ALGEBRA

JÜRGEN HAUSEN

Entwurf, Fassung vom 28. Juli 2023

Inhaltsverzeichnis

1. Grundbegriffe der Gruppentheorie 1

1.1. Gruppen 1

Verknüpfungen, Verknüpfungstafeln, neutrale und inverse Elemente, Gruppen, Ordnung, Gruppen der Ordnung höchstens drei, Matrizengruppen, Einheitswurzelgruppen, Symmetrische Gruppe

Aufgaben zu Abschnitt 1.1 7

1.2. Untergruppen, Faktorgruppen 9

Untergruppen, Erzeugnis, Links- und Rechtsnebenklassen, homogene Räume, Satz von Lagrange, Normalteiler, Faktorgruppen, Diedergruppe, Faktorgruppe $\mathbb{Z}/n\mathbb{Z}$, Alternierende Gruppe

Aufgaben zu Abschnitt 1.2 15

1.3. Homomorphismen 17

Homomorphismen, Mono-, Epi- und Isomorphismen, Kern und Bild, Restklassenepimorphismus, Homomorphiesatz, Isomorphiesätze

Aufgaben zu Abschnitt 1.3 21

1.4. Universelle Konstruktionen 23

Direktes Produkt, Kommutatorgruppe, Reduktion auf eine abelsche Gruppe, Halbgruppen und Monoide, Grothendieckgruppe

Aufgaben zu Abschnitt 1.4 27

2. Struktur endlicher Gruppen 29

2.1. Zyklische Gruppen 29

Klassifikation zyklischer Gruppen, Kleiner Fermatscher Satz, Untergruppen und Automorphismengruppe einer zyklischen Gruppe

Aufgaben zu Abschnitt 2.1 33

2.2. Gruppenoperationen 35

Gruppenoperationen, Satz von Cayley, Isotropiegruppe, Bahn, Bahnenraum, Bahnengleichung, Klassengleichung

Aufgaben zu Abschnitt 2.2 39

2.3. Das Theorem von Sylow 41

p-Untergruppen, p-Sylowgruppen, Sätze von Sylow mit Beweis nach Helmut Wielandt

Aufgaben zu Abschnitt 2.3 45

2.4. Auflösbare Gruppen 47

Normalreihen, Auflösbarkeit, Iterierte Kommutatorgruppen, Auflösbarkeit von p-Gruppen, Auflösbarkeit von S_n und A_n für $n \leq 4$ und Nichtauflösbarkeit von S_n und A_n für $n \geq 5$

Aufgaben zu Abschnitt 2.4 51

3. Kommutative Ringe 53

3.1. Grundbegriffe 53

Kommmutative Ringe mit Einselement, Integritätsringe, Körper, Unterringe, Homomorphismen, Quotientenkörper

Aufgaben zu Abschnitt 3.1 61

3.2. Potenzreihen- und Polynomringe 63

Polynom- und Potenzreihenring in einer bzw. mehreren Veränderlichen, universelle Eigenschaft, Auswertungshomomorphismus

Aufgaben zu Abschnitt 3.2 71

3.3. Ideale I 73

Ideale, Durchschnitt, Summe und Produkt von Idealen, Faktorringe, Homomorphiesatz, Chinesischer Restsatz

Aufgaben zu Abschnitt 3.3 77

3.4. Ideale II 79

Primideale, maximale Ideale, Hauptidealringe und noethersche Ringe, Hilbertscher Basissatz

Aufgaben zu Abschnitt 3.4 83

4. Teilbarkeitstheorie 85

4.1. Teilbarkeit in Integritätsringen 85

Teilbarkeitsbegriff, Assoziiertheit, größte gemeinsame Teiler, kleinste gemeinsame Vielfache, irreduzibel, prim

Aufgaben zu Abschnitt 4.1 89

4.2. Euklidische Ringe 91

Euklidische Ringe, Divisionsalgorithmus für Polynome, euklidischer Algorithmus

Aufgaben zu Abschnitt 4.2 97

4.3. Primfaktorzerlegung 99

Faktorielle Ringe, eindeutige Primfaktorzerlegung, Chinesischer Restsatz, Eulersche ϕ-Funktion

Aufgaben zu Abschnitt 4.3 103

4.4. Der Satz von Gauß 105

Polynomringe über faktoriellen Ringen, primitive Polynome, Lemma von Gauß, Satz von Gauß

Aufgaben zu Abschnitt 4.4 111

5. Moduln 113

5.1. Grundbegriffe 113

Moduln, Untermoduln, Produkt und direkte Summe, Homomorphismen, Homomorphiesatz

Aufgaben zu Abschnitt 5.1 119

5.2. Freie Moduln 121

Lineare Unabhängigkeit, Erzeugendensysteme, Basen, Rangbegriff für Moduln über Integritätsringen

Aufgaben zu Abschnitt 5.2 125

5.3. Torsion und Länge 127

Torsionselemente, Torsionsanteil eines Moduls, Länge eines Moduls, Längenberechnung

Aufgaben zu Abschnitt 5.3 131

5.4. Der Elementarteilersatz 133

Elementarteilersatz für endlich erzeugte Moduln über Hauptidealringen, Inhalt eines Elements

Aufgaben zu Abschnitt 5.4 137

5.5. Die Struktursätze 139

Struktursätze für endlich erzeugte Moduln über Hauptidealringen, Elementarteiler, primäre Elementarteiler

Aufgaben zu Abschnitt 5.5 143

6. Grundlagen der Körpertheorie 145

6.1. Grundbegriffe 145

Charakteristik, Primkörper, Körpererweiterungen, Gradformel, Körperadjunktion, Beispiele

Aufgaben zu Abschnitt 6.1 149

6.2. Algebraische Elemente 151

Algebraische und transzendente Elemente, Minimalpolynom, endliche, endlich erzeugte und algebraische Körpererweiterungen

Aufgaben zu Abschnitt 6.2 155

6.3. Konstruktionen mit Zirkel und Lineal 157

Elementare Konstruktionen, Konstruierbarkeitsbegriff, algebraische Eigenschaften von Mengen konstruierbarer Zahlen

Aufgaben zu Abschnitt 6.3 163

6.4. Drei klassische Probleme 165

Körpertheoretische Eigenschaften von Mengen konstruierbarer Zahlen, Quadratur des Kreises, Würfelverdopplung, Winkeldreiteilung

Aufgaben zu Abschnitt 6.4 169

6.5. Transzendenzbasen 171

Transzendenzbasen, Transzendenzgrad, Zerlegung einer Erweiterung in einen algebraischen und einen rein transzendenten Anteil

Aufgaben zu Abschnitt 6.5 175

7. Zerfällungskörper 177

7.1. Zerfällungskörper 177

Existenz und Eindeutigkeit von Zerfällungskörpern, normale Körpererweiterungen und Zerfällungskörper

Aufgaben zu Abschnitt 7.1 181

7.2. Algebraischer Abschluss 183

Algebraisch abgeschlossene Körper, Existenz und Eindeutigkeit des algebraischen Abschlusses

Aufgaben zu Abschnitt 7.2 187
7.3. Separable Polynome 189
Separable Polynome, Charakterisierung über formale Ableitung, vollkommene Körper
Aufgaben zu Abschnitt 7.3 193
7.4. Endliche Körper 195
Konstruktion und Klassifikation endlicher Körper, Unterkörper und Automorphismengruppe endlicher Körper
Aufgaben zu Abschnitt 7.4 199
7.5. Separable Erweiterungen 201
Separable Erweiterungen, Satz vom primitiven Element, endliche separable Erweiterungen und Zerfällungskörper
Aufgaben zu Abschnitt 7.5 205
8. Galoistheorie 207
8.1. Galoisgruppen und Fixkörper 207
Galoisgruppe einer Körpererweiterung, Fixkörper, endliche Automorphismengruppen, Spur
Aufgaben zu Abschnitt 8.1 211
8.2. Hauptsatz der Galoistheorie 213
Galoiserweiterungen, Hauptsatz der Galoistheorie, Beweis nach Emil Artin
Aufgaben zu Abschnitt 8.2 217
8.3. Charakterisierung der Galoiserweiterungen 219
Charakterisierung der Galoiserweiterungen als Zerfällungskörper separabler Polynome, Fundamentalsatz der Algebra
Aufgaben zu Abschnitt 8.3 223
8.4. Beispiele 225
Galois-Korrespondenz für quadratische und biquadratische Zahlkörper sowie für endliche Körper
Aufgaben zu Abschnitt 8.4 229
9. Das regelmäßige n-Eck 231
9.1. Einheitswurzeln 231
Einheitswurzeln, primitive Einheitswurzeln, Primrestklassengruppe, Eulersche ϕ-Funktion, Kreisteilungskörper
Aufgaben zu Abschnitt 9.1 235
9.2. Kreisteilungspolynome 237
Kreisteilungspolynome, Irreduzibilität der Kreisteilungspolynome, Galoisgruppe der Kreisteilungskörper
Aufgaben zu Abschnitt 9.2 241
9.3. Das regelmäßige n-Eck 243
Regelmäßige n-Ecke, Charakterisierungen der Konstruierbarkeit des regelmäßigen n-Ecks

Aufgaben zu Abschnitt 9.3 247

10. Galoisgruppe eines Polynoms 249

10.1. Die Galoisgruppe eines Polynoms 249

Galoisgruppe eines Polynoms, Operation auf der Nullstellenmenge, Polynome primen Grades mit zwei Nullstellen

Aufgaben zu Abschnitt 10.1 253

10.2. Resultante I 255

Definition der Resultante zweier Polynome, grundlegende Eigenschaften der Resultante

Aufgaben zu Abschnitt 10.2 259

10.3. Resultante II 261

Resultante und gemeinsame Nullstellen, Diskriminiante, Galoisgruppe von Polynomen dritten Grades

Aufgaben zu Abschnitt 10.3 265

11. Auflösbarkeit der Gleichungen 267

11.1. Symmetrische Funktionen 267

Symmetrische Polynome und Funktionen, elementarsymmetrische Funktionen, Körper der symmetrischen Funktionen

Aufgaben zu Abschnitt 11.1 271

11.2. Reine Polynome und Radikalerweiterungen 273

Reine Polynome, Galoisgruppe eines reinen Polynoms, Radikalerweiterungen, galoissche Radikalerweiterungen

Aufgaben zu Abschnitt 11.2 277

11.3. Auflösbarkeit von Gleichungen 277

Charakterisierung der Auflösbarkeit einer Gleichung durch Auflösbarkeit ihrer Galoisgruppe

Aufgaben zu Abschnitt 11.3 281

Literatur 283

1. Grundbegriffe der Gruppentheorie

1.1. **Gruppen.**

Definition 1.1.1. Es sei M eine Menge. Eine *Verknüpfung* auf M ist eine Abbildung

$$\kappa\colon M \times M \;\to\; M, \qquad (m_1, m_2) \;\mapsto\; \kappa(m_1, m_2).$$

Schreibweise 1.1.2. Für eine gegebene Verknüpfung $\kappa\colon M \times M \to M$ auf einer Menge M verwendet man auch gerne eine der folgenden Schreibweisen:

$$\begin{array}{rcll} m_1 * m_2 & := & \kappa(m_1, m_2), & \\ m_1 + m_2 & := & \kappa(m_1, m_2) & \text{“additiv”}, \\ m_1 m_2 & := & \kappa(m_1, m_2) & \text{“multiplikativ”}. \end{array}$$

Beispiel 1.1.3 (Ganze Zahlen)**.** Auf der Menge $\mathbb{Z}$ der ganzen Zahlen haben wir eine wohlbekannte Verknüpfung, die Addition:

$$\mathbb{Z} \times \mathbb{Z} \;\to\; \mathbb{Z}, \qquad (n, m) \;\mapsto\; n + m.$$

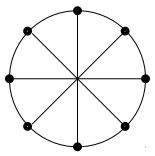
Beispiel 1.1.4 (Matrizen)**.** Auf der Menge $\mathrm{Mat}(n, n; \mathbb{K})$ aller $n \times n$-Matrizen über eine Körper $\mathbb{K}$, z.B. $\mathbb{K} = \mathbb{Q}, \mathbb{R}, \mathbb{C}$, liefert die Matrizenmultiplikation eine Verknüpfung:

$$\mathrm{Mat}(n, n; \mathbb{K}) \times \mathrm{Mat}(n, n; \mathbb{K}) \;\to\; \mathrm{Mat}(n, n; \mathbb{K}), \qquad (A, B) \mapsto AB$$

Ebenso definiert die Matrizenmultiplikation eine Verknüpfung auf der Teilmenge $\mathrm{GL}(n, \mathbb{K}) \subset \mathrm{Mat}(n, n; \mathbb{K})$ aller invertierbaren Matrizen.

Beispiel 1.1.5 (Einheitswurzeln)**.** Wir betrachten die Menge der n-ten Einheitswurzeln in $\mathbb{C}$; sie ist gegeben durch

$$C_n \;:=\; \{\zeta \in \mathbb{C};\ \zeta^n = 1\} \;=\; \{e^{2\pi i k/n};\ k = 0, \ldots, n-1\}.$$



C_n für $n = 8$

Für je zwei $\zeta_1, \zeta_2 \in C_n$ liegt das Produkt $\zeta_1\zeta_2$ wieder in C_n. Folglich haben wir eine Verknüpfung auf C_n:

$$C_n \times C_n \;\to\; C_n, \qquad (\zeta_1, \zeta_2) \;\mapsto\; \zeta_1\zeta_2.$$

Beispiel 1.1.6 (Permutationen)**.** Für eine beliebige Menge X betrachten wir die Menge ihrer *Permutationen*:

$$S(X) \;:=\; \{\sigma\colon X \to X;\ \sigma \text{ ist bijektiv}\}.$$

Die Hintereinanderausführung von Abbildungen definiert eine Verknüpfung auf der Menge $S(X)$:

$$S(X) \times S(X) \;\to\; S(X), \qquad (\sigma, \tau) \;\mapsto\; \sigma \circ \tau.$$

Ein wichtiger Spezialfall ist die n-elementige Menge $X_n := \{1, 2, \ldots, n\}$. Wir schreiben

$$S_n \;:=\; S(X_n).$$

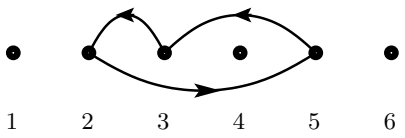
Man beachte, dass S_n genau $n!$ Elemente besitzt. Eine bewährte Schreibweise für die Elemente von S_n sei am Beispiel $n = 3$ vorgeführt:

$$\begin{aligned}
\mathrm{id}_{X_n} &= \left[\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{smallmatrix}\right]: \quad 1 \mapsto 1,\ 2 \mapsto 2,\ 3 \mapsto 3 \\
&\left[\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{smallmatrix}\right]: \quad 1 \mapsto 2,\ 2 \mapsto 1,\ 3 \mapsto 3 \\
&\left[\begin{smallmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{smallmatrix}\right]: \quad 1 \mapsto 3,\ 2 \mapsto 2,\ 3 \mapsto 1 \\
&\left[\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{smallmatrix}\right]: \quad 1 \mapsto 1,\ 2 \mapsto 3,\ 3 \mapsto 2 \\
&\left[\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{smallmatrix}\right]: \quad 1 \mapsto 2,\ 2 \mapsto 3,\ 3 \mapsto 1 \\
&\left[\begin{smallmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{smallmatrix}\right]: \quad 1 \mapsto 3,\ 2 \mapsto 1,\ 3 \mapsto 2
\end{aligned}$$

Ein *Zykel der Länge k* in S_n ist eine Abbildung $\sigma\colon X_n \to X_n$, welche die Elemente einer k-elementigen Teilmenge $\{i_1, \ldots, i_k\} \subseteq X_n$ "zyklisch" vertauscht, d.h.,

$$\sigma(i_1) = i_2, \quad \sigma(i_2) = i_3, \quad \ldots \quad \sigma(i_{k-1}) = i_k, \quad \sigma(i_k) = i_1,$$

und alle $i \in X \setminus \{i_1, \ldots, i_k\}$ fest lässt, d.h., $\sigma(i) = i$ erfüllt; man schreibt häufig $\sigma = (i_1, \ldots, i_k)$. Einen Zykel der Länge 2 nennt man eine *Transposition*.



Der Zykel $(2, 5, 3)$ in S_6

Man beachte, dass die Schreibweise $\sigma = (i_1, \ldots, i_k)$ für einen Zykel im allgemeinen nicht eindeutig ist; es gilt etwa $(1, 2) = (2, 1)$.

Bemerkung 1.1.7. Eine Verknüpfung "$*$" auf einer Menge $M = \{m_1, \ldots, m_r\}$ ist durch ihre *Verknüpfungstafel* beschrieben:

$(M, *)$	m_1	$\ldots$	m_r
m_1	$m_1 * m_1$	$\ldots$	$m_1 * m_r$
$\vdots$	$\vdots$		$\vdots$
m_r	$m_r * m_1$	$\ldots$	$m_r * m_r$

Beispiel 1.1.8. Die Menge C_3 der dritten Einheitswurzeln in $\mathbb{C}$ ist gegeben durch

$$C_3 = \{1, \zeta_1, \zeta_2\}, \quad \text{wobei} \quad \zeta_1 := e^{2\pi i/3}, \quad \zeta_2 := e^{4\pi i/3}.$$

Die in Beispiel 1.1.5 definierte Verknüpfung auf C_3 besitzt folgende Verknüpfungstafel:

$(C_3, *)$	1	ζ_1	ζ_2
1	1	ζ_1	ζ_2
ζ_1	ζ_1	ζ_2	1
ζ_2	ζ_2	1	ζ_1

Definition 1.1.9. Eine Verknüpfung $(m_1, m_2) \mapsto m_1 * m_2$ auf einer Menge M nennt man

(i) *assoziativ*, falls stets gilt:

$$(m_1 * m_2) * m_3 = m_1 * (m_2 * m_3).$$

(ii) *kommutativ*, falls stets gilt:

$$m_1 * m_2 = m_2 * m_1$$

Ein Element $e \in M$ nennt man ein *neutrales Element (der Verknüpfung "$*$")*, falls stets gilt

$$e * m \;=\; m * e \;=\; m.$$

Bemerkung 1.1.10. Eine Verknüpfung "$*$" auf einer Menge M besitzt höchstens ein neutrales Element.

Beweis. Es seien Elemente $e, e' \in M$ mit der Eigenschaft eines neutralen Elements gegeben. Dann erhalten wir

$$e \;=\; e * e' \;=\; e'.$$

Je zwei Elemente mit den Eigenschaften eines neutralen Elements stimmen also überein. Das beweist die Eindeutigkeit. □

Definition 1.1.11. Es sei M eine Menge mit einer Verknüpfung "$*$" und neutralem Element $e \in M$. Man nennt $m_2 \in M$ *Inverses* zu $m_1 \in M$ (bezüglich "$*$"), falls gilt

$$m_2 * m_1 \;=\; e \;=\; m_1 * m_2.$$

Bemerkung 1.1.12. Es sei M eine Menge mit einer assoziativen Verknüpfung und neutralem Element. Dann besitzt jedes $m \in M$ höchstens ein Inverses.

Beweis. Es seien $m_1, m_2 \in M$ inverse Elemente zu gegebenem $m \in M$. Dann erhalten wir:

$$m_1 \;=\; m_1 * (m * m_2) \;=\; (m_1 * m) * m_2 \;=\; m_2.$$

□

Schreibweise 1.1.13. Es sei M eine Menge mit Verknüpfung. Ist $m_2 \in M$ ein Inverses zu $m_1 \in M$ bezüglich, so bezeichnet man dieses auch durch $m_1^{-1} := m_2$ (bzw. $-m_1 := m_2$ in der additiven Schreibweise).

Definition 1.1.14. Eine *Gruppe* ist eine Menge G zusammen mit einer assoziativen Verknüpfung

$$G \times G \;\to\; G, \qquad (g_1, g_2) \;\mapsto\; g_1 g_2$$

und einem neutralen Element $e \in G$, sodass jedes $g \in G$ ein Inverses $g^{-1} \in G$ besitzt; d.h., in G gilt stets

$$g_1(g_2 g_3) \;=\; (g_1 g_2) g_3,$$

$$eg \;=\; g \;=\; ge,$$

$$g^{-1} g \;=\; e \;=\; g g^{-1}.$$

Eine Gruppe G nennt man *abelsch (auch kommutativ)*, falls ihre Verknüpfung kommutativ ist; d.h., zusätzlich zu den obigen Regeln gilt stets

$$g_1 g_2 \;=\; g_2 g_1.$$

Schreibweise 1.1.15. Es sei G eine Gruppe.

(i) Wollen wir die Verknüpfung einer Gruppe G näher bezeichnen, so schreiben wir auch genauer $(G, \cdot)$, bzw. $(G, +)$ etc., anstatt G.
(ii) Sofern keine Verwechslungsmöglichkeiten bestehen, wählen wir meistens die Bezeichnung $g_1 g_2$ für die Verknüpfung von $g_1, g_2 \in G$.
(iii) Das neutrale Element $e \in G$ bezeichnen wir, um Verwechslungen vorzubeugen, oft auch mit e_G.

Beispiel 1.1.16. Die in den Beispielen 1.1.3 bis 1.1.6 vorgestellten Verknüpfungen liefern Gruppen:

(i) Die ganzen Zahlen bilden zusammen mit der Addition eine abelsche Gruppe $(\mathbb{Z}, +)$; das neutrale Element in $\mathbb{Z}$ ist die 0, und das Inverse zu $n \in \mathbb{Z}$ ist $-n \in \mathbb{Z}$.
(ii) $\mathrm{GL}(n, \mathbb{K})$ ist eine Gruppe, die *allgemeine lineare Gruppe über* $\mathbb{K}$; das neutrale Element in $\mathrm{GL}(n, \mathbb{K})$ ist die $(n \times n)$-Einheitsmatrix, und das Inverse zu $A \in \mathrm{GL}(n, \mathbb{K})$ ist die inverse Matrix A^{-1}. Für $n \geq 2$ ist $\mathrm{GL}(n, \mathbb{K})$ nicht abelsch.
(iii) Die n-ten komplexen Einheitswurzeln mit der Multiplikation bilden eine abelsche Gruppe $(C_n, \cdot)$; das neutrale Element in C_n ist die $1 = e^0$, und das Inverse zu $e^{2\pi k/n}$ ist $e^{-2\pi ik/n}$.
(iv) $(S_n, \circ)$ ist eine Gruppe, die *symmetrische Gruppe*; das neutrale Element in S_n ist die identische Abbildung, und das Inverse zu $\sigma \in S_n$ ist die Umkehrabbildung $\sigma^{-1} \in S_n$. Die Gruppen S_1 und S_2 sind abelsch, für $n \geq 3$ ist S_n nicht mehr abelsch.

Bemerkung 1.1.17. Es sei G eine Gruppe, und es seien $g_1, g_2 \in G$. Dann gilt

$$(g_1 g_2)^{-1} \;=\; g_2^{-1} g_1^{-1}.$$

Beweis. Mit der Assoziativität der Verknüpfung erhalten wir

$$(g_2^{-1} g_1^{-1})(g_1 g_2) \;=\; g_2^{-1}(g_1^{-1}(g_1 g_2)) \;=\; g_2^{-1}((g_1^{-1} g_1) g_2) \;=\; g_2^{-1} g_2 \;=\; e.$$

Analog verifiziert man $(g_1 g_2)(g_2^{-1} g_1^{-1}) = e$. □

Definition 1.1.18. Es sei G eine Gruppe, und es sei ein Element $g \in G$ gegeben. Wir definieren rekursiv:

$$\begin{array}{lcll} g^0 & := & e, & \\ g^n & := & g g^{n-1} \;=\; \underbrace{g \cdots g}_{n\text{-mal}} & \text{für } n \in \mathbb{Z}_{>0}, \\ g^n & := & g^{-1} g^{n+1} \;=\; \underbrace{g^{-1} \cdots g^{-1}}_{|n|\text{-mal}} & \text{für } n \in \mathbb{Z}_{<0}. \end{array}$$

Bemerkung 1.1.19. Es seien G eine Gruppe und $g \in G$. Für $n, n_1, n_2 \in \mathbb{Z}$ gilt stets

$$(g^n)^{-1} \;=\; g^{-n}, \qquad g^{n_1} g^{n_2} \;=\; g^{n_2} g^{n_1} \;=\; g^{n_1 + n_2}, \qquad (g^{n_1})^{n_2} \;=\; g^{n_1 n_2}.$$

Definition 1.1.20. Die *Ordnung* einer Gruppe G (bzw. einer Menge M) ist die Anzahl ihrer Elemente; wir bezeichnen sie mit $|G|$ (bzw. mit $|M|$).

Satz 1.1.21. *Es sei M eine Menge mit $1 \leq |M| \leq 3$, und es sei $e \in M$ ein beliebiges Element. Dann gibt es genau eine Verknüpfung "$*$" auf M, sodass $(M, *)$ eine Gruppe mit neutralem Element $e \in M$ ist. In jedem der drei Fälle ist $(M, *)$ dann eine abelsche Gruppe.*

Lemma 1.1.22. *Es sei G eine Gruppe. Dann definiert jedes Element $h \in G$ bijektive Abbildungen*

$$L_h \colon G \;\to\; G, \qquad g \;\mapsto\; hg,$$

$$R_h \colon G \;\to\; G, \qquad g \;\mapsto\; gh.$$

Insbesondere kommt jedes $g \in G$ in jeder Zeile und ebenso in jeder Spalte der Verknüpfungstafel von G genau einmal vor.

Beweis. Die Abbildung $L_{h^{-1}}$ ist eine Umkehrabbildung zu L_h, denn für jedes $g \in G$ haben wir

$$\begin{aligned} L_{h^{-1}} \circ L_h(g) &= h^{-1}(hg) = (h^{-1}h)g = eg = g, \\ L_h \circ L_{h^{-1}}(g) &= h(h^{-1}g) = (hh^{-1})g = eg = g. \end{aligned}$$

Folglich ist L_h bijektiv. Analog sieht man, dass $R_{h^{-1}}$ eine Umkehrabbildung zu R_h ist, und R_h somit bijektiv ist. □

Beweis von Satz 1.1.21. Der Fall $|M| = 1$ ist trivial: Es gibt überhapt nur eine Verknüpfung auf M, und das einzige Element von M erfüllt die Bedingungen des neutralen Elements.

Betrachten wir den Fall $|M| = 2$. Hier gilt $M = \{e, m\}$. Nach Lemma 1.1.22 muss die zugehörige Verknüpfungstafel wie folgt aussehen:

$(M, *)$	e	m
e	e	m
m	m	e

Es bleibt zu zeigen, dass eine Verknüpfung "$*$" mit dieser Verknüpfungstafel den Axiomen einer abelschen Gruppe genügt. Das ist der Tafel jedoch unmittelbar anzusehen.

Kommen wir zum Fall $n = 3$: Hier haben wir $M = \{e, m_1, m_2\}$. Ein guter Teil der Verknüpfungstafel steht durch die von e verlangten Eigenschaften bereits fest:

$(M, *)$	e	m_1	m_2
e	e	m_1	m_2
m_1	m_1		
m_2	m_2		

Für das Element $m_1 * m_1$ gibt es nach Lemma 1.1.22 höchstens zwei Möglichkeiten: Erstens $m_1 * m_1 = m_2$, zweitens $m_1 * m_1 = e$:

$(M, *)$	e	m_1	m_2
e	e	m_1	m_2
m_1	m_1	m_2	
m_2	m_2		

$(M, *)$	e	m_1	m_2
e	e	m_1	m_2
m_1	m_1	e	
m_2	m_2		

Von diesen beiden Möglichkeiten kann nur die erste vervollständigt werden, ohne dabei die Aussage von Lemma 1.1.22 zu verletzen; und das geht wie folgt:

$(M, *)$	e	m_1	m_2
e	e	m_1	m_2
m_1	m_1	m_2	e
m_2	m_2	e	m_1

Es bleibt wiederum zu zeigen, dass das Ergebnis die Verknüpfungstafel einer abelschen Gruppe ist, aber diesmal genügt ein Vergleich mit der Verknüpfungstafel der Gruppe C_3 aus Beispiel 1.1.8. □

Aufgaben zu Abschnitt 1.1.

Aufgabe 1.1.23. Es sei $\varphi\colon X \to Y$ eine Abbildung beliebiger Mengen X und Y.

(i) Für jede Familie Y_i, $i \in I$, von Teilmengen $Y_i \subseteq Y$ gilt

$$\varphi^{-1}\left(\bigcup_{i\in I} Y_i\right) = \bigcup_{i\in I} \varphi^{-1}(Y_i), \qquad \varphi^{-1}\left(\bigcap_{i\in I} Y_i\right) = \bigcap_{i\in I} \varphi^{-1}(Y_i).$$

(ii) Für jede Familie X_i, $i \in I$, von Teilmengen $X_i \subseteq X$ gilt

$$\varphi\left(\bigcup_{i\in I} X_i\right) = \bigcup_{i\in I} \varphi(X_i), \qquad \varphi\left(\bigcap_{i\in I} X_i\right) \subseteq \bigcap_{i\in I} \varphi(X_i).$$

Gib ein Beispiel an, bei dem im letzten Fall keine Gleichheit gilt.

Aufgabe 1.1.24. Es seien X, Y endliche Mengen mit $|X| = |Y|$, und es sei $\varphi\colon X \to Y$ eine Abbildung. Beweise die Äquivalenz folgender Aussagen:

(i) $\varphi\colon X \to Y$ ist injektiv.
(ii) $\varphi\colon X \to Y$ ist surjektiv.
(iii) $\varphi\colon X \to Y$ ist bijektiv.

Aufgabe 1.1.25. Es sei M eine Menge mit einer assoziativen Verknüpfung "$*$", und es seien $m_1, \ldots, m_r \in M$. Definiere rekursiv

$$m_1 * \ldots * m_r \quad := \quad (m_1 * \ldots * m_{r-1}) * m_r,$$

wobei man im Falle $r = 1$ die linke Seite einfach zu m_1 setze. Zeige: Für jede Familie von Zahlen $1 \le i_1 \le i_2 \le \ldots \le i_k \le r$ gilt

$$m_1 * \ldots * m_r \quad = \quad (m_1 * \ldots * m_{i_1}) * (m_{i_2} * \ldots * m_{i_3}) * \ldots * (m_{i_k} * \ldots * m_{i_r}).$$

Aufgabe 1.1.26. Zeige: Die Gruppe S_n besitzt genau $n!$ Elemente.

Aufgabe 1.1.27. Berechne folgende Ausdrücke in S_9:

(i) $\begin{pmatrix} 1&2&3&4&5&6&7&8&9\\ 8&7&4&3&6&2&9&5&1 \end{pmatrix} \circ \begin{pmatrix} 1&2&3&4&5&6&7&8&9\\ 6&1&3&5&4&7&2&9&8 \end{pmatrix}$,

(ii) $\begin{pmatrix} 1&2&3&4&5&6&7&8&9\\ 9&7&3&2&4&5&6&8&1 \end{pmatrix}^{-2}$.

Aufgabe 1.1.28. Zeige: Für $n \ge 3$ ist S_3 nicht abelsch. *Hinweis:* Betrachte die Transpositionen $(1, 2)$ und $(2, 3)$.

Aufgabe 1.1.29. Zeige: Für $n = 1, 2, 3$ ist jedes Element aus S_n ein Zykel. Gib ein Element in S_4 an, das kein Zykel ist.

Aufgabe 1.1.30. Zeige für jeden Zykel $(i_1, \ldots, i_k) \in S_n$ gilt

$$(i_1, \ldots, i_k)^{-1} \quad = \quad (i_k, \ldots, i_1).$$

Aufgabe 1.1.31. Zeige: Für jeden 3-Zykel $(i_1, i_2, i_3) \in S_n$, wobei $n \ge 3$, hat man eine Darstellung

$$(i_1, i_2, i_3) \quad = \quad (i_1, i_3) \circ (i_2, i_3) \circ (i_1, i_3)^{-1} \circ (i_2, i_3)^{-1}.$$

Aufgabe 1.1.32. Es seien $(i_1, \ldots, i_k) \in S_n$ ein k-Zykel und $\sigma \in S_n$ ein beliebiges Element. Zeige:

$$\sigma \circ (i_1, \ldots, i_k) \circ \sigma^{-1} \quad = \quad (\sigma(i_1), \ldots, \sigma(i_k)).$$

Aufgabe 1.1.33. Betrachte die vierelementige Menge $G := \{e, a, b, c\}$ und die "angefangenen" Verknüpfungstafeln

$(G,*)$	e	a	b	c
e	e	a	b	c
a	a	e		
b	b		e	
c	c			e

$(G,*)$	e	a	b	c
e	e	a	b	c
a	a	b		
b	b	c		
c	c	e		

Zeige: Es gibt für jede der beiden Tafeln genau eine Möglichkeit sie zu vervollständigen, sodass G zusammen mit "$*$" eine Gruppe ist.

Aufgabe 1.1.34. Vegleiche die zweite Verknüpfungstafel aus der vorigen Aufgabe mit der Verknüpfungstafel der Einheitswurzelgruppe C_4.

Aufgabe 1.1.35. Zeige: Für $n \geq 2$ ist $\mathrm{GL}(n, \mathbb{K})$, wobei $\mathbb{K} = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ keine abelsche Gruppe.

Aufgabe 1.1.36. Es sei $Q \subseteq \mathbb{R}^2$ eine Teilmenge. Zeige: Zusammen mit der Matrizenmultiplikation ist die Menge

$$G_Q \quad := \quad \{A \in \mathrm{GL}(2;\mathbb{R});\ AQ = Q\}$$

eine Gruppe. Bestimme G_Q explizit für den Fall, dass $Q \subset \mathbb{R}^2$ das regelmäßige Viereck ist mit den Eckpunkten

$$v_1 \ := \ (1,0), \quad v_2 \ := \ (0,1), \quad v_3 \ := \ (-1,0), \quad v_4 \ := \ (0,-1).$$

Bestimme die Verknüpfungstafel der Gruppe G_Q in diesem Fall.

Aufgabe 1.1.37 (Quaternionengruppe)**.** Betrachte die folgenden Elemente in $\mathrm{Mat}(2,2;\mathbb{C})$, wobei $i \in \mathbb{C}$ wie üblich die imaginäre Einheit bezeichnet:

$$E \ := \ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad I \ := \ \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \quad J \ := \ \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}, \quad K \ := \ \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}.$$

Zeige: Zusammen mit der Matrizenmultiplikation ist $\{\pm E, \pm I, \pm J, \pm K\}$ eine Gruppe. Stelle die Verknüpfungstafel auf.

Aufgabe 1.1.38. Es sei G eine Menge mit einer assoziativen Verknüpfung "$*$". Zeige: G ist genau dann eine Gruppe, wenn folgendes gilt

(i) Es gibt ein *linksneutrales Element* $e \in G$, d.h., für jedes $g \in G$ gilt $e * g = g$.
(ii) Zu jedem $g \in G$ gibt es ein *Linksinverses* $g' \in G$, d.h., es gilt $g' * g = e$.

Aufgabe 1.1.39. Es seien G eine Gruppe, $g \in G$, und $n, n_1, n_2 \in \mathbb{Z}$. Beweise die Rechenregeln aus Bemerkung 1.1.19:

$$(g^n)^{-1} \ = \ g^{-n}, \qquad g^{n_1} g^{n_2} \ = \ g^{n_2} g^{n_1} \ = \ g^{n_1+n_2}, \qquad (g^{n_1})^{n_2} \ = \ g^{n_1 n_2}.$$

Aufgabe 1.1.40. Es seien G eine Gruppe, $g_1, \ldots, g_r \in G$ und $\nu_1, \ldots, \nu_r \in \mathbb{Z}$. Zeige:

$$(g_1^{\nu_1} g_2^{\nu_2} \cdots g_r^{\nu_r})^{-1} \quad = \quad g_r^{-\nu_r} g_{r-1}^{-\nu_{r-1}} \cdots g_1^{-\nu_1}.$$

Aufgabe 1.1.41. Es sei G eine Gruppe. Zeige:

(i) Gilt $(gh)^2 = g^2 h^2$ für alle $g, h \in G$, so ist G abelsch.
(ii) Gilt $g^2 = e_G$ für jedes $g \in G$, so ist G abelsch.

Aufgabe 1.1.42. Es sei G eine endliche abelsche Gruppe. Zeige:

$$\prod_{g \in G} g^2 \quad = \quad e_G.$$

Aufgabe 1.1.43. Es seien M eine Menge, G eine Gruppe und $\mathrm{Abb}(M, G)$ die Menge aller Abbildungen $M \to G$. Betrachte die durch

$$(\varphi * \psi)(m) \quad := \quad \varphi(m)\psi(m)$$

definierte Verknüpfung "$*$" auf der Menge $\mathrm{Abb}(M, G)$. Zeige: Das Paar $(\mathrm{Abb}(M, G), *)$ ist eine Gruppe.

Aufgabe 1.1.44. Es seien G und H Gruppen. Zeige: Das kartesische Produkt $G \times H$ wird zu einer Gruppe durch komponentenweise Verknüpfung:

$$(g, h)(g', h') \quad := \quad (gg', hh').$$

1.2. **Untergruppen, Faktorgruppen.**

Definition 1.2.1. Es sei G eine Gruppe, und es sei $H \subseteq G$ eine Teilmenge mit folgenden Eigenschaften

$$e_G \in H, \qquad h_1, h_2 \in H \;\Rightarrow\; h_1 h_2 \in H, \qquad h \in H \;\Rightarrow\; h^{-1} \in H.$$

Dann nennen wir H zusammen mit der *induzierten Verknüpfung* $(h_1, h_2) \mapsto h_1 h_2$ eine *Untergruppe* der Gruppe G; wir schreiben dafür auch $H \leq G$.

Bemerkung 1.2.2. Jede Untergruppe H einer Gruppe G ist wieder eine Gruppe; das neutrale Element ist dabei $e_H = e_G$.

Beispiel 1.2.3.
(i) $(\mathbb{Z}, +)$ ist eine Untergruppe von $(\mathbb{Q}, +)$.
(ii) Für jedes $n \in \mathbb{Z}$ ist $(n\mathbb{Z}, +)$ eine Untergruppe von $(\mathbb{Z}, +)$.
(iii) Die Einheitswurzelgruppe $(C_n, \cdot)$ ist eine Untergruppe von $(\mathbb{C}^*, \cdot)$.
(iv) Die Quaternionengruppe 1.1.37 ist eine Untergruppe von $\mathrm{GL}(2, \mathbb{C})$.
(v) Jede Gruppe G besitzt die Untergruppen $\{e_G\} \leq G$ und $G \leq G$.

Bemerkung 1.2.4. Es sei G eine Gruppe und H eine Untergruppe. Sind Elemente $h_1, \ldots, h_r \in H$ und Zahlen $n_1, \ldots, n_r \in \mathbb{Z}$ gegeben, so gilt $h_1^{n_1} \cdots h_r^{n_r} \in H$.

Bemerkung 1.2.5. Es seien G eine Gruppe und $H_i \subseteq G$, $i \in I$, Untergruppen. Dann ist der Durchschnitt $\bigcap_{i \in I} H_i$ wieder eine Untergruppe von G.

Konstruktion 1.2.6. Es seien G eine Gruppe und $A \subseteq G$ eine Teilmenge. Ist A nicht leer, so setzen wir

$$\langle A \rangle \;=\; \{g_1^{n_1} \cdots g_r^{n_r};\; r \in \mathbb{Z}_{\geq 1},\; g_i \in A,\; n_i =\in \mathbb{Z}\},$$

und für $A = \emptyset$ setzen wir $\langle A \rangle := \{e_G\}$. Dann ist $\langle A \rangle$ eine Untergruppe von G; die *von A erzeugte Untergruppe in G*. Für $A = \{g_1, \ldots, g_r\}$ schreibt man auch

$$\langle g_1, \ldots, g_r \rangle \;:=\; \langle A \rangle$$

und spricht von der *von $g_1, \ldots, g_r$ erzeugten Untergruppe*. Für die durch ein Element $g \in G$ erzeugte Untergruppe $\langle g \rangle$ in G hat man

$$\langle g \rangle \;=\; \{g^n;\; n \in \mathbb{Z}\}.$$

Beweis. Wir weisen die Eigenschaften einer Untergruppe für $\langle A \rangle$ nach. Ist A leer, so ist nichts zu zeigen. Ist A nicht leer, so wählen wir ein $g \in A$ und erhalten $e_G = g^0 \in \langle A \rangle$. Für je zwei Elemente $g_1^{n_1} \cdots g_r^{n_r}$ und $h_1^{m_1} \cdots h_s^{m_s}$ aus $\langle A \rangle$ erhalten wir weiter

$$(g_1^{n_1} \cdots g_r^{n_r})(h_1^{m_1} \cdots n_n^{m_s}) \;=\; g_1^{n_1} \cdots g_r^{n_r} h_1^{m_1} \cdots h_n^{m_s} \;\in\; \langle A \rangle,$$
$$(g_1^{n_1} \cdots g_r^{n_r})^{-1} \;=\; (g_r^{-n_r} \cdots g_1^{-n_1}) \;\in\; \langle A \rangle.$$

□

Satz 1.2.7. *Es seien G eine Gruppe und $A \subseteq G$ eine Teilmenge. Dann ist die von A erzeugte Untergruppe in G gegeben durch*

$$\langle A \rangle \;:=\; \bigcap_{A \subseteq H \leq G} H.$$

Beweis. Zur Inklusion "$\subseteq$". Ist $H \leq G$ eine Untergruppe mit $A \subseteq H$, so gilt offenbar auch $\langle A \rangle \subseteq H$. Zur Inklusion "$\supseteq$". Da $\langle A \rangle$ eine Untergruppe von G ist erhalten wir

$$\langle A \rangle \;\supseteq\; \langle A \rangle \cap \bigcap_{A \subseteq H \leq G} H \;=\; \bigcap_{A \subseteq H \leq G} H.$$

□

Beispiel 1.2.8. Die Gruppe C_4 der vierten Einheitswurzeln besitzt genau die folgenden Untergruppen:

$$C_1 \ = \ \langle 1 \rangle \ = \ \{1\}, \qquad C_2 \ = \ \langle -1 \rangle \ = \ \{1, -1\}, \qquad C_4 \ = \ \langle i \rangle \ = \ \langle -i \rangle.$$

Beispiel 1.2.9. Es sei $n \in \mathbb{Z}_{\geq 3}$. Die *Diedergruppe* D_n ist die von den Permutationen

$$\delta \ := \ \begin{bmatrix} 1 & 2 & \ldots & n-1 & n \\ 2 & 3 & \ldots & n & 1 \end{bmatrix}, \qquad \sigma \ := \ \begin{bmatrix} 1 & 2 & 3 & \ldots & n-1 & n \\ 1 & n & n-1 & \ldots & 3 & 2 \end{bmatrix}$$

erzeugte Untergruppe von S_n. Die Abbildungen δ und σ lassen sich als Symmetrien des regelmäßigen n-Ecks interpretieren.

δ σ

Definition 1.2.10. Es seien G eine Gruppe und $H \leq G$ eine Untergruppe.

(i) Die *Linksnebenklasse* eines Elements $g \in G$ ist

$$gH \ := \ \{gh; \ h \in H\} \ \subseteq \ G.$$

(ii) Die *Rechtsnebenklasse* eines Elements $g \in G$ ist

$$Hg \ := \ \{hg; \ h \in H\} \ \subseteq \ G.$$

Lemma 1.2.11. *Es seien G eine Gruppe und $H \leq G$ eine Untergruppe. Dann gilt für jedes $g \in G$:*

$$|gH| \ = \ |H| \ = \ |Hg|.$$

Beweis. Man erhält die Aussage durch Anwenden der Bijektionen $L_g, R_g \colon G \to G$ aus Lemma 1.1.22. Es gilt:

$$L_g(H) \ = \ gH, \qquad\qquad R_g(H) \ = \ Hg.$$

□

Definition 1.2.12. Es seien G eine Gruppe und $H \leq G$ eine Untergruppe. Der zugehörige *homogene Raum* ist die Menge G/H aller Linksnebenklassen:

$$G/H \quad := \quad \{gH; \ g \in G\}.$$

Der *Index* von H in G ist die Ordnung des homogenen Raumes G/H, und wird geschrieben als

$$[G : H] \quad := \quad |G/H|.$$

Satz 1.2.13. *Es seien G eine Gruppe und $H \leq G$ eine Untergruppe. Dann erhält man eine Äquivalenzrelation auf G durch:*

$$g_1 \ \sim_H \ g_2 \quad : \Longleftrightarrow \quad g_2^{-1} g_1 \ \in \ H.$$

Die Äquivalenzklasse eines Elements $g \in G$ ist genau die Linksnebenklasse gH. Insbesondere hat man eine Darstellung als disjunkte Vereinigung

$$G \ = \ \bigsqcup_{gH \ \in \ G/H} gH.$$

Beweis. Zunächst weisen wir für "$\sim_H$" die Eigenschaften einer Äquivalenzrelation nach, d.h., wir zeigen

- $g \sim_H g$ für alle $g \in G$ (Reflexivität),
- $g_1 \sim_H g_2 \Rightarrow g_2 \sim_H g_1$ für alle $g_1, g_2 \in G$ (Symmetrie),
- $g_1 \sim_H g_2$ und $g_2 \sim_H g_3 \Rightarrow g_1 \sim_H g_3$ für alle $g_1, g_2, g_3 \in G$ (Transitivität).

Die Relexivität ist offensichtlich. Zur Symmetrie: Gilt $g_1 \sim_H g_2$, so bedeutet dies $g_2^{-1} g_1 \in H$. Invertieren ergibt $g_1^{-1} g_2 \in H$. Das bedeutet $g_2 \sim_H g_1$. Zur Transitivität: Gilt $g_1 \sim_H g_2$ und $g_2 \sim_H g_3$, so haben wir $g_1^{-1} g_2 \in H$ und $g_2^{-1} g_3 \in H$. Wir schließen $g_1 \sim_H g_3$ mit

$$g_3^{-1} g_1 \;=\; (g_3^{-1} g_2)(g_2^{-1} g_1) \;\in\; H.$$

Wir zeigen nun, dass für jedes Element $g \in G$ die zugehörige Äquivalenzklasse $[g]$ gerade die Linksnebenklasse gH ist: Für jedes Element $g' \in G$ gilt

$$g' \in [g] \;\Leftrightarrow\; g' \sim_H g \;\Leftrightarrow\; g^{-1} g' \in H \;\Leftrightarrow\; g' \in gH.$$

Die Äquivalenzklassen einer Äquivalenzrelation auf einer Menge zerlegen diese stets disjunkt. In unserem Fall bedeutet dies, dass man G als disjunkte Vereinigung der Linksnebenklassen von H erhält. □

Satz 1.2.14 (Satz von Lagrange)**.** *Es seien G eine Gruppe und $H \leq G$ eine Untergruppe. Dann gilt*

$$|G| \;=\; [G : H] \cdot |H|.$$

Insbesondere ist im Fall einer endlichen Gruppe G die Ordnung $|H|$ ein Teiler der Ordnung $|G|$.

Beweis. Gemäß Satz 1.2.13 und Lemma 1.2.11 sowie der Definition des Index haben wir

$$G \;=\; \bigsqcup_{gH \,\in\, G/H} gH, \qquad |gH| \;=\; |H|, \qquad |G/H| \;=\; [G : H].$$

Gilt $|G| = \infty$, so muss also mindestens eine der Mengen H und G/H unendlich sein, was die Behauptung in diesem Fall beweist. Gilt $|G| < \infty$, so erhalten wir

$$|G| \;=\; \sum_{gH \,\in\, G/H} |gH| \;=\; \sum_{gH \,\in\, G/H} |H| \;=\; |G/H||H| \;=\; [G : H]|H|.$$

□

Folgerung 1.2.15. *Es sei G eine endliche Gruppe. Ist $|G|$ eine Primzahl, so sind $\{e_G\}$ und G die einzigen Untergruppen von G.*

Definition 1.2.16. Es sei G eine Gruppe. Die *Ordnung* eines Elements $g \in G$ ist $\mathrm{ord}(g) := |\langle g \rangle|$.

Folgerung 1.2.17. *Es sei G eine endliche Gruppe. Dann ist für jedes $g \in G$ die Ordnung* $\mathrm{ord}(g)$ *ein Teiler der Gruppenordnung $|G|$.*

Definition 1.2.18. Eine Untergruppe $H \leq G$ einer Gruppe G heisst *Normalteiler* in G, geschrieben $H \trianglelefteq G$, falls $gHg^{-1} = H$ für jedes $g \in G$ gilt.

Bemerkung 1.2.19. Eine Untergruppe $H \leq G$ einer Gruppe G ist genau dann ein Normalteiler in G, wenn $gH = Hg$ für jedes $g \in G$ gilt.

Bemerkung 1.2.20. Ist G eine abelsche Gruppe, so ist jede Untergruppe $H \leq G$ ein Normalteiler.

Konstruktion 1.2.21 (Faktorgruppe)**.** Es seien G eine Gruppe und $H \trianglelefteq G$ ein Normalteiler. Dann besitzt der homogene Raum G/H eine Verknüpfung

$$G/H \times G/H \;\to\; G/H, \qquad (g_1H, g_2H) \;\mapsto\; g_1g_2H.$$

Zusammen mit dieser Verknüpfung ist G/H eine Gruppe; das neutrale Element ist e_GH und das Inverse eines Elements gH ist $g^{-1}H$.

Beweis. Wir zeigen zunächst, dass die Verknüpfung wohldefiniert ist. Dazu betrachten wir zwei Nebenklassen

$$g_1H \;=\; g_1'H, \qquad g_2H \;=\; g_2'H.$$

Zu zeigen ist $g_1g_2H = g_1'g_2'H$. Die Normalteilereigenschaft liefert $g_2'H = Hg_2'$. Damit erhalten wir

$$g_1g_2H \;=\; g_1g_2'H \;=\; g_1Hg_2' \;=\; g_1'Hg_2' \;=\; g_1'g_2'H.$$

Die Axiome einer Gruppe für G/H ergeben sich nun direkt aus den entsprechenden Eigenschaften für G. □

Erinnerung 1.2.22 (Division mit Rest)**.** Es sei $n \in \mathbb{Z}_{\geq 1}$. Dann besitzt jedes $m \in \mathbb{Z}$ eine eindeutige Darstellung der Form $m = qn+r$ mit $q \in \mathbb{Z}$ und einem "Rest" $r \in \mathbb{Z}$, sodass $0 \leq r \leq n-1$ gilt.

Beispiel 1.2.23. Für $n \in \mathbb{Z}_{\geq 1}$ betrachten wir den Normalteiler $n\mathbb{Z} \trianglelefteq \mathbb{Z}$. Division mit Rest liefert eine disjunkte Zerlegung

$$\mathbb{Z} \;=\; n\mathbb{Z} \;\sqcup\; 1+n\mathbb{Z} \;\sqcup\; \ldots \;\sqcup\; n-1+n\mathbb{Z}.$$

Folglich gilt $[\mathbb{Z} : n\mathbb{Z}] = n$, und die zugehörige Faktorgruppe $\mathbb{Z}/n\mathbb{Z}$ ist von der Ordnung n.

Definition 1.2.24. Es sei $n \in \mathbb{Z}_{\geq 1}$. Das *Signum* einer Permutation $\sigma \in S_n$ ist definiert als

$$\operatorname{sg}(\sigma) \;:=\; \prod_{1 \leq i < j \leq n} \frac{\sigma(j)-\sigma(i)}{j-i}$$

Satz 1.2.25. *Es sei $n \in \mathbb{Z}_{\geq 1}$.*

(i) *Für jedes $\sigma \in S_n$ gilt $\operatorname{sg}(\sigma) = (-1)^{m(\sigma)}$, wobei $m(\sigma)$ die Zahl der Paare (i,j) mit $i<j$ und $\sigma(i) > \sigma(j)$ ist.*
(ii) *Für je zwei τ, σ gilt $\operatorname{sg}(\sigma \circ \tau) = \operatorname{sg}(\sigma)\operatorname{sg}(\tau)$.*

Beweis. Aussage (i) ergibt sich sofort mit

$$\begin{aligned}
\prod_{i<j} \sigma(j)-\sigma(i) &= \prod_{\substack{i<j \\ \sigma(i)>\sigma(j)}} \sigma(j)-\sigma(i) \;\cdot\; \prod_{\substack{i<j \\ \sigma(i)<\sigma(j)}} \sigma(j)-\sigma(i) \\
&= (-1)^{m(\sigma)} \prod_{\substack{i<j \\ \sigma(i)>\sigma(j)}} -\sigma(j)+\sigma(i) \;\cdot\; \prod_{\substack{i<j \\ \sigma(i)<\sigma(j)}} \sigma(j)-\sigma(i) \\
&= (-1)^{m(\sigma)} \prod_{\substack{j<i \\ \sigma(j)>\sigma(i)}} -\sigma(i)+\sigma(j) \;\cdot\; \prod_{\substack{i<j \\ \sigma(i)<\sigma(j)}} \sigma(j)-\sigma(i) \\
&= (-1)^{m(\sigma)} \prod_{\sigma(i)<\sigma(j)} \sigma(j)-\sigma(i) \\
&= (-1)^{m(\sigma)} \prod_{i<j} j-i.
\end{aligned}$$

Aussage (ii) folgt direkt aus

$$\prod_{i<j} \frac{\sigma\circ\tau(j)-\sigma\circ\tau(i)}{j-i} \quad = \quad \prod_{i<j} \frac{\sigma\circ\tau(j)-\sigma\circ\tau(i)}{\tau(j)-\tau(i)} \cdot \prod_{i<j} \frac{\tau(j)-\tau(i)}{j-i}$$

und

$$\begin{aligned}
\prod_{i<j} \frac{\sigma\circ\tau(j)-\sigma\circ\tau(i)}{\tau(j)-\tau(i)} &= \prod_{\substack{i<j\\ \tau(i)<\tau(j)}} \frac{\sigma\circ\tau(j)-\sigma\circ\tau(i)}{\tau(j)-\tau(i)} \prod_{\substack{i<j\\ \tau(i)>\tau(j)}} \frac{\sigma\circ\tau(j)-\sigma\circ\tau(i)}{\tau(j)-\tau(i)} \\
&= \prod_{\substack{i<j\\ \tau(i)<\tau(j)}} \frac{\sigma\circ\tau(j)-\sigma\circ\tau(i)}{\tau(j)-\tau(i)} \prod_{\substack{j<i\\ \tau(j)>\tau(i)}} \frac{\sigma\circ\tau(i)-\sigma\circ\tau(j)}{\tau(i)-\tau(j)} \\
&= \prod_{\tau(i)<\tau(j)} \frac{\sigma\circ\tau(j)-\sigma\circ\tau(i)}{\tau(j)-\tau(i)} \\
&= \prod_{i<j} \frac{\sigma(j)-\sigma(i)}{j-i}.
\end{aligned}$$

□

Beispiel 1.2.26. Es sei $n \in \mathbb{Z}_{\geq 1}$. Die *alternierende Gruppe* A_n ist die Untergruppe

$$A_n \ := \ \{\sigma \in S_n;\ \mathrm{sg}(\sigma) = 1\} \ \leq \ S_n.$$

Für den Index von A_n in S_n erhalten wir $[S_n : A_n] = 2$, da man für $n \geq 2$ mit der Transposition $(1, n)$ eine Zerlegung erhält

$$S_n \quad = \quad A_n \ \sqcup \ (1,n)A_n$$

Weiter ist A_n ein Normalteiler in S_n, denn für jedes $\alpha \in A_n$ und jedes $\sigma \in S_n$ gilt

$$\begin{aligned}
\mathrm{sg}(\sigma\circ\alpha\circ\sigma^{-1}) &= \mathrm{sg}(\sigma)\,\mathrm{sg}(\alpha)\,\mathrm{sg}(\sigma^{-1}) \\
&= \mathrm{sg}(\sigma)\,\mathrm{sg}(\sigma^{-1})\,\mathrm{sg}(\alpha) \\
&= \mathrm{sg}(\mathrm{id})\,\mathrm{sg}(\alpha) \\
&= 1.
\end{aligned}$$

Aufgaben zu Abschnitt 1.2.

Aufgabe 1.2.27 (Kleinsche Vierergruppe)**.** Zeige, dass die folgende Teilmenge eine Untergruppe von S_4 ist:

$$V_4 \quad := \quad \{\mathrm{id}_{X_4},\, (1,2)\circ(3,4),\, (1,3)\circ(2,4),\, (1,4)\circ(2,3)\}\,.$$

Aufgabe 1.2.28. Bestimme sämtliche Untergruppen der Einheitswurzelgruppe C_6, der symmetrischen Gruppe S_3 und der Faktorgruppe $\mathbb{Z}/541\mathbb{Z}$. Gib jeweils an, ob es sich um Normalteiler handelt.

Aufgabe 1.2.29. Es seien G eine Gruppe und $H_1, H_2 \leq G$ Untergruppen. Beweise die Äquivalenz folgender Aussagen:

(i) $H_1 \cup H_2$ ist eine Untergruppe von G.
(ii) Es gilt $H_1 \subseteq H_2$ oder $H_2 \subseteq H_1$.

Aufgabe 1.2.30. Es seien G eine Gruppe und $A \subseteq G$ eine nichtleere Teilmenge. Zeige: Ist G endlich, so gilt

$$\langle A\rangle \quad = \quad \{e_G\} \;\cup\; \{g_1 \cdots g_r;\; r \in \mathbb{Z}_{\geq 1},\; g_i \in A\}.$$

Schließe daraus:

(i) Eine nichtleere Teilmenge H einer endlichen Gruppe G ist genau dann eine Untergruppe, wenn für je zwei $g_1, g_2 \in G$ gilt

$$g_1, g_2 \in H \quad \Longrightarrow \quad g_1 g_2 \in H.$$

(ii) Die Ordnung eines Elements g einer beliebigen Gruppe G ist die kleinste Zahl $n \in \mathbb{Z}_{\geq 1}$ mit $g^n = e_G$.

Aufgabe 1.2.31. Zeige: Für jeden k-Zykel $(i_1, \ldots, i_k) \in S_n$ gilt

$$\mathrm{ord}(i_1, \ldots, i_k) \quad = \quad k.$$

Aufgabe 1.2.32. Betrachte folgende Elemente in der Gruppe $\mathrm{GL}(2,\mathbb{R})$ aller invertierbaren reellen 2×2-Matrizen:

$$g \;:=\; \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \qquad h \;:=\; \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}.$$

Zeige:

$$\mathrm{ord}(g) \;=\; 4, \qquad \mathrm{ord}(h) \;=\; 3, \qquad \mathrm{ord}(gh) \;=\; \infty.$$

Aufgabe 1.2.33. Zeige: $D_3 = S_3$.

Aufgabe 1.2.34. Betrachte die Diedergruppe $D_n \leq S_n$ und die beiden erzeugenden Elemente $\delta, \sigma \in D_n$ aus Beispiel 1.2.9. Zeige:

$$\sigma^2 = e, \qquad \delta^n = e, \qquad \delta^k \neq e \text{ für } 0 < k < n, \qquad \sigma\delta = \delta^{-1}\sigma.$$

Zeige weiter, dass D_n genau aus den Elementen der Form $\delta^k \circ \sigma^j$ besteht, wobei $0 \leq k < n$ und $j = 0, 1$. Schließe daraus $|D_n| = 2n$.

Aufgabe 1.2.35. Es seien G eine Gruppe, $H \leq G$ eine Untergruppe und $g_1, g_2 \in G$. Zeige:

$$g_1 H \;=\; g_2 H \quad \Longleftrightarrow \quad H g_1^{-1} \;=\; H g_2^{-1}.$$

Aufgabe 1.2.36. Es seien G eine Gruppe und $H \leq G$ eine Untergruppe. Zeige: H ist genau dann ein Normalteiler in G, wenn $gH = Hg$ für jedes $g \in G$ gilt.

Aufgabe 1.2.37. Es seien G eine endliche Gruppe und $H \leq G$ eine Untergruppe. Zeige:

(i) H besitzt genau $[G : H]$ Rechtsnebenklassen.
(ii) Gilt $[G : H] = 2$, so ist H ein Normalteiler.

Aufgabe 1.2.38. Es seien G eine Gruppe und $H_1, H_2 \trianglelefteq G$ Normalteiler. Zeige: $H_1 H_2 \subseteq G$ ist eine Untergruppe.

Aufgabe 1.2.39. Es seien G eine Gruppe und $M \subseteq G$ eine Teilmenge. Der *Normalisator* von M in G ist die Menge

$$N_G(M) \quad = \quad \{g \in G;\ gMg^{-1} = M\}$$

Beweise folgende Aussagen:

(i) Der Normalisator $N_G(M)$ ist eine Untergruppe von G.
(ii) Ist $H \leq G$ eine Untergruppe, so gilt $H \trianglelefteq N_G(H)$.
(iii) Für jede Untergruppe $H \leq G$ gilt $H \trianglelefteq G \ \Leftrightarrow \ N_G(H) = G$.

Aufgabe 1.2.40. Es sei $n \in \mathbb{Z}_{\geq 1}$. Jedes Element $\mu \in \mathbb{Z}/n\mathbb{Z}$ besitzt eine eindeutige Darstellung $\mu = m + n\mathbb{Z}$ mit $0 \leq m \leq n-1$. Bestimme diese Darstellungen für die Elemente

$$-(13+7\mathbb{Z}) \ \in \ \mathbb{Z}/7\mathbb{Z}, \qquad (5+4\mathbb{Z})+(6+4\mathbb{Z}) \ \in \ \mathbb{Z}/4\mathbb{Z}, \qquad 27(100+12\mathbb{Z}) \ \in \ \mathbb{Z}/12\mathbb{Z}.$$

Aufgabe 1.2.41. Berechne das Signum folgender Permutationen in S_9:

(i) $\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 7 & 4 & 3 & 6 & 2 & 9 & 5 & 1 \end{bmatrix}$,

(ii) $\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 1 & 3 & 5 & 4 & 7 & 2 & 9 & 8 \end{bmatrix}$,

(iii) $\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 7 & 3 & 2 & 4 & 5 & 6 & 8 & 1 \end{bmatrix}$.

1.3. **Homomorphismen.**

Definition 1.3.1. Ein *Homomorphismus* von Gruppen G und H ist eine Abbildung $\varphi\colon G \to H$, sodass für je zwei $g_1, g_2 \in G$ gilt

$$\varphi(g_1 g_2) \;=\; \varphi(g_1)\varphi(g_2).$$

Bemerkung 1.3.2.
(i) Für jede Gruppe G ist die Identität $\mathrm{id}_G\colon G \to G$ ein Homomorphismus von Gruppen.
(ii) Sind $\varphi\colon G \to H$ und $\psi\colon H \to F$ Homomorphismen von Gruppen, so ist dies auch die Hintereinanderausführung $\psi \circ \varphi\colon G \to F$.

Bemerkung 1.3.3. Es sei $\varphi\colon G \to H$ ein Homomorphismus von Gruppen. Dann gilt stets

$$\varphi(e_G) \;=\; e_H, \qquad\qquad \varphi(g^{-1}) \;=\; \varphi(g)^{-1}.$$

Beweis. Für den Nachweis der ersten Gleichung vermerken wir zunächst

$$\varphi(e_G) \;=\; \varphi(e_G e_G) \;=\; \varphi(e_G)\varphi(e_G).$$

Multiplikation mit $\varphi(e_G)^{-1}$ ergibt $e_H = \varphi(e_G)$. Für jedes $g \in G$ haben wir

$$\varphi(g^{-1})\varphi(g) \;=\; \varphi(g^{-1}g) \;=\; \varphi(e_G) \;=\; e_H.$$

Analog erhält man $\varphi(g)\varphi(g^{-1}) = e_H$. Das impliziert $\varphi(g^{-1}) = \varphi(g)^{-1}$. □

Beispiel 1.3.4. Die Exponentialfunktion definiert einen Homomorphismus

$$\exp\colon (\mathbb{C}, +) \;\to\; (\mathbb{C}^*, \cdot), \qquad z \mapsto e^z$$

Beispiel 1.3.5. Es sei $n \in \mathbb{Z}_{\geq 1}$. Dann haben wir einen Homomorphismus von den ganzen Zahlen in die Gruppe der n-ten Einheitswurzeln:

$$\varphi_n\colon (\mathbb{Z}, +) \;\to\; (C_n, \cdot), \qquad k \;\mapsto\; e^{2\pi i k/n}.$$

Beispiel 1.3.6. Für jeden Körper $\mathbb{K}$, z.B. $\mathbb{K} = \mathbb{Q}, \mathbb{R}, \mathbb{C}$, definiert die Determinante einen Homomorphismus

$$\det\colon \mathrm{GL}(n, \mathbb{K}) \;\to\; (\mathbb{K}^*, \cdot), \qquad A \;\mapsto\; \det(A).$$

Beispiel 1.3.7. Für jedes $n \in \mathbb{Z}_{\geq 1}$ definiert das Signum einen Homomorphismus

$$\mathrm{sg}\colon S_n \;\to\; C_2, \qquad \sigma \;\mapsto\; \mathrm{sg}(\sigma).$$

Definition 1.3.8. Es seien G und H Gruppen. Ein Homomorphismus $\varphi\colon G \to H$ heisst

(i) *Monomorphismus*, falls $\varphi\colon G \to H$ injektiv ist, bzw. *Epimorphismus*, falls $\varphi\colon G \to H$ surjektiv ist,
(ii) *Isomorphismus*, falls $\varphi\colon G \to H$ einen *Umkehrhomomorphismus* besitzt, d.h., einen Homomorphismus $\psi\colon H \to G$ mit

$$\psi \circ \varphi \;=\; \mathrm{id}_G, \qquad\qquad \varphi \circ \psi \;=\; \mathrm{id}_H.$$

Man nennt die Gruppen G und H *isomorph* zueinander, in Zeichen $G \cong H$, falls es einen Isomorphismus $\varphi\colon G \to H$ gibt.

Satz 1.3.9. *Es seien G und H Gruppen und $\varphi\colon G \to H$ ein Gruppenhomomorphismus. Dann sind folgende Aussagen äquivalent:*

(i) *$\varphi\colon G \to H$ ist ein Isomorphismus.*
(ii) *$\varphi\colon G \to H$ ist bijektiv.*

Beweis. Die Implikation "(i)⇒(ii)" ist klar. Zu "(ii)⇒(i)". Da $\varphi\colon G \to H$ bijektiv ist, gibt es eine Umkehrabbildung $\psi\colon H \to G$. Für je zwei $h_1, h_2 \in H$ gilt

$$h_1 h_2 \;=\; \varphi\left(\psi(h_1)\right)\varphi\left(\psi(h_2)\right) \;=\; \varphi\left(\psi(h_1)\,\psi(h_2)\right).$$

Wendet man ψ auf diese Identität an, so erhält man $\psi(h_1h_2) = \psi(h_1)\psi(h_2)$ für je zwei Elemente $h_1, h_2 \in H$. □

Konstruktion 1.3.10. Es seien G eine Gruppe und $H \trianglelefteq G$ ein Normalteiler. Dann hat man einen kanonischen Epimorphismus:

$$\pi\colon G \;\to\; G/H, \qquad g \;\mapsto\; gH.$$

Beweis. Offensichtlich ist $\pi\colon G \to H$ surjektiv. Die Homomorphieeigenschaft ergibt sich direkt aus der Definition der Verknüpfung auf G/H. Es gilt stets

$$\pi(g_1g_2) \;=\; g_1g_2H \;=\; g_1Hg_2H \;=\; \pi(g_1)\pi(g_2).$$

□

Definition 1.3.11. Es seien G und H Gruppen und $\varphi\colon G \to H$ ein Homomorphismus. *Kern* und *Bild* von φ sind definiert als

$$\begin{aligned} \operatorname{Kern}(\varphi) &:= \{g \in G;\ \varphi(g) = e_H\} \;=\; \varphi^{-1}(e_H), \\ \operatorname{Bild}(\varphi) &:= \{\varphi(g);\ g \in G\} \;=\; \varphi(G). \end{aligned}$$

Beispiel 1.3.12. Der Homomorphismus $\varphi_n\colon \mathbb{Z} \to C_n,\ k \;\mapsto\; e^{2\pi ik/n}$ besitzt die Untergruppe $n\mathbb{Z} \subseteq \mathbb{Z}$ als Kern und C_n als Bild.

Bemerkung 1.3.13. Es seien G eine Gruppe, $N \trianglelefteq G$ ein Normalteiler und $\pi\colon G \to G/N$, $g \mapsto gN$ der kanonische Epimorphismus. Dann gilt $\operatorname{Kern}(\pi) = N$.

Beweis. Die Aussage ergibt sich direkt aus

$$\pi(g) = e_GN \iff gN = e_GN \iff g \in N.$$

□

Satz 1.3.14. *Es sei $\varphi\colon G \to H$ ein Homomorphismus von Gruppen. Dann sind folgende Aussagen äquivalent:*

(i) *φ ist ein Monomorphismus.*
(ii) *Es gilt* $\operatorname{Kern}(\varphi) = \{e_G\}$.

Beweis. Zur Implikation "(i)⇒(ii)". Wegen der Injektivität von φ kann es höchstens ein Element $g \in G$ geben mit $\varphi(g) = e_H$, und e_G hat diese Eigenschaft.

Zur Implikation "(ii)⇒(i)". Es seien Elemente $g_1, g_2 \in G$ mit $\varphi(g_1) = \varphi(g_2)$ gegeben. Dann gilt

$$e_H \;=\; \varphi(g_2)^{-1}\varphi(g_1) \;=\; \varphi(g_2^{-1}g_1).$$

Das bedeutet $g_2^{-1}g_1 \in \operatorname{Kern}(\varphi)$ und somit, nach Voraussetzung, $g_2^{-1}g_1 = e_G$. Multiplikation mit g_2 von links ergibt $g_1 = g_2$. □

Bemerkung 1.3.15. Es sei $\varphi\colon G \to H$ ein Homomorphismus von Gruppen. Dann gilt:

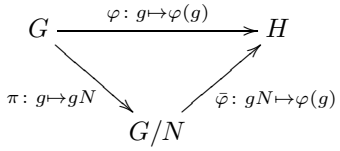
(i) Für jede Untergruppe $H' \leq H$ ist das Urbild $\varphi^{-1}(H')$ eine Untergruppe von G.
(ii) Gilt $H' \trianglelefteq H$, so gilt $\varphi^{-1}(H') \trianglelefteq G$; insbesondere ist $\operatorname{Kern}(\varphi) = \varphi^{-1}(e_H)$ Normalteiler in G.
(iii) Für jede Untergruppe $G' \leq G$ ist das Bild $\varphi(G')$ eine Untergruppe von H; insbesondere gilt $\operatorname{Bild}(\varphi) \leq H$.

(iv) Ist $\varphi\colon G \to H$ ein Epimorphismus, so gilt $\varphi(G') \trianglelefteq H$ für jeden Normalteiler $G' \trianglelefteq G$.

Beispiel 1.3.16. Die alternierende Gruppe $A_n \leq S_n$ ist ein Normalteiler in S_n, denn man hat

$$A_n \;=\; \{\sigma \in S_n;\ \mathrm{sg}(\sigma) = 1\} \;=\; \mathrm{Kern}(\mathrm{sg}).$$

Satz 1.3.17 (Homomorphiesatz)**.** *Es seien $\varphi\colon G \to H$ ein Gruppenhomomorphismus und $N \trianglelefteq G$ ein Normalteiler mit $N \subseteq \mathrm{Kern}(\varphi)$. Dann gibt es ein kommutatives Diagramm*



wohldefinierter Gruppenhomomorphismen. Der Homomorphismus $\bar\varphi\colon G/N \to H$ ist durch dieses kommutative Diagramm eindeutig bestimmt. Es gilt weiter

(i) *$\bar\varphi$ ist injektiv $\Leftrightarrow$ $N = \mathrm{Kern}(\varphi)$;*
(ii) *$\bar\varphi$ ist surjektiv $\Leftrightarrow$ φ ist surjektiv.*

Beweis. Wir zeigen zunächst, dass $\bar\varphi\colon gN \mapsto \varphi(g)$ wohldefiniert ist, d.h., nicht von der Wahl des Repräsentanten g der Nebenklasse gN abhängt. Dazu sei $g' \in G$ mit $g'N = gN$. Dann gilt $g' = gn$ mit einem $n \in N$. Wegen $N \subseteq \mathrm{Kern}(\varphi)$ gilt $\varphi(n) = e_H$, und es folgt

$$\varphi(g') \;=\; \varphi(gn) \;=\; \varphi(g)\varphi(n) \;=\; \varphi(g).$$

Nachdem wir die Wohldefiniertheit nachgewiesen haben, ist klar, dass das obige Diagramm mit diesem Ansatz für $\bar\varphi$ kommutativ ist. Weiter ist $\bar\varphi\colon G/N \to H$ ein Homomorphismus, denn für $g_1N, g_2N \in G/N$ erhalten wir

$$\bar\varphi(g_1Ng_2N) \;=\; \bar\varphi(g_1g_2N) \;=\; \varphi(g_1g_2) \;=\; \varphi(g_1)\varphi(g_2) \;=\; \bar\varphi(g_1N)\bar\varphi(g_2N).$$

Die Eindeutigkeit von $\bar\varphi\colon G/N \to H$ ist eine Folge der Kommutativität des Diagramms: Für jede Nebenklasse $gN \in G/N$ haben wir $\bar\varphi(gN) = \varphi(g)$, was den Homomorphismus $\bar\varphi$ bereits festlegt.

Wir zeigen (ii). Der Homomorphismus $\bar\varphi\colon G/N \to H$ ist genau dann injektiv, wenn $\mathrm{Kern}(\bar\varphi) = \{e_GN\}$ gilt. Wir müssen also zeigen:

$$\mathrm{Kern}(\bar\varphi) = \{e_GN\} \quad\Longleftrightarrow\quad \mathrm{Kern}(\varphi) = N.$$

Zur Implikation "$\Rightarrow$": Aufgrund der Kommutativität des Diagramms erhalten wir:

$$\mathrm{Kern}(\varphi) \;=\; \varphi^{-1}(e_H) \;=\; \pi^{-1}(\bar\varphi^{-1}(e_H)) \;=\; \pi^{-1}(\mathrm{Kern}(\bar\varphi)) \;=\; \pi^{-1}(e_GN) \;=\; N.$$

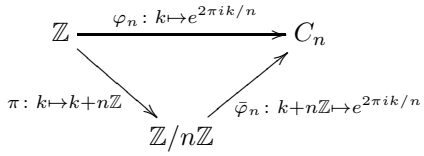
Zur Implikation "$\Leftarrow$". Wir erhalten $\mathrm{Kern}(\bar\varphi) = \{e_GN\}$ mit

$$\bar\varphi(gN) = e_H \iff \varphi(g) = e_H \iff g \in N \iff gN = e_GN.$$

Zu (ii). Das kommutative Diagramm und die Surjektivität von $\pi\colon G \to G/H$ liefern $\mathrm{Bild}(\bar\varphi) = \mathrm{Bild}(\varphi)$. Damit folgt die Behauptung. □

Folgerung 1.3.18. *Es sei $\varphi\colon G \to H$ ein Epimorphismus von Gruppen. Dann ist der induzierte Homomorphismus $\bar\varphi\colon G/\mathrm{Kern}(\varphi) \to H$ ein Isomorphismus.*

Beispiel 1.3.19. Wir betrachten den Epimorphismus $\varphi_n\colon \mathbb{Z} \to C_n$, $k \mapsto e^{2\pi ik/n}$. Nach dem Homomorphiesatz 1.3.17 gibt es ein kommutatives Diagramm



Wegen $\mathrm{Kern}(\varphi_n) = n\mathbb{Z}$ ist der induzierte Homomomorphismus $\bar{\varphi}_n\colon \mathbb{Z}/n\mathbb{Z} \to C_n$ ein Isomorphismus.

Satz 1.3.20 (Erster Isomorphiesatz)**.** *Es seien G eine Gruppe, $H \leq G$ eine Untergruppe, und $N \trianglelefteq G$ ein Normalteiler. Dann gilt*

(i) *HN ist eine Untergruppe von G.*
(ii) *N ist ein Normalteiler in HN.*
(iii) *$H \cap N$ ist ein Normalteiler in H.*
(iv) *Es gibt einen kanonischen Isomorphismus*

$$H/(H \cap N) \;\to\; (HN)/N, \qquad h(H \cap N) \;\mapsto\; hN.$$

Beweis. Zu (i). Offensichtlich gilt $e_G \in HN$. Weiter ergibt sich aus der Normalteilereigenschaft von N für beliebige $h, h' \in H$ und $n, n' \in N$:

$$hnh'n' \;\in\; HNHN \;=\; HN, \qquad (hn)^{-1} \;=\; n^{-1}h^{-1} \;\in\; NH \;=\; HN.$$

Aussage (ii) ergibt sich trivialerweise aus der Tatsache, dass N Normalteiler in G ist.

Um die noch offenen Aussagen (iii) und (iv) zu beweisen, betrachten wir den Epimorphismus

$$\varphi\colon H \to HN/N, \qquad h \mapsto hN.$$

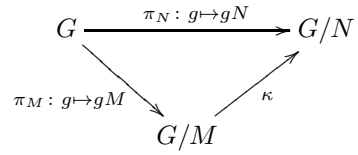
Dann gilt $\mathrm{Kern}(\varphi) = H \cap N$. Folglich ist $H \cap N$ Normalteiler in H, was Aussage (iii) beweist. Weiter erhalten wir Aussage (iv) mit Folgerung 1.3.18. □

Satz 1.3.21 (Zweiter Isomorphiesatz)**.** *Es seien G eine Gruppe, $M \trianglelefteq G$ und $N \trianglelefteq G$ Normalteiler in G mit $M \subseteq N$. Dann gilt:*

(i) *N/M ist ein Normalteiler in G/M.*
(ii) *Es gibt einen kanonischen Isomorphismus*

$$G/M \Big/ N/M \;\to\; G/N, \qquad (gM)(N/M) \;\mapsto\; gN.$$

Beweis. Nach dem Homomorphiesatz gibt es einen Epimorphismus $\kappa\colon G/M \to G/N$ mit dem das Diagramm



kommutativ wird. Unter Verwendung der Surjektivität von $\pi_M\colon G \to G/M$ erhalten wir

$$\mathrm{Kern}(\kappa) \;=\; \pi_M(\mathrm{Kern}(\pi_N)) \;=\; N/M \;\trianglelefteq\; G/M.$$

Das beweist Aussage (i). Wendet man weiter Folgerung 1.3.18 auf $\kappa\colon G/M \to G/N$ an, so erhält man Aussage (ii). □

Aufgaben zu Abschnitt 1.3.

Aufgabe 1.3.22. Es seien G, G' Gruppen und $\varphi\colon G \to G'$ ein Homomorphismus. Zeige:

(i) Der Homomorphismus φ ist genau dann ein Monomorphismus, wenn für je zwei Gruppenhomomorphismen $\psi_1, \psi_2\colon H \to G$ gilt
$$\psi_1 = \psi_2 \quad \Longleftrightarrow \quad \varphi \circ \psi_1 = \varphi \circ \psi_2.$$
(ii) Der Homomorphismus φ ist genau dann ein Epimorphismus, wenn $\varphi(G) \trianglelefteq G'$ gilt und für je zwei Gruppenhomomorphismen $\psi_1, \psi_2\colon G' \to H$ gilt
$$\psi_1 = \psi_2 \quad \Longleftrightarrow \quad \psi_1 \circ \varphi = \psi_2 \circ \varphi.$$

Aufgabe 1.3.23. Es sei $\varphi\colon G \to H$ ein Homomorphismus von Gruppen. Beweise die Aussagen von Bemerkung 1.3.15:

(i) Für jede Untergruppe $H' \leq H$ ist das Urbild $\varphi^{-1}(H')$ eine Untergruppe von G.
(ii) Gilt $H' \trianglelefteq H$, so gilt $\varphi^{-1}(H') \trianglelefteq G$; insbesondere ist $\mathrm{Kern}(\varphi) = \varphi^{-1}(e_H)$ Normalteiler in G.
(iii) Für jede Untergruppe $G' \leq G$ ist das Bild $\varphi(G')$ eine Untergruppe von H; insbesondere gilt $\mathrm{Bild}(\varphi) \leq H$.
(iv) Ist $\varphi\colon G \to H$ ein Epimorphismus, so gilt $\varphi(G') \trianglelefteq H$ für jeden Normalteiler $G' \trianglelefteq G$.

Aufgabe 1.3.24. Es sei $\varphi\colon G \to H$ ein Homomorphismus endlicher Gruppen. Beweise folgende Aussagen:

(i) Es gilt $|G| = |\mathrm{Kern}(\varphi)| \cdot |\mathrm{Bild}(\varphi)|$.
(ii) $|\mathrm{Bild}(\varphi)|$ teilt $|G|$.

Aufgabe 1.3.25. Zeige: Es gibt einen eindeutig bestimmten Homomorphismus $\varrho\colon S_n \to \mathrm{GL}(n, \mathbb{Q})$, sodass für jede Transposition $(i, j) \in S_n$ gilt
$$\varrho((i,j)) \quad = \quad (a_{kl})_{0 \leq k,l \leq n}, \quad \text{wobei } a_{kl} \ := \ \left\{ \begin{array}{ll} 1 & \text{falls } k = l,\ k \neq i, j, \\ 1 & \text{falls } k = i,\ l = j, \\ 1 & \text{falls } k = j,\ l = i, \\ 0 & \text{sonst.} \end{array} \right\}.$$
Zeige weiter, dass man mit diesem Homomorphismus ein kommutatives Diagramm von Gruppenhomomorphismen erhält:
$$\begin{array}{ccc} S_n & \xrightarrow{\varrho} & \mathrm{GL}(n, \mathbb{Q}) \\ {\scriptstyle \mathrm{sg}}\downarrow & & \downarrow{\scriptstyle \det} \\ C_2 & \xrightarrow[\subset]{} & \mathbb{Q}^* \end{array}$$

Aufgabe 1.3.26. Verwende Folgerung 1.3.18 für den Nachweis der Isomorphien $S_n/A_n \cong C_2$ und $\mathbb{C}^*/C_n \cong \mathbb{C}^*$. *Hinweis:* Im zweiten Fall betrachte den Homomorphismus $z \mapsto z^n$.

Aufgabe 1.3.27. Es sei $\mathbb{F}_2$ der Körper mit 2 Elementen. Zeige: Die Gruppe $\mathrm{GL}(2, \mathbb{F}_2)$ ist isomorph zu S_3.

Aufgabe 1.3.28. Es sei $B(n, \mathbb{C}) \subset \mathrm{GL}(n, \mathbb{C})$ die Menge der invertierbaren oberen Dreiecksmatrizen, und es sei
$$U(n, \mathbb{C}) \quad := \quad \{A \in B(n, \mathbb{C});\ a_{11} = \ldots = a_{nn} = 1\}$$
Zeige, dass $B(n, \mathbb{C})$ und $U(n, \mathbb{C})$ Untergruppen von $\mathrm{GL}(n, \mathbb{C})$ sind. Zeige weiter, dass $U(n, \mathbb{C})$ Normalteiler in $B(n, \mathbb{C})$ ist, und dass gilt
$$B(n, \mathbb{C})/U(n, \mathbb{C}) \quad \cong \quad (\mathbb{C}^*)^n.$$

Aufgabe 1.3.29. Betrachte folgende Untergruppen der Permutationsgruppe S_4:
$$S_3' \ := \ \{\sigma \in S_4;\ \sigma(4) = 4\}, \qquad V_4 \ := \ \langle (1,2)(3,4), (1,3)(2,4) \rangle.$$
Bestimme alle Elemente von V_4 und beweise folgende Aussagen:
$$S_3' \cong S_3, \qquad V_4 \trianglelefteq S_4, \qquad S_4 = S_3' V_4, \qquad S_4/V_4 \cong S_3.$$

Hinweis: Verwende den ersten Isomorphiesatz 1.3.20.

Aufgabe 1.3.30. Es seien G eine beliebige Gruppe und $H, N \leq G$ endliche Untergruppen, wobei N ein Normalteiler in G sei. Zeige:

$$|HN| \quad = \quad \frac{|H|\,|N|}{|H \cap N|}.$$

Aufgabe 1.3.31. Es seien $m, n, r \in \mathbb{Z}$ mit $m = nr$. Zeige: $(\mathbb{Z}/m\mathbb{Z})\big/(n\mathbb{Z}/m\mathbb{Z}) \;\cong\; \mathbb{Z}/n\mathbb{Z}$.

1.4. **Universelle Konstruktionen.**

Konstruktion 1.4.1 (Produkt I)**.** Es seien G_1 und G_2 Gruppen. Dann ist die Menge $G_1 \times G_2$ zusammen mit der komponentenweisen Verknüpfung

$$(g_1, g_2)(g_1', g_2') \quad := \quad (g_1 g_1', g_2 g_2')$$

eine Gruppe, das *(direkte) Produkt* der Gruppen G_1 und G_2. Neutrales Element und Inversenbildung in $G_1 \times G_2$ sind gegeben durch

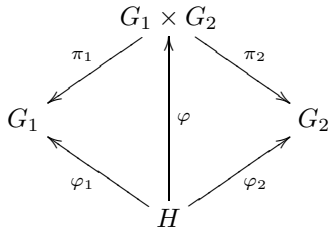
$$e_{G_1 \times G_2} \; = \; (e_{G_1}, e_{G_2}), \qquad\qquad (g_1, g_2)^{-1} \; = \; (g_1^{-1}, g_2^{-1}).$$

Weiter hat man kanonische Projektionshomomorphismen von $G_1 \times G_2$ auf die Faktoren G_1 und G_2:

$$\pi_1 \colon G_1 \times G_2 \; \to \; G_1, \quad (g_1, g_2) \; \mapsto \; g_1, \qquad \pi_2 \colon G_1 \times G_2 \; \to \; G_2, \quad (g_1, g_2) \; \mapsto \; g_2.$$

Satz 1.4.2. *Es seien G_1 und G_2 Gruppen. Dann besitzt $G_1 \times G_2$ zusammen mit den Homomorphismen $\pi_i \colon G_1 \times G_2 \to G_i$ die folgende universelle Eigenschaft:*

(PR) *Ist H eine Gruppe und sind $\varphi_1 \colon H \to G_1$ und $\varphi_2 \colon H \to G_2$ Homomorphismen, so gibt es einen eindeutig bestimmten Homomorphismus $\varphi \colon H \to G_1 \times G_2$, mit dem das folgende Diagramm kommutativ wird*



Beweis. Man kann den gewünschten Homomorphismus φ explizit angeben:

$$\varphi \colon H \; \to \; G_1 \times G_2, \qquad h \; \mapsto \; (\varphi_1(h), \varphi_2(h)).$$

Die Eindeutigkeit von φ ist bereits aus mengentheoretischen Gründen klar. □

Konstruktion 1.4.3 (Produkt II)**.** Es seien I eine beliebige Indexmenge und G_i, $i \in I$, eine Familie von Gruppen. Dann wird das kartesische Produkt $\prod_{i \in I} G_i$ durch komponentenweise Verknüpfung

$$(g_i)_{i \in I} \; (h_i)_{i \in I} \quad := \quad (g_i h_i)_{i \in I}$$

zu einer Gruppe, dem Produkt der Gruppen G_i, $i \in I$. Für jedes $j \in I$ hat man einen kanonischen Projektionshomomorphismus, nämlich

$$\pi_j \colon \prod_{i \in I} G_i \; \to \; G_j, \qquad (g_i)_{i \in I} \; \mapsto \; g_j.$$

Das Produkt $\prod_{i \in I} G_i$ erfüllt folgende universelle Eigenschaft: Zu jeder Familie $\varphi_i \colon H \to G_i$, $i \in I$, von Gruppenhomomorphismen gibt es einen eindeutig bestimmten Homomorphismus $\varphi \colon H \to \prod_{i \in I} G_i$ mit $\varphi_i = \pi_i \circ \varphi$ für jedes $i \in I$.

Schreibweise 1.4.4. Ist G eine Gruppe, so schreibt man auch G^n für das n-fache Produkt $\prod_{i=1}^{n} G$.

Definition 1.4.5. Es sei G eine Gruppe. Der *Kommutator* zweier Elemente g, h aus G ist das Element

$$[g, h] \; := \; ghg^{-1}h^{-1} \; \in \; G.$$

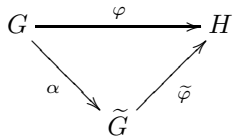
Die *Kommutatorgruppe* von G ist die von allen $[g, h]$, wobei $g, h \in G$, erzeugte Untergruppe von G; man bezeichnet sie mit $[G, G]$.

Bemerkung 1.4.6. Es sei G eine Gruppe.

(i) Für je zwei Elemente $g, h \in G$ gilt
$$[g,h] = e_G \iff ghg^{-1}h^{-1} = e_G \iff gh = hg.$$
(ii) Für je zwei Elemente $g, h \in G$ gilt
$$gh \;=\; ghg^{-1}h^{-1}hg \;=\; [g,h]hg.$$
(iii) Für je zwei Elemente $g, h \in G$ gilt
$$[g,h]^{-1} \;=\; (ghg^{-1}h^{-1})^{-1} \;=\; hgh^{-1}g^{-1} \;=\; [h,g].$$
(iv) $[G,G]$ besteht aus Produkten von Kommutatoren.
(v) Für je drei Elemente $a, g, h \in G$ gilt
$$\begin{aligned} a[g,h]a^{-1} &= aghg^{-1}h^{-1}a^{-1} \\ &= aga^{-1}aha^{-1}ag^{-1}a^{-1}ah^{-1}a^{-1} \\ &= [aga^{-1}, aha^{-1}]. \end{aligned}$$
(vi) $[G,G]$ ist ein Normalteiler in G.

Satz 1.4.7. *Es sei G eine Gruppe. Dann ist $\widetilde{G} := G/[G,G]$ eine abelsche Gruppe. Zusammen mit dem kanonischen Epimorphismus $\alpha\colon G \to \widetilde{G}$ besitzt sie folgende universelle Eigenschaft:*

(AB) *Zu jedem Homomorphismus $\varphi\colon G \to H$ in eine abelsche Gruppe H gibt es genau einen Homomorphismus $\widetilde{\varphi}\colon \widetilde{G} \to H$, sodass das folgende Diagramm kommutativ wird*



Beweis. Wir zeigen zunächst, dass $\widetilde{G}$ abelsch ist. Zu $\widetilde{g}, \widetilde{h} \in \widetilde{G}$ wählen wir Urbilder $g \in \alpha^{-1}(\widetilde{g})$ und $h \in \alpha^{-1}(\widetilde{h})$. Dann erhalten wir
$$\widetilde{g}\widetilde{h} \;=\; \alpha(gh) \;=\; \alpha([g,h]\,hg) \;=\; \alpha([g,h])\alpha(hg) \;=\; \alpha(hg) \;=\; \widetilde{h}\widetilde{g}.$$
Zur universellen Eigenschaft: Ist $\varphi\colon G \to H$ ein Homomorphismus in eine abelsche Gruppe, so gilt stets
$$\varphi([g,h]) \;=\; \varphi(ghg^{-1}h^{-1}) \;=\; \varphi(g)\varphi(h)\varphi(g)^{-1}\varphi(h)^{-1} \;=\; e_H.$$
Folglich haben wir $[G,G] \subseteq \operatorname{Kern}(\varphi)$. Der Homomorphiesatz 1.3.17 liefert dann Existenz und Eindeutigkeit des gewünschten Homomorphismus $\widetilde{\varphi}\colon \widetilde{G} \to H$. □

Definition 1.4.8. Eine *Halbgruppe* ist eine Menge H zusammen mit einer assoziativen Verknüpfung $(h_1, h_2) \mapsto h_1 * h_2$. Eine Halbgruppe heisst

(i) *abelsch (auch kommutativ)*, falls die Verknüpfung "$*$" kommutativ ist,
(ii) *Monoid* falls die Verknüpfung "$*$" ein neutrales Element besitzt.

Ein *Homomorphismus* von Halbgruppen H und H' ist eine Abbildung $\varphi\colon H \to H'$, sodass stets gilt
$$\varphi(h_1 * h_2) \;=\; \varphi(h_1) * \varphi(h_2).$$
Sind dabei H, H' Monoide und gilt $\varphi(e_H) = e_{H'}$ für die neutralen Elemente, so nennt man $\varphi\colon H \to H'$ auch einen *Homomorphismus* von Monoiden.

Wie bei Gruppenhomomorphismen definiert man die Begriffe Mono-, Epi-, bzw. Isomorphismus; dies sind injektive, surjektive, bzw. bijektive Homomorphismen.

Definition 1.4.9. Eine abelsche Halbgruppe H genügt der *Kürzungsregel*, falls für je drei Elemente a, b, c gilt

$$ab \;=\; ac \quad\Longrightarrow\quad b \;=\; c.$$

Beispiel 1.4.10. Die Menge $\mathbb{N} = \mathbb{Z}_{\geq 0}$ zusammen mit der Addition ist ein abelsches Monoid mit Kürzungsregel, aber keine Gruppe. Die Einbettung $\mathbb{N} \subseteq \mathbb{Z}$ in die Gruppe der ganzen Zahlen ist ein Monomorphimus von Monoiden.

Konstruktion 1.4.11 (Grothendieckgruppe)**.** Es sei $(M, \cdot)$ ein abelsches Monoid mit Kürzungsregel. Wir definieren eine Äquivalenzrelation auf $M \times M$ durch

$$(a_1, a_2) \;\sim\; (b_1, b_2) \quad :\Longleftrightarrow \quad a_1 b_2 \;=\; a_2 b_1.$$

Den zugehörigen Restklassenraum bezeichnen wir mit $G(M)$, und die Restklasse eines Elementes (a_1, a_2) mit a_1/a_2. Wir definieren eine Verknüpfung

$$G(M) \times G(M) \;\to\; G(M), \qquad \left(\frac{a_1}{a_2}\right)\left(\frac{b_1}{b_2}\right) \;:=\; \frac{a_1 b_1}{a_2 b_2}.$$

Die Menge $G(M)$ zusammen mit dieser Verknüpfung ist eine abelsche Gruppe; die *Grothendieckgruppe* des Monoids M.

Das neutrale Element von $G(M)$ ist e_M/e_M, das Inverse zu a_1/a_2 ist a_2/a_1, und man hat einen kanonischen Monoidmonomorphismus

$$\imath\colon M \;\to\; G(M), \qquad a \;\mapsto\; \frac{a}{e_M}.$$

Beweis. Zunächt ist zu zeigen, dass durch "$\sim$" tatsächlich eine Äquivalenzrelation auf $M \times M$ definiert wird, d.h., wir brauchen

- *Reflexivität:* Es gilt $a \sim a$ für alle $a \in M \times M$.
- *Symmetrie:* Es gilt $a \sim b \Rightarrow b \sim a$ für alle $a, b \in M \times M$.
- *Transitivität:* Es gilt $a \sim b$ und $b \sim c \Rightarrow a \sim c$ für alle $a, b, c \in M \times M$.

Reflexivität und Symmetrie sind offensichtlich gegeben. Zur Transitivität. Wir schreiben $a = (a_1, a_2)$, etc.. Aus $a \sim b$ und $b \sim c$ erhalten wir

$$a_1 b_2 \;=\; a_2 b_1, \qquad b_1 c_2 \;=\; b_2 c_1.$$

Multiplikation dieser beiden Gleichungen ergibt

$$a_1 b_2 b_1 c_2 \quad=\quad a_2 b_1 b_2 c_1.$$

Wendet man nun die Kürzungsregel an, so ergibt sich $a_1 c_2 = a_2 c_1$. Wir erhalten also $a \sim c$.

Der nächste Schritt ist, die Wohldefiniertheit der Verknüpfung auf $G(M)$ nachzuweisen. Dazu müssen wir zeigen, dass

$$\frac{a_1 b_1}{a_2 b_2} \quad=\quad \frac{a_1' b_1'}{a_2' b_2'}$$

gilt, sobald $a \sim a'$ und $b \sim b'$ gelten, wobei wie bisher $a = (a_1, a_2)$, etc. gelte. Schreiben wir letztere Äquivalenzen aus, so erhalten wir

$$a_1 a_2' \;=\; a_2 a_1', \qquad b_1 b_2' \;=\; b_2 b_1'.$$

Multipliziert man diese beiden Gleichungen miteinander, so ergibt sich die gewünschte Äquivalenz.

Der Rest ist nun einfach: Mit e_M/e_M haben wir offensichtlich ein neutrales Element in $G(M)$, und die Inversenbildung ist ebenfalls leicht: Man hat stets

$$\left(\frac{a_1}{a_2}\right)\left(\frac{a_2}{a_1}\right) \;=\; \frac{a_1 a_2}{a_2 a_1} \;=\; \frac{e_M}{e_M}.$$

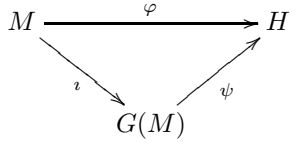
Die Tatsache, dass die kanonische Abbildung $\imath\colon M \to G(M)$ ein Monoidmonomorphismus ist, ergibt sich sofort aus

$$\left(\frac{a}{e_M}\right)\left(\frac{b}{e_M}\right) \;=\; \frac{ab}{e_M}, \qquad\qquad \frac{a}{e_M} = \frac{b}{e_M} \;\iff\; a = b.$$

□

Satz 1.4.12. *Es sei M ein abelsches Monoid mit Kürzungsregel. Dann besitzt die zugehörige Grothendieckgruppe $G(M)$ zusammen mit dem kanonischen Monomorphismus $\imath\colon M \to G(M)$ die folgende universelle Eigenschaft:*

(GR) *Zu jedem Monoidhomomorphismus $\varphi\colon M \to H$ in eine abelsche Gruppe H gibt es genau einen Gruppenhomomorphismus $\psi\colon G(M) \to H$, sodass das folgende Diagramm kommutativ wird*



Beweis. Es sei $\varphi\colon M \to H$ ein Homomorphismus in eine abelsche Gruppe H. Wir setzen

$$\psi\colon G(M) \;\to\; H, \qquad \frac{a_1}{a_2} \;\mapsto\; \varphi(a_1)\varphi(a_2)^{-1}.$$

Dies hängt nicht von der Wahl des Repräsentanten (a_1, a_2), denn wir haben

$$\begin{aligned}(a_1, a_2) \;\sim\; (a_1', a_2') \quad &\Longrightarrow \quad a_1 a_2' \;=\; a_2 a_1' \\ &\Longrightarrow \quad \varphi(a_1)\varphi(a_2') \;=\; \varphi(a_2)\varphi(a_1') \\ &\Longrightarrow \quad \varphi(a_1)\varphi(a_2)^{-1} \;=\; \varphi(a_1')\varphi(a_2')^{-1}.\end{aligned}$$

Die Homomorphieeigenschaft von ψ ist ebenfalls leicht zu sehen: Es gilt

$$\begin{aligned}\psi\left(\frac{a_1}{a_2}\,\frac{b_1}{a_2}\right) \;&=\; \psi\left(\frac{a_1 b_1}{a_2 b_2}\right) \\ &=\; \varphi(a_1 b_1)\varphi(a_2 b_2)^{-1} \\ &=\; \varphi(a_1)\varphi(a_2)^{-1}\varphi(b_1)\varphi(b_2)^{-1} \\ &=\; \psi\left(\frac{a_1}{a_2}\right)\psi\left(\frac{b_1}{a_2}\right).\end{aligned}$$

Zur Kommutativität des Diagramms vermerken wir zunächst, dass $\varphi(e_M) = e_H$ gilt; dies ist für Monoidhomomorphismen in eine Gruppe genauso einzusehen wie für Gruppenhomomorphismen. Damit erhalten wir

$$\psi(\imath(a)) \;=\; \psi\left(\frac{a}{e_M}\right) \;=\; \varphi(a)\varphi(e_M)^{-1} \;=\; \varphi(a).$$

Kommen wir zur Eindeutigkeit von $\psi\colon G(M) \to H$. Dazu betrachten wir einen weiteren Homomorphismus $\psi'\colon G(M) \to H$ mit $\psi' \circ \imath = \varphi$. Dann erhalten wir stets

$$\psi'\left(\frac{a}{e_M}\right) \;=\; \varphi(a) \;=\; \psi\left(\frac{a}{e_M}\right), \qquad\qquad \psi'\left(\frac{e_M}{b}\right) \;=\; \varphi(b)^{-1} \;=\; \psi'\left(\frac{e_M}{b}\right)$$

wobei man die zweite Gleichung durch Invertieren der ersten erhält. Multiplikation dieser Gleichungen ergibt $\psi'(a/b) = \psi(a/b)$. □

Aufgaben zu Abschnitt 1.4.

Aufgabe 1.4.13. Es seien G, H, Γ Gruppen und $\pi_G\colon \Gamma \to G$ sowie $\pi_H\colon \Gamma \to H$ Homomorphismen mit der Eigenschaft (PR) aus Satz 1.4.2. Zeige: Die Gruppe Γ ist isomorph zum gruppentheoretischen Produkt $G \times H$.

Aufgabe 1.4.14. Es seien G eine Gruppe und $H_1, H_2 \trianglelefteq G$ Normalteiler mit

(i) $G = H_1H_2$,
(ii) $H_1 \cap H_2 = \{e_G\}$.

Zeige: Es gilt $G \cong H_1 \times H_2$.

Aufgabe 1.4.15 (Semidirektes Produkt)**.** Es seien G, H Gruppen, und es sei $\Phi\colon G \to \mathrm{Aut}(H)$ ein Homomorphismus. Zeige: $G \times H$ wird zu einer Gruppe durch

$$(g,h) *_\Phi (g',h') \qu:=\quad (g\Phi(g')(h), g'h').$$

Aufgabe 1.4.16. Zeige: Für die Gruppe $\mathrm{GL}(2,\mathbb{C})$ der invertierbaren (2×2)-Matrizen und die Untergruppe $\mathrm{SL}(2,\mathbb{C}) \leq \mathrm{GL}(2,\mathbb{C})$ aller (2×2)-Matrizen der Determinante 1 gelten

$$[\mathrm{GL}(2,\mathbb{C}), \mathrm{GL}(2,\mathbb{C})] \;=\; \mathrm{SL}(2,\mathbb{C}), \qquad [\mathrm{SL}(2,\mathbb{C}), \mathrm{SL}(2,\mathbb{C})] \;=\; \mathrm{SL}(2,\mathbb{C}).$$

Aufgabe 1.4.17. Es sei $B(2,\mathbb{C}) \leq \mathrm{GL}(2,\mathbb{C})$ die Untergruppe der invertierbaren oberen (2×2)-Dreiecksmatrizen, und es sei

$$U(2,\mathbb{C}) \;:=\; \{A \in B(2,\mathbb{C});\; a_{11} = a_{22} = 1\} \;\leq\; B(2,\mathbb{C}).$$

Zeige:

$$[B(2,\mathbb{C}), B(2,\mathbb{C})] \;=\; U(2,\mathbb{C}), \qquad [U(2,\mathbb{C}), U(2,\mathbb{C})] \;=\; \{E_2\}.$$

Aufgabe 1.4.18. Es sei $\varphi\colon G \to G'$ ein Homomorphismus von Gruppen. Zeige: Für jede Untergruppe $H \leq G$ gilt

$$\varphi([H,H]) \quad=\quad [\varphi(H), \varphi(H)]$$

Zeige weiter: Ist $\varphi\colon G \to G'$ ein Epimorphismus, so gilt für jede Untergruppe $H' \leq G'$:

$$\varphi^{-1}([H',H']) \quad=\quad [\varphi^{-1}(H'), \varphi^{-1}(H')].$$

Aufgabe 1.4.19. Es seien G eine Gruppe Γ eine abelsche Gruppe und $\alpha\colon G \to \Gamma$ ein Epimorphismus mit der Eigenschaft (AB) aus Satz 1.4.7. Zeige: Die Gruppe Γ ist isomorph zu $G/[G,G]$.

Aufgabe 1.4.20. Verallgemeinere Konstruktion 1.4.11 auf eine beliebige abelsche Halbgruppe M. Verwende dabei die Relation

$$(a',b') \;\sim\; (a,b) \quad :\Longleftrightarrow \quad a'bc \;=\; ab'c \text{ mit einem } c \in M.$$

Zeige: Der kanonische Halbgruppenhomomorphismus $\imath\colon M \to G(M)$, $a \mapsto a^2/a$ ist genau dann injektiv, wenn M der Kürzungsregel genügt.

2. Struktur endlicher Gruppen

2.1. **Zyklische Gruppen.**

Definition 2.1.1. Eine Gruppe G heißt *zyklisch*, falls sie ein *erzeugendes Element* besitzt, d.h., falls es ein $g \in G$ gibt mit $G = \langle g \rangle$.

Bemerkung 2.1.2. Ist G eine zyklische Gruppe mit erzeugendem Element $g \in G$, so haben wir $G = \{g^n;\ n \in \mathbb{Z}\}$.

Beispiel 2.1.3. Die additive Gruppe $\mathbb{Z}$ ist zyklisch: Es gilt $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$. Weiter betrachten wir für $n \in \mathbb{Z}_{\geq 1}$ die Faktorgruppe $\mathbb{Z}/n\mathbb{Z}$. Dann gilt

$$\mathbb{Z}/n\mathbb{Z} \ = \ \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}, \qquad \overline{m} \ := \ m + n\mathbb{Z} \ \in \ \mathbb{Z}/n\mathbb{Z}.$$

Insbesondere ist $\mathbb{Z}/n\mathbb{Z}$ eine zyklische Gruppe der Ordnung n, und das Element $\overline{1} \in \mathbb{Z}/n\mathbb{Z}$ ist ein Erzeugendes.

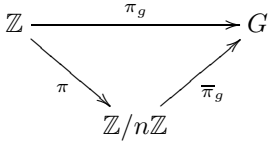
Satz 2.1.4. *Es sei G eine endliche Gruppe, sodass $|G|$ eine Primzahl ist. Dann gilt $G = \langle g \rangle$ für jedes $g \in G$ mit $g \neq e_G$. Insbesondere ist G zyklisch.*

Beweis. Es sei $g \in G$ mit $g \neq e_G$ gegeben. Wir betrachten $H := \langle g \rangle \leq G$. Wegen $g \neq e_G$ gilt $|H| > 1$ und nach dem Satz von Lagrange ist $|H|$ ein Teiler von $|G|$. Da $|G|$ prim ist, folgt $|H| = |G|$. Das impliziert $H = G$. □

Satz 2.1.5. *Es seien G eine zyklische Gruppe und $g \in G$ ein Element mit $G = \langle g \rangle$. Dann hat man einen Epimorphismus*

$$\pi_g \colon \mathbb{Z} \ \to \ G, \qquad k \ \mapsto \ g^k.$$

Gilt $|G| = \infty$, so ist $\pi_g \colon \mathbb{Z} \to G$ ein Isomorphismus. Gilt $|G| = n < \infty$, so hat man ein kommutatives Diagramm



wobei $\pi \colon \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ den Restklassenhomomorphismus bezeichnet und die induzierte Abbildung $\overline{\pi}_g \colon \mathbb{Z}/n\mathbb{Z} \to G$ ein Isomorphismus ist.

Folgerung 2.1.6 (Klassifikation zyklischer Gruppen)**.** *Es sei G eine zyklische Gruppe. Dann gilt entweder $G \cong \mathbb{Z}$ oder G ist endlich und man hat $G \cong \mathbb{Z}/n\mathbb{Z}$, wobei $n = |G|$.*

Lemma 2.1.7. *Es sei $H \leq \mathbb{Z}$ eine Untergruppe. Dann gilt $H = n\mathbb{Z}$ mit einem $n \in \mathbb{Z}_{\geq 0}$. Insbesondere ist H zyklisch.*

Beweis. Falls $H = \{0\}$ gilt, erfüllt $n = 0$ die Aussage. Betrachten wir nun den Fall $H \neq \{0\}$. Dann muss H positive Elemente enthalten. Wir wählen $n \in \mathbb{Z}_{\geq 1}$ minimal mit $n \in H$, und zeigen

$$H \quad = \quad n\mathbb{Z}.$$

Die Inklusion "$\supseteq$" ist offensichtlich. Zur Inklusion "$\subseteq$". Nehmen wir an, es existiere ein $m \in H \setminus n\mathbb{Z}$. Dann dürfen wir $m \in \mathbb{Z}_{\geq 1}$ annehmen. Division mit Rest liefert eine Darstellung

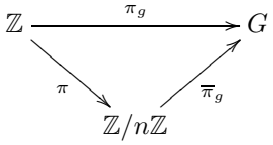
$$m \quad = \quad kn + m'$$

mit $k \in \mathbb{Z}_{\geq 0}$ und einer Zahl $m' \in \mathbb{Z}_{\geq 1}$ mit $m' < n$. Der obigen Gleichung entnehmen wir insbesondere $m' = m - kn \in H$. Das steht jedoch im Widerspruch zur Minimalität von n. □

Beweis von Satz 2.1.5. Die Tatsache, dass $\pi_g\colon \mathbb{Z} \to G$ ein Epimorphismus ist, folgt unmittelbar aus den Potenzgesetzen 1.1.19. Nach Lemma 2.1.7 gibt es ein $n \in \mathbb{Z}_{\geq 0}$ mit

$$\operatorname{Kern}(\pi_g) \quad = \quad n\mathbb{Z}.$$

Gilt $n = 0$, so ist $\pi_g\colon \mathbb{Z} \to G$ ein Isomorphismus, und wir erhalten insbesondere $|G| = \infty$. Gilt $n > 0$, so liefert uns Folgerung 1.3.18 ein kommutatives Diagramm mit einem Isomorphismus $\overline{\pi}_g\colon \mathbb{Z}/n\mathbb{Z} \to G$, nämlich



Insbesondere besitzt G die Ordnung $n < \infty$. Die Aussagen des Satzes ergeben sich nun unmittelbar: $|G| = \infty$ führt zu $G \cong \mathbb{Z}$, und $|G| < \infty$ führt zu $G \cong \mathbb{Z}/n\mathbb{Z}$ mit $n \in \mathbb{Z}_{\geq 1}$. □

Folgerung 2.1.8 (Kleiner Fermatscher Satz)**.** *Es sei G eine endliche Gruppe. Dann gilt $g^{|G|} = e_G$ für jedes $g \in G$.*

Beweis. Nach dem Satz von Lagrange ist $n := |G|$ ein Vielfaches der Ordnung $m := \operatorname{ord}_G(g)$ der zyklischen Gruppe $\langle g \rangle$, etwa $n = dm$. Nach Satz 2.1.5 haben wir $\langle g \rangle \cong \mathbb{Z}/m\mathbb{Z}$ und erhalten somit

$$g^n \;=\; g^{dm} \;=\; (g^m)^d \;=\; e_G^d \;=\; e_G.$$

□

Folgerung 2.1.9. *Es seien G eine zyklische Gruppe und $H \leq G$ eine Untergruppe. Dann gilt:*

(i) *G ist abelsch;*
(ii) *H ist zyklisch;*
(iii) *G/H ist zyklisch.*

Beweis. Aussage (i) ist klar nach Satz 2.1.6. Für die weiteren Aussagen wählen wir ein $g \in G$ mit $G = \langle g \rangle$. Aussage (iii) ergibt sich direkt aus

$$G/H \;=\; \{g^n H;\; n \in \mathbb{Z}\} \;=\; \{(gH)^n;\; n \in \mathbb{Z}\} \;=\; \langle gH \rangle.$$

Wir kommen zu Aussage (ii). Satz 2.1.5 liefert einen Epimorphismus

$$\pi_g\colon \mathbb{Z} \;\to\; G, \qquad n \;\mapsto\; g^n.$$

Die Untergruppe $H' := \pi_g^{-1}(H)$ ist nach Lemma 2.1.7 zyklisch. Mit Aussage (iii) ergibt sich, dass $H \cong H'/\operatorname{Kern}(\pi_g)$ zyklisch ist. □

Satz 2.1.10. *Es seien $G = \langle g \rangle$ eine zyklische Gruppe mit $n := |G| < \infty$ und $d \in \mathbb{Z}_{\geq 1}$ ein Teiler von n. Dann gibt es genau eine Untergruppe $H \leq G$ mit $|H| = d$, nämlich $H := \langle g^m \rangle$ für $m := n/d$.*

Beweis. Nach Satz 2.1.5 dürfen wie annehmen, dass $G = \mathbb{Z}/n\mathbb{Z}$ mit einem $n \in \mathbb{Z}_{\geq 1}$ gilt. Wir betrachten $m = n/d$ und die zugehörige Untergruppe

$$H \;:=\; \langle \overline{m} \rangle \;=\; \{\overline{0}, \overline{m}, 2\overline{m}, \ldots, (d-1)\overline{m}\} \;\leq\; G.$$

Offensichtlich gilt $|H| = d$; die Gruppe G besitzt also (mindestens) eine Untergruppe der Ordnung d.

