$\begin{aligned}L^{\langle\sigma\rangle}&=\{x\in L\mid\sigma(x)=x\}\\&=\{x\in L\mid x_1=x_5=0,\ x_2=0=x_6,\ x_3=-x_7=0\}\\&=\{x=x_0+x_4i\}\\&=\mathbb{Q}(i).\end{aligned}$$

Ferner

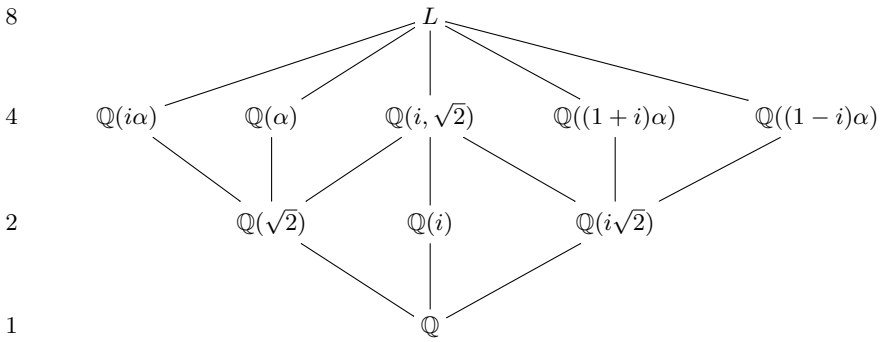
$$\begin{aligned} L^{\langle \sigma^2, \sigma\tau\rangle} &= \{x \in L \mid \sigma^2(x) = x = \sigma\tau(x)\} \\ &= \{x \in L \mid x_1 = x_3 = x_5 = x_7 = 0,\ x_2 = x_4 = 0\} \\ &= \{x = x_0 + x_6 i\sqrt{2}\} \\ &= \mathbb{Q}(i\sqrt{2}). \end{aligned}$$

Es sind noch die Fixkörper der Untergruppen der Ordnung 2 zu berechnen. Wir demonstrieren dies nur am folgenden Beispiel:

$$\begin{aligned} L^{\langle \sigma\tau\rangle} &= \{x \in L \mid \sigma\tau(x) = x\} \\ &= \{x \in L \mid x_1 = x_5,\ x_2 = 0 = x_4,\ x_3 = -x_7,\} \\ &= \{x = x_0 + x_1(1+i)\alpha + x_6 i\alpha^2 + x_3(1-i)\alpha^3\} \\ &= \{x = x_0 + x_1(1+i)\alpha + x_6/2((1+i)\alpha)^2 - x_3/2((1+i)\alpha)^3\} \\ &= \mathbb{Q}((1+i)\alpha). \end{aligned}$$

Analog ergibt sich $L^{\langle \sigma^2\rangle} = \mathbb{Q}(i, \sqrt{2})$, $L^{\langle \tau\rangle} = \mathbb{Q}(\alpha)$, $L^{\langle \sigma^2\tau\rangle} = \mathbb{Q}(i\alpha)$ und $L^{\langle \sigma^3\tau\rangle} = \mathbb{Q}((1-i)\alpha)$.

(6) Der Hauptsatz der Galoistheorie liefert daher den Zwischenkörperverband:



(7) Da (außer G und $\{1\}$) gerade die Untergruppen $\langle \sigma^2, \tau\rangle$, $\langle \sigma\rangle$, $\langle \sigma^2, \sigma\tau\rangle$ (vom Index 2) und $\langle \sigma^2\rangle$ Normalteiler von G sind, folgt aus dem Hauptsatz der Galoistheorie, dass von den Zwischenkörpern (außer $\mathbb{Q}$ und L selbst) genau die Zwischenkörper $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(i)$, $\mathbb{Q}(i\sqrt{2})$ und $\mathbb{Q}(i, \sqrt{2})$ normal (äquivalent: galoissch) über $\mathbb{Q}$ sind.

Aufgaben

Ü 10.1. Sei $\omega = e^{2\pi i/3}$ eine primitive dritte Einheitswurzel, und sei $\alpha = \sqrt[3]{2}$. Man bestimme die Galoisgruppe und den Zwischenkörperverband von $\mathbb{Q}(\alpha, \omega)/\mathbb{Q}$.

Ü 10.2. Man bestimme Galoisgruppe und Zwischenkörperverband der Körpererweiterung $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{-1})/\mathbb{Q}$.

Ü 10.3. Man bestimme die Galoisgruppe und den Zwischenkörperverband der folgenden Körpererweiterungen L/K mit $K = \mathbb{Q}$, sowie das Minimalpolynom des jeweils angegebenen primitiven Elements.

(1) $L = \mathbb{Q}(\sqrt{2 + \sqrt{2}})$.

(2) $L = \mathbb{Q}(\sqrt{4 + 3\sqrt{-1}})$.

11. Endliche Körper

Proposition 11.1

Sei K ein endlicher Körper. Dann gibt es eine Primzahl p und eine natürliche Zahl $n \geq 1$ mit $|K| = p^n$.

Beweis. Die Charakteristik von K ist eine Primzahl p, und es ist $n \stackrel{def}{=} [K : \Pi(K)] < \infty$. D. h. K ist ein n-dimensionaler Vektorraum über dem Körper $\Pi(K) = \mathbb{F}_p$, hat also p^n Elemente. ∎

Die folgende Aussage wird erst an späteren Stellen benötigt.

Satz 11.2

Sei K ein Körper, und G eine endliche Untergruppe der Einheitengruppe $E(K) = (K \setminus \{0\}, \cdot)$. Dann ist G zyklisch.

Beweis. G ist eine endliche abelsche Gruppe. Sei $n = |G|$. Dann gilt $x^n = 1$ für jedes $x \in G$. Sei $m \stackrel{def}{=} \min\{i \geq 1 \mid x^i = 1 \text{ für alle } x \in G\}$. Es gilt also $x^m = 1$ für jedes $x \in G$, d. h. jedes $x \in G$ ist Nullstelle des Polynoms $T^m - 1 \in \Pi(K)[T]$. Man hat also (mind.) n Nullstellen, andererseits hat es höchsten m Nullstellen. Es folgt $m = n$.

Zu zeigen ist noch, dass es ein $x \in G$ der Ordnung m gibt: Sei $m = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ die Primfaktorzerlegung von m ($p_1, \dots, p_r$ paarweise verschieden prim, $\alpha_i \geq 1$). Wegen der Minimalität ist m ein Teiler des kgV's der Ordnungen aller Elemente von G, also gibt es zu jedem i ein $g_i \in G$, dessen Ordnung von $p_i^{\alpha_i}$ geteilt wird. Ist $k_i p_i^{\alpha_i} = \mathrm{ord}(g_i)$, so hat $g_i^{k_i}$ die Ordnung $p_i^{\alpha_i}$; vgl. Ü I.2.1. Das Element $g \stackrel{def}{=} g_1^{k_1} g_2^{k_2} \dots g_r^{k_r}$ hat dann, vgl. Ü I.2.3, die Ordnung $p_1^{\alpha_1} \dots p_r^{\alpha_r} = m$, was zu zeigen war. ∎

Proposition 11.3

Sei K ein endlicher Körper mit $q = p^n$ Elementen (p prim). Dann ist K ein Zerfällungskörper des Polynoms $T^q - T \in \mathbb{F}_p[T]$.

Beweis. Ist $x \in K$, $x \neq 0$, also $x \in E(K)$, so gilt nach dem kleinen Satz von Fermat $x^{q-1} = 1$, damit $x^q = x$. Letzteres gilt auch für $x = 0$. Die q verschiedenen Elemente aus K sind also gerade die Nullstellen $x_1, \dots, x_q$ des Polynoms $T^q - T \in \Pi(K)[T]$. Da sicherlich auch $K = \Pi(K)(x_1, \dots, x_q)$ gilt, ist K der Zerfällungskörper des Polynoms $T^q - T$ über $\Pi(K) \simeq \mathbb{F}_p$. ∎

Satz 11.4

Sei $q = p^n$ mit p prim und $n \geq 1$.

(1) [Galois (1830)] *Es gibt einen Körper K mit q Elementen.*

(2) [Moore (1893)] *Je zwei Körper mit q Elementen sind isomorph.*

Beweis. (1) Sei K Zerfällungskörper des Polynoms $f = T^q - T \in \mathbb{F}_p[T]$. Die Menge N der Nullstellen von f in K bildet einen Teilkörper von K: Denn sind $x, y \in K$ Nullstellen von f, so gilt wegen $p \mid \binom{p}{i}$ für $1 \leq i \leq p-1$

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

und dann per Induktion nach n

$$(x+y)^q = x^q + y^q = x + y,$$

und außerdem ist

$$(xy)^q = x^q y^q = xy,$$

und ebenso für $x \neq 0$, $(x^{-1})^q = (x^q)^{-1} = x^{-1}$, und $(-x)^q = -x$ (unterscheide die Fälle p gerade bzw. ungerade). Also ist N ein Teilkörper von K. Da aber f schon über N in Linearfaktoren zerfällt, gilt $N = K$. Damit besteht K aus den Nullstellen von f. Nun ist $D(f) = qT^{q-1} - 1 = -1$, und daher ist $\mathrm{ggT}(f, D(f)) =$

1 und es hat f nur einfache Nullstellen, vgl. Satz 4.3. Damit hat f genau q verschiedene Nullstellen, und K ist ein Körper mit q Elementen.

(2) Folgt aus Proposition 11.3 und der Eindeutigkeit des Zerfällungskörpers (genauer Satz 2.3). ∎

Notation: Einen Körper mit $q = p^n$ Elementen bezeichnen wir mit $\mathbb{F}_q$. Endliche Körper werden oft auch *Galoisfelder* genannt.

12. Der Frobenius-Endomorphismus

Definition 12.1

Sei K ein Körper der Charakteristik $p > 0$. Dann ist die Abbildung $\sigma_p \colon K \to K$, $x \mapsto x^p$ ein Morphismus von Ringen, und heißt der *Frobenius-Endomorphismus* von K. Er ist immer injektiv. Sein Bild $\sigma_p(K)$ wird mit K^p bezeichnet.

Erweiterungen endlicher Körper. Die beiden folgenden Sätze vervollständigen die Klassifikation endlicher Körper, hier in Bezug auf ihre (endlichen) Körpererweiterungen und Zwischenkörperverbände.

Satz 12.2

Sei $q = p^n$ (p prim, $n \geq 1$). Dann ist $\mathbb{F}_q/\mathbb{F}_p$ galoissch mit zyklischer Galoisgruppe der Ordnung n, erzeugt von dem Frobenius-Automorphismus $\sigma_p \colon x \mapsto x^p$.

Beweis. $\mathbb{F}_q$ ist Zerfällungskörper des Polynoms $T^q - T$ über $\mathbb{F}_p$. Dieses Polynom ist separabel, denn der ggT von $T^q - T$ und $D(T^q - T) = -1 \neq 0$ ist eine Einheit. Damit ist $\mathbb{F}_q/\mathbb{F}_p$ normal und separabel nach Satz 8.1.

Es ist offenbar $\sigma \colon x \mapsto x^p$ ein $\mathbb{F}_p$-Automorphismus von $\mathbb{F}_q$. Denn für jedes $x \in \mathbb{F}_p$ gilt $x^p = x$, und σ ist injektiv, und wegen der Endlichkeit auch surjektiv. Sei m die Ordnung von σ. Da die Ordnung der Galoisgruppe gleich dem Körpergrad $[\mathbb{F}_q : \mathbb{F}_p] = n$ ist, folgt $m \mid n$. Für jedes $x \in \mathbb{F}_q$ folgt $x = \sigma^m(x) = x^{p^m}$. Also sind alle $q = p^n$ Elemente von $\mathbb{F}_q$ Nullstellen des Polynoms $T^{p^m} - T$, und es folgt $p^m = p^n$, also $m = n$. ∎

Bemerkung. Sei L/K eine Körpererweiterung endlicher Körper. Sei $\mathrm{Char}(K) = p$ (Primzahl). Ist $[L : K] = s$ und $[K : \mathbb{F}_p] = n$, so gilt $K = \mathbb{F}_{p^n}$ und $L = \mathbb{F}_{p^{sn}}$.

Satz 12.3

Sei L/K eine endliche Körpererweiterung des endlichen Körpers K und sei $s = [L : K]$ sowie $|K| = p^n =: q$.

(1) *Es ist L/K galoissch.*

(2) *Die Galoisgruppe $\mathrm{Gal}(L/K)$ ist zyklisch, erzeugt von $\sigma_q = \sigma_p{}^n \colon x \mapsto x^q$, der n-ten Potenz des Frobenius-Automorphismus' von L.*

(3) *Sei M ein Zwischenkörper. Dann ist $|M| = p^{rn}$ für einen Teiler r von s. Zu jedem Teiler r von s gibt es genau einen Zwischenkörper M mit $|M| = p^{rn}$.*

Beweis. (1) Es ist K Zwischenkörper von der Galoiserweiterung $L/\mathbb{F}_p$. Also ist auch L/K galoissch.

(2) Es ist $K = \mathbb{F}_{p^n}$ und $L = \mathbb{F}_{p^{sn}}$. Für jedes $x \in K$ ist $\sigma_q(x) = x^q = x$, also ist σ_q ein K-Automorphismus. Es hat σ_p die Ordnung $[L : \mathbb{F}_p] = sn$. Daher hat $\sigma_q = \sigma_p{}^n$ die Ordnung s.

(3) Die Aussage über die Anzahl folgt aus dem Gradsatz. Die zyklische Gruppe $\mathrm{Gal}(L/K)$ hat zu jedem Teiler r von s genau eine Untergruppe U der Ordnung

s/r. Übergang zu den Fixkörpern, den Hauptsatz der Galoistheorie ausnutzend, folgt das Ergebnis. ■

Aufgaben

Ü 12.1. (1) Sei K ein endlicher Körper. Seien f, $g \in K[T]$ irreduzibel und vom selben Grad. Man zeige, dass f und g denselben Zerfällungskörper über K haben.

(2) Man zerlege $T^4 + 1 \in \mathbb{F}_3[T]$ in irreduzible Faktoren und bestimme den Zerfällungskörper von $T^4 + 1$ über $\mathbb{F}_3$.

(3) Man mache das gleiche für $T^5 + 2T^3 + 2 \in \mathbb{F}_3[T]$. (Hinweis: Man probiere einen Teiler aus (2).)

Ü 12.2. Sei K ein endlicher Körper. Es gibt zu jedem $n \in \mathbb{N}$ irreduzible Polynome in $K[T]$ vom Grad n.

Ü 12.3. Sei $K = \mathbb{F}_q$ der endliche Körper mit q Elementen. Sei $n \geq 1$ eine natürliche Zahl. Es bezeichne $N_q(n)$ die Anzahl aller normierten, irreduziblen Polynome in $K[T]$ vom Grad n. Es sei $L = \mathbb{F}_{q^n}$. Also $[L : K] = n$.

(1) Das Produkt aller normierten, irreduziblen Polynome in $K[T]$ vom Grad d, über alle (positiven) Teiler d von n, ist das Polynom $T^{q^n} - T$.

(2) Jedes normierte, irreduzible Polynom vom Grad $d \mid n$ hat in L genau d verschiedene Nullstellen.

(3) Es folgt $q^n = \sum_{d|n} dN_q(d)$.

(4) Es gilt $N_q(n) = \frac{1}{n} \sum_{d|n} \mu(d) q^{n/d}$. Hierbei ist $\mu\colon \mathbb{N}_{\geq 1} \to \{-1, 0, 1\}$ die Möbius-Funktion, definiert durch

$$\mu(n) = \begin{cases} 1 & \text{falls } n = 1 \\ (-1)^k & \text{falls } n \text{ Produkt von } k \text{ verschiedenen Primzahlen ist} \\ 0 & \text{falls } n \text{ vom Quadrat einer Primzahl geteilt wird.} \end{cases}$$

(5) Für $n = 1, 2, 3, 4, 5, 6$ gebe man $N_q(n)$ direkt an.

Ü 12.4. Sei K ein endlicher Körper. Dann ist jedes Element in K Summe von zwei Quadraten, also von der Form $x^2 + y^2$ mit x, $y \in K$. (Betrachte die Abbildung $K^\times \to K^\times$, $x \mapsto x^2$.)

Ü 12.5. Sei p eine Primzahl. Man beschreibe den Zwischenkörperverband von $\mathbb{F}_{p^{36}}/\mathbb{F}_p$.

13. Perfekte Körper *

Definition 13.1

Ein Körper K heißt *perfekt* (oder *vollkommen*), wenn jedes (nicht-konstante) Polynom $f \in K[T]$ separabel über K ist.

Bemerkung. Es genügt offenbar, irreduzible (und normierte) Polynome zu betrachten. Ein Körper K ist genau dann perfekt, wenn jede endliche Körpererweiterung L/K separabel ist.

Folgerung 13.2

Jeder endliche Körper ist perfekt.

Beweis. Dies folgt aus Satz 12.3; alternativ (und direkter) auch aus folgendem Satz. ■

Satz 13.3 (*Steinitz*)

Sei K ein Körper. Genau in den folgenden beiden Fällen ist K perfekt:

- $\mathrm{Char}(K) = 0$.
- $\mathrm{Char}(K) = p > 0$, *und der Frobenius-Endomorphismus* $K \to K$, $x \mapsto x^p$ *ist surjektiv (d. h. es gilt* $K^p = K$*).*

Beweis. Ist $\mathrm{Char}(K) = 0$, so folgt aus Satz 5.4, dass K perfekt ist. Nehmen wir also $\mathrm{Char}(K) = p > 0$ an. Zu zeigen ist: K ist perfekt genau dann, wenn der Frobenius-Endomorphismus surjektiv ist.

Sei der Frobenius-Endomophismus surjektiv. Sei $f \in K[T]$ vom Grad ≥ 1. Offenbar gilt $D(f) = 0$ genau dann, wenn f eine Polynom in T^p ist. Sei etwa $f = \sum_{i=0}^{n} a_{ip} T^{ip}$. Nach Voraussetzung gibt es $b_i \in K$ mit $a_{ip} = {b_i}^p$, und dann ist

$$f = \left(\sum_{i=0}^{n} b_i T^i \right)^p$$

nicht irreduzibel. Anders ausgedrückt: Ist $f \in K[T]$ irreduzibel, so gilt $D(f) \neq 0$, und daher hat f nach Satz 4.3 nur einfache Nullstellen, ist also separabel.

Der Frobenius-Endomorphismus sei nicht surjektiv. Dann gibt es ein $a \in K$, so dass das Polynom $f = T^p - a \in K[T]$ keine Nullstelle in K hat. Sei L Zerfällungskörper von f über K. Es gibt ein $b \in L$ mit $f(b) = 0$, also mit $a = b^p$, und es folgt

$$f = T^p - b^p = (T - b)^p.$$

Sei g ein irreduzibler (und ohne Einschränkung normierter) Faktor von f in $K[T]$. Dann ist g auch ein Faktor von f in $L[T]$, und muss daher von der Form $g = (T - b)^m$ sein, wobei $m \leq p$ gilt sowie $m \geq 2$ (denn für $m = 1$ folgt $b \in K$). Damit hat das irreduzible Polynom $g \in K[T]$ eine mehrfache Nullstelle, ist also nicht separabel über K. ∎

Ü 13.1. Sei L/K eine endliche Körpererweiterung. Es ist K perfekt genau dann, wenn L perfekt ist.

14. Der Satz vom primitiven Element

Erinnerung: Für eine algebraische Körpererweiterung L/K heisst $\alpha \in L$ ein *primitives Element*, falls $L = K(\alpha)$ gilt.

Satz 14.1 (*Steinitz' Satz über die Zwischenkörper (1910)*)

Sei L/K eine endliche Körpererweiterung. Es gibt ein $\alpha \in L$ mit $L = K(\alpha)$ genau dann, wenn es nur endlich viele Zwischenkörper von L/K gibt.

Beweis. "⇒" Gelte $L = K(\alpha)$. Sei F ein Zwischenkörper von L/K. Sei $f = T^n + \sum_{i=0}^{n-1} a_i T^i$ das Minimalpolynom von α über F und setze $E = K(a_0, a_1, \ldots, a_{n-1})$. Dann gilt $F = E$: Denn $F \supseteq E$ ist klar. Es ist f offenbar irreduzibel auch über E, und ist daher das Minimalpolynom von α über E. Es ist $L = F(\alpha)$ und $L = E(\alpha)$, und es folgt $[L : F] = \mathrm{grad}(f) = [L : E]$, und aus dem Gradsatz folgt dann $F = E$. – Nun ist f ein Teiler des Minimalpolynoms von α über K. Also gibt es für E wie oben nur endlich viele Möglichkeiten.

"⇐" Es habe L/K nur endlich viele Zwischenkörper. Ist K ein endlicher Körper, so auch L, und L/K ist einfach, da die Einheitengruppe $E(L)$ nach Satz 11.2 zyklisch ist. Also kann man im folgenden annehmen, dass K unendlich ist. Seien $\alpha, \beta \in L$. Durchläuft c die unendlich vielen Elemente aus K, gibt es nur endlich viele verschiedene (Zwischen-) Körper $K(\alpha + c\beta)$. Es gibt also $c_1, c_2 \in K$ mit $c_1 \neq c_2$ und

$$F \overset{def}{=} K(\alpha + c_1\beta) = K(\alpha + c_2\beta).$$

Das bedeutet, dass $\alpha + c_1\beta$ und $\alpha + c_2\beta$ im selben Körper F liegen, also auch $(c_1 - c_2)\beta \in F$, damit $\beta \in F$, und dann auch $\alpha \in F$. Es folgt $K(\alpha, \beta) = F = K(\alpha + c_1\beta)$, also wird $K(\alpha, \beta)$ schon von einem Element erzeugt.

Allgemein ist L von der Form $K(a_1, \ldots, a_n)$. Per Induktion führt man dies aber auf den gerade behandelten Fall zweier Erzeuger zurück. ∎

Satz 14.2 (*Satz vom primitiven Element*)

Sei L/K eine endliche Körpererweiterung. Ist L/K separabel, so gibt es ein $\alpha \in L$ mit $L = K(\alpha)$.

Beweis. Sei N/K normaler Abschluss von L/K. Dann ist N/K endlich galoissch, hat also nach dem Hauptsatz der Galoistheorie nur endlich viele Zwischenköper, nämlich genau so viele wie Untergruppen von $\mathrm{Gal}(N/K)$. Dann hat natürlich auch L/K nur endlich viele Zwischenkörper. Nun können wir den Satz über die Zwischenkörper anwenden. ■

Folgerung 14.3

Jede endliche Galoiserweiterung ist einfach algebraisch. ■

Folgerung 14.4

Sei L/K eine endliche Körpererweiterung mit $\mathrm{Char}(K) = 0$. Dann ist L/K einfach algebraisch. ■

Die einfachsten Beispiele für nicht-separable (endliche) Körpererweiterungen bzw. nicht-perfekte Körper sind durch folgende Aussage beschrieben.

Proposition 14.5

Sei p eine Primzahl. Sei $L = \mathbb{F}_p(X)$ der rationale Funktionenkörper über $\mathbb{F}_p$. Es gilt:

(a) *Der Frobenius-Endomorphismus $L \longrightarrow L$, $x \mapsto x^p$ ist nicht surjektiv. (D. h. der Körper L ist nicht perfekt.)*

(b) *Sei $K \subset L$ der Teilkörper $K = \mathbb{F}_p(X^p)$. Es gilt $[L : K] = p$, und L/K ist nicht separabel.*

Beweis. (a) Es liegt z. B. das Element X nicht im Bild des Frobenius-Endomorphismus: denn andernfalls würde gelten $X = \big(f(X)/g(X)\big)^p$ mit Polynomen $f, g \in \mathbb{F}_p[X]$. Dann folgte aber $X \cdot g(X^p) = X \cdot g(X)^p = f(X)^p = f(X^p)$, was offenbar nicht möglich ist.

(b) Man zeigt leicht, dass $1, X, X^2, \ldots, X^{p-1}$ eine K-Basis von L ist. Das (primitive) Element $X \in L$ ist nicht separabel über K: denn das Minimalpolynom von X über K ist (vgl. obige Basis) $T^p - X^p \in K[T]$, und wegen $T^p - X^p = (T - X)^p$ ist X eine p-fache Nullstelle in L. ■

Bemerkung. Die Körpererweiterung in (b) (die das primitive Element X hat) ist auch ein Beispiel dafür, dass im Satz vom primitiven Element allgemein nicht die Umkehrung gilt. — Für ein Beispiel einer endlichen Körpererweiterung, die kein primitives Element enthält, siehe Ü 14.8.

Bemerkung. [Alternativer Beweis ohne Hauptsatz] Der Satz vom primitiven Element geht im wesentlichen auf E. Galois (um 1830) zurück[2]. Vor Emil Artins Beiträgen zur Galoistheorie [1], in denen ein Schwerpunkt darauf lag, die linearen Aspekte zu betonen, wurde der Satz vom primitiven Element *vor* dem Hauptsatz bewiesen und *umgekehrt* zum Beweis des letzteren benutzt. Heutzutage sind beide Wege in der Lehrbuchliteratur weit verbreitet. Für einen solchen eher "klassischen" Beweis können wir z. B. Ü 6.9 verwenden, die insbesondere folgendes aussagt.

Ist L/K endlich separabel und N/K normaler Abschluss von L/K, so ist die Anzahl der K-Monomorphismen $L \to N$ gleich $[L : K]$.

[2]Vgl. Neumann [12], Lemma III, Seite 111, auch Seiten 205, 207. Primitive Elemente wurden lange Zeit auch *Galoissche Resolventen* genannt. Schon Lagrange war nah an der Existenz dran, hat sie aber nicht explizit formuliert. Wie Galois' (davon unabhängige) lückenhafte Beweisargumentation seines Lemma III leicht geschlossen werden kann, wird in [5, §37] gezeigt.

Beweisskizze. Induktion nach $n = [L : K]$. Der Fall $n = 1$ ist trivial, also sei $n > 1$. Seien $\alpha \in L$, $\alpha \notin K$ und $f = \mathrm{MIPO}(\alpha/K)$, welches separabel ist. Also zerfällt f über N in s paarweise verschiedene Linearfaktoren, wobei $s = \mathrm{grad}(f) = [K(\alpha) : K]$. Seien $\alpha_1, \ldots, \alpha_s$ in N die Nullstellen von f. Aus dem Isomorphismen-Erweiterungs-Theorem folgt, dass es zu jedem i einen K-Automorphismus σ_i von N gibt mit $\sigma_i(\alpha) = \alpha_i$. Da auch $L/K(\alpha)$ separabel und $N/K(\alpha)$ normal ist, folgt aus der Induktionsvoraussetzung, dass es genau $[L : K(\alpha)] = n/s = r$ viele $K(\alpha)$-Monomorphismen $\tau_1, \ldots, \tau_r \colon L \to N$ gibt. Die Kompositionen $\sigma_i\tau_j$ sind dann n verschiedene (!) K-Monomorphismen $L \to N$. Dies sind alle: ist $\sigma \colon L \to N$ ein beliebiger K-Monomorphismus, so gibt es wegen $f(\sigma(\alpha)) = 0$ ein i mit $\sigma(\alpha) = \alpha_i$. Dann ist $\sigma_i^{-1}\sigma$ ein $K(\alpha)$-Monomorphismus $L \to N$, und daher wie oben schon gezeigt von der Form τ_j für ein j. Es folgt $\sigma = \sigma_i\tau_j$. —

Nun zum primitiven Element. Sei L/K endlich separabel mit normalem Abschluss N. Seien $\sigma_1, \ldots, \sigma_n \colon L \to N$ die verschiedenen K-Monomorphismen, wobei $n = [L : K]$ gilt. Für alle $i \neq j$ ist $\sigma_i - \sigma_j \colon L \to N$ eine K-lineare Abbildung. Sei $\Delta := \prod_{i<j}(\sigma_i - \sigma_j)$.

Jedes $a \in L$ mit $\Delta(a) \neq 0$ ist ein primitives Element für L.

Denn sei $f = \mathrm{MIPO}(a/K)$. Dieses hat (inklusive a) die n verschiedenen Nullstellen $\sigma_1(a), \ldots, \sigma_n(a) \in N$. Es folgt $n \leq \mathrm{grad}(f) = [K(a) : K] \leq [L : K] = n$. Also $L = K(a)$.

Es bleibt die Existenz eines solchen a zu zeigen. Dazu nehmen wir K unendlich an (für endliche K folgt die Existenz eines primitiven Elements direkt aus Satz 11.2). Wir betrachten $\mathrm{Kern}(\sigma_i - \sigma_j) \subsetneq L$ für $i < j$. Es ist eine leichte Übung in der Linearen Algebra, dass ein Vektorraum über einem unendlichen Körper K niemals eine endliche Vereinigung von echten Unterräumen sein kann. Deshalb gibt es ein $a \in L$ mit $\sigma_i(a) - \sigma_j(a) \neq 0$ für alle $i < j$, also mit $\Delta(a) \neq 0$.

Aufgaben

Ü 14.1. Sei L/K eine endliche Körpererweiterung. Äquivalent sind:
(1) L/K ist galoissch.
(2) L ist Zerfällungskörper eines irreduziblen, separablen Polynoms über K.

Ü 14.2. Man bestimme mit dem (Beweis vom) Satz über die Zwischenkörper alle Zwischenkörper von $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$. Man vergleiche das Ergebnis mit der Menge der Untergruppen von $\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q})$. Was fällt auf? Erklärung?

Ü 14.3. Jede einfach transzendente Körpererweiterung $K(\alpha)/K$ hat unendlich viele Zwischenkörper.

Ü 14.4. Sei L/K eine (algebraische) separable Körpererweiterung, und es gebe eine natürliche Zahl $n \geq 1$, so dass jedes Element α von L vom Grad $\leq n$ über K ist. Dann gilt $[L : K] \leq n$.

Ü 14.5. Ist gemäß obiger Bemerkung der Satz vom primitiven Element schon *vor* dem Satz von Artin gezeigt, so lässt sich der Beweis des Satzes von Artin mit Hilfe der vorstehenden Übung drastisch verkürzen.

Ü 14.6. Sei L/K eine einfach algebraische Erweiterung. Ist M ein Zwischenkörper von L/K, so ist auch M/K einfach algebraisch.

Ü 14.7. Die Erweiterung $\mathbb{F}_p(X)/\mathbb{F}_p(X^p)$ ist normal. Die Galoisgruppe besteht nur aus der Identität.

Ü 14.8. Sei $k = \mathbb{F}_p$ (mit p prim). Sei L der Quotientenkörper $k(X, Y)$ des Polynomrings $k[X, Y] = k[X][Y]$ in zwei Unbestimmten X und Y, über dem Körper k. Sei K der Teilkörper $k(X^p, Y^p)$ von L. Dann gilt $L = K(X, Y)$, und L/K ist eine endliche Körpererweiterung vom Grad $[L : K] = p^2$. Es gilt $\mathrm{Gal}(L/K) = \{1\}$. Die Zwischenkörper $K(X + \lambda Y)$ sind für $\lambda \in K$ *paarweise verschieden*, definieren also unendlich viele Zwischenkörper von L/K. Diese endliche Erweiterung besitzt also kein primitives Element.

(Man vgl. den Beweis des Satzes über die Zwischenkörper und zeige $[K(X+\lambda Y) : K] = p$ mit Hilfe des Frobenius-Endomorphismus'.)

Ü 14.9. Sei L/K eine endliche Körpererweiterung mit $\mathrm{Char}(K) = p > 0$. Es gelte $[L : K] > p$, und für jedes x in L gelte $x^p \in K$. Dann gilt [Steinitz]:

(1) L/K hat *kein* primitives Element.
(2) L/K hat unendlich viele Zwischenkörper. — (Man zeige (2) direkt, d. h. ohne Verwendung der Aussage des Satzes über die Zwischenkörper.)

Ü 14.10. Sei K unendlich und L/K eine endliche Körpererweiterung. Man zeige direkt, dass L nicht eine Vereinigung von endlich vielen echten Zwischenkörpern sein kann. Dies gibt einen schnellen (aber nicht-"konstruktiven") Beweis für die Richtung "$\Leftarrow$" im Satz über die Zwischenkörper (für K unendlich).

Ü 14.11. Sei L/K endlich galoissch, sei $a \in L$ ein primitives Element. Sei H eine Untergruppe von $\mathrm{Gal}(L/K)$. Wir betrachten den Fixkörper L^H.

