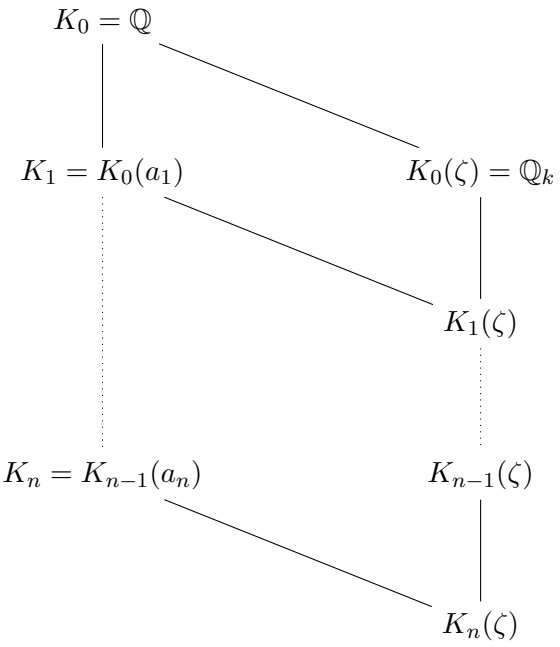
Algebra

Vorlesungen im Wintersemester 2018/19
und Sommersemester 2019

Benjamin Sambale

Version: 24. Dezember 2023



Inhaltsverzeichnis

Vorwort

Die ersten beiden Teile (Algebra I & II) des vorliegenden Skripts entstanden aus $(4+2)$-Vorlesungen im Wintersemester 2018/19 (15 Wochen) und Sommersemester 2019 (14 Wochen) an der Friedrich-Schiller-Universität Jena und richten sich vorrangig an Studierende der Studiengänge Bachelor und Master Mathematik. Es werden Kenntnisse der Linearen Algebra 1–2 und Analysis 1 vorausgesetzt. Die Themen finden sich größtenteils auch in folgenden Büchern:

- Karpfinger, Meyberg: *Algebra*, 4. Auflage, Springer Spektrum, 2017
- Wüstholz: *Algebra*, 2. Auflage, Springer Spektrum, 2013
- Bosch: *Algebra*, 7. Auflage, Springer Spektrum, 2013
- Jantzen, Schwermer : *Algebra*, 2. Auflage, Springer Spektrum, 2014
- Rotman: *Advanced Modern Algebra 1 & 2*, 3. Auflage, AMS, 2017
- Isaacs: *Algebra*, AMS, 1994

Nachträglich wurden viele Inhalte ergänzt (insbesondere hat es die Vorlesung „Algebra 3“ nie gegeben). Auf meiner Homepage stehen weitere Skripte zur Verfügung. Im Anhang werden einige Highlights der Algebra besprochen, die in einer gewöhnlichen Vorlesung keinen Platz finden. Das Skript in der jetzigen Form dient mir hauptsächlich als eigene Referenz. Ich bedanke mich bei Burkhard Külshammer und Till Müller für einige Korrekturhinweise.

Algebra I

1 Motivation

Gibt es eine Lösungsformel für die Gleichung

$$x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = 0 \qquad (a_0, a_1, \ldots, a_{n-1} \in \mathbb{Q})? \tag{I.1.1}$$

- $n = 1$: $x = -a_0$ ist die einzige Lösung.
- $n = 2$: $x = -\frac{a_1}{2} \pm \sqrt{\frac{a_1^2}{4} - a_0}$ (p-q-Formel).
- $n = 3$: Gelöst von Tartaglia, del Ferro und Cardano:[1] Die Substitution $y = x + \frac{a_2}{3}$ führt zu

  $$y^3 + py + q = 0$$

  für gewisse $p, q \in \mathbb{Q}$. Der Ansatz $y = u + v$ ergibt $u^3 + v^3 = -q$ und $u^3 v^3 = -p^3/27$. Daher sind u^3 und v^3 die Lösungen von

  $$z^2 + qz - \frac{p^3}{27} = 0.$$

  Man erhält

  $$y = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$$

  bei geeigneter Wahl der kubischen Wurzeln. Selbst wenn alle Lösungen reell sind, benötigt man für deren Darstellung in der Regel komplexe Zahlen (dieses Phänomen heißt *casus irreducibilis*).
- $n = 4$: Gelöst von Ferrari und Cardano: Mit der Substitution $y = x + \frac{a_3}{4}$ erhält man

  $$y^4 + py^2 + qy + r.$$

  Der Ansatz $y^4 + py^2 + qy + r = (y^2 + sy + u)(y^2 - sy + v)$ führt zu

  $$s^6 + 2ps^4 + (p^2 - 4r)s^2 - q^2 = 0.$$

  Damit hat man das Problem auf eine kubische Gleichung in s^2 zurückgeführt. Anschließend berechnet man $u = \frac{1}{2}(s^2 + p - q/s)$, $v = s^2 + p - u$ und löst die beiden quadratischen Gleichungen nach y.
- $n \geq 5$: Es gibt keine allgemeine Formel! (Satz von Abel-Ruffini).

Weitere Ziele der Vorlesung:

- Fundamentalsatz der Algebra: Gleichung I.1.1 besitzt genau n komplexe Lösungen gezählt mit Vielfachheiten.
- Welche regelmäßigen n-Ecke kann man mit Zirkel und Lineal konstruieren? (gleichseitiges Dreieck und Quadrat sind leicht, Fünfeck schwieriger, 7-Eck geht nicht).
- Quadratur des Kreises: Mit Zirkel und Lineal lässt sich kein Quadrat konstruieren, das den gleichen Flächeninhalt wie der Einheitskreis hat.

[1] zum historischen Hintergrund siehe Wikipedia

2 Zahlentheorie

Bemerkung I.2.1. Wir benutzen die üblichen Zahlbereiche:

- Natürliche Zahlen: $\mathbb{N} = \{1, 2, \ldots\}$, $\mathbb{N}_0 = \{0, 1, \ldots\}$.
- Ganze Zahlen: $\mathbb{Z} = \{\ldots, -1, 0, 1, \ldots\}$.
- Rationale Zahlen: $\mathbb{Q} = \{\frac{a}{b} : a, b \in \mathbb{Z},\ b \neq 0\}$.
- Reelle Zahlen: $\mathbb{R}$ (Analysis).
- Komplexe Zahlen: $\mathbb{C} = \{a + b\mathrm{i} : a, b \in \mathbb{R}\}$.

Satz I.2.2 (Division mit Rest)**.** *Für $a \in \mathbb{Z}$ und $d \in \mathbb{N}$ existieren eindeutig bestimmte $q, r \in \mathbb{Z}$ mit $a = qd + r$ und $0 \leq r < d$.*

Beweis. Offenbar ist die Menge $M := \{a - cd : c \in \mathbb{Z} \text{ mit } a - cd \geq 0\} \subseteq \mathbb{N}_0$ nicht leer und besitzt daher ein minimales Element $r := a - qd \geq 0$ mit $q \in \mathbb{Z}$. Im Fall $r \geq d$ wäre auch $a - (q + 1)d = r - d \in M$ im Widerspruch zur Minimalität von r. Also ist $0 \leq r < d$. Seien nun $q', r' \in \mathbb{Z}$ mit $a = q'd + r'$ und $0 \leq r' < d$. Aus $d|q - q'| = |dq - dq'| = |r' - r| < d$ folgt dann $q = q'$ und $r = r'$. □

Bemerkung I.2.3. Man nennt r in Satz I.2.2 den *Rest* bei der Division von a durch d.

Beispiel I.2.4. Die Division 20 durch 7 lässt Rest 6, denn $20 = 2 \cdot 7 + 6$.

Definition I.2.5. Für $a, b \in \mathbb{Z}$ sagt man a *teilt* b (oder a ist ein *Teiler* von b oder b ist durch a *teilbar*), falls ein $c \in \mathbb{Z}$ mit $ac = b$ existiert. Man schreibt dann $a \mid b$.

Lemma I.2.6. *Für $a, b, c, d, e \in \mathbb{Z}$ gilt*

(i) $\pm 1 \mid a \mid 0$,

(ii) $0 \mid a \iff a = 0$,

(iii) $a \mid b \mid c \implies a \mid c$,

(iv) $a \mid b \mid a \implies a = \pm b$,

(v) $a \mid b, c \implies a \mid (bd + ce)$,

(vi) $a \mid b \neq 0 \implies |a| \leq |b|$.

Beweis. Alle Aussagen sind leicht. Wir beweisen als Muster (iv). Wegen $a \mid b \mid a$ existieren $c, d \in \mathbb{Z}$ mit $ac = b$ und $bd = a$. Also ist $a = bd = cda$. Im Fall $a = 0$ ist auch $b = ac = 0$. Anderenfalls ist $cd = 1$ und $c = \pm 1$. Dann ist $a = \pm b$. □

Definition I.2.7. Für $a_1, \ldots, a_n \in \mathbb{Z}$ sei

$$\mathrm{gT}(a_1, \ldots, a_n) := \{d \in \mathbb{Z} : d \mid a_1, \ldots, a_n\}$$

die Menge der *gemeinsamen Teiler* von $a_1, \ldots, a_n$. Ein $g \in \mathrm{gT}(a_1, \ldots, a_n) \cap \mathbb{N}_0$ heißt *größter gemeinsamer Teiler* von $a_1, \ldots, a_n$, falls $d \mid g$ für alle $d \in \mathrm{gT}(a_1, \ldots, a_n)$ gilt. Man schreibt dann $\mathrm{ggT}(a_1, \ldots, a_n) := g$. Im Fall $\mathrm{ggT}(a_1, \ldots, a_n) = 1$ nennt man $a_1, \ldots, a_n$ *teilerfremd*.

Bemerkung I.2.8.

(i) Sind g und g' größte gemeinsame Teiler von $a_1, \ldots, a_n$, so gilt $g \mid g' \mid g$ und $g = \pm g'$ nach Lemma I.2.6(iv). Wegen $g, g' \geq 0$ ist also $g = g'$, d. h. es existiert höchstens ein gemeinsamer Teiler von $a_1, \ldots, a_n$ (dies rechtfertigt die Schreibweise ggT).

(ii) Die Bezeichnung „größter gemeinsamer Teiler“ ist irreführend, denn $\mathrm{gT}(0, 0) = \mathbb{Z}$, aber $\mathrm{ggT}(0, 0) = 0$.

(iii) Für die Berechnung von $\mathrm{ggT}(a_1, \ldots, a_n)$ kann man offenbar $a_1 > \ldots > a_n > 0$ annehmen. Für $d \in \mathrm{gT}(a_1, \ldots, a_n)$ gilt $d \mid a_1$ und $d \mid \mathrm{ggT}(a_2, \ldots, a_n)$. Also ist $\mathrm{gT}(a_1, \ldots, a_n) \subseteq \mathrm{gT}(a_1, \mathrm{ggT}(a_2, \ldots, a_n))$. Für $d \in \mathrm{gT}(a_1, \mathrm{ggT}(a_2, \ldots, a_n))$ gilt umgekehrt $d \mid \mathrm{ggT}(a_2, \ldots, a_n) \mid a_i$ für $i = 2, \ldots, n$, also $d \in \mathrm{gT}(a_1, \ldots, a_n)$. Dies zeigt

$$\mathrm{ggT}(a_1, \ldots, a_n) = \mathrm{ggT}(a_1, \mathrm{ggT}(a_2, \ldots, a_n)).$$

Es genügt also den ggT von zwei natürlichen Zahlen berechnen zu können.

(iv) Sei $a > b > 0$. Division mit Rest liefert $a = bq + r$ mit $q, r \in \mathbb{Z}$ und $0 \leq r < b$. Nach Lemma I.2.6(v) ist $\mathrm{gT}(a, b) = \mathrm{gT}(bq + r, b) = \mathrm{gT}(r, b)$ und daher $\mathrm{ggT}(a, b) = \mathrm{ggT}(r, b)$. Im Fall $r > 0$ kann man b mit Rest durch r teilen und erhält dadurch immer kleinere Zahlen. Man Ende ist $\mathrm{ggT}(a, b) = \mathrm{ggT}(r, b) = \ldots = \mathrm{ggT}(d, 0) = d$. Insbesondere existiert der ggT immer. Der folgende Satz gibt genauere Auskunft.

Satz I.2.9 (Erweiterter euklidischer Algorithmus)**.**
Eingabe: $a, b \in \mathbb{N}$.
Initialisierung: $(x_0, y_0, z_0) := (1, 0, a)$, $(x_1, y_1, z_1) := (0, 1, b)$ *und* $k := 0$.
Solange $z_{k+1} > 0$ *wiederhole:*
Division mit Rest: $z_k = q_{k+1} z_{k+1} + r_{k+1}$ *mit* $0 \leq r_{k+1} < z_{k+1}$.
Setze $(x_{k+2}, y_{k+2}, z_{k+2}) := (x_k - x_{k+1} q_{k+1}, y_k - y_{k+1} q_{k+1}, r_{k+1})$ *und* $k := k + 1$.
Ausgabe: $z_k = x_k a + y_k b = \mathrm{ggT}(a, b)$.

Beweis. Wegen $z_1 > r_1 = z_2 > r_2 = z_3 > \ldots$ terminiert der Algorithmus. Am Ende gilt

$$\begin{aligned} z_k &= \mathrm{ggT}(z_k, 0) = \mathrm{ggT}(z_k, z_{k+1}) = \mathrm{ggT}(z_k, r_k) = \mathrm{ggT}(z_k, z_{k-1} - q_k z_k) \\ &= \mathrm{ggT}(z_k, z_{k-1}) = \ldots = \mathrm{ggT}(z_0, z_1) = \mathrm{ggT}(a, b). \end{aligned}$$

Für $i = 0, 1$ gilt $x_i a + y_i b = z_i$. Induktiv folgt

$$\begin{aligned} x_{i+1} a + y_{i+1} b &= (x_{i-1} - x_i q_i) a + (y_{i-1} - y_i q_i) b = x_{i-1} a + y_{i-1} b - (x_i a + y_i b) q_i \\ &= z_{i-1} - z_i q_i = r_i = z_{i+1}. \end{aligned}$$

Daher ist $\mathrm{ggT}(a, b) = z_k = x_k a + y_k b$. □

Beispiel I.2.10. Für $a := 45$ und $b := 24$ erhält man:

x_i	y_i	z_i	q_i
1	0	45	
0	1	24	1
1	-1	21	1
-1	2	$\boxed{3}$	7
		0	

Also ist $\mathrm{ggT}(45, 24) = 3 = -45 + 2 \cdot 24$.

Folgerung I.2.11. *Für $a_1, \ldots, a_n, b \in \mathbb{Z}$ gilt*

$$\mathrm{ggT}(a_1, \ldots, a_n) \mid b \iff \exists b_1, \ldots, b_n \in \mathbb{Z} : a_1 b_1 + \ldots + a_n b_n = b.$$

Beweis. Sei $g := \mathrm{ggT}(a_1, \ldots, a_n)$.

$\Rightarrow$: Sei $gd = b$. Nach Bemerkung I.2.8(iii) und Satz I.2.9 existieren $c_1, \ldots, c_n \in \mathbb{Z}$ mit $g = a_1 c_1 + \ldots + a_n c_n$. Die Behauptung folgt mit $b_i := dc_i$ für $i = 1, \ldots, n$.

$\Leftarrow$: Wegen $g \mid a_i$ für $i = 1, \ldots, n$ gilt $g \mid a_1 b_1 + \ldots + a_n b_n = b$. □

Definition I.2.12. Man nennt $v \in \mathbb{Z}$ ein *gemeinsames Vielfaches* von $a_1, \ldots, a_n \in \mathbb{Z}$, falls $a_i \mid v$ für $i = 1, \ldots, n$ gilt. Ein gemeinsames Vielfaches $v \in \mathbb{N}_0$ heißt *kleinstes gemeinsames Vielfache*, falls v jedes gemeinsame Vielfache von $a_1, \ldots, a_n$ teilt. Man schreibt dann $\mathrm{kgV}(a_1, \ldots, a_n) := v$.

Bemerkung I.2.13. Wie beim ggT zeigt man, dass höchstens ein kgV existiert. Außerdem ist

$$\mathrm{kgV}(a_1, \ldots, a_n) = \mathrm{kgV}(a_1, \mathrm{kgV}(a_2, \ldots, a_n)).$$

Wir berechnen das kgV über einen Umweg.

Definition I.2.14. Man nennt $p \in \mathbb{N}$ *Primzahl*, falls p genau zwei positive Teiler hat, nämlich 1 und p. Die Menge der Primzahlen bezeichnen wir mit $\mathbb{P}$. Man nennt $p \in \mathbb{P}$ *Primteiler* von $a \in \mathbb{Z}$, falls $p \mid a$.

Bemerkung I.2.15.

(i) Beachte: 1 ist *keine* Primzahl!

(ii) Zwei verschiedene Primzahlen sind stets teilerfremd.

Lemma I.2.16.

(i) Für $a, b \in \mathbb{Z}$ und $p \in \mathbb{P}$ gilt $p \mid ab \Longrightarrow p \mid a \vee p \mid b$.

(ii) Jedes $a \in \mathbb{N} \setminus \{1\}$ besitzt einen Primteiler.

Beweis.

(i) Sei $p \mid ab$ und $p \nmid a$. Nach dem euklidischen Algorithmus existieren $c, d \in \mathbb{Z}$ mit $1 = \mathrm{ggT}(a, p) = ac + pd$. Es folgt $p \mid abc + pbd = b1 = b$.

(ii) Sei $p > 1$ ein möglichst kleiner Teiler von a (notfalls $p = a$). Im Fall $p \notin \mathbb{P}$ existiert $1 < q < p$ mit $q \mid p \mid a$ im Widerspruch zur Wahl von p. Also ist $p \in \mathbb{P}$. □

Satz I.2.17 (Euklid)**.** *Es gibt unendlich viele Primzahlen.*

Beweis. Annahme: $\mathbb{P} = \{p_1 = 2, \ldots, p_n\}$. Nach Lemma I.2.16 existiert ein Primteiler q von $a = p_1 \ldots p_n + 1$. Nach der Annahme ist $q \in \{p_1, \ldots, p_n\}$ und man erhält den Widerspruch $q \mid (a - p_1 \ldots p_n) = 1$. □

Satz I.2.18 (Eindeutige Primfaktorzerlegung)**.** *Für jedes $n \in \mathbb{N}$ existieren eindeutig bestimmte $a_p \in \mathbb{N}_0$ für $p \in \mathbb{P}$ mit*

$$n = \prod_{p \in \mathbb{P}} p^{a_p}.$$

Beweis. Induktion nach n: Im Fall $n = 1$ ist $a_p = 0$ für alle $p \in \mathbb{P}$. Sei nun $n \geq 2$ und p ein Primteiler von n. Nach Induktion besitzt n/p eine Primfaktorzerlegung und daher auch $n = p \cdot n/p$. Sei $n = \prod p^{a_p} = \prod p^{b_p}$ und $a_q < b_q$ für ein $q \in \mathbb{P}$. Dann ist

$$q \mid \frac{n}{q^{a_q}} = \prod_{p \neq q} p^{a_p}$$

und Lemma I.2.16(i) zeigt $q = p$ für ein $p \in \mathbb{P} \setminus \{q\}$. Widerspruch. □

Beispiel I.2.19. Sei $k \geq 2$ und $n \in \mathbb{N}$ nicht die k-te Potenz einer natürlichen Zahl. Dann ist $\sqrt[k]{n}$ irrational, denn anderenfalls existieren teilerfremde $a, b \in \mathbb{N}$ mit $\sqrt[k]{n} = a/b$. Dann ist $nb^k = a^k$. Die eindeutige Primfaktorzerlegung zeigt $b^k = 1$ und man erhält den Widerspruch $n = a^k$.

Bemerkung I.2.20.

(i) Die Teiler von $n = \prod_{p \in \mathbb{P}} p^{a_p}$ haben die Form $n = \prod_{p \in \mathbb{P}} p^{a'_p}$ mit $0 \leq a'_p \leq a_p$ für alle $p \in \mathbb{P}$. Für $m = \prod_{p \in \mathbb{P}} p^{b_p}$ gilt daher

$$\boxed{\operatorname{ggT}(n, m) = \prod_{p \in \mathbb{P}} p^{\min\{a_p, b_p\}}, \quad \operatorname{kgV}(n, m) = \prod_{p \in \mathbb{P}} p^{\max\{a_p, b_p\}}.}$$

Dies zeigt

$$\boxed{nm = \operatorname{ggT}(n, m) \operatorname{kgV}(n, m),}$$

denn $a_p + b_p = \min\{a_p, b_p\} + \max\{a_p, b_p\}$. Da man keinen schnellen Algorithmus zur Primfaktorzerlegung kennt, ist der euklidische Algorithmus zur Berechnung von ggT und kgV in der Regel zu bevorzugen.

(ii) Satz I.2.18 erlaubt folgende Verallgemeinerung von Lemma I.2.16(i): Sind $a, b \in \mathbb{Z}$ teilerfremd und $a \mid bc$, so folgt $a \mid c$.

Definition I.2.21. Für $a, b \in \mathbb{Z}$ und $d \in \mathbb{N}$ schreiben wir $a \equiv b \pmod{d}$, falls $d \mid (a - b)$. Man sagt dann: a und b sind *kongruent modulo d*.

Beispiel I.2.22.

(i) Im Dezimalsystem rechnet man modulo 10 und im Binärsystem modulo 2.

(ii) Man betrachtet Sekunden und Minuten modulo 60 und Stunden modulo 12 oder 24.

(iii) Wochentage zählt man modulo 7.

(iv) Eurocent rechnet man modulo 100.

(v) In der Musik betrachtet man Töne modulo 8 (*c, d, e, f, g, a, h*) oder 12 (*c, cis, d, . . . , h*).

Satz I.2.23. *Die Kongruenz modulo $d \in \mathbb{N}$ ist eine Äquivalenzrelation auf $\mathbb{Z}$, d. h. es gilt*

(i) $a \equiv a \pmod{d}$ (*reflexiv*),

(ii) $a \equiv b \pmod{d} \Longrightarrow b \equiv a \pmod{d}$ (*symmetrisch*),

(iii) $a \equiv b \equiv c \pmod{d} \Longrightarrow a \equiv c \pmod{d}$ (*transitiv*).

Außerdem gilt

(iv)

$$\left.\begin{array}{ll} a \equiv a' & (\mathrm{mod}\ d) \\ b \equiv b' & (\mathrm{mod}\ d) \end{array}\right\} \Longrightarrow a \dot{+} b \equiv a' \dot{+} b' \pmod{d}.$$

Beweis.

(i) $d \mid 0 = a - a$.

(ii) $d \mid a - b \Longrightarrow d \mid -(a - b) = b - a$.

(iii) $d \mid a - b \wedge d \mid b - c \Longrightarrow d \mid (a - b) + (b - c) = a - c$.

(iv) Sei $d \mid a - a'$ und $d \mid b - b'$. Dann folgt $d \mid (a - a') + (b - b') = (a + b) - (a' + b')$ sowie $d \mid (a - a')b + (b - b')a' = ab - a'b'$. □

Bemerkung I.2.24. Die Äquivalenzklassen in der Situation von Satz I.2.23 heißen *Restklassen* modulo d. Sie haben die Form $a + d\mathbb{Z} := \{a + cd : c \in \mathbb{Z}\}$ für $a \in \mathbb{Z}$ (alle Elemente in $a + d\mathbb{Z}$ lassen den gleichen Rest bei der Division durch d). Die Menge aller Restklassen modulo d bezeichnen wir mit $\mathbb{Z}/d\mathbb{Z}$. Offenbar ist

$$\mathbb{Z}/d\mathbb{Z} = \{0 + d\mathbb{Z} = d\mathbb{Z},\, 1 + d\mathbb{Z}, \ldots, d - 1 + d\mathbb{Z}\}$$

und $|\mathbb{Z}/d\mathbb{Z}| = d$.

Beispiel I.2.25.

(i) Gleichung (iv) vereinfacht viele Rechnungen. Wir prüfen, ob $7^{90} + 111^7$ durch 5 teilbar ist:

$$7^{90} + 111^7 \equiv 2^{90} + 1^7 \equiv 4^{45} + 1 \equiv (-1)^{45} + 1 \equiv 0 \pmod{5}.$$

In Folgerung I.7.18 zeigen wir, dass man auch die Exponenten reduzieren darf, allerdings modulo 4.

(ii) (DHM-*Schlüsselaustausch*) Zur geheimen Kommunikation möchten sich die Personen A und B zunächst auf einen geheimen Schlüssel einigen. Hierfür werden (öffentlich) teilerfremde natürliche Zahlen $m < n$ gewählt, wobei n „groß“ ist ($n > 10^{1000}$). Person A wählt geheim und zufällig $a \in \mathbb{N}$ und schickt $am + n\mathbb{Z}$ an B. Person B wählt geheim und zufällig $b \in \mathbb{N}$ und schickt $bm + n\mathbb{Z}$ an A. Beide können nun $a(bm + n\mathbb{Z}) = b(am + n\mathbb{Z})$ als geheimen Schlüssel verwenden. Da man bislang keinen effizienten Algorithmus zur Berechnung des *diskreten Logarithmus* (um beispielsweise a aus $am + n\mathbb{Z}$ und m zu berechnen) kennt, ist dieses Verfahren aktuell sicher.[1]

Lemma I.2.26 (Kürzen von Kongruenzen)**.** *Für $a, b \in \mathbb{Z}$ und $d, e \in \mathbb{N}$ gilt*

$$\boxed{ae \equiv be \pmod{d} \iff a \equiv b \pmod{\frac{d}{\operatorname{ggT}(d,e)}}.}$$

Beweis. Sei $ae \equiv be \pmod{d}$ und $g := \operatorname{ggT}(d, e)$. Dann ist $d \mid (a-b)e$ und $\frac{d}{g} \mid (a-b)\frac{e}{g}$. Wegen $\operatorname{ggT}(\frac{d}{g}, \frac{e}{g}) = 1$ folgt $\frac{d}{g} \mid (a-b)$ (Bemerkung I.2.20(ii)) und $a \equiv b \pmod{\frac{d}{g}}$. Ist umgekehrt $a \equiv b \pmod{\frac{d}{g}}$, so gilt $d \mid d\frac{e}{g} = \frac{d}{g}e \mid (a-b)e$, also $ae \equiv be \pmod{d}$. □

Beispiel I.2.27. Eine ISBN zur Indizierung von Büchern besteht aus neun Ziffern $z_1, \ldots, z_9 \in \{0, \ldots, 9\}$ sowie einer Prüfziffer $s \in \{0, \ldots, 9, X\}$ mit

$$s \equiv \sum_{k=1}^{9} kz_k \pmod{11},$$

wobei 10 durch X ersetzt wird. Wegen

$$\begin{aligned} kz_k \equiv kz_k' \pmod{11} &\iff z_k \equiv z_k' \pmod{11}, \\ kz_k + lz_k \equiv kz_l + lz_k \pmod{11} &\iff (k-l)z_k \equiv (k-l)z_l \pmod{11} \iff z_k \equiv z_l \pmod{11} \end{aligned}$$

erkennt die Prüfziffer eine fehlerhafte Ziffer oder eine Vertauschung von zwei Ziffern (aber nicht beides gleichzeitig). Siehe Kapitel III.10.

Satz I.2.28 (Kongruenzgleichungen)**.** *Seien $a, b \in \mathbb{Z}$ und $d \in \mathbb{N}$. Genau dann existiert ein $x \in \mathbb{Z}$ mit $ax \equiv b \pmod{d}$, falls $\operatorname{ggT}(a, d) \mid b$. Gegebenenfalls bilden diese x eine Restklasse modulo $\frac{d}{\operatorname{ggT}(a,d)}$.*

Beweis. Erste Aussage:

$$\exists x \in \mathbb{Z} : ax \equiv b \pmod{d} \iff \exists x, c \in \mathbb{Z} : b = ax + cd \overset{I.2.11}{\iff} \operatorname{ggT}(a, d) \mid b.$$

Zweite Aussage:

$$ax \equiv ay \pmod{d} \overset{I.2.26}{\iff} x \equiv y \pmod{\frac{d}{\operatorname{ggT}(a,d)}}.$$ □

Bemerkung I.2.29. Satz I.2.28 besagt, dass die Gleichung $ax \equiv b \pmod{d}$ im Falle der Lösbarkeit zu einer Gleichung der Form $x \equiv c \pmod{d/\operatorname{ggT}(a, d)}$ äquivalent ist.

[1] Dieses einfache Prinzip wurde erst in den 1970er Jahren von Diffie, Hellman und Merkle entdeckt. Zu diesem Zeitpunkt war Alan Turing, der Entschlüssler der Enigma aus dem zweiten Weltkrieg, bereits 20 Jahre tot.

Beispiel I.2.30. Wie wertvoll ist ein 124,76 g schwerer Haufen von 1- und 2-Centmünzen? Eine 1-Centmünze wiegt 2300 mg und eine 2-Centmünze 3060 mg. Ansatz: $2300x + 3060y = 124.760$. Wir teilen durch $\operatorname{ggT}(2300, 3060) = 20$ und erhalten $115x + 153y = 6238$. Modulo 115 ergibt sich

$$38y \equiv 28 \pmod{115}.$$

Nach dem euklidischen Algorithmus ist $1 = \operatorname{ggT}(38, 115) = -3 \cdot 38 + 115 \equiv -3 \cdot 38 \pmod{115}$. Einsetzen liefert $38y \equiv 28 \cdot (-3 \cdot 38) \pmod{115}$. Lemma I.2.26 zeigt

$$y \equiv -3 \cdot 28 \equiv 31 \pmod{115}.$$

Für $y \geq 31 + 115$ wäre $3060y \geq 446.760 > 124.760$. Also ist $y = 31$ die einzige Lösung und $x = \frac{6238 - 153y}{115} = 13$ folgt.

Antwort: $13 + 2 \cdot 31 = 75$ Cent.

Bemerkung I.2.31. Für $\alpha, \beta, \gamma \in \mathbb{N}_0$ gilt $\min\{\max\{\alpha, \beta\}, \gamma\} = \max\{\min\{\alpha, \gamma\}, \min\{\beta, \gamma\}\}$ (betrachte o. B. d. A. $\alpha \geq \beta$). Dies zeigt

$$\operatorname{ggT}\big(\operatorname{kgV}(a, b), c\big) = \operatorname{kgV}\big(\operatorname{ggT}(a, c), \operatorname{ggT}(b, c)\big) \tag{I.2.1}$$

für $a, b, c \in \mathbb{Z}$ (Bemerkung I.2.20).

Satz I.2.32 (Chinesischer Restsatz)**.** *Seien $a_1, \ldots, a_n \in \mathbb{Z}$ und $d_1, \ldots, d_n \in \mathbb{N}$. Genau dann existiert ein $x \in \mathbb{Z}$ mit $x \equiv a_i \pmod{d_i}$ für $i = 1, \ldots, n$, falls $a_i \equiv a_j \pmod{\operatorname{ggT}(d_i, d_j)}$ für alle i, j gilt. Gegebenenfalls bilden die x eine Restklasse modulo $\operatorname{kgV}(d_1, \ldots, d_n)$.*

Beweis. Existiert $x \in \mathbb{Z}$ mit $x \equiv a_i \pmod{d_i}$ für $i = 1, \ldots, n$, so gilt $\operatorname{ggT}(d_i, d_j) \mid (a_i - x) + (x - a_j) = a_i - a_j$, also $a_i \equiv a_j \pmod{\operatorname{ggT}(d_i, d_j)}$ für alle i, j.

Eindeutigkeit:

$$\begin{aligned} \forall i : x \equiv y \pmod{d_i} &\iff \forall i : d_i \mid x - y \iff \operatorname{kgV}(d_1, \ldots, d_n) \mid x - y \\ &\iff x \equiv y \pmod{\operatorname{kgV}(d_1, \ldots, d_n)}. \end{aligned}$$

Existenz: Sei $a_i \equiv a_j \pmod{\operatorname{ggT}(d_i, d_j)}$ für i, j gegeben. Wir argumentieren durch Induktion nach n. Für $n = 1$ löst $x := a_1$ die Kongruenz. Sei nun $n \geq 2$. Nach dem euklidischen Algorithmus existieren $e_1, e_2 \in \mathbb{Z}$ mit $g := \operatorname{ggT}(d_1, d_2) = d_1 e_1 + d_2 e_2$. Wir setzen $b := a_1 + d_1 e_1 \frac{a_2 - a_1}{g} \in \mathbb{Z}$. Dann gilt

$$\begin{aligned} &b \equiv a_1 \pmod{d_1}, \\ &b = a_1 + (g - d_2 e_2)\frac{a_2 - a_1}{g} = a_1 + (a_2 - a_1) - d_2 e_2 \frac{a_2 - a_1}{g} \equiv a_2 \pmod{d_2}, \end{aligned}$$

d. h. b löst die ersten beiden Gleichungen. Nach der bereits gezeigten Eindeutigkeit sind diese Gleichungen äquivalent zu

$$x \equiv b \pmod{\operatorname{kgV}(d_1, d_2)}.$$

Um die Induktionsvoraussetzung zu benutzen, müssen wir $b \equiv a_i \pmod{\operatorname{ggT}(\operatorname{kgV}(d_1, d_2), d_i)}$ für $i = 3, \ldots, n$ zeigen. Es gilt $b \equiv a_1 \equiv a_i \pmod{\operatorname{ggT}(d_1, d_i)}$ und $b \equiv a_2 \equiv a_i \pmod{\operatorname{ggT}(d_2, d_i)}$. Dies zeigt

$$b \equiv a_i \pmod{\operatorname{kgV}(\operatorname{ggT}(d_1, d_i), \operatorname{ggT}(d_2, d_i))}$$

und die Behauptung folgt aus (I.2.1). □

Bemerkung I.2.33. Die Bedingungen $a_i \equiv a_j \pmod{\operatorname{ggT}(d_i, d_j)}$ in Satz I.2.32 sind stets erfüllt, wenn $d_1, \ldots, d_n$ paarweise teilerfremd sind.[2]

Beispiel I.2.34.

(i) Betrachte das System

$$\begin{aligned} x &\equiv 3 \pmod 7, \\ x &\equiv 4 \pmod{11}, \\ x &\equiv 5 \pmod{13}. \end{aligned}$$

Der Ansatz $x = 3 + 7a$ löst zunächst die erste Gleichung und liefert $7a \equiv 1 \pmod{11}$ in der zweiten Gleichung. Nach Satz I.2.28 ist dies zu $a \equiv -3 \pmod{11}$ äquivalent (die Lösung -3 kann man leicht erraten). Wir setzen nun $a = -3 + 11b$ und erhalten $x = -18 + 77b$. Dies löst die ersten beiden Gleichungen. Die dritte Gleichung liefert $77b \equiv 23 \pmod{13}$, also $b \equiv 3 \pmod{13}$. Die allgemeine Lösung des Systems lautet daher $x = -18 + 77(3 + 13c) = 213 + 1001c$ mit $c \in \mathbb{Z}$.

(ii) Was sind die letzten beiden Dezimalziffern von 47^{88}? Wir suchen $0 \leq x \leq 99$ mit

$$x \equiv 47^{88} \pmod{100}.$$

Wegen $\operatorname{kgV}(4, 25) = 100$ ist diese Kongruenz nach Satz I.2.32 äquivalent zum System

$$\begin{aligned} x &\equiv 47^{88} \pmod 4, \\ x &\equiv 47^{88} \pmod{25}. \end{aligned}$$

Es gilt $47^{88} \equiv (-1)^{88} \equiv 1 \pmod 4$ und

$$47^{88} \equiv (-3)^{3\cdot 29+1} \equiv (-2)^{29}(-3) \equiv (-2)^{7\cdot 4+1}(-3) \equiv (-3)^4 6 \equiv 11 \pmod{25}.$$

Der Ansatz $x = 1 + 4a$ löst die erste Gleichung und ergibt $4a \equiv 10 \pmod{25}$ in der zweiten Gleichung. Es folgt $2a \equiv 5 \pmod{25}$ und $a \equiv 13 \cdot 2a \equiv 13 \cdot 5 \equiv 15 \pmod{25}$. Also ist $x = 1 + 4 \cdot 15 = 61$.

Definition I.2.35. Man nennt

$$\begin{aligned} \varphi\colon \mathbb{N} &\to \mathbb{N}, \\ n &\mapsto |\{1 \leq k \leq n : \operatorname{ggT}(n, k) = 1\}| \end{aligned}$$

EULER*sche φ-Funktion.*

Bemerkung I.2.36. Für $b \in a + n\mathbb{Z}$ gilt $\operatorname{ggT}(b, n) = \operatorname{ggT}(a, n)$. Da $a + n\mathbb{Z}$ genau einen Repräsentanten b mit $1 \leq b \leq n$ besitzt, gilt

$$\varphi(n) = |\{a + n\mathbb{Z} : \operatorname{ggT}(a, n) = 1\}|.$$

Satz I.2.37. *Es gilt*

(i) $\varphi(nm) = \varphi(n)\varphi(m)$, *falls* $\operatorname{ggT}(n, m) = 1$.

(ii) $\varphi(p^n) = p^n - p^{n-1}$ *für jede Primzahlpotenz* $p^n \neq 1$.

[2] $\operatorname{ggT}(d_1, \ldots, d_n) = 1$ reicht *nicht*! (betrachte $\operatorname{ggT}(6, 10, 15)$)

Beweis.

(i) Seien $1 \leq a \leq n$ und $1 \leq b \leq m$ mit $\mathrm{ggT}(a,n) = 1 = \mathrm{ggT}(b,m)$. Nach dem chinesischen Restsatz existiert genau ein $1 \leq c \leq \mathrm{kgV}(n,m) = nm$ mit $c \equiv a \pmod{n}$ und $c \equiv b \pmod{m}$. Offenbar ist dann $\mathrm{ggT}(c, nm) = 1$. Ist umgekehrt $1 \leq c \leq nm$ mit $\mathrm{ggT}(c,nm) = 1$ gegeben, so gilt auch $\mathrm{ggT}(c,n) = 1 = \mathrm{ggT}(c,m)$. Daher sind die Mengen

$$\{1 \leq a \leq n : \mathrm{ggT}(a,n) = 1\} \times \{1 \leq b \leq m : \mathrm{ggT}(b,m) = 1\}$$

und $\{1 \leq c \leq nm : \mathrm{ggT}(c,nm) = 1\}$ gleichmächtig und die Behauptung folgt.

(ii) Es gilt $\mathrm{ggT}(p^n, k) = 1$ genau dann, wenn $p \nmid k$. Zwischen 1 und p^n liegen genau p^{n-1} Vielfache von p, nämlich $p, 2p, \ldots, p^{n-1}p$. Dies zeigt die Behauptung. □

Bemerkung I.2.38. Sei $n = \prod_{p\in\mathbb{P}} p^{a_p} \in \mathbb{N}$. Nach Satz I.2.37 ist dann

$$\boxed{\varphi(n) = \prod_{p\in\mathbb{P}} \varphi(p^{a_p}) = \prod_{\substack{p\in\mathbb{P}\\ a_p>0}} (p^{a_p} - p^{a_p-1}).}$$

Beispiel I.2.39. Es gilt

$$\varphi(36) = \varphi(2^2 \cdot 3^2) = (2^2 - 2^1)(3^2 - 3^1) = 2 \cdot 6 = 12$$

und

$$\{1 \leq a \leq 36 : \mathrm{ggT}(a, 36) = 1\} = \{1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35\}.$$

Definition I.2.40. Man nennt

$$\mu\colon \mathbb{N} \to \mathbb{N},$$
$$n \mapsto \begin{cases} (-1)^s & \text{falls } n = p_1 \ldots p_s \text{ mit paarweise verschiedenen } p_1, \ldots, p_s \in \mathbb{P}, \\ 0 & \text{sonst} \end{cases}$$

Möbius-*Funktion*. Dabei ist $\mu(1) = 1$ $(s = 0)$.

Bemerkung I.2.41. Sind $p_1, \ldots, p_s$ die verschiedenen Primteiler von $n > 1$, so gilt

$$\sum_{d|n} \mu(d) = \sum_{k=0}^{s} \sum_{q_1,\ldots,q_k \in \{p_1,\ldots,p_s\}} \mu(q_1 \ldots q_k) = \sum_{k=0}^{s} \sum_{\substack{M\subseteq\{p_1,\ldots,p_s\}\\ |M|=k}} (-1)^k = \sum_{k=0}^{s} (-1)^k \binom{s}{k} = (1-1)^s = 0,$$

wobei nur über die positiven Teiler summiert wird.

Satz I.2.42 (Möbius-Inversion)**.** *Für $f, F\colon \mathbb{N} \to \mathbb{C}$ sind äquivalent:*

(1) $F(n) = \sum_{d|n} f(d)$ *für alle* $n \in \mathbb{N}$.

(2) $f(n) = \sum_{d|n} \mu(d) F(\frac{n}{d}) = \sum_{d|n} \mu(\frac{n}{d}) F(d)$ *für alle* $n \in \mathbb{N}$.

Beweis.

(1) $\Rightarrow$ (2):

$$\sum_{d|n} \mu(d)F(n/d) \overset{(1)}{=} \sum_{d|n} \sum_{e|\frac{n}{d}} \mu(d)f(e) = \sum_{de|n} \mu(d)f(e) = \sum_{e|n} f(e) \sum_{d|\frac{n}{e}} \mu(d) \overset{I.2.41}{=} f(n).$$

(2) $\Rightarrow$ (1):

$$\sum_{d|n} f(d) \overset{(2)}{=} \sum_{d|n} \sum_{e|d} \mu(d/e)F(e) = \sum_{e|n} F(e) \sum_{d|\frac{n}{e}} \mu(d) \overset{I.2.41}{=} F(n). \qquad \square$$

Beispiel I.2.43. Für $n = \prod_{p\in\mathbb{P}} p^{a_p} \in \mathbb{N}$ gilt

$$\sum_{d|n} \varphi(d) \overset{I.2.20}{=} \prod_{p\in\mathbb{P}} \sum_{k=0}^{a_p} \varphi(p^k) \overset{I.2.37}{=} \prod_{p\in\mathbb{P}} (1 + (p-1) + (p^2-p) + \ldots + (p^{a_p} - p^{a_p-1})) = \prod_{p\in\mathbb{P}} p^{a_p} = n.$$

Für $f = \varphi$ ist also $F = \mathrm{id}_{\mathbb{N}}$ in Satz I.2.42 und man erhält

$$\varphi(n) = \sum_{d|n} \mu(d)\frac{n}{d}$$

für alle $n \in \mathbb{N}$.

3 Gruppen

Definition I.3.1. Eine *Gruppe* ist eine Menge G zusammen mit einer Verknüpfung $\cdot\colon G \times G \to G$, $(x, y) \mapsto x \cdot y$, sodass folgende Eigenschaften gelten:

- $\forall x, y, z \in G : (x \cdot y) \cdot z = x \cdot (y \cdot z)$ (*assoziativ*),
- $\exists e \in G : \forall x \in G : e \cdot x = x$ (*neutrales Element*),
- $\forall x \in G : \exists y \in G : y \cdot x = e$ (*inverses Element*).

Gilt zusätzlich

- $\forall x, y \in G : x \cdot y = y \cdot x$ (*kommutativ*),

so nennt man G *abelsch*. Die *Ordnung* von G ist die Mächtigkeit $|G|$.

Bemerkung I.3.2.

(i) Im Folgenden sei G stets eine Gruppe. Wenn die Verknüpfung klar ist, schreiben wir xy statt $x \cdot y$.

(ii) Für $x \in G$ existieren $y, z \in G$ mit $yx = e = zy$. Es folgt

$$xy = e(xy) = (zy)(xy) = z(yx)y = z(ey) = zy = e$$

und $xe = x(yx) = (xy)x = ex = x$. Ist auch $e' \in G$ ein neutrales Element, so gilt $e' = e'e = e$. Also ist e eindeutig bestimmt und wir schreiben $e = 1_G = 1$. Sei nun $y' \in G$ mit $y'x = e$. Dann ist $y' = y'e = y'(xy) = (y'x)y = ey = y$. Somit hat x genau ein Inverses und wir schreiben $y = x^{-1}$.

(iii) Für $x, y \in G$ ist $\boxed{(x^{-1})^{-1} = x}$ und $\boxed{(xy)^{-1} = y^{-1}x^{-1}}$ (Achtung!).

(iv) Für $x_1, \ldots, x_n \in G$ spielt die Klammerung in $x_1 \ldots x_n$ keine Rolle: Für $n = 3$ folgt dies aus der Assoziativität. Gilt die Behauptung bereits für $n - 1$, so hat jede Klammerung von $x_1 \ldots x_n$ die Form $(x_1 \ldots x_k)(x_{k+1} \ldots x_n)$ mit $1 \leq k < n$. Nun gilt

$$x_1(x_2 \ldots x_n) = x_1(x_2(x_3 \ldots x_n)) = (x_1x_2)(x_3 \ldots x_n) = \ldots = (x_1 \ldots x_{n-1})x_n.$$

(v) Für $x \in G$ und $k \in \mathbb{Z}$ definieren wir

$$x^k := \begin{cases} 1_G & \text{falls } k = 0, \\ x \ldots x \text{ (k Faktoren)} & \text{falls } k > 0, \\ (x^{-1})^{-k} & \text{falls } k < 0. \end{cases}$$

Sicher ist dann $x^m x^n = x^{m+n}$ und $(x^m)^n = x^{mn}$ für $n, m \in \mathbb{Z}$. Im Fall $G = \{x^i : i \in \mathbb{Z}\}$ nennt man G *zyklisch*. Wegen $x^m x^n = x^{m+n} = x^n x^m$ ist G dann auch abelsch.

Beispiel I.3.3.

(i) Die *triviale* Gruppe $G = \{1\}$. Wir schreiben dann auch $G = 1$.

(ii) Die ganzen Zahlen $\mathbb{Z}$ bilden bzgl. Addition eine abelsche Gruppe. Das neutrale Element ist dabei 0. Dagegen ist $\mathbb{Z}$ bzgl. Multiplikation *keine* Gruppe (2 hat kein Inverses).

(iii) Für jeden Körper K ist $K^\times := K \setminus \{0\}$ eine abelsche Gruppe bzgl. Multiplikation.

(iv) Die invertierbaren $n \times n$-Matrizen über einem Körper K bilden bzgl. Matrizenmultiplikation die *allgemeine lineare Gruppe* $\mathrm{GL}(n, K)$ vom *Grad* n über K. Das neutrale Element ist die Einheitsmatrix 1_n. Es gilt $\mathrm{GL}(1, K) = K^\times$. Für $n \geq 2$ ist $\mathrm{GL}(n, K)$ nichtabelsch.

(v) Die Bijektionen einer Menge Ω auf sich selbst bilden bzgl. Komposition von Abbildungen die *symmetrische Gruppe* $\mathrm{Sym}(\Omega)$ mit neutralem Element id_Ω. Die Elemente von $\mathrm{Sym}(\Omega)$ heißen *Permutationen*. Für $\Omega = \{1, \ldots, n\}$ schreiben wir $S_n := \mathrm{Sym}(\Omega)$ und nennen n den *Grad* von S_n. Es gilt $|S_n| = n!$.

(vi) Für Gruppen $G_1, \ldots, G_n$ wird das kartesische Produkt $G_1 \times \ldots \times G_n$ durch

$$(g_1, \ldots, g_n) \cdot (h_1, \ldots, h_n) := (g_1 h_1, \ldots, g_n h_n)$$

für $g_i, h_i \in G_i$ zu einer Gruppe mit neutralem Element $(1_{G_1}, \ldots, 1_{G_n})$ (nachrechnen). Man nennt $G_1 \times \ldots \times G_n$ das *direkte Produkt* von $G_1, \ldots, G_n$. Im Fall $G_1 = \ldots = G_n$ schreiben wir auch G_1^n statt $G_1 \times \ldots \times G_n$.

Definition I.3.4. Eine nichtleere Teilmenge $H \subseteq G$ mit $xy^{-1} \in H$ für alle $x, y \in H$ heißt *Untergruppe* von G. Wir schreiben dann $H \leq G$ und $H < G$, falls H eine *echte* Untergruppe ist, d. h. $H \neq G$. Die Mengen der Form $gH := \{gh : h \in H\}$ nennt man *(Links)nebenklassen* von H in G. Die Menge aller Linksnebenklassen ist $G/H := \{gH : g \in G\}$ und $|G : H| := |G/H|$ ist der *Index* von H in G.

Bemerkung I.3.5. Sei $H \leq G$. Dann existiert ein $x \in H$. Also ist auch $1_G = xx^{-1} \in H$ und $x^{-1} = 1_G x^{-1} \in H$. Für $x, y \in H$ ist außerdem $xy = x(y^{-1})^{-1} \in H$. Dies zeigt, dass H mit der eingeschränkten Verknüpfung selbst eine Gruppe ist. Ist G abelsch, so auch H. Aus $K \leq H$ folgt $K \leq G$, d. h. $\leq$ ist transitiv und damit eine (partielle) Ordnungsrelation.

Beispiel I.3.6.

(i) Jede Gruppe G besitzt die Untergruppen 1 und G.

(ii) Für jede Familie von Untergruppen $H_i \leq G$ $(i \in I)$ ist $\bigcap_{i \in I} H_i \leq G$ (nachrechnen).

(iii) Für $U \subseteq G$ ist

$$\langle U \rangle := \bigcap_{U \subseteq H \leq G} H$$

die von U *erzeugte* Untergruppe (die „kleinste“ Untergruppe, die U enthält). Offenbar enthält $\langle U \rangle$ alle Elementen der Form $x_1^{\pm 1} \ldots x_n^{\pm 1}$ mit $x_1, \ldots, x_n \in U$. Umgekehrt bilden diese Elemente selbst eine Untergruppe, die dann mit $\langle U \rangle$ übereinstimmen muss. Im Fall $\langle U \rangle = G$ ist U ein *Erzeugendensystem* von G. Wir schreiben auch $\langle x_1, \ldots, x_n \rangle := \langle \{x_1, \ldots, x_n\} \rangle$. Die Untergruppen der Form $\langle x \rangle$ sind zyklisch. Man nennt dann $|\langle x \rangle|$ die *Ordnung* von x.

(iv) Für $n \in \mathbb{Z}$ ist $n\mathbb{Z} = \langle n \rangle \leq \mathbb{Z}$. Die Linksnebenklassen sind dann genau die Restklassen modulo n (beachte: die Verknüpfung ist $+$).

(v) Die oberen Dreiecksmatrizen in $\mathrm{GL}(n, K)$ bilden eine Untergruppe.

(vi) Für $n \leq m$ gilt $S_n \leq S_m$.

Lemma I.3.7. *Für $x \in G$ gilt*

$$|\langle x\rangle| = \inf\{n \in \mathbb{N} : x^n = 1\},$$

wobei $\inf \varnothing := \infty$. *Im Fall* $n := |\langle x\rangle| < \infty$ *gilt*

(i) $x^k = 1 \iff n \mid k$ *für* $k \in \mathbb{Z}$.

(ii) $x^k = x^l \iff k \equiv l \pmod{n}$ *für* $k, l \in \mathbb{Z}$.

(iii) $\boxed{|\langle x^k\rangle| = \dfrac{n}{\mathrm{ggT}(n,k)}}$ *für* $k \in \mathbb{Z}$.

Beweis. Sei zunächst $n \in \mathbb{N}$ minimal mit $x^n = 1$. Für $k \in \mathbb{Z}$ existieren $q, r \in \mathbb{Z}$ mit $k = qn + r$ und $0 \le r < n$ (Division mit Rest). Dann ist $x^k = x^{qn+r} = (x^n)^q x^r = 1^q x^r = x^r$ und es folgt $\langle x\rangle = \{1, x, x^2, \ldots, x^{n-1}\}$. Nehmen wir an es existieren $0 \le k < l < n$ mit $x^k = x^l$. Dann wäre $x^{l-k} = 1$ mit $1 \le l - k < n$ im Widerspruch zur Wahl von n. Dies zeigt $|\langle x\rangle| = n$.

Sei nun $x^n \neq 1$ für alle $n \in \mathbb{N}$. Für $1 \le k < l$ ist dann $x^k \neq x^l$, denn anderenfalls wäre $x^{l-k} = 1$. Dies zeigt, dass die Elemente $x, x^2, \ldots$ paarweise verschiedenen sind. Insbesondere ist $|\langle x\rangle| = \infty$.

(i) Division mit Rest liefert $k = qn + r$ mit $q, r \in \mathbb{Z}$ und $0 \le r < n$. Wie oben ist $x^k = x^r$ und es folgt $x^k = 1 \iff r = 0 \iff n \mid k$.

(ii) Nach (i) ist $x^k = x^l \iff x^{k-l} = 1 \iff n \mid k - l \iff k \equiv l \pmod{n}$.

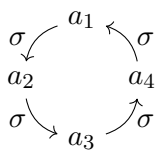
(iii) Es gilt

$$\begin{aligned} |\langle x^k\rangle| &= \inf\{m \in \mathbb{N} : x^{km} = (x^k)^m = 1\} \overset{\text{(i)}}{=} \inf\{m \in \mathbb{N} : km \equiv 0 \pmod{n}\} \\ &\overset{I.2.26}{=} \inf\left\{m \in \mathbb{N} : m \equiv 0 \pmod{\frac{n}{\mathrm{ggT}(n,k)}}\right\} = \frac{n}{\mathrm{ggT}(n,k)}. \end{aligned}$$

□

Bemerkung I.3.8 (Wiederholung Lineare Algebra)**.** Für $k \ge 2$ nennt man $\sigma \in S_n$ einen (k-)*Zyklus* (oder Zyklus der *Länge* k), falls paarweise verschiedene $1 \le a_1, \ldots, a_k \le n$ existieren, sodass

$$\sigma(x) = \begin{cases} a_{i+1} & \text{falls } x = a_i \text{ mit } i < k, \\ a_1 & \text{falls } x = a_k, \\ x & \text{sonst} \end{cases}$$



gilt. Man schreibt dann $\sigma = (a_1, \ldots, a_k)$. Diese Schreibweise ist eindeutig bis auf „Rotation“, d. h.

$$\sigma = (a_2, \ldots, a_k, a_1) = \ldots = (a_k, a_1, \ldots, a_{k-1}).$$

Außerdem ist $(a_1, \ldots, a_k)^{-1} = (a_k, a_{k-1}, \ldots, a_1)$.

Zyklen der Länge 2 heißen *Transpositionen*. Zyklen $\sigma = (a_1, \ldots, a_k)$ und $\tau = (b_1, \ldots, b_l)$ heißen *disjunkt*, falls

$$\{a_1, \ldots, a_k\} \cap \{b_1, \ldots, b_l\} = \varnothing.$$

Gegebenenfalls gilt $\sigma\tau = \tau\sigma$. Bekanntlich ist jede Permutation $\sigma \in S_n$ ein Produkt von paarweise disjunkten Zyklen $\sigma = \sigma_1 \ldots \sigma_s$, die bis auf die Reihenfolge eindeutig bestimmt sind. Hat σ_i Länge l_i, so nennt man $(l_1, \ldots, l_s)$ den *Zyklentyp* von σ, wobei man $l_1 \ge \ldots \ge l_s$ annehmen kann. Wegen $(a_1, \ldots, a_k) = (a_1, a_2)(a_2, a_3) \ldots (a_{k-1}, a_k)$ (Abbildungen von rechts nach links auswerten) ist jede Permutation ein Produkt von (nicht unbedingt disjunkten) Transpositionen.

Lemma I.3.9. *Für $\sigma \in S_n$ mit Zyklentyp $(l_1, \ldots, l_s)$ gilt*

$$\boxed{|\langle\sigma\rangle| = \mathrm{kgV}(l_1, \ldots, l_s).}$$

Beweis. Sei $\sigma = \sigma_1 \ldots \sigma_s$ mit disjunkten Zyklen σ_i der Länge l_i. Offenbar ist $|\langle\sigma_i\rangle| = l_i$ für $i = 1, \ldots, s$. Für $k \in \mathbb{N}$ sind auch $\sigma_1^k, \ldots, \sigma_s^k$ paarweise disjunkt und daher vertauschbar. Mit Lemma I.3.7 folgt

$$\begin{aligned}\sigma^k = 1 &\iff \sigma_1^k \ldots \sigma_s^k = 1 \iff \sigma_1^k = \ldots = \sigma_s^k = 1\\ &\iff l_1 \mid k, \ldots, l_s \mid k \iff \mathrm{kgV}(l_1, \ldots, l_s) \mid k.\end{aligned}$$

Dies zeigt die Behauptung. □

Beispiel I.3.10.

(i) In S_6 ist $\begin{pmatrix}1&2&3&4&5&6\\4&1&6&2&5&3\end{pmatrix} = (1,4,2)(3,6)$ ein Element der Ordnung 6. Andererseits besitzt S_6 kein Element der Ordnung 10, denn dafür braucht man mindestens sieben Ziffern.

(ii) In S_5 gilt $(2,5,3,1)(3,1,6) = (1,6)(2,5,3)$.

(iii) Es gilt $S_3 = \big\{1, (1,2), (1,3), (2,3), (1,2,3), (1,3,2)\big\}$. Wegen $(1,2)(1,3) = (1,3,2) \neq (1,2,3) = (1,3)(1,2)$ ist S_n genau dann abelsch, wenn $n \leq 2$.

Satz I.3.11 (Lagrange)**.** *Für jede Gruppe G und $H \leq G$ gilt*

$$\boxed{|G| = |G : H||H|.}$$

Insbesondere sind $|H|$ und $|G : H|$ Teiler von $|G|$, falls $|G| < \infty$.

Beweis. Für $x, y \in G$ sei

$$x \sim y :\iff x^{-1}y \in H.$$

Wegen $1 \in H$ ist $x \sim x$. Für $x \sim y$ gilt $y^{-1}x = (x^{-1}y)^{-1} \in H$ und $y \sim x$. Aus $x \sim y \sim z$ folgt schließlich $x^{-1}z = (x^{-1}y)(y^{-1}z) \in H$ und $x \sim z$. Also ist $\sim$ eine Äquivalenzrelation. Wegen

$$x \sim y \iff x^{-1}y \in H \iff y \in xH$$

sind die Äquivalenzklassen genau die Linksnebenklassen von H in G. Insbesondere ist G die disjunkte Vereinigung aller Linksnebenklassen. Da die Abbildung $H \to xH$, $h \mapsto xh$ eine Bijektion ist (mit Umkehrabbildung $g \mapsto x^{-1}g$), sind alle Linksnebenklassen gleich groß. Dies zeigt

$$|G| = \Big|\bigcup_{gH \in G/H} gH\Big| = \sum_{gH \in G/H} |gH| = |G : H||H|.$$ □

Bemerkung I.3.12.

(i) Der Beweis zeigt

$$\boxed{xH = yH \iff x^{-1}y \in H}$$

für alle $x, y \in G$. Man kann völlig analog $x \sim y :\iff xy^{-1} \in H$ definieren und erhält dann die *Rechtsnebenklassen* Hg von H in G als Äquivalenzklassen. Der Beweis zeigt, dass es genau so viele Links- wie Rechtsnebenklassen gibt. Im Allgemeinen ist aber $gH \neq Hg$.

(ii) Für $|G| < \infty$ und $x \in G$ ist $|\langle x \rangle|$ ein Teiler von $|G|$. Nach Lemma I.3.7 folgt $x^{|G|} = 1$.

Definition I.3.13. Für $X, Y \subseteq G$ sei $XY := \{xy : x \in X,\, y \in Y\}$.

Lemma I.3.14. *Für $U, V, W \leq G$ gilt*

(i) $U \subseteq V \Longrightarrow |G : U| = |G : V||V : U|$.

(ii) $UV \leq G \iff UV = VU$.

(iii) $\boxed{|UV| = |U : U \cap V||V| = |V : U \cap V||U|.}$

(iv) $U \subseteq W \Longrightarrow UV \cap W = U(V \cap W)$ (DEDEKIND-*Identität*).

Beweis. Aufgabe I.19. □

Bemerkung I.3.15. Für $U, V \leq G$ ist nicht unbedingt $UV \leq G$ (Aufgabe I.21)!

Definition I.3.16. Eine Untergruppe $H \leq G$ heißt *Normalteiler* von G (oder *normal* in G), falls $gH = Hg$ für alle $g \in G$ gilt. Gegebenenfalls schreiben wir $H \trianglelefteq G$ und $H \triangleleft G$, falls $H < G$.

Beispiel I.3.17.

(i) Stets sind 1 und G normal in G.

(ii) Untergruppen von abelschen Gruppen sind stets normal. Insbesondere ist $n\mathbb{Z} \trianglelefteq \mathbb{Z}$.

(iii) Untergruppen $H \leq G$ mit Index 2 sind normal, denn für $g \in G \setminus H$ ist $gH = G \setminus H = Hg$.

(iv) Für $N, M \trianglelefteq G$ und $g \in G$ ist $g(N \cap M) = gN \cap gM = Ng \cap Mg = (N \cap M)g$ und $N \cap M \trianglelefteq G$. Außerdem ist
$$NM = \bigcup_{x \in N} xM = \bigcup_{x \in N} Mx = MN$$
und Lemma I.3.14(ii) zeigt $NM \leq G$. Wegen $gNM = NgM = NMg$ für $g \in G$ ist auch $NM \trianglelefteq G$.

(v) Wegen
$$(1,3)S_2 = \{(1,3), \underbrace{(1,3)(1,2)}_{=(1,2,3)}\} \neq \{(1,3), \underbrace{(1,2)(1,3)}_{=(1,3,2)}\} = S_2(1,3)$$
gilt $S_2 \not\trianglelefteq S_3$.

(vi) Aus $M \trianglelefteq N \trianglelefteq G$ folgt nicht unbedingt $M \trianglelefteq G$ (Aufgabe I.21), d. h. $\trianglelefteq$ ist nicht transitiv.

Lemma I.3.18. *Genau dann ist $H \leq G$ normal in G, falls $ghg^{-1} \in H$ für alle $g \in G$ und $h \in H$ gilt.*

Beweis. Sei $H \trianglelefteq G$, $g \in G$ und $h \in H$. Dann ist $ghg^{-1} \in gHg^{-1} = Hgg^{-1} = H$. Ist umgekehrt $ghg^{-1} \in H$ für alle $g \in G$ und $h \in H$, so folgt
$$gH = \{ghg^{-1}g : h \in H\} \subseteq Hg = \{gg^{-1}hg : h \in H\} = \{gg^{-1}h(g^{-1})^{-1} : h \in H\} \subseteq gH.$$
Dies zeigt $H \trianglelefteq G$. □

Satz I.3.19. *Sei G eine Gruppe und $N \trianglelefteq G$. Dann wird G/N mit der Verknüpfung*

$$xN \cdot yN := xyN$$

für $xN, yN \in G/N$ zu einer Gruppe mit neutralem Element $1N = N$.

Beweis. Wir müssen zunächst zeigen, dass die Verknüpfung nicht von der Wahl der Repräsentanten x und y abhängt. Sei dazu $xN = x'N$ und $yN = y'N$. Wegen $N \trianglelefteq G$ ist dann

$$x'y'N = x'yN = x'Ny = xNy = xyN.$$

Also ist $xN \cdot yN = xyN$ wohldefiniert. Für $xN, yN, zN \in G/N$ gilt

$$(xN \cdot yN) \cdot zN = xyN \cdot zN = (xy)zN = x(yz)N = xN \cdot yzN = xN \cdot (yN \cdot zN).$$

Außerdem ist $1N \cdot xN = 1xN = xN$ sowie $x^{-1}N \cdot xN = x^{-1}xN = 1N$. □

Definition I.3.20. In der Situation von Satz I.3.19 nennt man G/N die *Faktorgruppe* von G nach N.

Bemerkung I.3.21. Ist G abelsch, so auch G/N.

Beispiel I.3.22. Für $n \in \mathbb{N}$ ist $\mathbb{Z}/n\mathbb{Z}$ eine Gruppe der Ordnung n (vgl. Satz I.2.23).

Definition I.3.23. Eine Abbildung $f\colon G \to H$ für Gruppen G und H heißt

- *Homomorphismus*, falls $f(xy) = f(x)f(y)$ für $x, y \in G$ gilt.
- *Monomorphismus*, falls f ein injektiver Homomorphismus ist.
- *Epimorphismus*, falls f ein surjektiver Homomorphismus ist.
- *Isomorphismus*, falls f ein bijektiver Homomorphismus ist.
- *Endomorphismus*, falls f ein Homomorphismus mit $G = H$ ist.
- *Automorphismus*, falls f ein bijektiver Endomorphismus ist.

Bemerkung I.3.24.

(i) Für einen Homomorphismus $f\colon G \to H$ gilt

$$f(1_G) = f(1_G)f(1_G)f(1_G)^{-1} = f(1_G1_G)f(1_G)^{-1} = f(1_G)f(1_G)^{-1} = 1_H$$

und

$$f(x^{-1}) = f(x^{-1})f(x)f(x)^{-1} = f(x^{-1}x)f(x)^{-1} = f(1_G)f(x)^{-1} = 1_Hf(x)^{-1} = f(x)^{-1}$$

für $x \in G$. Hat x endliche Ordnung, so ist $|\langle f(x)\rangle|$ ein Teiler von $|\langle x\rangle|$, denn $f(x)^{|\langle x\rangle|} = f(x^{|\langle x\rangle|}) = f(1_G) = 1_H$ (Lemma I.3.7).

(ii) Für $U \leq G$ und $V \leq H$ ist $f(U) \leq H$ und $f^{-1}(V) := \{x \in G : f(x) \in V\} \leq G$ (nachrechnen). Insbesondere ist $f(G) \leq H$. Im Fall $U \trianglelefteq G$ gilt $f(U) \trianglelefteq f(G)$, aber nicht unbedingt $f(U) \trianglelefteq H$ (Aufgabe I.21)! Für $V \trianglelefteq H$ gilt stets $f^{-1}(V) \trianglelefteq G$. Insbesondere ist

$$\mathrm{Ker}(f) := f^{-1}(1) \trianglelefteq G.$$

Man nennt $\mathrm{Ker}(f)$ den *Kern* von f.

(iii) Ist $g\colon H \to K$ ein weiterer Homomorphismus, so ist auch $g \circ f\colon G \to K$ ein Homomorphismus, denn

$$(g \circ f)(xy) = g(f(xy)) = g(f(x)f(y)) = g(f(x))g(f(y)) = (g \circ f)(x)(g \circ f)(y)$$

für $x, y \in G$.

(iv) Ist $f\colon G \to H$ ein Isomorphismus, so auch $f^{-1}\colon H \to G$, denn

$$f^{-1}(xy) = f^{-1}(f(f^{-1}(x))f(f^{-1}(y))) = f^{-1}(f(f^{-1}(x)f^{-1}(y))) = f^{-1}(x)f^{-1}(y)$$

für $x, y \in H$. Man sagt dann G und H sind *isomorph* und schreibt $G \cong H$. Offenbar ist die Isomorphie von Gruppen eine Äquivalenzrelation. Da isomorphe Gruppen die gleichen Eigenschaften haben, interessiert man sich in der Regel nur für Gruppen bis auf Isomorphie.

(v) Nach (iii) und (iv) bilden die Automorphismen von G eine Untergruppe $\mathrm{Aut}(G) \leq \mathrm{Sym}(G)$. Man nennt $\mathrm{Aut}(G)$ die *Automorphismengruppe* von G.

Beispiel I.3.25.

(i) Es existiert stets der triviale Homomorphismus $G \to H$, $g \mapsto 1_H$ und der triviale Automorphismus $\mathrm{id}_G\colon G \to G$, $g \mapsto g$ (neutrales Element von $\mathrm{Aut}(G)$).

(ii) Für $H \leq G$ ist die Inklusionsabbildung $H \to G$, $h \mapsto h$ ein Monomorphismus.

(iii) Für $N \trianglelefteq G$ gibt es den *kanonischen* Epimorphismus $G \to G/N$, $g \mapsto gN$ mit Kern N.

(iv) Für jede Körper K und $n \in \mathbb{N}$ ist $\det\colon \mathrm{GL}(n, K) \to K^\times$ ein Epimorphismus (Lineare Algebra). Man nennt

$$\mathrm{SL}(n, K) := \mathrm{Ker}(\det) = \{A \in \mathrm{GL}(n, K) : \det(A) = 1\} \trianglelefteq \mathrm{GL}(n, K)$$

die *spezielle lineare Gruppe* vom *Grad* n über K.

(v) Die Exponentialfunktion $\exp\colon (\mathbb{R}, +) \to \mathbb{R}^\times$, $a \mapsto e^a$ ist ein Monomorphismus, denn $e^{a+b} = e^a e^b$ für $a, b \in \mathbb{R}$.

Satz I.3.26. *Für $n \in \mathbb{N}$ existiert ein Homomorphismus $\mathrm{sgn}\colon S_n \to \{\pm 1\}$ mit*

$$\boxed{\mathrm{sgn}(\sigma) = (-1)^{l_1 + \ldots + l_s - s}}$$

für $\sigma \in S_n$ mit Zyklentyp $(l_1, \ldots, l_s)$.

Beweis. Wir definieren

$$\mathrm{sgn}(\sigma) := \prod_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i} \in \{\pm 1\}$$

für $\sigma \in S_n$. Für $\sigma, \tau \in S_n$ gilt dann

$$\begin{aligned}\mathrm{sgn}(\sigma\tau) &= \prod_{i<j} \frac{\sigma(\tau(j)) - \sigma(\tau(i))}{j - i} = \prod_{i<j} \frac{\sigma(\tau(j)) - \sigma(\tau(i))}{\tau(j) - \tau(i)} \frac{\tau(j) - \tau(i)}{j - i} \\ &= \prod_{i<j} \frac{\sigma(\tau(j)) - \sigma(\tau(i))}{\tau(j) - \tau(i)} \prod_{i<j} \frac{\tau(j) - \tau(i)}{j - i} = \mathrm{sgn}(\sigma)\,\mathrm{sgn}(\tau).\end{aligned}$$

Also ist sgn ein Homomorphismus. Für jede Transposition $\sigma = (s,t)$ mit $s < t$ gilt

$$\operatorname{sgn}(\sigma) = \frac{s-t}{t-s} \prod_{s<j\neq t} \frac{j-t}{j-s} \prod_{s\neq i<t} \frac{s-i}{t-i}.$$

Die Faktoren sind genau dann negativ, wenn $s < j < t$ bzw. $s < i < t$ gilt. Man erhält $\operatorname{sgn}(\sigma) = -(-1)^{2(t-s-1)} = -1$. Da sich jeder k-Zyklus $\sigma = (a_1, \ldots, a_k)$ als Produkt von $k-1$ Transpositionen $\sigma = (a_1, a_2)(a_2, a_3)\ldots(a_{k-1}, a_k)$ schreiben lässt, gilt $\operatorname{sgn}(\sigma) = (-1)^{k-1}$. Daraus folgt die Behauptung. □

Definition I.3.27. Man nennt sgn *Signum* (oder *Vorzeichen*) und

$$A_n := \operatorname{Ker}(\operatorname{sgn}) = \{\sigma \in S_n : \operatorname{sgn}(\sigma) = 1\} \trianglelefteq S_n$$

die *alternierende Gruppe* vom *Grad n*. Die Elemente in A_n (bzw. $S_n \setminus A_n$) heißen *gerade* (bzw. *ungerade*) Permutationen. Beachte: Ein Zyklus gerader Länge ist ungerade.

Lemma I.3.28. *Genau dann ist ein Homomorphismus $f\colon G \to H$ injektiv, wenn* $\operatorname{Ker}(f) = 1$.

Beweis. Ist f injektiv, so gilt $f(x) = 1 = f(1)$ genau dann, wenn $x = 1$. Dies zeigt $\operatorname{Ker}(f) = 1$. Sei umgekehrt $\operatorname{Ker}(f) = 1$ und $x, y \in G$ mit $f(x) = f(y)$. Dann ist $f(y^{-1}x) = f(y)^{-1}f(x) = 1$ und $y^{-1}x \in \operatorname{Ker}(f) = 1$. Dies zeigt $x = y$ und f ist injektiv. □

Satz I.3.29.

(i) (*Homomorphiesatz*[1]) *Für jeden Homomorphismus $f\colon G \to H$ gilt*

$$\boxed{G/\operatorname{Ker}(f) \cong f(G).}$$

(ii) (*Korrespondenzsatz*) *Für $N \trianglelefteq G$ induziert der kanonische Epimorphismus $G \to G/N$ eine Bijektion zwischen der Menge der Untergruppen $H \leq G$ mit $N \leq H$ und der Menge der Untergruppen von G/N.*

(iii) (*1. Isomorphiesatz*) *Für $H \leq G$ und $N \trianglelefteq G$ gilt $N \trianglelefteq HN \leq G$, $H \cap N \trianglelefteq H$ und*

$$\boxed{HN/N \cong H/H \cap N.}$$

(iv) (*2. Isomorphiesatz*) *Für $N \trianglelefteq G$ und $N \leq H \leq G$ ist $H \trianglelefteq G$ genau dann, wenn $H/N \trianglelefteq G/N$. Gegebenenfalls ist*

$$\boxed{G/H \cong (G/N)/(H/N).}$$

Beweis.

(i) Sei $x, y \in G$ und

$$\begin{aligned} F\colon G/\operatorname{Ker}(f) &\to f(G),\\ x\operatorname{Ker}(f) &\mapsto f(x). \end{aligned}$$

[1] In der englischsprachigen Literatur wird der Homomorphiesatz als „first isomorphism theorem“ bezeichnet und die Nummerierung der Isomorphiesätze erhöht sich entsprechend.

Wegen

$$x\mathrm{Ker}(f) = y\mathrm{Ker}(f) \overset{I.3.12}{\iff} y^{-1}x \in \mathrm{Ker}(f) \iff f(y)^{-1}f(x) = f(y^{-1}x) = 1 \iff f(x) = f(y)$$

ist F wohldefiniert und injektiv. Nach Definition ist F auch surjektiv. Schließlich ist

$$F\big(x\mathrm{Ker}(f) \cdot y\mathrm{Ker}(f)\big) = F(xy\mathrm{Ker}(f)) = f(xy) = f(x)f(y) = F\big(x\mathrm{Ker}(f)\big)F\big(y\mathrm{Ker}(f)\big).$$

Also ist F ein bijektiver Homomorphismus, d. h. ein Isomorphismus.

(ii) Sei $f\colon G \to G/N$ der kanonische Epimorphismus, $\mathcal{H} := \{H \leq G : N \leq H\}$ und $\mathcal{K} := \{U \leq G/N\}$. Für $H \in \mathcal{H}$ ist sicher $H/N = f(H) \in \mathcal{K}$. Für $U \in \mathcal{K}$ gilt umgekehrt $N \leq f^{-1}(U) \leq G$, denn $f(N) = 1 \leq U$. Also ist $f^{-1}(U) \in \mathcal{H}$ und man erhält Abbildungen

$$\begin{aligned} \varphi\colon \mathcal{H} &\to \mathcal{K}, & \psi\colon \mathcal{K} &\to \mathcal{H}, \\ H &\mapsto f(H), & U &\mapsto f^{-1}(U). \end{aligned}$$

Sei $H \in \mathcal{H}$ und $x \in f^{-1}(f(H))$. Dann existiert $h \in H$ mit $f(x) = f(h)$. Es folgt $f(h^{-1}x) = f(h)^{-1}f(x) = 1$ und $x = h(h^{-1}x) \in H\mathrm{Ker}(f) = HN = H$. Dies zeigt $f^{-1}(f(H)) = H$ und $\psi \circ \varphi = \mathrm{id}_{\mathcal{H}}$. Da f surjektiv ist, gilt auch $f(f^{-1}(U)) = U$ für alle $U \in \mathcal{K}$, d. h. $\varphi \circ \psi = \mathrm{id}_{\mathcal{K}}$. Daher sind φ und ψ zueinander inverse Bijektionen.

(iii) Wir betrachten die Abbildung $f\colon H \to G/N$, $h \mapsto hN$. Wegen $f(xy) = xyN = xNyN = f(x)f(y)$ für $x, y \in H$ ist f ein Homomorphismus. Für $h \in H$ gilt $f(h) = 1 \iff hN = N \iff h \in H \cap N$. Dies zeigt $\mathrm{Ker}(f) = H \cap N \trianglelefteq H$ und (i) liefert $H/H \cap N = H/\mathrm{Ker}(f) \cong f(H) = HN/N \leq G/N$. Aus (ii) folgt $HN \leq G$.

(iv) Nach (ii) ist $H/N \leq G/N$. Für $g \in G$ und $h \in H$ gilt

$$ghg^{-1} \in H \iff (gN)(hN)(gN)^{-1} = ghg^{-1}N \in H/N.$$

Es folgt $H \trianglelefteq G \iff H/N \trianglelefteq G/N$ nach Lemma I.3.18. Sei nun $H \trianglelefteq G$ und $f\colon G/N \to G/H$, $gN \mapsto gH$. Für $x, y \in G$ gilt

$$xN = yN \Longrightarrow y^{-1}x \in N \leq H \Longrightarrow xH = yH.$$

Daher ist f wohldefiniert. Offenbar ist f ein Epimorphismus mit $\mathrm{Ker}(f) = \{gN \in G/N : gH = H\} = H/N$. Also folgt $(G/N)/(H/N) = (G/N)/\mathrm{Ker}(f) \cong f(G/N) = G/H$ aus (i). □

Beispiel I.3.30.

(i) Der Homomorphiesatz für $\det\colon \mathrm{GL}(n, K) \to K^\times$ zeigt $\mathrm{GL}(n, K)/\mathrm{SL}(n, K) \cong K^\times$.

(ii) Für $n \geq 2$ ist $\mathrm{sgn}\colon S_n \to \{\pm 1\}$ surjektiv wegen $\mathrm{sgn}((1, 2)) = -1$. Es folgt $S_n/A_n \cong \{\pm 1\}$ und $|A_n| = n!/2$.

(iii) Für $n, m \in \mathbb{N}$ mit $n \mid m$ gilt $m\mathbb{Z} \leq n\mathbb{Z}$ sowie $(\mathbb{Z}/m\mathbb{Z})/(n\mathbb{Z}/m\mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z}$.

Satz I.3.31. *Für jede zyklische Gruppe G existiert genau ein $n \in \mathbb{N}_0$ mit $G \cong \mathbb{Z}/n\mathbb{Z}$.*

Beweis. Sei $G = \langle x \rangle$ und $f\colon \mathbb{Z} \to G$, $k \mapsto x^k$. Wegen $f(a + b) = x^{a+b} = x^a x^b = f(a)f(b)$ für $a, b \in \mathbb{Z}$ ist f ein Epimorphismus mit

$$\mathrm{Ker}(f) = \{k \in \mathbb{Z} : x^k = 1\} = \begin{cases} 0\mathbb{Z} & \text{falls } |G| = \infty, \\ n\mathbb{Z} & \text{falls } |G| = n \end{cases}$$

nach Lemma I.3.7. Die Behauptung folgt nun aus dem Homomorphiesatz. □

Definition I.3.32. Nach Satz I.3.31 gibt es im Wesentlichen nur eine zyklische Gruppe für jede Ordnung n. Diese bezeichnen wir mit C_n (das ist kürzer als $\mathbb{Z}/n\mathbb{Z}$).

Beispiel I.3.33. Sei G eine Gruppe mit Primzahlordnung p. Für $x \in G \setminus \{1\}$ gilt dann $\langle x \rangle = G$ nach Lagrange. Also ist $G \cong C_p$.

Satz I.3.34.

(i) Für teilerfremde $n, m \in \mathbb{N}$ gilt $\boxed{C_n \times C_m \cong C_{nm}.}$

(ii) Für jedes $d \mid n$ besitzt C_n genau eine Untergruppe (und genau eine Faktorgruppe) der Ordnung d. Diese ist zu C_d isomorph.

Beweis.

(i) Nach dem chinesischen Restsatz ist der Homomorphismus $f\colon \mathbb{Z} \to (\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$, $a \mapsto (a + n\mathbb{Z}, a + m\mathbb{Z})$ surjektiv. Dabei gilt

$$\operatorname{Ker}(f) = \{a \in \mathbb{Z} : a \in n\mathbb{Z} \cap m\mathbb{Z} = \operatorname{kgV}(n, m)\mathbb{Z} = mn\mathbb{Z}\} = mn\mathbb{Z}.$$

Der Homomorphiesatz zeigt $C_{nm} \cong \mathbb{Z}/mn\mathbb{Z} \cong f(\mathbb{Z}) = (\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z}) \cong C_n \times C_m$.

(ii) Sei $\langle x \rangle \cong C_n$. Für $d \mid n$ ist $\langle x^{n/d} \rangle$ eine Untergruppe der Ordnung d nach Lemma I.3.7. Sei umgekehrt $H \leq \langle x \rangle$ mit $|H| = d \mid n$ (Lagrange). Nach Bemerkung I.3.12(ii) gilt $x^{n/d}H = (xH)^{|G/H|} = H$ und $x^{n/d} \in H$. Dies zeigt $H = \langle x^{n/d} \rangle$. Wegen $\langle x \rangle / H = \langle xH \rangle \cong C_{n/d}$ ist auch die Behauptung über Faktorgruppen klar. □

4 Gruppenoperationen

Definition I.4.1. Eine *Operation* von G auf einer nichtleeren Menge Ω ist eine Abbildung $G \times \Omega \to \Omega$, $(x, \omega) \mapsto {}^x\omega$ mit folgenden Eigenschaften:

- $\forall \omega \in \Omega : {}^1\omega = \omega$.
- $\forall x, y \in G,\ \omega \in \Omega : {}^x({}^y\omega) = {}^{xy}\omega$.

Man sagt dann: G *operiert* auf Ω oder Ω ist eine G*-Menge*. Für $\omega \in \Omega$ nennt man

$$ {}^G\omega := \{{}^g\omega : g \in G\} \subseteq \Omega $$

die *Bahn* von ω und $G_\omega := \{g \in G : {}^g\omega = \omega\}$ den *Stabilisator* von ω in G. Man nennt $|{}^G\omega|$ die *Länge* der Bahn. Gilt ${}^G\omega = \Omega$ für ein $\omega \in \Omega$, so heißt die Operation *transitiv*.

Bemerkung I.4.2. Sei Ω eine G-Menge und $f_x \colon \Omega \to \Omega, \omega \mapsto {}^x\omega$ für $x \in G$. Für $x, y \in G$ und $\omega \in \Omega$ gilt dann $(f_x \circ f_y)(\omega) = f_x({}^y\omega) = {}^x({}^y\omega) = {}^{xy}\omega = f_{xy}(\omega)$. Insbesondere ist $f_x \circ f_{x^{-1}} = f_1 = \mathrm{id}_\Omega = f_{x^{-1}} \circ f_x$ und $f_x \in \mathrm{Sym}(\Omega)$. Außerdem ist $f \colon G \to \mathrm{Sym}(\Omega)$, $x \mapsto f_x$ ein Homomorphismus.

Sei nun umgekehrt ein Homomorphismus $f \colon G \to \mathrm{Sym}(\Omega)$ gegeben. Dann erhält man durch

$$ {}^x\omega := (f(x))(\omega) \qquad (x \in G,\ \omega \in \Omega) $$

eine Operation (nachrechnen). Operationen sind also nichts anderes als Homomorphismen in die symmetrische Gruppe. Die Operation heißt *treu* (bzw. *trivial*), falls $\mathrm{Ker}(f) = 1$ (bzw. $\mathrm{Ker}(f) = G$) gilt. Im ersten Fall ist G nach dem Homomorphiesatz zu einer Untergruppe von $\mathrm{Sym}(\Omega)$ isomorph. Man nennt G dann *Permutationsgruppe* auf Ω.

Lemma I.4.3. *Jede G-Menge Ω ist die disjunkte Vereinigung von Bahnen und $G_\omega \leq G$ für alle $\omega \in \Omega$.*

Beweis. Wir zeigen, dass

$$ \alpha \sim \beta \ :\Longleftrightarrow\ \exists g \in G : {}^g\alpha = \beta $$

eine Äquivalenzrelation auf Ω definiert. Wegen ${}^1\alpha = \alpha$ ist $\sim$ reflexiv. Aus ${}^g\alpha = \beta$ folgt ${}^{g^{-1}}\beta = {}^{g^{-1}}({}^g\alpha) = {}^{g^{-1}g}\alpha = {}^1\alpha = \alpha$. Also ist $\sim$ symmetrisch. Sei schließlich ${}^g\alpha = \beta$ und ${}^h\beta = \gamma$ für $g, h \in G$ und $\alpha, \beta, \gamma \in \Omega$. Dann ist ${}^{hg}\alpha = {}^h({}^g\alpha) = {}^h\beta = \gamma$. Daher ist $\sim$ transitiv und eine Äquivalenzrelation. Die Äquivalenzklassen sind genau die Bahnen. Insbesondere ist Ω die disjunkte Vereinigung der Bahnen von G.

Für die zweite Behauptung beobachten wir $1 \in G_\omega \neq \varnothing$. Für $x, y \in G_\omega$ ist

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

Dies zeigt $xy^{-1} \in G_\omega$ und $G_\omega \leq G$. □

Beispiel I.4.4.

(i) Jede Untergruppe $H \leq G$ operiert treu auf G durch Linksmultiplikation, d. h. ${}^h g := hg$ für $g \in G$, $h \in H$ (denn: ${}^1 g = g$, ${}^h({}^k g) = h(kg) = (hk)g = {}^{hk} g$ und ${}^h g = g \iff h = 1$). Die Bahnen sind die Rechtsnebenklassen von H in G. Analog operiert H von rechts durch ${}^h g := gh^{-1}$ (Achtung!) und man erhält die Linksnebenklassen als Bahnen.

(ii) G operiert auf sich selbst durch *Konjugation* ${}^x g := xgx^{-1}$ für $x, g \in G$. Die Bahnen heißen dabei *Konjugationsklassen* und der Stabilisator von $g \in G$ ist der *Zentralisator*

$$\mathrm{C}_G(g) := \{x \in G : gx = xg\}.$$

Die Anzahl $k(G)$ der Konjugationsklassen nennt man die *Klassenzahl* von G. Zwei Elemente in der gleichen Konjugationsklasse nennt man *konjugiert*. Der Kern der Operation ist das *Zentrum*

$$\mathrm{Z}(G) := \{x \in G : \forall y \in G : xy = yx\} \trianglelefteq G$$

von G und das Bild ist die *innere Automorphismengruppe* $\mathrm{Inn}(G) \leq \mathrm{Aut}(G)$ (Aufgabe I.22).

(iii) Analog operiert G durch Konjugation auf der Menge der Untergruppen von G, d. h. ${}^x H := xHx^{-1} \leq G$ für $x \in G$ und $H \leq G$. Die Bahnen heißen auch hier Konjugationsklassen und der Stabilisator von $H \leq G$ ist der *Normalisator*

$$\mathrm{N}_G(H) := \{x \in G : xHx^{-1} = H\}.$$

Dies ist die „größte“ Untergruppe, in der H normal ist (vgl. Aufgabe I.17). Die Bahnen der Länge 1 entsprechen den Normalteilern. Allgemeiner operiert $\mathrm{N}_G(H)$ durch Konjugation auf H mit Kern

$$\mathrm{C}_G(H) := \bigcap_{h \in H} \mathrm{C}_G(h) \trianglelefteq \mathrm{N}_G(H).$$

Satz I.4.5 (Cayley)**.** *Jede endliche Gruppe G ist zu einer Untergruppe von $S_{|G|}$ isomorph.*

Beweis. Nach Beispiel I.4.4(i) operiert G treu durch Linksmultiplikation auf sich selbst. Dies liefert einen Monomorphismus $f\colon G \to \mathrm{Sym}(G)$. Nach dem Homomorphiesatz ist G zu einer Untergruppe von $\mathrm{Sym}(G)$ isomorph. Wir zeigen schließlich $\mathrm{Sym}(G) \cong S_{|G|}$. Sei $|G| = n$ und $F\colon \{1, \ldots, n\} \to G$ eine Bijektion. Dann ist die Abbildung $\Delta\colon S_n \to \mathrm{Sym}(G)$, $\sigma \mapsto F \circ \sigma \circ F^{-1}$ eine Bijektion mit Umkehrabbildung $\tau \mapsto F^{-1} \circ \tau \circ F$. Wegen

$$\Delta(\sigma\tau) = F\sigma\tau F^{-1} = (F\sigma F^{-1})(F\tau F^{-1}) = \Delta(\sigma)\Delta(\tau)$$

ist Δ ein Isomorphismus. □

Bemerkung I.4.6.

(i) Ist $H \leq G$, so operiert G auf G/H durch Linksmultiplikation, d. h. ${}^g(xH) := gxH$ (der Fall $H = 1$ entspricht Satz I.4.5). Für den entsprechenden Homomorphismus $f\colon G \to \mathrm{Sym}(G/H)$ gilt $\mathrm{Ker}(f) \leq H$, denn für $g \in \mathrm{Ker}(f)$ ist $1H = {}^g(1H) = gH$. Die Operation ist außerdem transitiv, denn für jedes $xH \in G/H$ gilt ${}^x(1H) = xH$.

(ii) Der Satz von Cayley hat keine praktische Relevanz, denn $S_{|G|}$ ist sehr viel größer als G. In den meisten Fällen kann man G aber mit Hilfe von (i) in einer kleineren symmetrischen Gruppe einbetten, in der man effizient rechnen kann. Zum Beispiel kann man die

$$43.252.003.274.489.856.000$$

Zustände des $3 \times 3 \times 3$-Zauberwürfels als Untergruppe von S_{48} realisieren.

(iii) Da S_n nur endlich viele Untergruppen besitzt, gibt es auch nur endlich viele Gruppen der Ordnung n bis auf Isomorphie.

Satz I.4.7. *Für jede G-Menge Ω und $\omega \in \Omega$ gilt* $\boxed{|{}^G\omega| = |G : G_\omega|.}$ *Insbesondere ist $|{}^G\omega|$ ein Teiler von $|G|$, falls $|G| < \infty$. Operiert G zusätzlich transitiv, so ist $|\Omega|$ ein Teiler von $|G|$.*

Beweis. Wir zeigen, dass die Abbildung

$$\begin{aligned} F\colon G/G_\omega &\to {}^G\omega, \\ xG_\omega &\mapsto {}^x\omega \end{aligned}$$

wohldefiniert und injektiv ist:

$$xG_\omega = yG_\omega \iff y^{-1}x \in G_\omega \iff {}^{y^{-1}x}\omega = \omega \iff {}^x\omega = {}^y({}^{y^{-1}x}\omega) = {}^y\omega.$$

Offenbar ist F auch surjektiv. Dies zeigt die erste Behauptung. Die letzten beiden Aussagen folgen nach Lagrange. □

Bemerkung I.4.8. Ist $\Delta \subseteq \Omega$ ein Repräsentantensystem für die Bahnen von G auf Ω, so gilt die *Bahnengleichung*

$$\boxed{|\Omega| = \sum_{\delta \in \Delta} |{}^G\delta| = \sum_{\delta \in \Delta} |G : G_\delta|}$$

nach Lemma I.4.3 und Satz I.4.7. Im Spezialfall der Konjugationsoperation erhält man die *Klassengleichung*

$$\boxed{|G| = \sum_{x \in R} |G : \mathrm{C}_G(x)|,}$$

wobei R ein Repräsentantensystem für die Konjugationsklassen von G ist. Für $x \in \mathrm{Z}(G)$ ist $\{x\}$ eine Konjugationsklasse und man erhält $x \in R$ sowie $\mathrm{C}_G(x) = G$. Dies zeigt

$$|G| = |\mathrm{Z}(G)| + \sum_{x \in R \setminus \mathrm{Z}(G)} |G : \mathrm{C}_G(x)|.$$

Beispiel I.4.9. Sei Ω eine G-Menge mit $|G| = 77$ und $|\Omega| = 23$. Nach der Bahnengleichung existieren $a, b, c \in \mathbb{N}_0$ mit $23 = a + 7b + 11c$. Es folgt $a > 0$, d. h. G hat stets einen Fixpunkt auf Ω.

Definition I.4.10. Für eine Primzahl p nennt man G eine *p-Gruppe*, falls $|G| = p^n$ für ein $n \in \mathbb{N}_0$ gilt.

Satz I.4.11. *Für jede p-Gruppe $G \neq 1$ ist $\mathrm{Z}(G) \neq 1$.*

Beweis. Sei R ein Repräsentantensystem für die Konjugationsklassen von G. Die Klassengleichung zeigt

$$0 \equiv |G| = |\mathrm{Z}(G)| + \sum_{x \in R \setminus \mathrm{Z}(G)} |G : \mathrm{C}_G(x)| \equiv |\mathrm{Z}(G)| \pmod{p}.$$

Insbesondere ist $\mathrm{Z}(G) \neq 1$. □

Folgerung I.4.12. *Jede p-Gruppe der Ordnung p^2 ist abelsch.*

Beweis. Sei $|G| = p^2$. Nach Satz I.4.11 ist $|G : \mathrm{Z}(G)| \leq p$. Insbesondere ist $G/\mathrm{Z}(G)$ zyklisch und die Behauptung folgt aus Aufgabe I.22. □

Satz I.4.13 (FRATTINI-Argument[1])**.** *Sei Ω eine G-Menge und $H \leq G$. Operiert H transitiv auf Ω, so gilt $G = HG_\omega$ für alle $\omega \in \Omega$.*

Beweis. Sei $g \in G$ beliebig. Dann existiert ein $h \in H$ mit ${}^g\omega = {}^h\omega$. Also ist $h^{-1}g \in G_\omega$ und $g = h(h^{-1}g) \in HG_\omega$. Umgekehrt ist sicher auch $HG_\omega \subseteq G$. □

Satz I.4.14 (SYLOW)**.** *Sei G eine Gruppe der Ordnung $p^a m$ für eine Primzahl $p \nmid m$ und $a \in \mathbb{N}_0$. Dann gilt:*

(i) Für jedes $b \in \{0, \ldots, a\}$ besitzt G eine Untergruppe der Ordnung p^b. Insbesondere ist die Menge der p-Sylowgruppen $\mathrm{Syl}_p(G) := \{P \leq G : |P| = p^a\}$ nicht leer.

(ii) Jede p-Untergruppe von G ist in einer p-Sylowgruppe enthalten.

(iii) Je zwei p-Sylowgruppen sind in G konjugiert.

(iv) Für $P \in \mathrm{Syl}_p(G)$ ist $|\mathrm{Syl}_p(G)| = |G : \mathrm{N}_G(P)| \equiv 1 \pmod p$. Insbesondere ist $|\mathrm{Syl}_p(G)|$ ein Teiler von m.

Beweis (ROBINSON).

(i) Wir argumentieren durch Induktion nach $|G|$. Im Fall $b = 0$ ist die Behauptung trivial. Sei also $0 < b \leq a$. Sei $R \subseteq G$ ein Repräsentantensystem für die Konjugationsklassen von G. Nehmen wir zunächst an, dass $|G : \mathrm{C}_G(x)| \not\equiv 0 \pmod p$ für ein $x \in R \setminus \mathrm{Z}(G)$ gilt. Dann ist $|\mathrm{C}_G(x)| = p^a m'$ mit $m' < m$. Nach Induktion besitzt $\mathrm{C}_G(x)$ eine Untergruppe der Ordnung p^b und somit auch G. Wir können also $|G : \mathrm{C}_G(x)| \equiv 0 \pmod p$ für alle $x \in R \setminus \mathrm{Z}(G)$ annehmen. Die Klassengleichung zeigt dann

$$0 \equiv |G| = |\mathrm{Z}(G)| + \sum_{x \in R \setminus \mathrm{Z}(G)} |G : \mathrm{C}_G(x)| \equiv |\mathrm{Z}(G)| \pmod p,$$

d. h. $|\mathrm{Z}(G)|$ ist durch p teilbar. Im Fall $\mathrm{Z}(G) < G$ besitzt $\mathrm{Z}(G)$ nach Induktion eine Untergruppe Z der Ordnung p. Sicher ist $Z \trianglelefteq G$ und nach Induktion existiert $P/Z \leq G/Z$ mit $|P/Z| = p^{b-1}$ (Korrespondenzsatz). Offenbar ist dann $P \leq G$ mit $|P| = |P/Z||Z| = p^b$. Wir können also $\mathrm{Z}(G) = G$ annehmen, d. h. G ist abelsch. Sei $M < G$ eine größtmögliche echte Untergruppe. Ist $|M|$ durch p teilbar, so existiert nach Induktion ein $Z \leq M$ mit $|Z| = p$ und die Behauptung folgt wie oben. Sei also $|G/M| \equiv 0 \pmod{p^a}$. Für $x \in G \setminus M$ gilt $G = M\langle x\rangle$, da G abelsch und $|M|$ maximal ist. Wegen

$$|\langle x\rangle/\langle x\rangle \cap M| = |\langle x\rangle M/M| = |G/M| \equiv 0 \pmod{p^a}$$

ist $|\langle x\rangle|$ durch p^a teilbar. Nach Satz I.3.34 besitzt $\langle x\rangle$ eine Untergruppe der Ordnung p^b und damit auch G.

(ii) Sei $P \in \mathrm{Syl}_p(G)$ und $Q \leq G$ eine p-Untergruppe. Wie üblich operiert Q auf G/P durch Linksmultiplikation (Bemerkung I.4.6(i)), wobei die Bahnenlängen Teiler von $|Q|$ sind, also p-Potenzen. Wegen $|G/P| = m \not\equiv 0 \pmod p$ existiert eine Bahn der Länge 1, d. h. es existiert ein $x \in G$ mit $QxP = xP$. Es folgt $Q = Qx1x^{-1} \subseteq QxPx^{-1} = xPx^{-1} \in \mathrm{Syl}_p(G)$ (beachte $|xPx^{-1}| = |P|$).

[1] geht eigentlich auf CAPELLI zurück, siehe [M. Brescia, F. de Giovanni, M. Trombetti, *The true story behind Frattini's argument*, Adv. Group Theory Appl. 3 (2017), 117–129]

(iii) Folgt aus dem Beweis von (ii), indem man $P, Q \in \mathrm{Syl}_p(G)$ wählt.

(iv) Nach (iii) operiert G durch Konjugation transitiv auf $\mathrm{Syl}_p(G)$. Der Stabilisator von P ist dabei $\mathrm{N}_G(P)$. Die Bahnengleichung zeigt $|\mathrm{Syl}_p(G)| = |G : \mathrm{N}_G(P)|$. Offenbar operiert auch P auf $\mathrm{Syl}_p(G)$. Sei $Q \in \mathrm{Syl}_p(G)$ dabei ein Fixpunkt, d. h. $P \subseteq \mathrm{N}_G(Q)$. Nach (iii) existiert dann ein $x \in \mathrm{N}_G(Q)$ mit $P = xQx^{-1} = Q$. Also ist P der einzige Fixpunkt von P auf $\mathrm{Syl}_p(G)$. Die Bahnengleichung liefert $|\mathrm{Syl}_p(G)| \equiv 1 \pmod{p}$. □

Folgerung I.4.15. *Für $P \in \mathrm{Syl}_p(G)$ gilt $P \trianglelefteq G \iff \mathrm{Syl}_p(G) = \{P\}$.*

Beweis. Es gilt

$$P \trianglelefteq G \iff \mathrm{N}_G(P) = G \iff |\mathrm{Syl}_p(G)| = 1.$$ □

Satz I.4.16 (Cauchy)**.** *Für jeden Primteiler p von $|G|$ besitzt G ein Element der Ordnung p.*

Beweis. Wähle $b = 1$ in Satz I.4.14(i). □

Beispiel I.4.17.

(i) Für $|G| = 15 = 3 \cdot 5$ ist $|\mathrm{Syl}_3(G)|$ ein Teiler von 5 und 1 modulo 3 nach Satz I.4.14(iv). Dies zeigt $|\mathrm{Syl}_3(G)| = 1$. Analog zeigt man, dass G nur eine 5-Sylowgruppe besitzt. Also enthält G nur sieben Elemente der Ordnung 1, 3 oder 5. Daher existieren Elemente der Ordnung 15, d. h. $G \cong C_{15}$.

(ii) Sei $|G| = 12 = 2^2 \cdot 3$. Wie in (i) ist dann $|\mathrm{Syl}_3(G)| \in \{1, 4\}$. Nehmen wir $\mathrm{Syl}_3(G) = \{P_1, \ldots, P_4\}$ an. Nach Lagrange ist $P_i \cap P_j = 1$ für $i \neq j$. Dies zeigt $|P_1 \cup \ldots \cup P_4| = 1 + 4 \cdot 2 = 9$. Also ist nur noch Platz für eine 2-Sylowgruppe. In jeden Fall hat G einen Normalteiler der Ordnung 3 oder 4.

(iii) Nach Sylow besitzt A_4 Untergruppen der Ordnung $1, 2, 3, 4, 12$. Allerdings gibt es keine Untergruppe der Ordnung 6 (Aufgabe I.21). Die Umkehrung von Lagrange ist also falsch.

(iv) Sei $N \trianglelefteq G$ und $P \in \mathrm{Syl}_p(N)$. Dann operiert G durch Konjugation auf $\mathrm{Syl}_p(N)$ und N operiert transitiv nach Sylow. Das Frattini-Argument zeigt $G = N\mathrm{N}_G(P)$.

Lemma I.4.18. *Sei $N \trianglelefteq G$ und $P \in \mathrm{Syl}_p(G)$. Dann ist $P \cap N \in \mathrm{Syl}_p(N)$ und $PN/N \in \mathrm{Syl}_p(G/N)$.*

Beweis. Wegen $P \cap N \leq P$ ist $P \cap N$ eine p-Untergruppe von N. Nach dem ersten Isomorphiesatz ist $PN \leq G$ und Lemma I.3.14 zeigt

$$|N : P \cap N| = |PN : P| \not\equiv 0 \pmod{p}.$$

Also ist $P \cap N \in \mathrm{Syl}_p(N)$. Wegen $PN/N \cong P/P \cap N$ ist PN/N eine p-Untergruppe von G/N und der zweite Isomorphiesatz liefert

$$|G/N : PN/N| = |G : PN| = \frac{|G : P|}{|PN : P|} \not\equiv 0 \pmod{p}.$$

Dies zeigt $PN/N \in \mathrm{Syl}_p(G/N)$. □

Satz I.4.19 (Burnsides Lemma[2]). *Sei G eine endliche Gruppe und Ω eine G-Menge. Für $g \in G$ sei $f(g) := |\{\omega \in \Omega : g \in G_\omega\}|$ die Anzahl der Fixpunkte von g auf Ω. Dann ist*

$$\boxed{\frac{1}{|G|}\sum_{g\in G} f(g)}$$

die Anzahl der Bahnen von G auf Ω.

Beweis. Liegen $\alpha, \beta \in \Omega$ in der gleichen Bahn, so gilt $|G : G_\alpha| = |{}^G\alpha| = |{}^G\beta| = |G : G_\beta|$ nach Satz I.4.7. Nach Lagrange folgt $|G_\alpha| = |G_\beta|$ (beachte $|G| < \infty$). Sei $\Delta \subseteq \Omega$ ein Repräsentantensystem für die Bahnen von G auf Ω. Dann gilt

$$\begin{aligned}\sum_{g\in G} f(g) &= |\{(g,\omega) \in G \times \Omega : {}^g\omega = \omega\}| = \sum_{\omega\in\Omega} |G_\omega| = \sum_{\delta\in\Delta} |{}^G\delta||G_\delta| \\ &= \sum_{\delta\in\Delta} |G : G_\delta||G_\delta| = \sum_{\delta\in\Delta} |G| = |\Delta||G|.\end{aligned}$$

□

Beispiel I.4.20.

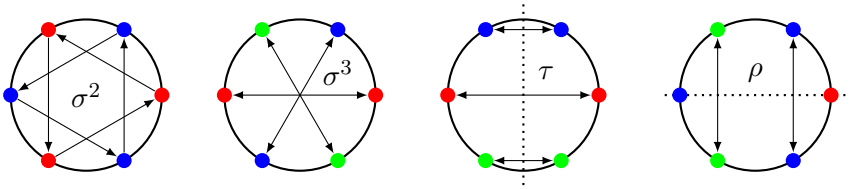
(i) Im Fall der Konjugationsoperation von G auf G erhält man

$$k(G) = \frac{1}{|G|}\sum_{g\in G} |\mathrm{C}_G(g)|.$$

(ii) Sei G eine endliche Gruppe, die transitiv auf Ω mit $|\Omega| > 1$ operiert. Nach Burnsides Lemma ist 1 die durchschnittliche Anzahl an Fixpunkten von Elementen aus G. Andererseits gilt $f(1) = |\Omega| > 1$. Es muss daher stets fixpunktfreie Elemente in G geben.

(iii) Wir wollen Halsketten mit sechs Perlen zählen, wobei Perlen in drei Farben zur Verfügung stehen. Naiverweise gibt es zunächst 3^6 solche Halsketten, von denen jedoch einige identisch sind. Wir ordnen die Halskette so an, dass die Perlen ein regelmäßiges 6-Eck bilden. Rotation um $\pi/3$ wird die Halsketten nicht verändern. Ebenso können wir die Halskette im Raum drehen und dadurch eine Spiegelung der 6 Eckpunkte realisieren. Zwei Halsketten sind also genau dann identisch, wenn sie in der gleichen Bahn unter der Diedergruppe $G := D_{12}$ liegen (siehe Aufgabe I.20). Wir wenden Burnsides Lemma auf die Menge Ω der 3^6 Halsketten an.

Sicher ist $f(1) = 3^6$. Eine Drehung $\sigma \in G$ um $\pi/3$ lässt nur die drei einfarbigen Halsketten fest, d. h. $f(\sigma) = 3$. Die Drehung σ^2 um $2\pi/3$ lässt die einfarbigen Halsketten und die Halsketten mit alternierenden Farben fest. Davon gibt es $f(\sigma^2) = 3^2$ Stück. Analog zeigt man $f(\sigma^3) = 3^3$. Außerdem ist $f(\sigma^4) = f(\sigma^{-2}) = 3^2$, $f(\sigma^5) = f(\sigma^{-1}) = 3$ sowie $\sigma^6 = 1$. Sei nun τ eine der drei Spiegelung durch zwei Seitenmittelpunkte. Dann ist $f(\tau) = 3^3$. Ist schließlich ρ eine der drei Spiegelungen durch zwei Eckpunkte, so gilt $f(\rho) = 3^4$.



[2]war schon vor Burnside bekannt, siehe [P. M. Neumann, *A lemma that is not Burnside's*, Math. Sci. 4 (1979), 133–141]

Nach Burnsides Lemma gibt es

$$\begin{aligned}\frac{1}{12}\left(3^6 + 2\cdot 3 + 2\cdot 3^2 + 3^3 + 3\cdot 3^3 + 3\cdot 3^4\right) &= \frac{1}{4}\left(3^4(3+1) + 3^2(1+3) + 2 + 6\right)\\ &= 81 + 9 + 2 = 92\end{aligned}$$

verschiedene Halsketten.

5 Abelsche Gruppen

Bemerkung I.5.1. Mit direkten Produkten lassen sich neue Gruppen aus alten konstruieren. Wir versuchen nun umgekehrt vorgegebene Gruppen als direkte Produkte zu schreiben.

Lemma I.5.2. *Für $N, M \trianglelefteq G$ mit $N \cap M = 1$ gilt $xy = yx$ für alle $x \in N$ und $y \in M$. Dies gilt insbesondere, wenn* $\mathrm{ggT}(|N|, |M|) = 1$.

Beweis. Für $x \in N$ und $y \in M$ gilt

$$\overbrace{\underbrace{xyx^{-1}}_{\in M}y^{-1}}^{\in N} \in N \cap M = 1,$$

d. h. $xy = yx$. Nach Lagrange ist $|N \cap M|$ ein Teiler von $\mathrm{ggT}(|N|, |M|)$. Daher folgt die zweite Aussage aus der ersten. □

Lemma I.5.3. *Seien $N_1, \ldots, N_k \trianglelefteq G$ mit $G = N_1 \ldots N_k$ und $N_i \cap \prod_{j \neq i} N_j = 1$ für $i = 1, \ldots, n$. Dann ist $G \cong N_1 \times \ldots \times N_k$.*

Beweis. Wir zeigen, dass die Abbildung

$$\begin{aligned} F \colon N_1 \times \ldots \times N_k &\to G, \\ (x_1, \ldots, x_k) &\mapsto x_1 \ldots x_k \end{aligned}$$

ein Isomorphismus ist. Nach Voraussetzung gilt $N_i \cap N_j \subseteq N_i \cap \prod_{l \neq i} N_l = 1$ für $i \neq j$. Lemma I.5.2 zeigt $xy = yx$ für $x \in N_i$ und $y \in N_j$. Seien nun $x_i, y_i \in N_i$ für $i = 1, \ldots, k$. Dann gilt

$$F(x_1, \ldots, x_k)F(y_1, \ldots, y_k) = x_1 \ldots x_k y_1 \ldots y_k = x_1 y_1 x_2 y_2 \ldots x_k y_k = F((x_1, \ldots, x_k)(y_1, \ldots, y_k)).$$

Also ist F ein Homomorphismus. Wegen $G = N_1 \ldots N_k$ ist F surjektiv. Sei $(x_1, \ldots, x_k) \in \mathrm{Ker}(F)$. Angenommen es existiert $1 \leq l \leq k$ mit $x_l \neq 1$. Sei l maximal. Dann wäre $x_l^{-1} = x_1 \ldots x_{l-1} \in N_l \cap N_1 \ldots N_{l-1} = 1$. Also ist $\mathrm{Ker}(F) = 1$ und F ist auch injektiv. □

Definition I.5.4. In der Situation von Lemma I.5.3 nennt man G die *direkte Summe* von $N_1, \ldots, N_k$ und schreibt $G = N_1 \oplus \ldots \oplus N_k$.

Bemerkung I.5.5.

(i) Ist umgekehrt $G = G_1 \times \ldots \times G_k$ gegeben, so gilt $G = N_1 \oplus \ldots \oplus N_k$ mit

$$N_i := \{(g_1, \ldots, g_k) \in G : g_j = 1 \, \forall j \neq i\}$$

für $i = 1, \ldots, k$. Daher sind direkte Summen und direkte Produkte nur verschiedene Sichtweisen des gleichen Sachverhalts (wie bei Vektorräumen).

(ii) Im Allgemeinen sind die Summanden einer direkten Summe nicht eindeutig bestimmt. Zum Beispiel gilt

$$V_4 = \langle (1,2)(3,4)\rangle \oplus \langle (1,3)(2,4)\rangle = \langle (1,2)(3,4)\rangle \oplus \langle (1,4)(2,3)\rangle = \langle (1,3)(2,4)\rangle \oplus \langle (1,4)(2,3)\rangle$$

(Aufgabe I.16).

(iii) Sicher ist $N_1 \oplus N_2 = N_2 \oplus N_1$. Sei

$$G = (N_1 \oplus N_2) \oplus N_3.$$

Da $\trianglelefteq$ nicht transitiv ist, ist nicht unmittelbar klar, ob $N_1 \trianglelefteq G$ gilt. Wegen $N_1 \cap N_3 \subseteq N_1N_2 \cap N_3 = 1$ ist $xy = yx$ für $x \in N_1$ und $y \in N_3$. Dies zeigt $N_3 \leq \mathrm{C}_G(N_1) \leq \mathrm{N}_G(N_1)$. Außerdem ist $N_1 \trianglelefteq N_1 \oplus N_2$ und daher $N_1N_2 \leq \mathrm{N}_G(N_1)$. Insgesamt ist

$$G = (N_1N_2)N_3 \leq \mathrm{N}_G(N_1),$$

d. h. $N_1 \trianglelefteq G$. Analog ist $N_2 \trianglelefteq G$. Sei schließlich $x = yz \in N_1 \cap N_2N_3$ mit $y \in N_2$ und $z \in N_3$. Dann ist $z = y^{-1}x \in N_3 \cap N_2N_1 = 1$ und $x = y \in N_1 \cap N_2 = 1$. Dies zeigt $N_1 \cap N_2N_3 = 1$ und analog $N_2 \cap N_1N_3 = 1$. Also ist $G = N_1 \oplus N_2 \oplus N_3$. Direkte Summen sind also kommutativ und assoziativ.

Beispiel I.5.6. Seien $p_1, \ldots, p_n$ die Primteiler von $|G|$. Nehmen wir $\mathrm{Syl}_{p_i}(G) = \{P_i\}$ für $i = 1, \ldots, n$ an (Gruppen mit dieser Eigenschaft nennt man *nilpotent*). Nach Folgerung I.4.15 gilt $P_1, \ldots, P_n \trianglelefteq G$. Nach Lagrange ist $P_i \cap P_j = 1$ für $i \neq j$. Nach Lemma I.3.14 gilt daher $|P_1P_2| = |P_1||P_2|$. Wieder nach Lagrange ist $P_3 \cap P_1P_2 = 1$. Induktiv folgt leicht

$$|P_1 \ldots P_n| = |P_1| \ldots |P_n| = |G|$$

und $P_i \cap \prod_{j \neq i} P_j = 1$. Also ist $G = P_1 \oplus \ldots \oplus P_n$. Insbesondere ist jede abelsche Gruppe die direkte Summe ihrer Sylowgruppen.

Definition I.5.7. Für eine abelsche p-Gruppe G sei

$$\Omega(G) := \{g \in G : g^p = 1\},$$
$$\mho(G) := \{g^p : g \in G\}.$$

Wegen $1^p = 1$ und $(gh^{-1})^p = g^ph^{-p}$ für $g, h \in G$ gilt $\Omega(G), \mho(G) \leq G$.

Beispiel I.5.8. Es gilt $\Omega(G \oplus H) = \Omega(G) \oplus \Omega(H)$ und $\mho(G \oplus H) = \mho(G) \oplus \mho(H)$ sowie $\Omega(C_{p^a}) \cong C_p$ und $\mho(C_{p^a}) \cong C_{p^{a-1}}$ für $a \in \mathbb{N}$.

Satz I.5.9 (Hauptsatz über endliche abelsche Gruppen)**.** *Für jede endliche abelsche Gruppe G existieren eindeutig bestimmte Primzahlpotenzen $q_1 \geq \ldots \geq q_n > 1$ mit*

$$G \cong C_{q_1} \times \ldots \times C_{q_n}.$$

Beweis (MacCluer). Nach Beispiel I.5.6 ist G die direkte Summe ihrer Sylowgruppen. Da direkte Summen kommutativ und assoziativ sind, können wir annehmen, dass G eine p-Gruppe ist. Sei H eine zyklische Untergruppe von G mit möglichst großer Ordnung p^a. Durch Induktion nach $|G|$ genügt es zu zeigen, dass H ein direkter Summand von G ist. Nehmen wir zunächst an, dass ein Element

$x \in G \setminus H$ der Ordnung p existiert. Dann ist $H\langle x\rangle/\langle x\rangle \cong H/H \cap \langle x\rangle = H/1 \cong H$ eine maximal zyklische Untergruppe von $G/\langle x\rangle$ (da G abelsch ist, sind alle Untergruppen normal). Nach Induktion ist $G/\langle x\rangle = H\langle x\rangle/\langle x\rangle \oplus K/\langle x\rangle$ für ein $K \leq G$ (Korrespondenzsatz). Sicher ist dann $G = H\langle x\rangle K = HK$ und

$$H \cap K = H \cap H\langle x\rangle \cap K = H \cap \langle x\rangle = 1.$$

Dies zeigt $G = H \oplus K$. Wir können also annehmen, dass alle Elemente der Ordnung $\leq p$ von G in H liegen. Da H zyklisch ist, gibt es nur p solche Elemente (Satz I.3.34). Der Kern des Endomorphismus $f\colon G \to G$, $g \mapsto g^p$ hat daher Ordnung p. Es folgt $|f(G)| = |G|/p$ aus dem Homomorphiesatz. Nach Cauchy hat auch $f(G)$ genau p Elemente der Ordnung $\leq p$ (außer im Fall $f(G) = 1$). Wiederholte Anwendung von f zeigt daher

$$1 = |f^a(G)| = |G|/p^a = |G : H|$$

nach Wahl von H. Somit ist $G = H$ zyklisch und die Existenz der Zerlegung ist bewiesen.

Für die Eindeutigkeit der Zerlegung sei

$$G = G_1 \oplus \ldots \oplus G_n \cong C_{p^{a_1}} \times \ldots \times C_{p^{a_n}}$$

mit $a_1 \geq \ldots \geq a_n \geq 1$. Nach Beispiel I.5.8 ist

$$|\Omega(G)| = |\Omega(G_1) \oplus \ldots \oplus \Omega(G_n)| = |C_p \times \ldots \times C_p| = p^n.$$

Insbesondere ist n durch G eindeutig bestimmt. Außerdem ist

$$\mho(G) = \mho(G_1) \oplus \ldots \oplus \mho(G_n) \cong C_{p^{a_1-1}} \times \ldots \times C_{p^{a_n-1}}.$$

Nach Induktion sind die $a_i > 1$ eindeutig durch G bestimmt. Da man n bereits kennt, ist auch die Anzahl der $a_i = 1$ eindeutig bestimmt. □

Beispiel I.5.10.

(i) Wir wissen bereits, dass 1, C_2, C_3 die einzigen Gruppen der Ordnung 1, 2 und 3 sind. Sei nun $|G| = 4$. Nach Folgerung I.4.12 ist G abelsch und daher entweder zu C_4 oder $C_2 \times C_2$ isomorph. Zum Beispiel ist $V_4 \cong C_2 \times C_2$ (Aufgabe I.16).

(ii) Sei $|G| = 6$ und $P \in \mathrm{Syl}_2(G)$. Wie üblich operiert G auf G/P mit Kern $N \leq P$ (Bemerkung I.4.6(i)). Im Fall $N = 1$ erhält man einen Isomorphismus $G \to \mathrm{Sym}(G/P) \cong S_3$. Sei nun $P = N \trianglelefteq G$. Nach Sylow besitzt G auch eine normale 3-Sylowgruppe Q. Aus Beispiel I.5.6 und Satz I.3.34 folgt $G = P \oplus Q \cong C_2 \times C_3 \cong C_6$. Also sind C_6 und S_3 die einzigen Gruppen der Ordnung 6 bis auf Isomorphie. Insbesondere ist $D_6 \cong S_3$, denn D_6 ist nicht abelsch.

(iii) Für jede Primzahl p gibt es genau drei abelsche Gruppen der Ordnung p^3 bis aus Isomorphie: C_{p^3}, $C_{p^2} \times C_p$ und $C_p \times C_p \times C_p$.

Bemerkung I.5.11. Nach Satz I.3.34 kennen wir die Unter- und Faktorgruppen von zyklischen Gruppen. Wir bestimmen nun die Isomorphietypen von Unter- und Faktorgruppen einer beliebigen abelschen Gruppe.

Satz I.5.12. *Sei $H \leq G \cong C_{q_1} \times \ldots \times C_{q_n}$ mit Primzahlpotenzen $q_1, \ldots, q_n$. Dann existieren Teiler $r_i \mid q_i$ für $i = 1, \ldots, n$ mit $H \cong C_{r_1} \times \ldots \times C_{r_n}$. Zu vorgegebenen (positiven) Teilern $r_i \mid q_i$ existiert umgekehrt ein $H \leq G$ mit $H \cong C_{r_1} \times \ldots \times C_{r_n}$.*

Beweis. Induktion nach $|G|$: Da die (einzige) p-Sylowgruppe von H in der p-Sylowgruppe von G liegt, dürfen wir annehmen, dass G und H p-Gruppen sind. Sei also $G \cong C_{p^{a_1}} \times \ldots \times C_{p^{a_n}}$ und $H \cong C_{p^{b_1}} \times \ldots \times C_{p^{b_m}}$ mit o. B. d. A. $a_1 \geq \ldots \geq a_n \geq 1$ und $b_1 \geq \ldots \geq b_m \geq 1$. Wegen $\Omega(H) \subseteq \Omega(G)$ ist $p^m = |\Omega(H)| \leq |\Omega(G)| = p^n$ und $m \leq n$. Nach Beispiel I.5.8 ist

$$C_{p^{b_1-1}} \times \ldots \times C_{p^{b_m-1}} \cong \mho(H) \leq \mho(G) \cong C_{p^{a_1-1}} \times \ldots \times C_{p^{a_n-1}}.$$

Induktion liefert $b_i \leq a_i$ für $i = 1, \ldots, m$. Dies zeigt die erste Behauptung.

Für Teiler $r_i \mid q_i$ existiert nach Satz I.3.34 eine Untergruppe $C_{r_i} \leq C_{q_i}$. Sicher ist dann $C_{r_1} \times \ldots \times C_{r_n} \leq C_{q_1} \times \ldots \times C_{q_n}$ und die zweite Behauptung folgt. □

Bemerkung I.5.13. Die analoge Aussage gilt auch für Faktorgruppen (Aufgabe I.29).

Beispiel I.5.14. Die Gruppe $C_8 \times C_4$ besitzt Untergruppen (sowie Faktorgruppen) vom Typ C_1, C_2, C_4, C_8, C_2^2, $C_4 \times C_2$, $C_8 \times C_2$, C_4^2 und $C_8 \times C_4$. Es ist schwierig zu bestimmen, wie viele Untergruppen von jedem Typ existieren. Zum Beispiel hat $V_4 \cong C_2^2$ drei Untergruppen vom Typ C_2.

6 Auflösbare und einfache Gruppen

Definition I.6.1. Eine endliche Gruppe G heißt

- *einfach*, falls G genau zwei Normalteiler besitzt (nämlich 1 und $G \neq 1$; vgl. Primzahl).
- *auflösbar*, falls Untergruppen $1 = G_0 \trianglelefteq \ldots \trianglelefteq G_n = G$ existieren, sodass G_i/G_{i-1} für $i = 1, \ldots, n$ abelsch ist.

Bemerkung I.6.2. Beachte: Bei der Auflösbarkeit wird nicht $G_i \trianglelefteq G$ gefordert.

Beispiel I.6.3.

(i) Nach Lagrange sind die Gruppen C_p für $p \in \mathbb{P}$ einfach.

(ii) Jede abelsche Gruppe ist auflösbar (setze $n = 1$).

(iii) Nach Aufgabe I.20 besitzt D_{2n} einen zyklischen Normalteiler vom Index 2. Also ist D_{2n} auflösbar. Insbesondere ist $S_3 \cong D_6$ auflösbar.

(iv) Sei G einfach und auflösbar mit $1 = G_0 \trianglelefteq \ldots \trianglelefteq G_n = G$ wie in Definition I.6.1. O. B. d. A. sei $G_{n-1} < G$ (beachte $G \neq 1$). Wegen $G_{n-1} \trianglelefteq G$ ist $G_{n-1} = 1$ und $G \cong G_n/G_{n-1}$ ist abelsch. Insbesondere ist jede Untergruppe von G normal und wegen der Einfachheit besitzt G keine nicht-triviale, echte Untergruppe. Nach Cauchy ist $|G|$ eine Primzahl. Die Gruppen C_p ($p \in \mathbb{P}$) sind daher die einzigen einfachen, auflösbaren Gruppen.

Satz I.6.4. *Eine endliche Gruppe G ist genau dann auflösbar, wenn Untergruppen $1 = G_0 \trianglelefteq \ldots \trianglelefteq G_n = G$ existieren, sodass G_i/G_{i-1} für $i = 1, \ldots, n$ zyklisch ist.*

Beweis. Da zyklische Gruppen abelsch sind, ist jede Gruppe mit der angegebenen Bedingung auflösbar. Sei umgekehrt G auflösbar und $1 = G_0 \trianglelefteq \ldots \trianglelefteq G_n = G$ mit abelschen Faktoren. Zwischen G_{i-1} und G_i fügen wir weitere Untergruppen ein, sodass die entstehenden Faktoren zyklisch sind. Nach dem Korrespondenzsatz dürfen wir dafür $G = G_i/G_{i-1}$ annehmen, d. h. G ist abelsch. Nach Satz I.5.9 existieren zyklische Normalteiler $N_1, \ldots, N_k$ mit $G = N_1 \oplus \ldots \oplus N_k$. Wegen

$$N_1 \ldots N_i / N_1 \ldots N_{i-1} \cong N_i/(N_i \cap N_1 \ldots N_{i-1}) = N_i/1 \cong N_i$$

hat die Reihe $1 \leq N_1 \leq N_1N_2 \leq \ldots \leq N_1 \ldots N_k = G$ zyklische Faktoren. □

Satz I.6.5. *Sei G eine endliche Gruppe mit $H \leq G$ und $N \trianglelefteq G$.*

(i) Ist G auflösbar, so auch H und G/N.

(ii) Sind N und G/N auflösbar, so auch G.

Beweis.

(i) Sei $1 = G_0 \trianglelefteq \ldots \trianglelefteq G_n = G$ mit abelschen Faktoren. Dann ist $1 = G_0 \cap H \trianglelefteq G_1 \cap H \trianglelefteq \ldots \trianglelefteq G_n \cap H = H$ und

$$(G_i \cap H)/(G_{i-1} \cap H) = (G_i \cap H)/((G_i \cap H) \cap G_{i-1}) \cong (G_i \cap H)G_{i-1}/G_{i-1} \leq G_i/G_{i-1}$$

ist abelsch für $i = 1, \ldots, n$. Analog ist $1 = G_0N/N \trianglelefteq G_1N/N \trianglelefteq \ldots \trianglelefteq G_nN/N = G/N$ und

$$\begin{aligned}(G_iN/N)/(G_{i-1}N/N) &\cong G_iN/G_{i-1}N = G_i(G_{i-1}N)/G_{i-1}N \cong G_i/(G_i \cap G_{i-1}N) \\ &\overset{I.3.14}{=} G_i/(G_i \cap N)G_{i-1} \cong (G_i/G_{i-1})/((G_i \cap N)G_{i-1}/G_{i-1})\end{aligned}$$

ist abelsch für $i = 1, \ldots, n$.

(ii) Seien $1 = N_0 \trianglelefteq \ldots \trianglelefteq N_r = N$ und $1 = G_0/N \trianglelefteq \ldots \trianglelefteq G_s/N = G/N$ mit abelschen Faktoren. Dann ist $1 = N_0 \trianglelefteq \ldots \trianglelefteq N_r = N = G_0 \trianglelefteq \ldots \trianglelefteq G_s = G$. Wegen $G_i/G_{i-1} \cong (G_i/N)/(G_{i-1}/N)$ sind auch die Faktoren dieser Reihe abelsch. □

Beispiel I.6.6. Nach Beispiel I.4.17 besitzt jede Gruppe G der Ordnung 12 einen Normalteiler N der Ordnung 3 oder 4. Offenbar sind dann N und G/N auflösbar, also auch G. Insbesondere ist A_4 auflösbar (vgl. Aufgabe I.16). Wegen $|S_4 : A_4| = 2$ ist auch S_4 auflösbar.

Satz I.6.7. *p-Gruppen sind auflösbar.*

Beweis. Sei G eine p-Gruppe mit $|G| = p^n$. Induktion nach n: Für $n = 0$ ist $G = 1$ auflösbar. Sei nun $n \geq 1$. Nach Satz I.4.11 ist $\mathrm{Z}(G) \neq 1$. Als abelsche Gruppe ist $\mathrm{Z}(G)$ auflösbar. Nach Induktion ist $G/\mathrm{Z}(G)$ auflösbar. Nach Satz I.6.5 ist auch G auflösbar. □

Lemma I.6.8. *Gruppen der Ordnung pq mit $p, q \in \mathbb{P}$ sind auflösbar.*

Beweis. Nach Satz I.6.7 können wir $p < q$ annehmen. Für $Q \in \mathrm{Syl}_q(G)$ ist $|G : \mathrm{N}_G(Q)|$ ein Teiler von p und 1 modulo q nach Sylow. Dies zeigt $Q \trianglelefteq G$. Da Q und $G/Q \cong C_p$ auflösbar sind, ist auch G auflösbar. □

Lemma I.6.9. *Sei G nichtabelsch und einfach. Für $H < G$ gilt dann $|G : H| \geq 5$.*

Beweis. Nach Bemerkung I.4.6 existiert ein Homomorphismus $f\colon G \to \mathrm{Sym}(G/H)$ mit $\mathrm{Ker}(f) \leq H < G$. Da G einfach ist, gilt $\mathrm{Ker}(f) = 1$ und G ist zu einer Untergruppe von $\mathrm{Sym}(G/H)$ isomorph. Im Fall $|G : H| \leq 4$ wäre $\mathrm{Sym}(G/H) \leq S_4$ auflösbar und somit auch G. Widerspruch. □

Satz I.6.10. *Gruppen der Ordnung < 60 sind auflösbar.*

Beweis. Sei G ein minimales Gegenbeispiel. Nach Satz I.6.5 ist G einfach. Nach Satz I.6.7 ist G keine p-Gruppe. Für jede Sylowgruppe P von G gilt daher $|G : P| \geq 5$ nach Lemma I.6.9. Die Ordnungen $|G| = 35 = 5 \cdot 7$ und $|G| = 55 = 5 \cdot 11$ sind nach Lemma I.6.8 ausgeschlossen. Es verbleiben folgende Ordnungen für $|G|$:

$$30, 40, 42, 45, 56.$$

Wir betrachten nur den ersten Fall (Rest in Aufgabe I.30). Nach Sylow gilt $\mathrm{Syl}_5(G) = \{P_1, \ldots, P_6\}$ wegen $|G| = 30 = 2 \cdot 3 \cdot 5$. Wegen $|P_1 \cup \ldots \cup P_6| = 1 + 6 \cdot 4 = 25$ ist nur noch Platz für höchstens zwei 3-Sylowgruppen. Nach Sylow folgt $|\mathrm{Syl}_3(G)| = 1$ im Widerspruch zur Einfachheit von G. □

Lemma I.6.11. *Für $n \in \mathbb{N}$ wird A_n von den 3-Zyklen erzeugt.*

Beweis. Für $n \leq 2$ ist $A_n = 1 = \langle \varnothing \rangle$. Sei also $n \geq 3$. Nach Bemerkung I.3.8 und Satz I.3.26 lässt sich $\sigma \in A_n$ als Produkt einer geraden Anzahl von Transpositionen schreiben. Für das Produkt von zwei Transpositionen gilt

$$(a,b)(c,d) = \begin{cases} 1 & \text{falls } \{a,b\} = \{c,d\}, \\ (a,d,b) & \text{falls } a = c,\ b \neq d, \\ (a,c,b)(a,c,d) & \text{falls } \{a,b\} \cap \{c,d\} = \varnothing. \end{cases}$$

□

Bemerkung I.6.12. Für $\sigma, (a_1, \ldots, a_k) \in S_n$ gilt

$$\sigma(a_1, \ldots, a_k)\sigma^{-1} = (\sigma(a_1), \ldots, \sigma(a_k)). \tag{I.6.1}$$

Satz I.6.13. *Für $n \geq 5$ ist A_n einfach. Insbesondere ist S_n nicht auflösbar.*

Beweis. Sei $1 \neq N \trianglelefteq A_n$. Wir müssen $N = A_n$ zeigen. Sei zunächst $n = 5$. Nach Beispiel I.3.30 ist

$$|A_5| = \frac{5!}{2} = 60 = 2^2 \cdot 3 \cdot 5$$

und A_5 besteht nach Aufgabe I.15 aus folgenden Elementen: Identität, 15 Elemente der Ordnung 2 (Zyklentyp $(2,2)$), 20 Elemente der Ordnung 3 (Zyklentyp (3)) und 24 Elemente der Ordnung 5 (Zyklentyp (5)). Nehmen wir an, dass $|N|$ einen Primteiler $p \in \{3,5\}$ besitzt. Nach Sylow enthält N dann alle p-Sylowgruppen und somit alle p-Elemente von A_5. Dies zeigt $|N| = 1 + |N \setminus \{1\}| \geq 1 + 20$ und Lagrange liefert $|N| \in \{30, 60\}$. Also enthält N sogar alle 3-Elemente und 5-Elemente. Dies zeigt $|N| \geq 44$ und $N = A_5$.

Sei nun $|N|$ eine 2-Potenz. Im Fall $|N| = 4$ hätte A_5 nur eine 2-Sylowgruppe und nur drei Elemente der Ordnung 2. Also ist $|N| = 2$, sagen wir $N = \langle (1,2)(3,4) \rangle$. Dann erhält man den Widerspruch $(1,2,3)(1,2)(3,4)(1,2,3)^{-1} = (1,4)(2,3) \notin N$. Dies zeigt $N = A_5$ und A_5 ist einfach.

Sei jetzt $n \geq 6$ und $\sigma \in N \setminus \{1\}$. Wähle $1 \leq a \leq n$ mit $b := \sigma(a) \neq a$ und $c \in \{1, \ldots, n\} \setminus \{a, b, \sigma(b)\}$. Nach (I.6.1) ist

$$N \ni \sigma(a,b,c)\sigma^{-1}(a,b,c)^{-1} = (b, \sigma(b), \sigma(c))(b,a,c) =: \tau \neq 1.$$

Wähle $d, e \in \{1, \ldots, n\}$ mit $|\{a,b,c,d,e\}| = 5$ und

$$\tau \in A_n \cap \mathrm{Sym}(\{a,b,c,d,e\}) =: H.$$

Ist $f \colon \{1, \ldots, 5\} \to \{a,b,c,d,e\}$ eine Bijektion, so ist $A_5 \to H$, $\alpha \mapsto f\alpha f^{-1}$ ein Isomorphismus. Nach dem ersten Teil des Beweises ist H einfach. Nach dem ersten Isomorphiesatz ist $1 \neq \tau \in H \cap N \trianglelefteq H$ und es folgt $(a,b,c) \in H = H \cap N \leq N$. Sei $(a',b',c') \in A_n$ beliebig und $\alpha \in S_n$ mit $\alpha(a) = a'$, $\alpha(b) = b'$, $\alpha(c) = c'$. Durch eventuelle Multiplikation mit (d,e) kann man $\alpha \in A_n$ erreichen. Nach (I.6.1) gilt dann

$$(a',b',c') = \alpha(a,b,c)\alpha^{-1} \in N.$$

Aus Lemma I.6.11 folgt $N = A_n$. Also ist A_n einfach. Nach Beispiel I.6.3(iv) ist A_n nicht auflösbar. Die zweite Behauptung folgt aus Satz I.6.5. □

Bemerkung I.6.14.

(i) Eines der größten mathematischen Projekte war die Klassifikation aller endlichen einfachen Gruppen. Neben den Familien C_p und A_n gibt es eine Reihe von Matrixgruppen (Gruppen vom *Lie-Typ* wie

$$\mathrm{PSL}(n,K) := \mathrm{SL}(n,K)/\mathrm{Z}(\mathrm{SL}(n,K))$$

für einen endlichen Körper K mit $(n,|K|) \notin \{(2,2),(2,3)\}$) sowie 26 Ausnahmen (*sporadische* Gruppen). Die größte sporadische Gruppe ist die *Monstergruppe* mit

$$808.017.424.794.512.875.886.459.904.961.710.757.005.754.368.000.000.000 \approx 10^{54}$$

Elementen. Der Beweis der Klassifikation hat über 10.000 Seiten[1].

(ii) Burnside hat bewiesen, dass Gruppen der Ordnung $p^a q^b$ für Primzahlen p und q auflösbar sind (Satz II.13.33). Feit und Thompson haben bewiesen, dass Gruppen ungerader Ordnung auflösbar sind. Dieser Beweis hat ca. 250 Seiten.

(iii) Im Folgenden beweisen wir eine eindeutige „Primfaktorzerlegung“ für Gruppen.

Definition I.6.15. Eine Folge von Untergruppen $1 = G_0 \trianglelefteq \ldots \trianglelefteq G_n = G$ nennt man *Kompositionsreihe*, wenn die Faktoren G_i/G_{i-1} für $i = 1,\ldots,n$ einfach sind.

Bemerkung I.6.16. Jede endliche Gruppe G besitzt eine Kompositionsreihe: Dies ist klar, falls $G = 1$ (setze $n = 0$). Sei nun $G \neq 1$ und $N \lhd G$ ein größtmöglicher echter Normalteiler von G. Durch Induktion nach $|G|$ können wir annehmen, dass N eine Kompositionsreihe $1 = N_0 \trianglelefteq \ldots \trianglelefteq N_k = N$ besitzt. Nach dem zweiten Isomorphiesatz ist G/N einfach. Also ist $1 = N_0 \trianglelefteq \ldots \trianglelefteq N_k \trianglelefteq G$ eine Kompositionsreihe von G. Wir beschäftigen uns nun mit der Eindeutigkeit von Kompositionsreihen.

Satz I.6.17 (Jordan-Hölder)**.** *Seien $1 = G_k \trianglelefteq \ldots \trianglelefteq G_0 = G$ und $1 = H_l \trianglelefteq \ldots \trianglelefteq H_0 = G$ Kompositionsreihen von G. Dann ist $k = l$ und es existiert ein $\pi \in S_k$ mit $G_{i-1}/G_i \cong H_{\pi(i)-1}/H_{\pi(i)}$ für $i = 1,\ldots,k$. Man nennt $G_0/G_1,\ldots,G_{k-1}/G_k$ die* Kompositionsfaktoren *von G.*

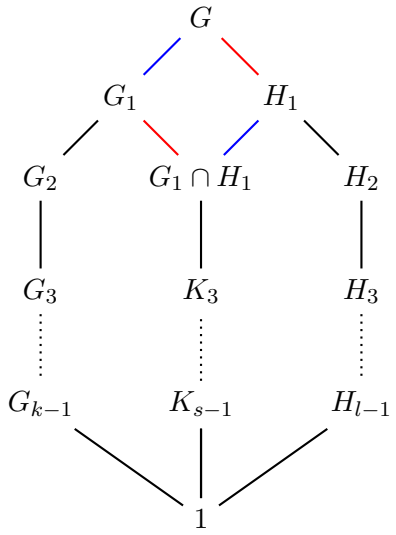
Beweis. Induktion nach $|G|$: O. B. d. A. sei $G \neq 1$. Im Fall $G_1 = H_1$ folgt die Behauptung mit Induktion. Sei also $G_1 \neq H_1$. Wegen $G_1, H_1 \trianglelefteq G$ ist auch $G_1H_1 = H_1G_1 \trianglelefteq G$. Da G/G_1 einfach ist, folgt $G = G_1H_1$. Der erste Isomorphiesatz zeigt

$$G/G_1 = H_1G_1/G_1 \cong H_1/H_1 \cap G_1, \qquad G/H_1 = G_1H_1/H_1 \cong G_1/G_1 \cap H_1. \tag{I.6.2}$$

Sei $1 = K_s \trianglelefteq \ldots \trianglelefteq K_2 = G_1 \cap H_1$ eine beliebige Kompositionsreihe. Nach Induktion sind dann die Kompositionsreihen $G_k \trianglelefteq \ldots \trianglelefteq G_1$ und $K_s \trianglelefteq \ldots \trianglelefteq K_2 \trianglelefteq G_1$ gleich lang (d. h. $k = s$) und ihre Faktoren sind (bis auf die Reihenfolge) isomorph. Nun sind auch die Kompositionsreihen $1 = K_k \trianglelefteq \ldots \trianglelefteq K_2 \trianglelefteq H_1$ und $1 = H_l \trianglelefteq \ldots \trianglelefteq H_1$ gleich lang mit isomorphen Faktoren. Also ist $k = s = l$ und nach (I.6.2) haben die Kompositionsreihen

[1] Aktueller Stand: [Solomon, *The Classification of Finite Simple Groups: A Progress Report*, Notices of the AMS 65 (2018), 646–651, `https://www.ams.org/journals/notices/201806/rnoti-p646.pdf`]

$G_k \trianglelefteq \ldots \trianglelefteq G_0$,
$K_k \trianglelefteq \ldots \trianglelefteq K_2 \trianglelefteq G_1 \trianglelefteq G_0$,
$K_k \trianglelefteq \ldots \trianglelefteq K_2 \trianglelefteq H_1 \trianglelefteq H_0$,
$H_k \trianglelefteq \ldots \trianglelefteq H_0$



isomorphe Faktoren. □

Beispiel I.6.18.

(i) Offenbar ist $1 < \langle (1,2)(3,4) \rangle < V_4 < A_4 < S_4$ eine Kompositionsreihe von S_4 (vgl. Aufgabe I.16). Daher sind C_2, C_2, C_2, C_3 die Kompositionsfaktoren von S_4. Ersetzt man $(1,2)(3,4)$ durch $(1,3)(2,4)$ oder $(1,4)(2,3)$, so erhält man weitere Kompositionsreihen.

(ii) Nach Satz I.6.13 ist $1 < A_n < S_n$ eine Kompositionsreihe von S_n für $n \geq 5$.

(iii) Nach Satz I.6.5 sind die Kompositionsfaktoren einer auflösbaren Gruppe auflösbar und daher von Primzahlordnung. Eine Gruppe ist also genau dann auflösbar, wenn alle Kompositionsfaktoren Primzahlordnung haben. Insbesondere ist C_p (bis auf Vielfachheit) der einzige Kompositionsfaktor jeder nicht-trivialen p-Gruppe.

(iv) Für vorgegebene einfache Gruppen $G_1, \ldots, G_n$ existiert stets eine Gruppe mit Kompositionsfaktoren $G_1, \ldots, G_n$, nämlich $G_1 \times \ldots \times G_n$. In der Regel gibt es aber viele nicht-isomorphe Gruppen mit den gleichen Kompositionsfaktoren.

7 Ringe

Definition I.7.1. Ein *Ring* ist eine Menge R mit Verknüpfungen $+$ und $\cdot$, sodass gilt:

- $(R, +)$ ist eine abelsche Gruppe mit neutralem Element 0,
- $\forall a, b, c \in R : a \cdot (b \cdot c) = (a \cdot b) \cdot c$ (assoziativ),
- $\exists 1 \in R : \forall a \in R : 1 \cdot a = a = a \cdot 1$ (neutrales Element),
- $\forall a, b, c \in R : a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ und $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$ (distributiv).

Ist $\cdot$ zusätzlich kommutativ, so nennt man R *kommutativ*.

Bemerkung I.7.2.

(i) Wie üblich schreiben wir ab statt $a \cdot b$. Das Inverse von $a \in R$ bzgl. $+$ nennen wir $-a$ und schreiben $a - b := a + (-b)$. Um Klammern zu sparen verabreden wir „Punktrechnung vor Strichrechnung“, d. h. $ab + c := (ab) + c$.

(ii) Für $a \in R$ ist $a0 = a(0 + 0) = a0 + a0 = 0 = 0a$.

(iii) Im Fall $0 = 1$ ist $a = a1 = a0 = 0$ für alle $a \in R$, d. h. $R = \{0\}$ ist der *Nullring*. Dieser uninteressante Ring wird im Folgenden vernachlässigt.

(iv) Ist $\cdot$ kommutativ, so genügt es eines der beiden Distributivgesetze zu fordern. Im Gegensatz zu Gruppen spricht man nicht von abelschen Ringen.

Beispiel I.7.3.

(i) Die ganzen Zahlen $\mathbb{Z}$ und jeder Körper sind kommutative Ringe.

(ii) Für Ringe $R_1, \ldots, R_n$ ist auch das *direkte Produkt* $R_1 \times \ldots \times R_n$ ein Ring mit den komponentenweisen Verknüpfungen (wie für Gruppen).

(iii) Für jeden Körper K und $n \in \mathbb{N}$ ist der *Matrixring* $K^{n \times n}$ ein Ring bzgl. Addition und Multiplikation von Matrizen. Für $n \geq 2$ ist $K^{n \times n}$ nicht kommutativ.

Definition I.7.4. Sei $R \neq \{0\}$ ein Ring.

- Man nennt $a \in R$ *invertierbar* (oder *Einheit*), falls $b \in R$ mit $ba = 1 = ab$ existiert. Wie üblich ist dann b eindeutig bestimmt und man schreibt $a^{-1} := b$. Die invertierbaren Elemente von R bilden eine Gruppe $R^\times \subseteq R \setminus \{0\}$, die man *Einheitengruppe* von R nennt (nachrechnen).[1]
- Man nennt $a \in R \setminus \{0\}$ *Nullteiler*, falls $b \in R \setminus \{0\}$ mit $ab = 0 = ba$ existiert. Ein kommutativer Ring ohne Nullteiler heißt *Integritätsbereich*.
- Ein Element $a \in R$ heißt *Idempotent*, falls $a^2 = a$ (Aufgabe II.7).

[1] Manche Autoren schreiben $U(R)$ (units) anstelle von $R^\times$

- Man nennt $a \in R$ *nilpotent*, falls ein $n \in \mathbb{N}$ mit $a^n = 0$ existiert (Aufgabe II.42).

Beispiel I.7.5.

(i) Ein Ring R mit $R^\times = R \setminus \{0\}$ heißt *Schiefkörper*. Ein kommutativer Schiefkörper ist ein Körper. In der Algebra II zeigen wir, dass jeder endliche Schiefkörper ein Körper ist (Satz II.8.7).

(ii) Sei $a \in \mathbb{Z}$ invertierbar und $b \in \mathbb{Z}$ mit $ba = 1$. Dann folgt $a \in \{\pm 1\}$. Dies zeigt $\mathbb{Z}^\times = \{\pm 1\}$.

(iii) Für jeden Körper K und $n \in \mathbb{N}$ ist $(K^{n\times n})^\times = \mathrm{GL}(n, K)$.

(iv) Für Ringe R, S gilt $(R \times S)^\times = R^\times \times S^\times$.

(v) Jeder Körper ist ein Integritätsbereich und jeder endliche Integritätsbereich ist ein Körper (Aufgabe I.36).

(vi) $\mathbb{Z}$ ist ein Integritätsbereich, aber kein Körper.

(vii) $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right)$ ist ein Nullteiler in $K^{2\times 2}$.

Bemerkung I.7.6. In jedem Integritätsbereich gilt die *Kürzungsregel* $ab = ac \Longrightarrow b = c$ für $a, b, c \in R$ und $a \neq 0$. Dies folgt aus $a(b - c) = 0$.

Definition I.7.7. Sei R ein Ring.

(i) Ein *Teilring* von R ist eine Teilmenge $S \subseteq R$ mit $1, a - b, ab \in S$ für $a, b \in S$.

(ii) Ein *Ideal* von R ist eine nichtleere Teilmenge $I \subseteq R$ mit $a - b, xa, ax \in I$ für $a, b \in I$ und $x \in R$. Man schreibt dann $I \trianglelefteq R$ oder $I \triangleleft R$, falls I ein *echtes* Ideal ist, d. h. $I \neq R$.

(iii) Ein $I \triangleleft R$ heißt *maximal*, falls kein $J \triangleleft R$ mit $I \subsetneq J$ existiert.

Bemerkung I.7.8.

(i) Jeder Teilring $S \subseteq R$ wird mit den eingeschränkten Verknüpfungen selbst zu einem Ring (nachrechnen).

(ii) Jedes $I \trianglelefteq R$ ist eine abelsche Gruppe bzgl. $+$ (nachrechnen). Insbesondere ist $0 \in I$.

Beispiel I.7.9.

(i) R ist ein Teilring von R, aber $\{0\}$ nicht (außer $R = \{0\}$).

(ii) $\{0\}$ und R sind Ideale von R.

(iii) Für jeden Ring R ist das *Zentrum*

$$\mathrm{Z}(R) := \{x \in R : rx = xr \ \forall r \in R\}$$

ein kommutativer Teilring.

(iv) Jeder Teilring eines Körpers ist ein Integritätsbereich. Zum Beispiel $\mathbb{Z} \subseteq \mathbb{Q}$.

(v) Durchschnitte, Summen und Produkte von Idealen sind wieder Ideale (Aufgabe I.37).

(vi) Für $U \subseteq R$ ist

$$(U) := \bigcap_{U \subseteq I \trianglelefteq R} I \trianglelefteq R$$

das von U *erzeugte* Ideal. Wir schreiben auch $U = (x_1, \ldots, x_n) := (\{x_1, \ldots, x_n\})$. Ist R kommutativ, so gilt $(x) = Rx = \{ax : a \in R\}$ für $x \in R$. Man nennt (x) dann *Hauptideal*. Zum Beispiel sind $\{0\} = (0)$ und $R = (1)$ stets Hauptideale.

(vii) Sei $\{0\} \neq I \trianglelefteq \mathbb{Z}$ und $n \in I \cap \mathbb{N}$ minimal. Für $m \in I$ liefert Division mit Rest $m = qn + r$ mit $0 \leq r < n$. Wegen $r = m - qn \in I$ folgt $r = 0$ und $I = n\mathbb{Z} = (n)$. Wegen $d \mid n \iff (n) \subseteq (d)$ ist (n) genau dann maximal, wenn $n \in \mathbb{P}$.

Satz I.7.10 (Faktorring)**.** *Für jeden Ring R und $I \trianglelefteq R$ wird $R/I := \{a + I : a \in R\}$ durch*

$$(a + I) \dot{+} (b + I) := (a \dot{+} b) + I$$

zu einem Ring mit Nullelement $0 + I$ und Einselement $1 + I$.

Beweis. Nach Satz I.3.19 ist R/I bereits eine Gruppe bzgl. $+$. Die anderen Axiome beweist man wie in Satz I.2.23. □

Beispiel I.7.11. $\mathbb{Z}/4\mathbb{Z}$ ist ein kommutativer Ring, aber kein Integritätsbereich, denn $(2 + 4\mathbb{Z})^2 = 0$.

Satz I.7.12. *Sei R ein kommutativer Ring und $I \trianglelefteq R$. Genau dann ist R/I ein Körper, wenn I maximal ist.*

Beweis. Sei R/I ein Körper und $J \trianglelefteq R$ mit $I \subsetneq J$. Wähle $a \in J \setminus I$. Dann ist $a + I \neq 0$ in R/I und es existiert $b \in R$ mit $ab + I = (a + I)(b + I) = 1 + I$. Sei $x \in I$ mit $1 = ab + x$. Dann ist $R = R1 = Rab + Rx \subseteq J + I = J$ und I ist maximal.

Sei umgekehrt I maximal in R und $a + I \neq 0 + I$. Wegen $I \subsetneq (a) + I \trianglelefteq R$ folgt $R = (a) + I$. Sei $b \in R$ und $x \in I$ mit $1 = ba + x$. Dann gilt

$$(b + I)(a + I) = ba + I = 1 - x + I = 1 + I.$$

Also ist $a + I$ invertierbar in R/I und R/I ist ein Körper. □

Folgerung I.7.13. *Für $n \in \mathbb{N}$ ist $\mathbb{Z}/n\mathbb{Z}$ genau dann ein Körper, wenn $n \in \mathbb{P}$ gilt.*

Beweis. Nach Beispiel I.7.9 ist $n\mathbb{Z}$ genau dann maximal, wenn $n \in \mathbb{P}$. □

Definition I.7.14. Für $p \in \mathbb{P}$ setzt man $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$.

Satz I.7.15. *Für $n \in \mathbb{N}$ gilt $(\mathbb{Z}/n\mathbb{Z})^\times = \{a + n\mathbb{Z} : \mathrm{ggT}(a, n) = 1\}$. Insbesondere ist* $\boxed{|(\mathbb{Z}/n\mathbb{Z})^\times| = \varphi(n).}$

Beweis. Für $a \in \mathbb{Z}$ gilt

$$\begin{aligned} \mathrm{ggT}(a, n) = 1 &\overset{I.2.28}{\iff} \exists x \in \mathbb{Z} : ax \equiv 1 \pmod{n} \\ &\iff \exists x \in \mathbb{Z} : (a + n\mathbb{Z})(x + n\mathbb{Z}) = ax + n\mathbb{Z} = 1 + n\mathbb{Z} \\ &\iff a + n\mathbb{Z} \in (\mathbb{Z}/n\mathbb{Z})^\times. \end{aligned}$$

□

Bemerkung I.7.16. Die Elemente aus $(\mathbb{Z}/n\mathbb{Z})^\times$ nennt man *prime* Restklassen modulo n.

Beispiel I.7.17. Wir wollen das Inverse von $7 + 31\mathbb{Z}$ in $(\mathbb{Z}/31\mathbb{Z})^\times$ bestimmen. Der euklidische Algorithmus liefert $1 = \mathrm{ggT}(7, 31) = 9 \cdot 7 - 2 \cdot 31$. Also ist $(7 + 31\mathbb{Z})^{-1} = 9 + 31\mathbb{Z}$.

Folgerung I.7.18 (Euler-Fermat)**.** *Für $a \in \mathbb{Z}$ und $n \in \mathbb{N}$ mit $\mathrm{ggT}(a, n) = 1$ gilt $a^{\varphi(n)} \equiv 1 \pmod{n}$. Insbesondere ist $a^{p-1} \equiv 1 \pmod{p}$ für $p \in \mathbb{P}$ mit $p \nmid a$.*

Beweis. Für $G := (\mathbb{Z}/n\mathbb{Z})^\times$ gilt

$$a^{\varphi(n)} + n\mathbb{Z} = (a + n\mathbb{Z})^{\varphi(n)} = (a + n\mathbb{Z})^{|G|} = 1 + n\mathbb{Z}.$$

nach Bemerkung I.3.12. Die zweite Aussage folgt aus $\varphi(p) = p - 1$. □

Beispiel I.7.19 (RSA-Verfahren)**.**

(i) Euler möchte Gauß eine geheime Nachricht $n \in \mathbb{N}$ über einen unsicheren Kanal (z. B. Internet) schicken. Dafür wählt Gauß verschiedene Primzahlen $p, q > \max\{n, 10^{1000}\}$ und $d \in \mathbb{Z}$ mit $\mathrm{ggT}(d, \varphi(pq)) = 1$. Nach Satz I.7.15 existieren $e, k \in \mathbb{Z}$ mit $de = 1 + k\varphi(pq)$. Die Zahlen pq und e bilden den öffentlichen Schlüssel von Gauß, während d geheim bleibt. Nun verschickt Euler die verschlüsselte Nachricht $\tilde{n} \equiv n^e \pmod{pq}$. Zum Entschlüsseln benutzt Gauß die Formel

$$\tilde{n}^d \equiv n^{de} \equiv n^{1+k\varphi(pq)} \equiv n(n^{\varphi(pq)})^k \equiv n \pmod{pq}$$

nach Euler-Fermat (wegen $n < pq$ ist das Ergebnis eindeutig bestimmt). Ohne Kenntnis von p und q kann ein Angreifer weder $\varphi(pq)$ noch d berechnen (vgl. Aufgabe I.12). Da man keinen effizienten Faktorisierungsalgorithmus (für pq) kennt, ist dieses Verfahren (bis jetzt) sicher. Die meisten (großen) Internetseiten sind heutzutage auf diese Weise verschlüsselt (`https`).

(ii) Anstatt $\tilde{n}^d \pmod{pq}$ zu berechnen, kann Gauß auch die kleineren Potenzen

$$\begin{aligned} \tilde{n}^d &\equiv \tilde{n}^{d_p} \pmod{p} && \text{mit } d_p \equiv d \pmod{p-1}, \\ \tilde{n}^d &\equiv \tilde{n}^{d_q} \pmod{q} && \text{mit } d_q \equiv d \pmod{q-1} \end{aligned}$$

bestimmen und anschließend den chinesischen Restsatz benutzen (vgl. Beispiel I.2.34). Zur effizienten Berechnung von $\tilde{n}^d$ benutzt man außerdem die Binärdarstellung von d. Zum Beispiel

$$\tilde{n}^{11} = \big((\tilde{n}^2)^2\tilde{n}\big)^2\tilde{n}.$$

Dies benötigt nur fünf (anstatt zehn) Multiplikationen.

Bemerkung I.7.20. Im Gegensatz zu $\mathbb{Z}/n\mathbb{Z}$ ist $(\mathbb{Z}/n\mathbb{Z})^\times$ in der Regel nicht zyklisch. Für jedes ungerade $a \in \mathbb{Z}$ ist beispielsweise $a^2 \equiv 1 \pmod{8}$. Dies zeigt $(\mathbb{Z}/8\mathbb{Z})^\times \cong C_2 \times C_2$.

Definition I.7.21. Ein (*Ring*)*homomorphismus* zwischen Ringen R und S ist eine Abbildung $f\colon R \to S$ mit $f(1_R) = 1_S$ und $f(a \mathbin{\dot{+}} b) = f(a) \mathbin{\dot{+}} f(b)$ für alle $a, b \in R$. Wie üblich definiert man Mono-, Epi-, Endo-, Iso- und Automorphismen von Ringen. Außerdem sei $\mathrm{Ker}(f) := \{x \in R : f(x) = 0\}$.

Bemerkung I.7.22.

(i) Die Eigenschaft $f(1) = 1$ verhindert, dass die Abbildung $R \to S$, $a \mapsto 0$ ein Ringhomomorphismus ist.

(ii) Jeder Ringhomomorphismus $f\colon R \to S$ ist ein Gruppenhomomorphismus $(R,+) \to (S,+)$. Nach Lemma I.3.28 ist f genau dann injektiv, wenn $\mathrm{Ker}(f) = \{0\}$. Durch Einschränkung erhält man einen Gruppenhomomorphismus $(R^\times,\cdot) \to (S^\times,\cdot)$.

Beispiel I.7.23.

(i) Ist R ein Teilring von S, so ist die Inklusion $R \hookrightarrow S$ ein Monomorphismus.

(ii) Für $I \trianglelefteq R$ existiert (wie für Gruppen) der *kanonische* Epimorphismus $R \to R/I$, $a \mapsto a + I$.

Satz I.7.24. *Für teilerfremde $n, m \in \mathbb{N}$ gilt* $\boxed{(\mathbb{Z}/nm\mathbb{Z})^\times \cong (\mathbb{Z}/n\mathbb{Z})^\times \times (\mathbb{Z}/m\mathbb{Z})^\times.}$

Beweis. Aus dem Beweis von Satz I.3.34 kennen wir bereits den Gruppenisomorphismus

$$\begin{aligned} f\colon \mathbb{Z}/nm\mathbb{Z} &\to (\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z}),\\ a + nm\mathbb{Z} &\mapsto (a + n\mathbb{Z}, a + m\mathbb{Z}). \end{aligned}$$

Offenbar ist f sogar ein Ringisomorphismus und die Behauptung folgt aus Beispiel I.7.5(iv). □

Beispiel I.7.25. Es gilt $(\mathbb{Z}/12\mathbb{Z})^\times \cong (\mathbb{Z}/4\mathbb{Z})^\times \times (\mathbb{Z}/3\mathbb{Z})^\times \cong C_2 \times C_2$.

Bemerkung I.7.26. Wir werden später die Struktur von $(\mathbb{Z}/p^n\mathbb{Z})^\times$ für $p \in \mathbb{P}$ bestimmen (Satz I.8.34).

Satz I.7.27. *Für $n \in \mathbb{N}$ gilt* $\mathrm{Aut}(C_n) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.

Beweis. Sei $\langle x\rangle \cong C_n$. Für $\alpha \in \mathrm{Aut}(\langle x\rangle)$ ist $\alpha(x) = x^a$ mit $a \in \mathbb{Z}$. Wegen

$$n = |\langle \alpha(x)\rangle| = |\langle x^a\rangle| \overset{I.3.7}{=} \frac{n}{\mathrm{ggT}(n,a)}$$

ist $a + n\mathbb{Z} \in (\mathbb{Z}/n\mathbb{Z})^\times$. Man erhält somit eine Abbildung

$$\begin{aligned} \Phi\colon \mathrm{Aut}(\langle x\rangle) &\to (\mathbb{Z}/n\mathbb{Z})^\times,\\ \alpha &\mapsto a + n\mathbb{Z}. \end{aligned}$$

Für $\beta \in \mathrm{Aut}(\langle x\rangle)$ mit $\beta(x) = x^b$ gilt

$$(\alpha \circ \beta)(x) = \alpha(\beta(x)) = \alpha(x^b) = \alpha(x)^b = x^{ab}.$$

Dies zeigt, dass Φ ein Homomorphismus ist. Gilt $a + n\mathbb{Z} = 1 + n\mathbb{Z}$, so ist $\alpha(x^i) = \alpha(x)^i = (x^a)^i = x^i$ für alle $i \in \mathbb{Z}$, d. h. $\alpha = 1$. Also ist Φ injektiv. Hat man umgekehrt $a + n\mathbb{Z} \in (\mathbb{Z}/n\mathbb{Z})^\times$ gegeben, so sieht man leicht, dass die Abbildung $x^i \mapsto x^{ia}$ einen Automorphismus von $\langle x\rangle$ definiert. Daher ist Φ auch surjektiv. □

Satz I.7.28.

(i) (Homomorphiesatz) Für jeden Ringhomomorphismus $f\colon R \to S$ ist $\mathrm{Ker}(f) \trianglelefteq R$ und $f(R)$ ist ein Teilring von S. Außerdem ist

$$\boxed{R/\mathrm{Ker}(f) \cong f(R)}$$

ein Isomorphismus von Ringen.

(ii) (*1. Isomorphiesatz*) *Sei S ein Teilring von R und $I \trianglelefteq R$. Dann ist $S + I$ ein Teilring von R, $I \trianglelefteq S + I$, $S \cap I \trianglelefteq S$ und*

$$\boxed{S/(S \cap I) \cong (S + I)/I.}$$

(iii) (*2. Isomorphiesatz*) *Seien $I, J \trianglelefteq R$ mit $I \subseteq J$. Dann ist $J/I \trianglelefteq R/I$ und*

$$\boxed{(R/I)/(J/I) \cong R/J.}$$

Beweis. Wir zeigen nur den Homomorphiesatz (für die Isomorphiesätze siehe Aufgabe I.38). Es gilt $0 \in \operatorname{Ker}(f) \neq \varnothing$. Für $a, b \in \operatorname{Ker}(f)$ und $x \in R$ ist $f(a-b) = f(a)-f(b) = 0-0 = 0$, $f(xa) = f(x)f(a) = f(x)0 = 0$ und $f(ax) = f(a)f(x) = 0f(x) = 0$. Dies zeigt $\operatorname{Ker}(f) \trianglelefteq R$. Analog ist $1_S = f(1_R) \in f(R)$ und für $f(a), f(b) \in f(R)$ ist auch $f(a) - f(b) = f(a - b) \in f(R)$ sowie $f(a)f(b) = f(ab) \in f(R)$. Also ist $f(R)$ ein Teilring von S. Wir betrachten nun

$$\begin{aligned} F\colon R/\operatorname{Ker}(f) &\to f(R), \\ a + \operatorname{Ker}(f) &\mapsto f(a). \end{aligned}$$

Für $a, b \in R$ gilt

$$\begin{aligned} a + \operatorname{Ker}(f) = b + \operatorname{Ker}(f) &\iff a - b \in \operatorname{Ker}(f) \iff f(a) - f(b) = f(a - b) = 0 \\ &\iff f(a) = f(b) \iff F(a + \operatorname{Ker}(f)) = F(b + \operatorname{Ker}(f)). \end{aligned}$$

Somit ist F wohldefiniert und injektiv. Nach Definition ist F auch surjektiv. Wegen $F(1 + \operatorname{Ker}(f)) = f(1) = 1$ und

$$\begin{aligned} F((a + \operatorname{Ker}(f)) \dot{+} (b + \operatorname{Ker}(f))) &= F(a \dot{+} b + \operatorname{Ker}(f)) = f(a \dot{+} b) = f(a) \dot{+} f(b) \\ &= F(a + \operatorname{Ker}(f)) \dot{+} F(b + \operatorname{Ker}(f)), \end{aligned}$$

für $a, b \in R$ ist F ein Ringisomorphismus. □

Bemerkung I.7.29. In der Kategorientheorie verallgemeinert man die Konzepte Gruppe, Ring, Körper, Vektorraum, ... und muss dann den Homomorphiesatz nur einmal für Kategorien beweisen (Kapitel III.5).

Satz I.7.30 (Chinesischer Restsatz für Ringe)**.** *Sei R ein Ring und $I_1, \ldots, I_n \trianglelefteq R$ mit $I_i + I_j = R$ für $i \neq j$. Dann ist*

$$\begin{aligned} R/(I_1 \cap \ldots \cap I_n) &\to R/I_1 \times \ldots \times R/I_n, \\ a + I_1 \cap \ldots \cap I_n &\mapsto (a + I_1, \ldots, a + I_n) \end{aligned}$$

ein Ringisomorphismus. Ist R kommutativ, so gilt zusätzlich $I_1 \cap \ldots \cap I_n = I_1 \ldots I_n$.

Beweis. Offenbar ist

$$\begin{aligned} f\colon R &\to R/I_1 \times \ldots \times R/I_n, \\ a &\mapsto (a + I_1, \ldots, a + I_n) \end{aligned}$$

ein Ringhomomorphismus mit Kern $I := I_1 \cap \ldots \cap I_n$. Nach dem Homomorphiesatz müssen wir zeigen, dass f surjektiv ist. Seien $a_1, \ldots, a_n \in R$ gegeben. Sei $1 \leq i \leq n$ fest. Wegen $I_i + I_j = R$ für $j \neq i$ existieren $x_j \in I_i$ und $y_j \in I_j$ mit $x_j + y_j = 1$. Die Idealeigenschaft zeigt

$$1 = \prod_{j \neq i}(x_j + y_j) = \tilde{x}_i + \prod_{j \neq i} y_j = \tilde{x}_i + \tilde{y}_i \in I_i + \bigcap_{j \neq i} I_j$$

für $i = 1, \ldots, n$. Für $a := a_1\tilde{y}_1 + \ldots + a_n\tilde{y}_n$ gilt dann

$$a + I_i = a_i\tilde{y}_i + I_i = a_i\tilde{y}_i + a_i\tilde{x}_i + I_i = a_i(\tilde{x}_i + \tilde{y}_i) + I_i = a_i + I_i$$

für $i = 1, \ldots, n$. Also ist $f(a) = (a_1 + I_1, \ldots, a_n + I_n)$ und f ist surjektiv.

Sei nun R kommutativ. Multipliziert man das Produkt $R = \prod_{i \neq j}(I_i + I_j)$ über alle Paare $i \neq j$ aus, so treten in jeden Summanden mindestens $n - 1$ verschiedene I_i auf (treten nämlich I_k und I_l nicht auf, so hätte man keinen Faktor aus $I_k + I_l$). Aus der Kommutativität von R folgt

$$I_1 \ldots I_n \subseteq I_1 \cap \ldots \cap I_n = (I_1 \cap \ldots \cap I_n) \prod_{i \neq j}(I_i + I_j) \subseteq I_1 \ldots I_n. \qquad \square$$

Beispiel I.7.31. Sei $R = \mathbb{Z}$ und $I_i = (d_i)$ für $i = 1, \ldots, n$. Die Bedingung $I_i + I_j = R$ ist dann äquivalent zu $\mathrm{ggT}(d_i, d_j) = 1$ nach Folgerung I.2.11. Außerdem ist

$$I_1 \cap \ldots \cap I_n = I_1 \ldots I_n = (d_1 \ldots d_n) = (\mathrm{kgV}(d_1, \ldots, d_n)).$$

Satz I.7.30 impliziert daher einen Spezialfall des klassischen chinesischen Restsatzes I.2.32.

Bemerkung I.7.32. In Analogie zu Gruppen nennt man einen Ring $R \neq \{0\}$ *einfach*, wenn $\{0\}$ und R die einzigen Ideale von R sind. In der Algebra II (oder Darstellungstheorie) zeigt man unter gewissen Endlichkeitsbedingungen, dass jeder einfache Ring zu einem Matrixring über einem Schiefkörper isomorph ist (siehe Bemerkung II.8.14).

8 Polynome

Bemerkung I.8.1. Im Folgenden sei K stets ein Körper.

Definition I.8.2.

(i) Ein (formales) *Polynom* über K ist eine unendliche Folge $\alpha = (a_0, a_1, \ldots) \in K^\infty$, bei der nur endliche viele Glieder a_i ungleich 0 sind. Wir schreiben α meist als formale Summe der Form $\alpha := \sum_{n=0}^{\infty} a_n X^n = \sum a_n X^n$, wobei X eine *Unbekannte* ist. Dabei gilt

$$\sum a_n X^n = \sum b_n X^n \iff a_n = b_n \ \forall n \geq 0.$$

Einzelne X-Potenzen werden als *Monome* bezeichnet. Die Menge der Polynome über K wird mit $K[X]$ bezeichnet.

(ii) Indem wir $a \in K$ mit dem *konstanten* Polynom $(a, 0, 0, \ldots) = aX^0$ identifizieren, können wir K als Teilmenge von $K[X]$ auffassen. Insbesondere ist $0, 1 \in K[X]$.

(iii) Der *Grad* von $\alpha = \sum a_n X^n \in K[X]$ ist $\deg \alpha := \sup\{n \geq 0 : a_n \neq 0\}$ mit der Konvention $\deg 0 = \sup \varnothing = -\infty$.

(iv) Man nennt $\alpha = \sum a_n X^n \in K[X] \setminus \{0\}$ *normiert*, falls $a_{\deg \alpha} = 1$. Im Allgemeinen nennt man $a_{\deg \alpha}$ den *führenden* Koeffizienten und a_0 das *Absolutglied* von α.

Beispiel I.8.3.

(i) $X^2 + 1 \in \mathbb{R}[X]$.

(ii) Es gilt $\deg(\alpha) = 0$ genau dann, wenn $\alpha \in K^\times$.

(iii) Jedes $\alpha \in K[X] \setminus \{0\}$ lässt sich durch Multiplikation mit $a_{\deg \alpha}^{-1}$ *normieren.*

Satz I.8.4. *Durch*

$$\sum a_n X^n + \sum b_n X^n := \sum (a_n + b_n) X^n,$$
$$\sum a_n X^n \cdot \sum b_n X^n := \sum_n \Big(\sum_{k=0}^{n} a_k b_{n-k} \Big) X^n$$

wird $K[X]$ zu einem kommutativen Ring mit Teilring K.

Beweis. Seien $\alpha = \sum a_n X^n, \beta = \sum b_n X^n, \gamma = \sum c_n X^n \in K[X]$. Wegen

$$\{n \in \mathbb{N}_0 : a_n + b_n \neq 0\} \subseteq \{n \in \mathbb{N}_0 : a_n \neq 0\} \cup \{n \in \mathbb{N}_0 : b_n \neq 0\}$$

ist $\alpha + \beta \in K[X]$. Die Axiome

$$(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma), \qquad \alpha + \beta = \beta + \alpha, \qquad \alpha + 0 = \alpha$$

folgen direkt aus den entsprechenden Axiomen von K. Für $-\alpha := \sum(-a_n)X^n$ gilt sicher $\alpha + (-\alpha) = 0$. Also ist $K[X]$ eine abelsche Gruppe bzgl. $+$.

Für $n > \deg(\alpha) + \deg(\beta)$ ist $\sum_{k=0}^{n} a_k b_{n-k} = 0$. Daher ist $\alpha\beta \in K[X]$. Der n-te Koeffizient von $\alpha(\beta\gamma)$ ist

$$\sum_{i=0}^{n} a_i \sum_{j=0}^{n-i} b_j c_{n-i-j} = \sum_{i+j+k=n} a_i b_j c_k = \sum_{i=0}^{n} \Big(\sum_{j=0}^{i} a_j b_{i-j} \Big) c_{n-i}.$$

Dies zeigt $\alpha(\beta\gamma) = (\alpha\beta)\gamma$. Wegen $\sum_{k=0}^{n} a_k b_{n-k} = \sum_{k=0}^{n} b_k a_{n-k}$ ist $\alpha\beta = \beta\alpha$. Die Gleichung $\alpha \cdot 1 = \alpha$ ist leicht zu sehen. Der n-te Koeffizient von $\alpha(\beta + \gamma)$ ist

$$\sum_{k=0}^{n} a_k (b_{n-k} + c_{n-k}) = \sum_{k=0}^{n} a_k b_{n-k} + \sum_{k=0}^{n} a_k c_{n-k}$$

und $\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$ folgt. Die Addition und Multiplikation konstanter Polynome entspricht genau der Addition und Multiplikation in K. Also ist K ein Teilring von $K[X]$. □

Bemerkung I.8.5. Offenbar ist $K[X]$ auch ein K-Vektorraum, wobei die Skalarmultiplikation der Multiplikation in $K[X]$ entspricht. Die X-Potenzen $1, X, X^2, \ldots$ bilden eine Basis. Insbesondere ist $\dim K[X] = \infty$.

Lemma I.8.6. *Für $\alpha, \beta \in K[X]$ gilt*

(i) $\deg(\alpha + \beta) \le \max\{\deg(\alpha), \deg(\beta)\}$,

(ii) $\deg \alpha < \deg \beta \Longrightarrow \deg(\alpha + \beta) = \deg \beta$,

(iii) $\deg(\alpha\beta) = \deg(\alpha) + \deg(\beta)$.

Insbesondere ist $K[X]$ ein Integritätsbereich.

Beweis. Wir dürfen $\alpha \neq 0 \neq \beta$ annehmen. Sei $\alpha = \sum a_n X^n$, $\beta = b_n X^n$, $d := \deg \alpha$ und $e := \deg \beta$. Dann ist $a_n + b_n = 0$, falls $n > \max\{d, e\}$. Dies zeigt die erste Behauptung. Für $d < e$ ist $a_e + b_e = b_e \neq 0$ und die zweite Behauptung folgt. Die dritte Behauptung folgt aus

$$\alpha\beta = \sum_{n=0}^{d+e} \Big(\sum_{k=0}^{n} a_k b_{n-k} \Big) X^n = \underbrace{a_d b_e}_{\neq 0} X^{d+e} + \sum_{n=0}^{d+e-1} \Big(\sum_{k=0}^{n} a_k b_{n-k} \Big) X^n.$$

Nun ergibt sich die letzte Behauptung:

$$\alpha\beta = 0 \Longrightarrow \deg(\alpha) + \deg(\beta) = \deg(\alpha\beta) = -\infty \Longrightarrow \alpha = 0 \vee \beta = 0.$$ □

Bemerkung I.8.7.

(i) Der Beweis zeigt auch: Sind $\alpha, \beta \in K[X]$ normiert, so auch $\alpha\beta$.

(ii) Nach Aufgabe I.40 kann man $K[X]$ als Teilring seines *Quotientenkörpers*

$$K(X) := Q(K[X]) = \Big\{ \frac{\alpha}{\beta} : \alpha, \beta \in K[X],\ \beta \neq 0 \Big\}$$

auffassen. Man nennt $K(X)$ den Körper der *rationalen Funktionen* über K.

Folgerung I.8.8. *Es gilt* $K[X]^\times = K^\times$.

Beweis. Sicher ist $K^\times \subseteq K[X]^\times$. Seien nun $\alpha, \beta \in K[X]^\times$ mit $\alpha\beta = 1$. Dann ist $\deg(\alpha) + \deg(\beta) = \deg(\alpha\beta) = \deg(1) = 0$ nach Lemma I.8.6. Wegen $\deg(\alpha), \deg(\beta) \geq 0$ folgt $\deg(\alpha) = \deg(\beta) = 0$ und $\alpha, \beta \in K^\times$. □

Definition I.8.9. Für $\alpha = \sum a_n X^n, \beta \in K[X]$ sei $\alpha(\beta) := \sum a_n \beta^n \in K[X]$ (*Einsetzen*). Man nennt $x \in K$ *Nullstelle* von α, falls $\alpha(x) = 0$.

Satz I.8.10. *Für* $x \in K$ *ist die Abbildung* $F_x \colon K[X] \to K$, $\alpha \mapsto \alpha(x)$ *ein Ringhomomorphismus, den man* Einsetzungshomomorphismus *nennt.*

Beweis. Es gilt $F_x(1) = 1(x) = 1$. Für $\alpha = \sum a_n X^n \in K[X]$ und $\beta = \sum b_n X^n \in K[X]$ ist

$$(\alpha + \beta)(x) = \sum (a_n + b_n) x^n = \sum a_n x^n + \sum b_n x^n = \alpha(x) + \beta(x).$$

Analog ist

$$(\alpha\beta)(x) = \Big(\sum_n \sum_{k=0}^n a_k b_{n-k} X^n\Big)(x) = \sum_n \sum_{k=0}^n a_k b_{n-k} x^n = \Big(\sum a_n x^n\Big)\Big(\sum b_n x^n\Big) = \alpha(x)\beta(x). \quad \square$$

Bemerkung I.8.11.

(i) Der gleiche Beweis zeigt $(\alpha + \beta)(\gamma) = \alpha(\gamma) + \beta(\gamma)$ und $(\alpha\beta)(\gamma) = \alpha(\gamma)\beta(\gamma)$ für $\alpha, \beta, \gamma \in K[X]$. Andererseits ist im Allgemeinen $\alpha(\beta + \gamma) \neq \alpha(\beta) + \alpha(\gamma)$ und $\alpha(\beta\gamma) \neq \alpha(\beta)\alpha(\gamma)$.

(ii) Zur effizienten Berechnung von $\alpha(x)$ für $\alpha = a_n X^n + \ldots + a_1 X + a_0 \in K[X]$ und $x \in K$ benutzt man das Horner-Schema:

$$\big(\ldots\big((a_n x + a_{n-1})x + a_{n-2}\big)x + \ldots\big)x + a_0.$$

Dies erfordert nur n (anstatt $2n - 1$) Multiplikationen. Damit wurde früher die Einkommensteuer berechnet.

(iii) Ist K endlich, so können verschiedene Polynome die gleiche Abbildung $K \to K$ durch Einsetzen induzieren, denn es gibt nur endlich viele solche Abbildungen. Man kann also nicht wie in der Analysis Polynome mit ihren Funktionen gleichsetzen.

Beispiel I.8.12. Für $\alpha := X^2 + X \in \mathbb{F}_2[X]$ gilt $\alpha(x) = 0$ für alle $x \in \mathbb{F}_2$.

Definition I.8.13. Wie in $\mathbb{Z}$ definieren wir die Teilbarkeit $\alpha \mid \beta$ für $\alpha, \beta \in K[X]$, falls ein $\gamma \in K[X]$ mit $\alpha\gamma = \beta$ existiert. Allgemeiner sei $\alpha \equiv \beta \pmod{\gamma}$, falls $\gamma \mid (\alpha - \beta)$.

Bemerkung I.8.14. Wie in $\mathbb{Z}$ beweist man die üblichen Rechenregeln:

- $\pm 1 \mid \alpha \mid 0$,
- $0 \mid \alpha \iff \alpha = 0$,
- $\alpha \mid \beta \mid \gamma \implies \alpha \mid \gamma$,
- $\alpha \mid \beta \mid \alpha \implies \exists c \in K^\times : \alpha = c\beta$,

- $\alpha \mid \beta, \gamma \Longrightarrow \alpha \mid (\beta\delta + \gamma\psi)$,
- $\alpha \mid \beta \neq 0 \Longrightarrow \deg \alpha \leq \deg \beta$

für $\alpha, \beta, \gamma, \delta, \psi \in K[X]$.

Satz I.8.15 (Division mit Rest)**.** *Für $\alpha \in K[X]$ und $\beta \in K[X] \setminus \{0\}$ existieren eindeutig bestimmte $\gamma, \delta \in K[X]$ mit $\alpha = \beta\gamma + \delta$ und $\deg \delta < \deg \beta$.*

Beweis. Wähle $\gamma \in K[X]$, sodass

$$\delta := \alpha - \beta\gamma = \sum a_n X^n$$

möglichst kleinen Grad $d \in \mathbb{N}_0 \cup \{-\infty\}$ hat. Sei $\beta = \sum b_n X^n$ und $e := \deg \beta$. Gilt $d \geq e$, so ist

$$\deg\big(\alpha - \beta(\gamma + a_d b_e^{-1} X^{d-e})\big) = \deg\big(\delta - a_d b_e^{-1} X^{d-e}\beta\big) < d$$

im Widerspruch zur Wahl von γ. Also ist $d < e$ und $\alpha = \beta\gamma + \delta$.

Sei nun $\alpha = \beta\tilde{\gamma} + \tilde{\delta}$ mit $\deg \tilde{\delta} < e$. Nach Lemma I.8.6 ist

$$e + \deg(\tilde{\gamma} - \gamma) = \deg(\beta(\tilde{\gamma} - \gamma)) = \deg(\delta - \tilde{\delta}) \leq \max\{\deg(\delta), \deg(\tilde{\delta})\} < e$$

und es folgt $(\tilde{\gamma}, \tilde{\delta}) = (\gamma, \delta)$. □

Definition I.8.16. Für $\alpha_1, \ldots, \alpha_n \in K[X]$ sei (wie in $\mathbb{Z}$) $\mathrm{gT}(\alpha_1, \ldots, \alpha_n)$ die Menge der gemeinsamen Teiler von $\alpha_1, \ldots, \alpha_n$. Ein normiertes $\alpha \in \mathrm{gT}(\alpha_1, \ldots, \alpha_n)$ (oder $\alpha = 0$) heißt *größter gemeinsamer Teiler* von $\alpha_1, \ldots, \alpha_n$, falls $\beta \mid \alpha$ für alle $\beta \in \mathrm{gT}(\alpha_1, \ldots, \alpha_n)$ gilt.

Bemerkung I.8.17. Sind α, β größte gemeinsame Teiler von $\alpha_1, \ldots, \alpha_n$, so gilt $\alpha \mid \beta \mid \alpha$. Nach Bemerkung I.8.14 existiert $c \in K^\times$ mit $\alpha = c\beta$. Da α und β normiert sind (oder 0), gilt $\alpha = \beta$. Also gibt es höchstens einen größten gemeinsamen Teiler und wir schreiben (wie in $\mathbb{Z}$) $\mathrm{ggT}(\alpha_1, \ldots, \alpha_n) := \alpha$. Der folgende Satz zeigt die Existenz des ggTs.

Satz I.8.18 (Erweiterter euklidischer Algorithmus in $K[X]$)**.**
Eingabe: $\alpha, \beta \in K[X] \setminus \{0\}$.
Initialisierung: $(\sigma_0, \tau_0, \rho_0) := (1, 0, \alpha)$, $(\sigma_1, \tau_1, \rho_1) := (0, 1, \beta)$ *und* $k := 0$.
Solange $\rho_{k+1} \neq 0$ *wiederhole:*
    Division mit Rest: $\rho_k = \lambda_{k+1}\rho_{k+1} + \epsilon_{k+1}$ *mit* $\deg(\epsilon_{k+1}) < \deg(\rho_{k+1})$.
    Setze $(\sigma_{k+2}, \tau_{k+2}, \rho_{k+2}) := (\sigma_k - \sigma_{k+1}\lambda_{k+1}, \tau_k - \tau_{k+1}\lambda_{k+1}, \epsilon_{k+1})$ *und* $k := k + 1$.
Wähle $a \in K$*, sodass* $a\rho_k$ *normiert ist.*
Ausgabe: $a\rho_k = a\sigma_k\alpha + a\tau_k\beta = \mathrm{ggT}(\alpha, \beta)$.

Beweis. Wie in $\mathbb{Z}$ (siehe auch Lineare Algebra 2). □

Beispiel I.8.19. Seien $\alpha = X^3 + 2X - 1$ und $\beta = X^2 - X + 4$ in $\mathbb{Q}[X]$. Polynomdivision ergibt $\alpha = \beta(X + 1) - X - 5$ und $\beta = (X + 5)(X - 6) + 34$. Also

σ_i	τ_i	ρ_i	λ_i
1	0	α	
0	1	β	$X + 1$
1	$-X - 1$	$-X - 5$	$-X + 6$
$X - 6$	$-X^2 + 5X + 7$	$\boxed{34}$	
		0	

.

Normierung liefert $\mathrm{ggT}(\alpha,\beta) = 1 = \frac{1}{34}(X-6)\alpha - \frac{1}{34}(X^2-5X-7)\beta$.

Definition I.8.20. Polynome $\alpha_1,\dots,\alpha_n \in K[X]$ heißen *teilerfremd*, falls $\mathrm{ggT}(\alpha_1,\dots,\alpha_n) = 1$.

Folgerung I.8.21. *Genau dann sind $\alpha,\beta \in K[X]$ teilerfremd, wenn $\tilde{\alpha},\tilde{\beta} \in K[X]$ mit $\alpha\tilde{\alpha}+\beta\tilde{\beta}=1$ existieren.*

Beweis. Ist $\mathrm{ggT}(\alpha,\beta)=1$, so folgt die Existenz von $\tilde{\alpha}$ und $\tilde{\beta}$ aus Satz I.8.18. Ist umgekehrt $\alpha\tilde{\alpha}+\beta\tilde{\beta}=1$, so gilt $\mathrm{ggT}(\alpha,\beta) \mid (\alpha\tilde{\alpha}+\beta\tilde{\beta}) = 1$ und $\mathrm{ggT}(\alpha,\beta)=1$. □

Definition I.8.22. Ein normiertes Polynom $\alpha \in K[X]\setminus K$ heißt *irreduzibel*, falls es sich nicht in der Form $\alpha=\beta\gamma$ mit $\beta,\gamma \in K[X]\setminus K$ schreiben lässt (d. h. α hat genau zwei normierte Teiler nämlich 1 und α, vgl. Primzahl). Anderenfalls nennt man α *reduzibel*.

Beispiel I.8.23.

(i) Normierte Polynome vom Grad 1 sind stets irreduzibel. Wir zeigen später, dass jedes irreduzible Polynom in $\mathbb{C}[X]$ Grad 1 hat (Fundamentalsatz der Algebra).

(ii) X^2-2 ist irreduzibel in $\mathbb{Q}[X]$, aber nicht in $\mathbb{R}[X]$, denn $X^2-2 = (X-\sqrt{2})(X+\sqrt{2}) \in \mathbb{R}[X]$ und $\sqrt{2} \notin \mathbb{Q}$.

(iii) X^2+1 ist irreduzibel in $\mathbb{R}[X]$, aber nicht in $\mathbb{C}[X]$, denn $X^2+1 = (X-\mathrm{i})(X+\mathrm{i}) \in \mathbb{C}[X]$.

(iv) X^2+X+1 ist irreduzibel in $\mathbb{F}_2[X]$, denn $X^2+X+1 \notin \{X^2, X(X+1)=X^2+X, (X+1)^2=X^2+1\}$.

Satz I.8.24 (Primfaktorzerlegung in $K[X]$)**.** *Für jedes Polynom $\alpha \in K[X]\setminus\{0\}$ existieren bis auf die Reihenfolge eindeutig bestimmte irreduzible Polynome $\sigma_1,\dots,\sigma_n \in K[X]$ und eine eindeutig bestimmte Konstante $c \in K^\times$ mit $\alpha = c\sigma_1\dots\sigma_n$.*

Beweis.
Existenz: Wegen $\alpha \neq 0$ existiert $c \in K^\times$, sodass $c^{-1}\alpha$ normiert ist. Wir können also annehmen, dass α normiert ist. Induktion nach $d := \deg\alpha$: Im Fall $d=0$ ist $\alpha=1$ und wir wählen $n=0$ (leeres Produkt). Ist α irreduzibel (zum Beispiel $d=1$), so sind wir ebenfalls fertig. Anderenfalls ist $\alpha=\beta\gamma$ mit $\beta,\gamma \in K[X]\setminus K$. Wegen $d=\deg(\beta\gamma)=\deg(\beta)+\deg(\gamma)$ ist $\deg\beta, \deg\gamma < d$. Nach Induktion sind β und γ Produkte von irreduziblen Polynomen und Konstanten und daher auch α.

Eindeutigkeit: Offenbar ist c als führender Koeffizient von α eindeutig bestimmt. Wir können also wieder annehmen, dass α normiert ist. Sei $\alpha = \sigma_1\dots\sigma_n = \tau_1\dots\tau_m$ mit irreduziblen $\sigma_1,\dots,\sigma_n,\tau_1,\dots,\tau_m \in K[X]$. Induktion nach m: Im Fall $m=1$ ist $n=1$ und $\sigma_1=\alpha=\tau_1$. Sei nun $m \geq 2$. Im Fall $\sigma_1=\tau_1$ ist $\sigma_2\dots\sigma_n = \tau_2\dots\tau_m$ und Induktion liefert die Behauptung. Sei nun $\sigma_1 \neq \tau_1$. Dann existieren $\tilde{\sigma},\tilde{\tau} \in K[X]$ mit $\sigma_1\tilde{\sigma}+\tau_1\tilde{\tau}=1$ nach Folgerung I.8.21. Es folgt

$$\sigma_1(\tilde{\sigma}\tau_2\dots\tau_m + \sigma_2\dots\sigma_n\tilde{\tau}) = \sigma_1\tilde{\sigma}\tau_2\dots\tau_m + \tau_1\dots\tau_m\tilde{\tau} = (\sigma_1\tilde{\sigma}+\tau_1\tilde{\tau})(\tau_2\dots\tau_m) = \tau_2\dots\tau_m.$$

Induktiv erhält man $\sigma_1=\tau_i$ für ein $i \in \{1,\dots,m\}$. Dann ist $\sigma_2\dots\sigma_n = \tau_1\dots\tau_{i-1}\tau_{i+1}\dots\tau_m$ und Induktion liefert die Behauptung. □

Beispiel I.8.25. In $\mathbb{F}_2$ ist $X^4-X = X(X+1)(X^2+X+1)$ die Primfaktorzerlegung von X^4-X.

Bemerkung I.8.26. Ringe, die eine eindeutige Primfaktorzerlegung zulassen nennt man *faktoriell* (Definition II.5.11). In der algebraischen Zahlentheorie geht man einen Schritt weiter und untersucht Ringe, in denen Ideale eindeutig zerlegt werden können (Satz II.11.28). Dies ist für den Beweis von *Fermats letzten Satz* relevant ($x^n + y^n = z^n$ hat keine Lösung $(x, y, z) \in \mathbb{N}^3$ für $n \geq 3$).

Lemma I.8.27. *Ist $x \in K$ eine Nullstelle von $\alpha \in K[X]$, so ist $X - x$ ein Teiler von α.*

Beweis. Division mit Rest liefert $\alpha = (X-x)\beta+r$ mit $\beta \in K[X]$ und $r \in K$. Dann ist $r = \alpha(x) = 0$. □

Definition I.8.28. In der Situation von Lemma I.8.27 ist $X - x$ ein *Linearfaktor* von α. Die größte natürliche Zahl m mit $(X - x)^m \mid \alpha$ heißt *Vielfachheit* der Nullstelle. Im Fall $m = 1$ ist x eine *einfache* Nullstelle und anderenfalls eine *mehrfache* Nullstelle.

Satz I.8.29. *Jedes $\alpha \in K[X] \setminus \{0\}$ hat höchstens $\deg \alpha$ Nullstellen in K (mit Vielfachheiten).*

Beweis. Induktion nach $d := \deg \alpha$. Im Fall $d = 0$ ist α konstant und hat daher keine Nullstelle. Sei nun $d > 0$ und $x \in K$ eine Nullstelle von α mit Vielfachheit m. Dann ist $\alpha = (X - x)^m\beta$ für ein $\beta \in K[X]$ mit $\deg \beta = d - m < d$. Für jede weitere Nullstelle $y \neq x$ von α gilt $0 = \alpha(y) = (y - x)^m\beta(y) = \beta(y)$. Also ist y auch Nullstelle von β. Nach Induktion besitzt β höchstens $d - m$ Nullstellen. Insgesamt hat α also höchstens $m + d - m = d$ Nullstellen. □

Beispiel I.8.30 (Interpolation)**.** Hat man Koordinaten $(x_1, y_1), \ldots, (x_n, y_n) \in K^2$ mit paarweise verschiedenen $x_1, \ldots, x_n$ gegeben, so verläuft das LAGRANGE-Polynom

$$\alpha := \sum_{i=1}^{n} y_i \prod_{j \neq i} \frac{X - x_j}{x_i - x_j} \in K[X]$$

vom Grad $< n$ genau durch die Punkte $(x_1, y_1), \ldots, (x_n, y_n)$. Ist auch $\beta \in K[X]$ mit $\deg \beta < n$ und $\beta(x_i) = y_i$ für $i = 1, \ldots, n$, so sind $x_1, \ldots, x_n$ Nullstellen von $\alpha - \beta$ mit $\deg(\alpha - \beta) < n$. Satz I.8.29 zeigt $\alpha = \beta$, d. h. α ist das einzige Polynom vom Grad $< n$, dass die gegebenen Punkte interpoliert.

Satz I.8.31. *Jede endliche Untergruppe von $K^\times$ ist zyklisch.*

Beweis. Sei $G \leq K^\times$ endlich. Als abelsche Gruppe ist G die direkte Summe ihrer Sylowgruppen (Beispiel I.5.6). Nach Lemma I.5.3 und Satz I.3.34 genügt es zu zeigen, dass die Sylowgruppen von G zyklisch sind. Sei also $|G| = p^n$ mit $p \in \mathbb{P}$ und o. B. d. A. $n \geq 1$. Nach Satz I.8.29 hat das Polynom $X^{p^{n-1}} - 1 \in K[X]$ höchstens $p^{n-1} < |G|$ Nullstellen. Also existiert ein $g \in G$ mit $g^{p^{n-1}} \neq 1$. Nach Lagrange ist andererseits $|\langle g \rangle|$ ein Teiler von p^n. Dies zeigt $G = \langle g \rangle$. □

Bemerkung I.8.32. Insbesondere ist $\mathbb{F}_p^\times$ für $p \in \mathbb{P}$ zyklisch. Man nennt $x \in \mathbb{F}_p$ mit $\mathbb{F}_p^\times = \langle x \rangle$ eine *Primitivwurzel* modulo p. Man kennt keine Formel um Primitivwurzeln für ein gegebenes p zu berechnen, aber in der Regel findet man „kleine“ Primitivwurzeln[1]. Nach Lemma I.3.7 ist die Anzahl der Primitivwurzeln $\varphi(p - 1)$. Für $y \in \mathbb{F}_p^\times = \langle x \rangle$ kennt man auch keinen schnellen Algorithmus zur Berechnung von $k \in \mathbb{Z}$ mit $y = x^k$ (diskreter Logarithmus). Diesen Umstand nutzt man in der Kryptografie aus (Beispiel I.2.25).

[1] Siehe `https://oeis.org/A001918`

Beispiel I.8.33. Wir suchen eine Primitivwurzel modulo 7. Jedes $x \in \mathbb{F}_7^\times$ hat Ordnung $1, 2, 3$ oder $\varphi(7) = 6$ nach Lagrange. Wegen $2^3 \equiv 1 \pmod 7$ ist 2 keine Primitivwurzel modulo 7. Wegen $3^2 \equiv 2 \pmod 7$ und $3^3 \equiv 2 \cdot 3 \equiv -1 \pmod 7$ ist 3 eine Primitivwurzel modulo 7.

Satz I.8.34 (Gauss)**.** *Für $p \in \mathbb{P}$ und $n \in \mathbb{N}$ gilt*

$$(\mathbb{Z}/p^n\mathbb{Z})^\times \cong \begin{cases} C_2 \times C_{2^{n-2}} & \text{falls } p = 2 \leq n, \\ C_{p^{n-1}(p-1)} & \text{sonst.} \end{cases}$$

Beweis. Sei $G := (\mathbb{Z}/p^n\mathbb{Z})^\times$. Sei zunächst $p > 2$. Wegen $|G| = \varphi(p^n) = p^{n-1}(p-1)$ genügt es zu zeigen, dass G zyklisch ist. Für $n = 1$ folgt die Behauptung aus Satz I.8.31. Sei nun $n \geq 2$. Die kanonische Abbildung $\Psi\colon G \to (\mathbb{Z}/p\mathbb{Z})^\times$, $a + p^n\mathbb{Z} \mapsto a + p\mathbb{Z}$ ist offenbar ein wohldefinierter Epimorphismus. Nach dem Homomorphiesatz ist $P := \operatorname{Ker}(\Psi) \in \operatorname{Syl}_p(G)$ und $G/P \cong C_{p-1}$. Nach dem Hauptsatz über endliche abelsche Gruppen genügt es zu zeigen, dass P zyklisch ist. Wir zeigen genauer, dass P von $1 + p + p^n\mathbb{Z} \in P$ erzeugt wird. Dafür berechnet man

$$(1+p)^{p^{n-2}} = \sum_{k=0}^{p^{n-2}} \binom{p^{n-2}}{k} p^k \equiv 1 + p^{n-1} \not\equiv 1 \pmod{p^n}.$$

Sei nun $p = 2$ und o. B. d. A. $n \geq 2$. Dann ist $|G| = 2^{n-1}$. Wegen $(-1 + 2^n\mathbb{Z})^2 = 1 + 2^n\mathbb{Z}$ genügt es

$$G = \langle -1 + 2^n\mathbb{Z} \rangle \oplus \langle 5 + 2^n\mathbb{Z} \rangle$$

zu zeigen. Der Fall $n = 2$ ist klar. Sei also $n \geq 3$. Man berechnet

$$5^{2^{n-3}} = (1+4)^{2^{n-3}} = \sum_{k=0}^{2^{n-3}} \binom{2^{n-3}}{k} 2^{2k} \equiv 1 + 2^{n-1} \pmod{2^n}.$$

und

$$5^{2^{n-2}} \equiv (1 + 2^{n-1})^2 \equiv 1 \pmod{2^n}.$$

Also ist $|\langle 5 + 2^n\mathbb{Z} \rangle| = 2^{n-2}$. Wegen $-1 \not\equiv 1 + 2^{n-1} \pmod{2^n}$ ist auch $\langle -1 + 2^n\mathbb{Z} \rangle \cap \langle 5 + 2^n\mathbb{Z} \rangle = 1$. □

Folgerung I.8.35. *Genau dann ist $(\mathbb{Z}/n\mathbb{Z})^\times$ zyklisch, wenn $n \in \{4, p^m, 2p^m\}$ für eine ungerade Primzahl p und $m \in \mathbb{N}_0$ gilt.*

Beweis. Besitzt n mehrere ungerade Primteiler, so ist $C_2 \times C_2$ eine Untergruppe von $G := (\mathbb{Z}/n\mathbb{Z})^\times$ nach Satz I.7.24 und Satz I.5.12. Dann kann G aber nicht zyklisch sein (Satz I.3.34). Genauso kann n nicht gleichzeitig durch 4 und eine ungerade Primzahl teilbar sein. Nach Satz I.8.34 kann n auch nicht durch 8 teilbar sein. Wegen $(\mathbb{Z}/2p^m\mathbb{Z})^\times \cong (\mathbb{Z}/p^m\mathbb{Z})^\times$ ist G in den angegebenen Fällen stets zyklisch. □

Bemerkung I.8.36. Für $\alpha \in K[X]$ kann man das Hauptideal $(\alpha) = K[X]\alpha$ bilden, sodass $K[X]/(\alpha)$ ein Ring wird (Satz I.7.10). Es gilt dann

$$\beta + (\alpha) = \gamma + (\alpha) \iff \beta - \gamma \in (\alpha) \iff \alpha \mid (\beta - \gamma) \iff \beta \equiv \gamma \pmod{\alpha}$$

(vgl. $\mathbb{Z}/n\mathbb{Z}$).

Lemma I.8.37. *Jedes Ideal von $K[X]$ ist ein Hauptideal. Dabei gilt $(\alpha) \subseteq (\beta) \iff \beta \mid \alpha$.*

Beweis. Sei $(0) \neq I \trianglelefteq K[X]$ und $\alpha \in I \setminus \{0\}$ mit minimalem Grad $d \geq 0$. Für $\beta \in I$ existieren $\gamma, \delta \in K[X]$ mit $\beta = \alpha\gamma + \delta$ und $\deg \delta < d$. Wegen $\delta = \beta - \alpha\gamma \in I$ ist $\delta = 0$ und $\beta = \alpha\gamma \in (\alpha)$. Dies zeigt $I = (\alpha)$. Die zweite Aussage folgt leicht. □

Satz I.8.38. *Genau dann ist $\alpha \in K[X]$ irreduzibel, wenn $K[X]/(\alpha)$ ein Körper ist.*

Beweis. Die Behauptung folgt aus Satz I.7.12 und Lemma I.8.37. □

Beispiel I.8.39. Wir wissen bereits, dass $\alpha = X^2 - 2 \in \mathbb{Q}[X]$ irreduzibel ist. Also ist $X + (\alpha)$ im Körper $\mathbb{Q}[X]/(\alpha)$ invertierbar. Der euklidische Algorithmus liefert

$$1 = \mathrm{ggT}(X, \alpha) = \frac{1}{2}X^2 - \frac{1}{2}\alpha \equiv \frac{1}{2}X^2 \pmod{\alpha}.$$

Daher ist $(X + (\alpha))^{-1} = \frac{1}{2}X + (\alpha)$.

Definition I.8.40. Einen Ringhomomorphismus zwischen Körpern nennt man *(Körper)homomorphismus*.

Lemma I.8.41. *Jeder Körperhomomorphismus ist injektiv.*

Beweis. Sei $\sigma\colon K \to L$ ein Körperhomomorphismus und $x \in \mathrm{Ker}(\sigma)$. Im Fall $x \neq 0$ wäre $1 = \sigma(1) = \sigma(xx^{-1}) = \sigma(x)\sigma(x^{-1}) = 0$. Also ist $\mathrm{Ker}(\sigma) = \{0\}$ und die Behauptung folgt aus Bemerkung I.7.22. □

Bemerkung I.8.42.

(i) Genau dann ist $\sigma\colon K \to L$ ein Körperhomomorphismus, wenn $\sigma\colon (K, +) \to (L, +)$ und $\sigma\colon (K^\times, \cdot) \to (L^\times, \cdot)$ Gruppenmonomorphismen sind.

(ii) Die Isomorphismen $K \to K$ nennt man *Automorphismen*. Sie bilden die Automorphismengruppe $\mathrm{Aut}(K)$ bzgl. Komposition.

Beispiel I.8.43.

(i) Sei $\sigma \in \mathrm{Aut}(\mathbb{F}_p)$ für $p \in \mathbb{P}$. Dann ist $\sigma(1) = 1$, $\sigma(1 + 1) = \sigma(1) + \sigma(1) = 1 + 1$, usw. Dies zeigt $\sigma = \mathrm{id}$ und $\mathrm{Aut}(\mathbb{F}_p) = \{\mathrm{id}\} = 1$.

(ii) Nach Aufgabe I.53 ist $\mathrm{Aut}(\mathbb{Q}) = 1$ und $\mathrm{Aut}(\mathbb{R}) = 1$.

(iii) Die komplexe Konjugation ist ein Körperautomorphismus auf $\mathbb{C}$. Mit dem Auswahlaxiom kann man zeigen, dass $\mathrm{Aut}(\mathbb{C})$ überabzählbar ist (Satz II.4.21).

Lemma I.8.44. *Jeder Körperhomomorphismus $\sigma\colon K \to L$ lässt sich zu einem Ringhomomorphismus*

$$K[X] \to L[X],$$
$$\sum a_n X^n \mapsto \sum \sigma(a_n) X^n$$

fortsetzen, den wir ebenfalls mit σ bezeichnen. Für $\alpha \in K[X]$ und $x \in K$ gilt dabei

$$\boxed{\sigma(\alpha(x)) = \sigma(\alpha)(\sigma(x)).}$$

Beweis. Sicher ist $\sigma(1) = 1$. Für $\alpha = \sum a_n X^n, \beta = \sum b_n X^n$ gilt

$$\begin{aligned}\sigma(\alpha+\beta) &= \sum \sigma(a_n + b_n)X^n = \sum \sigma(a_n)X^n + \sum \sigma(b_n)X^n = \sigma(\alpha) + \sigma(\beta),\\ \sigma(\alpha\beta) &= \sum_n \sigma\Big(\sum_{k=0}^{n} a_k b_{n-k}\Big)X^n = \sum_n \Big(\sum_{k=0}^{n} \sigma(a_k)\sigma(b_{n-k})\Big)X^n\\ &= \sum \sigma(a_n)X^n \cdot \sum \sigma(b_n)X^n = \sigma(\alpha)\sigma(\beta).\end{aligned}$$

Also ist $\sigma\colon K[X] \to L[X]$ ein Ringhomomorphismus. Die zweite Aussage folgt mit

$$\sigma(\alpha(x)) = \sigma\Big(\sum a_n x^n\Big) = \sum \sigma(a_n)\sigma(x)^n = \sigma(\alpha)(\sigma(x)).$$ □

Bemerkung I.8.45. Die Polynome mit ganzzahligen Koeffizienten bilden den Unterring $\mathbb{Z}[X]$ von $\mathbb{Q}[X]$. Achtung: In $\mathbb{Z}[X]$ gibt es keine Division mit Rest! Wir beweisen drei Irreduzibilitätskriterien mit Hilfe von $\mathbb{Z}[X]$.

Definition I.8.46. Man nennt $\sum_{k=0}^{n} a_k X^k \in \mathbb{Z}[X]$ *primitiv*, falls $\mathrm{ggT}(a_0, \ldots, a_n) = 1$.

Beispiel I.8.47. Normierte Polynome sind primitiv.

Lemma I.8.48 (Gauss)**.** *Sind $\alpha, \beta \in \mathbb{Z}[X]$ primitiv, so auch $\alpha\beta$.*

Beweis. Sei $\alpha = \sum a_n X^n$ und $\beta = \sum b_n X^n$. Nehmen wir indirekt an, dass $p \in \mathbb{P}$ alle Koeffizienten von $\alpha\beta$ teilt. Da α und β primitiv sind, existieren minimale Zahlen $s, t \in \mathbb{N}_0$ mit $p \nmid a_s$ und $p \nmid b_t$. Für den Koeffizienten von X^{s+t} in $\alpha\beta$ ergibt sich dann der Widerspruch

$$\sum_{k=0}^{s+t} a_k b_{s+t-k} \equiv a_s b_t \not\equiv 0 \pmod{p}.$$ □

Bemerkung I.8.49. Um (naiv) zu prüfen, ob $\alpha \in \mathbb{Q}[X]$ irreduzibel ist, müsste man Probedivisionen durch unendlich viele rationale Polynome kleineren Grades durchführen. Mit Gauß' Lemma braucht man nur endlich viele Faktoren testen. Sei beispielsweise $\beta, \gamma \in \mathbb{Q}[X] \setminus \mathbb{Q}$ mit $\alpha = \beta\gamma$. Dann existieren $b, c \in \mathbb{Q}$, sodass $b\beta \in \mathbb{Z}[X]$ und $c\gamma \in \mathbb{Z}[X]$ primitiv sind. Nach Gauß ist auch $bc\alpha = b\beta c\gamma \in \mathbb{Z}[X]$ primitiv. Offenbar ist $bc\alpha$ durch α bis auf Vorzeichen eindeutig bestimmt. Die Möglichkeiten für $b\beta$ und $c\gamma$ ergeben sich durch Koeffizientenvergleich. Das Verfahren ist allerdings aufwendig.

Beispiel I.8.50. Ist $\alpha = X^3 - \frac{1}{2}X^2 + 1 \in \mathbb{Q}[X]$ reduzibel, so existieren $a, b, c, d, e \in \mathbb{Z}$ mit

$$2\alpha = 2X^3 - X^2 + 2 = (aX + b)(cX^2 + dX + e).$$

O. B. d. A. sei $a, c \in \mathbb{N}$. Koeffizientenvergleich liefert

$$ac = 2, \qquad ad + bc = -1, \qquad ae + bd = 0, \qquad be = 2.$$

Im Fall $a = 1$ erhält man $c = 2$, $-1 = d + 2b \equiv d \pmod 2$ und $0 = e + bd \equiv e + b \pmod 2$. Also ist $b \equiv e \pmod 2$ im Widerspruch zu $be = 2$. Sei nun $a = 2$. Dann ist $c = 1$, $-1 = 2d + b \equiv b \pmod 2$ und $0 = 2e + bd \equiv d \pmod 2$. Es folgt $-1 = 2d + b \equiv b \pmod 4$. Wegen $be = 2$ ist daher $b = -1$, $e = -2$ und $d = 0$. Dies widerspricht $0 = 2e + bd$. Fazit: α ist irreduzibel.

Folgerung I.8.51. *Sei $\alpha \in \mathbb{Z}[X]$ und $\alpha = \beta\gamma$ mit normierten $\beta, \gamma \in \mathbb{Q}[X]$. Dann ist $\beta, \gamma \in \mathbb{Z}[X]$. Jede rationale Nullstelle von α ist ganzzahlig und teilt das Absolutglied von α.*

Beweis. Seien $b, c \in \mathbb{Q}$, sodass $b\beta, c\gamma \in \mathbb{Z}[X]$ primitiv sind. Da β und γ normiert sind, gilt $b, c \in \mathbb{Z}$, o. B. d. A. $b, c \in \mathbb{N}$. Nach Gauß ist $bc\alpha$ primitiv. Wegen $\alpha \in \mathbb{Z}[X]$ ist aber jeder Koeffizient von $bc\alpha$ durch bc teilbar. Dies zeigt $bc = 1$ und $b = c = 1$, d. h. $\beta, \gamma \in \mathbb{Z}[X]$. Sei nun $x \in \mathbb{Q}$ eine Nullstelle von α. Nach Lemma I.8.27 existiert ein normiertes $\beta = \sum b_n X^n \in \mathbb{Q}[X]$ mit $\alpha = (X - x)\beta$. Der erste Teil des Beweises zeigt $x, b_0 \in \mathbb{Z}$. Weiter gilt $x \mid (-x)b_0 = a_0$, wobei a_0 das Absolutglied von α ist. □

Beispiel I.8.52.

(i) Ist $\alpha = X^3 - 2X^2 + X - 1 \in \mathbb{Q}[X]$ reduzibel, so existiert eine Nullstelle $x \in \mathbb{Q}$. Folgerung I.8.51 zeigt $x = \pm 1$. Wegen $\alpha(1) = -1 \neq 0 \neq -5 = \alpha(-1)$ ist dies ausgeschlossen. Also ist α irreduzibel.

(ii) Ist $x := \sqrt{2} + \sqrt[3]{3} \in \mathbb{R}$ rational? Es gilt

$$3 = (x - \sqrt{2})^3 = x^3 - 3\sqrt{2}x^2 + 3 \cdot 2x - 2\sqrt{2} = x^3 + 6x - \sqrt{2}(3x^2 + 2)$$

und

$$18x^4 + 24x^2 + 8 = 2(3x^2 + 2)^2 = (x^3 + 6x - 3)^2 = x^6 + 12x^4 - 6x^3 + 36x^2 - 36x + 9.$$

Also ist x Nullstelle von $X^6 - 6X^4 - 6X^3 + 12X^2 - 36X + 1$. Wegen $x > 1$ kann x nach Folgerung I.8.51 nicht rational sein.