Es sei nun $H' \leq G$ eine weitere Untergruppe mit $|H'| = d$. Dann gilt $H' = \langle \overline{k} \rangle$ mit $0 \leq k \leq n$. Wegen $d\overline{k} = \overline{0}$ erhalten wir $dk \in n\mathbb{Z}$ und somit

$$dk \;=\; ln \;=\; ldm$$

mit einem $l \in \mathbb{Z}_{\geq 1}$. Es folgt $k = lm$ und somit $\overline{k} = l\overline{m} \in H$. Das impliziert $H' \subseteq H$. Wegen $|H'| = |H|$ ergibt sich $H' = H$. □

Konstruktion 2.1.11. Es sei $n \in \mathbb{Z}_{\geq 1}$. Dann hat man für jedes $a \in \mathbb{Z}$ einen wohldefinierten Homomorphismus

$$\varphi_a \colon \mathbb{Z}/n\mathbb{Z} \;\to\; \mathbb{Z}/n\mathbb{Z}, \qquad \overline{m} \;\mapsto\; a\overline{m} = \overline{am}.$$

Dabei gilt stets $\varphi_{a+kn} = \varphi_a$. Weiter hat man für je zwei $a, b \in \mathbb{Z}$:

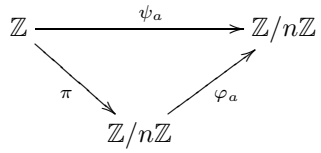
$$\varphi_b \circ \varphi_a \;=\; \varphi_{ba} \;=\; \varphi_{ab} \;=\; \varphi_a \circ \varphi_b.$$

Beweis. Nur zur Wohldefiniertheit von φ_a ist etwas zu zeigen; diese lässt sich zwar auch elementar einsehen, wir wollen aber den Homomorphisatz anwenden.

Die Verkettung der Homomorphismen $\mathbb{Z} \to \mathbb{Z}$, $m \mapsto am$ und $\mathbb{Z} \mapsto n\mathbb{Z}$, $m \mapsto \overline{m}$ definiert einen Homomorphismus

$$\psi_a \colon \mathbb{Z} \;\to\; \mathbb{Z}/n\mathbb{Z}, \qquad m \;\mapsto\; a\overline{m} = \overline{am}.$$

Der Homomorphiesatz liefert dann ein kommutatives Diagramm, das unseren Homomorphismus φ_a enthält:



□

Satz 2.1.12. *Es seien $n \in \mathbb{Z}_{\geq 1}$, $a \in \mathbb{Z}$ und $\varphi_a \colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $\overline{m} \;\mapsto = \overline{am}$ wie in Konstruktion 2.1.11. Dann sind folgende Aussagen äquivalent:*

(i) *Der Homomorphismus φ_a ist ein Isomorphismus,*
(ii) *Die Zahlen a und n sind teilerfremd.*

Beweis. Zur Implikation "(i)⇒(ii)". Es sei d ein gemeinsamer Teiler von a und n. Dann hat man

$$a \;=\; a_1 d, \qquad n \;=\; n_1 d$$

mit $a_1, n_1 \in \mathbb{Z}$. Es folgt

$$\varphi_a(\overline{n_1}) \;=\; a\overline{n_1} \;=\; \overline{an_1} \;=\; \overline{a_1 n} \;=\; \overline{0}.$$

Die Injektivität von φ_a liefert $\overline{n_1} = \overline{0}$ und somit $n_1 \in n\mathbb{Z}$. Das impliziert $d = \pm 1$. Mit anderen Worten, a und n sind teilerfremd.

Zur Implikation "(ii)⇒(i)". Es genügt zu zeigen, dass φ_a injektiv ist. Für jedes $\overline{m} \in \mathbb{Z}/n\mathbb{Z}$ gilt:

$$\begin{aligned}
\varphi_a(m) \;=\; \overline{0} \quad &\Longrightarrow \quad \overline{am} \;=\; \overline{0} \\
&\Longrightarrow \quad am \;\in\; n\mathbb{Z} \\
&\Longrightarrow \quad am \;=\; nl \text{ mit einem } l \in \mathbb{Z} \\
&\Longrightarrow \quad m \;=\; n\frac{l}{a} \text{ mit einem } l \in \mathbb{Z} \\
&\Longrightarrow \quad m \;\in\; n\mathbb{Z} \\
&\Longrightarrow \quad \overline{m} \;=\; \overline{0},
\end{aligned}$$

wobei im vorletzten Schritt die Teilerfremdheit von a und n die Ganzzahligkeit von l/a garantiert. □

Konstruktion 2.1.13. Es sei $n \in \mathbb{Z}_{\geq 1}$. Die *Primrestklassengruppe modulo* n ist die Menge

$$\mathrm{PR}_n \ := \ \{\overline{a} \in \mathbb{Z}/n\mathbb{Z};\ a, n \text{ sind teilerfremd}\}$$

zusammen mit der (kommutativen) Verknüpfung

$$\mathrm{PR}_n \times \mathrm{PR}_n \ \to \ \mathrm{PR}_n, \qquad \overline{a}\,\overline{b} \ := \ \overline{ab}.$$

Beweis. Offensichtlich ist die Verknüpfung wohldefiniert, assoziativ, kommutativ und hat $\overline{1}$ als neutrales Element. Ist $\overline{a} \in \mathrm{PR}_n$ gegeben, so gibt es ein $\overline{b} \in \mathbb{Z}/n\mathbb{Z}$ mit

$$1 \ = \ \varphi_a(\overline{b}) \ = \ \overline{ab} \ = \ \overline{a}\overline{b}.$$

Es bleibt zu zeigen, dass $\overline{b} \in \mathrm{PR}_n$ gilt, d.h., dass b und n teilerfremd sind. Dazu sei d ein gemeinsamer Teiler von b und n. Dann haben wir

$$b \ = \ b_1 d, \qquad\qquad n \ = \ n_1 d.$$

Die vorige Gleichung liefert $ab = 1 + ln$ mit einem $l \in \mathbb{Z}$ und somit $1 = (ab_1 - ln_1)d$. Das impliziert $d = \pm 1$, was die Teilerfremdheit von b und n bedeutet. □

Konstruktion 2.1.14. Es sei G eine Gruppe. Die *Automorphismengruppe* von G ist die Untergruppe

$$\mathrm{Aut}(G) \ := \ \{\varphi\colon G \to G;\ \varphi \text{ ist Gruppenisomorphismus}\} \ \leq \ S(G).$$

Satz 2.1.15. *Es sei $n \in \mathbb{Z}_{\geq 1}$. Dann hat man einen Gruppenisomorphismus*

$$\mathrm{PR}_n \ \to \ \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}), \qquad \overline{a} \ \mapsto \ \varphi_a.$$

Beweis. Die Wohldefiniertheit und Homomorphieeigenschaft ergeben sich direkt aus Bemerkung 2.1.11. Die Injektivität folgt direkt aus

$$\varphi_a = \varphi_b \ \implies \ \varphi_a(\overline{1}) = \varphi_b(\overline{1}) \ \implies \ \overline{a} = \overline{b} \in \mathbb{Z}/n\mathbb{Z}.$$

Für den Nachweis der Surjektivität sei $\varphi \in \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ gegeben. Dann gilt $\varphi(\overline{1}) = \overline{a}$ mit $a \in \{1, \ldots, n-1\}$. Das impliziert bereits $\varphi = \varphi_a$, denn für jedes $\overline{m} \in \mathbb{Z}/n\mathbb{Z}$ gilt

$$\varphi(\overline{m}) \ = \ \varphi(m\overline{1}) \ = \ m\varphi(\overline{1}) \ = \ m\overline{a} \ = \ m\varphi_a(\overline{1}) \ = \ \varphi_a(m\overline{1}) \ = \ \varphi_a(\overline{m}).$$

□

Aufgaben zu Abschnitt 2.1.

Aufgabe 2.1.16. Es sei G eine Gruppe. Beweise die Äquivalenz folgender Aussagen:

(i) G ist von endlicher Ordnung.
(ii) G besitzt nur endlich viele Untergruppen.

Aufgabe 2.1.17. Betrachte $(\mathbb{Z},+)$ als Untergruppe von $(\mathbb{Q},+)$ und zeige für die Faktorgruppe $\mathbb{Q}/\mathbb{Z}$:

(i) Jedes Element von $\mathbb{Q}/\mathbb{Z}$ besitzt endliche Ordnung.
(ii) Jede endliche Untergruppe von $\mathbb{Q}/\mathbb{Z}$ ist zyklisch.
(iii) Zu jedem $n \in \mathbb{Z}_{\geq}1$ gibt es genau eine Untergruppe der Ordnung n in $\mathbb{Q}/\mathbb{Z}$.

Aufgabe 2.1.18. Es seien $n \in \mathbb{Z}_{\geq 2}$ und $\overline{m} \in \mathbb{Z}/n\mathbb{Z}$. Beweise die Äquivalenz folgender Aussagen:

(i) Das Element $\overline{m}$ erzeugt die additive Gruppe $\mathbb{Z}/n\mathbb{Z}$.
(ii) Die Zahlen m und n sind teilerfremd.

Aufgabe 2.1.19. Es seien $m,n \in \mathbb{Z}_{\geq 1}$. Betrachte das Element $\overline{m} \in \mathbb{Z}/n\mathbb{Z}$ und zeige:

$$\operatorname{ord}(\overline{m}) \quad = \quad \frac{n}{\operatorname{ggT}(m,n)}.$$

Aufgabe 2.1.20. Es seien $m,n \in \mathbb{Z}_{\geq 1}$. Beweise die Äquivalenz folgender Aussagen:

(i) Die Zahlen m und n sind teilerfremd.
(ii) Es gibt ganze Zahlen a,b mit $am+bn=1$.
(iii) Es gibt einen Isomorphismus $\mathbb{Z}/nm\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

Aufgabe 2.1.21. Welche der folgenden Gruppen ist zyklisch (Begründung):

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \qquad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}, \qquad \mathbb{Z}/21\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}, \qquad \mathbb{Z}/15\mathbb{Z} \times \mathbb{Z}/28\mathbb{Z}.$$

Aufgabe 2.1.22. Es seien $n,m \in \mathbb{Z}_{\geq 1}$. Zeige: Es gibt genau dann einen nichttrivialen Homomorphismus $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$, wenn n und m einen gemeinsamen Teiler besitzen.

Aufgabe 2.1.23. Bestimme alle Homomorphismen $\mathbb{Z}/24\mathbb{Z} \to \mathbb{Z}/18\mathbb{Z}$.

Aufgabe 2.1.24. Es sei G eine Gruppe. Beweise Konstruktion 2.1.14: Zusammen mit der Hintereinanderausführung ist die Menge

$$\operatorname{Aut}(G) \quad := \quad \{\varphi\colon G \to G;\ \varphi \text{ ist Gruppenisomorphismus}\}$$

eine Gruppe. Betrachte weiter für jedes $a \in G$ die Abbildung $\kappa_a\colon G \to G$, $g \mapsto a^{-1}ga$. Zeige, dass die Menge all dieser Abbildungen eine Untergruppe von $\operatorname{Aut}(G)$ ist.

Aufgabe 2.1.25. Bestimme die Automorphismengruppe der additiven Gruppe $\mathbb{Z}$.

Aufgabe 2.1.26. Es sei $p \in \mathbb{Z}_{\geq 1}$ eine Primzahl. Zeige: Für jede Zahl $a \in \mathbb{Z} \setminus p\mathbb{Z}$ gilt $a^{p-1} \equiv 1 \bmod p$. *Hinweis*: Betrachte das Element $\varphi_a \in \operatorname{Aut}(\mathbb{Z}/p\mathbb{Z})$ und verwende den kleinen Satz von Fermat.

Aufgabe 2.1.27. Es sei $n \in \mathbb{Z}_{\geq 1}$ eine ganze Zahl, und es sei $n = p_1^{\nu_1} \cdots p_r^{\nu_r}$ mit paarweise verschiedenen Primzahlen $p_i \in \mathbb{Z}_{\geq 1}$. Zeige: Man hat einen Isomorphismus von Gruppen

$$\begin{array}{rcl} \kappa\colon \mathbb{Z}/n\mathbb{Z} & \to & \mathbb{Z}/p_1^{\nu_1}\mathbb{Z} \times \ldots \times \mathbb{Z}/p_r^{\nu_r}\mathbb{Z} \\ \overline{m} & \mapsto & (\overline{m},\ldots,\overline{m}) \end{array}$$

Aufgabe 2.1.28. Es seien $p_1,\ldots p_r \in \mathbb{Z}_{\geq 1}$ paarweise verschiedene Primzahlen, und es seien $\nu_1,\ldots,\nu_r \in \mathbb{Z}_{\geq 1}$ Zeige: Man hat einen kanonischen Isomorphismus von Automorphismengrupppen:

$$\begin{array}{rcl} \operatorname{Aut}(\mathbb{Z}/p_1^{\nu_1}\mathbb{Z}) \times \ldots \times \operatorname{Aut}(\mathbb{Z}/p_r^{\nu_r}\mathbb{Z}) & \to & \operatorname{Aut}(\mathbb{Z}/p_1^{\nu_1}\mathbb{Z} \times \ldots \times \mathbb{Z}/p_r^{\nu_r}\mathbb{Z}), \\ (\varphi_1,\ldots,\varphi_r) & \mapsto & \left[(\overline{k}_1,\ldots,\overline{k}_r) \mapsto (\varphi_1(\overline{k}_1),\ldots,\varphi_r(\overline{k}_r))\right]. \end{array}$$

2.2. **Gruppenoperationen.**

Definition 2.2.1. Es seien G eine Gruppe und X eine Menge. Eine *Operation*, auch *Wirkung* von G auf X ist eine Abbildung

$$\mu\colon G \times X \ \to \ X, \qquad (g,x) \ \mapsto \ \mu(g,x] \ =: \ g \cdot x,$$

sodas für alle $x \in X$ und $g_1, g_2 \in G$ gilt:

$$e_G \cdot x \ = \ x, \qquad g_2 \cdot (g_1 \cdot x) \ = \ (g_2 g_1) \cdot x.$$

Beispiel 2.2.2. Es sei $\mathbb{K}$ ein Körper, z.B. $\mathbb{K} = \mathbb{Q}, \mathbb{R}, \mathbb{C}$. Die *Skalarmultiplikation* liefert eine Operation der multiplikativen Gruppe $\mathbb{K}^*$ auf $\mathbb{K}^n$:

$$\mathbb{K}^* \times \mathbb{K}^n \ \to \ \mathbb{K}^n, \qquad (a,x) \ \mapsto \ a \cdot x \ := \ (ax_1, \ldots, ax_n).$$

Die *Matrix-Vektor-Multiplikation* liefert eine Operation der allgemeinen linearen Gruppe $\mathrm{GL}(n;\mathbb{K})$ auf $\mathbb{K}^n$:

$$\mathrm{GL}(n,\mathbb{K})\mathbb{K}^* \times \mathbb{K}^n \ \to \ \mathbb{K}^n, \qquad (A,x) \ \mapsto \ A \cdot x \ := \ \left(\sum a_{1j}x_j, \ldots, \sum a_{nj}x_j\right).$$

Beispiel 2.2.3. Es sei G eine Gruppe. Dann haben wir die folgenden Operationen $G \times G \to G$ von G auf sich selbst:

(i) Durch Multiplikation von links: $g \cdot h := gh$,
(ii) durch Multiplikation mit dem Inversen von rechts: $g \cdot h := hg^{-1}$,
(iii) durch Konjugation: $g \cdot h := ghg^{-1}$.

Beispiel 2.2.4. Es sei X eine Menge, und es sei $S(X)$ die Gruppe der bijektiven Selbstabbildungen von X. Zur Erinnerung: Die Verknüpfung ist gegeben durch

$$S(X) \times S(X) \ \to \ S(X), \qquad (\varphi, \psi) \ \mapsto \ \varphi \circ \psi,$$

das neutrale Element in $S(X)$ ist id_X, und das Inverse zu $\varphi \in S(X)$ ist die Umkehrabbildung φ^{-1}. Man hat eine kanonische Operation:

$$S(X) \times X \ \to X, \qquad \varphi \cdot x \ := \ \varphi(x).$$

Konstruktion 2.2.5. Die Gruppe G operiere auf der Menge X. Dann definiert jedes $g \in G$ eine Bijektion

$$T_g\colon X \ \to \ X, \qquad x \ \mapsto \ g \cdot x.$$

Dabei ist die zugehörige Umkehrabbildung gegeben durch

$$T_{g^{-1}}\colon X \ \to \ X, \qquad x \ \mapsto \ g^{-1} \cdot x.$$

Beweis. Die Behauptung ergibt sich direkt aus den Eigenschaften einer Gruppenoperation:

$$T_{g^{-1}}(T_g(x)) \ = \ g^{-1} \cdot (g \cdot x) \ = \ (g^{-1}g) \cdot x \ = \ e_G \cdot x \ = \ x,$$
$$T_g(T_{g^{-1}}(x)) \ = \ g \cdot (g^{-1} \cdot x) \ = \ (gg^{-1}) \cdot x \ = \ e_G \cdot x \ = \ x.$$

□

Satz 2.2.6. *Es seien G eine Gruppe und X eine Menge. Dann hat man zueinander inverse Bijektionen*

$$\begin{array}{rcl} \{G\text{-Operationen auf } X\} & \longleftrightarrow & \{\text{Homomorphismen } G \to S(X)\} \\ \mu & \mapsto & [g \mapsto T_g] \\ g \cdot x := \varrho(g)(x) & \leftarrow\!\shortmid & \varrho. \end{array}$$

Beweis. Wir zeigen zunächst, dass die Zuordnungen wohldefiniert sind. Wir beginnen mit einer Operation $\mu\colon G \times X \to X$ und zeigen, dass die zugehörige Abbildung

$$\varrho_\mu\colon G \ \to \ S(X), \qquad g \ \mapsto \ T_g$$

ein Homomorphismus ist. Dazu seien $g_1, g_2 \in G$ gegeben. Dann erhalten wir für jedes $x \in X$:

$$T_{g_2g_1}(x) \ = \ (g_2g_1) \cdot x \ = \ g_2 \cdot (g_1 \cdot x) \ = \ T_{g_2}(T_{g_1}(x)) \ = \ (T_{g_2} \circ T_{g_1})(x).$$

Folglich gilt $T_{g_2g_1} = T_{g_2} \circ T_{g_1}$. Das ist genau die Homomorphieeigenschaft für die Abbildung $\varrho_\mu\colon G \to S(X)$.

Es sei nun ein Homomorphismus $\varrho\colon G \to S(X)$ gegeben. Wir müssen zeigen, dass man dann eine G-Operation erhält durch

$$\mu_\varrho\colon G \times X \ \to \ X, \qquad (g,x) \ \mapsto \ g \cdot x := \varrho(g)(x).$$

Für den Nachweis der Eigenschaften einer Operation seien $g_1, g_2 \in G$ und $x \in X$ gegeben. Dann erhalten wir

$$e_G \cdot x \ = \ \varrho(e_G)(x) \ = \ \mathrm{id}_X(x) \ = \ x$$

und

$$g_2 \cdot (g_1 \cdot x) \ = \ \varrho(g_2)(\varrho(g_1)(x)) \ = \ (\varrho(g_2) \circ \varrho(g_1))(x) \ = \ \varrho(g_2g_1)(x) \ = \ (g_2g_1) \cdot x.$$

Damit ist die Wohldefiniertheit der Zuordnungen nachgewiesen. Wir müssen also nur noch zeigen, dass die Abbildungen invers zueinander sind, d.h., dass gilt

$$\mu_{\varrho_\mu} \ = \ \mu, \qquad \varrho_{\mu_\varrho} \ = \ \varrho.$$

Das geschieht wiederum durch einfaches Nachrechnen: Für jedes $g \in G$ und jedes $x \in X$ erhalten wir

$$\begin{aligned} \mu_{\varrho_\mu}(g,x) \ &= \ \varrho_\mu(g)(x) \ = \ T_g(x) \ = \ \mu(g,x), \\ \varrho_{\mu_\varrho}(g)(x) \ &= \ T_g(x) \ = \ \mu_\varrho(g,x) \ = \ \varrho(g)(x). \end{aligned}$$

□

Folgerung 2.2.7 (Satz von Cayley)**.** *Es sei $n \in \mathbb{Z}_{\geq 1}$. Dann ist jede Gruppe G der Ordnung n isomorph zu einer Untergruppe der Permutationsgruppe S_n.*

Beweis. Wir betrachten die Operation von G auf $X := G$ durch Linkstranslation. Der zugehörige Homomorphismus $\varrho\colon G \to S(X)$ ist injektiv:

$$\varrho(g) = \mathrm{id}_X \quad \Longrightarrow \quad gg' = g' \text{ für alle } g' \in G \quad \Longrightarrow \quad g = e_G.$$

Folglich ist G isomorph zu der Untergruppe $\varrho(G) \leq S(X)$. Die Behauptung folgt nun mit $S(X) \cong S_n$. □

Definition 2.2.8. Die Gruppe G operiere auf der Menge X.

(i) Die *Isotropiegruppe* eines Punktes $x \in X$ ist

$$G_x \ := \ \{g \in G;\ g \cdot x = x\} \ \leq \ G.$$

(ii) Die *Bahn* eines Punktes $x \in X$ ist

$$G \cdot x \ := \ \{g \cdot x;\ g \in G\} \ \subseteq \ X.$$

(iii) Der *Bahnenraum* ist die Menge aller G-Bahnen in X:

$$X/G \ := \ \{G \cdot x;\ x \in X\}.$$

Lemma 2.2.9. *Die Gruppe G operiere auf der Menge X.*

(i) *Für jedes $g \in G$ und jedes $x \in X$ gilt $G_{g \cdot x} = gG_xg^{-1}$.*
(ii) *Für jedes $x \in X$ hat man eine Bijektion $\beta_x\colon G/G_x \to G \cdot x$, $gG_x \mapsto g \cdot x$.*

(iii) *Für jedes* $x \in X$ *gilt* $|G \cdot x| = [G : G_x]$.

Beweis. Aussage (iii) folgt direkt aus (ii). Für den Nachweis von (i), seien $x \in X$ und $g \in G$ gegeben. Für jedes $h \in G$ erhält man

$$h \in G_{g\cdot x} \;\Leftrightarrow\; h \cdot (g \cdot x) = g \cdot x \;\Leftrightarrow\; g^{-1}hg \cdot x = x \;\Leftrightarrow\; g^{-1}hg \in G_x \;\Leftrightarrow\; h \in gG_xg^{-1}.$$

Zu (ii). Die Abbildung β_x ist offensichtlich wohldefiniert und surjektiv. Zur Injektivität: Gilt $\beta_x(gG_x) = \beta_x(hG_x)$, so folgt $h^{-1}g \in G_x$ und somit $gG_x = hG_x$. □

Satz 2.2.10. *Die Gruppe* G *operiere auf der Menge* X*. Dann hat man eine Äquivalenzrelation auf* X*:*

$$x_2 \sim_G x_1 \quad :\Longleftrightarrow \quad x_2 = g \cdot x_1 \text{ mit einem } g \in G.$$

Die zugehörigen Äquivalenzklassen sind genau die G*-Bahnen in* X*. Insbesondere erhält man eine disjunkte Zerlegung von* X *in* G*-Bahnen*

$$X = \bigsqcup_{G\cdot x \in X/G} G \cdot x = \bigsqcup_{i\in I} G \cdot x_i,$$

die Bahnzerlegung*, wobei* x_i*,* $i \in I$*, ein vollständiges Repräsentantensystem der Äquivalenzrelation "*$\sim_G$*" sei.*

Beweis. Die Relation "$\sim_G$" ist reflexiv, da stets $x = e_G \cdot x$ gilt. Weiter ist "$\sim_G$" symmetrisch, denn wir haben stets

$$x_2 = g \cdot x_1 \quad \Longleftrightarrow \quad x_1 = g^{-1} \cdot x_2.$$

Zum Nachweis der Transitivität, seien $x_1 \sim_G x_2$ und $x_2 \sim_G x_3$. Dann gibt es $g, h \in G$ mit $x_2 = h \cdot x_1$ und $x_3 = g \cdot x_2$. Es folgt $x_3 = (gh) \cdot x_1$ und somit $x_1 \sim_G x_3$.

Die Tatsache, dass die Äquivalenzklassen von "$\sim_G$" genau die G-Bahnen in X sind, ist offensichtlich, und mit ihr erhält man die disjunkte Zerlegung von X in G-Bahnen. □

Satz 2.2.11 (Bahnengleichung)**.** *Es sei* $G \times X \to X$ *eine Operation einer Gruppe* G *auf einer Menge* X*, und es sei* x_i*,* $i \in I$*, ein vollständiges Repräsentantensystem für "*$\sim_G$*". Dann gilt*

$$|X| = \sum_{i\in I} |G \cdot x_i| = \sum_{i\in I} [G : G_{x_i}].$$

Beweis. Nach Satz 2.2.10 ist X die disjunkte Vereinigung aller G-Bahnen in X, d.h., es gilt

$$X = \bigsqcup_{i\in I} G \cdot x_i.$$

Das beweist die erste Gleichung. Nach Bemerkung 2.2.9 (ii) gilt $|G \cdot x_i| = [G : G_{x_i}]$ für jedes $i \in I$. Das beweist die zweite Gleichung. □

Definition 2.2.12. Die Gruppe G operiere auf der Menge X. Ein Element $x \in X$ heißt *Fixpunkt* dieser Operation, falls $g \cdot x = x$ für jedes $g \in G$ gilt.

Satz 2.2.13 (Fixpunktsatz)**.** *Es sei* $G \times X \to X$ *eine Operation einer endlichen Gruppe auf einer endlichen Menge* X*. Gilt* $|G| = p^k$ *und* $p \nmid |X|$ *mit einer Primzahl* p*, so besitzt die* G*-Operation einen Fixpunkt.*

Beweis. Es sei $x_1, \ldots, x_r$ ein vollständiges Repräsentantensystem für den Bahnenraum X/G. Nach dem Satz von Lagrange gilt

$$[G : G_{x_i}] \;=\; p^{l_i}$$

mit ganzen Zahlen $l_i \leq k$. Mit der Bahnengleichung erhalten wir daher

$$|X| \;=\; \sum_{i=1}^{r} [G : G_{x_i}] \;=\; \sum_{i=1}^{r} p^{l_i}.$$

Da p nach Voraussetzung kein Teiler von $|X|$ ist, gibt es (mindestens) ein i mit $l_i = 0$. Das zugehörige x_i ist der gesuchte Fixpunkt der G-Operation. □

Definition 2.2.14. Es sei G eine Gruppe.

(i) Der *Zentralisator* eines Elements $g \in G$ ist die Untergruppe

$$Z_g \;:=\; \{a \in G;\; ag = ga\} \;\leq\; G.$$

(ii) Das *Zentrum* von G ist die (abelsche) Untergruppe

$$Z_G \;:=\; \bigcap_{g \in G} Z_g \;:=\; \{a \in G;\; ag = ga \text{ für alle } g \in G\} \;\leq\; G.$$

Satz 2.2.15 (Klassengleichung)**.** *Es sei G eine endliche Gruppe. Man betrachte die Operation durch Konjugation*

$$G \times G \;\to\; G, \qquad g \cdot h \;:=\; ghg^{-1}.$$

(i) *Für jedes $h \in G$ gilt*

$$G_h \;=\; Z_h, \qquad h \text{ ist Fixpunkt} \;\Leftrightarrow\; h \in Z_G.$$

(ii) *Gilt $G = G \cdot h_1 \sqcup \ldots \sqcup G \cdot h_r$ mit $h_i \in G$ so gilt*

$$|G| \;=\; |Z_G| + \sum_{[G:Z_{h_i}] \geq 2} [G : Z_{h_i}].$$

Beweis. Aussage (i) ist offensichtlich. Aussage (ii) ergibt sich mit (i) und der Bahnengleichung:

$$\begin{aligned}
|G| &= \sum_{i=1}^{r} |G \cdot h_i| \\
&= \sum_{|G \cdot h_i| = 1} |G \cdot h_i| + \sum_{|G \cdot h_i| \geq 2} |G \cdot h_i| \\
&= |Z_G| + \sum_{[G:G_{h_i}] \geq 2} [G : G_{h_i}] \\
&= |Z_G| + \sum_{[G:Z_{h_i}] \geq 2} [G : Z_{h_i}].
\end{aligned}$$

□

Bemerkung 2.2.16. Die Bahn $G \cdot h = \{ghg^{-1};\; g \in G\}$ von $h \in G$ unter der Operation aus 2.2.15 nenn man auch die *Konjugationsklasse* von $h \in G$. Die Klassengleichung stellt einen Zusammenhang zwischen der Ordnung von G, der Ordnung des Zentrums Z_G und den Ordnungen der nichttrivialen Konjugationsklassen von G her.

Aufgaben zu Abschnitt 2.2.

Aufgabe 2.2.17. Es seien G eine Gruppe und $H \leq G$ eine Untergruppe. Zeige: Man hat eine Operation

$$H \times G \;\to\; G, \qquad h \cdot g \;:=\; gh^{-1}.$$

Die Bahnen dieser Operation sind genau die Linksnebenklassen gH, $g \in G$. Zeige weiter: Der zugehörige Bahnenraum G/H besitzt eine Operation

$$G \times G/H \;\to\; G/H, \qquad g' \cdot (gH) \;:=\; (g'g)H.$$

Die Isotropiegruppe einer Nebenklasse gH ist dabei genau die zu H konjugierte Untergruppe gHg^{-1}.

Aufgabe 2.2.18. Es sei G eine Gruppe, und es sei $X := \{H \subseteq G;\ H \leq G\}$ die Menge aller Untergruppen von G. Zeige:

$$G \times X \;\to\; X, \qquad g \cdot H \;\mapsto\; gHg^{-1}$$

ist eine Operation der Gruppe G auf der Menge X. Zeige weiter:

(i) Ein Element $H \in X$ ist genau dann Normalteiler in G, wenn es Fixpunkt der obigen Operation ist.
(ii) Für jedes $H \in X$ ist die Isotropiegruppe G_H genau der *Normalisator* $N_G(H) := \{g \in G;\ gH = Hg\}$ von H in G.

Aufgabe 2.2.19. Bestimme den Bahnenraum der Operation

$$\mathrm{GL}(n, \mathbb{C}) \times \mathrm{Mat}(n, n; \mathbb{C}) \;\to\; \mathrm{Mat}(n, n; \mathbb{C}), \qquad S \cdot A \;:=\; SAS^{-1}.$$

Aufgabe 2.2.20. Eine Operation $G \times X \to X$ heißt *frei*, falls jede Isotropiegruppe G_x, wobei $x \in X$, trivial ist. Zeige: Operiert eine Gruppe G frei auf einer endlichen Menge X, so ist G endlich und $|X|$ ist ein Vielfaches von $|G|$.

Aufgabe 2.2.21. Eine Operation $G \times X \to X$ heißt *transitiv*, falls es zu je zwei $x_1, x_2 \in X$ ein $g \in G$ gibt mit $x_2 = g \cdot x_1$. Zeige: Operiert eine endliche Gruppe G transitiv auf einer Menge X, so ist X endlich und $|G|$ ist ein Vielfaches von $|X|$.

Aufgabe 2.2.22. Gib einen Isomorphismus von $\mathbb{Z}/n\mathbb{Z}$ auf eine Untergruppe der Permutationsgruppe S_n an.

Aufgabe 2.2.23. Gib einen Isomorphismus von $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ auf eine Untergruppe der Permutationsgruppe S_4 an.

Aufgabe 2.2.24. Es seien G eine Gruppe, X eine Menge und $\mu\colon G \times X \to X$ eine Operation von G auf X. Der *Stabilisator* einer Teilmenge $Y \subseteq X$ ist

$$G_Y \;:=\; \{g \in G;\ g \cdot Y = Y\} \;\subseteq\; G.$$

Zeige, dass G_Y eine Untergruppe von G ist, und dass $g \cdot y := \mu(g, y)$ eine Operation von G auf Y definiert.

Aufgabe 2.2.25. Es sei $\langle\ ,\ \rangle$ das Standardskalarprodukt auf $\mathbb{R}^n$. Dann ist die Einheitssphäre in $\mathbb{R}^n$ gegeben durch

$$S^{n-1} \;:=\; \{v \in \mathbb{R}^n;\ \langle v, v\rangle = 1\}$$

Betrachte die Operation von $\mathrm{GL}(n, \mathbb{R})$ auf $\mathbb{R}^n$ und zeige, dass die Gruppe $O(n)$ der orthogonalen $(n \times n)$-Matrizen der Stabilisator der Einheitssphäre S^{n-1} ist. Betrachte weiter die Menge der Eckpunkte eines regelmäßigen n-Ecks in $\mathbb{R}^2$:

$$\begin{aligned} Y \;&=\; \left\{(1,0),\ \left(\cos\left(\tfrac{2\pi}{n}\right), \sin\left(\tfrac{2\pi}{n}\right)\right),\ \ldots,\ \left(\cos\left(\tfrac{2\pi(n-1)}{n}\right), \sin\left(\tfrac{2\pi(n-1)}{n}\right)\right)\right\} \\ &\subseteq\; S^1 \end{aligned}$$

und zeige, dass der Stabilisator der Teilmenge $Y \subseteq S^1$ unter der Operation von $O(2)$ auf S^1 gegeben ist durch

$$O(2)_Y \;=\; \{\Delta_n^0, \ldots, \Delta_n^{n-1}\} \;\cup\; \{\Delta_n^0 \cdot \Sigma, \ldots, \Delta_n^{n-1} \cdot \Sigma\}.$$

wobei die Matrix Δ_n die Drehung um den Winkel $2\pi/n$ darstellt und Σ die Spiegelung an der x_1-Achse. d.h., wir haben

$$\Delta_n^k \;=\; \begin{pmatrix} \cos\left(\frac{2\pi k}{n}\right) & -\sin\left(\frac{2\pi k}{n}\right) \\ \sin\left(\frac{2\pi k}{n}\right) & \cos\left(\frac{2\pi k}{n}\right) \end{pmatrix}, \qquad \Sigma \;=\; \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Erinnerung: Eine reelle $(n \times n)$-Matrix heißt *orthogonal*, falls sie invertierbar ist und $A^{-1} = A^t$ gilt. Folgende Aussagen sind äquivalent:

(i) A ist orthogonal.
(ii) $T_A\colon \mathbb{R}^n \to \mathbb{R}^n$ ist eine *Isometrie*, d.h., man hat stets $\langle A \cdot v, A \cdot w\rangle = \langle v, w\rangle$.
(iii) Die Spalten von A bilden eine Orthonormalbasis für $\mathbb{R}^n$.
(iv) Die Zeilen von A bilden eine Orthonormalbasis für $\mathbb{R}^n$.

Aufgabe 2.2.26. Es seien G eine Gruppe und $Z_G \leq G$ ihr Zentrum. Zeige:

(i) Z_G ist ein Normalteiler in G.
(ii) Ist G/Z_G zyklisch, so ist G abelsch.

Aufgabe 2.2.27. Es sei G eine Gruppe. Ein *innerer Automorphismus von* G ist eine Abbildung der Form

$$\kappa_a\colon G \;\to\; G, \quad g \;\mapsto\; aga^{-1}, \qquad \text{wobei } a \in G.$$

Zeige: Die inneren Automorphismen von G bilden eine Untergruppe $\mathrm{Aut}_{\mathrm{inner}}(G) \leq \mathrm{Aut}(G)$. Zeige weiter, dass $\mathrm{Aut}_{\mathrm{inner}}(G) \cong G/Z_G$ gilt.

2.3. **Das Theorem von Sylow.**

Definition 2.3.1. Es seien G eine endliche Gruppe und p eine Primzahl.

(i) Eine *p-Untergruppe* von G ist eine Untergruppe $H \leq G$ mit $|H| = p^k$ für ein $k \in \mathbb{Z}_{\geq 0}$.
(ii) Eine *p-Sylow-Gruppe* in G ist eine p-Untergruppe $H \leq G$, sodass p kein Teiler von $[G : H]$ ist.

Beispiel 2.3.2. Wir betrachten die Gruppe $G := \mathbb{Z}/12\mathbb{Z}$. Es gilt $|G| = 12 = 2^2 \cdot 3$ und wir erhalten Untergruppen von G durch

$$H_2 \ := \ \{\bar{0}, \bar{6}\}, \qquad H_4 \ := \ \{\bar{0}, \bar{3}, \bar{6}, \bar{9}\}, \qquad H_3 \ := \ \{\bar{0}, \bar{4}, \bar{8}\}.$$

Nach Satz 2.1.10 sind H_2, H_4 und H_3 die einzigen nicht-trivialen p-Untergruppen von G. Dabei sind H_4 und H_3 jeweils p-Sylow-Gruppen in G.

Bemerkung 2.3.3. Ist G eine zyklische Gruppe der Ordnung $n = p_1^{\nu_1} \cdots p_r^{\nu_r}$ mit paarweise verschiedenen Primzahlen $p_i \in \mathbb{Z}_{\geq 1}$, so gibt es zu jedem p_i genau eine p_i-Sylow-Gruppe in G. Diese ist gegeben durch $H_i := \langle \overline{m}_i \rangle$ mit $m_i := n/p_i^{\nu_i}$ und ist isomorph zu $\mathbb{Z}/p_i^{\nu_i}\mathbb{Z}$; siehe Satz 2.1.10.

Beispiel 2.3.4. Für die symmetrische Gruppe S_3 haben wir $|S_3| = 6 = 2 \cdot 3$. Die nicht-trivialen p-Sylow-Gruppen in S_3 sind gegeben durch

$$\begin{aligned} p = 2\colon &\quad \langle (1,2) \rangle, \qquad \langle (1,3) \rangle, \qquad \langle (2,3) \rangle, \\ p = 3\colon &\quad \langle (1,2,3) \rangle. \end{aligned}$$

Man beachte dabei, dass die 2-Sylow-Gruppen jeweils konjugiert zueinander sind; konkret gilt

$$\langle (1,3) \rangle \ = \ (2,3)\langle (1,2) \rangle (2,3)^{-1}, \qquad \langle (2,3) \rangle \ = \ (1,3)\langle (1,2) \rangle (1,3)^{-1}.$$

Satz 2.3.5. *Es seien G eine endliche Gruppe und $|G| = p_1^{\nu_1} \cdots p_r^{\nu_r}$ mit mit paarweise verschiedenen Primzahlen $p_i \in \mathbb{Z}_{\geq 1}$.*

(i) *Die p_i-Sylow-Gruppen in G sind genau die Untergruppen $H \leq G$ der Ordnung $|H| = p_i^{\nu_i}$.*
(ii) *Ist $H \leq G$ eine p-Sylow-Gruppe, so ist auch jede dazu konjugierte Untergruppe gHg^{-1}, wobei $g \in G$, eine p-Sylow-Gruppe in G.*

Beweis. Aussage (i) ist klar. Für Aussage (ii) ist nur zu zeigen, dass gHg^{-1} eine Untergruppe ist. Wir haben offensichtlich $e_G = ge_Gg^{-1} \in gHg^{-1}$. Weiter gilt

$$\begin{aligned} gh_1g^{-1}, gh_2g^{-1} \in gHg^{-1} \quad &\Longrightarrow \quad gh_1g^{-1}gh_2g^{-1} = gh_1h_2g^{-1} \in gHg^{-1} \\ ghg^{-1} \in gHg^{-1} \quad &\Longrightarrow \quad (ghg^{-1})^{-1} = gh^{-1}g^{-1} \in gHg^{-1}. \end{aligned}$$

□

Theorem 2.3.6 (Sylow)**.** *Es seien G eine endliche Gruppe, $n := |G|$ und $p \in \mathbb{Z}_{\geq 1}$ eine Primzahl.*

(i) *Jede p-Untergruppe von G ist in einer p-Sylowgruppe von G enthalten.*
(ii) *Je zwei p-Sylow-Gruppen in G sind konjugiert zueinander.*
(iii) *Für die Anzahl s der p-Sylow-Gruppen in G gilt*

$$s \neq 0, \qquad s \mid n, \qquad s \equiv 1 \mod p.$$

Beispiel 2.3.7. Für die (bereits ermittelte) Anzahl s der nicht-trivialen p-Sylow-Gruppen in S_3 liefert Aussage (iii) von Theorem 2.3.6 folgende Bedingungen:

$$\begin{aligned} p = 2\colon &\quad s \mid 6, \qquad s \in \{1, 3, 5, \ldots, \}, \\ p = 3\colon &\quad s \mid 6, \qquad s \in \{1, 4, 7, \ldots, \}. \end{aligned}$$

Für $p = 2$ kommen a priori $s = 1$ und $s = 3$ in Frage. Wie bereits gesehen, gilt hier $s = 3$. Für $p = 3$ ist nur $s = 1$ möglich.

Beispiel 2.3.8. Wir betrachten die Diedergruppe $D_5 = \langle \delta, \sigma \rangle$; siehe 1.2.9. Es gilt $|D_5| = 10 = 2 \cdot 5$. Die Anzahlen s der nicht-trivialen p-Sylow-Gruppen erfüllen

$$\begin{aligned} p = 2\colon &\quad s \mid 10, \qquad s \in \{1, 3, 5, \ldots, \}, \\ p = 5\colon &\quad s \mid 10, \qquad s \in \{1, 6, 11, \ldots, \} \end{aligned}$$

gemäß Theorem 2.3.6 (iii): Wir erhalten tatsächlich eine 5-Sylowgruppe und fünf 2-Sylowgruppen in D_5. Diese sind konkret gegeben durch

$$\langle \delta \rangle \le D_5, \qquad \langle \delta^k \sigma \delta^{-k} \rangle \le D_5, \quad k = 1, \ldots, 5.$$

Unser Beweis des Sylowschen Theorems geht auf Helmut Wielandt zurück [8]. Der Schlüssel zum Erfolg liegt in der genauen Untersuchung der folgenden Gruppenoperationen.

Konstruktion 2.3.9. Es seien G eine endliche Gruppe und $|G| = p^k m$ mit einer Primzahl p und $k \in \mathbb{Z}_{\ge 0}$; der Fall $p|m$ ist dabei erlaubt. Wir betrachten die Menge aller p^k-elementigen Teilmengen von G:

$$X \;:=\; \{U \subseteq G;\ |U| = p^k\} \;\subseteq\; \mathrm{Pot}(G).$$

Man beachte, dass insbesondere jede Untergruppe $H \le G$ der Ordnung p^k ein Element der Menge X ist. Die Gruppe G operiert auf natürliche Weise auf X:

$$G \times X \;\to\; X, \qquad (g, U) \;\mapsto\; g * U := gU = \{gu;\ u \in U\}.$$

Für $U \in X$ bezeichne $G_U \le G$ wie üblich die zugehörige Isotropiegruppe. Dann haben wir für jedes $U \in X$ eine Operation

$$G_U \times U \;\to\; U, \qquad (g, u) \;\mapsto\; gu.$$

Lemma 2.3.10. *Wir betrachten die Operation $G \times X \to X$ aus 2.3.9 und den zugehörigen Bahnenraum X/G. Dann hat man eine injektive Abbildung*

$$\{H \le G;\ |H| = p^k\} \;\to\; X/G, \qquad H \;\mapsto\; G * H.$$

Beweis. Es ist klar, dass die Zuordnung $H \mapsto G * H$ wohldefiniert ist. Wir müssen uns also nur um die Injektivität kümmern.

Dazu betrachten wir zwei Untergruppen $H, H' \le G$ der Ordnung p^k, die dieselbe G-Bahn in X definieren. Das bedeutet

$$\{gH;\ g \in G\} \;=\; G * H \;=\; G * H' \;=\; \{gH';\ g \in G\}.$$

Insbesondere gibt es dann ein $g \in G$ mit $gH' = H$. Folglich gibt es ein $h' \in H'$ mit $gh' = e$. Das impliziert $g \in H'$ und somit $H' = H$. □

Lemma 2.3.11. *Wir betrachten die Operation $G \times X \to X$ aus 2.3.9. Für jedes $U \in X$ gibt es ein $l \le k$, sodass für die Isotropiegruppe $G_U \le G$ gilt:*

$$|G_U| \;=\; p^l, \qquad\qquad [G : G_U] \;=\; p^{k-l} m.$$

Beweis. Wir betrachten die Bahnzerlegung $U = G_U u_1 \sqcup \ldots \sqcup G_U u_r$. Mit Lemma 1.2.11 erhalten wir

$$p^k \;=\; |U| \;=\; \sum_{i=1}^{r} |G_U u_i| \;=\; r|G_U|.$$

Also gilt $|G_U| = p^l$ mit einem $l \leq k$. Die zweite Gleichung erhält man aus der ersten mit Hilfe des Satzes von Lagrange 1.2.14. □

Lemma 2.3.12. *Wir betrachten die Operation $G \times X \to X$ aus 2.3.9. Für jedes Element $U \in X$ sind folgende Aussagen äquivalent:*

(i) $|G_U| = p^k$
(ii) *$G * U$ enthält eine Untergruppe $H \leq G$ der Ordnung p^k.*

Beweis. Zur Implikation "(i)⇒(ii)". Wir betrachten ein beliebiges Element $u \in U$. Dann haben wir

$$G_U u \;=\; \{gu;\; g \in G_U\} \;\subseteq\; \bigcup_{g \in G_U} g * U \;=\; U.$$

Mit Lemma 1.2.11 erhalten wir weiter

$$|G_U u| \;=\; |G_U| \;=\; p^k \;=\; |U|.$$

Somit ergibt sich $G_U u = U$. Die Untergruppe $H := u^{-1} G_U u$ besitzt die Ordnung p^k und wir haben

$$H \;=\; u^{-1} * G_U u \;=\; u^{-1} * U \;\in\; G * U.$$

Zur Implikation "(ii)⇒(i)". Wir wählen ein $g \in G$ mit $H = g * U$. Für die Isotropiegruppen haben wir

$$G_H \;=\; g G_U g^{-1},$$

siehe Lemma 2.2.9. Es folgt

$$|G_U| \;=\; |g G_U g^{-1}| \;=\; |G_H| \;=\; |\{g \in G;\; gH = H\}| \;=\; |H| \;=\; p^k.$$

□

Lemma 2.3.13. *Es sei G eine Gruppe der Ordnung $n = p^k m$ mit einer Primzahl p und $m \in \mathbb{Z}_{\geq 1}$. Dann ist die Anzahl der Untergruppen $H \leq G$ der Ordnung p^k gegeben durch*

$$|\{H \leq G;\; |H| = p^k\}| \;\equiv\; \binom{n-1}{p^k - 1} \mod p.$$

Beweis. Wir betrachten die Bahnzerlegung $X = G * U_1 \sqcup \ldots \sqcup G * U_r$. Nach Lemma 2.3.11 gibt es Zahlen $l_i \leq k$ mit

$$|G_{U_i}| \;=\; p^{l_i}.$$

Durch geeignete Nummerierung $i = 1, \ldots, s, s+1, \ldots, r$ erreichen wir, dass $l_i = k$ für $i = 1, \ldots, s$ und $l_i < k$ für $i = s+1, \ldots, r$ gelten.

Lemma 2.3.12 besagt, dass $G * U_1, \ldots, G * U_s$ genau die Bahnen sind, die eine Untergruppe $H_i \leq G$ der Ordnung p^k enthalten. Nach Lemma 2.3.10 ist H_i dabei die einzige Untergruppe in $G * U_i$. Folglich ist s gerade die Anzahl der p^k-elementigen Untergruppen von G. Mit der Bahnengleichung erhalten wir

$$\binom{n}{p^k} \;=\; |X| \;=\; \sum_{i=1}^{r} |G * U_i| \;=\; \sum_{i=1}^{r} [G : G_{U_i}] \;=\; m \sum_{i=1}^{r} p^{k-l_i} \;=\; ms + \sum_{i=s+1}^{r} m p^{k-l_i}.$$

Rechnen wir modulo p, so ergibt sich daraus

$$s \quad \equiv \quad \frac{1}{m}\binom{n}{p^k} \mod p.$$

Die Behauptung erhält man nun durch eine einfache Umrechung der Binomialkoeffizienten:

$$\binom{n}{p^k} \;=\; \frac{n!}{(n-p^k)!p^k!} \;=\; \frac{n}{p^k}\frac{(n-1)!}{(n-p^k)!(p^k-1)!} \;=\; m\binom{n-1}{p^k-1}.$$

□

Lemma 2.3.14. *Es seien p eine Primzahl, $k, m \in \mathbb{Z}_{>0}$ und $n := mp^k$. Dann gilt*

$$\binom{n-1}{p^k-1} \quad \equiv \quad 1 \mod p.$$

Beweis. Wir betrachten $G := \mathbb{Z}/n\mathbb{Z}$. Nach Satz 2.1.10 gibt es genau eine Untergruppe $H \leq G$ der Ordnung p^k. Die Behauptung folgt somit aus Lemma 2.3.13. □

Lemma 2.3.15. *Es seien G eine Gruppe, $H \leq G$ eine p-Untergruppe und $H' \leq G$ eine p-Sylow-Gruppe. Dann gibt es ein $g \in G$ mit $H \subseteq gH'g^{-1}$.*

Beweis. Wir betrachten die kanonische Operation der Gruppe H auf dem homogenen Raum G/H':

$$H \times G/H' \;\to\; G/H', \qquad h \cdot gH' \;:=\; hgH'.$$

Es gilt $|H| = p^l$ mit einem $l \in \mathbb{Z}_{\geq 0}$ und $p \nmid |G/H'|$. Nach Satz 2.2.13 besitzt diese Operation einen Fixpunkt. Wir haben also $HgH' = gH'$ für ein $g \in G$. Es folgt $Hg \subseteq gH'$ und somit $H \subseteq gH'g^{-1}$. □

Beweis von Theorem 2.3.6. Der zweite Teil von Aussage (iii) ist mit Lemmata 2.3.13 und 2.3.14 bereits bewiesen. Insbesondere sehen wir, dass $s \neq 0$ gilt, d.h., es existieren p-Sylow-Gruppen in G.

Wir zeigen Aussage (i). Es seien $H \leq G$ eine p-Untergruppe und $H' \leq G$ eine p-Sylowgruppe. Nach Lemma 2.3.15 gilt $H \subseteq gH'g^{-1}$ mit einem $g \in G$. Nach Satz 2.3.5 ist $gH'g^{-1}$ eine p-Sylow-Gruppe in G.

Für den Beweis von Aussage (ii) betrachten wir zwei p-Sylow-Gruppen $H, H' \leq G$. Nach Lemma 2.3.15 gilt $H \subseteq gH'g^{-1}$ mit einem $g \in G$. Da beide Gruppen dieselbe Ordnung haben, folgt $H = gH'g^{-1}$.

Für Aussage (iii) bleibt noch zu zeigen, dass die Anzahl s aller p-Sylow-Gruppen in G ein Teiler von $|G|$ ist. Dazu betrachten wir die Menge S aller p-Sylow-Gruppen in G und die Operation

$$G \times S \;\to\; S, \qquad (g, H) \;\mapsto\; g \cdot H := gHg^{-1}$$

Nach (ii) sind je zwei p-Sylow-Gruppen konjugiert zueinander. Somit besteht S aus einer einzigen G-Bahn. Die Bahnengleichung liefert

$$s \;=\; |S| \;=\; |G \cdot H| \;=\; [G : G_H]$$

für jede p-Sylow-Gruppe $H \leq G$. Nach dem Satz von Lagrange ist $[G : G_H]$ ein Teiler der Gruppenordnung $n = |G|$. □

Satz 2.3.16. *Es seien G eine endliche Gruppe, p eine Primzahl und $k \in \mathbb{Z}_{\geq 0}$. Ist p^k ein Teiler von $|G|$, so besitzt G eine Untergruppe $H \leq G$ mit $|H| = p^k$.*

Beweis. Die Behauptung folgt sofort aus Lemma 2.3.13 und Lemma 2.3.14. □

Aufgaben zu Abschnitt 2.3.

Aufgabe 2.3.17. Bestimme alle Sylow-Gruppen der symmetrischen Gruppe S_6, der Diedergruppe D_9 und der alternierenden Gruppe A_4.

Aufgabe 2.3.18. Zeige: Die Diedergruppe D_4 besitzt eine Untergruppe $H \cong \mathbb{Z}/4\mathbb{Z}$ und eine Untergruppe $H' \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Insbesondere sind nicht je zwei 2-Untergruppen der Ordnung vier in D_4 konjugiert zueinander.

Aufgabe 2.3.19. Es sei $\varphi\colon G \to G'$ ein Homomorphismus endlicher Gruppen. Beweise folgende Aussagen:

(i) Ist $H' \leq G'$ eine p-Sylowgruppe, so ist auch das Urbild $\varphi^{-1}(H') \leq G$ eine p-Sylowgruppe.
(ii) Ist $\varphi\colon G \to G'$ surjektiv und ist $H \leq G$ eine p-Sylowgruppe, so ist auch das Bild $\varphi(H) \leq G'$ eine p-Sylowgruppe.

Aufgabe 2.3.20 (Satz von Cauchy)**.** Es seien G eine endliche Gruppe und p eine Primzahl. Zeige: Ist p ein Teiler von G, so gibt es ein Element der Ordnung p in G.

Aufgabe 2.3.21. Es seien G eine endliche Gruppe und $p \in \mathbb{Z}_{\geq 1}$ eine Primzahl. Beweise die Äquivalenz folgender Aussagen:

(i) Für jedes $g \in G$ ist $\mathrm{ord}(g)$ eine Potenz von p.
(ii) Es gilt $|G| = p^k$ mit einem $k \in \mathbb{Z}_{\geq 0}$.

Aufgabe 2.3.22. Es seien $p, q \in \mathbb{Z}_{\geq 1}$ Primzahlen mit $p < q$ und $p \nmid q - 1$. Weiter sei G eine Gruppe der Ordnung pq. Zeige:

(i) Es gibt genau eine q-Sylow-Gruppe $H_q \subseteq G$ und diese ist ein Normalteiler in G.
(ii) Es gibt genau eine p-Sylow-Gruppe $H_p \subseteq G$ und diese ist ein Normalteiler in G.
(iii) Es gilt $H_p \cap H_q = \{e_G\}$ und man hat Isomorphismen

$$G \;\cong\; G/H_q \times G/H_p \;\cong\; \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \;\cong\; \mathbb{Z}/pq\mathbb{Z}.$$

Aufgabe 2.3.23. Es sei $q \in \mathbb{Z}_{\geq 3}$ eine Primzahl. Zeige: Eine Gruppe G der Ordnung $2q$ ist entweder zyklisch oder isomorph zur Diedergruppe D_q. *Hinweise:*

- Zeige, dass es genau eine q-Sylowgruppe $H_q \subseteq G$ gibt, und dass für die Anzahl s_2 der 2-Sylowgruppen in G gilt: $s_2 = 1$ oder $s_2 = q$. Zeige wie in Aufgabe 2.3.22, dass G im Falle $s_2 = 1$ zyklisch ist.
- Im Fall $s_2 = q$ beachte, dass $G = \langle \alpha, \beta \rangle$ gilt, wobei α ein Erzeuger von H_q ist und $\beta \in G$ ein Element mit $G = H_q \sqcup \beta H_q$ ist. Zeige, dass β sowie $\beta\alpha$ die Ordnung 2 besitzen und dass es einen Isomorphismus $G \to D_q$ gibt mit $\alpha \mapsto \delta$ und $\beta \mapsto \sigma$.

Aufgabe 2.3.24. Bestimme, bis auf Isomorphie, alle Gruppen der Ordnungen 1, 2, 3, 4, 5, 6, 7, 10, 11, 13, 14 und 15.

Aufgabe 2.3.25. Es sei G eine abelsche Gruppe. Weiter sei $|G| = p_1^{\nu_1} \cdots p_r^{\nu_r}$ mit paarweise verschiedenen Primzahlen $p_1, \ldots, p_r$ und $G_i \subseteq G$ bezeichne die Menge aller Elemente $g \in G$, deren Ordnung eine Potenz von p_i ist. Zeige:

(i) G_i ist eine Untergruppe von G.
(ii) G_i ist die einzige p_i-Sylowgruppe von G.
(iii) Es gilt $G \cong G_1 \times \ldots \times G_r$.

Aufgabe 2.3.26. Es seien G eine endliche Gruppe, $H \subseteq G$ eine p-Sylow-Gruppe in G und $N_G(H) = \{g \in G;\ gHg^{-1} = H\}$ der Normalisator von H in G. Zeige, dass die Anzahl der p-Sylow-Gruppen in G durch $[G : N_G(H)]$ gegeben ist.

2.4. **Auflösbare Gruppen.**

Definition 2.4.1. Es sei G eine Gruppe. Eine *Normalreihe in* G ist eine absteigende Kette von Untergruppen

$$G = G_0 \trianglerighteq G_1 \trianglerighteq \ldots \trianglerighteq G_n = \{e_G\},$$

wobei, wie angedeutet, G_{i+1} Normalteiler in G_i ist. Der *i-te Faktor* einer solchen Normalreihe ist G_{i-1}/G_i.

Definition 2.4.2. Eine Gruppe G heißt *auflösbar*, wenn sie eine Normalreihe besitzt, deren Faktoren alle abelsch sind.

Bemerkung 2.4.3. Jede abelsche Gruppe G ist auflösbar mit der Normalreihe $G = G_0 \trianglerighteq G_1 = \{e_G\}$.

Beispiel 2.4.4. Die symmetrische Gruppe S_3 ist auflösbar: Eine geeignete Normalreihe ist

$$S_3 = G_0 \trianglerighteq G_1 = \langle (1,2,3) \rangle \trianglerighteq G_2 = \{\mathrm{id}\}.$$

Beispiel 2.4.5. Die Gruppe $B(2,\mathbb{R}) \subset \mathrm{GL}(2,\mathbb{R})$ der oberen Dreiecksmatrizen ist auflösbar. Man erhält eine Normalreihe $B(2,\mathbb{R}) \trianglerighteq U(2,\mathbb{R}) \trianglerighteq \{E_2\}$ mit

$$U(2,\mathbb{R}) \;=\; [B(2,\mathbb{R}), B(2,\mathbb{R})] \;=\; \{A \in B(2,\mathbb{R});\; a_{11} = a_{22} = 1\}.$$

Konstruktion 2.4.6. Es sei G eine Gruppe. Wir betrachten die *iterierten Kommutatorgruppen* von G:

$$\begin{aligned} D^0G &:= G, \\ D^1G &:= [D^0G, D^0G] = [G,G], \\ &\vdots \\ D^{i+1}G &:= [D^iG, D^iG] \\ &\vdots \end{aligned}$$

Nach Bemerkung 1.4.6 ist die Kommutatorgruppe einer Gruppe Normalteiler. Folglich erhalten wir

$$G = D^0G \trianglerighteq D^1G \trianglerighteq D^2G \trianglerighteq \ldots$$

Weiter ist gemäß Satz 1.4.7 jede der Faktorgruppen $D^{i-1}G/D^iG$ eine abelsche Gruppe.

Satz 2.4.7. *Eine Gruppe G ist genau dann auflösbar, wenn es ein $n \in \mathbb{Z}_{\geq 0}$ gibt mit $D^nG = \{e_G\}$.*

Beweis. Wenn $D^nG = \{e_G\}$ für ein $n \in \mathbb{Z}_{\geq 0}$ gilt, so liefert Konstruktion 2.4.6 eine Normalreihe für G. Es sei nun G eine auflösbare Gruppe. Dann wählen wir eine Normalreihe

$$G = G_0 \trianglerighteq G_1 \trianglerighteq \ldots \trianglerighteq G_n = \{e_G\}.$$

Wir betrachten den kanonischen Epimorphismus $\pi_0 \colon G_0 \to G_0/G_1$. Da G_0/G_1 abelsch ist, erhalten wir

$$D^1G \;=\; [G,G] \;\subseteq\; \mathrm{Kern}(\pi_0) \;=\; G_1.$$

Weiter betrachten wir den kanonischen Epimorphismus $\pi_1 \colon G_1 \to G_1/G_2$. Da G_1/G_2 abelsch ist, ergibt sich

$$D^2G \;=\; [D^1G, D^1G] \;\subseteq\; [G_1, G_1] \;\subseteq\; \mathrm{Kern}(\pi_1) \;=\; G_2.$$

So verfahren wir weiter und erhalten schließlich $D^nG \subseteq G_n = \{e_G\}$. □

Satz 2.4.8. *Es sei G eine endliche Gruppe. Gilt $|G| = p^k$ mit einer Primzahl p und $k \in \mathbb{Z}_{\geq 0}$, so ist G auflösbar.*

Lemma 2.4.9. *Es seien G eine Gruppe und $|G| = p^k$ mit einer Primzahl p und $k \in \mathbb{Z}_{\geq 1}$. Dann gilt $|Z_G| = p^l$ mit $l \in \mathbb{Z}_{\geq 1}$. Insbesondere ist das Zentrum $Z_G \leq G$ nicht trivial.*

Beweis. Für jedes $g \in G \setminus Z_G$ gilt $[G : Z_g] = p^{m(g)}$ mit einem $m(g) \in \mathbb{Z}_{\geq 1}$. Somit liefert die Klassengleichung

$$p^k \;=\; |G| \;=\; |Z_G| + \sum_{i=1}^{r} [G : Z_{g_i}] \;=\; |Z_G| + ps$$

mit einem $s \in \mathbb{Z}_{\geq 0}$. Folglich muss die Ordnung des Zentrums Z_G ein Vielfaches von p sein. Damit folgt die Behauptung. □

Beweis von Satz 2.4.8. Wir beweisen den Satz durch Induktion über k. In den Fällen $k = 0, 1$ ist die Aussage offensichtlich richtig.

Zum Induktionsschritt. Nach Lemma 2.4.9 gilt $1 < |Z_G| = p^l$ mit einem $l \leq k$. Wir betrachten die Faktorgruppe $G' := G/Z_G$. Nach Induktionsvoraussetzung ist G' auflösbar. Es gibt also eine Normalreihe

$$G' = G'_0 \;\trianglerighteq\; G'_1 \;\trianglerighteq\; \ldots \;\trianglerighteq\; G'_n = \{e_{G'}\}$$

mit ausschließlich abelschen Faktoren G'_{i-1}/G'_i. Bezeichnet $\pi\colon G \to G'$ den kanonischen Epimorphismus, so erhalten wir Untergruppen $G_i := \pi^{-1}(G'_i) \leq G$. Dabei ist G_{i+1} stets Normalteiler in G_i, und wir erhalten eine Normalreihe

$$G = G_0 \;\trianglerighteq\; G_1 \;\trianglerighteq\; \ldots \;\trianglerighteq\; G_n = Z_G \;\trianglerighteq\; G_{n+1} = \{e_G\}.$$

Es bleibt zu zeigen, dass sämtliche Faktoren dieser Normalreihe abelsch sind. Für $G_n/G_{n+1} \cong Z_G$ ist das klar. Für die verbleibenden Faktoren verschaffen wir uns mit Hilfe des Homomorphiesatzes 1.3.17 jeweils ein kommutatives Diagramm

$$\begin{array}{ccc} G_i & \xrightarrow{\kappa} & G_{i-1}/G_i \\ {\scriptstyle\pi}\downarrow & & \downarrow{\scriptstyle\varphi} \\ G'_i & \xrightarrow[\lambda]{} & G'_{i-1}/G'_i \end{array}$$

mit den kanonischen Epimorphismen κ, λ und einem noch zu gewinnenden Homomorphismus φ. Dafür vermerken wir

$$\operatorname{Kern}(\lambda \circ \pi) \;=\; \pi^{-1}(\lambda^{-1}(e)) \;=\; \pi^{-1}(G'_i) \;=\; G_i \;=\; \operatorname{Kern}(\kappa).$$

Somit greift der Homomorphiesatz und liefert Existenz und Injektivität von φ. Weiter ist φ ist surjektiv, da dies für $\lambda \circ \pi$ gilt. Folglich ist φ ein Isomorphismus. Insbesondere ist $G_{i-1}/G_i \cong G'_{i-1}/G'_i$ abelsch. □

Theorem 2.4.10 (Feit, Thompson)**.** *Jede endliche Gruppe ungerader Ordnung ist auflösbar.*

Bemerkung 2.4.11. Wir betrachten die alternierende Gruppe A_4. Die *Kleinsche Vierergruppe* ist die Untergruppe

$$V_4 \;:=\; \{\mathrm{id},\, (1,2)(3,4),\, (1,3)(2,4),\, (1,4)(2,3)\} \;\leq\; A_4.$$

Die Kleinsche Vierergruppe ist ein Normalteiler in A_4 und man hat einen Isomorphismus

$$\begin{array}{rcl} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & \to & V_4, \\ (\overline{0},\overline{0}) & \mapsto & \mathrm{id}, \\ (\overline{1},\overline{0}) & \mapsto & (1,2)(3,4), \\ (\overline{0},\overline{1}) & \mapsto & (1,3)(2,4), \\ (\overline{1},\overline{1}) & \mapsto & (1,4)(2,3). \end{array}$$

Satz 2.4.12. *Es sei $n \in \mathbb{Z}_{\geq 1}$. Dann gilt*

$$\begin{array}{rcll} [S_n, S_n] & = & A_n & \text{für } n \geq 1, \\ [A_n, A_n] & = & \begin{cases} \{\mathrm{id}\} & \text{für } n = 1,2,3, \\ V_4 & \text{für } n = 4, \\ A_n & \text{für } n \geq 5. \end{cases} & \end{array}$$

Folgerung 2.4.13. *Die Gruppen S_n und A_n sind für $n \leq 4$ auflösbar, für $n \geq 5$ jedoch nicht mehr.*

Definition 2.4.14. Zwei Zykel $(i_1, \ldots, i_k)$ und $(j_1, \ldots, j_l)$ in S_n heißen *elementfremd*, falls $\{i_1, \ldots, i_k\}$ und $\{j_1, \ldots, j_l\}$ disjunkte Mengen sind.

Beispiel 2.4.15. Die Zykeln $(1,3)$ und $(2,4,5)$ in S_5 sind elementfremd:

Lemma 2.4.16. *Es sei $n \in \mathbb{Z}_{\geq 2}$.*

(i) *Für je zwei elementfremde Zykeln in $\sigma_1, \sigma_2 \in S_n$ gilt $\sigma_2 \circ \sigma_1 = \sigma_1 \circ \sigma_2$.*
(ii) *Jedes Element $\sigma \in S_n$ ist ein Produkt elementfremder Zykeln.*
(iii) *Jedes Element $\sigma \in S_n$ ist ein Produkt von Transpositionen.*

Beweis. Die erste Aussage ist offensichtlich. Die dritte folgt aus der zweiten und der Identität

$$(i_1, \ldots, i_k) \quad = \quad (i_1, i_2)(i_2, i_3) \ldots (i_{k-1}, i_k).$$

Zum Nachweis der zweiten Aussage betrachten wir die folgende Operation der zyklischen Gruppe $H := \langle \sigma \rangle$ auf $X_n = \{1, \ldots, n\}$:

$$H \times X_n \ \to \ X_n, \qquad h \cdot i \ := \ h(i).$$

Für $i \in X_n$ setzen wir $k(i) := |H \cdot i| = [H : H_i]$. Satz 2.1.10 liefert uns dann $H_i = \langle \sigma^{k(i)} \rangle$ und somit

$$H \cdot i \ = \ \{i, \sigma(i), \ldots, \sigma^{k(i)-1}(i)\}.$$

Weiter gilt $\sigma(H \cdot i) = H \cdot i$ und die Permutation σ wird auf der Bahn $H \cdot i$ durch einen Zykel dargestellt:

$$\sigma|_{H \cdot i} \ = \ (i, \, \sigma(i), \, \ldots, \, \sigma^{k-1}(i)).$$

Es sei nun $i_1, \ldots, i_r$ in X ein Vertretersystem für den Bahnenraum X_n/H. Wir setzen $k_j := [H : H_{i_j}] - 1$ Dann erhalten wir

$$\sigma \quad = \quad (i_1, \, \sigma(i_1), \, \ldots, \, \sigma^{k_1}(i_1)) \cdots (i_r, \, \sigma(i_r), \, \ldots, \, \sigma^{k_r}(i_r)).$$

□

Lemma 2.4.17. *Die alternierende Gruppe $A_n \subseteq S_n$ besteht genau aus den Produkten von 3-Zykeln.*

Beweis. Für $n = 1, 2$ ist die Aussage trivial. Es sei also $n \geq 3$. Nach Lemma 2.4.16 ist jedes Element von A_n ein Produkt einer geraden Anzahl von Transpositionen. Wir haben

$$\begin{array}{lcll} (i_1, i_2)(i_2, i_3) & = & (i_1, i_2, i_3) & \text{für } i_1, i_2, i_3 \text{ paarweise verschieden,} \\ (i_1, i_2)(i_3, i_4) & = & (i_1, i_3, i_2)(i_1, i_3, i_4) & \text{für } i_1, i_2, i_3, i_4 \text{ paarweise verschieden.} \end{array}$$

Folglich ist jedes Element aus A_n ein Produkt von 3-Zykeln. Die erste Gleichung zeigt zudem, dass jeder 3-Zykel und damit auch jedes Produkt von 3-Zykeln in A_n liegt. □

Beweis von Satz 2.4.12. Wir zeigen $[S_n, S_n] = A_n$. Der Signumshomomorphismus $\mathrm{sg}\colon S_n \to C_2$ liefert

$$[S_n, S_n] \ \subseteq \ \mathrm{Kern}(\mathrm{sg}) \ = \ A_n,$$

wobei wir verwenden, dass C_2 abelsch ist. Zur Inklusion $A_n \subseteq [S_n, S_n]$. Für jeden 3-Zykel $(i_1, i_2, i_3) \in S_n$ hat man eine Darstellung

$$(i_1, i_2, i_3) \ = \ (i_1, i_3)(i_2, i_3)(i_1, i_3)^{-1}(i_2, i_3)^{-1}$$

Insbesondere sind 3-Zykeln Kommutatoren. Lemma 2.4.17 liefert uns daher die gewünschte Inklusion $A_n \subseteq [S_n, S_n]$.

Wir bestimmen die Kommutatorgruppe $[A_n, A_n]$. In den Fällen $n = 1, 2, 3$ erhalten wir $[A_n, A_n] = \{\mathrm{id}\}$, da A_n abelsch ist wegen

$$|A_1| \ = \ 1 \ = \ \frac{|S_2|}{2} \ = \ |A_2|, \qquad |A_3| \ = \ \frac{|S_3|}{2} \ = \ 3.$$

Zum Fall $n = 4$. Wir zeigen zunächst $[A_4, A_4] \supseteq V_4$. Für paarweise verschiedene Elemente $i_1, \ldots, i_4$ hat man stets

$$(i_1, i_2, i_3)(i_1, i_2, i_4)(i_1, i_2, i_3)^{-1}(i_1, i_2, i_4)^{-1} \quad = \quad (i_1, i_2)(i_3, i_4)$$

Zur umgekehrten Inklusion. Es gilt $|A_4| = 12$ und $|V_4| = 4$. Also ist A_4/V_4 von der Ordnung 3 und somit abelsch. Das impliziert $[A_4, A_4] \subseteq V_4$.

Zum Fall $n \geq 5$. Nach Lemma 2.4.17 ist jedes Element in A_n Produkt von 3-Zykeln. Es genügt daher zu zeigen, dass jeder 3-Zykel $(i_1, i_2, i_3) \in A_n$ ein Kommutator ist. Dazu wählen wir $i_4, i_5 \in \{1, \ldots, n\}$, sodass $i_1, \ldots, i_5$ paarweise verschieden sind. Dann erhalten wir

$$(i_1, i_2, i_3) \quad = \quad (i_1, i_2, i_4)(i_1, i_3, i_5)(i_1, i_2, i_4)^{-1}(i_1, i_3, i_5)^{-1}.$$

□

Aufgaben zu Abschnitt 2.4.

Aufgabe 2.4.18. Es seien p eine Primzahl und G eine Gruppe mit $|G| = p^k$, wobei $k \geq 1$. Zeige:

(i) Gilt $k = 1$ oder $k = 2$, so ist G abelsch.
(ii) Gilt $k = 3$, so ist G entweder abelsch, oder es gilt $|Z_G| = p$.

Aufgabe 2.4.19. Die Diedergruppe D_4 sowie die Quaternionengruppe Q sind nichtabelsche Gruppen der Ordnung 8. Zeige:

(i) $Z_{D_4} \cong Z_Q$.
(ii) $D_4/Z_{D_4} \cong Q/Z_Q$.
(iii) D_4 und Q sind nicht isomorph.

Aufgabe 2.4.20. Zeige, dass die Gruppe $B(n, \mathbb{C}) \leq \mathrm{GL}(n, \mathbb{C})$ aller invertierbaren oberen $(n \times n)$-Dreiecksmatrizen auflösbar ist.

Aufgabe 2.4.21. Es sei G eine Gruppe. Zeige:

(i) Ist G auflösbar, so ist auch jede Untergruppe $H \leq G$ auflösbar.
(ii) Für jeden Normalteiler $N \trianglelefteq G$ gilt

$$G \text{ auflösbar} \iff N \text{ und } G/N \text{ auflösbar}.$$

Aufgabe 2.4.22 (Kleinsche Vierergruppe)**.** Beweise Bemerkung 2.4.11: Die Teilmenge

$$V_4 := \{\mathrm{id}, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\} \subset A_4$$

ist ein Normalteiler in der alternierenden Gruppe A_4, und man hat einen Isomorphismus

$$\begin{aligned} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} &\to V_4, \\ (\overline{0}, \overline{0}) &\mapsto \mathrm{id}, \\ (\overline{1}, \overline{0}) &\mapsto (1,2)(3,4), \\ (\overline{0}, \overline{1}) &\mapsto (1,3)(2,4), \\ (\overline{1}, \overline{1}) &\mapsto (1,4)(2,3). \end{aligned}$$

Aufgabe 2.4.23. Zeige: $\mathrm{GL}(2, \mathbb{C})$ und $\mathrm{SL}(2, \mathbb{C})$ sind nicht auflösbar.

Aufgabe 2.4.24. Es seien $p \in \mathbb{Z}_{\geq 1}$ eine Primzahl und G eine Gruppe der Ordnung $2p^k$, wobei $k \in \mathbb{Z}_{\geq 0}$. Zeige: G ist auflösbar.

3. Kommutative Ringe

3.1. **Grundbegriffe.**

Definition 3.1.1. Ein *kommutativer Ring mit Eins*, im folgenden kurz *K1-Ring* genannt ist eine Menge R mit Verknüpfungen

$$\begin{aligned} \text{add}\colon R \times R \to R, &\qquad (a,b) \mapsto a+b, \\ \text{mult}\colon R \times R \to R, &\qquad (a,b) \mapsto ab \end{aligned}$$

(üblicherweise Addition und Multiplikation genannt), sodass folgende Bedingungen erfüllt sind:

(i) (R, add) ist eine abelsche Gruppe, d.h.,
- es gilt stets $a + (b + c) = (a + b) + c$,
- es gilt stets $a + b = b + a$,
- es gibt ein Element $0 = 0_R \in R$ mit $0 + a = a$ für alle $a \in R$,
- zu jedem $a \in R$ gibt es ein Element $-a \in R$ mit $a + (-a) = 0$.

(ii) (R, mult) ist ein abelsches Monoid, d.h.,
- es gilt stets $a(bc) = (ab)c$,
- es gilt stets $ab = ba$,
- es gibt ein Element $1 = 1_R \in R$ mit $1a = a$. für alle $a \in R$,

(iii) Es gilt $a(b + c) = ab + ac$ für alle $a, b, c \in R$.

Satz 3.1.2. *Es sei R ein K1-Ring.*

(i) *Die neutralen Elemente $0 = 0_R$ der Addition und $1 = 1_R$ der Multiplikation in R sind eindeutig bestimmt.*

(ii) *Für jedes $r \in R$ gilt $0r = 0$. Insbesondere ist $1_R = 0_R$ nur in dem trivialen K1-Ring $R = \{0\}$ möglich.*

(iii) *Für jedes $r \in R$ gilt $(-1)r = -r$. Weiter hat man für je zwei $a, b \in R$:*

$$(-a)b \;=\; a(-b) \;=\; -(ab), \qquad (-a)(-b) \;=\; ab.$$

Beweis. Die Eindeutigkeit neutraler Elemente haben wir bereits in 1.1.10 nachgewiesen. Für den Nachweis von $0r = 0$ vermerken wir zunächst, dass

$$0r \;=\; (0+0)r \;=\; 0r + 0r$$

für jedes $r \in R$ gilt. Addiert man $-0r$ zu dieser Gleichung, so erhält man $0r = 0$. Gilt $1 = 0$ in einem K1-Ring R, so ergibt sich jedes $r \in R$:

$$r \;=\; 1r \;=\; 0r \;=\; 0.$$

Wir müssen nun zeigen, dass $(-1)r$ das additive Inverse zu r ist. Unter Verwendung von $0r = 0$ ergibt sich dies wie folgt:

$$(-1)r + r \;=\; (-1+1)r \;=\; 0r \;=\; 0.$$

Die verbleibenden Aussagen über $a, b \in R$ sind dann direkte Folgerungen aus $(-1)r = -r$:

$$\begin{aligned} (-a)b \;&=\; (-1)ab \;=\; -ab \;=\; a(-1)b \;=\; a(-b), \\ (-a)(-b) \;&=\; (-1)(-1)ab \;=\; (-(-1))ab \;=\; 1ab. \end{aligned}$$

□

Beispiel 3.1.3. Die ganzen Zahlen $\mathbb{Z}$ mit der üblichen Addition und Multiplikation bilden einen K1-Ring.

Beispiel 3.1.4. Es sei $n \in \mathbb{Z}_{\geq 1}$. Dann kann man auf der (additiven) Faktorgruppe $(\mathbb{Z}/n\mathbb{Z})$ eine Multiplikation definieren durch

$$\overline{a}\,\overline{b} \;:=\; \overline{ab}, \qquad \text{wobei} \quad \overline{a} = a + n\mathbb{Z}, \quad \overline{b} = b + n\mathbb{Z}, \quad \overline{ab} = ab + n\mathbb{Z}.$$

Dies hängt nicht von der Wahl der Repräsentanten a und b ab und macht $\mathbb{Z}/n\mathbb{Z}$ zu einem K1-Ring mit Nullelement $\overline{0} = 0 + n\mathbb{Z}$ und Einselement $\overline{1} = 1 + n\mathbb{Z}$.

Konstruktion 3.1.5. Es seien R_i, $i \in I$, K1-Ringe. Dann wird das kartesische Produkt $\prod_{i\in I} R_i$ mit den komponentenweisen Verknüpfungen

$$\begin{aligned}(a_i)_{i\in I} \ + \ (b_i)_{i\in I} &= (a_i + b_i)_{i\in I},\\ (a_i)_{i\in I}(b_i)_{i\in I} &= (a_i b_i)_{i\in I}.\end{aligned}$$

zu einem K1-Ring, dem *direkten Produkt* der Ringe R_i, $i \in I$. Die neutralen Elemente bezüglich Addition und Multiplikation sind $(0)_{i\in I}$ und $(1)_{i\in I}$.

Definition 3.1.6. Es sei R ein K1-Ring. Man nennt ein Element $a \in R$

(i) *Einheit*, falls $ab = 1$ mit einem $b \in R$ gilt;
(ii) *Nullteiler*, falls $ab = 0$ mit einem $b \in R \setminus \{0\}$ gilt;
(iii) *nilpotent*, falls $a^n = 0$ mit einem $n \in \mathbb{Z}_{\geq 1}$ gilt.

Beispiel 3.1.7.
(i) Der K1-Ring $\mathbb{Z}$ besitzt 1 und -1 als Einheiten. Es gibt keine Nullteiler und somit auch keine nilpotenten Elemente in $\mathbb{Z} \setminus \{0\}$.
(ii) In dem direkten Produkt $\mathbb{Z} \times \mathbb{Z}$ des K1-Ringes $\mathbb{Z}$ mit sich selbst gibt es echte (d.h. von Null verschiedene) Nullteiler: Es gilt beispielsweise

$$(1, 0) \cdot (0, 1) \ = \ (1 \cdot 0, 0 \cdot 1) \ = \ (0, 0).$$

(iii) Der K1-Ring $\mathbb{Z}/4\mathbb{Z}$ besitzt ein echtes nilpotentes Element: Es gilt

$$(2 + 4\mathbb{Z})(2 + 4\mathbb{Z}) \ = \ 4 + 4\mathbb{Z} \ = \ 0 + 4\mathbb{Z}.$$

Bemerkung 3.1.8. Die Menge R^* aller Einheiten eines K1-Ringes R zusammen mit der Multiplikation ist eine abelsche Gruppe mit neutralem Element 1_R. Wie üblich bezeichnen wir das multiplikative Inverse einer Einheit $a \in R^*$ mit a^{-1}.

Satz 3.1.9. *Es sei $n \in \mathbb{Z}_{\geq 1}$. Die Gruppe der Einheiten des Ringes $\mathbb{Z}/n\mathbb{Z}$ ist gegeben durch*

$$(\mathbb{Z}/n\mathbb{Z})^* \ = \ \{\overline{a} \in \mathbb{Z}/n\mathbb{Z};\ \mathrm{ggT}(a, n) = 1\}.$$

Beweis. Zu $a \in \mathbb{Z}$ betrachten wir den Homomorphismus $\varphi_a \colon \overline{b} \mapsto a\overline{b} = \overline{ab}$ aus Satz 2.1.12. Dann gilt:

$$\begin{aligned}a \in (\mathbb{Z}/n\mathbb{Z})^* \quad &\iff \quad \overline{ab} = \overline{1} \text{ mit einem } b \in \mathbb{Z}\\ &\iff \quad \varphi_a \circ \varphi_b = \varphi_b \circ \varphi_a = \mathrm{id}_{\mathbb{Z}/n\mathbb{Z}} \text{ mit einem } b \in \mathbb{Z}\\ &\iff \quad \varphi_a \in \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}, +)\\ &\iff \quad \mathrm{ggT}(a, n) = 1,\end{aligned}$$

Wobei die letzte Äquivalenz genau die Aussage von Satz 2.1.12 ist. □

Definition 3.1.10. Es sei R ein K1-Ring.

(i) R heißt *Integritätsring*, auch *Integritätsbereich*, falls $R \neq \{0\}$ gilt und R keine von Null verschiedenen Nullteiler besitzt.
(ii) R heißt *Körper*, falls $R \neq \{0\}$ gilt und $R^* = R \setminus \{0\}$ gilt, d.h., jedes von Null verschiedene Element eine Einheit ist.

Beispiel 3.1.11.
(i) Der Ring $\mathbb{Z}$ ist ein Integritätsring.
(ii) Das direkte Produkt $\mathbb{Z}^2$ ist kein Integritätsring.
(iii) $\mathbb{Q}$, $\mathbb{R}$ und $\mathbb{C}$ sind Körper.
(iv) Sei $n \in \mathbb{Z}_{\geq 1}$. Dann gilt:

$$\mathbb{Z}/n\mathbb{Z} \text{ ist Körper} \quad \iff \quad n \text{ ist Primzahl.}$$

Lemma 3.1.12 (Kürzungsregel)**.** *Es seien R ein Integritätsring und $a, b, c \in R$. Gelten $ab = ac$ und $a \neq 0$, so gilt $b = c$.*

Beweis. Die Kürzungsregel ergibt sich direkt aus der Nullteilerfreiheit: Durch einfache Umformungen erhalten wir

$$\begin{aligned} ab = ac &\Leftrightarrow ab - ac = 0 \\ &\Leftrightarrow a(b-c) = 0. \end{aligned}$$

Die letzte Gleichung impliziert $a = 0$ oder $b - c = 0$. Ersteres ist nach Voraussetzung ausgeschlossen. Also gilt $b - c = 0$. Das impliziert $b = c$. □

Definition 3.1.13. Es seien R ein K1-Ring, und $S \subseteq R$ eine Teilmenge mit folgenden Eigenschaften:

$$0, 1 \in S, \qquad a, b \in S \;\Rightarrow\; a - b \in S, \qquad a, b \in S \;\Rightarrow\; ab \in S.$$

Man nennt S zusammen mit den Verknüpfungen $(a, b) \mapsto a + b$ und $(a, b) \mapsto ab$ einen *Unterring* von R und bezeichnet das Paar $S \subseteq R$ auch als *Ringerweiterung*.

Beispiel 3.1.14. $\mathbb{Z} \subset \mathbb{Q}$ ist eine Ringerweiterung.

Konstruktion 3.1.15. Es seien R ein K1-Ring und S_i, $i \in I$, eine Familie von Unterringen $S_i \subseteq R$. Dann erhält man einen neuen Unterring

$$\bigcap_{i \in I} S_i \quad \subseteq \quad R.$$

Konstruktion 3.1.16. Es seien R ein K1-Ring, $S \subseteq R$ ein Unterring und $A \subseteq R$ eine nichtleere Teilmenge. Dann *erzeugt* A einen Unterring über S:

$$S[A] \;:=\; \left\{ \sum_{i=1}^{n} s_{i,1} \dots s_{i,m_i};\; n \in \mathbb{Z}_{\geq 1},\; s_{i,j} \;\in\; S \cup A \right\} \;\subseteq\; R.$$

Fü $A = \{a_1, \dots, a_r\}$ schreibt man auch $S[a_1, \dots, a_r]$ anstelle von $S[A]$. Man sagt auch, dass $S[A]$ durch *Ringadjunktion* von A an S entsteht. Es gilt stets

$$S[A] \quad = \bigcap_{S' \subseteq R \text{ Unterring},\; S \cup A \subseteq S'} S'.$$

Bemerkung 3.1.17. Ist R ein Integritätsring, so ist auch jeder Unterring $S \subseteq R$ ein Integritätsring.

Beispiel 3.1.18 (Ring der ganzen Gaußschen Zahlen)**.** Wir betrachten die Ringerweiterung $\mathbb{Z} \subseteq \mathbb{C}$ und die imaginäre Einheit $I \in \mathbb{C}$. Dann gilt

$$\mathbb{Z}[I] \quad = \quad \{n + Im;\; n, m \in \mathbb{Z}\}.$$

Man nennt $\mathbb{Z}[I]$ den *Ring der ganzen Gaußschen Zahlen*. Als Unterring des Integritätsringes $\mathbb{C}$ ist $\mathbb{Z}[I]$ ein Integritätsring.

Definition 3.1.19. Ein *Homomorphismus* von K1-Ringen R und S ist eine Abbildung $\varphi\colon R \to S$ mit folgender Eigenschaft: Für alle $a, b \in R$ gilt

$$\varphi(a + b) \;=\; \varphi(a) + \varphi(b), \qquad \varphi(ab) \;=\; \varphi(a)\varphi(b), \qquad \varphi(1) \;=\; 1.$$

Man nennt ein solches $\varphi\colon R \to S$ *Monomorphismus*, falls es injektiv ist, *Epimorphismus*, falls es surjektiv ist, *Isomorphismus*, wenn

$$\psi \circ \varphi \;=\; \mathrm{id}_R, \qquad \varphi \circ \psi \;=\; \mathrm{id}_S$$

mit einen Homomorphismus $\psi\colon S \to R$ von K1-Ringen gilt. Weiter definiert man Kern und Bild von $\varphi\colon R \to S$ als

$$\mathrm{Kern}(\varphi) \;:=\; \{u \in R;\; \varphi(u) = 0\}, \qquad \mathrm{Bild}(\varphi) \;:=\; \{\varphi(u);\; u \in R\}.$$

Bemerkung 3.1.20. Es seien $\varphi\colon R \to S$ und $\psi\colon S \to T$ Homomorphismen von K1-Ringen. Dann ist auch $\psi \circ \varphi\colon S \to T$ ein Homomorphismus von K1-Ringen.

Bemerkung 3.1.21. Es sei R_i, $i \in I$ eine Familie von K1-Ringen. Dann hat man kanonische Epimorphismen vom Produkt $\prod_{i\in I} R_i$ auf die einzelnen Faktoren:

$$\prod_{i\in I} R_i \ \to \ R_j \qquad (r_i)_{i\in I} \ \mapsto \ r_j.$$

Satz 3.1.22. *Es sei $\varphi\colon R \to S$ ein Homomorphismus von K1-Ringen.*

(i) *Ist $R' \subseteq R$ ein Unterring, so ist $\varphi(R') \subseteq S$ ein Unterring. Insbesondere ist* $\mathrm{Bild}(\varphi)$ *ein Unterring von S.*
(ii) *Ist $S' \subseteq S$ ein Unterring, so ist $\varphi^{-1}(S') \subseteq R$ ein Unterring.*
(iii) *Der Homomorphismus $\varphi\colon R \to S$ ist genau dann injektiv, wenn* $\mathrm{Kern}(\varphi) = \{0\}$ *gilt.*
(iv) *Der Homomorphismus $\varphi\colon R \to S$ ist genau dann ein Isomorphismus, wenn er bijektiv ist.*

Beweis. Zu (i): Wegen $1_R \in R'$ und $\varphi(1_R) = 1_S$ haben wir $1_S \in \varphi(R')$. Zu $b_1, b_2 \in \varphi(R')$ wählen wir $a_i \in R'$ mit $\varphi(a_i) = b_i$ und erhalten

$$b_1 - b_2 \ = \ \varphi(a_1) - \varphi(a_2) \ = \ \varphi(a_1 - a_2) \ \in \ \varphi(R'),$$

$$b_1 b_2 \ = \ \varphi(a_1)\varphi(a_2) \ = \ \varphi(a_1 a_2) \ \in \ \varphi(R').$$

Zu (ii). Wegen $1_S \in S'$ und $\varphi(1_R) = 1_S$ erhalten wir $1_R \in \varphi^{-1}(S')$. Sind weiter $a_1, a_2 \in \varphi^{-1}(S)$ gegeben, so erhalten wir $a_1 - a_2, a_1 a_2 \in \varphi^{-1}(S')$ wegen

$$\varphi(a_1 - a_2) \ = \ \varphi(a_1) - \varphi(a_2) \ \in \ S', \qquad \varphi(a_1 a_2) \ = \ \varphi(a_1)\varphi(a_2) \ \in \ S'.$$

Für (iii) und (iv) beachte man zunächst, dass $\varphi\colon R \to S$ auch ein Homomorphismus der zu Grunde liegenden additiven Gruppen $(R, +)$ und $(S, +)$ ist. Aussage (iii) erhalten wir mit der entsprechenden Aussage 1.3.14 über Gruppenhomomorphismen.

Zu (iv). Es ist klar, dass die Existenz eines Umkehrhomomorphismus $\psi\colon S \to R$ die Bijektivität impliziert. Ist $\varphi\colon R \to S$ bijektiv, so liefert 1.3.9 einen Umkehrhomomorphismus $\psi\colon S \to R$ der zu Grunde liegenden additiven Gruppen. Es gilt

$$\psi(1_S) \ = \ \psi(\varphi(1_R)) \ = \ 1_R.$$

Wir müssen also nur noch zeigen, dass ψ mit der Multiplikation verträglich ist. Das geht wie im Beweis von 1.3.9: Für je zwei $s_1, s_2 \in S$ gilt

$$s_1 s_2 \ = \ \varphi(\psi(s_1))\varphi(\psi(s_2)) \ = \ \varphi(\psi(s_1)\psi(s_2)).$$

Wendet man nun ψ auf diese Gleichung an, so ergibt sich die gewünschte Homomorphieeigenschaft. □

Bemerkung 3.1.23. Der Kern eines Homomorphismus von K1-Ringen ist im allgemeinen kein Unterring: Die Restklassenabbildung $\pi\colon \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ ist ein Epimorphismus von K1-Ringen und für $n \geq 2$ ist $\mathrm{Kern}(\varphi) = n\mathbb{Z}$ kein Unterring.

Bemerkung 3.1.24 (Bruchrechnen)**.** Wir betrachten die Ringerweiterung $\mathbb{Z} \subset \mathbb{Q}$. Die Elemente von $\mathbb{Q}$ sind Brüche a/b mit $a, b \in \mathbb{Z}$ und $b \neq 0$. Man hat

$$\frac{a_1}{a_2} \ = \ \frac{b_1}{b_2} \quad \Longleftrightarrow \quad a_1 b_2 \ = \ a_2 b_1.$$

Konstruktion 3.1.25 (Quotientenkörper)**.** Es sei R ein Integritätsring. Dann definieren wir eine Äquivalenzrelation auf $R \times (R \setminus \{0\})$ durch

$$(a_1, a_2) \ \sim \ (b_1, b_2) \quad :\Longleftrightarrow \quad a_1 b_2 \ = \ a_2 b_1.$$

Den zugehörige Menge der Äquivalenzklassen bezeichnet man mit $Q(R)$ und die Äquivalenzklasse eines Elementes (a, b) mit a/b. Wir definieren Verknüpfungen

$$\begin{aligned} \text{add}\colon\ Q(R)\times Q(R) &\to Q(R), & \frac{a_1}{a_2}+\frac{b_1}{b_2} &:= \frac{a_1b_2+a_2b_1}{a_2b_2} \\ \text{mult}\colon\ Q(R)\times Q(R) &\to Q(R), & \frac{a_1}{a_2}\frac{b_1}{b_2} &:= \frac{a_1b_1}{a_2b_2}. \end{aligned}$$

Zusammen mit diesen Verknüpfungen bildet die Menge $Q(R)$ einen Körper, den *Quotientenkörper* von R. Die neutralen Elemente sind

$$0_{Q(R)} = \frac{0_R}{1_R}, \qquad 1_{Q(R)} = \frac{1_R}{1_R}.$$

Weiter ist das multiplikative Inverse zu einem Element $0_{Q(R)} \neq a_1/a_2 \in Q(R)$ gegeben durch a_2/a_1.

Beweis. Symmetrie und Reflexivität der Relation "$\sim$" sind offensichtlich gegeben.

Die Transitivität weisen wir wie bei Konstruktion 1.4.11 nach: Wir schreiben $a = (a_1, a_2)$, etc.. Aus $a \sim b$ und $b \sim c$ erhalten wir dann

$$a_1b_2 = a_2b_1, \qquad b_1c_2 = b_2c_1.$$

Gilt $b_1 = 0$, so erhalten wir $a_1 = c_1 = 0$ und somit $a \sim c$. Gilt $b_1 \neq 0$, so multiplizieren wir die beiden obigen Gleichungen miteinander und erhalten

$$a_1b_2b_1c_2 = a_2b_1b_2c_1.$$

Wegen $b_1b_2 \neq 0$ können wir die Kürzungsregel 3.1.12 anwenden. Das ergibt $a_1c_2 = a_2c_1$. Wir erhalten also $a \sim c$.

Der nächste Schritt ist, die Wohldefiniertheit der Verknüpfungen auf $Q(R)$ nachzuweisen. Zur Addition: Wir müssen zeigen, dass

$$\frac{a_1b_2+a_2b_1}{a_2b_2} = \frac{a_1'b_2'+a_2'b_1'}{a_2'b_2'}$$

gilt, sobald $a \sim a'$ und $b \sim b'$ gelten, wobei wie üblich $a = (a_1, a_2)$, etc.. Schreiben wir letztere Äquivalenzen aus, so erhalten wir

$$a_1a_2' = a_2a_1', \qquad b_1b_2' = b_2b_1'.$$

Multipliziert man die erste Gleichung mit b_2b_2' und die zweite mit a_2a_2', so ergibt sich nach Umsortieren

$$a_2'b_2'a_1b_2 = a_2b_2a_1'b_2', \qquad a_2'b_2'a_2b_1 = a_2b_2a_2'b_1'.$$

Addition dieser beiden Gleichungen und anschließendes Ausklammern von $a_2'b_2'$ bzw. a_2b_2 ergibt die gewünschte Äquivalenz:

$$a_2'b_2'(a_1b_2+a_2b_1) = a_2b_2(a_1'b_2'+a_2'b_1').$$

Zur Multiplikation. Es seien $a \sim a'$ und $b \sim b'$ gelten, wobei wieder $a = (a_1, a_2)$, etc.. Dann haben wir

$$a_1a_2' = a_2a_1', \qquad b_1b_2' = b_2b_1'.$$

Multipliziert man diese beiden Gleichungen miteinander, so ergibt sich die gewünschte Äquivalenz

$$\frac{a_1b_1}{a_2b_2} = \frac{a_1'b_1'}{a_2'b_2'}.$$

Die Tatsache, dass $0_R/1_R$ bzw. $1_R/1_R$ die neutralen Elemente von Addition und Multiplikation sind, folgt unmittelbar aus der Definition der Verknüpfungen:

$$\frac{0_R}{1_R} + \frac{a_1}{a_2} \;=\; \frac{0_R a_2 + 1_R a_1}{1_R a_2} \;=\; \frac{a_1}{a_2}, \qquad \frac{1_R}{1_R} \cdot \frac{a_1}{a_2} \;=\; \frac{1_R a_1}{1_R a_2} \;=\; \frac{a_1}{a_2}.$$

Die multiplikative Inversenbildung in $Q(R) \setminus \{0/1\}$ geht wie folgt: für $a_1, a_2 \in R$ mi $a_2 \neq 0$ hat man

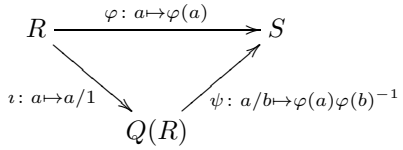
$$\left(\frac{a_1}{a_2}\right)\left(\frac{a_2}{a_1}\right) \;=\; \frac{a_1 a_2}{a_2 a_1} \;=\; \frac{1_R}{1_R}.$$

□

Satz 3.1.26. *Es seien R ein Integritätsring und $Q(R)$ sein Quotientenkörper. Dann hat man einen kanonischen Monomorphismus*

$$\imath\colon\; R \;\to\; Q(R), \qquad a \;\mapsto\; \frac{a}{1}.$$

Ist $\varphi\colon R \to S$ ein Homomorphismus von K1-Ringen mit $\varphi(R \setminus \{0\}) \subseteq S^*$, so gibt es ein kommutatives Diagramm



wohldefinierter Ringhomomorphismen. Der Homomorphismus $\psi\colon Q(R) \to S$ ist dabei eindeutig bestimmt.

Beweis. Nach Definition von $Q(R)$ ist klar, dass $\imath\colon R \to Q(R)$ ein Homomorphismus ist. Die Injektivität ergibt sich mit

$$\imath(a) \;=\; 0 \iff \frac{a}{1} \;=\; \frac{0}{1} \iff 1 \cdot a \;=\; 1 \cdot 0 \iff a \;=\; 0.$$

Um die Wohldefiniertheit von ψ einzusehen, betrachten wir zwei Darstellungen $a_1/a_2 = a_1'/a_2'$ eines Elements in $Q(R)$. Dann erhalten wir

$$\begin{aligned} \frac{a_1}{a_2} = \frac{a_1'}{a_2'} \quad &\iff \quad a_1 a_2' = a_1' a_2 \\ &\implies \quad \varphi(a_1 a_2') = \varphi(a_1' a_2) \\ &\implies \quad \varphi(a_1)\varphi(a_2)^{-1} = \varphi(a_1')\varphi(a_2')^{-1}. \end{aligned}$$

Der nächste Schritt ist es, die Homomorphieeigenschaften von $\psi\colon Q(R) \to S$ nachzuprüfen. Diese ergeben sich wie folgt:

$$\psi\left(\frac{1}{1}\right) \;=\; \varphi(1)\varphi(1)^{-1} \;=\; 1,$$

$$\begin{aligned} \psi\left(\frac{a_1}{a_2} + \frac{b_1}{b_2}\right) \;&=\; \psi\left(\frac{a_1 b_2 + a_2 b_1}{a_2 b_2}\right) \\ &=\; \varphi(a_1 b_2 + a_2 b_1)\varphi(a_2 b_2)^{-1} \\ &=\; \varphi(a_1)\varphi(a_2)^{-1} + \varphi(b_1)\varphi(b_2)^{-1} \\ &=\; \psi\left(\frac{a_1}{a_2}\right) + \psi\left(\frac{b_1}{b_2}\right), \end{aligned}$$

$$\begin{aligned}\psi\left(\frac{a_1}{a_2}\,\frac{b_1}{b_2}\right) &= \psi\left(\frac{a_1b_1}{a_2b_2}\right)\\ &= \varphi(a_1b_1)\varphi(a_2b_2)^{-1}\\ &= \varphi(a_1)\varphi(a_2)^{-1}\varphi(b_1)\varphi(b_2)^{-1}\\ &= \psi\left(\frac{a_1}{a_2}\right)\psi\left(\frac{b_1}{b_2}\right).\end{aligned}$$

Schließlich müssen wir uns noch davon überzeugen, dass ψ eindeutig bestimmt ist. Für jeden weiteren Homomorphismus $\psi'\colon Q(R) \to S$ mit $\psi' \circ \imath = \varphi$ erhalten wir

$$\psi'\left(\frac{a}{1}\right) = \varphi(a), \qquad \psi'\left(\frac{1}{b}\right) = \psi'\left(\left(\frac{b}{1}\right)^{-1}\right) = \psi'\left(\frac{b}{1}\right)^{-1} = \varphi(b)^{-1}$$

und somit

$$\psi'\left(\frac{a}{b}\right) = \psi'\left(\frac{a}{1}\frac{1}{b}\right) = \psi'\left(\frac{a}{1}\right)\psi'\left(\frac{1}{b}\right) = \varphi(a)\varphi(b)^{-1}.$$

□

Aufgaben zu Abschnitt 3.1.

Aufgabe 3.1.27. Es sei R ein K1-Ring, und es seien $a, b \in R$. Zeige: Für jedes $n \in \mathbb{Z}_{\geq 0}$ gilt

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

Aufgabe 3.1.28. Bestimme alle Einheiten, Nullteiler und nilpotenten Elemente der K1-Ringe $\mathbb{Z}/4\mathbb{Z}$ sowie $\mathbb{Z}/36\mathbb{Z}$.

Aufgabe 3.1.29. Es seien $n \in \mathbb{Z}_{\geq 2}$ und $\overline{m} \in \mathbb{Z}/n\mathbb{Z}$. Beweise die Äquivalenz folgender Aussagen:

(i) $\overline{m}$ erzeugt die additive Gruppe $\mathbb{Z}/n\mathbb{Z}$;
(ii) $\overline{m}$ ist eine Einheit in dem K1-Ring $\mathbb{Z}/n\mathbb{Z}$.

Aufgabe 3.1.30. Es sei R ein K1-Ring mit nur endlich vielen Elementen. Beweise die Äquivalenz folgender Aussagen:

(i) R ist ein Integritätsring.
(ii) R ist ein Körper.

Aufgabe 3.1.31. Es seien R ein $K1$-Ring, $a \in R$ nilpotent und $b \in R$ eine Einheit. Zeige: Das Element $a+b$ ist eine Einheit.

Aufgabe 3.1.32. Beweise die folgende Aussage über den Ring $\mathbb{Z}[I] \subseteq \mathbb{C}$ der ganzen Gaußschen Zahlen aus Beispiel 3.1.18: Es gilt

$$\mathbb{Z}[I] \quad = \quad \{n + Im;\ n, m \in \mathbb{Z}\}.$$

Zeige weiter, dass die Einheitengruppe von $\mathbb{Z}[I]$ genau aus den komplexen Zahlen $1, -1, I, -I$ besteht.

Aufgabe 3.1.33. Betrachte die Ringerweiterung $\mathbb{Z} \subseteq \mathbb{C}$. Für $d \in \mathbb{Z}_{\geq 0}$, bezeichne $\sqrt{d} \in \mathbb{R}_{\geq 0}$ wie üblich die Wurzel, und für $d \in \mathbb{Z}_{<0}$ setzen wir $\sqrt{d} := I\sqrt{-d}$, wobei $I \in \mathbb{C}$ die imaginäre Einheit bezeichnet. Es sei nun $d \in \mathbb{Z}$ quadratfrei. Zeige:

(i) Es gilt $\mathbb{Z}[\sqrt{d}] \ = \ \{m + n\sqrt{d};\ m, n \in \mathbb{Z}\}$.
(ii) Die Abbildung $N\colon \mathbb{Z}[\sqrt{d}] \to \mathbb{Z},\ \ m+n\sqrt{d} \mapsto m^2 - n^2 d$ erfüllt $N(ab) \ = \ N(a)N(b)$ für je zwei $a, b \in \mathbb{Z}[\sqrt{d}]$.
(iii) Für die Menge der Einheiten in $\mathbb{Z}[\sqrt{d}]$ gilt $\mathbb{Z}[\sqrt{d}]^* \ = \ \{a \in \mathbb{Z}[\sqrt{d}];\ N(a) = \pm 1\}$.

Aufgabe 3.1.34. Es seien X eine Menge und R ein K1-Ring. Zeige: Zusammen mit den punktweisen Verknüpfungen

$$(f+g)(x) \ := \ f(x) + g(x), \qquad (fg)(x) \ := \ f(x)g(x)$$

wird die Menge $\mathrm{Abb}(X, R)$ aller Abbildungen $X \to R$ zu einem K1-Ring. Ist $\mathrm{Abb}(X, R)$ ein Integritätsring, wenn dies für R gilt?

Aufgabe 3.1.35.
(i) Es sei $U \subset \mathbb{C}$ eine offene Menge. Man zeige: Der Ring $\mathcal{O}(U)$ der holomorphen Funktionen auf U ist genau dann ein Integritätsring, wenn U zusammenhängend ist.
(ii) Es sei $[a, b]$ ein Intervall in $\mathbb{R}$. Welcher der folgenden Ringe von Funktionen auf $[a, b]$ ist ein Integritätsring:
  (a) Der Ring $C[a, b]$ aller stetigen reellwertigen Funktionen,
  (b) der Ring $C^\infty[a, b]$ aller differenzierbaren reellwertigen Funktionen,
  (c) der Ring $C^{\mathrm{an}}[a, b]$ aller analytischen reellwertigen Funktionen?

Aufgabe 3.1.36. Zeige: Für $R = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{Z}/n\mathbb{Z}$ ist die Identität id_R der einzigen Homomorphismus $R \to R$ von K1-Ringen. Zeige weiter, dass es einen Homomorphismus $\mathbb{C} \to \mathbb{C}$ gibt, der nicht die Identität ist.

Aufgabe 3.1.37. Es sei $\varphi\colon R \to S$ ein Monomorphismus von Integritätsringen. Zeige: Es gibt einen eindeutig bestimmten Homomorphismus $Q(\varphi)\colon Q(R) \to Q(S)$ mit dem folgendes Diagramm kommutativ wird

$$\begin{array}{ccc} R & \xrightarrow{\varphi} & S \\ {\scriptstyle \imath}\downarrow & & \downarrow{\scriptstyle \imath} \\ Q(R) & \xrightarrow[Q(\varphi)]{} & Q(S) \end{array}$$

3.2. **Potenzreihen- und Polynomringe.**

Bemerkung 3.2.1. Intuitiv versteht man unter einer formalen Potenzreihe in der Veränderlichen T über einem K1-Ring R einen Ausdruck

$$\sum_{\nu=0}^{\infty} a_\nu T^\nu$$

mit Koeffizienten $a_\nu \in R$. Ein Polynom in der Veränderlichen T über R ist dann eine endliche formale Potenzreihe in T, d.h., ein Ausdruck

$$\sum_{\nu=0}^{\infty} a_\nu T^\nu, \qquad \text{wobei } a_\nu \neq 0 \text{ für höchstens endlich viele } \nu \in \mathbb{Z}_{\geq 0}.$$

Formale Potenzreihen (und damit auch Polynome) in der Veränderlichen T kann man addieren beziehungsweise multiplizieren:

$$\begin{aligned}
\left(\sum_{\nu=0}^{\infty} a_\nu T^\nu\right) \;+\; \left(\sum_{\nu=0}^{\infty} b_\nu T^\nu\right) \;&:=\; \sum_{\nu=0}^{\infty} (a_\nu + b_\nu) T^\nu, \\
\left(\sum_{\nu=0}^{\infty} a_\nu T^\nu\right) \;\cdot\; \left(\sum_{\nu=0}^{\infty} b_\nu T^\nu\right) \;&:=\; \sum_{\nu=0}^{\infty} c_\nu T^\nu, \qquad \text{wobei } c_\nu \;:=\; \sum_{\nu=\mu+\kappa} a_\mu b_\kappa.
\end{aligned}$$

Wir werden sehen, dass die formalen Potenzreihen mit diesen Verknüpfungen einen K1-Ring bilden und die Polynome einen Unterring darin.