(1) Es ist $f := \prod_{\sigma \in H}(T - \sigma(a)) \in L^H[T]$ das Minimalpolynom von a über L^H.
(2) Schreiben wir $f = T^m + c_1 T^{m-1} + \ldots + c_{m-1}T + c_m$, so gilt $L^H = K(c_1, \ldots, c_m)$.

Ü 14.12. Der Satz vom primitiven Element kann etwas verbessert werden: Sei $L = K(a, c_1, \ldots, c_n)$ eine Körpererweiterung, wobei $a, c_1, \ldots, c_n$ über K algebraisch und $c_1, \ldots, c_n$ über K separabel sind. Dann hat L/K ein primitives Element.

KAPITEL VII

Anwendungen der Galoistheorie

In dem Kapitel besprechen wir drei wesentliche Anwendungen der Galoistheorie:

I. Galois' Kriterium zur Auflösbarkeit von Gleichungen durch Radikale. Dieser Block wird in den Paragraphen 1.–5. behandelt. (Weitere Resultate aus dem Bereich werden im anschließenden optionalen Kapitel behandelt.)
II. Gauß' Satz über die Konstruierbarkeit regelmäßiger n-Ecke. Dies überdeckt die Paragraphen 6.–7., und wird ergänzt durch ein allgemeines Kriterium in 8.
III. Der Fundamentalsatz der Algebra soll hier weitestgehend algebraisch bewiesen werden, Paragraph 9.

1. Einheitswurzeln

Sei K ein Körper, sei $n \geq 1$ eine natürliche Zahl. Ein $\zeta \in K$ heißt n-te *Einheitswurzel*, falls $\zeta^n = 1$ gilt. Die Menge der n-ten Einheitswurzeln in K bilden eine Gruppe $\mu_n(K)$, eine Untergruppe der Einheitengruppe $E(K)$. Da jede n-te Einheitswurzel in K Nullstelle des Polynoms $T^n - 1 \in K[T]$ ist, hat $\mu_n(K)$ endliche Ordnung $\leq n$. Aus Satz VI.11.2 folgt, dass $\mu_n(K)$ eine zyklische Gruppe ist. Ist $\zeta \in \mu_n(K)$ von der Ordnung n, so heißt ζ eine *primitive* n-te Einheitswurzel. Die Menge aller primitiven n-ten Einheitswurzeln in K bezeichen wir mit $\mu_n^*(K)$.

Definition 1.1

Seien K ein Körper und $n \geq 1$ eine natürliche Zahl. Mit $E_n(K)$ bezeichnen wir einen Zerfällungskörper von $T^n - 1$ über K. Man nennt $E_n(K)$ den n-ten *Kreisteilungskörper* über K.

Proposition 1.2

Seien K ein Körper und $n \geq 1$ eine natürliche Zahl, die nicht von $\mathrm{Char}(K)$ geteilt wird (z. B. $\mathrm{Char}(K) = 0$).

(1) *Die Erweiterung $E_n(K)/K$ ist galoissch.*
(2) *Die Anzahl der primitiven n-ten Einheitswurzeln in $E_n(K)$ ist gleich $\varphi(n) = |E(\mathbb{Z}/n\mathbb{Z})| = |\{1 \leq k < n \mid \mathrm{ggT}(k,n) = 1\}|$.*

Beweis. (1) Das Polynom $T^n - 1$ hat keine mehrfachen Nullstellen in $E_n(K)$, da $D(T^n - 1) = nT^{n-1} \neq 0$ offenbar teilerfremd zu $T^n - 1$ ist. Als Zerfällungskörper des separablen Polynoms $T^n - 1$ über K ist daher $E_n(K)/K$ galoissch.

(2) Sei $L = E_n(K)$. Als endliche Untergruppe von $E(L)$ ist $\mu_n(L)$ zyklisch, erzeugt von einer primitiven Einheitswurzel ζ und von der Ordnung n. Es ist also $\mu_n^*(L) = \{\zeta^k \mid 1 \leq k < n,\ \zeta^k \text{ primitiv}\}$. Nun ist ζ^k primitiv genau dann, wenn es eine natürliche Zahl $s > 0$ gibt mit $(\zeta^k)^s = \zeta$, was aber gerade $ks = 1 + rn$ für ein $r \in \mathbb{Z}$ bedeutet. Dies ist äquivalent dazu, dass k eine Einheit in $\mathbb{Z}/n\mathbb{Z}$ ist, und auch dazu, dass $\mathrm{ggT}(k,n) = 1$ gilt. ∎

Satz 1.3

Seien $n \geq 1$ und K ein Körper, dessen Charakteristik n nicht teilt. Dann ist $\mathrm{Gal}(E_n(K)/K)$ isomorph zu einer Untergruppe von $E(\mathbb{Z}/n\mathbb{Z})$ und damit insbesondere abelsch.

Beweis. Sei $\zeta \in E_n(K)$ eine feste primitive n-te Einheitswurzel. Es gilt $E_n(K) = K(\zeta)$. Die Abbildung $\phi_n \colon \mathrm{Gal}(E_n(K)/K) \to E(\mathbb{Z}/n\mathbb{Z}), \sigma \mapsto [k] = k \bmod n$, wobei $1 \leq k < n$ gilt mit $\sigma(\zeta) = \zeta^k$. Da $\sigma(\zeta)$ wieder primitiv ist, gilt, dass k teilerfremd zu n ist, also ist $[k]$ eine Einheit in $\mathbb{Z}/n\mathbb{Z}$. Gelte $\sigma(\zeta) = \zeta^k$ und $\tau(\zeta) = \zeta^l$ mit $1 \leq k, l < n$. Es ist

$$\sigma\tau(\zeta) = \sigma(\zeta^l) = (\sigma(\zeta))^l = (\zeta^k)^l = \zeta^{kl} = \zeta^{kl \bmod n},$$

und es folgt $\phi_n(\sigma\tau) = [kl] = [k] \cdot [l] = \phi_n(\sigma)\phi_n(\tau)$. Also ist ϕ_n ein Gruppenmorphismus. Sei $\sigma \in \mathrm{Gal}(E_n(K)/K)$ mit $\phi_n(\sigma) = [1]$. Dann gilt $\sigma(\zeta) = \zeta$, und es folgt $\sigma = 1_{E_n(K)}$. ∎

Aufgaben

Ü 1.1. Ist in Satz 1.3 $n = p$ prim, so ist die Galoisgruppe sogar zyklisch.

Ü 1.2. Sei $p = \mathrm{Char}(K) > 0$. Man bestimme den Zerfällungskörper von $T^{p^m} - 1$ über K.

Ü 1.3. Seien $n \geq 1$ und K ein Körper, der eine primitive n-te Einheitswurzel enthält. Dann ist $\mathrm{Char}(K)$ kein Teiler von n.

Ü 1.4. Seien $n \geq 1$ und K ein Körper, der eine primitive n-te Einheitswurzel enthält. Dann enthält K für jeden positiven Teiler d von n eine primitive d-te Einheitswurzel.

2. Zyklische Erweiterungen

Definition 2.1

Eine Körpererweiterung L/K heisst *zyklisch* (bzw. *abelsch*), wenn sie galoissch mit zyklischer (bzw. abelscher) Galoisgruppe ist.

Definition 2.2

Eine Körpererweiterung L/K heißt *einfache Radikalerweiterung*, falls es ein $b \in L$ gibt mit $L = K(b)$ und mit $b^n \in K$ für eine natürliche Zahl $n \geq 1$.

Gilt hierbei $b^n = a \in K$, so schreibt man auch $b = \sqrt[n]{a}$ und $L = K(\sqrt[n]{a})$. Es bezeichnet also $\sqrt[n]{a}$ *eine* Nullstelle des Polynoms $T^n - a$. Ein Polynom dieser Form nennt man auch ein *reines Polynom*. Einen Ausdruck der Form $\sqrt[n]{a}$ nennt man auch ein *Radikal*. (Diese können auch ineinander verschachtelt sein.)

Satz 2.3 (*Galois*)

Sei K ein Körper, der eine primitive n-te Einheitswurzel ζ enthält.

(1) *Jede Körpererweiterung der Form $K(\sqrt[n]{a})/K$ mit $a \in K$ ist eine zyklische Erweiterung; die Ordnung der Galoisgruppe teilt n.*

(2) *Ist L/K eine zyklische Erweiterung vom Grad $[L : K] = n$, so ist L Zerfällungskörper eines Polynoms $T^n - a$ für ein $a \in K^\times$; also $L = K(\sqrt[n]{a})$.*

Beweis. (1) Sei $a \neq 0$. Ist y eine Nullstelle von $T^n - a$, so sind alle Nullstellen von $T^n - a$ von der Form $y\zeta^k$ für eine ganze Zahl k, also ist $K(y) = K(\sqrt[n]{a})$ Zerfällungskörper des Polynoms $T^n - a$, also $K(\sqrt[n]{a})/K$ galoissch. Jedes $\sigma \in \mathrm{Gal}(K(y)/K)$ ist durch das Bild $\sigma(y) = y\zeta^k$, also durch $k \bmod n$ eindeutig bestimmt. Es ist leicht zu sehen, dass damit $\sigma \mapsto k \bmod n$ einen injektiven Gruppenhomomorphismus $\mathrm{Gal}(K(y)/K) \to (\mathbb{Z}/n\mathbb{Z}, +)$ induziert. Daher kann

$\mathrm{Gal}(K(y)/K)$ mit einer Untergruppe der zyklischen Gruppe $\mathbb{Z}/n\mathbb{Z}$ identifiziert werden und ist dann als solche selbst zyklisch.

(2) Sei σ ein erzeugendes Element der Galoisgruppe G. Zu jedem $y \in L$ betrachten wir die sogenannte *Lagrangesche Resolvente*

$$R(\zeta, y) = \sum_{i=0}^{n-1} \zeta^i \sigma^i(y).$$

Behauptung: *Es gibt ein $y \in L$ mit $R(\zeta, y) \neq 0$.*

Nehmen wir das zunächst an. Schreibe $b := R(\zeta, y) \neq 0$. Wegen $\zeta \in K$ gilt $\sigma(\zeta) = \zeta$. Da außerdem $\sigma^n = 1_L$ gilt, folgt

$$\sigma(b) = \sum_{i=0}^{n-1} \zeta^i \sigma^{i+1}(y) = \zeta^{-1} \sum_{i=1}^{n} \zeta^i \sigma^i(y) = \zeta^{-1} b.$$

Es ergibt sich

$$\sigma^i(b) = \zeta^{-i} b$$

für $i = 1, \ldots, n$. Ist nun $\tau = \sigma^i$ ein K-Automorphismus von L, der b festlässt, so folgt wegen $b \neq 0$, dass $\tau = 1_L$ gelten muss. Es ist also $U \stackrel{def}{=} \mathrm{Gal}(L/K(b)) = \{1\}$. Aus dem Hauptsatz der Galoistheorie folgt $K(b) = L^U = L^{\{1\}} = L$. Ferner ist

$$\sigma(b^n) = \sigma(b)^n = \zeta^{-n} b^n = b^n,$$

also $a := b^n \in L^G = K$. Dies bedeutet aber, dass $b = \sqrt[n]{a}$ ein Radikal über K ist, und damit $L = K(b)$ Zerfällungskörper von $T^n - a$ über K. —

Es bleibt obige Behauptung zu beweisen. Es genügt zu zeigen: Sind $a_0, \ldots, a_{n-1} \in L$ und gilt

$$\sum_{i=0}^{n-1} a_i \sigma^i(y) = 0$$

für alle $y \in L$, so gilt $a_0 = a_1 = \cdots = a_{n-1} = 0$. Angenommen, dies ist falsch. Dann sei s die kleinste ganze Zahl, so dass

$$\sum_{i=0}^{s} a_i \sigma^i(y) = 0$$

für alle y gilt mit $a_0, \ldots, a_s$ und mit $a_s \neq 0$. Es gilt offenbar $0 < s < n$. Es können offenbar nicht alle Koeffizienten a_i mit $0 \leq i < s$ verschwinden. Es sei $0 \leq t < s$ die größte ganze Zahl mit $a_t \neq 0$. Wähle ein $z \in L$ mit $\sigma^t(z) \neq \sigma^s(z)$. Dann gilt

$$\sum_{i=0}^{s} a_i \sigma^i(z)\sigma^i(y) = \sum_{i=0}^{s} a_i \sigma^i(zy) = 0$$

und

$$\sum_{i=0}^{s} a_i \sigma^s(z)\sigma^i(y) = 0.$$

Subtraktion ergibt: Für jedes $y \in L$ gilt

$$\sum_{i=0}^{t} a_i \big(\sigma^i(z) - \sigma^s(z)\big)\sigma^i(y) = 0.$$

Wegen $a_t\big(\sigma^t(z) - \sigma^s(z)\big) \neq 0$ ist dies ein Widerspruch zur Minimalität von s. ■

Aufgaben

Ü 2.1. Sei K ein Körper der Charakteristik 0, der eine primitive p-te Einheitswurzel enthält (p prim). Sei $a \in K$. Dann ist das Polynom $T^p - a$ entweder irreduzibel in $K[T]$ oder es zerfällt in $K[T]$ in Linearfaktoren.

Ü 2.2. Seien $n \geq 1$ und K ein Körper, dessen Charakteristik n nicht teilt. Sei $a \in K^\times$ und L Zerfällungskörper von $T^n - a$ über K. Dann enthält L eine primitive n-te Einheitswurzel ζ, und $\mathrm{Gal}(L/K(\zeta))$ ist zyklisch von einer Ordnung, die n teilt.

Ü 2.3. Man zeige, dass die einfachen Radikalerweiterungen, die man mit $\mathbb{Q}(\sqrt[4]{4})$ bezeichnen könnte, nicht alle untereinander isomorph sind.

Ü 2.4. Sei L/K eine zyklische Erweiterung mit $[L : K] = n$. Sei σ ein Erzeuger von $\mathrm{Gal}(L/K)$. Für $x \in L$ definiere die Norm $N(x) = x\sigma(x)\dots\sigma^{n-1}(x)$. Ferner $N_i(x) = x\sigma(x)\dots\sigma^{i-1}(x)$ für $i \geq 0$; also $N(x) = N_n(x)$.

(i) Es gilt $N(xy) = N(x)N(y)$ und $N(x) \in K$.

(ii) [Hilberts Satz 90] Für $\beta \in L$ gilt

$$N(\beta) = 1 \quad \Leftrightarrow \quad \text{es gibt ein } \alpha \in L^\times \text{ mit } \beta = \alpha/\sigma(\alpha).$$

(Hinweis: Gelte $N(\beta) = 1$. Betrachte $\sum_{i=0}^{n-1} N_i(\beta)\sigma^i$ und vgl. obigen Beweis mit der Lagrangeschen Resolvente.)

(iii) Aus der Aussage von Hilberts Satz 90 folgere man Satz 2.3(2).

Ü 2.5. [Kummer-Erweiterungen] Sei $n \geq 1$ und K ein Körper, der eine primitive n-te Einheitswurzel ζ enthält. Seien $a_1, \dots, a_s \in K$, und sei L Zerfällungskörper von $f = \prod_{i=1}^{s}(T^n - a_i)$ und $G = \mathrm{Gal}(L/K)$. Dann gilt:

(i) L/K ist eine abelsche Erweiterung.

(ii) Das kgV aller $\mathrm{ord}(g)$ für $g \in G$ ist ein Teiler von n.

(Hinweis: Sind $\sigma, \tau \in G$, so gilt $\sigma\tau(a_i) = \tau\sigma(a_i)$ für $i = 1, \dots, s$.)

Bemerkung. Es gilt auch die Umkehrung: Sei L/K eine endliche Erweiterung, so dass K eine primitive n-te Einheitswurzel enthält, so dass (i) und (ii) gelten. Dann gibt es $a_1, \dots, a_s \in K$, so dass L Zerfällungskörper von $f = \prod_{i=1}^{s}(T^n - a_i)$ über K ist. — Man nennt Erweiterungen dieses Typs *Kummer-Erweiterungen*. Vgl. etwa Theoreme 23 und 25 in [1], oder Theorem 11.4 in [11].

3. Der Satz über natürliche Irrationalitäten

Der Satz über zyklische Erweiterungen deutet schon an, dass es für gewisse Fragen wichtig sein wird, dass man gewisse Einheitswurzeln zur Verfügung hat und Erweiterungen galoissch sind; falls nicht, muss man passende Elemente hinzuadjungieren. Dies ist in der Tat entscheidend bei Galois' Strategie (Verkleinerung der Galoisgruppe; vgl. die beiden Folgerungen am Ende dieses Abschnitts) zur Untersuchung von Auflösbarkeit von Gleichungen, wie wir im nächsten Abschnitt sehen werden. Dazu ist der folgende Satz ein wichtiges Hilfsmittel.

Satz 3.1 (*Natürliche Irrationalitäten*)

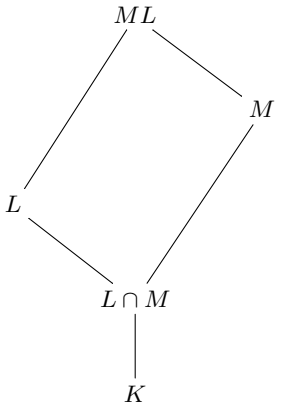
Sei L/K eine endliche Galoiserweiterung, etwa $L = K(\alpha_1, \dots, \alpha_n)$, und M/K eine beliebige Körpererweiterung. Sei $ML = M(L) := M(\alpha_1, \dots, \alpha_n)$ (gebildet in einem gemeinsamen Oberkörper). Dann ist ML/M eine endliche Galoiserweiterung, und die Einschränkung $\sigma \mapsto \sigma_{|L}$ induziert einen Gruppenisomorphismus

$$\theta\colon\ \mathrm{Gal}(ML/M) \xrightarrow{\sim} \mathrm{Gal}(L/L \cap M).$$

Bemerkung. Die Aussage wird manchmal auch *Translationssatz* [7] oder *(Galois') Satz über natürliche Irrationalitäten* [1] genannt. Man nennt den Morphismus θ auch

Translation [3, A.V.70]. Die Bedeutung der Namensgebung "natürliche Irrationalitäten" ist sehr schön im Buch [4] erklärt, Abschnitt 12.2 D.

(3.1)



Beweis. (1) ML/M ist galoissch: L ist Zerfällungskörper eines separablen Polynoms f in $K[T]$, also $L = K(x_1, \ldots, x_n)$, wobei $x_1, \ldots, x_n$ die Nullstellen von f sind. Natürlich gilt $f \in M[T]$, und f ist auch separabel über M. Es ist dann offenbar $ML = M(x_1, \ldots, x_n)$ Zerfällungskörper von f über M.

(2) Sei $\sigma \in \mathrm{Gal}(ML/M)$. Insbesondere ist σ ein K-Automorphismus. Weil L/K normal ist, folgt $\sigma(L) = L$ aus dem Einschränkungssatz. Also ergibt Einschränkung $\sigma \mapsto \sigma_{|L}$ einen Gruppenmorphismus $\mathrm{Gal}(ML/M) \to \mathrm{Gal}(L/K)$. Da σ aber auch die Elemente aus M fix lässt, ist $\sigma_{|L} \in \mathrm{Gal}(L/L \cap M)$. Liegt σ im Kern, also $\sigma_{|L} = 1_L$, so gilt wegen $\sigma_{|M} = 1_M$, dass σ schon die Identität auf ML ist. Wir erhalten damit, dass θ injektiv ist.

(3) θ ist surjektiv: Ist $U = \mathrm{Bild}(\theta)$, so folgt aus dem Hauptsatz $U = \mathrm{Gal}(L/L^U)$. Nach (2) ist klar, dass $L \cap M \subseteq L^U$ gilt. Sei $x \in L^U$. Dann gilt $x \in L$. Für jedes $\sigma \in \mathrm{Gal}(ML/M)$ gilt $\sigma(x) = \sigma_{|L}(x) = x$. Es folgt, da ML/M galoissch ist, $x \in (ML)^{\mathrm{Gal}(ML/M)} = M$. Damit $L^U = L \cap M$, und damit $U = \mathrm{Gal}(L/L \cap M)$. ∎

Folgerung 3.2

Sei L/K endlich galoissch und M/K eine beliebige Körpererweiterung. Dann ist $[ML : M]$ ein Teiler von $[L : K]$.

Bemerkung. In der Situation des Satzes ist L Zerfällungskörper eines (separablen) Polynoms $f \in K[T]$. Definiere Ω als Zerfällungskörper von f über M. Also $\Omega = M(\beta_1, \ldots, \beta_n)$, wobei die β_i die Nullstellen von f in Ω sind. Es ist Ω/M eine (endliche Galois-) Erweiterung. Es ist $L' := K(\beta_1, \ldots, \beta_n) \subseteq \Omega$ ein Zwischenkörper von Ω/K, der offenbar ein Zerfällungskörper von f über K ist. Wir können also L durch einen K-isomorphen Körper L' ersetzen und erhalten, dass es zu L' und M einen gemeinsamen Oberkörper Ω gibt. Ohne Einschränkung können wir das dann auch gleich für L und M annehmen (und so konstruiert ist dann $\Omega = ML$).

Definition 3.3 (*Galoisgruppe eines Polynoms*)

Sei K ein Körper und $f \in K[T]$ ein separables Polynom. (Im Fall $\mathrm{Char}(K) = 0$ ist die Separabilität automatisch.) Sei L ein Zerfällungskörper von f über K. Es ist L/K eine endliche Galoiserweiterung. Sei $\mathrm{Gal}(f/K) \stackrel{def}{=} \mathrm{Gal}(L/K)$, die *Galoisgruppe* von f *über* K.

Wegen der Eindeutigkeit eines Zerfällungskörpers bis auf K-Isomorphie, ist die Galoisgruppe $\mathrm{Gal}(f/K)$ (bis auf Isomorphie) eindeutig bestimmt.

Folgerung 3.4 (*Galois*)

Sei L Zerfällungskörper eines separablen Polynoms f über K. Sei t Nullstelle eines Polynoms $g \in K[T]$. Dann kann $G' = \mathrm{Gal}(f/K(t))$ identifiziert werden

mit einer Untergruppe von $G = \mathrm{Gal}(f/K)$. Ist g irreduzibel vom Grad m, so ist der Index $[G : G']$ ein Teiler von m.

Denn der Index ist $[L \cap K(t) : K]$, ein Teiler von $[K(t) : K] = m$. Werden alle Nullstellen von g hinzuadjungiert, so erhält man einen Normalteiler:

Folgerung 3.5 (*Galois*)

Mit den Bezeichnungen der vorherigen Folgerung: ist M Zerfällungskörper von g über K, so ist $\mathrm{Gal}(f/M)$ ein Normalteiler von $\mathrm{Gal}(f/K)$.

Beweis. Die Körpererweiterung $L \cap M/K$ hat ein primitives Element u; dessen Minimalpolynom zerfällt sowohl über L wie über M, da beide normale Erweiterungen von K sind. Es folgt, dass $L \cap M = K(u)/K$ normal ist. ∎

Bemerkung. Die wichtigsten Anwendungsfälle der beiden letzten Folgerungen sind Adjunktion (1) von primitiven Einheitswurzeln und (2) von Radikalen, sowie der Spezialfall $m = p$ prim (wir nehmen $\mathrm{Char}(K) = 0$ an):

(1) $g = (T^p - 1)/(T - 1) \in K[T]$, p prim. Falls g irreduzibel über K ist, so ist $m = p - 1$.

(2) $g = T^p - a \in K[T]$, p prim. Hier ist g irreduzibel über K, falls a nicht selbst schon eine p-te Potenz eines Elements in K ist (vgl. Ü 3.1 in Kapitel VIII), und dann ist $m = p$. Enthält K schon eine primitive p-te Einheitswurzel (was man durch vorherige Anwendung von (1) erreichen kann), so liegen alle Nullstellen von g in $K(\sqrt[p]{a})$ (und die Irreduzibilität von g folgt aus Satz 2.3(1)). Dann ist $\mathrm{Gal}(f/K(\sqrt[p]{a}))$ ein Normalteiler von $\mathrm{Gal}(f/K)$ vom Index 1 oder p. (Nur im Fall $= p$ hat man etwas gewonnen.)

Erhält man im Schritt (2) einen echten Normalteiler, so setzt man das Verfahren iterativ fort, bis man (falls möglich) $\mathrm{Gal}(f/K') = \{1\}$ erhält, wobei K' durch Hinzufügung endlich vieler Radikale bzw. Einheitswurzeln aus K hervorgeht. Gelingt dies, so zerfällt f über K' in Linearfaktoren, und alle Nullstellen von f lassen sich aus bekannten Größen und Radikalen davon darstellen. Vgl. die Definitionen und das Vorgehen im nächsten Abschnitt.

Aufgaben

Ü 3.1. [Galois] Sei K ein Körper, der eine primitive p-te Einheitswurzel enthält (p prim). Sei $f \in K[T]$ ein irreduzibles, separables Polynom vom Grad p. Sei $K' = K(\sqrt[p]{a})$ eine einfache Radikalerweiterung (mit $a \in K$). Dann gilt:

Über K' ist f entweder weiterhin irreduzibel oder es zerfällt vollständig in Linearfaktoren.

Ü 3.2. Sei K ein Körper und $f \in K[T]$ ein separables Polynom mit $\mathrm{grad}(f) \geq 1$. Sei K'/K eine endliche Erweiterung. Dann gilt:

$$f \text{ zerfällt über } K' \text{ in Linearfaktoren} \quad \Leftrightarrow \quad \mathrm{Gal}(f/K') = \{1\}.$$

4. Auflösbarkeit von Gleichungen. Galois' Kriterium

Wir nehmen im folgenden der Einfachheit halber an, dass alle vorkommenden Körper die Charakteristik 0 haben. Insbesondere ist dann jedes über K algebraische Element separabel.

Definition 4.1

Eine Körpererweiterung L/K heißt *Radikalerweiterung* (oder nur *radikal*), falls es einen Körperturm

$$K = K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_{n-1} \subseteq K_n = L \tag{4.1}$$

gibt, so dass K_i/K_{i-1} eine einfache Radikalerweiterung ist für jedes $i = 1, \dots, n$. Wir nennen (4.1) auch einen *Radikalturm* für L/K. Eine Körpererweiterung L/K heisst *auflösbar* (durch Radikale), falls es eine Erweiterung M/L gibt, so dass M/K radikal ist.

Definition 4.2

Sei $f \in K[T]$. Die Gleichung $f(x) = 0$ heißt *auflösbar* (durch Radikale; über K), falls der Zerfällungskörper von f eine auflösbare Erweiterung von K ist.

Beispiele. (1) ("p-q-Formel"; "quadratische Ergänzung") Sei $f = T^2 + pT + q \in K[T]$. (Die Normierung stellt keine Einschränkung dar.) Die Nullstellen lassen sich in einem Zerfällungskörper L über K beschreiben als $x = -p/2 \pm \sqrt{p^2/4 - q}$. Es ist also $L = K\big(\sqrt{p^2/4 - q}\big)$ (es wird nur $\mathrm{Char}(K) \neq 2$ benötigt), und dies ist eine Radikalerweiterung. Es ist also die Gleichung $f(x) = 0$ auflösbar. In Babylonien waren Lösungsformeln quadratischer Gleichungen schon vor mehr als 3500 Jahren bekannt.

(2) (Cardanische Formeln; Cardano 1545, Tartaglia um 1535, del Ferro 1515) Sei $f = T^3 + aT^2 + bT + c \in \mathbb{Q}[T]$. Durch Substitution $T = T - \frac{a}{3}$ bekommt man ein Polynom

$$f = T^3 + pT + q$$

mit rationalen Koeffizienten. Es genügt, die Nullstellen für solch ein Polynom zu bestimmen. Die 3 Nullstellen x, y und z dieses Polynoms sind gegeben durch $x = a+b$, $y = \varepsilon^2 a + \varepsilon b$, $z = \varepsilon a + \varepsilon^2 b$, wobei

$$a = \sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}\,, \quad b = -\frac{p}{3a} \quad \text{und} \quad \varepsilon = -\frac{1}{2} + \frac{1}{2}i\sqrt{3}.$$

Man sieht, dass der Zerfällungskörper $L = \mathbb{Q}(x, y, z)$ von f in einer Radikalerweiterung liegt:

$$\mathbb{Q} \subset \mathbb{Q}(a_1) \subset \mathbb{Q}(a_1, a_2) \subset \mathbb{Q}(a_1, a_2, a_3)$$

mit

$$a_1 = \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3},\ a_2 = \sqrt[3]{-\frac{q}{2} + a_1},\ a_3 = \varepsilon,$$

und es gilt $L \subset \mathbb{Q}(a_1, a_2, a_3)$.

(3) Auch für Polynome f vom Grad 4 über $\mathbb{Q}$ gibt es Formeln, die zeigen, dass die Gleichung $f(x) = 0$ durch Radikale auflösbar ist. (Ferrari 1540.)

Es wird sich zeigen, dass dies allgemein für Polynome vom Grad ≥ 5 (über $\mathbb{Q}$) nicht mehr richtig ist. Dies geht auf Abel (1824/26) und Ruffini (1799/1813) zurück. Etwas später hat Galois mit Satz 4.5 (der den Hauptsatz der Galoistheorie verwendet) die Thematik wesentlich eleganter und systematischer gelöst.

Um dieses Problem dem Hauptsatz der Galoistheorie zugänglich zu machen, benötigen wir die nachfolgende wichtige Proposition. Zuvor ein paar einfache Invarianzeigenschaften für Radikalerweiterungen:

Lemma 4.3

(1) [Transitivität] *Sind L/K und M/L radikal, so ist auch M/K radikal.*
(2) [Translation] *Seien L/K und M/K Erweiterungen, die beide in einem gemeinsamen Oberkörper liegen. Ist L/K radikal, so auch ML/M. (Vgl. Diagramm (3.1).)*
(3) [Kompositum] *Liegen L und M in einem gemeinsamen Oberkörper, und sind L/K und M/K radikal, so ist auch ML/K radikal.*
(4) [Konjugation] *Sei M/K endlich, sei L ein Zwischenkörper und $\sigma \in \mathrm{Gal}(M/K)$. Ist L/K radikal, so auch $\sigma(L)/K$.*

Beweis. (1) ist trivial.

(2) Ist (4.1) ein Radikalturm für L/K, so ist $\ldots \subseteq MK_{i-1} \subseteq MK_i \subseteq \ldots$ ein solcher für ML/M. Denn aus $K_i = K_{i-1}(a_i)$ mit ${a_i}^{n_i} = b_i \in K_{i-1}$ folgt $MK_i = MK_{i-1}(a_i)$ mit ${a_i}^{n_i} = b_i \in K_{i-1} \subseteq MK_{i-1}$.

(3) folgt sofort aus (1) und (2).

(4) Es genügt, dies für jeden Schritt in einem Körperturm (4.1) zu zeigen: ist $K_i = K_{i-1}(a_i)$ mit ${a_i}^{n_i} = b_i \in K_{i-1}$, so ist $\sigma(K_i) = \sigma(K_{i-1})(\sigma(a_i))$ und $\sigma(a_i)^{n_i} = \sigma(b_i) \in \sigma(K_{i-1})$. ∎

Proposition 4.4

Es gelte $\mathrm{Char}(K) = 0$. *Jede Radikalerweiterung L/K ist in einer galoisschen Radikalerweiterung N/K enthalten.*

Beweis. Genauer: der normale Abschluss N von L/K ist eine Radikalerweiterung. Dies folgt sofort aus dem Lemma zusammen mit Proposition VI.6.6. ∎

Satz 4.5 (*Auflösbarkeitskriterium (Galois 1831)*)

Sei K ein Körper mit $\mathrm{Char}(K) = 0$. *Sei $f \in K[T]$. Genau dann ist die Gleichung $f(x) = 0$ durch Radikale auflösbar, wenn die Gruppe* $\mathrm{Gal}(f/K)$ *auflösbar ist.*

Beweis. (1) "⇒". Sei zunächst die Gleichung $f(x) = 0$ auflösbar. Sei M Zerfällungskörper von f über K. Dieser ist nach der Proposition in einer galoisschen Radikalerweiterung L/K enthalten. Da M/K als Zerfällungskörper normal ist, hat man nach dem Hauptsatz der Galoistheorie eine Isomorphie von Gruppen $\mathrm{Gal}(M/K) \simeq \mathrm{Gal}(L/K)/\mathrm{Gal}(L/M)$. Es gibt also einen surjektiven Gruppenhomomorphismus $\pi\colon \mathrm{Gal}(L/K) \to \mathrm{Gal}(M/K)$. Es genügt daher nach Satz III.7.3 zu zeigen, dass $\mathrm{Gal}(L/K)$ auflösbar ist.