Bemerkung I.8.53. Die (komplexen) Nullstellen von ganzzahligen normierten Polynomen nennt man *ganz-algebraisch*. Nach Folgerung I.8.51 ist jede rationale ganz-algebraische Zahl ganzzahlig. In der Algebra II zeigt man, dass die ganz-algebraischen Zahlen einen Teilring von $\mathbb{C}$ bilden (Satz II.11.7).

Lemma I.8.54 (Eisenstein-Kriterium[2])**.** *Sei $\alpha = X^n + a_{n-1}X^{n-1} + \ldots + a_0 \in \mathbb{Z}[X]$ mit $p \mid a_0, \ldots, p \mid a_{n-1}$ und $p^2 \nmid a_0$ für ein $p \in \mathbb{P}$. Dann ist α irreduzibel in $\mathbb{Q}[X]$.*

Beweis. Sei indirekt $\alpha = \beta\gamma$ mit $\beta, \gamma \in \mathbb{Q}[X] \setminus \mathbb{Q}$. Wir können annehmen, dass β und γ normiert sind. Nach Folgerung I.8.51 ist $\beta = \sum b_i X^i \in \mathbb{Z}[X]$ und $\gamma = \sum c_i X^i \in \mathbb{Z}[X]$. Wegen $p \mid a_0 = b_0 c_0$ und $p^2 \nmid a_0$ können wir o. B. d. A. $p \mid b_0$ und $p \nmid c_0$ annehmen. Sei $k < n$ minimal mit $p \nmid b_k$ (existiert, da β normiert). Dann ergibt sich der Widerspruch

$$0 \equiv a_k = \sum_{i=0}^{k} b_i c_{k-i} \equiv b_k c_0 \not\equiv 0 \pmod{p}.$$ □

Beispiel I.8.55. Sei $p \in \mathbb{P}$ und $\alpha = X^{p-1} + X^{p-2} + \ldots + X + 1 \in \mathbb{Q}[X]$. Offenbar ist α genau dann irreduzibel, wenn $\beta := \alpha(X + 1)$ irreduzibel ist (Definition I.8.9). Wegen $(X - 1)\alpha = X^p - 1$ (geometrische Reihe) ist

$$X\beta = (X + 1)^p - 1 = \sum_{k=1}^{p} \binom{p}{k} X^k$$

[2] zuerst von Schönemann entdeckt, siehe [D. A. Cox, *Why Eisenstein Proved the Eisenstein Criterion and Why Schönemann Discovered It First*, Amer. Math. Monthly 118 (2011), 3–21]

und

$$\beta = X^{p-1} + \sum_{k=1}^{p-1} \binom{p}{k} X^{k-1}.$$

Für $1 \leq k \leq p-1$ ist $\binom{p}{k} = \frac{p(p-1)\ldots(p-k+1)}{1\cdot 2\cdot\ldots\cdot k} \equiv 0 \pmod{p}$ und $\binom{p}{1} = p \not\equiv 0 \pmod{p^2}$. Nach Eisenstein ist β irreduzibel und somit auch α.

Lemma I.8.56 (Reduktion modulo p)**.** *Sei $\alpha = \sum a_n X^n \in \mathbb{Z}[X]$ normiert und reduzibel in $\mathbb{Q}[X]$. Dann ist $\overline{\alpha} := \sum (a_n + p\mathbb{Z}) X^n$ reduzibel in $\mathbb{F}_p[X]$ für alle $p \in \mathbb{P}$.*

Beweis. Nach Folgerung I.8.51 existieren normierte $\beta, \gamma \in \mathbb{Z}[X] \setminus \mathbb{Z}$ mit $\alpha = \beta\gamma$. Wie in Lemma I.8.44 lässt sich der kanonische Ringhomomorphismus $\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ zu $f\colon \mathbb{Z}[X] \to \mathbb{F}_p[X]$ fortsetzen. Dabei gilt $\overline{\alpha} = f(\alpha) = f(\beta)f(\gamma)$ mit $f(\beta), f(\gamma) \in \mathbb{F}_p[X] \setminus \mathbb{F}_p$. □

Beispiel I.8.57. Da $\alpha := X^3 + X + 1 \in \mathbb{F}_2[X]$ keine Nullstelle in $\mathbb{F}_2$ besitzt, ist α irreduzibel. Daher ist auch $\beta := X^3 + 2X^2 - 7X + 333 \in \mathbb{Q}[X]$ irreduzibel, denn $\overline{\beta} = \alpha$. Achtung: Die Umkehrung ist falsch. Zum Beispiel ist $X^2 + 1$ irreduzibel in $\mathbb{Q}[X]$, aber nicht in $\mathbb{F}_2[X]$.

9 Körpererweiterungen

Definition I.9.1.

(i) Ein *Teilkörper* eines Körpers L ist eine Teilmenge $K \subseteq L$, die mit den eingeschränkten Verknüpfungen $+$ und $\cdot$ selbst einen Körper bildet. Man nennt dann $K \subseteq L$ eine *Körpererweiterung*.

(ii) Für jede Körpererweiterung $K \subseteq L$ ist L ein K-Vektorraum, wobei die Skalarmultiplikation die Multiplikation in L ist. Man nennt $|L : K| := \dim_K L$ den *Grad* von L über K. Im Fall $|L : K| < \infty$ nennt man die Körpererweiterung *endlich* (trotzdem kann dann K unendlich sein).[1]

(iii) Ist $x \in L$ Nullstelle eines Polynoms $\mu \in K[X] \setminus K \subseteq L[X]$, so heißt x *algebraisch* (über K). Ist jedes $x \in L$ algebraisch über K, so nennt man die Körpererweiterung $K \subseteq L$ *algebraisch*. Ist $x \in L$ nicht algebraisch, so heißt x *transzendent* (über K).

(iv) Sind $K \subseteq L$ und $K \subseteq M$ Körpererweiterungen und $\sigma\colon L \to M$ ein Isomorphismus mit $\sigma_K = \mathrm{id}_K$ (Einschränkung), so nennt man σ einen *K-Isomorphismus*.

Beispiel I.9.2.

(i) $\mathbb{Q} \subseteq \mathbb{R}$ ist eine unendliche Körpererweiterung, denn $\mathbb{Q}$ ist abzählbar und $\mathbb{R}$ überabzählbar.

(ii) $\mathbb{R} \subseteq \mathbb{C}$ ist eine Körpererweiterung vom Grad 2 mit Basis $1, \mathrm{i}$.

(iii) Jeder Durchschnitt von Teilkörpern ist wieder ein Teilkörper (nachrechnen). Für eine Körpererweiterung $K \subseteq L$ und eine Teilmenge $S \subseteq L$ sei $K(S)$ der Durchschnitt aller Teilkörper von L, die K und S enthalten. Man sagt $K(S)$ entsteht durch *Adjunktion* von S zu K. Wir schreiben auch $K(x_1, \ldots, x_n) := K(\{x_1, \ldots, x_n\})$.

(iv) Jedes $x \in K$ ist algebraisch über K als Nullstelle von $X - x$.

(v) $\sqrt{2} \in \mathbb{R}$ ist algebraisch über $\mathbb{Q}$ als Nullstelle von $X^2 - 2$.

(vi) Sei $x := a + b\mathrm{i} \in \mathbb{C}$ mit $a, b \in \mathbb{R}$. Dann ist x als Nullstelle von $(X - a)^2 + b^2 \in \mathbb{R}[X]$ algebraisch über $\mathbb{R}$. Daher ist $\mathbb{R} \subseteq \mathbb{C}$ algebraisch.

(vii) Mit $\mathbb{Q}$ ist auch $\mathbb{Q}[X]$ abzählbar. Nach Satz I.8.29 hat jedes $\alpha \in \mathbb{Q}[X] \setminus \{0\}$ nur endlich viele Nullstellen. Also gibt es in $\mathbb{R}$ nur abzählbar viele algebraische Zahlen über $\mathbb{Q}$. „Fast alle“ reellen Zahlen sind daher transzendent, aber deren explizite Konstruktion ist schwierig (Satz I.13.12).

Bemerkung I.9.3.

(i) Sei $K \subseteq L$ eine Körpererweiterung und $x \in L$ algebraisch über K. Dann hat der Einsetzungshomomorphismus $F_x\colon K[X] \to L$, $\alpha \mapsto \alpha(x)$ (Satz I.8.10) einen nicht-trivialen Kern. Nach Lemma I.8.37 existiert genau ein normiertes Polynom $\mu_x \in K[X]$ mit $\mathrm{Ker}(F_x) = (\mu_x)$. Für jedes $\alpha \in K[X]$ mit Nullstelle x gilt dann $\mu_x \mid \alpha$. Insbesondere ist $\deg \mu_x$ minimal unter allen Polynomen $\alpha \neq 0$ mit Nullstelle x. Daher ist μ_x irreduzibel. Man nennt μ_x das *Minimalpolynom* von x (über K).

[1] Achtung: $|L : K|$ ist *nicht* der Index von $(K, +)$ in $(L, +)$!

(ii) Mit den Bezeichnungen aus (i) ist die Abbildung $t_x\colon L \to L$, $a \mapsto xa$ K-linear und μ_x ist das Minimalpolynom von t_x aus der linearen Algebra 2.

(iii) Für Teilmengen $S, T \subseteq L$ gilt offenbar $K(S \cup T) = K(S)(T) = K(T)(S)$. Für $\sigma \in \mathrm{Aut}(L)$ gilt außerdem $\sigma(K(S)) = \sigma(K)(\sigma(S))$.

(iv) Ist $x \in L$ transzendent, so ist der Einsetzungshomomorphismus $F_x\colon K[X] \to L$ injektiv. Wegen $\alpha(x) \in K(x)$ für alle $\alpha \in K[X]$ ist $F_x(K[X]) \subseteq K(x)$. Nach Aufgabe I.40 lässt sich F_x zu einem Körperhomomorphismus $\hat{F}_x\colon K(X) \to K(x)$ fortsetzen. Wegen $x = F_x(X) \in \hat{F}_x(K(X))$ ist $\hat{F}_x(K(X))$ ein Teilkörper von L, der x enthält. Daher ist $\hat{F}_x$ surjektiv und es folgt $K(X) \cong K(x)$. Insbesondere hängt der Isomorphietyp von $K(x)$ nicht von x ab (solange x transzendent ist).

Beispiel I.9.4. Wegen $\sqrt{2} \notin \mathbb{Q}$ ist $X^2 - 2$ das Minimalpolynom von $\sqrt{2}$ über $\mathbb{Q}$. Analog ist $X^2 + 1$ das Minimalpolynom von $\mathrm{i} \in \mathbb{C}$ über $\mathbb{Q}$ (oder über $\mathbb{R}$).

Satz I.9.5 (Gradsatz)**.** *Für Körpererweiterungen $K \subseteq L \subseteq M$ gilt*

$$\boxed{|M : K| = |M : L||L : K|.}$$

Beweis. Ist $|M : L|$ oder $|L : K|$ unendlich, so auch $|M : K|$. Sei also $|M : L||L : K| < \infty$. Sei $b_1, \ldots, b_n \in L$ eine K-Basis von L und $c_1, \ldots, c_m \in M$ eine L-Basis von M. Jedes $x \in M$ lässt sich in der Form $x = \sum_{i=1}^m x_i c_i$ mit $x_i \in L$ schreiben. Außerdem ist $x_i = \sum_{j=1}^n x_{ij} b_j$ mit $x_{ij} \in K$. Insgesamt ist $x = \sum_{i,j} x_{ij} b_j c_i$ und $\{b_i c_j : i = 1, \ldots, n,\ j = 1, \ldots, m\}$ ein Erzeugendensystem von M als K-Vektorraum. Sei nun $\sum_{i,j} x_{ij} b_i c_j = 0$ für gewisse $x_{ij} \in K$. Wegen

$$\sum_j \Big(\underbrace{\sum_i x_{ij} b_i}_{\in L} \Big) c_j = 0$$

folgt $\sum_i x_{ij} b_i = 0$ für alle j aus der linearen Unabhängigkeit von $c_1, \ldots, c_m$. Da $b_1, \ldots, b_n$ linear unabhängig über K sind, folgt $x_{ij} = 0$ für alle i, j. Daher ist $\{b_i c_j : i = 1, \ldots, n,\ j = 1, \ldots, m\}$ eine K-Basis von M. □

Satz I.9.6. *Jede endliche Körpererweiterung ist algebraisch.*

Beweis. Sei $K \subseteq L$ eine endliche Körpererweiterung und $x \in L$. Dann existiert ein $n \in \mathbb{N}$, sodass $1, x, \ldots, x^n$ linear abhängig über K sind. Also existieren $a_0, \ldots, a_n \in K$ (nicht alle 0) mit $a_0 + a_1 x + \ldots + a_n x^n = 0$. Als Nullstelle von $\sum a_i X^i \in K[X] \setminus \{0\}$ ist x algebraisch über K. □

Bemerkung I.9.7. Endliche Körpererweiterungen von $\mathbb{Q}$ in $\mathbb{C}$ nennt man (*algebraische*) *Zahlkörper*.

Satz I.9.8. *Sei $K \subseteq L$ eine Körpererweiterung und $x \in L$ algebraisch mit Minimalpolynom μ_x. Dann ist* $\boxed{K(x) \cong K[X]/(\mu_x)}$ *und* $\boxed{|K(x) : K| = \deg \mu_x.}$

Beweis. Sei $F_x\colon K[X] \to L$ der Einsetzungshomomorphismus. Der Homomorphiesatz für Ringe zeigt

$$K[X]/(\mu_x) \cong F_x(K[X]) \subseteq K(x).$$

Nach Satz I.8.38 ist $K[X]/(\mu_x)$ ein Körper und somit auch $F_x(K[X])$. Wegen $x = F_x(X) \in F_x(K[X])$ gilt $F_x(K[X]) = K(x)$.

Für die zweite Behauptung genügt es zu zeigen, dass $1+(\mu_x), X+(\mu_x), X^2+(\mu_x), \ldots, X^{d-1}+(\mu_x)$ mit $d := \deg \mu_x$ eine K-Basis von $K[X]/(\mu_x)$ ist. Division mit Rest zeigt, dass diese Elemente ein Erzeugendensystem von $K[X]/(\mu_x)$ bilden. Da μ_x kein Polynom vom Grad $e \in \{0, \ldots, d-1\}$ teilen kann, sind $1+(\mu_x), X+(\mu_x), \ldots, X^{d-1}+(\mu_x)$ auch linear unabhängig über K. □

Bemerkung I.9.9. Der Beweis zeigt $K(x) = \{\alpha(x) : \alpha \in K[X]\}$, falls x algebraisch über K ist (vgl. Bemerkung I.9.3(iv)). Außerdem ist $1, x, x^2, \ldots, x^{d-1}$ eine K-Basis von $K(x)$ mit $d := \deg \mu_x$.

Beispiel I.9.10. Es gilt $\mathbb{Q}(\sqrt{2}) \cong \mathbb{Q}[X]/(X^2-2)$.

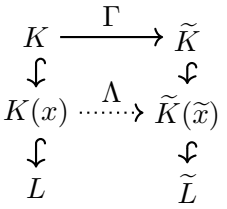
Lemma I.9.11. *Ist $K \subseteq L$ eine algebraische Körpererweiterung, so ist jeder K-Homomorphismus $L \to L$ ein Automorphismus.*

Beweis. Sei $\sigma\colon L \to L$ ein K-Homomorphismus. Nach Lemma I.8.41 ist σ injektiv. Sei $x \in L$ und $\mu \in K[X]$ das Minimalpolynom von x. Nach Lemma I.8.44 gilt

$$\mu(\sigma(x)) = \sigma(\mu)(\sigma(x)) = \sigma(\mu(x)) = \sigma(0) = 0,$$

d. h. $\sigma(x)$ ist eine Nullstelle von μ. Da σ injektiv ist, werden die Nullstellen von μ durch σ permutiert. Insbesondere existiert eine Nullstelle $y \in L$ von μ mit $\sigma(y) = x$. Also ist σ surjektiv. □

Satz I.9.12 (Fortsetzungssatz)**.** *Seien $K \subseteq L$ und $\widetilde{K} \subseteq \widetilde{L}$ Körpererweiterungen und $x \in L$ algebraisch mit Minimalpolynom $\mu \in K[X]$. Sei $\Gamma\colon K \to \widetilde{K}$ ein Körperisomorphismus und $\widetilde{x} \in \widetilde{L}$ eine Nullstelle von $\Gamma(\mu) \in \widetilde{K}[X]$ (Lemma I.8.44). Dann existiert ein Isomorphismus $\Lambda\colon K(x) \to \widetilde{K}(\widetilde{x})$ mit $\Lambda_K = \Gamma$ und $\Lambda(x) = \widetilde{x}$.*



Beweis. Nach Lemma I.8.44 kann man Γ zu einem Ringisomorphismus $K[X] \to \widetilde{K}[X]$ mit $X \mapsto X$ fortsetzen. Komposition mit dem kanonischen Epimorphismus $\widetilde{K}[X] \to \widetilde{K}[X]/(\Gamma(\mu))$ liefert einen Epimorphismus $K[X] \to \widetilde{K}[X]/(\Gamma(\mu))$ mit $X \mapsto X + (\Gamma(\mu))$. Mit dem Homomorphiesatz erhält einen Isomorphismus

$$\Delta\colon K[X]/(\mu) \to \widetilde{K}[X]/(\Gamma(\mu))$$

mit $X + (\mu) \mapsto X + (\Gamma(\mu))$. Nach Satz I.9.8 existiert ein Isomorphismus $f_x\colon K(x) \to K[X]/(\mu)$ mit $x \mapsto X + (\mu)$. Mit μ ist auch $\Gamma(\mu) \in \widetilde{K}[X]$ irreduzibel. Daher ist $\Gamma(\mu)$ das Minimalpolynom von $\widetilde{x}$ und man erhält einen Isomorphismus $f_{\widetilde{x}}\colon \widetilde{K}(\widetilde{x}) \to \widetilde{K}[X]/(\Gamma(\mu))$ mit $\widetilde{x} \mapsto X + (\Gamma(\mu))$. Der Isomorphismus $\Lambda := f_{\widetilde{x}}^{-1} \circ \Delta \circ f_x\colon K(x) \to \widetilde{K}(\widetilde{x})$ erfüllt dann $\Lambda_K = \Gamma$ und $\Lambda(x) = \widetilde{x}$. □

Beispiel I.9.13. Wähle $K = \widetilde{K} = \mathbb{Q}$, $L = \widetilde{L} = \mathbb{R}$, $x = \sqrt{2}$, $\Gamma = \mathrm{id}_{\mathbb{Q}}$ und $\widetilde{x} := -\sqrt{2}$. Dies liefert $\Lambda \in \mathrm{Aut}(\mathbb{Q}(\sqrt{2}))$ mit $\Lambda(\sqrt{2}) = -\sqrt{2}$.

Definition I.9.14. Sei $\alpha \in K[X] \setminus K$. Ein Körper $L \supseteq K$ heißt *Zerfällungskörper* von α, falls

$$\alpha = c \prod_{i=1}^{n} (X - x_i) \in L[X]$$

und $L = K(x_1, \ldots, x_n)$ mit $c \in K$.

Beispiel I.9.15. Wegen $X^2 - 2 = (X - \sqrt{2})(X + \sqrt{2}) \in \mathbb{Q}(\sqrt{2})[X]$ ist $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(\pm\sqrt{2})$ Zerfällungskörper von $X^2 - 2 \in \mathbb{Q}[X]$. Andererseits ist $\mathbb{R}$ *kein* Zerfällungskörper von $X^2 - 2$, denn $\mathbb{Q}(\sqrt{2}) \neq \mathbb{R}$ (abzählbar vs. überabzählbar). Es ist keineswegs klar, ob jedes Polynom einen Zerfällungskörper besitzt. So muss man beispielsweise das Symbol i als Nullstelle von $X^2 + 1 \in \mathbb{R}[X]$ einführen, sodass $\mathbb{C}$ Zerfällungskörper von $X^2 + 1$ wird. Bekanntlich gilt dann $\mathbb{C} \cong \mathbb{R}[X]/(X^2 + 1)$. Wir werden diesen Isomorphismus umkehren, um beliebige Zerfällungskörper zu konstruieren.

Satz I.9.16 (Kronecker)**.** *Jedes $\alpha \in K[X] \setminus K$ besitzt einen Zerfällungskörper L mit $|L : K| \leq \deg(\alpha)!$.*

Beweis. Induktion nach $d := \deg \alpha$. Im Fall $d = 1$ ist K ein Zerfällungskörper. Sei also $d > 1$. Sei $\beta \in K[X]$ ein irreduzibler Teiler von α und $M := K[X]/(\beta)$. Durch $a \mapsto a + (\beta)$ können wir K als Teilkörper von M auffassen. Wir betrachten nun den Polynomring $M[Y]$ über M in einer neuen Unbekannten Y. Dann hat $\alpha \in M[Y]$ die Nullstelle $y := X + (\beta)$ in M, denn

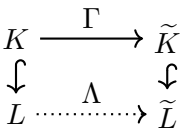
$$\alpha(X + (\beta)) = \alpha(X) + (\beta) = 0 \in M.$$

Schreibe $\alpha = (Y - y)\gamma$ mit $\gamma \in M[Y]$. Nach Induktion existiert ein Zerfällungskörper L von γ über M. Wegen $M = K(y)$ ist L auch ein Zerfällungskörper von α über K und

$$|L : K| \overset{I.9.5}{=} |L : M||M : K| \leq \deg(\gamma)! \deg \beta \leq (d-1)!d = d!. \qquad \square$$

Beispiel I.9.17. Nach Beispiel I.8.23 ist $\alpha = X^2 + X + 1 \in \mathbb{F}_2[X]$ irreduzibel. Der Zerfällungskörper L von α ist daher größer als $\mathbb{F}_2$. Wegen $|L : \mathbb{F}_2| \leq \deg(\alpha)! = 2$ folgt $|L| = 4$. Auf diese Weise konstruieren wir später alle endlichen Körper.

Satz I.9.18 (Steinitz)**.** *Sei $\Gamma\colon K \to \widetilde{K}$ ein Körperisomorphismus und $\alpha \in K[X] \setminus K$. Sei L ein Zerfällungskörper von α und sei $\widetilde{L}$ ein Zerfällungskörper von $\Gamma(\alpha) \in \widetilde{K}[X]$. Dann existiert ein Isomorphismus $\Lambda\colon L \to \widetilde{L}$ mit $\Lambda_K = \Gamma$. Insbesondere ist L eindeutig bis auf K-Isomorphie.*



Beweis. Induktion nach $d := \deg \alpha$. Im Fall $d = 1$ ist $\Lambda = \Gamma$. Sei $d > 1$ und $\beta \in K[X]$ ein irreduzibler Teiler von α mit Nullstelle $x \in L$. Wegen $\Gamma(\beta) \mid \Gamma(\alpha)$ besitzt $\widetilde{L}$ eine Nullstelle $\widetilde{x}$ von $\Gamma(\beta)$. Nach dem Fortsetzungssatz lässt sich Γ zu $\widehat{\Gamma}\colon K(x) \to \widetilde{K}(\widetilde{x})$ fortsetzen. Sei $\alpha = (X - x)\gamma$ mit $\gamma \in K(x)[X]$. Dann ist L Zerfällungskörper von γ und $\widetilde{L}$ ist Zerfällungskörper von $\widehat{\Gamma}(\gamma)$. Nach Induktion lässt sich $\widehat{\Gamma}$ zu $\Lambda\colon L \to \widetilde{L}$ fortsetzen. Die zweite Behauptung ergibt sich mit $K = \widetilde{K}$ und $\Gamma = \mathrm{id}_K$. $\square$

10 Galois-Theorie

Lemma I.10.1. *Sei $K \subseteq L$ eine endliche Körpererweiterung mit $L = \bigcup_{i=1}^{n} M_i$ für Zwischenkörper $K \subseteq M_i \subseteq L$. Dann ist $L = M_i$ für ein $i \in \{1, \dots, n\}$.*

Beweis. Wir können annehmen, dass n minimal ist und $n > 1$ gilt. Sei $x_i \in M_i \setminus \bigcup_{j \neq i} M_j$ für $i = 1, 2$. Ist K unendlich, so existieren $\lambda, \mu \in K$ mit $\lambda \neq \mu$ und $x_1 + \lambda x_2, x_1 + \mu x_2 \in M_i$ für ein $i \in \{1, \dots, n\}$ (Schubfachprinzip). Dann ist $x_2 = (\lambda - \mu)^{-1}((x_1 + \lambda x_2) - (x_1 + \mu x_2)) \in M_i$ und $i = 2$. Dies liefert den Widerspruch $x_1 = (x_1 + \lambda x_2) - \lambda x_2 \in M_2$.

Sei nun K endlich. Dann ist auch L endlich und nach Satz I.8.31 existiert ein $x \in L$ mit $L^\times = \langle x \rangle$. Sei $x \in M_i$ für ein $i \in \{1, \dots, n\}$. Dann ist $L = \{0\} \cup \langle x \rangle \subseteq M_i$ und die Behauptung folgt. □

Definition I.10.2. Für eine Körpererweiterung $K \subseteq L$ sei

$$\mathrm{Gal}(L|K) := \{\sigma \in \mathrm{Aut}(L) : \sigma_K = \mathrm{id}_K\} \leq \mathrm{Aut}(L)$$

die *Galoisgruppe* von L über K. Für $H \leq \mathrm{Gal}(L|K)$ sei

$$L^H := \{x \in L : \sigma(x) = x \ \forall \sigma \in H\}$$

der *Fixkörper* von H in L. Für $\sigma \in \mathrm{Gal}(L|K)$ sei $L^\sigma := L^{\langle \sigma \rangle}$.

Bemerkung I.10.3. Man zeigt leicht, dass $\mathrm{Gal}(L|K)$ eine Untergruppe von $\mathrm{Aut}(L)$ und L^H ein Teilkörper von L ist.

Beispiel I.10.4.

(i) Die komplexe Konjugation $\sigma \in \mathrm{Gal}(\mathbb{C}|\mathbb{R})$. Dabei gilt $\mathbb{C}^\sigma = \mathbb{R}$.

(ii) Für jeden Zahlkörper K gilt $\mathrm{Gal}(K|\mathbb{Q}) = \mathrm{Aut}(K)$, denn für $\sigma \in \mathrm{Aut}(K)$ ist $\sigma_{\mathbb{Q}} \in \mathrm{Aut}(\mathbb{Q}) = \{\mathrm{id}_{\mathbb{Q}}\}$ nach Aufgabe I.53.

Bemerkung I.10.5. Ist $x \in L$ algebraisch über K mit Minimalpolynom $\mu \in K[X]$ und $\sigma \in \mathrm{Gal}(L|K)$, so gilt $\sigma(\mu) = \mu$ und

$$\mu(\sigma(x)) = \sigma(\mu)(\sigma(x)) \overset{I.8.44}{=} \sigma(\mu(x)) = \sigma(0) = 0.$$

Fazit: $\mathrm{Gal}(L|K)$ operiert auf der Menge der Nullstellen von μ. Ist L Zerfällungskörper von μ, so ist diese Operation treu, denn L wird in diesem Fall von den Nullstellen erzeugt. Man erhält dann einen Monomorphismus $\mathrm{Gal}(L|K) \to S_{\deg \mu}$ (Satz I.8.29).

Satz I.10.6. *Für jede Körpererweiterung $K \subseteq L$ gilt $|\mathrm{Gal}(L|K)| \leq |L : K|$.*

Beweis. Wir können $|L:K| < \infty$ annehmen. Sei $L = K(x_1, \ldots, x_n)$ und $\sigma \in \mathrm{Gal}(L|K) =: G$. Dann ist $\sigma(x_i)$ eine Nullstelle des Minimalpolynoms von x_i. Insbesondere gibt es nur endlich viele Möglichkeiten für $\sigma(x_i)$. Wegen $L = K(x_1, \ldots, x_n)$ ist σ durch $\{\sigma(x_i) : i = 1, \ldots, n\}$ bereits eindeutig bestimmt. Dies zeigt $|G| < \infty$.

Für $\sigma \in G \setminus \{1\}$ gilt $L^\sigma \neq L$. Nach Lemma I.10.1 existiert ein $x \in L \setminus \bigcup_{1 \neq \sigma \in G} L^\sigma$. Das Minimalpolynom $\mu \in K[X]$ von x hat dann paarweise verschiedene Nullstellen $\sigma(x)$ für $\sigma \in G$. Dies zeigt

$$|G| \overset{I.8.29}{\leq} \deg \mu \overset{I.9.8}{=} |K(x):K| \leq |L:K|. \qquad \square$$

Definition I.10.7. Eine Körpererweiterung $K \subseteq L$ heißt *Galois-Erweiterung*, falls

$$|\mathrm{Gal}(L|K)| = |L:K| < \infty.$$

Beispiel I.10.8.

(i) Wegen $\mathrm{Gal}(\mathbb{C}|\mathbb{R}) = \{\mathrm{id}, \sigma\}$ mit der komplexen Konjugation σ ist $\mathbb{R} \subseteq \mathbb{C}$ eine Galois-Erweiterung. Nach Beispiel I.9.13 ist auch $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2})$ eine Galois-Erweiterung.

(ii) Offenbar ist $\mu := X^3 - 2$ das Minimalpolynom von $x := \sqrt[3]{2} \in \mathbb{R}$ über $\mathbb{Q}$. Jedes $\sigma \in \mathrm{Gal}(\mathbb{Q}(x)|\mathbb{Q})$ muss x auf eine Nullstelle von μ abbilden. Dabei gilt $\sigma(x) \in \mathbb{Q}(x) \subseteq \mathbb{R}$. Da x die einzige reelle Nullstelle von μ ist (die anderen sind $x\zeta$ und $x\bar{\zeta}$ mit $\zeta = e^{2\pi \mathrm{i}/3} = \frac{1}{2}(-1 + \sqrt{3}\mathrm{i})$), folgt $\sigma(x) = x$ und $\sigma = \mathrm{id}$. Daher ist $|\mathrm{Gal}(\mathbb{Q}(x)|\mathbb{Q})| = 1 < 3 = |\mathbb{Q}(x):\mathbb{Q}|$ und $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2})$ ist *keine* Galois-Erweiterung.

Satz I.10.9 (Artin)**.** *Für jede endliche Körpererweiterung $K \subseteq L$ mit $G := \mathrm{Gal}(L|K)$ sind äquivalent:*

(1) $K \subseteq L$ ist Galois-Erweiterung.

(2) $L^G = K$.

(3) L ist Zerfällungskörper eines Polynoms $\alpha \in K[X]$ mit paarweise verschiedenen Nullstellen.

(4) Es existiert ein $x \in L$ mit $L = K(x)$ und Minimalpolynom μ, sodass μ über L in paarweise verschiedene Linearfaktoren zerfällt.

Beweis.

(1) $\Rightarrow$ (2): Es gilt $K \subseteq L^G$ und $|L:K| \overset{(1)}{=} |G| \leq |\mathrm{Gal}(L|L^G)| \overset{I.10.6}{\leq} |L:L^G| \leq |L:K|$. Also ist $L^G = K$.

(2) $\Rightarrow$ (3): Sei $L = K(x_1, \ldots, x_n)$, $S := \{\sigma(x_i) : \sigma \in G,\ i = 1, \ldots, n\} \subseteq L$ und

$$\alpha := \prod_{s \in S} (X - s) \in L[X].$$

Dann ist

$$\sigma(\alpha) = \prod_{s \in S} (X - \sigma(s)) = \prod_{s \in S} (X - s) = \alpha$$

für alle $\sigma \in G$. Aus (2) folgt $\alpha \in L^G[X] = K[X]$. Nach Konstruktion ist L Zerfällungskörper von α und die Nullstellen $s \in S$ sind paarweise verschieden.

(3) $\Rightarrow$ (1): Sei α wie in (3) mit paarweise verschiedenen Nullstellen $x_1, \ldots, x_n \in L$. Wir argumentieren durch Induktion nach $|L : K|$ und können dabei $|L : K| > 1$ annehmen. Sei $\beta \in K[X]$ ein irreduzibler Teiler von α mit Nullstellen $x_1, \ldots, x_s$ (o. B. d. A.). Nach dem Fortsetzungssatz gibt es paarweise verschiedene K-Isomorphismen $\sigma_i \colon K(x_1) \to K(x_i)$ für $i = 1, \ldots, s$. Da L auch Zerfällungskörper von α über $K(x_1)$ ist, kann man jedes σ_i nach L fortsetzen (Steinitz). Jede dieser Fortsetzungen kann man mit $\gamma \in \mathrm{Gal}(L|K(x_1))$ verketten. Nach Induktion ist $|\mathrm{Gal}(L|K(x_1))| = |L : K(x_1)|$. Man erhält auf diese Weise also

$$|L : K(x_1)|s = |L : K(x_1)| \deg \beta = |L : K(x_1)||K(x_1) : K| = |L : K|$$

verschiedene Elemente von G. Nach Satz I.10.6 kann es auch nicht mehr geben.

(1) $\Rightarrow$ (4): Sei $x \in L \setminus \bigcup_{1 \neq \sigma \in G} L^\sigma$ (Lemma I.10.1) wie im Beweis von Satz I.10.6. Dann hat das Minimalpolynom $\mu \in K[X]$ von x paarweise verschiedene Nullstellen $\sigma(x)$ ($\sigma \in G$). Es folgt

$$|L : K| \overset{(1)}{=} |G| \leq \deg \mu = |K(x) : K| \leq |L : K|.$$

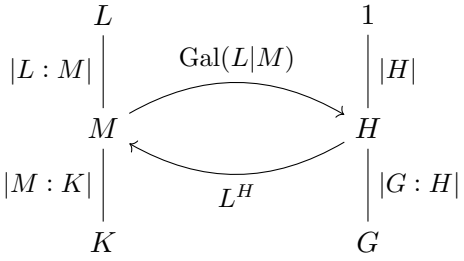
Also ist $L = K(x)$ und μ hat genau die Nullstellen $\sigma(x)$ ($\sigma \in G$).

(4) $\Rightarrow$ (3): Wähle $\alpha = \mu$. □

Beispiel I.10.10. Der Zerfällungskörper $\mathbb{Q}(\sqrt[3]{2}, e^{2\pi \mathrm{i}/3})$ von $X^3 - 2$ ist eine Galois-Erweiterung über $\mathbb{Q}$, denn die Nullstellen von $X^3 - 2$ sind paarweise verschieden.

Satz I.10.11 (Hauptsatz der Galois-Theorie[1])**.** *Sei $K \subseteq L$ eine Galois-Erweiterung, $G := \mathrm{Gal}(L|K)$, $\mathcal{M} := \{M \text{ Körper} : K \subseteq M \subseteq L\}$ und $\mathcal{H} := \{H : H \leq G\}$. Dann gilt:*

(i) Die Abbildungen $M \mapsto \mathrm{Gal}(L|M)$ und $H \mapsto L^H$ sind zueinander inverse, inklusionsumkehrende Bijektionen zwischen $\mathcal{M}$ und $\mathcal{H}$. Dabei gilt $\boxed{|L : L^H| = |H|}$ *und* $\boxed{|L^H : K| = |G : H|.}$



(ii) Für $M \in \mathcal{M}$ ist $M \subseteq L$ eine Galois-Erweiterung.

(iii) Genau dann ist $K \subseteq M \in \mathcal{M}$ eine Galois-Erweiterung, wenn $\mathrm{Gal}(L|M) \trianglelefteq G$. Gegebenenfalls ist

$$\boxed{\mathrm{Gal}(M|K) \cong \mathrm{Gal}(L|K)/\mathrm{Gal}(L|M).}$$

Beweis.

(ii) Nach Artin ist L Zerfällungskörper eines Polynoms $\alpha \in K[X]$ mit paarweise verschiedenen Nullstellen. Sicher ist dann auch L Zerfällungskörper von $\alpha \in M[X]$ und wieder nach Artin ist $M \subseteq L$ eine Galois-Erweiterung.

[1] Zu Galois' Leben siehe [T. Rothman, *Genius and biographers: the fictionalization of Évariste Galois*, Amer. Math. Monthly 89 (1982), 84–106]

(i) Für $M \in \mathcal{M}$ ist $M \subseteq L$ nach (ii) eine Galois-Erweiterung. Mit Artin folgt $L^{\mathrm{Gal}(L|M)} = M$. Sei umgekehrt $H \in \mathcal{H}$. Dann ist $H \leq \mathrm{Gal}(L|L^H)$. Nach Artin existiert ein $x \in L$ mit $L = K(x)$. Es gilt $\alpha := \prod_{\sigma \in H}(X - \sigma(x)) \in L^H[X]$. Für $\sigma \in \mathrm{Gal}(L|L^H)$ ist $\sigma(x)$ eine Nullstelle von $\sigma(\alpha) = \alpha$. Also existiert ein $\tau \in H$ mit $\sigma(x) = \tau(x)$. Wegen $K(x) = L$ folgt $\sigma = \tau \in H$. Insgesamt ist $H = \mathrm{Gal}(L|L^H)$. Daher sind die angegebenen Abbildungen zueinander inverse Bijektionen. Wegen

$$H_1 \subseteq H_2 \Longrightarrow L^{H_2} \subseteq L^{H_1}$$

sind die Abbildungen inklusionsumkehrend. Außerdem ist $|L : L^H| = |\mathrm{Gal}(L|L^H)| = |H|$ und $|L^H : K| = |L : K|/|L : L^H| = |G : H|$.

(iii) Nehmen wir zunächst an, dass $K \subseteq M$ eine Galois-Erweiterung ist. Nach Artin ist M Zerfällungskörper eines $\alpha \in K[X]$. Da jedes $\sigma \in G$ die Nullstellen von $\alpha = \sigma(\alpha)$ permutiert, folgt $\sigma(M) = M$. Mit $H := \mathrm{Gal}(L|M)$ gilt

$$\begin{aligned} L^H &\overset{\text{(i)}}{=} M = \sigma(M) = \sigma(L^H) = \big\{\sigma(x) \in \sigma(L) : \forall \gamma \in H : \gamma(x) = x\big\} \\ &= \big\{x \in L : \forall \gamma \in H : \gamma(\sigma^{-1}(x)) = \sigma^{-1}(x)\big\} \\ &= \big\{x \in L : \forall \gamma \in H : (\sigma\gamma\sigma^{-1})(x) = x\big\} = L^{\sigma H \sigma^{-1}} \end{aligned}$$

und $\sigma H \sigma^{-1} = H$ nach (i). Dies zeigt $H \trianglelefteq G$.

Sei nun umgekehrt $H := \mathrm{Gal}(L|M) \trianglelefteq G$. Für $\sigma \in G$ gilt dann $\sigma(M) = \sigma(L^H) = L^{\sigma H \sigma^{-1}} = L^H = M$. Daher ist die Einschränkung $\Gamma\colon G \to \mathrm{Gal}(M|K)$ wohldefiniert mit $\mathrm{Ker}(\Gamma) = H$. Es folgt

$$|M : K| \overset{\text{(i)}}{=} |G : H| = |G/\mathrm{Ker}(\Gamma)| \overset{I.3.29}{\leq} |\mathrm{Gal}(M|K)| \overset{I.10.6}{\leq} |M : K|.$$

Also ist $K \subseteq M$ eine Galois-Erweiterung und $\mathrm{Gal}(M|K) = \Gamma(G) \cong G/H$. □

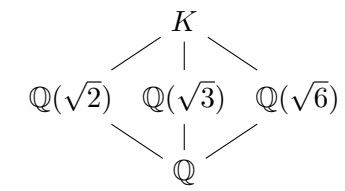
Beispiel I.10.12. Wir wissen bereits, dass $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2})$ eine Galois-Erweiterung vom Grad 2 ist. Annahme: $\sqrt{3} \in \mathbb{Q}(\sqrt{2})$. Dann existieren $a, b \in \mathbb{Q}$ mit $\sqrt{3} = a + \sqrt{2}b$. Es folgt $3 = a^2 + 2b^2 + 2\sqrt{2}ab$. Da $1, \sqrt{2}$ linear unabhängig über $\mathbb{Q}$ sind, gilt $ab = 0$. Wegen $\sqrt{3} \notin \mathbb{Q}$ ist $a = 0$ und $3 = 2b^2$. Durch Multiplizieren mit dem Nenner von b erhält man $3c^2 = 2d^2$ mit $c, d \in \mathbb{N}$. Dies widerspricht der eindeutigen Primfaktorzerlegung. Also ist $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$ und $X^2 - 3$ ist das Minimalpolynom von $\sqrt{3}$ über $\mathbb{Q}(\sqrt{2})$. Für $K := \mathbb{Q}(\sqrt{2}, \sqrt{3})$ gilt daher

$$|K : \mathbb{Q}| \overset{I.9.5}{=} |K : \mathbb{Q}(\sqrt{2})||\mathbb{Q}(\sqrt{2}) : \mathbb{Q}| = 4.$$

Der Fortsetzungssatz liefert $G := \mathrm{Gal}(K|\mathbb{Q}) = \{\mathrm{id}, \alpha, \beta, \gamma\}$ mit

$$\begin{aligned} &\alpha(\sqrt{2}) = \sqrt{2}, && \beta(\sqrt{2}) = -\sqrt{2}, && \gamma(\sqrt{2}) = -\sqrt{2}, \\ &\alpha(\sqrt{3}) = -\sqrt{3}, && \beta(\sqrt{3}) = \sqrt{3}, && \gamma(\sqrt{3}) = -\sqrt{3}. \end{aligned}$$

Insbesondere ist $\mathbb{Q} \subseteq K$ eine Galois-Erweiterung. Wegen $\alpha^2 = \beta^2 = \gamma^2 = \mathrm{id}_K$ ist $G \cong C_2 \times C_2$ nach dem Hauptsatz über endliche abelsche Gruppen. Die Untergruppen von G sind 1, $\langle\alpha\rangle$, $\langle\beta\rangle$, $\langle\gamma\rangle$ und G. Offenbar ist $\mathbb{Q}(\sqrt{2}) \subseteq K^\alpha$. Wegen $|K^\alpha : \mathbb{Q}| = |G : \langle\alpha\rangle| = 2$ gilt $K^\alpha = \mathbb{Q}(\sqrt{2})$. Analog erhält man die verbleibenden Zwischenkörper $K^\beta = \mathbb{Q}(\sqrt{3})$ und $K^\gamma = \mathbb{Q}(\sqrt{6})$. Da G abelsch ist, bilden all diese Zwischenkörper Galois-Erweiterungen über $\mathbb{Q}$.



Bemerkung I.10.13. Die Zwischenkörper einer beliebigen Galois-Erweiterung $K \subseteq L$ lassen sich im Allgemeinen durch ein lineares Gleichungssystem bestimmen. Für $H \leq \mathrm{Gal}(L|K)$ gilt $x \in L^H$ nämlich genau dann, wenn x im Kern der K-linearen Abbildungen $\sigma - \mathrm{id}_L$ für $\sigma \in H$ liegt. Oft ist es einfacher, wenn man ein „zufälliges“ Element $x \in L$ wählt und die *Spur* $\mathrm{tr}(x) := \sum_{\sigma \in H} \sigma(x)$ betrachtet. Für $\tau \in H$ gilt

$$\tau(\mathrm{tr}(x)) = \sum_{\sigma \in H} \tau(\sigma(x)) = \sum_{\gamma \in H} \gamma(x) = \mathrm{tr}(x) \in L^H.$$

Es kann natürlich passieren, dass $\mathrm{tr}(x)$ in K liegt, sodass man keine Information über L^H erhält. Mit $x := \sqrt{2} + \sqrt{3}$ und $H := \langle \beta \rangle$ in Beispiel I.10.12 bekommt man $\mathrm{tr}(x) = 2\sqrt{3}$.

Definition I.10.14. Für $i = 1, 2$ seien $K \subseteq M_i \subseteq L$ Körpererweiterungen. Man nennt

$$M_1 M_2 := M_1(M_2) = M_2(M_1)$$

das *Kompositum* von M_1 und M_2 (der „kleinste“ Teilkörper von L, der M_1 und M_2 enthält).

Satz I.10.15. *Für endliche Körpererweiterungen $K \subseteq M_i \subseteq L$ mit $i = 1, 2$ gilt:*

(i)
$$\mathrm{kgV}\big(|M_1 : K|, |M_2 : K|\big) \;\big|\; |M_1 M_2 : K| \leq |M_1 : K||M_2 : K|.$$

(ii) (*Verschiebungssatz*) *Ist $K \subseteq M_1$ eine Galois-Erweiterung, so auch $M_2 \subseteq M_1 M_2$ und es gilt*

$$\boxed{\mathrm{Gal}(M_1 M_2|M_2) \cong \mathrm{Gal}(M_1|M_1 \cap M_2).}$$

(iii) Sind $K \subseteq M_1$ und $K \subseteq M_2$ Galois-Erweiterungen, so auch $K \subseteq M_1 M_2$. Gegebenenfalls ist $\mathrm{Gal}(M_1 M_2|K)$ zu einer Untergruppe von $\mathrm{Gal}(M_1|K) \times \mathrm{Gal}(M_2|K)$ isomorph. Gleichheit gilt genau dann, wenn $M_1 \cap M_2 = K$.

(iv) Ist $K \subseteq L$ eine Galois-Erweiterung mit $G := \mathrm{Gal}(L|K)$ und $H_1, H_2 \leq G$, so gilt $\boxed{L^{H_1} L^{H_2} = L^{H_1 \cap H_2}}$ und $\boxed{L^{H_1} \cap L^{H_2} = L^{\langle H_1, H_2 \rangle}.}$

Beweis.

(i) Der Gradsatz impliziert $|M_i : K| \;\big|\; |M_1 M_2 : K|$ für $i = 1, 2$. Für die zweite Behauptung genügt es $|M_1 M_2 : M_2| \leq |M_1 : K|$ zu zeigen. Sei $b_1, \ldots, b_n$ eine K-Basis von M_1. Dann ist

$$M_1 \cup M_2 \subseteq S := M_2 b_1 + \ldots + M_2 b_n \subseteq M_1 M_2$$

und es genügt zu zeigen, dass S ein Körper ist. Sicher ist $(S, +)$ eine abelsche Gruppe. Für $i, j \in \{1, \ldots, n\}$ ist $b_i b_j \in M_1 \subseteq S$. Dies zeigt $xy \in S$ für $x, y \in S$. Für $x \neq 0$ ist die Abbildung $\sigma \colon S \to S$, $y \mapsto xy$ injektiv. Da S ein endlich-dimensionaler M_2-Vektorraum ist, ist σ sogar M_2-linear und damit bijektiv. Insbesondere existiert ein $y \in L$ mit $xy = 1$, d. h. $x^{-1} = y \in S$.

(ii) Nach Artin ist M_1 der Zerfällungskörper eines $\alpha \in K[X]$ mit paarweise verschiedenen Nullstellen $x_1, \ldots, x_d \in M_1$. Offenbar ist $M_1 M_2 = M_2(M_1) = M_2(x_1, \ldots, x_d)$ der Zerfällungskörper von $\alpha \in M_2[X]$. Nach Artin ist $M_2 \subseteq M_1 M_2$ eine Galois-Erweiterung. Für $\sigma \in G := \mathrm{Gal}(M_1 M_2|M_2)$ gilt $\sigma(M_1) = K(\sigma(x_1), \ldots, \sigma(x_d)) = M_1$ wegen $\sigma(\alpha) = \alpha$. Wie im Hauptsatz der Galois-Theorie ist die Einschränkung $\Gamma \colon G \to H := \mathrm{Gal}(M_1|M_1 \cap M_2)$ ein wohldefinierter Monomorphismus. Für $x \in M_1 \setminus M_2$ existiert ein $\sigma \in G$ mit $\sigma(x) \neq x$ wegen $(M_1 M_2)^G = M_2$. Dies zeigt $M_1^{\Gamma(G)} = M_1 \cap M_2$ und $\Gamma(G) = H$ nach dem Hauptsatz der Galois-Theorie.

(iii) Sei M_i Zerfällungskörper von $\alpha_i \in K[X]$ mit paarweise verschiedenen Nullstellen. Dann ist M_1M_2 Zerfällungskörper von $\frac{\alpha_1\alpha_2}{\mathrm{ggT}(\alpha_1,\alpha_2)} \in K[X]$ mit paarweise verschiedenen Nullstellen. Nach Artin ist $K \subseteq M_1M_2$ eine Galois-Erweiterung. Offenbar ist die Abbildung

$$\begin{aligned}\Gamma\colon \mathrm{Gal}(M_1M_2|K) &\to \mathrm{Gal}(M_1|K) \times \mathrm{Gal}(M_2|K),\\ \sigma &\mapsto (\sigma_{|M_1}, \sigma_{|M_2})\end{aligned}$$

ein wohldefinierter Monomorphismus. Aus (ii) folgt

$$|\mathrm{Gal}(M_1M_2|K)| = |M_1M_2 : K| = |M_1M_2 : M_2||M_2 : K| = |M_1 : M_1 \cap M_2||M_2 : K|.$$

Also ist Γ genau dann surjektiv, wenn $M_1 \cap M_2 = K$.

(iv) Da $\langle H_1, H_2\rangle$ aus Produkten von Elementen aus $H_1 \cup H_2$ besteht, gilt $L^{H_1} \cap L^{H_2} = L^{\langle H_1,H_2\rangle}$. Schließlich ist $L^{H_i} \subseteq L^{H_1}L^{H_2} \subseteq L^{H_1\cap H_2}$ und $H_1 \cap H_2 \subseteq \mathrm{Gal}(L|L^{H_1}L^{H_2}) \subseteq H_1 \cap H_2$. Dies zeigt $L^{H_1}L^{H_2} = L^{H_1\cap H_2}$. □

Beispiel I.10.16. Ersetzt man K durch $M_1 \cap M_2$ in Satz I.10.15(i),(ii), so erhält man $|M_1M_2 : M_2| \leq |M_1 : M_1 \cap M_2|$ und

$$\boxed{\mathrm{Gal}(M_1M_2|M_1 \cap M_2) \cong \mathrm{Gal}(M_1|M_1 \cap M_2) \times \mathrm{Gal}(M_2|M_1 \cap M_2).}$$

Ist weder M_1 noch M_2 eine Galois-Erweiterung über K, so kann die Ungleichung strikt sein wie im Fall $M_1 = \mathbb{Q}(\sqrt[3]{2})$ und $M_2 = \mathbb{Q}(\sqrt[3]{2}e^{2\pi\mathrm{i}/3})$.

11 Endliche Körper

Definition I.11.1.

(i) Offenbar existiert genau ein Ringhomomorphismus $\Phi\colon \mathbb{Z} \to K$ (denn $\Phi(1) = 1$, $\Phi(2) = \Phi(1+1) = 1+1$, usw.). Nach Beispiel I.7.9(vii) existiert genau ein $c \in \mathbb{N}_0$ mit $\operatorname{Ker}(\Phi) = c\mathbb{Z}$. Man nennt $\operatorname{char} K := c$ die *Charakteristik* von K. Im Folgenden werden wir $z \in \mathbb{Z}$ mit $\Phi(z) \in K$ identifizieren.

(ii) Der *Primkörper* $P(K)$ von K ist der Durchschnitt aller Teilkörper von K. Offenbar ist $P(K)$ dann der „kleinste" Teilkörper von K.

Beispiel I.11.2.

(i) Da die Einbettung $\Phi\colon \mathbb{Z} \to \mathbb{Q}$ injektiv ist, gilt $\operatorname{char} \mathbb{Q} = 0$. Dies gilt auch für jede Erweiterung von $\mathbb{Q}$.

(ii) Für $p \in \mathbb{P}$ gilt $\underbrace{1 + \ldots + 1}_{p\text{-mal}} = 0$ in $\mathbb{F}_p$. Dies zeigt $\operatorname{char} \mathbb{F}_p = p$.

Satz I.11.3. *Es gilt* $\operatorname{char} K \in \mathbb{P} \cup \{0\}$ *und*

$$P(K) \cong \begin{cases} \mathbb{Q} & \textit{falls } \operatorname{char} K = 0, \\ \mathbb{F}_p & \textit{falls } \operatorname{char} K = p > 0. \end{cases}$$

Beweis. Im Fall $\operatorname{char} K = 0$ lässt sich der Ringmonomorphismus $\Phi\colon \mathbb{Z} \to P(K)$ nach Aufgabe I.40 zu einem Körperhomomorphismus $\widehat{\Phi}\colon \mathbb{Q} \to P(K)$ fortsetzen. Also ist $\widehat{\Phi}(\mathbb{Q})$ ein Teilkörper von $P(K)$ und es folgt $P(K) = \widehat{\Phi}(\mathbb{Q}) \cong \mathbb{Q}$.

Sei nun $c := \operatorname{char} K > 0$. Der Homomorphiesatz liefert einen Isomorphismus $\widehat{\Phi}\colon \mathbb{Z}/c\mathbb{Z} \to \Phi(\mathbb{Z}) \subseteq P(K)$. Als Teilring von $P(K)$ ist $\Phi(\mathbb{Z}) \cong \mathbb{Z}/c\mathbb{Z}$ ein endlicher Integritätsbereich. Nach Aufgabe I.36 ist $\mathbb{Z}/c\mathbb{Z}$ ein Körper und es folgt $\widehat{\Phi}(\mathbb{Z}) = P(K)$. Nach Folgerung I.7.13 ist $c \in \mathbb{P}$ und die Behauptung folgt. □

Beispiel I.11.4. Ist K endlich, so gilt $P(K) \cong \mathbb{F}_p$ für ein $p \in \mathbb{P}$. Da K ein endlich-dimensionaler Vektorraum über $P(K)$ ist, gilt $|K| = p^n$ für ein $n \in \mathbb{N}$. Insbesondere gibt es keinen Körper mit sechs Elementen. Wir werden umgekehrt zeigen, dass es für jede Primzahlpotenz $p^n \neq 1$ im Wesentlichen genau einen Körper mit p^n Elementen gibt.

Definition I.11.5. Für $\alpha = \sum_{n=0}^{\infty} a_n X^n \in K[X]$ ist $\alpha' := \sum_{n=1}^{\infty} n a_n X^{n-1} \in K[X]$ die (formale) *Ableitung* von α.

Beispiel I.11.6. In $\mathbb{F}_2[X]$ gilt $(X^2)' = 2X = 0$.

Lemma I.11.7. *Für $a, b \in K$ und $\alpha, \beta \in K[X]$ gilt*

$$(a\alpha + b\beta)' = a\alpha' + b\beta' \qquad \text{(Summenregel)},$$
$$(\alpha\beta)' = \alpha'\beta + \alpha\beta' \qquad \text{(Produktregel)}.$$

Beweis. Für $\alpha = \sum a_n X^n$ und $\beta = \sum b_n X^n$ ist

$$\begin{aligned}(a\alpha + b\beta)' &= \Big(\sum (aa_n + bb_n)X^n\Big)' = \sum n(aa_n + bb_n)X^{n-1} \\ &= a\sum na_n X^{n-1} + b\sum nb_n X^{n-1} = a\alpha' + b\beta'\end{aligned}$$

und daher

$$\begin{aligned}(\alpha\beta)' &= \Big(\sum_{i,j} a_i b_j X^{i+j}\Big)' = \sum_{i,j} a_i b_j \big(X^{i+j}\big)' = \sum_{i,j} (i+j) a_i b_j X^{i+j-1} \\ &= \sum_{i,j} i a_i b_j X^{i-1+j} + \sum_{i,j} j a_i b_j X^{j-1+i} = \alpha'\beta + \alpha\beta'.\end{aligned}$$

□

Lemma I.11.8. *Eine Nullstelle $x \in K$ von $\alpha \in K[X]$ ist genau dann eine mehrfache Nullstelle, wenn $\alpha'(x) = 0$.*

Beweis. Sei $\beta \in K[X]$ mit $\alpha = (X - x)\beta$. Nach der Produktregel gilt

$$\alpha' = \beta + (X - x)\beta'.$$

Daher gilt $\beta(x) = 0$ genau dann, wenn $\alpha'(x) = 0$. □

Bemerkung I.11.9. In Lemma I.11.8 kann man annehmen, dass K ein Zerfällungskörper von α ist.

Lemma I.11.10. *Für $\operatorname{char} K = p > 0$ ist die Abbildung $F\colon K \to K$, $x \mapsto x^p$ ein Körperhomomorphismus, den man* Frobenius-Homomorphismus *nennt.*

Beweis. Sicher ist $F(1) = 1^p = 1$. Für $x, y \in K$ ist außerdem $F(xy) = (xy)^p = x^p y^p = F(x)F(y)$ und

$$F(x + y) = (x + y)^p = \sum_{k=0}^{p} \binom{p}{k} x^k y^{p-k} = x^p + y^p = F(x) + F(y),$$

denn $\binom{p}{k} = \frac{p(p-1)\ldots(p-k+1)}{1\cdot 2\cdot \ldots \cdot k} \equiv 0 \pmod p$ für $0 < k < p$. □

Beispiel I.11.11. In $\mathbb{F}_p$ gilt daher die „falsche“ binomische Formel $(a + b)^p = a^p + b^p$.[1] Für $a \in \mathbb{N}$ ist außerdem $a^p = (1 + \ldots + 1)^p \equiv 1^p + \ldots + 1^p \equiv a \pmod p$ (vgl. Euler-Fermat). Für $\alpha = \sum a_n X^n \in \mathbb{F}_p[X]$ gilt

$$\alpha(X^p) = \sum a_n X^{pn} = \sum a_n^p X^{pn} = \Big(\sum a_n X^n\Big)^p = \alpha^p.$$

Satz I.11.12. *Für jede Primzahlpotenz $q \neq 1$ existiert bis auf Isomorphie genau ein Körper $\mathbb{F}_q$ mit q Elementen. Umgekehrt ist jeder endliche Körper zu einem $\mathbb{F}_q$ isomorph.*

[1] auch *Freshman's Dream* genannt

Beweis. Sei $\mathbb{F}_q$ ein Zerfällungskörper von $X^q - X$ über $\mathbb{F}_p$, wobei $q = p^n$. Wegen $(X^q - X)' = qX^{q-1} - 1 = -1$ hat $X^q - X$ nach Lemma I.11.8 paarweise verschiedene Nullstellen $x_1, \ldots, x_q$ in $\mathbb{F}_q = \mathbb{F}_p(x_1, \ldots, x_q)$. Wir zeigen, dass diese Nullstellen selbst einen Körper bilden. Für $1 \leq i, j \leq q$ gilt $(x_i x_j)^q = x_i^q x_j^q = x_i x_j$ und

$$(x_i - x_j)^q = F^n(x_i - x_j) = F^n(x_i) - F^n(x_j) = x_i^q - x_j^q = x_i - x_j,$$

wobei F der Frobenius-Homomorphismus ist. Für $x_i \neq 0$ ist zusätzlich $(x_i^{-1})^q = (x_i^q)^{-1} = x_i^{-1}$. Also ist $\{x_1, \ldots, x_q\}$ ein Teilkörper von $\mathbb{F}_q$, der den Primkörper $\mathbb{F}_p$ enthalten muss. Dies zeigt $\mathbb{F}_q = \mathbb{F}_p(x_1, \ldots, x_q) = \{x_1, \ldots, x_q\}$ und $|\mathbb{F}_q| = q$.

Sei nun K ein weiterer Körper mit $|K| = q$. Dann ist $P(K) \cong \mathbb{F}_p$ und nach Bemerkung I.3.12(ii) gilt $x^{q-1} = 1$ für alle $x \in K^\times$. Somit ist K ebenfalls Zerfällungskörper von $X^q - X$ und $K \cong \mathbb{F}_q$ folgt mit Steinitz. Nach Beispiel I.11.4 ist also jeder endliche Körper zu einem $\mathbb{F}_q$ isomorph. □

Beispiel I.11.13. Nach Beispiel I.9.17 ist $\mathbb{F}_4 = \{0, 1, a, b\}$ (auch) der Zerfällungskörper von $X^2 + X + 1 \in \mathbb{F}_2[X]$. Es gilt daher $a^2 + a + 1 = 0 = b^2 + b + 1$ und man erhält:

$+$	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

$\cdot$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

Satz I.11.14. *Für jede Primzahlpotenz $q = p^n \neq 1$ ist $\mathbb{F}_p \subseteq \mathbb{F}_q$ eine Galois-Erweiterung und*

$$\boxed{\mathrm{Gal}(\mathbb{F}_q|\mathbb{F}_p) = \mathrm{Aut}(\mathbb{F}_q) = \langle F \rangle \cong C_n}$$

mit dem Frobenius-Homomorphismus F. Die Teilkörper von $\mathbb{F}_q$ sind

$$\{x \in \mathbb{F}_q : x^{p^d} = x\} \cong \mathbb{F}_{p^d}$$

mit $d \mid n$.

Beweis. Nach Konstruktion ist $\mathbb{F}_q$ Zerfällungskörper von $X^q - X \in \mathbb{F}_p[X]$ mit paarweise verschiedenen Nullstellen. Nach Artin ist $\mathbb{F}_p \subseteq \mathbb{F}_q$ eine Galois-Erweiterung. Nach Lemma I.9.11 ist $F \in \mathrm{Aut}(\mathbb{F}_q)$. Ein beliebiger Automorphismus $\sigma \in \mathrm{Aut}(\mathbb{F}_q)$ muss den Primkörper $\mathbb{F}_p$ elementweise festlassen (denn $\sigma(1) = 1$, $\sigma(1+1) = \sigma(1) + \sigma(1) = 1 + 1$, usw.) Also ist $\mathrm{Aut}(\mathbb{F}_q) = \mathrm{Gal}(\mathbb{F}_q|\mathbb{F}_p)$. Für $k \geq 1$ sind die Fixpunkte von F^k Nullstellen von $X^{p^k} - X$. Nach Satz I.8.29 gibt es höchstens p^k solche Fixpunkte. Insbesondere ist $F^k \neq \mathrm{id}$ für $k < n$. Dies zeigt

$$n \leq |\langle F \rangle| \leq |\mathrm{Gal}(\mathbb{F}_q|\mathbb{F}_p)| = |\mathbb{F}_q : \mathbb{F}_p| = n$$

und die zweite Behauptung folgt. Nach Satz I.3.34 haben die Untergruppen von $\langle F \rangle$ die Form $\langle F^d \rangle$ für $d \mid n$. Die letzte Aussage folgt daher aus dem Hauptsatz der Galois-Theorie. □

Beispiel I.11.15. Die Teilkörper von $\mathbb{F}_8$ sind $\mathbb{F}_2$ und $\mathbb{F}_8$ und nicht etwa $\mathbb{F}_4$.

Bemerkung I.11.16. Beachte: Für $n > 1$ ist $\mathbb{F}_{p^n} \ncong \mathbb{Z}/p^n\mathbb{Z}$. Nach Artin und Satz I.9.8 existiert ein irreduzibles Polynom $\alpha \in \mathbb{F}_p[X]$ vom Grad n mit $\mathbb{F}_{p^n} \cong \mathbb{F}_p[X]/(\alpha)$. Auf diese Weise kann man $\mathbb{F}_{p^n}$ explizit konstruieren. Das folgende Lemma zeigt, wie man geeignete α finden kann.

Lemma I.11.17. *Für jede Primzahlpotenz $q = p^n \neq 1$ ist*

$$X^q - X = \prod_{\substack{\varphi \in \mathbb{F}_p[X] \text{ irreduzibel} \\ \deg(\varphi) \mid n}} \varphi.$$

Beweis. Sei $\varphi \in \mathbb{F}_p[X]$ ein irreduzibler Teiler von $X^q - X$. Dann besitzt φ eine Nullstelle $x \in \mathbb{F}_q$, denn $\mathbb{F}_q$ ist Zerfällungskörper von $X^q - X$. Nach dem Gradsatz ist $\deg \varphi = |\mathbb{F}_p(x) : \mathbb{F}_p|$ ein Teiler von $|\mathbb{F}_q : \mathbb{F}_p| = n$.

Sei nun umgekehrt $\varphi \in \mathbb{F}_p[X]$ irreduzibel mit $d := \deg \varphi \mid n$. Dann ist $K := \mathbb{F}_p[X]/(\varphi)$ ein Körper mit p^d Elementen. Für $a := X + (\varphi) \in K$ gilt also $a^{p^d} = a$ und $a^{p^n} = a^{p^d \cdots p^d} = a$. Dies zeigt $X^q - X \equiv 0 \pmod{\varphi}$ und $\varphi \mid X^q - X$. Im Fall $\varphi^2 \mid X^q - X$ wäre $\varphi \mid (X^q - X)' = -1$ nach der Produktregel. Die Behauptung folgt nun aus der eindeutigen Primfaktorzerlegung in $\mathbb{F}_p[X]$ (Satz I.8.24). □

Beispiel I.11.18. In $\mathbb{F}_2[X]$ gilt

$$\frac{X^8 - X}{X(X+1)} = \frac{X^7 - 1}{X - 1} = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1 = (X^3 + X + 1)(X^3 + X^2 + 1).$$

Rechts stehen die irreduziblen Polynome vom Grad 3.

Definition I.11.19. Ein Körper K heißt *vollkommen*[2], falls $\operatorname{char} K = 0$ oder der Frobenius-Homomorphismus surjektiv ist (vgl. Aufgabe I.62).

Satz I.11.20. *Für jeden Körper K sind die folgenden Aussagen äquivalent:*

(1) K ist vollkommen.

(2) Für jedes irreduzible Polynom $\alpha \in K[X]$ ist $\operatorname{ggT}(\alpha, \alpha') = 1$.

(3) Für jedes irreduzible Polynom $\alpha \in K[X]$ ist $\alpha' \neq 0$.

(4) Jedes irreduzible Polynom in $K[X]$ hat nur einfache Nullstellen in seinem Zerfällungskörper.

Beweis. Wir zeigen zunächst die Äquivalenz von (2), (3) und (4). Für jedes irreduzible Polynom $\alpha \in K[X]$ gilt $\operatorname{ggT}(\alpha, \alpha') \in \{1, \alpha\}$. Wegen $\deg \alpha' < \deg \alpha$ ist (2) äquivalent zu (3). Für jede Nullstelle x von α in einem Zerfällungskörper ist α das Minimalpolynom von x. Daher gilt $\alpha'(x) = 0$ genau dann, wenn $\alpha' = 0$. Mit Lemma I.11.8 folgt (3)⇔(4).

Sei nun K vollkommen. Im Fall $\operatorname{char} K = 0$ ist sicher $\alpha' \neq 0$. Sei also $\operatorname{char} K = p > 0$ und der Frobenius-Homomorphismus F surjektiv. Im Fall $\alpha' = 0$ hat α die Form $\alpha = \sum_{i=0}^{n} a_i X^{ip}$ mit $a_0, \ldots, a_n \in K$. Da F surjektiv ist, existieren $b_0, \ldots, b_n \in K$ mit $b_i^p = F(b_i) = a_i$ für $i = 0, \ldots, n$. Es folgt

$$\alpha = \sum b_i^p X^{ip} = \sum (b_i X^i)^p \overset{I.11.11}{=} \left(\sum b_i X^i \right)^p$$

im Widerspruch zur Irreduzibilität von α. Dies zeigt (1)⇒(3).

Nehmen wir schließlich (4) an. Um (1) zu zeigen, können wir $\operatorname{char} K = p > 0$ annehmen. Sei $a \in K$ und x eine Nullstelle von $X^p - a$ in einem Zerfällungskörper. Dann gilt $(X - x)^p = X^p - x^p = X^p - a$. Also hat jeder irreduzible Teiler $\alpha \in K[X]$ von $X^p - a$ die Form $\alpha = (X - x)^n$. Nach (4) gilt dabei $n = 1$, d. h. $x \in K$. Dies zeigt $a = x^p = F(x)$ und F ist surjektiv. □

[2] oder *perfekt*

Bemerkung I.11.21.

(i) Nach Satz I.8.31 ist $\mathbb{F}_{p^n}^\times$ zyklisch. Wir untersuchen die Struktur der abelschen Gruppe $(\mathbb{F}_{p^n}, +)$. Wegen $\operatorname{char} \mathbb{F}_{p^n} = p$ gilt $\underbrace{a + \ldots + a}_{p\text{-mal}} = 0$ für alle $a \in \mathbb{F}_{p^n}$. Aus dem Hauptsatz über endliche abelsche Gruppen folgt

$$(\mathbb{F}_{p^n}, +) \cong C_p \times \ldots \times C_p = C_p^n.$$

Gruppen von dieser Bauart nennt man im Allgemeinen *elementarabelsche* p-Gruppen. Prominentes Beispiel ist V_4.

(ii) Bekanntlich rechnen Computer mit Bits, also Elementen von $\mathbb{F}_2$. Ein Byte besteht aus acht Bits und kann daher als Element von $\mathbb{F}_{2^8}$ aufgefasst werden. Dies ist für CD-Player und QR-Codes von praktischer Relevanz (siehe Kapitel III.10).

12 Kreisteilungskörper

Bemerkung I.12.1. Offenbar ist $\mathbb{F}_q$ Zerfällungskörper von $X^{q-1}-1$ über $\mathbb{F}_p$. Wir untersuchen in diesem Abschnitt die entsprechenden Körper in Charakteristik 0.

Satz I.12.2. *Sei* $\operatorname{char} K = 0$.

(i) Für jeden Zerfällungskörper L von $\alpha \in K[X] \setminus K$ ist $K \subseteq L$ eine Galois-Erweiterung.

(ii) Jede endliche Körpererweiterung $K \subseteq L$ liegt in einer Galois-Erweiterung $K \subseteq M$, d. h. $L \subseteq M$.

Beweis.

(i) Sei $\alpha = \alpha_1^{n_1} \dots \alpha_k^{n_k}$ die Zerlegung in paarweise verschiedene irreduzible Polynome $\alpha_1, \dots, \alpha_k \in K[X]$. Nach Satz I.11.20 hat jedes α_i nur einfache Nullstellen. Wegen $\operatorname{ggT}(\alpha_i, \alpha_j) = 1$ für $i \neq j$ hat $\beta := \alpha_1 \dots \alpha_k$ paarweise verschiedenen Nullstellen in L. Offenbar ist L auch Zerfällungskörper von β und die Behauptung folgt mit Artin.

(ii) Sei $x_1, \dots, x_n$ eine K-Basis von L. Seien $\mu_1, \dots, \mu_n \in K[X]$ die Minimalpolynome von $x_1, \dots, x_n$ und sei M ein Zerfällungskörper von $\mu_1 \dots \mu_n$. Nach (i) ist $K \subseteq M$ eine Galois-Erweiterung und $L = K(x_1, \dots, x_n) \subseteq M$. □

Satz I.12.3 (Satz vom primitiven Element)**.** *Für jede endliche Körpererweiterung $K \subseteq L$ mit* $\operatorname{char} K = 0$ *existiert ein $x \in L$ mit $L = K(x)$. Man nennt x* primitives Element.

Beweis. Nach Satz I.12.2 existiert eine Galois-Erweiterung $K \subseteq M$ mit $L \subseteq M$. Nach dem Hauptsatz der Galois-Theorie gibt es nur endlich viele Körper zwischen K und M. Daher gibt es auch nur endlich viele Körper $M_1, \dots, M_n$ mit $K \subseteq M_i \subsetneq L$. Nach Lemma I.10.1 existiert ein $x \in L \setminus \bigcup M_i$. Dann ist $K(x) \neq M_i$ für $i = 1, \dots, n$ und es folgt $K(x) = L$. □

Bemerkung I.12.4. Nach Satz I.8.31 gilt der Satz vom primitiven Element auch für endliche Körper, aber nicht für beliebige Körper positiver Charakteristik.

Beispiel I.12.5. Sei $K := \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Nach Beispiel I.10.12 wird $\sqrt{2}+\sqrt{3}$ von allen nicht-trivialen Galois-Automorphismen in $\operatorname{Gal}(K|\mathbb{Q})$ verändert. Dies zeigt $\mathbb{Q}(\sqrt{2}+\sqrt{3}) = K$ und $\sqrt{2}+\sqrt{3}$ ist ein primitives Element.

Definition I.12.6. Sei $n \in \mathbb{N}$. Man nennt $\zeta \in K$ *n-te Einheitswurzel*, falls $\zeta^n = 1$. Im Fall $|\langle\zeta\rangle| = n$ heißt ζ *primitiv*. Der Zerfällungskörper $\mathbb{Q}_n$ von $X^n - 1$ über $\mathbb{Q}$ heißt *n-ter Kreisteilungskörper*.

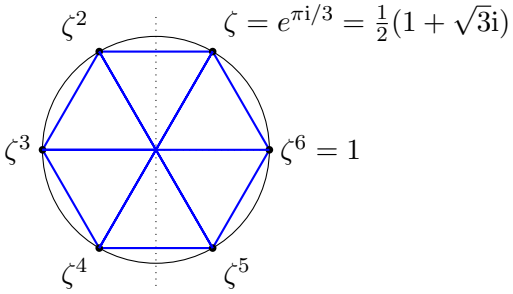
Bemerkung I.12.7.

(i) Wegen $(X^n-1)' = nX^{n-1} \neq 0$ hat X^n-1 nur einfache Nullstellen in $\mathbb{Q}_n$ (Lemma I.11.8), d. h. es gibt genau n n-te Einheitswurzeln. Diese bilden offenbar eine Gruppe $G \leq \mathbb{Q}_n^\times$, die nach Satz I.8.31 zyklisch ist, sagen wir $G = \langle\zeta\rangle$. Die primitiven n-ten Einheitswurzeln haben die Form ζ^k mit $\mathrm{ggT}(n,k) = 1$ nach Lemma I.3.7. Das Polynom

$$\Phi_n := \prod_{\substack{1\leq k\leq n,\\ \mathrm{ggT}(n,k)=1}} (X-\zeta^k) \in \mathbb{Q}_n[X]$$

heißt *n-tes Kreisteilungspolynom*. Es gilt $\deg \Phi_n = \varphi(n)$ mit der eulerschen φ-Funktion.

(ii) Bekanntlich ist $e^{2\pi\mathrm{i}/n} \in \mathbb{C}$ eine primitive n-te Einheitswurzel. Man kann also $\mathbb{Q}_n$ mit $\mathbb{Q}(e^{2\pi\mathrm{i}/n}) \subseteq \mathbb{C}$ identifizieren (Steinitz). Die Zahlen $e^{2\pi\mathrm{i}k/n}$ mit $k = 1,\ldots,n$ teilen den Einheitskreis in der komplexen Ebene in n gleich große Teile, d. h. sie bilden ein regelmäßiges n-Eck. Beispiel $n = 6$:



(iii) In Charakteristik $p > 0$ ist 1 die einzige p-te Einheitswurzel, denn $X^p - 1 = (X-1)^p$.

Beispiel I.12.8. Es gilt $\mathbb{Q}_1 = \mathbb{Q}_2 = \mathbb{Q}$ und $\Phi_1 = X-1$, $\Phi_2 = X+1$ sowie

$$\Phi_3 = (X - e^{2\pi\mathrm{i}/3})(X - e^{-2\pi\mathrm{i}/3}) = X^2 + X + 1.$$

Für $n \mid m$ gilt allgemeiner $\mathbb{Q}_n \subseteq \mathbb{Q}_m$, denn jede n-te Einheitswurzel ist auch eine m-te Einheitswurzel.

Lemma I.12.9. *Für $n \in \mathbb{N}$ ist $X^n - 1 = \prod_{d\mid n} \Phi_d$. Insbesondere gilt $\Phi_n \in \mathbb{Z}[X]$.*

Beweis. Sei $\zeta \in \mathbb{Q}_n$ eine primitive n-te Einheitswurzel. Für $d \mid n$ ist dann ζ^d eine primitive n/d-te Einheitswurzel (Lemma I.3.7). Dies zeigt

$$X^n - 1 = \prod_{i=1}^{n}(X-\zeta^i) = \prod_{d\mid n} \prod_{\substack{1\leq k\leq n/d\\ \mathrm{ggT}(k,n/d)=1}} (X-\zeta^{dk}) = \prod_{d\mid n} \Phi_{n/d} = \prod_{d\mid n} \Phi_d.$$

Für die zweite Behauptung argumentieren wir durch Induktion nach n. Für $n = 1$ ist $\Phi_1 = X-1 \in \mathbb{Z}[X]$. Sei nun $n > 1$ und die Behauptung für $d < n$ bewiesen. Dann ist

$$\alpha := \prod_{\substack{d\mid n\\ d\neq n}} \Phi_d \in \mathbb{Z}[X]$$

normiert. Da die Polynomdivision $\Phi_n = (X^n-1)/\alpha$ in $\mathbb{Q}_n[X]$ aufgeht, geht sie auch in $\mathbb{Q}[X]$ auf (der eindeutig bestimmte Rest bei der Division hängt nicht vom Körper ab), d. h. $\Phi_n \in \mathbb{Q}[X]$. Da α und Φ_n normiert sind, folgt $\Phi_n \in \mathbb{Z}[X]$ aus Folgerung I.8.51. □

Beispiel I.12.10. Mit Lemma I.12.9 lassen sich Kreisteilungspolynome rekursiv berechnen. Für $p \in \mathbb{P}$ und $n \in \mathbb{N}$ gilt

$$\Phi_{p^n} = \frac{X^{p^n}-1}{\prod_{0\le d<n}\Phi_{p^d}} = \frac{X^{p^n}-1}{X^{p^{n-1}}-1} = X^{p^{n-1}(p-1)} + X^{p^{n-1}(p-2)} + \ldots + X^{p^{n-1}} + 1.$$

Im Fall $n = 1$ ist $\Phi_p = X^{p-1} + X^{p-2} + \ldots + X + 1$ irreduzibel nach Beispiel I.8.55. Wir zeigen, dass dies auch im Allgemeinen stimmt.

Satz I.12.11 (Gauss)**.** *Kreisteilungspolynome sind irreduzibel in* $\mathbb{Q}[X]$.

Beweis. Sei $\Phi_n = \alpha\beta$ mit $\alpha, \beta \in \mathbb{Q}[X]$ und α irreduzibel. Da Φ_n und α normiert sind, ist auch β normiert. Aus Lemma I.12.9 und Folgerung I.8.51 folgt $\alpha, \beta \in \mathbb{Z}[X]$. Wir müssen $\alpha = \Phi_n$ zeigen. Sei $\zeta \in \mathbb{Q}_n$ eine Nullstelle von α. Dann ist ζ auch eine Nullstelle von Φ_n und damit eine primitive n-te Einheitswurzel. Da jede Nullstelle von Φ_n die Form ζ^k mit $\mathrm{ggT}(n,k) = 1$ hat, genügt es $\alpha(\zeta^k) = 0$ zu zeigen. Durch Induktion nach der Anzahl der Primteiler von k dürfen wir annehmen, dass $k = p$ selbst eine Primzahl ist (die n nicht teilt).

Nehmen wir $\alpha(\zeta^p) \neq 0$ an. Dann ist $\beta(\zeta^p) = 0$ und $\beta(X^p) \in \mathbb{Z}[X]$ hat die Nullstelle ζ. Da α das Minimalpolynom von ζ über $\mathbb{Q}$ ist, folgt $\alpha \mid \beta(X^p)$ in $\mathbb{Q}[X]$. Sei also $\beta(X^p) = \alpha\gamma$ mit $\gamma \in \mathbb{Q}[X]$. Da α normiert ist, gilt sogar $\gamma \in \mathbb{Z}[X]$ nach Folgerung I.8.51. Für die Reduktion modulo p (Lemma I.8.56) gilt

$$\overline{\alpha}\cdot\overline{\gamma} = \overline{\alpha\gamma} = \overline{\beta(X^p)} \overset{I.11.11}{=} \overline{\beta}^p.$$

Für einen irreduziblen Teiler $\overline{\delta}$ von $\overline{\alpha}$ gilt dann $\overline{\delta} \mid \overline{\beta}$ (Satz I.8.24) und

$$\overline{\delta}^2 \mid \overline{\alpha\beta} = \overline{\Phi_n} \mid X^n - \overline{1}.$$

Mit der Produktregel folgt $\overline{\delta} \mid (X^n - \overline{1})' = \overline{n}X^{n-1} \neq 0$ wegen $p \nmid n$. Also ist $\overline{\delta} = X$ und man erhält den Widerspruch $\overline{\delta} \nmid X^n - \overline{1}$. □

Satz I.12.12. *Für* $n \in \mathbb{N}$ *ist* $\mathbb{Q} \subseteq \mathbb{Q}_n$ *eine Galois-Erweiterung mit* $\mathrm{Gal}(\mathbb{Q}_n|\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$. *Für jeden Teilkörper* $L \subseteq \mathbb{Q}_n$ *ist* $\mathbb{Q} \subseteq L$ *eine Galois-Erweiterung mit abelscher Galoisgruppe.*

Beweis. Nach Satz I.12.2 ist $\mathbb{Q} \subseteq \mathbb{Q}_n$ eine Galois-Erweiterung. Sei $\zeta \in \mathbb{Q}_n$ eine primitive n-te Einheitswurzel und $\sigma \in G := \mathrm{Gal}(\mathbb{Q}_n|\mathbb{Q})$. Dann ist $\sigma(\zeta)$ ebenfalls Nullstelle von $X^n - 1$, d. h. $\sigma(\zeta) \in \langle\zeta\rangle$. Wegen $\mathbb{Q}_n = \mathbb{Q}(\zeta)$ ist σ durch $\sigma(\zeta)$ eindeutig bestimmt. Durch Einschränken erhält man einen Monomorphismus

$$\Gamma\colon G \to \mathrm{Aut}(\langle\zeta\rangle) \overset{I.7.27}{\cong} (\mathbb{Z}/n\mathbb{Z})^\times.$$

Nach Gauß ist Φ_n das Minimalpolynom von ζ über $\mathbb{Q}$. Dies zeigt

$$|G| = |\mathbb{Q}_n : \mathbb{Q}| = \deg\Phi_n = \varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|.$$

Also ist Γ ein Isomorphismus.

Sei nun $L \subseteq \mathbb{Q}_n$ ein Teilkörper. Sicher ist dann $\mathbb{Q} = P(\mathbb{Q}_n) \subseteq L$. Nach dem ersten Teil des Beweises ist G abelsch. Insbesondere ist jede Untergruppe von G normal. Die zweite Behauptung folgt daher aus dem Hauptsatz der Galois-Theorie. □

Beispiel I.12.13. Mit den Sätzen I.7.24 und I.8.34 lässt sich die Struktur von $G = \mathrm{Gal}(\mathbb{Q}_n|\mathbb{Q})$ bestimmen. Damit erhält man die Untergruppen von G und die Teilkörper von $\mathbb{Q}_n$ (vgl. Beispiel I.5.14). Zum Beispiel ist

$$\mathrm{Gal}(\mathbb{Q}_{12}|\mathbb{Q}) \cong (\mathbb{Z}/12\mathbb{Z})^\times \cong (\mathbb{Z}/4\mathbb{Z})^\times \times (\mathbb{Z}/3\mathbb{Z})^\times \cong C_2 \times C_2.$$

Die Untergruppen der Ordnung 2 von $(\mathbb{Z}/12\mathbb{Z})^\times$ sind $\langle -1 + 12\mathbb{Z}\rangle$, $\langle 5 + 12\mathbb{Z}\rangle$ und $\langle -5 + 12\mathbb{Z}\rangle$. Die entsprechenden Teilkörper von $\mathbb{Q}_{12}$ sind

$$\mathbb{Q}(\zeta + \bar{\zeta}) = \mathbb{Q}(\sqrt{3}), \qquad \mathbb{Q}(\zeta^3) = \mathbb{Q}_4 = \mathbb{Q}(\mathrm{i}), \qquad \mathbb{Q}(\zeta^2) = \mathbb{Q}_6 = \mathbb{Q}(\sqrt{3}\mathrm{i}) = \mathbb{Q}_3$$

(vgl. Bemerkung I.10.13).

Satz I.12.14. *Für $n, m \in \mathbb{N}$ ist $\mathbb{Q}_n \cap \mathbb{Q}_m = \mathbb{Q}_{\mathrm{ggT}(n,m)}$ und $\mathbb{Q}_n\mathbb{Q}_m = \mathbb{Q}_{\mathrm{kgV}(n,m)}$.*

Beweis. Wir betrachten $\mathbb{Q}_n$ und $\mathbb{Q}_m$ als Teilkörper von $\mathbb{Q}_k$ mit $k := \mathrm{kgV}(n, m)$. Auf diese Weise ist das Kompositum $\mathbb{Q}_n\mathbb{Q}_m \subseteq \mathbb{Q}_k$ wohldefiniert. Sei $G_1 := (\mathbb{Z}/k\mathbb{Z})^\times$ und $G_d := \{l + k\mathbb{Z} \in G_1 : l \equiv 1 \pmod d\} \leq G_1$ für $d \mid k$. Nach Satz I.12.12 ist dann $\mathbb{Q}_d = \mathbb{Q}_k^{G_d}$ für $d \mid k$. Offenbar ist $G_n \cap G_m = G_k = 1$ und

$$\mathbb{Q}_n\mathbb{Q}_m = \mathbb{Q}_k^{G_n}\mathbb{Q}_k^{G_m} \overset{I.10.15}{=} \mathbb{Q}_k^{G_n \cap G_m} = \mathbb{Q}_k$$

Mit $g := \mathrm{ggT}(n, m)$ ist $\langle G_n, G_m\rangle = G_nG_m \leq G_g$. Für $l + k\mathbb{Z} \in G_g$ existieren umgekehrt $a, b \in \mathbb{Z}$ mit $l + k\mathbb{Z} = 1 + an + bm + k\mathbb{Z} = (1 + an + k\mathbb{Z})(1 + bm + k\mathbb{Z}) \in G_nG_m$. Also ist

$$\mathbb{Q}_n \cap \mathbb{Q}_m = \mathbb{Q}_k^{G_n} \cap \mathbb{Q}_k^{G_m} \overset{I.10.15}{=} \mathbb{Q}_k^{G_nG_m} = \mathbb{Q}_k^{G_g} = \mathbb{Q}_g. \qquad \square$$

Lemma I.12.15. *Seien $n, a \in \mathbb{N}$ und p ein Primteiler von $\Phi_n(a)$. Dann ist $p \mid n$ oder $n \mid p - 1$.*

Beweis. Wegen $\Phi_n(a + p) \equiv \Phi_n(a) \pmod p$ dürfen wir $a > 1$ annehmen. Nach Lemma I.12.9 ist $p \mid \Phi_n(a) \mid (a^n - 1)$, also $a^n \equiv 1 \pmod p$. Die Ordnung k von $a + p\mathbb{Z} \in \mathbb{F}_p^\times$ teilt daher n (Lemma I.3.7). Im Fall $k = n$ folgt $n \mid p - 1$ aus Lagrange. Sei also $k < n$ und $b := a^k \equiv 1 \pmod p$. Wegen $a^k > 1$ gilt

$$\frac{n}{k} \equiv 1 + b + \ldots + b^{n/k-1} = \frac{b^{n/k} - 1}{b - 1} = \frac{a^n - 1}{a^k - 1} = \prod_{\substack{d \mid n \\ d \nmid k}} \Phi_d(a) \equiv 0 \pmod p.$$

Es folgt $p \mid \frac{n}{k} \mid n$. $\square$

Bemerkung I.12.16. Das folgende Resultat ist ein Spezialfall des DIRICHLETschen Primzahlsatzes: Für $\mathrm{ggT}(a, n) = 1$ liegen unendlich viele Primzahlen in $a + n\mathbb{Z}$ (in Aufgabe I.5 und im Anhang werden einige Spezialfälle besprochen; ein allgemeiner Beweis steht in meinem Zahlentheorie-Skript).[1]

Satz I.12.17. *Für $n \in \mathbb{N}$ gibt es unendlich viele Primzahlen $p \equiv 1 \pmod n$.*

Beweis. Seien $p_1, \ldots, p_s$ Primzahlen mit $p_i \equiv 1 \pmod n$ für $i = 1, \ldots, s$ (der Fall $s = 0$ ist zugelassen). Für $m := np_1 \ldots p_s$ existiert ein $k \in \mathbb{N}$ mit $\Phi_m(km) > 1$, denn Φ_m induziert als normiertes Polynom eine unbeschränkte Funktion $\mathbb{R} \to \mathbb{R}$. Sei p ein Primteiler von $\Phi_m(km)$. Wegen $p \mid ((km)^m - 1)$ ist $p \nmid m$ und Lemma I.12.15 zeigt $p \equiv 1 \pmod m$. Dann ist auch $p \equiv 1 \pmod n$. Wegen $p \nmid m$ haben wir eine neue Primzahl der gewünschten Form gefunden. $\square$

[1] Die Primzahlen verteilen sich sogar gleichmäßig auf die primen Restklassen modulo n. Eine zufällig gewählte Primzahl endet daher mit gleicher Wahrscheinlichkeit auf eine der Ziffern 1, 3, 7 oder 9.

Bemerkung I.12.18. Das bislang ungelöste *inverse Galois-Problem* fragt, ob man jede endliche Gruppe als Galoisgruppe einer Galois-Erweiterung über $\mathbb{Q}$ realisieren kann. SCHAFAREWITSCH bewies dies für auflösbare Gruppen. Wir behandeln abelsche Gruppen und später symmetrische Gruppen (Satz II.11.47).

Satz I.12.19. *Für jede endliche abelsche Gruppe G existiert eine Galois-Erweiterung $\mathbb{Q} \subseteq K$ mit* $\mathrm{Gal}(K|\mathbb{Q}) \cong G$.

Beweis. Nach dem Hauptsatz über endliche abelsche Gruppen existieren $d_1, \ldots, d_n \in \mathbb{N}$ mit $G \cong C_{d_1} \times \ldots \times C_{d_n}$. Nach Satz I.12.17 existieren paarweise verschiedene $p_1, \ldots, p_n \in \mathbb{P}$ mit $p_i \equiv 1 \pmod{d_i}$ für $i = 1, \ldots, n$. Wegen $d_i \mid p_i - 1 = \varphi(p_i)$ besitzt $(\mathbb{Z}/p_i\mathbb{Z})^\times$ eine Faktorgruppe der Ordnung d_i (Satz I.3.34), d. h. es gibt einen Epimorphismus $f_i \colon (\mathbb{Z}/p_i\mathbb{Z})^\times \to C_{d_i}$. Dann ist auch

$$\begin{aligned}(\mathbb{Z}/p_1\mathbb{Z})^\times \times \ldots \times (\mathbb{Z}/p_n\mathbb{Z})^\times &\to C_{d_1} \times \ldots \times C_{d_n},\\ (x_1, \ldots, x_n) &\mapsto (f_1(x_1), \ldots, f_n(x_n))\end{aligned}$$

ein Epimorphismus. Mit Satz I.12.12 und Satz I.7.24 erhält man einen Epimorphismus

$$\Gamma \colon \mathrm{Gal}(\mathbb{Q}_{p_1 \ldots p_n}|\mathbb{Q}) \cong (\mathbb{Z}/p_1 \ldots p_n\mathbb{Z})^\times \cong (\mathbb{Z}/p_1\mathbb{Z})^\times \times \ldots \times (\mathbb{Z}/p_n\mathbb{Z})^\times \to C_{d_1} \times \ldots \times C_{d_n} \cong G.$$

Sei $N := \mathrm{Ker}(\Gamma)$ und $K := \mathbb{Q}^N_{p_1 \ldots p_n}$. Nach dem Hauptsatz der Galois-Theorie ist dann

$$\mathrm{Gal}(K|\mathbb{Q}) \cong \mathrm{Gal}(\mathbb{Q}_{p_1 \ldots p_n}|\mathbb{Q})/\mathrm{Gal}(\mathbb{Q}_{p_1 \ldots p_n}|K) \cong \mathrm{Gal}(\mathbb{Q}_{p_1 \ldots p_n}|\mathbb{Q})/N \cong \Gamma(\mathrm{Gal}(\mathbb{Q}_{p_1 \ldots p_n}|\mathbb{Q})) \cong G. \qquad \square$$

Beispiel I.12.20. Der Beweis liefert $\mathrm{Gal}(\mathbb{Q}(\zeta + \zeta^{-1})|\mathbb{Q}) \cong C_3$ mit $\zeta := e^{2\pi \mathrm{i}/7}$ (wähle $p_1 = 7$).

Satz I.12.21 (KRONECKER-WEBER)**.** *Sei $\mathbb{Q} \subseteq K$ eine Galois-Erweiterung mit abelscher Galoisgruppe. Dann ist $K \subseteq \mathbb{Q}_n$ für ein $n \geq 1$.*

Beweis. Zahlentheorie.[2] $\square$

Bemerkung I.12.22. Wir betrachten den kleinsten Spezialfall mit Hilfe einer *Gauß-Summe* (siehe Definition A.1.5).

Satz I.12.23. *Sei K ein quadratischer Zahlkörper, d. h. $|K : \mathbb{Q}| = 2$. Dann ist $K \subseteq \mathbb{Q}_n$ für ein $n \in \mathbb{N}$.*

Beweis. Sei $x \in K \setminus \mathbb{Q}$ mit Minimalpolynom $\mu \in \mathbb{Q}[X]$. Dann ist $K = \mathbb{Q}(x)$ und $\mu = X^2 + aX + b$ mit $a, b \in \mathbb{Q}$. Für $d := a^2/4 - b \in \mathbb{Q}$ gilt $x = -a/2 \pm \sqrt{d}$ nach der p-q-Formel. Dies zeigt

$$K = \mathbb{Q}\Big(x + \frac{a}{2}\Big) = \mathbb{Q}(\sqrt{d}).$$

Wegen $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(e\sqrt{d}) = \mathbb{Q}(\sqrt{e^2 d})$ für alle $e \in \mathbb{N}$ können wir $d \in \mathbb{Z}$ annehmen. Wir müssen $\sqrt{d} \in \mathbb{Q}_{n_d}$ für ein $n_d \in \mathbb{N}$ zeigen. Ist dies für $d > 0$ bereits gezeigt, so gilt

$$\mathbb{Q}(\sqrt{-d}) \subseteq \mathbb{Q}(\mathrm{i}, \sqrt{d}) \subseteq \mathbb{Q}_{4n_d}$$

wegen $\mathrm{i} \in \mathbb{Q}_4 \subseteq \mathbb{Q}_{4n_d}$. Wir können also $d > 0$ annehmen. Gilt die Behauptung für $e, f \in \mathbb{N}$, so auch für $d = ef$, denn $\mathbb{Q}(\sqrt{ef}) \subseteq \mathbb{Q}(\sqrt{e}, \sqrt{f}) \subseteq \mathbb{Q}_{n_e n_f}$. Wir können daher $p := d \in \mathbb{P}$ voraussetzen.

[2] Siehe zum Beispiel Abschnitt 17.5 in [A. Leutbecher, *Zahlentheorie*, Springer, Berlin, 1996]

Sei zuerst $p > 2$ und sei $\zeta \in \mathbb{Q}_p$ eine primitive p-te Einheitswurzel. Für $1 \leq k, l \leq q := \frac{p-1}{2}$ gilt

$$2k \equiv \pm 2l \pmod{p} \overset{I.2.26}{\iff} k \equiv \pm l \pmod{p} \iff k = l.$$

Mit Beispiel I.12.10 folgt

$$p = \Phi_p(1) = \prod_{k=1}^{p-1}(1-\zeta^k) = \prod_{k=1}^{q}(1-\zeta^{2k})(1-\zeta^{-2k}) = \prod_{k=1}^{q}(\zeta^k - \zeta^{-k})(\zeta^{-k} - \zeta^k) = (-1)^q \prod_{k=1}^{q}(\zeta^k - \zeta^k)^2.$$

Mit $\epsilon := (-1)^q$ ergibt sich

$$\sqrt{p} = \sqrt{\epsilon}\sqrt{\epsilon p} = \pm\sqrt{\epsilon}\prod_{k=1}^{q}(\zeta^k - \zeta^{-k}) \in \mathbb{Q}_{4p}.$$

Sei schließlich $p = 2$ und $\zeta \in \mathbb{Q}_8$ eine primitive 8-te Einheitswurzel. Dann ist $\zeta^2 = \pm\mathrm{i}$, $(\zeta + \zeta^{-1})^2 = \zeta^2 + \zeta^{-2} + 2 = 2$ und $\sqrt{2} = \pm(\zeta + \zeta^{-1}) \in \mathbb{Q}_8$. □

13 Algebraischer Abschluss

Bemerkung I.13.1. Durch Hinzunahme eines neutralen Elements wird die *Halbgruppe* $\mathbb{N}$ zum *Monoid* $\mathbb{N}_0$. Ergänzt man inverse Elemente, so gelangt man zur Gruppe $\mathbb{Z}$, die gleichzeitig ein Integritätsbereich ist. Bildung des Quotientenkörpers macht aus $\mathbb{Z}$ den Körper $\mathbb{Q}$. In der Analysis *vervollständigt* man $\mathbb{Q}$ bzgl. der euklidischen Metrik und erhält daraus $\mathbb{R}$. In diesem Abschnitt konstruieren wir (unter anderem) den *algebraischen Abschluss* $\mathbb{C}$ von $\mathbb{R}$. Dabei verliert man allerdings die *Anordnung* von $\mathbb{R}$. Unter Aufgabe der Kommutativität der Multiplikation kann man $\mathbb{C}$ zum *Quaternionenschiefkörper* $\mathbb{H}$ erweitern (Aufgabe I.50). Schließlich gelangt man von $\mathbb{H}$ zu den *Oktonionen* $\mathbb{O}$, für die die Multiplikation nicht mehr assoziativ ist.

Lemma I.13.2. *Sind $K \subseteq L \subseteq M$ algebraische Körpererweiterungen, so ist auch $K \subseteq M$ algebraisch.*

Beweis. Sei $x \in M$ beliebig. Da x algebraisch über L ist, existieren $y_0, \dots, y_n \in L$ (nicht alle 0) mit $\sum y_i x^i = 0$. Nach Voraussetzung sind $y_0, \dots, y_n$ algebraisch über K. Also gilt

$$|K(y_0, \dots, y_n) : K| = |K(y_0, \dots, y_n) : K(y_0, \dots, y_{n-1})| \dots |K(y_0) : K| < \infty.$$

Nun ist x algebraisch über $\widehat{K} := K(y_0, \dots, y_n)$ und es folgt

$$|K(x) : K| \leq |\widehat{K}(x) : K| = |\widehat{K}(x) : \widehat{K}||\widehat{K} : K| < \infty.$$

Also ist x algebraisch über K (Satz I.9.6). □

Bemerkung I.13.3. Die entsprechende Aussage von Lemma I.13.2 gilt nicht für Galois-Erweiterungen: Nach Aufgabe I.57 sind $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2})$ und $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt[4]{2})$ Galois-Erweiterungen, aber nicht $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[4]{2})$, denn $\mathbb{Q}(\sqrt[4]{2}) \subseteq \mathbb{R}$ (vgl. Beispiel I.10.8).

Satz I.13.4. *Sei $K \subseteq L$ eine Körpererweiterung. Dann bilden die algebraischen Elemente von L über K einen Körper M mit $K \subseteq M \subseteq L$.*

Beweis. Da die Inklusion $K \subseteq M \subseteq L$ trivial ist, bleibt nur zu zeigen, dass M ein Körper ist. Für $x, y \in M$ ist $x - y \in K(x, y)$ sowie $xy^{-1} \in K(x, y)$ falls $y \neq 0$. Wegen

$$|K(x, y) : K| = |K(x, y) : K(x)||K(x) : K| < \infty$$

ist daher auch $x - y, xy^{-1} \in M$ (Satz I.9.6). Dies zeigt die Behauptung. □

Definition I.13.5.

(i) Man nennt K *algebraisch abgeschlossen*, falls jedes $\alpha \in K[X] \setminus K$ eine Nullstelle in K hat. Nach Lemma I.8.27 zerfällt α dann sogar in Linearfaktoren, d. h. α hat genau $\deg \alpha$ Nullstellen in K mit Vielfachheiten.

(ii) Ein algebraisch abgeschlossener Körper $\overline{K} \supseteq K$ heißt *algebraischer Abschluss* von K, falls die Körpererweiterung $K \subseteq \overline{K}$ algebraisch ist.

Bemerkung I.13.6. Ist K endlich, so hat das Polynom $1 + \prod_{x \in K}(X - x) \in K[X]$ keine Nullstelle in K. Ein algebraisch abgeschlossener Körper muss also unendlich sein.

Satz I.13.7 (Fundamentalsatz der Algebra)**.** *Der Körper $\mathbb{C}$ ist algebraisch abgeschlossen.*

Beweis. Sei $\alpha \in \mathbb{C}[X] \setminus \mathbb{C}$ und $\beta := \alpha\overline{\alpha} \in \mathbb{R}[X]$, wobei $\overline{\alpha}$ das komplex konjugierte Polynom bezeichnet. Hat β eine Nullstelle $z \in \mathbb{C}$, so gilt $\alpha(z) = 0$ oder $\alpha(\overline{z}) = \overline{\alpha}(z) = 0$. Wir können also $\alpha \in \mathbb{R}[X]$ annehmen.

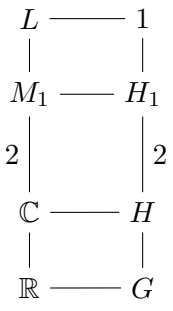
Sei L ein Zerfällungskörper von α über $\mathbb{C}$. Wir nehmen indirekt $L \neq \mathbb{C}$ an. Offenbar ist L auch Zerfällungskörper von $(X^2 + 1)\alpha$ über $\mathbb{R}$. Nach Satz I.12.2 ist $\mathbb{R} \subseteq L$ eine Galois-Erweiterung wegen $\operatorname{char} \mathbb{R} = 0$. Sei $G := \operatorname{Gal}(L|\mathbb{R})$, $S \in \operatorname{Syl}_2(G)$ und $M := L^S$. Nach dem Satz vom primitiven Element existiert ein $x \in M$ mit $M = \mathbb{R}(x)$. Für das Minimalpolynom μ von x über $\mathbb{R}$ gilt dann

$$\deg \mu = |M : \mathbb{R}| = |L^S : \mathbb{R}| = |G : S| \equiv 1 \pmod 2$$

nach dem Hauptsatz der Galois-Theorie. Die stetige Funktion $\mu\colon \mathbb{R} \to \mathbb{R}$ erfüllt daher $\lim_{r \to \pm\infty} \mu(r) = \pm\infty$. Nach dem Zwischenwertsatz der Analysis besitzt μ eine Nullstelle in $\mathbb{R}$, d. h. $\deg \mu = 1$ und $G = S$.

Sei $H := \operatorname{Gal}(L|\mathbb{C}) \leq G$. Wegen $L \neq \mathbb{C}$ ist $H \neq 1$. Als 2-Gruppe besitzt H eine Untergruppe H_1 vom Index 2 (Sylow). Für $M_1 := L^{H_1}$ ist dann $\mathbb{C} \subseteq M_1$ und

$$|M_1 : \mathbb{C}| = |H : H_1| = 2.$$



Für $z \in M_1 \setminus \mathbb{C}$ ist $M_1 = \mathbb{C}(z)$. Also hat das Minimalpolynom von z die Form $X^2 + aX + b \in \mathbb{C}[X]$ (vgl. Satz I.12.23). Wenn wir zeigen können, dass $w := a^2/4 - b \in \mathbb{C}$ eine Quadratwurzel $\sqrt{w} \in \mathbb{C}$ besitzt, so folgt der Widerspruch $z \in \mathbb{C}$ (p-q-Formel). Sei $w = x + y\mathrm{i}$ mit $x, y \in \mathbb{R}$ und o. B. d. A. $y \neq 0$. Dann ist

$$\sqrt{\frac{1}{2}\big(x + \sqrt{x^2 + y^2}\big)} + \frac{y}{|y|}\sqrt{\frac{1}{2}\big(-x + \sqrt{x^2 + y^2}\big)}\mathrm{i} \in \mathbb{C}$$

eine Wurzel von w (nachrechnen). □

Bemerkung I.13.8.

(i) Einen kürzeren Beweis mit etwas mehr Analysis findet man in Satz A.5.2.

(ii) (Partialbruchzerlegung) Nach Satz I.13.7 hat jedes irreduzible Polynom in $\mathbb{C}[X]$ Grad 1. Die Primfaktorzerlegung eines normierten Polynoms $\alpha \in \mathbb{C}[X]$ hat daher die Form $\alpha = (X - x_1)^{a_1} \dots (X - x_n)^{a_n}$ mit paarweise verschiedenen Nullstellen $x_1, \dots, x_n \in \mathbb{C}$. Da $\alpha/(X - x_i)^{a_1}, \dots, \alpha/(X - x_n)^{a_n}$ teilerfremd sind, existieren $\beta_1, \dots, \beta_n \in \mathbb{C}[X]$ mit $\beta_1\alpha/(X - x_i)^{a_1} + \dots + \beta_n\alpha/(X - x_n)^{a_n} = 1$. Division mit Rest liefert $\beta_i = \gamma_i(X - x_i)^{a_i} + \rho_i$ mit $\deg \rho_i < a_i$ für $i = 1, \dots, n$. Ein Gradvergleich von

$$(\gamma_1 + \dots + \gamma_n)\alpha + \rho_1\frac{\alpha}{(X - x_1)^{a_1}} + \dots + \rho_n\frac{\alpha}{(X - x_n)^{a_n}} = 1$$

zeigt $\gamma_1 + \dots + \gamma_n = 0$, d. h.

$$\frac{1}{\alpha} = \frac{\rho_1}{(X - x_1)^{a_1}} + \dots + \frac{\rho_n}{(X - x_n)^{a_n}} \in \mathbb{C}(X).$$

Da $1, (X-x_i), (X-x_i)^2, \ldots$ eine $\mathbb{C}$-Basis von $\mathbb{C}[X]$ ist, existieren $c_{i1}, \ldots, c_{ia_i} \in \mathbb{C}$ mit $\rho_i = c_{i1}(X-x_i)^{a_i-1} + \ldots + c_{ia_i}$. Insgesamt erhält man die *Partialbruchzerlegung*

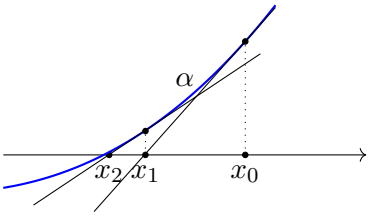
$$\frac{1}{\alpha} = \sum_{i=1}^{n} \sum_{j=1}^{a_i} \frac{c_{ij}}{(X-x_i)^j}.$$

Dies ist nützlich zur Integration rationaler Funktionen.

(iii) Wir zeigen später, dass sich die Nullstellen eines Polynoms im Allgemeinen nicht exakt berechnen lassen. In der Praxis gibt es Näherungsverfahren wie das von Newton:

Gegeben: $\alpha \in \mathbb{R}[X]$, $x_0 =$ Schätzung einer Nullstelle von α.
Iteriere:

$$x_{n+1} := x_n - \frac{\alpha(x_n)}{\alpha'(x_n)} \qquad (n \geq 0).$$



Beispiel I.13.9. Sei $\alpha := X^5 - 4X + 2$ und $x_0 := 0{,}5$. Mit $\alpha' = 5X^4 - 4$ erhält man $x_1 = 0{,}50847\ldots$ und $x_2 = 0{,}50849948\ldots$ (alle angegebenen Dezimalstellen sind korrekt).

Satz I.13.10. *Der Körper $\mathbb{Q}$ besitzt einen algebraischen Abschluss $\overline{\mathbb{Q}} \subseteq \mathbb{C}$.*

Beweis. Sei $\overline{\mathbb{Q}} \subseteq \mathbb{C}$ der Körper der algebraischen Elemente in $\mathbb{C}$ über $\mathbb{Q}$ (Satz I.13.4). Sicher ist dann $\mathbb{Q} \subseteq \overline{\mathbb{Q}}$ eine algebraische Körpererweiterung. Nach dem Fundamentalsatz der Algebra hat jedes Polynom $\alpha \in \overline{\mathbb{Q}}[X] \setminus \overline{\mathbb{Q}}$ eine Nullstelle $x \in \mathbb{C}$. Offenbar ist x algebraisch über $\overline{\mathbb{Q}}$ und nach Lemma I.13.2 ist x auch algebraisch über $\mathbb{Q}$. Dies zeigt $x \in \overline{\mathbb{Q}}$ und $\overline{\mathbb{Q}}$ ist algebraisch abgeschlossen. □

Bemerkung I.13.11. Wie bereits in Beispiel I.9.2 erwähnt ist $\overline{\mathbb{Q}}$ abzählbar und die Menge der transzendenten Zahlen $\mathbb{C} \setminus \overline{\mathbb{Q}}$ ist überabzählbar. Wir konstruieren nun eine transzendente Zahl.

Satz I.13.12 (Liouville)**.** *Die reelle Zahl $\xi := \sum_{k=1}^{\infty} 10^{-k!} = 0{,}1100010\ldots$ ist transzendent.*

Beweis. [1] Sicher ist ξ als Grenzwert einer Cauchyfolge reell. Sei indirekt $\xi \in \overline{\mathbb{Q}}$ mit Minimalpolynom $\mu \in \mathbb{Q}[X]$. Sei $a \in \mathbb{N}$ mit $\alpha := a\mu = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X]$. Wähle $m \in \mathbb{N}$ mit

$$\sum_{i=1}^{n} |a_i| \leq 10^{(m-n)m!}.$$

Sei $t := 10^{m!}$ und $s \in \mathbb{N}$ mit $s/t = \sum_{k=1}^{m} 10^{-k!}$. Dann ist

$$\xi - \frac{s}{t} = \sum_{k>m} 10^{-k!} \leq \frac{2}{10^{(m+1)!}} = \frac{2}{t^{m+1}} < \frac{1}{t^m}. \tag{I.13.1}$$

Da μ irreduzibel ist, gilt $\alpha(s/t) \neq 0$ und es folgt

$$|\alpha(s/t)| = \Big|\sum_{i=0}^{n} a_i (s/t)^i\Big| \geq \frac{1}{t^n}. \tag{I.13.2}$$

[1] Mit dem Mittelwertsatz der Analysis lassen sich die Rechnungen vereinfachen.

Für $i \geq 0$ ist $X^i - \xi^i = (X-\xi)\sum_{k=0}^{i-1} \xi^k X^{i-1-k}$. Wegen $s/t \leq \xi \leq 1/2$ ergibt sich damit der Widerspruch

$$|\alpha(s/t)| = |\alpha(s/t) - \alpha(\xi)| = \Big|\sum_{i=0}^{n} a_i((s/t)^i - \xi^i)\Big| = (s/t-\xi)\Big|\sum_{i=1}^{n} a_i \sum_{k=0}^{i-1} \xi^k (s/t)^{i-1-k}\Big|$$
$$\leq (s/t-\xi)\sum_{i=1}^{n} |a_i| i\xi^{i-1} \leq (s/t-\xi)\sum_{i=1}^{n} |a_i| < \frac{10^{(m-n)m!}}{t^m} = \frac{1}{t^n}. \qquad \square$$

Satz I.13.13 (Lindemann)**.** *Die Kreiszahl $\pi = 3{,}14\ldots$ ist transzendent.*

Beweis. Der Beweis basiert auf der eulerschen Formel $e^{\pi \mathrm{i}} + 1 = 0$. Siehe Beispiel A.9.6. $\square$

Satz I.13.14. *Jeder (abzählbare) Körper K besitzt genau einen algebraischen Abschluss bis auf K-Isomorphie.*

Beweis. Wir beschränken uns auf den Fall, in dem K abzählbar ist. Der allgemeine Fall benötigt Zorns Lemma (äquivalent zum Auswahlaxiom, siehe Satz II.2.9). Ist K abzählbar, so lassen sich auch alle Polynome abzählen, d. h. $K[X] = \{\alpha_1, \alpha_2, \ldots\}$. Sei $K_0 := K$ und induktiv K_n Zerfällungskörper von α_n über K_{n-1} für $n = 1, 2, \ldots$. Offenbar ist dann $\overline{K} := \bigcup K_n$ ein Körper und die Erweiterung $K \subseteq \overline{K}$ ist algebraisch nach Lemma I.13.2. Ist $\alpha \in \overline{K}[X] \setminus \overline{K}$, so ist jede Nullstelle x von α (in einem Zerfällungskörper) algebraisch über $\overline{K}$ und damit auch algebraisch über K. Insbesondere ist x Nullstelle eines Polynoms in $K[X]$. Dies zeigt $x \in \overline{K}$ und $\overline{K}$ ist in der Tat ein algebraischer Abschluss von K.

Ist $\widetilde{K}$ ein weiterer algebraischer Abschluss von K, so enthält $\widetilde{K}$ einen Zerfällungskörper $\widetilde{K}_n$ von $\alpha_1 \ldots \alpha_n$ für $n \geq 1$. Da die Erweiterung $K \subseteq \widetilde{K}$ algebraisch ist, gilt auch $\widetilde{K} = \bigcup \widetilde{K}_n$. Sei $\sigma_0 := \mathrm{id}_K$. Nach Steinitz existieren K-Isomorphismen $\sigma_n \colon K_n \to \widetilde{K}_n$ mit $(\sigma_n)_{K_{n-1}} = \sigma_{n-1}$ für $n \geq 1$. Wir betrachten die Abbildung $\sigma \colon \overline{K} \to \widetilde{K}$ mit $\sigma(x) := \sigma_n(x)$ für $x \in K_n$. Ist $x \in K_n \cup K_m$ mit $n \leq m$, so gilt $\sigma_n(x) = \sigma_m(x)$. Daher ist σ eine wohldefinierte Bijektion. Für $x, y \in \overline{K}$ existiert ein $n \in \mathbb{N}$ mit $x, y \in K_n$. Es gilt dann

$$\sigma(x \mathbin{\dot{+}} y) = \sigma_n(x \mathbin{\dot{+}} y) = \sigma_n(x) \mathbin{\dot{+}} \sigma_n(y) = \sigma(x) \mathbin{\dot{+}} \sigma(y).$$

Also ist σ ein K-Isomorphismus. $\square$

Beispiel I.13.15. Für $p \in \mathbb{P}$ gilt

$$\mathbb{F}_p \subseteq \mathbb{F}_{p^{2!}} \subseteq \mathbb{F}_{p^{3!}} \subseteq \ldots$$

nach Satz I.11.14. Offenbar ist $\overline{\mathbb{F}_p} := \bigcup_{n \geq 1} \mathbb{F}_{p^{n!}}$ eine algebraische Körpererweiterung über $\mathbb{F}_p$. Nach Konstruktion zerfallen die Polynome $X^{p^{n!}} - X \in \overline{\mathbb{F}_p}[X]$ für alle $n \in \mathbb{N}$ vollständig in Linearfaktoren. Nach Lemma I.11.17 zerfallen alle (irreduziblen) Polynome aus $\mathbb{F}_p[X]$ in Linearfaktoren über $\overline{\mathbb{F}_p}$. Ist nun $\alpha \in \overline{\mathbb{F}_p}[X] \setminus \overline{\mathbb{F}_p}$ mit Nullstelle x in einem Zerfällungskörper von α, so ist x algebraisch über $\overline{\mathbb{F}_p}$ und auch über $\mathbb{F}_p$. Dies zeigt $x \in \overline{\mathbb{F}_p}$ und $\overline{\mathbb{F}_p}$ ist ein algebraischer Abschluss von $\mathbb{F}_p$.

14 Auflösbarkeit von Gleichungen

Lemma I.14.1 (Dedekind)**.** *Für jede endliche Körpererweiterung $K \subseteq L$ ist* $\mathrm{Gal}(L|K)$ *eine linear unabhängige Teilmenge im L-Vektorraum aller Abbildungen $L \to L$.*

Beweis. Wir nehmen das Gegenteil an und wählen $\sigma_1, \ldots, \sigma_n \in \mathrm{Gal}(L|K)$ und $a_1, \ldots, a_n \in L^\times$ mit $\sum a_i\sigma_i = 0$. Sei n dabei so klein wie möglich. Sicher ist $n \geq 2$ und es existiert ein $y \in L$ mit $\sigma_1(y) \neq \sigma_n(y)$. Für alle $x \in L$ ist dann

$$\sum_{i=1}^{n-1} a_i\big(\sigma_i(y) - \sigma_n(y)\big)\sigma_i(x) = \sum_{i=1}^{n} a_i\sigma_i(yx) - \sigma_n(y)\sum_{i=1}^{n} a_i\sigma_i(x) = 0.$$

Dies zeigt $\sum_{i=1}^{n-1} a_i(\sigma_i(y) - \sigma_n(y))\sigma_i = 0$ im Widerspruch zur Wahl von n. □

Lemma I.14.2 (Kummer)**.** *Sei* $\mathrm{char}\, K = 0$ *und $n \in \mathbb{N}$, sodass K eine primitive n-te Einheitswurzel enthält. Sei $K \subseteq L$ eine Galois-Erweiterung. Genau dann ist* $\mathrm{Gal}(L|K)$ *zyklisch der Ordnung $d \mid n$, wenn L Zerfällungskörper von $X^n - x$ für ein $x \in K$ ist.*

Beweis. Sei $\zeta \in K$ eine primitive n-te Einheitswurzel. Sei zunächst $G := \mathrm{Gal}(L|K) = \langle\Gamma\rangle \cong C_d$ mit $d \mid n$. Dann ist $\gamma := \zeta^{n/d} \in K$ ist eine primitive d-te Einheitswurzel. Nach Dedekind existiert ein $b \in L$ mit

$$a := \gamma\Gamma(b) + \ldots + \gamma^d\Gamma^d(b) \neq 0.$$

Dann ist $\Gamma^i(a) = \gamma^{-i}a \in K(a)$ für $i = 1, \ldots, d$ und die Einschränkungen von $\Gamma, \ldots, \Gamma^d$ auf $K(a)$ sind paarweise verschieden. Mit Satz I.10.6 folgt $L = K(a)$. Außerdem ist

$$x := a^n = \gamma^{-n}a^n = \Gamma(a^n) \in L^\Gamma = K.$$

Die Nullstellen von $X^n - x$ sind gerade $a\zeta^i$ mit $i = 1, \ldots, n$. Also ist L Zerfällungskörper von $X^n - x$.

Sei nun umgekehrt L Zerfällungskörper von $X^n - x \in K[X]$. Sei $a \in L$ mit $a^n = x$. Die Nullstellen von $X^n - x$ sind dann $a\zeta^i$ mit $i = 1, \ldots, n$. Dies zeigt $L = K(a)$. Jedes $\Gamma \in \mathrm{Gal}(L|K) =: G$ ist durch $\Gamma(a) = a\zeta^i$ bereits eindeutig bestimmt. Daher ist die Abbildung

$$\begin{aligned} F\colon G &\to \mathbb{Z}/n\mathbb{Z}, \\ \Gamma &\mapsto i + n\mathbb{Z} \end{aligned}$$

injektiv. Für $\Lambda \in G$ mit $\Lambda(a) = a\zeta^j$ gilt

$$(\Gamma \circ \Lambda)(a) = \Gamma(a\zeta^j) = \Gamma(a)\zeta^j = a\zeta^{i+j}.$$

Also ist F ein Monomorphismus und G ist nach dem Homomorphiesatz zu einer Untergruppe von $\mathbb{Z}/n\mathbb{Z}$ isomorph. Die Behauptung folgt nun aus Satz I.3.34. □

Bemerkung I.14.3. In der *Artin-Schreier-Theorie* betrachtet man die analoge Situation für $\mathrm{char}\, K > 0$ (siehe Satz A.7.7).

Beispiel I.14.4. Der Zerfällungskörper von $X^4 - 2$ über $K := \mathbb{Q}_4 = \mathbb{Q}(\mathrm{i})$ ist $L := \mathbb{Q}(\mathrm{i}, \sqrt[4]{2})$. Wegen $\sqrt{2} \notin K$ ist $X^4 - 2$ irreduzibel über K. Daher ist $\mathrm{Gal}(L|K)$ zyklisch der Ordnung $|L : K| = 4$.

Definition I.14.5.

(i) Eine Körpererweiterung $K \subseteq L$ heißt *Radikalerweiterung*, falls Zwischenkörper $K = K_0 \subseteq \ldots \subseteq K_n = L$ und Elemente $a_i \in K_i$, $k_i \in \mathbb{N}$ mit $K_i = K_{i-1}(a_i)$ und $a_i^{k_i} \in K_{i-1}$ für $i = 1, \ldots, n$ existieren.

(ii) Ein Polynom $\alpha \in \mathbb{Q}[X] \setminus \mathbb{Q}$ heißt *auflösbar*, wenn es in einer Radikalerweiterung über $\mathbb{Q}$ in Linearfaktoren zerfällt. Dies bedeutet, dass man die Lösungen der Gleichung $\alpha(X) = 0$ durch rationale Zahlen, Grundrechenarten und Wurzelziehen ausdrücken kann (zum Beispiel p-q-Formel für $\deg \alpha = 2$).

(iii) Ist K ein Zerfällungskörper von $\alpha \in \mathbb{Q}[X] \setminus \mathbb{Q}$, so nennt man $\mathrm{Gal}(\alpha) := \mathrm{Gal}(K|\mathbb{Q})$ die *Galoisgruppe* von α. Da K bis auf $\mathbb{Q}$-Isomorphie eindeutig bestimmt ist (Steinitz), ist $\mathrm{Gal}(\alpha)$ bis auf Isomorphie eindeutig bestimmt. Mit dem Fundamentalsatz der Algebra kann man K auch eindeutig als Teilkörper von $\mathbb{C}$ wählen.

Beispiel I.14.6.

(i) Sei $n \in \mathbb{N}$ und $\alpha := X^n - 2 \in \mathbb{Q}[X]$. Der Zerfällungskörper von α ist offenbar $L = \mathbb{Q}_n(\sqrt[n]{2})$ (vgl. Aufgabe I.55). Wegen $\mathbb{Q}_n = \mathbb{Q}(e^{2\pi \mathrm{i}/n})$ ist $\mathbb{Q} \subseteq L$ eine Radikalerweiterung und α ist auflösbar. Sei $G := \mathrm{Gal}(\alpha) = \mathrm{Gal}(L|\mathbb{Q})$. Nach Kummer ist $N := \mathrm{Gal}(L|\mathbb{Q}_n)$ eine zyklische Untergruppe von G. Da auch $\mathbb{Q} \subseteq \mathbb{Q}_n$ eine Galois-Erweiterung ist (Satz I.12.12), gilt $N \trianglelefteq G$ nach dem Hauptsatz der Galois-Theorie. Außerdem ist $G/N \cong \mathrm{Gal}(\mathbb{Q}_n|\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$ abelsch. Daher ist G auflösbar nach Satz I.6.5.

(ii) Achtung: Ein Polynom α kann auflösbar sein, obwohl sein Zerfällungskörper *keine* Radikalerweiterung bildet. Ein konkretes Beispiel wird in Bemerkung I.14.24(ii) gegeben.

Bemerkung I.14.7. Man kann erahnen, dass der Hauptsatz der Galois-Theorie Radikalerweiterungen via Kummer in auflösbare Gruppen verwandelt. Dafür muss man sich aber zunächst eine Galois-Erweiterung verschaffen.

Lemma I.14.8. *Jede Radikalerweiterung $K \subseteq L$ mit* $\mathrm{char}\, K = 0$ *liegt in einer Radikalerweiterung, die auch Galois-Erweiterung ist.*

Beweis. Sei $K = K_0 \subseteq \ldots \subseteq K_n = L$ und $K_i = K_{i-1}(a_i)$ mit $a_i^{k_i} \in K_{i-1}$ für $i = 1, \ldots, n$. Nach Satz I.12.2 existiert eine Galois-Erweiterung $K \subseteq M$ mit $L \subseteq M$. Sei $\mathrm{Gal}(M|K) = \{\mathrm{id}_M = \sigma_1, \ldots, \sigma_k\}$ und

$$K_{ij} := K(\sigma_1(a_1), \ldots, \sigma_k(a_1), \ldots, \sigma_1(a_{i-1}), \ldots, \sigma_k(a_{i-1}), \sigma_1(a_i), \ldots, \sigma_j(a_i))$$

für $i = 1, \ldots, n$ und $j = 1, \ldots, k$. Wegen $\sigma_i(K_{nk}) = K_{nk}$ für $i = 1, \ldots, k$ ist $K_{nk}^{\mathrm{Gal}(K_{nk}|K)} \subseteq M^{\mathrm{Gal}(M|K)} = K$, d. h. $K \subseteq K_{nk}$ ist eine Galois-Erweiterung nach Artin. Außerdem gilt $L = K(a_1, \ldots, a_n) \subseteq K_{nk}$.

Sicher ist $K_{11} = K(a_1)$ mit $a_1^{k_1} \in K_0 = K$. Für $i = 1, \ldots, n$ und $j = 2, \ldots, k$ gilt $K_{ij} = K_{i,j-1}(\sigma_j(a_i))$ und

$$\sigma_j(a_i)^{k_i} = \sigma_j(a_i^{k_i}) \in \sigma_j(K_{i-1}) = \sigma_j(K(a_1, \ldots, a_{i-1})) \subseteq K_{i-1,j} \subseteq K_{i,j-1}.$$

Für $i = 2, \ldots, n$ ist schließlich auch $K_{i1} = K_{i-1,k}(a_i)$ mit $a_i^{k_i} \in K_{i-1} \subseteq K_{i-1,k}$. Also ist $K \subseteq K_{11} \subseteq K_{12} \subseteq \ldots \subseteq K_{nk}$ eine Radikalerweiterung. □

Satz I.14.9 (Galois). *Ein $\alpha \in \mathbb{Q}[X] \setminus \mathbb{Q}$ ist genau dann auflösbar, wenn* $\mathrm{Gal}(\alpha)$ *auflösbar ist.*

Beweis.
Schritt 1: $\Longrightarrow$
Nach Lemma I.14.8 existiert eine Radikal- und Galois-Erweiterung $\mathbb{Q} = K_0 \subseteq \ldots \subseteq K_n$, sodass ein Zerfällungskörper L von α in K_n liegt. Sei $a_i \in K_i$ und $k_i \in \mathbb{N}$ mit $K_i = K_{i-1}(a_i)$ und $a_i^{k_i} \in K_{i-1}$ für $i = 1, \ldots, n$. Sei $k := k_1 \ldots k_n$ und $\zeta \in \mathbb{Q}_k$ eine primitive k-te Einheitswurzel. Nach Artin ist K_n Zerfällungskörper eines $\gamma \in K_0[X]$. Daher ist $K_n(\zeta)$ Zerfällungskörper von $(X^k - 1)\gamma \in K_0[X]$. Insbesondere ist $K_0 \subseteq K_n(\zeta)$ eine Galois-Erweiterung (Satz I.12.2). Nach Satz I.12.12 ist $\mathbb{Q} = K_0 \subseteq K_0(\zeta) = \mathbb{Q}_k$ eine Galois-Erweiterung mit abelscher Galoisgruppe. Der Hauptsatz der Galois-Theorie zeigt

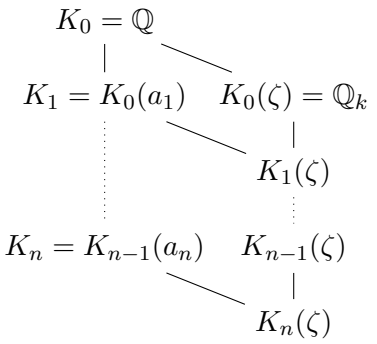
$$G_n := \mathrm{Gal}(K_n(\zeta)|K_0(\zeta)) \trianglelefteq \mathrm{Gal}(K_n(\zeta)|K_0) =: G$$

und $G/G_n \cong \mathrm{Gal}(K_0(\zeta)/K_0)$ ist abelsch.

Wir betrachten nun die Galois-Erweiterung $K_{i-1}(\zeta) \subseteq K_n(\zeta)$ für $i = 1, \ldots, n$ (Satz I.10.11). Offenbar ist $K_i(\zeta) = K_{i-1}(\zeta, a_i)$ Zerfällungskörper von $X^{k_i} - a_i^{k_i} \in K_{i-1}(\zeta)[X]$. Nach Satz I.12.2 und Kummer ist $K_{i-1}(\zeta) \subseteq K_i(\zeta)$ eine Galois-Erweiterung mit zyklischer Galoisgruppe. Also gilt $G_{n-i} := \mathrm{Gal}(K_n(\zeta)|K_i(\zeta)) \trianglelefteq G_{n-i+1}$ und $G_{n-i+1}/G_{n-i} \cong \mathrm{Gal}(K_i(\zeta)|K_{i-1}(\zeta))$ ist zyklisch. Insgesamt hat man eine Reihe

$$1 = G_0 \trianglelefteq \ldots \trianglelefteq G_n \trianglelefteq G$$

mit abelschen Faktoren, d. h. G ist auflösbar. Da $\mathbb{Q} \subseteq L$ eine Galois-Erweiterung ist, ist auch $\mathrm{Gal}(\alpha) \cong \mathrm{Gal}(L|\mathbb{Q}) \cong G/\mathrm{Gal}(K_n(\zeta)|L)$ auflösbar (Satz I.6.5).



Schritt 2: $\Longleftarrow$
Sei $\mathrm{Gal}(\alpha)$ auflösbar der Ordnung n. Sei K ein Zerfällungskörper von α und sei $\zeta \in \mathbb{Q}_n$ eine primitive n-te Einheitswurzel. Es genügt zu zeigen, dass $\mathbb{Q}_n \subseteq K(\zeta)$ eine Radikalerweiterung ist, denn dann ist auch $\mathbb{Q} \subseteq \mathbb{Q}(\zeta) = \mathbb{Q}_n \subseteq K(\zeta)$ eine Radikalerweiterung. Als Zerfällungskörper von α über $\mathbb{Q}_n$ ist $\mathbb{Q}_n \subseteq K(\zeta)$ eine Galois-Erweiterung (Satz I.12.2). Für $\Gamma \in G := \mathrm{Gal}(K(\zeta)|\mathbb{Q}_n)$ gilt $\Gamma(\alpha) = \alpha$ und $\Gamma(K) = K$. Die Einschränkungsabbildung

$$G \to \mathrm{Gal}(K|\mathbb{Q}) \cong \mathrm{Gal}(\alpha)$$

ist also ein wohldefinierter Homomorphismus mit Kern $\mathrm{Gal}(K(\zeta)|\mathbb{Q}_n(K)) = 1$. Nach dem Homomorphiesatz können wir G als Untergruppe von $\mathrm{Gal}(\alpha)$ auffassen. Insbesondere ist G auflösbar (Satz I.6.5). Sei $1 = G_0 \trianglelefteq \ldots \trianglelefteq G_m = G$ mit zyklischen Faktoren (Satz I.6.4). Für $K_i := K(\zeta)^{G_{m-i}}$ gilt dann $\mathbb{Q}_n = K_0 \subseteq \ldots \subseteq K_m = K(\zeta)$. Für $i = 1, \ldots, m$ ist $K_{i-1} \subseteq K_m$ eine Galois-Erweiterung und wegen

$$\mathrm{Gal}(K_m|K_i) = \mathrm{Gal}(K_m|K_m^{G_{m-i}}) = G_{m-i} \trianglelefteq G_{m-i+1} = \mathrm{Gal}(K_m|K_{i-1})$$

ist auch $K_{i-1} \subseteq K_i$ eine Galois-Erweiterung mit $\mathrm{Gal}(K_i|K_{i-1}) \cong G_{m-i+1}/G_{m-i}$ (Satz I.10.11). Nach Lagrange ist $|G_{m-i+1}/G_{m-i}|$ ein Teiler von $|G|$ und damit ein Teiler von $|\mathrm{Gal}(\alpha)| = n$ wegen $G \leq \mathrm{Gal}(\alpha)$. Nach Kummer existiert ein $a_i \in K_i$ mit $K_i = K_{i-1}(a_i)$ und $a_i^n \in K_{i-1}$. Also ist $\mathbb{Q}_n \subseteq K(\zeta)$ eine Radikalerweiterung und α ist auflösbar. □

Satz I.14.10 (Cardano, del Ferro, Tartaglia, Ferrari). *Polynome vom Grad ≤ 4 sind auflösbar.*

Beweis. Sei $\alpha \in \mathbb{Q}[X] \setminus \mathbb{Q}$ mit $d := \deg \alpha \leq 4$. Bemerkung I.10.5 liefert einen Monomorphismus $\mathrm{Gal}(\alpha) \to S_d \leq S_4$. Nach Beispiel I.6.6 ist S_4 auflösbar und daher auch $\mathrm{Gal}(\alpha)$. Die Behauptung folgt nun mit Galois. □

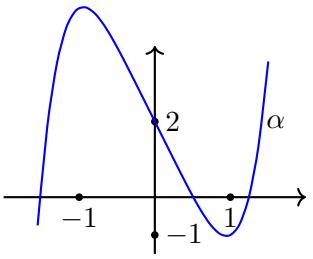
Lemma I.14.11. *Ist $\sigma \in S_5$ ein 5-Zyklus und $\tau \in S_5$ eine Transposition, so gilt $S_5 = \langle \sigma, \tau \rangle$.*

Beweis. Sei $\sigma = (a_1, \ldots, a_5)$, $\tau = (b_1, b_2)$ und $G := \langle \sigma, \tau \rangle$. Wegen $\sigma = (a_2, a_3, a_4, a_5, a_1) = \ldots$ können wir $a_1 = b_1$ annehmen. Wegen $\sigma^i = (a_1, a_{i+1}, \ldots)$ für $1 \leq i \leq 4$ können wir $a_2 = b_2$ annehmen, indem wir σ durch ein geeignetes σ^i ersetzen. Es gilt dann $\tau\sigma\tau^{-1} = (a_1, a_3, a_4, a_5, a_2) \notin \langle \sigma \rangle$. Also enthält G mindestens die beiden 5-Sylowgruppen $\langle \sigma \rangle$ und $\langle \tau\sigma\tau^{-1} \rangle$. Nach Sylow besitzt G mindestens sechs 5-Sylowgruppen. Diese liegen alle in $G \cap A_5 \trianglelefteq G$. Insbesondere ist $|G \cap A_5| \geq 6 \cdot 4 = 24$. Nach Satz I.6.13 ist A_5 einfach und kann nach Beispiel I.3.17(iii) keine Untergruppe vom Index 2 enthalten. Daher gilt $A_5 = G \cap A_5 \leq G$. Wegen $\tau \notin A_5$ folgt schließlich $G = S_5$. □

Satz I.14.12 (Abel, Ruffini[1])**.** *Es gibt nicht-auflösbare Polynome vom Grad 5.*

Beweis. Nach Eisenstein mit $p = 2$ ist $\alpha := X^5 - 4X + 2 \in \mathbb{Q}[X]$ irreduzibel. Nach Satz I.11.20 hat α paarweise verschiedene Nullstellen $x_1, \ldots, x_5$ in einem Zerfällungskörper $K \subseteq \mathbb{C}$. Also ist

$$5 = \deg \alpha = |\mathbb{Q}(x_1) : \mathbb{Q}| \;\Big|\; |K : \mathbb{Q}| = |\mathrm{Gal}(\alpha)|.$$



Nach Cauchy besitzt $\mathrm{Gal}(\alpha)$ ein Element der Ordnung 5. Bemerkung I.10.5 liefert einen Monomorphismus $\Gamma\colon \mathrm{Gal}(\alpha) \to \mathrm{Sym}(x_1, \ldots, x_5)$, dessen Bild einen 5-Zyklus σ enthält. Wegen $\alpha' = 5X^4 - 4$ hat der Graph von $\alpha\colon \mathbb{R} \to \mathbb{R}$ zwei Extremstellen, nämlich bei $\pm\sqrt[4]{4/5}$. Aus $\alpha(0) = 2$ und $\alpha(1) = -1$ folgt, dass α genau drei reelle Nullstellen hat (vgl. Beispiel I.13.9). Die komplexe Konjugation auf K liefert dann eine Transposition τ im Bild von Γ. Nach Lemma I.14.11 ist $\langle \sigma, \tau \rangle = \mathrm{Sym}(x_1, \ldots, x_5)$ und daher $\mathrm{Gal}(\alpha) \cong \Gamma(\mathrm{Gal}(\alpha)) \cong S_5$. Da S_5 nicht auflösbar ist (Satz I.6.13), folgt die Behauptung mit Galois. □

Bemerkung I.14.13.

(i) Der Beweis von Satz I.14.12 zeigt, dass die Abschätzung $|L : K| \leq \deg(\alpha)!$ im Satz von Kronecker nicht verbessert werden kann.

(ii) Man muss sich klar machen, dass $\sqrt[n]{z}$ für $z \in \mathbb{C}$ lediglich ein Symbol für eine nicht näher bestimmte Nullstelle von $X^n - z$ ist (in der Analysis könnte man konkret $\sqrt[n]{z} := \exp(\log(z)/n)$ mit dem Hauptwert des komplexen Logarithmus definieren). Völlig gleichberechtigt könnte man ein neues Symbol, sagen wir $q_n(z)$, für eine Nullstelle von $X^n + X - z$ definieren und fragen, welche Gleichungen sich nur mittels Grundrechenarten und q_n lösen lassen. Tatsächlich zeigten Bring und Jerrard, dass man jede Gleichung fünften Grades durch Grundrechenarten und Wurzelziehen in die reduzierte Form $X^5 + X - z = 0$ überführen kann.

(iii) Man kann Gleichungen fünften (und höheren) Grades durch modulare elliptische Funktionen oder hypergeometrische Reihen „lösen“.[2]

(iv) Im Folgenden bestimmen wir $\mathrm{Gal}(\alpha)$ als Permutationsgruppe auf den Nullstellen von $\alpha \in \mathbb{Q}[X]$.

[1] Zur Geschichte siehe [M. I. Rosen, *Nils Hendrik Abel and Equations of the Fifth Degree*, Amer. Math. Monthly 102 (1995), 495–505]

[2] siehe [King, *Beyond the quartic equation*, Birkhäuser, Boston, 1996]

Definition I.14.14.

(i) Der Polynomring mit mehreren Unbekannten $X_1, \ldots, X_n$ wird induktiv durch $K[X_1, \ldots, X_n] := K[X_1, \ldots, X_{n-1}][X_n]$ definiert. Jedes Element in $K[X_1, \ldots, X_n]$ hat dann die Form

$$\alpha = \sum_{i_1,\ldots,i_n \geq 0} a_{i_1,\ldots,i_n} X_1^{i_1} \ldots X_n^{i_n}$$

mit $a_{i_1,\ldots,i_n} \in K$. Man setzt $\deg \alpha := \sup\{i_1 + \ldots + i_n : a_{i_1,\ldots,i_n} \neq 0\}$. Es gilt (weiterhin) $\deg(\alpha\beta) = \deg \alpha + \deg \beta$ und $\deg(\alpha + \beta) \leq \max\{\deg \alpha, \deg \beta\}$ mit Gleichheit falls $\deg \alpha \neq \deg \beta$.

(ii) Ein Polynom $\alpha \in K[X_1, \ldots, X_n]$ heißt *symmetrisch*, falls $\alpha = \alpha(X_{\pi(1)}, \ldots, X_{\pi(n)})$ für jedes $\pi \in S_n$ gilt. Die *elementarsymmetrischen* Polynome der Ordnung n sind $\sigma_0 := 1$ und

$$\sigma_k := \sum_{1 \leq i_1 < \ldots < i_k \leq n} X_{i_1} \ldots X_{i_k} \in K[X_1, \ldots, X_n] \qquad (k = 1, \ldots, n).$$

Bemerkung I.14.15. Die symmetrischen Polynome bilden einen Teilring von $K[X_1, \ldots, X_n]$ (vgl. Bemerkung I.8.11).

Beispiel I.14.16.

(i) Offenbar ist $XY^3 + X^3Y - X - Y + 2 \in K[X, Y]$ symmetrisch vom Grad 4.

(ii) Für $n = 3$ ist

$$\sigma_0 = 1, \qquad \sigma_1 = X_1 + X_2 + X_3, \qquad \sigma_2 = X_1X_2 + X_1X_3 + X_2X_3, \qquad \sigma_3 = X_1X_2X_3.$$

(iii) Im Allgemeinen ist $\deg \sigma_k = k$ für $k = 0, \ldots, n$.

Satz I.14.17 (Vieta). *Für $\alpha = X^n + a_{n-1}X^{n-1} + \ldots + a_0 \in \mathbb{Q}[X]$ mit Nullstellen $x_1, \ldots, x_n \in \mathbb{C}$ gilt*

$$a_{n-k} = (-1)^k \sigma_k(x_1, \ldots, x_n)$$

für $k = 1, \ldots, n$.

Beweis.

$$\alpha = \prod_{i=1}^{n} (X - x_i) = \sum_{k=0}^{n} \Big((-1)^k \sum_{1 \leq i_1 < \ldots < i_k \leq n} x_{i_1} \ldots x_{i_k} \Big) X^{n-k}. \qquad \square$$

Beispiel I.14.18. Für $\alpha = X^2 + aX + b$ mit Nullstellen x_1 und x_2 gilt $x_1 + x_2 = -a$ sowie $x_1x_2 = b$.

Satz I.14.19 (Hauptsatz über symmetrische Polynome). *Für jedes symmetrische $\alpha \in K[X_1, \ldots, X_n]$ existiert genau ein $\gamma \in K[X_1, \ldots, X_n]$ mit $\alpha = \gamma(\sigma_1, \ldots, \sigma_n)$.*

Beweis.
Existenz: Sei o. B. d. A.

$$\alpha = \sum_{i_1,\ldots,i_n} a_{i_1,\ldots,i_n} X_1^{i_1} \ldots X_n^{i_n} \neq 0.$$

Wir ordnen die Tupel $(i_1, \ldots, i_n)$ lexikografisch und argumentieren durch Induktion nach

$$f(\alpha) := \max\big\{(i_1, \ldots, i_n) : a_{i_1,\ldots,i_n} \neq 0\big\}.$$

Im Fall $f(\alpha) = (0, \ldots, 0)$ ist $\gamma := \alpha = a_{0,\ldots,0} \in K$. Sei nun $f(\alpha) = (d_1, \ldots, d_n) > (0, \ldots, 0)$. Wegen $\alpha = \alpha(X_{\pi(1)}, \ldots, X_{\pi(n)})$ für alle $\pi \in S_n$ ist $d_1 \geq \ldots \geq d_n$. Sei

$$\beta := a_{d_1,\ldots,d_n} \sigma_1^{d_1-d_2} \sigma_2^{d_2-d_3} \ldots \sigma_{n-1}^{d_{n-1}-d_n} \sigma_n^{d_n}.$$

Es gilt $f(\sigma_k^{d_k-d_{k+1}}) = (d_k - d_{k+1}) f(\sigma_k) = (d_k - d_{k+1}, \ldots, d_k - d_{k+1}, 0, \ldots, 0)$ und

$$f(\beta) = f(\sigma_1^{d_1-d_2}) + \ldots + f(\sigma_n^{d_n}) = (d_1, \ldots, d_n).$$

Das symmetrische Polynom $\alpha - \beta$ erfüllt daher $f(\alpha - \beta) < (d_1, \ldots, d_n)$ und die Existenz von γ folgt mit Induktion.

Eindeutigkeit: Seien $\gamma, \delta \in K[X_1, \ldots, X_n]$ mit $\gamma(\sigma_1, \ldots, \sigma_n) = \delta(\sigma_1, \ldots, \sigma_n)$. Für $\rho := \gamma - \delta$ ist dann $\rho(\sigma_1, \ldots, \sigma_n) = 0$ und wir müssen $\rho = 0$ zeigen. Sei indirekt $\rho \neq 0$. Sei $d_1 \geq \ldots \geq d_n$ das lexikografisch größte n-Tupel, sodass der Koeffizient von $X_1^{d_1-d_2} X_2^{d_2-d_3} \ldots X_n^{d_n}$ in ρ nicht verschwindet. Wie oben gilt $f(\sigma_1^{d_1-d_2} \ldots \sigma_n^{d_n}) = (d_1, \ldots, d_n)$. Für jeden weiteren Summanden $X_1^{e_1-e_2} \ldots X_n^{e_n}$ von ρ ist $f(\sigma_1^{e_1-e_2} \ldots \sigma_n^{e_n}) < (d_1, \ldots, d_n)$. Dies ergibt $f(\rho(\sigma_1, \ldots, \sigma_n)) = (d_1, \ldots, d_n)$ im Widerspruch zu $\rho(\sigma_1, \ldots, \sigma_n) = 0$. □

Beispiel I.14.20.

(i) Wir betrachten $\alpha = XY^3 + X^3Y - X - Y \in K[X, Y]$. Mit den Bezeichnungen aus dem Beweis ist $f(\alpha) = (3, 1)$ und

$$\beta := \sigma_1^2 \sigma_2 = (X + Y)^2 XY = X^3Y + 2X^2Y^2 + XY^3.$$

Es folgt $\alpha - \beta = -2X^2Y^2 - X - Y$. Im nächsten Schritt ist $f(\alpha - \beta) = (2, 2)$ und

$$\beta_2 := -2\sigma_2^2 = -2X^2Y^2.$$

Es bleibt $\alpha - \beta - \beta_2 = -X - Y = -\sigma_1$. Schließlich ist

$$\alpha = \beta + \beta_2 - \sigma_1 = \sigma_1^2\sigma_2 - 2\sigma_2^2 - \sigma_1 = \gamma(\sigma_1, \sigma_2)$$

mit $\gamma = X^2Y - 2Y^2 - X$.

(ii) Für $k \in \mathbb{N}_0$ ist $\rho_k = X_1^k + \ldots + X_n^k \in K[X_1, \ldots, X_n]$ symmetrisch. Für $0 \leq l \leq n-1$ sei

$$\alpha(k, l) := \sum_{i=1}^{n} X_i^k \sigma_l(X_1, \ldots, X_{i-1}, X_{i+1}, \ldots, X_n).$$

Dann gilt

$$\sigma_i \rho_{k-i} = \begin{cases} \rho_k = \alpha(k, 0) & \text{falls } i = 0, \\ \alpha(k-i, i) + \alpha(k-i+1, i-1) & \text{falls } 1 \leq i \leq k < n, \\ \alpha(k-n+1, n-1) & \text{falls } i = n \leq k. \end{cases}$$

Als Teleskopsumme erhält man die GIRARD-NEWTON-Identitäten:

$$\boxed{\sum_{i=0}^{\min\{k,n\}} (-1)^i \sigma_i \rho_{k-i} = \begin{cases} 0 & \text{falls } k \geq n, \\ (-1)^k (n-k)\sigma_k & \text{falls } k < n \end{cases}}$$

(beachte $\alpha(0,l) = (n-l)\sigma_l$). Damit kann man ρ_k rekursiv durch $\sigma_0, \ldots, \sigma_n$ ausdrücken.

Definition I.14.21. Sei $\alpha \in \mathbb{Q}[X]$ normiert mit Nullstellen $x_1, \ldots, x_n \in \mathbb{C}$ (mit Vielfachheiten). Dann heißt

$$D_\alpha := \prod_{1 \leq i < j \leq n} (x_i - x_j)^2$$

die *Diskriminante* von α (hängt nicht von der Reihenfolge der x_i ab).

Bemerkung I.14.22. Ist L ein Zerfällungskörper von $\alpha \in \mathbb{Q}[X]$, so gilt $D_\alpha \in L^{\mathrm{Gal}(\alpha)} = \mathbb{Q}$ nach Artin. Man kann D_α als symmetrisches Polynom in $x_1, \ldots, x_n$ auffassen. Nach dem obigen Hauptsatz und Vieta lässt sich D_α als Polynom in den Koeffizienten von α ausdrücken. Für $\alpha = X^2 + aX + b$ erhält man

$$\boxed{D_\alpha = (x_1 - x_2)^2 = \sigma_1^2 - 4\sigma_2 = a^2 - 4b.}$$

Für $\alpha = X^3 + aX^2 + bX + c$ führt die TSCHIRNHAUS-Transformation $X \mapsto X - a/3$ zu einem reduzierten Polynom der Form $\alpha = X^3 + aX + b$ (dabei ändern sich weder D_α noch L). Nach der Produktregel gilt

$$(x_i - x_j)(x_i - x_k) = \alpha'(x_i) = 3x_i^2 + a$$

für $\{i,j,k\} = \{1,2,3\}$. Es folgt

$$\begin{aligned} -D_\alpha = \alpha'(x_1)\alpha'(x_2)\alpha'(x_3) &= (3x_1^2 + a)(3x_2^2 + a)(3x_3^2 + a) = \\ &= 27(x_1x_2x_3)^2 + 9a\big((x_1x_2)^2 + (x_1x_3)^2 + (x_2x_3)^2\big) + 3a^2(x_1^2 + x_2^2 + x_3^2) + a^3. \end{aligned}$$

Mit

$$\begin{aligned} (x_1x_2x_3)^2 &= \sigma_3^2 = b^2, \\ (x_1x_2)^2 + (x_1x_3)^2 + (x_2x_3)^2 &= (x_1x_2 + x_1x_3 + x_2x_3)^2 - 2x_1x_2x_3(x_1 + x_2 + x_3) = \sigma_2^2 - 2\sigma_3\sigma_1 = a^2, \\ x_1^2 + x_2^2 + x_3^2 &= (x_1 + x_2 + x_3)^2 - 2(x_1x_2 + x_1x_3 + x_2x_3) = \sigma_1^2 - 2\sigma_2 = -2a \end{aligned}$$

ergibt sich

$$\boxed{D_\alpha = -27b^2 - 9a^3 - 3a^2(-2a) - a^3 = -4a^3 - 27b^2.}$$

Im Allgemeinen lässt sich die Diskriminante über Determinanten berechnen (Beispiel III.2.43).

Satz I.14.23. *Für jedes irreduzible $\alpha \in \mathbb{Q}[X]$ gilt $\mathrm{Gal}(\alpha) \leq A_{\deg \alpha}$ genau dann, wenn $\sqrt{D_\alpha} \in \mathbb{Q}$.*

Beweis. Seien $x_1, \ldots, x_n$ die Nullstellen von α in einem Zerfällungskörper $L \subseteq \mathbb{C}$. Als irreduzibles Polynom hat α keine mehrfachen Nullstellen (Satz I.11.20) und $D_\alpha \neq 0$ folgt. Für $\Gamma \in G := \mathrm{Gal}(\alpha) \leq S_n$ gilt

$$\Gamma(\sqrt{D_\alpha}) = \prod_{i<j} (\Gamma(x_i) - \Gamma(x_j)) = \mathrm{sgn}(\Gamma)\sqrt{D_\alpha}.$$

Also ist $G \leq A_n$ genau dann, wenn $\sqrt{D_\alpha} \in L^G = \mathbb{Q}$. □

Bemerkung I.14.24.

(i) Sei $\alpha = X^3 + aX + b \in \mathbb{Q}[X]$ irreduzibel mit $a > 0$. Nach Bemerkung I.14.22 ist $D_\alpha = -4a^3 - 27b^2 < 0$ und $\mathrm{Gal}(\alpha) \cong S_3$ folgt aus Satz I.14.23. Wegen $\alpha' = 3X^2 + a$ hat der Graph von α keine Extremstellen und daher nur eine reelle Nullstelle. Die komplexe Konjugation liefert also eine Transposition in $\mathrm{Gal}(\alpha)$.

(ii) Nach Folgerung I.8.51 ist $\alpha = X^3 - 3X + 1$ irreduzibel mit $D_\alpha = 4 \cdot 3^3 - 27 = 3^4 = 9^2$. Daher gilt

$$G := \mathrm{Gal}(\alpha) \cong A_3 \cong C_3$$

nach Satz I.14.23. Die komplexe Konjugation operiert somit trivial auf den Nullstellen von α, d. h. α besitzt drei reelle Nullstellen. Insbesondere liegt der Zerfällungskörper K von α in $\mathbb{R}$ und hat Grad 3 über $\mathbb{Q}$. Ist K eine Radikalerweiterung, so existiert ein positives $x \in \mathbb{Q}$ mit $K = \mathbb{Q}(\sqrt[3]{x})$. Nun muss G aber auch die Nullstellen von $X^3 - x$ permutieren. Da zwei von diesen nicht-reell sind, müsste $\sqrt[3]{x}$ unter G festbleiben. Dies widerspricht $K^G = \mathbb{Q}$. Also ist K keine Radikalerweiterung, obwohl α auflösbar ist.

(iii) Mit einer Transformation wie in Bemerkung I.14.22 kann man ein Polynom vom Grad 4 in die reduzierte Form $\alpha = X^4 + aX^2 + bX + c \in \mathbb{Q}[X]$ überführen. Sei α irreduzibel mit Nullstellen $x_1, \ldots, x_4$ in einem Zerfällungskörper $L \subseteq \mathbb{C}$. Dann permutiert $G := \mathrm{Gal}(\alpha)$ die Zahlen

$$y_1 := x_1x_2 + x_3x_4, \qquad y_2 := x_1x_3 + x_2x_4, \qquad y_3 := x_1x_4 + x_2x_3.$$

Es gilt

$$\begin{aligned} y_1 + y_2 + y_3 &= \sigma_2 = a, \\ y_1y_2 + y_1y_3 + y_2y_3 &= \sigma_1\sigma_3 - 4\sigma_4 = -4c, \\ y_1y_2y_3 &= \sigma_1^2\sigma_4 + \sigma_3^2 - 4\sigma_2\sigma_4 = b^2 - 4ac. \end{aligned}$$

Nach Vieta sind y_1, y_2, y_3 die Lösungen der *kubischen Resolvente*

$$\beta := Y^3 - aY^2 - 4cY - b^2 + 4ac.$$

Wegen $y_1 - y_2 = (x_1 - x_4)(x_2 - x_3)$ usw. gilt $D_\alpha = D_\beta$. Zerfällt β in Linearfaktoren über $\mathbb{Q}$, so ist $G = \langle (1,2)(3,4), (1,3)(2,4) \rangle = V_4$. Hat β genau eine rationale Nullstelle, sagen wir y_1, so gilt

$$C_4 \cong \langle (1,3,2,4) \rangle \leq G \leq \langle (1,3,2,4), (1,2) \rangle \overset{\text{Aufgabe I.24}}{\cong} D_8.$$

Ist schließlich β irreduzibel, so erhält man

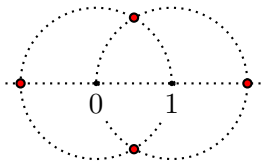
$$G = \begin{cases} A_4 & \text{falls } \sqrt{D_\beta} \in \mathbb{Q}, \\ S_4 & \text{falls } \sqrt{D_\beta} \notin \mathbb{Q}. \end{cases}$$

15 Konstruktion mit Zirkel und Lineal

Bemerkung I.15.1. Wir betrachten im Folgenden die Menge der komplexen Zahlen als zweidimensionale Zeichenfläche.

Definition I.15.2. Sei $\mathcal{M}_0 := \{0, 1\} \subseteq \mathbb{C}$ und induktiv $\mathcal{M}_{i-1} \subseteq \mathbb{C}$ mit $i \geq 1$. Sei $\mathcal{G}$ die Menge aller Geraden in $\mathbb{C}$, die durch zwei Punkte in $\mathcal{M}_{i-1}$ verlaufen. Analog sei $\mathcal{K}$ die Menge aller Kreise in $\mathbb{C}$, deren Mittelpunkt in $\mathcal{M}_{i-1}$ liegt und deren Radius gleich dem Abstand zweier Punkte in $\mathcal{M}_{i-1}$ ist. Schließlich sei $\mathcal{M}_i$ die Menge der Schnittpunkte von zwei verschiedenen Figuren aus $\mathcal{G} \cup \mathcal{K}$. Ein Punkt $z \in \mathbb{C}$ heißt (*mit Zirkel und Lineal*) *konstruierbar*, falls $z \in \mathcal{M} := \bigcup_{i \geq 0} \mathcal{M}_i$.

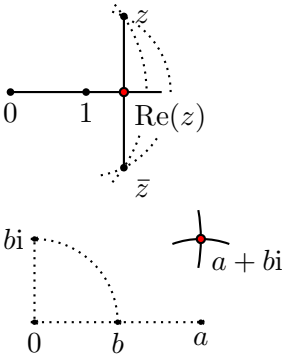
Beispiel I.15.3. Es gilt $\mathcal{M}_1 := \left\{-1, 0, 1, 2, \frac{1}{2}(1 \pm \sqrt{3}\mathrm{i})\right\}$.



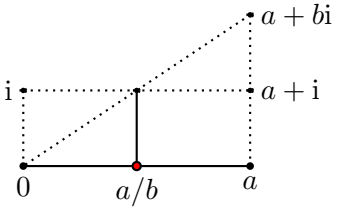
Lemma I.15.4. *Die konstruierbaren Punkte bilden einen Teilkörper von $\mathbb{C}$, der unter Quadratwurzelziehen und komplexer Konjugation abgeschlossen ist.*

Beweis.
Schritt 1: $z \in \mathcal{M} \Longrightarrow |z| \in \mathcal{M}$.
Durch die Punkte $0, 1 \in \mathcal{M}$ erhält man alle Schnittpunkte auf der x-Achse. Nun ist $|z|$ der Schnittpunkt der x-Achse mit dem Kreis mit Mittelpunkt 0 und Radius $|z|$.

Schritt 2: $z \in \mathcal{M} \iff \mathrm{Re}(z), \mathrm{Im}(z) \in \mathcal{M}$.
Zieht man Kreise um 1 und -1 mit Radius 2 und verbindet die beiden Schnittpunkte, so erhält man die y-Achse. Für ein beliebiges $z \in \mathcal{M}$ konstruiert man $\mathrm{Re}(z), \mathrm{Im}(z)\mathrm{i} \in \mathcal{M}$, indem man das Lot auf der x- und y-Achse fällt (siehe Abbildung). Mit Schritt 1 folgt auch $\mathrm{Im}(z) \in \mathcal{M}$. Sind umgekehrt $a, b \in \mathcal{M} \cap \mathbb{R}$ gegeben, dann konstruiert man zunächst $b\mathrm{i}$ und anschließend $a + b\mathrm{i}$ als Schnittpunkt zweier Kreise (siehe Abbildung).

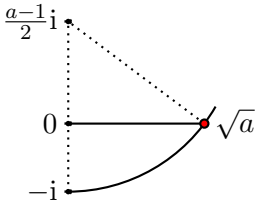


Schritt 3: $\mathcal{M} \cap \mathbb{R}$ ist ein Körper.
Nach Definition ist $0, 1 \in \mathcal{M} \cap \mathbb{R}$. Für $a, b \in \mathcal{M} \cap \mathbb{R}$ erhält man $a - b \in \mathcal{M} \cap \mathbb{R}$ als Schnittpunkt der x-Achse mit dem Kreis mit Mittelpunkt a und Radius b. Für $a, b \in \mathcal{M} \cap \mathbb{R} \setminus \{0\}$ erhält man $a/b \in \mathcal{M}$ mit dem Strahlensatz (o. B. d. A. $a, b > 0$, siehe Abbildung).



Schritt 4: $a \in \mathcal{M} \cap \mathbb{R} \Longrightarrow \sqrt{a} \in \mathcal{M}$.
Im Fall $a < 0$ ist $\sqrt{a} = \sqrt{|a|}\mathrm{i}$. Wir können also $a > 0$ annehmen. Die Behauptung folgt nun mit dem Satz des Pythagoras (siehe Abbildung):

$$\left(\frac{a-1}{2}\right)^2 + \sqrt{a}^2 = \left(\frac{a+1}{2}\right)^2.$$



Schritt 5: $\mathcal{M}$ ist ein Körper.
Für $z, w \in \mathcal{M}$ ist $z + w = \mathrm{Re}(z) + \mathrm{Re}(w) + \mathrm{Im}(z)\mathrm{i} + \mathrm{Im}(w)\mathrm{i} \in \mathcal{M}$ nach den vorherigen Schritten. Für $z, w \in \mathcal{M} \setminus \{0\}$ ist analog

$$\frac{z}{w} = \frac{z\overline{w}}{|w|^2} = \frac{\mathrm{Re}(z)\mathrm{Re}(w) + \mathrm{Im}(z)\mathrm{Im}(w)}{|w|^2} + \frac{\mathrm{Im}(z)\mathrm{Re}(w) - \mathrm{Re}(z)\mathrm{Im}(w)}{|w|^2}\mathrm{i} \in \mathcal{M}.$$

Schritt 6: $z \in \mathcal{M} \Longrightarrow \overline{z}, \sqrt{z} \in \mathcal{M}$.
Die Behauptung $\overline{z} = \mathrm{Re}(z) - \mathrm{Im}(z)\mathrm{i} \in \mathcal{M}$ folgt sofort aus den bisherigen Schritten. Wegen $\sqrt{-z} = \sqrt{z}\mathrm{i}$ können wir $\mathrm{Im}(z) \geq 0$ annehmen. Es gilt dann

$$\sqrt{z} = \sqrt{\frac{1}{2}\big(\mathrm{Re}(z) + \sqrt{\mathrm{Re}(z)^2 + \mathrm{Im}(z)^2}\big)} + \sqrt{\frac{1}{2}\big(-\mathrm{Re}(z) + \sqrt{\mathrm{Re}(z)^2 + \mathrm{Im}(z)^2}\big)}\mathrm{i} \in \mathcal{M}$$

nach Schritt 4. □

Satz I.15.5. *Genau dann ist $z \in \mathbb{C}$ konstruierbar, wenn Körper $\mathbb{Q} = K_0 \subseteq \ldots \subseteq K_n$ mit $|K_i : K_{i-1}| = 2$ für $i = 1, \ldots, n$ und $z \in K_n$ existieren.*

Beweis. Sei zunächst $\mathbb{Q} = K_0 \subseteq \ldots \subseteq K_n$ mit $|K_i : K_{i-1}| = 2$ für $i = 1, \ldots, n$ und $z \in K_n$. Dann existieren $a_i \in K_{i-1}$ mit $K_i = K_{i-1}(\sqrt{a_i})$ für $i = 1, \ldots, n$ (siehe Beweis von Satz I.12.23). Mit Lemma I.15.4 ist $a_1 \in K_0 = \mathbb{Q} = P(\mathcal{M}) \subseteq \mathcal{M}$, $K_1 = K_0(\sqrt{a_1}) \subseteq \mathcal{M}$ und induktiv $z \in K_n \subseteq \mathcal{M}$.

Sei nun umgekehrt z konstruierbar, d. h. $z \in \mathcal{M}_k$ für ein $k \geq 0$. Wir argumentieren durch Induktion nach k. Im Fall $k = 0$ ist $\mathbb{Q}(z) = \mathbb{Q}$ und die Behauptung gilt für $n = 0$. Sei also $k \geq 1$. Dann ergibt sich z durch eine Konstruktion aus $a_1, \ldots, a_l \in \mathcal{M}_{k-1}$. Nach Induktion existieren Körper $\mathbb{Q} = K_{i,0} \subseteq \ldots \subseteq K_{i,m_i}$ mit $a_i \in K_{i,m_i}$ und $|K_{i,j} : K_{i,j-1}| = 2$ für $j = 1, \ldots, m_i$ und $i = 1, \ldots, l$. Komplexe Konjugation liefert eine analoge Erweiterungskette für $\overline{a_i}$. Wie oben ergeben sich all diese Erweiterungen durch iterative Adjunktion von Quadratwurzeln. Adjungiert man all diese Quadratwurzeln nacheinander, so erhält man

$$\mathbb{Q} = K_0 \subseteq \ldots \subseteq K_n$$

mit $a_1, \ldots, a_l, \overline{a_1}, \ldots, \overline{a_l} \in K_n$ und $|K_i : K_{i-1}| = 2$ für $i = 1, \ldots, n$. Wir unterscheiden nun die drei Konstruktionsprinzipien.

Fall 1: z ist Schnittpunkt von zwei verschiedenen Geraden.
Dann existieren $a, b, c, d \in K_n$ und $r, s \in \mathbb{R}$ mit $z = a + rb = c + sd$. Also ist (r, s) die einzige Lösung des Gleichungssystems

$$\begin{pmatrix} \mathrm{Re}(b) & -\mathrm{Re}(d) \\ \mathrm{Im}(b) & -\mathrm{Im}(d) \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \mathrm{Re}(c-a) \\ \mathrm{Im}(c-a) \end{pmatrix}.$$

Wegen $\mathrm{Re}(a) = (a + \bar{a})/2 \in K_n$ usw. folgt $r \in K_n$ und $z = a + rb \in K_n$ nach Lemma I.15.4.

Fall 2: z ist Schnittpunkt einer Geraden und eines Kreises.
Dann existieren $a, b, c \in K_n$, $r \in K_n \cap \mathbb{R}$ und $s \in \mathbb{R}$ mit $z = a + sb$ und

$$\mathrm{Re}(a + sb - c)^2 + \mathrm{Im}(a + sb - c)^2 = r^2.$$

Dies ist eine quadratische Gleichung für s mit Koeffizienten in K_n. Also liegen s und z in einer quadratischen Erweiterung von K_n. Die Behauptung folgt mit Lemma I.15.4.

Fall 3: z ist Schnittpunkt von zwei verschiedenen Kreisen.
Dann existieren $a_i \in K_n$ und $r_i \in K_n \cap \mathbb{R}$ mit $\mathrm{Re}(z - a_i)^2 + \mathrm{Im}(z - a_i)^2 = r_i^2$ für $i = 1, 2$. Subtraktion ergibt

$$\mathrm{Re}(a_1 - a_2)\mathrm{Re}(z) + \mathrm{Im}(a_1 - a_2)\mathrm{Im}(z) \in K_n \cap \mathbb{R}. \tag{I.15.1}$$

Da die Mittelpunkte a_1 und a_2 der Kreise verschieden sind, beschreibt (I.15.1) eine Gerade, auf der mindestens zwei Punkte aus K_n liegen. Die Behauptung folgt nun mit Fall 2. □

Folgerung I.15.6. *Ist $z \in \mathbb{C}$ konstruierbar, so ist $|\mathbb{Q}(z) : \mathbb{Q}|$ eine 2-Potenz. Insbesondere ist z algebraisch über $\mathbb{Q}$.*

Beweis. Mit den Bezeichnungen aus Satz I.15.5 gilt $|\mathbb{Q}(z) : \mathbb{Q}| \mid |K_n : K_0| = 2^n$. □

Bemerkung I.15.7.

(i) Satz I.15.5 zeigt, dass $\mathcal{M}$ der „kleinste“ Teilkörper von $\mathbb{C}$ ist, der unter Quadratwurzelziehen abgeschlossen ist.

(ii) Die Umkehrung von Folgerung I.15.6 ist falsch: Nach Eisenstein mit $p = 2$ ist $\alpha = X^4 + 2X - 2 \in \mathbb{Q}[X]$ irreduzibel mit kubischer Resolvente $\beta = Y^3 + 8Y - 4$ (siehe Bemerkung I.14.24). Da β keine ganzzahlige Nullstelle hat, ist β irreduzibel nach Folgerung I.8.51. Wegen $D_\alpha = D_\beta < 0$ ist $G := \mathrm{Gal}(\alpha) \cong S_4$. Für eine Nullstelle z von α in einem Zerfällungskörper L ist $|\mathbb{Q}(z) : \mathbb{Q}| = 4$ und $H := \mathrm{Gal}(L|\mathbb{Q}(z)) \leq G$ hat Ordnung 6. Nach Sylow besitzt G genau vier 3-Sylowgruppen, von denen genau eine, sagen wir P, in H liegt. Es folgt $H = \mathrm{N}_G(P)$. Existiert eine Untergruppe $H < K < G$, so hätte man den Widerspruch

$$|\mathrm{Syl}_3(K)| = |K : \mathrm{N}_K(P)| = |K : H| = 2 \not\equiv 1 \pmod 3.$$

Der Hauptsatz der Galois-Theorie impliziert, dass $\mathbb{Q}(z)$ keine Teilkörper vom Grad 2 über $\mathbb{Q}$. Somit ist z nicht konstruierbar, aber $|\mathbb{Q}(z) : \mathbb{Q}| = 4$.

Satz I.15.8 (Probleme der Antike)**.**

(i) (*Quadratur des Kreises*) *Mit Zirkel und Lineal lässt sich kein Quadrat konstruieren, das den gleichen Flächeninhalt wie der Einheitskreis hat.*

(ii) (*Winkeldreiteilung*) *Nicht jeder Winkel lässt sich mit Zirkel und Lineal in drei gleichgroße Winkel teilen.*

(iii) (*delisches Problem*) *Mit Zirkel und Lineal lässt sich kein Würfel konstruieren, der doppelt so groß wie der Einheitswürfel ist.*

Beweis.

(i) Da der Einheitskreis Flächeninhalt π hat, beträgt die Seitenlänge des entsprechenden Quadrats $\sqrt{\pi}$. Nach Lindemann sind π und $\sqrt{\pi}$ transzendent. Die Behauptung folgt aus Folgerung I.15.6.

(ii) Nehmen wir an, dass man 120° dreiteilen kann. Dann kann man 40° konstruieren und damit eine primitive 9-te Einheitswurzel ζ. Nach Satz I.12.12 ist $|\mathbb{Q}(\zeta) : \mathbb{Q}| = \varphi(9) = 6$ keine 2-Potenz. Die Behauptung folgt aus Folgerung I.15.6.

(iii) Die Kantenlänge des entsprechenden Würfels beträgt $z := \sqrt[3]{2}$. Bekanntlich ist $X^3 - 2$ das Minimalpolynom von z und $|\mathbb{Q}(z) : \mathbb{Q}| = 3$ ist keine 2-Potenz. Wieder folgt die Behauptung aus Folgerung I.15.6. □

Lemma I.15.9. *Ist $2^n + 1$ eine Primzahl mit $n \in \mathbb{N}$, so ist n eine 2-Potenz.*

Beweis. Besitzt n einen ungeraden Teiler $q > 1$, so ist

$$2^n + 1 = (2^{n/q} + 1) \sum_{i=0}^{q-1} (-2^{n/q})^i \qquad \text{(geometrische Reihe)}$$

keine Primzahl. □

Bemerkung I.15.10. Die Primzahlen der Form $F_n := 2^{2^n} + 1$ heißen FERMAT-*Primzahlen* (vgl. Aufgabe I.4). Die einzig bekannten sind $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ und $F_4 = 65537$. Es gilt

$$\begin{aligned}
&641 = 5^4 + 2^4 \mid 2^{28}(5^4 + 2^4) = 5^4 \cdot 2^{28} + 2^{32},\\
&641 = 5 \cdot 2^7 + 1 \mid (5 \cdot 2^7 + 1)(5 \cdot 2^7 - 1)(5^2 \cdot 2^{14} + 1) = 5^4 \cdot 2^{28} - 1,\\
&641 \,\Big|\, (5^4 \cdot 2^{28} + 2^{32}) - (5^4 \cdot 2^{28} - 1) = 2^{32} + 1 = F_5 \notin \mathbb{P}.
\end{aligned}$$

Allgemeiner weiß man $F_n \notin \mathbb{P}$ für $n = 5, \ldots, 32$ (`http://www.fermatsearch.org`).

Satz I.15.11 (GAUSS[1])**.** *Genau dann lässt sich das regelmäßige n-Eck mit Zirkel und Lineal konstruieren, wenn n das Produkt einer 2-Potenz und paarweise verschiedenen Fermat-Primzahlen ist.*

Beweis. Das regelmäßige n-Eck ist genau dann konstruierbar, wenn man eine primitive n-te Einheitswurzel $\zeta \in \mathbb{C}$ konstruieren kann. Sei $n = p_1^{a_1} \ldots p_k^{a_k}$ die Primfaktorzerlegung von n. Dann ist

$$|\mathbb{Q}(\zeta) : \mathbb{Q}| \overset{I.12.12}{=} \varphi(n) \overset{I.2.38}{=} p_1^{a_1 - 1}(p_1 - 1) \ldots p_k^{a_k - 1}(p_k - 1).$$

Ist ζ konstruierbar, so ist $\varphi(n)$ nach Folgerung I.15.6 eine 2-Potenz. Dies zeigt $p_i = 2$ oder $p_i^{a_i}$ ist eine Fermat-Primzahl nach Lemma I.15.9 für jedes $i \in \{1, \ldots, k\}$.

Ist umgekehrt n das Produkt einer 2-Potenz und paarweise verschiedenen Fermat-Primzahlen, so ist $\varphi(n)$ eine 2-Potenz. Nach Satz I.12.12 ist $\mathbb{Q} \subseteq \mathbb{Q}(\zeta)$ eine Galois-Erweiterung und $G := \mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q})$ ist eine 2-Gruppe. Nach Sylow existieren $1 = G_0 < \ldots < G_m = G$ mit $|G_i : G_{i-1}| = 2$ für $i = 1, \ldots, m$. Für $K_i := \mathbb{Q}(\zeta)^{G_{m-i}}$ gilt dann $\mathbb{Q} = K_0 \subseteq \ldots \subseteq K_m = \mathbb{Q}(\zeta)$ mit $|K_i : K_{i-1}| = 2$ für $i = 1, \ldots, m$ nach dem Hauptsatz der Galois-Theorie. Nach Satz I.15.5 ist ζ konstruierbar. □

[1] Gauß schrieb dazu: „Durch angestrengtes Nachdenken über den Zusammenhang aller Wurzeln untereinander nach arithmetischen Gründen glückte es mir, bei einem Ferienaufenthalt in Braunschweig am Morgen des gedachten Tages (ehe ich aus dem Bette aufgestanden war) diesen Zusammenhang auf das klarste anzuschauen, so daß ich die spezielle Anwendung auf das 17-Eck und die numerische Bestätigung auf der Stelle machen konnte."

Beispiel I.15.12.

(i) Das regelmäßige n-Eck lässt sich für $n = 3, 4, 5, 6, 8, 10, 12, 15, 16, 17, \ldots$ konstruieren.

(ii) (Konstruktion des regelmäßigen 5-Ecks) Für $\zeta := e^{2\pi \mathrm{i}/5}$ und $\omega := \zeta + \zeta^{-1} = 2\mathrm{Re}(\zeta)$ gilt

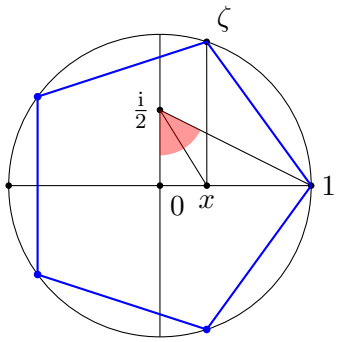
$$0 = \Phi_5(\zeta) = \zeta^4 + \zeta^3 + \zeta^2 + \zeta + 1 = \zeta^2 + 2 + \zeta^{-2} + \zeta + \zeta^{-1} - 1 = \omega^2 + \omega - 1.$$

Dies zeigt $\mathrm{Re}(\zeta) = \frac{\omega}{2} = \frac{1}{4}(\sqrt{5} - 1) \in \mathcal{M}$ (beachte: $\mathrm{Re}(\zeta) > 0$).

(1) Konstruiere $\frac{\mathrm{i}}{2}$. Nach Pythagoras hat die Strecke $(\frac{\mathrm{i}}{2}, 1)$ Länge $\frac{\sqrt{5}}{2}$.

(2) Halbiere den Winkel $(0, \frac{i}{2}, 1)$. Die Winkelhalbierende teilt die Strecke $(0, 1)$ im Verhältnis der anliegenden Seiten (Winkelhalbierendensatz). Für den Schnittpunkt $x \in \mathbb{R}$ der Winkelhalbierenden mit der x-Achse gilt daher $\frac{x}{1-x} = \frac{1}{\sqrt{5}}$ und

$$x = \frac{1}{\sqrt{5}+1} = \frac{\sqrt{5}-1}{4} = \mathrm{Re}(\zeta).$$



(3) Fälle das Lot bei x. Der Schnittpunkt des Lots mit dem Einheitskreis ist ζ.

(4) Trage die Strecke $(1, \zeta)$ dreimal auf dem Einheitskreis ab.

(5) Verbinde die entstandenen Punkte.

Bemerkung I.15.13. Nach Gauß lässt sich $\zeta := e^{2\pi \mathrm{i}/17}$ konstruieren. In der Tat ist

$$\mathrm{Re}(\zeta) = \frac{1}{16}\left(2\sqrt{17 + 3\sqrt{17} - \sqrt{34 - 2\sqrt{17}} - 2\sqrt{34 + 2\sqrt{17}}} + \sqrt{34 - 2\sqrt{17}} + \sqrt{17} - 1\right)$$

(ohne Beweis).

Satz I.15.14 (Mohr, Mascheroni)**.** *Jeder konstruierbare Punkt lässt sich auch nur mit Zirkel konstruieren.*

Beweis. Siehe zum Beispiel [N. Hungerbühler, *A short elementary proof of the Mohr-Mascheroni Theorem*, Amer. Math. Monthly 101 (1994), 784–787]. □

Aufgaben

Zahlentheorie

Aufgabe I.1 (3 Punkte)**.** Lösen Sie die Gleichung

$$x^3 - 3x^2 + x - 1 = 0$$

in $\mathbb{C}$.

Aufgabe I.2 (3 Punkte)**.** Berechnen Sie $\mathrm{ggT}(813, 1329)$ und finden Sie $a, b \in \mathbb{Z}$ mit

$$813a + 1329b = \mathrm{ggT}(813, 1329).$$

Aufgabe I.3 (2 Punkte)**.** Sei $2 \leq b \in \mathbb{N}$. Zeigen Sie, dass sich jedes $n \in \mathbb{N}_0$ eindeutig in der Form

$$n = \sum_{i=0}^{\infty} n_i b^i \qquad (b\text{-}adische\ Entwicklung)$$

mit $0 \leq n_i \leq b - 1$ für $i \geq 0$ schreiben lässt.

Aufgabe I.4 ($2 + 2 + 2$ Punkte)**.** Für $n \in \mathbb{N}_0$ sei $F_n := 2^{2^n} + 1$. Zeigen Sie:

(a) $\prod_{k=0}^{n-1} F_k = F_n - 2$ für $n \in \mathbb{N}_0$.

(b) $\mathrm{ggT}(F_n, F_m) = 1$ für $n \neq m$.

(c) Geben Sie mit Hilfe von (b) einen neuen Beweis für $|\mathbb{P}| = \infty$.

Aufgabe I.5 ($2 + 2$ Punkte)**.**

(a) Zeigen Sie, dass es unendlich viele Primzahlen der Form $4n - 1$ gibt.
Hinweis: Untersuchen Sie die Primteiler von $4p_1 \dots p_k - 1$ mit $p_1, \dots, p_k \in \mathbb{P}$.

(b) Zeigen Sie, dass es unendlich viele Primzahlen der Form $6n - 1$ gibt.

Aufgabe I.6 (2 Punkte)**.** Bestimmen Sie die kleinste natürliche Zahl n mit der Eigenschaft

$$\forall p \in \mathbb{P} : p \mid n \iff (p - 1) \mid n.$$

Hinweis: Die Lösung hat Bezug zu Jena.

Aufgabe I.7 ($2 + 2 + 2$ Punkte)**.**

(a) Berechnen Sie $\mathrm{kgV}(10.403, 10.807)$.

(b) Lösen Sie die Gleichung $47x \equiv 27 \pmod{89}$ in $\mathbb{Z}$.

(c) Lösen Sie das System

$$\begin{aligned} x &\equiv 11 \pmod{37}, \\ 2x &\equiv 13 \pmod{41}. \end{aligned}$$

Aufgabe I.8 (2 + 2 + 2 Punkte)**.** Sei $n \in \mathbb{N}$. Zeigen Sie:

(a) Genau dann ist n durch 3 (bzw. 9) teilbar, wenn die Quersumme von n durch 3 (bzw. 9) teilbar ist. (Die Quersumme ist die Summe der Dezimalziffern.)

(b) Genau dann ist n durch 11 teilbar, wenn die alternierende Summe der Dezimalziffern von n durch 11 teilbar ist. (Es spielt keine Rolle, ob man die Summe von links oder rechts beginnt.)

(c) Wir gruppieren nun die Dezimalziffern in 3er Blöcke beginnend von rechts. Genau dann ist n durch 7 teilbar, wenn die alternierende Summe dieser Blöcke durch 7 teilbar ist (Beispiel: $12.345.678 \to 678 - 345 + 12 = 345 = 7 \cdot 50 - 5 \equiv 2 \pmod{7}$).

Aufgabe I.9 (3 Punkte)**.** (Wilson) Sei $2 \leq n \in \mathbb{N}$. Zeigen Sie, dass n genau dann eine Primzahl ist, wenn

$$(n-1)! \equiv -1 \pmod{n}$$

gilt.

Aufgabe I.10 (3 Punkte)**.** (Lamé) Wie groß müssen $a, b \in \mathbb{N}$ mindestens sein, damit der euklidische Algorithmus zur Berechnung von $\mathrm{ggT}(a, b)$ genau $k \in \mathbb{N}$ Iterationen durchläuft?
Hinweis: Die Lösung führt auf eine bekannte Zahlenfolge.

Aufgabe I.11 (3 Punkte)**.** Fünf Piraten und ein Affe stranden auf einer einsamen Insel. Am ersten Tag sammeln Sie n Kokosnüsse. In der folgenden Nacht wacht ein Pirat auf, um sich seinen Anteil zu sichern. Er teilt den Haufen der Kokosnüsse in fünf gleichgroße Teile, wobei eine Kokosnuss übrig bleibt, die er dem Affen schenkt. Danach bringt er einen der fünf Teile in ein Geheimversteck und legt sich wieder schlafen. Kurze Zeit später wacht auch der zweite Pirat auf, um die gleiche Prozedur durchzuführen (wieder bleibt eine Nuss für den Affen übrig). Im weiteren Verlauf der Nacht führen auch die übrigen drei Piraten diese Prozedur durch. Am nächsten Morgen wird der verbleibende Haufen zu gleichen Teilen an die fünf Piraten verteilt, wobei diesmal keine Nuss übrig bleibt. Wie groß war n mindestens?

Aufgabe I.12 (2 + 2 Punkte)**.**

(a) Bestimmen Sie alle $n \in \mathbb{N}$ mit $\varphi(n) = 14$.

(b) Bestimmen Sie die Primfaktorzerlegung von 626.257.
Hinweis: Hilft es, wenn man $\varphi(626.257) = 624.640$ weiß?

Aufgabe I.13 (3 Punkte)**.** Zeigen Sie, dass es 48 aufeinander folgende natürliche Zahlen gibt, die alle einen quadratischen Teiler haben.
Hinweis: Verwenden Sie den chinesischen Restsatz.

Aufgabe I.14 (3 Punkte)**.** Zeigen Sie $\mathrm{ggT}(a^n - 1, a^m - 1) = a^{\mathrm{ggT}(n,m)} - 1$ für $a, n, m \in \mathbb{N}$.

Gruppentheorie

Aufgabe I.15 $(1+1+1+1$ Punkte$)$**.** Bestimmen Sie die Zyklentypen der Elemente in S_5. Wie viele Elemente gibt es von jedem Typ? Welche Ordnung und welches Vorzeichen haben diese Elemente?

Aufgabe I.16 (3 Punkte)**.** Zeigen Sie:

$$V_4 := \big\{1, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\big\} = \big\langle (1,2)(3,4), (1,3)(2,4)\big\rangle \trianglelefteq S_4.$$

Man nennt V_4 die *Kleinsche Vierergruppe*.

Aufgabe I.17 $(2+2$ Punkte$)$**.** Seien $H \leq G$ Gruppen. Zeigen Sie:

(a) $H_G := \bigcap_{g\in G} gHg^{-1}$ ist der „größte“ Normalteiler von G, der in H liegt, d. h. für $N \trianglelefteq G$ mit $N \subseteq H$ gilt $N \subseteq H_G$.

(b) $H^G := \langle \bigcup_{g\in G} gHg^{-1}\rangle$ ist der „kleinste“ Normalteiler von G, der H enthält, d. h. für $N \trianglelefteq G$ mit $H \subseteq N$ gilt $H^G \subseteq N$.

Aufgabe I.18 $(3+2$ Punkte$)$**.** Zeigen Sie, dass für jede Gruppe G die folgenden Aussagen äquivalent sind:

(1) G ist abelsch.

(2) $G \to G$, $g \mapsto g^{-1}$ ist ein Automorphismus.

(3) $G \to G$, $g \mapsto g^2$ ist ein Endomorphismus.

Wann ist $G \to G$, $g \mapsto g^2$ ein Automorphismus (nehmen Sie dafür $|G| < \infty$ an)?

Aufgabe I.19 $(2+2+2+2+2+2$ Punkte$)$**.** Sei G eine Gruppe und $U, V, W \leq G$. Zeigen Sie:

(a) $U \subseteq V \Longrightarrow |G:U| = |G:V||V:U|$.

(b) $U \cup V \leq G \iff U \cup V \in \{U, V\}$.

(c) $UV \leq G \iff UV = VU$.

(d) $|UV| = |U : U \cap V||V| = |V : U \cap V||U|$.

(e) $U \subseteq W \Longrightarrow UV \cap W = U(V \cap W)$.

(f) Sind $|G:U|$ und $|G:V|$ endlich und teilerfremd, so ist $|G : U \cap V| = |G:U||G:V|$ und $G = UV$.

Aufgabe I.20 $(2+2$ Punkte$)$**.** Für $3 \leq n \in \mathbb{N}$ sei

$$D_{2n} := \langle \sigma, \tau\rangle \leq \mathrm{Sym}(\mathbb{C})$$

mit $\sigma(z) := e^{\frac{2\pi \mathrm{i}}{n}} z$ und $\tau(z) := \overline{z}$ (komplexe Konjugation) für $z \in \mathbb{C}$. Zeigen Sie:

(a) $\langle\sigma\rangle \trianglelefteq D_{2n}$ und $|D_{2n}| = 2n$.

(b) Ist $\Delta \subseteq \mathbb{C}$ das regelmäßige n-Eck in der komplexen Ebene mit Mittelpunkt 0 und Eckpunkt 1 (also die konvexe Hülle der n-ten Einheitswurzeln), so gilt

$$D_{2n} = \{\alpha \colon \mathbb{C} \to \mathbb{C} : \alpha(\Delta) = \Delta,\ |\alpha(x) - \alpha(y)| = |x - y|\ \forall x, y \in \mathbb{C}\},$$

d. h. D_{2n} ist die *Symmetriegruppe* des regelmäßigen n-Ecks.

Man nennt D_{2n} *Diedergruppe* der Ordnung $2n$.

Aufgabe I.21 $(1 + 1 + 1 + 1$ Punkte$)$**.**

(a) Konstruieren Sie Gruppen $U, V \leq G$ mit $UV \not\leq G$.

(b) Konstruieren Sie einen Gruppenhomomorphismus $f \colon G \to H$ mit $f(G) \not\trianglelefteq H$.

(c) Konstruieren Sie Gruppen $N \trianglelefteq M \trianglelefteq G$ mit $N \not\trianglelefteq G$.

(d) Zeigen Sie, dass A_4 keine Untergruppe der Ordnung 6 besitzt.

Aufgabe I.22 $(2 + 2 + 2 + 2 + 2 + 2$ Punkte$)$**.** Sei G eine Gruppe und $g \in G$. Zeigen Sie:

(a) Die Abbildung $\alpha_g \colon G \to G,\ x \mapsto gxg^{-1}$ ist ein Automorphismus. Man nennt α_g den von g induzierten *inneren Automorphismus*.

(b) Die Abbildung $\alpha \colon G \to \mathrm{Aut}(G),\ g \mapsto \alpha_g$ ist ein Homomorphismus. Man nennt $\mathrm{Inn}(G) := \alpha(G) \leq \mathrm{Aut}(G)$ die *innere Automorphismengruppe* von G.

(c) Es gilt $G/\mathrm{Z}(G) \cong \mathrm{Inn}(G)$.

(d) Ist $G/\mathrm{Z}(G)$ zyklisch, so ist G abelsch (d. h. $G/\mathrm{Z}(G) = 1$).

(e) Es gilt $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$. Man nennt $\mathrm{Out}(G) := \mathrm{Aut}(G)/\mathrm{Inn}(G)$ die *äußere Automorphismengruppe*.

(f) Für $H \leq G$ ist $\mathrm{N}_G(H)/\mathrm{C}_G(H)$ zu einer Untergruppe von $\mathrm{Aut}(H)$ isomorph.

Aufgabe I.23 (2 Punkte)**.** Zeigen Sie, dass jede Gruppe der Ordnung 220 einen Normalteiler der Ordnung 55 besitzt.
Hinweis: Konstruieren Sie zunächst einen kleineren Normalteiler und verwenden Sie anschließend den zweiten Isomorphiesatz.

Aufgabe I.24 (2 Punkte)**.** Zeigen Sie, dass die 2-Sylowgruppen von S_4 zu D_8 isomorph sind.
Hinweis: Untersuchen Sie die Operation von D_8 auf der Menge der vierten Einheitswurzeln (siehe Aufgabe I.20).

Aufgabe I.25 $(2 + 2$ Punkte$)$**.** Seien $H \leq G$ Gruppen mit $n := |G : H| < \infty$. Zeigen Sie:

(a) $|G : H_G| \leq n!$ mit der Bezeichnung aus Aufgabe I.17.

(b) Ist G endlich und n der kleinste Primteiler von $|G|$, so ist $H \trianglelefteq G$ (dies verallgemeinert Beispiel I.3.17(iii)).

Hinweis: Untersuchen Sie die Operation von G auf G/H (Bemerkung I.4.6(i)).

Aufgabe I.26 (2 + 2 + 2 + 2 + 2 + 2 Punkte)**.** Sei G eine nichtabelsche Gruppe der Ordnung 8. Zeigen Sie:

(a) G besitzt ein Element x der Ordnung 4.
Hinweis: Aufgabe I.18.

(b) Für $y \in G \setminus \langle x \rangle$ gilt $y^4 = 1$ und $yx = x^{-1}y$.

(c) Die Multiplikationstabelle von G ist durch die Ordnung von y eindeutig bestimmt.

(d) Im Fall $y^2 = 1$ ist $G \cong D_8$.

(e) Im Fall $y^2 \neq 1$ ist

$$G \cong Q_8 := \left\langle \begin{pmatrix} \mathrm{i} & 0 \\ 0 & -\mathrm{i} \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right\rangle \leq \mathrm{GL}(2, \mathbb{C})$$

mit $\mathrm{i} = \sqrt{-1}$. Man nennt Q_8 *Quaternionengruppe* der Ordnung 8.
Hinweis: Es genügt zu zeigen, dass Q_8 die gewünschten Eigenschaften hat.

(f) Konstruieren Sie alle Gruppen der Ordnung 8 bis auf Isomorphie.
Hinweis: Zeigen Sie $D_8 \ncong Q_8$, indem Sie Elemente der Ordnung 2 zählen.

Aufgabe I.27 (3 Punkte)**.** Wie viele Würfel mit einfarbigen Seitenflächen gibt es, wenn fünf Farben zur Verfügung stehen?
Hinweis: Beachten Sie, dass sich gespiegelte Würfel unterscheiden lassen.

Aufgabe I.28 (2 Punkte)**.** Bestimmen Sie alle abelschen Gruppen der Ordnung 720 bis auf Isomorphie.

Aufgabe I.29 (2 + 2 Punkte)**.**

(a) Sei G eine endliche abelsche Gruppe. Zeigen Sie, dass eindeutig bestimmte Zahlen $d_1, \ldots, d_n \in \mathbb{N} \setminus \{1\}$ mit $G \cong C_{d_1} \times \ldots \times C_{d_n}$ und $d_1 \mid d_2 \mid \ldots \mid d_n$ existieren.

(b) Sei $N \trianglelefteq G \cong C_{q_1} \times \ldots \times C_{q_n}$ mit Primzahlpotenzen $q_1, \ldots, q_n$. Zeigen Sie, dass Teiler $r_i \mid q_i$ für $i = 1, \ldots, n$ existieren mit $G/N \cong C_{r_1} \times \ldots \times C_{r_n}$.

Aufgabe I.30 (1 + 1 + 1 + 1 Punkte)**.** Zeigen Sie, dass alle Gruppen der Ordnungen $40, 42, 45, 56$ auflösbar sind.

Aufgabe I.31 (2 + 2 + 2 Punkte)**.** Für eine Gruppe G und $x, y \in G$ nennt man $[x, y] := xyx^{-1}y^{-1}$ den *Kommutator* von x und y. Außerdem ist

$$G' := \langle [x, y] : x, y \in G \rangle$$

die *Kommutatorgruppe* von G. Mit $G^{(0)} := G$ sei $G^{(n+1)} := (G^{(n)})'$ für $n \geq 0$. Zeigen Sie:

(a) Aus $G' \subseteq H \leq G$ folgt $H \trianglelefteq G$ und G/H ist abelsch.
Hinweis: Betrachten Sie zunächst den Fall $G' = H$ und verwenden Sie für den allgemeinen Fall den zweiten Isomorphiesatz.

(b) Ist $N \trianglelefteq G$ mit abelscher Faktorgruppe G/N, so gilt $G' \leq N$. (Daher ist G' der „kleinste“ Normalteiler mit abelscher Faktorgruppe.)

(c) Sei nun $|G| < \infty$. Genau dann ist G auflösbar, wenn ein $n \in \mathbb{N}$ mit $G^{(n)} = 1$ existiert.
Hinweis: Argumentieren Sie durch Induktion nach $|G|$.

Aufgabe I.32 $(2 + 2$ Punkte$)$**.** Für eine endliche Gruppe G und einen Primteiler p von $|G|$ sei

$$\Omega := \{(x_1, \ldots, x_p) \in G^p : x_1 \ldots x_p = 1\}.$$

(a) Zeigen Sie, dass $\mathbb{Z}/p\mathbb{Z}$ auf Ω operiert durch

$$^{k+p\mathbb{Z}}(x_1, \ldots, x_p) := (x_{1+k}, \ldots, x_{p+k}),$$

wobei die Indizes modulo p zu lesen sind.

(b) (McKay) Benutzen Sie die Bahnengleichung, um den Satz von Cauchy abzuleiten.

Aufgabe I.33 (2 Punkte)**.** Zeigen Sie $\mathrm{Aut}(S_3) \cong S_3$.

Aufgabe I.34 (2 Punkte)**.** (Landau) Sei $n \in \mathbb{N}$. Zeigen Sie, dass es nur endlich viele endliche Gruppen G mit $k(G) = n$ gibt.
Hinweis: Zeigen Sie, dass die Klassengleichung in der Form $1 = \frac{1}{|\mathrm{C}_G(x_1)|} + \ldots + \frac{1}{|\mathrm{C}_G(x_n)|}$ nur endlich viele Lösungen besitzt.

Aufgabe I.35 (3 Punkte)**.** Zeigen Sie, dass die Potenzmenge $\mathcal{P}(\Omega)$ einer endlichen Menge Ω mit der *symmetrischen Differenz*

$$A \ominus B := (A \cup B) \setminus (A \cap B) \qquad (A, B \subseteq \Omega)$$

zu einer Gruppe wird und bestimmen Sie deren Isomorphietyp.

Ringtheorie

Aufgabe I.36 (2 Punkte)**.** Zeigen Sie, dass jeder endliche Integritätsbereich ein Körper ist.

Aufgabe I.37 $(2 + 2 + 2 + 2$ Punkte$)$**.** Sei R ein Ring und $I, J \trianglelefteq R$. Zeigen Sie:

(a) $I \cap J \trianglelefteq R$.

(b) $I + J := \{x + y : x \in I,\, y \in J\} \trianglelefteq R$.

(c) $IJ := \left\{\sum_{i=1}^{k} x_i y_i : k \in \mathbb{N},\, x_i \in I,\, y_i \in J\right\} \trianglelefteq R$.

(d) $IJ \subseteq I \cap J \subseteq I + J$.

Aufgabe I.38 $(2 + 2$ Punkte$)$**.** Sei R ein Ring mit Teilring $S \subseteq R$ und $I, J \trianglelefteq R$ mit $I \subseteq J$. Beweisen Sie:

(a) $S + I$ ist ein Teilring von R, $I \trianglelefteq S + I$, $S \cap I \trianglelefteq S$ und $S/(S \cap I) \cong (S + I)/I$.

(b) $J/I \trianglelefteq R/I$ und $(R/I)/(J/I) \cong R/J$.

Hinweis: Verwenden Sie den Homomorphiesatz.

Aufgabe I.39 $(2+2+2$ Punkte$)$**.** Sei K ein Körper und $n \in \mathbb{N}$. Zeigen Sie:

(a) Die oberen Dreiecksmatrizen bilden einen Teilring R von $K^{n\times n}$.

(b) Die oberen Dreiecksmatrizen mit Nullen auf der Hauptdiagonale bilden ein Ideal I von R.

(c) Es existiert ein Ringisomorphismus $R/I \cong K^n$.

Aufgabe I.40 $(2+2+2+2$ Punkte$)$**.** Sei R ein Integritätsbereich.

(a) Zeigen Sie, dass
$$(x,y) \sim (x',y') :\Longleftrightarrow xy' = x'y$$
eine Äquivalenzrelation auf $R \times (R \setminus \{0\})$ definiert. Sei $[x,y]$ die Äquivalenzklasse von (x,y).

(b) Zeigen Sie, dass $Q(R) := \{[x,y] : x,y \in R,\ y \neq 0\}$ mit den Verknüpfungen
$$[a,b] + [c,d] := [ad+bc, bd],$$
$$[a,b] \cdot [c,d] := [ac, bd]$$
zu einem Körper wird. Man nennt $Q(R)$ den *Quotientenkörper* von R.

(c) Zeigen Sie, dass die Abbildung $R \to Q(R)$, $x \mapsto [x,1]$ ein Ringmonomorphismus ist. Auf diese Weise kann man R als Teilring von $Q(R)$ auffassen.

(d) (Universelle Eigenschaft) Für jeden Körper K und jeden Ringmonomorphismus $f\colon R \to K$ existiert genau ein Körperhomomorphismus $g\colon Q(R) \to K$ mit $g([x,1]) = \alpha(x)$ für $x \in R$, d. h. g setzt f fort. Daher ist $Q(R)$ der „kleinste“ Körper, der R enthält.

Bemerkung: Dies verallgemeinert die Konstruktion von $\mathbb{Q}$ aus $\mathbb{Z}$.

Aufgabe I.41 $(2+2$ Punkte$)$**.**

(a) Schreiben Sie $(\mathbb{Z}/2200\mathbb{Z})^\times$ als direktes Produkt zyklischer Gruppen von Primzahlpotenzordnung.

(b) Bestimmen Sie alle Erzeuger von $(\mathbb{Z}/22\mathbb{Z})^\times$.

Aufgabe I.42 $(1+3$ Punkte$)$**.**

(a) Bestimmen Sie die Periodenlänge in der Dezimalbruchentwicklung von $1/22$ und $1/23$.

(b) Sei $n \in \mathbb{N}$ mit $\mathrm{ggT}(n,10) = 1$. Zeigen Sie, dass die Periodenlänge $\rho(n)$ in der Dezimalbruchdarstellung von $1/n$ genau die Ordnung von $10 + n\mathbb{Z}$ in $(\mathbb{Z}/n\mathbb{Z})^\times$ ist. Folgern Sie $\rho(n) \mid \varphi(n)$.

Bemerkung: Eine offene Vermutung von Gauß besagt, dass es unendlich viele Primzahlen p mit $\rho(p) = p-1$ gibt.

Aufgabe I.43 $(2+2+2+2$ Punkte$)$**.** Sei $1 \neq n \in \mathbb{N} \setminus \mathbb{P}$ mit $a^{n-1} \equiv 1 \pmod{n}$ für alle $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a,n) = 1$. Zeigen Sie:

(a) (Korselt) Für jeden Primteiler p von n gilt $n \equiv 1 \pmod{p-1}$.
Hinweis: Die Gleichung $a^{n-1} \equiv 1 \pmod{n}$ beschränkt die Ordnung der Elemente in $(\mathbb{Z}/n\mathbb{Z})^\times$.

(b) n ist ungerade und quadratfrei.

(c) n besitzt mindestens drei Primteiler.

(d) Es gibt ein solches n. Man nennt n CARMICHAEL-Zahl.

Bemerkung: Die Umkehrung vom „kleinen Fermat“ (Folgerung I.7.18) ist also falsch. Trotzdem ist das ein brauchbarer Primzahltest.

Aufgabe I.44 (2 Punkte)**.** Beweisen Sie, dass die Automorphismengruppe von $(\mathbb{Z}, +)$ zu C_2 isomorph ist.

Aufgabe I.45 (2 Punkte)**.** (*Universelle Eigenschaft* des Polynomrings) Sei $\varphi\colon R \to S$ ein Homomorphismus kommutativer Ringe R, S und $s \in S$. Zeigen Sie, dass φ genau eine Fortsetzung $\hat{\varphi}\colon R[X] \to S[X]$ mit $\hat{\varphi}(X) = s$ besitzt.

Aufgabe I.46 $(2 + 2$ Punkte)**.** Sei K ein Körper und $\alpha \in K[X]$.

(a) Beschreiben Sie $(K[X]/(\alpha))^\times$.

(b) Berechnen Sie $(X^3 + X + 1 + (\alpha))^{-1}$ in $\mathbb{F}_2[X]/(\alpha)$ für $\alpha = X^4 + X^2 + 1 \in \mathbb{F}_2[X]$ (falls das Inverse existiert).

Aufgabe I.47 $(2 + 2 + 2 + 2$ Punkte)**.** Untersuchen Sie, welche der folgenden Polynome irreduzibel in $\mathbb{Q}[X]$ sind:

(a) $X^3 - 2X^2 - 18X + 15$

(b) $X^3 + \frac{2}{3}X^2 + \frac{1}{3}X + 1$

(c) $X^4 + 4X^2 + X + 6$

(d) $X^5 + 20X + 16$
Hinweis: Eisenstein.

Aufgabe I.48 $(2 + 3$ Punkte)**.** (a) Zeigen Sie, dass $(2, X)$ kein Hauptideal in $\mathbb{Z}[X]$ ist und bestimmen Sie $\mathbb{Z}[X]/(2, X)$.

(b) Beweisen oder widerlegen Sie: $\mathbb{Z}[X]/(X^2 - 1) \cong \mathbb{Z}^2$.

Aufgabe I.49 $(2 + 2$ Punkte)**.** Zeigen Sie, dass

$$R := \left\{ a + b\frac{1 + \sqrt{-3}}{2} : a, b \in \mathbb{Z} \right\}$$

ein Teilring von $\mathbb{C}$ ist und bestimmen Sie $R^\times$.
Bemerkung: Die Elemente von R heißen *Eisenstein-Zahlen*.

Aufgabe I.50 (2 Punkte)**.** Zeigen Sie, dass

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

als Teilring von $\mathbb{C}^{2\times 2}$ ein nicht-kommutativer Schiefkörper ist. Man nennt $\mathbb{H}$ nach HAMILTON den *Quaternionenschiefkörper* (vgl. Aufgabe I.26).

Aufgabe I.51 (2 Punkte)**.** Sei $n \in \mathbb{N}$ und $d \mid n$. Zeigen Sie, dass $(\mathbb{Z}/n\mathbb{Z})^\times \to (\mathbb{Z}/d\mathbb{Z})^\times$, $k+n\mathbb{Z} \mapsto k+d\mathbb{Z}$ ein wohldefinierter Gruppenepimorphismus ist.

Aufgabe I.52 (2 Punkte)**.** Sei $2 < p \in \mathbb{P}$ und $a \in \mathbb{Z}$ mit $(\mathbb{Z}/p^2\mathbb{Z})^\times = \langle a + p^2\mathbb{Z}\rangle$. Zeigen Sie $(\mathbb{Z}/p^n\mathbb{Z})^\times = \langle a + p^n\mathbb{Z}\rangle$ für alle $n \geq 2$.

Körpertheorie

Aufgabe I.53 ($2+2$ Punkte)**.** Zeigen Sie $\mathrm{Aut}(\mathbb{Q}) = \{\mathrm{id}_\mathbb{Q}\}$ und $\mathrm{Aut}(\mathbb{R}) = \{\mathrm{id}_\mathbb{R}\}$.
Hinweis: Die zweite Aussage folgt aus der ersten, wenn Sie zeigen können, dass jeder Automorphismus stetig ist. Benutzen Sie dafür, dass jede positive reelle Zahl eine reelle Quadratwurzel besitzt.

Aufgabe I.54 (4 Punkte)**.** Entscheiden Sie, welche der folgenden Zahlen algebraisch über $\mathbb{Q}$ sind

$$\sqrt[5]{1+\sqrt{2}},\ e^{3\pi i/5},\ \sqrt{2}+\sqrt[3]{5},\ \pi^2\mathrm{i}.$$

Hinweis: Sie dürfen die Transzendenz von π benutzen.

Weihnachtsrätsel (+3 Zusatzpunkte)**.** Bestimmen Sie ohne Computer die 42. Nachkommastelle von

$$\left(\sqrt{2}+\sqrt{3}\right)^{666}.$$

Hinweis: Man kann Beispiel I.10.12 verwenden, aber es geht auch elementar.

Aufgabe I.55 ($2+2+2+2+2+2$ Punkte)**.** Nach Beispiel I.10.10 bildet der Zerfällungskörper K von X^3-2 eine Galois-Erweiterung über $\mathbb{Q}$.

(a) Bestimmen Sie $|K : \mathbb{Q}|$.

(b) Bestimmen Sie $G := \mathrm{Gal}(K|\mathbb{Q})$.

(c) Bestimmen Sie alle Untergruppen von G.

(d) Bestimmen Sie alle Teilkörper von K.

(e) Welche Teilkörper von K bilden Galois-Erweiterungen über $\mathbb{Q}$?

(f) Finden Sie ein $x \in K$ mit $K = \mathbb{Q}(x)$.

Bemerkung: Das ist die algebraische Version einer Kurvendiskussion.

Aufgabe I.56 (2 Punkte)**.** Zeigen Sie, dass die Körper $\mathbb{Q}(\sqrt{2})$ und $\mathbb{Q}(\sqrt{3})$ nicht isomorph sind.

Aufgabe I.57 (2 Punkte)**.** Sei K ein Körper mit $\operatorname{char} K \neq 2$ oder $|K| < \infty$. Zeigen Sie, dass jede Körpererweiterung vom Grad 2 über K eine Galois-Erweiterung ist.

Aufgabe I.58 (2 + 2 Punkte)**.** Sei K ein Körper und $\alpha \in K[X]$. Die *k-te Ableitung* $\alpha^{(k)}$ ist induktiv definiert durch $\alpha^{(0)} := \alpha$ und $\alpha^{(k)} := (\alpha^{(k-1)})'$. Zeigen Sie für $\alpha, \beta \in K[X]$ und $x \in K$:

(a) $(\alpha(\beta))' = \alpha'(\beta)\beta'$ (Kettenregel).

(b) $\alpha = \sum_{k=0}^{\infty} \frac{\alpha^{(k)}(x)}{k!}(X - x)^k$, falls $\operatorname{char} K = 0$ (Taylorreihe).

Aufgabe I.59 (4 Punkte)**.** Konstruieren Sie $\mathbb{F}_9$ und geben Sie die entsprechenden Verknüpfungstabellen an.

Aufgabe I.60 (2 + 2 + 2 Punkte)**.** Sei $p \in \mathbb{P}$, $k, n \in \mathbb{N}$ und $q := p^k$.

(a) Bestimmen Sie die Ordnungen von $\mathrm{GL}(n, \mathbb{F}_q)$ und $\mathrm{SL}(n, \mathbb{F}_q)$.
Hinweis: Eine quadratische Matrix ist genau dann invertierbar, wenn ihre Zeilen linear unabhängig sind.

(b) Zeigen Sie, dass die oberen Dreiecksmatrizen mit Einsen auf der Hauptdiagonale eine p-Sylowgruppe P_n von $\mathrm{SL}(n, \mathbb{F}_q)$ bilden. Ist auch $P_n \in \mathrm{Syl}_p(\mathrm{GL}(n, \mathbb{F}_q))$?

(c) Zeigen Sie $|\mathrm{Syl}_p(\mathrm{SL}(2, \mathbb{F}_p))| = p + 1$.
Hinweis: Der Normalisator von P_2 enthält Diagonalmatrizen.

Aufgabe I.61 (2 + 2 Punkte)**.** Sei $I_d(p)$ die Anzahl der irreduziblen Polynome vom Grad d über $\mathbb{F}_p$. Leiten Sie eine Formel für $I_d(p)$ her, indem Sie Möbius-Inversion (Satz I.2.42) auf Lemma I.11.17 anwenden. Berechnen Sie damit $I_{12}(2)$.

Aufgabe I.62 (2 + 2 + 2 Punkte)**.** Sei $K := \mathbb{F}_2(X)$ der Körper der rationalen Funktionen über $\mathbb{F}_2$. Sei L ein Zerfällungskörper von $Y^2 - X$ über $K[Y]$. Zeigen Sie:

(a) Der Frobenius-Homomorphismus auf K ist nicht surjektiv.

(b) $|L : K| = 2$.

(c) $K \subseteq L$ ist keine Galois-Erweiterung.

Aufgabe I.63 (2 + 2 + 2 Punkte)**.**

(a) Zeigen Sie, dass jedes irreduzible Polynom in $\mathbb{R}[X]$ Grad 1 oder 2 hat.

(b) Berechnen Sie das Kreisteilungspolynom Φ_{15}.

(c) Zeigen Sie $\Phi_{2n}(X) = \Phi_n(-X)$ für jede ungerade Zahl $n > 1$.

Aufgabe I.64 (3 Punkte)**.** Bestimmen Sie alle Teilkörper von $\mathbb{Q}_{15}$ mit Grad 2 über $\mathbb{Q}$.

Aufgabe I.65 (3 Punkte)**.** Konstruieren Sie eine Galois-Erweiterung $\mathbb{Q} \subseteq K$ mit $\mathrm{Gal}(K|\mathbb{Q}) \cong C_7$.
Hinweis: Es genügt die Angabe eines primitiven Elements. Benutzen Sie dafür den Beweis von Satz 12.18.

Aufgabe I.66 (3 Punkte)**.** Sei K ein Körper mit algebraischem Abschluss $\overline{K}$. Seien $K \subseteq L$ und $K \subseteq M$ Galois-Erweiterungen mit $L, M \subseteq \overline{K}$. Zeigen Sie, dass L und M genau dann K-isomorph sind, wenn $L = M$.
Bemerkung: Im Fall $K \in \{\mathbb{Q}, \mathbb{R}, \mathbb{F}_p\}$ kann man „K-isomorph“ durch „isomorph“ ersetzen, denn $\mathrm{Aut}(K) = 1$.