Konstruktion 3.2.2 (Potenzreihen- und Polynomring in einer Veränderlichen)**.** Es sei R ein K1-Ring. Wir betrachten die Menge aller Folgen in R:

$$S(R) \;:=\; \prod_{\mathbb{Z}_{\geq 0}} R.$$

Auf $S(R)$ erhalten wir durch die komponentenweise Addition und das Cauchy-Produkt zwei Verknüpfungen:

$$\begin{aligned}
(a_\nu)_{\nu\in\mathbb{Z}_{\geq 0}} \;+\; (b_\nu)_{\nu\in\mathbb{Z}_{\geq 0}} \;&:=\; (a_\nu + b_\nu)_{\nu\in\mathbb{Z}_{\geq 0}}, \\
(a_\nu)_{\nu\in\mathbb{Z}_{\geq 0}} \;\cdot\; (b_\nu)_{\nu\in\mathbb{Z}_{\geq 0}} \;&:=\; (c_\nu)_{\nu\in\mathbb{Z}_{\geq 0}}, \qquad \text{wobei } c_\nu \;:=\; \sum_{\nu=\mu+\kappa} a_\mu b_\kappa.
\end{aligned}$$

Zusammen mit diesen Verknüpfungen wird $S(R)$ zu einem K1-Ring; die neutralen Elemente bezüglich Addition und Multiplikation sind die Folgen

$$(0, 0, 0, \ldots), \qquad (1, 0, 0, \ldots).$$

Weiter bilden die Folgen $(a_\nu)_{\nu\in\mathbb{Z}_{\geq 0}}$ mit nur endlich vielen nichttrivialen Folgengliedern einen Unterring:

$$S_0(R) \;:=\; \left\{(a_\nu)_\nu \in \mathbb{Z}_{\geq 0};\; a_\nu \neq 0 \text{ für höchstens endlich viele } \nu \in \mathbb{Z}_{\geq 0}\right\}.$$

Beweis. Wir müssen die Axiome eines K1-Ringes für $S(R)$ nachweisen. Dabei ist klar, dass $(S(R), +)$ eine abelsche Gruppe ist, denn hier liegt einfach ein gruppentheoretisches Produkt von $(R, +)$ über der Indexmenge $\mathbb{Z}_{\geq 0}$ vor. Die Kommutativität der Multiplikation auf $S(R)$ ist offensichtlich:

$$\begin{aligned}
(a_\nu)_\nu \cdot (b_\nu)_\nu \;&=\; \left(\sum_{\nu=\mu+\kappa} a_\mu b_\kappa\right)_\nu \\
&=\; \left(\sum_{\nu=\mu+\kappa} b_\mu a_\kappa\right)_\nu \\
&=\; (b_\nu)_\nu \cdot (a_\nu)_\nu.
\end{aligned}$$

Zur Assoziativität der Multiplikation:

$$\begin{aligned}
(a_\nu)_\nu \cdot ((b_\nu)_\nu \cdot (c_\nu)_\nu) &= (a_\nu)_\nu \cdot \left(\sum_{\nu=\mu+\kappa} b_\mu c_\kappa \right)_\nu \\
&= \left(\sum_{\nu=\nu'+\nu''} a_{\nu'} \left(\sum_{\nu''=\mu+\kappa} b_\mu c_\kappa \right) \right)_\nu \\
&= \left(\sum_{\nu=\nu'+\nu''+\nu'''} a_{\nu'} b_{\nu''} c_{\nu'''} \right)_\nu \\
&= \left(\sum_{\nu=\nu'+\nu''} \left(\sum_{\nu'=\mu+\kappa} a_\mu b_\kappa \right) c_{\nu''} \right)_\nu \\
&= \left(\sum_{\nu=\mu+\kappa} a_\mu b_\kappa \right)_\nu \cdot (c_\nu)_\nu \\
&= ((a_\nu)_\nu \cdot (b_\nu)_\nu) \cdot (c_\nu)_\nu.
\end{aligned}$$

Zur Distributivität von Multiplikation und Addition:

$$\begin{aligned}
(a_\nu)_\nu \cdot ((b_\nu)_\nu + (c_\nu)_\nu) &= (a_\nu)_\nu \cdot (b_\nu + c_\nu)_\nu \\
&= \left(\sum_{\nu=\mu+\kappa} a_\mu (b_\kappa + c_\kappa) \right)_\nu \\
&= \left(\sum_{\nu=\mu+\kappa} a_\mu b_\kappa + a_\mu c_\kappa \right)_\nu \\
&= \left(\sum_{\nu=\mu+\kappa} a_\mu b_\kappa + \sum_{\nu=\mu+\kappa} a_\mu c_\kappa \right)_\nu \\
&= \left(\sum_{\nu=\mu+\kappa} a_\mu b_\kappa \right)_\nu + \left(\sum_{\nu=\mu+\kappa} a_\mu c_\kappa \right)_\nu \\
&= ((a_\nu)_\nu \cdot (b_\nu)_\nu) + ((a_\nu)_\nu \cdot (c_\nu)_\nu).
\end{aligned}$$

Die Tatsache, dass $(1, 0, 0, \ldots)$ neutrales Element bezüglich der Multiplikation ist, ergibt sich direkt aus der Definition der Multiplikation. □

Schreibweise 3.2.3. Es seien R, $S(R)$ und $S_0(R)$ wie in Konstruktion 3.2.2. Um $S(R)$ und $S_0(R)$ besser handhaben zu können, arbeitet man mit dem Element

$$T \ := \ (0, 1, 0, 0, \ldots) \ \in \ S(R).$$

Nach Definition der Multiplikation in $S(R)$ ist für jedes $\mu \in \mathbb{Z}_{\geq 0}$ die entsprechende Potenz T^μ von T gegeben durch

$$T^\mu \ = \ (\delta_{\mu\nu})_{\nu \in \mathbb{Z}_{\geq 0}}, \qquad \delta_{\mu\nu} \ := \ \begin{cases} 1, & \mu = \nu, \\ 0, & \mu \neq \nu. \end{cases}$$

Für den Ring $S(R)$ und seine Elemente $(a_\nu)_{\nu \in \mathbb{Z}_{\geq 0}} \in S(R)$ verwenden wir dann künftig die Bezeichnungen

$$R[[T]] \ := \ S(R), \qquad \sum_{\nu=0}^{\infty} a_\nu T^\nu \ := \ (a_\nu)_{\nu \in \mathbb{Z}_{\geq 0}}.$$

Die Elemente von $R[[T]]$ nennt man *formale Potenzreihen* über R in der Veränderlichen T und bezeichnet dabei die Folgenglieder a_ν als ihre *Koeffizienten*.

Weiter nennt man $R[T] := S_0(R)$ den *Polynomring* über R in der Veränderlichen T. Die Elemente von $R[T]$ heissen *Polynome*. Zu jedem Poynom

$$f \;=\; \sum_{\nu=0}^{\infty} a_\nu T^\nu \;\in R[T]$$

gibt es ein $n \in \mathbb{Z}_{\geq 0}$, sodass $\alpha_\nu = 0$ für alle $\nu \geq n+1$ gilt; nach Definition der Addition in $R[T]$ erhalten wir dann

$$f \;=\; \sum_{\nu=0}^{\infty} a_\nu T^\nu \;=\; \sum_{\nu=0}^{n} a_\nu T^\nu \;=\; a_n T^n + a_{n-1}T^{n-1} + \ldots + a_1 T + a_0.$$

Dabei schreibt man a für aT^0. Die neutralen Elemente bezüglich der Addition und der Multiplikation in $R[T]$ bzw. $R[[T]]$ sind gegeben durch

$$0_{R[T]} \;=\; 0_{R[[T]]} \;=\; 0, \qquad\qquad 1_{R[T]} \;=\; 1_{R[[T]]} \;=\; 1.$$

Bemerkung 3.2.4. Es seien R ein K1-Ring und $a, b \in R$. Nach Definition der Multiplikation gilt in $R[T]$ sowie in $R[[T]]$ stets

$$(aT^\nu) \cdot (bT^\mu) \;=\; abT^{\nu+\mu}.$$

Weiter erhält das Produkt zweier Polynome $\sum a_\nu T^\nu$ und $\sum b_\mu T^\mu$ in $R[T]$ durch Ausmultiplizieren der Summen.

Bemerkung 3.2.5. Es seien R ein K1-Ring und $R[T]$ der zugehörige Polynomring. Dann ist $R[T]$ als Ring durch $RT^0 \cup \{T\}$ erzeugt.

Satz 3.2.6 (Universelle Eigenschaft des Polynomrings)**.** *Es sei R ein K1-Ring. Dann hat man einen kanonischen Monomorphismus*

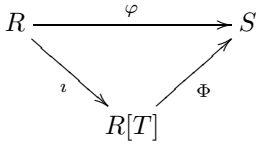
$$\imath\colon R \;\to\; R[T], \qquad a \;\mapsto\; aT^0.$$

Ist $\varphi\colon R \to S$ ein Homomorphismus von K1-Ringen und ist $s \in S$, so erhält man durch

$$\Phi\colon R[T] \;\to\; S, \qquad \sum_{\nu=0}^{n} a_\nu T^\nu \;\mapsto\; \sum_{\nu=0}^{n} \varphi(a_\nu) s^\nu$$

einen Homomorphismus; dieser besitzt folgende Eigenschaften und ist dadurch eindeutig bestimmt:

(i) *Es gilt $\Phi(T) = s$,*
(ii) *das folgende Diagramm ist kommutativ*



Beweis. Die Tatsache, dass $\imath\colon R \to R[T]$ ein Homomorphismus ist ergibt sich direkt aus den Definitionen von Addition und Multiplikation in $R[T]$:

$$\imath(a+b) \;=\; (a+b)T^0 \;=\; aT^0 + bT^0 \;=\; \imath(a) + \imath(b),$$

$$\imath(ab) \;=\; (ab)T^0 \;=\; aT^0 \cdot bT^0 \;=\; \imath(a) \cdot \imath(b).$$

Um die Injektivität des Homomorphismus $\imath\colon R \to R[T]$ zu erhalten, machen wir uns klar, dass er trivialen Kern besitzt: Es gilt

$$\imath(a) = 0 \;\Leftrightarrow\; aT^0 = 0T^0 \;\Leftrightarrow\; a = 0.$$

Die Tatsache, dass $\Phi\colon R[T] \to S$ ein Homomorphismus ist, ergibt sich mit Bemerkung 3.2.4; wir führen den Beweis dennoch explizit:

$$\Phi(1T^0) \;=\; \varphi(1)s^0 \;=\; 1,$$

$$\begin{aligned}
\Phi\left(\sum_\nu a_\nu T^\nu + \sum_\nu b_\nu T^\nu\right) &= \Phi\left(\sum_\nu (a_\nu + b_\nu) T^\nu\right) \\
&= \sum_\nu \varphi(a_\nu + b_\nu) s^\nu \\
&= \sum_\nu (\varphi(a_\nu) + \varphi(b_\nu)) s^\nu \\
&= \sum_\nu \varphi(a_\nu) s^\nu + \sum_\nu \varphi(a_\nu) s^\nu \\
&= \Phi\left(\sum_\nu a_\nu T^\nu\right) + \Phi\left(\sum_\nu a_\nu T^\nu\right),
\end{aligned}$$

$$\begin{aligned}
\Phi\left(\left(\sum_\nu a_\nu T^\nu\right)\left(\sum_\nu b_\nu T^\nu\right)\right) &= \Phi\left(\sum_\nu \left(\sum_{\mu+\kappa=\nu} a_\mu b_\kappa\right) T^\nu\right) \\
&= \sum_\nu \varphi\left(\sum_{\mu+\kappa=\nu} a_\mu b_\kappa\right) s^\nu \\
&= \sum_\nu \left(\sum_{\mu+\kappa=\nu} \varphi(a_\mu)\varphi(b_\kappa)\right) s^\nu \\
&= \left(\sum_\nu \varphi(a_\nu) s^\nu\right)\left(\sum_\nu \varphi(b_\nu) s^\nu\right) \\
&= \Phi\left(\sum_\nu a_\nu T^\nu\right) \Phi\left(\sum_\nu b_\nu T^\nu\right).
\end{aligned}$$

Weiter sind die Eigenschaften (i) und (ii) klar nach Definition von Φ. Die Tatsache, dass Φ durch diese Eigenschaften festgelegt ist, folgt mit Bemerkung 3.2.5. □

Bemerkung 3.2.7. Die Tatsache, dass man einen kanonischen Monomorphismus $R \to R[T]$ vorliegen hat, erlaubt es uns, in Zukunft R als Unterring von $R[T]$ aufzufassen.

Folgerung 3.2.8. *Es sei R ein K1-Ring. Jedes Element $r \in R$ definiert einen* Auswertungshomomorphismus

$$\varepsilon_r\colon R[T] \;\to\; R, \qquad f = \sum a_\nu T^\nu \;\mapsto\; f(r) := \sum a_\nu r^\nu.$$

Definition 3.2.9. Es sei R ein K1-Ring. Der *Grad* eines Polynomes in $\sum a_\nu T^\nu \in R[T]$ ist definiert als

$$\deg\left(\sum a_\nu T^\nu\right) \;:=\; \begin{cases} \max(\nu \in \mathbb{Z}_{\geq 0};\; a_\nu \neq 0) & \text{falls } f \neq 0, \\ -\infty & \text{falls } f = 0. \end{cases}$$

Gilt $n := \deg(\sum a_\nu T^\nu) > -\infty$, so nennt man a_n den *Leitkoeffizienten* des Polynoms $\sum a_\nu T^\nu$.

Bemerkung 3.2.10. Es sei R ein K1-Ring.

(i) Für jedes $\nu \in \mathbb{Z}_{\geq 0}$ hat man $\deg(T^\nu) = \nu$.
(ii) Für jedes $f \in R[T]$ gilt $\deg(f) = -\infty \Leftrightarrow f = 0$.

(iii) Besitzt $0 \neq f \in R[T]$ den Leitkoeffizienten a_f, so gilt

$$f \;=\; a_f T^{\deg(f)} + \sum_{\nu=0}^{\deg(f)-1} a_\nu T^\nu.$$

Bemerkung 3.2.11. Es seien R ein K1-Ring, und es seien $f, g \in R[T]$ nichttriviale Polynome mit Leitkoeffizienten $a_f, a_g \in R$, und es seien $d_f := \deg(f)$ sowie $d_g := \deg(g)$. Dann sind Summe und Produkt der Polynome f, g von der Form

$$f+g \;=\; bT^{\max(d_f,d_g)} + \sum_{\nu=0}^{\max(d_f,d_g)-1} c_\nu T^\nu,$$

$$\text{wobei } b := \begin{cases} a_f & \text{falls } d_f > d_g, \\ a_g & \text{falls } d_f < d_g, \\ a_f + a_g & \text{falls } d_f = d_g, \end{cases}$$

$$fg \;=\; a_f a_g T^{d_f+d_g} + \sum_{\nu=0}^{d_f+d_g-1} c_\nu T^\nu.$$

Folgerung 3.2.12. *Es seien R ein K1-Ring und $f, g \in R[T]$. Dann gilt:*

$$\begin{aligned} \deg(f+g) &\leq \max(\deg(f), \deg(g)), \\ \deg(fg) &\leq \deg(f) + \deg(g) \end{aligned}$$

Ist R ein Integritätsring, so hat man im zweiten Fall stets Gleichheit.

Folgerung 3.2.13. *Es sei R ein K1-Ring. Dann gilt*

$$R \text{ ist Integritätsring} \iff R[T] \text{ ist Integritätsring}$$

Gilt eine der beiden Aussagen, so hat man $R[T]^* = R^*$.

Beweis. Zu "⇒". Sind $f, g \in R[T]$ von Null verschiedene Elemente, so sehen wir mit Bemerkung 3.2.11, dass fg ebenfalls nichttrival ist. Zu "⇐". Nach Satz 3.2.6 ist R ein Unterring des Integritätsringes $R[T]$ und muss somit selbst Integritätsring sein.

Die Inklusion $R^* \subseteq R[T]^*$ ist offensichtlich. Zum Nachweis der Inklusion $R^* \supseteq R[T]^*$ betrachten wir ein $f \in R[T]^*$. Dann gibt es ein $g \in R[T]$ mit $fg = T^0$. Mit Folgerung 3.2.12 erhalten wir $\deg(f) = \deg(g) = 0$. Das bedeutet $f, g \in R$, was weiter $f \in R^*$ impliziert. □

Konstruktion 3.2.14 (Potenzreihen- und Polynomring in n Veränderlichen)**.** Es seien R ein K1-Ring und $n \in \mathbb{Z}_{\geq 1}$. Wir betrachten die Indexmenge $\mathbb{Z}_{\geq 0}^n := (\mathbb{Z}_{\geq 0})^n$ und das kartesische Produkt

$$S^n(R) \;:=\; \prod_{\nu \in \mathbb{Z}_{\geq 0}^n} R.$$

In formaler Analogie zu Konstruktion 3.2.2 führen wir Verknüpfungen auf $S^n(R)$ ein: Die komponentenweise Addition und ein Cauchy-Produkt

$$\begin{aligned} (a_\nu)_{\nu \in \mathbb{Z}_{\geq 0}^n} \;+\; (b_\nu)_{\nu \in \mathbb{Z}_{\geq 0}^n} &:= (a_\nu + b_\nu)_{\nu \in \mathbb{Z}_{\geq 0}^n}, \\ (a_\nu)_{\nu \in \mathbb{Z}_{\geq 0}^n} \;\cdot\; (b_\mu)_{\mu \in \mathbb{Z}_{\geq 0}^n} &:= (c_\kappa)_{\kappa \in \mathbb{Z}_{\geq 0}^n}, \qquad \text{wobei } c_\kappa := \sum_{\nu+\mu=\kappa} a_\nu b_\mu. \end{aligned}$$

Zusammen mit diesen Verknüpfungen wird $S^n(R)$ zu einem K1-Ring; die neutralen Elemente bezüglich Addition und Multiplikation sind gegeben durch

$$(z_\nu)_{\nu\in\mathbb{Z}^n_{\geq 0}} \quad \text{wobei} \quad z_\nu = 0 \text{ für alle } \nu \in \mathbb{Z}^n_{\geq 0},$$
$$(e_\nu)_{\nu\in\mathbb{Z}^n_{\geq 0}} \quad \text{wobei} \quad \begin{cases} e_\nu = 1 & \text{falls } \nu = (0,\ldots,0), \\ e_\nu = 0 & \text{falls } \nu \neq (0,\ldots,0). \end{cases}$$

Weiter bilden die Elemente $(a_\nu)_{\nu\in\mathbb{Z}^n_{\geq 0}}$ mit nur endlich vielen nichttrivialen Gliedern a_ν einen Unterring:

$$S^n_0(R) \;:=\; \big\{(a_\nu)_\nu \in \mathbb{Z}^n_{\geq 0};\ a_\nu \neq 0 \text{ für höchstens endlich viele } \nu \in \mathbb{Z}^n_{\geq 0}\big\}$$

Beweis. Die Konstruktion verläuft völlig analog zu der im Fall einer Veränderlichen. Beim Nachweis der Axiome eines K1-Ringes wurde dort nur von der Tatsache Gebrauch gemacht, dass die Indexmenge $\mathbb{Z}_{\geq 0}$ ein abelsches Monoid ist. Das ist für $\mathbb{Z}^n_{\geq 0}$ ebenso gegeben. □

Schreibweise 3.2.15. Es seien R, $S^n(R)$ und $S^n_0(R)$ wie in Konstruktion 3.2.14. Für jedes $i = 1,\ldots,n$ definiert man ein Element

$$T_i \;:=\; (\tau_{i,\nu})_{\nu\in\mathbb{Z}^n_{\geq 0}}, \qquad \tau_{i,\nu} \;:=\; \begin{cases} 1, & \nu = e_i, \\ 0, & \nu \neq e_i, \end{cases}$$

wobei $e_1 = (1,0,\ldots,0),\ldots,e_n = (0,\ldots,0,1)$ die Einheitsvektoren in $\mathbb{Z}^n_{\geq 0}$ sind. Für $\nu \in \mathbb{Z}^n_{\geq 0}$ setzt man

$$T^\nu \;:=\; T_1^{\nu_1}\cdots T_n^{\nu_n}.$$

Für den Ring $S^n(R)$ und seine Elemente $(a_\nu)_{\nu\in\mathbb{Z}^n_{\geq 0}} \in S^n(R)$ verwenden wir künftig die Bezeichnungen

$$R[[T_1,\ldots,T_n]] \;:=\; S^n(R), \qquad \sum_{\nu=0}^{\infty} a_\nu T^\nu \;:=\; (a_\nu)_{\nu\in\mathbb{Z}^n_{\geq 0}}.$$

Die Elemente von $R[[T_1,\ldots,T_n]]$ heissen *formale Potenzreihen* über R in den Veränderlichen $T_1,\ldots,T_n$ und man nennt die Folgenglieder a_ν ihre *Koeffizienten*.

Weiter nennt man $R[T_1,\ldots,T_n] := S^n_0(R)$ den *Polynomring* über R in den Veränderlichen $T_1,\ldots,T_n$. Die Elemente von $R[T_1,\ldots,T_n]$ heissen *Polynome*.

Bemerkung 3.2.16. Es seien R ein K1-Ring und $a, b \in R$. Dann gilt in $R[T_1,\ldots,T_n]$ und somit auch in $R[[T_1,\ldots,T_n]]$ stets

$$\begin{aligned} aT^\nu \cdot bT^\mu &= aT_1^{\nu_1}\cdots T_n^{\nu_n}\cdot bT_1^{\mu_1}\cdots T_n^{\mu_n} \\ &= abT_1^{\nu_1+\mu_1}\cdots T_n^{\nu_n+\mu_n} \\ &= abT^{\nu+\mu}. \end{aligned}$$

Weiter man erhält man das Produkt zweier Polynome $\sum a_\nu T^\nu$ und $\sum b_\mu T^\mu$ durch Ausmultiplizieren der Summen.

Bemerkung 3.2.17. Es sei R ein K1-Ring. Dann ist der Polynomring $R[T_1,\ldots,T_n]$ als Ring durch $RT^0 \cup \{T_1,\ldots,T_n\}$ erzeugt.

Satz 3.2.18 (Universelle Eigenschaft des Polynomrings)**.** *Es sei R ein K1-Ring. Dann hat man einen kanonischen Monomorphismus*

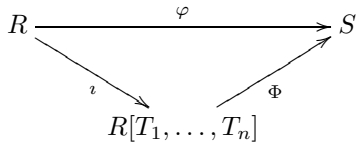
$$\imath\colon R \;\to\; R[T_1,\ldots,T_n], \qquad a \;\mapsto\; aT^0.$$

Ist $\varphi\colon R \to S$ ein Homomorphismus von K1-Ringen und sind $s_1,\ldots,s_n \in S$, so erhält man durch

$$\Phi\colon R[T_1,\ldots T_n] \;\to\; S, \qquad \sum_{\nu\in\mathbb{Z}^n_{\geq 0}} a_\nu T^\nu \;\mapsto\; \sum_{\nu\in\mathbb{Z}^n_{\geq 0}} \varphi(a_\nu)s^\nu, \ \text{wobei } s^\nu := s_1^{\nu_1}\cdots s_n^{\nu_n}.$$

einen Homomorphismus; dieser besitzt folgende Eigenschaften und ist dadurch eindeutig bestimmt:

(i) *Es gilt* $\Phi(T_i) = s_i$ *für jedes* $i = 1, \ldots, n$,
(ii) *das folgende Diagramm ist kommutativ*



Beweis. Der Beweis verläuft völlig analog zu dem im Fall einer Veränderlichen. □

Folgerung 3.2.19. *Es seien* $n \in \mathbb{Z}_{\geq 1}$ *und* R *ein K1-Ring. Jedes Element* $r \in R^n$ *definiert einen* Auswertungshomomorphismus

$$\varepsilon_r \colon R[T_1, \ldots, T_n] \;\to\; R, \qquad f = \sum a_\nu T^\nu \;\mapsto\; f(a) := \sum a_\nu r^\nu.$$

Satz 3.2.20. *Es sei* R *ein K1-Ring. Dann gilt* $R[T_1, \ldots, T_n] \cong R[T_1, \ldots, T_{n-1}][T]$.

Beweis. Mit der universellen Eigenschaft des Polynomringes erhalten wir Homomorphismen

$$\begin{aligned}
\Phi \colon R[T_1, \ldots, T_n] &\to R[T_1, \ldots, T_{n-1}][T], \\
R \ni a &\mapsto a, \\
T_1 &\mapsto T_1, \\
&\vdots \\
T_{n-1} &\mapsto T_{n-1}, \\
T_n &\mapsto T, \\
R[T_1, \ldots, T_n] &\leftarrow R[T_1, \ldots, T_{n-1}][T] \\
P &\leftarrow\!\shortmid P \in R[T_1, \ldots, T_{n-1}], \\
T_n &\leftarrow\!\shortmid T.
\end{aligned}$$

Die Eindeutigkeitsaussage der universellen Eigenschaft liefert, dass Komposition $\Psi \circ \Phi$ und $\Phi \circ \Psi$ jeweils die Identität sind. □

Folgerung 3.2.21. *Es sei* R *ein Integritätsring. Dann gilt:*

(i) *Der Polynomring* $R[T_1, \ldots, T_n]$ *ist ein Integritätsring.*
(ii) $R[T_1, \ldots, T_n]^* = R^*$.

Beweis. Durch Induktion über n. Der Fall $n = 1$ ist 3.2.13, und der Induktionsschritt ergibt sich aus 3.2.20 und 3.2.13. □

Aufgaben zu Abschnitt 3.2.

Aufgabe 3.2.22. Es sei $R = \mathbb{Z}/4\mathbb{Z}$. Bestimme alle Einheiten, Nullteiler und nilpotenten Elemente in den Ringen $R[T]$ und $R[[T]]$.

Aufgabe 3.2.23. Es sei R ein nicht notwendigerweise nullteilerfreier K1-Ring. Zeige:

$$R[T]^* \quad = \quad \left\{ \sum a_\nu T^\nu;\ a_0 \in R^*;\ a_\nu \text{ nilpotent für } \nu \geq 1 \right\}.$$

Aufgabe 3.2.24. Es seien $n \in \mathbb{Z}_{\geq 0}$ und R ein K1-Ring. Zeige: Man hat einen kanonischen Ringhomomorphismus

$$R[T_1, \ldots, T_n] \ \to \ \mathrm{Abb}(R^n, R), \qquad f \ \mapsto \ [a \mapsto f(a)].$$

Zeige durch Angabe expliziter Beispiele, dass dieser Homomorphismus im allgemeinen weder surjektiv noch injektiv ist.

Aufgabe 3.2.25. Es sei R ein K1-Ring. Die *Ordnung* einer formalen Potenzreihe in $R[[T_1, \ldots, T_n]]$ ist definiert als:

$$\mathrm{ord}\left(\sum_{\nu \in \mathbb{Z}^n_{\geq 0}} a_\nu T^\nu \right) \quad := \quad \begin{cases} \infty & \text{falls f=0,} \\ \min_{a_\nu \neq 0}(\nu_1 + \ldots + \nu_n) & \text{sonst.} \end{cases}$$

Zeige: Für je zwei formale Potenzreihen $f, g \in R[[T_1, \ldots, T_n]]$ gilt

(i) $\mathrm{ord}(f+g) \geq \min(\mathrm{ord}(f), \mathrm{ord}(g))$.
(ii) $\mathrm{ord}(fg) \geq \mathrm{ord}(f) + \mathrm{ord}(g)$.
(iii) $\mathrm{ord}(fg) = \mathrm{ord}(f) + \mathrm{ord}(g)$, falls R nullteilerfrei ist.

Aufgabe 3.2.26. Es sei R ein K1-Ring. Beweise die Äquivalenz folgender Aussagen:

(i) R ist Integritätsring.
(ii) $R[[T_1, \ldots, T_n]]$ ist Integritätsring.

Aufgabe 3.2.27. Es sei $n \in \mathbb{Z}_{\geq 1}$, und es sei R ein nicht notwendigerweise nullteilerfreier K1-Ring. Zeige:

$$R[[T_1, \ldots, T_n]]^* \quad = \quad \left\{ \sum a_\nu T^\nu;\ a_0 \in R^* \right\}.$$

Hinweis: Es genügt, multiplikative Inverse für Potenzreihen der Form $f = \sum a_\nu T^\nu$ mit $a_0 = 1$ anzugeben. Dazu betrachte die formale unendliche Summe

$$g \quad := \quad \sum_{n=0}^{\infty} (1-f)^n$$

Zeige, dass für festes ν nur endlich viele $(1-f)^n$ einen nichtrivialen Koeffizienten vor T^ν stehen haben. Insbesondere definiert g ein Element in $R[[T_1, \ldots, T_n]]$. Zeige nun $fg = 1$.

3.3. **Ideale I.**

Definition 3.3.1. Es sei R ein K1-Ring. Eine nichtleere Teilmenge $\mathfrak{a} \subseteq R$ heißt *Ideal*, geschrieben $\mathfrak{a} \leq_R R$, falls sie folgende Eigenschaften besitzt:

(i) Für je zwei $a, a' \in \mathfrak{a}$ gilt $a + a' \in \mathfrak{a}$.
(ii) Für jedes $r \in R$ und jedes $a \in \mathfrak{a}$ gilt $ra \in \mathfrak{a}$.

Bemerkung 3.3.2. Es sei R ein K1-Ring. Dann haben wir die Ideale $\{0\} \leq_R R$ und $R \leq_R R$.

Bemerkung 3.3.3. Es seien R ein K1-Ring und $\mathfrak{a} \leq_R R$ ein Ideal. Dann ist $\mathfrak{a}$ eine Untergruppe von $(R, +)$, aber im Allgemeinen kein Unterring von R.

Beispiel 3.3.4. Die Menge $2\mathbb{Z}$ der geraden Zahlen ist ein Ideal im Ring $\mathbb{Z}$ der ganzen Zahlen. Allgemeiner gilt für eine beliebige Teilmenge $\mathfrak{a} \subseteq \mathbb{Z}$:

$$\mathfrak{a} \leq_{\mathbb{Z}} \mathbb{Z} \Leftrightarrow \mathfrak{a} \leq \mathbb{Z} \Leftrightarrow \mathfrak{a} = n\mathbb{Z} \text{ mit einem } n \in \mathbb{Z}_{\geq 0}.$$

Dabei ist klar, dass $n\mathbb{Z}$ stets ein Ideal ist. Umgekehrt ist jedes Ideal $\mathfrak{a} \subseteq \mathbb{Z}$ eine Untergruppe von $(\mathbb{Z}, +)$ und daher nach Lemma 2.1.7 von der Form $\mathfrak{a} = n\mathbb{Z}$.

Beispiel 3.3.5. Es seien R ein K1-Ring, $R[T_1, \ldots, T_n]$ der Polynomring in den Veränderlichen $T_1, \ldots, T_n$ und $X \subseteq R^n$. Dann definiert X ein *Verschwindungsideal*:

$$I(X) := \{f \in R[T_1, \ldots, T_n];\ f(x) = 0 \text{ für alle } x \in X\} \leq_{R[T_1,\ldots,T_n]} R[T_1, \ldots, T_n].$$

Satz 3.3.6. *Es seien R ein K1-Ring, $R^* \subseteq R$ seine Einheitengruppe und $\mathfrak{a} \leq_R R$. Dann haben wir*

$$\mathfrak{a} = R \Leftrightarrow \mathfrak{a} \cap R^* \neq \emptyset.$$

Beweis. Gilt $\mathfrak{a} = R$, so folgt $\mathfrak{a} \cap R^* \neq \emptyset$ mit $1 \in R^*$. Gilt $\mathfrak{a} \cap R^* \neq \emptyset$, so betrachten wir ein $c \in \mathfrak{a} \cap R^*$. Wegen $c \in R$ gibt es ein $c' \in R$ mit $c'c = 1$. Die Idealeigenschaften liefern $r = r1 = rc'c \in \mathfrak{a}$ für jedes $r \in R$. □

Bemerkung 3.3.7. Es seien R ein K1-Ring und $\mathfrak{a}_i$, $i \in I$, eine Familie von Idealen. Dann ist der Durchschnitt über alle $\mathfrak{a}_i$ wieder ein Ideal in R:

$$\bigcap_{i \in I} \mathfrak{a}_i \leq_R R.$$

Konstruktion 3.3.8. Es sei R ein K1-Ring. Jede Teilmenge $A \subseteq R$ *erzeugt* ein Ideal:

$$\langle A \rangle := \left\{ \sum r_i a_i;\ n \in \mathbb{Z}_{\geq 0},\ r_i \in R,\ a_i \in A. \right\} \leq_R R.$$

Gilt $A = \{a_1, \ldots, a_n\}$, so schreibt man auch $\langle a_1, \ldots, a_n \rangle$ für $\langle A \rangle$. Für das von einer Teilmenge $A \subseteq R$ erzeugte Ideal in R gilt

$$\langle A \rangle = \bigcap_{A \subseteq \mathfrak{a} \leq_R R} \mathfrak{a} \leq_R R.$$

Somit ist $\langle A \rangle$ das kleinste Ideal in R, welches A enthält. Das von einem Element $a \in R$ erzeugte Ideal, auch das von a erzeugte *Hauptideal* genannt, ist gegeben als

$$\langle a \rangle = Ra = \{ra;\ r \in R\}.$$

Beispiel 3.3.9. Im Ring $\mathbb{Z}$ der ganzen Zahlen wird jedes Ideal von einem Element erzeugt, siehe Beispiel 3.3.4.

Satz 3.3.10. *Ein K1-Ring R mit $1 \neq 0$ ist genau dann ein Körper, wenn $\{0\}$ und R seine einzigen Ideale sind.*

Beweis. Es sei zunächst R ein Körper. Dann ist jedes $a \in R \setminus \{0\}$ eine Einheit. Ist $\mathfrak{a} \subseteq R$ ein Ideal, so gilt also entweder $\mathfrak{a} = \{0\}$ oder $\mathfrak{a} \cap R^* \neq \emptyset$. Letzteres ist nach Satz 3.3.6 äquivalent zu $\mathfrak{a} = R$.

Es seien nun $\{0\}$ und R die einzigen Ideale von R. Wir müssen zeigen, dass jedes $a \in R \setminus \{0\}$ eine Einheit ist. Dazu betrachten wir das von a erzeugte Ideal

$$\langle a \rangle \;=\; \{ra;\; r \in R\}.$$

Dann gilt $\langle a \rangle \neq \{0\}$ und somit $\langle a \rangle = R$. Insbesondere haben wir $1 \in \langle a \rangle$. Folglich gibt es ein $a' \in R$ mit $1 = a'a$. Das beweist $a \in R^*$. □

Satz 3.3.11. *Es sei $\varphi\colon R \to S$ ein Homomorphismus von K1-Ringen.*

(i) *Ist $\mathfrak{b} \subseteq S$ ein Ideal, so ist $\varphi^{-1}(\mathfrak{b})$ ein Ideal in R; insbesondere ist* $\operatorname{Kern}(\varphi) = \varphi^{-1}(0)$ *ein Ideal in R.*
(ii) *Ist $\mathfrak{a} \subseteq R$ ein Ideal und ist φ ein Epimorphismus von Ringen, so ist $\varphi(\mathfrak{a})$ ein Ideal in S.*

Beweis. Zu (i). Es sei $\mathfrak{b} \leq_S S$. Um die definierenden Eigenschaften eines Ideals für $\varphi^{-1}(\mathfrak{b})$ nachzuprüfen, seien $a_1, a_2 \in \varphi^{-1}(\mathfrak{b})$ und $r \in R$ gegeben. Dann erhalten wir $a_1 + a_2 \in \varphi^{-1}(\mathfrak{b})$ und $ra_1 \in \varphi^{-1}(\mathfrak{b})$ mit

$$\varphi(a_1 + a_2) \;=\; \varphi(a_1) + \varphi(a_2) \;\in\; \mathfrak{b}, \qquad \varphi(ra_1) \;=\; \varphi(r)\varphi(a_1) \;\in\; \mathfrak{b}.$$

Zu (ii). Es seien $\varphi\colon R \to S$ ein Epimorphismus und $\mathfrak{a} \leq_R R$. Sind $b_1, b_2 \in \varphi(\mathfrak{a})$ und $s \in S$ gegeben, so wählen wir $a_1, a_2 \in \mathfrak{a}$ mit $\varphi(a_i) = b_i$ und $r \in R$ mit $\varphi(r) = s$. Dann erhalten wir

$$b_1 + b_2 \;=\; \varphi(a_1) + \varphi(a_2) \;=\; \varphi(a_1 + a_2) \;\in\; \varphi(\mathfrak{a}),$$
$$sb_1 \;=\; \varphi(r)\varphi(a_1) \;=\; \varphi(ra_1) \;\in\; \varphi(\mathfrak{a}).$$

□

Folgerung 3.3.12. *Jeder Körperhomomorphismus ist injektiv.*

Beweis. Es sei $\varphi\colon \mathbb{K} \to \mathbb{K}'$ ein Homomorphismus von Körpern. Satz 3.3.11 liefert $\operatorname{Kern}(\varphi) \leq_{\mathbb{K}} \mathbb{K}$. Wegen $\varphi(1) = 1 \neq 0$ gilt $\operatorname{Kern}(\varphi) \neq \mathbb{K}$. Nach Satz 3.3.10 muss dann bereits $\operatorname{Kern}(\varphi) = \{0\}$ gelten. Somit ist φ injektiv. □

Beispiel 3.3.13. Es seien R ein K1-Ring, $R[T_1, \ldots, T_n]$ der Polynomring in den Veränderlichen $T_1, \ldots, T_n$, und für $x \in R^n$ bezeichne

$$\varepsilon_x\colon R[T_1, \ldots, T_n] \;\to\; R, \qquad f \;\mapsto\; f(x)$$

wie gewohnt den Auswertungshomomorphismus. Ist $X \subseteq R^n$ eine Teilmenge, so gilt für deren Verschwindungsideal

$$I(X) \;=\; \{f \in R[T_1, \ldots, T_n];\; f(x) = 0 \text{ für alle } x \in X\} \;=\; \bigcap_{x \in X} \operatorname{Kern}(\varepsilon_x).$$

Konstruktion 3.3.14 (Faktorring)**.** Es seien R ein K1-Ring und $\mathfrak{a} \leq_R R$ ein Ideal. Wir betrachten die (additive) Faktorgruppe

$$R/\mathfrak{a} \;:=\; \{r + \mathfrak{a};\; r \in R\}$$

und definieren eine Multiplikation auf $R/\mathfrak{a}$, indem wir für zwei Nebenklassen $r + \mathfrak{a}$ und $s + \mathfrak{a}$ setzen:

$$(r + \mathfrak{a})(s + \mathfrak{a}) \;:=\; rs + \mathfrak{a}.$$

Damit wird $R/\mathfrak{a}$ zu einem K1-Ring, dem *Faktorring* von R nach $\mathfrak{a}$. Die neutralen Elemente bezüglich Addition und Multiplikation in $R/\mathfrak{a}$ sind

$$0+\mathfrak{a} \;\in\; R/\mathfrak{a}, \qquad 1+\mathfrak{a} \;\in\; R/\mathfrak{a}.$$

Man hat einen kanonischen Epimorphismus von dem K1-Ring R auf den Faktorring $R/\mathfrak{a}$:

$$\pi\colon R \;\to\; R/\mathfrak{a}, \qquad r \;\mapsto\; r+\mathfrak{a}.$$

Beweis. Es ist nur zu zeigen, dass die Multiplikation wohldefiniert ist. dazu betrachten wir $r, r' \in R$ und $s, s' \in R$ mit

$$r+\mathfrak{a} \;=\; r'+\mathfrak{a}, \qquad s+\mathfrak{a} \;=\; s'+\mathfrak{a}.$$

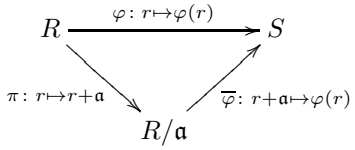
Wir müssen zeigen, dass rs und $r's'$ dieselbe Nebenklasse in $R/\mathfrak{a}$ definieren. Es gilt $r-r' \in \mathfrak{a}$ und $s-s' \in \mathfrak{a}$. Weiter erhalten wir

$$\begin{aligned} rs &= (r'+(r-r'))(s'+(s-s')) \\ &= r's'+r'(s-s')+s'(r-r')+(r-r')(s-s'). \end{aligned}$$

Die letzten drei Summanden liegen alle im Ideal $\mathfrak{a}$. Folglich definieren die Elemente rs und $r's'$ dieselbe Nebenklasse in $R/\mathfrak{a}$. □

Beispiel 3.3.15. Der für $n \in \mathbb{Z}_{\geq 0}$ in Beispiel 3.1.4 definierte K1-Ring $\mathbb{Z}/n\mathbb{Z}$ ist der Faktorring von $\mathbb{Z}$ nach dem Ideal $n\mathbb{Z}$.

Satz 3.3.16 (Homomorphiesatz)**.** *Es sei $\varphi\colon R \to S$ ein Homomorphismus von K1-Ringen, und es sei $\mathfrak{a} \leq_R R$ ein Ideal mit $\mathfrak{a} \subseteq \mathrm{Kern}(\varphi)$. Dann gibt es ein kommutatives Diagramm*



von wohldefinierten Homomorphismen zwischen K1-Ringen. Dabei ist der Homomorphismus $\overline{\varphi}\colon R/\mathfrak{a} \to S$ durch $\varphi\colon R \to S$ und das obige Diagramm eindeutig bestimmt. Es gilt weiter

(i) *$\overline{\varphi}$ ist injektiv $\Leftrightarrow$ $\mathfrak{a} = \mathrm{Kern}(\varphi)$;*
(ii) *$\overline{\varphi}$ ist surjektiv $\Leftrightarrow$ φ ist surjektiv.*

Beweis. Da φ und π Homomorphismen der zu Grunde liegenden additiven (abelschen) Gruppen sind, besagt der Homomorphiesatz 1.3.17, dass $\overline{\varphi}\colon R/\mathfrak{a} \to S$, $r+\mathfrak{a} \mapsto \varphi(r)$ ein (wohldefinierter) Gruppenhomomorphismus mit den entsprechenden Eigenschaften ist. Die noch fehlenden Eigenschaften eines Ringhomomorphismus lassen sich leicht nachweisen:

$$\overline{\varphi}(1_{R/\mathfrak{a}}) \;=\; \varphi(1_R) \;=\; 1_S.$$

$$\overline{\varphi}((r+\mathfrak{a})(r'+\mathfrak{a})) \;=\; \overline{\varphi}(rr'+\mathfrak{a}) \;=\; \varphi(rr') \;=\; \varphi(r)\varphi(r') \;=\; \overline{\varphi}(r+\mathfrak{a})\overline{\varphi}(r'+\mathfrak{a}).$$

□

Konstruktion 3.3.17. Es seien R ein K1-Ring und $\mathfrak{a}_i$, $i \in I$, eine Familie von Idealen. Dann erhält man neue Ideale in R:

(i) Die *Summe*

$$\sum_{i\in I} \mathfrak{a}_i \;:=\; \left\{ \sum_{j\in J} a_j;\; J \subseteq I \text{ endlich},\; a_j \in \mathfrak{a}_j \right\} \;\leq_R\; R.$$

(ii) Falls I endlich ist, das *Produkt*

$$\prod_{i\in I}\mathfrak{a}_i \;:=\; \left\langle \prod_{i\in I} a_i;\; a_i\in\mathfrak{a}_i \right\rangle \;\leq_R\; R.$$

Bemerkung 3.3.18. Es seien R ein K1-Ring und $\mathfrak{a}_i$, $i\in I$ eine (ggf. endliche) Familie von Idealen in R. Dann gilt

$$\sum_{i\in I}\mathfrak{a}_i \;=\; \left\langle \bigcup_{i\in I}\mathfrak{a}_i \right\rangle, \qquad \prod_{i\in I}\mathfrak{a}_i \;\subseteq\; \bigcap_{i\in I}\mathfrak{a}_i.$$

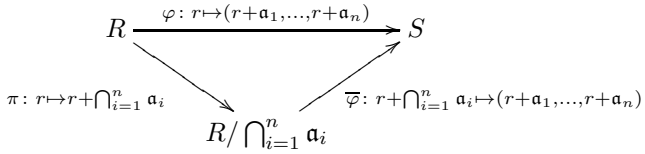
Satz 3.3.19 (Chinesischer Restsatz)**.** *Es sei R ein K1-Ring, und es seien $\mathfrak{a}_1,\ldots,\mathfrak{a}_n$ Ideale in R mit $\mathfrak{a}_i+\mathfrak{a}_j=R$ für alle i,j mit $i\neq j$. Dann hat man einen Isomorphimus*

$$\begin{aligned} R\Big/\bigcap_{i=1}^{n}\mathfrak{a}_i \quad &\to \quad R/\mathfrak{a}_1\times\ldots\times R/\mathfrak{a}_n,\\ r+\bigcap_{i=1}^{n}\mathfrak{a}_i \quad &\mapsto \quad (r+\mathfrak{a}_1,\ldots,r+\mathfrak{a}_n). \end{aligned}$$

Beweis. Man hat einen kanonischen Homomorphismus von R auf das direkte Produkt der Faktorringe $R/\mathfrak{a}_i$:

$$\varphi\colon R\;\to\; R/\mathfrak{a}_1\times\ldots\times R/\mathfrak{a}_n, \qquad r\;\mapsto\; (r+\mathfrak{a}_1,\ldots,r+\mathfrak{a}_n).$$

Der Kern dieses Homomorphismus ist gegeben durch $\mathrm{Kern}(\varphi)=\bigcap_{i=1}^n\mathfrak{a}_i$. Der Homomorphiesatz 3.3.16 liefert daher ein kommutatives Diagramm



Nach 3.3.16 ist nur noch zu zeigen, dass φ surjektiv ist. Dafür wählen wir zu jedem $j\neq i$ Elemente $a_j\in\mathfrak{a}_i$ und $b_j\in\mathfrak{a}_j$ mit $a_j+b_j=1$. Damit erhalten wir

$$\begin{aligned} 1_R \;&=\; \prod_{j\neq i}(a_j+b_j)\\ &\in\; \mathfrak{a}_i \;+\; \prod_{j\neq i} b_j\\ &\subseteq\; \mathfrak{a}_i \;+\; \bigcap_{j\neq i}\mathfrak{a}_j. \end{aligned}$$

Das liefert uns für jedes für jedes i Elemente $c_i\in\mathfrak{a}_i$ und $d_i\in\bigcap_{j\neq i}\mathfrak{a}_j$ mit $c_i+d_i=1_R$. Damit ergibt sich

$$\varphi(d_i) \;=\; (0_{R/\mathfrak{a}_1},\ldots,0_{R/\mathfrak{a}_{i-1}},1_{R/\mathfrak{a}_i},0_{R/\mathfrak{a}_{i+1}},\ldots,0_{R/\mathfrak{a}_n}).$$

Damit sehen wir, dass jedes Element $(r_1+\mathfrak{a}_1,\ldots,r_n+\mathfrak{a}_n)\in R/\mathfrak{a}_1\times\ldots\times R/\mathfrak{a}_n$ im Bild von φ liegt: Es gilt

$$(r_1+\mathfrak{a}_1,\ldots,r_n+\mathfrak{a}_n) \;=\; \varphi(r_1d_1+\ldots+r_nd_n).$$

□

Aufgaben zu Abschnitt 3.3.

Aufgabe 3.3.20. Es seien $m, n \in \mathbb{Z}_{\geq 0}$. Beweise folgende Identitäten:

$$\langle m\rangle \cap \langle n\rangle \;=\; \langle \mathrm{kgV}(m,n)\rangle, \qquad \langle m\rangle + \langle n\rangle \;=\; \langle \mathrm{ggT}(m,n)\rangle, \qquad \langle m\rangle\langle n\rangle \;=\; \langle mn\rangle.$$

Aufgabe 3.3.21. Zeige: Zu jedem Tripel (a_1, a_2, a_3) ganzer Zahlen gibt es eine ganze Zahl a mit

$$a \equiv a_1 \mod 35, \qquad a \equiv a_2 \mod 44, \qquad a \equiv a_3 \mod 57,$$

wobei die Schreibweise "$a \equiv b \mod c$" wie üblich bedeutet, dass c ein Teiler der Differenz $b - a$ ist.

Aufgabe 3.3.22. Es seien R ein K1-Ring und $\mathfrak{a} \leq_R R$ ein Ideal. Das *Radikal* von $\mathfrak{a}$ ist definiert als

$$\sqrt{\mathfrak{a}} \;:=\; \{b \in R;\ b^n \in \mathfrak{a} \text{ für ein } n \in \mathbb{Z}_{\geq 0}\}.$$

Zeige: Das Radikal $\sqrt{\mathfrak{a}}$ ist wieder ein Ideal. *Hinweis:* Verwende den binomischen Lehrsatz.

Aufgabe 3.3.23 (Erster Isomorphiesatz für Ringe)**.** Es seien R ein K1-Ring, $S \subseteq R$ ein Unterring und $\mathfrak{a} \leq_R R$ ein Ideal. Zeige: $S \cap \mathfrak{a}$ ist ein Ideal in S und es gilt

$$(S + \mathfrak{a})/\mathfrak{a} \;\cong\; S/(S \cap \mathfrak{a}).$$

Aufgabe 3.3.24 (Zweiter Isomorphiesatz für Ringe)**.** Es seien R ein K1-Ring und $\mathfrak{a}$, $\mathfrak{b}$ Ideale in R mit $\mathfrak{a} \subseteq \mathfrak{b}$. Zeige: $\mathfrak{b}/\mathfrak{a}$ ist ein Ideal in $R/\mathfrak{a}$ und es gilt

$$(R/\mathfrak{a})/(\mathfrak{b}/\mathfrak{a}) \;\cong\; R/\mathfrak{b}.$$

Aufgabe 3.3.25. Betrachte die Ideale $\mathfrak{a} := \langle 9\rangle$ und $\mathfrak{b} := \langle 12\rangle$ in $\mathbb{Z}$ sowie $\mathfrak{c} := \langle T^2\rangle$ und $\mathfrak{d} := \langle T^2 + T\rangle$ in $\mathbb{Q}[T]$ und bestimme jeweils einen Erzeuger für

$$\mathfrak{a} + \mathfrak{b}, \qquad \mathfrak{a} \cap \mathfrak{b}, \qquad \mathfrak{c} + \mathfrak{d}, \qquad \mathfrak{c}\mathfrak{d}.$$

Aufgabe 3.3.26. Es seien $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ Ideale in einem K1-Ring R. Zeige:

(i) $\mathfrak{a}(\mathfrak{b} + \mathfrak{c}) = \mathfrak{a}\mathfrak{b} + \mathfrak{a}\mathfrak{c}$,
(ii) $\mathfrak{a} \cap (\mathfrak{b} + \mathfrak{c}) \supseteq (\mathfrak{a} \cap \mathfrak{b}) + (\mathfrak{a} \cap \mathfrak{c})$; Gleichheit gilt, falls $\mathfrak{b} \subseteq \mathfrak{a}$ oder $\mathfrak{c} \subseteq \mathfrak{a}$ gilt,
(iii) $(\mathfrak{a} + \mathfrak{b})(\mathfrak{a} \cap \mathfrak{b}) \subseteq \mathfrak{a}\mathfrak{b}$.

Aufgabe 3.3.27. Sind $\mathfrak{a}$ und $\mathfrak{b}$ Ideale eines K1-Ringes R, so definiert man den *Idealquotienten* $(\mathfrak{a} : \mathfrak{b})$ als

$$(\mathfrak{a} : \mathfrak{b}) := \{r \in R;\ r\mathfrak{b} \subseteq \mathfrak{a}\}$$

Zeige: Der Idealquotient $(\mathfrak{a} : \mathfrak{b})$ ist wieder ein Ideal in R. Beweise folgende Aussagen für Ideale $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$, $\mathfrak{a}_i$, $i \in I$ und $\mathfrak{b}_j$, $j \in J$, Ideale eines K1-Ringes R:

(i) $\mathfrak{a} \subseteq (\mathfrak{a} : \mathfrak{b})$,
(ii) $(\mathfrak{a} : \mathfrak{b})\mathfrak{b} \subseteq \mathfrak{a}$,
(iii) $((\mathfrak{a} : \mathfrak{b}) : \mathfrak{c}) = (\mathfrak{a} : \mathfrak{b}\mathfrak{c}) = ((\mathfrak{a} : \mathfrak{c}) : \mathfrak{b})$,
(iv) $(\bigcap_{i\in I} \mathfrak{a}_i : \mathfrak{b}) = \bigcap_{i\in I}(\mathfrak{a}_i : \mathfrak{b})$,
(v) $(\mathfrak{a} : \sum_{j\in J} \mathfrak{b}_j) = \bigcap_{j\in J}(\mathfrak{a} : \mathfrak{b}_j)$.

Aufgabe 3.3.28. Es seien m, $n \in \mathbb{Z}$. Beweise die Identität $(\langle m\rangle : \langle n\rangle) = \langle m/\mathrm{ggT}(m,n)\rangle$.

3.4. **Ideale II.**

Definition 3.4.1. Es sei R ein K1-Ring. Ein Ideal $\mathfrak{p} \leq_R R$ heißt *Primideal*, falls folgendes gilt:

(i) $\mathfrak{p}$ ist ein echtes Ideal in R, d.h., es gilt $\mathfrak{p} \neq R$;
(ii) sind $a, b \in R$ mit $ab \in \mathfrak{p}$, so gilt $a \in \mathfrak{p}$ oder $b \in \mathfrak{p}$.

Beispiel 3.4.2. Für $p \in \mathbb{Z}_{\geq 0}$ betrachten wir das Ideal $\langle p \rangle \leq_{\mathbb{Z}} \mathbb{Z}$. Dann gilt für jede Zahl $c \in \mathbb{Z}$:

$$c \in \langle p \rangle \iff c \in p\mathbb{Z} \iff p|c.$$

Damit erhält man, dass $\langle p \rangle$ genau dann ein Primideal in $\mathbb{Z}$ ist, wenn $p = 0$ gilt oder p eine Primzahl ist.

Satz 3.4.3. *Es seien R ein K1-Ring und $\mathfrak{p} \leq_R R$ ein Ideal. Dann sind folgende Aussagen äquivalent:*

(i) *$\mathfrak{p}$ ist ein Primideal.*
(ii) *$R/\mathfrak{p}$ ist Integritätsring.*

Beweis. Zur Implikation "(i)⇒(ii)". Da $\mathfrak{p} \neq R$ gilt, sind Null- und Einselement in $R/\mathfrak{p}$ verschieden.

Wir zeigen nun, dass es keine echten Nullteiler in $R/\mathfrak{p}$ gibt. Dazu seien Restklassen $a + \mathfrak{p}$ und $b + \mathfrak{p}$ in $R/\mathfrak{p}$ gegeben mit

$$(a + \mathfrak{p})(b + \mathfrak{p}) \;=\; 0 + \mathfrak{p} \;\in\; R/\mathfrak{p}.$$

Dann gilt $ab \in \mathfrak{p}$. Da $\mathfrak{p}$ ein Primideal ist, erhalten wir $a \in \mathfrak{p}$ oder $b \in \mathfrak{p}$. Das bedeutet

$$a + \mathfrak{p} \;=\; 0 + \mathfrak{p} \;\in\; R/\mathfrak{p} \qquad \text{oder} \qquad b + \mathfrak{p} \;=\; 0 + \mathfrak{p} \;\in\; R/\mathfrak{p}.$$

Zur Implikation "(ii)⇒(i)". Als Integritätsring besitzt $R/\mathfrak{p}$ mindestens zwei Elemente. Folglich muss $\mathfrak{p} \neq R$ gelten.

Wir weisen nun die zweite definierende Eigenschaft eines Primideals nach. Es seien $a, b \in R$ mit $ab \in \mathfrak{p}$ gegeben. Dann gilt

$$(a + \mathfrak{p})(b + \mathfrak{p}) \;=\; ab + \mathfrak{p} \;=\; 0 + \mathfrak{p} \;\in\; R/\mathfrak{p}.$$

Da $R/\mathfrak{p}$ als Integritätsring keine echten Nullteiler besitzt, erhalten wir

$$a + \mathfrak{p} \;=\; 0 + \mathfrak{p} \;\in\; R/\mathfrak{p} \qquad \text{oder} \qquad b + \mathfrak{p} \;=\; 0 + \mathfrak{p} \;\in\; R/\mathfrak{p}.$$

Das bedeutet $a \in \mathfrak{p}$ oder $b \in \mathfrak{p}$. □

Definition 3.4.4. Es sei R ein K1-Ring. Ein Ideal $\mathfrak{m} \leq_R R$ heißt *maximal*, falls folgendes gilt:

(i) $\mathfrak{m}$ ist ein echtes Ideal in R, d.h., es gilt $\mathfrak{m} \neq R$;
(ii) für jedes echte Ideal $\mathfrak{a} \subsetneq R$ mit $\mathfrak{m} \subseteq \mathfrak{a}$ gilt $\mathfrak{a} = \mathfrak{m}$.

Beispiel 3.4.5. Es sei $\mathbb{K}$ ein Körper. Dann ist $\langle T \rangle \subseteq \mathbb{K}[T]$ ein maximales Ideal in $\mathbb{K}[T]$. Dazu vermerken wir zunächst

$$\langle T \rangle \;=\; \left\{ \sum_{\nu=1}^{n} a_\nu T^\nu;\; n \in \mathbb{Z}_{\geq 1},\; a_\nu \in \mathbb{K} \right\}.$$

Somit ist jedes $f \in \mathbb{K}[T] \setminus \langle T \rangle$ von der Form $f = c + g$ mit $g \in \langle T \rangle$ und $c \in \mathbb{K}^* = \mathbb{K}[T]^*$. Folglich enthält jedes Ideal $\mathfrak{a} \subseteq \mathbb{K}[T]$ mit $\langle T \rangle \subsetneq \mathfrak{a}$ Einheiten. Insbesondere kann $\langle T \rangle$ nicht echte Teilmenge eines echten Ideals sein.

Satz 3.4.6. *Es seien R ein K1-Ring und $\mathfrak{m} \leq_R R$ ein Ideal. Dann sind folgende Aussagen äquivalent:*

(i) $\mathfrak{m}$ *ist maximal,*
(ii) $R/\mathfrak{m}$ *ist ein Körper.*

Beweis. Zur Implikation "(i)⇒(ii)". Wegen $\mathfrak{m} \neq R$ sind Einselement und Nullelement in $R/\mathfrak{m}$ verschieden.

Weiter müssen wir zeigen, dass jedes von Null verschiedene Element in $a+\mathfrak{m} \in R/\mathfrak{m}$ eine Einheit ist. Wir betrachten das Ideal

$$\mathfrak{b} \ := \ Ra + \mathfrak{m} \ \leq_R \ R.$$

Wegen $a+\mathfrak{m} \neq 0_{R/\mathfrak{m}}$ gilt $a \notin \mathfrak{m}$ und somit $\mathfrak{m} \subsetneq \mathfrak{b}$. Die Maximalität von $\mathfrak{m}$ impliziert $\mathfrak{b} = R$. Insbesondere erhalten wir eine Darstellung

$$1 \ = \ ca + m \ \in \ R$$

mit einem Element $c \in R$ und einem Element $m \in \mathfrak{m}$. Damit ergibt sich, dass $a+\mathfrak{m}$ eine Einheit in $R/\mathfrak{m}$ ist:

$$(c+\mathfrak{m})(a+\mathfrak{m}) \ = \ ca + \mathfrak{m} \ = \ 1 + \mathfrak{m}.$$

Zur Implikation "(ii)⇒(i)". Wir arbeiten mit dem kanonischen Epimorphismus auf den Faktorring

$$\pi\colon R \ \to \ R/\mathfrak{m}, \qquad a \ \mapsto \ a + \mathfrak{m}.$$

Da Nullelement und Einselement in dem Körper $R/\mathfrak{m}$ voneinander verschieden sind, ist $\mathfrak{m} = \pi^{-1}(0)$ ein echtes Ideal.

Es sei nun $\mathfrak{a} \leq_R R$ ein Ideal mit $\mathfrak{m} \subseteq \mathfrak{a}$. Nach Satz 3.3.11 (ii) ist $\pi(\mathfrak{a})$ ein Ideal in $R/\mathfrak{m}$. Da $R/\mathfrak{m}$ ein Körper ist, lässt Satz 3.3.12 nur folgende Fälle zu:

$$\pi(\mathfrak{a}) \ = \ R/\mathfrak{m} \qquad \text{oder} \qquad \pi(\mathfrak{a}) \ = \ \{0+\mathfrak{m}\}.$$

Im Fall $\pi(\mathfrak{a}) = R/\mathfrak{m}$ gibt es ein $r \in \mathfrak{a}$ mit $\pi(r) = r + \mathfrak{m} = 1 + \mathfrak{m}$. Das bedeutet $1 - r \in \mathfrak{m}$. Wegen $\mathfrak{m} \subseteq \mathfrak{a}$ folgt $1 \in \mathfrak{a}$ und somit $\mathfrak{a} = R$.

Im Fall $\pi(\mathfrak{a}) = \{0+\mathfrak{m}\}$ erhalten wir $\mathfrak{a} \subseteq \pi^{-1}(\pi(\mathfrak{a})) = \pi^{-1}(0+\mathfrak{m}) = \mathfrak{m}$. Das bedeutet $\mathfrak{m} = \mathfrak{a}$. Damit ist die Maximalität von $\mathfrak{m}$ bewiesen. □

Folgerung 3.4.7. *Es sei R ein K1-Ring. Dann ist jedes maximale Ideal in R ein Primideal in R.*

Beispiel 3.4.8. Im Ring $\mathbb{Z}$ der ganzen Zahlen ist $\{0\} \leq_{\mathbb{Z}} \mathbb{Z}$ ein Primideal, aber nicht maximal. Für jedes Ideal $\{0\} \neq \mathfrak{a} \leq_{\mathbb{Z}} \mathbb{Z}$ gilt

$$\begin{aligned} \mathfrak{a} \text{ Primideal} \quad &\iff \quad \mathbb{Z}/\mathfrak{a} \text{ Integritätsring} \\ &\iff \quad \mathbb{Z}/\mathfrak{a} \text{ Körper} \\ &\iff \quad \mathfrak{a} \text{ maximales Ideal.} \end{aligned}$$

Satz 3.4.9. *Jedes echte Ideal $\mathfrak{a} \leq_R R$ eines K1-Ringes R ist in einem maximalen Ideal $\mathfrak{m} \leq_R R$ enthalten.*

Lemma 3.4.10 (Zorn)**.** *Es sei $(M, \leq)$ eine nichtleere teilgeordnete Menge. Besitzt jede Kette, d.h., jede total geordnete Teilmenge $\emptyset \neq M' \subseteq M$ eine obere Schranke in M, so enthält M maximale Elemente.*

Beweis von Satz 3.4.9. Wir betrachten die Menge M aller echten Ideale $\mathfrak{b} \leq_R R$ mit $\mathfrak{a} \subseteq \mathfrak{b}$. Dann ist M teilgeordnet bezüglich "$\subseteq$", und wegen $\mathfrak{a} \in M$ ist M nicht leer. Es sei nun $\emptyset \neq M' \subseteq M$ total geordnet. Wir zeigen, dass

$$\mathfrak{b} := \bigcup_{\mathfrak{b}' \in M'} \mathfrak{b}'$$

eine obere Schranke für M' in M ist. Wegen $\mathfrak{a} \subseteq \mathfrak{b}$ ist $\mathfrak{b}$ nicht leer. Weiter gilt $\mathfrak{b} \neq R$, da wir $1 \notin \mathfrak{b}'$ für alle $\mathfrak{b}' \in M'$ haben. Es bleibt zu verifizieren, dass $\mathfrak{b}$ ein Ideal in R ist. Dazu seien $r \in R$ und $s, s' \in \mathfrak{b}$ gegeben. Dann haben wir

$$s \in \mathfrak{b}' \qquad s' \in \mathfrak{b}''$$

mit geeigneten Idealen $\mathfrak{b}', \mathfrak{b}'' \in M'$. Da M' total geordnet ist, erhalten wir $\mathfrak{b}' \subseteq \mathfrak{b}''$ oder $\mathfrak{b}'' \subseteq \mathfrak{b}'$. Dementsprechend ergibt sich

$$rs, s + s' \in \mathfrak{b}'' \subseteq \mathfrak{b}, \qquad rs, s + s' \in \mathfrak{b}' \subseteq \mathfrak{b}.$$

Damit haben wir $\mathfrak{a} \subseteq \mathfrak{b} \leq_R R$ und $\mathfrak{b}$ ist eine obere Schranke von M' in M. Nach dem Zornschen Lemma 3.4.10 gibt es ein maximales Element $\mathfrak{m} \in M$. Dieses ist offensichtlich das gesuchte maximale Ideal in R mit $\mathfrak{a} \subseteq \mathfrak{m}$. □

Definition 3.4.11. Es sei R ein K1-Ring.

(i) Ein Ideal $\mathfrak{a} \leq_R R$ heißt *Hauptideal*, falls es von einem Element erzeugt wird, d.h., falls es ein $a \in R$ gibt mit $\mathfrak{a} = \langle a \rangle$.
(ii) Man nennt R einen *Hauptidealring*, falls er ein Integritätsring ist und jedes seiner Ideale Hauptideal ist.

Beispiel 3.4.12. (i) $\mathbb{Z}$ ist ein Hauptidealring.
(ii) Jeder Körper ist ein Hauptidealring.

Definition 3.4.13. Ein K1-Ring R heißt *noethersch*, falls jedes Ideal $\mathfrak{a} \leq_R R$ endlich erzeugt ist d.h., falls es $a_1, \ldots, a_n \in R$ gibt mit $\mathfrak{a} = \langle a_1, \ldots, a_n \rangle$.

Bemerkung 3.4.14. Jeder Hauptidealring ist noethersch.

Satz 3.4.15. *Es sei R ein K1-Ring. Dann sind folgende Aussagen äquivalent:*

(i) *Der Ring R ist noethersch.*
(ii) *Jede aufsteigende Kette $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \ldots$ von Idealen $\mathfrak{a}_i \leq_R R$ wird stationär (d.h., es gibt ein $n \in \mathbb{Z}_{\geq 1}$ mit $\mathfrak{a}_i = \mathfrak{a}_n$ für alle $i \geq n$).*

Beweis. Zu "(i) ⇒ (ii)". Es sei eine aufsteigende Kette $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \ldots$ von Idealen in $\mathfrak{a}_i \leq_R R$ gegeben. Dann erhält man ein Ideal

$$\mathfrak{a} := \bigcup_{i \in \mathbb{Z}_{\geq 1}} \mathfrak{a}_i \leq_R R.$$

Nach Voraussetzung ist $\mathfrak{a}$ endlich erzeugt, etwa von Elementen $a_1, \ldots, a_m$. Wir finden dann ein $n \in \mathbb{Z}_{\geq 1}$, sodass alle a_i in $\mathfrak{a}_n$ liegen. Offenbar gilt $\mathfrak{a}_i = \mathfrak{a}_n$ für $i \geq n$.

Zu "(ii) ⇒ (i)". Es sei $\mathfrak{a} \leq_R R$ ein Ideal. Nehmen wir an, $\mathfrak{a}$ sei nicht endlich erzeugt. Dann gilt $\{0\} =: \mathfrak{a}_1 \subsetneq \mathfrak{a}$. Folglich gibt es ein $a_2 \in \mathfrak{a} \setminus \mathfrak{a}_1$. Dann ist $\mathfrak{a}_2 := \langle a_2 \rangle + \mathfrak{a}_1$ endlich erzeugt, und wir haben $\mathfrak{a}_1 \subsetneq \mathfrak{a}_2 \subsetneq \mathfrak{a}$. Auf diese Weise erhält man eine echt aufsteigende Kette von Idealen. Widerspruch zu (ii). □

Satz 3.4.16 (Hilbertscher Basissatz)**.** *Ist R ein noetherscher Ring, so ist der Polynomring $R[T]$ ebenfalls noethersch.*

Beweis. Es seien R ein noetherscher Ring und $\mathfrak{a} \leq_{R[T]} R[T]$ ein Ideal. Zu $i \in \mathbb{Z}_{\geq 0}$ betrachten wir die Menge

$$\mathfrak{a}_i \;:=\; \left\{ a \in R;\ \text{es gibt ein } f \in \mathfrak{a} \text{ mit } f = aT^i + \sum_{\nu=0}^{i-1} a_\nu T^\nu \right\}.$$

Dann ist jedes $\mathfrak{a}_i$ ein Ideal in R, und wir erhalten $\mathfrak{a}_0 \subseteq \mathfrak{a}_1 \subseteq \ldots$. Da R noethersch ist, wird diese Kette stationär. Es gibt also ein $n \in \mathbb{Z}_{\geq 0}$ mit $\mathfrak{a}_i = \mathfrak{a}_n$ für alle $i \geq n$. Jedes Ideal $\mathfrak{a}_i \leq_R R$ ist endlich erzeugt, etwa $\mathfrak{a}_i = \langle a_{i1}, \ldots, a_{is_i} \rangle$ mit $a_{ij} \in R$. Wir wählen Polynome

$$f_{ij} \;=\; a_{ij}T^i + \sum_{\nu=0}^{i-1} a_{ij\nu} T^\nu \;\in\; \mathfrak{a}.$$

Wir behaupten, dass die f_{ij}, wobei $i = 0, \ldots, n$ und jeweils $j = 1, \ldots, s_i$, bereits das Ideal $\mathfrak{a}$ erzeugen. Andernfalls findet man Elemente

$$g \;=\; aT^m + \sum_{\nu=0}^{m-1} a_\nu T^\nu \;\in\; \mathfrak{a} \setminus \langle f_{ij};\ i = 0, \ldots, n,\ j = 1, \ldots, s_i \rangle.$$

Darunter gibt es auch ein g minimalen Grades m. Der Leitkoeffizient a von g liegt in $\mathfrak{a}_m$. Mit $d := \min(m, n)$ erhalten wir eine Darstellung

$$a \;=\; \sum_{j=1}^{s_d} r_j a_{dj}, \qquad r_j \in R, \quad \mathfrak{a}_d = \langle a_{d1}, \ldots, a_{ds_d} \rangle.$$

Nach Wahl der Polynome f_{ij} ist dabei jedes a_{dj} Leitkoeffizient eines Polynoms $f_{dj} \in \mathfrak{a}$ vom Grad $d \leq m$. Gemäß Wahl von g ergibt sich

$$g' \;:=\; g - T^{m-d} \sum_{j=1}^{s_d} r_j f_{dj} \;\in\; \langle f_{ij};\ i = 0, \ldots, n,\ j = 1, \ldots, s_i \rangle,$$

da $\deg(g') < \deg(g)$. Das impliziert jedoch $g \in \langle f_{ij};\ i = 0, \ldots, n, j = 1, \ldots, s_i \rangle$. Widerspruch zur Wahl von g. □

Folgerung 3.4.17. *Es sei R ein K1-Ring. Ist R ein noethersch, so ist auch der Polynomring $R[T_1, \ldots, T_n]$ noethersch.*

Beweis. Wegen $R[T_1, \ldots, T_n] \cong R[T_1, \ldots, T_{n-1}][T]$ kann man die Aussage durch Induktion über n beweisen. □

Folgerung 3.4.18. (i) *$\mathbb{Z}[T_1, \ldots, T_n]$ ist ein noetherscher Ring.*
(ii) *Ist $\mathbb{K}$ ein Körper, so ist $\mathbb{K}[T_1, \ldots, T_n]$ ein noetherscher Ring.*

Lemma 3.4.19. *Es sei $\varphi\colon R \to S$ ein Epimorphismus von Ringen. Ist R noethersch, so ist auch S noethersch.*

Beweis. Es sei $\mathfrak{b} \leq_S S$ ein Ideal. Dann ist $\mathfrak{a} := \varphi^{-1}(\mathfrak{b})$ ein Ideal in R. Da R noethersch ist, gilt $\mathfrak{a} = \langle a_1, \ldots, a_n \rangle$ mit gewissen $a_i \in R$. Es folgt $\mathfrak{b} = \langle b_1, \ldots, b_n \rangle$ mit $b_i := \varphi(a_i)$. □

Folgerung 3.4.20. *Es seien $S \subseteq R$ eine Ringerweiterung und $a_1, \ldots, a_n \in R$. Ist S noethersch, so ist auch $S[a_1, \ldots, a_n]$ noethersch.*

Beweis. Die universelle Eigenschaft des Polynomringes liefert einen Epimorphismus $S[T_1, \ldots, T_n] \to S[a_1, \ldots, a_n]$. Die Behauptung folgt daher mit Lemma 3.4.19. □

Aufgaben zu Abschnitt 3.4.

Aufgabe 3.4.21. Es seien R ein endlicher K1-Ring und $\mathfrak{a} \subseteq R$ ein Ideal. Beweise die folgenden Aussagen:

(i) Ist R ein Integritätsring, so ist R ein Körper.
(ii) Ist $\mathfrak{a} \subseteq R$ Primideal, so ist $\mathfrak{a} \subseteq R$ bereits ein maximales Ideal in R.

Aufgabe 3.4.22. Betrachte den Polynomring $\mathbb{Z}[T]$. Zeige: Das Ideal $\langle T \rangle \subseteq \mathbb{Z}[T]$ ist prim, aber nicht maximal.

Aufgabe 3.4.23. Es sei $\mathbb{K}$ ein Körper. Betrachte den Polynomring $\mathbb{K}[T_1, T_2]$ und beweise folgende Aussagen:

(i) Das Ideal $\langle T_1, T_2 \rangle \subseteq \mathbb{K}[T_1, T_2]$ ist maximal.
(ii) Das Ideal $\langle T_1 \rangle \subseteq \mathbb{K}[T_1, T_2]$ ist prim, aber nicht maximal.

Aufgabe 3.4.24. Es sei R ein Integritätsring. Zeige: Der Potenzreihenring $R[[T_1, \ldots, T_n]]$ besitzt genau ein maximales Ideal, nämlich $\langle T_1, \ldots, T_n \rangle$.

Aufgabe 3.4.25. Es sei R ein K1-Ring. Beweise die Äquivalenz folgender Aussagen:

(i) R ist noethersch.
(ii) Jede nichtleere Menge von Idealen in R besitzt maximale Elemente.

Aufgabe 3.4.26. Zeige: Der Unterring $\mathbb{Q}[T^2, T^3] \subseteq \mathbb{Q}[T]$ ist noethersch, aber er ist kein Hauptidealring.

Aufgabe 3.4.27. Es sei R ein Integritätsring. Zeige, dass $R[T_1, T_2]$ kein Hauptidealring ist. *Hinweis:* Betrachte das Ideal $\langle T_1, T_2 \rangle$ in $R[T_1, T_2]$.

Aufgabe 3.4.28. Es sei $\mathbb{K}$ ein Körper. Die *Nullstellenmenge* eines Polynoms f aus $\mathbb{K}[T_1, \ldots, T_n]$ ist definiert als

$$V(\mathbb{K}^n; f) \quad := \quad \{z \in \mathbb{K}^n;\ f(z) = 0\}.$$

Zeige: Ist f_i, $i \in I$, eine beliebige Familie von Polynomen in $\mathbb{K}[T_1, \ldots, T_n]$, so gibt es (endlich viele) Polynome $g_1, \ldots, g_m \in \mathbb{K}[T_1, \ldots, T_n]$ mit

$$\bigcap_{i \in I} V(\mathbb{K}^n; f_i) \quad = \quad V(\mathbb{K}^n; g_1) \cap \ldots \cap V(\mathbb{K}^n; g_m).$$

4. Teilbarkeitstheorie

4.1. **Teilbarkeit in Integritätsringen.**

Definition 4.1.1. Es seien R ein Integritätsring und $a, b \in R$. Man sagt *a ist ein Teiler von b*, auch *a teilt b*, geschrieben $a \mid b$, falls es ein $r \in R$ gibt mit $b = ra$.

Bemerkung 4.1.2. Es seien R ein Integritätsring und $a \in R$. Dann gilt $a \mid a$ sowie $a \mid 0_R$ und weiter $c \mid a$ für jedes $c \in R^*$, denn man hat

$$a \;=\; 1_R a, \qquad 0_R \;=\; 0_R a, \qquad a \;=\; (ac^{-1})c.$$

Beispiel 4.1.3. Die Teiler von 12 im Ring $\mathbb{Z}$ der ganzen Zahlen sind ± 1, ± 2, ± 3, ± 4, ± 6 und ± 12.

Beispiel 4.1.4. Die Teiler des Polynoms $f := T^2 - 1 \in \mathbb{Q}[T]$ sind genau die Polynome

$$a, \quad b(T-1), \quad c(T+1), \quad d(T^2-1), \qquad \text{wobei } a, b, c, d \in \mathbb{Q}^*.$$

Dazu beachte man, dass $f = gh$ nur für $\deg(g) + \deg(h) = 2$ möglich ist. Die darin enthaltenen Fälle lassen sich dann schnell durchspielen.

Satz 4.1.5. *Es sei R ein Integritätsring, und es seien $a, b \in R$. Dann gilt:*

$$a \mid b \iff b \in \langle a \rangle \iff \langle b \rangle \subseteq \langle a \rangle.$$

Weiter gilt:

$$a \mid b \text{ und } b \mid a \iff \langle a \rangle = \langle b \rangle \iff b = ca \text{ mit einem } c \in R^*.$$

Beweis. Die erste Reihe von Äquivalenzen folgt sofort aus der Definition von $a \mid b$ und $\langle a \rangle = Ra$. In der zweiten Reihe ist lediglich zur Implikation "$\Rightarrow$" der letzten Äquivalenz etwas zu vermerken: Aus $a \in \langle b \rangle$ schliessen wir $a = rb$ mit einem $r \in R$. Aus $b \in \langle a \rangle$ schliessen wir $b = r'a$ mit einem $r' \in R$. Es folgt $a = rb = rr'a$. Da R Integritätsring ist, erhalten wir $rr' = 1_R$ und somit $r' \in R^*$. □

Definition 4.1.6. Es sei R ein Integritätsring. Wir nennen zwei Elemente $a, b \in R$ *assoziiert zueinander*, in Zeichen $a \sim b$, falls $b = ca$ mit einer Einheit $c \in R^*$ gilt.

Beispiel 4.1.7. In dem Ring $\mathbb{Z}$ der ganzen Zahlen gilt genau dann $m \sim n$, wenn man $m = \pm n$ hat.

Beispiel 4.1.8. Es sei $\mathbb{K}$ ein Körper. Zwei Polynome $f, g \in \mathbb{K}[T]$ sind genau dann assoziiert zueinander, wenn $g = af$ mit einem $a \in \mathbb{K}^*$ gilt.

Satz 4.1.9. *Es sei R ein Integritätsring.*

(i) *Durch "$a \sim b$", d.h., a assoziiert zu b, wird eine Äquivalenzrelation auf R definiert.*
(ii) *Für je zwei Elemente $a, b \in R$ gilt $a \sim b$ genau dann, wenn man $a \mid b$ und $b \mid a$ hat.*
(iii) *Gilt $a \sim b$ für zwei $a, b \in R$, so haben a und b dasselbe Teilbarkeitsverhalten, d.h., für jedes $r \in R$ gilt*

$$a \mid r \iff b \mid r, \qquad r \mid a \iff r \mid b.$$

Sind umgekehrt $a, b \in R$ zwei Elemente in R, die dasselbe Teilbarkeitsverhalten in obigem Sinne aufweisen, so gilt $a \sim b$.

Beweis. Aussage (ii) ist bereits in Satz 4.1.5 bewiesen worden. Zu (i). Die Reflexivität von "$\sim$" ist klar mit $a = 1a$. Zur Symmetrie: Gilt $b = ca$ mit $c \in R^*$, so gilt $a = c^{-1}b$. Zur Transitivität: Gelten $b = ca$ und $d = c'b$ mit $c, c' \in R^*$, so hat man $d = c'ca$ und $cc' \in R^*$.

Zu (iii). Sind a und b assoziiert zueinander, etwa $b = ca$ mit $c \in R^*$, so hat man für jedes $r \in R$:

$$a \mid r \iff r = r'a \iff r = r'c^{-1}b \iff b \mid r,$$

$$r \mid a \iff a = a'r \iff b = ca'r \iff r \mid b.$$

Weisen umgekehrt a und b dasselbe Teilbarkeitsverhalten auf, so erhalten wir $a \mid b$ und $b \mid a$ aus $a \mid a$. Satz 4.1.5 liefert dann $a \sim b$. □

Definition 4.1.10. Es seien R ein Integritätsring und $a_1, \ldots, a_n \in R$.

(i) Ein *größter gemeinsamer Teiler* von $a_1, \ldots, a_n$ ist ein $a \in R$ mit
- $a \mid a_i$ für $i = 1, \ldots, n$;
- $a' \mid a_i$ für $i = 1, \ldots, n \Rightarrow a' \mid a$.

(ii) Die Menge aller größten gemeinsamen Teiler von $a_1, \ldots, a_n$ bezeichnen wir mit $\mathrm{ggT}(a_1, \ldots, a_n)$.

(iii) Die Elemente $a_1, \ldots, a_n \in R$ heißen *teilerfremd*, falls $1_R \in \mathrm{ggT}(a_1, \ldots, a_n)$ gilt.

Beispiel 4.1.11. In dem Ring $\mathbb{Z}$ der ganzen Zahlen gilt $\mathrm{ggT}(12, 18) = \{\pm 6\}$.

Bemerkung 4.1.12. Es seien R ein Integritätsring und $a, a_1, \ldots, a_n \in R$ mit $a \in \mathrm{ggT}(a_1, \ldots, a_n)$. Dann gilt

$$\mathrm{ggT}(a_1, \ldots, a_n) \;=\; \{a' \in R;\ a' \sim a\}.$$

Satz 4.1.13. *Es sei R ein Hauptidealring, und es seien $a_1, \ldots, a_n \in R$. Für jedes $a \in R$ gilt:*

$$a \;\in\; \mathrm{ggT}(a_1, \ldots, a_n) \quad\Longleftrightarrow\quad \langle a \rangle \;=\; \langle a_1, \ldots, a_n \rangle.$$

Insbesondere besitzen $a_1, \ldots, a_n \in R$ größte gemeinsame Teiler und jedes Element $a \in \mathrm{ggT}(a_1, \ldots, a_n)$ hat eine "Vielfachsummendarstellung"

$$a \;=\; r_1a_1 + \ldots + r_na_n \text{ mit } r_1, \ldots, r_n \in R.$$

Beweis. Es sei zunächst $a \in \mathrm{ggT}(a_1, \ldots, a_n)$. Dann gilt $a \mid a_i$ und somit $a_i \in \langle a \rangle$. Es folgt $\langle a_1, \ldots, a_n \rangle \subseteq \langle a \rangle$. Da R Hauptidealring ist, gilt weiter $\langle a_1, \ldots, a_n \rangle = \langle b \rangle$ mit einem $b \in R$. Das impliziert $a_i \in \langle b \rangle$ und somit $b \mid a_i$. Wegen $a \in \mathrm{ggT}(a_1, \ldots, a_n)$ erhalten wir $b \mid a$ und somit $\langle a \rangle \subseteq \langle b \rangle = \langle a_1, \ldots, a_n \rangle$.

Es sei nun $\langle a \rangle = \langle a_1, \ldots, a_n \rangle$. Dann gilt $a_i \in \langle a \rangle$ und somit $a \mid a_i$. Ist $a' \in R$ ein weiterer gemeinsamer Teiler von $a_1, \ldots, a_n$, so folgt $a_i \in \langle a' \rangle$. Das impliziert $\langle a_1, \ldots, a_n \rangle \subseteq \langle a' \rangle$, und wir erhalten $a \in \langle a' \rangle$. Folglich gilt $a' \mid a$. Wir haben also $a \in \mathrm{ggT}(a_1, \ldots, a_n)$ nachgewiesen. □

Folgerung 4.1.14. *Es seien R ein Hauptidealring und $a_1, \ldots, a_n \in R$. Die Elemente $a_1, \ldots, a_n$ sind genau dann teilerfremd, wenn man $1_R \in R$ als "Linearkombination" aus ihnen erhält:*

$$1_R \;=\; r_1a_1 + \ldots + r_na_n \quad \text{mit } r_i \in R.$$

Definition 4.1.15. Es sei R ein Integritätsring.

(i) Ein Element $q \in R$ heißt *irreduzibel*, falls gilt:
- $q \neq 0_R$ und $q \notin R^*$,
- $q = ab$ mit $a, b \in R$ impliziert stets $a \in R^*$ oder $b \in R^*$.

(ii) Ein Element $p \in R$ heißt *prim*, falls gilt:
- $p \neq 0_R$ und $p \notin R^*$,
- $p \mid ab$ mit $a, b \in R$ impliziert stets $p \mid a$ oder $p \mid b$.

Bemerkung 4.1.16. Ein Element $0_R \neq q \in R \setminus R^*$ eines Integritätsringes R ist genau dann irreduzibel, wenn es keine "echten" Teiler besitzt, d.h., wenn $a \mid q$ stets $a \in R^*$ oder $a \sim q$ impliziert.

Beispiel 4.1.17. Eine Zahl $p \in \mathbb{Z}_{\geq 1}$ nennt man bekanntlich Primzahl, falls 1 und p die einzigen Teiler von p sind. Nach Bemerkung 4.1.16 sind Primzahlen irreduzible Elemente in $\mathbb{Z}$.

Beispiel 4.1.18. Es sei R ein Integritätsring. Dann ist jedes Polynom der Form $f = T + a \in R[T]$ irreduzibel in $R[T]$. Denn gilt $f = gh$ mit $g, h \in R[T]$, so hat man

$$1 \;=\; \deg(f) \;=\; \deg(g) + \deg(h).$$

Wir dürfen dabei annehmen, dass $\deg(g) = 0$ und $\deg(h) = 1$ gelten. Dann haben wir $g = b$ und $h = cT + d$ mit $b, c, d \in R$. Somit gilt

$$T + a \;=\; b(cT + d) \;=\; bcT + bd.$$

Ein Koeffizientenvergreich liefert $bc = 1$ und somit $b \in R^*$. Das bedeutet $g \in R[T]^*$.

Satz 4.1.19. *Es sei R ein Integritätsring. Dann ist jedes Primelement $p \in R$ irreduzibel.*

Beweis. Wir müssen nur die zweite Bedingung der Irreduzibilität nachprüfen. Dazu sei $p = ab$ mit $a, b \in R$. Da p prim ist, gilt $p \mid a$ oder $p \mid b$. Wir dürfen $p \mid a$ annehmen. Dann haben wir $a = rp$ mit einem $r \in R$. Folglich erhalten wir $p = ab = rpb$. Da $p \neq 0$ gilt und R ein Integritätsring ist, folgt $rb = 1$, d.h., b ist eine Einheit. □

Beispiel 4.1.20. In dem Ring $\mathbb{Z}[I\sqrt{5}] \subseteq \mathbb{C}$ sind die Elemente $3 \in \mathbb{Z}[I\sqrt{5}]$ und $2 \pm I\sqrt{5} \in \mathbb{Z}[I\sqrt{5}]$ jeweils irreduzibel, aber nicht prim.

Satz 4.1.21. *Es seien R ein Integritätsring und $p \in R \setminus \{0\}$. Dann sind folgende Aussagen äquivalent:*

(i) *p ist ein Primelement;*
(ii) *$\langle p \rangle$ ist ein Primideal.*

Beweis. Zur Implikation "(i)⇒(ii)". Zunächst müssen wir zeigen, dass $\langle p \rangle \neq R$ gilt. Andernfalls wäre $1 \in \langle p \rangle$. Wir hätten dann $1 = rp$ mit einem $r \in R$, und p müsste eine Einheit sein; Widerspruch zu p prim. Es seien nun $a, b \in R$ mit $ab \in \langle p \rangle$. Nach Satz 4.1.5 gilt dann $p \mid ab$. Da p prim ist, folgt $p \mid a$ oder $p \mid b$. Satz 4.1.5 liefert dann $a \in \langle p \rangle$ oder $b \in \langle p \rangle$.

Zur Implikation "(ii)⇒(i)". Nach Voraussetzung gilt $p \neq 0$, und wegen $\langle p \rangle \neq R$ kann p keine Einheit sein. Es seien nun $a, b \in R$ mit $p \mid ab$. Nach Satz 4.1.5 bedeutet dies $ab \in \langle p \rangle$. Da $\langle p \rangle$ Primideal ist, muss entweder $a \in \langle p \rangle$ oder $b \in \langle p \rangle$ gelten. Satz 4.1.5 besagt dann $p \mid a$ oder $p \mid b$. □

Satz 4.1.22. *Es seien R ein Integritätsring und $q \in R \setminus \{0\}$. Dann sind folgende Aussagen äquivalent:*

(i) *q ist irreduzibel,*
(ii) *$\langle q \rangle$ ist maximal unter den echten Hauptidealen von R.*

Beweis. Zur Implikation "(i)⇒(ii)". Da q keine Einheit ist, haben wir $\langle q \rangle \neq R$. Für den Nachweis der Maximalitätseigenschaft sei $\langle q \rangle \subseteq \langle a \rangle$ mit einem $a \in R$, sodass $\langle a \rangle \neq R$. Satz 4.1.5 liefert $q = ab$ mit einem $b \in R$. Da q irreduzibel ist, muss b eine Einheit sein (für a kann dies wegen $\langle a \rangle \neq R$ nicht gelten). Es folgt $\langle q \rangle = \langle a \rangle$.

Zur Implikation "(ii)⇒(i)". Da $\langle q \rangle$ ein echtes Ideal ist, gilt $q \notin R^*$. Es sei nun $q = ab$ mit $a, b \in R$. Nach Satz 4.1.5 gilt $\langle q \rangle \subseteq \langle a \rangle$. Mit der Maximalitätseigenschaft von $\langle q \rangle$ erhalten wir $\langle a \rangle = R$ oder $\langle q \rangle = \langle a \rangle$. Im ersten Fall ist a eine Einheit. Satz 4.1.5 liefert für den zweiten Fall, dass $q = ca$ mit einem $c \in R^*$ gilt. Es folgt $ca = ab$ und somit $b = c$, d.h., b ist eine Einheit. □

Folgerung 4.1.23. *Es seien R ein Hauptidealring und $q \in R \setminus \{0\}$. Dann sind folgende Aussagen äquivalent:*

(i) *q ist irreduzibel.*
(ii) *$\langle q \rangle \subseteq R$ ist ein maximales Ideal.*
(iii) *$R/\langle q \rangle$ ist ein Körper.*
(iv) *$R/\langle q \rangle$ ist ein Integritätsring.*
(v) *$\langle q \rangle \subseteq R$ ist ein Primideal.*
(vi) *q ist prim.*

Beweis. Die Implikation "(i)⇒(ii)" ergibt sich aus Satz 4.1.22 und der Voraussetzung, dass R ein Hauptidealring ist. Die Implikation "(ii)⇒(iii)" ist Teil von Satz 3.4.6. Die Implikation "(iii)⇒(iv)" ist offensichtlich. Die Implikation "(iv)⇒(v)" ist Teil von Satz 3.4.3. Die Implikation "(v)⇒(vi)" folgt aus Satz 4.1.21. Die Implikation "(vi)⇒(i)" wurde in Satz 4.1.19 gezeigt. □

Aufgaben zu Abschnitt 4.1.

Aufgabe 4.1.24. Es sei R ein Integritätsring und es seien $a, a_1, \ldots, a_n \in R$ gegeben. Ein *kleinstes gemeinsames Vielfaches* von $a_1, \ldots, a_n$ ist ein Element $b \in R$ mit

- $a_i \mid b$ für $i = 1, \ldots, n$;
- $a_i \mid b'$ für $i = 1, \ldots, n \Rightarrow b \mid b'$.

Die Menge aller kleinsten gemeinsamen Vielfachen von $a_1, \ldots, a_n$ bezeichnen wir mit $\mathrm{kgV}(a_1, \ldots, a_n)$. Beweise folgende Aussagen:

(i) Gilt $b \in \mathrm{kgV}(a_1, \ldots, a_n)$, so hat man $\mathrm{kgV}(a_1, \ldots, a_n) = \{b' \in R;\ b' \sim b\}$.
(ii) Für jedes $a \in R$ gilt $a \in \mathrm{kgV}(a_1, \ldots, a_n) \iff \langle a \rangle = \langle a_1 \rangle \cap \ldots \cap \langle a_n \rangle$.

Aufgabe 4.1.25. Zeige: Der Polynomring $\mathbb{Z}[T]$ ist noethersch, aber er ist kein Hauptidealring. *Hinweis:* Folgerung 4.1.23.

Aufgabe 4.1.26. Beweise die Aussage aus Beispiel 4.1.20: Die Elemente $3 \in \mathbb{Z}[I\sqrt{5}]$ und $2 \pm I\sqrt{5} \in \mathbb{Z}[I\sqrt{5}]$ sind irreduzibel, aber nicht prim.

Aufgabe 4.1.27. Es seien R ein Integritätsring und $f = a_3T^3 + a_2T^2 + a_1T + a_0 \in R[T]$ mit $a_3 \neq 0$. Beweise die Äquivalenz folgender Aussagen:

(i) Das Polynom f ist irreduzibel in $R[T]$.
(ii) Kein Teiler von a_0 ist Nullstelle von f.

4.2. **Euklidische Ringe.**

Beispiel 4.2.1. Wir betrachten den Ring $\mathbb{Z}$ der ganzen Zahlen und den Absolutbetrag

$$\mathbb{Z} \;\mapsto\; \mathbb{Z}_{\geq 0}, \qquad a \;\mapsto\; |a|.$$

Für je zwei ganze Zahlen $a, b \in \mathbb{Z}$ mit $b \neq 0$ liefert die Division mit Rest eine Darstellung

$$a \;=\; qb + r, \qquad \text{mit } q, r \in \mathbb{Z},\ |r| < |b|.$$

Definition 4.2.2. Ein *euklidischer Ring* ist ein Integritätsring R zusammen mit einer Abbildung

$$\delta\colon R \setminus \{0\} \;\to\; \mathbb{Z}_{\geq 0},$$

sodass zu $a, b \in R$ mit $b \neq 0$ stets $q, r \in R$ existieren mit

$$a \;=\; qb + r, \qquad \delta(r) < \delta(b) \text{ oder } r = 0.$$

Man nennt $\delta\colon R \setminus \{0\} \to \mathbb{Z}_{\geq 0}$ dann eine *Gradabbildung* auf R und die Darstellung $a = qb + r$ nennt man eine *Division mit Rest* in R.

Satz 4.2.3. *Der Ring $\mathbb{Z}[I] \subseteq \mathbb{C}$ der ganzen Gaußschen Zahlen ist zusammen mit $\delta(m + in) := m^2 + n^2$ ein euklidischer Ring.*

Beweis. Es seien $a, b \in \mathbb{Z}[I]$ mit $b \neq 0$. Um die benötigte Darstellung $a = qb + r$ zu erhalten, betrachten wir zunächst die komplexe Zahl

$$ab^{-1} \;=\; u + Iv \;\in\; \mathbb{C}, \quad \text{wobei } u, v \in \mathbb{R}$$

und wählen $s, t \in \mathbb{Z}$ mit $|u - s| \leq 1/2$ sowie $|v - t| \leq 1/2$. Dann setzen wir $q := s + It$ und erhalten $a = qb + r$ mit $r := a - qb = b(ab^{-1} - q)$. Es folgt

$$\delta(r) \;=\; \delta(b)\delta(ab^{-1} - q) \;=\; \delta(b)\left((u - s)^2 + (v - t)^2\right) \;\leq\; \frac{\delta(b)}{2} \;<\; \delta(b).$$

□

Satz 4.2.4. *Es seien $\mathbb{K}$ ein Körper und $f, g \in \mathbb{K}[T]$ Polynome mit* $\deg(g) \geq 0$. *Dann besitzt f eine Darstellung*

$$f \;=\; qg + r, \qquad q, r \in \mathbb{K}[T], \quad \deg(r) < \deg(g).$$

Insbesondere ist der Polynomring $\mathbb{K}[T]$ zusammen mit der Abbildung $f \mapsto \deg(f)$ ein euklidischer Ring.

Beweis. Es seien $m := \deg(f)$ und $n := \deg(g)$. Wir beweisen die Existenz einer der Darstellung durch Induktion über m. Es gilt

$$f \;=\; \sum_{\mu=0}^{m} a_\mu T^\mu, \qquad g \;=\; \sum_{\nu=0}^{n} b_\nu T^\nu.$$

Der Fall $m = 0$ ist einfach: Falls $n \geq 1$ gilt kommt man mit $q := 0$ und $r := f$ durch; falls $\deg(g) = 0$ gilt kommt man mit $q := f/g$ und $r = 0$ durch.

Kommen wir zum Induktionsschritt. Der Fall $m < n$ ist trivial; hier ist $f = 0g + f$ die gewünschte Darstellung. Für den Fall $m \geq n$ betrachten wir das Polynom

$$f' \;:=\; f - \frac{a_m}{b_n} T^{m-n} g.$$

Darauf können wir die Induktionsvoraussetzung anwenden, und erhalten eine Darstellung

$$f - \frac{a_m}{b_n} T^{m-n} g \;=\; f' \;=\; q'g + r'$$

mit $\deg(r') < \deg(g)$. Indem man $a_m/b_n T^{m-n} g$ auf die rechte Seite bringt, erhält man die gewünschte Darstellung:

$$f \;=\; \left(\frac{a_m}{b_n} T^{m-n} + q' \right) g + r'.$$

□

Folgerung 4.2.5. *Es seien $\mathbb{K}$ ein Körper, $f \in \mathbb{K}[T]$ und $a \in \mathbb{K}$. Gilt $f(a) = 0$, so hat man $f = (T-a)g$ mit einem Polynom $g \in \mathbb{K}[T]$.*

Beweis. Nach Satz 4.2.4 hat man eine Darstellung $f = (T-a)g + b$ mit $b \in \mathbb{K}$. Wegen $f(a) = 0$ muss $b = 0$ gelten. □

Bemerkung 4.2.6 (Polynomdivision)**.** Es seien $\mathbb{K}$ ein Körper und $f, g \in \mathbb{K}[T]$ mit $g \neq 0_{\mathbb{K}[T]}$. Weiter seien $m := \deg(g)$ und $b \in \mathbb{K}$ der Leitkoeffizient von g.

Das folgende Verfahren ermöglicht es, eine Darstellung $f = qg + r$ wie in Satz 4.2.4 explizit zu bestimmen.

- Schritt 0. Setze $q_0 := 0$ und $f_0 := f$. Falls $n_0 := \deg(f_0) < \deg(g)$: Abbrechen mit $q := q_0$ und $r := f_0$.
- Schritt 1. Es sei a_0 der Leitkoeffizient von f_0. Bestimme die Polynome

  $$q_1 \;:=\; \frac{a_0}{b} T^{n_0 - m}, \qquad f_1 \;:=\; f_0 - q_1 g.$$

  Falls $n_1 := \deg(f_1) < \deg(g)$: Abbrechen mit $q := q_0 + q_1$ und $r := f_1$.

  $$\vdots$$

- Schritt k. Es sei a_{k-1} der Leitkoeffizient von f_{k-1}. Bestimme die Polynome

  $$q_k \;:=\; \frac{a_{k-1}}{b} T^{n_{k-1} - m}, \qquad f_k \;:=\; f_{k-1} - q_k g.$$

  Falls $n_k := \deg(f_k) < \deg(g)$: Abbrechen mit $q := q_0 + \ldots + q_k$ und $r := f_k$.

  $$\vdots$$

Da der Grad von f_k in jedem Schritt echt veringert wird, bricht das Verfahren bei irgendeinem $k = n$ ab. Dann hat man

$$\begin{aligned} f_{n-1} &= q_n g + r, \\ f_{n-2} &= f_{n-1} + q_{n-1} g = (q_{n-1} + q_n) g + r \\ &\vdots \\ f = f_0 &= (q_0 + q_1 + \ldots + q_n) g + r = qg + r. \end{aligned}$$

Beispiel 4.2.7. Für die Polynome $f = T^3 + 2T + 1$ und $g = T - 1$ aus $\mathbb{Q}[T]$ erhält man die Darstellung $f = qg + r$ mittels Polynomdivision wie folgt:

$$\begin{aligned}
\underbrace{T^3 + 2T + 1}_{f_0 = f} &= (\underbrace{T - 1}_{g}) \cdot (\underbrace{\underbrace{T^2}_{q_1} + \underbrace{T}_{q_2} + \underbrace{3}_{q_3}}_{q}) + \underbrace{4}_{r} \\
&\quad -(\underbrace{T^3 - T^2}_{q_1 g}) \\
&= \underbrace{T^2 + 2T + 1}_{f_1 = f_0 - q_1 g} \\
&\quad -(\underbrace{T^2 - T}_{q_2 g}) \\
&= \underbrace{3T + 1}_{f_2 = f_1 - q_2 g} \\
&\quad -(\underbrace{3T - 3}_{q_3 g}) \\
&= \underbrace{4}_{r = f_3 = f_2 - q_3 g}
\end{aligned}$$

Satz 4.2.8. *Jeder euklidische Ring ist ein Hauptidealring.*

Beweis. Es sei R ein euklidischer Ring mit Gradabbildung δ. Zu einem gegebenen Ideal $\langle 0 \rangle \neq \mathfrak{a} \subseteq R$ betrachten wir ein Element $0 \neq b \in \mathfrak{a}$ mit minimalem Grad $\delta(b)$. Wir zeigen $\mathfrak{a} = \langle b \rangle$. Ist $a \in \mathfrak{a}$ ein beliebiges Element, so haben wir eine Darstellung

$$a = qb + r, \qquad \text{wobei } \delta(r) < \delta(b) \text{ oder } r = 0.$$

Man beachte, dass dabei $r = a - qb \in \mathfrak{a}$ gilt. Da b minimalen Grad unter den Elementen von $\mathfrak{a}$ besitzt, muss $r = 0$ gelten. Folglich erhalten wir $a = qb$. Mit anderen Worten, es gilt $a \in \langle b \rangle$. □

Folgerung 4.2.9. *Die Ringe $\mathbb{Z}$ und $\mathbb{Z}[I]$ sind Hauptidealringe. Weiter ist für jeden Körper $\mathbb{K}$ der Polynomring $\mathbb{K}[T]$ ein Hauptidealring.*

Satz 4.2.10. *Es sei R ein K1-Ring. Dann sind folgende Aussagen äquivalent:*

(i) *R ist ein Körper.*
(ii) *$(R[T], \deg)$ ist ein euklidischer Ring.*
(iii) *$R[T]$ ist ein Hauptidealring.*

Beweis. Nur zur Implikation "(iii)⇒(i)" ist noch etwas zu zeigen. Wegen $\deg(T) = 1$ ist T irreduzibel in $R[T]$. Nach Folgerung 4.1.23 ist $R \cong R[T]/\langle T \rangle$ ein Körper. □

Konstruktion 4.2.11 (Euklidischer Algorithmus)**.** Es sei R ein euklidischer Ring mit Gradabbildung δ, und es seien $a, b \in R$, wobei $b \neq 0$.

- *Schritt 0.* Setze $c_{-1} := a$ und $c_0 := b$.
- *Schritt 1.* Wähle $c_1, q_1 \in R$ mit

  $$c_{-1} = q_1 c_0 + c_1, \qquad \text{wobei } \delta(c_1) < \delta(c_0) \text{ oder } c_1 = 0.$$

  Falls $c_1 = 0$: Verfahren abbrechen.

- *Schritt 2.* Wähle $c_2, q_2 \in R$ mit

  $$c_0 \;=\; q_2 c_1 + c_2, \qquad \text{wobei } \delta(c_2) < \delta(c_1) \text{ oder } c_2 = 0.$$

  Falls $c_2 = 0$: Verfahren abbrechen.

$$\vdots$$

- *Schritt n.* Wähle $c_n, q_n \in R$ mit

  $$c_{n-2} \;=\; q_n c_{n-1} + c_n, \qquad \text{wobei } \delta(c_n) < \delta(c_{n-1}) \text{ oder } c_n = 0.$$

  Falls $c_n = 0$: Verfahren abbrechen.

$$\vdots$$

Das Verfahren bricht bei einem $n \in \mathbb{Z}_{>0}$ mit $c_n = 0$ ab. Dabei ist c_{n-1} ein größter gemeinsamer Teiler von a und b, und man erhält eine Darstellung

$$c_{n-1} \;=\; ua + vb, \qquad \text{mit } u, v \in R.$$

Beweis. Da im euklidischen Algorithmus $\delta(c_{i+1}) < \delta(c_i)$ für jedes $i \geq 0$ gilt, muss das Verfahren irgendwann mit $c_n = 0$ abbrechen. Um zu sehen, dass c_{n-1} dann ein gemeinsamer Teiler von a und b ist, betrachten wir das Schema

$$\begin{array}{rcrcl}
 & & c_{n-2} & = & q_n c_{n-1} \\
 & & c_{n-3} & = & q_{n-1} c_{n-2} + c_{n-1} \\
 & & c_{n-4} & = & q_{n-2} c_{n-3} + c_{n-2} \\
 & & \vdots & & \\
 & & c_1 & = & q_3 c_2 - c_3 \\
b & = & c_0 & = & q_2 c_1 + c_2 \\
a & = & c_{-1} & = & q_1 c_0 + c_1
\end{array}$$

Indem wir Darstellung von c_{n-2} in die von c_{n-3} einsetzen, sehen wir, dass c_{n-3} ein Vielfaches von c_{n-1} ist. Es folgt, dass c_{n-4} Vielfaches von c_{n-1} ist, usw., und schließlich sieht man, das b und a Vielfache von c_{n-1} sind.

Um zu sehen, das jeder gemeinsame Teiler c von a und b auch ein Teiler von c_{n-1} ist, schreiben wir das obige Schema um, indem wir in jeder Gleichung nach dem c_i mit dem größten i auflösen:

$$\begin{array}{rcl}
c_{n-1} & = & c_{n-3} - q_{n-1} c_{n-2} \\
c_{n-2} & = & c_{n-4} - q_{n-2} c_{n-3} \\
c_{n-3} & = & c_{n-5} - q_{n-3} c_{n-4} \\
 & \vdots & \\
c_2 & = & c_0 - q_2 c_1 \\
c_1 & = & c_{-1} - q_1 c_0 \\
 & = & a - q_1 b.
\end{array}$$

Die unterste Gleichung liefert, dass mit a und b auch c_1 ein Vielfaches von c ist. Geht man eine Gleichung höher, so erhält man, dass c_2 Vielfaches von c ist usw..

Weiter liefert die oberste Gleichung, dass man c_{n-1} linear aus c_{n-3} und c_{n-2} kombinieren kann. Entsprechend liefert die zweite Gleichung, dass man c_{n-2} linear aus c_{n-3} und c_{n-4} kombinieren kann. Durch sukzessives Einsetzen erhält man so eine Darstellung $c_{n-1} = ua + vb$. □

Beispiel 4.2.12. Wir führen den euklidischen Algorithmus in $\mathbb{Z}$ mit $a := 60$ und $b := 42$ durch. Er bricht im dritten Schritt ab:

$$60 \;=\; 1 \cdot 42 + 18, \qquad 42 \;=\; 2 \cdot 18 + 6, \qquad 18 \;=\; 3 \cdot 6$$

Folglich ist 6 ein größter gemeinsamer Teiler von 60 und 42. Weiter erhalten wir die Vielfachsummendarstellung

$$6 \;=\; 42 - 2 \cdot 18 \;=\; 42 - 2 \cdot (60 - 42) \;=\; 2 \cdot 60 - 3 \cdot 42.$$

Aufgaben zu Abschnitt 4.2.

Aufgabe 4.2.13. Es sei R ein euklidischer Ring mit Graddabbildung $\delta\colon R\setminus\{0\}\to\mathbb{Z}_{\geq 0}$, sodass $\delta(u)\leq\delta(uv)$ für je zwei $u,v\in R\setminus\{0\}$ gilt. Beweise folgende Aussagen:

(i) Ein Element $c\in R\setminus\{0\}$ ist genau dann eine Einheit in R, wenn $\delta(c)=\delta(1_R)$ gilt.
(ii) Ein gemeinsamer Teiler $c\in R\setminus\{0\}$ von $a,b\in R\setminus\{0\}$ ist genau dann ein größter gemeinsamer Teiler von a,b, wenn $\delta(d)\leq\delta(c)$ für jeden weiteren gemeinsamen Teiler $d\in R\setminus\{0\}$ von a,b gilt.

Aufgabe 4.2.14. Es seien $\mathbb{K}$ ein Körper und $f,g\in\mathbb{K}[T]$ Polynome, wobei $g\neq 0$. Zeige: In der Darstellung $f=qg+r$ aus Satz 4.2.4 sind die Polynome q und r eindeutig bestimmt.