Es gibt einen Körperturm

$$K = L_0 \subseteq L_1 \subseteq \cdots \subseteq L_{s-1} \subseteq L_s = L$$

mit $L_i = L_{i-1}(a_i)$ und ${a_i}^{n_i} \in L_{i-1}$ für eine natürliche Zahl $n_i \geq 2$ $(i = 1, \ldots, s)$. Sei $n = n_1 n_2 \ldots n_s$. Definiere $K' = E_n(K)$, $L'_i = E_n(L_i)$ $(i = 1, \ldots, n)$, $L' = E_n(L)$. Offenbar kann man dabei $L'_{i-1} \subseteq L'_i$ annehmen. Es enthält K', insbesondere L'_{i-1}, eine primitive n_i-te Einheitswurzel (vgl. Ü 1.4). Man erhält einen Körperturm

$$K' = L'_0 \subseteq L'_1 \subseteq \cdots \subseteq L'_{s-1} \subseteq L'_s = L'.$$

Hierbei ist jedes L'_i/L'_{i-1} eine einfache Radikalerweiterung. Ist L Zerfällungskörper eines Polynoms g über K, so ist L' Zerfällungskörper von $g \cdot (T^n - 1)$ über K, also ist L'/K galoissch. Da auch L/K galoissch ist, gilt nach dem Hauptsatz der Galoistheorie, dass $\mathrm{Gal}(L'/L)$ ein Normalteiler in $\mathrm{Gal}(L'/K)$ ist und

$$\mathrm{Gal}(L/K) \simeq \mathrm{Gal}(L'/K)/\mathrm{Gal}(L'/L)$$

ist als homomorphes Bild von $\mathrm{Gal}(L'/K)$ auflösbar, wenn gezeigt wird, dass $\mathrm{Gal}(L'/K)$ auflösbar ist.

Es ist $\mathrm{Gal}(K'/K)$ als Untergruppe von $E(\mathbb{Z}/n\mathbb{Z})$ (Satz 1.3) abelsch, also auflösbar. Ebenso folgt aus dem Hauptsatz

$$\mathrm{Gal}(K'/K) \simeq \mathrm{Gal}(L'/K)/\mathrm{Gal}(L'/K'),$$

und daher genügt zu zeigen, dass $G := \mathrm{Gal}(L'/K')$ auflösbar ist.

Für $j = 0, \ldots, s$ sei $U_j = \mathrm{Gal}(L'/L'_j)$. Der Vorteil ist nun, dass durch das Vorhandensein der n_i-ten Einheitswurzeln die Erweiterungen L'_i/L'_{i-1} galoissch sind mit zyklischen (insbesondere abelschen) Galoisgruppen nach Satz 2.3 (1). Mit dem Hauptsatz (beide Teile) bekommen wir daher eine Normalreihe

$$G = U_0 \rhd U_1 \rhd \ldots \rhd U_{s-1} \rhd U_s = \{1\}$$

mit zyklischen Faktoren $U_{j-1}/U_j \simeq \mathrm{Gal}(L'/L'_{j-1})/\mathrm{Gal}(L'/L'_j) \simeq \mathrm{Gal}(L'_j/L'_{j-1})$. Also ist G auflösbar.

(2) "⇐". Sei L Zerfällungskörper von f über K und $n = [L : K]$. Sei $\mathrm{Gal}(L/K)$ auflösbar. Setze $K' = E_n(K)$ und $L' = E_n(L)$, wobei L' als Erweiterungskörper von K' aufgefasst werden kann. Als Zerfällungskörper des Polynoms $f \cdot (T^n - 1)$ über K ist L' über K galoissch. Zu zeigen genügt, dass L'/K eine Radikalerweiterung ist.

Nach Satz 3.1 über natürliche Irrationalitäten ist $\mathrm{Gal}(L'/K') \to \mathrm{Gal}(L/K)$, $\sigma \mapsto \sigma_{|L}$ ein injektiver Gruppenmorphismus. Es ist also mit $\mathrm{Gal}(L/K)$ auch die (eingebettete) Untergruppe $\mathrm{Gal}(L'/K')$ auflösbar, und L'/K' ist galoissch mit $n' = [L' : K']$ ein Teiler von n. Damit enthält K' eine primitive n'-te Einheitswurzel (vgl. Ü 1.4). Zu zeigen genügt, dass L'/K' eine Radikalerweiterung ist. Da K'/K eine Radikalerweiterung ist, folgt dies dann auch für L'/K.

Wir zeigen nun generell:

Ist L'/K' endlich galoissch mit $\mathrm{Gal}(L'/K')$ auflösbar, und enthält K' eine n'-te primitive Einheitswurzel, so ist L'/K' eine Radikalerweiterung.

Da $G = \mathrm{Gal}(L'/K')$ auflösbar ist, gibt es nach Satz III.7.5 eine prim-zyklische Normalreihe

$$\{1\} = U_0 \lhd U_1 \lhd \ldots \lhd U_{t-1} \lhd U_t = G,$$

so dass also die Faktoren U_j/U_{j-1} zyklisch von Primzahlordnung q_j sind. Dabei gilt $n' = q_1 \ldots q_t$. Also enthält K' alle q_j-ten Einheitswurzeln (Ü 1.4). Übergang zu den Fixkörpern liefert nach dem Hauptsatz der Galoistheorie einen Körperturm

$$K' = K'_t \subset K'_{t-1} \subset \ldots \subset K'_1 \subset K'_0 = L'.$$

Dabei ist jede Erweiterung K'_{j-1}/K'_j galoissch (denn $\mathrm{Gal}(L'/K'_{j-1}) = U_{j-1}$ ist Normalteiler in $U_j = \mathrm{Gal}(L'/K'_j)$) mit zyklischer Galoisgruppe

$$\mathrm{Gal}(K'_{j-1}/K'_j) \simeq U_j/U_{j-1}$$

von Primzahlordnung q_j. Aus Satz 2.3 (2) folgt, dass $K'_{j-1} = K'_j(a_j)$ für ein $a_j \in K'_{j-1}$ und ${a_j}^{q_j} \in K'_j$. Also ist L'/K' eine Radikalerweiterung. ∎

Bemerkung. Der vorstehende Beweis mag auf den ersten Blick relativ lang und kompliziert erscheinen. Die Länge entsteht nur durch die vielen Reduktionen, die vorgenommen werden, um eine bessere Situation auf Seite der Körpererweiterungen zu haben (galoissch, Vorhandensein von Einheitswurzeln). Dazu muss man gewährleisten, dass die entsprechenden Modifikationen auf Gruppenseite mit der Fragestellung kompatibel sind. Dies geschieht durch den Hauptsatz VI.9.2 und Satz III.7.3, sowie mit dem Satz über natürliche Irrationalitäten. Sieht man von all diesen Reduktionen ab, so bleibt nur noch folgende Aussage übrig.

Sei L/K eine Galoiserweiterung mit $[L : K] = n$, so dass K eine primitive n-te Einheitswurzel enthält. Dann gilt:

$$L/K \text{ Radikalerweiterung} \quad \Leftrightarrow \quad \mathrm{Gal}(L/K) \text{ auflösbar.}$$

Per Induktion wird diese Aussage weiter reduziert auf:

(1) L/K *einfache Radikalerweiterung* $\Rightarrow$ $\mathrm{Gal}(L/K)$ *auflösbar.*

(2) $\mathrm{Gal}(L/K)$ *der Ordnung $n = p$ prim* $\Rightarrow$ L/K *einfache Radikalerweiterung.*

Diese Aussagen folgen unmittelbar aus den jeweiligen Teilen von Satz 2.3. (Die Reduktion auf (2) folgt mit Satz III.7.5.) Man kann also sagen, dass Satz 4.5 vollständig reduziert wird auf Satz 2.3.

Bemerkung. Das Auflösbarkeitskriterium Satz 4.5 formulierte Galois in seiner grundlegenden Arbeit nicht explizit als Satz/Theorem, sondern beschrieb es als Vorgehensweise in einem längeren Text[1]. Die Hauptargumente waren auch damals schon: Hinzuadjungieren von Einheitswurzeln, im wesentlichen Satz 2.3 (zumindestens für $n = p$ prim), sukzessives Reduzieren der Gruppengröße. — Galois' "eigentliches" Hauptresultat in der Arbeit waren die Sätze in Abschnitt VIII.2, insbesondere Satz VIII.2.3. Siehe [**12**] oder [**5**] für die Originaltexte.

[1] Neumann [**12**], Seite 121 ff., "Proposition V"'.

Aufgaben

Ü 4.1. In der Situation von Satz 3.1 gilt: ist L/K auflösbar, so ist auch ML/M auflösbar.

Ü 4.2. Sei $L \supseteq M \supseteq K$ ein Körperturm endlicher Erweiterungen. Es ist L/K auflösbar genau dann, wenn L/M und M/K beide auflösbar sind.

Ü 4.3. Sei L/K galoissch mit $n = [L : K]$, und K enthalte eine primitive n-te Einheitswurzel. Es ist L/K radikal genau dann, wenn L/K auflösbar ist.

5. Nichtauflösbare Gleichungen

Sei $f \in K[T]$ separabel. Seien $a_1, \ldots, a_m$ die verschiedenen Nullstellen von f in einem Zerfällungskörper L. Für jedes $\sigma \in \mathrm{Gal}(f/K)$ gilt $\sigma(\{a_1, \ldots, a_m\}) = \{a_1, \ldots, a_m\}$, d. h. σ ist eine Permutation der Elemente $a_1, \ldots, a_m$. Offenbar lässt nur $\sigma = 1_L$ alle a_i fest. Man erhält damit einen injektiven Gruppenhomomorphismus $\mathrm{Gal}(f/K) \to \mathbb{S}(X) = \mathbb{S}_m$, in die symmetrische Gruppe der Menge $X = \{a_1, \ldots, a_m\}$.

Proposition 5.1

Ist $f \in K[T]$ irreduzibel (ohne Einschränkung normiert), so operiert $\mathrm{Gal}(f/K)$ transitiv *auf der Menge X, d. h. sind a_i, $a_j \in X$, so gibt es ein $\sigma \in \mathrm{Gal}(f/K)$ mit $\sigma(a_i) = a_j$.*

Beweis. Es ist f das Minimalpolynom sowohl von a_i als auch von a_j, und die Aussage ergibt sich aus Satz V.2.4 und Satz VI.2.3. ∎

Zunächst das "positive" Ergebnis:

Proposition 5.2

Sei K ein Körper der Charakeristik 0 und $f \in K[T]$ ein Polynom vom Grad ≤ 4. Dann ist die Gleichung $f(x) = 0$ durch Radikale auflösbar.

Beweis. $G = \mathrm{Gal}(f/K)$ ist zu einer Untergruppe der symmetrischen Gruppe $\mathbb{S}_n$ mit $n \leq 4$ isomorph. Die $\mathbb{S}_n$ für $n \leq 4$ sind auflösbar. Es ist etwa

$$\{e\} \lhd \mathbb{V}_4 \lhd \mathbb{A}_4 \lhd \mathbb{S}_4$$

eine abelsche Normalreihe für $\mathbb{S}_4$; hierbei ist $\mathbb{V}_4 \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$ die Gruppe, die erzeugt wird von den Produkten je zwei disjunkter Transpositionen. ∎

Ziel des Abschnitts ist der folgende Satz.

Satz 5.3

Sei p eine Primzahl und $f \in \mathbb{Q}[T]$ irreduzibel und vom Grad p. Es habe f genau zwei nicht-reelle Nullstellen. Dann ist $\mathrm{Gal}(f/\mathbb{Q}) \simeq \mathbb{S}_p$. *Für $p \geq 5$ ist insbesondere die Gleichung $f(x) = 0$ nicht durch Radikale auflösbar.*

Folgerung 5.4

Sei $f = T^5 - 6T + 3 \in \mathbb{Q}[T]$. Dann ist die Gleichung $f(x) = 0$ nicht auflösbar.

Beweis. Das Polynom ist irreduzibel nach Eisenstein und hat genau zwei nicht-reelle Nullstellen (Übung 5.3). ∎

Lemma 5.5

Die symmetrische Gruppe $\mathbb{S}_n$ ($n \geq 2$) wird von der Transposition $\tau = (1\ 2)$ und dem n-Zykel $\sigma = (1\ 2\ \ldots\ n)$ erzeugt.

Beweis. Sei G die Untergruppe von $\mathbb{S}_n$, die von σ und τ erzeugt wird. Dann enthält G auch

$$\sigma\tau\sigma^{-1} = (2\ 3),\ \sigma^2\tau\sigma^{-2} = (3\ 4),\ \ldots,$$

also alle Transpositionen der Form $(i\ i+1)$. Aber dann enthält G auch die Transpositionen

$$(1\ 2)(2\ 3)(1\ 2) = (1\ 3),\ (1\ 3)(3\ 4)(1\ 3) = (1\ 4),\ \ldots,$$

also alle Transpositionen der Form $(1\ i)$. Aber dann enthält G auch eine beliebige Transposition $(i\ j) = (1\ i)(1\ j)(1\ i)$. Da jede Permutation in $\mathbb{S}_n$ ein Produkt von Transpositionen ist, folgt $G = \mathbb{S}_n$. ∎

Beweis von Satz 5.3. Wegen Charakteristik 0 hat f genau p verschiedene Nullstellen $x_1, x_2, \ldots, x_p$ im Zerfällungskörper $L \subseteq \mathbb{C}$. Es ist $[\mathbb{Q}(x_1) : \mathbb{Q}] = p$. Die Ordnung der Gruppe $G = \mathrm{Gal}(f/\mathbb{Q})$ ist also ein Vielfaches von p. Wie oben beschrieben kann man G als Untergruppe von $\mathbb{S}_p$ auffassen. Nach dem Satz von Cauchy hat G ein Element σ der Ordnung p. Die einzigen Elemente der Ordnung p in $\mathbb{S}_p$ sind p-Zykel. Sind etwa x_1 und x_2 die nicht-reellen Nullstellen, so gilt $x_2 = \overline{x_1}$. Da $L/\mathbb{Q}$ normal ist, folgt aus Satz VI.6.5, dass komplexe Konjugation einen $\mathbb{Q}$-Automorphismus $\tau\colon L \to L$ induziert, also ein Element der Ordnung 2, welches der Transposition $\tau = (1\ 2)$ entspricht. Nach evtl. Potenzierung von σ und Umnummerierung der reellen Nullstellen $x_3, \ldots, x_p$ kann man annehmen, dass σ der p-Zykel $\sigma = (1\ 2\ \ldots\ p)$ ist. Nach dem vorherigen Lemma folgt dann aber $G = \mathbb{S}_p$. Wir haben früher gesehen, dass $\mathbb{S}_p$ für $p \geq 5$ nicht auflösbar ist (Satz III.7.4). ∎

Aufgaben

Ü 5.1. Sei $f \in K[T]$ separabel mit mindestens zwei nicht zueinander assoziierten irreduziblen Faktoren. Dann ist die in Proposition 5.1 beschriebene Operation nicht transitiv.

Ü 5.2. Sei $f \in K[T]$ separabel. Seien $\alpha_1, \ldots, \alpha_n$ die verschiedenen Nullstellen (im Zerfällungskörper). Gilt $\mathrm{Gal}(f/K) \simeq \mathbb{S}_n$, so folgt $\mathrm{Gal}(f/K(\alpha_1)) \simeq \mathbb{S}_{n-1}$.

Ü 5.3. Das Polynom $f = T^5 - 6T + 3 \in \mathbb{C}[T]$ hat genau zwei nicht-reelle Nullstellen.

6. Kreisteilungspolynome

Wir betrachten nun alles über $\mathbb{Q}$ bzw. in $\mathbb{C}$.

Definition 6.1

Das n-te *Kreisteilungspolynom* $\Phi_n \in \mathbb{C}[T]$ ist definiert durch

$$\Phi_n = \prod_{\zeta} (T - \zeta),$$

wobei ζ die primitiven n-ten Einheitswurzeln in $\mathbb{C}$ durchläuft.

Dies ist ein normiertes Polynom vom Grad $\varphi(n)$.

Sei $\zeta \in \mathbb{C}$ eine n-te Einheitswurzel. Dann ist für genau einen Teiler d von n (innerhalb der natürlichen Zahlen) ζ eine *primitive* d-te Einheitswurzel. Umgekehrt, jede (primitive) d-te Einheitswurzel, wobei d ein Teiler von n ist, ist auch n-te Einheitswurzel. Man erhält also

$$T^n - 1 = \prod_{\zeta \in \mu_n(\mathbb{C})} (T - \zeta) = \prod_{d|n} \Phi_d. \tag{6.1}$$

Proposition 6.2

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

Beweis. Induktion nach n. Für $n = 1$ ist $\Phi_1 = T-1 \in \mathbb{Z}[T]$. Sei nun $n > 1$. Dann gilt $T^n - 1 = f \cdot \Phi_n$ in $\mathbb{C}[T]$, wobei $f = \prod_{d|n,\, d\neq n} \Phi_d$. Nach Induktionsvoraussetzung gilt $f \in \mathbb{Z}[T]$, und f ist normiert. Polynomdivision mit Rest liefert eindeutig bestimmte q, $r \in \mathbb{Z}[T]$ mit $T^n - 1 = fq + r$ mit $r = 0$ oder $\operatorname{grad}(r) < \operatorname{grad}(f)$. Man erhält $r = f(\Phi_n - q)$. Aus Gradgründen ergibt sich $\Phi_n = q$. ∎

Bemerkung. Die Formel $T^n - 1 = \prod_{d|n} \Phi_d$ erlaubt eine rekursive Berechnung der Kreisteilungspolynome Φ_n. Es ist $\Phi_1 = T - 1$. Für eine Primzahl p gibt sich wegen $T^p - 1 = \Phi_1\Phi_p = (T-1) \cdot \Phi_p$ nochmal die aus den Übungen bekannte Aussage

$$\Phi_p = T^{p-1} + T^{p-2} + \cdots + T + 1.$$

Aus $T^4 - 1 = \Phi_1\Phi_2\Phi_4$ folgt $\Phi_4 = T^2 + 1$. Aus $T^6 - 1 = \Phi_1\Phi_2\Phi_3\Phi_6$ folgt $\Phi_6 = (T^6 - 1)/(T^4 + T^3 - T - 1) = T^2 - T + 1$, u.s.w.

Satz 6.3 (*Gauß (1801/08)*)

Das n-te Kreisteilungspolynom Φ_n ist irreduzibel über $\mathbb{Q}$.

Beweis. Es genügt zu zeigen, dass Φ_n in $\mathbb{Z}[T]$ irreduzibel ist. Sei $f \in \mathbb{Z}[T]$ ein (normierter) irreduziber Faktor. Zu zeigen genügt, dass f denselben Grad wie Φ_n hat.

Sei x eine Nullstelle von f in $E_n(\mathbb{Q})$. Dann ist x (als Nullstelle von Φ_n) eine primitive n-te Einheitswurzel. Es genügt zu zeigen, dass alle primitiven n-ten Einheitswurzeln Nullstellen von f sind, denn dann ist $\operatorname{grad}(f) = \varphi(n) = \operatorname{grad}(\Phi_n)$. Die primitiven n-ten Einheitswurzeln sind von der Form x^k wobei $1 \leq k < n$ teilerfremd zu n ist. Es genügt zu zeigen: Ist p prim und teilerfremd zu n, so ist x^p eine Nullstelle von f. Denn ist k eine beliebige zu n teilerfremde Zahl, so zerlegt man $k = p_1 \dots p_r$ in Primfaktoren, und es ist für $1 \leq j \leq r$ auch $x^{p_1 \cdots p_j}$ eine primitive n-te Einheitswurzel, und man schließt sukzessive

$$0 = f(x) = f(x^{p_1}) = f((x^{p_1})^{p_2}) = f(x^{p_1 p_2}) = \cdots = f(x^k).$$

Sei also p prim, teilerfremd zu n. Wir nehmen an, dass $f(x^p) \neq 0$ und wollen das zum Widerspruch führen. Es ist f als Teiler von Φ_n auch ein Teiler von $T^n - 1$ in $\mathbb{Z}[T]$. Es gibt also ein $g \in \mathbb{Z}[T]$ mit $T^n - 1 = fg$. Es ist x^p eine n-te Einheitswurzel, und aus unserer Annahme folgt $g(x^p) = 0$. Es ist also x eine Nullstelle des Polynoms $g(T^p) \in \mathbb{Z}[T]$. Da f das Minimalpolynom von x über $\mathbb{Q}$ ist, folgt, dass f ein Teiler von $g(T^p)$ in $\mathbb{Q}[T]$ ist, etwa $g(T^p) = fh$ für ein $h \in \mathbb{Q}[T]$. Da f normiert ist, kann man in $\mathbb{Z}[T]$ auch durch f mit Rest dividieren, und da dies dann auch in $\mathbb{Q}[T]$ gilt, folgt aus Eindeutigkeitsgründen, dass $h \in \mathbb{Z}[T]$ gilt.

Betrachte nun die kanonischen Surjektion $\nu\colon \mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$, $x \mapsto \overline{x} \stackrel{def}{=} x \bmod n$. Dies ergibt den Homomorphismus $\nu^*\colon \mathbb{Z}[T] \to \mathbb{F}_p[T]$, $f \mapsto \overline{f}$. Wir erhalten

$$\overline{f} \cdot \overline{h} = \overline{g(T^p)} = \overline{g}^p.$$

Sei nun $\overline{f}_0$ ein irreduzibler Faktor von $\overline{f}$ in $\mathbb{F}_p[T]$. Dann ist $\overline{f}_0$ auch ein irreduzibler Faktor von $\overline{g}$, und aus der Darstellung $\overline{T^n - 1} = \overline{f} \cdot \overline{g}$ folgt, dass $\overline{f}_0^2$ ein Teiler von $\overline{T^n - 1} = T^n - \overline{1}$ ist. Damit hat $T^n - \overline{1}$ eine mehrfache Nullstelle (in einem Zerfällungskörper). Andererseits ist $D(T^n - \overline{1}) = \overline{n}T^{n-1} \neq 0$ (da p kein Teiler von n ist), also teilerfremd zu $T^n - \overline{1}$, Widerspruch. ∎

Folgerung 6.4

$[E_n(\mathbb{Q}) : \mathbb{Q}] = \varphi(n)$.

Beweis. Es ist $E_n(\mathbb{Q}) = \mathbb{Q}(\zeta)$, wobei ζ eine primitive n-te Einheitswurzel ist. Das Minimalpolynom von ζ ist Φ_n (nach dem Satz), und $\operatorname{grad}(\Phi_n) = \varphi(n)$. ∎

Folgerung 6.5

Es ist $\mathrm{Gal}(E_n(\mathbb{Q})/\mathbb{Q}) \simeq E(\mathbb{Z}/n\mathbb{Z})$, *also insbesondere abelsch.*

Beweis. Nach Satz 1.3 haben wir einen injektiven Homomorphismus $\mathrm{Gal}(E_n(\mathbb{Q})/\mathbb{Q}) \to E(\mathbb{Z}/n\mathbb{Z})$. Da beide Gruppen dieselbe Ordnung $\varphi(n)$ haben, ist dies ein Isomorphismus. ∎

Bemerkung. Gauß bewies den Satz um 1801 im Falle, dass $n = p$ prim ist. Später vereinfachten (unabhängig voneinander) Eisenstein und Schönemann den Beweis drastisch[2]. Vgl. Ü IV.7.1. Gauß notierte 1808 in seinem Tagebuch, dass er den Satz nun auch für beliebige n bewiesen hätte. Leider ist der Beweis verschollen. (Vgl. [4].) Publiziert wurde ein Beweis zuerst 1854 von Kronecker. Die oben dargestellte Argumentation geht im wesentlichen auf Dedekind (1857) zurück.

Aufgaben

Ü 6.1. Sei $K = \mathbb{Q}$.

(1) Man berechne die Kreisteilungspolynome $\Phi_{27}(T)$ und $\Phi_{32}(T)$.

(2) Es gilt $\Phi_2(T) = -\Phi_1(-T)$.

(3) Sei $n > 1$ ungerade. Dann gilt $\Phi_{2n}(T) = \Phi_n(-T)$. (Hinweis: $T^{2n} - 1 = (T^n - 1)(T^n + 1)$.)

(4) Sei p eine Primzahl, die n nicht teilt. Dann gilt

$$\Phi_{pn}(T) = \frac{\Phi_n(T^p)}{\Phi_n(T)}.$$

(5) Man berechne $\Phi_{54}(T)$ und $\Phi_{96}(T)$.

Ü 6.2. Sei $K = \mathbb{Q}$, sei p eine Primzahl und $r \geq 1$ eine natürliche Zahl.

(1) $\Phi_{p^r}(T) = \dfrac{T^{p^r} - 1}{T^{p^{r-1}} - 1}$.

(2) *Ohne* Verwendung von Satz 6.3 zeige, dass $\Phi_{p^r}(T)$ irreduzibel über $\mathbb{Q}$ ist. (Aus (1) mit $T \mapsto T + 1$ und dem Kriterium von Eisenstein.)

Ü 6.3. Sei G eine endliche zyklische Gruppe. Dann gibt es eine (endliche) Galoiserweiterung $L/\mathbb{Q}$, so dass $\mathrm{Gal}(L/\mathbb{Q}) \simeq G$.

(Hinweis: Folgerung 6.5, Hauptsatz, und die Tatsache (Satz von Dirichlet), dass es zu jedem $n \in \mathbb{N}$ eine Primzahl p gibt mit $n \mid p - 1$.)

7. Reguläre n-Ecke

Wir wollen die natürlichen Zahlen n (≥ 3) charakterisieren, für die das reguläre n-Eck (mit Zirkel und Lineal aus $M = \{0, 1\}$) konstruierbar ist. Dies ist gleichbedeutend dazu, dass die komplexe Zahl $z = e^{2\pi i/n}$ konstruierbar ist.

Definition 7.1

Eine ungerade Primzahl p heißt *Fermatsche Primzahl*, falls $p - 1$ eine Potenz von 2 ist.

Lemma 7.2

Sei p eine Primzahl. p ist Fermatsche Primzahl genau dann, wenn $p = 2^{2^t} + 1$ gilt für eine ganze Zahl $t \geq 0$.

[2] David A. Cox, *Why Eisenstein Proved the Eisenstein Criterion and Why Schönemann Discovered It First*, The American Mathematical Monthly, 118:1 (2011), 3–21.

Beweis. Ist p fermatsch, dann ist $p = 2^m + 1$ für ein $m \geq 1$. Ist s eine ungerade positive Zahl, so ist -1 eine Nullstelle von $T^s + 1$, also gilt $T^s + 1 = (T + 1) \cdot g$ für ein $g \in \mathbb{Z}[T]$. Für jede positive ganze Zahl r gilt also

$$2^{rs} + 1 = (2^r)^s + 1 = (2^r + 1) \cdot g(2^r).$$

Ist dies eine Primzahl, so muss $s = 1$ sein. Es folgt: Ist $p = 2^m + 1$ prim, so enthält m (außer 1) keinen ungeraden Teiler, ist also eine Potenz von 2. ∎

Bemerkung. Es ist allerdings unklar, welche der Zahlen $p = 2^{2^t} + 1$ überhaupt Primzahlen sind. Bisher ist dies nur für $t = 0, 1, \ldots, 4$ bekannt. D. h. die zur Zeit einzig bekannten Fermatschen Primzahlen sind 3, 5, 17, 257 und 65.537. Für $t = 5$ hat man $4.294.967.297 = 641 \times 6.700.417$ (Euler).

Lemma 7.3

(1) *Sei p eine Primzahl und $k \geq 1$. Dann gilt $\varphi(p^k) = p^k - p^{k-1}$.*
(2) *Sind $m, n \in \mathbb{N}$ teilerfremd, so gilt $\varphi(mn) = \varphi(m)\varphi(n)$.*
(3) *Sei $n = p_1^{k_1} \ldots p_t^{k_t}$ mit $k_i \geq 1$ und paarweise verschiedenen Primzahlen $p_1, \ldots, p_t$. Dann gilt*

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

Beweis. (1) Von den p^k Elementen 1, 2, …, p^k sind genau die p^{k-1} Elemente $p \cdot m$ ($1 \leq m \leq p^{k-1}$) nicht teilerfremd zu p^k.

(2) Es gilt $\mathbb{Z}_{mn} \simeq \mathbb{Z}_m \times \mathbb{Z}_n$, und es folgt $E(\mathbb{Z}_{mn}) \simeq E(\mathbb{Z}_m) \times E(\mathbb{Z}_n)$, und die Behauptung folgt.

(3) Folgt sofort aus (1) und (2). ∎

Satz 7.4 (*Gauß (1796/1801)*)

Sei $n \geq 1$ eine natürliche Zahl und $\zeta \in \mathbb{C}$ eine primitive n-te Einheitswurzel. Äquivalent sind:

(1) *ζ ist konstruierbar (aus 0, 1) (d. h. das reguläre n-Eck ist konstruierbar).*
(2) *$\varphi(n)$ ist eine Potenz von 2.*
(3) *Es ist $n = 2^r p_1 \ldots p_t$ mit $r \geq 0$ und paarweise verschiedenen Fermatschen Primzahlen $p_1, \ldots, p_t$ ($t \geq 0$).*

Beweis. "(1)⇒(2)". Ist ζ konstruierbar, so zeigt Folgerung V.5.5, dass $\varphi(n) = [E_n(\mathbb{Q}) : \mathbb{Q}] = [\mathbb{Q}(\zeta) : \mathbb{Q}]$ eine 2-er Potenz sein muss.

"(2)⇒(1)". $E_n(\mathbb{Q})/\mathbb{Q}$ ist galoissch mit abelscher Galoisgruppe G der Ordnung $\varphi(n)$, nach Folgerung 6.5. Hat nun G eine Ordnung 2^m, so folgt mit dem Satz von Cauchy (abelsche Version, Lemma II.3.1), dass es eine prim-zyklische Normalreihe gibt für G, wobei jeder Faktor die Ordnung 2 hat: denn ist U eine Untergruppe der Ordnung 2, so ist auch G/U abelsch und von der Ordnung 2^{m-1}, und man argumentiert dann induktiv. Auf diese Normalreihe wendet man den Hauptsatz der Galoistheorie an, um einen Körperturm

$$\mathbb{Q} = K_0 \subset K_1 \subset \ldots \subset K_{m-1} \subset K_m = E_n(\mathbb{Q}) \ni \zeta$$

mit $[K_i : K_{i-1}] = 2$ für $i = 1, \ldots, n$ zu bekommen.

"(3)⇒(2)". Ist $n = 2^r p_1 \ldots p_t$ mit $r \geq 0$ und paarweise verschiedenen Fermatschen Primzahlen $p_1, \ldots, p_t$, so gilt

$$\varphi(n) = (2^r - 2^{r-1}) \cdot (p_1 - 1) \cdot \ldots \cdot (p_t - 1),$$

wobei der erste Faktor nur für $r \geq 1$ auftaucht. Aus der Form der Fermatschen Primzahlen folgt, dass $\varphi(n)$ eine Potenz von 2 ist.

"(2)⇒(3)". Sei umgekehrt $\varphi(n)$ eine Potenz von 2. Sei $n = p_1^{k_1} \dots p_t^{k_t}$ die Primfaktorzerlegung. Dann gilt

$$\varphi(n) = \prod_{i=1}^{t} (p_i^{k_i} - p_i^{k_i - 1}),$$

und daher muss jedes $p_i^{k_i} - p_i^{k_i-1}$ eine Potenz von 2 sein. Ist $p_i \neq 2$, so muss dann $k_i = 1$ sein, da sonst p_i ein Teiler wäre. Es ist also n von der Form $n = 2^r p_1 \dots p_t$ mit $r \geq 0$ und paarweise verschiedenen ungeraden Primzahlen p_i, und es ist $p_i - 1 = \varphi(p_i)$ eine Potenz von 2, also p_i fermatsch. ■

Bemerkung. Für $n = 3, \dots, 20$ gilt für genau die fettgedruckten n, dass $\varphi(n)$ eine 2-er Potenz ist, also das reguläre n-Eck konstruierbar ist.

n	**3**	**4**	**5**	**6**	7	**8**	9	**10**	11	**12**	13	14	**15**	**16**	**17**	18	19	**20**
$\varphi(n)$	2	2	4	2	6	4	6	4	10	4	12	6	8	8	16	6	18	8

Auch hier sieht man nochmal, dass die Dreiteilung des Winkels nicht geht: das reguläre 3-Eck ($\hat{=}$ 120°-Winkel) ist konstruierbar, das reguläre 9-Eck ($\hat{=}$ 40°-Winkel) aber nicht.