Aufgabe I.67 (2 Punkte)**.** Schreiben Sie das symmetrische Polynom

$$X^2Y^2 + X^2Z^2 + Y^2Z^2 + 1$$

als Polynom elementarsymmetrischer Polynome.

Aufgabe I.68 (3 Punkte)**.** Sei $\alpha \in \mathbb{Z}[X]$ normiert. Zeigen Sie, dass D_α kongruent zu 0 oder 1 modulo 4 ist.
Hinweis: Für die Nullstellen $x_1, \ldots, x_n \in \mathbb{C}$ von α gilt $D_\alpha = \prod_{i<j}\big((x_i + x_j)^2 - 4x_ix_j\big)$.

Aufgabe I.69 (3 Punkte)**.** Seien $x, y, z \in \mathbb{C}$ die Nullstellen von $X^3 + 2X^2 - 3X + 1 \in \mathbb{Q}[X]$. Berechnen Sie $x^3 + y^3 + z^3$.
Hinweis: Man braucht dafür nicht x, y, z zu berechnen.

Aufgabe I.70 (3 Punkte)**.** Lösen Sie das nicht-lineare Gleichungssystem

$$\begin{aligned} x + y + z &= 3, \\ x^2 + y^2 + z^2 &= 15, \\ x^3 + y^3 + z^3 &= 45. \end{aligned}$$

Aufgabe I.71 (2 + 2 Punkte)**.** Sei K ein Körper und $G \leq K^\times$ mit $n := |G| < \infty$. Sei $d \mid n$.

(a) Zeigen Sie mit Hilfe von Satz I.8.29, dass G höchstens $\varphi(d)$ Elemente der Ordnung d besitzt.

(b) Folgern Sie mit Hilfe von Beispiel I.2.43, dass G zyklisch ist.

Bemerkung: Dies ist ein elementarer Beweis von Satz I.8.31.

Aufgabe I.72 (2 + 2 Punkte)**.**

(a) Bestimmen Sie die Galoisgruppe von $X^4 - X^3 + 1$.

(b) Konstruieren Sie ein Polynom $\alpha \in \mathbb{Q}[X]$ mit $\mathrm{Gal}(\alpha) \cong A_4$.

Aufgabe I.73 (2 + 2 + 2 + 2 Punkte)**.**

(a) Zeigen Sie, dass jeder konstruierbare Punkt $z \in \mathbb{C}$ Nullstelle eines auflösbaren Polynoms in $\mathbb{Q}[X]$ ist.

(b) Seien $n, m \in \mathbb{N}$ teilerfremd, sodass die regelmäßigen n- und m-Ecke konstruierbar sind. Zeigen Sie ohne Verwendung von Satz I.15.11, dass das mn-Eck konstruierbar ist.

(c) Drücken Sie $\cos(\frac{2\pi}{2^n})$ für $n \in \mathbb{N}$ durch rationale Zahlen, Grundrechenarten und Quadratwurzeln aus. *Hinweis:* Dies ist möglich, da das regelmäßige 2^n-Eck konstruierbar ist.

(d) Begründen Sie, warum sich $\cos(2\pi/7)$ durch rationale Zahlen, Grundrechenarten, Quadratwurzeln und kubischen Wurzeln ausdrücken lässt.

Algebra II

1 Mengenlehre

Bemerkung II.1.1. In der linearen Algebra beweist man die Existenz von Basen für endlich erzeugte Vektorräume. In Satz I.13.14 haben den algebraischen Abschluss für abzählbare Körper konstruiert. Um diese und andere Aussagen ohne Endlichkeitsbedingung beweisen zu können, benötigt man Varianten des Auswahlaxioms aus der Mengenlehre.

Satz II.1.2 (Cantor-Bernstein[1])**.** *Seien A und B Mengen mit injektiven Abbildungen $f\colon A \to B$ und $g\colon B \to A$. Dann sind A und B gleichmächtig.*

Beweis. Wir definieren $C_0 := A \setminus g(B)$ und $C_n := g(f(C_{n-1}))$ für $n \geq 1$. Weiter sei $C := \bigcup_{n=0}^{\infty} C_n$ und $h\colon A \to B$ mit

$$h(x) := \begin{cases} f(x) & \text{falls } x \in C, \\ g^{-1}(x) & \text{falls } x \notin C. \end{cases}$$

Im Fall $x \notin C$ ist $x \notin C_0$, d. h. $x \in g(B)$. Folglich ist $g^{-1}(x)$ durch die Injektivität von g eindeutig bestimmt und h ist wohldefiniert. Seien nun $x, y \in A$ mit $h(x) = h(y)$. Nehmen wir $x \in C$ und $y \notin C$ an. Dann ist $f(x) = g^{-1}(y)$ und $g(f(x)) = y$. Sei $x \in C_n$ für ein $n \geq 0$. Dann folgt der Widerspruch $y = g(f(x)) \in g(f(C_n)) = C_{n+1} \subseteq C$. Also gilt $x, y \in C$ oder $x, y \notin C$ und man erhält $x = y$. Somit ist h injektiv.

Sei nun $y \in B$ beliebig. Im Fall $g(y) \notin C$ ist $h(g(y)) = g^{-1}(g(y)) = y$. Sei also $g(y) \in C_n$ für ein $n \geq 1$. Es existiert dann ein $x \in C_{n-1}$ mit $g(f(x)) = g(y)$. Aus der Injektivität von g folgt $h(x) = f(x) = y$. Also ist h auch surjektiv und bijektiv. □

Definition II.1.3. Sei $\leq$ eine Ordnungsrelation (reflexiv, transitiv und antisymmetrisch) auf einer Menge A und $B \subseteq A$.

(i) Wie üblich benutzen wir die Schreibweisen $a \geq a'$ (falls $a' \leq a$), $a < a'$ (falls $a \leq a' \neq a$) und $a > a'$ (falls $a' \leq a \neq a'$) für $a, a' \in A$.

(ii) Ein $b \in B$ heißt

- *größtes Element* von B, falls $\forall b' \in B : b' \leq b$.
- *maximales Element* von B, falls $\nexists b' \in B : b < b'$.

(iii) Ein $a \in A$ heißt *obere Schranke* von B, falls $\forall b \in B : b \leq a$. Analog definiert man *kleinstes Element*, *minimales Element* und *untere Schranke*.

(iv) Man nennt A *total geordnet* (oder *Kette*), falls $\forall a, a' \in A : (a \leq a' \vee a' \leq a)$.[2]

(v) Man nennt A *wohlgeordnet*, falls jede nichtleere Teilmenge von A ein kleinstes Element enthält.

[1] auch Schröder-Bernstein-Satz genannt, siehe [A. Hinkis, *Proofs of the Cantor-Bernstein Theorem*, Springer, Heidelberg, 2013]

[2] Ist A endlich, so lassen sich die Elemente in einer „Kette“ anordnen $A = \{a_1 < \ldots < a_n\}$.

Beispiel II.1.4. Die Teilbarkeitsrelation $\mid$ auf $A := \{1, \dots, 10\}$ ist eine Ordnungsrelation. Wegen $\mathrm{kgV}(A) > 10$ besitzt A kein größtes Element. Andererseits sind $6, \dots, 10$ die maximalen Elemente von A. Schließlich ist 6 die einzige obere Schranke von $B := \{2, 3\}$. Wegen $2 \nmid 3 \nmid 2$ ist A nicht total geordnet. Da B kein kleinstes Element besitzt, ist A auch nicht wohlgeordnet.

Bemerkung II.1.5.

(i) Im Allgemeinen existieren weder größte Elemente, noch maximale Elemente, noch obere Schranken. Größte Elemente sind maximal und eindeutig, wenn sie existieren. Wohlgeordnete Mengen sind stets total geordnet. Endliche total geordnete Mengen sind wohlgeordnet.

(ii) Im Folgenden benutzen wir das *Auswahlaxiom*: Ist $(M_i)_{i \in I}$ eine Familie von nichtleeren Mengen, so ist auch das kartesische Produkt $\bigtimes_{i \in I} M_i$ nichtleer.

Satz II.1.6 (Zorns Lemma)**.** *Sei M eine geordnete Menge, in der jede total geordnete Teilmenge eine obere Schranke besitzt. Dann enthält M ein maximales Element.*

Beweis (Weston). Da die leere Teilmenge eine obere Schranke besitzt, ist M selbst nicht leer. Nach dem Auswahlaxiom existiert eine Funktion f, die jeder nichtleeren Teilmenge $N \subseteq M$ ein Element $f(N) \in N$ zuordnet. Für jede total geordnete Teilmenge $N \subseteq M$ sei $\hat{N}$ die Menge der oberen Schranken von N in $M \setminus N$ ($\hat{N} = \varnothing$ ist möglich). Ein solches N heißt *speziell*, falls für alle $A \subseteq N$ gilt

$$f(\hat{A}) \text{ ist minimal in } \hat{A} \cap N \text{ oder } \hat{A} \cap N = \varnothing.$$

Wir zeigen, dass die Vereinigung N_0 aller speziellen Teilmengen total geordnet ist. Für $x, y \in N_0$ existieren spezielle Teilmengen $N_1, N_2 \subseteq M$ mit $x \in N_1$ und $y \in N_2$. Im Fall $x \in N_2$ gilt $x \leq y$ oder $y \leq x$, da N_2 total geordnet ist. Sei also $x \notin N_2$ und

$$A := \{a \in N_1 \cap N_2 : a < x\}.$$

Da N_1 speziell ist und $x \in \hat{A} \cap N_1$, ist $f(\hat{A}) \in N_1$ und $f(\hat{A}) \leq x$. Im Fall $\hat{A} \cap N_2 \neq \varnothing$ wäre analog $f(\hat{A}) \in N_2$ und man hätte den Widerspruch $f(\hat{A}) \in A \cap \hat{A} = \varnothing$. Daher gilt $y \notin \hat{A}$ und es existiert ein $a \in A$ mit $y < a < x$, da N_2 total geordnet ist.

Nun beweisen wir, dass N_0 speziell ist. Sei dafür $A \subseteq N_0$ mit $\hat{A} \cap N_0 \neq \varnothing$. Dann existiert eine spezielle Teilmenge $N \subseteq N_0$ mit $f(\hat{A})$ minimal in $\hat{A} \cap N$. Wäre $f(\hat{A})$ nicht minimal in $\hat{A} \cap N_0$, so existiert $x \in \hat{A} \cap N_0$ mit $x < f(\hat{A})$. Man könnte aber N mit $x \in N$ wählen und erhält auf diese Weise einen Widerspruch. Also ist N_0 speziell. Jetzt nehmen wir $\hat{N_0} \neq \varnothing$ an und betrachten die total geordnete Menge

$$N_1 := N_0 \cup \{f(\hat{N_0})\}.$$

Sei $A \subseteq N_1$ mit $\hat{A} \cap N_1 \neq \varnothing$. Im Fall $\hat{A} \cap N_0 \neq \varnothing$ ist $f(\hat{A})$ minimal in $\hat{A} \cap N_0$ und auch in $\hat{A} \cap N_1$. Sei daher $\hat{A} \cap N_0 = \varnothing$, $f(\hat{N_0}) \in \hat{A}$ und $A \subseteq N_0$. Dann existiert für jedes $x \in N_0$ ein $a \in A$ mit $x < a$, da N_0 total geordnet ist. Es folgt $\hat{A} \subseteq \hat{N_0} \subseteq \hat{A}$. Also ist $f(\hat{A}) = f(\hat{N_0})$ minimal in $\{f(\hat{N_0})\} = \hat{N_0} \cap N_1 = \hat{A} \cap N_1$. Somit ist N_1 speziell im Widerspruch zur Konstruktion von N_0. Dies zeigt $\hat{N_0} = \varnothing$. Nach Voraussetzung existiert eine obere Schranke $m \in M$ von N_0. Dabei gilt $m \in N_0$ und m ist die einzige obere Schranke von N_0. Also ist m maximal in M. □

Bemerkung II.1.7. Man kann zeigen, dass Zorns Lemma äquivalent zum Auswahlaxiom ist. Das Gleiche gilt für den *Wohlordnungssatz*: Jede Menge kann wohlgeordnet werden. Außerdem gilt Zorns Lemma auch in der dualen Version für untere Schranken und minimale Elemente, indem man $\leq$ durch $\geq$ ersetzt.

Beispiel II.1.8. Sei F eine (endliche) Menge von Frauen und M eine Menge von Männern. Für $f \in F$ sei $M_f \subseteq M$ die Menge der Freunde von f. Damit jede Frau f einen Partner in M_f findet, muss offenbar $|\bigcup_{e\in E} M_e| \geq |E|$ für alle $E \subseteq F$ gelten (Monogamie vorausgesetzt). Der nächste Satz zeigt, dass diese Bedingung sogar hinreichend ist.

Satz II.1.9 (Halls Heiratssatz)**.** *Sei $(M_i)_{i\in I}$ eine Familie von Teilmengen einer Menge M mit $|I| < \infty$ oder $\forall i \in I : |M_i| < \infty$. Genau dann existieren paarweise verschiedene $x_i \in M_i$ für $i \in I$, wenn $|\bigcup_{i\in J} M_i| \geq |J|$ für jede endliche Teilmenge $J \subseteq I$ gilt.*

Beweis. Für $J \subseteq I$ schreiben wir $M_J := \bigcup_{i\in J} M_i$. Nehmen wir an, dass paarweise verschiedene $x_i \in M_i$ existieren (man nennt $(x_i)_{i\in I}$ ein *Vertretersystem*). Offenbar ist dann $|M_J| \geq |\{x_i : i \in J\}| = |J|$ für jede endliche Teilmenge $J \subseteq I$. Sei umgekehrt die Bedingung

$$|M_J| \geq |J| \qquad (J \subseteq I,\ |J| < \infty) \tag{II.1.1}$$

erfüllt. Wir unterscheiden zwei Fälle:

Fall 1: $|I| < \infty$.
Induktion nach $n := |I|$: Der Fall $n \leq 1$ ist offensichtlich. Sei also $n > 1$ und o. B. d. A. $I = \{1, \ldots, n\}$. Eine Teilmenge $J \subseteq I$ heißt *kritisch*, falls $1 \leq |M_J| = |J| < n$ gilt.

Nehmen wir zunächst an, dass keine kritischen Teilmengen existieren. Wegen $|M_1| = |M_{\{1\}}| \geq 1$ existiert ein $x_1 \in M_1$. Für $i \in J := \{2, \ldots, n\}$ sei $N_i := M_i \setminus \{x_1\}$. Für jede Teilmenge $K \subseteq J$ gilt dann $|N_K| \geq |M_K| - 1 \geq |K|$, denn K ist nicht kritisch. Also erfüllt $(N_i)_{i\in J}$ Bedingung (II.1.1) und nach Induktion existiert ein Vertretersystem $(x_i)_{i\in J}$ von $(N_i)_{i\in J}$. Sicher ist dann $(x_i)_{i\in I}$ ein Vertretersystem für $(M_i)_{i\in I}$.

Nehmen wir schließlich an, dass eine kritische Teilmenge $J \subseteq I$ existiert. Dann gilt $1 \leq m := |J| = |M_J| < n$. Nach Induktion besitzt $(M_i)_{i\in J}$ ein Vertretersystem $(x_i)_{i\in J}$. Für $i \in I \setminus J$ sei $N_i := M_i \setminus M_J$. Für jede Teilmenge $K \subseteq I \setminus J$ gilt dann

$$|N_K| = |M_K \setminus M_J| = |M_{K\cup J}| - |M_J| \geq |K \cup J| - m = |K| + |J| - m = |K|,$$

d. h. $(N_i)_{i\in I\setminus J}$ erfüllt (II.1.1). Nach Induktion existiert ein Vertretersystem $(x_i)_{i\in I\setminus J}$. Nach Konstruktion ist dann $(x_i)_{i\in I}$ ein Vertretersystem für $(M_i)_{i\in I}$.

Fall 2: $\forall i \in I : |M_i| < \infty$.
Sei $\mathcal{M}$ die Menge aller Familien $(N_i)_{i\in I}$ mit $N_i \subseteq M_i$ (für alle $i \in I$), für die (II.1.1) gilt. Wegen $(M_i)_{i\in I} \in \mathcal{M}$ ist $\mathcal{M}$ nichtleer und durch

$$(N_i)_{i\in I} \leq (N'_i)_{i\in I} :\Longleftrightarrow \forall i \in I : N_i \subseteq N'_i$$

geordnet. Sei $\varnothing \neq \mathcal{N} \subseteq \mathcal{M}$ eine total geordnete Teilmenge und $K_j := \bigcap_{(N_i)_{i\in I}\in\mathcal{N}} N_j$ für $j \in I$. Dann ist $(K_i)_{i\in I} \leq (N_i)_{i\in I}$ für alle $(N_i)_{i\in I} \in \mathcal{N}$. Sei $J \subseteq I$ eine endliche Teilmenge und $j \in J$. Wegen $|M_j| < \infty$ existiert eine endliche Teilmenge $\mathcal{N}_1 \subseteq \mathcal{N}$ mit

$$K_j = \bigcap_{(N_i)_{i\in I}\in\mathcal{N}_1} N_j$$

für alle $j \in J$. Da $\mathcal{N}$ total geordnet ist, besitzt $\mathcal{N}_1$ ein kleinstes Element $(N_i)_{i\in I}$. Offenbar ist dann $(K_j)_{j\in J} = (N_j)_{j\in J}$. Insbesondere ist $|K_J| = |N_J| \geq |J|$. Dies zeigt, dass $(K_i)_{i\in I}$ Bedingung (II.1.1) erfüllt und somit eine untere Schranke von $\mathcal{N}$ in $\mathcal{M}$ ist. Nach Zorns Lemma existiert ein minimales

Element $(N_i)_{i\in I} \in \mathcal{M}$. Da jedes Vertretersystem von $(N_i)_{i\in I}$ auch ein Vertretersystem von $(M_i)_{i\in I}$ ist, können wir $(M_i)_{i\in I}$ durch $(N_i)_{i\in I}$ ersetzen und $\mathcal{M} = \{(M_i)_{i\in I}\}$ annehmen.

Sei $x \in M_I$ und $N_i := M_i \setminus \{x\}$ für $i \in I$. Wegen $(N_i)_{i\in I} \notin \mathcal{M}$ existiert eine endliche Teilmenge $J \subseteq I$ mit $|M_J| - 1 \leq |N_J| < |J| \leq |M_J|$. Es folgt $|M_J| = |J|$ und $x \in M_J$. Wir definieren nun

$$N_i := \begin{cases} M_i & \text{falls } i \in J, \\ M_i \setminus M_J & \text{falls } i \in I \setminus J. \end{cases}$$

Sei $K \subseteq I$ endlich. Dann gilt

$$\begin{aligned} |N_K| &= |N_{K\cap J} \cup N_{K\setminus J}| = |M_{K\cap J}| + |M_{K\setminus J} \setminus M_J| \\ &= |M_{K\cap J}| + |M_{K\cup J}| - |M_J| \geq |K \cap J| + |K \cup J| - |J| = |K|. \end{aligned}$$

Dies zeigt $(N_i)_{i\in I} \in \mathcal{M} = \{(M_i)_{i\in I}\}$ und $M_i \cap M_J = \varnothing$ für $i \in I \setminus J$. Es folgt $M_{I\setminus J} \cap M_J = \varnothing$. Nach Fall 1 existieren paarweise verschiedene $x_i \in M_i$ für $i \in J$. Setzt man nun

$$N_i := \begin{cases} \{x_i\} & \text{falls } i \in J, \\ M_i & \text{falls } i \in I \setminus J, \end{cases}$$

so erfüllt $(N_i)_{i\in I}$ wieder (II.1.1). Also gilt $M_i = \{x_i\}$ für $i \in J$. Da x beliebig gewählt war, gilt sogar $|M_i| = 1$ für alle $i \in I$. Offenbar sind die M_i auch paarweise disjunkt und die Behauptung folgt. □

Bemerkung II.1.10. Satz II.1.9 gilt nicht für $|I| = \infty$, wenn nicht alle M_i endlich sind: Wähle $I := \mathbb{N} =: M_1$ und $M_i := \{i - 1\}$ für $i \geq 2$.

2 Anwendungen von Zorns Lemma

Bemerkung II.2.1. Im Folgenden sei V ein Vektorraum über einem Körper K. Eine Teilmenge $S \subseteq V$ heißt *linear abhängig*, falls paarweise verschiedene $s_1, \ldots, s_n \in S$ ($n \in \mathbb{N}$) und $\lambda_1, \ldots, \lambda_n \in K^\times$ mit $\sum_{i=1}^n \lambda_i s_i = 0$ existieren. Anderenfalls heißt S *linear unabhängig*. Eine linear unabhängige Teilmenge $B \subseteq V$ heißt *Basis* von V, falls

$$V = \sum_{b \in B} Kb =: \operatorname{Span}_K B =: \langle B \rangle.$$

Der folgende Satz wird in der linearen Algebra nur für endlich erzeugte Vektorräume bewiesen.

Satz II.2.2 (Basisergänzungssatz)**.** *Sei V ein Vektorraum mit Erzeugendensystem $E \subseteq V$ und linear unabhängiger Teilmenge $U \subseteq E$. Dann existiert eine Basis B von V mit $U \subseteq B \subseteq E$. Insbesondere besitzt jeder Vektorraum eine Basis.*[1]

Beweis. Die Menge $\mathcal{M}$ aller linear unabhängigen Teilmengen $M \subseteq V$ mit $U \subseteq M \subseteq E$ ist wegen $U \in \mathcal{M}$ nichtleer und durch $\subseteq$ geordnet. Sei $\varnothing \neq \mathcal{N} \subseteq \mathcal{M}$ eine total geordnete Teilmenge. Dann ist $U \subseteq W := \bigcup_{M \in \mathcal{N}} M \subseteq E$. Sei $\sum_{i=1}^n \lambda_i w_i = 0$ mit $\lambda_1, \ldots, \lambda_n \in K$ und $w_1, \ldots, w_n \in W$ paarweise verschieden. Dann existieren $M_1, \ldots, M_n \in \mathcal{N}$ mit $w_i \in M_i$ für $i = 1, \ldots, n$. Da $\mathcal{N}$ total geordnet ist, können wir $M_1 \subseteq M_2 \subseteq \ldots \subseteq M_n$ annehmen. Insbesondere ist $w_1, \ldots, w_n \in M_n$. Da M_n linear unabhängig ist, folgt $\lambda_1 = \ldots = \lambda_n = 0$. Daher ist $W \in \mathcal{M}$ eine obere Schranke von $\mathcal{N}$. Nach Zorns Lemma besitzt $\mathcal{M}$ ein maximales Element B. Nach Definition von $\mathcal{M}$ ist B linear unabhängig. Für $e \in E \setminus B$ ist $B \cup \{e\}$ linear abhängig, denn $B \subsetneq B \cup \{e\} \subseteq E$. Also ist $e \in \langle B \rangle$ und $V = \langle E \rangle \subseteq \langle B \rangle$. Dies zeigt, dass B eine Basis von V ist. Die zweite Aussage folgt, indem man $U = \varnothing$ und $E = V$ wählt. □

Folgerung II.2.3. *Jeder Unterraum U eines Vektorraums V besitzt ein* Komplement $W \leq V$*, d. h.* $V = U \oplus W$.

Beweis. Nach Satz II.2.2 lässt sich eine Basis C von U zu einer Basis B von V ergänzen. Die Behauptung folgt dann mit $W := \langle B \setminus C \rangle$. □

Satz II.2.4. *Je zwei Basen eines Vektorraums sind gleichmächtig.*

Beweis. Seien B und C Basen eines Vektorraums V. Für jedes $b \in B$ existiert dann eine endliche Teilmenge $C_b \subseteq C$ mit $b \in \langle C_b \rangle$. Also gilt $V = \langle B \rangle \subseteq \langle \bigcup_{b \in B} C_b \rangle$ und $\bigcup_{b \in B} C_b = C$, da C ein minimales Erzeugendensystem von V ist. Sei $B_1 \subseteq B$ eine endliche Teilmenge und $C_1 := \bigcup_{b \in B_1} C_b$. Dann ist B_1 eine linear unabhängige Teilmenge im Vektorraum $U := \langle C_1 \rangle$ mit $\dim U = |C_1| < \infty$. Aus der linearen Algebra folgt $|B_1| \leq |C_1|$. Nach dem Heiratssatz existieren paarweise verschiedene $c_b \in C_b$ für $b \in B$. Die Abbildung $B \to C$, $b \mapsto c_b$ ist also injektiv. Aus Symmetriegründen muss es auch eine injektive Abbildung $C \to B$ geben und die Behauptung folgt mit Cantor-Bernstein. □

[1] In der Funktionalanalysis spricht man von *Hamelbasen*.

Bemerkung II.2.5. Die Mächtigkeit einer Basis eines Vektorraums V nennt man wie üblich *Dimension* von V. Nach Satz II.2.4 hängt dies nicht von der Wahl der Basis ab. Wir zeigen später, dass obige Sätze auch für „Vektorräume“ über Schiefkörpern gelten (Satz II.9.10).

Beispiel II.2.6. Für jeden Körper K hat der Polynomring $K[X]$ als K-Vektorraum die abzählbare Basis $1, X, X^2, \ldots$. Daher ist $\dim K[X] = \aleph_0$. Andererseits gilt $\dim_{\mathbb{Q}} \mathbb{R} > \aleph_0$.

Satz II.2.7 (Krull)**.** *Sei R ein Ring und $I \lhd R$ ein echtes Ideal. Dann existiert ein maximales Ideal M von R mit $I \subseteq M$. Insbesondere besitzt jeder Ring $R \neq \{0\}$ ein maximales Ideal.*

Beweis. Die Menge $\mathcal{M}$ aller Ideale $J \lhd R$ mit $I \subseteq J$ ist wegen $I \in \mathcal{M}$ nicht leer und durch $\subseteq$ geordnet. Sei $\varnothing \neq \mathcal{N} \subseteq \mathcal{M}$ total geordnet. Dann ist $0 \in I \subseteq \cup_{N \in \mathcal{N}} N =: J$. Für $x, y \in J$ existieren $X, Y \in \mathcal{N}$ mit $x \in X$ und $y \in Y$. Da $\mathcal{N}$ total geordnet ist, gilt o. B. d. A. $X \subseteq Y$. Sicher ist dann $x - y, ax, xa \in Y \subseteq J$ für alle $a \in R$. Dies zeigt $J \trianglelefteq R$. Für alle $N \in \mathcal{N}$ gilt $1 \notin N$, denn anderenfalls wäre $R = R1 \subseteq N$. Also ist $1 \notin J$ und $J \in \mathcal{M}$ ist eine obere Schranke von $\mathcal{N}$. Nach Zorn besitzt $\mathcal{M}$ ein maximales Element M. Es gilt dann $I \subseteq M \lhd R$. Ist $M \subsetneq L \trianglelefteq R$, so ist $L \notin \mathcal{M}$ und man erhält $L = R$. Daher ist M ein maximales Ideal. Die zweite Aussage folgt, indem man $I = \{0\}$ wählt. □

Bemerkung II.2.8. In Definition I.14.14 haben wir den Polynomring $K[X_1, \ldots, X_n]$ über einem Körper K in endlich vielen Unbekannten $X_1, \ldots, X_n$ definiert. Ist I eine beliebige Indexmenge, so definieren wir

$$K[X_i : i \in I] := \bigcup_{\substack{J \subseteq I \\ |J| < \infty}} K[X_j : j \in J].$$

Jedes Element von $K[X_i : i \in I]$ ist ein Polynom in endlich vielen Unbekannten. Daher ist $K[X_i : i \in I]$ (immer noch) ein Ring. Wir beweisen im Folgenden die Existenz und Eindeutigkeit des algebraischen Abschlusses eines beliebigen Körpers (vgl. Satz I.13.14).

Satz II.2.9. *Jeder Körper K besitzt einen algebraischen Abschluss.*

Beweis. Sei $R := K[X_\alpha : \alpha \in K[X] \setminus K]$ und

$$I := (\alpha(X_\alpha) : \alpha \in K[X] \setminus K) \trianglelefteq R.$$

Nehmen wir $I = R$ an. Dann existieren $\alpha_1, \ldots, \alpha_n \in K[X] \setminus K$ und $\beta_1, \ldots, \beta_n \in R$ mit

$$1 = \beta_1 \alpha_1(X_{\alpha_1}) + \ldots + \beta_n \alpha_n(X_{\alpha_n}) \in I. \tag{II.2.1}$$

Nach Kronecker existiert ein Zerfällungskörper L von $\alpha_1 \ldots \alpha_n$. Seien $x_1, \ldots, x_n \in L$ mit $\alpha_i(x_i) = 0$ für $i = 1, \ldots, n$. Ersetzt man jedes X_{α_i} in (II.2.1) durch x_i, so erhält man den Widerspruch $1 = 0$ in L. Daher ist $I \neq R$. Nach Krull existiert ein maximales Ideal $M \lhd R$ mit $I \subseteq M$. Nach Satz I.7.12 ist $K_1 := R/M$ ein Körper und die kanonische Abbildung $\Gamma\colon K \to K_1$, $a \mapsto a + M$ ist ein Körperhomomorphismus. Da Γ nach Lemma I.8.41 injektiv ist, können wir K durch $\Gamma(K)$ ersetzen und somit $K \subseteq K_1$ annehmen. Für $\alpha \in K[X] \setminus K$ sei $x_\alpha := X_\alpha + M \in K_1$. Wegen

$$\alpha(x_\alpha) = \alpha(X_\alpha + M) = \alpha(X_\alpha) + M \in (I + M)/M = 0$$

besitzt jedes α eine Nullstelle in K_1. Außerdem sind die x_α algebraisch über K. Da jedes Element in K_1 die Form

$$\sum_{i_1,\dots,i_n\geq 0} a_{i_1,\dots,i_n} X_{\alpha_1}^{i_1}\dots X_{\alpha_n}^{i_n} + M = \sum_{i_1,\dots,i_n\geq 0} a_{i_1,\dots,i_n} x_{\alpha_1}^{i_1}\dots x_{\alpha_n}^{i_n} \qquad (\alpha_1,\dots,\alpha_n \in K[X]\setminus K)$$

hat, ist die Erweiterung $K \subseteq K_1$ nach Satz I.13.4 algebraisch. Das gleiche Argument mit K_1 anstelle von K liefert eine algebraische Erweiterung $K_1 \subseteq K_2$, sodass jedes Polynom in $K_1[X]\setminus K_1$ eine Nullstelle in K_2 besitzt. Auf diese Weise erhält man Körper $K \subseteq K_1 \subseteq K_2 \subseteq \dots$ und definiert

$$\overline{K} := \bigcup_{n=1}^{\infty} K_n$$

(vgl. Satz I.13.14). Offenbar ist $\overline{K}$ ein Körper und $K \subseteq \overline{K}$ ist algebraisch nach Lemma I.13.2. Jedes Polynom in $\overline{K}[X]\setminus\overline{K}$ hat Koeffizienten in einem K_n und besitzt daher eine Nullstelle in $K_{n+1} \subseteq \overline{K}$. Also ist $\overline{K}$ algebraisch abgeschlossen.[2] □

Satz II.2.10. *Sei $K \subseteq L$ eine algebraische Körpererweiterung und S ein algebraisch abgeschlossener Körper. Dann lässt sich jeder Homomorphismus $K \to S$ zu einem Homomorphismus $L \to S$ fortsetzen.*

Beweis. Sei $\sigma\colon K \to S$ ein Homomorphismus. Sei $\mathcal{M}$ die Menge aller Paare (M,τ), wobei M ein Körper mit $K \subseteq M \subseteq L$ ist und $\tau\colon M \to S$ ein Homomorphismus mit Einschränkung $\tau_K = \sigma$. Wegen $(K,\sigma) \in \mathcal{M}$ ist $\mathcal{M} \neq \varnothing$. Durch

$$(M,\tau) \leq (M',\tau') \;:\Longleftrightarrow\; M \subseteq M',\ \tau'_M = \tau$$

ist $\mathcal{M}$ geordnet. Sei $\varnothing \neq \mathcal{N} \subseteq \mathcal{M}$ total geordnet. Wie üblich ist dann $N := \bigcup_{(M,\tau)\in\mathcal{N}} M$ ein Körper mit $K \subseteq N \subseteq L$. Für jedes $x \in N$ existiert ein $(M,\tau) \in \mathcal{N}$ mit $x \in M$. Wir definieren $\gamma(x) := \tau(x)$. Ist auch $(M',\tau') \in \mathcal{N}$ mit $x \in M'$, so gilt o. B. d. A. $(M,\tau) \leq (M',\tau')$ und $\tau'(x) = \tau'_M(x) = \tau(x)$. Daher hängt $\gamma\colon N \to S$ nicht von der Wahl von (M,τ) ab. Für $x,y \in N$ existiert analog $(M,\tau) \in \mathcal{N}$ mit $x,y \in M$. Es gilt dann

$$\gamma(x \mathbin{\dot{+}} y) = \tau(x \mathbin{\dot{+}} y) = \tau(x) \mathbin{\dot{+}} \tau(y) = \gamma(x) \mathbin{\dot{+}} \gamma(y).$$

Also ist γ ein Homomorphismus mit $\gamma_K = \sigma$. Folglich ist (N,τ) eine obere Schranke von $\mathcal{N}$. Nach Zorn existiert ein maximales Element $(K',\sigma') \in \mathcal{M}$.

Annahme: $K' \neq L$.
Sei $x \in L \setminus K'$ mit Minimalpolynom $\mu \in K'[X]$ (beachte: $K \subseteq L$ ist algebraisch). Da S algebraisch abgeschlossen ist, besitzt $\sigma'(\mu) \in S[X]$ eine Nullstelle in S. Nach dem Fortsetzungssatz kann man σ' zu $\tau\colon K'(x) \to S$ fortsetzen. Dann wäre aber $(K'(x),\tau) \in \mathcal{M}$ im Widerspruch zur Wahl von (K',σ'). Also ist $K' = L$ und $\sigma'\colon L \to S$ ist eine Fortsetzung von σ. □

Folgerung II.2.11. *Je zwei algebraische Abschlüsse eines Körpers K sind K-isomorph.*

Beweis. Seien S_1, S_2 algebraische Abschlüsse von K. Nach Satz II.2.10 lässt sich die Inklusionsabbildung $K \hookrightarrow S_2$ zu einem Monomorphismus $\sigma\colon S_1 \to S_2$ fortsetzen (Lemma I.8.41). Jedes $x \in S_2$ ist Nullstelle seines Minimalpolynoms $\mu \in K[X]$. Nun zerfällt μ im algebraisch abgeschlossenen Körper S_1 und σ bildet diese Nullstellen auf die Nullstellen von $\sigma(\mu) = \mu$ ab. Daher ist $x \in \sigma(S_1)$ und σ ist ein K-Isomorphismus. □

[2] Nach Satz II.3.16 ist K_1 bereits algebraisch abgeschlossen.

3 Separable Erweiterungen

Bemerkung II.3.1. Wir haben in den Sätzen I.12.2 und I.12.3 gesehen, dass Zerfällungskörper in Charakteristik 0 stets Galois-Erweiterungen sind und primitive Elemente besitzen. Nach Artin ist dies allgemeiner für vollkommene Körper richtig (vgl. Aufgabe I.57). Wir zeigen in diesem Kapitel, dass eine beliebige Körpererweiterung $K \subseteq L$ stets einen Zwischenkörper besitzt, der sich wie eine Erweiterung über einem vollkommenen Körper verhält.

Definition II.3.2. Sei $K \subseteq L$ eine Körpererweiterung.

- Ein irreduzibles Polynom $\alpha \in K[X]$ heißt *separabel*, falls $\alpha' \neq 0$.
- Ein algebraisches Element $a \in L$ heißt *separabel* über K, falls sein Minimalpolynom separabel ist. Anderenfalls heißt a *inseparabel* über K.
- Die Erweiterung $K \subseteq L$ heißt *separabel*, wenn jedes $a \in L$ separabel über K ist. Anderenfalls heißt $K \subseteq L$ *inseparabel*. Sind alle $a \in L \setminus K$ inseparabel über K, so heißt die Erweiterung *rein inseparabel*.

Beispiel II.3.3.

(i) Jedes $a \in K$ ist separabel über K, denn das Minimalpolynom $X - a$ hat Ableitung 1. Achtung: Die triviale Erweiterung $K \subseteq K$ ist sowohl separabel als auch rein inseparabel.

(ii) Jede separable (oder rein inseparable) Erweiterung ist algebraisch. Daher ist $\mathbb{Q} \subseteq \mathbb{C}$ inseparabel.

(iii) Ist $K \subseteq L$ separabel (oder rein inseparabel), so auch $K \subseteq M$ für alle Teilkörper $M \subseteq L$, die K enthalten.

(iv) Nach Satz I.11.20 ist jede algebraische Erweiterung eines vollkommenen Körpers separabel. Wie dort zeigt man, dass ein irreduzibles $\alpha \in K[X]$ im Allgemeinen genau dann separabel ist, wenn α in einem Zerfällungskörper keine mehrfachen Nullstellen besitzt. Dies benutzen wir im Folgenden.

(v) Nach Aufgabe I.62 ist $\alpha := Y^2 - X \in \mathbb{F}_2(X)[Y]$ irreduzibel, aber nicht separabel, denn $\alpha' = 2Y = 0$.

Satz II.3.4. *Sei $K \subseteq L$ eine endliche, separable Körpererweiterung. Dann gilt:*

(i) Es existiert eine Galois-Erweiterung $K \subseteq M$ mit $L \subseteq M$.

(ii) Es existiert ein $x \in L$ mit $L = K(x)$ (Satz vom primitiven Element).

Beweis.

(i) Sei $x_1, \ldots, x_n$ eine K-Basis von L. Seien $\mu_1, \ldots, \mu_n \in K[X]$ die (separablen) Minimalpolynome von $x_1, \ldots, x_n$ über K. O. B. d. A. seien $\mu_1, \ldots, \mu_k$ paarweise verschieden und $\{\mu_1, \ldots, \mu_k\} = \{\mu_1, \ldots, \mu_n\}$. Wegen $\mathrm{ggT}(\mu_i, \mu_j) = 1$ für $1 \leq i < j \leq k$ hat $\alpha = \mu_1 \ldots \mu_k \in K[X]$ paarweise verschiedene Nullstellen in einem Zerfällungskörper M. Nach Artin ist $K \subseteq M$ eine Galois-Erweiterung mit $L = K(x_1, \ldots, x_n) \subseteq M$.

(ii) Sei M wie in (i). Nach dem Hauptsatz der Galois-Theorie existieren nur endlich viele Körper $L_1, \ldots, L_m$ mit $K \subseteq L_i \subsetneq L$ für $i = 1, \ldots, m$. Nach Lemma I.10.1 existiert ein $x \in L \setminus \bigcup_{i=1}^m L_i$. Sicher ist dann $K(x) = L$. □

Lemma II.3.5. *Sei $K \subseteq L$ eine Körpererweiterung mit $p := \operatorname{char} K > 0$ und $a \in L$ algebraisch über K. Genau dann ist $a \in L$ separabel über K, wenn $K(a) = K(a^p)$ gilt.*

Beweis. In jedem Fall ist $K(a^p) \subseteq K(a)$. Sei a separabel mit Minimalpolynom $\mu \in K[X]$. Das Minimalpolynom $\nu \in K(a^p)[X]$ von a über $K(a^p)$ ist ein Teiler von μ und daher selbst separabel. Andererseits teilt ν auch $(X-a)^p \overset{I.11.10}{=} X^p - a^p \in K(a^p)[X]$. Dies zeigt $\nu = X - a$ und $a \in K(a^p)$. Also ist $K(a) = K(a^p)$.

Sei nun a inseparabel über K. Dann ist $\mu' = 0$ und daher

$$\mu = \sum_{k=0}^{n} a_k X^{pk} = \gamma(X^p) \qquad (a_i \in K)$$

für ein $\gamma \in K[X]$. Das Minimalpolynom von a^p über K teilt γ und es folgt

$$|K(a^p) : K| \leq \deg \gamma < \deg \mu = |K(a) : K|.$$

Also ist $K(a^p) \neq K(a)$. □

Satz II.3.6. *Galois-Erweiterungen sind separabel.*

Beweis. Sei $K \subseteq L$ eine Galois-Erweiterung und $a \in L$. O. B. d. A. sei $p := \operatorname{char} K > 0$. Nach dem Hauptsatz der Galois-Theorie ist auch $K(a^p) \subseteq L$ eine Galois-Erweiterung. Für $\sigma \in G := \operatorname{Gal}(L|K(a^p))$ ist

$$(\sigma(a) - a)^p \overset{I.11.10}{=} \sigma(a)^p - a^p = \sigma(a^p) - a^p = a^p - a^p = 0$$

und $\sigma(a) = a$. Dies zeigt $K(a) \subseteq L^G = K(a^p) \subseteq K(a)$ nach Artin. Nach Lemma II.3.5 ist a separabel über K. □

Lemma II.3.7. *Sind $K \subseteq L$ und $L \subseteq M$ separable Körpererweiterungen, so auch $K \subseteq M$.*

Beweis. Nach Lemma I.13.2 ist $K \subseteq M$ algebraisch. Sei $x \in M$ und $\sum_{k=0}^n a_k X^k \in L[X]$ das (separable) Minimalpolynom von x über L. Dann ist x auch separabel über $K(a_0, \ldots, a_n) \subseteq L$. Nach dem Satz vom primitiven Element existiert $c \in L$ mit $K(a_0, \ldots, a_n) = K(c)$. Nach Lemma II.3.5 ist

$$K(c, x) = K(c)(x) = K(c^p)(x^p) = K(c^p, x^p).$$

Daher ist jedes Element aus $K(c, x)$ eine K-Linearkombination von p-ten Potenzen. Wie üblich besitzt $K(x)$ eine K-Basis der Form $1, x, \ldots, x^k$. Diese ergänzen wir zu einer K-Basis $x_1, \ldots, x_l$ von $K(c, x)$. Für ein beliebiges $b = \sum_{i=1}^l b_i x_i \in K(c, x)$ mit $b_1, \ldots, b_l \in K$ gilt dann $b^p = \sum_{i=1}^l b_i^p x_i^p$. Da jedes Element aus $K(c, x)$ eine Linearkombination von p-ten Potenzen ist, bilden auch $x_1^p, \ldots, x_l^p$ eine K-Basis von $K(c, x)$. Insbesondere sind $1, x^p, \ldots, x^{pk}$ linear unabhängig über K. Dies zeigt

$$|K(x^p) : K| \geq k + 1 = |K(x) : K| \geq |K(x^p) : K|$$

und $K(x^p) = K(x)$. Nach Lemma II.3.5 ist x separabel über K. □

Satz II.3.8. *Die separablen Elemente einer algebraischen Körpererweiterung $K \subseteq L$ bilden einen Teilkörper M von L mit $K \subseteq M$. Dabei ist $M \subseteq L$ rein inseparabel.*

Beweis. Sicher ist $K \subseteq M$. Seien $a, b \in M$ mit (separablen) Minimalpolynomen $\mu_a, \mu_b \in K[X]$. Dann hat

$$\mu := \frac{\mu_a \mu_b}{\mathrm{ggT}(\mu_a, \mu_b)} \in K[X]$$

paarweise verschiedene Nullstellen in einem Zerfällungskörper Z. Nach Artin ist Z eine Galois-Erweiterung mit $K(a, b) \subseteq Z$. Nach Satz II.3.6 ist $K \subseteq Z$ separabel. Daher sind auch $a \dot{+} b$ und a/b (falls $b \neq 0$) als Elemente von $K(a, b)$ separabel über K. Dies zeigt, dass M ein Teilkörper von L ist.

Nehmen wir nun an, dass ein $x \in L \setminus M$ separabel über M ist. Wie oben ist dann $M \subseteq M(x)$ separabel und nach Lemma II.3.7 ist auch $K \subseteq M(x)$ separabel. Dies liefert den Widerspruch $x \in M$. Daher ist $M \subseteq L$ rein inseparabel. □

Definition II.3.9. In der Situation von Satz II.3.8 nennt man M den *separablen Abschluss* von K in L.[1] Außerdem heißt $|L : K|_s := |M : K|$ *Separabilitätsgrad* von L über K.

Satz II.3.10. *Sei L ein Körper und G eine endliche Untergruppe von $\mathrm{Aut}(L)$. Dann ist $L^G \subseteq L$ eine Galois-Erweiterung mit Galoisgruppe G.*

Beweis. Sei $K := L^G$ und $x \in L$. Sei $\{x_1, \ldots, x_n\}$ die Bahn von x unter G. Dann ist x eine Nullstelle von $\alpha := \prod_{i=1}^{n} (X - x_i) \in K[X]$. Insbesondere ist $|K(x) : K| \leq n \leq |G|$. Das Minimalpolynom von x ist als Teiler von α separabel über K. Wir wählen x, sodass $|K(x) : K|$ möglichst groß ist. Angenommen es existiert $y \in L \setminus K(x)$. Nach Satz II.3.8 ist $K \subseteq K(x, y)$ endlich und separabel. Nach dem Satz vom primitiven Element existiert $z \in L$ mit $K(x, y) = K(z)$ und $|K(z) : K| > |K(x) : K|$. Dies widerspricht der Wahl von x. Also ist $L = K(x)$ und $|L : K| \leq |G|$. Nach Satz I.10.6 ist umgekehrt $|G| \leq |\mathrm{Aut}(L|K)| \leq |L : K|$. Also ist $K \subseteq L$ eine Galois-Erweiterung mit $\mathrm{Gal}(L|K) = G$. □

Satz II.3.11. *Sei $p := \mathrm{char}\, K > 0$ und $\overline{K}$ ein algebraischer Abschluss von K. Dann ist*

$$\overline{K}_p := \{x \in \overline{K} : \exists n \in \mathbb{N} : x^{p^n} \in K\}$$

ein vollkommener Körper und $\overline{K}_p \subseteq \overline{K}$ ist separabel. Außerdem ist $K \subseteq \overline{K}_p$ rein inseparabel und jede rein inseparable Erweiterung L von K zu einem Teilkörper von $\overline{K}_p$ K-isomorph.

Beweis. Seien $x, y \in \overline{K}_p$ mit $x^{p^n}, y^{p^m} \in K$. O. B. d. A. sei $n \geq m$. Dann ist $(x \dot{+} y)^{p^n} = x^{p^n} \dot{+} y^{p^n} \in K$ und ebenso $(xy^{-1})^{p^n} \in K$ falls $y \neq 0$. Dies zeigt, dass $\overline{K}_p$ ein Teilkörper von $\overline{K}$ ist, der offenbar K enthält. Da $\overline{K}$ algebraisch abgeschlossen ist, besitzt $X^p - x$ eine Nullstelle $z \in \overline{K}$. Wegen $z^{p^{n+1}} = x^{p^n} \in K$ ist $z \in \overline{K}_p$. Also ist z ein Urbild von x unter dem Frobenius-Homomorphismus. Folglich ist $\overline{K}_p$ vollkommen und $\overline{K}_p \subseteq \overline{K}$ ist separabel. Sei nun $x \notin K$. Dann besitzt das Minimalpolynom von x über K als Teiler von $X^{p^n} - x^{p^n} = (X - x)^{p^n}$ nur eine Nullstelle bis auf Vielfachheit. Daher ist x inseparabel über K. Insgesamt ist $K \subseteq \overline{K}_p$ rein inseparabel.

Sei schließlich auch $K \subseteq L$ rein inseparabel (und damit algebraisch). Nach Satz II.2.10 lässt sich die Inklusionsabbildung $K \hookrightarrow \overline{K}$ zu einem Körperhomomorphismus $\Gamma\colon L \to \overline{K}$ fortsetzen. Wir können daher L durch $\Gamma(L)$ ersetzen. Es genügt dann $L \subseteq \overline{K}_p$ zu zeigen. Für $x \in L \setminus K$ ist $|K(x^p) : K| < |K(x) : K|$

[1] Ist L „der“ algebraische Abschluss von K, so nennt man M „den“ separablen Abschluss von K.

nach Lemma II.3.5. Durch Induktion nach $|K(x):K|$ können wir $x^p \in \overline{K}_p$ annehmen. Dann existiert ein $n \in \mathbb{N}$ mit $x^{p^{n+1}} = (x^p)^{p^n} \in K$, d. h. $x \in \overline{K}_p$. □

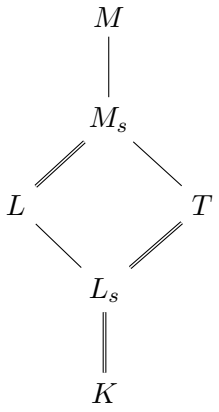
Folgerung II.3.12. *Der Grad einer endlichen rein inseparablen Körpererweiterung $K \subsetneq L$ ist eine Potenz von $p := \operatorname{char} K$.*

Beweis. Offenbar ist $p > 0$. Nach Satz II.3.11 können wir $L \subseteq \overline{K}_p$ annehmen. Für jedes $a \in L$ existiert dann ein $n \in \mathbb{N}$ mit $a^{p^n} \in K$. Das Minimalpolynom $\mu \in K[X]$ von a teilt daher $X^{p^n} - a^{p^n} = (X-a)^{p^n}$ und hat deshalb nur eine Nullstelle bis auf Vielfachheit. Für jeden Zwischenkörper $K \subseteq M \subseteq L$ ist das Minimalpolynom von a über M ein Teiler von μ und besitzt daher ebenfalls nur eine Nullstelle bis auf Vielfachheit. Insbesondere ist a auch inseparabel über M, falls $a \notin M$. Daher sind die Erweiterungen $K \subseteq M$ und $M \subseteq L$ rein inseparabel. Durch Induktion nach $|L:K|$ können wir mit dem Gradsatz annehmen, dass keine echten Zwischenkörper M existieren. Für $a \in L \setminus K$ ist dann $L = K(a)$. Nach Lemma II.3.5 ist $K(a^p) \subsetneq K(a)$, also $a^p \in K$. Das Minimalpolynom μ von a über K teilt daher $X^p - a^p$. Wegen $\mu' = 0$ ist andererseits $\deg \mu \geq p$. Dies zeigt $|L:K| = |K(a):K| = \deg \mu = p$. □

Satz II.3.13 (Gradsatz für $|L:K|_s$)**.** *Seien $K \subseteq L \subseteq M$ endliche Körpererweiterungen. Dann gilt*

$$\boxed{|M:K|_s = |M:L|_s |L:K|_s.}$$

Beweis. Wir können $p := \operatorname{char} K > 0$ annehmen, denn anderenfalls folgt die Behauptung aus dem Gradsatz. Seien L_s und M_s die separablen Abschlüsse von K in L bzw. von L in M. Sei T der separable Abschluss von L_s in M_s. Nach Lemma II.3.7 ist auch $K \subseteq T$ separabel. Sei $x \in M$ separabel über K. Dann ist x auch separabel über L und damit in M_s enthalten. Außerdem ist x auch separabel über L_s und daher in T enthalten. Dies zeigt, dass T der separable Abschluss von K in M ist. Es folgt



$$|M:K|_s = |T:K| = |T:L_s||L_s:K| = |T:L_s||L:K|_s.$$

Wir müssen also $|T:L_s| = |M:L|_s = |M_s:L|$ zeigen. Nach dem Satz vom primitiven Element existiert ein $x \in T$ mit $T = L_s(x)$. Das Minimalpolynom $\mu \in L_s[X]$ ist separabel. Sei $\nu \in L[X]$ ein irreduzibler Teiler von μ. Nach Vieta lassen sich die Koeffizienten von ν durch die Nullstellen (in einem Zerfällungskörper) ausdrücken. Da diese Nullstellen separabel über L_s sind, sind auch die Koeffizienten von ν separabel über L_s. Andererseits liegen die Koeffizienten von ν in L und $L_s \subseteq L$ ist rein inseparabel nach Satz II.3.8. Dies zeigt $\nu \in L_s[X]$ und es folgt $\nu = \mu$. Also ist

$$|T:L_s| = |L_s(x):L_s| = \deg \mu = \deg \nu = |L(x):L| \leq |M_s:L|.$$

Sei nun x ein primitives Element der separablen Erweiterung $L \subseteq M_s$, also $M_s = L(x)$. Da $T \subseteq M_s$ rein inseparabel ist, existiert nach Satz II.3.11 ein $n \in \mathbb{N}$ mit $y := x^{p^n} \in T$. Nach Lemma II.3.5 ist $L(x) = L(x^p) = \ldots = L(y)$. Mit dem gleichen Argument wie oben ist das Minimalpolynom von y über L_s auch irreduzibel in $L[X]$. Dies zeigt

$$|M_s:L| = |L(x):L| = |L(y):L| = |L_s(y):L_s| \leq |T:L_s|.$$ □

Bemerkung II.3.14.

(i) Sei I eine beliebige Indexmenge. Der Quotientenkörper von $K[X_i : i \in I]$ ist der Körper der rationalen Funktionen $K(X_i : i \in I)$ bestehend aus den Elementen α/β mit $\alpha, \beta \in K[X_i : i \in I]$ und $\beta \neq 0$ (Aufgabe I.40).

(ii) Sei $K \subseteq L$ eine Körpererweiterung und $S \subseteq L$ eine Teilmenge. Dann enthält $K(S)$ die Elemente $\alpha(S)/\beta(S)$ mit $\alpha, \beta \in K[X_s : s \in S]$ und $\beta(S) \neq 0$. Andererseits bilden diese Elemente selbst einen Teilkörper von L, der dann mit $K(S)$ übereinstimmen muss.

Beispiel II.3.15. Wir betrachten die Erweiterung

$$K := \mathbb{F}_2(X^2, Y^2) \subseteq \mathbb{F}_2(X, Y) =: L.$$

Nehmen wir $X \in K$ an. Dann existieren $\alpha, \beta \in \mathbb{F}_2[X, Y]$ mit $X = \frac{\alpha(X^2,Y^2)}{\beta(X^2,Y^2)}$. Es folgt $X\beta(X^2, Y^2) = \alpha(X^2, Y^2)$. Auf der linken Seite tritt X nur mit ungeraden Potenzen auf, auf der rechten Seite aber nur mit geraden Potenzen. Dieser Widerspruch zeigt $X \notin K$. Analog zeigt man $Y \notin K(X) = \mathbb{F}_2(X, Y^2)$. Daher ist

$$|L : K| = |L : K(X)||K(X) : K| = 4.$$

Für jedes $\alpha = \sum_{i,j\geq 0} a_{ij} X^i Y^j \in \mathbb{F}_2[X, Y]$ ist $\alpha^2 = \sum a_{ij}^2 X^{2i} Y^{2j} \in K$. Daher ist auch $a^2 \in K$ für alle $a \in L$. Im Fall $a \notin K$ ist $Z^2 - a^2 = (Z - a)^2 \in K[Z]$ das Minimalpolynom von a. Also ist $K \subseteq L$ rein inseparabel. Außerdem besitzt L kein primitives Element. Für $a \in K$ betrachten wir den Teilkörper $M_a := K(X + aY)$. Sicher ist $|M_a : K| \leq 2$. Sei $b \in K$ mit $M_a = M_b$. Im Fall $a \neq b$ wäre dann

$$Y = \frac{1}{a - b}\big(X + aY - X - bY\big) \in M_a$$

und $X = X + aY - aY \in M_a$. Dies liefert den Widerspruch $M_a = L$. Also gilt $M_a \neq M_b$ für $a \neq b$. Insbesondere besitzt $K \subseteq L$ unendlich viele Zwischenkörper (vgl. Aufgabe II.19).

Satz II.3.16. *Sei $K \subseteq L$ eine algebraische Körpererweiterung, sodass jedes Polynom in $K[X]$ eine Nullstelle in L besitzt. Dann ist L ein algebraischer Abschluss von K.*

Beweis. Jedes Polynom in $L[X]$ besitzt eine Nullstelle x in einem Zerfällungskörper. Nun ist x algebraisch über L und auch über K. Also ist x Nullstelle eines Polynoms in $K[X]$. Es genügt daher zu zeigen, dass jedes $\alpha \in K[X]$ über L in Linearfaktoren zerfällt. O. B. d. A. sei α irreduzibel.

Sei zunächst $K \subseteq L$ (und damit α) separabel. Nach Artin ist der Zerfällungskörper M von α eine Galois-Erweiterung und hat somit die Form $M = K(y)$ für ein $y \in M$. Das Minimalpolynom $\beta \in K[X]$ von y besitzt nach Voraussetzung eine Nullstelle $z \in L$. Nun hat man einen K-Isomorphismus

$$M = K(y) = K[X]/(\beta) \cong K(z).$$

Also zerfällt α auch in $K(z) \subseteq L$ wie gewünscht.

Sei nun $K \subseteq L$ inseparabel und $p := \operatorname{char} K$. Wie in Satz II.3.11 konstruieren wir den Körper

$$L_p := \{a \in L : \exists n \in \mathbb{N} : a^{p^n} \in K\}.$$

Sei $a \in L_p$ mit $a^{p^n} \in K$. Nach Voraussetzung besitzt $X^{p^{n+1}} - a^{p^n} \in K[X]$ eine Nullstelle $b \in L$. Wegen $(b^p - a)^{p^n} = 0$ ist $b \in L_p$ ein Urbild von a unter dem Frobenius-Homomorphismus. Also ist L_p

vollkommen und $L_p \subseteq L$ separabel. Nach dem ersten Teil des Beweises genügt es zu zeigen, dass jedes Polynom $\gamma = \sum_{k=0}^{n} c_k X^k \in L_p[X]$ eine Nullstelle in L besitzt. Es existiert $m \in \mathbb{N}$ mit

$$\gamma^m = \sum_{k=0}^{n} c_i^m X^{km} \in K[X].$$

Nach Voraussetzung besitzt γ^m eine Nullstelle in L, also auch γ. □

4 Transzendente Erweiterungen

Bemerkung II.4.1. Nach Satz I.13.4 besitzt jede Körpererweiterung $K \subseteq L$ einen Zwischenkörper $K \subseteq M \subseteq L$, sodass $K \subseteq M$ algebraisch ist und jedes $x \in L \setminus M$ transzendent ist über M. In diesem Abschnitt konstruieren wir mit Zorns Lemma einen Zwischenkörper $K \subseteq M' \subseteq L$ mit der umgekehrten Eigenschaft: $M' \subseteq L$ ist algebraisch und jedes $x \in M' \setminus K$ ist transzendent über K.

Definition II.4.2. Sei $K \subseteq L$ eine Körpererweiterung.

- Eine Teilmenge $S \subseteq L$ heißt *algebraisch unabhängig* über K, falls jedes $s \in S$ transzendent über $K(S \setminus \{s\})$ ist. Anderenfalls nennt man S *algebraisch abhängig* über K.
- Besitzt L ein über K transzendentes Element, so nennt man die Erweiterung $K \subseteq L$ *transzendent*. Ist sogar jedes $x \in L \setminus K$ transzendent über K, so heißt $K \subseteq L$ *absolut transzendent*. Existiert eine algebraisch unabhängige Teilmenge $S \subseteq L$ mit $L = K(S)$, so nennt man $K \subseteq L$ *rein transzendent*.
- Eine algebraisch unabhängige Teilmenge $S \subseteq L$ heißt *Transzendenzbasis* von L über K, falls die Erweiterung $K(S) \subseteq L$ algebraisch ist.

Beispiel II.4.3.

(i) Genau dann ist $\{a\}$ algebraisch unabhängig über K, wenn a transzendent über K ist. Nach Lindemann ist $\{\pi\}$ algebraisch unabhängig über $\mathbb{Q}$. Andererseits ist offen, ob $\{\pi, e\}$ algebraisch unabhängig über $\mathbb{Q}$ ist.

(ii) Ist S algebraisch unabhängig über K, so auch jede Teilmenge von S.

(iii) Die Erweiterung $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}, \pi)$ ist transzendent, aber nicht absolut transzendent.

(iv) Der Körper der rationalen Funktionen $K(X)$ ist rein transzendent über K mit Transzendenzbasis $\{X\}$ (vgl. Bemerkung I.9.3(iv)). Allerdings ist auch $\{X^2\}$ eine Transzendenzbasis mit $|K(X) : K(X^2)| = 2$.

(v) Jede algebraische Körpererweiterung besitzt nur die Transzendenzbasis $\varnothing$. Insbesondere ist die triviale Erweiterung $K \subseteq K$ rein transzendent.

Satz II.4.4 (Lindemann-Weierstrass)**.** *Genau dann sind $a_1, \ldots, a_n \in \overline{\mathbb{Q}}$ linear abhängig über $\mathbb{Q}$, wenn $e^{a_1}, \ldots, e^{a_n}$ algebraisch abhängig über $\mathbb{Q}$ sind.*

Beweis. Siehe Folgerung A.9.7. □

Bemerkung II.4.5. Satz II.4.4 sagt (vereinfacht), dass der Gruppenhomomorphismus $\exp\colon (\mathbb{C}, +) \to \mathbb{C}^\times$ linear abhängige Elemente auf algebraisch abhängige Elemente abbildet. Daraus erhält man die Transzendenz von e (mit $a_1 = 1$) und π (wäre π algebraisch, so auch $\pi\mathrm{i}$ und $e^{\pi\mathrm{i}} = -1$ wäre transzendent).

Lemma II.4.6. *Sei $K \subseteq L$ eine Körpererweiterung und $S \subseteq L$ eine Teilmenge. Genau dann ist S algebraisch unabhängig über K, wenn der Einsetzungshomomorphismus*

$$\begin{aligned} K[X_s : s \in S] &\to K(S), \\ \alpha &\mapsto \alpha(S) \end{aligned}$$

injektiv ist.

Beweis. Sei zunächst S algebraisch unabhängig und $\alpha \in K[X_s : s \in S]$ mit $\alpha(S) = 0$. Dann kommen nur endlich viele $s_1, \ldots, s_n \in S$ in $\alpha(S)$ vor. Die Gleichung $\alpha(S) = 0$ bedeutet, dass s_1 algebraisch über $K(s_2, \ldots, s_n) \subseteq K(S \setminus \{s_1\})$ ist. Daher muss $\alpha = 0$ gelten und der Einsetzungshomomorphismus ist injektiv.

Sei nun umgekehrt S algebraisch abhängig. Dann ist ein $s \in S$ algebraisch über $K(S \setminus \{s\})$. Sei also $\alpha \in K(S \setminus \{s\})[X] \setminus \{0\}$ mit $\alpha(s) = 0$. Multipliziert man α mit einem gemeinsamen Nenner seiner Koeffizienten, so kann man annehmen, dass diese Koeffizienten die Form $\alpha_i(s_1, \ldots, s_n)$ mit $s_1, \ldots, s_n \in S \setminus \{s\}$ und $\alpha_i \in K[X_1, \ldots, X_n]$ haben. Also existiert ein Polynom $\beta \in K[X_1, \ldots, X_{n+1}] \setminus \{0\}$ mit $\beta(s_1, \ldots, s_n, s) = 0$, d. h. der Einsetzungshomomorphismus ist nicht injektiv. □

Bemerkung II.4.7. Aus Lemma II.4.6 folgt, dass $S \subseteq L$ genau dann algebraisch unabhängig ist, wenn jede *endliche* Teilmenge von S algebraisch unabhängig ist. Ist dies der Fall, so setzt sich der Einsetzungshomomorphismus $K[X_s : s \in S] \to K(S)$ zu einem Isomorphismus $K(X_s : s \in S) \cong K(S)$ fort (universelle Eigenschaft des Quotientenkörpers, Aufgabe I.40). Dies entspricht der Aussage, dass jeder n-dimensionale Vektorraum über K zu K^n isomorph ist (lineare Algebra).

Beispiel II.4.8. Der Hauptsatz I.14.19 über symmetrische Polynome impliziert, dass die elementarsymmetrischen Polynome $\sigma_1, \ldots, \sigma_n$ als Teilmenge von $K(X_1, \ldots, X_n)$ algebraisch unabhängig über K sind. Für beliebige Polynome in $K(X_1, \ldots, X_n)$ kann man mit der Jacobi-Matrix der partiellen Ableitungen prüfen, ob eine Transzendenzbasis vorliegt (siehe Satz A.6.9).

Lemma II.4.9. *Jede rein transzendente Körpererweiterung ist absolut transzendent.*

Beweis. Sei $K \subseteq L$ eine rein transzendente Körpererweiterung und $S \subseteq L$ algebraisch unabhängig mit $L = K(S)$. Für $a \in L \setminus K$ existieren $s_1, \ldots, s_n \in S$ mit $a \in K(s_1, \ldots, s_n) = K(s_1, \ldots, s_{n-1})(s_n)$. Dabei sei n minimal gewählt. Dann existieren teilerfremde $\alpha, \beta \in K(s_1, \ldots, s_{n-1})[X]$ mit $a = \alpha(s_n)/\beta(s_n)$. Ist a algebraisch über K, so existieren $\lambda_0, \ldots, \lambda_k \in K$ mit $\lambda_k \neq 0$ und $\sum_{i=0}^{k} \lambda_i a^i = 0$, d. h.

$$\Big(\sum_{i=0}^{k} \lambda_i \alpha^i \beta^{k-i}\Big)(s_n) = \beta^k(s_n) \sum_{i=0}^{k} \lambda_i \Big(\frac{\alpha(s_n)}{\beta(s_n)}\Big)^i = 0.$$

Da s_n transzendent über $K(s_1, \ldots, s_{n-1}) \subseteq K(S \setminus \{s_n\})$ ist, gilt $\sum \lambda_i \alpha^i \beta^{k-i} = 0$. Es folgt

$$\beta \mid \lambda_{k-1} \alpha^{k-1} \beta + \ldots + \lambda_0 \beta^k = -\lambda_k \alpha^k.$$

Wegen $\mathrm{ggT}(\alpha, \beta) = 1$ ergibt sich $\beta \in K(s_1, \ldots, s_{n-1})$. Ein Gradvergleich von $\sum \lambda_i \alpha^i \beta^{k-i} = 0$ ergibt auch $\alpha \in K(s_1, \ldots, s_{n-1})$. Dies liefert $a = \alpha(s_n)/\beta(s_n) = \alpha/\beta \in K(s_1, \ldots, s_{n-1})$ im Widerspruch zur Wahl von n. □

Bemerkung II.4.10.

(i) Wir zeigen in Beispiel II.4.16, dass die Umkehrung von Lemma II.4.9 falsch ist.

(ii) Die folgenden Sätze zeigen, dass sich Transzendenzbasen wie Basen von Vektorräumen verhalten.

Lemma II.4.11. *Für eine Körpererweiterung $K \subseteq L$ und eine Teilmenge $S \subseteq L$ sind äquivalent:*

(1) S ist eine Transzendenzbasis von L über K.

(2) S ist algebraisch unabhängig über K und für jedes $a \in L \setminus S$ ist $S \cup \{a\}$ algebraisch abhängig über K.

(3) $K(S) \subseteq L$ ist algebraisch und für jedes $s \in S$ ist $K(S \setminus \{s\}) \subseteq L$ transzendent.

Beweis.

(1) $\Rightarrow$ (2): Nach Definition ist S algebraisch unabhängig und $K(S) \subseteq L$ ist algebraisch. Für $a \in L \setminus S$ ist a algebraisch über $K(S)$, d. h. $S \cup \{a\}$ ist algebraisch abhängig.

(2) $\Rightarrow$ (3): Sei $a \in L \setminus K(S) \subseteq L \setminus S$. Dann ist $S \cup \{a\}$ algebraisch abhängig. Nach Lemma II.4.6 existieren $s_1, \ldots, s_n \in S \cup \{a\}$ und $\alpha \in K[X_1, \ldots, X_n] \setminus \{0\}$ mit $\alpha(s_1, \ldots, s_n) = 0$. Da S algebraisch unabhängig ist, muss a in $\alpha(s_1, \ldots, s_n)$ auftauchen. Somit ist a algebraisch über $K(S)$ und $K(S) \subseteq L$ ist algebraisch. Für $s \in S$ ist s transzendent über $K(S \setminus \{s\})$, d. h. $K(S \setminus \{s\}) \subseteq L$ ist transzendent.

(3) $\Rightarrow$ (1): Wir müssen zeigen, dass S algebraisch unabhängig ist. Nehmen wir dazu an, dass $s \in S$ algebraisch über $K(S \setminus \{s\})$ ist. Dann ist $K(S \setminus \{s\}) \subseteq K(S)$ eine endliche Körpererweiterung und damit algebraisch. Dann wäre aber auch $K(S \setminus \{s\}) \subseteq L$ algebraisch nach Lemma I.13.2. □

Satz II.4.12 (Basisergänzungssatz)**.** *Sei $K \subseteq L$ eine Körpererweiterung mit algebraisch unabhängiger Teilmenge $U \subseteq L$ und $U \subseteq S \subseteq L$, sodass $K(S) \subseteq L$ algebraisch ist. Dann existiert eine Transzendenzbasis B von L über K mit $U \subseteq B \subseteq S$. Insbesondere besitzt jede Körpererweiterung eine Transzendenzbasis.*

Beweis. Die Menge

$$\mathcal{M} := \{U \subseteq M \subseteq S : M \text{ algebraisch unabhängig über } K\}$$

ist nichtleer und durch $\subseteq$ geordnet. Sei $\varnothing \neq \mathcal{N} \subseteq \mathcal{M}$ total geordnet und $N := \bigcup_{M \in \mathcal{N}} M \subseteq S$. Sei $N_1 \subseteq N$ eine endliche Teilmenge. Da $\mathcal{N}$ total geordnet ist, existiert ein $M \in \mathcal{N}$ mit $N_1 \subseteq M$. Mit M ist dann auch N_1 algebraisch unabhängig über K. Nach Bemerkung II.4.7 ist auch N algebraisch unabhängig über K, d. h. $N \in \mathcal{M}$. Daher ist N eine obere Schranke von $\mathcal{N}$. Nach Zorns Lemma existiert ein maximales Element $B \in \mathcal{M}$. Für jedes $s \in S \setminus B$ ist dann $B \cup \{s\}$ algebraisch abhängig, d. h. s ist algebraisch über $K(B)$. Ist $x \in K(S)$ beliebig, so existieren $s_1, \ldots, s_n \in S$ mit $x \in K(s_1, \ldots, s_n)$. Wegen $|K(B)(s_1, \ldots, s_n) : K(B)| < \infty$ ist auch x algebraisch über $K(B)$. Somit ist $K(B) \subseteq K(S)$ algebraisch und damit auch $K(B) \subseteq L$. Also ist B eine Transzendenzbasis mit der gewünschten Eigenschaft. Die zweite Behauptung folgt, indem man $U = \varnothing$ und $S = L$ wählt. □

Satz II.4.13 (Austauschsatz)**.** *Sei $K \subseteq L$ eine Körpererweiterung und $U \subseteq L$ eine endliche algebraisch unabhängige Teilmenge. Für jede Teilmenge $S \subseteq L$ mit $K(S) \subseteq L$ algebraisch gilt dann $|U| \leq |S|$.*

Beweis. Sei $U = \{u_1, \ldots, u_n\}$ und o. B. d. A. $S = \{s_1, \ldots, s_m\}$ (im Fall $|S| = \infty$ sind wir fertig). Dann ist u_1 algebraisch über $K(S)$, d. h. es existiert ein $\alpha \in K(S)[X] \setminus \{0\}$ mit Nullstelle u_1. Multipliziert man α mit einem gemeinsamen Nenner seiner Koeffizienten, so erhält man $\beta \in K[X_1, \ldots, X_m, X]$ mit $\beta(s_1, \ldots, s_m, u_1) = 0$. Da u_1 transzendent über K ist, taucht ein s_i, sagen wir s_1, in $\beta(s_1, \ldots, s_m, u_1)$ auf. Insbesondere ist s_1 algebraisch über $K(u_1, s_2, \ldots, s_m)$. Also sind die Erweiterungen

$$K(u_1, s_2, \ldots, s_m) \subseteq K(\{u_1\} \cup S) \subseteq L$$

algebraisch und so auch $K(u_1, s_2, \ldots, s_m) \subseteq L$. Wir können also S durch $\{u_1, s_2, \ldots, s_m\}$ ersetzen und das Argument mit u_2 wiederholen. Da $\{u_1, u_2\}$ algebraisch unabhängig ist, lässt sich auch u_2 durch ein s_i, sagen wir s_2, austauschen. Iteration ergibt schließlich $S = \{u_1, \ldots, u_n, s_{n+1}, \ldots, s_m\}$ und $n \leq m$. □

Satz II.4.14. *Je zwei Transzendenzbasen einer Körpererweiterung sind gleichmächtig.*

Beweis. Sei $K \subseteq L$ eine Körpererweiterung mit Transzendenzbasen B und C. Jedes $b \in B$ ist dann algebraisch über $K(C)$ und damit auch über $K(C_b)$ für eine endliche Teilmenge $C_b \subseteq C$. Umgekehrt ist jedes $c \in C$ algebraisch über $K(B)$ und damit auch über $K(\bigcup_{b\in B} C_b)$. Also sind $K(\bigcup_{b\in B} C_b) \subseteq K(C) \subseteq L$ algebraische Körpererweiterungen und Lemma II.4.11 zeigt $C = \bigcup_{b\in B} C_b$.

Sei nun $B_1 \subseteq B$ eine endliche Teilmenge. Dann ist $L_1 := K(B_1 \cup \bigcup_{b\in B_1} C_b)$ algebraisch (sogar endlich) über $K(\bigcup_{b\in B_1} C_b)$. Satz II.4.13 mit L_1 anstatt L zeigt $|B_1| \leq \left|\bigcup_{b\in B_1} C_b\right|$. Halls Heiratssatz liefert nun paarweise verschiedene $c_b \in C_b$ für alle $b \in B$. Also ist die Abbildung $B \to C$, $b \mapsto c_b$ injektiv. Aus Symmetriegründen gibt es auch eine injektive Abbildung $C \to B$. Nach Cantor-Bernstein sind B und C gleichmächtig. □

Definition II.4.15. Die Mächtigkeit einer Transzendenzbasis einer Körpererweiterung $K \subseteq L$ nennt man *Transzendenzgrad* von L über K und schreibt dafür $\operatorname{trg}(L|K)$ (nach Satz II.4.14 ist dies wohldefiniert).

Beispiel II.4.16.

(i) Genau dann ist $K \subseteq L$ algebraisch, wenn $\operatorname{trg}(L|K) = 0$.

(ii) $\operatorname{trg}(K(X)|K) = \operatorname{trg}(\mathbb{Q}(\pi)|\mathbb{Q}) = 1$.

(iii) Sind L und M rein transzendente Erweiterungen von K mit dem gleichen Transzendenzgrad, so gilt

$$L = K(B) \overset{II.4.7}{\cong} K(X_b : b \in B) \cong M,$$

wobei B eine Transzendenzbasis von L ist.

(iv) Sei $K := \mathbb{Q}(X)$ und L ein Zerfällungskörper von $\alpha := Y^2 + X^2 + 1 \in K[Y]$. Wir zeigen, dass $\mathbb{Q} \subseteq L$ absolut transzendent, aber nicht rein transzendent ist. Angenommen α besitzt eine Nullstelle $y \in K$. Dann existieren $\beta, \gamma \in \mathbb{Q}[X] \setminus \{0\}$ mit $y = \beta/\gamma$ und $(\beta/\gamma)^2 = -X^2 - 1$. Man erhält den Widerspruch $\beta^2 = -(X^2 + 1)\gamma^2$ (vergleiche Vorzeichen der führenden Koeffizienten). Also ist α irreduzibel und $|L : K| = 2$. Sei nun ω eine Nullstelle von α in L.

Sei $x \in L$ algebraisch über $\mathbb{Q}$. Dann existieren $a, b \in K$ mit $x = a + b\omega$. Als Galois-Erweiterung vom Grad 2 (Aufgabe I.57) besitzt L einen Automorphismus $\sigma \in \operatorname{Gal}(L|K)$ mit $\sigma(\omega) = -\omega$. Mit x ist auch $\sigma(x)$ algebraisch über $\mathbb{Q}$. Nach Satz I.13.4 ist auch

$$\frac{1}{4}(x - \sigma(x))^2 = b^2\omega^2 = -b^2(X^2 + 1) \in K$$

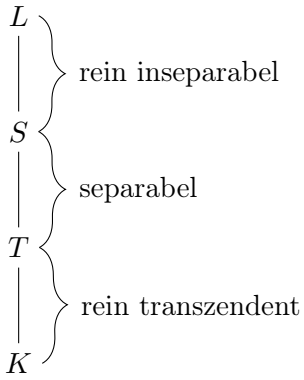
algebraisch über $\mathbb{Q}$. Da $\mathbb{Q} \subseteq K$ nach Lemma II.4.9 absolut transzendent ist, folgt $q := b^2(X^2+1) \in \mathbb{Q}$. Schreibt man $b = \beta/\gamma$ mit $\beta, \gamma \in \mathbb{Q}[X]$, so erhält man $\beta^2(X^2+1) = q\gamma^2$. Im Fall $b \neq 0$ ist die Vielfachheit des irreduziblen Polynoms X^2+1 auf der linken Seite ungerade und rechts gerade. Die eindeutige Primfaktorzerlegung (Satz I.8.24) impliziert daher $b = 0$ und $x = a \in K$. Da $\mathbb{Q} \subseteq K$ absolut transzendent ist, ergibt sich $x \in \mathbb{Q}$. Also ist $\mathbb{Q} \subseteq L$ absolut transzendent.

Da $\{X\}$ eine Transzendenzbasis von L über $\mathbb{Q}$ ist, gilt $\operatorname{trg}(L|\mathbb{Q}) = 1$. Nehmen wir an es existiert eine Transzendenzbasis $\{z\}$ mit $L = \mathbb{Q}(z)$. Dann existieren $\beta, \gamma, \delta, \rho \in \mathbb{Q}[X] \setminus \{0\}$ mit $X = \beta(z)/\gamma(z)$ und $\omega = \delta(z)/\rho(z)$. Aus $\omega^2 + X^2 + 1 = 0$ folgt

$$\delta(z)^2\gamma(z)^2 + \beta(z)^2\rho(z)^2 + \gamma(z)^2\rho(z)^2 = 0.$$

Da z über $\mathbb{Q}$ transzendent ist, gilt $(\delta\gamma)^2 + (\beta^2+\gamma^2)\rho^2 = 0$. Dies ist ausgeschlossen, denn der führende Koeffizient dieses Polynoms ist positiv. Daher ist $\mathbb{Q} \subseteq L$ nicht rein transzendent. Man kann zeigen, dass jeder Teilkörper von $\mathbb{Q}(X)$ rein transzendent ist (Satz A.6.3).

Bemerkung II.4.17. Nach Satz II.3.8 und den obigen Resultaten lässt sich jede Körpererweiterung $K \subseteq L$ aufspalten in $K \subseteq T \subseteq S \subseteq L$, wobei $K \subseteq T$ rein transzendent, $T \subseteq S$ separabel und $S \subseteq L$ rein inseparabel ist.



Satz II.4.18 (Gradsatz für $\operatorname{trg}(L|K)$)**.** *Für Körpererweiterungen $K \subseteq L \subseteq M$ gilt*

$$\boxed{\operatorname{trg}(M|K) = \operatorname{trg}(M|L) + \operatorname{trg}(L|K).}$$

Beweis. Seien B und C Transzendenzbasen von L über K bzw. M über L. Es genügt zu zeigen, dass $B \cup C$ eine Transzendenzbasis von M über K ist mit $B \cap C = \varnothing$. Jedes $c \in C$ ist transzendent über L und daher nicht in $B \subseteq L$ enthalten. Dies zeigt $B \cap C = \varnothing$. Nach Voraussetzung sind $K(B) \subseteq L$ und $L(C) \subseteq M$ algebraisch. Also sind auch $K(B \cup C) \subseteq L(C)$ und $K(B \cup C) \subseteq M$ algebraisch. Nach Satz II.4.12 existiert eine Transzendenzbasis S von M über K mit $B \subseteq S \subseteq B \cup C$. Mit $K(S) \subseteq L$ ist auch $L(S \cap C) \subseteq M$ algebraisch, denn $K(S) = K(B)(S \cap C) \subseteq L(S \cap C)$. Lemma II.4.11 zeigt $S = B \cap C$. □

Beispiel II.4.19. Sei B eine Transzendenzbasis von $\mathbb{C}$ über $\mathbb{Q}$. Nehmen wir an, dass B höchstens abzählbar ist. Als abzählbare Vereinigung abzählbarer Mengen ist dann auch

$$\mathbb{Q}(B) \cong \mathbb{Q}(X_1, \ldots) = \bigcup_{n=1}^{\infty} \mathbb{Q}(X_1, \ldots, X_n)$$

abzählbar. Da $\mathbb{Q}(B) \subseteq \mathbb{C}$ algebraisch ist, ist jede komplexe Zahl Nullstelle eines Polynoms in $\mathbb{Q}(B)[X]$. Also wäre auch $\mathbb{C}$ abzählbar. Dieser Widerspruch zeigt, dass B überabzählbar ist. Genauer gilt $\operatorname{trg}(\mathbb{C}|\mathbb{Q}) = |\mathbb{R}|$. Wegen $\operatorname{trg}(\mathbb{C}|\mathbb{R}) = 0$ ist auch $\operatorname{trg}(\mathbb{R}|\mathbb{Q}) = |\mathbb{R}|$ nach Satz II.4.18.

Bemerkung II.4.20. Nach Aufgabe I.53 ist $\mathrm{Aut}(\mathbb{Q}) = 1 = \mathrm{Aut}(\mathbb{R})$. Sei $\sigma \in \mathrm{Aut}(\mathbb{C})$ mit $\sigma(\mathbb{R}) = \mathbb{R}$. Dann ist $\sigma_{\mathbb{R}} \in \mathrm{Aut}(\mathbb{R})$ und $\sigma_{\mathbb{R}} = \mathrm{id}_{\mathbb{R}}$. Als Galois-Automorphismus von $\mathbb{C}$ über $\mathbb{R}$ ist σ entweder trivial oder die komplexe Konjugation. Wir zeigen, dass $\mathbb{C}$ sehr viele weitere Automorphismen besitzt (die dann $\mathbb{R}$ nicht festlassen können).

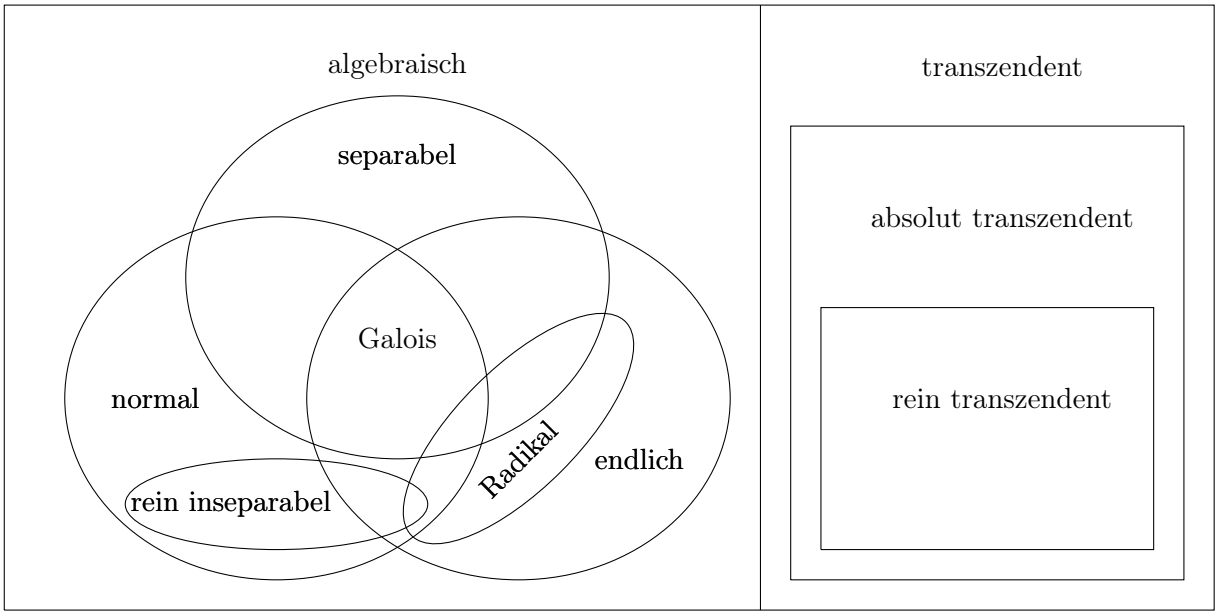
Satz II.4.21. *Der Körper $\mathbb{C}$ besitzt überabzählbar viele Automorphismen.*

Beweis. Sei B eine Transzendenzbasis von $\mathbb{C}$ über $\mathbb{Q}$. Jede Permutation $\sigma \in \mathrm{Sym}(B)$ induziert einen Automorphismus $\hat{\sigma}$ auf $\mathbb{Q}[X_b : b \in B]$ mit $\hat{\sigma}(X_b) = X_{\sigma(b)}$. Nach der universellen Eigenschaft des Quotientenkörpers (Aufgabe I.40) können wir $\hat{\sigma}$ zu einem Automorphismus auf $\mathbb{Q}(X_b : b \in B)$ fortsetzen. Wegen $\mathbb{Q}(B) \cong \mathbb{Q}(X_b : b \in B)$ erhält man daraus einen Automorphismus $\Gamma_\sigma \in \mathrm{Aut}(\mathbb{Q}(B))$ mit $\Gamma_\sigma(b) = \sigma(b)$. Da $\mathbb{Q}(B) \subseteq \mathbb{C}$ algebraisch ist und $\mathbb{C}$ algebraisch abgeschlossen, lässt sich Γ_σ nach Satz II.2.10 zu einem Homomorphismus $\hat{\Gamma}_\sigma \colon \mathbb{C} \to \mathbb{C}$ fortsetzen. Jedes $x \in \mathbb{C}$ ist Nullstelle seines Minimalpolynoms $\mu \in \mathbb{Q}(B)[X]$. Da $\Gamma_{\sigma^{-1}}(\mu) \in \mathbb{Q}(B)[X]$ über $\mathbb{C}$ in Linearfaktoren zerfällt, existiert ein $y \in \mathbb{C}$ mit $\hat{\Gamma}_\sigma(y) = x$. Daher ist $\hat{\Gamma}_\sigma$ surjektiv und wie üblich auch injektiv (Lemma I.8.41). Mit B sind auch $\mathrm{Sym}(B)$ und $\mathrm{Aut}(\mathbb{C})$ überabzählbar. □

Bemerkung II.4.22.

(i) Mit etwas mehr Mengenlehre[1] kann man $|\mathrm{Aut}(\mathbb{C})| \geq |\mathrm{Sym}(B)| = |\mathrm{Sym}(\mathbb{R})| > |\mathbb{R}|$ zeigen. Siehe auch Folgerung A.7.12.

(ii) Mit den in Aufgabe II.23 definierten *normalen* Körpererweiterungen ergibt sich folgende Übersicht, bei der die triviale Erweiterung $K \subseteq K$ vernachlässigt wurde:



[1] Siehe Sätze 8.3, 8.8 und 8.6 in meinem Mengenlehre-Skript

5 Teilbarkeit in Integritätsbereichen

Bemerkung II.5.1. In diesem Kapitel untersuchen wir, wann ein Ring eine eindeutige Primfaktorzerlegung so wie in $\mathbb{Z}$ oder $K[X]$ besitzt. Dazu sei R stets ein Integritätsbereich (kommutativer Ring ohne Nullteiler).

Definition II.5.2. Für $a, b \in R$ schreiben wir (wie üblich) $a \mid b$, falls ein $c \in R$ mit $ac = b$ existiert. Man sagt dann: *a teilt b*, a ist ein *Teiler* von b oder b ist durch a *teilbar*.

Bemerkung II.5.3. Für $a, b, c, d, e \in R$ gelten die üblichen Rechenregeln:

- $\pm 1 \mid a \mid 0$,
- $0 \mid a \iff a = 0$,
- $a \mid b \mid c \implies a \mid c$,
- $a \mid b, c \implies a \mid (bd + ce)$.

Lemma II.5.4. *Für $a, b \in R$ sind die folgenden Aussagen äquivalent:*

(1) $a \mid b \mid a$,

(2) $\exists e \in R^\times : a = be$,

(3) $(a) = (b)$.

Gegebenenfalls nennt man a und b assoziiert.

Beweis.

(1) $\Rightarrow$ (2): Es existieren $d, e \in R$ mit $ad = b$ und $be = a$. Daher ist $a(de - 1) = be - a = 0$. Im Fall $a = 0$ ist auch $b = 0d = 0$ und die Behauptung gilt mit $e = 1$. Anderenfalls gilt $de = 1 = ed$, da R nullteilerfrei und kommutativ ist. Es folgt $e \in R^\times$ mit $a = be$.

(2) $\Rightarrow$ (3): Nach Voraussetzung gilt

$$(a) = aR = beR \subseteq bR = (b) = ae^{-1}R \subseteq aR = (a).$$

(3) $\Rightarrow$ (1): Wegen $a \in (a) = (b) = bR$ existiert ein $c \in R$ mit $a = bc$. Also ist $b \mid a$ und aus Symmetriegründen gilt auch $a \mid b$. □

Bemerkung II.5.5. Die Einheitengruppe $R^\times$ operiert durch ${}^e a := ea$ auf R. Zwei Elemente $a, b \in R$ sind genau dann assoziiert, wenn sie in der gleichen Bahn dieser Operation liegen. Daher ist die Assoziiertheit eine Äquivalenzrelation auf R.

Beispiel II.5.6.

(i) Die zu 1 assoziierten Elemente in R sind genau die Einheiten $R^\times$. In einem Körper sind daher alle von Null verschiedenen Elemente assoziiert.

(ii) In $R = \mathbb{Z}$ sind a und b genau dann assoziiert, wenn $b = \pm a$ gilt (Beispiel I.7.5).

Definition II.5.7. Man nennt $p \in R \setminus (R^\times \cup \{0\})$

- *irreduzibel*, falls für alle $a, b \in R$ gilt: $p = ab \Rightarrow a \in R^\times \vee b \in R^\times$ (vgl. Primzahl).
- *Primelement*, falls für alle $a, b \in R$ gilt: $p \mid ab \Rightarrow p \mid a \vee p \mid b$ (vgl. Lemma I.2.16).

Lemma II.5.8. *Primelemente sind irreduzibel.*

Beweis. Sei $p \in R$ ein Primelement und $p = ab$ mit $a, b \in R$. Dann ist p ein Teiler von a oder b, sagen wir $p \mid a$. Wegen $a \mid p$ sind a und p assoziiert. Sei $e \in R^\times$ mit $p = ae$. Dann folgt $a(b - e) = 0$. Wegen $p \neq 0 \neq a$ gilt $b = e \in R^\times$. Also ist p irreduzibel. □

Beispiel II.5.9.

(i) Ist R ein Körper, so existieren weder irreduzible Elemente noch Primelemente, denn $R = R^\times \cup \{0\}$.

(ii) In $\mathbb{Z}$ gilt: p irreduzibel $\iff p$ Primelement $\iff |p|$ Primzahl. In $K[X]$ für einen Körper K stimmen die irreduziblen Elemente ebenso mit den Primelementen überein (Satz I.8.24) und jedes solche Element ist zu genau einem irreduziblen Polynom assoziiert (beachte: irreduzible Polynome sind normiert).

(iii) Ist $p \in R$ irreduzibel (bzw. Primelement), so auch jedes zu p assoziierte Element.

(iv) Im Allgemeinen ist nicht jedes irreduzible Element ein Primelement (siehe auch Aufgabe II.24): Wir betrachten

$$R := \mathbb{Z}[\sqrt{-5}] := \mathbb{Z} + \mathbb{Z}\sqrt{-5} = \left\{a + b\sqrt{-5} : a, b \in \mathbb{Z}\right\}.$$

Wegen $(a + b\sqrt{-5})(c + d\sqrt{-5}) = ac - 5bd + (bc + ad)\sqrt{-5}$ ist R ein Teilring von $\mathbb{C}$ und daher ein Integritätsbereich. Für alle $x = a + b\sqrt{-5} \in R$ gilt $|x|^2 = a^2 + 5b^2 \in \mathbb{Z}$. Sei $x := 1 + \sqrt{-5} \in R$. Im Fall $x \in R^\times$ wäre $1 = |x|^2|x^{-1}|^2 = 6|x^{-1}|^2 \in 6\mathbb{Z}$. Also ist $x \notin R^\times$. Für $y, z \in R$ mit $x = yz$ gilt $|y|^2|z|^2 = |x|^2 = 6$. Da die Gleichung $a^2 + 5b^2 = 2$ keine ganzzahlige Lösung hat, ist o. B. d. A. $|y|^2 = 1$. Dies zeigt $y = \pm 1 \in R^\times$. Also ist x irreduzibel. Andererseits gilt $x \mid x\bar{x} = 6 = 2 \cdot 3$. Wäre x ein Primelement, so gäbe es $y \in R$ mit $xy = 2$ oder $xy = 3$. Dies ist wegen $|xy|^2 = 6|y|^2 \notin \{4, 9\}$ ausgeschlossen. Also ist x kein Primelement.

Lemma II.5.10. *Seien $p_1, \ldots, p_s, q_1, \ldots, q_t \in R$ Primelemente mit $p_1 \ldots p_s = q_1 \ldots q_t$. Dann ist $s = t$ und bei geeigneter Nummerierung ist p_i zu q_i assoziiert für $i = 1, \ldots, s$.*

Beweis. Induktion nach s: Im Fall $s = 0$ ist $q_1 \ldots q_t = 1$ und $q_1 \in R^\times$. Da Primelemente keine Einheiten sind, gilt $t = 0$. Sei nun $s \geq 1$ und die Behauptung für $s-1$ bereits bewiesen. Aus $p_s \mid p_1 \ldots p_s = q_1 \ldots q_t$ folgt $p_s \mid q_i$ für ein $i \in \{1, \ldots, t\}$, sagen wir $i = t$. Sei also $e \in R$ mit $p_s e = q_t$. Da q_t nach Lemma II.5.8 irreduzibel ist, gilt $e \in R^\times$. Insbesondere sind p_s und q_t assoziiert. Es folgt

$$(p_1 \ldots p_{s-1} - q_1 \ldots q_{t-1}e)p_s = p_1 \ldots p_s - q_1 \ldots q_t = 0.$$

Wegen $p_s \neq 0$ ist $p_1 \ldots p_{s-1} = q_1 \ldots (q_{t-1}e)$. Nach Induktion ist $s = t$ und bei geeigneter Nummerierung ist p_i zu q_i bzw. zu $q_{t-1}e$ assoziiert für $i = 1, \ldots, s-1$. Dies zeigt die Behauptung. □

Definition II.5.11. Ein Integritätsbereich R heißt *faktoriell*[1], falls jedes Element aus $R \setminus (R^\times \cup \{0\})$ ein Produkt von Primelementen ist.

Satz II.5.12. *Die folgenden Aussagen sind äquivalent:*

(1) R ist faktoriell.

(2) Jedes $a \in R \setminus (R^\times \cup \{0\})$ lässt sich als Produkt irreduzibler Elemente schreiben und jedes irreduzible Element ist ein Primelement.

(3) Jedes $a \in R \setminus (R^\times \cup \{0\})$ lässt sich bis auf Reihenfolge und Assoziiertheit eindeutig als Produkt irreduzibler Elemente schreiben.

Beweis.

(1) $\Rightarrow$ (2): Da jedes Primelement irreduzibel ist, müssen wir nur den zweiten Teil zeigen. Jedes irreduzible Element $p \in R$ lässt sich als Produkt von Primelementen schreiben. Da Primelemente keine Einheiten sind, ist p selbst ein Primelement.

(2) $\Rightarrow$ (3): Folgt aus Lemma II.5.10.

(3) $\Rightarrow$ (1): Es genügt zu zeigen, dass jedes irreduzible Element $p \in R$ ein Primelement ist. Sei $p \mid ab$ für $a, b \in R$. Sei $c \in R$ mit $pc = ab$. Wir zerlegen $a = a_1 \dots a_r$, $b = b_1 \dots b_s$ und $c = c_1 \dots c_t$ in irreduzible Elemente. Aus der Eindeutigkeit der Zerlegung

$$pc_1 \dots c_t = a_1 \dots a_r b_1 \dots b_s$$

folgt, dass p zu einem a_i oder zu einem b_i assoziiert ist. Daher gilt $p \mid a$ oder $p \mid b$. Also ist p ein Primelement. □

Beispiel II.5.13.

(i) Jeder Körper ist faktoriell.

(ii) Sicher sind $\mathbb{Z}$ und $K[X]$ für einen Körper K faktoriell.

(iii) Nach Beispiel II.5.9 ist $\mathbb{Z}[\sqrt{-5}]$ nicht faktoriell, denn $1+\sqrt{-5}$ ist irreduzibel, aber kein Primelement. Dieses Phänomen machte Cauchys und Lamés Beweisversuche für Fermats letzten Satz zunichte.

(iv) Die meisten Integritätsbereiche sind bereits dann faktoriell, wenn jedes irreduzible Element ein Primelement ist (Aufgabe II.31).[2]

Bemerkung II.5.14.

(i) Sei R faktoriell und $P \subseteq R$ ein Repräsentantensystem für die Klassen assoziierter Primelemente (zum Beispiel die Primzahlen in $R = \mathbb{Z}$ oder die irreduziblen Polynome in $R = K[X]$). Dann besitzt jedes $x \in R \setminus \{0\}$ eine eindeutige *Primfaktorzerlegung*

$$x = e \prod_{p \in P} p^{\nu_p(x)}$$

[1] oder *ZPE-Ring* (**Z**erlegung **P**rimelemente **e**indeutig) bzw. im Englischen *UFD* (unique factorization domain)

[2] Ein Gegenbeispiel wird in `http://ramanujan.math.trinity.edu/rdaileda/teach/m4363s07/non_ufd.pdf` konstruiert.

mit $e \in R^\times$ und $\nu_p(x) \in \mathbb{N}_0$ für $p \in P$. Für $x, y \in R \setminus \{0\}$ gilt $x \mid y$ genau dann, wenn $\nu_p(x) \leq \nu_p(y)$ für alle $p \in P$. Für $x_1, \ldots, x_n \in R \setminus \{0\}$ setzt man

$$\mathrm{ggT}(x_1, \ldots, x_n) := \prod_{p \in P} p^{\min\{\nu_p(x_1), \ldots, \nu_p(x_n)\}},$$
$$\mathrm{kgV}(x_1, \ldots, x_n) := \prod_{p \in P} p^{\max\{\nu_p(x_1), \ldots, \nu_p(x_n)\}}.$$

Bis auf Assoziiertheit hängen ggT und kgV nicht von P ab. Im Fall $\mathrm{ggT}(x_1, \ldots, x_n) \in R^\times$ nennt man $x_1, \ldots, x_n$ *teilerfremd*.

(ii) Im Quotientenkörper $Q(R)$ hat jedes $x \in Q(R) \setminus \{0\}$ eine eindeutige Zerlegung in der Form

$$x = e \prod_{p \in P} p^{\nu_p(x)}$$

mit $e \in R^\times$ und $\nu_p(x) \in \mathbb{Z}$ für $p \in P$.

Definition II.5.15. Ein Integritätsbereich R heißt *Hauptidealring*, falls jedes Ideal in R ein Hauptideal ist.

Beispiel II.5.16. Nach Beispiel I.7.9(vii) und Lemma I.8.37 sind $\mathbb{Z}$ und $K[X]$ Hauptidealringe. Nach Aufgabe I.48 ist $\mathbb{Z}[X]$ kein Hauptidealring.

Bemerkung II.5.17. Nach Aufgabe II.4 ist $P \lhd R$ ein *Primideal*, falls $ab \in P \Rightarrow a \in P \vee b \in P$ für alle $a, b \in R$ gilt. Ist $p \in R$ ein Primelement, so ist (p) ein Primideal.

Lemma II.5.18. *Für jedes Element $p \neq 0$ eines Hauptidealrings R sind die folgenden Aussagen äquivalent:*

(1) (p) ist maximales Ideal,

(2) (p) ist Primideal,

(3) p ist Primelement,

(4) p ist irreduzibel.

Beweis. Nach Aufgabe II.4 gilt (1)⇒(2). Ist (p) ein Primideal und $p \mid ab$, so gilt $ab \in (p)$, also $a \in (p)$ oder $b \in (p)$. Dies zeigt $p \mid a$ oder $p \mid b$. Daher ist p ein Primelement. Nach Lemma II.5.8 gilt (3)⇒(4). Sei schließlich p irreduzibel. Wegen $p \notin R^\times$ ist $(p) \neq R$. Sei $(p) \subseteq I \lhd R$. Da R ein Hauptidealring ist, existiert ein $a \in R$ mit $I = (a)$. Wegen $p \in I$ existiert ein $b \in R$ mit $p = ab$. Wegen $I \neq R$ ist $a \notin R^\times$. Da p irreduzibel ist, gilt also $b \in R^\times$. Dies zeigt $I = (p)$ nach Lemma II.5.4. Daher ist (p) ein maximales Ideal. □

Satz II.5.19. *Hauptidealringe sind faktoriell.*

Beweis. Sei R ein Hauptidealring. Nach Lemma II.5.18 ist jedes irreduzible Element ein Primelement. Nach Satz II.5.12 genügt es zu zeigen, dass jedes $x_1 \in R \setminus (R^\times \cup \{0\})$ ein Produkt irreduzibler Elemente ist. Nehmen wir das Gegenteil an. Dann existieren $x_2, y \in R \setminus R^\times$ mit $x_1 = x_2 y$, wobei x_2 nicht irreduzibel ist. Wegen $y \notin R^\times$ ist $(x_1) \subsetneq (x_2)$. Wir können nun das Argument mit x_2 wiederholen und erhalten $x_3 \in R \setminus R^\times$ mit $(x_2) \subsetneq (x_3)$ usw. Offenbar ist dann $I := \bigcup_{i=1}^{\infty}(x_i)$ ein Ideal. Da R ein Hauptidealring ist, existiert ein $x \in R$ mit $I = (x)$. Dann existiert ein $i \in \mathbb{N}$ mit $x \in (x_i)$. Dies liefert den Widerspruch $(x_{i+1}) \subseteq I = (x) \subseteq (x_i)$. □

Lemma II.5.20 (Bézout)**.** *Sei R ein Hauptidealring und $a_1, \ldots, a_n \in R \setminus \{0\}$. Dann existieren $x_1, \ldots, x_n \in R$ mit $\mathrm{ggT}(a_1, \ldots, a_n) = x_1 a_1 + \ldots + x_n a_n$.*

Beweis. Sei $g := \mathrm{ggT}(a_1, \ldots, a_n)$. Da R ein Hauptidealring ist, existiert ein $a \in R$ mit $(a) = (a_1, \ldots, a_n) \subseteq (g)$. Sei P ein Repräsentantensystem für die Klassen assoziierter Primelemente. Wegen $(a_i) \subseteq (a) \subseteq (g)$ gilt $\nu_p(g) \leq \nu_p(a) \leq \nu_p(a_i)$ für $i = 1, \ldots, n$ und $p \in P$. Daher ist

$$\nu_p(g) \overset{II.5.14}{=} \min_{1 \leq i \leq n} \nu_p(a_i) = \nu_p(a)$$

für alle $p \in P$, d. h. a und g assoziiert. Es folgt $(g) = (a) = (a_1, \ldots, a_n) = Ra_1 + \ldots + Ra_n$. Daher existieren $x_1, \ldots, x_n$ mit $x_1 a_1 + \ldots + x_n a_n = g$. □

Bemerkung II.5.21. Als Teilring von $Q(R)[X]$ ist der Polynomring $R[X]$ über R ein Integritätsbereich. Wegen $\deg(\alpha\beta) = \deg(\alpha) + \deg(\beta)$ ist $R[X]^\times = R^\times$. Irreduzible Elemente in R sind auch irreduzibel in $R[X]$. Insbesondere können irreduzible Elemente in $R[X]$ auch konstant sein (z. B. 2 in $\mathbb{Z}[X]$). Im Folgenden verallgemeinern wir unsere früheren Ergebnisse über $\mathbb{Z}[X]$ (Lemma I.8.48).

Definition II.5.22. Ein Polynom $\alpha \in R[X]$ über einem faktoriellen Ring R heißt *primitiv*, falls der ggT seiner Koeffizienten eine Einheit ist.

Beispiel II.5.23. Ein primitives Polynom besitzt keine Teiler in $R \setminus R^\times$. Insbesondere ist jedes irreduzible Element $\alpha \in R[X] \setminus R$ primitiv.

Lemma II.5.24. *Sei R faktoriell mit Quotientenkörper $K = Q(R)$ und $\alpha, \beta \in R[X]$.*

(i) Genau dann ist $\alpha\beta$ primitiv, wenn α und β primitiv sind.

(ii) Für $\alpha \in K[X] \setminus \{0\}$ existieren $b \in K$ und $\tilde{\alpha} \in R[X]$ primitiv mit $\alpha = b\tilde{\alpha}$.

(iii) Sind $\alpha, \beta \in R[X]$ primitiv und $\alpha \mid \beta$ in $K[X]$, so gilt $\alpha \mid \beta$ auch in $R[X]$.

(iv) Ist $\alpha \in R[X] \setminus R$ irreduzibel in $R[X]$, so ist α auch irreduzibel in $K[X]$ (bis auf Normierung).

Ist R faktoriell und $\alpha, \beta \in R[X]$ primitiv, so ist auch $\alpha\beta$ primitiv.

Beweis.

(i) Offensichtlich kann $\alpha\beta$ nur dann primitiv sein, wenn α und β primitiv sind. Nehmen wir umgekehrt an, dass $\alpha\beta$ nicht primitiv ist. Da R faktoriell ist, ist $\alpha\beta$ durch ein Primelement $p \in R$ teilbar. Indem wir die Koeffizienten durch ihre Restklassen in $\overline{R} := R/(p)$ ersetzen, erhalten wir $\overline{\alpha\beta} = 0$ in $\overline{R}[X]$ (Reduktion modulo p). Da (p) ein Primideal ist, ist $\overline{R}$ ein Integritätsbereich nach Aufgabe II.4. Daher ist auch $\overline{R}[X]$ ein Integritätsbereich und es folgt $\overline{\alpha} = 0$ oder $\overline{\beta} = 0$ (wie üblich ist die

Reduktion modulo p ein Ringhomomorphismus). Daher sind die Koeffizienten von α oder β durch p teilbar.

(ii) Sei $r \neq 0$ ein gemeinsamer Nenner der Koeffizienten von α. Dann ist $r\alpha \in R[X]$. Sei s ein ggT der Koeffizienten von $r\alpha$. Dann ist $b := \frac{s}{r} \in K$ und $\tilde{\alpha} := b^{-1}\alpha \in R[X]$ ist primitiv.

(iii) Nach Voraussetzung existiert ein $\gamma \in K[X]$ mit $\alpha\gamma = \beta$. Nach (ii) existiert ein $b \in K$, sodass $b\gamma \in R[X]$ primitiv ist. Nach (i) ist auch $b\alpha\gamma = b\beta$ primitiv. Da β primitiv ist, folgt $b \in R^\times$ und $\gamma \in R[X]$. Daher gilt $\alpha \mid \beta$ in $R[X]$.

(iv) Nach Beispiel II.5.23 ist α primitiv. Nehmen wir indirekt $\alpha = \beta\gamma$ mit $\beta, \gamma \in K[X] \setminus K$ an. Nach (ii) existieren primitive $\tilde{\beta}, \tilde{\gamma} \in R[X]$ sowie $b, c \in K$ mit $\beta = b\tilde{\beta}$ und $\gamma = c\tilde{\gamma}$. Nach (i) ist $\tilde{\beta}\tilde{\gamma}$ primitiv und $\alpha = bc\tilde{\beta}\tilde{\gamma} \in R[X]$. Da α primitiv ist, folgt $bc \in R^\times$. Da α irreduzibel ist, wäre nun $\tilde{\beta}$ order $\tilde{\gamma}$ in $R[X]^\times = R^\times \subseteq K$. □

Satz II.5.25 (Gauss)**.** *Ist R faktoriell, so auch $R[X]$.*

Beweis. Sei $K = Q(R)$. Wir zeigen zunächst, dass jedes $\alpha \in R[X] \setminus (R^\times \cup \{0\})$ ein Produkt irreduzibler Elemente ist. Sei $\alpha = a\tilde{\alpha}$ mit $a \in R$ und $\tilde{\alpha} \in R[X]$ primitiv. Da R faktoriell ist, ist a ein Produkt irreduzibler Elemente von R, die auch irreduzibel in $R[X]$ sind. Wir können also $\alpha = \tilde{\alpha}$ annehmen. Ist α reduzibel in $R[X]$, so existieren $\beta, \gamma \in R[X] \setminus R$ mit $\alpha = \beta\gamma$. Man kann nun α durch β bzw. γ ersetzen. Wegen $\deg\beta, \deg\gamma < \deg\alpha$ erhält man schließlich eine Zerlegung in irreduzible Elemente.

Nun zeigen wir, dass jedes irreduzible Element $\alpha \in R[X]$ ein Primelement ist. Sei $\alpha \mid \beta\gamma$ für $\beta, \gamma \in R[X]$. Wir schreiben $\beta = b\tilde{\beta}$ und $\gamma = c\tilde{\gamma}$ mit $b, c \in R$ und $\tilde{\beta}, \tilde{\gamma} \in R[X]$ primitiv. Im Fall $\alpha \in R$ ist α auch irreduzibel in R und damit ein Primelement von R, da R faktoriell ist. Da $\tilde{\beta}\tilde{\gamma}$ primitiv ist (Lemma II.5.24), gilt dann $\alpha \mid bc$ und o. B. d. A. $\alpha \mid b$. Dies zeigt $\alpha \mid b\tilde{\beta} = \beta$. Sei nun $\alpha \notin R$. Nach Lemma II.5.24 ist dann α irreduzibel in $K[X]$. Da $K[X]$ als Hauptidealring faktoriell ist, ist α ein Primelement in $K[X]$. Nach Lemma II.5.24 ist dann α auch ein Primelement in $R[X]$. Nach Satz II.5.12 ist $R[X]$ faktoriell. □

Beispiel II.5.26. Nach Satz II.5.25 ist $\mathbb{Z}[X]$ faktoriell, aber kein Hauptidealring (Aufgabe I.48). Induktiv erhält man, dass auch $K[X_1, \ldots, X_n]$ für jeden Körper K faktoriell ist.

Bemerkung II.5.27. Auf ähnliche Weise lassen sich das Eisenstein-Kriterium und das Reduktionskriterium (Lemma I.8.56) auf faktorielle Ringe verallgemeinern (Aufgabe II.27).

Beispiel II.5.28. Das Polynom $X^2 + Y^3(Y-2)X + Y - 2$ ist irreduzibel in $\mathbb{Z}[X,Y] = \mathbb{Z}[Y][X]$ nach Eisenstein, denn $Y - 2$ ist irreduzibel (also ein Primelement) in $\mathbb{Z}[Y]$.

Definition II.5.29. Ein Integritätsbereich R heißt *euklidisch*, falls eine Abbildung $H\colon R \to \mathbb{N}_0$ mit folgender Eigenschaft existiert: Für alle $a, b \in R$ mit $b \neq 0$ existieren $q, r \in R$ mit $a = qb + r$ und $H(r) < H(b)$ (Division mit Rest).[3]

Satz II.5.30. *Euklidische Ringe sind Hauptidealringe und damit faktoriell.*

[3] Um Rechnungen zu vereinfachen verlangt man oft zusätzlich $H(0) = 0$ und $H(a) \leq H(ab)$ für alle $a, b \in R \setminus \{0\}$, siehe [P. Samuel, *About Euclidean rings*, J. Algebra 19 (1971), 282–301]

Beweis. Sei $I \trianglelefteq R$ und o. B. d. A. $I \neq \{0\}$. Dann besitzt $M := \{H(a) : 0 \neq a \in I\}$ als nichtleere Teilmenge von $\mathbb{N}_0$ ein kleinstes Element $H(b)$ für ein $b \in I \setminus \{0\}$. Sicher ist $(b) \subseteq I$. Für $a \in I$ existieren $q, r \in R$ mit $a = qb + r$ und $H(r) < H(b)$. Wegen $r = a - qb \in I$ folgt $r = 0$ aus der Wahl von b. Dies zeigt $a = qb \in (b)$ und $I = (b)$. □

Beispiel II.5.31.

(i) Jeder Körper K ist euklidisch mit $H(0) := 0$ und $H(a) := 1$ falls $a \neq 0$.

(ii) Offenbar ist $\mathbb{Z}$ mit $H(a) := |a|$ euklidisch. Analog ist $K[X]$ mit $H(0) := 0$ und $H(\alpha) := 1 + \deg \alpha$ für $\alpha \neq 0$ euklidisch nach Satz I.8.15.

(iii) Wir zeigen, dass der Ring der *Gaußschen Zahlen*

$$\mathbb{Z}[\mathrm{i}] := \mathbb{Z} + \mathbb{Z}\mathrm{i} \subseteq \mathbb{C}$$

euklidisch ist mit $H(x) := |x|^2 = a^2 + b^2$ für $x = a + b\mathrm{i} \in \mathbb{Z}[\mathrm{i}]$. Wegen $(a + b\mathrm{i})(c + d\mathrm{i}) = ac - bd + (ad + bc)\mathrm{i}$ für $a, b, c, d \in \mathbb{Z}$ ist $\mathbb{Z}[\mathrm{i}]$ ein Teilring von $\mathbb{C}$ und daher ein Integritätsbereich. Für $x, y \in \mathbb{Z}[\mathrm{i}]$ mit $y \neq 0$ ist $\frac{x}{y} = \alpha + \beta\mathrm{i}$ mit $\alpha, \beta \in \mathbb{R}$. Wähle $s, t \in \mathbb{Z}$ mit $|\alpha - s|, |\beta - t| \leq \frac{1}{2}$ und setze $q := s + t\mathrm{i} \in \mathbb{Z}[\mathrm{i}]$ sowie $r := x - qy$. Dann ist

$$H(r) = |x - qy|^2 = |y|^2 \Big|\frac{x}{y} - q\Big|^2 = |y|^2\big(|\alpha - s|^2 + |\beta - t|^2\big) \leq \frac{1}{2}|y|^2 < |y|^2 = H(y).$$

Analog zeigt man, dass $\mathbb{Z}[\sqrt{d}]$ für $d \in \{-2, 2, 3\}$ euklidisch ist (Aufgabe II.29). Andererseits ist $\mathbb{Z}[\sqrt{-5}]$ nicht euklidisch, da nicht faktoriell.

(iv) Man kann zeigen, dass $\mathbb{Z}\Big[\frac{1+\sqrt{-19}}{2}\Big]$ ein nicht-euklidischer Hauptidealring ist.[4] Merke:

$$\begin{aligned} \text{Körper} &\implies \text{euklidisch} \implies \text{Hauptidealring} \implies \text{faktoriell} \\ &\implies \text{Integritätsbereich} \implies \text{kommutativ} \end{aligned}$$

Bemerkung II.5.32. In jedem euklidischen Ring R lässt sich ein $\mathrm{ggT}(a, b)$ für $a, b \in R \setminus \{0\}$ mit dem erweiterten euklidischen Algorithmus bestimmen:

- Setze $(x_0, y_0, z_0) := (1, 0, a)$, $(x_1, y_1, z_1) := (0, 1, b)$ und $k := 0$.
- Solange $z_{k+1} \neq 0$ wiederhole:

  $$(x_{k+2}, y_{k+2}, z_{k+2}) := (x_k - x_{k+1}q_{k+1}, y_k - y_{k+1}q_{k+1}, r_{k+1}),$$

  wobei $z_k = q_{k+1}z_{k+1} + r_{k+1}$ mit $H(r_{k+1}) < H(z_{k+1})$.
- Für $z_{k+1} = 0$ ist $\mathrm{ggT}(a, b) = z_k = x_k a + y_k b$.

Beispiel II.5.33. Wir bestimmen die Einheiten und Primelemente von $R = \mathbb{Z}[\mathrm{i}]$. Für $e = a + b\mathrm{i} \in R^\times$ gilt $1 = |ee^{-1}|^2 = H(e)H(e^{-1})$. Dies zeigt $a^2 + b^2 = H(e) = 1$ und $R^\times = \{\pm 1, \pm\mathrm{i}\}$. Sei nun $\pi \in R$ ein Primelement. Wegen $\pi \notin R^\times$ ist $\pi \mid \pi\overline{\pi} = |\pi|^2 \geq 2$. Daher teilt π einen Primteiler p von $H(\pi)$. Teilt π auch $q \in \mathbb{P} \setminus \{p\}$, so teilt π auch $\mathrm{ggT}(p, q) = 1$ und man erhält den Widerspruch $\pi \in R^\times$. Also ist p die einzige durch π teilbare Primzahl. Man kann somit die Primelemente in R bestimmen, indem man die Primzahlen in Primelemente zerlegt. Jedes $\pi \in R$ mit $H(\pi) \in \mathbb{P}$ ist offenbar irreduzibel und

[4] Siehe [R.A. Wilson, *An elementary proof that not all principal ideal domains are Euclidean domains*, Math. Gaz. 101 (2017), 289–293, `http://www.maths.qmul.ac.uk/~raw/MTH5100/PIDnotED.pdf`]

daher ein Primelement in R. Insbesondere ist $1+\mathrm{i} \in R$ ein Primelement und $2 = -\mathrm{i}(1+\mathrm{i})^2$ ist die Primfaktorzerlegung von 2 (man sagt: 2 ist *verzweigt*).

Sei nun $p \equiv 3 \pmod 4$ und $\sigma, \tau \in R$ mit $p = \sigma\tau$. Dann ist

$$H(\sigma)H(\tau) = H(p) = p^2. \tag{II.5.1}$$

Wegen $a^2 + b^2 \not\equiv 3 \pmod 4$ für alle $a, b \in \mathbb{Z}$ hat die Gleichung $a^2 + b^2 = p$ keine ganzzahligen Lösungen. Daher ist p ein Primelement in R (man sagt: p ist *träge*).

Sei schließlich $p \equiv 1 \pmod 4$ und $q := (p-1)/2 \in 2\mathbb{Z}$. Nach Wilson (Aufgabe I.9) ist

$$-1 \equiv (p-1)! \equiv \prod_{k=1}^{q} k(p-k) \equiv (-1)^q (q!)^2 \equiv (q!)^2 \pmod p.$$

Dies zeigt $p \mid (q!)^2 + 1 = (q! - \mathrm{i})(q! + \mathrm{i})$. Wäre p ein Primelement in R, so wäre $p = \bar{p} \mid q! \pm \mathrm{i}$ und

$$0 \not\equiv 2q! = (q! + \mathrm{i}) + (q! - \mathrm{i}) \equiv 0 \pmod p.$$

Also ist p kein Primelement und nach (II.5.1) existiert ein Primteiler $\pi \mid p$ mit $\pi\overline{\pi} = H(\pi) = p$. O. B. d. A. sei $\pi \mid q! + \mathrm{i}$. Angenommen π und $\overline{\pi}$ sind assoziiert. Dann wären π und $\overline{\pi}$ Teiler von $q! \pm \mathrm{i}$ und daher auch Teiler von $2 = \mathrm{i}((q! - \mathrm{i}) - (q! + \mathrm{i}))$. Wir wissen aber bereits, dass jedes Primelement nur eine Primzahl teilt. Daher sind π und $\overline{\pi}$ nicht assoziiert (man sagt: p ist *zerlegt*). Zum Beispiel ist $5 = (2+\mathrm{i})(2-\mathrm{i})$.

Satz II.5.34. *Genau dann lässt sich $n \in \mathbb{N}$ als Summe von zwei ganzzahligen Quadraten schreiben, wenn die Vielfachheit jeder Primzahl $p \equiv 3 \pmod 4$ in der Primfaktorzerlegung von n gerade ist. Insbesondere ist jede Primzahl $p \equiv 1 \pmod 4$ Summe zweier Quadrate.*

Beweis.

$\Rightarrow$: Sei $n = a^2 + b^2 = (a+b\mathrm{i})(a-b\mathrm{i})$ mit $a, b \in \mathbb{Z}$. Nach Beispiel II.5.33 erhält man die Primfaktorzerlegung von $a + b\mathrm{i}$ wie folgt

$$a + b\mathrm{i} = e(1+\mathrm{i})^{\delta_2} \prod_{\substack{p \in \mathbb{P} \\ p \equiv 3 \pmod 4}} p^{\delta_p} \prod_{\substack{p \in \mathbb{P} \\ p \equiv 1 \pmod 4}} \pi_p^{\delta_p} \overline{\pi_p}^{\delta'_p}$$

mit $e \in \{\pm 1, \pm \mathrm{i}\}$ und $\delta_2, \delta_p, \delta'_p \in \mathbb{N}_0$. Daher ist

$$n = |a + b\mathrm{i}|^2 = 2^{\delta_2} \prod_{\substack{p \in \mathbb{P} \\ p \equiv 3 \pmod 4}} p^{2\delta_p} \prod_{\substack{p \in \mathbb{P} \\ p \equiv 1 \pmod 4}} p^{\delta_p + \delta'_p}$$

die Primfaktorzerlegung von n.

$\Leftarrow$: Nach Voraussetzung ist

$$n = 2^{\delta_2} \prod_{\substack{p \in \mathbb{P} \\ p \equiv 3 \pmod 4}} p^{2\delta_p} \prod_{\substack{p \in \mathbb{P} \\ p \equiv 1 \pmod 4}} p^{\delta_p} = |\alpha|^2 = H(\alpha)$$

mit

$$\alpha = (1+\mathrm{i})^{\delta_2} \prod_{\substack{p \in \mathbb{P} \\ p \equiv 3 \pmod 4}} p^{\delta_p} \prod_{\substack{p \in \mathbb{P} \\ p \equiv 1 \pmod 4}} \pi_p^{\delta_p} \in \mathbb{Z}[i].$$

Daher existieren $a, b \in \mathbb{Z}$ mit $\alpha = a + b\mathrm{i}$ und $a^2 + b^2 = H(\alpha) = n$. □

6 Moduln

Bemerkung II.6.1. Wir untersuchen in diesem Kapitel Vektorräume über Ringen anstelle von Körpern. Anders als in der linearen Algebra existieren in dieser Situation im Allgemeinen keine Basen. Selbst wenn Basen existieren, müssen sie nicht gleich groß sein. Die Theorie wird dadurch komplizierter, aber auch reichhaltiger.

Definition II.6.2. Sei R ein Ring (nicht unbedingt kommutativ). Eine abelsche Gruppe $(M, +)$ heißt *(R-)Linksmodul*[1], falls eine Skalarmultiplikation $R \times M \to M$, $(r, m) \mapsto rm$ mit folgenden Eigenschaften existiert:

- $r(m + n) = rm + rn$,
- $(r + s)m = rm + sm$,
- $(rs)m = r(sm)$,
- $1_R m = m$

für alle $r, s \in R$ und $m, n \in M$. Analog definiert man Rechtsmoduln.

Bemerkung II.6.3. Im Folgenden verstehen wir unter *Moduln* stets Linksmoduln. In der englischsprachigen Literatur und in Computeralgebrasystemen bevorzugt man oft Rechtsmoduln.

Beispiel II.6.4.

(i) Der *triviale* Modul $0 := \{0\}$.

(ii) Ist R ein Körper, so sind die Moduln genau die Vektorräume.

(iii) Jede abelsche Gruppe A ist ein $\mathbb{Z}$-Modul, wenn man (wie in Bemerkung I.3.2)

$$za := \begin{cases} a + \ldots + a \ (z \text{ Summanden}) & \text{falls } z \geq 0, \\ -|z|a & \text{falls } z < 0 \end{cases}$$

für $z \in \mathbb{Z}$ und $a \in A$ definiert. Umgekehrt ist natürlich jeder ($\mathbb{Z}$-)Modul eine abelsche Gruppe.

(iv) Mit der Ringaddition und Ringmultiplikation wird R zu einem R-Modul, den man *regulären* R-Modul nennt.

(v) Ersetzt man die Multiplikation in R durch

$$a * b := ba \qquad (a, b \in R) \qquad (a, b \in R),$$

so erhält man den *entgegengesetzten* Ring R^o mit $1_{R^0} = 1_R$. Jeder R-Linksmodul M wird durch $mr := rm$ ($r \in R$, $m \in M$) zu einem R^o-Rechtsmodul, denn für $r, s \in R$ gilt

$$m(r * s) = m(sr) = (sr)m = s(rm) = (rm)s = (mr)s.$$

[1] Anders als in der Studienordnung heißt es in der Mathematik: *der* Modul [ˈmoːdʊl] (maskulin) und die Moduln.

(vi) Sei K ein Körper und $R := K^{n\times n}$ für $n \in \mathbb{N}$. Für $m \in \mathbb{N}$ ist dann $K^{n\times m}$ mit der Matrizenmultiplikation ein R-Modul.

(vii) Ist M ein R-Modul und $f\colon S \to R$ ein Ringhomomorphismus, so wird M durch $sm := f(s)m$ ($s \in S$, $m \in M$) zu einem S-Modul. Ist S ein Teilring von R und f die Inklusionsabbildung, so erhält man auf diese Weise die *Einschränkung* von M auf S. Im Fall $R = S/I$ für ein $I \trianglelefteq S$ kann man den kanonischen Epimorphismus $f\colon S \to S/I$ wählen. Jeder S/I-Modul ist daher auch ein S-Modul.

(viii) Ist $(M_i)_{i\in I}$ eine Familie von R-Moduln, so wird das *direkte Produkt* $\bigtimes_{i\in I} M_i$ mit den komponentenweisen Verknüpfungen zu einem R-Modul. Im Fall $I = \{1, \ldots, n\}$ schreibt man wie üblich $M_1 \times \ldots \times M_n$ und M_1^n falls $M_1 = \ldots = M_n$.

Bemerkung II.6.5. Sei M ein R-Modul, $r \in R$ und $m \in M$. Dann gilt

$$r0_M = r(0_M + 0_M) = r0_M + r0_M = 0_M,$$
$$0_R m = (0_R + 0_R)m = 0_R m + 0_R m = 0_M.$$

Definition II.6.6. Eine Teilmenge N eines R-Moduls M heißt *Untermodul* von M, falls N mit den eingeschränkten Verknüpfungen selbst ein R-Modul ist. Wie bei Gruppen schreiben wir dann $N \leq M$ oder $N < M$, falls $N \neq M$.

Bemerkung II.6.7. Eine Teilmenge N eines R-Moduls M ist genau dann ein Untermodul, wenn $(N, +) \leq (M, +)$ und $rN \subseteq N$ für alle $r \in R$ gilt. Äquivalent ist auch: $N \neq \varnothing$ und $rx + sy \in N$ für alle $x, y \in N$ und $r, s \in R$.

Beispiel II.6.8.

(i) Bei Moduln über Körpern sind die Untermoduln natürlich die Untervektorräume.

(ii) Die Untermoduln eines $\mathbb{Z}$-Moduls sind genau die Untergruppen.

(iii) Stets sind 0 und M Untermoduln von M.

(iv) Der Durchschnitt beliebig vieler Untermoduln ist ein Untermodul.

(v) Für einen R-Modul M und $S \subseteq M$ ist

$$RS := \langle S\rangle := \bigcap_{\substack{N\leq M\\ S\subseteq N}} N \leq M$$

der von S *erzeugte* Untermodul. Offenbar besteht RS aus den Elementen der Form $r_1s_1 + \ldots + r_ns_n$ mit $r_1, \ldots, r_n \in R$ und $s_1, \ldots, s_n \in S$. Im Fall $RS = M$ ist S ein *Erzeugendensystem* von M. Ist zusätzlich $|S| < \infty$, so nennt man M *endlich erzeugt*.

(vi) Für jede Familie von Untermodul $(N_i)_{i\in I}$ von M ist auch die *Summe*

$$\sum_{i\in I} N_i := \Big\langle \bigcup_{i\in I} N_i \Big\rangle = \Big\{ x_1 + \ldots + x_n : n \in \mathbb{N},\ x_1, \ldots, x_n \in \bigcup N_i \Big\}$$

ein Untermodul von M. Im Fall $N_i \cap \sum_{j\neq i} N_j = 0$ für alle $i \in I$ nennen wir die Summe *direkt* und schreiben wie bei Gruppen $\bigoplus_{i\in I} N_i$. Dies bedeutet, dass die Darstellung eines Elements $x = x_1 + \ldots + x_n$ mit $x_j \in N_{i_j}$ $(j = 1, \ldots, n)$ bis auf die Reihenfolge der Summanden eindeutig ist.

(vii) Die Untermoduln des regulären Moduls nennt man *Linksideale* von R. Sicher ist jedes Ideal ein Linksideal. Ist R kommutativ, so gilt auch die Umkehrung. Künftig werden wir das Nullideal mit 0 anstatt $\{0\}$ bezeichnen.

(viii) Ist M ein R-Modul und $I \trianglelefteq R$, so ist

$$IM := \left\{ \sum_{i=1}^{n} x_i m_i : n \in \mathbb{N}, x_1, \ldots, x_n \in I, m_1, \ldots, m_n \in M \right\} \leq M.$$

Satz II.6.9. *Sind $N \leq M$ R-Moduln, so wird die Faktorgruppe M/N durch*

$$r(x+N) := rx + N \qquad (r \in R, x \in M)$$

zu einem R-Modul, den man Faktormodul *nennt.*

Beweis. Da M eine abelsche Gruppe ist, ist jede Untergruppe normal und M/N ist eine Gruppe. Für $x, y \in M$ mit $x + N = y + N$ gilt $x - y \in N \Longrightarrow rx - ry = r(x-y) \in N \Longrightarrow rx + N = ry + N$. Daher ist die Skalarmultiplikation wohldefiniert. Die Rechenregeln übertragen sich leicht von M nach M/N. □

Definition II.6.10. Eine Abbildung $f\colon M \to N$ für R-Moduln M, N heißt *Homomorphismus* (oder *R-linear*), falls $f(rx + y) = rf(x) + f(y)$ für $r \in R$ und $x, y \in M$ gilt. Die Menge aller Homomorphismen bezeichnet man mit $\mathrm{Hom}_R(M, N)$. Wie üblich definiert man Mono-, Epi-, Endo-, Iso- und Automorphismen. Abweichend von Gruppen und Ringen schreiben wir $M \simeq N$ oder genauer $M \simeq_R N$ für die Isomorphie von Moduln.

Bemerkung II.6.11.

(i) Jeder Homomorphismus $f\colon M \to N$ von R-Moduln ist auch ein Gruppenhomomorphismus. Wie üblich gilt daher $\mathrm{Ker}(f) \leq M$ und $f(M) \leq N$.

(ii) Für Moduln $N \leq M$ ist der *kanonische* Gruppenepimorphismus $M \to M/N$ auch R-linear.

(iii) Ist $f\colon M \to N$ ein bijektiver Homomorphismus, so ist auch $f^{-1}\colon N \to M$ ein Homomorphismus, denn

$$f^{-1}(rm) = f^{-1}\big(rf(f^{-1}(m))\big) = f^{-1}\big(f(rf^{-1}(m))\big) = rf^{-1}(m)$$

für $m \in M$ und $r \in R$.

(iv) Sind $f, g\colon M \to N$ R-linear, so auch $f+g\colon M \to N, m \mapsto f(m)+g(m)$. Dadurch wird $\mathrm{Hom}_R(M, N)$ zu einer abelschen Gruppe. Im Fall $M = N$ ist auch $f \circ g \in \mathrm{Hom}_R(M, M) =: \mathrm{End}_R(M)$. Wie üblich gilt dann $f\circ(g+h) = f\circ g + f\circ h$ und $(f+g)\circ h = f\circ h + g\circ h$ für $f, g, h \in \mathrm{End}_R(M)$. Auf diese Weise wird $\mathrm{End}_R(M)$ zu einem Ring mit Einselement id_M (im Fall endlich-dimensionaler Vektorräume ist $\mathrm{End}_R(M)$ nichts weiter als ein Matrixring). Man nennt $\mathrm{End}_R(M)$ den *Endomorphismenring* von M.

(v) Jeder R-Modul M wird durch $\varphi \cdot m := \varphi(m)$ für $\varphi \in \mathrm{End}_R(M)$ und $m \in M$ zu einem $\mathrm{End}_R(M)$-Modul.

Satz II.6.12.

(i) (Homomorphiesatz) Für jeden Homomorphismus von Moduln $f\colon M \to N$ gilt

$$\boxed{M/\mathrm{Ker}(f) \simeq f(M).}$$

(ii) (*Korrespondenzsatz*) *Für Moduln $N \leq M$ induziert der kanonische Epimorphismus $M \to M/N$ eine Bijektion zwischen der Menge der Untermoduln $L \leq M$ mit $N \leq L$ und der Menge der Untermoduln von M/N.*

(iii) (*1. Isomorphiesatz*) *Für $U, V \leq M$ gilt $V \leq U + V \leq M$, $U \cap V \leq U$ und*

$$\boxed{(U+V)/V \simeq U/U \cap V.}$$

(iv) (*2. Isomorphiesatz*) *Für Moduln $U \leq V \leq M$ ist*

$$\boxed{M/V \simeq (M/U)/(V/U).}$$

Beweis. Wir wissen aus Satz I.3.29 bereits, dass die Abbildung $F\colon M/\mathrm{Ker}(f) \to f(M)$, $m + \mathrm{Ker}(f) \mapsto f(m)$ ein wohldefinierter Gruppenisomorphismus ist. Wegen

$$F\big(r(m + \mathrm{Ker}(f))\big) = F(rm + \mathrm{Ker}(f)) = f(rm) = rf(m) = rF(m + \mathrm{Ker}(f))$$

für $r \in R$ und $m \in M$ ist F auch ein Isomorphismus von Moduln. Die anderen Aussagen sind Folgerungen aus dem Homomorphiesatz und gelten daher ebenfalls für Moduln. □

Definition II.6.13. Ein R-Modul $M \neq 0$ heißt *einfach*, wenn 0 und M die einzigen Untermoduln von M sind.

Lemma II.6.14 (Schurs Lemma)**.** *Seien M und N nicht-isomorphe einfache R-Moduln. Dann ist* $\mathrm{End}_R(M)$ *ein Schiefkörper und* $\mathrm{Hom}_R(M, N) = 0$.

Beweis. Sei $f \in \mathrm{Hom}_R(M, N)$. Aus der Einfachheit von M und N folgt $\mathrm{Ker}(f) \in \{0, M\}$ und $f(M) \in \{0, N\}$. Im Fall $\mathrm{Ker}(f) = 0$ erhält man den Widerspruch $M \simeq M/\mathrm{Ker}(f) \simeq f(M) = N$. Also ist $\mathrm{Ker}(f) = M$, d. h. $f = 0$. Im Fall $M = N$ erhält man

$$f \neq 0 \iff \mathrm{Ker}(f) = 0 \wedge f(M) = N \iff f \text{ bijektiv.}$$

Mit f ist dann auch $f^{-1} \in \mathrm{End}_R(M)$. Also gilt $\mathrm{End}_R(M)^\times = \mathrm{End}_R(M) \setminus \{0\}$. □

Beispiel II.6.15.

(i) Ein Vektorraum V über einem Körper K ist nur dann einfach, wenn $\dim V = 1$. Gegebenenfalls ist $\mathrm{End}_K(V) \cong K$.

(ii) Eine abelsche Gruppe A ist genau dann ein einfacher $\mathbb{Z}$-Modul, wenn A als Gruppe einfach ist. Ggf. ist $A \cong C_p$ und $\mathrm{End}_{\mathbb{Z}}(A) \cong \mathbb{F}_p$ für ein $p \in \mathbb{P}$ (Beispiel I.6.3).

(iii) Sei I ein echtes Linksideal eines Rings R. Wie im Satz von Krull beweist man mit Zorns Lemma die Existenz eines maximalen Linksideals M von R mit $I \subseteq M$. Nach dem Korrespondenzsatz (angewendet auf den regulären Modul) ist dann R/M ein einfacher R-Modul. Insbesondere besitzt jeder Ring $R \neq \{0\}$ einen einfachen Modul (wähle $I = 0$).

(iv) Sei umgekehrt M ein einfacher R-Modul und $0 \neq m \in M$. Dann ist die Abbildung $f\colon R \to M$, $r \mapsto rm$ ein Epimorphismus und der Homomorphiesatz zeigt $M \simeq R/\mathrm{Ker}(f)$.

Bemerkung II.6.16. Wie bei Gruppen definiert man Kompositionsreihen für Moduln und beweist den Satz von Jordan-Hölder (der Beweis ist sogar einfacher, da man sich nicht mehr um die Normalteilereigenschaft kümmern muss). Allerdings besitzt nicht jeder Modul eine Kompositionsreihe (zum Beispiel der reguläre $\mathbb{Z}$-Modul).

7 Endlichkeitsbedingungen

Bemerkung II.7.1. In der linearen Algebra beweist man Sätze für endlich-dimensionale Vektorräume. Da sich endlich erzeugte Moduln im Allgemeinen weniger anständig verhalten, führen wir eine Reihe von stärkeren Endlichkeitsbedingungen ein.

Satz II.7.2. *Für einen R-Modul M sind die folgenden Aussagen äquivalent:*

(1) Jeder Untermodul von M ist endlich erzeugt.

(2) Jede aufsteigende Folge von Untermoduln $N_1 \subseteq N_2 \subseteq \ldots$ von M wird stationär*, d. h. es existiert ein $k \in \mathbb{N}$ mit $N_k = N_{k+1} = \ldots$.*

(3) Jede nichtleere Menge von Untermoduln von M besitzt ein maximales Element (bzgl. $\subseteq$).

Gegebenenfalls nennt man M noethersch.

Beweis.

(1) $\Rightarrow$ (2): Sei $N_1 \subseteq N_2 \subseteq \ldots$ eine Folge von Untermoduln von M. Nach (1) gilt $\sum_{i=1}^{\infty} N_i = Rm_1 + \ldots + Rm_n$ für gewisse $m_1, \ldots, m_n \in M$. Sei $k \in \mathbb{N}$ mit $m_1, \ldots, m_n \in N_k$. Für $l \geq k$ ist dann

$$N_l \subseteq \sum_{i=1}^{\infty} N_i = Rm_1 + \ldots + Rm_n \leq N_k \leq N_l.$$

(2) $\Rightarrow$ (3): Sei $\mathcal{N}$ eine nichtleere Menge von Untermoduln von M und $N_1 \in \mathcal{N}$. Ist N_1 maximal, so sind wir fertig. Anderenfalls existiert $N_2 \in \mathcal{N}$ mit $N_1 \subsetneq N_2$. Ist auch N_2 nicht maximal, so existiert $N_3 \in \mathcal{N}$ mit $N_1 \subsetneq N_2 \subsetneq N_3$ usw. Nach (2) findet man nach endlich vielen Schritten auf diese Weise ein maximales Element.

(3) $\Rightarrow$ (1): Sei $N \leq M$. Ist N nicht endlich erzeugt, so existieren $x_1, x_2, \ldots \in N$ mit

$$Rx_1 \subsetneq Rx_1 + Rx_2 \subsetneq \ldots.$$

Dann besitzt die Menge der Untermoduln $Rx_1 + \ldots + Rx_n$ ($n \in \mathbb{N}$) aber kein maximales Element im Widerspruch zu (3). □

Satz II.7.3. *Für einen R-Modul M sind die folgenden Aussagen äquivalent:*

(1) Jede absteigende Folge von Untermoduln $N_1 \supseteq N_2 \supseteq \ldots$ von M wird stationär.

(2) Jede nichtleere Menge von Untermoduln von M besitzt ein minimales Element (bzgl. $\subseteq$).

Gegebenenfalls nennt man M artinsch.

Beweis.

(1) $\Rightarrow$ (2): Sei $\mathcal{N}$ eine nichtleere Menge von Untermoduln von M und $N_1 \in \mathcal{N}$. Ist N_1 minimal, so sind wir fertig. Anderenfalls existiert $N_2 \in \mathcal{N}$ mit $N_1 \supsetneq N_2$ usw. Nach endlich vielen Schritten findet man ein minimales Element.

(2) $\Rightarrow$ (1): Sei $N_1 \supseteq N_2 \supseteq \ldots$ eine Folge von Untermoduln von M. Dann besitzt die Menge $\{N_i : i \in \mathbb{N}\}$ ein minimales Element N_k. Für $l \geq k$ gilt dann $N_l \subseteq N_k \subseteq N_l$. □

Satz II.7.4. *Für einen R-Modul M sind die folgenden Aussagen äquivalent:*

(1) M ist eine Summe von einfachen Untermoduln.

(2) M ist eine direkte Summe von einfachen Untermoduln.

(3) Für jeden Untermodul $U \leq M$ existiert ein $V \leq M$ mit $M = U \oplus V$.

Gegebenenfalls nennt man M halbeinfach.

Beweis.

(1) $\Rightarrow$ (2): Sei $M = \sum_{i\in I} S_i$ mit einfachen Untermoduln $S_i \leq M$ $(i \in I)$. Dann ist

$$\mathcal{I} := \Big\{ J \subseteq I : \sum_{j\in J} S_j = \bigoplus_{j\in J} S_j \Big\}$$

wegen $\varnothing \in \mathcal{I}$ nichtleer und durch $\subseteq$ geordnet. Für eine total geordnete Teilmenge $\varnothing \neq \mathcal{K} \subseteq \mathcal{I}$ sei $T := \bigcup_{K\in\mathcal{K}} K \subseteq I$ und $N := \sum_{t\in T} S_t$. Nehmen wir $0 \neq x \in S_t \cap \sum_{i\in T\setminus\{t\}} S_i$ für ein $t \in T$ an. Dann existieren $t_1, \ldots, t_n \in T \setminus \{t\}$ und $x_i \in S_{t_i}$ mit $x = x_1 + \ldots + x_n$. Da $\mathcal{K}$ total geordnet ist, existiert $K \in \mathcal{K}$ mit $t, t_1, \ldots, t_n \in K$. Dann wäre aber $\sum_{k\in K} S_k \neq \bigoplus_{k\in K} S_k$. Also ist $N = \bigoplus_{t\in T} S_t$ und $T \in \mathcal{I}$ ist eine obere Schranke von $\mathcal{K}$. Nach Zorn besitzt $\mathcal{I}$ ein maximales Element J. Im Fall $\bigoplus_{j\in J} S_j \neq M$ existiert ein $i \in I$ mit $S_i \nsubseteq \bigoplus_{j\in J} S_j$. Da $S_i \cap \bigoplus_{j\in J} S_j$ ein echter Untermodul des einfachen Moduls S_i ist, folgt $S_i \cap \bigoplus_{j\in J} S_j = 0$. Also ist

$$S_i + \bigoplus_{j\in J} S_j = \bigoplus_{j\in J\cup\{i\}} S_j$$

im Widerspruch zur Maximalität von J. Dies zeigt $M = \bigoplus_{j\in J} S_j$.

(2) $\Rightarrow$ (3): Sei $M = \bigoplus_{i\in I} S_i$ mit einfachen Untermoduln $S_i \leq M$ $(i \in I)$. Für $U \leq M$ besitzt

$$\mathcal{I} := \Big\{ J \subseteq I : U \cap \sum_{j\in J} S_j = 0 \Big\}$$

wie oben ein maximales Element J. Im Fall $M \neq U + \sum_{j\in J} S_j$ existiert ein $i \in I$ mit $S_i \nsubseteq U + \sum_{j\in J} S_j$. Wie oben ist $S_i \cap \big(U + \sum_{j\in J} S_j\big) = 0$. Dann wäre aber auch $U \cap \sum_{j\in J\cup\{i\}} S_j = 0$ im Widerspruch zur Maximalität von J. Dies zeigt $M = U \oplus \sum_{j\in J} S_j$ und wir können $V := \sum_{j\in J} S_j$ setzen.

(3) $\Rightarrow$ (1): Sei U die Summe aller einfachen Untermoduln von M. Dann existiert $V \leq M$ mit $M = U \oplus V$. Nehmen wir $V \neq 0$ an und wählen $0 \neq x \in V$. Die Abbildung $\alpha\colon R \to V$, $r \mapsto rx$ ist dann ein Homomorphismus des regulären R-Moduls nach V. Wegen $1 \notin \operatorname{Ker}(\alpha)$ existiert ein maximales Linksideal I von R mit $\operatorname{Ker}(\alpha) \subseteq I$ (Beispiel II.6.15). Nach dem Korrespondenzsatz ist R/I ein

einfacher R-Modul. Nach Voraussetzung existiert $N \leq M$ mit $\alpha(I) \oplus N = M$. Die Dedekind-Identität zeigt

$$\alpha(R) = M \cap \alpha(R) = (\alpha(I) + N) \cap \alpha(R) = \alpha(I) + (N \cap \alpha(R)) = \alpha(I) \oplus (N \cap \alpha(R)).$$

Daher ist $N \cap \alpha(R) \simeq \alpha(R)/\alpha(I) \simeq R/I$ einfach und es ergibt sich der Widerspruch $N \cap \alpha(R) \subseteq U \cap V = 0$. Also ist $M = U$ eine Summe einfacher Untermoduln. □

Beispiel II.7.5.

(i) Jeder einfache Modul ist halbeinfach.

(ii) Nach Folgerung II.2.3 ist jeder Vektorraum V halbeinfach. Dagegen gilt

$$V \text{ noethersch} \iff \dim V < \infty \iff V \text{ artinsch}.$$

(iii) Jede endliche abelsche Gruppe ist noethersch und artinsch als $\mathbb{Z}$-Modul, denn sie besitzt nur endlich viele Untermoduln. Andererseits ist $V_4 \cong C_2 \times C_2$ halbeinfach, aber C_4 nicht. Außerdem ist $\mathbb{Z}$ noethersch (da jede Untergruppe zyklisch ist, also endlich erzeugt), aber nicht artinsch wegen $\mathbb{Z} \supsetneq 2\mathbb{Z} \supsetneq 4\mathbb{Z} \supsetneq \ldots$.

(iv) Wir betrachten die *Prüfergruppe*

$$A_p := \left\{ \frac{a}{p^n} + \mathbb{Z} : a \in \mathbb{Z},\ n \in \mathbb{N} \right\} \leq \mathbb{Q}/\mathbb{Z}$$

zur Primzahl p. Sei $B < A_p$ und $\frac{1}{p^n} + \mathbb{Z} \in B$ mit $n \in \mathbb{N}_0$ maximal gewählt. Für $\frac{a}{p^m} + \mathbb{Z} \in B$ mit $p \nmid a$ existieren $k, l \in \mathbb{Z}$ mit $ak + p^m l = \mathrm{ggT}(a, p^m) = 1$. Dann ist

$$\frac{1}{p^m} + \mathbb{Z} = k\frac{a}{p^m} + l + \mathbb{Z} = k\frac{a}{p^m} + \mathbb{Z} \in B$$

und die Maximalität von n zeigt $m \leq n$. Also ist

$$B = \left\{ \frac{a}{p^n} + \mathbb{Z} : a = 0, \ldots, p^n - 1 \right\} = \left\langle \frac{1}{p^n} + \mathbb{Z} \right\rangle \cong C_{p^n}.$$

Insbesondere ist jede echte Untergruppe von A_p endlich. Daher ist A_p ein artinscher $\mathbb{Z}$-Modul, aber wegen

$$\left\langle \frac{1}{p} + \mathbb{Z} \right\rangle \subsetneq \left\langle \frac{1}{p^2} + \mathbb{Z} \right\rangle \subsetneq \ldots$$

nicht noethersch. Es gibt also keinerlei Implikationen zwischen den drei Endlichkeitsbedingungen noethersch, artinsch und halbeinfach.

(v) Sei $M = \bigoplus_{i \in I} S_i$ halbeinfach mit einfachen Untermoduln $S_i \leq M$. Ist M zusätzlich noethersch (oder artinsch), so ist $|I| < \infty$, denn anderenfalls gäbe es eine Kette $S_{i_1} < S_{i_1} \oplus S_{i_2} < \ldots$ (bzw. $M > \bigoplus_{i \in I \setminus \{i_1\}} S_i > \ldots$). Gegebenenfalls ist M auch artinsch (bzw. noethersch).

Lemma II.7.6. *Seien $N \leq M$ Moduln. Genau dann ist M noethersch (bzw. artinsch), wenn N und M/N noethersch (bzw. artinsch) sind.*

Beweis. Sei M noethersch. Jede Folge von Untermoduln $N_1 \subseteq N_2 \subseteq \ldots$ von N ist dann auch eine Folge von Untermoduln von M und wird daher stationär. Ist analog $M_1/N \subseteq M_2/N \subseteq \ldots$ eine Folge von Untermoduln von M/N, so wird auch $M_1 \subseteq M_2 \subseteq \ldots$ stationär (Korrespondenzsatz). Daher sind N und M/N noethersch.

Seien nun N und M/N noethersch. Sei $M_1 \subseteq M_2 \subseteq \ldots$ eine Folge von Untermoduln von M. Dann sind $M_1 \cap N \subseteq M_2 \cap N \subseteq \ldots$ Untermoduln von N und es existiert ein $k \in \mathbb{N}$ mit $M_k \cap N = M_{k+1} \cap N = \ldots$. Analog sind $(M_1 + N)/N \subseteq (M_2 + N)/N \subseteq \ldots$ Untermoduln von M/N und es existiert ein $l \in \mathbb{N}$ mit $M_l + N = M_{l+1} + N = \ldots$. Für $n \geq \max\{k, l\}$ gilt dann nach der Dedekind-Identität:

$$M_n = M_n + (N \cap M_n) = M_n + (N \cap M_{n+1}) = (M_n + N) \cap M_{n+1} = (M_{n+1} + N) \cap M_{n+1} = M_{n+1}.$$

Analog zeigt man die Aussage für artinsch anstatt noethersch. □

Bemerkung II.7.7. Sind M und N noethersche (bzw. artinsche) R-Moduln, so auch $M \times N$, denn $(M \times N)/(M \times 0) \simeq N$.

Satz II.7.8. *Ein R-Modul M besitzt genau dann eine Kompositionsreihe, wenn M noethersch und artinsch ist.*

Beweis. Sei $0 = M_0 \leq \ldots \leq M_l = M$ eine Kompositionsreihe. Für $l = 0$ ist $M = 0$ sicher noethersch und artinsch. Sei nun $l > 0$. Dann ist $0 = M_0 \leq \ldots \leq M_{l-1}$ eine Kompositionsreihe von M_{l-1}. Durch Induktion nach l können wir annehmen, dass M_{l-1} noethersch und artinsch ist. Der einfache Modul M/M_{l-1} ist ebenfalls noethersch und artinsch. Nach Lemma II.7.6 ist M noethersch und artinsch.

Sei nun umgekehrt M noethersch und artinsch. Sei $\mathcal{M}$ die Menge aller Untermoduln von M, die eine Kompositionsreihe besitzen. Wegen $0 \in \mathcal{M}$ ist $\mathcal{M} \neq \varnothing$. Da M noethersch ist, besitzt $\mathcal{M}$ ein maximales Element $N \leq M$. Nehmen wir $N < M$ an. Mit M ist auch M/N artinsch (Lemma II.7.6). Daher besitzt die Menge aller nicht-trivialer Untermoduln von M/N ein minimales Element L/N. Offenbar ist dann L/N einfach. Dann besitzt aber auch L eine Kompositionsreihe im Widerspruch zur Wahl von N. Also besitzt $M = N$ eine Kompositionsreihe. □

Bemerkung II.7.9. Nehmen wir an, dass der reguläre R-Modul eine Kompositionsreihe besitzt. Sei M ein einfacher R-Modul. Nach Beispiel II.6.15 existiert ein Linksideal I von R mit $M \simeq R/I$. Nach Satz II.7.8 und Lemma II.7.6 besitzt auch I eine Kompositionsreihe, die man zu einer Kompositionsreihe von R ergänzen kann. Insbesondere ist M zu einem Kompositionsfaktor von R isomorph. Nach Jordan-Hölder gibt es daher nur endlich viele einfache R-Moduln bis auf Isomorphie.

Lemma II.7.10. *Ist M ein halbeinfacher R-Modul und $N \leq M$, so sind auch N und M/N halbeinfach.*

Beweis. Für $U \leq N$ existiert ein $V \leq M$ mit $M = U \oplus V$. Nach der Dedekind-Identität ist

$$N = M \cap N = (U \oplus V) \cap N = U \oplus (V \cap N)$$

mit $V \cap N \leq N$. Daher ist N halbeinfach. Außerdem existiert ein $N' \leq M$ mit $M = N \oplus N'$. Dann ist auch $N' \simeq M/N$ halbeinfach. □

Beispiel II.7.11. Die Umkehrung von Lemma II.7.10 ist falsch: C_4 ist als $\mathbb{Z}$-Modul nicht halbeinfach, aber $C_2 \leq C_4$ und $C_4/C_2 \cong C_2$.

Satz II.7.12. *Für einen R-Moduln $M \neq 0$ sind die folgenden Aussagen äquivalent:*

(1) Es gibt keine echten Untermoduln $M_1, M_2 < M$ mit $M = M_1 \oplus M_2$.

(2) 0 und id_M sind die einzigen Idempotente in $\mathrm{End}_R(M)$.

Gegebenenfalls nennt man M unzerlegbar.

Beweis.

(1) $\Rightarrow$ (2): Sei $f \in \mathrm{End}_R(M)$ ein Idempotent. Sei $M_1 := \mathrm{Ker}(f)$ und $M_2 := f(M)$. Für $x \in M$ gilt $f(x) = f(f(x))$ und $x - f(x) \in M_1$. Dies zeigt $x = (x - f(x)) + f(x) \in M_1 + M_2$. Für $x \in M_1 \cap M_2$ existiert ein $y \in M$ mit $x = f(y)$. Es folgt $x = f(f(y)) = f(x) = 0$. Also gilt $M_1 \cap M_2 = 0$ und $M = M_1 \oplus M_2$. Aus der Voraussetzung folgt $M_1 = 0$, $M_2 = M$ oder $M_1 = M$, $M_2 = 0$. Im ersten Fall ist f bijektiv und $f = f^2 f^{-1} = f f^{-1} = \mathrm{id}_M$. Im zweiten Fall ist $f = 0$.

(2) $\Rightarrow$ (1): Seien $M_1, M_2 \leq M$ mit $M = M_1 \oplus M_2$. Sei $\pi_i \colon M \to M_i$ die i-te Projektion für $i = 1, 2$. Aus $\pi_i^2 = \pi_i$ folgt $\pi_i = \mathrm{id}_M$ oder $\pi_i = 0$ nach Voraussetzung. Im ersten Fall ist $M_1 = M$ und im zweiten Fall ist $M_2 = M$. □

Beispiel II.7.13.

(i) Jeder einfache Modul ist unzerlegbar. Umgekehrt ist jeder unzerlegbare, halbeinfache Modul einfach.

(ii) Der $\mathbb{Z}$-Modul C_4 ist unzerlegbar, aber nicht (halb)einfach.

Lemma II.7.14 (Fitting)**.** *Sei M ein noetherscher und artinscher R-Modul. Für $f \in \mathrm{End}_R(M)$ existiert ein $k \in \mathbb{N}$ mit $M = \mathrm{Ker}(f^k) \oplus f^k(M)$.*

Beweis. Da M noethersch und artinsch ist, werden die Folgen $\mathrm{Ker}(f) \subseteq \mathrm{Ker}(f^2) \subseteq \ldots$ und $f(M) \supseteq f^2(M) \supseteq \ldots$ stationär. Sei $k \in \mathbb{N}$ mit $\mathrm{Ker}(f^k) = \mathrm{Ker}(f^{k+1}) = \ldots$ und $f^k(M) = f^{k+1}(M) = \ldots$. Für $x \in \mathrm{Ker}(f^k) \cap f^k(M)$ existiert $y \in M$ mit $f^k(y) = x$. Aus $f^{2k}(y) = f^k(x) = 0$ folgt $y \in \mathrm{Ker}(f^{2k}) = \mathrm{Ker}(f^k)$ und $x = f^k(y) = 0$. Also gilt $\mathrm{Ker}(f^k) \cap f^k(M) = 0$. Für ein beliebiges $x \in M$ existiert $y \in M$ mit $f^k(x) = f^{2k}(y)$. Es folgt $x - f^k(y) \in \mathrm{Ker}(f^k)$ und

$$x = (x - f^k(y)) + f^k(y) \in \mathrm{Ker}(f^k) + f^k(M). \qquad \square$$

Lemma II.7.15. *Sei M ein noetherscher, artinscher, unzerlegbarer R-Modul und $f, g \in \mathrm{End}_R(M)$. Ist $f + g$ bijektiv, so ist f oder g bijektiv.*

Beweis. Für $\tilde{f} := (f+g)^{-1} \circ f$ und $\tilde{g} := (f+g)^{-1} \circ g$ gilt $\tilde{f} + \tilde{g} = \mathrm{id}_M$. O. B. d. A. sei f nicht bijektiv. Dann ist auch $\tilde{f}$ nicht bijektiv. Nach Fitting existiert $k \in \mathbb{N}$ mit $\tilde{f}^k = 0$, da M unzerlegbar ist. Wegen

$$(\mathrm{id}_M - \tilde{f})(\mathrm{id}_M + \tilde{f} + \ldots + \tilde{f}^{k-1}) = \mathrm{id}_M$$

ist $\tilde{g} = \mathrm{id}_M - \tilde{f}$ bijektiv. Damit ist auch $g = (f+g) \circ \tilde{g}$ bijektiv. □

Satz II.7.16 (Krull-Schmidt)**.** *Jeder noethersche, artinsche R-Modul M besitzt eine Zerlegung in unzerlegbare Moduln $M = M_1 \oplus \ldots \oplus M_k$, die bis auf Reihenfolge und Isomorphie eindeutig bestimmt sind.*

Beweis.
Existenz: Ist M unzerlegbar, so gilt die Behauptung mit $M_1 = M$. Sei also $M = M_1 \oplus M_2$ mit $M_1, M_2 < M$. Sind M_1 und M_2 unzerlegbar, so sind wir fertig. Sei also o. B. d. A. $M_1 = M_3 \oplus M_4$ mit $M_3, M_4 < M_1$. Iteration liefert eine Folge $M > M_1 > M_3 > \ldots$. Da M artinsch ist, muss der Prozess abbrechen. Man hat dann eine gewünschte Zerlegung gefunden.

Eindeutigkeit: Seien $M = M_1 \oplus \ldots \oplus M_k = N_1 \oplus \ldots \oplus N_l$ Zerlegungen in unzerlegbare Moduln. Induktion nach k: Für $k = 1$ ist M unzerlegbar und $l = 1$. Sei also $k \geq 2$. Sei $\pi_i \colon M \to M_i$ die i-te Projektion der ersten Zerlegung und $\rho \colon M \to N_1$ die erste Projektion der zweiten Zerlegung. Dann ist

$$\mathrm{id}_{N_1} = \rho_{|N_1} = \rho \circ (\pi_1 + \ldots + \pi_k)_{|N_1} = (\rho \circ \pi_1)_{|N_1} + \ldots + (\rho \circ \pi_k)_{|N_1}.$$

Nach Lemma II.7.15 ist $(\rho \circ \pi_i)_{|N_1}$ für ein i bijektiv; o. B. d. A. $i = 1$. Insbesondere ist $(\pi_1)_{|N_1}$ injektiv und $\rho_{|M_1}$ surjektiv. Für $\sigma := \pi_1 \circ (\rho \circ \pi_1)^{-1}_{|N_1} \circ \rho_{|M_1} \in \mathrm{End}_R(M_1)$ gilt offenbar

$$\sigma^2 = \pi_1 \circ (\rho \circ \pi_1)^{-1}_{|N_1} \circ \rho \circ \pi_1 \circ (\rho \circ \pi_1)^{-1}_{|N_1} \circ \rho_{|M_1} = \sigma \neq 0.$$

Aus Satz II.7.12 folgt $\sigma = \mathrm{id}_{M_1}$. Daher ist $(\pi_1)_{|N_1}$ auch surjektiv. Dies zeigt $N_1 \simeq M_1$. Für $x \in M_1$ existiert $y \in N_1$ mit $\pi_1(x) = x = \pi_1(y)$ und $x - y \in \mathrm{Ker}(\pi_1) = M_2 + \ldots + M_k$. Es folgt $M = N_1 + M_2 + \ldots + M_k$. Für $x \in N_1 \cap (M_2 + \ldots + M_k)$ ist $\pi_1(x) = 0$ und $x = 0$, da $(\pi_1)_{|N_1}$ injektiv ist. Damit ist

$$M = N_1 \oplus M_2 \oplus \ldots + \oplus M_k$$

gezeigt. Wegen $M_2 \oplus \ldots \oplus M_k \simeq M/N_1 \simeq N_2 \oplus \ldots \oplus N_l$ folgt die Behauptung nun durch Induktion. □

Definition II.7.17. Für einen R-Modul M heißt

$$\mathrm{Ann}_R(M) := \{r \in R : rM = 0\} \subseteq R$$

der *Annullator* von M.

Beispiel II.7.18.

(i) Für den regulären R-Modul gilt $\mathrm{Ann}_R(R) = 0$.

(ii) Sei $A \cong C_{n_1} \times \ldots \times C_{n_k}$ eine abelsche Gruppe. Dann gilt

$$m \in \mathrm{Ann}_{\mathbb{Z}}(A) \iff \forall a \in A : ma = 0 \iff \forall a \in A : |\langle a \rangle| \,\big|\, m \iff n_1, \ldots, n_k \mid m.$$

Also ist $\mathrm{Ann}_{\mathbb{Z}}(A) = \mathbb{Z}\,\mathrm{kgV}(n_1, \ldots, n_k)$.

Lemma II.7.19.

(i) Annullatoren sind Ideale.

(ii) Isomorphe Moduln haben die gleichen Annullatoren.

Beweis.

(i) Sei M ein R-Modul. Wegen $0 \in \mathrm{Ann}_R(M)$ ist $\mathrm{Ann}_R(M)$ nichtleer. Für $x, y \in \mathrm{Ann}_R(M)$ und $r \in R$ gilt $(x - y)M \subseteq xM - yM = 0$, $rxM = r0 = 0$ und $xrM \subseteq xM = 0$.

(ii) Sei $f \colon M \to N$ ein Isomorphismus von R-Moduln. Dann gilt

$$r \in \mathrm{Ann}_R(M) \iff rM = 0 \iff rN = rf(M) = f(rM) = 0 \iff r \in \mathrm{Ann}_R(N). \qquad \square$$

Lemma II.7.20. *Für R-Moduln M, M', N, N' gilt*

(i) *Für jedes Idempotent $e \in R$ ist* $\mathrm{End}_R(Re) \cong (eRe)^o$. *Insbesondere ist* $\boxed{\mathrm{End}_R(R) \cong R^o.}$

(ii) $\boxed{\mathrm{End}_R(M^n) \cong \mathrm{End}_R(M)^{n\times n}}$ *für* $n \in \mathbb{N}$.

(iii) $\mathrm{Hom}_R(M,N) = 0 = \mathrm{Hom}_R(N,M) \implies \mathrm{End}_R(M \times N) \cong \mathrm{End}_R(M) \times \mathrm{End}_R(N)$.

(iv) $\mathrm{Hom}_R(M, N \times N') \simeq_{\mathbb{Z}} \mathrm{Hom}_R(M,N) \times \mathrm{Hom}_R(M,N')$.

(v) $\mathrm{Hom}_R(M \times M', N) \simeq_{\mathbb{Z}} \mathrm{Hom}_R(M,N) \times \mathrm{Hom}_R(M',N)$.

Beweis.

(i) Nach Aufgabe II.7 ist eRe ein Ring mit Einselement e. Offenbar ist Re ein Linksideal von R. Wir betrachten die Abbildung

$$\begin{aligned}\Phi\colon \mathrm{End}_R(Re) &\to (eRe)^o,\\ f &\mapsto f(e) = f(e^2) = ef(e).\end{aligned}$$

Wegen $\mathrm{id}(e) = e$, $(f+g)(e) = f(e) + g(e)$ und

$$(f \circ g)(e) = f(g(e)) = f(g(e)e) = g(e)f(e) = f(e) * g(e)$$

ist Φ ein Ringhomomorphismus. Aus $f(e) = 0$ folgt $f(re) = rf(e) = 0$ für alle $r \in R$. Daher ist Φ injektiv. Für ein gegebenes $x \in eRe$ ist die Abbildung $f_x\colon Re \to Re$, $s \mapsto sx$ R-linear. Wegen $\Phi(f_x) = f_x(e) = ex = x$ ist Φ auch surjektiv. Die letzte Behauptung ergibt sich mit $e = 1$.

(ii) Für $i = 1, \dots, n$ sind die Abbildungen

$$\begin{aligned}\pi_i\colon M^n &\to M,\ (m_1, \dots, m_n) \mapsto m_i,\\ \rho_i\colon M &\to M^n,\ m \mapsto (0, \dots, 0, m, 0, \dots, 0)\end{aligned}$$

R-linear. Es gilt

$$\pi_i\rho_j = \begin{cases}\mathrm{id}_M & \text{falls } i = j,\\ 0 & \text{falls } i \neq j,\end{cases} \qquad \mathrm{id}_{M^n} = \sum_{i=1}^n \rho_i\pi_i.$$

Wir definieren $\Phi\colon \mathrm{End}_R(M^n) \to \mathrm{End}_R(M)^{n\times n}$, $f \mapsto (\pi_i f \rho_j)_{i,j=1}^n$. Dann ist $\Phi(\mathrm{id}) = (\pi_i\rho_j)_{i,j} = 1_n$ und $\Phi(f+g) = \Phi(f) + \Phi(g)$ für $f, g \in \mathrm{End}_R(M^n)$. Außerdem ist

$$\Phi(fg) = (\pi_i f\,\mathrm{id}\, g\rho_j)_{i,j} = \Big(\pi_i f \sum_{k=1}^n \rho_k\pi_k g\rho_j\Big)_{i,j} = (\pi_i f\rho_j)_{i,j}(\pi_i g\rho_j)_{i,j} = \Phi(f)\Phi(g).$$

Daher ist Φ ein Ringhomomorphismus. Für $\Phi(f) = 0$ ist auch

$$f = \Big(\sum_{i=1}^n \rho_i\pi_i\Big) f \Big(\sum_{j=1}^n \rho_j\pi_j\Big) = \sum_{i,j=1}^n \rho_i(\pi_i f\rho_j)\pi_j = 0$$

und Φ ist injektiv. Sei schließlich $(f_{ij})_{i,j} \in \mathrm{End}_R(M)^{n\times n}$ gegeben. Dann ist $f := \sum_{i,j=1}^n \rho_i f_{ij}\pi_j \in \mathrm{End}_R(M^n)$ mit

$$\Phi(f) = \Big(\pi_i \sum_{k,l=1}^n \rho_k f_{kl}\pi_l\rho_j\Big)_{i,j} = (\mathrm{id}\, f_{ij}\, \mathrm{id})_{i,j} = (f_{ij})_{i,j}.$$

Also ist Φ surjektiv.

(iii) Mit den Bezeichnungen aus (ii) sei $\Phi\colon \mathrm{End}_R(M\times N) \to \mathrm{End}_R(M)\times\mathrm{End}_R(N)$, $f \mapsto (\pi_1 f\rho_1, \pi_2 f\rho_2)$. Man zeigt leicht, dass Φ ein Ringhomomorphismus ist. Sei $\Phi(f) = 0$. Wegen

$$\pi_1 f\rho_2 \in \mathrm{Hom}_R(N, M) = 0 \qquad\qquad \pi_2 f\rho_1 \in \mathrm{Hom}_R(M, N) = 0$$

ist auch

$$f = (\rho_1\pi_1 + \rho_2\pi_2)f(\rho_1\pi_1 + \rho_2\pi_2) = 0$$

und Φ ist injektiv. Für $(f_1, f_2) \in \mathrm{End}_R(M)\times\mathrm{End}_R(N)$ sei $f\colon = \rho_1 f_1\pi_1 + \rho_2 f_2\pi_2 \in \mathrm{End}_R(M\times N)$. Dann ist

$$\Phi(f) = \big(\pi_1(\rho_1 f_1\pi_1 + \rho_2 f_2\pi_2)\rho_1, \pi_2(\rho_1 f_1\pi_1 + \rho_2 f_2\pi_2)\rho_2\big) = (f_1, f_2).$$

Daher ist Φ auch surjektiv.

(iv) Man zeigt leicht, dass die Abbildungen

$$\begin{aligned} \mathrm{Hom}_R(M, N\times N') &\to \mathrm{Hom}_R(M, N)\times\mathrm{Hom}_R(M, N'), & f &\mapsto (\pi_1 f, \pi_2 f),\\ \mathrm{Hom}_R(M, N)\times\mathrm{Hom}_R(M, N') &\to \mathrm{Hom}_R(M, N\times N'), & (g_1, g_2) &\mapsto \rho_1 g_1 + \rho_2 g_2 \end{aligned}$$

zueinander inverse Isomorphismen von $\mathbb{Z}$-Moduln sind.

(v) Analog. □

8 Halbeinfache und artinsche Ringe

Bemerkung II.8.1. Wir übertragen die Endlichkeitsbedingungen für Moduln auf Ringe und werden feststellen, dass es (im Gegensatz zu Moduln) durchaus Abhängigkeiten zwischen den Begriffen gibt.

Definition II.8.2. Ein Ring R heißt (*links*)*noethersch* (bzw. (*links*)*artinsch*, (*links*)*halbeinfach*), falls der reguläre R-Linksmodul noethersch (bzw. artinsch, halbeinfach) ist.[1]

Beispiel II.8.3.

(i) Jeder Körper K ist noethersch, artinsch und halbeinfach, denn hier sind 0 und K die einzigen Linksideale.

(ii) Jeder Hauptidealring ist noethersch, denn hier ist jeder Untermodul ein Hauptideal und daher von nur einem Element erzeugt. Andererseits sind die Hauptidealringe $\mathbb{Z}$ und $K[X]$ nicht artinsch (siehe Beispiel II.7.5).

(iii) Der (endliche) Ring $\mathbb{Z}/4\mathbb{Z}$ ist artinsch, aber nicht halbeinfach.

(iv) Sei K ein Körper, $n \in \mathbb{N}$ und $R := K^{n\times n}$. Jedes Linksideal $M \leq R$ ist dann ein K-Vektorraum wegen $\lambda m = (\underbrace{\lambda 1_n}_{\in R})m \in M$ für alle $m \in M$ und $\lambda \in K$. Aus Dimensionsgründen ist R sowohl noethersch als auch artinsch.

(v) Sei nun Q ein Schiefkörper, $n \in \mathbb{N}$ und $R := Q^{n\times n}$. Die Menge der Spaltenvektoren $Q^{n\times 1}$ ist offenbar ein R-Modul bzgl. Matrizenmultiplikation. Sei $0 \neq a = (a_1, \ldots, a_n)^{\mathrm{t}} \in Q^{n\times 1}$ und $b \in Q^{n\times 1}$ beliebig. Sei $a_i \neq 0$ und $x := ba_i^{-1}e_i \in R$, wobei $e_i := (0, \ldots, 0, 1, 0, \ldots, 0)$. Dann gilt $xa = b$. Dies zeigt, dass $Q^{n\times 1}$ einfach ist. Offenbar ist dann

$$R = Q^{n\times 1}e_1 \oplus \ldots \oplus Q^{n\times 1}e_n \simeq (Q^{n\times 1})^n$$

halbeinfach. Nach Bemerkung II.7.9 ist außerdem jeder einfache R-Modul zu $Q^{n\times 1}$ isomorph.

Lemma II.8.4.

(i) Ist R noethersch (bzw. artinsch), so ist jeder endlich erzeugt R-Modul noethersch (bzw. artinsch).

(ii) Ist R halbeinfach, so ist jeder R-Modul halbeinfach.

Beweis.

(i) Sei $M = Rm_1 + \ldots + Rm_k$. Dann ist die Abbildung $f\colon R^k \to M$, $(r_1, \ldots, r_k) \mapsto r_1m_1 + \ldots + r_km_k$ ein Epimorphismus. Nach Bemerkung II.7.7 und Lemma II.7.6 sind R^k und $M \simeq R^k/\mathrm{Ker}(f)$ noethersch (bzw. artinsch).

[1] Achtung: In den meisten Büchern ist noethersch = linksnoethersch + rechtsnoethersch (vgl. Aufgabe II.38). Genauso mit artinsch und halbeinfach.

(ii) Wegen $R = \sum_{m\in M} Rm$ genügt es zu zeigen, dass Rm halbeinfach ist. Dies folgt aus Lemma II.7.10, denn für $f\colon R \to Rm$, $r \mapsto rm$ gilt $Rm \simeq R/\mathrm{Ker}(f)$. □

Satz II.8.5 (Artin-Wedderburn). *Für jeden Ring R sind die folgenden Aussagen äquivalent:*

(1) R ist halbeinfach.

(2) Es existieren $n_1, \ldots, n_k \in \mathbb{N}$ und Schiefkörper $Q_1, \ldots, Q_k$ mit

$$R \cong Q_1^{n_1\times n_1} \times \ldots \times Q_k^{n_k\times n_k}.$$

Gegebenenfalls ist k die Anzahl der Isomorphieklassen einfacher R-Moduln und die Paare (n_i, Q_i) sind bis auf die Reihenfolge (und Isomorphie) eindeutig bestimmt.

Beweis.

(1) ⇒ (2): Sei R halbeinfach und $R = \bigoplus_{i\in I} M_i$ mit einfachen Untermoduln $M_i \leq R$ für $i \in I$. Dann ist $1 = x_1 + \ldots + x_n$ mit o. B. d. A. $x_i \in M_i \setminus \{0\}$ für $i = 1, \ldots, n$. Aus der Einfachheit der M_i folgt $M_i = Rx_i$ für $i = 1, \ldots, n$. Daher ist

$$R = R1 \subseteq Rx_1 + \ldots + Rx_n = M_1 \oplus \ldots \oplus M_n \subseteq R.$$

Nach Umnummerierung gilt also $R \simeq M_1^{n_1} \oplus \ldots \oplus M_k^{n_k}$ mit $M_i \not\simeq M_j$ für $i \neq j$. Nach Schurs Lemma ist $\mathrm{Hom}_R(M_i, M_j) = 0$ für $i \neq j$ und $\mathrm{End}_R(M_i)$ ist ein Schiefkörper. Damit ist auch $Q_i := \mathrm{End}_R(M_i)^o$ ein Schiefkörper für $i = 1, \ldots, k$. Aus Lemma II.7.20 folgt

$$\begin{aligned} R &\cong \mathrm{End}_R(R)^o \cong \mathrm{End}_R(M_1^{n_1} \times \ldots \times M_k^{n_k})^o \cong (\mathrm{End}_R(M_1^{n_1}) \times \ldots \times \mathrm{End}_R(M_k^{n_k}))^o \\ &\cong (\mathrm{End}_R(M_1)^{n_1\times n_1} \times \ldots \times \mathrm{End}_R(M_k)^{n_k\times n_k})^o \\ &\cong (\mathrm{End}_R(M_1)^{n_1\times n_1})^o \times \ldots \times (\mathrm{End}_R(M_k)^{n_k\times n_k})^o. \end{aligned}$$

Schließlich ist die Transpositionsabbildung $(\mathrm{End}_R(M_i)^{n_i\times n_i})^o \to (\mathrm{End}_R(M_i)^o)^{n_i\times n_i} = Q_i^{n_i\times n_i}$, $A \mapsto A^{\mathrm{t}}$ ein Ringisomorphismus, denn

$$(BA)^{\mathrm{t}} = \Big(\sum_{k=1}^{n} b_{jk}a_{ki}\Big)_{i,j} = \Big(\sum_{k=1}^{n} a_{ki} * b_{jk}\Big)_{i,j} = A^{\mathrm{t}} * A^{\mathrm{t}}.$$

Also hat R die angegebene Struktur.

(2) ⇒ (1): Nach Beispiel II.8.3 sind die Ringe $R_i := Q_i^{n_i\times n_i}$ halbeinfach und es gilt $R_i = M_{i1} \oplus \ldots \oplus M_{in_i}$ mit einfachen R_i-Moduln $M_{i1} \simeq \ldots \simeq M_{in_i}$. Offenbar sind dann

$$\widetilde{M}_{ij} := 0 \times \ldots \times 0 \times M_{ij} \times 0 \times \ldots \times 0 \qquad (1 \leq i \leq k,\ 1 \leq j \leq n_i)$$

einfache R-Moduln mit

$$R = \bigoplus_{i=1}^{k} \bigoplus_{j=1}^{n_i} \widetilde{M}_{ij}.$$

Also ist auch R halbeinfach. Offenbar sind $\widetilde{M}_{i1}, \ldots, \widetilde{M}_{in_i}$ auch isomorph als R-Moduln. Andererseits liegt $(1_{n_1}, \ldots, 1_{n_{i-1}}, 0, 1_{n_{i+1}}, \ldots, 1_{n_k})$ im Annullator von $\widetilde{M}_{i1}$, aber nicht im Annullator von $\widetilde{M}_{j1}$ falls $i \neq j$. Nach Lemma II.7.19 sind die R-Moduln $\widetilde{M}_{i1}$ und $\widetilde{M}_{j1}$ nicht isomorph (selbst wenn $R_i = R_j$). Nach Bemerkung II.7.9 kommt jeder einfache R-Modul als Kompositionsfaktor

von R vor. Daher ist k die Anzahl der Isomorphieklassen einfacher R-Moduln. Außerdem ist n_i als Vielfachheit des Kompositionsfaktors $\widetilde{M}_{i1}$ eindeutig durch R bestimmt. Für

$$e_i := (0, \ldots, 0, \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}, 0, \ldots, 0) \in R$$

gilt $e_i^2 = e_i$ und $Re_i = \widetilde{M}_{i1}$. Nach Lemma II.7.20 ist

$$\mathrm{End}_R(\widetilde{M}_{i1}) = \mathrm{End}_R(Re_i) \cong (e_i R e_i)^o = (0, \ldots, 0, \begin{pmatrix} Q_i & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}, 0, \ldots, 0)^o \cong Q_i^o.$$

Auf diese Weise wird auch der Isomorphietyp von Q_i durch R bestimmt. □

Folgerung II.8.6. *Jeder halbeinfache Ring ist artinsch.*

Beweis. Wie im Beweis von Satz II.8.5 ist $R = M_1 \oplus \ldots \oplus M_n$ mit einfachen Moduln $M_1, \ldots, M_n$. Offenbar ist dann $0 \leq M_1 \leq M_1 + M_2 \leq \ldots \leq R$ eine Kompositionsreihe des regulären R-Moduls. Nach Satz II.7.8 ist R artinsch. □

Satz II.8.7 (Wedderburn)**.** *Endliche Schiefkörper sind Körper.*

Beweis (Witt). Sei R ein endlicher Schiefkörper. Dann ist das Zentrum $Z := \mathrm{Z}(R)$ ein kommutativer Teilring von R. Wegen $xr = rx \Leftrightarrow rx^{-1} = x^{-1}r$ ist Z sogar ein Körper. Sei $q := |Z|$. Offenbar ist R ein Z-Vektorraum und daher $|R| = q^n$ für ein $n \in \mathbb{N}$. Wir nehmen indirekt $n > 1$ an. Für $x \in R$ ist auch der Zentralisator $\mathrm{C}_R(x) = \{r \in R : rx = xr\}$ ein Z-Vektorraum (nachrechnen) und es folgt $|\mathrm{C}_R(x)| = q^{a_x}$ für ein $a_x \leq n$. Sei S ein Repräsentantensystem für die Konjugationsklassen der Einheitengruppe $G := R^\times = R \setminus \{0\}$. Die Klassengleichung zeigt

$$\begin{aligned} q^n - 1 = |G| &= \sum_{x \in S} |G : \mathrm{C}_G(x)| = |\mathrm{Z}(G)| + \sum_{x \in S \setminus Z} |G : \mathrm{C}_G(x)| \\ &= |Z^\times| + \sum_{x \in S \setminus Z} \frac{|R \setminus \{0\}|}{|\mathrm{C}_R(x) \setminus \{0\}|} = q - 1 + \sum_{x \in S \setminus Z} \frac{q^n - 1}{q^{a_x} - 1}. \end{aligned} \tag{II.8.1}$$

Nach Lagrange ist $q^{a_x} - 1 = |\mathrm{C}_G(x)|$ ein Teiler von $|G| = q^n - 1$. Nach dem euklidischen Algorithmus existieren $s, t \in \mathbb{Z}$ mit

$$q^{\mathrm{ggT}(a_x, n)} = q^{sa_x + tn} = (q^{a_x})^s (q^n)^t \equiv 1 \pmod{q^{a_x} - 1}.$$

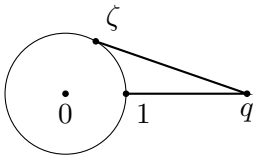
Aus $\mathrm{ggT}(a_x, n) \leq a_x$ folgt $a_x \mid n$ für alle $x \in R$.

Für alle $x \in R \setminus Z$ gilt $a_x < n$. Mit den Kreisteilungspolynomen ergibt sich

$$\Phi_n(q) \mid \prod_{\substack{d \mid n \\ d \nmid a_x}} \Phi_d(q) \overset{I.12.9}{=} \frac{q^n - 1}{q^{a_x} - 1} \mid q^n - 1.$$

Aus (II.8.1) folgt nun $\Phi_n(q) \mid q-1$. Insbesondere ist $|\Phi_n(q)| \leq q-1$. Für jede primitive n-te Einheitswurzel $\zeta := \alpha + \beta\mathrm{i}$ mit $\alpha, \beta \in \mathbb{R}$ ist $\alpha < 1$ wegen $n > 1$. Es folgt

$$\begin{aligned} |q-\zeta|^2 &= (q-\alpha)^2 + \beta^2 = q^2 - 2\alpha q + \alpha^2 + \beta^2 \\ &> q^2 - 2q + |\zeta|^2 = q^2 - 2q + 1 = (q-1)^2 \end{aligned}$$



und $|q-\zeta| > |q-1| \geq 1$. Damit erhält man den Widerspruch

$$|\Phi_n(q)| = \prod_{\substack{1 \leq k \leq n \\ \mathrm{ggT}(k,n)=1}} |q - \zeta^k| > |q-1|. \qquad \square$$

Definition II.8.8. Für einen R-Modul M sei $\mathrm{J}(M)$ der Durchschnitt aller maximalen Untermoduln von M. Besitzt M keine maximalen Untermoduln, so setzt man $\mathrm{J}(M) = M$. Man nennt $\mathrm{J}(M)$ das (*Jacobson-*)*Radikal* von M. Außerdem sei $\mathrm{J}(R)$ das Radikal des regulären R-Moduls.

Beispiel II.8.9.

(i) Sei M ein halbeinfacher R-Modul und $M = \bigoplus_{i \in I} S_i$ mit einfachen Untermoduln $S_i \leq M$ $(i \in I)$. Für $i \in I$ ist dann $M_i := \bigoplus_{j \in I \setminus \{i\}} S_j$ ein maximaler Untermodul von M, denn $M/M_i \simeq S_i$ ist einfach. Dies zeigt

$$\mathrm{J}(M) \subseteq \bigcap_{i \in I} M_i = 0.$$

(ii) Sei M ein artinscher R-Modul mit $\mathrm{J}(M) = 0$. Dann existieren bereits endlich viele maximale Untermoduln $M_1, \ldots, M_k \leq M$ mit $M_1 \cap \ldots \cap M_k = 0$ (anderenfalls könnte man eine absteigende Kette konstruieren). Da der kanonische Homomorphismus

$$\begin{aligned} M &\to M/M_1 \times \ldots \times M/M_k, \\ m &\mapsto (m + M_1, \ldots, m + M_k) \end{aligned}$$

injektiv ist, ist M zu einem Untermodul des halbeinfachen Moduls $M/M_1 \times \ldots \times M/M_k$ isomorph. Nach Lemma II.7.10 ist M selbst halbeinfach. Im Allgemeinen ist $\mathrm{J}(M)$ also der „kleinste“ Untermodul von M, sodass $M/\mathrm{J}(M)$ halbeinfach ist.

(iii) Für jeden Körper K und $n \in \mathbb{N}$ ist $\mathrm{J}(K^{n \times n}) = 0$ nach (i) (vgl. Aufgabe II.3).

(iv) Die maximalen Untermoduln von $\mathbb{Z}$ haben die Form $\mathbb{Z}p$ für $p \in \mathbb{P}$. Dies zeigt $\mathrm{J}(\mathbb{Z}) = 0$. Der einzige maximale Untermodul des $\mathbb{Z}$-Moduls C_4 ist C_2, also $\mathrm{J}(C_4) = C_2$.

Lemma II.8.10 (Nakayama)**.** *Sei M ein endlich erzeugter R-Modul und $N \leq M$ mit $M = N + \mathrm{J}(M)$. Dann ist $M = N$. Insbesondere ist $\mathrm{J}(M) < M$, falls $M \neq 0$.*

Beweis. Sei $M = Rm_1 + \ldots + Rm_k$. Nehmen wir $N \neq M$ an. Dann ist $\mathcal{M} := \{L < M : N \leq L\} \neq \varnothing$. Sei $\varnothing \neq \mathcal{W} \subseteq \mathcal{M}$ total geordnet. Wie üblich ist $L := \bigcup_{W \in \mathcal{W}} W \leq M$. Im Fall $L = M$ existiert ein $W \in \mathcal{W}$ mit $m_1, \ldots, m_k \in W$. Dann erhält man den Widerspruch $M = Rm_1 + \ldots + Rm_k \subseteq W < M$. Also ist $L \in \mathcal{M}$ eine obere Schranke für $\mathcal{W}$. Nach Zorn existiert daher ein maximaler Untermodul $S \leq M$, der N enthält. Man erhält den Widerspruch $M = N + \mathrm{J}(M) \subseteq S < M$. $\square$

Lemma II.8.11. *Sei $R \neq \{0\}$ ein Ring und sei $\mathcal{M}$ ein Repräsentantensystem für die Isomorphieklassen einfacher R-Moduln. Dann gilt*

$$\mathrm{J}(R) = \bigcap_{M \in \mathcal{M}} \mathrm{Ann}_R(M).$$

Insbesondere ist $\mathrm{J}(R)$ ein echtes Ideal von R.

Beweis. Nach Beispiel II.6.15 ist $\mathcal{M} \neq \varnothing$. Für $0 \neq m \in M \in \mathcal{M}$ ist die Abbildung $f\colon R \to M$, $r \to rm$ ein Epimorphismus. Nach dem Homomorphiesatz ist $R/\mathrm{Ker}(f) \simeq M$ einfach und $\mathrm{Ker}(f)$ ist ein maximales Linksideal. Daher ist $\mathrm{J}(R) \subseteq \mathrm{Ker}(f)$ und $\mathrm{J}(R)m = 0$. Dies zeigt $\mathrm{J}(R) \subseteq \mathrm{Ann}_R(M)$ und

$$\mathrm{J}(R) \subseteq \bigcap_{M \in \mathcal{M}} \mathrm{Ann}_R(M) =: A$$

Sei umgekehrt $N \leq R$ ein maximales Linksideal. Dann existiert ein $M \in \mathcal{M}$ mit $R/N \simeq M$. Nach Lemma II.7.19 ist $A \subseteq \mathrm{Ann}_R(M) = \mathrm{Ann}_R(R/N)$. Daher gilt

$$(A + N)/N \subseteq (AR + N)/N = A(R/N) = 0$$

und $A \subseteq N$. Dies zeigt $A \subseteq \mathrm{J}(R)$. Als Durchschnitt von Idealen ist $\mathrm{J}(R) = A \trianglelefteq R$ (Lemma II.7.19). Wegen $\mathcal{M} \neq \varnothing$ ist $\mathrm{J}(R) \neq R$. □

Bemerkung II.8.12. Für jeden halbeinfachen R-Modul M ist $\mathrm{J}(R)M = 0$ nach Lemma II.8.11. Für $r + \mathrm{J}(R) = s + \mathrm{J}(R)$ und $m \in M$ gilt daher $rm = (r - s + s)m = (r - s)m + sm = sm$. Durch

$$(r + \mathrm{J}(R))m := rm \qquad (r \in R,\ m \in M)$$

wird M also zu einem $R/\mathrm{J}(R)$-Modul (wohldefiniert). Die einfachen R-Moduln entsprechen auf diese Weise den einfachen $R/\mathrm{J}(R)$-Moduln. Also ist M auch halbeinfach als $R/\mathrm{J}(R)$-Modul. Umgekehrt ist jeder halbeinfache $R/\mathrm{J}(R)$-Modul auch halbeinfach als R-Modul.

Lemma II.8.13. *Sei R artinsch und M ein endlich erzeugter R-Modul. Dann ist $R/\mathrm{J}(R)$ ein halbeinfacher Ring und $\mathrm{J}(M) = \mathrm{J}(R)M$.*

Beweis. Mit R ist auch der R-Modul $R/\mathrm{J}(R)$ artinsch. Nach dem Korrespondenzsatz gilt $\mathrm{J}(R/\mathrm{J}(R)) = 0$. Also ist $R/\mathrm{J}(R)$ ein halbeinfacher R-Modul nach Beispiel II.8.9. Nach Bemerkung II.8.12 ist auch der reguläre $R/\mathrm{J}(R)$-Modul halbeinfach.

Nach Lemma II.8.4 ist M artinsch mit $\mathrm{J}(M/\mathrm{J}(M)) = 0$. Nach Beispiel II.8.9 ist $M/\mathrm{J}(M)$ halbeinfach und $\mathrm{J}(R)(M/\mathrm{J}(M)) = 0$. Dies zeigt $\mathrm{J}(R)M \subseteq \mathrm{J}(M)$. Andererseits $M/\mathrm{J}(R)M$ ein $R/\mathrm{J}(R)$-Modul. Mit $R/\mathrm{J}(R)$ ist auch $M/\mathrm{J}(R)M$ halbeinfach (Lemma II.8.4). Es folgt $\mathrm{J}(M/\mathrm{J}(R)M) = 0$ und $\mathrm{J}(M) \subseteq \mathrm{J}(R)M$. □

Bemerkung II.8.14.

(i) Ein Ring $R \neq \{0\}$ heißt *einfach*, falls 0 und R die einzigen Ideale von R sind. Aus Lemma II.8.11 folgt dann $\mathrm{J}(R) = 0$. Leider sind nicht alle einfachen Ringe halbeinfach (Aufgabe II.47). Ist aber R zusätzlich artinsch, so ist R nach Lemma II.8.13 halbeinfach. Nach Artin-Wedderburn ist dann R zu einem Matrixring über einem Schiefkörper isomorph. Umgekehrt sind solche Matrixringe stets einfach (vgl. Aufgabe II.3).

(ii) Für $I, J \trianglelefteq R$ ist nach Aufgabe I.37 auch

$$IJ = \Big\{ \sum_{i=1}^{n} x_i y_j : x_1, \ldots, x_n \in I, y_1, \ldots, y_n \in J \Big\}$$

ein Ideal von R mit $IJ \subseteq I \cap J$. Wir definieren $I^0 := R$ und induktiv $I^{n+1} := II^n$ für $n \in \mathbb{N}$. Es gilt dann $R \supseteq I \supseteq I^2 \supseteq \ldots$. Existiert ein $n \in \mathbb{N}$ mit $I^n = 0$, so nennt man I *nilpotent*.

Lemma II.8.15. *Ist R artinsch, so ist $\mathrm{J}(R)$ nilpotent und jedes nilpotente Ideal von R liegt in $\mathrm{J}(R)$.*

Beweis. Da der reguläre R-Modul artinsch ist, wird die Folge $J := J(R) \supseteq J(R)^2 \supseteq \ldots$ stationär. Sei also $k \in \mathbb{N}$ mit $J^k = J^{k+1} = \ldots$. Nehmen wir $J^k \neq 0$. Dann ist die Menge $\mathcal{M}$ aller Linksideale $I \leq R$ mit $J^k I \neq 0$ nichtleer und besitzt somit ein minimales Element $I \in \mathcal{M}$. Insbesondere existiert ein $x \in I$ mit $J^k x \neq 0$. Mit J^k ist auch $J^k x$ ein Linksideal und es gilt

$$J^k(J^k x) = J^{2k} x = J^k x \neq 0,$$

d. h. $J^k x \in \mathcal{M}$. Wegen $J^k x \subseteq Rx \subseteq I$ folgt $I = J^k x$ aus der Minimalität von I. Daher ist $x = yx$ für ein $y \in J^k \subseteq J$. Nach Aufgabe II.45 ist $1 - y \in R^\times$ und es folgt der Widerspruch $x \in Rx = R(1-y)x = R(x - yx) = 0$. Also ist $\mathrm{J}(R)$ nilpotent.

Sei umgekehrt $I \trianglelefteq R$ nilpotent. Dann ist $\bar{I} := (I + \mathrm{J}(R))/\mathrm{J}(R)$ ein nilpotentes Ideal des halbeinfachen Rings $\overline{R} := R/\mathrm{J}(R)$. Sei $\overline{R} = Q_1^{n_1 \times n_1} \times \ldots \times Q_k^{n_k \times n_k}$ die Artin-Wedderburn-Zerlegung. Dann ist auch die Projektion von $\bar{I}$ auf $Q_i^{n_i \times n_i}$ ein nilpotentes Ideal $\bar{I}_i$. Nach Bemerkung II.8.14 ist $Q_i^{n_i \times n_i}$ einfach und es folgt $\bar{I}_i = 0$ für $i = 1, \ldots, k$. Dies zeigt $\bar{I} = 0$ und $I \subseteq \mathrm{J}(R)$. □

Satz II.8.16 (Hopkins-Levitzki)**.** *Jeder artinsche Ring ist noethersch.*

Beweis. Sei R artinsch. Nach Lemma II.8.15 existiert ein $k \in \mathbb{N}$ mit $\mathrm{J}(R)^k = 0$. Nach Lemma II.7.6 sind die R-Moduln $J_i := \mathrm{J}(R)^{i-1}/\mathrm{J}(R)^i$ für $i = 1, \ldots, k$ artinsch. Dabei gilt

$$\mathrm{J}(J_i) \overset{II.8.13}{=} \mathrm{J}(R)\mathrm{J}(R)^{i-1}/\mathrm{J}(R)^i = 0.$$

Nun ist J_i halbeinfach nach Beispiel II.8.9. Aus Beispiel II.7.5 folgt, dass J_i noethersch ist. Nach Lemma II.7.6 sind mit $J_k, J_{k-1}, \ldots, J_1$ auch $\mathrm{J}(R)^{k-1} \simeq J_k$, $\mathrm{J}(R)^{k-2}, \ldots, \mathrm{J}(R)^0 = R$ noethersch. Also ist R als Ring noethersch. □

Bemerkung II.8.17.

(i) Für Ringe haben wir gezeigt: halbeinfach $\Longrightarrow$ artinsch $\Longrightarrow$ noethersch. Die Umkehrungen sind jeweils falsch (Beispiel II.8.3).

(ii) Im Folgenden studieren wir die Struktur artinscher Ringe R. Nach Lemma II.8.4, Satz II.7.8 und Krull-Schmidt besitzt jeder endlich erzeugte R-Modul eine Kompositionsreihe und eine „eindeutige“ Zerlegung in unzerlegbare Moduln. Nach Lemma II.8.13 und Artin-Wedderburn ist R genau dann halbeinfach, wenn $\mathrm{J}(R) = 0$.

Definition II.8.18. Idempotente e, f eines Rings R heißen *orthogonal*, falls $ef = fe = 0$. Besitzt $e \neq 0$ keine Zerlegung $e = e_1 + e_2$ mit orthogonalen Idempotenten $e_1, e_2 \in R \setminus \{0\}$, so nennt man e *primitiv*. Man nennt e *zentral-primitiv*, falls $e \in \mathrm{Z}(R)$ und e primitiv in $\mathrm{Z}(R)$ ist.

Beispiel II.8.19.

(i) Ist $e \in R$ ein Idempotent, so auch $1-e$ und e ist orthogonal zu $1-e$, denn $e(1-e) = e - e^2 = e - e = 0 = (1-e)e$.

(ii) Sind $e, f \in R$ orthogonale Idempotente, so ist auch $e+f$ ein Idempotent, denn $(e+f)^2 = e^2 + ef + fe + f^2 = e + f$.

(iii) Ist $e \in R$ ein (primitives) Idempotent und $x \in R^\times$, so ist auch xex^{-1} ein (primitives) Idempotent.

(iv) Sei Q ein Schiefkörper und $R := Q^{n\times n}$. Die Matrizen $E_{kk} := (\delta_{ik}\delta_{jk})_{i,j} \in A$ (δ_{is} ist das Kronecker-Delta) mit einer Eins an Position (k,k) und sonst nur Nullen sind offenbar paarweise orthogonale Idempotente mit

$$1_n = E_{11} + \ldots + E_{nn}.$$

Lemma II.8.21 wird zeigen, dass 1_n zentral-primitiv und E_{kk} primitiv ist, denn R ist ein einfacher Ring (Bemerkung II.8.14) und $AE_{kk} = Q^{n\times 1}$ ist ein einfacher R-Modul (Beispiel II.8.3).

(v) Sei K ein Körper und $e \in K^{n\times n}$ ein Idempotent. Dann ist das Minimalpolynom von e ein Teiler von $X^2 - X$. Insbesondere ist e diagonalisierbar mit Eigenwerten $0, 1$ (zum Beispiel nach der Weierstraß-Normalform, Bemerkung II.10.7). Daher existiert $x \in \mathrm{GL}(n, K)$ mit $xex^{-1} = E_{11} + \ldots + E_{kk}$ für ein $0 \leq k \leq n$.

Bemerkung II.8.20. Im Folgenden nennen wir ein Ideal I eines Rings R *unzerlegbar*, wenn es keine Ideale $I_1, I_2 \neq 0$ von R mit $I = I_1 \oplus I_2$ gibt.

Lemma II.8.21. *Für jedes Idempotent e eines Ring R gilt:*

(i) Genau dann ist e primitiv, wenn der R-Modul Re unzerlegbar ist.

(ii) Genau dann ist e zentral-primitiv, wenn $e \in \mathrm{Z}(R)$ und das Ideal $Re \trianglelefteq R$ unzerlegbar ist.

Beweis. Sei $e = e_1 + e_2$ mit orthogonalen Idempotenten $e_1, e_2 \in R \setminus \{0\}$. Dann ist $Re \subseteq Re_1 + Re_2$ und $Re_i = Re_i^2 = Re_i e \subseteq Re$ für $i = 1, 2$. Wegen $e_i = e_i^2 \in Re_i$ ist $Re_i \neq 0$. Für $x \in Re_1 \cap Re_2$ gilt $x = xe_1 = xe_1e_2 = 0$. Dies zeigt $R = Re_1 \oplus Re_2$. Sind zusätzlich $e, e_1, e_2 \in \mathrm{Z}(R)$, so sind $Re = ReR$ und $Re_i = Re_iR$ Ideale.

Sei umgekehrt $Re = R_1 \oplus R_2$ mit nicht-trivialen Linksidealen I_1, I_2. Dann existieren $e_i \in I_i$ mit $e = e_1 + e_2$. Im Fall $e_1 = 0$ wäre $Re = Re_2 \subseteq I_2$. Also gilt $e_1 \neq 0 \neq e_2$. Aus $e_1 \in Re$ folgt $e_1 = e_1e = e_1^2 + e_1e_2$. Die eindeutige Darstellung in der direkten Summe zeigt $e_1^2 = e_1$ und $e_1e_2 = 0$. Analog ist $e_2^2 = e_2$ und $e_2e_1 = 0$. Also sind e_1 und e_2 orthogonale Idempotente und e ist nicht primitiv. Sind $I_1, I_2 \trianglelefteq R$ und $e \in \mathrm{Z}(R)$, so gilt $ae_1 + ae_2 = ae = ea = e_1a + e_2a$ und es folgt $ae_i = e_ia$ für alle $a \in R$. Dies zeigt $e_1, e_2 \in \mathrm{Z}(R)$ und e ist nicht zentral-primitiv. □

Satz II.8.22. *Sei R ein artinscher Ring. Dann existieren paarweise orthogonale primitive Idempotente $e_1, \ldots, e_n \in R$ mit $1 = e_1 + \ldots + e_n$. Ist auch $1 = f_1 + \ldots + f_m$ eine solche Zerlegung, so ist $n = m$ und es existiert $x \in R^\times$ mit $e_i = xf_ix^{-1}$ für $i = 1, \ldots, n$ bei geeigneter Anordnung. Außerdem ist*

$$R = Re_1 \oplus \ldots \oplus Re_n$$

eine Zerlegung in unzerlegbare Moduln.

Beweis. Nach Krull-Schmidt besitzt der reguläre R-Modul eine Zerlegung in unzerlegbare Linksideale $R = R_1 \oplus \ldots \oplus R_n$. Sei $e_i \in R_i$ mit $1 = e_1 + \ldots + e_n$. Wie im Beweis von Lemma II.8.21 zeigt man, dass $e_1, \ldots, e_n$ paarweise orthogonale primitive Idempotente sind. Sei auch $1 = f_1 + \ldots + f_m$ eine solche Zerlegung. Nach Lemma II.8.21 ist $R = Rf_1 \oplus \ldots \oplus Rf_m$ eine Zerlegung in unzerlegbare R-Moduln. Nach Krull-Schmidt ist $n = m$ und bei geeigneter Anordnung existieren Isomorphismen $\gamma_i \colon R_i \to Rf_i$. Offenbar definiert

$$\begin{aligned} \gamma &\colon R \to R, \\ a_1 + \ldots + a_n &\mapsto \gamma_1(a_1) + \ldots + \gamma_n(a_n) \qquad (a_i \in R_i) \end{aligned}$$

einen Automorphismus des regulären R-Modul. Sei $x := \gamma(1)$ und $y := \gamma^{-1}(1)$. Aus $xy = \gamma^{-1}(x1) = \gamma^{-1}(\gamma(1)) = 1 = yx$ folgt $x = y^{-1} \in R^\times$. Wegen

$$\begin{aligned} e_1 + \ldots + e_n = 1 = \gamma^{-1}(x) &= \gamma^{-1}(xf_1 1 + \ldots + xf_n 1) \\ &= \underbrace{xf_1\gamma^{-1}(1)}_{\in R_1} + \ldots + \underbrace{xf_n\gamma^{-1}(1)}_{\in R_n} = xf_1x^{-1} + \ldots + xf_nx^{-1} \end{aligned}$$

ist $e_i = xf_ix^{-1}$ für $i = 1, \ldots, n$. □

Satz II.8.23 (Peirce)**.** *Sei R artinsch. Dann existieren nur endlich viele zentral-primitive Idempotente $z_1, \ldots, z_k \in \mathrm{Z}(R)$. Es gilt $1 = z_1 + \ldots + z_k$ und*

$$R = Rz_1 \oplus \ldots \oplus Rz_k,$$

wobei $Rz_1, \ldots, Rz_k$ die unzerlegbaren Ideale von R sind. Außerdem ist $Rz_i = z_iRz_i$ ein Ring mit Einselement z_i für $i = 1, \ldots, k$.

Beweis. Eine Anwendung von Satz II.8.22 auf $\mathrm{Z}(R)$ liefert $1 = z_1 + \ldots + z_k$ mit paarweise orthogonalen zentral-primitiven Idempotenten $z_1, \ldots, z_k \in \mathrm{Z}(R)$. Sei umgekehrt $w \in \mathrm{Z}(R)$ ein zentral-primitives Idempotent. Dann kann man $R = Rw \oplus R(1-w)$ zu einer Zerlegung in unzerlegbare Moduln verfeinern. Nach Lemma II.8.21 erhält man eine entsprechende Zerlegung in paarweise orthogonale zentral-primitive Idempotente $1 = w_1 + \ldots + w_k$ mit $w = w_1$. Nach Satz II.8.22 existiert $x \in \mathrm{Z}(R)^\times$ mit $w = xz_ix^{-1} = z_i$ für ein $1 \leq i \leq k$ (beachte: $\mathrm{Z}(R)$ ist kommutativ). Also sind $z_1, \ldots, z_k$ die einzigen zentral-primitiven Idempotente. Nach Lemma II.8.21 ist $R = Rz_1 \oplus \ldots \oplus Rz_k$ die einzige Zerlegung in unzerlegbare Ideale. Die letzte Behauptung folgt aus Aufgabe II.7. □

Bemerkung II.8.24.

(i) Ist $R = Q_1^{n_1 \times n_1} \oplus \ldots \oplus Q_k^{n_k \times n_k}$ halbeinfach mit Schiefkörpern $Q_1, \ldots, Q_k$, so sind $Q_i^{n_i \times n_i}$ unzerlegbare (sogar minimale) Ideale von R. Die Peirce-Zerlegung stimmt also mit der Artin-Wedderburn-Zerlegung überein.

(ii) In der Situation von Satz II.8.23 nennt man $Rz_1, \ldots, Rz_k$ die *Blöcke* von R. Außerdem nennt man z_i das *Blockidempotent* von Rz_i. Das nächste Resultat führt die Bestimmung der einfachen Moduln von R auf die potentiell „kleineren“ Blöcke zurück.

(iii) Die Zerlegung $1 = z_1 + \ldots + z_k$ in zentral-primitive Idempotente lässt sich zu einer Zerlegung in paarweise orthogonale primitive Idempotente verfeinern, indem man Krull-Schmidt auf jeden Block anwendet.

Satz II.8.25. *Sei R artinsch und M ein unzerlegbarer R-Modul. Dann existiert genau ein Block B von R mit $BM \neq 0$. Gegebenenfalls ist M ein B-Modul. Umgekehrt ist jeder B-Modul auch ein R-Modul. Dabei gilt*

(i) Genau dann ist ein B-Modul M einfach (bzw. unzerlegbar), wenn M als R-Modul einfach (bzw. unzerlegbar) ist.

(ii) Zwei B-Moduln sind genau dann isomorph, wenn sie als R-Moduln isomorph sind.

Beweis. Seien $B_1, \ldots, B_k$ die Blöcke von R und $e_1, \ldots, e_k$ die entsprechenden Blockidempotente. Dann gilt $M = RM = B_1M + \ldots + B_kM$, wobei $B_1M, \ldots, B_kM$ nach Beispiel II.6.8 Untermoduln von M sind. Seien $b_i \in B_i$ und $m_1, \ldots, m_k \in M$ mit $b_1m_1 + \ldots + b_km_k = 0$. Dann gilt

$$b_im_i = e_i(b_1m_1 + \ldots + b_km_k) = 0$$

für $i = 1, \ldots, k$. Also ist $M = B_1M \oplus \ldots \oplus B_kM$. Da M unzerlegbar ist, folgt $B_iM \neq 0$ und $B_jM = 0$ für ein i und alle $j \neq i$. Für jeden Untermodul $N \leq M$ gilt $N = RN = B_iN$. Insbesondere ist M als B-Modul einfach (bzw. unzerlegbar), wenn M als R-Modul einfach (bzw. unzerlegbar) ist. Sei schließlich $f\colon M \to N$ ein Isomorphismus von R-Moduln. Dann gilt

$$B_iN = B_if(M) = f(B_iM) = f(M) = N.$$

Also sind M und N auch als B-Moduln isomorph.

Sei umgekehrt M ein B_i-Modul. Man prüft leicht, dass M durch $r \cdot m := re_im$ für $r \in R$ und $m \in M$ zu einem R-Modul wird. Natürlich können auch die B-Untermoduln von M als R-Moduln aufgefasst werden. Daraus folgt (i). Sei $f\colon M \to N$ ein Isomorphismus von B-Moduln. Für $r \in R$ und $m \in M$ gilt $f(rm) = f(re_im) = re_if(m) = rf(m)$. Daher sind M und N auch als R-Moduln isomorph. □

Bemerkung II.8.26. Die folgenden Ergebnisse gelten für beliebige Ringe R. Wir benutzen dabei, dass jeder R-Modul M auch ein $\mathrm{End}_R(M)$-Modul ist via $\varphi \cdot m := \varphi(m)$ für $\varphi \in \mathrm{End}_R(M)$ und $m \in M$ (Bemerkung II.6.11).

Lemma II.8.27. *Sei S ein einfacher R-Modul und $D := \mathrm{End}_R(S)$. Sei $T \subseteq S$ eine endliche Teilmenge und $L := \{r \in R : rT = 0\}$. Für $s \in S$ mit $Ls = 0$ gilt dann $s \in DT$.*

Beweis. Induktion nach $|T|$. Im Fall $T = \varnothing$ ist $L = R$ und $s = 0 \in DT$. Sei also $t \in T$ und die Behauptung für $T' := T \setminus \{t\}$ bereits gezeigt. Sei

$$L' := \{r \in R : rT' = 0\}.$$

Im Fall $L't = 0$ ist $L' = L$ und $s \in DT' \subseteq DT$ nach Induktion. Sei also $L't \neq 0$. Offenbar ist $L't$ ein R-Untermodul von S und die Einfachheit von S liefert $L't = S$. Wir betrachten $f\colon S \to S$, $xt \mapsto xs$ mit $x \in L'$. Sind $x, y \in L'$ mit $xt = yt$, so ist $(x - y)t = 0$, also $x - y \in L$ und es folgt $xs = ys$. Daher ist f wohldefiniert und offenbar auch R-linear, d. h. $f \in D$. Für $x \in L'$ folgt

$$x(s - f(t)) = xs - xf(t) = xs - f(xt) = 0.$$

Also ist $L'(s - f(t)) = 0$ und $s - f(t) \in DT'$ nach Induktion. Dies zeigt $s \in DT$. □

Satz II.8.28 (Jacobsons Dichtheitssatz)**.** *Sei S ein einfacher R-Modul und $Q := \mathrm{End}_R(S)$. Sei $T \subseteq S$ eine endliche Teilmenge und $f \in \mathrm{End}_Q(S)$. Dann existiert ein $x \in R$ mit $f(t) = xt$ für alle $t \in T$.*

Beweis. Induktion nach $|T|$: O. B. d. A. sei $T \neq \varnothing$, $s \in T$ und $T' := T \setminus \{s\}$. Nach Induktion existiert $x' \in R$ mit $f(t) = x't$ für alle $t \in T'$. Nehmen wir zunächst $s = \sum_{t \in T'} \lambda_t t$ mit $\lambda_t \in Q$ an. Dann gilt

$$f(s) = \sum_{t \in T'} \lambda_t f(t) = \sum_{t \in T'} \lambda_t x't = \sum_{t \in T'} \lambda_t (x't) = x' \sum_{t \in T'} \lambda_t t = x's.$$

Sei nun $s \notin DT$ und $L := \{r \in R : rT' = 0\}$. Nach Lemma II.8.27 ist dann $Ls \neq 0$. Wie üblich ist $Ls = S$ und es existiert $r \in L$ mit $rs = f(s) - x's$. Für $x := x' + r \in R$ und $t \in T$ gilt nun

$$f(t) = \begin{cases} x't = xt & \text{falls } t \neq s, \\ xt & \text{falls } t = s. \end{cases}$$

□

Bemerkung II.8.29.