Aufgabe 4.2.15. Finde eine explizite Darstellung $f=qg+r$ mit $\deg(r)\leq\deg(g)$ in $\mathbb{Q}[T]$ für die Polynome

$$f\ :=\ 3T^5-6T^4+19T^3-25T^2+15T-8,\qquad g\ :=\ T^3+5T+1.$$

Aufgabe 4.2.16. Bestimme mittels euklidischem Algorithmus einen größten gemeinsamen Teiler für die Polynome

$$f\ :=\ 6T^5-15T^4+13T^3-3T^2-6T+4,\qquad g\ :=\ 3T^4-3T^3+2T^2+T-1.$$

Aufgabe 4.2.17. Es seien $p\in\mathbb{Z}$ eine Primzahl und $c\in\mathbb{Z}$ mit $\mathrm{ggT}(p,c)=1$, sodass $cp=m^2+n^2$ mit ganzen Zahlen m,n gilt. Zeige:

(i) $p=p+I\cdot 0$ ist kein Primelement in dem Ring $\mathbb{Z}[I]$ der ganzen Gaußschen Zahlen.
(ii) Es gibt ganze Zahlen a,b mit $p=a^2+b^2$.

Aufgabe 4.2.18. Es sei $p\in\mathbb{Z}_{\geq}1$ eine Primzahl. Zeige:

(i) Es gilt $(p-1)!\ \equiv\ -1\mod p$. *Hinweis:* Betrachte das entsprechende Produkt in dem Körper $\mathbb{Z}/p\mathbb{Z}$.
(ii) Gilt $p=4m+1$ mit $m\in\mathbb{Z}_{\geq 0}$, so gibt es ein $c\in\mathbb{Z}$ mit $c^2\equiv -1\mod p$. *Hinweis:* Betrachte $c:=(2m)!$.

Aufgabe 4.2.19. Es sei $p\in\mathbb{Z}$ eine Primzahl der Form $p=4m+1$ mit einem $m\in\mathbb{Z}$. Zeige: Es gibt ganze Zahlen a,b mit $p=a^2+b^2$. *Hinweis:* Es gibt ein $x\in\mathbb{Z}$ mit $|x|\leq p/2$, sodas $x^2\equiv -1\mod p$ gilt; verwende Aufgaben 4.2.18 und 4.2.17.

4.3. **Primfaktorzerlegung.**

Bemerkung 4.3.1. Der Hauptsatz der elementaren Zahlentheorie besagt, dass man jede natürliche Zahl n auf eindeutige Weise zerlegen kann als

$$n \quad = \quad p_1^{\nu_1} \cdots p_r^{\nu_r}$$

mit Primzahlen $p_1 < \ldots < p_r$; beispielsweise $60 = 2^2 \cdot 3 \cdot 5$. Wir werden diesen Satz als Folgerung allgemeinerer Überlegungen erhalten.

Definition 4.3.2. Einen Integritätsring R nennt man *faktoriell*, falls jedes $a \in R$ mit $0_R \neq a \notin R^*$ eine Zerlegung $a = p_1 \cdots p_n$ mit Primelementen $p_1, \ldots, p_n \in R$ besitzt.

Satz 4.3.3. *Es seien R ein faktorieller Ring und $p \in R$. Dann sind folgende Aussagen äquivalent:*

(i) *p ist prim.*
(ii) *p ist irreduzibel.*

Beweis. Die Implikation "(i)⇒(ii)" gilt nach Satz 4.1.19 in jedem Integritätsring. Zur Implikation "(ii)⇒(i)". Es sei $p = p_1 \cdots p_n$ eine Zerlegung mit $p_i \in R$ prim. Gilt $n = 1$, so ist $p = p_1$ prim. Für $n \geq 2$ muss $p_2 \cdots p_n$ wegen der Irreduzibilität von p eine Einheit sein; dieser Fall tritt also nicht ein. □

Beispiel 4.3.4. Der Integritätsring $\mathbb{Z}[I\sqrt{5}] \subseteq \mathbb{C}$ ist nicht faktoriell, da z.B. die Elemente 3 sowie $2 \pm I\sqrt{5}$ irreduzibel aber nicht prim sind; siehe Aufgabe 4.1.20.

Satz 4.3.5. *Jeder Hauptidealring ist ein faktorieller Ring.*

Lemma 4.3.6. *Es seien R ein Hauptidealring und $0 \neq a_0 \in R \setminus R^*$. Dann gibt es eine Darstellung $a_0 = a_1 p_1$ mit Element $0 \neq a_1 \in R$ und einem Primelement $p_1 \in R$. Dabei gilt $\langle a_0 \rangle \subsetneq \langle a_1 \rangle$.*

Beweis. Nach Satz 3.4.9 gilt $\langle a_0 \rangle \subseteq \mathfrak{m}$ mit einem maximalen Ideal $\mathfrak{m} \subseteq R$. Da R ein Hauptidealring ist, haben wir $\mathfrak{m} = \langle p_1 \rangle$ mit einem Element $p_1 \in R$. Als maximales Ideal ist $\langle p_1 \rangle$ prim, siehe Satz 3.4.7. Nach Satz 4.1.21 ist p_1 prim. Wir erhalten $a_0 = a_1 p_1$ mit $0 \neq a_1 \in R$. Es bleibt $\langle a_0 \rangle \subsetneq \langle a_1 \rangle$ zu zeigen. Andernfalls hätten wir $\langle a_0 \rangle = \langle a_1 \rangle$ und folglich $a_1 = c a_0 = c a_1 p_1$ mit einem $c \in R$ was $p_1 \in R^*$ impliziert; Widerspruch. □

Beweis von Satz 4.3.5. Es sei $0 \neq a_0 \in R \setminus R^*$ gegeben. Nach Lemma 4.3.6 gilt $a_0 = a_1 p_1$ mit $0 \neq a_1 \in R$ und einem Primelement $p_1 \in R$, sodass $\langle a_0 \rangle \subsetneq \langle a_1 \rangle$ gilt. Falls $a_1 \notin R^*$ gilt, liefert Lemma 4.3.6 eine Zerlegung $a_1 = a_2 p_2$ mit $a_2, p_2 \in R$, wobei p_2 prim und wir haben

$$a_0 \;=\; a_1 p_1 \;= a_2 p_2 p_1, \qquad\qquad \langle a_0 \rangle \;\subsetneq\; \langle a_1 \rangle \;\subsetneq\; \langle a_2 \rangle.$$

Jetzt betrachten wir a_2 usw.. Da R ein Hauptidealring ist, muss dieser Prozess irgendwann abbrechen, d.h., es muss $a_n \in R^*$ für ein $n \in \mathbb{Z}_{\geq 0}$ gelten; siehe Satz 3.4.15. Dann ist $a_n p_n$ ein Primelement und $a = a_n p_n p_{n-1} \cdots p_1$ ist die gesuchte Zerlegung. □

Folgerung 4.3.7. *Die Ring $\mathbb{Z}$ und $\mathbb{Z}[I]$ sind faktoriell. Weiter ist für jeden Körper $\mathbb{K}$ der Polynomring $\mathbb{K}[T]$ faktoriell.*

Definition 4.3.8. Es sei R ein Integritätsring. Unter einem *Primsystem* für R verstehen wir eine Teilmenge $P \subset R$ von Primelementen, sodass folgendes gilt:

(i) Ist $q \in R$ ein Primelement, so gilt $q \sim p$ mit einem $p \in P$.
(ii) Sind zwei verschiedene $p, p' \in P$ gegeben, so gilt $p \not\sim p'$.

Bemerkung 4.3.9. Ein Primsystem $P \subset R$ ist ein Repräsentantensystem für die Assoziiertheit "$\sim$" auf der Menge aller Primelemente von R.

Beispiel 4.3.10. Die Primzahlen $2, 3, 5, 7, \ldots$ bilden ein Primsystem in dem Ring $\mathbb{Z}$ der ganzen Zahlen.

Satz 4.3.11. *Es seien R ein faktorieller Ring und $P \subset R$ Primsystem. Dann besitzt jedes $a \in R \setminus \{0_R\}$ eine eindeutige Primfaktorzerlegung bezüglich P, d.h., eine Darstellung*

$$a \quad = \quad c \prod_{p \in P} p^{\nu_p(a)}$$

mit einer eindeutig bestimmten Einheit $c \in R^*$ und eindeutig bestimmten "Vielfachheiten" $\nu_p(a) \in \mathbb{Z}_{\geq 0}$, von denen höchstens endlich viele von Null verschieden sind.

Lemma 4.3.12. *Es sei R ein Integritätsring. Sind $p, q_1, \ldots, q_k \in R$ Primelemente mit $p \mid q_1 \cdots q_k$, so gilt bereits $p \sim q_i$ für ein i.*

Beweis. Wir beweisen die Aussage durch Induktion über k. Zum Fall $k = 1$. Wegen $p \mid q_1$ haben wir $q_1 = cp$ mit einem $c \in R$. Als Primelement ist q_1 nach Satz 4.1.19 irreduzibel. Folglich muß c eine Einheit sein. Das bedeutet $p \sim q_1$. Zum Induktionsschritt. Gilt $p \mid q_1 \cdots q_k$, so gilt $p \mid q_1 \cdots q_{k-1}$ oder $p \mid q_k$, da p prim ist. Folglich liefert die Induktionsvoraussetzung $p \sim q_i$ für ein i. □

Beweis von Satz 4.3.11. Da R faktoriell ist, haben wir $a = q_1 \cdots q_l$ mit Primelementen $q_j \in R$. Jedes q_i ist assoziiert zu einem $p_i \in P$; wir haben also $q_i = c_i p_i$ mit $c_i \in R^*$. Zusammenfassen gleicher p_i ergibt die gewünschte Darstellung für a mit $c := c_1 \cdots c_l$.

Es bleibt die Eindeutigkeit der Primfaktorzerlegung nachzuweisen. Dazu vergleichen wir zwei Darstellungen

$$c \prod_{p \in P} p^{\nu_p} \quad = \quad c' \prod_{p \in P} p^{\mu_p}.$$

Wir betrachten $k := \sum \nu_p$ und $l := \sum \mu_p$ und zeigen durch Induktion über k, dass $c = c'$ sowie $\nu_p(a) = \mu_p(a)$ für alle $p \in P$ gelten.

Gilt $k = 0$, so hat man $\nu_p = 0$ für alle $p \in P$ und auf der linken Seite steht eine Einheit. Folglich muss auch auf der rechten Seite eine Einheit stehen, was $\mu_p = 0$ für alle $p \in P$ und $c = c'$ impliziert.

Gilt $k > 0$, so muss auch $l > 0$ gelten. Weiter hat man $\nu_{p_0} \neq 0$ für ein $p_0 \in P$. Nach Lemma 4.3.12 findet man auf der rechten Seite ein $q_0 \in P$ mit $q_0 \sim p_0$. Da P ein Primsystem ist, folgt $p_0 = q_0$, d.h., wir haben $\mu_{p_0} > 0$. Kürzt man durch p_0, so liefert die Induktionsvoraussetzung $c = c'$ sowie $\nu_p = \mu_p$ für alle $p \in P$. □

Beispiel 4.3.13. Bezüglich des Primsystems $P = \{2, 3, 5, 7, \ldots\}$ ist die Primfaktorzerlegung von $-360 \in \mathbb{Z}$ gegeben durch

$$-360 \quad = \quad -1 \cdot 2^3 \cdot 3^2 \cdot 5.$$

Weiter erhält man den *Hauptsatz der elementaren Zahlentheorie*: Jede natürliche Zahl n kann auf eindeutige Weise zerlegen als

$$n \quad = \quad p_1^{\nu_1} \cdots p_r^{\nu_r} \quad \text{mit Primzahlen } p_1 < \ldots < p_r.$$

Bemerkung 4.3.14. Es seien R ein faktorieller Ring, $P \subset R$ ein Primsystem, $a_1, \ldots, a_n \in R$ und

$$a_i \quad = \quad c_i \prod_{p \in P} p^{\nu_p(a_i)}.$$

die zugehörigen Primfaktorzerlegungen mit Einheiten $c_i \in R^*$ und Vielfachheiten $\nu_p(a_i) \in \mathbb{Z}_{\geq 0}$. Die Teilbarkeit $a_i \mid a_j$ wird charakterisiert durch

$$a_i \mid a_j \quad \Longleftrightarrow \quad \nu_p(a_i) \leq \nu_p(a_j) \text{ für alle } p \in P.$$

Weiter kann man einen größten gemeinsamen Teiler für die Elemente $a_1, \ldots, a_n$ angeben, nämlich

$$\prod_{p \in P} p^{\min(\nu_p(a_i))} \quad \in \quad \mathrm{ggT}(a_1, \ldots, a_n),$$

Satz 4.3.15. *Es seien R ein Hauptidealring und $a \in R$ von der Form $a = cp_1^{\nu_1} \cdots p_n^{\nu_n}$, wobei $c \in R^*$ gelte und die p_i paarweise nichtassoziierte Primelemente seien. Dann erhält man einen Isomorphismus von Ringen*

$$R/\langle a \rangle \quad \cong \quad R/\langle p_1^{\nu_1} \rangle \ \times \ \ldots \ \times \ R/\langle p_n^{\nu_n} \rangle.$$

Beweis. Es genügt, den Fall $c = 1$ zu behandeln. Wir zeigen zunächst, dass die Elemente $p_i^{\nu_i}$ und $p_j^{\nu_j}$ für $i \neq j$ teilerfremd sind.

Ist $d \in R$ ein gemeinsamer Teiler von $p_i^{\nu_i}$ und $p_j^{\nu_j}$, so hat man $p_i^{\nu_i} = bd$. Da p_i prim ist, muss $p_i \mid b$ oder $p_i \mid d$ gelten. Der Fall $p_i \mid d$ scheidet aus, da wir dann $p_i \mid p_j^{\nu_j}$ erhielten, was nach Lemma 4.3.12 nicht möglich ist. Also gilt $p_i \mid b$. Es folgt $p_i^{\nu_i - 1} = b'd$ mit einem $b' \in R$. Wiederholen des obigen Arguments liefert schließlich $d \mid p_i$. Analog verifiziert man $d \mid p_j$. Mit $p_i \not\sim p_j$ ergibt sich $d \in R^*$.

Die Teilerfremdheit der Elemente $p_i^{\nu_i}$ und $p_j^{\nu_j}$ können wir nach Satz 4.1.13 idealtheoretisch ausdrücken: Es gilt

$$\langle p_i^{\nu_i} \rangle + \langle p_j^{\nu_j} \rangle \ = \ \langle p_i^{\nu_i}, p_j^{\nu_j} \rangle \ = \ \langle 1_R \rangle \ = \ R.$$

Damit können wir den Chinesischen Restsatz 3.3.19 ins Spiel bringen; er liefert im vorliegenden Fall einen Isomorphismus von Ringen

$$R/\left(\langle p_1^{\nu_1} \rangle \ \cap \ \ldots \ \cap \ \langle p_n^{\nu_n} \rangle\right) \quad = \quad R/\langle p_1^{\nu_1} \rangle \ \times \ \ldots \ \times \ R/\langle p_n^{\nu_n} \rangle.$$

Zum Beweis der Aussage müssen wir also nur noch die folgende Identität von Idealen nachzuweisen:

$$\langle p_1^{\nu_1} \ldots p_n^{\nu_n} \rangle \quad = \quad \langle p_1^{\nu_1} \rangle \ \cap \ \ldots \ \cap \ \langle p_n^{\nu_n} \rangle.$$

Die Inklusion "$\subseteq$" ist dabei offensichtlich. Die Inklusion "$\supseteq$" ergibt sich wie folgt. Liegt $b \in R$ in der rechten Seite, so erhält man $b = b_1 p_1^{\nu_1}$ mit einem $b_1 \in R$. Wegen $p_2^{\nu_2} \mid b$ und $p_2 \nmid p_1^{\nu_1}$ erhält man $p_2^{\nu_1} \mid b_1$ also $b = p_1^{\nu_1} p_2^{\nu_2} b_2$ mit einem $b_2 \in R$, siehe Lemma 4.3.12. Auf diese Weise gelangt man schliesslich zu $p_1^{\nu_1} \cdots p_n^{\nu_n} \mid b$, also $b \in \langle p_1^{\nu_1} \cdots p_n^{\nu_n} \rangle$. □

Bemerkung 4.3.16. Es sei $n \in \mathbb{Z}_{\geq 1}$, und es sei $n = p_1^{\nu_1} \ldots p_r^{\nu_r}$ die zugehörige Primfaktorzerlegung. Satz 4.3.15 liefert einen Isomorphismus von K1-Ringen

$$\mathbb{Z}/n\mathbb{Z} \quad \cong \quad \mathbb{Z}/\langle p_1^{\nu_1} \rangle \ \times \ \ldots \ \times \ \mathbb{Z}/\langle p_r^{\nu_r} \rangle.$$

Dieser ist insbesondere ein Isomorphismus der zu Grunde liegenden abelschen Gruppen. Weiter erhält man für die Einheitengruppen

$$\begin{aligned}(\mathbb{Z}/n\mathbb{Z})^* &\cong (\mathbb{Z}/\langle p_1^{\nu_1}\rangle \times \ldots \times \mathbb{Z}/\langle p_r^{\nu_r}\rangle)^* \\ &\cong (\mathbb{Z}/\langle p_1^{\nu_1}\rangle)^* \times \ldots \times (\mathbb{Z}/\langle p_r^{\nu_r}\rangle)^*.\end{aligned}$$

Definition 4.3.17. Die *Eulersche ϕ-Funktion* ordnet jeder Zahl $n \in \mathbb{Z}_{\geq 1}$ die Anzahl $\phi(n)$ der zu n teilerfremden ganzen Zahlen m mit $1 \leq m \leq n$ zu:

$$\phi(n) := |\{m \in \mathbb{Z}_{\geq 1};\ m \leq n,\ 1 \in \mathrm{ggT}(m,n)\}|.$$

Satz 4.3.18. *Für $n \in \mathbb{Z}_{\geq 2}$ sei $n = p_1^{\nu_1} \cdots p_r^{\nu_r}$ eine Darstellung mit paarweise verschiedenen Primzahlen $p_1, \ldots, p_r$ gegeben. Dann gilt*

$$\phi(n) \ = \ \phi(p_1^{\nu_1}) \cdots \Phi(p_r^{\nu_r}) \ = \ n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right).$$

Beweis. Wir betrachten zunächst den Fall $n = p^\nu$ mit einer Primzahl p. Die ganzen Zahlen zwischen 1 und p^l, die einen gemeinsamen Teiler mit p^l sind Vielfache von p, d.h., möglich sind dabei

$$1,\ p, 2p,\ \ldots,\ p^{\nu-1}p$$

Damit erhalten wir $\phi(p^\nu) = p^\nu - p^{\nu-1}$. Für den allgemeinen Fall vermerken wir zunächst, dass $\phi(n) = |\mathbb{Z}/n\mathbb{Z}^*|$ gilt, da $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ genau dann Einheit ist, wenn $\mathrm{ggT}(a,n) = 1$ gilt. Mit Bemerkung 4.3.16 ergibt sich

$$\begin{aligned}\phi(n) &= \Phi(p_1^{\nu_1}) \cdots \Phi(p_r^{\nu_r}) \\ &= (p_1^{\nu_1} - p_1^{\nu_1 - 1}) \cdots (p_r^{\nu_r} - p_r^{\nu_r - 1}) \\ &= n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right).\end{aligned}$$

□

Aufgaben zu Abschnitt 4.3.

Aufgabe 4.3.19. Beweise folgende Aussagen. Die Familie $(T-a;\ a\in\mathbb{C})$ ist ein Primsystem in dem Polynomring $\mathbb{C}[T]$. Jedes nichtkonstante $f\in\mathbb{C}[T]$ lässt sich eindeutig schreiben als

$$f \quad = \quad c\prod_{a\in\mathbb{C}}(T-a)^{\nu_a(f)},$$

wobei $c\in\mathbb{C}^*$. Die Vielfachheit $\nu_a(f)$ des Primfaktors $T-a$ in f ist dabei genau die Ordnung der Nullstelle a von f. *Hinweis:* Es darf verwendet werden, dass jedes nichtkonstante $f\in\mathbb{C}[T]$ in Linearfaktoren zerfällt.

Aufgabe 4.3.20. Zeige: Die folgenden Polynome bilden ein Primsystem in dem Polynomring $\mathbb{R}[T]$:

$$T-a,\ \text{wobei } a\in\mathbb{R}, \qquad T^2+bT+c,\ \text{wobei } b,c\in\mathbb{R},\ b^2<4c.$$

Aufgabe 4.3.21. Zeige: Der Polynomring $\mathbb{Q}[T]$ besitzt irreduzible Polynome beliebig hohen Grades.

Aufgabe 4.3.22. Beweise Bemerkung 4.3.14.

Aufgabe 4.3.23. Zeige: Der Ring $\mathbb{Z}[\sqrt{d}]$ ist euklidisch für $d=\pm2$ und für $d=3$. Zeige weiter, dass $\mathbb{Z}[\sqrt{d}]$ für $d=-3$ nicht euklidisch ist.

Aufgabe 4.3.24. Es seien $m,n\in\mathbb{Z}_{\geq1}$. Betrachte die Eulersche ϕ-Funktion und beweise die Äquivalenz folgender Aussagen:

(i) Die Zahlen m und n sind teilerfremd.
(ii) Es gilt $m^{\phi(n)}\equiv 1 \mod n$.

4.4. **Der Satz von Gauß.**

Satz 4.4.1 (Gauß)**.** *Es sei R ein faktorieller Ring. Dann ist auch der Polynomring $R[T]$ faktoriell.*

Folgerung 4.4.2. *Es sei R ein faktorieller Ring. Dann ist auch $R[T_1, \dots, T_n]$ ein faktorieller Ring.*

Folgerung 4.4.3. *Der Ring $\mathbb{Z}[T_1, \dots, T_n]$ ist ein faktoriell. Weiter ist $\mathbb{K}[T_1, \dots, T_n]$ faktoriell für jeden Körper $\mathbb{K}$.*

Erinnerung 4.4.4. Es seien R ein Integritätsring und $Q(R)$ sein Quotientenkörper. Dann ist der Polynomring $Q(R)[T]$ nach Folgerung 4.3.7 faktoriell. Weiter gibt es ein kommutatives Diagramm

$$\begin{array}{ccc} R & \xrightarrow{a \mapsto aT^0} & R[T] \\ {\scriptstyle a \mapsto \frac{a}{1}}\downarrow & & \downarrow{\scriptstyle \sum a_i T^i \mapsto \sum \frac{a_i}{1} T^i} \\ Q(R) & \xrightarrow[\frac{a}{b} \mapsto \frac{a}{b} T^0]{} & Q(R)[T] \end{array}$$

von kanonischen Monomorphismen. Dies erlaubt es uns, R als Unterring von $Q(R)$ bzw. $R[T]$ aufzufassen, und weiter $Q(R)$ sowie $R[T]$ als Unterringe von $Q(R)[T]$ aufzufassen.

Satz 4.4.5. *Es seien R ein Integritätsring und $p \in R$ ein beliebiges Element. Dann gilt:*

$$p \text{ prim in } R \quad \Longleftrightarrow \quad p \text{ prim in } R[T].$$

Lemma 4.4.6. *Es seien R ein K1-Ring und $p \in R$. Dann hat man ein kommutatives Diagramm*

$$\begin{array}{ccc} & R[T] & \\ {\scriptstyle \pi\colon \sum a_i T^i \mapsto (\sum a_i T^i) + \langle pT^0 \rangle}\swarrow & & \searrow{\scriptstyle \kappa\colon \sum a_i T^i \mapsto \sum (a_i + \langle p \rangle) T^i} \\ R[T]/\langle pT^0 \rangle & \xrightarrow[(\sum a_i T^i) + \langle pT^0 \rangle \mapsto \sum (a_i + \langle p \rangle) T^i]{} & (R/\langle p \rangle)[T] \end{array}$$

von wohldefinierten Ringhomomorphismen; dabei ist $R[T]/\langle pT^0 \rangle \to (R/\langle p \rangle)[T]$ ein Isomorphismus.

Beweis. Bei $\pi\colon R[T] \to R[T]/\langle pT^0 \rangle$ handelt es sich um den Restklassenepimorphismus. Der Homomorphismus $\kappa\colon R[T] \to (R/\langle p \rangle)[T]$ existiert nach der universellen Eigenschaft des Polynomrings; er ist die Fortsetzung der Komposition

$$R \xrightarrow{r \mapsto r + \langle p \rangle} R/\langle p \rangle \xrightarrow{r + \langle p \rangle \mapsto (r + \langle p \rangle) T^0} (R/\langle p \rangle)[T]$$

auf $R[T]$ mit $T \mapsto T$; siehe Satz 3.2.6. Offensichtlich ist κ surjektiv. Nach dem Homomorphiesatz 3.3.16 genügt es deshalb zu zeigen, dass $\operatorname{Kern}(\kappa) = \operatorname{Kern}(\pi)$ gilt. Das ergibt sich wie folgt:

$$\begin{aligned} \kappa\left(\sum a_i T^i\right) = 0 \quad &\Longleftrightarrow \quad a_i \in \langle p \rangle \text{ für alle } i \\ &\Longleftrightarrow \quad p \mid a_i \text{ für alle } i \\ &\Longleftrightarrow \quad pT^0 \mid \sum a_i T^i \\ &\Longleftrightarrow \quad \sum a_i T^i \in \langle pT^0 \rangle \\ &\Longleftrightarrow \quad \pi\left(\sum a_i T^i\right) = 0. \end{aligned}$$

□

Beweis von Satz 4.4.5. Im Falle $p = 0$ ist nichts zu zeigen; wir dürfen daher $p \neq 0$ annehmen. Die Aussage ergibt sich dann direkt aus $R[T]/\langle p\rangle \cong (R/\langle p\rangle)[T]$ und den Äquivalenzen 4.1.21, 3.4.3 und 3.2.13: Es gilt

$$\begin{aligned} p \text{ prim in } R &\iff \langle p\rangle \leq_R R \text{ Primideal} \\ &\iff R/\langle p\rangle \text{ Integritätsring} \\ &\iff (R/\langle p\rangle)[T] \text{ Integritätsring} \\ &\iff R[T]/\langle p\rangle \text{ Integritätsring} \\ &\iff \langle p\rangle \leq_{R[T]} R[T] \text{ Primideal} \\ &\iff p \text{ prim in } R[T]. \end{aligned}$$

□

Satz 4.4.7. *Es seien R ein faktorieller Ring und $P \subset R$ ein Primsystem. Dann besitzt jedes $q \in Q(R)^*$ eine eindeutige Darstellung*

$$q \;=\; c \prod_{p \in P} p^{\nu_p(q)}$$

mit einer Einheit $c \in R^*$ und "Vielfachheiten" $\nu_p(q) \in \mathbb{Z}$, wobei $\nu_p(q) \neq 0$ für höchstens endlich viele $p \in P$. Es gilt

$$\nu_p(qq') \;=\; \nu_p(q) + \nu_p(q')$$

für je zwei Elemente $q, q' \in Q(R)^*$ und alle $p \in P$. Für jedes $q \in Q(R)^*$ haben wir weiter

$$\begin{aligned} q \in R &\iff \nu_p(q) \geq 0 \text{ für alle } p \in P. \\ q \in R^* &\iff \nu_p(q) = 0 \text{ für alle } p \in P. \end{aligned}$$

Beweis. Um die Existenz der obigen Darstellung von $q \in Q(R)$ nachzuweisen, wählen wir $a, b \in R \setminus \{0\}$ mit $q = a/b$. Da R faktoriell ist, liefert uns Satz 4.3.11 Darstellungen

$$a \;=\; c_a \prod_{p \in P} p^{\nu_p(a)}, \qquad\qquad b \;=\; c_b \prod_{p \in P} p^{\nu_p(b)}$$

mit $c_a, c_b \in R^*$ und $\nu_p(a), \nu_p(b) \in \mathbb{Z}_{\geq 0}$ von denen höchstens endlich viele nicht verschwinden. Dividiert man die linke durch die rechte Gleichung, so erhält man die gewünschte Darstellung für q.

Um die Eindeutigkeit der Darstellung nachzuweisen, vergleichen wir zwei dieser Darstellungen:

$$c \prod_{p \in P} p^{\nu_p} \;=\; d \prod_{p \in P} p^{\mu_p}.$$

Indem man beide Seiten mit dem Hauptnenner multipliziert, erhält man eine Identität mit nichtnegativen Exponenten

$$c \prod_{p \in P} p^{\nu'_p} \;=\; d \prod_{p \in P} p^{\mu'_p}.$$

Wegen der Eindeutigkeit der Primfaktorzerlegung folgt dann $\nu'_p = \mu'_p$ für alle $p \in P$ und somit auch $c = d$. Ersteres liefert $\nu_p = \mu_p$ für alle $p \in P$. □

Definition 4.4.8. Es seien R ein faktorieller Ring, $P \subset R$ ein Primsystem und $p \in P$. Weiter sei

$$f \;=\; \sum a_i T^i \;\in\; Q(R)[T].$$

Mit den Vielfachheiten $\nu_p(a_i)$ aus Satz 4.4.7 für $a_i \neq 0$ und $\nu_p(0) := \infty$ definiert man

$$\nu_p(f) \;:=\; \min(\nu_p(a_i);\; i \in \mathbb{Z}_{\geq 0}).$$

Beispiel 4.4.9. Wir betrachten $\mathbb{Z}$ mit dem Primsystem $P = \{2, 3, 5, 7, 11, \ldots\}$. Es gilt $\mathbb{Q} = Q(\mathbb{Z})$ und in dem zugehörigen Polynomring $\mathbb{Q}[T]$ haben wir

$$\nu_3\left(\frac{1}{3}T^2 + 3T + 2\right) \;=\; -1.$$

Bemerkung 4.4.10. Es seien R ein faktorieller Ring, $P \subset R$ ein Primsystem und $f = \sum_{i=0}^{n} a_i T^i \in Q(R)[T]$.

(i) Man hat genau dann $f = 0$, wenn $\nu_p(f) = \infty$ für alle $p \in P$ gilt.
(ii) Man hat genau dann $f \in R[T]$, wenn $\nu_p(f) \geq 0$ für alle $p \in P$ gilt.
(iii) Gilt $0 \leq \nu_p(f) < \infty$ für alle $p \in P$, so hat man

$$\prod_{p \in P} p^{\nu_p(f)} \quad\in\quad \mathrm{ggT}(a_0, \ldots, a_n).$$

Definition 4.4.11. Es sei R ein faktorieller Ring. Man nennt nichttriviales Polynom $\sum_{i=0}^{n} a_i T^i \in R[T]$ *primitiv*, falls seine Koeffizienten $a_0, \ldots, a_n$ teilerfremd sind, d.h., falls $1 \in \mathrm{ggT}(a_0, \ldots, a_n)$ gilt.

Beispiel 4.4.12. Das Polynom $12T^2 - 35T \in \mathbb{Z}[T]$ ist primitiv, das Polynom $35T + 7 \in \mathbb{Z}[T]$ hingegen nicht.

Lemma 4.4.13. *Es seien R ein faktorieller Ring und $P \subset R$ ein Primsystem.*

(i) *Ein Polynom $f \in R[T]$ ist genau dann primitiv, wenn $\nu_p(f) = 0$ für alle $p \in P$ gilt.*
(ii) *Zu jedem $0 \neq f \in Q(R)[T]$. Dann gibt es ein $c \in Q(R)$, sodass cf ein primitives Polynom in $R[T]$ ist.*

Beweis. Aussage (i) ergibt sich direkt aus Bemerkung 4.4.10 (iii). Für den Nachweis von (ii) schreiben wir $f = \sum a_i/b_i T^i$, mit $a_i, b_i \in R$. Mit $b := \prod b_i$ gilt dann $bf \in R[T]$. Ist $a \in R$ ein größter gemeinsamer Teiler der Koeffizienten von bf, so ist $c := b/a$ das gesuchte Element. □

Satz 4.4.14 (Lemma von Gauß)**.** *Es seien R ein faktorieller Ring, $P \subset R$ ein Primsystem und $f, g \in Q(R)[T]$. Dann gilt für jedes $p \in P$:*

$$\nu_p(fg) \;=\; \nu_p(f) + \nu_p(g).$$

Beweis. Es seien zunächst $f, g \in R[T]$ primitiv. Dann gilt $\nu_p(f) = \nu_p(g) = 0$ und es ist $\nu_p(fg) = 0$ zu zeigen. Dazu betrachten wir den Homomorphismus

$$\kappa\colon R[T] \;\to\; (R/\langle p\rangle)[T], \qquad \sum a_i T^i \;\mapsto\; \sum (a_i + \langle p\rangle) T^i.$$

Der Kern von κ besteht genau aus denjenigen Polynomen, für die alle Koeffizienten durch p teilbar sind:

$$\mathrm{Kern}(\kappa) \;=\; \left\{\sum a_i T^i \in R[T];\; p \mid a_i \text{ für alle } i\right\} \;=\; \{h \in R[T];\; \nu_p(h) > 0\}.$$

Wir müssen also $\kappa(fg) \neq 0$ zeigen. Lemma 4.4.13 liefert $\kappa(f) \neq 0 \neq \kappa(g)$. Da mit $R/\langle p\rangle$ auch $(R/\langle p\rangle)[T]$ ein Integritätsring ist, ergibt sich $\kappa(fg) = \kappa(f)\kappa(g) \neq 0$.

Wir behandeln nun den Fall $f \in Q(R)^*$ und $0 \neq g = \sum b_j T^j \in Q(R)[T]$. Für jedes Element $p \in P$ erhalten wir

$$\nu_p(fg) = \min(\nu_p(fb_j);\ j \in \mathbb{Z}_{\geq 0}) = \min(\nu_p(f) + \nu_p(b_j);\ j \in \mathbb{Z}_{\geq 0}) = \nu_p(f) + \nu_p(g).$$

Für $f = 0$ oder $g = 0$ ist nichts zu zeigen. Für $f, g \in Q(R)[T] \setminus \{0\}$ gibt es $c, d \in Q(R)^*$, sodass cf und dg primitiv sind; siehe Lemma 4.4.13. Dabei gilt stets

$$0 \ = \ \nu_p(cf) \ = \ \nu_p(c) + \nu_p(f) \ = \ -\nu_p(c^-1) + \nu_p(f)$$

Es folgt $\nu_p(f) = \nu_p(c^{-1})$. Analog erhalten wir $\nu_p(g) = \nu_p(d^{-1})$ für alle $p \in P$. Damit ergibt sich:

$$\begin{array}{rclcrcl} \nu_p(fg) & = & \nu_p((cd)^{-1}(cfdg)) & = & \nu_p((cd)^{-1}) + \nu_p((cf)(dg)) & = & \nu_p((cd)^{-1}) \\ & = & \nu_p(c^{-1}) + \nu_p(d^{-1}) & = & \nu_p(f) + \nu_p(g). & & \end{array}$$

□

Folgerung 4.4.15. *Es seien R ein faktorieller Ring und $q, f \in R[T]$, wobei q primitiv. Gilt $q \mid f$ in $Q(R)[T]$, so gilt bereits $q \mid f$ in $R[T]$.*

Beweis. Es sei $P \subset R$ ein Primsystem. Gilt $q \mid f$ in $Q(R)[T]$, so gibt es ein Polynom $h \in Q(R)[T]$ mit $f = qh$. Es folgt

$$0 \ \leq \ \nu_p(f) \ = \ \nu_p(qh) \ = \ \nu_p(q) + \nu_p(h) \ = \ \nu_p(h)$$

für jedes Element $p \in P$; siehe Satz 4.4.14. Das bedeutet $h \in R[T]$. Mit anderen Worten: Es gilt $q \mid f$ in $R[T]$. □

Folgerung 4.4.16. *Es seien R ein faktorieller Ring und $q \in R[T]$ ein primitives Polynom. Dann gilt*

$$q \text{ prim in } R[T] \quad \Longleftrightarrow \quad q \text{ prim in } Q(R)[T].$$

Beweis. Für den Fall $\deg(q) = 0$ ist die Aussage richtig, da die primitiven Polynome in $R[T]$ vom Grad 0 nach Lemma 4.4.13 (i) genau die Einheiten von R sind. Wir dürfen also $\deg(q) \geq 1$ annehmen.

Es sei zunächst q prim in $Q(R)[T]$. Sind $f, g \in R[T]$ mit $q \mid fg$ in $R[T]$ gegeben, so gilt auch $q \mid fg$ in $Q(R)[T]$. Foglich gilt $q \mid f$ oder $q \mid g$ in $Q(R)[T]$. Nach Folgerung 4.4.15 gilt dann $q \mid f$ oder $q \mid g$ in $R[T]$.

Es sei nun q prim in in $R[T]$. Sind $f, g \in Q(R)[T]$ mit $q \mid fg$ in $Q(R)[T]$ gegeben, so wählen wir Elemente $c_f, c_g \in R$, sodass $f' := c_f f$ und $g' := c_g g$ in $R[T]$ liegen. Dann haben wir $q \mid f'g'$ in $Q(R)[T]$. Nach Folgerung 4.4.15 gilt $q \mid f'g'$ in $R[T]$. Da q prim in $R[T]$ ist, folgt $q \mid f'$ oder $q \mid g'$ in $R[T]$. Mit $f = c_f^{-1} f'$ und $g = c_g^{-1} g'$ erhalten wir $q \mid f$ in $Q(R)[T]$. □

Beweis des Satzes von Gauß 4.4.1. Wir behandeln zunächst den Fall, dass $f \in R[T]$ primitiv ist. Nach Folgerung 4.3.7 ist $Q(R)[T]$ faktoriell. Somit gibt es eine Darstellung

$$f \ = \ c \prod_{i=1}^{n} f_i$$

mit $c \in Q(R)^* = Q(R)[T]^*$ und Primelementen $f_i \in Q(R)[T]$. Durch geeignete Wahl von c erreichen wir, dass $f_i \in R[T]$ gilt und jedes f_i primitiv ist. Ist $P \subseteq R$ ein Primsystem, so folgt mit Lemma 4.4.14

$$\nu_p(f) \ = \ \nu_p(c) + \nu_p(f_1) + \ldots + \nu_p(f_n).$$

für jedes $p \in P$. Wegen $\nu_p(f_1) = \ldots = \nu_p(f_n) = 0$ ergibt sich $\nu_p(c) = 0$. Es folgt $c \in R^*$. Nach Folgerung 4.4.16 ist jedes f_i prim in $R[T]$. Damit haben f als Produkt von Primelementen aus $R[T]$ dargestellt.

Im allgemeinen Fall schreibe man $f = af'$ mit $a \in R$ und $f' \in R[T]$ primitiv. Es sei $a = a_1 \cdots a_m$ mit Primelementen $a_i \in R$. Nach Satz 4.4.5 sind die a_i auch prim in $R[T]$. Weiter besitzt das primitive Polynom f' in $R[T]$ nach obiger Überlegung eine Darstellung $f' = f'_1 \cdots f'_n$ mit Primelementen $f'_i \in R[T]$. Die gesuchte Darstellung von f als Produkt von Primelementen in $R[T]$ ist dann

$$f \quad = \quad a_1 \cdots a_m \cdot f'_1 \cdots f'_n.$$

□

Aufgaben zu Abschnitt 4.4.

Aufgabe 4.4.17. Es sei R ein Integritätsring, und es seien Elemente $a_1, \ldots, a_n \in R$ sowie $b_1, \ldots, b_m \in R$ gegeben. Zeige: Ist $p \in R$ ein Primelement mit

$$p \mid \sum_{i+j=k} a_i b_j, \qquad \text{für } k = 0, 1, \ldots, m+n,$$

so gilt $p \mid a_i$ für $i = 1, \ldots, n$ oder $p \mid b_j$ für $j = 1, \ldots, m$. *Hinweis:* Arbeite in dem Polynomring $R[T]$.

Aufgabe 4.4.18. Es seien R ein faktorieller Ring und $f, g \in Q(R)[T]$. Beweise folgende Aussagen:

(i) Sind f und g primitiv, so ist auch fg primitiv.
(ii) Gilt $fg \in R[T]$ und ist g primitiv, so gilt $f \in R[T]$.

Aufgabe 4.4.19. Es seien $a, b, c, d \in \mathbb{Z}_{\geq 1}$ mit $1 \in \mathrm{ggT}(a, b)$ und $1 \in \mathrm{ggT}(c, d)$. Zeige: Es gilt $1 \in \mathrm{ggT}(ac, bd, ad + bc)$.

Aufgabe 4.4.20. Es sei R ein K1-Ring. Zeige: Ist der Polynomring $R[T]$ faktoriell, so ist auch R faktoriell.

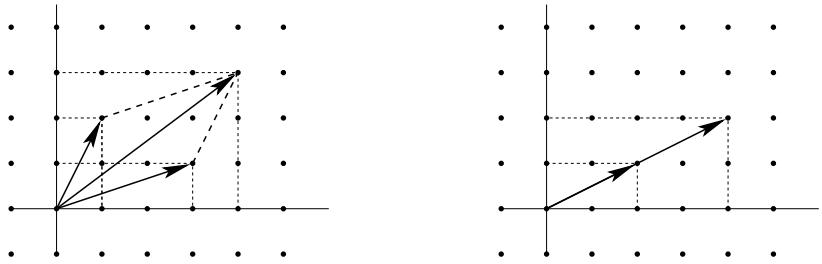
Aufgabe 4.4.21. Es sei R ein faktorieller Ring. Zeige: Der Polynomring $R[T_1, \ldots, T_n]$ besitzt unendlich viele Primelemente.

Aufgabe 4.4.22. Es seien R ein faktorieller Ring, $f \in R[T]$ und $p \in R$ prim. Beweise das *Reduktionskriterium*: Gilt $p \nmid a_f$ für den Leitkoeffizienten von $a_f \in R$ von f und ist das Bild von f in $(R/\langle p \rangle)[T]$ irreduzibel, so ist f irreduzibel in $Q(R)[T]$.

5. Moduln

5.1. **Grundbegriffe.**

Beispiel 5.1.1. Die Teilmenge $\mathbb{Z}^2 \subseteq \mathbb{R}^2$ ist eine Untergruppe der additiven Gruppe $\mathbb{R}^2$, und wir haben Skalarmultiplikation mit ganzen Zahlen auf $\mathbb{Z}^2$:



Definition 5.1.2. Es sei R ein K1-Ring. Ein *(unitärer) R-Modul* ist eine abelsche Gruppe $(M,+)$ zusammen mit einer Abbildung

$$R \times M \;\to\; M, \qquad (r,u) \;\mapsto\; r \cdot u,$$

genannt *Skalarmultiplikation*, sodass für $r, r' \in R$ und $u, u' \in M$ stets folgendes gilt:

$$1_R \cdot u \;=\; u, \quad (r'r)\cdot u \;=\; r'\cdot(r\cdot u), \quad (r'+r)\cdot u \;=\; r'\cdot u + r\cdot u, \quad r\cdot(u+u') \;=\; r\cdot u + r\cdot u'.$$

Bemerkung 5.1.3. Der Begriff des Moduls verallgemeinert den Begriff des Vektorraumes: Die Moduln über einem Körper $\mathbb{K}$ sind genau die Vektorräume über $\mathbb{K}$.

Beispiel 5.1.4. Es sei R ein K1-Ring. Dann wird die Menge R^n zu einem R-Modul durch komponentenweise Addition und komponentenweise Skalarmultiplikation

$$\begin{aligned} (r_1,\ldots,r_n) \;+\; (s_1,\ldots,s_n) \;&:=\; (r_1+s_1,\ldots,r_n+s_n), \\ a\cdot(r_1,\ldots,r_n) \;&:=\; (ar_1,\ldots,ar_n). \end{aligned}$$

Konstruktion 5.1.5. Jede abelsche Gruppe $(G,+)$ ist auf kanonische Weise ein $\mathbb{Z}$-Modul: Man definiert eine Skalarmultiplikation $\mathbb{Z} \times G \to G$ durch

$$n \cdot g \;:=\; ng \;=\; \begin{cases} \underbrace{g+\ldots+g}_{n\text{-mal}} & \text{falls } n>0, \\ 0 & \text{falls } n=0, \\ \underbrace{-g-\ldots-g}_{|n|\text{-mal}} & \text{falls } n<0. \end{cases}$$

Definition 5.1.6. Es seien R ein K1-Ring, M ein R-Modul, und $N \subseteq M$ eine nichtleere Teilmenge mit

$$v, v' \in N \;\implies\; v+v' \in N, \qquad v \in N, r \in R \;\implies\; r\cdot v \;\in\; N.$$

Dann nennen wir N zusammen mit der induzierten Verknüpfungen $(v,v') \mapsto v+v'$ sowie $(r,v) \mapsto r\cdot v$ einen *(R-)Untermodul von M*; wir schreiben dafür auch $N \leq_R M$.

Bemerkung 5.1.7. Es seien R ein K1-Ring, M ein R-Modul und $N \leq_R M$ ein Untermodul. Dann ist N eine Untergruppe der additiven Gruppe M und N ist bezüglich der induzierten Verknüpfungen wieder ein R-Modul.

Bemerkung 5.1.8. Es sei G eine abelsche Gruppe. Dann ist G ein $\mathbb{Z}$-Modul gemäß 5.1.5. Die $\mathbb{Z}$-Untermoduln von G sind genau die Untergruppen von G.

Bemerkung 5.1.9. Es sei R ein K1-Ring. Dann wird $(R,+)$ ein R-Modul durch $r \cdot u := ru$. Die R-Untermoduln von R sind genau die Ideale des Ringes R.

Definition 5.1.10. Es seien R ein K1-Ring, M ein R-Modul und $\mathcal{F} = (u_i)_{i\in I}$ eine Familie in M, wobei $I \neq \emptyset$. Eine *(R-)Linearkombination über* $\mathcal{F}$ ist ein Element der Form

$$\sum_{i\in I} a_i \cdot u_i \ \in \ M, \qquad \text{wobei } a_i \in R,\ a_i \neq 0_R \text{ für höchstens endlich viele } i \in I.$$

Konstruktion 5.1.11. Es seien R ein K1-Ring, M ein R-Modul und $\mathcal{F} = (u_i)_{i\in I}$ eine Familie in M, wobei $I \neq \emptyset$.

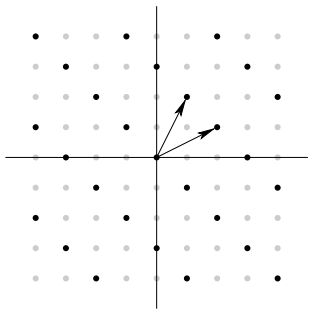
Der von $\mathcal{F}$ *erzeugte Untermodul* (auch die *lineare Hülle*, das *Erzeugnis*, der *Aufspann*) von $\mathcal{F}$ in M ist definiert

$$\operatorname{Lin}(\mathcal{F}) \ := \ \{u \in M;\ u \text{ ist Linearkombination über } \mathcal{F}\} \ \leq_R \ M.$$

Der Vollständigkeit halber definieren wir die lineare Hülle der leeren Familie durch $\operatorname{Lin}(\,) := \{0_M\}$. Für eine Teilmenge $A \subseteq M$ setzt man auch

$$\langle A\rangle \ := \ \operatorname{Lin}(A) \ := \ \operatorname{Lin}((u)_{u\in A}) \ \leq_R \ M.$$

Beispiel 5.1.12. Für den von $v_1 := (2,1)$ und $v_2 := (1,2)$ erzeugten Untermodul $\operatorname{Lin}(v_1, v_2)$ in $\mathbb{Z}^2$ erhält man folgendes Bild;



Konstruktion 5.1.13. Es seien R ein K1-Ring, M ein R-Modul und $N_i \leq_R M$, $i \in I$, Untermoduln. Dann ist die *Summe* dieser Untermoduln der Untermodul

$$\sum_{i\in I} N_i \ := \ \left\langle \bigcup_{i\in I} N_i \right\rangle \ = \ \left\{\sum u_i;\ u_i \in N_i\right\} \ \leq_R \ M.$$

Definition 5.1.14. Es sei R ein K1-Ring. Ein *Homomorphismus* (auch *lineare Abbildung*) von R-Moduln M und N ist eine Abbildung $\varphi\colon M \to N$, sodass stets gilt

$$\varphi(u + u') \ = \ \varphi(u) + \varphi(u'), \qquad \varphi(r \cdot u) \ = \ r \cdot \varphi(u).$$

Man nennt einen Modulhomomorphismus $\varphi\colon M \to N$ einen *Monomorphismus*, falls er injektiv ist, *Epimorphismus*, falls er surjektiv ist, *Isomorphismus*, falls es einen Modulhomomorphismus $\psi\colon N \to M$ gibt mit

$$\psi \circ \varphi \ = \ \mathrm{id}_M, \qquad \varphi \circ \psi \ = \ \mathrm{id}_N;$$

man nennt die Moduln M und N dann isomorph zueinander und schreibt dafür $M \cong N$. Weiter definiert man *Kern* und *Bild* eines beliebigen Modulhomomorphismus $\varphi\colon M \to N$ als

$$\operatorname{Kern}(\varphi) \ := \ \{u \in M;\ \varphi(u) = 0\}, \qquad \operatorname{Bild}(\varphi) \ := \ \{\varphi(u);\ u \in M\}.$$

Bemerkung 5.1.15. Es seien R ein K1-Ring, und $\varphi\colon M \to N$ sowie $\psi\colon N \to K$ Homomorphismen von R-Moduln. Dann ist auch $\psi \circ \varphi\colon M \to K$ ein Homomorphismus.

Bemerkung 5.1.16. Es seien G und H abelsche Gruppen.

(i) Eine Abbildung $\varphi\colon G \to H$ ist genau dann ein Homomorphismus der $\mathbb{Z}$-Moduln G und H, wenn sie ein Gruppenhomomorphismus ist.
(ii) G und H sind genau dann isomorph als $\mathbb{Z}$-Moduln, wenn sie als Gruppen isomorph sind.

Bemerkung 5.1.17. Es seien R ein K1-Ring und $\varphi\colon M \to N$ ein Homomorphismus von R-Moduln.

(i) Für jeden Untermodul $M' \leq_R M$ ist das Bild $\varphi(M')$ ein Untermodul von N; insbesondere ist Bild(φ) ein Untermodul von N.
(ii) Für jeden Untermodul $N' \leq_R N$ ist das Urbild $\varphi^{-1}(N')$ ein Untermodul von M; insbesondere ist Kern(φ) ein Untermodul von M.
(iii) Der Homomorphismus $\varphi\colon M \to N$ ist genau dann injektiv, wenn Kern(φ) $= \{0\}$ gilt.
(iv) Der Homomorphismus $\varphi\colon M \to N$ ist genau dann ein Isomorphismus, wenn er bijektiv ist.

Konstruktion 5.1.18. Es seien R ein K1-Ring und M_i, $i \in I$, eine Familie von R-Moduln und

$$\prod_{i\in I} M_i \quad := \quad \{(u_i)_{i\in I};\ u_i \in M_i\}$$

das (mengentheoretische) direkte Produkt. Dann ist $\prod_{i\in I} M_i$ zusammen mit den komponentenweisen Verknüpfungen

$$\begin{aligned}(u_i)_{i\in I} \ + \ (u_i')_{i\in I} \quad &:= \quad (u_i + u_i')_{i\in I},\\ r \cdot (u_i)_{i\in I} \quad &:= \quad (r \cdot u_i)_{i\in I}\end{aligned}$$

ein R-Modul, das *direkte Produkt* der R-Moduln M_i, $i \in I$. Die *direkte Summe* der R-Moduln M_i, $i \in I$, ist der Untermodul

$$\begin{aligned}\bigoplus_{i\in I} M_i \quad &:= \quad \left\{(u_i)_{i\in I} \in \prod_{i\in I} M_i;\ u_i \neq 0 \text{ für höchstens endlich viele } i \in I\right\}\\ &\leq_R \quad \prod_{i\in I} M_i.\end{aligned}$$

Die Projektionen auf die Faktoren liefern kanonische surjektive Modulhomomorphismen

$$\pi_j\colon \prod_{i\in I} M_i \to M_j, \quad (u_i)_{i\in I} \mapsto u_j, \qquad\qquad \pi_j\colon \bigoplus_{i\in I} M_i \to M_j, \quad (u_i)_{i\in I} \mapsto u_j.$$

Ist die Indexmenge I endlich, so stimmen direkte Summe und Produkt der Moduln M_i, $i \in I$, überein.

Konstruktion 5.1.19. Es seien R ein K1-Ring, M ein R-Modul und $N \leq_R M$ ein Untermodul. Dann hat man eine wohldefinierte Skalarmultiplikation

$$R \times M/N \ \to \ M/N, \qquad r \cdot (u + N) \ := \ r \cdot u + N$$

Damit wird die Faktorgruppe M/N zu einem R-Modul, dem *Restklassenmodul* von M nach N.

Weiter hat man einen surjektiven Modulhomomorphismus $\pi\colon M \to M/N$ mit Kern(π) $= N$, nämlich

$$\pi\colon M \ \to \ M/N, \qquad u \ \mapsto \ u + N.$$

Beweis. Wir wissen bereits, dass M/N eine abelsche Gruppe ist, und dass $\pi\colon M \to M/N$ ein surjektiver Gruppenhomomorphismus mit $\mathrm{Kern}(\pi) = N$ ist.

Um zu zeigen, dass die Skalarmultiplikation wohldefiniert ist, betrachten wir zwei $u, u' \in N$ mit $u + N = u' + N$. Dann gilt $u - u' \in N$. Für jedes $r \in R$ erhält man $r \cdot (u - u') = r \cdot u - r \cdot u' \in N$. Das bedeutet $r \cdot (u + N) = r \cdot (u' + N)$.

Es bleiben die Modulaxiome für die Skalarmultiplikation zu verifizieren. Offensichtlich gilt $1_R \cdot (u + N) = u + N$ für alle $u + N \in M/N$. Weiter haben wir für alle $u, u' \in M$ und alle $r, r' \in R$:

$$\begin{aligned}
(r'r) \cdot (u + N) &= ((r'r) \cdot u) + N \\
&= (r' \cdot (r \cdot u)) + N \\
&= r' \cdot ((r \cdot u) + N) \\
&= r' \cdot (r \cdot (u + N)).
\end{aligned}$$

$$\begin{aligned}
(r + r') \cdot (u + N) &= ((r + r') \cdot u) + N \\
&= (r \cdot u + r' \cdot u) + N \\
&= (r \cdot u + N) \ + \ (r' \cdot u + N) \\
&= r \cdot (u + N) \ + \ r' \cdot (u + N).
\end{aligned}$$

$$\begin{aligned}
r \cdot ((u + N) + (u' + N)) &= r \cdot ((u + u') + N) \\
&= (r \cdot (u + u')) + N \\
&= (r \cdot u + r \cdot u') + N \\
&= (r \cdot u + N) \ + \ (r \cdot u' + N) \\
&= r \cdot (u + N) \ + \ r \cdot (u' + N).
\end{aligned}$$

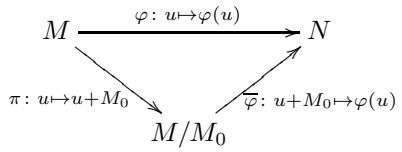
Es bleibt zu zeigen, dass die Abbildung $\pi\colon M \to M/N$ mit der Skalarmultiplikation verträglich ist. Für alle $u, u' \in v$ und alle $r, r' \in R$ gilt

$$\begin{aligned}
\pi(r \cdot u + r' \cdot u') &= (r \cdot u + r' \cdot u') + N \\
&= (r \cdot u + N) + (r' \cdot u' + N) \\
&= r \cdot (u + N) + r' \cdot (u' + N) \\
&= r \cdot \pi(u) + r' \cdot \pi(u').
\end{aligned}$$

□

Beispiel 5.1.20. Es seien R ein K1-Ring und $\mathfrak{a} \leq_R R$ ein Ideal. Dann ist der Restklassenring $R/\mathfrak{a}$ ein R-Modul.

Satz 5.1.21 (Homomorphiesatz)**.** *Es seien R ein K1-Ring, $\varphi\colon M \to N$ ein Homomorphismus von R-Moduln, und $M_0 \leq_R M$ ein Untermodul mit $M_0 \subseteq \mathrm{Kern}(\varphi)$. Dann gibt es ein kommutatives Diagramm*



von wohldefinierten R-Modulhomomorphismen. Dabei ist der Modulhomomorphismus $\overline{\varphi}\colon M/M_0 \to N$ durch $\varphi\colon M \to N$ und das obige Diagramm eindeutig bestimmt. Es gilt weiter

(i) *$\overline{\varphi}$ ist injektiv $\Leftrightarrow$ $M_0 = \mathrm{Kern}(\varphi)$;*
(ii) *$\overline{\varphi}$ ist surjektiv $\Leftrightarrow$ φ ist surjektiv.*

Beweis. Der Homomorphiesatz 1.3.17 liefert die entsprechenden Aussagen für die abelschen Gruppen M, N und M/M_0. Es ist daher nur noch zu zeigen, dass $\overline{\varphi}\colon M/M_0 \to N$ mit der Skalarmultiplikation verträglich ist. Das ergibt sich jedoch sofort mit

$$\overline{\varphi}(r \cdot (u + M_0)) \;=\; \varphi(r \cdot u) \;=\; r \cdot \varphi(u) \;=\; r \cdot \overline{\varphi}(u + M_0).$$

□

Folgerung 5.1.22. *Es seien R ein K1-Ring und $\varphi\colon M \to N$ ein surjektiver Homomorphismus von R-Moduln. Dann gilt $N \cong M/\mathrm{Kern}(\varphi)$.*

Konstruktion 5.1.23. Es seien R ein K1-Ring und M, N zwei R-Moduln. Die Menge $\mathrm{Hom}_R(M,N)$ aller R-Modulhomomorphismen wird durch

$$(\varphi + \psi)(u) \;:=\; \varphi(u) + \psi(u), \qquad (r \cdot \varphi)(u) \;:=\; r \cdot \varphi(u)$$

zu einem R-Modul. Insbesondere erhält man für den Speziallfall $N = R$ den *zu M dualen R-Modul* $M^* := \mathrm{Hom}_R(M,R)$.

Beweis. Es ist zunächst die Wohldefiniertheit nachzuweisen, d.h., wir müssen zeigen, dass mit $\varphi, \psi \in \mathrm{Hom}_R(M,R)$ und $r \in R$ die Abbildungen $\varphi + \psi$ und $r \cdot \varphi$ wieder Homomorphismen sind.

$$\begin{aligned}
(\varphi+\psi)(u_1+u_2) &= \varphi(u_1+u_2) + \psi(u_1+u_2)\\
&= \varphi(u_1) + \varphi(u_2) + \psi(u_1) + \psi(u_2)\\
&= \varphi(u_1) + \psi(u_1) + \varphi(u_2) + \psi(u_2)\\
&= (\varphi+\psi)(u_1) + (\varphi+\psi)(u_2),\\
(\varphi+\psi)(r\cdot u) &= \varphi(r\cdot u) + \psi(r\cdot u)\\
&= r\cdot\varphi(u) + r\cdot\psi(u)\\
&= r\cdot(\varphi(u)+\psi(u))\\
&= r\cdot(\varphi+\psi)(u),\\
(r\cdot\varphi)(u_1+u_2) &= r\cdot(\varphi(u_1+u_2))\\
&= r\cdot(\varphi(u_1)+\varphi(u_2))\\
&= r\cdot\varphi(u_1) + r\cdot\varphi(u_2)\\
&= (r\cdot\varphi)(u_1) + (r\cdot\varphi)(u_2),\\
(r\cdot\varphi)(a\cdot u) &= r\cdot\varphi(a\cdot u)\\
&= r\cdot(a\cdot\varphi(u))\\
&= a\cdot(r\cdot\varphi(u))\\
&= a\cdot((r\cdot\varphi)(u)).
\end{aligned}$$

Man beachte, dass zum Nachweis der Verträglichkeit von $r \cdot \varphi$ mit der Skalarmultiplikation die Kommutativität des Ringes R benötigt wird. Die Modulaxiome für $\mathrm{Hom}_R(M,N)$ lassen sich nun leicht punktweise nachprüfen. □

Aufgaben zu Abschnitt 5.1.

Aufgabe 5.1.24. In Konstruktion 5.1.5 wurde auf jeder additiven abelschen Gruppe G eine Skalarmultiplikation $\mathbb{Z} \times G \to G$ definiert durch

$$n \cdot g \;:=\; ng \;=\; \begin{cases} \underbrace{g + \ldots + g}_{n\text{-mal}} & \text{falls } n > 0, \\ 0 & \text{falls } n = 0, \\ \underbrace{-g - \ldots - g}_{|n|\text{-mal}} & \text{falls } n < 0. \end{cases}$$

Zeige, dass G dadurch zu einem $\mathbb{Z}$-Modul wird, d.h., verifiziere die Modulaxiome explizit.

Aufgabe 5.1.25. Es seien R ein K1-Ring und $\varphi\colon M \to N$ ein Homomorphismus von R-Moduln. Beweise die Aussagen aus Bemerkung 5.1.17:

(i) Für jeden Untermodul $M' \leq_R M$ ist das Bild $\varphi(M')$ ein Untermodul von N; insbesondere ist Bild(φ) ein Untermodul von N.
(ii) Für jeden Untermodul $N' \leq_R N$ ist das Urbild $\varphi^{-1}(N')$ ein Untermodul von M; insbesondere ist Kern(φ) ein Untermodul von M.
(iii) Der Homomorphismus $\varphi\colon M \to N$ ist genau dann injektiv, wenn $\mathrm{Kern}(\varphi) = \{0\}$ gilt.
(iv) Der Homomorphismus $\varphi\colon M \to N$ ist genau dann ein Isomorphismus, wenn es einen Homomorphismus $\psi\colon N \to M$ gibt mit

$$\psi \circ \varphi \;=\; \mathrm{id}_M, \qquad\qquad \varphi \circ \psi \;=\; \mathrm{id}_N.$$

Aufgabe 5.1.26. Es seien $v_1 := (2,1)$ und $v_2 := (1,2)$ und $N := \mathrm{Lin}(v_1, v_2) \leq_{\mathbb{Z}} \mathbb{Z}^2$. Zeige: Es gilt $\mathbb{Z}^2/N \cong \mathbb{Z}/3\mathbb{Z}$.

Aufgabe 5.1.27. Es sei M ein $\mathbb{Z}$-Modul, sodass $M = \mathbb{Z} \cdot u$ für ein $u \in M$ gilt. Zeige:

(i) Es gilt $M \cong \mathbb{Z}/n\mathbb{Z}$ mit einem eindeutig bestimmten $n \in \mathbb{Z}_{\geq 0}$. *Hinweis:* Konstruiere einen surjektiven Homomorphismus $\mathbb{Z} \to M$ mit $1 \mapsto u$.
(ii) Ist n wie in (i) und gilt $n = p_1^{\nu_1} \cdots p_r^{\nu_r}$ mit paarweise verschiedenen Primzahlen $p_1, \ldots, p_r \in \mathbb{Z}_{\geq 2}$, so hat man einen $\mathbb{Z}$-Modulisomorphismus

$$M \;\cong\; \mathbb{Z}/p_1^{\nu_1}\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/p_r^{\nu_r}\mathbb{Z}.$$

Aufgabe 5.1.28. Es sei M ein $\mathbb{Z}$-Modul. Zeige: Ist $p := |M|$ eine Primzahl, so gilt $M \cong \mathbb{Z}/p\mathbb{Z}$.

Aufgabe 5.1.29 (Isomorphiesätze für Moduln)**.** Es seien R ein K1-Ring und M ein R-Modul. Zeige:

(i) Für je zwei Untermoduln $L \leq_R M$ und $N \leq_R M$ hat man einen kanonischen Isomorphismus

$$N/(N \cap L) \;\to\; (N + L)/L, \qquad v + (N \cap L) \;\mapsto\; v + L.$$

(ii) Für jede Schachtelung $L \leq_R N \leq_R M$ von Untermoduln hat man einen kanonischen Isomorphismus

$$M/L\Big/N/L \;\to\; M/N, \qquad (u + L) + (N/L) \;\mapsto\; u + N.$$

Aufgabe 5.1.30. Es seien $p, q \in \mathbb{Z}_{\geq 0}$ Primzahlen. Zeige: Für den Modul der Homomorphismen zwischen den $\mathbb{Z}$-Moduln $\mathbb{Z}/p\mathbb{Z}$ und $\mathbb{Z}/q\mathbb{Z}$ gilt

$$\mathrm{Hom}(\mathbb{Z}/p\mathbb{Z}, \mathbb{Z}/q\mathbb{Z}) \;\cong\; \begin{cases} \mathbb{Z}/p\mathbb{Z} & \text{falls } p = q, \\ \{0\} & \text{falls } p \neq q. \end{cases}$$

5.2. **Freie Moduln.**

Definition 5.2.1. Es seien R ein K1-Ring und M ein R-Modul.

(i) Eine Familie $\mathcal{F} = (u_i)_{i\in I}$ in M heißt *Erzeugendensystem für M*, falls jedes $u \in M$ eine R-Linearkombination über $\mathcal{F}$ ist.
(ii) Eine Familie $\mathcal{F} = (u_i)_{i\in I}$ in M heißt *linear unabhängig*, falls für jede R-Linearkombination $\sum r_i u_i$ über $\mathcal{F}$ gilt

$$\sum r_i u_i \;=\; 0_M \quad\Longrightarrow\quad r_i \;=\; 0_R \text{ für alle } i \in I.$$

(iii) Der R-Modul M heißt *endlich erzeugt*, falls er ein endliches Erzeugendensystem besitzt.
(iv) Der R-Modul M heißt *frei*, falls $M = \{0_M\}$ gilt oder M eine *Basis*, d.h., ein linear unabhängiges Erzeugendensystem, besitzt.

Beispiel 5.2.2. Es seien R ein K1-Ring und $I \neq \emptyset$ eine Menge. Dann ist der R-Modul $R^I := \bigoplus_{i\in I} R$ frei; er besitzt eine kanonische Basis $(e_i)_{i\in I}$, wobei

$$e_i \;:=\; (\delta_{ij})_{j\in I} \quad \text{mit } \delta_{ij} \;:=\; \begin{cases} 1_R & \text{falls } j = i, \\ 0_R & \text{falls } j \neq i. \end{cases}$$

Beispiel 5.2.3. In $\mathbb{Z}^2$ betrachten wir die Elemente $v_1 := (2, 1)$ und $v_2 := (1, 2)$. Dann ist $\mathcal{F} := (v_1, v_2)$ linear unabhängig aber nicht erzeugend; beispielsweise kann man $(1, 0)$ nicht als $\mathbb{Z}$-Linearkombination über $\mathcal{F}$ darstellen.

Satz 5.2.4. *Es seien R ein K1-Ring und M ein R-Modul mit Basis $\mathcal{B} = (u_i)_{i\in I}$. Dann besitzt jedes $u \in M$ eine eindeutige Darstellung*

$$u \;=\; \sum_{i\in I} r_i \cdot u_i \qquad \textit{mit } r_i \in R. \tag{5.1}$$

Beweis. Da $\mathcal{B}$ ein Erzeugendensystem für M ist, besitzt jedes $u \in M$ eine Darstellung (5.1).

Zum Nachweis der Eindeutigkeit seien zwei Darstellungen $u = \sum_{i\in I} r_i \cdot u_i$ und $u = \sum_{i\in I} s_i \cdot u_i$ gegeben. Dann erhalten wir

$$\begin{aligned} 0_M &= u - u \\ &= \sum_{i\in I} r_i \cdot u_i \;-\; \sum_{i\in I} s_i \cdot u_i \\ &= \sum_{i\in I} (r_i - s_i) \cdot u_i. \end{aligned}$$

Da $\mathcal{B}$ linear unabhängig ist, muss $r_i = s_i$ für jedes $i \in I$ gelten. Folglich stimmen die Darstellungen von u überein. □

Definition 5.2.5. Es seien R ein K1-Ring und M ein R-Modul mit Basis $\mathcal{B} = (u_i)_{i\in I}$. Für jedes $u \in M$ nennt man die Darstellung

$$u \;=\; \sum_{i\in I} r_i \cdot u_i$$

die *Entwicklung* von u nach der Basis $\mathcal{B}$, und man nennt $x_{\mathcal{B}}(u) := (r_i)_{i\in I} \in R^I$ den *Koordinatenvektor* von u bezüglich $\mathcal{B}$.

Satz 5.2.6. *Es seien R ein K1-Ring und M ein freier R-Modul mit einer Basis $B = (u_i)_{i\in I}$. Weiter seien und N ein R-Modul und $(v_i)_{i\in I}$ eine Familie in N.*

(i) *Es gibt einen eindeutig bestimmten Homomomorphismus $\varphi\colon M \to N$ mit $\varphi(u_i) = v_i$ für alle $i \in I$, nämlich*

$$\varphi\left(\sum_{i\in I} r_i \cdot u_i\right) \ := \ \sum_{i\in I} r_i \cdot v_i.$$

(ii) *Der Homomorphismus $\varphi\colon M \to N$ aus (ii) ist genau dann ein Isomorphismus, wenn $(v_i)_{i\in I}$ eine Basis für N ist.*

Beweis. Zu (i). Wegen der Eindeutigkeit des Koordinatenvektors ist Abbildung $\varphi\colon M \to N$ wohldefiniert. Weiter haben wir $\varphi(u_i) = v_i$.

Zum Nachweis der Linearität seien $u, u' \in M$ und $a, a' \in \mathbb{K}$ gegeben. Wir betrachten die Entwicklungen

$$u \ = \ \sum_{i\in I} r_i \cdot u_i, \qquad\qquad u' \ = \ \sum_{i\in I} r'_i \cdot u_i$$

bezüglich der Basis $\mathcal{B} = (u_i)_{i\in I}$ von M. Gemäß unserer Definition von φ erhalten wir dann

$$\begin{aligned}
\varphi(a \cdot u + a' \cdot u') &= \varphi\left(\sum_{i=1}^{n} (ar_i + a'r'_i) \cdot u_i\right) \\
&= \sum_{i=1}^{n} (ar_i + a'r'_i) \cdot v_i \\
&= \sum_{i=1}^{n} (ar_i) \cdot v_i \ + \ \sum_{i=1}^{n} (a'r'_i) \cdot v_i \\
&= a \cdot \sum_{i=1}^{n} r_i \cdot v_i \ + \ a' \cdot \sum_{i=1}^{n} r'_i \cdot v_i \\
&= a \cdot \varphi(v) \ + \ a' \cdot \varphi(v').
\end{aligned}$$

Es bleibt zu zeigen, dass φ durch die Vorgabe der Werte v_i auf den u_i eindeutig bestimmt ist. Ist $\varphi'\colon M \to N$ eine weitere lineare Abbildung mit $\varphi'(u_i) = v_i$, so erhalten wir für jedes $u = \sum r_i \cdot u_i$:

$$\varphi'(u) \ = \ \varphi'\left(\sum r_i \cdot u_i\right) \ = \ \sum r_i \cdot \varphi'(u_i) \ = \ \sum r_i \cdot \varphi(u_i) \ = \ \varphi\left(\sum r_i \cdot u_i\right) \ = \ \varphi(u).$$

Zu (ii). Es sei zunächst $\varphi\colon M \to N$ ein Isomorphismus. Wir zeigen, dass $\mathcal{C} := (v_i)_{i\in I}$ ein Erzeugendensystem für N ist. Dazu sei $v \in N$ gegeben. Da φ surjektiv ist, gibt es ein $u \in M$ mit $\varphi(u) = v$. Ist $u = \sum r_i \cdot u_i$ die Etwicklung von u bezüglich $\mathcal{B}$, so erhalten wir

$$v \ = \ \varphi(u) \ = \ \varphi\left(\sum_{i\in I} r_i \cdot u_i\right) \ = \ \sum_{i\in I} r_i \cdot v_i \ \in \ \mathrm{Lin}(\mathcal{C})$$

Zum Nachweis der linearen Unabhängigkeit von $\mathcal{C}$ sei eine Linearkombination $\sum r_i \cdot v_i = 0_N$ gegeben. Dann erhalten wir

$$0_M \ = \ \varphi^{-1}(0_N) \ = \ \varphi^{-1}\left(\sum_{i\in I} r_i \cdot v_i\right) \ = \ \sum_{i\in I} r_i \cdot u_i,$$

wobei $\varphi^{-1}\colon N \to M$ den Umkehrhomomorphismus bezeichnet. Da $(u_i)_{i\in I}$ linear unabhängig ist, ergibt sich $r_i = 0_R$ für alle $i \in I$.

Es sei nun $(v_i)_{i\in I}$ eine Basis für N. Dann erhält man nach (i) einen Homomorphismus $\psi\colon N \to M$ mit $\psi(v_i) = u_i$ für alle $i \in I$. Man prüft leicht nach, dass ψ eine Umkehrabbildung zu φ: Es gilt stets

$$\begin{aligned}\varphi \circ \psi \left(\sum_{i\in I} r_i \cdot v_i \right) &= \varphi \left(\sum_{i\in I} r_i \cdot u_i \right) = \sum_{i\in I} r_i \cdot v_i, \\ \psi \circ \varphi \left(\sum_{i\in I} r_i \cdot u_i \right) &= \psi \left(\sum_{i\in I} r_i \cdot v_i \right) = \sum_{i\in I} r_i \cdot u_i.\end{aligned}$$

□

Folgerung 5.2.7. *Es seien R ein $K1$-Ring und M eine freier R-Modul mit Basis $\mathcal{B} = (u_i)_{i\in I}$. Dann hat man einen Isomorphismus*

$$\varphi_{\mathcal{B}}\colon M \to R^I, \qquad u \mapsto x_{\mathcal{B}}(u).$$

Folgerung 5.2.8. *Ein freier R-Modul M ist genau dann endlich erzeugt, wenn er eine endliche Basis besitzt.*

Beweis. Besitzt M eine endliche Basis, so ist M auch endlich erzeugt. Es sei nun M endlich erzeugt. Als freier Modul besitzt M dann eine Basis $\mathcal{B} = (u_i)_{i\in I}$. Nach Folgerung 5.2.7 ist M isomorph zu R^I; insbesondere ist letzterer Modul ebenfalls endlich erzeugt. Das geht nur, wenn I endlich ist. □

Definition 5.2.9. Es seien R ein Integritätsring und M ein R-Modul. Der *Rang* $\mathrm{rg}_R(M)$ von M ist das Supremum über alle Längen $|I|$ linear unabhängiger Familien $(u_i)_{i\in I}$ in M.

Beispiel 5.2.10. Es sei $\mathbb{K}$ ein Körper. Der Rang $\mathrm{rg}_{\mathbb{K}}(V)$ eines $\mathbb{K}$-Vektorraumes V ist seine Dimension $\dim_{\mathbb{K}}(V)$.

Beispiel 5.2.11. Es sei $n \in \mathbb{Z}_{\geq 1}$. Dann gilt $\mathrm{rg}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}) = 0$. Noch schlimmer: Für jede beliebige Familie $n_i \in \mathbb{Z}_{\geq 1}$, $i \in I$ gilt

$$\mathrm{rg}_{\mathbb{Z}} \left(\bigoplus_{i\in I} \mathbb{Z}/n_i\mathbb{Z} \right) = 0,$$

denn man hat $n_i \cdot v = 0$ für jedes $v \in \mathbb{Z}/n_i\mathbb{Z}$ und folglich gibt es für jede Familie in $\bigoplus \mathbb{Z}/n_i\mathbb{Z}$ nichttriviale annullierende Linearkombinationen.

Satz 5.2.12. *Es seien R ein Integritätsring und M, N zwei R-Moduln. Dann gilt*

$$\mathrm{rg}_R(M \oplus N) = \mathrm{rg}_R(M) + \mathrm{rg}_R(N).$$

Beweis. Wir zeigen zunächst die Abschätzung "$\geq$". Dazu seien $(u_i)_{i\in I}$ und $(v_j)_{j\in J}$ linear unabhängige Familien in M bzw. N. Dann ist auch die Familie

$$(w_k)_{k\in I\sqcup J} \quad \text{mit} \quad w_k := \begin{cases} u_k & k \in I, \\ v_k & k \in J \end{cases}$$

linear unabhängig und sie besitzt die Länge $|I|+|J|$ Elemente. Folglich ist der Rang von $M \oplus N$ mindestens die Summe $\mathrm{rg}_R(M) + \mathrm{rg}_R(N)$.

Nun zur Abschätzung "$\leq$". Es ist nur etwas zu zeigen, wenn $m := \mathrm{rg}_R(M)$ und $n := \mathrm{rg}_R(N)$ endlich sind. Wir haben dann zu zeigen, dass jede Familie der Form

$$C = ((u_1, v_1), \ldots, (u_{m+n}, v_{m+n}), (u_{m+n+1}, v_{m+n+1}))\,.$$

linear abhängig ist. Dabei dürfen wir annehmen, dass $(u_1, \ldots, u_d)$ eine maximale linear unabhängige Teilfamilie von $(u_1, \ldots, u_{m+n+1})$ ist, wobei $d \leq m$ gilt.

In einem ersten Schritt wählen wir für jedes $j = d+1, \ldots, m+n+1$ eine nichttriviale Linearkombination

$$\sum_{i=1}^{d} r_{ij} u_i \ + \ r_j u_j \quad = \quad 0.$$

Wegen der linearen Unabhängigkeit von $(u_1, \ldots, u_d)$ muss dabei $r_j \neq 0$ gelten. Wir definieren

$$L_j \quad := \quad (r_{1j}, \ldots, r_{dj}, 0, \ldots, 0, r_j, 0, \ldots, 0).$$

In einem zweiten Schritt betrachten wir für $j = d+1, \ldots, m+n+1$ die folgenden Elemente in dem Modul N:

$$v'_j \quad := \quad \sum_{i=1}^{d} r_{ij} v_i \ + \ r_j v_j.$$

Dies sind mindestens $n+1$ Elemente. Wegen $\mathrm{rg}_R(N) = n$ ist $(v'_{d+1}, \ldots, v'_{m+n+1})$ linear abhängig. Es gibt es also eine nichttriviale Linearkombination

$$b_{d+1} v'_{d+1} + \ldots + b_{m+n+1} v'_{m+n+1} \quad = \quad 0.$$

Da R ein Integritätsring ist, besitzt $L := b_{d+1} L_{d+1} + \ldots + b_{m+n+1} L_{m+n+1}$ mindestens eine nichtriviale Komponente $b_j r_j$. Nach Konstruktion leisten die Komponenten von $l_1, \ldots, l_{m+n+1}$ von L jedoch

$$l_1(u_1, v_1) + \ldots + l_{m+n+1}(u_{m+n+1}, v_{m+n+1}) \quad = \quad 0.$$

□

Satz 5.2.13. *Es seien R ein Integritätsring und M ein R-Modul. Besitzt M eine Basis $(u_1, \ldots, u_m)$, so gilt $\mathrm{rg}_R(M) = m$.*

Beweis. Wir führen den Beweis der Aussage mittels Induktion über die Länge m der Basis $(u_1, \ldots, u_m)$.

Im Fall $n = 1$ haben wir $M = Ru_1$ und $\mathrm{rg}_R(M) \geq 1$. Wir müssen $\mathrm{rg}_R(M) > 1$ ausschließen. In diesem Fall hätte man eine linear unabhängige Familie (u, u') in M. Mit geeigneten $a, a' \in R \setminus \{0\}$ gilt $u = au_1$ und $u' = a'u_1$. Das führt zu einem Widerspruch, denn man erhält eine nichttriviale Linearkombination

$$a'u \ + \ (-a)u' \quad = \quad 0.$$

Der Induktionsschritt ist einfach. Offensichtlich haben wir eine direkte Summenzerlegung

$$M \quad \cong \quad \mathrm{Lin}(u_1) \ \oplus \ \mathrm{Lin}(u_2, \ldots, u_m).$$

Nach Induktionsvoraussetzung besitzen die Moduln auf der rechten Seite die Ränge 1 bzw. $m-1$. Mit Satz 5.2.12 folgt $\mathrm{rg}_R(M) = m$. □

Aufgaben zu Abschnitt 5.2.

Aufgabe 5.2.14. Es sei R ein K1-Ring. Zeige: Zu jedem R-Modul M gibt es einen Epimorphismus $F \to M$ mit einem freien R-Modul F. *Hinweis:* Betrachte $F := \oplus_M R$.

Aufgabe 5.2.15. Es seien $a_1, \ldots, a_n \in \mathbb{Z}$, und es sei $v := (a_1, \ldots, a_n)$. Beweise die Äquivalenz folgender Aussagen:

(i) Es gibt eine Basis $(v, v_2, \ldots, v_n)$ für $\mathbb{Z}^n$.
(ii) Die Zahlen $a_1, \ldots, a_n$ sind teilerfremd.

Aufgabe 5.2.16. Es seien R ein K1-Ring und M ein freier R-Modul mit einer endlichen Basis $(u_1, \ldots, u_n)$. Dann ist auch der duale Modul $M^* = \mathrm{Hom}_R(M, R)$ frei, und man hat eine duale Basis $(u_1^*, \ldots, u_n^*)$ für M^* mit

$$u_i^*(u_j) \quad = \quad \begin{cases} 1 & \text{falls } i = j, \\ 0 & \text{falls } i \neq j. \end{cases}$$

Aufgabe 5.2.17. Es sei R ein K1-Ring, und es seien M, N freie R-Moduln mit Basen $(u_1, \ldots, u_m)$ bzw. $(v_1, \ldots, v_n)$. Zeige: Man hat zueinander inverse Bijektionen

$$\begin{array}{rcl} \mathrm{Hom}_R(M, N) & \longleftrightarrow & \mathrm{Mat}(n, m; R) \\ \varphi & \mapsto & (v_i^*(\varphi(u_j)))_{i,j} \\ \left[u_j \mapsto \sum_i a_{ij} v_i \right] & \mapsfrom & (a_{ij})_{i,j} \end{array}$$

Dabei entspricht die Hintereinanderausführung der Matrizenmultiplikation; insbesondere entsprechen für $n = m$ die Isomorphismen den invertierbaren Matrizen.

Aufgabe 5.2.18. Der freie $\mathbb{Z}$-Modul $\mathbb{Z}^2$ besitzt den Rang 2. Zeige: Der durch $v_1 = (2, 1)$ und $v_2 = (1, 2)$ erzeugte Untermodul $M \leq_{\mathbb{Z}} \mathbb{Z}^2$ ist ebenfalls frei und vom Rang 2. Beachte, dass $M \neq \mathbb{Z}^2$ gilt.

5.3. **Torsion und Länge.**

Beispiel 5.3.1. Für $n \in \mathbb{Z}_{\geq 2}$ betrachten wir den $\mathbb{Z}$-Modul $\mathbb{Z}/n\mathbb{Z}$. Für jedes Element $\overline{a} = a + n\mathbb{Z}$ hat man

$$n \cdot \overline{a} \;=\; (na) \cdot \overline{1} \;=\; (an) \cdot \overline{1} \;=\; a \cdot \overline{n} \;=\; \overline{0}.$$

Insbesondere ist die Familie $(\overline{a})$ linear abhängig. Somit kann $\mathbb{Z}/n\mathbb{Z}$ kein freier $\mathbb{Z}$-Modul sein.

Definition 5.3.2. Es seien R ein Integritätsringring und M ein R-Modul.

(i) Man nennt $u \in M$ ein *Torsionselement*, falls $r \cdot u = 0$ mit einem $0 \neq r \in R$ gilt. Die Menge aller Torsionselemente in M bezeichnen wir mit $T(M)$.
(ii) Man nennt M einen *Torsionsmodul*, falls $M = T(M)$ gilt, und man nennt M *torsionsfrei*, falls $T(M) = \{0\}$ gilt.

Beispiel 5.3.3. Es seien R ein Integritätsring und $0 \neq a \in R$. Dann ist $R/\langle a \rangle$ ein Torsionsmodul über R.

Satz 5.3.4. *Es seien R ein Integritätsring und M ein R-Modul.*

(i) *Die Menge $T(M) \subseteq M$ der Torsionselemente ist ein Untermodul von M.*
(ii) *Ist M frei, so ist M torsionsfrei.*
(iii) *Ist M torsionsfrei, so ist auch jeder Untermodul $N \leq_R M$ torsionsfrei.*

Beweis. Zu (i). Es gilt stets $0_M \in T(M)$. Sind $u, u' \in T(M)$ gegeben, so gibt es $0_R \neq r, r' \in R$ mit $r \cdot u = 0_M = r' \cdot u'$. Da R ein Integritätsring ist, gilt $rr' \neq 0_R$. Weiter haben wir

$$(rr') \cdot (u + u') \;=\; r' \cdot (r \cdot u) + r \cdot (r' \cdot u') \;=\; 0_M$$

Das bedeutet $u + u' \in T(M)$. Sind $u \in M$ und $s \in R$ gegeben, so wählen wir wieder $0_R \neq r \in R$ mit $r \cdot u = 0_M$. Dann ergibt sich $s \cdot u \in T(M)$ mit

$$r \cdot (s \cdot u) \;=\; s \cdot (r \cdot u) \;=\; 0_M.$$

Zu (ii). Wir zeigen, dass $T(M) = \{0_M\}$ gilt. Dazu sei $(u_i)_{i \in I}$ eine Basis für M. Ist $u \in T(M)$, gegeben, so besitzt u eine Entwicklung $\sum r_i \cdot u_i$. Man hat

$$0_M \;=\; r \cdot \sum_{i \in I} r_i \cdot u_i \;=\; \sum_{i \in I} (rr_i) \cdot u_i.$$

Die lineare Unabhängigkeit von $(u_i)_{i \in I}$ liefert $rr_i = 0_R$ für alle $i \in I$. Da R Integritätsring ist, erhalten wir $r_i = 0_R$ für alle $i \in I$. Das bedeutet $u = 0_M$. □

Definition 5.3.5. Es seien R ein K1-Ring und M ein R-Modul. Die *Länge* $l_R(M)$ von M ist das Supremum über alle Längen r von Untermodulketten der Form

$$\{0\} \;\subsetneq\; M_1 \;\subsetneq\; M_2 \;\subsetneq\; \ldots \;\subsetneq\; M_r \;=\; M, \qquad M_i \leq_R M.$$

Bemerkung 5.3.6. Es seien R ein K1-Ring und M ein R-Modul. Dann gilt:

$$l_R(M) \;=\; 0 \quad\Longleftrightarrow\quad M \;=\; \{0\}.$$

Beispiel 5.3.7.
(i) Es seien $\mathbb{K}$ ein Körper und V ein $\mathbb{K}$-Vektorraum. Dann gilt $l_{\mathbb{K}}(V) = \dim(V)$.
(ii) Es gilt $l_{\mathbb{Z}}(\mathbb{Z}) = \infty$, denn mit jedem $a \in \mathbb{Z}_{\geq 2}$ kann man beliebig lange Untermodulketten konstruieren:

$$\{0\} \;\subsetneq\; \langle a^n \rangle \;\subsetneq\; \langle a^{n-1} \rangle \;\subsetneq\; \ldots \;\subsetneq\; \langle a \rangle \;\subsetneq\; \mathbb{Z}.$$

(iii) Für jede Primzahl $p \in \mathbb{Z}$ hat man $l_{\mathbb{Z}}(\mathbb{Z}/p\mathbb{Z}) = 1$, da $\{0\}$ und $\mathbb{Z}/p\mathbb{Z}$ die einzigen Untermoduln von $\mathbb{Z}/p\mathbb{Z}$ sind.

Satz 5.3.8. *Es sei R ein K1-Ring, und es seien M, N zwei R-Moduln. Dann gilt*

$$l_R(M \oplus N) \quad = \quad l_R(M) + l_R(N).$$

Beweis. Wir verifizieren zunächst die Abschätzung "$\geq$". Dazu betrachten wir zwei aufsteigende Untermodulketten

$$\{0\} \subsetneq M_1 \subsetneq \ldots \subsetneq M_r = M, \qquad \{0\} \subsetneq N_1 \subsetneq \ldots \subsetneq N_s = N.$$

Daraus gewinnt man eine echt aufsteigende Kette der Länge $r+s$ in der direkten Summe $M \oplus N$, nämlich

$$\{0\} \subsetneq M_1 \oplus \{0\} \subsetneq \ldots \subsetneq M_r \oplus \{0\} \subsetneq M_r \oplus N_1 \subsetneq \ldots \subsetneq M_r \oplus N_s = M \oplus N.$$

Beim Nachweis der Abschätzung "$\leq$" arbeiten wir mit den kanonischen Homomorphismen

$$\imath\colon M \to M \oplus N,\ u \mapsto (u,0), \qquad \pi\colon M \oplus N \to N,\ (u,v) \mapsto v.$$

Man hat also $\imath(M) = \operatorname{Kern}(\pi)$. Es sei $\{0\} \subsetneq U_1 \subsetneq \ldots \subsetneq U_r = M \oplus N$ eine aufsteigende Kette von Untermoduln. Wir zeigen, dass dann für jedes j gilt:

$$(*) \qquad \imath^{-1}(U_j) \subsetneq \imath^{-1}(U_{j+1}) \qquad \text{oder} \qquad \pi(U_j) \subsetneq \pi(U_{j+1}).$$

Nehmen wir an, es wäre für ein j in beiden Fällen Gleichheit gegeben. Wir führen dies zum Widerspruch, indem wir zeigen, dass dann $U_{j+1} \subseteq U_j$ und somit $U_j = U_{j+1}$ gelten müsste.

Dazu sei $(u,v) \in U_{j+1}$ gegeben. Wegen $\pi(U_j) = \pi(U_{j+1})$ gibt es dann ein Element $(u',v) \in U_j$. Offensichtlich gilt

$$(u-u',0) \ = \ (u,v) - (u',v) \ \in \ U_{j+1}.$$

Folglich hat man $u - u' \in \imath^{-1}(U_{j+1}) = \imath^{-1}(U_j)$. Das impliziert $(u-u',0) \in U_j$, und wir erhalten

$$(u,v) \ = \ (u',v) + (u-u',0) \ \in \ U_j.$$

Damit haben wir $(*)$ verifiziert. Folglich kann man aus den Untermoduln $\imath^{-1}(U_j) \subseteq M$ und $\pi(U_j) \subseteq N$ echt aufsteigende Ketten in M bzw. N bilden, sodass die Summe der Kettenlängen mindestens r beträgt. □

Satz 5.3.9. *Es sei R ein Hauptidealring, und es seien $q_1, \ldots, q_n \in R$ Primelemente. Dann gilt*

$$l_R(R/\langle q_1 \cdots q_n \rangle) \quad = \quad n.$$

Lemma 5.3.10. *Es seien R ein Hauptidealring und $a \in R$ von der Form $a = cp_1^{\nu_1} \ldots p_n^{\nu_n}$, wobei $c \in R^*$ gelte und die p_i paarweise nichtassoziierte Primelemente seien. Dann erhält man einen Isomorphismus von R-Moduln*

$$R/\langle a \rangle \quad \cong \quad R/\langle p_1^{\nu_1} \rangle \ \times \ \ldots \ \times \ R/\langle p_n^{\nu_n} \rangle.$$

Beweis. Nach Satz 4.3.15 hat man sogar einen Isomorphismus der entsprechenden Faktorringe. Das liefert insbesondere den gewünschten Isomorphismus der Restklassenmoduln. □

Beweis von Satz 5.3.9. Wir behandeln zunächst den Fall $q_1 = \ldots = q_n =: q$. Wir arbeiten mit dem surjektiven Homomorphismus $\pi\colon R \to R/\langle q^n \rangle$.

Die Ungleichung $l_R(R/\langle q^n \rangle) \geq n$ ist leicht einzusehen: Man hat eine echt aufsteigende Kette der Länge n von Idealen in R, nämlich

$$\{0\} \subsetneq \langle q^{n-1} \rangle \subsetneq \ldots \subsetneq \langle q \rangle \subsetneq \langle 1_R \rangle = R.$$

Die Inklusionen sind jeweils echt, da wir sonst $q^{i+1} \mid q^i$ für ein i hätten. Als Ideale in R sind die $\langle q^i \rangle$ auch Untermoduln von R.

Die Bilder $\pi(\langle q^i \rangle)$ der Untermoduln $\langle q^i \rangle \leq_R R$ liefern eine aufsteigende Untermodulkette in $R/\langle q^n \rangle$:

$$\{0\} \subsetneq \pi(\langle q^{n-1} \rangle) \subsetneq \ldots \subsetneq \pi(\langle q \rangle) \subsetneq \pi(\langle 1_R \rangle) = R/\langle q^n \rangle.$$

Diese Kette ist tatsächlich echt aufsteigend, denn sonst hätte man $\pi(\langle q^i + 1 \rangle) = \pi(\langle q^i \rangle)$ für ein i, was sofort zu einem Widerspruch führt:

$$q^i \in \pi^{-1}(\pi(\langle q^{i+1} \rangle)) = \langle q^{i+1} \rangle + \langle q^n \rangle = \langle q^{i+1} \rangle.$$

Zum Nachweis der Ungleichung $l_R(R/\langle q^n \rangle) \leq n$ betrachten wir eine aufsteigende Kette

$$\{0\} \subsetneq M_1 \subsetneq \ldots \subsetneq M_r = R/\langle q^n \rangle$$

von Untermoduln in $R/\langle q^n \rangle$ Die Urbilder $\pi^{-1}(M_i)$ sind Ideale in dem Ring R, und sie bilden eine echt aufsteigende Kette

$$\{0\} \subsetneq \langle q^n \rangle \subsetneq \pi^{-1}(M_1) \subsetneq \pi^{-1}(M_2) \subsetneq \ldots \subsetneq \pi^{-1}(M_r) = R.$$

Da R Hauptidealring ist, wird jedes Ideal $\pi^{-1}(M_i)$ von einem Element $s_i \in R$ erzeugt, und wir erhalten $s_i | q^n$, d.h., es gilt $s_i = c_i q^{n_i}$ mit $c_i \in R^*$. Da die Kette echt aufsteigt, muss $n > n_1 > \ldots > n_1 = 0$ gelten. Folglich kann die Kette höchstens die Länge n besitzen.

Für den allgemeinen Fall schreiben wir $q_1 \cdots q_n = c p_1^{\nu_1} \cdots p_m^{\nu_m}$ mit paarweise nichtassoziierten Primelementen q_i. Lemma 5.3.10 liefert einen Isomorphismus von R-Moduln

$$R/\langle c p_1^{\nu_1} \cdots p_m^{\nu_m} \rangle \cong \bigoplus_{i=1}^{m} R/\langle p_i^{\nu_i} \rangle.$$

Die gewünschte Aussage über die Längen ergibt sich dann aus dem bereits behandelten Fall und Satz 5.3.8: Es gilt

$$\begin{aligned} l_R\left(R/\langle c p_1^{\nu_1} \cdots p_m^{\nu_m} \rangle\right) &= l_R\left(R/\langle p_1^{\nu_1} \rangle \oplus \ldots \oplus R/\langle p_m^{\nu_m} \rangle\right) \\ &= l_R\left(R/\langle p_1^{\nu_1} \rangle\right) + \ldots + \left(R/\langle p_m^{\nu_m} \rangle\right) \\ &= \nu_1 + \ldots + \nu_m \\ &= n. \end{aligned}$$

□

Satz 5.3.11. *Es seien R ein Hauptidealring und $a_1, \ldots, a_n, b_1, \ldots, b_m \in R$ Nichteinheiten mit $a_{i+1} | a_i$ für $i = 1, \ldots, n-1$ bzw. $b_{j+1} | b_j$ für $j = 1, \ldots, m-1$. Gilt*

$$\bigoplus_{i=1}^{n} R/\langle a_i \rangle \cong \bigoplus_{j=1}^{m} R/\langle b_j \rangle$$

als Isomorphie von R-Moduln, so hat man bereits $m = n$, und es gilt $b_i = c_i a_i$ mit Einheiten $c_i \in R$.

Beweis. Wir zeigen zunächst $\langle a_i \rangle = \langle b_i \rangle$ für $i \leq \min(m, n)$. Nehmen wir einmal an es existierten $k \leq \min(m, n)$ mit $\langle a_k \rangle \neq \langle b_k \rangle$. Dann wählen wir k minimal mit dieser Eigenschaft. Für $l \geq 0$ hat man $a_{k+l} | a_k$, somit $a_k R \subseteq \langle a_{k+l} \rangle$, und wir erhalten

$$M' := a_k \cdot \bigoplus_{i=1}^{n} R/\langle a_i \rangle \cong \bigoplus_{i=1}^{k-1} a_k \cdot (R/\langle a_i \rangle).$$

Andererseits erhalten wir mit $\langle a_i\rangle = \langle b_i\rangle$ für $i = 1, \ldots, k-1$ die folgende Darstellung für den R-Modul M':

$$M' \;\cong\; a_k \cdot \bigoplus_{j=1}^{m} R/\langle b_j\rangle \;=\; \bigoplus_{i=1}^{k-1} a_k \cdot (R/\langle a_i\rangle) \;\oplus\; \bigoplus_{j=k}^{m} a_k \cdot (R/\langle b_j\rangle).$$

Verwendet man nun die Additivität 5.3.8 der Länge $l_R(M')$, so ergibt ein Vergleich dieser beiden Darstellungen

$$l_R\left(\bigoplus_{j=k}^{m} a_k \cdot (R/\langle b_j\rangle)\right) \quad = \quad 0.$$

Folglich muss der Modul auf der linken Seite trivial sein. Insbesondere erhalten wir $a_k R \subseteq \langle b_k\rangle$. Analog sieht man $b_k R \subseteq \langle a_k\rangle$. Das ergibt $\langle a_k\rangle = \langle b_k\rangle$; Widerspruch zu unserer Annahme. Bis $\min(n, m)$ muss also $\langle a_i\rangle = \langle b_i\rangle$ gelten.

Wir nehmen nun an, dass m und n voneinander verschieden sind, etwa $m < n$. Nach Voraussetzung und wegen $\langle b_j\rangle = \langle a_j\rangle$ für $1 \le j \le m$ gilt

$$\bigoplus_{i=1}^{m} R/\langle a_i\rangle \oplus \bigoplus_{i=m+1}^{n} R/\langle a_i\rangle \;\cong\; \bigoplus_{j=1}^{m} R/\langle b_j\rangle \;=\; \bigoplus_{j=1}^{m} R/\langle a_j\rangle.$$

Wiederum kann man mit Satz 5.3.8 eine Längenberechnung durchführen, und erhält $R/\langle a_n\rangle = \{0\}$; Widerspruch zu $a_n \notin R^*$. □

Aufgaben zu Abschnitt 5.3.

Aufgabe 5.3.12. Als abelsche Gruppe ist $(\mathbb{Q}, +)$ ist ein $\mathbb{Z}$-Modul. Zeige: $(\mathbb{Q}, +)$ ist torsionsfrei, aber nicht frei.

Aufgabe 5.3.13. Berechne die Länge des $\mathbb{Z}$-Moduls $\mathbb{Z}/36\mathbb{Z}$. Gib eine Kette maximaler Länge in $\mathbb{Z}/36\mathbb{Z}$ an.

5.4. **Der Elementarteilersatz.**

Satz 5.4.1 (Elementarteilersatz)**.** *Es seien R ein Hauptidealring, F ein freier R-Modul von endlichem Rang und $M \leq_R F$ ein Untermodul. Dann gibt es eine Basis $(v_1, \ldots, v_n)$ von F und Elemente $a_1, \ldots, a_m \in R$, sodass*

(i) *$(a_1 v_1, \ldots, a_m v_m)$ eine Basis für M ist,*
(ii) *$a_i | a_{i+1}$ für $1 \leq i \leq m-1$ gilt.*

Die Elemente $a_1, \ldots, a_m \in R$ (auch die Elementarteiler *von M genannt) sind durch diese Eigenschaften bis auf Assoziiertheit eindeutig bestimmt. Weiter gilt*

$$\widetilde{M} \;:=\; \mathrm{Lin}(v_1, \ldots, v_m) \;=\; \{v \in F;\; rv \in M \text{ für ein } 0 \neq r \in R\},$$

$$\widetilde{M}/M \;\cong\; \bigoplus_{i=1}^{m} R/\langle a_i \rangle.$$

Bemerkung 5.4.2. Es seien R ein K1-Ring, F ein freier R-Modul und F^* der zugehörige duale R-Modul. Dann definiert jedes $v \in F$ ein Ideal

$$\mathfrak{a}_v \;:=\; \{u(v);\; u \in F^*\} \;\leq_R\; R.$$

Beweis. Wir müssen zeigen, dass $\mathfrak{a}_v$ tatsächlich ein Ideal in R ist. Dies ergibt sich jedoch sofort mit

$$u(v) + u'(v) \;=\; (u+u')(v), \qquad a(u(v)) \;=\; (au)(v).$$

□

Definition 5.4.3. Es seien R ein Hauptidealring und F ein freier R-Modul. Ein *Inhalt* eines Elementes $v \in F$ ist ein Erzeuger des Ideals

$$\mathfrak{a}_v \;=\; \{u(v);\; u \in F^*\} \;\leq_R\; R.$$

Die Menge aller Inhalte von $v \in F$ bezeichnen wir mit $\mathrm{cont}(v)$. Wir nennen $v \in F$ *primitiv*, falls $\mathrm{cont}(v) = R^*$ gilt.

Bemerkung 5.4.4. Es seien R ein Hauptidealring, F ein freier R-Modul und $v \in F$.

(i) Zu jedem $c \in \mathrm{cont}(v)$ gibt es ein $u \in F^*$ mit $u(v) = c$.
(ii) Für jedes $c \in \mathrm{cont}(v)$ und jedes $u \in F^*$ gilt $c | u(v)$.
(iii) Je zwei Elemente $c, c' \in \mathrm{cont}(v)$ sind assoziiert zueinander.
(iv) Für jedes $a \in R$ gilt $\mathrm{cont}(av) = a\,\mathrm{cont}(v)$.

Lemma 5.4.5. *Es seien R ein Hauptidealring, F ein freier R-Modul und $M \leq_R F$ ein Untermodul. Dann gibt es ein Element $v_0 \in M$ minimalen Inhalts, d.h., jedes $c_0 \in \mathrm{cont}(v_0)$ teilt jedes $c \in \mathrm{cont}(v)$ für beliebiges $v \in M$.*

Beweis. Wir betrachten die Menge der Ideale $\langle \mathrm{cont}(v) \rangle \leq_R R$, wobei $v \in M$. Da R als Hauptidealring noethersch ist, gibt es ein maximales Element $\langle \mathrm{cont}(v_0) \rangle$ unter diesen Idealen. Wir zeigen, dass $v_0 \in M$ die gewünschte Eigenschaft besitzt.

Nach Bemerkung 5.4.4 (i) gibt es eine Linearform $u_0 \in F^*$ mit $u_0(v_0) \in \mathrm{cont}(v_0)$. Wiederum nach Bemerkung 5.4.4 (i) genügt es zu zeigen, dass $u_0(v_0)$ jedes $u(v)$ teilt, wobei $v \in M$ und $u \in F^*$.

In einem ersten Schritt zeigen wir, dass $u_0(v_0) | u_0(v)$ für jedes $v \in M$ gilt. Zum Nachweis dieser Aussage, sei $v \in M$ gegeben. Wir wählen dann $a, b \in R$ mit

$$d \;:=\; a u_0(v_0) + b u_0(v) \;\in\; \mathrm{ggT}(u_0(v_0), u_0(v)).$$

Nach 5.4.4 (ii) ist jedes $c \in \operatorname{cont}(av_0+bv)$ ein Teiler von $d = u_0(av_0+bv)$ und somit auch von $u_0(v_0)$. Wir haben also

$$\langle \operatorname{cont}(v_0) \rangle \ \subseteq \ \langle \operatorname{cont}(av_0 + bv) \rangle \ \ni \ d.$$

Nach Wahl von v_0 muss Gleichheit gelten. Das bedeutet $d \in \langle \operatorname{cont}(v_0) \rangle$. Wir erhalten also $u_0(v_0)|d$ und somit $u_0(v_0)|u_0(v)$.

Im zweiten Schritt zeigen wir, dass $u_0(v_0)|u(v)$ für jede Linearform $u \in F^*$ gilt. Wir betrachten dazu

$$v' \ := \ v - \frac{u_0(v)}{u_0(v_0)} v_0, \qquad u' \ := \ u - \frac{u(v_0)}{u_0(v_0)} u_0.$$

Nach Schritt 1 ist v' wohldefiniert, und u' existiert wegen 5.4.4 (ii). Eine leichte Rechnung ergibt

$$u_0(v') \ = \ 0, \qquad u'(v_0) \ = \ 0.$$

Wendet man die zweite Identität und nochmals Schritt 1 an, so erhält man

$$u'(v') \ = \ u'(v) \ = \ u(v) - \frac{u(v_0)}{u_0(v_0)} u_0(v) \ = \ u(v) - \frac{u(v_0)}{u_0(v_0)} \frac{u_0(v)}{u_0(v_0)} u_0(v_0).$$

Insbesondere genügt es zu zeigen, dass $u_0(v_0)$ Teiler von $u'(v')$ ist. Dazu seien $a', b' \in R$ mit

$$d' \ := \ a' u_0(v_0) + b' u'(v') \ \in \ \operatorname{ggT}(u_0(v_0), u'(v')).$$

Unter Verwendung von $u_0(v') = 0$ und $u'(v_0) = 0$ erhalten wir

$$d' \ = \ a' u_0(v_0) + b' u'(v') \ = \ (u_0 + u')(a' v_0 + b' v').$$

Nach 5.4.4 (ii) ist jedes $c' \in \operatorname{cont}(a'v_0 + b'v')$ ein Teiler von d' und somit auch von $u_0(v_0)$. Es folgt

$$\langle u_0(v_0) \rangle \ = \ \langle \operatorname{cont}(v_0) \rangle \ \subseteq \ \langle \operatorname{cont}(a'v_0 + b'v') \rangle \ \ni \ d'.$$

Nach Wahl von v_0 gilt Gleichheit der Ideale. Das impliziert $u_0(v_0)|d'$ und somit $u_0(v_0)|u'(v')$. □

Lemma 5.4.6. *Es seien R ein Hauptidealring, F ein freier R-Modul von endlichem Rang. Dann gibt es zu jedem $v \in F$ ein primitives $v' \in F$ mit $v \in \operatorname{cont}(v) \cdot v'$.*

Beweis. Es sei $(v_1, \ldots, v_n)$ eine Basis für F. Entwickeln von v nach dieser Basis liefert eine Darstellung

$$v \ = \ a_1 v_1 + \ldots + a_n v_n, \qquad a_1, \ldots, a_n \ \in \ R.$$

Da R ein Hauptidealring ist, gibt es einen größten gemeinsamen Teiler d für $a_1, \ldots, a_n$. Wir setzen

$$v' \ := \ a_1' v_1 + \ldots + a_n' v_n, \qquad a_i' \ := \ \frac{a_i}{d}.$$

Dann sind die Elemente $a_1', \ldots, a_n'$ teilerfremd und somit erhalten wir eine Darstellung

$$1 \ = \ b_1 a_1' + \ldots + b_n a_n', \qquad b_1, \ldots, b_n \ \in \ R.$$

Bezeichnet nun $(v_1^*, \ldots, v_n^*)$ die zu $(v_1, \ldots, v_n)$ duale Basis von $F^* = \operatorname{Hom}(F, R)$, so erhalten wir mit $u' := b_1 v_1^* + \ldots + b_n v_n *$:

$$u'(v') \ = \ \sum_{i,j} b_i v_i^*(a_j' v_j) \ = \ \sum_{i=1}^{n} b_i a_i' \ = \ 1.$$

□

Lemma 5.4.7. *Es seien R ein Hauptidealring, F ein freier R-Modul und $\{0\} \neq M \leq_R F$ ein Untermodul. Sind ein Element $m_1 \in M$ minimalen Inhalts und ein primitives Element $v_1 \in F$ mit $m_1 \in \mathrm{cont}(m_1)v_1$ gegeben, so gibt es einen Untermodul $F' \leq_R F$ und direkte Summenzerlegungen*

$$F \;\cong\; Rv_1 \;\oplus\; F', \qquad M \;\cong\; Rm_1 \;\oplus\; (F' \cap M).$$

Beweis. Wir wählen eine Linearform $u_1 \in F^*$ mit $u_1(v_1) \in \mathrm{cont}(v_1) = R^*$ und arbeiten mit deren Kern

$$F' \;:=\; \mathrm{Kern}(u_1) \;\leq_R F.$$

Wir zeigen zunächst $F \cong Rv_1 \oplus F'$. Da $u_1(v_1) \neq 0$ gilt und R ein Integritätsring ist, erhalten wir

$$Rv_1 \cap F' \;=\; \{rv_1;\; r \in R,\; ru_1(v_1) = 0\} \;=\; \{0\}$$

Wir müssen also nur noch $F = Rv_1 + F'$ nachweisen. Wegen $u_1(v_1) \in R^*$ haben wir für jedes $v \in F$ eine wohldefinierte Zerlegung:

$$v \;=\; \underbrace{\frac{u_1(v)}{u_1(v_1)}v_1}_{\in Rv_1} \;+\; \underbrace{\left(v - \frac{u_1(v)}{u_1(v_1)}v_1\right)}_{\in F'}.$$

Wir kommen zur Isomorphie $M \cong Rm_1 \oplus (F' \cap M)$. Zunächst erhalten wir mit obiger Überlegung

$$Rm_1 \cap (F' \cap M) \;\subseteq\; Rv_1 \cap F' \;=\; \{0\}.$$

Für den Nachweis von $M = Rm_1 + (F' \cap M)$ verwenden wir, dass m_1 minimalen Inhalt besitzt: Für jedes $m \in M$ erhält man damit eine wohldefinierte Zerlegung

$$m \;=\; \underbrace{\frac{u_1(m)}{u_1(m_1)}m_1}_{\in Rm_1} \;+\; \underbrace{\left(m - \frac{u_1(m)}{u_1(m_1)}m_1\right)}_{\in F' \cap M}.$$

□

Satz 5.4.8. *Es seien R ein Hauptidealring und F ein R-Modul von endlichem Rang. Ist F frei, so ist auch jeder Untermodul $M \leq_R F$ frei.*

Beweis. Zunächst vermerken wir, dass offensichtlich $\mathrm{rg}_R(M) \leq \mathrm{rg}_R(F)$ gilt. Insbesondere haben wir $s := \mathrm{rg}_R(M) < \infty$, und wir können den Satz mittels Induktion über s beweisen.