8. Allgemeines Konstruierbarkeitskriterium *

Das folgende allgemeine Kriterium ist eine modifizierte Version vom notwendigen Kriterium Folgerung V.5.5. Der Beweis erfordert den Hauptsatz der Galoistheorie.

Satz 8.1 (*Hinreichendes und notwendiges Konstruierbarkeitskriterium*)

Sei $z \in \mathbb{C}$. Äquivalent sind:

(1) *z ist konstruierbar.*

(2) *z ist algebraisch, und der Grad des Zerfällungskörpers des Minimalpolynoms von z über $\mathbb{Q}$ ist eine Potenz von 2.*

Beweis. "(1)⇒(2)". Sei z konstruierbar. Dann gibt es einen Körperturm

$$\mathbb{Q} = K_0 \subset K_1 \subset \dots \subset K_n$$

mit $[K_i : K_{i-1}] = 2$ für $i = 1, \dots, n$ und mit $z \in K_n$. Jedes K_i wird über K_{i-1} durch ein Element vom Grad 2 erzeugt. Quadratische Ergänzung zeigt dann, dass $K_i = K_{i-1}(\sqrt{a_i})$ für ein $a_i \in K_{i-1}$ gilt ($i = 1, \dots, n$). Es gilt:

Es gibt eine endliche Galois*erweiterung $L/\mathbb{Q}$, die K_n als Zwischenkörper enthält, und einen Körperturm*

$$\mathbb{Q} = L_0 \subseteq L_1 \subseteq \dots \subseteq L_m = L$$

mit $[L_i : L_{i-1}] \leq 2$ ($i = 1, \dots, m$).

Beweis durch Induktion nach n. Für $n = 0$ und $n = 1$ ist die Aussage trivial. Sei nun $n \geq 2$. Setze $K = K_n$, $K' = K_{n-1}$, und sei per Induktionsvoraussetzung L' eine Erweiterung von K' mit $L'/\mathbb{Q}$ galoissch und das obere Ende eines Körperturms wie behauptet. Sei $b \in K$ mit $K = K'(b)$ und mit $b^2 \in K'$. Wir betrachten $L'K = L'(b)$, das Kompositum gebildet in $\mathbb{C}$. Sei L der normale Abschluss von $L'K$ über $\mathbb{Q}$. Ist $\sigma \in G := \mathrm{Gal}(L/\mathbb{Q})$, so ist $\sigma(L'K) = \sigma(L'(b)) = \sigma(L')(\sigma(b)) = L'(\sigma(b))$; letzte Gleichung, weil $L'/\mathbb{Q}$ normal ist; ferner enthält L' damit auch den Körper $\sigma(K')$. Da L nach Proposition VI.6.6 das Kompositum aller Konjugierten von $L'K$ ist, folgt $L = L'\big(\sigma(b) : \sigma \in G\big)$. Wegen $b^2 \in K' \subseteq L'$ ergibt sich $[L'(b) : L'] \leq 2$, und wegen $\sigma(b)^2 \in \sigma(K') \subseteq L'$ ebenso, dass bei jedem weiteren Hinzuadjungieren eines Konjugierten von b ein Grad ≤ 2 hinzukommt, bis L erreicht ist. Es folgt die Behauptung. —

Da nun $L/\mathbb{Q}$ normal ist mit $z \in L$, enthält L einen Zerfällungskörper F des Minimalpolynoms von z über $\mathbb{Q}$. Es ist nach Konstruktion $[L : \mathbb{Q}]$ eine Potenz von 2, also auch $[F : \mathbb{Q}]$ als Teiler dieser Zahl.

"(2)⇒(1)". Sei L Zerfällungskörper des Minimalpolynoms von z über $\mathbb{Q}$, und es sei $[L : \mathbb{Q}] = 2^m$. Es ist $L/\mathbb{Q}$ eine Galoiserweiterung. Beweise per Induktion nach m, dass jedes $x \in L$ konstruierbar ist. Für $m = 0$ (oder $m = 1$) ist die Sache klar. Sei nun $m \geq 1$. Die Gruppe $G = \mathrm{Gal}(L/\mathbb{Q})$ hat die Ordnung 2^m und hat daher ein nichttriviales Zentrum, nach Proposition I.5.7, und dies Zentrum enthält (Cauchy) ein Element der Ordnung 2; die davon erzeugte Untergruppe N ist ein Normalteiler von G. Sei $K = L^N$. Nach dem Hauptsatz der Galoistheorie ist $K/\mathbb{Q}$ galoissch, vom Grad $[K : \mathbb{Q}] = 2^{m-1}$. Nach Induktionsvoraussetzung ist jedes Element in K konstruierbar. Da jedes $x \in L$ einer quadratischen Gleichung über K genügt, ist dann auch x konstruierbar. ■

9. Der Fundamentalsatz der Algebra *

Ziel dieses Abschnitts ist es, einen weitesgehend algebraischen Beweis des folgenden Satzes zu geben.

Satz 9.1 (*Fundamentalsatz der Algebra*)

Der Körper $\mathbb{C}$ der komplexen Zahlen ist algebraisch abgeschlossen.

Dabei heisst ein Körper K *algebraisch abgeschlossen*, wenn jedes nicht-konstante Polynom $f \in K[T]$ in K eine Nullstelle hat, oder äquivalent, wenn es über K vollständig in Linearfaktoren zerfällt. Die elegantesten Beweise des Satzes werden in der Funktionentheorie geführt mit dem Satz von Liouville. Hier soll der Beweis als Anwendung der Galoistheorie und der Sylowsätze erfolgen.

Analytische Eigenschaften der reellen Zahlen. Für den Beweis des Fundamentalsatzes der Algebra benötigen wir die folgenden, wohl-bekannten Eigenschaften des Körpers $\mathbb{R}$ der reellen Zahlen:

(1) jedes Polynom $f \in \mathbb{R}[T]$ ungeraden Grades hat eine reelle Nullstelle (dies folgt aus dem Zwischenwertsatz);
(2) jede positive reelle Zahl hat eine reelle Quadratwurzel.

Aus (1) ergibt sich sofort:

Lemma 9.2

Ist $L/\mathbb{R}$ eine endliche Körpererweiterung mit $[L : \mathbb{R}]$ ungerade, so gilt $L = \mathbb{R}$.

Beweis. Da $\mathbb{R}$ perfekt ist, gibt es nach dem Satz vom primitiven Element ein $x \in L$ mit $L = \mathbb{R}(x)$. Dann hat $f = \mathrm{MIPO}(x/\mathbb{R})$ ungeraden Grad n, ist irreduzibel und hat eine reelle Nullstelle, was nur für $n = 1$ möglich ist. ■

Aus (2) kann man leicht (z. B. aus der Polarkoordinatendarstellung) ableiten, dass jede komplexe Zahl eine (komplexe) Quadratwurzel besitzt. Daraus folgt:

Lemma 9.3

Ist $L/\mathbb{C}$ eine Körpererweiterung mit $[L : \mathbb{C}] \leq 2$, so gilt $L = \mathbb{C}$.

Beweis. Wie beim vorherigen Lemma. ■

Beweis von Satz 9.1. (Gauß-Artin) Es sei $L/\mathbb{C}$ eine endliche Körpererweiterung. Dann ist auch $L/\mathbb{R}$ endlich. Sei $N \supseteq L$ normaler Abschluss von $L/\mathbb{R}$. Dann ist $N/\mathbb{R}$ galoissch. Wir werden $N = \mathbb{C}$ zeigen, was den Fundamentalsatz beweist. Sei $G = \mathrm{Gal}(N/\mathbb{R})$. Es ist $|G| = [N : \mathbb{R}] = [N : \mathbb{C}] \cdot [\mathbb{C} : \mathbb{R}] = 2[N : \mathbb{C}]$

gerade. Sei P eine 2-Sylowgruppe von G. Sei $M = N^P$ der Fixkörper von P in N. Dann ist $[M : \mathbb{R}] = [G : P]$ ungerade. Nach dem ersten Lemma folgt $M = \mathbb{R}$. Damit ist G eine 2-Gruppe (eine Gruppe der Ordnung 2^m). Dann ist auch $H := \mathrm{Gal}(N/\mathbb{C}) \subseteq \mathrm{Gal}(N/\mathbb{R})$ eine 2-Gruppe. Sagen wir, $|H| = 2^n$. Angenommen, $n > 0$. Eine maximale Untergruppe $U \neq H$ von H (existiert!) hat die Ordnung 2^{n-1}, also $[H : U] = 2$: dies zeigt man per Induktion nach n; man nutzt aus, dass H für $n \geq 1$ ein nicht-triviales Zentrum hat (Proposition I.5.7), das eine Untergruppe V der Ordnung 2 enthält (Satz von Cauchy); dann wendet man die Induktionsvoraussetzung auf die Faktorgruppe H/V an. — Für den Fixkörper N^U gilt also $[N^U : \mathbb{C}] = 2$. Das ist aber nach dem zweiten Lemma nicht möglich. Also gilt $n = 0$, und damit $[N : \mathbb{C}] = |H| = 2^0 = 1$, also $N = \mathbb{C}$. ■

Bemerkung. Beweisversuche des Fundamentalsatzes gab es von vielen großen Mathematikern (Leibniz, Euler, Lagrange, Laplace,...), wobei d'Alembert (1746) besonders hervorzuheben ist. Alle diese Beweisansätze waren jedoch lückenhaft. C. F. Gauß hat mindestens vier unterschiedliche Beweise des Fundamentalsatzes veröffentlicht. Sein erster von 1799, auf Grundlage von d'Alemberts Idee, ist aber ebenfalls noch nicht ganz vollständig, weil Gauß ohne Beweis Eigenschaften von Kurven verwendete, die damals noch nicht bekannt waren. Erst sein zweiter Beweis von 1816 gilt aus heutiger Sicht als komplett. Zuvor hatte R. Argand 1814 ebenfalls einen nahezu vollständigen Beweis vorgelegt, auf Grundlage des Ansatzes von d'Alembert; allerdings war die von ihm verwendete Existenz eines Minimums einer stetigen Funktion auf einem Kompaktum damals noch nicht rigoros bewiesen. Der Fundamentalsatz wird manchmal auch *Satz von Gauß-d'Alembert* genannt.

Recht ausführlich zusammengefasst ist die Historie in dem von R. Remmert verfassten Kapitel zum Fundamentalsatz der Algebra in dem Buch H.-D. Ebbinghaus et. al., *Numbers*, Springer 1991. (Auch auf deutsch als *Zahlen* (2. Auflage 1988) erhältlich.)

KAPITEL VIII

Ergänzende Themen zur Auflösbarkeit von Gleichungen *

1. Die allgemeine Gleichung n-ten Grades

Sei k ein Körper und $k(t_1,\dots,t_n)$ der Quotientenkörper des Polynomrings $k[t_1,\dots,t_n]$ in n Unbestimmten über k. Sei $f(X)\in L[X]$ das folgende Polynom in einer Unbestimmten X über dem Körper $L=k(t_1,\dots,t_n)$:

$$f(X)=(X-t_1)\cdot(X-t_2)\cdot\ldots\cdot(X-t_n)=X^n-s_1X^{n-1}+\cdots+(-1)^n s_n,$$

wobei die $s_i\in k(t_1,\dots,t_n)$ die *elementar-symmetrischen Polynome* sind:

$$s_1=t_1+t_2+\cdots+t_n,\ s_2=\sum_{1\le i<j\le n}t_it_j,\ \ldots,\ s_n=t_1t_2\ldots t_n.$$

Es heisst $f(X)$ das *allgemeine Polynom* n-ten Grades über k, und $f(x)=0$ die *allgemeine Gleichung* n-ten Grades über k. Es ist $K=k(s_1,\dots,s_n)$ ein Teilkörper von L, und $f(X)\in K[X]$. Offenbar ist L der Zerfällungskörper von $f(X)$ über K.

Proposition 1.1

L/K ist eine Galoiserweiterung vom Grad $[L:K]=n!$ und mit Galoisgruppe $\mathbb{S}_n$.

Beweis. Es ist klar, dass jedes $\sigma\in\mathbb{S}_n$ vermöge $t_i\mapsto t_{\sigma(i)}$ einen K-Automorphismus von L induziert. Nach dem Satz von Artin ist $L/L^{\mathbb{S}_n}$ galoissch mit Galoisgruppe $\mathbb{S}_n$ und $[L:L^{\mathbb{S}_n}]=|\mathbb{S}_n|=n!$. Offenbar gilt $K=k(s_1,\dots,s_n)\subseteq L^{\mathbb{S}_n}$. Da L Zerfällungskörper von $f(X)$ (Polynom vom Grad n) über K ist, gilt außerdem $[L:K]\le n!$. Damit ergibt sich $K=L^{\mathbb{S}_n}$. ∎

Bemerkung. Ein $f\in L=k(t_1,\dots,t_n)$ heisst *symmetrisch*, falls $f=f^\sigma$ gilt für jedes $\sigma\in\mathbb{S}_n$, also wenn $f\in L^{\mathbb{S}_n}$. Die Schlussfolgerung $L^{\mathbb{S}_n}=k(s_1,\dots,s_n)$ ist dann gerade Teil des *Hauptsatzes über symmetrische Funktionen*: die symmetrischen Funktionen sind gerade die durch die elementar-symmetrischen Polynome erzeugten Funktionen. (Zu diesem Hauptsatz vgl. auch unten stehende Proposition.)

Aus Satz VII.4.5 folgt sofort:

Satz 1.2 (*Ruffini-Abel (1799/1813, 1824/26)*)

Sei f das allgemeine Polynom n-ten Grades über einem Körper der Charakteristik 0. Für $n\ge 5$ ist $f(x)=0$ nicht auflösbar durch Radikale.

Eine wesentliche Lücke in Ruffinis Beweis von Satz 1.2 bestand in der Unklarheit, ob bei ihm die Bildung von Radikalen tatsächlich im Körper L stattfinden muss, was er stillschweigend annahm. Diese Lücke wurde von Abel geschlossen mit folgender Aussage, die er natürlich noch ohne Galoistheorie bewiesen hatte. Der unten stehende Beweis verwendet Galoistheorie und ist im Gegensatz zu Abels Beweis (vgl. [**15**] oder [**16**]) nahezu trivial.

Proposition 1.3 (*Satz von Abel über natürliche Irrationalitäten*)

Sei L/K die Körpererweiterung mit $L = \mathbb{C}(t_1, \ldots, t_n)$ und $K = \mathbb{C}(s_1, \ldots, s_n)$. Sei $v \in L$ ein Element, welches in einer Radikalerweiterung R/K liegt. Dann gibt es eine Radikalerweiterung R'/K mit $R' \subseteq L$ und $v \in R'$.

Kurz: Radikale, die außerhalb von L gebildet werden, etwa $\sqrt[7]{s_1}$, bieten keinen zusätzlichen Nutzen.

Beweis. Allgemeiner sei K ein Körper der Charakteristik 0, der alle Einheitswurzeln enthält, und L/K eine endliche Galoiserweiterung. Wir können ohne Einschränkung annehmen, dass R/K eine galoissche Radikalerweiterung ist, vgl. Proposition VII.4.4. Dann ist $\mathrm{Gal}(R/K)$ auflösbar.

Sei $f = \mathrm{MIPO}(v/K)$. Weil $v \in L \cap R$, und weil L/K und R/K normal sind, zerfällt f über L und über R in Linearfaktoren. Ist M der Zerfällungskörper von f über K, so können wir also $M \subseteq L \cap R$ annehmen[1]. M/K ist galoissch, und $\mathrm{Gal}(M/K) \simeq \mathrm{Gal}(R/K)/\mathrm{Gal}(R/M)$ ist auflösbar. Da K alle Einheitswurzeln enthält, folgt, dass M/K eine Radikalerweiterung ist, vgl. den letzten Beweisteil von Satz VII.4.5. Wegen $v \in M$ und $M \subseteq L$ folgt die Behauptung mit $R' := M$. ∎

Der Vollständigkeit halber zeigen wir noch folgenden zweiten Teil des Hauptsatzes über symmetrische Funktionen.

Proposition 1.4

Die elementar-symmetrischen Polynome $s_1, \ldots, s_n$ sind über k algebraisch unabhängig. D. h. ist $f \in k[S_1, \ldots, S_n]$ ein Polynom in den n Unbestimmten $S_1, \ldots, S_n$, und gilt $f(s_1, \ldots, s_n) = 0$, so ist schon $f = 0$. Es folgt also, dass $k[s_1, \ldots, s_n]$ selbst ein Polynomring über k in den Unbestimmten $s_1, \ldots, s_n$ ist und $K = k(s_1, \ldots, s_n)$ dessen rationaler Funktionenkörper.

Beweis. [9, IV, §6] Induktion nach n. Nehmen wir stattdessen an, dass $f \neq 0$ gilt. Wir können außerdem annehmen, dass f dabei minimalen Grad hat (wobei per definitionem jedes S_i den Grad 1 hat, und ein Monom die Summe der auftauchenden Exponenten als Grad). Schreibe f als Polynom in der Unbestimmten S_n:

$$f = f_0(S_1, \ldots, S_{n-1}) + f_1(S_1, \ldots, S_{n-1}) \cdot S_n + \ldots + f_d(S_1, \ldots, S_{n-1}) \cdot S_n^d.$$

Dabei gilt $f_0(S_1, \ldots, S_{n-1}) \neq 0$: denn sonst wäre $f = g \cdot S_n$ für ein Polynom $g \in k[S_1, \ldots, S_{n-1}] \subseteq k[S_1, \ldots, S_n]$, $g \neq 0$, und Einsetzen der s_i ergibt $0 = g(s_1, \ldots, s_{n-1})s_n$, und daher $g(s_1, \ldots, s_{n-1}) = 0$; aber g hat einen kleineren Grad als f. —

Einsetzen der s_i in obige Gleichung liefert

$$0 = f_0(s_1, \ldots, s_{n-1}) + f_1(s_1, \ldots, s_{n-1}) \cdot s_n + \ldots + f_d(s_1, \ldots, s_{n-1}) \cdot s_n^d.$$

Dies ist insbesondere eine Gleichung in $k[t_1, \ldots, t_n]$. Substituieren wir $t_n = 0$, so ergibt dies wegen $s_n = t_1 \cdot \ldots \cdot t_n$, dass alle Summanden verschwinden, bis auf den 0-ten: $0 = f_0(s'_1, \ldots, s'_{n-1})$, wobei hier s'_i aus s_i durch Substitution $t_n = 0$ hervorgeht. Dies ist nun eine nicht-triviale Relation in den elementar-symmetrischen Polynomen in $k[t_1, \ldots, t_{n-1}]$, und dies ergibt einen Widerspruch nach der Induktionsannahme. ∎

[1] Um präzise zu sein: Weil $R/K(v)$ galoissch ist, ist R Zerfällungskörper eines (separablen) Polynoms g über $K(v)$. Es sei $\Omega = L(\alpha_1, \ldots, \alpha_s)$ Zerfällungskörper von g über L, mit $\alpha_1, \ldots, \alpha_s$ die Nullstellen von g in Ω. Dann ist offenbar $K(v)(\alpha_1, \ldots, \alpha_s) \subseteq \Omega$ ein Zerfällungskörper von g über $K(v)$. Dieser ist $K(v)$-isomorph zum Zerfällungskörper R. Wir können ohne Einschränkung Gleichheit annehmen. Dann spielt sich alles in Ω ab, und f hat in L und in R dieselben Nullstellen.

Bemerkung. Das allgemeine Polynom n-ten Grades ist eigentlich ein ganz spezielles Polynom. Es ist aber insofern "allgemein", weil man in die Koeffizienten (die selbst in keinerlei algebraischer Relation zueinander stehen; vgl. vorherige Proposition) beliebige Körperelemente aus k einsetzen kann, und dann ein "konkretes" Polynom in $k[X]$ vom Grad n erhält. Klar ist dann: wenn sich das allgemeine Polynom n-Grades über k durch Radikale auflösen lässt, dann auch *jedes* Polynom n-ten Grades in $k[X]$; die "Lösungsformel" wäre dabei sogar sozusagen "universell" durch die des allgemeinen Polynoms vorgegeben. (Für $n \leq 4$ kann man dies ausnutzen.) Umgekehrt sagt die Nichtauflösbarkeit (durch Radikale) des allgemeinen Polynoms n-ten Grades wie im vorstehenden Satz nichts über die Auflösbarkeit einzelner, konkreter Polynome n-Grades in $k[X]$ aus. So schließt Satz 1.2 theoretisch nicht aus, dass etwa sogar alle Polynome 5-ten Grades in $\mathbb{Q}[X]$ auflösbar wären (was ja nach Folgerung VII.5.4 nicht der Fall ist). Daher ist Galois' Satz VII.4.5, mit dem wir ja auch Satz 1.2 bewiesen haben, eine deutliche Verbesserung vom letzteren.

Aufgaben

Ü 1.1. [Satz von Abel (1829)] Sei $\mathrm{Char}(K) = 0$ und $f \in K[T]$ vom Grad n mit Nullstellen $x = x_1, x_2, \ldots, x_n$ im Zerfällungskörper L. Es gebe rationale Funktionen $\theta_i \in K(T)$ mit

- $\theta_i(x) = x_i$ für $i = 1, \ldots, n$, sowie
- $\theta_i\big(\theta_j(x)\big) = \theta_j\big(\theta_i(x)\big)$ für alle $1 \leq i, j \leq n$.

(In dem Fall nennt man $f(x) = 0$ eine *abelsche Gleichung*[2].)

Dann ist $f(x) = 0$ auflösbar. — Genauer: $\mathrm{Gal}(f/K)$ ist abelsch.

Ü 1.2. Für das n-te Kreisteilungspolynom Φ_n über $\mathbb{Q}$ ist die Gleichung $\Phi_n(x) = 0$ abelsch.

Ü 1.3. Sei $f \in K[T]$ irreduzibel und separabel. Genau dann ist die Gleichung $f(x) = 0$ abelsch, wenn die Gruppe $\mathrm{Gal}(f/K)$ abelsch ist.

2. Auflösbarkeit von irreduziblen Gleichungen von Primgrad

Es gelte $\mathrm{Char}(K) = 0$. Sei p eine Primzahl. Sei $f \in K[T]$ irreduzibel (separabel) und vom Grad p. Wir identifizieren die Nullstellenmenge von f mit der Menge $X = \{0, 1, \ldots, p-1\}$ und betrachten diese als die Elementmenge des Körpers $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Wir wissen, dass $\mathrm{Gal}(f/K)$ transitiv auf X operiert. Sei $\mathrm{GA}(p) \subseteq \mathbb{S}_p$ die Untergruppe der bijektiven, affinen Abbildungen $m_{a,b}\colon \mathbb{F}_p \to \mathbb{F}_p$, $x \mapsto ax+b$ mit $a, b \in \mathbb{F}_p$, $a \neq 0$. Dann ist $m_{1,1} = \sigma := (0\,1 \ldots\, p{-}1)$ ein p-Zykel. Schreiben wir $m_a = m_{a,0}$, so ist leicht zu sehen, dass $m_a\sigma = \sigma^a m_a$ gilt und jedes Element in $\mathrm{GA}(p)$ sich eindeutig in der Form $\sigma^b m_a$ (mit $1 \leq a \leq p-1$, $0 \leq b \leq p-1$) schreiben lässt, und $\mathrm{GA}(p)$ damit die Ordnung $p(p-1)$ hat. Offensichtlich operiert $\langle\sigma\rangle$ transitiv auf X, also auch $\mathrm{GA}(p)$. Zudem ist leicht zu sehen, dass $\langle\sigma\rangle$ ein (abelscher) Normalteiler in $\mathrm{GA}(p)$ ist mit abelschem Faktor. Daher ist $\mathrm{GA}(p)$ auflösbar. Ferner gilt insbesondere für $\mathrm{GA}(p)$ folgende Aussage:

Sei $G < \mathbb{S}_p$ eine Untergruppe mit $\sigma \in G$ und $|G| < p^2$. Dann sind die Elemente σ^j (mit $1 \leq j \leq p-1$) die einzigen p-Zykeln in G.

Denn sei $\tau \in G$ ein p-Zykel. Dann können nicht alle Elemente $\sigma^i\tau^j$ mit $1 \leq i, j \leq p-1$ verschieden sein. Etwa $\sigma^i\tau^j = \sigma^s\tau^t$, mit $i \neq s$ und $j \neq t$. In dem Körper $\mathbb{F}_p$ hat $t-j$ ein Inverses u. Dann folgt $\tau = \tau^{u(t-j)} = \sigma^{u(i-s)}$.

Satz 2.1 (*Galois*)

Sei G eine Untergruppe von $\mathbb{S}_p$. Es ist G transitiv und auflösbar genau dann, wenn G konjugiert zu einer Untergruppe von $\mathrm{GA}(p)$ ist, die σ enthält.

[2] Dies ist der Grund dafür, dass später kommutative Gruppen *abelsch* genannt wurden.

Beweis. "⇐" ist klar, weil jede Gruppe, isomorph zu einer Untergruppe der auflösbaren Gruppe $\mathrm{GA}(p)$, selbst auflösbar ist.

"⇒" Es gibt nach Satz III.7.5 eine prim-zyklische Normalreihe

$$\{1\} = U_0 \lhd U_1 \lhd \cdots \lhd U_{n-1} \lhd U_n = G.$$

Jeder nicht-triviale Normalteiler N einer transitiven Gruppe H in $\mathbb{S}_p$ ist selbst transitiv mit $p \mid |N|$.

Denn alle n verschiedenen N-Bahnen $N.x$ von X sind gleichmächtig (weil H transitiv und $N \lhd H$), und die N-Bahnenzerlegung von X liefert $p = |X| = n \cdot |N.x|$, damit (wegen p prim und $N \to \mathbb{S}(X)$, $n \mapsto [x \mapsto n.x]$ injektiv nach dem Abschnitt vor VII.5.1) $n = 1$, und mit dem Bahnenlemma folgt $p \mid |N|$. —

Insbesondere folgt dies (induktiv) für $U_{n-1}, \ldots, U_1$, und $|U_1| = p$. Es enthält U_1 also einen p-Zykel. Es gibt also $\tau \in \mathbb{S}_p$ mit $\tau\sigma\tau^{-1} \in G$, bzw. $\sigma \in \tau^{-1}U_1\tau \subseteq \mathrm{GA}(p)$. Da $g \mapsto \tau^{-1}g\tau$ ein Automorphismus von $\mathbb{S}_p$ ist, können wir zur Vereinfachung der Notation ohne Einschränkung annehmen, dass $\tau = 1$ ist. Also $\sigma \in U_1 < \mathrm{GA}(p)$. Wegen $U_1 \lhd U_2$ folgt $u\sigma u^{-1} \in \mathrm{GA}(p)$ für alle $u \in U_2$. Mit nachfolgendem Argument schließen wir daraus $u \in \mathrm{GA}(p)$, also $U_2 \subseteq \mathrm{GA}(p)$, und setzt dies dann induktiv fort bis $G = U_n \subseteq \mathrm{GA}(p)$. Es ist also noch zu zeigen:

Ist $\beta \in \mathbb{S}_p$ mit $\beta\sigma\beta^{-1} \in \mathrm{GA}(p)$, so gilt $\beta \in \mathrm{GA}(p)$.

Denn offenbar ist $\beta\sigma\beta^{-1}$ ein p-Zykel. Da dieser in $\mathrm{GA}(p)$ liegt, folgt aus der Vorbemerkung zum Satz, dass $\beta\sigma\beta^{-1} = \sigma^j$ für ein $j \in \{1, \ldots, p-1\}$ gilt. Also $\beta\sigma = \sigma^j\beta$. Das bedeutet $\beta(x+1) = \beta(x) + j$ in $\mathbb{F}_p$, und es folgt induktiv $\beta(x) = jx + \beta(0)$ in $\mathbb{F}_p$. Damit $\beta = m_{j,\beta(0)} \in \mathrm{GA}(p)$. ∎

Bemerkung. Insbesondere folgt:

$$f(x) = 0 \text{ auflösbar} \quad \Rightarrow \quad p \mid \; |\mathrm{Gal}(f/K)| \; \mid p(p-1).$$

Für $p = 5$ zum Beispiel kommen als Ordnungen nur 5, 10 und 20 in Frage, obwohl die $\mathbb{S}_5$ ja 120 Elemente hat. Für $p = 7$ gilt schon $|\mathbb{S}_7| = 5040$, aber nur 7, 14, 21 und 42 kommen als Ordnungen im Falle der Auflösbarkeit in Frage.

Lemma 2.2

Sei G eine transitive Untergruppe von $\mathbb{S}_p$. Es ist G auflösbar genau dann, wenn das einzige Element in G, welches zwei Elemente fest lässt, das neutrale Element ist.

Beweis. "⇒" Hier genügt es zu beoachten, dass alle Untergruppen von $\mathrm{GA}(p)$ und deren konjugierten die behauptete Eigenschaft haben.

"⇐" Es gelte, dass das neutrale Element das einzige in G ist, das mindestens zwei Fixpunkte hat. Dann folgt, dass die Standuntergruppen von zwei verschiedenen Elementen disjunkt sind, wenn man jeweils das neutrale Element heraus nimmt. Jede Standuntergruppe hat wegen der Transitivität genau $q := |G|/p$ Elemente (Bahnenlemma). Da jedes $1 \neq g \in G$ entweder in der Standuntergruppe $\mathrm{St}_G(x)$ eines (eindeutigen) Elementes $x \in X$ liegt oder keinen Fixpunkt hat, zeigt ein einfaches Abzählargument, dass G genau $p-1$ Elemente ohne Fixpunkte hat. Sei $\gamma \in G$ ein solches. Dann gilt:

γ ist ein p-Zykel. Die γ^j mit $1 \leq j \leq p-1$ sind alle p-Zykel in G.

Denn: Würde γ^j ein Element $x \in X$ fix lassen, so auch das Element $\gamma(x) \neq x$, und daher muss $\gamma^j = 1$ gelten. Es folgt also, dass für jedes $x \in X$ die Standuntergruppe $\mathrm{St}_{\langle\gamma\rangle}(x)$ trivial ist und damit jede $\langle\gamma\rangle$-Bahn genau $|\langle\gamma\rangle| > 1$ viele Elemente hat. Da $|X| = p$ prim, kann es dann nur eine $\langle\gamma\rangle$-Bahn geben, und diese hat p Elemente. —

Es ist γ konjugiert zu σ. Zur Vereinfachung der Notation können wir auch hier wieder annehmen, dass diese Konjugation trivial ist, also $\gamma = \sigma$. Ist nun $\beta \in G$, so ist $\beta\sigma\beta^{-1}$ von der Form σ^j (weil ohne Fixpunkte). Insbesondere $\beta\sigma\beta^{-1} \in \mathrm{GA}(p)$.

Aus einer Aussage aus dem Beweis des vorherigen Satzes folgt $\beta \in \mathrm{GA}(p)$. Also $G < \mathrm{GA}(p)$ auflösbar. ■

Satz 2.3 (*Galois*)

Sei $f \in K[T]$ irreduzibel (separabel) vom Grad p prim und mit Zerfällungskörper L. Genau dann ist die Gleichung $f(x) = 0$ durch Radikale auflösbar, wenn für alle Paare von Nullstellen x, y von f mit $x \neq y$ gilt, dass $L = K(x, y)$ ist.

Beweis. Nach dem Hauptsatz gilt $L = K(x, y)$ genau dann, wenn $\mathrm{Gal}(L/K(x, y)) = \{1_L\}$ gilt, also genau wenn jedes $\sigma \in \mathrm{Gal}(L/K)$, welches zwei Nullstellen festhält, die Identität ist. Die Aussage folgt dann aus dem Lemma mit Satz VII.4.5. ■

Aus dem Satz kann man ähnliche Aussagen wie in Satz VII.5.3 ableiten, zum Beispiel:

Folgerung 2.4

Es gelte $K \subseteq \mathbb{R}$. Sei $f \in K[T]$ irreduzibel vom Grad p prim. Es seien mindestens zwei, aber nicht alle Nullstellen von f reell. (Insbesondere folgt $p \geq 5$.) Dann ist die Gleichung $f(x) = 0$ nicht auflösbar.