(i) Ist S in der Situation von Satz II.8.28 als Q-Modul endlich erzeugt, so kann man für T ein Erzeugendensystem wählen. Man erhält dann $R/\mathrm{Ann}_R(S) \cong \mathrm{End}_Q(S)$. Wir zeigen in Folgerung II.9.12, dass $\mathrm{End}_Q(S)$ ein Matrixring über dem Schiefkörper Q^o ist. Dies ist eine weitere Verallgemeinerung von Artin-Wedderburn.

(ii) In Kapitel III.1 beschäftigen wir uns mit kommutativen noetherschen Ringen.

9 Moduln über Hauptidealringen

Definition II.9.1.

(i) Eine Teilmenge S eines R-Moduls M heißt (wie in Bemerkung II.2.1) *linear abhängig*, falls paarweise verschiedene $s_1, \dots, s_n \in S$ ($n \in \mathbb{N}$) und $r_1, \dots, r_n \in R \setminus \{0\}$ mit $\sum_{i=1}^n r_i s_i = 0$ existieren. Anderenfalls heißt S *linear unabhängig*. Man nennt M *frei*, falls M ein linear unabhängiges Erzeugendensystem E besitzt. Gegebenenfalls nennt man E eine *Basis* von M. Ein freier $\mathbb{Z}$-Modul heißt *freie abelsche Gruppe*.

(ii) Für jede Familie von R-Moduln $(M_i)_{i\in I}$ ist das *Koprodukt*

$$\coprod_{i\in I} M_i := \Big\{(m_i) \in \bigtimes M_i : \big|\{i \in I : m_i \neq 0\}\big| < \infty\Big\}$$

ein Untermodul von $\bigtimes_{i\in I} M_i$.

Bemerkung II.9.2. Ist M ein freier R-Modul mit Basis B, so gilt $M = \bigoplus_{b\in B} Rb$. Die Abbildung

$$\begin{aligned}\coprod_{b\in B} R &\to M,\\ (r_b)_{b\in B} &\mapsto \sum_{b\in B} r_b b\end{aligned}$$

ist dann ein Isomorphismus. Daher ist jeder freie Modul zu $\coprod_{b\in B} R$ isomorph für eine Menge B.

Beispiel II.9.3.

(i) Nach Satz II.2.2 ist jeder Vektorraum ein freier Modul.

(ii) Der triviale Modul 0 ist frei mit Basis $\varnothing$.

(iii) Der reguläre R-Modul ist frei mit Basis $\{1\}$. Allgemeiner ist auch $R^n = \coprod_{i=1}^n R$ ein freier R-Modul mit der Standardbasis $(1, 0, \dots, 0)$, $(0, 1, 0, \dots, 0), \dots, (0, \dots, 0, 1)$.

(iv) Eine endliche abelsche Gruppe A ist nur dann frei, wenn $A = 0$, denn die freien Moduln $\coprod \mathbb{Z}$ sind unendlich oder trivial.

Satz II.9.4. *Jeder R-Modul ist zu einem Faktormodul eines freien R-Moduls isomorph.*

Beweis. Sei M ein R-Modul. Dann ist die Abbildung $\coprod_{m\in M} R \to M$, $(r_m)_{m\in M} \mapsto \sum_{m\in M} r_m m$ ein Epimorphismus. Die Behauptung folgt aus dem Homomorphiesatz. □

Lemma II.9.5. *Jeder endlich erzeugte freie R-Modul besitzt eine endliche Basis.*

Beweis. Sei $M = Rm_1 + \ldots + Rm_k$ ein endlich erzeugter freier R-Modul mit Basis B. Dann lässt sich jedes m_i als Linearkombination von nur endlich vielen $b \in B$ schreiben. Daher existiert eine endliche Teilmenge $C \subseteq B$ mit

$$M = Rm_1 + \ldots + Rm_k \subseteq \bigoplus_{c \in C} Rc \subseteq M.$$

Also ist C eine endliche Basis von M. □

Beispiel II.9.6.

(i) Der obige Beweis zeigt, dass zwei Basen B und C eines freien Moduls entweder beide endlich oder beide unendlich sind. Im Gegensatz zu Vektorräumen kann aber $|B| \neq |C|$ gelten: Sei $S \neq 0$ ein beliebiger Ring, $M := \times_{i \in \mathbb{N}} S$ und $R := \mathrm{End}_S(M)$. Offenbar ist $M \times M \to M$, $((a_i)_i, (b_i)_i) \mapsto (a_1, b_1, a_2, b_2, \ldots)$ ein Isomorphismus von S-Moduln. Nach Lemma II.7.20 existiert ein $\mathbb{Z}$-Isomorphimus

$$F \colon R \times R \to \mathrm{Hom}_S(M \times M, M) \simeq R, \qquad (\varphi, \psi) \mapsto \varphi\pi_1 + \psi\pi_2,$$

wobei $\pi_i \colon M \times M \to M$ die i-te Projektion ist. Offenbar ist F auch R-linear. Für den regulären R-Modul gilt also $R \simeq R \times R \simeq R^3 \simeq \ldots$, d. h. R besitzt Basen von jeder endlichen Mächtigkeit. Wir zeigen im Folgenden, dass die Situation für Schiefkörper und Hauptidealringe wesentlich besser ist.

(ii) Mit etwas mehr Mengenlehre kann man zeigen, dass je zwei unendliche Basen eines freien Moduls gleichmächtig sind.

Satz II.9.7. *Ist R kommutativ, so sind je zwei Basen eines freien R-Moduls gleichmächtig.*

Beweis. Sei M ein freier R-Modul mit Basis B. Nach Krull existiert ein maximales Ideal $I \trianglelefteq R$. Dann ist $IM \leq M$ und $K := R/I$ ist ein Körper nach Satz I.7.12. Durch

$$(r + I)(m + IM) := rm + IM$$

wird der R-Modul M/IM zu einem K-Vektorraum mit Erzeugendensystem $\{b + IM : b \in B\}$. Wegen $M = \bigoplus_{b \in B} Rb$ ist

$$IM \subseteq \bigoplus_{b \in B} IRb \subseteq \bigoplus_{b \in B} Ib \subseteq IM.$$

Für

$$\sum_{b \in B} r_b b + IM = \sum_{b \in B} (r_b + I)(b + IM) = 0 \in M/IM$$

mit $r_b \in R$ folgt also $r_b \in I$ für alle $b \in B$. Daher ist $\{b + IM : b \in B\}$ auch eine K-Basis von M/IM. Nach Satz II.2.4 ist die Mächtigkeit von B eindeutig bestimmt. □

Definition II.9.8. Sei M ein freier Modul über einem kommutativen Ring. Die Mächtigkeit einer Basis von M bezeichnet man dann als *Rang* von M und schreibt dafür $\mathrm{rk}\, M$ (wohldefiniert nach Satz II.9.7).

Satz II.9.9. *Ein Ring $R \neq \{0\}$ ist genau dann ein Schiefkörper, wenn jeder R-Modul frei ist.*

Beweis. Sei R ein Schiefkörper. Nach Artin-Wedderburn ist R halbeinfach. Nach Lemma II.8.4 ist auch jeder R-Modul M halbeinfach. Sei also $M = \bigoplus_{i\in I} M_i$ mit einfachen R-Moduln $M_i \leq M$ $(i \in I)$. Für $0 \neq m_i \in M_i$ gilt dann $M_i = Rm_i$. Seien $r_1, \ldots, r_n \in R$ mit

$$\sum_{i=1}^{n} r_i m_i = 0.$$

Dann ist $r_1 m_1 = \ldots = r_n m_n = 0$. Im Fall $r_i \in R \setminus \{0\} = R^\times$ wäre $m_i = r_i^{-1} r_i m_i = 0$. Also ist $r_1 = \ldots = r_n = 0$ und $\{m_i : i \in I\}$ ist eine Basis von M.

Sei umgekehrt jeder R-Modul frei. Nach Beispiel II.6.15 existiert ein einfacher R-Modul M. Da M frei ist, gilt $M \simeq \coprod_{b\in B} R$ für eine Basis B von M. Die Einfachheit von M zeigt $|B| = 1$ und $M \simeq R$. Insbesondere ist der reguläre R-Modul einfach. Für jedes $x \in R \setminus \{0\}$ gilt daher $Rx = R$, d. h. jedes von Null verschiedene Element ist linksinvertierbar. Also ist $R \setminus \{0\}$ eine Gruppe und es folgt $R \setminus \{0\} = R^\times$. Somit ist R ein Schiefkörper. □

Satz II.9.10. *Sei R ein Schiefkörper und M ein R-Modul. Dann gilt*

(i) (*Basisergänzungssatz*) *Sei $E \subseteq M$ ein Erzeugendensystem von M und $U \subseteq E$ eine linear unabhängige Teilmenge. Dann besitzt M eine Basis B mit $U \subseteq B \subseteq E$.*

(ii) (*Austauschsatz*) *Für jede endliche linear unabhängige Teilmenge $U \subseteq M$ und jedes Erzeugendensystem E von M gilt $|U| \leq |E|$.*

(iii) Je zwei Basen von M haben die gleiche Mächtigkeit.

Beweis.

(i) Wir argumentieren wie in Satz II.2.2. Sei $\mathcal{M}$ die Menge aller linear unabhängigen Teilmengen $S \subseteq M$ mit $U \subseteq S \subseteq E$. Wegen $U \in \mathcal{M}$ ist $\mathcal{M}$ nichtleer und durch $\subseteq$ geordnet. Für eine total geordnete Teilmenge $\varnothing \neq \mathcal{N} \subseteq \mathcal{M}$ ist $\bigcup_{N\in\mathcal{N}} N \in \mathcal{M}$ eine obere Schranke von $\mathcal{N}$ (dafür benötigt man noch nicht, dass R ein Schiefkörper ist). Nach Zorn besitzt $\mathcal{M}$ ein maximales Element B. Für $e \in E \setminus B$ ist $B \cup \{e\}$ linear abhängig. Also existieren $r_b \in R$ $(b \in B)$ und $r_e \in R \setminus \{0\} = R^\times$ mit $r_e e + \sum_{b\in B} r_b b = 0$. Dies liefert $e = -r_e^{-1} \sum_{b\in B} r b_b \in \langle B\rangle$. Daher ist $M = \langle E\rangle \subseteq \langle B\rangle \subseteq M$ und B ist eine Basis von M.

(ii) Sei $U = \{u_1, \ldots, u_n\}$ und o. B. d. A. $E = \{e_1, \ldots, e_m\}$ (im Fall $|E| = \infty$ ist nichts zu tun). Da U linear unabhängig ist, gilt $0 \neq u_1 = \sum_{i=1}^{m} \lambda_i e_i$, wobei nicht alle $\lambda_1, \ldots, \lambda_m \in R$ verschwinden. Sei also o. B. d. A. $\lambda_1 \in R \setminus \{0\} = R^\times$ und daher

$$e_1 = \lambda_1^{-1} u_1 - \sum_{i=2}^{m} \lambda_1^{-1} \lambda_i e_i \in \langle u_1, e_2, \ldots, e_m\rangle.$$

Folglich ist auch $\{u_1, e_2, \ldots, e_m\}$ ein Erzeugendensystem mit m Elementen. Wegen $u_2 \notin \langle u_1\rangle$ kann man u_2 auf die gleiche Weise gegen ein e_i, sagen wir e_2, austauschen. Wiederholt man diesen Prozess, so erhält man schließlich das Erzeugendensystem $\{u_1, \ldots, u_n, e_{n+1}, \ldots, e_m\}$. Insbesondere ist $|U| = n \leq m = |E|$.

(iii) Hier argumentieren wir wie in Satz II.2.4. Seien B und C Basen von M. Für jedes $b \in B$ existiert eine endliche Teilmenge $C_b \subseteq C$ mit $c \in \sum_{c\in C_b} Rc$. Also ist

$$M = \sum_{b\in B} Rb = \sum_{b\in B} \sum_{c\in C_b} Rc.$$

Da C ein minimales Erzeugendensystem von M ist, folgt $C = \bigcup_{b\in B} C_b$. Sei $B_1 \subseteq B$ eine endliche Teilmenge und $C_1 := \bigcup_{b\in B_1} C_b$. Dann ist B_1 eine linear unabhängige Teilmenge im Modul $\langle C_1\rangle$ und (ii) zeigt $|B_1| \leq |C_1|$. Nach dem Heiratssatz existieren paarweise verschiedene $c_b \in C_b$ für $b \in B$. Die Abbildung $B \to C$, $b \mapsto c_b$ ist also injektiv. Aus Symmetriegründen muss es auch eine injektive Abbildung $C \to B$ geben und die Behauptung folgt aus Cantor-Bernstein. □

Bemerkung II.9.11. Ist $R \subseteq S$ eine Erweiterung von Schiefkörpern, so kann man S sowohl als freien R-Linksmodul als auch als freien R-Rechtsmodul auffassen. Selbst in dieser speziellen Situation müssen die entsprechenden Dimensionen nicht gleich sein. Es ist sogar möglich, dass eine Dimension endlich und die andere unendlich ist.[1]

Folgerung II.9.12. *Sei R ein Ring und S ein einfacher R-Modul, der über dem Schiefkörper $Q := \mathrm{End}_R(S)$ Dimension $d < \infty$ hat. Dann gilt $R/\mathrm{Ann}_R(S) \cong (Q^o)^{d\times d}$.*

Beweis. Es gilt

$$R/\mathrm{Ann}_R(S) \overset{II.8.29}{\cong} \mathrm{End}_Q(S) \cong \mathrm{End}_Q(Q^d) \overset{II.7.20}{\cong} \mathrm{End}_Q(Q)^{d\times d} \overset{II.7.20}{\cong} (Q^o)^{d\times d}. \qquad \square$$

Bemerkung II.9.13. Sei R ein Integritätsbereich mit Quotientenkörper Q und $n \in \mathbb{N}$. Man kann dann $R^{n\times n}$ als Teilring von $Q^{n\times n}$ auffassen. Daher gelten die gewohnten Rechenregeln für Determinanten auch in $R^{n\times n}$. Die Leibniz-Formel für $A = (a_{ij}) \in R^{n\times n}$ zeigt

$$\det A = \sum_{\sigma\in S_n} \mathrm{sgn}(\sigma) \prod_{i=1}^{n} a_{i\sigma(i)} \in R.$$

Wir definieren $\mathrm{GL}(n, R) := (R^{n\times n})^\times$.

Lemma II.9.14. *Für jeden Integritätsbereich R und $n \in \mathbb{N}$ gilt* $\mathrm{GL}(n, R) = \{A \in R^{n\times n} : \det A \in R^\times\}$.

Beweis. Für $A \in \mathrm{GL}(n, R)$ gilt $\det(A)\det(A^{-1}) = \det(AA^{-1}) = \det(1_n) = 1 = \det(A^{-1})\det(A)$ und es folgt $\det A \in R^\times$. Sei umgekehrt $A \in R^{n\times n}$ mit $\det A \in R^\times$. In der linearen Algebra konstruiert man die zu A *komplementäre* Matrix

$$\widetilde{A} := \big((-1)^{i+j} \det A_{ji}\big)_{i,j},$$

wobei A_{ij} aus A durch Streichen der i-ten Zeile und j-ten Spalte entsteht. Insbesondere ist $\widetilde{A} \in R^{n\times n}$. Über dem Quotientenkörper von R gilt $A^{-1} = \det(A)^{-1}\widetilde{A} \in R^{n\times n}$. Daher ist $A \in \mathrm{GL}(n, R)$. □

Beispiel II.9.15. Nach Lemma II.9.14 gilt

$$\mathrm{GL}(n, \mathbb{Z}) = \{A \in \mathbb{Z}^{n\times n} : \det A = \pm 1\},$$
$$\mathrm{GL}(n, K[X]) = \{A \in K[X]^{n\times n} : \det A \in K^\times\}.$$

Definition II.9.16. Sei R ein Integritätsbereich und $n, m \in \mathbb{N}$. Matrizen $A, B \in R^{n\times m}$ heißen *äquivalent*, falls $S \in \mathrm{GL}(n, R)$ und $T \in \mathrm{GL}(m, R)$ mit $A = SBT$ existieren. Gegebenenfalls schreiben wir $A \sim B$.

[1] Siehe Abschnitt 5.9 in [P. M. Cohn, *Skew fields*, Cambridge University Press, Cambridge, 1997]

Bemerkung II.9.17. Die Äquivalenz von Matrizen ist ein Äquivalenzrelation. Ist R ein Körper, so sind zwei Matrizen (vom gleichen Format) genau dann äquivalent, wenn sie den gleichen Rang haben (Gauß-Elimination).

Satz II.9.18 (Smith-Normalform)**.** *Sei R ein Hauptidealring und $A \in R^{n\times m}$. Dann ist A äquivalent zu einer Matrix der Form*

$$\begin{pmatrix} d_1 & & 0 \\ & d_2 & \\ 0 & & \ddots \end{pmatrix}$$

mit $d_1 \mid d_2 \mid \ldots$. Dabei sind $d_1, d_2, \ldots$ bis auf Assoziiertheit eindeutig bestimmt.

Beweis.
Existenz: Im Folgenden fixieren wir ein Repräsentantensystem für die Klassen assoziierter Primelemente von R (Bemerkung II.5.14). Für $a \in R \setminus \{0\}$ sei $\pi(a)$ die Anzahl der Primfaktoren von a gezählt mit Vielfachheiten ($\pi(a) = 0 \Leftrightarrow a \in R^\times$). Zusätzlich sei $\pi(0) := \infty$. Sei

$$\Pi(A) := \min\{\pi(a_{ij}) : 1 \le i \le n, 1 \le j \le m\},$$

wobei $A = (a_{ij})_{i,j}$. Ist $\Pi(A) = \infty$, so ist $A = 0$ und wir sind fertig. Sei also $\Pi(A) < \infty$. Offenbar sind Permutationsmatrizen über R invertierbar (die Inverse ist die Permutationsmatrix der inverse Permutation). Durch Multiplikation mit Permutationsmatrizen von links und rechts kann man Zeilen und Spalten von A permutieren ohne die Äquivalenzklasse zu verlassen. Wir können daher $\Pi(A) = \pi(a_{11})$ annehmen. Im Fall $a_{11} \nmid a_{12}$ existieren nach Bézout Elemente $x, y \in R$ mit $d := \mathrm{ggT}(a_{11}, a_{12}) = a_{11}x + a_{12}y$. Dann ist

$$M := \begin{pmatrix} x & -\frac{a_{12}}{d} & 0 \\ y & \frac{a_{11}}{d} & 0 \\ 0 & 0 & 1_{m-2} \end{pmatrix} \in \mathrm{GL}(m, R)$$

und der erste Eintrag von AM ist d. Indem wir A durch AM ersetzen, erreichen wir $\Pi(A) \le \pi(d) < \pi(a_{11})$. Wegen $\Pi(A) \ge 0$ lässt sich dieser Prozess nur endlich oft wiederholen. Am Ende ist $a_{11} \mid a_{12}$. Analog geht man für die anderen Einträge in der ersten Zeile (und ersten Spalte) vor. Dann ist $a_{11} \mid a_{1i}$ und $a_{11} \mid a_{i1}$ für alle i. Durch Multiplikation von links und rechts mit (invertierbaren) Elementarmatrizen der Form

$$\begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \lambda & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}$$

überführt man A in die Form

$$\begin{pmatrix} a_{11} & 0 & \cdots & 0 \\ 0 & * & \cdots & * \\ \vdots & \vdots & & \vdots \\ 0 & * & \cdots & * \end{pmatrix}$$

ohne die Äquivalenzklasse zu verlassen. Gilt nun $a_{11} \nmid a_{ij}$ für gewisse $i, j \ge 2$, so addiere man die i-te Zeile zur ersten (mittels Elementarmatrizenmultiplikation) und fange von vorn an. Dabei nimmt $\Pi(A)$ weiter ab. Nach endlich vielen Schritten gilt somit $a_{11} \mid a_{ij}$ für alle i, j. Man wende nun das Verfahren auf die Matrix $A' := (a_{ij})_{i,j\ge 2}$ an. Die obigen Elementarumformungen werden die Eigenschaft $a_{11} \mid a_{ij}$ stets erhalten. Am Ende erhält man eine äquivalente Matrix in der gewünschten Form.

Eindeutigkeit: Sei $D_k(A)$ das von allen $k \times k$-Unterdeterminanten von A erzeugte Ideal in R. Sei $T \in \mathrm{GL}(m, R)$. Die Spalten von AT sind dann R-Linearkombinationen der Spalten von A. Dies gilt auch für $k \times k$-Untermatrizen. Aus der Multilinearität der Determinante ergibt sich

$$D_k(A) \supseteq D_k(AT) \supseteq D_k(ATT^{-1}) = D_k(A).$$

Analog gilt $D_k(A) = D_k(SA)$ für $S \in \mathrm{GL}(n, R)$. Dies zeigt $D_k(A) = D_k(\mathrm{diag}(d_1, \ldots)) = (d_1 \ldots d_k)$. Also sind $d_1, d_1 d_2, \ldots$ bis auf Assoziiertheit eindeutig durch A bestimmt. Daraus folgt die Eindeutigkeit von $d_1, d_2, \ldots$ bis auf Assoziiertheit. □

Definition II.9.19. Die Elemente $d_1, d_2, \ldots$ in Satz II.9.18 heißen *Elementarteiler* von A. Für $R = \mathbb{Z}$ (oder $K[X]$) kann man die Smith-Normalform vollständig eindeutig machen, indem man $d_i \geq 0$ (bzw. d_i normiert) wählt.

Folgerung II.9.20. *Matrizen vom gleichen Format sind genau dann äquivalent, wenn sie die gleichen Elementarteiler (bis auf Assoziiertheit) besitzen.*

Beweis. Folgt aus der Eindeutigkeit der Smith-Normalform. □

Beispiel II.9.21. Die Smith-Normalform ist nützlich um ganzzahlige lineare Gleichungssysteme zu lösen: Wir suchen alle $x \in \mathbb{Z}^3$ mit

$$Ax := \begin{pmatrix} 21 & -5 & 26 \\ 3 & -1 & 4 \\ -8 & 2 & -10 \end{pmatrix} x = \begin{pmatrix} 47 \\ 7 \\ -18 \end{pmatrix} =: b. \tag{II.9.1}$$

Der Algorithmus im Beweis von Satz II.9.18 (mit $R = \mathbb{Z}$) ergibt:

$$\begin{pmatrix} 21 & -5 & 26 \\ 3 & -1 & 4 \\ -8 & 2 & -10 \end{pmatrix} \sim \begin{pmatrix} -1 & 3 & 4 \\ -5 & 21 & 26 \\ 2 & -8 & -10 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 \\ 5 & 6 & 6 \\ -2 & -2 & -2 \end{pmatrix}$$
$$\sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & 6 & 6 \\ 0 & -2 & -2 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 2 \\ 0 & 6 & 6 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 0 \end{pmatrix} =: D.$$

Für

$$S := \begin{pmatrix} -5 & -8 & -2 \\ -1 & -1 & 0 \\ 2 & 3 & 1 \end{pmatrix} \in \mathrm{GL}(3, \mathbb{Z}), \qquad T := \begin{pmatrix} -1 & 1 & -2 \\ -1 & 0 & -1 \\ 2 & -2 & 3 \end{pmatrix} \in \mathrm{GL}(3, \mathbb{Z})$$

gilt $SDT = A$. Daher ist (II.9.1) äquivalent zu

$$Dy = S^{-1}b = \begin{pmatrix} -3 \\ -4 \\ 0 \end{pmatrix}$$

mit $y := Tx$. Dies zeigt $y = (-3, -2, a)$ mit $a \in \mathbb{Z}$. Also ist $x = T^{-1}y = (a - 4, 5 - a, 6 - a)$ für $a \in \mathbb{Z}$.

Satz II.9.22. *Sei R ein Hauptidealring und M ein freier R-Modul mit $n := \mathrm{rk}\, M < \infty$. Jeder Untermodul $N \leq M$ ist dann frei mit $m := \mathrm{rk}\, N \leq n$. Außerdem existiert eine Basis $b_1, \ldots, b_n$ von M und Elemente $d_1, \ldots, d_m \in R$ mit $d_1 \mid d_2 \mid \ldots \mid d_m$, sodass $d_1 b_1, \ldots, d_m b_m$ eine Basis von N ist. Dabei sind $d_1, \ldots, d_m$ bis auf Assoziiertheit eindeutig bestimmt.*

Beweis.
Existenz: Sei $a_1, \ldots, a_n$ zunächst irgendeine Basis von M. Nach Beispiel II.8.3 ist R noethersch und daher auch M nach Lemma II.8.4. Insbesondere ist N endlich erzeugt, sagen wir durch $c_1, \ldots, c_k$. Wir schreiben $c_i = \sum_{j=1}^{n} x_{ij} a_j$ mit $x_{ij} \in R$ für $i = 1, \ldots, k$ und setzen $A := (x_{ij})_{i,j}$. Nach Satz II.9.18 existieren $S = (s_{ij})_{i,j} \in \mathrm{GL}(k, R)$ und $T = (t_{ij})_{i,j} \in \mathrm{GL}(n, R)$ mit $SAT = \mathrm{diag}(d_1, d_2, \ldots)$ und $d_1 \mid d_2 \mid \ldots$. Sei $T^{-1} = (t'_{ij})_{i,j}$ und $b_i := \sum_{j=1}^{n} t'_{ij} a_j \in M$ für $i = 1, \ldots, n$. Wie in der linearen Algebra zeigt man, dass auch $b_1, \ldots, b_n$ eine Basis von M ist (Stichwort: Basistransformation). Wegen

$$c_i = \sum_{j=1}^{n} x_{ij} a_j = \sum_{j=1}^{n} \sum_{l=1}^{n} s'_{il} d_l t'_{lj} a_j = \sum_{l=1}^{n} s'_{il} d_l b_l$$

ist $\{d_1 b_1, \ldots, d_n b_n\}$ ein Erzeugendensystem von N. Aus der linearen Unabhängigkeit von $b_1, \ldots, b_n$ folgt $d_i b_i = 0 \Leftrightarrow d_i = 0$. Wegen $d_1 \mid d_2 \mid \ldots \mid d_n$ befinden sich die Nullen in der Folge $d_1, \ldots, d_n$ am Ende. Durch Streichen dieser Elemente erhält man das Erzeugendensystem $d_1 b_1, \ldots, d_m b_m$ von N. Seien $r_1, \ldots, r_m \in R$ mit $r_1 d_1 b_1 + \ldots + r_m d_m b_m = 0$. Da $b_1, \ldots, b_m$ linear unabhängig sind, folgt $r_1 d_1 = \ldots = r_m d_m = 0$. Da R ein Integritätsbereich ist, gilt $r_1 = \ldots = r_m = 0$. Also ist $d_1 b_1, \ldots, d_m b_m$ tatsächlich eine Basis von N.

Eindeutigkeit: Sei $b'_1, \ldots, b'_n$ eine weitere Basis von M und $d'_1 \mid d'_2 \mid \ldots \mid d'_m$, sodass $d'_1 b'_1, \ldots, d'_m b'_m$ eine Basis von N ist (beachte Satz II.9.7). Dann existieren $x_{ij}, y_{ij} \in R$ mit $b'_i = \sum_{j=1}^{n} x_{ij} b_j$ und $d'_i b'_i = \sum_{j=1}^{m} y_{ij} d_j b_j$ für alle i. Da man b_i umgekehrt auch durch b'_j ausdrücken kann, ist $X := (x_{ij}) \in \mathrm{GL}(n, R)$ und analog $Y := (y_{ij}) \in \mathrm{GL}(m, R)$. Ein Koeffizientenvergleich zeigt $d'_i x_{ij} = y_{ij} d_j$. Daher ist

$$\mathrm{diag}(d'_1, \ldots, d'_m) X = Y \,\mathrm{diag}(d_1, \ldots, d_m).$$

Also sind $\mathrm{diag}(d_1, \ldots, d_m)$ und $\mathrm{diag}(d'_1, \ldots, d'_m)$ äquivalent und die Behauptung folgt aus Folgerung II.9.20. □

Bemerkung II.9.23.

(i) Mit Zorns Lemma lässt sich zeigen, dass der erste Teil von Satz II.9.22 auch im Fall $n = \infty$ gilt (siehe Satz A.10.1).

(ii) Satz II.9.22 wird falsch, wenn R kein Hauptidealring ist: Jedes Ideal I von R ist ein Untermodul des (freien) regulären R-Moduls. Ist I kein Hauptideal, so muss eine Basis von I mindestens zwei Elemente besitzen. Andererseits sind je zwei Elemente $x, y \in I$ linear abhängig über R wegen $yx + (-x)y = 0$. Daher können nur Hauptideale frei sein.

Definition II.9.24. Sei $R \neq \{0\}$ ein Integritätsbereich und M ein R-Modul. Dann nennt man

$$\mathrm{T}(M) := \{m \in M : \exists r \in R \setminus \{0\} : rm = 0\}$$

den *Torsionsmodul* von M. Im Fall $\mathrm{T}(M) = 0$ heißt M *torsionsfrei*.

Bemerkung II.9.25. Sicher ist $0 \in \mathrm{T}(M)$. Für $x, y \in \mathrm{T}(M)$ existieren $r, s \in R \setminus \{0\}$ mit $rx = sy = 0$. Da R ein Integritätsbereich ist, gilt $rs \neq 0$ und $rs(x - y) = s(rx) - r(sy) = 0$. Dies zeigt $x - y \in \mathrm{T}(M)$. Für $t \in R$ ist ebenso $r(tx) = t(rx) = 0$ und $tx \in \mathrm{T}(M)$. Daher ist $\mathrm{T}(M) \leq M$.

Satz II.9.26. *Sei R ein Hauptidealring und M ein endlich erzeugter R-Modul. Dann gilt:*

(i) $M = \mathrm{T}(M) \oplus F$ für einen freien R-Modul F, dessen Rang eindeutig bestimmt ist.

(ii) $\mathrm{T}(M) \simeq R/(d_1) \times \ldots \times R/(d_n)$ *mit eindeutig bestimmten Idealen* $R \neq (d_1) \supseteq (d_2) \supseteq \ldots \supseteq (d_n) \neq (0)$.

(iii) Es existieren Primelemente $p_1, \ldots, p_k \in R$ *und* $a_1, \ldots, a_k \in \mathbb{N}$ *mit*

$$\mathrm{T}(M) \simeq R/(p_1^{a_1}) \times \ldots \times R/(p_k^{a_k}).$$

Dabei sind die Ideale $(p_1^{a_1}), \ldots, (p_k^{a_k})$ *bis auf die Reihenfolge eindeutig bestimmt.*

Beweis. Sei $m_1, \ldots, m_s$ ein Erzeugendensystem von M und L der Kern des Epimorphismus $R^s \to M$, $(r_1, \ldots, r_s) \mapsto \sum_{i=1}^s r_i m_i$. Nach Satz II.9.22 existiert eine Basis $b_1, \ldots, b_s$ von R^s und $d_1, \ldots, d_n \in R \backslash \{0\}$ mit $d_1 \mid \ldots \mid d_n$, sodass $d_1 b_1, \ldots, d_n b_n$ eine Basis von L ist. Der Epimorphismus

$$\begin{aligned} R^s &\to R/(d_1) \times \ldots \times R/(d_n) \times R^{s-n}, \\ \sum_{i=1}^s r_i b_i &\mapsto (r_1 + (d_1), \ldots, r_n + (d_n), r_{n+1}, \ldots, r_s) \end{aligned}$$

hat dann ebenfalls Kern L. Der Homomorphiesatz liefert

$$M \simeq R^s/L \simeq R/(d_1) \times \ldots \times R/(d_n) \times R^{s-n}.$$

Für $d_i \in R^\times$ gilt $R/(d_i) = 0$. Indem wir diese Elemente streichen, erreichen wir $R \neq (d_1) \supseteq (d_2) \supseteq \ldots \supseteq (d_n) \neq (0)$. Wir identifizieren nun M mit $R/(d_1) \times \ldots \times R/(d_n) \times R^{s-n}$. Offenbar ist dann $\mathrm{T}(M) = R/(d_1) \times \ldots \times R/(d_n)$ und wir können $F = R^{s-n}$ wählen. Nach Satz II.9.7 ist der Rang von $F \simeq M/\mathrm{T}(M)$ eindeutig bestimmt. Im Folgenden können wir daher $M = \mathrm{T}(M)$ annehmen.

Zum Nachweis der Eindeutigkeit in (ii) beobachten wir zunächst

$$\mathrm{Ann}_R(M) = (d_n) =: I.$$

Insbesondere ist (d_n) eindeutig bestimmt. Sei also $n \geq 2$. Nach dem zweiten Isomorphiesatz für Ringe ist $\overline{R} := R/I$ ebenfalls ein Hauptidealring. Durch

$$(r + I)m := rm \qquad (r \in R,\ m \in M)$$

wird M zu einem $\overline{R}$-Modul (wohldefiniert), den wir mit $\overline{M}$ bezeichnen. Nach (i) gilt

$$\overline{M} = \mathrm{T}(\overline{M}) \oplus \overline{F} = R/(d_1) \times \ldots \times R/(d_l) \times \overline{R}^{n-l} \simeq \overline{R}/((d_1)/I) \times \ldots \times \overline{R}/((d_l)/I) \times \overline{R}^{n-l},$$

wobei $(d_l) \supsetneq (d_{l+1}) = (d_{l+2}) = \ldots = (d_n)$. Dabei ist $\mathrm{rk}\, \overline{F} = n - l$ eindeutig bestimmt. Durch Induktion nach n sind $(d_1)/I, \ldots, (d_l)/I$ eindeutig bestimmt. Sicher sind dann auch $(d_1), \ldots, (d_n)$ eindeutig bestimmt.

In (iii) können wir $M = R/(d)$ annehmen. Sei $d = p_1^{a_1} \ldots p_k^{a_k}$ die Primfaktorzerlegung von d (Bemerkung II.5.14). Für $i \neq j$ gilt $(p_i^{a_i}) + (p_j^{a_j}) = (\mathrm{ggT}(p_i^{a_i}, p_j^{a_j})) = R$. Der chinesische Restsatz für Ringe (I.7.30) liefert einen Isomorphismus

$$M = R/(d) \cong R/(p_1^{a_1}) \times \ldots \times R/(p_k^{a_k}),$$

der auch ein Isomorphismus von R-Moduln ist. Da man die Elemente $d_1, \ldots, d_n$ in (ii) aus den Primelementen in (iii) bis auf Assoziiertheit zurückgewinnen kann (vgl. Aufgabe I.29), sind diese Primelemente bis auf Reihenfolge und Assoziiertheit eindeutig bestimmt. Daher sind die Ideale $(p_1^{a_1}), \ldots, (p_k^{a_k})$ bis auf die Reihenfolge eindeutig bestimmt. □

Bemerkung II.9.27.

(i) Nach Satz II.9.26 sind endlich erzeugte Moduln über Hauptidealringen genau dann frei, wenn sie torsionsfrei sind. Für unendlich erzeugte Moduln ist dies falsch (Aufgabe II.51).

(ii) Im Spezialfall $R = \mathbb{Z}$ nennt man Satz II.9.26 den *Hauptsatz über endlich erzeugte abelsche Gruppen* (vgl. Satz I.5.9 und Aufgabe I.29). Zum Beispiel ist

$$C_2 \times C_6 \times C_{60} \times \mathbb{Z}^5 \cong C_2^2 \times C_3^2 \times C_4 \times C_5 \times \mathbb{Z}^5.$$

Satz II.9.28. *Sei A eine freie abelsche Gruppe mit Basis $a_1, \ldots, a_n$. Sei $B = \langle b_1, \ldots, b_m \rangle \leq A$ und $b_i = \sum_{j=1}^n x_{ij} a_j$ für $i = 1, \ldots, m$ und $x_{ij} \in \mathbb{Z}$. Genau dann ist A/B endlich, wenn die Matrix $M := (x_{ij})_{i,j} \in \mathbb{Z}^{m \times n}$ Rang n hat. Gegebenenfalls ist $|A/B| = \det M$ falls $m = n$.*

Beweis. Nach einem Basiswechsel wie in Satz II.9.22 können wir annehmen, dass $d_1 a_1, \ldots, d_k a_k$ eine Basis von B ist für gewisse $d_1, \ldots, d_k \in R \setminus \{0\}$. Dabei gilt $k \leq m$ und M ist zu $D := \operatorname{diag}(d_1, \ldots, d_k, 0, \ldots, 0)$ äquivalent. Insbesondere haben M und D den gleichen Rang. Wie in Satz II.9.26 gilt

$$A/B = \mathbb{Z}/d_1\mathbb{Z} \times \ldots \times \mathbb{Z}/d_k\mathbb{Z} \times \mathbb{Z}^{n-k}.$$

Dies zeigt

$$|A/B| < \infty \iff k = n \iff \operatorname{rk} D = n \iff \operatorname{rk} M = n.$$

Gegebenenfalls ist $|A/B| = |d_1 \ldots d_n| = |\det D| = |\det M|$ nach Beispiel II.9.15. □

10 Frobenius-Normalform

Bemerkung II.10.1. Im Folgenden sei K ein Körper und $n \in \mathbb{N}$. Wir wenden die Ergebnisse des letzten Kapitels auf den Hauptidealring $K[X]$ an, um eine Normalform von Matrizen zu konstruieren.

Definition II.10.2.

- Matrizen $A, B \in K^{n\times n}$ heißen *ähnlich*, falls ein $S \in \mathrm{GL}(n, K)$ mit $A = SBS^{-1}$ existiert (lineare Algebra).
- Für $\alpha = X^n + a_{n-1}X^{n-1} + \ldots + a_0 \in K[X] \setminus K$ nennt man

$$B_\alpha := \begin{pmatrix} 0 & & & -a_0 \\ 1 & \ddots & & \vdots \\ & \ddots & 0 & -a_{n-2} \\ 0 & & 1 & -a_{n-1} \end{pmatrix} \in K^{n\times n}$$

  die *Begleitmatrix* von α.

Beispiel II.10.3. Die Begleitmatrix von X^n ist der $n \times n$-Jordanblock zum Eigenwert 0.

Lemma II.10.4. *Jedes $\alpha \in K[X] \setminus K$ ist das charakteristische Polynom von B_α.*

Beweis. Sei $\alpha := X^n + a_{n-1}X^{n-1} + \ldots + a_0$. Im Fall $n = 1$ ist $X + a_0 = \alpha$ das charakteristische Polynom. Sei nun $n \geq 2$ und die Behauptung für $n-1$ bereits bewiesen. Wir entwickeln die $\det(X1_m - B_\alpha)$ nach der ersten Zeile

$$\begin{aligned} \det(X1_m - B_\alpha) &= X \begin{vmatrix} X & & & a_1 \\ -1 & \ddots & & \vdots \\ & \ddots & X & a_{n-2} \\ 0 & & -1 & X + a_{n-1} \end{vmatrix} + (-1)^{n-1}a_0 \begin{vmatrix} -1 & X & & 0 \\ & \ddots & \ddots & \\ & & \ddots & X \\ 0 & & & -1 \end{vmatrix} \\ &= X(X^{n-1} + a_{n-1}X^{n-2} + \ldots + a_1) + a_0 = \alpha. \end{aligned}$$

□

Bemerkung II.10.5 (Wiederholung Lineare Algebra 2)**.** Sei $A \in K^{n\times n}$. Man zeigt leicht, dass die Abbildung

$$\begin{aligned} F_A \colon K[X] &\to K^{n\times n}, \\ \alpha = \sum_{k=0}^{\infty} a_k X^k &\mapsto \alpha(A) := \sum_{k=0}^{\infty} a_k A^k \end{aligned}$$

ein Ringhomomorphismus ist. Wegen $\dim_K K^{n\times n} = n^2 < \infty = \dim_K K[X]$ ist F_A nie injektiv. Da $K[X]$ ein Hauptidealring ist, existiert genau ein normiertes Polynom $\mu_A \in K[X]$ mit $\mathrm{Ker}(F_A) = (\mu_A)$. Man nennt μ_A das *Minimalpolynom* von A. Im Gegensatz zu Minimalpolynomen algebraischer Elemente ist μ_A oft reduzibel, denn $K^{n\times n}$ besitzt Nullteiler.

Satz II.10.6 (FROBENIUS-Normalform)**.** *Für jedes $A \in K^{n\times n}$ existieren eindeutig bestimmte normierte Polynome $\alpha_1, \ldots, \alpha_k \in K[X] \setminus K$ mit $\alpha_1 \mid \ldots \mid \alpha_k$, sodass A zu*

$$\begin{pmatrix} B_{\alpha_1} & & 0 \\ & \ddots & \\ 0 & & B_{\alpha_k} \end{pmatrix}$$

ähnlich ist.

Beweis. Sei $R := K[X]$. Durch den Einsetzungshomomorphismus F_A wird der $K^{n\times n}$-Modul $V := K^{n\times 1}$ zu einem R-Modul mit $\alpha v = \alpha(A)v$ für $\alpha \in R$ und $v \in V$ (Beispiel II.6.4(vii)). Wegen $\dim_K V = n$ ist V als R-Modul endlich erzeugt. Für das Minimalpolynom μ von A gilt $\mu V = \mu(A)V = 0V = 0$. Insbesondere ist $V = \mathrm{T}(V)$. Nach Satz II.9.26 existieren normierte Polynome $\alpha_1, \ldots, \alpha_k \in R \setminus K$ mit $\alpha_1 \mid \ldots \mid \alpha_k$ und $V \simeq R/(\alpha_1) \times \ldots \times R/(\alpha_k)$. Wir identifizieren daher V mit $R/(\alpha_1) \times \ldots \times R/(\alpha_k)$. Sei $1 \le i \le k$ fest und $\alpha_i = X^{d_i} + a_{d_i-1}X^{d_i-1} + \ldots + a_0$. Für $j = 0, \ldots, d_i - 1$ sei

$$b_{ij} := (0, \ldots, 0, X^j + (\alpha_i), 0, \ldots, 0) \in V.$$

Dann ist $B := \{b_{ij} : 1 \le i \le k,\ 1 \le j \le d_i\}$ eine K-Basis von V und es gilt

$$\begin{aligned} Ab_{ij} = Xb_{ij} &= X(0, \ldots, 0, X^j + (\alpha_i), 0, \ldots, 0) = (0, \ldots, 0, X^{j+1} + (\alpha_i), 0, \ldots, 0) \\ &= \begin{cases} b_{i,j+1} & \text{falls } j < d_i - 1, \\ -a_0 b_{i,0} - \ldots - a_{d_i-1} b_{i,d_i-1} & \text{falls } j = d_i - 1. \end{cases} \end{aligned}$$

Also hat A bzgl. B die angegebene Form.

Seien nun auch $\beta_1, \ldots, \beta_l \in R \setminus K$ normiert mit $\beta_1 \mid \ldots \mid \beta_l$, sodass A zu

$$\begin{pmatrix} B_{\beta_1} & & 0 \\ & \ddots & \\ 0 & & B_{\beta_l} \end{pmatrix}$$

ähnlich ist. Indem man eine geeignete K-Basis wählt, erhält man eine entsprechende Zerlegung $V = V_1 \oplus \ldots \oplus V_l$. Wegen $XV_i = AV_i \subseteq V_i$ sind $V_1, \ldots, V_l$ dabei R-Untermoduln von V. Sei $1 \le i \le l$ fest und $\beta_i = X^{e_i} + b_{e_i-1}X^{e_i-1} + \ldots + b_0$. Dann besitzt V_i eine Basis $c_{i1}, \ldots, c_{i,e_i}$ mit

$$Ac_{ij} = \begin{cases} c_{i,j+1} & \text{falls } j < e_i - 1, \\ -b_0 c_{i,0} - \ldots - b_{e_i-1} c_{i,e_i-1} & \text{falls } i = e_i - 1. \end{cases}$$

Man erhält einen Isomorphismus von Vektorräumen $f\colon V_i \to R/(\beta_i)$ mit $f(c_{ij}) = X^j + (\beta_i)$ für $j = 0, \ldots, e_i - 1$. Wegen $f(Xc_{ij}) = f(Ac_{ij}) = Xf(c_{ij})$ ist f auch R-linear. Dies zeigt $V_i \simeq R/(\beta_i)$ und

$$V \simeq R/(\beta_1) \times \ldots \times R/(\beta_l).$$

Aus Satz II.9.26 folgt $k = l$ und $(\alpha_i) = (\beta_i)$ für $i = 1, \ldots, k$. Da alle α_i und β_i normiert sind, gilt sogar $\alpha_i = \beta_i$ für $i = 1, \ldots, k$. □

Bemerkung II.10.7.

(i) Im Gegensatz zur Jordanschen Normalform existiert die Frobenius-Normalform über beliebigen Körpern und verändert sich auch nicht, wenn man den Körper „vergrößert“ (wegen der Eindeutigkeit). Außerdem sind die Matrixblöcke bei der Frobenius-Normalform eindeutig sortiert.

(ii) Die Zerlegung $V \simeq R/(\alpha_1) \times \ldots \times R/(\alpha_k)$ im obigen Beweis zeigt $\mathrm{Ann}_{K[X]}(V) = (\alpha_k)$. Also ist $\alpha_k(A) = 0$ mit $\deg \alpha_k$ minimal, d. h. α_k ist das Minimalpolynom von A und auch von B_{α_k}. Insbesondere hat die Frobenius-Normalform nur dann Diagonalgestalt, wenn A eine Skalarmatrix ist, d. h. $A \in K1_n$. Nach Lemma II.10.4 ist $\chi := \alpha_1 \ldots \alpha_k$ das charakteristische Polynom von A. Damit erhält man den Satz von Cayley-Hamilton aus der linearen Algebra: $\chi(A) = 0$.

(iii) Hat das charakteristische Polynom χ von $A \in K^{n\times n}$ paarweise verschiedene Nullstellen in einem Zerfällungskörper, so ist B_χ die Frobenius-Normalform von A.

(iv) Benutzt man Teil (iii) anstatt (ii) in Satz II.9.26, so erhält man die *Weierstraß-Normalform* von A:

$$\begin{pmatrix} B_{\rho_1^{a_1}} & & 0 \\ & \ddots & \\ 0 & & B_{\rho_s^{a_s}} \end{pmatrix}$$

mit irreduziblen Polynomen $\rho_1, \ldots, \rho_s \in K[X]$ und $a_1, \ldots, a_s \in \mathbb{N}$. Dabei sind die Potenzen $\rho_1^{a_1}, \ldots, \rho_s^{a_s}$ bis auf die Reihenfolge eindeutig bestimmt (sie entstehen aus der Primfaktorzerlegung von $\alpha_1, \ldots, \alpha_k$ und hängen daher von K ab). Ist A diagonalisierbar über K, so zerfällt das Minimalpolynom α_k in paarweise verschiedene Linearfaktoren (lineare Algebra). Gegebenenfalls ist $\deg(\rho_1^{a_1}) = \ldots = \deg(\rho_s^{a_s}) = 1$, d. h. die Weierstraß-Normalform hat Diagonalgestalt.

Beispiel II.10.8. Die Matrix

$$A := \begin{pmatrix} 7 & -1 & -3 \\ 30 & -4 & -15 \\ 0 & 0 & 1 \end{pmatrix} \in \mathbb{Q}^{3\times 3}$$

hat charakteristisches Polynom $((X-7)(X+4)+30)(X-1) = (X^2-3X+2)(X-1) = (X-1)^2(X-2)$. Wegen

$$(A - 1_2)(A - 2 \cdot 1_2) = \begin{pmatrix} 6 & -1 & -3 \\ 30 & -5 & -15 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 5 & -1 & -3 \\ 30 & -6 & -15 \\ 0 & 0 & -1 \end{pmatrix} = 0$$

ist $\mu = (X-1)(X-2)$ das Minimalpolynom von A. Also ist

$$\begin{pmatrix} B_{X-1} & 0 \\ 0 & B_\mu \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -2 \\ 0 & 1 & 3 \end{pmatrix}$$

die Frobenius-Normalform von A. Die Weierstraß-Normalform ist hingegen $\mathrm{diag}(1, 1, 2)$. Der folgende Beweis zeigt, dass man die Frobenius-Normalform jeder Matrix $A \in K^{n\times n}$ über die Smith-Normalform von $X1_n - A \in K[X]^{n\times n}$ berechnen kann.

Satz II.10.9. *Für $A, B \in K^{n\times n}$ sind äquivalent:*

(1) A und B sind ähnlich.

(2) A und B haben die gleiche Frobenius-Normalform.

(3) $X1_n - A$ und $X1_n - B$ sind äquivalent in $K[X]^{n\times n}$.

Beweis. Die Äquivalenz von (1) und (2) folgt aus der Eindeutigkeit der Frobenius-Normalform. Für die Äquivalenz zu (3) analysieren wir wie die Polynome $\alpha_1, \ldots, \alpha_k$ in Satz II.10.6 entstehen. Wie dort sei $R := K[X]$. Sei $e_1, \ldots, e_n$ die Standardbasis von $V = K^{n\times 1}$ als K-Vektorraum. Dann ist

$$F\colon R^n \to V,$$
$$(\gamma_1, \ldots, \gamma_n) \mapsto \sum_{i=1}^{n} \gamma_i(A) e_i$$

ein Epimorphismus von R-Moduln. Wegen $K \subseteq R$ ist F auch K-linear. Insbesondere ist $\mathrm{Ker}(F)$ ein K-Vektorraum. Sei $\widetilde{A} := X1_n - A = (\alpha_{ij})_{i,j} \in R^{n\times n}$. Für $i = 1, \ldots, n$ gilt

$$\sum_{j=1}^{n} \alpha_{ji}(A) e_j = (A - a_{ii}1_n)e_i - \sum_{j\neq i} a_{ji} e_j = Ae_i - \begin{pmatrix} a_{1i} \\ \vdots \\ a_{ni} \end{pmatrix} = 0.$$

Daher liegen die Spalten $\widetilde{\alpha}_1, \ldots, \widetilde{\alpha}_n$ von $\widetilde{A}$ im $\mathrm{Ker}(F)$. Es folgt $L := \sum_{i=1}^{n} R\widetilde{\alpha}_i \subseteq \mathrm{Ker}(F)$. Wir zeigen, dass Gleichheit gilt. Wie im Beweis von Satz II.9.22 drückt man $\widetilde{\alpha}_1, \ldots, \widetilde{\alpha}_n$ durch die Standardbasis von R^n aus. Dabei erhält man gerade die Koeffizientenmatrix $\widetilde{A}$. Nun überführt man $\widetilde{A}$ in die Smith-Normalform

$$\begin{pmatrix} \beta_1 & & 0 \\ & \ddots & \\ 0 & & \beta_n \end{pmatrix}$$

mit $\beta_1, \ldots, \beta_n \in R$ und $\beta_1 \mid \ldots \mid \beta_n$. Wie im Beweis von Satz II.9.26 ist dann

$$R^n/L \simeq R/(\beta_1) \times \ldots \times R/(\beta_n).$$

Da $\det \widetilde{A}$ das charakteristische Polynom von A ist, gilt

$$\begin{aligned} n &= \deg(\det \widetilde{A}) = \deg(\beta_1 \ldots \beta_n) = \deg(\beta_1) + \ldots + \deg(\beta_n) \\ &= \dim_K(R/(\beta_1)) + \ldots + \dim_K(R/(\beta_n)) = \dim_K(R^n/L) \\ &\geq \dim_K(R^n/\mathrm{Ker}(F)) = \dim_K V = n. \end{aligned}$$

Dies zeigt schließlich $L = \mathrm{Ker}(F)$ und

$$V \simeq R^n/L \simeq R/(\beta_1) \times \ldots \times R/(\beta_n).$$

Wegen $\mathrm{T}(V) = V$ sind $\beta_1, \ldots, \beta_n \in R \setminus \{0\}$. Nach Normierung gilt dann $\beta_1 = \ldots = \beta_{n-k} = 1$ und $\beta_{n-k+i} = \alpha_i$ für $i = 1, \ldots, k$ mit den α_i aus Satz II.10.6. Die Frobenius-Normalform von A bestimmt daher die Smith-Normalform von $\widetilde{A} = X1_n - A$ und umgekehrt. Die Äquivalenz von (2) und (3) folgt nun aus Folgerung II.9.20. □

Folgerung II.10.10. *Jede Matrix $A \in K^{n\times n}$ ist zu A^{t} ähnlich.*

Beweis. Sei D die Smith-Normalform von $X1_n - A$ und $S, T \in \mathrm{GL}(n, K[X])$ mit $D = S(X1_n - A)T$. Dann ist

$$T^{\mathrm{t}}(X1_n - A^{\mathrm{t}})S^{\mathrm{t}} = D^{\mathrm{t}} = D = S(X1_n - A)T.$$

Also sind $X1_n - A$ und $X1_n - A^{\mathrm{t}}$ äquivalent und die Behauptung folgt aus Satz II.10.9. □

Bemerkung II.10.11. Die Frobenius-Normalform findet Anwendung in der Galois-Theorie: Nach Artin besitzt jede Galois-Erweiterung $K \subseteq L$ eine *Potenzbasis* $1, x, \dots, x^d$ für ein $x \in L$. Die Elemente $\sigma(x)$ mit $\sigma \in G := \mathrm{Gal}(L|K)$ sind dann paarweise verschieden, aber nicht unbedingt linear unabhängig über K. Wir zeigen, dass stets eine *Normalbasis* der Form $\{\sigma(y) : \sigma \in G\}$ mit $y \in L$ existiert. Damit vereinfacht sich die Berechnung von Zwischenkörpern, denn für $H \leq G$ ist

$$\Big\{ \sum_{\tau \in H\sigma} \tau(y) : \sigma \in R \Big\}$$

eine K-Basis von L^H, wobei R ein Repräsentantensystem für die Rechtsnebenklassen von H in G ist (beachte $|L^H : K| = |G : H| = |R|$). Dies findet zum Beispiel in der Kryptographie Anwendung.

Satz II.10.12 (Satz von der Normalbasis)**.** *Für jede Galois-Erweiterung $K \subseteq L$ existiert ein $a \in L$, sodass $\{\Gamma(a) : \Gamma \in \mathrm{Gal}(L|K)\}$ eine K-Basis von L ist.*

Beweis. Sei $n := |L : K|$ und $G := \mathrm{Gal}(L|K)$.

Fall 1: $|K| < \infty$.
Sei $p := \mathrm{char}\, K$. Nach Satz I.11.14 ist $\mathbb{F}_p \subseteq L$ eine Galois-Erweiterung und $G \leq \mathrm{Gal}(L|\mathbb{F}_p)$ ist zyklisch. Sei $G = \langle \Gamma \rangle$. Dann ist $\Gamma \in \mathrm{End}_K(L)$ und nach Dedekind sind die Potenzen $1, \Gamma, \dots, \Gamma^{n-1}$ linear unabhängig über K. Andererseits ist $\Gamma^n - 1 = 0$ in $\mathrm{End}_K(L)$. Also ist $X^n - 1$ das Minimalpolynom von Γ. Die Frobenius-Normalform von Γ ist daher

$$B_{X^n-1} = \begin{pmatrix} 0 & & & 1 \\ 1 & \ddots & & 0 \\ & \ddots & \ddots & \vdots \\ 0 & & 1 & 0 \end{pmatrix}.$$

Insbesondere besitzt L eine K-Basis der Form $\{\Gamma^i(a) : i = 0, \dots, n-1\} = \{\Gamma(a) : \Gamma \in G\}$.

Fall 2: $|K| = \infty$.
Nach Artin existiert ein $x \in L$ mit $L = K(x)$, sodass das Minimalpolynom $\mu \in K[X]$ von x paarweise verschiedene Nullstellen $x = x_1, \dots, x_n \in L$ hat. Sei $G = \{\Gamma_1, \Gamma_2, \dots, \Gamma_n\}$ mit $\Gamma_i(x) = x_i$ für $i = 1, \dots, n$. Sei

$$\varphi := \prod_{j=2}^{n} \frac{X - x_j}{x - x_j} \in L[X].$$

Für das Lagrange-Polynom

$$\alpha := \sum_{i=1}^{n} \Gamma_i(\varphi) = \sum_{i=1}^{n} \prod_{j \neq i} \frac{X - x_j}{x_i - x_j} \in L[X]$$

gilt $\alpha(x_k) = 1$ für $k = 1, \dots, n$. Nach Beispiel I.8.30 ist $\alpha = 1$. Es folgt

$$\Gamma_i(\varphi)\Gamma_j(\varphi) \equiv \begin{cases} 0 \pmod{\mu} & \text{falls } i \neq j. \\ \sum_{k=1}^{n} \Gamma_i(\varphi)\Gamma_k(\varphi) = \Gamma_i(\varphi) \pmod{\mu} & \text{falls } i = j. \end{cases} \tag{II.10.1}$$

Wir betrachten nun die Matrix $M := (\Gamma_i\Gamma_j(\varphi))_{i,j=1}^n \in L[X]^{n \times n}$. Es gilt

$$\begin{aligned} M^{\mathrm{t}}M &= \Big(\sum_{k=1}^{n} \Gamma_k\Gamma_i(\varphi)\Gamma_k\Gamma_j(\varphi) \Big)_{i,j} = \Big(\sum_{k=1}^{n} \Gamma_k(\Gamma_i(\varphi)\Gamma_j(\varphi)) \Big)_{i,j} \\ &\overset{\text{(II.10.1)}}{\equiv} \Big(\delta_{ij} \sum_{k=1}^{n} \Gamma_k(\Gamma_i(\varphi)) \Big)_{i,j} \equiv \Big(\delta_{i,j} \sum_{k=1}^{n} \Gamma_k(\varphi) \Big)_{i,j} \equiv 1_n \pmod{\mu}. \end{aligned}$$

Insbesondere ist $(\det M)^2 = \det(M^{\mathrm{t}}M) \equiv 1 \pmod{\mu}$ und $\gamma := \det M \in K[X] \setminus \{0\}$. Da γ nur endlich viele Nullstellen besitzt (Satz I.8.29), aber K unendlich groß ist, existiert ein $y \in K$ mit $\gamma(y) \neq 0$. Sei schließlich $a := \varphi(y)$ und $A := (\Gamma_i\Gamma_j(a))_{i,j} \in L^{n\times n}$. Dann ist

$$\det A = \det(\Gamma_i\Gamma_j(\varphi)(y)) = \gamma(y) \neq 0.$$

Sei $\sum_{j=1}^{n} \lambda_j\Gamma_j(a) = 0$ mit $\lambda_1, \ldots, \lambda_n \in K$. Wendet man Γ_i auf beiden Seiten an, so folgt $\sum_j \lambda_j\Gamma_i\Gamma_j(a) = 0$, d. h. $(\lambda_1, \ldots, \lambda_n)$ ist Lösung des linearen Gleichungssystems $Az = 0$. Aus $\det A \neq 0$ folgt $\lambda_1 = \ldots = \lambda_n = 0$. Also ist $\{\Gamma_1(a), \ldots, \Gamma_n(a)\}$ linear unabhängig und damit eine K-Basis von L. □

Beispiel II.10.13.

(i) Offenbar ist $1 + \sqrt{2}$, $1 - \sqrt{2}$ eine Normalbasis von $\mathbb{Q}(\sqrt{2})$ über $\mathbb{Q}$. Dagegen sind 1, $\sqrt{2}$ oder $\sqrt{2}$, $-\sqrt{2}$ *keine* Normalbasen.

(ii) Wir wissen bereits, dass $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$ eine $\mathbb{Q}$-Basis von $L := \mathbb{Q}(\sqrt{2}, \sqrt{3})$ ist (Beispiel I.10.12). Daraus folgt leicht, dass die vier Elemente $(1 \pm \sqrt{2})(1 \pm \sqrt{3})$ eine Normalbasis von L bilden.

11 Primidealzerlegung in Dedekindringen

Bemerkung II.11.1. In diesem Kapitel verallgemeinern wir algebraische Körpererweiterungen auf kommutative Ringe. Anschließend entwickeln wir eine Alternative der Primfaktorzerlegung in nichtfaktoriellen Ringen.

Definition II.11.2. Sei S ein kommutativer Ring mit Teilring R.

- Ein Element $x \in S$ heißt *ganz* über R, falls ein normiertes Polynom $\alpha \in R[X]$ mit $\alpha(x) = 0$ existiert. Sind alle $x \in S$ ganz über R, so nennt man $R \subseteq S$ eine *ganze Ringerweiterung*.
- Für eine Teilmenge $T \subseteq S$ sei $R[T]$ der Durchschnitt aller Teilringe von S, die R und T enthalten. Wie immer ist dann $R[T]$ der „kleinste“ Teilring, der R und T enthält. Außerdem ist $R[T]$ das Bild des Einsetzungshomomorphismus $R[X_t : t \in T] \to S$ (vgl. Bemerkung II.3.14). Insbesondere ist $R[t] := R[\{t\}] = \sum_{n=0}^{\infty} Rt^n$.

Beispiel II.11.3.

(i) Jedes $x \in R$ ist ganz über R als Nullstelle von $X - x$.

(ii) Ist R ein Körper, so ist $x \in S$ genau dann ganz, wenn x algebraisch über R ist, denn das Minimalpolynom von x ist stets normiert.

(iii) Für $R = \mathbb{Z}$ und $S = \mathbb{C}$ nennt man die ganzen Elemente auch *ganz-algebraische Zahlen*. Beispielsweise sind i und $\sqrt[3]{2}$ ganz-algebraisch. Nach Bemerkung I.8.53 sind alle rationalen ganz-algebraischen Zahlen bereits ganzzahlig.

Bemerkung II.11.4. Wir hatten in Bemerkung II.9.13 bereits gesehen, dass die Regeln für Determinanten aus der linearen Algebra auch in beliebigen Integritätsbereichen gelten (durch Einbettung in den Quotientenkörper). Sei nun R ein beliebiger kommutativer Ring. Dann ist der Polynomring

$$\widehat{R} := \mathbb{Z}[X_r : r \in R]$$

ein Integritätsbereich und der Einsetzungshomomorphismus $F\colon \widehat{R} \to R$, $X_r \mapsto r$ ist surjektiv. Komponentenweise setzt sich F zu einem Ringepimorphismus $F\colon \widehat{R}^{n\times n} \to R^{n\times n}$ fort. Damit übertragen sich die Rechenregeln von $\widehat{R}^{n\times n}$ nach $R^{n\times n}$. Sei beispielsweise $A \in R^{n\times n}$ und $\widehat{A} \in \widehat{R}^{n\times n}$ ein Urbild von A unter F. Sei $C \in \widehat{R}^{n\times n}$ die zu $\widehat{A}$ komplementäre Matrix und $\widetilde{A} := F(C)$. Dann gilt

$$\widetilde{A}A = F(C)F(\widehat{A}) = F(C\widehat{A}) = F(\det(\widehat{A})1_n) = \det(F(\widehat{A}))1_n = \det(A)1_n.$$

Lemma II.11.5. *Für jeden kommutativen Ring S mit Teilring R und $x \in S$ sind die folgenden Aussagen äquivalent:*

(1) x ist ganz über R.

(2) $R[x]$ ist ein endlich erzeugter R-Modul.

(3) Es existiert ein endlich erzeugter R-Untermodul M von S mit $1 \in M$ und $xM \subseteq M$.

Beweis.

(1) $\Rightarrow$ (2): Nach Voraussetzung existieren $n \in \mathbb{N}$ und $a_0, \ldots, a_{n-1} \in R$ mit $x^n + a_{n-1}x^{n-1} + \ldots + a_0 = 0$. Insbesondere ist

$$\begin{aligned} x^n &= -a_{n-1}x^{n-1} - \ldots - a_0 \in R + Rx + \ldots + Rx^{n-1} =: M, \\ x^{n+1} &= -a_{n-1}x^n - \ldots - a_0 x \in M, \\ &\vdots \end{aligned}$$

Dies zeigt $R[x] = \sum_{k=0}^{\infty} Rx^k = M$.

(2) $\Rightarrow$ (3): Wähle $M := R[x]$.

(3) $\Rightarrow$ (1): Sei $M = Rs_1 + \ldots + Rs_n$ mit $s_1, \ldots, s_n \in S \setminus \{0\}$. Wegen $xM \subseteq M$ existieren $a_{ij} \in R$ mit $xs_i = \sum_{j=1}^{n} a_{ij}s_j$ für $i = 1, \ldots, n$. Für $A := (a_{ij})_{i,j} \in R^{n\times n}$ und $v := (s_1, \ldots, s_n) \in S^n$ gilt

$$Av = \Big(\sum_{j=1}^{n} a_{ij}s_j\Big)_{i=1}^{n} = xv.$$

Sei $B := x1_n - A \in S^{n\times n}$ und $\widetilde{B} \in S^{n\times n}$ mit $\widetilde{B}B = \det(B)1_n$ wie in Bemerkung II.11.4. Dann ist $\det(B)v = \widetilde{B}Bv = \widetilde{B}0 = 0$, also $\det(B)s_i = 0$ für $i = 1, \ldots, n$. Wegen $1 \in M$ ist daher auch $\det(B) = \det(B)1 = 0$. Schließlich ist $\det(B) = \det(x1_n - A)$ ein normiertes Polynom in x (vom Grad n) mit Koeffizienten in R. Also ist x ganz über R. □

Beispiel II.11.6. Sei $R \subseteq S$ eine Ringerweiterung, sodass S als R-Modul endlich erzeugt ist. Dann ist $R \subseteq S$ ganz nach Lemma II.11.5 mit $M = S$.

Satz II.11.7. *Sei S ein kommutativer Ring mit Teilring R. Dann bilden die über R ganzen Elemente in S einen Teilring T von S mit $R \subseteq T$. Außerdem liegt jedes über T ganze Element von S bereits in T.*

Beweis. Nach Beispiel II.11.3 ist $R \subseteq T$. Seien nun $a, b \in T$. Nach Lemma II.11.5 existieren endlich erzeugte R-Moduln $M, N \subseteq S$ mit $1 \in M \cap N$, $aM \subseteq M$ und $bN \subseteq N$. Wir schreiben $M = Rx_1 + \ldots + Rx_m$ und $N = Ry_1 + \ldots + Ry_n$. Dann ist auch $L := MN = \sum_{i,j} Rx_iy_j$ ein endlich erzeugter R-Modul mit $1 \in L$, $(a-b)L \subseteq aMN + bNM \subseteq MN = L$ und $abL \subseteq aMbN \subseteq MN = L$. Nach Lemma II.11.5 folgt $a - b, ab \in T$ und T ist ein Teilring von S.

Sei nun $x \in S$ ganz über T. Dann existieren $a_0, \ldots, a_{n-1} \in T$ mit $x^n + a_{n-1}x^{n-1} + \ldots + a_0 = 0$. Folglich ist x auch über $R[a_0, \ldots, a_{n-1}]$ ganz. Nach Lemma II.11.5 existieren $k_0, \ldots, k_n \in \mathbb{N}$ mit $R[a_0] = R + Ra_0 + \ldots + Ra_0^{k_0}$, $R[a_0, a_1] = R[a_0] + R[a_0]a_1 + \ldots + R[a_0]a_1^{k_1}$, $\ldots$,

$$R[a_0, \ldots, a_{n-1}, x] = \sum_{i_0=0}^{k_0} \ldots \sum_{i_n=0}^{k_n} Ra_0^{i_0} \ldots a_{n-1}^{i_{n-1}} x^{i_n}.$$

Daher ist $M := R[a_0, \ldots, a_{n-1}, x]$ ein endlich erzeugter R-Modul mit $1 \in M$ und $xM \subseteq M$. Nach Lemma II.11.5 ist x ganz über R, d. h. $x \in T$. □

Definition II.11.8. In der Situation von Satz II.11.7 nennt man T den *ganzen Abschluss* von R in S. Im Fall $T = R$ nennt man R *ganz-abgeschlossen* in S. Ein Integritätsbereich R heißt *ganz-abgeschlossen*, wenn er in seinem Quotientenkörper ganz-abgeschlossen ist.

Beispiel II.11.9. Nach Beispiel II.11.3 ist $\mathbb{Z}$ ganz-abgeschlossen. Wir verallgemeinern dies.

Satz II.11.10. *Jeder faktorielle Ring ist ganz-abgeschlossen.*

Beweis. Sei R faktoriell mit Quotientenkörper Q. Sei $x \in Q$ ganz über R. Dann existieren teilerfremde $a, b \in R$ mit $x = \frac{a}{b}$. Außerdem existieren $a_0, \ldots, a_{n-1} \in R$ mit $x^n + a_{n-1}x^{n-1} + \ldots + a_0 = 0$. Multiplikation mit b^n ergibt

$$a^n + a_{n-1}ba^{n-1} + \ldots + a_0 b^n = 0.$$

Dies zeigt $b \mid a^n$. Wegen $\mathrm{ggT}(a, b) = 1$ ist $b \in R^\times$ und $x = ab^{-1} \in R$. □

Bemerkung II.11.11. Der ganze Abschluss von $\mathbb{Z}$ in einem Zahlkörper K heißt *Ganzheitsring*[1] von K und wird meist mit $\mathbb{Z}_K$ notiert. Jeder quadratische Zahlkörper K hat bekanntlich die Form $K = \mathbb{Q}(\sqrt{d})$ mit $d \in \mathbb{Q}$ (siehe Beweis von Satz I.12.23). Wegen $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(e^2\sqrt{d}) = \mathbb{Q}(\sqrt{de})$ für $e \in \mathbb{Z}$ können wir annehmen, dass d eine quadratfreie ganze Zahl ist und $0 \neq d \neq 1$.

Satz II.11.12. *Sei $d \in \mathbb{Z} \setminus \{0, 1\}$ quadratfrei und $K = \mathbb{Q}(\sqrt{d})$. Dann gilt*

$$\mathbb{Z}_K = \begin{cases} \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] = \mathbb{Z} + \mathbb{Z}\frac{1+\sqrt{d}}{2} & \text{falls } d \equiv 1 \pmod 4, \\ \mathbb{Z}[\sqrt{d}] = \mathbb{Z} + \mathbb{Z}\sqrt{d} & \text{sonst.} \end{cases}$$

Beweis. Da $\sqrt{d}$ als Nullstelle von $X^2 - d$ ganz-algebraisch ist, gilt in jedem Fall $\mathbb{Z}[\sqrt{d}] \subseteq \mathbb{Z}_K$ nach Satz II.11.7. Im Fall $d \equiv 1 \pmod 4$ ist $X^2 - X + \frac{1-d}{4} \in \mathbb{Z}[X]$ mit Nullstelle $\omega := \frac{1+\sqrt{d}}{2}$. Dann ist also auch $\mathbb{Z}[\omega] \subseteq \mathbb{Z}_K$.

Sei nun umgekehrt $x \in \mathbb{Z}_K$. Dann existieren $a, b \in \mathbb{Q}$ mit $x = a + b\sqrt{d}$. Sei $\sigma \in \mathrm{Gal}(K|\mathbb{Q})$ mit $\sigma(\sqrt{d}) = -\sqrt{d}$. Mit x ist auch $\sigma(x)$ ganz-algebraisch (Nullstelle des selben ganzzahligen Polynoms). Daher ist $x + \sigma(x) = 2a \in \mathbb{Q}$ ganz-algebraisch, also $2a \in \mathbb{Z}$. Analog ist $x\sigma(x) = a^2 - b^2 d \in \mathbb{Q} \cap \mathbb{Z}_K = \mathbb{Z}$. Wegen $(2b)^2 d = (2a)^2 - 4(a^2 - b^2 d) \in \mathbb{Z}$ ist auch $2b \in \mathbb{Z}$, denn d ist quadratfrei. Für $\widetilde{a} := 2a$ und $\widetilde{b} := 2b$ gilt

$$\frac{\widetilde{a}^2 - \widetilde{b}^2 d}{4} = a^2 - b^2 d \in \mathbb{Z}.$$

Dies zeigt $\widetilde{a}^2 \equiv \widetilde{b}^2 d \pmod 4$, wobei $d \not\equiv 0 \pmod 4$. Daher ist $\widetilde{a}$ genau dann gerade, wenn $\widetilde{b}$ gerade ist. Gegebenenfalls ist $x = a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$. Im Fall $\widetilde{a} \equiv \widetilde{b} \equiv 1 \pmod 2$ gilt $1 \equiv \widetilde{a}^2 \equiv \widetilde{b}^2 d \equiv d \pmod 4$. Dann ist

$$x = \frac{\widetilde{a} + \widetilde{b}\sqrt{d}}{2} = \frac{\widetilde{a} - \widetilde{b}}{2} + \widetilde{b}\frac{1 + \sqrt{d}}{2} \in \mathbb{Z}[\omega].$$ □

Bemerkung II.11.13.

(i) Wir hatten in Beispiel II.5.31 und Aufgabe II.29 bereits gesehen, dass die Ganzheitsringe von $K := \mathbb{Q}(\sqrt{d})$ für $d \in \{-3, -2, -1, 2, 3\}$ euklidisch sind, aber für $d = -5$ nicht. Man vermutet, dass $\mathbb{Z}_K$ für unendlich viele positive d euklidisch ist. Für negative d ist $\mathbb{Z}_K$ aber nur genau

[1] oder *Maximalordnung*

dann euklidisch, wenn $-d \in \{1,2,3,7,11\}$ (ohne Beweis). Allgemeiner hat Heegner gezeigt, dass $\mathbb{Z}_K$ für negative d genau dann ein Hauptidealring ist, falls $-d \in \{1,2,3,7,11,19,43,67,163\}$ (*Heegner-Zahlen*). Damit lässt sich begründen, warum

$$e^{\pi\sqrt{163}} = 262537412640768743{,}99999999999925\ldots$$

fast eine ganze Zahl ist (ohne Beweis).

(ii) Die Ganzheitsringe von $K := \mathbb{Q}(\sqrt{-2})$ und $L := \mathbb{Q}(\sqrt{-7})$ sind nach (i) euklidisch. Seien P_K und P_L Repräsentantensysteme für die nicht-assoziierten Primelemente in $\mathbb{Z}_K$ bzw. $\mathbb{Z}_L$. Man zeigt leicht $\mathbb{Z}_K^\times = \{\pm 1\} = \mathbb{Z}_L^\times$. Daher ist die Abbildung $K^\times \to L^\times$, $\pm\prod_{p\in P_K} p^{a_p} \mapsto \pm\prod_{p\in P_L} p^{a_p}$ ein Isomorphismus. Offenbar gilt auch $(K,+) \cong \mathbb{Q}^2 \cong (L,+)$. Nach Aufgabe I.66 ist andererseits $K \ncong L$.

Satz II.11.14. *Sei R ein Integritätsbereich mit Quotientenkörper Q. Sei $Q \subseteq K$ eine endliche Körpererweiterung und S der ganze Abschluss von R in K. Für jedes $x \in K$ existiert dann ein $r \in R \setminus \{0\}$ mit $rx \in S$. Insbesondere ist K zum Quotientenkörper von S isomorph.*

Beweis. Sei $\mu = X^n + a_{n-1}X^{n-1} + \ldots + a_0 \in Q[X]$ das Minimalpolynom von x über Q. Dann existiert ein $r \in R \setminus \{0\}$ mit $ra_i \in R$ für $i = 0,\ldots,n-1$. Folglich ist rx als Nullstelle des normierten Polynoms $X^n + a_{n-1}rX^{n-1} + \ldots + a_0r^n \in R[X]$ ganz über R. Also ist $rx \in S$. Nach der universellen Eigenschaft des Quotientenkörpers (Aufgabe I.40) lässt sich die Inklusionsabbildung $S \hookrightarrow K$ zu einem Körperhomomorphismus $\sigma\colon Q(S) \to K$ fortsetzen. Mit den obigen Bezeichnungen ist dann $\sigma(rx/r) = x$. Also ist σ surjektiv und damit ein Isomorphismus. □

Satz II.11.15. *Der Ganzheitsring eines Zahlkörpers K ist eine freie abelsche Gruppe vom Rang $|K:\mathbb{Q}|$.*

Beweis. Sei $x \in K$ ein primitives Element ($K = \mathbb{Q}(x)$). Nach Satz II.11.14 (mit $R = \mathbb{Z}$) existiert ein $a \in \mathbb{Z} \setminus \{0\}$ mit $ax \in \mathbb{Z}_K$. Wegen $\mathbb{Q}(x) = \mathbb{Q}(ax)$ können wir $x \in \mathbb{Z}_K$ annehmen. Sei $\alpha \in \mathbb{Z}[X]$ normiert mit Nullstelle x. Dann ist das Minimalpolynom $\mu \in \mathbb{Q}[X]$ ein Teiler von α. Aus Folgerung I.8.51 folgt $\mu \in \mathbb{Z}[X]$. Daher sind alle Nullstellen $x = x_0,\ldots,x_{n-1}$ von μ in einem Zerfällungskörper ganz-algebraisch. Wegen $|K:\mathbb{Q}| = |\mathbb{Q}(x):\mathbb{Q}| = \deg\mu = n$ ist $1, x, \ldots, x^{n-1}$ eine $\mathbb{Q}$-Basis von K. Für $z \in \mathbb{Z}_K$ existieren daher $a_0,\ldots,a_{n-1} \in \mathbb{Q}$ mit

$$z = a_0 + a_1x + \ldots + a_{n-1}x^{n-1}.$$

Sei $\mathrm{Gal}(\mu) = \{\sigma_0,\ldots,\sigma_{n-1}\}$ mit $\sigma_i(x) = x_i$ für $i = 0,\ldots,n-1$. Mit z ist dann auch $z_i := \sigma_i(z) = a_0 + a_1x_i + \ldots + a_{n-1}x_i^{n-1}$ ganz-algebraisch (Nullstelle des selben Polynoms). Dies liefert ein Gleichungssystem $Av = w$, wobei $A := (x_i^j)_{i,j=0}^{n-1} \in \mathbb{Z}_K^{n\times n}$, $v := (a_0,\ldots,a_{n-1}) \in \mathbb{Q}^n$ und $w := (z_0,\ldots,z_{n-1}) \in \mathbb{Z}_K^n$. Da A eine Vandermonde-Matrix ist, gilt

$$d := \det A = \prod_{i<j}(x_j - x_i) \in \mathbb{Z}_K \setminus \{0\}$$

(lineare Algebra). Außerdem ist $d^2 = D_\mu \in \mathbb{Q}$ (Diskriminante). Multiplikation mit der komplementären Matrix $\widetilde{A} \in \mathbb{Z}_K^{n\times n}$ ergibt $dv = \widetilde{A}Av = \widetilde{A}w$ und

$$d^2v = d\widetilde{A}w \in \mathbb{Q}^n \cap \mathbb{Z}_K^n = \mathbb{Z}^n.$$

Dies zeigt

$$z = a_0 + \ldots + a_{n-1}x^{n-1} \in \mathbb{Z}\frac{1}{d^2} + \mathbb{Z}\frac{x}{d^2} + \ldots + \mathbb{Z}\frac{x^{n-1}}{d^2} =: M.$$

Offenbar ist M eine freie abelsche Gruppe mit Basis $1/d^2, \ldots, x^{n-1}/d^2$. Nach Satz II.9.22 ist auch $\mathbb{Z}_K$ eine freie abelsche Gruppe vom Rang höchstens n. Umgekehrt enthält $\mathbb{Z}_K$ die freie abelsche Gruppe $\mathbb{Z}[x]$ vom Rang n. Daher hat auch $\mathbb{Z}_K$ Rang $n = |K : \mathbb{Q}|$. □

Bemerkung II.11.16. Eine $\mathbb{Z}$-Basis von $\mathbb{Z}_K$ für einen Zahlkörper K nennt man *Ganzheitsbasis* von K. Für quadratische Zahlkörper haben wir in Satz II.11.12 Ganzheitsbasen bestimmt ($1, \sqrt{d}$ bzw. $1, \frac{1+\sqrt{d}}{2}$). Für den n-ten Kreisteilungskörper $\mathbb{Q}_n$ ist $1, \zeta, \ldots, \zeta^{\varphi(n)-1}$ eine Ganzheitsbasis, wobei ζ eine primitive n-te Einheitswurzel ist (Satz A.3.17). Im Allgemeinen besitzt aber nicht jeder Ganzheitsring eine Basis bestehend aus Potenzen eines Elements (d. h. es gibt keine primitiven Elemente für Ganzheitsringe).

Satz II.11.17. *Sei $R \subseteq S$ eine ganze Ringerweiterung und $P \subsetneq Q$ Primideale in S. Dann sind $P \cap R \subsetneq Q \cap R$ Primideale in R.*

Beweis. Offensichtlich sind $P \cap R$ und $Q \cap R$ Primideale in R. Nehmen wir $Q \cap R \subseteq P$ an. Sei $x \in Q \setminus P$. Da x über R ganz ist, existieren $a_0, \ldots, a_{n-1} \in R$ mit $x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = 0$. Im Fall $a_i \in P$ für alle i wäre $x^n \in P$ und daher auch $x \in P$. Also existiert ein $i \in \{0, \ldots, n-1\}$ mit $a_i \notin P$ und $a_0, \ldots, a_{i-1} \in P$. Dann ist

$$x^i(x^{n-i} + \ldots + a_i) = -(a_{i-1}x^{i-1} + \ldots + a_1 x + a_0) \in P$$

und $x^{n-i} + \ldots + a_i \in P \subseteq Q$. Wegen $x^{n-i} + \ldots + a_{i+1}x \in Q$ folgt der Widerspruch $a_i \in Q \cap R \subseteq P$. Also ist $P \cap R \subsetneq Q \cap R$. □

Definition II.11.18. Sei R ein Integritätsbereich mit Quotientenkörper $Q(R)$. Ein *gebrochenes Ideal* von R ist ein R-Untermodul $I \neq 0$ von $Q(R)$ mit $rI \subseteq R$ für ein $r \in R \setminus \{0\}$.

Beispiel II.11.19. Offenbar ist jedes nicht-triviale Ideal von R ein gebrochenes Ideal. Andererseits ist $\mathbb{Z}\frac{1}{2}$ ein gebrochenes Ideal von $\mathbb{Z}$, aber kein Ideal. Für gebrochene Ideale I, J definiert man IJ (wie bei Idealen) als R-Spann von $\{xy : x \in I, y \in J\}$.

Lemma II.11.20. *Für jeden Integritätsbereich R gilt:*

(i) Jeder nicht-triviale endlich erzeugte R-Untermodul von $Q(R)$ ist ein gebrochenes Ideal. Insbesondere ist Rx für $x \in Q(R)^\times$ ein gebrochenes Hauptideal.

(ii) Sind I und J gebrochene Ideale von R, so auch $I + J$, IJ und $I \cap J$.

(iii) Für jedes gebrochene Ideal I von R ist auch $I^{-1} := \{x \in Q(R) : xI \subseteq R\}$ ein gebrochenes Ideal von R.

(iv) Sind I, J gebrochene Ideale mit $IJ = R$, so ist $J = I^{-1}$.

Beweis.

(i) Sei $I = R\frac{r_1}{s_1} + \ldots + R\frac{r_n}{s_n} \subseteq Q(R)$ mit $r_1, \ldots, r_n, s_1, \ldots, s_n \in R$. Dann ist $(s_1 \ldots s_n)I \subseteq R$.

(ii) Nach Definition sind $IJ \subseteq I \cap J \subseteq I + J$ nicht-triviale R-Moduln. Sei $r, s \in R$ mit $rI, sI \subseteq R$. Dann ist $rsIJ \subseteq rs(I \cap J) \subseteq rs(I + J) \subseteq s(rI) + r(sI) \subseteq R$.

(iii) Sei $r \in R \setminus \{0\}$ mit $rI \subseteq R$. Dann ist $r \in I^{-1} \neq 0$. Offenbar ist I^{-1} ein R-Modul und $xI^{-1} \subseteq R$ für $x \in I \setminus \{0\}$.

(iv) Offenbar ist $J \subseteq I^{-1} = I^{-1}IJ \subseteq J$. □

Definition II.11.21. Ein ganz-abgeschlossener, noetherscher Integritätsbereich R heißt *Dedekindring*, falls jedes nicht-triviale Primideal von R maximal ist.

Satz II.11.22. *Jeder Hauptidealring ist ein Dedekindring.*

Beweis. Nach Satz II.5.19 ist jeder Hauptidealring R faktoriell und daher ganz-abgeschlossen nach Satz II.11.10. Offensichtlich ist R auch noethersch. Nach Lemma II.5.18 sind die nicht-trivialen Primideale maximal. □

Beispiel II.11.23. Nicht jeder faktorielle Ring ist ein Dedekindring. Zum Beispiel ist das Primideal (X) in $\mathbb{Z}[X]$ nicht maximal. Wir zeigen in Folgerung II.11.36 aber, dass Dedekindringe nicht weit von Hauptidealringen entfernt sind.

Satz II.11.24. *Der Ganzheitsring $\mathbb{Z}_K$ jedes Zahlkörpers K ist ein Dedekindring.*

Beweis. Nach Satz II.11.14 mit $R = \mathbb{Z}$ ist $\mathbb{Z}_K$ ein ganz-abgeschlossener Integritätsbereich mit $Q(\mathbb{Z}_K) = K$. Nach Satz II.11.15 ist $\mathbb{Z}_K$ eine freie abelsche Gruppe mit Rang $|K : \mathbb{Q}| < \infty$. Nach Satz II.9.22 ist jedes Ideal (sogar jede Untergruppe) von $\mathbb{Z}_K$ endlich erzeugt als $\mathbb{Z}$-Modul und daher auch als R-Modul. Somit ist R noethersch. Seien $P, Q \trianglelefteq \mathbb{Z}_K$ Primideale mit $(0) \subsetneq P \subseteq Q$. Nach Satz II.11.17 sind $(0) \subsetneq P \cap \mathbb{Z} \subseteq Q \cap \mathbb{Z}$ Primideal in $\mathbb{Z}$. Dies zeigt $P \cap \mathbb{Z} = Q \cap \mathbb{Z}$ und $P = Q$. Also ist jedes nicht-triviale Primideal von $\mathbb{Z}_K$ maximal. □

Definition II.11.25. Ein gebrochenes Ideal I von R heißt *invertierbar*, falls $II^{-1} = R$.

Lemma II.11.26. *Sei R ein Dedekindring und $0 \neq I \lhd R$. Dann existieren Primideale $P_1, \ldots, P_n \trianglelefteq R$ mit $P_1 \ldots P_n \subseteq I \subseteq P_1 \cap \ldots \cap P_n$.*

Beweis. Sei $I \lhd R$ ein maximales Gegenbeispiel (existiert, da R noethersch). Dann ist I kein Primideal. Also existieren $J_1, J_2 \trianglelefteq R$ mit $J_1 J_2 \subseteq I$, aber $J_1, J_2 \nsubseteq I$. Wegen

$$(I + J_1)(I + J_2) \subseteq I + J_1 J_2 = I \subseteq (I + J_1) \cap (I + J_2)$$

ist $I + J_1 \neq R \neq I + J_2$. Folglich gilt die Aussage für $I + J_1$ und $I + J_1$ und damit auch für I. Widerspruch. □

Lemma II.11.27. *In jedem Dedekindring sind die nicht-trivialen Primideale invertierbar.*

Beweis. Sei $0 \neq P \trianglelefteq R$ ein Primideal und $a \in P \setminus \{0\}$. Nach Lemma II.11.26 existieren nicht-triviale Primideale $P_1, \ldots, P_n \trianglelefteq R$ mit $P_1 \ldots P_n \subseteq (a) \subseteq P$. Dabei sei n minimal gewählt. Aus der Primidealeigenschaft folgt $P_i \subseteq P$ für ein $i \in \{1, \ldots, n\}$; o. B. d. A. $i = 1$. Da jedes nicht-triviale Primideal maximal in R ist, gilt $P = P_1$. Wegen $P_2 \ldots P_n \nsubseteq (a)$ existiert ein $b \in P_2 \ldots P_n \setminus (a)$ (im Fall $n = 1$ sei $b \in R \setminus (a)$). Dann ist $Pb = P_1 b \subseteq P_1 \ldots P_n \subseteq (a)$ und $a^{-1}bP \subseteq R$, also $x := a^{-1}b \in P^{-1}$. Im Fall $x \in R$ wäre $b \in x(a) \subseteq (a)$.

Wegen $P \subseteq R$ ist $1 \in P^{-1}$ und $P \subseteq PP^{-1} \trianglelefteq R$. Da P maximal ist, können wir $PP^{-1} = P$ annehmen. Es folgt $PP^{-n} = P$ und $ax^n \in P \subseteq R$ für $n \geq 0$. Also ist $aR[x] \trianglelefteq R$. Da R noethersch ist, existieren

$a_1, \ldots, a_k \in R$ mit $aR[x] = Ra_1 + \ldots + Ra_k$. Dann ist auch $R[x] = R\frac{a_1}{a} + \ldots + R\frac{a_n}{a}$ ein endlich erzeugter R-Modul. Nach Lemma II.11.5 ist x ganz über R und man erhält den Widerspruch $x \in R$, da R ganz-abgeschlossen ist. □

Satz II.11.28 (Primidealzerlegung)**.** *Jedes nicht-triviale Ideal eines Dedekindrings ist ein Produkt von (bis auf die Reihenfolge) eindeutig bestimmten Primidealen.*

Beweis. Sei R ein Dedekindring und $0 \neq I \trianglelefteq R$. Im Fall $I = R$ ist I das leere Produkt von Primidealen. Sei also $I \neq R$. Nach Lemma II.11.26 gibt es nicht-triviale Primideale $P_1, \ldots, P_n$ mit $P_1 \ldots P_n \subseteq I$. Sei n minimal. Im Fall $n = 1$ ist $I = P_1$, da P_1 maximal ist. Sei also $n \geq 2$. Sei M ein maximales Ideal mit $I \subseteq M$. Wie üblich ist $P_i \subseteq M$ für ein $i \in \{1, \ldots, n\}$; sagen wir $i = 1$. Dann gilt sogar $P_1 = M$ und

$$P_2 \ldots P_n = M^{-1}P_1 \ldots P_n \subseteq M^{-1}I \subseteq M^{-1}M = R$$

nach Lemma II.11.27. Mit Induktion nach n ist $M^{-1}I$ ein Produkt von Primidealen, also auch $M(M^{-1}I) = I$.

Sei nun $P_1 \ldots P_n = Q_1 \ldots Q_m$ mit nicht-trivialen Primidealen $P_1, \ldots, P_n, Q_1, \ldots, Q_m \trianglelefteq R$. Dann ist $Q_1 \ldots Q_m \subseteq P_1$ also $Q_i \subseteq P_1$ für ein $i \in \{1, \ldots, m\}$. O. B. d. A. sei $i = 1$. Aus der Maximalität von Q_1 folgt $Q_1 = P_1$ und $Q_2 \ldots Q_m = Q_1^{-1}Q_1 \ldots Q_m = P_1^{-1}P_1 \ldots P_n = P_2 \ldots P_n$ nach Lemma II.11.27. Die Behauptung folgt nun mit Induktion nach n. □

Bemerkung II.11.29.

(i) Als Primideal ist auch (0) ein Produkt von Primidealen, wobei die Faktoren allerdings nicht mehr eindeutig bestimmt sind, denn $(0)^2 = (0)$.

(ii) Der Beweis von Satz II.11.28 zeigt, dass ein Primideal P genau dann in der Zerlegung von $I \trianglelefteq R$ vorkommt, wenn $I \subseteq P$.

Beispiel II.11.30. Wir hatten in Beispiel II.5.9 gesehen, dass $R := \mathbb{Z}[\sqrt{-5}]$ nicht faktoriell ist, denn

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}),$$

sind zwei verschiedene „Primfaktorzerlegungen“. Andererseits ist R nach Satz II.11.12 der Ganzheitsring des Zahlkörper $\mathbb{Q}(\sqrt{-5})$ und daher ein Dedekindring nach Satz II.11.24. Sei $P := (2, 1 + \sqrt{-5}) \trianglelefteq R$. Im Fall $1 \in P$ existieren $a, b, c, d \in \mathbb{Z}$ mit

$$1 = 2(a + b\sqrt{-5}) + (1 + \sqrt{-5})(c + d\sqrt{-5}) = 2a + c - 5d + (2b + c + d)\sqrt{-5}.$$

Dann wäre

$$1 = 2a + c - 5d \equiv c + d \equiv 2b + c + d \equiv 0 \pmod 2.$$

Also ist $P \lhd R$ und $R/P \cong \mathbb{F}_2$. Folglich ist P ein maximales Ideal und ein Primideal. Wegen

$$2 = 2(1 + \sqrt{-5}) - 2^2 - (1 + \sqrt{-5})^2 \in P^2$$
$$(1 + \sqrt{-5})^2 = 2(-2 + \sqrt{-5}) \in (2)$$

ist $(2) = P^2$. Analog zeigt man $(3) = Q\overline{Q}$ mit den Primidealen $Q := (3, 1 + \sqrt{-5})$ und $\overline{Q} := (3, 1 - \sqrt{-5})$ von R. Insgesamt ist $(6) = P^2Q\overline{Q}$ die eindeutige Primidealzerlegung von (6) in R. Im Folgenden untersuchen wir solche Zerlegungen systematisch.

Satz II.11.31. *Die gebrochenen Ideale eines Dedekindrings R bilden eine freie abelsche Gruppe I_R bzgl. Multiplikation mit Einselement R. Die gebrochenen Hauptideale bilden einen Normalteiler $H_R \trianglelefteq I_R$.*

Beweis. Sei I ein gebrochenes Ideal von R und $rI \subseteq R$ für ein $r \in R \setminus \{0\}$. Dann ist $rI, rR \trianglelefteq R$. Nach Satz II.11.28 existieren Primideale $P_1, \ldots, P_n, Q_1, \ldots, Q_m$ mit $rI = P_1 \ldots P_n$ und $rR = Q_1 \ldots Q_m$. Aus $(rR)(r^{-1}R) = R = Q_1 \ldots Q_m Q_1^{-1} \ldots Q_m^{-1}$ folgt $r^{-1}R = Q_1^{-1} \ldots Q_m^{-1}$ nach Lemma II.11.20(iv). Dies zeigt

$$I = (rI)(r^{-1}R) = P_1 \ldots P_n Q_1^{-1} \ldots Q_m^{-1}$$

und $I^{-1} = P_1^{-1} \ldots P_n^{-1} Q_1 \ldots Q_m$. Folglich ist jedes gebrochene Ideal invertierbar und die abelsche Gruppe I_R wird von den Primidealen erzeugt. Die Eindeutigkeit in Satz II.11.28 zeigt, dass die Primideale sogar eine Basis von I_R bilden. Offenbar ist $H_R \leq I_R$. Da I_R abelsch ist, gilt auch $H_R \trianglelefteq I_R$. □

Definition II.11.32. Man nennt I_R die *Idealgruppe* und I_R/H_R die *Klassengruppe* von R. Außerdem ist $|I_R/H_R|$ die *Klassenzahl* von R.

Bemerkung II.11.33.

(i) Die Dedekindringe mit Klassenzahl 1 sind offenbar genau die Hauptidealringe. Die Klassenzahl misst also wie weit ein Dedekindring von einem Hauptidealring entfernt ist. Man kann zeigen, dass $\mathbb{Z}[\sqrt{-5}]$ Klassenzahl 2 hat. Allgemeiner haben die Ganzheitsringe von Zahlkörpern stets endliche Klassenzahl (ohne Beweis).

(ii) Im Folgenden fassen wir die eindeutige Faktorisierung eines gebrochenen Ideals I in der Form $I = \prod_{i=1}^n P_i^{a_i}$ zusammen, wobei $P_1, \ldots, P_n$ paarweise verschiedene Primideale sind und $a_1, \ldots, a_n \in \mathbb{Z} \setminus \{0\}$.

(iii) Der nächste Satz zeigt, dass jede der Voraussetzungen eines Dedekindrings tatsächlich notwendig ist für die Existenz einer Primidealzerlegung.

Satz II.11.34. *Ein Integritätsbereich ist genau dann ein Dedekindring, wenn jedes gebrochene Ideal invertierbar ist.*

Beweis. Nach Satz II.11.31 erfüllt jeder Dedekindring die angegebene Bedingung. Sei umgekehrt R ein Integritätsbereich, in dem jedes gebrochene Ideal invertierbar ist. Sei $0 \neq I \trianglelefteq R$. Dann existieren $a_1, \ldots, a_n \in I$ und $b_1, \ldots, b_n \in I^{-1}$ mit $1 = a_1b_1 + \ldots + a_nb_n$. Für $x \in I$ gilt $x = (xb_1)a_1 + \ldots + (xb_n)a_n \in Ra_1 + \ldots + Ra_n$. Also ist $I = (a_1, \ldots, a_n)$ und R ist noethersch.

Sei nun $\{0 \neq P \trianglelefteq R$ ein Primideal und $M \trianglelefteq R$ maximal mit $P \subseteq M$. Wegen $M^{-1}P \subseteq M^{-1}M = R$ ist $M^{-1}P \trianglelefteq R$. Aus $M(M^{-1}P) = RP = P$ folgt $M = P$ oder $M^{-1}P \subseteq P$. Im zweiten Fall erhält man den Widerspruch $R = MM^{-1}PP^{-1} \subseteq MPP^{-1} \subseteq M$. Daher ist jedes nicht-triviale Primideal maximal.

Sei schließlich $x \in Q(R)^\times$ ganz über R. Dann ist $R[x] \neq 0$ endlich erzeugt, also ein gebrochenes Ideal nach Lemma II.11.20. Nach Voraussetzung ist $x \in R[x] = R[x]R[x]R[x]^{-1} = R[x]R[x]^{-1} = R$. Also ist R ganz-abgeschlossen und somit ein Dedekindring. □

Satz II.11.35. *Sei R ein Dedekindring und $I = \prod_{i=1}^n P_i^{a_i}$ und $J = \prod_{i=1}^n P_i^{b_i}$ Primidealzerlegungen mit $a_1, b_1, \ldots, a_n, b_n \in \mathbb{N}_0$. Dann gilt*

$$I + J = \prod_{i=1}^n P_i^{\min\{a_i, b_i\}}.$$

Insbesondere ist

(i) $I \subseteq J \iff \forall i : a_i \geq b_i$.

(ii) $I + J = R \iff \forall i : a_i b_i = 0$.

Beweis. Sei $c_i := \min\{a_i, b_i\}$ für $i = 1, \ldots, n$. Da $\prod P_i^{c_i}$ ein Faktor in $\prod P_i^{a_i}$ ist, gilt $I \subseteq \prod P_i^{c_i}$ und analog $J \subseteq \prod P_i^{c_i}$. Da das Produkt ein Ideal ist, folgt $I+J \subseteq \prod P_i^{c_i}$. Angenommen es gilt $I+J \subseteq P_i^{c_i+1}$ für ein i. O. B. d. A. sei $a_i = c_i$. Aus $I \subseteq I + J \subseteq P_i^{c_i+1}$ folgt $\prod_{j \neq i} P_j^{a_j} \subseteq P_i$. Dies widerspricht der Primidealeigenschaft. Daher ist $\prod P_i^{c_i}$ die Primidealzerlegung von $I + J$. Die letzten beiden Aussagen folgen unmittelbar. □

Folgerung II.11.36. *Sei R ein Dedekindring und $0 \neq x \in I \trianglelefteq R$. Dann existiert $y \in I$ mit $I = (x, y)$.*

Beweis. Seien $I = \prod_{i=1}^n P_i^{a_i}$ und $(x) = \prod_{i=1}^n P_i^{b_i}$ die Primidealzerlegungen von I und (x). Wegen $(x) \subseteq I$ gilt $a_i \leq b_i$ für $i = 1, \ldots, n$. Seien $x_i \in P_i^{a_i} \setminus P_i^{a_i+1}$. Nach Satz II.11.35 gilt $P_i^{a_i+1} + P_j^{a_j+1} = R$ für $i \neq j$. Nach dem chinesischen Restsatz I.7.30 existiert $y \in R$ mit $y \equiv x_i \pmod{P_i^{a_i+1}}$ für $i = 1, \ldots, n$. Dann gilt $y \in P_i^{a_i} \setminus P_i^{a_i+1}$, d. h. a_i ist der Exponent von P_i in der Primidealzerlegung von (y). Mit Satz II.11.35 folgt $I = (x) + (y) = (x, y)$. □

Lemma II.11.37. *Seien $R \subseteq S$ Dedekindringe und S ganz über R. Für $I \lhd R$ ist $SI \lhd S$ und für $0 \neq J \trianglelefteq S$ ist $0 \neq J \cap R \trianglelefteq R$.*

Beweis. Wir fassen R, S und $Q(R)$ als Teilringe von $Q(S)$ auf. Da R ganz-abgeschlossen ist, gilt $S \cap Q(R) = R$. Sicher ist $SI \trianglelefteq S$ und es genügt $SI \neq S$ zu zeigen. Dafür können wir annehmen, dass I maximal ist. Für $x \in I \setminus I^2$ gilt $Rx = II'$, wobei $I' \trianglelefteq R$ ein Produkt von Primidealen $\neq I$ ist. Insbesondere gilt $I + I' = R$ nach Satz II.11.35. Sei $1 = y + a$ mit $y \in I$ und $a \in I'$. Dann ist $a \notin I$ und $aI \subseteq II' = Rx$. Im Fall $SI = S$ wäre $aS = aIS \subseteq xS$ und $a = xz$ mit $z = \frac{a}{x} \in S \cap Q(R) = R$, d. h. $a \in I$. Widerspruch.

Sicher ist $J \cap R \trianglelefteq R$ und es genügt $J \cap R \neq 0$ zu zeigen. Sei $x \in J \setminus \{0\}$. Da S ganz über R ist, existieren $a_0, \ldots, a_n \in R$ mit $x^{n+1} + a_n x^n + \ldots + a_0 = 0$. O. B. d. A. sei $a_0 \neq 0$. Dann ist $a_0 = -x^{n+1} - a_n x^n - \ldots - a_1 x \in J \cap R$. □

Definition II.11.38. Sei K ein Zahlkörper und $P \trianglelefteq \mathbb{Z}_K$ ein nicht-triviales Primideal. Lemma II.11.37 mit $R = \mathbb{Z}$ zeigt $P \cap \mathbb{Z} = (p)$ für eine Primzahl $p \in \mathbb{N}$.

- Der Exponent $e_p(P)$ von P in der Primidealzerlegung von $\mathbb{Z}_K p$ heißt *Verzweigungsindex* von P bzgl. p.
- Wegen $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} \cong (\mathbb{Z} + P)/P \subseteq \mathbb{Z}_K/P$ kann man $\mathbb{Z}_K/P$ als Körpererweiterung von $\mathbb{F}_p$ ansehen. Man nennt $f_p(P) := |\mathbb{Z}_K/P : \mathbb{F}_p|$ den *Trägheitsgrad* von P bzgl. p. Nach Satz II.11.15 ist $f_p(P) < \infty$, d. h. $\mathbb{Z}_K/P \cong \mathbb{F}_{p^{f_p(P)}}$.

Satz II.11.39 (Fundamentalgleichung)**.** *Sei K ein Zahlkörper und $p \in \mathbb{N}$ eine Primzahl. Seien $P_1, \ldots, P_n$ die Primideale von $\mathbb{Z}_K$, die p enthalten. Dann gilt*

$$\boxed{|K : \mathbb{Q}| = \sum_{i=1}^{n} e_p(P_i) f_p(P_i).}$$

Beweis. Sei $d := |K : \mathbb{Q}|$. Nach Satz II.11.15 ist $\mathbb{Z}_K$ eine freie abelsche Gruppe mit Basis $b_1, \ldots, b_d$. Offenbar ist $pb_1, \ldots, pb_d$ eine Basis von $\mathbb{Z}_K p$. Dies zeigt $|\mathbb{Z}_K/\mathbb{Z}_K p| = p^d$ (Satz II.9.28). Sei $e_i := e_p(P_i)$ und $f_i := f_p(P_i)$ für $i = 1, \ldots, n$. Für $i \neq j$ gilt $P_i^{e_i} + P_j^{e_j} = \mathbb{Z}_K$ nach Satz II.11.35. Mit dem chinesischen Restsatz folgt

$$\mathbb{Z}_K/\mathbb{Z}_K p = \mathbb{Z}_K/P_1^{e_1} \ldots P_n^{e_n} \cong (\mathbb{Z}_K/P_1^{e_1}) \times \ldots \times (\mathbb{Z}_K/P_n^{e_n}).$$

Es genügt daher $|\mathbb{Z}_K/P_i^{e_i}| = p^{e_i f_i}$ für $i = 1, \ldots, n$ zu beweisen. Wir zeigen genauer $|P_i^k/P_i^{k+1}| = p^{f_i}$ für $k \in \mathbb{N}_0$. Für $a \in P_i^k \setminus P_i^{k+1}$ ist die Abbildung

$$\begin{aligned} \varphi\colon \mathbb{Z}_K &\to P_i^k/P_i^{k+1}, \\ x &\mapsto xa + P_i^{k+1} \end{aligned}$$

ein Homomorphismus vom $\mathbb{Z}_K$-Moduln mit $P_i \subseteq \mathrm{Ker}(\varphi)$. Wegen $a \notin P_i^{k+1}$ ist $\mathrm{Ker}(\varphi) \lhd \mathbb{Z}_K$. Die Maximalität von P_i zeigt $\mathrm{Ker}(\varphi) = P_i$. Sei $\varphi(\mathbb{Z}_K) = Q/P_i^{k+1}$ mit $Q = \mathbb{Z}_K a + P_i^{k+1} \trianglelefteq \mathbb{Z}_K$. Wegen $P_i^{k+1} \subsetneq Q$ ist P_i das einzige Primideal, das Q enthält. Die eindeutige Primidealzerlegung liefert $Q = P_i^k$, d. h. φ ist surjektiv. Dies zeigt

$$|P_i^k/P_i^{k+1}| = |\varphi(\mathbb{Z}_K)| = |\mathbb{Z}_K/\mathrm{Ker}(\varphi)| = |\mathbb{Z}_K/P_i| = p^{f_i}$$

wie behauptet. □

Satz II.11.40. *Sei $p \in \mathbb{P}$, $\mathbb{Q} \subseteq K$ eine Galois-Erweiterung und $P \trianglelefteq \mathbb{Z}_K$ ein Primideal mit $p \in P$. Dann ist $\{\alpha(P) : \alpha \in \mathrm{Gal}(K|\mathbb{Q})\}$ die Menge der Primideale von $\mathbb{Z}_K$, die p enthalten. Insbesondere hängen $e_p(P)$ und $f_p(P)$ nicht von der Wahl von P ab. Außerdem ist $e_p(P) f_p(P)$ ein Teiler von $|K : \mathbb{Q}|$.*

Beweis. Für $\sigma \in G := \mathrm{Gal}(K|\mathbb{Q})$ und $x \in \mathbb{Z}_K$ ist auch $\sigma(x) \in \mathbb{Z}_K$ (gleiches Minimalpolynom). Das gleiche Argument mit σ^{-1} liefert $\sigma(\mathbb{Z}_K) \subseteq \mathbb{Z}_K = \sigma(\sigma^{-1}(\mathbb{Z}_K)) \subseteq \sigma(\mathbb{Z}_K)$, d. h. σ ist ein Ringautomorphismus von $\mathbb{Z}_K$. Mit P ist auch $\sigma(P)$ ein Primideal mit $p = \sigma(p) \in \sigma(P)$. Angenommen es existiert ein Primideal $Q \trianglelefteq \mathbb{Z}_K$ mit $p \in Q$ außerhalb der Bahn von P unter G. Nach dem chinesischen Restsatz für Ringe existiert $x \in P$ mit $x \equiv 1 \pmod{\sigma(Q)}$ für alle $\sigma \in G$. Dann ist einerseits

$$\prod_{\sigma \in G} \sigma(x) \in P \cap \mathbb{Q} = P \cap \mathbb{Z}_K \cap \mathbb{Q} = P \cap \mathbb{Z} = (p)$$

und andererseits

$$\prod_{\sigma \in G} \sigma(x) \in (1+Q)^{|G|} \cap \mathbb{Z} \subseteq (1+Q) \cap \mathbb{Z} = 1 + (p).$$

Dieser Widerspruch zeigt die erste Behauptung. Die zweite Behauptung ergibt sich, indem man $\sigma \in G$ auf die Primidealzerlegung von $\mathbb{Z}_K p$ anwendet. Die letzte Behauptung folgt aus Satz II.11.39. □

Bemerkung II.11.41. In der Situation von Satz II.11.40 nennt man p

- *träge*, falls $f_p(P) = |K : \mathbb{Q}|$ (dann ist p ein Primelement in $\mathbb{Z}_K$).
- *verzweigt*, falls $e_p(P) > 1$.
- *zerlegt*, falls $e_p(P) = f_p(P) = 1$.

(vgl. Beispiel II.5.33).

Satz II.11.42. *Sei $\mathbb{Q} \subseteq K$ eine Galois-Erweiterung mit primitivem Element $x \in \mathbb{Z}_K$. Sei μ das Minimalpolynom von x. Dann ist jede verzweigte Primzahl ein Teiler der Diskriminante D_μ. Insbesondere existieren nur endlich viele verzweigte Primzahlen bzgl. K.*

Beweis. Sei $p \in \mathbb{P}$ kein Teiler von D_μ und $P \trianglelefteq \mathbb{Z}_K$ ein Primideal mit $p \in P$. Sei $G := \mathrm{Gal}(K|\mathbb{Q})$ und $G_P := \{\sigma \in G : \sigma(P) = P\}$ der Stabilisator von P. Nach Satz II.11.40 und Satz I.4.7 gilt

$$|G| = |K : \mathbb{Q}| = |G : G_P| e_p(P) f_p(P)$$

und $|G_P| = e_p(P) f_p(P)$. Da x ganz ist, gilt $\mu \in \mathbb{Z}[X]$ und $\mu = (X - x_1) \dots (X - x_n)$ mit $x_1, \dots, x_n \in \mathbb{Z}_K$. Die Reduktion $\overline{\mu} \in \mathbb{F}_p[X]$ zerfällt in $\overline{K} := \mathbb{Z}_K / P$ in der Form $\overline{\mu} = (X - \overline{x_1}) \dots (X - \overline{x_n})$, wobei $\overline{x_i} := x_i + P$. Nach Voraussetzung ist $D_{\overline{\mu}} = \overline{D_\mu} \neq 0$. Daher sind $\overline{x_1}, \dots \overline{x_n}$ paarweise verschieden. Wie im Beweis von Satz II.11.40 gilt $g(\mathbb{Z}_K) = \mathbb{Z}_K$ für alle $g \in G$. Für $g \in G_P$ ist $\overline{K} \to \overline{K}$, $\lambda + P \mapsto g(\lambda) + P$ ein Körperautomorphismus. Dies liefert einen Homomorphismus $\varphi \colon G_P \to \mathrm{Gal}(\overline{K}|\mathbb{F}_p)$. Da G treu auf $\{x_1, \dots, x_n\}$ operiert, ist auch die Operation von G_P auf $\{\overline{x_1}, \dots, \overline{x_n}\}$ treu. Insbesondere ist φ injektiv und

$$e_p(P) f_p(P) = |G_P| \leq |\mathrm{Gal}(\overline{K}|\mathbb{F}_p)| = |\mathbb{Z}_K : \mathbb{F}_p| = f_p(P). \tag{II.11.1}$$

Es folgt $e_p(P) = 1$ und p ist unverzweigt. □

Satz II.11.43 (Dedekind)**.** *Sei $\alpha \in \mathbb{Z}[X]$ normiert und $p \in \mathbb{P}$ kein Teiler von D_α. Die Reduktion $\overline{\alpha} \in \mathbb{F}_p[X]$ sei ein Produkt von irreduziblen Polynomen mit Graden $d_1, \dots, d_k$. Dann besitzt* $\mathrm{Gal}(\alpha)$ *ein Element vom Zyklentyp $(d_1, \dots, d_k)$ bzgl. der Operation auf den Nullstellen von α.*

Beweis. Wir benutzen die Bezeichnungen aus dem Beweis von Satz II.11.42 mit α anstelle von μ (Irreduzibilität wird nicht benötigt). Wegen $p \nmid D_\alpha$ und (II.11.1) ist $\varphi \colon G \to \overline{G} := \mathrm{Gal}(\overline{K}|\mathbb{F}_p)$ sogar ein Isomorphismus. Nach Satz I.11.14 ist $\overline{G} = \langle F \rangle$ zyklisch, wobei F der Frobenius-Automorphismus ist. Sei $\overline{\alpha} = \overline{\alpha}_1 \dots \overline{\alpha}_k$ mit $d_k = \deg \overline{\alpha}_i$ für $i = 1, \dots, k$. Da die Nullstellen von $\overline{\alpha}$ paarweise verschiedenen sind, gilt $\overline{\alpha}_i \neq \overline{\alpha}_j$ für $i \neq j$. Da $\overline{\alpha}_i$ irreduzibel ist, muss F die Nullstellen von $\overline{\alpha}_i$ transitiv permutieren. Also hat F den Zyklentyp $(d_1, \dots, d_k)$ auf den Nullstellen von $\overline{\alpha}$. Man wähle nun $\varphi^{-1}(F) \in G$. □

Bemerkung II.11.44. Der im Beweis von Satz II.11.43 konstruierte Galois-Automorphismus $\gamma := \varphi^{-1}(F)$ erfüllt $\gamma(x) \equiv F(x) \equiv x^p \pmod{P}$ für alle $x \in \mathbb{Z}_K$ und heißt daher *Frobenius-Element* von K bzgl. P. Da die p enthaltenden Primideale von $\mathbb{Z}_K$ unter G konjugiert sind, bestimmt jede unverzweigte Primzahl p genau eine Konjugationsklasse von Frobenius-Elementen. Nach dem tiefliegende *Dichtheitssatz* von Tschebotarjow verteilen sich die unverzweigten Primzahlen „gleichmäßig“ auf die Konjugationsklassen von G: Für $g \in G$ beträgt der Anteil der Primzahlen, deren Frobenius-Element zu g konjugiert ist, genau $\frac{1}{|\mathrm{C}_G(g)|}$. Insbesondere findet man für jeden Zyklentyp von Elementen von G unendlich viele entsprechende Primzahlen. Der Anteil der zerlegten Primzahlen (d. h. das Frobenius-Element ist 1) beträgt $\frac{1}{|G|} = \frac{1}{|K:\mathbb{Q}|}$.

Beispiel II.11.45.

(i) Sei $n \in \mathbb{N}$, $K = \mathbb{Q}_n$ und $\zeta \in K$ eine primitive n-te Einheitswurzel. Dann ist $G := \mathrm{Gal}(K|\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$ abelsch. Nach Bemerkung A.3.18 stimmen die Primteiler von n und D_{Φ_n} überein. Sei also $p \in \mathbb{P}$ mit $p \nmid n$ und $P \trianglelefteq \mathbb{Z}_K$ ein Primideal mit $p \in P$. Sei $\sigma \in G_P$ mit $\sigma(\zeta) = \zeta^a$. Nach Satz A.3.17 gilt $\mathbb{Z}_K = \mathbb{Z}[\zeta]$. Daher ist σ genau dann das Frobenius-Element bzgl. P, wenn $\zeta^a \equiv \zeta^p \pmod{P}$ gilt. Wegen $D_{\overline{\Phi_n}} = \overline{D_{\Phi_n}} \neq 0$ sind die primitiven Einheitswurzeln modulo P paarweise verschieden. Es gilt also

$$\zeta^a \equiv \zeta^p \pmod{P} \iff \zeta^a = \zeta^p \iff p \equiv a \pmod{n}.$$

Nach dem Dichtheitssatz ist der Anteil der Primzahlen $p \in a + n\mathbb{Z}$ genau $\frac{1}{\varphi(n)}$. Insbesondere gibt es unendlich viele solche Primzahlen für jedes $a + n\mathbb{Z} \in (\mathbb{Z}/n\mathbb{Z})^\times$, d. h. Dirichlets Primzahlsatz gilt.

(ii) Es gibt eine einfache Methode zur Konstruktion von Galoisgruppen mit vorgegebenen Zyklentypen. Für $p \in \mathbb{P}$ und $d \in \mathbb{N}$ gibt es $\varphi(p^d - 1)$ Erzeuger der zyklischen Gruppe $\mathbb{F}_{p^d}^\times$. Das Minimalpolynom jedes Erzeugers über $\mathbb{F}_p$ ist irreduzibel vom Grad d. Je d solche Erzeuger bestimmen also ein irreduzibles Polynom in $\mathbb{F}_p[X]$ vom Grad d. Da $\varphi(p^d - 1)/d$ mit p gegen unendlich strebt, findet man für genügend große p beliebig viele paarweise verschiedene irreduzible Polynome vom Grad d.

Sei nun $(d_1, \ldots, d_k)$ eine Partition von $n \in \mathbb{N}$, d. h. $d_1 + \ldots + d_k = n$. Dann existiert für „große“ p ein normiertes Polynom $\beta_p \in \mathbb{F}_p[X]$ vom Grad n mit paarweise verschiedenen Primfaktoren mit den Graden $d_1, \ldots, d_k$. Ist eine weitere Partition $(e_1, \ldots, e_l)$ von n gegeben, so findet man eine Primzahl $q \neq p$ und $\beta_q \in \mathbb{F}_q[X]$ normiert mit paarweise verschiedenen Primfaktoren mit Graden $e_1, \ldots, e_l$. Auf die gleiche Weise kann man beliebig viele weitere Zyklentypen hinzunehmen. Nach dem chinesischen Restsatz existiert $\alpha \in \mathbb{Z}[X]$ mit $\alpha \equiv \beta_p \pmod{p}$ und $\alpha \equiv \beta_q \pmod{q}$. Da β_p und β_q normiert vom Grad n sind, kann man auch α normiert vom Grad n wählen. Da β_p und β_q paarweise verschiedene Nullstellen haben, ist D_α weder durch p noch durch q teilbar. Satz II.11.43 liefert Elemente in $\mathrm{Gal}(\alpha)$ mit Zyklentyp $(d_1, \ldots, d_k)$ und $(e_1, \ldots, e_l)$.

(iii) Sei $\alpha \in \mathbb{Z}[X]$ normiert vom Grad n und $p \in \mathbb{P}$ zerlegt bzgl. des Zerfällungskörpers von α. Dann zerfällt die Reduktion $\overline{\alpha} \in \mathbb{F}_p[X]$ in paarweise verschiedene Linearfaktoren. Insbesondere ist $p \geq n$.

Lemma II.11.46. *Sei $G \leq S_n$ transitiv. Enthält G eine Transposition und einen Zyklus der Länge $n - 1$, so gilt $G = S_n$.*

Beweis. O. B. d. A. sei $\sigma := (2, \ldots, n) \in G$. Sei $\tau := (a, b) \in G$ eine Transposition. Da G transitiv ist, existiert $\rho \in G$ mit $\rho(a) = 1$. Indem wir τ durch $\rho\tau\rho^{-1} = (\rho(a), \rho(b))$ ersetzen, können wir $a = 1$ annehmen. Konjugation von τ mit den Potenzen von σ liefert die Transpositionen $(1, 2), (1, 3), \ldots, (1, n) \in G$. Bekanntlich wird S_n von diesen Transpositionen erzeugt. □

Satz II.11.47. *Für jedes $n \in \mathbb{N}$ existiert ein Polynom $\alpha \in \mathbb{Q}[X]$ mit Galoisgruppe S_n.*

Beweis. O. B. d. A. sei $n \geq 2$. Nach Beispiel II.11.45 existiert ein normiertes Polynom $\alpha \in \mathbb{Z}[X]$, sodass $G := \mathrm{Gal}(\alpha)$ Zyklen der Länge 2, $n - 1$ und n besitzt. Insbesondere operiert G transitiv auf der Menge der Nullstellen von α. Aus Lemma II.11.46 folgt $G \cong S_n$. □

12 Endlich-dimensionale Algebren

Bemerkung II.12.1. Viele der bisher betrachteten Ringe besitzen auch eine Vektorraumstruktur (z. B. $K[X]$ oder $K^{n\times n}$). Mit Methoden der linearen Algebra werden wir frühere Strukturaussagen verbessern. Anschließend ordnen wir jeder endlichen Gruppe einen solchen Ring zu und untersuchen seine Eigenschaften.

Definition II.12.2. Eine *Algebra* über einem Körper K (kurz eine *K-Algebra*) ist ein Ring A und zugleich ein K-Vektorraum, sodass die Skalarmultiplikation und die Ringmultiplikation kompatibel sind, d. h. es gilt

$$\lambda(ab) = (\lambda a)b = a(\lambda b)$$

für alle $\lambda \in K$ und $a, b \in A$. Man nennt A *endlich-dimensional*, falls $\dim_K A < \infty$. Eine Algebra, die als Ring ein Schiefkörper ist, bezeichnet man als *Divisionsalgebra*.

Bemerkung II.12.3.

(i) Eine *Unteralgebra* einer K-Algebra A ist ein Teilring von A, der zugleich ein K-Vektorraum ist. Man kann K mit dem Teilring $K1_A$ von A identifizieren.

(ii) Wenn nichts anderes gesagt wird, nehmen wir im Folgenden stets an, dass A eine endlich-dimensionale K-Algebra ist und dass jeder A-Modul M endlich erzeugt ist. Durch

$$\lambda m := (\lambda 1_A)m \qquad (\lambda \in K,\ m \in M)$$

wird M zu einem K-Vektorraum. Sei $b_1, \ldots, b_s \in A$ eine K-Basis von A und $M = Am_1 + \ldots + Am_t$ mit $m_1, \ldots, m_t \in M$. Dann ist

$$M = \sum_{i=1}^{s} \sum_{j=1}^{t} Kb_i m_j,$$

d. h. $\{b_i m_j : 1 \le i \le s, 1 \le j \le t\}$ ist ein Erzeugendensystem von M als K-Vektorraum. Insbesondere ist $\dim_K M < \infty$. Da auch alle Untermoduln von M Untervektorräume sind, ist M noethersch und artinsch. Die Wahl $M = A$ zeigt, dass auch A artinsch (und noethersch) ist. Wir können daher die Sätze aus Kapitel II.8 anwenden. Insbesondere besitzt A eine Peirce-Zerlegung in Blöcke, die selbst Algebren sind (da Ideale).

(iii) Sei $f\colon M \to N$ ein Homomorphismus von A-Moduln. Wegen

$$f(\lambda m) = f((\lambda 1_A)m) = (\lambda 1_A)f(m) = \lambda f(m)$$

für $\lambda \in K$ und $m \in M$ ist f auch K-linear. Es gilt also $\mathrm{Hom}_A(M,N) \subseteq \mathrm{Hom}_K(M,N)$ und $\mathrm{End}_A(M) \subseteq \mathrm{End}_K(M)$. Für $f \in \mathrm{End}_A(M)$ und $\lambda \in K$ gilt $\lambda f := (\lambda 1_A)f \in \mathrm{End}_A(M)$. Auf diese Weise wird $\mathrm{End}_A(M)$ zu einer K-Algebra. Nach Schurs Lemma ist $\mathrm{End}_A(M)$ eine Divisionsalgebra, falls M einfach ist.

(iv) Ein *Homomorphismus* von K-Algebren A und B ist ein Ringhomomorphismus $A \to B$, der zugleich K-linear ist. Wie üblich definiert man Epi-, Mono-, Iso- und Automorphismen von Algebren. Der Homomorphiesatz, die Isomorphiesätze und der chinesische Restsatz gelten dann auch für Algebren (alle Abbildungen sind K-linear).

(v) Ist A eine halbeinfache Algebra, so existieren Divisionsalgebren $D_1, \ldots, D_k$ mit $A \cong D_1^{d_1 \times d_1} \times \ldots \times D_k^{d_k \times d_k}$. Da die im Beweis von Artin-Wedderburn benutzen Abbildungen alle K-linear sind, handelt es sich dabei um einen Isomorphismus von Algebren. Außerdem ist d_i die Vielfachheit des einfachen A-Moduls $M_i := D_i^{d_i \times 1}$ als Kompositionsfaktor des regulären Moduls. Gleichzeitig ist d_i die Dimension von M_i über $\mathrm{End}_A(M_i) \cong D_i^o$.

Beispiel II.12.4.

(i) Für jeden Körper K und $n \in \mathbb{N}$ ist $K^{n \times n}$ eine endlich-dimensionale K-Algebra. Dagegen sind $K[X]$ und $K[[X]]$ (Aufgabe II.30) unendlich-dimensionale K-Algebren.

(ii) Für jede K-Algebra A ist auch $\mathrm{Z}(A)$ eine K-Algebra.

(iii) Sind $A_1, \ldots, A_n$ Algebren über K, so auch das direkte Produkt $A_1 \times \ldots \times A_n$.

(iv) Ist $K \subseteq L$ eine Körpererweiterung, so ist L eine K-Algebra.

(v) Jeder Schiefkörper Q ist eine $\mathrm{Z}(Q)$-Algebra.

Lemma II.12.5. *Für jede Algebra A und $n \in \mathbb{N}$ gilt:*

(i) $\boxed{\mathrm{Z}(A^{n \times n}) = \mathrm{Z}(A)1_n \cong \mathrm{Z}(A).}$

(ii) $\boxed{\mathrm{J}(A^{n \times n}) = \mathrm{J}(A)^{n \times n}.}$

Beweis.

(i) Sicher ist $\mathrm{Z}(A)1_n \subseteq \mathrm{Z}(A^{n \times n})$. Sei umgekehrt $M = (a_{ij}) \in \mathrm{Z}(A^{n \times n})$. Für $s \neq t$ sei $E_{st} := (\delta_{is}\delta_{jt})_{i,j}$ die Matrix mit einer 1 an Position (s,t) und sonst nur Nullen Dann ist

$$(\delta_{jt}a_{is})_{i,j} = \Big(\sum_{k=1}^{n} a_{ik}\delta_{ks}\delta_{jt}\Big)_{i,j} = ME_{st} = E_{st}M = \Big(\sum_{k=1}^{n} \delta_{is}\delta_{kt}a_{kj}\Big)_{i,j} = (\delta_{is}a_{tj})_{i,j}$$

und es folgt $M \in A1_n$. Sicher ist auch $M \in \mathrm{Z}(A1_n) = \mathrm{Z}(A)1_n$.

(ii) Sei $J := \mathrm{J}(A)$. Eine Induktion nach k zeigt $(J^{n \times n})^k \subseteq (J^k)^{n \times n}$. Da J nach Lemma II.8.15 nilpotent ist, ist auch $J^{n \times n}$ nilpotent. Dies zeigt $J^{n \times n} \subseteq \mathrm{J}(A^{n \times n})$. Sei umgekehrt $a = (a_{ij})_{ij} \in \mathrm{J}(A^{n \times n})$ und $E_{st} = (\delta_{is}\delta_{jt}) \in A^{n \times n}$. Sei $I \trianglelefteq A$ das von a_{st} erzeugte Ideal. Dann ist

$$IE_{11} \subseteq (E_{1s}aE_{t1}) \subseteq \mathrm{J}(A^{n \times n}).$$

Da $\mathrm{J}(A^{n \times n})$ nilpotent ist, muss auch I nilpotent sein. Dies zeigt $a_{st} \in I \subseteq J$ und $\mathrm{J}(A^{n \times n}) \subseteq J^{n \times n}$. □

Lemma II.12.6. *Jede Divisionsalgebra über einem algebraisch abgeschlossenen Körper K ist zu K isomorph.*

Beweis. Sei D eine K-Divisionsalgebra und $x \in D$. Dann sind die Potenzen $1_D, x, x^2, \ldots$ linear abhängig über K. Daher existiert ein normiertes $\alpha \in K[X] \setminus K$ mit $\alpha(x) = 0$. Da K algebraisch abgeschlossen ist, zerfällt α in Linearfaktoren, etwa $\alpha = (X - \lambda_1 1_D) \ldots (X - \lambda_n 1_D)$ mit $\lambda_1, \ldots, \lambda_n \in K$. Als Divisionsalgebra besitzt D keine Nullteiler. Aus $\alpha(x) = 0$ folgt also $x - \lambda_i 1_D = 0$ für ein $i \in \{1, \ldots, n\}$. Daher ist $x = \lambda_i 1_D$ und $D = K1_D \cong K$. □

Bemerkung II.12.7. Frobenius hat gezeigt, dass $\mathbb{R}$, $\mathbb{C}$ und $\mathbb{H}$ (Aufgabe I.50) die einzigen endlichdimensionalen Divisionsalgebren über $\mathbb{R}$ sind (siehe Satz III.7.24).

Definition II.12.8. Ein Ring R heißt *lokal*, wenn R nur ein maximales Linksideal besitzt.

Beispiel II.12.9.

(i) Jeder Schiefkörper ist ein lokaler Ring mit maximalem Linksideal 0.

(ii) Sei R ein Dedekindring mit nicht-trivialem Primideal P. Dann ist R/P^n für alle $n \in \mathbb{N}$ lokal mit maximalem (Links)ideal P/P^n. Insbesondere erhält man die lokalen Ringe $K[X]/(X^n)$ und $\mathbb{Z}/2^n\mathbb{Z}$.

(iii) Der Ring der formalen Potenzreihen $K[[X]]$ (Aufgabe II.30) ist lokal mit maximalem Ideal (X), denn $K[[X]]^\times = K[[X]] \setminus (X)$.

(iv) Sei R ein lokaler Hauptidealring (z. B. $K[[X]]$). Dann sind die Potenzen von $\mathrm{J}(R)$ die einzigen echten Ideale von R. Man spricht dann von einem *diskreten Bewertungsring*.

Lemma II.12.10 (Heben von Idempotenten)**.** *Sei R ein Ring und $I \trianglelefteq R$ nilpotent. Für jedes Idempotent $\bar{e} \in R/I$ existiert ein Idempotent $e \in R$ mit $e + I = \bar{e}$.*

Beweis (Koh). Sei $a \in R$ beliebig mit $a + I = \bar{e}$. Dann ist $(1-a)a = a - a^2 \in I$. Da I nilpotent ist, existiert ein $n \in \mathbb{N}$ mit $(1-a)^n a^n = ((1-a)a)^n = 0$. Sei

$$e := \sum_{i=0}^{n} \binom{2n}{i} (1-a)^i a^{2n-i}, \qquad f := \sum_{i=n+1}^{2n} \binom{2n}{i} (1-a)^i a^{2n-i}.$$

Dann gilt

$$e + f = \sum_{i=0}^{2n} \binom{2n}{i} (1-a)^i a^{2n-i} = ((1-a) + a)^{2n} = 1.$$

Wegen $a^{2n-i}(1-a)^j = 0$ für $0 \le i \le n$ und $n+1 \le j \le 2n$ gilt $ef = 0$. Dies zeigt $e = e(e+f) = e^2 + ef = e^2$ und $e \equiv a^{2n} \equiv a \pmod{I}$. □

Satz II.12.11. *Für jede Algebra A sind folgende Aussagen äquivalent:*

(1) A ist lokal.

(2) $A/\mathrm{J}(A)$ ist eine Divisionsalgebra.

(3) Jedes Element in A ist invertierbar oder nilpotent.

(4) 0 und 1 sind die einzigen Idempotente von A.

(5) Der reguläre A-Modul ist unzerlegbar.

Beweis.

(1) $\Rightarrow$ (2): Offenbar ist $\mathrm{J}(A)$ das einzige maximale Linksideal. Insbesondere ist $A/\mathrm{J}(A)$ eine einfache Algebra, also von der Form $A/\mathrm{J}(A) = D^{n\times n}$ für eine Divisionsalgebra D. Im Fall $n > 1$ wäre $D^{n\times 1}$ ein echtes Linksideal in $A/\mathrm{J}(A)$. Nach dem Korrespondenzsatz ist dies ausgeschlossen.

(2) $\Rightarrow$ (3): Nach Lemma II.8.15 ist $\mathrm{J}(A)$ nilpotent und besteht daher nur aus nilpotenten Elementen. Sei $a \in A \setminus \mathrm{J}(A)$. Nach Voraussetzung existiert $b \in A$ mit $ab \equiv 1 \pmod{\mathrm{J}(A)}$ und $c := 1 - ab \in \mathrm{J}(A)$. Dann existiert ein $n \in \mathbb{N}$ mit $c^n = 0$. Dies zeigt

$$a \cdot b \sum_{k=0}^{n-1} c^k = (1-c) \sum_{k=0}^{n-1} c^k = 1.$$

Eine analoge Rechnung mit $1 - ba$ ergibt $a \in A^\times$.

(3) $\Rightarrow$ (4): Sei $e = e^2 \in A$. Im Fall $e \in A^\times$ ist $e = 1$. Anderenfalls ist $e^n = 0$ für ein $n \in \mathbb{N}$. Dann folgt $e = e^2 = \ldots = e^n = 0$.

(4) $\Leftrightarrow$ (5): Folgt aus $A \cong \mathrm{End}_A(A)^o$ (Lemma II.7.20) und Satz II.8.22.

(4) $\Rightarrow$ (1): Nach Lemma II.12.10 besitzt die halbeinfache Algebra $A/\mathrm{J}(A)$ (Lemma II.8.13) nur die Idempotente 0 und 1. Jede Komponente $D^{n\times n}$ in der Artin-Wedderburn-Zerlegung von $A/\mathrm{J}(A)$ liefert aber (mindestens) n Idempotente $E_{11}, \ldots, E_{nn}$ nach Beispiel II.8.19. Daher muss $A/\mathrm{J}(A)$ selbst eine Divisionsalgebra sein. □

Bemerkung II.12.12.

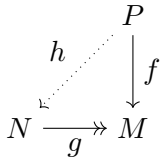
(i) Eine einfache lokale Algebra ist eine Divisionsalgebra.

(ii) Ein A-Modul M ist genau dann unzerlegbar, wenn $\mathrm{End}_A(M)$ lokal ist (Satz II.8.22).

Satz II.12.13. *Für jeden Ring R und jeden R-Modul P sind folgende Aussagen äquivalent:*

(1) P ist ein direkter Summand eines freien R-Moduls.

(2) Für jeden Homomorphismus $f\colon P \to M$ und jeden Epimorphismus $g\colon N \to M$ existiert ein Homomorphismus $h\colon P \to N$ mit $g \circ h = f$.



(3) Für jeden Epimorphismus $g\colon M \to P$ existiert ein Untermodul $N \leq M$ mit $M = \mathrm{Ker}(g) \oplus N$.

Gegebenenfalls nennt man P projektiv.

Beweis.

(1) $\Rightarrow$ (2): Sei F ein freier R-Modul mit Basis B und $F = P \oplus Q$. Sei $\pi\colon F \to P$ die Projektion. Für $b \in B$ existiert $x_b \in N$ mit $g(x_b) = f(\pi(b))$, da g surjektiv ist. Wir definieren $h\colon F \to N$ durch $h(b) := x_b$. Für $x = \sum_{b\in B} \lambda_b b \in P$ mit $\lambda_b \in A$ gilt

$$g(h(x)) = \sum_{b\in B} \lambda_b g(h(b)) = \sum_{b\in B} \lambda_b g(x_b) = \sum_{b\in B} \lambda_b f(\pi(b)) = f\Big(\pi\Big(\sum_{b\in B} \lambda_b b\Big)\Big) = f(\pi(x)) = f(x).$$

(2) $\Rightarrow$ (3): Für $f = \mathrm{id}_P$ existiert $h\colon P \to M$ mit $g \circ h = f$. Sei $N := h(P) \leq M$. Für $m \in M$ und $x := h(g(m)) \in N$ gilt $g(m) = f(g(m)) = g(x)$ und $m - x \in \mathrm{Ker}(g)$. Dies zeigt $M = \mathrm{Ker}(g) + N$. Für $h(x) \in \mathrm{Ker}(g) \cap N$ gilt $x = f(x) = g(h(x)) = 0$ und $h(x) = 0$. Also ist $M = \mathrm{Ker}(g) \oplus N$.

(3) $\Rightarrow$ (1): Nach Satz II.9.4 existiert ein freier Modul F und ein Epimorphismus $g\colon F \to P$. Nach Voraussetzung ist $F = \mathrm{Ker}(g) \oplus N$ mit $N \simeq F/\mathrm{Ker}(g) \simeq g(F) = P$. $\square$

Beispiel II.12.14.

(i) Jeder freie A-Modul ist projektiv. Ist umgekehrt jeder projektive Modul frei, so ist der reguläre Modul unzerlegbar und A ist lokal nach Satz II.12.11. Kaplansky hat bewiesen, dass in einer lokalen Algebra jeder projektive Modul frei ist (für endlich-dimensionale Moduln folgt dies aus Krull-Schmidt). Quillen hat bewiesen, dass jeder endlich erzeugte projektive Modul über $K[X_1, \ldots, X_n]$ (für einen Körper K) frei ist.

(ii) Sind P und Q projektiv, so auch $P \times Q$, denn ist P (bzw. Q) ein direkter Summand des freien Moduls F_P (bzw. F_Q), so ist $P \times Q$ ein direkter Summand des freien Moduls $F_P \times F_Q$. Allgemeiner ist das Koprodukt von projektiven Moduln projektiv.

(iii) Ist A halbeinfach, so ist jeder einfache Modul projektiv. Nach Lemma II.8.13 und (ii) sind sogar alle A-Moduln projektiv.

(iv) Jeder direkte Summand eines projektiven Moduls ist projektiv. Eine besondere Rolle spielen daher die projektiven, unzerlegbaren (kurz *projektiv-unzerlegbaren*) Moduln.

Lemma II.12.15 (Schanuel)**.** *Seien P_1 und P_2 projektive A-Moduln. Sei $U_i \leq P_i$ mit $P_1/U_1 \simeq P_2/U_2$. Dann gilt $U_1 \times P_2 \simeq U_2 \times P_1$.*

Beweis. Sei $\varphi\colon P_1/U_1 \to P_2/U_2$ ein Isomorphismus.

$$M := \big\{(x, y) \in P_1 \times P_2 : \varphi(x + U_1) = y + U_2\big\} \leq P_1 \times P_2.$$

Die Projektionen $\pi_i\colon M \to P_i$ sind offenbar surjektiv. Da P_i projektiv ist, folgt $M = \mathrm{Ker}(\pi_1) \oplus N_1 = \mathrm{Ker}(\pi_2) \oplus N_2$ mit $N_i \simeq M/\mathrm{Ker}(\pi_i) \simeq P_i$, $\mathrm{Ker}(\pi_1) = \{0\} \times U_2 \simeq U_2$ und $\mathrm{Ker}(\pi_2) = U_1 \times \{0\} \simeq U_1$. $\square$

Satz II.12.16. *Für jede Algebra A gilt:*

(i) Die projektiv-unzerlegbaren Moduln P sind die unzerlegbaren Summanden des regulären A-Moduln. Insbesondere wird P von einem Element erzeugt.

(ii) Die Abbildung $P \mapsto P/\mathrm{J}(P)$ induziert eine Bijektion zwischen der Menge der Isomorphieklassen projektiv-unzerlegbarer A-Moduln und der Menge der Isomorphieklassen einfacher A-Moduln.

Beweis.

(ii) Wir beweisen die Aussage zunächst nur für endlich erzeugte projektiv-unzerlegbare Moduln P. Sei $\overline{P} := P/\mathrm{J}(P)$. Für $f \in \mathrm{End}_A(P)$ gilt

$$f(\mathrm{J}(P)) \overset{II.8.13}{=} f(\mathrm{J}(R)P) = \mathrm{J}(R)f(P) \subseteq \mathrm{J}(R)P \subseteq \mathrm{J}(P).$$

Man erhält eine wohldefinierte Abbildung $\overline{f} \in \mathrm{End}_A(\overline{P})$ mit $\overline{f}(x + \mathrm{J}(P)) := f(x) + \mathrm{J}(P)$ für $x \in P$.

Sei umgekehrt $\varphi \in \mathrm{End}_A(\overline{P})$ gegeben. Dann ist $f\colon P \to \overline{P}$, $x \mapsto \varphi(x + \mathrm{J}(P))$ ein Homomorphismus und $g\colon P \to \overline{P}$, $x \mapsto x + \mathrm{J}(P)$ ein Epimorphismus von A-Moduln. Nach Satz II.12.13 existiert $h \in \mathrm{End}_A(P)$ mit $g \circ h = f$. Dies zeigt $\overline{h} = \varphi$. Also ist $\mathrm{End}_A(P) \to \mathrm{End}_A(\overline{P})$, $f \mapsto \overline{f}$ ein Epimorphismus von Algebren. Nach Bemerkung II.12.12 ist $\mathrm{End}_A(P)$ lokal. Ist f invertierbar

(bzw. nilpotent), so auch $\overline{f}$. Satz II.12.11 zeigt, dass $\mathrm{End}_A(\overline{P})$ lokal ist, d. h. $\overline{P}$ ist unzerlegbar. Andererseits ist $\overline{P}$ halbeinfach nach Beispiel II.8.9. Insgesamt ist $\overline{P}$ einfach.

Sind P und Q isomorphe projektiv-unzerlegbare Moduln, so ist sicher $\overline{P} \simeq \overline{Q}$. Sei umgekehrt $\varphi\colon \overline{P} \to \overline{Q}$ ein Isomorphismus. Für den Homomorphismus $f\colon P \to \overline{Q}$, $x \mapsto \varphi(x + \mathrm{J}(P))$ existiert nach Satz II.12.13 ein Homomorphismus $h\colon P \to Q$ mit

$$h(x) + \mathrm{J}(Q) = f(x) = \varphi(x + \mathrm{J}(P))$$

für alle $x \in P$. Dies zeigt $h(P) + \mathrm{J}(Q) = Q$. Aus Nakayamas Lemma folgt $h(P) = Q$. Nach Satz II.12.13 existiert $N \leq P$ mit $P = \mathrm{Ker}(h) \oplus N$. Da P unzerlegbar ist, muss $\mathrm{Ker}(h) = 0$ gelten. Also ist $h\colon P \to Q$ ein Isomorphismus.

Sei schließlich S ein beliebiger einfacher A-Modul und $s \in S \setminus \{0\}$. Sei $A = P_1 \oplus \ldots \oplus P_k$ eine Zerlegung in projektiv-unzerlegbare Moduln. Wie üblich existiert ein Epimorphismus $f\colon A \to S$. Sei $f(P_i) \neq 0$. Da S einfach ist, gilt $P_i/\mathrm{Ker}(f) \simeq f(P_i) = S$. Insbesondere ist $\mathrm{Ker}(f)$ ein maximaler Untermodul von P_i und $\mathrm{J}(P_i) \leq \mathrm{Ker}(P_i)$. Nach dem ersten Teil des Beweises ist $P_i/\mathrm{J}(P_i)$ einfach und es folgt $\mathrm{J}(P_i) = \mathrm{Ker}(f)$. Insgesamt ist $S \simeq P_i/\mathrm{J}(P_i)$.

(i) Sei P ein projektiv-unzerlegbarer A-Modul (nicht unbedingt endlich-erzeugt). Da $\mathrm{J}(A)$ nilpotent ist, gilt $\mathrm{J}(A)P < P$ und $P/\mathrm{J}(A)P$ ist halbeinfach. Also existiert ein maximaler Untermodul $M < P$. Nach dem ersten Teil des Beweises existiert ein unzerlegbarer Summand Q von A und ein Isomorphismus $\varphi\colon Q/\mathrm{J}(Q) \simeq P/M$. Aus der Projektivität von P erhält einen Homomorphismus $f\colon P \to Q$ mit $\varphi(f(x) + \mathrm{J}(Q)) = x + M$ für $x \in P$. Nach Nakayama ist f surjektiv. Die Projektivität von Q hingegen zeigt $P = \mathrm{Ker}(f) \oplus N$. Da P unzerlegbar ist, muss $\mathrm{Ker}(f) = 0$ und $P \simeq Q$ gelten. Damit ist der Beweis von (ii) abgeschlossen. Da $Q/\mathrm{J}(Q)$ einfach ist, existiert ein $x \in Q$ mit $Rx + \mathrm{J}(Q) = Q$. Nach Nakayama gilt bereits $Q = Rx$. □

Satz II.12.17. *Sei K algebraisch abgeschlossen und P ein projektiv-unzerlegbarer A-Modul. Dann ist $\dim_K(P/\mathrm{J}(P))$ die Vielfachheit von P in der Krull-Schmidt-Zerlegung des regulären A-Moduls.*

Beweis. Sei $A = P_1 \oplus \ldots \oplus P_n$ eine Zerlegung in projektiv-unzerlegbare A-Moduln. Nach Satz II.12.16 ist $\overline{P_i} := P_i/\mathrm{J}(P_i)$ ein einfacher A-Modul und ein einfacher $A/\mathrm{J}(A)$-Modul (Bemerkung II.8.12). Andererseits ist $A/\mathrm{J}(A) \simeq \overline{P_1} \oplus \ldots \oplus \overline{P_n}$ halbeinfach. Da K algebraisch abgeschlossen ist, gilt $\mathrm{End}_A(\overline{P_i}) \cong K$. Nach Bemerkung II.12.3 ist $\dim_K \overline{P_i}$ die Vielfachheit von $\overline{P_i}$ als Kompositionsfaktor von $A/\mathrm{J}(A)$. Satz II.12.16 liefert

$$\dim \overline{P} = \big|\{1 \leq i \leq n : \overline{P_i} \simeq \overline{P}\}\big| = \big|\{1 \leq i \leq n : P_i \simeq P\}\big|. \qquad \square$$

Lemma II.12.18. *Sei P ein projektiv-unzerlegbarer A-Modul, $E := \mathrm{End}_A(P)^o$ und $S := P/\mathrm{J}(P)$. Für einen beliebigen A-Modul M gilt:*

(i) $E/\mathrm{J}(E) \cong \mathrm{End}_A(S)^o =: D$.

(ii) Durch $f \cdot \varphi := \varphi \circ f$ für $f \in E$ und $\varphi \in \mathrm{Hom}_A(P, M)$ wird $\mathrm{Hom}_A(P, M)$ zu einem E-Modul.

(iii) Die Vielfachheit von S als Kompositionsfaktor von M ist $\dim_K \mathrm{Hom}_A(P, M)/\dim_K D$.

Beweis.

(i) Da P unzerlegbar ist, ist E lokal. Da $\mathrm{J}(P)$ der einzige maximale Untermodul von P ist, gilt $f(\mathrm{J}(P)) \subseteq \mathrm{J}(P)$ für alle $f \in E$. Insbesondere ist $\overline{f} \in D$ mit $\overline{f}(x + \mathrm{J}(E)) = f(x) + \mathrm{J}(P)$ für $x \in P$ wohldefiniert. Da P projektiv ist, existiert umgekehrt für alle $\varphi \in D$ ein $f \in E$ mit

$\overline{f} = \varphi$ (siehe Beweis von Satz II.12.16). Folglich ist $E \to D$, $f \mapsto \overline{f}$ ein Epimorphismus mit Kern $\mathrm{J}(E) = \mathrm{Hom}_A(P, \mathrm{J}(P))$.

(ii) Für $f, g \in E$ gilt $(fg)\varphi = \varphi \circ (g \circ f) = f(g\varphi)$. Die anderen Axiome sind offensichtlich.

(iii) Sei $0 = M_0 < \ldots < M_k = M$ eine Kompositionsreihe von M. Dann ist

$$0 = \mathrm{Hom}_A(P, M_0) \leq \ldots \leq \mathrm{Hom}_A(P, M_k) = \mathrm{Hom}_A(P, M)$$

eine Folge von E-Moduln nach (ii). Für $i \geq 1$ hat der kanonische Homomorphismus $\mathrm{Hom}_A(P, M_i) \to \mathrm{Hom}_A(P, M_i/M_{i-1})$ Kern $\mathrm{Hom}_A(P, M_{i-1})$. Da M_i/M_{i-1} einfach ist, gilt $\mathrm{Hom}_A(P, M_i/M_{i-1}) = 0$ falls $M_i/M_{i-1} \not\simeq S$ nach Satz II.12.16. Ggf. ist $\mathrm{Hom}_A(P, M_i) = \mathrm{Hom}_A(P, M_{i-1})$. Sei nun $M_i/M_{i-1} \simeq S$ und $f, g \in \mathrm{Hom}_A(P, S) \setminus \{0\}$. Da P projektiv ist, existiert $\hat{f} \in E$ mit $\hat{f}(x) + \mathrm{J}(P) = f(x)$ für alle $x \in P$ (vgl. Beweis von Satz II.12.16). Da $\mathrm{J}(P)$ der einzige maximale Untermodul von P ist, gilt $\hat{f}(P) = P$ und $\hat{f} \in E^\times$. Analog existiert $\hat{g} \in E$ mit $\hat{g}(x) + \mathrm{J}(P) = g(x)$. Schließlich gilt

$$\hat{g}\hat{f}^{-1} \cdot f = f \circ \hat{f}^{-1} \circ \hat{g} = g.$$

Dies zeigt, dass $\mathrm{Hom}_A(P, S)$ ein einfacher E-Modul ist. Da E lokal ist, gilt $\mathrm{Hom}_A(P, S) \simeq E/\mathrm{J}(E)$. Aus (i) folgt $\dim_K \mathrm{Hom}_A(P, S) = \dim_K D$. Die Existenz des kanonischen Epimorphismus $P \to S$ liefert $\mathrm{Hom}_A(P, M_i)/\mathrm{Hom}_A(P, M_{i-1}) \simeq \mathrm{Hom}_A(P, S)$. Die Vielfachheit von S als Kompositionsfaktor von M ist daher die Anzahl der einfachen Faktoren von $\mathrm{Hom}_A(P, M_0) \leq \ldots \leq \mathrm{Hom}_A(P, M)$. Da alle anderen Faktoren trivial sind, ergibt sich die Behauptung. □

Definition II.12.19. Seien $P_1, \ldots, P_k$ die projektiv-unzerlegbaren A-Moduln bis auf Isomorphie.

- Man nennt $A^b := \mathrm{End}_A(P_1 \times \ldots \times P_k)^o$ die *Basisalgebra* von A.
- Sei c_{ij} die Vielfachheit von $P_i/\mathrm{J}(P_i)$ als Kompositionsfaktor von P_j. Man nennt $C(A) := (c_{ij})_{i,j} \in \mathbb{N}_0^{k \times k}$ die *Cartan-Matrix* von A.

Satz II.12.20. *Seien $e_1, \ldots, e_k \in A$ paarweise orthogonale primitive Idempotente, sodass $Ae_1, \ldots, Ae_k$ die Isomorphieklassen projektiv-unzerlegbarer A-Moduln repräsentieren.*

(i) Für $e := e_1 + \ldots + e_k$ gilt $A^b \cong eAe$.

(ii) Sei $D_i := \mathrm{End}_A(Ae_i/\mathrm{J}(Ae_i))$ und $C(A) = (c_{ij})$. Dann gilt $c_{ij} \dim_K D_i = \dim_K e_i A e_j$.

Beweis.

(i) Wegen $Ae = Ae_1 \oplus \ldots \oplus Ae_k$ folgt die Behauptung aus Lemma II.7.20.

(ii) Wie in Lemma II.7.20 zeigt man, dass

$$\begin{aligned} \mathrm{Hom}_A(Ae_i, Ae_j) &\to e_i A e_j, \\ \varphi &\mapsto \varphi(e_i) = \varphi(e_i^2) = e_i \varphi(e_i) \end{aligned}$$

ein Vektorraumisomorphismus ist. Daher folgt die Behauptung aus Lemma II.12.18. □

Bemerkung II.12.21.

(i) In der Situation von Satz II.12.20 nennt man $e = e_1 + \ldots + e_k$ ein *Basisidempotent* für A (nicht eindeutig bestimmt).

(ii) Die nächsten Sätze zeigen, dass man viele Fragen über die Modulstruktur von A durch die „kleinere“ Basisalgebra beantworten kann. Es genügt oft nur die Basisalgebren der Blöcke von A heranzuziehen (Satz II.12.29).

(iii) Ist K algebraisch abgeschlossen, so gilt $D_i = K$ und $c_{ij} = \dim_K e_iAe_j$. Aus $A^b = \bigoplus_{i,j=1}^k e_iAe_j$ folgt dann $\dim A^b = \sum_{i,j=1}^k c_{ij}$.

Beispiel II.12.22.

(i) Ist A halbeinfach, so sind die projektiv-unzerlegbaren Moduln $P_1, \ldots, P_k$ genau die einfachen A-Moduln (bis auf Isomorphie) und man erhält $C(A) = 1_k$ und $A^b \cong \mathrm{End}_A(P_1)^o \times \ldots \times \mathrm{End}_A(P_k)^o = D_1 \times \ldots \times D_k$ mit Divisionsalgebren $D_1, \ldots, D_k$ (Lemma II.7.20). Insbesondere gilt $(D^{n\times n})^b \cong D$ für jede Divisionsalgebra D.

(ii) Sei $A/\mathrm{J}(A)$ eine direkte Summe von Divisionsalgebren. Nach Bemerkung II.12.3 tritt dann jeder projektiv-unzerlegbare Modul mit Vielfachheit 1 im regulären A-Modul auf. Dies zeigt

$$A^b = \mathrm{End}_A(P_1 \times \ldots \times P_k)^o \cong \mathrm{End}_A(A)^o \cong A.^1$$

Insbesondere gilt $A \cong A^b$ für alle kommutativen Algebren.

(iii) Sei $A \subseteq K^{n\times n}$ die Algebra der oberen Dreiecksmatrizen. Die strikten oberen Dreiecksmatrizen (d. h. Nullen auf der Hauptdiagonale) bilden offenbar ein nilpotentes Ideal $J \trianglelefteq A$ mit $A/J \cong K^n$. Dies zeigt $J = \mathrm{J}(A)$. Aus (ii) folgt $A \cong A^b$. Für die primitiven Idempotente kann man $e_i := E_{ii} = (\delta_{si}\delta_{ti})_{st} \in A$ wählen. Dann gilt $e_iAe_j = Ke_i$ falls $i \leq j$ und $e_iAe_j = 0$ sonst. Dies zeigt

$$C(A) = \begin{pmatrix} 1 & \cdots & 1 \\ & \ddots & \vdots \\ 0 & & 1 \end{pmatrix}.$$

Lemma II.12.23. *Für jedes Idempotent e einer Algebra A gilt* $\mathrm{J}(eAe) = e\mathrm{J}(A)e$.

Beweis. Da $\mathrm{J}(A)$ nilpotent ist, ist $e\mathrm{J}(A)e \subseteq \mathrm{J}(A)$ ein nilpotentes Ideal von eAe. Nach Lemma II.8.15 folgt $e\mathrm{J}(A)e \subseteq \mathrm{J}(eAe) =: J$. Umgekehrt ist auch J nilpotent, sagen wir $J^n = 0$. Dann gilt $AJA \trianglelefteq A$ mit

$$(AJA)^{n+1} = A(JeAe)^nJA = AJ^{n+1}A = 0.$$

Dies zeigt $AJA \subseteq \mathrm{J}(A)$ und $J \subseteq eAeJeAe \subseteq e\mathrm{J}(A)e$. □

Satz II.12.24. *Für jede Algebra A gilt $C(A) = C(A^b)$ bei geeigneter Anordnung. Insbesondere haben A und A^b gleich viele einfache Moduln bis auf Isomorphie. Ist K algebraisch abgeschlossen, so hat jeder einfache A^b-Modul Dimension* 1.

Beweis. Mit den Bezeichnungen aus Satz II.12.20 gilt

$$A^b = eAe = eAe_1 \oplus \ldots \oplus eAe_k = A^be_1 \oplus \ldots \oplus A^be_k$$

mit $E_i := \mathrm{End}_{A^b}(A^be_i)^o \cong e_iA^be_i = e_iAe_i \cong \mathrm{End}_A(Ae_i)^o$. Nach Bemerkung II.12.3 und Lemma II.12.18 ist $\overline{A} := A/\mathrm{J}(A) \cong D_1^{n_1\times n_1} \times \ldots \times D_k^{n_k\times n_k}$ mit Divisionsalgebren $D_i \cong E_i/\mathrm{J}(E_i)$. O. B. d. A. sei $\overline{e_i} := e_i + \mathrm{J}(A) = (0, \ldots, E_{11}, \ldots, 0)$, wobei $E_{11} = (\delta_{i1}\delta_{j1})_{ij} \in D^{n_i\times n_i}$. Nach Lemma II.12.23 gilt

$$A^b/\mathrm{J}(A^b) = eAe/e\mathrm{J}(A)e = \bar{e}\overline{A}\bar{e} \cong D_1 \times \ldots \times D_k.$$

[1] In der englischsprachigen Literatur nennt man solche Algebren *basic*.

Daher sind $A^b e_1, \ldots, A^b e_k$ genau die projektiv-unzerlegbaren A^b-Moduln bis auf Isomorphie. Aus Lemma II.12.18 folgt

$$C(A) = \Big(\frac{\dim_K \operatorname{Hom}_A(Ae_i, Ae_j)}{\dim_K D_i}\Big)_{ij} = \Big(\frac{\dim_K e_i A e_j}{\dim_K D_i}\Big)_{ij} = \Big(\frac{\dim_K e_i A^b e_j}{\dim_K D_i}\Big)_{ij} = C(A^b).$$

Ist K algebraisch abgeschlossen, so gilt $D_1 = \ldots = D_k = K$ und die letzte Behauptung folgt aus Bemerkung II.12.3. □

Satz II.12.25. *Für jede Algebra A existiert ein $n \in \mathbb{N}$ mit $A \cong e(A^b)^{n\times n}e$, wobei e ein Idempotent von $(A^b)^{n\times n}$ ist.*

Beweis. Seien wie bisher $P_1, \ldots, P_k$ die projektiv-unzerlegbaren A-Moduln bis auf Isomorphie. Sei $P := P_1 \times \ldots \times P_k$. Sei n die maximale Vielfachheit eines P_i im regulären A-Modul. Dann ist A ein direkter Summand von P^n, etwa $P^n = A \oplus Q$. Sei $\varphi \in \operatorname{End}_A(P^n)$ die Projektion auf A. Dann ist $\varphi\operatorname{End}_A(P^n)\varphi \to \operatorname{End}_A(A)$, $\varphi f \varphi \mapsto \varphi f \varphi_A$ ein Isomorphismus von Algebren. Unter dem bekannten Isomorphismus

$$\operatorname{End}_A(P^n)^o \cong (\operatorname{End}_A(P)^{n\times n})^o \cong (\operatorname{End}_A(P)^o)^{n\times n} = (A^b)^{n\times n}$$

(vgl. Beweis von Artin-Wedderburn und Lemma II.7.20) wird φ auf ein Idempotent $e \in (A^b)^{n\times n}$ abgebildet. Es gilt nun $A \cong \operatorname{End}_A(A)^o \cong e(A^b)^{n\times n}e$. □

Lemma II.12.26. *Für Algebren A, B und $n, m \in \mathbb{N}$ gilt*

$$\boxed{(A \times B)^{n\times n} \cong A^{n\times n} \times B^{n\times n}} \qquad \boxed{(A^{n\times n})^{m\times m} \cong A^{nm\times nm}.}$$

Beweis. Offenbar ist die Abbildung

$$\begin{aligned}(A \times B)^{n\times n} &\to A^{n\times n} \times B^{n\times n},\\ (a_{ij}, b_{ij})_{ij} &\mapsto \big((a_{ij})_{ij}, (b_{ij})_{ij}\big)\end{aligned}$$

ein Isomorphismus. Den zweiten Isomorphismus erhält man, indem Matrizen in $A^{nm\times nm}$ in $n\times n$-Blöcke aufteilt (es besteht also nur ein formaler Unterschied zwischen den Algebren). □

Satz II.12.27. *Für jede Algebra A mit Basisidempotent e gilt $\mathrm{Z}(A^b) \cong \mathrm{Z}(eAe) = e\mathrm{Z}(A)e \cong \mathrm{Z}(A)$.*

Beweis. Offenbar ist

$$\Gamma\colon \mathrm{Z}(A) \to \mathrm{Z}(eAe) \cong \mathrm{Z}(A^b), \qquad z \mapsto ez = eze$$

ein Ringhomomorphismus. Sei $e = e_1 + \ldots + e_k$ mit primitiven Idempotenten $e_1, \ldots, e_k$. Wir können $1 = e + (1 - e)$ zu einer Zerlegung $1 = e_1 + \ldots + e_n$ in primitive Idempotente verfeinern. Sei $z \in \mathrm{Z}(A)$ mit $ez = 0$. Für jedes $i \le n$ existiert ein $j \le k$ mit $Ae_j \simeq Ae_i$. Nach Satz II.8.22 existiert ein $x \in A^\times$ mit $xe_jx^{-1} = e_i$. Es folgt

$$e_i z = xe_jx^{-1}z = xe_jzx^{-1} = xe_jezx^{-1} = 0.$$

Insgesamt ist $z = (e_1 + \ldots + e_n)z = 0$. Daher ist Γ injektiv und $\dim \mathrm{Z}(A) \le \dim \mathrm{Z}(A^b)$.

Sei nun $A \cong f(A^b)^{m\times m}f$ für ein Idempotent $f \in (A^b)^{m\times m} =: \hat{A}$ wie in Satz II.12.25. Wir zerlegen $f = f_1 + \ldots + f_l$ in paarweise orthogonale primitive Idempotente. Sei $A^b/\mathrm{J}(A^b) \cong D_1 \times \ldots \times D_k$. Nach Lemma II.12.5 und Lemma II.12.26 gilt

$$\hat{A}/\mathrm{J}(\hat{A}) = \hat{A}/\mathrm{J}(A^b)^{m\times m} \cong (A^b/\mathrm{J}(A^b))^{m\times m} \cong D_1^{m\times m} \times \ldots \times D_k^{m\times m}.$$

Insbesondere hat $\hat{A}$ genauso viele einfache Moduln wir A. Folglich ist jeder projektiv-unzerlegbare $\hat{A}$-Modul zu einem $\hat{A}f_i$ isomorph sein (anderenfalls hätte $A \cong f\hat{A}f$ weniger einfache Moduln, vgl. Beweis von Satz II.12.24). Wir können nun das Argument aus den ersten Teil des Beweises auf $\hat{A}$ anwenden und erhalten $\dim \mathrm{Z}(A^b) \overset{II.12.5}{=} \dim \mathrm{Z}(\hat{A}) \leq \dim \mathrm{Z}(A)$. Also ist Γ ein Isomorphismus. □

Bemerkung II.12.28.

(i) Für ein beliebiges Idempotent $e \in A$ gilt nicht unbedingt $\mathrm{Z}(eAe) = e\mathrm{Z}(A)e$ (Aufgabe II.61).

(ii) Im Folgenden bezeichnen wir eine $n \times n$-Matrix $M = (m_{ij})$ als *unzerlegbar*, falls keine nichtleere Teilmenge $I \subsetneq \{1, \ldots, n\}$ mit $a_{ij} = 0 = a_{ji}$ für alle $i \in I$ und $j \notin I$ existiert.

Satz II.12.29. *Sei $A = B_1 \oplus \ldots \oplus B_s$ die Peirce-Zerlegung der Algebra A. Dann gilt*

$$C(A) = \begin{pmatrix} C(B_1) & & 0 \\ & \ddots & \\ 0 & & C(B_s) \end{pmatrix}$$

bei geeigneter Anordnung. Außerdem sind die Matrizen $C(B_i)$ unzerlegbar.

Beweis. Sei $1 = z_1 + \ldots + z_s$ die Zerlegung in zentral primitive Idempotente mit $B_i = Az_i$. Wir zerlegen $z_i = e_{i1} + \ldots + e_{ik_i}$ in paarweise orthogonale primitive Idempotente. Dann gilt

$$\mathrm{Hom}_{B_i}(B_i e_{ij}, B_i e_{ik}) \simeq_K e_{ij} B_i e_{ik} = e_{ij} A e_{ik} \simeq_K \mathrm{Hom}_A(Ae_{ij}, Ae_{ik})$$

und $\mathrm{End}_{B_i}(B_i e_{ij})^o \cong \mathrm{End}_A(Ae_{ij})$. Nach Lemma II.12.18 stimmen die Einträge von $C(B_i)$ mit den entsprechenden Einträgen aus $C(A)$ überein. Sei nun $i \neq j$. Dann gilt

$$e_{is} A e_{jt} = z_i e_{is} A e_{jt} z_j = e_{is} A e_{jt} z_i z_j = 0.$$

Die Blockdiagonalgestalt von $C(A)$ folgt aus Satz II.12.20.

Nehmen wir nun an $C(B_i)$ sei zerlegbar. O. B. d. A. sei $i = 1$ und $\varnothing \neq I \subsetneq \{1, \ldots, k_1\}$ mit $e_{1i} A e_{1j} = 0 = e_{1j} A e_{1i}$ für alle $i \in I$ und $j \notin I$. Sei $e := \sum_{i \in I} e_{1i}$ und $a \in A$. Dann gilt

$$ea = ez_1 a \sum_{i=1}^{s} z_i = eaz_1 = \sum_{i \in I} e_{1i} a \sum_{j=1}^{k} e_{1j} = eae = \ldots = ae$$

und $a \in \mathrm{Z}(A)$. Die Zerlegung $z_1 = e + (z_1 - e)$ widerspricht der Primitivität von z_1 in $\mathrm{Z}(A)$. Also ist $C(B_i)$ unzerlegbar. □

Bemerkung II.12.30. Die nicht-negativen, unzerlegbaren Cartan-Matrizen $C = C(B_i)$ in Satz II.12.29 erfüllen die Voraussetzungen des Satz von Perron-Frobenius: Der *Spektralradius*

$$\rho(C) := \max\{|\lambda| : \lambda \in \mathbb{C} \text{ Eigenwert von } C\}$$

ist ein Eigenwert mit algebraischer Vielfachheit 1 und der entsprechende Eigenraum wird von einem Vektor mit positiven Einträgen aufgespannt. Dieser Satz hat für Algebren jedoch noch keine Anwendung erfahren.

Folgerung II.12.31. *Zwei einfache A-Moduln S, T gehören genau dann zum gleichen Block, wenn projektiv-unzerlegbare A-Moduln $P_1, \ldots, P_k$ mit folgenden Eigenschaften existieren:*

(i) $S \simeq P_1/\mathrm{J}(P_1)$ *und* $T \simeq P_k/\mathrm{J}(P_k)$.

(ii) Für $i = 1, \ldots, k-1$ *haben* P_i *und* P_{i+1} *einen gemeinsamen Kompositionsfaktor.*

Beweis. Nehmen wir an $P_1, \ldots, P_k$ existieren und S gehört zum Block B. Wegen $S \simeq P_1/\mathrm{J}(P_1)$ gehört auch P_1 zu B. Induktiv sei bereits gezeigt, dass P_i zu B gehört. Sei S_i ein gemeinsamer Kompositionsfaktor von P_i und P_{i+1}. Dann ist der Eintrag in $C(A)$ bzgl. S_i und P_i ungleich 0. Aus Satz II.12.29 folgt, dass S_i zu B gehört. Aus dem gleichen Grund gehört auch P_{i+1} zu B. Auf diese Weise folgt schließlich, dass T zu B gehört.

Nehmen wir umgekehrt an, dass S und T zu B gehören. Seien $P_1, \ldots, P_n$ die projektiv-unzerlegbaren B-Moduln mit $S \simeq P_1/\mathrm{J}(P_1)$ und $T \simeq P_n/\mathrm{J}(P_n)$. Sei Γ der Graph mit Ecken $P_1, \ldots, P_n$, sodass P_i und P_j genau dann mit einer Kante verbunden sind, falls sie einen gemeinsamen Kompositionsfaktor haben. Sei $\{P_i : i \in I\}$ die Zusammenhangskomponente von P_1. Für $C(B) = (c_{ij})$ gilt nun $c_{ij} = 0 = c_{ji}$ für alle $i \in I$ und $j \notin I$. Aus Satz II.12.29 folgt $I = \{1, \ldots, n\}$. Insbesondere sind P_1 und P_n verbunden. □

Definition II.12.32. Für eine endliche Gruppe G sei KG die Menge aller Abbildungen $G \to K$. Durch

$$\begin{aligned}(\alpha + \beta)(g) &:= \alpha(g) + \beta(g) \qquad (\alpha, \beta \in KG,\ g \in G),\\ (\alpha\beta)(g) &:= \sum_{h \in G} \alpha(h)\beta(h^{-1}g) \qquad (\textit{Faltung}),\\ (\lambda\alpha)(g) &:= \lambda\alpha(g) \qquad (\lambda \in K)\end{aligned}$$

wird KG zu einer K-Algebra. Die Assoziativität der Multiplikation folgt aus

$$\begin{aligned}((\alpha\beta)\gamma)(g) &= \sum_{h \in G} (\alpha\beta)(h)\gamma(h^{-1}g) = \sum_{h \in G} \sum_{k \in G} \alpha(k)\beta(k^{-1}h)\gamma(h^{-1}g)\\ &= \sum_{\substack{x,y,z \in G\\ xyz = g}} \alpha(x)\beta(y)\gamma(z) = \ldots = (\alpha(\beta\gamma))(g)\end{aligned}$$

für $\alpha, \beta, \gamma \in KG$ und $g \in G$ (die anderen Axiome sind leicht). Man nennt KG die *Gruppenalgebra* von G über K. Seine Elemente schreibt man meist als formale Linearkombinationen $\alpha = \sum_{g \in G} \alpha_g g$, wobei $\alpha_g = \alpha(g) \in K$. Die Multiplikation funktioniert dann wie bei Polynomen (vgl. Aufgabe II.63):

$$\sum_{g \in G} \alpha_g g \cdot \sum_{g \in G} \beta_g g = \sum_{g,h \in G} \alpha_g \beta_h gh = \sum_{g \in G} \Big(\sum_{h \in G} \alpha_h \beta_{h^{-1}g} \Big) g.$$

Bemerkung II.12.33. Indem wir $g \in G$ mit $1_K g$ identifizieren, können wir G als Teilmenge von KG auffassen. Dann ist 1_G das Einselement von KG und G ist eine K-Basis von KG. Insbesondere ist $\dim_K KG = |G|$. Außerdem ist KG genau dann kommutativ, wenn G abelsch ist.

Beispiel II.12.34. Für $x := (1,2) + (1,3) \in \mathbb{F}_2 S_3$ gilt

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

Lemma II.12.35. *Die Abbildung*

$$\begin{aligned}\nu\colon KG &\to K,\\ \sum_{g\in G}\alpha_g g &\mapsto \sum_{g\in G}\alpha_g\end{aligned}$$

ist ein Epimorphismus von K-Algebren mit

$$I(KG) := \operatorname{Ker}(\nu) = \sum_{g\in G\setminus\{1\}} K(g-1).$$

Beweis. Sicher ist $\nu(1)=1$ und $\nu(\alpha+\beta)=\nu(\alpha)+\nu(\beta)$ für $\alpha,\beta\in KG$. Außerdem ist

$$\nu(\alpha\beta) = \sum_{g\in G}\sum_{h\in G}\alpha_h\beta_{h^{-1}g} = \sum_{g,h\in G}\alpha_g\beta_h = \sum_{g\in G}\alpha_g\cdot\sum_{h\in G}\beta_h = \nu(\alpha)\nu(\beta).$$

Schließlich ist auch $\nu(\lambda\alpha)=\lambda\nu(\alpha)$ für $\lambda\in K$. Also ist ν ein Epimorphismus von Algebren.

Nach dem Homomorphiesatz (für Vektorräume) ist $\dim_K I(KG) = \dim_K KG - \dim_K K = |G|-1$. Offenbar liegen die Elemente $g-1$ für $g\in G\setminus\{1\}$ in $I(KG)$. Da G eine K-Basis von KG ist, sind die Elemente $g-1$ linear unabhängig. Sie bilden also eine Basis von $I(KG)$. □

Definition II.12.36. Man nennt $\nu\colon KG\to K$ die *Augmentationsabbildung* und $I(KG)$ das *Augmentationsideal* von KG. Außerdem nennt man $KG/I(KG)\simeq K$ den *trivialen* KG-Modul.

Bemerkung II.12.37.

(i) Achtung: Für beliebige Ringe hatten wir den Modul 0 trivial genannt.

(ii) Die Existenz des trivialen Moduls unterscheidet Gruppenalgebren von beliebigen Algebren. So kann $K^{2\times 2}$ beispielsweise keine Gruppenalgebra sein. Außerdem ist eine Gruppenalgebra KG genau dann lokal, wenn K bis auf Isomorphie der einzige einfache A-Modul ist. Ggf. ist $\mathrm{J}(KG)=I(KG)$.

(iii) Der triviale Modul findet sich auch als Untermodul von KG wieder: $K\sum_{g\in G} g$.

(iv) Nach Satz II.8.25 lässt sich der triviale Modul genau einem Block B_0 von KG zuordnen. Man nennt B_0 den *Hauptblock* von KG. Für einen beliebigen Block B von KG gilt

$$B = B_0 \iff BK\neq 0 \iff B1\neq 0 \iff \nu(B)\neq 0 \iff \nu(B)=K.$$

Satz II.12.38 (Maschke)**.** *Genau dann ist KG halbeinfach, wenn* $\operatorname{char} K$ *kein Teiler von $|G|$ ist. Insbesondere ist KG halbeinfach, falls* $\operatorname{char} K = 0$.

Beweis.

⇒: Sei KG halbeinfach, d. h. der reguläre KG-Modul ist halbeinfach. Insbesondere besitzt $I := I(KG)$ ein Komplement J. Hierbei ist J ein Linksideal von KG mit $KG = I\oplus J$. Nach Lemma II.12.35 ist J eindimensional, sagen wir $J=K\alpha$ mit $\alpha=\sum_{g\in G}\alpha_g g\in KG$. Für jedes $h\in G$ ist

$$(h-1)\alpha \in I\alpha\cap(h-1)J\subseteq I\cap J = 0,$$

d. h. $\sum_{g\in G}\alpha_g hg = h\alpha = \alpha = \sum_{g\in G}\alpha_g g$. Es folgt $\alpha_g=\alpha_{hg}$ für alle $h\in H$. Dies zeigt $\alpha_g=\alpha_1$ für alle $g\in G$. Insbesondere ist $|G|\alpha_1=\nu(\alpha)\neq 0$ und $\operatorname{char} K\nmid |G|$.

$\Leftarrow$: Sei nun $\operatorname{char} K \nmid |G|$ und M ein Linksideal von KG. Nach Folgerung II.2.3 existiert ein K-Unterraum $M' \subseteq KG$ mit $KG = M \oplus M'$ (allerdings ist M' nicht unbedingt ein Linksideal). Sei $\pi\colon KG \to M$ die Projektion und

$$\begin{aligned} f\colon KG &\to M, \\ \alpha &\mapsto \frac{1}{|G|} \sum_{g \in G} g\pi(g^{-1}\alpha) \end{aligned}$$

(wegen $|G| \neq 0$ in K ist dies wohldefiniert). Sicher ist f K-linear. Für $h \in G$ ist zusätzlich

$$f(h\alpha) = \frac{1}{|G|} \sum_{g \in G} g\pi(g^{-1}h\alpha) = \frac{1}{|G|} \sum_{g \in G} hh^{-1}g\pi(g^{-1}h\alpha) = h\frac{1}{|G|} \sum_{x \in G} x\pi(x^{-1}\alpha) = hf(\alpha),$$

d. h. f ist KG-linear. Insbesondere ist $N := \operatorname{Ker}(f)$ ein Linksideal von KG. Für $m \in M$ ist

$$f(m) = \frac{1}{|G|} \sum_{g \in G} g\pi(\underbrace{g^{-1}m}_{\in M}) = \frac{1}{|G|} \sum_{g \in G} gg^{-1}m = m.$$

Dies zeigt $f(KG) = M$ und der Homomorphiesatz liefert $\dim_K M + \dim_K N = \dim_K KG$. Für $m \in M \cap N$ ist außerdem $m = f(m) = 0$. Also ist $KG = M \oplus N$ und KG ist halbeinfach. $\square$

Bemerkung II.12.39. Sei G eine endliche Gruppe und K algebraisch abgeschlossen mit $\operatorname{char} K \nmid |G|$. Nach Maschke ist KG halbeinfach. Aus Bemerkung II.12.3 und Lemma II.12.6 folgt

$$\boxed{KG \cong K^{d_1 \times d_1} \times \ldots \times K^{d_k \times d_k},}$$

wobei $d_1, \ldots, d_k$ die Dimensionen der einfachen KG-Moduln sind. Insbesondere ist

$$|G| = \dim_K KG = d_1^2 + \ldots + d_k^2.$$

Beispiel II.12.40. Nach dem Fundamentalsatz der Algebra ist $K = \mathbb{C}$ algebraisch abgeschlossen.

(i) Ist G abelsch, so ist $\mathbb{C}G$ kommutativ und es gilt $d_1 = \ldots = d_k = 1$ in Bemerkung II.12.39. Dies zeigt $\mathbb{C}G \cong \mathbb{C}^{|G|}$.

(ii) Bekanntlich ist $G = S_3$ nichtabelsch. Daher ist $d_i > 1$ für mindestens ein i (anderenfalls wäre $\mathbb{C}G$ kommutativ). Wegen $6 = |G| = d_1^2 + \ldots + d_k^2$ folgt $k = 3$ und

$$\mathbb{C}S_3 \cong \mathbb{C}^{2\times 2} \times \mathbb{C}^2.$$

Definition II.12.41. Für eine Konjugationsklasse C von G sei $C^+ := \sum_{g \in C} g \in KG$ die *Klassensumme* von C.

Satz II.12.42. *Die Klassensummen bilden eine K-Basis vom Zentrum $\mathrm{Z}(KG)$. Insbesondere ist*

$$\dim_K \mathrm{Z}(KG) = k(G)$$

die Klassenzahl von G.

Beweis. Sei C eine Konjugationsklasse von G. Für $g \in G$ gilt

$$gC^+ = \sum_{c \in C} gc = \sum_{c \in C} gcg^{-1}g = \sum_{d \in C} dg = C^+ g.$$

Dies zeigt $C^+ \in \mathrm{Z}(KG)$.

Sei umgekehrt $\alpha = \sum_{g \in G} \alpha_g g \in \mathrm{Z}(KG)$. Für $h \in G$ gilt dann

$$\alpha = h\alpha h^{-1} = \sum_{g \in G} \alpha_g hgh^{-1}$$

und $\alpha_g = \alpha_{hgh^{-1}}$. Daher ist α konstant auf den Konjugationsklassen von G. Folglich ist α eine K-Linearkombination der Klassensummen. Da verschiedene Konjugationsklassen disjunkt sind, sind die Klassensummen linear unabhängig. □

Bemerkung II.12.43. Über $\mathbb{C}$ gilt

$$\mathrm{Z}(\mathbb{C}G) \cong \mathrm{Z}(\mathbb{C}^{d_1 \times d_1} \times \ldots \times \mathbb{C}^{d_k \times d_k}) = \mathrm{Z}(\mathbb{C}^{d_1 \times d_1}) \times \ldots \times \mathrm{Z}(\mathbb{C}^{d_k \times d_k}) \overset{II.12.5}{=} \mathbb{C}1_{d_1} \times \ldots \times \mathbb{C}1_{d_k} \cong \mathbb{C}^k.$$

Daher ist $k = \dim \mathrm{Z}(\mathbb{C}G) = k(G)$ auch die Anzahl der einfachen $\mathbb{C}G$-Moduln bis auf Isomorphie. Somit ist $(\mathbb{C}G)^b \cong \mathbb{C}^{k(G)}$ die Basisalgebra von $\mathbb{C}G$.

Beispiel II.12.44. Wir bestimmen die Konjugationsklassen von $G = A_4$. Sicher ist $\langle (1,2,3) \rangle \in \mathrm{Syl}_3(G)$. Nach Sylow ist jedes Element $g \in G$ der Ordnung 3 zu $(1,2,3)$ oder zu $(1,2,3)^2 = (1,3,2)$ konjugiert. Diese beiden 3-Zyklen sind andererseits nicht konjugiert, denn sonst wären auch die entsprechenden Nebenklassen in der abelschen Gruppe $G/V_4 \cong C_3$ konjugiert (Aufgabe I.16). Daher repräsentieren $(1,2,3)$ und $(1,3,2)$ alle Konjugationsklassen von Elementen der Ordnung 3 in G. Die Elemente der Ordnung 2 in G liegen alle in V_4 und werden durch Konjugation mit $(1,2,3)$ aufeinander abgebildet. Daher ist $V_4 \setminus \{1\}$ eine weitere Konjugationsklasse. Bekanntlich besitzt G keine Elemente der Ordnung 6 oder 12. Zusammen mit $\{1\}$ haben wir daher alle Konjugationsklassen gefunden. Also ist $k(G) = 4$ und $12 = |G| = d_1^2 + \ldots + d_4^2$ für $d_1, \ldots, d_4 \in \mathbb{N}$. Eine einfache Fallunterscheidung liefert $d_1 = 3$ und $d_2 = d_3 = d_4 = 1$. Man erhält

$$\mathbb{C}A_4 \cong \mathbb{C}^{3 \times 3} \times \mathbb{C}^3.$$

13 Darstellungen und Charaktere

Bemerkung II.13.1. In diesem Kapitel betrachten wir der Einfachheit halber nur endliche Gruppen G und deren Gruppenalgebren über Körpern der Charakteristik 0. Wir werden sehen, dass man sämtliche Informationen über die Moduln von $\mathbb{C}G$ aus einer komplexen Matrix vom Format $k(G) \times k(G)$ ablesen kann. Damit lassen sich tiefliegende Sätze über endliche Gruppen beweisen.

Definition II.13.2. Eine *Darstellung* vom *Grad* $n \in \mathbb{N}$ von G über einem Körper K (kurz eine *K-Darstellung*) ist ein Gruppenhomomorphismus $\Delta\colon G \to \mathrm{GL}(n, K)$. Wenn K nicht erwähnt wird, nehmen wir $K = \mathbb{C}$ an.

Bemerkung II.13.3.

(i) Jede Darstellung $\Delta\colon G \to \mathrm{GL}(n, K)$ setzt sich zu einem Homomorphismus von Algebren fort:

$$\begin{aligned} &\Delta\colon KG \to K^{n\times n}, \\ &\sum_{g\in G} \alpha_g g \mapsto \sum_{g\in G} \alpha_g \Delta(g). \end{aligned}$$

Für $v \in V_\Delta := K^{n\times 1}$ und $\alpha \in KG$ definieren wir

$$\alpha v := \Delta(\alpha)v \in V_\Delta.$$

Man zeigt leicht, dass V_Δ auf diese Weise ein KG-Modul wird.

(ii) Sei umgekehrt ein endlich-dimensionaler KG-Modul M gegeben. Jedes $g \in G$ induziert eine Abbildung $f_g \in \mathrm{End}_K(M)$ durch $f_g(m) := gm$ für $m \in M$. Wegen

$$(f_g \circ f_{g^{-1}})(m) = g(g^{-1}m) = (gg^{-1})(m) = 1m = m$$

für alle $m \in M$ ist f_g invertierbar, d. h. $f_g \in \mathrm{GL}(M)$. Indem man eine K-Basis von M wählt, erhält man eine Darstellung $G \to \mathrm{GL}(n, K)$, $g \mapsto f_g$. Auf diese Weise entsprechen sich Darstellungen von G und endlich-dimensionale KG-Moduln.

Beispiel II.13.4.

(i) Die *triviale* Darstellung $G \to \mathrm{GL}(1, K) = K^\times$, $g \mapsto 1$ gehört zum trivialen Modul und setzt sich zur Augmentationsabbildung $KG \to K$ fort.

(ii) Sei Ω eine G-Menge und V ein K-Vektorraum mit Basis Ω. Durch die Operation von G auf Ω wird V ein KG-Modul, den man *Permutationsmodul* nennt. Die entsprechende *Permutationsdarstellung* $G \to \mathrm{GL}(V)$ wird durch Permutationsmatrizen beschrieben (jedes $g \in G$ permutiert die Basis Ω). Im Spezialfall $\Omega = G$ mit der Operation durch Linksmultiplikation erhält man den regulären KG-Modul. Die *reguläre* Darstellung entspricht im Wesentlichen dem Homomorphismus $G \to \mathrm{Sym}(G)$ aus dem Satz von Cayley.

(iii) Ist Δ eine K-Darstellung, so auch Δ^* mit $\Delta^*(g) := \Delta(g^{-1})^{\mathrm{t}}$, denn

$$\Delta\big((gh)^{-1}\big)^{\mathrm{t}} = \Delta(h^{-1}g^{-1})^{\mathrm{t}} = \big(\Delta(h^{-1})\Delta(g^{-1})\big)^{\mathrm{t}} = \Delta(g^{-1})^{\mathrm{t}}\Delta(h^{-1})^{\mathrm{t}}$$

für $g, h \in G$. Man nennt Δ^* die zu Δ *duale* Darstellung.

(iv) Ist $\Delta\colon G \to \mathrm{GL}(n, K)$ eine Darstellung und $H \leq G$, so ist die *Einschränkung* $\Delta_H\colon H \to \mathrm{GL}(n, K)$, $h \mapsto \Delta(h)$ eine Darstellung von H.

(v) Sind $\Delta\colon G \to \mathrm{GL}(n, K)$ und $\Gamma\colon G \to \mathrm{GL}(m, K)$ Darstellungen, so auch die *direkte Summe* $\Delta \oplus \Gamma\colon G \to \mathrm{GL}(n+m, K)$ mit

$$(\Delta \oplus \Gamma)(g) = \begin{pmatrix} \Delta(g) & 0 \\ 0 & \Gamma(g) \end{pmatrix}$$

für alle $g \in G$.

(vi) Das Signum $\mathrm{sgn}\colon S_n \to \mathbb{Q}^\times$ ist eine (nicht-triviale) $\mathbb{Q}$-Darstellung vom Grad 1 der symmetrischen Gruppe.

(vii) Für $G = \langle g \rangle \cong C_n$ definiert $\Delta(g) := B_{\Phi_n} \in \mathrm{GL}(\varphi(n), \mathbb{Q})$ eine $\mathbb{Q}$-Darstellung, wobei B_{Φ_n} die Begleitmatrix des n-ten Kreisteilungspolynoms ist (beachte $B_{\Phi_n}^n = 1_{\varphi(n)}$).

(viii) Die Diedergruppe D_{2n} wird von der Drehung σ um $2\pi/n$ und der Spiegelung τ an der x-Achse erzeugt (Aufgabe I.20). Daher existiert eine Darstellung $\Delta\colon D_{2n} \to \mathrm{GL}(2, \mathbb{R})$ mit

$$\Delta(\sigma) = \begin{pmatrix} \cos(2\pi/n) & -\sin(2\pi/n) \\ \sin(2\pi/n) & \cos(2\pi/n) \end{pmatrix}, \qquad \Delta(\tau) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Definition II.13.5. Zwei K-Darstellungen Δ und Γ vom Grad n heißen *ähnlich*, falls ein $S \in \mathrm{GL}(n, K)$ mit $\Delta(g) = S\Gamma(g)S^{-1}$ für alle $g \in G$ existiert.

Lemma II.13.6. *K-Darstellungen sind genau dann ähnlich, wenn die entsprechenden KG-Moduln isomorph sind.*

Beweis. Seien Δ und Γ ähnliche Darstellungen vom Grad n und seien $V_\Delta = K^{n\times 1}$ und $V_\Gamma = K^{n\times 1}$ die entsprechenden KG-Moduln. Sei $S \in \mathrm{GL}(n, K)$ mit $\Delta(g) = S\Gamma(g)S^{-1}$ für alle $g \in G$. Dann ist die Abbildung $f\colon V_\Gamma \to V_\Delta$, $v \mapsto Sv$ zunächst ein Vektorraumisomorphismus. Für $g \in G$ und $v \in V_\Gamma$ gilt

$$f(gv) = Sgv = S\Gamma(g)v = S\Gamma(g)S^{-1}Sv = \Delta(g)Sv = \Delta(g)f(v) = gf(v).$$

Daher ist f auch KG-linear.

Sei umgekehrt $f\colon V_\Gamma \to V_\Delta$ ein Isomorphismus von KG-Moduln. Da f auch K-linear ist, existiert ein $S \in \mathrm{GL}(n, K)$ mit $f(v) = Sv$ für alle $v \in V_\Gamma$. Dann ist

$$S\Gamma(g)v = f(\Gamma(g)v) = f(gv) = gf(v) = \Delta(g)f(v) = \Delta(g)Sv$$

für alle $v \in V_\Gamma$. Dies zeigt $S\Gamma(g)S^{-1} = \Delta(g)$ für alle $g \in G$. Also sind Δ und Γ ähnlich. □

Definition II.13.7. Eine K-Darstellung Δ heißt *irreduzibel*, falls der entsprechende KG-Modul V_Δ einfach ist. Anderenfalls heißt Δ *reduzibel*.

Bemerkung II.13.8.

(i) Eine Darstellung $\Delta\colon G \to \mathrm{GL}(n,K)$ ist genau dann reduzibel, wenn ein Unterraum $0 \neq U \subsetneq V_\Delta$ mit $\Delta(g)(U) \subseteq U$ für alle $g \in G$ existiert. Setzt man eine Basis von U zu einer Basis von V_Δ fort, so haben die Matrizen $\Delta(g)$ die Form $\left(\begin{smallmatrix} A & B \\ 0 & D \end{smallmatrix}\right)$. Sei nun $\operatorname{char} K = 0$. Nach Maschke und Lemma II.8.4 besitzt U dann ein Komplement W. Durch geeignete Basiswahl erreichen wir $B = 0$, d. h. Δ hat die Form $\Gamma \oplus \Lambda$. Jede $\mathbb{C}$-Darstellung ist daher (bis auf Ähnlichkeit) eine direkte Summe von irreduziblen Darstellungen. Nach Jordan-Hölder sind die direkten Summanden dabei bis auf Ähnlichkeit eindeutig bestimmt, denn sie entsprechen den Kompositionsfaktoren von V_Δ.

(ii) Die Anzahl der irreduziblen $\mathbb{C}$-Darstellungen bis auf Ähnlichkeit ist die Anzahl der einfachen Moduln bis auf Isomorphie und stimmt daher mit der Klassenzahl von G überein (Bemerkung II.12.43).

Definition II.13.9. Sei $\operatorname{char} K = 0$. Für eine K-Darstellung $\Delta\colon G \to \mathrm{GL}(n,K)$ nennt man die Abbildung $\chi_\Delta\colon G \to K$, $g \mapsto \operatorname{tr}\Delta(g)$ den *Charakter* von Δ. Man nennt $\chi_\Delta(1) = n$ den *Grad* von χ_Δ. Ist Δ (ir)reduzibel, so nennt man auch χ_Δ *(ir)reduzibel*.

Bemerkung II.13.10.

(i) Über Körpern mit positiver Charakteristik sind Charaktere weniger aussagekräftig, denn es kann $\chi(1) = 0$ gelten.

(ii) Für K-Darstellungen Δ und Γ und $g \in G$ gilt $\chi_{\Delta\oplus\Gamma}(g) = \chi_\Delta(g) + \chi_\Gamma(g)$. Daher ist die (komponentenweise) Summe von Charakteren wieder ein Charakter. Nach Bemerkung II.13.8 ist jeder Charakter die Summe von irreduziblen Charakteren.

(iii) Der nächste Satz zeigt, dass Charaktere die „Schatten“ von Darstellungen sind: Obwohl man ein n^2-dimensionales Objekt $(\Delta(g))$ durch ein 1-dimensionales Objekt $(\chi(g))$ ersetzt, bleibt die wesentliche Information erhalten.

(iv) Für $A = (a_{ij}) \in K^{n\times m}$ und $B = (b_{ij}) \in K^{m\times n}$ gilt

$$\operatorname{tr}(AB) = \sum_{i=1}^{n}\sum_{j=1}^{m} a_{ij}b_{ji} = \sum_{j=1}^{m}\sum_{i=1}^{n} b_{ji}a_{ij} = \operatorname{tr}(BA).$$

Satz II.13.11. *K-Darstellungen sind genau dann ähnlich, wenn sie den gleichen Charakter haben.*

Beweis. Seien Δ und Γ K-Darstellungen von G mit Charakter χ_Δ bzw. χ_Γ. Sei $S \in \mathrm{GL}(n,K)$ mit $\Delta(g) = S\Gamma(g)S^{-1}$ für alle $g \in G$. Nach Bemerkung II.13.10 gilt

$$\chi_\Delta(g) = \operatorname{tr}\Delta(g) = \operatorname{tr}(S\Gamma(g)S^{-1}) = \operatorname{tr}(S^{-1}S\Gamma(g)) = \operatorname{tr}\Gamma(g) = \chi_\Gamma(g)$$

für alle $g \in G$.

Sei nun umgekehrt $\chi_\Delta = \chi_\Gamma$. Sei $\Lambda_1, \ldots, \Lambda_k$ ein Repräsentantensystem für die Ähnlichkeitsklassen irreduzibler Darstellungen und sei χ_i der Charakter von Λ_i (nach dem ersten Teil des Beweises hängt χ_i nicht von der Wahl des Repräsentanten ab). Bis auf Ähnlichkeit gilt $\Delta = a_1\Lambda_1 \oplus \ldots \oplus a_k\Lambda_k$ und $\Gamma = b_1\Lambda_1 \oplus \ldots \oplus b_k\Lambda_k$ mit $a_1, \ldots, a_k, b_1, \ldots, b_k \in \mathbb{N}_0$. Ebenso ist

$$a_1\chi_1 + \ldots + a_k\chi_k = \chi_\Delta = \chi_\Gamma = b_1\chi_1 + \ldots + b_k\chi_k.$$

Seien $e_1, \ldots, e_k$ die zentral-primitiven Idempotente von KG. Nach Satz II.8.23 bewirkt die Multiplikation mit e_i die Identität auf dem i-ten einfachen KG-Modul und die Nullabbildung auf allen anderen einfachen

Moduln. Wenn wir obige Darstellungen und Charaktere also nach KG fortsetzen, gilt $\Lambda_j(e_i) = \delta_{ij} 1_{d_i}$ und $\chi_j(e_i) = \delta_{ij} d_i$. Dies zeigt

$$a_i d_i = (a_1\chi_1 + \ldots + a_k\chi_k)(e_i) = \chi_\Delta(e_i) = \chi_\Gamma(e_i) = b_i d_i.$$

Daher ist $(a_1, \ldots, a_k) = (b_1, \ldots, b_k)$ und Δ und Γ sind ähnlich. □

Definition II.13.12. Die Menge der Charaktere von irreduziblen K-Darstellungen von G sei $\mathrm{Irr}_K(G)$ und $\mathrm{Irr}(G) := \mathrm{Irr}_{\mathbb{C}}(G)$. Die Menge der Konjugationsklassen von G sei $\mathrm{Cl}(G)$.

Beispiel II.13.13.

(i) Nach Bemerkung II.12.39 und Satz II.13.11 ist $|\mathrm{Irr}(G)| = k(G) = |\mathrm{Cl}(G)|$ und

$$\boxed{|G| = \sum_{\chi \in \mathrm{Irr}(G)} \chi(1)^2.}$$

Insbesondere ist G genau dann abelsch, wenn alle irreduziblen Charaktere Grad 1 haben.

(ii) Jede K-Darstellung vom Grad 1 stimmt mit ihrem Charakter überein. Man spricht dann von *linearen* Charakteren. Insbesondere ist der *triviale* Charakter $\mathbb{1}_G$ gleich der trivialen Darstellung. Sind λ und μ lineare Charaktere, so auch $\lambda\mu$ mit $(\lambda\mu)(g) := \lambda(g)\mu(g)$ für $g \in G$ (dies wird in Satz II.13.38 verallgemeinert).

(iii) Die komplexe Konjugation (angewendet auf jeden Matrixeintrag) induziert einen Gruppenautomorphismus auf $\mathrm{GL}(n, \mathbb{C})$. Für eine Darstellung $\Delta\colon G \to \mathrm{GL}(n, \mathbb{C})$ ist daher auch $\overline{\Delta}$ mit $\overline{\Delta}(g) := \overline{\Delta(g)}$ eine Darstellung. Wir werden in Bemerkung II.13.18 sehen, dass $\overline{\Delta}$ mit der dualen Darstellung Δ^* übereinstimmt. Für den Charakter gilt $\chi_{\overline{\Delta}}(g) = \overline{\chi(g)}$ für $g \in G$. Man setzt $\overline{\chi_\Delta} := \chi_{\overline{\Delta}}$.

(iv) Der *reguläre* Charakter ρ von G gehört zur regulären K-Darstellung Δ. Wir hatten bereits gesehen, dass $\Delta(g)(h) = gh$ für $g, h \in G$ gilt. Für $g \neq 1$ ist stets $gh \neq h$, d. h. $\Delta(g)$ hat nur Nullen auf der Hauptdiagonale. Dies zeigt $\rho(1) = |G|$ und $\rho(g) = 0$ für $g \neq 1$. Andererseits ist der reguläre $\mathbb{C}G$-Modul die direkte Summe aller einfachen Moduln, wobei der Modul mit Dimension d_i mit Vielfachheit d_i auftritt (Bemerkung II.12.39). Dies zeigt

$$\rho = \sum_{\chi \in \mathrm{Irr}(G)} \chi(1)\chi.$$

(v) Ist Δ eine K-Darstellung mit Charakter χ, so ist $\det\Delta\colon G \to K$, $g \mapsto \det\Delta(g)$ ein linearer Charakter, den wir mit $\det\chi$ bezeichnen (wie üblich hängt $\det\chi$ nicht von Δ ab).

Definition II.13.14. Eine Abbildung $G \to \mathbb{C}$ heißt *Klassenfunktion*, wenn sie auf den Konjugationsklassen von G konstant ist. Die Menge aller Klassenfunktionen von G bildet mit komponentenweiser Addition und Skalarmultiplikation einen $k(G)$-dimensionalen $\mathbb{C}$-Vektorraum $\mathrm{CF}(G)$. Durch

$$\boxed{(\chi, \psi) := \frac{1}{|G|} \sum_{g \in G} \chi(g)\overline{\psi(g)}} \qquad (\chi, \psi \in \mathrm{CF}(G))$$

ist ein Skalarprodukt auf $\mathrm{CF}(G)$ gegeben (dies entspricht bis auf Normierungsfaktoren genau dem Standardskalarprodukt auf $\mathbb{C}^{k(G)}$).

Beispiel II.13.15. Für jede Darstellung Δ und $g, h \in G$ gilt

$$\chi_\Delta(ghg^{-1}) = \operatorname{tr}\Delta(ghg^{-1}) = \operatorname{tr}(\Delta(g)\Delta(h)\Delta(g)^{-1}) = \operatorname{tr}(\Delta(g)^{-1}\Delta(g)\Delta(h)) = \operatorname{tr}\Delta(h) = \chi_\Delta(h).$$

Daher sind Charaktere Klassenfunktionen.

Definition II.13.16. Sei $\operatorname{Irr}(G) = \{\chi_1, \dots, \chi_k\}$ und $g_1, \dots, g_k \in G$ ein Repräsentantensystem für $\operatorname{Cl}(G)$. Dann nennt man die Matrix $T := (\chi_i(g_j))_{i,j=1}^n \in \mathbb{C}^{k\times k}$ *Charaktertafel* von G. Sie hängt natürlich von der Reihenfolge der χ_i und der g_j ab (aber nicht von der Wahl der g_j nach Beispiel II.13.15). In der Regel wählt man $\chi_1 = \mathbb{1}_G$ und $g_1 = 1$.

Beispiel II.13.17.

(i) Nach Beispiel II.12.40 besteht $\operatorname{Irr}(S_3)$ aus dem trivialen Charakter $\mathbb{1}$, den Charakter sgn und einen weiteren Charakter vom Grad 2. Aus Beispiel II.13.4 erhält man eine Darstellung von $S_3 \overset{I.5.10}{\cong} D_6$ vom Grad 2:

$$\Delta((1,2,3)) = \frac{1}{2}\begin{pmatrix} -1 & \sqrt{2} \\ -\sqrt{2} & -1 \end{pmatrix} \qquad \Delta((1,2)) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

mit Charakter $\chi((1,2,3)) = -1$ und $\chi((1,2)) = 0$. Wegen $\chi \notin \{2\mathbb{1}, \mathbb{1} + \operatorname{sgn}, 2\operatorname{sgn}\}$ ist χ irreduzibel. Daher ist $\operatorname{Irr}(S_3) = \{\mathbb{1}_G, \operatorname{sgn}, \chi\}$ und man erhält die Charaktertafel von S_3:

	1	$(1,2)$	$(1,2,3)$
$\mathbb{1}$	1	1	1
sgn	1	-1	1
χ	2	0	-1

Alternativ lässt sich χ auch über den regulären Charakter ρ berechnen: $\chi = \frac{1}{2}(\rho - \mathbb{1} - \operatorname{sgn})$.

(ii) Sei $G = \langle g \rangle$ zyklisch der Ordnung n. Nach Beispiel II.13.13 haben die irreduziblen Charaktere $\chi_1, \dots, \chi_n$ von G Grad 1, sie sind also auch Darstellungen. Wegen $\chi_i(g)^n = \chi_i(g^n) = \chi_i(1) = 1$ ist $\chi_i(g)$ eine n-te Einheitswurzel. Für eine primitive n-te Einheitswurzel $\zeta \in \mathbb{C}$ gilt also $\chi_i(g) = \zeta^{i-1}$ bei geeigneter Anordnung. Somit ist $(\zeta^{ij})_{i,j=0}^{n-1}$ die Charaktertafel von G.

Bemerkung II.13.18. Sei $\Delta\colon G \to \operatorname{GL}(n, \mathbb{C})$ eine Darstellung und $g \in G$. Wegen $\Delta(g)^{|G|} = \Delta(g^{|G|}) = \Delta(1) = 1_n$ ist das Minimalpolynom μ von $\Delta(g)$ ein Teiler von $X^{|G|} - 1$. Daher zerfällt μ in paarweise verschiedene Linearfaktoren über $\mathbb{C}$. Folglich ist $\Delta(g)$ diagonalisierbar (Bemerkung II.10.7). Indem wir zu einer ähnlichen Darstellung übergehen, können wir $\Delta(g) = \operatorname{diag}(\zeta_1, \dots, \zeta_n)$ annehmen. Wegen $\Delta(g)^{|G|} = 1_n$ sind die ζ_i $|G|$-te Einheitswurzeln. Dies zeigt

$$\Delta^*(g) = \Delta(g^{-1}) = \operatorname{diag}(\zeta_1^{-1}, \dots, \zeta_n^{-1}) = \operatorname{diag}(\overline{\zeta_1}, \dots, \overline{\zeta_n}) = \overline{\Delta(g)} = \overline{\Delta}(g)$$

und $\chi_\Delta(g^{-1}) = \overline{\chi_\Delta(g)} = \overline{\chi_\Delta}(g)$. Die Gleichung $\chi(g^{-1}) = \overline{\chi(g)}$ gilt für jeden Charakter einer K-Darstellung (auch wenn K nicht unter komplexer Konjugation abgeschlossen ist).

Lemma II.13.19. *Die zentral-primitiven Idempotente von $\mathbb{C}G$ sind*

$$\boxed{e_\chi = \frac{\chi(1)}{|G|}\sum_{g\in G}\overline{\chi(g)}g} \qquad (\chi \in \operatorname{Irr}(G)).$$

Beweis. Sei $\Delta_1, \dots, \Delta_k$ ein Repräsentantensystem für die Ähnlichkeitsklassen irreduzibler Darstellungen. Sei χ_i der Charakter von Δ_i. Seien $e_1, \dots, e_k$ die zentral-primitiven Idempotente von $\mathbb{C}G$. Wie im Beweis von Satz II.13.11 gilt $\Delta_i(e_j) = \delta_{ij} 1_{\chi_i(1)}$ und $\chi_i(e_j) = \delta_{ij}\chi_i(1)$, wobei man Δ_i und χ_i nach $\mathbb{C}G$ fortsetzt. Für $g \in G$ gilt $\Delta_i(ge_j) = \Delta_i(g)\Delta_i(e_j) = \delta_{ij}\Delta_i(g)$ und $\chi_i(ge_j) = \delta_{ij}\chi_i(g)$. Wir schreiben $e_i = \sum_{g\in G} e_i(g)g$ mit $e_i(g) \in \mathbb{C}$. Für den regulären Charakter $\rho = \sum_{i=1}^k \chi_i(1)\chi_i$ gilt dann

$$e_i(g)|G| \overset{II.13.13}{=} \rho(g^{-1}e_i) = \sum_{j=1}^k \chi_j(1)\chi_j(g^{-1}e_i) = \chi_i(1)\chi_i(g^{-1}) \overset{II.13.18}{=} \chi_i(1)\overline{\chi_i(g)}. \qquad \square$$

Satz II.13.20. *Die irreduziblen Charaktere bilden eine Orthonormalbasis von* $\mathrm{CF}(G)$.

Beweis. Mit den Bezeichnungen aus dem vorherigen Beweis gilt

$$\frac{\delta_{ij}\chi_i(1)}{|G|} \sum_{g\in G} \overline{\chi_i(g)}g = \delta_{ij}e_i = e_ie_j = \frac{\chi_i(1)\chi_j(1)}{|G|^2} \sum_{g\in G} \Big(\sum_{h\in G} \overline{\chi_i(h)\chi_j(h^{-1}g)} \Big) g.$$

Ein Koeffizientenvergleich an der Stelle $g = 1$ zeigt

$$\delta_{ij} = \frac{1}{|G|} \sum_{h\in G} \overline{\chi_i(h)\chi_j(h^{-1})} = \frac{1}{|G|} \sum_{h\in G} \overline{\chi_i(h)}\chi_j(h) = (\chi_i, \chi_j).$$

Daher sind die irreduziblen Charaktere orthonormal und insbesondere linear unabhängig. $\square$

Bemerkung II.13.21. Jeder Charakter ψ von G lässt sich eindeutig in der Form $\psi = \sum_{\chi\in \mathrm{Irr}(G)} a_\chi \chi$ mit $a_\chi \in \mathbb{N}_0$ schreiben. Dabei gilt $a_\chi = (\psi, \chi)$ und $(\psi, \psi) = \sum_{\chi\in\mathrm{Irr}(G)} a_\chi^2$. Daher ist ψ genau dann irreduzibel, falls $(\psi, \psi) = 1$.

Satz II.13.22 (Orthogonalitätsrelationen)**.** *Sei* $\mathrm{Irr}(G) = \{\chi_1, \dots, \chi_k\}$ *und* $g_1, \dots, g_k$ *ein Repräsentantensystem für* $\mathrm{Cl}(G)$. *Für* $1 \le i, j \le k$ *gilt dann*

$$\boxed{\sum_{l=1}^k \frac{\chi_i(g_l)\overline{\chi_j(g_l)}}{|\mathrm{C}_G(g_l)|} = \delta_{ij},} \tag{1}$$

$$\boxed{\sum_{l=1}^k \chi_l(g_i)\overline{\chi_l(g_j)} = \delta_{ij}|\mathrm{C}_G(g_i)|.} \tag{2}$$

Beweis. Die Konjugationsklasse von g_i enthält genau $|G : \mathrm{C}_G(g_i)|$ Elemente (Satz I.4.7). Da Charaktere Klassenfunktionen sind, folgt

$$\sum_{l=1}^k \frac{\chi_i(g_l)\overline{\chi_j(g_l)}}{|\mathrm{C}_G(g_l)|} = \frac{1}{|G|} \sum_{g\in G} \chi_i(g)\overline{\chi_j(g)} = (\chi_i, \chi_j) \overset{II.13.20}{=} \delta_{ij}.$$

Für $A := \big(\chi_i(g_j)/|\mathrm{C}_G(g_j)|\big)_{i,j} \in \mathbb{C}^{k\times k}$ und $B := \big(\overline{\chi_j(g_i)}\big)_{i,j} \in \mathbb{C}^{k\times k}$ gilt also $AB = 1_k$. Dies zeigt $BA = 1_k = \overline{B}\,\overline{A}$, d. h. die zweite Orthogonalitätsrelation gilt. $\square$

Bemerkung II.13.23. Sei $N \trianglelefteq G$ und $\epsilon\colon G \to G/N$ der kanonische Epimorphismus. Jede Darstellung $\Delta\colon G/N \to \mathrm{GL}(n, K)$ induziert eine Darstellung $\widehat{\Delta} := \Delta \circ \epsilon\colon G \to \mathrm{GL}(n, K)$. Man nennt $\widehat{\Delta}$ die *Inflation* von Δ. Ist Δ irreduzibel, so auch $\widehat{\Delta}$. Für die Charaktere gilt $\chi_{\widehat{\Delta}}(g) = \chi_\Delta(gN)$ für $g \in G$.

Beispiel II.13.24. Nach der zweiten Orthogonalitätsrelation sind die Spalten der Charaktertafel paarweise orthogonal. Dies ist nützlich für die Berechnung fehlender Charakterwerte: Sei $G = A_4$ und $N = V_4$. Dann ist $G/N \cong C_3$. Durch Inflation erhält man lineare Charaktere $\chi_1, \chi_2, \chi_3 \in \operatorname{Irr}(G)$ mit $\chi_i((1,2,3)) = \zeta^{i-1}$, wobei $\zeta := \frac{1}{2}(-1 + \sqrt{3}\mathrm{i})$ (Beispiel II.13.17). Nach Beispiel II.12.44 besitzt G noch einen weiteren irreduziblen Charakter ψ vom Grad 3. Dies liefert folgenden Teil der Charaktertafel:

A_4	1	$(1,2)(3,4)$	$(1,2,3)$	$(1,3,2)$
χ_1	1	1	1	1
χ_2	1	1	ζ	$\overline{\zeta}$
χ_3	1	1	$\overline{\zeta}$	ζ
ψ	3			

Die letzte Zeile ergibt sich leicht aus der zweiten Orthogonalitätsrelation:

A_4	1	$(1,2)(3,4)$	$(1,2,3)$	$(1,3,2)$
χ_1	1	1	1	1
χ_2	1	1	ζ	$\overline{\zeta}$
χ_3	1	1	$\overline{\zeta}$	ζ
ψ	3	-1	0	0

Bemerkung II.13.25. Nach Bemerkung II.13.18 und Satz II.11.7 sind Charakterwerte als Summen von Einheitswurzeln ganz-algebraisch.