Zu $s = 0$. In diesem Fall ist M ein Torsionsmodul. Andererseits ist F frei und somit torsionsfrei. Folglich ist $M \leq_R F$ ebenfalls torsionsfrei. Das bedeutet $M = \{0\}$. Der triviale Modul ist nach Definition frei.

Für den Induktionsschritt verwenden wir Lemma 5.4.5 bis 5.4.7 und erhalten ein Element minimalen Inhalts $0 \neq m_1 \in M$, einen Untermodul $F' \leq_R F$ und eine Zerlegung

$$M \;\cong\; Rm_1 \;\oplus\; (F' \cap M).$$

Beide Summanden sind torsionsfrei. Für Rm_1 bedeutet dies, dass $\{m_1\}$ eine Basis ist. Folglich ist Rm_1 frei und vom Rang eins. Satz 5.2.12 liefert daher $\mathrm{rg}_R(F' \cap M) = s - 1$. Nach Induktionsvoraussetzung ist also auch $F' \cap M$ frei. Als direkte Summe zweier freier Moduln ist M wieder frei. □

Beweis des Elementarteilersatzes 5.4.1. Man beachte, dass $\mathrm{rg}_R(M) < \infty$ gilt. Wir können also Induktion über $\mathrm{rg}_R(M)$ verwenden. Im Falle $\mathrm{rg}(M) = 0$ gilt $M = \{0\}$, und es ist nichts zu zeigen.

Gilt $\mathrm{rg}_R(M) > 0$, so wenden wir Lemma 5.4.5 bis 5.4.7 an und erhalten Elemente $m_1 \in M$ und $v_1 \in F$ sowie einen Untermodul $F' \leq_R M$ und direkte Summenzerlegungen

$$F \;=\; Rv_1 \;\oplus\; F', \qquad M \;=\; Rm_1 \;\oplus\; (F' \cap M).$$

Der Modul $F' \leq_R F$ besitzt endlichen Rang und ist nach Satz 5.4.8 frei. Weiter besitzt Rm_1 nach Satz 5.2.13 den Rang 1. Folglich besitzt $F' \cap M$ nach Satz 5.2.12 den Rang $\mathrm{rg}_R(M) - 1$. Nach Induktionsvoraussetzung gibt es also eine Basis $(v_2, \ldots, v_n)$ von F' und Elemente $a_2, \ldots, a_m \in R$ mit

(i) $(a_2v_2, \ldots, a_mv_m)$ ist eine Basis für $F' \cap M$,
(ii) $a_i | a_{i+1}$ für $2 \leq i \leq m-1$.

Wir wählen $a_1 \in \mathrm{cont}(m_1)$ mit $m_1 = a_1v_1$. Dann ist nur noch $a_1 | a_2$ nachzuweisen. Dies ergibt sich wie folgt. Da $v_2 \in F$ als Basiselement primitiv ist, gilt

$$a_2 \;\in\; a_2\mathrm{cont}(v_2) \;=\; \mathrm{cont}(a_2v_2).$$

Da $m_1 \in M$ minimalen Inhalt besitzt, ist $a_1 \in \mathrm{cont}(m_1)$ ein Teiler von $a_2 \in \mathrm{cont}(av_2)$.

Wir verifizieren die Zusatzaussagen über den Untermodul $\widetilde{M} = \mathrm{Lin}(v_1, \ldots, v_m)$, nämlich

$$\widetilde{M} \;=\; \{v \in F;\; rv \in M \text{ für ein } 0 \neq r \in R\}, \qquad \widetilde{M}/M \;\cong\; \bigoplus_{i=1}^{m} R/\langle a_i \rangle.$$

Die erste ist offensichtlich, und für die zweiten wende man den Homomorphiesatz an auf den Epimorphismus

$$\widetilde{M} \to \bigoplus_{i=1}^{m} R/\langle a_i \rangle, \qquad \sum_{i=1}^{m} c_iv_i \mapsto (c_1 + \langle a_1 \rangle, \ldots, c_m + \langle a_m \rangle).$$

Wir kommen zur Eindeutigkeitsaussage des Elementarteilersatzes. Nehmen wir an, es seien zwei Basen $v_1, \ldots, v_n$ bzw. $w_1, \ldots, w_{n'}$ mit entsprechenden Elementen $a_1, \ldots, a_m$ bzw. $b_1, \ldots, b_{m'}$ wie in der Aussage gegeben. Mit Satz 5.2.13 erhalten wir

$$n \;=\; \mathrm{rg}_R(F) \;=\; n', \qquad m \;=\; \mathrm{rg}_R(M) \;=\; m'.$$

Sind $a_1, \ldots, a_l$ bzw. $b_1, \ldots, b_k$ die jeweiligen Einheiten unter den Elementen a_i bzw. b_j, so erhalten wir Isomorphismen

$$\bigoplus_{i=l+1}^{m} R/\langle a_i \rangle \;\cong\; \widetilde{M}/M \;\cong\; \bigoplus_{j=k+1}^{m} R/\langle b_j \rangle$$

Lemma 5.3.11 zeigt dann, dass erstens $l = k$ gelten muss, und zweitens erhalten wir $a_i \sim b_i$ für $i = 1, \ldots, m$. □

Aufgaben zu Abschnitt 5.4.

Aufgabe 5.4.9. Es seien R ein Hauptidealring, F ein freier R-Modul mit einer Basis $(v_1, \ldots, v_n)$ und

$$v \;=\; a_1 v_1 + \ldots + a_n v_n \;\in\; F$$

ein beliebiges Element, wobei $a_1, \ldots, a_n \in R$. Dann ist die Menge aller Inhalte von v gegeben durch

$$\mathrm{cont}(v) \quad = \quad \mathrm{ggT}(a_1, \ldots, a_n).$$

Insbesondere ist v genau dann primitiv, wenn $a_1, \ldots, a_n$ teilerfremd sind. Weiter sind die Elemente einer Basis stets primitiv.

Aufgabe 5.4.10. Bestimme die Elementarteiler des folgenden Untermoduls

$$M \;:=\; \mathrm{Lin}\,((2,0,2),\ (2,-3,8),\ (0,3,-6)) \;\leq_R\; \mathbb{Z}^3.$$

Aufgabe 5.4.11 (Smith-Normalform)**.** Es seien R ein Hauptidealring und $A \in \mathrm{Mat}(n,n;R)$ eine $(n \times n)$-Matrix mit Einträgen aus R. Beweise folgende Aussagen:

(i) Es gibt über R invertierbare Matrizen $S, T \in \mathrm{Mat}(n,n;R)$ und $a_1, \ldots, a_d \in R$ mit $a_1 | a_2, \ldots, a_{d-1} | a_d$ und

$$S \cdot A \cdot T \quad = \quad \begin{bmatrix} a_1 & 0 & & \cdots & & 0 \\ 0 & \ddots & & & & 0 \\ & & a_d & & & \\ \vdots & & & 0 & & \vdots \\ & & & & \ddots & \\ 0 & 0 & & \cdots & & 0 \end{bmatrix}$$

(ii) Die Elemente $a_1, \ldots, a_d$ aus (i) sind durch ihre Eigenschaften bis auf Assoziiertheit eindeutig bestimmt.

Aufgabe 5.4.12. Es seien R ein Hauptidealring, F ein freier R-Modul endlichen Ranges und $M \leq_R F$ ein Untermodul. Beweise die Äquivalenz folgender Aussagen:

(i) Der Restklassenmodul F/M ist torsionsfrei.
(ii) Die Elementarteiler von M sind Einheiten.
(iii) Es gibt einen Untermodul $M' \leq_R F$ mit $M \cap M' = \{0\}$ und $F = M + M'$.

5.5. **Die Struktursätze.**

Satz 5.5.1. *Es seien R ein Hauptidealring und M ein endlich erzeugter R-Modul. Dann gibt es eine direkte Zerlegung*

$$M \;\cong\; F \,\oplus\, T(M)$$

mit einem endlich erzeugten freien R-Untermodul F und dem Torsionsmodul $T(M) \leq_R M$. Es gilt weiter

$$T(M) \;\cong\; \bigoplus_{i=1}^{m} R/\langle a_i\rangle$$

mit nichtverschwindenden Nichteinheiten $a_1, \ldots, a_m \in R$, sodass $a_i | a_{i+1}$ gilt; die $a_1, \ldots, a_m \in R$ sind dabei bis auf Assoziiertheit eindeutig bestimmt.

Lemma 5.5.2. *Es seien R ein K1-Ring, M_i, $i \in I$, R-Moduln und $N_i \leq_R M_i$ Untermoduln. Dann gilt*

$$\left(\bigoplus_{i\in I} M_i\right) \Big/ \left(\bigoplus_{i\in I} N_i\right) \;\cong\; \bigoplus_{i\in I} M_i/N_i.$$

Beweis. Man hat einen kanonischen surjektiven Homomorphismus von R-Moduln:

$$\pi\colon \bigoplus_{i\in I} M_i \;\to\; \left(\bigoplus_{i\in I} M_i\right) \Big/ \left(\bigoplus_{i\in I} N_i\right), \qquad (u_i)_{i\in I} \;\mapsto\; (u_i + N_i)_{i\in I}$$

mit $\ker(\pi) = \bigoplus_{i\in I} N_i$. Der Homomorphiesatz 5.1.21 liefert die Behauptung. □

Beweis von Satz 5.5.1. Es seien $u_1, \ldots, u_n \in M$ Erzeugende für M. Dann erhalten wir einen surjektiven Homomorphismus von R-Moduln:

$$\pi\colon \;\to\; M, \qquad (r_1, \ldots, r_n) \;\mapsto\; r_1u_1 + \ldots + r_nu_n.$$

Der Homomorphiesatz 5.1.21 liefert $M \cong R^n/N$ mit $N := \mathrm{Kern}(\pi)$. Nach Satz 5.4.1 gibt es eine Basis $(v_1, \ldots, v_n)$ für R^n und $a_1, \ldots, a_s \in R \setminus \{0_R\}$ mit $a_i | a_{i+1}$ und

$$N \;=\; R\cdot a_1 \cdot v_1 \,\oplus\, \ldots \,\oplus\, R\cdot a_s \cdot v_s.$$

Mit Hilfe von Lemma 5.5.2 können wir also den Modul $M \cong R^n/N$ gut beschreiben: Sind $a_1, \ldots, a_k$ die Einheiten unter den a_i, so erhalten wir

$$\begin{aligned}
M \;&\cong\; R^n/N \\
&\cong\; (R\cdot v_1 \oplus \ldots \oplus R\cdot v_n) \,/ (R\cdot a_1\cdot v_1 \,\oplus\, \ldots \,\oplus\, R\cdot a_s\cdot v_s, R\cdot v_{s+1} \oplus \ldots \oplus R\cdot v_n) \\
&\cong\; \bigoplus_{i=1}^{k} R/\langle a_i\rangle \;\oplus\; \bigoplus_{i=k+1}^{s} R/\langle a_i\rangle \;\oplus\; R^{n-s} \\
&\cong\; R^{n-s} \;\oplus\; \bigoplus_{i=k+1}^{s} R/\langle a_i\rangle.
\end{aligned}$$

Dabei ist der erste Summand ein freier R-Modul, und der zweite Summand ist der Torsionsmodul; er wird durch das Element $0 \neq a_{k+1} \cdots a_s$ annulliert.

Die Eindeutigkeitsaussage über die Elemente $a_{k+1}, \ldots, a_s \in R$ ist eine direkte Anwendung von Satz 5.3.11. □

Definition 5.5.3. Es seien R ein Hauptidealring, M ein R-Modul und $p \in R$ ein Primelement.

(i) Ein Element $v \in M$ heißt *p-Torsionselement*, falls $p^n \cdot v = 0$ mit einem $n \in \mathbb{Z}_{\geq 0}$ gilt.

(ii) Der *p-Torsionsmodul von M* ist die Menge $M_p \subseteq M$ aller p-Torsionselemente von M.
(iii) Falls $M = M_p$ gilt, so nennt man den Modul M selbst einen *p-Torsionsmodul*.

Satz 5.5.4. *Es seien R ein Hauptidealring, $P \subset R$ ein Primsystem und M ein endlich erzeugter R-Modul. Dann gibt es eine Zerlegung*

$$M \quad \cong \quad F \oplus \bigoplus_{p \in P} M_p,$$

mit einem endlich erzeugten freien R-Modul F und den p-Torsionsmoduln $M_p \leq_R M$; nur endlich viele M_p sind dabei nichttrivial, und jedes nichttriviale M_p ist von der Form

$$M_p \quad \cong \quad \bigoplus_{i=1}^{d(p)} R/\langle p^{\nu_{p,i}} \rangle$$

mit ganzen Zahlen $1 \leq \nu_{p,1} \leq \ldots \leq \nu_{p,d(p)}$. Die Zahlen $d(p)$ und $\nu_{p,1}, \ldots, \nu_{p,d(p)}$ sind durch den Isomorphietyp von M eindeutig bestimmt.

Beweis. Satz 5.5.1 liefert eine Zerlegung $M \cong F \oplus T(M)$ in einen freien Anteil und den Torsionsmodul sowie $0_R \neq a_1, \ldots, a_m \in R \setminus R^*$ mit $a_i | a_{i+1}$ und

$$T(M) \quad \cong \quad \bigoplus_{i=1}^{m} R/\langle a_i \rangle.$$

Wir müssen den Torsionsmodul $T(M)$ auf geeignete Weise als direkte Summe seiner p-Torsionsmoduln darstellen. Dazu betrachten wir die Primfaktorzerlegungen

$$a_i \quad = \quad c_i \prod_{p \in P} p^{\nu(p,i)}$$

mit Einheiten $c_i \in R^*$ und Exponenten $\nu(p,i) \in \mathbb{Z}_{\geq 0}$. Mit der Variante 5.3.10 des Chinesischen Restsatzes erhalten wir eine Zerlegung von R-Moduln:

$$R/\langle a_i \rangle \quad \cong \quad \bigoplus_{p \in P} R/\langle p^{\nu(p,i)} \rangle. \tag{5.2}$$

Damit gehen wir in die Zerlegung von $T(M)$ und fassen für jedes $p \in P$ alle Terme der Form $R/\langle p^{\nu(p,i)} \rangle$ zu einem Summanden zusammen. Das ergibt

$$\begin{aligned} \bigoplus_{i=1}^{m} R/\langle a_i \rangle \quad &\cong \quad \bigoplus_{i=1}^{m} \left(\bigoplus_{p \in P} R/\langle p^{\nu(p,i)} \rangle \right) \\ &\cong \quad \bigoplus_{p \in P} \left(\bigoplus_{i=1}^{m} R/\langle p^{\nu(p,i)} \rangle \right) \\ &=: \quad \overline{M}. \end{aligned}$$

Man beachte, dass wegen der Teilbarkeitsrelationen $a_i | a_{i+1}$ stets $\nu(p,i) \leq \nu(p,i+1)$ gelten muss. Für jedes $p \in P$ setzen wir

$$d(p) \quad := \quad |\{i;\ \nu_{p,i} > 0\}|,$$

und für p mit $d(p) \neq 0$ definieren wir $\nu_{p,i} := \nu(p, i + m_p)$, wobei m_p die erste Zahl mit $\nu(p, 1 + m_p) > 0$ bezeichne. Dann haben wir

$$\overline{M} \quad = \quad \bigoplus_{p \in P} \left(\bigoplus_{i=1}^{d(p)} R/\langle p^{\nu_{p,i}} \rangle \right).$$

Zum Beweis der Existenzaussage müssen wir also nur noch zeigen, dass wir den p-Torsionsmodul $\overline{M}_p \leq_R \overline{M}$ erhalten als

$$\overline{M}_p \;=\; M'_p \;:=\; \bigoplus_{i=1}^{d(p)} R/\langle p^{\nu_{p,i}}\rangle.$$

Jedes M'_p enthält nur p-Torsionselemente. Ist ein p-Torsionselement $v \in \overline{M}_p$ gegeben, so haben wir eine eindeutige Darstellung mit Elementen $v_p \in M'_p$ und $v_q \in M'_q$:

$$v \;=\; v_p + \sum_{p\neq q\in P} v_q.$$

Da v ein p-Torsionselement ist, gibt es ein $\nu \in \mathbb{Z}_{\geq 1}$ mit $p^\nu \cdot v_q = 0$ für alle $q \in P$. In jedem M'_q erhalten wir mit geeigneten $r_{q,i} \in R$:

$$0 \;=\; p^\nu \cdot v_q \;=\; p^\nu \sum_{i=1}^{d(q)} r_{q,i} + \langle q^{\nu_{q,i}}\rangle \;=\; \sum_{i=1}^{d(q)} p^\nu r_{q,i} + \langle q^{\nu_{q,i}}\rangle$$

Das bedeutet $p^\nu r_{q,i} \in \langle q^{\nu_{q,i}}\rangle$. Falls $q \neq p$ gilt, muss also $q^{\nu_{q,i}}$ stets ein Teiler von $r_{q,i}$ sein. Das bedeutet $v_q = 0$ und somit $v = v_p \in M'_p$.

Zur Eindeutigkeitsaussage: Es ist klar, dass der Isomorphietyp des p-Torsionsmoduls $M_p \leq M$ durch den von M festgelegt ist. Die Eindeutigkeit der Zahlen $d(p)$ und $\nu_{p,i}$ ergibt sich daher mit Lemma 5.3.11. □

Folgerung 5.5.5 (Hauptsatz für endlich erzeugte abelsche Gruppen)**.** *Es sei G eine endlich erzeugte abelsche Gruppe. Dann hat man eine eindeutige Darstellung*

$$G \;\cong\; \mathbb{Z}^d \;\times\; \prod_{p\in P} \left[\prod_{i=1}^{d(p)} \mathbb{Z}/p^{\nu_{p,i}}\mathbb{Z}\right]$$

wobei $P \subset \mathbb{Z}_{\geq 2}$ die Menge der Primzahlen bezeichnet, $d(p) > 0$ für höchstens endlich viele p gilt und für diese p stets $1 \leq \nu_{p,1} \leq \ldots \leq \nu_{p,d(p)}$ erfüllt ist.

Beweis. Als endlich erzeugte abelsche Gruppe ist G ein endlich erzeugter $\mathbb{Z}$-Modul, siehe Beispiel 5.1.5. Satz 5.5.4 liefert daher die gewünschte Zerlegung von G. □

Beispiel 5.5.6. Mit Hilfe der Eindeutigkeitsaussage von Satz 5.5.5 kann man oft schnell entscheiden, ob zwei gegebene abelsche Gruppen isomorph zueinander sind oder nicht, etwa

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \;\ncong\; \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}.$$

Definition 5.5.7. Es seien R ein Hauptidealring, M ein endlich erzeugter R-Modul und $T(M) \leq_R M$ der zugehörige Torsionsmodul.

(i) *Elementarteiler* für M sind nichttriviale Nichteinheiten $a_1, \ldots, a_m \in R$ mit $a_i | a_{i+1}$ und

$$T(M) \;\cong\; \bigoplus_{i=1}^{m} R/\langle a_i\rangle.$$

(ii) *Primäre Elementarteiler* für M sind Elemente $p_i^{\nu_{ij}} \in R$, wobei $p_1, \ldots, p_r \in R$ paarweise nichtassoziierte Primelemente und $1 \leq \nu_{i1} \leq \ldots \leq \nu_{id_i}$, mit

$$T(M) \;\cong\; \bigoplus_{i=1}^{r} \left(\bigoplus_{j=1}^{d_i} R/\langle p_i^{\nu_{ij}}\rangle\right)$$

Beispiel 5.5.8. Wir betrachten den $\mathbb{Z}$-Modul $M := \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$ und wollen Elementarteiler sowie primäre Elementarteiler dafür bestimmen. Mit der Variante 5.3.10 des Chinesischen Restsatzes erhalten wir

$$M \cong \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$$

Die letzte Darstellung ist wie in Satz 5.5.4. Folglich sind $2^1, 2^2, 3^1$ primäre Elementarteiler für M. Um Elementarteiler zu gewinnen, schreiben wir die primären Elementarteiler in ein Schema

$$\begin{array}{lll} p = 2: & 2, & 2^2, \\ p = 3: & 1, & 3. \end{array}$$

Aufmultiplizieren der Spalten ergibt dann Elementarteiler $a_1 = 2 \cdot 1 = 2$ und $a_2 = 2^2 \cdot 3 = 12$ für M. Um dies zu verifizieren, verwenden wir nochmals Variante 5.3.10 des Chinesischen Restsatzes: Sie liefert

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \cong M.$$

Bemerkung 5.5.9. Es seien R ein Hauptidealring und M ein endlich erzeugter R-Modul.

(i) Hat man primäre Elementarteiler $p_i^{\nu_{ij}}$, wobei $1 \le i \le r$ und $1 \le \nu_{i1} \le \ldots \le \nu_{id_i}$, für M vorliegen, so betrachtet man das Schema

$$\begin{array}{ccccccc} 1 & \ldots & 1 & p_1^{\nu_{11}} & \ldots & p_1^{\nu_{1d_1}} \\ & & \vdots & & & \\ p_m^{\nu_{m1}} & \ldots & & & \ldots & p_m^{\nu_{md_m}} \\ & & \vdots & & & \\ 1 & \ldots & 1 & p_r^{\nu_{r1}} & \ldots & p_r^{\nu_{rd_r}} \end{array}$$

wobei d_m maximal inter den d_i. Aufmultiplizieren der Einträge aus den Spalten liefert dann Elementarteiler $a_r = p_1^{\nu_{1d_1}} \cdots p_r^{\nu_{rd_r}}$, etc., für M.

(ii) Hat man Elementarteiler $a_1, \ldots, a_m$ für M vorliegen, so wählt man ein Primsystem $P \subset R$ und betrachtet die Primfaktorzerlegungen

$$a_1 = c_1 \cdot p_1^{\nu_{11}} \cdots p_r^{\nu_{r1}}, \quad \ldots, \quad a_m = c_m \cdot p_1^{\nu_{1d_1}} \cdots p_r^{\nu_{rd_r}}.$$

Die darin auftretenden Primpotenzen $p_i^{\nu_{ij}}$ sind dann primäre Elementarteiler für M, wobei die $p_i^{\nu_{ij}} = 1$ jeweils zu entfernen sind.

Aufgaben zu Abschnitt 5.5.

Aufgabe 5.5.10. Bestimme Elementarteiler und primäre Elementarteiler für die folgenden $\mathbb{Z}$-Moduln:

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}, \qquad \mathbb{Z}/4\mathbb{Z}, \qquad \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}, \qquad \mathbb{Z}/72\mathbb{Z}.$$

Aufgabe 5.5.11. Bestimme, bis auf Isomorphie, alle abelschen Gruppen der Ordnungen 8, 12, 16, und 18.

6. Grundlagen der Körpertheorie

6.1. **Grundbegriffe.**

Erinnerung 6.1.1. Ein *Körper* ist ein K1-Ring $\mathbb{K}$ mit $1_{\mathbb{K}} \neq 0_{\mathbb{K}}$, sodass jedes Element aus $\mathbb{K} \setminus \{0_{\mathbb{K}}\}$ eine Einheit ist. Einige Beispiele:

- die Körper $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ der rationalen, reellen, bzw. komplexen Zahlen,
- die Körper $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$, wobei $p \in \mathbb{Z}_{\geq 2}$ eine Primzahl ist,
- der *Quotientenkörper* $Q(R)$ eines beliebigen Integritätsringes R,
- der *Körper der rationalen Funktionen* über einem Körper $\mathbb{K}$:

$$\mathbb{K}(T_1, \ldots, T_n) \quad := \quad Q(\mathbb{K}[T_1, \ldots, T_n]).$$

Ein *Homomorphismus von Körpern* $\mathbb{L} \to \mathbb{K}$ ist ein Homomorphismus der K1-Ringe $\mathbb{L}$ und $\mathbb{K}$. Die *komplexe Konjugation*

$$\mathbb{C} \ \to \ \mathbb{C}, \qquad z = x + Iy \ \mapsto \ \bar{z} = x - Iy$$

ist ein Beispiel für einen Körperhomomorphismus. Körperhomomorphismen sind stets injektiv.

Definition 6.1.2. Es sei R ein K1-Ring. Für $k \in \mathbb{Z}_{>0}$ setze $k \cdot 1_R := \sum_{i=1}^{k} 1_R$. Die *Charakteristik* des Ringes R ist dann definiert als

$$\mathrm{Char}(R) \quad := \quad \begin{cases} 0, & k \cdot 1_R \neq 0_R \text{ für alle } k \in \mathbb{Z}_{>0}, \\ \min(k \in \mathbb{Z}_{>0};\ k \cdot 1_R = 0_R) & \text{sonst.} \end{cases}$$

Bemerkung 6.1.3. Es sei R ein K1-Ring mit $0 \cdot 1_r := 0_R$ und $k \cdot 1_R := -|k| \cdot 1_R$ für $k < 0$ erhalten wir einen Ringhomomorphismus

$$\kappa \colon \mathbb{Z} \to R, \qquad k \ \mapsto \ k \cdot 1_R.$$

Die Charakteristik eines K1-Ringes R ist dann das eindeutig bestimmte nichtnegative Erzeugende des Ideals $\mathrm{Kern}(\kappa) \leq_{\mathbb{Z}} \mathbb{Z}$.

Beispiel 6.1.4. Es gilt:

(i) $\mathrm{Char}(\mathbb{Q}) = \mathrm{Char}(\mathbb{R}) = \mathrm{Char}(\mathbb{C}) = 0$.
(ii) $\mathrm{Char}(\mathbb{Z}/n\mathbb{Z}) = n$ für jede ganze Zahl $n \in \mathbb{Z}_{>0}$.

Definition 6.1.5. Es sei $\mathbb{K}$ ein Körper. Ein *Unterkörper* von $\mathbb{K}$ ist ein Unterring $\mathbb{L} \subseteq \mathbb{K}$, sodass $a^{-1} \in \mathbb{L}$ für jedes $0 \neq a \in \mathbb{L}$ gilt.

Bemerkung 6.1.6. Ist $\mathbb{L}$ Unterkörper eines Körpers $\mathbb{K}$, so gilt $\mathrm{Char}(\mathbb{L}) = \mathrm{Char}(\mathbb{K})$.

Konstruktion 6.1.7. Es seien $\mathbb{K}$ ein Körper und $\mathbb{L}_i$, $i \in I$, eine Familie von Unterkörpern. Dann ist der Durchschnitt

$$\bigcap_{i \in I} \mathbb{L}_i \quad \subseteq \quad \mathbb{K}$$

wieder ein Unterkörper von $\mathbb{K}$. Er ist der größte Unterkörper von $\mathbb{K}$, der in allen $\mathbb{L}_i$, $i \in I$, enthalten ist.

Konstruktion 6.1.8. Es sei $\mathbb{K}$ ein Körper. Dann besitzt $\mathbb{K}$ einen eindeutig bestimmten kleinsten Unterkörper:

$$\mathbb{P}_{\mathbb{K}} \ := \bigcap_{\substack{\mathbb{L} \subseteq \mathbb{K} \\ \text{Unterkörper}}} \quad = \ \left\{ m \cdot 1_{\mathbb{K}} \cdot (n \cdot 1_{\mathbb{K}})^{-1};\ m, n \in \mathbb{Z},\ n \cdot 1_{\mathbb{K}} \neq 0_{\mathbb{K}} \right\} \ \subseteq \ \mathbb{K}.$$

Man nennt $\mathbb{P}_{\mathbb{K}}$ den *Primkörper* von $\mathbb{K}$. Er ist durch die Charakteristik von $\mathbb{K}$ bis auf Isomorphie festgelegt: Es gilt

$$\begin{aligned} \mathrm{Char}(\mathbb{K}) = 0 \quad &\iff \quad \mathbb{P}_{\mathbb{K}} \ \cong \ \mathbb{Q}, \\ \mathrm{Char}(\mathbb{K}) = p > 0 \quad &\iff \quad \mathbb{P}_{\mathbb{K}} \ \cong \ \mathbb{F}_p. \end{aligned}$$

Insbesondere ist die Charakteristik eines Körpers eine Primzahl, sofern sie von Null verschieden ist.

Beweis. Als kleinster Unterkörper von $\mathbb{K}$ besteht $\mathbb{P}_\mathbb{K}$ offensichtlich genau aus den Elementen $m \cdot 1_\mathbb{K} \cdot (n \cdot 1_\mathbb{K})^{-1}$ mit $m, n \in \mathbb{Z}$ und $n \cdot 1_\mathbb{K} \neq 0$. Falls $\operatorname{Char}(\mathbb{K}) = 0$ gilt, ist der Homomorphismus $\kappa\colon \mathbb{Z} \to \mathbb{K}$ aus Bemerkung 6.1.3 injektiv und somit liefert Satz 3.1.26 einen Isomorphismus $\mathbb{Q} \to \mathbb{P}_\mathbb{K}$. Falls $\operatorname{Char}(\mathbb{K}) = p$ mit $p \in \mathbb{Z}_{\geq 1}$ gilt, ist das Bild $\kappa(\mathbb{Z})$ nach Bemerkung 6.1.3 und dem Homomorphiesatz 3.3.16 isomorph zu $\mathbb{Z}/p\mathbb{Z}$. Als Unterring von $\mathbb{K}$ ist $\kappa(\mathbb{Z})$ ein Integritätsring. Das ist nur möglich, wenn p eine Primzahl ist. In diesem Fall ist $\mathbb{Z}/p\mathbb{Z}$ bereits ein Körper und es folgt $\mathbb{Z}/p\mathbb{Z} \cong \kappa(\mathbb{Z}) = \mathbb{P}_\mathbb{K}$. □

Definition 6.1.9. Eine *Körpererweiterung* ist ein Paar $k \subseteq \mathbb{K}$, wobei $\mathbb{K}$ ein Körper und k ein Unterkörper von $\mathbb{K}$ ist.

Beispiel 6.1.10. Die Paare $\mathbb{Q} \subseteq \mathbb{R}$ und $\mathbb{Q} \subseteq \mathbb{C}$ sowie $\mathbb{R} \subseteq \mathbb{C}$ sind Körpererweiterungen.

Bemerkung 6.1.11. Für jeden Körper $\mathbb{K}$ liefert der zugehörige Primkörper eine Körpererweiterung $\mathbb{P}_\mathbb{K} \subseteq \mathbb{K}$.

Bemerkung 6.1.12. Ist $k \subseteq \mathbb{K}$ eine Körpererweiterung, so ist $\mathbb{K}$ auf kanonische Weise ein k-Vektorraum: Die Addition von Elementen $b, b' \in \mathbb{K}$ ist die übliche Addition in $\mathbb{K}$ und die Skalarmultiplikation $a \cdot b$ für $a \in k$ und $b \in \mathbb{K}$ ist die übliche Multiplikation in $\mathbb{K}$.

Definition 6.1.13. Der *Grad* einer Körpererweiterung $k \subseteq \mathbb{K}$ ist definiert als die Dimension des k-Vektorraumes $\mathbb{K}$:

$$[\mathbb{K} : k] \quad := \quad \dim_k(\mathbb{K}).$$

Gilt $[\mathbb{K} : k] < \infty$, so nennt man $k \subseteq \mathbb{K}$ eine *Körpererweiterung von endlichem Grad*, oder auch eine *endliche Körpererweiterung*.

Beispiel 6.1.14. Die Körpererweiterung $\mathbb{R} \subseteq \mathbb{C}$ besitzt den Grad $[\mathbb{C} : \mathbb{R}] = 2$, denn $(1, I)$ ist eine Basis des $\mathbb{R}$-Vektorraumes $\mathbb{C}$.

Konstruktion 6.1.15. Es seien k ein Körper und $f \in k[T]$ ein irreduzibles Polynom. Dann erhält man einen Körper $\mathbb{K}$ und einen kanonischen Monomorphismus $k \to \mathbb{K}$ durch

$$\mathbb{K} \;:=\; k[T]/\langle f \rangle, \qquad\qquad k \to \mathbb{K}, \quad a \mapsto aT^0 + \langle f \rangle.$$

Wir identifizieren k mit seinem Bild $kT^0 + \langle f \rangle$ in $\mathbb{K}$ und erhalten so eine Körpererweiterung $k \subseteq \mathbb{K}$. Man hat einen kanonischen Isomorphismus von k-Vektorräumen:

$$\alpha\colon \bigoplus_{i=0}^{\deg(f)-1} kT^i \;\to\; \mathbb{K}, \qquad\qquad h \;\mapsto\; h + \langle f \rangle.$$

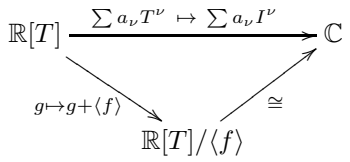
Insbesondere besitzen beide k-Vektorräume dieselbe Dimension, d.h., wir erhalten $[\mathbb{K} : k] = \deg(f)$ für den Grad der Körpererweiterung $k \subseteq \mathbb{K}$.

Beweis. Das Polynom $f \in k[T]$ ist ein irreduzibles Element des Hauptidealringes $k[T]$ und somit ist $\mathbb{K} = k[T]/\langle f \rangle$ ein Körper; siehe Folgerung 4.1.23. Die Abbildung $k \to \mathbb{K}$ ist die Komposition der kanonischen Homomorphismen $k \to k[T]$ und $k[T] \to k[T]/\langle f \rangle$. Wie jeder Körperhomomorphismus ist sie injektiv; siehe Folgerung 3.3.12.

Die Abbildung α ist offensichtlich ein Homomorphismus von $\mathbb{K}$-Vektorräumen. Da $\langle f \rangle$ außer dem Nullpolynom nur Polynome vom Grad mindestens $\deg(f)$ enthält,

ist α injektiv. Um zu sehen, dass α auch surjektiv ist, sei $g+\langle f\rangle \in \mathbb{K}$ gegeben. Division mit Rest liefert eine Darstellung $g = qf + r$ mit Polynomen $q, r \in k[T]$, sodass $r = 0$ oder $\deg(r) < \deg(f)$. Dabei gilt $g + \langle f\rangle = r + \langle f\rangle = \alpha(r)$. □

Beispiel 6.1.16. Das Polynom $f = T^2 + 1 \in \mathbb{R}[T]$ ist irreduzibel und somit ist $\mathbb{R}[T]/\langle f\rangle$ ein Körper. Man hat ein kommutatives Diagramm



Dafür beachte man $I^2 = -1$ und verwende den Homomorphiesatz. Somit erhalten wir einen Isomorphismus von Körpern

$$\mathbb{R}[T]/\langle f\rangle \ \to\ \mathbb{C}, \qquad\qquad a + bT + \langle f\rangle \ \mapsto\ a + Ib.$$

Beispiel 6.1.17. Das Polynom $f = T^2 + T + \overline{1} \in \mathbb{F}_2[T]$ ist irreduzibel, denn die einzig möglichen Produkte von Polynomen vom Grad Eins in $\mathbb{F}_2[T]$ sind

$$T^2 \ =\ T \cdot T, \qquad T^2 + T \ =\ (T + \overline{1}) \cdot T \qquad T^2 + \overline{1} \ =\ (T + \overline{1}) \cdot (T + \overline{1}).$$

Damit ist $\mathbb{F}_4 := \mathbb{F}_2[T]/\langle f\rangle$ ein Körper, $\mathbb{F}_2 \subseteq \mathbb{F}_4$ ist der Primkörper und für $\eta := T + \langle f\rangle$ ist $(\overline{1}, \eta)$ eine $\mathbb{F}_2$-Basis für $\mathbb{F}_4$. Insbesondere gilt

$$[\mathbb{F}_4 : \mathbb{F}_2] \ =\ 2, \qquad\qquad |\mathbb{F}_4| \ =\ 4.$$

Die Elemente von $\mathbb{F}_4$ sind $\overline{0}, \overline{1}, \eta, \overline{1} + \eta$. Für das Produkt η^2 erhalten wir

$$\eta^2 \ =\ T^2 + \langle f\rangle \ =\ T + \overline{1} + \langle f\rangle \ =\ 1 + \eta.$$

Satz 6.1.18. *Es sei $\mathbb{K}$ ein endlicher Körper. Dann gilt $\mathrm{Char}(\mathbb{K}) = p$ mit einer Primzahl $p \in \mathbb{Z}$ und es gibt ein $n \in \mathbb{Z}_{\geq 1}$, sodass $|\mathbb{K}| = p^n$ gilt.*

Beweis. Für den Primkörper $\mathbb{P}_\mathbb{K}$ von $\mathbb{K}$ haben wir $\mathbb{P}_\mathbb{K} \cong \mathbb{F}_p$; insbesondere hat $\mathbb{P}_\mathbb{K}$ genau p Elemente. Da $\mathbb{K}$ endlich ist, ist der $\mathbb{P}_\mathbb{K}$-Vektorraum $\mathbb{K}$ endlichdimensional. Es gilt also $\mathbb{K} \cong \mathbb{P}_\mathbb{K}^n$ mit einem $n \in \mathbb{Z}_{\geq}1$. Damit gilt dann $|\mathbb{K}| = p^n$. □

Definition 6.1.19. Ein *Zwischenkörper* einer Körpererweiterung $k \subseteq \mathbb{K}$ ist ein Unterkörper $\mathbb{L} \subseteq \mathbb{K}$ mit $k \subseteq \mathbb{L}$.

Beispiel 6.1.20. Wir haben die Körpererweiterungen $\mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$.

Satz 6.1.21. *Es seien $k \subseteq \mathbb{L} \subseteq \mathbb{K}$ Körpererweiterungen. Ist $A := (a_i;\ i \in I)$ eine k-Basis für $\mathbb{L}$ und $B := (b_j;\ j \in J)$ eine $\mathbb{L}$-Basis für $\mathbb{K}$, so ist*

$$C \ :=\ (a_i b_j;\ (i, j) \in I \times J)$$

eine k-Basis für $\mathbb{K}$. Insbesondere erhalten wir für die Erweiterungen $k \subseteq \mathbb{L} \subseteq \mathbb{K}$ die Gradformel

$$[\mathbb{K} : k] \ =\ [\mathbb{K} : \mathbb{L}] \cdot [\mathbb{L} : k].$$

Beweis. Die zweite Aussage ist eine direkte Folgerung aus der ersten. Wir zeigen, dass C den k-Vektorraum $\mathbb{K}$ erzeugt. Dazu sei $c \in \mathbb{K}$ gegeben. Dann gilt

$$c \ =\ \sum_j s_j b_j$$

mit Koeffizienten $s_j \in \mathbb{L}$. Für jeden der Koeffizienten $s_j \in \mathbb{L}$ haben wir eine Darstellung

$$s_j \ =\ \sum_i r_{ij} a_i$$

mit Koeffizienten $r_{ij} \in k$. Wir erhalten

$$c \;=\; \sum_j s_j b_j \;=\; \sum_j \left(\sum_i r_{ij} a_i \right) b_j \;=\; \sum_{i,j} r_{ij} a_i b_j.$$

Folglich erzeugt C den k-Vektorraum $\mathbb{K}$. Wir zeigen, dass C linear unabhängig ist. Dazu seien $r_{ij} \in k$ gegeben mit

$$\sum_{i,j} r_{ij} a_i b_j \;=\; 0.$$

Dann haben wir

$$0 \;=\; \sum_{i,j} r_{ij} a_i b_j \;=\; \sum_j \left(\sum_i r_{ij} a_i \right) b_j.$$

Dabei sind die Koeffizienten der b_j auf der rechten Seite jeweils Elemente aus $\mathbb{L}$. Mit der linearen Unabhängigkeit von B über $\mathbb{L}$ ergibt sich daher

$$\sum_i r_{ij} a_i \;=\; 0$$

für jedes j. Die lineare Unabhängigkeit von A über k liefert, dass alle r_{ij} verschwinden. Folglich ist C linear unabhängig über k. □

Konstruktion 6.1.22. Es sei $k \subseteq \mathbb{K}$ eine Körpererweiterung, und es sei $B \subseteq \mathbb{K}$ eine Teilmenge. Dann erhält man einen Zwischenkörper

$$k(B) \;:=\; \{ab^{-1};\; a, b \in k[B],\, b \neq 0\}.$$

Ist $B = \{b_1, \ldots, b_r\}$ eine endliche Menge, so schreibt man auch $k(b_1, \ldots, b_r)$ anstelle von $k(B)$. Es gilt stets

$$k(B) \;=\; \bigcap_{\mathbb{L} \subseteq \mathbb{K} \text{ Unterkörper},\; k \cup B \subseteq \mathbb{L}} \mathbb{L}.$$

Wir sagen in dieser Situation, dass $k(B) \subseteq \mathbb{K}$ durch *Körperadjunktion* von B an k entsteht.

Beispiel 6.1.23. Für die Körpererweiterung $\mathbb{R} \subseteq \mathbb{C}$ erhalten wir $\mathbb{C} = \mathbb{R}(I)$, wegen $I \notin \mathbb{R}$ und $[\mathbb{C} : \mathbb{R}] = 2$.

Bemerkung 6.1.24. Es seien $k \subseteq \mathbb{L}_i \subseteq \mathbb{K}$ Körpererweiterungen, wobei $i = 1, 2$. Dann ist

$$\mathbb{L}_1 \mathbb{L}_2 \;:=\; k(\mathbb{L}_1 \cup \mathbb{L}_2) \;\subseteq\; \mathbb{K}$$

ein Unterkörper von $\mathbb{K}$. Man nennt $\mathbb{L}_1 \mathbb{L}_2$ auch das *Kompositum* der beiden Unterkörper $\mathbb{L}_1, \mathbb{L}_2 \subseteq \mathbb{K}$.

Aufgaben zu Abschnitt 6.1.

Aufgabe 6.1.25 (Frobenius-Homomorphismus)**.** Es sei $\mathbb{K}$ ein Körper der Charakteristik $p > 0$. Zeige:

(i) Die folgende Abbildung ist ein Monomorphismus:

$$\mathrm{Frob}_{\mathbb{K}} \colon \mathbb{K} \to \mathbb{K}, \qquad a \mapsto a^p.$$

(ii) Der Primkörper $\mathbb{P}_{\mathbb{K}}$ von $\mathbb{K}$ ist gegeben durch

$$\mathbb{P}_{\mathbb{K}} \quad = \quad \{a \in \mathbb{K};\ \mathrm{Frob}_{\mathbb{K}}(a) = a\}$$

Aufgabe 6.1.26. Es seien $f := T^3 + T + \overline{1} \in \mathbb{F}_2[T]$ und $\mathbb{K} := \mathbb{F}_2[T]/\langle f \rangle$.

(i) Zeige: Das Polynom f ist irreduzibel in $\mathbb{F}_2[T]$ und der Faktorring $\mathbb{K}$ ist ein Körper.
(ii) Zeige: Mit $\eta := T + \langle f \rangle$ und $\zeta := T^2 + \langle f \rangle$ besitzt jedes Element $u \in \mathbb{K}$ eine eindeutige Darstellung $u = a\zeta + b\eta + c$, wobei $a, b, c \in \mathbb{F}_2$.
(iii) Stelle die Verknüpfungstafeln der Gruppen $(\mathbb{K}, +)$ und $(\mathbb{K}, \cdot)$ auf. Stelle beide Gruppen als Produkt zyklischer Gruppen dar.

Aufgabe 6.1.27. Es sei $k \subseteq \mathbb{K}$ eine Körpererweiterung. Zeige: Ist $[\mathbb{K} : k]$ eine Primzahl, so gilt $\mathbb{K} = k(a)$ mit einem $a \in \mathbb{K}$.

Aufgabe 6.1.28. Es seien $k \subseteq \mathbb{K}$ eine Körpererweiterung, und es seien $b_1, \ldots, b_n \in \mathbb{K}$ gegeben. Zeige:

$$\begin{aligned} \mathbb{K}[b_1, \ldots, b_n] &= \{f(b_1, \ldots, b_n);\ f \in k[T_1, \ldots, T_n]\}\,, \\ \mathbb{K}(b_1, \ldots, b_n) &= \left\{ \frac{f(b_1, \ldots, b_n)}{g(b_1, \ldots, b_n)};\ f, g \in k[T_1, \ldots, T_n],\ g(b_1, \ldots, b_n) \neq 0 \right\}. \end{aligned}$$

Gib ein explizites Beispiel einer Körpererweiterung $k \subseteq \mathbb{K}$ mit Elementen $b_1, \ldots, b_n \in \mathbb{K}$ an, sodass $k[b_1, \ldots, b_n] \neq k(b_1, \ldots, b_n)$ gilt.

Aufgabe 6.1.29. Betrachte die Körperweiterung $\mathbb{Q} \subseteq \mathbb{C}$. Zeige, dass die Zwischenkörper $\mathbb{Q}(\sqrt{2})$ und $\mathbb{Q}(I)$ zwar als $\mathbb{Q}$-Vektorräume isomorph zueinander sind, jedoch nicht als Körper.

6.2. **Algebraische Elemente.**

Definition 6.2.1. Es sei $k \subseteq \mathbb{K}$ eine Körpererweiterung.

(i) Ein Element $a \in \mathbb{K}$ heißt *algebraisch über* k, falls es ein Polynom $0 \neq f \in k[T]$ gibt mit $f(a) = 0$.
(ii) Ein Element $a \in \mathbb{K}$ heißt *transzendent über* k, falls es nicht algebraisch über k ist.

Beispiel 6.2.2. Wie betrachten die Körpererweiterungen $\mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$.

(i) Die imaginäre Einheit $I \in \mathbb{C}$ ist algebraisch über $\mathbb{R}$; sie ist Nullstelle des Polynoms $T^2 + 1 \in \mathbb{R}[T]$.
(ii) Die Zahlen $e, \pi \in \mathbb{R}$ sind transzendent über $\mathbb{Q}$; dies sind nichttriviale Ergebnisse der Zahlentheorie.

Lemma 6.2.3. *Es sei $k \subseteq \mathbb{K}$ eine Körpererweiterung, und es sei $a \in \mathbb{K}$ algebraisch über k.*

(i) *Die folgende Vorschrift definiert einen Homomorphismus:*

$$\varepsilon_a \colon k[T] \ \to \ \mathbb{K}, \qquad f = \sum b_\nu T^\nu \ \mapsto \ f(a) := \sum b_\nu a^\nu.$$

(ii) *Das Ideal* $\mathrm{Kern}(\varepsilon_a) \leq_{k[T]} k[T]$ *wird von einem normierten irreduziblen Polynom $f_a \in k[T]$ erzeugt.*
(iii) *Ist $f \in k[T]$ ein irreduzibles normiertes Polynom mit $f(a) = 0$, so gilt $f = f_a$.*

Beweis. Zu (i). Die Tatsache, dass ε_a ein Homomorphismus ist, ergibt sich direkt aus der universellen Eigenschaft 3.2.6 des Polynomringes $k[T]$.

Zu (ii). Nach Satz 4.2.10 ist $k[T]$ ein Hauptidealring. Nach Definition eines algebraischen Elements ist $\mathrm{Kern}(\varepsilon_a)$ nicht trivial. Somit gilt $\mathrm{Kern}(\varepsilon_a) = \langle f_a \rangle$ mit einem normierten $0 \neq f_a \in k[T]$. Wir müssen zeigen, dass f_a irreduzibel ist. Wegen $f_a(a) = 0$ muss $f_a \notin k^*$ gelten. Es sei nun $f_a = gh$ mit $g, h \in k[T]$. Dann gilt

$$0 \ = \ (gh)(a) \ = \ g(a)h(a).$$

Es folgt $g(a) = 0$ oder $h(a) = 0$. Wir dürfen $g(a) = 0$ annehmen. Dann gilt $g \in \langle f_a \rangle$ und man hat $g = h' f_a$ mit einem $h' \in k[T]$. Es folgt $hh' = 1$ und somit ist h eine Einheit in $k[T]$. Das beweist die Irreduzibilität von $f_a \in k[T]$.

Zu (iii). Ist $f \in k[T]$ ein normiertes irreduzibles Polynom mit $f(a) = 0$, so gilt $f \in \langle f_a \rangle$, d.h., man hat $f = h f_a$ mit einem $h \in k[T]$. Da f irreduzibel ist, muss h eine Einheit in $k[T]$ sein. Wegen der Normiertheit von f und f_a folgt $h = 1$, d.h., man hat $f = f_a$. □

Definition 6.2.4. Es sei $k \subseteq \mathbb{K}$ eine Körpererweiterung, und es sei $a \in \mathbb{K}$ algebraisch über k. Das Polynom f_a aus Lemma 6.2.3 nennt man das *Minimalpolynom* von a über k.

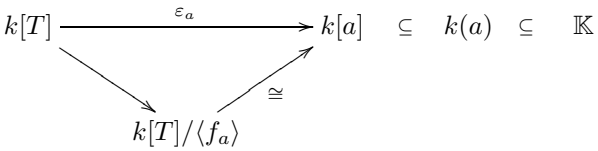
Beispiel 6.2.5. Das Minimalpolynom von $\sqrt{2} \in \mathbb{R}$ über $\mathbb{Q}$ ist $T^2 - 2$. Das Minimalpolynom von $I \in \mathbb{C}$ über $\mathbb{R}$ ist $T^2 + 1$.

Satz 6.2.6. *Es seien $k \subseteq \mathbb{K}$ eine Körpererweiterung und $a \in \mathbb{K}$ algebraisch über k mit Minimalpolynom $f_a \in k[T]$. Dann gilt:*

$$k(a) \ = \ k[a] \ \cong \ k[T]/\langle f_a \rangle, \qquad\qquad [k(a) : k] \ = \ \deg(f_a).$$

Weiter ist für $n := \deg(f_a)$ die Familie $(1, a, a^2, \ldots, a^{n-1})$ eine Basis für den k-Vektorraum $\mathbb{K}$.

Beweis. Wir betrachten den Auswertungshomomorphismus $\varepsilon_a\colon k[T] \to \mathbb{K}$. Der Homomorphiesatz liefert uns ein kommutatives Diagramm



Insbesondere ist $k[a] \cong k[T]/\langle f_a\rangle$ ein Körper, siehe Konstruktion 6.1.15. Es folgt $k[a] = k(a)$. Die weiteren Aussagen folgen direkt aus Konstruktion 6.1.15. □

Beispiel 6.2.7. Das Polynom $T^3 - 1 \in \mathbb{Q}[T]$ annulliert die dritte Einheitswurzel $e^{\frac{2\pi i}{3}} \in \mathbb{C}$. Die Primfaktorzerlegung von $T^3 - 1 \in \mathbb{Q}[T]$ ist gegeben durch

$$T^3 - 1 \;=\; (T-1)(T^2+T+1).$$

Somit ist $T^2 + T + 1$ das Minimalpolynom von $e^{\frac{2\pi i}{3}}$ über $\mathbb{Q}$. Nach Satz 6.2.6 ist die Körpererweiterung $\mathbb{Q} \subseteq \mathbb{Q}(e^{\frac{2\pi i}{3}})$ vom Grad 2 und $(1, e^{\frac{2\pi i}{3}})$ ist eine k-Basis für $\mathbb{K}$.

Satz 6.2.8 (Eisensteinsches Irreduzibilitätskriterium)**.** *Es sei R ein faktorieller Ring, und es sei*

$$f \;=\; a_n T^n + a_{n-1}T^{n-1} + \ldots + a_1 T + a_0 \;\in\; R[T]$$

ein primitives Polynom mit $a_n \neq 0$ und $n \geq 1$. Gibt es ein Primelement $p \in R$ mit

$$p \nmid a_n, \qquad p \mid a_{n-1}, \ldots, p \mid a_0, \qquad p^2 \nmid a_0,$$

so ist das Polynom f ein Primelement in $R[T]$, und somit auch in dem Ring $Q(R)[T]$.

Beweis. Nach dem Satz von Gauß 4.4.1 ist $R[T]$ faktoriell. Also genügt es zu zeigen, dass f irreduzibel in $R[T]$ ist, siehe Satz 4.3.3 und Folgerung 4.4.16. Dazu betrachten wir eine Zerlegung $f = gh$ in $R[T]$ mit Polynomen

$$g \;=\; b_m T^m + \ldots + b_0, \qquad h \;=\; c_l T^l + \ldots + c_0.$$

Dabei dürfen wir $n = m + l$ und $m \geq 1$ annehmen. Gilt $l = 0$, so folgt $c_0 \mid a_i$ für alle i. Da f primitiv ist, folgt $c_0 \in R^*$, was wiederum $h \in R[T]^*$ impliziert. Es bleibt somit, den Fall $l \geq 1$ auszuschliessen. Aus den Voraussetzungen erhalten wir

$$a_n = b_m c_l, \qquad p \nmid b_m, \qquad p \nmid c_l, \qquad a_0 = b_0 c_0, \qquad p \mid b_0 c_0, \qquad p^2 \nmid b_0 c_0.$$

Wir dürfen dabei $p \mid b_0$ annehmen. Dann muss $p \nmid c_0$ gelten. Es sei k maximal mit $p \mid b_i$ für alle $0 \leq i \leq k$. Dann gilt $k < m$ und man hat, mit $c_j := 0$ für $j \geq l+1$,

$$\begin{aligned} a_{k+1} &= b_0 c_{k+1} + \ldots + b_k c_1 + b_{k+1} c_0 \\ &= pb + b_{k+1} c_0 \end{aligned}$$

mit einem geeigneten $b \in R$. Folglich gilt $p \nmid a_{k+1}$. Das impliziert $k + 1 = n$ und somit $m = n$. Widerspruch zu $l \geq 1$ und $n = m + l$. □

Beispiel 6.2.9. Es seien $n \in \mathbb{Z}_{\geq 1}$ und $p \in \mathbb{Z}$ eine Primzahl. Dann ist das Polynom $T^n - p \in \mathbb{Q}[T]$ irreduzibel. Die Körpererweiterung $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[n]{p})$ besitzt den Grad n.

Beispiel 6.2.10. Für $d \in \mathbb{Z}_{\geq 0}$ bezeichne $\sqrt{d}$ die übliche Quadratwurzel und für $d \in \mathbb{Z}_{\leq 0}$ setzen wir $\sqrt{d} := I\sqrt{|d|}$. Für quadratfreies $d \in \mathbb{Z}$ nennt man

$$\mathbb{Q} \;\subseteq\; \mathbb{Q}(\sqrt{d}) \;\subseteq\; \mathbb{C},$$

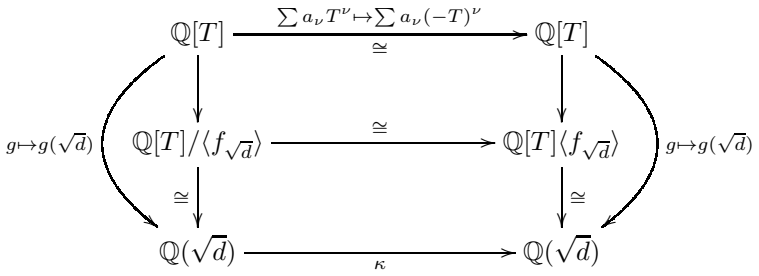
einen *quadratischen Zahlkörper* über $\mathbb{Q}$. Das Minimalpolynom von $\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ über $\mathbb{Q}$ ist gegeben durch

$$f_{\sqrt{d}} \;=\; T^2 - d \;\in\; \mathbb{Q}[T].$$

Insbesondere gilt $[\mathbb{Q}(\sqrt{d}) : \mathbb{Q}] = 2$, wir haben einen Epimorphismus $\mathbb{Q}[T] \to \mathbb{Q}(\sqrt{d})$, $g \mapsto g(\sqrt{d})$, und $\mathbb{Q}(\sqrt{d})$ besitzt $(1, \sqrt{d})$ als $\mathbb{Q}$-Basis. Letzteres impliziert

$$\mathbb{Q}(\sqrt{d}) \quad = \quad \{a + b(\sqrt{d});\ a, b \in \mathbb{Q}\}.$$

Die *Konjugation* auf $\mathbb{Q}(\sqrt{d})$ ist der eindeutig bestimmte Körperisomorphismus $\kappa\colon \mathbb{Q}(\sqrt{d}) \to \mathbb{Q}(\sqrt{d})$ mit dem das folgende Diagramm kommutativ wird



Konkret ist $\kappa\colon \mathbb{Q}(\sqrt{d}) \to \mathbb{Q}(\sqrt{d})$ gegeben durch $a + b\sqrt{d} \mapsto a - b\sqrt{d}$. *Spur* und *Norm* auf $\mathbb{Q}(\sqrt{d})$ sind die Abbildungen

$$\mathrm{Sp}\colon \mathbb{Q}(\sqrt{d}) \to \mathbb{Q}, \quad z \mapsto z + \kappa(z), \qquad\qquad N\colon \mathbb{Q}(\sqrt{d}) \to \mathbb{Q}, \quad z \mapsto z\kappa(z).$$

Für $z = a + b\sqrt{d}$ mit $a, b \in \mathbb{Q}$ erhalten wir

$$\mathrm{Sp}(a + b\sqrt{d}) \ = \ 2a, \qquad\qquad \mathrm{N}(a + b\sqrt{d}) \ = \ a^2 - db^2.$$

Jedes Element $z \in \mathbb{Q}(\sqrt{d}) \setminus \mathbb{Q}$ ist algebraisch über $\mathbb{Q}$ und das zugehörige Minimalpoynom ist gegeben durch

$$f_z \ = \ (T - z)(T - \kappa(z)) \ = \ T^2 - \mathrm{Sp}(z) + \mathrm{N}(z) \ = \ T^2 - 2aT + a^2 - db^2.$$

Definition 6.2.11. Eine Körpererweiterung $k \subseteq \mathbb{K}$ heißt *algebraisch*, falls jedes Element $a \in \mathbb{K}$ algebraisch über k ist.

Satz 6.2.12. *Für jede Körpererweiterung $k \subseteq \mathbb{K}$ gilt:*

(i) *Ist $k \subseteq \mathbb{K}$ endlich, so ist $k \subseteq \mathbb{K}$ eine algebraische Körpererweiterung.*
(ii) *Sind $a_1, \ldots, a_n \in \mathbb{K}$ algebraisch über k, so ist $k \subseteq k(a_1, \ldots, a_n)$ endlich und algebraisch.*
(iii) *Ist $k \subseteq \mathbb{L} \subseteq \mathbb{K}$ ein Zwischenkörper, für den $k \subseteq \mathbb{L}$ und $\mathbb{L} \subseteq \mathbb{K}$ algebraisch sind, so ist auch $k \subseteq \mathbb{K}$ algebraisch.*

Beweis. Zu (i). Wir setzen $d := [\mathbb{K} : k]$. Für jedes $b \in \mathbb{K}$ ist dann die Familie $1, b, \ldots, b^d$ linear abhängig über k. Ein annulierndes Polynom für b erhält man also aus jeder nicht trivialen Linearkombination

$$a_0 + a_1 b + \ldots + a_d b^d \quad = \quad 0.$$

Wir zeigen (ii). Gemäß Satz 6.2.6 erhält man für jedes $i = 1, \ldots, n$ endliche Körpererweiterungen

$$k(a_1, \ldots, a_{i-1}) \ \subseteq \ k(a_1, \ldots, a_{i-1})(a_i) \ = \ k(a_1, \ldots, a_i).$$

Nach Satz 6.1.21 ist damit auch $k \subseteq k(a_1, \ldots, a_n)$ endlich und somit gemäß Aussage (i) algebraisch.

Zu (iii). Es sei $a \in \mathbb{K}$ gegeben. Dann ist a algebraisch über $\mathbb{L}$. Es gibt also Elemente $b_0, \ldots, b_n \in \mathbb{L}$, mit

$$b_0 + b_1 a + \ldots + b_{n-1} a^{n-1} + b_n a^n \quad = \quad 0,$$

wobei mindestens ein b_i nicht verschwindet. Insbesondere ist a algebraisch über $k(b_0, \ldots, b_n)$. Nach Aussage (ii) ist jede der Körpererweiterungen

$$k \ \subseteq \ k(b_0, \ldots, b_n) \ \subseteq \ k(b_0, \ldots, b_n)(a) \ = \ k(b_0, \ldots, b_n, a)$$

endlich. Nach Satz 6.1.21 ist $k \subseteq k(b_0, \ldots, b_n, a)$ endlich und somit, nach Aussage (i), algebraisch. Insbesondere ist a algebraisch über k. □

Definition 6.2.13. Eine Körpererweiterung $k \subseteq \mathbb{K}$ heißt *endlich erzeugt*, falls $\mathbb{K} = k(B)$ mit einer endlichen Menge $B \subseteq \mathbb{K}$ gilt.

Folgerung 6.2.14. *Es sei $k \subseteq \mathbb{K}$ eine Körpererweiterung. Dann sind folgende Aussagen äquivalent:*

(i) *$k \subseteq \mathbb{K}$ ist endlich.*
(ii) *$k \subseteq \mathbb{K}$ ist endlich erzeugt und algebraisch.*

Beweis. Zur Implikation "(i)⇒(ii)". Ist $(a_1, \ldots, a_n) \subseteq \mathbb{K}$ eine Basis für den k-Vektorraum $\mathbb{K}$, so gilt insbesondere $\mathbb{K} = k(a_1, \ldots, a_n)$. Somit ist $k \subseteq \mathbb{K}$ endlich erzeugt. Nach Satz 6.2.12 (i) ist $k \subseteq \mathbb{K}$ algebraisch. Die Implikation "(ii)⇒(i)" ergibt sich direkt aus Satz 6.2.12 (ii). □

Folgerung 6.2.15. *Es sei $k \subseteq \mathbb{K}$ eine Körpererweiterung. Dann ist die Menge $L \subseteq \mathbb{K}$ aller über k algebraischen Elemente ein Zwischenkörper von $k \subseteq \mathbb{K}$.*

Beweis. Es ist klar, dass $k \subseteq L$ gilt. Wir müssen daher nur zeigen, dass für je zwei $a, b \in L$ gilt

$$-a \in L, \qquad a + b \in L, \qquad a^{-1} \in L, \qquad ab \in L.$$

All diese Elemente sind in $k(a, b)$ enthalten. Nach Satz 6.2.12 ist $k \subseteq k(a, b)$ algebraisch. Das bedeutet $k(a, b) \subseteq L$. □

Aufgaben zu Abschnitt 6.2.

Aufgabe 6.2.16. Es sei $k \subseteq \mathbb{K}$ eine Körpererweiterung. Beweise folgende Aussagen:

(i) Ein Element $a \in \mathbb{K}^*$ ist genau dann algebraisch über k, wenn $a^{-1} \in k[a]$ gilt.
(ii) Sind $a_1, \ldots, a_n \in \mathbb{K}$ algebraisch über k, so gilt $k(a_1, \ldots, a_n) = k[a_1, \ldots, a_n]$.
(iii) Die Körpererweiterung $k \subseteq \mathbb{K}$ ist genau dann algebraisch, wenn jeder Unterring $R \subseteq \mathbb{K}$ mit $k \subseteq R$ ein Körper ist.

Aufgabe 6.2.17. Beweise folgende Aussagen:

(i) Ist $\mathbb{R} \subsetneq \mathbb{K}$ eine echte algebraische Erweiterung mit $\mathbb{K} = \mathbb{R}(a)$ für ein $a \in \mathbb{K}$, so ist $[\mathbb{K} : \mathbb{R}]$ eine gerade Zahl.
(ii) Der Körper $\mathbb{C}$ der komplexen Zahlen erlaubt keine Erweiterung $\mathbb{C} \subseteq \mathbb{K}$ mit $[\mathbb{K} : \mathbb{C}] = 2$.

Aufgabe 6.2.18. Für $p, q \in \mathbb{Z}_{\geq 2}$ quadratfrei mit $p \neq q$ betrachte $\mathbb{K} := \mathbb{Q}(\sqrt{p}, \sqrt{q}) \subseteq \mathbb{R}$. Zeige: Es gilt $[\mathbb{K} : \mathbb{Q}] = 4$ und $(1, \sqrt{p}, \sqrt{q}, \sqrt{pq})$ ist eine $\mathbb{Q}$-Basis für $\mathbb{K}$. *Hinweis:* Zeige zunächst $\sqrt{q} \notin \mathbb{Q}(\sqrt{p})$.

Aufgabe 6.2.19. Bestimme, jeweils mit Begründung, den Grad $[\mathbb{Q}(a) : \mathbb{Q}]$ für

$$a \;=\; \sqrt{2 + \sqrt[3]{2}} \;\in\; \mathbb{R}, \qquad\qquad a \;=\; \sqrt{2 + \sqrt{2 + \sqrt{2}}} \;\in\; \mathbb{R}.$$

Aufgabe 6.2.20. Zeige: $[\mathbb{R} : \mathbb{Q}] = \infty$.

Aufgabe 6.2.21. Es sei $\mathbb{Q} \subseteq \mathbb{K}$ eine Körpererweiterung vom Grad zwei. Zeige: $\mathbb{K}$ ist isomorph zu einem quadratischen Zahlkörper.

Aufgabe 6.2.22. Betrachte die Körpererweiterungen $\mathbb{Q} \subseteq \mathbb{L}_i \subseteq \mathbb{C}$, wobei $\mathbb{L}_1 = \mathbb{Q}(\sqrt[3]{2})$, $\mathbb{L}_2 = \mathbb{Q}(e^{\frac{2\pi I}{3}} \sqrt[3]{2}))$ und $\mathbb{L}_3 = \mathbb{Q}(e^{\frac{2\pi I}{3}})$. Beweise folgende Aussagen:

(i) $\mathbb{L}_1 \cap \mathbb{L}_2 = \mathbb{L}_1 \cap \mathbb{L}_3 = \mathbb{Q}$,
(ii) $[\mathbb{L}_1 : \mathbb{Q}] = [\mathbb{L}_2 : \mathbb{Q}] = 3$, $[\mathbb{L}_3 : \mathbb{Q}] = 2$,
(iii) $\mathbb{L}_1\mathbb{L}_2 = \mathbb{L}_1\mathbb{L}_3 = \mathbb{Q}(\sqrt[3]{2}, e^{\frac{2\pi I}{3}})$,
(iv) $[\mathbb{L}_1\mathbb{L}_2 : \mathbb{Q}] = [\mathbb{L}_1\mathbb{L}_3 : \mathbb{Q}] = 6$.

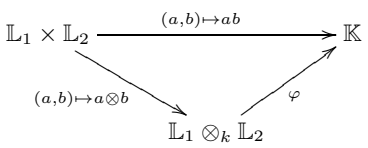
Zeige weiter, dass $(1, 2^{\frac{1}{3}}, 2^{\frac{2}{3}}, e^{\frac{2\pi I}{3}}, 2^{\frac{1}{3}} e^{\frac{2\pi I}{3}}, 2^{\frac{2}{3}} e^{\frac{2\pi I}{3}})$ eine $\mathbb{Q}$-Basis für $\mathbb{L}_1\mathbb{L}_2$ ist. *Hinweis:* Betrachte die Polynome $T^3 - 2 \in \mathbb{Q}[T]$ und $T^3 - 1 = (T-1)(T^2 + T + 1) \in \mathbb{Q}[T]$.

Aufgabe 6.2.23. Es sei $k \subseteq \mathbb{K}$ eine endliche Körpererweiterung, und es sei $a \in \mathbb{K}$. Betrachte die k-lineare Abbildung $\varphi_a \colon \mathbb{K} \to \mathbb{K}$, $v \mapsto av$ und zeige:

(i) Das Minimalpolynom $f_a \in k[T]$ des Elements $a \in \mathbb{K}$ ist auch das Minimalpolynom des k-linearen Endomorphismus $\varphi_a \colon \mathbb{K} \to \mathbb{K}$.
(ii) Gilt $\mathbb{K} = k(a)$, so ist das Minimalpolynom f_a gerade das charakteristische Polynom $\det(T \cdot \mathrm{id}_{\mathbb{K}} - \varphi_a)$ von φ_a.
(iii) Das charakteristische Polynom von φ_a ist stets eine Potenz des Minimalpolynoms f_a.

Aufgabe 6.2.24. Es seien $k \subseteq \mathbb{K}$ eine Körpererweiterung und $a, b \in \mathbb{K}$. Zeige: Sind $m := [k(a) : k]$ und $n := [k(b) : k]$ teilerfremd, so gilt $[k(a, b) : k] = mn$.

Aufgabe 6.2.25. Es seien $k \subseteq \mathbb{L}_i \subseteq \mathbb{K}$ Körpererweiterungen, wobei $i = 1, 2$ und $k \subseteq \mathbb{L}_i$ endlich sei. Zeige: Es gibt ein kommutatives Diagramm



mit einer eindeutig bestimmten k-linearen Abbildung $\varphi \colon \mathbb{L}_1 \otimes_k \mathbb{L}_2 \to \mathbb{K}$. Zeige, dass das Bild von φ gegeben ist durch

$$\varphi(\mathbb{L}_1 \otimes_k \mathbb{L}_2) \;=\; \mathbb{L}_1\mathbb{L}_2 \;:=\; k(\mathbb{L}_1 \cup \mathbb{L}_2) \;\subseteq\; \mathbb{K}$$

Es seien weiter eine k-Basis $(a_1, \ldots, a_m)$ für $\mathbb{L}_1$ und eine k-Basis $(b_1, \ldots, b_n)$ für $\mathbb{L}_2$ gegeben. Beweise die Äquivalenz der folgenden Aussagen:

(i) $(a_i b_j;\ i = 1, \ldots, m,\ j = 1, \ldots, n)$ ist linear unabhängig über k.
(ii) Die lineare Abbildung $\varphi\colon \mathbb{L}_1 \otimes_k \mathbb{L}_2 \to \mathbb{K}$ ist injektiv.
(iii) Für das Kompositum $\mathbb{L}_1\mathbb{L}_2$ gilt $[\mathbb{L}_1\mathbb{L}_2 : k] = [\mathbb{L}_1 : k] \cdot [\mathbb{L}_2 : k]$.

Zeige weiter: Gilt eine der drei obigen Aussagen, so haben wir $\mathbb{L}_1 \cap \mathbb{L}_2 = k$. *Anmerkung:* Für $\mathbb{Q} \subseteq \mathbb{L}_i \subseteq \mathbb{C}$ mit $\mathbb{L}_1 = \mathbb{Q}(\sqrt[3]{2})$ und $\mathbb{L}_2 = \mathbb{Q}(e^{\frac{2\pi I}{3}}\sqrt[3]{2})$ gilt gemäß Aufgabe 6.2.22:

$$\mathbb{L}_1 \cap \mathbb{L}_2 \ = \ \mathbb{Q}, \qquad [\mathbb{L}_1\mathbb{L}_2 : \mathbb{Q}] \ = \ 6, \qquad [\mathbb{L}_1 : \mathbb{Q}] \cdot [\mathbb{L}_2 : \mathbb{Q}] \ = \ 9.$$

6.3. **Konstruktionen mit Zirkel und Lineal.**

Bemerkung 6.3.1 (Lineal)**.** Für zwei Punkte $p, q \in \mathbb{C}$, wobei $p \neq q$, kann man mit dem Lineal die zugehörige Verbindungsgerade konstruieren:

$$\overline{p,q} \;:=\; \{p + t(q-p);\; t \in \mathbb{R}\} \;\subseteq\; \mathbb{C}.$$

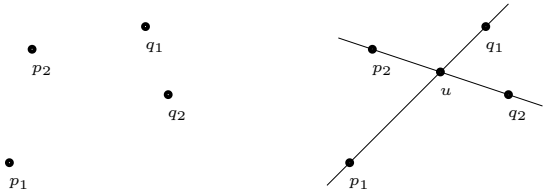
Bemerkung 6.3.2 (Zirkel)**.** Für einen Punkt $p \in \mathbb{C}$ und ein Paar $p_1, q_1 \in \mathbb{C}$ kann man mit dem Zirkel den Kreis um p mit Radius $|q_1 - p_1|$ konstruieren:

$$K(p, |q_1 - p_1|) \;:=\; \{z \in \mathbb{C};\; |z-p| = |q_1 - p_1|\} \;\subseteq\; \mathbb{C}.$$

Konstruktion 6.3.3 (Schnitt Gerade–Gerade)**.** Sind $p_1, q_1, p_2, q_2 \in \mathbb{C}$, mit $p_i \neq q_i$ und $\overline{p_1, q_1} \neq \overline{p_2, q_2}$ gegeben, so gilt

$$\overline{p_1, q_1} \;\cap\; \overline{p_2, q_2} \quad=\quad \{u\}$$

mit einem eindeutig bestimmten Punkt $u \in \mathbb{C}$. Wir sagen in diesem Fall, dass u durch einen *Schnitt Gerade–Gerade* aus p_1, q_1, p_2, q_2 konstruiert wird.

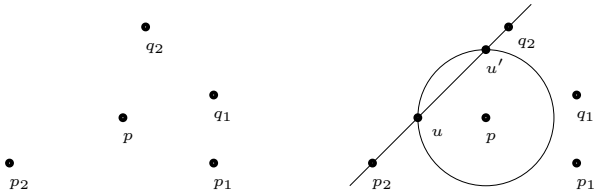


Die obige Skizze verdeutlicht, dass die geometrische Konstruktion des Punktes u allein mit Hilfe des Lineals möglich ist.

Konstruktion 6.3.4 (Schnitt Kreis–Gerade)**.** Sind Punkte p, p_1, q_1 und p_2, q_2 mit $p_2 \neq q_2$ aus $\mathbb{C}$ gegeben, so betrachten wir den Durchschnitt des zu p, p_1, q_1 gehörigen Kreises und der zu p_2, q_2 gehörigen Geraden:

$$U \;:=\; K(p, |q_1 - p_1|) \;\cap\; \overline{p_2, q_2} \;\subseteq\; \mathbb{C}.$$

Je nach Lage der Punkte p, p_i, q_i enthält U keinen, einen oder zwei Punkte. Falls U Punkte enthält, so sagen wir, dass diese durch einen *Schnitt Kreis–Gerade* aus den Punkten p, p_i, q_i konstruiert werden.

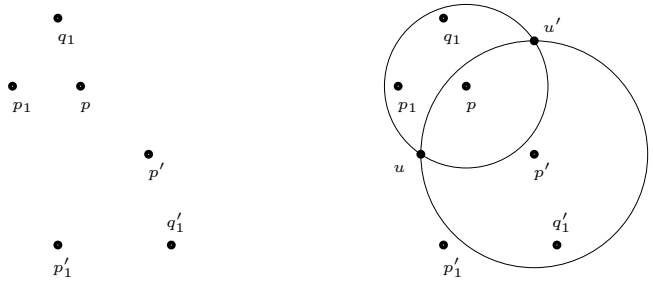


Die obige Skizze zeigt den Fall, dass die Schnittmenge zwei Punkte enhält: $U = \{u, u'\}$. Die geometrische Konstruktion der Menge U erfordert sowohl Zirkel als auch Lineal.

Konstruktion 6.3.5 (Schnitt Kreis–Kreis)**.** Sind Punkte p, p_1, q_1 und p', p_1', q_1' aus $\mathbb{C}$ mit $K(p, |q_1 - p_1|) \neq K(p', |q_1' - p_1'|)$ gegeben, so betrachten wir den Durchschnitt der zu diesen Punktetripeln gehörigen Kreise:

$$U \;:=\; K(p, |q_1 - p_1|) \;\cap\; K(p', |q_1' - p_1'|) \;\subseteq\; \mathbb{C}$$

Je nach Lage der Punkte p, p_1, q_2 und p', p_1', q_2' enthält U keinen, einen oder zwei Punkte. Falls U Punkte enthält, so sagen wir, dass diese durch einen *Schnitt Kreis–Kreis* aus p, p_1, q_1 und p', p_1', q_1' konstruiert werden.



Die obige Skizze zeigt den Fall, dass die Schnittmenge zwei Punkte enhält: $U = \{u, u'\}$. Die geometrische Konstruktion der Menge U ist allein mit Hilfe des Zirkels möglich.

Definition 6.3.6. Es sei $M \subseteq \mathbb{C}$ eine Teilmenge.

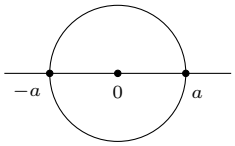
(i) Wir nennen $M \subseteq M' \subseteq \mathbb{C}$ eine *elementare Vergrößerung* von M, falls M' aus M durch Hinzunahme der durch eine der Konstruktionen 6.3.3, 6.3.4 oder 6.3.5 gewonnenen Punkte entsteht.

(ii) Wir nennen einen Punkt $z \in \mathbb{C}$ *aus M konstruierbar*, falls es eine Folge elementarer Vergrößerungen $M = M_1 \subseteq M_2 \subseteq \ldots \subseteq M_n = M'$ gibt mit $z \in M'$. Wir setzen

$$\mathrm{Kon}(M) \ := \ \{z \in \mathbb{C};\ z \text{ aus } M \text{ konstruierbar}\}.$$

Lemma 6.3.7. *Es sei $M \subseteq \mathbb{C}$ mit $0 \in M$. Gilt $a \in \mathrm{Kon}(M)$ für eine reelle Zahl a, so gilt auch $-a \in \mathrm{Kon}(M)$.*

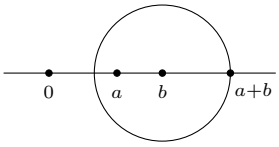
Beweis. Für $a \neq 0$ ist $-a \in \mathbb{R}$ einer der Schnittpunkte des Kreises $K(0, |a-0|)$ mit der reellen Achse $\overline{0, a}$:



□

Lemma 6.3.8. *Es sei $M \subseteq \mathbb{C}$ mit $0 \in M$. Gilt $a, b \in \mathrm{Kon}(M)$ für zwei reelle Zahlen a und b, so gilt auch $a + b \in \mathrm{Kon}(M)$.*

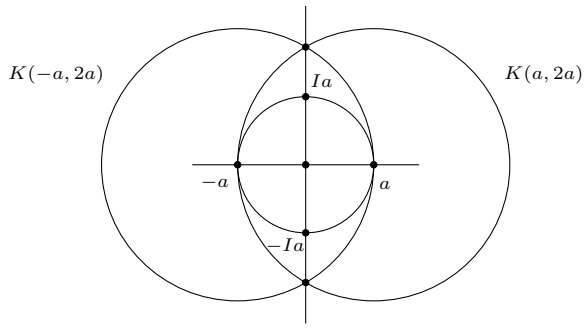
Beweis. Für $a \neq 0$ ist die Summe $a + b \in \mathbb{R}$ einer der Schnittpunkte des Kreises $K(b, |a-0|)$ mit der reellen Achse $\overline{0, a}$:



□

Lemma 6.3.9. *Es sei $M \subseteq \mathbb{C}$ mit $0 \in M$. Gilt $a \in \mathrm{Kon}(M)$ für eine reelle Zahl a, so gilt auch $\pm Ia \in \mathrm{Kon}(M)$.*

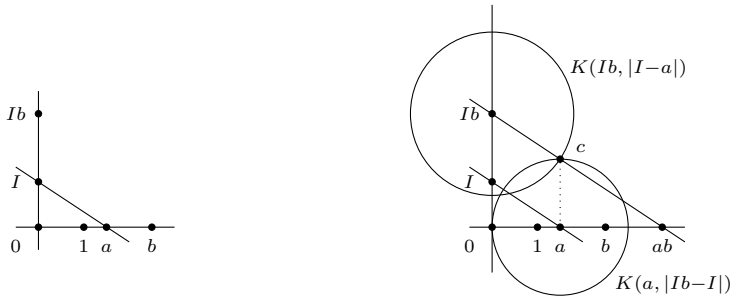
Beweis. Lemma 6.3.7 liefert $-a \in \mathrm{Kon}(M)$. Somit dürfen wir $a > 0$ annehmen. Wir erhalten die imaginäre Achse $I\mathbb{R}$ als Verbindungsgerade



der Schnittpunkte der Kreise vom Radius $2a$ um $-a$ bzw. a. Die Punkte $\pm Ia$ sind dann genau die Schnittpunkte von $I\mathbb{R}$ mit dem Kreis $K(0,a)$. □

Lemma 6.3.10. *Es sei $M \subseteq \mathbb{C}$ mit $0,1 \in M$. Gilt $a,b \in \mathrm{Kon}(M)$ für zwei reelle Zahlen a und b, so gilt auch $ab \in \mathrm{Kon}(M)$.*

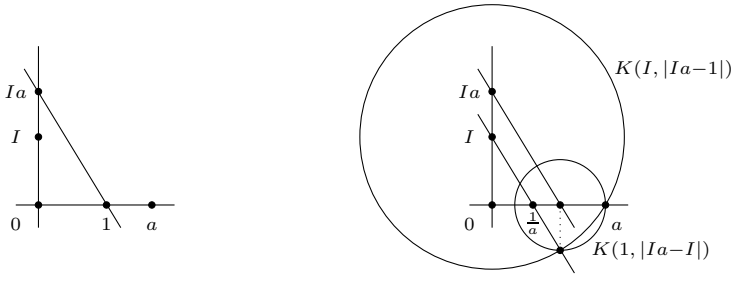
Beweis. Wir dürfen $a,b>0$ annehmen; siehe Lemma 6.3.7. Lemma 6.3.9 liefert uns $I, Ib \in \mathrm{Kon}(M)$. Weiter ziehen wir die Verbindungsgerade $\overline{I,a}$.



Mittels Parallelogrammkonstruktion erhält man die Parallele $\overline{Ib,c}$ zu $\overline{I,a}$ durch Ib. Der Schnittpunkt von $\overline{Ib,c}$ mit der reellen Achse ist der gesuchte Punkt ab. □

Lemma 6.3.11. *Es sei $M \subseteq \mathbb{C}$ mit $0,1 \in M$. Gilt $a \in \mathrm{Kon}(M)$ für eine reelle Zahl $a \neq 0$, so gilt auch $1/a \in \mathrm{Kon}(M)$.*

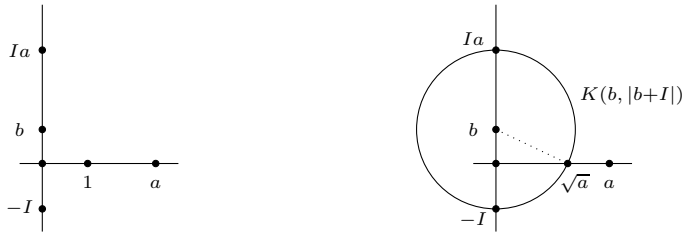
Beweis. Nach Lemma 6.3.7 dürfen wir $a>0$ annehmen. Lemma 6.3.9 liefert uns $I, Ia \in \mathrm{Kon}(M)$. Weiter ziehen wir die Verbindungsgerade $\overline{Ia,1}$



und konstruieren die Parallele H zu $\overline{Ia,1}$ durch I. Der Schnittpunkt von H mit der reellen Achse ist dann der Punkt $1/a$. □

Lemma 6.3.12. *Es sei $M \subseteq \mathbb{C}$ mit $0,1 \in M$. Gilt $a \in \mathrm{Kon}(M)$ für eine positive reelle Zahl, so gilt auch $\sqrt{a} \in \mathrm{Kon}(M)$.*

Beweis. Nach Lemmata 6.3.7 bis 6.3.11 gilt $I, Ia \in \mathrm{Kon}(M)$ sowie $b \in \mathrm{Kon}(M)$ für das Mittel $b = (Ia - I)/2$ von Ia und $-I$.



Die Quadratwurzel $\sqrt{a}$ ist dann der positive Schnittpunkt q des Kreises $K(b, |b+I|)$ mit der reellen Achse, denn mit dem Satz von Pythagoras erhalten wir

$$q^2 \;=\; |b+I|^2 - |b|^2 \;=\; \left|\frac{Ia+I}{2}\right|^2 - \left|\frac{Ia-I}{2}\right|^2 \;=\; \frac{1}{4}\left((a+1)^2 - (a-1)^2\right) \;=\; a.$$

□

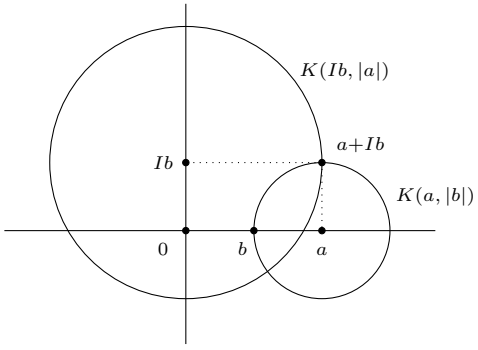
Satz 6.3.13. *Es sei* $\{0,1\} \subseteq M \subseteq \mathbb{R}$. *Für die Menge* $\mathrm{Kon}(M)$ *der aus* M *konstruierbaren komplexen Zahlen gilt:*

(i) $\mathrm{Kon}(M) \cap \mathbb{R}$ *ist ein Zwischenkörper von* $\mathbb{Q}(M) \subseteq \mathbb{R}$.
(ii) *Gilt* $a^2 \in \mathrm{Kon}(M)$ *für ein* $a \in \mathbb{R}_{\geq 0}$, *so gilt auch* $a \in \mathrm{Kon}(M)$.

Beweis. Mit Lemmata 6.3.7 bis 6.3.11 erhalten wir $\mathbb{Q}(M) \subseteq \mathrm{Kon}(M)$ und die Tatsache, dass $\mathrm{Kon}(M) \cap \mathbb{R}$ ein Körper ist. Das beweist die erste Aussage. Die zweite Aussage ist Lemma 6.3.12. □

Lemma 6.3.14. *Es sei* $M \subseteq \mathbb{C}$ *mit* $0 \in M$. *Gilt* $a, b \in \mathrm{Kon}(M)$ *für reelle Zahlen* a, b, *so gilt auch* $a + Ib \in \mathrm{Kon}(M)$.

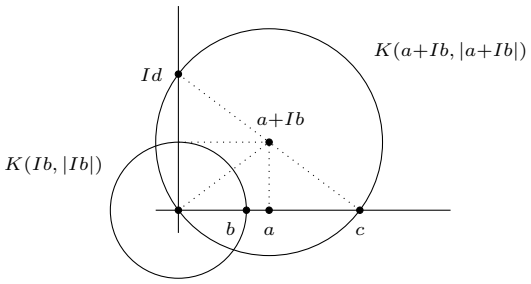
Beweis. Nach Lemma 6.3.9 gilt $Ib \in \mathrm{Kon}(M)$. Die Zahl $a+Ib$ ist dann Schnittpunkt der Kreise $K(Ib, |a|)$ und $K(a, |b|)$:



□

Lemma 6.3.15. *Es sei* $M \subseteq \mathbb{C}$ *mit* $0, 1 \in M$. *Gilt* $a + Ib \in \mathrm{Kon}(M)$ *mit reellen Zahlen* a, b, *so gilt* $a, b \in \mathrm{Kon}(M)$.

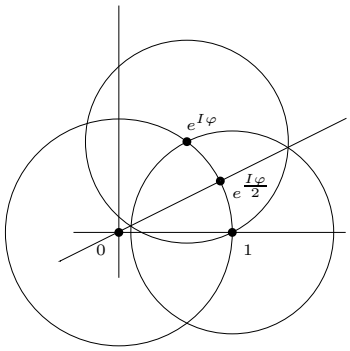
Beweis. Wir konstruieren zunächst die Achsen $\mathbb{R} = \overline{0,1}$ und $I\mathbb{R} = \overline{0,I}$; siehe Lemma 6.3.9. Für die von Null verschiedenen Schnittpunkte c, Id der Achsen mit dem



Kreis $K(a+Ib, |a+Ib|)$ gilt $a = c/2$ und $Ib = Id/2$. Weiter ist $b = d/2$ Schnittpunkt von $\mathbb{R}$ mit $K(Ib, |Ib|)$. Lemmata 6.3.8, 6.3.10, 6.3.11 liefern $a, b \in \mathrm{Kon}(M)$. □

Lemma 6.3.16. *Es sei $M \subseteq \mathbb{C}$ mit $0, 1 \in M$. Gilt $e^{I\varphi} \in \mathrm{Kon}(M)$ mit $\varphi \in [0, 2\pi]$, so gilt $e^{\frac{I\varphi}{2}} \in \mathrm{Kon}(M)$.*

Beweis. Man konstruiert die Winkelhalbierende H zu den Geraden $\overline{0,1}$ und $\overline{0, e^{I\varphi}}$. Der Punkt $e^{\frac{I\varphi}{2}}$ ist dann ein Schnittpunkt von H und der Einheitskreislinie.



□

Satz 6.3.17. *Es sei $\{0, 1\} \subseteq M \subseteq \mathbb{C}$, Für die Menge $\mathrm{Kon}(M)$ der aus M konstruierbaren komplexen Zahlen gilt:*

(i) *$\mathrm{Kon}(M)$ ist ein Zwischenkörper von $\mathbb{Q}(M \cup \overline{M}) \subseteq \mathbb{C}$.*
(ii) *Gilt $a^2 \in \mathrm{Kon}(M)$ für ein $a \in \mathbb{C}$, so gilt auch $a \in \mathrm{Kon}(M)$.*

Beweis. Für zwei komplexe Zahlen $z, w \in \mathrm{Kon}(M)$ betrachten wir ihre Zerlegungen $z = a + Ib$ und $w = c + Id$ in Real- und Imaginärteil. Dann gilt

$$\begin{aligned} \overline{z} &= a - Ib \\ -z &= -a - Ib \\ z + w &= a + c + I(b + d) \\ zw &= ac - bd + I(ad + bc) \\ z^{-1} &= \frac{a}{a^2 + b^2} - I\frac{b}{a^2 + b^2}. \end{aligned}$$

Mit Lemmata 6.3.14, 6.3.15 und Satz 6.3.13 (i) ergibt sich daher, dass die oben angeführten Zahlen in $\mathrm{Kon}(M)$ liegen. Das beweist die erste Aussage. Die zweite Aussage folgt direkt aus der ersten Aussage, Satz 6.3.13 (ii) und Lemma 6.3.16. □

Aufgaben zu Abschnitt 6.3.

Aufgabe 6.3.18. Es sei $M \subseteq \mathbb{C}$ eine Teilmenge mit $0, 1 \in M$. Zeige, dass $\mathrm{Kon}(M) = \overline{\mathrm{Kon}(M)}$ gilt. Gibt es einen Zwischenkörper $\mathbb{Q} \subseteq \mathbb{L} \subseteq \mathbb{C}$ mit $\mathbb{L} \neq \overline{\mathbb{L}}$?

Aufgabe 6.3.19. Es seien $z, w \in \mathbb{C}$ gegeben. Konstruiere die Zahl $(z + w)/2$ aus der Menge $M = \{z, w\}$.

Aufgabe 6.3.20. Konstruiere die Lösungen $z_1, z_2 \in \mathbb{C}$ der Gleichung $z^2 + 3z + 1 = 0$ aus der Menge $M = \{0, 1\}$.

Aufgabe 6.3.21. Zeige, dass die Menge $\mathrm{Kon}(0, 1) \subseteq \mathbb{C}$ der aus 0 und 1 konstruierbaren Punkte abzählbar ist.

6.4. **Drei klassische Probleme.**

Erinnerung 6.4.1. Wir sagen, dass ein Punkt $z \in \mathbb{C}$ aus einer Menge M (mit Zirkel und Lineal) konstruiert werden kann, wenn es eine Folge

$$M = M_0 \subseteq \ldots \subseteq M_r \subseteq \mathbb{C}$$

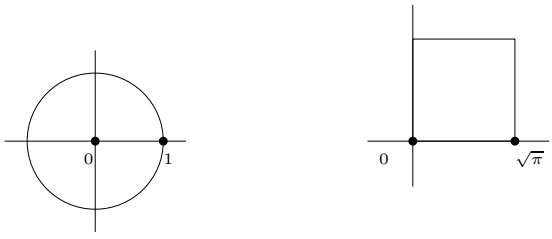
mit $z \in M_r$ gibt, wobei $M_j \subseteq M_{j+1}$ eine elementare Vergrößerung ist in dem Sinne, dass M_{j+1} aus M_j entsteht durch Hinzunahme des Durchschnittes

- zweier verschiedener Geraden $\overline{p_1, q_1}$ und $\overline{p_2, q_2}$ durch Punkte $p_i, q_i \in M_j$ oder
- einer Geraden $\overline{p_1, q_1}$ und eines Kreises $K(p, |p_2 - q_2|)$ mit Punkten $p, p_i, q_i \in M_j$ oder
- zweier verschiedener Kreise $K(p, |p_2 - q_2|)$ und $K(p', |p_1' - q_1'|)$ mit Punkten $p, p', p_1, q_1, p_1', q_1' \in M_j$.

Gilt $0, 1 \in M$, so ist die Menge $\mathrm{Kon}(M) \subseteq \mathbb{C}$ der aus M konstruierbaren Punkte ein Unterkörper von $\mathbb{C}$ mit $\mathbb{Q}(M \cup \overline{M}) \subseteq \mathrm{Kon}(M)$. Ist $a \in \mathbb{C}$ ein Punkt mit $a^2 \in \mathrm{Kon}(M)$, so gilt bereits $a \in \mathrm{Kon}(M)$.

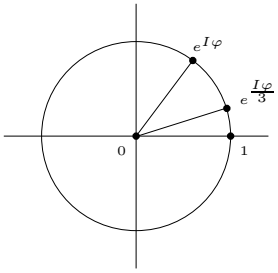
Problem 6.4.2. Die folgenden drei klassische Fragen legen Konstruierbarkeit mit Zirkel und Lineal im obigen Sinn zu Grunde.

(i) Die *Quadratur des Kreises*. Kann man aus $\{0, 1\}$ die Kantelänge Quadrats konstruieren, das denselben Flächeninhalt wie der Einheitskreis besitzt?



(ii) Die *Würfelverdopplung*. Kann man aus $\{0, 1\}$ die Kantenlänge eines Würfels konstruieren, der das doppelte Volumen des Einheitswürfels besitzt?

(iii) Die *Winkeldreiteilung*. Kann man einen gegebenen Winkel in drei gleiche Teilwinkel zerlegen, d.h. aus $\{0, 1, e^{I\varphi}\}$ die Zahl $\{0, 1, e^{\frac{I\varphi}{3}}\}$ konstruieren?



Satz 6.4.3. *Es sei $M \subseteq \mathbb{C}$ eine Teilmenge mit $0, 1 \in M$, und es sei $z \in \mathbb{C}$. Dann sind folgende Aussagen äquivalent:*

(i) *Es gilt $z \in \mathrm{Kon}(M)$.*
(ii) *Es gibt Zwischenkörper $\mathbb{Q}(M \cup \overline{M}) = \mathbb{L}_0 \subseteq \mathbb{L}_1 \subseteq \ldots \subseteq \mathbb{L}_n \subseteq \mathbb{C}$ mit*

$$z \in \mathbb{L}_n, \qquad [\mathbb{L}_i : \mathbb{L}_{i-1}] = 2 \text{ für } i = 1, \ldots, n.$$

Lemma 6.4.4. *Es sei $\mathbb{L} \subseteq \mathbb{C}$ ein Unterkörper mit $\mathbb{L} = \overline{\mathbb{L}}$ und $I \in \mathbb{L}$. Ist $z \in \mathbb{C}$ in einer elementaren Vergrößerung von $\mathbb{L}$ enthalten, so gibt es ein $w \in \mathbb{C}$ mit folgenden Eigenschaften:*

(i) *Es gilt $w^2 \in \mathbb{L}$ und $z \in \mathbb{L}(w)$.*
(ii) *Jeder Punkt von $\mathbb{L}(w)$ ist aus $\mathbb{L}$ konstruierbar.*
(iii) *Es gilt*

$$[\mathbb{L}(w) : \mathbb{L}] \quad = \quad \begin{cases} 1 & \text{falls } w \in \mathbb{L}, \\ 2 & \text{falls } w \notin \mathbb{L}. \end{cases}$$

Beweis. Zunächst sei vermerkt, dass wegen $\mathbb{L} = \overline{\mathbb{L}}$ und $i \in \mathbb{L}$ mit jedem Element $u \in \mathbb{L}$ auch Real- und Imaginärteil von u in $\mathbb{L}$ enthalten sind, denn wir haben

$$\Re(u) \; = \; \frac{u + \overline{u}}{2}, \qquad \Im(u) \; = \; \frac{u - \overline{u}}{2i}.$$

Wir zeigen nun, dass ein $w \in \mathbb{C}$ mit den Eigenschaften aus Teil (i) der Behauptung existiert. Dazu unterscheiden wir die folgenden drei Fälle.

Fall 1: Der Punkt $z \in \mathbb{C}$ ist der Schnittpunkt zweier (voneinander verschiedener) Geraden $G_1 = \overline{p_1, q_1}$ und $G_2 = \overline{p_2, q_2}$ mit $p_j, q_j \in \mathbb{L}$. Dann gibt es eindeutig bestimmte relle Zahlen t_1 und t_2 mit

$$z \; = \; p_1 + t_1(q_1 - p_1) = \; p_2 + t_2(q_2 - p_2).$$

Es seien nun $p_j = a_j + Ib_j$ und $q_j = c_j + Id_j$ die Zerlegungen von p_j und q_j in Real- und Imaginärteil. Dann erfüllen t_1 und t_2 das folgende Gleichungssystem:

$$\begin{aligned} a_1 + t_1(c_1 - a_1) \quad &= \quad a_2 + t_2(c_2 - b_2), \\ b_1 + t_1(d_1 - b_1) \quad &= \quad b_2 + t_2(d_2 - b_2). \end{aligned}$$

Wie eingangs beobachtet, haben wir $a_j, b_j, c_j, d_j \in \mathbb{L} \cap \mathbb{R}$. Folglich müssen t_1 und t_2 in $\mathbb{L} \cap \mathbb{R}$ liegen. Damit ergibt sich $z = p_1 + t_1(q_1 - p_1) \in \mathbb{L}$ und $w := z$ hat die gewünschten Eigenschaften.

Fall 2: Der Punkt $z \in \mathbb{C}$ ist Schnittpunkt eines Kreises $K(p, |q_1 - p_1|)$ und einer Geraden $\overline{p_2, q_2}$ mit $p, p_j, q_j \in \mathbb{L}$. In diesem Fall genügt z den Bedingungen

$$z \; = \; p_2 + t(q_2 - p_2), \qquad (z - p)\overline{(z - p)} \; = \; (q_1 - p_1)\overline{(q_1 - p_1)}$$

mit einer eindeutig bestimmten reellen Zahl t. Setzt man die linke Darstellung von z in die rechte Gleichung ein, so sieht man, dass t eine Gleichung

$$at^2 + bt + c \quad = \quad 0$$

mit Koeffizienten $a, b, c \in \mathbb{L}$ erfüllt, wobei $a \neq 0$. Wählt man nun ein $w \in \mathbb{C}$ mit $w^2 = b^2 - 4ac$, so gilt $w^2 \in \mathbb{L}$ und man erhält

$$z \; \in \; \left\{ p_2 + \frac{-b \pm w}{2a}(q_2 - p_2) \right\} \; \subseteq \; \mathbb{L}(w).$$

Fall 3: Der Punkt $z \in \mathbb{C}$ ist Schnittpunkt zweier (voneinander verschiedener) Kreise $K := K(p, |q_1 - p_1|)$ und $K' := K(p', |q_1' - p_1'|)$ mit $p, p', p_1, p_1', q_1, q_1' \in \mathbb{L}$. In diesem Fall genügt z den Gleichungen

$$(z - p)\overline{(z - p)} \; = \; (q_1 - p_1)\overline{(q_1 - p_1)}, \qquad (z - p')\overline{(z - p')} \; = \; (q_1' - p_1')\overline{(q_1' - p_1')}.$$

Subtrahiert man die zweite Gleichung von der ersten, so erhält man eine Bedingung der Form

$$az + b\overline{z} + c \quad = \quad 0$$

mit Koeffizienten $a, b, c \in \mathbb{L}$. Man beachte dabei, dass $p \neq p'$ bereits $a \neq 0 \neq b$ impliziert.

Wir zerlegen die Koeffizienten a, b, c jeweils in Real- und Imaginärteil: $a = a_1 + Ia_2$, $b = b_1 + Ib_2$ und $c = c_1 + Ic_2$. Dann erhalten wir für $z = x + Iy$ eine Bedingung der Form

$$A\begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} c_1 \\ c_2 \end{pmatrix} \quad = \quad \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \qquad \text{wobei } A \; = \; \begin{bmatrix} a_1 & b_1 \\ a_2 & b_2 \end{bmatrix}, \; a_j, b_j, c_j \in \mathbb{L} \cap R.$$

Dabei ist die Matrix A nicht trivial. Ist A vom Rang 2, so besitzt dieses Gleichungsystem genau eine Lösung (x, y), und es gilt $x, y \in \mathbb{L} \cap \mathbb{R}$. Das impliziert $z \in \mathbb{L}$ und somit hat $w := z$ die gewünschten Eigenschaften.

Ist A vom Rang 1, so besitzt das Gleichungssystem mindestens zwei Lösungen (x_1, y_1) und (x_2, y_2), mit $x_j, y_j \in \mathbb{L} \cap \mathbb{R}$. Es folgt, dass z Schnittpunkt der Geraden durch $x_1 + Iy_1$ und $x_2 + Iy_2$ mit einem der beiden Kreise K, K' ist. Fall 2 liefert also die Existenz des gesuchten $w \in \mathbb{C}$.

Die Tatsache, dass jeder Punkt aus $\mathbb{L}(w)$ aus $\mathbb{L}$ konstuierbar ist ergibt sich direkt aus Satz 6.3.17. Weiter gilt $[\mathbb{L}(w) : \mathbb{L}] \leq 2$, da $T^2 - w^2 \in \mathbb{L}[T]$ ein annullierendes Polynom für w ist. □

Beweis von Satz 6.4.3. Zu "(i)⇒(ii)". Wir wählen zunächst eine Folge elementarer Vergrößerungen $M = M_0 \subset \ldots \subset M_k$, sodass $z \in M_k$ gilt. Da M_j durch elementare Vergrößerung aus M_{j-1} entsteht, gilt $M_j = M_{j-1} \cup \{z_j\} \cup \{z_j'\}$ mit zwei nicht notwendigerweise verschiedenen Punkten $z_j, z_j' \in \mathbb{C}$.

Anfangend mit $\mathbb{L}_0 = \mathbb{Q}(M \cup \overline{M})$ konstruieren wir die gewünschte Folge von Zwischenkörpern. Zunächst setzen wir $\mathbb{K}_1 := \mathbb{L}_0(I)$. Dann ist $\mathbb{L}_0 \subseteq \mathbb{K}_1$ eine Erweiterung vom Grad höchstens 2, und wegen $\mathbb{L}_0 = \overline{\mathbb{L}_0}$ erhalten wir $\mathbb{K}_1 = \overline{\mathbb{K}_1}$.

Zu z_1 und $\mathbb{K}_1$ wählen wir $w_1 \in \mathbb{C}$ wie in Lemma 6.4.4 und setzen $\mathbb{K}_2 := \mathbb{K}_1(w_1)$. Dann ist $\mathbb{K}_1 \subseteq \mathbb{K}_2$ eine Erweiterung vom Grad höchstens 2. Wegen $\mathbb{K}_1 = \overline{\mathbb{K}_1}$ gilt $\overline{w_1}^2 = \overline{w^2} \in \mathbb{K}_1$, und wir erhalten mit $\mathbb{K}_3 := \mathbb{K}_2(\overline{w_1})$ eine Erweiterung $\mathbb{K}_2 \subseteq \mathbb{K}_3$ vom Grad höchstens 2, sodass mit $z_1 \in \mathbb{K}_3$ und $\mathbb{K}_3 = \overline{\mathbb{K}_3}$ gelten. Da z_1' und $\mathbb{K}_3$ ebenfalls die Voraussetzungen von Lemma 6.4.4 erfüllen, erhalten wir analog Erweiterungen $\mathbb{K}_3 \subseteq \mathbb{K}_4$ und $\mathbb{K}_4 \subseteq \mathbb{K}_5$ jeweils vom Grad höchstens 2, sodass $z_1' \in \mathbb{K}_5$ und $\mathbb{K}_5 = \overline{\mathbb{K}_5}$ gelten. Man beachte, dass jetzt $M_1 \subseteq \mathbb{K}_5$ gilt.

Dieses Verfahren können wir iterieren und erhalten schließlich eine Folge von Erweiterungen $\mathbb{L}_0 \subseteq \mathbb{K}_1 \subseteq \ldots \subseteq \mathbb{K}_l$ jeweils vom Grad höchstens zwei, sodass $z \in \mathbb{K}_l$ gilt. Indem man alle redundanten Schritte $\mathbb{K}_{j-1} = \mathbb{K}_j$ auslässt, erhält man daraus die gewünschte Folge $\mathbb{L}_0 \subset \ldots \subset \mathbb{L}_n$.

Zu "(ii)⇒(i)". Wir zeigen mittels Induktion über n, dass sämtliche Punkte von $\mathbb{L}_n$ aus M konstruierbar sind. Der Fall $n = 0$ ist Satz 6.3.17.

Zum Induktionsschritt. Da die Erweiterung $\mathbb{L}_{n-1} \subseteq \mathbb{L}_n$ vom Grad 2 ist, gilt $\mathbb{L}_n = \mathbb{L}_{n-1}(a)$ mit einem $a \in \mathbb{C}$. Das Minimalpolynom von a über $\mathbb{L}_{n-1}$ ist von der Form $T^2 + bT + c$ mit $b, c \in \mathbb{L}_{n-1}$. Folglich gilt

$$a \quad = \quad \frac{-b \pm \sqrt{b^2 - 4c}}{2}.$$

Das bedeutet, dass a aus $\mathbb{L}_{n-1}$ konstruierbar ist. Mit $\mathbb{L} = \mathbb{L}_{n-1}(a)$ sehen wir, dass damit jeder Punkt aus $\mathbb{L}_n$ aus $\mathbb{L}_{n-1}$ und somit gemäß Induktionsvoraussetzung aus M konstruierbar ist. □

Folgerung 6.4.5. *Es seien $M \subseteq \mathbb{C}$ mit $0, 1 \in M$ und $\mathbb{L} := \mathbb{Q}(M \cup \overline{M})$. Ist z aus M konstruierbar, so ist $[\mathbb{L}(z) : \mathbb{L}]$ eine Potenz von 2. Insbesondere ist z algebraisch über $\mathbb{L}$.*

Folgerung 6.4.6. *Die Quadratur des Kreises mit Zirkel und Lineal ist nicht möglich.*

Beweis. Es sei ein Kreis mit Radius 1 um 0 gegeben. Dieser Kreis hat bekanntlich den Flächeninhalt π. Die Frage ist, ob man mit Zirkel und Lineal aus den definierenden Daten $0, 1$ ein Quadrat des Inhalts π konstruieren kann. Ein solches Quadrat hätte die Kantenläge $\sqrt{\pi}$, die dann aus $0, 1$ konstruierbar wäre. Damit wäre auch $\pi = \sqrt{\pi}\sqrt{\pi}$ aus $0, 1$ konstruierbar. Nach Folgerung 6.4.5 wäre π dann algebraisch über $\mathbb{Q}$. Dies ist bekanntlich nicht der Fall. □

Folgerung 6.4.7 (Delisches Problem)**.** *Die Würfelverdopplung mit Zirkel und Lineal ist nicht möglich.*

Beweis. Die Frage ist, ob man aus den Eckpunkten $0, 1$ einer Kante des Einheitswürfels die Eckpunkte $0, a$ einer Kante eines Würfels doppelten Volumens konstruieren kann — anders formuliert, ob man $a = \sqrt[3]{2}$ aus $\{0, 1\}$ konstruieren kann. Wäre dies der Fall, so hätte man $[\mathbb{Q}(a) : \mathbb{Q}] = 2^n$ für ein $n \in \mathbb{Z}_{\geq 1}$ nach Folgerung 6.4.5. Das Minimalpolynom von a über $\mathbb{Q}$ ist jedoch $T^3 - 2$, und somit gilt $[\mathbb{Q}(a) : \mathbb{Q}] = 3$. □

Folgerung 6.4.8. *Die Winkeldreiteilung mit Zirkel und Lineal ist im allgemeinen nicht möglich.*

Beweis. Die Frage ist, ob man für gegebenes $\zeta = e^{i\alpha}$ stets $\eta = e^{i\beta}$ mit $\beta = \alpha/3$ aus $M = \{0, 1, \zeta\}$ konstruieren kann. Wir arbeiten mit

$$a \;:=\; \cos(\alpha) \;=\; \Re(\zeta), \qquad b \;:=\; \cos(\beta) \;=\; \Re(\eta).$$

Man beachte, dass die Konstruierbarkeit von β aus M äquivalent zur Konstruierbarkeit von b aus $M' := \{0, 1, a\}$ ist. Weiter gilt

$$\cos(3\beta) \quad = \quad 4\cos(\beta)^3 - 3\cos(\beta).$$

Wir zeigen, dass man für $a = \cos(\pi/3) = 1/2$ die Zahl $b = \cos(\pi/9)$ nicht aus M' konstruieren kann. Man beachte, dass $\mathbb{Q}(M' \cup \overline{M'}) = \mathbb{Q}$ gilt. Wegen obiger Identität für die Cosinusfunktion erhält man weiter ein annullierendes Polynom für b durch

$$f \;:=\; 4T^3 - 3T - \frac{1}{2} \;\in\; \mathbb{Q}(M' \cup \overline{M'})[T] \;=\; \mathbb{Q}[T].$$

Wir behaupten, dass f irreduzibel ist. Dazu betrachten wir den Isomorphismus $\mathbb{Q}[T] \mapsto \mathbb{Q}[T]$ mit $T \mapsto 1/2T$. Dieser bildet $2f$ ab auf $g := T^3 - 3T - 1$. Das Polynom g ist irreduzibel in $\mathbb{Z}[T]$, da es dort keine Nullstellen hat (mindestens ein Faktor einer nichttrivialen Zerlegung wäre vom Grad 1). Folglich ist g irreduzibel in $\mathbb{Q}[T]$ und somit ist auch f irreduzibel in $\mathbb{Q}[T]$.

Es folgt $[\mathbb{Q}(b) : \mathbb{Q}] = 3$. Nach Folgerung 6.4.5 kann b also nicht aus M' konstruiert werden. Somit kann der Winkel $\alpha = \pi/3$ nicht mittels Zirkel und Lineal dreigeteilt werden. □

Aufgaben zu Abschnitt 6.4.