Beweis. Seien x und y zwei reelle Nullstellen. Sei L der Zerfällungskörper von f über K. Weil es nicht-reelle Nullstellen gibt, kann $L = K(x, y)$ wegen $K(x, y) \subseteq \mathbb{R}$ nicht gelten. ■

Bemerkung. Bemerkenswert ist, dass der vorstehende Satz (und sein Korollar) völlig ohne Rückgriff auf Gruppen formuliert ist, und dass bei den Beweisen die Einfachheit der $\mathbb{A}_p$ bzw. die Nichtauflösbarkeit der $\mathbb{S}_p$ ($p \geq 5$) nicht verwendet wird.[3]

Bemerkung. Ein sehr lesenswerter, historischer Übersichtsartikel über die Sätze von Ruffini-Abel und Galois zur Auflösbarkeit von Gleichungen ist von M. Rosen[4]. Dort wird auch erwähnt, dass L. Kronecker 1856 die vorstehende Folgerung mit Abels Methoden bewiesen hat, offenbar in Unkenntnis des Resultats von Galois.

Beispiel. Als Beispiel können wir auch hier wieder $K = \mathbb{Q}$ und $f = T^5 - 6T + 3$ nennen. Man beachte jedoch, dass etwa für $K = \mathbb{R}$ die Gleichung $f(x) = 0$ über K auflösbar ist, denn f ist dann nicht mehr irreduzibel. Über $\mathbb{R}$ ist jede Gleichung auflösbar, weil $\mathbb{C} = \mathbb{R}(\sqrt{-1})/\mathbb{R}$ Radikalerweiterung (und algebraisch abgeschlossen) ist.

Aufgaben

Ü 2.1. Sei $p \geq 5$ prim. Das Polynom $f = T^p - 4T + 2 \in \mathbb{Q}[T]$ ist irreduzibel und (Kurvendiskussion) hat genau drei reelle Nullstellen. Also ist die Gleichung $f(x) = 0$ nicht auflösbar.

Ü 2.2. Sei p prim und $L \subseteq \mathbb{C}$ der Zerfällungskörper von $T^p - 2 \in \mathbb{Q}[T]$. Es gilt $L = \mathbb{Q}(e^{2\pi i/p}, \sqrt[p]{2})$ und $\mathrm{Gal}(L/\mathbb{Q}) \simeq \mathrm{GA}(p)$.

Ü 2.3. Sei p prim und $g = T^{p-1} + T^{p-2} + \ldots + T + 1 \in \mathbb{Q}[T]$ mit Nullstellen $x_0, \ldots, x_{p-2} \in \mathbb{C}$. Es ist $\mathrm{Gal}(g/\mathbb{Q})$ zyklisch von der Ordnung $p - 1$, erzeugt von $x_i \mapsto x_{i+1}$ (Indizes modulo $p - 1$) bei geeigneter Nummerierung.

Ü 2.4. Sei p prim und $f = T^p - 2 \in \mathbb{Q}[T]$. Es gilt $\mathrm{Gal}(f/\mathbb{Q}(e^{2\pi i/p})) \simeq \langle\sigma\rangle \lhd \mathrm{GA}(p)$ und $\mathrm{GA}(p)/\langle\sigma\rangle \simeq \mathrm{Gal}(g/\mathbb{Q})$ (mit g aus der vorigen Aufgabe), die Faktorgruppe gegeben durch die Menge der Nebenklassen $[m_a]$ ($1 \leq a \leq p - 1$).

[3] Galois notierte in seinem Testamentsbrief, dass die kleinste (nicht-abelsche) einfache Gruppe die Ordung 60 hat. (Satz III.5.8.) Ob er das mit damaligen Methoden bewiesen haben konnte, wird in folgendem lesenswerten Artikel beleuchtet. Ian Stewart: *Galois and the simple group of order* 60. Archive for History of Exact Sciences 78 (2024), 1–28.

[4] Michael Rosen: *Niels Hendrik Abel and Equations of the Fifth Degree.* The American Mathematical Monthly 102:6 (1995), 495–505.

Sei nun $p = 5$. Dann ist

$$\{1\} \lhd \langle\sigma\rangle \lhd \langle\sigma, m_4\rangle \lhd \mathrm{GA}(5)$$

eine prim-zyklische Normalreihe. Es gilt $\mathrm{GA}(5) \cap \mathbb{A}_5 = \langle\sigma, m_4\rangle \simeq \mathbb{D}_5$.

Ü 2.5. Statt $\mathbb{A}_5$ hatte Galois folgende Gruppe von 2×2-Matrizen über dem Körper $\mathbb{F}_5$ betrachtet: $\mathrm{PSL}_2(\mathbb{F}_5) := \mathrm{SL}_2(\mathbb{F}_5)/\pm 1$, wobei hier 1 die Einheitsmatrix meint. Es gilt $\mathrm{PSL}_2(\mathbb{F}_5) \simeq \mathbb{A}_5$. Alternativ: $\mathrm{PSL}_2(\mathbb{F}_5)$ ist eine einfache Gruppe der Ordnung 60.

3. Einheitswurzeln als Radikale

Sei K ein Teilkörper von $\mathbb{C}$. Im Beweis von Satz VII.4.5 wurde wesentlich Gebrauch von Einheitswurzeln gemacht, die man ggfs. einfach hinzu adjungiert hat. Bezeichnet man *eine* beliebige Nullstellen eines Polynoms der Form $f = T^n - a \in K[T]$ $(a \neq 0)$ mit $\sqrt[n]{a} \in \mathbb{C}$, so bekommen wir *alle* Nullstellen von f als $\zeta^k \cdot \sqrt[n]{a}$, wobei ζ eine n-te primitive Einheitswurzel ist. Daher kann man $\sqrt[n]{a}$ einen konkreten Wert geben, indem man sich an die Konvention hält, dass für positiv-reelles a mit $\sqrt[n]{a}$ die eindeutig bestimmte positiv-reelle n-te Wurzel von a genommen wird. Ist $0 \neq a \in \mathbb{C}$, so ist $a = r \cdot e^{i\alpha}$ (mit eindeutigen $r > 0$ und $0 \leq \alpha < 2\pi$). Dann ist $\sqrt[n]{a} := \sqrt[n]{r} \cdot e^{i\alpha/n}$ eine mögliche Konvention, dem Radikal $\sqrt[n]{a}$ einen eindeutigen Wert zu geben, und alle anderen Nullstellen von $T^n - a$ haben dann durch $\zeta^k \cdot \sqrt[n]{a}$ mit $k = 1, \ldots, n-1$ und $\zeta = e^{2\pi i/n}$ eine eindeutige Bedeutung. Aber:

(I) *Ist eine primitive n-ten Einheitswurzel ζ selbst ein "Radikal"?*

Nach Definition VII.2.2 ist die Antwort (trivialerweise) *ja*, denn ζ ist (eine) Nullstelle von $T^n - 1$, also "$\zeta = \sqrt[n]{1}$". Aber man könnte dies im Sinne von "Auflösung durch Radikale" als symbolisch-abstrakt und unvollständig ansehen.

Die dritte primitive Einheitswurzel $\zeta = e^{2\pi i/3}$ z. B. können wir auch schreiben als

$$\zeta = \frac{-1 + i\sqrt{3}}{2}.$$

D. h. ζ liegt in der (einfachen) Radikalerweiterung $\mathbb{Q}(\sqrt{-3})$ über $\mathbb{Q}$. Und dies ist gegenüber der Schreibweise "$\zeta = \sqrt[3]{1}$" sicherlich eine viel bessere Darstellung von ζ durch Radikale.

Eine weitere Frage ist:

(II) *Wenn man beim Auflösen einer Gleichung $f(x) = 0$ iterativ Radikale der Form $\sqrt[n]{a}$ adjungiert, sind dann* alle *Werte von $\sqrt[n]{a}$ zulässig zum Bauen einer Nullstelle von f?*

Man möchte ja keine falsche Auswahl treffen (können).

Vermöge $\sqrt[r]{\sqrt[s]{\ldots}} = \sqrt[r]{\sqrt[s]{\ldots}}$ sieht man, dass es genügt, die Fragen für $n = p$ prim zu beantworten, vgl. auch Satz III.7.5. Ist im jeweiligen Schritt das Polynom $T^p - a$ *irreduzibel* (über der bis dahin erreichten Teil-Radikalerweiterung K_i von K), so lassen sich je zwei Nullstellen davon stets durch einen K_i-Isomorphismus ineinander überführen nach Satz V.2.4, der sich dann auf den ganzen Zerfällungskörper von f erweitert, nach Satz VI.2.3. Hat man Frage (I) erstmal positiv beantwortet und alle nötigen Einheitswurzeln hinzuadjungiert, löst sich Frage (II) durch die (einfache) Übung VII.2.1; denn ist $T^p - a$ nicht irreduzibel über K_i, so zerfällt es schon über K_i in Linearfaktoren, d. h. durch Hinzuadjungieren der Nullstellen vergrößert sich K_i nicht, und wir können den Schritt dann auslassen.

Zur Frage (I) haben wir[5]:

Satz 3.1 (*Gauß (1801)*)

Sei K ein Körper der Charakteristik 0. Sei q eine Primzahl. Jede q-te (primitive) Einheitswurzel ζ liegt in einer Radikalerweiterung L/K, die durch einen Körperturm

$$K = K_0 \subset K_1 \subset \cdots \subset K_{r-1} \subset K_r = L$$

gegeben ist mit $K_i = K_{i-1}(a_i)$ und $a_i \in K_i$ ist Nullstelle eines irreduziblen Polynoms $T^{p_i} - b_i \in K_{i-1}[T]$ mit $p_i < q$ prim.

Beweis. Für $q = 2$ ist die Aussage offenbar richtig. Sei $q > 2$ prim und die Aussage für kleinere Primzahlen bereits bewiesen. Nach Satz 1.3 ist $E_q(K)/K$ galoissch mit abelscher (sogar zyklischer) Galoisgruppe G, deren Ordnung $q-1$ teilt. Sei $p_1 \cdot \ldots \cdot p_r$ die Primfaktorzerlegung von $[E_q(K) : K]$. Wenden wir den Haupsatz der Galoistheorie an auf eine prim-zyklische Kompositionsreihe für G (Satz III.7.5), dann erhalten wir einen Körperturm

$$K = K_0 \subset K_1 \subset \cdots \subset K_{r-1} \subset K_r = E_q(K)$$

mit $[K_i : K_{i-1}] = p_i$ (nach evtl. Umnummerierung); die K_i/K_{i-1} sind galoissch mit zyklischer Galoisgruppe. Sei $K' = K(\zeta_1, \ldots, \zeta_r)$, mit primitiven p_i-ten Einheitswurzeln ζ_i. Per Induktionsvoraussetzung (mehrfach angewendet für jeden Primfaktor) liegt K' in einer Radikalerweiterung L_0 von der behaupteten Form. Setze $L_i := L_0(K_i)$ für $i = 1, \ldots, r$. Dann ist auch L_i/L_{i-1} galoissch mit zyklischer Galoisgruppe, deren Ordnung ein Teiler von p_i ist, also $= 1$ oder $= p_i$: Denn Einschränkung liefert einen Monomorphismus

$$\mathrm{Gal}(L_i/L_{i-1}) \to \mathrm{Gal}(K_i/K_{i-1}),$$

nach Satz VII.3.1 über natürliche Irrationalitäten. Wir erhalten einen Körperturm

$$K \subseteq L_0 \subseteq L_1 \subseteq \cdots \subseteq L_{r-1} \subseteq L_r =: L$$

Die L_i mit $[L_i : L_{i-1}] = 1$ können wir in der Aufzählung weglassen. Gilt $[L_i : L_{i-1}] = p_i$, so können wir Satz VII.2.3 anwenden, der zeigt, dass $L_i = L_{i-1}(b_i)$ ist, mit b_i eine Nullstelle eines Polynoms $T^{p_i} - a_i \in L_{i-1}[T]$. Dieses Polynom ist irreduzibel, da der Körpergrad sonst kleiner als p_i (bzw. genauer $= 1$) wäre. Es gilt $\zeta \in E_q(K) \subseteq L$. Mit der erwähnten Induktionsvoraussetzung für L_0/K folgt die Behauptung. ∎

Damit erhält man für eine Richtung in Satz VII.4.5 eine stärkere Fassung:

Satz 3.2 (*Galois*)

Sei K ein Körper der Charakteristik 0 und $f \in K[T]$. Wenn die Gruppe $\mathrm{Gal}(f/K)$ auflösbar ist, so gibt es einen Körperturm

$$K = K_0 \subset K_1 \subset \cdots \subset K_{r-1} \subset K_r = L$$

mit $K_i = K_{i-1}(a_i)$ und $a_i \in K_i$ ist Nullstelle eines irreduziblen *Polynoms $T^{p_i} - b_i \in K_{i-1}[T]$ mit p_i prim, so dass alle Nullstellen von f in L liegen.*

Aufgaben

Ü 3.1. Sei K ein Körper mit $\mathrm{Char}(K) = 0$ und $f = T^p - a \in K[T]$ mit p prim. Dann sind äquivalent:
(1) f ist irreduzibel über K.
(2) f hat keine Nullstelle in K.

[5] Vgl. §62 in van der Waerden [17], oder Corollary 12.29 und Theorem 13.3 in Tignol [16], oder Theorem 21.2 in Stewart [15]. Nach Stewart [15, §21] (auch Edwards [5, §24]) wurde dieser Satz, den Stewart *Satz von Vandermonde-Gauß* nennt, vollständig erst von Galois bewiesen, nämlich mit Hilfe seines Satzes über natürliche Irrationalitäten, vgl. Satz VII.3.1.

(3) a ist keine p-te Potenz eines Elementes in K.

(Hinweis: Für "(3)⇒(1)" untersuche man, wie sich f über dem Zerfällungskörper mit Hilfe von p-ten Einheitswurzeln in Linearfaktoren zerlegt und was das für eine nicht-triviale Zerlegung von f über K bedeuten würde.)

4. Anhang: Galoisgruppen à la Galois

Der Begriff eines Körpers wurde wohl erst von Dedekind 1871 eingeführt, wenn auch noch konkret nur aus reellen oder komplexen Zahlen bestehend, und eine allgemeine Theorie wurde erst allmählich aufgebaut durch Kronecker, Weber, Steinitz und andere. Von Weber (1893) stammt wohl die erste abstrakte Definition eines Körpers. Auch der Gruppenbegriff existierte zu Lebzeiten von Galois (1811–1832) noch nicht. Er verwendete das Wort Gruppe zwar in seinem Hauptwerk über die Auflösbarkeit von Gleichungen, aber für ihn waren dies Permutationen (von Nullstellen). Der abstrakte Begriff wurde erst von Cayley (1854) definiert. Auch der Begriff Permutation hatte damals noch nicht die heutige Bedeutung als bijektive Abbildung, sondern war eine "Auflistung" oder "Substitution" von Buchstaben (bei Galois waren diese Buchstaben Symbole für die Nullstellen eines Polynoms). Insofern ist eine interessante Frage, wie Galois selbst die Gruppe zu einer Gleichung f (bzw. $f(x) = 0$) gesehen bzw. definiert hat. Das soll hier kurz erläutert werden. Dazu wird hier mit heutigen (!) Techniken ad hoc gezeigt, dass seine Gruppe mit der heutigen Definition der Galoisgruppe übereinstimmt; Galois' mathematische Sprache war im Detail sogar noch ein wenig anders, siehe [**12**] oder [**16**].

Galois selbst betrachtete, wie man heute sagen würde, separable Körpererweiterungen L/K. Er sprach von "bekannten Größen", welche man heute als die Elemente des "Grundkörpers" K ansehen würde, und er sprach von Adjunktion von Elementen, insbesondere auch von Radikalen. Für eine Gleichung $f(x) = 0$ mit $f \in K[T]$ betrachtete er (abstrakt) die Nullstellen $\alpha_1, \ldots, \alpha_n$, wobei ohne Einschränkung angenommen wurde, dass die Nullstellen alle einfach sind; also $\operatorname{grad}(f) = n$. Insofern arbeitete er dann im Zerfällungskörper $L = K(\alpha_1, \ldots, \alpha_n)$ von f, dessen Elemente er als "Funktionen in den Nullstellen" auffasste. Der Körper der rationalen Funktionen $K(t_1, \ldots, t_n)$ spielt auch indirekt mit. Wir wissen, dass wir $\operatorname{Gal}(f/K)$ auffassen können als Untergruppe der symmetrischen Gruppe $\mathbb{S}_n$, welche auf den Nullstellen operiert qua $\sigma(\alpha_i) = \alpha_{\sigma(i)}$. Wenn man nur in Termen dieser Permutationen denkt, wie kann man beschreiben, welche Permutationen genau in der Galoisgruppe liegen? Für Galois kamen nur die in Frage, die die algebraischen Relationen zwischen den Nullstellen invariant lassen, und zudem nur die Elemente aus dem Grundkörper invariant unter allen diesen Permutationen bleiben. Galois formulierte dies (in englischer Übersetzung[6]) so:

> THEOREM. *Let an equation be given of which the m roots are a, b, c, ...*
> *There will always be a group of permutations of the letters a, b, c, ...*
> *which will enjoy the following property:*
> 1. *That every function of the roots invariant under the substitutions of this group will be rationally known;*
> 2. *Conversely, that every function of the roots that is rationally determinable will be invariant under the substitutions.*

Wir wissen, dass die heutige $\operatorname{Gal}(f/K)$ die Bedingung 1. erfüllt (wegen L/K galoissch). Aber sie erfüllt auch die Bedingung 2.: Denn jedes $x \in L$ lässt sich schreiben als $x = g(\alpha_1, \ldots, \alpha_n)$ für ein Polynom $g \in K[t_1, \ldots, t_n]$ (da alle α_i algebraisch über K sind; Folgerung V.3.3). Es ist dann $x \in K$, genau wenn $\tilde{g}(\alpha_1, \ldots, \alpha_n) = 0$ mit $\tilde{g} = g - a \in K[t_1, \ldots, t_n]$ und $a := x$. Bedingung 2. bedeutet also gerade,

[6] Neumann [**12**], Seite 113 f., "Proposition I".

dass für alle $x \in K$ und alle $\sigma \in \mathrm{Gal}(L/K)$ gilt, $\sigma(\tilde{g}(\alpha_1, \ldots, \alpha_n)) = 0$, was für K-Automorphismen ja klar ist.

Wir formulieren das nochmal um: Sei $R = K[t_1, \ldots, t_n]$ der Polynomring in n Unbestimmten über K. Sei I die Menge aller $g \in R$ mit $g(\alpha_1, \ldots, \alpha_n) = 0$; dies ist offenbar ein Ideal in R, und beschreibt gerade die (über K) *algebraischen Relationen* der Nullstellen. Einsetzen von α_i in t_i liefert $R/I \simeq K[\alpha_1, \ldots, \alpha_n] = L$. Für $\sigma \in \mathbb{S}_n$ und $g \in R$ sei $g^\sigma = g(t_{\sigma(1)}, \ldots, t_{\sigma(n)}) \in R$ und $I^\sigma = \{g^\sigma \mid g \in I\}$. Dann haben wir:

Lemma 4.1

Eine Permutation $\sigma \in \mathbb{S}_n$ liegt in $\mathrm{Gal}(f/K)$ genau dann, wenn $I^\sigma = I$.

Beweis. Sei $\sigma \in \mathrm{Gal}(L/K)$. Sei $g \in I$, etwa $g = \sum a_{(i_1,\ldots,i_n)} t_1^{i_1} \ldots t_n^{i_n}$. Dann gilt

$$0 = \sigma(0) = \sigma\left(\sum a_{(i_1,\ldots,i_n)} \alpha_1^{i_1} \ldots \alpha_n^{i_n}\right) = \sum a_{(i_1,\ldots,i_n)} \alpha_{\sigma(1)}^{i_1} \ldots \alpha_{\sigma(n)}^{i_n} = g^\sigma(\alpha_1, \ldots, \alpha_n),$$

also $g^\sigma \in I$. Gilt umgekehrt $I^\sigma = I$ für ein $\sigma \in \mathbb{S}_n$, so induziert σ durch entsprechende Permutierung der Unbestimmten einen wohldefinierten Automorphismus des Faktorrings R/I, der Elemente aus K festlässt, und damit ein Element in $\mathrm{Gal}(L/K)$. ∎

Beispiel. Sei $L = \mathbb{Q}(i, \sqrt[4]{2})$. Dies ist Zerfällungskörper des (irreduziblen) Polynoms $f = T^4 - 2$ über $K = \mathbb{Q}(i)$. Nullstellen sind $\alpha := \alpha_1 := \sqrt[4]{2}$, $\alpha_2 = i\alpha_1$, $\alpha_3 = -\alpha_1$, $\alpha_4 = -i\alpha_1$. Hier sieht man auch schon einige der algebraischen Relationen zwischen den α_i (über K): etwa liegen die Polynome $g_1 = t_1 + t_3$, $g_2 = t_2 + t_4$, $g_3 = it_1 - t_2$ in I. Man sieht, dass nur die Permutationen, die vom Zykel $\sigma = (1\,2\,3\,4)$ erzeugt werden, diese Relationen bewahren; z. B. gilt ${g_1}^\sigma = g_2$ und ${g_2}^\sigma = g_1$, sowie ${g_3}^{\sigma^{-1}} \in I$ und ${g_3}^{\sigma^{-1}} \in I$; aber z. B. liefert die Transposition $(1\,2)$ kein Element der Galoisgruppe, da z. B. ${g_3}^{(1\,2)} = it_2 - t_1 \notin I$ gilt (denn $\alpha_1 = i\alpha_2$ gilt *nicht*; – stattdessen $\alpha_1 = -i\alpha_2$). Damit ist die Galoisgruppe zyklisch von der Ordnung 4, erzeugt von $\alpha \mapsto i\alpha$ (vgl. Beispiel VI.1 (4)).

Ü 4.1. Wie im obigen Beispiel sei $L = \mathbb{Q}(i, \sqrt[4]{2})$, aber $K = \mathbb{Q}$. Durch Betrachtung der über K algebraischen Relationen der Nullstellen zeige man, dass $\mathrm{Gal}(L/K)$ erzeugt wird von den Permutationen $\sigma = (1\,2\,3\,4)$ und $\tau = (1\,2)(3\,4)$. Umgekehrt sieht man, wie durch Adjunktion des Radikals $i = \sqrt{-1}$ sich dann konkret die Galoisgruppe von f verkleinert, gemäß dem Satz über natürliche Irrationalitäten.

Die Invarianzeigenschaft von Lemma 4.1 war für Galois Anforderung bzw. Ziel, definiert hat er die Gruppe expliziter. Wir nennen sie hier $\Sigma(f)$, oder genauer $\Sigma_K(f)$.

Es existiert ein primitives Element $y \in L$ von L/K. (Vgl. auch Bemerkung und Fußnote in Abschnitt VI.14.) Es gibt[7] also $f_i \in K[T]$ mit $f_i(y) = \alpha_i$ $(i = 1, \ldots, n)$. Sei $\mu = \mathrm{MIPO}(y/K)$ mit Nullstellen $y = y_1, y_2, \ldots, y_m$. Galois definierte[8]

$$\Sigma(f) := \{\sigma_j \mid j = 1, \ldots, m\}, \text{ wobei } \sigma_j \colon \alpha_i \mapsto f_i(y_j) \text{ für alle } i = 1, \ldots, n. \tag{4.1}$$

Heute wissen wir (Bemerkung VI.1), dass die Elemente $\tau_j \colon y \mapsto y_j$ die Galoisgruppe induzieren. Mittels der Polynome f_i wird in (4.1) deren Wirkung in eine (als σ_j) auf die α_i übersetzt: $\sigma_j(\alpha_i) := f_i(\tau_j(y))$. In diesem Kontext nennt man y (oder μ) auch eine *Galoissche Resolvente* der Gleichung.

[7] Vgl. §14 in J.-P. Tignol [16]. Vieles im vorliegenden Abschnitt ist von diesem Buch inspiriert.

[8] Genau genommen waren die Elemente der Gruppe für Galois gewisse "Arrangements" der (symbolischen) Nullstellen; diese konnten durch Substitutionen (also Permutationen, die wir heute als die Elemente ansehen) ineinander überführt werden. In [16] wird das genauer erklärt.

Lemma 4.2

Jedes σ_j permutiert die Nullstellen $\alpha_1, \dots, \alpha_n$ von f. Es gilt also $\Sigma(f) \subseteq \mathbb{S}(\{\alpha_1, \dots, \alpha_n\}) = \mathbb{S}_n$.

Beweis. Es gilt $ff_i(y) = f(\sigma_1(\alpha_i)) = f(\alpha_i) = 0$, und damit $\mu \mid ff_i$. Es folgt $f(\sigma_j(\alpha_i)) = ff_i(y_j) = 0$. Gilt $\sigma_j(\alpha_i) = \sigma_j(\alpha_k)$, so folgt $f_i(y_j) = f_k(y_j)$, und mit dem vorherigen Argument auch $\alpha_i = f_i(y) = f_k(y) = \alpha_k$, und damit $i = k$. ∎

Aus der Definition (4.1) ist direkt weder klar, dass $\Sigma(f)$ eine Gruppe ist, noch, ob sie unabhängig von der Auswahl einer Galoisschen Resolventen ist. Weber[9] arbeitete heraus, dass die Galoissche Gruppe eine Untergruppe G von $\mathbb{S}_n$ und durch folgende Bedingungen (wie oben) charakterisiert ist:

(i) G enthält gerade diejenigen Permutationen wie in Lemma 4.1.
(ii) Für jedes $g \in K[t_1, \dots, t_n]$ mit $g^\sigma(\alpha_1, \dots, \alpha_n) = g(\alpha_1, \dots, \alpha_n)$ für alle $\sigma \in G$ folgt, dass $g(\alpha_1, \dots, \alpha_n) \in K$ gilt.

Proposition 4.3

Es gilt $\Sigma_K(f) = \mathrm{Gal}(f/K)$.

Es hat also $\Sigma_K(f)$ die Eigenschaften wie in Galois' oben zitierter "Proposition I".

Beweis. Sei $g \in I$, also mit

$$0 = g(\alpha_1, \dots, \alpha_n) = g(f_1(y), \dots, f_n(y)) = h(y)$$

für ein $h \in K[T]$. Es folgt $\mu \mid h$, und dann

$$g^{\sigma_j}(\alpha_1, \dots, \alpha_n) = g(f_1(y_j), \dots, f_n(y_j)) = h(y_j) = 0,$$

und damit $g^{\sigma_j} \in I$. Da dies für alle j gilt, folgt $\Sigma(f) \subseteq \mathrm{Gal}(f/K)$ aus Lemma 4.1.

Sei umgekehrt $\tau \in \mathrm{Gal}(L/K)$. Dann gibt es j mit $\tau(y) = y_j$, und für alle i folgt

$$\tau(\alpha_i) = \tau(f_i(y)) = f_i(\tau(y)) = f_i(y_j) = \sigma_j(\alpha_i),$$

also $\tau = \sigma_j$. ∎

Beispiel. Sei $f = T^4 - T^2 - 2 \in \mathbb{Q}[T]$. Die komplexen Nullstellen sind $\alpha_1 = i$, $\alpha_2 = \sqrt{2}$, $\alpha_3 = -i$ und $\alpha_4 = -\sqrt{2}$. Ein primitives Element von dem Zerfällungskörper $L = \mathbb{Q}(i, \sqrt{2})$ ist

$$y = \sqrt{i} = \frac{\sqrt{2} + i\sqrt{2}}{2}$$

(vgl. Beispiel in V.3) mit Minimalpolynom $\mu = T^4 + 1$. Die Nullstellen von μ sind $y = y_1$, $y_2 = iy$, $y_3 = -y$, $y_4 = -iy$. Man findet

$$\alpha_1 = y^2,\ \alpha_2 = 2y/(1 + y^2),\ \alpha_3 = -y^2,\ \alpha_4 = -2y/(1 + y^2).$$

Nutzt man $y^4 = -1$ aus, so ergibt eine elementare Rechnung $(1 + y^2)^{-1} = \frac{1}{2}(1 - y^2)$. Damit bekommen wir $\alpha_j = f_j(y)$ mit

$$f_1 = T^2,\ f_2 = -T^3 + T,\ f_3 = -T^2,\ f_4 = T^3 - T.$$

Gemäß (4.1) bekommt man $\sigma_1 = 1_L$,

$$\sigma_2 \colon \alpha_1 \mapsto \alpha_3,\ \alpha_2 \mapsto \alpha_4,\ \alpha_3 \mapsto \alpha_1,\ \alpha_4 \mapsto \alpha_2$$

$$\sigma_3 \colon \alpha_1 \mapsto \alpha_1,\ \alpha_2 \mapsto \alpha_4,\ \alpha_3 \mapsto \alpha_3,\ \alpha_4 \mapsto \alpha_2$$

$$\sigma_4 \colon \alpha_1 \mapsto \alpha_3,\ \alpha_2 \mapsto \alpha_2,\ \alpha_3 \mapsto \alpha_1,\ \alpha_4 \mapsto \alpha_4,$$

und damit $\sigma_3 = (2\,4)$, $\sigma_4 = (1\,3)$ und $\sigma_2 = \sigma_3\sigma_4$. Es folgt $\Sigma(f) = \langle \sigma_3, \sigma_4 \rangle \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$.

[9] Heinrich Weber, *Die allgemeinen Grundlagen der Galois'schen Gleichungstheorie*. Mathematische Annalen 43 (1893), 521–549.

Der Hauptsatz der Galoistheorie. Nach Galois' Definition (4.1) der Galoisgruppe ergeben sich der Satz VII.3.1 über natürliche Irrationalitäten (in Form der Folgerungen dort) sowie der Hauptsatz VI.9.2 (1) fast von selbst. Für Galois waren f und die (abstrakt existierenden) Nullstellen (im Zerfällungskörper L) fest gegeben. Der Körper K der "bekannten Größen" wurde vergrößert, um dementsprechend die Gruppe zu verkleinern, wie im Abschnitt VII.3 beschrieben.

Sei y eine Galoissche Resolvente der Gleichung, also ein primitives Element von L/K. Ist K'/K eine Körpererweiterung, so ist $\mu' = \mathrm{MIPO}(y/K')$ ein Teiler von $\mu = \mathrm{MIPO}(y/K)$, und die Nullstellen von μ' sind daher eine Teilmenge von denen von μ, und es ergibt sich aus (4.1) sofort, dass $G' := \Sigma_{K'}(f)$ eine Untergruppe von $G := \Sigma_K(f)$ ist, und nicht nur bis auf Isomorphie. Die Untergruppe G' von G bestimmt nach oben zitierter "Proposition I" von Galois einen Zwischenkörper K' von L/K eindeutig, nämlich als Fixkörper $L^{G'}$; die Abbildung $\Phi\colon K' \mapsto G'$ ist also injektiv.

Die Surjektivität folgt so: Ist G' eine Untergruppe von G und $K' := L^{G'}$, so gilt offenbar $G' \subseteq G'' := \Sigma_{K'}(f)$. Zu zeigen ist $G' = G''$. Angenommen, es wäre $G' \subsetneq G''$. Es ist

$$\mu' = \prod_{\sigma \in G''} (T - \sigma(y)) \in K'[T]$$

irreduzibel. Auf der anderen Seite ist y auch Nullstelle von

$$g := \prod_{\sigma \in G'} (T - \sigma(y)).$$

Da dies Polynom aufgrund der Annahme $G' \subsetneq G''$ einen kleineren Grad als μ' hat, können nicht alle Koeffizienten von g in K' liegen; andererseits liegen die Koeffizienten aber in $L^{G'} = K'$, Widerspruch. Damit ist die Abbildung $\Phi\colon K' \mapsto G'$ auch surjektiv, genauer mit $G' = \Sigma_{K'}(f)$. — Für mehr Details vgl. [**5**, §63].

Aufgaben

Ü 4.2. Sei $f \in K[T]$ irreduzibel und separabel vom Grad n. Seien $\alpha_0, \alpha_1, \ldots, \alpha_{n-1}$ die Nullstellen von f im Zerfällungskörper. Es gelte (nach evtl. Umnummerierung), dass es ein $g \in K[T]$ gibt mit $g(\alpha_i) = \alpha_{i+1 \bmod n}$ für alle $i = 0, \ldots, n-1$. Dann ergibt (4.1) $\mathrm{Gal}(f/K) \simeq \mathbb{Z}_n$, die n-elementige zyklische Gruppe.