Satz II.13.26. *Für $\chi \in \operatorname{Irr}(G)$ ist die Abbildung*

$$\begin{aligned} \omega_\chi \colon \mathrm{Z}(\mathbb{C}G) &\to \mathbb{C}, \\ C^+ &\mapsto |C| \frac{\chi(g)}{\chi(1)} \qquad (g \in C \in \mathrm{Cl}(G)) \end{aligned}$$

ein Homomorphismus von Algebren. Dabei ist $\omega_\chi(C^+)$ ganz-algebraisch für alle $C \in \mathrm{Cl}(G)$.

Beweis. Nach Satz II.12.42 ist ω_χ als $\mathbb{C}$-lineare Abbildung durch $\omega_\chi(C^+)$ eindeutig bestimmt. Sei Δ eine Darstellung mit Charakter χ und mit einfachem $\mathbb{C}G$-Modul V_Δ. Sei $n := \chi(1)$. Wir setzen Δ wie zuvor linear nach $\mathbb{C}G$ fort. Für $x \in G$, $C \in \mathrm{Cl}(G)$ und $v \in V_\Delta$ gilt dann

$$\Delta(C^+)(xv) = C^+(xv) = (C^+x)v = (xC^+)v = x(C^+v) = x\Delta(C^+)(v).$$

Dies zeigt $\Delta(C^+) \in \operatorname{End}_{\mathbb{C}G}(V_\Delta)$. Nach Schurs Lemma und Lemma II.12.6 ist $\operatorname{End}_{\mathbb{C}G}(V_\Delta) = \mathbb{C}\,\mathrm{id}$. Daher ist $\Delta(C^+) = \lambda 1_n$ mit

$$\lambda = \frac{1}{n} \operatorname{tr} \Delta(C^+) = \frac{1}{n} \sum_{c \in C} \operatorname{tr} \Delta(c) = |C| \frac{\chi(g)}{n} = \omega_\chi(C^+),$$

wobei $g \in C$. Mit Δ ist nun auch ω_χ ein Homomorphismus von Algebren. Für $D \in \mathrm{Cl}(G)$ gilt weiter

$$C^+D^+ = \sum_{E \in \mathrm{Cl}(G)} a_E E^+$$

mit $a_E \in \mathbb{N}_0$ (ausmultiplizieren). Es folgt

$$\omega_\chi(C^+)\omega_\chi(D^+) = \omega_\chi(C^+D^+) = \sum_{E \in \mathrm{Cl}(G)} a_E \omega_\chi(E^+) \in \sum_{E \in \mathrm{Cl}(G)} \mathbb{Z}\omega_\chi(E^+) =: M.$$

Daher ist M ein endlich erzeugter $\mathbb{Z}$-Modul mit $\omega_\chi(C^+)M \subseteq M$ und $1 = \omega_\chi(1) \in M$. Die zweite Behauptung folgt nun aus Lemma II.11.5. □

Satz II.13.27. *Für alle $\chi \in \mathrm{Irr}(G)$ ist $\chi(1)$ ein Teiler von $|G|$.*

Beweis. Sei $\mathrm{Cl}(G) = \{C_1, \ldots, C_k\}$ und $g_i \in C_i$ für $i = 1, \ldots, k$. Nach der ersten Orthogonalitätsrelation ist

$$\frac{|G|}{\chi(1)} = \sum_{i=1}^{k} |C_i| \frac{\chi(g_i)}{\chi(1)} \chi(g_i^{-1}) = \sum_{i=1}^{k} \omega_\chi(C_i^+) \chi(g_i^{-1}).$$

Nach Bemerkung II.13.25 und Satz II.13.26 ist $|G|/\chi(1) \in \mathbb{Q}$ ganz-algebraisch. Die Behauptung folgt aus Beispiel II.11.3. □

Lemma II.13.28. *Sei $\Delta\colon G \to \mathrm{GL}(n, \mathbb{C})$ eine Darstellung mit Charakter χ. Für $g \in G$ gilt dann:*

(i) $|\chi(g)| \leq n$.

(ii) $|\chi(g)| = n \iff \Delta(g) \in \mathbb{C}^\times 1_n$.

(iii) $\chi(g) = n \iff g \in \mathrm{Ker}(\Delta)$.

Beweis. Nach Bemerkung II.13.18 sind die Eigenwerte $\epsilon_1, \ldots, \epsilon_n \in \mathbb{C}$ von $\Delta(g)$ Einheitswurzeln. Die Cauchy-Schwarz-Ungleichung mit den Vektoren $v := (\epsilon_1, \ldots, \epsilon_n)$ und $w := (1, \ldots, 1)$ ergibt

$$|\chi(g)| = |\epsilon_1 + \ldots + \epsilon_n| = |\langle v, w \rangle| \leq |v||w| = \sqrt{n}\sqrt{n} = n.$$

Dies zeigt (i). Gilt Gleichheit, so sind v und w linear abhängig und es folgt $\epsilon := \epsilon_1 = \epsilon_2 = \ldots = \epsilon_n$. Da $\Delta(g)$ diagonalisierbar ist (Bemerkung II.13.18), folgt $\Delta(g) = \epsilon 1_n$. Ist umgekehrt $\Delta(g) \in \mathbb{C}^\times 1_n$, so folgt $|\chi(g)| = n$. Ist sogar $\chi(g) = n$, so ist $\epsilon = 1$ und $g \in \mathrm{Ker}(\Delta)$. Die Umkehrung ist hier auch klar. □

Definition II.13.29. In der Situation von Lemma II.13.28 definieren wir

$$\mathrm{Ker}(\chi) := \mathrm{Ker}(\Delta) = \{g \in G : \chi(g) = n\},$$
$$\mathrm{Z}(\chi) := \Delta^{-1}(\mathbb{C}^\times 1_n) = \{g \in G : |\chi(g)| = n\}.$$

Man nennt $\mathrm{Ker}(\chi)$ den *Kern* und $\mathrm{Z}(\chi)$ das *Zentrum* von χ. Im Fall $\mathrm{Ker}(\chi) = 1$ nennt man χ *treu*.

Bemerkung II.13.30. Wegen $\mathbb{C}^\times 1_n \trianglelefteq \mathrm{GL}(n, \mathbb{C})$ sind $\mathrm{Ker}(\chi)$ und $\mathrm{Z}(\chi)$ Normalteiler von G mit $\mathrm{Ker}(\chi) \leq \mathrm{Z}(\chi)$ (Bemerkung I.3.24). Nach dem Homomorphiesatz ist $G/\mathrm{Ker}(\chi)$ zu einer Untergruppe von $\mathrm{GL}(n, \mathbb{C})$ isomorph und $\mathrm{Z}(\chi)/\mathrm{Ker}(\chi)$ ist zu einer Untergruppe von $\mathbb{C}^\times 1_n \cong \mathbb{C}^\times$ isomorph. Nach Satz I.8.31 ist $\mathrm{Z}(\chi)/\mathrm{Ker}(\chi)$ stets zyklisch.

Lemma II.13.31. *Sei $\chi \in \mathrm{Irr}(G)$ und $g \in C \in \mathrm{Cl}(G)$ mit $\mathrm{ggT}(\chi(1), |C|) = 1$. Dann ist $g \in \mathrm{Z}(\chi)$ oder $\chi(g) = 0$.*

Beweis. Sei $g \notin \mathrm{Z}(\chi)$ und $\alpha := \frac{\chi(g)}{\chi(1)}$. Wegen $\mathrm{ggT}(\chi(1), |C|) = 1$ existieren $a, b \in \mathbb{Z}$ mit $a\chi(1) + b|C| = 1$. Mit $\omega_\chi(C^+)$ und $\chi(g)$ ist auch

$$\alpha = \frac{\chi(g)}{\chi(1)}(a\chi(1) + b|C|) = a\chi(g) + b\omega_\chi(C^+)$$

ganz-algebraisch. Sei $n := |\langle g\rangle|$. Als Summe n-ter Einheitswurzeln ist $\chi(g) \in \mathbb{Q}_n$. Für $\sigma \in \mathcal{G} := \mathrm{Gal}(\mathbb{Q}_n|\mathbb{Q})$ ist auch $\sigma(\alpha)$ ganz-algebraisch (Nullstelle des selben Polynoms). Daher ist auch

$$\beta := \prod_{\sigma\in\mathcal{G}} \sigma(\alpha) \in \mathbb{Q}_n^{\mathcal{G}} \overset{I.10.9}{=} \mathbb{Q}$$

ganz-algebraisch, also $\beta \in \mathbb{Z}$. Wegen $g \notin \mathrm{Z}(\chi)$ ist $|\alpha| < 1$ nach Lemma II.13.28. Mit $\chi(g)$ ist auch $\sigma(\chi(g))$ eine Summe von Einheitswurzeln. Mit der Dreiecksungleichung folgt $|\sigma(\chi(g))| \leq \chi(1)$ und $|\sigma(\alpha)| \leq 1$ für alle $\sigma \in \mathcal{G}$. Folglich ist $|\beta| = \prod_{\sigma\in\mathcal{G}} |\sigma(\alpha)| < 1$, d. h. $\beta = 0$ wegen $\beta \in \mathbb{Z}$. Also ist $\alpha = 0$ und $\chi(g) = 0$. □

Lemma II.13.32. *Sei G nichtabelsch und einfach und $C \in \mathrm{Cl}(G)$. Ist $|C| = p^k$ eine Primzahlpotenz, so ist $C = \{1\}$.*

Beweis. Nehmen wir indirekt $C \neq \{1\}$ an. Sei $g \in C$ und $\chi \in \mathrm{Irr}(G) \setminus \{\mathbb{1}_G\}$. Da G einfach und nichtabelsch ist, ist $\mathrm{Ker}(\chi) = 1 = \mathrm{Z}(\chi)$ nach Bemerkung II.13.30. Im Fall $p \nmid \chi(1)$ ist also $\chi(g) = 0$ nach Lemma II.13.31. Nach der zweiten Orthogonalitätsrelation ist

$$0 = \frac{1}{p} \sum_{\chi\in\mathrm{Irr}(G)} \chi(1)\chi(g) = \frac{1}{p} + \sum_{\substack{\chi\in\mathrm{Irr}(G)\\ p\,|\,\chi(1)}} \frac{\chi(1)}{p}\chi(g).$$

Dann wäre aber $1/p$ ganz-algebraisch im Widerspruch zu Beispiel II.11.3. □

Satz II.13.33 (Burnsides p^aq^b-Satz)**.** *Gruppen der Ordnung p^aq^b mit $p, q \in \mathbb{P}$ und $a, b \in \mathbb{N}_0$ sind auflösbar.*

Beweis. Sei G ein minimales Gegenbeispiel und $1 \neq N \trianglelefteq G$. Im Fall $N \neq G$ wären N und G/N auflösbar und daher auch G (Satz I.6.5). Also ist G einfach und nichtabelsch. O. B. d. A. sei $1 \neq P \in \mathrm{Syl}_p(G)$. Nach Satz I.4.11 existiert $g \in \mathrm{Z}(P) \setminus \{1\}$. Dann ist $P \subseteq \mathrm{C}_G(g)$. Die Länge $|C| = |G : \mathrm{C}_G(g)|$ der Konjugationsklasse C von g ist daher eine q-Potenz. Aus Lemma II.13.32 folgt der Widerspruch $g = 1$. □

Bemerkung II.13.34. Satz II.13.33 war eine der ersten Anwendungen der Darstellungstheorie zur Untersuchung endlicher Gruppen. Mittlerweile kennt man auch einen (deutlich schwierigeren) Beweis, der ohne Darstellungstheorie auskommt.[1] Für den nächsten (rein gruppentheoretischen) Satz kennt man hingegen keinen Beweis, der ohne Charaktertheorie auskommt.

Satz II.13.35 (Frobenius)**.** *Sei $1 < H < G$ mit $gHg^{-1} \cap H = 1$ für alle $g \in G \setminus H$. Dann existiert $N \trianglelefteq G$ mit $G = HN$ und $H \cap N = 1$.*

Beweis (Knapp-Schmid). Sei

$$H^* := \Big(\bigcup_{g\in G} gHg^{-1}\Big) \setminus \{1\}$$

und $N := G \setminus H^*$. Nach Voraussetzung gilt $\mathrm{N}_G(H) = H$, d. h. H besitzt genau $|G : H|$ Konjugierte in G. Für je zwei verschiedene Konjugierte xHx^{-1} und yHy^{-1} gilt

$$xHx^{-1} \cap yHy^{-1} = x(H \cap x^{-1}yHy^{-1}x)x^{-1} = 1.$$

[1] siehe Abschnitt 10.2 in [H. Kurzweil, B. Stellmacher, *Theorie der endlichen Gruppen*, Springer, Berlin, 1998]

Dies zeigt $|H^*| = |G:H|(|H|-1) = |G| - |G:H|$ und $|N| = |G:H|$. Wenn wir zeigen können, dass die Klassenfunktion

$$\rho\colon G \to \mathbb{C}, \qquad g \mapsto \begin{cases} |H| & \text{falls } g \in N, \\ 0 & \text{falls } g \in H^*. \end{cases}$$

ein Charakter von G ist, so folgt $N = \mathrm{Ker}(\rho) \trianglelefteq G$. Wegen $N \cap H = 1$ ist dann $|HN| = |H||N| = |G|$ und $G = HN$. Für $\chi \in \mathrm{Irr}(G)$ müssen wir $(\chi, \rho) \in \mathbb{N}_0$ zeigen. Zunächst gilt $(\rho, \mathbb{1}_G) = \frac{|H||N|}{|G|} = 1$. Für $\chi \neq \mathbb{1}_G$ gilt nach der ersten Orthogonalitätsrelation

$$\begin{aligned} c_\chi := (\chi, \rho) &= \frac{1}{|G|} \sum_{g \in N} \chi(g)|H| = \frac{1}{|N|} \sum_{g \in G} \chi(g) - \frac{1}{|N|} \sum_{g \in H^*} \chi(g) \\ &= - \sum_{g \in H \setminus \{1\}} \chi(g) = \chi(1) - |H|(\chi_H, \mathbb{1}_H) \in \mathbb{Z}. \end{aligned}$$

Wir können $c_\chi \neq 0$ annehmen. Die Cauchy-Schwarz-Ungleichung angewendet auf die Vektoren $(\chi(g) : g \in N)$ und $(1, \ldots, 1)$ ergibt

$$(|N|c_\chi)^2 = \Big(\sum_{g \in N} \chi(g)\Big)^2 \leq |N| \sum_{g \in N} |\chi(g)|^2.$$

Es folgt

$$1 = (\chi, \chi) = \frac{1}{|G|} \sum_{g \in N} |\chi(g)|^2 + \frac{1}{|G|} \sum_{g \in H^*} |\chi(g)|^2 \geq \frac{1}{|H|}\Big(c_\chi^2 + \sum_{g \in H \setminus \{1\}} |\chi(g)|^2\Big) > 0.$$

Wegen $c_\chi^2 - \chi(1)^2 = (c_\chi + \chi(1))(c_\chi - \chi(1))$ ist andererseits

$$\frac{1}{|H|}\Big(c_\chi^2 + \sum_{g \in H \setminus \{1\}} |\chi(g)|^2\Big) = \frac{1}{|H|}\big(c_\chi^2 - \chi(1)^2\big) + (\chi_H, \chi_H) = (\chi_H, \chi_H) - (c_\chi + \chi(1))(\chi_H, \mathbb{1}_H) \in \mathbb{Z}.$$

Daher gilt Gleichheit in der Cauchy-Schwarz-Ungleichung. Dies impliziert $\chi(g) = \chi(1)$ für alle $g \in N$. Also ist $c_\chi = \chi(1) > 0$ wie gewünscht. □

Bemerkung II.13.36. In der Situation von Satz II.13.35 nennt man G eine *Frobeniusgruppe* mit *Komplement* H und *Kern* N.

Beispiel II.13.37. Sei $n \geq 3$ ungerade. Dann ist $D_{2n} = \langle \sigma, \tau : \sigma^n = \tau^2 = 1, \tau\sigma\tau = \sigma^{-1} \rangle$ eine Frobeniusgruppe mit Komplement $\langle \tau \rangle$ und Kern $\langle \sigma \rangle$, denn $\sigma^i \tau \sigma^{-i} = \sigma^{2i}\tau \neq \tau$ für $i = 1, \ldots, n-1$.

Satz II.13.38. *Sind χ und ψ Charaktere von G, so auch $\chi\psi$ mit $(\chi\psi)(g) := \chi(g)\psi(g)$ für $g \in G$.*

Beweis. Sei V ein $\mathbb{C}G$-Modul zum Charakter $\overline{\chi}$ und W ein $\mathbb{C}G$-Modul zum Charakter ψ. Wir betrachten den $\mathbb{C}$-Vektorraum $U := \mathrm{Hom}_{\mathbb{C}}(V, W)$. [2] Für $\varphi \in U$ und $g \in G$ sei $g\varphi\colon V \to W$, $v \mapsto g\varphi(g^{-1}v)$. Offenbar ist $g\varphi \in U$ und

$$((gh)\varphi)(v) = (gh)\varphi((gh)^{-1}v) = g(h\varphi(h^{-1}(g^{-1}v))) = g((h\varphi)(g^{-1}v)) = (g(h\varphi))(v)$$

für $g, h \in G$. Auf diese Weise wird U zu einem $\mathbb{C}G$-Modul. Sei $b_1, \ldots, b_n$ eine Basis von V und $c_1, \ldots, c_m$ eine Basis von W. Dann bilden die Funktionen $\varphi_{ij}\colon V \to W$, $b_k \mapsto \delta_{ik}c_j$ mit $i = 1, \ldots, n$, $j = 1, \ldots, m$

[2] Die meisten Lehrbücher führen stattdessen das Tensorprodukt $V \otimes W$ ein. Wir tun dies erst in Definition III.3.17.

eine Basis von U. Sei $\Delta\colon G \to \mathrm{GL}(nm,\mathbb{C})$ die Darstellung von U bzgl. dieser Basis. Sei $g \in G$, $g^{-1}b_i = \sum_{j=1}^n \alpha_{ji} b_j$ und $gc_i = \sum_{j=1}^m \beta_{ji} c_j$ mit $\alpha_{ji}, \beta_{ji} \in \mathbb{C}$. Dann gilt $\chi(g) = \overline{\chi}(g^{-1}) = \alpha_{11} + \ldots + \alpha_{nn}$ und $\psi(g) = \beta_{11} + \ldots + \beta_{mm}$. Außerdem ist

$$\begin{aligned}(g\varphi_{ij})(b_k) = g\varphi_{ij}(g^{-1}b_k) &= \sum_{l=1}^n \alpha_{lk} g\varphi_{ij}(b_l) = \alpha_{ik} g c_j = \alpha_{ik} \sum_{l=1}^m \beta_{lj} c_l \\ &= \alpha_{ik} \sum_{l=1}^m \beta_{lj} \varphi_{kl}(b_k) = \sum_{k=1}^n \alpha_{ik} \sum_{l=1}^m \beta_{lj} \varphi_{kl}(b_k)\end{aligned}$$

für $i,k = 1,\ldots,n$ und $j = 1,\ldots,m$. Dies zeigt

$$\chi_\Delta(g) = \sum_{i=1}^n \alpha_{ii} \sum_{j=1}^m \beta_{jj} = \chi(g)\psi(g). \qquad \square$$

Satz II.13.39. *Seien G und H endliche Gruppen. Für $\chi \in \mathrm{Irr}(G)$ und $\psi \in \mathrm{Irr}(H)$ sei*

$$\begin{aligned}\chi \times \psi\colon G \times H &\to \mathbb{C}, \\ (g,h) &\mapsto \chi(g)\psi(h).\end{aligned}$$

Dann gilt $\mathrm{Irr}(G \times H) = \big\{\chi \times \psi : \chi \in \mathrm{Irr}(G), \psi \in \mathrm{Irr}(H)\big\}$.

Beweis. Wegen $(G\times H)/H \cong G$ lässt sich $\chi \in \mathrm{Irr}(G)$ durch Inflation als Charakter von $G \times H$ auffassen. Dabei gilt $\chi(g,h) = \chi(g)$ für $(g,h) \in G \times H$. Anlog können wir $\mathrm{Irr}(H) \subseteq \mathrm{Irr}(G \times H)$ annehmen. Nach Satz II.13.38 ist $\chi \times \psi$ ein Charakter von $G \times H$. Für $\chi, \chi' \in \mathrm{Irr}(G)$ und $\psi, \psi' \in \mathrm{Irr}(H)$ gilt

$$\begin{aligned}(\chi \times \psi, \chi' \times \psi') &= \frac{1}{|G \times H|} \sum_{(g,h) \in G \times H} \chi(g)\overline{\chi'(g)}\psi(h)\overline{\psi'(h)} = \frac{1}{|G|}\sum_{g\in G} \chi(g)\overline{\chi'(g)} \frac{1}{|H|} \sum_{h \in H} \psi(h)\overline{\psi'(h)} \\ &= (\chi,\chi')(\psi,\psi') = \delta_{\chi\chi'}\delta_{\psi\psi'}.\end{aligned}$$

Nach Bemerkung II.13.21 sind $\chi \times \psi$ paarweise irreduzible Charaktere von $G \times H$. Wegen

$$\sum_{\chi \in \mathrm{Irr}(G)} \sum_{\psi \in \mathrm{Irr}(H)} (\chi \times \psi)(1)^2 = \sum_{\chi \in \mathrm{Irr}(G)} \chi(1)^2 \sum_{\psi \in \mathrm{Irr}(H)} \psi(1)^2 = |G||H| = |G \times H|$$

haben wir alle irreduziblen Charaktere gefunden. $\square$

Bemerkung II.13.40. Sind $g_1,\ldots,g_n \in G$ und $h_1,\ldots,h_m \in H$ Repräsentantensysteme für die Konjugationsklassen von G bzw. H, so ist $(g_1,h_1),(g_1,h_2),\ldots,(g_n,h_m) \in G \times H$ offenbar ein Repräsentantensystem für die Konjugationsklassen von $G \times H$. Sind $T_G = (a_{ij})$ und T_H die Charaktertafeln von G bzw. H, so erhält man die Charaktertafel von $G \times H$ durch das *Kronecker-Produkt* von Matrizen

$$T_{G\times H} = T_G \otimes T_H = \begin{pmatrix} a_{11}T_H & \cdots & a_{1n}T_H \\ \vdots & & \vdots \\ a_{na}T_H & \cdots & a_{nn}T_H \end{pmatrix} \in \mathbb{C}^{nm \times nm}.$$

Beispiel II.13.41. Da wir bereits die Charaktertafeln der zyklischen Gruppen kennen (Beispiel II.13.17), lassen sich mit dem Hauptsatz über endliche abelsche Gruppen auch die Charaktertafeln von abelschen Gruppen angeben. Zum Beispiel

$$\begin{array}{c|cccc} C_2^2 & 1 & x & y & xy \\ \hline \mathbb{1} & 1 & 1 & 1 & 1 \\ \chi & 1 & -1 & 1 & -1 \\ \psi & 1 & 1 & -1 & -1 \\ \chi\psi & 1 & -1 & -1 & 1 \end{array} \quad = \quad \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Lemma II.13.42. *Die linearen Charaktere von G bilden eine Gruppe $\hat{G} \cong G/G'$, die durch Multiplikation auf* $\mathrm{Irr}(G)$ *operiert, d. h. für $\lambda \in \hat{G}$ und $\chi \in \mathrm{Irr}(G)$ gilt $\lambda\chi \in \mathrm{Irr}(G)$.*

Beweis. Wir wissen bereits, dass $\hat{G}$ aus den Inflationen von $\mathrm{Irr}(G/G')$ besteht. Offensichtlich ist $\hat{G}$ eine Gruppe bzgl. Multiplikation. Sei

$$G/G' \cong \langle g_1 \rangle \times \ldots \times \langle g_n \rangle \cong C_{d_1} \times \ldots \times C_{d_n}$$

und $\lambda_i \in \mathrm{Irr}(\langle g_i \rangle)$ mit $\lambda_i(g_i) = e^{2\pi \mathrm{i}/d_i}$. Nach Satz II.13.39 ist

$$G/G' \to \hat{G}, g_1^{k_1} \ldots g_n^{k_n} \mapsto \lambda_1^{k_1} \times \ldots \times \lambda_n^{k_n}$$

ein Isomorphismus.

Für die zweite Aussage benutzen wir $\lambda(gh) = \lambda(g)\lambda(h)$ für $g, h \in G$. Es gilt

$$(\chi\lambda, \chi\lambda) = \frac{1}{|G|} \sum_{g \in G} \chi(g)\lambda(g)\lambda(g^{-1})\chi(g^{-1}) = (\chi, \chi) = 1$$

und die Behauptung folgt aus Bemerkung II.13.21. □

Bemerkung II.13.43. Für die konkrete Berechnung von Darstellungen mit dem Computer ist es notwendig den Körper $\mathbb{C}$ durch kleinere Körper zu approximieren. Nach Bemerkung II.13.18 liegen die Charakterwerte von G in $\mathbb{Q}_n$, wobei $n = |G|$. Brauers tiefliegender Induktionssatz impliziert, dass jede $\mathbb{C}$-Darstellung von G zu einer $\mathbb{Q}_n$-Darstellung ähnlich ist. Wir beweisen mit weniger Aufwand eine schwächere Aussage.

Satz II.13.44. *Für jede endliche Gruppe G existiert ein Zahlkörper K, sodass jede $\mathbb{C}$-Darstellung von G zu einer K-Darstellung ähnlich ist.*

Beweis. Die meisten unserer bisherigen Ergebnisse gelten auch für $\overline{\mathbb{Q}}$ anstelle von $\mathbb{C}$, denn wir haben nur Charakteristik 0 (Maschke), algebraisch abgeschlossen (Artin-Wedderburn) und die komplexe Konjugation (Skalarprodukt) benutzt. Seien also $\psi_1, \ldots, \psi_k$ die Charaktere von irreduziblen $\overline{\mathbb{Q}}$-Darstellungen. Wie in Satz II.13.20 ist $\{\psi_1, \ldots, \psi_k\}$ eine Orthonormalbasis von $\mathrm{CF}(G)$ und $k = k(G)$. Da jede $\overline{\mathbb{Q}}$-Darstellung auch eine $\mathbb{C}$-Darstellung ist, gilt

$$\psi_i = \sum_{\chi \in \mathrm{Irr}(G)} a_{i,\chi}\chi$$

für $1 \leq i \leq k$ und gewisse $a_{i,\chi} \in \mathbb{N}_0$. Aus $1 = (\psi_i, \psi_i)_G = \sum_{\chi \in \mathrm{Irr}(G)} a_{i,\chi}^2$ folgt $\psi_i \in \mathrm{Irr}(G)$ und $\mathrm{Irr}(G) = \{\psi_1, \ldots, \psi_k\}$. Jede (irreduzible) $\mathbb{C}$-Darstellung ist also zu einer $\overline{\mathbb{Q}}$-Darstellung Δ ähnlich (Satz II.13.11). Die Einträge von $\Delta(g)$ für $g \in G$ sind algebraische Zahlen, sie liegen somit in einem Zahlkörper K. Wir können K so groß wählen, dass jede (irreduzible) $\overline{\mathbb{Q}}$-Darstellung Einträge in K hat. □

Definition II.13.45. Eine Darstellung über einem Zahlkörper K heißt *absolut irreduzibel*, wenn sie als $\mathbb{C}$-Darstellung irreduzibel ist. Sind alle irreduziblen K-Darstellungen absolut irreduzibel, so nennt man K einen *Zerfällungskörper* von G.

Beispiel II.13.46.

(i) Nach Satz II.13.44 besitzt jede Gruppe einen Zerfällungskörper mit endlichem Grad über $\mathbb{Q}$. Nach Bemerkung II.13.18 ist $\mathbb{Q}_n$ ein Zerfällungskörper jeder abelschen Gruppe der Ordnung n. Man kann zeigen, dass $\mathbb{Q}$ ein Zerfällungskörper der symmetrischen Gruppen ist (ohne Beweis, Aufgabe II.71).

(ii) Die Begleitmatrix $B := B_{\Phi_3} = \left(\begin{smallmatrix} 0 & -1 \\ 1 & -1 \end{smallmatrix}\right)$ hat Ordnung 3. Da die Eigenwerte von B irrational sind, ist die Einbettung $\Delta\colon \langle B\rangle \hookrightarrow \mathrm{GL}(2,\mathbb{Q})$ eine irreduzible $\mathbb{Q}$-Darstellung. Nach Beispiel II.13.13 hat andererseits jede irreduzible $\mathbb{C}$-Darstellung der abelschen Gruppe $\langle B\rangle \cong C_3$ Grad 1. Daher ist Δ nicht absolut irreduzibel.

Satz II.13.47. *Für jede Darstellung $\Delta\colon G \to \mathrm{GL}(n,K)$ über einem Zahlkörper K sind die folgenden Aussagen äquivalent:*

(1) Δ *ist absolut irreduzibel.*

(2) $\mathrm{C}_{K^{n\times n}}(\Delta(G)) = K1_n$.

(3) $\Delta(KG) = K^{n\times n}$.

Beweis. Sei $V := K^n$ der zu Δ gehörende einfache KG-Modul, d. h. $gv = \Delta(g)(v)$ für $g \in G$ und $v \in V$. Für $f \in \mathrm{End}_K(V) \cong K^{n\times n}$ gilt $f \in \mathrm{End}_{KG}(V)$ genau dann, wenn

$$(f \circ \Delta(g))(v) = f(gv) = gf(v) = (\Delta(g) \circ f)(v)$$

für alle $v \in V$. Dies zeigt $D := \mathrm{End}_{KG}(V) \cong \mathrm{C}_{K^{n\times n}}(\Delta(G))$.

(1) $\Rightarrow$ (2): Nach Schurs Lemma gilt $\mathrm{C}_{\mathbb{C}^{n\times n}}(\Delta(G)) \cong \mathrm{End}_{\mathbb{C}G}(V) \cong \mathbb{C}$. Dies zeigt

$$\mathrm{C}_{K^{n\times n}}(\Delta(G)) = K^{n\times n} \cap \mathrm{C}_{\mathbb{C}^{n\times n}}(\Delta(G)) = K^{n\times n} \cap \mathbb{C}1_n = K1_n.$$

(2) $\Rightarrow$ (3): Nach Jacobsons Dichtheitssatz (Bemerkung II.8.29) ist $\Delta\colon KG \to \mathrm{End}_D(V) = \mathrm{End}_K(V) \cong K^{n\times n}$ surjektiv.

(3) $\Rightarrow$ (1): Angenommen Δ ist als $\mathbb{C}$-Darstellung reduzibel. Nach geeigneter Basiswahl besteht $\Delta(\mathbb{C}G)$ dann aus Matrizen der Form $\left(\begin{smallmatrix} A & 0 \\ 0 & B \end{smallmatrix}\right)$. Dies widerspricht (3). □

Satz II.13.48 (Minkowski)**.** *Jede endliche Untergruppe G von $\mathrm{GL}(n,\mathbb{Q})$ ist zu einer Untergruppe von $\mathrm{GL}(n,\mathbb{Z})$ konjugiert. Außerdem ist G für jede Primzahl $p > 2$ zu einer Untergruppe von $\mathrm{GL}(n,p)$ isomorph. Insbesondere ist $|G|$ durch eine Funktion in n beschränkt.*

Beweis. Offenbar ist $M := \sum_{g\in G} g\mathbb{Z}^n \subseteq \mathbb{Q}^n$ ein $\mathbb{Z}$-Modul, der den freien $\mathbb{Z}$-Modul $\mathbb{Z}^n$ enthält. Ist k das kgV aller Nenner von Matrixeinträgen aus allen $g \in G$, so gilt $k\mathbb{Z}^n \subseteq kM \subseteq \mathbb{Z}^n$. Nach Satz II.9.22 ist M frei vom Rang n. Sei $\gamma\colon \mathbb{Z}^n \to M$ ein entsprechender Isomorphismus von $\mathbb{Z}$-Moduln. Da $\mathbb{Z}^n$ die Standardbasis von $\mathbb{Q}^n$ enthält, lässt sich γ (eindeutig) zu einem Isomorphismus $\gamma\colon \mathbb{Q}^n \to \mathbb{Q}^n$ von $\mathbb{Q}$-Vektorräumen fortsetzen. Für $g \in G$ gilt

$$(\gamma^{-1}g\gamma)(\mathbb{Z}^n) = (\gamma^{-1}g)(M) = \gamma^{-1}(M) = \mathbb{Z}^n.$$

Dies zeigt $\gamma^{-1}G\gamma \leq \mathrm{GL}(n,\mathbb{Z})$.

Für die zweite Behauptung können wir $G \leq \mathrm{GL}(n,\mathbb{Z})$ annehmen. Es genügt zu zeigen, dass die Reduktion modulo p, $\Gamma\colon G \to \mathrm{GL}(n,p)$, injektiv ist. Im Fall $\mathrm{Ker}(\Gamma) \neq 1$ existiert ein $g \in \mathrm{Ker}(\Gamma)$ mit Primzahlordnung q. Sei $g = 1_n + dA$ mit $d \in \mathbb{Z}$ und $A \in \mathbb{Z}^{n\times n}$ mit teilerfremden Einträgen. Wegen $g \equiv 1_n \pmod p$ ist $p \mid d$. Nach der binomischen Formel gilt

$$\begin{aligned} 1_n = g^q = (1_n + dA)^q &= 1_n + qdA + \frac{q(q-1)}{2}d^2A^2 + \ldots + d^qA^q, \\ -qA = \frac{q(q-1)}{2}dA + \ldots + d^{q-1}A^q &\equiv 0 \pmod p. \end{aligned}$$

Dies zeigt $q = p$. Wegen $p > 2$ erhält man den Widerspruch

$$-A = \frac{p-1}{2}dA + \ldots + \frac{d^{p-1}}{p}A^p \equiv 0 \pmod p. \qquad \square$$

Bemerkung II.13.49.

(i) Die Begleitmatrix $B_{\Phi_6} = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix}\right) \in \mathrm{GL}(2,\mathbb{Z})$ hat Ordnung 6. Wegen $\mathrm{GL}(2,2) \cong S_3$ kann Satz II.13.48 nicht für $p = 2$ gelten. Der Beweis zeigt aber, dass der Kern der Abbildung $G \to \mathrm{GL}(n,2)$ eine elementarabelsche 2-Gruppe ist.

(ii) Der nächste Satz verallgemeinert die komplexe Konjugation von Charakteren.

Satz II.13.50. *Sei G eine Gruppe der Ordnung n. Sei $\zeta := e^{2\pi\mathrm{i}/n} \in \mathbb{Q}_n$ und $\sigma \in \mathcal{G} := \mathrm{Gal}(\mathbb{Q}_n|\mathbb{Q})$ mit $\sigma(\zeta) = \zeta^k$. Dann gilt:*

(i) Durch ${}^{\sigma}({}^{G}g) := {}^{G}(g^k)$ für $g \in G$ operiert $\mathcal{G}$ auf $\mathrm{Cl}(G)$.

(ii) Durch $\boxed{({}^{\sigma}\chi)(g) := \sigma(\chi(g)) = \chi(g^k)}$ für $g \in G$ und $\chi \in \mathrm{Irr}(G)$ operiert $\mathcal{G}$ auf $\mathrm{Irr}(G)$.

Beweis.

(i) Wegen $\mathrm{ggT}(k,n) = 1$ existiert $l \in \mathbb{Z}$ mit $kl \equiv 1 \pmod n$. Daher ist $G \to G$, $g \mapsto g^k$ eine Bijektion mit Umkehrabbildung $g \mapsto g^l$. Für $g,h,x \in G$ gilt $g = xhx^{-1} \iff g^k = xh^kx^{-1}$. Also ist ${}^{\sigma}C \in \mathrm{Cl}(G)$ für alle $C \in \mathrm{Cl}(G)$. Für $\tau \in \mathcal{G}$ mit $\tau(\zeta) = \zeta^l$ gilt

$${}^{\sigma\tau}({}^{G}g) = {}^{G}(g^{kl}) = {}^{\sigma}({}^{G}(g^l)) = {}^{\sigma}({}^{\tau}({}^{G}g)).$$

Somit operiert $\mathcal{G}$ auf $\mathrm{Cl}(G)$.

(ii) Sei K ein Zahlkörper wie in Satz II.13.44 und $\Delta\colon G \to \mathrm{GL}(d,K)$ eine Darstellung mit Charakter χ. Nach Satz I.12.2 können wir annehmen, dass $\mathbb{Q} \subseteq K$ eine Galois-Erweiterung ist. Sei $L := K\mathbb{Q}_n \subseteq \mathbb{C}$ das Kompositum von K und $\mathbb{Q}_n$. Nach Satz I.10.15 ist auch $\mathbb{Q} \subseteq L$ eine Galois-Erweiterung und die Einschränkung $\mathrm{Gal}(L|\mathbb{Q}) \to \mathrm{Gal}(\mathbb{Q}_n|\mathbb{Q})$ ist surjektiv. Sei $\hat\sigma \in \mathrm{Gal}(L|\mathbb{Q})$ mit $\hat\sigma_{|\mathbb{Q}_n} = \sigma$. Die Anwendung von $\hat\sigma$ auf Matrixeinträge liefert einen Automorphismus von $\mathrm{GL}(d,K)$. Also ist $\hat\sigma \circ \Delta\colon G \to \mathrm{GL}(d,K)$ eine irreduzible K-Darstellung mit Charakter

$$g \mapsto \mathrm{tr}\big(\hat\sigma(\Delta(g))\big) = \sigma(\mathrm{tr}\,\Delta(g)) = \sigma(\chi(g))$$

für $g \in G$. Seien $\zeta^{a_1}, \ldots, \zeta^{a_d} \in \mathbb{Q}_n$ die Eigenwerte von $\Delta(g)$ (Bemerkung II.13.18). Dann gilt

$$\chi(g^k) = \mathrm{tr}\,\Delta(g^k) = \zeta^{a_1k} + \ldots + \zeta^{a_dk} = \sigma(\zeta^{a_1} + \ldots + \zeta^{a_d}) = \sigma(\chi(g)).$$

Man sieht leicht, dass $(\sigma,\chi) \mapsto {}^{\sigma}\chi$ eine Operation definiert. $\square$

Bemerkung II.13.51.

(i) Konjugationsklassen bzw. Charaktere, die in der gleichen Bahn unter $\mathcal{G}$ liegen, nennt man *Galois-konjugiert*.

(ii) Da $\mathcal{G}$ abelsch ist, erhält man auch durch ${}^{\sigma}({}^{G}g) := {}^{G}(g^{k'})$ mit $kk' \equiv 1 \pmod{n}$ eine Operation. Es gilt dann $({}^{\sigma}\chi)({}^{\sigma}C) = \chi(C) := \chi(g)$ für $C := {}^{G}g$.

(iii) Die natürliche Operation von $\mathrm{Aut}(G)$ auf G (d. h. die Einbettung $\mathrm{Aut}(G) \hookrightarrow \mathrm{Sym}(G)$) induziert Operationen von $\mathrm{Aut}(G)$ auf $\mathrm{Cl}(G)$ und $\mathrm{Irr}(G)$. Für $\alpha \in \mathrm{Aut}(G)$, $\chi \in \mathrm{Irr}(G)$ und $g \in C \in \mathrm{Cl}(G)$ gilt dabei ${}^{\alpha}C := {}^{G}\alpha(g)$ und $({}^{\alpha}\chi)(g) = \chi(\alpha^{-1}(g))$. Wieder erhält man $({}^{\alpha}\chi)({}^{\alpha}C) = \chi(C)$. Da $\mathrm{Inn}(G)$ im Kern der Operation liegt, genügt es die Operation von $\mathrm{Out}(G)$ zu betrachten.

(iv) Die Operationen von $\mathcal{G}$ und $\mathrm{Out}(G)$ bewirken Permutationen der Zeilen und Spalten der Charaktertafel von G. Das nächste Resultat impliziert, dass Zeilen und Spalten nicht unabhängig permutiert werden können.

Satz II.13.52 (Brauers Permutationslemma)**.** *Seien G, H endliche Gruppen, sodass G auf $\mathrm{Cl}(H)$ und $\mathrm{Irr}(H)$ operiert. Für alle $g \in G$, $C \in \mathrm{Cl}(H)$ und $\chi \in \mathrm{Irr}(H)$ gelte dabei $({}^{g}\chi)({}^{g}C) = \chi(C)$. Dann stimmt der Zyklentyp von $g \in G$ in $\mathrm{Sym}(\mathrm{Cl}(H))$ mit dem Zyklentyp von g in $\mathrm{Sym}(\mathrm{Irr}(H))$ überein. Insbesondere gilt*

$$|\{C \in \mathrm{Cl}(H) : {}^{g}C = C\}| = |\{\chi \in \mathrm{Irr}(H) : {}^{g}\chi = \chi\}|$$

für alle $g \in G$.

Beweis. Sei $\mathrm{Cl}(H) = \{C_1, \ldots, C_k\}$ und $\mathrm{Irr}(H) = \{\chi_1, \ldots, \chi_k\}$. Sei $X := (\chi_i(C_j))_{i,j}$ die Charaktertafel von H. Sei $g \in G$ fest. Die Operation von g auf $\mathrm{Cl}(H)$ (bzw. $\mathrm{Irr}(H)$) wird dann durch eine Permutationsmatrix P (bzw. Q) beschrieben. Dabei gilt

$$QX = ({}^{g}\chi_i(C_j)) = (\chi_i({}^{g^{-1}}C_j)) = XP.$$

Nach der zweiten Orthogonalitätsrelation ist X invertierbar. Es folgt $Q = XPX^{-1}$, d. h. Q und P sind ähnlich. Sei $(l_1, \ldots, l_n)$ der Zyklentyp von P. Dann ist P zu einer Blockdiagonalmatrix $\mathrm{diag}(P_1, \ldots, P_l)$ ähnlich, wobei der Block P_i dem Zyklus der Länge l_i entspricht. Außerdem ist P_i zur Begleitmatrix von $X^{l_i} - 1$ ähnlich. Aus Lemma II.10.4 erhält man die Eigenwerte von P:

$$\{e^{2\pi \mathrm{i} j/l_1} : j = 0, \ldots, l_1 - 1\} \cup \ldots \cup \{e^{2\pi \mathrm{i} j/l_n} : j = 0, \ldots, l_n - 1\}$$

(mit Vielfachheiten). Da P und Q die gleichen Eigenwerte haben, ist $(l_1, \ldots, l_n)$ auch der Zyklentyp von Q. Die letzte Behauptung erhält man durch Zählen von Einerzyklen. □

Satz II.13.53 (Schur)**.** *Sei χ ein treuer Charakter von G mit Werten in einem Zahlkörper K. Dann ist $|G|$ durch eine Funktion in $\chi(1)$ und $|K : \mathbb{Q}|$ beschränkt.*

Beweis. Nach Bemerkung II.13.18 können wir $K \subseteq \mathbb{Q}_n$ mit $n = |G|$ annehmen. Da $\mathrm{Gal}(\mathbb{Q}_n|\mathbb{Q})$ abelsch ist, gilt $\mathrm{Gal}(\mathbb{Q}_n|K) \trianglelefteq \mathrm{Gal}(\mathbb{Q}_n|\mathbb{Q})$. Nach dem Hauptsatz der Galois-Theorie ist $\mathbb{Q} \subseteq K$ eine Galois-Erweiterung. Sei $\mathrm{Gal}(K|\mathbb{Q}) = \{\sigma_1, \ldots, \sigma_k\}$ mit $k := |K : \mathbb{Q}|$ und $d := \chi(1)$. Dann ist

$$\psi := \sum_{i=1}^{k} {}^{\sigma_i}\chi$$

ein Charakter vom Grad dk mit Werten in $\mathbb{Q}$. Als ganz-algebraische Zahlen liegen die Werte von ψ sogar in $\mathbb{Z}$. Offenbar ist ψ auch treu, denn die entsprechende Darstellung bildet auf Blockdiagonalmatrizen ab. Nach Lemma II.13.28 gilt $\psi(g) \in \{-dk, \ldots, dk\}$ für alle $g \in G$. Insbesondere nimmt ψ nur endlich viele Werte $dk = x_0, \ldots, x_s$ an, wobei $s \leq 2dk$. Sei $m_i := |\{g \in G : \psi(g) = x_i\}|$ für $0 \leq i \leq s$. Dann gilt $m_0 = 1$, da ψ treu ist. Da ψ^l ein Charakter ist, gilt

$$\sum_{i=0}^{s} m_i x_i^l = \sum_{g \in G} \psi(g)^l = |G|(\psi^l, \mathbb{1}_G) \equiv 0 \pmod{|G|}$$

für $l = 0, 1, \ldots$. Also ist $v = (m_0, \ldots, m_s)$ eine Lösung des Gleichungssystems $Av \equiv 0 \pmod{|G|}$ mit ganzzahliger Vandermonde-Matrix $A := (x_j^i)_{i,j=0}^{s}$. Multiplikation mit der zu A komplementären Matrix zeigt $\det(A)v \equiv 0 \pmod{|G|}$. Die Auswertung an der ersten Koordinate liefert

$$0 \neq \prod_{0 \leq i < j \leq s} (x_j - x_i) = m_0 \det(A) \equiv 0 \pmod{|G|}.$$

Insbesondere ist

$$|G| \leq \prod_{i<j} |x_j - x_i| \leq \prod_{t=1}^{2dk} t^{2dk-t+1} = \prod_{t=1}^{2dk} t!. \qquad \square$$

Beispiel II.13.54. Sei G nichtabelsch und einfach. Sei $\mathbb{1}_G \neq \chi \in \mathrm{Irr}(G)$. Wegen $\mathrm{Ker}(\chi) \lhd G$ ist χ treu. Wegen $G' = G$ ist $\chi(1) > 1$. Nehmen wir $\chi(1) = 2$ an. Nach Satz II.13.27 ist $|G|$ gerade und nach Cauchy existiert eine Involution $g \in G$. Nach Beispiel II.13.13 ist $\chi(g) = \epsilon_1 + \epsilon_2$ mit $\epsilon_i \in \{\pm 1\}$. Wegen $\mathrm{Ker}(\chi) = \mathrm{Z}(\chi) = 1$ gilt $\epsilon_1 = -\epsilon_2$ nach Lemma II.13.28. Nun ist aber $(\det \chi)(g) = \epsilon_1\epsilon_2 = -1$ und $\det \chi \neq \mathbb{1}_G$. Dies widerspricht $G' = G$.

Lemma II.13.55. *Sei $K \subseteq L$ eine separable Körpererweiterung mit $n := |L : K| < \infty$. Dann existieren genau n K-Homomorphismen $\sigma_1, \ldots, \sigma_n \colon L \to \overline{K}$. Sei $\Delta \colon L \to \mathrm{End}_K(L)$ die reguläre Darstellung (d. h. $\Delta(a)(x) = ax$ für $a, x \in L$). Dann gilt $\mathrm{tr}\,\Delta(a) = \sigma_1(a) + \ldots + \sigma_n(a)$ für alle $a \in L$.*

Beweis. Nach dem Satz vom primitiven Element gilt $L = K(x)$ für ein $x \in L$. Das Minimalpolynom μ_x von x hat Grad n und paarweise verschiedene Nullstellen $x_1, \ldots, x_n \in \overline{K}$. Durch $\sigma_i(x) := x_i$ erhält man alle K-Homomorphismen $L \to \overline{K}$. Die Matrix von $\Delta(x)$ bzgl. der Basis $1, x, \ldots, x^{n-1}$ ist gerade die Begleitmatrix B von μ_x. Da B das charakteristische Polynom μ_x besitzt, sind $x_1, \ldots, x_n$ die Eigenwerte von $\Delta(x)$. Daher gilt $\mathrm{tr}\,\Delta(x^i) = x_1^i + \ldots + x_n^i$ für $i = 0, \ldots, n-1$. Sei nun $a = a_0 + a_1 x + \ldots + a_{n-1}x^{n-1}$ mit $a_0, \ldots, a_n \in K$. Dann gilt

$$\mathrm{tr}\,\Delta(a) = \sum_{i=0}^{n-1} a_i \,\mathrm{tr}\,\Delta(x^i) = \sum_{i=0}^{n-1} a_i \sum_{j=1}^{n-1} x_j^i = \sum_{j=1}^{n} \sum_{i=0}^{n-1} a_i x_j^i = \sum_{j=1}^{n-1} \sigma_j(a). \qquad \square$$

Beispiel II.13.56. Die reguläre Darstellung von $\mathbb{C}$ als $\mathbb{R}$-Algebra bzgl. der Basis $1, \mathrm{i}$ ist gegeben durch

$$\Delta \colon \mathbb{C} \to \mathbb{R}^{2\times 2}, \qquad a + b\mathrm{i} \mapsto \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$$

mit $\mathrm{tr}\,\Delta(x) = x + \overline{x} = 2\mathrm{Re}(x)$ für $x \in \mathbb{C}$.

Definition II.13.57. Für einen Körper $K \subseteq \mathbb{C}$ und einen Charakter χ von G definieren wir

$$K(\chi) := K(\chi(g) : g \in G) \subseteq \mathbb{C}.$$

Bemerkung II.13.58. In der Situation von Definition II.13.57 gilt $K(\chi) \subseteq K\mathbb{Q}_n$ mit $n := |G|$. Nach Satz I.10.15 ist $K \subseteq K\mathbb{Q}_n$ eine Galois-Erweiterung mit abelscher Galoisgruppe

$$\mathcal{G} := \mathrm{Gal}(K\mathbb{Q}_n|K) \cong \mathrm{Gal}(\mathbb{Q}_n|\mathbb{Q}_n \cap K) \leq \mathrm{Gal}(\mathbb{Q}_n|\mathbb{Q}).$$

Wegen $\mathrm{Gal}(K\mathbb{Q}_n|K(\chi)) \trianglelefteq \mathcal{G}$, ist auch $K \subseteq K(\chi)$ eine Galois-Erweiterung. Sei $\sigma \in \mathrm{Gal}(K(\chi)|K)$ mit ${}^{\sigma}\chi = \chi$. Dann ist $K(\chi) = K(\chi)^{\sigma}$ und der Hauptsatz der Galois-Theorie impliziert $\sigma = 1$. Daher sind die Galois-konjugierten Charaktere ${}^{\sigma}\chi$ mit $\sigma \in \mathrm{Gal}(K(\chi)|K)$ paarweise verschieden.

Lemma II.13.59. *Für verschiedene $\chi, \psi \in \mathrm{Irr}_K(G)$ gilt $(\chi, \psi) = 0$.*

Beweis. Seien M und N einfache KG-Moduln bzgl. χ und ψ. Nach Lemma II.13.6 und Satz II.13.11 ist $M \not\cong N$. Für ein zentral-primitives Idempotent $e \in KG$ gilt $em = m$ und $en = 0$ für alle $m \in M$ und $n \in N$. Nehmen wir indirekt $(\chi, \psi) \neq 0$ an. Dann existiert ein einfacher $\mathbb{C}G$-Modul V, der als Kompositionsfaktor von M und N auftritt (aufgefasst als $\mathbb{C}G$-Moduln). Da e nicht gleichzeitig trivial und als Identität auf V operieren kann, hat man einen Widerspruch. □

Satz II.13.60. *Sei $K \subseteq L$ eine endliche Körpererweiterung mit $L \subseteq \mathbb{C}$ und Δ eine absolut irreduzible L-Darstellung mit Charakter χ. Dann existiert genau ein $m \in \mathbb{N}$ mit*

$$m \sum_{\sigma \in \mathrm{Gal}(K(\chi)|K)} {}^{\sigma}\chi \in \mathrm{Irr}_K(G).$$

Dabei gilt $m \,\big|\, |L : K(\chi)|$.

Beweis. Sei $\Delta\colon G \to \mathrm{GL}(d, L)$ und $n := |L : K|$. Da Δ absolut irreduzibel ist, ist $\chi \in \mathrm{Irr}(G)$. Die reguläre Darstellung $\gamma\colon L \to \mathrm{End}_K(L) \cong K^{n\times n}$ setzt sich zu einem Homomorphismus $\Gamma\colon L^{d\times d} \to K^{nd\times nd}$, $(x_{ij}) \mapsto (\gamma(x_{ij}))$ fort. Daher ist $\hat{\Delta} := \Gamma \circ \Delta\colon G \to \mathrm{GL}(nd \times nd)$ eine K-Darstellung. Für $g \in G$ sei $\Delta(g) = (\delta_{ij}(g))$. Nach Lemma II.13.55 existieren genau n K-Homomorphismen $\sigma_1, \ldots, \sigma_n\colon L \to \mathbb{C}$. Für den Charakter ψ von $\hat{\Delta}$ gilt

$$\psi(g) = \mathrm{tr}\,\Gamma(\Delta(g)) = \sum_{i=1}^{d} \mathrm{tr}\,\gamma(\delta_{ii}(g)) = \mathrm{tr}\,\gamma(\chi(g)) = \sum_{i=1}^{n} \sigma_i(\chi(g)).$$

Nach Bemerkung II.13.58 ist $K \subseteq K(\chi)$ eine Galois-Erweiterung. Insbesondere gilt $\sigma_i(K(\chi)) = K(\chi)$, d. h. die Einschränkung von σ_i liegt in $\mathcal{G} := \mathrm{Gal}(K(\chi)|K)$ für $i = 1, \ldots, n$. Jeder der $|K(\chi) : K|$ Elemente von $\mathcal{G}$ besitzt nach dem Fortsetzungssatz genau $|L : K(\chi)|$ Fortsetzungen nach L. Dies zeigt

$$\psi = |L : K(\chi)| \sum_{\sigma \in \mathcal{G}} {}^{\sigma}\chi$$

Wir können nun ψ in Charaktere von irreduziblen K-Darstellungen zerlegen $\psi = \psi_1 + \ldots + \psi_k$. Sei $\theta \in \mathrm{Irr}(G)$ ein irreduzibler Bestandteil von ψ_i als Charakter über $\mathbb{C}$. Dann existiert ein $\sigma \in \mathcal{G}$ mit $\theta = {}^{\sigma}\chi$. Wegen $K(\psi_i) = K$ gilt $(\psi_i, \theta) = (\psi_i, \chi)$. Also existieren $m_1, \ldots, m_k$ mit

$$\psi_i = m_i \sum_{\sigma \in \mathcal{G}} {}^{\sigma}\chi$$

für $i = 1, \ldots, k$. Im Fall $m_i \neq m_j$ wäre $m_i m_j |\mathcal{G}| = (\psi_i, \psi_j) = 0$ nach Lemma II.13.59. Dies zeigt $m := m_1 = \ldots = m_k$ und $m \mid km = m_1 + \ldots + m_k = |L : K(\chi)|$. □

Definition II.13.61. In der Situation von Satz II.13.60 nennt man $m_K(\chi) := m$ den *Schur-Index* von χ bzgl. K (man beachte, dass $m_K(\chi)$ nicht von L abhängt).

Lemma II.13.62. *Sei $\chi \in \mathrm{Irr}(G)$ und ψ ein Charakter einer K-Darstellung von G. Dann gilt $m_K(\chi) \mid (\chi, \psi)$. Insbesondere ist $m_K(\chi) \mid \chi(1) \,\big|\, |G|$.*

Beweis. O. B. d. A. sei $\psi \in \mathrm{Irr}_K(G)$ und $(\chi, \psi) \neq 0$. Wegen $\hat{\chi} := m_K(\chi) \sum_{\sigma \in \mathrm{Gal}(K(\chi)|K)} {}^{\sigma}\chi \in \mathrm{Irr}_K(G)$ gilt $\psi = \hat{\chi}$ nach Lemma II.13.59. Da die Charaktere ${}^{\sigma}\chi$ nach Bemerkung II.13.58 paarweise verschieden sind, gilt $(\chi, \psi) = m_K(\chi)$. Die zweite Aussage ergibt sich, indem man für ψ den regulären Charakter wählt. □

Beispiel II.13.63.

(i) Für $\chi \in \mathrm{Irr}(G)$ gilt $m_{\mathbb{R}}(\chi) \,\big|\, |\mathbb{C} : \mathbb{R}| = 2$. Für $\chi \in \mathrm{Irr}(Q_8)$ vom Grad 2 gilt $m_{\mathbb{R}}(\chi) = 2$ (siehe Bemerkung A.12.12).

(ii) Für alle $\chi \in \mathrm{Irr}(S_n)$ gilt $m_{\mathbb{Q}}(\chi) = 1$ (Folgerung III.4.20).

(iii) Fein hat bewiesen, dass $m_{\mathbb{Q}}(\chi)$ ein Teiler von $n(\chi^n, \mathbb{1}_G)$ für alle $n \in \mathbb{N}$ ist. Im Fall $\chi = \overline{\chi}$ folgt daraus der Satz von Brauer-Speiser $m_{\mathbb{Q}}(\chi) \leq 2$. Im Allgemeinen kann $m_{\mathbb{Q}}(\chi)$ aber beliebig groß werden, wobei $m_{\mathbb{Q}}(\chi)^2$ ein Teiler von $|G|$ ist nach Fein-Yamada.

(iv) Schur-Indizes lassen sich im Prinzip auch für Körper positiver Charakteristik definieren, allerdings sind sie dort stets gleich 1 (ohne Beweis).

Aufgaben

Mengenlehre

Aufgabe II.1 $(1+1+2+2+2+2$ Punkte$)$**.** Sei A eine geordnete Menge. Zeigen Sie:

(a) Jedes kleinste Element von A ist minimal.

(b) A besitzt höchstens ein kleinstes Element.

(c) Ist A wohlgeordnet, so ist A auch total geordnet.

(d) Ist A endlich und total geordnet, so ist A auch wohlgeordnet.

(e) Konstruieren Sie eine total geordnete Menge, die nicht wohlgeordnet ist.

(f) Konstruieren Sie eine Wohlordnung auf $\mathbb{Z}$.

Aufgabe II.2 $(2+2+3$ Punkte$)$**.** Sei G eine endliche Gruppe und $H \leq G$. Sei $x_1, \ldots, x_n \in G$ ein Repräsentantensystem für die Linksnebenklassen nach H.

(a) Zeigen Sie, dass $x_1^{-1}, \ldots, x_n^{-1}$ ein Repräsentantensystem für die Rechtsnebenklassen nach H ist.

(b) Konstruieren Sie ein Beispiel, in dem $x_1, \ldots, x_n$ *kein* Repräsentantensystem für die Rechtsnebenklassen nach H ist.

(c) Zeigen Sie, dass stets ein Repräsentantensystem für die Linksnebenklassen nach H existiert, das gleichzeitig ein Repräsentantensystem für die Rechtsnebenklassen ist.
Hinweis: Halls Heiratssatz.

Ideale

Aufgabe II.3 (2 Punkte)**.** Sei K ein Körper und $n \in \mathbb{N}$. Bestimmen Sie alle Ideale von $K^{n\times n}$.

Aufgabe II.4 $(2+2+3$ Punkte$)$**.** Sei $R \neq \{0\}$ ein Ring. Ein echtes Ideal $P \lhd R$ heißt *Primideal*, falls für alle $I, J \trianglelefteq R$ gilt:

$$IJ \subseteq P \Rightarrow (I \subseteq P \vee J \subseteq P).$$

Die Menge der Primideale von R nennt man *Spektrum* von R und schreibt dafür $\operatorname{Spec}(R)$. Zeigen Sie:

(a) Jedes maximale Ideal ist ein Primideal. Insbesondere ist $\operatorname{Spec}(R) \neq \varnothing$.

(b) Nicht jedes Primideal ist maximal (Beispiel?).

(c) Ist R kommutativ, so sind die folgenden Aussagen äquivalent:

(1) P ist ein Primideal.

(2) Für alle $a, b \in R$ gilt: $ab \in P \Rightarrow a \in P \vee b \in P$.

(3) R/P ist ein Integritätsbereich.

Aufgabe II.5 (2 + 2 + 2 Punkte)**.** Sei R ein kommutativer Ring. Für $I \trianglelefteq R$ sei

$$\mathcal{P}(I) := \{P \in \operatorname{Spec}(R) : I \subseteq P\}.$$

Zeigen Sie:

(i) $\mathcal{P}(\{0\}) = \operatorname{Spec}(R)$ und $\mathcal{P}(R) = \varnothing$.

(ii) Für jede Familie von Idealen $(I_j)_{j\in J}$ gilt $\mathcal{P}(\sum I_j) = \bigcap_{j\in J} \mathcal{P}(I_j)$.

(iii) Für $I, J \trianglelefteq R$ gilt $\mathcal{P}(IJ) = \mathcal{P}(I \cap J) = \mathcal{P}(I) \cup \mathcal{P}(J)$.

Bemerkung: Auf diese Weise erhält man die *Zariski-Topologie* auf $\operatorname{Spec}(R)$, wobei die $\mathcal{P}(I)$ für $I \trianglelefteq R$ die abgeschlossenen Mengen sind. Für $R = K[X_1, \ldots, X_n]$ gibt es eine Beziehung zur Zariski-Topologie auf K^n.

Aufgabe II.6 (2 + 2 + 2 Punkte)**.** Seien R und S kommutative Ringe.

(a) Zeigen Sie, dass $\operatorname{Spec}(R)$ bzgl. der Zariski-Topologie kompakt ist (d. h. zu jeder Überdeckung $\operatorname{Spec}(R) = \bigcup_{i\in I} A_i$ mit offenen Mengen A_i existiert eine endliche Teilüberdeckung).

(b) Sei $f\colon R \to S$ ein Ringhomomorphismus. Zeigen Sie $f^{-1}(P) \in \operatorname{Spec}(R)$ für alle $P \in \operatorname{Spec}(S)$.

(c) Zeigen Sie, dass die Abbildung $\operatorname{Spec}(S) \to \operatorname{Spec}(R)$, $P \mapsto f^{-1}(P)$ bzgl. der Zariski-Topologie stetig ist (Urbilder offener Mengen sind offen).

Aufgabe II.7 (1 + 2 + 2 + 3 Punkte)**.** Sei R ein Ring und $e \in R$ ein Idempotent ($e^2 = e$). Zeigen Sie:

(a) $1 - e$ ist ein Idempotent.

(b) eRe ist ein Ring mit Einselement e.
Bemerkung: Im Fall $e \neq 1$ ist eRe nach unserer Definition *kein* Teilring von R.

(c) Jedes Ideal von eRe hat die Form eIe mit $I \trianglelefteq R$.

(d) Besteht R nur aus Idempotenten, so ist R kommutativ.[3]
Hinweis: Zeigen Sie zunächst $1 + 1 = 0$ in R.

Aufgabe II.8 (2 Punkte)**.** Seien I und J nilpotente Ideale eines Rings R. Zeigen Sie, dass $I + J$ nilpotent ist.

Aufgabe II.9 (3 Punkte)**.** Sei $K := \mathbb{Q}(\sqrt{-3})$. Bestimmen Sie die Primidealzerlegung von $\mathbb{Z}_K 30$.

[3] Jacobson hat gezeigt, dass R bereits dann kommutativ ist, wenn für jedes $x \in R$ ein $n(x) > 1$ mit $x^{n(x)} = x$ existiert, siehe [S. W. Dolan, *A proof of Jacobson's Theorem*, Canad. Math. Bull. 19 (1976), 59–61]. Dies verallgemeinert auch den Satz II.8.7 von Wedderburn.

Aufgabe II.10 (2 Punkte)**.** Sei I ein Ideal eines kommutativen Rings R. Man nennt

$$\sqrt{I} := \{x \in R : \exists n \in \mathbb{N} : x^n \in I\}$$

das *Radikal* von I in R. Zum Beispiel ist $\sqrt{\{0\}}$ die Menge der nilpotenten Elemente von R. Zeigen Sie $I \subseteq \sqrt{I} \trianglelefteq R$ und $\sqrt{I} = \sqrt{\sqrt{I}}$.

Aufgabe II.11 $(2+2+2+2$ Punkte)**.** Sei R ein kommutativer Ring und $A, B, C \trianglelefteq R$. Zeigen Sie:

(a) $C \subseteq (A{:}B) \iff BC \subseteq A$.

(b) $((A{:}B){:}C) = (A{:}BC)$.

(c) $(A \cap B{:}C) = (A{:}C) \cap (B{:}C)$.

(d) $(A{:}B + C) = (A{:}B) \cap (A{:}C)$.

Aufgabe II.12 (2 Punkte)**.** Bestimmen Sie die primären Ideale und die Radikalideale von $\mathbb{Z}$.

Aufgabe II.13 (2 Punkte)**.** Sei R ein kommutativer Ring und $I \trianglelefteq R$. Beweisen oder widerlegen Sie folgende Aussage: Ist $\sqrt{I}$ ein Primideal, so ist I primär.

Aufgabe II.14 (2 Punkte)**.** Zeigen Sie, dass $(X^2, XY) = (X) \cap (X^2, XY, Y^2) = (X) \cap (X^2, Y)$ zwei verschiedene Primärzerlegungen in $K[X, Y, Z]$ sind.

Körpererweiterungen

Aufgabe II.15 $(2+2$ Punkte)**.** Sei $K := \mathbb{F}_4(X)$ und L ein Zerfällungskörper von $\alpha := Y^2 + X \in K[Y]$ über K.

(a) Zeigen Sie $|L : \mathbb{F}_2(X)| = 4$.

(b) Bestimmen Sie den separablen Abschluss von $\mathbb{F}_2(X)$ in L.

Aufgabe II.16 $(2+2$ Punkte)**.** Zeigen Sie:

(a) Eine endliche Körpererweiterung $K \subseteq L$ ist genau dann separabel, wenn eine Galois-Erweiterung $K \subseteq M$ mit $L \subseteq M$ existiert.

(b) Sind $K \subseteq L$ und $L \subseteq M$ rein inseparable Körpererweiterungen, so ist auch die Erweiterung $K \subseteq M$ rein inseparabel.

Aufgabe II.17 $(1+1+1+1$ Punkte)**.** Zeigen Sie, dass für jeden Körper K die folgenden Aussagen äquivalent sind:

(a) K ist vollkommen.

(b) Jede endliche Körpererweiterung von K ist separabel.

(c) Jede algebraische Körpererweiterung von K ist separabel.

(d) Der algebraische Abschluss $\overline{K}$ von K stimmt mit dem separablen Abschluss von K in $\overline{K}$ überein.

Aufgabe II.18 (2 Punkte)**.** Sei $K \subseteq L$ eine endliche, separable Körpererweiterung und $\overline{K}$ der algebraische Abschluss von K. Zeigen Sie, dass genau $|L : K|$ Homomorphismen der Form $L \to \overline{K}$ existieren.

Aufgabe II.19 $(1 + 1 + 2 + 2$ Punkte)**.** Zeigen Sie mit den folgenden Schritten, dass eine endliche Körpererweiterung $K \subseteq L$ genau dann ein primitives Element besitzt, wenn nur endlich viele Körper zwischen K und L liegen:

(a) Für eine Implikation kann man wie beim Satz vom primitiven Element argumentieren.

(b) Sei umgekehrt $L = K(x)$ und $\mu \in K[X]$ das Minimalpolynom von x. Für jeden Körper M mit $K \subseteq M \subseteq L$ sei μ_M das Minimalpolynom von x über M. Zeigen Sie $\mu_M \mid \mu$.

(c) Zeigen Sie $M = K(a_1, \ldots, a_n)$, wobei $a_1, \ldots, a_n$ die Koeffizienten von μ_M sind.

(d) Zeigen Sie, dass die Abbildung $M \mapsto \mu_M$ injektiv ist und folgern Sie, dass nur endlich viele M existieren.

Aufgabe II.20 (2 Punkte)**.** Sei K ein Körper und G eine endliche Gruppe. Konstruieren Sie Körper-Erweiterungen $K \subseteq L \subseteq M$, sodass $L \subseteq M$ eine Galois-Erweiterung mit Galoisgruppe G ist.
Hinweis: $M := K(X_1, \ldots, X_{|G|})$.

Aufgabe II.21 $(2 + 2$ Punkte)**.** Überprüfen Sie, ob die Teilmenge $\{\pi, X\}$ von $\mathbb{R}(X)$ algebraisch unabhängig über $\mathbb{Q}(\sqrt{2})$ ist. Handelt es sich um eine Transzendenzbasis?

Aufgabe II.22 (3 Punkte)**.** Sei K ein Körper und $P \subseteq K[X]$ die Menge der irreduziblen Polynome. Zeigen Sie, dass

$$\left\{X^i : i \in \mathbb{N}_0\right\} \cup \left\{\frac{X^i}{\alpha^j} : \alpha \in P,\ 0 \leq i < \deg \alpha,\ j \in \mathbb{N}\right\}$$

eine K-Basis von $K(X)$ ist.
Hinweis: Partialbruchzerlegung.

Aufgabe II.23 $(2 + 2 + 2 + 2 + 2 + 2$ Punkte)**.** Eine algebraische Körpererweiterung $K \subseteq L$ heißt *normal*, falls für jedes $a \in L$ das Minimalpolynom $\mu_a \in K[X]$ in $L[X]$ vollständig in Linearfaktoren zerfällt. Zeigen Sie:

(a) Jede rein inseparable Körpererweiterung ist normal.

(b) Jede Körpererweiterung vom Grad 2 ist normal.

(c) Jede algebraische Erweiterung eines endlichen Körpers ist normal.

(d) Jede Galois-Erweiterung ist normal.
Hinweis: $\mathrm{Gal}(L|K)$ operiert auf den Nullstellen von μ_a.

(e) Jede endliche, separable, normale Körpererweiterung ist eine Galois-Erweiterung.

(f) Es gibt nicht-normale Körpererweiterungen.

Teilbarkeit

Aufgabe II.24 (4 + 3 Punkte)**.**

(a) Welche der folgenden Polynome sind Primelemente in $\mathbb{Z}[X]$:

$$-1,\ 2,\ -X^2,\ X+1?$$

Hinweis: Lemma I.8.48.

(b) Zeigen Sie, dass

$$R := \Big\{\sum_{n=0}^{\infty} a_n X^n \in \mathbb{Z}[X] : a_1 = 0\Big\}$$

ein Teilring von $\mathbb{Z}[X]$ ist. Welche der Potenzen X^n mit $n \geq 2$ sind irreduzibel bzw. Primelemente in R?

Aufgabe II.25 (2 Punkte)**.** Zeigen Sie, dass die Einheitengruppe des Rings

$$R := \{a + b\sqrt{2} : a, b \in \mathbb{Z}\} \subseteq \mathbb{R}$$

unendlich ist.
Hinweis: Es genügt eine Einheit mit unendlicher Ordnung zu finden.

Aufgabe II.26 (2 Punkte)**.** Untersuchen Sie, ob $X^2 - Y^2 + 2Y - 1$ in $\mathbb{Z}[X, Y]$ irreduzibel ist.

Aufgabe II.27 (2 Punkte)**.** (Eisenstein) Sei R ein faktorieller Ring und $p \in R$ ein Primelement. Sei

$$\alpha = a_n X^n + a_{n-1} X^{n-1} + \ldots + a_0 \in R[X]$$

primitiv mit $p \mid a_0, \ldots, a_{n-1}$ und $p^2 \nmid a_0$. Zeigen Sie, dass α irreduzibel ist.

Aufgabe II.28 (2 Punkte)**.** Berechnen Sie einen größten gemeinsamen Teiler von $5 + 3\mathrm{i}$ und $6 + 7\mathrm{i}$ in $\mathbb{Z}[\mathrm{i}]$.

Aufgabe II.29 (1 + 1 + 1 + 1 Punkte)**.** Zeigen Sie, dass die Ringe

$$\mathbb{Z} + \mathbb{Z}\sqrt{-2}, \qquad \mathbb{Z} + \mathbb{Z}\sqrt{2}, \qquad \mathbb{Z} + \mathbb{Z}\sqrt{3}, \qquad \mathbb{Z} + \mathbb{Z}\frac{1+\sqrt{-3}}{2}$$

euklidisch sind.

Aufgabe II.30 (1 + 2 + 2 + 3 Punkte)**.** Eine (formale) *Potenzreihe* über einem Körper K ist eine (möglicherweise unendliche) Summe $\sum_{n=0}^{\infty} a_n X^n$ mit $a_0, a_1, \ldots \in K$.

(a) Vergewissern Sie sich, dass die Menge $K[[X]]$ aller Potenzreihen einen Integritätsbereich bildet, wobei Addition und Multiplikation wie für Polynome definiert sind.

(b) Zeigen Sie $K[[X]]^\times = \big\{\sum a_n X^n \in K[[X]] : a_0 \neq 0\big\}$.

(c) Zeigen Sie, dass $K[[X]]$ durch

$$H(\alpha) := \begin{cases} \min\{n \in \mathbb{N} : a_{n-1} \neq 0\} & \text{falls } \alpha \neq 0, \\ 0 & \text{falls } \alpha = 0 \end{cases}$$

für $\alpha = \sum a_n X^n \in K[[X]]$ zu einem euklidischen Ring wird.

(d) Eine (formale) *Laurentreihe* über K hat die Form $\sum_{n=k}^{\infty} a_n X^n$ mit $k \in \mathbb{Z}$ (es sind also auch negative Exponenten zugelassen). Zeigen Sie, dass die Menge $K((X))$ aller Laurentreihen einen Körper bildet, der zum Quotientenkörper $Q(K[[X]])$ isomorph ist.
Hinweis: Benutzen Sie die universelle Eigenschaft von $Q(K[[X]])$.

Aufgabe II.31 (2 Punkte)**.** Sei R ein noetherscher Integritätsbereich, in dem jedes irreduzible Element ein Primelement ist. Zeigen Sie, dass R faktoriell ist.
Hinweis: Beweis von Satz II.5.19.

Aufgabe II.32 (2 Punkte)**.** Seien $a, b, c, d \in \mathbb{N}$ mit $a^2 + b^2 = c^2 + d^2 \in \mathbb{P}$. Zeigen Sie $\{a, b\} = \{c, d\}$.
Bemerkung: Die Darstellung einer Primzahl als Summe von zwei Quadraten (Satz II.5.34) ist also im Wesentlichen eindeutig.

Aufgabe II.33 (2 + 2 + 2 Punkte)**.** Sei

$$n = 2^{\delta_2} \prod_{\substack{p \in \mathbb{P} \\ p \equiv 3 \pmod 4}} p^{2\delta_p} \prod_{\substack{p \in \mathbb{P} \\ p \equiv 1 \pmod 4}} p^{\delta_p}$$

die Primfaktorzerlegung von $n \in \mathbb{N}$. Sei

$$\chi \colon \mathbb{Z} \to \mathbb{Z}, \qquad n \mapsto \begin{cases} (-1)^{\frac{n-1}{2}} & \text{falls } n \text{ ungerade}, \\ 0 & \text{falls } n \text{ gerade}. \end{cases}$$

Zeigen Sie:

(a) $q(n) := |\{(a, b) \in \mathbb{Z}^2 : a^2 + b^2 = n\}| = 4 \prod_{\substack{p \in \mathbb{P} \\ p \equiv 1 \pmod 4}} (\delta_p + 1)$.

(b) $q(n) = 4 \sum_{d|n} \chi(d)$.

(c)

$$\frac{\pi}{4} = 1 - \frac{1}{3} + \frac{1}{5} \mp \dots .$$

Hinweis: Zählen Sie ganzzahlige Gitterpunkte innerhalb des Kreises mit Mittelpunkt $(0, 0)$ und Radius r. Betrachten Sie $r \to \infty$.

Moduln

Aufgabe II.34 (2 + 2 Punkte)**.** Sei $R := \mathbb{Z}/6\mathbb{Z}$. Bestimmen Sie die einfachen R-Moduln bis auf Isomorphie. Wie sehen die entsprechenden Endomorphismenringe aus?

Aufgabe II.35 $(2+2+2+2$ Punkte$)$**.** Wir betrachten $\mathbb{Q}$ als $\mathbb{Z}$-Modul. Zeigen Sie:

(a) Die rationalen Zahlen mit ungeradem Nenner bilden einen Untermodul von $\mathbb{Q}$.

(b) Jeder endlich erzeugte Untermodul von $\mathbb{Q}$ ist zyklisch, also von der Form $\mathbb{Z}q$ für ein $q \in \mathbb{Q}$.

(c) $\mathbb{Q}$ ist nicht endlich erzeugt und daher nicht noethersch.

(d) Untersuchen Sie, ob $\mathbb{Q}$ artinsch ist.

Aufgabe II.36 $(2+2+2$ Punkte$)$**.** Sei K ein Körper und R der Ring der oberen Dreiecksmatrizen in $K^{3\times 3}$.

(a) Bestimmen Sie eine Kompositionsreihe des regulären R-Moduls.

(b) Wie viele einfache R-Moduln gibt es bis auf Isomorphie?

(c) Untersuchen Sie, ob der reguläre R-Modul halbeinfach ist.

Hinweis: Aufgabe I.39.

Aufgabe II.37 $(2+2+2$ Punkte$)$**.** Sei R ein Ring und M ein R-Modul. Die Summe $\mathrm{Soc}(M)$ aller einfachen Untermoduln von M bezeichnet man als *Sockel* von M (dies ist der „größte“ halbeinfache Untermodul von M). Zeigen Sie:

(a) $\mathrm{Soc}(M \times N) = \mathrm{Soc}(M) \times \mathrm{Soc}(N)$ für R-Moduln M und N.

(b) Für Moduln $N \leq M$ gilt $\mathrm{Soc}(N) = N \cap \mathrm{Soc}(M)$ und $(\mathrm{Soc}(M) + N)/N \subseteq \mathrm{Soc}(M/N)$.

(c) Der Sockel des regulären R-Moduls ist ein Ideal von R.

Aufgabe II.38 $(2+2+2$ Punkte$)$**.** Sei

$$R := \left\{ \begin{pmatrix} a & 0 \\ b & c \end{pmatrix} : a \in \mathbb{Z},\ b, c \in \mathbb{Q} \right\}.$$

Zeigen Sie:

(a) R ist ein Teilring von $\mathbb{Q}^{2\times 2}$.

(b) Der reguläre R-Linksmodul ist noethersch, während der reguläre R-Rechtsmodul nicht noethersch ist.

(c) Folgern Sie $R \ncong R^o$.
Bemerkung: Vergleich Aufgabe III.37.

Aufgabe II.39 $(3+3$ Punkte$)$**.** Zeigen Sie:

(a) Ein Integritätsbereich ist ein Hauptidealring, wenn jedes Primideal ein Hauptideal ist.

(b) (Cohen) Ein kommutativer Ring ist noethersch, wenn jedes Primideal endlich erzeugt ist.

Hinweis: Zorns Lemma.

Aufgabe II.40 (2 Punkte)**.** Sei R ein Ring. Zeigen Sie, dass der reguläre R-Linksmodul genau dann halbeinfach ist, wenn der reguläre R-Rechtsmodul halbeinfach ist.
Hinweis: Artin-Wedderburn.

Aufgabe II.41 ($2+2+2$ Punkte)**.** Bestimmen Sie $\mathrm{J}(\mathbb{Z}/n\mathbb{Z})$, $\mathrm{J}(K[X])$ und $\mathrm{J}(K[[X]])$ für $n \in \mathbb{N}$ und jeden Körper K.

Aufgabe II.42 ($2+2+1+1$ Punkte)**.** Sei $N \subseteq R$ die Menge aller nilpotente Elemente eines Rings R. Zeigen Sie:

(a) Ist R artinsch, so gilt $\mathrm{J}(R) \subseteq N$.

(b) Ist R kommutativ, so gilt $N \trianglelefteq R$ und $N \subseteq \mathrm{J}(R)$.

(c) Es gibt artinsche Ringe R mit $\mathrm{J}(R) \subsetneq N$.

(d) Es gibt kommutative Ringe R mit $N \subsetneq \mathrm{J}(R)$.
Hinweis: Aufgabe II.41.

Aufgabe II.43 (2 Punkte)**.** Zeigen Sie, dass jeder artinsche Integritätsbereich ein Körper ist.

Aufgabe II.44 ($2+2$ Punkte)**.** Nach Aufgabe II.36 ist der Ring R der oberen Dreiecksmatrizen in $K^{3\times 3}$ für jeden Körper K artinsch. Bestimmen Sie $\mathrm{J}(R)$ und die kleinste natürliche Zahl k mit $\mathrm{J}(R)^k = 0$.

Aufgabe II.45 (4 Punkte)**.** Sei R ein Ring und $x \in R$. Zeigen Sie, dass die folgenden Aussagen äquivalent sind:

(1) $x \in \mathrm{J}(R)$.

(2) Für alle $r, s \in R$ ist $1 + rxs \in R^\times$.

Hinweis: Nakayamas Lemma mit dem regulären R-Modul.

Aufgabe II.46 ($2+2$ Punkte)**.** Sei B ein Block eines artinschen Rings R mit Blockidempotent e. Zeigen Sie $\mathrm{Z}(B) = \mathrm{Z}(R) \cap B = e\mathrm{Z}(R)e$ und $\mathrm{J}(B) = \mathrm{J}(R) \cap B = e\mathrm{J}(R)e$. Folgern Sie, dass $\mathrm{Z}(B)$ lokal ist.

Aufgabe II.47 ($2+2+2$ Punkte)**.** Sei K ein Körper und V ein abzählbar unendlich dimensionaler K-Vektorraum (z. B. $V = K[X]$). Sei $R := \mathrm{End}_K(V)$. Zeigen Sie:

(a) $I := \{f \in R : \dim f(V) < \infty\} \trianglelefteq R$.

(b) Für jedes $f \in R \setminus I$ existieren $g, h \in R$ mit $gfh = \mathrm{id}_V$.

(c) Der Ring R/I ist einfach, aber nicht halbeinfach.

Aufgabe II.48 (2 Punkte)**.** Zeigen Sie, dass das Zentrum eines einfachen Rings ein Körper ist.

Moduln über Hauptidealringen

Aufgabe II.49 (1 + 1 Punkte)**.** Sei R ein Ring und M ein freier R-Modul. Beweisen oder widerlegen Sie folgende Aussagen:

(a) Jede linear unabhängige Teilmenge von M lässt sich zu einer Basis von M ergänzen.

(b) Jedes Erzeugendensystem von M enthält eine Basis von M.

Aufgabe II.50 (3 + 3 Punkte)**.**

(a) Bestimmen Sie die Smith-Normalform von

$$\begin{pmatrix} 8 & -25 & -16 \\ 43 & -131 & -86 \\ -20 & 61 & 40 \end{pmatrix} \in \mathbb{Z}^{3\times 3}.$$

(b) Sei $N := \mathbb{Z}(4,5,6) + \mathbb{Z}(7,8,9) \leq \mathbb{Z}^3$. Bestimmen Sie die Struktur von $\mathbb{Z}^3/N$ gemäß Satz II.9.26(ii) und (iii).

Aufgabe II.51 (2 + 2 Punkte)**.** Zeigen Sie, dass der $\mathbb{Z}$-Modul $\mathbb{Q}$ torsionsfrei aber nicht frei ist.
Bemerkung: Daher ist Satz II.9.26 für unendlich erzeugte Moduln falsch.

Aufgabe II.52 (2 + 2 + 4 + 2 + 2 Punkte)**.** Seien A und B Moduln über einem kommutativen Ring R. Sei F der freie R-Modul mit Basis $A \times B$. Sei E der von den Elementen

$$\begin{aligned} &(a+a',b)-(a,b)-(a',b), && (a,a' \in A, b,b' \in B, r \in R)\\ &(a,b+b')-(a,b)-(a,b'),\\ &(ra,b)-r(a,b),\\ &(a,rb)-r(a,b) \end{aligned}$$

erzeugte Untermodul von F. Den Faktormodul F/E nennt man das *Tensorprodukt* von A und B und schreibt dafür $A \otimes_R B := F/E$. Für $a \in A$ und $b \in B$ sei $a \otimes b := (a,b) + E \in A \otimes_R B$. Zeigen Sie:

(a) Für $a, a' \in A$, $b, b' \in B$ und $r \in R$ gilt

$$\begin{aligned} (a+a') \otimes b &= a \otimes b + a' \otimes b,\\ a \otimes (b+b') &= a \otimes b + a \otimes b',\\ (ra) \otimes b &= r(a \otimes b) = a \otimes (rb). \end{aligned}$$

(b) (universelle Eigenschaft) Zu jedem R-Modul M und jeder bilinearen Abbildung $f\colon A \times B \to M$ existiert genau ein Homomorphismus $\hat{f}\colon A \otimes_R B \to M$ mit $\hat{f}(a \otimes b) = f(a,b)$.

(c) Für R-Moduln A, B und C gilt

$$\begin{aligned} A \otimes_R B &\simeq B \otimes_R A,\\ A \otimes_R (B \otimes_R C) &\simeq (A \otimes_R B) \otimes_R C,\\ (A \times B) \otimes C &\simeq (A \otimes C) \times (B \otimes C),\\ R \otimes_R A &\simeq A \end{aligned}$$

(d) Für R-Moduln A, B und C gilt

$$\mathrm{Hom}_R(A \otimes B, C) \simeq \mathrm{Hom}(A, \mathrm{Hom}_R(B, C))$$

(dies bedeutet, dass Hom und $\otimes$ zueinander adjungierte Funktoren sind).

(e) Sind $f\colon A \to A'$ und $g\colon B \to B'$ Homomorphismen von R-Moduln, so existiert ein Homomorphismus $f \otimes g\colon A \otimes B \to A' \otimes B'$ mit $(f \otimes g)(a \otimes b) = f(a) \otimes g(b)$.

Aufgabe II.53 (3 Punkte)**.** Bestimmen Sie die Frobenius-Normalform von

$$A = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix} \in \mathbb{F}_2^{4\times 4}.$$

Aufgabe II.54 (2 + 2 Punkte)**.**

(a) Sei $A \in \mathrm{GL}(3, \mathbb{Q})$ mit endlicher Ordnung. Zeigen Sie $|\langle A\rangle| \in \{1, 2, 3, 4, 6\}$.
Hinweis: Welche Minimalpolynome kommen in Frage?

(b) Sei K ein endlicher Körper. Bestimmen Sie ein Repräsentantensystem für die Konjugationsklassen von $\mathrm{GL}(2, K)$. Welche dieser Matrizen liegen in $\mathrm{SL}(2, K)$?
Hinweis: Frobenius-Normalform.

Aufgabe II.55 (2 + 2 Punkte)**.**

(a) Konstruieren Sie eine Normalbasis für $\mathbb{Q} \subseteq L$, wobei L der Zerfällungskörper von $X^3 - 2$ ist (vgl. Aufgabe I.55).

(b) Sei $p \in \mathbb{P}$ und $\zeta \in \mathbb{C}$ eine primitive p-te Einheitswurzel. Zeigen Sie, dass $\zeta, \ldots, \zeta^{p-1}$ eine Normalbasis von $\mathbb{Q}_p$ über $\mathbb{Q}$ ist.

Aufgabe II.56 (2 + 2 + 2 + 2 Punkte)**.** Entscheiden Sie welche der folgenden Ringerweiterungen ganz sind:

$$\mathbb{Z} \subseteq \mathbb{Z}[X], \qquad \mathbb{Z}[\sqrt{2}] \subseteq \mathbb{Z}[\sqrt[4]{2}], \qquad \mathbb{Q}[X] \subseteq \mathbb{Q}[X, \sqrt{2}], \qquad \mathbb{F}_3(1,1) \subseteq \mathbb{F}_3 \times \mathbb{F}_3.$$

Aufgabe II.57 (2 Punkte)**.** Sei $R \subseteq S$ eine ganze Ringerweiterung und $I \trianglelefteq S$. Zeigen Sie, dass auch $(R + I)/I \subseteq S/I$ eine ganze Ringerweiterung ist.

Algebren und Darstellungen

Aufgabe II.58 (2 Punkte)**.** Sei A eine endlich-dimensionale K-Algebra und M ein A-Modul. Zeigen Sie, dass die folgenden Aussagen äquivalent sind:

(1) Für jeden Homomorphismus $f\colon M \to P$ und jeden Monomorphismus $g\colon M \to N$ existiert ein Homomorphismus $h\colon N \to P$ mit $h \circ g = f$.

(2) Für jeden Monomorphismus $f\colon P \to M$ existiert ein $N \leq M$ mit $M = f(P) \oplus N$.

Gegebenenfalls nennt man M *injektiv*.

Aufgabe II.59 (2 + 2 + 2 Punkte)**.** Sei K ein Körper und G eine endliche Gruppe mit $N \trianglelefteq G$. Zeigen Sie:

(a) Der kanonische Epimorphismus $G \to G/N$ induziert einen Epimorphismus von Algebren $\nu_N \colon KG \to K[G/N]$.

(b) Bestimmen Sie eine K-Basis von $\mathrm{Ker}(\nu_N)$.

(c) $\mathrm{Ker}(\nu_N) = KG \cdot I(KN) = I(KN) \cdot KG$, wobei $I(KN)$ das Augmentationsideal von KN ist.

Aufgabe II.60 (3 Punkte)**.** (Skolem-Noether) Sei K ein Körper und $\gamma \colon K^{n\times n} \to K^{n\times n}$ ein Isomorphismus von Algebren. Zeigen Sie, dass ein $x \in K^{n\times n}$ mit $\gamma(a) = xax^{-1}$ für alle $a \in K^{n\times n}$ existiert.
Hinweis: K^n wird durch $av = v$ als auch durch $av = \gamma(a)v$ zu einem einfachen $K^{n\times n}$-Modul.

Aufgabe II.61 (2 + 2 + 2 Punkte)**.** Sei $A := \mathbb{F}_2 S_3$.

(a) Verifizieren Sie, dass

$$1 = \underbrace{1 + (12) + (23) + (123)}_{=:e_1} + \underbrace{1 + (12) + (23) + (132)}_{=:e_2} + \underbrace{1 + (123) + (132)}_{=:e_3}$$

eine Zerlegung in paarweise orthogonale primitive Idempotente von A ist.

(b) Folgern Sie, dass $(12) + (23) + (132)$ ein Basisidempotent von A ist.

(c) Zeigen Sie $e_1\mathrm{Z}(A)e_1 \neq \mathrm{Z}(e_1Ae_1)$.

Aufgabe II.62 (3 Punkte)**.** (Higman) Sei K ein Körper und $H \leq G$ endliche Gruppen mit $p \nmid |G : H|$. Sei V ein KG-Modul, sodass die Einschränkung V_H halbeinfach ist. Zeigen Sie, dass V halbeinfach ist.
Bemerkung: Der Fall $V = KG$ und $H = 1$ impliziert eine Richtung von Maschkes Satz.

Aufgabe II.63 (2 + 2 + 1 Punkte)**.** Sei G eine zyklische Gruppe der Ordnung $n < \infty$ und K ein Körper. Zeigen Sie, dass die K-Algebren KG und $K[X]/(X^n - 1)$ isomorph sind. Folgern Sie

$$\mathbb{Q}G \cong \bigtimes_{d|n} \mathbb{Q}_d.$$

Berechnen Sie die Grade der irreduziblen $\mathbb{Q}$-Darstellungen von G.
Hinweis: Chinesischer Restsatz für Ringe.

Aufgabe II.64 (2 Punkte)**.** Sei K ein Körper und G eine endliche Gruppe. Zeigen Sie, dass ein endlich erzeugter KG-Modul M genau dann projektiv ist, wenn M injektiv ist.

Aufgabe II.65 (2 Punkte)**.** Sei K ein Körper und $n \in \mathbb{N}$. Zeigen Sie $\mathrm{C}_{\mathrm{GL}(n,K)}(\mathrm{SL}(n, K)) = K1_n$.

Aufgabe II.66 (3 Punkte)**.** Zeigen Sie, dass die Diedergruppe D_8 und die Quaternionengruppe Q_8 die gleiche Charaktertafel besitzen (bei geeigneter Anordnung).

Aufgabe II.67 (2 + 2 Punkte)**.** Seien $\Delta\colon G \to \mathrm{GL}(n,\mathbb{C})$, $\Gamma\colon G \to \mathrm{GL}(m,\mathbb{C})$ irreduzible Matrixdarstellungen und $A \in \mathbb{C}^{n\times m}$ mit $A\Gamma(g) = \Delta(g)A$ für alle $g \in G$. Zeigen Sie:

(a) Sind Δ und Γ nicht ähnlich, so ist $A = 0$.

(b) Ist $\Delta = \Gamma$, so ist $A \in \mathbb{C}1_n$.

Aufgabe II.68 (2 + 2 + 2 + 2 Punkte)**.**

(a) Zeigen Sie, dass für $n \in \mathbb{N}$ die Abbildung $P\colon S_n \to \mathrm{GL}(n,\mathbb{C})$, $\sigma \mapsto (\delta_{i,\sigma(j)})_{i,j=1}^n$ eine Darstellung von S_n ist. Man nennt $P(\sigma)$ die zu σ gehörige *Permutationsmatrix*.

(b) Nach Bemerkung I.4.2 induziert jede Operation einer Gruppe G einen Homomorphismus $G \to S_n$. Komposition mit P liefert eine Darstellung $\Delta\colon G \to \mathrm{GL}(n,\mathbb{C})$. Beschreiben Sie den Charakter χ von Δ.

(c) Zeigen Sie, dass $(\chi, \mathbb{1}_G)$ die Anzahl der Bahnen der Operation ist. Insbesondere ist $\chi - \mathbb{1}_G$ stets ein Charakter von G.

(d) Berechnen Sie $\chi - \mathbb{1}_G$ für die natürliche Operation von $G = S_4$ auf $\{1,\dots,4\}$ und zeigen Sie, dass dieser Charakter irreduzibel ist.

Aufgabe II.69 (2 Punkte)**.** Sei K ein Körper, $A \in K^{n\times n}$ und $B \in K^{m\times m}$. Zeigen Sie für das Kronecker-Produkt $\det(A \otimes B) = \det(A)^m \det(B)^n$.
Hinweis: Gauß-Algorithmus.

Aufgabe II.70 (2 Punkte)**.** Sind χ und ψ Charaktere von G, so gilt $\det(\chi\psi) = \det(\chi)^{\psi(1)} \det(\psi)^{\chi(1)}$.

Aufgabe II.71 (2 + 2 + 2 Punkte)**.** Zeigen Sie für $G = S_n$:

(a) $g, h \in G$ sind genau dann konjugiert, wenn sie den gleichen Zyklentyp haben.

(b) Jedes $g \in G$ ist zu allen Erzeugern von $\langle g\rangle$ konjugiert.

(c) Die Charaktertafel von G ist ganzzahlig.
Hinweis: Brauers Permutationslemma.

Aufgabe II.72 (2 Punkte)**.** Sei $\chi \in \mathrm{Irr}(G)$, $g \in G$ und $z \in \mathrm{Z}(\chi)$. Zeigen Sie $\chi(gz) = \frac{\chi(z)}{\chi(1)}\chi(g)$.

Aufgabe II.73 (3 Punkte)**.** Ein *Charakter-Sudoku*: Vervollständigen Sie folgende Charaktertafel, in der die erste Spalte zum trivialen Element gehört:

χ_1					
χ_2					
χ_3					
χ_4	1	-1	1	1	i
χ_5	2	2	2	-1	0
χ_6					
χ_7	3	3	-1	0	1
χ_8					
χ_9					
χ_{10}					

Algebra III

1 Kommutative Algebra

Bemerkung III.1.1. Als Fortsetzung zu Kapitel II.11 studieren wir kommutative Ringe R, die nicht unbedingt nullteilerfrei sind. Ist R noethersch, so lässt sich mit der Primärzerlegung ein Ersatz für die Primfaktor- und Primidealzerlegung konstruieren. Anschließend entwickeln wir einen Dimensionsbegriff, der im nächsten Kapitel geometrisch interpretiert wird.

Satz III.1.2 (HILBERTs Basissatz)**.** *Ist R kommutativ und noethersch, so auch $R[X]$.*

Beweis. Nehmen wir an, dass $I \trianglelefteq R[X]$ nicht endlich erzeugt ist. Sei $f_0 := 0 \in R[X]$. Für $k \geq 1$ wählen wir induktiv $f_k \in I \setminus (f_0, \ldots, f_{k-1})$ mit minimalem Grad d_k. Dann ist sicher $0 \leq d_1 \leq d_2 \leq \ldots$. Sei $a_k \in R$ der führende Koeffizient von f_k, d. h. $f_k = a_k X^{d_k} + \ldots$. Nach Voraussetzung wird $(a_1) \subseteq (a_1, a_2) \subseteq \ldots$ stationär. Insbesondere existiert ein $k \in \mathbb{N}$ mit $a_k = \sum_{i=1}^{k-1} r_i a_i$ für gewisse $r_i \in R$. Definiere

$$g_k := f_k - \sum_{i=1}^{k-1} r_i X^{d_k - d_i} f_i.$$

Dann ist $g_k \in I \setminus (f_0, \ldots, f_{k-1})$, aber $\deg g_k < d_k$ im Widerspruch zur Wahl von f_k. □

Definition III.1.3. Eine Teilmenge S eines Rings R heißt *multiplikativ abgeschlossen*, falls $1 \in S$, $0 \notin S$ und $xy \in S$ für alle $x, y \in S$.

Lemma III.1.4. *Sei R ein kommutativer Ring und $S \subseteq R$ multiplikativ abgeschlossen. Dann gilt:*

(i) Durch

$$(r, s) \sim (r', s') \;:\Longleftrightarrow\; \exists t \in S : t(rs' - r's) = 0$$

wird eine Äquivalenzrelation auf $R \times S$ definiert. Sei $[r, s]$ die Äquivalenzklasse von (r, s).

(ii) Durch

$$[r, s] + [r', s'] := [rs' + r's, ss'],$$
$$[r, s] \cdot [r', s'] := [rr', ss']$$

wird die Menge der Äquivalenzklassen zu einem kommutativen Ring $R[S^{-1}]$ mit $0 := [0, 1]$ und $1 := [1, 1]$.

(iii) Die Abbildung $\Phi\colon R \to R[S^{-1}]$, $r \mapsto [r, 1]$ ist ein Ringhomomorphismus mit $\Phi(S) \subseteq R[S^{-1}]^\times$.

Beweis.

(i) Reflexivität und Symmetrie sind offensichtlich. Sei $(r, s) \sim (r', s') \sim (r'', s'')$ und $t, t' \in S$ mit $t(rs' - r's) = 0 = t'(r's'' - r''s')$. Dann ist $tt's' \in S$ mit

$$tt's'(rs'' - r''s) = (trs')t's'' - (t'r''s')ts = (tr's)t's'' - (t'r's'')ts = 0.$$

Dies zeigt $(r, s) \sim (r'', s'')$.

(ii) Für die Wohldefiniertheit sei $[a,b]=[a',b']$, $[c,d]=[c',d']$ und $s,t\in S$ mit $s(ab'-a'b)=0$ und $t(cd'-c'd)=0$. Dann gilt

$$st((ad+cb)b'd'-(a'd'+c'b')bd)=tdd's(ab'-a'b)+sbb't(cd'-c'd)=0$$

und $[a,b]+[c,d]=[ad+cb,bd]=[a'd'+c'b',b'd']=[a',b']+[c',d']$. Analog ist

$$\begin{aligned}st(acb'd'-a'c'bd)&=st(acb'd'-a'bcd'+a'bcd'-a'c'bd)\\&=tcd's(ab'-a'b)+sa'bt(cd'-c'd)=0\end{aligned}$$

und $[a,b][c,d]=[ac,bd]=[a'c',b'd']=[a',b'][c',d']$. Offenbar sind beide Verknüpfungen kommutativ und die Multiplikation ist assoziativ. Für die Addition gilt

$$\begin{aligned}([a,b]+[c,d])+[e,f]&=[ad+cb,bd]+[e,f]=[(ad+cb)f+ebd,bdf]=[adf+(cf+ed)b,bdf]\\&=[a,b]+[cf+ed,df]=[a,b]+([c,d]+[e,f]).\end{aligned}$$

Sicher ist $[0,1]$ neutral bzgl. $+$ und $[1,1]$ neutral bzgl. $\cdot$. Außerdem gilt $[a,b]+[-a,b]=[0,1]$. Das Distributivgesetz folgt aus

$$\begin{aligned}[a,b]([c,d]+[e,f])&=[a,b][cf+ed,df]=[a(cf+ed),bdf]=[acbf+aebd,b^2df]\\&=[ac,bd]+[ae,bf]=[a,b][c,d]+[a,b][e,f].\end{aligned}$$

(iii) Es gilt $\Phi(1)=[1,1]=1$, $\Phi(a+b)=[a+b,1]=[a,1]+[b,1]$ und $\Phi(ab)=[ab,1]=[a,1][b,1]$. Für $s\in S$ gilt $[s,1][1,s]=1$. Daher ist $\Phi(s)$ eine Einheit in $R[S^{-1}]$. □

Definition III.1.5. Man nennt $R[S^{-1}]$ die *Lokalisierung* von R nach S.

Bemerkung III.1.6.

(i) Die Definition von $\sim$ besagt, dass $[r,s]$ bis auf „Erweitern und Kürzen“ eindeutig bestimmt ist.

(ii) Ist R ein Integritätsbereich, so kann man in der Definition von $\sim$ stets $t=1$ wählen. In diesem Fall ist Φ injektiv und wir schreiben $\frac{r}{s}$ anstatt $[r,s]$. Die Wahl $S=R\setminus\{0\}$ liefert den Quotientenkörper $R[S^{-1}]=Q(R)$ von R und Φ ist die kanonische Einbettung aus Aufgabe I.40. Für eine kleinere Teilmenge S kann man $R[S^{-1}]$ als Ringadjunktion in $R\subseteq Q(R)$ auffassen (die Verwendung der eckigen Klammern ist daher konsistent).

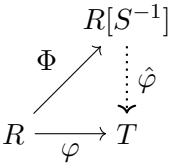
(iii) Die Elemente aus S werden mittels Φ in Lemma III.1.4 invertierbar gemacht. Dies erklärt die Schreibweise $R[S^{-1}]$. Besteht S bereits aus Einheiten, so ist Φ ein Isomorphismus und man hat nichts gewonnen. Ist nämlich $[r,1]=[0,1]$, so existiert $t\in S$ mit $tr=0$. Dies zeigt $r=t^{-1}tr=0$. Ist $[r,s]\in R[S^{-1}]$ beliebig, so gilt $[r,s]=[rs^{-1},1]\in\Phi(R)$.

Beispiel III.1.7.

(i) Sei $x\in R\setminus\{0\}$ und $S=\{x^n:n\in\mathbb{N}_0\}\setminus\{0\}$. Dann nennt man $R[x^{-1}]:=R[S^{-1}]$ die Lokalisierung von R nach x. Für $R=K[X]$ und $x=X$ erhält man den Ring der *Laurent-Polynome* $K[X,X^{-1}]$.

(ii) Ist $P\trianglelefteq R$ ein Primideal, so kann man $S=R\setminus P$ wählen. Man schreibt dann $R_P:=R[S^{-1}]$. Offenbar ist $R_PP:=(\Phi(P))=\{[r,s]:r\in P,s\notin P\}\trianglelefteq R_P$. Für $R=\mathbb{Z}$ und $P=(p)$ mit $p\in\mathbb{P}$ erhält man $\mathbb{Z}_{(p)}=\{\frac{a}{b}:a,b\in\mathbb{Z},p\nmid b\}$.

Satz III.1.8 (Universelle Eigenschaft)**.** *Sei $\varphi\colon R \to T$ ein Homomorphismus von kommutativen Ringen. Sei $S \subseteq R$ multiplikativ abgeschlossen mit $\varphi(S) \subseteq T^\times$. Dann existiert genau ein Ringhomomorphismus $\hat{\varphi}\colon R[S^{-1}] \to T$ mit $\hat{\varphi}([r,1]) = \varphi(r)$ für alle $r \in R$.*



Beweis. Für $[a,b] \in R[S^{-1}]$ sei $\hat{\varphi}([a,b]) := \varphi(a)\varphi(b)^{-1} \in T$. Sei $[a,b] = [c,d]$, $s \in S$ mit $s(ad - cb) = 0$. Dann folgt $\varphi(s)\varphi(a)\varphi(b)^{-1} = \varphi(s)\varphi(c)\varphi(d)^{-1}$. Wegen $\varphi(s) \in T^\times$ ergibt sich $\hat{\varphi}([a,b]) = \varphi(a)\varphi(b)^{-1} = \varphi(c)\varphi(d)^{-1} = \hat{\varphi}([c,d])$, d. h. $\hat{\varphi}$ ist wohldefiniert. Sicher ist $\hat{\varphi}([1,1]) = 1$ und $\hat{\varphi}([a,b][c,d]) = \hat{\varphi}([a,b])\hat{\varphi}([c,d])$. Schließlich gilt

$$\begin{aligned}\hat{\varphi}([a,b] + [c,d]) &= \hat{\varphi}([ad + cb, bd]) = \varphi(ad + cb)\varphi(bd)^{-1} \\ &= \varphi(a)\varphi(b)^{-1} + \varphi(c)\varphi(d)^{-1} = \hat{\varphi}([a,b]) + \hat{\varphi}([c,d]).\end{aligned}$$

Also ist $\hat{\varphi}$ ein Ringhomomorphismus. Sei auch $\gamma\colon R[S^{-1}] \to T$ ein Homomorphismus mit $\gamma([a,1]) = \varphi(a)$ für alle $a \in R$. Dann gilt

$$\gamma([a,b]) = \gamma([a,1][1,b]) = \gamma([a,1])\gamma([b,1])^{-1} = \varphi(a)\varphi(b)^{-1} = \hat{\varphi}([a,b])$$

für alle $[a,b] \in R[S^{-1}]$. Dies zeigt $\gamma = \hat{\varphi}$. □

Satz III.1.9. *Mit den Bezeichnungen aus Lemma III.1.4 sind die Abbildungen*

$$P \mapsto \Phi^{-1}(P), \qquad Q \mapsto (\Phi(Q))$$

zueinander inverse Bijektionen zwischen der Menge der Primideale von $R[S^{-1}]$ und der Menge der zu S disjunkten Primideale von R.

Beweis. Für ein Primideal $P \trianglelefteq R[S^{-1}]$ ist auch $\Phi^{-1}(P) \trianglelefteq R$ ein Primideal, da Φ ein Homomorphismus ist. Angenommen es existiert $s \in S \cap \Phi^{-1}(P)$. Dann ist $\Phi(s) \in P \cap R[S^{-1}]^\times$ und man erhält den Widerspruch $P = R[S^{-1}]$. Also ist $\Phi^{-1}(P) \cap S = \varnothing$. Selbstverständlich ist $(\Phi(\Phi^{-1}(P))) \subseteq P$. Sei umgekehrt $[r,s] \in P$. Dann ist $[r,1] = [s,1][r,s] \in P$ also $r \in \Phi^{-1}(P)$ und $[r,s] = [1,s][r,1] \in (\Phi(\Phi^{-1}(P)))$. Dies zeigt $(\Phi(\Phi^{-1}(P))) = P$

Sei nun umgekehrt $Q \trianglelefteq R$ ein Primideal mit $Q \cap S = \varnothing$. Nach Definition ist $(\Phi(Q)) \trianglelefteq R[S^{-1}]$. Im Fall $(\Phi(Q)) = R[S^{-1}]$ enthält $\Phi(Q)$ eine Einheit, sagen wir $[q,1]$. Sei $[rq,s] = [r,s][q,1] = 1$. Dann existiert $t \in S$ mit $t(rq - s) = 0$. Dies ergibt den Widerspruch $st = trq \in S \cap Q = \varnothing$. Also ist $(\Phi(Q))$ ein echtes Ideal. Seien $[a,b], [c,d] \in R[S^{-1}]$ mit $[ac,bd] = [a,b][c,d] \in (\Phi(Q))$. Sei $[r,s] \in R[S^{-1}]$ und $q \in Q$ mit $[ac,bd] = [rq,s]$. Wieder existiert $t \in S$ mit $t(acs - rqbd) = 0$. Aus $acst = rbdq \in Q$ folgt $ac \in Q$, da Q ein Primideal ist und $st \in S$. O. B. d. A. sei $a \in Q$. Dann ist $[a,b] = [a,1][1,b] \in (\Phi(Q))$. Somit ist $(\Phi(Q))$ ein Primideal von $R[S^{-1}]$ mit $Q \subseteq \Phi^{-1}((\Phi(Q)))$. Sei schließlich $x \in \Phi^{-1}((\Phi(Q)))$. Dann existieren $q \in Q$ und $[r,s] \in R[S^{-1}]$ mit $[x,1] = [r,s][q,1] = [rq,s]$. Sei $t \in S$ mit $t(xs - rq) = 0$. Aus $xst = trq \in Q$ folgt $x \in Q$. Damit ist $\Phi^{-1}((\Phi(Q))) = Q$ gezeigt. □

Satz III.1.10. *Sei R ein kommutativer, noetherscher Ring und $S \subseteq R$ multiplikativ abgeschlossen. Dann ist $R[S^{-1}]$ noethersch.*

Beweis. Für $I \trianglelefteq R[S^{-1}]$ ist $J := \Phi^{-1}(I) \trianglelefteq R$ endlich erzeugt, sagen wir $J = Rx_1 + \ldots + Rx_n$. Mit $[r,s] \in I$ ist auch $[r,1] = [s,1][r,s] \in I$ und $y \in J$. Dann existieren $r_1, \ldots, r_n \in R$ mit $r = r_1x_1 + \ldots + r_nx_n$. Es folgt $[r,s] = [r_1,s][x_1,1] + \ldots + [r_n,s][x_n,1]$. Daher wird I von $[x_1,1], \ldots, [x_n,1]$ erzeugt. Dies zeigt, dass jedes (Links)ideal von $R[S^{-1}]$ endlich erzeugt ist. □

Bemerkung III.1.11. Ein kommutativer Ring R ist offenbar genau dann lokal, wenn $R/\mathrm{J}(R)$ ein Körper ist (vgl. Satz II.12.11).

Satz III.1.12. *Für jedes Primideal P eines kommutativen Rings R ist R_P lokal mit $\mathrm{J}(R_P) = R_P P$ und $R_P/\mathrm{J}(R_P) \cong Q(R/P)$.*

Beweis. Nach Satz III.1.9 korrespondieren die Primideale von R_P mit den Primidealen von R, die in P enthalten sind. Daher muss $R_P P = (\Phi(P))$ das einzige maximale Ideal von R_P sein.

Der kanonische Ringhomomorphismus $\varphi\colon R \to R/P \hookrightarrow Q(R/P)$, $r \mapsto r+P$ erfüllt $\varphi(R\setminus P) \subseteq Q(P/R)^\times$. Nach der universellen Eigenschaft lässt er sich zu $\hat{\varphi}\colon R_P \to Q(R/P)$, $[r,s] \mapsto \frac{r+P}{s+P}$ fortsetzen. Wegen $Q(R)^\times = \{s+P : s \in R\setminus P\}$ ist $\hat{\varphi}$ surjektiv. Nach dem Homomorphiesatz muss $\mathrm{Ker}(\hat{\varphi})$ ein maximales Ideal sein, d. h. $\mathrm{Ker}(\hat{\mu}) = \mathrm{J}(R_P)$ und $R_P/\mathrm{J}(R_P) \cong Q(R)$. □

Bemerkung III.1.13. Sei R kommutativ und $I \trianglelefteq R$. In Aufgabe II.10 wurde das *Radikal*

$$\sqrt{I} := \{x \in R : \exists n \in \mathbb{N} : x^n \in I\} \trianglelefteq R$$

von I eingeführt. Es gilt $I \subseteq \sqrt{I} = \sqrt{\sqrt{I}}$ und $I = R \Leftrightarrow \sqrt{I} = R$.

Lemma III.1.14. *Sei R kommutativ und noethersch. Für jedes Ideal $I \trianglelefteq R$ existiert ein $n \in \mathbb{N}$ mit $\sqrt{I}^n \subseteq I$.*

Beweis. Da R noethersch ist, ist $\sqrt{I}$ endlich erzeugt, sagen wir $\sqrt{I} = (x_1, \ldots, x_k)$. Sei $x_i^{n_i} \in I$ für $i = 1, \ldots, k$ und $n := n_1 + \ldots + n_k$. Für $r_1x_1 + \ldots + r_kx_k \in \sqrt{I}$ gilt dann

$$(r_1x_1 + \ldots + r_kx_k)^n = \sum_{\substack{(i_1,\ldots,i_k)\in\mathbb{N}_0^k \\ i_1+\ldots+i_k=n}} \binom{n}{i_1, \ldots, i_k} r_1^{i_1}x_1^{i_1} \ldots r_k^{i_k}x_k^{i_k} \in I,$$

denn für mindestens ein j ist $i_j \geq n_j$. Dies zeigt $\sqrt{I}^n \subseteq I$. □

Satz III.1.15. *Für jedes Ideal I eines kommutativen Rings R ist $\sqrt{I}$ der Durchschnitt aller Primideale von R, die I enthalten.*

Beweis. Sei $x \in \sqrt{I}$ mit $x^n \in I$. Für jedes Primideal $P \supseteq I$ gilt dann $x \in P$. Sei nun $x \in R \setminus \sqrt{I}$. Mit Zorns Lemma zeigt man leicht, dass $\{J \trianglelefteq R : I \subseteq J, x^n \notin J \forall n \in \mathbb{N}\}$ ein maximales Element P besitzt. Angenommen es existieren $a, b \in R \setminus P$ mit $ab \in P$. Dann existieren $n, m \in \mathbb{N}$ mit $x^n \in (P, a)$ und $x^m \in (P, b)$. Seien $r, s \in R$ und $p, q \in P$ mit $x^n = p + ra$ und $x^m = q + sb$. Dann erhält man den Widerspruch $x^{n+m} = (p + ra)(q + sb) = pq + raq + psb + rsab \in P$. Also ist P ein Primideal mit $x \notin P$. □

Definition III.1.16. Sei R kommutativ und $I \trianglelefteq R$. Man nennt I

- *Radikalideal*, falls $I = \sqrt{I}$, d. h. aus $x^n \in I$ folgt $x \in I$ für alle $x \in R$ und $n \in \mathbb{N}$.
- *primär*, falls $I \neq R$ und für alle $x, y \in R$ gilt: Aus $xy \in I$ folgt $x \in I$ oder $y \in \sqrt{I}$.

Bemerkung III.1.17.

(i) Die Bedingung $xy \in I \Rightarrow x \in I \vee y \in \sqrt{I}$ gilt natürlich auch für yx. Sie lässt sich also symmetrisch formulieren: $xy \in I \Rightarrow x \in I \vee y \in I \vee x, y \in \sqrt{I}$.

(ii) Nach Satz III.1.15 ist jedes Radikalideal ein Durchschnitt von Primidealen. Umgekehrt sieht man leicht, dass jeder Durchschnitt von Primidealen ein Radikalideal ist.

Beispiel III.1.18.

(i) Die Primideale von R sind genau die primären Radikalideale.

(ii) Das Ideal $(4) \trianglelefteq \mathbb{Z}$ ist primär, aber weder ein Primideal noch ein Radikalideal.

(iii) Das Ideal $(2) \times (0) \trianglelefteq \mathbb{Z} \times \mathbb{Z}$ ist ein Radikalideal, aber weder ein Primideal noch primär.

Lemma III.1.19. *Ist $I \trianglelefteq R$ primär, so ist $\sqrt{I}$ ein Primideal.*

Beweis. Sei $x, y \in R$ mit $xy \in \sqrt{I}$. Dann existiert $n \in \mathbb{N}$ mit $x^n y^n \in I$. Es folgt $x^n \in I$ oder $y^{nm} \in I$ für ein $m \in \mathbb{N}$. Dies zeigt $x \in \sqrt{I}$ oder $y \in \sqrt{I}$. Also ist $\sqrt{I}$ ein Primideal. □

Definition III.1.20. Sei R kommutativ, $I \trianglelefteq R$ und $S \subseteq R$. Wir definieren

$$(I{:}S) := \{r \in R : \forall s \in S : rs \in I\}.$$

Man zeigt leicht: $I \subseteq (I{:}S) \trianglelefteq R$. Für $S = \{s\}$ schreiben wir $(I{:}s)$ anstelle von $(I{:}S)$. Die Primideale der Form $(I{:}s)$ nennt man die zu I *assoziierten* Primideale.

Satz III.1.21 (Lasker-Noether)**.** *Sei R kommutativ und noethersch. Für jedes Ideal $I \trianglelefteq R$ existieren primäre Ideale $P_1, \ldots, P_n \trianglelefteq R$ mit $I = P_1 \cap \ldots \cap P_n$, $\bigcap_{j \neq i} P_j \nsubseteq P_i$ für $i = 1, \ldots, n$ und $\sqrt{P_i} \neq \sqrt{P_j}$ für $i \neq j$. Dabei sind $\sqrt{P_1}, \ldots, \sqrt{P_n}$ die zu I assoziierten Primideale. Insbesondere ist n eindeutig bestimmt.*

Beweis.

Existenz:
Im Fall $I = R$ gilt die Behauptung mit $n = 0$. Sei $\mathcal{M}$ die Menge der Ideale, die sich nicht als Durchschnitt von primären Idealen schreiben lassen. Nehmen wir $\mathcal{M} \neq \varnothing$ an. Da R noethersch ist, existiert ein maximales Element $M \in \mathcal{M}$. Existieren $I, J \trianglelefteq R$ mit $I \neq M \neq J$ und $M = I \cap J$, so ist $I, J \notin \mathcal{M}$. Dann sind aber I und J Durchschnitte von primären Idealen und somit auch M. Also ist M kein Schnitt von größeren Idealen. Wir zeigen, dass M selbst primär ist. Sei dafür $x, y \in R$ mit $xy \in M$ und $y \notin \sqrt{M}$. Offenbar gilt $M \subseteq (M{:}y) \subseteq (M{:}y^2) \subseteq \ldots$. Da R noethersch ist, gilt

$$I := (M{:}y^n) = (M{:}y^{n+1}) = \ldots$$

für ein $n \in \mathbb{N}$. Sei $J := M + (y^n) \trianglelefteq R$ und $r \in I \cap J$. Dann existieren $s \in R$ und $t \in M$ mit $r = t + sy^n$ und $ty^n + sy^{2n} = ry^n \in M$. Es folgt $sy^{2n} \in M$ und $s \in (M{:}y^{2n}) = (M{:}y^n) = I$. Nun ist $r = t + sy^n \in M$ und $I \cap J = M$. Aus dem ersten Teil des Beweises folgt $I = M$, denn $y^n \in J \setminus M$. Also gilt $x \in (M{:}y) \subseteq I \subseteq M$ und M ist primär. Damit hat man den Widerspruch $M \notin \mathcal{M}$. Jedes Ideal I ist also ein Durchschnitt von primären Idealen $P_1, \ldots, P_n$.

Im Fall $\bigcap_{j \neq i} P_j \subseteq P_i$ für ein i entfernt man P_i ohne den Durchschnitt zu verändern. Sei $\sqrt{P_i} = \sqrt{P_j}$ mit $i \neq j$. Seien $x, y \in R$ mit $xy \in P_i \cap P_j$. Dann gilt $x \in P_i \cap P_j$ oder $y \in \sqrt{P_i} = \sqrt{P_j} = \sqrt{P_i \cap P_j}$.

Also ist $P_i \cap P_j$ primär und wir können P_i, P_j durch $P_i \cap P_j$ ersetzen. Nach endlich vielen Ersetzungen gilt $\sqrt{P_i} \neq \sqrt{P_j}$ für $i \neq j$.

Eindeutigkeit: Sei $1 \leq i \leq n$ und $Q_i := \bigcap_{j \neq i} P_j$ (für $n = 1$ sei $Q_i = R$). Nach Lemma III.1.14 gilt $\sqrt{P_i}^m \subseteq P_i$ und $\sqrt{P_i}^m Q_i \subseteq P_i \cap Q_i = I$, falls m groß genug ist. Sei m minimal mit $\sqrt{P_i}^m Q_i \subseteq I$. Dann existiert $y \in \sqrt{P_i}^{m-1} Q_i \setminus I$ (notfalls $m = 1$). Wir zeigen $\sqrt{P_i} = (I{:}y)$. Wegen $y \notin I$ ist $y \in Q_i \setminus P_i$. Für $r \in R$ mit $yr \in I \subseteq P_i$ gilt $r \in \sqrt{P_i}$, da P_i primär ist. Dies zeigt $(I{:}y) \subseteq \sqrt{P_i}$. Umgekehrt gilt $\sqrt{P_i} y \subseteq \sqrt{P_i}^m Q_i \subseteq I$, also $\sqrt{P_i} \subseteq (I{:}y)$.

Es bleibt zu zeigen, dass jedes zu I assoziierte Primideal $(I{:}r)$ unter den $\sqrt{P_i}$ auftritt. Im Fall $r \in I$ wäre $(I{:}r) = R$ kein Primideal. Sei also $r \notin I$. Dann ist $Q := \prod_{r \notin P_i} P_i \neq R$ nicht das leere Produkt. Es folgt $Qr \subseteq P_1 \cap \ldots \cap P_n = I$ und $Q \subseteq (I{:}r)$. Da $(I{:}r)$ ein Primideal ist, ergibt sich $P_i \subseteq (I{:}r)$ für ein i mit $r \notin P_i$. Es folgt $\sqrt{P_i} \subseteq \sqrt{(I{:}r)} = (I{:}r)$. Sei umgekehrt $s \in R$ mit $rs \in I \subseteq P_i$. Dann folgt $s \in \sqrt{P_i}$, da P_i primär ist. Dies zeigt $(I{:}r) \subseteq P_i$. □

Bemerkung III.1.22. Man nennt $I = P_1 \cap \ldots \cap P_n$ in Satz III.1.21 eine *Primärzerlegung* von I. Im Allgemeinen sind die primären Ideale $P_1, \ldots, P_n$ nicht eindeutig bestimmt (Aufgabe II.14). Ist I jedoch ein Radikalideal, so kann man nach Satz III.1.15 für $P_1, \ldots, P_n$ Primideale wählen. Es gilt dann $\sqrt{P_i} = P_i$ für $i = 1, \ldots, n$.

Beispiel III.1.23.

(i) Sei R ein faktorieller Ring und $x = p_1^{a_1} \ldots p_n^{a_n} \in R$ eine Primfaktorzerlegung. Dann ist $(x) = (p_1^{a_1}) \cap \ldots \cap (p_n^{a_n})$ eine Primärzerlegung mit $\sqrt{(p_i^{a_i})} = (p_i)$ für $i = 1, \ldots, n$.

(ii) Sei R ein Dedekindring und $I = P_1^{a_1} \ldots P_n^{a_n} \trianglelefteq R$ eine Primidealzerlegung. Dann ist $I = P_1^{a_1} \cap \ldots \cap P_n^{a_n}$ eine Primärzerlegung mit $\sqrt{P_i^{a_i}} = P_i$ für $i = 1, \ldots, n$. Die Primärzerlegung kann daher als gemeinsame Verallgemeinerung der Primfaktor- und Primidealzerlegung angesehen werden. Zum Beispiel ist $\mathbb{Z}[\sqrt{-5}][X]$ noethersch nach Hilberts Basissatz, aber weder faktoriell noch ein Dedekindring.

(iii) Offenbar sind (X, Z) und (Y, Z) Primideale in $R := K[X, Y, Z]$, denn $R/(X, Z) \cong K[Y] \cong R/(Y, Z)$ ist ein Integritätsbereich. Daher ist $I := (XY, Z) = (X, Z) \cap (Y, Z)$ eine Primärzerlegung. Nehmen wir an, dass I ein Produkt von Primidealen $I = P_1 \ldots P_n$ ist. Wegen $I \subseteq (X, Z)$ und $I \subseteq (Y, Z)$ existieren i, j mit $P_i \subseteq (X, Z)$ und $P_j \subseteq (Y, Z)$. Im Fall $i = j$ ist $P_i = I$. Wegen $X, Y \notin I$ ist I aber kein Primideal. Daher ist $i \neq j$ und man erhält den Widerspruch

$$Z \in I \subseteq P_i P_j = (RX + RZ)(RY + RZ) = (XY, XZ, YZ, Z^2)$$

(man setze gedanklich $X = Y = 0$). Also besitzt I keine Primidealzerlegung.

Satz III.1.24. *Sei R kommutativ, $I \trianglelefteq R$ und $P \trianglelefteq R$ ein Primideal mit $I \subseteq P$. Dann existiert ein minimales Primideal Q mit $I \subseteq Q \subseteq P$ (d. h. zwischen I und Q liegt kein Primideal). Ist R zusätzlich noethersch, so ist Q zu I assoziiert. Insbesondere gibt es dann nur endlich viele Q.*

Beweis. Die Menge $\mathcal{M}$ aller Primideale zwischen I und P ist wegen $P \in \mathcal{M}$ nichtleer und durch $\subseteq$ geordnet. Sei $\mathcal{N} \subseteq \mathcal{M}$ total geordnet und $S := \bigcap_{N \in \mathcal{N}} N$. Sind $x_1, x_2 \in R \setminus S$, so existieren $N_i \in \mathcal{N}$ mit $x_i \notin N_i$ für $i = 1, 2$. O. B. d. A. sei $N_1 \subseteq N_2$. Da N_1 ein Primideal ist, folgt $x_1 x_2 \notin N_1$ und $x_1 x_2 \notin S$. Daher ist S ein Primideal mit $I \subseteq S$, d. h. $S \in \mathcal{M}$ ist eine untere Schranke von $\mathcal{N}$. Nach Zorns Lemma besitzt $\mathcal{M}$ ein minimales Element Q.

Sei nun R noethersch und $I = P_1 \cap \ldots \cap P_n$ eine Primärzerlegung, sodass $\sqrt{P_1}, \ldots, \sqrt{P_n}$ die zu I assoziierten Primideale sind. Aus $P_1 \ldots P_n \subseteq I \subseteq Q$ folgt $P_i \subseteq Q$ und $\sqrt{P_i} \subseteq Q$ für ein $1 \leq i \leq n$. Die Minimalität von Q liefert $Q = \sqrt{P_i}$. Die letzte Aussage folgt aus Lasker-Noether. □

Bemerkung III.1.25. In der Situation von Satz III.1.24 sagt man: Q *liegt minimal* über I. Ist I selbst ein Primideal, so ist $Q = I$. Ist I ein Radikalideal, so ist I der Durchschnitt der zu I assoziierten Primideale $P_1, \ldots, P_n$ (Bemerkung III.1.22). Die Eindeutigkeit der Primärzerlegung zeigt, dass $P_1, \ldots, P_n$ minimal über I liegen. Im Allgemeinen sind jedoch nicht alle zu I assoziierten Primideale minimal über I.

Lemma III.1.26. *Sei R kommutativ und M ein endlich erzeugter R-Modul. Sei $I \trianglelefteq R$ mit $IM = M$. Dann existiert $a \in I$ mit $(1-a)M = 0$.*

Beweis. Sei $M = Rx_1 + \ldots + Rx_n$. Wegen $IM = M$ gilt auch $M = Ix_1 + \ldots + Ix_n$. Seien $a_{ij} \in I$ mit $x_i = \sum_{j=1}^n a_{ij}x_j$ für $i = 1, \ldots, n$. Mit $b_{ij} := \delta_{ij} - a_{ij}$ gilt $\sum_{j=1}^n b_{ij}x_j = 0$ für $i = 1, \ldots, n$. Die Leibniz-Formel für $B := (b_{ij}) \in R^{n\times n}$ impliziert $\det B = 1 - a$ für ein $a \in I$. Sei B_{ij} die Streichmatrix aus der Laplace-Entwicklung und $d_{ij} := (-1)^{i+j} \det B_{ij}$. Dann gilt $\det B = \sum_{i=1}^n b_{ij}d_{ij}$ durch Entwicklung nach der j-ten Spalte. Ersetzt man die j-te Spalte von B durch die k-te Spalte für $k \neq j$, so erhält man $\sum_{i=1}^n b_{ik}d_{ij} = 0$, denn die neue Matrix besitzt zwei identische Spalten. Daraus folgt

$$\det(B)x_j = \sum_{i=1}^n b_{ij}d_{ij}x_j = \sum_{k=1}^n x_k \sum_{i=1}^n b_{ik}d_{ij} = \sum_{i=1}^n d_{ij} \sum_{k=1}^n b_{ik}x_k = 0$$

für $j = 1, \ldots, n$. Zusammen erhält man $(1-a)M = 0$. □

Satz III.1.27 (Krulls Durchschnittsatz)**.** *Sei R kommutativ und noethersch. Sei $I \lhd R$ und $J := \bigcap_{n\in\mathbb{N}} I^n$. Dann gilt $IJ = J$ und es existiert ein $a \in I$ mit $(1-a)J = 0$. Ist R lokal oder ein Integritätsbereich, so ist $J = 0$.*

Beweis. Sei $P \trianglelefteq R$ primär mit $IJ \subseteq P \subseteq \sqrt{P}$. Aus Lemma III.1.19 folgt $J \subseteq \sqrt{P}$, denn $J \subseteq I$. Nach Lemma III.1.14 gilt $\sqrt{P}^n \subseteq P$ für ein $n \in \mathbb{N}$. Dies zeigt $J = J^n \subseteq P$. Da IJ nach Lasker-Noether ein Durchschnitt von primären Idealen ist, ergibt sich $J \subseteq IJ \subseteq J$. Nach Lemma III.1.26 mit $M = J$ existiert $a \in I$ mit $(1-a)J = 0$. Ist R lokal, so ist $1 - a \in R \setminus \mathrm{J}(R)$ invertierbar und $J = 0$. Ist R nullteilerfrei, so gilt ebenfalls $J = 0$, denn $a \neq 1$. □

Definition III.1.28. Sei R kommutativ und $P \trianglelefteq R$ ein Primideal. Die *Höhe* $h(P) \in \mathbb{N}_0$ von P ist die maximale Länge l einer Kette von Primidealen $P = P_0 \supsetneq P_1 \supsetneq \ldots \supsetneq P_l$. Gibt es beliebig lange solche Ketten, so sei $h(P) = \infty$. Schließlich sei

$$\dim R := \sup\big\{h(P) : P \trianglelefteq R \text{ Primideal}\big\}$$

die *Krull-Dimension* von R.

Beispiel III.1.29.

(i) Ein Integritätsbereich R hat Krull-Dimension 0 genau dann, wenn R ein Körper ist. Andererseits hat auch der lokale Ring $\mathbb{Z}/4\mathbb{Z}$ Krull-Dimension 0.

(ii) Jeder Dedekindring, der kein Körper ist, hat Krull-Dimension 1, denn die nicht-trivialen Primideale sind maximal.

(iii) Die Folge von Primidealen $(0) \subsetneq (X_1) \subsetneq (X_1, X_2) \subsetneq \ldots \subsetneq (X_1, \ldots, X_n)$ in $R := K[X_1, \ldots, X_n]$ zeigt $\dim R \geq n$. Wir werden zeigen, dass Gleichheit gilt. Wegen $(0) \subsetneq (X) \subsetneq (X, 2)$ ist andererseits $\dim \mathbb{Z}[X] \geq 2$.

Lemma III.1.30. *Sei R kommutativ und noethersch. Für jedes maximale Ideal $P \trianglelefteq R$ und $n \in \mathbb{N}$ ist R/P^n ein artinscher R-Modul.*

Beweis. Induktion nach n: Wegen $R/P^{n-1} \simeq (R/P^n)/(P^{n-1}/P^n)$ genügt es nach Lemma II.7.6 zu zeigen, dass der R-Modul $M := P^{n-1}/P^n$ artinsch ist (wobei $P^0 := R$). Wegen $PM = 0$ kann man M als Vektorraum über dem Körper R/P auffassen (vgl. Beweis von Satz II.9.7). Die Untermoduln entsprechen den Unterräumen. Da R noethersch ist, sind P^{n-1} und M endlich erzeugte R-Moduln. Somit ist M endlich-dimensional und die Behauptung folgt. □

Lemma III.1.31. *Sei R kommutativ, noethersch und lokal. Sei $a \in \mathrm{J}(R)$, sodass R/Ra ein artinscher R-Modul ist. Dann existiert höchstens ein Primideal, welches a nicht enthält.*

Beweis. Sei $P \trianglelefteq R$ ein Primideal mit $a \notin P$. Für $n \in \mathbb{N}$ sei

$$P_n := \{r \in R : \exists s \in R \setminus P : rs \in P^n\} = \Phi^{-1}((R_P P)^n) \trianglelefteq R$$

wie in Satz III.1.9. Da P ein Primideal ist, gilt $P = P_1 \supseteq P_2 \supseteq \ldots$. Sei $Q := P \cap Ra \trianglelefteq R$. Da $P/Q \simeq (P + Ra)/Ra \subseteq R/Ra$ artinisch ist, wird die Folge

$$(P_1 + Q)/Q \supseteq (P_2 + Q)/Q \supseteq \ldots$$

stationär. Sei $n \in \mathbb{N}$ mit $P_m + Q = P_{m+1} + Q$ für alle $m \geq n$. Mit $P_n \trianglelefteq R$ ist auch $M := P_n/P_m$ ein endlich erzeugter R-Modul. Für $x \in P_n \subseteq P_m + Q \subseteq P_m + Ra$ existieren $y \in P_m$ und $r \in R$ mit $x = y + ra$. Wegen $ra = x - y \in P_n$ existiert $s \in R \setminus P$ mit $ras \in P^n$. Aus $a \notin P$ folgt $r \in P_n$. Dies zeigt $a(r + P_m) = x + P_m$ und $aM = M$. Da $a \in \mathrm{J}(R)$, gilt $\mathrm{J}(R)M = M$. Nach Lemma III.1.26 existiert $b \in \mathrm{J}(R)$ mit $(1 - b)M = 0$. Da R lokal ist, gilt $1 - b \in R^\times$ und $M = 0$, d. h. $P_n = P_m$ für $m \geq n$.

Krulls Durchschnittsatz angewendet auf den lokalen Ring R_P zeigt $\bigcap_{m \geq 1} (R_P P)^m = 0$. Es folgt $P_n = \bigcap_{m \geq n} P_m = \Phi^{-1}(0)$ und $P \subseteq \sqrt{P_n} = \sqrt{\Phi^{-1}(0)}$. Sei umgekehrt $x \in \sqrt{P_n}$ und $x^k \in P_n$. Dann existiert $s \in R \setminus P$ mit $x^k s \in P^n \subseteq P$. Da P ein Primideal ist, gilt $x \in P$. Daher ist $P = \sqrt{\Phi^{-1}(0)}$ eindeutig bestimmt. □

Satz III.1.32 (Krulls Hauptidealsatz)**.** *Sei R kommutativ und noethersch. Sei $I \trianglelefteq R$ ein Hauptideal und $P \trianglelefteq R$ ein minimales Primideal über I. Dann gilt $h(P) \leq 1$.*

Beweis. Sei $I = Ra$. Sei zunächst R lokal und $P = \mathrm{J}(R)$. Dann ist P das einzige Primideal, welches a enthält. Nach Satz III.1.15 ist $\sqrt{I} = P$. Nach Lemma III.1.14 ist $P^n \subseteq I$ für ein $n \in \mathbb{N}$. Nach Lemma III.1.30 und Lemma II.7.6 ist $R/I \simeq (R/P^n)/(I/P^n)$ ein artinscher R-Modul. Nach Lemma III.1.31 gibt es neben P höchstens ein weiteres Primideal. Insbesondere ist $h(P) \leq 1$.

Sei nun R beliebig (kommutativ und noethersch). Nach Satz III.1.10 und Satz III.1.12 ist R_P noethersch und lokal. Nach Satz III.1.9 ist $R_P P$ ein minimales Primideal über $(\Phi(I)) = R_P a$. Der erste Teil des Beweises zeigt, dass die Aussage in R_P gilt. Mit Satz III.1.9 gilt sie auch in R. □

Lemma III.1.33 (Primvermeidung[1]). *Sei R kommutativ, $I \trianglelefteq R$ und $P_1, \ldots, P_n \trianglelefteq R$ Primideale mit $I \subseteq P_1 \cup \ldots \cup P_n$. Dann gilt $I \subseteq P_i$ für ein $i \in \{1, \ldots, n\}$.*

Beweis. Sei $n > 1$ minimal. Dann existieren $x_i \in I \setminus \bigcup_{j \neq i} P_j \subseteq P_i$. Betrachte $y := x_1 + x_2 \ldots x_n \in I$. Wegen $x_1 \notin P_i$ für $i > 1$ ist $y \in P_1$ und daher auch $x_2 \ldots x_n \in P_1$. Da P_1 ein Primideal ist, folgt $x_i \in P_1$ für ein $i > 1$. Widerspruch. □

Bemerkung III.1.34. Sei R noethersch und $I \trianglelefteq R$. Nach Lemma II.7.6 ist der R-Modul R/I noethersch. Damit ist jeder Untermodul von R/I auch als R/I-Modul endlich erzeugt, d. h. der reguläre R/I-Modul ist noethersch. Also ist R/I als Ring noethersch. Dieses Argument wird im Folgenden mehrfach benutzt.

Lemma III.1.35. *Sei R kommutativ und noethersch. Seien $P_0, \ldots, P_n, Q_1, \ldots, Q_m \trianglelefteq R$ Primideale mit $P_0 \subsetneq \ldots \subsetneq P_n \nsubseteq Q_1 \cup \ldots \cup Q_m$. Dann existieren Primideale $P_1', \ldots, P_{n-1}' \nsubseteq Q_1 \cup \ldots \cup Q_m$ mit $P_0 \subsetneq P_1' \subsetneq \ldots \subsetneq P_{n-1}' \subsetneq P_n$.*

Beweis. Induktion nach n: Im Fall $n \leq 1$ ist nichts zu tun. Sei $n \geq 2$ und $P_2', \ldots, P_{n-1}' \nsubseteq Q_1 \cup \ldots \cup Q_m$ mit $P_1 \subsetneq P_2' \subsetneq \ldots \subsetneq P_{n-1}' \subsetneq P_n$ bereits konstruiert. Nach Lemma III.1.33 gilt $P_2' \nsubseteq P_1 \cup Q_1 \cup \ldots \cup Q_m$. Sei $x \in P_2' \setminus (P_1 \cup Q_1 \cup \ldots \cup Q_m)$. Nach Satz III.1.24 existiert ein minimales Primideal P_1' über $Rx + P_0$ mit $P_1' \subseteq P_2'$. Offenbar gilt $P_0 \subsetneq P_1'$ und $P_1' \nsubseteq Q_1 \cup \ldots \cup Q_m$.

Zum Nachweis von $P_1' \neq P_2'$ gehen wir zum noetherschen Ring $\overline{R} := R/P_0$ über (Bemerkung III.1.34). Wegen $P_0 \subsetneq P_1 \subsetneq P_2'$ hat P_2'/P_0 in $\overline{R}$ mindestens Höhe 2. Andererseits ist P_1'/P_0 minimal über dem Hauptideal $(Rx + P_0)/P_0$. Krulls Haupidealsatz zeigt $h(P_1'/P_0) \leq 1$ und es folgt $P_1' \neq P_2'$. □

Satz III.1.36 (Krulls Höhensatz). *Sei R kommutativ und noethersch. Seien $x_1, \ldots, x_n \in R$ und $P \trianglelefteq R$ ein minimales Primideal über $(x_1, \ldots, x_m)$. Dann gilt $h(P) \leq n$. Insbesondere hat jedes Primideal in R endliche Höhe.*

Beweis. Induktion nach n: Nach dem Hauptidealsatz dürfen wir $n \geq 2$ voraussetzen. Sei $I := (x_1, \ldots, x_{n-1})$. Ist P minimal über I, so gilt $h(P) \leq n - 1$ nach Induktion. Nehmen wir also das Gegenteil an. Nach Satz III.1.24 existieren nur endlich viele Primideale $Q_1, \ldots, Q_m$ minimal über I. Nach Lemma III.1.33 ist $P \nsubseteq Q_1 \cup \ldots \cup Q_m$. Seien $P = P_0 \supsetneq P_1 \supsetneq \ldots \supsetneq P_h$ Primideale. Nach Lemma III.1.35 können wir $P_{h-1} \nsubseteq Q_1 \cup \ldots \cup Q_m$ annehmen. Im noetherschen Ring $\overline{R} := R/I$ (Bemerkung III.1.34) sind die Primideale $Q_1/I, \ldots, Q_m/I$ minimal, aber P/I nicht. Andererseits ist P/I minimal über dem Hauptideal $(x_1, \ldots, x_n)/I \simeq Rx_n/(Rx_n \cap I)$. Nach dem Hauptidealsatz gilt $h(P/I) = 1$. Sei Q ein Primideal mit $P \supseteq Q \supsetneq P_{h-1} + I$. Dann ist $Q \nsubseteq Q_1 \cup \ldots \cup Q_m$ und Q kann nicht minimal über I sein. Dies zeigt $h(Q/I) \geq 1$ und $Q = P$. Daher ist P/P_{h-1} minimal über $(P_{h-1} + I)/P_{h-1} \simeq I/(I \cap P_{h-1})$. Nach Induktion gilt $h - 1 \leq h(P/P_{h-1}) \leq n - 1$, also $h \leq n$.

Die zweite Behauptung folgt, da P als Ideal eines noetherschen Rings endlich erzeugt ist. □

Bemerkung III.1.37. Obwohl noethersche Ringe in der Regel nicht artinsch sind, zeigt Satz III.1.36, dass absteigende Ketten von Primidealen stationär werden müssen. Die Länge solcher Ketten ist allerdings nicht beschränkt, d. h. es gibt noethersche Ringe mit unendlicher Krull-Dimension (Beispiel von Nagata).

[1] im Original *prime avoidance* genannt

Lemma III.1.38. *Sei R ein noetherscher Integritätsbereich und $P \trianglelefteq R[X]$ ein Primideal mit $P \cap R = 0$. Dann gilt $h(P) \leq 1$.*

Beweis. Sei $S := R \setminus \{0\}$ multiplikativ abgeschlossen, $Q = Q(R) = R[S^{-1}]$ der Quotientenkörper von R und $\hat{R} := R[X][S^{-1}]$ die Lokalisierung von $R[X]$ nach S. Nach der universellen Eigenschaft lässt sich die Einbettung $R[X] \hookrightarrow Q[X]$ zu einem Homomorphismus $\hat{\varphi}\colon \hat{R} \to Q[X]$, $\frac{\alpha}{s} \mapsto \frac{\alpha}{s}$ fortsetzen ($\alpha \in R[X]$, $s \in S$). Es gilt $\frac{\alpha}{s} = 0$ in $Q[X]$ genau dann, wenn $\alpha = 0$ in $R[S]$. Also ist $\hat{\varphi}$ injektiv. Da sich jedes Polynom in $Q[X]$ in der Form $\frac{\alpha}{s}$ mit $\alpha \in R[X]$ und $s \in S$ (Hauptnenner der Koeffizienten) schreiben lässt, ist $\hat{\varphi}$ ein Isomorphismus.[2] Insbesondere ist $\hat{R}$ ein Hauptidealring. Sei $0 \neq P' \trianglelefteq R[X]$ ein Primideal mit $P' \subseteq P$. Es gilt $P' \cap S \subseteq P \cap R \cap S = \{0\} \cap S = \varnothing$. Nach Satz III.1.9 sind $(\Phi(P')) \subseteq (\Phi(P))$ nicht-triviale Primideale im Hauptidealring $\hat{R}$. Aus Lemma II.5.18 folgt $(\Phi(P')) = (\Phi(P))$ und $P' = P$ nach Satz III.1.9. Dies zeigt $h(P) \leq 1$. □

Satz III.1.39. *Für jeden noetherschen Integritätsbereich R gilt* $\boxed{\dim R[X] = 1 + \dim R.}$

Beweis. Da R ein Integritätsbereich ist, ist $(X) \trianglelefteq R[X]$ ein Primideal. Jede Kette von Primidealen in $R[X]/(X) \cong R$ entspricht einer Kette von Primidealen in $R[X]$, die man durch (0) verlängern kann. Dies zeigt $\dim R[X] \geq 1 + \dim R$. Insbesondere können wir $n := \dim R < \infty$ annehmen und durch Induktion nach n argumentieren. Im Fall $n = 0$ ist R ein Körper und $R[X]$ ein Hauptidealring mit Krull-Dimension 1. Sei daher $n \geq 1$ und $P_0 \supsetneq \ldots \supsetneq P_m = (0)$ eine Kette von Primidealen in $R[X]$. Es genügt $m \leq n + 1$ zu zeigen. O. B. d. A. sei $m \geq 2$.

Angenommen es gilt $P_{m-1} \cap R = 0$. Aus Lemma III.1.38 folgt dann $P_{m-2} \cap R \neq 0$. Sei $0 \neq x \in P_{m-2} \cap R$. Wegen $h(P_{m-2}) \geq 2$ kann P_{m-2} nach dem Hauptidealsatz nicht minimal über Rx liegen. Sei $Q \trianglelefteq R$ ein minimales Primideal über Rx mit $Q \subsetneq P_{m-2}$. Wir können P_{m-1} durch Q ersetzen und ab jetzt $I := P_{m-1} \cap R \neq 0$ annehmen. Da $I \trianglelefteq R$ ein Primideal ist, ist $\overline{R} := R/I$ ein noetherscher Integritätsbereich. Wie üblich folgt $\dim \overline{R} \leq \dim(R) - 1 = n - 1$. Nach Induktion gilt $\dim \overline{R}[X] \leq n$. Der kanonische Epimorphismus $R \to \overline{R}$ setzt sich zu einem Epimorphismus $\mu\colon R[X] \to \overline{R}[X]$ fort. Für $P := \operatorname{Ker}(\mu) \trianglelefteq R[X]$ gilt daher $\dim(R[X]/P) = \dim \overline{R}[X] \leq n$. Da P aus den Polynomen mit Koeffizienten in $I \subseteq P_{m-1}$ besteht, ergibt sich $P \subseteq R[X]I \subseteq P_{m-1}$. Die Kette von Primidealen $P_0/P \supsetneq \ldots \supsetneq P_{m-1}/P$ zeigt $m - 1 \leq \dim(R[X]/P) \leq n$, also $m \leq n + 1$. □

Folgerung III.1.40. *Für jeden Körper K gilt* $\dim K[X_1, \ldots, X_n] = n$.

[2] Informell ausgedrückt: $R[X][S^{-1}] = R[X, S^{-1}] = R[S^{-1}][X] = Q[X]$.

2 Algebraische Geometrie

Bemerkung III.2.1. In der linearen Algebra untersucht man die Lösungsmengen linearer Gleichungssysteme. Mit der Hauptachsentransformation lassen sich auch die Lösungen einer einzelnen quadratischen Gleichung beschreiben (man erhält Kegelschnitte im $\mathbb{R}^2$ bzw. Quadriken im $\mathbb{R}^n$). In der algebraischen Geometrie interessiert man sich allgemeiner für die Lösungsmengen von Systemen von Polynomgleichungen. Fermats letzter Satz fragt beispielsweise nach den rationalen Lösungen der Gleichung $X^n+Y^n = Z^n$ für $n \geq 3$. Da die Theorie bereits für eine Variable kompliziert ist (siehe Kapitel I.14), beschränken wir uns auf algebraisch abgeschlossene Körper. Wir bringen die besagten Lösungsmengen mit Radikalidealen im Polynomring in Verbindung, um einen Dimensionsbegriff mit Hilfe der Krullschen Sätze einzuführen.

Satz III.2.2 (Zariskis Lemma)**.** *Sei $K \subseteq L$ eine Körpererweiterung. Existiert ein Ringepimorphismus $K[X_1, \ldots, X_n] \to L$, so ist $|L : K| < \infty$.*

Beweis. Sei $x_i \in L$ das Bild von X_i unter den gegebenen Epimorphismus. Nehmen wir an, dass eine Transzendenzbasis $B \neq \varnothing$ von L über K existiert. Sei $b \in B$. Indem man K durch $K(B \setminus \{b\})$ ersetzt, kann man $B = \{b\}$ annehmen. Da $K(b) \subseteq L$ algebraisch ist, existiert

$$m := \max_{1 \leq i \leq n} |K(x_i, b) : K(b)|.$$

Also ist jedes Element aus L eine $K(b)$-Linearkombination der Elemente $x_1^{k_1} \ldots x_n^{k_n}$ mit $0 \leq k_1, \ldots, k_n \leq m$. Insbesondere ist $d := |L : K(b)| < \infty$. Sei $e_1, \ldots, e_d \in L$ eine $K(b)$-Basis von L. Für $1 \leq i, j \leq d$ und $1 \leq s \leq n$ sei

$$e_i e_j = \sum_{k=1}^{d} \frac{\alpha_{ijk}(b)}{\beta_{ijk}(b)} e_k \qquad\qquad x_s = \sum_{t=1}^{d} \frac{\gamma_{st}(b)}{\delta_{st}(b)} e_t$$

mit $\alpha_{ijk}, \beta_{ijk}, \gamma_{st}, \delta_{st} \in K[X]$. Jedes $a \in L$ ist eine K-Linearkombination von Produkten der x_i. Nach Ausmultiplizieren ist a eine $K(b)$-Linearkombination der e_i, wobei die Nenner der Koeffizienten Produkte der $\delta_{st}(b)$ und $\beta_{ijk}(b)$ sind. Insbesondere können nur endlich viele irreduzible Polynome aus $K[X]$ als Faktoren dieser Nenner auftreten. Da $K[X]$ aber unendlich viele irreduzible Polynome besitzt (für $|K| = \infty$ nehme man $X + a$ mit $a \in K$ und für $|K| < \infty$ benutze man Bemerkung I.11.16), können die e_i nicht linear unabhängig sein. Dieser Widerspruch zeigt $B = \varnothing$ und $K \subseteq L$ ist algebraisch. Wie oben ist dann $|L : K| < \infty$. □

Bemerkung III.2.3. Die Bedingung in Satz III.2.2 bedeutet, dass L als K-Algebra endlich erzeugt ist. Beachte: $K[X]$ ist als K-Algebra endlich erzeugt, aber nicht endlich-dimensional (vgl. Satz III.2.24).

Folgerung III.2.4 (Schwacher Nullstellensatz)**.** *Sei K ein algebraisch abgeschlossener Körper und $I \lhd K[X_1, \ldots, X_n]$. Dann existieren $x_1, \ldots, x_n \in K$ mit $\alpha(x_1, \ldots, x_n) = 0$ für alle $\alpha \in I$.*

Beweis. Nach Krulls Satz II.2.7 können wir annehmen, dass I maximal ist. Nach Satz I.7.12 ist $L := K[X_1, \dots, X_n]/I$ eine Körpererweiterung von $(K + I)/I \cong K/(K \cap I) \cong K$. Nach Satz III.2.2 ist $|L : K| < \infty$. Da K algebraisch abgeschlossen ist, gilt sogar $|L : K| = 1$ und $K[X_1, \dots, X_n] = K + I$. Für $i = 1, \dots, n$ sei $x_i \in K$ mit $X_i - x_i \in I$. Dann ist $J := (X_1 - x_1, \dots, X_n - x_n) \subseteq I$. Wegen $K[X_1, \dots, X_n]/J \cong K$ ist auch J maximal und es folgt $I = J$. Dies zeigt die Behauptung. □

Definition III.2.5. Sei K ein algebraisch abgeschlossener Körper und $R := K[X_1, \dots, X_n]$. Für $P \subseteq R$ und $A \subseteq K^n$ sei

$$\mathcal{V}(P) := \big\{(x_1, \dots, x_n) \in K^n : \forall \alpha \in P : \alpha(x_1, \dots, x_n) = 0\big\},$$
$$\mathcal{I}(A) := \big\{\alpha \in R : \forall (x_1, \dots, x_n) \in A : \alpha(x_1, \dots, x_n) = 0\big\}.$$

Die Mengen der Form $\mathcal{V}(P)$ für $P \subseteq R$ nennt man (*affine*) *Varietäten*. Sei $\mathrm{A}(K^n)$ die Menge aller Varietäten von K^n.

Bemerkung III.2.6.

(i) Die folgenden Ergebnisse über Varietäten beziehen sich stets auf algebraisch abgeschlossene Körper.

(ii) Für $P \subseteq R$ gilt $\mathcal{V}(P) = \mathcal{V}((P)) = \mathcal{V}(\sqrt{(P)})$. Jede Varietät hat also die Form $\mathcal{V}(I)$ für ein Radikalideal I. Nach Hilberts Basissatz existieren außerdem Polynome $\alpha_1, \dots, \alpha_k \in R$ mit $I = (\alpha_1, \dots, \alpha_k)$. Wir setzen $\mathcal{V}(\alpha_1, \dots, \alpha_k) := \mathcal{V}(I)$.

Beispiel III.2.7. Besteht P aus linearen Polynomen in $X_1, \dots, X_n$ (d. h. $\deg \alpha \leq 1$ für alle $\alpha \in P$), so ist $\mathcal{V}(P)$ die Lösungsmenge eines linearen Gleichungssystems. Im Fall $\mathcal{V}(P) \neq \varnothing$ ist $\mathcal{V}(P)$ dann ein affiner Unterraum, also von der Form $x + U$ mit $x \in K^n$ und $U \leq K^n$.

Lemma III.2.8. *Für $P, Q, P_i \trianglelefteq R := K[X_1, \dots, X_n]$ gilt*

(i) $\mathcal{V}(\varnothing) = K^n$, $\mathcal{V}(R) = \varnothing$.

(ii) $\bigcap_{i \in I} \mathcal{V}(P_i) = \mathcal{V}(\bigcup_{i \in I} P_i) = \mathcal{V}(\sum_{i \in I} P_i)$.

(iii) $P \subseteq Q \Rightarrow \mathcal{V}(Q) \subseteq \mathcal{V}(P)$.

(iv) $\mathcal{V}(P) \cup \mathcal{V}(Q) = \mathcal{V}(P \cap Q)$.

Beweis. Alle Aussagen bis auf $\mathcal{V}(P \cap Q) \subseteq \mathcal{V}(P) \cup \mathcal{V}(Q)$ sind trivial. Sei $x \in K^n \setminus (\mathcal{V}(P) \cup \mathcal{V}(Q))$. Dann existieren $\alpha \in P$ und $\beta \in Q$ mit $\alpha(x) \neq 0 \neq \beta(x)$. Dann ist $(\alpha\beta)(x) \neq 0$ und $\alpha\beta \in PQ \subseteq P \cap Q$. Dies zeigt $x \notin \mathcal{V}(P \cap Q)$. □

Bemerkung III.2.9. Nach Lemma III.2.8 erhält man eine Topologie auf K^n, indem man für die abgeschlossenen Mengen die Varietäten wählt (die offenen Mengen sind die Komplemente von abgeschlossenen Mengen). Sie heißt *Zariski-Topologie*. Für eine beliebige Teilmenge $M \subseteq K^n$ nennt man $\overline{M} := \mathcal{V}(\mathcal{I}(M)) \in \mathrm{A}(K^n)$ den *Zariski-Abschluss* von M in K^n.

Beispiel III.2.10. Nach Beispiel III.2.7 sind die einelementigen Teilmengen von K^n abgeschlossen bzgl. der Zariski-Topologie und somit auch alle endlichen Teilmengen. Im Fall $R = K[X]$ hat jedes nicht-triviale Ideal die Form (α) mit $\alpha \neq 0$. Da α nur endlich viele Nullstellen besitzt, sind hier alle Varietäten außer K endlich.

Satz III.2.11 (HILBERTs Nullstellensatz)**.** *Die Abbildungen $\mathcal{V}$ und $\mathcal{I}$ sind zueinander inverse Bijektionen zwischen der Menge der Radikalideale von $K[X_1, \ldots, X_n]$ und $\mathrm{A}(K^n)$.*

Beweis (RABINOWITSCH). Für ein Radikalideal $I \trianglelefteq R := K[X_1, \ldots, X_n]$ und $A \in \mathrm{A}(K^n)$ gilt $I \subseteq \mathcal{I}(\mathcal{V}(I))$ und $A \subseteq \mathcal{V}(\mathcal{I}(A))$ nach Definition. Eine Anwendung von $\mathcal{V}$ auf die erste Inklusion ergibt $\mathcal{V}(\mathcal{I}(\mathcal{V}(I))) \subseteq \mathcal{V}(I)$. Speziell für $A = \mathcal{V}(I)$ folgt $\mathcal{V}(\mathcal{I}(A)) \subseteq A$. Also ist $\mathcal{V}(\mathcal{I}(A)) = A$.

Sei nun $\alpha \in \mathcal{I}(\mathcal{V}(I)) \setminus \{0\}$ und $\widehat{I} := (I, \alpha Y - 1) \trianglelefteq R[Y]$. Angenommen es existiert $(x_1, \ldots, x_n, y) \in \mathcal{V}(\widehat{I})$. Dann ist $(x_1, \ldots, x_n) \in \mathcal{V}(I)$ und man erhält den Widerspruch

$$(\alpha Y - 1)(x_1, \ldots, x_n, y) = \alpha(x_1, \ldots, x_n)y - 1 = -1 \neq 0.$$

Also ist $\mathcal{V}(\widehat{I}) = \varnothing$ und der schwache Nullstellensatz impliziert $\widehat{I} = R[Y]$. Daher existieren $\beta_1, \ldots, \beta_k, \gamma \in R[Y]$ und $\alpha_1, \ldots, \alpha_k \in I$ mit

$$\beta_1\alpha_1 + \ldots + \beta_k\alpha_k + \gamma(\alpha Y - 1) = 1.$$

Indem wir Y durch α^{-1} substituieren, erhalten wir

$$\sum_{i=1}^{k} \beta_1(X_1, \ldots, X_n, \alpha^{-1})\alpha_i = 1 \in K(X_1, \ldots, X_n)$$

Multipliziert man mit einer genügend hohen Potenz α^m, so folgt $\alpha^m \in I$ und $\alpha \in \sqrt{I} = I$. □

Bemerkung III.2.12. In der Situation von Satz III.2.11 korrespondieren die maximalen Ideale in R mit den einelementigen Varietäten, also mit den Elementen von K^n (vgl. Beweis von Folgerung III.2.4).

Definition III.2.13. Eine Varietät $A \in \mathrm{A}(K^n)$ heißt *reduzibel*, falls $B, C \in \mathrm{A}(K^n)$ mit $A = B \cup C$ und $B, C \subsetneq A$ existieren. Eine nicht-leere Varietät heißt *irreduzibel*, wenn sie nicht reduzibel ist.

Lemma III.2.14. *Genau dann ist $A \in \mathrm{A}(K^n)$ irreduzibel, wenn $\mathcal{I}(A)$ ein Primideal ist.*

Beweis. Sei $A = B \cup C$ reduzibel mit Varietäten $B, C \subsetneq A$. Dann gilt $\mathcal{I}(B), \mathcal{I}(C) \nsubseteq \mathcal{I}(A)$, aber $\mathcal{I}(B)\mathcal{I}(C) \subseteq \mathcal{I}(A)$. Folglich ist $\mathcal{I}(A)$ kein Primideal. Ist umgekehrt $\mathcal{I}(A)$ kein Primideal, so existieren $\alpha, \beta \in R \setminus \mathcal{I}(A)$ mit $\alpha\beta \in \mathcal{I}(A)$. Für $B := \mathcal{V}((\mathcal{I}(A), \alpha))$ und $C := \mathcal{V}((\mathcal{I}(A), \beta))$ gilt $A = B \cup C$ und $B, C \subsetneq A$. □

Bemerkung III.2.15. Sei $\varnothing \neq \mathcal{A} \subseteq \mathrm{A}(K^n)$. Da R noethersch ist, besitzt die Menge $\{\mathcal{I}(A) : A \in \mathcal{A}\}$ ein maximales Element, sagen wir $\mathcal{I}(A)$ mit $A \in \mathcal{A}$. Offenbar ist A nun ein minimales Element von $\mathcal{A}$.

Satz III.2.16. *Für jede Varietät $A \in \mathrm{A}(K^n)$ existieren (bis auf die Reihenfolge) eindeutig bestimmte irreduzible Varietäten $A_1, \ldots, A_k$ mit $A = A_1 \cup \ldots \cup A_k$ und $A_i \nsubseteq A_j$ für alle $i \neq j$.*

Beweis. Sei $\mathcal{A} \subseteq \mathrm{A}(K^n)$ die Menge der Varietäten, die keine solche Zerlegung besitzen. Nehmen wir $\mathcal{A} \neq \varnothing$ an. Nach Bemerkung III.2.15 besitzt $\mathcal{A}$ ein minimales Element A. Da A keine Zerlegung besitzt, ist A reduzibel, sagen wir $A = B \cup C$. Wegen $B, C \subsetneq A$ gilt $B, C \notin \mathcal{A}$, d. h. B und C lassen sich in der gewünschten Form zerlegen. Dann lässt sich aber auch $B \cup C = A$ zerlegen. Dieser Widerspruch zeigt $\mathcal{A} = \varnothing$.

Zum Nachweis der Eindeutigkeit gehen wir von zwei Zerlegungen $A = B_1 \cup \ldots \cup B_k = C_1 \cup \ldots \cup C_l$ aus. Für $1 \leq i \leq k$ gilt $B_i = B_i \cap A = (B_i \cap C_1) \cup \ldots \cup (B_i \cap C_l)$. Da B_i irreduzibel ist, gilt $B_i \subseteq C_j$ für ein $1 \leq j \leq l$. Analog existiert $1 \leq s \leq k$ mit $C_j \subseteq B_s$. Aus $B_i \subseteq B_s$ folgt $i = s$ und $B_i = C_j$. □

Bemerkung III.2.17. In der Situation von Satz III.2.16 nennt man $A_1, \ldots, A_k$ die (*irreduziblen*) *Komponenten* von A. Die Eindeutigkeit der Komponenten zeigt, dass $\mathcal{I}(A) = \mathcal{I}(A_1) \cap \ldots \cap \mathcal{I}(A_k)$ eine Primärzerlegung von $\mathcal{I}(A)$ ist, wobei die Primideale $\mathcal{I}(A_i) = \sqrt{\mathcal{I}(A_i)}$ zu $\mathcal{I}(A)$ assoziiert sind. Nach Satz III.1.24 und Bemerkung III.1.25 sind $\mathcal{I}(A_1), \ldots, \mathcal{I}(A_k)$ genau die minimalen Primideale über $\mathcal{I}(A)$.

Beispiel III.2.18.

(i) Die Komponenten einer endlichen Varietät sind nach Beispiel III.2.10 einelementig.

(ii) Sei $\alpha \in K[X_1, \ldots, X_n] \setminus K$ mit Primfaktorzerlegung $\alpha = \alpha_1^{e_1} \ldots \alpha_k^{e_k}$. Dann sind $\mathcal{V}(\alpha_1), \ldots, \mathcal{V}(\alpha_k)$ die Komponenten von $\mathcal{V}(\alpha)$ nach Beispiel III.1.23.

(iii) Sei $I := (X^2 - YZ, XZ - X) \trianglelefteq K[X, Y, Z]$ und $A = \mathcal{V}(I) \in \mathrm{A}(K^3)$. Wegen $XZ - X = X(Z - 1)$ gilt

$$\begin{aligned} I &= (X^2 - YZ, X) \cap (X^2 - YZ, Z - 1) = (YZ, X) \cap (X^2 - Y, Z - 1) \\ &= (X, Y) \cap (X, Z) \cap (X^2 - Y, Z - 1). \end{aligned}$$

Dabei sind (X, Y) und (X, Z) Primideale und $K[X, Y, Z]/(X^2 - Y, Z - 1) \cong K[X, Y]/(X^2 - Y)$. Da $X^2 - Y$ irreduzibel ist (Ansatz: $X^2 - Y = (X + aY + b)(X + cY + d)$), ist auch $(X^2 - Y, Z - 1)$ ein Primideal. Als Durchschnitt von Primidealen ist I ein Radikalideal (Bemerkung III.1.17). Offensichtlich gibt es keine Inklusionen unter den drei Primidealen. Die Komponenten von A sind daher

$$\begin{aligned} \mathcal{V}(X, Y) &= \{(0, 0, z) : z \in K\}, \\ \mathcal{V}(X, Z) &= \{(0, y, 0) : y \in K\}, \\ \mathcal{V}(X^2 - Y, Z - 1) &= \{(x, x^2, 1) : x \in K\}. \end{aligned}$$

Definition III.2.19. Für $A \in \mathrm{A}(K^n)$ nennt man

$$K[A] := K[X_1, \ldots, X_n]/\mathcal{I}(A)$$

den *Koordinatenring* von A. Man nennt $\dim A := \dim K[A]$ die *Dimension* von A ($\dim K[A]$ ist die Krull-Dimension). Zusätzlich setzt man $\dim \varnothing := -\infty$.

Bemerkung III.2.20.

(i) Aus Folgerung III.1.40 folgt $d := \dim A \leq n$ für jede Varietät $A \in \mathrm{A}(K^n)$. Sind $P_0/\mathcal{I}(A) \subsetneq \ldots \subsetneq P_d/\mathcal{I}(A)$ Primideale in $K[A]$, so sind $A \supseteq \mathcal{V}(P_0) \supsetneq \ldots \supsetneq \mathcal{V}(P_d)$ irreduzible Varietäten und umgekehrt. Man kann $\dim A$ daher auch als maximale Länge einer Kette von irreduziblen Varietäten in A definieren.

(ii) Seien $\alpha_1, \ldots, \alpha_k \in K[X_1, \ldots, X_n]$ lineare Polynome ohne Absolutglied. Dann ist $A = \mathcal{V}(\alpha_1, \ldots, \alpha_k)$ als Lösungsmenge eines homogenen Gleichungssystems ein Unterraum von K^n. O. B. d. A. seien $\alpha_1, \ldots, \alpha_k$ linear unabhängig (insbesondere $k \leq n$). Nach dem Gauß-Algorithmus können wir $\alpha_i = X_i + a_i X_{i+1} + \ldots$ für $i = 1, \ldots, k$ und $a_i \in K$ annehmen. Nun folgt leicht $K[A] \cong K[X_{k+1}, \ldots, X_n]$ und $\dim A = n - k$ nach Folgerung III.1.40. Daher stimmt $\dim A$ mit dem Dimensionsbegriff aus der linearen Algebra überein.

Lemma III.2.21. *Sind $A_1, \ldots, A_k$ die Komponenten von $A \in \mathrm{A}(K^n)$, so gilt*

$$\dim A = \max_{1 \le i \le k} \dim A_i.$$

Beweis. Sind $P_0/\mathcal{I}(A_i) \subsetneq \ldots \subsetneq P_h/\mathcal{I}(A_i)$ Primideale in $K[A_i]$, so sind $P_0/\mathcal{I}(A) \subsetneq \ldots \subsetneq P_h/\mathcal{I}(A)$ Primideale in $K[A]$. Dies zeigt $\dim A_i \le \dim A$ für $i = 1, \ldots, k$. Seien umgekehrt $P_0/\mathcal{I}(A) \subsetneq \ldots \subsetneq P_h/\mathcal{I}(A)$ Primideale in $K[A]$ mit $h = \dim A$. Dann ist P_0 minimal über $\mathcal{I}(A)$. Nach Bemerkung III.2.17 ist $P_0 = \mathcal{I}(A_i)$ für ein $1 \le i \le k$. Nun sind $P_0/\mathcal{I}(A_i) \subsetneq \ldots \subsetneq P_h/\mathcal{I}(A_i)$ Primideale in $K[A_i]$. Es folgt $\dim A = h \le \dim A_i$. □

Lemma III.2.22.

(i) Eine Varietät A ist genau dann endlich, wenn $\dim A \le 0$.

(ii) Für $I = (\alpha_1, \ldots, \alpha_k) \lhd K[X_1, \ldots, X_n]$ mit $k < n$ gilt $\dim \mathcal{V}(I) \ge 1$.

Beweis.

(i) O. B. d. A. sei $A \neq \varnothing$. Sei A endlich, o. B. d. A. $A = \{(x_1, \ldots, x_n)\}$ nach Lemma III.2.21 und Beispiel III.2.18. Dann ist $\mathcal{I}(A) = (X_1 - x_1, \ldots, X_n - x_n)$ und $K[A] \cong K$. Dies zeigt $\dim A = 0$. Sei umgekehrt $\dim A = 0$ und o. B. d. A. A irreduzibel. Dann ist $K[A]$ ein Körper (Beispiel III.1.29) und $\mathcal{I}(A)$ ein maximales Ideal. Bemerkung III.2.12 zeigt $|A| = 1$.

(ii) Sei $A := \mathcal{V}(I)$. Wegen $I \neq K[X_1, \ldots, X_n]$ ist $\dim A \ge 0$. Nehmen wir $\dim A = 0$ an. Sei $P \trianglelefteq K[X_1, \ldots, X_n]$ ein Primideal minimal über $\mathcal{I}(A) = \sqrt{I}$. Das Primideal $P/\sqrt{I} \trianglelefteq K[A]$ muss dann maximal sein. Damit ist auch P maximal in $K[X_1, \ldots, X_n]$. Bekanntlich hat P die Form $P = (X_1 - x_1, \ldots, X_n - x_n)$. Die Primideale $(0) \subsetneq (X_1 - x_1) \subsetneq (X_1 - x_1, X_2 - x_2) \ldots \subsetneq P$ zeigen $h(P) = n$. Sei Q ein Primideal mit $I \subseteq Q \subseteq P$. Wegen $\sqrt{I} \subseteq \sqrt{Q} = Q$ ist $Q = P$, d. h. P ist auch minimal über I. Krulls Höhensatz liefert den Widerspruch $h(P) \le k < n$. □

Bemerkung III.2.23.

(i) Sind die Polynome $\alpha_1, \ldots, \alpha_k$ in Lemma III.2.22 linear, so erhält man die bekannte Aussage, dass ein unterbestimmtes lineares Gleichungssystem entweder keine oder unendlich viele Lösungen besitzt (sofern $|K| = \infty$). Im Allgemeinen gilt Lemma III.2.22 allerdings nicht für beliebige (unendliche) Körper. Zum Beispiel besitzt $X^2 + Y^2 = 0$ nur die triviale Lösung $(0, 0)$ in $\mathbb{R}^2$.

(ii) Für $A \neq \varnothing$ kann man $K[A]$ als Vektorraum über

$$K \cong K/(K \cap \mathcal{I}(A)) \cong (K + \mathcal{I}(A))/\mathcal{I}(A) \subseteq K[A]$$

auffassen. Ist A irreduzibel, so ist $K[A]$ ein Integritätsbereich (Lemma III.2.14) mit Quotientenkörper $K(A) := Q(K[A])$. Wir zeigen in dieser Situation, dass $\dim A$ mit dem Transzendenzgrad von $K(A)$ über K übereinstimmt (Satz III.2.26).

(iii) Der folgende Satz gilt für beliebige Körper K und liefert Transzendenzbasen für Ringe.

Satz III.2.24 (NOETHER-Normalisierung)**.** *Sei K ein Körper und $K[X_1, \ldots, X_n] \to R$ ein Ringepimorphismus. Dann ist R als Modul über einem Teilring $S \cong K[Y_1, \ldots, Y_d]$ mit $d \le n$ endlich erzeugt.*

Beweis. Wir identifizieren K mit seinem Bild unter dem gegebenen Epimorphismus $\Phi\colon K[X_1,\dots,X_n]\to R$. Ist Φ injektiv, so gilt die Behauptung mit $d=n$ und $S=R$. Dies schließt den Fall $n=0$ ein. Sei also $n\geq 1$ und die Existenz von S für $n-1$ bereits bewiesen. Sei $x_i:=\Phi(X_i)\in R$ für $i=1,\dots,n$. Sei $\alpha\in\operatorname{Ker}(\Phi)\setminus\{0\}$ und $q:=1+\deg\alpha$. Wir substituieren X_i durch $X_i+X_n^{q^i}$ für $i=1,\dots,n-1$. Aus einem Monom $X_1^{a_1}\dots X_n^{a_n}$ in α wird dann

$$(X_1+X_n^q)^{a_1}\dots(X_{n-1}+X_n^{q^{n-1}})^{a_{n-1}}X_n^{a_n}=\ldots+X_n^{a_1q+\ldots+a_{n-1}q^{n-1}+a_n}.$$

Wegen $a_1,\dots,a_n<q$ ist $a_n+a_1q+\ldots+a_{n-1}q^{n-1}$ eine q-adische Entwicklung. Für verschiedene n-Tupel $(a_1,\dots,a_n)$ erhält man also verschiedene X_n-Potenzen. Insbesondere existiert genau eine solche Potenz X_n^e mit maximalem Exponenten e. Ist $c\in K^\times$ der entsprechende Koeffizient, so ist

$$\beta:=c^{-1}\alpha(X_1+X_n^q,\dots,X_{n-1}+X_n^{q^{n-1}},X_n)$$

normiert vom Grad e als Polynom in X_n. Sei $y_i:=x_i-x_n^{q^i}\in R$ für $i=1,\dots,n-1$ und $T:=K[y_1,\dots,y_{n-1}]\subseteq R$. Nach Induktion ist T über einem Teilring $S\cong K[Y_1,\dots,Y_d]$ mit $d\leq n-1$ endlich erzeugt. Außerdem ist $\gamma:=\beta(y_1,\dots,y_{n-1},X_n)\in T[X_n]$ normiert vom Grad e mit

$$\gamma(x_n)=c^{-1}\alpha(x_1,\dots,x_n)=c^{-1}\Phi(\alpha)=0.$$

Umstellen ergibt $x_n^e=\sum_{i=1}^{m-1}\gamma_ix_n^i$ mit $\gamma_1,\dots,\gamma_{d-1}\in T$. Nach Voraussetzung wird R als K-Vektorraum von den Monomen in $x_1,\dots,x_n$ erzeugt. Dabei dürfen wir $x_1,\dots,x_{n-1}$ durch $y_1,\dots,y_{n-1}$ ersetzen. Daher wird R als T-Modul von $1,x_n,\dots,x_n^{e-1}$ erzeugt. Somit ist R auch ein endlich erzeugter S-Modul. □

Definition III.2.25. In der Situation von Satz III.2.24 nennt man den Teilring $K[Y_1,\dots,Y_d]\cong S\subseteq R$ eine *Noether-Normalisierung* von R.

Satz III.2.26. *Ist $A\in\mathrm{A}(K^n)$ irreduzibel, so ist $\dim A$ der Transzendenzgrad von $K(A)$ über K.*

Beweis. Sei $K[Y_1,\dots,Y_d]\cong S\subseteq K[A]$ eine Noether-Normalisierung von $K[A]$. Nach Beispiel II.11.6 ist $S\subseteq K[A]$ eine ganze Ringerweiterung und Satz II.11.17 zeigt $\dim A=\dim K[A]=\dim S$. Nach Folgerung III.1.40 gilt $\dim S=d$. Sei jetzt $\alpha_1,\dots,\alpha_k$ ein Erzeugendensystem von $K[A]$ als S-Modul. Dann gilt $K(A)=Q(S)(\alpha_1,\dots,\alpha_k)$. Da $S\subseteq K[A]$ ganz ist, ist die Körpererweiterung $K(Y_1,\dots,Y_d)\cong Q(S)\subseteq K(A)$ algebraisch. Dies zeigt $\operatorname{trg}(K(A)|K)=d=\dim A$. □

Folgerung III.2.27. *Für $\alpha\in K[X_1,\dots,X_n]\setminus K$ gilt $\dim\mathcal{V}(\alpha)=n-1$.*

Beweis. Für die Primfaktorzerlegung $\alpha=\alpha_1^{e_1}\dots\alpha_k^{e_k}$ gilt $A:=\mathcal{V}(\alpha)=\mathcal{V}(\alpha_1)\cup\ldots\cup\mathcal{V}(\alpha_k)$. Wir können daher annehmen, dass α irreduzibel ist. Dann gilt $\mathcal{I}(A)=\sqrt{(\alpha)}=(\alpha)$. Sei $\overline{X_i}:=X_i+(\alpha)\in K(A)$ für $i=1,\dots,n$. Wegen $\alpha(\overline{X_1},\dots,\overline{X_n})=0$ sind $\overline{X_1},\dots,\overline{X_n}$ algebraisch abhängig über K. Aus dem Basisergänzungssatz II.4.12 folgt $\operatorname{trg}(K(A)|K)\leq n-1$. Für die umgekehrte Ungleichung können wir o. B. d. A. annehmen, dass X_n in α vorkommt. Angenommen es gibt ein $\beta\in K[X_1,\dots,X_{n-1}]$ mit $\beta(\overline{X_1},\dots,\overline{X_{n-1}})=0$ in $K(A)$. Dann folgt $\alpha\mid\beta$. Da X_n aber nicht in β vorkommt, muss $\beta=0$ gelten. Dies zeigt, dass $\overline{X_1},\dots,\overline{X_{n-1}}$ algebraisch unabhängig über K sind. □

Bemerkung III.2.28. Folgerung III.2.27 suggeriert die Bezeichnung *Hyperfläche* (als nicht-lineare Version der Hyperebene) für Varietäten der Form $\mathcal{V}(\alpha)$ mit $\alpha\in K[X_1,\dots,X_n]\setminus K$.

Beispiel III.2.29. Sei $A = \mathcal{V}(X^2 - YZ, XZ - X)$ wie in Beispiel III.2.18. Die Komponenten $\mathcal{V}(X, Y)$ und $\mathcal{V}(X, Z)$ haben offensichtlich Dimension 1. Für $A_3 := \mathcal{V}(X^2 - Y, Z - 1)$ gilt $K[A_3] \cong K[X, Y]/(X^2 - Y)$. Nach Folgerung III.2.27 ist A_3 eine Hyperfläche in K^2 und daher $\dim A = 1$ nach Lemma III.2.21.

Lemma III.2.30. *Sei $I \trianglelefteq K[X_1, \ldots, X_n]$ und $a_1, \ldots, a_d \in K^n \setminus \mathcal{V}(I)$. Dann existiert ein $\alpha \in I$ mit $\alpha(a_i) \neq 0$ für $i = 1, \ldots, d$.*

Beweis. Induktion nach d: Im Fall $d = 1$ ist die Behauptung trivial. Sei $d \geq 2$. Nach Induktion existieren $\alpha_i \in I$ mit $\alpha_i(a_j) \neq 0$ für $i \neq j$. O. B. d. A. sei $\alpha_i(a_i) = 0$ für $i = 1, \ldots, d$ (anderenfalls wähle $\alpha := \alpha_i$). Nun hat $\alpha := \alpha_1 + \alpha_2 \ldots \alpha_d$ die gewünschte Eigenschaft. □

Bemerkung III.2.31. Bekanntlich bestimmt die Diskriminante eines Polynoms $\alpha \in K[X]$, ob α eine mehrfache Nullstelle im algebraischen Abschluss von K besitzt. Wir definieren eine Invariante, die anzeigt, ob zwei beliebige Polynome eine gemeinsame Nullstelle (Teiler) besitzen.

Definition III.2.32. Sei R ein Integritätsbereich, $\alpha = \sum_{i=0}^{d} a_i X^i \in R[X]$ und $\beta = \sum_{i=0}^{e} b_i X^i \in R[X]$ mit $a_d \neq 0 \neq b_e$. Man nennt

$$S(\alpha, \beta) := \begin{pmatrix} a_0 & & & 0 & b_0 & & 0 \\ a_1 & \ddots & & & b_1 & \ddots & \\ \vdots & \ddots & \ddots & & \vdots & \ddots & b_0 \\ a_d & & \ddots & a_0 & \vdots & & b_1 \\ & \ddots & & a_1 & b_e & & \vdots \\ & & \ddots & \vdots & & \ddots & \vdots \\ 0 & & & a_d & 0 & & b_e \end{pmatrix} \in R^{(d+e)\times(d+e)}$$

die *Sylvester-Matrix* von α, β (falls $d + e > 0$). Ihre Determinante $\operatorname{res}(\alpha, \beta) := \det S(\alpha, \beta) \in R$ heißt *Resultante* von α, β.[1] Für $d = e = 0$ sei $\operatorname{res}(\alpha, \beta) := 1$. Außerdem sei $\operatorname{res}(0, \beta) = 0 = \operatorname{res}(\alpha, 0)$.

Beispiel III.2.33.

(i) Für $d = 0$ gilt $S(\alpha, \beta) = \operatorname{diag}(a_0, \ldots, a_0)$ und $\operatorname{res}(\alpha, \beta) = a_0^e$. Außerdem ist

$$\operatorname{res}(X - a, X - b) = \begin{vmatrix} -a & -b \\ 1 & 1 \end{vmatrix} = b - a.$$

(ii) Durch de Vertauschungen zweier benachbarter Spalten von $S(\alpha, \beta)$ erhält man $\operatorname{res}(\beta, \alpha) = (-1)^{de} \operatorname{res}(\alpha, \beta)$.

Satz III.2.34. *Sei R faktoriell und $\alpha, \beta \in R[X] \setminus \{0\}$. Genau dann ist* $\operatorname{ggT}(\alpha, \beta) \in R$, *wenn* $\operatorname{res}(\alpha, \beta) \neq 0$.

[1] Man verwechsele die Resultante nicht mit der (kubischen) Resolvente.

Beweis. Nach Gauß ist $R[X]$ faktoriell. Sei $d := \deg\alpha$ und $e := \deg\beta$. Sei $\delta \in R[X] \setminus R$ ein gemeinsamer Teiler von α, β. Dann gilt $\alpha\frac{\beta}{\delta} - \beta\frac{\alpha}{\delta} = 0$. Wir schreiben $\frac{\beta}{\delta} = \sum a'_i X^i$ und $-\frac{\alpha}{\delta} = \sum b'_i X^i$. Wegen $\deg\delta > 0$ gilt $a'_i = b'_j = 0$ für $i \geq e$ und $j \geq d$. Dies zeigt

$$\begin{aligned} a_0a'_0 + b_0b'_0 &= 0 \\ a_1a'_0 + a_0a'_1 + b_1b'_0 + b_0b'_1 &= 0 \\ &\vdots \\ a_da'_{e-1} + b_eb'_{d-1} &= 0. \end{aligned}$$

Daher ist $(a'_0, \ldots, a'_{e-1}, b'_0, \ldots, b'_{d-1})$ eine nicht-triviale Lösung des homogenen Gleichungssystems mit Koeffizientenmatrix $S(\alpha, \beta)$. Nach Übergang zu $Q(R)$ folgt $\operatorname{res}(\alpha, \beta) = 0$.

Ist umgekehrt $\operatorname{res}(\alpha, \beta) = 0$, so existiert eine nicht-triviale Lösung $(a'_0, \ldots, a'_{e-1}, b'_0, \ldots, b'_{d-1}) \in Q(R)^{d+e}$ des besagten Gleichungssystems. Nach Multiplikation mit einem gemeinsamen Nenner können wir $(a'_0, \ldots, a'_{e-1}, b'_0, \ldots, b'_{d-1}) \in R^{d+e}$ annehmen. Für $\tilde{\alpha} = \sum a'_i X^i$ und $\tilde{\beta} = \sum b'_i X^i$ gilt nun $\alpha\tilde{\alpha} + \beta\tilde{\beta} = 0$, also $\alpha\tilde{\alpha} = -\beta\tilde{\beta}$. Im Fall $\operatorname{ggT}(\alpha, \beta) \in R$ müsste jeder nicht-konstante Primteiler von α ein Teiler von $\tilde{\beta}$ sein. Dies ist wegen $\deg\tilde{\beta} < d$ aber ausgeschlossen. Damit ist $\operatorname{ggT}(\alpha, \beta) \notin R$ gezeigt. □

Bemerkung III.2.35.

(i) Ist R ein Körper, so bedeutet die Bedingung $\operatorname{ggT}(\alpha, \beta) \in R$, dass α und β teilerfremd sind.

(ii) Das nächste Ergebnis ist ein Ersatz für Bézouts Lemma.

Lemma III.2.36. *Sei R ein Integritätsbereich und $\alpha, \beta \in R[X] \setminus R$. Dann existieren $\gamma, \delta \in R[X]$ mit $\alpha\gamma + \beta\delta = \operatorname{res}(\alpha, \beta)$.*

Beweis. Wie bisher sei $d := \deg\alpha$ und $e := \deg\beta$. Nach Voraussetzung ist $d, e \geq 1$. Für $i = 2, \ldots, d+e$ addieren wir das X^{i-1}-fache der i-te Zeile der Sylvester-Matrix auf die erste (Gauß-Algorithmus):

$$\operatorname{res}(\alpha, \beta) = \begin{vmatrix} \alpha & X\alpha & \cdots & X^{e-1}\alpha & \beta & \cdots & X^{d-1}\beta \\ a_1 & \ddots & & & b_1 & \ddots & \\ \vdots & \ddots & \ddots & & \vdots & \ddots & b_0 \\ a_d & & \ddots & a_0 & \vdots & & b_1 \\ & \ddots & & a_1 & b_e & & \vdots \\ & & \ddots & \vdots & & \ddots & \vdots \\ & & & a_d & & & b_e \end{vmatrix}.$$

Laplace-Entwicklung nach der ersten Zeile liefert $r_0, \ldots, r_{e-1}, s_0, \ldots, s_{d-1} \in R$ mit

$$\operatorname{res}(\alpha, \beta) = \sum_{i=0}^{e-1} \alpha X^i r_i + \sum_{i=0}^{d-1} \beta X^i s_i.$$

Die Behauptung folgt mit $\gamma = \sum r_i X^i$ und $\delta = \sum s_i X^i$. □

Lemma III.2.37. *Sei R ein Integritätsbereich und $\alpha, \beta, \gamma \in R[X]$. Dann gilt*

$$\operatorname{res}(\alpha\beta, \gamma) = \operatorname{res}(\alpha, \gamma)\operatorname{res}(\beta, \gamma).$$

Beweis. Wir dürfen R durch $K := Q(R)$ ersetzen. O. B. d. A. sei $\alpha \neq 0 \neq \gamma$ mit $d := \deg \alpha$ und $f := \deg \gamma$. Aus der Linearität der Determinante in den Spalten der Sylvester-Matrix folgt $\operatorname{res}(\alpha, c\gamma) = c^d \operatorname{res}(\alpha, \gamma)$ für alle $c \in K$. Wir können daher annehmen, dass γ normiert ist. Wir betrachten den K-Vektorraum V aller Polynome vom Grad $< d + f$ bzgl. der Basen

$$B := \{1, X, \ldots, X^{d+f-1}\},$$
$$C := \{1, X, \ldots, X^{f-1}, \gamma, X\gamma, \ldots, X^{d-1}\gamma\}.$$

Sei $F_\alpha \in \operatorname{End}_K(V)$ mit $F_\alpha(X^i) := \alpha X^i$ für $i = 0, \ldots, f-1$ und $F_\alpha(X^i\gamma) := X^i\gamma$ für $i = 0, \ldots, d-1$. Bezüglich C und B hat F_α die Darstellungsmatrix ${}_B[F_\alpha]_C := S(\alpha, \gamma)$. Die Basiswechselmatrix T von B nach C ist eine obere Dreiecksmatrix mit Einsen auf der Hauptdiagonale, da γ normiert ist. Insbesondere gilt $\det T = 1$. Für die Darstellungsmatrix von F_α bzgl. B und B gilt daher ${}_B[F_\alpha]_B = {}_B[F_\alpha]_C T$ und $\det F_\alpha = \det(S(\alpha, \gamma)) \det(T) = \operatorname{res}(\alpha, \gamma)$.

Da F_α trivial auf dem Unterraum $W := \langle \gamma, X\gamma, \ldots, X^{d-1}\gamma \rangle$ operiert, induziert F_α einen Endomorphismus $\overline{F_\alpha}$ auf $\overline{V} := V/W \simeq K[X]/(\gamma)$ mit der gleichen Determinante. Tatsächlich beschreibt $\overline{F_\alpha}$ lediglich die Multiplikation mit α modulo (γ). Insbesondere ist $\overline{F_{\alpha\beta}} = \overline{F_\alpha} \circ \overline{F_\beta}$. Dies zeigt

$$\operatorname{res}(\alpha\beta, \gamma) = \det \overline{F_{\alpha\beta}} = \det(\overline{F_\alpha} \circ \overline{F_\beta}) = \det(F_\alpha) \det(F_\beta) = \operatorname{res}(\alpha, \gamma) \operatorname{res}(\beta, \gamma). \qquad \square$$

Bemerkung III.2.38. Für $d = \deg \alpha$, $e = \deg \beta$ und $f = \deg \gamma$ gilt

$$\operatorname{res}(\gamma, \alpha\beta) = (-1)^{f(d+e)} \operatorname{res}(\alpha\beta, \gamma) = (-1)^{df} \operatorname{res}(\alpha, \gamma)(-1)^{ef} \operatorname{res}(\beta, \gamma) = \operatorname{res}(\gamma, \alpha) \operatorname{res}(\gamma, \beta)$$

nach Beispiel III.2.33.

Satz III.2.39. *Sei R ein Integritätsbereich und $\alpha, \beta \in R[X]$ normiert. Seien $x_1, \ldots, x_d$ bzw. $y_1, \ldots, y_e$ die Nullstellen von α bzw. β im algebraischen Abschluss $\overline{Q(R)}$. Dann gilt*

$$\operatorname{res}(\alpha, \beta) = \prod_{i=1}^{d} \prod_{j=1}^{e} (y_j - x_i).$$

Beweis. O. B. d. A. sei $R = \overline{Q(R)}$. Aus Lemma III.2.37, Bemerkung III.2.38 und Beispiel III.2.33 folgt

$$\begin{aligned} \operatorname{res}(\alpha, \beta) &= \operatorname{res}((X - x_1) \ldots (X - x_d), (X - y_1) \ldots (X - y_e)) \\ &= \prod_{i=1}^{d} \prod_{j=1}^{e} \operatorname{res}(X - x_i, X - y_j) = \prod_{i=1}^{d} \prod_{j=1}^{e} (y_j - x_i). \end{aligned} \qquad \square$$

Bemerkung III.2.40. Die Definition I.14.21 der Diskriminante für normierte rationale Polynome lässt sich auf beliebige Körper K (sogar Integritätsbereiche) ausdehnen, indem man Nullstellen in $\overline{K}$ betrachtet.

Folgerung III.2.41. *Sei $\alpha \in K[X] \setminus K$ normiert vom Grad d. Dann ist $D_\alpha = (-1)^{\frac{d(d-1)}{2}} \operatorname{res}(\alpha', \alpha)$.*

Beweis. O. B. d. A. sei $K = \overline{K}$. Nach Satz I.11.20 ist K vollkommen. Im Fall $\alpha' = 0$ ist $\alpha = \beta^p$ mit $\beta \in K[X]$ und $p = \operatorname{char} K > 0$ (vgl. Beweis von Satz I.11.20). Dann besitzt α eine mehrfache Nullstelle

und es folgt $D_\alpha = 0 = \operatorname{res}(\alpha', \alpha)$. Sei daher $\alpha = (X - x_1) \dots (X - x_d)$ und $\alpha' = c(X - y_1) \dots (X - y_e)$ mit $c \in K^\times$. Nach der Produktregel gilt $\alpha' = \sum_{i=1}^{d} \frac{\alpha}{X - x_i}$. Dies zeigt

$$c \prod_{j=1}^{e} (x_i - y_j) = \alpha'(x_i) = \prod_{j \neq i} (x_i - x_j)$$

für $i = 1, \dots, d$. Mit Satz III.2.39 folgt

$$\operatorname{res}(\alpha', \alpha) = c^d \prod_{i=1}^{d} \prod_{j=1}^{e} (x_i - y_j) = \prod_{i=1}^{d} \prod_{j \neq i} (x_i - x_j) = (-1)^{\frac{d(d-1)}{2}} \prod_{i<j} (x_j - x_i)^2 = (-1)^{\frac{d(d-1)}{2}} D_\alpha. \qquad \square$$

Bemerkung III.2.42.

(i) Für $\operatorname{char} K \nmid \deg(\alpha)$ ist $\deg \alpha = \deg(\alpha') + 1$ und $\operatorname{res}(\alpha', \alpha) = \operatorname{res}(\alpha, \alpha')$ nach Beispiel III.2.33.

(ii) Mittels der Sylvester-Matrix ermöglicht Folgerung III.2.41 die Berechnung der Diskriminante ohne R zu verlassen.

Beispiel III.2.43. Sei $\operatorname{char} K \neq 3$ und $\alpha = X^3 + aX + b \in K[X]$. Dann gilt

$$D_\alpha = -\operatorname{res}(\alpha', \alpha) = -\begin{vmatrix} a & . & . & b & . \\ . & a & . & a & b \\ 3 & . & a & . & a \\ . & 3 & . & 1 & . \\ . & . & 3 & . & 1 \end{vmatrix} = -\begin{vmatrix} 3 & . & a & . & a \\ . & 3 & . & 1 & . \\ . & . & 3 & . & 1 \\ a & . & . & b & . \\ . & a & . & a & b \end{vmatrix} = -\begin{vmatrix} 3 & . & a & . & a \\ . & 3 & . & 1 & . \\ . & . & 3 & . & 1 \\ . & . & -\frac{1}{3}a^2 & b & -\frac{1}{3}a^2 \\ . & . & . & \frac{2}{3}a & b \end{vmatrix}$$

$$= -\begin{vmatrix} 3 & . & a & . & a \\ . & 3 & . & 1 & . \\ . & . & 3 & . & 1 \\ . & . & . & b & -\frac{2}{9}a^2 \\ . & . & . & \frac{2}{3}a & b \end{vmatrix} = -27(b^2 + \frac{4}{27}a^3) = -4a^3 - 27b^2$$

(vgl. Bemerkung I.14.22).

Satz III.2.44. *Enthält $I \trianglelefteq K[X_1, \dots, X_n]$ ein Polynom, das bzgl. X_n normiert ist, so ist die Projektion*

$$\pi \colon \mathcal{V}(I) \to \mathcal{V}(I \cap K[X_1, \dots, X_{n-1}]) \subseteq K^{n-1},$$
$$(x_1, \dots, x_n) \mapsto (x_1, \dots, x_{n-1})$$

surjektiv.

Beweis. Offensichtlich ist die Projektion zumindest wohldefiniert. Sei $(x_1, \dots, x_{n-1}) \in K^{n-1} \setminus \pi(\mathcal{V}(I))$. Sei $\alpha \in I$ normiert in X_n. Im Fall $\alpha = 1$ sind beide Mengen leer. Sei also $\alpha \notin K$. Seien $y_1, \dots, y_d$ die Nullstellen von $\tilde{\alpha} := \alpha(x_1, \dots, x_{n-1}, X_n) \in K[X_n] \setminus K$. Nach Lemma III.2.30 existiert $\beta \in I$ mit $\beta(x_1, \dots, x_{n-1}, y_i) \neq 0$ für $i = 1, \dots, d$. Im Fall $\beta \in R := K[X_1, \dots, X_{n-1}]$ gilt bereits $(x_1, \dots, x_{n-1}) \notin \mathcal{V}(I \cap R)$. Sei also $\tilde{\beta} := \beta(x_1, \dots, x_{n-1}, X_n) \in K[X] \setminus K$. Da $\tilde{\alpha}$ und $\tilde{\beta}$ keine gemeinsame Nullstelle besitzen, sind sie teilerfremd. Für $\gamma := \operatorname{res}(\alpha, \beta) \in R$ gilt daher $\gamma(x_1, \dots, x_{n-1}) = \operatorname{res}(\tilde{\alpha}, \tilde{\beta}) \neq 0$ nach Satz III.2.34. Nach Lemma III.2.36 ist $\gamma \in (\alpha, \beta) \cap R \subseteq I \cap R$. Dies zeigt $(x_1, \dots, x_{n-1}) \notin \mathcal{V}(I \cap R)$. $\square$

Beispiel III.2.45. Offenbar besitzt $I := (1 - XY) \trianglelefteq K[X, Y]$ *kein* normiertes Polynom in Y. In der Tat ist die Projektion $\pi \colon \mathcal{V}(I) \to \mathcal{V}(I \cap K[X]) = \mathcal{V}(0) = K$ auch nicht surjektiv, denn $0 \notin \pi(\mathcal{V}(I))$.

Bemerkung III.2.46. Satz III.2.44 ermöglicht die Elimination von Variablen (konkret X_n). Man nennt $I \cap K[X_1, \ldots, X_{n-1}]$ daher ein *Eliminationsideal*. Die Berechnung von Eliminationsidealen in der Praxis führt auf ein allgemeineres Problem:

Wie kann man feststellen, ob ein Polynom $\alpha \in R := K[X_1, \ldots, X_n]$ in einem gegebenen Ideal $I := (\beta_1, \ldots, \beta_k) \trianglelefteq R$ liegt? Für $n = 1$ lässt sich $\gamma := \mathrm{ggT}(\beta_1, \ldots, \beta_k)$ mit dem euklidischen Algorithmus berechnen. Es gilt dann $\alpha \in I \iff \gamma \mid \alpha$ (Bézouts Lemma). Für $n \geq 2$ ist R allerdings nicht euklidisch und die Resultante reicht zu Berechnung des ggT nicht aus. Wir suchen daher einen Ersatz für die Division mit Rest. Hierfür sei K ein beliebiger Körper (nicht unbedingt $K = \overline{K}$).

Definition III.2.47. Sei $\mathcal{M} := \{X_1^{i_1} \ldots X_n^{i_n} : i_1, \ldots, i_n \in \mathbb{N}_0\}$ die Menge aller Monome von $R := K[X_1, \ldots, X_n]$. Eine totale Ordnungsrelation $\leq$ auf $\mathcal{M}$ heißt *Monomordnung* auf R, falls für alle $\alpha, \beta, \gamma \in \mathcal{M}$ gilt

- $1 \leq \alpha$.
- $\alpha < \beta \implies \alpha\gamma < \beta\gamma$.

Bemerkung III.2.48. Seien $\alpha, \beta \in \mathcal{M}$ mit $\alpha \mid \beta$. Aus $1 \leq \frac{\beta}{\alpha}$ folgt $\alpha \leq \beta$. Die Teilbarkeitsrelation kann für $n \geq 2$ jedoch keine Monomordnung sein, da sie nicht total ist.

Beispiel III.2.49.

(i) Für $n = 1$ ist $\alpha \leq \beta \iff \deg \alpha \leq \deg \beta$ die einzige Monomordnung.

(ii) Im Beweis von Satz I.14.19 haben wir bereits die lexikografische Ordnung mit $X_1 > \ldots > X_n$ benutzt. Man zeigt leicht, dass sie eine Monomordnung ist. Eine weitere Monomordnung wird in Aufgabe III.6 konstruiert.

Lemma III.2.50 (Dickson)**.** *Für $M \subseteq \mathcal{M}$ existiert eine endliche Teilmenge $N \subseteq M$ mit $(M) = (N)$.*

Beweis. Nach Hilberts Basissatz existieren $\alpha_1, \ldots, \alpha_k \in K[X_1, \ldots, X_n]$ mit $(M) = (\alpha_1, \ldots, \alpha_k)$. Für ein festes i seien $\beta_1, \ldots, \beta_s \in M$ und $\gamma_1, \ldots, \gamma_s \in K[X_1, \ldots, X_n]$ mit $\alpha_i = \beta_1\gamma_1 + \ldots + \beta_s\gamma_s$. Jedes Monom von α_i tritt in einem der Summanden $\beta_j\gamma_j$ und liegt daher in (β_j). Also wird α_i durch endlich viele Elemente in M erzeugt. Insgesamt wird auch $(\alpha_1, \ldots, \alpha_k)$ durch endlich viele Elemente in M erzeugt. □

Lemma III.2.51. *Sei $\leq$ eine Monomordnung auf $K[X_1, \ldots, X_n]$. Dann existiert keine unendliche absteigende Kette $\alpha_1 > \alpha_2 > \ldots$ in $\mathcal{M}$. Insbesondere besitzt jede nicht-leere Teilmenge von $\mathcal{M}$ ein kleinstes Element.*

Beweis. Angenommen es existieren $\alpha_1, \ldots \in \mathcal{M}$ mit $\alpha_1 > \alpha_2 > \ldots$. Nach Lemma III.2.50 existieren $\beta_1, \ldots, \beta_k \in \{\alpha_1, \ldots\}$ mit $(\alpha_1, \ldots) = (\beta_1, \ldots, \beta_k)$ und o. B. d. A. $\beta_1 > \ldots > \beta_k$. Sei $\alpha_m < \beta_k$. Dann existieren $\gamma_1, \ldots, \gamma_k \in K[X_1, \ldots, X_n]$ mit $\alpha_m = \beta_1\gamma_1 + \ldots + \beta_k\gamma_k$. Es folgt $\beta_i \mid \alpha_m$ für ein $1 \leq i \leq k$. Aus Bemerkung III.2.48 erhält man den Widerspruch $\beta_i \leq \alpha_m < \beta_k \leq \beta_i$.

In jeder nicht-leeren Teilmenge $M \subseteq \mathcal{M}$ existiert nun ein minimales Element $\alpha \in M$. Da $\leq$ total ist, muss α das kleinste Element von M sein (Bemerkung II.1.5). □

Definition III.2.52. Im Folgenden sei $\leq$ stets eine fest gewählte Monomordnung. Wir sortieren die Monome eines Polynoms $\alpha \in K[X_1, \ldots, X_n] \setminus \{0\}$ entsprechend $\leq$ ohne Berücksichtigung der Koeffizienten. Das größte Monom (*Leitmonom*) in α sei $\operatorname{lm} \alpha \in \mathcal{M}$ und sein Koeffizient (*Leitkoeffizient*) sei $\operatorname{lc} \alpha \in K^\times$. Zusätzlich sei $\operatorname{lm} 0 := 0 =: \operatorname{lc} 0$, wobei $0 < \rho$ für alle $\rho \in \mathcal{M}$ gelte (dies entspricht $\deg 0 = -\infty$). Im Fall $\operatorname{lc} \alpha = 1$ nennt man α *normiert*.

Satz III.2.53. *Sei $R := K[X_1, \ldots, X_n]$. Für $\alpha, \beta_1, \ldots, \beta_k \in R \setminus \{0\}$ existieren $\gamma_1, \ldots, \gamma_k, \delta \in R$ mit*

(i) $\alpha = \beta_1\gamma_1 + \ldots + \beta_k\gamma_k + \delta$.

(ii) $\operatorname{lm}(\beta_i\gamma_i) \leq \operatorname{lm} \alpha$ *für* $i = 1, \ldots, k$.

(iii) Kein Monom in δ ist durch ein $\operatorname{lm} \beta_i$ teilbar.

Beweis. Ist kein Monom in α durch ein $\operatorname{lm} \beta_i$ teilbar, so gilt die Aussage mit $\gamma_1 = \ldots = \gamma_k = 0$ und $\delta = \alpha$. Sei also ρ_1 das größte Monom in $\alpha_1 := \alpha$, das durch ein $\operatorname{lm} \beta_i$ teilbar ist. Dann existiert $c_1 \in K$, sodass ρ_1 nicht mehr in

$$\alpha_2 := \alpha_1 - c_1 \frac{\rho_1}{\operatorname{lm} \beta_i} \beta_i$$

vorkommt (es wurde durch kleinere Monome ersetzt). Wir wiederholen den Prozess mit α_2 und erhalten eine Folge $\alpha_1, \alpha_2, \ldots$ mit Monomen $\rho_1 > \rho_2 > \ldots$. Nach Lemma III.2.51 muss die Folge abbrechen, sagen wir an der Stelle $\alpha_s =: \delta$. Nun ist kein Monom in δ durch ein $\operatorname{lm} \beta_i$ teilbar. Außerdem gilt $\alpha = \beta_1\gamma_1 + \ldots + \beta_k\gamma_k + \delta$, wobei jedes γ_i eine Summe von Termen der Form $c_j \frac{\rho_j}{\operatorname{lm} \beta_i}$ ist. Insbesondere gilt $\operatorname{lm}(\beta_i\gamma_i) \leq \rho_1 \leq \operatorname{lm} \alpha$ für $i = 1, \ldots, k$. □

Bemerkung III.2.54. Für $n = 1$ liefert Satz III.2.53 genau die Division mit Rest. Im Allgemeinen sind $\gamma_1, \ldots, \gamma_k, \delta$ durch die angegebenen Eigenschaften nicht eindeutig bestimmt (wir haben im Beweis nicht spezifiziert, welches β_i gewählt werden soll, wenn es mehrere gibt, die ρ_1 teilen). Dennoch nennen wir δ einen *Rest* bei der Division von α durch $\beta_1, \ldots, \beta_k$. Für $\alpha = 0$ ist $\gamma_1 = \ldots = \gamma_k = 0 = \delta$ wegen $\operatorname{lm}(\beta_i\gamma_i) \leq \operatorname{lm} \alpha = 0$.

Beispiel III.2.55. Sei $\alpha = X^2Y - Y$, $\beta_1 = XY - X$ und $\beta_2 = X^2 - Y$. Bezüglich der lexikografischen Monomordnung ist $\rho_1 = X^2Y$ durch $\operatorname{lm} \beta_1 = XY$ teilbar. Man erhält

$$\alpha_2 = \alpha - X\beta_1 = X^2 - Y = \beta_2.$$

Also gilt $\alpha = X\beta_1 + \beta_2$ mit $\delta = 0$. Allerdings ist ρ_1 auch durch $\operatorname{lm} \beta_2 = X^2$ teilbar. Diesmal erhält man

$$\alpha_2 = \alpha - Y\beta_2 = Y^2 - Y.$$

Nun ist $\rho_2 = \operatorname{lm} \alpha_2 = Y^2$ nicht mehr durch $\operatorname{lm} \beta_1$ oder $\operatorname{lm} \beta_2$ teilbar. Hier gilt also $\delta = Y(Y-1) \neq 0$ und $\alpha = 0\beta_1 + Y\beta_2 + \delta$.

Definition III.2.56. Sei $I \trianglelefteq R := K[X_1, \ldots, X_n]$ und $\operatorname{lm} I := (\operatorname{lm} \alpha : \alpha \in I) \trianglelefteq R$. Man nennt $\beta_1, \ldots, \beta_k \in R \setminus \{0\}$ eine *Gröbnerbasis* von I, falls $I = (\beta_1, \ldots, \beta_k)$ und $\operatorname{lm} I = (\operatorname{lm} \beta_1, \ldots, \operatorname{lm} \beta_k)$.

Bemerkung III.2.57. Trotz ihres Namens können zwei Gröbnerbasen eines Ideals I unterschiedlich viele Elemente aufweisen. Ist beispielsweise B eine Gröbnerbasis von I und $\alpha \in I \setminus B$, so ist auch $B \cup \{\alpha\}$ eine Gröbnerbasis von I. Wir führen in Definition III.2.66 eine Minimalitätsbedingung ein.

Satz III.2.58 (Gröbner). *Sei $\beta_1, \ldots, \beta_k$ eine Gröbnerbasis von $I \trianglelefteq R := K[X_1, \ldots, X_n]$. Für $\alpha \in R$ ist der Rest δ bei der Division von α durch $\beta_1, \ldots, \beta_k$ eindeutig bestimmt und es gilt $\alpha \in I$ genau dann, wenn $\delta = 0$.*

Beweis. Seien $\alpha = \beta_1\gamma_1 + \ldots + \beta_k\gamma_k + \delta = \beta_1\tilde{\gamma}_1 + \ldots + \beta_k\tilde{\gamma}_k + \tilde{\delta}$ zwei Zerlegungen wie in Satz III.2.53. Dann gilt $\delta - \tilde{\delta} \in I$ und es existieren $\sigma_1, \ldots, \sigma_k \in R$ mit $\operatorname{lm}(\delta - \tilde{\delta}) = \sigma_1 \operatorname{lm}\beta_1 + \ldots \sigma_k \operatorname{lm}\beta_k$. Im Fall $\delta \neq \tilde{\delta}$ wäre ein Monom von δ oder $\tilde{\delta}$ durch ein $\operatorname{lm}\beta_i$ teilbar. Dies widerspricht Satz III.2.53. Also gilt $\delta = \tilde{\delta}$.

Aus $\delta = 0$ folgt sofort $\alpha \in I$. Sei umgekehrt $\alpha \in I$. Dann gilt $\delta \in (\alpha, \beta_1, \ldots, \beta_k) = I$. Im Fall $\delta \neq 0$ wäre $\operatorname{lm}\delta \in \operatorname{lm} I$ und $\operatorname{lm}\beta_i \mid \operatorname{lm}\delta$ für ein i im Widerspruch zu Satz III.2.53. Also ist $\delta = 0$. □

Beispiel III.2.59. Nach Beispiel III.2.55 ist $\beta_1 = XY - X$, $\beta_2 = X^2 - Y$ *keine* Gröbnerbasis von $I = (\beta_1, \beta_2)$. Wegen $Y = X\beta_1 - (Y-1)\beta_2 \in I$ und $X = XY - \beta_1 \in I$ ist X, Y eine Gröbnerbasis von I.

Satz III.2.60. *Jedes Ideal in $K[X_1, \ldots, X_n]$ besitzt eine Gröbnerbasis.*

Beweis. Sei $I \trianglelefteq R := K[X_1, \ldots, X_n]$. Im Fall $I = 0$ wähle man die Gröbnerbasis $\varnothing$. Sei also $I \neq 0$. Nach Lemma III.2.50 existieren $\beta_1, \ldots, \beta_k \in I \setminus \{0\}$ mit $\operatorname{lm} I = (\operatorname{lm}\beta_1, \ldots, \operatorname{lm}\beta_k)$. Sei $\alpha \in I$ beliebig. Seien $\gamma_1, \ldots, \gamma_k, \delta \in R$ wie in Satz III.2.53. Dann gilt auch $\delta \in I$. Im Fall $\delta \neq 0$ ist $\operatorname{lm}\delta \in \operatorname{lm} I$. Wie im Beweis von Satz III.2.58 wäre dann $\operatorname{lm}\beta_i \mid \operatorname{lm}\delta$ für ein i. Also ist $\delta = 0$ und $\alpha \in (\beta_1, \ldots, \beta_k)$. Dies zeigt $I = (\beta_1, \ldots, \beta_k)$, d. h. $\beta_1, \ldots, \beta_k$ ist eine Gröbnerbasis von I. □

Bemerkung III.2.61. Der Beweis von Satz III.2.60 zeigt, dass $\beta_1, \ldots, \beta_k \in K[X_1, \ldots, X_n]$ bereits dann eine Gröbnerbasis von I ist, wenn $\operatorname{lm} I = (\operatorname{lm}\beta_1, \ldots, \operatorname{lm}\beta_k)$ gilt, d. h. die Bedingung $I = (\beta_1, \ldots, \beta_k)$ ist überflüssig.