Aufgabe 6.4.9. Zeige: Für $n = 3, 4, 6$ gilt $[\mathbb{Q}(e^{\frac{2\pi I}{n}}) : \mathbb{Q}] = 2$. Folgere, dass die Menge C_n der n-ten komplexen Einheitswurzeln für $n = 3, 4, 6$ aus 0 und 1 konstruierbar ist.

Aufgabe 6.4.10. Zeige mittels expliziter Konstruktionen, dass dass, die Menge C_n der n-ten komplexen Einheitswurzeln für $n = 3, 4, 5, 6$ aus 0 und 1 konstruierbar ist.

Aufgabe 6.4.11. Zeige: Die Menge C_7 der siebten komplexen Einheitswurzeln ist nicht aus 0 und 1 konstruierbar.

6.5. **Transzendenzbasen.**

Definition 6.5.1. Es sei $k \subseteq \mathbb{K}$ eine Körpererweiterung.

(i) Ein Element $a \in \mathbb{K}$ heißt *transzendent* über k, falls es nicht algebraisch über k ist.
(ii) Eine Körpererweiterung $k \subseteq \mathbb{K}$ heißt *transzendent* über k, falls sie nicht algebraisch ist.
(iii) Die Körpererweiterung $k \subseteq \mathbb{K}$ heißt, *rein transzendent*, falls jedes Element aus $\mathbb{K} \setminus k$ transzendent ist.

Definition 6.5.2. Es sei $k \subseteq \mathbb{K}$ eine Körpererweiterung.

(i) Eine Teilmenge $B \subseteq \mathbb{K}$ heißt *algebraisch unabhängig* über k, falls für jede endliche Teilmenge $\{b_1, \ldots, b_n\} \subseteq B$, wobei $b_i \neq b_j$ für $i \neq j$, und für jedes Polynom $f \in k[T_1, \ldots, T_n]$ gilt
$$f(b_1, \ldots, b_n) \;=\; 0 \quad \Longrightarrow \quad f \;=\; 0.$$
(ii) Eine maximale algebraisch unabhängige Teilmenge $B \subseteq \mathbb{K}$ nennt man eine *Transzendenzbasis* der Körpererweiterung $k \subseteq \mathbb{K}$.

Beispiel 6.5.3. Wir betrachten die Körpererweiterung $k \subseteq k(T_1, \ldots, T_n)$. Die Menge $\{T_1, \ldots, T_n\}$ ist algebraisch unabhängig über k, denn für jedes Polynom $f \in k[T_1, \ldots, T_n]$ hat man
$$f(T_1, \ldots, T_n) \;=\; 0 \quad \Longleftrightarrow \quad f \;=\; 0.$$
Weiter ist $\{T_1, \ldots, T_n\}$ maximal, denn jede Vergrösserung $\{T_1, \ldots, T_n, f/g\}$ ist algebraisch abhängig über k: Mit den Polynomen $f'(T_1, \ldots, T_{n+1}) := -f(T_1, \ldots, T_n)$ und $g'(T_1, \ldots, T_{n+1}) := g(T_1, \ldots, T_n)T_{n+1}$ hat man
$$(g' + f')(T_1, \ldots, T_n, f/g) \;=\; 0.$$
Folglich ist $\{T_1, \ldots, T_n\}$ eine Transzendenzbasis für $k(T_1, \ldots, T_n)$. Da $k(T_1, \ldots, T_n)$ zudem über k von $\{T_1, \ldots, T_n\}$ erzeugt wird, ist $k \subset k(T_1, \ldots, T_n)$ eine rein transzendente Erweiterung, wie wir später sehen werden.

Bemerkung 6.5.4. Es sei $k \subseteq \mathbb{K}$ eine Körpererweiterung. Ein Element $a \in \mathbb{K}$ ist genau dann transzendent über k, wenn $\{a\}$ algebraisch unabhängig über k ist.

Satz 6.5.5. *Ist $B = \{b_1, \ldots, b_n\}$ eine algebraisch unabhängige Teilmenge der Körpererweiterung $k \subseteq \mathbb{K}$, so gilt $k(B) \cong k(T_1, \ldots, T_n)$.*

Beweis. Die universelle Eigenschaft des Polynomringes 3.2.17 liefert uns einen Epimorphismus von Ringen
$$\Phi\colon k[T_1, \ldots, T_n] \;\to\; k[b_1, \ldots, b_n], \qquad f \;\mapsto\; f(b_1, \ldots, b_n).$$
Da $\{b_1, \ldots, b_n\}$ algebraisch unabhängig ist, gilt $\ker(\Phi) = \{0\}$. Somit ist Φ ein Isomorphismus und mit Satz 3.1.26 erhalten wir ein kommutatives Diagramm
$$\begin{array}{ccc} k[T_1, \ldots, T_n] & \xrightarrow{f \mapsto \Phi(f)} & k[b_1, \ldots, b_n] \\ {\scriptstyle f \mapsto \frac{f}{1}}\downarrow & & \downarrow{\scriptstyle b \mapsto b} \\ k(T_1, \ldots, T_n) & \xrightarrow[\frac{f}{g} \mapsto \frac{\Phi(f)}{\Phi(g)}]{} & k(b_1, \ldots, b_n) \end{array}$$
von Ringhomomorphismen. Nach Definition von $k(b_1, \ldots, b_n)$ ist der untere waagerechte Pfeil ein Epimorphismus von Körpern und somit ein Isomorphismus. $\square$

Satz 6.5.6. *Es sei $k \subseteq \mathbb{K}$ eine Körpererweiterung. Dann gilt:*

(i) *Sind $A \subseteq B \subseteq \mathbb{K}$ Teilmengen, und ist A algebraisch unabhängig über k, so gibt es eine Transzendenzbasis $C \subseteq B$ für $k \subseteq k(B)$ mit $A \subseteq C \subseteq B$.*
(ii) *Ist $B \subseteq \mathbb{K}$ eine Transzendenzbasis für $k \subseteq \mathbb{K}$, so ist $k \subseteq k(B)$ rein transzendent und $k(B) \subseteq \mathbb{K}$ ist algebraisch.*
(iii) *Für je zwei Transzendenzbasen $B, B' \subseteq \mathbb{K}$ von $k \subseteq \mathbb{K}$ gilt $|B| = |B'|$.*

Folgerung 6.5.7. *Jede Körpererweiterung $k \subseteq \mathbb{K}$ besitzt eine Transzendenzbasis.*

Beweis. Man wende Satz 6.5.6 (i) auf die Mengen $A = \emptyset$ und $B = \mathbb{K}$ an. □

Definition 6.5.8. Der *Transzendenzgrad* einer Körpererweiterung $k \subseteq \mathbb{K}$ ist die Ordnung einer Transzendenzbasis $B \subseteq \mathbb{K}$ für $k \subseteq \mathbb{K}$:

$$\operatorname{trdeg}_k(\mathbb{K}) \quad := \quad |B|.$$

Beispiel 6.5.9. Es sei k ein Körper. Für den Körper $k(T_1, \ldots, T_n)$ der rationalen Funktionen über k erhalten wir $\operatorname{trdeg}_k(k(T_1, \ldots, T_n)) = n$; siehe Beispiel 6.5.3.

Bemerkung 6.5.10. Es sei $k \subseteq \mathbb{K}$ eine endlich erzeugte Körpererweiterung. Dann gilt $\mathbb{K} = k(B)$ mit einer endlichen Menge $B \subseteq \mathbb{K}$. Nach Satz 6.5.6 (i) gibt es eine Transzendenzbasis C für $k \subseteq \mathbb{K}$ mit $C \subseteq B$. Es folgt $\operatorname{trdeg}_k(\mathbb{K}) = |C| < \infty$.

Lemma 6.5.11. *Es sei $k \subseteq \mathbb{K}$ eine Körpererweiterung,. und es sei $B \subseteq \mathbb{K}$ algebraisch unabhängig über k. Dann gilt:*

(i) *Jedes Element $b \in k(B) \setminus k$ ist transzendent über k.*
(ii) *Ein Element $a \in \mathbb{K}$ ist genau dann transzendent über $k(B)$, wenn $B \cup \{a\}$ algebraisch unabhängig über k ist.*

Beweis. Zu (i): Nehmen wir an, $b \in k(B) \setminus k$ sei algebraisch über k. Dann gibt es ein nichttriviales Polynom $f \in k[T]$ mit $f(b) = 0$. Wegen $b \in k(B) \setminus k$ gibt es weiter Elemente $b_1, \ldots, b_n \in B$, sodass

$$b \quad = \quad \frac{g(b_1, \ldots, b_n)}{h(b_1, \ldots, b_n)}$$

gilt mit teilerfremden Polynomen $g, h \in k[T_1, \ldots, T_n]$, von denen mindestens eines nicht konstant ist. Setzen wir diese Darstellung in $f(b) = 0$ ein, so erhalten wir algebraische Abhängigkeit von $\{b_1, \ldots, b_n\}$ wie folgt:

$$h(b_1, \ldots, b_n)^{\deg(f)} f\left(\frac{g(b_1, \ldots, b_n)}{h(b_1, \ldots, b_n)}\right) \quad = \quad 0.$$

Zu (ii): Es sei zunächst a transzendent über $k(B)$. Wäre $B \cup \{a\}$ algebraisch abhängig über k, so gäbe es $b_1, \ldots, b_r \in B$ und ein $f \in k[T_1, \ldots, T_{r+1}]$ mit

$$f(b_1, \ldots, b_r, a) \quad = \quad 0.$$

Sortiert man nun nach Potenzen der letzten Variablen, so ergibt sich, dass a algebraisch über $k(B)$ ist. Widerspruch.

Es sei jetzt $B \cup \{a\}$ algebraisch unabhängig. Nehmen wir an, a sei algebraisch über $k(B)$. Dann erhalten wir

$$c_0 + c_1 a + \ldots + c_{n-1} a^{n-1} + a^n \quad = \quad 0$$

mit gewissen Elementen $c_i \in k(B)$. Nun ist jedes dieser c_i mit geeigneten $b_j \in B$ und $g_i, h_i \in k[T_1, \ldots, T_r]$ von der Gestalt

$$c_i \quad = \quad \frac{g_i(b_1, \ldots, b_r)}{h_i(b_1, \ldots, b_r)}.$$

Geht man mit diesen Darstellungen der c_i in das oben gewählte annullierende Polynom von a und multipliziert mit dem Hauptnenner durch, so ergibt sich algebraische Abhängigkeit von $B \cup \{a\}$. Widerspruch. □

Beweis von Satz 6.5.6. Zu (i). Wir betrachten die (nichtleere) Menge M aller über k algebraisch unabhängigen Teilmengen $D \subseteq B$ mit $A \subseteq D$. Es sei D_i, $i \in I$, eine aufsteigende Kette in M. Dann ist

$$\bigcup_{i \in I} D_i$$

offensichtlich wieder algebraisch unabhängig und somit eine obere Schranke in M für die Kette D_i, $i \in I$. Nach dem Zornschen Lemma besitzt die Menge M also maximale Elemente. Es sei $C \in M$ ein solches.

Wir zeigen, dass C die gewünschte Transzendenzbasis für $k \subseteq k(B)$ ist. Offenbar gilt $A \subseteq C \subseteq B$. Wäre C nicht maximal in $k(B)$, so gäbe es ein Element $a \in k(B) \setminus C$, sodass $C \cup \{a\}$ algebraisch unabhängig über k ist. Nach Lemma 6.5.11 (ii) ist a transzendent über $k(C)$. Nun ist a von der Form

$$a \;=\; \frac{f(b_1, \ldots, b_r)}{g(b_1, \ldots, b_r)}$$

mit $f, g \in k[T_1, \ldots, T_r]$ und $b_i \in B$. Da a transzendent über $k(C)$ ist, muss nach Satz 6.2.12 (ii) ein b_i transzendent über $k(C)$ sein. Also ist $C \cup \{b_i\}$ nach Lemma 6.5.11 (ii) über k algebraisch unabhängige Menge. Dies widerspricht jedoch der Maximalität von $C \in M$.

Zu (ii). Die Tatsache, dass $k \subseteq k(B)$ rein transzendent ist, war bereits in Lemma 6.5.11 (i) bewiesen worden. Wäre $k(B) \subseteq \mathbb{K}$ nicht algebraisch, so gäbe es ein über $k(B)$ transzendentes Element $a \in \mathbb{K}$. Nach Lemma 6.5.11 (ii) wäre dann $B \cup \{a\}$ algebraisch unabhängig über k. Widerspruch zur Maximalität von B.

Zu (iii). Falls alle Transzendenzbasen von $k \subseteq \mathbb{K}$ unendlich sind, ist nichts zu zeigen. Wir dürfen also annehmen, dass eine endliche Transzendenzbasis $B = \{b_1, \ldots, b_n\}$ von $k \subseteq \mathbb{K}$ existiert. Zum Beweis von (iii) genügt es zu zeigen, dass jede weitere Transzendenzbasis von $k \subseteq \mathbb{K}$ höchstens n Elemente besitzt.

Nehmen wir an, eine Transzendenzbasis C von $k \subseteq \mathbb{K}$ besitze mehr als n Elemente. Wir wählen ein $c_1 \in C$ und betrachten die Körpererweiterung

$$k \;\subseteq\; k(c_1, b_1, \ldots, b_n).$$

Nach Aussage (i) finden wir eine Transzendenzbasis C_1 für diese Körpererweiterung, so dass $C_1 \subseteq B \cup \{c_1\}$ und $c_1 \in C_1$ gelten. Nach geeignetem Umnumerieren von $b_1, \ldots, b_n$ gilt also

$$C_1 \;=\; \{c_1, b_1, \ldots, b_{n_1}\}, \qquad \text{mit } n_1 < n.$$

Man beachte, dass nach der bereits bewiesenen Aussage (ii) die beiden Körpererweiterungen

$$k(C_1) \;\subseteq\; k(B \cup \{c_1\}), \qquad k(B \cup \{c_1\}) \;\subseteq\; \mathbb{K}$$

algebraisch sind. Nach Satz 6.2.12 (iii) ist damit auch die Erweiterung $k(C_1) \subseteq \mathbb{K}$ algebraisch.

In einem zweiten Schritt wählen wir ein $c_2 \in C$ mit $c_2 \neq c_1$, sodass $\{c_1, c_2\}$ algebraisch unabhängig ist. Wie oben erhalten wir nach Umnumerieren von $b_1, \ldots, b_{n_1}$ eine Tanszendenzbasis

$$C_2 \;=\; \{c_1, c_2, b_1, \ldots, b_{n_2}\}, \qquad \text{mit } n_2 < n_1$$

für die Körpererweiterung $k \subseteq k(C_1 \cup \{c_2\})$. Wie im ersten Schritt hat man auch hier algebraische Erweiterungen

$$k(C_2) \ \subseteq \ k(C_1 \cup \{c_2\}), \qquad k(C_1 \cup \{c_2\}) \ \subseteq \ \mathbb{K}$$

Folglich ist $k(C_2) \subseteq \mathbb{K}$ algebraisch. Nehmen wir nun nach diesem Verfahren weitere Elemente c_i aus C hinzu, so gelangen wir schließlich zu einer Menge

$$C_r \ = \ \{c_1, \ldots, c_r\}, \qquad r \leq n,$$

für die $k(C_r) \subseteq \mathbb{K}$ eine algebraische Erweiterung ist. Wegen $C_r \subsetneq C$ widerspricht das der algebraischen Unabhängigkeit von C. □

Aufgaben zu Abschnitt 6.5.

Aufgabe 6.5.12. Es seien $k \subseteq \mathbb{K}$ eine Körpererweiterung und $a \in \mathbb{K}$ transzendent über $\mathbb{K}$. Zeige: Für jedes $n \in \mathbb{Z}_{\geq 1}$ gilt

(i) $a^n \in \mathbb{K}$ ist transzendent über k,
(ii) $[k(a) : k(a^n)] = n$.

Aufgabe 6.5.13. Es sei $k \subseteq \mathbb{K}$ eine transzendente Körpererweiterung. Zeige: $k \subseteq \mathbb{K}$ besitzt unendlich viele echte Zwischenkörper.

Aufgabe 6.5.14. Es seien $k \subseteq \mathbb{K}$ Körpererweiterung und $B \subseteq \mathbb{K}$ eine Transzendenzbasis für $k \subseteq \mathbb{K}$. Beweise die Äquivalenz folgender Aussagen:

(i) Die Menge $k \cup B$ ist abzählbar.
(ii) Die Menge $\mathbb{K}$ ist abzählbar.

Hinweis: Satz 6.5.6 (ii). Folgere, dass jede Transzendenzbasis von $\mathbb{R}$ über $\mathbb{Q}$ überzählbar ist. Schließe insbesondere $\mathrm{trdeg}_{\mathbb{Q}}(\mathbb{R}) = \infty$.

7. Zerfällungskörper

7.1. **Zerfällungskörper.**

Erinnerung 7.1.1. Es sei $k \subseteq \mathbb{K}$ eine Körpererweiterung. Für jedes $b \in \mathbb{K}$ liefert die universelle Eigenschaft des Polynomringes einen Auswertungshomomorphismus

$$\varepsilon_b \colon k[T] \;\to\; \mathbb{K}, \qquad f = \sum a_\nu T^\nu \;\mapsto\; f(b) := \sum a_\nu b^\nu.$$

Man nennt $b \in \mathbb{K}$ eine *Nullstelle* des Polynoms $f \in k[T]$, falls $f(b) = 0$ gilt. Ist $b \in \mathbb{K}$ Nullstelle von $f \in k[T]$, so kann man den Linearfaktor $T - b$ in $\mathbb{K}[T]$ abspalten:

$$f \;=\; (T-b)g \qquad \text{mit einem } g \in \mathbb{K}[T].$$

Man sagt, dass ein Polynom $f \in k[T]$ über $\mathbb{K}$ in *Linearfaktoren* zerfällt, falls es Elemente $c \in k$ und $a_1, \ldots, a_n \in \mathbb{K}$ gibt mit

$$f \;=\; c \cdot (T-a_1) \cdots (T-a_n) \;\in\; \mathbb{K}[T].$$

Definition 7.1.2. Es seien k ein Körper und $f \in k[T]$ ein Polynom. Eine Körpererweiterung $k \subseteq \mathbb{K}$ heißt *Zerfällungskörper* für f, falls f über $\mathbb{K}$ in Linearfaktoren zerfällt und $\mathbb{K}$ minimal mit dieser Eigenschaft ist, d.h., f zerfällt über keinem Zwischenkörper $k \subseteq \mathbb{L} \subsetneq \mathbb{K}$ in Linearfaktoren.

Beispiel 7.1.3. Die Erweiterung $\mathbb{R} \subseteq \mathbb{C}$ ist ein Zerfällungskörper für das Polynom $T^2 + 1 \in \mathbb{R}[T]$.

Satz 7.1.4. *Es seien $k \subseteq \mathbb{K}$ eine Körpererweiterung, $f \in k[T]$ ein Polynom und $a_1, \ldots, a_n \in \mathbb{K}$ die Nullstellen von f in $\mathbb{K}$.*

(i) *Zerfällt f über $\mathbb{K}$ in Linearfaktoren, so ist die Erweiterung $k \subseteq k(a_1, \ldots, a_n)$ ein Zerfällungskörper für f.*
(ii) *Ist $k \subseteq \mathbb{K}$ ein Zerfällungskörper für f, so gilt $\mathbb{K} = k(a_1, \ldots, a_n)$. Insbesondere ist $k \subseteq \mathbb{K}$ endlich und algebraisch.*

Beweis. Zu (i). Offensichtlich zerfällt f über $k(a_1, \ldots, a_n)$ in Linearfaktoren. Ist $k \subseteq \mathbb{L} \subseteq k(a_1, \ldots, a_n)$ ein Zwischenkörper, sodass f bereits über $\mathbb{L}$ in Linearfaktoren zerfällt, so liegen die Nullstellen $a_1, \ldots, a_n$ von f in $\mathbb{L}$. Das impliziert $\mathbb{L} = k(a_1, \ldots, a_n)$. Aussage (ii) ergibt sich direkt aus der Minimalitätseigenschaft des Zerfällungskörpers und aus Satz 6.2.12 (ii). □

Beispiel 7.1.5. Die Erweiterung $\mathbb{Q} \subseteq \mathbb{Q}(I)$ ist Zerfällungskörper für das Polynom $T^2 + 1 \in \mathbb{Q}[T]$.

Beispiel 7.1.6. Wir betrachten das Polynom $f := T^3 - 2 \in \mathbb{Q}[T]$. Es zerfällt über dem Körper $\mathbb{C}$ der komplexen Zahlen:

$$f \;=\; (T-a_1)(T-a_2)(T-a_3), \qquad a_1 := \sqrt[3]{2}, \quad a_2 := e^{\frac{2\pi i}{3}} \sqrt[3]{2}, \quad a_3 := e^{\frac{4\pi i}{3}} \sqrt[3]{2}.$$

Also ist $\mathbb{Q} \subseteq \mathbb{K}$ mit $\mathbb{K} := \mathbb{Q}(a_1, a_2, a_3)$ ein Zerfällungskörper für f. Wir wollen den Grad $[\mathbb{K} : \mathbb{Q}]$ bestimmen und betrachten dazu

$$\mathbb{Q} \;\subseteq\; \mathbb{L} \;\subseteq\; \mathbb{K}, \qquad \mathbb{L} \;:=\; \mathbb{Q}(a_1).$$

Das Polynom $f \in \mathbb{Q}[T]$ ist irreduzibel; andernfalls könnte man einen Linearfaktor $g \in \mathbb{Q}[T]$ abspalten, was wegen $a_1, a_2, a_3 \notin \mathbb{Q}$ nicht möglich ist. Also ist $f \in \mathbb{Q}[T]$ das Minimalpolynom von $a_1 = \sqrt[3]{2}$, und wir erhalten

$$[\mathbb{L} : \mathbb{Q}] \;=\; \deg(f) \;=\; 3.$$

Jetzt wollen wir den Grad $[\mathbb{K} : \mathbb{L}]$ bestimmen. Dazu beachte man $\mathbb{K} = \mathbb{L}(e^{2\pi i/3})$. Also müssen wir das Minimalpolynom $g \in \mathbb{L}[T]$ von $e^{2\pi i/3}$ finden. Ein annullierendes Polynom ist

$$T^3 - 1 \;=\; (T-1)(T^2+T+1) \;\in\; \mathbb{L}[T].$$

Da T^2+T+1 keine reellen Nullstellen besitzt ist es irreduzibel über $\mathbb{L}$ und somit haben wir $g = T^2+T+1$ als Minimalpolynom für $e^{2\pi i/3}$. Das liefert $[\mathbb{K} : \mathbb{L}] = 2$ und somit

$$[\mathbb{K} : \mathbb{Q}] \;=\; [\mathbb{K} : \mathbb{L}] \cdot [\mathbb{L} : \mathbb{Q}] \;=\; 3 \cdot 2 \;=\; 6.$$

Satz 7.1.7. *Es seien k ein Körper und $f \in k[T]$. Dann gibt es einen Zerfällungskörper $k \subseteq \mathbb{K}$ für f.*

Lemma 7.1.8 (Kronecker)**.** *Es seien k ein Körper und $f \in k[T]$ nicht konstant. Dann gibt es eine Körpererweiterung $k \subseteq \mathbb{K}$, sodass f eine Nullstelle in $\mathbb{K}$ besitzt.*

Beweis. Nach Satz 4.3.7 besitzt f einen Primfaktor $p \in k[T]$. Nach Satz 4.1.22 ist $\langle p \rangle \subseteq k[T]$ ein maximales Ideal. Nach Satz 3.4.6 ist $\mathbb{K} := k[T]/\langle p \rangle$ ein Körper.

Weiter haben wir den Monomorphismus $k \to \mathbb{K}$, $a \mapsto a + \langle p \rangle$, und zu gegebenem $b \in \mathbb{K}$ haben wir den Auswertungshomomorphismus

$$\varepsilon_b \colon k[T] \;\to\; \mathbb{K}, \qquad f = \sum a_\nu T^\nu \;\mapsto\; f(b) := \sum a_\nu b^\nu.$$

Wir betrachten nun das Element $b := T + \langle p \rangle \in \mathbb{K}$. Werten wir das Polynom $p \in k[T]$ in b aus, so ergibt sich

$$\varepsilon_b(b) \;=\; p(b) \;=\; p(T + \langle p \rangle) \;=\; p(T) + \langle p \rangle \;=\; p + \langle p \rangle \;=\; 0 \;\in\; \mathbb{K}.$$

Mit anderen Worten: Das Element $b \in \mathbb{K}$ ist Nullstelle von $p \in k[T]$, und somit auch von $f \in k[T]$. □

Beweis von Satz 7.1.7. Es sei $n := \deg(f)$. Nach Lemma 7.1.8 gibt es eine Körpererweiterung $k \subseteq \mathbb{K}_1$, sodass $f \in k[T]$ eine Nullstelle a_1 in $\mathbb{K}_1$ besitzt. Abspalten des entsprechenden Linearfaktors liefert eine Darstellung

$$f \;=\; (T - a_1) f_1, \qquad f_1 \in \mathbb{K}_1[T], \quad \deg(f_1) = \deg(f) - 1.$$

Erneute Anwendung von Lemma 7.1.8 liefert eine Körpererweiterung $\mathbb{K}_1 \subseteq \mathbb{K}_2$, sodass $f_1 \in \mathbb{K}_1[T]$ eine Nullstelle a_2 in $\mathbb{K}_1$ besitzt. Damit erhalten wir eine Darstellung

$$f \;=\; (T - a_1)(T - a_2) f_2, \qquad f_2 \in \mathbb{K}_2[T], \quad \deg(f_2) = \deg(f) - 2.$$

Iteriert man diesen Prozess, so erhält man nach n Schritten eine Körpererweiterung $k \subseteq \mathbb{K}_n$, sodass f über $\mathbb{K}_n$ in Linearfaktoren zerfällt. Satz 7.1.4 liefert dann die Behauptung. □

Lemma 7.1.9. *Es sei $\varphi \colon \mathbb{K} \to \mathbb{K}'$ ein Homomorphismus von Körpern und es sei $\mathbb{K}'' := \varphi(\mathbb{K}) \subseteq \mathbb{K}'$ sein Bild.*

(i) *Man erhält eine kanonische Fortsetzung von $\varphi \colon \mathbb{K} \to \mathbb{K}'$ auf die Polynomringe durch*

$$\Phi \colon \mathbb{K}[T] \;\to\; \mathbb{K}'[T], \qquad \sum c_i T^i \;\mapsto\; \sum \varphi(c_i) T^i.$$

Ist $\varphi \colon \mathbb{K} \to \mathbb{K}'$ ein Isomorphismus, so ist $\Phi \colon \mathbb{K}[T] \to \mathbb{K}'[T]$ ebenfalls ein Isomorphismus.

(ii) *Ist $a \in \mathbb{K}$ Nullstelle eines Polynoms $f \in \mathbb{K}[T]$, so ist $\varphi(a) \in \mathbb{K}'$ Nullstelle des Polynoms $\Phi(f) \in \mathbb{K}'[T]$.*

(iii) *Durch $a \mapsto \varphi(a)$ erhalten wir eine Bijektion von der Menge N der Nullstellen von f in $\mathbb{K}$ auf die Menge N'' der Nullstellen von $\Phi(f)$ in $\mathbb{K}''$.*

Beweis. Aussage (i) folgt sofort aus der universellen Eigenschaft des Polynomringes. Zu (ii). Besitzt $f = \sum c_i T^i \in \mathbb{K}[T]$ die Nullstelle $a \in \mathbb{K}$, so haben wir

$$\Phi(f)(\varphi(a)) \;=\; \sum \varphi(c_i)\varphi(a)^i \;=\; \varphi\left(\sum c_i a^i\right) \;=\; \varphi(f(a)) \;=\; \varphi(0) \;=\; 0.$$

Zu (iii). Wir dürfen φ als Isomorphismus von $\mathbb{K}$ auf den Unterkörper $\mathbb{K}'' \subseteq \mathbb{K}$ auffassen. Nach (ii) liefert $a \mapsto \varphi(a)$ eine Injektion von N in die Menge N'' der Nullstellen von $\Phi(f)$ in $\mathbb{K}''$. Analog definiert $\varphi^{-1}\colon \mathbb{K}'' \to \mathbb{K}$ eine Injektion von N'' in die Menge N der Nullstellen von $\Phi^{-1}(\Phi(f)) = f$ in $\mathbb{K}$. □

Lemma 7.1.10. *Es seien $\varphi\colon k \to k'$ ein Körperisomorphismus und $\Phi\colon k[T] \to k'[T]$ seine Fortsetzung mit $\Phi(T) = T$. Weiter seien*

- *$f \in k[T]$ ein irreduzibles Polynom und $k \subseteq \mathbb{K}$ eine Körpererweiterung mit einer Nullstelle $a \in \mathbb{K}$ von f,*
- *$f' := \Phi(f) \in k'[T]$ und $k' \subseteq \mathbb{K}'$ eine Körpererweiterung mit einer Nullstelle $a' \in \mathbb{K}'$ von f'.*

Dann gibt es einen eindeutig bestimmten Isomorphismus $\widehat{\varphi}\colon k(a) \to k'(a')$, sodass $\widehat{\varphi}(a) = a'$ gilt und das folgende Diagramm kommutativ ist:

$$\begin{array}{ccc} k & \subseteq & k(a) \\ {\scriptstyle\varphi}\downarrow & & \downarrow{\scriptstyle\widehat{\varphi}} \\ k' & \subseteq & k'(a') \end{array}$$

Dabei definiert $b \mapsto \widehat{\varphi}(b)$ eine Bijektion $N \to N'$ von der Menge N der Nullstellen von f in $k(a)$ auf die Menge N' der Nullstellen von f' in $k'(a')$.

Beweis. Wir dürfen annehmen, dass f (und somit auch f') normiert ist. Dann ist f das Minimalpolynom zu a und f' das Minimalpolynom zu a'. Mit Satz 6.2.6 erhalten wir ein kommutatives Diagramm

$$\begin{array}{ccccccc} & & & & T\mapsto a & & \\ & & & \curvearrowright & & \curvearrowright & \\ k & \subseteq & k[T] & \longrightarrow & k[T]/\langle f\rangle & \xrightarrow{\cong} & k(a) \\ {\scriptstyle\varphi}\downarrow{\scriptstyle\cong} & & {\scriptstyle\Phi}\downarrow{\scriptstyle\cong} & & {\scriptstyle\cong}\downarrow{\scriptstyle\widehat{\Phi}} & & {\scriptstyle\cong}\downarrow{\scriptstyle\widehat{\varphi}} \\ k' & \subseteq & k'[T] & \longrightarrow & k[T]/\langle f'\rangle & \xrightarrow[\cong]{} & k'(a') \\ & & & \curvearrowright & & \curvearrowright & \\ & & & & T\mapsto a' & & \end{array}$$

wobei wir Existenz und Surjektivität des Körperhomomorphismus $\widehat{\Phi}$ mit dem Homomorphiesatz 3.3.16 erhalten. Das liefert die Existenz von $\widehat{\varphi}\colon k(a) \to k'(a)$, weiter $\widehat{\varphi}|_k = \varphi$ sowie $\widehat{\varphi}(a) = a'$ und die Eindeutigkeit von $\widehat{\varphi}$. □

Satz 7.1.11. *Es seien $\varphi\colon k \to k'$ ein Körperisomorphismus, $\Phi\colon k[T] \to k'[T]$ seine kanonische Fortsetzung und $k \subseteq \mathbb{K}$ bzw. $k' \subseteq \mathbb{K}'$ Zerfällungskörper für $f \in k[T]$ bzw. $f' := \Phi(f) \in k'[T]$. Dann gibt es ein kommutatives Diagramm*

$$\begin{array}{ccc} k & \subseteq & \mathbb{K} \\ {\scriptstyle\varphi}\downarrow & & \downarrow{\scriptstyle\widehat{\varphi}} \\ k' & \subseteq & \mathbb{K}' \end{array}$$

mit einem Körperisomorphismus $\widehat{\varphi}\colon \mathbb{K} \to \mathbb{K}'$. Dabei bildet $\widehat{\varphi}$ die Menge der Nullstellen von f in $\mathbb{K}$ bijektiv auf die Menge der Nullstellen von f' in $\mathbb{K}'$ ab.

Beweis. Gilt $k = \mathbb{K}$, so erhalten wir $k' = \mathbb{K}'$ mit Lemma 7.1.9 (iii) und Satz 7.1.4. Gilt $k \neq \mathbb{K}$, so besitzt $f \in k[T]$ eine Nullstelle $a_1 \in \mathbb{K} \setminus k$. Es sei $f_1 \in k[T]$ ein Primfaktor von f mit $f_1(a_1) = 0$; man beachte dabei, dass f_1 keine Nullstelle in k besitzt. Dann ist $f_1' \in k'[T]$ ein Primfaktor von f' und nach Lemma 7.1.9 (iii) hat f_1' keine Nullstelle in k'. Wir finden also eine Nullstelle $a_1' \in \mathbb{K}' \setminus k_1'$ von f_1'. Lemma 7.1.10 liefert ein kommutatives Diagramm

$$\begin{array}{ccccc} k & \subseteq & k(a_1) & =: & k_1 \\ {\scriptstyle\varphi}\downarrow{\scriptstyle\cong} & & {\scriptstyle\cong}\downarrow & & {\scriptstyle\cong}\downarrow{\scriptstyle\varphi_1} \\ k' & \subseteq & k'(a_1') & =: & k_1' \end{array}$$

mit einem Isomorphismus $\varphi_1 \colon k_1 \to k_1'$, sodass $\varphi_1(a_1) = a_1'$ gilt und φ_1 die Menge der Nullstellen von f_1 in k_1 bijektiv auf die Menge der Nullstellen von f_1' in k_1' abbildet. Gilt $k_1 = \mathbb{K}$, so haben wir die gesuchte Fortsetzung gefunden. Andernfalls besitzt f eine Nullstelle $a_2 \in \mathbb{K} \setminus k$. Dann wiederholen wir die obige Konstruktion mit $\varphi_1 \colon k_1 \to k_1'$ und erhalten entsprechend eine Fortsetzung $\varphi_2 \colon k_2 \to k_2'$. In jedem Schritt dieser Art verringert sich die Anzahl der Nullstellen von f in $\mathbb{K} \setminus k_i$. Somit terminiert das Verfahren nach endlich vielen Schritten mit $k_n = \mathbb{K}$. □

Definition 7.1.12. Eine algebraische Körpererweiterung $k \subseteq \mathbb{K}$ heißt *normal*, falls für jedes $a \in \mathbb{K}$ das Minimalpolynom $f_a \in k[T]$ über $\mathbb{K}$ in Linearfaktoren zerfällt.

Satz 7.1.13. *Es sei $k \subseteq \mathbb{K}$ eine endliche Körpererweiterung. Dann sind folgende Aussagen äquivalent:*

(i) *$k \subseteq \mathbb{K}$ ist normal.*
(ii) *$k \subseteq \mathbb{K}$ ist Zerfällungskörper eines Polynoms $f \in k[T]$.*
(iii) *Für jede Körpererweiterung $\mathbb{K} \subseteq \mathbb{L}$ und jeden Homomorphismus $\varphi \colon \mathbb{K} \to \mathbb{L}$ mit $\varphi|_k = \mathrm{id}_k$ gilt $\varphi(\mathbb{K}) \subseteq \mathbb{K}$.*

Beweis. Zur Implikation "(i)⇒(ii)". Nach Folgerung 6.2.14 gilt $\mathbb{K} = k(a_1, \ldots, a_n)$ mit $a_1, \ldots, a_n \in \mathbb{K}$. Da jedes der Minimalpolynome $f_i \in k[T]$ von $a_i \in \mathbb{K}$ über $\mathbb{K}$ in Linearfaktoren zerfällt, gilt dies auch für $f := f_1 \cdots f_n$. Da $a_1, \ldots, a_n$ Nullstellen von f sind, ist $\mathbb{K} = k(a_1, \ldots, a_n)$ ein Zerfällungskörper von f; siehe Satz 7.1.4.

Zur Implikation "(ii)⇒(iii)". Wir haben $\mathbb{K} = k(a_1, \ldots, a_n)$ mit den Nullstellen eines Polynoms $f \in k[T]$. Lemma 7.1.9 (ii) liefert $\varphi(a_i) = a_i$ und somit $\varphi(\mathbb{K}) = \mathbb{K}$.

Zur Implikation "(iii)⇒(i)". Für jedes $a \in \mathbb{K}$ ist zu zeigen, dass das Minimalpolynom $f_a \in k[T]$ über $\mathbb{K}$ in Linearfaktoren zerfällt. Nach Folgerung 6.2.14 ist $k \subseteq \mathbb{K}$ algebraisch und es gilt $\mathbb{K} = k(a_1, \ldots, a_n)$ mit $a_i \in \mathbb{K}$. Es sei $f_i \in k[T]$ das Minimalpolynom von $a_i \in \mathbb{K}$. Wir wählen einen Zerfällungskörper $\mathbb{K} \subseteq \mathbb{L}$ für

$$f \;:=\; f_a f_1 \cdots f_n \;\in\; k[T] \;\subseteq\; \mathbb{K}[T].$$

Für jede Nullstelle $b \in \mathbb{L}$ von f_a müssen wir $b \in \mathbb{K}$ zeigen. Lemma 7.1.10 liefert einen Isomorphismus $\varphi \colon k(a) \to k(b)$ mit $\varphi(a) = b$, der id_k fortsetzt. Weiter sind $k(a) \subseteq \mathbb{L}$ und $k(b) \subseteq \mathbb{L}$ Zerfällungskörper für $f \in k(a)[T]$ bzw. für $f \in k(b)[T]$. Mit Satz 7.1.11 erhalten wir daher eine Fortsetzung $\widehat{\varphi} \colon \mathbb{L} \to \mathbb{L}$ von φ. Eigenschaft (iii) liefert $\widehat{\varphi}(\mathbb{K}) = \mathbb{K}$. Insbesondere erhalten wir $b = \widehat{\varphi}(a) \in \mathbb{K}$. □

Aufgaben zu Abschnitt 7.1.

Aufgabe 7.1.14. Bestimme eine explizite Darstellung $\mathbb{K} = \mathbb{Q}(a_1, \ldots, a_r)$ mit $a_i \in \mathbb{C}$ sowie den Grad $[\mathbb{K} : \mathbb{Q}]$ für den Zerfällungskörper $\mathbb{Q} \subseteq \mathbb{K}$ von $f \in \mathbb{Q}[T]$ für

$$f = T^2 - 3, \qquad f = T^3 - 5, \qquad f = T^4 - 2.$$

Aufgabe 7.1.15. Welche der folgenden Körpererweiterungen sind normal (jeweils mit Begründung):

(i) $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{3})$,
(ii) $\mathbb{Q}(\sqrt{3}) \subseteq \mathbb{Q}(\sqrt[4]{3})$,
(iii) $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[4]{3})$.

Die Körper $\mathbb{Q}(\sqrt{3})$ und $\mathbb{Q}(\sqrt[4]{3})$ sind dabei als Unterkörper des Körpers $\mathbb{C}$ der komplexen Zahlen aufzufassen.

Aufgabe 7.1.16. Zeige: Jede Körpererweiterung vom Grad 2 ist normal.

7.2. **Algebraischer Abschluss.**

Definition 7.2.1. Es sei k ein Körper. Eine Körpererweiterung $k \subseteq \overline{k}$ heißt *algebraischer Abschluss* von k, falls

(i) jedes $f \in \overline{k}[T]$ über $\overline{k}$ in Linearfaktoren zerfällt,
(ii) die Körpererweiterung $k \subseteq \overline{k}$ algebraisch ist.

Man nennt k *algebraisch abgeschlossen*, falls $k \subseteq k$ ein algebraischer Abschluss ist, d.h., falls jedes $f \in k[T]$ über k in Linearfaktoren zerfällt.

Beispiel 7.2.2. Die Körper $\mathbb{Q}$ und $\mathbb{R}$ sind nicht algebraisch abgeschlossen. Nach dem Fundamentalsatz der Algebra 8.3.8 ist der Körper $\mathbb{C}$ algebraisch abgeschlossen.

Satz 7.2.3. *Sind k ein algebraisch abgeschlossener Körper, und $k \subseteq \mathbb{K}$ eine algebraische Erweiterung, so gilt $k = \mathbb{K}$.*

Beweis. Zu gegebenem $a \in \mathbb{K}$ betrachten wir das Minimalpolynom $f_a \in k[T]$. Da k algebraisch abgeschlossen ist, zerfällt f_a über k in Linearfaktoren:

$$f_a \;=\; c \cdot (T - a_1) \cdots (T - a_n) \;\in\; k[T]$$

mit $c, a_1, \ldots, a_n \in k$. Wegen $f_a(a) = 0$ folgt $a = a_i$ für ein i, und wir erhalten $a \in k$. Das impliziert $k = \mathbb{K}$. □

Satz 7.2.4. *Es sei $k \subseteq \mathbb{K}$ eine Körpererweiterung, sodass jedes $f \in \mathbb{K}[T]$ über $\mathbb{K}$ in Linearfaktoren zerfällt. Dann erhält man einen algebraischen Abschluss durch*

$$k \;\subseteq\; \overline{k} \;:=\; \{a \in \mathbb{K};\; a \text{ ist algebraisch über } k\}.$$

Beweis. Nach Folgerung 6.2.15 ist $\overline{k}$ ein Zwischenkörper von $k \subseteq \mathbb{K}$, und nach Definition ist $k \subseteq \overline{k}$ algebraisch.

Es sei nun ein Polynom $f \in \overline{k}[T]$ gegeben. Dann gibt es $a_i \in \mathbb{K}$ und eine Zerlegung in Linearfaktoren

$$f \;=\; c \cdot (T - a_1) \cdots (T - a_n) \;\in\; \mathbb{K}[T].$$

Nach Satz 6.2.12 (ii) ist $\overline{k} \subseteq \overline{k}(a_1, \ldots, a_n)$ algebraisch. Nach Satz 6.2.12 (iii) ist daher auch $k \subseteq \overline{k}(a_1, \ldots, a_n)$ algebraisch. Das impliziert $a_i \in \overline{k}$. □

Satz 7.2.5. *Jeder Körper k besitzt einen algebraischen Abschluss.*

Konstruktion 7.2.6 (Polynomring in beliebig vielen Unbestimmten)**.** Es seien R ein K1-Ring, und I eine beliebige Menge. Ein *Polynom* über R in der Veränderlichen T_i, $i \in I$, ist eine endliche formale Summe

$$\sum r_{i_1 \ldots i_k} T_{i_1}^{\nu_{i_1}} \cdots T_{i_k}^{\nu_{i_k}}$$

mit Koeffizienten $r_{i_1 \ldots i_k} \in R$. Analog zur Konstruktion 3.2.14 des Polynomringes in endlich vielen Veränderlichen definiert man Addition und Multiplikation auf der Menge dieser Polynome und gewinnt so den *Polynomring* $R[T_i;\; i \in I]$.

Ähnlich wie beim Polynomring in endlich vielen Veränderlichen hat man eine universelle Eigenschaft: Ist $\varphi\colon R \to S$ ein Homomorphismus von K1-Ringen, und sind Elemente $s_i \in S$, wobei $i \in I$, gegeben, so gibt es einen eindeutig bestimmten Homomorphismus $\Phi\colon R[T_i, i \in I] \to S$ mit $\Phi_{|R} = \varphi$ und $\Phi(T_i) = s_i$ für jedes $i \in I$.

Beweis von Satz 7.2.5. Nach Emil Artin. Wir teilen den Beweis in drei Schritte auf.

Schritt 1. Wir konstruieren eine Körpererweiterung $k \subseteq \mathbb{K}_1$, sodass jedes nicht konstante Polynom $f \in k[T]$ eine Nullstelle in $\mathbb{K}_1$ besitzt.

Wir betrachten die Menge I aller nichtkonstanten Polynome aus $k[T]$ und den Polynomring in den Veränderlichen S_f, $f \in I$:

$$I \ := \ k[T] \setminus k, \qquad R \ := \ k[S_f; \ f \in I].$$

Dann gilt $k \subseteq R$, und jedes Element $f \in I = k[T] \setminus k$ definiert auf kanonische Weise ein Element in R:

$$f(S_f) \ = \ \sum a_\nu S_f^\nu, \qquad \text{wobei } f \ = \ \sum a_\nu T^\nu.$$

Es sei $\mathfrak{a} \leq_R R$ das von allen Elementen $f(S_f)$, wobei $f \in I$, erzeugte Ideal. Wir zeigen, dass $\mathfrak{a}$ ein echtes Ideal ist. Andernfalls gäbe es $f_i \in I$ und $g_i \in R$ mit

$$1 \quad = \quad g_1 f_1(S_{f_1}) + \ldots + g_n f_n(S_{f_n}).$$

Durch wiederholte Anwendung von Lemma 7.1.8 erhalten wir eine Körpererweiterung $k \subseteq \mathbb{L}$, sodass jedes f_i in $k[T]$ eine Nullstelle $a_i \in \mathbb{L}$ besitzt.

Als Spezialfall der universellen Eigenschaft des Polynomringes R erhalten wir einen eindeutig bestimmten Auswertungshomomorphismus

$$\varphi\colon R \ \to \ \mathbb{L}, \qquad k \ni a \ \mapsto \ a \in \mathbb{L}, \quad S_f \ \mapsto \ \begin{cases} a_i & f = f_i \text{ mit } 1 \leq i \leq n, \\ 0 & f \notin \{f_1, \ldots, f_n\}. \end{cases}$$

Wendet man diesen Homomorphismus auf die obige Darstellung von $1 \in R$ an, so führt dies zu einem Widerspruch:

$$\mathbb{L} \ \ni \ 1 \ = \ \varphi(1) \ = \ \varphi(g_1) f_1(a_1) + \ldots + \varphi(g_n) f_n(a_n) \ = \ 0 \ \in \ \mathbb{L}.$$

Folglich ist $\mathfrak{a} \leq_R R$ ein echtes Ideal, und als solches ist es ein einem maximalen Ideal $\mathfrak{m} \leq_R R$ enthalten, siehe Satz 3.4.9. Der Restklassenring

$$\mathbb{K}_1 \quad := \quad R/\mathfrak{m}$$

ist nach Satz 3.4.6 ein Körper. Der kanonische Monomorphismus $k \to R \to \mathbb{K}_1$ bettet k als Unterkörper in $\mathbb{K}_1$ ein. Für jedes $f \in k[T] \setminus k$ gilt

$$f(S_f + \mathfrak{m}) \ = \ f(S_f) + \mathfrak{m} \ = \ 0 \ \in \ \mathbb{K}_1.$$

Also besitzt jedes nichtkonstante $f \in k[T]$ eine Nullstelle in $\mathbb{K}_1$. Damit ist Schritt 1 abgeschlossen.

Schritt 2. Wir konstruieren eine Körpererweiterung $k \subseteq \mathbb{K}$, sodass jedes Polynom $f \in \mathbb{K}[T]$ über $\mathbb{K}$ in Linearfaktoren zerfällt.

Durch wiederholtes Anwenden von Schritt 1 erhalten wir eine aufsteigende Kette von Körpererweiterungen

$$k \ = \ \mathbb{K}_0 \ \subseteq \ \mathbb{K}_1 \ \subseteq \ \mathbb{K}_2 \ \subseteq \ \ldots$$

sodass jedes Polynom $f \in \mathbb{K}_i[T]$ eine Nullstelle in $\mathbb{K}_{i+1}$ besitzt. Wir betrachten den "induktiven Limes"

$$\mathbb{K} \ := \ \left(\bigsqcup_{i=0}^{\infty} \mathbb{K}_i \right) \Big/ \sim, \qquad \text{wobei } \mathbb{K}_i \ni a \ \sim a \in \mathbb{K}_{i+l}, \ l \geq 0.$$

Dann ist $\mathbb{K}$ auf kanonische Weise ein Körper: Zu $a, b \in \mathbb{K}$ gibt es immer ein $\mathbb{K}_i$ mit $a, b \in \mathbb{K}_i$, daher kann man die Summe $a + b$ in $\mathbb{K}$ bilden etc..

Weiter erfüllt $\mathbb{K}$ die gewünschte Eigenschaft: Ist $f \in \mathbb{K}[T]$, so gilt $f \in \mathbb{K}_m[T]$ für ein m und f besitzt eine Nullstelle $a_1 \in \mathbb{K}_{m+1}$ und somit auch in $\mathbb{K}$. Nach Folgerung 4.2.5 gibt es eine Zerlegung

$$f \;=\; (T - a_1)f_1 \;\in\; \mathbb{K}[T],$$

wobei $\deg(f_1) < \deg(f)$. Wiederholt man dieses Verfahren für f_1 etc., so gelangt man nach $\deg(f) - 1$ Schritten zu einer Zerlegung von f in Linearfaktoren $T - a_i$ mit $a_i \in \mathbb{K}$.

Schritt 3. Es sei $\overline{k} \subseteq \mathbb{K}$ die Teilmenge aller Elemente $a \in \mathbb{K}$, die algebraisch über k sind. Nach Satz 7.2.4 ist $k \subseteq \overline{k}$ dann ein algebraischer Abschluss. □

Satz 7.2.7. *Es seien k ein Körper, $k \subseteq \overline{k}$ ein algebraischer Abschluss, $k \subseteq \mathbb{L} \subseteq \mathbb{K}$ algebraische Körpererweiterungen und $\varphi\colon \mathbb{L} \to \overline{k}$ ein Homomorphismus mit $\varphi|_k = \mathrm{id}_k$. Dann gibt es einen Homomorphismus $\Phi\colon \mathbb{K} \to \overline{k}$ mit $\Phi|_{\mathbb{L}} = \varphi$.*

Beweis. Es sei $\varphi\colon \mathbb{L} \to \overline{k}$ ein Homomorphismus mit $\varphi|_k = \mathrm{id}_k$. Wir betrachten die Menge S aller Paare (M, ψ), wobei $\mathbb{L} \subseteq M \subseteq \mathbb{K}$ ein Zwischenkörper ist und $\psi\colon M \to \overline{k}$ eine Fortsetzung von $\varphi\colon \mathbb{L} \to \overline{k}$ ist.

Die Menge S ist nicht leer; es gilt beispielsweise $(\mathbb{L}, \varphi) \in S$. Weiter haben wir eine natürliche Teilordnung auf S, nämlich

$$(M_1, \psi_1) \;\leq\; (M_2, \psi_2) \quad :\Longleftrightarrow \quad M_1 \subseteq M_2 \text{ und } \psi_2|_{M_1} = \psi_1.$$

Wir zeigen nun, dass jede total geordnete Teilmenge $S' \subseteq S$ eine obere Schranke in S besitzt. Dazu betrachten wir

$$M \;:=\; \bigcup_{(M',\psi') \in S'} M', \qquad \psi\colon M \;\to\; \overline{k},\; M' \ni a \;\mapsto\; \psi'(a) \in \overline{k}.$$

Dann ist M auf natürliche Weise ein Zwischenkörper von $k \subseteq \mathbb{K}$ und $\psi\colon M \to \overline{k}$ ist eine wohldefinierte Fortsetzung von $\varphi\colon \mathbb{L} \to \overline{k}$.

Nach dem Zornschen Lemma 3.4.10 besitzt die Menge S ein maximales Element (K, ψ). Wir zeigen, dass $K = \mathbb{K}$ gilt. Dazu nehmen wir an, es existiere ein $a \in \mathbb{K} \setminus K$. Nach Satz 6.2.6 gibt es einen Epimorphismus

$$\pi_a\colon K[T] \;\to\; K(a), \qquad f \;\mapsto\; f(a).$$

Nach Lemma 6.2.3 wird $\mathrm{Kern}(\pi_a)$ durch das Minimalpolynom $f_a \in K[T]$ erzeugt. Es sei $\Psi\colon K[T] \to \overline{k}[T]$ die kanonische Fortsetzung von $\psi\colon K \to \overline{k}$. Nach Lemma 7.1.9 besitzt $g_a := \Psi(f_a)$ mit $b := \psi(a)$ eine Nullstelle in $\overline{k}$. Das Polynom $g_a \in \overline{k}[T]$ liegt also im Kern der Auswertung

$$\pi_b\colon \overline{k}[T] \;\to\; \overline{k}, \qquad g \;\mapsto\; g(b).$$

Der Homomorphiesatz 3.3.16 liefert daher einen Homomorphismus $\psi_a\colon K(a) \to \overline{k}$, mit welchem das folgende Diagramm kommutativ wird:

$$\begin{array}{ccc}
K & \xrightarrow{\psi} & \overline{k} \\
\downarrow & & \downarrow \\
K[T] & \xrightarrow[\Psi]{T \mapsto T} & \overline{k}[T] \\
{\scriptstyle T \mapsto a}\downarrow & & \downarrow{\scriptstyle T \mapsto b} \\
K(a) & \xrightarrow[\psi_a]{} & \overline{k}
\end{array}
\qquad
\begin{array}{c}
\\ \\ \\ {\scriptstyle \pi_a}\downarrow \\ \\
\end{array}
\qquad
\begin{array}{c}
\\ \\ \\ {\scriptstyle \pi_b}\downarrow \\ \\
\end{array}$$

Nach Konstruktion ist ψ_a eine Fortsetzung von ψ. Damit ist $(K(a), \psi_a) \in S$ ein Element das echt größer ist als (M, ψ). Das steht im Widerspruch zur Maximalität von (M, ψ). □

Folgerung 7.2.8. *Es seien k ein Körper und $k \subseteq \overline{k}$ ein algebraischer Abschluss. Ist $k \subseteq \mathbb{K}$ eine algebraische Erweiterung, so gibt es einen Monomorphismus $\varphi\colon \mathbb{K} \to \overline{k}$ mit $\varphi|_k = \mathrm{id}_k$.*

Folgerung 7.2.9. *Es sei k ein Körper. Sind $k \subseteq k_1$ und $k \subseteq k_2$ algebraische Abschlüsse, so gibt es einen Isomorphismus $\varphi\colon k_1 \to k_2$ mit $\varphi|_k = \mathrm{id}_k$.*

Beweis. Nach Folgerung 7.2.8 gibt es einen Monomorphismus $\varphi\colon k_1 \to k_2$ mit $\varphi|_k = \mathrm{id}_k$. Somit erhalten algebraische Körperweiterungen $k \subseteq \varphi(k_1) \subseteq k_2$. Da $\varphi(k_1) \cong k_1$ algebraisch abgeschlossen ist, ergibt sich $\varphi(k_1) = k_2$ mit Satz 7.2.3. □

Aufgaben zu Abschnitt 7.2.

Aufgabe 7.2.10. Es sei $\mathbb{K}$ ein Körper. Beweise die Äquivalenz folgender Aussagen:

(i) $\mathbb{K}$ ist algebraisch abgeschlossen.
(ii) Jedes $f \in \mathbb{K}[T]$ besitzt eine Nullstelle in k.
(iii) Die irreduziblen Elemente in $\mathbb{K}[T]$ sind genau die Polynome vom Grad 1.
(iv) Für jede algebraische Körpererweiterung $\mathbb{K} \subseteq \mathbb{K}'$ gilt $\mathbb{K} = \mathbb{K}'$.

Aufgabe 7.2.11. Zeige: Jeder algebraisch abgeschlossene Körper besitzt unendlich viele Elemente.

Aufgabe 7.2.12. Zeige: Ist k ein abzählbarer Körper, so ist auch sein algebraischer Abschluss $\overline{k}$ abzählbar.

7.3. **Separable Polynome.**

Definition 7.3.1. Es seien k ein Körper, $k \subseteq \overline{k}$ ein algebraischer Abschluss und $f \in k[T]$. In der (eindeutigen) Primfaktorzerlegung

$$f \;=\; c\prod_{a\in\overline{k}}(T-a)^{\mu_f(a)}$$

in dem Polynomring $\overline{k}[T]$ nennt man den Exponenten $\mu_f(a) \in \mathbb{Z}_{\geq 0}$ die *Vielfachheit* von f in a.

Definition 7.3.2. Es sei R ein K1-Ring. Die *formale Ableitung* auf dem Polynomring $R[T]$ ist die Abbildung

$$D\colon R[T] \;\to\; R[T], \qquad \sum_{\nu=0}^{n} a_\nu T^\nu \;\mapsto\; \sum_{\nu=1}^{n} \nu a_\nu T^{\nu-1},$$

wobei wir νa_ν für $\nu \cdot 1_R \cdot a_\nu$ im letzten Term schreiben und $D(a_0T^0) := 0$ für jedes konstante Polynom $a_0T^0 \in R[T]$ setzen.

Beispiel 7.3.3. Das Polynom $f := (T-1)^2T = T^3 - 2T^2 + T \in \mathbb{R}[T]$ besitzt in $a \in \mathbb{C}$ die Vielfachheit

$$\mu_f(a) \;=\; \begin{cases} 1, & a = 0, \\ 2, & a = 1, \\ 0 & \text{sonst.} \end{cases}$$

Bemerkung 7.3.4. Es sei R ein K1-Ring. Für je zwei Polynome $f, g \in R[T]$ und je zwei Elemente $a, b \in R$ erfüllt die formale Ableitung die *Produktregel*:

$$D(af + bg) \;=\; aD(f) + bD(g), \qquad D(fg) \;=\; fD(g) + gD(f).$$

Lemma 7.3.5. *Es seien k ein Körper, $k \subseteq \overline{k}$ ein algebraischer Abschluss und $f \in k[T]$. Dann gilt für jedes $a \in \overline{k}$:*

$$\begin{aligned} \mu_f(a) = 1 \quad &\Longleftrightarrow \quad f(a) = 0 \text{ und } (D(f))(a) \neq 0, \\ \mu_f(a) > 1 \quad &\Longleftrightarrow \quad f(a) = 0 \text{ und } (D(f))(a) = 0. \end{aligned}$$

Beweis. Für jedes $a \in \overline{k}$ hat man eine Darstellung $f = (T-a)^{\mu_f(a)}g$ mit einem Polynom $g \in \overline{k}[T]$, sodass $g(a) \neq 0$ gilt. Wir erhalten

$$D(f) \;=\; \mu_f(a)(T-a)^{\mu_f(a)-1}g + (T-a)^{\mu_f(a)}D(g)$$

mit Hilfe der Produktregel aus Lemma 7.3.5. Damit lässt sich die Behauptung direkt verifizieren. □

Lemma 7.3.6. *Es seien k ein Körper, $k \subseteq \overline{k}$ ein algebraischer Abschluss und $f \in k[T]$. Dann sind äquivalent:*

(i) *Das Polynom f hat eine mehrfache Nullstelle in $\overline{k}$, d.h., es gilt $\mu_f(a) \geq 2$ für ein $a \in \overline{k}$.*
(ii) *Die Polynome f und $D(f)$ haben einen nicht-konstanten gemeinsamen Teiler in $k[T]$.*

Beweis. Zur Implikation "(i)⇒(ii)". Besitzt f eine mehrfache Nullstelle $a \in \overline{k}$, so gilt $f(a) = D(f)(a) = 0$ nach Lemma 7.3.5. Folglich ist das Minimalpolynom $f_a \in k[T]$ ein (nicht konstanter) Teiler von f und $D(f)$ in $k[T]$.

Zur Implikation "(ii)⇒(i)". Es sei $g \in k[T]$ ein nicht konstanter gemeinsamer Teiler von f und $D(f)$. Dann gilt $g(a) = 0$ für ein $a \in \overline{k}$. Es folgt $f(a) = D(f)(a) = 0$. Nach Lemma 7.3.5 besitzt f daher eine mehrfache Nullstelle. □

Bemerkung 7.3.7. Es seien R ein K1-Ring und $f, g \in R[T]$. Nach der universellen Eigenschaft des Polynomrings gibt es einen eindeutig bestimmten Homomorphismus

$$\Phi\colon R[T] \to R[T], \qquad \text{mit } \Phi_{|R} = \mathrm{id}_R \text{ und } \Phi(T) = g.$$

Man definiert die *Verkettung* der Polynome f und g als $f(g) := \Phi(f)$. Die formale Ableitung erfüllt die *Kettenregel*:

$$D(f(g)) \;=\; D(f)(g)D(g).$$

Lemma 7.3.8. *Es seien k ein Körper und $f \in k[T]$ ein Polynom.*

(i) *Im Falle* $\mathrm{Char}(k) = 0$ *hat man*

$$D(f) = 0 \quad\Longleftrightarrow\quad f \text{ ist konstant.}$$

(ii) *Im Falle* $\mathrm{Char}(k) = p > 0$ *hat man*

$$D(f) = 0 \quad\Longleftrightarrow\quad f = g(T^p) \text{ mit einem } g \in k[T].$$

Beweis. Es sei $f = \sum_{\nu=0}^{n} a_\nu T^\nu$. Wir zeigen (i). Die formale Ableitung $D(f)$ ist nach Definition gegeben als

$$D(f) \;=\; \sum_{\nu=1}^{n} \nu a_\nu T^{\nu-1}.$$

Für jedes $\nu = 1, \ldots, n$ haben wir wegen $\mathrm{Char}(\mathbb{K}) = 0$ genau dann $\nu a_\nu = 0$, wenn $a_\nu = 0$ gilt. Mit der obigen Formel ergibt sich daher

$$D(f) = 0 \iff a_1 = \ldots = n a_n = 0 \iff a_1 = \ldots = a_n = 0 \iff f = a_0 T^0.$$

Wir zeigen (ii). Es sei zunächst $f = g(T^p)$ mit einem Polynom $g \in k[T]$. Mit Bemerkung 7.3.7 erhalten wir

$$D(f) \;=\; D(g(T^p)) \;=\; D(g)(T^p)D(T^p) \;=\; D(g)(T^p)pT^{p-1} \;=\; 0 \;\in\; k[T].$$

Gilt $D(f) = 0$, so folgt $\nu a_\nu = 0$ für jedes $\nu \geq 1$. Wegen $\mathrm{Char}(k) = p$ haben wir genau dann $\nu = \nu \cdot 1_k = 0$, wenn $\nu = p\kappa$ mit einem $\kappa \in \mathbb{Z}_{\geq 0}$ gilt. Somit erhalten wir

$$f \;=\; \sum_{\kappa} a_{p\kappa} T^{p\kappa}.$$

Mit $g := \sum a_{p\kappa} T^\kappa$ haben wir also ein Polynom in $k[T]$ gefunden, das $f = g(T^p)$ leistet. □

Definition 7.3.9. Es seien k ein Körper und $k \subseteq \overline{k}$ ein algebraischer Abschluss.

(i) Ein irreduzibles Polynom $f \in k[T]$ heißt *separabel*, falls $\mu_f(a) \leq 1$ für jedes $a \in \overline{k}$ gilt.
(ii) Ein beliebiges Polynom $f \in k[T]$ heißt *separabel*, falls jeder irreduzible Faktor $p \in k[T]$ von f separabel ist.

Satz 7.3.10. *Es sei k ein Körper. Ein irreduzibles Polynom $f \in k[T]$ ist genau dann separabel, wenn $D(f) \neq 0$ gilt.*

Beweis. Es sei zunächst $f \in k[T]$ separabel. Ist $k \subseteq \overline{k}$ ein algebraischer Abschluss, so besitzt f eine Nullstelle $a \in \overline{k}$. Diese ist nach Voraussetzung einfach. Mit Lemma 7.3.5 erhalten wir daher $(Df)(a) \neq 0$. Folglich muss $D(f) \neq 0$ gelten.

Es sei nun $D(f) \neq 0$. Wäre f nicht separabel, so gäbe es nach Lemma 7.3.6 einen nichtkonstanten gemeinsamen Teiler $g \in k[T]$ von f und $D(f)$. Insbesondere hat man $\deg(g) \leq \deg(D(f)) < \deg(f)$. Wegen der Irreduzibilität von f muss aber $\deg(g) = \deg(f)$ gelten, Widerspruch. □

Definition 7.3.11. Ein Körper k heißt *vollkommen*, falls jedes nichtkonstante Polynom $f \in k[T]$ separabel ist.

Satz 7.3.12. *Jeder Körper der Charakteristik Null ist vollkommen.*

Beweis. Nach Lemma 7.3.8 und Satz 7.3.10 ist jedes irreduzible Polynom $f \in k[T]$ separabel. □

Beispiel 7.3.13. Es sei $p \in \mathbb{Z}_{\geq 0}$ eine Primzahl. Wir betrachten $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ und den Funktionenkörper $k := \mathbb{F}_p(T)$. Das Polynom

$$f \;:=\; S^p - T \;\in\; k[S]$$

ist f irreduzibel, denn es erfüllt die Bedingungen des Eisensteinkriteriums 6.2.8 zum Primelement $T \in \mathbb{F}_p[T]$. Weiter haben wir

$$D(f) \;=\; pS^{p-1} \;=\; 0 \;\in\; k[S].$$

Folglich ist das Polynom $f \in k[S]$ nicht separabel. Insbesondere ist der Funktionenkörper $k = \mathbb{F}_p(T)$ nicht vollkommen.

Konstruktion 7.3.14. Es sei $\mathbb{K}$ ein Körper der Charakteristik $p > 0$. Der *Frobeniushomomorphismus* auf $\mathbb{K}$ ist der Monomorphismus

$$\mathrm{Frob}_{\mathbb{K}} \colon \mathbb{K} \;\to\; \mathbb{K}, \qquad a \;\mapsto\; a^p.$$

Beweis. Wir müssen lediglich zeigen, dass $\mathrm{Frob}_{\mathbb{K}}$ mit der Addition verträglich ist. Für je zwei $a, b \in \mathbb{K}$ erhalten wir mit dem binomischen Lehrsatz:

$$(a+b)^p \;=\; \sum_{i=k}^{p} \binom{p}{k} \cdot 1_{\mathbb{K}}\, a^{p-k} b^k \;=\; a^p + b^p.$$

□

Satz 7.3.15. *Es sei $\mathbb{K}$ ein endlicher Körper. Dann gilt:*

(i) $\mathrm{Frob}_{\mathbb{K}} \colon \mathbb{K} \to \mathbb{K}$ *ist ein Isomorphismus.*
(ii) *Gilt* $\mathbb{K} \cong \mathbb{F}_p$*, so gilt* $\mathrm{Frob}_{\mathbb{K}} = \mathrm{id}_{\mathbb{K}}$.

Beweis. Aussage (i) ist klar, da jede injektive Selbstabbildung einer endlichen Menge auf sich bijektiv ist. Aussage (ii) erhält man mit

$$\mathrm{Frob}_{\mathbb{F}_p}(\overline{n}) \;=\; \mathrm{Frob}_{\mathbb{F}_p}(\overline{1} + \ldots + \overline{1}) \;=\; \overline{1} + \ldots + \overline{1} \;=\; \overline{n}.$$

□

Satz 7.3.16. *Es sei $\mathbb{K}$ ein Körper mit* $\mathrm{Char}(\mathbb{K}) = p > 0$*. Dann sind folgende Aussagen äquivalent:*

(i) $\mathbb{K}$ *ist vollkommen.*
(ii) $\mathrm{Frob}_{\mathbb{K}} \colon \mathbb{K} \to \mathbb{K}$ *ist surjektiv.*

Beweis. Zu "(i)⇒(ii)". Ist $a \in \mathbb{K}$ gegeben, so suchen wir ein $b \in \mathbb{K}$ mit $a = b^p$. Dazu betrachten wir das Polynom

$$f \;:=\; T^p - a \;\in\; \mathbb{K}[T]$$

und einen irreduziblen Faktor $g \in \mathbb{K}[T]$ von f. Es sei $\mathbb{K} \subseteq \bar{\mathbb{K}}$ ein algebraischer Abschluss. Dann besitzt g eine Nullstelle $b \in \bar{\mathbb{K}}$, und für diese gilt $a = b^p$. Es folgt

$$f \;=\; T^p - b^p \;=\; (T-b)^p \;\in\; \bar{\mathbb{K}}[T].$$

Als Faktor von $f \in \bar{\mathbb{K}}[T]$ ist $g \in \bar{\mathbb{K}}[T]$ deshalb von der Gestalt $g = (T-b)^l$ mit einem $l \leq k$. Da $\mathbb{K}$ vollkommen ist, muss g separabel über $\mathbb{K}$ sein. Das impliziert $g = T - b$, und wir erhalten $b \in \mathbb{K}$.

Zu "(ii)⇒(i)". Es sei $g \in \mathbb{K}[T]$ ein irreduzibles Polynom. Wir müssen zeigen, dass g separabel über $\mathbb{K}$ ist.

Nehmen wir an, g sei nicht separabel. Nach Satz 7.3.10 gilt dann $D(g) = 0$. Nach Lemma 7.3.8 gibt es ein $h \in \mathbb{K}[T]$ mit

$$g \;=\; h(T^p) \;=\; a_n(T^p)^n + \ldots + a_1T^p + a_0,$$

wobei $h = \sum a_\nu T^\nu$. Nach Voraussetzung gibt es Elemente $b_\nu \in \mathbb{K}$ mit $b_\nu^p = a_\nu$. Damit erhalten wir

$$g \;=\; b_n^p(T^p)^n + \ldots + b_1^pT^p + b_0 \;=\; (b_n(T)^n + \ldots + b_1T + b_0)^p.$$

Das steht jedoch im Widerspruch zur Irreduzibilität von g. Folglich muss g separabel sein, d.h., der Körper $\mathbb{K}$ ist vollkommen. □

Folgerung 7.3.17. *Jeder endliche Körper ist vollkommen.*

Aufgaben zu Abschnitt 7.3.

Aufgabe 7.3.18. Es sei R ein K1-Ring. Beweise die Rechenregeln aus Bemerkung 7.3.4: Für je zwei Polynome $f, g \in R[T]$ und je zwei Elemente $a, b \in R$ gilt

$$D(af + bg) \;=\; aD(f) + bD(g), \qquad D(fg) \;=\; fD(g) + gD(f).$$

Aufgabe 7.3.19. Es seien R ein K1-Ring und $f, g \in R[T]$ zwei Polynome. Beweise folgende Eigenschaften der Verkettung $f(g) \in R[T]$, vgl. Bemerkung 7.3.7:

(i) Für jedes $a \in R$ hat man $f(g)(a) = f(g(a))$.
(ii) Für die formale Ableitung gilt $D(f(g)) = D(f)(g)D(g)$.

7.4. **Endliche Körper.**

Erinnerung 7.4.1. Für jede Primzahl $p \in \mathbb{Z}_{\geq 0}$ ist $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ ein endlicher Körper. Es gilt

$$|\mathbb{F}_p| \;=\; p, \qquad \mathrm{Char}(\mathbb{F}_p) \;=\; p$$

und $\mathbb{F}_p$ ist sein eigener Primkörper. Ist $\mathbb{K}$ ein endlicher Körper, so ist $p := \mathrm{Char}(\mathbb{K})$ eine Primzahl und wir haben

$$\mathbb{P}_{\mathbb{K}} \;\cong\; \mathbb{F}_p, \qquad |\mathbb{K}| = p^n, \text{ wobei } n := [\mathbb{K} : \mathbb{P}_{\mathbb{K}}].$$

Ein Beispiel für einen Körper mit $4 = 2^2$ Elementen ist der Faktorring $\mathbb{F}_2[T]/\langle f\rangle$ mit dem irreduziblen Polynom $f := T^2 + T + \overline{1} \in \mathbb{F}_2[T]$.

Lemma 7.4.2. *Es sei $\mathbb{K}$ ein endlicher Körper. Dann ist das Produkt aller Einheiten von $\mathbb{K}$ gegeben durch*

$$\prod_{a\in\mathbb{K}^*} a \;\;=\;\; -1_{\mathbb{K}}.$$

Beweis. Wir zerlegen das fragliche Produkt zunächst in die Produkte über alle a mit $a = a^{-1}$ bzw. $a \neq a^{-1}$. Das liefert

$$\prod_{a\in\mathbb{K}^*} a \;=\; \left(\prod_{\substack{a\in\mathbb{K}^*\\ a=a^{-1}}} a\right)\left(\prod_{\substack{a\in\mathbb{K}^*\\ a\neq a^{-1}}} a\right) \;=\; \prod_{\substack{a\in\mathbb{K}^*\\ a=a^{-1}}} a.$$

Weiter impliziert $a = a^{-1}$, dass a Nullstelle von $T^2 - 1$ ist, und somit gilt $a = \pm 1$. Damit folgt die Behauptung. □

Folgerung 7.4.3 (Satz von Wilson)**.** *Für jede Primzahl $p \in \mathbb{Z}_{\geq 1}$ gilt $(p-1)! \equiv -1 \mod p$.*

Beweis. Die Behauptung ergibt sich durch Anwenden von Lemma 7.4.2 auf den Körper $\mathbb{F}_p$: Dort gilt

$$\overline{1}\cdot\overline{2}\cdots\overline{p-1} \;=\; -\overline{1} \;=\; \overline{-1}.$$

□

Satz 7.4.4 (Klassifikation endlicher Körper)**.** *Für eine Primzahl $p \in \mathbb{Z}_{\geq 2}$ und $n \in \mathbb{Z}_{\geq 1}$ bezeichne $\mathbb{F}_{p^n}$ den Zerfällungskörper des Polynoms $f := T^{p^n} - T \in \mathbb{F}_p[T]$.*

(i) *Der Körper $\mathbb{F}_{p^n}$ hat genau p^n Elemente.*
(ii) *Jedes Element $a \in \mathbb{F}_{p^n}$ ist Nullstelle von f, d.h., es gilt $a^{p^n} = a$,*

Ist $\mathbb{K}$ ein endlicher Körper, so gilt $|\mathbb{K}| = p^n$ mit einer Primzahl p und einem $n \in \mathbb{Z}_{\geq 1}$ und $\mathbb{K}$ isomorph zu $\mathbb{F}_{p^n}$.

Beweis. Zu (i) und (ii). Wir betrachten das Polynom $f := T^{p^n} - T \in \mathbb{F}_p[T]$ und die Menge seiner Nullstellen in $\mathbb{F}_{p^n}$:

$$\mathbb{L} \;:=\; \{a \in \mathbb{F}_{p^n};\; f(a) = 0\} \;:=\; \left\{a \in \mathbb{F}_{p^n};\; a^{p^n} = a\right\} \;\subseteq\; \mathbb{F}_{p^n}.$$

Wir zeigen, dass $\mathbb{L}$ ein Unterkörper von $\mathbb{K}$ ist. Für je zwei Elemente $a, b \in \mathbb{L}$ erhält man $a \pm b \in \mathbb{L}$ wegen

$$(a \pm b)^{p^n} \;=\; a^{p^n} \pm b^{p^n} \;=\; a \pm b.$$

Weiter ergibt sich für $a, b \in \mathbb{L}$ stets $ab \in \mathbb{L}$ und, falls $b \neq 0$, auch $b^{-1} \in \mathbb{L}$, denn es gilt

$$(ab)^{p^n} \;=\; a^{p^n} b^{p^n} \;=\; ab, \qquad \left(b^{-1}\right)^{p^n} \;=\; \left(b^{p^n}\right)^{-1} \;=\; b^{-1}.$$

Die Menge $\mathbb{L} \subseteq \mathbb{F}_{p^n}$ der Nullstellen von f ist also ein Zwischenkörper von $\mathbb{F}_p \subseteq \mathbb{F}_{p^n}$. Andererseits ist $\mathbb{F}_p \subseteq \mathbb{F}_{p^n}$ ein Zerfällungskörper von f. Das impliziert

$$\mathbb{L} \;=\; \mathbb{F}_{p^n}.$$

Wegen $D(f) = p^n T^{p^n-1} - 1 = -1$ besitzt f keine mehrfachen Nullstellen in $\mathbb{F}_{p^n}$, siehe Lemma 7.3.5. Folglich gilt

$$|\mathbb{F}_{p^n}| \;=\; |\mathbb{L}| \;=\; p^n.$$

Ist $\mathbb{K}$ ein endlicher Körper, so gilt $|\mathbb{K}| = p^n$ mit einer Primzahl p und einem $n \in \mathbb{Z}_{>0}$; siehe Satz 6.1.18. Der kleine Fermatsche Satz 2.1.8 liefert $a^{p^n-1} = 1$ für jedes $a \in \mathbb{K}^*$. Es folgt $a^{p^n} = a$ für jedes $a \in \mathbb{K}$. Somit ist $\mathbb{K}$ ein Zerfällungskörper des Polynoms $T^{p^n} - T \in \mathbb{P}_{\mathbb{K}}[T]$. Mit $\mathbb{P}_{\mathbb{K}} \cong \mathbb{F}_p$ erhalten wir $\mathbb{K} \cong \mathbb{F}_{p^n}$; siehe Satz 7.1.11. □

Folgerung 7.4.5. *Zu jedem Paar (p, n) mit einer Primzahl p und einer positiven ganzen Zahl n gibt es bis auf Isomorphie genau einen Körper der Ordnung p^n.*

Satz 7.4.6. *Es seien $\mathbb{K}$ ein endlicher Körper und $|\mathbb{K}| = p^n$.*

(i) *Ist $\mathbb{P}_{\mathbb{K}} \subseteq \mathbb{L} \subseteq \mathbb{K}$ ein Zwischenkörper, so gilt $|\mathbb{L}| = p^d$ mit einem Teiler d von n.*
(ii) *Zu jedem Teiler d von n gibt es genau einen Zwischenkörper $\mathbb{P}_{\mathbb{K}} \subseteq \mathbb{L} \subseteq \mathbb{K}$ mit $|\mathbb{L}| = p^d$.*

Lemma 7.4.7. *Es seien k ein Körper und $p, d, m \in \mathbb{Z}_{\geq 1}$. Mit $n := md$ gilt*

$$p^n - 1 \;=\; (p^d - 1)(p^{(m-1)d} + p^{(m-2)d} + \ldots + p^d + 1).$$

In $k[T]$ gilt mit $a := p^{(m-1)d} + p^{(m-2)d} + \ldots + p^d + 1$ zudem

$$T^{p^n-1} - 1 \;=\; (T^{p^d-1} - 1)(T^{(p^d-1)(a-1)} + T^{(p^d-1)(a-2)} + \ldots + T^{p^d-1} + 1).$$

Beweis. Die Gleichungen verifiziert man direkt durch Ausmultiplizieren. □

Beweis von Satz 7.4.6. Wir zeigen (i). Es sei $\mathbb{P}_{\mathbb{K}} \subseteq \mathbb{L} \subseteq \mathbb{K}$ ein Zwischenkörper. Dann ist $\mathbb{L}$ ein endlicher Körper der Charakteristik p und somit gilt $|\mathbb{L}| = p^d$ mit einem $d \in \mathbb{Z}_{\geq 1}$. Nach der Gradformel gilt

$$n \;=\; [\mathbb{K} : \mathbb{P}_{\mathbb{K}}] \;=\; [\mathbb{K} : \mathbb{L}] \cdot [\mathbb{L} : \mathbb{P}_{\mathbb{K}}] \;=\; [\mathbb{K} : \mathbb{L}] \cdot d.$$

Wir zeigen (ii). Nach Satz 7.4.4 dürfen wir annehmen, dass $\mathbb{K} = \mathbb{F}_{p^n}$ gilt. Wir zeigen, dass zu jedem Teiler d von n ein Zwischenkörper $\mathbb{F}_p \subseteq \mathbb{L} \subseteq \mathbb{F}_{p^n}$ mit $|\mathbb{L}| = p^d$ existiert. Dazu betrachten wir die Polynome

$$f \;=\; T^{p^n} - T \;\in\; \mathbb{F}_p[T], \qquad\qquad g \;=\; T^{p^d} - T \;\in\; \mathbb{F}_p[T].$$

Nach Lemma 7.4.7 gilt $f = gh$ mit einem Polynom $h \in \mathbb{F}_p[T]$. Insbesondere zerfällt mit f auch g über $\mathbb{F}_{p^n}$ in Linearfaktoren. Damit erhalten wir den gewünschten Zwischenkörper:

$$\mathbb{F}_p \;\subseteq\; \mathbb{L} \;:=\; \mathbb{F}_{p^d} \;=\; \{a \in \mathbb{F}_{p^n};\; a^{p^d} = a\} \;\subseteq\; \mathbb{F}_{p^n}.$$

Es sei nun $\mathbb{F}_p \subseteq \mathbb{L}' \subseteq \mathbb{F}_{p^n}$ ein weiterer Zwischenkörper mit $|\mathbb{L}'| = p^d$. Nach Satz 7.4.4 gilt $a^{p^d} = a$ für alle $a \in \mathbb{L}'$. Es folgt $\mathbb{L}' \subseteq \mathbb{F}_{p^d}$ und somit $\mathbb{L}' = \mathbb{F}_{p^d}$. □

Satz 7.4.8. *Es sei $\mathbb{K}$ ein beliebiger Körper. Dann ist jede endliche multiplikative Untergruppe $G \subseteq \mathbb{K}^*$ zyklisch.*

Beweis. Die endliche Gruppe G ist abelsch. Der Hauptsatz für endlich erzeugte abelsche Gruppen 5.5.5 liefert somit

$$G \cong \prod_{p\in\mathbb{Z}_{\geq 2}\text{prim}} G_p, \qquad \text{wobei } G_p = \mathbb{Z}/p^{\nu_1}\mathbb{Z} \times \ldots \times \mathbb{Z}/p^{\nu_{d(p)}}\mathbb{Z}$$

mit ganzen Zahlen $0 \leq \nu_1 \leq \ldots \leq \nu_{d(p)}$. Offensichtlich annulliert $p^{\nu_{d(p)}}$ den Summanden G_p. Multiplikativ geschrieben bedeutet das

$$a^{p^{\nu_{d(p)}}} = 1 \quad \text{für alle } a \in G_p.$$

Folglich ist $G_p \subseteq \mathbb{K}$ in der Nullstellenmenge des Polynoms $T^{p^{\nu_{d(p)}}} - 1 \in \mathbb{K}[T]$ enthalten. Das impliziert $|G_p| \leq p^{\nu_{d(p)}}$. Damit ergibt sich $G_p = \mathbb{Z}/p^{\nu_d(p)}\mathbb{Z}$, und wir erhalten mit dem Chinesischen Restsatz

$$G \quad \cong \quad \prod_{p\in\mathbb{Z}_{\geq 2}\ \text{prim}} \mathbb{Z}/p^{\nu_{d(p)}}\mathbb{Z} \quad \cong \quad \mathbb{Z}\Big/\left(\prod_{p\in\mathbb{Z}_{\geq 2}\ \text{prim}} p^{\nu_{d(p)}}\right)\mathbb{Z}.$$

□

Folgerung 7.4.9. *Es sei $\mathbb{K}$ ein endlicher Körper mit $|\mathbb{K}| = p^n$.*

(i) *Die multiplikative Gruppe $\mathbb{K}^*$ ist zyklisch. Insbesondere gibt es ein $a \in \mathbb{K}$ mit*
$$\mathbb{K} = \{0, 1, a, \ldots, a^{p^n-2}\}.$$

(ii) *Für $a \in \mathbb{K}$ wie in (i) gilt $\mathbb{K} = \mathbb{P}_{\mathbb{K}}(a)$ und das Minimalpolynom $f_a \in \mathbb{P}_{\mathbb{K}}[T]$ besitzt den Grad*
$$\deg(f_a) = [\mathbb{K} : \mathbb{P}_{\mathbb{K}}] = n.$$

Definition 7.4.10. Die *Automorphismengruppe* $\mathrm{Aut}(\mathbb{K})$ eines Körpers $\mathbb{K}$ ist die Menge aller Körperisomorphismen $\mathbb{K} \to \mathbb{K}$ mit der Komposition als Verknüpfung.

Erinnerung 7.4.11. Es seien $\mathbb{K}$ ein endlicher Körper und $p := \mathrm{Char}(\mathbb{K})$. Dann haben wir einen Automorphismus

$$\mathrm{Frob}_{\mathbb{K}} \colon \mathbb{K} \to \mathbb{K}, \qquad a \mapsto a^p.$$

Satz 7.4.12. *Es seien $\mathbb{K}$ ein endlicher Körper und $|\mathbb{K}| = p^n$. Dann hat man einen Isomorphismus von Gruppen*

$$\mathbb{Z}/n\mathbb{Z} \to \mathrm{Aut}(\mathbb{K}), \qquad \overline{m} \mapsto \mathrm{Frob}_{\mathbb{K}}^m.$$

Mit anderen Worten: Die Automorphismengruppe von $\mathbb{K}$ ist zyklisch von der Ordnung n und wird durch den Frobeniushomomorphismus erzeugt.

Lemma 7.4.13. *Es seien $\mathbb{K}$ ein Körper mit Primkörper $\mathbb{P}_{\mathbb{K}} \subseteq \mathbb{K}$ und $\varphi \in \mathrm{Aut}(\mathbb{K})$. Dann gilt $\varphi|_{\mathbb{P}_{\mathbb{K}}} = \mathrm{id}_{\mathbb{P}_{\mathbb{K}}}$.*

Beweis. Nach Konstruktion 6.1.8 besteht $\mathbb{P}_{\mathbb{K}}$ aus den Elementen $m \cdot 1_{\mathbb{K}}/n \cdot 1_{\mathbb{K}}$ mit $m, n \in \mathbb{Z}$, $n \cdot 1_{\mathbb{K}} \neq 0$. Es folgt

$$\varphi(m \cdot 1_{\mathbb{K}}) = \varphi(1_{\mathbb{K}} + \ldots + 1_{\mathbb{K}}) = \varphi(1_{\mathbb{K}}) + \ldots + \varphi(1_{\mathbb{K}}) = 1_{\mathbb{K}} + \ldots + 1_{\mathbb{K}} = m \cdot 1_{\mathbb{K}}.$$

□

Beweis von Satz 7.4.12. Wir wählen ein Element $a \in \mathbb{K}$ wie in Folgerung 7.4.9 (i). Dann lässt sich $\mathbb{K}$ darstellen als

$$\mathbb{K} = \{0, 1, a, a^2, \ldots, a^{p^n-2}\}.$$

Damit erhalten wir, dass der Frobeniushomomorphismus $\mathrm{Frob}_{\mathbb{K}}\colon \mathbb{K} \to \mathbb{K}$ mindestens die Ordnung n besitzt: Es gilt

$$\begin{array}{rcll} \mathrm{Frob}^1_{\mathbb{K}}(a) & = & a^p & \neq\ a, \\ \mathrm{Frob}^2_{\mathbb{K}}(a) & = & a^{p^2} & \neq\ a, \\ & \vdots & & \\ \mathrm{Frob}^{n-1}_{\mathbb{K}}(a) & = & a^{p^{n-1}} & \neq\ a, \\ \mathrm{Frob}^n_{\mathbb{K}}(a) & = & a^{p^n} & =\ a. \end{array}$$

Es ist also nur noch $|\mathrm{Aut}(\mathbb{K})| \leq n$ zu zeigen. Wegen $\mathbb{K} = \{0, 1, a, \ldots, a^{p^n-2}\}$ ist jedes $\varphi \in \mathrm{Aut}(\mathbb{K})$ durch seinen Wert $\varphi(a)$ festgelegt. Für das Minimalpolynom $f_a = \sum b_\nu T^\nu \in k[T]$ haben wir

$$f_a(\varphi(a)) \ = \ \sum b_\nu \varphi(a)^\nu \ = \ \sum \varphi(b_\nu)\varphi(a^\nu) \ = \ \varphi\left(\sum b_\nu a^\nu\right) \ = \ \varphi(f_a(a)) \ = \ 0,$$

wobei wir Lemma 7.4.13 für die zweite Gleichung verwenden. Somit ist $\varphi(a)$ Nullstelle von f_a. Wegen $\deg(f_a) = n$ besitzt f_a höchstens n Nullstellen. Also gibt es höchstens n mögliche Werte $\varphi(a)$. $\square$

Aufgaben zu Abschnitt 7.4.

Aufgabe 7.4.14. Es seien $p \in \mathbb{Z}_{\geq 2}$ eine Primzahl und $n \in \mathbb{Z}_{\geq 1}$. Zeige:

(i) Für jedes irreduzible Polynom $f \in \mathbb{F}_p[T]$ sind die beiden folgenden Aussagen äquivalent:
- f teilt $T^{p^n} - T$ in $\mathbb{F}_p[T]$,
- $\deg(f)$ teilt n in $\mathbb{Z}$.

(ii) Das Polynom $T^{p^n} - T$ ist das Produkt über alle irreduziblen normierten Polynome $f \in \mathbb{F}_p[T]$ mit $\deg(f) \mid n$.

7.5. **Separable Erweiterungen.**

Definition 7.5.1. Es sei $k \subseteq \mathbb{K}$ eine Körpererweiterung.

(i) Ein Element $a \in \mathbb{K}$ heißt *separabel* über k, falls es algebraisch über k ist und sein Minimalpolynom $f_a \in k[T]$ separabel ist.
(ii) Die Körpererweiterung $k \subseteq \mathbb{K}$ heißt *separabel*, falls jedes $a \in \mathbb{K}$ separabel über k ist.

Bemerkung 7.5.2. Ist k ein vollkommener Körper, so ist jede algebraische Erweiterung $k \subseteq \mathbb{K}$ separabel.

Satz 7.5.3 (Satz vom primitiven Element)**.** *Es sei $k \subseteq \mathbb{K}$ eine endlich erzeugte separable Körpererweiterung. Dann existiert ein $a \in \mathbb{K}$ mit $\mathbb{K} = k(a)$.*

Lemma 7.5.4. *Es seien $k \subseteq \mathbb{K}$ eine Körpererweiterung. Besitzen $f, g \in k[T]$ eine gemeinsame Nullstelle in $\mathbb{K}$, so besitzen sie einen nichtkonstanten gemeinsamen Teiler in $k[T]$.*

Beweis. Wir dürfen $f, g \neq 0$ annehmen. Ist $a \in \mathbb{K}$ mit $f(a) = g(a) = 0$ gegeben, so ist das Minimalpolynom $f_a \in k[T]$ ein nicht konstanter gemeinsamer Teiler von f und g. □

Beweis von Satz 7.5.3. Ist k ein endlicher Körper, so ist auch $\mathbb{K}$ endlich, da $k \subseteq \mathbb{K}$ als endlich erzeugte algebraische Erweiterung nach Folgerung 6.2.14 endlichen Grad besitzt. Somit ist die multiplikative Gruppe $\mathbb{K}^*$ zyklisch und für jeden Erzeuger $a \in \mathbb{K}^*$ haben wir $\mathbb{K} = k(a)$; siehe Folgerung 7.4.9 (ii) .

Wir behandeln den Fall, dass k unendlich viele Elemente besitzt. Nach Voraussetzung gilt $\mathbb{K} = k(a_1, \ldots, a_n)$ mit $a_1, \ldots, a_n \in \mathbb{K}$. Wir beweisen die Aussage durch Induktion über n. Für den Fall $n = 1$ ist nichts zu zeigen. Nehmen wir also an, die Behauptung gelte für $n - 1$. Die Induktionsannahme liefert dann

$$\mathbb{K} \;=\; k(a_1, \ldots, a_n) \;=\; k(a_1, \ldots, a_{n-1})(a_n) \;=\; k(a, b),$$

wobei $a \in k(a_1, \ldots, a_{n-1})$ ein Element mit $k(a_1, \ldots, a_{n-1}) = k(a)$ ist und wir $b := a_n$ schreiben. Wir suchen ein $c \in k(a, b)$ mit $k(a, b) = k(c)$. Dazu betrachten wir die Minimalpolynome $f_a, f_b \in k[T]$ von $a, b \in \mathbb{K}$ und einen Zerfällungskörper $\mathbb{K} \subseteq \mathbb{L}$ für das Produkt $f = f_a f_b \in \mathbb{K}[T]$. Dann haben wir in $\mathbb{L}[T]$ die Zerlegungen

$$f_a \;=\; (T - \alpha_1) \cdots (T - \alpha_r), \qquad\qquad f_b \;=\; (T - \beta_1) \cdots (T - \beta_s),$$

wobei wir $\alpha_1 := a$ und $\beta_1 := b$ annehmen dürfen und die α_i sowie die β_j wegen der Separabilität von f_a und f_b jeweils paarweise verschieden sind. Da k unendlich viele Elemente besitzt, finden wir ein $\gamma \in k$ mit

$$\gamma \;\neq\; \frac{a - \alpha_i}{\beta_j - b} \quad \text{für alle } i = 1, \ldots, r,\ j = 2, \ldots, s.$$

Wir zeigen, dass $c := a + \gamma b \in \mathbb{K} = k(a, b)$ die gewünschte Eigenschaft $\mathbb{K} = k(c)$ besitzt. Nach Wahl von γ gilt

$$c \;\neq\; \alpha_i + \gamma \beta_j \quad \text{für alle } i = 2, \ldots, r,\ j = 2, \ldots, s.$$

Weiter betrachten wir das Polynom $f'_a := f_a(c - \gamma T) \in k(c)[T]$. Für die Nullstellen $b = \beta_1, \beta_2, \ldots, \beta_s \in \mathbb{L}$ von f_b gilt

$$f'_a(b) = f_a(c - \gamma b) = f_a(a) = 0, \qquad f'_a(\beta_j) = f_a(c - \gamma \beta_j) \neq 0 \text{ für } j \geq 2.$$

Also ist $T - b$ gemeinsamer Teiler von f'_a und f_b in $\mathbb{L}[T]$. Da $f_b = (T - \beta_1) \cdots (T - \beta_s)$ eine Primfaktorzerlegung in $\mathbb{L}[T]$ ist, sehen wir, dass $T - b$ ein größter gemeinsamer Teiler von f'_a und f_b in $\mathbb{L}[T]$ ist. Wendet man nun Lemma 7.5.4 auf $k(c) \subseteq \mathbb{L}$

und $f'_a, f_b \in k(c)[T]$ an, so ergibt sich $T - b \in k(c)[T]$. Es folgt $b \in k(c)$ und $a = c - \gamma b \in k(c)$. Das impliziert $\mathbb{K} = k(a,b) = k(c)$. □

Definition 7.5.5. Es sei $k \subseteq \mathbb{K}$ eine Körpererweiterung.

(i) Man nennt $a \in \mathbb{K}$ ein *primitives Element* für $k \subseteq \mathbb{K}$ falls $\mathbb{K} = k(a)$ mit einem $a \in \mathbb{K}$ gilt.
(ii) Die Körpererweiterung $k \subseteq \mathbb{K}$ heißt *einfach*, falls sie ein primitives Element besitzt.

Folgerung 7.5.6. *Ist k ein vollkommener Körper, so ist jede endliche Erweiterung $k \subseteq \mathbb{K}$ einfach.*

Folgerung 7.5.7. *Ist k ein Körper mit $\mathrm{Char}(k) = 0$, so ist jede endliche Erweiterung $k \subseteq \mathbb{K}$ einfach.*

Satz 7.5.8. *Es seien $k \subseteq \mathbb{K}$ eine endliche Körpererweiterung und $\mathbb{K} \subseteq \overline{\mathbb{K}}$ ein algebraischer Abschluss. Dann sind folgende Aussagen äquivalent:*

(i) *Es gilt $\mathbb{K} = k(a_1, \ldots, a_n)$ mit separablen Elementen $a_1, \ldots, a_n \in \mathbb{K}$ über k.*
(ii) *Es gibt genau $[\mathbb{K} : k]$ Homomorphismen $\varphi\colon \mathbb{K} \to \overline{\mathbb{K}}$ mit $\varphi|_k = \mathrm{id}_k$.*
(iii) *Die Körpererweiterung $k \subseteq \mathbb{K}$ ist separabel.*

Lemma 7.5.9. *Es seien $k \subseteq \mathbb{K}$ eine Körpererweiterung, $\mathbb{K}$ algebraisch abgeschlossen, $a \in \mathbb{K}$ algebraisch über k und m bezeichne die Anzahl der Nullstellen des Minimalpolynoms $f_a \in k[T]$ in $\mathbb{K}$. Dann besitzt jeder Homomorphismus $\varphi\colon k \to \mathbb{K}$ genau m verschiedene Fortsetzungen $k(a) \to \mathbb{K}$.*

Beweis. Es seien $\Phi\colon k[T] \to \mathbb{K}[T]$ die Fortsetzung von $\varphi\colon k \to \mathbb{K}$ mit $\Phi(T) = T$ und $k' := \varphi(k)$. Dann besitzt das Polynom $\Phi(f_a) \in k'[T]$ genau m Nullstellen $b_1, \ldots, b_m \in \mathbb{K}$; siehe Satz 7.1.11. Lemma 7.1.10 liefert zu jedem b_i genau einen Homomorphismus $\varphi_i\colon k(a) \to k'(b_i)$ mit

$$\varphi_i(a) \;=\; b_i, \qquad \varphi_i|_k \;=\; \varphi.$$

Folglich gibt es mindestens m mögliche Fortsetzungen $k(a) \to \mathbb{K}$ von φ. Ist andererseits $\psi\colon k(a) \to \mathbb{K}$ eine Fortsetzung von φ und bezeichnet $\Psi\colon k(a)[T] \to \mathbb{K}[T]$ die kanonische Fortsetzung auf den Polynomring, so erhalten wir

$$0 \;=\; f_a(a) \;=\; \psi(f_a(a)) \;=\; \Psi(f_a)(\psi(a)) \;=\; \Phi(f_a)(\psi(a)).$$

Das bedeutet $\psi(a) \in \{b_1, \ldots, b_m\}$, d.h., wir haben $\psi(a) = b_i$ für ein i. Wegen der Eindeutigkeit der Fortsetzung $\varphi_i\colon k(a) \to k'(b_i)$ muss $\psi = \varphi_i$ gelten. □

Lemma 7.5.10. *Es seien $k \subseteq \mathbb{K}$ eine Körpererweiterung und $\mathbb{K}$ algebraisch abgeschlossen. Weiter seien $a_1, \ldots, a_n \in \mathbb{K}$ algebraisch über k, und wir betrachten die Erweiterungen*

$$k_0 := k \;\subseteq\; k_1 := k(a_1) \;\subseteq\; k_2 := k(a_1, a_2) \;\subseteq\; \ldots \;\subseteq\; k_n := k(a_1, \ldots a_n) \;\subseteq\; \mathbb{K}$$

Bezeichnet m_i die Anzahl der paarweise verschiedenen Nullstellen des Minimalpolynoms $f_i \in k_{i-1}[T]$ von $a_i \in k_i$ in $\mathbb{K}$, so gibt es genau $m_1 \cdots m_n$ verschiedene Homomorphismen $\varphi\colon k_n \to \mathbb{K}$ mit $\varphi|_k = \mathrm{id}_k$.

Beweis. Wir beweisen die Aussage durch Induktion über n. Der Fall $n = 1$ ist Lemma 7.5.9. Kommen wir zum Induktionsschritt. Nach Induktionsannahme gibt es genau $m_1 \cdots m_{n-1}$ verschiedene Homomorphismen $\psi\colon k_{n-1} \to \mathbb{K}$ mit $\psi|_k = \mathrm{id}_k$. Erneute Anwendung von Lemma 7.5.9 zeigt, dass jedes ψ genau m_n verschiedene Fortsetzungen $k_n \to \mathbb{K}$ erlaubt. Diese ergeben zusammen die $m_1 \cdots m_n$ möglichen Homomorphismen $\varphi\colon k_n \to \mathbb{K}$ mit $\varphi|_k = \mathrm{id}_k$. □

Lemma 7.5.11. *Es seien $k \subseteq \mathbb{K} \subseteq \mathbb{L}$ algebraische Körpererweiterungen. Ist $a \in \mathbb{K}$ separabel über k, so ist a auch separabel über $\mathbb{L}$.*

Beweis. Wir betrachten die Minimalpolynom $f_a \in k[T]$ und $g_a \in \mathbb{L}[T]$ von a über k bzw. $\mathbb{L}$. Dann haben wir

$$f_a \ \in \ \langle g_a \rangle \ \subseteq \ \mathbb{L}[T].$$

Folglich ist $g_a \in \mathbb{L}[T]$ ein Teiler von $f_a \in \mathbb{L}[T]$. Mit Folgerung 7.2.8 erhalten wir ein kommutatives Diagramm

$$\begin{array}{ccc} \overline{k} & \xleftrightarrow{\cong} & \overline{\mathbb{L}} \\ \cup\mathsf{I} & & \cup\mathsf{I} \\ k & \subseteq & \overline{\mathbb{L}} \end{array}$$

Ist nun a separabel über k, so besitzt f_a nur einfache Nullstellen in $\overline{k}$. Somit beistzt auch g_a nur einfache Nullstellen in $\overline{\mathbb{L}}$, d.h., a ist separabel über $\mathbb{L}$. □

Beweis von Satz 7.5.8. Wir beginnen mit einer Vorüberlegung. Da $k \subseteq \mathbb{K}$ endlichem ist, kann man Elemente $a_1, \ldots, a_n \in \mathbb{K}$ mit $\mathbb{K} = k(a_1, \ldots, a_n)$ wählen. Wir betrachten die Schachtelung

$$k_0 := k \ \subseteq \ k_1 := k(a_1) \ \subseteq \ k_2 := k(a_1, a_2) \ \subseteq \ \ \ldots \ \ \subseteq \ k_n := k(a_1, \ldots a_n) = \mathbb{K}.$$

Die Gradformel 6.1.21 besagt

$$[\mathbb{K} : k] \ \ = \ \ [k_1 : k_0] \cdots [k_n : k_{n-1}].$$

Bezeichnet m_i die Anzahl der verschiedenen Nullstellen des Minimalpolynoms f_i von a_i über k_{i-1} in einem algebraischen Abschluss $\overline{\mathbb{K}}$ von $\mathbb{K}$, so gilt

$$m_i \ \leq \ \deg(f_i) \ = \ [k_i : k_{i-1}].$$

Gleichheit $m_i = \deg(f_i)$ ist genau dann gegeben, wenn das Element a_i separabel über k_{i-1} ist. Weiter gibt es nach Lemma 7.5.10 genau $m_1 \cdots m_n$ mögliche Homomorphismen $\varphi\colon \mathbb{K} \to \overline{\mathbb{K}}$ mit $\varphi|_k = \mathrm{id}_k$.

Zu "(i)⇒(ii)". Jedes a_i ist separabel über k, und somit nach Lemma 7.5.11 auch über k_{i-1}. Also ist die Anzahl der möglichen Homomorphismen $\varphi\colon \mathbb{K} \to \overline{\mathbb{K}}$ mit $\varphi|_k = \mathrm{id}_k$ gegeben als

$$m_1 \cdots m_n \ = \ \deg(f_1) \cdots \deg(f_n) \ = \ [k_1 : k_0] \cdots [k_n : k_{n-1}] \ = \ [\mathbb{K} : k].$$

Zur "(ii)⇒(iii)". Nehmen wir an, $k \subseteq \mathbb{K}$ sei nicht separabel. Dann gibt es ein $a \in \mathbb{K}$, das nicht separabel über k ist. Wir dürfen in unserer Vorüberlegung annehmen, dass $a = a_1$ gilt, d.h., wir haben dann $m_1 < \deg(f_1)$. Das führt zu einem Widerspruch, denn für die Anzahl s der Homomorphismen $\varphi\colon \mathbb{K} \to \overline{\mathbb{K}}$ mit $\varphi|_k = \mathrm{id}_k$ erhalten wir

$$s \ = \ m_1 \cdots m_n \ < \ \deg(f_1) \cdots \deg(f_n) \ = \ [k_1 : k_0] \cdots [k_n : k_{n-1}] \ = \ [\mathbb{K} : k].$$

Zu "(iii)⇒(i)". Als endliche und separable Körpererweiterung ist $k \subseteq \mathbb{K}$ insbesondere durch endlich viele separable Elemente erzeugt. □

Folgerung 7.5.12. *Es sei $k \subseteq \mathbb{K}$ eine Körpererweiterung. Sind $a_1, \ldots, a_n \in \mathbb{K}$ separabel über k, so ist $k \subseteq k(a_1, \ldots, a_n)$ eine separable Körpererweiterung.*

Satz 7.5.13. *Es sei $k \subseteq \mathbb{K}$ eine Körpererweiterung. Dann sind folgende Aussagen äquivalent.*

(i) *$k \subseteq \mathbb{K}$ ist endlich, normal und separabel.*
(ii) *$k \subseteq \mathbb{K}$ ist Zerfällungskörper eines separablen Polynoms $f \in k[T]$.*

Beweis. Wir zeigen "(i)⇒(ii)". Als normale Erweiterung von endlichem Grad ist $k \subseteq \mathbb{K}$ nach Satz 7.1.13 Zerfällungskörper eines Polynoms $f \in k[T]$. Wir müssen zeigen, dass f separabel über k ist. Dazu sei $g \in k[T]$ ein irreduzibler Faktor von f. Ist $a \in \mathbb{K}$ eine Nullstelle, so gilt $g = bf_a \in k[T]$ mit dem Minimalpolynom $f_a \in k[T]$ von a und dem Leitkoeffizienten $b \in k^*$ von g. Da $a \in \mathbb{K}$ nach Voraussetzung separabel über k ist, zerfällt f_a und somit auch g über $\mathbb{K}$ in verschiedene Linearfaktoren.

Zu "(ii)⇒(i)". Es gilt $\mathbb{K} = k(a_1, \ldots, a_n)$ mit den Nullstellen $a_1, \ldots, a_n \in \mathbb{K}$ des Polynoms $f \in k[T]$. Nach Folgerung 6.2.14 ist $k \subseteq \mathbb{K}$ endlich, nach Satz 7.1.13 normal und nach Folgerung 7.5.12 separabel. □

Aufgaben zu Abschnitt 7.5.

Aufgabe 7.5.14. Es sei k ein Körper der Charakteristik $p > 0$. Weiter seien $k \subseteq \mathbb{K}$ eine Körpererweiterung und $a \in \mathbb{K}$. Beweise die Äquivalenz folgender Aussagen:

(i) Das Element $a \in \mathbb{K}$ ist separabel über k.
(ii) Es gilt $k(a) = k(a^p)$.

Aufgabe 7.5.15. Beweise die Implikation "(i)⇒(ii)" von Satz 7.5.8 unter Verwendung von Satz 7.5.3.

Aufgabe 7.5.16. Bestimme ein primitives Element für den Zerfällungskörper $\mathbb{Q} \subseteq \mathbb{L}$ des Polynoms $T^3 - 2 \in \mathbb{Q}[T]$. *Hinweis*: Beachte $\mathbb{L} = \mathbb{Q}(\sqrt[3]{2}, e^{\frac{2\pi i}{3}})$ und gehe wie im Beweis von Satz 7.5.3 vor.

Aufgabe 7.5.17. Es seien $k \subseteq \mathbb{K}$ eine Körpererweiterung und $k \subseteq \mathbb{L} \subseteq \mathbb{K}$ ein Zwischenkörper. Beweise die Äquivalenz folgender Aussagen:

(i) Die Erweiterung $k \subseteq \mathbb{K}$ ist separabel.
(ii) Die Erweiterungen $k \subseteq \mathbb{L}$ und $\mathbb{L} \subseteq \mathbb{K}$ sind separabel.

8. Galoistheorie

8.1. Galoisgruppen und Fixkörper.

Konstruktion 8.1.1. Die *Galoisgruppe* einer Körperweiterung $k \subseteq \mathbb{K}$ ist die Untergruppe

$$\mathrm{Aut}(\mathbb{K}, k) \;:=\; \{\varphi \in \mathrm{Aut}(\mathbb{K});\; \varphi|_k = \mathrm{id}_k\} \;\leq\; \mathrm{Aut}(\mathbb{K}).$$

Jede Untergruppe $G \subseteq \mathrm{Aut}(\mathbb{K}, k)$ definiert einen Zwischenkörper in $k \subseteq \mathbb{K}$, den zu G gehörigen *Fixkörper*:

$$k \;\subseteq\; \mathbb{K}^G := \{a \in \mathbb{K};\; \varphi(a) = a \text{ für alle } \varphi \in G\} \;\subseteq\; \mathbb{K}.$$

Bemerkung 8.1.2. Für jeden Körper $\mathbb{K}$ hat man die Körpererweiterung $\mathbb{P}_\mathbb{K} \subseteq \mathbb{K}$. Für alle $\varphi \in \mathrm{Aut}(\mathbb{K})$ und $m \in \mathbb{Z}$ haben wir

$$\varphi(m \cdot 1_\mathbb{K}) = \varphi(1_\mathbb{K} + \ldots + 1_\mathbb{K}) = \varphi(1_\mathbb{K}) + \ldots + \varphi(1_\mathbb{K}) = 1_\mathbb{K} + \ldots + 1_\mathbb{K} = m \cdot 1_\mathbb{K}.$$

Nach Konstruktion 6.1.8 enthält $\mathbb{P}_\mathbb{K}$ genau die Elemente der Form $m \cdot 1_\mathbb{K}/n \cdot 1_\mathbb{K}$ mit $m, n \in \mathbb{Z}$, $n \cdot 1_\mathbb{K} \neq 0$. Folglich gilt $\varphi(a) = a$ alle $a \in \mathbb{P}_\mathbb{K}$ und wir erhalten

$$\mathrm{Aut}(\mathbb{K}, \mathbb{P}_\mathbb{K}) \;=\; \mathrm{Aut}(\mathbb{K}).$$

Bemerkung 8.1.3. Es sei $\mathbb{K}$ ein endlicher Körper der Charakteristik p. Nach Satz 7.4.12 wird $\mathrm{Aut}(\mathbb{K})$ erzeugt durch den Frobeniushomomorphismus

$$\mathrm{Frob}_\mathbb{K} \colon \mathbb{K} \;\to\; \mathbb{K}, \qquad a \;\mapsto\; a^p.$$

Es gilt genau dann $\mathrm{Frob}_\mathbb{K}(a) = a$, wenn a Nullstelle des Polynoms $T^p - T \in \mathbb{P}_\mathbb{K}[T]$ ist. Somit fixiert $\mathrm{Frob}_\mathbb{K}$ genau die Elemente von $\mathbb{P}_\mathbb{K}$. Wir schließen

$$\mathbb{K}^{\mathrm{Aut}(\mathbb{K}, \mathbb{P}_\mathbb{K})} \;=\; \mathbb{P}_\mathbb{K}.$$

Beispiel 8.1.4. Für die Körpererweiterung $\mathbb{Q} \subseteq \mathbb{R}$ gilt $\mathrm{Aut}(\mathbb{R}, \mathbb{Q}) = \{\mathrm{id}_\mathbb{R}\}$. Insbesondere haben wir

$$\mathbb{R}^{\mathrm{Aut}(\mathbb{R}, \mathbb{Q})} \;=\; \mathbb{R} \;\neq\; \mathbb{Q}.$$

Beispiel 8.1.5. Die Galoisgruppe $\mathrm{Aut}(\mathbb{C}, \mathbb{R})$ wird durch die komplexe Konjugation $\kappa \colon \mathbb{C} \to \mathbb{C}$, $z \mapsto \bar{z}$ erzeugt. Insbesondere erhalten wir

$$\mathrm{Aut}(\mathbb{C}, \mathbb{R}) \;\cong\; \mathbb{Z}/2\mathbb{Z}, \qquad\qquad \mathbb{C}^{\mathrm{Aut}(\mathbb{C}, \mathbb{R})} \;=\; \mathbb{R}.$$

Satz 8.1.6. *Es seien $\mathbb{K}$ ein Körper und $G \subseteq \mathrm{Aut}(\mathbb{K}) = \mathrm{Aut}(\mathbb{K}, \mathbb{P}_\mathbb{K})$ eine endliche Untergruppe. Dann gilt*

$$[\mathbb{K} : \mathbb{K}^G] \;=\; |G|, \qquad\qquad \mathrm{Aut}(\mathbb{K}, \mathbb{K}^G) \;=\; G.$$

Den Beweis dieses Satzes führen wir am Ende des Abschnittes und kümmern uns zunächst um die nötigen Vorarbeiten. Wir folgen dabei [1], siehe auch [3, 6].