Ü 4.3. Seien $\mathrm{Char}(K) = 0$ und $f \in K[T]$ irreduzibel von Primgrad p und mit Zerfällungskörper L. Äquivalent sind:
(1) $\mathrm{Gal}(f/K)$ ist zyklisch von der Ordnung p.
(2) $L = K(x)$ für eine (äquivalent: jede) Nullstelle x von f.

Ü 4.4. Sei $f = T^5 + T^4 - 4T^3 - 3T^2 + 3T + 1 \in \mathbb{Q}[T]$. Dann gilt:
(1) f ist irreduzibel über $\mathbb{Q}$ und alle Nullstellen sind reell.
(2) Gilt $f(\alpha) = 0$, so auch $f(\alpha^2 - 2) = 0$.
(3) $\mathrm{Gal}(f/\mathbb{Q})$ ist zyklisch von der Ordnung 5.

KAPITEL IX

Algebraische Körpererweiterungen

1. Algebraischer Abschluss

In Proposition V.3.5 wurde gezeigt, dass ein Körper *innerhalb* eines vorgegebenen Erweiterungskörpers einen algebraischen Abschluss besitzt. Es gibt aber auch einen algebraischen Abschluss eines Körpers schlechthin. Der Beweis dafür ist aber wesentlich schwieriger und benötigt das Auswahlaxiom.

Definition 1.1

Ein Körper K heisst *algebraisch abgeschlossen*, falls jedes Polynom $f \in K[T]$ vom Grad ≥ 1 eine Nullstelle in K besitzt.

Es folgt dann, dass jedes Polynom $0 \neq f \in K[T]$ vollständig in Linearfaktoren zerfällt: $f = c \cdot (T - a_1) \cdot \ldots \cdot (T - a_n)$ mit $c \in K^\times$, und $a_1, \ldots, a_n \in K$ (nicht notwendig paarweise verschieden). Offenbar gilt für einen Körper K: Genau dann ist K algebraisch abgeschlossen, wenn jedes irreduzible $f \in K[T]$ den Grad 1 hat.

Beispiele. (1) *Der Körper $\mathbb{C}$ der komplexen Zahlen ist algebraisch abgeschlossen.* Dies ist der sog. Fundamentalsatz der Algebra. Vgl. Satz VII.9.1.

(2) Der Körper $\mathbb{R}$ der reellen Zahlen ist nicht algebraisch abgeschlossen, denn z. B. hat das Polynom $T^2 + 1 \in \mathbb{R}[T]$ keine reelle Nullstelle.

Bemerkung. Für den Satz, dass jeder Körper in einem algebraischen abgeschlossenen Körper liegt, brauchen wir einige Hilfsmittel.

(1) Polynomringe $R[X_i \mid i \in I]$ in einer beliebigen "Zahl" von Unbestimmten X_i ($i \in I$), wobei I eine beliebige Indexmenge ist, also auch unendlich sein darf. In jedem Polynom kommen allerdings immer nur Monome vor, die aus nur endlich vielen der Variablen bestehen.

(2) Das Lemma von Zorn. Es ist äquivalent zum Auswahlaxiom und besagt, dass jede nichtleere (partiell) geordnete Menge $(X, \leq)$, die induktiv ist, ein maximales Element enthält. Dabei heisst induktiv, dass jede total geordnete Teilmenge L von X eine obere Schranke $s \in X$ hat (d. h. für alle $x \in L$ gilt $x \leq s$). Mit dem Lemma von Zorn zeigt man z. B. die Existenz von Basen in (beliebigen, auch nicht-endlich erzeugten) Vektorräumen. Oder die folgende Aussage[1]:

Lemma 1.2 (*Krull*)

Ist R ein (kommutativer) Ring und $I \subsetneq R$ ein Ideal, so gibt es ein maximales Ideal M mit $I \subseteq M \subsetneq R$. (Es ist dann der Faktorring R/M ein Körper; dies folgt aus II.6.6.)

Beweis. Sei $\mathcal{X}$ die Menge aller Ideale J mit $I \subseteq J \subsetneq R$. Diese Menge ist nichtleer (da sie I enthält), und induktiv geordnet: Sei $\mathcal{L} \subseteq \mathcal{X}$ total geordnet. Dann ist $S = \bigcup_{J \in \mathcal{L}} J$ ein Ideal. Es gilt $S \in \mathcal{X}$, denn $S = R$ würde $1 \in S$ und damit $1 \in J$ und $J = R$ für ein $J \in \mathcal{X}$ nach sich ziehen. Offenbar ist S eine obere Schranke für $\mathcal{L}$. Nach dem Lemma von Zorn gibt es ein maximales Element $M \in \mathcal{L}$, und es folgt die Behauptung. ∎

[1] Wolfgang Krull, *Idealtheorie in Ringen ohne Endlichkeitsbedingung.* Math. Ann. 101 (1929), 729–744.

Satz 1.3 (*Steinitz (1910)*)

Sei K ein Körper. Dann gibt es einen algebraisch abgeschlossenen Körper L, der K als Teilkörper enthält.

Beweis. Konstruiere einen Körper E_1, in dem jedes Polynom $f \in K[T]$ vom Grad ≥ 1 eine Nullstelle enthält. (Die Konstruktion geht auf Emil Artin zurück.) Für jedes solche Polynom f sei X_f eine Unbestimmte. Wir betrachten den Polynomring in diesen unendlich vielen Variablen,

$$R = K[X_f \mid f \in K[T]; \operatorname{grad}(f) \geq 1].$$

Jedes Element in R ist eine endliche Linearkombination von Monomen in den X_f [dabei kommen jeweils nur endlich viele Variablen vor]. Sei $I \subseteq R$ das Ideal, welches erzeugt wird von allen Polynomen in R von der Form $f(X_f)$ ($f \in K[T]$ vom Grad ≥ 1), also in jeweils einer ("seiner") Variablen.

Dieses Ideal I ist nicht ganz R: Sonst hätte man eine Darstellung

$$\sum_{i=1}^{n} g_i(X_1, \ldots, X_N) f_i(X_i) = 1$$

(nur endlich viele Variablen sind involviert, wobei wir abkürzend $X_i = X_{f_i}$ schreiben). In einem Zerfällungskörper E von $f = f_1 \cdot \ldots \cdot f_n$ über K haben alle Polynome f_i (für $i = 1, \ldots, n$) mindestens eine Nullstelle α_i (sogar alle). Setzt man für alle X_i dann α_i ein, so erhält man $0 = 1$, Widerspruch.

Wegen $I \subsetneq R$ gibt es nach obigem Lemma ein maximales Ideal $M \subsetneq R$, welches I enthält. Es ist dann der Faktorring $E_1 := R/M$ ein Körper. Sei $\pi\colon R \longrightarrow R/M$ die kanonische Surjektion. Mit der Inklusion $K \subseteq R$ induziert dies einen Monomorphismus $j\colon K \to E_1$. Identifikation von K mit $j(K) \subseteq E_1$ liefert dann eine Körpererweiterung E_1/K. Für jedes $f \in K[T]$ vom Grad ≥ 1 hat das Polynom $j^*(f)$ eine Nullstelle in E_1, nämlich $[X_f] \stackrel{def}{=} X_f + M$, denn: $j^*(f)([X_f]) = [f(X_f)] = [0]$, weil $f(X_f) \in I \subseteq M$.

Induktiv konstruiert man Körpererweiterungen

$$E_1 \subseteq E_2 \subseteq E_3 \subseteq \ldots,$$

so dass jedes Polynom $f \in E_n[T]$ vom Grad ≥ 1 eine Nullstelle in E_{n+1} besitzt. Definiere dann L als die Vereinigung $\bigcup_{n\geq 1} E_n$. Dies ist offenbar wieder ein Körper, und ein Polynom $f \in L[T]$ vom Grad ≥ 1 hat alle Koeffizienten in einem E_n liegend und daher eine Nullstelle in in $E_{n+1} \subseteq L$. ∎

Folgerung 1.4

Sei K ein Körper. Dann gibt es eine algebraische Körpererweiterung L/K, wobei L algebraisch abgeschlossen ist.

Beweis. Sei E/K eine Körpererweiterung, so dass E algebraisch abgeschlossen ist. Sei L die Vereinigung aller Teilerweiterungen, die algebraisch über K sind, also (in der Notation von Proposition V.3.5) $L = E_a$. Dann ist L algebraisch über K. Sei $f \in L[T]$ vom Grad ≥ 1. Dann hat f eine Nullstelle $\alpha \in E$, und nach Proposition V.3.5 ist α algebraisch über L. Nach derselben Proposition ist α auch algebraisch über K. Es folgt $\alpha \in L$. ∎

Definition 1.5

Sei K ein Körper. Ein algebraisch abgeschlossener Körper L, so dass L/K algebraisch ist, heisst ein *algebraischer Abschluss* von K. Wir schreiben dafür auch $\overline{K}$.

Nach der Folgerung besitzt also jeder Körper K einen algebraischen Abschluss $\overline{K}$. Wir zeigen nun die Eindeutigkeit eines algebraischen Abschlusses (bis auf K-Isomorphie).

Lemma 1.6 (*Fortsetzungslemma*)

Sei $\sigma\colon K \to L$ ein Monomorphismus von K in einen algebraisch abgeschlossenen Körper L. Sei $E = K(\alpha)$, wobei α algebraisch über K ist mit Minimalpolynom $f \in K[T]$. Dann ist die Anzahl der möglichen Fortsetzungen von σ auf $K(\alpha)$ gleich der Anzahl der verschiedenen Nullstellen von $\sigma^*(f)$ in L.

Beweis. Sei β eine Nullstelle von $\sigma^*(f)$ in L. Sei $x = \sum_{i=0}^{n-1} a_i\alpha^i \in K(\alpha)$. Definiere $\overline{\sigma}(x) \stackrel{def}{=} \sum_{i=0}^{n} \sigma(a_i)\beta^i$. Dies definiert einen injektiven Körperhomomorphismus $\overline{\sigma}\colon K(\alpha) \to L$ mit $\overline{\sigma}_{|K} = \sigma$ (folgt aus Satz V.2.5). Für jede andere Nullstelle β' von $\sigma^*(f)$ in L erhält man analog eine weitere Fortsetzung. Sei umgekehrt $\tau\colon K(\alpha) \to L$ eine Fortsetzung von σ. Dann ist $\beta = \tau(\alpha) \in L$, und $\sigma^*(f)(\beta) = \tau(f(\alpha)) = \tau(0) = 0$, also ist β eine Nullstelle von $\sigma^*(f) \in L[T]$. Ferner gilt für jedes $x = \sum_{i=0}^{n-1} a_i\alpha^i \in K(\alpha)$ auch

$$\tau(x) = \sum_{i=0}^{n-1} \tau(a_i)(\tau(\alpha))^i = \sum_{i=0}^{n-1} \sigma(a_i)\beta^i = \overline{\sigma}(x),$$

also $\tau = \overline{\sigma}$. ∎

Satz 1.7 (*Fortsetzungssatz (Steinitz (1910))*)

Sei E/K eine algebraische Erweiterung, sei $\sigma\colon K \to L$ ein Monomorphismus in einen algebraisch abgeschlossenen Körper L. Dann gibt es eine Fortsetzung von σ auf E.

Beweis. Sei $\mathscr{S}$ die Menge aller Paare (F, τ), wobei F ein Zwischenkörper von E/K ist und τ eine Fortsetzung von σ auf F. Für zwei solcher Paare (F, τ) und (F', τ') definiere $(F, \tau) \leq (F', \tau')$ falls $F \subseteq F'$ gilt und $\tau'_{|F} = \tau$. Es gilt $\mathscr{S} \neq \emptyset$. Diese Menge ist induktiv geordnet, denn ist $\{(F_i, \tau_i)\}$ eine total geordnete Teilmenge, so sei $F = \cup_i F_i$ und definiere τ auf F, so dass es auf F_i gleich τ_i ist. Dies ist eine obere Schranke für die total geordnete Teilmenge. Man kann dann Zorns Lemma anwenden, und erhält damit, dass $\mathscr{S}$ ein maximales Element (F, τ) enthält. Wir zeigen $F = E$. Andernfalls gäbe es ein $x \in E \setminus F$. Man kann nach dem vorherigen Lemma τ fortsetzen auf $F(x) \supsetneq F$, im Widerspruch zur Maximalität von (F, τ). ∎

Folgerung 1.8 (*Eindeutigkeit des algebraischen Abschlusses*)

Sei K ein Körper, und seien L und L' zwei algebraische Abschlüsse von K. Dann gibt es einen K-Isomorphismus $\sigma\colon L \xrightarrow{\sim} L'$.

Beweis. Da L/K algebraisch ist, gibt es nach dem vorherigen Satz eine Fortsetzung $\sigma\colon L \to L'$ von $i\colon K \to L'$, $i(x) = x$ für alle $x \in K$. Es ist nur zu zeigen, dass σ surjektiv ist. Es ist aber das Bild $\sigma(L) \simeq L$ algebraisch abgeschlossen, und L' ist algebraisch über $\sigma(L)$. Also folgt $\sigma(L) = L'$. ∎

Die Ergebnisse dieses Abschnitts, Existenz sowie die Eindeutigkeit eines algebraischen Abschlusses, wurden zuerst 1910 von Ernst Steinitz in einer grundlegenden Arbeit [14] gezeigt[2]. Dies betrifft auch viele Resultate und Konzepte in der Körpertheorie, etwa den Satz von den Zwischenkörpern, Zerfällungskörper, und die Behandlung normaler und separabler Körpererweiterungen.

[2]Steinitz (1871-1928) war bis 1910 tätig an der TH Berlin-Charlottenburg, der heutigen TU Berlin. Nach Bourbaki [3] kann Steinitz' Arbeit von 1910 als "Ursprung der heutigen Auffassung von der Algebra" angesehen werden.

Ein alternativer Beweis (siehe etwa [6] oder [11]) zum Existenzsatz eines algebraischen Abschlusses beruht auf der folgenden Kardinalitätaussage von algebraischen Erweiterungen, die auch für sich genommen interessant ist (und auch schon in [14] erwähnt wird).

Lemma 1.9

Sei L/K eine algebraische Körpererweiterung. Dann gilt für die Kardinalzahlen $|L| \leq \aleph_0|K|$. Dies bedeutet: Ist K endlich, so gilt $|L| \leq \aleph_0$; ist K unendlich, so gilt $|L| = |K|$.

Hierbei ist $\aleph_0 = |\mathbb{N}|$ die abzählbare Kardinalität; ist $|K|$ unendlich, so gilt $\aleph_0|K| = |K|$.

Beweis. Sei $\mathcal{P}_n := \{f \in K[T] \mid f \text{ normiert, } \operatorname{grad}(f) = n\}$. Dann gilt $|\mathcal{P}_n| = |K^n|$. Die Menge $\mathcal{P} = \bigcup_{n\geq 0} \mathcal{P}_n$ aller normierten Polynome über K hat Kardinalität $|\mathcal{P}| = \aleph_0|K|$ (unterscheide K endlich/unendlich). Für jedes $f \in \mathcal{P}$ sei die Reihenfolge der Nullstellen $a_1, \ldots, a_s$ in L festgelegt. Dann ist $L \to \mathcal{P} \times \mathbb{N}$, $a \mapsto (\mathrm{MIPO}(a/K), i)$, mit $a = a_i$, eine injektive Abbildung. Es folgt $|L| \leq \aleph_0|\mathcal{P}| = |\mathcal{P}|$, denn $\mathcal{P}$ ist immer unendlich. ∎

Aufgaben

Ü 1.1. Sei L/K eine algebraische Körpererweiterung und $\sigma\colon L \to L$ ein K-Monomorphismus. Dann ist σ ein K-Automorphismus.

Ü 1.2. Jeder algebraisch abgeschlossene Körper K hat unendlich viele Elemente.

Ü 1.3. Der Körper der algebraischen komplexen Zahlen ist algebraisch abgeschlossen.

Ü 1.4. Sei L/K eine algebraische Körpererweiterung. Dann gibt es einen algebraischen Abschluss $\overline{K}$ von K, von der L ein Teilkörper ist.

Ü 1.5. Sei K ein Körper. Die folgenden Aussagen sind äquivalent:
(1) K ist algebraisch abgeschlossen, d. h. jedes nicht-konstante Polynom $f \in K[T]$ hat eine Nullstelle in K.
(2) Jedes nicht-konstante Polynom $f \in K[T]$ zerfällt in $K[T]$ vollständig in Linearfaktoren.
(3) Für jede algebraische Körpererweiterung L/K gilt $L = K$.
(4) Für jede endliche Körpererweiterung L/K gilt $L = K$.
(5) Jedes irreduzible Polynom $f \in K[T]$ hat den Grad 1.

Ü 1.6. Sei L/K eine algebraische Körpererweiterung, so dass jedes irreduzible Polynom $f \in K[T]$ über L in Linearfaktoren zerfällt. Dann ist L algebraisch abgeschlossen (und daher ein algebraischer Abschluss von K).

Bemerkung. Es gilt sogar die stärkere Aussage, dass L (algebraisch über K) schon algebraisch abgeschlossen ist, wenn jedes irreduzible $f \in K[T]$ (mindestens) eine Nullstelle in L hat. Aber das ist schwieriger zu zeigen, vgl. Ü 4.22. Insbesondere folgt aus dieser stärkeren Aussage, dass E_1, der im ersten Schritt des Beweises von Satz 1.3 konstruierte Oberkörper von K, schon einen algebraischen Abschluss von K enthält.

Ü 1.7. Sei L/K eine algebraische Körpererweiterung. Dann gilt:
(1) Ist L ein algebraischer Abschluss von K, so gibt es zu jeder algebraischen Erweiterung E/K einen K-Monomorphismus $E \to L$.
(2) Gibt es umgekehrt zu jeder endlichen Erweiterung E/K einen K-Monomorphismus $E \to L$, so ist L ein algebraischer Abschluss von K.

2. Transitivität separabler Erweiterungen *

Der folgende Satz charakterisiert endliche separable Erweiterungen.

Satz 2.1 (*Anzahl der Fortsetzungen*)

Sei L/K eine endliche Körpererweiterung. Sei $i\colon K \to \overline{K}$ ein Monomorphismus (in den algebraischen Abschluss von K). Dann gibt es mindestens eine und

höchstens $[L:K]$ verschiedene Fortsetzungen $\sigma\colon L \to \overline{K}$. Es gibt genau $[L:K]$ Fortsetzungen genau dann, wenn L/K eine separable Erweiterung ist.

Beweis. Wir betrachten zunächst den separablen Fall. Per Induktion nach $n = [L:K]$. Für $n = 1$ ist die Aussage klar. Sei $n > 1$. Sei $\alpha \in L$, aber $\alpha \notin K$. Für das Minimalpolynom f von α über K hat $i^*(f)$ in $\overline{K}$ nur einfache Nullstellen. Ist $L = K(\alpha)$, so hat $i^*(f)$ genau n verschiedene Nullstellen und die Aussage folgt aus Lemma 1.6. Gilt $L \neq K(\alpha)$, so sind $L/K(\alpha)$ und $K(\alpha)/K$ nach Proposition VI.5.5 separabel und jeweils vom Grad $< n$. Wieder nach Lemma 1.6 hat i die Fortsetzungen $\tau_1, \ldots, \tau_s\colon K(\alpha) \to \overline{K} = \overline{K(\alpha)}$, wobei $s = [K(\alpha):K]$. Jedes τ_i hat per Induktionsannahme $[L:K(\alpha)]$ viele Fortsetzungen auf L, also gibt es insgesamt $[L:K(\alpha)] \cdot [K(\alpha):K] = [L:K]$ viele.

Um im allgemeinen Fall $\leq$ (und ≥ 1) zu bekommen geht man genauso per Induktion vor. Im nicht-separablen Fall findet man ein Element $\alpha \in L$, $\alpha \notin K$, welches nicht separabel über K ist. Dann hat i nach Lemma 1.6 $< [K(\alpha):K]$ viele Fortsetzungen auf $K(\alpha)$, und daher $< [L:K]$ Fortsetzungen auf L. ■

Bemerkung. Seien die Voraussetzungen und Bezeichnungen wie im Satz 2.1. Sei $j\colon K \to E$ ein weiterer Monomorphismus in einen algebraisch abgeschlossenen Körper E. Nach dem Fortsetzungssatz gibt es einen K-Isomorphismus $\varepsilon\colon \overline{K} \to L$ mit $\varepsilon \circ i = j$. Dann definiert die Zuordnung $\sigma \mapsto \varepsilon \circ \sigma =: \tau$ eine Bijektion zwischen den Fortsetzungen σ von i und den Fortsetzungen τ von j, denn $\tau_{|K} = \varepsilon\sigma_{|K} = \varepsilon i = j$. Die Anzahl der Fortsetzungen ist also unabhängig von dem Monomorphismus $i\colon K \to \overline{K}$. Diese Anzahl wird mit $[L:K]_s$ bezeichnet und heißt der *Separabilitätsgrad* von L/K. Obiger Satz (und sein Beweis) zeigt:

- $1 \leq [L:K]_s \leq [L:K]$. (Es gilt sogar $[L:K]_s \mid [L:K]$. Vgl. Übung 4.19.)
- $[L:K]_s = [L:K]$ genau dann, wenn L/K separabel ist.
- Für jeden Körperturm von endlichen Erweiterungen $K \subseteq F \subseteq L$ gilt

$$[L:K]_s = [L:F]_s \cdot [F:K]_s.$$

Daraus folgt sofort folgende Transitivitätseigenschaft für endliche Erweiterungen.

Proposition 2.2

Sei $K \subseteq F \subseteq L$ ein Körperturm mit $[L:K] < \infty$. Sind L/F und F/K separabel, so ist auch L/K separabel. ■

Proposition 2.3

Sei $L = K(a_1, \ldots, a_n)$ eine endlich algebraische Erweiterung. Sind alle a_i separabel über K, so ist L/K separabel.

Beweis. Ist $f = f_1 \cdot \ldots \cdot f_n \in K[T]$ das Produkt der Minimalpolynome der a_i, so ist der Zerfällungskörper N eine endliche Galoiserweiterung von K, insbesondere separabel über K. Dann ist auch der Zwischenkörper L separabel über K. ■

Satz 2.4 (*Transitivität separabler Erweiterungen (Steinitz)*)

Sei $K \subseteq F \subseteq L$ ein Körperturm. Sind L/F und F/K separabel, so ist auch L/K separabel.

Beweis. Sei $\alpha \in L$. Dann ist $f = \mathrm{MIPO}(\alpha/F)$ separabel. Sind $a_1, \ldots, a_n \in F$ die Koeffizienten von f, so ist α separabel über dem Körper $F_0 := K(a_1, \ldots, a_n) \subseteq F$, der endlich separabel über K ist. Da auch $F_0(\alpha)/F_0$ endlich separabel ist, folgt die Aussage aus der Transitivität endlicher separabler Erweiterungen. ■

3. Normalität *

Erinnerung. Eine algebraische Körpererweiterung L/K heisst normal, falls jedes irreduzible Polynom $f \in K[T]$, welches (mindestens) eine Nullstelle in L hat, in $L[T]$ vollständig in Linearfaktoren zerfällt. Auch in diesem allgemeinerem Kontext gibt es eine direkte Verbindung zu Zerfällungskörpern.

Beispiel. Sei $\overline{K}$ algebraischer Abschluss des Körpers K. Dann ist $\overline{K}/K$ normal.

Bemerkung. [Adjunktionen beliebig vieler Elemente] Das Konzept der Adjunktion hat man nicht nur für endlich viele Elemente, sondern für beliebige Mengen von Elementen. Sei L/K eine Körpererweiterung und $\mathscr{S} \subseteq L$ eine Teilmenge. Dann bezeichne $K[\mathscr{S}]$ den kleinsten Teilring von L, der $K \cup \mathscr{S}$ enthält. Analog bezeichne $K(\mathscr{S})$ den kleinsten Teilkörper von L, der $K \cup \mathscr{S}$ enthält. Schreibt man die Menge $\mathscr{S}$ in der indizierten Form $\mathscr{S} = \{s_i \mid i \in I\}$, so hat man einen surjektiven Ringmorphismus $\varphi\colon K[X_i \mid i \in I] \to K[s_i \mid i \in I]$ mit $\varphi(X_i) = s_i$ für alle $i \in I$ und $\varphi_{|K} = 1_K$ (universelle Eigenschaft des Polynomrings in beliebig vielen Variablen). Die Elemente in $K[\mathscr{S}]$ sind also polynomielle Ausdrücken in jeweils endlich vielen der s_i. "Brüche" von solchen sind dann die Elemente in $K(\mathscr{S})$.

Sind L, M Erweiterungskörper von K, die beide in einem gemeinsamen Oberkörper Ω liegen, so schreibt man statt $K(L \cup M)$ eher $K(L, M) = K(L)(M) = K(M)(L)$, sogar einfach nur LM. Es ist LM also der kleinste Teilkörper von Ω, der L und M enthält. Man nennt LM auch das *Kompositum* der Körper L und M (in Ω).

Ü 3.1. Sei $L = K(a_i \mid i \in I)$. Sind die a_i für $i \in I$ alle algebraisch (bzw. separabel) über K, so ist L/K algebraisch (bzw. separabel).

Zerfällungskörper einer Familie von Polynomen. Wir dehnen den Begriff des Zerfällungsköpers auf Mengen von Polynomen über K aus: sei $\mathscr{S}$ eine Familie nicht-konstanter Polynome $f \in K[T]$. Ein Körper $L \supseteq K$ heisst *Zerfällungskörper* von $\mathscr{S}$ über K, wenn gilt

- alle $f \in \mathscr{S}$ zerfallen in Linearfaktoren über L; und
- $L = K(\mathcal{N})$, wobei $\mathcal{N}$ die Vereinigung aller Nullstellen aller $f \in \mathscr{S}$ ist.

Bemerkung. Betrachtet man die ganze Situation im algebraischen Abschluss $\overline{K}$ von K, so ergibt sich ein Zerfällungskörper L von $\mathscr{S}$ über K trivial durch Adjunktion aller Nullstellen in $\overline{K}$ aller Polynome in $\mathscr{S}$; es ist dann L offenbar der kleinste Teilkörper von $\overline{K}$, über dem jedes $f \in \mathscr{S}$ in Linearfaktoren zerfällt.[3] Ist $\mathscr{S}$ endlich, so ist L/K endlich; denn L entsteht dann aus K durch Adjunktion endlich vieler über K algebraischer Elemente.

Beispiel. Ein algebraischer Abschluss $\overline{K}$ eines Körpers K ist Zerfällungskörper der Familie $\mathscr{S} = \{\mathrm{MIPO}(\alpha/K) \mid \alpha \in \overline{K}\}$.

Satz 3.1

Sei L/K eine algebraische Körpererweiterung. Äquivalent sind:

(1) *L/K ist normal.*

(2) *L ist Zerfällungskörper einer Menge $\mathscr{S}$ von nicht-konstanten Polynomen in $K[T]$.*

(3) *Ist $\overline{L}$ ein algebraischer Abschluss von L und $\tau\colon L \to \overline{L}$ ein K-Monomorphismus, so gilt $\tau(L) = L$.*

Beweis. (1)⇒(2) L ist Zerfällungskörper der Familie $\mathscr{S} = \{\mathrm{MIPO}(\alpha/K) \mid \alpha \in L\}$.

(2)⇒(3) Es ist $\tau(L)$ offenbar Zerfällungskörper der Menge $\mathscr{S}' = \{\tau^*(f) \mid f \in \mathscr{S}\}$. Da τ ein K-Monomorphismus ist, gilt $\tau^*(f) = f$ für jedes $f \in \mathscr{S}$,

[3] Der allgemeine Existenzsatz wurde 1910 von Steinitz direkt gezeigt, und er erhielt (umgekehrt) daraus als Spezialfall den Existenzsatz des algebraischen Abschlusses, wobei $\mathscr{S}$ die Menge *aller* nicht-konstanten Polynome in $K[T]$ ist. Auch die Eindeutigkeit folgt mit einer zu Satz VI.2.3 analogen Aussage. (Siehe Übung 3.3.) Steinitz nannte Existenz- und Eindeutigkeitssatz zusammen den *Fundamentalsatz der algebraischen Erweiterungen.*

also $\mathscr{S}' = \mathscr{S}$. Insbesondere ist die Menge $\mathcal{N}$ aller Nullstellen gleich. Es folgt $\tau(L) = K(\mathcal{N}) = L$.

(3)⇒(1) Sei $f \in K[T]$ irreduzibel, ohne Einschränkung normiert. Es habe f eine Nullstelle α in L. Sei $\beta \in \overline{L}$ eine weitere. Nach dem Fortsetzungslemma und -satz gibt es einen K-Monomorphismus $\sigma\colon L \to \overline{L}$ mit $\sigma(\alpha) = \beta$. Aus (3) folgt $\beta \in L$. Also zerfällt f über L. ■

Folgerung 3.2 (*Einschränkungssatz*)

Sei L/K algebraisch und $\overline{L}$ algebraischer Abschluss von L. Äquivalent sind:

(1) *L/K ist normal.*

(2) *Für jeden K-Automorphismus $\sigma\colon \overline{L} \to \overline{L}$ gilt $\sigma(L) = L$.*

(3) *Ist E/L eine beliebige Körpererweiterung und $\sigma\colon E \to E$ ein K-Automorphismus, so gilt $\sigma(L) = L$.*

Beweis. Sei $\iota\colon L \to \overline{L}$ die Inklusionsabbildung. Dann ist σ wie in (2) genau dann, wenn $\tau = \sigma\iota$ wie in (3) im Satz ist; denn τ kann nach dem Fortsetzungssatz auf $\overline{L}$ fortgesetzt werden. Dies zeigt die Äquivalenz von (1) und (2).

Es genügt, noch (1)⇒(3) zu zeigen. Sei $\sigma\colon E \to E$ ein K-Automorphismus. Sei $\alpha \in L$. Dann liegen alle Nullstellen von $f = \mathrm{MIPO}(\alpha/K)$ in L. Wegen $f(\sigma(\alpha)) = \sigma(f(\alpha)) = \sigma(0) = 0$ folgt dann auch $\sigma(\alpha) \in L$. ■

Folgerung 3.3

Seien L und M Erweiterungskörper von K, die im algebraischen Abschluss $\overline{K}$ liegen. Sind L/K und M/K normal, so ist auch das Kompositum LM/K normal.

Beweis. Es ist $\overline{K}$ auch algebraischer Abschluss des Kompositums. Ist $\sigma\colon \overline{K} \to \overline{K}$ ein K-Automorphismus, so gilt $\sigma(L) = L$ und $\sigma(M) = M$, und es folgt dann auch $\sigma(LM) = LM$. ■

Normaler Abschluss. Sei L/K eine algebraische Körpererweiterung. Ein Körper N heisst *normaler Abschluss* von L/K, wenn gilt:

- N/K ist algebraisch und eine normale Erweiterung, die L als Zwischenkörper enthält, und
- für jede normale Erweiterung M/K mit $N \supseteq M \supseteq L$ gilt $M = N$.

Bemerkung. Die Existenz eines normalen Abschlusses N von L/K folgt sofort durch den Zerfällungskörper der Menge $\mathscr{S}$ über K, wobei $\mathscr{S}$ die Menge aller Minimalpolynome der $x \in L$ über K ist. Dabei gilt offenbar:

- Ist $[L : K]$ endlich, so ist auch $[N : K]$ endlich; denn ist $L = K(x_1, \ldots, x_n)$ mit $f_i = \mathrm{MIPO}(x_i/K)$, so ist N der Zerfällungskörper von $\{f_i \mid i = 1, \ldots, n\}$ über K, welcher identisch ist mit dem Zerfällungskörper des Polynoms $f = f_1 \cdot \ldots \cdot f_n$ über K.
- Ist L/K separabel, so auch N/K. (Vgl. obige Übung 3.1.)

Proposition 3.4

Sei K perfekt und L/K algebraisch. Es gelte, dass jedes irreduzible Polynom in $K[T]$ mindestens eine Nullstelle in L hat. Dann ist L algebraisch abgeschlossen.