Satz III.2.62 (Buchberger-Kriterium). *Seien $\beta_1, \ldots, \beta_k \in K[X_1, \ldots, X_n] \setminus \{0\}$ normiert, $\gamma_{ij} := \operatorname{kgV}(\operatorname{lm}\beta_i, \operatorname{lm}\beta_j)$ und*

$$\alpha_{ij} := \frac{\gamma_{ij}}{\operatorname{lm}\beta_i}\beta_i - \frac{\gamma_{ij}}{\operatorname{lm}\beta_j}\beta_j$$

für $i < j$. Sei δ_{ij} ein Rest bei der Division von α_{ij} durch $\beta_1, \ldots, \beta_k$. Genau dann ist $\beta_1, \ldots, \beta_k$ eine Gröbnerbasis von $(\beta_1, \ldots, \beta_k)$, wenn $\delta_{ij} = 0$ für alle $i < j$.

Beweis. Ist $\beta_1, \ldots, \beta_k$ eine Gröbnerbasis von I, so gilt $\delta_{ij} = 0$ für $i < j$ nach Satz III.2.58, denn $\alpha_{ij} \in I$. Nehmen wir umgekehrt $\delta_{ij} = 0$ für $i < j$ an. Jedes $\alpha \in I \setminus \{0\}$ hat die Form $\alpha = \beta_1\gamma_1 + \ldots + \beta_k\gamma_k$ mit $\gamma_1, \ldots, \gamma_k \in K[X_1, \ldots, X_n]$. Sei

$$\rho := \max_{1 \leq i \leq k} \operatorname{lm}(\beta_i\gamma_i).$$

Unter allen möglichen Darstellungen von α wählen wir $\gamma_1, \ldots, \gamma_k$, sodass ρ möglichst klein wird (das geht wegen Lemma III.2.51).

Annahme: ρ ist kein Monom von α.
Nach Umnummerierung können wir $\operatorname{lm}(\beta_i\gamma_i) = \rho$ für $i = 1, \ldots, l$ erreichen. Hierbei muss $l \geq 2$ gelten, denn anderenfalls könnte man ρ aus $\beta_1\gamma_1 + \ldots + \beta_k\gamma_k = \alpha$ nicht eliminieren. Aus dem gleichen Grund gilt $\operatorname{lm}(\beta_1\gamma_1 + \ldots + \beta_l\gamma_l) < \rho$. Sei $\operatorname{lc}\gamma_i = a_i$, $\operatorname{lm}\gamma_i = \rho_i$ und $\tilde{\beta}_i := \beta_i\rho_i$ für $i = 1, \ldots, k$. Dann gilt $\operatorname{lm}\tilde{\beta}_i = \rho$ für $i = 1, \ldots, l$ und $\operatorname{lm}(a_1\tilde{\beta}_1 + \ldots + a_l\tilde{\beta}_l) < \rho$. Es folgt $a_1 + \ldots + a_l = 0$. Wir setzen

$$\tilde{\alpha}_{ij} := \tilde{\beta}_i - \tilde{\beta}_j = \frac{\rho}{\operatorname{lm}\beta_i}\beta_i - \frac{\rho}{\operatorname{lm}\beta_j}\beta_j = \frac{\rho}{\gamma_{ij}}\Big(\frac{\gamma_{ij}}{\operatorname{lm}\beta_i}\beta_i - \frac{\gamma_{ij}}{\operatorname{lm}\beta_j}\beta_j\Big) = \frac{\rho}{\gamma_{ij}}\alpha_{ij}$$

für $i, j = 1, \ldots, l$. Dann gilt

$$\begin{aligned} a_1\tilde{\beta}_1 + \ldots + a_l\tilde{\beta}_l &= a_1(\tilde{\beta}_1 - \tilde{\beta}_2) + (a_1 + a_2)(\tilde{\beta}_2 - \tilde{\beta}_3) + \ldots + (a_1 + \ldots + a_{h-1})(\tilde{\beta}_{l-1} - \tilde{\beta}_l) \\ &\quad + (a_1 + \ldots + a_l)\tilde{\beta}_l \\ &= \tilde{a}_1\tilde{\alpha}_{12} + \tilde{a}_2\tilde{\alpha}_{23} + \ldots + \tilde{a}_{l-1}\tilde{\alpha}_{l-1,l} \end{aligned}$$

mit $\tilde{a}_i := a_1 + \ldots + a_i \in K$ für $i = 1, \ldots, l$. Wegen $\operatorname{lm}\tilde{\beta}_i = \rho = \operatorname{lm}\tilde{\beta}_j$ ist $\operatorname{lm}\tilde{\alpha}_{ij} < \rho$. Nach Voraussetzung lässt sich α_{ij} für $i < j$ ohne Rest durch $\beta_1, \ldots, \beta_k$ „teilen“. Das Gleiche gilt für α'_{ij} und $\tilde{a}_1\tilde{\alpha}_{12} + \tilde{a}_2\tilde{\alpha}_{23} + \ldots + \tilde{a}_{h-1}\tilde{\beta}_{h-1,h}$. Also existieren $\tilde{\gamma}_1, \ldots, \tilde{\gamma}_k \in K[X_1, \ldots, X_n]$ mit

$$a_1\rho_1\beta_1 + \ldots + a_l\rho_l\beta_l = \tilde{a}_1\tilde{\alpha}_{12} + \tilde{a}_2\tilde{\alpha}_{23} + \ldots + \tilde{a}_{l-1}\tilde{\alpha}_{l-1,l} = \tilde{\gamma}_1\beta_1 + \ldots + \tilde{\gamma}_k\beta_k$$

und $\operatorname{lm}(\tilde{\gamma}_i\beta_i) \leq \operatorname{lm}(a_1\tilde{\beta}_1 + \ldots + a_l\tilde{\beta}_l) < \rho$ für $i = 1, \ldots, k$. Wegen $a_i\rho_i = \operatorname{lc}\gamma_i \operatorname{lm}\gamma_i$ können wir die $\tilde{\gamma}_i$ abändern, sodass

$$\beta_1\gamma_1 + \ldots + \beta_l\gamma_l = \beta_1\tilde{\gamma}_1 + \ldots + \beta_k\tilde{\gamma}_k$$

mit $\operatorname{lm}(\beta_i\tilde{\gamma}_i) < \rho$ für $i = 1, \ldots, k$ gilt. Nochmalige Änderung der $\tilde{\gamma}_i$ ergibt

$$\alpha = \beta_1\gamma_1 + \ldots + \beta_k\gamma_k = \beta_1\tilde{\gamma}_1 + \ldots + \beta_k\tilde{\gamma}_k$$

immer noch mit $\operatorname{lm}(\beta_i\tilde{\gamma}_i) < \rho$ für $i = 1, \ldots, k$. Dies widerspricht der Wahl von ρ.

Also tritt das Monom ρ in α auf. Dies bedeutet $\operatorname{lm}(\beta_i\gamma_i) \leq \operatorname{lm}\alpha$ für $i = 1, \ldots, k$. Insbesondere ist $\operatorname{lm}\alpha$ eine K-Linearkombination der $\operatorname{lm}(\beta_i\gamma_i)$, d. h. $\operatorname{lm}\alpha \in (\operatorname{lm}\beta_1, \ldots, \operatorname{lm}\beta_k)$. Dies zeigt, dass $\beta_1, \ldots, \beta_k$ eine Gröbnerbasis von I ist. □

Satz III.2.63 (Buchberger-Algorithmus)**.**
Eingabe: $\beta_1, \ldots, \beta_k \in K[X_1, \ldots, X_n] \setminus \{0\}$.
Initialisierung: Normiere $\beta_1, \ldots, \beta_k$ *und setze* $B := \{\beta_1, \ldots, \beta_k\}$.
Wiederhole...
Für $i < j$ *berechne und normiere* δ_{ij} *wie in Satz III.2.62 bzgl. der Polynome in* B.
Füge die $\delta_{ij} \neq 0$ *der Menge* B *hinzu.*
... bis $\delta_{ij} = 0$ *für alle* $i < j$ *gilt.*
Ausgabe: B *ist eine Gröbnerbasis von* $(\beta_1, \ldots, \beta_k)$.

Beweis. Nach Definition gilt $\delta_{ij} \in (\beta_1, \ldots, \beta_k) =: I$ für $i < j$. In jedem Schritt bleibt daher $I = (B)$. Im Fall $\delta_{ij} \neq 0$ ist kein Monom in δ_{ij} durch ein $\operatorname{lm}\alpha$ mit $\alpha \in B$ teilbar. Dann gilt $(\operatorname{lm}\alpha : \alpha \in B) < (\operatorname{lm}\alpha, \operatorname{lm}\delta_{ij} : \alpha \in B)$. Da $K[X_1, \ldots, X_n]$ noethersch ist, muss diese Folge von Idealen stationär werden. Nach endlich vielen Schritten gilt also $\delta_{ij} = 0$ für alle $i < j$. Nach dem Buchberger-Kriterium ist B eine Gröbnerbasis von I. □

Beispiel III.2.64. Sei $\beta_1 = XY - Y \in \mathbb{C}[X, Y]$ und $\beta_2 = X - Y^2 \in \mathbb{C}[X, Y]$ bzgl. der lexikografischen Monomordnung. Wie in Satz III.2.62 sei $\gamma_{12} = XY$ und $\alpha_{12} = \beta_1 - Y\beta_2 = Y^3 - Y$. Wegen $\operatorname{lm}\alpha_{12} = Y^3 < \operatorname{lm}\beta_i$ muss $\beta_3 := \delta_{12} = \alpha_{12}$ gelten. Bezüglich $B = \{\beta_1, \beta_2, \beta_3\}$ berechnen wir

$$\begin{aligned} &\alpha_{12} = Y^2 - Y, && \alpha_{13} = Y^2\beta_1 - X\beta_3 = XY - Y^3, && \alpha_{23} = Y^3\beta_2 - X\beta_3 = XY - Y^5 \\ &\delta_{12} = \alpha_{12} - \beta_3 = 0, && \delta_{13} = \alpha_{13} - \beta_1 + \beta_3 = 0, && \delta_{23} = \alpha_{23} - \beta_1 + (Y^2 + 1)\beta_3 = 0. \end{aligned}$$

Folglich ist B eine Gröbnerbasis von (β_1, β_2). Wir prüfen, ob $\alpha = X^3 + Y$ in I liegt:

$$\alpha - X^2\beta_2 - (XY + Y)\beta_1 = X^2Y^2 + Y - (X^2Y^2 - Y^2) = Y^2 + Y.$$

Da Y^2 durch kein $\operatorname{lm}\beta_i$ teilbar ist, ist der Rest $\delta = Y^2 + Y \neq 0$, d. h. $\alpha \notin I$.

Bemerkung III.2.65. Der Buchberger-Algorithmus in Kombination mit Satz III.2.58 findet wichtige Anwendungen in der Computeralgebra:

(i) Es lässt sich entscheiden, ob ein System von Polynomgleichungen lösbar ist (prüfe $1 \in I$). Nach Aufgabe III.1 funktioniert dies sogar über beliebigen Körpern.

(ii) Man kann $\alpha \in \sqrt{(\beta_1, \ldots, \beta_k)}$ überprüfen. Dafür führt man wie im Beweis des Nullstellensatz eine neue Variable Y ein und prüft $\alpha \in (\beta_1, \ldots, \beta_k, \alpha Y - 1)$.

(iii) Eliminationsideale lassen sich berechnen (Aufgabe III.8).

(iv) Der Durchschnitt von Idealen $(\beta_1, \ldots, \beta_k) \cap (\gamma_1, \ldots, \gamma_l)$ lässt sich berechnen (Aufgabe III.9).

(v) Die Dimension einer Varietät $A \in \mathrm{A}(K^n)$ lässt sich wie folgt berechnen. Sei $\beta_1, \ldots, \beta_k$ eine Gröbnerbasis von $\mathcal{I}(A)$ und $S \subseteq \{X_1, \ldots, X_n\}$ eine größtmögliche Teilmenge mit

$$(S) \cap \{\operatorname{lm} \beta_1, \ldots, \operatorname{lm} \beta_k\} = \varnothing.$$

Dann gilt $\dim A = |S|$ (ohne Beweis).

In der Praxis liefert der Buchberger-Algorithmus oft redundante Basiselemente (siehe Beispiel III.2.68). Dies lässt sich wie folgt beheben.

Definition III.2.66. Eine Gröbnerbasis $\beta_1, \ldots, \beta_k$ heißt *reduziert*, falls gilt:

- $\beta_1, \ldots, \beta_k$ sind normiert.
- $\operatorname{lm} \beta_1 > \ldots > \operatorname{lm} \beta_k$.
- Kein Monom in β_i ist durch ein $\operatorname{lm} \beta_j$ mit $i \neq j$ teilbar.

Satz III.2.67. *Jedes Ideal $I \trianglelefteq K[X_1, \ldots, X_n]$ besitzt genau eine reduzierte Gröbnerbasis $\beta_1, \ldots, \beta_k$ (bzgl. $\leq$) und jede Gröbnerbasis von I enthält mindestens k Polynome.*

Beweis. O. B. d. A. sei $I \neq 0$. Sei $\beta_1, \ldots, \beta_k$ eine beliebige Gröbnerbasis von I. Nehmen wir o. B. d. A. an, dass ein Monom in β_k durch ein $\operatorname{lm} \beta_i$ teilbar ist. Satz III.2.53 liefert

$$\beta_k = \beta_1 \gamma_1 + \ldots + \beta_{k-1} \gamma_{k-1} + \delta,$$

wobei kein Monom in δ durch ein $\operatorname{lm} \beta_i$ teilbar ist. Offenbar gilt $(\beta_1, \ldots, \beta_k) = (\beta_1, \ldots, \beta_{k-1}, \delta)$. Wegen $\operatorname{lm}(\beta_i \gamma_i) \leq \operatorname{lm} \beta_k$ lässt sich $\operatorname{lm} \beta_k$ als Linearkombination von $\operatorname{lm}(\beta_1 \gamma_1), \ldots, \operatorname{lm}(\beta_{k-1} \gamma_{k-1}), \operatorname{lm} \delta$ schreiben. Dies zeigt $(\operatorname{lm} \beta_1, \ldots, \operatorname{lm} \beta_k) = (\operatorname{lm} \beta_1, \ldots, \operatorname{lm} \beta_{k-1}, \operatorname{lm} \delta)$. Im Fall $\delta = 0$ entfernen wir β_k und anderenfalls ersetzen wir β_k durch δ. Wie im Beweis von Satz III.2.53 lässt sich dieser Prozess nur endlich oft wiederholen und am Ende ist kein Monom in β_i durch ein $\operatorname{lm} \beta_j$ mit $i \neq j$ teilbar. Insbesondere ist $\operatorname{lm} \beta_i \neq \operatorname{lm} \beta_j$ für $i \neq j$ und $\operatorname{lm} \beta_1 > \ldots > \operatorname{lm} \beta_k$ nach umsortieren. Die Normierung der β_i ändert nichts an den anderen Eigenschaften. Damit haben wir eine reduzierte Gröbnerbasis B von I konstruiert.

Sei $\tilde{B}$ eine weitere reduzierte Gröbnerbasis von I und $\alpha \in (B \cup \tilde{B}) \setminus (B \cap \tilde{B})$ mit $\operatorname{lm} \alpha$ so klein wie möglich. O. B. d. A. sei $\alpha \in \tilde{B} \setminus B$. Dann existieren $\gamma_1, \ldots, \gamma_k \in K[X_1, \ldots, X_n]$ mit

$$\operatorname{lm} \alpha = \gamma_1 \operatorname{lm} \beta_1 + \ldots + \gamma_k \operatorname{lm} \beta_k.$$

Folglich ist $\operatorname{lm} \alpha$ durch ein $\operatorname{lm} \beta_i$ teilbar. Im Fall $\operatorname{lm} \beta_i < \operatorname{lm} \alpha$ wäre $\beta_i \in \tilde{B}$ im Widerspruch zur Reduziertheit von $\tilde{B}$. Also ist $\operatorname{lm} \beta_i = \operatorname{lm} \alpha$, aber $\beta_i \neq \alpha$ wegen $\alpha \notin B$. Nach Satz III.2.58 existieren $\gamma_1, \ldots, \gamma_k \in K[X_1, \ldots, X_n]$ mit $\alpha - \beta_i = \beta_1 \gamma_1 + \ldots + \beta_k \gamma_k$ und $\operatorname{lm}(\beta_j \gamma_j) \leq \operatorname{lm}(\alpha - \beta_i) < \operatorname{lm} \beta_i$ für

$j = 1, \ldots, k$. Es folgt $\gamma_j = 0$ für $j = 1, \ldots, i$. Sei $\operatorname{lm}(\beta_j\gamma_j) = \operatorname{lm}(\alpha - \beta_i)$. Dann ist $\operatorname{lm}\beta_j$ ein Teiler eines Monoms in α oder β_i. Wegen $\beta_j \in B \cap \tilde{B}$ ist beides ausgeschlossen. Dieser Widerspruch zeigt $B = \tilde{B}$.

Wie anfangs gezeigt lässt sich jede Gröbnerbasis reduzieren, indem man Elemente entfernt oder ersetzt. Daher muss jede Gröbnerbasis mindestens k Elemente besitzen. □

Beispiel III.2.68.

(i) Besitzt die reduzierte Gröbnerbasis eines Ideals I genau k Elementen, so kann es durchaus Erzeugendensysteme mit weniger als k Polynomen geben (Aufgabe III.11).

(ii) Die in Beispiel III.2.64 konstruierte Gröbnerbasis $\beta_1 = XY - Y$, $\beta_2 = X - Y^2$, $\beta_3 = Y^3 - Y$ von $I = (\beta_1, \beta_2)$ ist nicht reduziert, denn XY ist durch $\operatorname{lm}\beta_2 = X$ teilbar. Division mit Rest liefert $\beta_1 = Y\beta_2 + \beta_3$. Daher lässt sich β_1 entfernen und man erhält die reduzierte Gröbnerbasis β_2, β_3 von I.

(iii) Für ein Ideal I mit reduzierter Gröbnerbasis B gilt $I = K[X_1, \ldots, X_n]$ genau dann, wenn $B = \{1\}$ (Aufgabe III.12).

(iv) Die reduzierte Gröbnerbasis eines maximalen Ideals $I \trianglelefteq K[X_1, \ldots, X_n]$ hat die Form $X_1 - x_1, \ldots, X_n - x_n$ bzgl. der lexikografischen Monomordnung.

(v) Seien $\beta_1, \ldots, \beta_k \in K[X_1, \ldots, X_n]$ lineare Polynome. Dann ist $\mathcal{V}(\beta_1, \ldots, \beta_k)$ die Lösungsmenge eines Gleichungssystems, dessen Koeffizientenmatrix A aus den Koeffizienten der β_i gebildet wird. Die Koeffizienten der reduzierten Gröbnerbasis von $(\beta_1, \ldots, \beta_k)$ entsprechen genau der reduzierten Zeilenstufenform von A.

(vi) Für $\beta_1, \ldots, \beta_k \in K[X]$ ist $\operatorname{ggT}(\beta_1, \ldots, \beta_k)$ die reduzierte Gröbnerbasis von $(\beta_1, \ldots, \beta_k)$. Man kann die oben beschriebenen Verfahren daher als gemeinsame Verallgemeinerung des Gauß-Algorithmus und des euklidischen Algorithmus ansehen.

Bemerkung III.2.69. Für ein Polynom

$$\alpha = (X - x_1)^{a_1} \ldots (X - x_d)^{a_d} \in K[X]$$

nennt man a_i bekanntlich die Vielfachheit der Nullstelle x_i. Außerdem ist $\deg\alpha = \dim_K K[X]/(\alpha)$ die Anzahl aller Nullstellen gezählt mit Vielfachheiten. Dies lässt sich auf mehrere Unbekannte verallgemeinern. Sei $I = P_1 \cap \ldots \cap P_d$ eine Primärzerlegung von $I \trianglelefteq R := K[X_1, \ldots, X_n]$, sodass die Primideale $\sqrt{P_1}, \ldots, \sqrt{P_d}$ maximal sind. Jedes $\sqrt{P_i}$ entspricht dann einer Nullstelle $(x_1, \ldots, x_n) \in \mathcal{V}(I)$ und wir nennen $\dim_K R/P_i$ die *Vielfachheit* von $(x_1, \ldots, x_n)$. Ist P_i in einem maximalem Ideal $M \trianglelefteq R$ enthalten, so folgt $\sqrt{P_i} \subseteq \sqrt{M} = M$ und $M = \sqrt{P_i}$. Insbesondere ist $P_i + P_j = R$ für $i \neq j$. Die Anzahl der Nullstellen von I (gezählt mit Vielfachheiten) ist daher $\dim R/I = \dim(R/P_1) + \ldots + \dim(R/P_d)$ nach dem chinesischen Restsatz. Diese Zahl lässt sich mit Gröbnerbasen ausrechnen.

Definition III.2.70. Sei $\beta_1, \ldots, \beta_k$ eine Gröbnerbasis von $I \trianglelefteq K[X_1, \ldots, X_n]$. Man nennt

$$\mathcal{M} \setminus I = \mathcal{M} \setminus \operatorname{lm} I = \{\rho \in \mathcal{M} : \forall i : \beta_i \nmid \rho\}$$

die Menge der *Standard-Monome* bzgl. I.

Satz III.2.71. *Sei $I \trianglelefteq R := K[X_1, \ldots, X_n]$. Dann bilden die (Restklassen der) Standard-Monome eine K-Basis von R/I. Insbesondere ist die Anzahl der Standard-Monome gleich der Anzahl der Nullstellen von I.*

Beweis. Sei $\beta_1, \ldots, \beta_k$ eine Gröbnerbasis von I. Für $\alpha \in R$ sei $\delta \in R$ der (eindeutig bestimmte) Rest bei der Division von α durch $\beta_1, \ldots, \beta_k$. Jedes Monom ρ in δ ist durch keines der $\operatorname{lm} \beta_i$ teilbar. Dies zeigt $\rho \notin \operatorname{lm} I$, d. h. ρ ist ein Standard-Monom bzgl. I. Die (Restklassen der) Standard-Monome erzeugen daher R/I. Für die lineare Unabhängigkeit nehmen wir $\sum_{i=1}^{s} \lambda_i \rho_i \in I$ mit $\lambda_1, \ldots, \lambda_s \in K^\times$ und $\rho_1, \ldots, \rho_s \in \mathcal{M} \setminus I$ an. O. B. d. A. sei $\rho_1 > \ldots > \rho_s$. Dann wäre $\rho_1 \in \operatorname{lm} I$. □

3 Modulare Darstellungstheorie

Bemerkung III.3.1. In Kapitel II.13 haben wir gesehen, dass Moduln über der Gruppenalgebra $\mathbb{C}G$ im Wesentlichen durch ihren Charakter bestimmt sind. Über Körpern K mit positiver Charakteristik ist dies nach Maschke im Allgemeinen falsch, denn ein Charakter kann nicht zwischen halbeinfachen und unzerlegbaren Moduln mit den gleichen Kompositionsfaktoren unterscheiden. Tatsächlich kann der Charakter einer Darstellung sogar die Nullabbildung sein. Wir führen in diesem Kapitel einige neue Werkzeuge ein und bestimmen damit die Anzahl der einfachen und unzerlegbaren KG-Moduln. Wenn nichts anderes gesagt wird, seien Gruppen endlich, Algebren endlich-dimensional und Moduln endlich erzeugt.

Definition III.3.2. Für eine K-Algebra A sei $\gamma(A) := K\{ab - ba : a, b \in A\}$ der *Kommutatorraum* von A.

Bemerkung III.3.3. Achtung: $\gamma(A)$ ist weder ein Ideal noch ein Teilring von A.

Lemma III.3.4.

(i) Für K-Algebren A, B gilt $\gamma(A \times B) = \gamma(A) \times \gamma(B)$.

(ii) Für jede K-Algebra A und $I \trianglelefteq A$ gilt $\gamma(A/I) = (\gamma(A) + I)/I$.

(iii) Für $n \in \mathbb{N}$ gilt $\gamma(K^{n\times n}) = \{M \in K^{n\times n} : \operatorname{tr} M = 0\}$. Insbesondere ist $\dim_K(K^{n\times n}/\gamma(K^{n\times n})) = 1$.

Beweis.

(i) Für $a_1, a_2 \in A$ und $b_1, b_2 \in B$ gilt

$$(a_1, b_1)(a_2, b_2) - (a_2, b_2)(a_1, b_1) = (a_1a_2 - a_2a_1, b_1b_2 - b_2b_1) \in \gamma(A) \times \gamma(B).$$

(ii) Für $a, b \in A$ ist $(a + I)(b + I) - (b + I)(a + I) = ab - ba + I \in \gamma(A) + I$.

(iii) Für $a, b \in K^{n\times n}$ gilt bekanntlich $\operatorname{tr}(ab - ba) = \operatorname{tr}(ab) - \operatorname{tr}(ba) = 0$, d. h. $\gamma(K^{n\times n}) \subseteq \operatorname{Ker}(\operatorname{tr})$. Sei wie üblich $E_{st} = (\delta_{is}\delta_{jt})_{i,j} \in K^{n\times n}$. Für $s \neq t$ gilt

$$E_{st} = E_{s1}E_{1t} - E_{1t}E_{s1} \in \gamma(K^{n\times n}),$$
$$E_{ss} - E_{tt} = E_{st}E_{ts} - E_{ts}E_{st} \in \gamma(K^{n\times n}).$$

Offenbar bilden die Matrizen E_{st} $(s \neq t)$ und $E_{11} - E_{ss}$ $(2 \leq s \leq n)$ eine Basis von $\operatorname{Ker}(\operatorname{tr})$. Daher gilt $\operatorname{Ker}(\operatorname{tr}) \subseteq \gamma(K^{n\times n})$. Die zweite Behauptung folgt aus dem Homomorphiesatz für tr. □

Lemma III.3.5. *Sei $p := \operatorname{char} K > 0$ und A eine K-Algebra. Für $a, b \in A$ gilt:*

(i) $(a + b)^p \equiv a^p + b^p \pmod{\gamma(A)}$.

(ii) $a \in \gamma(A) \Longrightarrow a^p \in \gamma(A)$.

(iii) $\mathrm{J}(A) + \gamma(A) = \{a \in A : \exists n \in \mathbb{N} : a^{p^n} \in \gamma(A)\}$, *falls K algebraisch abgeschlossen ist.*

Beweis.

(i) Wenn man $(a+b)^p$ ausmultipliziert erhält man die Summe aller 2^p Terme der Form $c_1 \dots c_p$ mit $c_1, \dots, c_p \in \{a, b\}$.[1] Wegen

$$c_1 \dots c_p \equiv c_2 \dots c_p c_1 \equiv \dots \equiv c_p c_1 \dots c_{p-1} \pmod{\gamma(A)}$$

gilt

$$c_1 \dots c_p + c_2 \dots c_p c_1 + \dots + c_p c_1 \dots c_{p-1} \equiv p c_1 \dots c_p \equiv 0 \pmod{\gamma(A)}.$$

Modulo $\gamma(A)$ verbleiben in $(a+b)^p$ also nur die beiden Terme a^p und b^p.

(ii) Nach (i) können wir $a = bc - cb$ mit $c \in A$ annehmen. Dann gilt

$$a^p \equiv (bc)^p - (cb)^p \equiv bc \dots bc - cb \dots cb \equiv 0 \pmod{\gamma(A)}.$$

(iii) Nach (i) ist $T := \{a \in A : \exists n \in \mathbb{N} : a^{p^n} \in \gamma(A)\}$ ein Vektorraum. Da $\mathrm{J}(A)$ nilpotent ist, gilt $\mathrm{J}(A) \subseteq T$. Aus (ii) folgt $\gamma(A) \subseteq T$, also $\mathrm{J}(A) + \gamma(A) \subseteq T$. Nach Artin-Wedderburn und Lemma II.12.6 gilt $A/\mathrm{J}(A) \cong K^{n_1 \times n_1} \times \dots \times K^{n_k \times n_k}$. Zusammen mit Lemma III.3.4 ergibt sich

$$(\gamma(A) + \mathrm{J}(A))/\mathrm{J}(A) = \gamma(A/\mathrm{J}(A)) \cong \gamma(K^{n_1 \times n_1}) \times \dots \times \gamma(K^{n_k \times n_k}) \tag{III.3.1}$$

und $\dim A/(\gamma(A) + \mathrm{J}(A)) = k$. Andererseits sind die Idempotente

$$(E_{11}, 0, \dots, 0), \dots, (0, \dots, 0, E_{11}) \in K^{n_1 \times n_1} \times \dots \times K^{n_k \times n_k}$$

offenbar linear unabhängig modulo T. Dies zeigt $\dim A/T \geq k$ und $T \subseteq \gamma(A) + \mathrm{J}(A)$. □

Folgerung III.3.6. *Sei K algebraisch abgeschlossen mit Charakteristik $p > 0$ und A eine K-Algebra. Dann ist* $\dim A/(\gamma(A) + \mathrm{J}(A)) = \dim \mathrm{Z}(A/\mathrm{J}(A))$ *die Anzahl der einfachen A-Moduln (bis auf Isomorphie).*

Beweis. Folgt aus (III.3.1) im obigen Beweis. □

Definition III.3.7. Sei $p \in \mathbb{P}$. Man nennt $x \in G$ ein *p'-Element*, falls $p \nmid |\langle x \rangle|$. Sei G_p (bzw. $G_{p'}$) die Menge der p-Elemente (bzw. p'-Elemente) von G. Dann gilt $G_p \cap G_{p'} = \{1\}$, aber $G \neq G_p \cup G_{p'}$ im Allgemeinen. Man nennt $C \in \mathrm{Cl}(G)$ eine *p-Konjugationsklasse* (bzw. *p'-Konjugationsklasse*), falls $C \subseteq G_p$ (bzw. $C \subseteq G_{p'}$) (beachte: konjugierte Elemente haben die gleiche Ordnung).

Lemma III.3.8. *Jedes Element $x \in G$ lässt sich eindeutig in der Form $x = x_p x_{p'} = x_{p'} x_p$ mit $x_p \in G_p$ und $x_{p'} \in G_{p'}$ schreiben. Man nennt x_p den* p-Faktor *und $x_{p'}$ den* p'-Faktor *von G.*

Beweis. Sei $|\langle x \rangle| = p^a m$ mit $p \nmid m$. Dann existieren $\alpha, \beta \in \mathbb{Z}$ mit $\alpha p^a + \beta m = \mathrm{ggT}(p^a, m) = 1$. Für $x_p := x^{\beta m} \in G_p$ und $x_{p'} := x^{\alpha p^a} \in G_{p'}$ gilt $x = x^{\alpha p^a + \beta m} = x_p x_{p'} = x_{p'} x_p$.

Seien $y \in G_p$ und $z \in G_{p'}$ mit $x = yz = zy$. Dann sind y und z mit x, x_p und $x_{p'}$ vertauschbar. Es folgt $y^{-1} x_p = z x_{p'}^{-1} \in G_p \cap G_{p'} = \{1\}$, d. h. $y = x_p$ und $z = x_{p'}$. □

[1] Da a und b nicht unbedingt vertauschbar sind, darf man die binomische Formel nicht benutzen.

Bemerkung III.3.9. Für $x, g \in G$ gilt $(gxg^{-1})_p = gx_pg^{-1}$ und $(gxg^{-1})_{p'} = gx_{p'}g^{-1}$.

Definition III.3.10. Für $x \in G$ sei

$$\mathrm{Sec}_{p'}(x) := \{y \in G : \exists g \in G : y_{p'} = gx_{p'}g^{-1}\} \subseteq G$$

die p'-*Sektion* von x. Nach Bemerkung III.3.9 ist $\mathrm{Sec}_{p'}(x)$ eine Vereinigung von Konjugationsklassen von G.

Lemma III.3.11. *Für jeden algebraisch abgeschlossenen Körper K der Charakteristik $p > 0$ gilt*

$$\gamma(KG) = \Big\{\sum_{g\in G} \alpha_g g : \forall C \in \mathrm{Cl}(G) : \sum_{c\in C} \alpha_c = 0\Big\},$$
$$\gamma(KG) + \mathrm{J}(KG) = \Big\{\sum_{g\in G} \alpha_g g : \forall x \in G : \sum_{s\in \mathrm{Sec}_{p'}(x)} \alpha_s = 0\Big\}$$

Beweis.

(i) Sei Γ die rechte Seite der Gleichung. Für $g, h \in G$ gilt $gh - hg = gh - g^{-1}(gh)g \in \Gamma$. Daraus folgt $\gamma(KG) \subseteq \Gamma$. Sei umgekehrt $\sum_{g\in G} \alpha_g g \in \Gamma$ und $x_C \in C \in \mathrm{Cl}(G)$. Für jedes $c \in C$ existiert $g \in G$ mit $c = gx_Cg^{-1}$. Dann gilt $c - x_C = (gx_C)g^{-1} - g^{-1}(gx_C) \in \gamma(KG)$ und

$$\sum_{g\in G} \alpha_g g = \sum_{C\in \mathrm{Cl}(G)} \sum_{c\in C} \alpha_c(c - x_C) \in \gamma(KG).$$

(ii) Sei $|G| = p^a m$ mit $p \nmid m$ und $k \geq a$ mit $p^k \equiv 1 \pmod m$ (z. B. $k = a\varphi(m)$). Dann gilt $g^{p^k} = g_p^{p^k} g_{p'}^{p^k} = g_{p'}$ für $g \in G$ nach Lagrange. Sei $\alpha := \sum_{g\in G} \alpha_g g \in KG$ und $x_1, \ldots, x_l$ ein Repräsentantensystem für die p'-Konjugationsklassen von G. Für $g \in \mathrm{Sec}_{p'}(x_i)$ gilt $g_{p'} \equiv x_i \pmod{\gamma(KG)}$ nach (i). Aus Lemma III.3.5 folgt

$$\alpha^{p^k} \equiv \sum_{g\in G} \alpha_g^{p^k} g_{p'} \equiv \sum_{i=1}^{l} x_i \sum_{s\in \mathrm{Sec}_{p'}(x_i)} \alpha_s^{p^k} \equiv \sum_{i=1}^{l} x_i \Big(\sum_{s\in \mathrm{Sec}_{p'}(x_i)} \alpha_s\Big)^{p^k} \pmod{\gamma(KG)}. \qquad \text{(III.3.2)}$$

Gilt $\sum_{s\in \mathrm{Sec}_{p'}(x_i)} \alpha_s = 0$ für alle i, so ergibt sich $\alpha^{p^k} \in \gamma(KG)$ und $\alpha \in \gamma(KG) + \mathrm{J}(KG)$ nach (III.3.5). Ist umgekehrt $\alpha^{p^n} \in \gamma(KG)$ für ein $n \in \mathbb{N}$, so existiert ein $k \geq \max\{a, n\}$ mit $k \equiv 1 \pmod m$. Dann folgt $\sum_{s\in \mathrm{Sec}_{p'}(x_i)} \alpha_s = 0$ aus (III.3.2) für $i = 1, \ldots, l$. □

Satz III.3.12 (Brauer)**.** *Sei K ein algebraisch abgeschlossener Körper der Charakteristik $p > 0$. Dann stimmt die Anzahl der einfachen KG-Moduln mit der Anzahl der p'-Konjugationsklassen von G überein.*

Beweis. Offenbar stimmt die Anzahl l der p'-Konjugationsklassen mit der Anzahl der p'-Sektionen überein. Nach Lemma III.3.11 ist $\dim KG/(\gamma(KG) + \mathrm{J}(KG)) = l$ und die Behauptung folgt aus Folgerung III.3.6. □

Bemerkung III.3.13.

(i) Sei K ein beliebiger Körper und

$$(n, S) := \begin{cases} (|G|, G) & \text{falls } \operatorname{char} K = 0, \\ (|G|_{p'}, G_{p'}) & \text{falls } \operatorname{char} K = p. \end{cases}$$

Sei $\zeta \in \overline{K}$ eine primitive n-te Einheitswurzel und

$$Z := \{a + n\mathbb{Z} : \exists \gamma \in \operatorname{Gal}(K(\zeta)|K) : \gamma(\zeta) = \zeta^a\} \leq (\mathbb{Z}/n\mathbb{Z})^\times.$$

Durch

$$x \sim y :\Longleftrightarrow \exists g \in G, a + n\mathbb{Z} \in Z : gxg^{-1} = y^a \qquad (x, y \in S)$$

erhält man eine Äquivalenzrelation auf S. Nach einem Satz von Berman ist die Anzahl der einfachen KG-Moduln gleich der Anzahl der Äquivalenzklassen von $\sim$ auf S.

(ii) Die explizite Bestimmung der einfachen Moduln ist in positiver Charakteristik deutlich schwieriger als in Charakteristik 0. Zum Beispiel kennt man nicht einmal die Dimensionen der einfachen $\mathbb{F}_2 S_{20}$-Moduln.

Beispiel III.3.14.

(i) Ist K algebraisch abgeschlossen, so ist $\zeta \in K$ und $A = 1$ in Bemerkung III.3.13. Man erhält also Brauers Satz (bzw. Bemerkung II.12.39) zurück.

(ii) Für $K = \mathbb{Q}$ ist $A = (\mathbb{Z}/n\mathbb{Z})^\times$ und $x \sim y \iff \langle x \rangle = \langle y \rangle$. Die Anzahl der einfachen $\mathbb{Q}G$-Moduln ist also die Anzahl von Konjugationsklassen zyklischer Untergruppen von G.

(iii) Für $K = \mathbb{R}$ gilt $A = \langle -1 + n\mathbb{Z} \rangle$. Sei r die Anzahl der Konjugationsklassen $C = C^{-1}$ und $2s$ die Anzahl der Konjugationsklassen $C \neq C^{-1}$. Dann ist $r + s$ die Anzahl der einfachen $\mathbb{R}G$-Moduln. Ist $|G|$ ungerade, so ist $r = 1$ und es gibt genau $(k(G) + 1)/2$ einfache $\mathbb{R}G$-Moduln.

Satz III.3.15. *Für jeden Körper K der Charakteristik $p > 0$ gilt:*

(i) KG ist genau dann lokal, wenn G eine p-Gruppe ist.

(ii) Ist $G \cong C_{p^n}$, so besitzt KG genau p^n unzerlegbare KG-Moduln bis aus Isomorphie. Diese haben die Dimensionen $1, 2, \ldots, p^n$.

(iii) Ist G eine nicht-zyklische p-Gruppe, so besitzt KG unzerlegbare Moduln in jeder Dimension $d \in \mathbb{N}$.

Beweis.

(i) Nehmen wir zuerst an, dass G keine p-Gruppe ist. Nach Cauchy existiert eine Untergruppe $1 \neq H \leq G$ mit $|H| \not\equiv 0 \pmod{p}$, d. h. $|H|^{-1} \in K$. Man sieht leicht, dass $\frac{1}{|H|} \sum_{x \in H} x \in KG \setminus \{0, 1\}$ ein Idempotent ist. Nach Satz II.12.11 ist KG nicht lokal.

Sei nun G eine p-Gruppe. Bekanntlich enthält K den Primkörper $\mathbb{F}_p$. Sei M ein einfacher KG-Modul und

$$L := \sum_{g \in G} \mathbb{F}_p gm \subseteq M$$

für ein festes $m \in M \setminus \{0\}$. Offenbar ist L ein endlicher $\mathbb{F}_p$-Vektorraum. Insbesondere ist $|L|$ eine p-Potenz. Für $x \in G$ gilt $xL = \sum_{g \in G} \mathbb{F}_p xgm = L$. Daher operiert G auf L durch Linksmultiplikation. Sicher ist $0 \in L$ ein Fixpunkt von G. Da sowohl $|G|$ als auch $|L|$ Potenzen von p sind, muss G nach

der Bahnengleichung einen weiteren Fixpunkt $a \in L \setminus \{0\}$ haben. Nun ist Ka ein Untermodul des einfachen Moduls M und es folgt $M = Ka \simeq K$. Nach Bemerkung II.12.37 ist KG lokal.

(ii) Sei $G = \langle g \rangle$ und V ein unzerlegbarer KG-Modul. Das Minimalpolynom μ der linearen Abbildung $f\colon V \to V$, $v \mapsto gv$ teilt $X^{p^n} - 1 = (X-1)^{p^n}$. Also gilt $\mu = (X-1)^k$ für ein $1 \leq k \leq p^n$. Nach linearer Algebra existiert eine f-invariante Zerlegung $V = U \oplus W$, sodass $f_{|U}$ dem Jordanblock $J_k(1)$ entspricht (der Beweis benutzt Induktion nach k und funktioniert auch für $\dim V = \infty$).[2] Da V unzerlegbar ist, gilt $W = 0$ und $\dim V = \dim U = k$. Außerdem ist V bis auf Isomorphie eindeutig bestimmt. Umgekehrt kann man zu jedem $1 \leq k \leq p^n$ den Vektorraum $V := K^k$ durch $gv := J_k(1)v$ für $v \in V$ in einen KG-Modul umwandeln. Wegen der Eindeutigkeit der Jordanschen Normalform ist V unzerlegbar.

(iii) Nach Sylow besitzt G eine Untergruppe H mit Index p. Nach Aufgabe I.25 ist $H \trianglelefteq G$. Sei $x \in G \setminus H$. Da G nicht zyklisch ist, liegt x in einer maximalen Untergruppe $L \neq H$. Wir zeigen $|G : L| = p$ durch Induktion nach $|G|$. Dies ist klar für $|G| = p^2$. Nach Satz I.4.11 ist $Z := \mathrm{Z}(G) \neq 1$. Im Fall $Z \leq L$ ist L/Z maximal in G/Z nach dem Korrespondenzsatz. Induktion zeigt $|G : L| = |G/Z : L/Z| = p$. Sei also $Z \not\subseteq L$. Dann ist $G = LZ$, da L maximal ist. Aus $L, Z \subseteq \mathrm{N}_G(L)$ folgt $L \trianglelefteq G$. Nun ist G/L eine einfache p-Gruppe, also $|G : L| = p$ nach Beispiel I.6.3.

Nach Aufgabe I.25 ist auch $L \trianglelefteq G$ und $N := H \cap L \trianglelefteq G$. Es gilt

$$G/N = H/N \oplus L/N \cong C_p^2.$$

Ist U ein unzerlegbarer $K[G/N]$-Modul, so wird U durch $gu := (gN)u$ für $g \in G$ und $u \in U$ zu einem unzerlegbaren KG-Modul. Wir können daher $G = \langle g, h \rangle \cong C_p^2$ annehmen.

Wir konstruieren zunächst unzerlegbare Moduln in Dimension $2d$. Sei V_{2d} der K-Vektorraum mit Basis $b_1, \ldots, b_d, c_1, \ldots, c_d$. Seien $\alpha, \beta \in \mathrm{End}(V_{2d})$ mit

$$\alpha(b_i) = c_i, \quad \beta(b_j) = c_{j+1}, \quad \alpha(c_i) = \beta(c_i) = \beta(b_d) = 0 \quad (i = 1, \ldots, d,\ j = 1, \ldots, d-1).$$

Offenbar gilt $\alpha^2 = \beta^2 = \alpha\beta = \beta\alpha = 0$. Es folgt $(\mathrm{id} + \alpha)^p = \mathrm{id} + \alpha^p = \mathrm{id} = (\mathrm{id} + \beta)^p$. Daher definiert $\Delta\colon G \to \mathrm{GL}(V_{2d})$ mit $\Delta(g) = \mathrm{id} + \alpha$ und $\Delta(h) = \mathrm{id} + \beta$ eine Darstellung. Sei $f \in \mathrm{End}_{KG}(V_{2d})$ mit Matrix $M = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in K^{2d \times 2d}$ bzgl. der angegebenen Basis. Sei $J = J_d(0) \in K^{d \times d}$. Wegen $f(gv) = gf(v)$ für $v \in V_{2d}$ ist f mit α und β vertauschbar, d. h.

$$\begin{pmatrix} 0 & 0 \\ A & B \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1_n & 0 \end{pmatrix} \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \alpha M = M\alpha = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1_n & 0 \end{pmatrix} = \begin{pmatrix} B & 0 \\ D & 0 \end{pmatrix}$$
$$\begin{pmatrix} 0 & 0 \\ JA & JB \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ J & 0 \end{pmatrix} \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \beta M = M\beta = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} 0 & 0 \\ J & 0 \end{pmatrix} = \begin{pmatrix} BJ & 0 \\ DJ & 0 \end{pmatrix}.$$

Es folgt $A = D$, $B = 0$ und $AJ = JA$. Insbesondere ist M eine untere Dreiecksmatrix. Mit $A = (a_{ij})$ gilt konkret

$$\begin{pmatrix} a_{12} & \cdots & a_{1,n-1} & 0 \\ \vdots & & \vdots & \vdots \\ a_{n2} & \cdots & a_{n,n-1} & 0 \end{pmatrix} = AJ = JA = \begin{pmatrix} 0 & \cdots & 0 \\ a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n-1,1} & \cdots & a_{n-1,n} \end{pmatrix}.$$

Es folgt $a_{11} = \ldots = a_{nn}$. Im Fall $a_{11} \neq 0$ ist f invertierbar und anderenfalls ist f nilpotent. Also ist $\mathrm{End}_{KG}(V_{2d})$ lokal und V_{2d} unzerlegbar nach Bemerkung II.12.12.

[2] Siehe Satz 12.12 in meinem Skript Lineare Algebra A & B.

Für ungerade Dimension $2d+1$ erweitern wir V_{2d} zu $V_{2d+1} := V_{2d} \oplus Kc_{d+1}$ und setzen

$$\alpha(b_i) = c_i, \qquad \beta(b_i) = c_{i+1}, \qquad \alpha(c_j) = \beta(c_j) = 0 \qquad (i = 1, \dots, d,\ j = 1, \dots, d+1)$$

(da der triviale Modul unzerlegbar ist, können wir $d \geq 1$ annehmen). Eine ähnliche Rechnung zeigt $M = \left(\begin{smallmatrix} A & 0 \\ C & D \end{smallmatrix}\right)$ mit $A \in K^{d\times d}$, $C \in K^{(d+1)\times d}$ und

$$D = \begin{pmatrix} A & * \\ 0 & * \end{pmatrix} = \begin{pmatrix} * & 0 \\ * & A \end{pmatrix} = \begin{pmatrix} a_{11} & & 0 \\ & \ddots & \\ * & & a_{11} \end{pmatrix} \in K^{(d+1)\times(d+1)}.$$

Also ist auch V_{2d+1} unzerlegbar. □

Bemerkung III.3.16.

(i) Besitzt eine Algebra A nur endlich viele unzerlegbare Moduln bis auf Isomorphie, so sagt man: A hat endlichen *Darstellungstyp*. Die von Roiter bewiesene *Brauer-Thrall-Vermutung* besagt, dass eine Algebra von unendlichem Darstellungstyp unzerlegbare Moduln mit beliebig großer Dimension besitzt. Ist K algebraisch abgeschlossen, so gibt es ggf. unendlich viele $d \in \mathbb{N}$ mit unendlich vielen nicht-isomorphen unzerlegbaren Moduln in Dimension d (zweite Brauer-Thrall-Vermutung; vgl. Aufgabe III.16).

(ii) Für $\operatorname{char} K = p$ und $G = \langle g \rangle \cong C_{p^n}$ ist $KG \to K[X]/(X^{p^n})$, $g \mapsto 1+X+(X^{p^n})$ ein Isomorphismus von Algebren (vgl. Aufgabe II.63). Analog gilt $KC_p^2 \cong K[X,Y]/(X^p, Y^p)$.

Definition III.3.17.

(i) Für K-Vektorräume V und W mit Basen $b_1, \dots, b_n$ und $c_1, \dots, c_m$ sei $V \otimes W$ ein K-Vektorraum mit Basis $\{b_i \otimes c_j : i = 1, \dots, n,\ j = 1, \dots, m\}$. Man nennt $V \otimes W$ das *Tensorprodukt* von V und W. Für $v = \sum_{i=1}^n \lambda_i b_i$ und $w = \sum_{j=1}^m \mu_j c_j$ definiert man $v \otimes w := \sum_{i,j} \lambda_i \mu_j (b_i \otimes c_j)$.

(ii) Seien nun V und W zusätzlich KG-Moduln. Für $g \in G$ definiert $\gamma_g(b_i \otimes c_j) := gb_i \otimes gc_j$ eine lineare Abbildung auf $V \otimes W$. Für $v = \sum_{i=1}^n \lambda_i b_i$ und $w = \sum_{j=1}^m \mu_j c_j$ gilt

$$\gamma_g(v \otimes w) = \gamma_g\Big(\sum_{i,j} \lambda_i \mu_j (b_i \otimes c_j)\Big) = \sum_{i,j} \lambda_i \mu_j (gb_i \otimes gc_j) = gv \otimes gw.$$

Daher ist $\Delta\colon G \to \mathrm{GL}(V \otimes W)$, $g \mapsto \gamma_g$ eine Darstellung und $V \otimes W$ wird durch $g(v \otimes w) := gv \otimes gw$ zu einem KG-Modul.

Bemerkung III.3.18.

(i) Tensorprodukte von Moduln beliebiger Algebren und Ringe sind deutlich aufwendiger zu definieren (siehe Aufgabe II.52 und Definition III.6.14).

(ii) Für KG-Moduln U, V, W zeigt man leicht, dass die folgenden kanonischen Abbildungen Isomorphismen sind:

- $K \otimes V \simeq V$.
- $V \otimes W \simeq W \otimes V$.
- $U \otimes (V \otimes W) \simeq (U \otimes V) \otimes W$.
- $U \otimes (V \times W) \simeq (U \otimes V) \times (U \otimes W)$.

(iii) Seien $\Delta\colon G \to \mathrm{GL}(n,K)$ und $\Gamma\colon G \to \mathrm{GL}(m,K)$ die Darstellungen von V und W bzgl. der Basen $b_1,\dots,b_n$ bzw. $c_1,\dots,c_m$. Sei $g \in G$ und $\Delta(g) = (a_{ij}) \in K^{n\times n}$, d. h. $gb_i = \sum_{j=1}^n a_{ji}b_j$. Dann ist die zu $V \otimes W$ gehörende Darstellung $\Delta \otimes \Gamma$ bzgl. $b_1 \otimes c_1, b_1 \otimes c_2, \dots, b_n \otimes c_m$ durch

$$(\Delta \otimes \Gamma)(g) = \Delta(g) \otimes \Gamma(g) := \begin{pmatrix} a_{11}\Gamma(g) & \cdots & a_{1n}\Gamma(g) \\ \vdots & & \vdots \\ a_{na}\Gamma(g) & \cdots & a_{nn}\Gamma(g) \end{pmatrix} \in K^{nm\times nm}$$

gegeben (Kronecker-Produkt).

(iv) Sei nun $K = \mathbb{C}$. Für den Charakter von $\Delta \otimes \Gamma$ gilt dann

$$\chi_{\Delta\otimes\Gamma}(g) = a_{11}\operatorname{tr}\Gamma(g) + \ldots + a_{nn}\operatorname{tr}\Gamma(g) = \chi_\Delta(g)\chi_\Gamma(g)$$

für $g \in G$ (vgl. Satz II.13.38).

Satz III.3.19 (Universelle Eigenschaft des Tensorprodukts)**.** *Seien U, V und W KG-Moduln und $f\colon V \times W \to U$ eine bilineare Abbildung mit $gf(v,w) = f(gv,gw)$ für alle $g \in G$, $v \in V$ und $w \in W$. Dann existiert genau ein Homomorphismus $\hat{f}\colon V \otimes W \to U$ mit $\hat{f}(v \otimes w) = f(v,w)$ für alle $v \in V$ und $w \in W$.*

Beweis. Seien $b_1,\dots,b_n$ und $c_1,\dots,c_m$ Basen von V bzw. W. Wir definieren $\hat{f}(b_i \otimes c_j) := f(b_i,c_j)$ und setzen linear fort. Dann gilt $\hat{f}(v \otimes w) = f(v,w)$ für alle $v \in V$ und $w \in W$. Für $g \in G$ gilt

$$\hat{f}(g(v \otimes w)) = \hat{f}(gv \otimes gw) = f(gv,gw) = gf(v,w) = g\hat{f}(v \otimes w),$$

d. h. $\hat{f}$ ist ein Homomorphismus von KG-Moduln. Da $V \otimes W$ von $b_i \otimes c_j$ erzeugt wird, ist $\hat{f}$ eindeutig bestimmt. □

Lemma III.3.20. *Für KG-Moduln U, V, W mit $U \le V$ gilt $W \otimes (V/U) \simeq (W \otimes V)/(W \otimes U)$.*

Beweis. Die bilineare Abbildung $f\colon W \times V \to W \otimes (V/U)$, $(w,v) \mapsto w \otimes (v+U)$ erfüllt $gf(w,v) = gw \otimes g(v+U) = f(gw,gv)$. Daher existiert ein Epimorphismus $\hat{f}\colon W \otimes V \to W \otimes (V/U)$, $w \otimes v \mapsto w \otimes (v+U)$ mit $W \otimes U \le \operatorname{Ker}(\hat{f})$. Wegen $\dim(W \otimes (V/U)) = \dim W \dim(V/U) = \dim W \dim V - \dim W \dim U$ gilt $\operatorname{Ker}(\hat{f}) = W \otimes U$. □

Bemerkung III.3.21.

(i) Seien V und W KG-Moduln. Für $g \in G$, $\varphi \in \mathrm{Hom}_K(V,W)$ und $v \in V$ definieren wir

$$\gamma_g(\varphi)(v) := g\varphi(g^{-1}v)$$

wie im Beweis von Satz II.13.38. Für $g,h \in G$ gilt

$$\gamma_{gh}(\varphi)(v) = gh\varphi(h^{-1}g^{-1}v) = g\gamma_h(\varphi)(g^{-1}v) = \gamma_g(\gamma_h(\varphi))(v).$$

Daher ist $\Delta\colon G \to \mathrm{GL}(\mathrm{Hom}_K(V,W))$, $g \mapsto \gamma_g$ eine Darstellung und $\mathrm{Hom}_K(V,W)$ wird durch $(g\varphi)(v) := g\varphi(g^{-1}v)$ zu einem KG-Modul der Dimension $\dim(V)\dim(W)$.

(ii) Wählt man den trivialen Modul $W = K$, so erhält man den *Dualraum* $V^* := \mathrm{Hom}_K(V,K)$ mit $(g\varphi)(v) = \varphi(g^{-1}v)$ für $g \in G$, $\varphi \in V^*$ und $v \in V$. Man spricht dann vom *dualen* Modul zu V. Im Fall $V \simeq V^*$ nennt man V *selbstdual*.

(iii) Für Untermoduln $U \leq V$ und $W \leq V^*$ sei

$$U^\perp := \{\varphi \in V^* : \varphi(U) = 0\}, \qquad W_\perp := \{v \in V : \forall \varphi \in W : \varphi(w) = 0\}.^3$$

Für $g \in G$, $\varphi \in U^\perp$, $\psi \in W_\perp$ und $v \in W_\perp$ gilt $(g\varphi)(U) = \varphi(g^{-1}U) = \varphi(U) = 0$ und $\psi(gv) = g^{-1}\psi(v) = 0$. Dies zeigt, dass $U^\perp$ und $W_\perp$ Untermoduln von V^* bzw. V sind. Nach linearer Algebra ist

$$\dim U + \dim U^\perp = \dim V = \dim V^* = \dim W + \dim W_\perp.$$

Nach Definition ist $U \subseteq (U^\perp)_\perp$ und $W \subseteq (W_\perp)^\perp$. Aus Dimensionsgründen gilt $U = (U^\perp)_\perp$ und $W = (W_\perp)^\perp$. Durch Einschränken erhält man außerdem $\boxed{V^*/U^\perp \simeq U^*.}$

(iv) Nach linearer Algebra ist die Abbildung $\Phi\colon V \to V^{**}$, $v \mapsto \Phi_v$ mit $\Phi_v(\varphi) = \varphi(v)$ ein Vektorraum-Isomorphismus. Für $g \in G$, $v \in V$ und $\varphi \in V^*$ gilt

$$\Phi(gv)(\varphi) = \varphi(gv) = (g^{-1}\varphi)(v) = \Phi(v)(g^{-1}\varphi) = (g\Phi(v))(\varphi).$$

Dies zeigt, dass Φ auch ein Isomorphismus von KG-Moduln ist. Für $v \in V$ und $W \leq V^*$ gilt

$$v \in W_\perp \iff \forall \varphi \in W : \varphi(v) = 0 \iff \forall \varphi \in W : \Phi_v(\varphi) = 0 \iff \Phi_v \in W^\perp.$$

Daher ist $\Phi(W_\perp) = W^\perp$. Aus (iii) erhält man $\boxed{V/W_\perp \simeq V^{**}/W^\perp \simeq W^*.}$

(v) Ist $f\colon V \to W$ ein Homomorphismus von KG-Moduln, so auch die *duale* Abbildung $f^*\colon W^* \to V^*$, $\varphi \mapsto \varphi \circ f$, denn

$$f^*(g\varphi)(v) = (g\varphi)(f(v)) = \varphi(g^{-1}f(v)) = \varphi(f(g^{-1}v)) = f^*(\varphi)(g^{-1}v) = (g(f^*(\varphi)))(v)$$

für $g \in G$, $\varphi \in W^*$ und $v \in V$. Insbesondere gilt

$$V \simeq W \Longrightarrow V^* \simeq W^* \Longrightarrow V \simeq V^{**} \simeq W^{**} \simeq W.$$

Seien $\Phi\colon V \to V^{**}$ und $\Psi\colon W \to W^{**}$ die Isomorphismen aus (iv). Für $\varphi \in W^*$ und $v \in V$ gilt $(\Phi(v) \circ f^*)(\varphi) = \Phi(v)(\varphi \circ f) = \varphi(f(v))$ und

$$(\Psi^{-1} \circ f^{**} \circ \Phi)(v) = \Psi^{-1}(\Phi(v) \circ f^*) = f(v).$$

Daher ist $\mathrm{Hom}_{KG}(V, W) \to \mathrm{Hom}_{KG}(W^*, V^*)$, $f \mapsto f^*$ ein Vektorraum-Isomorphismus.

(vi) Sei $\Delta\colon G \to \mathrm{GL}(n, K)$ eine Darstellung zu V bzgl. einer Basis $b_1, \ldots, b_n$. Sei $g \in G$ und $g^{-1}b_i = \sum_{j=1}^n a_{ji}b_j$. Sei $\beta_1, \ldots, \beta_n$ die entsprechende duale Basis von V^*, d. h. es gilt $\beta_i(b_j) = \delta_{ij}$ für $1 \leq i, j \leq n$. Dann folgt $(g\beta_i)(b_j) = \beta_i(g^{-1}b_j) = a_{ij}$ und $g\beta_i = \sum_{j=1}^n a_{ij}\beta_j$. Für die zu V^* gehörende Darstellung $\Delta^*\colon G \to \mathrm{GL}(n, K)$ bzgl. $\beta_1, \ldots, \beta_n$ gilt also $\Delta^*(g) = \Delta(g^{-1})^{\mathrm{t}}$ für $g \in G$ (vgl. Beispiel II.13.4). Im Fall $K = \mathbb{C}$ gilt für den Charakter bekanntlich $\chi_{\Delta^*} = \overline{\chi_\Delta}$. Insbesondere ist V genau dann selbstdual, wenn χ_Δ reell ist.

Lemma III.3.22. *Für KG-Moduln U, V, W gilt*

(i) $(V \times W)^* \simeq V^* \times W^*$ *und* $(V \otimes W)^* \simeq V^* \otimes W^*$.

(ii) $\mathrm{Hom}_K(V, W) \simeq V^* \otimes W$.

(iii) $\mathrm{Hom}_K(U \otimes V, W) \simeq \mathrm{Hom}_K(U, \mathrm{Hom}_K(V, W))$.

[2]Die Bilinearform $V \times V^*\colon (v, \varphi) \mapsto \varphi(v)$ erklärt die Verwendung des Symbols $\perp$.

Beweis.

(i) Die Abbildung $(V \times W)^* \to V^* \times W^*$, $\varphi \mapsto (\varphi_{|V}, \varphi_{|W})$ ist offenbar Monomorphismus von KG-Modul. Aus Dimensionsgründen ist es ein Isomorphismus. Seien $\varphi \in V^*$ und $\psi \in W^*$. Nach der universellen Eigenschaft für Tensorprodukte von Vektorräumen existiert $f_{\varphi,\psi} \in (V \otimes W)^*$ mit $f_{\varphi,\psi}(v \otimes w) := \varphi(v)\psi(w)$. Die bilineare Abbildung $f\colon V^* \times W^* \to (V \otimes W)^*$, $(\varphi, \psi) \mapsto f_{\varphi,\psi}$ erfüllt

$$\begin{aligned} f(g\varphi, g\psi)(v \otimes w) &= f_{g\varphi,g\psi}(v \otimes w) = (g\varphi)(v)(g\psi)(w) = \varphi(g^{-1}v)\psi(g^{-1}w) \\ &= f_{\varphi,\psi}(g^{-1}(v \otimes w)) = (gf(\varphi, \psi))(v \otimes w). \end{aligned}$$

Aus der universellen Eigenschaft erhält man einen Homomorphismus

$$\begin{aligned} \hat{f}\colon V^* \otimes W^* &\to (V \otimes W)^*, \\ \varphi \otimes \psi &\mapsto f_{\varphi,\psi}. \end{aligned}$$

Seien $b_1, \ldots, b_n$ und $c_1, \ldots, c_m$ Basen von V bzw. W. Seien $\beta_1, \ldots, \beta_n$ und $\gamma_1, \ldots, \gamma_m$ die entsprechenden dualen Basen von V^* und W^*. Sei $\alpha \in (V \otimes W)^*$ mit $\alpha(b_i \otimes c_j) := \alpha_{ij}$. Für $\rho := \sum_{i,j} \alpha_{ij}\beta_i \otimes \gamma_j \in V^* \otimes W^*$ gilt

$$\hat{f}(\rho)(b_s \otimes c_t) = \sum_{i,j} \alpha_{ij}\beta_i(b_s)\gamma_j(c_t) = \alpha_{st} = \alpha(b_s \otimes c_t) \qquad (s = 1, \ldots, n,\ t = 1, \ldots, m).$$

Also ist $\hat{f}$ surjektiv und aus Dimensionsgründen auch injektiv.

(ii) Für $\varphi \in V^*$ und $w \in W$ sei $f_{\varphi,w}\colon V \to W$, $v \mapsto \varphi(v)w$. Offenbar ist $f_{\varphi,w} \in \mathrm{Hom}_K(V, W)$ und die Abbildung $f\colon V^* \times W \to \mathrm{Hom}_K(V, W)$, $(\varphi, w) \mapsto f_{\varphi,w}$ ist bilinear. Für $g \in G$ gilt

$$f(g\varphi, gw)(v) = (g\varphi)(v)(gw) = g\varphi(g^{-1}v)w = (gf_{\varphi,w})(v).$$

Die universelle Eigenschaft liefert einen Homomorphismus

$$\begin{aligned} \hat{f}\colon V^* \otimes W &\to \mathrm{Hom}_K(V, W), \\ \varphi \otimes w &\mapsto f_{\varphi,w}. \end{aligned}$$

Seien $b_1, \ldots, b_n$ und $c_1, \ldots, c_m$ Basen von V bzw. W. Sei $\varphi \in \mathrm{Hom}_K(V, W)$ mit $\varphi(b_i) = \sum_{j=1}^m \lambda_{ij}c_j$ und $\lambda_{ij} \in K$. Sei $\beta_1, \ldots, \beta_n$ die duale Basis von V^*. Wir definieren $\rho := \sum_{i,j} \lambda_{ij}\beta_i \otimes c_j \in V^* \otimes W$. Dann gilt

$$\hat{f}(\rho)(b_k) = \sum_{i,j} \lambda_{ij}\beta_i(b_k)c_j = \sum_{j=1}^m \lambda_{kj}c_j = \varphi(b_k)$$

für $k = 1, \ldots, m$. Also ist $\hat{f}$ surjektiv und aus Dimensionsgründen auch injektiv.

(iii) Es gilt

$$\begin{aligned} \mathrm{Hom}_K(U \otimes V, W) &\overset{\text{(ii)}}{\simeq} (U \otimes V)^* \otimes W \overset{\text{(i)}}{\simeq} U^* \otimes V^* \otimes W \\ &\simeq U^* \otimes \mathrm{Hom}_K(V, W) \simeq \mathrm{Hom}_K(U, \mathrm{Hom}_K(V, W)). \end{aligned}$$

□

Satz III.3.23. *Für jeden KG-Modul V gilt*

(i) V ist genau dann einfach (bzw. unzerlegbar), wenn V^* es ist.

(ii) V ist genau dann frei (bzw. projektiv), wenn V^* es ist.

(iii) V ist genau dann projektiv-unzerlegbar, wenn V^* es ist.

Beweis. Wegen $V^{**} \simeq V$ genügt es jeweils eine Richtung zu beweisen.

(i) Sei V einfach und $W < V^*$. Dann ist $W_\perp = V$ und $W^* \simeq V/W_\perp \simeq 0$. Dies zeigt $W = 0$. Sei nun V unzerlegbar und $V^* = U \oplus W$. Dann gilt $V \simeq V^{**} \cong U^* \oplus W^*$ nach Lemma III.3.22. Wieder erhält man $U = 0$ oder $W = 0$.

(ii) Ist V frei, so besitzt V nach Lemma II.9.5 eine endliche Basis. Sei also $V \simeq (KG)^n$. Dann ist $V^* \simeq ((KG)^*)^n$. Die reguläre Darstellung $\Delta\colon G \to \mathrm{GL}(|G|, K)$ bildet auf Permutationsmatrizen ab und diese sind bekanntlich orthogonal. Daher ist $\Delta^* = \Delta$ und $(KG)^* \simeq KG$. Also ist V^* frei. Sei schließlich V projektiv. Dann existiert ein Epimorphismus $f\colon (KG)^n \to V$ und $V \times \mathrm{Ker}(f) \simeq (KG)^n$. Wegen $V^* \times \mathrm{Ker}(f)^* \simeq ((KG)^n)^* \simeq (KG)^n$ ist V^* projektiv.

(iii) Folgt aus (i) und (ii). □

Bemerkung III.3.24.

(i) Für eine beliebige Familie von KG-Moduln V_i $(i \in I)$ gilt $\left(\coprod_{i\in I} V_i\right)^* \simeq \times_{i\in I} V_i^*$. Ist V frei mit unendlichem Rang (oder halbeinfach), so muss V^* nicht frei (bzw. halbeinfach) sein.

(ii) In Aufgabe II.37 wurde der Sockel $\mathrm{Soc}(V)$ eines Moduls V als Summe aller einfachen Untermoduln definiert. Er verhält sich „dual“ zum Radikal $\mathrm{J}(V)$.

Lemma III.3.25. *Für jeden KG-Modul V ist* $\mathrm{Soc}(V)^\perp = \mathrm{J}(V^*)$ *und* $\mathrm{J}(V)^\perp = \mathrm{Soc}(V^*)$. *Folglich gilt* $\boxed{\mathrm{Soc}(V)^* \simeq V^*/\mathrm{J}(V^*)}$ *und* $\boxed{\mathrm{Soc}(V^*) \simeq (V/\mathrm{J}(V))^*.}$

Beweis. Nach Bemerkung III.3.21 sind die Abbildungen $U \mapsto U^\perp$ und $W \mapsto W_\perp$ zueinander inverse Bijektionen zwischen den Untermoduln von V und den Untermoduln von V^*. Dabei gilt $V^*/U^\perp \simeq U^*$ und $V/W_\perp \simeq W^*$. Nach Satz III.3.23 wird der größte halbeinfache Untermodul von V auf den kleinsten Untermodul von V^* mit halbeinfachen Faktormoduln abgebildet. Dies zeigt $\mathrm{Soc}(V)^\perp = \mathrm{J}(V^*)$ und analog $\mathrm{J}(V)^\perp = \mathrm{Soc}(V^*)$. Es folgt $\mathrm{Soc}(V)^* \simeq V^*/\mathrm{Soc}(V)^\perp = V^*/\mathrm{J}(V^*)$ und $\mathrm{Soc}(V^*) \simeq V/\mathrm{Soc}(V^*)_\perp = V/(\mathrm{J}(V)^\perp)_\perp = V/\mathrm{J}(V)$. □

Bemerkung III.3.26. Im nächsten Beweis benutzen wir die Linearform

$$\lambda\colon KG \to K, \qquad \sum_{g\in G} \alpha_g g \mapsto \alpha_1.$$

Für $a = \sum \alpha_g g$ und $b = \sum \beta_g g$ gilt

$$\lambda(ab) = \sum_{g\in G} \alpha_g \beta_{g^{-1}} = \sum_{h\in G} \beta_h \alpha_{h^{-1}} = \lambda(ba).$$

Durch $\beta\colon KG \times KG \to K$, $(a, b) \mapsto \lambda(ab)$ erhält man eine symmetrische, nicht-ausgeartete Bilinearform mit $\beta(ab, c) = \beta(a, bc)$ für alle $a, b, c \in KG$. Für einen Unterraum $U \leq KG$ sei $U^\perp := \{a \in KG : \beta(a, U) = 0\}$. Wie üblich gilt $|G| = \dim U + \dim U^\perp$.

Satz III.3.27. *Für jeden projektiv-unzerlegbaren KG-Modul P gilt* $\mathrm{Soc}(P) \simeq P/\mathrm{J}(P)$.

Beweis. Sei $e \in KG$ ein primitives Idempotent mit $P = KGe$. Nach Lemma III.3.25 ist $S := \mathrm{Soc}(P) \subseteq P$ ein einfacher KG-Modul. Sei $s = \sum_{g \in G} \alpha_g g \in S \setminus \{0\}$. Dann existiert ein $g \in G$ mit $\alpha_g \neq 0$. Mit Bemerkung III.3.26 folgt

$$\lambda(eg^{-1}s) = \lambda(g^{-1}se) = \lambda(g^{-1}s) = \alpha_g \neq 0.$$

Insbesondere ist $0 \neq eg^{-1}s \in S$ und $P \to S$, $x \mapsto xg^{-1}s$ ist ein nicht-trivialer Homomorphismus. Da S einfach ist, folgt $P/\mathrm{J}(P) \simeq S$. □

Satz III.3.28. *Ist K algebraisch abgeschlossen, so ist die Cartan-Matrix von KG symmetrisch.*

Beweis. Sei $C(KG) = (c_{ij})$. Sei $1 = e_1 + \ldots + e_n$ eine Zerlegung in paarweise orthogonale primitive Idempotente. O. B. d. A. seien $KGe_1, \ldots, KGe_k$ Repräsentanten der projektiv-unzerlegbaren KG-Moduln bis auf Isomorphie. Nach Bemerkung II.12.21 ist $c_{ij} = \dim e_i KG e_j$ für $1 \leq i, j \leq k$. Mit der Bilinearform β aus Bemerkung III.3.26 gilt

$$\beta(e_iKGe_j, e_sKGe_t) = \beta\big((e_iKGe_j)e_s, KGe_t\big) = 0 = \beta\big((e_sKGe_t)e_i, KGe_j\big) = \beta(e_sKGe_t, e_iKGe_j)$$

für alle $(s,t) \neq (j,i)$. Dies zeigt $\bigoplus_{(s,t)\neq(j,i)} e_sKGe_t \subseteq (e_iKGe_j)^\perp$ und

$$c_{ij} = \dim e_iKGe_j = |G| - \dim(e_iKGe_j)^\perp \leq |G| - \sum_{(s,t)\neq(j,i)} \dim e_sKGe_t = \dim e_jKGe_i = c_{ji}.$$

Aus Symmetriegründen gilt auch $c_{ji} \leq c_{ij}$. □

Bemerkung III.3.29.

(i) Sei $C(KG) = (c_{ij})$. Ist $c_{ii} = 1$, so folgt $c_{ij} = 0$ für alle $j \neq i$ aus Satz III.3.27.

(ii) Für $\mathrm{char}\, K = 0$ ist $C(KG) = 1_k$ nach Maschke. Im Allgemeinen kann man zeigen, dass $C = C(KG)$ positiv definit ist (falls $K = \overline{K}$). Im Fall $p := \mathrm{char}\, K > 0$ sind die Elementarteiler von C (als ganzzahlige Matrix) Potenzen von p. Insbesondere ist $\det C$ eine p-Potenz (ohne Beweis). Für beliebige Algebren ist die Cartan-Matrix im Allgemeinen nicht invertierbar (Aufgabe III.20).

(iii) Die Voraussetzung $K = \overline{K}$ in Satz III.3.28 ist notwendig:

$$C(\mathbb{F}_2 A_4) = \begin{pmatrix} 2 & 1 \\ 2 & 3 \end{pmatrix}, \qquad C(\mathbb{F}_4 A_4) = \begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 2 \end{pmatrix}.$$

Definition III.3.30. Für einen KG-Modul V und $H \leq G$ erhält man durch Einschränkung den KH-Modul V_H. Wir konstruieren umgekehrt aus einem KH-Modul U einen KG-Modul. Dafür betrachten wir den K-Vektorraum

$$U^G := (KG \otimes U)/\,\mathrm{Span}_K\big\{gh \otimes u - g \otimes hu : g \in G, h \in H, u \in U\big\}.$$

Im Folgenden werden wir die Elemente von U^G mit geeigneten Repräsentanten aus $KG \otimes U$ identifizieren. Es gilt dann $gh \otimes u = g \otimes hu$ für $g \in G$, $h \in KH$ und $u \in U$.

Lemma III.3.31. *Durch $x(g \otimes u) := xg \otimes u$ für $x, g \in G, u \in U$ wird U^G zu einem KG-Modul der Dimension $|G : H| \dim U$. Man nennt U^G den von U* induzierten *Modul.*

Beweis. Sei B eine Basis von U und R ein Repräsentantensystem für G/H. Für jedes $g \in G$ existieren $r \in R$ und $h \in H$ mit $g = rh$. Für $u \in U$ gilt dann $g \otimes u = r \otimes hu$. Daher wird U^G als K-Vektorraum von den Elementen der Form $r \otimes b$ mit $r \in R$ und $b \in B$ erzeugt. Insbesondere ist $\dim U^G \leq |G : H| \dim U$. Für $r, s \in R$ definieren wir eine K-lineare Abbildung $\varphi_r \colon KG \otimes U \to U$, $sh \otimes b \mapsto \delta_{rs} hb$ mit $h \in H$ und $b \in B$. Dann ist

$$\begin{aligned} \varphi \colon KG \otimes U &\to U^{|G:H|}, \\ x &\mapsto (\varphi_r(x))_{r \in R} \end{aligned}$$

K-linear und surjektiv. Wegen $\varphi_r(rh \otimes u - r \otimes hu) = hu - hu = 0$ gilt $gh \otimes u - g \otimes hu \in \operatorname{Ker}(\varphi)$ für alle $g \in G$, $h \in H$ und $u \in U$. Es folgt

$$|G : H| \dim U = \dim(U^{|G:H|}) = \dim(KG \otimes U) - \dim \operatorname{Ker}(\varphi) \leq \dim U^G \leq |G : H| \dim U.$$

Also bilden die Elemente $r \otimes b$ mit $r \in R$ und $b \in B$ eine Basis von U^G. Wir definieren $g(r \otimes b) := gr \otimes b$ und setzen linear fort. Für ein beliebiges $x \in G$ existieren $r \in R$ und $h \in H$ mit $x = rh$. Es gilt dann

$$g(x \otimes u) = g(r \otimes hu) = gr \otimes hu = grh \otimes u = gx \otimes u.$$

Dies zeigt $(gg')(x \otimes u) = (gg')x \otimes u = g(g'x) \otimes u = g(g'(x \otimes u))$ für $g, g' \in G$. Auf diese Weise wird U^G zu einem KG-Modul. □

Bemerkung III.3.32. Sei $\Delta \colon H \to \mathrm{GL}(n, K)$ eine Darstellung mit KH-Modul U bzgl. einer Basis B. Seien $r_1, \ldots, r_k$ Repräsentanten für G/H. Wie im Beweis von Lemma III.3.31 ist $\hat{B} := \{r_i \otimes b : b \in B,\ i = 1, \ldots, k\}$ eine Basis von U^G. Für $g \in G$ und $r_i \in R$ existiert genau ein $r_j \in R$ mit $r_j^{-1} g r_i \in H$. Es gilt dann $g(r_i \otimes b) = r_j \otimes r_j^{-1} g r_i b$. Wir definieren $\hat{\Delta}(g) := \Delta(g)$ falls $g \in H$ und $\hat{\Delta}(g) := 0 \in K^{n \times n}$ sonst. Die *induzierte* Darstellung Δ^G von U^G bzgl. $\hat{B}$ hat dann die Form

$$\Delta^G(g) = \begin{pmatrix} \hat{\Delta}(r_1^{-1} g r_1) & \cdots & \hat{\Delta}(r_1^{-1} g r_k) \\ \vdots & & \vdots \\ \hat{\Delta}(r_k^{-1} g r_1) & \cdots & \hat{\Delta}(r_k^{-1} g r_k) \end{pmatrix}.$$

Sei nun $K = \mathbb{C}$ und ψ der Charakter von Δ. Für den *induzierten* Charakter ψ^G von Δ^G gilt

$$\psi^G(g) = \sum_{i=1}^{k} \operatorname{tr} \hat{\Delta}(r_i^{-1} g r_i^{-1}) = \sum_{\substack{1 \leq i \leq k \\ g \in r_i H r_i^{-1}}} \psi(r_i^{-1} g r_i) = \sum_{\substack{xH \in G/H \\ gxH = xH}} \psi(x^{-1} g x).$$

Beispiel III.3.33. Sei Ω eine transitive G-Menge und $H := G_\omega$ für ein $\omega \in \Omega$. Für die Basis des Permutationsmoduls V aus Beispiel II.13.4 kann man nach Satz I.4.7 die Nebenklassen $G/H = \{r_1 H, \ldots, r_k H\}$ wählen. Es gilt dann $V \simeq U^G$, wobei $U \simeq K$ der triviale Modul von H ist. Der Permutationscharakter ist daher $(\mathbb{1}_H)^G$. Insbesondere ist $(\mathbb{1}_1)^G$ der reguläre Charakter. Ist $H \trianglelefteq G$, so ist U^G die Inflation des regulären $K[G/N]$-Moduls.

Lemma III.3.34 (Frobenius-Nakayama-Reziprozität)**.** *Sei V ein KG-Modul, $H \leq G$ und U ein KH-Modul. Dann sind*

$$\begin{aligned} \operatorname{Hom}_{KH}(U, V_H) &\to \operatorname{Hom}_{KG}(U^G, V), \qquad \varphi \mapsto \widehat{\varphi} \\ \operatorname{Hom}_{KH}(V_H, U) &\to \operatorname{Hom}_{KG}(V, U^G), \qquad \psi \mapsto \widetilde{\psi} \end{aligned}$$

Vektorraum-Isomorphismen mit $\widehat{\varphi}(g \otimes u) = g\varphi(u)$ und $\widetilde{\psi}(v) = \sum_{gH \in G/H} g \otimes \psi(g^{-1} v)$ für $g \in G$, $u \in U$ und $v \in V$.

Beweis. Wie im Beweis von Lemma III.3.31 sei R ein Repräsentantensystem für G/H und B eine Basis von U.

(i) Für $\varphi \in \mathrm{Hom}_{KH}(U, V_H)$ definieren wir $\widehat{\varphi}(r \otimes b) := r\varphi(b)$ für $r \in R$ und $b \in B$. Sei $u \in U$ und $g = rh \in G$ mit $r \in R$ und $h \in H$. Sei $hu = \sum_{b \in B} \alpha_b b \in U$ mit $\alpha_b \in K$. Dann folgt

$$\widehat{\varphi}(g \otimes u) = \widehat{\varphi}(r \otimes hu) = \widehat{\varphi}\Big(\sum_{b \in B} \alpha_b (r \otimes b)\Big) = \sum_{b \in B} \alpha_b r\varphi(b) = r\varphi(hu) = rh\varphi(u) = g\varphi(u).$$

Für $x \in G$ gilt $\widehat{\varphi}(xg \otimes u) = (xg)\varphi(u) = x(g\varphi(u)) = x\widehat{\varphi}(g \otimes u)$. Dies zeigt $\widehat{\varphi} \in \mathrm{Hom}_{KG}(U^G, V)$. Ist $\widehat{\varphi} = 0$, so gilt $\varphi(b) = \widehat{\varphi}(1 \otimes b) = 0$ und $\varphi = 0$. Daher ist die Abbildung $\varphi \mapsto \widehat{\varphi}$ injektiv und K-linear. Ist umgekehrt $\rho \in \mathrm{Hom}_{KG}(U^G, V)$ gegeben, so ist $\varphi \colon U \to V_H$, $u \mapsto \rho(1 \otimes u)$ offenbar ein Homomorphismus mit $\widehat{\varphi} = \rho$.

(ii) Für $\psi \in \mathrm{Hom}_{KH}(V_H, U)$ können wir direkt $\widetilde{\psi}(v) = \sum_{r \in R} r \otimes \psi(r^{-1}v)$ für $v \in V$ definieren. Ist R' ein weiteres Repräsentantensystem für G/H, so existiert eine Bijektion $R \to R'$, $r \mapsto r'$ mit $r^{-1}r' \in H$ für $r \in R$. Es folgt

$$r' \otimes \psi((r')^{-1}v) = rr^{-1}r' \otimes \psi((r')^{-1}v) = r \otimes r^{-1}r'\psi((r')^{-1}v) = r \otimes \psi(r^{-1}v).$$

Also hängt $\widetilde{\psi}$ nicht von der Wahl von R ab. Für $g \in G$ ist auch gR ein Repräsentantensystem für G/H. Dies impliziert

$$\widetilde{\psi}(gv) = \sum_{r \in R} r \otimes \psi(r^{-1}gv) = \sum_{r \in R} gr \otimes \psi((gr)^{-1}gv) = g \sum_{r \in R} r \otimes \psi(r^{-1}v) = g\widetilde{\psi}(v)$$

und $\widetilde{\psi} \in \mathrm{Hom}_{KG}(V, U^G)$. Sei $\widetilde{\psi} = 0$. Da die Elemente $r \otimes \psi(r^{-1}v)$ für $r \in R$ linear unabhängig sind, folgt $\psi(r^{-1}v) = 0$ für alle $v \in V$. Daher ist $\psi = 0$ und die Abbildung $\psi \mapsto \widetilde{\psi}$ ist injektiv und K-linear.

Schließlich sei $\rho \in \mathrm{Hom}_{KG}(V, U^G)$ gegeben. Für $v \in V$ sei $\rho_r(v) \in U$ mit $\rho(v) = \sum_{r \in R} r \otimes \rho_r(v)$. O. B. d. A. sei $1 \in R$. Für $h \in H$ gilt

$$\sum_{r \in R} r \otimes \rho_r(hv) = \rho(hv) = h\rho(v) = \sum_{r \in R} hr \otimes \rho_r(v) = 1 \otimes h\rho_1(v) + \sum_{r \in R \setminus \{1\}} hr \otimes \rho_r(v).$$

Daher ist $\rho_1 \colon V_H \to U$ ein Homomorphismus. Für $s \in R$ gilt außerdem

$$\sum_{r \in R} r \otimes \rho_r(s^{-1}v) = \rho(s^{-1}v) = s^{-1}\rho(v) = \sum_{r \in R} s^{-1}r \otimes \rho_r(v) = 1 \otimes \rho_s(v) + \sum_{r \in R \setminus \{s\}} s^{-1}r \otimes \rho_r(v).$$

Folglich gilt $\rho_1(s^{-1}v) = \rho_s(v)$ und

$$\widetilde{\rho_1}(v) = \sum_{r \in R} r \otimes \rho_1(r^{-1}v) = \rho(v).$$

Also ist $\psi \mapsto \widetilde{\psi}$ auch surjektiv. □

Bemerkung III.3.35. Sei $K = \mathbb{C}$ in der Situation von Lemma III.3.34. Dann sind alle Moduln halbeinfach und wir können $U \simeq T_1^{a_1} \times \ldots \times T_k^{a_k}$ und $V_H \simeq T_1^{b_1} \times \ldots \times T_k^{b_k}$ mit paarweise nichtisomorphen einfachen KH-Moduln $T_1, \ldots, T_k$ schreiben. Seien ψ und χ die Charaktere von U und V. Nach Schurs Lemma und Lemma II.7.20 gilt

$$(\psi, \chi_H) = a_1b_1 + \ldots + a_kb_k = \dim \mathrm{Hom}_{\mathbb{C}H}(U, V_H) \overset{III.3.34}{=} \dim \mathrm{Hom}_{\mathbb{C}G}(U^G, V) = (\psi^G, \chi).$$

Diese Gleichung bezeichnet man als *Frobenius-Reziprozität*. Sind U und V einfach, so erhält man: Die Vielfachheit von U in V_H ist die Vielfachheit von V in U^G.

Lemma III.3.36. *Für Untergruppen $H \leq L \leq G$, KH-Moduln U, V und einen KG-Modul W gilt*

(i) $(U \times V)^G \simeq U^G \times V^G$.

(ii) $(U^*)^G \simeq (U^G)^*$.

(iii) $(U^L)^G \simeq U^G$.

(iv) $U^G \otimes W \simeq (U \otimes W_H)^G$.

(v) Ist U frei (bzw. projektiv), so auch U^G.

(vi) Ist W frei (bzw. projektiv), so auch W_H.

(vii) Ist W frei (bzw. projektiv), so auch $Q \otimes W$ für jeden KG-Modul Q.

Beweis.

(i) Da $\varphi\colon U \times V \to (U^G \times V^G)_H$, $(u, v) \mapsto (1 \otimes u, 1 \otimes v)$ ein Homomorphismus ist, existiert $\widehat{\varphi}\colon (U \times V)^G \to U^G \times V^G$, $g \otimes (u, v) \mapsto (g \otimes u, g \otimes v)$ nach Lemma III.3.34. Wegen $\widehat{\varphi}(g \otimes (u, 0)) = (g \otimes u, 0)$ ist $\widehat{\varphi}$ surjektiv und aus Dimensionsgründen auch injektiv.

(ii) Für $\lambda \in U^*$ sei $\overline{\lambda} \in (U^G)^*$ mit

$$\overline{\lambda}(g \otimes u) = \begin{cases} \lambda(gu) & \text{falls } g \in H, \\ 0 & \text{sonst.} \end{cases}$$

Für $h \in H$ gilt $\overline{h\lambda} = h\overline{\lambda}$. Daher ist $\varphi\colon U^* \to ((U^G)^*)_H$, $\lambda \mapsto \overline{\lambda}$ ein Homomorphismus. Nach Lemma III.3.34 existiert $\widehat{\varphi}\colon (U^*)^G \to (U^G)^*$, $g \otimes \lambda \mapsto g\overline{\lambda}$. Sei R ein Repräsentantensystem für G/H und $\sum_{r \in R} r \otimes \lambda_r \in \operatorname{Ker}(\widehat{\varphi})$. Für $s \in R$ und $u \in U$ gilt

$$0 = \sum_{r \in R} r\overline{\lambda_r}(s \otimes u) = \sum_{r \in R} \overline{\lambda_r}(r^{-1}s \otimes u) = \lambda_s(u).$$

Dies zeigt $\lambda_s = 0$ für alle $s \in R$. Folglich ist $\widehat{\varphi}$ injektiv und aus Dimensionsgründen auch surjektiv.

(iii) Mit $\varphi\colon U^L \to (U^G)_L$, $x \otimes u \mapsto x \otimes u$ ist auch $\widehat{\varphi}\colon (U^L)^G \to (U^G)$, $g \otimes (x \otimes u) \mapsto gx \otimes u$ ein Homomorphismus. Offenbar ist $\widehat{\varphi}$ surjektiv und wegen

$$\dim(U^L)^G = |G : L| \dim U^L = |G : L||L : H| \dim U = |G : H| \dim U = \dim U^G$$

auch injektiv.

(iv) Die Abbildung $f\colon U \times W_H \to (U^G \otimes W)_H$, $(u, w) \mapsto (1 \otimes u) \otimes w$ ist bilinear und erfüllt

$$f(h(u, w)) = (1 \otimes hu) \otimes hw = (h \otimes u) \otimes hw = h(f(u, w))$$

für $h \in H$. Nach der universellen Eigenschaft existiert ein Homomorphismus $\varphi\colon U \otimes W_H \to (U^G \otimes W)_H$, $u \otimes w \mapsto (1 \otimes u) \otimes w$. Dies ergibt einen Homomorphismus $\widehat{\varphi}\colon (U \otimes W_H)^G \to U^G \otimes W$, $g \otimes (u \otimes w) \mapsto (g \otimes u) \otimes gw$. Man sieht leicht, dass $\widehat{\varphi}$ surjektiv ist. Wegen

$$\dim(U \otimes W_H)^G = |G : H| \dim(U) \dim(W) = \dim(U^G) \dim W = \dim(U^G \otimes W)$$

ist $\widehat{\varphi}$ injektiv.

(v) Die Inklusion $\varphi\colon KH \to KG$ induziert einen Homomorphismus $\widehat{\varphi}\colon (KH)^G \to KG$, $g \otimes a \mapsto ga$ für $a \in KH$. Offenbar ist $\widehat{\varphi}$ ein Isomorphismus. Ist U frei, so gilt $U \simeq (KH)^n$ und $U^G \simeq ((KH)^n)^G \simeq ((KH)^G)^n \simeq KG^n$ nach (i). Also ist U^G frei. Die analoge Aussage für projektive Moduln folgt ebenfalls aus (i).

(vi) Für $g \in G$ ist $KH \to KHg$, $h \mapsto hg$ ein Isomorphismus von KH-Moduln. Sei R ein Repräsentantensystem für die Rechtsnebenklassen von G nach H. Dann gilt $KG = \bigoplus_{r\in R} KHr \simeq (KH)^{|G:H|}$. Daraus folgt leicht die Behauptung.

(vii) Sei $n \in \mathbb{N}$ mit $W = KG^n$. Für den trivialen $K1$-Modul $U \simeq K$ gilt $KG \simeq U^G$ und

$$Q \otimes W \simeq (Q \otimes U^G)^n \overset{\text{(v)}}{\simeq} ((Q_1 \otimes U)^G)^n \simeq ((U^{\dim Q})^G)^n \overset{\text{(i)}}{\simeq} KG^{n \dim Q}.$$

Daher ist $Q \otimes W$ frei. Sei nun W projektiv mit $W \oplus W' = KG^n$. Dann gilt $(Q \otimes W) \oplus (Q \otimes W') \simeq Q \otimes KG^n$. Also ist $Q \otimes W$ projektiv. □

Satz III.3.37. *Sei K ein Körper der Charakteristik $p > 0$ und $|G| = p^a n$ mit $p \nmid n$. Dann sind die folgenden Aussagen äquivalent:*

(1) $C(KG)$ ist eine Diagonalmatrix.

(2) Der Hauptblock von KG ist lokal.

(3) Es existiert ein $N \trianglelefteq G$ mit $|N| = n$.

Beweis.

(1) ⇒ (2): Satz II.12.29 impliziert, dass der triviale Modul K der einzige einfache Modul des Hauptblocks B_0 ist. Wegen $\mathrm{End}_{B_0}(K) \cong K$ gilt $B_0/\mathrm{J}(B_0) \cong K$ nach Bemerkung II.12.3.

(2) ⇒ (3): Sei $e_0 = \sum_{g\in G} \alpha_g g \in \mathrm{Z}(KG)$ das Hauptblockidempotent. Nach Voraussetzung ist der Hauptblock $B_0 = KGe_0$ ein projektiv-unzerlegbarer KG-Modul. Nach Satz II.12.29 sind alle Kompositionsfaktoren von B_0 trivial. Sei $\Delta\colon G \to \mathrm{GL}(B_0)$ die Darstellung durch Linksmultiplikation und $N := \mathrm{Ker}(\Delta) \trianglelefteq G$. Sei $g \in G$ ein p'-Element. Nach Masche ist B_0 ein halbeinfacher $K\langle g\rangle$-Modul, dessen Kompositionsfaktoren nach wie vor trivial sind. Dies zeigt $g \in N$. Sei umgekehrt $g \in N$. Wegen $g_{p'} \in N$ ist auch $g_p \in N$. Aus $g_p e_0 = e_0$ folgt $\alpha_x = \alpha_{xh}$ für $x \in G$ und $h \in H := \langle g_p\rangle$. Für die Augmentationsabbildung $\nu\colon KG \to K$ gilt

$$1 = \nu(e_0) = \sum_{x\in G} \alpha_x = \sum_{xH\in G/H} |H|\alpha_x$$

nach Bemerkung II.12.37. Dies zeigt $H = 1$ und $g = g_{p'}$. Also besteht N aus allen p'-Elementen von G. Nach Lagrange ist $|N|$ ein Teiler von n. Wegen $xN = x_pN$ ist andererseits G/N eine p-Gruppe. Folglich ist $|N| = n$.

(3) ⇒ (1): Sei $P \in \mathrm{Syl}_p(G)$. Nach Lagrange gilt $P \cap N = 1$. Aus $|PN| = |P||N| = |G|$ folgt $G = PN$ und $G/N \cong P$. Durch Inflation wird KP ein KG-Modul. Nach Maschke ist KN halbeinfach. Daher gilt $KN = U \oplus W$, wobei $U \simeq K$ der triviale KN-Modul ist. Dies zeigt

$$KG \simeq KN^G \simeq U^G \oplus W^G \overset{III.3.33}{\simeq} K[G/N] \oplus W^G \simeq KP \oplus W^G.$$

Insbesondere ist KP ein projektiver KG-Modul. Für jeden einfachen KG-Modul V ist auch $V \otimes KP$ projektiv nach Lemma III.3.36. Da P eine p-Gruppe ist, sind alle Kompositionsfaktoren von KP trivial. Ist S/T ein solcher Kompositionsfaktor, so ist

$$(V \otimes S)/(V \otimes T) \overset{III.3.20}{\simeq} V \otimes (S/T) \simeq V$$

ein Kompositionsfaktor von $V \otimes KP$. Daher sind alle Kompositionsfaktoren von $V \otimes KP$ zu V isomorph. Ein projektiv-unzerlegbarer Summand Q von $V \otimes KP$ erfüllt daher $Q/\mathrm{J}(Q) \simeq V$. Außerdem sind alle Kompositionsfaktoren von Q zu V isomorph. Da V ein beliebiger einfacher KG-Modul war, muss $C(KG)$ eine Diagonalmatrix sein. □

Bemerkung III.3.38. In der Situation von Satz III.3.37 ist $e := \frac{1}{n}\sum_{x \in N} x \in \mathrm{Z}(KG)$ ein zentrales Idempotent. Für $y \in N$ gilt $ye = e$. Sei $P \in \mathrm{Syl}_p(G)$. Dann ist $G = PN$ und jedes $g \in G$ lässt sich eindeutig in der Form $g = xy$ mit $x \in P$ und $y \in N$ schreiben. Es gilt $ge = xe$. Für verschiedene $x, x' \in P$ ist $xN \cap x'N = \varnothing$. Daher ist $KP \to KGe$, $x \mapsto xe$ ein Isomorphismus von Algebren. Mit KP ist auch KGe unzerlegbar und e ist primitiv. Wegen $\nu(e) = 1$ muss $B_0 := KGe$ der Hauptblock von KG sein. Es gilt also $B_0 \cong KP$.

Satz III.3.39 (Dickson)**.** *Sei $p := \operatorname{char} K > 0$ und $|G| = p^a n$ mit $p \nmid n$. Sei M ein projektiver KG-Modul. Dann ist $\dim_K M$ durch p^a teilbar.*

Beweis. Sei $P \in \mathrm{Syl}_p(G)$. Nach Lemma III.3.36 ist M_P projektiv. Nach Satz III.3.15 ist $KP \cong \mathrm{End}_{KP}(KP)^o$ lokal, d. h. der reguläre KP-Modul ist unzerlegbar. Also ist M_P sogar ein freier KP-Modul nach Krull-Schmidt; sagen wir $M_P \simeq (KP)^k$. Dann folgt $\dim_K M = k|P| = kp^a$. □

Beispiel III.3.40. Sei $p := \operatorname{char} K > 0$ und $|G| = p^a n$ mit $p \nmid n$. Angenommen es existiert eine Untergruppe $H \leq G$ mit $|H| = n$ (ein Satz von Hall aus der Gruppentheorie besagt, dass H für auflösbare Gruppen G stets existiert). Sei U ein 1-dimensionaler KH-Modul. Nach Maschke ist U projektiv und daher auch $V := U^G$. Wegen $\dim V = |G : H| \dim U = p^a$ ist V projektiv-unzerlegbar nach Dickson. Sei nun $U \simeq K$ der triviale KH-Modul. Nach Lemma III.3.34 ist

$$\dim \mathrm{Hom}_{KG}(V, K) = \dim \mathrm{Hom}_{KH}(U, U) = 1$$

und es folgt $V/\mathrm{J}(V) \simeq K$. Ist G auflösbar und K algebraisch abgeschlossen, so existiert für jeden projektiv-unzerlegbaren KG-Modul V ein einfacher KH-Modul U mit $V \simeq U^G$ (ohne Beweis).

Lemma III.3.41. *Sei V ein KG-Modul und $H \leq G$ mit $|G : H| \in K^\times$. Dann ist V ein direkter Summand von $(V_H)^G$.*

Beweis. Die Identität $V_H \to V_H$ liefert mit Lemma III.3.34 Homomorphismen

$$\begin{aligned} \varphi\colon (V_H)^G &\to V, & g \otimes v &\mapsto gv, \\ \psi\colon V &\to (V_H)^G, & v &\mapsto \sum_{gH \in G/H} g \otimes g^{-1}v. \end{aligned}$$

Wegen $(\varphi\psi)(v) = |G : H|v \neq 0$ ist ψ injektiv und φ surjektiv. Insbesondere ist $V \simeq \psi(V) \leq (V_H)^G$. Für $U := \mathrm{Ker}(\varphi) \leq (V_H)^G$ gilt $\psi(V) \cap U = 0$ und $\dim V = \dim((V_H)^G/U) = \dim(V_H)^G - \dim U$. Dies zeigt $(V_H)^G = \psi(V) \oplus U$. □

Bemerkung III.3.42.

(i) Seien $S, T \leq G$. Dann operiert $S \times T$ auf G durch ${}^{(s,t)}g := sgt^{-1}$ für $(s,t) \in S \times T$. Die Bahnen haben die Form SgT und heißen *Doppelnebenklassen* von G nach S, T.

(ii) Sei $g \in G$, $H \leq G$ und U ein KH-Modul. Dann ist $gHg^{-1} \leq G$ und $g \otimes U = \{g \otimes u : u \in U\}$ ist ein gHg^{-1}-Modul mit

$$ghg^{-1}(g \otimes u) := g \otimes hu$$

für $h \in H$ und $u \in U$ (die Axiome übertragen sich von U^G auf $g \otimes U$).

Lemma III.3.43 (Mackey-Formeln)**.** *Seien $S, T \leq G$ und R ein Repräsentantensystem für die Doppelnebenklassen von G nach S, T. Sei U ein KS-Modul und V ein KT-Modul. Dann gilt:*

$$\boxed{(V^G)_S \simeq \bigtimes_{r \in R} \big((r \otimes V)_{rTr^{-1} \cap S}\big)^S,}$$

$$\boxed{U^G \otimes V^G \simeq \bigtimes_{r \in R} \big(U_{rTr^{-1} \cap S} \otimes (r \otimes V)_{rTr^{-1} \cap S}\big)^G.}$$

Beweis.

(i) Offenbar ist die Abbildung

$$\varphi\colon \bigtimes_{r \in R} \big((r \otimes V)_{rTr^{-1} \cap S}\big)^S \to (V^G)_S$$
$$(s_r \otimes r \otimes v)_{r \in R} \mapsto \sum_{r \in R} s_r r \otimes v_r.$$

ein Homomorphismus von KS-Moduln. Für jedes $g \in G$ existiert ein genau Tripel $(s, r, t) \in S \times R \times T$ mit $g = srt$. Daher ist φ surjektiv. Außerdem ist SR ein Repräsentantensystem für G/T. Ist also $(s_r \otimes r \otimes v)_{r \in R} \in \operatorname{Ker}(\varphi)$, so folgt $s_r r \otimes v_r = 0 = v_r$ für alle $r \in R$. Daher ist φ auch injektiv.

(ii) Nach Lemma III.3.36 und (i) gilt

$$\begin{aligned} U^G \otimes V^G &\simeq (U \otimes (V^G)_S)^G \simeq \Big(U \otimes \bigtimes_{r \in R} \big((r \otimes V)_{rTr^{-1} \cap S}\big)^S\Big)^G \\ &\simeq \Big(\bigtimes_{r \in R} \big(U \otimes ((r \otimes V)_{rTr^{-1} \cap S})^S\big)\Big)^G \simeq \Big(\bigtimes_{r \in R} \big(U_{rTr^{-1} \cap S} \otimes (r \otimes V)_{rTr^{-1} \cap S}\big)^S\Big)^G \\ &\simeq \bigtimes_{r \in R} \big(U_{rTr^{-1} \cap S} \otimes (r \otimes V)_{rTr^{-1} \cap S}\big)^G. \end{aligned}$$

□

Satz III.3.44 (Higman)**.** *Sei K ein Körper der Charakteristik $p > 0$ und $P \in \operatorname{Syl}_p(G)$.*

(i) Ist P zyklisch, so hat jeder unzerlegbare KG-Modul Dimension $\leq |G|$ und es gibt höchstens endlich viele solche Moduln bis auf Isomorphie.

(ii) Ist P nicht zyklisch, so gibt es unzerlegbare KG-Moduln mit beliebig großer Dimension.

Insbesondere hat KG genau dann endlichen Darstellungstyp, wenn P zyklisch ist.

Beweis.

(i) Sei V ein unzerlegbarer KG-Modul. Nach Lemma III.3.41 ist $(V_P)^G \simeq V \oplus U$. Sei $V_P = V_1 \oplus \ldots \oplus V_k$ mit unzerlegbaren Moduln $V_1, \ldots, V_k$. Dann gilt $V \oplus U \simeq V_1^G \oplus \ldots \oplus V_k^G$. Nach Krull-Schmidt ist V zu einem direkten Summand von V_i^G isomorph. Aus Satz III.3.15 folgt

$$\dim V \leq \dim V_i^G = |G : P| \dim V_i \leq |G : P||P| = |G|.$$

Offenbar hat V_i^G höchstens $\dim V_i^G$ viele direkte Summanden. Da KP nur je einen unzerlegbaren Moduln in Dimension $d \in \{1, \ldots, |P|\}$ besitzt, gibt es höchstens

$$|G : P| \sum_{d=1}^{|P|} d = |G| \frac{|P| + 1}{2} < \infty$$

unzerlegbare KG-Moduln bis auf Isomorphie.

(ii) Nach Satz III.3.15 existiert für jedes $d \in \mathbb{N}$ ein unzerlegbarer KP-Modul U der Dimension d. Sei R ein Repräsentantensystem für die Doppelnebenklassen von G nach P, P mit $1 \in R$. Nach der Mackey-Formel ist $U \simeq 1 \otimes U$ ein direkter Summand von $(U^G)_P$. Daher existiert ein unzerlegbarer KG-Modul V, sodass U ein Summand von V_P ist.[4] Insbesondere gilt $\dim V \geq \dim U = d$. □

Bemerkung III.3.45.

(i) Sei $N \trianglelefteq G$ und U ein KN-Modul. Für $g \in G$ ist $g \otimes U$ ebenfalls ein KN-Modul, denn $gNg^{-1} = N$. Wegen $g \otimes (h \otimes U) \simeq gh \otimes U$ für $g, h \in G$ operiert G auf der Menge der Isomorphieklassen von KN-Moduln. Sei

$$G_U := \{g \in G : g \otimes U \simeq U\} \leq G$$

der Stabilisator von U in G. Sicher ist $N \leq G_U$.

(ii) Die Abbildung $U \to g \otimes U$, $u \mapsto g \otimes u$ induziert eine Bijektion zwischen den Mengen der Untermoduln. Insbesondere ist U genau dann einfach (bzw. unzerlegbar), wenn $g \otimes U$ es ist. Außerdem ist $KN \to g \otimes KN$, $x \mapsto g \otimes g^{-1}xg$ für $x \in N$ ein Isomorphismus von KN-Moduln. Somit ist U genau dann frei (bzw. projektiv), wenn $g \otimes U$ es ist.

(iii) Ist U einfach, so ist $(U^G)_N \simeq \bigtimes_{gN \in G/N} g \otimes U$ halbeinfach.

(iv) Für $N \leq H \leq G$ sei $\Gamma(H, U)$ die Menge der Isomorphieklassen einfacher KH-Moduln W, sodass U zu einem Untermodul von W_N isomorph ist.

Satz III.3.46 (Clifford). *Sei V ein einfacher KG-Modul, $N \trianglelefteq G$ und U ein einfacher KN-Modul. Dann gilt*

(i) Genau dann ist U zu einem Untermodul von V_N isomorph, wenn V zu einem Untermodul von U^G isomorph ist.

(ii) Ist $U \leq V_N$, so existiert $e \leq |G_U : N|$ mit

$$\boxed{V_N \simeq \bigtimes_{gG_U \in G/G_U} (g \otimes U)^e.}$$

[4] Dies zeigt auch, dass die Abschätzung in (i) nicht optimal ist.

(iii) Die Abbildung $\Gamma(G_U, U) \to \Gamma(G, U)$, $W \mapsto W^G$ ist eine Bijektion, wobei U genauso oft in W_N wie in $(W^G)_N$ als direkter Summand vorkommt. Außerdem tritt W nur einmal als Kompositionsfaktor von $(W^G)_{G_U}$ auf.

Beweis.

(ii) Offenbar ist $\sum_{g\in G} gU \neq 0$ ein Untermodul von V. Da V einfach ist, folgt $V = \sum_{g\in G} gU$. Sei R ein Repräsentantensystem für G/G_U. Für $r \in R$ und $h \in G_U$ gilt

$$rhU \simeq rh \otimes U \simeq r \otimes (h \otimes U) \simeq r \otimes U.$$

Da $r \otimes U$ ein einfacher KN-Modul ist, folgt

$$V_r := \sum_{h\in G_U} rhU = \sum_{hN\in G_U/N} rhU \simeq (r \otimes U)^e$$

für ein $e \leq |G_U : N|$ nach Satz II.7.4. Für $r \neq s \in R$ gilt $r \otimes U \not\simeq s \otimes U$. Dies impliziert $V = \bigoplus_{r\in R} V_r$. Da die Abbildung $V_r \to V_s$, $x \mapsto sr^{-1}x$ ein Vektorraum-Isomorphismus ist, gilt $V_s \simeq (s \otimes U)^e$ für alle $s \in R$.

(i) Sei $U \leq V_N$ (bis auf Isomorphie). Nach (ii) ist V_N halbeinfach und daher $V_N = U \oplus W$ für ein KN-Modul W. Aus Frobenius-Nakayama folgt $\mathrm{Hom}_{KG}(V, U^G) \simeq \mathrm{Hom}_{KN}(V_N, U) \neq 0$. Da V einfach ist, ist jeder nicht-triviale Homomorphismus $V \to U^G$ injektiv. Also ist V zu einem Untermodul von U^G isomorph. Sei umgekehrt $V \leq U^G$. Dann ist $\mathrm{Hom}_{KN}(V_H, U) \simeq \mathrm{Hom}_{KG}(V, U^G) \neq 0$. Nun ist jeder nicht-triviale Homomorphismus $V_N \to U$ surjektiv. Daher ist U ein Kompositionsfaktor von V_N. Da V_N halbeinfach ist, ist U auch zu einem Untermodul von V_N isomorph.

(iii) Sei $W \in \Gamma(G_U, U)$ und M ein maximaler Untermodul von W^G. Dann ist $V := W^G/M$ ein einfacher KG-Modul. Nach Frobenius-Nakayama ist $\mathrm{Hom}_{KG_U}(W, V_{G_U}) \neq 0$ und $W \leq V_{G_U}$ bis auf Isomorphie. Dies zeigt $U \leq W_N \leq V_N$ und $V \in \Gamma(G, U)$. Aus (ii) erhält man $e, f \in \mathbb{N}$ mit

$$V_N \simeq \bigtimes_{r\in R} (r \otimes U)^e, \qquad\qquad W_N \simeq U^f.$$

Wegen $W_N \leq V_N$ gilt $f \leq e$. Andererseits gilt

$$e|R| \dim U = \dim V \leq \dim W^G = |G : G_U| \dim W \leq |R| f \dim U.$$

Dies zeigt $e = f$ und $W^G \simeq V \in \Gamma(G, U)$. Die Vielfachheit von U als direkter Summand von W_N bzw. $(W^G)_N$ ist jeweils e. Insbesondere kann W auch nur einmal als Kompositionsfaktor von $(W^G)_{G_U}$ auftreten.

Angenommen es existiert $W \not\simeq W' \in \Gamma(G_U, U)$ mit $(W')^G \simeq V$. Dann ist $W \oplus W' \leq V_{G_U}$ und U müsste mit Vielfachheit $2e$ in V_N auftreten. Dieser Widerspruch zeigt die Injektivität von $W \mapsto W^G$.

Sei umgekehrt $V \in \Gamma(G, U)$ gegeben. Nach (i) ist $V \leq U^G = (U^{G_U})^G$ bis auf Isomorphie. Aus Frobenius-Nakayama folgt $\mathrm{Hom}_{KG_U}(V_{G_U}, U^{G_U}) \neq 0$. Daher existiert ein Kompositionsfaktor W von U^{G_U} mit $\mathrm{Hom}_{KG}(V, W^G) \simeq \mathrm{Hom}_{KG_U}(V_{G_U}, W) \neq 0$. Die Mackey-Formel liefert $(U^{G_U})_N = \bigtimes_{gN\in G_U/N} (g \otimes U) \simeq U^{|G_U:N|}$. Somit sind alle Kompositionsfaktoren von W_N zu U isomorph. Insbesondere ist $W \in \Gamma(G_U, U)$ und der erste Teil des Beweises zeigt $V \simeq W^G$. Dies zeigt die Surjektivität von $W \mapsto W^G$. □

Folgerung III.3.47. *Sei V ein halbeinfacher KG-Modul und $N \trianglelefteq G$. Dann ist V_N halbeinfach.*

Bemerkung III.3.48.

(i) In der Situation von Satz III.3.46(ii) nennt man e den *Verzweigungsindex* von U in G. Im Fall $e = 1$ ist $V_N = \bigoplus_{gG_U \in G/G_U} gU$, wobei die Summanden von G permutiert werden. Im Allgemeinen permutiert G nur die halbeinfachen Summanden V_r im obigen Beweis.

(ii) Die Bijektion in (iii) heißt *Clifford-Korrespondenz*. Entsprechend nennt man W (bzw. W^G) den *Clifford-Korrespondenten* von W^G (bzw. W).

Satz III.3.49 (Greens Unzerlegbarkeitssatz)**.** *Sei K ein algebraisch abgeschlossener Körper der Charakteristik $p > 0$ und $N \trianglelefteq G$, sodass G/N eine p-Gruppe ist. Für jeden unzerlegbaren KN-Modul U ist dann auch U^G unzerlegbar.*

Beweis. Induktion nach $|G/N|$: Im Fall $G = N$ ist nichts zu zeigen. Sei also $N < G$ und $Z/N \leq \mathrm{Z}(G/N)$ mit $|Z/N| = p$ (Satz I.4.11). Dann gilt $Z \trianglelefteq G$ nach dem Korrespondenzsatz. Ist die Behauptung für kleinere Indizes bereits bewiesen, so sind U^Z und $U^G \simeq (U^Z)^G$ unzerlegbar. Wir können daher $G = Z$ annehmen, d. h. $|G/N| = p$.

Sei $V \leq U^G$ ein unzerlegbarer direkter Summand. Dann ist

$$V_N \leq (U^G)_N = \bigoplus_{i=1}^{p} g^i \otimes U$$

für ein $g \in G \setminus N$. Sei zunächst $G_U = N$. Nach Krull-Schmidt existiert $1 \leq i \leq p$ mit $g^i \otimes U \leq V_N$. Offenbar ist auch $g^{i+1} \otimes U = g(g^i \otimes U) \leq gV_N = V$. Da die $g^i \otimes U$ paarweise nicht isomorph sind, folgt $\dim V \geq p \dim U = \dim U^G$ und $V = U^G$. Also ist U^G unzerlegbar.

Sei nun $G_U = G$ und $(U^G)_N \simeq U^p$. Nach Bemerkung II.12.12 genügt es zu zeigen, dass $E := \mathrm{End}_{KG}(U^G)$ lokal ist. Sei $\gamma \in E$ die Multiplikation mit g. Dann gilt

$$E = \{\varphi \in \mathrm{End}_{KN}(U^p) : \varphi\gamma = \gamma\varphi\}.$$

Nach Lemma II.7.20 ist $\mathrm{End}_{KN}(U^p) \cong \mathrm{End}_{KN}(U)^{p\times p}$. Dabei ist $F := \mathrm{End}_{KN}(U)$ lokal und $F/\mathrm{J}(F) \cong K$, da K algebraisch abgeschlossen ist. Nach Lemma II.12.26 ist

$$\overline{F^{p\times p}} := F^{p\times p}/\mathrm{J}(F^{p\times p}) = F^{p\times p}/\mathrm{J}(F)^{p\times p} \cong K^{p\times p}.$$

Sei

$$\overline{E} := (E + \mathrm{J}(F)^{p\times p})/\mathrm{J}(F)^{p\times p} \cong E/(E \cap \mathrm{J}(F)^{p\times p})$$

Da $E \cap \mathrm{J}(F)^{p\times p}$ nilpotent ist, gilt $E/\mathrm{J}(E) \cong \overline{E}/\mathrm{J}(\overline{E})$. Also reicht es zu zeigen, dass $\overline{E} \subseteq K^{p\times p}$ lokal ist.

Für $1 \leq i \leq p$ sei $e_{i1} \colon g^i \otimes U \to g \otimes U$ ein Isomorphismus von KN-Moduln. Für $j \in \mathbb{Z}$ setzen wir $e_{i+jp,1} := e_{i1}$ und

$$e_{i+j,1+j} := \alpha^j e_{i1} \alpha^{-j} \colon g^{i+j} \otimes U \to g^{1+j} \otimes U.$$

Wir setzen e_{ij} nach $(U^G)_N$ fort durch $e_{ij}(g^k \otimes U) = 0$ für $k \not\equiv i \pmod p$. Für $x \in N$ und $u \in g^i \otimes U$ gilt

$$\begin{aligned}(\alpha^j e_{i1}\alpha^{-j})(xu) &= \alpha^j(e_{i1}(g^{-j}xu)) = \alpha^j(e_{i1}(g^{-j}xg^j \cdot g^{-j}u)) = \alpha^j(g^{-j}xg^j e_{i1}(g^{-j}u)) \\ &= xg^j e_{i1}(g^{-j}u) = x(\alpha^j e_{ij}\alpha^{-j})(u).\end{aligned}$$

Dies zeigt $e_{ij} \in \mathrm{End}_{KN}(U^p)$. Wegen $\alpha^p e_{ij} = e_{ij}\alpha^p$ hängt e_{ij} nur von den Restklassen $i + p\mathbb{Z}$ und $j + p\mathbb{Z}$ ab. Außerdem ist $\alpha e_{ij}\alpha^{-1} = e_{i+1,j+1}$ für alle $i, j \in \mathbb{Z}$. Sei nun $1 \leq i, j \leq p$. Das Bild $\overline{e_{ij}} \in K^{p\times p}$ von

e_{ij} ist überall 0 außer an Position (i,j). Daher lässt sich jede Matrix $a \in K^{p\times p}$ eindeutig in der Form $a = \sum_{i,j=1}^{p} a_{ij}\overline{e_{ij}}$ mit $a_{ij} \in K$ schreiben. Wegen $\alpha a \alpha^{-1} = \sum a_{ij} e_{i+1,j+1}$ gilt $a \in \overline{E}$ genau dann, wenn $a_{ij} = a_{i+1,j+1}$ für alle i,j, wobei die Indizes modulo p zu lesen sind. Sei $P = (\delta_{i,j+1})_{i,j} \in K^{p\times p}$ die Permutationsmatrix von $(1,\dots,p)$. Dann gilt

$$\overline{E} = \Big\{ \sum_{i=1}^{p} \lambda_i P^i : \lambda_1,\dots,\lambda_p \in K \Big\} \cong K[X]/(X^p-1) = K[X]/(X-1)^p \cong K[X]/(X)^p.$$

Nach Beispiel II.12.9 ist $\overline{E}$ lokal. □

Bemerkung III.3.50. Greens Satz gilt nicht für beliebige Körper: Da $\mathbb{F}_2$ keine primitive 3-te Einheitswurzel besitzt, existiert ein 2-dimensionaler einfacher $\mathbb{F}_2A_3$-Modul U. Wegen $(\mathbb{F}_2A_3)^{S_3} \simeq \mathbb{F}_2S_3$ ist U^{S_3} ein projektiv-unzerlegbarer Modul der Dimension 4. Nach Dickson besitzt $\mathbb{F}_2S_3$ nur noch einen weiteren projektiv-unzerlegbaren Modul. Andererseits ist

$$1 = \big(1 + (1,2,3) + (1,3,2)\big) + \big(1 + (1,2) + (2,3) + (1,2,3)\big) + \big(1 + (1,2) + (2,3) + (1,3,2)\big)$$

eine Zerlegung in drei paarweise orthogonale (primitive) Idempotente (Aufgabe II.61). Also ist U^{S_3} zerlegbar.

4 Darstellungen der symmetrischen Gruppe

Bemerkung III.4.1. Wir wissen aus Aufgabe II.71, dass die Charaktertafel der symmetrischen Gruppe S_n ganzzahlig ist. In diesen Kapitel konstruieren wir die irreduziblen Darstellungen von S_n und geben einen Algorithmus zur Bestimmung der Charaktertafel an. Es zeigt sich, dass alle Darstellungen über $\mathbb{Q}$ realisiert werden können, d. h. $\mathbb{Q}$ ist ein Zerfällungskörper für S_n.

Definition III.4.2.

- Eine *Partition* von $n \in \mathbb{N}$ ist eine Folge von natürlichen Zahlen $\lambda = (\lambda_1, \ldots, \lambda_k)$ mit $\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_k \geq 1$ und $\lambda_1 + \ldots + \lambda_k = n$. Man nennt λ_i die *Teile* von λ. Gleiche Teile fassen wir oft in der Form $(a, a, a, b, b, c, \ldots) = (a^3, b^2, c, \ldots)$ zusammen. Aus technischen Gründen setzen wir gelegentlich stillschweigend $\lambda_{k+1} = \lambda_{k+2} = \ldots = 0$. Die Menge der Partitionen von n sei $P(n)$.
- Die *lexikografische Ordnung* auf $P(n)$ ist definiert durch

$$\lambda < \mu \ :\Longleftrightarrow\ \exists k \in \mathbb{N} : \lambda_1 = \mu_1, \ldots, \lambda_{k-1} = \mu_{k-1}, \lambda_k < \mu_k.$$

- Die *Dominanz-Ordnung* auf $P(n)$ ist definiert durch

$$\lambda \trianglelefteq \mu \ :\Longleftrightarrow\ \forall k \in \mathbb{N} : \lambda_1 + \ldots + \lambda_k \leq \mu_1 + \ldots + \mu_k.$$

  Wie üblich benutzen wir $\leq$, $>$, $\geq$, $\lhd$, $\rhd$ und $\trianglerighteq$.

Beispiel III.4.3. Die Partitionen von 4 sind $(1^4) < (2, 1^2) < (2^2) < (3, 1) < (4)$. Im Gegensatz zur lexikografischen Ordnung ist die Dominanz-Ordnung nicht total. Die Partitionen von 6 sind:

$$\begin{array}{ccccccccccccccc}
 & & & & & & (2^3) & & & & (3^2) & & & & \\
 & & & & & \rhd & & \lhd & & \rhd & & \lhd & & & \\
(1^6) & \lhd & (2,1^4) & \lhd & (2^2,1^2) & & & & (3,2,1) & & & & (4,2) & \lhd & (5,1) & \lhd & (6) \\
 & & & & & \lhd & & \rhd & & \lhd & & \rhd & & & \\
 & & & & & & (3,1^3) & & & & (4,1^2) & & & &
\end{array}$$

Lemma III.4.4. *Gilt $\lambda \trianglelefteq \mu$ für $\lambda, \mu \in P(n)$, so auch $\lambda \leq \mu$.*

Beweis. Im Fall $\lambda = \mu$ ist die Behauptung klar. Sei also $k \in \mathbb{N}$ minimal mit $\lambda_k \neq \mu_k$. Dann gilt

$$\lambda_k = (\lambda_1 + \ldots + \lambda_k) - (\mu_1 + \ldots + \mu_{k-1}) \leq (\mu_1 + \ldots + \mu_k) - (\mu_1 + \ldots + \mu_{k-1}) = \mu_k.$$

Dies zeigt $\lambda \leq \mu$. □

Definition III.4.5.

- Das *Young-Diagramm* Y einer Partition $\lambda = (\lambda_1, \ldots, \lambda_k)$ ist eine Anordnung von n Boxen mit λ_i Boxen in der i-ten Zeile (siehe Beispiel III.4.6). Durch Spiegelung an der Diagonalen erhält man das *entgegengesetzte* Young-Diagramm Y' zur Partition $\lambda' = (\lambda'_1, \ldots, \lambda'_l)$ mit $\lambda'_i := |\{j : \lambda_j \geq i\}|$ für $i = 1, \ldots, l$. Sicher ist $\lambda'' = \lambda$. Im Fall $\lambda' = \lambda$ nennt man λ *symmetrisch*.

- Ein (*Young-*) *Tableau* T ist ein ausgefülltes Young-Diagramm, wobei jede der Zahlen $1, \ldots, n$ in genau einer Box steht. Mit T' bezeichnen wir das entsprechende entgegengesetzte Young-Tableau (die Zeilen von T' sind die Spalten von T). Die Menge aller Tableaus zu einer Partition λ bezeichnen wir mit $T(\lambda)$.

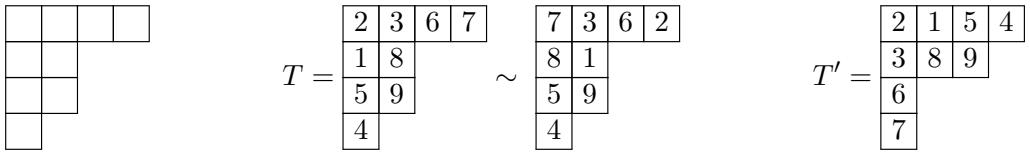
- Tableaus T, U heißen äquivalent (geschrieben $T \sim U$), falls die Zahlen in jeder Zeile von T und U bis auf die Reihenfolge übereinstimmen. Die Äquivalenzklasse von T bezeichnen wir mit $[T]$ und $T(\lambda)/\sim := \{[T] : T \in T(\lambda)\}$ sei die Menge der Äquivalenzklassen.

- Ein Tableau T mit Zeilen $T_1, \ldots, T_k$ bestimmt eine *Young-Untergruppe*

$$S_T := \mathrm{Sym}(T_1) \times \ldots \times \mathrm{Sym}(T_k) \cong S_{\lambda_1} \times \ldots \times S_{\lambda_k}.$$

  Offenbar hängt S_T nur von $[T]$ ab.

Beispiel III.4.6. Das Young-Diagramm von $\lambda = (4, 2^2, 1)$, ein Tableau, ein äquivalentes Tableau und das entgegengesetzte Tableau sind gegeben durch:



Bemerkung III.4.7.

(i) Sei T ein Tableau. Einen kanonischen Repräsentanten für $[T]$ erhält man, indem die Boxen in jeder Zeile von T der Größe nach (aufsteigend) sortiert.

(ii) Der Zyklentyp einer Permutation $\sigma \in S_n$ ist offensichtlich eine Partition von n. Aus Aufgabe II.71 erhält man eine Bijektion $P(n) \to \mathrm{Cl}(S_n)$. Wegen $k(S_n) = |\mathrm{Irr}(S_n)|$ suchen wir eine analoge Bijektion $P(n) \to \mathrm{Irr}(S_n)$.

(iii) Durch Permutieren der Zahlen in den Boxen operiert S_n auf der Menge aller Tableaus. Die Bahnen sind $T(\lambda)$ für $\lambda \in P(n)$. Für ein Tableau T und $\sigma \in S_n$ gilt $({}^\sigma T)' = {}^\sigma T'$. Äquivalente Tableaus werden auf äquivalente Tableaus abgebildet. Daher operiert S_n auch transitiv auf $T(\lambda)/\sim$. Der Stabilisator einer Äquivalenzklasse $[T]$ ist die Young-Untergruppe S_T. Insbesondere gilt $[T] = S_T T$, $|[T]| = |S_Y| = \lambda_1! \ldots \lambda_k!$ und

$$|T(\lambda)/\sim| = \frac{n!}{\lambda_1! \ldots \lambda_k!}.$$

Definition III.4.8. Für $\lambda \in P(n)$ sei M_λ der $\mathbb{C}$-Vektorraum mit Basis $T(\lambda)/\sim$. Durch die Operation von S_n wird M_λ zu einem $\mathbb{C}S_n$-Permutationsmodul. Sei $(.,.)\colon M_\lambda \times M_\lambda \to \mathbb{C}$ das hermitesche Skalarprodukt mit Orthonormalbasis $T(\lambda)/\sim$.

Beispiel III.4.9. Für $\lambda = (n) \in P(n)$ sind alle Tableaus äquivalent. Daher ist M_λ der triviale Modul. Für $\lambda = (1^n)$ sind die Tableaus paarweise nicht-äquivalent und können mit den Permutation von S_n identifiziert werden. Dann ist M_λ der reguläre $\mathbb{C}S_n$-Modul. Im Fall $\lambda = (n, 1)$ lassen sich die Äquivalenzklassen mit den Eintrag in der zweiten Zeile identifizieren. Dann ist $M_\lambda \simeq \mathbb{C}^n$ der Permutationsmodul der natürlichen Operation von S_n auf $\{1, \dots, n\}$.

Definition III.4.10. Für $W \subseteq S_n$ sei (wie bisher) $W^+ = \sum_{w \in W} w \in \mathbb{C}S_n$ und

$$W^- := \sum_{w \in W} \operatorname{sgn}(w) w \in \mathbb{C}S_n.$$

Für $T \in T(\lambda)$ sei

$$q(T) := S^-_{T'}[T] = \sum_{\sigma \in S_{T'}} \operatorname{sgn}(\sigma)[{}^\sigma T] \in M_\lambda.$$

Man nennt

$$Q_\lambda := \operatorname{Span}_{\mathbb{C}}\big\{q(T) : T \in T(\lambda)\big\} \leq M_\lambda$$

den *Specht-Modul* von λ.

Bemerkung III.4.11. Für $T \in T(\lambda)$ und $\sigma \in S_n$ gilt (wie für jeden Stabilisator)

$$\begin{aligned} \sigma S_T \sigma^{-1} &= \sigma(\operatorname{Sym}(T_1) \times \ldots \times \operatorname{Sym}(T_k))\sigma^{-1} = \operatorname{Sym}({}^\sigma T_1) \times \ldots \times \operatorname{Sym}({}^\sigma T_k) \\ &= \operatorname{Sym}(({}^\sigma T)_1) \times \ldots \times \operatorname{Sym}(({}^\sigma T)_k) = S_{{}^\sigma T}. \end{aligned}$$

Dies zeigt

$$\sigma q(T) = (\sigma S_{T'} \sigma^{-1})^- \sigma[T] = S_{[{}^\sigma T']}[{}^\sigma T] = q({}^\sigma T) \in Q_\lambda.$$

Daher operiert S_n tatsächlich auf Q_λ. Außerdem wird Q_λ als $\mathbb{C}S_n$-Modul von einem (beliebigen) $q(T)$ erzeugt. Wählt man aus den Elementen $q(T)$ eine Basis, so erhält man eine Matrixdarstellung $S_n \to \mathrm{GL}(d, \mathbb{Z})$, wobei wir $d = \dim Q_\lambda$ noch bestimmen müssen.

Beispiel III.4.12. Sei $\lambda = (1^n)$ und $T \in T(\lambda)$. Dann ist $S_{T'} = S_n$ und $q(T) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma)[{}^\sigma T]$. Für $\tau \in S_n$ folgt

$$\tau q(T) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma)[{}^{\tau\sigma} T] = \sum_{\sigma \in S_n} \operatorname{sgn}(\tau)\operatorname{sgn}(\sigma)[{}^\sigma T] = \operatorname{sgn}(\tau) q(T).$$

Daher ist $Q_\lambda = \mathbb{C}q(T)$ der Modul zur alternierenden Darstellung. Für $n = 3$ sind $Q_{(3)}$, $Q_{(2,1)}$ und $Q_{(1^3)}$ Repräsentanten der drei einfachen $\mathbb{C}S_3$-Moduln.

Lemma III.4.13. *Seien $\lambda, \mu \in P(n)$, $T \in T(\lambda)$ und $U \in T(\mu)$. Liegen die Zahlen in jeder Zeile von T in paarweise verschiedenen Spalten von U, so gilt $\lambda \trianglelefteq \mu$.*

Beweis. Sei T_i bzw. U_i die i-te Zeile von T bzw. U. Wir können die Einträge in jeder Spalte von U so sortieren, dass die Zahlen von T_1 in U_1 liegen. Insbesondere gilt $\lambda_1 \leq \mu_1$. Auf die gleiche Weise können wir erreichen, dass die Einträge von T_2 in $U_1 \cup U_2$ liegen. Dies zeigt $\lambda_1 + \lambda_2 \leq \mu_1 + \mu_2$ usw. (beachte: es muss nicht unbedingt $\lambda_2 \leq \mu_2$ gelten). □

Lemma III.4.14. *Sei $\lambda \in P(n)$, $T \in T(\lambda)$ und $G \leq S_n$.*

(i) Für $v, w \in M_\lambda$ gilt $(G^- v, w) = (v, G^- w)$.

(ii) Enthält G die Transposition (a,b), so existiert ein $\gamma \in \mathbb{C}S_n$ mit $G^- = \gamma(1-(a,b))$.

(iii) Liegen a,b in der gleichen Zeile von T und ist $(a,b) \in G$, so gilt $G^-[T] = 0$.

Beweis.

(i) Für $\sigma \in G$ und $T, U \in T(\lambda)$ gilt $(\sigma[T], \sigma[U]) = \delta_{[\sigma T],[\sigma U]} = \delta_{[T],[U]} = ([T],[U])$, d. h. σ operiert unitär auf M_λ. Es folgt

$$(G^- v, w) = \sum_{\sigma \in G} \operatorname{sgn}(\sigma)(\sigma v, w) = \sum_{\sigma \in G} \operatorname{sgn}(\sigma)(v, \sigma^{-1} w) = \sum_{\sigma \in G} \big(v, \operatorname{sgn}(\sigma^{-1})\sigma^{-1} w\big) = (v, G^- w).$$

(ii) Sei $R \subseteq G$ ein Repräsentantensystem für $G/\langle (a,b) \rangle$. Dann gilt

$$G^- = \sum_{r \in R} (\operatorname{sgn}(r) r + \operatorname{sgn}(r(a,b)) r(a,b) = \sum_{r \in R} \operatorname{sgn}(r) r (1 - (a,b)).$$

(iii) Nach Voraussetzung ist $(a,b)[T] = [T]$. Aus (ii) folgt daher $G^-[T] = \gamma([T] - (a,b)[T]) = 0$ für ein $\gamma \in \mathbb{C}S_n$. □

Folgerung III.4.15. *Seien $\lambda, \mu \in P(n)$, $T \in T(\lambda)$ und $U \in T(\mu)$. Dann gilt*

(i) $S^-_{U'}[T] \neq 0 \Longrightarrow \lambda \trianglelefteq \mu$.

(ii) $\lambda = \mu$, $S^-_{U'}[T] \neq 0 \Longrightarrow S^-_{U'}[T] = \pm q(U)$.

(iii) $v \in M_\mu \Longrightarrow S^-_{U'} v \in \mathbb{C} q(U)$.

Beweis.

(i) Seien a, b Zahlen aus einer Zeile von T. Angenommen a, b liegen in der gleichen Spalte von U. Dann wäre $(a,b) \in S_{U'}$ und $S^-_{U'}[T] = 0$ nach Lemma III.4.14. Also liegen a, b in verschiedenen Spalten von U. Aus Lemma III.4.13 folgt $\lambda \trianglelefteq \mu$.

(ii) Wie in (i) liegen die Einträge in einer Zeile von T in verschiedenen Spalten von U. Wie im Beweis von Lemma III.4.13 existiert ein $\sigma \in S_{U'}$ mit $\sigma[T] = [U]$ (beachte $\lambda = \mu$). Nun gilt

$$S^-_{U'}[T] = (S_{U'}\sigma)^-[T] = \sum_{\tau \in S_{U'}} \operatorname{sgn}(\tau) \operatorname{sgn}(\sigma) \tau[U] = \operatorname{sgn}(\sigma) q(U).$$

(iii) Für jedes $T \in T(\mu)$ gilt $S^-_{U'}[T] \in \{0, \pm q(U)\}$ nach (ii). Daraus folgt die Behauptung. □

Satz III.4.16 (James' Untermodulsatz)**.** *Sei $\lambda \in P(n)$ und $V \leq M_\lambda$. Dann gilt $Q_\lambda \leq V$ oder $V \leq Q_\lambda^\perp$. Insbesondere ist Q_λ einfach.*

Beweis. Sei $T \in T(\lambda)$. Nehmen wir zunächst $S^-_{T'} V = 0$ an. Für $v \in V$ gilt $(v, q(T)) = (v, S^-_{T'}[T]) = (S^-_{T'} v, [T]) = 0$ nach Lemma III.4.14. Da Q_λ von $q(T)$ erzeugt wird, gilt $V \leq Q_\lambda^\perp$.

Sei nun $S^-_{T'} V \neq 0$. Nach Folgerung III.4.15 existieren $v \in V$ und $a \in \mathbb{C}^\times$ mit $S^-_{T'} v = a q(T)$. Dann ist $Q_\lambda = \mathbb{C}S_n q(T) = \mathbb{C}S_n a^{-1} S_{T'} v \leq V$.

Für die zweite Aussage sei $V < Q_\lambda$. Dann folgt $V \leq Q_\lambda \cap Q_\lambda^\perp = 0$. Also ist Q_λ einfach. □

Bemerkung III.4.17. Die Specht-Moduln lassen sich über beliebigen Körpern definieren. Über Körpern mit positiver Charakteristik ist allerdings nicht unbedingt $Q_\lambda \cap Q_\lambda^\perp = 0$. Man kann aber zeigen, dass $Q_\lambda/(Q_\lambda \cap Q_\lambda^\perp)$ einfach ist.

Lemma III.4.18. *Seien $\lambda, \mu \in P(n)$. Dann gilt*

(i) $\operatorname{Hom}(Q_\lambda, M_\mu) \neq 0 \Longrightarrow \mu \trianglelefteq \lambda$.

(ii) $\operatorname{Hom}(Q_\lambda, M_\lambda) = \operatorname{End}(Q_\lambda) \cong \mathbb{C}$.

Beweis. Sei $0 \neq \varphi \in \operatorname{Hom}(Q_\lambda, M_\mu)$. Dann existiert ein $T \in T(\lambda)$ mit $\varphi(q(T)) \neq 0$. Wegen $M_\lambda = Q_\lambda \oplus Q_\lambda^\perp$ lässt sich φ nach M_λ fortsetzen, indem man $\varphi(Q_\lambda^\perp) = 0$ definiert. Nun existieren $a_{[U]} \in \mathbb{C}$ mit

$$0 \neq \varphi(q(T)) = \varphi(S_{T'}^-[T]) = S_{T'}^- \varphi([T]) = \sum_{U \in T(\mu)/\sim} a_{[U]} S_{T'}^-[U].$$

Aus Folgerung III.4.15 erhält man $\mu \trianglelefteq \lambda$. Im Fall $\lambda = \mu$ gilt $\varphi(q(T)) = bq(T) \in Q_\lambda$ für ein $b \in \mathbb{C}^\times$ nach Folgerung III.4.15. Für alle $\sigma \in S_n$ ist $\varphi(q({}^\sigma T)) = \sigma\varphi(q(T)) = b[{}^\sigma T]$. Da S_n transitiv auf $T(\lambda)$ operiert, folgt $\varphi = b\,\mathrm{id} \in \operatorname{End}(Q_\lambda)$ und $\operatorname{End}(Q_\lambda) \cong \mathbb{C}$ (folgt auch aus Schurs Lemma). □

Satz III.4.19 (Frobenius-Young)**.** *Jeder irreduzible $\mathbb{C}S_n$-Modul ist zu genau einem Specht-Modul isomorph.*

Beweis. Wegen $|P(n)| = k(S_n) = |\operatorname{Irr}(S_n)|$ genügt es zu zeigen, dass Specht-Moduln zu verschiedenen Partitionen $\lambda, \mu \in P(n)$ nicht isomorph sind. Im Fall $Q_\lambda \simeq Q_\mu$ gilt $\operatorname{Hom}(Q_\lambda, M_\mu) \neq 0 \neq \operatorname{Hom}(Q_\mu, M_\lambda)$. Aus Lemma III.4.18 folgt $\lambda = \mu$. □

Folgerung III.4.20. *Der Körper $\mathbb{Q}$ ist ein Zerfällungskörper für S_n.*

Beweis. Nach Bemerkung III.4.11 lassen sich die Specht-Moduln als $\mathbb{Q}$-Darstellungen realisieren. □

Folgerung III.4.21. *Für $\lambda \in P(n)$ gilt*

$$M_\lambda = Q_\lambda \oplus \bigoplus_{\mu \rhd \lambda} m_\mu Q_\mu$$

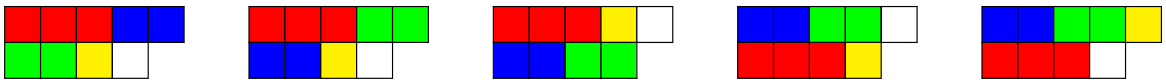
mit $m_\mu \in \mathbb{N}_0$ für $\mu \rhd \lambda$.

Beweis. Aus $Q_\mu \leq M_\lambda$ folgt $\operatorname{Hom}(Q_\mu, M_\lambda) \neq 0$ und $\mu \trianglerighteq \lambda$ nach Lemma III.4.18. Würde Q_λ mehrfach in M_λ auftreten, so wäre $\dim_{\mathbb{C}} \operatorname{Hom}(Q_\lambda, M_\lambda) \geq 2$ im Widerspruch zu Lemma III.4.18. □

Definition III.4.22. Für $\lambda \in P(n)$ sei π_λ der Permutationscharakter von M_λ und $\chi_\lambda \in \operatorname{Irr}(S_n)$ der Charakter von Q_λ. Für $g \in S_n$ vom Zyklentyp $\mu \in P(n)$ sei $\pi_\lambda(\mu) := \pi_\lambda(g)$ und $\chi_\lambda(\mu) := \chi_\lambda(g)$ (das ist nach Aufgabe II.71 wohldefiniert).

Satz III.4.23. *Sei $\lambda, \mu \in P(n)$. Dann ist $\pi_\lambda(\mu)$ die Anzahl der Möglichkeiten die Zeilen des Young-Diagramms von μ auf das Young-Diagramm von λ zu verteilen (siehe Beispiel III.4.24).*

Beispiel III.4.24. Sei $\lambda = (5,4)$ und $\mu = (3,2^2,1^2)$. Dann ist $\pi_\lambda(\mu) = 5$, veranschaulicht durch eingefärbte Young-Diagramme:



Beweis von Satz III.4.23. Sei $\sigma = \sigma_1 \dots \sigma_k$ von Zyklentyp $\mu = (\mu_1, \dots, \mu_k)$ mit disjunkten Zyklen σ_i der Länge μ_i für $i = 1, \dots, k$. Bekanntlich ist $\pi_\lambda(\sigma)$ die Anzahl der Äquivalenzklassen von Tableaus $[T]$ mit $[{}^\sigma T] = [T]$. Diese Bedingung gilt genau dann, wenn die Ziffern von σ_i in einer Zeile von T auftreten für $i = 1, \dots, k$. Dies liefert eine Verteilung der μ_i auf die Zeilen des Young-Diagramms von λ. Da wir nur Äquivalenzklassen von Tableaus zählen, ist die genaue Position von μ_i in einer Zeile unerheblich. □

Bemerkung III.4.25.

(i) Folgerung III.4.21 und Satz III.4.23 ermöglichen es die Charaktertafel von S_n rekursiv zu berechnen: Es gilt $\chi_{(n)} = \pi_{(n)} = \mathbb{1}_{S_n}$ und

$$\boxed{\chi_\lambda = \pi_\lambda - \sum_{\mu \rhd \lambda} (\pi_\lambda, \chi_\mu)\chi_\mu.}$$

Dadurch lässt sich χ_λ auch als ganzzahlige Linearkombination der π_μ ausdrücken. Die Koeffizienten (π_λ, χ_μ) nennt man *Kostka-Zahlen*. Sie sind positiv für alle $\mu \trianglerighteq \lambda$ (ohne Beweis).

(ii) Da S_n transitiv auf $T(\lambda)/\sim$ operiert, gilt $(\pi_\lambda, \mathbb{1}_{S_n}) = 1$ nach Aufgabe II.68. Insbesondere ist $\chi_{(n-1,1)} = \pi_{(n-1,1)} - \mathbb{1}_{S_n}$.

(iii) Die Gleichung $(\pi_\lambda, \chi_\lambda) = 1$ zusammen mit Lemma II.13.62 impliziert Folgerung III.4.20.

(iv) Sei $\mu = (\mu_1, \dots) = (1^{m_1}, \dots, n^{m_n})$ mit $m_1, \dots, m_n \in \mathbb{N}_0$. Eine Verteilung der μ_i auf die Zeilen des Young-Diagramms Y von λ setzt sich wie folgt zusammen: Man wähle $a_{ij} \in \mathbb{N}_0$ Teile i und verteile sie auf die j-te Zeile von Y. Dann ist $a_{i,1} + \dots + a_{i,k} = m_i$ und $a_{1,j}1 + a_{2,j}2 + \dots + a_{n,j}n = \lambda_j$ für $i = 1, \dots, n$ und $j = 1, \dots, k$. Daher ist $\pi_\lambda(\mu)$ der Koeffizient von $X_1^{\lambda_1} \dots X_k^{\lambda_k}$ in dem symmetrischen Polynom

$$\prod_{i=1}^{n} (X_1^i + \dots + X_k^i)^{m_i} = \prod_{i=1}^{n} \sum_{a_{i1}+\dots+a_{ik}=m_i} \binom{m_i}{a_{i1}, \dots, a_{ik}} X_1^{a_{i1}} \dots X_k^{a_{ik}}.$$

Satz III.4.26. *Für $\lambda \in P(n)$ ist Q_λ der einzige gemeinsame Bestandteil von M_λ und $Q_{(1^n)} \otimes M_{\lambda'}$. Insbesondere ist $Q_{(1^n)} \otimes Q_\lambda \simeq Q_{\lambda'}$ und* $\boxed{\chi_{\lambda'} = \operatorname{sgn} \cdot \chi_\lambda.}$

Beweis. Sei $T \in T(\lambda)$. Der Permutationscharakter π_λ von M_λ ist nach Beispiel III.3.33 die Induktion des trivialen Charakters $\mathbb{1}_{S_T}$. Nach Beispiel III.4.12 ist $Q_{(1^n)}$ der Modul der alternierenden Darstellung mit Charakter sgn. Nach Lemma III.3.36 gilt $\operatorname{sgn} \cdot (\mathbb{1}_{S_{T'}})^{S_n} = (\operatorname{sgn}_{S_{T'}})^{S_n}$. Dies zeigt

$$(\chi_\lambda, \operatorname{sgn} \pi_{\lambda'}) = (\chi_\lambda, \operatorname{sgn}(\mathbb{1}_{S_{T'}})^{S_n}) = (\chi_\lambda, (\operatorname{sgn}_{S_{T'}})^{S_n}) \overset{III.3.35}{=} ((\chi_\lambda)_{S_{T'}}, \operatorname{sgn}_{S_{T'}}).$$

Wir können $q(T)$ zu einer Basis von Q_λ ergänzen. Für $\sigma \in S_{T'}$ ist $\sigma q(T) = \operatorname{sgn}(\sigma) q(T)$. Daher ist $\operatorname{sgn}_{S_{T'}}$ ein irreduzibler Bestandteil von $(\chi_\lambda)_{S_{T'}}$ und χ_λ ist ein Bestandteil von $\operatorname{sgn} \pi_{\lambda'}$. Für die Eindeutigkeit

genügt es $(\pi_\lambda, \operatorname{sgn}\pi_{\lambda'}) = 1$ zu zeigen. Nach der Mackey-Formel gilt

$$\begin{aligned}(\pi_\lambda, \operatorname{sgn}\pi_{\lambda'}) &= (\mathbb{1}_{S_T}^{S_n}, (\operatorname{sgn}_{S_{T'}})^{S_n}) = ((\mathbb{1}_{S_T}^{S_n})_{S_{T'}}, \operatorname{sgn}_{S_{T'}}) \\ &= \sum_{S_{T'}\sigma S_T \in S_{T'}\backslash S_n/S_T} (\mathbb{1}_{D_\sigma}^{S_{T'}}, \operatorname{sgn}_{S_{T'}}) = \sum_{S_{T'}\sigma S_T \in S_{T'}\backslash S_n/S_T} (\mathbb{1}_{D_\sigma}, \operatorname{sgn}_{D_\sigma}) \qquad \text{(III.4.1)}\end{aligned}$$

mit $D_\sigma := S_{T'} \cap \sigma S_T \sigma^{-1} = S_{T'} \cap S_{\sigma T}$. Sei $(\mathbb{1}_{D_\sigma}, \operatorname{sgn}_{D_\sigma}) > 0$ für ein $\sigma \in S_n$. Angenommen es existieren Zahlen a, b, die in der gleichen Zeile von ${}^\sigma T$ und in der gleichen Spalte von T liegen. Dann liegt die Transposition (a, b) in D_σ und man erhält den Widerspruch $\mathbb{1}_{D_\sigma} \neq \operatorname{sgn}_{D_\sigma}$. Daher verteilen sich die Zahlen einer Zeile von ${}^\sigma T$ auf paarweise verschiedene Spalten von T. Insbesondere existiert ein $\tau_1 \in S_{T'}$, sodass die ersten Zeilen von ${}^\sigma T$ und ${}^{\tau_1} T$ als Mengen übereinstimmen. Analog findet man ein $\tau_2 \in S_{T'}$, sodass die ersten beiden Zeilen von ${}^\sigma T$ und ${}^{\tau_2\tau_1} T$ übereinstimmen usw. Schließlich existiert ein $\tau \in S_{T'}$ mit ${}^\sigma T \sim {}^\tau T$, d. h. $\tau^{-1}\sigma \in S_T$ und $S_{T'}\sigma S_T = S_{T'} S_T$. Man kann also $\sigma = 1$ in (III.4.1) annehmen. Umgekehrt gilt dann $D_\sigma = 1$ und $(\mathbb{1}_{D_\sigma}, \operatorname{sgn}_{D_\sigma}) = 1$. Daraus folgt die erste Behauptung.

Für die zweite Behauptung beobachten wir, dass $\operatorname{sgn}\chi_\lambda$ und $\chi_{\lambda'}$ gemeinsame irreduzible Bestandteile von $\operatorname{sgn}\pi_\lambda = \operatorname{sgn}\pi_{\lambda''}$ und $\operatorname{sgn}^2\pi_{\lambda'} = \pi_{\lambda'}$ sind. Nach dem ersten Teil des Beweises müssen sie gleich sein. □

Bemerkung III.4.27. Die Zerlegung von $Q_\lambda \otimes Q_\mu$ für $\lambda, \mu \in P(n)$ in einfache Moduln ist im Allgemeinen ein offenes Problem. Die auftretenden Vielfachheiten nennt man *Kronecker-Koeffizienten.*

Beispiel III.4.28. Sei $n = 5$. Die Partitionen von 5 sind $(5) \rhd (4,1) \rhd (3,2) \rhd (3,1^2) \rhd (2^2,1) \rhd (2,1^3) \rhd (1^5)$. Wegen Satz III.4.26 brauchen wir π_λ nur für drei Partitionen zu berechnen:

σ	(1^5)	$(2,1^3)$	$(2^2,1)$	$(3,1^2)$	$(3,2)$	$(4,1)$	(5)
$\lvert S_5 : \mathrm{C}_{S_5}(\sigma)\rvert$	1	10	15	20	20	30	24
$\pi_{(4,1)}$	5	3	1	2	0	1	0
$\pi_{(3,2)}$	10	4	2	1	1	0	0
$\pi_{(3,1^2)}$	20	6	0	2	0	0	0

Die zweite Zeile enthält dabei die Längen der Konjugationsklassen. Aus Bemerkung III.4.25 ergibt sich $\chi_{(4,1)} = \pi_{(4,1)} - \mathbb{1}_{S_5}$. Weiter ist $(\pi_{(3,2)}, \chi_{(4,1)})_{S_5} = 1$ und $\chi_{(3,2)} = \pi_{(3,2)} - 1_{S_n} - \chi_{(4,1)}$. Schließlich ist $(\pi_{(3,1^2)}, \chi_{(3,2)})_{S_5} = 1$ und $(\pi_{(3,1^2)}, \chi_{(4,1)})_{S_5} = 2$. Also ist $\chi_{(3,1^2)} = \varphi_{(3,1^2)} - 1_{S_5} - \chi_{(3,2)} - 2\chi_{(4,1)}$.

S_5	(1^5)	$(2,1^3)$	$(2^2,1)$	$(3,1^2)$	$(3,2)$	$(4,1)$	(5)
(5)	1	1	1	1	1	1	1
$(4,1)$	4	2	0	1	−1	0	−1
$(3,2)$	5	1	1	−1	1	−1	0
$(3,1^2)$	6	0	−2	0	0	0	1
$(2^2,1)$	5	−1	1	−1	−1	1	0
$(2,1^3)$	4	−2	0	1	1	0	−1
(1^5)	1	−1	1	1	−1	−1	1

Bemerkung III.4.29. Wir konstruieren als Nächstes eine kanonische Basis von Q_λ bestehend aus $q(T)$ für gewisse $T \in T(\lambda)$. Wegen $q({}^\sigma T) = \operatorname{sgn}(\sigma) q(T)$ für $\sigma \in S_{T'}$ braucht man nur solche T, deren Spalten (aufsteigend) sortiert sind.

Definition III.4.30. Ein Tableau T heißt *Standard-Tableau*, wenn die Ziffern in den Zeilen und Spalten von T jeweils aufsteigend sortiert sind. Sei $ST(\lambda)$ die Menge der Standard-Tableaus zur Partition λ.

Beispiel III.4.31. Zu jeder Partition $\lambda \in P(n)$ existiert mindestens ein Standard-Tableau, zum Beispiel kann man die Zahlen $1, \ldots, n$ von links nach rechts und von oben nach unten auf die Boxen verteilen. Im Fall $\lambda \in \{(n), (1^n)\}$ ist dies die einzige Möglichkeit. Im Allgemeinen steht die Zahl 1 stets links oben. Für $\lambda = (3^2)$ gibt es fünf Standard-Tableaus:

1	2	3
4	5	6

1	2	4
3	5	6

1	2	5
3	4	6

1	3	4
2	5	6

1	3	5
2	4	6

Jede Äquivalenzklasse von Tableaus enthält höchstens ein Standard-Tableau.

Definition III.4.32.

- Eine *Komposition* von $n \in \mathbb{N}$ ist eine Folge $\lambda = (\lambda_1, \lambda_2, \ldots) \in \mathbb{N}_0^\infty$ mit $\sum_{i=1}^\infty \lambda_i = n$. Sei $K(n)$ die Menge aller Kompositionen von n. Die *Dominanz-Ordnung* für Partitionen übertragt sich auf Kompositionen.
- Für ein Tableau T und $k \in \mathbb{N}$ definieren die Komposition $\lambda_T^{(k)} := (\lambda_1, \ldots)$, wobei λ_i die Anzahl der Zahlen $\leq k$ in der i-ten Zeile von T ist. Offenbar hängt $\lambda_T^{(k)}$ nur von $[T]$ ab.
- Für Tableaus $T, U \in T(\lambda)$ sei

$$[T] \trianglelefteq [U] \iff \lambda_T^{(k)} \trianglelefteq \mu_T^{(k)} \text{ für } k = 1, \ldots, n.$$

Beispiel III.4.33. Für

$$T = \begin{array}{|c|c|c|}\hline 3 & 4 & 7 \\ \hline 2 & 5 & 8 \\ \hline 1 & 6 \\ \cline{1-2} 9 \\ \cline{1-1} \end{array}$$

ist

$\lambda_T^{(1)}$	$\lambda_T^{(2)}$	$\lambda_T^{(3)}$	$\lambda_T^{(4)}$	$\lambda_T^{(5)}$	$\lambda_T^{(6)}$	$\lambda_T^{(7)}$	$\lambda_T^{(8)}$	$\lambda_T^{(9)}$
$(0,0,1)$	$(0,1,1)$	$(1,1,1)$	$(2,1,1)$	$(2,2,1)$	$(2,2,2)$	$(3,2,2)$	$(3,3,2)$	$(3,3,2,1)$

Bemerkung III.4.34. Im Gegensatz zu Partitionen sind Kompositionen nicht unbedingt absteigend sortiert. Durch die Möglichkeit $\lambda_i = 0$ gibt es daher stets unendlich viele Kompositionen von n. Man prüft leicht, dass $\trianglelefteq$ eine Ordnungsrelation auf $K(n)$ und $T(\lambda)/\sim$ ist.

Lemma III.4.35. *Sei $T \in T(\lambda)$ und $k < l$, sodass k in Zeile s und l in Zeile t von T mit $s > t$ auftritt. Für die Transposition $\sigma = (k, l) \in S_n$ gilt dann $[T] \trianglelefteq [{}^\sigma T]$.*

Beweis. Sei $U = {}^\sigma T$. Für $i < k$ und $i \geq l$ gilt sicher $\lambda_T^{(i)} = \lambda_U^{(i)}$. Sei also $k \leq i < l$. Dann entsteht $\lambda_U^{(i)}$ aus $\lambda_T^{(i)} = (\lambda_1, \ldots)$, indem man λ_s um 1 verringert und λ_t um 1 erhöht. Wegen $s > t$ folgt die Behauptung. □

Lemma III.4.36. *Für $T \in ST(\lambda)$ und $\sigma \in S_{T'}$ gilt $[{}^\sigma T] \trianglelefteq [T]$.*

Beweis. O. B. d. A. sei $\sigma \neq 1$. Da die Spalten von T sortiert sind, existiert ein Paar (k,l) wie in Lemma III.4.35. Man kann also σ durch $(k,l)\sigma$ ersetzen. Dadurch reduziert sich die Anzahl der Paare (k,l). Nach endlich vielen Wiederholungen erreicht man $\sigma = 1$. □

Satz III.4.37. *Sei $\lambda \in P(n)$. Dann ist $\{q(T) : T \in ST(\lambda)\}$ linear unabhängig.*

Beweis. Sei $ST(\lambda) = \{T_1, \ldots, T_k\}$ mit $[T_1] \rhd \ldots \rhd [T_k]$. Seien $a_1, \ldots, a_k \in \mathbb{C}$ mit $a_1 q(T_1) + \ldots + a_k q(T_k) = 0$. Im Fall $a_1 \neq 0$ muss $[T_1]$ als Summand eines $q(T_i)$ mit $i > 1$ auftreten. Dann existiert ein $\sigma \in S_{T_i'}$ mit $T_1 = {}^{\sigma}T_i$ und Lemma III.4.36 liefert den Widerspruch $[T_1] \lhd [T_i]$. Also ist $a_1 = 0$. Man kann nun das Argument mit a_2 wiederholen. Am Ende ist $a_1 = \ldots = a_k = 0$. □

Definition III.4.38. Sei $T = (t_{ij}) \in T(\lambda) \setminus ST(\lambda)$ mit aufsteigend sortierten Spalten. Dann existieren i, j mit $t_{i,j} > t_{i,j+1}$. Sei $A := \{t_{i,j}, t_{i+1,j}, \ldots, t_{l,j}\}$ und $B := \{t_{1,j+1}, t_{2,j+1}, \ldots, t_{i,j+1}\}$, wobei l die Länge der j-ten Spalte von T ist. Sei $G_{i,j}$ die Menge der Permutationen $\pi \in \mathrm{Sym}(A \cup B) \leq S_n$, sodass die Spalten von ${}^{\pi}T$ aufsteigend sortiert sind. Man nennt $G_{i,j}^- \in \mathbb{C}S_n$ das GARNIR-*Element* von T bzgl. (i,j).

Bemerkung III.4.39. Für jede Teilmenge $A' \subseteq A \cup B$ mit $|A'| = |A|$ gibt es genau ein $\pi \in G_{i,j}$ mit $\pi(A) = A'$. Daher gilt

$$|G_{i,j}| = \binom{|A \cup B|}{|A|} = \frac{(|A| + |B|)!}{|A|!|B|!}.$$

Tatsächlich ist $G_{i,j}$ ein Repräsentantensystem für die Linksnebenklassen von $\mathrm{Sym}(A) \times \mathrm{Sym}(B)$ in $\mathrm{Sym}(A \cup B)$.

Beispiel III.4.40. Sei

$$T = \begin{array}{|c|c|c|}\hline 1 & 2 & 3 \\ \hline 5 & 4 \\ \cline{1-2} 6 & 7 \\ \cline{1-2}\end{array}$$

mit $(i,j) = (2,1)$, $A = \{5,6\}$ und $B = \{2,4\}$. Dann besteht $G_{i,j}$ aus folgenden Permutationen:

π	1	$(4,5)$	$(4,6,5)$	$(2,4,5)$	$(2,4,6,5)$	$(2,5)(4,6)$
${}^{\pi}T$	1 2 3 / 5 4 / 6 7	1 2 3 / 4 5 / 6 7	1 2 3 / 4 6 / 5 7	1 4 3 / 2 5 / 6 7	1 4 3 / 2 6 / 5 7	1 5 3 / 2 6 / 4 7

Lemma III.4.41. *Mit den Bezeichnungen aus Definition III.4.38 gilt $G_{i,j}^- q(T) = 0$.*

Beweis. Zur Abkürzung sei $S(A) := \mathrm{Sym}(A)$, $S(B) := \mathrm{Sym}(B)$ und $S(AB) := \mathrm{Sym}(A \cup B)$. Sei $\sigma \in S_{T'}$. Dann ist A bzw. B eine Teilmenge der j-ten bzw. $(j+1)$-ten Spalte von ${}^{\sigma}T$. Da $|A| + |B|$ um 1 größer ist als die Länge der j-ten Spalte, existieren verschiedene $x, y \in A \cup B$, die in der gleichen Zeile von ${}^{\sigma}T$ stehen. Wegen der Transposition $\sigma = (x,y) \in S(AB)$ gilt $S(AB)^-[{}^{\sigma}T] = 0$ nach Lemma III.4.14. Die Summe über $\sigma \in S_{T'}$ liefert $S(AB)^- q(T) = 0$.

Nach Bemerkung III.4.39 ist $S(AB) = \bigcup_{\pi \in G_{i,j}} \pi S(A)S(B)$. Für $\sigma \in S(A)S(B) \leq S_{T'}$ gilt $\sigma q(T) = \mathrm{sgn}(\sigma) q(T)$. Dies zeigt $(S(A)S(B))^- q(T) = |A|!|B|! q(T)$. Insgesamt ist

$$G_{i,j}^- q(T) = \frac{1}{|A|!|B|!} \sum_{\pi \in G_{i,j}} \mathrm{sgn}(\pi) \pi (S(A)S(B))^- q(T) = \frac{1}{|A|!|B|!} S(AB)^- q(T) = 0.$$ □

Satz III.4.42 (Specht). *Sei $\lambda \in P(n)$. Dann ist $\{q(T) : T \in ST(\lambda)\}$ eine Basis von Q_λ. Insbesondere ist $\chi_\lambda(1) = \dim Q_\lambda = |ST(\lambda)|$.*

Beweis (Peel). Sei $T = (t_{ij}) \in T(\lambda) \setminus ST(\lambda)$. Nach Satz III.4.37 genügt es $q(T)$ als Linearkombination der $q(U)$ mit $U \in ST(\lambda)$ zu schreiben. Wegen $q({}^\sigma T) = \operatorname{sgn}(\sigma) q(T)$ für $\sigma \in S_{T'}$ können wir annehmen, dass T aufsteigend sortierte Spalten besitzt. Wir argumentieren durch Induktion nach der dualen Dominanz-Ordnung auf $T(\lambda)$, die durch $T \trianglelefteq' U \iff [T'] \trianglelefteq [U']$ definiert ist. Man macht sich klar, dass das größte Element bzgl. $\trianglelefteq'$ gegeben ist durch das Standard-Tableau T_0, dessen Boxen spaltenweise aufsteigend von links nach rechts und von oben nach unten nummeriert sind. Beispiel:

$$T_0 = \begin{array}{|c|c|c|}\hline 1 & 5 & 8 \\ \hline 2 & 6 & 9 \\ \hline 3 & 7 \\ \cline{1-2} 4 \\ \cline{1-1} \end{array} \longrightarrow \begin{array}{cccccccc} \lambda^{(1)}_{T_0'} & \lambda^{(2)}_{T_0'} & \lambda^{(3)}_{T_0'} & \lambda^{(4)}_{T_0'} & \lambda^{(5)}_{T_0'} & \cdots & \lambda^{(9)}_{T_0'} \\ \hline (1) & (2) & (3) & (4) & (4,1) & \cdots & (4,3,2) \end{array}$$

Wegen $T \notin ST(\lambda)$ ist $T \triangleleft' T_0$. Daher existieren (i,j) wie in Definition III.4.38. Nach Voraussetzung gilt

$$t_{1,j+1} < t_{2,j+1} < \ldots < t_{i,j+1} < t_{i,j} < t_{i+1,j} < \ldots < t_{l,j}.$$

Für $\pi \in G_{i,j} \setminus \{1\}$ folgt daher ${}^\pi T \rhd' T$ (vgl. Lemma III.4.35). Nach Induktion lassen sich die $q({}^\pi T)$ bereits als Linearkombination der Standard-Tableaus schreiben. Nach Lemma III.4.41 ist

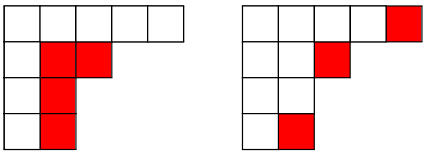
$$q(T) = q(T) - G^-_{i,j} q(T) = - \sum_{\pi \in G_{i,j} \setminus \{1\}} \operatorname{sgn}(\pi) q({}^\pi T). \qquad \square$$

Definition III.4.43. Sei Y ein Young-Diagramm von $\lambda \in P(n)$. Der *Haken* von Y an Position (s,t) ist die Menge der Boxen

$$H_{st} := \big\{(s,j) : j \geq t\big\} \cup \big\{(i,t) : i \geq s\big\}$$

in Y. Sei $h_{st} := |H_{st}| = \lambda_s + \lambda'_t - s - t + 1$ die *Länge* des Hakens. Wir bezeichnen die Box an Position (s,t) als *Ecke* von Y, falls $h_{st} = 1$ gilt (d. h. $\lambda_s = s$ und $\lambda'_t = t$). Durch Entfernen dieser Ecke erhält man ein Young-Diagramm einer Partition $\mu \in P(n-1)$. Sei $\lambda^- \subseteq P(n-1)$ die Menge aller μ, die durch Entfernen einer Ecke entstehen. Analog sei $\lambda^+ := \{\mu \in P(n+1) : \lambda \in \mu^-\} \subseteq P(n+1)$.

Beispiel III.4.44. Der Haken $H_{2,2}$ mit Länge 4 und die Ecken $(1,5)$, $(2,3)$ und $(4,2)$ in $\lambda = (5,3,2^2)$ sind rot markiert:



Es gilt $\lambda^- = \big\{(4,3,2^2), (5,2^3), (5,3,2,1)\big\}$ und $\lambda^+ = \big\{(6,3,2^2), (5,4,2^2), (5,3^2,2)\big\}$.

Satz III.4.45 (Verzweigungsregel). *Für $\lambda \in P(n)$ gilt*

$$(Q_\lambda)_{S_{n-1}} = \bigoplus_{\mu \in \lambda^-} Q_\mu \qquad (n \geq 2),$$
$$(Q_\lambda)^{S_{n+1}} = \bigoplus_{\mu \in \lambda^+} Q_\mu.$$

Beweis. Seien $e_1, \ldots, e_k$ die Ecken des Young-Diagramms zu λ. Sei $\lambda^- = \{\mu_1, \ldots, \mu_k\}$, wobei μ_i durch Entfernen von e_i entsteht. Steht n in einer Ecke e_i von $T \in T(\lambda)$, so erhält man durch Entfernen von n ein Tableau $T_i \in T(\mu_i)$. Wir betrachten die lineare Abbildung $\varphi_i \colon M_\lambda \to M_{\mu_i}$ mit

$$\varphi_i([T]) := \begin{cases} [T_i] & \text{falls } n \text{ in } e_i \text{ liegt,} \\ 0 & \text{sonst,} \end{cases}$$

wobei wir annehmen können, dass $T \in T(\lambda)$ aufsteigend sortierte Zeilen hat. Für $\sigma \in S_{n-1}$ gilt offenbar $\varphi_i([{}^\sigma T]) = {}^\sigma\varphi_i([T])$, d. h. φ_i ist ein Homomorphismus von $\mathbb{C}S_{n-1}$-Moduln.

In jedem Standard-Tableau steht n offenbar an einer der Ecken. Sei

$$Q_i := \operatorname{Span}_{\mathbb{C}}\big\{q(T) : T \in ST(\lambda) \text{ mit } n \text{ in Ecke } e_j \text{ wobei } j \leq i\big\}$$

für $i = 0, \ldots, k$. Für $\sigma \in S_{n-1}$ und $q(T) \in Q_i$ gilt $\sigma q(T) = q({}^\sigma T) \in Q_i$ nach Bemerkung III.4.11, d. h. Q_i ist ein $\mathbb{C}S_{n-1}$-Modul. Nach Specht ist $0 = Q_0 \leq Q_1 \leq \ldots \leq Q_k = Q_\lambda$. Außerdem ist $\varphi_i(Q_i) = Q_{\mu_i}$ mit $Q_{i-1} \leq \operatorname{Ker}(\varphi_i)$. Da jedes Standard-Tableau von λ durch Anfügen von n aus einem Standard-Tableau eines μ_i entsteht, gilt

$$\begin{aligned} \dim Q_\lambda &= \sum_{i=1}^{k} \dim(Q_i/Q_{i-1}) \geq \sum_{i=1}^{k} \dim(Q_i/(Q_i \cap \operatorname{Ker}(\varphi_i))) = \sum_{i=1}^{k} \dim Q_{\mu_i} \\ &= \sum_{i=1}^{k} |ST(\mu_i)| = |ST(\lambda)| = \dim Q_\lambda. \end{aligned}$$

Dies zeigt $Q_i/Q_{i-1} = Q_i/(Q_i \cap \operatorname{Ker}(\varphi_i)) \cong \varphi_i(Q_i) \cong Q_{\mu_i}$ für $i = 1, \ldots, k$. Daraus folgt die erste Behauptung. Für die zweite Behauptung sei $\mu \in P(n+1)$. Mit Frobenius-Reziprozität gilt

$$(\chi_\lambda^{S_{n+1}}, \chi_\mu) = (\chi_\lambda, (\chi_\mu)_{S_n}) = \sum_{\nu \in \mu^-} (\chi_\lambda, \chi_\nu) = \begin{cases} 1 & \text{falls } \mu \in \nu^+ = \lambda^+, \\ 0 & \text{sonst.} \end{cases}$$ □

Bemerkung III.4.46. Um eine handliche Formel für $\chi_\lambda(1)$ herzuleiten, benötigen wir eine Identität von Polynomen. Ein Polynom $\alpha \in K[X_1, \ldots, X_n]$ heißt *homogen* (vom Grad d), falls jedes Monom in α den gleichen Grad (d) besitzt. Produkte von homogenen Polynomen sind wieder homogen, wobei sich der Grad addiert. Offenbar sind die elementarsymmetrischen Polynome homogen.

Lemma III.4.47. *Sei* $\Delta := \prod_{1 \leq i < j \leq m}(X_i - X_j) \in \mathbb{Q}[X_1, \ldots, X_m]$ *und*

$$\alpha := \sum_{i=1}^{m} X_i \Delta(X_1, \ldots, X_i + Y, \ldots, X_m) \in \mathbb{Q}[X_1, \ldots, X_m, Y].$$

Dann gilt

$$\alpha = \Big(X_1 + \ldots + X_m + \binom{m}{2} Y\Big)\Delta.$$

Beweis. Sei $i < j$ und $i \neq k \neq j$. Vertauschen von i und j ändert das Vorzeichen von Δ (siehe Beweis von Satz I.3.26). Damit ändert auch $X_k\Delta(\ldots, X_k + Y, \ldots)$ das Vorzeichen. Durch Vertauschen von i und j werden außerdem die Summanden $X_i\Delta(\ldots, X_i + Y, \ldots)$ und $X_j\Delta(\ldots, X_j + Y, \ldots)$ vertauscht und sie ändern zusätzlich ihr Vorzeichen. Insgesamt ändert α das Vorzeichen beim Vertauschen von i und j. Setzt man $X_i = X_j$, so wird $\alpha = 0$. Als Polynom in X_i hat α daher Nullstelle X_j. Man kann

also den Faktor $X_i - X_j$ im Polynomring $\mathbb{Q}(X_1, \ldots, X_{i-1}, X_{i+1}, \ldots, X_m)[X_i]$ abspalten. Da $X_i - X_j$ normiert ist, treten bei der Division keine Nenner auf. Daher ist $X_i - X_j$ ein Teiler von α im faktoriellen Ring $\mathbb{Q}[X_1, \ldots, X_m]$. Da die Faktoren $X_i - X_j$ von Δ irreduzibel und paarweise nicht assoziiert sind, ist α auch durch Δ teilbar. Sei also $\alpha = \beta\Delta$. Da α und Δ homogen sind, ist β homogen vom Grad 1. Da die Aussage für $Y = 0$ stimmt, gilt $\beta = X_1 + \ldots + X_m + cY$ für ein $c \in \mathbb{Q}$. Man erhält c, indem man nach Y ableitet und anschließend $Y = 0$ setzt. Es gilt

$$\big(X_i\Delta(X_1, \ldots, X_i + Y, \ldots, X_m)\big)'(0) = X_i\Big(\sum_{j>i} \frac{\Delta}{X_i - X_j} - \sum_{j<i} \frac{\Delta}{X_j - X_i}\Big) = X_i\Delta \sum_{j\neq i} \frac{1}{X_i - X_j}$$

$$c = \sum_{i=1}^{m} \sum_{j\neq i} \frac{X_i}{X_i - X_j} = \sum_{i<j} \frac{X_i - X_j}{X_i - X_j} = \binom{m}{2}. \qquad \square$$

Bemerkung III.4.48. Für jede Partition λ sei $f(\lambda) := |ST(\lambda)|$ (wir lassen hier die Partition (0) mit dem „leeren“ Tableau zu). Ist $\lambda \in \mathbb{N}_0^m$ eine beliebige Folge aber keine Partition, so setzen wir $f(\lambda) := 0$. Dann ist f durch die Rekursion aus der Verzweigungsregel eindeutig bestimmt:

$$f(0) = 1, \tag{III.4.2}$$

$$f(\lambda_1, \ldots, \lambda_m, 0) = f(\lambda_1, \ldots, \lambda_m) \qquad (\lambda \in \mathbb{N}_0^m), \tag{III.4.3}$$

$$f(\lambda_1, \ldots, \lambda_m) = 0 \qquad (\exists i : \lambda_i + 1 = \lambda_{i+1}), \tag{III.4.4}$$

$$f(\lambda_1, \ldots, \lambda_m) = f(\lambda_1 - 1, \lambda_2, \ldots, \lambda_m) + \ldots + f(\lambda_1, \ldots, \lambda_{m-1}, \lambda_m - 1) \qquad (\lambda_1 \geq \ldots \geq \lambda_m \geq 1). \tag{III.4.5}$$

Satz III.4.49 (Hakenformel)**.** *Für $\lambda \in P(n)$ mit Young-Diagramm Y gilt*

$$\boxed{\chi_\lambda(1) = \dim Q_\lambda = |ST(\lambda)| = \frac{n!}{\prod\limits_{(s,t)\in Y} h_{st}}.} \tag{III.4.6}$$

Beweis (Glass-Ng). Sei $\lambda = (\lambda_1, \ldots, \lambda_m)$. Es genügt zu zeigen, dass die rechte Seite von (III.4.6) die gleiche Rekursionsvorschrift wie die Funktion f aus Bemerkung III.4.48 erfüllt. Das Produkt der Hakenlängen in der k-ten Zeile von λ ist (von rechts nach links gelesen):

$$[1 \cdot 2 \cdot \ldots \cdot (\lambda_k - \lambda_{k+1})][(\lambda_k - \lambda_{k+1} + 2) \ldots (\lambda_k - \lambda_{k+2} + 1)]$$
$$[(\lambda_k - \lambda_{k+2} + 3) \ldots (\lambda_k - \lambda_{k+3} + 2)] \ldots [(\lambda_k - \lambda_m + m - k + 1) \ldots (\lambda_k + m - k)]$$
$$= \frac{(\lambda_k + m - k)!}{\prod_{l>k}(\lambda_k - \lambda_l - k + l)}.$$

Die rechte Seite von (III.4.6) ist daher

$$g(\lambda) := n!\frac{\prod_{i<j}(\lambda_i - \lambda_j + j - i)}{\prod_{i=1}^{m}(\lambda_i + m - i)!} = \Big(\sum_{i=1}^{m} \lambda_i\Big)!\frac{\Delta(\lambda_1 + m - 1, \lambda_2 + m - 2, \ldots, \lambda_m)}{\prod_{i=1}^{m}(\lambda_i + m - i)!}.$$

Man sieht leicht, dass (III.4.2) für g gilt. Für $\lambda_m = 0$ ist

$$g(\lambda) = n!\frac{\Delta(\lambda_1 + m - 1, \lambda_2 + m - 2, \ldots, \lambda_{m-1} + 1)\prod_{i=1}^{m-1}(\lambda_i + m - i)}{\prod_{i=1}^{m-1}(\lambda_i + m - i)!}$$
$$= n!\frac{\Delta(\lambda_1 + m - 2, \lambda_2 + m - 3, \ldots, \lambda_{m-1})}{\prod_{i=1}^{m-1}(\lambda_i + m - i - 1)!} = g(\lambda_1, \ldots, \lambda_{m-1}),$$

d. h. (III.4.3) gilt. Für $\lambda_i + 1 = \lambda_{i+1}$ ist $\lambda_i + m - i = \lambda_{i+1} + m - (i+1)$ und mit Δ verschwindet auch $g(\lambda)$, d. h. (III.4.4) gilt. Schließlich substituieren wir $X_i := \lambda_i + m - i$ für $i = 1, \ldots, m$ und $Y = -1$ in Lemma III.4.47. Dann ist einerseits

$$\begin{aligned}\alpha &= \sum_{i=1}^{m} (\lambda_i + m - i)\Delta(\lambda_1 + m - 1, \ldots, \lambda_i + m - i - 1, \ldots, \lambda_m) \\ &= \frac{1}{(n-1)!} \prod_{i=1}^{m} (\lambda_i + m - i)! \sum_{i=1}^{m} g(\lambda_1, \ldots, \lambda_i - 1, \ldots, \lambda_m)\end{aligned}$$

und andererseits

$$\begin{aligned}\alpha &= \Big(\sum_{i=1}^{m} (\lambda_i + m - i) - \binom{m}{2}\Big)\Delta(\lambda_1 + m - 1, \ldots, \lambda_m) = n\Delta(\lambda_1 + m - 1, \ldots, \lambda_m) \\ &= \frac{1}{(n-1)!} \prod_{i=1}^{m} (\lambda_i + m - i)! g(\lambda).\end{aligned}$$

Damit folgt auch (III.4.5). □

Beispiel III.4.50. Wir betrachten $\lambda = (4, 2^2, 1)$ und schreiben die Hakenlängen in das Young-Diagramm:

7	5	2	1
4	2		
3	1		
1			

Man berechnet

$$\chi_\lambda(1) = \frac{9!}{7 \cdot 5 \cdot 4 \cdot 3 \cdot 2^2} = 9 \cdot 8 \cdot 3 = 6^3 = 216.$$

Bemerkung III.4.51. Mit den Charakteren der S_n lassen sich Potenzen von Charakteren beliebiger Gruppen in kleinere Bestandteile zerlegen. Seien dafür allgemein G und H endliche Gruppen mit Darstellungen $\Delta\colon G \to \mathrm{GL}(V)$ und $\Gamma\colon H \to \mathrm{GL}(V)$ auf demselben $\mathbb{C}$-Vektorraum V, sodass

$$\Delta(g)\Gamma(h) = \Gamma(h)\Delta(g) \qquad \forall g \in G, h \in H$$

gilt. Wir können $\Delta\Gamma$ als Darstellung von $G \times H$ auffassen. Sei $\Gamma = \bigoplus_{i=1}^{k} a_i\Gamma_i$ mit paarweise nichtähnlichen irreduziblen Darstellungen $\Gamma_1, \ldots, \Gamma_k$ und $a_1, \ldots, a_k \in \mathbb{N}$. Sei d_i der Grad von Γ_i. Dann gilt $\dim V = a_1d_1 + \ldots + a_kd_k$. Wir schreiben $\Delta(g)$ als Blockmatrix $\Delta(g) = (\Delta_{ij}(g))$ mit $\Delta_{ij}(g) \in \mathbb{C}^{a_id_i \times a_jd_j}$. Jeder Block lässt sich weiter zerlegen als $\Delta_{ij}(g) = (\Delta_{ij}^{st}(g))_{s,t}$ mit $\Delta_{ij}^{st}(g) \in \mathbb{C}^{d_i \times d_j}$ für $s = 1, \ldots, a_i$ und $t = 1, \ldots, a_j$. Aus $\Delta(g)\Gamma(h) = \Gamma(h)\Delta(g)$ folgt

$$\Delta_{ij}^{st}(g)\Gamma_j(h) = \Gamma_i(h)\Delta_{ij}^{st}(g) \qquad \forall g \in G, h \in H.$$

Mit Aufgabe II.67 ergibt sich $\Delta_{ij}(g) = 0$ für $i \neq j$ und $\Delta_{ii}^{st}(g) = \lambda_{ist}(g)1_{d_i}$ mit $\lambda_{ist}(g) \in \mathbb{C}$. Es gilt also

$$\Delta(g)\Gamma(h) = \begin{pmatrix} \lambda_{1,1,1}(g)\Gamma_1(h) & & & & * \\ & \ddots & & & \\ & & \lambda_{1,a_1,a_1}\Gamma_1(h) & & \\ & & & \ddots & \\ * & & & & \lambda_{k,a_k,a_k}\Gamma_k(h) \end{pmatrix}.$$

Sei $\Lambda_i(g) := (\lambda_{ist}(g))_{s,t} \in \mathbb{C}^{a_i \times a_i}$. Dann existiert eine Permutationsmatrix T mit

$$T\Delta(g)T^{-1} = \operatorname{diag}\big(\underbrace{\Lambda_1(g), \dots, \Lambda_1(g)}_{d_1}, \dots, \underbrace{\Lambda_k(g), \dots, \Lambda_k(g)}_{d_k}\big).$$

Also sind $\Lambda_1, \dots, \Lambda_k$ (nicht unbedingt irreduzible) Darstellungen von G und Δ ist zu $\bigoplus_{i=1}^k d_i\Lambda_i$ ähnlich. Grad und Vielfachheit von Γ_i und Λ_i verhalten sich umgekehrt zueinander. Für die entsprechenden Charaktere gilt

$$\chi_{\Delta\Gamma}(g,h) = \operatorname{tr}\big(\Delta(g)\Gamma(h)\big) = \sum_{i=1}^k \operatorname{tr}(\Gamma_i(h)) \sum_{s=1}^{a_i} \lambda_{iss} = \sum_{i=1}^k \chi_{\Gamma_i}(h) \operatorname{tr}(\Lambda_i(g)) = \sum_{i=1}^k \chi_{\Lambda_i}(g)\chi_{\Gamma_i}(h) \quad \text{(III.4.7)}$$

für $g \in G$ und $h \in H$.

Satz III.4.52. *Sei χ ein Charakter von G und λ ein Charakter von $H \le S_n$. Für $h \in H$ sei $c_i(h)$ die Anzahl der i-Zyklen von h. Dann besitzt G einen Charakter (oder die Nullabbildung) θ_λ mit*

$$\boxed{\theta_\lambda(g) = \frac{1}{|H|} \sum_{h \in H} \lambda(h) \prod_{i=1}^n \chi(g^i)^{c_i(h)}} \qquad (g \in G)$$

$$\chi^n = \sum_{\lambda \in \operatorname{Irr}(H)} \lambda(1)\theta_\lambda.$$

Beweis. Da die eingerahmte Formel linear in λ ist, können wir $\lambda \in \operatorname{Irr}(H)$ annehmen. Sei W ein $\mathbb{C}G$-Modul zu χ und $V := W \otimes \dots \otimes W$ mit n Faktoren. Sei Ψ eine Darstellung zu W und $\Delta := \Psi \otimes \dots \otimes \Psi$ die diagonale Darstellung auf V, d. h.

$$\Delta(g)(v_1 \otimes \dots \otimes v_n) = \Psi(v_1) \otimes \dots \otimes \Psi(v_n)$$

für $g \in G$ und $v_1 \otimes \dots \otimes v_n \in V$. Schließlich sei $\Gamma\colon H \to \operatorname{GL}(V)$ die Darstellung mit

$$\Gamma(h)(v_1 \otimes \dots \otimes v_n) := v_{h^{-1}(1)} \otimes \dots \otimes v_{h^{-1}(n)}$$

(Aufgabe III.14). Offenbar gilt $\Delta(g)\Gamma(h) = \Gamma(h)\Delta(g)$ für alle $g \in G$ und $h \in H$. Wir können also Bemerkung III.4.51 anwenden. Jeder irreduzible Bestandteil Γ_i von Γ entspricht einem $\lambda \in \operatorname{Irr}(H)$ (wir lassen zu, dass die Vielfachheit a_i gleich 0 sein kann). Entsprechend hat man eine Darstellung Λ_i von G mit Charakter θ_λ oder die Nullabbildung, falls $a_i = 0$. Die Vielfachheit von Λ_i als Summand von Δ ist $\lambda(1)$. Dies zeigt

$$\chi^n = \chi_\Delta = \sum_{\lambda \in \operatorname{Irr}(H)} \lambda(1)\theta_\lambda.$$

Aus Bemerkung III.4.51 erhält man

$$\chi_{\Delta\Gamma}(g,h) = \sum_{\lambda \in \operatorname{Irr}(H)} \theta_\lambda(g)\chi_\lambda(h) \quad \text{(III.4.8)}$$

für $(g,h) \in G \times H$. Wir berechnen diesen Charakter auf andere Weise. Sei $b_1, \dots, b_d \in W$ eine Basis von W. Sei $[d] := \{1, \dots, d\}$ und $[d]^n := \{f\colon [n] \to [d]\}$. Dann ist

$$\big\{b_f := b_{f(1)} \otimes \dots \otimes b_{f(n)} : f \in [d]^n\big\}$$

eine Basis von V. Mit $\Psi(g) = (\alpha_{ij}(g)) \in \mathbb{C}^{d\times d}$ gilt $\chi(g) = \sum_{i=1}^d \alpha_{ii}(g)$, $\chi(g^2) = \sum_{i,j=1}^d \alpha_{ij}(g)\alpha_{ji}(g)$ und induktiv

$$\chi(g^k) = \sum_{f\in[d]^k} \alpha_{f(1),f(2)}(g)\alpha_{f(2),f(3)}(g)\dots\alpha_{f(k),f(1)}(g) \tag{III.4.9}$$

für $k \in \mathbb{N}$. Wir berechnen

$$\begin{aligned}\Delta(g)\Gamma(h)b_f &= \Delta(g)(b_{fh^{-1}(1)} \otimes \dots \otimes b_{fh^{-1}(n)}) \\ &= \Big(\sum_{j=1}^d \alpha_{j,fh^{-1}(1)}b_j\Big) \otimes \dots \otimes \Big(\sum_{j=1}^d \alpha_{j,fh^{-1}(n)}b_j\Big) \\ &= \sum_{f'\in[d]^n} \alpha_{f'(1),fh^{-1}(1)}\dots\alpha_{f'(n),fh^{-1}(n)}b_{f'}.\end{aligned}$$

Daraus folgt

$$\chi_{\Delta\Gamma}(g,h) = \sum_{f\in[d]^n} \alpha_{f(1),fh^{-1}(1)}\dots\alpha_{f(n),fh^{-1}(n)}.$$

Sei $h = h_1\dots h_k$ die Zerlegung in disjunkte Zyklen (inklusive Einerzyklen), wobei k_i die Länge von h_i sei. Sei $[h_i]$ die Menge der Ziffern in h_i und $x_i \in [h_i]$. Anstelle von $1,\dots,n$ kann man die α auch in der Reihenfolge der Zyklen multiplizieren:

$$\begin{aligned}\chi_{\Delta\Gamma}(g,h) &= \sum_{f\in[d]^n}\prod_{i=1}^k \alpha_{f(x_i),fh^{-1}(x_i)}\alpha_{fh^{-1}(x_i),fh^{-2}(x_i)}\dots\alpha_{fh^{1-k_i}(x_i),f(x_i)} \\ &= \prod_{i=1}^k\Big(\sum_{f\in[h_i]^n} \alpha_{f(x_i),fh^{-1}(x_i)}\alpha_{fh^{-1}(x_i),fh^{-2}(x_i)}\dots\alpha_{fh^{1-k_i}(x_i),f(x_i)}\Big) \qquad \text{(III.4.10)} \\ &\overset{\text{(III.4.9)}}{=} \prod_{i=1}^k \chi(g^{k_i}) = \prod_{i=1}^n \chi(g^i)^{c_i(h)}.\end{aligned}$$

Nach der ersten Orthogonalitätsrelation ist schließlich

$$\begin{aligned}\theta_\lambda(g) &= \sum_{\mu\in\mathrm{Irr}(H)} \theta_\mu(g)(\lambda,\mu) = \sum_{\mu\in\mathrm{Irr}(H)} \theta_\mu(g)\frac{1}{|H|}\sum_{h\in H}\lambda(h)\mu(h) = \frac{1}{|H|}\sum_{h\in H}\lambda(h)\sum_{\mu\in\mathrm{Irr}(H)}\theta_\mu(g)\mu(h) \\ &\overset{\text{(III.4.8)}}{=} \frac{1}{|H|}\sum_{h\in H}\lambda(h)\chi_{\Delta\Gamma}(g,h) \overset{\text{(III.4.10)}}{=} \frac{1}{|H|}\sum_{h\in H}\lambda(h)\prod_{i=1}^n\chi(g^i)^{c_i(h)}.\end{aligned}$$

□

Folgerung III.4.53. *Sei ψ ein Charakter von G und $\lambda \in P(n)$. Dann besitzt G einen Charakter (oder die Nullabbildung) θ_λ mit*

$$\boxed{\theta_\lambda(g) = \frac{1}{n!}\sum_{\sigma\in S_n}\chi_\lambda(\sigma)\prod_{i=1}^n\psi(g^i)^{c_i(\sigma)}} \qquad (g\in G),$$

$$\psi^n = \sum_{\lambda\in P(n)}\chi_\lambda(1)\theta_\lambda.$$

Beweis. Wähle $H = S_n$ und χ_λ anstelle von λ in Satz III.4.52. □

Bemerkung III.4.54. In der Situation von Folgerung III.4.53 nennt man θ_λ den *Symmetrisator* von ψ bzgl. $\lambda \in P(n)$.

Beispiel III.4.55.

(i) Für lineare Charaktere ψ gilt

$$\theta_\lambda(g) = \frac{1}{n!}\sum_{\sigma\in S_n} \chi_\lambda(\sigma)\psi(g)^n = \begin{cases}\psi(g)^n & \text{falls } \lambda = (n),\\ 0 & \text{sonst.}\end{cases}$$

(ii) Für $n = 2$ gilt

$$\theta_{(2)}(g) = \frac{1}{2}\big(\psi(g)^2 + \psi(g^2)\big), \qquad \theta_{(1^2)}(g) = \frac{1}{2}\big(\psi(g)^2 - \psi(g^2)\big)$$

Man nennt $\theta_{(2)}$ das *symmetrische Quadrat* und $\theta_{(1^2)}$ das *alternierende Quadrat* von ψ. Sie sind für Frobenius-Schur-Indikatoren relevant (Kapitel A.12).

(iii) Für $n = 3$ erhält man

$$\begin{aligned}\theta_{(3)}(g) &= \frac{1}{6}\big(\psi(g)^3 + 3\psi(g)\psi(g^2) + 2\psi(g^3)\big),\\ \theta_{(1^3)}(g) &= \frac{1}{6}\big(\psi(g)^3 - 3\psi(g)\psi(g^2) + 2\psi(g^3)\big),\\ \theta_{(2,1)}(g) &= \frac{1}{3}\big(\psi(g)^3 - \psi(g^3)\big).\end{aligned}$$

Für $\psi(1) \le 2$ ist $\theta_{(1^3)} = 0$.

(iv) Wir wählen $H = \langle(1,\dots,n)\rangle \le S_n$ in Satz III.4.52 und $\lambda \in \mathrm{Irr}(H)$ treu. Für $d \mid n$ sei $f(d)$ die Summe der primitiven d-ten Einheitswurzeln. Dann gilt $f(1) = 1$ und $\sum_{d|n} f(d) = 0$ für $n > 1$. Mit Möbius-Inversion folgt $f = \mu$ und

$$\theta_\lambda(g) = \frac{1}{n}\sum_{d|n}\sum_{\substack{h\in H\\ |\langle h\rangle| = d}} \lambda(h)\psi(g^d)^{\frac{n}{d}} = \frac{1}{n}\sum_{d|n}\mu(d)\psi(g^d)^{\frac{n}{d}}.$$

Im Fall $n = p \in \mathbb{P}$ vereinfacht sich dies zu

$$\theta_\lambda(g) = \frac{1}{p}\big(\psi(g)^p - \psi(g^p)\big).$$

(v) Für $H = V_4 \le S_4$ und $\lambda \in \mathrm{Irr}(H) \setminus \{\mathbb{1}_H\}$ erhält man

$$\theta_\lambda(g) = \frac{1}{4}\big(\psi(g)^4 - \psi(g^2)^2\big).$$

Definition III.4.56. Für $\lambda \in P(n)$ und $d \in \mathbb{N}$ nennt man

$$\beta_\lambda := \frac{1}{n!}\sum_{\sigma\in S_n}\chi_\lambda(\sigma)\prod_{i=1}^{n}(X_1^i + \ldots + X_d^i)^{c_i(\sigma)}$$

das *Schur-Polynom* zu λ.

Bemerkung III.4.57.

(i) Offenbar ist β_λ ein symmetrisches Polynom, welches (wie die elementarsymmetrischen Polynome) auch von d abhängt. Sei ψ ein Charakter von G vom Grad d. Für $g \in G$ existieren bekanntlich Einheitswurzeln $\zeta_1, \ldots, \zeta_d \in \mathbb{C}$ mit $\psi(g^i) = \zeta_1^i + \ldots + \zeta_d^i$ für $i \in \mathbb{N}_0$. Nach Folgerung III.4.53 gilt $\theta_\lambda(g) = \beta_\lambda(\zeta_1, \ldots, \zeta_d)$.

(ii) Wir bestimmen nun die irreduziblen Charaktere der alternierenden Gruppe. Sei $\xi \in \mathrm{Irr}(A_n)$ und $\chi_\lambda \in \mathrm{Irr}(S_n)$ ein Bestandteil von ξ^{S_n}. Im Fall $\lambda \neq \lambda'$ kommt auch $\chi_{\lambda'} = \operatorname{sgn} \chi_\lambda$ in ξ^{S_n} vor, denn $((\chi_{\lambda'})_{A_n}, \xi) = ((\chi_\lambda)_{A_n}, \xi) \neq 0$. Offenbar gilt $\xi^{S_n} = \chi_\lambda + \chi_{\lambda'}$ und $\xi_\lambda := \xi = (\chi_\lambda)_{A_n}$. Im Fall $\lambda' = \lambda$ hingegen ist $\xi^{S_n} = \chi_\lambda$ und

$$(\chi_\lambda) = \xi + {}^{(1,2)}\xi =: \xi_\lambda^+ + \xi_\lambda^-$$

nach Clifford (die Zuordnung $\xi \leftrightarrow \xi_\lambda^+$ ist willkürlich). Sei $\sigma \in A_n$. Sind σ und ${}^{(1,2)}\sigma$ in A_n konjugiert, so gilt $\xi(\sigma) = \frac{1}{2}\chi_\lambda(\sigma)$. Für die restlichen Charakterwerte müssen wir die Konjugationsklasse von A_n untersuchen, die keine Konjugationsklassen von S_n.

Satz III.4.58. *Sei $\sigma \in A_n$ vom Zyklentyp $(\lambda_1, \ldots, \lambda_k)$. Genau dann ist σ nicht zu ${}^{(1,2)}\sigma$ in A_n konjugiert, wenn die λ_i ungerade und paarweise verschieden sind.*

Beweis. Sei $\sigma \in C \in \mathrm{Cl}(A_n)$. Genau dann gilt $C \in \mathrm{Cl}(S_n)$, wenn $|A_n : \mathrm{C}_{A_n}(\sigma)| = |K| = |S_n : \mathrm{C}_{S_n}(\sigma)|$. Wegen $|A_n : \mathrm{C}_{A_n}(\sigma)| = |A_n : A_n \cap \mathrm{C}_{S_n}(\sigma)| = |A_n \mathrm{C}_{S_n}(\sigma) : \mathrm{C}_{S_n}(\sigma)|$ ergibt sich

$$C \notin \mathrm{Cl}(S_n) \iff \mathrm{C}_{S_n}(\sigma) \subseteq A_n.$$

Sei $\sigma = \sigma_1 \ldots \sigma_k$ mit disjunkten Zyklen σ_i der Länge λ_i. Ist λ_i gerade, so ist $\sigma_i \in \mathrm{C}_{S_n}(g) \setminus A_n$. Also können wir annehmen, dass alle λ_i ungerade sind. Sei $\lambda_i = \lambda_j$ mit $i \neq j$. Wir schreiben $\sigma_i = (a_1, \ldots, a_{\lambda_i})$ und $\sigma_j = (b_1, \ldots, b_{\lambda_i})$. Dann ist $\tau := (a_1, b_1)(a_2, b_2) \ldots (a_{\lambda_i}, b_{\lambda_i}) \notin \mathrm{C}_{S_n}(\sigma) \setminus A_n$.

Seien nun umgekehrt die λ_i ungerade und paarweise verschieden. Wir berechnen $|S_n : \mathrm{C}_{S_n}(\sigma)|$, indem wir die Elemente vom Zyklentyp $(\lambda_1, \ldots, \lambda_k)$ zählen. Für die λ_1 Elemente des Zyklus σ_1 gibt es $\frac{n!}{(n-\lambda_1)!}$ Möglichkeiten. Davon liefern allerdings je λ_1 Möglichkeiten das gleiche Element. Also gibt es $\frac{n!}{\lambda_1(n-\lambda_1)!}$ Möglichkeiten für σ_1. Analog gibt es danach noch $\frac{(n-\lambda_1)!}{\lambda_2(n-\lambda_1-\lambda_2)!}$ Möglichkeiten für σ_2 usw. Dies zeigt

$$|S_n : \mathrm{C}_{S_n}(\sigma)| = \frac{n!(n-\lambda_1)!(n-\lambda_1-\lambda_2)! \ldots (n-\lambda_1-\ldots-\lambda_{k-1})!}{\lambda_1 \ldots \lambda_k (n-\lambda_1)!(n-\lambda_1-\lambda_2)! \ldots (\underbrace{n-\lambda_1-\ldots-\lambda_k}_{=0})!} = \frac{n!}{\lambda_1 \ldots \lambda_k}$$

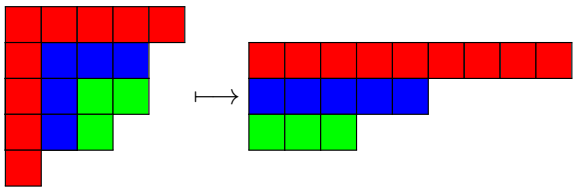
und $|\mathrm{C}_{S_n}(\sigma)| = \lambda_1 \ldots \lambda_k$. Offenbar ist $\langle \sigma_1 \rangle \ldots \langle \sigma_k \rangle \subseteq \mathrm{C}_{S_n}(\sigma)$ und $|\langle \sigma_1 \rangle \ldots \langle \sigma_k \rangle| = |\langle \sigma_1 \rangle| \ldots |\langle \sigma_k \rangle| = \lambda_1 \ldots \lambda_k$. Also ist $\mathrm{C}_{S_n}(\sigma) = \langle \sigma_1 \rangle \ldots \langle \sigma_k \rangle \subseteq A_n$. □

Beispiel III.4.59. Für $n \geq 3$ gibt es stets ein $C \in \mathrm{Cl}(A_n)$ mit $C \notin \mathrm{Cl}(S_n)$. Für ungerades n kann man Zyklentyp (n) in Satz III.4.58 wählen und für gerades n Zyklentyp $(n-1, 1)$.

Bemerkung III.4.60. Wie üblich operiert $\langle (1,2) \rangle$ auf $\mathrm{Irr}(A_n)$ und auf $\mathrm{Cl}(A_n)$. Nach Brauers Permutationslemma gibt es genau so viele Paare ${}^{(1,2)}\xi_\lambda \neq \xi_\lambda \in \mathrm{Irr}(A_n)$ wie es Paare ${}^{(1,2)}C \neq C \in \mathrm{Cl}(A_n)$ gibt.

Dies sieht man auch durch die Bijektion:

$$\Phi\colon \{\lambda = \lambda' \in P(n)\} \longrightarrow \{\lambda = (\lambda_1, \ldots, \lambda_k) \in P(n) \text{ mit } \lambda_i \text{ ungerade und paarweise verschieden}\},$$
$$(\lambda_1, \ldots, \lambda_k) \longmapsto (h_{11}, h_{22}, \ldots) = (2\lambda_1 - 1, 2\lambda_2 - 3, 2\lambda_3 - 5, \ldots)$$



Sei $\lambda = \lambda' \in P(n)$ und $g \in A_n$ vom Zyklentyp $\mu = (\mu_1, \ldots, \mu_k)$. Bei geeigneter Wahl der ξ_λ gilt

$$\xi_\lambda^{\pm}(g) = \begin{cases} \frac{1}{2}\chi_\lambda(\mu) \pm \frac{1}{2}\sqrt{(-1)^{\frac{n-k}{2}}\mu_1 \ldots \mu_k} & \text{falls } \mu = \Phi(\lambda) \\ \frac{1}{2}\chi_\lambda(\mu) & \text{falls } \mu \neq \Phi(\lambda) \end{cases}$$

(ohne Beweis).

Beispiel III.4.61. Für $n = 5$ ist $\lambda = (3, 1^2) = \lambda'$ die einzige symmetrische Partition und $\Phi(\lambda) = (5)$. Aus Beispiel III.4.28 die Charaktertafel von A_5:

A_5	(1^5)	$(2^2, 1)$	$(3, 1^2)$	$(5)^+$	$(5)^-$
(5)	1	1	1	1	1
$(4, 1)$	4	0	1	-1	-1
$(3, 2)$	5	1	-1	0	0
$(3, 1^2)^+$	3	-1	0	$\frac{1+\sqrt{5}}{2}$	$\frac{1-\sqrt{5}}{2}$
$(3, 1^2)^-$	3	-1	0	$\frac{1-\sqrt{5}}{2}$	$\frac{1+\sqrt{5}}{2}$

5 Kategorien-Theorie

Bemerkung III.5.1.

(i) Eine mathematische Kategorie ist ein Oberbegriff für nahezu alle algebraischen Objekte wie Mengen, Gruppen, Vektorräume, Ringe, Moduln etc. In diesem Kapitel entwickeln wir eine abstrakte Theorie für Kategorien, die viele der Beweise aus früheren Kapiteln vereinheitlicht. Mit Hilfe der Yoneda-Einbettung lässt sich jede (lokal kleine) Kategorie in eine größere Kategorie mit „besseren“ Eigenschaften einbetten. Wir hatten beispielsweise bereits gesehen, dass man Sätze über endliche Gruppen beweisen kann, indem man mit den entsprechenden Gruppenalgebren arbeitet. Gruppenalgebren oder allgemeine Ringe kann man wiederum durch ihre Modulkategorie studieren.

(ii) Bekanntlich ist die Ansammlung aller Mengen selbst keine Menge. Im Folgenden verwenden wir informell den Begriff *Klasse*, um Ansammlungen dieser Art zu beschreiben. Wir benutzen die üblichen Regeln der Mengenlehre auch für Klassen.

Definition III.5.2. Eine *Kategorie* $\mathcal{C}$ besteht aus

- einer Klasse $\mathrm{Ob}(\mathcal{C})$ von *Objekten*,
- Klassen $\mathrm{Hom}_{\mathcal{C}}(A,B)$ von *Morphismen* für alle $A,B \in \mathrm{Ob}(\mathcal{C})$.

Dabei gilt

- $\mathrm{Hom}_{\mathcal{C}}(A,B) \cap \mathrm{Hom}_{\mathcal{C}}(C,D) = \varnothing$ falls $(A,B) \neq (C,D)$.
- Für $A,B,C \in \mathrm{Ob}(\mathcal{C})$ existiert eine Verknüpfung

$$\mathrm{Hom}_{\mathcal{C}}(A,B) \times \mathrm{Hom}_{\mathcal{C}}(B,C) \to \mathrm{Hom}_{\mathcal{C}}(A,C), \qquad (f,g) \mapsto g \circ f$$

  mit $f \circ (g \circ h) = (f \circ g) \circ h$ (falls definiert).
- Für $A \in \mathrm{Ob}(\mathcal{C})$ existiert eine *Identität* $\mathrm{id}_A \in \mathrm{Hom}_{\mathcal{C}}(A,A)$ mit $f \circ \mathrm{id}_A = f = \mathrm{id}_B \circ f$ für alle $B \in \mathrm{Ob}(\mathcal{C})$ und $f \in \mathrm{Hom}_{\mathcal{C}}(A,B)$.

Bemerkung III.5.3.

(i) Wir schreiben Morphismen $f \in \mathrm{Hom}_{\mathcal{C}}(A,B)$ häufig in der Form $f\colon A \to B$, auch wenn es sich nicht um Abbildungen handeln muss. Ebenso werden wir das Kompositionszeichen $\circ$ gelegentlich einsparen.

(ii) Wie üblich zeigt man, dass id_A durch die Eigenschaft $f \circ \mathrm{id}_A = f = \mathrm{id}_B \circ f$ eindeutig bestimmt ist. Daher lassen sich die Objekte einer Kategorie aus den Morphismen rekonstruieren.

(iii) Eine Kategorie $\mathcal{C}$ heißt *lokal klein*, wenn $\mathrm{Hom}_{\mathcal{C}}(A,B)$ für alle $A,B \in \mathrm{Ob}(\mathcal{C})$ eine Menge ist (anstatt einer Klasse). Ist zusätzlich $\mathrm{Ob}(\mathcal{C})$ eine Menge, so nennt man $\mathcal{C}$ *klein*.

Beispiel III.5.4.

(i) Die (lokal kleine) Kategorie **Set** besteht aus allen Mengen als Objekte und $\mathrm{Hom}(A,B)$ ist die Menge aller Abbildungen $f\colon A \to B$ für Mengen $A, B \in \mathrm{Ob}(\mathbf{Set})$ mit der üblichen Identitätsabbildung. Möchte man nur endliche Mengen als Objekte zulassen, so erhält man die *Unterkategorie* **set**. Analog kann man sich auf injektive, surjektive oder bijektive Morphismen beschränken. Bekanntlich ist weder **Set** noch **set** klein.

(ii) In ähnlicher Weise erhält man die Kategorien **Grp**, **grp**, **Ab**, **Rng** aller Gruppen, aller endlichen Gruppen, aller abelschen Gruppe und aller Ringe. Hierbei besteht $\mathrm{Hom}(A,B)$ nur aus den entsprechenden Homomorphismen. Für einen Ring R seien ${}_R\mathbf{Mod}$, $\mathbf{Mod}_R$, ${}_R\mathbf{mod}$ die Kategorien aller R-Linksmoduln, aller R-Rechtsmoduln und aller endlich-erzeugten R-Linksmoduln.

(iii) Sei R ein kommutativer Ring und $\mathrm{Ob}(\mathcal{C}) = \mathbb{N}$. Für $a, b \in \mathbb{N}$ sei $\mathrm{Hom}(a,b) = R^{a\times b}$. Mit der Matrizenmultiplikation als Verknüpfung wird R-**mat** $:= \mathcal{C}$ eine Kategorie.

(iv) Jede Gruppe G kann man als Kategorie mit einem Objekt A auffassen. Dabei ist $\mathrm{Hom}(A,A) = G$ und $x \circ y = xy$ für $x, y \in G$.

(v) Zu jeder Kategorie $\mathcal{C}$ gibt es die *duale* Kategorie $\mathcal{C}^o$ mit $\mathrm{Ob}(\mathcal{C}^o) := \mathrm{Ob}(\mathcal{C})$, $\mathrm{Hom}_{\mathcal{C}^o}(A,B) := \mathrm{Hom}_{\mathcal{C}}(B,A)$ und $f \circ_{\mathcal{C}^o} g := g \circ_{\mathcal{C}} f$ für $f \in \mathrm{Hom}_{\mathcal{C}^o}(B,C)$ und $g \in \mathrm{Hom}_{\mathcal{C}^o}(A,B)$.

(vi) Für Kategorien $\mathcal{C}, \mathcal{D}$ definiert man die *Produktkategorie* $\mathcal{C}\times\mathcal{D}$ durch $\mathrm{Ob}(\mathcal{C}\times\mathcal{D}) := \mathrm{Ob}(\mathcal{C}) \times \mathrm{Ob}(\mathcal{D})$, $\mathrm{Hom}_{\mathcal{C}\times\mathcal{D}}((A,B),(C,D)) := \mathrm{Hom}_{\mathcal{C}}(A,C) \times \mathrm{Hom}_{\mathcal{D}}(B,D)$, $\mathrm{id}_{(A,B)} := (\mathrm{id}_A, \mathrm{id}_B)$ und $(f,g)\circ(f',g') := (f\circ f', g\circ g')$.

Definition III.5.5. Ein Morphismus $f \in \mathrm{Hom}_{\mathcal{C}}(A,B)$ einer Kategorie $\mathcal{C}$ heißt

- *Monomorphismus*, falls für alle $C \in \mathrm{Ob}(\mathcal{C})$ und $g, h \in \mathrm{Hom}_{\mathcal{C}}(C,A)$ gilt $f\circ g = f\circ h \Longrightarrow g = h$.
- *Epimorphismus*, falls für alle $C \in \mathrm{Ob}(\mathcal{C})$ und $g, h \in \mathrm{Hom}_{\mathcal{C}}(B,C)$ gilt $g\circ f = h\circ f \Longrightarrow g = h$.
- *Isomorphismus*, falls ein $g \in \mathrm{Hom}_{\mathcal{C}}(B,A)$ mit $f\circ g = \mathrm{id}_B$ und $g\circ f = \mathrm{id}_A$ existiert. Ggf. schreibt man $A \cong_{\mathcal{C}} B$ (für $\mathcal{C} = {}_R\mathbf{Mod}$ benutzen wir weiterhin $\simeq$). Im Fall $A = B$ nennt man f einen *Automorphismus*.

Beispiel III.5.6.

(i) Jeder Isomorphismus ist offenbar ein Mono- und Epimorphismus. Die Monomorphismen (bzw. Epimorphismen) in $\mathcal{C}$ entsprechen den Epimorphismen (bzw. Monomorphismen) in $\mathcal{C}^o$.

(ii) Für alle $A \in \mathrm{Ob}(\mathcal{C})$ ist id_A ein Isomorphismus. Sei $f \in \mathrm{Hom}_{\mathcal{C}}(A,B)$ ein Isomorphismus. Wie üblich existiert genau ein $g \in \mathrm{Hom}_{\mathcal{C}}(B,A)$ mit $f\circ g = \mathrm{id}_B$ und $g\circ f = \mathrm{id}_A$. Wir schreiben $f^{-1} := g$. Offenbar ist auch f^{-1} ein Isomorphismus. Sind $f\colon A\to B$ und $g\colon B\to C$ Isomorphismen, so auch $g\circ f$. Daher bilden die Automorphismen von A eine Gruppe $\mathrm{Aut}_{\mathcal{C}}(A)$.

(iii) Man zeigt leicht, dass die Mono-, Epi- und Isomorphismen in **Set** genau die injektiven, surjektiven und bijektiven Abbildungen sind.

(iv) Sei $\mathrm{Ob}(\mathcal{C}) = \{A, B\}$ mit $\mathrm{Hom}_{\mathcal{C}}(A,A) = \{\mathrm{id}_A\}$, $\mathrm{Hom}_{\mathcal{C}}(B,B) = \{\mathrm{id}_B\}$, $\mathrm{Hom}_{\mathcal{C}}(A,B) = \varnothing$. Dann ist jeder Morphismus $B \to A$ ein Mono- und Epimorphismus, aber kein Isomorphismus. Insbesondere müssen Monomorphismen nicht injektiv und Epimorphismen nicht surjektiv sein (falls Morphismen Abbildungen zwischen Mengen sind).