Definition 8.1.7. Es seien G ein Gruppe und $\mathbb{K}$ ein Körper. Ein ($\mathbb{K}$-*wertiger*) *Charakter* auf G ist ein Gruppenhomomorphismus $\chi \colon G \to \mathbb{K}^*$.

Satz 8.1.8. *Es seien G eine Gruppe und $\mathbb{K}$ ein Körper. Dann ist die Menge $\mathbb{X}(G)$ aller $\mathbb{K}$-wertigen Charaktere auf G eine linear unabhängige Teilmenge des $\mathbb{K}$-Vektorraumes $\mathrm{Abb}(G, \mathbb{K})$ aller Abbildungen $G \to \mathbb{K}$.*

Beweis. Nehmen wir an, die Menge $\mathbb{X}(G)$ sei linear abhängig. Dann gibt es Linearkombiationen

$$\sum_{i=1}^{r} \alpha_i \chi_i \ = \ 0$$

mit $\alpha_i \in \mathbb{K}^*$ und paarweise verschiedenen $\chi_i \in \mathbb{X}(G)$. Offensichtlich muss dabei stets $r \geq 2$ gelten. Es gibt also ein $g_0 \in G$ mit

$$\chi_1(g_0) \ \neq \ \chi_r(g_0).$$

Wir betrachten nun eine Linearkombination mit minimaler Länge r und schreiben diese in der Form

$$\chi_r + \sum_{i=1}^{r-1} \beta_i \chi_i \ = \ 0.$$

Für beliebiges $g \in G$ können wir einerseits $g_0 g$ einsetzen, andererseits g einsetzen und mit $\chi_r(g_0)$ multiplizieren. Dies führt zu neuen Gleichungen

$$\begin{aligned} \chi_r(g_0)\chi_r(g) + \sum_{i=1}^{r-1} \beta_i \chi_i(g_0)\chi_i(g) &= 0, \\ \chi_r(g_0)\chi_r(g) + \sum_{i=1}^{r-1} \beta_i \chi_r(g_0)\chi_i(g) &= 0. \end{aligned}$$

Subtrahieren der zweiten Gleichung von der ersten liefert eine Identität von Charakteren

$$\sum_{i=1}^{r-1} \beta_i (\chi_i(g_0) - \chi_r(g_0))\chi_i \ = \ 0.$$

Nach Wahl von g_0 ist dies eine nichttriviale Linearkombination. Das steht im Widerspruch zur Wahl von r. □

Folgerung 8.1.9. *Es seien $\mathbb{K}, \mathbb{L}$ Körper und $\varphi_1, \ldots, \varphi_n \colon \mathbb{K} \to \mathbb{L}$ paarweise verschiedene Homorphismen. Dann ist die Familie $(\varphi_1, \ldots, \varphi_n)$ linear unabhängig in* $\mathrm{Abb}(\mathbb{K}, \mathbb{L})$.

Beweis. Es sei $G := \mathbb{K}^*$. Dann sind die Einschränkungen $\varphi_i|_G$ paarweise verschiedene $\mathbb{L}$-wertige Charaktere auf G. Nach Satz 8.1.8 ist $(\varphi_1|_G, \ldots, \varphi_n|_G)$ linear unabhängig in $\mathrm{Abb}(G, \mathbb{L})$. Damit ist auch $(\varphi_1, \ldots, \varphi_n)$ linear unabhängig in $\mathrm{Abb}(\mathbb{K}, \mathbb{L})$. □

Lemma 8.1.10. *Es seien $\mathbb{K}, \mathbb{L}$ Körper und $\varphi_1, \ldots, \varphi_n \colon \mathbb{K} \to \mathbb{L}$ paarweise verschiedene Homorphismen. Dann ist*

$$\mathbb{K}_0 \ := \ \{a \in \mathbb{K};\ \varphi_1(a) = \ldots = \varphi_n(a)\}$$

ein Unterkörper von $\mathbb{K}$. Weiter gilt $[\mathbb{K} : \mathbb{K}_0] \geq n$ für den Grad der Körpererweiterung $\mathbb{K}_0 \subseteq \mathbb{K}$.

Beweis. Offensichtlich ist $\mathbb{K}_0 \subseteq \mathbb{K}$ ein Unterkörper. Wir führen $m := [\mathbb{K} : \mathbb{K}_0] < n$ zum Widerspruch. Dazu sei $(a_1, \ldots, a_m)$ eine $\mathbb{K}_0$-Basis für $\mathbb{K}$. Wir betrachten

$$A \ := \ \begin{bmatrix} \varphi_1(a_1) & \cdots & \varphi_n(a_1) \\ \vdots & & \vdots \\ \varphi_1(a_m) & \cdots & \varphi_n(a_m) \end{bmatrix} \ \in \ \mathrm{Mat}(m, n; \mathbb{L}).$$

Wegen $\mathrm{rg}(A) \leq m < n$ gibt es ein $0 \neq b \in \mathbb{L}^n$ mit $A \cdot b = 0$. Jedes $a \in \mathbb{K}$ besitzt eine Entwicklung $a = \gamma_1 a_1 + \ldots + \gamma_m a_m$ mit $\gamma_j \in \mathbb{K}_0$. Damit erhalten wir

$$\begin{aligned}\sum_{i=1}^{n} b_i \varphi_i(a) &= \sum_{i=1}^{n} b_i \varphi_i \left(\sum_{j=1}^{m} \gamma_j a_j \right) = \sum_{i=1}^{n} b_i \sum_{j=1}^{m} \varphi_i(\gamma_j)\varphi_i(a_j) \\ &= \sum_{i=1}^{n} b_i \sum_{j=1}^{m} \varphi_1(\gamma_j)\varphi_i(a_j) = \sum_{j=1}^{m} \varphi_1(\gamma_j) \sum_{i=1}^{n} b_i \varphi_i(a_j) = 0,\end{aligned}$$

wobei $\varphi_1(\gamma_j) = \varphi_i(\gamma_j)$ wegen $\gamma_j \in \mathbb{K}_0$. Wir schließen $b_1\varphi_1 + \ldots + b_n\varphi_n = 0$. Nach Folgerung 8.1.9 ist $(\varphi_1, \ldots, \varphi_n)$ jedoch linear unabhängig; Widerspruch. □

Definition 8.1.11. Es seien $\mathbb{K}$ ein Körper und $G \leq \mathrm{Aut}(\mathbb{K})$ eine endliche Untergruppe. Die *G-Spur* in $\mathbb{K}$ ist die Abbildung

$$\mathrm{Tr}_G \colon \mathbb{K} \to \mathbb{K}, \qquad a \mapsto \sum_{\varphi \in G} \varphi(a).$$

Lemma 8.1.12. *Es seien $\mathbb{K}$ ein Körper und $G \leq \mathrm{Aut}(\mathbb{K})$ eine endliche Untergruppe. Dann gilt $\{0\} \neq \mathrm{Tr}_G(\mathbb{K}) \subseteq \mathbb{K}^G$.*

Beweis. Nach Folgerung 8.1.9 ist $G \subseteq \mathrm{Abb}(\mathbb{K}, \mathbb{K})$ linear unabhängig. Das impliziert $\mathrm{Tr}_G(\mathbb{K}) \neq \{0\}$. Wir zeigen $\mathrm{Tr}_G(a) \in \mathbb{K}^G$ für alle $a \in \mathbb{K}$. Für jedes $\psi \in G$ haben wir

$$\psi(\mathrm{Tr}_G(a)) = \psi \left(\sum_{\varphi \in G} \varphi(a) \right) = \sum_{\varphi \in G} (\psi \circ \varphi)(a) = \sum_{\varphi \in G} \varphi(a) = \mathrm{Tr}_G(a).$$

□

Beweis von Satz 8.1.6. Wir zeigen $[\mathbb{K} : \mathbb{K}^G] = |G|$. Gemäß Lemma 8.1.10 haben wir $[\mathbb{K} : \mathbb{K}^G] \geq |G|$. Es ist also nur noch $[\mathbb{K} : \mathbb{K}^G] \leq |G|$ nachzuweisen. Es sei $G = \{\varphi_1, \ldots, \varphi_n\}$. Insbesondere haben wir damit $|G| = n$.

Wir müssen zeigen, dass jede Familie $(a_1, \ldots, a_m)$ der Länge $m > n$ in $\mathbb{K}$ linear abhängig über $\mathbb{K}^G$ ist. Wir betrachten die Matrix

$$A := \begin{bmatrix} \varphi_1^{-1}(a_1) & \cdots & \varphi_1^{-1}(a_m) \\ \vdots & & \vdots \\ \varphi_n^{-1}(a_1) & \cdots & \varphi_n^{-1}(a_m) \end{bmatrix} \in \mathrm{Mat}(n, m; \mathbb{K}).$$

Wegen $m > n$ gibt es ein $0 \neq b \in \mathbb{K}^m$ mit $A \cdot b = 0$. Es sei etwa $b_l \neq 0$. Nach Lemma 8.1.12 gibt es ein $c \in \mathbb{K}$ mit $\mathrm{Tr}_G(c) \neq 0$. Wir setzen $b'_j := cb_l^{-1}b_j$. Dann gilt

$$\mathrm{Tr}_G(b'_l) = \mathrm{Tr}_G(c) \neq 0.$$

Für jedes $i = 1, \ldots, n$ haben wir

$$\sum_{j=1}^{m} a_j \varphi_i(b'_j) = \varphi_i(cb_l^{-1})\varphi_i \left(\sum_{j=1}^{m} \varphi_i^{-1}(a_j) b_j \right) = \varphi_i(cb_l^{-1})\varphi_i((A \cdot b)_i) = 0.$$

Aufsummieren dieser Gleichungen ergibt wegen $\mathrm{Tr}_G(b'_l) \neq 0$ eine nichttriviale Linearkombination

$$0 = \sum_{i=1}^{n} \sum_{j=1}^{m} a_j \varphi_i(b'_j) = \sum_{j=1}^{m} a_j \sum_{i=1}^{n} \varphi_i(b'_j) = \sum_{j=1}^{m} \mathrm{Tr}_G(b'_j) a_j.$$

Nach Lemma 8.1.12 gilt dabei $\mathrm{Tr}_G(b'_j) \in \mathbb{K}^G$ für $j = 1, \ldots, m$. Somit ist die Familie $(a_1, \ldots, a_m)$ linear abhängig über $\mathbb{K}^G$.

Wir zeigen $\mathrm{Aut}(\mathbb{K}, \mathbb{K}^G) = G$. Offenbar gilt $G \subseteq \mathrm{Aut}(\mathbb{K}, \mathbb{K}^G)$ und, wie gerade gezeigt, $[\mathbb{K} : \mathbb{K}^G] = |G|$. Nehmen wir an, es existiere ein $\varphi \in \mathrm{Aut}(\mathbb{K}, \mathbb{K}^G) \setminus G$. Dann gilt

$$\begin{aligned} \mathbb{K}^G &= \{a \in \mathbb{K};\ a = \varphi_2(a) = \ldots = \varphi_n(a)\} \\ &= \{a \in \mathbb{K};\ a = \varphi_2(a) = \ldots = \varphi_n(a) = \varphi(a)\}, \end{aligned}$$

wobei $\varphi_1 = \mathrm{id}_{\mathbb{K}}, \varphi_2, \ldots, \varphi_n$ die Elemente von G bezeichnen. Mit Lemma 8.1.10 erhalten wir $[\mathbb{K} : \mathbb{K}^G] \geq n + 1 > |G|$; Widerspruch. □

Aufgaben zu Abschnitt 8.1.

Aufgabe 8.1.13. Zeige $\mathrm{Aut}(\mathbb{R},\mathbb{Q}) = \{\mathrm{id}_{\mathbb{R}}\}$. *Hinweise*: Jeder Körperautomorphismus $\varphi\colon \mathbb{R} \to \mathbb{R}$ ist monoton, denn für $a, b \in \mathbb{R}$ mit $a \leq b$ hat man

$$\varphi(b) - \varphi(a) \;=\; \varphi(\sqrt{b-a})^2 \;\geq\; 0.$$

Ist nun $x \in \mathbb{R}$ gegeben, so findet man eine streng monotone wachsende bzw. fallende rationale Folgen (p_n) bzw. (q_n), jeweils mit Grenzwert x.

Aufgabe 8.1.14. Beweise die Aussagen aus Beispiel 8.1.5: Die Galoisgruppe $\mathrm{Aut}(\mathbb{C},\mathbb{R})$ wird erzeugt durch die komplexe Konjugation. Insbesondere gilt $\mathrm{Aut}(\mathbb{C},\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z}$. *Hinweis*: Jeder Automorphismus $\varphi \in \mathrm{Aut}(\mathbb{C},\mathbb{R})$ ist auch eine $\mathbb{R}$-lineare Abbildung.

Aufgabe 8.1.15. Es seien G eine Gruppe und $\mathbb{K}$ ein Körper. Zeige:

(i) Die Menge $\mathbb{X}_{\mathbb{K}}(G)$ der Charaktere $G \to \mathbb{K}^*$ ist eine abelsche Gruppe bezüglich punktweiser Multiplikation.
(ii) Es gilt stets $\mathbb{X}_{\mathbb{K}}(G) \cong \mathbb{X}_{\mathbb{K}}(G/[G,G])$.
(iii) Für $n \in \mathbb{Z}_{\geq 2}$ bestimme:

$$\mathbb{X}_{\mathbb{C}}(\mathbb{Z}/n\mathbb{Z}), \qquad \mathbb{X}_{\mathbb{C}}(A_n), \qquad \mathbb{X}_{\mathbb{C}}(S_n).$$

8.2. **Hauptsatz der Galoistheorie.**

Definition 8.2.1. Eine Körpererweiterung $k \subseteq \mathbb{K}$ heißt *Galoiserweiterung* oder *galoissch*, wenn es eine endliche Untergruppe $G \subseteq \mathrm{Aut}(\mathbb{K})$ mit $k = \mathbb{K}^G$ gibt.

Theorem 8.2.2. *Es sei $k \subseteq \mathbb{K}$ eine Galoiserweiterung. Dann hat man zueinander inverse Bijektionen:*

$$\begin{array}{rcl} \{\textit{Zwischenkörper von } k \subseteq \mathbb{K}\} & \xrightarrow{\mathrm{Gal}} & \{\textit{Untergruppen von } \mathrm{Aut}(\mathbb{K}, k)\} \\ \mathbb{L} & \mapsto & \mathrm{Aut}(\mathbb{K}, \mathbb{L}), \\ \{\textit{Zwischenkörper von } k \subseteq \mathbb{K}\} & \xleftarrow{\mathrm{Fix}} & \{\textit{Untergruppen von } \mathrm{Aut}(\mathbb{K}, k)\} \\ \mathbb{K}^G & \mapsfrom & G. \end{array}$$

Es sei zusätzlich $k \subseteq \mathbb{L} \subseteq \mathbb{K}$ ein Zwischenkörper. Dann sind die Grade der Erweiterungen gegeben durch

$$[\mathbb{K} : \mathbb{L}] \;=\; |\mathrm{Aut}(\mathbb{K}, \mathbb{L})|, \qquad\qquad [\mathbb{L} : k] \;=\; [\mathrm{Aut}(\mathbb{K}, k) : \mathrm{Aut}(\mathbb{K}, \mathbb{L})].$$

Dabei ist $\mathbb{L} \subseteq \mathbb{K}$ stets galoissch. Die Erweiterung $k \subseteq \mathbb{L}$ ist genau dann galoissch, wenn $\mathrm{Aut}(\mathbb{K}, \mathbb{L})$ Normalteiler in $\mathrm{Aut}(\mathbb{K}, k)$ ist. In letzterem Fall gilt

$$\mathrm{Aut}(\mathbb{L}, k) \;\cong\; \mathrm{Aut}(\mathbb{K}, k)/\mathrm{Aut}(\mathbb{K}, \mathbb{L}).$$

Wir unterteilen den Beweis von Theorem 8.2.2 in eigenständige Sätze; vgl. [1, 3, 6]. Die einzelnen Aussagen des Theorems findet man wie folgt:

- Die Identität $\mathrm{Gal} \circ \mathrm{Fix} = \mathrm{id}$ ist Satz 8.2.3 (ii).
- Die Identität $\mathrm{Fix} \circ \mathrm{Gal} = \mathrm{id}$ ist Satz 8.2.4 (ii).
- Folgerung 8.2.5 liefert die Formeln für $[\mathbb{K} : \mathbb{L}]$ und $[\mathbb{L} : k]$.
- Die Aussage $\mathbb{L} \subseteq \mathbb{K}$ galoissch ist Satz 8.2.4 (i).
- Die Charakterisierung von $k \subseteq \mathbb{L}$ galoissch ist Teil von Satz 8.2.7.
- Lemma 8.2.6 liefert $\mathrm{Aut}(\mathbb{L}, k) \cong \mathrm{Aut}(\mathbb{K}, k)/\mathrm{Aut}(\mathbb{K}, \mathbb{L})$.

Satz 8.2.3. *Es sei $k \subseteq \mathbb{K}$ eine Galoiserweiterung.*

(i) *Die Gruppe $\mathrm{Aut}(\mathbb{K}, k)$ ist endlich, und es gilt $\mathbb{K}^{\mathrm{Aut}(\mathbb{K},k)} = k$.*
(ii) *Für jede Untergruppe $H \leq \mathrm{Aut}(\mathbb{K}, k)$ gilt $\mathrm{Aut}(\mathbb{K}, \mathbb{K}^H) = H$.*

Beweis. Zu (i). Nach Definition einer Galois-Erweiterung haben wir $k = \mathbb{K}^G$ mit einer endlichen Untergruppe $G \subseteq \mathrm{Aut}(\mathbb{K})$. Satz 8.1.6 liefert somit

$$\mathrm{Aut}(\mathbb{K}, k) \;=\; \mathrm{Aut}(\mathbb{K}, \mathbb{K}^G) \;=\; G.$$

Insbesondere ist die Galoisgruppe $\mathrm{Aut}(\mathbb{K}, k)$ endlich. Weiter erhalten wir mit obiger Identität:

$$k \;=\; \mathbb{K}^G \;=\; k^{\mathrm{Aut}(\mathbb{K},k)}.$$

Zu (ii). Nach Aussage (i) ist H eine endliche Gruppe. Mit Satz 8.1.6 erhalten wir daher

$$\mathrm{Aut}(\mathbb{K}, \mathbb{K}^H) \;=\; H.$$

□

Satz 8.2.4. *Es seien $k \subseteq \mathbb{K}$ eine Galoiserweiterung und $k \subseteq \mathbb{L} \subseteq \mathbb{K}$ ein Zwischenkörper. Dann gilt:*

(i) *$\mathbb{L} \subseteq \mathbb{K}$ ist eine Galoiserweiterung.*
(ii) *Man hat $\mathbb{K}^{\mathrm{Aut}(\mathbb{K},\mathbb{L})} = \mathbb{L}$.*

Beweis. Wir setzen $G := \mathrm{Aut}(\mathbb{K}, k)$. Nach Satz 8.2.3 ist G eine endliche Gruppe und es gilt $k = \mathbb{K}^G$. Wir betrachten

$$H \ := \ \mathrm{Aut}(\mathbb{K}, \mathbb{L}), \qquad\qquad \mathbb{L}' \ := \ \mathbb{K}^H.$$

Dann ist $H \leq G$ endlich. Es genügt daher, zu zeigen, dass $\mathbb{L} = \mathbb{L}'$ gilt. Die Inklusion $\mathbb{L} \subseteq \mathbb{L}'$ ergibt sich direkt aus der Definition:

$$\mathbb{L} \ \subseteq \ \mathbb{K}^{\mathrm{Aut}(\mathbb{K},\mathbb{L})} \ = \ \mathbb{K}^H \ = \ \mathbb{L}'.$$

Für den Nachweis von $\mathbb{L} \supseteq \mathbb{L}'$ sei $\varphi_1 = \mathrm{id}_{\mathbb{K}}, \varphi_2, \ldots, \varphi_n$ ein Repräsentantensystem des homogenen Raumes G/H. Damit erhalten wir eine disjunkte Vereinigung

$$G \ = \ H \sqcup \varphi_2 H \sqcup \ldots \sqcup \varphi_n H.$$

Wir betrachten die Einschränkungen $\psi_i := \varphi_i|_{\mathbb{L}} \colon \mathbb{L} \to \mathbb{K}$, wobei $i = 1, \ldots, n$. Jedes ψ_i ist ein Monomorphismus, und wir haben

$$\psi_i = \psi_j \ \Rightarrow \ (\varphi_j^{-1} \circ \varphi_i)|_{\mathbb{L}} = \mathrm{id}_{\mathbb{L}} \ \Rightarrow \ \varphi_j^{-1} \circ \varphi_i \in H \ \Rightarrow \ \varphi_i H = \varphi_j H \ \Rightarrow \ i = j.$$

Mit anderen Worten: Die Monomorphismen $\psi_1, \ldots, \psi_n$ sind paarweise verschieden. Weiter behaupten wir

$$k \ = \ \{a \in \mathbb{L};\ \psi_1(a) = \ldots = \psi_n(a)\}.$$

Für $a \in k$ gilt $a \in \mathbb{L}$ und $\psi_i(a) = \varphi_i(a) = a$. Für $a \in \mathbb{L}$ mit $\psi_1(a) = \ldots = \psi_n(a)$ gilt $a \in \mathbb{K}^G = k$, denn jedes $\varphi \in G$ ist von der Form $\varphi = \varphi_i\psi$ mit $\psi \in H$ und somit

$$\varphi(a) \ = \ (\varphi_i \circ \psi)(a) \ = \ \varphi_i(\psi(a)) \ = \ \varphi_i(a) \ = \ \psi_i(a) \ = \ \psi_1(a) \ = \ a.$$

Lemma 8.1.10 angewandt auf $\psi_i \colon \mathbb{L} \to \mathbb{K}$, $i = 1, \ldots, n$ liefert $[\mathbb{L} : k] \geq n$. Mit den Sätzen 6.1.21, 8.2.3 und 8.1.6, sowie 1.2.14 ergibt sich weiter

$$[\mathbb{K} : \mathbb{L}'][\mathbb{L}' : \mathbb{L}][\mathbb{L} : k] \ = \ [\mathbb{K} : k] \ = \ |G| \ = \ [G : H]|H| \ = \ n[\mathbb{K} : \mathbb{L}'].$$

Mit $[\mathbb{L} : k] \geq n$ können wir daraus $[\mathbb{L}' : \mathbb{L}] = 1$ schließen, was wiederum $\mathbb{L} = \mathbb{L}'$ impliziert. □

Folgerung 8.2.5. *Es sei $k \subseteq \mathbb{K}$ eine Galoiserweiterung. Dann gilt für jeden Zwischenkörper $k \subseteq \mathbb{L} \subseteq \mathbb{K}$:*

$$[\mathbb{K} : \mathbb{L}] \ = \ |\mathrm{Aut}(\mathbb{K}, \mathbb{L})|, \qquad [\mathbb{L} : k] \ = \ [\mathrm{Aut}(\mathbb{K}, k) : \mathrm{Aut}(\mathbb{K}, \mathbb{L})].$$

Beweis. Satz 8.2.4 liefert $\mathbb{L} = \mathbb{K}^{\mathrm{Aut}(\mathbb{K},\mathbb{L})}$. Mit Satz 8.1.6 folgt $[\mathbb{K} : \mathbb{L}] = |\mathrm{Aut}(\mathbb{K}, \mathbb{L})|$, Die zweite Gleichung erhält man aus der ersten und der Gradformel 6.1.21:

$$[\mathbb{L} : k] \ = \ \frac{[\mathbb{K} : k]}{[\mathbb{K} : \mathbb{L}]} \ = \ \frac{|\mathrm{Aut}(\mathbb{K}, k)|}{|\mathrm{Aut}(\mathbb{K}, \mathbb{L})|} \ = \ [\mathrm{Aut}(\mathbb{K}, k) : \mathrm{Aut}(\mathbb{K}, \mathbb{L})].$$

□

Lemma 8.2.6. *Es seien $k \subseteq \mathbb{K}$ eine Galoiserweiterung und $k \subseteq \mathbb{L} \subseteq \mathbb{K}$ ein Zwischenkörper mit $\varphi(\mathbb{L}) = \mathbb{L}$ für jedes $\varphi \in \mathrm{Aut}(\mathbb{K}, k)$. Dann ist*

$$\varrho \colon \mathrm{Aut}(\mathbb{K}, k) \ \to \ \mathrm{Aut}(\mathbb{L}, k), \qquad \varphi \ \mapsto \ \varphi|_{\mathbb{L}}$$

ein Epimorphismus, und es gilt $\mathrm{Kern}(\varrho) = \mathrm{Aut}(\mathbb{K}, \mathbb{L})$. *Insbesondere ist* $\mathrm{Aut}(\mathbb{K}, \mathbb{L})$ *ein Normalteiler in* $\mathrm{Aut}(\mathbb{K}, k)$, *und man hat einen Isomorphismus*

$$\mathrm{Aut}(\mathbb{K}, k)/\mathrm{Aut}(\mathbb{K}, \mathbb{L}) \ \to \ \mathrm{Aut}(\mathbb{L}, k), \qquad \varphi\mathrm{Aut}(\mathbb{K}, \mathbb{L}) \ \mapsto \ \varphi|_{\mathbb{L}}.$$

Beweis. Offensichtlich ist die Einschränkung $\varphi \mapsto \varphi|_{\mathbb{L}}$ ein Homomorphismus und es gilt $\mathrm{Kern}(\varphi) = \mathrm{Aut}(\mathbb{K}, \mathbb{L})$. Mit $G := \{\varphi|_{\mathbb{L}};\ \varphi \in \mathrm{Aut}(\mathbb{K}, k)\}$ haben wir

$$k \ = \ \mathbb{K}^{\mathrm{Aut}(\mathbb{K},k)} \ = \ \mathbb{L} \cap \mathbb{K}^{\mathrm{Aut}(\mathbb{K},k)} \ = \ \mathbb{L}^G,$$

wobei Satz 8.2.3 die erste Gleichung garantiert. Die Surjektivität von $\varrho\colon \varphi \mapsto \varphi|_{\mathbb{L}}$ erhalten wir nun mit Satz 8.1.6:

$$\mathrm{Aut}(\mathbb{L}, k) \ = \ \mathrm{Aut}(\mathbb{L}, \mathbb{L}^G) \ = \ G.$$

□

Satz 8.2.7. *Es seien $k \subseteq \mathbb{K}$ eine Galoiserweiterung und $k \subseteq \mathbb{L} \subseteq \mathbb{K}$ ein Zwischenkörper. Dann sind folgende Aussagen äquivalent:*

(i) *$k \subseteq \mathbb{L}$ ist eine Galoiserweiterung.*
(ii) *Für jedes $\varphi \in \mathrm{Aut}(\mathbb{K}, k)$ gilt $\varphi(\mathbb{L}) = \mathbb{L}$.*
(iii) *$\mathrm{Aut}(\mathbb{K}, \mathbb{L})$ ist Normalteiler in $\mathrm{Aut}(\mathbb{K}, k)$.*

Beweis. Zur Implikation "(i)⇒(ii)". Nach Satz 8.2.3 ist $\mathrm{Aut}(\mathbb{L}, k)$ endlich, etwa $\mathrm{Aut}(\mathbb{L}, k) = \{\psi_1 = \mathrm{id}_{\mathbb{L}}, \psi_2, \ldots, \psi_n\}$. Weiter erhalten wir

$$k \ = \ \mathbb{L}^{\mathrm{Aut}(\mathbb{L},k)}, \qquad\qquad [\mathbb{L} : k] \ = \ [\mathbb{L} : \mathbb{L}^{\mathrm{Aut}(\mathbb{L},k)}] \ = \ n,$$

siehe Satz 8.2.3 für die erste Gleichung und Satz 8.1.6 für die letzte. Wir betrachten nun ein beliebiges Element $\varphi \in \mathrm{Aut}(\mathbb{K}, k)$. Offensichtlich gilt

$$k \ = \ \mathbb{L}^{\mathrm{Aut}(\mathbb{L},k)} \ = \ \{a \in \mathbb{L};\ a = \psi_1(a) = \ldots = \psi_n(a) = \varphi|_{\mathbb{L}}(a)\}.$$

Folglich muss $\varphi|_{\mathbb{L}} \in \{\psi_1, \ldots, \psi_n\}$ gelten, denn sonst erhielte man $[\mathbb{L} : k] \geq n + 1$ gemäß Lemma 8.1.10. Das bedeutet $\varphi(\mathbb{L}) = \mathbb{L}$.

Zur Implikation "(ii)⇒(i)". Nach Lemma 8.2.6 ist die Einschränkungsabbildung $\mathrm{Aut}(\mathbb{K}, k) \to \mathrm{Aut}(\mathbb{L}, k)$ surjektiv. Folglich ist $H := \mathrm{Aut}(\mathbb{L}, k)$ eine endliche Gruppe. Wir müssen also nur noch zeigen:

$$k \ = \ \mathbb{L}^H.$$

Die Inklusion "$\subseteq$" ist offensichtlich. Zu "$\supseteq$". Nehmen wir an, es existiere ein $a \in \mathbb{L}^H \setminus k$. Dann gibt es wegen $k = \mathbb{K}^{\mathrm{Aut}(\mathbb{K},k)}$ ein Element $\varphi \in \mathrm{Aut}(\mathbb{K}, k)$ mit $\varphi(a) \neq a$. Für $\psi := \varphi|_{\mathbb{L}}$ gilt nach Voraussetzung $\psi \in \mathrm{Aut}(\mathbb{L}, k) = H$, aber wir haben $\psi(a) \neq a$; Widerspruch zu $a \in \mathbb{L}^H$.

Die Implikation "(ii)⇒(iii)" ergibt sich direkt aus Lemma 8.2.6: Als Kern der Einschränkung $\mathrm{Aut}(\mathbb{K}, k) \to \mathrm{Aut}(\mathbb{L}, k)$ ist $\mathrm{Aut}(\mathbb{K}, \mathbb{L})$ ein Normalteiler in $\mathrm{Aut}(\mathbb{K}, k)$.

Zur Implikation "(iii)⇒(ii)". Ist ein beliebiges Element $\varphi \in \mathrm{Aut}(\mathbb{K}, k)$ gegeben, so ist $k \subseteq \varphi(\mathbb{L}) \subseteq \mathbb{K}$ ein Zwischenkörper und es gilt

$$\mathrm{Aut}(\mathbb{K}, \varphi(\mathbb{L})) \ = \ \varphi \mathrm{Aut}(\mathbb{K}, \mathbb{L}) \varphi^{-1} \ = \ \mathrm{Aut}(\mathbb{K}, \mathbb{L}),$$

wie man direkt nachprüft. Wenden wir nun Satz 8.2.4 auf die Zwischenkörper $\varphi(\mathbb{L})$ und $\mathbb{L}$ an, so ergibt sich

$$\varphi(\mathbb{L}) \ = \ \mathbb{K}^{\mathrm{Aut}(\mathbb{K},\varphi(\mathbb{L}))} \ = \ \mathbb{K}^{\mathrm{Aut}(\mathbb{K},\mathbb{L})} \ = \ \mathbb{L}.$$

□

Aufgaben zu Abschnitt 8.2.

Aufgabe 8.2.8. Es sei $k \subseteq \mathbb{K}$ eine endliche Galoiserweiterung. Beweise folgende Aussagen:

(i) Ist $\mathrm{Aut}(\mathbb{K}, k)$ zyklisch, so gibt es zu jedem Teiler $d \in \mathbb{Z}_{\geq 1}$ von $[\mathbb{K} : k]$ genau einen Zwischenkörper $k \subseteq \mathbb{L} \subseteq \mathbb{K}$ mit $[\mathbb{K} : \mathbb{L}] = d$.

(ii) Sind $p \in \mathbb{Z}_{\geq 2}$ eine Primzahl und $k \in \mathbb{Z}_{\geq 1}$ mit $p^k | [\mathbb{K} : k]$, so gibt es einen Zwischenkörper $k \subseteq \mathbb{L} \subseteq \mathbb{K}$ mit $[\mathbb{K} : \mathbb{L}] = p^k$.

(iii) Gilt $[\mathbb{K} : k] = pq$ mit Primzahlen $p < q$, sodass $p \nmid q - 1$, so ist $\mathrm{Aut}(\mathbb{K}, k)$ zyklisch.

8.3. **Charakterisierung der Galoiserweiterungen.**

Erinnerung 8.3.1. Eine Körpererweiterung $k \subseteq \mathbb{K}$ heißt *normal*, falls sie algebraisch ist und für jedes $a \in \mathbb{K}$ das Minimalpolynom $f_a \in k[T]$ über $\mathbb{K}$ in Linearfaktoren zerfällt.

Erinnerung 8.3.2. Es sei k ein Körper. Ein Polynom $f \in k[T]$ ist *separabel*, wenn es nur irreduzible Faktoren g mit $D(g) \neq 0$ besitzt. Eine Körpererweiterung $k \subseteq \mathbb{K}$ heißt *separabel*, wenn jedes $a \in \mathbb{K}$ separabel über k ist, d.h., das Minimalpolynom $f_a \in k[T]$ separabel ist.

Satz 8.3.3. *Für eine Körpererweiterung $k \subseteq \mathbb{K}$ sind äquivalent:*

(i) *$k \subseteq \mathbb{K}$ ist galoissch.*
(ii) *$k \subseteq \mathbb{K}$ ist endlich, normal und separabel.*
(iii) *$k \subseteq \mathbb{K}$ ist Zerfällungskörper eines separablen Polynoms $f \in k[T]$.*

Folgerung 8.3.4. *Es seien k ein vollkommener Körper und $0 \neq f \in k[T]$. Dann ist der Zerfällungskörper $k \subseteq \mathbb{K}$ von f eine Galoiserweiterung.*

Folgerung 8.3.5. *Für jedes $0 \neq f \in \mathbb{Q}[T]$ ist der Zerfällungskörper $\mathbb{Q} \subseteq \mathbb{K}$ von f eine Galoiserweiterung.*

Satz 8.3.6. *Es seien $k \subseteq \mathbb{K}$ eine Galoisereweiterung und $a \in \mathbb{K}$ Weiter seien $G := \mathrm{Aut}(\mathbb{K}, k)$ und*

$$G{\cdot}a \;=\; \{\varphi(a);\ \varphi \in G\} \;=\; \{a_1, \ldots, a_n\},\ \textit{wobei } a_i \neq a_j \textit{ für } i \neq j.$$

Dann gilt $f := (T - a_1) \cdots (T - a_n) \in k[T]$ und f ist das Minimalpolynom von $a \in \mathbb{K}$ über k.

Beweis. Für jedes $\varphi \in G = \mathrm{Aut}(\mathbb{K}, k)$ ist die Abbildung $G{\cdot}a \to G{\cdot}a$, $a_i \mapsto \varphi(a_i)$ bijektiv. Folglich haben wir für jedes $\varphi \in G$:

$$(T - a_1) \cdots (T - a_n) \;=\; (T - \varphi(a_1)) \cdots (T - \varphi(a_n)).$$

Zu gegebenem $\varphi \in G$ sei $\Phi\colon \mathbb{K}[T] \to \mathbb{K}[T]$ der (eindeutig bestimmte) Homomorphismus mit $\Phi|_{\mathbb{K}} = \varphi$ und $\Phi(T) = T$. Dann gilt

$$\Phi(f) \;=\; \Phi\left((T - a_1) \cdots (T - a_n)\right) \;=\; (T - \varphi(a_1)) \cdots (T - \varphi(a_n)) \;=\; f.$$

Ausmultiplizieren der linken Seite liefert zudem eine Darstellung $f = \sum_{j=0}^{n} b_j T^j$ mit Koeffizienten $b_j \in \mathbb{K}$. Damit erhalten wir

$$\sum_{j=0}^{n} \varphi(b_j) T^j \;=\; \Phi(f) \;=\; f \;=\; \sum_{j=0}^{n} b_j T^j.$$

Wir schließen $\varphi(b_j) = b_j$ für $j = 0, \ldots, n$ und jedes $\varphi \in G$. Es folgt $b_j \in \mathbb{K}^G = k$ für $j = 0, \ldots, n$. Also haben wir $f \in k[T]$.

Wegen $a \in \{a_1, \ldots, a_n\}$ haben wir $f(a) = 0$. Weiter ist f normiert. Um zu sehen, dass f das Minimalpolynom von a ist, müssen wir also nur noch zeigen, dass f irreduzibel in $k[T]$ ist.

Dazu seien $g, h \in k[T]$ mit $f = gh$. Dann gilt $g(a)h(a) = f(a) = 0$, und wir dürfen $g(a) = 0$ annehmen. Wir zeigen, dass $a_1, \ldots, a_n$ Nullstellen von g sind. Es gilt $a_i = \varphi_i(a)$ mit $\varphi_i \in G$. Mit $\varphi_i|_k = \mathrm{id}_k$ ergibt sich

$$g(a_i) \;=\; g(\varphi_i(a)) \;=\; \varphi_i(g(a)) \;=\; \varphi_i(0) \;=\; 0.$$

Da die Elemente $a_1, \ldots, a_n \in \mathbb{K}$ paarweise verschieden sind, muss f ein Teiler von g in $\mathbb{K}[T]$ sein, d.h., es gilt $g = fg'$ mit einem $g' \in \mathbb{K}[T]$. Daraus schließen wir $1 = g'h \in \mathbb{K}[T]$. Das impliziert $\deg(h) = 0$. Folglich muss $h \in k^* = k[T]^*$ gelten. □

Beweis von Satz 8.3.3. Die Äquivalenz von (ii) und (iii) wurde bereits in Satz 7.5.13 nachgewiesen.

Wir zeigen "(i)⇒(ii)". Nach Satz 8.2.3 ist $G := \operatorname{Aut}(\mathbb{K}, k)$ endlich und es gilt $k = \mathbb{K}^G$. Satz 8.1.6 liefert $[\mathbb{K} : k] = |G|$. Folglich ist $k \subseteq \mathbb{K}$ endlich und somit algebraisch. Nach Satz 8.3.6 zerfällt für jedes $a \in \mathbb{K}$ das Minimalpolynom $f_a \in k[T]$ über $\mathbb{K}$ in paarweise verschiedene Linearfaktoren. Somit ist $k \subseteq \mathbb{K}$ normal und separabel.

Wir zeigen "(iii)⇒(i)". Zunächst wählen wir einen algebraischen Abschluss $\mathbb{K} \subseteq \overline{\mathbb{K}}$ und überzeugen uns von der Gleichheit

$$\operatorname{Aut}(\mathbb{K}, k) \quad = \quad \{\varphi\colon \mathbb{K} \to \overline{\mathbb{K}};\ \varphi \text{ Homomorphismus mit } \ \varphi|_k = \mathrm{id}_k\}.$$

Die Inklusion "⊆" ist dabei offensichtlich. Zum Nachweis der Inklusion "⊇" sei $\varphi\colon \mathbb{K} \to \overline{\mathbb{K}}$ mit $\varphi|_k = \mathrm{id}_k$ gegeben. Nach Lemma 7.1.9 (iii) bildet φ die Nullstellenmenge $\{a_1, \ldots, a_n\} \subseteq \mathbb{K}$ von $f \in k[T]$ bijektiv auf sich selbst ab. Damit folgt

$$\varphi(\mathbb{K}) \ = \ \varphi(k(a_1, \ldots, a_n)) \ = \ k(a_1, \ldots, a_n) \ = \ \mathbb{K}.$$

Wir setzen nun $G := \operatorname{Aut}(\mathbb{K}, k)$. Mit obiger Überlegung und Satz 7.5.8 ergibt sich dann

$$|G| \quad = \quad [\mathbb{K} : k].$$

Satz 8.1.6 liefert uns

$$|G| \quad = \quad [\mathbb{K} : \mathbb{K}^G].$$

Es gilt offensichtlich $k \subseteq \mathbb{K}^G$. Wendet man die Gradformel 6.1.21 auf $k \subseteq \mathbb{K}^G \subseteq \mathbb{K}$ an, so ergibt sich $k = \mathbb{K}^G$. Somit ist $k \subseteq \mathbb{K}$ eine Galoiserweiterung. □

Satz 8.3.7. *Es seien $k \subseteq \mathbb{K}$ eine Körpererweiterung und $a_1, \ldots, a_n \in \mathbb{K}$ separabel über k mit $\mathbb{K} = k(a_1, \ldots, a_n)$. Dann gilt:*

(i) *Die Erweiterung $k \subseteq \mathbb{K}$ ist endlich, separabel und einfach.*
(ii) *Es gibt eine Galoiserweiterung $k \subseteq \mathbb{K}'$, die $\mathbb{K}$ als Zwischenkörper enthält.*

Beweis. Nach Satz 6.2.12 ist $k \subseteq \mathbb{K}$ endlich und algebraisch, nach Folgerung 7.5.12 separabel und nach Satz 7.5.3 einfach. Das beweist Aussage (i).

Zu (ii). Es sei $f_i \in k[T]$ das Minimalpolynom von $a_i \in \mathbb{K}$. Dann ist jedes f_i separabel über k und somit auch das Polynom

$$f \ := \ f_1 \cdots f_n \ \in \ k[T].$$

Es sei $\mathbb{K} \subseteq \mathbb{K}'$ ein Zerfällungskörper von f über $\mathbb{K}$. Mit den Nullstellen $a_1, \ldots, a_n$, $b_1, \ldots, b_m$ von f in $\mathbb{K}'$ erhalten wir dann

$$\mathbb{K}' \ = \ \mathbb{K}(b_1, \ldots, b_m) \ = \ k(a_1, \ldots, a_n, b_1, \ldots, b_m).$$

Folglich ist $k \subseteq \mathbb{K}'$ ein Zerfällungskörper für f über k. Wie bereits gesehen, ist f separabel über k. Nach Satz 8.3.3 ist $k \subseteq \mathbb{K}'$ eine Galoiserweiterung. □

Theorem 8.3.8 (Fundamentalsatz der Algebra)**.** *Der Körper $\mathbb{C}$ der komplexen Zahlen ist algebraisch abgeschlossen.*

Lemma 8.3.9. *Es sei $f \in \mathbb{R}[T]$. Ist $\deg(f)$ ungerade, so besitzt f eine Nullstelle in $\mathbb{R}$.*

Beweis. Da $\deg(f)$ ungerade ist, finden wir $a, b \in \mathbb{R}$ mit $a < b$ und $f(a) \leq 0$ sowie $f(b) \geq 0$. Der Zwischenwertsatz liefert eine Nullstelle $x \in [a, b]$. □

Lemma 8.3.10. *Ist $f \in \mathbb{C}[T]$ ein Polynom vom Grad 2, so besitzt f eine Nullstelle in $\mathbb{C}$.*

Beweis. Die Aussage ergibt sich direkt aus der Lösungsformel für quadratische Gleichungen und der Tatsache, dass man zu jeder komplexen Zahl explizit eine Quadratwurzel bilden kann. □

Lemma 8.3.11. *Besitzt ein Körper $\mathbb{K}$ keine echten endlichen Erweiterungen, so ist er algebraisch abgeschlossen.*

Beweis. Es genügt zu zeigen, dass jedes nichtkonstante Polynom $f \in \mathbb{K}[T]$ eine Nullstelle in $\mathbb{K}$ besitzt. Nach Lemma 7.1.8 gibt es eine Erweiterung $\mathbb{K} \subseteq \mathbb{K}'$, sodass f eine Nullstelle $a \in \mathbb{K}'$ besitzt. Die Erweiterung $\mathbb{K} \subseteq \mathbb{K}(a)$ ist dann endlich erzeugt, algebraisch und somit endlich. Folglich gilt $\mathbb{K} = \mathbb{K}(a)$, und wir haben mit a eine Nullstelle von f in $\mathbb{K}$ gefunden. □

Beweis von Theorem 8.3.8. Nach Lemma 8.3.11 genügt es zu zeigen, dass $\mathbb{C}$ keine echten endlichen Erweiterungen erlaubt. Ist $\mathbb{C} \subseteq \mathbb{K}$ endlich, so ist auch $\mathbb{R} \subseteq \mathbb{K}$ endlich und folglich hat man

$$\mathbb{K} \;=\; \mathbb{R}(a_1, \ldots, a_n)$$

mit $a_1, \ldots, a_n \in \mathbb{K}$. Wegen $\mathrm{Char}(\mathbb{R}) = 0$ ist jedes a_i separabel. Nach Satz 8.3.7 haben wir Erweiterungen $\mathbb{R} \subseteq \mathbb{K} \subseteq \mathbb{L}$, wobei $\mathbb{R} \subseteq \mathbb{L}$ galoissch ist. Nach der Gradformel 6.1.21 haben wir

$$[\mathbb{L} : \mathbb{R}] \;=\; [\mathbb{L} : \mathbb{C}] \cdot [\mathbb{C} : \mathbb{R}].$$

Folglich gilt $[\mathbb{L} : \mathbb{R}] = 2m$ mit einer ganzen Zahl $m \in \mathbb{Z}_{\geq 1}$. Der Hauptsatz der Galoistheorie 8.2.2 liefert uns

$$|\mathrm{Aut}(\mathbb{L}, \mathbb{R})| \;=\; [\mathbb{L} : \mathbb{R}] \;=\; 2m.$$

Wir betrachten nun eine 2-Sylowgruppe $S \leq \mathrm{Aut}(\mathbb{L}, \mathbb{R})$. Für den zugehörigen Fixkörper erhalten wir nach Theorem 8.2.2:

$$[\mathbb{L}^S : \mathbb{R}] \;=\; [\mathrm{Aut}(\mathbb{L}, \mathbb{R}) : S].$$

Auf der rechten Seite steht eine ungerade Zahl. Wieder ist $\mathbb{R} \subseteq \mathbb{L}^S$ eine separable Erweiterung. Nach dem Satz vom primitiven Element 7.5.3 gilt daher $\mathbb{L}^S = \mathbb{R}(a)$ mit einem $a \in \mathbb{L}^S$. Für das Minimalpolynom $f_a \in \mathbb{R}[T]$ von a erhalten wir

$$\deg(f_a) \;=\; [\mathbb{L}^S : \mathbb{R}];$$

es handelt sich also um eine ungerade Zahl. Nach Lemma 8.3.9 muss deshalb $\deg(f_a) = 1$ gelten. Das bedeutet $\mathbb{L}^S = \mathbb{R}$, und wir erhalten, dass $\mathrm{Aut}(\mathbb{L}, \mathbb{R}) = S$ eine Gruppe der Ordnung 2^k mit einem $k \in \mathbb{Z}_{\geq 0}$ ist. Somit ist

$$\mathrm{Aut}(\mathbb{L}, \mathbb{C}) \;\leq\; \mathrm{Aut}(\mathbb{L}, \mathbb{R})$$

eine Gruppe der Ordnung 2^l mit einem $l \leq k$. Mit dem Hauptsatz der Galoistheorie haben wir

$$[\mathbb{L} : \mathbb{C}] \;=\; |\mathrm{Aut}(\mathbb{L}, \mathbb{C})| \;=\; 2^l.$$

Wir müssen zeigen, dass $l = 0$ gilt. Wäre l positiv, so hätte man nach Satz 2.3.16 eine Untergruppe $H \leq \mathrm{Aut}(\mathbb{L}, \mathbb{C})$ mit

$$2 \;=\; [\mathrm{Aut}(\mathbb{L}, \mathbb{C}) : H] \;=\; [\mathbb{L}^H : \mathbb{C}].$$

Ist $a \in \mathbb{L}^H \setminus \mathbb{C}$, so gilt $\mathbb{L}^H = \mathbb{C}(a)$, und für das Minimalpolynom $f_a \in \mathbb{C}[T]$ wäre vom Grad 2. Nach Lemma 8.3.10 zerfällt jedoch jedes komplexe Polynom vom Grad 2. Das widerspricht der Irreduzibilität von $f_a \in \mathbb{C}[T]$. □

Aufgaben zu Abschnitt 8.3.

Aufgabe 8.3.12. Betrachte das Polynom $f := (T^2-3)(T^2-5) \in \mathbb{Q}[T]$. Zeige, dass $\mathbb{Q} \subset \mathbb{Q}(\sqrt{3},\sqrt{5})$ ein Zerfällungskörper für f ist. Zeige weiter:

$$\mathrm{Aut}(\mathbb{Q}(\sqrt{3},\sqrt{5}),\mathbb{Q}) \quad \cong \quad \mathbb{Z}/2\mathbb{Z} \ \times \mathbb{Z}/2\mathbb{Z}.$$

Aufgabe 8.3.13. Es seien $k \subseteq \mathbb{L}_i \subseteq \mathbb{K}$ Körpererweiterungen, wobei $i = 1, 2$ und $k \subseteq \mathbb{L}_i$ galoissch seien. Beweise folgende Aussagen:

(i) Die Erweiterung $k \subseteq \mathbb{L}_1\mathbb{L}_2$ ist galoissch.
(ii) Es gilt $[\mathbb{L}_1\mathbb{L}_2 : k] = [\mathbb{L}_1 : k] \cdot [\mathbb{L}_2 : k] \ \Leftrightarrow \ \mathbb{L}_1 \cap \mathbb{L}_2 = k$.

Hinweise: Aussage (i) erhält man mit Satz 8.3.3. Die Implikation "⇒" von (ii) folgt mit Aufgabe 6.2.25 und für "⇐" zeige

$$H_1H_2 \ \leq \ G, \qquad k \ = \ \mathbb{L}_1 \cap \mathbb{L}_2 \ = \ \mathbb{L}_1\mathbb{L}_2^{H_1H_2}$$

für die Galoisgruppen G von $k \subseteq \mathbb{L}_1\mathbb{L}_2$ sowie H_i von $\mathbb{L}_i \subseteq \mathbb{L}_1\mathbb{L}_2$ und schließe daraus $G \cong H_1 \times H_2$.

Aufgabe 8.3.14. Es sei $\mathbb{Q} \subseteq \mathbb{K}$ eine normale Körpererweiterung vom Grad 350. Zeige: Es gibt einen Zwischenkörper $\mathbb{Q} \subseteq \mathbb{L} \subseteq \mathbb{K}$, sodass $\mathbb{Q} \subseteq \mathbb{L}$ eine normale Körpererweiterung vom Grad 14 ist.

8.4. **Beispiele.**

Satz 8.4.1. *Es seien $p \in \mathbb{Z}$ keine Quadratzahl und $\mathbb{L} := \mathbb{Q}(\sqrt{p}) \subseteq \mathbb{C}$. Es gilt $\mathbb{L} = \mathbb{Q} \oplus \mathbb{Q}\sqrt{p}$ und man hat einen Körperautomorphismus*

$$\kappa_p \colon \mathbb{L} \to \mathbb{L}, \qquad a + b\sqrt{p} \ \mapsto a - b\sqrt{q}$$

Dann ist $\mathbb{Q} \subseteq \mathbb{L}$ eine Galoiserweiterung und die zugehörige Galoisgruppe ist gegeben als $\mathrm{Aut}(\mathbb{L}, \mathbb{Q}) = \langle \kappa_p \rangle \cong \mathbb{Z}/2\mathbb{Z}$.

Beweis. Da p keine Quadratzahl ist, haben wir $\sqrt{p} \notin \mathbb{Q}$. Somit ist $T^2 - p$ das Minimalpolynom von $\sqrt{p}$ über $\mathbb{Q}$ und Satz 6.2.6 liefert $[\mathbb{L} : \mathbb{Q}] = 2$. Dabei ist $(1, \sqrt{p})$ eine $\mathbb{Q}$-Basis für $\mathbb{L}$ und wir erhalten $\kappa_p \in \mathrm{Aut}(\mathbb{L})$, sodass

$$\kappa_p|_{\mathbb{Q}} \ = \ \mathrm{id}_{\mathbb{Q}}, \qquad \kappa_p(\sqrt{p}) \ = \ -\sqrt{p},$$

siehe Lemma 7.1.10 mit $\varphi = \mathrm{id}_{\mathbb{Q}}$, $k = k' = \mathbb{Q}$, $\mathbb{K} = \mathbb{K}' = \mathbb{L}$, $a = \sqrt{p}$, $a' = -\sqrt{p}$ sowie $f = T^2 - p$. Es gilt $\langle \kappa_p \rangle \cong \mathbb{Z}/2\mathbb{Z}$ und $\mathbb{Q}$ ist der Fixkörper von $\langle \kappa_p \rangle$. Insbesondere ist $\mathbb{Q} \subseteq \mathbb{L}$ galoissch mit Galoisgruppe $\langle \kappa_p \rangle$; siehe Satz 8.1.6. □

Bemerkung 8.4.2. Es seien $\mathbb{Q} \subseteq \mathbb{L} \subseteq \mathbb{C}$ Körpererweiterungen. Dann sind folgende Aussagen äquivalent:

(i) Es gilt $[\mathbb{L} : \mathbb{Q}] = 2$.
(ii) Es gilt $\mathbb{L} = \mathbb{Q}(\sqrt{p})$ mit $p \in \mathbb{Z}$ quadratfrei.
(iii) $\mathbb{Q} \subseteq \mathbb{L}$ ist galoissch mit Galoisgruppe $\mathbb{Z}/2\mathbb{Z}$.

Satz 8.4.3. *Es seien $p, q \in \mathbb{Z}$ quadratfrei mit $p \neq q$ und $\mathbb{K} := \mathbb{Q}(\sqrt{p}, \sqrt{q}) \subseteq \mathbb{C}$. Dann hat man einen Isomorphismus von $\mathbb{Q}$-Vektorräumen*

$$\mathbb{K} \ = \ \mathbb{Q} \oplus \mathbb{Q}\sqrt{p} \oplus \mathbb{Q}\sqrt{q} \oplus \mathbb{Q}\sqrt{pq}.$$

Die Konjugationen der quadratischen Zahlkörper $\mathbb{Q}(\sqrt{p})$ und $\mathbb{Q}(\sqrt{q})$ setzen sich fort zu Körperautomorphismen

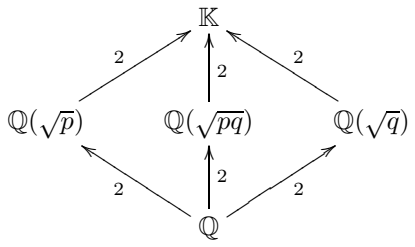
$$\kappa_p \colon \mathbb{K} \to \mathbb{K}, \qquad a + b\sqrt{p} + c\sqrt{q} + d\sqrt{pq} \ \mapsto a - b\sqrt{p} + c\sqrt{q} - d\sqrt{pq},$$

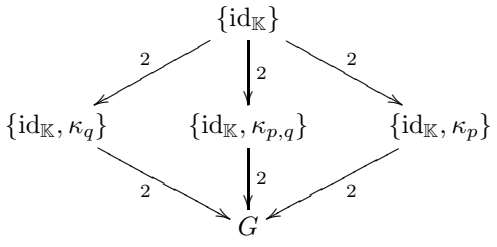
$$\kappa_q \colon \mathbb{K} \to \mathbb{K}, \qquad a + b\sqrt{p} + c\sqrt{q} + d\sqrt{pq} \ \mapsto a + b\sqrt{p} - c\sqrt{q} - d\sqrt{pq},$$

Weiter ist $\mathbb{Q} \subseteq \mathbb{K}$ eine Galoiserweiterung und die Galoisgruppe $G := \mathrm{Aut}(\mathbb{K}, \mathbb{Q})$ ist gegeben durch

$$G \ = \ \langle \kappa_p, \kappa_q \rangle \ \cong \ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Für die Verbände von der Untergruppen von G und der Zwischenkörper von $\mathbb{Q} \subseteq \mathbb{K}$ erhalten wir folgende Darstellungen:





wobei $\kappa_{p,q} := \kappa_p \circ \kappa_q$, die Pfeile für Inklusion stehen und die Zahlen an den Pfeilen den Gruppenindex bzw. den Grad der Körpererweiterung angeben.

Beweis. Wir bestimmen zunächst den Grad der Körpererweiterung $\mathbb{Q} \subseteq \mathbb{K}$ und eine $\mathbb{Q}$-Basis für $\mathbb{K}$. Wir arbeiten mit dem Zwischenkörper wir die Erweiterungen

$$\mathbb{Q} \ \subseteq \ \mathbb{L} \ \subseteq \ \mathbb{K}, \qquad \mathbb{L} := \mathbb{Q}(\sqrt{p}) \ \subseteq \mathbb{C}.$$

Weiter ist $(1, \sqrt{p})$ eine $\mathbb{Q}$-Basis für $\mathbb{L}$. Damit sehen wir $\sqrt{q} \notin \mathbb{L}$: Andernfalls hätte man $a, b \in \mathbb{Q}$ mit $\sqrt{q} = a + b\sqrt{p}$ und somit

$$q = a^2 + 2ab\sqrt{p} + b^2 p \;\Rightarrow\; a = 0 \text{ oder } b = 0,$$

was wegen $\sqrt{p} \notin \mathbb{Q}$ nicht möglich ist. Folglich ist $T^2 - q \in \mathbb{L}[T]$ irreduzibel und somit das Minimalpolynom von $\sqrt{q}$ über $\mathbb{L}$. Zudem haben wir

$$\mathbb{L} \;=\; \mathbb{Q} \oplus \mathbb{Q}\sqrt{p}, \qquad \mathbb{K} \;=\; \mathbb{L} \oplus \mathbb{L}\sqrt{p}.$$

Satz 6.1.21 liefert

$$[\mathbb{K} : \mathbb{Q}] \;=\; [\mathbb{K} : \mathbb{L}] \cdot [\mathbb{L} : \mathbb{Q}] \;=\; 2 \cdot 2 \;=\; 4$$

und dass $(1, \sqrt{p}, \sqrt{q}, \sqrt{pq})$ eine $\mathbb{Q}$-Basis für $\mathbb{K}$ ist. Wir konstruieren die Automorphismen κ_p und κ_q in $\mathrm{Aut}(\mathbb{K}, \mathbb{Q})$. Zunächst wählen wir $\psi \in \mathrm{Aut}(\mathbb{L})$ mit

$$\psi|_{\mathbb{Q}} \;=\; \mathrm{id}_{\mathbb{Q}}, \qquad \psi(\sqrt{p}) \;=\; -\sqrt{p},$$

siehe Satz 8.4.1. Mit Hilfe von Lemma 7.1.10 erhalten wir dann Automorphismen $\kappa_p, \kappa_q \in \mathrm{Aut}(\mathbb{K}) = \mathrm{Aut}(\mathbb{K}, \mathbb{Q})$, sodass

$$\kappa_p|_{\mathbb{L}} = \psi,\ \kappa_p(\sqrt{q}) = \sqrt{q}, \qquad \kappa_q|_{\mathbb{L}} = \mathrm{id}_{\mathbb{L}},\ \kappa_q(\sqrt{q}) = -\sqrt{q}.$$

Dabei sind κ_p, κ_q und $\kappa_{p,q} = \kappa_p \circ \kappa_q$ paarweise verschieden und durch ihre Werte auf $\sqrt{p}$, $\sqrt{q}$ eindeutig bestimmt. Es folgt $\kappa_p^2 = \kappa_q^2 = \mathrm{id}_{\mathbb{K}}$ und somit

$$G \;:=\; \{\mathrm{id}_{\mathbb{K}}, \kappa_p, \kappa_q, \kappa_{p,q}\} \;\leq\; \mathrm{Aut}(\mathbb{K}, \mathbb{Q}), \qquad G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Wir bestimmen den Fixkörper zu G. Jedes Element $z \in \mathbb{K}$ hat eine eindeutige Darstellung $z = a + b\sqrt{p} + c\sqrt{q} + d\sqrt{pq}$ mit $a, b, c, d \in \mathbb{Q}$. Damit erhalten wir

$$\begin{aligned} \mathbb{K}^G &= \{z \in \mathbb{K};\ \kappa_p(z) = \kappa_q(z) = \kappa_{p,q}(z) = z\} \\ &= \{a + b\sqrt{p} + c\sqrt{q} + d\sqrt{pq};\ a \in \mathbb{Q},\ b = c = d = 0\} \\ &= \mathbb{Q}. \end{aligned}$$

Somit ist die Erweiterung $\mathbb{Q} \subseteq \mathbb{K}$ galoissch mit Galoisgruppe G, siehe Satz 8.1.6. Analog zur Bestimmung von $\mathbb{K}^G$ erhalten wir

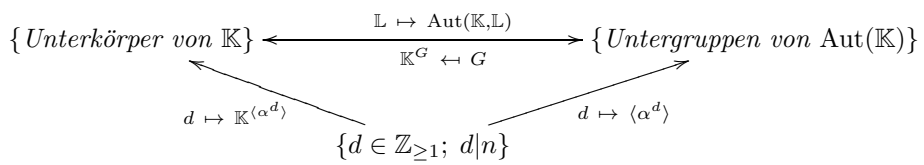
$$\mathbb{K}^H \;=\; \mathbb{Q}(\sqrt{p}),\ \mathbb{Q}(\sqrt{q}),\ \mathbb{Q}(\sqrt{pq}), \qquad H \;=\; \langle\kappa_q\rangle,\ \langle\kappa_p\rangle,\ \langle\kappa_{p,q}\rangle \;\leq\; G.$$

□

Bemerkung 8.4.4. Es seien $\mathbb{Q} \subseteq \mathbb{K} \subseteq \mathbb{C}$ Körpererweiterungen. Dann sind folgende Aussagen äquivalent:

(i) Es gilt $\mathbb{K} = \mathbb{Q}(\sqrt{p}, \sqrt{q})$, wobei $p, q \in \mathbb{Z}$ quadratfrei mit $p \neq q$.
(ii) $\mathbb{Q} \subseteq \mathbb{K}$ ist galoissch mit Galoisgruppe $\mathrm{Aut}(\mathbb{K}, \mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Satz 8.4.5. *Es seien $p \in \mathbb{Z}_{\geq 2}$ eine Primzahl, $n \in \mathbb{Z}_{\geq 1}$ eine natürliche Zahl, $\mathbb{K}$ ein Körper mit p^n Elementen und $\alpha := \mathrm{Frob}_{\mathbb{K}}$. Dann hat man ein kommutatives Diagramm von Bijektionen:*



Für jeden Teiler d von n ist dabei $\mathbb{L}_d := \mathbb{K}^{\langle\alpha^d\rangle}$ ein Körper mit p^d Elementen, die Erweiterung $\mathbb{L}_d \subseteq \mathbb{K}$ ist galoissch und es gilt $\mathrm{Aut}(\mathbb{K} : \mathbb{L}_d) \cong \mathbb{Z}/m\mathbb{Z}$ mit $m := n/d$.

Beweis. Wir betrachten die Körpererweiterung $\mathbb{P}_{\mathbb{K}} \subseteq \mathbb{K}$. Nach Satz 7.4.4 ist $\mathbb{K}$ Zerfällungskörper des separablen Polynoms $\mathbb{T}^{p^n} - T \in \mathbb{P}_{\mathbb{K}}[T]$. Nach Satz 8.3.3 ist daher $\mathbb{P}_{\mathbb{K}} \subseteq \mathbb{K}$ galoissch. Weiter ist die Automorphismengruppe $\mathrm{Aut}(\mathbb{K})$ endlich und wird nach Satz 7.4.12 von $\alpha = \mathrm{Frob}_{\mathbb{K}}$ erzeugt. Die Aussage ist nun eine direkte Folge der Galois-Korrespondenz 8.2.2 und der Tatsache, dass die Untergruppen einer endlichen zyklischen Gruppe den Teilern ihrer Ordnung entsprechen, siehe Satz 2.1.10. □

Aufgaben zu Abschnitt 8.4.

Aufgabe 8.4.6. Es seien $f_1, \ldots, f_r \in \mathbb{Q}[T]$ mit $\deg(f_i) = 2$ für $i = 1, \ldots, r$ und $\mathbb{L} \subseteq \mathbb{C}$ der Zerfällungskörper von $f_1 \cdots f_r$. Zeige: Es gibt quadratfreie Zahlen $b_1, \ldots, b_s \in \mathbb{Z}$, wobei $s \leq r$, mit $\mathbb{L} = \mathbb{Q}(\sqrt{b_1}, \ldots, \sqrt{b_s})$.

Aufgabe 8.4.7. Es seien $\mathbb{Q} \subseteq \mathbb{L} \subseteq \mathbb{C}$ Körpererweiterungen. Beweise Bemerkung 8.4.2, d.h., zeige, dass die folgenden Aussagen äquivalent sind:

(i) Es gilt $[\mathbb{L} : \mathbb{Q}] = 2$.
(ii) Es gilt $\mathbb{L} = \mathbb{Q}(\sqrt{p})$ mit $p \in \mathbb{Z}$ quadratfrei.
(iii) $\mathbb{Q} \subseteq \mathbb{L}$ ist galoissch mit Galoisgruppe $\mathbb{Z}/2\mathbb{Z}$.

Aufgabe 8.4.8. Es seien $\mathbb{Q} \subseteq \mathbb{L} \subseteq \mathbb{C}$ Körpererweiterungen. Beweise Bemerkung 8.4.4, d.h., zeige, dass die folgenden Aussagen äquivalent sind:

(i) Es gilt $\mathbb{K} = \mathbb{Q}(\sqrt{p}, \sqrt{q})$, wobei $p, q \in \mathbb{Z}$ quadratfrei mit $p \neq q$.
(ii) $\mathbb{Q} \subseteq \mathbb{K}$ ist galoissch mit Galoisgruppe $\mathrm{Aut}(\mathbb{K}, \mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Aufgabe 8.4.9. Es seien $\mathbb{K} := \mathbb{Q}(\sqrt{p}, \sqrt{q}) \subseteq \mathbb{C}$, wobei $p, q \in \mathbb{Z}$ quadratfrei mit $p \neq q$ und $x := a + b\sqrt{p} + c\sqrt{q} + d\sqrt{pq}$ mit $a, b, c, d \in \mathbb{Q}$, sodass bc, bd, cd nicht verschwinden. Zeige: Das Minimalpolynom von $x \in \mathbb{K}$ über $\mathbb{Q}$ ist $f_x = T^4 - 4aT^3 + s_2T^2 + s_1T + s_0$ mit

$$\begin{aligned} s_2 &= -2(d^2pq + b^2p + c^2q) + 6a^2, \\ s_1 &= 4a(d^2pq + b^2p + c^2q - a^2) - 8bcdpq, \\ s_0 &= (d^2pq - b^2p - c^2q + a^2)^2 - 4pq(ad - bc)^2. \end{aligned}$$

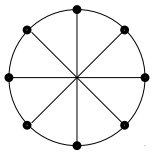
9. Das regelmässige n-Eck

9.1. **Einheitswurzeln.**

Beispiel 9.1.1 (Komplexe Einheitswurzeln)**.** Die Menge der n-ten Einheitswurzeln. im Körper $\mathbb{C}$ der komplexen Zahlen ist gegeben durch

$$E_n(\mathbb{C}) \;:=\; \{\zeta \in \mathbb{C};\ \zeta^n = 1\} \;=\; \{e^{2\pi i k/n};\ k = 0, \ldots, n-1\}.$$

Die n-ten komplexen Einheitswurzeln sind also die Eckpunkte des regelmäßigen n-Ecks. Hier sehen wir den Fall $n = 8$:



Definition 9.1.2. Es seien $n \in \mathbb{Z}_{\geq 1}$ und $\mathbb{K}$ ein Körper, sodass $T^n - 1$ über $\mathbb{K}$ in Linearfaktoren zerfällt. Die Menge der *n-ten Einheitswurzeln in* $\mathbb{K}$ ist

$$E_n(\mathbb{K}) \;:=\; \{\text{Nullstellen von } T^n - 1 \text{ in } \mathbb{K}\} \;=\; \{\zeta \in \mathbb{K};\ \zeta^n = 1\} \;\subseteq\; \mathbb{K}.$$

Ist $k \subseteq \mathbb{K}$ ein Unterkörper, so gilt $T^n - 1 \in k[T]$ und man nennt die Elemente von $E_n(\mathbb{K})$ dann auch die *n-ten Einheitswurzeln über k.*

Beispiel 9.1.3 (Endliche Körper)**.** Es sei $\mathbb{K}$ ein endlicher Körper. Dann haben wir $\mathrm{Char}(\mathbb{K}) = p$ mit einer Primzahl p. Die Theorie endlicher Körper liefert, dass $\mathbb{K}$ isomorph zum Zerfällungskörper $\mathbb{F}_{p^n}$ des Polynoms

$$T^{p^n} - T \;=\; T(T^{p^n-1} - 1) \;\in\; \mathbb{F}_p[T]$$

ist, wobei n eine natürliche Zahl ist, und $\mathbb{F}_p$ wie üblich den Körper $\mathbb{Z}/p\mathbb{Z}$ bezeichnet. Der Körper $\mathbb{F}_{p^n}$ besitzt genau p^n Elemente, und jedes von Null verschiedene Element ist eine $(p^n - 1)$-te Einheitswurzel. Damit erhalten wir

$$E_{p^n-1}(\mathbb{K}) \quad = \quad \mathbb{K}^*.$$

Satz 9.1.4. *Es sei $\mathbb{K}$ ein Körper und $T^n - 1 \in \mathbb{K}[T]$ zerfalle über $\mathbb{K}$ in Linearfaktoren. Dann ist $E_n(\mathbb{K})$ eine zyklische Untergruppe der multiplikativen Gruppe $\mathbb{K}^*$. Es gilt*

$$|E_n(\mathbb{K})| \quad \leq \quad n.$$

Ist die Charakteristik von $\mathbb{K}$ kein Teiler von n, so hat man sogar Gleichheit vorliegen, d.h., es gibt dann genau n verschiedene n-te Einheitswurzeln.

Erinnerung 9.1.5 (Mehrfache Nullstellen)**.** Es seien k ein Körper und $k \subseteq \overline{k}$ ein algebraischer Abschluss. Jedes $f \in k[T] \setminus \{0\}$ besitzt eine eindeutige Darstellung

$$f \;=\; c \prod_{a \in \overline{k}} (T - a)^{\mu_f(a)} \;\in\; \overline{k}[T], \qquad \text{wobei } c \in k^*,\ a \in \overline{k},\ \mu_f(a) \in \mathbb{Z}_{\geq 0}.$$

Für nicht konstante f ist dies ist gerade die Primfaktorzerlegung in $\overline{k}[T]$, und man nennt den Exponenten $\mu_f(a) \in \mathbb{Z}_{\geq 0}$ die *Vielfachheit* von f in a.

Um zu testen, ob ein gegebenes Element $a \in \overline{k}$ mehrfache Nullstelle eines Polynoms $f \in k[T]$ ist verwendet man die *formale Differentiation*:

$$D\colon k[T] \;\to\; k[T], \qquad f = \sum_{\nu=0}^{n} a_\nu T^\nu \;\mapsto\; D(f) := \sum_{\nu=1}^{n} \nu a_\nu T^{\nu-1},$$

wobei man $D(a_0T^0) := 0$ für jedes konstante Polynom $a_0T^0 \in R[T]$ setzt. Für jedes $a \in \overline{k}$ gelten dann folgende Aussagen:

$$\begin{aligned} \mu_f(a) = 1 &\iff f(a) = 0 \text{ und } (D(f))(a) \neq 0 \\ \mu_f(a) > 1 &\iff f(a) = 0 \text{ und } (D(f))(a) = 0 \end{aligned}$$

Beweis von Satz 9.1.4. Es ist offensichtlich, dass die n-ten Einheitswurzeln eine Untergruppe der multiplikativen Gruppe $\mathbb{K}^*$ bilden: Man hat $1 \in E_n(\mathbb{K})$, und für je zwei Elemente $\zeta_1, \zeta_2 \in E_n(\mathbb{K})$ gilt

$$(\zeta_1\zeta_2)^n \;=\; \zeta_1^n\zeta_2^n \;=\; 1, \qquad (\zeta_1^{-1})^n \;=\; \zeta_1^{-n} \;=\; (\zeta_1^n)^{-1} \;=\; 1.$$

Jede n-te Einheitswurzel in $\mathbb{K}$ ist Nullstelle des Polynoms $T^n - 1 \in \mathbb{K}[T]$. Folglich besitzt $E_n(\mathbb{K})$ höchstens $n = \deg(T^n - 1)$ Elemente. Als endliche Untergruppe der multiplikativen Gruppe $\mathbb{K}^*$ ist $E_n(\mathbb{K})$ zyklisch, siehe Satz 7.4.8.

Es sei nun $\mathrm{Char}(\mathbb{K})$ kein Teiler von n. Dann ist die formale Ableitung $D(f) = nT^{n-1}$ von $f := T^n - 1$ ein nicht triviales Polynom, und es gilt $D(f)(\zeta) \neq 0$ für jede n-te Einheitswurzel ζ über $\mathbb{K}$. Somit besizt $T^n - 1$ keine mehrfachen Nullstellen in $\mathbb{K}_n$, und es folgt $|E_n(\mathbb{K})| = n$. □

Bemerkung 9.1.6. Die Voraussetzung, dass n nicht durch die Charakteristik $\mathrm{Char}(\mathbb{K})$ geteilt wird ist wesentlich für $|E_n(\mathbb{K})| = n$. Für $\mathbb{K} = \mathbb{F}_2$ haben wir

$$T^2 - 1 \;=\; (T-1)(T-1)$$

und somit besteht die Menge $E_2(\mathbb{F}_2)$ der 2-ten Einheitswurzeln in $\mathbb{F}_2$ nur aus dem Element 1.

Erinnerung 9.1.7 (Zyklische Gruppen)**.** Ist $G = \langle g \rangle$ eine zyklische Gruppe der Ordnung n, so hat man wohldefinierte Isomorphismen

$$G \;\leftrightarrow\; \mathbb{Z}/n\mathbb{Z}, \qquad g^m \;\mapsto\; \overline{m}, \qquad g^m \;\leftarrow\!\shortmid\; \overline{m}.$$

Für Strukturaussagen über endliche zyklische Gruppen G kann man sich also auf den Fall $G = \mathbb{Z}/n\mathbb{Z}$ beschränken.

Die Untergruppen der Gruppe $\mathbb{Z}/n\mathbb{Z}$ entsprechen den Teilern von n: Man hat zueinander inverse Bijektionen

$$\begin{aligned} \{\text{Teiler von } n\} &\longleftrightarrow \{\text{Untergruppen von } \mathbb{Z}/n\mathbb{Z}\} \\ d &\mapsto \langle \overline{n/d} \rangle \\ |H| &\leftarrow\!\shortmid\; H. \end{aligned}$$

Die Gruppe $\mathbb{Z}/n\mathbb{Z}$ wird durch $\overline{a} \cdot \overline{b} := \overline{ab}$ zu einem K1-Ring. Ist $n = p_1^{\nu_1} \cdots p_r^{\nu_r}$ die Primfaktorzerlegung, so liefert der Chinesische Restsatz einen Isomorphismus von Ringen

$$\mathbb{Z}/n\mathbb{Z} \;\cong\; \mathbb{Z}/p_1^{\nu_1}\mathbb{Z} \;\times\; \ldots \;\times\; \mathbb{Z}/p_r^{\nu_r}\mathbb{Z}.$$

Die multiplikative Gruppe $(\mathbb{Z}/n\mathbb{Z})^*$ der Einheiten des Ringes $\mathbb{Z}/n\mathbb{Z}$ nennt man auch die *Primrestklassengruppe modulo* n. Für jedes $a \in \mathbb{Z}$ gilt

$$\begin{aligned} \overline{a} \in (\mathbb{Z}/n\mathbb{Z})^* &\iff \overline{ab} = \overline{1} \text{ für ein } \overline{b} \in \mathbb{Z}/n\mathbb{Z} \\ &\iff ab = 1 + ln \text{ mit } b, l \in \mathbb{Z} \\ &\iff \mathrm{ggT}(a, n) = 1 \\ &\iff \langle a \rangle = \mathbb{Z}/n\mathbb{Z} \\ &\iff \mathrm{ord}(\overline{a}) = n. \end{aligned}$$

Die oben angebene direkte Produktzerlegung von $\mathbb{Z}/n\mathbb{Z}$ liefert eine Zerlegung der Primrestklassengruppe modulo n:

$$(\mathbb{Z}/n\mathbb{Z})^* \;\cong\; (\mathbb{Z}/p_1^{\nu_1}\mathbb{Z})^* \;\times\; \ldots \;\times\; (\mathbb{Z}/p_r^{\nu_r}\mathbb{Z})^*.$$

Erinnerung 9.1.8. Die *Eulersche ϕ-Funktion* ordnet jeder Zahl $n \in \mathbb{Z}_{\geq 1}$ die Anzahl $\phi(n)$ der zu n teilerfremden ganzen Zahlen m mit $1 \leq m \leq n$ zu:

$$\begin{aligned}\phi(n) &= |\{m \in \mathbb{Z}_{\geq 1};\ m \leq n,\ 1 \in \mathrm{ggT}(m,n)\}| \\ &= |(\mathbb{Z}/n\mathbb{Z})^*|.\end{aligned}$$

Für $n \in \mathbb{Z}_{\geq 2}$ sei $n = p_1^{\nu_1} \cdots p_r^{\nu_r}$ eine Darstellung mit paarweise verschiedenen Primzahlen $p_1, \ldots, p_r$. Dann hat man folgende Identitäten

$$\begin{aligned}\phi(n) &= \phi(p_1^{\nu_1}) \cdots \varphi(p_r^{\nu_r}) \\ &= (p_1^{\nu_1} - p_1^{\nu_1 - 1}) \cdots (p_r^{\nu_r} - p_r^{\nu_r - 1}) \\ &= n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right).\end{aligned}$$

Definition 9.1.9. Eine *primitive n-te Einheitswurzel* ist ein Element $\eta \in E_n(\mathbb{K})$ mit $E_n(\mathbb{K}) = \langle \eta \rangle$. Die Menge aller primitiven n-ten Einheitswurzeln in $\mathbb{K}$ bezeichnen wir mit $PE_n(\mathbb{K})$.

Beispiel 9.1.10. Die Mengen der vierten Einheitswurzeln bzw. der primitiven vierten Einheitswurzeln in $\mathbb{C}$ sind gegeben durch

$$E_4(\mathbb{C}) \;=\; \{1, i, -1, -i\}, \qquad PE_4(\mathbb{C}) \;=\; \{i, -i\}.$$

Satz 9.1.11. *Es seien $\mathbb{K}$ ein Körper und $n \in \mathbb{Z}_{\geq 1}$ mit $\mathrm{Char}(\mathbb{K}) \nmid n$, sodass $T^n - 1$ über $\mathbb{K}$ in Linearfaktoren zerfällt. Dann besitzt $\mathbb{K}$ (mindestens) eine primitive n-te Einheitswurzel η_0. Diese definiert einen Isomorphismus abelscher Gruppen*

$$\mathbb{Z}/n\mathbb{Z} \;\to\; E_n(\mathbb{K}), \qquad \overline{m} \;\mapsto\; \eta_0^m.$$

Für jeden Teiler $1 \leq d \leq n$ von n besitzt $E_n(\mathbb{K})$ genau eine Untergruppe der Ordnung d; mit $m := d/n$ ist diese gegeben als

$$E_d(\mathbb{K}) \;=\; \{1, \eta_0^m, \eta_0^{2m}, \ldots, \eta_0^{(d-1)m}\}.$$

Weiter gibt es genau $\phi(n)$ voneinander verschiedene primitive n-te Einheitswurzeln in $\mathbb{K}$; konkret haben wir

$$PE_n(\mathbb{K}) \;=\; \{\eta \in E_n(\mathbb{K});\ \mathrm{ord}(\eta) = n\} \;=\; \{\eta_0^a;\ 1 \leq a \leq n,\ \mathrm{ggT}(a,n) = 1\}.$$

Beweis. Als zyklische Gruppe wird $E_n(\mathbb{K})$ von einem Element η_0 erzeugt. Dieses ist nach Definition eine primitive n-te Einheitswurzel. Die restlichen Aussagen erhält man aus den entsprechende Eigenschaften zyklischer Gruppen, wobei man von der additiven zur multiplikativen Schreibweise übergehen muss. □

Satz 9.1.12. *Es seien $\mathbb{K}$ ein Körper und $n \in \mathbb{Z}_{\geq 1}$ mit $\mathrm{Char}(\mathbb{K}) \nmid n$, sodass $T^n - 1$ über $\mathbb{K}$ in Linearfaktoren zerfällt. Dann erhält man die Menge $E_n(\mathbb{K})$ der n-ten Einheitswurzeln als disjunkte Vereinigung*

$$E_n(\mathbb{K}) \;=\; \bigsqcup_{d|n} PE_d(\mathbb{K}).$$

Beweis. Für jedes $\eta \in E_n(\mathbb{K})$ ist $\mathrm{ord}(\eta)$ ein Teiler von n. Zu gegebenem Teiler d von n haben wir

$$PE_d(\mathbb{K}) \;\subseteq\; E_d(\mathbb{K}) \;\subseteq\; E_n(\mathbb{K}).$$

Nach Satz 9.1.11 besteht $PE_d(\mathbb{K})$ genau aus den Einheitswurzeln der Ordnung d. Die Behauptung folgt. □

Definition 9.1.13. Es seien $\mathbb{K}$ ein Körper, $n \in \mathbb{Z}_{\geq 1}$ mit $\mathrm{Char}(\mathbb{K}) \nmid n$, sodass $T^n - 1$ über $\mathbb{K}$ in Linearfaktoren zerfällt, $k \subseteq \mathbb{K}$ ein Unterkörper, $\zeta_1, \ldots, \zeta_n \in \mathbb{K}$ die n-ten Einheitswurzeln über k und $k_n := k(\zeta_1, \ldots, \zeta_n) \subseteq \mathbb{K}$. Dann nennt man $k \subseteq k_n$ den *n-ten Kreisteilungskörper* über k.

Satz 9.1.14. *Es seien $\mathbb{K}$ ein Körper, $n \in \mathbb{Z}_{\geq 1}$ mit $\mathrm{Char}(\mathbb{K}) \nmid n$, sodass $T^n - 1$ über $\mathbb{K}$ in Linearfaktoren zerfällt und $k \subseteq \mathbb{K}$ ein Unterkörper.*

(i) *Die Erweiterung $k \subseteq k_n$ ist Zerfällungskörper von $T^n - 1 \in k[T]$,*
(ii) *Für jede primitive n-te Einheitswurzel $\eta \in \mathbb{K}$ haben wir $k_n = k(\eta)$.*
(iii) *Die Erweiterung $k \subseteq k_n$ ist galoissch.*

Beweis. Aussagen (i) und (ii) sind offensichtlich. Da $T^n - 1$ separabel ist, erhalten wir Aussage (iii) mit Satz 8.3.3. □

Satz 9.1.15. *Es seien $\mathbb{K}$ ein Körper, $n \in \mathbb{Z}_{\geq 1}$ mit $\mathrm{Char}(\mathbb{K}) \nmid n$, sodass $T^n - 1$ über $\mathbb{K}$ in Linearfaktoren zerfällt, $k \subseteq \mathbb{K}$ ein Unterkörper und $\eta \in PE_n(\mathbb{K})$.*

(i) *Für jedes $\psi \in \mathrm{Aut}(k_n, k)$ ist $\psi(\eta)$ eine primitive n-te Einheitswurzel und somit von der Gestalt*
$$\psi(\eta) \;=\; \eta^{a_\psi}, \quad a_\psi \in \mathbb{Z}_{\geq 1},\ \mathrm{ggT}(a_\psi, n) = 1.$$
(ii) *Man hat einen wohldefinierten Monomorphismus von $\mathrm{Aut}(k_n, k)$ in die Primrestklassengruppe modulo n:*
$$\mathrm{Aut}(k_n, k) \;\to\; (\mathbb{Z}/n\mathbb{Z})^*, \qquad \psi \;\mapsto\; \bar{a}_\psi$$
(iii) *Die Galoisgruppe $\mathrm{Aut}(k_n, k)$ der Körpererweiterung $k \subseteq k_n$ ist abelsch.*

Beweis. Zu (i). Offensichtlich gilt $\psi(PE_n(\mathbb{K})) = PE_n(\mathbb{K})$. Mit Satz 9.1.11 erhält man dann eine Darstellung $\psi(\eta) = \eta^{a_\psi}$ wie in (i).

Zu (ii). Die Restklasse $\bar{a}_\psi \in \mathbb{Z}/n\mathbb{Z}$ des Elements a_ψ aus (i) ist eindeutig bestimmt, denn wir haben
$$\eta^{a_\psi} = \eta^{a'_\psi} \implies \eta^{a_\psi - a'_\psi} = 1 \implies a_\psi - a'_\psi \in n\mathbb{Z}.$$
Folglich ist die Abbildung aus Aussage (ii) wohldefiniert. Die Homomorphieeigenschaft erhält man mit
$$(\psi \circ \kappa)(\eta) \;=\; \psi(\eta^{a_\kappa}) \;=\; (\eta^{a_\kappa})^{a_\psi} \;=\; \eta^{a_\psi a_\kappa}.$$
Zur Injektivität. Gilt $\bar{a}_\psi = \bar{1} \in \mathbb{Z}/n\mathbb{Z}$, so haben wir $\psi(\eta) = \eta$. Es folgt $\psi(\zeta) = \zeta$ für jede n-te Einheitswurzel ζ und somit $\psi = \mathrm{id}_{k_n}$. □

Aufgaben zu Abschnitt 9.1.

Aufgabe 9.1.16. Es sei $n \in \mathbb{Z}_{\geq 1}$ mit Primfaktorzerlegung $\prod_p p^{\nu(p)}$. Beweise folgende Aussagen über die Primrestklassengruppe: Gilt $8 \nmid n$, so haben wir

$$(\mathbb{Z}/n\mathbb{Z})^* \ \cong \ \prod_p \mathbb{Z}/(p-1)p^{\nu(p)-1}\mathbb{Z}.$$

Gilt $8 \mid n$, so haben wir

$$(\mathbb{Z}/n\mathbb{Z})^* \ \cong \ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{\nu(2)-2}\mathbb{Z} \times \prod_{p \neq 2} \mathbb{Z}/(p-1)p^{\nu(p)-1}\mathbb{Z}.$$

Schließe, dass $(\mathbb{Z}/n\mathbb{Z})^*$ genau dann zyklisch ist, wenn $n = 1, 2, 4$ gilt oder $n = p^r, 2p^r$ mit einer Primzahl $p \neq 2$ und $r > 0$ gilt.

9.2. **Kreisteilungspolynome.**

Definition 9.2.1. Es seien $\mathbb{K}$ ein Körper und $n \in \mathbb{Z}_{\geq 1}$ mit $\mathrm{Char}(\mathbb{K}) \nmid n$, sodass $T^n - 1$ über $\mathbb{K}$ in Linearfaktoren zerfällt. Weiter seien $\eta_1, \ldots, \eta_{\varphi(n)}$ die primitiven n-ten Einheitswurzeln in $\mathbb{K}$. Das *n-te Kreisteilungspolynom* ist

$$\Phi_n \;:=\; (T-\eta_1)\cdots(T-\eta_{\varphi(n)}) \;\in\; \mathbb{K}[T].$$

Satz 9.2.2. *Es seien $\mathbb{K}$ ein Körper und $n \in \mathbb{Z}_{\geq 1}$ mit $\mathrm{Char}(\mathbb{K}) \nmid n$, sodass $T^n - 1$ über $\mathbb{K}$ in Linearfaktoren zerfällt. Das n-te Kreisteilungspolynom $\Phi_n \in \mathbb{K}[T]$ besitzt den Grad $\varphi(n)$, und es gilt*

$$T^n - 1 \;=\; \prod_{1\leq d\leq n,\; d\mid n} \Phi_d.$$

Die Koeffizienten von Φ_n sind von der Gestalt $m\cdot 1_{\mathbb{K}}$ mit $m \in \mathbb{Z}$. Insbesondere gilt $\Phi_n \in \mathbb{P}_{\mathbb{K}}[T]$ mit dem Primkörper $\mathbb{P}_{\mathbb{K}} \subseteq \mathbb{K}$.

Lemma 9.2.3. *Es seien R ein Integritätsring und $f, g \in R[T]$ zwei nichttriviale Polynome. Dann gibt es eine eindeutige Darstellung*

$$b^k f \;=\; qg + r,$$

wobei $b \in R$ der Leitkoeffizient von g ist, $k := \max(0, \deg(f) - \deg(g) + 1)$ gilt und $q, r \in R[T]$ Polynome mit $\deg(r) < \deg(g)$ sind.

Beweis. Es seien $m := \deg(f)$ und $n := \deg(g)$. Wir beweisen zunächst die Existenz der Darstellung durch Induktion über m. Dazu seien

$$f \;=\; aT^m + \sum_{i=0}^{m-1} a_i T^i, \qquad g \;=\; bT^n + \sum_{j=0}^{n-1} b_j T^j.$$

Zum Fall $m = 0$. Gilt $n \geq 1$, so kommt man mit $q := 0$ und $r := f$ durch; gilt $n = 0$, so erfüllen $q := f$ und $r = 0$ den gewünschten Zweck.

Kommen wir zum Induktionsschritt. Im Fall $m < n$ ist $b^k f = 0g + b^k f$ die gewünschte Darstellung. Für den Fall $n \leq m$ betrachten wir das Polynom

$$f' \;:=\; bf - aT^{m-n}g.$$

Es gilt $\deg(f') < m$, und somit können wir die Induktionsvoraussetzung auf f' anwenden. Das liefert eine Darstellung

$$b^{k'}(bf - aT^{m-n}g) \;=\; b^{k'} f' \;=\; q'g + r'$$

mit $\deg(r') < \deg(g)$. Indem man die Gleichungen mit $b^{k-k'-1}$ multipliziert und $b^{k-k'-1}aT^{m-n}g$ auf die rechte Seite bringt, erhält man die gewünschte Darstellung:

$$b^k f \;=\; \left(b^{k-1}aT^{m-n} + b^{k-k'-1}q'\right) g + b^{k-k'-1}r'.$$

Wir kommen nun zur Eindeutigkeit der Darstellung. Dazu vergleichen wir zwei dieser Darstellungen:

$$b^k f \;=\; qg + r \;=\; q'g + r' \;\Longrightarrow\; (q - q')g \;=\; r' - r.$$

Wegen $\deg(r), \deg(r') < \deg(g)$ folgt $q' - q = 0$ und $r' - r = 0$, was die gewünschte Eindeutigkeit beweist. □

Beweis von Satz 9.2.2. Die beiden ersten Aussagen folgen direkt aus der Definition der Kreisteilungspolynome und Satz 9.1.12. Um zu sehen, dass die Koeffizienten von Φ_n von der Gestalt $m\cdot 1_{\mathbb{K}}$ sind, verwenden wir Induktion über n.

Im Fall $n = 1$ haben wir $\Phi_1 = T - 1$ und die Aussage ist trivialerweise richtig. Für den Induktionsschritt betrachten wir den Unterring $\mathbb{Z}_{\mathbb{K}} := \mathbb{Z}\cdot 1_{\mathbb{K}}$ von $\mathbb{K}$.

Nach Induktionsannahme gilt $\Phi_d \in \mathbb{Z}_{\mathbb{K}}[T]$ für alle Teiler $1 \leq d < n$ von n. Lemma 9.2.3 liefert somit eine eindeutige Darstellung

$$T^n - 1 \;=\; q \cdot \prod_{d|n, d<n} \Phi_d \;+\; r$$

mit Polynomen $q, r \in \mathbb{Z}_{\mathbb{K}}[T]$, wobei $\deg(r) < n - \varphi(n)$ gilt. Diese Darstellung ist ebenfalls eindeutig in $\mathbb{K}[T]$. Das impliziert $\Phi_n = q$ und somit $\Phi_n \in \mathbb{Z}_{\mathbb{K}}[T]$. □

Folgerung 9.2.4. *Ist $p \in \mathbb{Z}_{\geq 1}$ eine Primzahl, so gilt für das p-te Kreisteilungspolynom:*

$$\Phi_p \;=\; \frac{T^p - 1}{T - 1} \;=\; T^{p-1} + T^{p-2} + \ldots + T + 1.$$

Folgerung 9.2.5. *Die Kreisteilungspolynome Φ_n lassen sich rekursiv berechnen: Es gilt*

$$\Phi_n \;=\; \frac{T^n - 1}{\prod_{d|n, d<n} \Phi_d}.$$

Folgerung 9.2.6. *Die ersten 6 Kreisteilungspolynome in $\mathbb{Q}[T]$ sind gegeben durch*

$$\begin{aligned}
\Phi_1 &= T - 1, \\
\Phi_2 &= T + 1, \\
\Phi_3 &= T^2 + T + 1, \\
\Phi_4 &= T^2 + 1, \\
\Phi_5 &= T^4 + T^3 + T^2 + T + 1, \\
\Phi_6 &= T^2 - T + 1.
\end{aligned}$$

Bemerkung 9.2.7. Die Koeffezienten der Kreisteilungspolynome $\Phi_n \in \mathbb{Q}[T]$ sind nicht grundsätzlich von der Gestalt $0, \pm 1$, sie können vielmehr beliebig groß werden. Für $n = 105$ tauchen erstmals Koffizienten vom Betrag größer Eins auf.

Bemerkung 9.2.8. Die explizite Kenntnis der Kreisteilungspolynome liefert diverse Identitäten für primitive Einheitswurzeln. Beispielsweise erhält man mit

$$\Phi_3 \;=\; T^2 + T + 1 \;=\; (T - \eta_1)(T - \eta_2)$$

durch Ausmultiplizieren die beiden Identitäten $\eta_1 + \eta_2 = -1$ und $\eta_1 \eta_2 = 1$ für die primitiven dritten Einheitswurzeln $\eta_1 = e^{2\pi i/3}$ und $\eta_2 = e^{4\pi i/3}$ in $\mathbb{C}$.

Satz 9.2.9. *Das n-te Kreisteilungspolynom $\Phi_n \in \mathbb{Q}[T]$ ist irreduzibel.*

Lemma 9.2.10. *Es sei $f \in \mathbb{Z}[T]$ ein irreduzibler Faktor eines Kreisteilungspolynoms $\Phi_n \in \mathbb{Z}[T]$. Ist $\zeta \in \mathbb{K}$ eine Nullstelle von f so ist auch ζ^p für jede Primzahl p mit $p \nmid n$ eine Nullstelle von f.*

Beweis. Da f Teiler von Φ_n ist und Φ_n wiederum Teiler $T^n - 1$ ist, gibt es ein $g \in \mathbb{Z}[T]$ mit

$$T^n - 1 \;=\; fg.$$

Ein Vergleich der Leitkoeffizienten zeigt, dass wir f und g als normierte Polynome in $\mathbb{Z}[T]$ annehmen dürfen. Nehmen wir nun an, dass $f(\zeta^p) \neq 0$ gilt. Wegen

$$(\zeta^p)^n \;=\; \zeta^{np} \;=\; (\zeta^n)^p \;=\; 1^p \;=\; 1$$

ist ζ^p eine Nullstelle von $T^n - 1$, und wir erhalten $g(\zeta^p) = 0$. Also ist ζ Nullstelle des Polynoms $g(T^p) \in \mathbb{Z}[T]$.

Als normiertes irreduzibles Polynom mit $f(\zeta) = 0$ ist f bereits das Minimalpolynom von ζ über $\mathbb{Q}$. Folglich gibt es ein Polynom $h \in \mathbb{Q}[T]$ mit

$$g(T^p) \quad = \quad fh.$$

Division mit Rest in $\mathbb{Z}[T]$ für die Polynome $g(T^p) \in \mathbb{Z}[T]$ und $f \in \mathbb{Z}[T]$ zeigt, dass sogar $h \in \mathbb{Z}[T]$ gelten muss. Wir betrachten nun den kanonischen Homomorphismus

$$\mathbb{Z}[T] \ \to \ \mathbb{Z}/p\mathbb{Z}[T], \qquad q = \sum a_i T^i \ \mapsto \ \overline{q} = \sum \overline{a_i} T^i.$$

Da f normiert ist und positiven Grad besitzt, ist $\overline{f}$ nicht konstant. Es sei nun $g = \sum b_i T^i$. Anwenden des Frobeniushomorphismus $q \mapsto q^p$ im Quotientenkörper von $\mathbb{Z}/p\mathbb{Z}[T]$ liefert

$$\overline{fh} = \overline{g(T^p)} = \sum \overline{b_i} T^{ip} = \sum \overline{b_i}^p T^{ip} = \Big(\sum \overline{b_i} T^i\Big)^p = \overline{g}^p$$

Da $\mathbb{Z}/p\mathbb{Z}[T]$ als euklidischer Ring faktoriell ist, besitzt $\overline{f}$ einen Primfaktor $\overline{f}_0$. Dieser ist nach obiger Identität auch ein Teiler von $\overline{g}$.

Folglich ist $\overline{f}_0^2$ ein Teiler von $T^n - \overline{1} \in \mathbb{Z}/p\mathbb{Z}[T]$. Das bedeutet jedoch, dass $T^n - \overline{1}$ mehrfache Nullstellen in seinem Zerfällungskörper besitzt. Wegen $p \nmid n$ steht das im Widerspruch zu Satz 9.1.4 □

Beweis von Satz 9.2.9. Es genügt zu zeigen, dass Φ_n ein Primelement in dem faktoriellen Ring $\mathbb{Z}[T]$ ist. Dazu sei $f \in \mathbb{Z}[T]$ ein Primfaktor von Φ_n. Dann besitzt f eine Nullstelle $\eta_0 \in \mathbb{C}$. Diese ist auch Nullstelle von Φ_n und somit eine primitive n-te Einheitswurzel.

Jede weitere primitive Einheitswurzel $\eta \in PE_n(\mathbb{C})$ ist von der Gestalt $\eta = \eta_0^m$ mit einer zu n teilerfremden ganzen Zahl. Es sei nun $m = p_1 \cdots p_r$ die Primfaktorzerlegung. Dann gilt $p_i \nmid n$ für $i = 1, \ldots, r$.

Nach Lemma 9.2.10 ist $\eta_1 := \eta_0^{p_1}$ eine Nullstelle von f. Erneute Anwednung von Lemma 9.2.10 zeigt, dass auch $\eta_2 := \eta_1^{p_2}$ Nullstelle von f. So verfährt man weiter und erhält schließlich, dass $\eta_r = \eta$ eine Nullstelle von f ist.

Folglich besitzen f und Φ_n dieselben Nullstellen. Das impliziert $f = \Phi_n$. Insbesondere ist Φ_n prim in $\mathbb{Z}[T]$. □

Folgerung 9.2.11. *Der n-te Kreisteilungskörper $\mathbb{Q} \subseteq \mathbb{Q}_n$ ist eine Galoiserweiterung vom Grad*

$$[\mathbb{Q}_n : \mathbb{Q}] \ = \ \phi(n) \ = \ |\mathrm{Aut}(\mathbb{Q}_n, \mathbb{Q})|.$$

Jede primitive n-te Einheitswurzel $\eta \in \mathbb{C}^*$ besitzt Φ_n als Minimalpolynom und definiert somit $\mathbb{Q}$-Basis für $\mathbb{Q}_n = \mathbb{Q}(\eta)$ durch

$$(1, \eta, \eta^2, \ldots, \eta^{\phi(n)-1}).$$

Weiter definiert $\psi \mapsto \bar{a}_\psi$ aus 9.1.15 (ii) einen Isomorphismus von $\mathrm{Aut}(\mathbb{Q}_n, \mathbb{Q})$ auf die Primrestklassengruppe $(\mathbb{Z}/\mathbb{Z}_n)^*$.

Beweis. Nach Satz 9.1.14 ist $\mathbb{Q} \subseteq \mathbb{Q}_n$ galoissch und $\mathbb{Q}_n = \mathbb{Q}(\eta)$ mit $\eta \in PE_n(\mathbb{C})$. Nach Satz 9.2.9 ist Φ_n das Minimalpolynom von η über $\mathbb{Q}$. Satz 6.2.6 liefert

$$[\mathbb{Q}_n : \mathbb{Q}] \ = \ \deg(\Phi_n) \ = \ \phi(n).$$

Nach Theorem 8.2.2 besitzt $\mathrm{Aut}(\mathbb{Q}_n, \mathbb{Q})$ die Ordnung $\phi(n)$. Folglich ist der Monomorphismus $\mathrm{Aut}(\mathbb{Q}_n, \mathbb{Q}) \to (\mathbb{Z}/\mathbb{Z}_n)^*$ aus Satz 9.1.15 ein Isomorphismus. □

Aufgaben zu Abschnitt 9.2.

Aufgabe 9.2.12. Es seien $m, n \in \mathbb{Z}_{\geq 1}$ teilerfremd und $\eta_m \in PE_m(\mathbb{C})$ sowie $\eta_n \in PE_n(\mathbb{C})$. Beweise folgende Aussagen:

(i) $\mathbb{Q}_{mn} = \mathbb{Q}(\eta_m \eta_n) = \mathbb{Q}(\eta_m, \eta_n)$,
(ii) $[\mathbb{Q}_{mn} : \mathbb{Q}] = [\mathbb{Q}_m : \mathbb{Q}] \cdot [\mathbb{Q}_n : \mathbb{Q}]$,
(iii) $\mathbb{Q}_m \cap \mathbb{Q}_n = \mathbb{Q}$.

Hinweise: Das Kompositum von $\mathbb{Q}_m$ und $\mathbb{Q}_n$ ist gegeben durch $\mathbb{Q}_m \mathbb{Q}_n = \mathbb{Q}_{mn}$. Verwende Aufgabe 6.2.25.

9.3. **Das regelmäßige n-Eck.**

Erinnerung 9.3.1 (Konstruktionen mit Zirkel und Lineal)**.** Wir starten einer Menge $M \subseteq \mathbb{C}$ von Punkten in der Ebene. Unsere Hilfsmittel für die Konstruktion sind:

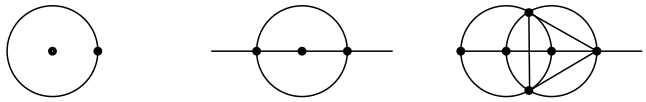
- *Der Zirkel.* Damit können wir einen Radius r abgreifen und einen Kreis mit Radius r um einen gegebenen Punkt schlagen.
- *Das Lineal.* Damit können wir die Verbindungsgerade durch zwei gegebene Punkte ziehen.

Jetzt darf man mit Hilfe von Zirkel und Lineal die Menge M schrittweise vergrößern, indem man

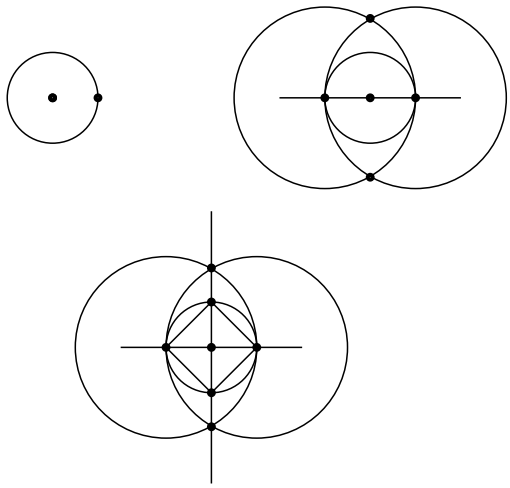
(GG) Schnittpunkte zweier (verschiedener) Verbindungsgeraden hinzunimmt,
(GK) Schnittpunkte von Verbindungsgeraden mit Kreisen hinzunimmt,
(KK) Schnittpunkte zweier (verschiedener) Kreise hinzunimmt.

Wir sagen, dass ein Punkt $z \in \mathbb{C}$ aus M *konstruierbar* ist, wenn man ihn durch die obigen schrittweisen Vergrößerungen aus M gewinnen kann. Die Menge aller aus M konstruierbaren Punkte bezeichnen wir mit $\mathrm{Kon}(M)$.

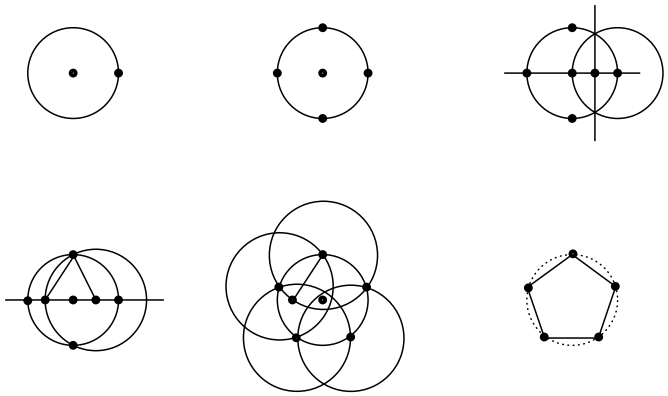
Beispiel 9.3.2 (Euklid)**.** Man kann die dritten Einheitswurzeln aus aus $\{0, 1\}$ konstruieren; sie bilden die Eckpunkte eines gleichschenkligen Dreiecks.



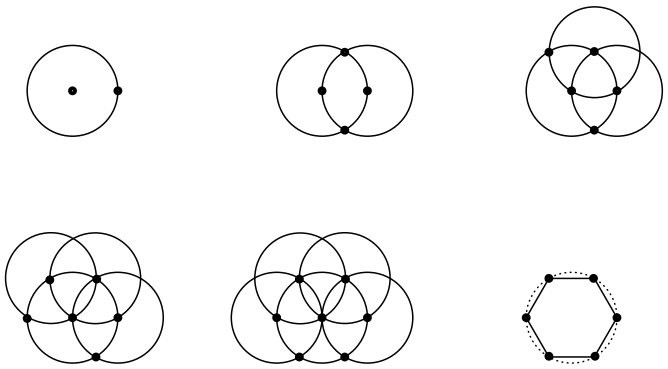
Beispiel 9.3.3 (Euklid)**.** Man kann die vierten Einheitswurzeln aus aus $\{0, 1\}$ konstruieren; sie bilden die Eckpunkte eines Quadrats.



Beispiel 9.3.4 (Euklid)**.** Man kann die fünften Einheitswurzeln aus aus $\{0, 1\}$ konstruieren; sie bilden die Eckpunkte eines regelmäßigen Fünfecks.



Beispiel 9.3.5. Man kann die sechsten Einheitswurzeln aus aus $\{0,1\}$ konstruieren; sie bilden die Eckpunkte eines regelmäßigen Sechsecks.



Erinnerung 9.3.6. [Algebraische Charakterisierung der Konstruierbarkeit] Es sei $M \subseteq \mathbb{C}$ eine Teilmenge mit $0, 1 \in M$, und es sei $z \in \mathbb{C}$. Dann sind äquivalent:

(i) Der Punkt z ist aus M konstruierbar, d.h., es gilt $z \in \mathrm{Kon}(M)$.
(ii) Es gibt Zwischenkörper $\mathbb{Q}(M \cup \overline{M}) = \mathbb{L}_0 \subseteq \mathbb{L}_1 \subseteq \ldots \subseteq \mathbb{L}_n \subseteq \mathbb{C}$ mit

$$z \in \mathbb{L}_n, \qquad [\mathbb{L}_i : \mathbb{L}_{i-1}] = 2 \text{ für } i = 1, \ldots, n.$$

Insbesondere muss für jeden aus $\mathbb{Q}$ konstruierbaren Punkt $z \in \mathbb{C}$ der Grad $[\mathbb{Q}(z) : \mathbb{Q}]$ eine Zweierpotenz sein.

Beispiel 9.3.7. Die Menge $E_9(\mathbb{C})$ der neunten Einheitswurzeln kann nicht aus $\{0,1\}$ konstruiert werden. Dies würde insbesondere implizieren, dass Winkel $\alpha = 20^\circ$ konstruiert werden könnte, was bekanntlich nicht möglich ist.

Definition 9.3.8. Für $n \in \mathbb{Z}_{\geq 1}$ heisst $F_n := 2^{(2^n)} + 1$ die *n-te Fermatsche Zahl.*

Beispiel 9.3.9. Die ersten 5 Fermatschen Zahlen sind prim; sie sind gegeben durch

$$F_0 = 3, \quad F_1 = 5, \quad F_2 = 17, \quad F_3 = 257, \quad F_4 = 65537.$$

Die Fermatsche Zahl $F_5 = 2^{32} + 1$ ist keine Primzahl mehr.