Beweis. Sei F ein Teilkörper von $\overline{L} = \overline{K}$, so dass F/K eine endliche Erweiterung ist. Es genügt zu zeigen, dass $F \subseteq L$ gilt. (Denn ist $x \in \overline{L}$, so ist x algebraisch über K, und $K(x)/K$ ist endlich.) Sei $N \subseteq \overline{L}$ ein normaler Abschluss von F/K. (Ohne Einschränkung kann dieser innerhalb von $\overline{L}$ gebildet werden.) Zu genügt: $N \subseteq L$. Es ist N/K endlich und normal. Da K perfekt ist, ist N/K auch separabel. Nach

dem Satz vom primitiven Element gibt es daher ein $\alpha \in N$ mit $N = K(\alpha)$. Sei $f = \mathrm{MIPO}(\alpha/K)$. Dieses irreduzible Polynom hat einerseits nach Voraussetzung eine Nullstelle $\beta \in L$, andererseits zerfällt f über N wegen der Normalität komplett in Linearfaktoren. Also gilt auch $\beta \in N$. Nun ist $K(\beta) \subseteq N$, aber da β denselben Grad wie α über K hat, folgt $N = K(\beta)$. Damit $N \subseteq L$. ∎

Bemerkung. Die Aussage gilt auch ohne die Annahme, dass K perfekt ist. Vgl. Ü 4.22.

Aufgaben

Ü 3.2. Sei L/K eine algebraische Körpererweiterung. Äquivalent sind:
(1) L/K ist normal und separabel.
(2) L ist Zerfällungskörper einer Menge $\mathscr{S}$ von nicht-konstanten, separablen Polynomen in $K[T]$.

Ü 3.3. (Isomorphismen-Erweiterungs-Theorem) [Steinitz] Sei $i\colon K \to K'$ ein Körperisomorphismus. Sei $\mathscr{S}$ eine Familie nicht-konstanter Polynome $f \in K[T]$ und L ein Zerfällungskörper von $\mathscr{S}$ über K. Sei $\mathscr{S}'$ die entsprechende Familie der Polynome $\{i^*(f) \mid f \in \mathscr{S}\}$ und L' ein Zerfällungskörper von $\mathscr{S}'$ über K'. Dann gibt es einen Isomorphismus von Erweiterungen $\sigma\colon L/K \to L'/K'$ mit $\sigma_{|K} = i$. Außerdem gilt: Ist $\alpha \in L$, und ist $\alpha' \in L'$ eine beliebige Nullstelle von $i^*(\mathrm{MIPO}(\alpha/K))$, so gibt es eine Erweiterung σ mit $\sigma(\alpha) = \alpha'$.
(Vgl. den Beweis von Satz 1.7. Ein detaillierter Beweis findet sich in [**11**, Thm. 3.20].)

Ü 3.4. Sei K ein Körper mit algebraischem Abschluss $\overline{K}$. Dann ist $\overline{K}/K$ eine normale Körpererweiterung.

Ü 3.5. Sei L/K eine Körpererweiterung. Äquivalent sind:
(1) L ist ein algebraischer Abschluss von K.
(2) L ist ein Zerfällungskörper der Menge aller nicht-konstanten Polynome in $K[T]$.

Ü 3.6. Sei L/K eine endliche Körpererweiterung und $\overline{L}$ ein algebraischer Abschluss von L. Seien $\sigma_1, \ldots, \sigma_n$ die K-Monomorphismen $L \to \overline{L}$ (mit $n \leq [L : K]$, vgl. Satz 2.1). Das Kompositum $\sigma_1(L)\sigma_2(L)\ldots\sigma_n(L)$ in $\overline{L}$ ist ein normaler Abschluss von L/K.

4. Unendliche Galoiserweiterungen *

Erinnerung. Eine algebraische Körpererweiterung L/K heisst galoissch, falls $L^{\mathrm{Gal}(L/K)} = K$ gilt.

Satz 4.1

Sei L/K algebraisch. Dann sind äquivalent:
(1) *L/K ist galoissch.*
(2) *L/K ist normal und separabel.*

Beweis. Setze $G = \mathrm{Gal}(L/K)$.

(1)⇒(2) Es gelte $L^G = K$. Sei $\alpha \in L$ und $f = \mathrm{MIPO}(\alpha/K)$. Seien $\alpha_1, \ldots, \alpha_n$ die verschiedenen Elemente aus der Menge $\{\sigma(\alpha) \mid \sigma \in G\}$; diese Menge ist endlich, weil sie aus Nullstellen (in L) von f besteht (Lemma V.2.3). Setze

$$g := \prod_{i=1}^{n}(T - \alpha_i) \in L[T].$$

Für jedes $\sigma \in G$ gilt offenbar $\sigma^*(g) = g$. Es folgt $g \in L^G[T] = K[T]$. Da f als Minimalpolynom g teilt, folgt, dass mit g auch f über L in paarweise verschiedene Linearfaktoren zerfällt.

(2)⇒(1) Sei L/K normal und separabel. Sei $\overline{K} = \overline{L}$ der algebraische Abschluss von K. Sei $\alpha \in L^G$ und $f = \mathrm{MIPO}(\alpha/K)$. Sei $\iota\colon K(\alpha) \to \overline{K}$ ein K-Monomorphismus. Dieser setzt sich fort zu einem K-Monomorphismus $\sigma\colon L \to \overline{K}$ (Fortsetzungssatz 1.7). Da L/K normal ist, folgt $\sigma(L) = L$. Also $\sigma \in G$. Wegen $\sigma(\alpha) = \alpha$ folgt, ι ist die identische Abbildung auf $K(\alpha)$. Es folgt, dass α die

einzige Nullstelle von f in $\overline{K}$ ist. Weil f separabel ist, folgt notwendig $f = T - \alpha$, und damit $\alpha \in K$. ■

Folgerung 4.2

Sei L/K galoissch und M ein Zwischenkörper. Dann ist auch L/M galoissch.

Erinnerung. Sei L/K eine Körpererweiterung mit Galoisgruppe $G = \mathrm{Gal}(L/K)$. Bezeichne mit $\mathcal{Z}$ die Menge aller Zwischenkörper M von L/K, also so, dass $K \subseteq M \subseteq L$ ein Körperturm ist. Bezeichne mit $\mathcal{U}$ die Menge aller Untergruppen von G. Wir betrachten die Abbildungen $\Phi\colon M \mapsto \mathrm{Gal}(L/M)$ und $\Psi\colon U \mapsto L^U$.

Folgerung 4.3

Sei L/K galoissch. Dann gilt. $\Psi \circ \Phi = 1_{\mathcal{Z}}$.

Bemerkung. Die analoge Aussage für $\Phi \circ \Psi$ ist im unendlichen Galoisfall allgemein nicht richtig. Es gilt $\Phi \circ \Psi(U) = \mathrm{Gal}(L/L^U) \supseteq U$. D. h. es liegen allgemein nicht alle Untergruppen von G im Bild von Φ.

Lemma 4.4

Sei L/K galoissch. Sei U eine Untergruppe von $G = \mathrm{Gal}(L/K)$. Folgende Aussagen sind äquivalent:

(1) *Es gilt $\Phi \circ \Psi(U) = U$. Das heißt $\mathrm{Gal}(L/L^U) = U$.*
(2) *Es gibt einen Zwischenkörper M von L/K mit $\Phi(M) = U$, d. h. mit $\mathrm{Gal}(L/M) = U$.*

Beweis. (1)⇒(2) Setze $M := \Psi(U)$. Dann folgt $\Phi(M) = \Phi \circ \Psi(U) = U$.
(2)⇒(1) Gilt $U = \Phi(M)$, so folgt $\Phi \circ \Psi(U) = \Phi(\Psi \circ \Phi(M)) = \Phi(M) = U$. ■

Definition 4.5

Sei L/K galoissch mit Galoisgruppe $G = \mathrm{Gal}(L/K)$. Eine Untergruppe U von G heisst *abgeschlossen*, falls eine der äquivalenten Bedingungen im Lemma erfüllt ist. Mit $\mathcal{U}^a$ bezeichnen wir die Menge der abgeschlossenen Untergruppen von G.

Bemerkung. Ist L/K endlich galoissch, so ist jede Untergruppe von $\mathrm{Gal}(L/K)$ abgeschlossen. Also $\mathcal{U}^a = \mathcal{U}$. — Dies folgt aus dem Hauptsatz der Galoistheorie, bzw. genauer, aus dem Satz von Artin.

Bemerkung. Wir bezeichnen (nicht ganz korrekt) die durch Einschränkung des Werte- bzw. Definitionsbereichs induzierten Abbildungen $\Phi\colon \mathcal{Z} \to \mathcal{U}^a$, $M \mapsto \mathrm{Gal}(L/M)$ und $\Psi\colon \mathcal{U}^a \to \mathcal{Z}$, $U \mapsto L^U$ mit den selben Buchstaben.

Es ergibt sich nun ohne weiteres:

Satz 4.6 (*Hauptsatz der unendlichen Galoistheorie*)

Sei L/K galoissch.

(1) *Die Abbildungen $\Phi\colon \mathcal{Z} \to \mathcal{U}^a$, $M \mapsto \mathrm{Gal}(L/M)$ und $\Psi\colon \mathcal{U}^a \to \mathcal{Z}$, $U \mapsto L^U$ sind ordnungsumkehrend und zueinander invers.*
(2) *Sei M ein Zwischenkörper. Es ist M/K galoissch genau dann, wenn $\mathrm{Gal}(L/M)$ ein Normalteiler in G ist. Ist dies erfüllt, so induziert Einschränkung $\sigma \mapsto \sigma_{|M}$ einen Isomorphismus*

$$\frac{\mathrm{Gal}(L/K)}{\mathrm{Gal}(L/M)} \xrightarrow{\sim} \mathrm{Gal}(M/K).$$

Proposition 4.7

Sei L/K galoissch. Dann ist L die Vereinigung aller in L liegenden endlichen *Galoiserweiterungen von K. Jeder Zwischenkörper E mit E/K endlich liegt in einem Zwischenkörper N mit N/K endlich galoissch.*

Beweis. Ist nämlich $x \in L$, so ist x algebraisch über K, also ist $K(x)/K$ endlich und separabel. Wir können den normalen Abschluss N von $K(x)/K$ im algebraischen Abschluss $\overline{L}$ von L bilden. Es ist dann N/K endlich galoissch mit $x \in N$. Zu zeigen ist noch $N \subseteq L$. Konkret wird N als Zerfällungskörper von $f = \mathrm{MIPO}(x/K)$ in $\overline{L}$ gebildet. Da f mit x eine Nullstelle in L hat und L/K normal ist, liegen alle Nullstellen von f in L, und es folgt $N \subseteq L$. Ist E/K ein endlicher Zwischenkörper, $E = K(\alpha_1, \ldots, \alpha_n)$, so ist der normale Abschluss N von E ebenfalls endlich galoissch über K. ∎

Sei L/K galoissch. Sei $\{M_i \mid i \in I\}$ eine Menge von Zwischenkörpern, wobei I geordnet ist durch $i \leq j$ genau wenn $M_i \subseteq M_j$, und so, dass zu je zwei Elementen $i, j \in I$ stets ein $k \in I$ existiert mit $i, j \leq k$. (Man nennt die Menge $(I, \leq)$ dann *gerichtet*.) Es gelte, dass alle M_i/K galoissch sind, und weiter

$$L = \bigcup_{i \in I} M_i.$$

Beispiel. Nach der Proposition sind diese Bedingungen insbesondere dann erfüllt, wenn $\{M_i \mid i \in I\}$ die Menge *aller* Zwischenkörper mit M_i/K *endlich* galoissch ist; zur Gerichtetheit: für M_k nimmt man etwa das Kompositum M_iM_j in L, denn M_iM_j/K ist endlich galoissch.

Weil M_i/K normal ist, hat man einen Einschränkungsmorphismus $\rho_i\colon \mathrm{Gal}(L/K) \to \mathrm{Gal}(M_i/K)$, der surjektiv ist, weil auch L/M_i normal ist. (Z. B. erweitere man zunächst auf $\overline{L}$ und schränke dann auf L ein.) Gilt $M_i \subseteq M_j$, so hat man ebenso einen Einschränkungsmorphismus $\rho_{ij}\colon \mathrm{Gal}(M_j/K) \to \mathrm{Gal}(M_i/K)$, und es gilt $\rho_{ij} \circ \rho_j = \rho_i$. Dies definiert ein sog. inverses System (ρ_{ij}) von Morphismen zwischen Gruppen der Form $\mathrm{Gal}(M_i/K)$ $(i \in I)$, und es gibt daher einen natürlichen Morphismus von Gruppen

$$\rho\colon \mathrm{Gal}(L/K) \to \varprojlim_{i \in I} \mathrm{Gal}(M_i/K), \quad \sigma \mapsto \big(\rho_i(\sigma)\big)_{i \in I}, \tag{4.1}$$

wobei der sog. (inverse oder) projektive Limes definiert ist als die Teilmenge (und ist dann eine Untergruppe) in der Produktgruppe $\prod_i \mathrm{Gal}(M_i/K)$, bestehend aus den Tupeln $(\sigma_i)_{i \in I}$, für die stets

$$\rho_{ij}(\sigma_j) = \sigma_i \quad \text{für } i \leq j \tag{4.2}$$

gilt. Der Kern von ρ ist trivial, denn ein Element im Kern ist die Identität auf jedem M_i, ist also die Identität auf L wegen $L = \bigcup_{i \in I} M_i$.

Satz 4.8

In (4.1) ist ρ ein Isomorphismus.

Beweis. Es ist nur noch die Surjektivität zu zeigen. Ist ein Tupel $(\sigma_i)_{i \in I}$ gegeben, das alle Bedingungen (4.2) erfüllt, so sei $\sigma := \rho_i^{-1}(\sigma_i)$. Wegen der Injektivität ist das Urbild eindeutig, und wegen (4.2) ist es unabhängig von i. Es gilt dann $\rho(\sigma) = (\sigma_i)_{i \in I}$. ∎

Bemerkung. In der vorherigen Klasse von Beispielen sind die Galoisgruppen $\mathrm{Gal}(M_i/K)$ sogar endlich. Als projektiver Limes endlicher Gruppen sagt man deswegen auch, dass $\mathrm{Gal}(L/K)$ *profinit* ist (für jede Galoiserweiterung L/K).

Bemerkung. Es folgt für L/K galoissch: Genau dann ist $\mathrm{Gal}(L/K)$ abelsch, wenn alle $\mathrm{Gal}(M/K)$ abelsch sind, für jeden Zwischenkörper M mit M/K (endlich) galoissch.

Satz 4.9 (*Natürliche Irrationalitäten*)

Sei L/K eine Galoiserweiterung und M/K eine beliebige Körpererweiterung. Sei $ML = M(L)$ gebildet in einem gemeinsamen Oberkörper Ω. Dann gilt:

(1) *ML/M ist galoissch.*

(2) *Einschränkung $\sigma \mapsto \sigma_{|L}$ induziert einen Gruppenisomorphismus*

$$\theta\colon \mathrm{Gal}(ML/M) \xrightarrow{\sim} \mathrm{Gal}(L/L\cap M).$$

Siehe Grafik VII.(3.1).

Beweis. (1) Dass ML/M galoissch ist, folgt wie in der endlichen Version des Satzes, nur dass man hier Mengen von Polynomen betrachten muss: L ist Zerfällungskörper einer Menge $\mathscr{S}$ von separablen Polynomen in $K[T]$, also $L = K(\mathcal{N})$, wobei $\mathcal{N}$ die Menge der gesamten Nullstellen ist. Die Polynome in $\mathscr{S}$ sind natürlich erst recht Polynome im $M[T]$, und auch separabel über M. Es ist dann offenbar $ML = M(\mathcal{N})$ Zerfällungskörper von $\mathscr{S}$ über M.

(2) Die Injektivität von θ folgt wörtlich wie im Beweis von Satz VII.3.1.

(3) Die Surjektivität ist schwieriger zu zeigen. Wir wissen dies bereits im Spezialfall, wenn L/K endlich ist. Für den unendlichen Fall nehmen wir jetzt ohne Einschränkung an, dass $K = L\cap M$ gilt. Sei $\mathcal{N}_i$ eine beliebige endliche Teilmenge der Nullstellenmenge $\mathcal{N}$, die abgeschlossen ist unter Konjugierten (d. h. mit $\alpha \in \mathcal{N}_i$ enthält $\mathcal{N}_i$ auch alle anderen Nullstellen von $\mathrm{MIPO}(\alpha/K)$). Setze $L_i = K(\mathcal{N}_i)$ und $ML_i = M(\mathcal{N}_i)$. Dann sind L_i/K und ML_i/M endlich galoissch. Einschränkung auf L_i liefert daher Isomorphismen $\theta_i\colon \mathrm{Gal}(ML_i/M) \to \mathrm{Gal}(L_i/K)$. Durchläuft $\mathcal{N}_i$ für eine Indexmenge I alle endlichen Teilmengen von $\mathcal{N}$, so gilt $\mathcal{N} = \bigcup_{i\in I}\mathcal{N}_i$ und daher $L = \bigcup_{i\in I} L_i$, sowie $ML = \bigcup_{i\in I} ML_i$. Wir erhalten also wie oben beschrieben Isomorphismen

$$\rho\colon \mathrm{Gal}(L/K) \xrightarrow{\sim} \varprojlim \mathrm{Gal}(L_i/K)$$

und

$$\rho'\colon \mathrm{Gal}(ML/M) \xrightarrow{\sim} \varprojlim \mathrm{Gal}(ML_i/M).$$

Wir verwenden weiterhin obige Bezeichnungen für die (Einschränkungs-) Morphismen ρ_i, ρ_{ij}, und analog ρ'_i, ρ'_{ij}. Zudem gibt es noch die Isomorphismen θ_i. Da es sich bei all diesen Abbildungen um Einschränkungen handelt, sieht man leicht, dass zwischen ihnen folgende Beziehungen gelten:

$$\theta_i \circ \rho_i = \rho'_i \circ \theta,\ \theta_i \circ \rho_{ij} = \rho'_{ij} \circ \theta_j.$$

Definieren wir nun die Abbildung $\varprojlim \theta_i$ durch $(\sigma_i)_{i\in I} \mapsto (\theta_i(\sigma_i))_{i\in I}$, so sieht man unmittelbar, dass dies einen Isomorphismus zwischen den beiden projektiven Limiten ergibt, und dass $\varprojlim \theta_i \circ \rho = \rho' \circ \theta$ gilt. Denn für jedes $\sigma \in \mathrm{Gal}(ML/M)$ ist

$$\varprojlim \theta_i \circ \rho(\sigma) = \varprojlim \theta_i((\rho_i(\sigma))_i) = (\theta_i\rho_i(\sigma))_i = (\rho'_i\theta(\sigma))_i = \rho'(\theta(\sigma)) = \rho' \circ \theta(\sigma).$$

Da nun ρ, ρ' und $\varprojlim \theta_i$ allesamt Isomorphismen sind, folgt dies auch für θ, was den Beweis beendet. ∎

Bemerkung. Ist im Satz L/K zusätzlich endlich, so gilt dies auch für ML/M.

Bemerkung. [Krull-Topologie] Sei L/K galoissch. Auf der Gruppe $G = \mathrm{Gal}(L/K)$ kann man eine Topologie definieren, die sog. *Krull-Topologie*[4]. G wird dann zu einer *topologischen Gruppe*, d. h. Multiplikation und Inversenbildung in G sind stetige Abbildungen. Wir skizzieren dies hier kurz. Ist $S \subseteq L$ eine endliche Teilmenge, dann ist $\overline{S} := \bigcup_{\sigma\in G} \sigma S$ ebenfalls endlich und G-stabil. Sei $V(S) := \{\sigma \in G \mid$

[4]Wolfgang Krull: *Galoissche Theorie der unendlichen algebraischen Erweiterungen.* Math. Ann. 100 (1928), 687–698.

$\sigma(s) = s$ für alle $s \in S\}$. Es gilt $V(\overline{S}) = \bigcap_{\sigma\in G} V(\sigma S)$. Ferner gilt offenbar $V(S) = V(K(S)) := \{\sigma \in G \mid \sigma(x) = x$ für alle $x \in K(S)\}$. Sicher gilt $1 = 1_K \in V(\overline{S})$. Man kann zeigen, dass es genau eine Topologie auf G gibt, die *Krull-Topologie*, so dass die Mengen $V(S)$ bzw. (vgl. Proposition 4.7) $V(\overline{S})$ ($S \subseteq L$ endlich) eine offene Umgebungsbasis der 1 bilden. Das heisst, jede offene Menge in G, die 1 enthält, enthält als Teilmenge ein $V(S)$. Die Teilmengen der Form $\sigma V(S)$ bilden dann eine offene Umgebungsbasis von $\sigma \in G$. Es gilt also:

Eine Teilmenge $A \subseteq G$ ist offen genau dann, wenn es zu jedem $\sigma \in A$ eine endliche Menge $S \subseteq L$ gibt mit $\sigma V(S) \subseteq A$.

(Für mehr Details vgl. Ü 4.3.) Insbesondere sind alle Teilmengen der Form $A = \sigma V(S)$ offen (man nimmt für jedes $\tau \in A$ dasselbe S), und daher insbesondere die Linksnebenklassen der Form $\sigma\,\mathrm{Gal}(L/E)$ (E/K endlich, $\sigma \in G$). Da der Index $[G : \mathrm{Gal}(L/E)]$ endlich ist, gibt es in $G \setminus \sigma\,\mathrm{Gal}(L/E)$ nur endlich viele Linksnebenklassen. Diese sind also alle auch abgeschlossen. Es folgt dann, dass für jeden Zwischenkörper M von L/K auch $\mathrm{Gal}(L/M) = \bigcap_{S\subseteq M} \mathrm{Gal}(L/K(S))$ (alle S endlich) als Durchschnitt abgeschlossener Mengen abgeschlossen ist. Auf der anderen Seite gilt, dass der topologische Abschluss einer Untergruppe H von G gegeben ist durch $\mathrm{Gal}(L/L^H)$; vgl. nachfolgendes Lemma. Also:

[Krull] *Eine Untergruppe ist topologisch abgeschlossen in G genau dann, wenn sie die Eigenschaften aus der (ad hoc) Definition 4.5 besitzt.*

Die obigen surjektiven Einschränkungsmorphismen $\rho_i \colon G \to \mathrm{Gal}(M_i/K)$ (M_i/K galoissch), sind stetig, denn das Urbild von der abgeschlossenen Teilmenge $\{1_E\}$ ist jeweils gerade $\mathrm{Gal}(L/M_i)$, also abgeschlossen. Die obigen projektiven Limiten erhalten jeweils die durch die sog. Produkttopologie induzierte Topologie. Alle Morphismen ρ_i, ρ_{ij} und auch ρ und θ sind dann stetige Abbildungen, und ρ und θ damit sogar sog. Isomorphismen von topologischen Gruppen. Letzteres gilt auch für den Isomorphismus im Hauptsatz. — In den Formulierungen und Beweisen obiger Resultate haben wir von diesen topologischen Dingen keinen Gebrauch gemacht. (Im vorigen Beweis kamen ein paar davon implizit vor, ohne sie zu benennen.) Für mehr Details vergleiche etwa [**2**], [**11**] oder [**3**]. —

Ausgehend von Satz 4.8 kann man aber auch umgekehrt vorgehen und die Krull-Topologie "abstrakt" definieren: stattet man endliche (Galois-) Gruppen mit der diskreten Topologie aus (d. h. alle Teilmengen sind offen), so induziert die Produkttopologie (mit Hilfe des Isomorphismus' (4.1)) eindeutig eine Topologie auf der Gruppe $\mathrm{Gal}(L/K)$, und ρ ist dann automatisch stetig. Diese Topologie ist mit der Krull-Topologie identisch. Man erhält z. B. auch, dass die topologische Gruppe $\mathrm{Gal}(L/K)$ profinit sowie (vgl. Satz von Tychonoff aus der Topologie) hausdorffsch und kompakt ist.

Lemma 4.10

Sei L/K galoissch und H eine Untergruppe von $G = \mathrm{Gal}(L/K)$. Sei $\overline{H}$ der Abschluss von H in G, d. h. die kleinste abgeschlossene Untergruppe von G, die H enthält. Dann gilt:

(1) $\overline{H} = \mathrm{Gal}(L/L^H)$.

(2) $\overline{H} = \bigcap_E \mathrm{Gal}(L/E \cap L^H) = \bigcap_E H \cdot \mathrm{Gal}(L/E)$, *wobei E die Zwischenkörper von L/K mit E/K endlich galoissch durchläuft.*

(3) *Gilt $H \lhd G$, so auch $\overline{H} \lhd G$.*

Die Aussagen gelten sowohl mit "abgeschlossen" wie in 4.5 als auch in der Krull-Topologie. Die Konzepte stimmen also überein.

Beweis. (1) Offensichtlich ist $H \subseteq \mathrm{Gal}(L/L^H)$, und $\mathrm{Gal}(L/L^H)$ ist nach Definition abgeschlossen. Sei $U < G$ abgeschlossen, gemäß 4.5, also von der Form $U = \mathrm{Gal}(L/M)$ für einen Zwischenkörper M von L/K, und es gelte $H \subseteq U$. Dann hält jedes $\sigma \in H$ jedes $x \in M$ fest. Es folgt $M \subseteq L^H$, und damit $\mathrm{Gal}(L/L^H) \subseteq \mathrm{Gal}(L/M) = U$.

(2) Zunächst ist beliebiger Durchschnitt abgeschlossener Untergruppen auch gemäß Definition 4.5 abgeschlossen: denn $\bigcap_{i\in I}\mathrm{Gal}(L/M_i)=\mathrm{Gal}\big(L/K(\bigcup_{i\in I}M_i)\big)$. Daher ist der Durchschnitt über alle $\mathrm{Gal}(L/M)$, wobei M ein Zwischenkörper von L/K ist und $H\subseteq\mathrm{Gal}(L/M)$ gilt, die kleinste abgeschlossene Untergruppe von G, die H enthält; mit (1) folgt, dass all diese M in L^H liegen, und L^H das Kompositum all dieser M ist. Da L/K algebraisch ist, genügt es, nur solche M mit M/K endlich zu betrachten, oder wegen Proposition 4.7 sogar nur $E\cap L^H$ mit endlich galoisschen E/K, denn es ist $\mathrm{Gal}(L/E\cap L^H)\supseteq H\cdot\mathrm{Gal}(L/E)\supseteq H$.

Wir zeigen nun (1) für den topologischen Abschluss. Nach obiger Beschreibung der offenen Teilmengen von G ist der topologische Abschluss $\overline{H}$ von H gegeben durch alle $\sigma\in G$, so dass für alle Zwischenkörper E von L/K mit E/K endlich galoissch, $E=K(S)$, gilt $\sigma V(S)\cap H\neq\emptyset$, d. h. es existiert ein $\tau\in H$ mit $\tau_{|E}=\sigma_{|E}$. (Es folgt dann $\sigma=\tau\cdot(\tau^{-1}\sigma)\in H\cdot\mathrm{Gal}(L/E)$, und damit die zweite Gleichheit in (2).) Einschränkung auf E liefert einen Morphismus $H\xrightarrow{\rho}\mathrm{Gal}(E/E\cap L^H)<\mathrm{Gal}(E/K)$. Sei H_0 das Bild von ρ. Wegen $E^{H_0}=L^H\cap E$ folgt aus dem endlichen Hauptsatz $H_0=\mathrm{Gal}(E/L^H\cap E)$. — Wir zeigen nun, dass $\mathrm{Gal}(L/L^H)$ im topologischen Abschluss von H liegt; es folgt dann (1). Sei $\sigma\in\mathrm{Gal}(L/L^H)$ und E ein Zwischenkörper wie zuvor. Wegen $\sigma_{|E}\in\mathrm{Gal}(E/L^H\cap E)$ gibt es ein $\tau\in H$ mit $\tau_{|E}=\sigma_{|E}$. Also liegt σ im topologischen Abschluss von H.

(3) Für jedes $\sigma\in G$ gilt $\sigma\,\mathrm{Gal}(L/L^H)\sigma^{-1}=\mathrm{Gal}(L/\sigma(L^H))=\mathrm{Gal}(L/L^{\sigma H\sigma^{-1}})$ $=\mathrm{Gal}(L/L^H)$. ∎

Ü 4.1. Mit der Notation des Lemmas gilt für die Fixkörper $L^H=L^{\overline{H}}$.

Ü 4.2. Sei L/K galoissch mit Galoisgruppe G und M ein Zwischenkörper und $U=\mathrm{Gal}(L/M)$. Es ist U offen in der Krull-Topologie von G genau dann, wenn M/K endlich ist. Wenn dies gilt, so ist der Index $[G:U]$ endlich und gleich dem Grad $[M:K]$.

Ü 4.3. [Umgebungsbasen und induzierte Topologie] Sei X eine Menge, $x\in X$ und $\emptyset\neq\mathcal{B}(x)\subseteq 2^X$. Es heisst $\mathcal{B}(x)$ eine *Umgebungsbasis* von x, falls $x\in B$ gilt für alle $B\in\mathcal{B}$, und falls für alle $B_1,B_2\in\mathcal{B}(x)$ ein $B\in\mathcal{B}(x)$ existiert mit $B\subseteq B_1\cap B_2$. Es ist dann $\mathcal{F}(x)=\{V\subseteq X\mid\text{es gibt }B\in\mathcal{B}(x)\text{ mit }V\supseteq B\}$ ein sog. *Umgebungsfilter* von x. Die $V\in\mathcal{F}(x)$ heißen *Umgebungen* von x. Wir nennen die $\mathcal{F}(x)$ ein *System offener Umgebungsfilter*, wenn zusätzlich folgendes gilt: zu jedem $x\in X$ und zu jedem $V\in\mathcal{F}(x)$ gibt es $W\in\mathcal{F}(x)$ mit $W\subseteq V$ und so, dass für jedes $y\in W$ gilt, dass $W\in\mathcal{F}(y)$ ist. Ist dies der Fall, so induziert dies eine Topologie $\mathcal{T}$ auf X, indem definiert wird, dass $U\subseteq X$ *offen* ist genau dann, wenn für alle $x\in U$ gilt, dass $U\in\mathcal{F}(x)$ ist. D. h. das System $\mathcal{T}$ der offenen Teilmengen von X erfüllt folgende Eigenschaften: (i) $\emptyset$, $X\in\mathcal{T}$; (ii) Durchschnitte endlich vieler offener Mengen sind offen; (iii) Vereinigungen offener Mengen über beliebige Indexmengen sind offen. — Per definitionem sind die *abgeschlossenen* Teilmengen von X gerade die Komplemente der offenen Mengen. Ferner gilt $V\in\mathcal{F}(x)$ genau dann, wenn es $U\in\mathcal{T}$ gibt mit $x\in U\subseteq V$ (also V im Sinne der Topologie $\mathcal{T}$ eine Umgebung von x ist).

Sei L/K galoissch mit Galoisgruppe G. Sei $\tau\in G$. Dann ist das System $\mathcal{B}(\tau)=\{\tau V(E)\mid E/K\text{ endl. galoissch}\}$ eine Umgebungsbasis von τ. Dabei gilt $\tau V(E)=\{\sigma\in G\mid\sigma_{|E}=\tau_{|E}\}$, jedes $V(E)$ ist eine Untergruppe von G, und für $\sigma\in G$ gilt $\sigma\in\tau V(E)$ genau wenn $\sigma V(E)=\tau V(E)$. Wir erhalten also ein System offener Umgebungsfilter. Es definiert $\mathcal{B}'(\tau)=\{\tau V(E)\mid E/K\text{ endlich}\}$ ebenfalls eine Umgebungsbasis von τ, die zu denselben Umgebungsfiltern führt.

Wir kommen nun zu einigen Beispielen unendlicher Galoiserweiterungen.

Beispiel. [Die absolute Galoisgruppe eines Körpers] Sei $\overline{K}$ algebraischer Abschluss des Körpers K. Die Menge der Elemente in $\overline{K}$, die separabel über K sind, bilden einen Teilkörper $\overline{K}^s$ von $\overline{K}$, den *separablen (algebraischen) Abschluss* von K. (Ist K perfekt, so gilt natürlich $\overline{K}^s=\overline{K}$.) Die Erweiterung $\overline{K}^s/K$ ist galoissch. Man nennt $\mathrm{Gal}(\overline{K}^s/K)$ die *absolute Galoisgruppe* von K. — Vgl. Übungen, etwa Ü 4.25.