(v) Sei $f\colon \mathbb{Q} \to R$ ein Ringhomomorphismus. Für $a, b \in \mathbb{Z}$ mit $b \neq 0$ gilt $f(b)f(\frac{1}{b}) = f(b \cdot \frac{1}{b}) = 1$ und $f(\frac{a}{b}) = f(a)f(b)^{-1}$. Daher ist f durch $f(a)$ für $a \in \mathbb{Z}$ bereits eindeutig bestimmt. Also ist $\mathbb{Z} \hookrightarrow \mathbb{Q}$ ein nicht-surjektiver Epimorphismus in **Rng**.

Satz III.5.7. *In* **Grp**, **Ab** *und* ${}_R\mathbf{Mod}$ *sind die Mono-, Epi- und Isomorphismen genau die injektiven, surjektiven bzw. bijektiven Homomorphismen.*

Beweis. Sei $\mathcal{C} \in \{\mathbf{Grp}, \mathbf{Ab}, {}_R\mathbf{Mod}\}$. Offensichtlich sind injektive, surjektive und bijektive Homomorphismen Monomorphismen, Epimorphismen bzw. Isomorphismen in $\mathcal{C}$. Sei nun $f\colon A \to B$ ein Monomorphismus in $\mathcal{C}$. Sei $x \in \mathrm{Ker}(f)$ und $K := \langle x \rangle$. Dann existieren Homomorphismen $g, h\colon K \to A$ mit $g(x) = x$ und $h(x) = 1$ (bzw. $h(x) = 0$ in ${}_R\mathbf{Mod}$). Aus $f \circ g = f \circ h$ folgt $g = h$ und $x = 1$ (bzw. 0). Also ist f injektiv.

Sei schließlich $f\colon A \to B$ ein Epimorphismus in $\mathcal{C}$. Im Fall $\mathcal{C} \in \{\mathbf{Ab}, {}_R\mathbf{Mod}\}$ existiert der triviale Homomorphismus $g\colon B/f(A) \to B/f(A)$ und $h := \mathrm{id}_{B/f(A)}$. Aus $g \circ f = h \circ f$ folgt $f = h$ und $B = f(A)$, d. h. f ist surjektiv. Sei nun $\mathcal{C} = \mathbf{Grp}$. Sei $\Omega := B/f(A) \dot\cup \{\omega\}$ und

$$g\colon B \to \mathrm{Sym}(B/f(A)) \hookrightarrow \mathrm{Sym}(\Omega)$$

die Operation durch Linksmultiplikation auf $B/f(A)$. Sei $t\colon \mathrm{Sym}(\Omega) \to \mathrm{Sym}(\Omega)$ der von der Transposition $(1f(A), \omega)$ induzierte innere Automorphismus. Für $h := t \circ g$ gilt dann $g \circ f = h \circ f$, denn $g(f(A))$ ist im Stabilisator von $1f(A)$. Da B transitiv auf $B/f(A)$ operiert, muss $f(A) = B$ gelten, d. h. f is surjektiv. □

Definition III.5.8. Ein *Funktor* zwischen Kategorien $\mathcal{C}$ und $\mathcal{D}$ ist eine Klasse von Abbildungen $\Phi\colon \mathrm{Ob}(\mathcal{C}) \to \mathrm{Ob}(\mathcal{D})$ und $\Phi\colon \mathrm{Hom}_{\mathcal{C}}(A, B) \to \mathrm{Hom}_{\mathcal{D}}(\Phi(A), \Phi(B))$ mit folgenden Eigenschaften:

- $\Phi(\mathrm{id}_A) = \mathrm{id}_{\Phi(A)}$,
- $\Phi(g \circ f) = \Phi(g) \circ \Phi(f)$ für $f \in \mathrm{Hom}_{\mathcal{C}}(A, B)$ und $g \in \mathrm{Hom}_{\mathcal{C}}(B, C)$.

Wir schreiben ggf. $\Phi\colon \mathcal{C} \to \mathcal{D}$. Man nennt Φ

- *voll*, falls $\Phi\colon \mathrm{Hom}_{\mathcal{C}}(A, B) \to \mathrm{Hom}_{\mathcal{D}}(\Phi(A), \Phi(B))$ für alle $A, B \in \mathrm{Ob}(\mathcal{C})$ surjektiv ist.
- *treu*, falls $\Phi\colon \mathrm{Hom}_{\mathcal{C}}(A, B) \to \mathrm{Hom}_{\mathcal{D}}(\Phi(A), \Phi(B))$ für alle $A, B \in \mathrm{Ob}(\mathcal{C})$ injektiv ist.

Das *Bild* von Φ ist die Kategorie $\Phi(\mathcal{C})$ mit $\mathrm{Ob}(\Phi(\mathcal{C})) = \{\Phi(A) : A \in \mathrm{Ob}(\mathcal{C})\}$ und $\mathrm{Hom}_{\Phi(\mathcal{C})}(A, B) = \{\Phi(f) : f \in \mathrm{Hom}_{\mathcal{C}}(A, B)\}$.

Beispiel III.5.9.

(i) Der *Identitätsfunktor* $\mathrm{id}_{\mathcal{C}}\colon \mathcal{C} \to \mathcal{C}$ mit $A \mapsto A$ und $f \mapsto f$ für $A \in \mathrm{Ob}(\mathcal{C})$ und $f \in \mathrm{Hom}(A, B)$ ist voll und treu.

(ii) Für $D \in \mathrm{Ob}(\mathcal{D})$ existiert der *konstante* Funktor $\Phi_D\colon \mathcal{C} \to \mathcal{D}$ mit $\Phi(A) := D$ und $\Phi(f) := \mathrm{id}_D$ für $A \in \mathrm{Ob}(\mathcal{C})$ und $f \in \mathrm{Hom}_{\mathcal{C}}(A, B)$. Im Allgemeinen ist Φ_D weder voll noch treu.

(iii) Sogenannte *Vergiss-Funktoren* $\Phi\colon \mathbf{Rng} \to \mathbf{Ab}$, $\mathbf{Ab} \to \mathbf{Grp}$, $\mathbf{Grp} \to \mathbf{Set}$, … mit $\Phi(A) = A$ und $\Phi(f) = f$ für $f \in \mathrm{Hom}(A, B)$. Der Funktor „vergisst“ also die algebraische Struktur einer (abelschen) Gruppe oder eines Rings. Sie sind treu, aber im Allgemeinen nicht voll. Obwohl sie treu sind, ist die Abbildung $\Phi\colon \mathrm{Ob}(\mathbf{Grp}) \to \mathrm{Ob}(\mathbf{Set})$ nicht injektiv.

(iv) Für eine lokal kleine Kategorie $\mathcal{C}$ und $A \in \mathrm{Ob}(\mathcal{C})$ existiert der *Hom-Funktor*

$$\mathrm{Hom}(A,.)\colon \mathcal{C} \to \mathbf{Set}, \qquad B \mapsto \mathrm{Hom}_{\mathcal{C}}(A,B)$$

mit $\mathrm{Hom}(A,f)(g) := f \circ g$ für $f \in \mathrm{Hom}_{\mathcal{C}}(B,C)$ und $g \in \mathrm{Hom}_{\mathcal{C}}(A,B)$.

(v) $\mathrm{GL}(n,.)\colon \mathbf{Rng} \to \mathbf{Grp}$, $R \mapsto \mathrm{GL}(n,R)$ und $\mathrm{GL}(n,f)(a_{ij}) := (f(a_{ij}))$ für $f \in \mathrm{Hom}(R,S)$.

(vi) $\Phi_K\colon \mathbf{grp} \to \mathbf{Rng}$, $G \mapsto KG$ für einen Körper K. Für $f\colon G \to H$ ist $\Phi_K(f)(\sum_{g\in G} \alpha_g g) := \sum_{g\in G} \alpha_g f(g)$.

(vii) Sei G eine Gruppe und $\mathcal{C}$ die dazu gehörige Kategorie aus Beispiel III.5.4(iv) mit $\mathrm{Ob}(\mathcal{C}) = \{A\}$. Sei $\Phi\colon \mathcal{C} \to \mathbf{Set}$ ein Funktor und $\Omega := \Phi(A)$. Für $g,h \in G$ gilt $\Phi(gh) = \Phi(g)\Phi(h)$. Daher ist $\Phi\colon G \to \mathrm{Sym}(\Omega)$ eine Gruppenoperation. Analog entspricht jeder Funktor $\mathcal{C} \to K\text{-}\mathbf{mat}$ einer Darstellung von G.

(viii) Sind $\Phi\colon \mathcal{C} \to \mathcal{D}$ und $\Psi\colon \mathcal{D} \to \mathcal{E}$ Funktoren, so auch $\Psi \circ \Phi\colon \mathcal{C} \to \mathcal{E}$. Man nennt Φ einen *Isomorphismus* von Kategorien, falls ein Funktor $\Psi\colon \mathcal{D} \to \mathcal{C}$ mit $\Psi \circ \Phi = \mathrm{id}_{\mathcal{C}}$ und $\Phi \circ \Psi = \mathrm{id}_{\mathcal{D}}$ existiert. Ggf. schreiben wir $\mathcal{C} \cong \mathcal{D}$.

(ix) Transponieren liefert einen (zu sich selbst inversen) Isomorphismus $\Phi\colon K\text{-}\mathbf{mat} \to K\text{-}\mathbf{mat}^o$, $n \mapsto n$, $A \mapsto A^{\mathrm{t}}$.

(x) Für einen Ring R ist ${}_R\mathbf{Mod} \cong \mathbf{Mod}_{R^o}$, denn nach Beispiel II.6.4 ist jeder R-Linksmodul M ein R^o-Rechtsmodul und jeder R-Homomorphismus ist ein R^o-Homomorphismus.

(xi) Die lokal kleinen Kategorien sind die Objekte der Kategorie **Cat**. Die Morphismen von **Cat** sind genau die Funktoren zwischen lokal kleinen Kategorien.[1]

Bemerkung III.5.10. Funktoren gemäß Definition III.5.8 werden gelegentlich *kovariant* genannt, während ein *kontravarianter* Funktor zwischen $\mathcal{C}$ und $\mathcal{D}$ ein Funktor der Form $\mathcal{C}^o \to \mathcal{D}$ ist. Für diesen gilt $\Phi(f) \in \mathrm{Hom}_{\mathcal{C}}(B,A)$ und $\Phi(g \circ f) = \Phi(f) \circ \Phi(g)$ für $f \in \mathrm{Hom}_{\mathcal{C}}(A,B)$ und $g \in \mathrm{Hom}_{\mathcal{C}}(B,C)$. Zum Beispiel ist der Hom-Funktor in der ersten Komponente $\mathrm{Hom}(.,B)\colon \mathcal{C} \to \mathbf{Set}$, $A \mapsto \mathrm{Hom}_{\mathcal{C}}(A,B)$ mit $\mathrm{Hom}(f,B)(g) := f \circ g$ kontravariant. Für einen Körper K erhält man speziell den (kontravarianten) Funktor ${}_K\mathbf{mod} \to {}_K\mathbf{mod}$, der V auf seinen Dualraum $V^* := \mathrm{Hom}(V,K)$ und $f\colon V \to W$ auf die duale Abbildung $f^*\colon W^* \to V^*$ abbildet.

Definition III.5.11.

(i) Eine *Kongruenz* einer Kategorie $\mathcal{C}$ ist eine Klasse von Äquivalenzrelationen $\sim_{A,B}$ auf $\mathrm{Hom}_{\mathcal{C}}(A,B)$ für $A,B \in \mathrm{Ob}(\mathcal{C})$ mit folgenden Eigenschaften:

- Für $f,g \in \mathrm{Hom}_{\mathcal{C}}(A,B)$ und $h \in \mathrm{Hom}_{\mathcal{C}}(B,C)$ gilt $f \sim_{A,B} g \Longrightarrow h \circ f \sim_{A,C} h \circ g$.
- Für $f,g \in \mathrm{Hom}_{\mathcal{C}}(A,B)$ und $h \in \mathrm{Hom}_{\mathcal{C}}(C,A)$ gilt $f \sim_{A,B} g \Longrightarrow f \circ h \sim_{C,B} g \circ h$.

(ii) Sei $\sim$ eine Kongruenz einer Kategorie $\mathcal{C}$. Für $f \in \mathrm{Hom}_{\mathcal{C}}(A,B)$ sei $[f]$ die Äquivalenzklasse bzgl. $\sim_{A,B}$. Die *Quotientenkategorie* $\mathcal{C}/\!\sim$ von $\mathcal{C}$ besteht aus den gleichen Objekten wie $\mathcal{C}$ und

$$\mathrm{Hom}_{\mathcal{C}/\sim}(A,B) := \{[f] : f \in \mathrm{Hom}_{\mathcal{C}}(A,B)\}$$

für $A,B \in \mathrm{Ob}(\mathcal{C})$. Dabei gilt $[f] \circ [g] := [f \circ g]$ (man prüfe die Wohldefiniertheit).

[1] Man muss sich auf lokal kleine Kategorien beschränken, um subtile Probleme der Typen-Theorie zu vermeiden.

Satz III.5.12 (Homomorphiesatz)**.** *Sei $\Phi\colon \mathcal{C} \to \mathcal{D}$ ein Funktor. Für $f, g \in \mathrm{Hom}_{\mathcal{C}}(A, B)$ definiert*

$$f \sim_{A,B} g \ :\Longleftrightarrow\ \Phi(f) = \Phi(g)$$

eine Kongruenz auf $\mathcal{C}$. Sei $\mathcal{C}/\mathrm{Ker}(\Phi) := \mathcal{C}/\sim$ die entsprechende Quotientenkategorie. Dann existiert ein Isomorphismus $\overline{\Phi}\colon \mathcal{C}/\mathrm{Ker}(\Phi) \to \Phi(\mathcal{C})$.

Beweis. Offenbar ist $\sim_{A,B}$ eine Äquivalenzrelation. Für $h \in \mathrm{Hom}_{\mathcal{C}}(B, C)$ gilt

$$f \sim_{A,B} g \implies \Phi(h \circ f) = \Phi(h)\Phi(f) = \Phi(h)\Phi(g) = \Phi(h \circ g) \implies h \circ f \sim_{A,C} h \circ g$$

und analog für $f \circ h = g \circ h$. Also ist $\sim$ eine Kongruenz. Nach Definition ist der Funktor $\overline{\Phi}\colon \mathcal{C}/\mathrm{Ker}(\Phi) \to \Phi(\mathcal{C})$, $A \mapsto A$, $[f] \mapsto \Phi(f)$ wohldefiniert. Außerdem ist $\Psi\colon \Phi(\mathcal{C}) \to \mathcal{C}/\mathrm{Ker}(\Phi)$, $A \mapsto A$, $\Phi(f) \mapsto [f]$ ein Funktor mit $\overline{\Phi}\Psi = \mathrm{id}$ und $\Psi\overline{\Phi} = \mathrm{id}$. □

Definition III.5.13. Seien $\Phi, \Psi\colon \mathcal{C} \to \mathcal{D}$ Funktoren zwischen Kategorien $\mathcal{C}$, $\mathcal{D}$. Eine *natürliche Transformation* α zwischen Φ und Ψ ist eine Klasse von Morphismen $\alpha_A \in \mathrm{Hom}_{\mathcal{D}}(\Phi(A), \Psi(A))$ für $A \in \mathrm{Ob}(\mathcal{C})$ mit $\alpha_B \circ \Phi(f) = \Psi(f) \circ \alpha_A$ für $f \in \mathrm{Hom}_{\mathcal{C}}(A, B)$, d. h. das folgende Diagramm ist kommutativ:

$$\begin{array}{ccc} \Phi(A) & \xrightarrow{\alpha_A} & \Psi(A) \\ {\scriptstyle \Phi(f)}\downarrow & & \downarrow{\scriptstyle \Psi(f)} \\ \Phi(B) & \xrightarrow[\alpha_B]{} & \Psi(B) \end{array}$$

Wir schreiben ggf. $\alpha\colon \Phi \Rightarrow \Psi$.

Bemerkung III.5.14. Wie immer gibt es die *identische* Transformation $\mathrm{id}_\Phi\colon \Phi \Rightarrow \Phi$ mit $(\mathrm{id}_\Phi)_A = \mathrm{id}_{\Phi(A)}$ für alle $A \in \mathrm{Ob}(\mathcal{C})$. Sind $\alpha\colon \Phi \Rightarrow \Psi$ und $\beta\colon \Psi \Rightarrow \Gamma$ natürliche Transformationen von Funktoren $\Phi, \Psi, \Gamma\colon \mathcal{C} \to \mathcal{D}$, so auch $\gamma := \beta \circ \alpha\colon \Phi \Rightarrow \Gamma$ mit $\gamma_A := \beta_A \circ \alpha_A$, denn

$$\gamma_B \circ \Phi(f) = \beta_B \circ (\alpha_B \circ \Phi(f)) = (\beta_B \circ \Psi(f)) \circ \alpha_A = \Gamma(f) \circ \beta_A \circ \alpha_A = \Gamma(f) \circ \gamma_A$$

für $f \in \mathrm{Hom}_{\mathcal{C}}(A, B)$. Auf diese Weise wird die Klasse der Funktoren zwischen $\mathcal{C}$ und $\mathcal{D}$ zu einer Kategorie $\mathcal{D}^{\mathcal{C}}$, deren Morphismen die natürlichen Transformationen sind. Man nennt $\mathcal{D}^{\mathcal{C}}$ die *Funktorenkategorie* zwischen $\mathcal{C}$ und $\mathcal{D}$. Einen Isomorphismus $\alpha\colon \Phi \Rightarrow \Psi$ nennt man *natürlichen Isomorphismus*. Dies bedeutet, dass α_A für alle $A \in \mathrm{Ob}(\mathcal{C})$ Isomorphismen sind. Ggf. nennt man Φ und Ψ *isomorph* und schreibt $\Phi \cong_{\mathcal{D}^{\mathcal{C}}} \Psi$.

Beispiel III.5.15.

(i) Sei K ein Körper und $\mathcal{C} := {}_K\mathbf{mod}$ die Kategorie der endlich-dimensionalen K-Vektorräume. Sei $\Phi := \mathrm{id}_{\mathcal{C}}$ der Identitätsfunktor und $\Psi\colon \mathcal{C} \to \mathcal{C}$, $V \mapsto V^{**} := \mathrm{Hom}(\mathrm{Hom}(V, K), K)$ (Bidualraum von V) mit $\Psi(f) := f^{**}$ (biduale Abbildung). Für $F \in V^{**}$ und $\lambda \in W^*$ gilt

$$f^{**}(F)(\lambda) = (F \circ f^*)(\lambda) = F(\lambda \circ f).$$

Für $V \in \mathrm{Ob}(\mathcal{C})$ sei $\alpha_V \in \mathrm{Hom}_K(V, V^{**})$ mit $(\alpha_V(v))(\lambda) := \lambda(v)$ für $v \in V$ und $\lambda \in V^*$. Für $f \in \mathrm{Hom}_K(V, W)$, $v \in V$ und $\lambda \in W^*$ gilt

$$(\alpha_W \circ f)(v)(\lambda) = \lambda(f(v)) = \alpha_V(v)(\lambda \circ f) = (f^{**} \circ \alpha_V)(v)(\lambda) = (\Psi(f) \circ \alpha_V)(v)(\lambda).$$

Also ist $\alpha\colon \mathrm{id}_{\mathcal{C}} \Rightarrow \Psi$ eine natürliche Transformation. Da α_V ein Isomorphismus ist, ist α sogar ein natürlicher Isomorphismus.

(ii) Sei **CRng** die Kategorie der kommutativen Ringen und $\mathrm{GL}(n, .)\colon \mathbf{CRng} \to \mathbf{Grp}$ sowie $.^\times\colon \mathbf{CRng} \to \mathbf{Grp}$, $R \mapsto R^\times$ Funktoren. Für $f\colon R \to S$ sei dabei $f^\times := f_{|R^\times}$ die Einschränkung auf $R^\times$. Dann ist $\det\colon \mathrm{GL}(n, .) \Rightarrow .^\times$ eine natürliche Transformation mit $\det_R\colon \mathrm{GL}(n, R) \to R^\times$, $A \mapsto \det(A)$, denn

$$(\det_S \circ \mathrm{GL}(n, f))(A) = \det(f(A)) = f_{|R^\times}(\det(A)) = (f^\times \circ \det_R)(A)$$

für $A \in \mathrm{GL}(n, R)$ jeden Ringhomomorphismus $f\colon R \to S$.

Lemma III.5.16 (Yoneda)**.** *Sei $\mathcal{C}$ eine lokal kleine Kategorie, $A \in \mathrm{Ob}(\mathcal{C})$ und $\Phi\colon \mathcal{C} \to \mathbf{Set}$ ein Funktor. Dann ist die Abbildung*

$$\mathrm{Hom}_{\mathbf{Set}^{\mathcal{C}}}\big(\mathrm{Hom}(A, .), \Phi\big) \to \Phi(A), \qquad \alpha \mapsto \alpha_A(\mathrm{id}_A)$$

eine Bijektion.

Beweis. Nach Bemerkung III.5.14 ist $\Omega := \mathrm{Hom}_{\mathbf{Set}^{\mathcal{C}}}\big(\mathrm{Hom}(A, .), \Phi\big)$ die Klasse der natürlichen Transformationen $\mathrm{Hom}(A, .) \Rightarrow \Phi$. Da $\mathcal{C}$ lokal klein ist, ist Ω eine Menge. Für $\alpha \in \Omega$ ist $\alpha_A\colon \mathrm{Hom}_{\mathcal{C}}(A, A) \to \Phi(A)$ und $\alpha_A(\mathrm{id}_A) \in \Phi(A)$ wie behauptet. Für $x \in \Phi(A)$ sei $\beta^x_B\colon \mathrm{Hom}_{\mathcal{C}}(A, B) \to \Phi(B)$, $f \mapsto \Phi(f)(x)$. Für $f \in \mathrm{Hom}_{\mathcal{C}}(B, C)$ und $\varphi \in \mathrm{Hom}_{\mathcal{C}}(A, B)$ gilt

$$\big(\beta^x_C \circ \mathrm{Hom}(A, f)\big)(\varphi) = \beta^x_C(f \circ \varphi) = \Phi(f \circ \varphi)(x) = \Phi(f)\big(\Phi(\varphi)(x)\big) = (\Phi(f) \circ \beta^x_B)(\varphi).$$

Also ist $\beta^x\colon \mathrm{Hom}(A, .) \Rightarrow \Phi$ eine natürliche Transformation.

Wendet man die gegebene Abbildung auf $\alpha = \beta$ an, so ergibt sich $\beta^x_A(\mathrm{id}_A) = \Phi(\mathrm{id}_A)(x) = \mathrm{id}_{\Phi(A)}(x) = x$. Sei umgekehrt $x = \alpha_A(\mathrm{id}_A)$. Für $B \in \mathrm{Ob}(\mathcal{C})$ und $f \in \mathrm{Hom}_{\mathcal{C}}(A, B)$ gilt

$$\beta^x_B(f) = \Phi(f)(x) = (\Phi(f) \circ \alpha_A)(\mathrm{id}_A) = \big(\alpha_B \circ \mathrm{Hom}(A, f)\big)(\mathrm{id}_A) = \alpha_B(f).$$

Daher ist $\Phi(A) \to \Omega$, $x \mapsto \beta^x$ die Umkehrabbildung zu $\Omega \to \Phi(A)$, $\alpha \mapsto \alpha_A(\mathrm{id}_A)$. □

Satz III.5.17 (Yoneda-Einbettung)**.** *Für jede lokal kleine Kategorie $\mathcal{C}$ existiert ein voller und treuer Funktor $\mathcal{C} \to \mathbf{Set}^{\mathcal{C}^o}$, $A \mapsto \mathrm{Hom}(., A)$.*

Beweis. Nach Bemerkung III.5.10 ist $\mathrm{Hom}(., A)$ für $A \in \mathrm{Ob}(\mathcal{C})$ ein kontravarianter Funktor, also ein Funktor $\mathcal{C}^o \to \mathbf{Set}$. Wir beweisen die Aussage für $\mathcal{C}^o$ anstatt $\mathcal{C}$. Sei also $\Gamma\colon \mathcal{C}^o \to \mathbf{Set}^{\mathcal{C}}$, $A \mapsto \mathrm{Hom}(A, .)$. Sei $A, B \in \mathrm{Ob}(\mathcal{C})$. Yonedas Lemma mit $\Phi = \mathrm{Hom}(B, .)$ liefert eine Bijektion

$$\Delta_{A,B}\colon \mathrm{Hom}_{\mathbf{Set}^{\mathcal{C}}}\big(\mathrm{Hom}(A, .), \mathrm{Hom}(B, .)\big) \to \mathrm{Hom}_{\mathcal{C}}(B, A) = \mathrm{Hom}_{\mathcal{C}^o}(A, B).$$

Für $f \in \mathrm{Hom}_{\mathcal{C}^o}(A, B)$ sei $\Gamma(f) := \Delta^{-1}_{A,B}(f)$. Aus dem Beweis von Yonedas Lemma erhält man

$$\Gamma(f)_C\colon \mathrm{Hom}_{\mathcal{C}}(A, C) \to \mathrm{Hom}_{\mathcal{C}}(B, C), \qquad \varphi \mapsto \mathrm{Hom}(B, \varphi)(f) = \varphi \circ f$$

für $C \in \mathrm{Ob}(\mathcal{C})$. Insbesondere ist $\Gamma(\mathrm{id}_A) = \mathrm{id}_{\mathrm{Hom}(A,.)}$ für $A \in \mathrm{Ob}(\mathcal{C})$. Für $g \in \mathrm{Hom}_{\mathcal{C}^o}(B, C)$, $D \in \mathrm{Ob}(\mathcal{C})$ und $\varphi \in \mathrm{Hom}_{\mathcal{C}}(A, D)$ folgt

$$\Gamma(g \circ_{\mathcal{C}^o} f)_D(\varphi) = \varphi \circ (g \circ_{\mathcal{C}^o} f) = (\varphi \circ f) \circ g = \big(\Gamma(g)_D \circ \Gamma(f)_D\big)(\varphi).$$

Dies zeigt, dass Γ ein Funktor ist.

Sei nun eine natürliche Transformation $\alpha\colon \mathrm{Hom}(A, .) \Rightarrow \mathrm{Hom}(B, .)$ gegeben. Für $f := \Delta_{A,B}(\alpha) \in \mathrm{Hom}_{\mathcal{C}}(B, A)$ gilt dann $\Gamma(f) = \alpha$. Also ist Γ treu. Schließlich seien $f, g \in \mathrm{Hom}_{\mathcal{C}^o}(A, B)$ mit $\Gamma(f) = \Gamma(g)$. Dann folgt $f = \Delta_{A,B}(\Gamma(f)) = \Delta_{A,B}(\Gamma(g)) = g$ und Γ ist treu. □

Lemma III.5.18. *Der Funktor $\Phi\colon \mathcal{C} \to \mathcal{D}$ sei voll und treu. Dann gilt $A \cong_{\mathcal{C}} B \iff \Phi(A) \cong_{\mathcal{D}} \Phi(B)$ für $A, B \in \mathrm{Ob}(\mathcal{C})$.*

Beweis. Sei $f\colon A \to B$ ein Isomorphismus in $\mathcal{C}$. Dann ist

$$\Phi(f) \circ \Phi(f^{-1}) = \Phi(f \circ f^{-1}) = \Phi(\mathrm{id}_B) = \mathrm{id}_{\Phi(B)}$$

und analog $\Phi(f^{-1}) \circ \Phi(f) = \mathrm{id}_{\Phi(A)}$. Dies zeigt, dass $\Phi(f)\colon \Phi(A) \to \Phi(B)$ ein Isomorphismus in $\mathcal{D}$ ist. Sei nun umgekehrt $g\colon \Phi(A) \to \Phi(B)$ ein Isomorphismus in $\mathcal{D}$. Da Φ voll ist, existieren $f \in \mathrm{Hom}_{\mathcal{C}}(A, B)$ und $f' \in \mathrm{Hom}_{\mathcal{C}}(B, A)$ mit $\Phi(f) = g$ und $\Phi(f') = g^{-1}$. Es folgt $\Phi(f \circ f') = g \circ g^{-1} = \mathrm{id}_{\Phi(B)} = \Phi(\mathrm{id}_B)$. Da Φ treu ist, erhält man $f \circ f' = \mathrm{id}_B$. Analog ist $f' \circ f = \mathrm{id}_A$. Also ist f ein Isomorphismus in $\mathcal{C}$. □

Folgerung III.5.19. *Sei $\mathcal{C}$ eine lokal kleine Kategorie und $A, B \in \mathrm{Ob}(\mathcal{C})$. Dann gilt*

$$\mathrm{Hom}(A, .) \cong_{\mathbf{Set}^{\mathcal{C}}} \mathrm{Hom}(B,) \implies A \cong_{\mathcal{C}} B.$$

Beweis. Sei $\alpha\colon \mathrm{Hom}(A, .) \Rightarrow \mathrm{Hom}(B, .)$ ein natürlicher Isomorphismus von Funktoren $\mathcal{C} \to \mathbf{Set}$. Für $C \in \mathrm{Ob}(\mathcal{C})$ sind dann $\alpha_C\colon \mathrm{Hom}_{\mathcal{C}^o}(C, A) \to \mathrm{Hom}_{\mathcal{C}^o}(C, B)$ Bijektionen. Für $f \in \mathrm{Hom}_{\mathcal{C}^o}(C, D)$ und $\varphi \in \mathrm{Hom}_{\mathcal{C}^o}(C, A)$ gilt $\mathrm{Hom}(f, A)(\varphi) = \varphi \circ_{\mathcal{C}^o} f = f \circ \varphi = \mathrm{Hom}(A, f)(\varphi)$. Also ist $\alpha\colon \mathrm{Hom}(., A) \Rightarrow \mathrm{Hom}(., B)$ ein natürlicher Isomorphismus von Funktoren $\mathcal{C}^o \to \mathbf{Set}$. Nach Lemma III.5.18 sind die Urbilder der Yoneda-Einbettung ebenfalls isomorph, d. h. $A \cong_{\mathcal{C}} B$. □

Beispiel III.5.20. Seien G und H Gruppen. Für alle Gruppen X existiere eine Bijektion $\alpha_X\colon \mathrm{Hom}(G, X) \to \mathrm{Hom}(H, X)$ mit

$$\alpha_Y(f \circ \varphi) = f \circ \alpha_X(\varphi)$$

für alle Gruppenhomomorphismen $f\colon X \to Y$ und $\varphi\colon G \to X$. Dann ist $\alpha\colon \mathrm{Hom}(G, .) \Rightarrow \mathrm{Hom}(H, .)$ ein natürlicher Isomorphismus und Folgerung III.5.19 zeigt $G \cong H$.

Definition III.5.21. Ein Funktor $\Phi\colon \mathcal{C} \to \mathcal{D}$ heißt *Äquivalenz*, falls ein Funktor $\Psi\colon \mathcal{D} \to \mathcal{C}$ mit $\Phi \circ \Psi \cong \mathrm{id}_{\mathcal{D}}$ und $\Psi \circ \Phi \cong \mathrm{id}_{\mathcal{C}}$ existiert. Ggf. nennen wir $\mathcal{C}$ und $\mathcal{D}$ äquivalent und schreiben $\mathcal{C} \approx \mathcal{D}$.

Bemerkung III.5.22.

(i) Isomorphe Kategorien sind äquivalent, aber nicht umgekehrt (siehe Beispiel III.5.24). Wir zeigen im Folgenden, dass viele algebraische Konzepte durch Äquivalenzen erhalten werden.

(ii) Nach Definition ist $\approx$ reflexiv und symmetrisch. Aus Lemma III.5.23 folgt leicht, dass $\approx$ auch transitiv ist. Es handelt sich also um eine Äquivalenzrelation.

(iii) Genau dann ist $\Phi\colon \mathcal{C} \to \mathcal{D}$ eine Äquivalenz, wenn $\Phi\colon \mathcal{C}^o \to \mathcal{D}^o$ eine Äquivalenz ist.

(iv) Sei $\alpha\colon \Psi\Phi \Rightarrow \mathcal{C}$ ein natürlicher Isomorphismus und $A \in \mathrm{Ob}(\mathcal{C})$. Dann ist $\alpha_A\colon \Psi(\Phi(A)) \to A$ ein Isomorphismus in $\mathcal{C}$. Für $f \in \mathrm{Hom}_{\mathcal{C}}(A, B)$ gilt

$$\Psi(\Phi(f)) = \alpha_B^{-1} \circ f \circ \alpha_A,$$

d. h. f und $\Psi(\Phi(f))$ unterscheiden sich nur durch Isomorphismen von links und rechts. Dies zeigt

- f Monomorphismus $\iff$ $\Phi(f)$ Monomorphismus.
- f Epimorphismus $\iff$ $\Phi(f)$ Epimorphismus.
- f Isomorphismus $\iff$ $\Phi(f)$ Isomorphismus.

Lemma III.5.23. *Ein Funktor $\Phi\colon \mathcal{C} \to \mathcal{D}$ ist genau dann eine Äquivalenz, wenn Φ voll und treu ist und für alle $D \in \mathrm{Ob}(\mathcal{D})$ ein $C \in \mathrm{Ob}(\mathcal{C})$ mit $\Phi(C) \cong D$ existiert.*

Beweis. Sei Φ eine Äquivalenz und $\Psi\colon \mathcal{D} \to \mathcal{C}$ mit natürlichen Isomorphismen $\alpha\colon \Psi\Phi \Rightarrow \mathrm{id}_{\mathcal{C}}$ und $\beta\colon \Phi\Psi \Rightarrow \mathrm{id}_{\mathcal{D}}$. Seien $f, g \in \mathrm{Hom}_{\mathcal{C}}(A, B)$ mit $\Phi(f) = \Phi(g)$. Dann gilt

$$f = \alpha_B \circ \Psi\Phi(f) \circ \alpha_A^{-1} = \alpha_B \circ \Psi\Phi(g) \circ \alpha_A^{-1} = g$$

und Φ ist treu. Analog ist auch Ψ treu. Sei nun $g \in \mathrm{Hom}_{\mathcal{D}}(\Phi(A), \Phi(B))$ gegeben. Für $f := \alpha_B \Psi(g) \alpha_A^{-1} \in \mathrm{Hom}_{\mathcal{C}}(A, B)$ gilt dann

$$\Psi(g) = \alpha_B^{-1} \circ f \circ \alpha_A = \Psi\Phi(f).$$

Da Ψ treu ist, folgt $g = \Phi(f)$ und Φ ist voll. Schließlich sei $D \in \mathrm{Ob}(\mathcal{D})$ gegeben. Setze $C := \Psi(D) \in \mathrm{Ob}(\mathcal{C})$. Dann ist $\beta_D\colon \Phi(C) \to D$ ein Isomorphismus.

Sei umgekehrt Φ voll und treu und für alle $D \in \mathrm{Ob}(\mathcal{D})$ existiere ein $C_D \in \mathrm{Ob}(\mathcal{C})$ mit $\Phi(C_D) \cong D$. Wir setzen $\Psi(D) := C_D$ und wählen Isomorphismen $\beta_D\colon \Phi(\Psi(D)) \to D$. Für $g \in \mathrm{Hom}_{\mathcal{D}}(D, E)$ sei

$$\Psi(g) := \Phi^{-1}(\beta_E^{-1} \circ g \circ \beta_D) \in \mathrm{Hom}_{\mathcal{C}}(\Psi(D), \Psi(E)).$$

Dann gilt $\Psi(\mathrm{id}_D) = \mathrm{id}_{\Psi(D)}$. Für $h \in \mathrm{Hom}_{\mathcal{D}}(E, F)$ ist

$$\begin{aligned}\Psi(h \circ g) &= \Phi^{-1}(\beta_E^{-1} h \beta_E \circ \beta_E^{-1} g \beta_D) = \Phi^{-1}(\Phi(\Phi^{-1}(\beta_E^{-1} h \beta_E)) \circ \Phi(\Phi^{-1}(\beta_E^{-1} g \beta_D))) \\ &= \Phi^{-1}(\beta_E^{-1} h \beta_E) \circ \Phi^{-1}(\beta_E^{-1} g \beta_D) = \Psi(h) \circ \Psi(g).\end{aligned}$$

Somit ist $\Psi\colon \mathcal{D} \to \mathcal{C}$ ein Funktor. Außerdem ist $\beta_E \circ \Phi\Psi(g) = g \circ \beta_D$ und $\beta\colon \Phi\Psi \to \mathrm{id}_{\mathcal{D}}$ ist ein natürlicher Isomorphismus. Nach Konstruktion ist Ψ treu. Für $f \in \mathrm{Hom}_{\mathcal{C}}(\Psi(D), \Psi(E))$ sei $g := \beta_E \Phi(f) \beta_D^{-1} \in \mathrm{Hom}_{\mathcal{D}}(D, E)$. Dann gilt $\Psi(g) = f$ und Ψ ist voll. Sei $A \in \mathrm{Ob}(\mathcal{C})$ gegeben. Nach Definition von Ψ existiert ein $C \in \mathcal{C}$ mit $\Phi(C) = \Phi(A)$ und $\Psi(\Phi(A)) = C$. Nun ist $\Phi^{-1}(\mathrm{id}_{\Phi(A)})\colon A \to C$ ein Isomorphismus. Somit erfüllt Ψ die gleichen Voraussetzungen wie Ψ. Nach dem bereits Gezeigtem existiert ein natürlicher Isomorphismus $\alpha\colon \Psi\Phi \Rightarrow \mathrm{id}_{\mathcal{C}}$. □

Beispiel III.5.24.

(i) Sei K ein Körper und $\Phi\colon K\text{-}\mathbf{mat}^o \to {}_K\mathbf{mod}$, $n \mapsto K^n$ mit $\Phi(A)(v) := Av \in K^m$ für $A \in K^{m \times n}$ und $v \in K^n$. Offenbar ist Φ ein voller und treuer Funktor. Da jeder endlich-dimensionale K-Vektorraum zu einem K^n isomorph ist, ist Φ eine Äquivalenz nach Lemma III.5.23. Da es überabzählbar viele (endlich-dimensionale) Vektorräume, können $K\text{-}\mathbf{mat}^o$ und ${}_K\mathbf{mod}$ nicht isomorph sein.

(ii) Angenommen es existiert eine Äquivalenz $\Phi\colon \mathbf{Set} \to \mathbf{Set}^o$. Seien A und B Mengen mit $|A| = 1$ und $|B| = 2$. Dann gilt

$$2 = |\operatorname{Hom}_{\mathbf{Set}}(A, B)| = |\operatorname{Hom}_{\mathbf{Set}^o}(\Phi(A), \Phi(B))| = |\operatorname{Hom}_{\mathbf{Set}}(\Phi(B), \Phi(A)|.$$

Daraus folgt $|\Phi(B)| = 1$ und $|\Phi(A)| = 2$ und man hat den Widerspruch $|\operatorname{Hom}_{\mathbf{Set}}(A, A)| \neq |\operatorname{Hom}_{\mathbf{Set}}(\Phi(A), \Phi(A))|$. Also gilt $\mathbf{Set} \not\approx \mathbf{Set}^o$.

Definition III.5.25. Sei $\mathcal{C}$ eine kleine Kategorie. Man erhält eine *Skelett-Kategorie* $\bar{\mathcal{C}}$ von $\mathcal{C}$, indem man für $\operatorname{Ob}(\mathcal{C})$ ein Repräsentantensystem für die Isomorphieklassen von Objekten in $\mathcal{C}$ wählt und $\operatorname{Hom}_{\bar{\mathcal{C}}}(A, B) := \operatorname{Hom}_{\mathcal{C}}(A, B)$ setzt.[2]

Satz III.5.26. *Für kleine Kategorien $\mathcal{C}$ und $\mathcal{D}$ gilt $\mathcal{C} \approx \bar{\mathcal{C}}$ und $\mathcal{C} \approx \mathcal{D} \iff \bar{\mathcal{C}} \cong \overline{\mathcal{D}}$.*

Beweis. Lemma III.5.23 zeigt, dass die Einbettung $\Phi\colon \bar{\mathcal{C}} \to \mathcal{C}$, $A \mapsto A$, $f \mapsto f$ eine Äquivalenz ist. Sei nun $\Phi\colon \mathcal{C} \to \mathcal{D}$ eine Äquivalenz und $\overline{\mathcal{D}} := \Phi(\bar{\mathcal{C}})$ eine Unterkategorie von $\mathcal{D}$. Nach Lemma III.5.23 existiert für jedes $D \in \operatorname{Ob}(\mathcal{D})$ ein $C \in \operatorname{Ob}(\mathcal{C})$ mit $\Phi(C) = D$. Sei $\alpha_C\colon C \to \overline{C} \in \bar{\mathcal{C}}$ ein Isomorphismus. Dann ist auch $\Phi(\alpha_C)\colon D \to \Phi(\overline{C})$ ein Isomorphismus. Sei auch $\overline{B} \in \operatorname{Ob}(\bar{\mathcal{C}})$ mit $\Phi(\overline{B}) \cong D$. Dann folgt $\overline{B} = \overline{C}$ und $B = C$ aus Lemma III.5.18. Dies zeigt, dass $\overline{\mathcal{D}}$ eine Skelett-Kategorie von $\mathcal{D}$ ist. Außerdem ist der eingeschränkte Funktor $\overline{\Phi}\colon \bar{\mathcal{C}} \to \overline{\mathcal{D}}$ ein Isomorphismus nach Aufgabe III.23.

Nehmen wir nun an, dass ein Isomorphismus $\overline{\Phi}\colon \bar{\mathcal{C}} \to \overline{\mathcal{D}}$ zwischen Skelett-Kategorien gegeben ist. Für $C \in \operatorname{Ob}(\mathcal{C})$ und $D \in \operatorname{Ob}(\mathcal{D})$ wählen wir Isomorphismen $\alpha_C\colon C \to \overline{C} \in \operatorname{Ob}(\bar{\mathcal{C}})$ und $\beta_D\colon D \to \overline{D} \in \operatorname{Ob}(\overline{\mathcal{D}})$. Sei $\Phi\colon \mathcal{C} \to \mathcal{D}$, $C \mapsto \overline{\Phi}(\overline{C})$ mit $\Phi(f) := \overline{\Phi}(\alpha_B f \alpha_A^{-1})$ für $f \in \operatorname{Hom}_{\mathcal{C}}(A, B)$. Offenbar ist Φ ein Funktor. Mit $\overline{\Phi}$ ist auch Φ voll und treu. Für jedes $D \in \operatorname{Ob}(\mathcal{D})$ existiert zudem ein $\overline{C} \in \operatorname{Ob}(\bar{\mathcal{C}})$ mit $\Phi(\overline{C}) = \overline{D} \cong D$. Nach Lemma III.5.23 ist Φ eine Äquivalenz. □

Bemerkung III.5.27. Nach Satz III.5.26 ist eine Skelett-Kategorie einer kleinen Kategorie $\mathcal{C}$ bis auf Äquivalenz eindeutig bestimmt. Sie ist außerdem die „kleinste“ zu $\mathcal{C}$ äquivalente Kategorie.

Definition III.5.28. Seien $\Phi\colon \mathcal{C} \to \mathcal{D}$ und $\Psi\colon \mathcal{D} \to \mathcal{C}$ Funktoren zwischen lokal kleinen Kategorien $\mathcal{C}, \mathcal{D}$. Man nennt Φ *links-adjungiert* zu Ψ (und Ψ *rechts-adjungiert* zu Φ), falls die Funktoren

$$\operatorname{Hom}(\Phi(.), .)\colon \mathcal{C}^o \times \mathcal{D} \to \mathbf{Set},\ (A, B) \mapsto \operatorname{Hom}_{\mathcal{D}}(\Phi(A), B),\ \operatorname{Hom}(\Phi(f_A), f_B)(\varphi) = f_B \circ \varphi \circ \Phi(f_A),$$
$$\operatorname{Hom}(., \Psi(.))\colon \mathcal{C}^o \times \mathcal{D} \to \mathbf{Set},\ (A, B) \mapsto \operatorname{Hom}_{\mathcal{C}}(A, \Psi(B)),\ \operatorname{Hom}(f_A, \Psi(f_B))(\varphi) = \Psi(f_B) \circ \varphi \circ f_A$$

isomorph sind.

Beispiel III.5.29. Sei $\mathcal{C} := \mathbf{Set}$ und $\mathcal{D} := {}_K\mathbf{Mod}$ die Kategorie der K-Vektorräume für einen Körper K. Sei $\Psi\colon \mathcal{D} \to \mathcal{C}$ der Vergiss-Funktor und $\Phi\colon \mathcal{C} \to \mathcal{D}$, $B \mapsto \coprod_{b \in B} K$. Wir betrachten B als Standardbasis von $\Phi(B)$. Für $f\colon B \to C$ sei $\Phi(f)\colon \coprod_{b \in B} K \to \coprod_{c \in C} K$, $(x_b)_{b \in B} \mapsto \sum_{b \in B} x_{f(b)}$. Offenbar ist Φ ein Funktor. Für $B \in \operatorname{Ob}(\mathcal{D})$ und $V \in \operatorname{Ob}(\mathcal{C})$ sei

$$\alpha_{(B,V)}\colon \operatorname{Hom}_{\mathcal{D}}(\Phi(B), V) \to \operatorname{Hom}_{\mathcal{C}}(B, V), \qquad f \mapsto f_{|B}$$

die Einschränkung. Da jeder Homomorphismus $\Phi(B) \to V$ durch die Bilder von B eindeutig bestimmt ist, ist $\alpha_{(B,V)}$ bijektiv. Für $f = (f_B, f_V) \in \operatorname{Hom}_{\mathcal{C}^o \times \mathcal{D}}((B, V), (C, W))$ und $\varphi \in \operatorname{Hom}_{\mathcal{D}}(\Phi(B), V)$ gilt

$$\big(\alpha_{(C,W)} \circ \operatorname{Hom}(\Phi(f_B), f_V)\big)(\varphi) = (f_V \varphi \Phi(f_B))_C = f_V \varphi_{|B} f_C = \big(\operatorname{Hom}(f_B, \Psi(f_V)) \circ \alpha_{(B,V)}\big)(\varphi).$$

[2] Die Voraussetzung „klein“ lässt verallgemeinern, sodass zum Beispiel auch $\overline{\mathbf{Grp}}$ wohldefiniert ist.

Daher ist $\alpha\colon \mathrm{Hom}(\Phi(.),.) \Rightarrow \mathrm{Hom}(.,\Psi(.))$ ein natürlicher Isomorphismus und Φ ist links-adjungiert zu Ψ.

Definition III.5.30. Sei $(A_i)_{i\in I}$ eine Familie von Objekten einer Kategorie $\mathcal{C}$.

- Man nennt $P \in \mathrm{Ob}(\mathcal{C})$ ein *Produkt* von (A_i), falls Morphismen $p_i\colon P \to A_i$ für $i \in I$ mit folgender universeller Eigenschaft existieren: Für jede Familie von Morphismen $f_i\colon C \to A_i$ existiert genau ein Morphismus $f\colon C \to P$ mit $p_i \circ f = f_i$ für $i \in I$. Ggf. nennt man p_i die i-te *Projektionen* von P.
- Man nennt $Q \in \mathrm{Ob}(\mathcal{C})$ ein *Koprodukt* von (A_i), falls Morphismen $q_i\colon A_i \to Q$ für $i \in I$ mit folgender universeller Eigenschaft existieren: Für jede Familie von Morphismen $f_i\colon A_i \to C$ existiert genau ein Morphismus $f\colon Q \to C$ mit $f \circ q_i = f_i$ für $i \in I$. Ggf. nennt man q_i die i-te *Injektionen* von Q.

Bemerkung III.5.31.

(i) Nicht in jeder Kategorie müssen (Ko)produkte existieren.

(ii) Ein Produkt (bzw. Koprodukt) von (A_i) in $\mathcal{C}$ entspricht einem Koprodukt (bzw. Produkt) von (A_i) in $\mathcal{C}$ (alle Pfeile sind umgekehrt).

Lemma III.5.32. *Sei $(A_i)_{i\in I}$ eine Familie von Objekten einer Kategorie $\mathcal{C}$.*

(i) Sind $P, P' \in \mathrm{Ob}(\mathcal{C})$ Produkte von (A_i) bzgl. p_i bzw. p_i', so existiert genau ein Isomorphismus $f\colon P' \to P$ mit $p_i f = p_i'$ für $i \in I$.

(ii) Sind $Q, Q' \in \mathrm{Ob}(\mathcal{C})$ Koprodukte von (A_i) bzgl. q_i bzw. q_i', so existiert genau ein Isomorphismus $f\colon Q' \to Q$ mit $f q_i' = q_i$ für $i \in I$.

Beweis.

(i) Die universelle Eigenschaft von P angewendet auf $f_i = p_i'$ liefert genau ein $f\colon P' \to P$ mit $p_i f = p_i'$ für $i \in I$. Analog existiert ein $g\colon P' \to P$ mit $p_i' g = p_i$ für $i \in I$. Für $fg\colon P \to P$ gilt nun $p_i fg = p_i$. Nach der universellen Eigenschaft von P ist id_P der einzige Morphismus mit dieser Eigenschaft. Dies zeigt $fg = \mathrm{id}_P$ und analog $gf = \mathrm{id}_{P'}$. Also ist f ein Isomorphismus und durch die Gleichung $p_i f = p_i'$ eindeutig bestimmt.

(ii) Wendet man (i) auf die Produkte Q und Q' von (A_i) in $\mathcal{C}^o$ an, so erhält man genau einen Isomorphismus $f\colon Q' \to Q$ in $\mathcal{C}^o$ mit $q_i f = q_i'$ für $i \in I$. Nun ist $f\colon Q \to Q'$ ein Isomorphismus in $\mathcal{C}$ mit $f q_i = q_i'$ für $i \in I$. Der angegebene Isomorphismus ist f^{-1}. □

Beispiel III.5.33.

(i) Das Produkt von (A_i) in **Set**, **Grp** oder **Ab** ist das gewohnte kartesische (direkte) Produkt $\times_{i\in I} A_i$. Das Koprodukt in **Set** ist die disjunkte Vereinigung $\bigsqcup_{i\in I} A_i$, während es in **Ab** das bekannte Koprodukt $\coprod_{i\in I} A_i$ ist (im Fall $|I| < \infty$ stimmt hier Produkt und Koprodukt überein). In **Grp** ist das Koprodukt hingegen das *freie Produkt*, dessen Existenz man erst nachweisen muss.[3]

(ii) Sei P das Produkt von $A_i := A$ für $i \in I$ bzgl. p_i. Dann existiert genau ein $d\colon A \to P$ mit $p_i d = \mathrm{id}_A$ für $i \in I$. Man nennt d den *diagonalen Morphismus* bzgl. P. Für das Koprodukt Q von A_i existiert analog der *codiagonale Morphismus* $c\colon Q \to A$ mit $c q_i = \mathrm{id}_A$ für alle $i \in I$.

[3] Siehe Kombinatorische Gruppentheorie

6 Morita-Theorie

Bemerkung III.6.1. Gruppen und Ringe lassen sich bekanntlich durch ihre Darstellungen und Moduln untersuchen. Morita-Theorie ist das Studium der Modulkategorie eines beliebigen Rings R. Im Gegensatz zu allgemeinen Kategorien hat ${}_R\mathbf{Mod}$ die Zusatzeigenschaft, dass man Morphismen addieren kann (mit $f, g\colon M \to N$ ist bekanntlich auch $f+g\colon M \to N, m \mapsto f(m)+g(m)$ ein Homomorphismus).[1] Außerdem ist $M \times N$ sowohl das Produkt als auch das Koprodukt von R-Moduln bzgl. der kanonischen Projektionen und Injektionen. Wir zeigen, dass äquivalente Modulkategorien einige nützliche Eigenschaften erhalten. Mit dem Satz von Morita geben wir ein handliches Kriterium, um zu erkennen wann die Modulkategorien zweier Ringe äquivalent sind.

Lemma III.6.2. *Seien R, S Ringe und $\Phi\colon {}_R\mathbf{Mod} \to {}_S\mathbf{Mod}$ eine Äquivalenz. Für jede Familie von R-Moduln $(M_i)_{i\in I}$ gilt*

$$\Phi\Big(\bigtimes_{i\in I} M_i\Big) \simeq \bigtimes_{i\in I} \Phi(M_i), \qquad \Phi\Big(\coprod_{i\in I} M_i\Big) \simeq \coprod_{i\in I} \Phi(M_i).$$

Beweis. Sei $M := \bigtimes_{i\in I} M_i$, $N := \bigtimes_{i\in I} \Phi(M_i)$ und $p_i\colon M \to M_i$, $p_i'\colon N \to \Phi(M_i)$ die i-ten Projektionen. Sei $\Psi\colon {}_S\mathbf{Mod} \to {}_R\mathbf{Mod}$, und $\alpha\colon \Psi\Phi \Rightarrow \mathrm{id}_{{}_R\mathbf{Mod}}$ ein natürlicher Isomorphismus. Wegen $\Phi(p_i) \in \mathrm{Hom}_S(\Phi(M), \Phi(M_i))$, $\Psi(p_i') \in \mathrm{Hom}_R(\Psi(N), \Psi(\Phi(M_i))$ und $\alpha_{M_i} \in \mathrm{Hom}_R(\Psi(\Phi(M_i)), M_i)$ sind

$$\begin{aligned} f\colon \Phi(M) \to N, &\qquad x \mapsto \big(\Phi(p_i)(x)\big)_{i\in I}, \\ g\colon \Psi(N) \to M, &\qquad y \mapsto \big((\alpha_{M_i} \circ \Psi(p_i'))(y)\big)_{i\in I} \end{aligned}$$

S- bzw. R-linear. Da Ψ treu ist, können wir $h := \Psi^{-1}(\alpha_M^{-1} \circ g) \in \mathrm{Hom}_S(N, \Phi(M))$ definieren. Dann gilt

$$\begin{aligned} \Psi(p_i' \circ f \circ h) &= \Psi(\Phi(p_i) \circ h) = \Psi(\Phi(p_i)) \circ \Psi(h) = \Psi(\Phi(p_i)) \circ \alpha_M^{-1} \circ g \\ &= \alpha_{M_i}^{-1} \circ p_i \circ g = \alpha_{M_i}^{-1} \circ \alpha_{M_i} \circ \Psi(p_i') = \Psi(p_i'). \end{aligned}$$

Dies impliziert $p_i' f h = p_i'$. Da dies für alle $i \in I$ gilt, erhält man $fh = \mathrm{id}_N$.

Analog gilt

$$p_i \circ g \circ \Psi(f) = \alpha_{M_i} \circ \Psi(p_i') \circ \Psi(f) = \alpha_{M_i} \circ \Psi(p_i' \circ f) = \alpha_{M_i} \circ \Psi(\Phi(p_i)) = p_i \circ \alpha_M$$

für alle $i \in I$. Es folgt $g \circ \Psi(f) = \alpha_M$ und

$$\Psi(h \circ f) = \Psi(h) \circ \Psi(f) = \alpha_M^{-1} \circ g \circ \Psi(f) = \mathrm{id}_{\Psi\Phi(M)} = \Psi(\mathrm{id}_{\Phi(M)}).$$

Dies zeigt $hf = \mathrm{id}_{\Phi(M)}$ und $f\colon \Phi(M) \to N$ ist ein S-Isomorphismus. Der gleiche Beweis zeigt die entsprechende Isomorphie für das Koprodukt. □

Lemma III.6.3. *Seien R, S Ringe und $\Phi\colon {}_R\mathbf{Mod} \to {}_S\mathbf{Mod}$ eine Äquivalenz. Für R-Moduln A, B gilt:*

(i) Für den trivialen Modul $A = 0$ ist auch $\Phi(A) = 0$.

[1] Man spricht von *abelschen* Kategorien.

(ii) Für die triviale Abbildung $f\colon A \to B$, $a \mapsto 0$ ist auch $\Phi(f)$ trivial.

(iii) $\Phi\colon \operatorname{Hom}_R(A,B) \to \operatorname{Hom}_S(\Phi(A),\Phi(B))$ ist ein Gruppenisomorphismus.

Beweis.

(i) Jeder Modul $B \neq 0$ besitzt neben id_B die triviale Abbildung $B \to B$. Daher ist der triviale Modul A das einzige Objekt in ${}_R\mathbf{Mod}$ mit $|\operatorname{Hom}(A,A)| = 1$. Da Φ voll und treu ist, folgt $|\operatorname{Hom}(\Phi(A),\Phi(A))| = 1$ und $\Phi(A) = 0$.

(ii) Die triviale Abbildung f ist der einzige Morphismus mit $g \circ f = f$ für alle Morphismen $g\colon B \to B$. Da Φ voll ist, muss auch $\Phi(f)$ trivial sein.

(iii) Nach Lemma III.5.23 ist $\Phi\colon \operatorname{Hom}_R(A,B) \to \operatorname{Hom}_S(\Phi(A),\Phi(B))$ bijektiv. Es verbleibt also

$$\Phi(f+g) = \Phi(f) + \Phi(g)$$

für $f, g \in \operatorname{Hom}_R(A,B)$ zu zeigen. Sei $A_1 := A =: A_2$. Seien $p_i\colon A_1 \times A_2 \to A_i$, $p_i'\colon \Phi(A_1)\times\Phi(A_2) \to \Phi(A_i)$ und $q_i\colon A_i \to A_1 \times A_2$, $q_i'\colon \Phi(A_i) \to \Phi(A_1) \times \Phi(A_2)$ die Projektionen und Injektionen. Der Beweis von Lemma III.6.2 liefert den Isomorphismus

$$\gamma\colon \Phi(A_1 \times A_2) \to \Phi(A_1) \times \Phi(A_2), \qquad x \mapsto \big(\Phi(p_1)(x), \Phi(p_2)(x)\big).$$

Es gilt also $p_i'\gamma = \Phi(p_i)$ für $i = 1, 2$. Nach (ii) ist $\Phi(p_i q_j) = 0$ für $i \neq j$. Daraus folgt

$$\gamma\Phi(q_i) = (q_1'p_1' + q_2'p_2')\gamma\Phi(q_i) = q_1'\Phi(p_1)\Phi(q_i) + q_2'\Phi(p_2)\Phi(q_i) = q_i'\Phi(p_iq_i) = q_i'\Phi(\mathrm{id}_{A_i}) = q_i'$$

für $i = 1, 2$. Sei $d\colon A \to A_1 \times A_2$, $a \mapsto (a, a)$ der diagonale Morphismus (Beispiel III.5.33) und $c\colon A_1 \times A_2 \to B$, $(x, y) \mapsto f(x) + g(y)$. Dann gilt $f + g = c \circ d$. Für

$$d' := \gamma\Phi(d)\colon \Phi(A) \to \Phi(A_1) \times \Phi(A_2)$$

gilt $p_i'd' = \Phi(p_i d) = \Phi(\mathrm{id}_{A_i}) = \mathrm{id}_{\Phi(A_i)}$ und es folgt $d'(x) = (x, x)$ für $x \in \Phi(A)$. Für

$$c' := \Phi(c)\gamma^{-1}\colon \Phi(A_1) \times \Phi(A_2) \to \Phi(B)$$

hat man $c'q_i' = \Phi(c)\Phi(q_i) = \Phi(f_i)$ mit $f_1 = f$ und $f_2 = g$. Dies zeigt $c'(x, y) = \Phi(f)(x) + \Phi(g)(y)$ und

$$\Phi(f+g) = \Phi(c \circ d) = \Phi(c) \circ \Phi(d) = c'd' = \Phi(f) + \Phi(g). \qquad \square$$

Bemerkung III.6.4. Nicht jeder Funktor $\Phi\colon {}_R\mathbf{Mod} \to {}_S\mathbf{Mod}$ erfüllt $\Phi(f+g) = \Phi(f)+\Phi(g)$. Sei zum Beispiel $\Phi(A) := S$ und $\Phi(f) := \mathrm{id}_S$ für alle R-Moduln A und R-Homomorphismen f. Offensichtlich ist Φ ein Funktor und $\Phi(f + f) = \mathrm{id}_S \neq 2\,\mathrm{id}_S = \Phi(f) + \Phi(f)$.

Satz III.6.5. *Seien R, S Ringe und $\Phi\colon {}_R\mathbf{Mod} \to {}_S\mathbf{Mod}$ eine Äquivalenz. Dann existiert für jeden R-Modul M eine Bijektion $\hat{\Phi}\colon \{N : N \leq M\} \to \{N : N \leq \Phi(M)\}$ mit*

$$N \leq N' \iff \hat{\Phi}(N) \leq \hat{\Phi}(N'), \qquad \hat{\Phi}(N + N') = \hat{\Phi}(N) + \hat{\Phi}(N'), \qquad \hat{\Phi}(N \cap N') = \hat{\Phi}(N) \cap \hat{\Phi}(N').$$

Beweis. Da aus $N \leq M$ nicht unbedingt $\Phi(N) \leq \Phi(M)$ folgt, müssen wir einen Umweg gehen. Sei $\Psi\colon {}_S\mathbf{Mod} \to {}_R\mathbf{Mod}$, und $\alpha\colon \Psi\Phi \Rightarrow \mathrm{id}_{{}_R\mathbf{Mod}}$ eine natürliche Äquivalenz. Für Untermoduln $N \leq M$ sei $\nu_N^M\colon N \hookrightarrow M$ die Inklusionsabbildung. Dann ist $\Phi(\nu_N^M) \in \mathrm{Hom}_S(\Phi(N), \Phi(M))$. Wir definieren

$$\begin{aligned}
&\hat{\Phi}\colon \{N : N \leq M\} \to \{N : N \leq \Phi(M)\}, \qquad N \mapsto \Phi(\nu_N^M)(\Phi(N)),\\
&\hat{\Psi}\colon \{N : N \leq \Phi(M)\} \to \{N : N \leq \Psi\Phi(M)\}, \qquad N \mapsto \Psi(\nu_N^{\Phi(M)})(\Psi(N)),\\
&\hat{\alpha}\colon \{N : N \leq \Psi\Phi(M)\} \to \{N : N \leq M\}, \qquad N \mapsto \alpha_M(N).
\end{aligned}$$

Mit ν_N^M ist $\Phi(\nu_N^M)$ injektiv (Satz III.5.7+Bemerkung III.5.22). Also existiert ein S-Isomorphismus $f\colon \Phi(N) \to \hat{\Phi}(N)$ mit $\Phi(\nu_N^M) = \nu_{\hat{\Phi}(N)}^{\Phi(M)} \circ f$. Dies zeigt

$$\begin{aligned}
\hat{\alpha}\big(\hat{\Psi}(\hat{\Phi}(N))\big) &= \big(\alpha_M \circ \Psi(\nu_{\hat{\Phi}(N)}^{\Phi(M)})\big)(\Psi(\hat{\Phi}(N))) = \big(\alpha_M \circ \Psi(\nu_{\hat{\Phi}(N)}^{\Phi(M)}) \circ \Psi(f)\big)(\Psi\Phi(N))\\
&= \big(\alpha_M \circ \Psi(\nu_{\hat{\Phi}(N)}^{\Phi(M)} \circ f)\big)(\Psi\Phi(N)) = \big(\alpha_M \circ \Psi(\Phi(\nu_N^M))\big)(\Psi\Phi(N))\\
&= \big(\nu_N^M \circ \alpha_N)\big)(\Psi\Phi(N)) = \nu_N^M(N) = N
\end{aligned}$$

und $\hat{\alpha}\hat{\Psi}\hat{\Phi} = \mathrm{id}$. Mit α_M ist auch $\hat{\alpha}$ bijektiv. Daher ist $\hat{\Psi}$ surjektiv und $\hat{\Phi}$ injektiv. Da auch ein natürlicher Isomorphismus $\beta\colon \Phi\Psi \Rightarrow \mathrm{id}$ existiert, erhält man analog die Injektivität von $\hat{\Psi}$ und die Surjektivität von $\hat{\Phi}$. Insgesamt ist $\hat{\Phi}$ bijektiv.

Aus $N \leq N'$ folgt $\nu_N^M = \nu_{N'}^M \circ \nu_N^{N'}$ und

$$\hat{\Phi}(N) = \Phi(\nu_N^M)(\Phi(N)) \leq \Phi(\nu_{N'}^M)(\Phi(N')) = \hat{\Phi}(N').$$

Für $\hat{\Phi}(N) \leq \hat{\Phi}(N')$ gilt analog $\hat{\Psi}\hat{\Phi}(N) \leq \hat{\Psi}\hat{\Phi}(N')$ und

$$N = \alpha_M(\hat{\Psi}\hat{\Phi}(N)) \leq \alpha_M(\hat{\Psi}\hat{\Phi}(N')) = N'.$$

Für beliebige Untermoduln $N, N' \leq M$ ist $N + N'$ der kleinste (bzgl. Inklusion) Untermodul von M, der N und N' enthält. Daher ist $\Phi(N + N')$ der kleinste Untermodul von $\hat{\Phi}(M)$, der $\hat{\Phi}(N)$ und $\hat{\Phi}(N')$ enthält. Dies zeigt $\hat{\Phi}(N + N') = \hat{\Phi}(N) + \hat{\Phi}(N')$. Da $N \cap N'$ der größte Untermodul ist, der in N und in N' enthalten ist, gilt entsprechend $\hat{\Phi}(N \cap N') = \hat{\Phi}(N) \cap \hat{\Phi}(N')$. □

Satz III.6.6. *Seien R, S Ringe und $\Phi\colon {}_R\mathbf{Mod} \to {}_S\mathbf{Mod}$ eine Äquivalenz. Für jeden R-Modul M gilt:*

(i) M endlich erzeugt $\iff$ $\Phi(M)$ endlich erzeugt.

(ii) M (halb)einfach $\iff$ $\Phi(M)$ (halb)einfach.

(iii) M unzerlegbar $\iff$ $\Phi(M)$ unzerlegbar.

(iv) M projektiv $\iff$ $\Phi(M)$ projektiv.

(v) M noethersch (artinsch) $\iff$ $\Phi(M)$ noethersch (artinsch).

Beweis. Sei $\Psi\colon {}_S\mathbf{Mod} \to {}_R\mathbf{Mod}$ eine Äquivalenz mit $\Psi\Phi \cong \mathrm{id}$. Wegen $M \simeq \Psi\Phi(M)$ genügt es jeweils „⇒“ zu zeigen.

(i) Sei $f\colon \coprod_{i\in I} S \to \Phi(M)$ ein Epimorphismus. Nach Satz III.5.7, Bemerkung III.5.22 und Lemma III.6.2 existiert ein Epimorphismus

$$g\colon \coprod_{i\in I} \Psi(S) \simeq \Psi\Big(\coprod_{i\in I} S\Big) \xrightarrow{\Psi(f)} \Psi\Phi(M) \simeq M.$$

Da M endlich erzeugt ist, existiert eine endliche Teilmenge $J \subseteq I$ mit $g\big(\coprod_{j\in J} \Psi(S)\big) = M$. Daher gibt es einen Epimorphismus

$$\coprod_{j\in J} S \simeq \coprod_{j\in J} \Phi\Psi(S) \simeq \Phi\Big(\coprod_{j\in J} \Psi(S)\Big) \to \Phi(M).$$

Folglich ist $\Phi(M)$ endlich erzeugt.

(ii) Nach Satz III.6.5 ist M genau dann einfach, wenn $\Phi(M)$ einfach ist. Ist M halbeinfach, also ein Koprodukt von einfachen Moduln, so auch $\Phi(M)$ nach Lemma III.6.2.

(iii) Folgt aus Lemma III.6.2.

(iv) Sei M projektiv, $f \in \mathrm{Hom}_S(\Phi(M), N)$ und $g\colon L \to N$ ein S-Epimorphismus. Da $\Psi\Phi(M)$ projektiv ist, existiert ein $\hat{h} \in \mathrm{Hom}_S(\Psi\Phi(M), \Psi(L))$ mit $\Psi(g) \circ \hat{h} = \Psi(f)$. Da Ψ voll ist, existiert $h \in \mathrm{Hom}_R(\Phi(M), \Psi(L))$ mit $\Psi(h) = \hat{h}$. Nun ist $\Psi(g \circ h) = \Psi(f)$ und $g \circ h = f$, da Ψ treu ist. Also ist $\Phi(M)$ projektiv.

(v) Folgt aus Satz III.6.5. □

Bemerkung III.6.7. Achtung: Ist M frei, so muss $\Phi(M)$ in der Situation von Satz III.6.6 nicht unbedingt frei sein. Ebenso gibt es keinen Zusammenhang zwischen der minimalen Anzahl von Erzeugern von M und $\Phi(M)$ (Bemerkung III.6.42).

Satz III.6.8. *Seien R und S Ringe mit ${}_R\mathbf{Mod} \approx {}_S\mathbf{Mod}$. Dann existiert eine Bijektion $\Omega\colon \{I : I \trianglelefteq R\} \to \{I : I \trianglelefteq S\}$ mit*

$$I \subseteq J \Longleftrightarrow \Omega(I) \subseteq \Omega(J), \qquad \Omega(I+J) = \Omega(I) + \Omega(J),$$
$$\Omega(I \cap J) = \Omega(I) \cap \Omega(J), \qquad \Omega(\mathrm{J}(R)) = \mathrm{J}(S).$$

Beweis. Mit den üblichen Bezeichnungen sei $\Psi\Phi \cong \mathrm{id}$ ein natürlicher Isomorphismus. Für $I \trianglelefteq R$ und $J \trianglelefteq S$ definieren wir $\Omega(I) := \mathrm{Ann}_S(\Phi(R/I)) \trianglelefteq S$ und $\Delta(J) := \mathrm{Ann}_R(\Psi(S/J)) \trianglelefteq R$. Mit einem Erzeugendensystem X von $\Psi(S/J)$ erhält man einen R-Epimorphismus

$$\coprod_{x\in X} R/\Delta(J) \to \Psi(S/J), \qquad (r_x + \Phi(S/J))_x \mapsto \sum_{x\in X} r_x x$$

und einen R-Monomorphismus

$$R/\Delta(J) \to \prod_{x\in X} \Psi(S/J), \qquad r + \Delta(J) \mapsto (rx)_{x\in X}.$$

Durch Anwendung von Φ ergeben sich ein S-Epimorphismus und ein S-Monomorphismus

$$\coprod_{x\in X} \Phi(R/\Delta(J)) \simeq \Phi\Big(\coprod_{x\in X} R/\Delta(J)\Big) \to \Phi\Psi(S/J) \simeq S/J,$$
$$\Phi(R/\Delta(J)) \to \Phi\Big(\prod_{x\in X} \Psi(S/J)\Big) \simeq \prod_{x\in X} \Phi\Psi(S/J) \simeq \prod_{x\in X} S/J.$$

Dies zeigt

$$J = \mathrm{Ann}_S(S/J) = \mathrm{Ann}_S\Big(\prod_{x\in X} S/J\Big) \subseteq \mathrm{Ann}_S(\Phi(R/\Delta(J))) = \mathrm{Ann}_S\Big(\coprod_{x\in X} \Phi(R/\Delta(J))\Big) \subseteq \mathrm{Ann}_S(S/J)$$

und $J = \Omega(\Delta(J))$. Völlig analog ergibt sich $I = \Delta(\Omega(I))$ für $I \trianglelefteq R$. Sei nun $I \subseteq I'$. Dann sind $f\colon R/I \to R/I'$, $r + I \mapsto r + I'$ und $\Phi(f)$ Epimorphismen. Dies zeigt

$$\Omega(I) = \mathrm{Ann}_S(\Phi(R/I)) \subseteq \mathrm{Ann}_S(\Phi(R/I')) = \Omega(I').$$

Aus $\Omega(I) \subseteq \Omega(I')$ ergibt sich umgekehrt $I = \Delta(\Omega(I)) \subseteq \Delta(\Omega(I')) = I'$. Daraus folgt $\Omega(I + I') = \Omega(I) + \Omega(I')$ und $\Omega(I \cap I') = \Omega(I) \cap \Omega(I')$ wie in Satz III.6.5.

Für die letzte Behauptung sei N ein einfacher S-Modul. Nach Satz III.6.6 ist $\Psi(N)$ ein einfacher R-Modul. Für $x \in \Psi(N) \setminus \{0\}$ ist $R/\mathrm{J}(R) \to \Psi(N)$, $r + \mathrm{J}(R) \mapsto rx$ ein wohldefinierter R-Epimorphismus nach Lemma II.8.11. Also ist auch $\Phi(R/\mathrm{J}(R)) \to \Phi\Psi(N) \simeq N$ ein Epimorphismus und es folgt $\Omega(\mathrm{J}(R)) \subseteq \mathrm{Ann}_S(N)$. Aus Lemma II.8.11 erhält man $\Omega(\mathrm{J}(R)) \subseteq \mathrm{J}(S)$. Analog gilt $\mathrm{J}(R) = \Delta(\Omega(\mathrm{J}(R))) \subseteq \Delta(\mathrm{J}(S)) \leq \mathrm{J}(R)$ und $\Omega(\mathrm{J}(R)) = \mathrm{J}(S)$. □

Satz III.6.9. *Seien R und S Ringe mit ${}_R\mathbf{Mod} \approx {}_S\mathbf{Mod}$. Dann gilt*

(i) R (halb)einfach $\iff$ S (halb)einfach.

(ii) R noethersch (artinsch) $\iff$ S noethersch (artinsch).

Beweis. Nach Satz III.6.8 ist R genau dann einfach, wenn S einfach ist. Die anderen Aussagen folgen aus Lemma II.8.4 und Satz III.6.6. □

Bemerkung III.6.10. Ist R lokal, so muss S in der Situation von Satz III.6.9 nicht unbedingt lokal sein (Beispiel III.6.36).

Definition III.6.11. Seien R und S Ringe.

- Ein *R-S-Bimodul* M ist ein R-Linksmodul und zugleich ein S-Rechtsmodul mit $(rm)s = r(ms)$ für alle $m \in M$, $r \in R$ und $s \in S$.
- Ein *R-S-Homomorphismus* $f\colon M \to N$ zwischen R-S-Bimoduln M und N ist ein R-Homomorphismus und zugleich ein S-Homomorphismus, d. h. $f(r(m+m')s) = rf(m)s + rf(m')s$ für $r \in R$, $s \in S$ und $m, m' \in M$.

Sei ${}_R\mathbf{Mod}_S$ (bzw. ${}_R\mathbf{mod}_S$) die Kategorie der (endlich erzeugten) R-S-Bimoduln.

Beispiel III.6.12.

(i) Jedes Ideal $I \trianglelefteq R$ ist ein R-R-Bimodul und die Inklusion $I \hookrightarrow R$ ist ein R-R-Homomorphismus.

(ii) Bekanntlich ist jeder R-Linksmodul ein R^o-Rechtsmodul. Daher ist ein R-S-Bimodul ein S^o-R^o-Bimodul.

(iii) Da jeder R-Linksmodul M eine abelsche Gruppe bzgl. $+$ ist, ist M ein R-$\mathbb{Z}$-Bimodul. Alle Aussagen über Bimoduln lassen sich also auf Links- oder Rechtsmoduln übertragen. Ist R kommutativ, so ist M ein R-R-Bimodul mit $m \cdot r := rm$ für $r \in R$ und $m \in M$.

(iv) Für $n, m \in \mathbb{N}$ ist $R^{n\times m}$ ein $R^{n\times n}$-$R^{m\times m}$-Bimodul, denn die Matrizenmultiplikation ist assoziativ.

(v) Sei M ein S-Rechtsmodul und $R := \mathrm{End}_S(M)$. Durch $\varphi \cdot m := \varphi(m)$ für $\varphi \in R$ und $m \in M$ wird M ein R-Linksmodul (Bemerkung II.6.11). Wegen $(\varphi m)s = \varphi(m)s = \varphi(ms) = \varphi(ms)$ für $s \in S$ ist M ein R-S-Bimodul.

(vi) Sei M ein R-S-Bimodul und N ein R-T-Bimodul. Dann ist $\mathrm{Hom}_R(M,N)$ ein S-T-Bimodul mit $(s\varphi t)(m) := \varphi(ms)t$ für $s \in S$, $t \in T$ und $m \in M$ (nachrechnen). Ist N ein T-S-Bimodul, so ist $\mathrm{Hom}_S(M,N)$ ein T-R-Bimodul mit $(t\varphi r)(m) := t\varphi(rm)$.

(vii) Wie üblich definiert man Untermoduln von Bimoduln und Mono-, Epi- und Isomorphismen. Der Homomorphiesatz und die Isomorphiesätze gelten selbstverständlich auch für Bimoduln.

Bemerkung III.6.13. Wir hatten in Definition III.3.17 das Tensorprodukt von Moduln über Gruppenalgebren eingeführt. In Aufgabe II.52 wurde das Tensorprodukt für Moduln über kommutativen Ringen konstruiert. Für beliebige Ringe ist das Tensorprodukt von Moduln im Allgemeinen nur ein $\mathbb{Z}$-Modul. Mit Hilfe von Bimoduln kann man die Situation verbessern.

Definition III.6.14. Seien R, S, T Ringe, M ein R-S-Bimodul und N ein S-T-Bimodul.

- Sei A die freie abelsche Gruppe mit Basis $\{e_{m,n} : (m,n) \in M \times N\}$. Sei B die von den Elementen

$$e_{m+m',n} - e_{m,n} - e_{m',n}, \qquad e_{m,n+n'} - e_{m,n} - e_{m,n'}, \qquad e_{ms,n} - e_{m,sn}$$

  mit $m, m' \in M$, $n, n' \in N$ und $s \in S$ erzeugte Untergruppe von A. Wir definieren das *Tensorprodukt*

$$M \otimes_S N := A/B$$

  und $m \otimes n := e_{m,n} + B \in M \otimes_S N$.

- Sei C eine beliebige abelsche Gruppe. Ein Abbildung $f\colon M \times N \to C$ heißt *ausgeglichen*, falls

$$f(m+m',n) = f(m,n) + f(m',n), \quad f(m,n+n') = f(m,n) + f(m,n'), \quad f(ms,n) = f(m,sn)$$

  für $m, m' \in M$, $n, n' \in N$ und $r \in R$ gilt.

Bemerkung III.6.15.

(i) Die Elemente $m \otimes n$ bilden ein Erzeugendensystem von $M \otimes_S N$, aber im Allgemeinen keine Basis. Außerdem hat nicht jedes Element in $M \otimes_S N$ die Form $m \otimes n$. Abbildungen zwischen Tensorprodukten werden daher über eine universelle Eigenschaft definiert, um die Wohldefiniertheit zu garantieren.

(ii) Nach Konstruktion ist $M \times N \to M \otimes_S N$, $(m,n) \mapsto m \otimes n$ ausgeglichen.

Lemma III.6.16 (Universelle Eigenschaft des Tensorprodukts)**.** *Sei $f\colon M \times N \to C$ ausgeglichen mit den Bezeichnungen aus Definition III.6.14. Dann existiert genau ein $\mathbb{Z}$-Homomorphismus $\hat{f}\colon M \otimes_S N \to C$ mit $\hat{f}(m \otimes n) = f(m,n)$ für $m \in M$ und $n \in N$.*

Beweis. Wir definieren zunächst $\varphi\colon A \to C$ durch $\varphi(e_{m,n}) := f(m,n)$. Da f ausgeglichen ist, ist $B \subseteq \mathrm{Ker}(\varphi)$. Mit dem Homomorphiesatz erhält man $\hat{f}\colon M \otimes_S N = A/B \to C$ mit $\hat{f}(m \otimes n) = \varphi(e_{m,n}) = f(m,n)$. Da $M \otimes_S N$ durch die Elemente $m \otimes n$ erzeugt wird, ist $\hat{f}$ durch f eindeutig bestimmt. □

Lemma III.6.17. *Durch $r(m \otimes n) := rm \otimes n$ und $(m \otimes n)t := m \otimes nt$ für $r \in R$, $t \in T$, $m \in M$ und $n \in N$ wird $M \otimes_S N$ ein R-T-Bimodul.*

Beweis. Für $r \in R$ ist die Abbildung $f_r \colon M \times N \to M \otimes_S N$, $(m,n) \mapsto rm \otimes n$ ausgeglichen. Nach der universellen Eigenschaft existiert ein $\mathbb{Z}$-Homomorphismus $\hat{f}_r \colon M \otimes_S N \to M \otimes_S N$. Für $x \in M \otimes_S N$ und $r \in R$ ist nun $r \cdot x := \hat{f}_r(x)$ wohldefiniert. Mit $x := \sum_{i=1}^k m_i \otimes n_i$ und $y \in M \otimes_S N$ folgt

$$\begin{aligned} 1x &= \hat{f}_1(x) = x, \\ (r+s)x &= \hat{f}_{r+s}(x) = \sum_{i=1}^k (r+s)m_i \otimes n_i = \hat{f}_r(x) + \hat{f}_s(x) = rx + sx, \\ r(s(x)) &= \sum_{i=1}^k \hat{f}_r(sm \otimes n) = \sum_{i=1}^k rsm \otimes n = \hat{f}_{rs}(x) = (rs)x, \\ r(x+y) &= \hat{f}_r(x+y) = \hat{f}_r(x) + \hat{f}_r(y) = rx + ry. \end{aligned}$$

Also ist $M \otimes_S N$ ein R-Linksmodul. Völlig analog zeigt man, dass $M \otimes_S N$ ein T-Rechtsmodul ist. Wegen $(r(m \otimes n))s = (rm \otimes n)s = rm \otimes ns = r(m \otimes ns) = r((m \otimes n)s)$ handelt es sich um einen R-T-Bimodul. □

Beispiel III.6.18.

(i) Sei M ein R-S-Bimodul. Die ausgeglichene Abbildung $R \times M \to M$, $(r,m) \mapsto rm$ induziert einen $\mathbb{Z}$-Homomorphismus $f \colon R \otimes_R M \to M$, $r \otimes m \to rm$. Offensichtlich ist f ein R-S-Isomorphismus mit Umkehrabbildung $M \to R \otimes_R M$, $m \mapsto 1 \otimes m$. Insbesondere ist $\boxed{R \otimes_R M \simeq M.}$

(ii) Sei $R := \mathbb{Z}$, $M := \mathbb{Z}/m\mathbb{Z}$ und $N := \mathbb{Z}/n\mathbb{Z}$ mit $m,n \in \mathbb{N}_0$. Sei $g := \mathrm{ggT}(m,n)$ und $L := \mathbb{Z}/g\mathbb{Z}$. Dann ist $M \times N \to L$, $(x+m\mathbb{Z}, y+n\mathbb{Z}) \mapsto xy + g\mathbb{Z}$ wohldefiniert und ausgeglichen. Also existiert ein Homomorphismus

$$\varphi \colon M \otimes_{\mathbb{Z}} N \to L, \qquad (x+m\mathbb{Z}) \otimes (y+n\mathbb{Z}) \mapsto xy + g\mathbb{Z}.$$

Umgekehrt ist

$$\psi \colon L \to M \otimes_{\mathbb{Z}} N, \qquad z + g\mathbb{Z} \mapsto (z+m\mathbb{Z}) \otimes (1+n\mathbb{Z}) = (1+m\mathbb{Z}) \otimes (z+n\mathbb{Z})$$

ein wohldefinierter Homomorphismus mit $\psi \circ \varphi = \mathrm{id}_{M \otimes_{\mathbb{Z}} N}$ und $\varphi \circ \psi = \mathrm{id}_L$. Dies zeigt

$$\boxed{(\mathbb{Z}/m\mathbb{Z}) \otimes_{\mathbb{Z}} (\mathbb{Z}/n\mathbb{Z}) \simeq \mathbb{Z}/\mathrm{ggT}(m,n)\mathbb{Z}.}$$

(iii) Sei K ein Körper, G eine endliche Gruppe und $R = KG$ die Gruppenalgebra. Endlich-dimensionale R-Moduln M, N kann man als R-K-Bimodul bzw. K-R^o-Bimodul auffassen. Der R-R^o-Bimodul $M \otimes_K N$ wird durch

$$r \cdot (m \otimes n) := r(m \otimes n)r = rm \otimes rn$$

zu einem R-Linksmodul. Sei $b_1, \ldots, b_k$ eine K-Basis von M und $c_1, \ldots, c_l$ eine K-Basis von N. Offenbar ist dann $\{b_i \otimes b_j : 1 \le i \le k, 1 \le j \le l\}$ ein Erzeugendensystem von $M \otimes_K N$ als K-Vektorraum. Sei A die freie abelsche Gruppe mit Basis $\{e_{m,n} : m \in M, n \in N\}$ und B die entsprechende Untergruppe wie in Definition III.6.14. Durch $\lambda e_{m,n} := e_{\lambda m,n}$ für $\lambda \in K$ werden A und A/B zu K-Vektorräumen. Zum Vergleich sei $T := M \otimes N$ das in Definition III.3.17 definierte Tensorprodukt. Dann existiert ein K-Epimorphismus $\varphi \colon A \to T$, $e_{m,n} \mapsto m \otimes n$ mit $B \subseteq \mathrm{Ker}(\varphi)$. Dies zeigt

$$kl = \dim T = \dim A - \dim \mathrm{Ker}(\varphi) \le \dim A/B = \dim M \otimes_K N \le kl.$$

Also bilden $b_i \otimes c_j$ auch eine K-Basis von $M \otimes_S N$ und man erhält einen R-Isomorphismus $M \otimes_S N \simeq T$.

Lemma III.6.19. *Seien $f\colon M \to M'$ und $g\colon N \to N'$ Homomorphismen zwischen R-S-Bimoduln M, M' bzw. S-T-Bimoduln N, N'. Dann existiert genau ein R-T-Homomorphismus $f \otimes g\colon M \otimes_S M' \to N \otimes_T N'$, $m \otimes n \mapsto f(m) \otimes g(n)$.*

Beweis. Die ausgeglichene Abbildung $M \times N \to M' \otimes_S N'$, $(m, n) \mapsto f(m) \otimes g(n)$ setzt sich zu dem angegebenen $\mathbb{Z}$-Homomorphismus $f \otimes g$ fort. Für $r \in R$, $t \in T$, $m \in M$ und $n \in N$ gilt

$$\begin{aligned}(f \otimes g)(r(m \otimes n)t) = (f \otimes g)(rm \otimes nt) = f(rm) \otimes g(nt) = rf(m) \otimes g(n)t \\ = r(f(m) \otimes g(n))t = r(f \otimes g)(m \otimes n)t.\end{aligned}$$

Daher ist $f \otimes g$ ein R-T-Homomorphismus. □

Bemerkung III.6.20. Mit geeigneten Bezeichnungen gilt:

$$\begin{aligned}0 \otimes g = 0, \qquad f \otimes 0 = 0, \qquad & (f \otimes g) \circ (f' \otimes g') = (f \circ f') \otimes (g \circ g'), \\ f \otimes (g + g') = f \otimes g + f \otimes g', \qquad & (f + f') \otimes g = f \otimes g + f' \otimes g.\end{aligned}$$

Lemma III.6.21. *Seien R, S, T, U Ringe und A, B, C Bimoduln bzgl. (R, S), (S, T), (T, U). Dann existiert ein R-U-Isomorphismus*

$$A \otimes_S (B \otimes_T C) \to (A \otimes_S B) \otimes_T C, \qquad a \otimes (b \otimes c) \mapsto (a \otimes b) \otimes c.$$

Beweis. Für $a \in A$ existiert wie üblich ein S-T-Homomorphismus $f_a\colon B \otimes_T C \to (A \otimes_S B) \otimes_T C$, $b \otimes c \mapsto (a \otimes b) \otimes c$. Man zeigt leicht, dass $f\colon A \times (B \otimes_T C) \to (A \otimes_S B) \otimes_T C$, $(a, x) \mapsto f_a(x)$ ausgeglichen ist. Dies liefert einen R-U-Homomorphismus

$$\hat{f}\colon A \otimes_S (B \otimes_T C) \to (A \otimes_S B) \otimes_T C, \qquad a \otimes (b \otimes c) \mapsto f_a(b \otimes c) = (a \otimes b) \otimes c.$$

Völlig analog erhält man einen R-T-Homomorphismus $g\colon (A \otimes_S B) \otimes_T C \to A \otimes_S (B \otimes_T C)$, $(a \otimes b) \otimes c \mapsto a \otimes (b \otimes c)$. Offenbar ist $fg = \mathrm{id}$ und $gf = \mathrm{id}$. □

Lemma III.6.22. *Für Familien von R-S-Bimoduln $(M_i)_{i \in I}$ und S-T-Bimoduln $(N_j)_{j \in J}$ existiert ein R-T-Isomorphismus*

$$\Big(\coprod_{i \in I} M_i\Big) \otimes_S \Big(\coprod_{j \in J} N_j\Big) \to \coprod_{i \in I} \coprod_{j \in J} (M_i \otimes_S N_j), \qquad (m_i)_i \otimes (n_j)_j \mapsto (m_i \otimes n_j)_{i,j}.$$

Beweis. Wie üblich ist $\Big(\coprod_{i \in I} M_i\Big) \times \Big(\coprod_{j \in J} N_j\Big) \to \coprod_{i \in I} \coprod_{j \in J} (M_i \otimes_S N_j)$, $((m_i)_i, (n_j)_j) \mapsto (m_i \otimes n_j)_{i,j}$ ausgeglichen und die angegebene Abbildung ist ein R-T-Homomorphismus. Die Umkehrabbildung erhält man durch

$$\coprod_{i \in I} \coprod_{j \in J} (M_i \otimes_S N_j), (x_{ij})_{i,j} \mapsto \sum_{i \in I} \sum_{j \in J} x_{ij}$$

(nur endlich viele Summanden sind von 0 verschieden). □

Satz III.6.23. *Für Bimoduln A, B, C bzgl. (R, S), (S, T), (U, T) existiert ein U-R-Isomorphismus*

$$\mathrm{Hom}_T(A \otimes_S B, C) \simeq \mathrm{Hom}_S(A, \mathrm{Hom}_T(B, C)).$$

Beweis. Für $f \in \mathrm{Hom}_T(A \otimes_S B, C)$ und $a \in A$ ist $f_a \colon B \to C$, $b \mapsto f(a \otimes b)$ ein Homomorphismus von T-Rechtsmoduln. Außerdem ist $\Delta(f) \colon A \to \mathrm{Hom}_T(B, C)$, $a \mapsto f_a$ ein Homomorphismus von S-Rechtsmoduln, denn

$$\Delta(f)(as)(b) = f_{as}(b) = f(as \otimes b) = f(a \otimes sb) = f_a(sb) = (f_a s)(b) = (\Delta(f)(a)s)(b).$$

Für $g \in \mathrm{Hom}_T(A \otimes_S B, C)$ ist $\Delta(f+g) = \Delta(f) + \Delta(g)$. Für $u \in U$ und $r \in R$ gilt

$$\begin{aligned}\Delta(ufr)(a)(b) &= (ufr)_a(b) = (ufr)(a \otimes b) = f(ra \otimes b)u \\ &= f_{ra}(b)u = (\Delta(f)(ra)u)(b) = (u\Delta(f)r)(a)(b).\end{aligned}$$

Insgesamt ist $\Delta \colon \mathrm{Hom}_T(A \otimes_S B, C) \to \mathrm{Hom}_S(A, \mathrm{Hom}_T(B, C))$ ein U-R-Homomorphismus.

Sei umgekehrt $\varphi \in \mathrm{Hom}_S(A, \mathrm{Hom}_T(B, C))$ gegeben. Dann ist $A \times B \to C$, $(a, b) \mapsto \varphi(a)(b)$ ausgeglichen und man erhält einen $\mathbb{Z}$-Homomorphismus $\Gamma(\varphi) \colon A \otimes_S B \to C$, $a \otimes b \mapsto \varphi(a)(b)$. Man rechnet leicht nach, dass $\Gamma(\varphi)$ ein Homomorphismus von T-Rechtsmoduln ist. Für $\psi \in \mathrm{Hom}_S(A, \mathrm{Hom}_T(B, C))$ ist $\Gamma(\varphi + \psi) = \Gamma(\varphi) + \Gamma(\psi)$. Für $u \in U$ und $r \in R$ berechnet man

$$\Gamma(u\varphi r)(a \otimes b) = (u\varphi r)(a)(b) = (\varphi(ra)u)(b) = \varphi(ra)(b)u = \Gamma(\varphi)(ra \otimes b)u = (u\Gamma(\varphi)r)(a \otimes b).$$

Daher ist $\Gamma \colon \mathrm{Hom}_S(A, \mathrm{Hom}_T(B, C)) \to \mathrm{Hom}_T(A \otimes_S B, C)$ ein U-R-Homomorphismus.

Schließlich gilt

$$\begin{aligned}\Gamma(\Delta(f))(a \otimes b) &= \Delta(f)(a)(b) = f_a(b) = f(a \otimes b), \\ \Delta(\Gamma(\varphi))(a)(b) &= \Gamma(\varphi)_a(b) = \Gamma(\varphi)(a \otimes b) = \varphi(a)(b),\end{aligned}$$

d. h. $\Gamma\Delta = \mathrm{id}$ und $\Delta\Gamma = \mathrm{id}$. □

Bemerkung III.6.24. Wegen

$$(f \circ g) \otimes \mathrm{id} = (f \circ g) \otimes (\mathrm{id} \circ \mathrm{id}) = (f \otimes \mathrm{id}) \circ (g \otimes \mathrm{id})$$

ist $. \otimes_S B \colon {}_R\mathbf{Mod}_S \to {}_R\mathbf{Mod}_T$, $A \mapsto A \otimes_S B$ mit $f \otimes_S B := f \otimes \mathrm{id}_B$ für $f \colon A \to A'$ ein Funktor. Bekanntlich ist auch $\mathrm{Hom}(B, .) \colon {}_R\mathbf{Mod}_T \to {}_R\mathbf{Mod}_S$ ein Funktor. Die im Beweis von Satz III.6.23 konstruierte Bijektion $\alpha_{(A,C)} := \Delta \colon \mathrm{Hom}_T(A \otimes_S B, C) \to \mathrm{Hom}_S(A, \mathrm{Hom}_T(B, C))$ erfüllt

$$\begin{aligned}\big(\alpha_{(A',C')} \circ \mathrm{Hom}((f_A \otimes B), f_C)\big)(\varphi)(a)(b) &= \alpha_{(A',C')}\big(f_C \circ \varphi \circ (f_A \otimes \mathrm{id}_B)\big)(a)(b) \\ &= f_C\big(\varphi(f_A(a) \otimes b)\big) = (f_C \circ \varphi_{f_A(a)})(b) = \big(\mathrm{Hom}(B, f_C) \circ \alpha_{(A,C)}(\varphi) \circ f_A\big)(a)(b) \\ &= \big(\mathrm{Hom}(f_A, \mathrm{Hom}(B, f_C)) \circ \alpha_{(A,C)}\big)(\varphi)(a)(b)\end{aligned}$$

für $f = (f_A, f_C) \in \mathrm{Hom}_{({}_S\mathbf{Mod}_R)^o \times {}_R\mathbf{Mod}_T}(A \times C, A' \times C')$, $\varphi \in \mathrm{Hom}_T(A \otimes_S B, C)$, $a \in A'$, $b \in B$. Daher ist α ein natürlicher Isomorphismus und $. \otimes_S B$ ist links-adjungiert zu $\mathrm{Hom}(B, .)$.

Definition III.6.25. Ein R-Modul P heißt (R-)*Generator*, falls der Funktor $\mathrm{Hom}(P, .) \colon {}_R\mathbf{Mod} \to \mathbf{Ab}$ treu ist (für Rechtsmoduln betrachtet man $\mathrm{Hom}(P, .) \colon \mathbf{Mod}_R \to \mathbf{Ab}$).

Bemerkung III.6.26. Sei P ein Generator. Für R-Moduln M, N ist dann die Abbildung

$$\Gamma \colon \mathrm{Hom}_R(M, N) \to \mathrm{Hom}_{\mathbf{Ab}}\big(\mathrm{Hom}_R(P, M), \mathrm{Hom}_R(P, N)\big)$$

mit $\Gamma(f)(g) = f \circ g$ für $f \in \mathrm{Hom}_R(M, N)$ und $g \in \mathrm{Hom}_R(P, M)$ injektiv. Da Γ ein Gruppenhomomorphismus ist, ist die Injektivität äquivalent zu $\mathrm{Ker}(\Gamma) = 0$.

Lemma III.6.27. *Für jeden R-Modul P sind die folgenden Aussagen äquivalent:*

(1) P ist ein Generator.

(2) Der reguläre R-Modul ist (bis auf Isomorphie) ein direkter Summand von P^n für ein $n \in \mathbb{N}$.

(3) Jeder R-Modul ist zu einem Faktormodul von $\coprod_{i\in I} P$ isomorph, wobei I eine Indexmenge ist.

Beweis.

(1) $\Rightarrow$ (2): Sei $P^* := \mathrm{Hom}_R(P, R)$ und $J := \sum_{f\in P^*} f(P) \leq R$. Angenommen es gilt $J < R$. Dann ist der kanonische Epimorphismus $\pi\colon R \to R/J$ nicht-trivial. Da P ein Generator ist, existiert $g \in P^*$ mit $\pi \circ g \neq 0$, d. h. $g(P) \nsubseteq J$. Dieser Widerspruch zeigt $J = R$. Da R durch 1 erzeugt ist, existieren $f_1, \ldots, f_n \in P^*$ mit $R = f_1(P) + \ldots + f_n(P)$. Dies liefert einen Epimorphismus $\varphi\colon P^n \to R$. Da R projektiv ist, gilt $P^n = \mathrm{Ker}(\varphi) \oplus Q$ mit $Q \cong R$ (Satz II.12.13).

(2) $\Rightarrow$ (3): Für jeden R-Modul M existiert ein freier Modul, sagen wir $F := \coprod_{b\in B} R$ und ein Epimorphismus $F \to M$. Nach (2) erhält man durch Projektion einen Epimorphismus $\coprod_{b\in B} P^n \to F$. Die Komposition dieser Abbildungen zeigt (3).

(3) $\Rightarrow$ (1): Sei $f \in \mathrm{Hom}_R(M, N)$ nicht-trivial und $\pi\colon \coprod_{i\in I} P \to M$ ein Epimorphismus (garantiert durch (3)). Dann ist auch $f\circ\pi \neq 0$ und man findet eine Projektion $\rho\colon P \to \coprod_{i\in I} P$ mit $f\circ\pi\circ\rho \neq 0$. Für $g := \pi \circ \rho \in \mathrm{Hom}_R(P, M)$ gilt also $f \circ g \neq 0$ und P ist ein Generator. □

Bemerkung III.6.28. Ein endlich erzeugter projektiver Modul P erfüllt die zu Lemma III.6.27(2) duale Eigenschaft: P ist (bis auf Isomorphie) ein direkter Summand von R^n. Um beide Eigenschaften zu kombinieren, nennen wir einen endlich erzeugten projektiven (R-)Generator einen (R-)*Progenerator*.

Beispiel III.6.29.

(i) Jeder endlich erzeugte freie R-Modul ist ein Progenerator.

(ii) Ist A eine endlich-dimensionale K-Algebra und $P_1, \ldots, P_n$ ein Repräsentantensystem für die nicht-isomorphen projektiv-unzerlegbaren A-Moduln, so ist $P_1 \times \ldots \times P_n$ ein Progenerator.

(iii) Ist P ein Generator und $Q \to P$ ein R-Epimorphismus, so ist auch Q ein Generator (benutze Lemma III.6.27(3)).

(iv) Sei $\Phi\colon {}_R\mathbf{Mod} \to {}_S\mathbf{Mod}$ eine Äquivalenz und P ein R-Generator. Für jeden S-Modul N existiert ein R-Modul M mit $\Phi(M) \simeq N$. Da M ein Faktormodul von $\coprod_{i\in I} P$ ist, ist N ein Faktormodul von $\Phi\big(\coprod_{i\in I} P\big) \simeq \coprod_{i\in I} \Phi(P)$. Also ist $\Phi(P)$ ein S-Generator. Mit Satz III.6.6 folgt: P ist R-Progenerator $\iff$ $\Phi(P)$ ist S-Progenerator.

Definition III.6.30. Seien R und S Ringe. Ein *Morita-Kontext* ist ein 6-Tupel $(R, S, M, N, \mathfrak{R}, \mathfrak{S})$ mit folgenden Eigenschaften:

- M ist ein R-S-Bimodul und N ist ein S-R-Bimodul.
- $\mathfrak{R}\colon M \otimes_S N \to R$ ist ein R-R-Homomorphismus und $\mathfrak{S}\colon N \otimes_R M \to S$ ein S-S-Homomorphismus.
- $\mathfrak{R}(m \otimes n)m' = m\mathfrak{S}(n \otimes m')$ und $n\mathfrak{R}(m \otimes n') = \mathfrak{S}(n \otimes m)n'$ für $m, m' \in M$ und $n, n' \in N$.[2]

[2] Merkregel: Die Variablen m, n, m' und n, m, n' werden zyklisch permutiert.

Satz III.6.31. *Sei $(R, S, M, N, \mathfrak{R}, \mathfrak{S})$ ein Morita-Kontext mit surjektivem $\mathfrak{R}$. Dann gilt:*

(i) *$\mathfrak{R}$ ist ein R-R-Isomorphismus.*

(ii) *M und N sind endlich erzeugte projektive S-Moduln.*

(iii) *M und N sind R-Generatoren.*

(iv) *$\Omega\colon R \to \mathrm{End}_S(M)$, $\Omega \mapsto \Omega_r$ mit $\Omega_r(m) := rm$ und $\Omega'\colon R^o \to \mathrm{End}_R(N)$, $r \mapsto \Omega'_r$ mit $\Omega'_r(n) := nr$ sind Ringisomorphismen.*

Beweis. Nach Voraussetzung existieren $m_1, \ldots, m_k \in M$ und $n_1, \ldots, n_k \in N$ mit $\mathfrak{R}\big(\sum_{i=1}^k m_i \otimes n_i\big) = 1_R$.

(i) Seien $x_1, \ldots, x_l \in M$ und $y_1, \ldots, y_l \in N$ mit $\mathfrak{R}(\sum_{i=1}^l x_i \otimes y_i) = 0$. Dann gilt

$$\begin{aligned}\sum_{j=1}^{l} x_j \otimes y_j &= \sum_{j=1}^{l}\sum_{i=1}^{k}(x_j \otimes y_j)\mathfrak{R}(m_i \otimes n_i) = \sum_{j=1}^{l}\sum_{i=1}^{k} x_j \otimes y_j\mathfrak{R}(m_i \otimes n_i)\\ &= \sum_{j=1}^{l}\sum_{i=1}^{k} x_j \otimes \mathfrak{S}(y_j \otimes m_i)n_i = \sum_{j=1}^{l}\sum_{i=1}^{k} x_j\mathfrak{S}(y_j \otimes m_i) \otimes n_i\\ &= \sum_{j=1}^{l}\sum_{i=1}^{k} \mathfrak{R}(x_j \otimes y_j)m_i \otimes n_i = \mathfrak{R}\Big(\sum_{j=1}^{l} x_j \otimes y_j\Big)\sum_{i=1}^{k} m_i \otimes n_i = 0.\end{aligned}$$

Also ist $\mathfrak{R}$ injektiv.

(ii) Die Abbildungen

$$\begin{aligned} f\colon S^k &\to M, & (s_1, \ldots, s_k) &\mapsto m_1s_1 + \ldots + m_ks_k,\\ g\colon M &\to S^k, & m &\mapsto (\mathfrak{S}(n_1 \otimes m), \ldots, \mathfrak{S}(n_k \otimes m))\end{aligned}$$

sind S-Homomorphismen mit

$$f(g(m)) = \sum_{i=1}^{k} m_i\mathfrak{S}(n_i \otimes m) = \sum_{i=1}^{k} \mathfrak{R}(m_i \otimes n_i)m = m$$

für $m \in M$. Insbesondere ist f surjektiv und $M = \langle m_1, \ldots, m_k\rangle$ ein endlich erzeugter S-Modul. Außerdem ist g injektiv und $S^k = \mathrm{Ker}(f) \oplus g(M)$. Also ist $M \simeq g(M)$ projektiv als S-Modul. Für die zweite Behauptung betrachtet man analog $f\colon S^k \to N$, $(s_1, \ldots, s_k) \mapsto s_1n_1 + \ldots + s_kn_k$ und $g\colon N \to S^k$, $n \mapsto (\mathfrak{S}(n \otimes m_1), \ldots, \mathfrak{S}(n \otimes m_k))$.

(iii) Die Abbildung $f\colon M^k \to R$, $(x_1, \ldots, x_k) \mapsto \mathfrak{R}\big(\sum_{i=1}^k x_i \otimes n_i\big)$ ist ein R-Epimorphismus wegen $f(m_1, \ldots, m_k) = 1_R$. Mit R sind auch M^k und M Generatoren (Beispiel III.6.29). Für N betrachtet man analog $N^k \to R$, $(y_1, \ldots, y_k) \mapsto \mathfrak{R}\big(\sum_{i=1}^k m_i \otimes y_i\big)$.

(iv) Man zeigt leicht, dass Ω und Ω' Ringhomomorphismen sind (beachte $\Omega'(r \cdot r') = \Omega'_{r'r} = \Omega'_r \circ \Omega'_{r'}$). Für $r \in \mathrm{Ker}(\Omega)$ gilt

$$r = \sum_{i=1}^{k} r\mathfrak{R}(m_i \otimes n_i) = \sum_{i=1}^{k} \mathfrak{R}(rm_i \otimes n_i) = \sum_{i=1}^{k} \mathfrak{R}(\Omega_r(m) \otimes n_i) = 0,$$

d. h. Ω ist injektiv. Sei $\varphi \in \mathrm{End}_S(M)$ gegeben. Dann ist

$$\begin{aligned}\varphi(m) &= \sum_{i=1}^{k} \varphi(\mathfrak{R}(m_i \otimes n_i)m) = \sum_{i=1}^{k} \varphi(m_i \mathfrak{S}(n_i \otimes m)) \\ &= \sum_{i=1}^{k} \varphi(m_i)\mathfrak{S}(n_i \otimes m) = \sum_{i=1}^{k} \mathfrak{R}(\varphi(m_i) \otimes n_i)m.\end{aligned}$$

Es folgt $\Omega\big(\sum_{i=1}^{k} \mathfrak{R}(\varphi(m_i) \otimes n_i)\big) = \varphi$. Analog beweist man die Bijektivität von Ω'. □

Bemerkung III.6.32. Aus Symmetriegründen gilt Satz III.6.31 auch, wenn man $(R, M, \mathfrak{R})$ und $(S, N, \mathfrak{S})$ vertauscht.

Beispiel III.6.33. Sei M ein beliebiger R-Linksmodul, $S := \mathrm{End}_R(M)^o$ und $N := \mathrm{Hom}_R(M, R)$. Bekanntlich ist M ein $\mathrm{End}_R(M)$-Linksmodul und somit ein R-S-Bimodul. Nach Beispiel III.6.12 ist N ein S-R-Bimodul mit

$$r \cdot m \cdot \varphi = \varphi(rm) = r\varphi(m), \qquad \varphi \cdot \lambda \cdot r = (\lambda \circ \varphi)r = \lambda r \circ \varphi$$

für $r \in R$, $\varphi \in S$, $m \in M$ und $\lambda \in N$. Wegen $\lambda(m\varphi) = (\lambda \circ \varphi)(m) = (\varphi\lambda)(m)$ ist die Abbildung $M \times N \to R$, $(m, \lambda) \mapsto \lambda(m)$ ausgeglichen bzgl. S. Nach der universellen Eigenschaft des Tensorprodukts induziert sie einen $\mathbb{Z}$-Homomorphismus

$$\mathfrak{R}\colon M \otimes_S N \to R, \qquad m \otimes \lambda \mapsto \lambda(m).$$

Wegen $r\lambda(m)r' = \lambda(rm)r' = (\lambda r')(rm)$ für $r, r' \in R$ ist $\mathfrak{R}$ ein R-R-Homomorphismus. Für fest gewählte m und λ ist die Abbildung $\mathfrak{S}_{\lambda,m}\colon M \to M$, $x \mapsto \lambda(x)m$ ein R-Homomorphismus, also ein Element von S. Wegen

$$\mathfrak{S}_{\lambda r,m}(x) = (\lambda r)(x)m = \lambda(x)rm = \mathfrak{S}_{\lambda,rm}(x)$$

erhält man eine ausgeglichene Abbildung $N \times M \to S$, $(\lambda, m) \mapsto \mathfrak{S}_{\lambda,m}$. Also existiert ein $\mathbb{Z}$-Homomorphismus

$$\mathfrak{S}\colon N \otimes_R M \to S, \qquad \lambda \otimes m \mapsto \mathfrak{S}_{\lambda,m}.$$

Für $\varphi, \psi \in S$ gilt

$$\mathfrak{S}_{\varphi\lambda,m\psi}(x) = (\varphi\lambda)(x)(m\psi) = \lambda(\varphi(x))\psi(m) = \psi\big(\lambda(\varphi(x))m\big) = \psi\big(\mathfrak{S}_{\lambda,m}(\varphi(x))\big) = (\varphi \cdot \mathfrak{S}_{\lambda,m} \cdot \psi)(x),$$

d. h. $\mathfrak{S}$ ist ein S-S-Homomorphismus.

Für $m, m' \in M$ und $\lambda, \lambda' \in N$ gilt schließlich

$$\begin{aligned}\mathfrak{R}(m \otimes \lambda)m' &= \lambda(m)m' = \mathfrak{S}_{\lambda,m'}(m) = m\mathfrak{S}(\lambda \otimes m'), \\ (\lambda\mathfrak{R}(m \otimes \lambda'))(m') &= (\lambda\lambda'(m))(m') = \lambda(m')\lambda'(m) = \lambda'(\lambda(m')m) \\ &= (\lambda' \circ \mathfrak{S}_{\lambda,m})(m') = (\mathfrak{S}_{\lambda,m}\lambda')(m') = (\mathfrak{S}(\lambda \otimes m)\lambda')(m').\end{aligned}$$

Also ist $(R, S, M, N, \mathfrak{R}, \mathfrak{S})$ ein Morita-Kontext.

Satz III.6.34. *Für den konkreten Morita-Kontext aus Beispiel III.6.33 gilt:*

(i) Ist M ein endlich erzeugter projektiver R-Modul, so ist $\mathfrak{S}$ surjektiv.

(ii) Ist M ein R-Generator, so ist $\mathfrak{R}$ surjektiv.

Beweis.

(i) Nach Voraussetzung existieren $k \in \mathbb{N}$ und R-Homomorphismen $f\colon R^k \to M$ und $g\colon M \to R^k$ mit $f \circ g = \mathrm{id}_M$. Sei $e_1, \dots, e_k \in R^k$ die kanonische Basis von R^k und $\pi_i\colon R^k \to R$ die i-te Projektion. Es gilt also $x = \sum_{i=1}^k \pi_i(x) e_i$ für $x \in R^k$. Für $m \in M$ folgt

$$m = f(g(m)) = \sum_{i=1}^k f\big(\pi_i(g(m))e_i\big) = \sum_{i=1}^k \pi_i(g(m)) f(e_i).$$

Mit $m_i := f(e_i) \in M$ und $\lambda_i := \pi_i \circ g \in N$ folgt

$$1_S = \mathrm{id}_M = \sum_{i=1}^k \mathfrak{S}_{\lambda_i, m_i} = \mathfrak{S}\Big(\sum_{i=1}^k \lambda_i \otimes m_i\Big) \in \mathfrak{S}(N \otimes_R M).$$

Daher ist $\mathfrak{S}$ surjektiv.

(ii) Nach Lemma III.6.27 existiert eine Indexmenge I und ein R-Epimorphismus $f\colon \coprod_{i\in I} M \to R$. Sei $(m_i)_{i\in I} \in \coprod_{i\in I} M$ mit $f\big((m_i)_i\big) = 1_R$. Dann ist $J := \{i \in I : m_i \neq 0\}$ endlich. Sei $q_i\colon M \to \coprod_{i\in I} M$ die i-te Injektion. Dann gilt

$$1_R = \sum_{j\in J} f(q_j(m_j)) = \mathfrak{R}\Big(\sum_{j\in J} m_j \otimes (f \circ q_j)\Big) \in \mathfrak{R}(M \otimes_S N)$$

und $\mathfrak{R}$ ist surjektiv. □

Satz III.6.35 (Morita)**.** *Für Ringe R und S sind äquivalent:*

(1) ${}_R\mathbf{Mod} \approx {}_S\mathbf{Mod}$.

(2) Es existiert ein R-Progenerator M mit $\mathrm{End}_R(M) \cong S^o$.

(3) Es gibt einen R-S-Bimodul M und einen S-R-Bimodul N mit $R \simeq M \otimes_S N$ und $S \simeq N \otimes_R M$ als Bimoduln.

Gegebenenfalls nennt man R und S Morita-äquivalent.

Beweis.

(1) ⇒ (2): Sei $\Psi\colon {}_S\mathbf{Mod} \to {}_R\mathbf{Mod}$ eine Äquivalenz. Nach Beispiel III.6.29 ist $M := \Psi(S)$ ein R-Progenerator. Nach Lemma II.7.20 ist $S^o \cong \mathrm{End}_S(S)$. Nach Lemma III.5.23 und Lemma III.6.3 ist $\Psi\colon \mathrm{End}_S(S) \to \mathrm{End}_R(M)$ ein Ringisomorphismus.

(2) ⇒ (3): Nach Beispiel III.6.33 ist $(R, S, M, N, \mathfrak{R}, \mathfrak{S})$ ein Morita-Kontext mit $N = \mathrm{Hom}_R(M, R)$. Nach Satz III.6.34, Satz III.6.31 und Bemerkung III.6.32 sind $\mathfrak{R}$ und $\mathfrak{S}$ die gesuchten Isomorphismen.

(3) ⇒ (1): Seien $\varphi\colon M \otimes_S N \to R$ und $\psi\colon N \otimes_R M \to S$ Isomorphismen von Bimoduln. Wir definieren $\Phi\colon {}_R\mathbf{Mod} \to {}_S\mathbf{Mod}$, $A \mapsto N \otimes_R A$ mit $\Phi(f) := \mathrm{id}_N \otimes f$ für $f \in \mathrm{Hom}_R(A, B)$. Nach Bemerkung III.6.20 ist Φ ein Funktor. Analog ist $\Psi\colon {}_S\mathbf{Mod} \to {}_R\mathbf{Mod}$, $A \mapsto M \otimes_S A$ mit $\Psi(f) := \mathrm{id}_M \otimes f$ ein Funktor. Für jeden R-Modul A gilt

$$\Psi\Phi(A) = M \otimes_S \Phi(A) \overset{III.6.21}{\simeq} M \otimes_S N \otimes_R A \simeq R \otimes_R A \overset{III.6.18}{\simeq} A.$$

Sei $\alpha_A\colon \Psi\Phi(A) \to A$, $m \otimes n \otimes a \mapsto \varphi(m \otimes n)a$ ein entsprechender R-Isomorphismus. Für $f \in \mathrm{Hom}_R(A, B)$, $a \in A$, $m \in M$ und $n \in N$ gilt

$$\begin{aligned}\big(\alpha_B \circ \Psi\Phi(f)\big)(m \otimes n \otimes a) &= \alpha_B\big(m \otimes \Phi(f)(n \otimes a)\big) = \alpha_A\big(m \otimes n \otimes f(a)\big)\\ &= \varphi(m \otimes n)f(a) = f(\varphi(m \otimes n)a) = (f \circ \alpha_A)(m \otimes n \otimes a).\end{aligned}$$

Somit ist $\alpha\colon \Psi\Phi \Rightarrow \mathrm{id}$ ein natürlicher Isomorphismus. Analog zeigt man, dass $\beta_A\colon \Phi\Psi(A) \to A$, $n \otimes m \otimes a \mapsto \psi(n \otimes m)a$ einen natürlichen Isomorphismus $\beta\colon \Phi\Psi \Rightarrow \mathrm{id}$ definiert. □

Beispiel III.6.36.

(i) Für jeden Ring R und $n \in \mathbb{N}$ ist R^n ein Progenerator mit $\mathrm{End}_R(R^n)^o \cong R^{n\times n}$ (Lemma II.7.20). Daher sind R und $R^{n\times n}$ Morita-äquivalent.

(ii) Sei R halbeinfach und $M_1, \ldots, M_k$ ein Repräsentantensystem für die nicht-isomorphen einfachen R-Moduln. Dann ist $M = M_1 \times \ldots \times M_k$ ein Progenerator mit $\mathrm{End}_R(M)^o \cong Q_1 \times \ldots \times Q_k$ für die Schiefkörper $Q_i := \mathrm{End}_R(M_i)^o$. Also sind R und $Q_1 \times \ldots \times Q_k$ Morita-äquivalent.

(iii) Seien R und S Morita-äquivalente lokale Ringe. Sei M ein R-Progenerator mit $S \cong \mathrm{End}_R(M)^o$. Da der reguläre R-Modul unzerlegbar, ist M frei, sagen wir $M = R^n$ mit $n \in \mathbb{N}$. Nun ist $S \cong \mathrm{End}_R(R^n)^o \cong R^{n\times n}$. Für $n > 1$ ist $R^{n\times n} \simeq R^{n\times 1} \times \ldots \times R^{n\times 1}$ aber nicht lokal. Dies zeigt $n = 1$ und $S \cong \mathrm{End}_R(R)^o \cong R$.

Satz III.6.37. *Für Ringe R und S gilt*

(i) ${}_R\mathbf{Mod} \approx {}_S\mathbf{Mod} \iff {}_{R^o}\mathbf{Mod} \approx {}_{S^o}\mathbf{Mod} \iff \mathbf{Mod}_R \approx \mathbf{Mod}_S \iff {}_R\mathbf{mod} \approx {}_S\mathbf{mod}$.

(ii) $R \cong S \implies {}_R\mathbf{Mod} \cong {}_S\mathbf{Mod} \implies {}_R\mathbf{Mod} \approx {}_S\mathbf{Mod} \implies \mathrm{Z}(R) \cong \mathrm{Z}(S)$.

Beweis.

(i) Ist ${}_R\mathbf{Mod} \approx {}_S\mathbf{Mod}$, so existiert nach Morita ein R-Progenerator M und man erhält den Morita-Kontext $(R, S, M, N, \mathfrak{R}, \mathfrak{S})$ aus Beispiel III.6.33. Nach Satz III.6.31 ist der S-Rechtsmodul M ein Progenerator. Daher ist M als S^o-Linksmodul ebenfalls ein Progenerator. Für diesen gilt $\mathrm{End}_{S^o}(M) = \mathrm{End}_S(M) \cong R$ nach Satz III.6.31. Nach Morita folgt ${}_{R^o}\mathbf{Mod} \approx {}_{S^o}\mathbf{Mod}$. Dies ist bekanntlich zu $\mathbf{Mod}_R \approx \mathbf{Mod}_S$ äquivalent. Sei nun $\Phi\colon {}_R\mathbf{Mod} \to {}_S\mathbf{Mod}$ eine Äquivalenz. Nach Satz III.6.6 liefert die Einschränkung von Φ eine Äquivalenz ${}_R\mathbf{mod} \to {}_S\mathbf{mod}$. Sei umgekehrt eine Äquivalenz $\Psi\colon {}_S\mathbf{mod} \to {}_R\mathbf{mod}$ gegeben. Dann ist $M := \Psi(R)$ endlich erzeugt und projektiv als Objekt von ${}_R\mathbf{mod}$. Man prüft leicht, dass Satz II.12.13 in ${}_R\mathbf{mod}$ richtig bleibt. Daher ist M ein direkter Summand eines (endlich erzeugten) freien Moduln. Also ist M auch projektiv in ${}_R\mathbf{Mod}$. Auf die gleiche Weise sieht man mit Lemma III.6.27, dass M ein R-Generator ist. Außerdem ist $\mathrm{End}_R(M) \cong \mathrm{End}_S(S) \cong S^o$ nach Lemma III.6.3. Nach Morita sind R und S Morita-äquivalent.

(ii) Sei $\varphi\colon R \to S$ ein Ringisomorphismus. Jeder R-Modul M wird durch $s \cdot m := \varphi^{-1}(s)m$ für $s \in S$ und $m \in M$ zu einem S-Modul. Ein R-Homomorphismus ist auf diese Weise auch ein S-Homomorphismus. Der identische Funktor ${}_R\mathbf{Mod} \to {}_S\mathbf{Mod}$ ist also ein Isomorphismus. Aus ${}_R\mathbf{Mod} \cong {}_S\mathbf{Mod}$ folgt bekanntlich ${}_R\mathbf{Mod} \approx {}_S\mathbf{Mod}$.

Nehmen wir nun ${}_R\mathbf{Mod} \approx {}_S\mathbf{Mod}$. Wie im Beweis von Satz III.6.35 existiert ein Morita-Kontext $(R, S, M, N, \mathfrak{R}, \mathfrak{S})$ mit Isomorphismen $\mathfrak{R}$ und $\mathfrak{S}$. Satz III.6.31 liefert $\mathrm{Z}(R) \cong \mathrm{Z}(\mathrm{End}_S(M))$. Angewendet auf den Morita-Kontext $(S, R, N, M, \mathfrak{S}, \mathfrak{R})$ liefert der Satz auch $\mathrm{Z}(S) \cong \mathrm{Z}(S^o) \cong \mathrm{Z}(\mathrm{End}_S(M))$. Daher gilt $\mathrm{Z}(R) \cong \mathrm{Z}(S)$. □

Folgerung III.6.38. *Kommutative Ringe sind genau dann Morita-äquivalent, wenn sie isomorph sind.*

Beispiel III.6.39.

(i) Nach Aufgabe II.38 existiert ein noetherscher Ring R, sodass R^o nicht noethersch ist. Nach Satz III.6.9 gilt ${}_R\mathbf{Mod} \not\approx {}_{R^o}\mathbf{Mod}$.

(ii) Für einen Ring $R \neq 0$ hat die duale Kategorie $({}_R\mathbf{Mod})^o$ in der Regel keinen Bezug zu Moduln. Nehmen wir zum Beispiel an es existiert ein Ring S und eine Äquivalenz $\Phi\colon {}_S\mathbf{Mod} \to ({}_R\mathbf{Mod})^o$. Sei $P := \times_{i\in\mathbb{N}} S$ das Produkt und $Q := \coprod_{i\in\mathbb{N}} S$ das Koprodukt von abzählbar vielen Kopien von S. Dann wird der kanonische Monomorphismus $f\colon Q \to P$ auf einen Monomorphismus $\Phi(f)\colon \Phi(Q) \to \Phi(P)$ abgebildet. Dabei ist $\Phi(Q)$ ein Koprodukt und $\Phi(P)$ ein Produkt. In ${}_R\mathbf{Mod}$ erhält man einen Epimorphismus $\Phi(P) \to \Phi(Q)$, wobei $\Phi(P)$ nun ein Koprodukt und $\Phi(Q)$ ein Produkt von abzählbar vielen Kopien von $\Phi(S)$ ist (vgl. Lemma III.6.2). Mit S ist $\Phi(S)$ endlich erzeugt. Ist nun R abzählbar (z. B. $R = \mathbb{Z}$), so auch $\Phi(P)$. Andererseits ist $\Phi(Q)$ stets überabzählbar. Daher kann kein Epimorphismus $\Phi(P) \to \Phi(Q)$ existieren. [3]

Satz III.6.40. *Endlich-dimensionale K-Algebren sind genau dann Morita-äquivalent, wenn ihre Basisalgebren isomorph sind.*

Beweis. Seien A und B endlich-dimensionale Morita-äquivalente K-Algebren. Seien $P_1, \ldots, P_k$ die projektiv-unzerlegbaren A-Moduln bis auf Isomorphie. Dann ist $P := P_1 \times \ldots \times P_k$ ein Progenerator und A ist Morita-äquivalent zur Basisalgebra $A^b = \mathrm{End}_A(P)^o$. Wir können daher $A = A^b$ und $B = B^b$ annehmen. Sei M ein beliebiger A-Progenerator mit $B \cong \mathrm{End}_A(M)^o$. Da M projektiv ist, gilt $M \simeq P_1^{a_1} \times \ldots \times P_k^{a_k}$ mit $a_1, \ldots, a_k \in \mathbb{N}_0$. Da M ein Generator ist, gilt $a_1, \ldots, a_k \geq 1$. Also ist $A \simeq P_1 \times \ldots \times P_k$ ein direkter Summand von M und $A \cong \mathrm{End}_A(A)^o$ eine Unteralgebra von $\mathrm{End}_A(M)^o$. Dies zeigt $\dim B \geq \dim A$. Aus Symmetriegründen gilt auch $\dim A \geq \dim B$ und $A \cong B$. □

Beispiel III.6.41. Für endliche Gruppen G und H gilt ${}_{\mathbb{C}G}\mathbf{Mod} \approx {}_{\mathbb{C}H}\mathbf{Mod} \iff k(G) = k(H)$ (Bemerkung II.12.43). Die Bijektion $G \to G$, $g \mapsto g^{-1}$ setzt sich zu einem Ringisomorphismus $KG \to (KG)^o$ fort. Daher gilt ${}_{KG}\mathbf{Mod} \cong \mathbf{Mod}_{KG}$.

Bemerkung III.6.42. Seien A und B Morita-äquivalente K-Algebren und M ein A-Progenerator mit $B \cong \mathrm{End}_A(M)^o$. Wie im Beweis von Satz III.6.35 erhält man eine Äquivalenz $\Psi\colon {}_B\mathbf{Mod} \to {}_A\mathbf{Mod}$, $L \mapsto M \otimes_B L$. Mit $d := \dim M$ gilt also $\dim \Psi(L) = d \dim L$ für alle B-Moduln L. Nach Satz III.6.6 sind die Dimensionen der einfachen A-Moduln proportional zu den Dimensionen der einfachen B-Moduln. Außerdem haben A und B die gleiche Cartan-Matrix (bei geeigneter Anordnung) nach Satz II.12.24.

[3] Es gibt jedoch Ringe, in denen ein solcher Epimorphismus existiert: Mit Aufgabe III.28 kann man wie in Beispiel II.9.6 Ringe mit $R \simeq \times_{i\in\mathbb{N}} R$ konstruieren.

7 Zentral-einfache Algebren

Bemerkung III.7.1. Für jeden artinschen Ring R ist $R/\mathrm{J}(R)$ halbeinfach (Lemma II.8.13). Nach Artin-Wedderburn ist jeder halbeinfache Ring ein direktes Produkt von einfachen Ringen. Jeder einfache artinsche Ring S ist eine endlich-dimensionale $\mathrm{Z}(S)$-Algebra (Lemma II.12.5). In diesem Kapitel klassifizieren wir einfache Algebren mit vorgegebenem Zentrum. Die Menge der Morita-Äquivalenzklassen dieser Algebren erhält durch das Tensorprodukt eine Gruppenstruktur, deren Isomorphietyp wir in Beispielen ausrechnen. Wie früher betrachten wir stets endlich-dimensionale Algebren über einem Körper K.

Definition III.7.2. Eine K-Algebra A heißt *zentral*, falls $\mathrm{Z}(A) = K1_A$ gilt. Ist A als Ring zusätzlich einfach (d. h. 0 und $A \neq 0$ sind die einzige Ideale in A), so nennt man A *zentral-einfach*.

Bemerkung III.7.3. Sei A zentral-einfach.

(i) Nach Artin-Wedderburn existiert eine Divisionsalgebra D und $n \in \mathbb{N}$ mit $A \cong D^{n\times n}$ (vgl. Bemerkung II.8.14 und Bemerkung II.12.3). Nach Beispiel II.12.22 ist D die Basisalgebra von A. Nach Lemma II.12.5 gilt $K \cong \mathrm{Z}(A) \cong \mathrm{Z}(D^{n\times n}) \cong \mathrm{Z}(D)$. Daher ist auch D eine zentral-einfache Algebra.

(ii) Ist D eine Divisionsalgebra, so ist $D^{n\times n}$ für $n \in \mathbb{N}$ eine zentral-einfache $\mathrm{Z}(D)$-Algebra. Insbesondere ist jede einfache Algebra B eine zentral-einfache $\mathrm{Z}(B)$-Algebra.

(iii) Ist die K-Algebra B Morita-äquivalent zu A, so ist auch B zentral-einfach nach Satz III.6.9 und Satz III.6.37.

Definition III.7.4. Seien A und B Algebren mit Basen $a_1, \ldots, a_n$ bzw. $b_1, \ldots, b_m$ über K. Wir kennen bereits das Tensorprodukt $A \otimes B = A \otimes_K B$ als K-Vektorraum mit Basis $\{a_i \otimes b_j : 1 \leq i \leq n, 1 \leq j \leq m\}$. Durch

$$(a_i \otimes b_j)(a_r \otimes b_s) := a_i a_r \otimes b_j b_s$$

(und lineare Fortsetzung) wird $A \otimes B$ zu einer K-Algebra. Man nennt $A \otimes B$ das *Tensorprodukt* von A und B.

Bemerkung III.7.5.

(i) Für $a = \sum_{i=1}^n \alpha_i a_i$, $b = \sum_{j=1}^m \beta_j b_j$, $c = \sum_{r=1}^n \gamma_r a_r$ und $d = \sum_{s=1}^m \delta_s b_s$ gilt

$$\begin{aligned}(a \otimes b)(c \otimes d) &= \Big(\sum_{i,j} \alpha_i\beta_j(a_i \otimes b_j)\Big)\Big(\sum_{r,s} \gamma_r\delta_s(a_r \otimes b_s)\Big)\\ &= \sum_{i,j,r,s} \alpha_i\beta_j\gamma_r\delta_s(a_i a_r \otimes b_j b_s) = ac \otimes bd.\end{aligned}$$

(ii) Die *universelle Eigenschaft* für Tensorprodukte von Algebren lautet: Für jede bilineare Abbildung $f\colon A \times B \to C$ mit $f(1,1) = 1$ und $f(a,b)f(c,d) = f(ac,bd)$ für alle $(a,b),(c,d) \in A \times B$ existiert genau ein Homomorphismus $\hat{f}\colon A \otimes B \to C$ von Algebren mit $\hat{f}(a \otimes b) = f(a,b)$ für $(a,b) \in A \times B$.

(iii) Für K-Algebren A, B, C gibt es (wie in Bemerkung III.3.18) kanonische Isomorphismen von Algebren:

$$K \otimes A \cong A, \qquad (A \otimes B) \otimes C \cong A \otimes (B \otimes C),$$
$$A \otimes B \cong B \otimes A, \qquad (A \times B) \otimes C \cong (A \otimes C) \times (B \otimes C).$$

(iv) Jeder A-B-Bimodul M wird durch $(a \otimes b)m := amb$ zu einem $A \otimes B^o$-Linksmodul (man definiere zunächst $(a_i \otimes b_j)m$ und setze anschließend linear fort). Auf die gleiche Weise wird jeder $A \otimes B^o$-Linksmodul zu einem A-B-Bimodul.

Beispiel III.7.6. Für endliche Gruppen G und H gilt $K[G \times H] \cong KG \otimes KH$.

Lemma III.7.7. *Für K-Algebren A und B gilt* $\mathrm{Z}(A \otimes B) = \mathrm{Z}(A) \otimes \mathrm{Z}(B)$.

Beweis. Sicher ist $\mathrm{Z}(A) \otimes \mathrm{Z}(B) \subseteq \mathrm{Z}(A \otimes B)$. Sei $A = \mathrm{Z}(A) \oplus A_1$ eine Zerlegung in Untervektorräume und $z \in \mathrm{Z}(A \otimes B)$. Wir schreiben $z = x + y$ mit $x \in \mathrm{Z}(A) \otimes B$ und $y \in A_1 \otimes B$. Für $a \in A$ ist $a \otimes 1$ sowohl mit z als auch mit x vertauschbar. Daher ist $a \otimes 1$ auch mit y vertauschbar. Sei $b_1, \ldots, b_m$ eine Basis von B und $y = \sum_{i=1}^m a_i \otimes b_i$ mit $a_i \in A$. Wegen

$$\sum_{i=1}^m a_i a \otimes b_i = y(a \otimes 1) = (a \otimes 1)y = \sum_{i=1}^m a_i a \otimes b_i$$

gilt $a_i a = a a_i$ für $i = 1, \ldots, m$. Da $a \in A$ beliebig war, gilt $a_i \in \mathrm{Z}(A)$ für $i = 1, \ldots, m$. Dies zeigt $y \in (A_1 \otimes B) \cap (\mathrm{Z}(A) \otimes B) = 0$ und $\mathrm{Z}(A \otimes B) \subseteq \mathrm{Z}(A) \otimes B$. Wir können nun analog $B = \mathrm{Z}(B) \oplus B_1$ zerlegen und schreiben $z = x + y$ mit $x \in \mathrm{Z}(A) \otimes \mathrm{Z}(B)$ sowie $y \in \mathrm{Z}(A) \otimes B_1$. Dann ist y mit $1 \otimes b$ ($b \in B$) vertauschbar und man erhält leicht $y = 0$. Insgesamt ist $\mathrm{Z}(A \otimes B) \subseteq \mathrm{Z}(A) \otimes \mathrm{Z}(B)$. □

Bemerkung III.7.8. Man vergleiche das nächste Lemma mit Lemma II.12.26.

Lemma III.7.9. *Für K-Algebren A, B und $n, m \in \mathbb{N}$ gilt* $\boxed{A^{n\times n} \otimes B^{m\times m} \cong (A \otimes B)^{nm\times nm}.}$

Beweis. Für $a = (a_{ij})_{i,j} \in A^{n\times n}$ und $b = (b_{rs})_{r,s} \in B^{m\times m}$ definieren wir $a_{ij} \otimes b := (a_{ij} \otimes b_{rs})_{r,s} \in (A \otimes B)^{m\times m}$ und $a \otimes b := (a_{ij} \otimes b)_{i,j} \in (A \otimes B)^{nm\times nm}$ ähnlich dem Kronecker-Produkt. Dies liefert eine bilineare Abbildung

$$f\colon A^{n\times n} \times B^{m\times m} \to (A \otimes B)^{nm\times nm},$$
$$(a,b) \mapsto a \otimes b$$

mit $f(1_n, 1_m) = 1_{nm}$ und

$$f(a,b)f(c,d) = (a \otimes b)(c \otimes d) = \Big(\sum_{k=1}^n (a_{ik} \otimes b)(c_{kj} \otimes d)\Big)_{i,j}$$
$$= \Big(\Big(\sum_{k=1}^n a_{ik}c_{kj}\Big) \otimes bd\Big)_{i,j} = ac \otimes bd = f(ac,bd).$$

Nach der universellen Eigenschaft erhält man einen Homomorphismus von Algebren $\hat{f}\colon A^{n\times n}\otimes B^{m\times m}\to (A\otimes B)^{nm\times nm}$. Wählt man Basen $a_1,\dots,a_r$ von A und $b_1,\dots,b_s$ von B, so bilden die Matrizen a_iE_{kl} bzw. b_iE_{kl} Basen von $A^{n\times n}$ bzw. $B^{m\times m}$ (wie üblich sei $E_{kl}=(\delta_{ik}\delta_{jl})_{i,j}$). Außerdem bilden

$$\hat{f}(a_iE_{kl}\otimes b_jE_{pq})=(a_i\otimes b_j)E_{(k-1)m+p,(l-1)m+p}$$

eine K-Basis von $(A\otimes B)^{nm\times nm}$. Also ist $\hat{f}$ bijektiv. □

Lemma III.7.10. *Sei A eine einfache Algebra und B eine zentral-einfache Algebra. Dann ist $A\otimes B$ einfach.*

Beweis. Nach Bemerkung III.7.3 existieren Divisionsalgebren D_A und D_B und $n,m\in\mathbb{N}$ mit $A\cong D_A^{n\times n}$ sowie $B\cong D_B^{m\times m}$. Dabei ist $\mathrm{Z}(D_B)\cong\mathrm{Z}(D_B^{m\times m})\cong\mathrm{Z}(B)\cong K$. Mit Lemma III.7.9 folgt

$$A\otimes B\cong(D_A\otimes D_B)^{nm\times nm}.$$

Wir werden zeigen, dass $D_A\times D_B$ einfach ist, denn dann existiert eine Divisionsalgebra D und $k\in\mathbb{N}$ mit $D_A\otimes D_B\cong D^{k\times k}$ und

$$A\otimes B\cong D^{knm\times knm}$$

nach Lemma II.12.26. Wir können also $A=D_A$ und $B=D_B$ annehmen.

Sei $a_1,\dots,a_n$ eine K-Basis von A und $0\neq I\trianglelefteq A\otimes B$. Wähle $x\in I\setminus\{0\}$, sodass in der eindeutigen Darstellung $x=\sum_{i=1}^n a_i\otimes b_i$ möglichst viele der b_i verschwinden. O. B. d. A. sei $b_1\neq 0$. Nach Multiplikation mit $1\otimes b_1^{-1}$ können wir $b_1=1$ annehmen (beachte: $B=D_B$ ist eine Divisionsalgebra). Für alle $b\in B$ gilt dann

$$I\ni(1\otimes b)x-x(1\otimes b)=\sum_{i=2}^n a_i\otimes(bb_i-b_ib).$$

Die Wahl von x zeigt $bb_i=b_ib$, d. h. $b_i\in\mathrm{Z}(B)=K1_B$. Daher ist $x=\left(\sum_{i=1}^n b_ia_i\right)\otimes 1$. Insbesondere ist $J:=\{a\in A: a\otimes 1\in I\}$ ein nicht-triviales Ideal in A. Da A einfach ist, gilt $1\in J$ und daher $1=1\otimes 1\in I$. □

Beispiel III.7.11. Das Tensorprodukt von beliebigen einfachen Algebren muss nicht einfach sein: Als Körper ist $\mathbb{C}$ eine einfache $\mathbb{R}$-Algebra. Sei $x:=\mathrm{i}\otimes 1\in\mathbb{C}\otimes\mathbb{C}$ und $y:=1\otimes\mathrm{i}\in\mathbb{C}\otimes\mathbb{C}$. Wir definieren eine lineare Abbildung $f\colon\mathbb{C}\otimes\mathbb{C}\to\mathbb{C}\oplus\mathbb{C}$ durch $f(1\otimes 1):=(1,1)$, $f(x)=(\mathrm{i},\mathrm{i})$, $f(y)=(\mathrm{i},-\mathrm{i})$ und $f(xy)=f(x)f(y)=(-1,1)$. Wegen $f(x^2)=f(-1\otimes 1)=(-1,-1)=f(x)^2$ und $f(y^2)=f(y)^2$ ist f ein Isomorphismus von Algebren, d. h. $\mathbb{C}\otimes_{\mathbb{R}}\mathbb{C}\cong\mathbb{C}\times\mathbb{C}$. Offensichtlich ist $\mathbb{C}\times\mathbb{C}$ nicht einfach.

Satz III.7.12. *Sind A und B zentral-einfache Algebren, so auch $A\otimes B$.*

Beweis. Folgt aus Lemma III.7.7 und Lemma III.7.10. □

Satz III.7.13. *Eine Algebra A ist genau dann zentral-einfach, wenn die Abbildung $F\colon A\otimes A^o\to\mathrm{End}_K(A)$ mit $F(a\otimes b)(x):=axb$ ein Isomorphismus von Algebren ist.*

Beweis. Für $a, b \in A$ ist $f_{a,b}\colon A \to A$, $x \mapsto axb$ ein K-Endomorphismus mit $f_{1,1} = \mathrm{id}_A$ und $f_{aa',b'b} = f_{a,b} \circ f_{a',b'}$. Nach den Axiomen für Algebren ist die Abbildung $f\colon A \times A^o \to \mathrm{End}_K(A)$, $(a,b) \mapsto f_{a,b}$ bilinear mit $f((a,b)(a',b')) = f(aa',b'b) = f(a,b)f(a',b')$. Nach der universellen Eigenschaft ist F ein Homomorphismus von Algebren.

Sei nun A zentral-einfach. Nach Satz III.7.12 ist $A \otimes A^o$ einfach und daher $\mathrm{Ker}(F) = 0$. Wegen $\dim A \otimes A^o = \dim(A)^2 = \dim \mathrm{End}_K(A)$ ist F ein Isomorphismus. Sei umgekehrt F ein Isomorphismus. Dann ist $A \otimes A^o \cong \mathrm{End}_K(A) \cong K^{n\times n}$ zentral-einfach. Wegen $\mathrm{Z}(A) \otimes \mathrm{Z}(A) \cong \mathrm{Z}(A \otimes A^o) \cong \mathrm{Z}(K)$ ist auch $\mathrm{Z}(A) \cong K$. Für $0 \neq I \trianglelefteq A$ ist $0 \neq I \otimes A^o \trianglelefteq A \otimes A^o$. Da $A \otimes A^o$ einfach ist, folgt $\dim(I)\dim(A) = \dim(I \otimes A^o) = \dim(A \otimes A^o) = \dim^2(A)$ und $I = A$. Also ist A einfach. □

Definition III.7.14. Sei $[A]$ die Morita-Äquivalenzklasse einer zentral-einfachen K-Algebra A. Sei $\mathrm{Br}(K) := \big\{[A] : A \text{ zentral-einfach}\big\}$.

Bemerkung III.7.15. Nach Bemerkung III.7.3 enthält $[A]$ genau eine Divisionsalgebra bis auf Isomorphie.

Satz III.7.16. *Durch*

$$[A] \cdot [B] := [A \otimes B]$$

wird $\mathrm{Br}(K)$ *zu einer abelschen Gruppe. Man nennt* $\mathrm{Br}(K)$ *die* Brauergruppe *von* K*.*

Beweis. Seien D, D_A, D_B Divisionsalgebren mit $A \cong D_A^{n\times n}$, $B \cong D_B^{m\times m}$ und $D_A \times D_B \cong D^{k\times k}$. Wie in Lemma III.7.10 ist $A \otimes B \cong D^{nmk\times nmk}$. Daraus folgt leicht, dass $[A] \cdot [B]$ nicht von der Wahl der Repräsentanten A und B abhängt. Nach Satz III.7.12 und Bemerkung III.7.5 ist $\cdot$ wohldefiniert, assoziativ, kommutativ und $[K]$ ist ein neutrales Element. Nach Satz III.7.13 ist $[A]\cdot[A^o] = [\mathrm{End}_K(A)] = [K^{n\times n}] = [K]$. Also ist $[A^o]$ das Inverse zu $[A]$. □

Beispiel III.7.17.

(i) Für jeden algebraisch abgeschlossenen Körper K ist $\mathrm{Br}(K) = 1$ nach Lemma II.12.6. In dieser Situation ist auch $\mathrm{Br}(K(X)) = 1$ nach einem Satz von Tsen.

(ii) Ist K endlich, so auch jede (endlich-dimensionale) Divisionsalgebra über K nach Wedderburn (Satz II.8.7). Daher gilt auch hier $\mathrm{Br}(K) = 1$.

Satz III.7.18 (Skolem-Noether)**.** *Sei A zentral-einfach und B einfach. Dann existiert für alle Homomorphismen $f, g\colon B \to A$ ein $a \in A^\times$ mit $f(x) = ag(x)a^{-1}$ für alle $x \in B$.*

Beweis. Wir betrachten $M_f := A$ als $A \otimes B^o$-Modul (oder A-B-Bimodul) via

$$(a \otimes b)m := amf(b) \qquad (a \in A, b \in B, m \in M).$$

Nach Lemma III.7.10 ist $A \otimes B^o$ einfach. Insbesondere besitzt $A \otimes B^o$ nur einen einfachen Modul S bis auf Isomorphie. Daher ist $M_f \simeq S^k$ für ein $k \in \mathbb{N}$. Analog ist auch M_g ein $A \otimes B^o$-Modul der gleichen Dimension. Daher ist $M_f \simeq S^k \simeq M_g$. Sei $\varphi\colon M_f \to M_g$ ein Isomorphismus. Für $a := \varphi(1)$ und $x \in B$ gilt dann

$$ag(x) = (1 \otimes x)\varphi(1) = \varphi((1 \otimes x)1) = \varphi(f(x)) = \varphi((f(x) \otimes 1)1) = (f(x) \otimes 1)\varphi(1) = f(x)a.$$

Für $y := \varphi^{-1}(1) \in A$ gilt $ya = (y \otimes 1)\varphi(1) = \varphi((y \otimes 1)1) = \varphi(y) = 1 = \ldots = ay$. Daher ist $a \in A^\times$. □

Beispiel III.7.19. Für $A = B = K^{n\times n}$ und $g = \mathrm{id}_A$ erhält man, dass $K^{n\times n}$ nur innere Automorphismen besitzt (Aufgabe II.60).

Satz III.7.20 (Doppel-Zentralisator-Satz)**.** *Sei A eine zentral-einfache K-Algebra und $B \subseteq A$ eine einfache Unteralgebra. Dann gilt*

(i) Der Zentralisator $C := \mathrm{C}_A(B) := \{a \in A : \forall b \in B : ab = ba\}$ ist eine einfache Algebra.

(ii) Ist D eine Divisionsalgebra mit $C \cong D^{k\times k}$, so gilt $A \otimes B^o \cong D^{n\times n}$ mit $k \mid n$.

(iii) $\dim A = \dim(B)\dim(C)$.

(iv) $\mathrm{C}_A(C) = B$.

Beweis.

(i) Offenbar ist C eine Algebra. Wie im Beweis von Skolem-Noether betrachten wir $M := A$ als Modul der einfachen Algebra $A \otimes B^o$ mittels $(a \otimes b)m := amb$ für $m \in M$, $a \in A$ und $b \in B$. Sei S der einfache $A \otimes B^o$-Modul und $A \otimes B^o \simeq S^n$ der reguläre Modul. Für die Divisionsalgebra $D := \mathrm{End}_{A\otimes B^o}(S)$ (Schurs Lemma) gilt $(A \otimes B^o)^o \cong D^{n\times n}$. Sei $M \simeq S^k$ und $E := \mathrm{End}_{A\otimes B^o}(M) \cong D^{k\times k}$. Sei $\varphi \in E$ und $a := \varphi(1)$. Für $b \in B$ gilt dann

$$ab = (1 \otimes b)\varphi(1) = \varphi((1 \otimes b)1) = \varphi((b \otimes 1)1) = (b \otimes 1)\varphi(1) = ba,$$

d. h. $a \in C$. Dies liefert einen Algebren Homomorphismus $F\colon E \to C^o$, $\varphi \mapsto \varphi(1)$ (beachte $(\varphi\psi)(1) = \varphi(\psi(1)1) = \psi(1)\varphi(1)$). Da φ durch $\varphi(1)$ eindeutig bestimmt ist, ist F injektiv. Für jedes $c \in C$ ist umgekehrt die Abbildung $\varphi\colon M \to M$, $m \mapsto mc$ ein Element von E, denn

$$\varphi((a \otimes b)m) = \varphi(amb) = ambc = amcb = (a \otimes b)mc = (a \otimes b)\varphi(m).$$

Also ist F auch surjektiv. Folglich ist $C \cong E^o$ einfach.

(ii) Es gilt $C \cong E^o \cong (D^o)^{k\times k}$ und $A \otimes B^o \cong (D^o)^{n\times n}$. Wegen $k\dim(A)\dim(B) = kn^2\dim(D) = nk\dim(S) = n\dim(M_f) = n\dim(A)$ ist $k \mid n$.

(iii) Nun gilt

$$\begin{aligned}\dim(A)\dim(B)\dim(C) &= \dim(A \otimes B^o)\dim(E) = (nk\dim(D))^2\\ &= \dim(k\dim(S))^2 = \dim(M_f)^2 = \dim(A)^2.\end{aligned}$$

(iv) Da C einfach ist, können wir B durch C ersetzen und erhalten

$$\dim(C)\dim(\mathrm{C}_A(C)) = \dim(A) = \dim(C)\dim(B)$$

aus (iii). Wegen $B \subseteq \mathrm{C}_A(C)$ folgt $\mathrm{C}_A(C) = B$. □

Lemma III.7.21. *Ein Teilkörper L einer Divisionsalgebra D ist genau dann maximal, wenn $\mathrm{C}_D(L) = L$ gilt.*

Beweis. Im Fall $\mathrm{C}_D(L) = L$ ist L sicher maximal. Sei nun umgekehrt L maximal und $c \in \mathrm{C}_D(L)$. Dann ist auch $L(c)$ ein Teilkörper von D und es folgt $c \in L$. □

Satz III.7.22. *Sei L ein maximaler Teilkörper einer zentralen Divisionsalgebra D. Dann ist* $\dim D = \dim(L)^2$ *und* $L \otimes D \cong L^{n\times n}$ *mit* $n := \dim L$.

Beweis. Als Körper ist L eine einfache Unteralgebra von D und gleichzeitig eine Divisionsalgebra. Nach Lemma III.7.21 und dem Doppel-Zentralisator-Satz gilt $\dim D = \dim(L)\dim(\mathrm{C}_D(L)) = \dim(L)^2$ und $D \otimes L \cong D \otimes L^o \cong L^{n\times n}$. Dimensionsvergleich zeigt $n = \dim L$. □

Folgerung III.7.23. *Für jede zentral-einfache Algebra A ist* $\dim A$ *eine Quadratzahl.*

Beweis. Sei D eine zentrale Divisionsalgebra mit $A \cong D^{n\times n}$. Aus Dimensionsgründen existiert stets ein maximaler Teilkörper von D. Nach Satz III.7.22 ist $\dim D$ eine Quadratzahl und somit auch $\dim A = n^2 \dim D$. □

Satz III.7.24 (Frobenius)**.** *Jede $\mathbb{R}$-Divisionsalgebra ist zu $\mathbb{R}$, $\mathbb{C}$ oder $\mathbb{H}$ isomorph. Insbesondere ist* $\mathrm{Br}(\mathbb{R}) = \langle[\mathbb{H}]\rangle \cong C_2$.

Beweis. Sei D eine $\mathbb{R}$-Divisionsalgebra. Wir identifizieren $\mathbb{R}$ mit $\mathbb{R}1_D \subseteq D$ und nehmen $\mathbb{R} \neq D$ an. Sei $L \subseteq D$ ein maximaler Teilkörper und $x \in L$ ein primitives Element der separablen Körpererweiterung $\mathbb{R} \subseteq L$. Für das irreduzible Minimalpolynom $\mu \in \mathbb{R}[X]$ von x gilt bekanntlich $|L : \mathbb{R}| = |\mathbb{R}(x) : \mathbb{R}| = \deg \mu = 2$ nach dem Fundamentalsatz der Algebra. Sei $\mu = X^2 + aX + b$ mit $a, b \in \mathbb{R}$. Da μ irreduzibel ist, gilt $y := D_\mu = a^2 - 4b < 0$ und

$$L = \mathbb{R}(x) = \mathbb{R}(\sqrt{y}) = \mathbb{R}\Big(\frac{\sqrt{y}}{\sqrt{-y}}\Big) = \mathbb{R}(\sqrt{-1}) \cong \mathbb{C}.$$

Wir können daher $x^2 = -1$ annehmen. Im Fall $\mathrm{Z}(D) = L$ ist $D \cong \mathbb{C}$ nach Lemma II.12.6. Anderenfalls ist D zentral mit $\dim D = \dim(L)^2 = 4$ nach Satz III.7.22. Bekanntlich existiert $f \in \mathrm{Aut}(L)$ mit $f(x) = -x$. Wir können f zu $f\colon L \to D$ fortsetzen. Nach Skolem-Noether sind nun x und $-x$ in D konjugiert. Sei also $y \in D$ mit $yx = -xy$. Dann ist

$$y^2 \in \mathrm{C}_D(L) \cap \mathbb{R}(y) = L \cap \mathbb{R}(y) = \mathbb{R}$$

nach Lemma III.7.21. Im Fall $y^2 > 0$ wäre $y \in \mathbb{R} \subseteq L$, denn das Polynom $X^2 - y^2$ besitzt höchstens zwei Nullstellen in $\mathbb{R}(y)$. Nach Normierung können wir also $y^2 = -1$ annehmen. Wegen $y \notin L$ ist $1, x, y, xy$ eine $\mathbb{R}$-Basis von D und die Multiplikationstabelle ist eindeutig bestimmt. Dies zeigt $D \cong \mathbb{H}$. Da $\mathbb{C}$ als $\mathbb{R}$-Algebra nicht zentral ist, ist $[\mathbb{H}]$ das einzige nicht-triviale Element in $\mathrm{Br}(\mathbb{R})$. Es folgt $\mathrm{Br}(\mathbb{R}) = \langle[\mathbb{H}]\rangle \cong C_2$. □

Definition III.7.25. Für eine endliche Körpererweiterung $K \subseteq L$ und eine Algebra A sei $A_L := L \otimes A$. Durch

$$\lambda(x \otimes a) := (\lambda \otimes 1)(x \otimes a) = (\lambda x) \otimes a \qquad (\lambda, x \in L, a \in A)$$

wird A_L zu einer L-Algebra. Man sagt, A_L entsteht durch *Skalarerweiterung* aus A. Existiert ein Ringisomorphismus $A_L \cong L^{n\times n}$, so nennt man L einen *Zerfällungsköper* von A.

Bemerkung III.7.26.

(i) Wegen $A \cong A_K$ ist K genau dann ein Zerfällungskörper von A, wenn $[A] = 1$ gilt.

(ii) Ist $a_1, \ldots, a_n$ eine Basis von A, so ist $1 \otimes a_1, \ldots, 1 \otimes a_n$ eine L-Basis von A_L. Insbesondere ist $\dim A = \dim_L(A_L)$.

(iii) Sei $f\colon A_L \to L^{n\times n}$ ein Ringisomorphismus. Einschränken von f liefert einen Ringisomorphismus

$$L \otimes \mathrm{Z}(A) \cong \mathrm{Z}(A_L) \to \mathrm{Z}(L^{n\times n}) \cong L.$$

Insbesondere ist A_L zentral-einfach. Nach Skolem-Noether existiert für die Homomorphismen $f\colon \mathrm{Z}(A_L) \to L^{n\times n}$ und $g\colon \mathrm{Z}(A_L) \to L^{n\times n}$, $\lambda \otimes 1 \mapsto \lambda 1_n$ ein $a \in \mathrm{GL}(n, L)$ mit $f(x) = ag(x)a^{-1}$ für $x \in \mathrm{Z}(A_L)$. Wir können daher $f(\lambda \otimes 1) = \lambda 1_n$ für $\lambda \in L$ annehmen. Dann ist f auch ein Isomorphismus von L-Algebren.

(iv) Nach Satz III.7.22 besitzt jede zentrale Divisionsalgebra D einen Zerfällungskörper L, sagen wir $D_L \cong L^{n\times n}$. Wegen $L \otimes D^{k\times k} \overset{III.7.9}{\cong} D_L^{k\times k} \overset{II.12.26}{\cong} L^{nk\times nk}$ ist L auch ein Zerfällungskörper jeder zentral-einfachen Algebra mit Basisalgebra D.

(v) Mit L ist auch jede endliche Erweiterung M von L ein Zerfällungskörper von A, denn

$$A_M = M \otimes A \cong (M \otimes_L L) \otimes A \cong M \otimes_L A_L \cong M \otimes_L L^{n\times n} \cong (M \otimes_L L)^{n\times n} \cong M^{n\times n}.$$

Satz III.7.27. *Für jede endliche Körpererweiterung $K \subseteq L$ ist die Abbildung*

$$\Gamma\colon \mathrm{Br}(K) \to \mathrm{Br}(L), \qquad [A] \mapsto [A_L]$$

ein Homomorphismus. Man setzt $\mathrm{Br}(L|K) := \mathrm{Ker}(\Gamma)$.

Beweis. Sei A eine zentral-einfache K-Algebra. Nach Lemma III.7.10 ist A_L einfach und nach Lemma III.7.7 ist $\mathrm{Z}(A_L) \cong L \otimes \mathrm{Z}(A) \cong L \otimes K \cong L$. Also ist $[A_L] \in \mathrm{Br}(L)$. Sei $[A] = [B]$ mit $A \cong D^{n\times n}$ und $B \cong D^{m\times m}$ für eine Divisionsalgebra D. Dann ist $A_L = L \otimes D^{n\times n} \cong D_L^{n\times n}$ nach Lemma III.7.9. Wie bereits gezeigt, ist D_L eine einfache L-Algebra. Also existiert eine Divisionsalgebra E mit $D_L \cong E^{k\times k}$ und es folgt $A_L \cong E^{nk\times nk}$ sowie $B_L \cong E^{mk\times mk}$. Daher ist $[A_L] = [B_L]$ und Γ ist wohldefiniert. Für $[A], [B] \in \mathrm{Br}(K)$ gilt schließlich

$$(A \otimes B)_L = L \otimes A \otimes B \cong A \otimes (L \otimes_L L) \otimes B \cong (A \otimes L) \otimes_L (L \otimes B) \cong A_L \otimes_L B_L.$$

Dies zeigt $\Gamma([A][B]) = \Gamma([A \otimes B]) = [(A \otimes B)_L] = [A_L][B_L] = \Gamma([A])\Gamma([B])$. □

Bemerkung III.7.28. Offenbar besteht $\mathrm{Br}(L|K)$ genau aus den zentral-einfachen K-Algebren mit Zerfällungskörper L. Nach Bemerkung III.7.26 gilt daher

$$\mathrm{Br}(K) = \bigcup_{\substack{L\supseteq K,\\ |L:K|<\infty}} \mathrm{Br}(L|K).$$

Wir zeigen, dass es genügt über Galois-Erweiterungen von K zu vereinigen.

Beispiel III.7.29. Nach Satz III.7.22 ist $\mathbb{C}$ ein Zerfällungskörper von $\mathbb{H}$. Daher gilt $\mathrm{Br}(\mathbb{C}|\mathbb{R}) = \mathrm{Br}(\mathbb{R}) = \langle \mathbb{H} \rangle$ nach Satz III.7.24.

Satz III.7.30 (Noether-Jacobson)**.** *Jede zentrale Divisionsalgebra D besitzt einen maximalen Teilkörper L, sodass $K \subseteq L$ separabel ist.*

Beweis (Herstein). Wir argumentieren durch Induktion nach $\dim(D)$. Nach Beispiel II.3.3 können wir $\operatorname{char} K = p > 0$ und $D \neq K$ annehmen. Ist für jedes $x \in D$ der Körper $K(x)$ separabel über K, so folgt die Behauptung aus Satz III.7.22. Sei nun $x \in D \setminus K$ inseparabel mit Minimalpolynom μ. Wegen $\mu' = 0$ existiert ein irreduzibles Polynom $\nu \in K[X]$ mit $\mu(X) = \nu(X^p)$. Dann ist ν das Minimalpolynom von x^p. Ist auch x^p inseparabel, so können wir x^{p^2} betrachten usw. Am Ende erhalten wir ein inseparables Element $x \in D$, sodass x^p separabel ist. Nehmen wir $x^p \in K$ an und betrachten die Abbildung

$$\delta\colon D \to D, \qquad d \mapsto dx - xd.$$

Wegen $x \notin K = \mathrm{Z}(D)$, existiert ein $y \in D$ mit $\delta(y) \neq 0$. Sei $\delta_1, \delta_2 \in \operatorname{End}_K(D)$ mit $\delta_1(x) := dx$ und $\delta_2(x) := xd$. Dann gilt $\delta = \delta_1 - \delta_2$ in $\operatorname{End}_K(D)$. Wegen $\operatorname{char} K = p$ folgt $\delta^p = (\delta_1 - \delta_2)^p = \delta_1^p - \delta_2^p$. Insbesondere ist

$$\delta^p(y) = yx^p - x^p y = 0$$

wegen $x^p \in K$. Sei $m \in \mathbb{N}$ minimal mit $\delta^m(y) = 0$ und sei $z := \delta^{m-1}(y)$ sowie $w := \delta^{m-2}(y)$. Dann ist $z = \delta(w) = wx - xw$. Setze $u := x^{-1}z$. Wegen $\delta(z) = 0$ ist $ux = xu$. Es folgt

$$x = zu^{-1} = (wx - xw)u^{-1} = wxu^{-1} - xwu^{-1} = (wu^{-1})x - x(wu^{-1}).$$

Für $a := wu^{-1}$ gilt also $x = ax - xa$ und $a = 1 + xax^{-1}$. Wie zu Beginn des Beweises existiert eine Potenz $p^n = q$, sodass a^q separabel ist. Nun ist aber $a^q = 1 + xa^q x^{-1}$. Insbesondere sind x und a^q nicht vertauschbar und es folgt $a^q \notin K$. Damit haben wir eine separable Erweiterung $K \subsetneq K(a^q) =: M$ gefunden (Satz II.3.8).

Offenbar ist $C := \mathrm{C}_D(M)$ eine Divisionsalgebra und nach Satz III.7.20 ist $M \subseteq \mathrm{Z}(C) \subseteq \mathrm{C}_D(C) = M$. Also ist C zentral über M mit $\dim_M(C) < \dim_K(D)$. Nach Induktion besitzt C einen maximalen Teilkörper L, der separabel über M ist. Nach Lemma II.3.7 ist L dann auch separabel über K. Nun gilt

$$\dim D \overset{III.7.20}{=} \dim(M)\dim(C) \overset{I.9.5}{=} \dim_M(C)\dim(M)^2 \overset{III.7.22}{=} \dim_M(L)^2\dim(M)^2 \overset{I.9.5}{=} \dim(L)^2.$$

Nach Satz III.7.22 ist L also auch ein maximaler Teilkörper von D. □

Folgerung III.7.31. *Jede zentral-einfache Algebra besitzt einen Zerfällungskörper L, sodass $K \subseteq L$ eine Galois-Erweiterung ist.*

Beweis. Nach Bemerkung III.7.26 genügt es die Behauptung für zentrale Divisionsalgebren D zu beweisen. Nach Satz III.7.30 existiert ein maximaler Teilkörper $L \subseteq D$, sodass $K \subseteq L$ separabel ist. Nach Satz II.3.4 liegt $K \subseteq L$ in einer Galois-Erweiterung $K \subseteq M$. Nun ist auch M ein Zerfällungskörper von D. □

Definition III.7.32. In der Situation von Folgerung III.7.31 heißt L ein *Galois-Zerfällungskörper* von A.

Lemma III.7.33. *Sei L ein Zerfällungskörper einer zentralen Divisionsalgebra D. Dann ist L zu einem Teilkörper von $D^{n\times n}$ isomorph, wobei $\dim(L)^2 = n^2 \dim D$ gilt.*

Beweis. Sei $D_L \cong L^{k\times k}$ und sei $S \simeq L^{k\times 1}$ der einfache D_L-Modul. Durch $ds := (1 \otimes d)s$ für $s \in S$ und $d \in D$ wird S ein D-Modul. Für $\lambda \in L$ gilt $\lambda ds = (\lambda \otimes d)s = d\lambda s$. Daher induziert die Skalarmultiplikation von L auf S einen Algebrenhomomorphismus $f\colon L \to \operatorname{End}_D(S)$, der injektiv ist,

da L einfach ist. Da S über D eine Basis besitzt (Satz II.9.9), gilt $\mathrm{End}_D(S) \cong D^{n\times n}$ mit $n := \dim_D(S)$. Nun ist $\dim(D)\dim(L) = \dim(D_L) = k^2 \dim L$ und

$$k \dim L = \dim S = \dim_D(S) \dim D = nk^2.$$

Es folgt $\dim(L)^2 = n^2k^2 = n^2 \dim D$. □

Definition III.7.34. Sei $K \subseteq L$ eine Galois-Erweiterung und $G := \mathrm{Gal}(L|K)$. Sei $C^n(G, L^\times)$ Gruppe aller Abbildung $G^n \to L^\times$ bzgl. komponentenweiser Verknüpfung. Ein $\gamma \in C^2(G, L^\times)$ heißt *Faktorensystem* (oder 2-*Kozyklus*), falls

$$\boxed{\gamma(x,y)\gamma(xy,z) = x(\gamma(y,z))\gamma(x,yz)} \qquad \forall x, y, z \in G. \tag{III.7.1}$$

Die Faktorensysteme bilden eine Untergruppe $Z^2(G, L^\times) \leq C^2(G, L^\times)$.

Lemma III.7.35. *Die Abbildung $\partial\colon C^1(G, L^\times) \to Z^2(G, L^\times)$ mit $\partial\lambda(x, y) = \lambda(x)x(\lambda(y))\lambda(xy)^{-1}$ für $\lambda \in C^1(G, L^\times)$ und $x, y \in G$ ist ein Homomorphismus.*

Beweis. Für $x, y, z \in G$ gilt

$$\begin{aligned}\partial\lambda(x,y)\partial\lambda(xy,z) &= \lambda(x)x(\lambda(y))\lambda(xy)^{-1}\lambda(xy)(xy)(\lambda(z))\lambda(xyz)^{-1}\\ &= x(\lambda(y))x(y(\lambda(z)))\lambda(x)\lambda(xyz)^{-1}\\ &= x(\lambda(y)y(\lambda(z))\lambda(yz)^{-1})\lambda(x)x(\lambda(yz))\lambda(xyz)^{-1} = x(\partial\lambda(y,z))\partial\lambda(x,yz).\end{aligned}$$

Daher bildet ∂ nach $Z^2(G, L^\times)$ ab. Die Homomorphie-Eigenschaft ist offensichtlich. □

Definition III.7.36. Man setzt $B^2(G, L^\times) := \partial(C^1(G, L^\times))$ und nennt

$$H^2(G, L^\times) := Z^2(G, L^\times)/B^2(G, L^\times)$$

die *zweite Kohomologiegruppe* von G mit Werten in $L^\times$.

Lemma III.7.37. *Für $\gamma \in Z^2(G, L^\times)$ und $x \in G$ gilt $\gamma(1, x) = \gamma(1, 1)$ und $x(\gamma(1, 1)) = \gamma(x, 1)$. Jedes Element von $H^2(G, L^\times)$ enthält ein* normalisiertes *Faktorensystem γ mit $\gamma(1, x) = \gamma(x, 1) = 1$ für alle $x \in G$.*

Beweis. Setzt man $x = y = 1$ in (III.7.1), so folgt $\gamma(1, 1)\gamma(1, z) = \gamma(1, z)\gamma(1, z)$. Setzt man $y = z = 1$, so ergibt sich $\gamma(x, 1)\gamma(x, 1) = x(\gamma(1, 1))\gamma(x, 1)$. Für die zweite Behauptung ersetzt man γ durch $\delta := \gamma\partial\lambda$ mit $\lambda(1) := \gamma(1, 1)^{-1}$. Dann gilt

$$\delta(1, x) = \delta(1, 1) = \gamma(1, 1)\lambda(1)\lambda(1)\lambda(1)^{-1} = 1$$

und $\delta(x, 1) = x(\delta(1, 1)) = 1$. □

Satz III.7.38. *Für $\overline{\gamma} \in H^2(G, L^\times)$ ist $\overline{\gamma}^{|G|} = 1$.*

Beweis. Sei $\delta(x) := \prod_{g\in G} \gamma(x, g)$ für $x \in G$. Nach (III.7.1) ist

$$\gamma(x, y)^{|G|}\delta(xy) = \prod_{z\in G} \gamma(x, y)\gamma(xy, z) = \prod_{z\in G} x(\gamma(y, z))\gamma(x, yz) = x(\delta(y))\delta(x).$$

Dies zeigt $\gamma^{|G|} = \partial\delta \in B^2(G, L^\times)$. □

Beispiel III.7.39. Wir betrachten die Galois-Erweiterung $\mathbb{Q} \subseteq \mathbb{Q}(\mathrm{i})$ mit $G := \mathrm{Gal}(\mathbb{Q}(\mathrm{i})|\mathbb{Q}) = \langle\sigma\rangle$, wobei σ die komplexe Konjugation ist. Sei $\gamma \in Z^2(G, \mathbb{Q}(\mathrm{i})^\times)$ normalisiert. Dann ist γ durch $\zeta := \gamma(\sigma, \sigma)$ eindeutig bestimmt. Aus (III.7.1) mit $x = y = z = \sigma$ folgt $\sigma(\zeta) = \zeta \in \mathbb{Q}^\times$. Man prüft leicht, dass die übrigen Belegungen von x, y, z keine weiteren Einschränkungen liefern. Sei auch $\gamma' := \gamma\partial\mu$ normalisiert mit $\mu \in C^1(G, \mathbb{Q}(\mathrm{i})^\times)$. Dann gilt $1 = \gamma'(1,1) = \gamma(1,1)\mu(1)\mu(1)\mu(1)^{-1} = \mu(1)$. Für $\mu(\sigma) = a + b\mathrm{i}$ ist

$$\zeta' := \gamma'(\sigma,\sigma) = \zeta\mu(\sigma)\sigma(\mu(\sigma))\mu(\sigma^2)^{-1} = \zeta(a^2+b)^2.$$

Mit $a = \frac{a_1}{a_2}$ und $b = \frac{b_1}{b_2}$ (wobei $a_1, a_2, b_1, b_2 \in \mathbb{Z}$) folgt

$$\zeta' = \zeta\frac{(a_1b_2)^2 + (b_1a_2)^2}{(a_2b_2)^2}.$$

Nach Satz II.5.34 treten die Primfaktoren $p \equiv 3 \pmod 4$ mit gerader Vielfachheit in $(a_1b_2)^2 + (b_1a_2)^2$ auf. Die Vielfachheiten von p in ζ und ζ' haben also die gleiche Parität. Für jede solche Primzahl definieren wir nun $\gamma_p \in Z^2(G, \mathbb{Q}(\mathrm{i})^\times)$ durch $\gamma_p(\sigma,\sigma) = p$. Für verschiedene $p, q \in \mathbb{P}$ mit $p \equiv 3 \equiv q \pmod 4$ gilt dann $\overline{\gamma_p} \neq \overline{\gamma_q}$ in $H^2(G, \mathbb{Q}(\mathrm{i})^\times)$. Aus Aufgabe I.5 folgt $|H^2(G, \mathbb{Q}(\mathrm{i})^\times)| = \infty$. Da $H^2(G, \mathbb{Q}(\mathrm{i})^\times)$ abzählbar ist, gilt genauer $H^2(G, \mathbb{Q}(\mathrm{i})^\times) \cong \coprod_{k=1}^\infty C_2$ nach Satz III.7.38.

Definition III.7.40. Sei D eine zentrale Divisionsalgebra mit Galois-Zerfällungskörper L. Nach Lemma III.7.33 lässt sich L in die zentral-einfache Algebra $A := D^{n\times n}$ einbetten. Dabei gilt $\dim A = \dim(L)^2$. Nach dem Doppel-Zentralisator-Satz ist andererseits $\dim A = \dim(L)\dim(\mathrm{C}_A(L)) \geq \dim(L)^2$. Dies zeigt $\mathrm{C}_A(L) = L$. Sei $G := \mathrm{Gal}(L|K)$ und $x \in G$. Nach Skolem-Noether lässt sich x zu einem inneren Automorphismus von A fortsetzen. Sei also $a_x \in A^\times$ mit $x(\lambda) = a_x\lambda a_x^{-1}$ für alle $\lambda \in L$. Wegen $\mathrm{C}_A(L) = L$ ist a_x bis auf L-Multiplikation eindeutig bestimmt. Ist auch $y \in G$, so gilt

$$a_{xy}\lambda a_{xy}^{-1} = (xy)(\lambda) = x(y(\lambda)) = a_xa_y\lambda a_y^{-1}a_x^{-1}.$$

Daher ist $a_xa_y = \gamma(x,y)a_{xy}$ mit $\gamma(x,y) \in L^\times$.

Lemma III.7.41. *Mit den Bezeichnungen aus Definition III.7.40 ist $\gamma\colon G\times G \to L^\times$ ein Faktorensystem. Die entsprechende Nebenklasse $\overline{\gamma} \in H^2(G, L^\times)$ hängt nicht von der Wahl der a_x ab.*

Beweis. Für $x, y, z \in G$ gilt

$$\begin{aligned}\gamma(x,y)\gamma(xy,z)a_{xyz} &= \gamma(x,y)a_{xy}a_z = (a_xa_y)a_z = a_x(a_ya_z) = a_x\gamma(y,z)a_{yz}\\ &= x(\gamma(y,z))a_xa_{yz} = x(\gamma(y,z))\gamma(x,yz)a_{xyz}.\end{aligned}$$

Dies zeigt $\gamma \in Z^2(G, L^\times)$. Sei nun $\lambda\colon G \to L^\times$ mit $a'_x = \lambda(x)a_x$ und $a'_xa'_y = \gamma'(x,y)a'_{xy}$. Dann folgt

$$\gamma'(x,y)\lambda(xy)a_{xy} = \gamma'(x,y)a'_{xy} = a'_xa'_y = \lambda(x)a_x\lambda(y)a_y = \lambda(x)x(\lambda(y))\gamma(x,y)a_{xy}$$

und $\gamma'(x,y) = \gamma(x,y)\lambda(x)x(\lambda(y))\lambda(xy)^{-1}$. Dies zeigt $\gamma' = \gamma\partial_\lambda \in \overline{\gamma}$. □

Definition III.7.42. Sei $K \subseteq L$ eine Galois-Erweiterung, $G := \mathrm{Gal}(L|K)$ und $\gamma \in Z^2(G, L^\times)$. Wir definieren die *verschränkte Gruppenalgebra* $L_\gamma G$ als K-Vektorraum LG mit der Multiplikation

$$\lambda_x x \cdot \lambda_y y := \lambda_x x(\lambda_y)\gamma(x,y)xy \qquad (x, y \in G, \lambda_x, \lambda_y \in L).$$

Satz III.7.43. *Mit den Bezeichnungen aus Definition III.7.42 ist $L_\gamma G$ eine zentral-einfache K-Algebra mit Zerfällungskörper L und $\dim_K(L_\gamma G) = |G|^2 = |L:K|^2$.*

Beweis. Für $x, y, z \in G$ gilt

$$\begin{aligned}(\lambda_x x \cdot \lambda_y y) \cdot \lambda_z z &= \lambda_x x(\lambda_y)\gamma(x,y)xy \cdot \lambda_z z = \lambda_x x(\lambda_y)\gamma(x,y)(xy)(\lambda_z)\gamma(xy,z)xyz \\ &= \lambda_x x(\lambda_y y(\lambda_z))\gamma(x,y)\gamma(xy,z)xyz = \lambda_x x(\lambda_y y(\lambda_z))x(\gamma(y,z))\gamma(x,yz)xyz \\ &= \lambda_x x \cdot \lambda_y y(\lambda_z)\gamma(y,z)yz = \lambda_x x \cdot (\lambda_y y \cdot \lambda_z z).\end{aligned}$$

Dies zeigt die Assoziativität der Multiplikation in $A := L_\gamma G$. Das Einselement ist $e := \gamma(1,1)^{-1}1$, denn nach Lemma III.7.37 gilt

$$\begin{aligned}e \cdot \lambda_x x &= \gamma(1,1)^{-1}\lambda_x\gamma(1,x)x = \lambda_x x, \\ \lambda_x x \cdot e &= \lambda_x x(\gamma(1,1))^{-1}\gamma(x,1)x = \lambda_x x\end{aligned}$$

für alle $x \in G$. Wir können daher L mit $Le \subseteq A$ identifizieren. Die Distributivgesetze gelten durch lineare Fortsetzung der Multiplikationsvorschrift. Für $\mu \in K$ ist

$$\mu(\lambda_x x \cdot \lambda_y y) = \mu\lambda_x x(\lambda_y)\gamma(x,y)xy = (\mu\lambda_x x) \cdot \lambda_y y = \lambda_x x(\mu\lambda_y)\gamma(x,y)xy = \lambda_x x \cdot (\mu\lambda_y y).$$

Somit ist A eine K-Algebra.

Sei $a := \sum_{x\in G} \lambda_x x \in \mathrm{C}_A(L)$. Für $\mu \in L$ gilt

$$\sum_{x\in G} \mu\lambda_x x = \mu e \cdot a = a \cdot \mu e = \sum_{x\in G} \lambda_x x(\mu)x.$$

Im Fall $\lambda_x \neq 0$ ist daher $x(\mu) = \mu$ für alle $\mu \in L$. Dies zeigt $a = \lambda_1 1$ und $\mathrm{C}_A(L) = L$. Ist zusätzlich $a \in \mathrm{Z}(A)$, so gilt

$$x(\lambda_1\gamma(1,1)) = x(\lambda_1)\gamma(x,1)x = x \cdot a = a \cdot x = \lambda_1\gamma(1,x)x = \lambda_1\gamma(1,1)x$$

für alle $x \in G$. Es folgt $\lambda_1\gamma(1,1) \in L^G = K$ und $\mathrm{Z}(A) = Ke$, d. h. A ist zentral.

Sei nun $0 \neq I \trianglelefteq A$. Wir wählen $a = \sum_{x\in G} \lambda_x x \in I \setminus \{0\}$, sodass möglichst viele λ_x verschwinden. Nach Multiplikation mit einem $x \in G$ können wir $\lambda_1 \neq 0$ annehmen. Sei $\mu \in L$ beliebig. Dann gilt

$$I \ni a \cdot \mu e - \mu e \cdot a = \sum_{x\in G\setminus\{1\}} (\lambda_x x(\mu) - \mu\lambda_x)x$$

und es folgt $a \cdot \mu e = \mu e \cdot a$. Daher ist $a \in \mathrm{C}_A(L) = L$. Insbesondere ist a invertierbar und man erhält $I = A$. Also ist A einfach. Nach dem Doppel-Zentralisator-Satz ist $L \otimes A \cong A \otimes L^o \cong L^{n\times n}$. Somit ist L ein Zerfällungskörper von A. Ist $\mu_1, \ldots, \mu_n \in L$ eine K-Basis von L, so ist $\{\mu_i g : i = 1, \ldots, n, g \in G\}$ eine K-Basis von $L_\gamma G$. Die letzte Behauptung folgt daher aus $|G| = |L : K|$. □

Lemma III.7.44. *Für $\gamma, \delta, \in Z^2(G, L^\times)$ gilt $L_\gamma G \cong L_\delta G$ genau dann, wenn $\gamma \equiv \delta \pmod{B^2(G, L^\times)}$.*

Beweis. Sei $A := L_\gamma G$, $B := L_\delta G$ und $f\colon A \to B$ ein Isomorphismus von K-Algebren. Wie im Beweis von Satz III.7.43 lässt sich L als Teilkörper von A und B auffassen (betrachte $L \to A$, $\lambda \mapsto \lambda\gamma(1,1)^{-1}1$). Nach Skolem-Noether können wir dann $f(\lambda) = \lambda$ für alle $\lambda \in L$ annehmen. Sei $x \in G$ und $f(x) = \sum_{g\in G} \mu_g g \in B$. Für $\lambda \in L$ gilt

$$\sum_{g\in G} \mu_g g(\lambda)g = f(x)\lambda = f(x)f(\lambda) = f(x\lambda) = f(x(\lambda)x) = x(\lambda)f(x) = \sum_{g\in G} x(\lambda)\mu_g g.$$

Im Fall $\mu_g \neq 1$ erhält man $g(\lambda) = x(\lambda)$ für alle $\lambda \in L$. Dies zeigt $f(x) = \mu_x x =: \mu(x)x$. Nun ist

$$\begin{aligned}\gamma(x,y)\mu(xy)xy = \gamma(x,y)f(xy) = f(\gamma(x,y)xy) = f(x \cdot y) = f(x) \cdot f(y)\\ = \mu(x)x \cdot \mu(y)y = \mu(x)x(\mu(y))\delta(x,y)xy,\end{aligned}$$

also $\gamma = \delta\partial\mu \equiv \delta \pmod{B^2(G, L^\times)}$.

Sei umgekehrt $\gamma = \delta\partial\mu$ mit $\mu \in C^1(G, L^\times)$. Wir betrachten die K-lineare Abbildung $f\colon A \to B$, $\lambda x \mapsto \lambda\mu(x)x$ für $x \in G$ und $\lambda \in L$. Wegen $\gamma(1,1) = \delta(1,1)\mu(1)\mu(1)\mu(1)^{-1} = \delta(1,1)\mu(1)$ gilt

$$f(1_A) = f(\gamma(1,1)^{-1}1) = \gamma(1,1)^{-1}\mu(1)1 = \delta(1,1)^{-1}1 = 1_B.$$

Für $x, y \in G$ und $\lambda_x, \lambda_y \in L$ ist

$$\begin{aligned}f(\lambda_x x \cdot \lambda_y y) &= f(\lambda_x x(\lambda_y)\gamma(x,y)xy) = \lambda_x x(\lambda_y)\gamma(x,y)\mu(xy)xy\\ &= \lambda_x x(\lambda_y)\delta(x,y)\mu(x)x(\mu(y))xy = \lambda_x\mu(x)x \cdot \lambda_y\mu(y)y = f(\lambda_x x) \cdot f(\lambda_y y).\end{aligned}$$

Also ist f ein Homomorphismus. Da A einfach ist, ist f injektiv. Wegen $\dim A = |G|^2 = \dim B$ ist f auch surjektiv. □

Bemerkung III.7.45. Für die Konstruktion von $L_\gamma G$ kann man nach Lemma III.7.44 ein normalisiertes Faktorensystem $\gamma \in Z^2(G, L^\times)$ wählen. Dann ist $1 \in G$ das Einselement in $L_\gamma G$ wie in der gewöhnlichen Gruppenalgebra LG. Da $L = L1$ ein Teilkörper von $L_\gamma G$ ist, kann man $L_\gamma G$ auch als L-Vektorraum mit Basis G betrachten. Im Gegensatz zu LG ist $L_\gamma G$ aber keine L-Algebra (selbst wenn γ trivial ist), denn dafür bräuchte man $L \subseteq \mathrm{Z}(L_\gamma G)$.

Satz III.7.46. *Für jede Galois-Erweiterung $K \subseteq L$ mit $G := \mathrm{Gal}(L|K)$ ist*

$$\begin{aligned}\Gamma\colon H^2(G, L^\times) &\to \mathrm{Br}(L|K),\\ \gamma &\mapsto [L_\gamma G]\end{aligned}$$

ist ein Isomorphismus.

Beweis (Chase).
Schritt 1: Γ ist bijektiv.
Nach Satz III.7.43 und Lemma III.7.44 ist Γ wohldefiniert. Sei D eine zentrale Divisionsalgebra mit Zerfällungskörper L. Wie in Definition III.7.40 ist L zu einer Unteralgebra von $A := D^{n\times n}$ isomorph und man erhält $a_x \in A^\times$ und $\gamma \in Z^2(G, L^\times)$ mit $x(\lambda) = a_x\lambda a_x^{-1}$ und $a_x a_y = \gamma(x,y)a_{xy}$ für $x, y \in G$ und $\lambda \in L$. Wir definieren die K-lineare Abbildung $f\colon L_\gamma G \to A$, $\lambda x \mapsto \lambda a_x$ mit $\lambda \in L$ und $x \in G$. Für $\lambda x, \mu y \in L_\gamma G$ gilt

$$f(\lambda x \cdot \mu y) = f(\lambda x(\mu)\gamma(x,y)xy) = \lambda x(\mu)\gamma(x,y)a_{xy} = \lambda x(\mu)a_x a_y = \lambda a_x \cdot \mu a_y = f(\lambda x)f(\mu y),$$

d. h. f ist ein Homomorphismus von Algebren. Da $L_\gamma G$ einfach ist, ist f injektiv. Nach Lemma III.7.33 ist

$$\dim(L_\gamma G) = |L : K|^2 = \dim(L)^2 = n^2 \dim D = \dim A.$$

Also ist f ein Isomorphismus und Γ ist surjektiv.

Seien $\gamma, \delta \in Z^2(G, L^\times)$ mit $[L_\gamma G] = [L_\delta G]$. Dann haben $L_\gamma G$ und $L_\delta G$ eine gemeinsame Basisalgebra D. Wegen $\dim(L_\gamma G) = \dim(L)^2 = \dim(L_\delta G)$ folgt $L_\gamma G \cong D^{n\times n} \cong L_\delta G$. Aus Lemma III.7.44 ergibt sich $\overline{\gamma} = \overline{\delta}$ in $H^2(G, L^\times)$. Daher ist Γ bijektiv.

Schritt 2: Γ ist ein Homomorphismus.
Seien $\gamma, \delta \in Z^2(G, L^\times)$ normalisiert, $A := L_\gamma G$, $B := L_\delta G$ und $C := L_{\gamma\delta} G$. Nach Bemerkung III.7.45 ist A ein L-A-Bimodul und B ein L-B-Bimodul. Also ist $V := A^o \otimes_L B$ ein A^o-B-Bimodul, den wir als $A \otimes_K B$-Rechtsmodul auffassen können. Für $a \otimes b \in V$ und $x \otimes y \in A \otimes_K B$ gilt dabei

$$(a \otimes b)(x \otimes y) = (x * a) \otimes by = ax \otimes by,$$

wobei $*$ die Multiplikation in A^o bezeichnet. Speziell für $\lambda \in L$ gilt

$$\lambda a \otimes b = (a * \lambda) \otimes b = a \otimes \lambda b.$$

Wir definieren nun eine Skalarmultiplikation auf V mit C von links. Für $\lambda x \in C$ ist die Abbildung $A^o \times B \to V$, $(a, b) \mapsto \lambda xa \otimes xb$ ausgeglichen. Daher ist

$$(\lambda x)(a \otimes b) := \lambda xa \otimes xb$$

wohldefiniert. Durch lineare Fortsetzung erhält man die Distributivgesetze. Für $\lambda_x x, \lambda_y y \in C$ gilt

$$\begin{aligned}(\lambda_x x \cdot \lambda_y y)(a \otimes b) &= (\lambda_x x(\lambda_y)\gamma(x,y)\delta(x,y)xy)(a \otimes b) = \lambda_x x(\lambda_y)\gamma(x,y)\delta(x,y)xya \otimes xyb \\ &= \lambda_x x(\lambda_y)\gamma(x,y)xya \otimes \delta(x,y)xyb = (\lambda_x x)(\lambda_y ya \otimes yb) \\ &= (\lambda_x x)((\lambda_y y)(a \otimes b))\end{aligned}$$

Also ist V ein C-Linksmodul. Für $a' \otimes b' \in A \otimes_K B$ gilt

$$(\lambda x(a \otimes b))(a' \otimes b') = (\lambda xa \otimes xb)(a' \otimes b') = \lambda xaa' \otimes xbb' = \lambda x(aa' \otimes bb') = \lambda x((a \otimes b)(a' \otimes b')).$$

Die Skalarmultiplikation von rechts liefert somit einen Homomorphismus $f\colon (A \otimes_K B)^o \to \mathrm{End}_C(V)$. Da $A \otimes_K B$ einfach ist, ist f injektiv.

Mit $n := |G| = \dim L$ gilt $\dim_K(V) = |L : K| \dim_L(A) \dim_L(B) = n^3$. Sei $C \simeq S^r$ die Zerlegung des regulären C-Moduls mit dem einfachen Modul S der einfachen Algebra C. Wegen $n^2 = \dim C = r \dim S$ folgt $V \simeq S^{nr}$, da mit C auch V halbeinfach ist. Nach Lemma II.7.20 gilt $\mathrm{End}_C(V) \cong D^{nr \times nr}$ mit der Divisionsalgebra $D := \mathrm{End}_C(S)$. Außerdem ist

$$n^2 = \dim(C^o) = \dim \mathrm{End}_C(C) = \dim(D^{r \times r}) = r^2 \dim D.$$

Dies zeigt

$$\dim(A \otimes_K B)^o = n^4 = n^2 r^2 \dim D = \dim \mathrm{End}_C(V).$$

Daher ist f ein Isomorphismus. Insbesondere ist $(A \otimes_K B)^o \cong D^{nr \times nr}$ sowie $C^o \cong D^{r \times r}$. Dies liefert $[A] \cdot [B] = [C]$, d. h. Γ ist ein Homomorphismus. □

Folgerung III.7.47. *Für jeden Körper K ist* $\mathrm{Br}(K)$ *eine Torsionsgruppe, d. h. jedes Element hat endliche Ordnung.*

Beweis. Dies folgt aus Bemerkung III.7.28, Folgerung III.7.31, Satz III.7.46 und Satz III.7.38. □

Beispiel III.7.48. Nach Satz III.7.46 und Beispiel III.7.39 gilt

$$\mathrm{Br}(\mathbb{Q}(\mathrm{i})|\mathbb{Q}) \cong H^2(G, \mathbb{Q}(\mathrm{i})^\times) \cong \coprod_{i=1}^{\infty} C_2.$$

Mit dem Albert-Brauer-Hasse-Noether-Satz aus der Klassenkörpertheorie zeigt man

$$\mathrm{Br}(\mathbb{Q}) \cong C_2 \times \bigtimes_{k=1}^{\infty} \mathbb{Q}/\mathbb{Z}.$$

Definition III.7.49. Nach Folgerung III.7.23 ist die Dimension einer zentral-einfachen Algebra A eine Quadratzahl. Man nennt $\deg A := \sqrt{\dim A}$ den *Grad* und $e(A) := \deg(A^b)$ den *Index* von A, wobei A^b die Basisalgebra von A ist.

Bemerkung III.7.50. Für eine zentrale Divisionsalgebra D mit Zerfällungskörper L gilt $\deg D \mid \dim L$ nach Lemma III.7.33. Der folgende Satz verbessert daher Satz III.7.38.

Satz III.7.51. *Für* $[A] \in \mathrm{Br}(K)$ *gilt* $[A]^{e(A)} = 1$.

Beweis. Wir können annehmen, dass $D := A$ eine Divisionsalgebra ist mit $e := e(A) = \deg(D)$. Sei L ein Galois-Zerfällungskörper von D. Wie in Definition III.7.40 können wir L in $A := D^{n\times n}$ einbetten (eine „neue“ Algebra A). Dabei gilt $(ne)^2 = n^2 \dim D = \dim A = \dim(L)^2$ und $\dim L = ne$. Sei $G := \mathrm{Gal}(L|K)$. Dann existieren $a_x \in A^\times$ mit $x(\lambda) = a_x \lambda a_x^{-1}$ und $a_x a_y = \gamma(x,y) a_{xy}$ für $x, y \in G$, $\lambda \in L$ und $\gamma \in C^2(G, L^\times)$. Sei $S = D^{n\times 1}$ der einfache A-Modul. Durch Einschränkung wird S ein L-Vektorraum. Dabei gilt

$$\dim_L(S) = \frac{\dim S}{\dim L} = \frac{n \dim D}{ne} = e.$$

Sei $v_1, \ldots, v_e$ eine L-Basis von S. Für $x \in G$ sei $\alpha(x) = (\alpha_{ij}(x)) \in L^{e\times e}$ mit

$$a_x v_i = \sum_{j=1}^{e} \alpha_{ij}(x) v_j.$$

Für $x, y \in G$ gilt dann

$$\begin{aligned}\gamma(x,y) \sum_{j=1}^{e} \alpha_{ij}(xy) v_j = \gamma(x,y) a_{xy} v_i = a_x a_y v_i = a_x \Big(\sum_{k=1}^{e} \alpha_{ik}(y) v_k \Big) \\ = \sum_{k=1}^{e} x(\alpha_{ik}(y)) a_x v_k = \sum_{k,j=1}^{e} x(\alpha_{ik}(y)) \alpha_{kj}(x) v_j.\end{aligned}$$

Dies zeigt $\gamma(x,y)\alpha(xy) = x(\alpha(y))\alpha(x)$ für alle $x, y \in G$. Sei schließlich $\lambda(x) := \det(\alpha(x))$. Dann folgt

$$\gamma(x,y)^e \lambda(xy) = \det(\gamma(x,y)\alpha(xy)) = \det(x(\alpha(y))) \det(\alpha(x)) = x(\lambda(y))\lambda(x).$$

Also ist $\gamma^e = \partial\lambda \in B^2(G, L^\times)$ und die Behauptung ergibt sich aus Satz III.7.46. □

Lemma III.7.52. *Für jede zentral-einfache Algebra* A *haben* $e(A)$ *und* $|\langle [A] \rangle|$ *die gleichen Primteiler.*

Beweis. Nach Satz III.7.51 ist $|\langle [A] \rangle|$ ein Teiler von $e(A)$. Wir müssen also nur zeigen, dass ein Primteiler $p \mid e(A)$ auch $|\langle [A] \rangle|$ teilt. Sei $A \cong D^{n\times n}$ für eine Divisionsalgebra D. Sei L ein Galois-Zerfällungskörper von D mit $G := \mathrm{Gal}(L|K)$. Dann gilt $|G|^2 = \dim(L)^2 = n^2 \dim D = (ne(A))^2$ (Lemma III.7.33) und p teilt $|G|$. Sei $P \in \mathrm{Syl}_p(G)$ und $L_p := \mathrm{Fix}(P) \leq L$. Nach dem Hauptsatz der Galois-Theorie ist p kein Teiler von $|G : P| = |L_p : K| = \dim(L_p)$. Nach Lemma III.7.33 ist L_p kein Zerfällungskörper von D. Insbesondere ist $[A_{L_p}] \neq 1$. Andererseits ist

$$L \otimes_{L_p} A_{L_p} = L \otimes_{L_p} L_p \otimes_K A \cong L \otimes_K A \cong A_L,$$

d. h. $A_{L_p} \in \mathrm{Br}(L|L_p) \cong H^2(P, L^\times)$, denn $\mathrm{Gal}(L|L_p) = P$. Nach Satz III.7.38 ist $|\langle [A_{L_p}] \rangle|$ ein Teiler von $|P|$ und damit eine nicht-triviale p-Potenz. Nach Satz III.7.27 muss p auch $|\langle [A] \rangle|$ teilen. □

Bemerkung III.7.53.

(i) Für jede zentral-einfache Algebra A über einen Zahlkörper gilt $e(A) = |\langle A \rangle|$ (ohne Beweis).

(ii) Unser nächstes Ziel ist eine Verbindung zu den in Definition II.13.61 definierten Schur-Indizes.

Lemma III.7.54. *Sei $K \subseteq L$ eine Körpererweiterung. Sei V ein endlich-dimensionaler KG-Modul und V_L der entsprechende LG-Modul. Dann gilt*

$$\dim_K \operatorname{End}_{KG}(V) = \dim_L \operatorname{End}_{LG}(V_L).$$

Beweis. Sei $\Delta\colon G \to \mathrm{GL}(n,K) \subseteq \mathrm{GL}(n,L)$ die zu V bzw. V_L gehörende Darstellung. Nach dem Beweis von Satz II.13.47 gilt $\operatorname{End}_{KG}(V) \cong \mathrm{C}_{K^{n\times n}}(\Delta(G))$. Sei $\Delta(g) = (\gamma_{ij}(g))_{i,j}$ für $g \in G$. Dann gilt

$$\begin{aligned} A = (a_{ij}) \in \mathrm{C}_{K^{n\times n}}(\Delta(G)) &\iff \forall g \in G : A\Delta(g) = \Delta(g)A \\ &\iff \forall g \in G \forall 1 \le i,j \le n : \sum_{k=1}^{n} a_{ik}\gamma_{kj}(g) = \sum_{k=1}^{n} \gamma_{ik}(g)a_{kj}. \end{aligned}$$

Folglich ist $\mathrm{C}_{K^{n\times n}}(\Delta(G))$ der Lösungsraum eines homogenen Gleichungssystems in n^2 Variablen, dessen Koeffizientenmatrix $M \in K^{n^2|G|\times n^2}$ aus den $\gamma_{ij}(g)$ gebildet wird. Bekanntlich hängt die Dimension dieses Raums nur vom Rang von M ab. Der Rang von M wiederum ändert sich nicht, wenn man M als Matrix über L betrachtet. Daraus folgt die Behauptung. □

Satz III.7.55. *Sei $\chi \in \mathrm{Irr}(G)$ mit Werten in einem Zahlkörper K. Sei Δ eine irreduzible K-Darstellung mit Charakter $m_K(\chi)\chi$. Dann ist $A := \Delta(KG)$ eine zentral-einfache K-Algebra mit $e(A) = m_K(\chi)$.*

Beweis. Nach Artin-Wedderburn ist A eine einfache K-Algebra. Nach Satz II.13.44 existiert ein Zerfällungskörper $L \supseteq K$ von G mit $|L : K| < \infty$. Sei $\Delta_L\colon G \to \mathrm{GL}(d,L)$ mit $\Delta_L(g) = \Delta(g)$ für $g \in G$. Sei $\Gamma\colon G \to \mathrm{GL}(e,L)$ eine L-Darstellung mit Charakter χ. Nach Voraussetzung ist $d = em$ mit $m := m_K(\chi)$. Bei geeigneter Basiswahl gilt $\Delta(g) = \operatorname{diag}(\Gamma(g), \dots, \Gamma(g))$ für alle $g \in G$. Sei $z \in KG$ mit $\Delta(z) \in \mathrm{Z}(A)$. Nach Satz II.13.47 gilt $\Gamma(z) \in \mathrm{C}_{L^{e\times e}}(\Gamma(G)) = L1_e$. Daher existiert ein $\alpha \in L$ mit $\Delta(z) = \alpha 1_d$. Wegen $\alpha d = \operatorname{tr}\Delta(z) = m\chi(z) \in K$ gilt $\alpha \in K$ und $\mathrm{Z}(A) \cong K$. Dies zeigt, dass A eine zentral-einfache K-Algebra ist.

Seien V, V_L und W die einfachen Moduln zu Δ, Δ_L und Γ. Dann ist A eine Matrixalgebra über der Divisionsalgebra $E := \operatorname{End}_{KG}(V)^o$. Außerdem ist $\operatorname{End}_{LG}(W) \cong \mathrm{C}_{L^{e\times e}}(\Gamma(G)) \cong L$ nach Satz II.13.47. Nach Lemma II.7.20 gilt $\operatorname{End}_{LG}(V_L) = \operatorname{End}_{LG}(W^m) \cong \operatorname{End}_{LG}(W)^{m\times m} \cong L^{m\times m}$. Mit Lemma III.7.54 folgt

$$e(A) = e(E) = \sqrt{\dim_K E} = \sqrt{\dim_L \operatorname{End}_{LG}(V_L)} = m.$$ □

Lemma III.7.56. *Seien D_1 und D_2 zentrale Divisionsalgebren mit teilerfremden Graden (oder Dimensionen). Dann ist $D_1 \otimes D_2$ eine Divisionsalgebra.*

Beweis. Sei $D_1 \otimes D_2 \cong D^{n\times n}$ für eine Divisionsalgebra D. Sei $D_1^o \otimes D_1 \cong K^{k\times k}$ (beachte $[D_1]^{-1} = [D_1^o]$). Dann gilt $k^2 = \dim(D_1^o \otimes D_1) = \dim(D_1)^2$ und $k = \dim(D_1)$. Andererseits gilt

$$\begin{aligned} D_2^{k\times k} \cong (K \otimes D_2)^{k\times k} &\overset{III.7.9}{\cong} K^{k\times k} \otimes D_2 \cong D_1^o \otimes D_1 \otimes D_2 \\ &\cong D_1^o \otimes D^{n\times n} \cong (D_1^o \otimes D)^{n\times n} \cong (E^{l\times l})^{n\times n} \cong E^{nl\times nl} \end{aligned}$$

für eine weitere Divisionsalgebra E. Nach Artin-Wedderburn ist $D_2 \cong E$ und $k = nl$. Insbesondere ist $n \mid k = \dim(D_1) = \deg(D_1)^2$. Aus Symmetriegründen ist auch $n \mid \deg(D_2)^2$ und die Voraussetzung liefert $n = 1$, d. h. $D_1 \otimes D_2 \cong D$. □

Satz III.7.57. *Sei D eine zentrale Divisionsalgebra mit $\deg(D) = p_1^{a_1} \dots p_k^{a_k}$ (Primfaktorzerlegung). Dann existieren bis auf Isomorphie eindeutig bestimmte Divisionsalgebren $D_1, \dots, D_k$ mit $D \cong D_1 \otimes \dots \otimes D_k$ und $\deg(D_i) = p_i^{a_i}$ für $i = 1, \dots, k$.*

Beweis. Sei $\deg(D) = n_1 n_2$ mit teilerfremden $n_1, n_2 > 1$. Wir zeigen, dass bis auf Isomorphie eindeutig bestimmte Divisionsalgebren D_1 und D_2 mit $D \cong D_1 \otimes D_2$ und $\deg(D_i) = n_i$ für $i = 1, 2$ existieren. Die Behauptung folgt dann durch Induktion nach k. Seien $a, b \in \mathbb{Z}$ mit $an_1 + bn_2 = \mathrm{ggT}(n_1, n_2) = 1$. Seien D_1 und D_2 die eindeutig bestimmten Divisionsalgebren mit $[D]^{bn_2} = [D_1]$ und $[D]^{an_1} = [D_2]$. Dann gilt $[D_1 \otimes D_2] = [D]^{an_1 + bn_2} = [D]$ und

$$[D_1]^{n_1} = [D]^{b \deg(D)} = [D]^{be(D)} = 1$$

nach Satz III.7.51. Nach Lemma III.7.52 ist jeder Primteiler von $\deg(D_1)$ ein Teiler von n_1. Analoges gilt für D_2. Aus der Voraussetzung folgt $\mathrm{ggT}(\deg(D_1), \deg(D_2)) = 1$. Nun ist $D_1 \otimes D_2$ eine Divisionsalgebra nach Lemma III.7.56. Dies zeigt $D \cong D_1 \otimes D_2$. Wegen $n_1 n_2 = \deg(D) = \deg(D_1 \otimes D_2) = \deg(D_1)\deg(D_2)$ gilt $\deg(D_i) = n_i$ für $i = 1, 2$. □

Bemerkung III.7.58. Mit Hilfe von Satz III.7.57 kann man die Artin-Wedderburn-Zerlegung verfeinern.

8 Bewertungsringe

Bemerkung III.8.1. In der Darstellungstheorie endlicher Gruppen haben wir gesehen, dass die Wahl des zugrunde liegenden Körpers eine entscheidende Rolle spielt (sowohl die Charakteristik als auch die Existenz von Einheitswurzeln). Bewertungsringe dienen dazu Darstellungen von einem Körper zu einem anderen Körper zu transportieren. Die irreduziblen Darstellungen von $G = S_3$ über $\mathbb{C}$ lassen sich beispielsweise über $\mathbb{Z}$ realisieren und anschließend modulo einer Primzahl p reduzieren, sodass man Darstellungen über $\mathbb{F}_p$ erhält (irreduzible Darstellungen bleiben dabei im Allgemeinen nicht irreduzibel). Für beliebige Gruppen muss man größere Ringe mit entsprechenden Eigenschaften konstruieren. Dies führt zu vollständigen normierten Räumen mit interessantem und zugleich ungewohntem analytischen Konvergenzverhalten.

Definition III.8.2. Eine (*multiplikative*) *Bewertung* eines Integritätsbereichs R ist eine Abbildung $\nu\colon R \to \mathbb{R}$ mit folgenden Eigenschaften:

- $\nu(x) \geq 0$ und $\nu(x) = 0 \iff x = 0$ (*positiv definit*),
- $\nu(xy) = \nu(x)\nu(y)$ (*multiplikativ*),
- $\nu(x + y) \leq \nu(x) + \nu(y)$ (*subadditiv* oder *Dreiecksungleichung*)

für alle $x, y \in R$. Man nennt ν

- *vollständig*, falls R mit der Norm $|x| := \nu(x)$ ein vollständiger normierter Raum ist.
- *archimedisch*, falls ein $n \in \mathbb{N}$ mit $\nu(n \cdot 1) > 1$ existiert.
- *ultrametrisch*, falls $\nu(x + y) \leq \max\{\nu(x), \nu(y)\}$ für alle $x, y \in R$ gilt.

Beispiel III.8.3.

(i) Jeder Integritätsbereich R besitzt die *triviale* Bewertung ν mit $\nu(x) = 1$ für alle $x \in R \setminus \{0\}$. Sie ist vollständig, archimedisch und ultrametrisch. Endliche Körper K besitzen nur die triviale Bewertung, denn aus $\nu(x)^{|K|-1} = \nu(x^{|K|-1}) = 1$ folgt $\nu(x) = 1$ für $x \in K^\times$.

(ii) Jeder Teilring $R \subseteq \mathbb{C}$ besitzt die *euklidische* Bewertung $\nu(x) := |x| = \sqrt{x\overline{x}}$. Sie ist archimedisch und für $R \in \{\mathbb{R}, \mathbb{C}\}$ bekanntlich vollständig.

(iii) Für $x = \pm \prod_{p \in \mathbb{P}} p^{a_p} \in \mathbb{Z} \setminus \{0\}$ mit $a_p \in \mathbb{N}_0$ definiert $\nu_p(x) := p^{-a_p}$ die ultrametrische *p-adische* Bewertung auf $\mathbb{Z}$.

(iv) Für $\alpha = \sum_{k=0}^{\infty} a_k X^k \in R[X] \setminus \{0\}$ definiert $\nu(\alpha) := 2^{-\min\{k : a_k \neq 0\}}$ eine ultrametrische Bewertung auf $R[X]$ (man kann 2 durch jede andere Zahl > 1 ersetzen). Die gleiche Konstruktion funktioniert auch für den Ring $R[[X]]$ der formalen Potenzreihen aus Aufgabe II.30.

(v) Sei R ein Dedekindring mit Primideal $P \neq 0$. Nach Satz II.11.28 besitzt das Hauptideal (x) für $x \in R \setminus \{0\}$ eine eindeutige Primidealzerlegung $(x) = \prod_{Q \in \mathrm{Spec}(\mathbb{Z}_K)} Q^{a_Q}$ mit $a_P \in \mathbb{N}_0$. Dann definiert $\nu_P(x) := 2^{-a_P}$ eine Bewertung auf R. Ist R der Ganzheitsring eines Zahlkörpers, so erhält man durch $\nu_P(x) := |R : P|^{-a_P}$ die *P-adische* Bewertung als Verallgemeinerung der p-adischen Bewertung (nach Satz II.11.15 ist $|R : P| < \infty$).

(vi) Sei K ein Körper mit Bewertung ν und $\sigma \in \mathrm{Aut}(K)$. Dann ist auch $K \to \mathbb{R}$, $x \mapsto \nu(\sigma(x))$ eine Bewertung.

Bemerkung III.8.4. Sei ν eine Bewertung von R.

(i) Wegen $\nu(-1) > 0$ und $\nu(-1)^2 = \nu((-1)^2) = \nu(1) = 1$ gilt $\nu(-1) = 1$. Allgemeiner ist $\nu(-x) = \nu(x)$ für $x \in K$.

(ii) Wegen $\nu(x) = \nu(x-y+y) \leq \nu(x-y)+\nu(y)$ gilt $|\nu(x)-\nu(y)| \leq \nu(x-y)$ für $x, y \in R$. Konvergiert die Folge $(x_n)_n$ in R bzgl. ν gegen x, so gilt $|\nu(x) - \nu(x_n)| \leq \nu(x - x_n) \to 0$ mit $n \to \infty$ und

$$\lim_{n\to\infty} \nu(x_n) = \nu\Big(\lim_{n\to\infty} x_n\Big) = \nu(x),$$

d. h. ν ist stetig bzgl. der euklidischen Norm in $\mathbb{R}$.

(iii) Die ultrametrische Ungleichung $\nu(x + y) \leq \max\{\nu(x), \nu(y)\}$ impliziert die Dreiecksungleichung.

(iv) Ist ν ultrametrisch und $\nu(x) < \nu(y)$, so gilt

$$\nu(y) = \nu(x + y - x) \leq \max\{\nu(x + y), \nu(x)\} \leq \max\{\nu(x), \nu(y)\} = \nu(y).$$

Dies zeigt $\nu(x + y) = \nu(y)$. Geometrisch formuliert: Alle Dreiecke sind gleichschenklig.

(v) In manchem Büchern benutzt man *additive* Bewertungen $\nu\colon R \to \mathbb{R} \cup \{\infty\}$ mit den Axiomen

- $\nu(x) = \infty \iff x = 0$,
- $\nu(xy) = \nu(x) + \nu(y)$,
- $\nu(x + y) \geq \min\{\nu(x), \nu(y)\}$

für alle $x, y \in R$. Unter diesen Voraussetzungen ist $R \to \mathbb{R}$, $x \mapsto 2^{-\nu(x)}$ eine ultrametrische multiplikative Bewertung und umgekehrt. Archimedische Bewertungen werden auf diese Weise nicht berücksichtigt.

Lemma III.8.5. *Jede Bewertung ν eines Integritätsbereichs R lässt sich eindeutig zu einer Bewertung $\hat{\nu}$ auf dem Quotientenkörper $Q(R)$ fortsetzen. Dabei gilt $\hat{\nu}\big(\frac{x}{y}\big) = \frac{\nu(x)}{\nu(y)}$ für $\frac{x}{y} \in Q(R)$. Ist ν archimedisch (bzw. ultrametrisch), so auch $\hat{\nu}$.*

Beweis. Für $\frac{x}{y} \in Q(R) =: K$ ist $y \neq 0$ und $\nu(y) \neq 0$. Gilt $\frac{x}{y} = \frac{a}{b}$ in K, so ist $\nu(x)\nu(b) = \nu(xb) = \nu(ya) = \nu(y)\nu(a)$. Also ist $\hat{\nu}\colon K \to \mathbb{R}$ wohldefiniert und offensichtlich auch positiv definit und multiplikativ. Für beliebige $\frac{x}{y}, \frac{a}{b} \in K$ gilt

$$\hat{\nu}\Big(\frac{x}{y} + \frac{a}{b}\Big) = \frac{\nu(xb + ya)}{\nu(yb)} \leq \frac{\nu(x)\nu(b) + \nu(y)\nu(a)}{\nu(y)\nu(b)} = \frac{\nu(x)}{\nu(y)} + \frac{\nu(a)}{\nu(b)} = \hat{\nu}\Big(\frac{x}{y}\Big) + \hat{\nu}\Big(\frac{a}{b}\Big).$$

Daher ist $\hat{\nu}$ eine Bewertung von K. Für jede weitere Fortsetzung $\hat{\nu}'$ von ν gilt

$$\nu(x) = \hat{\nu}'(x) = \hat{\nu}'\Big(\frac{x}{y}\Big)\hat{\nu}'(y) = \hat{\nu}'\Big(\frac{x}{y}\Big)\nu(y)$$

und $\hat{\nu}'\big(\frac{x}{y}\big) = \frac{\nu(x)}{\nu(y)} = \hat{\nu}\big(\frac{x}{y}\big)$.