Satz 9.3.10 (Gauß)**.** *Es sei $n \in \mathbb{Z}_{\geq 2}$. Dann sind folgende Aussagen äquivalent.*

(i) *Das regelmäßige n-Eck ist konstruierbar, d.h., $E_n(\mathbb{C})$ ist aus $\{0,1\}$ konstruierbar.*
(ii) *Die Anzahl $\varphi(n)$ der zu n teilerfremden Zahlen $1 \leq m \leq n$ ist eine Potenz von 2.*
(iii) *Es gilt $n = 2^m p_1 \ldots p_r$ mit paarweise verschiedenen Fermatschen Primzahlen $p_1, \ldots, p_r$.*

Lemma 9.3.11. *Es sei $p \in \mathbb{Z}_{\geq 2}$ eine (ungerade) Primzahl. Ist $p-1$ eine Potenz von 2, so ist p eine Fermatsche Primzahl.*

Beweis. Es sei $p = 2^m + 1$. Wir müssen zeigen, dass $m = 2^n$ für ein $n \in \mathbb{Z}_{\geq 1}$ gilt. Andernfalls hätte man $m = ql$ mit einer ungeraden Zahl $q > 1$, und man würde

$$p \;=\; 2^{ql} + 1 \;=\; (2^l + 1)(2^{(q-1)l} - 2^{(q-2)l} + 2^{(q-3)l} - \ldots - 2^l + 1)$$

erhalten. Insbesondere könnte p keine Primzahl sein. Widerspruch zur Voraussetzung. □

Erinnerung 9.3.12. Es sei G eine Gruppe. Eine *Normalreihe in G* ist eine absteigende Kette von Untergruppen

$$G = G_0 \;\trianglerighteq\; G_1 \;\trianglerighteq\; \ldots \;\trianglerighteq\; G_{n-1} \;\trianglerighteq\; G_n = \{e_G\},$$

Der *i-te Faktor* einer solchen Normalreihe ist G_i/G_{i+1}. Die Gruppe G heißt *auflösbar*, wenn sie eine Normalreihe besitzt, deren Faktoren alle abelsch sind.

Ist G eine p-Gruppe, d.h., gilt $|G| = p^m$ mit einer Primzahl p und einer positiven ganzen Zahl m, so ist G auflösbar.

Satz 9.3.13. *Es sei G eine endliche auflösbare Gruppe. Dann gibt es eine Normalreihe*

$$G = G_0 \;\trianglerighteq\; G_1 \;\trianglerighteq\; \ldots \;\trianglerighteq\; G_{n-1} \;\trianglerighteq\; G_n = \{e_G\},$$

in G, sodass jeder Faktor G_i/G_{i+1} eine zyklische Gruppe von Primzahlordnung ist.

Beweis. Da G auflösbar ist, gibt es eine Normalreihe mit abelschen Faktoren in G, diese bezeichnen wir mit

$$G = H_0 \;\trianglerighteq\; H_1 \;\trianglerighteq\; \ldots \;\trianglerighteq\; H_{m-1} \;\trianglerighteq\; H_m = \{e_G\}.$$

Wir wollen diese Normalreihe so wählen, dass die Summe über alle Ordnungen von Faktoren, die nicht Primzahlordnung besitzen,

$$\sum_{|H_i/H_{i+1}| \text{ nicht prim}} |H_i/H_{i+1}|,$$

minimal ist. Wir wollen zeigen, dass diese Summe dann bereits verschwindet, d.h., dass die Normalreihe bereits die gewünschten Eigenschaften besitzt.

Nehmen wir an $|H_i/H_{i+1}|$ sei nicht prim für aufeinanderfolgende Glieder H_i und H_{i+1}. Da H_i/H_{i+1} eine endliche Gruppe ist, findet man ein Element $g \in H_i/H_{i+1}$, sodass $\mathrm{ord}(g)$ eine Primzahl ist. Bezeichnet $\pi\colon H_i \to H_i/H_{i+1}$ die Restklassenabbildung, so erhält man eine Untergruppe

$$H_i' \;:=\; \pi^{-1}(\langle g\rangle) \;\subseteq\; H_i.$$

Diese ist als Urbild eines Normalteilers ein Normalteiler in H_i; hierbei geht ein, dass H_i/H_{i+1} abelsch ist und somit $\langle g\rangle$ als Normalteiler enthält. Weiter ist $H_i'/H_{i+1} \cong \langle g\rangle$ eine zyklische Gruppe von Primzahlordnung. Damit können wir die Normalreihe verfeinern zu

$$G = H_0 \;\trianglerighteq\; H_1 \;\trianglerighteq\; \ldots \;\trianglerighteq\; H_i \;\trianglerighteq\; H_i' \;\trianglerighteq\; H_{i+1} \;\trianglerighteq\; \ldots \;\trianglerighteq\; H_{m-1} \;\trianglerighteq\; H_m = \{e_G\}.$$

Bildet man für diese Normalreihe die Summe aller Ordnungen ihrer Faktoren, die nicht zyklisch von Primzahlordnung sind, so erhält man eine geringeren Wert als für die ursprüngliche Normalreihe; Widerspruch zu deren Wahl. □

Beweis von Satz 9.3.10. Zu "(i) $\Rightarrow$ (ii)". Ist das regelmäßige n-Eck konstruierbar, so ist auch jede primitive n-te Einheitswurzel η konstruierbar. Satz 6.4.3 liefert $[\mathbb{Q}(\eta) : \mathbb{Q}] = 2^m$ mit einem $m \in \mathbb{Z}_{\geq 0}$. Mit Folgerung 9.2.11 erhalten wir also

$$\varphi(n) \;=\; [\mathbb{Q}(\eta) : \mathbb{Q}] \;=\; 2^m.$$

Zur Implikation "(ii) $\Rightarrow$ (i)". Es sei $\eta \in \mathbb{C}$ eine primitive n-te Einheitswurzel. Nach Satz 9.1.14 ist $\mathbb{Q} \subseteq \mathbb{Q}(\eta)$ eine Galoiserweiterung. Für die zugehörige Galoisgruppe $G := \mathrm{Aut}(\mathbb{Q}(\eta), \mathbb{Q})$ gilt nach Folgerung 9.2.11

$$|G| \;=\; [\mathbb{Q}(\eta) : \mathbb{Q}] \;=\; \varphi(n) \;=\; 2^m$$

mit einer ganzen Zahl $m \geq 0$. Folglich ist G eine 2-Gruppe und somit auflösbar. Satz 9.3.13 liefert eine Normalreihe

$$G = G_0 \;\trianglerighteq\; G_1 \;\trianglerighteq\; \ldots \;\trianglerighteq\; G_{n-1} \;\trianglerighteq\; G_n = \{e_G\},$$

in G, sodass jeder Faktor G_i/G_{i+1} eine zyklische Gruppe von Primzahlordnung ist. Da $|G_i/G_{i+1}|$ ein Teiler von $|G| = 2^m$ ist, muss $|G_i/G_{i+1}|P = 2$ gelten.

Nach dem Hauptsatz der Galoistheorie entspricht die obigen Normalreihe für G einer Kette von Zwischenkörpern

$$\mathbb{Q} = \mathbb{L}_0 \;\subseteq\; \mathbb{L}_1 \;\subseteq\; \ldots \;\subseteq\; \mathbb{L}_{n-1} \;\subseteq\; \mathbb{L}_n = \mathbb{Q}(\eta)$$

mit $[\mathbb{L}_i : \mathbb{L}_{i+1}] = 2$. Damit erfüllt die η das Kriterium 9.3.6 und ist aus $\{0, 1\}$ konstruierbar. Folglich sind auch alle weiteren n-ten Einheitswurzeln $\zeta = \eta^m$ aus $\{0, 1\}$ konstruierbar.

Zur Äquivalenz von (ii) und (iii). Wir betrachten die Primafaktorzerlegung $n = p_1^{\nu_1} \cdots p_r^{\nu_r}$. Mit den Eigenschaften der φ-Funktion ergibt sich

$$\varphi(n) \quad = \quad p_1^{\nu_1 - 1} \cdots p_r^{\nu_r - 1}(p_1 - 1) \cdots (p_r - 1).$$

Dieser Wert ist genau dann eine Zweierpotenz, wenn für $\nu_i = 1$ und $p_i - 1 = 2^{m_i}$ für jedes $p_i \neq 2$ gilt. Lemma 9.3.11 liefert dann die Behauptung. $\square$

Aufgaben zu Abschnitt 9.3.

Aufgabe 9.3.14. Führe die Konstruktionen der Mengen $E_n(\mathbb{C})$ für $n = 3, 4, 5, 6$ aus den Besipielen 9.3.2 bis 9.3.5 explizit durch.

10. Galoisgruppe eines Polynoms

10.1. **Die Galoisgruppe eines Polynoms.**

Definition 10.1.1. Es seien k ein Körper und $f \in k[T]$ ein Polynom. Ist $k \subseteq \mathbb{K}$ ein Zerfällungskörper für f, so nennt man $\mathrm{Gal}(f) := \mathrm{Aut}(\mathbb{K}, k)$ auch die *Galoisgruppe von f*, oder die *Galoisgruppe der Gleichung $f(x) = 0$*.

Definition 10.1.2. Eine Operation einer Gruppe G auf einer Menge X heißt *effektiv*, falls $T_g \colon X \to X$, $x \mapsto g \cdot x$ nur für $g = e_G$ die Identität auf X ist.

Satz 10.1.3. *Es sei $k \subseteq \mathbb{K}$ Zerfällungskörper eines Polynoms $f \in k[T]$ mit den Nullstellen $a_1, \ldots, a_n \in \mathbb{K}$, jede nur einmal aufgeführt. Dann hat man eine Operation*

$$\mathrm{Gal}(f) \times \{a_1, \ldots, a_n\} \to \{a_1, \ldots, a_n\}, \qquad \varphi \cdot (a_i) \ := \ \varphi(a_i)$$

der Galoisgruppe von f auf der Nullstellenmenge von f. Diese Operation ist effektiv, d.h., $\varphi(a_i) = a_i$ für $i = 1, \ldots, n$ impliziert bereits $\varphi = \mathrm{id}_{\mathbb{K}}$. Folglich ist

$$\mathrm{Gal}(f) \ \to \ S(\{a_1, \ldots, a_n\}), \qquad \varphi \ \mapsto \ \varphi|_{\{a_1, \ldots, a_n\}}$$

ein Monomorphismus. Insbesondere ist die Ordnung $|\mathrm{Gal}(f)|$ der Galoisgruppe ein Teiler von $n!$ und somit auch ein Teiler von $\deg(f)!$.

Lemma 10.1.4. *Es seien $k \subseteq \mathbb{K}$ eine Körpererweiterung, $\varphi \in \mathrm{Aut}(\mathbb{K}, k)$ und $f \in k[T]$. Ist $a \in \mathbb{K}$ Nullstelle von f, so ist $\varphi(a) \in \mathbb{K}$ ebenfalls Nullstelle von f.*

Beweis. Nach Voraussetzung haben wir eine Darstellung $f = \sum b_j T^j$ mit $b_j \in k$. Damit erhalten wir

$$f(\varphi(a)) = \sum b_j \varphi(a)^j = \sum \varphi(b_j)\varphi(a)^j = \varphi\left(\sum b_j a^j\right) = \varphi(f(a)) = \varphi(0) = 0.$$

□

Beweis von Satz 10.1.3. Gemäß Lemma 10.1.4 lässt $\mathrm{Gal}(f)$ die Nullstellenmenge von f invariant und operiert wie behauptet darauf. Zum Nachweis der Effektivität sei $\varphi \in \mathrm{Gal}(f)$ mit $\varphi(a_i) = a_i$ für $i = 1, \ldots, n$ gegeben. Jedes $a \in \mathbb{K} = k(a_1, \ldots, a_n)$ besitzt eine Darstellung

$$a \ = \ \frac{\sum b_{\nu_1, \ldots, \nu_n} a_1^{\nu_1} \cdots a_n^{\nu_n}}{\sum c_{\mu_1, \ldots, \mu_n} a_1^{\mu_1} \cdots a_n^{\mu_n}}, \qquad b_{\nu_1, \ldots, \nu_n} \ \in \ k, \quad c_{\mu_1, \ldots, \mu_n} \ \in \ k.$$

Das Element $\varphi \in \mathrm{Gal}(f) = \mathrm{Aut}(\mathbb{K}, k)$ lässt die Koeffizienten $b_{\nu_1, \ldots, \nu_n}$ und $c_{\mu_1, \ldots, \mu_n}$ jeweils fest und wir erhalten $\varphi(a) = a$. Das bedeutet $\varphi = \mathrm{id}_{\mathbb{K}}$ und somit operiert $\mathrm{Gal}(f)$ effektiv auf Nullstellenmenge von f. Die weiteren Aussagen sind unmittelbare Konsequenzen. □

Definition 10.1.5. Eine Operation einer Gruppe G auf einer Menge X heißt *transitiv*, falls zu je zwei Elementen x, x' ein $g \in G$ existiert mit $x' = g \cdot x$.

Bemerkung 10.1.6. Eine Operation einer Gruppe G auf einer Menge X ist genau dann transitiv, wenn $X = G \cdot x_0$ mit einem Elemement $x_0 \in X$ gilt.

Satz 10.1.7. *Es sei $k \subseteq \mathbb{K}$ Zerfällungskörper eines Polynoms $f \in k[T]$ vom Grad n mit paarweise verschiedenen Nullstellen $a_1, \ldots, a_n \in \mathbb{K}$. Dann ist $k \subseteq \mathbb{K}$ galoissch. Weiter sind folgende Aussagen äquivalent:*

(i) *f ist irreduzibel in $k[T]$.*
(ii) *$\mathrm{Gal}(f)$ operiert transitiv auf $\{a_1, \ldots, a_n\}$.*

Beweis. Da f genau $n = \deg(f)$ paarweise verschiedene Nullstellen in seinem Zerfällungskörper besitzt, ist es ein separables Polynom. Nach Satz 8.3.3 ist $k \subseteq \mathbb{K}$ eine Galoiserweiterung.

Zur Implikation "(i)⇒(ii)". Es seien a_i und a_j Nullstellen von f. Nach Lemma 7.1.10 gibt es einen eindeutig bestimmten Körperisomorphismus $\psi\colon k(a_i) \to k(a_j)$ mit $\psi|_k = \mathrm{id}_k$ und $\psi(a_i) = a_j$. Bezeichnet $k \subseteq \overline{k}$ einen algebraischen Abschluss mit $\mathbb{K} \subseteq \overline{k}$, so liefert Satz 7.2.7 eine Fortsetzung $\varphi\colon \mathbb{K} \to \overline{k}$ von ψ. Da $k \subseteq \mathbb{K}$ eine normale Erweiterung ist, gilt $\varphi(\mathbb{K}) = \mathbb{K}$; siehe Satz 7.1.13. Damit ist φ ein Element in $\mathrm{Gal}(f)$, das a_i nach a_j abbildet.

Zur Implikation "(ii)⇒(i)". Nehmen wir an, f erlaube eine Zerlegung $f = gh$ mit nichtkonstanten Polynomen $g, h \in k[T]$. Die Nullstellen $b_1, \ldots, b_l \in \mathbb{K}$ von g und $c_1, \ldots, c_m$ von h sind jeweils paarweise verschieden, und man hat eine disjunkte Vereinigung

$$\{a_1, \ldots, a_n\} \;=\; \{b_1, \ldots, b_l\} \;\cup\; \{c_1, \ldots, c_m\}.$$

Gemäß Lemma 10.1.4 bildet jedes $\varphi \in \mathrm{Gal}(f)$ jede Nullstelle von g (bzw. h) auf eine Nullstelle von g (bzw. h) ab. Insbesondere kann es kein $\varphi \in \mathrm{Gal}(f)$ mit $\varphi(b_1) = c_1$ geben. Das widerspricht der Transitivität der Operation von $\mathrm{Gal}(f)$ auf $\{a_1, \ldots, a_n\}$. □

Folgerung 10.1.8. *Es sei $k \subseteq \mathbb{K}$ Zerfällungskörper eines Polynoms $f \in k[T]$ vom Grad n mit paarweise verschiedenen Nullstellen $a_1, \ldots, a_n \in \mathbb{K}$. Gilt $[\mathbb{K} : k] = n!$, so ist f irreduzibel in $k[T]$ und man hat einen kanonischen Isomorphismus*

$$\mathrm{Gal}(f) \;\to\; S(\{a_1, \ldots, a_n\}), \qquad \varphi \;\mapsto\; \varphi|_{\{a_1,\ldots,a_n\}}.$$

Beweis. Nach Satz 10.1.7 ist die Erweiterung $k \subseteq \mathbb{K}$ galoissch. Folglich ist $\mathrm{Gal}(f)$ von der Ordnung $[\mathbb{K} : k] = n!$. Damit ist der Monomorphismus von Satz 10.1.3 ein Isomorphismus. Insbesondere operiert $\mathrm{Gal}(f)$ transitiv auf der Nullstellenmenge von f. Satz 10.1.7 liefert dann die Irreduzibilität von f. □

Beispiel 10.1.9. Wir betrachten das Polynom $f := T^3 - 1 \in \mathbb{Q}[T]$. Seine Nullstellen in $\mathbb{C}$ sind 1, $e^{2\pi i/3}$ und $e^{4\pi i/3}$. Weiter erhält man einen Zerfällungskörper

$$\mathbb{K} \;:=\; \mathbb{Q}(1, e^{2\pi i/3}, e^{4\pi i/3}) \;=\; \mathbb{Q}(e^{2\pi i/3}) \;\subseteq\; \mathbb{C}.$$

Wegen $\varphi(1) = 1$ für alle $\varphi \in \mathrm{Gal}(f) = \mathrm{Aut}(\mathbb{K}, \mathbb{Q})$ kann $\mathrm{Gal}(f)$ nicht transitiv auf der Nullstellenmenge von f wirken, also ist f nicht irreduzibel; tatsächlich gilt

$$T^3 - 1 \quad = \quad (T^2 + T + 1)(T - 1).$$

Da $\mathbb{K} = \mathbb{Q}(e^{2\pi i/3})$ gilt und $g := T^2 + T + 1 \in \mathbb{Q}[T]$ offenbar das Minimalpolynom für $e^{2\pi i/3}$ ist, erhalten wir für Galoisgruppe

$$|\mathrm{Gal}(f)| \;=\; [\mathbb{K} : \mathbb{Q}] \;=\; \deg(g) \;=\; 2.$$

Folglich ist $\mathrm{Gal}(f)$ zyklisch von der Ordnung zwei. Konkret ist $\mathrm{Gal}(f)$ die von der komplexen Konjugation $\kappa\colon x + iy \mapsto x - iy$ erzeugte Gruppe.

Satz 10.1.10. *Es seien p eine Primzahl und $f \in \mathbb{Q}[T]$ ein irreduzibles Polynom vom Grad p, das in $\mathbb{C}$ genau zwei nicht reelle Nullstellen hat. Dann gilt $\mathrm{Gal}(f) \cong S_p$.*

Lemma 10.1.11. *Es sei $p \in \mathbb{Z}_{\geq 2}$ eine Primzahl. Sind $\tau \in S_p$ eine Transposition und $\sigma \in S_p$ ein Element der Ordnung p, so gilt $S_p = \langle \tau, \sigma \rangle$.*

Beweis. Wir zeigen zunächst, dass σ ein Zykel ist. Lemma 2.4.16 liefert eine Darstellung $\sigma = \tau_1 \cdots \tau_r$ mit elementfremden Zykeln τ_i der Ordnungen k_i. Da elementfremde Zykeln kommutieren, ist die Ordnung p von σ ein gemeinsames Vielfaches

der Zykelordnungen k_i. Primalität von p impliziert $k_1 = \ldots = k_r = p$ und Elementfremdeiheit der τ_i erzwingt $r = 1$.

Wir kommen nun zum Beweis der Aussage. Es sei $\tau = (k, l)$. Durch Konjugieren mit dem Element $\varrho := (1, k)(2, l)$ erhalten wir

$$\varrho\tau\varrho^{-1} \quad = \quad (1, 2).$$

Weiter ist $\varrho\sigma\varrho^{-1}$ wieder ein p-Zykel in S_p. Folglich gibt es ein $1 \leq m \leq p-1$ mit

$$(\varrho\sigma\varrho^{-1})^m(1) \;=\; (\varrho\sigma^m\varrho^{-1})(1) \;=\; 2.$$

Das Element $(\varrho\sigma\varrho^{-1})^m$ ist wieder ein Zykel und besitzt, da p prim ist, wieder die Ordnung p. Folglich gibt es paarweise verschiedene $i_3, \ldots, i_p$ mit

$$(\varrho\sigma\varrho^{-1})^m \quad = \quad (1, 2, i_3, \ldots, i_p).$$

Wir betrachten weiter das Element

$$\pi \quad := \quad \left[\begin{array}{ccccc} 1 & 2 & 3 & \ldots & p \\ 1 & 2 & i_1 & \ldots & i_p \end{array} \right]^{-1}$$

Damit gilt

$$\begin{array}{rcll} \alpha & := & (\pi\varrho)\tau(\pi\varrho)^{-1} & = & (1, 2), \\ \beta & := & (\pi\varrho)\sigma^m(\pi\varrho)^{-1} & = & (1, 2, 3, \ldots, p). \end{array}$$

Es genügt nun zu zeigen, dass α und β bereits S_p erzeugen. Denn dann erzeugen auch τ und σ die gesamte Gruppe S_p wegen

$$|S_p| \;=\; |\langle\alpha, \beta\rangle| \;=\; |\langle\tau, \sigma^m\rangle| \;\leq\; |\langle\tau, \sigma\rangle|.$$

Da S_p von Transpositionen erzeugt wird, siehe Lemma 2.4.16, genügt es zu zeigen, dass man alle Transpositionen durch α und β darstellen kann. Das ergibt sich mit

$$\begin{array}{rcl} (2, 3) & = & (1, 2, 3, \ldots, p)(1, 2)(1, 2, 3, \ldots, p)^{-1}, \\ (3, 4) & = & (1, 2, 3, \ldots, p)(2, 3)(1, 2, 3, \ldots, p)^{-1}, \\ & \vdots & \\ (p-1, p) & = & (1, 2, 3, \ldots, p)(p-2, p-1)(1, 2, 3, \ldots, p)^{-1}, \\ \\ (1, 3) & = & (1, 2)(2, 3)(1, 2), \\ (1, 4) & = & (1, 3)(3, 4)(1, 4), \\ & \vdots & \\ (1, p) & = & (1, p-1)(p-1, p)(1, p-1), \\ \\ (k, l) & = & (1, k)(1, l)(1, k). \end{array}$$

□

Beweis von Satz 10.1.10. Nach Lemma 10.1.11 genügt es zu zeigen, dass $\mathrm{Gal}(f)$ eine Transposition und Element der Ordnung p enthält. Sind $a_1, a_2 \in \mathbb{C}$ die beiden nicht reellen Nullstellen und $a_3, \ldots, a_p \in \mathbb{R}$ die verbleibenden, so gilt

$$\overline{a_1} = a_2, \quad \overline{a_2} = a_1, \quad \overline{a_3} = a_3, \quad \ldots, \quad \overline{a_p} = a_p$$

für die komplexe Konjugation $\kappa\colon z \mapsto \overline{z}$. Folglich definiert κ eine Transposition in $\mathrm{Gal}(f)$. Um ein Element der Ordnung p zu gewinnen, bezeichnen wir mit $\mathbb{K} := \mathbb{Q}(a_1, \ldots, a_p)$ den Zerfällungskörper von f. Dann hat man

$$|\mathrm{Gal}(f)| \;=\; [\mathbb{K} : \mathbb{Q}] \;=\; [\mathbb{K} : \mathbb{K}(a_1)][\mathbb{K}(a_1) : \mathbb{Q}] \;=\; [\mathbb{K} : \mathbb{K}(a_1)]p,$$

wobei man für $[\mathbb{K}(a_1) : \mathbb{Q}] = p$ verwendet, dass f (bis auf Normierung) das Minimalpolynom von a_1 über $\mathbb{Q}$ ist, und $\mathbb{Q} \subseteq \mathbb{K}(a_1)$ daher vom Grad $\deg(f) = p$ ist. Nach Satz 2.3.16 besitzt $\mathrm{Gal}(f)$ daher ein Element der Ordnung p. □

Beispiel 10.1.12. Das Polynom $f := T^3 - 2 \in \mathbb{Q}[T]$ besitzt die Nullstellen in $\sqrt[3]{2}$, $\sqrt[3]{2}e^{\frac{2\pi i}{3}}$ und $\sqrt[3]{2}e^{\frac{4\pi i}{3}}$ in $\mathbb{C}$. Sein Zerfällungskörper $\mathbb{Q} \subseteq \mathbb{K}$ ist also gegeben durch

$$\mathbb{K} \ := \ \mathbb{Q}\left(\sqrt[3]{2}, \sqrt[3]{2}e^{\frac{2\pi i}{3}}, \sqrt[3]{2}e^{\frac{4\pi i}{3}}\right) \ \subseteq \ \mathbb{C}.$$

Als rationales Polynom dritten Grades ohne rationale Nullstellen ist f ist irreduzibel in $\mathbb{Q}[T]$. Mit Satz 10.1.10 erhalten wir

$$\mathrm{Gal}(f) \ \cong \ S_3, \qquad\qquad [\mathbb{K} : \mathbb{Q}] \ = \ 3! \ = \ 6.$$

Aufgaben zu Abschnitt 10.1.

Aufgabe 10.1.13. Beweise Bemerkung 10.1.6: Eine Operation einer Gruppe G auf einer Menge X ist genau dann transitiv, wenn $X = G{\cdot}x_0$ mit einem Elemement $x_0 \in X$ gilt.

10.2. **Resultante I.**

Problem 10.2.1. Es seien k ein Körper und $f, g \in k[T]$ zwei Polynome. Gesucht ist ein effizientes Verfahren, das entscheidet, ob f und g eine gemeinsame Nullstelle in einem algebraischen Abschluss $k \subseteq \overline{k}$ besitzen.

Definition 10.2.2. Es seien R ein K1-Ring, und es seien zwei Polynome in $R[T]$ gegeben:

$$f \;=\; a_0T^m + a_1T^{m-1} + \ldots + a_m, \qquad g \;=\; b_0T^n + b_1T^{n-1} + \ldots + b_n.$$

Aus den Koeffizienten $a_0, \ldots, a_m$ und $b_0, \ldots, b_n$ bilden wir ein Schema mit $m+n$ Zeilen und Spalten:

$$\begin{array}{c|cccccccc}
 & 1 & 2 & \ldots & m{+}1 & m{+}2 & m{+}3 & \ldots & m{+}n \\
1 & a_0 & a_1 & \ldots & a_m & 0 & 0 & \ldots & 0 \\
2 & 0 & a_0 & a_1 & \ldots & a_m & 0 & \ldots & 0 \\
\vdots & & & & & & & & \\
n & 0 & 0 & \ldots & 0 & a_0 & a_1 & \ldots & a_m \\
n{+}1 & b_0 & b_1 & \ldots & b_n & 0 & 0 & \ldots & 0 \\
n{+}2 & 0 & b_0 & b_1 & \ldots & b_n & 0 & \ldots & 0 \\
\vdots & & & & & & & & \\
n{+}m & 0 & 0 & \ldots & 0 & b_0 & b_1 & \ldots & b_n \\
 & 1 & 2 & \ldots & n{+}1 & n{+}2 & n{+}3 & \ldots & n{+}m
\end{array}$$

Fasst man diese Anordnung als eine Matrix $A(f,g) \in \mathrm{Mat}(m+n, m+n; R)$ auf, so ist die *Resultante von f und g zum Formalgrad (m,n)* definiert als

$$\mathrm{Res}(f,g) \;:=\; \det(A(f,g)).$$

Beispiel 10.2.3. Es seien R ein K1-Ring, und es seien $f = T - a$ und $g = T - b$ mit $a, b \in R$. Dann ist die Resultante zum Formalgrad $(1,1)$ von f und g gegeben durch

$$\mathrm{Res}(f,g) \;=\; \det\begin{pmatrix} 1 & -a \\ 1 & -b \end{pmatrix} \;=\; a - b.$$

Lemma 10.2.4. *Es seien R ein K1-Ring, $f, g \in R[T]$, und es seien $a, b \in R$. Dann gilt*

$$\mathrm{Res}(f,g) \;=\; (-1)^{mn}\mathrm{Res}(g,f), \qquad \mathrm{Res}(af,bg) \;=\; a^n b^m \mathrm{Res}(f,g).$$

Beweis. Die Aussagen ergeben sich direkt aus der Tatsache, dass die Determinante eine alternierende Multilinearform ist. □

Lemma 10.2.5. *Es seien R ein K1-Ring, und es seien zwei Polynome in $R[T]$ gegeben:*

$$f \;=\; a_0T^m + a_1T^{m-1} + \ldots + a_m, \qquad g \;=\; b_0T^n + b_1T^{n-1} + \ldots + b_n.$$

Ist $\varphi\colon R \to S$ ein Homomorphismus von K1-Ringen, so bezeichne $\Phi\colon R[T] \to S[T]$ die Fortsetzung von φ mit $\Phi(T) = T$. Es gilt dann

$$\mathrm{Res}(\Phi(f), \Phi(g)) \;=\; \varphi(\mathrm{Res}(f,g)).$$

Beweis. Setzt man $(c_{ij}) := A(f,g)$, so gilt $A(\Phi(f), \Phi(g)) := (\varphi(c_{ij}))$. Da φ ein Ringhomomorphismus ist, erhalten wir $\det(\varphi(c_{ij})) = \varphi(\det(c_ij))$. Damit folgt die Behauptung. □

Satz 10.2.6. *Es seien R ein K1-Ring und $m, n \in \mathbb{Z}_{\geq 0}$ mit $m+n \geq 1$. Weiter seien $f, g \in R[T]$ gegeben als*

$$f \;=\; a_0T^m + a_1T^{m-1} + \ldots + a_m, \qquad g \;=\; b_0T^n + b_1T^{n-1} + \ldots + b_n.$$

Dann gibt es Polynome $p, q \in R[T]$ mit $\deg(p) < n$ und $\deg(q) < m$, sodass man die Resultante von f und g erhält als

$$\operatorname{Res}(f,g) \quad = \quad pf + qg.$$

Lemma 10.2.7. *Es seien R ein K1-Ring, und es seien zwei Polynome in $R[T]$ gegeben:*

$$f \;=\; a_0T^m + a_1T^{m-1} + \ldots + a_m, \qquad g \;=\; b_0T^n + b_1T^{n-1} + \ldots + b_n.$$

Bezeichnet $R[T]_l \subseteq R[T]$ den (freien) R-Modul aller Polynome vom Grad $\leq l$, so hat man einen Modulhomomorphismus

$$\Psi\colon R[T]_n \oplus R[T]_m \;\to\; R[T]_{m+n}, \qquad (u,v) \;\mapsto\; uf + vg.$$

Dann besitzt Ψ bezüglich der Basen $\{(T^{n-1},0), \ldots, (T^0,0), (0,T^{m-1}), \ldots, (0,T^0)\}$ auf $R[T]_n \oplus R[T]_m$ und $\{T^{m+n-1}, \ldots, T^0\}$ auf $R[T]_{m+n}$ die Matrix $A(f,g)^t$.

Beweis. Für die Bilder der Basisvektoren $(T^i,0)$ bzw. $(0,T^i)$ unter Ψ erhalten wir

$$\begin{array}{lcll}
\Psi(T^{n-1},0) & = & T^{n-1}f & = \quad a_0T^{m+n-1} + \ldots + a_mT^{n-1}, \\
\vdots & & \vdots & \\
\Psi(T^0,0) & = & T^0 f & = \quad a_0T^m + \ldots + a_mT^0, \\
\\
\Psi(0,T^{m-1}) & = & T^{m-1}g & = \quad b_0T^{m+n-1} + \ldots + b_nT^{m-1}, \\
\vdots & & \vdots & \\
\Psi(0,T^0) & = & T^0 g & = \quad b_0T^n + \ldots + b_nT^0.
\end{array}$$

Damit ergibt sich, dass $A(f,g)^t$ die beschreibende Matrix von Ψ bezüglich der genannten Basen ist. □

Beweis von Satz 10.2.6. Es sei $A := A(f,g)^t$. Nach der Cramerschen Regel gibt es eine Matrix $B \in \operatorname{Mat}(m+n, m+n, R)$ mit

$$AB \quad = \quad \det(A)E_{m+n}.$$

Fixiert man auf $R[T]_{m+n}$ die Basis $\{T^{m+n-1}, \ldots, T^0\}$, so entspricht B einer linearen Abbildung $\Psi^*\colon R[T]_{m+n} \to R[T]_{m+n}$. Weiter haben wir einen Isomorphismus

$$\begin{array}{rcl}
\imath\colon R[T]_{m+n} & \to & R[T]_n \oplus R[T]_m, \\
T^{m+i} & \mapsto & (T^i,0) \quad \text{für } 0 \leq i \leq n-1, \\
T^i & \mapsto & (0,T^i) \quad \text{für } 0 \leq i \leq m-1.
\end{array}$$

Die zugehörige Matrix bezüglich der Basen $\{T^{m+n-1}, \ldots, T^0\}$ auf $R[T]_{m+n}$ und $\{(T^{n-1},0), \ldots, (T^0,0), (0,T^{m-1}), \ldots, (0,T^0)\}$ auf $R[T]_n \oplus R[T]_m$ ist die Einheitsmatrix.

Nach Lemma 10.2.7 besitzt $\Psi \circ \imath \circ \Psi^*$ bezüglich der Basis $\{T^{m+n-1}, \ldots, T^0\}$ auf $R[T]_{n+m}$ die Matrix AB. Damit ergibt sich

$$\Psi \circ \imath \circ \Psi^* \quad = \quad \operatorname{Res}(f,g) \cdot \operatorname{id}_{R[T]_{m+n}}.$$

Wendet man diesse Identität von Abbildungen nun auf das konstante Polynom 1 an, so ergibt sich

$$\operatorname{Res}(f,g) \;=\; \Psi \circ \imath \circ \Psi^*(1) \;=\; \Psi(p,q) \;=\; pf + qg$$

mit gewissen Polynomen $p \in R[T]_n$ und $q \in R[T]_m$. □

Lemma 10.2.8. *Es seien R ein K1-Ring und $f \in R[T]$ ein normiertes Polynom vom Grad m. Dann hat man einen Isomorphismus von freien R-Moduln*

$$R[T]_m \ \to \ R/\langle f\rangle, \qquad T^i \ \mapsto \ T^i + \langle f\rangle.$$

Beweis. Die Aussage ergibt sich als unmittelbare Anwendung der Division mit Rest 9.2.3 in dem Ring $R[T]$. □

Satz 10.2.9. *Es seien R ein K1-Ring, und es seien zwei Polynome $f, g \in R[T]$ gegeben als:*

$$f \ = \ T^m + a_1T^{m-1} + \ldots + a_m, \qquad g \ = \ b_0T^n + b_1T^{n-1} + \ldots + b_n.$$

Weiter sei $M := R[T]/\langle f\rangle$, und es sei $N_{M/R}(\overline{g}) \in R$ die Determinante des R-Modulhomomorphismus

$$\mu_g \colon M \ \to \ M, \qquad \overline{h} \ \mapsto \ g \cdot \overline{h} = \overline{g} \cdot \overline{h},$$

wobei $\overline{g} \in M$ die Restklasse von $g \in R[T]$ bezeichnet. Dann ist die Resultante von f und g gegeben als

$$\mathrm{Res}(f, g) \ = \ N_{M/R}(\overline{g}).$$

Lemma 10.2.10. *Es seien R ein K1-Ring, und es seien zwei Polynome $f, g \in R[T]$ gegeben als:*

$$f \ = \ T^m + a_1T^{m-1} + \ldots + a_m, \qquad g \ = \ b_0T^n + b_1T^{n-1} + \ldots + b_n.$$

Weiter seien $\mathfrak{B} := \{T^{m+n-1}, \ldots, T^0\}$ und $\mathfrak{B}' := \{fT^{n-1}, \ldots, fT^0, T^{m-1}, \ldots, T^0\}$ Dann gilt

(i) *$\mathfrak{B}$ und $\mathfrak{B}'$ sind Basen für $R[T]_{m+n}$, und der zugehörige Basiswechsel besitzt die Determinante* 1.
(ii) *$\mathrm{Res}(f, g)$ ist die Determinante des wie folgt definierten R-linearen Endomorphismus*

$$\Psi' \colon R[T]_{m+n} \ \to \ R_{m+n}, \qquad fT^i \ \mapsto \ fT^i, \quad T^i \ \mapsto \ gT^i.$$

Beweis. Zu (i). Die Elemente von $\mathfrak{B}'$ erhält man wie folgt als R-Linearkombinationen durch Elemente der Basis $\mathfrak{B}$:

$$\begin{array}{rcll} fT^i & = & T^{m+i} + a_1T^{m-1+i} + \ldots + a_0T^i & \text{für } 0 \le i \le n-1 \\ T^i & = & T^i & \text{für } 0 \le i \le m-1 \end{array}$$

Daraus ergibt sich, dass $\mathfrak{B}'$ eine Basis für $R[T]_{m+n}$ ist, und dass der zugehörige Basiswechsel durch eine Dreiecksmatrix mit Diagonaleinträgen 1 beschrieben wird.

Zu (ii). Wählt man $\mathfrak{B}'$ als Basis auf dem Urbildraum und $\mathfrak{B}$ als Basis auf dem Bildraum, so besitzt Ψ' bezüglich dieser Basen gerade die Matrix $A(f, g)^t$. Führt man nun im Bildraum einen Basiswechsel von $\mathfrak{B}$ zu $\mathfrak{B}'$ durch, so erhält man mit (ii) die Behauptung. □

Beweis von Satz 10.2.9. Mit Lemma 10.2.8 und Lemma 10.2.10 erhalten wir einen Isomorphismus von R-Moduln

$$\begin{array}{rcl} \imath \colon R[T]_{m+n} & \to & R[T]_n \oplus M, \\ fT^i & \mapsto & (T^i, 0) \quad \text{für } 0 \le i \le n-1, \\ T^i & \mapsto & (0, T^i + \langle f\rangle) \quad \text{für } 0 \le i \le m-1. \end{array}$$

Mit der Abbildung Ψ' aus Lemma 10.2.10 erhalten wir ein kommutatives Diagramm von R-Modulhomomorphismen

$$\begin{array}{ccc} R[T]_{m+n} & \xrightarrow{\Psi'} & R[T]_{m+n} \\ {\scriptstyle \imath}\downarrow{\scriptstyle \cong} & & {\scriptstyle \cong}\downarrow{\scriptstyle \imath} \\ R[T]_n \oplus M & \xrightarrow[\mathrm{id}\times\mu_g]{} & R[T]_n \oplus M \end{array}$$

Zum Nachweis der Kommutativität verfolge man die Elemente der Basis $\mathfrak{B}'$. Die waagerechten Endomorphismen dieses Diagramms dieselbe Determinante. Lemma 10.2.10 (ii) liefert nun die Behauptung. □

Aufgaben zu Abschnitt 10.2.

10.3. **Resultante II.**

Satz 10.3.1. *Es seien k ein Körper, $k \subseteq \overline{k}$ ein algebraischer Abschluss, $f, g \in k[T]$ Polynome mit $\deg(f) = m$ und $\deg(g) \leq n$. Dann sind folgende Aussagen äquivalent*

(i) *Die Polynome f und g haben eine gemeinsame Nullstelle in $\overline{k}$.*
(ii) *Die Resultante $\mathrm{Res}(f, g)$ zum Formalgrad (m, n) verschwindet.*

Beweis. Nach Lemma 10.2.4 dürfen wir für den Beweis annehmen, dass das Polynom f normiert ist.

Zur Implikation "(i)⇒(ii)". Nehmen wir an, es gelte $\mathrm{Res}(f, g) \neq 0$. Dann liefert Satz 10.2.9, dass die lineare Abbildung

$$k[T]/\langle f\rangle \;\to\; k[T]/\langle f\rangle, \qquad \overline{h} \;\mapsto\; \overline{g}\cdot\overline{h}$$

eine nichtverschwindende Determinate besitzt und somit invertierbar ist. Das bedeutet, dass $\overline{g}$ eine Einheit in dem Restklassenring $R/\langle f\rangle$ ist. Damit ergibt sich

$$uf + vg \;=\; 1 \;\in\; k[T] \qquad \text{mit geeigneten } u, f \in k[T].$$

Insbesondere sehen wir, dass f und g keine gemeinsame Nullstelle in $\overline{k}$ besitzen können. Widerspruch.

Zur Implikation "(ii)⇒(i)". Nehmen wir an, f und g hätten keine gemeinsame Nullstelle in $\overline{k}$. Dann sind f und g teilerfremd in $k[T]$, man hat also eine Darstellung

$$uf + vg \;=\; 1 \;\in\; k[T] \qquad \text{mit Polynomen } u, f \in k[T].$$

Es folgt, dass $\overline{g}$ eine Einheit in dem Restklassenring $k[T]/\langle f\rangle$ ist. Somit ist die lineare Abbildung

$$k[T]/\langle f\rangle \;\to\; k[T]/\langle f\rangle, \qquad \overline{h} \;\mapsto\; \overline{g}\cdot\overline{h}$$

invertierbar und besitzt deshalb eine nichtverschwindende Determinate. Satz 10.2.9 liefert, dass $\mathrm{Res}(f, g) \neq 0$ gilt. Widerspruch. □

Satz 10.3.2. *Es seien k ein Körper, $k \subseteq \overline{k}$ ein algebraischer Abschluss, $f, g \in k[T]$ Polynome mit Zerlegungen*

$$f \;=\; c\prod_{i=1}^{m}(T - a_i), \qquad g \;=\; d\prod_{j=1}^{n}(T - b_j)$$

in $\overline{k}[T]$. Dann ist die Resultante zum formalen Grad (m, n) von f und g gegeben durch

$$\mathrm{Res}(f, g) \;=\; c^n\prod_{i=1}^{m} g(a_i) \;=\; c^n d^m \prod_{\substack{1\leq i\leq m\\ 1\leq j\leq n}} (a_i - b_j).$$

Lemma 10.3.3. *Es seien k ein Körper, $k \subseteq \overline{k}$ ein algebraischer Abschluss, $f, g \in k[T]$ normierte Polynome mit Zerlegungen $f = f_1 f_2$ und $g = g_1 g_2$ in $k[T]$. Dann ist die Resultante zum formalen Grad (m, n) von f und g gegeben durch*

$$\mathrm{Res}(f, g) \;=\; \mathrm{Res}(f, g_1)\cdot\mathrm{Res}(f, g_2) \;=\; \mathrm{Res}(f_1, g)\cdot\mathrm{Res}(f_2, g).$$

Beweis. Die Determinante $N_{M/R}(?)$ aus Satz 10.2.9 ist multplikativ. Damit ergibt sich die erste Gleichung. Die zweite Gleichung folgt mit Lemma 10.2.4. □

Beweis von Satz 10.3.2. Nach Lemma 10.2.4 dürfen wir $c = d = 1$ annehmen. Mit Lemma 10.3.3 erhalten wir

$$\begin{aligned}\operatorname{Res}(f,g) &= \prod_{i=1}^{m} \operatorname{Res}(T-a_i, g) \\ &= \prod_{i=1}^{m} \left(\prod_{j=1}^{n} \operatorname{Res}(T-a_i, T-b_j) \right) \\ &= \prod_{\substack{1\le i\le m \\ 1\le j\le n}} (a_i - b_j).\end{aligned}$$

□

Beispiel 10.3.4. Es sei $f = T^2 + pT + q \in \mathbb{R}[T]$. Dann besitzt f nach der "Mitternachtsformel" die Nullstellen

$$x_{1,2} = \frac{-p \pm \sqrt{p^2 - 4q}}{2}$$

im Körper $\mathbb{C}$ der komplexen Zahlen. Die *Diskriminante* von f wird in der Schule üblicherweise definiert als

$$\Delta(f) := p^2 - 4q = (x_1 - x_2)^2.$$

Die Diskriminante besitzt bekanntlich Information über die möglichen Lösungen der Gleichung $f(x) = 0$ in $\mathbb{C}$:

- Gilt $\Delta(f) > 0$, so gibt es genau zwei Lösungen und diese sind reell.
- Gilt $\Delta(f) = 0$, so gibt es genau eine Lösung, und diese ist reell.
- Gilt $\Delta(f) < 0$, so gibt es genau zwei Lösungen und diese sind nicht reell.

Definition 10.3.5. Es seien k ein Körper, $k \subseteq \overline{k}$ ein algebraischer Abschluss und $f \in k[T]$ ein normiertes Polynom mit einer Zerlegung

$$f = \prod_{i=1}^{n} (T - a_i)$$

in $\overline{k}[T]$, wobei $a_1, \ldots, a_n \in \overline{k}$. Dann ist die *Diskriminante* des Polynoms $f \in k[T]$ definiert als

$$\Delta(f) = \prod_{1\le i<j\le n} (a_i - a_j)^2.$$

Bemerkung 10.3.6. Ein normiertes Polynom f über einem Körper k besitzt genau dann mehrfache Nullstellen in dem algebraischen Abschluss $\overline{k} \supseteq k$, wenn die Diskriminante $\Delta(f)$ verschwindet.

Problem 10.3.7. Wie berechnet man die Diskriminante eines gegebenen Polynoms?

Satz 10.3.8. *Es seien k ein Körper, und $f \in k[T]$ ein normiertes Polynom vom Grad m und $f' = D(f) \in k[T]$ seine formale Ableitung. Dann gilt*

$$\Delta(f) = (-1)^{\frac{m(m-1)}{2}} \operatorname{Res}(f, f').$$

Beweis. Es sei $k \subseteq \overline{k}$ ein algebraischer Abschluss. Wir betrachten die Zerlegung von f in Linearfaktoren:

$$f = \prod_{i=1}^{n} (T - a_i)$$

mit den Nullstellen $a_1, \ldots, a_n \in \overline{k}$. Nach der Produktregel erhalten wir für die formale Ableitung

$$f' \;=\; \sum_{i=1}^{m} (T-a_1)\ldots(T-a_{i-1})(T-a_{i+1})\ldots(T-a_m).$$

Auswerten von f' in a_j ergibt

$$f'(a_j) \;=\; (a_j-a_1)\ldots(a_j-a_{j-1})(a_j-a_{j+1})(a_j-a_m).$$

Mit Satz 10.3.2 erhalten wir

$$\begin{aligned}\operatorname{Res}(f,f') &= \prod_{j=1}^{m} f'(a_j)\\ &= \prod_{i\neq j}(a_i-a_j)\\ &= (-1)^{\frac{m(m-1)}{2}} \prod_{i<j}(a_i-a_j)^2.\end{aligned}$$

□

Folgerung 10.3.9. *Es seien k ein Körper, $R \subseteq k$ ein Unterring und $f \in R[T]$ ein normiertes Polynom. Dann gilt $\Delta(f) \in R$.*

Beispiel 10.3.10. Für einen Körper k betrachten wir das Polynom $f = T^3 + aT + b \in k[T]$. Dann gilt $f' = 3T^2 + a$. Die Diskriminante berechnet man also gemäß

$$\Delta(f) \;=\; -\operatorname{Res}(f,f') \;=\; -\det\begin{pmatrix} 1 & 0 & a & b & 0\\ 0 & 1 & 0 & a & b\\ 3 & 0 & a & 0 & 0\\ 0 & 3 & 0 & a & 0\\ 0 & 0 & 3 & 0 & a \end{pmatrix}$$

Durch Subtrahieren des 3-Fachen der ersten Zeile von der dritten sowie des 3-Fachen der zweiten Zeile von der vierten erhält man

$$\begin{pmatrix} 1 & 0 & a & b & 0\\ 0 & 1 & 0 & a & b\\ 3 & 0 & a & 0 & 0\\ 0 & 3 & 0 & a & 0\\ 0 & 0 & 3 & 0 & a \end{pmatrix} \;\sim\; \begin{pmatrix} 1 & 0 & a & b & 0\\ 0 & 1 & 0 & a & b\\ 0 & 0 & -2a & -3b & 0\\ 0 & 0 & 0 & -2a & -3b\\ 0 & 0 & 3 & 0 & a \end{pmatrix}$$

Folglich kann man die Diskriminante von f berechnen als

$$\Delta(f) \;=\; -\det\begin{pmatrix} -2a & -3b & 0\\ 0 & -2a & -3b\\ 3 & 0 & a \end{pmatrix} \;=\; -4a^3 - 27b^2.$$

Bemerkung 10.3.11. Es sei k ein Körper der Charakteristik Null. Weiter sei $f = T^3 + aT + b \in k[T]$ ein Polynom mit Zerfällungskörper $k \subseteq \mathbb{K}$, sodass keine der Nullstellen $a_1, a_2, a_3 \in \mathbb{K}$ von f in k liegt. Dann ist $f \in k[T]$ irreduzibel und somit Minimalpolynom für jede seiner Nullstellen $a_i \in \mathbb{K}$. Nach Folgerung 8.3.4 ist $k \subseteq \mathbb{K}$ eine Galoiserweiterung.

Fall 1. Es gilt $\mathbb{K} = k(a_i)$ für ein $i = 1, 2, 3$. Da f das Minimalpolynom für a_i über k ist, gilt dann $[\mathbb{K} : k] = \deg(f) = 3$. Folglich ist $\operatorname{Gal}(f)$ von der Ordnung 3 und somit isomorph zur zyklischen Gruppe $\mathbb{Z}/3\mathbb{Z}$.

Fall 2. Es gilt $\mathbb{K} \neq k(a_i)$ für jedes $i = 1, 2, 3$. Für die Ordnung m der Galoisgruppe $\operatorname{Gal}(f)$ erhalten wir dann $m = 6$ wegen

$$3 \;=\; [k(a_i) : k] \;<\; [\mathbb{K} : k] \;=\; m, \qquad m \mid \deg(f)!,$$

siehe Satz 10.1.3. Dabei ist $\mathrm{Gal}(f)$ nicht isomorph zu $\mathbb{Z}/6\mathbb{Z}$. Andernfalls hätten wir genau eine Untergruppe $H \leq \mathrm{Gal}(F)$ der Ordnung 2 und somit

$$k(a_1)^H \;=\; k(a_2)^H \;=\; k(a_3)^H \;=\; \mathbb{K}$$

gemäß Theorem 8.2.2; Widerspruch. Damit ist die Galoisgruppe $\mathrm{Gal}(f)$ isomorph zur symmetrischen Gruppe S_3. Insbesondere ist $\mathrm{Gal}(f)$ nicht abelsch.

Satz 10.3.12. *Es seien k ein Körper der Charakteristik Null und $f = T^3 + aT + b$ ein Polynom aus $k[T]$ ohne Nullstellen in k. Dann gilt*

$$\mathrm{Gal}(f) \;\cong\; \begin{cases} \mathbb{Z}/3\mathbb{Z} & \text{falls } \Delta(f) \text{ eine Quadratwurzel in } k \text{ besitzt,} \\ S_3 & \text{falls } \Delta(f) \text{ keine Quadratwurzel in } k \text{ besitzt.} \end{cases}$$

Beweis. Es sei $k \subseteq \mathbb{K}$ ein Zerfällungskörper für f, und es seien $a_1, a_2, a_3 \in \mathbb{K}$ die Nullstellen von f. Wir sind in der Situation von Bemerkung 10.3.11 und wissen deshalb, dass $\mathrm{Gal}(f)$ entweder isomorph zu $\mathbb{Z}/3\mathbb{Z}$ oder zu S_3 ist. Wir betrachten den Ausdruck

$$\delta \;:=\; (a_1 - a_2)(a_1 - a_3)(a_2 - a_3).$$

Dann ist die Diskriminante von f gegeben als $\Delta(f) = \delta^2$. Weiter erhält man für jedes Element $\varphi \in \mathrm{Gal}(f) \subseteq S(\{a_1, a_2, a_3\})$ der Galoisgruppe:

$$\varphi(\delta) \;=\; (\varphi(a_1) - \varphi(a_2))(\varphi(a_1) - \varphi(a_3))(\varphi(a_2) - \varphi(a_3)) \;=\; \mathrm{sg}(\varphi) \cdot \delta.$$

Gilt $\mathrm{Gal}(f) \cong \mathbb{Z}/3\mathbb{Z}$, so besteht $\mathrm{Gal}(f)$ aus geraden Permutationen, und es folgt $\varphi(\delta) = \delta$ für jedes $\varphi \in \mathrm{Gal}(f)$. Da $k \subseteq \mathbb{K}$ der Fixkörper von $\mathrm{Gal}(f)$ ist, erhalten wir $\delta \in k$. Somit besitzt $\Delta(f)$ in δ eine Quadratwurzel in k.

Gilt $\mathrm{Gal}(f) \cong S_3$, so besitzt $\mathrm{Gal}(f)$ auch ungerade Permutationen. Wie oben folgt $\delta \notin k$, und damit auch $-\delta \notin k$ Folglich kann $\Delta(f)$ keine Quadratwurzel in k besitzen. □

Beispiel 10.3.13. Die Polynome $T^3 - 3T + 1$ und $T^3 - 7T + 7$ aus $\mathbb{Q}[T]$ besitzen jeweils die Galoisgruppe $\mathbb{Z}/3\mathbb{Z}$. Das Polynom $T^3 - 2 \in \mathbb{Q}[T]$ besitzt die Galoisgruppe S_3.

Aufgaben zu Abschnitt 10.3.

Aufgabe 10.3.14. Zeige, dass die Aussagen von Bemerkung 10.3.11 und Satz 10.3.12 auch unter der schwächeren Voraussetzung $\mathrm{Char}(k) \neq 2, 3$ gelten.

11. Auflösbarkeit der Gleichungen

11.1. **Symmetrische Funktionen.**

Beispiel 11.1.1. Ein Polynom f in den Variablen T_1, T_2 nennt man *symmetrisch*, falls $f(T_1, T_2) = f(T_2, T_1)$ gilt. Beispiele sind etwa die Polynome $T_1 + T_2$ und $T_1 T_2$.

Bemerkung 11.1.2. Es bezeichne S_n die symmetrische Gruppe über $\{1, \ldots, n\}$, und es sei $\mathbb{K}$ ein Körper. Jedes Element $\sigma \in S_n$ definiert einen Ringautomorphismus

$$\begin{aligned} \sigma^\circ \colon \mathbb{K}[T_1, \ldots, T_n] &\to \mathbb{K}[T_1, \ldots, T_n], \\ \sum a_{\nu_1,\ldots,\nu_n} T_1^{\nu_1} \cdots T_n^{\nu_n} &\mapsto \sum a_{\nu_1,\ldots,\nu_n} T_{\sigma(1)}^{\nu_1} \cdots T_{\sigma(n)}^{\nu_n} \\ &= \sum a_{\nu_1,\ldots,\nu_n} T_1^{\nu_{\sigma^{-1}(1)}} \cdots T_n^{\nu_{\sigma^{-1}(n)}}. \end{aligned}$$

Nach der universellen Eigenschaft des Polynomrings ist σ° bereits definiert durch $\sigma^\circ(T_i) = T_{\sigma(i)}$. Damit erhalten wir

$$(\tau \circ \sigma)^\circ \;=\; \tau^\circ \circ \sigma^\circ, \qquad \sigma \neq \tau \implies \sigma^\circ \neq \tau^\circ \qquad \text{für je zwei } \tau, \sigma \in S_n.$$

Durch $\sigma \mapsto \sigma^\circ$ wird also ein Monomorphismus $S_n \to \mathrm{Aut}(\mathbb{K}[T_1, \ldots, T_n])$ in die Gruppe der Ringautomorphismen von $\mathbb{K}[T_1, \ldots, T_n]$ definiert.

Jeder Ringautomorphismus σ° besitzt eine eindeutige Fortsetzung auf den Quotientenkörper; diese ist explizit gegeben durch.

$$\sigma^\circ \colon \mathbb{K}(T_1, \ldots, T_n) \;\to\; \mathbb{K}(T_1, \ldots, T_n), \qquad \frac{f}{g} \;\mapsto\; \frac{\sigma^\circ(f)}{\sigma^\circ(g)}.$$

Wie vorhin wird durch $\sigma \mapsto \sigma^\circ$ wird ein Monomorphismus $S_n \to \mathrm{Aut}(\mathbb{K}(T_1, \ldots, T_n))$ in die Gruppe der Körperautomorphismen von $\mathbb{K}[T_1, \ldots, T_n]$ definiert.

Definition 11.1.3. Es sei $\mathbb{K}$ ein Körper. Der *Körper der symmetrischen Funktionen* über $\mathbb{K}$ in den Variablen $T_1, \ldots, T_n$ ist der Fixkörper

$$\mathbb{SF}_n \;:=\; \mathbb{K}(T_1, \ldots, T_n)^{S_n} \;\subseteq\; \mathbb{K}(T_1, \ldots, T_n).$$

Der Ring der *symmetrischen Polynome* ist der Unterring

$$\mathbb{SP}_n \;:=\; \mathbb{K}[T_1, \ldots, T_n]^{S_n} \;=\; \mathbb{SF}_n \cap \mathbb{K}[T_1, \ldots, T_n].$$

Bemerkung 11.1.4. Es sei $\mathbb{L} := \mathbb{K}(T_1, \ldots T_n)$. Jeder Automorphismus $\sigma^\circ \colon \mathbb{L} \to \mathbb{L}$ besitzt eine eindeutige Fortsetzung auf den Polynomring

$$\varrho_\sigma^\circ \colon \mathbb{L}[S] \;\to\; \mathbb{L}[S], \qquad \sum f_i S^i \;\mapsto\; \sum \sigma^\circ(f_i) S^i.$$

Damit gewinnt man Beispiele für symmetrische Funktionen: Man betrachtet das Polynom

$$F \;:=\; \prod_{i=1}^{n} (S - T_i) \;=\; \sum_{i=0}^{n} (-1)^i s_{n-i} S^i \;\in\; \mathbb{L}[S].$$

Es gilt $\varrho_\sigma^\circ(F) = F$, wie die folgende Rechnung zeigt:

$$\prod_{i=1}^{n} (S - T_i) \;=\; \prod_{i=1}^{n} (S - \sigma^\circ(T_i)) \;=\; \varrho_\sigma^\circ \left(\prod_{i=1}^{n} (S - T_i) \right).$$

In der Summendarstellung von F bedeutet das

$$\sum_{i=0}^{n} (-1)^i s_{n-i} S^i \;=\; \varrho_\sigma^\circ \left(\sum_{i=0}^{n} (-1)^i s_{n-i} S^i \right) \;=\; \sum_{i=0}^{n} (-1)^i \sigma^\circ(s_{n-i}) S^i.$$

Die Koeffizienten von F, und somit auch die Elemente $s_j \in \mathbb{L}$ sind also symmetrische Funktionen. Durch Ausmultiplizieren erhält man

$$\begin{aligned} s_0 &= 1, \\ s_1 &= T_1 + \ldots + T_n, \\ &\vdots \\ s_j &= \sum_{i_1<\ldots<i_j} T_{i_1} \cdots T_{i_j} \\ &\vdots \\ s_n &= T_1 \cdots T_n. \end{aligned}$$

Definition 11.1.5. Man nennt $s_0, \ldots, s_n \in \mathbb{K}[T_1, \ldots, T_n]$ aus Bemerkung 11.1.4 die *elementarsymmetrischen Funktionen* in den Variablen $T_1, \ldots, T_n$ über $\mathbb{K}$.

Satz 11.1.6. *Es seien $\mathbb{K}$ ein Körper, $\mathbb{SF}_n \subseteq \mathbb{K}(T_1, \ldots, T_n)$ der Körper der symmetrischen Funktionen und $s_0, \ldots, s_n \in \mathbb{SP}_n$ die elementarsymmetrischen Funktionen.*

(i) *Der Körper $\mathbb{SF}_n$ der symmetrischen Funktionen wird durch die elementarsymmetrischen Funktionen erzeugt:*

$$\mathbb{SF}_n \;=\; \mathbb{K}(s_1, \ldots, s_n).$$

(ii) *Die Erweiterung $\mathbb{SF}_n \subseteq \mathbb{K}(T_1, \ldots, T_n)$ ist Zerfällungskörper des separablen Polynoms*

$$F \;:=\; \prod_{i=1}^{n}(S - T_i) \;=\; \sum_{i=1}^{n}(-1)^i s_{n-i} S^i \;\in\; \mathbb{SF}_n[S].$$

(iii) *Die Erweiterung $\mathbb{SF}_n \subset \mathbb{K}(T_1, \ldots, T_n)$ ist galoissch, und man hat einen kanonischen Isomorphismus*

$$S_n \;\to\; \mathrm{Aut}(\mathbb{K}(T_1, \ldots, T_n), \mathbb{SF}_n), \qquad \sigma \;\mapsto\; \sigma^\circ.$$

Insbesondere ist der Grad der Erweiterung $\mathbb{SF}_n \subseteq \mathbb{K}(T_1, \ldots, T_n)$ gegeben durch

$$[\mathbb{K}(T_1, \ldots, T_n) : \mathbb{SF}_n] \;=\; n!.$$

Beweis. Wir betrachten zunächst den von den elementarsymmetrischen Funktionen erzeugten Körper $\mathbb{SF}'_n := \mathbb{K}(s_1, \ldots, s_n)$. Damit gilt

$$F \;=\; \prod_{i=1}^{n}(S - T_i) \;=\; \sum_{i=0}^{n}(-1)^i s_{n-i} S^i \;\in\; \mathbb{SF}'_n[S].$$

Das Polynom F ist separabel und $\mathbb{SF}'_n \subseteq \mathbb{K}(T_1, \ldots, T_n)$ ist ein Zerfällungskörper für F. Nach Satz 8.3.3 ist $\mathbb{SF}'_n \subseteq \mathbb{K}(T_1, \ldots, T_n)$ eine Galoiserweiterung. Mit Bemerkung 11.1.2 und Satz 10.1.3 erhalten wir:

$$\begin{aligned} n! &= |S_n| \\ &\leq |\mathrm{Aut}(\mathbb{K}(T_1, \ldots, T_n), \mathbb{SF}_n)| \\ &\leq |\mathrm{Aut}(\mathbb{K}(T_1, \ldots, T_n), \mathbb{SF}'_n)| \\ &\leq n!. \end{aligned}$$

Folglich muss überall Gleichheit herrschen. Das impliziert bereits $\mathbb{SF}'_n = \mathbb{SF}_n$, denn der Hauptsatz der Galoistheorie liefert

$$[\mathbb{SF}_n : \mathbb{SF}'_n] \;=\; [\mathrm{Aut}(\mathbb{K}(T_1, \ldots, T_n), \mathbb{SF}'_n) : \mathrm{Aut}(\mathbb{K}(T_1, \ldots, T_n), \mathbb{SF}_n)] \;=\; 1.$$

Mit $\mathbb{SF}_n = \mathbb{SF}'_n$ erhalten wir sofort die Aussagen (i), (ii) und (iii). □

Folgerung 11.1.7. *Jede endliche Gruppe ist isomorph zu der Galoisgruppe einer galoisschen Körpererweiterung.*

Beweis. Es sei G eine endliche Gruppe. Nach dem Satz von Cayley ist G isomorph zu einer Untergruppe von S_n, wobei man $n = |G|$ wählen kann. Es seien nun k ein Körper und $\mathbb{K} := k(T_1, \ldots, T_n)$. Nach Satz 11.1.6 (iii) ist G dann isomorph zu einer Untergruppe von $\mathrm{Aut}(\mathbb{K}, k)$ der Galoiserweiterung $k \subseteq \mathbb{K}$. Nach dem Hauptsatz der Galoistheorie liefert $\mathbb{L} := \mathbb{K}^G$ die gewünschte Erweiterung $\mathbb{L} \subseteq \mathbb{K}$. □

Satz 11.1.8. *Es seien $\mathbb{K}$ ein Körper, $\mathbb{SP}_n \subseteq \mathbb{K}[T_1, \ldots, T_n]$ der Ring der symmetrischen Polynome und $s_0, \ldots, s_n \in \mathbb{SP}_n$ die elementarsymmetrischen Funktionen. Dann gilt*

(i) $\mathbb{SP}_n = \mathbb{K}[s_1, \ldots, s_n]$
(ii) $\{s_1, \ldots, s_n\}$ *ist algebraisch unabhängig über* $\mathbb{K}$.

Insbesondere besitzt jedes symmetrische Polynom $f \in \mathbb{SP}_n$ eine eindeutige Darstellung

$$f \quad = \quad g(s_1, \ldots, s_n) \text{ mit } g \in \mathbb{K}[T_1, \ldots, T_n].$$

Erinnerung 11.1.9. Es sei $n \in \mathbb{Z}_{\geq 1}$. Die *lexikographische Ordnung* auf $\mathbb{Z}^n_{\geq 0}$ ist definiert durch

$$\nu < \nu' \iff \text{es gibt ein } 1 \leq k \leq n \text{ mit } \nu_k < \nu_k \text{ und } \nu_i = \nu'_i \text{ für } 1 \leq i \leq k-1.$$

Definition 11.1.10. Es seien $\mathbb{K}$ ein Körper und $f = \sum a_\nu T^\nu \in \mathbb{K}[T_1, \ldots, T_n]$.

(i) Der *lexikographische Grad* von f ist definiert als

$$\mathrm{lexdeg}(f) \quad := \quad \max(\nu \in \mathbb{Z}^n_{\geq 0};\ a_\nu \neq 0).$$

(ii) Für $f \neq 0$ ist der *Totalgrad* von f definiert als

$$\deg(f) \quad := \quad \max(\nu_1 + \ldots + \nu_n;\ \nu \in \mathbb{Z}^n_{\geq 0};\ a_\nu \neq 0).$$

Lemma 11.1.11. *Es seien $f \in \mathbb{SP}_n$ ein symmetrisches Polynom und $\mu := \mathrm{lexdeg}(f) \in \mathbb{Z}^n_{\geq 0}$. Dann gilt $\mu_1 \geq \mu_2 \geq \ldots \geq \mu_n$.*

Beweis. $f = \sum a_\nu T^\nu \in k[T_1, \ldots, T_n]$. Da f symmetrisch ist, erhalten wir

$$\begin{aligned} a_{(\mu_1,\mu_2,\mu_3,\mu_4,\mu_5,\ldots,\mu_n)} &\neq 0, \\ a_{(\mu_2,\mu_1,\mu_3,\mu_4,\mu_5,\ldots,\mu_n)} &\neq 0, \\ a_{(\mu_1,\mu_3,\mu_2,\mu_4,\mu_5,\ldots,\mu_n)} &\neq 0, \\ a_{(\mu_1,\mu_2,\mu_4,\mu_3,\mu_5,\ldots,\mu_n)} &\neq 0, \\ &\vdots \end{aligned}$$

Vergleicht man die jeweiligen Indizes mit μ, so ergibt sich die Behauptung. □

Beispiel 11.1.12. Für die elementarsymmetrischen Funktionen $s_1, \ldots, s_n \in \mathbb{SP}_n$ gilt

$$\mathrm{lexdeg}(s_i) \quad = \quad (\underbrace{1, \ldots, 1}_{i\text{-mal}}, 0, \ldots, 0).$$

Lemma 11.1.13. *Sind $f, g \in \mathbb{K}[T_1, \ldots, T_n]$ zwei Polynome, so gilt*

$$\mathrm{lexdeg}(fg) \ = \ \mathrm{lexdeg}(f) + \mathrm{lexdeg}(g), \qquad \deg(fg) \ = \ \deg(f) + \deg(g).$$

Beweis von Satz 11.1.8. Zu (i). Es sei $f = \sum a_\nu T^\nu$, und es sei $\mu := \operatorname{lexdeg}(f) \in \mathbb{Z}^n_{\geq 0}$. Mit Lemma 11.1.11 erhalten wir ein symmetrisches Polynom

$$f_1 \quad := \quad a_\mu s_1^{\mu_1-\mu_2} s_2^{\mu_2-\mu_3} \cdots s_{n-1}^{\mu_{n-1}-\mu_n} s_n^{\mu_n}.$$

Nach Beispiel 11.1.12 und Lemma 11.1.13 erhalten wir für die Grade

$$\begin{aligned}
\operatorname{lexdeg}(f_1) &= (\mu_1-\mu_2)(1,0,\ldots,0) + (\mu_2-\mu_3)(1,1,0,\ldots,0) + \ldots + \mu_n(1,\ldots,1) \\
&= \mu, \\
&= \operatorname{lexdeg}(f), \\
\deg(f_1) &= (\mu_1-\mu_2) + (\mu_2-\mu_3)2 + \ldots + \mu_n n. \\
&= \sum \mu_i \\
&\leq \deg(f).
\end{aligned}$$

Für das symmetrische Polynom $f - f_1$ erhält man also

$$\operatorname{lexdeg}(f-f_1) \; < \; \operatorname{lexdeg}(f), \qquad \deg(f-f_1) \; \leq \; \deg(f).$$

Durch wiederholen dieses Schrittes erhält man eine Folge symmetrischer Polynome strikt fallenden lexikographischen Grades:

$$f, \qquad f-f_1, \qquad f-f_1-f_2, \qquad \ldots \; .$$

Da diese Polynome vom Totalgrad beschränkt sind, landet man schließlich bei einem $f-f_1-\ldots-f_n$ vom lexikographischen Grad Null. Dieses ist trivial, was die gesuchte Darstellung für f liefert.

Zu (ii). Wir verwenden Induktion über n. Im Fall $n = 1$ haben wir $s_1 = T_1 \in \mathbb{K}(T_1)$, und dies ist ein transzendentes Element über $\mathbb{K}$.

Zum Induktionsschritt. Nehmen wir an, $\{s_1, \ldots, s_n\}$ sei algebraisch abhängig. Dann gibt es ein Polynom $g \in \mathbb{K}[T_1, \ldots, T_n]$ mit

$$g(s_1, \ldots, s_n) \quad = \quad 0.$$

Wir wollen dieses g so wählen, dass sein Grad $d := \deg(g)$ minimal ist. Durch Sortieren nach der letzten Variablen erhalten wir eine Darstellung

$$g \; = \; g_d T_n^d + \ldots + g_1 T_n + g_0, \qquad g_i \in \mathbb{K}[T_1, \ldots, T_{n-1}].$$

Dabei muss $g_0 \neq 0$ gelten, denn sonst hätte man eine Darstellung $g = g' T_n$, wobei $g' \in \mathbb{K}[T_1, \ldots, T_n]$ die Elemente $s_1, \ldots, s_n$ annuliert; Widerspruch zur Wahl von g. Einsetzen der elementarsymmetrischen Funktionen ergibt

$$0 \; = \; g_d(s_1, \ldots, s_{n-1}) s_n^d + \ldots + g_1(s_1, \ldots, s_{n-1}) s_n + g_0(s_1, \ldots, s_{n-1}) \; \in \; \mathbb{K}[T_1, \ldots, T_n].$$

Setzt man in dieser Relation die Variable T_n in den s_i zu Null, so führt dies zu der Relation

$$0 \quad = \quad g_0(r_1, \ldots, r_{n-1}),$$

wobei $r_1, \ldots, r_{n-1}$ die elementarsymmetrischen Funktionen in den $n-1$ Variablen $T_1, \ldots, T_{n-1}$ bezeichnen. Widerspruch zur Induktionsannahme. □

Aufgaben zu Abschnitt 11.1.

11.2. **Reine Polynome und Radikalerweiterungen.**

Definition 11.2.1. Es sei k ein Körper. Ein *reines Polynom über k* ist ein Element $f \in k[T]$ der Form

$$f \;=\; T^n - a, \qquad \text{wobei } n \in \mathbb{Z}_{\geq 1},\ a \in k.$$

Ist $k \subseteq \mathbb{K}$ eine Erweiterung, sodass $f = T^n - a$ über $\mathbb{K}$ in Linearfaktoren zerfällt, so nennt man die Nullstellen von f in $\mathbb{K}$ die *n-ten Wurzeln* von a.

Beispiel 11.2.2. Für $k = \mathbb{Q}$ und $\mathbb{K} = \mathbb{C}$ sind die dritten Wurzeln aus $2 \in k$ gegeben durch

$$\sqrt[3]{2}, \qquad \sqrt[3]{2}\cdot e^{\frac{2\pi i}{3}}, \qquad \sqrt[3]{2}\cdot e^{\frac{4\pi i}{3}}.$$

Bemerkung 11.2.3. Es seien k ein Körper und $n \in \mathbb{Z}_{\geq 1}$, sodass die Charakteristik $\mathrm{Char}(k)$ kein Teiler von n ist. Ist $f := T^n - a$ ein reines Polynom über k, so gilt

$$D(f) \;=\; nT^{n-1}.$$

Gilt $a \neq 0$, so besitzt f in jeder Erweiterung $k \subseteq \mathbb{K}$ nur einfache Nullstellen. Zerfällt f über $\mathbb{K}$ in Linearfaktoren, so besitzt a genau n verschiedene Wurzeln.

Bemerkung 11.2.4. Es seien $n \in \mathbb{Z}_{\geq 1}$ und k ein Körper, sodass $\mathrm{Char}(k)$ kein Teiler von n ist. Weiter sei $f = T^n - a$ ein reines Polynom über k mit $a \neq 0$, und $k \subseteq \mathbb{K}$ eine Erweiterung, sodass f über $\mathbb{K}$ in Linearfaktoren zerfällt.

(i) Sind $b_1, \ldots, b_n \in \mathbb{K}$ die n-ten Wurzeln aus a, so erhält man die n-ten Einheitswurzeln in $\mathbb{K}$ als

$$1 = \frac{b_1}{b_1},\ \zeta_2 = \frac{b_2}{b_1},\ \ldots,\ \zeta_n = \frac{b_n}{b_1}.$$

(ii) Sind $1, \zeta_2, \ldots, \zeta_n \in \mathbb{K}$ die n-ten Einheitswurzeln, und ist b_1 eine n-te Wurzel aus a, so erhält man die n-ten Wurzeln aus a als

$$b_1,\ b_1\zeta_2,\ \ldots,\ b_1\zeta_n.$$

Insbesondere enthält der Körper $\mathbb{K}$ die (paarweise verschiedenen) n-ten Einheitswurzeln $\zeta_1, \ldots, \zeta_n$ über k, und mit $k_n := k(\zeta_1, \ldots, \zeta_n)$ gilt für jede der n-ten Wurzeln $b_1, \ldots, b_n$ aus a:

$$k(b_1, \ldots, b_n) \;=\; k_n(b_i).$$

Satz 11.2.5. *Es seien $n \in \mathbb{Z}_{\geq 1}$ und k ein Körper, sodass* $\mathrm{Char}(k)$ *kein Teiler von n ist. Weiter sei $f = T^n - a$ ein reines Polynom über k mit $a \neq 0$, und es sei $k \subseteq \mathbb{K}$ ein Zerfällungskörper für f.*

(i) *Sind $\zeta_1, \ldots, \zeta_n \in \mathbb{K}$ die n-ten Einheitswurzeln und $k_n := k(\zeta_1, \ldots, \zeta_n)$, so hat man drei Galoiserweiterungen:*

$$k \subseteq k_n, \qquad k_n \subseteq \mathbb{K}, \qquad k \subseteq \mathbb{K}.$$

(ii) *Ist $\zeta \in \mathbb{K}$ eine primitive n-te Einheitswurzel und $b \in \mathbb{K}$ eine n-te Wurzel aus a, so hat man einen wohldefinierten Monomorphismus*

$$\Phi\colon \mathrm{Aut}(\mathbb{K}, k_n) \;\to\; \mathbb{Z}/n\mathbb{Z}, \quad \varphi \;\mapsto\; m + n\mathbb{Z}, \text{ wobei } \varphi(b) = \zeta^m b.$$

(iii) *Ist $T^n - a$ irreduzibel in $k_n[T]$, so ist $\Phi\colon \mathrm{Aut}(\mathbb{K}, k_n) \to \mathbb{Z}/n\mathbb{Z}$ ein Isomorphismus.*

Beweis. Zu (i). Als Zerfällungskörper des separablen Polyonoms $T^n - 1 \in k[T]$ ist $k \subseteq k_n$ galoissch, wie wir bereits in Bemerkung 9.1.14 gesehen haben. Da auch $T^n - a \in k[T]$ nach Bemerkung 11.2.3 separabel ist, liegt mit $k \subseteq \mathbb{K}$ ebenfalls eine Galoiserweiterung vor.

Um schließlich zu sehen, dass die Erweiterung $k_n \subseteq \mathbb{K}$ galoissch ist, kann man entweder Aussage (iii) des Hauptsatzes der Galoistheorie anwenden, oder man verwendet die Tatsache, dass $k_n \subseteq \mathbb{K}$ Zerfällungskörper des separablen Polynoms $T^n - a \in k_n[T]$ ist.

Zu (ii). Nach Bemerkung 11.2.4 gibt es n verschiedene n-te Wurzeln aus a, und diese sind gegeben als $\zeta^m b$, wobei $m = 0, \ldots n-1$. Für jedes $\varphi \in \operatorname{Aut}(\mathbb{K}, k_n)$ gilt

$$\varphi(b)^n \;=\; \varphi(b^n) \;=\; \varphi(a) \;=\; a.$$

Folglich hat man eine eindeutige Darstellung $\varphi(b) = \zeta^m b$ mit $0 \leq m \leq n-1$. Die Abbildung Φ ist daher wohldefiniert. Wegen $\mathbb{K} = k_n(b)$ ist sie weiter injektiv.

Die Homomorphieeigenschaft ergibt sich wie folgt: Gilt $\varphi(b) = \zeta^m b$ und $\psi(b) = \zeta^l b$ für $\varphi, \psi \in \operatorname{Aut}(\mathbb{K}, k_n)$, so erhält man

$$\psi \circ \varphi(b) \;=\; \psi(\zeta^m b) \;=\; \zeta^m \psi(b) \;=\; \zeta^m \zeta^l b \;=\; \zeta^{m+l} b.$$

Zu (iii). Ist $T^n - a$ irreduzibel in $k_n[T]$, so ist es das Minimalpolynom von b über k_n. Wegen $\mathbb{K} = k_n(b)$ folgt $[\mathbb{K} : k_n] = n$. Der Hauptsatz der Galoistheorie liefert, dass $\operatorname{Aut}(\mathbb{K}, k_n)$ die Ordnung n besitzt. Als Monomorphismus muss Φ dann schon surjektiv sein. □

Beispiel 11.2.6. Wir betrachten nocheinmal das reine Polynom $f := T^3 - 2 \in \mathbb{Q}[T]$. Seine Nullstellen in $\mathbb{C}$ sind

$$b_0 := \sqrt[3]{2}, \quad b_1 := \sqrt[3]{2}\zeta, \quad b_2 := \sqrt[3]{2}\zeta^2, \quad \text{wobei } \zeta := e^{\frac{2\pi i}{3}}.$$

Mit $\mathbb{K} := \mathbb{Q}(\sqrt[3]{2}, \zeta) \subseteq \mathbb{C}$ erhalten wir also einen Zerfällungskörper für $f = T^3 - 2$. Dieser enthält $\mathbb{Q}_3 = \mathbb{Q}(\zeta)$.

Wir wollen uns nun die einzelnen Galoisgruppen näher anschauen. Zunächst liefert Satz 10.1.10 einen Isomorphismus

$$\operatorname{Gal}(f) \;=\; \operatorname{Aut}(\mathbb{K}, \mathbb{Q}) \;\cong\; S(\{b_0, b_1, b_2\}) \;\cong\; S_3.$$

Die Elemente der Galoisgruppe $\operatorname{Aut}(\mathbb{K}, \mathbb{Q})$ entsprechen also genau den Permutationen der Nullstellenmenge $\{b_0, b_1, b_2\}$ von f.

Weiter ist $\mathbb{Q} \subseteq \mathbb{Q}_3$ nach Folgerung 9.2.11 eine Erweiterung vom Grad $\varphi(3) = 2$, und ihre Automorphismengruppe ist

$$\operatorname{Aut}(\mathbb{Q}_3, \mathbb{Q}) \;=\; \{\mathrm{id}_{\mathbb{Q}_3}, \kappa\} \qquad \text{mit } \kappa_0 \colon \zeta \mapsto \zeta^2.$$

Das Element $\kappa_0 \colon \mathbb{Q}_3 \to \mathbb{Q}_3$ ist die Einschränkung der komplexen Konjugation; wir erhalten es auch als Einschränkung eines Automorphismus $\kappa \in \operatorname{Gal}(f)$:

$$\kappa \colon \mathbb{K} \to \mathbb{K}, \qquad b_0 \mapsto b_0, \quad b_1 \mapsto b_2, \quad b_2 \mapsto b_1.$$

Weiter ist $\mathbb{Q}_3 \subseteq \mathbb{K}$ nach Satz 11.2.5 eine Erweiterung vom Grad 3, die zugehörige Galoisgruppe $\operatorname{Aut}(\mathbb{K}, \mathbb{Q}_3)$ ist zyklisch von der Ordnung 3 und ist erzeugt durch

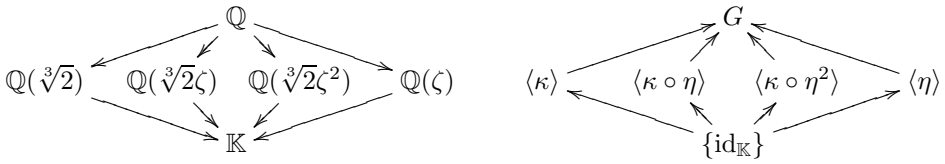
$$\eta \colon \mathbb{K} \to \mathbb{K}, \qquad b_0 \mapsto b_1, \quad b_1 \mapsto b_2, \quad b_2 \mapsto b_0.$$

Man beachte, dass η, wie jeder Automorphismus von $\mathbb{K}$, den Primkörper $\mathbb{Q} \subseteq \mathbb{K}$ elementweise festlässt, d.h., man hat $\eta \in \operatorname{Aut}(\mathbb{K}, \mathbb{Q})$.

Die Elemente κ und φ erzeugen $\operatorname{Aut}(\mathbb{K}, k)$; dies kann man leicht explizit prüfen, oder man kann Lemma 10.1.11 dafür heranziehen. Weiter gelten die Relationen

$$\kappa^2 \;=\; \mathrm{id}, \quad \eta^3 \;=\; \mathrm{id}, \quad \kappa \circ \eta \;=\; \eta^{-1} \circ \kappa.$$

Das allgemeine Element von $G := \mathrm{Aut}(\mathbb{K}, k)$ ist also von der Gestalt $\eta^j \circ \kappa^k$ mit $j = 0, 1, 2$ und $k = 0, 1$. Damit erhält man die gesamte Galoiskorrespondenz:



Folgerung 11.2.7. *Es seien $n \in \mathbb{Z}_{\geq 1}$ und k ein Körper, sodass $\mathrm{Char}(k)$ kein Teiler von n ist. Weiter seien $f = T^n - a$ ein reines Polynom über k mit Zerfällungskörper $k \subseteq \mathbb{K}$. Enthält k eine primitive n-te Einheitswurzel, so ist $\mathrm{Aut}(\mathbb{K}, k)$ zyklisch.*

Satz 11.2.8. *Es seien $n \in \mathbb{Z}_{\geq 1}$ und k ein Körper, sodass $\mathrm{Char}(k)$ kein Teiler von n ist und k eine primitive n-te Einheitswurzel enthält. Ist $k \subseteq \mathbb{K}$ eine Galoiserweiterung vom Grad n mit zyklischer Galoisgruppe $\mathrm{Aut}(\mathbb{K}, k)$, so ist $k \subseteq \mathbb{K}$ Zerfällungskörper eines reinen Polynoms $T^n - a$ über k.*

Beweis. Es sei $\zeta \in k$ eine primitive n-te Einheitswurzel, und es sei $\varphi \in \mathrm{Aut}(\mathbb{K}, k)$ ein erzeugendes Element. Wegen

$$|\mathrm{Aut}(\mathbb{K}, k)| \;=\; [\mathbb{K} : k] \;=\; n$$

sind $\mathrm{id}, \varphi, \ldots, \varphi^{n-1}$ paarweise verschieden, und somit linear unabhängig in dem $\mathbb{K}$-Vektorraum $\mathrm{Abb}(\mathbb{K}, \mathbb{K})$, siehe Folgerung 8.1.9. Insbesondere gilt

$$b \;:=\; s + \zeta\varphi(s) + \ldots + \zeta^{n-1}\varphi^{n-1}(s) \;\neq\; 0$$

mit einem geeigneten Element $s \in \mathbb{K}$. Anwenden von φ auf diese Gleichung ergibt

$$\varphi(b) \;=\; \varphi(s) + \zeta\varphi^2(s) + \ldots + \zeta^{n-2}\varphi^{n-1}(s) + \zeta^{n-1}s \;=\; \zeta^{-1}b.$$

Das impliziert $\varphi(b^n) = b^n$, und mit $G := \mathrm{Aut}(\mathbb{K}, k)$ erhalten wir $b^n \in \mathbb{K}^G$. Nach dem Hauptsatz der Galoistheorie gilt $\mathbb{K}^G = k$ und somit haben wir $a := b^n \in k$.

Wir wollen nun zeigen, dass $k \subseteq \mathbb{K}$ Zerfällungskörper von $T^n - a$ ist. Dafür genügt es, $\mathbb{K} = k(b)$ nachzuweisen. Wegen $\varphi^m(b) = \zeta^{-m}b$ sind $\mathrm{id}, \varphi, \ldots, \varphi^{n-1}$ paarweise verschieden auf $k(b)$. Nach Lemma 8.1.10 besitzt $k \subseteq k(b)$ mindestens den Grad n, was $k(b) = \mathbb{K}$ impliziert. □

Definition 11.2.9. Eine Körpererweiterung $k \subseteq \mathbb{K}$ heisst *Radikalerweiterung*, falls sie eine Kette

$$k = \mathbb{L}_0 \;\subseteq\; \mathbb{L}_1 \;\subseteq\; \ldots \;\subseteq\; \mathbb{L}_r = \mathbb{K}$$

von Zwischenkörpern erlaubt, wobei $\mathbb{L}_{i+1} = \mathbb{L}_i(b_i)$ mit einer n_i-ten Wurzel $b_i \in \mathbb{L}_{i+1}$ eines Elementes aus $\mathbb{L}_i$.

Satz 11.2.10. *Es sei k ein Körper der Charakeristik Null, und es sei $k \subseteq \mathbb{K}$ eine Radikalerweiterung. Dann gibt es eine Körpererweiterung $\mathbb{K} \subseteq \mathbb{K}'$, sodass $k \subseteq \mathbb{K}'$ eine galoissche Radikalerweiterung ist.*

Beweis. Wir beweisen die Aussage durch Induktion über $r := [\mathbb{K} : k]$. Im Falle $r = 1$ besitzt $\mathbb{K}' := \mathbb{K} = k$ die gewünschten Eigenschaften.

Kommen wir zum Induktionsschritt, d.h., wir nehmen an die Behauptung gelte für alle $1 \leq s < r$ und schließen daraus, dass sie auch für r gilt.

Nach Definition der Radikalerweiterung gibt es einen Zwischenkörper $k \subseteq \mathbb{L} \subsetneq \mathbb{K}$ sodass $k \subseteq \mathbb{L}$ Radikalerweiterung ist und $\mathbb{K} = \mathbb{L}(b)$ mit einer n-ten Wurzel $b \in \mathbb{K}$ aus einem Element aus $\mathbb{L}$ gilt.

Wegen $[\mathbb{L} : k] < r$ gibt es eine Erweiterung $\mathbb{L} \subseteq \mathbb{L}'$, sodass $k \subseteq \mathbb{L}'$ eine galoissche Radikalerweiterung ist. Insbesondere ist $k \subseteq \mathbb{L}'$ damit Zerfällungskörper eines Polynoms $f \in k[T]$. Wir setzen $G := \operatorname{Aut}(\mathbb{L}', k)$ und betrachten weiter

$$g \ := \ \prod_{\varphi \in G} (T^n - \varphi(b)^n) \ = \ \mathbb{L}'[T].$$

Für $\psi \in G$ sei $\overline{\psi}\colon \mathbb{L}'[T] \to \mathbb{L}'[T]$ die kanonische Fortsetzung. Dann gilt $\overline{\psi}(g) = g$. Folglich sind die Koeffizienten von g invariant unter ψ und liegen somit in $(\mathbb{L}')^G = k$. Mit anderen Worten: Es gilt $g \in k[T]$.

Es sei nun $\mathbb{L}' \subseteq \mathbb{K}'$ ein Zerfällungskörper für g. Wegen $g(b) = 0$ dürfen wir dabei $b \in \mathbb{K}'$ und somit $\mathbb{K} = \mathbb{L}(b) \subseteq \mathbb{K}'$ annehmen. Nun ist $k \subseteq \mathbb{K}'$ Zerfällungskörper für $fg \in k[T]$. Somit ist $k \subseteq \mathbb{K}'$ galoissch.

Es bleibt zu zeigen, dass $k \subseteq \mathbb{K}'$ eine Radikalerweiterung ist. Da $k \subseteq \mathbb{L}'$ Radikalerweiterung ist, genügt es, zu zeigen, dass $\mathbb{L}' \subseteq \mathbb{K}'$ Radikalerweiterung ist. Das ist jedoch klar nach Konstruktion: Als Zerfällungskörper von g ist $\mathbb{L}' \subseteq \mathbb{K}'$ von der Form $\mathbb{L}' \subseteq \mathbb{L}'(b_1, \ldots, b_m)$ mit den Nullstellen von g. Diese sind n-te Wurzeln von Elementen aus $\mathbb{L}'$. □

Aufgaben zu Abschnitt 11.2.

11.3. **Auflösbarkeit von Gleichungen.**

Problem 11.3.1. Wir suchen nach einer Formel für die möglichen komplexen Lösungen x der Gleichung

$$a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \;=\; 0, \qquad a_n, \ldots, a_0 \in \mathbb{C},\ a_n \neq 0. \tag{11.1}$$

Beispiel 11.3.2. Für $n = 2$ besitzt die Gleichung (11.1) je nach Koeffizienten genau eine oder genau zwei Lösungen, nämlich

$$x_{1,2} \;=\; \frac{-a_1 \pm \sqrt{a_1^2 - 4a_2a_0}}{2a_2}.$$

Beispiel 11.3.3 (S. Del Ferro / N. Fontana (1515), G. Cardano (1545))**.** Für $n = 3$ kann man die Lösungen der Gleichung (11.1) explizit bestimmen:

In einem ersten Schritt substituiert man $x = y - a_2/3a_3$ und erhält die zu (11.1) äquivalente Gleichung

$$y^3 + 3py + 2q \;=\; 0 \quad \text{mit} \quad p \;=\; \frac{3a_1a_3 - a_2^2}{9a_3^2}, \quad q \;=\; \frac{27a_0a_3^2 + 9a_1a_2a_3 + 2a_2^3}{54a_3^3}.$$

In einem zweiten Schritt löst man die neue Gleichung mittels Wurzelziehen in den komplexen Zahlen. Mit

$$\zeta \;:=\; e^{\frac{2\pi i}{3}}, \quad u \;:=\; \sqrt[3]{-q + \sqrt{q^2 + p^3}}, \quad v \;:=\; \sqrt[3]{-q - \sqrt{q^2 + p^3}},$$

wobei die dritten Wurzel mit der Bedingung $uv = -p$ zu wählen sind, erhält man als mögliche Lösungen der transformierten Gleichung als

$$u + v, \qquad \zeta u + \zeta^2 v, \qquad \zeta^2 u + \zeta v.$$

Daraus lassen sich dann die Lösungen der ursprünglichen Gleichung bestimmen. Je nach Koeffizienten erhält man eine, zwei oder drei Lösungen.

Beispiel 11.3.4 (L. Ferrari (1540))**.** Für $n = 4$ kann man die Lösungen der Gleichung (11.1) explizit bestimmen:

In einem ersten Schritt substituiert man $x = y - a_3/4a_4$, und erhält damit eine zu (11.1) äquivalente Gleichung der Form

$$y^4 + py^2 + qy + r \;=\; 0. \tag{11.2}$$

Um diese zu lösen betrachtet man zunächst die zugehörige *kubische Resolvente*, d.h., die Gleichung

$$z^3 + 2pz^2 + (p^2 - 4r)z + q^2 \;=\; 0. \tag{11.3}$$

Deren Lösungen z_1, z_2 und z_3 lassen sich, wie vorhin erläutert, explizit bestimmen. Die Lösungen von (11.2) sind dann

$$\begin{aligned}
y_1 &= \frac{1}{2}\left(\sqrt{-z_1} + \sqrt{-z_2} + \sqrt{-z_3}\right),\\
y_2 &= \frac{1}{2}\left(\sqrt{-z_1} - \sqrt{-z_2} - \sqrt{-z_3}\right),\\
y_3 &= \frac{1}{2}\left(-\sqrt{-z_1} + \sqrt{-z_2} - \sqrt{-z_3}\right),\\
y_4 &= \frac{1}{2}\left(-\sqrt{-z_1} - \sqrt{-z_2} + \sqrt{-z_3}\right),
\end{aligned}$$

wobei die Quadratwurzeln so zu wählen sind, dass $\sqrt{-z_1}\sqrt{-z_2}\sqrt{-z_3} = -q$ gilt. Daraus lassen sich dann die Lösungen der ursprünglichen Gleichung gewinnen.

Definition 11.3.5. Es sei k ein Körper und $f \in k[T]$. Man nennt die Gleichung $f(x) = 0$ *durch Radikale auflösbar*, falls es eine Radikalerweiterung $k \subset \mathbb{K}$ gibt, sodass f über $\mathbb{K}$ in Linearfaktoren zerfällt.

Bemerkung 11.3.6. Mit Hilfe der oben angeführten Lösungsverfahren sieht man, dass die Gleichung (11.1) für $n \leq 4$ durch Radikale auflösbar ist.

Satz 11.3.7. *Es seien k ein Körper der Charakteristik Null und $f \in k[T]$ ein nicht konstantes Polynom. Dann sind folgende Aussagen äquivalent:*

(i) *Die Gleichung $f(x) = 0$ ist durch Radikale auflösbar.*
(ii) *Die Galoisgruppe $\mathrm{Gal}(f)$ der Gleichung $f(x) = 0$ ist auflösbar.*

Folgerung 11.3.8. *Es sei k ein Körper der Charakteristik Null. Für $n = 1, 2, 3, 4$ ist jede Gleichung n-ten Grades über k durch Radikale auflösbar.*

Beweis. Es sei $f(x) = 0$ eine Gleichung vom Grad höchstens vier. Es ist zu zeigen, dass $\mathrm{Gal}(f)$ eine auflösbare Gruppe ist. Nach Satz 10.1.3 haben wir einen Monomorphismus $\mathrm{Gal}(f) \to S_n$, wobei $n \leq 4$. Da S_n für $n \leq 4$ eine auflösbare Gruppe ist, siehe Folgerung 2.4.13 und Untergruppen auflösbarer Gruppen wieder auflösbar sind, ergibt sich die Behauptung. □

Folgerung 11.3.9. *Die Gleichung $x^5 - 4x + 2 = 0$ über $\mathbb{Q}$ ist nicht durch Radikale auflösbar.*

Beweis. Eine Kurvendiskussion ergibt, dass $f(x) = x^5 - 4x + 2$ genau drei reelle Nullstellen besitzt. Somit liefert Satz 10.1.10, dass $\mathrm{Gal}(f) \cong S_5$ gilt. Nach Folgerung 2.4.13 ist S_5 nicht auflösbar. Also liefert Satz 11.3.7 die Behauptung. □

Definition 11.3.10. Es seien n eine natürliche Zahl, k ein Körper, $\mathbb{L} := k(T_1, \ldots, T_n)$ der Körper der rationalen Funktionen und $s_0, \ldots, s_n \in \mathbb{L}$ die elementarsymmetrischen Funktionen. Die *allgemeine Gleichung n-ten Grades über k* ist

$$\prod_{i=1}^{n}(x - T_i) \;=\; \sum_{i=0}^{n}(-1)^i s_{n-i} x^i \;=\; 0.$$

Folgerung 11.3.11. *Es sei k ein Körper der Charakteristik Null. Dann ist die allgemeine Gleichung n-ten Grades für $n \geq 5$ nicht durch Radikale auflösbar.*

Beweis. Nach Satz 11.1.6 besitzt die allgemeine Gleichung n-ten Grades die Galoisgruppe S_n. Diese ist nach Folgerung 2.4.13 für $n \geq 5$ nicht auflösbar. Satz 11.3.7 liefert daher die Behauptung. □

Folgerung 11.3.12. *Sind $a_0, \ldots, a_{n-1} \in \mathbb{C}$ algebraisch unabhängig über $\mathbb{Q}$, so ist die Gleichung $x^n + a_{n-1} + \ldots + a_1 x + a_0 = 0$ nicht durch Radikale auflösbar.*

Beweis. Da die elementarsymmetrischen Funktionen $s_1, \ldots, s_n$ eine algebraisch unabhängige Familie über $\mathbb{Q}$ bilden, erhält man ein kommutatives Diagramm von Körperisomorphismen

$$\begin{array}{ccc} & \mathbb{Q}(T_1, \ldots, T_n) & \\ \swarrow & & \searrow \\ \mathbb{Q}(-s_1, \ldots, (-1)^n s_n) & \longleftrightarrow & \mathbb{Q}(a_{n-1}, \ldots, a_0) \end{array}$$

Dabei wird $x^n + a_{n-1} + \ldots + a_1 x + a_0 = 0$ in die allgemeine Gleichung n-ten Grades überführt. Die Behauptung ergibt sich daher aus Folgerung 11.3.11. □

Lemma 11.3.13. *Es sei $\pi\colon G \to H$ ein Epimorphismus von Gruppen. Ist G auflösbar, so ist auch H auflösbar.*

Beweis. Wir wählen eine Normalreihe mit abelschen Faktoren in G:

$$G = G_0 \trianglerighteq G_1 \trianglerighteq \ldots \trianglerighteq G_{n-1} \trianglerighteq G_n = \{e_G\}.$$

Daraus erhält man eine Normalreihe mit abelschen Faktoren in H:

$$H = \pi(G_0) \trianglerighteq H_1 = \pi(G_1) \trianglerighteq \ldots \trianglerighteq H_{n-1} = \pi(G_{n-1}) \trianglerighteq H_n = \{e_H\}.$$

□

Lemma 11.3.14. *Es seien k ein Körper der Charakteristik Null, $k \subseteq \mathbb{K}$ eine Galoiserweiterung, $n \in \mathbb{Z}_{\geq 1}$ und $\zeta \in \overline{\mathbb{K}}$ eine primitive n-te Einheitswurzel. Dann sind auch $k \subseteq \mathbb{K}(\zeta)$ und $k(\zeta) \subseteq \mathbb{K}(\zeta)$ Galoiserweiterungen.*

Beweis. Als Galoiserweiterung ist $k \subseteq \mathbb{K}$ Zerfällungskörper eines Polynoms $f \in k[T]$. Somit ist $k \subseteq \mathbb{K}(\zeta)$ Zerfällungskörper von $f \cdot (T^n - 1)$ und daher galoissch. □

Beweis von Satz 11.3.7. Zur Implikation "(i) ⇒ (ii)". Es sei $k \subseteq \mathbb{K}$ eine Radikalerweiterung, sodass f über $\mathbb{K}$ in Linearfaktoren zerfällt. Nach Satz 11.2.10 dürfen wir annehmen, dass $k \subseteq \mathbb{K}$ eine Galoiserweiterung ist. Wir wählen nun eine Kette

$$k = \mathbb{L}_0 \subseteq \ldots \subseteq \mathbb{L}_r = \mathbb{K}$$

von Zwischenkörpern, wobei $\mathbb{L}_{i+1} = \mathbb{L}_i(b_i)$ mit einer n_i-ten Wurzel $b_i \in \mathbb{L}_{i+1}$ eines Elementes aus $\mathbb{L}_i$ gilt, d.h., wir haben $b^{n_i} \in \mathbb{L}_i$.

Wir setzen $n := n_0 \cdots n_{r-1}$ und wählen eine primitive n-te Einheitswurzel ζ über $\mathbb{K}$. Wir setzen weiter $k' := k(\zeta)$ und $\mathbb{L}'_i := \mathbb{L}_i(\zeta)$ sowie $\mathbb{K}' := \mathbb{K}(\zeta)$. Damit erhalten wir eine Kette von Körpererweiterungen:

$$k \subseteq k' = \mathbb{L}'_0 \subseteq \ldots \subseteq \mathbb{L}'_r = \mathbb{K}'$$

Wir betrachten nun die aus der Kette resultierende Schachtelung der zugehörigen Galoisgruppen:

$$\mathrm{Aut}(\mathbb{K}', k) \supseteq \mathrm{Aut}(\mathbb{K}', \mathbb{L}'_0) \supseteq \ldots \supseteq \mathrm{Aut}(\mathbb{K}', \mathbb{L}'_{r-1}) \supseteq \{\mathrm{id}_{\mathbb{K}'}\}.$$

Das Ziel ist es, zu zeigen, dass dies eine Normalreihe mit abelschen Faktoren für $\mathrm{Aut}(\mathbb{K}', k)$ ist.

Nach Lemma 11.3.14 ist $k \subseteq \mathbb{K}'$ eine Galoiserweiterung. Nach dem Hauptsatz der Galoistheorie ist dann auch jedes $\mathbb{L}'_i \subseteq \mathbb{K}'$ eine Galoiserweiterung.

Nach Bemerkung 9.1.14 ist $k \subseteq \mathbb{L}'_0$ eine Galoiserweiterung. Der Hauptsatz der Galoistheorie liefert somit

$$\mathrm{Aut}(\mathbb{K}', \mathbb{L}'_0) \trianglelefteq \mathrm{Aut}(\mathbb{K}', k), \qquad \mathrm{Aut}(\mathbb{K}', k)/\mathrm{Aut}(\mathbb{K}', \mathbb{L}'_0) \cong \mathrm{Aut}(\mathbb{L}'_0, k).$$

Letztere Gruppe ist nach Satz 9.1.15 abelsch. Somit ist der erste Faktor der Reihe eine abelsche Gruppe.

Um fortfahren zu können, müssen wir sehen, dass $\mathbb{L}'_i \subseteq \mathbb{L}'_{i+1}$ Zerfällungskörper von $T^{n_i} - b_i^{n_i} \in \mathbb{L}'_i[T]$ ist. Dies folgt aus der Tatsache, dass jedes $\mathbb{L}'_{i+1}$ mit ζ^{n/n_i} eine primitive n_i-te Einheitswurzel enthält und somit

$$\mathbb{L}'_{i+1} = \mathbb{L}_{i+1}(\zeta) = \mathbb{L}_i(b_i, \zeta) = \mathbb{L}'_i(b_i)$$

alle n_i Wurzeln aus $b_i^{n_i}$ enthält. Insbesondere ist die Erweiterung $\mathbb{L}'_i \subseteq \mathbb{L}'_{i+1}$ nach Satz 11.2.5 galoissch. Man kann wieder den Hauptsatz der Galoistheorie anwenden und erhält

$$\mathrm{Aut}(\mathbb{K}', \mathbb{L}'_{i+1}) \trianglelefteq \mathrm{Aut}(\mathbb{K}', \mathbb{L}'_i), \qquad \mathrm{Aut}(\mathbb{K}', \mathbb{L}'_{i+1})/\mathrm{Aut}(\mathbb{K}', \mathbb{L}'_i) \cong \mathrm{Aut}(\mathbb{L}'_{i+1}, \mathbb{L}'_i).$$

Letztere Gruppe ist nach Satz 11.2.5 zyklisch und somit abelsch. Das zeigt, dass die obige Reihe die gewünschten Eigenschaften besitzt; wir erhalten also, dass $\mathrm{Aut}(\mathbb{K}', k)$ eine auflösbare Gruppe ist.

Wir müssen nun für den Zerfällungskörper $k \subseteq \mathbb{L} \subseteq \mathbb{K}'$ von $f \in k[T]$ zeigen, dass $\mathrm{Aut}(\mathbb{L}, k)$ auflösbar ist. Zunächst vermerken wir, dass $k \subseteq \mathbb{L}$ wegen $\mathrm{Char}(k) = 0$ eine Galoiserweiterung ist. Nach dem Hauptsatz der Galoistheorie gilt deshalb

$$\mathrm{Aut}(\mathbb{K}', \mathbb{L}) \trianglelefteq \mathrm{Aut}(\mathbb{K}', k), \qquad \mathrm{Aut}(\mathbb{L}, k) \cong \mathrm{Aut}(\mathbb{K}', k)/\mathrm{Aut}(\mathbb{K}', \mathbb{L}).$$

Also ist $\mathrm{Aut}(\mathbb{L}, k)$ epimorphes Bild einer auflösbaren Gruppe und ist somit nach Lemma 11.3.13 auflösbar.

Zur Implikation "(ii) $\Rightarrow$ (i)". Es sei $k \subseteq \mathbb{K}$ der Zerfällungskörper von f, und es sei $G := \mathrm{Aut}(\mathbb{K}, k)$. Nach Voraussetzung ist G auflösbar. Satz 9.3.13 liefert eine Normalreihe

$$G = G_0 \trianglerighteq G_1 \trianglerighteq \ldots \trianglerighteq G_{m-1} \trianglerighteq G_m = \{e_G\}$$

in G, sodass jeder Faktor G_i/G_{i+1} eine zyklische Gruppe von Primzahlordnung ist. Aus dieser Normalreihe gewinnt man mit $\mathbb{L}_i := \mathbb{K}^{G_i}$ eine Kette von Unterkörpern

$$k = \mathbb{L}_0 \subseteq \mathbb{L}_1 \subseteq \ldots \subseteq \mathbb{L}_{m-1} \subseteq \mathbb{L}_m = \mathbb{K}.$$

Nach dem Hauptsatz der Galoistheorie ist dabei jede der Erweiterungen $\mathbb{L}_i \subseteq \mathbb{L}_{i+1}$ galoissch, und es gilt

$$\mathrm{Aut}(\mathbb{L}_{i+1}, \mathbb{L}_i) \cong G_{i+1}/G_i.$$

Insbesondere ist jede der Gruppen $\mathrm{Aut}(\mathbb{L}_{i+1}, \mathbb{L}_i)$ zyklisch, und ihre Ordnung ist ein Teiler von $n := |G|$.

Wir wählen nun eine primitive n-te Einheitswurzel ζ über k, und werden zeigen, dass $k \subseteq \mathbb{K}(\zeta)$ eine Radikalerweiterung ist. Dazu betrachten wir die folgende Kette von Körpererweiterungen

$$k \subseteq k(\zeta) = \mathbb{L}_0(\zeta) \subseteq \mathbb{L}_1(\zeta) \subseteq \ldots \subseteq \mathbb{L}_{m-1}(\zeta) \subseteq \mathbb{L}_m(\zeta) = \mathbb{K}(\zeta).$$

Wir müssen dann zeigen, dass jede Erweiterung $\mathbb{L}_i(\zeta) \subseteq \mathbb{L}_{i+1}(\zeta)$ Zerfällungskörper eines reinen Polynoms ist. Nach Satz 11.2.8 genügt es zu zeigen, dass $\mathbb{L}_i(\zeta) \subseteq \mathbb{L}_{i+1}(\zeta)$ eine Galoiserweiterung mit zyklischer Automorphismengruppe ist, deren Ordnung ein Teiler von n ist.

Da $\mathbb{L}_i \subseteq \mathbb{L}_{i+1}$ eine Galoiserweiterung ist, liefert Lemma 11.3.14, dass auch die Erweiterungen

$$\mathbb{L}_i \subseteq \mathbb{L}_{i+1}(\zeta), \qquad \mathbb{L}_i(\zeta) \subseteq \mathbb{L}_{i+1}(\zeta)$$

galoissch sind. Nach dem Hauptsatz der Galoistheorie, haben wir deshalb einen kanonischen Epimorphismus

$$\mathrm{Aut}(\mathbb{L}_{i+1}(\zeta), \mathbb{L}_i) \to \mathrm{Aut}(\mathbb{L}_{i+1}, \mathbb{L}_i), \qquad \varphi \mapsto \varphi_{|\mathbb{L}_{i+1}}.$$

Wegen $\mathrm{Aut}(\mathbb{L}_{i+1}(\zeta), \mathbb{L}_i(\zeta)) \subseteq \mathrm{Aut}(\mathbb{L}_{i+1}(\zeta), \mathbb{L}_i)$ liefert Einschränken einen wohldefinierten Homomorphismus

$$\varrho\colon \mathrm{Aut}(\mathbb{L}_{i+1}(\zeta), \mathbb{L}_i(\zeta)) \to \mathrm{Aut}(\mathbb{L}_{i+1}, \mathbb{L}_i), \qquad \varphi \mapsto \varphi_{|\mathbb{L}_{i+1}}.$$

Es genügt zu zeigen, dass ϱ injektiv ist; dann ist $\mathrm{Aut}(\mathbb{L}_{i+1}(\zeta), \mathbb{L}_i(\zeta))$ zyklisch und ihre Ordnung teilt die von $\mathrm{Aut}(\mathbb{L}_{i+1}, \mathbb{L}_i)$ und somit auch n.

Es sei also ein Element $\varphi \in \mathrm{Aut}(\mathbb{L}_{i+1}(\zeta), \mathbb{L}_i(\zeta))$ gegeben mit $\varrho(\varphi) = \mathrm{id}_{\mathbb{L}_{i+1}}$. Dann ist φ die Identität auf $\mathbb{L}_{i+1}$ und auf $\mathbb{L}_i(\zeta)$ folglich muss φ auch auch $\mathbb{L}_{i+1}(\zeta)$ die Identität sein. $\square$

Aufgaben zu Abschnitt 11.3.

Literatur

[1] Emil Artin, *Galois Theory*, Notre Dame Mathematical Lectures, no. 2, University of Notre Dame, Notre Dame, Ind., 1942. Edited and supplemented with a section on applications by Arthur N. Milgram.

[2] Siegfried Bosch, *Algebra*, 9th ed., Springer Spektrum, Berlin, 2020 (German).

[3] Gerd Fischer and Reinhard Sacher, *Einführung in die Algebra*, Teubner Studienbücher Mathematik, B. G. Teubner, Stuttgart, 1974.

[4] Jürgen Hausen, *Lineare Algebra 1*, Shaker Verlag, Aachen, 2017. 3. korrigierte Auflage.

[5] ———, *Lineare Algebra 2*, Shaker Verlag, Aachen, 2013.

[6] Ernst Kunz, *Algebra*, Vieweg, Braunschweig, 191 (German).

[7] Serge Lang, *Algebra*, 3rd ed., Graduate Texts in Mathematics, vol. 211, Springer-Verlag, New York, 2002.

[8] Helmut Wielandt, *Ein Beweis für die Existenz der Sylowgruppen*, Arch. Math. (Basel) **10** (1959), 401–402 (German).