Bemerkung. [Das Umkehrproblem der Galoistheorie] In der Zahlentheorie und auch bei dem sog. Umkehrproblem der Galoistheorie spielt die absolute Galoisgruppe $\Gamma = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ von $\mathbb{Q}$ eine wichtige Rolle. Das klassische *Umkehrproblem der Galoistheorie*, formuliert 1892 von David Hilbert, lautet:

Gibt es zu jeder endlichen Gruppe G eine (endliche) Galoiserweiterung $L/\mathbb{Q}$ mit Galoisgruppe $\mathrm{Gal}(L/\mathbb{Q}) \simeq G$*?*

Dieses Problem ist noch heute nicht vollständig gelöst. Man kann es äquivalent folgendermaßen formulieren:

Ist jede endliche Gruppe (ausgestattet mit der diskreten Topologie) ein stetiger Quotient der absoluten Galoisgruppe Γ (ausgestattet mit der Krull-Topologie)?

Denn wir haben ja gesehen, dass für jede endliche Galoiserweiterung $L/\mathbb{Q}$ die Galoisgruppe $\mathrm{Gal}(L/\mathbb{Q})$ Bild eines (stetigen) Gruppenmorphismus ist. Ist G endliche Gruppe und $\Gamma \to G$ surjektiver, stetiger Morphismus, so ist der Kern abgeschlossen, also von der Form $\mathrm{Gal}(\overline{\mathbb{Q}}/L)$, und da der Kern ein Normalteiler ist, folgt aus obigem Hauptsatz, dass $L/\mathbb{Q}$ galoissch ist mit $\mathrm{Gal}(L/\mathbb{Q}) \simeq G$.

Beispiel. [Die absolute Galoisgruppe endlicher Körper] Sei $\mathbb{F}_q$ der Körper mit $q = p^n$ Elementen (p Primzahl, $n \geq 1$). Sei $\overline{\mathbb{F}_q}$ $(= \overline{\mathbb{F}_p}^s)$ der algebraische Abschluss. Dabei werden die endlichen Körpererweiterungen $\mathbb{F}_{q^i}$ als eingebettet in $\overline{\mathbb{F}_q}$ und mit $\mathbb{F}_{q^i} \subseteq \mathbb{F}_{q^j}$ (falls $i \mid j$) verstanden. Es ist also $\overline{\mathbb{F}_q}$ die Vereinigung aller $\mathbb{F}_{q^j}$ $(j \geq 1)$. Da die $\mathbb{F}_{q^i}$ die einzigen endlichen Erweiterungen von $\mathbb{F}_q$ in $\overline{\mathbb{F}_q}$ sind, und auch galoissch, erhält man

$$\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q) \simeq \varprojlim_{i \geq 1} \mathrm{Gal}(\mathbb{F}_{q^i}/\mathbb{F}_q) \simeq \varprojlim_{i \geq 1} \mathbb{Z}/i\mathbb{Z} =: \widehat{\mathbb{Z}}.$$

Hierbei ist der projektive Limes ganz rechts gegeben durch die Tupel aller Restklassen modulo i, die kompatibel sind mit allen kanonischen surjektiven Morphismen $\mathbb{Z}/j\mathbb{Z} \to \mathbb{Z}/i\mathbb{Z}$, $k+j\mathbb{Z} \mapsto k+i\mathbb{Z}$ (für alle $i \mid j$). Die n-te Potenz des Frobenius-Automorphismus', also $\sigma_q \colon x \mapsto x^q$ auf der linken Seite entspricht dabei dem Element $([1]_1, [1]_2, [1]_3, \dots)$ auf der rechten.

Beispiel. Sei $a \geq 2$ eine fest gewählte Primzahl. Sei $K = \mathbb{F}_q$ mit algebraischem Abschluss wie oben. Sei darin $L = \bigcup_{i \geq 0} \mathbb{F}_{q^{a^i}}$. Dann ist L/K galoissch mit $\mathrm{Gal}(L/K) \simeq \varprojlim_{i \geq 0} \mathbb{Z}/a^i\mathbb{Z}$. Sei E ein Zwischenkörper von L/K mit $E \neq L$. Dann gibt es ein $k \geq 0$ mit $E = \mathbb{F}_{q^{a^k}}$. (Insbesondere: $[L : K] = \infty$, aber alle echten Zwischenkörper sind endlich.)

Denn sei $m \geq 1$ minimal, so dass ein $x \in L \setminus E$ existiert, wobei $[K(x) : K] = a^m$. Dann gilt $\mathbb{F}_{q^{a^i}} \not\subseteq E$ für alle $i \geq m$. Setze $n = m - 1$. Dann $\mathbb{F}_{q^{a^n}} \subseteq E$. Ist umgekehrt $y \in E$, dann ist $y \in \mathbb{F}_{q^{a^j}}$ mit $a^j = [K(y) : K]$, und es gilt $E \supseteq K(y) = \mathbb{F}_{q^{a^j}}$. Nach dem Argument zuvor muss $j < m$ gelten. Also $E \subseteq \mathbb{F}_{q^{a^n}}$, und daher $E = \mathbb{F}_{q^{a^k}}$ für ein k mit $0 \leq k \leq n$. Die Berechnung der Galoisgruppe ist klar. Da mit jedem $x \in L$ auch alle seine Konjugierten eine Potenz von a als Grad über K haben, ist L/K galoissch.

Beispiel. [Körper der konstruierbaren Zahlen] Sei $\widehat{\mathbb{Q}} = K(\{0, 1\})$ der Körper der konstruierbaren komplexen Zahlen. Die Erweiterung $\widehat{\mathbb{Q}}/\mathbb{Q}$ ist galoissch: denn es folgt aus dem ersten Beweisteil von Satz VII.8.1, dass mit einer konstruierbaren Zahl z auch alle weiteren Nullstellen seines Minimalpolynoms konstruierbar sind. Definierte man induktiv $K_0 = \mathbb{Q}$ und $K_{n+1} = K_n(\sqrt{\alpha} \mid \alpha \in K_n) \subset \widehat{\mathbb{Q}}$, so gilt

$$\mathbb{Q} = K_0 \subset K_1 \subset \ldots \subset K_n \subset K_{n+1} \subset \ldots \subset \widehat{\mathbb{Q}}$$

und $\widehat{\mathbb{Q}} = \bigcup_{n \geq 0} K_n$. Es gilt außerdem, dass jedes K_n/K_0 galoissch ist. Denn angenommen, es ist schon K_n/K_0 galoissch gezeigt. Sei $\sigma \colon \widehat{\mathbb{Q}} \to \widehat{\mathbb{Q}}$ ein $\mathbb{Q}$-Automorphismus. Dieser kann auf den algebraischen Abschluss erweitert werden. Nach Einschränkungssatz und Induktionsannahme gilt $\sigma(K_n) = K_n$. Um $\sigma(K_{n+1}) = K_{n+1}$ zu zeigen, genügt es, $\sigma(\sqrt{\alpha}) \in K_{n+1}$ einzusehen (für $\alpha \in K_n$). Dies folgt aber sofort aus $\sigma(\sqrt{\alpha}) = \pm\sqrt{\sigma(\alpha)} \in K_{n+1}$. Es folgt, dass auch K_{n+1}/K_0 normal, also galoissch ist.

Dies ergibt nun

$$\mathrm{Gal}(\widehat{\mathbb{Q}}/\mathbb{Q}) \simeq \varprojlim_{n\geq 0} \mathrm{Gal}(K_n/\mathbb{Q}),$$

wobei der projektive Limes aus denjenigen Tupeln $(\sigma_n)_{n\geq 0} \in \prod_{n\geq 0} \mathrm{Gal}(K_n/\mathbb{Q})$ besteht, so dass $\sigma_{n+1|K_n} = \sigma_n$ für alle $n \geq 1$ gilt.

Wir wollen $\mathrm{Gal}(\widehat{\mathbb{Q}}/\mathbb{Q})$ noch als projektiven Limes von *endlichen* Galoisgruppen darstellen. Zwar wissen wir aus der Proposition, dass dies abstrakt möglich ist. Aber wir wollen dies hier expliziter durchführen. Zunächst ist offenbar $\widehat{\mathbb{Q}} \subseteq \overline{\mathbb{Q}}$ abzählbar. Wir können also schreiben $\widehat{\mathbb{Q}} = \mathbb{Q}(a_i \mid i \in \mathbb{N})$. Sei $L_n = \mathbb{Q}(a_1, \ldots, a_n)$ und M_n ein normaler Abschluss von $L_n/\mathbb{Q}$ in $\overline{\mathbb{Q}}$. Da $\widehat{\mathbb{Q}}/\mathbb{Q}$ normal ist und L_n enthält, folgt $M_n \subseteq \widehat{\mathbb{Q}}$. Es ist M_n/K *endlich galoissch*, und es gilt $M_n \subseteq M_{n+1}$, sowie $\widehat{\mathbb{Q}} = \bigcup_{n\geq 1} M_n$. Es gilt also

$$\mathrm{Gal}(\widehat{\mathbb{Q}}/\mathbb{Q}) \simeq \varprojlim_{n\geq 0} \mathrm{Gal}(M_n/\mathbb{Q}).$$

Die Ordnungen der $\mathrm{Gal}(M_n/\mathbb{Q})$ bilden für $n = 1, 2, \ldots$ eine aufsteigende Kette von 2-er Potenzen: Denn es folgt leicht, dass M_n das Kompositum $N_1 N_2 \ldots N_n$ ist, wobei N_i normaler Abschluss von $K(\alpha_i)/K$ ist. Induktiv folgt dann mit dem Satz über natürliche Irrationalitäten (endliche Version), dass $[M_n : K] \mid \prod_{i=1}^{n} [N_i : K]$ gilt. Nach Satz VII.8.1 ist jedes $[N_i : K]$ eine 2-er Potenz, und es folgt die Behauptung.

Beispiel. [Maximale abelsche Erweiterung eines Körpers] Sei $\overline{K}^s$ separabler Abschluss des Körpers K, und $G = \mathrm{Gal}(\overline{K}^s/K)$ die absolute Galoisgruppe von K. Sei G' die derivierte Untergruppe von G; vgl. Ü III.7.11. Dann heisst der Fixkörper K^{ab} von G' in $\overline{K}^s$ die *maximale abelsche Erweiterung* von K. Denn es gilt:

(i) *K^{ab}/K ist eine abelsche Erweiterung.*
(ii) *Ist L/K^{ab} eine Erweiterung, so dass L/K abelsch ist, so folgt $L = K^{ab}$.*
(iii) *K^{ab} ist das Kompositum aller endlichen abelschen Erweiterungen von K in $\overline{K}^s$.*

Beweis: Wir schreiben zur Vereinfachung der Notation $F = \overline{K}^s$ und $H = G'$. (i) Es gilt $H \lhd G$, und daher ist F/K galoissch, und es ist auch $\overline{H} = \mathrm{Gal}(F/F^H)$ normal in G. Per Hauptsatz folgt $K^{ab} = F^{\overline{H}}$, und $\mathrm{Gal}(K^{ab}/K) \simeq G/\overline{H}$ ist als homomorphes Bild von G/H wie diese abelsch. (ii) Wir können $L \subseteq F$ annehmen. Dann ist $U = \mathrm{Gal}(F/L) < G'$ und $G/U \simeq \mathrm{Gal}(L/K)$ abelsch. Es folgt $G' \subseteq U$, also $G' = U$, und damit $L = K^{ab}$. (iii) Ist L/K endlich abelsch, so nach dem Satz über natürliche Irrationalitäten auch $K^{ab}L/K^{ab}$, also $K^{ab}L = K^{ab}$ nach (ii), also $L \subseteq K^{ab}$. Jede endliche Galoiserweiterung L/K, die in K^{ab} liegt, ist abelsch: denn $G' \subseteq U := \mathrm{Gal}(F/L) \lhd G$, und $\mathrm{Gal}(L/K) \simeq G/U$ ist daher abelsch.

Bemerkung: Aus dem *Satz von Kronecker-Weber* folgt $\mathbb{Q}^{ab} = \bigcup_{n\geq 1} E_n(\mathbb{Q})$.

Proposition 4.11

Sei K ein Körper mit separablem Abschluss $\overline{K}^s$. Sei $n \geq 1$ eine natürliche Zahl, die nicht von der Charakteristik von K geteilt wird. Bezeichne mit $\Phi_n \in K[T]$ das Polynom $\iota^*(\Phi_n)$, wobei $\Phi_n \in \mathbb{Z}[T]$ das n-te Kreisteilungspolynom über $\mathbb{Q}$ ist (selbes Symbol!) und $\iota\colon \mathbb{Z} \to K$ der natürliche Ringmorphismus $m \mapsto m\cdot 1_K$. Sei $\phi_n\colon \mathrm{Gal}(\overline{K}^s/K) \to E(\mathbb{Z}/n\mathbb{Z})$ der Gruppenmorphismus analog zum Beweis von Satz VII.1.3. Dann sind äquivalent:

(1) *Φ_n ist irreduzibel über K.*
(2) *ϕ_n ist surjektiv.*

Beweis. Aus Formel (6.1) in Kapitel VII folgt, dass die primitiven n-ten Einheitswurzeln in $\overline{K}^s$ gerade die Nullstellen von Φ_n sind und $\mathrm{grad}(\Phi_n) = \varphi(n)$ gilt. Also gilt $E_n(K) = K(\zeta)$ für jede Nullstelle von Φ_n. Es folgt: $\mathrm{grad}(\Phi_n) = [E_n(K) : K]$ genau wenn Φ_n irreduzibel über K ist. Auf der anderen Seite ist ϕ_n surjektiv genau dann, wenn $[E_n(K) : K] = |\mathrm{Gal}(E_n(K) : K)| = \varphi(n)$ gilt. Es folgt die Behauptung. ∎

Folgerung 4.12

Sei $\mathbb{F}_q$ der Körper mit q Elementen. Sei n teilerfremd zur Charakteristik p. Dann sind äquivalent:

(1) *Φ_n ist irreduzibel über $\mathbb{F}_q$.*

(2) *Die Restklasse $[q]$ erzeugt die Gruppe $E(\mathbb{Z}/n\mathbb{Z})$.*

Beweis. Es ist nur zu bemerken, dass $[q]$ das Bild unter ϕ_n vom (potenzierten Frobenius-) Automorphismus $\sigma_q\colon x \mapsto x^q$ ist. ∎

Beispiele. (1) $\Phi_7 = T^6 + T^5 + \cdots + T + 1$ ist irreduzibel über $\mathbb{F}_5$, weil $[5] \in E(\mathbb{Z}/7\mathbb{Z})$ ein Erzeuger ist.

(2) $\Phi_{11} = T^{10} + T^9 + \cdots + T + 1$ ist nicht irreduzibel über $\mathbb{F}_5$, weil $[5] \in E(\mathbb{Z}/11\mathbb{Z})$ kein Erzeuger ist (weil $[5]^5 = [1]$).

(3) $\Phi_{12} = \frac{\Phi_4(T^3)}{\Phi_4(T)} = \frac{T^6+1}{T^2+1} = T^4 - T^2 + 1$ ist nicht irreduzibel über $\mathbb{F}_5$, denn $[5] \in E(\mathbb{Z}/12\mathbb{Z})$ ist kein Erzeuger (weil $[5]^2 = [1]$).

Folgerung 4.13

Seien n, m teilerfremde natürliche Zahlen. Seien ζ_n, ζ_m primitive n-te bzw. m-te Einheitswurzeln. Das n-te Kreisteilungspolynom $\Phi_n \in \mathbb{Q}[T]$ ist irreduzibel über $\mathbb{Q}(\zeta_m)$.

Beweis. Da m und n teilerfremd sind, folgt offenbar $\mu_n(\mathbb{Q}) \cap \mu_m(\mathbb{Q}) = \{1\}$, es ist $\zeta_{mn} := \zeta_n\zeta_n$ eine primitive mn-te Einheitswurzel, und es gilt $\mathbb{Q}(\zeta_n, \zeta_m) = \mathbb{Q}(\zeta_{mn})$. Beachtet man noch $\varphi(mn) = \varphi(m)\varphi(n)$, so folgt unter Anwendung des Gradsatzes leicht $\mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\zeta_m) = \mathbb{Q}$. Aus dem Satz über natürliche Irrationalitäten folgt dann $\mathrm{Gal}(\mathbb{Q}(\zeta_n, \zeta_m)/\mathbb{Q}(\zeta_m)) \simeq \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \simeq E(\mathbb{Z}/n\mathbb{Z})$. Aus der Proposition ergibt sich die Behauptung. ∎

Bemerkung. Für die Proposition und für die Folgerungen braucht man natürlich nur die endliche Galoistheorie; man ersetzt in der Proposition – bei gegebenem n – den separablen Abschluss $\overline{K}^s$ durch den Kreisteilungskörper $E_n(K)$.

Aufgaben und weitere Themen

Ü 4.4. [Produktsatz] Seien L/K und M/K Galoiserweiterungen, so dass L und M in einem gemeinsamen Oberkörper liegen. Dann ist LM/K galoissch, und man hat einen injektiven Gruppenmorphismus

$$\mathrm{Gal}(LM/K) \xrightarrow{\sim} \mathrm{Gal}(L/K) \times \mathrm{Gal}(M/K), \quad \sigma \mapsto (\sigma_{|L}, \sigma_{|M}).$$

Dieser ist ein Isomorphismus, wenn $K = L \cap M$ gilt.

Ü 4.5. Sei $E = \mathbb{Q}\big(e^{2\pi i/n} \mid n \in \mathbb{N}\big)$ der kleinste Teilkörper von $\mathbb{C}$, der alle Einheitswurzeln enthält. Dann ist $E/\mathbb{Q}$ abelsch, d. h. algebraisch, galoissch mit abelscher Galoisgruppe.

Ü 4.6. Sei L/K eine galoissche, aber nicht endliche Körpererweiterung. Dann hat $\mathrm{Gal}(L/K)$ unendlich viele Elemente. (Hinweis: Satz 2.1.)

Ü 4.7. Ein Körper K ist perfekt genau dann, wenn jede algebraische Erweiterung L/K separabel ist.

Ü 4.8. Jeder algebraisch abgeschlossene Körper ist perfekt.

Ü 4.9. Sei L/K algebraisch. Ist K perfekt, so ist auch L perfekt. (Gilt auch die Umkehrung?)

Ü 4.10. Sei K ein Körper und $\overline{K}$ der algebraische Abschluss von K. Sei $G = \mathrm{Gal}(\overline{K}/K)$ die absolute Galoisgruppe von K. Sei L/K ein Zwischenkörper. Es operiert die Gruppe G auf der Menge

$$X_L = \{\iota\colon L \to \overline{K} \mid \iota \text{ ist } K\text{-Monomorphismus}\}$$

vermöge $\sigma.\iota := \sigma \circ \iota$. Sei $[L : K] < \infty$. Dann gilt:

(1) Es operiert G transitiv auf X_L.
(2) Für die Elementanzahl von X_L gilt $1 \leq |X_L| \leq [L : K]$. Falls K ein perfekter Körper ist, gilt $|X_L| = [L : K]$.

(Hinweis: Vgl. die Sätze 1.7 und 2.1, sowie Lemma 1.6.)

Die Aussage aus vorstehender Übung hat Anwendungen z. B. in der Algebraischen Geometrie[5]. Der folgende Spezialfall ist eine Variante davon.

Ü 4.11. Sei K ein endlicher Körper oder $K = \mathbb{Q}$ mit algebraischem Abschluss $\overline{K}$. Die absolute Galoisgruppe $G = \mathrm{Gal}(\overline{K}/K)$ von K operiert in natürlicher Weise auf $\overline{K}$ (vermöge $\sigma.x := \sigma(x)$). Zu jeder natürlichen Zahl $n \geq 1$ gibt es (mindestens ein) normiertes, irreduzibles Polynom $f \in K[T]$ vom Grad n. Jedes solche Polynom f zerfällt in $\overline{K}[T]$ in genau n verschiedene (normierte) Linearfaktoren. Die Menge der n verschiedenen Nullstellen von f in $\overline{K}$ bildet eine G-Bahn. Ist auch $f' \in K[T]$ ein normiertes, irreduzibles Polynom vom Grad n mit $f' \neq f$, so ist die zu f' gehörige G-Bahn disjunkt von der zu f.

Wir nennen ein Element $x \in \overline{K}$ *vom Grad* n über K, wenn das Minimalpolynom von x über K den Grad n hat. Es folgt also, dass für jedes $n \geq 1$ die Menge

$$\{x \in \overline{K} \mid x \text{ hat Grad } n \text{ über } K\} \neq \emptyset$$

ist und eine disjunkte Vereinigung von n-elementigen G-Bahnen ist. Die normierten, irreduziblen Polynome in $K[T]$ vom Grad n stehen in bijektiver Korrespondenz zu diesen n-elementigen G-Bahnen.

Rein-inseparable Erweiterungen. Sei L/K eine algebraische Körpererweiterung. Ein Element $\alpha \in L$ heisst *rein-inseparabel* über K, wenn $f = \mathrm{MIPO}(\alpha/K)$ in $\overline{K}$ nur eine einzige Nullstelle (mit Vielfachhheit) hat (nämlich α). L/K heisst *rein-inseparabel*, wenn jedes Element in L rein-inseparable über K ist. — Offenbar gilt: Ist L/K rein-inseparabel, so ist kein Element aus $L \setminus K$ separabel über K.

Ü 4.12. Sei L/K algebraisch. Ist $\alpha \in L$ separabel und rein-inseparabel über K, so gilt $\alpha \in K$.

Ü 4.13. Sei L/K eine algebraische Körpererweiterung, in der kein Element aus $L \setminus K$ separabel über K ist. Dann muss $\mathrm{Char}(K) = p > 0$ gelten. Ist $\alpha \in L \setminus K$ mit $f = \mathrm{MIPO}(\alpha/K)$, so gibt es ein $n \geq 1$ und ein $g \in K[T]$ irreduzibel und separabel mit $f(T) = g(T^{p^n})$. Es folgt $\alpha^{p^n} \in K$ und $f = (T - \alpha)^{p^n}$. Es ist L/K also rein-inseparabel. (Hinweis: Betrachte $D(f)$; induktives Vorgehen.)

Ü 4.14. Die Körpererweiterung L/K in Proposition 14.5 (b) ist rein-inseparabel.

Ü 4.15. [Interner separabler Abschluss] Sei L/K algebraisch. Die Teilmenge von L der über K separablen Elemente ist ein Zwischenkörper L_s von L/K.

Ü 4.16. Sei L/K algebraisch. Ist L/K normal, so ist auch L_s/K normal.

Ü 4.17. Sei L/K eine algebraische Körpererweiterung. Dann gibt es einen eindeutig bestimmten Zwischenkörper E von L/K, so dass E/K separabel und L/E rein-inseparabel ist. Es ist $E = L_s$.

Ü 4.18. Sei L/K eine rein-inseparable Körpererweiterung. Dann ist die Galoisgruppe trivial: $\mathrm{Gal}(L/K) = \{1_L\}$. (Gilt auch die Umkehrung?)

Ü 4.19. [Inseparabilitätsgrad] Sei L/K endlich. Dann gilt
(i) $[L_s : K]_s = [L_s : K]$.
(ii) $[L : L_s]_s = 1$. D. h. zu jedem Monomorphismus $j\colon L_s \to \overline{K}$ gibt es genau eine Fortsetzung $\sigma\colon L \to \overline{K}$. Folglich $[L : K]_s = [L_s : K]$.
(iii) Es ist $[L : K]_s$ ein Teiler von $[L : K]$. Der Quotient wird mit $[L : K]_i$ bezeichnet, und es heisst $[L : K]_i$ der *Inseparabilitätsgrad* von L/K. Es gilt also $[L : K] = [L : K]_s \cdot [L : K]_i$.
(iv) L/K ist rein-inseparabel genau wenn $[L : K]_i = [L : K]$ gilt.

[5]Vgl. Proposition 5.4 in: Ulrich Görtz, Torsten Wedhorn: *Algebraic Geometry I: Schemes.* Vieweg +Teubner Verlag, Springer Fachmedien Wiesbaden GmbH, 2010.

(v) Ist E ein Zwischenkörper von L/K, so gilt $[L:K]_i = [L:E]_i \cdot [E:K]_i$.

Ü 4.20. Sei L/K normale (algebraische) Körpererweiterung. Dann ist $L_i := \{a \in L \mid \sigma(a) = a \text{ für alle } \sigma \in \mathrm{Gal}(L/K)\} = L^{\mathrm{Gal}(L/K)}$ der eindeutig bestimmte Zwischenkörper, so dass L_i/K rein-inseparabel und L/L_i separabel ist.

Ü 4.21. Sei L/K normal. Seien die Zwischenkörper L_s und L_i wie oben definiert. Dann ist $L_i \cap L_s = K$ und $L = L_i L_s$.

Ü 4.22. Sei L/K algebraisch, und es gelte, dass jedes irreduzible $f \in K[T]$ eine Nullstelle in L hat. Dann ist L ein algebraischer Abschluss von K.

Hinweis: Sei $f \in K[T]$ irreduzibel und N Zerfällungskörper von f über K. Betrachte N_i und N_s sowie die vorige Aufgabe, und den Satz vom primitiven Element. Zeige $N \subseteq L$.

Separabler Abschluss. Sei K ein Körper mit algebraischem Abschluss $\overline{K}$. Dann heisst die Menge $\overline{K}^s$ der in $\overline{K}$ über K separablen Elemente der *separable Abschluss* von K, oder genauer: *separabler algebraischer Abschluss* von K. Ein separabler Abschluss von K ist nur insoweit eindeutig, wie es der algebraische Abschluss ist.

Ü 4.23. Sei K ein Körper. Dann ist der separable Abschluss $\overline{K}^s$ *separabel abgeschlossen*: D. h. ist $L/\overline{K}^s$ eine separable Körpererweiterung, so ist $L = \overline{K}^s$.

Ü 4.24. Ein Körper K ist genau dann perfekt, wenn $\overline{K} = \overline{K}^s$ gilt.

Ü 4.25. Sei K ein Körper.

(1) $\overline{K}^s$ ist ein Teilkörper von $\overline{K}$.
(2) Sei $L/\overline{K}^s$ eine (algebraische) separable Körpererweiterung. Dann gilt $L = \overline{K}^s$.
(3) Sei L/K eine (algebraische) separable Körpererweiterung. Dann gibt es einen K-Monomorphismus $L \to \overline{K}^s$.
(4) $\overline{K}^s/K$ ist eine normale und separable, also galoissche Körpererweiterung.
(5) Die Körpererweiterung $\overline{K}/\overline{K}^s$ ist rein-inseparable.
(6) Einschränkung liefert einen Gruppenisomorphismus $\mathrm{Gal}(\overline{K}/K) \xrightarrow{\sim} \mathrm{Gal}(\overline{K}^s/K)$.
(7) K ist perfekt genau dann, wenn $\overline{K}/K$ galoissch ist.

Derivationen. Sei L/K eine Körpererweiterung. Eine K-Derivation auf L ist eine Abbildung $\delta\colon L \to L$ mit $\delta(x+y) = \delta(x) + \delta(y)$ und $\delta(xy) = \delta(x)y + x\delta(y)$ für alle $x, y \in L$, und mit $\delta(a) = 0$ für alle $a \in K$. (Es ist dann δ insbesondere K-linear.)

Ü 4.26. Sei $\delta\colon L \to L$ eine K-Derivation und $x \in L$. Sei $f \in K[T]$. Dann gilt $\delta\big(f(x)\big) = D(f)(x) \cdot \delta(x)$.

Ü 4.27. Sei L/K eine (algebraische) separable Körpererweiterung. Dann ist die einzige K-Derivation von L die triviale $\delta = 0$.

Ü 4.28. Sei L/K eine einfache, rein-inseparable Erweiterung, $L = K(a)$, und es gelte $L \neq K$. Dann wird durch $\delta\big(f(a)\big) := D(f)(a)$ (für $f \in K[T]$) eine K-Derivation $\delta\colon L \to L$ mit $\delta \neq 0$ definiert. (Wohldefiniertheit!) Diese ist bis auf skalares Vielfaches die einzige K-Derivation auf L.

Ü 4.29. Sei L/K eine endliche Körpererweiterung, so dass nur die triviale K-Derivation $\delta = 0$ existiert. Dann ist L/K separabel. (Hinweis: Nehme $L_s \neq L$ an und zeige, dass es eine nicht-triviale K-Derivation von L gibt.)

Ausgezeichnete Klassen von Körpererweiterungen. Eine Klasse $\mathcal{C}$ von Körpererweiterungen L/K heisst *ausgezeichnet*, wenn folgende Eigenschaften erfüllt sind:

(1) Für einen Körperturm $L \supseteq M \supseteq K$ gilt: L/K ist in $\mathcal{C}$ genau dann, wenn L/M und M/K in $\mathcal{C}$ sind. ("$\Leftarrow$" heisst auch die Transitivität von $\mathcal{C}$.)

(2) (Translation) Ist L/K in $\mathcal{C}$ und E/K eine beliebige Körpererweiterung, so dass E und L in einem gemeinsamen Oberkörper Ω liegen, so ist EL/E in $\mathcal{C}$.
(3) (Kompositum) Sind L/K und M/K in $\mathcal{C}$, und liegen L und M in einem gemeinsamen Oberkörper Ω, so ist LM/K in $\mathcal{C}$.

Ü 4.30. Eigenschaft (3) folgt formal aus den Eigenschaften (1) und (2).

Ü 4.31. Die folgenden Eigenschaften definieren ausgezeichnete Klassen von Körpererweiterungen:
- algebraisch
- endlich
- separabel
- rein-inseparabel
- auflösbar (Charakteristik 0). Dabei heiße eine endliche Erweiterung L/K auflösbar, wenn für einen normalen Abschluss N von L/K gilt, dass die Gruppe $\mathrm{Gal}(N/K)$ auflösbar ist.
- auflösbar durch Radikale (Charakteristik 0). Dabei heiße eine endliche Erweiterung L/K auflösbar, wenn L in einer Radikalerweiterung von K liegt.

Ü 4.32. Normale (bzw. endliche normale) Körpererweiterungen bilden keine ausgezeichnete Klasse. Welche Eigenschaften von "ausgezeichnet" gelten für die Klasse der (endlichen) normalen Erweiterungen, welche nicht (Gegenbeispiel)?

Ü 4.33. Eine (algebraische) Galoiserweiterung L/K heisst *abelsch*, wenn die Gruppe $\mathrm{Gal}(L/K)$ abelsch ist. Welche Eigenschaften von "ausgezeichnet" gelten für die Klasse der abelschen Erweiterungen?

Literaturverzeichnis

[1] Emil Artin: *Galois Theory.* (Edited and with a supplemental chapter by Arthur N. Milgram. Reprint of the 1944 second edition.) Dover Publications, Inc., Mineola, NY, 1998. iv+82 pp.

[2] Siegfried Bosch: *Algebra.* (9. Auflage.) Springer Spektrum 2020

[3] Nicolas Bourbaki: *Algebra. Chapters 4–7.* Springer-Verlag 2003

[4] David A. Cox: *Galois Theory.* (2nd edition.) John Wiley & Sons 2012

[5] Harold M. Edwards: *Galois Theory.* (Corr. 3rd printing 1998.) Springer-Verlag 1984

[6] Thomas W. Hungerford: *Algebra.* Springer-Verlag 1974

[7] Jens Carsten Jantzen, Joachim Schwermer: *Algebra.* (2. Auflage.) Springer Spektrum 2014

[8] Christian Karpfinger, Kurt Meyberg: *Algebra. Gruppen - Ringe - Körper.* (5. Auflage.) Springer Spektrum 2021

[9] Serge Lang: *Algebra.* (3rd rev. edition, corr. printing 2005.) Springer-Verlag 2002

[10] James S. Milne: *Fields and Galois Theory*. Kea Books 2022

[11] Patrick Morandi: *Field and Galois Theory.* Springer-Verlag 1996

[12] Peter M. Neumann: *The mathematical writings of Évariste Galois.* Heritage of European Mathematics. European Mathematical Society (EMS), Zürich, 2011

[13] Joseph Rotman: *Galois Theory.* (2nd edition, corr. 2nd printing 2001.) Springer-Verlag 1998

[14] Ernst Steinitz, *Algebraische Theorie der Körper*, J. Reine Angew. Math. 137 (1910), 167–309.

[15] Ian Stewart: *Galois Theory.* (4th edition.) CRC Press (A Chapman & Hall Book) 2015

[16] Jean-Pierre Tignol: *Galois' Theory of Algebraic Equations.* (2nd edition.) World Scientific Publishing 2016

[17] Bartel Leendert van der Waerden: *Algebra I.* Unter Benutzung von Vorlesungen von E. Artin und E. Noether. (9. Auflage.) Springer-Verlag 1993 (Die Erstauflage erschien 1930 unter dem Titel *Moderne Algebra.*)

Index