Ist ν archimedisch, so auch $\hat{\nu}$. Ist ν ultrametrisch, so gilt

$$\hat{\nu}\Big(\frac{x}{y}+\frac{a}{b}\Big) = \frac{\nu(xb+ya)}{\nu(yb)} \le \frac{\max\{\nu(x)\nu(b),\nu(y)\nu(a)\}}{\nu(y)\nu(b)} = \max\Big\{\frac{\nu(x)}{\nu(y)},\frac{\nu(a)}{\nu(b)}\Big\} = \max\Big\{\hat{\nu}\Big(\frac{x}{y}\Big),\hat{\nu}\Big(\frac{a}{b}\Big)\Big\}.$$

Daher ist auch $\hat{\nu}$ ultrametrisch. □

Beispiel III.8.6. Die p-adische Bewertung auf $\mathbb{Z}$ setzt sich nach $\mathbb{Q}$ fort. Die in Beispiel III.8.3 definierten Bewertungen auf $K[X]$ und $K[[X]]$ für einen Körper K setzen sich nach $K(X)$ bzw. $K((X))$ fort (Aufgabe II.30).

Lemma III.8.7. *Jede nicht-triviale Bewertung ν eines Körpers K ist entweder archimedisch oder ultrametrisch. Ist* $\operatorname{char} K > 0$*, so ist ν ultrametrisch.*

Beweis. Ist ν ultrametrisch, so gilt $\nu(n\cdot 1) \le \max\{\nu((n-1)\cdot 1),\nu(1)\} \le \ldots \le \nu(1) = 1$ und ν ist nicht archimedisch. Nehmen wir umgekehrt an, dass ν nicht archimedisch ist. Für $x,y \in K$ mit $M := \max\{\nu(x),\nu(y)\}$ gilt

$$\nu(x+y)^n = \nu((x+y)^n) = \nu\Big(\sum_{k=0}^{n}\binom{n}{k}x^k y^{n-k}\Big) \le \sum_{k=0}^{n}\nu\Big(\binom{n}{k}\Big)\nu(x)^k\nu(y)^{n-k} \le (n+1)M^n.$$

Wegen

$$n\big(\log\nu(x+y) - \log(M)\big) \le \log(n+1) \tag{III.8.1}$$

für alle $n \in \mathbb{N}$ folgt $\nu(x+y) \le M = \max\{\nu(x),\nu(y)\}$. Also ist ν ultrametrisch.

Für $\operatorname{char} K = p > 0$ erfüllt jede Bewertung $\nu(\lambda)^{p-1} = \nu(\lambda^{p-1}) = \nu(1) = 1$ für $\lambda \in \mathbb{F}_p$. Daher kann ν nicht archimedisch sein. □

Definition III.8.8. Eine Bewertung ν eines Körper K heißt *diskret*, falls $\nu(K^\times) = \langle c\rangle \cong C_\infty$.

Satz III.8.9. *Sei ν eine ultrametrische Bewertung eines Körper K. Dann ist*

$$R := \{x \in K : \nu(x) \le 1\}$$

ein lokaler Teilring von K mit $\mathrm{J}(R) = \{x \in R : \nu(x) < 1\}$*. Umgekehrt ist K zum Quotientenkörper von R isomorph. Ist ν diskret, so ist R ein Hauptidealring.*

Beweis. Man zeigt leicht, dass R ein Teilring und $P := \{x \in R : \nu(x) < 1\}$ ein echtes Ideal von R ist. Sei $x \in I \lhd R$ gegeben. Im Fall $\nu(x) = 1$ ist auch $\nu(x^{-1}) = 1$ und $x^{-1} \in R$. Dann wäre $1 = xx^{-1} \in R$. Also gilt $I \subseteq P = \mathrm{J}(R)$ und R ist lokal. Die Inklusion $R \to K$ setzt sich zu einem Isomorphismus $Q(R) \to K$ fort, da für $x \in K \setminus R$ stets $x^{-1} \in R$ gilt.

Sei nun ν diskret und $\nu(K^\times) = \langle c\rangle$ mit $c \in \mathbb{R}$. O. B. d. A. sei $c < 1$ (anderenfalls ersetze c durch c^{-1}). Wähle $r \in R$ mit $\nu(r) = c$. Sei $I \trianglelefteq R$. Dann existiert ein minimales $k \in \mathbb{N}$ mit $\nu(x) \le c^k$ für alle $x \in I$. Es folgt $\nu(xr^{-k}) \le 1$ und $xr^{-k} \in R$. Dies zeigt $I \subseteq (r^k)$. Für $x \in I$ mit $\nu(x) = c^k$ erhält man $r^k x^{-1} \in R^\times$ und $(r^k) \subseteq I$. Also ist $I = (r^k)$ ein Hauptideal. □

Bemerkung III.8.10. In der Situation von Satz III.8.9 nennt man R den *Bewertungsring* und $\mathrm{J}(R)$ das *Bewertungsideal* von K.

Beispiel III.8.11.

(i) Für die triviale Bewertung auf K ist K der Bewertungsring und 0 das Bewertungsideal.

(ii) Für die p-adische Bewertung auf $\mathbb{Q}$ ist der Bewertungsring $R = \mathbb{Z}_{(p)}$ die Lokalisierung aus Beispiel III.1.7.

(iii) Sei ν die Bewertung von $K(X)$ mit $\nu(X) = 2^{-1}$. Dann ist $K[X]$ der Bewertungsring und (X) das Bewertungsideal. Für $K((X))$ ist analog $K[[X]]$ der Bewertungsring.

Lemma III.8.12. *Für nicht-triviale Bewertungen ν_1 und ν_2 eines Körper K sind folgende Eigenschaften äquivalent:*

(1) $\nu_1(x) < 1 \Longrightarrow \nu_2(x) < 1$ für alle $x \in K$.

(2) Es existiert ein $s > 0$ mit $\nu_1(x) = \nu_2(x)^s$ für alle $x \in K$.

(3) Die offenen Mengen von K bzgl. ν_1 und ν_2 stimmen überein.

Ggf. nennt man ν_1 und ν_2 äquivalent.

Beweis.

(1) $\Rightarrow$ (2): Für $x, y \in K$ gilt zunächst

$$\nu_1(x) < \nu_2(y) \implies \nu_1(x/y) < 1 \implies \nu_2(x/y) < 1 \implies \nu_2(x) < \nu_2(y).$$

Da ν_1 nicht trivial ist, existiert $a \in K$ mit $\rho_1 := \nu_1(a) > 1 = \nu_1(1)$. Es folgt $\rho_2 := \nu_2(a) > 1$. Für jedes $x \in K^\times$ existieren $\alpha, \beta \in \mathbb{R}$ mit $\nu_1(x) = \rho_1^\alpha$ und $\nu_2(x) = \rho_2^\beta$. Da $\mathbb{Q}$ dicht in $\mathbb{R}$ liegt, können wir α beliebig gut durch rationale Zahlen approximieren, etwa $\frac{n}{m} < \alpha < \frac{k}{m}$ mit $n, m, k \in \mathbb{Z}$. Da die Funktion $\mathbb{R} \to \mathbb{R}$, $r \mapsto \rho_1^r$ streng monoton wächst, folgt

$$\begin{aligned}
\rho_1^n < \rho_1^{\alpha m} < \rho_1^k, \\
\nu_1(a)^n < \nu_1(x)^m < \nu_1(a)^k, \\
\nu_2(a)^n < \nu_2(x)^m < \nu_2(a)^k, \\
\rho_2^n < \rho_2^{\beta m} < \rho_2^k.
\end{aligned}$$

Wegen $\rho_2 > 1$ ist $\frac{n}{m} < \beta < \frac{k}{m}$ und $\alpha = \beta$. Für $s := \frac{\log \rho_2}{\log \rho_1} > 0$ gilt

$$\nu_2(x) = e^{\beta \log \rho_2} = e^{\alpha s \log \rho_1} = (\rho_1^\alpha)^s = \nu_1(x)^s$$

für alle $x \in K$.

(2) $\Rightarrow$ (3): Sei $U \subseteq K$ offen bzgl. ν_1 und $x \in U$. Dann existiert ein $\epsilon > 0$ mit $\{y \in K : \nu_1(x-y) < \epsilon\} \subseteq U$. Wegen $\nu_2(x-y) = \nu_1(x-y)^{1/s}$ gilt $\nu_2(x-y) < \epsilon^{1/s} \Rightarrow y \in U$. Also ist U bzgl. ν_2 offen. Wegen $\nu_2(x) = \nu_1(x)^{1/s}$ für alle $x \in K$ gilt auch die Umkehrung.

(3) $\Rightarrow$ (1): Sei $x \in K$ mit $\nu_1(x) < 1$. Dann gilt $\lim_{n\to\infty} x^n = 0$ bzgl. ν_1. Nach Voraussetzung ist $(K, \nu_1) \to (K, \nu_2)$, $a \to a$ stetig (Urbilder offener Mengen sind offen). Also konvergiert x^n auch bzgl. ν_2 gegen 0. Dies impliziert $\nu_2(x) < 1$. □

Bemerkung III.8.13. Die Äquivalenz von Bewertungen ist offensichtlich eine Äquivalenzrelation. Ist ν eine diskrete (bzw. vollständige) Bewertung, so ist auch jede zu ν äquivalente Bewertung diskret (bzw. vollständig). Äquivalente ultrametrische Bewertungen definieren den gleichen Bewertungsring.

Satz III.8.14 (Ostrowski)**.** *Jede nicht-triviale Bewertung auf $\mathbb{Q}$ ist entweder zur euklidischen Bewertung oder zu genau einer p-adischen Bewertung äquivalent.*

Beweis. Sei ν eine nicht-triviale Bewertung auf $\mathbb{Q}$.

Fall 1: ν ist ultrametrisch.
Dann gilt $\nu(n) \leq 1$ für alle $n \in \mathbb{Z}$ und es existiert ein minimales $p \in \mathbb{N}$ mit $\nu(p) < 1$. Sei $p = ab$ mit $a, b \in \mathbb{N}$. Aus $\nu(a)\nu(b) = \nu(ab) < 1$ folgt $a = p$ oder $b = p$, d. h. $p \in \mathbb{P}$. Sei $q \in \mathbb{P} \setminus \{p\}$. Dann existieren $a, b \in \mathbb{Z}$ mit $ap + bq = 1$ und es folgt

$$1 = \nu(ap + bq) \leq \max\{\underbrace{\nu(a)\nu(p)}_{<1}, \nu(b)\nu(q)\} = \nu(b)\nu(q) = 1.$$

Daher ist $\nu(q) = 1$. Sei $x = \pm \prod_{q \in \mathbb{P}} q^{a_q} \in \mathbb{Q}^\times$. Dann gilt

$$\nu(x) < 1 \implies \nu(p)^{a_p} < 1 \implies a_p > 0 \implies \nu_p(x) = p^{-a_p} < 1.$$

Nach Lemma III.8.12 ist ν zur p-adischen Bewertung äquivalent. Für $q \in \mathbb{P} \setminus \{p\}$ ist ν wegen $\nu_q(q) < 1 = \nu(q)$ nicht zu ν_q äquivalent.

Fall 2: ν ist archimedisch.
Sei $a \in \mathbb{N}$ mit $\nu(a) > 1$ und $b \in \mathbb{N} \setminus \{1\}$. Für $n \in \mathbb{N}$ existieren ganze Zahlen $0 \leq \alpha_i \leq b - 1$ mit

$$a^n = \sum_{i=0}^{k} \alpha_i b^i \geq b^k$$

und $\alpha_k \neq 0$ (b-adische Entwicklung). Dabei gilt $k \leq n\frac{\log a}{\log b}$. Sei $\delta := \frac{\log a}{\log b}$. Nach der Dreiecksungleichung ist $\nu(\alpha_i) = \nu(1) + \ldots + \nu(1) \leq b$ für $i = 0, \ldots, k$. Mit $M := \max\{1, \nu(b)\}$ folgt

$$\nu(a)^n \leq \sum_{i=0}^{k} \nu(\alpha_i)\nu(b)^i \leq b(k+1)M^k \leq b(n\delta + 1)(M^\delta)^n.$$

Wie in (III.8.1) ergibt sich $\nu(a) \leq M^\delta$. Wegen $\nu(a) > 1$ ist $M = \nu(b) > 1$ und $\frac{\log \nu(a)}{\log a} \leq \frac{\log \nu(b)}{\log b}$. Durch Vertauschen von a und b erhält man

$$s := \frac{\log \nu(a)}{\log a} = \frac{\log \nu(b)}{\log b} > 0.$$

Also gilt $\nu(b) = b^s$ für alle $b \in \mathbb{N}$. Es folgt $\nu(q) = |q|^s$ für alle $q \in \mathbb{Q}$. Somit ist ν zur euklidischen Bewertung äquivalent. □

Folgerung III.8.15. *Jede diskrete Bewertung eines Körpers ist ultrametrisch.*

Beweis. Sei K ein Körper mit diskreter Bewertung ν. Nehmen wir an, dass ν archimedisch ist. Nach Lemma III.8.7 ist $\operatorname{char} K = 0$ und o. B. d. A. $\mathbb{Q} \subseteq K$. Außerdem existiert ein $n \in \mathbb{N}$ mit $\nu(n) > 1$. Daher ist die Einschränkung von ν auf $\mathbb{Q}$ ebenfalls eine archimedische Bewertung. Nach Ostrowski ist ν die euklidische Bewertung auf $\mathbb{Q}$. Insbesondere ist $\nu(\mathbb{Q}^\times) = \mathbb{Q}_+^\times$ nicht zyklisch. Somit kann auch $\nu(K^\times)$ nicht zyklisch sein. Widerspruch. □

Bemerkung III.8.16.

(i) Wir zeigen in Bemerkung III.8.42, dass die Umkehrung von Folgerung III.8.15 falsch ist.

(ii) Das Produkt über alle nicht-trivialen nicht-äquivalenten Bewertungen von $\mathbb{Q}$ ergibt interessanterweise die triviale Bewertung:

$$|x| \prod_{p \in \mathbb{P}} \nu_p(x) = 1 \qquad (x \in \mathbb{Q}^\times).$$

Satz III.8.17. *Für jeden Körper K mit Bewertung ν gilt:*

(i) Es existiert ein Körper $\hat{K}$ mit vollständiger Bewertung $\hat{\nu}$ und ein Monomorphismus $\Gamma\colon K \to \hat{K}$, sodass $\Gamma(K)$ dicht[1] in $\hat{K}$ liegt und $\hat{\nu} \circ \Gamma = \nu$ gilt.

(ii) Ist auch $\tilde{\Gamma}\colon K \to \tilde{K}$ wie in (i)*, so existiert genau ein stetiger Isomorphismus $\Theta\colon \hat{K} \to \tilde{K}$ mit $\Theta \circ \Gamma = \tilde{\Gamma}$.*

Man nennt $\hat{K}$ die Vervollständigung *von K bzgl. ν.*

Beweis.

(i) **Schritt 1:** Konstruktion von $\hat{K}$.
Sei R die Menge aller Cauchyfolgen[2] $\alpha := (a_n)_{n\in\mathbb{N}}$ von Elementen aus K. Nach Bemerkung III.8.4 ist $(\nu(a_n))_n$ ist eine reelle Cauchyfolge. Da $\mathbb{R}$ vollständig ist, existiert $\|\alpha\| := \lim_{n\to\infty} \nu(a_n) \in \mathbb{R}$. Für $\alpha := (a_n) \in R$ und $\beta := (b_n) \in R$ gilt

$$\begin{aligned} \nu(a_n + b_n - a_m - b_m) &\le \nu(a_n - a_m) + \nu(b_n - b_m), \\ \nu(a_n b_n - a_m b_m) = \nu(a_n b_n - a_n b_m + a_n b_m - a_m b_m) &\le \nu(a_n)\nu(b_n - b_m) + \nu(b_m)\nu(a_n - a_m). \end{aligned}$$

Daraus folgt $\alpha + \beta := (a_n + b_n)_n \in R$ und $\alpha \cdot \beta := (a_n b_n)_n \in R$. Auf diese Weise wird R mit $0 := (0, 0, \ldots)$ und $1 := (1, 1, \ldots)$ zu einem Ring. Außerdem ist $I := \{\alpha \in R : \|\alpha\| = 0\} \lhd R$. Für $\alpha \in R \setminus I$ existiert ein $N \in \mathbb{N}$ mit $\nu(a_n) > \frac{1}{2}\|\alpha\| > 0$ für alle $n \ge N$. Wir definieren $\beta := (b_n)_n = (1, \ldots, 1, a_N^{-1}, a_{N+1}^{-1}, \ldots)$. Dann gilt

$$\nu(b_n - b_m) = \nu\Big(\frac{a_m - a_n}{a_n a_m}\Big) \le 4\|\alpha\|^{-1}\nu(a_m - a_n)$$

für $n, m \ge N$ und es folgt $\beta \in R$. Außerdem ist $\|1 - \alpha\beta\| = 0$, d. h. $(\alpha + I)(\beta + I) = 1 + I$. Daher ist I ein maximales Ideal und $\hat{K} := R/I$ ist ein Körper. Offensichtlich ist $\Gamma\colon K \to \hat{K}$, $a \mapsto (a, a, \ldots) + I$ ein Monomorphismus.

Schritt 2: Konstruktion von $\hat{\nu}$.
Für $\alpha, \beta \in R$ gilt nach den üblichen Regeln für Grenzwerte

$$\begin{aligned} \|\alpha\| \ge 0 \text{ und } \|\alpha\| = 0 &\iff \alpha \in I, \\ \|\alpha\beta\| = \lim_{n\to\infty} \nu(a_n b_n) = \lim_{n\to\infty} \nu(a_n)\nu(b_n) &= \|\alpha\|\|\beta\|, \\ \|\alpha + \beta\| = \lim_{n\to\infty} \nu(a_n + b_n) \le \lim_{n\to\infty} (\nu(a_n) + \nu(b_n)) &= \|\alpha\| + \|\beta\|, \\ \alpha \equiv \beta \pmod{I} \implies \|\alpha\| = \|\alpha - \beta + \beta\| \le \|\alpha - \beta\| + \|\beta\| &= \|\beta\| \le \|\alpha\|. \end{aligned}$$

Also ist $\hat{\nu}\colon \hat{K} \to \mathbb{R}$, $\overline{\alpha} := \alpha + I \mapsto \|\alpha\|$ eine wohldefinierte Bewertung auf $\hat{K}$ mit $\hat{\nu}(\Gamma(a)) = \lim \nu(a) = \nu(a)$ für $a \in K$. Für $\epsilon > 0$ sei $N \in \mathbb{N}$ mit $\nu(a_n - a_m) < \epsilon$ für $n, m \ge N$. Dann gilt

$$\hat{\nu}(\overline{\alpha} - \Gamma(a_N)) = \lim_{n\to\infty} \nu(a_n - a_N) \le \epsilon.$$

[1] Erinnerung: Für alle $a \in \hat{K}$ und $\epsilon > 0$ existiert ein $b \in K$ mit $\hat{\nu}(a - b) < \epsilon$.
[2] Erinnerung: Für jedes $\epsilon > 0$ existiert ein $N \in \mathbb{N}$ mit $\nu(a_n - a_m) < \epsilon$ für alle $n, m \ge N$

Also liegt $\Gamma(K)$ dicht in $\hat{K}$.

Schritt 3: $\hat{\nu}$ ist vollständig.
Sei $(\overline{\alpha_n})_n$ eine Cauchyfolge in $\hat{K}$. Da $\Gamma(K)$ dicht in $\hat{K}$ liegt, existiert für jedes $n \in \mathbb{N}$ ein $a_n \in K$ mit $\hat{\nu}(\overline{\alpha_n} - \Gamma(a_n)) < \frac{1}{n}$. Sei $\alpha := (a_n)_n$ und $\epsilon > 0$. Dann existiert ein $N \in \mathbb{N}$ mit $\frac{1}{N} < \epsilon/4$ und $\hat{\nu}(\overline{\alpha_n} - \overline{\alpha_m}) < \epsilon/2$ für alle $n, m \geq N$. Es folgt

$$\begin{aligned}\nu(a_n - a_m) &= \hat{\nu}\big(\Gamma(a_n - a_m)\big) = \hat{\nu}\big(\Gamma(a_n) - \overline{\alpha_n} + \overline{\alpha_n} - \overline{\alpha_m} + \overline{\alpha_m} - \Gamma(a_m)\big) \\ &< \frac{1}{n} + \frac{\epsilon}{2} + \frac{1}{m} < \epsilon.\end{aligned}$$

Dies zeigt $\alpha \in R$. Außerdem ist

$$\begin{aligned}\hat{\nu}(\overline{\alpha} - \overline{\alpha_n}) &= \hat{\nu}(\overline{\alpha} - \Gamma(a_n) + \Gamma(a_n) - \overline{\alpha_n}) \leq \hat{\nu}(\overline{\alpha} - \Gamma(a_n)) + \hat{\nu}(\overline{\alpha_n} - \Gamma(a_n)) \\ &< \lim_{k\to\infty} \nu(a_k - a_n) + \frac{1}{n} \xrightarrow{n\to\infty} 0,\end{aligned}$$

d. h. $(\overline{\alpha_n})_n$ konvergiert gegen $\overline{\alpha}$ in K. Daher ist $\hat{\nu}$ vollständig.

(ii) **Schritt 1:** Konstruktion von Θ.
Für $\alpha = (a_n) \in R$ ist $\tilde{\nu}(\tilde{\Gamma}(a_n) - \tilde{\Gamma}(a_m)) = \nu(a_n - a_m)$. Also ist $(\tilde{\Gamma}(a_n))_n$ eine Cauchyfolge in $\tilde{K}$. Da $\tilde{\nu}$ vollständig ist, existiert

$$\Theta(\overline{\alpha}) := \lim_{n\to\infty} \tilde{\Gamma}(a_n) \in \tilde{K}.$$

Für $\beta = (b_n) \equiv \alpha \pmod{I}$ ist $(\tilde{\Gamma}(a_n) - \tilde{\Gamma}(b_n))_n$ eine Nullfolge. Dies zeigt, dass Θ wohldefiniert ist. Außerdem ist $\Theta(\Gamma(a)) = \lim \tilde{\Gamma}(a) = \tilde{\Gamma}(a)$ für alle $a \in K$. Mit $\tilde{\Gamma}$ ist auch Θ ein Ringhomomorphismus. Da $\hat{K}$ ein Körper ist, ist Θ injektiv. Da $\tilde{\Gamma}(K)$ dicht in $\tilde{K}$ liegt, ist jedes Element von $\tilde{K}$ Grenzwert einer Folge $(\tilde{\Gamma}(a_n))_n$. Mit $(\tilde{\Gamma}(a_n))_n$ ist auch $(a_n)_n$ eine Cauchyfolge. Daraus folgt die Surjektivität von Θ. Wegen

$$\tilde{\nu}\big(\Theta(\overline{\alpha})\big) = \tilde{\nu}\Big(\lim_{n\to\infty} \tilde{\Gamma}(a_n)\Big) \overset{III.8.4}{=} \lim_{n\to\infty} \nu(a_n) = \hat{\nu}(\overline{\alpha})$$

ist Θ isometrisch und daher (gleichmäßig) stetig.

Schritt 2: Eindeutigkeit von Θ.
Sei $\Psi\colon \hat{K} \to \tilde{K}$ ein weiterer stetiger Isomorphismus mit $\Psi \circ \Gamma = \tilde{\Gamma}$. Da $\Gamma(K)$ dicht in $\hat{K}$ liegt, existiert für $\overline{\alpha} \in \hat{K}$ eine Folge $(\Gamma(a_n))_n$ mit $\overline{\alpha} = \lim_{n\to\infty} \Gamma(a_n)$. Da Θ und Ψ stetig sind, gilt

$$\Psi(\overline{\alpha}) = \lim_{n\to\infty} \Psi(\Gamma(a_n)) = \lim_{n\to\infty} \tilde{\Gamma}(a_n) = \lim_{n\to\infty} \Theta(\Gamma(a_n)) = \Theta(\overline{\alpha}). \qquad \square$$

Beispiel III.8.18.

(i) Ist ν bereits vollständig, so ist $\hat{K} \cong K$ wegen der Eindeutigkeit von $\hat{K}$. Dies gilt zum Beispiel für die triviale Bewertung (jede Cauchyfolge ist konstant).

(ii) Bekanntlich ist $\mathbb{R}$ die Vervollständigung von $\mathbb{Q}$ bzgl. der euklidischen Bewertung.

(iii) Nach Aufgabe III.43 ist $K((X))$ die Vervollständigung von $K(X)$.

(iv) Sei $(a_n)_n$ eine ganzzahlige Cauchyfolge bzgl. der p-adischen Bewertung für $p \in \mathbb{P}$. Dann existiert für jedes $k \in \mathbb{N}$ ein $N \in \mathbb{N}$ mit $\nu_p(a_n - a_m) < p^{-k}$, d. h. $a_n \equiv a_m \pmod{p^k}$ für $n, m \geq N$. Dies motiviert folgende Definition.

Definition III.8.19. Für $p \in \mathbb{P}$ ist

$$\mathbb{Z}_{[p]} := \Big\{(a_n + p^n\mathbb{Z})_n \in \bigtimes_{n=1}^{\infty} \mathbb{Z}/p^n\mathbb{Z} : \forall n \in \mathbb{N} : a_n \equiv a_{n+1} \pmod{p^n}\Big\}$$

der Ring der *ganzen p-adischen Zahlen*. Für $\alpha = (a_n + p^n\mathbb{Z})_n \in \mathbb{Z}_{[p]} \setminus \{0\}$ existiert eine maximale Potenz p^k mit $p^k \mid a_k$. Wir definieren $\hat{\nu}_p(\alpha) := p^{-k}$ sowie $\hat{\nu}_p(0) := 0$.

Bemerkung III.8.20.

(i) Seien $\alpha := (a_n + p^n\mathbb{Z})_n \neq 0$ und $\beta := (b_n + p^n\mathbb{Z})_n \neq 0$ ganze p-adische Zahlen. Seien $k, l \in \mathbb{N}$ maximal mit $p^k \mid a_k$, $p^l \mid b_l$ und o. B. d. A. $k \leq l$. Wegen $b_k \equiv b_l \equiv 0 \pmod{p^k}$ gilt $p^k \mid a_k + b_k$ und es folgt

$$\hat{\nu}_p(\alpha + \beta) \leq p^{-k} = \max\big\{\hat{\nu}_p(\alpha), \hat{\nu}_p(\beta)\big\}.$$

Wegen $p^{k+l} \mid a_{k+l}b_{k+l}$ und $p^n \nmid a_nb_n$ für alle $n > k+l$ ist auch $\hat{\nu}_p(\alpha\beta) = \hat{\nu}(\alpha)\hat{\nu}(\beta)$. Insgesamt ist $\hat{\nu}_p$ eine ultrametrische Bewertung auf $\mathbb{Z}_{[p]}$. Aus $\alpha\beta \neq 0$ folgt außerdem, dass $\mathbb{Z}_{[p]}$ ein Integritätsbereich ist.

(ii) Den Quotientenkörper $\mathbb{Q}_{[p]}$ von $\mathbb{Z}_{[p]}$ nennt man Körper der *p-adischen Zahlen*.[3] Nach Lemma III.8.5 setzt sich $\hat{\nu}_p$ zu einer Bewertung auf $\mathbb{Q}_{[p]}$ fort. Offenbar ist $\mathbb{Z}_{[p]}$ der Bewertungsring von $\mathbb{Q}_{[p]}$ mit Bewertungsideal $p\mathbb{Z}_{[p]}$. Nach Satz III.8.9 ist $\mathbb{Z}_{[p]}$ lokal und $\mathbb{Z}_{[p]}^\times = \mathbb{Z}_{[p]} \setminus p\mathbb{Z}_{[p]}$.

(iii) Mittels des isometrischen Ringmonomorphismus $\mathbb{Z} \to \mathbb{Z}_{[p]}$, $a \mapsto (a + p^n\mathbb{Z})_n$ kann $\mathbb{Z}$ als Teilring von $\mathbb{Z}_{[p]}$ und $\mathbb{Q}$ als Teilkörper von $\mathbb{Q}_{[p]}$ auffassen. Insbesondere ist $\operatorname{char}\mathbb{Q}_{[p]} = 0$. Für $\alpha := (a_n + p^n\mathbb{Z})_n \in \mathbb{Z}_{[p]}$ können wir $0 \leq a_n < p^n$ für alle $n \in \mathbb{N}$ annehmen. Die Zahlen $b_0 := a_1$ und $b_n := \frac{a_{n+1} - a_n}{p^n}$ für $n \geq 1$ liegen dann in $\{0, \ldots, p-1\}$. Als Teleskopsumme erhält man eine (unendliche) p-adische Entwicklung

$$\alpha = \sum_{n=0}^{\infty} b_n p^n.$$

Für $\alpha \in \mathbb{N}$ stimmt dies mit der gewöhnlichen p-adischen Entwicklung überein (Aufgabe III.48). Umgekehrt definiert jede Folge $(b_n) \in \{0, \ldots, p-1\}^{\mathbb{N}_0}$ von Koeffizienten genau eine ganze p-adische Zahl. Insbesondere ist $\mathbb{Z}_{[p]}$ überabzählbar. Im Gegensatz zum Ring der formalen Potenzreihen $\mathbb{F}_p[[X]]$ werden p-adische Entwicklungen in $\mathbb{Z}_{[p]}$ mit „Übertrag“ addiert (außerdem ist $\operatorname{char}\mathbb{F}_p[[X]] = p$).

(iv) Sei $\frac{\alpha}{\beta} \in \mathbb{Q}_{[p]}$ und $\hat{\nu}_p(\beta) = p^{-k}$ mit $k \in \mathbb{N}_0$. Dann ist $p^{-k}\beta \in \mathbb{Z}_{[p]}^\times$ und es existiert eine p-adische Entwicklung $\alpha(p^{-k}\beta)^{-1} = \sum_{n=0}^{\infty} b_n p^n$. Also ist

$$\frac{\alpha}{\beta} = p^{-k}\frac{\alpha}{p^{-k}\beta} = \sum_{n=-k}^{\infty} b_{n+k}p^n =: \ldots b_{k+1}b_k{,}b_{k-1}\ldots b_0$$

(dies zeigt auch, dass $\mathbb{Q}_{[p]}$ mit der Lokalisierung $\mathbb{Z}_{[p]}[p^{-1}]$ übereinstimmt (Beispiel III.1.7)). Daher hat $\mathbb{Q}_{[p]}$ Ähnlichkeit mit dem Körper der formalen Laurentreihen $\mathbb{F}_p((X))$.

[3] In der Literatur wird oft die Bezeichnung $\mathbb{Q}_p$ gewählt, die bei uns bereits durch den Kreisteilungskörper belegt ist.

Beispiel III.8.21.

(i) Die Addition und Multiplikation in $\mathbb{Z}_{[p]}$ lässt sich wie im Dezimalsystem von Hand durchführen. Für $p = 3$ gilt zum Beispiel

$$12{,}1 + 2{,}21 = (p + 2p^0 + p^{-1}) + (2p^0 + 2p^{-1} + p^{-2}) = 2p + 2p^0 + p^{-2} = 22{,}01,$$
$$12{,}1 \cdot 2{,}21 = (p + 2p^0 + p^{-1})(2p^0 + 2p^{-1} + p^{-2}) = p^2 + p + 2p^0 + 2p^{-1} + p^{-2} + p^{-3} = 112{,}211.$$

(ii) Nach Bemerkung III.8.20 ist $3 \in \mathbb{Z}_{[2]}^\times$. Für $\alpha = (a_n)_n = 3^{-1}$ gilt $3a_n \equiv 1 \pmod{2^n}$ für alle $n \in \mathbb{N}$. Man prüft leicht

$$a_n \equiv \begin{cases} \frac{2^n+1}{3} & \text{falls } n \text{ ungerade,} \\ \frac{2^{n+1}+1}{3} & \text{falls } n \text{ gerade} \end{cases} \pmod{p^n}.$$

Dies liefert eine periodische 2-adische Entwicklung

$$\frac{1}{3} = 1 + 1 \cdot 2 + 0 \cdot 2^2 + 1 \cdot 2^3 + \ldots = \ldots 01011 = \ldots \overline{01}1.$$

Alternativ lässt sich das Ergebnis als geometrische Reihe interpretieren:

$$\frac{1}{3} = 1 + \sum_{k=0}^{\infty} 2^{2k+1} = 1 + \sum_{k=0}^{\infty} (2^{2k+2} - 2^{2k+1}) = \sum_{k=0}^{\infty} (-2)^k$$

(Aufgabe III.46).

Satz III.8.22. *Es existiert ein stetiger Isomorphismus $\hat{\mathbb{Q}} \to \mathbb{Q}_{[p]}$, wobei $\hat{\mathbb{Q}}$ die Vervollständigung von $\mathbb{Q}$ bzgl. ν_p ist.*

Beweis. Sei $\Gamma\colon \mathbb{Q} \to \mathbb{Q}_{[p]}$ die kanonische Einbettung. Nach Konstruktion gilt $\hat{\nu}_p(\Gamma(a)) = \nu_p(a)$ für $a \in \mathbb{Q}$. Für $\alpha = (a_n + p^n\mathbb{Z})_n \in \mathbb{Z}_{[p]}$ gilt $\hat{\nu}_p(\alpha - \Gamma(a_n)) \leq p^{-n}$. Daher liegt $\Gamma(\mathbb{Z})$ dicht in $\mathbb{Z}_{[p]}$. Nach Bemerkung III.8.20 lässt sich jedes Element in $\mathbb{Q}_{[p]}$ in der Form $p^{-k}\alpha$ mit $k \in \mathbb{N}_0$ und $\alpha \in \mathbb{Z}_{[p]}$ schreiben. Also ist $\Gamma(\mathbb{Q})$ dicht in $\mathbb{Q}_{[p]}$. Für jede Cauchyfolge $\left(\frac{\alpha_n}{\beta_n}\right)_n$ in $\mathbb{Q}_{[p]}$ existiert $p^k := \lim_{n\to\infty} \hat{\nu}_p\left(\frac{\alpha_n}{\beta_n}\right)$ nach Bemerkung III.8.4. Für ein $N \in \mathbb{N}$ gilt daher $\hat{\nu}_p(\alpha_n) = p^k \hat{\nu}_p(\beta_n)$ für alle $n \geq N$. O. B. d. A. sei $N = 1$. Nach Multiplikation mit p^{-k} können wir also $\beta_n = 1$ für alle $n \in \mathbb{N}$ annehmen.

Für $n \in \mathbb{N}$ existiert $a_n \in \mathbb{Z}$ mit $\hat{\nu}_p(\alpha_n - \Gamma(a_n)) < \frac{1}{n}$. Wie im Schritt 3 des Beweises von Satz III.8.17 zeigt man, dass $(\Gamma(a_n))_n$ eine Cauchyfolge in $\mathbb{Z}_{[p]}$ ist. Für $k \in \mathbb{N}$ sei $N_k \in \mathbb{N}$ mit $a_n \equiv a_m \pmod{p^k}$ für alle $n, m \geq N_k$. O. B. d. A. sei $k \leq N_k \leq N_l$ für $k \leq l$. Wir definieren $b_k := a_{N_k}$ für $k \in \mathbb{N}$. Dann ist $\beta := (b_k + p^k\mathbb{Z})_k \in \mathbb{Z}_{[p]}$. Für $n \geq N_k$ gilt $b_n = a_{N_n} \equiv a_n \pmod{p^k}$. Es folgt

$$\hat{\nu}_p(\beta - \alpha_n) \leq \hat{\nu}_p(\beta - \Gamma(a_n)) + \hat{\nu}_p(\Gamma(a_n) - \alpha_n) < p^{-k} + \frac{1}{n} \xrightarrow{n\to\infty} 0,$$

d. h. $(\alpha_n)_n$ konvergiert gegen β. Somit ist $\mathbb{Q}_{[p]}$ vollständig bzgl. $\hat{\nu}_p$ und Satz III.8.17(ii) liefert einen stetigen Isomorphismus $\Theta\colon \hat{\mathbb{Q}} \to \mathbb{Q}_{[p]}$. □

Bemerkung III.8.23. Im Vergleich zu $\mathbb{R}$ ist die Analysis in $\mathbb{Q}_{[p]}$ deutlich einfacher, da man zum Beispiel keine Konvergenzkriterien für Folgen benötigt (Aufgabe III.40).

Satz III.8.24 (Ostrowski)**.** *Bis auf Isomorphie sind $\mathbb{R}$ und $\mathbb{C}$ mit der euklidischen Bewertung die einzigen Körper mit vollständiger archimedischer Bewertung.*

Beweis. Sei K ein Körper mit vollständiger archimedischer Bewertung ν. Nach Lemma III.8.7 ist $\operatorname{char} K = 0$ und wir können $\mathbb{Q} \subseteq K$ annehmen.

Schritt 1: $\mathbb{R} \subsetneq K$ und $\nu(x) = |x|$ für $x \in \mathbb{R}$.
Nach Definition ist die Einschränkung von ν auf K archimedisch. Nach Satz III.8.14 existiert ein $s > 0$ mit $\nu(x) = |x|^s$ für alle $x \in \mathbb{Q}$. Sei $\tilde{\nu}(x) := \nu(x)^{1/s}$ für $x \in K$. Offenbar ist $\tilde{\nu}$ positiv definit und multiplikativ. Für $x, y \in K$ und $n \in \mathbb{N}$ gilt

$$\begin{aligned}\tilde{\nu}(x+y)^n = \tilde{\nu}\big((x+y)^n\big) &= \nu\Big(\sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}\Big)^{1/s} \le \Big(\sum_{k=0}^{n} \binom{n}{k}^s \nu(x)^k \nu(y)^{n-k}\Big)^{1/s} \\ &\le (n+1)^{1/s} \max\Big\{\binom{n}{k}^s \nu(x)^k \nu(y)^{n-k} : k = 0, \dots, n\Big\}^{1/s} \\ &= (n+1)^{1/s} \max\Big\{\binom{n}{k} \tilde{\nu}(x)^k \tilde{\nu}(y)^{n-k} : k = 0, \dots, n\Big\} \\ &\le (n+1)^{1/s} \big(\tilde{\nu}(x) + \tilde{\nu}(y)\big)^n.\end{aligned}$$

Wie in (III.8.1) folgt die Dreiecksungleichung $\tilde{\nu}(x+y) \le \tilde{\nu}(x) + \tilde{\nu}(y)$. Nach Konstruktion gilt $\nu(x) = |x|$ für $x \in \mathbb{Q}$. Da ν vollständig ist, enthält K den Grenzwert jeder Cauchyfolge aus $\mathbb{Q}$, d. h. wir können $\mathbb{R} \subsetneq K$ annehmen. Dann gilt $\nu(x) = |x|$ für $x \in \mathbb{R}$.

Schritt 2: $K \cong \mathbb{C}$.
Nach dem Fundamentalsatz der Algebra und Satz II.2.10 genügt es zu zeigen, dass $\mathbb{R} \subseteq K$ algebraisch ist. Sei $x \in K \setminus \mathbb{R}$ und

$$q\colon \mathbb{C} \to \mathbb{R}, \qquad z \mapsto \nu\big((x-z)(x-\overline{z})\big) = \nu(x^2 - (z+\overline{z})x + z\overline{z}).$$

Wegen $z + \overline{z}, z\overline{z} \in \mathbb{R}$ reicht es zu zeigen, dass q eine Nullstelle besitzt. Bezüglich der euklidischen Norm ist q stetig, denn

$$\begin{aligned}\big|\nu\big((x-z)(x-\overline{z})\big) - \nu\big((x-w)(x-\overline{w})\big)\big| &\le \nu\big(-(z-w+\overline{z}-\overline{w})x + z\overline{z} - w\overline{z} + w\overline{z} - w\overline{w}\big) \\ &\le 2|z-w|\nu(x) + |z-w|\big(|z| + |w|\big).\end{aligned}$$

Für $a, b, c \in K$ gilt bekanntlich $\nu(a-b+c) \ge \nu(a-b) - \nu(c) \ge \nu(a) - \nu(b) - \nu(c)$. Für $|z| > 3\nu(x)$ gilt daher

$$q(z) \ge |z|^2 - |z+\overline{z}|\nu(x) - \nu(x)^2 \ge |z|^2 - \frac{2}{3}|z|^2 - \frac{1}{9}|z|^2 > 2\nu(x)^2 \ge \nu(x)^2 = q(0).$$

Nach dem Satz vom Minimum nimmt q auf der kompakten Menge $\{z \in \mathbb{C} : |z| \le 3\nu(x)\}$ sein Minimum $m := \min\{q(z) : z \in \mathbb{C}\}$ an. Nehmen wir indirekt $m > 0$ an. Dann besitzt die nichtleere, kompakte Menge $M := \{z \in \mathbb{C} : q(z) = m\}$ ein Element z_0 mit größtmöglicher Norm $|z_0|$. Wir betrachten

$$\alpha := (X - z_0)(X - \overline{z_0}) + \epsilon = X^2 - (z_0 + \overline{z_0})X + |z_0|^2 + \epsilon \in \mathbb{R}[X],$$

wobei $0 < \epsilon < m$ sei. Für $s \in \mathbb{R}$ gilt $\alpha(s) = |s - z_0|^2 + \epsilon > 0$. Daher besitzt α zwei komplex-konjugierte Nullstellen $z_1, \overline{z_1}$. Das Produkt der Nullstellen ist das Absolutglied von α, d. h. $|z_1|^2 = |z_0|^2 + \epsilon > |z_0|^2$. Dies zeigt $z_1 \notin M$ und $q(z_1) > m$.

Für ungerades $n \in \mathbb{N}$ betrachten wir nun

$$\beta := (\alpha - \epsilon)^n + \epsilon^n = (X - z_0)^n (X - \overline{z_0})^n + \epsilon^n \in \mathbb{R}[X]$$

mit Nullstelle z_1. Wegen $\beta(s) = |s - z_0|^{2n} + \epsilon^n > 0$ für $s \in \mathbb{R}$ zerfällt β in paarweise komplex-konjugierte Linearfaktoren, sagen wir

$$\beta = \prod_{i=1}^{n} \big(X^2 - (z_i + \overline{z_i})X + |z_i|^2\big).$$

Für $X = x$ erhält man

$$q(z_1)m^{n-1} \leq \prod_{i=1}^{n} q(z_i) = \nu(\beta(x)) = \nu\big((x-z_0)^n(x-\overline{z_0})^n + \epsilon^n\big) \leq q(z_0)^n + \epsilon^n = m^n + \epsilon^n.$$

Dies liefert $q(z_1) \leq m + \frac{\epsilon^n}{m^{n-1}}$. Mit $n \to \infty$ ergibt sich der Widerspruch $q(z_1) \leq m$. Also ist $m = 0$ wie behauptet. □

Definition III.8.25. Sei V ein endlich-dimensionaler Vektorraum über einem Körper K mit Bewertung ν. Eine Abbildung $V \to \mathbb{R}$, $v \mapsto |v|$ heißt *Norm* von V, falls gilt:

- $|v| \geq 0$ und $|v| = 0 \iff v = 0$ (positiv definit),
- $|\lambda v| = \nu(\lambda)|v|$ (homogen),
- $|v + w| \leq |v| + |w|$ (subadditiv)

für alle $v, w \in V$ und $\lambda \in K$. Ggf. nennt man V einen *normierten Raum*. Zwei Normen $|.|_1$ und $|.|_2$ auf V heißen *äquivalent*, falls $s, t > 0$ mit $s|v|_1 \leq |v|_2 \leq t|v|_1$ für alle $v \in V$ existieren.

Beispiel III.8.26. Viele Normen lassen sich aus der Analysis übertragen. Der nächste Satz zeigt, dass wir in der Regel mit einer Norm auskommen. Auf $V = K^n$ existiert die *Maximumsnorm*

$$|v|_{\max} := \max\{\nu(v_i) : i = 1, \ldots, n\} \qquad (v = (v_1, \ldots, v_n) \in V).$$

Satz III.8.27. *Sei V ein n-dimensionaler normierter Raum über einem Körper K mit vollständiger Bewertung ν. Dann existiert ein stetiger Isomorphismus $K^n \to V$ mit stetiger Umkehrfunktion[4] bzgl. $|.|_{\max}$. Insbesondere ist V vollständig und je zwei Normen auf V sind äquivalent.*

Beweis. Sei $b_1, \ldots, b_n \in V$ eine Basis und $\beta := \max_{1 \leq i \leq n} |b_i|$. Dann definiert $f\colon K^n \to V$, $(x_i) \mapsto \sum_{i=1}^{n} x_i b_i$ einen Isomorphismus mit

$$|f(x)| \leq \sum_{i=1}^{n} |x_i b_i| \leq n \max_{1 \leq i \leq n} \{\nu(x_i)|b_i|\} \leq n\beta|x|_{\max}.$$

Wegen $|f(x) - f(y)| = |f(x-y)| \leq n\beta|x-y|_{\max}$ für $x, y \in K^n$ ist f (gleichmäßig) stetig. Nehmen wir nun indirekt an, dass eine Folge $(x^{(k)})_{k \in \mathbb{N}}$ mit

$$|x^{(k)}|_{\max} > k|f(x^{(k)})|$$

für $k \in \mathbb{N}$ existiert. Dann existiert $1 \leq i \leq n$ mit $\nu(x_i^{(k)}) = |x^{(k)}|_{\max}$ für unendlich viele k. Nach Übergang zu einer Teilfolge und Normierung können wir $x_1^{(k)} = |x^{(k)}|_{\max} = 1$ für alle $k \in \mathbb{N}$ annehmen. Indem man erneut eine Teilfolge wählt, kann man annehmen, dass alle $x^{(k)}$ auf den gleichen m Koordinaten verschwinden. Sei m dabei so groß wie möglich. Da die Vektoren $x^{(k)} - x^{(l)}$ auf mindestens $m+1$ Koordinaten verschwinden, existiert ein $\gamma > 0$ mit

$$|x^{(k)} - x^{(l)}|_{\max} \leq \gamma|f(x^{(k)}) - f(x^{(l)})| \leq \gamma\big(|f(x^{(k)})| + |f(x^{(l)})|\big) < \frac{\gamma}{k} + \frac{\gamma}{l}.$$

[4] Also ein *Homöomorphismus*

Also ist $x^{(k)}$ eine Cauchyfolge in K^n. Man zeigt leicht, dass mit K auch K^n vollständig ist bzgl. $|.|_{\max}$. Daher existiert $x := \lim_{k\to\infty} x^{(k)} \in K^n$. Wegen $x_1 = x_1^{(k)} = 1$ ist $x \neq 0$. Da f stetig ist, erhält man den Widerspruch

$$0 \neq f(x) = \lim_{k\to\infty} f(x^{(k)}) < \lim_{k\to\infty} \frac{1}{k} = 0.$$

Also existiert $\gamma > 0$ mit $|x|_{\max} \leq \gamma |f(x)|$ für alle $x \in K^n$, d. h. f^{-1} ist (gleichmäßig) stetig.

Die Vollständigkeit von K^n bzgl. $|.|_{\max}$ impliziert die Vollständigkeit von V bzgl. $|.|$. Ist $|.|'$ eine weitere Norm auf V, so existiert ein stetiger Isomorphismus $g\colon K^n \to V$ bzgl. $|.|'$ mit stetiger Umkehrfunktion. Dann ist auch $g \circ f^{-1}\colon V \to V$ ein solcher Isomorphismus. Daraus ergibt sich die Äquivalenz von $|.|$ und $|.|'$. □

Lemma III.8.28. *Seien $\nu_1, \ldots, \nu_n$ paarweise nicht-äquivalente nicht-triviale Bewertungen auf K. Dann existiert $x \in K$ mit $\nu_1(x) > 1$ und $\nu_i(x) < 1$ für $i = 2, \ldots, n$.*

Beweis. Da ν_1 und ν_2 nicht äquivalent sind, existieren $a, b \in K$ mit $\nu_1(a) < 1$, $\nu_2(a) \geq 1$ und $\nu_1(b) \geq 1$, $\nu_2(b) < 1$. Für $c := b/a \in K$ gilt dann $\nu_1(c) > 1$ und $\nu_2(c) < 1$. Damit ist der Fall $n = 2$ erledigt. Sei nun induktiv $y \in K$ mit $\nu_1(y) > 1$ und $\nu_i(y) < 1$ für $i = 3, \ldots, n$. Im Fall $\nu_2(y) \leq 1$ existiert ein $k \in \mathbb{N}$ mit

$$\nu_1(cy^k) = \nu_1(c)\nu_1(y)^k > 1, \qquad \nu_2(cy^k) \leq \nu_2(c) < 1, \qquad \nu_i(cy^k) < 1 \qquad (3 \leq i \leq n).$$

Die Behauptung gilt also für $x := cy^k$. Sei schließlich $\nu_2(y) > 1$. Für $k \in \mathbb{N}$ und $1 \leq i \leq n$ gilt wie üblich

$$|1 - \nu_i(y)^k| \leq \nu_i(1 + y^k) \leq 1 + \nu_i(y)^k.$$

Sei $z_k := \frac{y^k}{1+y^k}$. Für genügend große k ist dann

$$\nu_i(cz_k) = \nu_i(c)\frac{\nu_i(y)^k}{\nu_i(1+y^k)} \begin{cases} \geq \nu_1(c)\frac{\nu_1(y)^k}{1+\nu_1(y)^k} > 1 & \text{falls } i = 1, \\ \leq \nu_2(c)\frac{\nu_2(y)^k}{\nu_2(y)^k - 1} < 1 & \text{falls } i = 2, \\ \leq \nu_i(c)\frac{\nu_i(y)^k}{1-\nu_i(y)^k} < 1 & \text{falls } i \geq 3. \end{cases} \tag{III.8.2}$$

Wir können also $x := cz_k$ setzen. □

Satz III.8.29 (Artin-Whaples' Approximationssatz)**.** *Seien $\nu_1, \ldots, \nu_n$ paarweise nicht-äquivalente nicht-triviale Bewertungen auf K und $x_1, \ldots, x_n \in K$. Dann existiert für jedes $\epsilon > 0$ ein $x \in K$ mit $\nu_i(x - x_i) < \epsilon$ für $i = 1, \ldots, n$.*

Beweis. Nach Lemma III.8.28 existieren $y_1, \ldots, y_n \in K$ mit $\nu_i(y_i) > 1$ und $\nu_i(y_j) < 1$ für $i \neq j$. Wir definieren

$$s_k := \sum_{i=1}^{n} x_i \frac{y_i^k}{1 + y_i^k}$$

für $k \in \mathbb{N}$. Wie in (III.8.2) gilt

$$\nu_i(s_k - x_i) \leq \sum_{j\neq i} \nu_i(x_j)\frac{\nu_i(y_j)^k}{1 - \nu_i(y_j)^k} + \nu_i(x_i)\frac{1}{\nu_i(y_i^k) - 1} \xrightarrow{k\to\infty} 0$$

für $i = 1, \ldots, n$. Daher gilt die Behauptung für $x := s_k$, falls k genügend groß ist. □

Beispiel III.8.30. Seien $p_1, \ldots, p_n \in \mathbb{P}$ und $x_1, \ldots, x_n \in \mathbb{Z}$. Für jedes $\epsilon > 0$ liefert der chinesische Restsatz ein $x \in \mathbb{Z}$ mit $x \equiv x_i \pmod{p_i^{k_i}}$ für $i = 1, \ldots, n$, wobei $p_i^{-k_i} < \epsilon$. Dies bedeutet $\nu_p(x - x_i) < \epsilon$. Nimmt man eine weitere Ungleichung für die euklidische Bewertung hinzu, also $|x - x_{n+1}| < \epsilon$, so muss man $x \in \mathbb{Q}$ wählen. Der Approximationssatz kann daher als Verallgemeinerung des chinesischen Restsatz angesehen werden.

Lemma III.8.31 (Hensel)**.** *Sei K ein Körper mit ultrametrischer vollständiger Bewertung ν, Bewertungsring R und $\overline{R} := R/\mathrm{J}(R)$. Sei $\alpha \in R[X]$ und $\overline{\alpha} = \alpha_1\alpha_2 \in \overline{R}[X]$ mit $\mathrm{ggT}(\alpha_1, \alpha_2) = 1$ und α_1 normiert. Dann existieren $\beta, \gamma \in R[X]$ mit $\alpha = \beta\gamma$, $\overline{\beta} = \alpha_1$, $\overline{\gamma} = \alpha_2$ und β normiert.*

Beweis. Nach Satz III.8.9 ist R ein lokaler Ring und $\overline{R}$ ein Körper. Wir wählen zunächst $\beta_1, \gamma_1 \in R[X]$ mit $\overline{\beta_1} = \alpha_1$ und $\overline{\gamma_1} = \alpha_2$. O. B. d. A. sei β_1 normiert und $\deg(\alpha - \beta_1\gamma_1) < \deg\alpha =: n$ (d. h. α und γ_1 haben den gleichen führenden Koeffizienten). Da α_1, α_2 im euklidischen Ring $\overline{R}[X]$ teilerfremd sind, existieren $\sigma, \tau \in R[X]$ mit $\alpha_1\overline{\sigma} + \alpha_2\overline{\tau} = 1$. Die Koeffizienten von $\alpha - \beta_1\gamma_1$ und $\beta_1\sigma + \gamma_1\tau - 1$ liegen in $\mathrm{J}(R)$. Unter diesen Koeffizienten wählen wir $u \in \mathrm{J}(R)$, sodass $\nu(u)$ so groß wie möglich ist. Im Fall $u = 0$ ist $\alpha = \beta_1\gamma_1$ und wir sind fertig. Sei also $u \neq 0$. Für $k \in \mathbb{N}$ sei $(u^k) \trianglelefteq R[X]$. Für jeden Koeffizienten $s \in \mathrm{J}(R)$ von $\alpha - \beta_1\gamma_1$ oder $\beta_1\sigma + \gamma_1\tau - 1$ gilt $\nu(su^{-1}) \leq 1$, d. h. $su^{-1} \in R$ und $s = su^{-1}u \in (u)$. Daher gilt $\alpha \equiv \beta_1\gamma_1 \pmod{(u)}$ und $\beta_1\sigma + \gamma_1\tau \equiv 1 \pmod{(u)}$.

Für $k \geq 2$ konstruieren wir induktiv Polynome $\beta_k, \gamma_k \in R[X]$ mit folgenden Eigenschaften:

(a) β_k ist normiert und $\deg(\alpha - \beta_k\gamma_k) < n$,

(b) $\beta_k \equiv \beta_{k+1}$ und $\gamma_k \equiv \gamma_{k+1} \pmod{(u^k)}$,

(c) $\alpha \equiv \beta_k\gamma_k \pmod{(u^k)}$.

Seien dafür β_k, γ_k gegeben. Wähle $\delta \in R[X]$ mit $\alpha = \beta_k\gamma_k + u^k\delta$ und $\deg\delta < n$. Da β_k normiert ist, dürfen wir durch β_k mit Rest teilen ohne $R[X]$ zu verlassen. Dies liefert $\rho, \theta \in R[X]$ mit $\tau\delta = \beta_k\rho + \theta$ und $\deg\theta < \deg\beta_k$. Sei $d := \deg\gamma_1$ und $\mu, \eta \in R[X]$ mit $\sigma\delta + \gamma_k\rho = \mu + \eta X^d$ und $\deg\mu < d$. Dann erfüllen

$$\beta_{k+1} := \beta_k + u^k\theta, \qquad \gamma_{k+1} := \gamma_k + u^k\mu$$

bereits (a) und (b). Außerdem gilt

$$\delta \equiv (\beta_1\sigma + \gamma_1\tau)\delta \equiv (\beta_k\sigma + \gamma_k\tau)\delta \equiv \beta_k(\sigma\delta + \gamma_k\rho) + \gamma_k\theta \equiv \beta_k\mu + \beta_k\eta X^d + \gamma_k\theta \pmod{(u)}.$$

Hierbei ist $\deg\delta < n$, $\deg(\beta_k\mu) < \deg(\beta_k) + d = n$ und $\deg(\gamma_k\theta) < n$. Andererseits ist $\beta_k X^d$ normiert vom Grad n. Dies geht nur falls $\overline{\eta} = 0$. Es folgt

$$\beta_{k+1}\gamma_{k+1} \equiv \alpha - u^k\delta + (\beta_k\mu + \gamma_k\theta)u^k \equiv \alpha \pmod{(u^{k+1})},$$

d. h. (c) gilt für $k + 1$. Damit ist die Induktion abgeschlossen.

Nun schreiben wir $\beta_k = \sum_{j=0}^{e} b_{kj}X^j$ und $\gamma_k = \sum_{j=0}^{d} c_{kj}X^j$ mit $b_{ij}, c_{ij} \in R$. Nach Konstruktion gilt $\nu(b_{kj} - b_{lj}) \leq \nu(u)^k < 1$ für $k \leq l$ und analog für c_{kj}. Da K vollständig ist, existieren die Grenzwerte $b_j := \lim_{k\to\infty} b_{kj}$ und $c_j := \lim_{k\to\infty} c_{kj}$ in R. Wir definieren $\beta := \sum_{j=0}^{e} b_jX^j$ und $\gamma := \sum_{j=0}^{d} c_jX^j$. Mit β_k ist auch β normiert. Außerdem gilt $\overline{\beta} = \overline{\beta_1} = \alpha_1$ und $\overline{\gamma} = \overline{\gamma_1} = \alpha_2$. Wegen $\beta\gamma \equiv \beta_k\gamma_k \equiv \alpha \pmod{(u^k)}$ für alle $k \geq 1$ ist $\alpha = \beta\gamma$. □

Beispiel III.8.32. Nehmen wir an, dass $\overline{\alpha}$ wie in Hensels Lemma eine einfache Nullstelle $y \in \overline{R}$ besitzt. Dann kann man $\alpha_1 = X - y$ wählen. Also existiert ein normiertes Polynom $\beta \in R[X]$ mit $\beta \mid \alpha$ und $\overline{\beta} = \alpha_1$. Nun hat β die Form $\beta = X - x$, d. h. x ist eine Nullstelle von α mit $\overline{x} = y$.

Satz III.8.33. *Sei $p \in \mathbb{P}$ und $E \leq \mathbb{Q}_{[p]}^\times$ die Untergruppe der Einheitswurzeln. Dann gilt $E = \langle -1 \rangle \cong C_2$ falls $p = 2$ und $E \cong C_{p-1}$ falls $p > 2$.*

Beweis. Sei $\alpha = X^{p-1} - 1 \in \mathbb{Z}_{[p]}[X]$. Wegen $\mathbb{Z}_{[p]}/\mathrm{J}(\mathbb{Z}_{[p]}) \cong \mathbb{F}_p$ gilt $\overline{\alpha} = \prod_{a \in \mathbb{F}_p^\times}(X - a)$. Sei $\mathbb{F}_p^\times = \langle a \rangle$. Nach Beispiel III.8.32 besitzt α eine Nullstelle $x \in \mathbb{Z}_{[p]}$ mit $\bar{x} = a$. Offenbar ist x eine primitive Einheitswurzel der Ordnung $p - 1$. Für $p = 2$ ist offensichtlich -1 eine zweite Einheitswurzel (beachte $\operatorname{char} \mathbb{Q}_{[2]} = 0$).

Sei umgekehrt $x \in E$ mit Ordnung n. Aus $\hat{\nu}_p(x)^n = \hat{\nu}_p(x^n) = \hat{\nu}_p(1) = 1$ folgt $\hat{\nu}_p(x) = 1$ und $x \in \mathbb{Z}_{[p]}$. Also gilt $\overline{\alpha} := X^n - 1 = \prod_{k=1}^n (X - \bar{x}^k) \in \mathbb{F}_p[X]$. Sei zunächst $p \nmid n$. Wegen $\mathrm{ggT}(\overline{\alpha}, \overline{\alpha}') = 1$ gilt $\bar{x}^k \neq \bar{x}^l$ für $1 \leq k < l \leq n$. Also hat auch $\bar{x}$ Ordnung n in $\mathbb{F}_p^\times$. Dies zeigt $n \mid p - 1$. Sei nun $n = p > 2$. Dann ist $\bar{x} = \bar{x}^p = \overline{x^p} = 1$ und es existiert $y \in \mathbb{Z}_{[p]}$ mit $x = 1 + py$. Für $k \in \mathbb{N}$ folgt $x^k = \sum_{i=0}^k \binom{k}{i} y^i p^i \equiv 1 + kpy \pmod{p^2}$. Dies liefert den Widerspruch

$$0 = \frac{x^p - 1}{x - 1} = \sum_{k=0}^{p-1} x^k \equiv \sum_{k=0}^{p-1} (1 + kpy) = p + \frac{p-1}{2} p^2 y \equiv p \pmod{p^2}.$$

Sei schließlich $p = 2$ und $n = 4$. Sei wieder $x = 1 + 2y$. Dann wäre $-1 = x^2 \equiv 1 \pmod 4$. □

Lemma III.8.34. *Sei K ein Körper mit ultrametrischer vollständiger Bewertung ν. Sei $\alpha = \sum_{k=0}^n a_k X^k \in K[X]$ irreduzibel. Dann gilt $\max_{1 \leq k \leq n} \nu(a_k) = \max\{\nu(a_0), \nu(a_n)\}$.*

Beweis. Sei $s \geq 0$ minimal mit $\nu(a_s) = \max_{1 \leq k \leq n} \nu(a_k)$. Nehmen wir $s > 0$ an. Dann ist auch $\beta := a_s^{-1} \alpha \in R[X]$ irreduzibel in $K[X]$ und $\overline{\beta} = X^s \beta_1 \in \overline{R}[X]$ für ein $\beta_1 \in \overline{R}[X]$ mit $\beta_1(0) \neq 0$. Also sind X^s und β_1 teilerfremd. Nach Hensel existieren $\gamma, \delta \in R[X]$ mit $\alpha = \gamma\delta$, $\overline{\gamma} = X^s$ und $\overline{\delta} = \beta_1$. Wegen $s > 0$ muss $\deg \delta = 0$ gelten, da β irreduzibel ist. Dann ist aber auch $\deg \beta_1 = 0$ und $s = n$. □

Satz III.8.35 (Strassmann)**.** *Sei K ein Körper mit ultrametrischer Bewertung ν und Bewertungsring R. Sei $(a_n)_{n \in \mathbb{N}_0}$ eine Folge in K, sodass ein maximales $N \in \mathbb{N}_0$ mit $\nu(a_N) = \max_{n \in \mathbb{N}_0} \nu(a_n)$ existiert. Dann existieren höchstens N Elemente $x \in R$ mit $\sum_{n=0}^\infty a_n x^n = 0$.*

Beweis. Induktion nach N: Sei $N = 0$ und $x \in R$, sodass $\alpha(x) := \sum_{n=0}^\infty a_n x^n$ konvergiert. Nach Aufgabe III.40 gilt

$$\nu(a_1 x + a_2 x^2 + \ldots) \leq \max_{n \in \mathbb{N}} \nu(a_n x^n) < \nu(a_0)$$

wegen $\nu(x) \leq 1$. Aus Bemerkung III.8.4 folgt $\nu(\alpha(x)) = \nu(a_0) \neq 0$ und $\alpha(x) \neq 0$. Sei nun $N \geq 1$. Nehmen wir $a_0 = 0$ an. Dann ist $x = 0$ eine Lösung von $\alpha(x) = 0$. Jede weitere Lösung $y \neq 0$ erfüllt $b_0 + b_1 y + \ldots = 0$, wobei $b_n := a_{n+1}$ für $n \in \mathbb{N}_0$. Nach Induktion ist die Anzahl dieser y höchstens $N - 1$. Also gilt die Behauptung. Wir können daher $a_0 \neq 0$ annehmen. Für $x \in R$ mit $\alpha(x) = 0$ gilt $x \neq 0$. Wir dividieren die formale Potenzreihe $\alpha = \sum_{n=0}^\infty a_n X^n \in K[[X]]$ durch $X - x$ und erhalten $\beta = \sum_{n=0}^\infty b_n X^n \in K[[X]]$ mit $b_0 := -a_0 x^{-1}$ und $b_n := (b_{n-1} - a_n) x^{-1}$ für $n \in \mathbb{N}$. Jede Lösung $y \neq x$ von $\alpha(y) = 0$ erfüllt nun $\beta(y) = 0$. Für $k \in \mathbb{N}_0$ gilt

$$b_k = a_{k+1} + b_{k+1} x = a_{k+1} + x(a_{k+2} + b_{k+2} x) = \ldots = \sum_{n=0}^\infty a_{k+n+1} x^n.$$

Aus $\nu(x) \leq 1$ folgt $\nu(b_k) \leq \max_{n \in \mathbb{N}_0} \nu(a_{k+n+1}) \nu(x)^n < \nu(a_N)$ für $k \geq N$. Daher ist $\nu(b_{N-1}) = \nu(a_N + b_N x) = \max\{\nu(a_N), \nu(b_N x)\} = \nu(a_N)$. Für $k < N - 1$ gilt schließlich

$$\nu(b_k) \leq \max_{n \in \mathbb{N}_0} \nu(a_{k+n+1}) \nu(x)^n \leq \nu(a_N) = \nu(b_{N-1}).$$

Also ist $\nu(b_{N-1}) = \max_{n\in\mathbb{N}_0} \nu(b_n)$. Nach Induktion ist die Anzahl der $y \in R$ mit $\beta(y) = 0$ höchstens $N - 1$. □

Beispiel III.8.36.

(i) Sei $a_0 := 0$ und $a_n := \frac{2^n}{n} \in \mathbb{Q}_{[2]}$ für $n \in \mathbb{N}$. Dann gilt $N = 2$ mit den Bezeichnungen aus Satz III.8.35. Nach Aufgabe III.45 sind $x = 0, 1 \in \mathbb{Z}_{[2]}$ die einzigen Lösungen von $\sum a_n x^n = 0$.

(ii) Sei $\alpha = X^N - p \in \mathbb{Z}_{[p]}[X]$ mit $N \geq 2$. Wegen $\langle \hat{\nu}_p(\mathbb{Q}_{[p]})\rangle = \langle p^{-1}\rangle = \langle \nu_p(p)\rangle$ besitzt α keine Nullstelle in $\mathbb{Z}_{[p]}$. Daher ist die Abschätzung in Straßmanns Satz im Allgemeinen nicht optimal.

Bemerkung III.8.37. Wir hatten (zum Beispiel in Aufgabe III.35) bereits die Norm-Abbildung $N\colon L \to K$, $x \mapsto \prod_{\sigma\in\mathrm{Gal}(L|K|)} \sigma(x)$ für Galois-Erweiterungen $K \subseteq L$ benutzt. Wir führen nun eine allgemeinere Konstruktion ein.

Definition III.8.38. Sei $K \subseteq L$ eine endliche Körpererweiterung. Für $x \in L$ definiert $t_x\colon L \to L$, $y \mapsto xy$ eine K-lineare Abbildung. Wir nennen $N_K^L\colon L \to K$, $x \mapsto \det(t_x)$ die *Norm-Abbildung* von L bzgl. K.[5]

Lemma III.8.39. *Für endliche Körpererweiterungen $K \subseteq L \subseteq M$ gilt:*

(i) Für $x \in K$ ist $N_K^L(x) = x^{|L:K|}$.

(ii) Für $x, y \in L$ ist $N_K^L(xy) = N_K^L(x)N_K^L(y)$.

(iii) Für $x \in L$ ist $N_K^L(x) = N_K^{K(x)}(x)^{|L:K(x)|}$.

(iv) Für das Minimalpolynom μ_x über K gilt $N_K^L(x) = (-1)^{|L:K|}\mu_x(0)^{|L:K(x)|}$.

(v) $N_K^M = N_K^L \circ N_L^M$.

(vi) Ist $K \subseteq L$ eine Galois-Erweiterung, so gilt $N_K^L(x) = \prod_{\sigma\in\mathrm{Gal}(L|K)|} \sigma(x)$.

Beweis.

(i) Die Matrix der Abbildung t_x bzgl. einer beliebigen Basis von L ist $x1_n$, wobei $n = |L : K|$. Daher ist $N_K^L(x) = \det(t_x) = x^n$.

(ii) Offenbar gilt $t_{xy} = t_x \circ t_y$ und $N_K^L(xy) = \det(t_{xy}) = \det(t_x)\det(t_y) = N_K^L(x)N_K^L(y)$.

(iii) Sei $b_1, \ldots, b_n \in K(x)$ eine K-Basis von $K(x)$ und $c_1, \ldots, c_m \in L$ eine $K(x)$-Basis von L. Nach dem Beweis des Gradsatz ist $B := \{b_i c_j : 1 \leq i \leq n, 1 \leq j \leq m\}$ eine K-Basis von L. Sei $A \in K^{n\times n}$ die Matrix von $t'_x\colon K(x) \to K(x)$ bzgl. $b_1, \ldots, b_n$. Offenbar ist dann $\mathrm{diag}(A, \ldots, A) \in K^{nm\times nm}$ die Matrix von $t_x\colon L \to L$ bzgl. B. Dies zeigt $N_K^L(x) = \det(A)^m = N_K^{K(x)}(x)^{|L:K(x)|}$.

(iv) Nach Cayley-Hamilton ist μ_x ein Teiler des charakteristischen Polynoms von t_x. Wegen $d := \deg \mu_x = |K(x) : K|$ ist μ_x das charakteristische Polynom von $t'_x\colon K(x) \to K(x)$. Aus (iii) folgt

$$\begin{aligned} N_K^L(x) = N_K^{K(x)}(x)^{|L:K(x)|} = \det(t'_x)^{|L:K(x)|} &= \big((-1)^d \det(X\,\mathrm{id} - t'_x)(0)\big)^{|L:K(x)|} \\ = \big((-1)^d \mu_x(0)\big)^{|L:K(x)|} &= (-1)^{|L:K|}\mu_x(0)^{|L:K(x)|}. \end{aligned}$$

[5] Die Norm-Abbildung sollte nicht mit den Normen aus Definition III.8.25 verwechselt werden.

(v) Nach (iii) ist

$$N_K^M(x) = N_K^{K(x)}(x)^{|M:K(x)|} = N_K^{L(x)}(x)^{|M:L(x)|}, \qquad N_K^L\big(N_L^M(x)\big) = N_K^L\big(N_L^{L(x)}(x)\big)^{|M:L(x)|}$$

für $x \in M$. Wir können daher $M = L(x)$ annehmen. Sei $d := |L(x) : L|$. Dann ist $1, x, \ldots, x^{d-1}$ eine L-Basis von $L(x)$. Sei $b_1, \ldots, b_n \in L$ eine K-Basis von L. Die Matrix von $t_x \colon L(x) \to L(x)$ bzgl. der Basis

$$\{b_1, \ldots, b_n, b_1x, \ldots, b_nx, \ldots, b_1x^{d-1}, \ldots, b_nx^{d-1}\}$$

hat die Form

$$A := \begin{pmatrix} 0 & \cdots & 0 & A_1 \\ 1_n & \ddots & \vdots & \vdots \\ & \ddots & 0 & A_{d-1} \\ 0 & & 1_n & A_d \end{pmatrix}.$$

Nach $n(d-1)$ Zeilenvertauschungen erhält man $\det A = (-1)^{n(d-1)} \det(A_1)$. Sei $\mu_x = X^d + \lambda_{d-1}X^{d-1} + \ldots + \lambda_0 \in L[X]$ das Minimalpolynom von x über L. Dann gilt $x^d = -\lambda_{d-1}x^{d-1} - \ldots - \lambda_0$. Daher ist A_1 die Matrix von $t_{-\lambda_0} \colon L \to L$. Nach (iv) gilt $N_L^{L(x)}(x) = (-1)^d \mu_x(0) = (-1)^{d+1}(-\lambda_0)$ und

$$N_K^L(N_L^{L(x)}(x)) \overset{\text{(i),(ii)}}{=} (-1)^{n(d+1)} N_K^L(-\lambda_0) = (-1)^{n(d+1)} \det(A_1) = (-1)^{2nd} \det A = N_K^{L(x)}(x).$$

(vi) Bekanntlich permutiert $\mathrm{Gal}(L|K)$ die Nullstellen von μ_x. Daher gilt

$$\mu_x^{|L:K(x)|} = \prod_{\sigma \in \mathrm{Gal}(L|K)} (X - \sigma(x))$$

und

$$N_K^L(x) \overset{\text{(iv)}}{=} (-1)^{|L:K|} \mu_x(0)^{|L:K(x)|} = \prod_{\sigma \in \mathrm{Gal}(L|K)} \sigma(x). \qquad \square$$

Satz III.8.40. *Sei K ein Körper mit vollständiger Bewertung ν. Für jede endliche Körpererweiterung $K \subseteq L$ existiert genau eine Bewertung $\tilde{\nu}$ auf L, die ν fortsetzt. Außerdem ist $\tilde{\nu}$ vollständig und für $x \in L$ gilt*

$$\boxed{\tilde{\nu}(x) = \sqrt[|L:K|]{\nu\big(N_K^L(x)\big)}.}$$

Beweis. Die Abbildung $\tilde{\nu} \colon L \to L$, $x \mapsto \sqrt[|L:K|]{\nu(N_K^L(x))}$ ist nach Lemma III.8.39 eine positiv definite multiplikative Fortsetzung von ν.

Fall 1: ν ist trivial.
Hier ist auch $\tilde{\nu}$ trivial und vollständig. Angenommen ν' ist eine nicht-triviale Fortsetzung von ν. Sei $x \in L^\times$ mit $\tilde{\nu}(x) \neq 1$, o. B. d. A. $\tilde{\nu}(x) > 1$ (ersetze notfalls x durch x^{-1}). Wegen $|L : K| < \infty$ ist x algebraisch über K. Dies widerspricht Aufgabe III.39 angewendet auf das Minimalpolynom μ_x. Also ist $\nu' = \tilde{\nu}$ die einzige Fortsetzung von ν.

Fall 2: ν ist archimedisch.
Nach Ostrowski ist $K \in \{\mathbb{R}, \mathbb{C}\}$ und $\nu(x) = |x|^s$ für ein $s > 0$ und $x \in K$. Da $\mathbb{C}$ algebraisch abgeschlossen ist, können wir $(K, L) = (\mathbb{R}, \mathbb{C})$ annehmen. In der Tat ist

$$\tilde{\nu}(z) = \sqrt{\nu(N_{\mathbb{R}}^{\mathbb{C}}(z))} = \sqrt{z\bar{z}}^s = |z|^s$$

für $z \in \mathbb{C}$ zur euklidischen Bewertung auf $\mathbb{C}$ äquivalent. Sei ν' eine weitere Fortsetzung von ν. Nach Satz III.8.27 ist ν' als Norm zu $\tilde{\nu}$ äquivalent. Insbesondere definieren $\tilde{\nu}$ und ν' die gleichen offenen Mengen. Nach Lemma III.8.12 sind $\tilde{\nu}$ und ν' auch als Bewertungen äquivalent. Sei $t > 0$ mit $\nu'(z) = \tilde{\nu}(z)^t$ für alle $z \in \mathbb{C}$. Wegen $2^s = \tilde{\nu}(2) = \nu(2) = \nu'(2) = 2^{st}$ ist $t = 1$ und $\nu' = \tilde{\nu}$.

Fall 3: ν ist ultrametrisch.
Wir zeigen zuerst, dass $\tilde{\nu}$ die ultrametrische Ungleichung erfüllt. Sei $x, y \in L^\times$ mit $\tilde{\nu}(x) \geq \tilde{\nu}(y)$. Wegen $N_K^L(x+y) = N_K^L(x) N_K^L(1+\frac{y}{x})$ genügt es die Aussage $\tilde{\nu}(x) \leq 1 \Rightarrow \tilde{\nu}(1+x) \leq 1$ zu zeigen. Nach Lemma III.8.39 ist dies äquivalent zu

$$\nu\big(N_K^{K(x)}(x)\big) \leq 1 \implies \nu\big(N_K^{K(x)}(1+x)\big) \leq 1.$$

Für das Minimalpolynom $\mu_x = \sum_{k=0}^d a_k X^k \in K[X]$ gilt $\nu(a_0) = \nu((-1)^d a_0) = \nu\big(N_K^{K(x)}(x)\big) \leq 1$ nach Lemma III.8.39. Aus Lemma III.8.34 folgt $\max_{0\leq k\leq d} \nu(a_k) = \max\{\nu(a_0), 1\} = 1$. Offenbar ist $\mu_x(X-1)$ das Minimalpolynom von $1+x$. Daher gilt

$$\nu\big(N_K^{K(x)}(1+x)\big) = \nu(\mu_x(-1)) = \nu\Big(\sum_{k=0}^d (-1)^k a_k\Big) \leq \max_{0\leq k\leq d} \nu(a_k) \leq 1$$

wie gewünscht. Damit ist $\tilde{\nu}$ eine Bewertung auf L, die ν fortsetzt. Die Eindeutigkeit von $\tilde{\nu}$ zeigt man wie in Fall 2 mit Hilfe von Lemma III.8.12. Daraus ergibt sich auch die Vollständigkeit von $\tilde{\nu}$. □

Folgerung III.8.41. *Sei K ein Körper mit vollständiger Bewertung ν. Dann existiert genau eine Bewertung $\tilde{\nu}$ des algebraischen Abschluss $\overline{K}$, die ν fortsetzt.*

Beweis. Für jede endliche Körpererweiterung $K \subseteq L$ mit $L \subseteq \overline{K}$ sei ν_L die nach Satz III.8.40 eindeutig bestimmte Fortsetzung von ν. Für $x, y \in L$ ist $|K(x,y) : K| < \infty$, da $K \subseteq \overline{K}$ algebraisch ist. Außerdem gilt $\nu_{K(x)}(x) = \mu_{K(x,y)}(x)$. Dies zeigt, dass $\tilde{\nu}\colon \overline{K} \to \mathbb{R}$, $x \mapsto \nu_{K(x)}(x)$ eine Bewertung von $\overline{K}$ ist, die ν fortsetzt. Ist ν' eine weitere Fortsetzung von ν, so müssen $\tilde{\nu}$ und ν' auf $K(x)$ für alle $x \in \overline{K}$ übereinstimmen. Daher gilt $\nu' = \tilde{\nu}$. □

Bemerkung III.8.42.

(i) Sei $K := \mathbb{Q}_{[p]}$ und $\tilde{\nu}_p$ die eindeutige Fortsetzung von $\hat{\nu}_p$ nach $\overline{K}$.[6] Mit ν_p ist auch $\tilde{\nu}_p$ ultrametrisch. Nehmen wir an, dass $\tilde{\nu}_p$ diskret ist. Dann existiert $x \in \overline{K}$ mit $\langle \tilde{\nu}_p(x) \rangle = \tilde{\nu}_p(\overline{K}^\times)$. Da $\overline{K}$ algebraisch abgeschlossen ist, existiert $y \in \overline{K}$ mit $y^2 = x$. Außerdem existiert $a \in \mathbb{Z}$ mit $\tilde{\nu}_p(y) = \tilde{\nu}_p(x)^a$. Damit hat man den Widerspruch $\tilde{\nu}_p(x) = \tilde{\nu}_p(y)^2 = \tilde{\nu}_p(x)^{2a}$. Also ist $\tilde{\nu}_p$ nicht diskret.

(ii) Im Gegensatz zu Satz III.8.40 ist $\tilde{\nu}_p$ nicht vollständig (Aufgabe III.49). Wir zeigen, dass die algebraische Abgeschlossenheit erhalten bleibt, wenn man erneut zur Vervollständigung übergeht (Satz III.8.45).

Lemma III.8.43 (Krasner)**.** *Sei K ein Körper mit vollständiger ultrametrischer Bewertung ν. Sei $\overline{K}$ der algebraische Abschluss von K und $\tilde{\nu}$ die Fortsetzung von ν auf $\overline{K}$. Sei $\alpha \in K[X]$ irreduzibel und separabel mit Nullstellen $x_1, \ldots, x_d \in \overline{K}$. Sei*

$$r := \min_{i \neq j} \tilde{\nu}(x_i - x_j).$$

Für $y \in \overline{K}$ mit $\tilde{\nu}(x_1 - y) < r$ gilt $K(x_1) \subseteq K(y)$.

[6] Nach Konstruktion sind K, $\overline{K}$ und $\mathbb{C}$ gleichmächtig zur Potenzmenge von $\mathbb{N}$. Aus Satz A.6.4 folgt daher $\overline{K} \cong \mathbb{C}$.

Beweis. Sei $L := K(y)$. Der Zerfällungskörper $M \subseteq \overline{K}$ von α über L ist nach Artins Satz I.10.9 eine Galois-Erweiterung, da α separabel ist. Die Eindeutigkeit von $\tilde{\nu}$ auf M zeigt $\tilde{\nu}(\sigma(z)) = \tilde{\nu}(z)$ für alle $z \in M$ und $\sigma \in G := \mathrm{Gal}(M|L)$. Insbesondere ist

$$\tilde{\nu}(\sigma(x_1) - y) = \tilde{\nu}(x_1 - \sigma^{-1}(y)) = \tilde{\nu}(x_1 - y) < r$$

und

$$\tilde{\nu}(x_1 - \sigma(x_1)) = \tilde{\nu}(x_1 - y + y - \sigma(x_1)) \leq \max\{\tilde{\nu}(x_1 - y), \tilde{\nu}(y - \sigma(x_1))\} < r.$$

Nach Definition von r geht dies nur falls $\sigma(x_1) = x_1$. Insgesamt ist $x_1 \in M^G = L = K(y)$ wie behauptet. □

Folgerung III.8.44. *Mit den gleichen Voraussetzungen wie in Lemma III.8.43 sei $\alpha = \sum_{k=0}^{d} a_k X^k \in K[X]$. Dann existiert ein $\epsilon > 0$ mit folgender Eigenschaft: Jedes normierte Polynom $\beta = \sum_{k=0}^{d} b_k X^k \in K[X]$ mit $\nu(a_k - b_k) < \epsilon$ für $k = 0, \ldots, d$ ist irreduzibel.*

Beweis. Sei $m := \max_{0 \leq k \leq d} \nu(a_k)$ und $\epsilon := \min\{1, r^d(m+1)^{-d}\} > 0$. Sei β wie angegeben mit Nullstelle $y \in \overline{K}$. Nach Aufgabe III.39 gilt

$$\tilde{\nu}(y) \leq \max_{0 \leq k \leq d} \nu(b_k) \leq \max_{0 \leq k \leq d} \nu(a_k) + \max_{0 \leq k \leq d} \nu(a_k - b_k) < m + \epsilon \leq m + 1$$

und

$$\prod_{k=0}^{d} \tilde{\nu}(y - x_k) = \tilde{\nu}(\alpha(y)) = \tilde{\nu}((\alpha - \beta)(y)) \leq \max_{0 \leq k \leq d} \nu(a_k - b_k)\tilde{\nu}(y)^k < \epsilon(m+1)^d.$$

Also existiert ein k mit $\tilde{\nu}(y - x_k) < \sqrt[d]{\epsilon}(m+1) \leq r$. Aus Krasners Lemma folgt $K(x_k) \subseteq K(y)$. Andererseits ist $|K(y) : K| \leq \deg \beta = d = |K(x_k) : K|$. Dies zeigt $K(x_k) = K(y)$ und β ist irreduzibel. □

Satz III.8.45 (Kürschák)**.** *Sei K ein algebraisch abgeschlossener Körper mit Bewertung ν. Dann ist auch die Vervollständigung $\hat{K}$ bzgl. ν algebraisch abgeschlossen.*

Beweis. Ist ν archimedisch, so ist $\mathbb{R} \subseteq \hat{K} \subseteq \mathbb{C}$ nach Ostrowski. Da $X^2 + 1$ bereits eine Nullstelle im algebraisch abgeschlossenen Körper K besitzt, kann der Fall $\hat{K} \cong \mathbb{R}$ nicht auftreten. Somit ist $\hat{K} \cong \mathbb{C}$ algebraisch abgeschlossen.

Sei nun ν ultrametrisch. Wir zeigen zunächst, dass $\hat{K}$ vollkommen ist (Definition I.11.19). Dafür können wir $\mathrm{char}\, K = p > 0$ annehmen. Sei $x \in \hat{K}$. Da K dicht in $\hat{K}$ liegt, ist x der Grenzwert einer Folge aus K, etwa $x = \lim_{n \to \infty} x_n$. Da K algebraisch abgeschlossen ist, existieren $y_n \in K$ mit $y_n^p = x_n$. Wegen

$$\nu(y_k - y_l)^p = \nu\big((y_k - y_l)^p\big) = \nu(y_k^p - y_l^p) = \nu(x_k - x_l)$$

ist auch (y_n) eine Cauchyfolge. Für $y := \lim_{n \to \infty} y_n \in \hat{K}$ gilt offenbar $y^p = x$. Also ist $\hat{K}$ vollkommen.

Angenommen $\hat{K}$ ist nicht algebraisch abgeschlossen. Dann existiert ein irreduzibles Polynom $\alpha \in \hat{K}[X]$ vom Grad $d > 1$. Nach Beispiel II.3.3 ist α separabel. Da K dicht in $\hat{K}$ liegt, finden wir ein Polynom $\beta \in K[X]$ dessen Koeffizienten beliebig nah an den entsprechenden Koeffizienten von α liegen. Nach Folgerung III.8.44 können wir erreichen, dass β irreduzibel ist und ebenfalls Grad d hat. Dann wäre K aber nicht algebraisch abgeschlossen. □

Beispiel III.8.46. Sei K die Vervollständigung von $\overline{\mathbb{Q}_{[p]}}$. Dann ist K sowohl algebraisch abgeschlossen als auch vollständig. Sei R der Bewertungsring von K und $\overline{R} := R/\mathrm{J}(R)$. Sei $\alpha \in \overline{R}[X] \setminus \overline{R}$. Dann existiert $\beta \in R[X] \setminus R$ mit $\overline{\beta} = \alpha$. Da K algebraisch abgeschlossen ist, besitzt β eine Nullstelle $x \in K$. Nach Aufgabe III.39 ist $x \in R$ und $\overline{x}$ ist eine Nullstelle von α. Dies zeigt, dass $\overline{R}$ ebenfalls algebraisch abgeschlossen ist.

Bemerkung III.8.47. Sei K ein Zahlkörper vom Grad $n := |K : \mathbb{Q}|$. Wegen $\operatorname{char} K = 0$ existieren nach Aufgabe II.18 genau n (injektive) Homomorphismen $\sigma\colon K \to \mathbb{C}$. Im Fall $\sigma(K) \subseteq \mathbb{R}$ nennt man σ eine *reelle Einbettung* von K und anderenfalls eine *komplexe Einbettung*. Die komplexen Einbettungen treten in Paaren der Form $(\sigma, \overline{\sigma})$ auf, wobei $\overline{\sigma}(x) := \overline{\sigma(x)}$ für $x \in K$ gilt.

Lemma III.8.48. *Sei K ein Zahlkörper und $\sigma, \tau\colon K \to \mathbb{C}$ Einbettungen mit $|\sigma(x)| = |\tau(x)|$ für alle $x \in K$. Dann gilt $\sigma \in \{\tau, \overline{\tau}\}$.*

Beweis. Sei $\gamma := \sigma \circ \tau^{-1}\colon \tau(K) \to \sigma(K)$. Für $x, y \in K$ gilt

$$|\sigma(x) - \sigma(y)| = |\sigma(x - y)| = |\tau(x - y)| = |\tau(x) - \tau(y)|.$$

Dies zeigt, dass γ stetig bzgl. der euklidischen Bewertung ist. Man kann nun γ zur Vervollständigung $\widehat{\tau(K)}$ fortsetzen, indem man $\hat{\gamma}(x) := \lim_{n\to\infty} \gamma(x_n)$ für jede Cauchyfolge $(x_n)_n$ in $\tau(K)$ definiert (dies ist wohldefiniert, da γ Nullfolgen auf Nullfolgen abbildet). Man zeigt leicht, dass $\hat{\gamma}\colon \widehat{\tau(K)} \to \widehat{\sigma(K)}$ ein Isomorphismus ist. Nach Ostrowski gilt $\widehat{\tau(K)} = \widehat{\sigma(K)} \in \{\mathbb{R}, \mathbb{C}\}$. Da $\mathbb{Q}$ im Fixkörper von γ liegt, liegt $\mathbb{R}$ im Fixkörper von $\hat{\gamma}$. Daraus folgt $\hat{\gamma} = \mathrm{id}$ oder $\hat{\gamma}$ ist die komplexe Konjugation auf $\mathbb{C}$. □

Satz III.8.49. *Sei K ein Zahlkörper. Seien $\sigma_1, \ldots, \sigma_r$ die reellen Einbettungen von K und seien $\tau_1, \ldots, \tau_s$ Repräsentanten für die Paare von komplexen Einbettungen. Dann ist jede archimedische Bewertung von K zu genau einer der Bewertungen $x \mapsto |\sigma_i(x)|$ oder $x \mapsto |\tau_i(x)|$ äquivalent.*

Beweis. Sei ν eine archimedische Bewertung von K. Nach Ostrowski existiert ein Homomorphismus $\gamma\colon \hat{K} \to \mathbb{C}$ und $s > 0$ mit $\hat{\nu}(x) = |\gamma(x)|^s$ für alle $x \in K$. Also ist ν zu einer der angegebenen Bewertungen äquivalent. Seien nun σ und τ beliebige Einbettungen von K und $s > 0$ mit $|\sigma(x)| = |\tau(x)|^s$ für alle $x \in K$. Für $x = 2$ erhält man $2 = |\sigma(2)| = |\tau(2)|^s = 2^s$ und $s = 1$. Aus Lemma III.8.48 folgt nun $\sigma \in \{\tau, \overline{\tau}\}$. Also sind die angegebenen Bewertungen paarweise nicht-äquivalent. □

Bemerkung III.8.50. Die ultrametrischen Bewertungen eines Zahlkörpers K entstehen durch Wahl eines Primideals $P \trianglelefteq \mathbb{Z}_K$ wie in Beispiel III.8.3 beschrieben.

Lemma III.8.51. *Sei K ein Körper mit ultrametrischer Bewertung ν und Bewertungsring R. Sei V ein K-Vektorraum und $W \subseteq V$ ein endlich-erzeugter R-Modul. Dann existieren linear unabhängige Elemente $b_1, \ldots, b_n \in W$ über K mit $W = Rb1 + \ldots + Rb_n$.*

Beweis. Nach Satz III.8.9 ist $P := \mathrm{J}(R)$ ein maximales Ideal. Wie im Beweis von Satz II.9.7 können wir W/PW als R/P-Vektorraum betrachten. Da W endlich erzeugt ist, existiert eine Basis $b_1 + PW, \ldots, b_n + PW$ von W/PW über R/P. Folglich ist $W = Rb_1 + \ldots + Rb_n + PW$. Als Vektorraum ist W/PW halbeinfach und $\mathrm{J}(W) \subseteq PW$. Nakayamas Lemma liefert daher $R = Rb_1 + \ldots + Rb_n$. Angenommen es existieren $\lambda_1, \ldots, \lambda_n \in K$ (nicht alle 0) mit $\lambda_1 b_1 + \ldots + \lambda_n b_n = 0$. Sei $\mu := \max_{1 \le i \le n} \nu(\lambda_i) > 0$. Dann gilt $\frac{\lambda_1}{\mu} b_1 + \ldots + \frac{\lambda_n}{\mu} b_n + PW = 0$ in W/PW und es folgt $\frac{\lambda_i}{\mu} \in P$ für $i = 1, \ldots, n$. Damit hat man den Widerspruch $\nu(\lambda_i) < \mu$ für $i = 1, \ldots, n$. Also sind $b_1, \ldots, b_n$ linear unabhängig über K. □

Bemerkung III.8.52. Zu jeder endlichen Gruppe G existiert nach Satz II.13.44 ein Zahlkörper K, der Zerfällungskörper für G ist. Sei $\Delta\colon G \to \mathrm{GL}(n,K)$ eine Darstellung und $V := K^n$ der entsprechende KG-Modul. Sei $p \in \mathbb{P}$ und $P \trianglelefteq \mathbb{Z}_K$ ein maximales Ideal mit $p \in P$. Die P-adische Bewertung auf K ist ultrametrisch mit Bewertungsring R. Sei $e_1, \ldots, e_n \in K^n$ die Standardbasis und $W \subseteq V$ der von den Elementen ge_i ($g \in G$, $1 \leq i \leq n$) erzeugte R-Modul. Nach Lemma III.8.51 existieren linear unabhängige Elemente $b_1, \ldots, b_n \in W$ über K mit $W = Rb_1 + \ldots + Rb_n$. Wegen $e_1, \ldots, e_n \in W$ ist $b_1, \ldots, b_n$ eine K-Basis von V. Für $g \in G$ ist $gb_i \in W$ eine R-Linearkombination von $b_1, \ldots, b_n$. Durch den Basiswechsel $\{e_1, \ldots, e_n\} \to \{b_1, \ldots, b_n\}$ erhält man eine zu Δ ähnliche Darstellung $\Gamma\colon G \to \mathrm{GL}(n,R)$. Mit der Reduktion modulo P entsteht eine Darstellung $\overline{\Gamma}\colon G \to \mathrm{GL}(n, R/P)$ mit Einträgen in dem endlichen Körper R/P der Charakteristik p. Ersetzt man K durch den Körper aus Beispiel III.8.46, so erreicht man, dass K und R/P algebraisch abgeschlossen sind.

9 Allgemeine Galois-Theorie

Bemerkung III.9.1. In diesem Abschnitt entwickeln wir drei Erweiterungen des Hauptsatzes der Galois-Theorie: für gewisse Algebren, für Schiefkörper und für unendliche Körpererweiterungen.

Definition III.9.2. Sei $K \subseteq L$ eine Körpererweiterung und $G \leq \mathrm{Gal}(L|K)$.

- Für eine G-Menge S sei

$$\mathrm{Hom}_G(S, L) := \big\{\varphi\colon S \to L : \forall s \in S, g \in G : \varphi({}^g s) = g(\varphi(s))\big\}.$$

- Zwei G-Mengen S und T nennt man *isomorph*, falls eine Bijektion $\varphi\colon S \to T$ mit ${}^g\varphi(s) = \varphi({}^g s)$ für alle $g \in G$ und $s \in S$ existiert.
- Für zwei K-Algebren A und B sei $\mathrm{Alg}_K(A, B)$ die Menge der Algebra-Homomorphismen $A \to B$.
- Eine K-Algebra A heißt *L-separiert*, wenn für je zwei verschiedene Elemente $x, y \in A$ ein $f \in \mathrm{Alg}_K(A, L)$ mit $f(x) \neq f(y)$ existiert.

Bemerkung III.9.3.

(i) Man zeigt leicht, dass $\mathrm{Hom}_G(S, L)$ mit den komponentenweisen Verknüpfungen $(\alpha \mathbin{\dot{+}} \beta)(s) = \alpha(s) \mathbin{\dot{+}} \beta(s)$ und $(\lambda\alpha)(s) = \lambda\alpha(s)$ für $\alpha, \beta \in \mathrm{Hom}_G(S, L)$, $s \in S$ und $\lambda \in K$ eine K-Algebra ist.

(ii) Sei nun $K \subseteq L$ eine Galois-Erweiterung und $G := \mathrm{Gal}(L|K)$. Sei $R \subseteq S$ ein Repräsentantensystem für die Bahnen von G auf S. Für $r \in R$ sei G_r der Stabilisator von r. Für $g \in G_r$ und $\varphi \in \mathrm{Hom}_G(S, L)$ gilt $g(\varphi(r)) = \varphi({}^g r) = \varphi(r) \in L^{G_r}$. Sind umgekehrt $x_r \in L^{G_r}$ für $r \in R$ gegeben, so existiert genau ein $\varphi \in \mathrm{Hom}_G(S, L)$ mit $\varphi(r) = x_r$ für $r \in R$. Dies zeigt

$$\dim_K \mathrm{Hom}_G(S, L) = \sum_{r \in R} |L^{G_r} : K| = \sum_{r \in R} |G : G_r| = \sum_{r \in R} |{}^G r| = |S|.$$

(iii) Jede L-separierte K-Algebra ist kommutativ, denn für $x, y \in A$ und $f \in \mathrm{Alg}_K(A, L) =: S$ gilt $f(xy) = f(x)f(y) = f(y)f(x) = f(yx)$. Durch ${}^g\varphi(a) := g(\varphi(a))$ für $g \in G$, $a \in A$ und $\varphi \in S$ wird S eine G-Menge. Wie in Dedekinds Lemma (Lemma I.14.1) zeigt man, dass S linear unabhängig über L ist. Insbesondere gilt $|S| \leq \dim_K A$.

Satz III.9.4 (Allgemeine Galois-Korrespondenz)**.** *Sei $K \subseteq L$ eine Galois-Erweiterung und $G := \mathrm{Gal}(L|K)$. Dann induzieren die Abbildungen $S \mapsto \mathrm{Hom}_G(S, L)$ und $A \mapsto \mathrm{Alg}_K(A, L)$ zueinander inverse Bijektionen zwischen der Menge der Isomorphieklassen von endlichen G-Mengen und der Menge der K-Isomorphieklassen von endlich-dimensionalen L-separierten K-Algebren.*

Beweis. Sei S eine endliche G-Menge und $A := \mathrm{Hom}_G(S, L)$. Nach Bemerkung III.9.3 ist $\dim_K A = |S| < \infty$. Seien $\alpha, \beta \in A$ und $s \in S$ mit $\alpha(s) \neq \beta(s)$. Offenbar ist die Abbildung $\Gamma_s \colon A \to L$, $\varphi \mapsto \varphi(s)$ ein Homomorphismus von K-Algebren mit $\Gamma_s(\alpha) \neq \Gamma_s(\beta)$. Daher ist A L-separiert. Sei $T := \mathrm{Alg}_K(A, L)$ und $\Gamma \colon S \to T$, $s \mapsto \Gamma_s$. Seien $s, s' \in S$ mit $s \neq s'$. Sind s und s' in verschiedenen Bahnen von G, so existiert nach Bemerkung III.9.3 ein $\varphi \in A$ mit

$$\Gamma_s(\varphi) = \varphi(s) = 0 \neq 1 = \varphi(s') = \Gamma_{s'}(\varphi).$$

Anderenfalls wählen wir $g \in G \setminus G_s$ mit ${}^g s = s'$ und $x \in L^{G_s} \setminus L^g$. Dann existiert ein $\varphi \in A$ mit $\varphi(s) = x$ und $\varphi(s') = {}^g\varphi(s) = {}^g x \neq x = \varphi(s)$. In beiden Fällen gilt $\Gamma_s \neq \Gamma_{s'}$ und Γ ist injektiv. Wegen $|T| \leq \dim_K A = |S|$ ist Γ auch surjektiv. Für $g \in G$ und $s \in S$ ist schließlich $\Gamma_{{}^g s}(\varphi) = \varphi({}^g s) = {}^g\varphi(s) = {}^g\Gamma_s(\varphi)$ und $\Gamma({}^g s) = {}^g\Gamma(s)$. Dies zeigt, dass S und T isomorphe G-Mengen sind.

Sei umgekehrt A eine endlich-dimensionale L-separierte K-Algebra. Nach Bemerkung III.9.3 ist $S := \mathrm{Alg}_K(A, L)$ eine endliche G-Menge. Sei $B := \mathrm{Hom}_G(S, L)$ und $\Gamma \colon A \to B$, $a \mapsto \Gamma_a$ mit $\Gamma_a(f) := f(a)$ für $f \in S$. Für $g \in G$ gilt

$$\Gamma_a({}^g f) = {}^g f(a) = g(f(a)) = g(\Gamma_a(f)) = {}^g\Gamma_a(f).$$

Daher ist Γ wohldefiniert. Wie üblich ist Γ ein Homomorphismus von K-Algebren. Für verschiedene $a, b \in A$ existiert ein $f \in S$ mit $f(a) \neq f(b)$, da A L-separiert ist. Dies zeigt die Injektivität von Γ. Nach Bemerkung III.9.3 ist $\dim B = |S| \leq \dim A$ und Γ ist auch surjektiv. Daraus folgt, dass die angegebenen Abbildung zueinander inverse Bijektionen sind. □

Beispiel III.9.5. In der Situation von Satz III.9.4 sei S eine endliche transitive G-Menge und $s \in S$. Dann ist die Abbildung $\Gamma \colon \mathrm{Hom}_G(S, L) \to L^{G_s}$, $\varphi \mapsto \varphi(s)$ ein Homomorphismus von K-Algebren. Nach Bemerkung III.9.3 ist Γ sogar ein Isomorphismus von Körpern. Nach dem Beweis von Satz I.4.7 ist andererseits $G/G_s \to S$, $gG_s \mapsto {}^g s$ ein Isomorphismus von G-Mengen, wobei G durch Linksmultiplikation auf G/G_s operiert. Auf diese Weise erhält man eine Bijektion zwischen den K-Isomorphieklassen von Zwischenkörpern. Wir beweisen eine allgemeinere Korrespondenz für Schiefkörper in Satz III.9.21.

Bemerkung III.9.6. Sei $R \subseteq S$ eine Erweiterung von Schiefkörpern. Nach Satz II.9.9 lässt sich S als freier R-Linksmodul oder R-Rechtsmodul auffassen. Zur besseren Unterscheidung schreiben wir ${}_R S$ bzw. S_R. Wie in Bemerkung II.9.11 erwähnt stimmen die Dimensionen $\dim({}_R S)$ und $\dim(S_R)$ nicht unbedingt überein. Sei V ein S-Modul. Dann gilt wie bei Körpern der Gradsatz $\dim({}_R V) = \dim({}_S V) \dim({}_R S)$ bzw. $\dim(V_R) = \dim(V_S) \dim(S_R)$ (siehe Beweis von Satz I.9.5). Im Fall $R \subseteq \mathrm{Z}(S)$ ist jede Basis des R-Linksmoduls S auch eine Basis des R-Rechtsmoduls. Es gilt also $\dim_R(S) = \dim({}_R S) = \dim(S_R)$.

Satz III.9.7. *Sei $R \subseteq S$ eine Erweiterung von Schiefkörpern mit $\dim_{\mathrm{Z}(S)}(S) < \infty$. Dann gilt $\dim({}_R S) = \dim(S_R)$.*

Beweis. Sei $Z := \mathrm{Z}(S)$ und

$$A := \Big\{ \sum_{i=1}^{n} \lambda_i z_z : n \in \mathbb{N},\ \lambda_1, \ldots, \lambda_n \in R,\ z_1, \ldots, z_n \in Z \Big\}$$

der von Z und R erzeugte Teilring in S. Dann besitzt A als R-Linksmodul eine Basis mit Elementen aus Z. Offenbar ist dies auch eine Basis von A als R-Rechtsmodul. Gleichzeitig ist A ein endlich-dimensionaler Z-Vektorraum. Für $a \in A \setminus \{0\}$ ist die Z-lineare Abbildung $f_a \colon A \to A$, $x \mapsto ax$ injektiv,

da S ein Schiefkörper ist. Wegen $\dim_Z(A) \leq \dim_Z(S) < \infty$ ist f_a auch surjektiv und es folgt $a^{-1} \in A$. Also ist A ein Schiefkörper. Aus Bemerkung III.9.6 folgt

$$\begin{aligned}\dim({}_RS) &= \dim({}_AS)\dim({}_RA) = \frac{\dim({}_AS)\dim_Z(A)}{\dim_Z(A)}\dim(A_R) = \frac{\dim_Z(S)}{\dim_Z(A)}\dim(A_R)\\ &= \dim(S_A)\dim(A_R) = \dim(S_R).\end{aligned}$$

□

Bemerkung III.9.8.

(i) Sei S ein Schiefkörper und $\mathrm{End}(L,+)$ der Endomorphismenring der abelschen Gruppe $(L,+)$. Für $s \in S$ und $\varphi \in \mathrm{End}(L,+)$ sei $\varphi s\colon S \to S$, $x \mapsto \varphi(x)s$. Offenbar ist $\varphi s \in \mathrm{End}(L,+)$ und $\mathrm{End}(L,+)$ wird auf diese Weise zu einem S-Rechtsmodul.

(ii) Sei nun $R \subseteq S$ eine Erweiterung von Schiefkörpern und $E := \mathrm{End}({}_RS)$ der Ring aller R-linearen Abbildungen $S \to S$. Offenbar ist E ein S-Untermodul von $\mathrm{End}(L,+)$. Ist B eine Basis von ${}_RS$, so ist die „duale Basis“ $\{b^* : b \in B\}$ mit $b^*(c) := \delta_{bc}$ für $c \in B$ eine Basis von E_S. Es gilt also $\dim({}_RS) = \dim(E_S)$.

(iii) Für $G \leq \mathrm{Aut}(S)$ sei wie üblich

$$S^G := \{s \in S : \forall g \in G : g(s) = s\} \subseteq S$$

der *Fix-Schiefkörper* von G in S. Im Fall $R \subseteq S^G$ ist $G \subseteq E$ und man kann den S-Spann $GS \leq E_S$ bilden.

(iv) Sei $E^* := \mathrm{Hom}(E_S, S_S)$ die Menge der Homomorphismen zwischen den S-Rechtsmoduln E und S. Für $\lambda \in S$ hat man die „duale Abbildung“ $\lambda^* \in E^*$ mit $\lambda^*(f) := f(\lambda)$. Für $\Gamma \in E^*$ und $s \in S$ ist $s\Gamma \in E^*$ mit $(s\Gamma)(f) := s\Gamma(f)$. Auf diese Weise wird E^* zu einem S-Linksmodul. Analog definiert man $(GS)^*$.

(v) Sei V ein (Links- oder Rechts-)Modul über einem Schiefkörper R mit Basis B. Für $u \in U \leq V$ sei $B(u) \subseteq B$ minimal mit $u \in \langle B(u)\rangle$. Wir nennen $u \neq 0$ *minimal bzgl.* B, falls $U \cap \langle B(u)\rangle = \langle u\rangle$ gilt. Nach Aufgabe III.50 bilden die minimalen Elemente ein Erzeugendensystem von U.

Lemma III.9.9 (Ninot). *Sei S ein Schiefkörper, $G \leq \mathrm{Aut}(S)$ und $R := S^G$. Für $s_1, \ldots, s_n \in S$ sind äquivalent:*

(1) $s_1, \ldots, s_n$ sind linear unabhängig in ${}_RS$.

(2) $s_1^*, \ldots, s_n^*$ sind linear unabhängig in ${}_S(GS)^*$.

Beweis. (1) ⇒ (2): Sei

$$U := \left\{(\lambda_1, \ldots, \lambda_n) \in S^n : \sum_{i=1}^n \lambda_i s_i^* = 0\right\} \leq {}_S(S^n).$$

Wir nehmen indirekt $U \neq 0$ an und wählen $(\lambda_i)_i \in U \setminus \{0\}$ minimal bzgl. der Standardbasis von S^n (Bemerkung III.9.8). O. B. d. A. sei $\lambda_1 = 1$. Für $f \in GS$ gilt

$$0 = \sum_{i=1}^n (\lambda_i s_i^*)(f) = \sum_{i=1}^n \lambda_i f(s_i).$$

Darauf wenden wir $\sigma \in G$ an:

$$0 = \sum_{i=1}^{n} \sigma(\lambda_i)\sigma f(s_i) = \sum_{i=1}^{n} \sigma(\lambda_i) s_i^*(\sigma f).$$

Da mit f auch σf durch GS läuft, erhält man $(\sigma(\lambda_i))_i \in U$. Aus der Minimalität von $(\lambda_i)_i$ folgt $\sigma(\lambda_i) = \mu\lambda_i$ für ein $\mu \in S$ und $i = 1, \ldots, n$. Dabei gilt $\mu = \mu\lambda_1 = \sigma(\lambda_1) = 1$. Dies zeigt $(\lambda_i)_i \in (S^G)^n = R^n$. Für $f = \mathrm{id}$ hat man schließlich

$$0 = \sum_{i=1}^{n} (\lambda_i s_i^*)(f) = \sum_{i=1}^{n} \lambda_i s_i.$$

Die lineare Unabhängigkeit von $s_1, \ldots, s_n$ liefert den Widerspruch $\lambda_1 = \ldots = \lambda_n = 0$.

(2) $\Rightarrow$ (1): Seien $r_1, \ldots, r_n \in R$ mit $\sum_{i=1}^{n} r_i s_i = 0$. Für $\sigma \in G$ ist

$$0 = \sigma\Big(\sum_{i=1}^{n} r_i s_i\Big) = \sum_{i=1}^{n} r_i \sigma(s_i) = \sum_{i=1}^{n} r_i s_i^*(\sigma).$$

Da GS von G erzeugt wird, folgt $\sum_{i=1}^{n} r_i s_i^* = 0$. Nach Voraussetzung ist $r_1 = \ldots = r_n = 0$. □

Satz III.9.10. *Sei S ein Schiefkörper, $G \leq \mathrm{Aut}(S)$ und $R := S^G$. Dann gilt* $\mathrm{End}({}_R S) = GS$.

Beweis. Nach Bemerkung III.9.8 gilt $\dim(\mathrm{End}({}_R S)_S) = \dim({}_R S)$ und analog $\dim({}_S(GS)^*) = \dim((GS)_S)$ (duale Basis). Aus Lemma III.9.9 folgt daher $\dim(\mathrm{End}({}_R S)_S) \leq \dim((GS)_S)$. Wegen $GS \leq \mathrm{End}({}_R S)$ gilt Gleichheit. □

Definition III.9.11. Sei $R \subseteq S$ eine Erweiterung von Schiefkörpern.

- Wie bei Körpern sei

  $$G := \mathrm{Gal}(S|R) := \{\gamma \in \mathrm{Aut}(S) : \forall r \in R : \gamma(r) = r\}$$

  die *Galoisgruppe* von S über R.
- Wir nennen $R \subseteq S$ eine *Galois-Erweiterung*, falls $\dim({}_R S) < \infty$ und $S^G = R$ gilt.
- Für $s \in S^\times$ sei $\rho_s \colon S \to S$, $x \mapsto sxs^{-1}$ der von s induzierte *innere* Automorphismus von S. Dann ist $\rho \colon S^\times \to \mathrm{Aut}(S)$, $s \mapsto \rho_s$ ein Ringhomomorphismus. Man nennt $\mathrm{Inn}(S) := \rho(S^\times)$ die *innere Automorphismengruppe* von S. Für $\alpha \in \mathrm{Aut}(S)$ und $s \in S^\times$ gilt $\alpha\rho_s\alpha^{-1} = \rho_{\alpha(s)}$. Dies zeigt $\mathrm{Inn}(S) \trianglelefteq \mathrm{Aut}(S)$.
- Eine Untergruppe $H \leq G$ heißt *abgeschlossen*, falls $\rho^{-1}(H) \cup \{0\}$ ein Schiefkörper ist.

Bemerkung III.9.12. Da $\mathrm{Z}(S)^\times$ der Kern von ρ ist, gilt $\mathrm{Inn}(S) \cong S^\times/\mathrm{Z}(S)^\times$.

Beispiel III.9.13. Offenbar ist $\mathbb{R} \subseteq \mathbb{H}$ eine Galois-Erweiterung, denn $\dim_{\mathbb{R}}(\mathbb{H}) = 4$ und $\mathbb{H}^{\mathrm{Inn}(\mathbb{H})} = \mathrm{Z}(\mathbb{H}) = \mathbb{R}$. Nach Skolem-Noether gilt $G := \mathrm{Gal}(\mathbb{H}|\mathbb{R}) = \mathrm{Inn}(\mathbb{H})$. Im Gegensatz zu Galois-Erweiterungen von Körpern, kann G also unendlich groß sein. Wir werden sehen, dass die *äußere* Automorphismengruppe $G\mathrm{Inn}(S)/\mathrm{Inn}(S)$ stets endlich ist (Satz III.9.16).

Lemma III.9.14. *Sei S ein Schiefkörper und $\sigma_1, \ldots, \sigma_n \in \mathrm{Aut}(S)$ linear unabhängig in $\mathrm{Aut}(L,+)_S$. Seien $s_1, \ldots, s_n \in S^\times$ mit*

$$\gamma := \sum_{i=1}^{n} \sigma_i s_i \in \mathrm{Aut}(S).$$

Dann ist $\gamma = \rho_{s_i}^{-1}\sigma_i$ für $i = 1, \ldots, n$. Im Fall $\gamma = \rho_s$ für ein $s \in S^\times$ gilt $\sigma_i = \rho_{s_i s}$ für $i = 1, \ldots, n$.

Beweis. Für $s, t \in S$ gilt

$$\gamma(s) = \gamma(st)\gamma(t)^{-1} = \sum_{i=1}^{n} (\sigma_i s_i)(st)\gamma(t)^{-1} = \sum_{i=1}^{n} \sigma_i(s)\big(\sigma_i(t) s_i \gamma(t)^{-1}\big).$$

Da die σ_i linear unabhängig sind, folgt $s_i = \sigma_i(t) s_i \gamma(t)^{-1}$ und $\gamma(t) = s_i^{-1}\sigma_i(t)s_i$ für alle $t \in S$. Dies zeigt $\gamma = \rho_{s_i}^{-1}\sigma_i$ für $i = 1, \ldots, n$. Die zweite Aussage folgt durch Umstellen. □

Lemma III.9.15. *Sei S ein Schiefkörper, $s, s_1, \ldots, s_n \in S^\times$ und $Z := \mathrm{Z}(S)$. Dann sind äquivalent:*

(1) $s_1, \ldots, s_n$ sind linear unabhängig in ${}_Z S$ und $s \in \mathrm{Span}_Z\{s_1, \ldots, s_n\}$

(2) $\rho_{s_1}, \ldots, \rho_{s_n}$ sind linear unabhängig in $\mathrm{End}(S,+)_S$ und $\rho_s \in \mathrm{Span}_S\{\rho_{s_1}, \ldots, \rho_{s_n}\}$.

Beweis. Wir zeigen zunächst nur einen Teil von (1)⇒(2): Sei $s = \sum_{i=1}^n z_i s_i$ mit $z_1, \ldots, z_n \in Z$. Für $x \in S$ gilt

$$\rho_s(x) = sxs^{-1} = \sum_{i=1}^{n} z_i s_i x s^{-1} = \sum_{i=1}^{n} \rho_{s_i}(x)(s_i z_i s^{-1})$$

und $\rho_s \in \mathrm{Span}_S\{\rho_{s_1}, \ldots, \rho_{s_n}\}$.

(2) ⇒ (1): Sei $\rho_s = \sum_{i=1} \rho_{s_i}\lambda_i$ mit $\lambda_1, \ldots, \lambda_n \in S$. Aus Lemma III.9.14 folgt $\lambda_i = 0$ oder $\rho_{s_i} = \rho_{\lambda_i s}$ für $i = 1, \ldots, n$. Also existieren $z_1, \ldots, z_n \in Z$ mit $z_i s_i = \lambda_i s$ für $i = 1, \ldots, n$ (im Fall $\lambda_i = 0$ ist $z_i = 0$). Nun gilt

$$s = \rho_s(1)s = \sum_{i=1}^{n} \lambda_i s = \sum_{i=1}^{n} z_i s_i \in \mathrm{Span}_Z\{s_1, \ldots, s_n\}.$$

Nehmen wir nun an, dass $s_1, \ldots, s_n$ linear abhängig sind. O. B. d. A. sei $s_1 = \sum_{i=2}^n z_i s_i$ mit $z_2, \ldots, z_n \in Z$. Aus dem ersten Teil des Beweises folgt $\rho_{s_1} \in \mathrm{Span}_L\{\rho_{s_2}, \ldots, \rho_{s_n}\}$ im Widerspruch zur linearen Unabhängigkeit von $\rho_{s_1}, \ldots, \rho_{s_n}$.

(1) ⇒ (2): Es verbleibt zu zeigen, dass $\rho_{s_1}, \ldots, \rho_{s_n}$ linear unabhängig sind. O. B. d. A. seien $\rho_{s_2}, \ldots, \rho_{s_n}$ linear unabhängig und $\rho_{s_1} \in \mathrm{Span}_S\{\rho_{s_2}, \ldots, \rho_{s_n}\}$. Wegen (2)⇒(1) erhält man den Widerspruch $s_1 \in \mathrm{Span}_Z\{s_2, \ldots, s_n\}$. □

Satz III.9.16. *Sei $R \subseteq S$ eine Galois-Erweiterung von Schiefkörpern und $G := \mathrm{Gal}(S|R)$. Dann gilt*

$$\boxed{\dim({}_R S) = \dim_{\mathrm{Z}(S)}(\mathrm{C}_S(R))|G : G \cap \mathrm{Inn}(S)|,}$$

wobei $\mathrm{C}_S(R)$ der Zentralisator von R in S ist. Insbesondere ist $\boxed{\dim({}_R S) = \dim(S_R).}$

Beweis. Sei $\mathcal{C}$ eine Basis von $C := \mathrm{C}_S(R)$ über $Z := \mathrm{Z}(S)$ und sei $\Gamma \subseteq G$ ein Repräsentantensystem für $G/(G \cap \mathrm{Inn}(S))$. Sei $E := \mathrm{End}({}_RS)$. Wegen $\dim({}_RS) = \dim(E_S)$, genügt es zu zeigen, dass

$$B := \{\gamma\rho_c : c \in \mathcal{C},\ \gamma \in \Gamma\} \subseteq E$$

eine Basis von E_S ist. Ist B linear abhängig, so findet man eine nicht-triviale Linearkombination

$$\gamma\rho_c = \sum_{(i,j)\in I} \gamma_j \rho_{c_i} s_{ij} \tag{III.9.1}$$

mit $c, c_i \in \mathcal{C}$, $\gamma, \gamma_j \in \Gamma$ und $s_{ij} \in S^\times$ für $(i,j) \in I$. Dabei können wir annehmen, dass die Automorphismen $\gamma_j\rho_{c_i}$ auf der rechten Seite linear unabhängig in $E_S \subseteq \mathrm{End}(S,+)$ sind. Aus Lemma III.9.14 folgt $\gamma\rho_c = \rho_{s_{ij}}^{-1}\gamma_j\rho_{c_i}$ für alle $(i,j) \in I$. Also ist $\gamma \equiv \gamma_j \pmod{\mathrm{Inn}(S)}$ und $\gamma = \gamma_j$. Multipliziert man (III.9.1) von links mit γ^{-1}, so erhält man $\rho_c \in \mathrm{Span}_S\{\rho_{c_1}, \dots, \rho_{c_n}\}$, wobei wir I durch $\{1, \dots, n\}$ ersetzt haben. Aus Lemma III.9.15 folgt der Widerspruch $c \in \mathrm{Span}_Z\{c_1, \dots, c_n\}$.

Wegen $E = GS$ (Satz III.9.10) verbleibt zu zeigen, dass jedes $\sigma \in G$ von B erzeugt wird. Sei $\gamma \in \Gamma$ mit $\sigma \equiv \gamma \pmod{\mathrm{Inn}(S)}$. Dann existiert ein $c \in C$ mit $\sigma = \gamma\rho_c$. Seien $c_1, \dots, c_n \in \mathcal{C}$ mit $c \in \mathrm{Span}_Z\{c_1, \dots, c_n\}$. Aus Lemma III.9.15 folgt $\rho_c \in \mathrm{Span}_S\{\rho_{c_1}, \dots, \rho_{c_n}\}$. Also liegt σ in $\mathrm{Span}_S B$.

Für die zweite Behauptung überlegt man sich analog, dass $B' := \{\rho_c\gamma : c \in \mathcal{C}, \gamma \in \Gamma\}$ eine Basis von ${}_S\mathrm{End}(S_R)$ ist. □

Beispiel III.9.17. Ist $R \subseteq Z := \mathrm{Z}(S)$ in der Situation von Satz III.9.16, so erhält man $\dim_R(Z) = |G : G \cap \mathrm{Inn}(S)|$, denn $\dim_R(S) = \dim_Z(S)\dim_R(Z)$.

Satz III.9.18. *Sei $R \subseteq S$ eine Galois-Erweiterung von Schiefkörpern und T ein Schiefkörper mit $R \subseteq T \subseteq S$. Dann ist auch $T \subseteq S$ eine Galois-Erweiterung.*

Beweis. Sicher ist $\dim({}_TS) \le \dim({}_RS) < \infty$. Sei $G := \mathrm{Gal}(S|R)$ und $H := \mathrm{Gal}(S|T) \le G$. Sei $\Gamma \subseteq G$ eine Basis von $GS = \mathrm{End}({}_RS)_S$ (Satz III.9.10). Wir wählen $\varphi \in \mathrm{End}({}_TS) \le GS$ minimal bzgl. Γ (Bemerkung III.9.8). Sei $\varphi = \sum_{i=1}^n \gamma_i s_i$ mit $\gamma_1, \dots, \gamma_n \in \Gamma$ und $s_1, \dots, s_n \in S^\times$. O. B. d. A. sei $s_1 := 1$. Für $\lambda \in S$ liegt die Abbildung $f_\lambda \colon S \to S$, $s \mapsto s\lambda$ in $\mathrm{End}({}_TS)$. Also gilt auch $\varphi f_\lambda \in \mathrm{End}({}_TS)$ mit

$$(\varphi f_\lambda)(s) = \sum_{i=1}^n (\gamma_i s_i)(s\lambda) = \sum_{i=1}^n \gamma_i(s)\gamma_i(\lambda)s_i = \sum_{i=1}^n (\gamma_i\gamma_i(\lambda)s_i)(s)$$

für $s \in S$. Aus der Minimalität von φ folgt $\varphi f_\lambda = \varphi\mu$ für ein $\mu \in S$. Also ist $s_i\mu = \gamma_i(\lambda)s_i$ für $i = 1, \dots, n$. Insbesondere ist $\mu = s_1\mu = \gamma_1(\lambda)$. Nun gilt

$$\varphi(\lambda) = \sum_{i=1}^n \gamma_i(\lambda)s_i = \Big(\sum_{i=1}^n s_i\Big)\gamma_1(\lambda)$$

für alle $\lambda \in S$. Wegen $\varphi \neq 0$ ist $s := \sum_{i=1}^n s_i \in S^\times$ und

$$\varphi s^{-1} = \rho_s\gamma_1 \in \mathrm{End}({}_TS) \cap \mathrm{Aut}(S) = \mathrm{End}({}_TS) \cap G = H.$$

Da die minimalen Elemente ein Erzeugendensystem von $\mathrm{End}({}_TS)$ bilden (Aufgabe III.50), erhält man $\mathrm{End}({}_TS) = HS$. Sei nun $s \in S \setminus T$. Dann kann man $\{1, s\}$ zu einer Basis B von ${}_TS$ ergänzen. Wir konstruieren $f \in \mathrm{End}({}_TS)$ durch $f(s) = 0$ und $f(b) = b$ für alle $b \in B \setminus \{s\}$. Dann existieren

$s_1, \ldots, s_n \in S$ und $\sigma_1, \ldots, \sigma_n \in H$ mit $f = \sum_{i=1}^n \sigma_i s_i$. Wäre $\sigma_i(s) = s$ für alle i, so hätte man den Widerspruch

$$f(s) = \sum_{i=1}^n \sigma(s) s_i = s \sum_{i=1}^n s_i = s f(1) = s.$$

Dies zeigt $S^H = T$. □

Satz III.9.19 (Cartan-Jacobson)**.** *Sei $R \subseteq S$ eine Galois-Erweiterung von Schiefkörpern und $G := \mathrm{Gal}(S|R)$. Sei $\mathcal{T}$ die Menge aller Schiefkörper T mit $R \subseteq T \subseteq S$. Sei $\mathcal{H}$ die Menge aller abgeschlossenen Untergruppen von G. Dann sind die Abbildungen $\mathcal{T} \to \mathcal{H}$, $T \mapsto \mathrm{Gal}(S|T)$ und $\mathcal{H} \to \mathcal{T}$, $H \mapsto S^H$ zueinander inverse, inklusionsumkehrende Bijektionen.*

Beweis (Kasch). Sei $T \in \mathcal{T}$ und $H := \mathrm{Gal}(S|T) \leq G$. Wegen $\rho^{-1}(H) = \mathrm{C}_S(T)^\times$ ist $H \in \mathcal{H}$. Nach Satz III.9.18 gilt $S^H = T$. Sei umgekehrt $H \in \mathcal{H}$ und $T := S^H \in \mathcal{T}$. Nach Satz III.9.10 gilt

$$H \leq \mathrm{Gal}(S|T) \leq \mathrm{End}({}_T S) = HS.$$

Für $c \in \mathrm{C}_S(T)$ ist $\rho_c \in \mathrm{Gal}(S|T)$ und es existieren linear unabhängige Elemente $\gamma_1, \ldots, \gamma_n \in H$ und $s_1, \ldots, s_n \in S^\times$ mit $\rho_c = \sum_{i=1}^n \gamma_i s_i$. Nach Lemma III.9.14 ist $\gamma_i = \rho_{s_i c}$ mit $s_i c \in \rho^{-1}(H)$ für $i = 1, \ldots, n$. Nach Lemma III.9.15 ist $c \in \mathrm{Span}_{\mathrm{Z}(S)}(s_1 c, \ldots, s_n c)$. Wegen $H \in \mathcal{H}$ ist $\rho^{-1}(H) \cup \{0\}$ ein Schiefkörper. Aus $\mathrm{Z}(S)^\times \leq \rho^{-1}(H)$ folgt $c \in \rho^{-1}(H)$ und $\mathrm{C}_S(T)^\times \subseteq \rho^{-1}(H)$.

Sei schließlich $\sigma \in \mathrm{Gal}(S|T)$. Nach Lemma III.9.14 existieren $\gamma \in H$ und $s \in S^\times$ mit $\sigma = \rho_s^{-1}\gamma$. Wegen $\rho_s = \gamma\sigma^{-1} \in \mathrm{Gal}(S|T)$ gilt $s \in \mathrm{C}_S(T)^\times \subseteq \rho^{-1}(H)$ und es folgt $\sigma \in H$. Insgesamt ist $\mathrm{Gal}(S|S^H) = H$. Dies zeigt, dass die angegebenen Abbildungen zueinander inverse Bijektionen sind. Offensichtlich sind sie inklusionsumkehrend. □

Bemerkung III.9.20.

(i) In der Situation von Satz III.9.19 liegt $\rho^{-1}(H)$ zwischen $\mathrm{Z}(S)$ und $\mathrm{C}_S(R)$. Besteht G nur aus inneren Automorphismen, so induziert ρ einen Isomorphismus $\mathrm{C}_S(R)^\times/\mathrm{Z}(S)^\times \to G$. Ggf. stehen die Schiefkörper zwischen $\mathrm{Z}(S)$ und $\mathrm{C}_S(R)$ in Bijektion zu den abgeschlossenen Untergruppen von G. Die Abbildung $T \mapsto \mathrm{C}_S(T)$ ist dann eine Bijektion zwischen $\mathcal{M}$ und der Menge der Schiefkörper C mit $\mathrm{Z}(S) \subseteq C \subseteq \mathrm{C}_S(R)$.

(ii) Im Fall $Z := \mathrm{Z}(S) \subseteq R$ ist jedes Element in G ein Automorphismus der zentral einfachen Z-Algebra S. Nach Skolem-Noether besteht G dann nur aus inneren Automorphismen und wir sind in der Situation von (i).

(iii) Ist hingegen $\mathrm{C}_S(R) = \mathrm{Z}(S)$, so ist jede Untergruppe $H \leq G$ abgeschlossen, denn $\rho^{-1}(H) = \mathrm{Z}(S)^\times$. Dies trifft insbesondere zu, wenn S ein Körper ist. In diesem Fall erhält man den Hauptsatz der Galois-Theorie zurück.

Satz III.9.21 (Fortsetzungssatz)**.** *Sei $R \subseteq S$ eine Galois-Erweiterung von Schiefkörpern und $G := \mathrm{Gal}(S|R)$. Seien T_1, T_2 Schiefkörper mit $R \subseteq T_1, T_2 \subseteq S$. Dann lässt sich jeder R-lineare Ringisomorphismus $\varphi\colon T_1 \to T_2$ zu einem Element aus G fortsetzen. Insbesondere sind T_1 und T_2 genau dann R-isomorph, wenn $\mathrm{Gal}(S|T_1)$ und $\mathrm{Gal}(S|T_2)$ in G konjugiert sind.*

Beweis. Offenbar kann man φ nach $\mathrm{End}({}_RS)$ fortsetzen, indem man eine Basis von ${}_RT$ zu einer Basis von ${}_RS$ ergänzt und geeignete Bilder wählt. Wir wählen jedoch eine Basis $\Gamma \subseteq G$ von $\mathrm{End}({}_RS) = GS$. Sei $\psi = \sum_{\gamma\in\Gamma} \gamma s_\gamma \in GS$ eine Fortsetzung von φ, sodass möglichst viele s_γ verschwinden. Für $s, t \in T_1$ gilt

$$\sum_{\gamma\in\Gamma} \gamma(s)\gamma(t)s_\gamma = \psi(st) = \varphi(st) = \psi(s)\varphi(t) = \sum_{\gamma\in\Gamma} \gamma(s)s_\gamma\varphi(t).$$

Existiert ein $\gamma \in G$ mit $\gamma(t)s_\gamma = s_\gamma\varphi(t)$ für alle $t \in T_1$, so gilt die Behauptung mit $\sigma = \rho_{s_\gamma}^{-1}\gamma \in G$ (beachte $s_\gamma \in \mathrm{C}_S(R)$). Nehmen wir daher an, dass $\gamma \in G$ und $t \in T_1$ mit $d := \gamma(t)s_\gamma - s_\gamma\varphi(t) \neq 0$ existieren. Dann ist auch

$$\tilde{\psi} := \psi - \Big(\sum_{\delta\in\Gamma} \delta\delta(t)s_\delta - \psi\varphi(t)\Big)d^{-1}s_\gamma \in (G \setminus \{\gamma\})S$$

eine Fortsetzung von φ mit weniger von 0 verschiedenen Koeffizienten bzgl. Γ. Widerspruch.

Sei nun $\psi \in G$ eine Fortsetzung von φ. Sei $H_i := \mathrm{Gal}(S|T_i) \leq G$ für $i = 1, 2$. Dann gilt $\psi H_1\psi^{-1} = \mathrm{Gal}(S|\psi(T_1)) = H_2$. Nehmen wir umgekehrt an, dass H_1 und H_2 durch ein $\sigma \in G$ konjugiert sind. Nach Cartan-Jacobson gilt $\sigma(T_1) = \sigma(S^{H_1}) = S^{\sigma H_1\sigma^{-1}} = S^{H_2} = T_2$. Also sind T_1 und T_2 R-isomorph. □

Satz III.9.22. *Sei $R \subseteq S$ eine Galois-Erweiterung von Schiefkörpern und $G := \mathrm{Gal}(S|R)$. Sei $H \leq G$ abgeschlossen und $T := S^H$. Dann ist $\mathrm{Gal}(T|R) \cong \mathrm{N}_G(H)/H$. Genau dann ist $R \subseteq T$ eine Galois-Erweiterung, wenn $\mathrm{N}_G(H)$ in keiner abgeschlossenen echten Untergruppe von G liegt.*

Beweis. Für $\sigma \in \mathrm{N}_G(H)$ ist $\sigma(T) = \sigma(S^H) = S^{\sigma H\sigma^{-1}} = S^H = T$ (vgl. Beweis von Satz I.10.11). Also ist die Einschränkungsabbildung $\Gamma\colon \mathrm{N}_G(H) \to \mathrm{Gal}(T|R)$ ein Homomorphismus mit Kern $\mathrm{Gal}(S|T) = H$ (Satz III.9.19). Nach Satz III.9.21 lässt sich jeder Automorphismus in $\mathrm{Gal}(T|R)$ zu einem $\sigma \in G$ fortsetzen. Dabei gilt $\sigma H\sigma^{-1} = \mathrm{Gal}(S|\sigma(T)) = \mathrm{Gal}(S|T) = H$, d. h. $\sigma \in \mathrm{N}_G(H)$. Also ist Γ surjektiv und $\mathrm{N}_G(H)/H \cong \mathrm{Gal}(T|R)$. Sei nun $R \subseteq T$ eine Galois-Erweiterung. Wegen $H \leq \mathrm{N}_G(H)$ gilt

$$S^{\mathrm{N}_G(H)} = T^{\mathrm{N}_G(H)} = T^{\mathrm{Gal}(T|R)} = R = S^G.$$

Nach Cartan-Jacobson ist G die kleinste abgeschlossene Untergruppe, die $\mathrm{N}_G(H)$ enthält. Ist umgekehrt $R \subseteq T$ keine Galois-Erweiterung, so gilt $T_1 := T^{\mathrm{N}_G(H)} \supsetneq R$ und $\mathrm{Gal}(S|T_1) < G$ ist eine abgeschlossene Untergruppe, die $\mathrm{N}_G(H)$ enthält. □

Bemerkung III.9.23. Nach Satz II.3.6 und Aufgabe II.23 ist eine endliche Körpererweiterung $K \subseteq L$ genau dann eine Galois-Erweiterung, wenn sie separabel und normal ist. Auf diese Weise werden wir die Definition der Galois-Erweiterung auf unendliche Körpererweiterungen ausdehnen.

Lemma III.9.24. *Seien $K \subseteq L \subseteq \overline{K}$ Körpererweiterungen, wobei $\overline{K}$ der algebraische Abschluss von K ist. Genau dann ist $K \subseteq L$ normal, wenn $\alpha(L) = L$ für alle $\alpha \in \mathrm{Gal}(\overline{K}|K)$ gilt.*

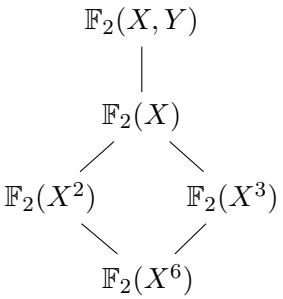
Beweis. Sei $x \in L$ und $\alpha \in \mathrm{Gal}(\overline{K}|K) =: G$. Dann ist $\alpha(x)$ eine Nullstelle des Minimalpolynoms $\mu_x \in K[X]$. Ist $K \subseteq L$ normal, so folgt $\alpha(x) \in L$ und $\alpha(L) \subseteq L$. Nach Lemma I.9.11 ist $\alpha(L) = L$. Nehmen wir nun an, dass eine Nullstelle $y \in \overline{K}$ von μ_x nicht in L liegt. Nach dem Fortsetzungssatz existiert ein K-Isomorphismus $K(x) \to K(y)$, der sich mit Satz II.2.10 und Lemma I.9.11 zu einem Automorphismus $\alpha \in G$ mit $\alpha(L) \neq L$ fortsetzen lässt. □

Satz III.9.25. *Sei $K \subseteq L$ eine algebraische Körpererweiterung und M die Vereinigung aller normalen Körpererweiterungen von K in L. Dann ist $K \subseteq M$ eine normale Körpererweiterung.*

Beweis. Seien $x, y \in M$. Dann existieren normale Erweiterungen $K \subseteq L_1$ und $K \subseteq L_2$ mit $x \in L_1$ und $y \in L_2$. Wir können $L \subseteq \overline{K}$ annehmen. Jedes Element des Kompositums L_1L_2 ist eine rationale Funktion in endlichen vielen Variablen aus L_2 und mit Koeffizienten aus L_1 (Bemerkung II.3.14). Aus Lemma III.9.24 folgt $\alpha(L_1L_2) = L_1L_2$ für alle $\alpha \in \mathrm{Gal}(\overline{K}|K)$. Also ist $K \subseteq L_1L_2$ eine normale Körpererweiterung. Insbesondere ist $x \mathbin{\dot{+}} y \in L_1L_2 \subseteq M$. Dies zeigt, dass M ein Körper ist. Offensichtlich ist $K \subseteq M$ normal. □

Definition III.9.26. In der Situation von Satz III.9.25 nennt man M den *normalen Abschluss* von K in L.

Beispiel III.9.27. Sei $K := \mathbb{F}_2(X^6)$ und $L := \mathbb{F}_2(X, Y)$. Dann ist $\mathbb{F}_2(X)$ der algebraische Abschluss von K in L. Nach Aufgabe II.23 ist die Erweiterung $K \subseteq \mathbb{F}_2(X^3)$ vom Grad 2 normal. Andererseits ist $K \subseteq \mathbb{F}_2(X^2)$ nicht normal, denn das Minimalpolynom $Y^3 - X^6 \in K[Y]$ von X^2 zerfällt erst in $\mathbb{F}_4(X^2)$ in Linearfaktoren. Also ist $\mathbb{F}_2(X^3)$ der normale Abschluss von K in L. Andererseits ist $K \subseteq \mathbb{F}_2(X^2)$ separabel, denn $(Y^3 - X^6)' = Y^2 \neq 0$, aber $K \subseteq \mathbb{F}_2(X^3)$ ist bekanntlich inseparabel. Daher ist $\mathbb{F}_2(X^2)$ der separable Abschluss von K in L.



Satz III.9.28. *Für jede algebraische Körpererweiterung $K \subseteq L$ sind folgende Aussagen äquivalent:*

(1) $K \subseteq L$ ist separabel und normal.

(2) Für jedes $x \in L$ zerfällt das Minimalpolynom $\mu_x \in K[X]$ in paarweise verschiedene Linearfaktoren in $L[X]$.

(3) $L^{\mathrm{Gal}(L|K)} = K$.

(4) L ist die Vereinigung aller Zwischenkörper $M \subseteq L$, sodass $K \subseteq M$ eine endliche Galois-Erweiterung ist.

Ggf. nennen wir $K \subseteq L$ eine (möglicherweise unendliche) Galois-Erweiterung.

Beweis. Sei $L \subseteq \overline{K}$ und $G := \mathrm{Gal}(L|K)$.

(1)⇔(2): Folgt aus der Definition von separabel und normal.

(2)⇒(3): Sicher gilt $K \subseteq L^G$. Sei $x \in L \setminus K$. Dann besitzt das Minimalpolynom $\mu_x \in K[X]$ eine weitere Nullstelle $y \in L \setminus \{x\}$. Nach dem Fortsetzungssatz existiert ein K-Isomorphismus $K(x) \to K(y)$, der sich wie üblich zu $\sigma \in \mathrm{Gal}(\overline{K}|K)$ fortsetzen lässt. Nach Lemma III.9.24 ist $\sigma_{|L} \in G$ mit $\sigma(x) = y \neq x$. Dies zeigt $x \notin L^G$ und $L^G = K$.

(3)⇒(4): Sei $x \in L$. Da G die Nullstellen von μ_x permutiert, ist $N := \{\sigma(x) : \sigma \in G\} \subseteq L$ endlich. Insbesondere ist $\alpha := \prod_{y \in N}(X - y) \in L^G[X] = K[X]$ wohldefiniert. Aus $\mu_x \mid \alpha$ folgt (2) und damit (1). Nach Satz II.3.4 lässt sich die endliche, separable Erweiterung $K \subseteq K(x)$ in eine (endliche) Galois-Erweiterung einbetten.

(4)⇒(2): Für $x \in L$ existiert eine (endliche) Galois-Erweiterung $K \subseteq M$ mit $x \in M$. Daher zerfällt μ_x bereits in $M[X]$ in paarweise verschiedene Linearfaktoren. □

Satz III.9.29. *Für jede unendliche Galois-Erweiterung $K \subseteq L$ ist* $\mathrm{Gal}(L|K)$ *überabzählbar.*

Beweis. Nach Satz III.9.28 existieren endliche Galois-Erweiterungen $K \subseteq L_i$ mit $L = \bigcup_{i\in I} L_i$. Durch Bildung von Komposita konstruiert man eine unendliche Folge $K := L_0 \subsetneq L_1 \subsetneq \ldots$, sodass alle $K \subseteq L_i$ endliche Galois-Erweiterungen sind. Wie üblich zeigt man, dass $M := \bigcup_{i\in\mathbb{N}} L_i$ eine Galois-Erweiterung von K ist. Jeder K-Automorphismus $\sigma\colon M \to M$ setzt sich zu einem K-Automorphismus $\hat\sigma\colon \overline{K} \to \overline{K}$ fort. Nach Lemma III.9.24 ist dann $\hat\sigma_{|L} \in \mathrm{Gal}(L|K) =: G$ eine Fortsetzung von σ. Wir können also $M = L$ annehmen. Nach dem Hauptsatz der Galois-Theorie ist $L_{i-1} \subsetneq L_i$ eine Galois-Erweiterung. Wir wählen $1 \neq \sigma_i \in \mathrm{Gal}(L_i|L_{i-1})$ für $i \in \mathbb{N}$. Sei $\hat\sigma_i \in G$ eine Fortsetzung von σ_i. Für jede unendliche Folge $a = (a_i)_i \in \{0,1\}^{\mathbb{N}}$ definieren wir $\sigma_a\colon L \to L$ durch

$$\sigma_a(x) = \hat\sigma_1^{a_1}\hat\sigma_2^{a_2}\ldots\hat\sigma_k^{a_k}(x)$$

für $x \in L_k$. Man sieht leicht, dass σ_a ein wohldefinierter Automorphismus in G ist (Lemma I.9.11). Sei $b = (b_i)_i \neq a$ eine weitere Folge und $k = \min\{i \in \mathbb{N} : a_i \neq b_i\}$. Dann existiert ein $x \in L_k$ mit $\sigma_k^{a_k}(x) \neq \sigma_k^{b_k}(y)$. Es folgt $\sigma_a \neq \sigma_b$. Daher ist $|G| \geq |\{0,1\}^{\mathbb{N}}|$ überabzählbar. □

Beispiel III.9.30.

(i) Sei $\overline{K}$ der algebraische Abschluss von K und L der separable Abschluss von K in $\overline{K}$. Für $x \in L$ ist jede Nullstelle des Minimalpolynoms $\mu_x \in K[X]$ separabel. Daher zerfällt μ_x in Linearfaktoren in $L[X]$ und $K \subseteq L$ ist eine Galois-Erweiterung. Man nennt $G := \mathrm{Gal}(L|K)$ die *absolute Galoisgruppe* von K. Sei $\sigma \in G$ mit Ordnung $k < \infty$. Ist $\mathrm{char}\, K = 0$, so ist $L = \overline{K}$ und $k \leq 2$ nach Folgerung A.7.12. Sei nun $p := \mathrm{char}\, K > 0$. Wie üblich lässt sich σ zu $\hat\sigma \in \mathrm{Gal}(\overline{K}|K)$ fortsetzen. Nach Satz II.3.8 ist $L \subseteq \overline{K}$ rein inseparabel. Für alle $x \in \overline{K}$ existiert nach Satz II.3.11 ein $n \in \mathbb{N}$ mit $x^{p^n} \in L$. Dies zeigt

$$(\hat\sigma^k(x) - x)^{p^n} = \hat\sigma^k(x^{p^n}) - x^{p^n} = 0$$

und $\hat\sigma^k(x) = x$. Also hat auch $\hat\sigma$ Ordnung k. Aus Folgerung A.7.12 folgt $\sigma = 1$, d. h. G ist torsionsfrei.

(ii) Betrachten wir speziell $K = \mathbb{F}_q$ für eine Primzahlpotenz $q \neq 1$. Angenommen es existieren $\sigma, \tau \in G := \mathrm{Gal}(\overline{K}|K)$ mit $\sigma\tau \neq \tau\sigma$. Dann existiert ein $x \in \mathbb{F}_{q^n} \subseteq K$ mit $\sigma\tau(x) \neq \tau\sigma(x)$. Da $\mathrm{Gal}(\mathbb{F}_{q^n}|K) \cong C_n$ abelsch ist, müssen aber die Einschränkungen von σ und τ auf $\mathbb{F}_{q^n}$ kommutieren. Dieser Widerspruch zeigt, dass G eine torsionsfreie abelsche Gruppe ist. Nach Satz III.9.29 ist G überabzählbar, während $\overline{K}$ abzählbar ist. Im Gegensatz zu endlichen Galois-Erweiterungen gilt also $|G| > |\overline{K} : K|$.

(iii) Sei $p \in \mathbb{P}$ und $\zeta_n := e^{2\pi\mathrm{i}/p^n} \in \mathbb{Q}_{p^n}$ für $n \in \mathbb{N}$. Nach Satz III.9.28 ist

$$\mathbb{Q}_{p^\infty} := \mathbb{Q}(\zeta_n : n \in \mathbb{N}) = \bigcup_{n\in\mathbb{N}} \mathbb{Q}_{p^n}$$

eine unendliche Galois-Erweiterung über $\mathbb{Q}$. Für $\sigma \in G := \mathrm{Gal}(\mathbb{Q}_{p^n}|\mathbb{Q})$ existieren $a_n \in (\mathbb{Z}/p^n\mathbb{Z})^\times$ mit $\sigma(\zeta_n) = \zeta_n^{a_n}$ und $a_{n+1} \equiv a_n \pmod{p^n}$ für alle $n \in \mathbb{N}$. Dies zeigt $G \cong \mathbb{Z}_{[p]}^\times$, wobei $\mathbb{Z}_{[p]}$ der Ring der ganzen p-adischen Zahlen ist (Definition III.8.19). Sei nun $p > 2$. Nach Satz I.8.34 existiert ein $a \in \mathbb{Z}$ mit $(\mathbb{Z}/p^2\mathbb{Z})^\times = \langle a + p^2\mathbb{Z}\rangle$. Nach Aufgabe I.52 gilt $(\mathbb{Z}/p^n\mathbb{Z})^\times = \langle a + p^n\mathbb{Z}\rangle$ für alle $n \in \mathbb{N}$. Für $\sigma \in G$ mit $\sigma(\zeta_n) = \zeta_n^a$ ist dann $\mathbb{Q}_{p^\infty}^\sigma = \mathbb{Q} = \mathbb{Q}_{p^\infty}^G$. Der Hauptsatz der (endlichen) Galois-Theorie überträgt sich also nicht direkt auf unendliche Erweiterungen.

(iv) Für $\pi \subseteq \mathbb{P}$ sei $\mathbb{Q}(\sqrt{\pi}) := \mathbb{Q}(\sqrt{p} : p \in \pi)$. Sei π zunächst endlich. Wir zeigen durch Induktion nach $|\pi|$, dass $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{\pi})$ eine Galois-Erweiterung von Grad $2^{|\pi|}$ ist. Dies ist klar für $|\pi| \leq 1$. Sei $q \in \pi$ und $\pi' := \pi \setminus \{q\}$. Für $\omega \subseteq \pi$ sei $p_\omega := \prod_{p\in\omega} p$. Nach Induktion ist $\{\sqrt{p_\omega} : \omega \subseteq \pi'\}$ eine $\mathbb{Q}$-Basis

von $\mathbb{Q}(\sqrt{\pi'})$. Nehmen wir $\sqrt{q} \in \mathbb{Q}(\sqrt{\pi'})$ an. Dann existieren $x_\omega \in \mathbb{Q}$ mit $\sqrt{q} = \sum_{\omega \subseteq \pi'} x_\omega \sqrt{p_\omega}$. Sei $r \in \omega \subseteq \pi'$ mit $x_\omega \neq 0$. Sei

$$x_1 := \sum_{\omega \subseteq \pi' \setminus \{r\}} x_{\omega \cup \{r\}} \sqrt{p_\omega}, \qquad x_2 := \sum_{\omega \subseteq \pi' \setminus \{r\}} x_\omega \sqrt{p_\omega}.$$

Dann gilt

$$q = \sqrt{q}^2 = (\sqrt{r}x_1 + x_2)^2 = rx_1^2 + x_2^2 + 2\sqrt{r}x_1x_2$$

mit $x_1, x_2 \in \mathbb{Q}(\sqrt{\pi' \setminus \{r\}})$. Nach Induktion ist $\sqrt{r} \notin \mathbb{Q}(\sqrt{\pi' \setminus \{r\}})$. Dies impliziert $x_1x_2 = 0$ und $x_2 = 0$ wegen $x_1 \neq 0$. Nun folgt $\sqrt{q} = \sqrt{r}x_1$. Da r beliebig war, gilt sogar $\sqrt{q} = x_\omega \sqrt{p_\omega}$ für ein $\omega \subseteq \pi'$. Dann hätte $q = x_\omega^2 p_\omega$ aber zwei verschiedene Primfaktorzerlegungen. Also ist $\sqrt{q} \notin \mathbb{Q}(\sqrt{\pi'})$ und $|\mathbb{Q}(\sqrt{\pi}) : \mathbb{Q}| = 2^{|\pi|}$ wie behauptet. Als (iteriertes) Kompositum der Galois-Erweiterungen $\mathbb{Q}(\sqrt{p})$ für $p \in \pi$ ist $\mathbb{Q}(\sqrt{\pi})$ eine Galois-Erweiterung mit $\mathrm{Gal}(\mathbb{Q}(\sqrt{\pi})|\mathbb{Q}) \cong C_2^{|\pi|}$ nach Satz I.10.15. Daher ist auch $\mathbb{Q}(\sqrt{\mathbb{P}}) = \bigcup_{|\pi|<\infty} \mathbb{Q}(\sqrt{\pi})$ eine Galois-Erweiterung. Für jede Teilmenge $\pi \subseteq \mathbb{P}$ existiert ein $\sigma_\pi \in G := \mathrm{Gal}(\mathbb{Q}(\sqrt{\mathbb{P}})|\mathbb{Q})$ mit

$$\sigma_\pi(\sqrt{p}) = \begin{cases} \sqrt{p} & \text{falls } p \in \pi, \\ -\sqrt{p} & \text{falls } p \notin \pi. \end{cases}$$

Umgekehrt ist jedes $\tau \in G$ durch die Bilder $\tau(\sqrt{p})$ für $p \in \mathbb{P}$ eindeutig bestimmt. Also ist $G \cong C_2^{\mathbb{N}}$. Für $H := \langle \sigma_\pi : |\pi| < \infty \rangle < G$ gilt $\mathbb{Q}(\sqrt{\mathbb{P}})^H = \mathbb{Q}$.

Satz III.9.31. *Seien $K \subseteq M \subseteq L$ Körpererweiterungen, sodass $K \subseteq L$ eine Galois-Erweiterung ist. Sei $G := \mathrm{Gal}(L|K)$ und $H := \mathrm{Gal}(L|M)$. Dann gilt*

(i) $M \subseteq L$ ist eine Galois-Erweiterung.

(ii) Ist $|M : K| < \infty$, so gilt $|G : H| = |M : K|$.

(iii) Genau dann ist $K \subseteq M$ eine Galois-Erweiterung, wenn $H \trianglelefteq G$. Ggf. gilt $\mathrm{Gal}(M|K) \cong G/H$.

Beweis.

(i) Sei $x \in L$. Nach Satz III.9.28 zerfällt das Minimalpolynom $\mu_x \in K[X]$ in paarweise verschiedene Linearfaktoren in $L[X]$. Das Minimalpolynom von x über M teilt μ_x und zerfällt daher ebenfalls in paarweise verschiedene Linearfaktoren.

(ii) Nach Aufgabe II.18 ist $|M : K|$ die Anzahl der Homomorphismen $\sigma\colon M \to \overline{L}$. Jeder dieser Homomorphismen setzt sich zu einem Isomorphismus $\overline{L} \to \overline{L}$ fort. Nach Lemma III.9.24 kann man diese Isomorphismen zu Elementen von G einschränken. Umgekehrt kann man jedes $\sigma \in G$ auf M einschränken. Für $\sigma, \tau \in G$ gilt dabei $\sigma H = \tau H$ genau dann, wenn σ und τ die gleiche Einschränkung auf M haben. Dies zeigt die Behauptung.

(iii) In jedem Fall ist $K \subseteq M$ separabel. Nehmen wir an, dass $K \subseteq M$ normal ist. Nach Lemma III.9.24 gilt $\sigma(M) = M$ für alle $\sigma \in G$. Die Einschränkung liefert daher einen Homomorphismus $\Gamma\colon G \to \mathrm{Gal}(M|K)$ mit Kern $H \trianglelefteq G$. Wie bisher lässt sich jeder K-Automorphismus $M \to M$ zu einem Element von G fortsetzen. Daher ist Γ surjektiv und $G/H \cong \Gamma(G) = \mathrm{Gal}(M|K)$.

Sei umgekehrt $H \trianglelefteq G$. Nach (i) und Satz III.9.28 ist $M = L^H$ und $\sigma(M) = L^{\sigma H \sigma^{-1}} = L^H = M$ für alle $\sigma \in G$ (vgl. Beweis von Satz I.10.11). Nach Lemma III.9.24 ist $K \subseteq M$ normal. □

Bemerkung III.9.32. Sei $K \subseteq L$ eine Galois-Erweiterung mit $G := \mathrm{Gal}(L|K)$. Nach Satz III.9.28 existieren endliche Galois-Erweiterungen $K \subseteq L_i$ mit $L = \bigcup_{i\in I} L_i$. Nach Satz III.9.31 ist $H_i := \mathrm{Gal}(L|L_i) \trianglelefteq G$ mit $|G : H_i| = |L_i : K| < \infty$ und $\bigcap_{i\in I} H_i = \mathrm{Gal}(L|\bigcup L_i) = 1$. Daher ist der Homomorphismus $G \to \times_{i\in I} G/H_i$, $g \mapsto (gH_i)_i$ injektiv und G ist zu einer Untergruppe von $\times_{i\in I} G/H_i$ isomorph. Gruppen mit dieser Eigenschaft nennt man *residual-endlich*.

Definition III.9.33. Sei $K \subseteq L$ eine Galois-Erweiterung und $G := \mathrm{Gal}(L|K)$. Sei

$$\mathcal{N} := \big\{\mathrm{Gal}(L|M) : K \subseteq M \text{ endliche Galois-Erweiterung}\big\}.$$

Eine Teilmenge $U \subseteq G$ heißt *offen*, falls U eine Vereinigung von (beliebig vielen) Nebenklassen gN mit $g \in G$ und $N \in \mathcal{N}$ ist. Wie üblich heißt $A \subseteq G$ *abgeschlossen*, falls $G \setminus A$ offen ist.

Lemma III.9.34. *Mit den Bezeichnungen aus Definition III.9.33 bilden die offenen Teilmengen eine Topologie auf G, d. h. es gilt*

(i) $\varnothing$ und G sind offen.

(ii) Die Vereinigung von offenen Mengen ist offen.

(iii) Der Durchschnitt von zwei offenen Mengen ist offen.

Beweis. Offenbar ist $\varnothing$ als leere Vereinigung offen und G ist die triviale Nebenklasse von $G \in \mathcal{N}$. Nach Definition gilt (ii). Seien $g, h \in G$ und $N, M \in \mathcal{N}$ mit $gN \cap hM \neq \varnothing$. Für $x \in gN \cap hM$ gilt

$$gN \cap hM = xN \cap xM = x(N \cap M).$$

Seien $K \subseteq L_1$ und $K \subseteq L_2$ endliche Galois-Erweiterungen mit $N = \mathrm{Gal}(L|L_1)$ und $M = \mathrm{Gal}(L|L_2)$. Nach Satz I.10.15 ist $K \subseteq L_1L_2$ eine endliche Galois-Erweiterung mit $\mathrm{Gal}(L|L_1L_2) = N \cap M$. Daraus folgt (iii). □

Definition III.9.35. Die Topologie aus Lemma III.9.34 heißt *Krull-Topologie* auf G.

Beispiel III.9.36. Nach Bemerkung III.9.32 existieren $N_i \in \mathcal{N}$ mit $\bigcap_{i\in I} N_i = 1$. Für $g \in G$ ist

$$G \setminus \{g\} = G \setminus \bigcap_{i\in I} gN_i = \bigcup_{i\in I} (G \setminus gN_i) = \bigcup_{i\in I} \bigcup_{hN_i \neq gN_i} hN_i$$

offen. Daher ist jede endliche Teilmenge von G abgeschlossen. Ist G endlich, so ist die Krull-Topologie diskret, d. h. jede Teilmenge ist offen und abgeschlossen.

Satz III.9.37 (Krull)**.** *Sei $K \subseteq L$ eine Galois-Erweiterung, $G := \mathrm{Gal}(L|K)$, $\mathcal{M} := \{M$ Körper $: K \subseteq M \subseteq L\}$ und $\mathcal{H} := \{H \leq G : H$ abgeschlossen$\}$. Dann sind die Abbildungen $M \mapsto \mathrm{Gal}(L|M)$ und $H \mapsto L^H$ zueinander inverse, inklusionsumkehrende Bijektionen zwischen $\mathcal{M}$ und $\mathcal{H}$.*

Beweis. Sei $M \in \mathcal{M}$ und $H := \mathrm{Gal}(L|M) \leq G$. Nach Satz III.9.28 existieren endliche Galois-Erweiterungen $K \subseteq L_i$ mit $L = \bigcup_{i\in I} L_i$. Nach Satz III.9.31 gilt $N_i := \mathrm{Gal}(L|L_i) \trianglelefteq G$ und $|G : N_i| = |L_i : K| < \infty$. Für $\sigma \in G \setminus H$ existieren $i \in I$ und $x \in M \cap L_i$ mit $\sigma(x) \neq x$. Für $\tau \in N_i$ gilt $\sigma\tau(x) = \sigma(x) \neq x$. Daher gilt $\sigma \in \sigma N_i \subseteq G \setminus H$. Also ist $G \setminus H$ offen und $H \in \mathcal{H}$.

Nach Satz III.9.31 ist $M \subseteq L$ eine Galois-Erweiterung und $L^H = M$. Sei umgekehrt $H \in \mathcal{H}$ gegeben. Dann ist $H \leq \mathrm{Gal}(L|L^H)$. Sei $\sigma \in \mathrm{Gal}(L|L^H)$. Da H abgeschlossen ist, existieren endliche Galois-Erweiterungen $K \subseteq L_i$ und $g_i \in G$ mit $G \setminus H = \bigcup_{i\in I} g_i N_i$, wobei $N_i := \mathrm{Gal}(L|L_i)$. Nehmen wir indirekt $\sigma \notin H$ an. Dann existiert $i \in I$ mit $\sigma \in g_i N_i$. Nach Artin ist $L^H \subseteq L_i L^H$ eine endliche Galois-Erweiterung. Daher ist die Einschränkung $\Phi\colon \mathrm{Gal}(L|L^H) \to \mathrm{Gal}(L_i L^H|L^H)$ ein wohldefinierter Homomorphismus. Offenbar gilt

$$(L_i L^H)^{\Phi(H)} = L^H = (L_i L^H)^{\mathrm{Gal}(L_i L^H|L^H)}.$$

Aus dem Hauptsatz der Galois-Theorie folgt $\Phi(H) = \mathrm{Gal}(L_i L^H|L^H)$. Insbesondere existiert ein $h \in H$ mit $\Phi(\sigma) = \Phi(h)$. Dies zeigt $\sigma^{-1}h \in \mathrm{Gal}(L|L_i) = N_i$ und $h \in hN_i = \sigma N_i \subseteq G \setminus H$. Widerspruch. Also gilt $H = \mathrm{Gal}(L|L^H)$ und die Abbildungen sind zueinander inverse Bijektionen. Wie üblich sind sie inklusionsumkehrend. □

Folgerung III.9.38. *Sei $K \subseteq L$ eine Galois-Erweiterung und H_1, H_2 endliche Untergruppen von $\mathrm{Gal}(L|K)$. Dann ist $L^{H_1} = L^{H_2}$ äquivalent zu $H_1 = H_2$.*

Beweis. Nach Beispiel III.9.36 sind H_1 und H_2 abgeschlossen. Daher gilt

$$L^{H_1} = L^{H_2} \iff H_1 = \mathrm{Gal}(L|L^{H_1}) = \mathrm{Gal}(L|L^{H_2}) = H_2.$$ □

Folgerung III.9.39. *Sei $K \subseteq L$ eine Galois-Erweiterung und $H \leq \mathrm{Gal}(L|K)$. Genau dann ist H offen, wenn H abgeschlossen ist und $|G : H| < \infty$.*

Beweis. Sei H offen, sagen wir $H = \bigcup_{i\in I} g_i N_i$ mit $g_i \in G$ und $N_i \in \mathcal{N}$. Dann existiert ein i mit $1 \in g_i N_i = N_i \subseteq H$. Es folgt $|G : H| \leq |G : N_i| < \infty$ und $G \setminus H = \bigcup_{x\in G\setminus H} xN_i$ ist offen, d. h. H ist abgeschlossen. Sei umgekehrt H abgeschlossen und $|G : H| < \infty$. Nach Krull ist $H = \mathrm{Gal}(L|L^H)$ und $|L^H : K| = |G : H| < \infty$. Nach Satz II.3.4 existiert eine endliche Galois-Erweiterung $K \subseteq M$ mit $L^H \subseteq M$. Nun ist $N := \mathrm{Gal}(L|M) \leq H$ offen und somit auch $H = \bigcup_{h\in H} hN$. □

Beispiel III.9.40.

(i) Sei $H := \langle \sigma_\pi : |\pi| < \infty\rangle \leq G := \mathrm{Gal}(\mathbb{Q}(\sqrt{\mathbb{P}})|\mathbb{Q}) \cong C_2^{\mathbb{N}}$ aus Beispiel III.9.30. Wir können G/H als $\mathbb{F}_2$-Vektorraum auffassen. Durch Wahl einer Basis findet man $H \leq N \leq G$ mit $|G : N| = 2$. Wäre N abgeschlossen, so hätte man den Widerspruch

$$\mathbb{Q} = \mathbb{Q}(\sqrt{\mathbb{P}})^G \subsetneq \mathbb{Q}(\sqrt{\mathbb{P}})^N \subseteq \mathbb{Q}(\sqrt{\mathbb{P}})^H = \mathbb{Q}.$$

(ii) Das in Bemerkung I.12.18 erwähnte inverse Galois-Problem ist äquivalent zu der Frage, ob für jede endliche Gruppe G ein stetiger Epimorphismus $\Gamma\colon \mathrm{Gal}(\overline{\mathbb{Q}}|\mathbb{Q}) \to G$ existiert, wobei man G mit der diskreten Topologie ausstattet. Die Stetigkeit von Γ garantiert, dass $N := \mathrm{Ker}(\Gamma)$ abgeschlossen ist. Nach Krull ist dann $\mathrm{Gal}(\overline{\mathbb{Q}}|\overline{\mathbb{Q}}^N) = N$ und $G \cong \mathrm{Gal}(\overline{\mathbb{Q}}^N|\mathbb{Q})$ nach Satz III.9.31.

Satz III.9.41. *Für Körpererweiterungen $K \subseteq M_i \subseteq L$ mit $i = 1, 2$ gilt:*

(i) Ist $K \subseteq M_1$ eine Galois-Erweiterung, so auch $M_2 \subseteq M_1 M_2$ und es gilt

$$\boxed{\mathrm{Gal}(M_1 M_2|M_2) \cong \mathrm{Gal}(M_1|M_1 \cap M_2).}$$

(ii) Sind $K \subseteq M_1$ und $K \subseteq M_2$ Galois-Erweiterungen, so auch $K \subseteq M_1M_2$ und

$$\boxed{\mathrm{Gal}(M_1M_2|M_1 \cap M_2) \cong \mathrm{Gal}(M_1|M_1 \cap M_2) \times \mathrm{Gal}(M_2|M_1 \cap M_2).}$$

(iii) Sei $K \subseteq L$ eine Galois-Erweiterung mit $G := \mathrm{Gal}(L|K)$ und $H_1, H_2 \leq G$ abgeschlossen. Dann gilt $\boxed{L^{H_1}L^{H_2} = L^{H_1 \cap H_2}}$ und $\boxed{L^{H_1} \cap L^{H_2} = L^{\langle H_1, H_2\rangle}.}$

Beweis.

(i) Für $x \in M_1M_2$ existieren $y_1, \ldots, y_n \in M_1$ mit $x \in M_2(y_1, \ldots, y_n)$. Da $K \subseteq M_1$ separabel ist, existiert eine endliche Galois-Erweiterung $K \subseteq L_1$ mit $K(y_1, \ldots, y_n) \subseteq L_1 \subseteq M_1$. Wir können wie in Satz I.10.15 argumentieren: L_1 ist der Zerfällungskörper eines separablen Polynoms $\alpha \in K[X]$. Da L_1M_2 der Zerfällungskörper von $\alpha \in M_2[X]$ ist, ist auch $M_2 \subseteq L_1M_2$ eine Galois-Erweiterung mit $x \in L_1M_2$. Als Vereinigung der Körper L_1M_2 ist M_1M_2 eine Galois-Erweiterung über M_2 nach Satz III.9.28. Nach Lemma III.9.24 ist die Einschränkung

$$\Gamma\colon \mathrm{Gal}(M_1M_2|M_2) \to \mathrm{Gal}(M_1|M_1 \cap M_2) =: G$$

wohldefiniert und injektiv. Sei $\sigma \in \mathrm{Gal}(M_1|M_1 \cap M_2)$. Nach Satz I.10.15 existiert genau eine Fortsetzung $\hat{\sigma}_{L_1} \in \mathrm{Gal}(L_1M_2|M_2)$ von $\sigma_{|L_1} \in \mathrm{Gal}(L_1|L_1 \cap M_2)$. Wir definieren

$$\hat{\sigma}\colon M_1M_2 \to M_1M_2, \qquad x \mapsto \hat{\sigma}_{L_1}(x).$$

Sei auch $K \subseteq L_1'$ eine endliche Galois-Erweiterung mit $x \in L_1'$. Dann ist auch $K \subseteq L_1 \cap L_1'$ eine Galois-Erweiterung. Daher müssen $\hat{\sigma}_{L_1}$ und $\hat{\sigma}_{L_1'}$ auf $L_1 \cap L_1'$ mit σ übereinstimmen. Insbesondere ist $\hat{\sigma}_{L_1}(x) = \hat{\sigma}_{L_1'}(x)$. Dies zeigt, dass $\hat{\sigma}$ wohldefiniert ist. Wie üblich zeigt man, dass $\hat{\sigma}$ ein Automorphismus in $\mathrm{Gal}(M_1M_2|M_2)$ ist. Also ist $\Gamma(\hat{\sigma}) = \sigma$ und Γ ist surjektiv.

(ii) Nach Satz III.9.28 existieren endliche Galois-Erweiterungen $K \subseteq M_{ij}$ mit $M_i = \bigcup_{j \in J_i} M_{ij}$ für $i = 1, 2$. Nach Satz I.10.15 sind $K \subseteq M_{1j}M_{2k}$ endliche Galois-Erweiterungen für alle $j \in J_1$ und $k \in J_2$. Wie in (i) zeigt man $M_1M_2 = \bigcup_{j \in J_1} \bigcup_{k \in J_2} M_{1j}M_{2k}$. Also ist $K \subseteq M_1M_2$ eine Galois-Erweiterung nach Satz III.9.28. Nach Satz III.9.31 ist auch $M_1 \cap M_2 \subseteq M_1M_2$ eine Galois-Erweiterung. Wie üblich ist die Abbildung

$$\Gamma\colon \mathrm{Gal}(M_1M_2|M_1 \cap M_2) \to \mathrm{Gal}(M_1|M_1 \cap M_2) \times \mathrm{Gal}(M_2|M_1 \cap M_2),\ \sigma \mapsto (\sigma_{|M_1}, \sigma_{|M_2})$$

ein wohldefinierter Monomorphismus. Für $\sigma_i \in \mathrm{Gal}(M_i|M_1 \cap M_2)$ existieren Fortsetzungen $\hat{\sigma}_i \in \mathrm{Gal}(M_1M_2|M_j)$ nach (i) für $\{i, j\} = \{1, 2\}$. Nun ist $\hat{\sigma}_1\hat{\sigma}_2 \in \mathrm{Gal}(M_1M_2|M_1 \cap M_2)$ ein Urbild von (σ_1, σ_2) unter Γ. Also ist Γ ein Isomorphismus.

(iii) Sicher ist $L^{H_1} \cap L^{H_2} = L^{\langle H_1, H_2\rangle}$ und $L^{H_1}L^{H_2} \subseteq L^{H_1 \cap H_2}$. Da H_1 und H_2 abgeschlossen sind, gilt

$$H_1 \cap H_2 \subseteq \mathrm{Gal}(L|L^{H_1 \cap H_2}) \subseteq \mathrm{Gal}(L|L^{H_1}L^{H_2}) \subseteq \mathrm{Gal}(L|L^{H_1}) \cap \mathrm{Gal}(L|L^{H_2}) = H_1 \cap H_2.$$

Dies zeigt $L^{H_1}L^{H_2} = L^{H_1 \cap H_2}$. □

10 Codierungstheorie

Bemerkung III.10.1. Mit dem DHM-Schlüsselaustausch in Beispiel I.2.25 und dem RSA-Verfahren in Beispiel I.7.19 hatten wir bereits Anwendungen der Algebra in der Kryptographie kennen gelernt. Die *Kryptologie* umfasst neben der Kryptographie auch die *Kryptoanalyse*, also die Wissenschaft vom Entschlüsseln von Daten (z. B. Entschlüsselung der Enigma im zweiten Weltkrieg durch Alan Turing). In der *Codierungstheorie* hingegen beschäftigt man sich mit der Fehlererkennung und -korrektur bei der Übertragung von digitalen Daten über einen störungsanfälligen Kanal (z. B. Mobilfunk, WLAN, GPS). Motiviert durch verschiedenste Anwendungsszenarien entwickelte sich diese Theorie deutlich mehr in die Breite als in die Tiefe. Ein Höhepunkt ist die Existenz und Eindeutigkeit der sogenannten Golay-Codes. Neben Methoden der Algebra sind auch statistische Aspekte relevant, auf die wir jedoch nur am Rande eingehen.

Beispiel III.10.2. Wer seinen Gesprächspartner akustisch nicht versteht, bittet ihn das Gesagt zu wiederholen. Die naheliegendste Idee zur Fehlererkennung ist daher Daten doppelt zu senden. Anstatt `geheim` wird `ggeehheeiimm` versendet. Durch einen Übertragungsfehler wird daraus `ggeemheeiimm`. An der Folge `mh` kann man sofort feststellen, dass ein Fehler unterlaufen ist. Allerdings lässt sich dieser nicht eindeutig korrigieren, denn neben `geheim` kommt auch `gemein` in Frage. Senden wir hingegen jeden Buchstaben gleich dreifach und erhalten `mmh`, so kann man annehmen, dass mit höherer Wahrscheinlichkeit das `h` falsch ist. Nachteil dieser Methode ist die linear wachsende Datenmenge. Wir werden bessere Verfahren kennen lernen (vgl. Aufgabe III.51).

Definition III.10.3. Sei $2 \leq q < \infty$ und A eine Menge (*Alphabet*) mit q Elementen (*Symbole*). Die Elemente aus dem n-fachen kartesischen Produkt A^n nennt man *Wörter*.

(i) Ein (*Block-*)*Code* der *Länge* n ist eine nichtleere Teilmenge $C \subseteq A^n$. Die Elemente von C nennt man *Codewörter*.

(ii) Für $x = (x_1, \ldots, x_n) \in A^n$ und $y = (y_1, \ldots, y_n) \in A^n$ sei

$$d(x, y) := |\{i : x_i \neq y_i\}|$$

die (HAMMING-)*Distanz* von x und y.

(iii) Man nennt

$$d(C) := \inf\{d(x, y) : x, y \in C,\ x \neq y\}$$

die *Minimaldistanz* von C (im Fall $|C| = 1$ sei $d(C) := \infty$).

(iv) Für $x \in A^n$ und $e \geq 0$ sei

$$K_e(x) := \{y \in A^n : d(x, y) \leq e\}$$

die „Kugel“ mit Radius e um x.

Bemerkung III.10.4.

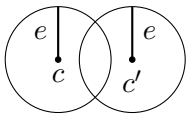
(i) Sei $C \subseteq A^n$ ein Code und S eine Menge von Daten, die versendet werden sollen. Die *Codierung* ist eine injektive Abbildung $\gamma\colon S \to C$. Da Übertragungsfehler auftreten können, definiert man die *Decodierung* als Abbildung $\gamma'\colon A^n \to S$ mit $\gamma' \circ \gamma = \mathrm{id}_S$ (bei fehlerfreier Übertragung ist also γ' die Umkehrabbildung von γ). Wir werden o. B. d. A. $S = C$, $\gamma = \mathrm{id}_C$ und $\gamma'\colon A^n \to C$ annehmen. Neben der Konstruktion von C ist auch eine effiziente Berechnung von γ' eine der Hauptaufgaben der Codierungstheorie.

(ii) Für $x, y \in A^n$ ist $d(x,y) = d(y,x)$ und $d(x,y) = 0 \iff x = y$. Unterscheiden sich x und y an den Positionen $i_1, \dots, i_k$ und unterscheiden sich y und z an den Positionen $j_1, \dots, j_l$, so können sich x und z höchstens an den Positionen $\{i_1, \dots, i_k\} \cup \{j_1, \dots, j_l\}$ unterscheiden. Dies zeigt die Dreiecksungleichung $d(x,z) \leq d(x,y) + d(y,z)$. Der Hamming-Abstand ist daher eine Metrik im Sinn der Analysis.

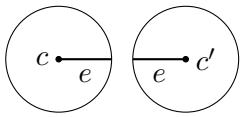
(iii) Treten bei der Übertragung genau e Fehler auf, so erhält Bob anstelle des Codeworts $c \in C$ ein Wort $x \in A^n$ mit $d(c,x) = e$. Damit Bob das Auftreten von Fehlern erkennen kann, muss $x \notin C$ gelten. Für verschiedene $c, c' \in C$ sollte also stets $d(c,c') > e$ gelten, d. h. $d(C) > e$. Damit Bob alle e Fehler korrigieren kann, muss c zusätzlich das einzige Codewort mit $d(c,x) \leq e$ sein. In diesem Fall muss $d(c,c') > 2e$ für verschiedene $c, c' \in C$ gelten, denn anderenfalls könnte man ein $x \in A^n$ mit $d(c,x), d(c',x) \leq e$ konstruieren. Dies rechtfertigt folgende Definition.

Definition III.10.5. Ein Code C

(i) *erkennt* e Fehler, falls $d(C) > e$ gilt.



(ii) *korrigiert* e Fehler, falls $d(C) > 2e$ gilt.



Bemerkung III.10.6. Die Korrektur von Fehlern geschieht unter der statistischen Annahme, dass Fehler „selten“, unabhängig und gleichverteilt auftreten (maximum likelihood decoding). Bei Kratzern auf CDs ist dies in der Regel nicht gegeben, denn ein einziger Kratzer (zer)stört viele benachbarte Bits. Man benötigt in diesem Fall eine Vorverarbeitung, auf die wir nicht näher eingehen.

Beispiel III.10.7.

(i) Die *trivialen* Codes C mit $|C| = 1$ können zwar jeden Fehler korrigieren ($d(C) = \infty$), aber keine Information übertragen. Ebenso nennt man den Code $C = A^n$ mit Minimaldistanz 1 *trivial*. Beide sind in der Praxis uninteressant.

(ii) Der *Wiederholungscode* $W_n(A) := \{(a, \dots, a) \in A^n\}$ der Länge n hat Minimaldistanz n und kann daher $n-1$ Fehler erkennen und $\lfloor \frac{n-1}{2} \rfloor$ Fehler korrigieren. Beispielsweise kann das Wort (a,a,a,b,b,b) nicht eindeutig korrigiert werden. Treten mehr als $n/2$ Fehler auf, so wird sogar falsch „korrigiert“!

Definition III.10.8. Man nennt $H \in \{\pm 1\}^{n\times n}$ eine HADAMARD-*Matrix*, falls $HH^{\mathrm{t}} = n1_n$ gilt.

Beispiel III.10.9. Sicher sind $H_1 := (1)$ und $H_2 := \left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right)$ Hadamard-Matrizen. Sind H_n und H_m Hadamard-Matrizen vom Format $n \times n$ bzw. $m \times m$, so ist das Kronecker-Produkt $H_n \otimes H_m$ eine $nm \times nm$-Hadamard-Matrix, denn

$$(H_n \otimes H_m)(H_n \otimes H_m)^{\mathrm{t}} = H_n H_n^{\mathrm{t}} \otimes H_m H_m^{\mathrm{t}} = nm1_{nm}.$$

Insbesondere erhält man durch $H_{2^n} := H_2 \otimes \ldots \otimes H_2$ eine $2^n \times 2^n$-Hadamard-Matrix, die mit der Charaktertafel von C_2^n übereinstimmt (Beispiel II.13.41).

Lemma III.10.10. *Ist $H \in \{\pm 1\}^{n\times n}$ eine Hadamard-Matrix mit $n > 2$, so ist $4 \mid n$.*

Beweis. Durch Permutieren von Zeilen und Spalten bleibt H eine Hadamard-Matrix. Wir können daher annehmen, dass die ersten drei Zeilen von H die Form

$$\begin{pmatrix} 1 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 1 \\ 1 & \cdots & \cdots & \cdots & \cdots & 1 & -1 & \cdots & \cdots & \cdots & \cdots & -1 \\ 1 & \cdots & 1 & -1 & \cdots & -1 & 1 & \cdots & 1 & -1 & \cdots & -1 \end{pmatrix}$$

haben. Aus der Orthogonalität der Zeilen folgt leicht, dass die vier Abschnitte der dritten Zeile alle gleich lang sind. □

Bemerkung III.10.11. Eine offene Vermutung besagt, dass für jedes $k \geq 1$ Hadamard-Matrizen vom Format $4k \times 4k$ existieren (man kennt bislang keine Hadamard-Matrix der Größe 668×668).

Satz III.10.12. *Sei H eine $n \times n$-Hadamard-Matrix. Dann bilden die Zeilen von H und $-H$ einen Code C mit $2n$ Elementen und Minimaldistanz $\frac{n}{2}$.*

Beweis. Für verschiedene Zeilen v und w von H gilt $vw^{\mathrm{t}} = 0 = (-v)w^{\mathrm{t}}$. Dies zeigt $|C| = 2n$ und $d(v, w) = n/2 = d(C)$. □

Bemerkung III.10.13.

(i) Sei H eine $n \times n$-Hadamard-Matrix und C der zugehörige Code. Nach Satz III.10.12 kann C mindestens $\frac{n}{4} - 1$ Fehler korrigieren. Wir konstruieren eine Decodierungsfunktion $\gamma' \colon \{\pm 1\}^n \to C$ wie folgt: Für $x \in \{\pm 1\}^n$ sei x_k ein betragsmäßig größter Eintrag von Hx^{t}. Wir definieren $\gamma(x)$ als die k-te Zeile von $\pm H$, wobei $\pm$ das Vorzeichen von x_k ist. Weicht x an $e < \frac{n}{4}$ Koordinaten von einem Codewort c ab, so gilt

$$|x_k| \geq xc^{\mathrm{t}} = n - 2e > \frac{n}{2}.$$

Da sich jedes weitere Codewort an $\frac{n}{2}$ Koordinaten von c unterscheidet, gilt $|x_l| \leq \frac{n}{2}$ für alle $l \neq k$. Dies zeigt $\gamma'(x) = c$.

(ii) Der in Satz III.10.12 konstruierte Code für $n = 32$ wurde zur Bildübertragung bei der *Mariner-9-Mission* zum Mars verwendet.

(iii) In der Praxis sucht man Codes $C \subseteq A^n$ mit möglichst großer Minimaldistanz, um viele Fehler korrigieren zu können. Gleichzeitig möchte man viel Information mit möglichst kleiner Datenmenge übertragen, d. h. die (*Informations-*)*Rate*

$$r(C) := \log_q(|C|)/n$$

sollte groß sein. Der nächste Satz zeigt, dass man nicht gleichzeitig $d(C)$ und $r(C)$ maximieren kann, sondern je nach Anwendung ein Kompromiss erforderlich ist. Bei Liveübertragungen gibt man beispielsweise $r(C)$ den Vorzug, um Verzögerungen zu vermeiden.

Satz III.10.14. *Für jeden Code $C \subseteq A^n$ mit $d := d(C)$ und $e := \lfloor \frac{d-1}{2} \rfloor$ gilt*

$$|C| \leq q^{n-d+1} \qquad \text{(Singleton-Schranke)},$$

$$|C| \sum_{k=0}^{e} \binom{n}{k} (q-1)^k \leq q^n \qquad \text{(Hamming-Schranke)}.$$

Ist $d > n\frac{q-1}{q}$, so gilt

$$|C| \leq \frac{d}{d - n\frac{q-1}{q}} \qquad \text{(Plotkin-Schranke)}.$$

Beweis.

(i) Die Projektion auf die ersten $n-d+1$ Komponenten ist eine injektive Abbildung $f\colon C \to A^{n-d+1}$, denn aus $f(c) = f(c')$ folgt $d(c,c') \leq d-1$ und $c = c'$. Dies zeigt $|C| = |f(C)| \leq |A^{n-d+1}| = q^{n-d+1}$.

(ii) Wegen $d \geq 2e+1$ gilt $K_e(c) \cap K_e(c') = \varnothing$ für verschiedene $c, c' \in C$ nach der Dreiecksungleichung. Sei $x \in K_e(c)$ mit $d(c,x) = k$. Für die Wahl der k Positionen, an denen sich c und x unterscheidet, gibt es $\binom{n}{k}$ Möglichkeiten. An jeder dieser Stellen kann x einen von $q-1$ verbleibenden Werten annehmen. Dies zeigt

$$|K_e(c)| = \sum_{k=0}^{e} \binom{n}{k} (q-1)^k.$$

Schließlich ist

$$|C| \sum_{k=0}^{e} \binom{n}{k} (q-1)^k = \sum_{c \in C} |K_e(c)| = \Big| \bigcup_{c \in C} K_e(c) \Big| \leq |A^n| = q^n.$$

(iii) Sei $A = \{a_1, \ldots, a_q\}$ und $m_{ij} := |\{c \in C : c_i = a_j\}|$ für $1 \leq i \leq n$ und $1 \leq j \leq q$. Offenbar ist $\sum_{j=1}^{q} m_{ij} = |C|$ für $i = 1, \ldots, n$. Wir summieren die Distanzen aller $|C|^2$ Paare von Codewörtern. Die i-te Koordinate trägt genau

$$\sum_{j=1}^{q} m_{ij}(|C| - m_{ij}) = |C|^2 - \sum_{j=1}^{q} m_{ij}^2$$

zu dieser Summe bei. Die Cauchy-Schwarz-Ungleichung angewendet auf die Vektoren $(m_{ij} : j = 1, \ldots, q)$ und $(1, \ldots, 1)$ zeigt

$$|C|^2 = \Big(\sum_{j=1}^{q} m_{ij} \Big)^2 \leq q \sum_{j=1}^{q} m_{ij}^2.$$

Daher ist

$$|C|(|C|-1)d \leq \sum_{c,c' \in C} d(c,c') \leq \sum_{i=1}^{n}\sum_{j=1}^{q} m_{ij}(|C|-m_{ij}) \leq \sum_{i=1}^{n} |C|^2\Big(1-\frac{1}{q}\Big) \leq n|C|^2\frac{q-1}{q}.$$

Umstellen ergibt

$$|C|\Big(d - n\frac{q-1}{q}\Big) \leq d$$

und die Behauptung folgt aus der Voraussetzung $d - n\frac{q-1}{q} > 0$. □

Satz III.10.15. *Für alle $1 \leq d \leq n$ existiert ein Code $C \subseteq A^n$ mit $d(C) \geq d$ und*

$$|C| \sum_{k=0}^{d-1} \binom{n}{k}(q-1)^k \geq q^n \qquad \text{(Gilbert-Schranke).}$$

Beweis. Sei $C \subseteq A^n$ mit $d(C) \geq d$ und $|C|$ maximal. Für jedes $x \in A^n$ existiert dann ein $c \in C$ mit $d(x,c) < d$, denn anderenfalls könnte x zu C hinzufügen im Widerspruch zur Maximalität von $|C|$. Also ist

$$q^n = \Big|\bigcup_{c\in C} K_{d-1}(c)\Big| \leq \sum_{c\in C} |K_{d-1}(c)| = |C| \sum_{k=0}^{d-1} \binom{n}{k}(q-1)^k. \qquad \square$$

Beispiel III.10.16. Für $q = 2$, $n = 10$ erhält man folgende Abschätzungen für $|C|$:

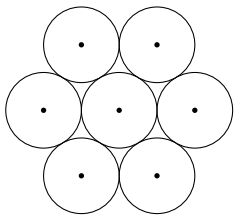
$d(C)$	Gilbert	Singleton	Hamming	Plotkin
1	2^{10}	2^{10}	2^{10}	
2	94	2^9	2^{10}	
3	16	256	93	
4	6	128	93	
5	3	64	15	
6	2	32	15	6
7	2	16	5	3

Sei o. B. d. A. $A = \{0,1\}$ und $(0,\ldots,0) \in C$. Im Fall $d(C) \geq 7$ besteht jedes nicht-triviale Codewort aus mindestens sieben Einsen. Zwei nicht-triviale Codewörter hätten daher mindestens vier gemeinsame Einsen. Dies zeigt $|C| \leq 2$.

Bemerkung III.10.17.

(i) Man nennt C einen MDS-*Code* (maximum distance separable), falls in der Singleton-Schranke Gleichheit gilt. Neben dem trivialen Code $C = A^n$ ist auch der Wiederholungscode W_n ein MDS-Code.

(ii) Gilt Gleichheit in der Hamming-Schranke, so heißt C *perfekt*. In diesem Fall ist $|C|$ eine q-Potenz und A^n die disjunkte Vereinigung von Kugeln um Codewörter mit Radius e.



Somit lässt sich *jeder* Fehler eindeutig „korrigieren“ (aber nicht immer richtig). Insbesondere ist $d(C) = 2e + 1$ ungerade. Der triviale Code $C = A^n$ ist der einzige perfekte Code mit $e = 0$. Für $q = 2$ und $n = 2e+1$ ist auch der Wiederholungscode W_n perfekt, denn jedes Wort $x \in \{0,1\}^n$ hat Distanz $\leq e$ zu genau einem der Codeworte $(0,\dots,0)$ oder $(1,\dots,1)$. Wir werden später sehen, dass es nur wenige weitere perfekte Codes gibt (vgl. Aufgabe III.53.

(iii) Nach SHANNONs Hauptsatz aus der Informationstheorie gibt es Codes C mit „guter“ Rate (aber großem n), sodass die Wahrscheinlichkeit einer fehlerhaften Decodierung beliebig klein ist. Der Beweis benutzt Statistik und ist nicht konstruktiv.

Beispiel III.10.18. Sei $A = \{0,1\}$ und $p = 10^{-3}$ die Wahrscheinlichkeit, dass ein Symbol falsch übertragen wird (also 0 statt 1 und umgekehrt). Sei $q := 1 - p$. Die Wahrscheinlichkeit einer fehlerfreien Übertragung von $n = 100$ Symbolen ohne Codierung beträgt dann $q^{100} \approx 0{,}90$. Unter Benutzung des Codes W_3 steigt die Wahrscheinlichkeit auf $(q^3 + 3q^2p)^{100} \approx 0{,}9997$.

Definition III.10.19. Codes $C, D \subseteq A^n$ heißen *äquivalent*, falls eine Permutation $\pi \in S_n$ mit

$$(x_1,\dots,x_n) \in C \iff (x_{\pi(1)},\dots,x_{\pi(n)}) \in D$$

existiert. Für $C = D$ bilden die entsprechenden π die *Automorphismengruppe* $\mathrm{Aut}(C)$ von C.

Bemerkung III.10.20. Äquivalente Codes haben offenbar die gleichen Eigenschaften (Länge, Mächtigkeit, Minimaldistanz, Rate, ...). Man interessiert sich daher nur für „interessante“ Äquivalenzklassenvertreter.

Definition III.10.21. Sei $A = \mathbb{F}_q$ ein endlicher Körper. Ein Code $C \subseteq \mathbb{F}_q^n$ heißt *linear*, falls C ein Untervektorraum von $\mathbb{F}_q^n$ ist. Ist $k := \dim C$ und $d := d(C)$, so ist C ein (n,k,d)-Code (noch genauer $(n,k,d)_q$-Code). Die Rate von C ist $r(C) = k/n$. Außerdem nennt man $w(x) := d(x,0)$ das *Gewicht* von $x \in \mathbb{F}_q^n$.

Beispiel III.10.22.

(i) Der *Paritätscode*

$$P_n := \Big\{ x \in \mathbb{F}_q^n : \sum_{i=1}^{n} x_i = 0 \Big\}$$

der Länge n hat Dimension $k = n - 1$ und Minimaldistanz $d = 2$. Er kann also einen Fehler erkennen, aber nicht korrigieren. Eine konkrete Version ist der ASCII-*Code* mit $q = 2$ und $n = 8$. Mit den ersten 7 Bits stellt man eines von $2^7 = 128$ häufig benutzten Symbolen dar:

`	´	ˆ	˜	¨	˝	°	ˇ	˘	¯	˙	¸	˛	,	‹	›
“	”	„	«	»	–	—		0	ı	ȷ	ff	fi	fl	ffi	ffl
␣	!	"	#	$	%	&	’	(	)	*	+	,	-	.	/
0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?
@	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
P	Q	R	S	T	U	V	W	X	Y	Z	[	\	]	^	_
‘	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
p	q	r	s	t	u	v	w	x	y	z	{	|	}	~	-

Das achte Bit (*Prüfbit*) ergibt sich aus der Summe der sieben vorherigen Bits (modulo 2). Beispielsweise hat der Buchstabe b Position $98 = 2^6 + 2^5 + 2$ und entspricht daher dem Codewort $(1, 1, 0, 0, 0, 1, 0, 1)$ (Prüfbit = 1). Die acht Bits ergeben zusammen ein *Byte* und lassen sich effizient auf Computern verarbeiten.

(ii) Den ISBN-*Code*

$$C := \left\{ x \in \mathbb{F}_{11}^{10} : \sum_{l=1}^{10} l x_l = 0 \right\} \leq \mathbb{F}_{11}^{10}$$

mit Länge $n = 10$, Dimension $k = 9$ und Minimaldistanz $d = 2$ haben wir bereits in Beispiel I.2.27 kennen gelernt.

Bemerkung III.10.23.

(i) Für $q = 2$ (bzw. $q = 3$) spricht man von *binären* (bzw. *ternären*) Codes.

(ii) Offenbar ist die Hamming-Distanz auf $\mathbb{F}_q^n$ *translationsinvariant*, d. h. für $x, y, z \in \mathbb{F}_q^n$ gilt $d(x, y) = d(x - z, y - z)$. Für einen linearen Code $C \leq \mathbb{F}_q^n$ ist daher

$$\begin{aligned} d(C) &= \min\{d(x, y) : x, y \in C,\ x \neq y\} = \min\{d(x - y, 0) : x, y \in C,\ x \neq y\} \\ &= \min\{w(c) : c \in C \setminus \{0\}\}. \end{aligned}$$

Man nennt $d(C)$ daher auch *Minimalgewicht* von C.

(iii) Äquivalente Codes sind isomorph als Vektorräume, aber nicht umgekehrt. Oft ist es zweckmäßiger Codes $C, C' \leq \mathbb{F}_q^n$ als äquivalent zu betrachten, wenn sie unter einer verallgemeinerten Permutationsmatrix $P \in \mathbb{F}_q^{n \times n}$ ineinander übergehen. Hierbei hat P in jeder Zeile und in jeder Spalte genau einen von 0 verschiedenen Eintrag. Es gibt also $\pi \in S_n$ und $a_1, \ldots, a_n \in \mathbb{F}_q^\times$ mit

$$(c_1, \ldots, c_n) \in C \iff (a_1 c_{\pi(1)}, \ldots, a_n c_{\pi(n)}) \in C'$$

für alle $c \in \mathbb{F}_q^n$. Offenbar haben C und C' immer noch die gleichen Eigenschaften.

(iv) Die Singleton-Schranke für (n, k, d)-Codes hat die Form $d \leq n - k + 1$ (unabhängig von q). Die Hamming-Schranke lässt sich in der Form

$$\sum_{i=0}^{e} \binom{n}{i} (q-1)^i \leq q^{n-k}$$

schreiben. Die Gilbert-Schranke gilt im Wesentlichen auch für lineare Codes: Sei $1 \leq d \leq n$ gegeben und C ein (n, k, d)-Code mit k maximal. Angenommen es existiert $x \in \mathbb{F}_q^n$ mit $d(x, c) \geq d$ für alle $c \in C$. Für $\alpha \in \mathbb{F}_q^\times$ und $c \in C$ gilt dann

$$w(c + \alpha x) = d(c + \alpha x, 0) = d(c, -\alpha x) = d(-\alpha^{-1} c, x) \geq d.$$

Daher wäre $C + \mathbb{F}_q x$ ein $(n, k + 1, d)$-Code im Widerspruch zur Maximalität von k. Es gilt also

$$\sum_{i=0}^{d-1} \binom{n}{i} (q-1)^i \geq q^{n-k}.$$

Beispiel III.10.24.

(i) Sei C ein perfekter $(n,k,7)$-Code mit $k \geq 1$ über $\mathbb{F}_2$. Dann ist $n \geq 7$ und

$$1 + n + \frac{n(n-1)}{2} + \frac{n(n-1)(n-2)}{6} = \sum_{i=0}^{e} \binom{n}{i} = 2^{n-k}.$$

Multiplikation mit 6 liefert

$$(n+1)(6 + n(n-1)) = 3 \cdot 2^{n-k+1}.$$

Die Substitution $N := n + 1 \geq 8$ führt zu

$$N(N^2 - 3N + 8) = 3 \cdot 2^{n-k+1}.$$

Ist N durch 16 teilbar, so ist $N^2 - 3N + 8 \equiv 8 \pmod{16}$ und es folgt $N^2 - 3N + 8 \in \{8, 24\}$. Dies widerspricht $N(N-3) + 8 \geq 8 \cdot 5 + 8 > 24$. Also ist N nicht durch 16 teilbar und man erhält $N \mid 24$. Wegen $N \geq 8$ ergeben sich folgende Fälle:

- $(n,k) = (7,1)$: Dies sind die Parameter des Wiederholungscodes W_7.
- $n = 11$: Hier geht die Gleichung nicht auf: $N^2 - 3N + 8 = 12 \cdot 9 + 8 = 116 = 4 \cdot 29$.
- $(n,k) = (23,12)$: Ein solcher Code wird in Beispiel III.10.42 definiert.

(ii) Für die Parameter $(n,k,d)_q = (90,78,5)_2$ erhält man ebenfalls $\sum_{i=0}^{2} \binom{n}{i} = 2^{n-k}$. Das folgende Lemma mit $s = 2$ zeigt, dass es keinen solchen Code geben kann.

Lemma III.10.25. *Sei C ein perfekter $(n,k,2e+1)$-Code über $\mathbb{F}_q$ und $0 \leq s \leq e$. Dann ist*

$$\binom{2e-s+1}{e} \;\Bigg|\; \binom{n-s}{e-s+1}(q-1)^{e-s+1}.$$

Beweis. Sei $V_s := \{x \in \mathbb{F}_q^n : \forall i = 1, \ldots, s : x_i = 1\}$ und

$$C_s := \{c \in C \cap V_s : w(c) = 2e+1\}.$$

Jeder der $\binom{n-s}{e-s+1}(q-1)^{e-s+1}$ Vektoren $x \in V_s$ mit $w(x) = e+1$ liegt in genau einer Kugel $B_e(c)$ mit $c \in C$. Wegen $w(c) \geq 2e+1$ gilt $x_i \neq 0 \Rightarrow x_i = c_i$ und $c \in C_s$. Andererseits enthält $B_e(c)$ genau $\binom{2e-s+1}{e}$ Vektoren $x \in V_s$ mit $w(x) = e+1$. Dies zeigt

$$|C_s| = \frac{\binom{n-s}{e-s+1}}{\binom{2e-s+1}{e}}(q-1)^{e-s+1} \in \mathbb{N}. \qquad \square$$

Satz III.10.26. *Für jeden (n,k,d)-Code $0 \neq C \leq \mathbb{F}_q^n$ gilt*

$$\sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil \leq n \qquad \text{(Griesmer-Schranke).}$$

Beweis. Induktion nach k: Für $k = 1$ ist die Behauptung trivial. Sei also $k \geq 2$. Sei $b_1, \ldots, b_k \in C$ eine Basis von C. Nach Übergang zu einem äquivalenten Code wie in Bemerkung III.10.23(iii) können wir $b_1 = (1, \ldots, 1, 0, \ldots, 0)$ mit $w(b_1) = d$ annehmen. Sei $b_i' \in \mathbb{F}_q^{n-d}$ der aus den letzten $n - d$ Koordinaten von b_i gebildete Vektor $(i = 2, \ldots, k)$.

Angenommen es gibt eine nicht-triviale Linearkombination c' von $b_2', \ldots, b_k'$ mit $w(c') < d/q$. Sei $c = (c_1, c') \in C$ die entsprechende Linearkombination von $b_2, \ldots, b_k$. Wegen $w(c) \geq d$ verschwinden höchstens $w(c')$ Koordinaten von c_1. Wegen $(q-1)w(c') < d - w(c')$ tritt ein $\lambda \in \mathbb{F}_q^\times$ mehr als $w(c')$-Mal in c_1 auf. Wir ersetzen c durch $\lambda^{-1}c$. Dann gilt

$$d(c, b_1) < d - w(c') + w(c') = d$$

und es folgt $c = b_1$. Dies widerspricht der linearen Unabhängigkeit von $b_1, \ldots, b_k$. Also ist $w(c') \geq d/q$. Insgesamt ist $C' := \langle b_2', \ldots, b_k' \rangle \leq \mathbb{F}_q^{n-d}$ ein $(k-1)$-dimensionaler Code mit $d' := d(C') \geq d/q$. Nach Induktion gilt

$$\sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil = d + \sum_{i=1}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil \leq d + \sum_{i=0}^{k-2} \left\lceil \frac{d'}{q^i} \right\rceil \leq d + n - d = n. \qquad \square$$

Definition III.10.27. Sei $C \leq \mathbb{F}_q^n$ ein (n, k, d)-Code.

(i) Man nennt $G \in \mathbb{F}_q^{k \times n}$ *Erzeuger-Matrix* von C, falls $C = \{xG : x \in \mathbb{F}_q^k\}$ gilt. Außerdem nennt man $H \in \mathbb{F}_q^{(n-k) \times n}$ *Kontroll-Matrix* von C, falls $C = \{x \in \mathbb{F}_q^n : Hx^{\mathrm{t}} = 0\}$ gilt.

(ii) Wie üblich definiert

$$xy^{\mathrm{t}} = \sum_{i=1}^{n} x_i y_i \qquad (x, y \in \mathbb{F}_q^n)$$

eine Bilinearform auf $\mathbb{F}_q^n$. Man nennt

$$C^\perp := \{x \in \mathbb{F}_q^n : \forall c \in C : xc^{\mathrm{t}} = 0\} \leq \mathbb{F}_q^n$$

den zu C *dualen* Code. Im Fall $C = C^\perp$ heißt C *selbstdual*.

Bemerkung III.10.28.

(i) Genau dann ist $G \in \mathbb{F}_q^{k \times n}$ eine Erzeuger-Matrix von C, wenn die Zeilen von G eine Basis von C bilden. Genau dann ist $H \in \mathbb{F}_q^{(n-k) \times n}$ eine Kontroll-Matrix, wenn die Zeilen von H eine Basis für den Lösungsraum des homogenen Gleichungssystems $Gx = 0$ bilden. Insbesondere existieren beide Matrizen stets (aber nicht eindeutig) und haben vollen Rang.

(ii) Indem man zu einem äquivalenten Code übergeht, kann man annehmen, dass die ersten k Spalten von G linear unabhängig sind. Durch eine Basistransformation erreicht man, dass G die Form $G = (1_k | L)$ hat. Jedes Codewort ist also bereits durch die ersten k Komponenten eindeutig bestimmt. Nun ist $H = (-L^{\mathrm{t}} | 1_{n-k})$ eine Kontroll-Matrix von C.

(iii) Die Minimaldistanz ist offenbar die minimale Anzahl linear abhängiger Spalten einer Kontroll-Matrix.

(iv) Ist G eine Erzeuger-Matrix von C, so liegt $C^\perp$ im Lösungsraum von $Gx = 0$ und es folgt $\dim(C^\perp) \leq n - k$. Ist H eine Kontroll-Matrix von C, so liegen die Zeilen von H in $C^\perp$ und es folgt $\dim(C^\perp) \geq n - k$. Also ist $\dim(C^\perp) = n - k$ und G (bzw. H) ist eine Kontroll-Matrix (bzw. Erzeuger-Matrix) von $C^\perp$. Selbstduale Codes haben daher gerade Länge $n = 2k$ und Dimension k.

(v) Es gilt $(C^\perp)^\perp = C$. Im Gegensatz zum euklidischen Raum $\mathbb{R}^n$, kann über $\mathbb{F}_q^n$ durchaus $C = C^\perp \neq 0$ eintreten. Zum Beispiel für $C = W_2 = \langle (1,1) \rangle \leq \mathbb{F}_2^2$.

Beispiel III.10.29. Der Wiederholungscode W_n hat folgende Erzeuger- und Kontrollmatrizen:

$$G = \begin{pmatrix} 1 & \cdots & 1 \end{pmatrix}, \qquad H = \begin{pmatrix} 1 & & 0 & -1 \\ & \ddots & & \vdots \\ 0 & & 1 & -1 \end{pmatrix}.$$

Offenbar ist $W_n^\perp = P_n$ der Paritätscode.

Satz III.10.30. *Mit der Bezeichnung aus Bemerkung III.10.23*(iii) *gibt es genau* $\binom{Q+n-k-1}{n-k}$ *nicht-äquivalente lineare* $(n,k)_q$*-Codes, wobei* $Q := 1 + \frac{q^k-1}{q-1}$.

Beweis. Mit dem Gauß-Algorithmus lässt sich die Erzeuger-Matrix G in genau eine reduzierte Zeilenstufenform überführen. Durch Multiplikation mit einer verallgemeinerten Permutationsmatrix von rechts ändert sich die Äquivalenzklasse nicht. Da G vollen Rank hat, kann man durch Koordinatenpermutation erreichen, dass die ersten k Spalten eine Einheitsmatrix bilden. Die übrigen $n-k$ Spalten bilden eine Multimenge von $\mathbb{F}_q^k$. Durch Skalieren kann man annehmen, dass die von 0 verschiedenen Spalten mit einer 1 beginnen. Man hat also eine $(n-k)$-elementige Multimenge aus $Q = 1 + \frac{q^k-1}{q-1}$ möglichen Vektoren. Die Anzahl dieser Multimengen beträgt $\binom{Q+n-k-1}{n-k}$.[1] □

Bemerkung III.10.31. Für $k = 1$ erhält man $Q = 2$ und genau n nicht-äquivalente Codes. Diese werden durch die Vektoren der Form $(1, \ldots, 1, 0, \ldots, 0)$ erzeugt.

Satz III.10.32 (Syndrom-Decodierung)**.** *Sei* $C \leq \mathbb{F}_q^n$ *ein linearer Code. Aus jeder Nebenklasse* $x + C \in \mathbb{F}_q^n / C$ *wählen wir einen Vertreter* $e_x \in x + C$*, sodass* $w(e_x)$ *minimal ist. Dann ist* $c := x - e_x \in C$ *ein Codewort mit minimaler Distanz zu* x*. Man kann also* x *zu* c *decodieren.*

Beweis. Sei $c' \in C$ mit $d(x,c') < d(x,c)$. Dann ist $e := x - c' \in x + C$ mit $w(e) = d(x,c') < d(x,c) = w(e_x)$ im Widerspruch zur Wahl von e_x. □

Bemerkung III.10.33. Sei $k := \dim C$. In der Praxis bestimmt man zunächst für jede der q^{n-k} Nebenklassen $x + C$ ein e_x wie in Satz III.10.32. Um zu entscheiden, ob ein $y \in \mathbb{F}_q^n$ in der gleichen Nebenklasse wie e_x liegt, benutzt man die Kontroll-Matrix H von C. Es gilt

$$x + C = y + C \iff x - y \in C \iff H(x-y) = 0 \iff Hx = Hy.$$

Man nenn Hx das *Syndrom* von x bzgl. C. Im Gegensatz zu nicht-linearen Codes hat man also einen „effizienten“ Decodierungsalgorithmus.

Definition III.10.34. Sei $m \geq 2$. Seien $\langle v_1 \rangle, \ldots, \langle v_n \rangle$ die eindimensionalen Untervektorräume von $\mathbb{F}_q^m$. Der Code H_n mit Kontroll-Matrix $\begin{pmatrix} v_1 & \cdots & v_n \end{pmatrix} \in \mathbb{F}_2^{m \times n}$ heißt *Hamming-Code* der Länge n.

[1] Siehe Satz 1.22 in Diskrete Mathematik

Beispiel III.10.35. Sei $q = 2$, $m = 3$ und $n = 2^3 - 1 = 7$. Eine Kontroll-Matrix von H_7 ist

$$\begin{pmatrix} 1 & . & . & . & 1 & 1 & 1 \\ . & 1 & . & 1 & . & 1 & 1 \\ . & . & 1 & 1 & 1 & . & 1 \end{pmatrix}.$$

Dies liefert die Erzeuger-Matrix

$$\begin{pmatrix} . & 1 & 1 & 1 & . & . & . \\ 1 & . & 1 & . & 1 & . & . \\ 1 & 1 & . & . & . & 1 & . \\ 1 & 1 & 1 & . & . & . & 1 \end{pmatrix}.$$

Satz III.10.36. *Der Hamming-Code H_n hat Länge $n = \frac{q^m-1}{q-1}$, Dimension $n - m$ und Minimaldistanz 3. Außerdem ist H_n perfekt.*

Beweis. Jedes $v \in \mathbb{F}_q^n \setminus \{0\}$ spannt einen eindimensionalen Unterraum auf. Jeder solche Unterraum besitzt q Vektoren und je zwei verschiedene Unterräume haben trivialen Schnitt. Dies zeigt $n = \frac{q^m-1}{q-1}$. Da die Standardbasisvektoren $\{(1, 0, \ldots, 0), \ldots, (0, \ldots, 0, 1)\}$ bis auf Skalierung als Spalten der Kontroll-Matrix H auftreten, hat H vollen Rang und es folgt $k := \dim H_n = n - m$. Da je zwei verschiedene Spalten von H linear unabhängig sind, gilt $d(H_n) \geq 3$. Andererseits treten die linear abhängigen Vektoren $(1, 0, \ldots, 0)$, $(0, 1, 0, \ldots, 0)$ und $(1, 1, 0, \ldots, 0)$ bis auf Skalierung als Spalten von H auf. Somit ist $d(H_n) = 3$.

Die Hamming-Schranke mit $e = 1$ ergibt

$$\sum_{i=0}^{1} \binom{n}{i} (q-1)^i = 1 + n(q-1) = q^m = q^{n-k}.$$

Also ist H_n perfekt. □

Bemerkung III.10.37.

(i) Der Hamming-Code hängt von der Wahl der v_i ab. Verschiedene Wahlen der v_i liefern allerdings äquivalente Codes im Sinn von Bemerkung III.10.23(iii).

(ii) Die Korrektur von einem Fehler lässt sich im Hamming-Code besonders effizient durchführen. Sei H die Kontroll-Matrix, $c \in H_n$ und $x = c + e$ mit $w(e) = 1$. Dann ist $Hx = H(c + e) = He$. Die Position des aufgetretenen Fehlers ist die Position der Spalte Hx in H.

(iii) Ein Nachteil der Hamming-Codes ist, dass sie nur für gewisse n existieren (insbesondere wenn q klein ist).

Satz III.10.38. *Jeder lineare perfekte $(n, k, 3)$-Code C ist zu H_n äquivalent.*

Beweis. Die Hamming-Schranke liefert $1 + n(q-1) = q^{n-k}$, d. h. $n = \frac{q^{n-k}-1}{q-1}$. Wegen $d(C) = 3$ sind je zwei Spalten einer Kontroll-Matrix $H \in \mathbb{F}_q^{(n-k)\times n}$ von C linear unabhängig. Die Anzahl der 1-dimensionalen Unterräume von $\mathbb{F}_q^{n-k}$ ist andererseits $\frac{q^{n-k}-1}{q-1} = n$. Daher ist H bis auf Äquivalenz die Kontroll-Matrix von H_n. □

Beispiel III.10.39. Für $q = 2$ ist W_3 zu H_3 äquivalent.

Definition III.10.40. Für einen linearen Code $C \leq \mathbb{F}_q^n$ sei

$$\widehat{C} := \Big\{(x_1, \ldots, x_{n+1}) \in \mathbb{F}_q^{n+1} : (x_1, \ldots, x_n) \in C,\ \sum_{i=1}^{n+1} x_i = 0\Big\} \leq \mathbb{F}_q^{n+1}$$

der *erweiterte* Code.

Bemerkung III.10.41. Sicher ist $\dim \widehat{C} = \dim C$ und $d(\widehat{C}) \geq 2$. Ist C ein binärer Code mit ungeradem Gewicht d, so gilt $d(\widehat{C}) = d + 1$. Auf diese Weise lässt sich die Anzahl der erkennbaren (aber nicht der korrigierbaren) Fehler leicht erhöhen. Gleichzeitig sinkt die Rate von $\frac{k}{n}$ zu $\frac{k}{n+1}$.

Beispiel III.10.42.

(i) Der Paritätscode P_n ist die Erweiterung des trivialen Codes $\mathbb{F}_q^{n-1}$.

(ii) Der erweiterte Hamming-Code $\widehat{H_7}$ über $\mathbb{F}_2$ ist ein $(8, 4, 4)$-Code mit Erzeuger-Matrix

$$G = \begin{pmatrix} . & 1 & 1 & 1 & . & . & . & 1 \\ 1 & . & 1 & . & 1 & . & . & 1 \\ 1 & 1 & . & . & . & 1 & . & 1 \\ 1 & 1 & 1 & . & . & . & 1 & . \end{pmatrix}$$

nach Beispiel III.10.35. Wegen $GG^{\mathrm{t}} = 0$ ist $\widehat{H_7}$ selbstdual.

(iii) Nach Aufgabe III.54 ist $\widehat{H_7}$ zu den Codes C und $\widetilde{C}$ mit Erzeugermatrizen

$$G = \begin{pmatrix} 1 & 1 & . & 1 & . & . & . & 1 \\ . & 1 & 1 & . & 1 & . & . & 1 \\ . & . & 1 & 1 & . & 1 & . & 1 \\ . & . & . & 1 & 1 & . & 1 & 1 \end{pmatrix}, \qquad \widetilde{G} = \begin{pmatrix} . & . & . & 1 & . & 1 & 1 & 1 \\ . & . & 1 & . & 1 & 1 & . & 1 \\ . & 1 & . & 1 & 1 & . & . & 1 \\ 1 & . & 1 & 1 & . & . & . & 1 \end{pmatrix}$$

äquivalent. Mit deren Hilfe definieren wir den *erweiterten binären* Golay-*Code* durch

$$G_{24} := \big\{(c + e, d + e, c + d + e) : c, d \in C,\ e \in \widetilde{C}\big\} \leq \mathbb{F}_2^{24}.$$

Der *binäre Golay-Code* $G_{23} \leq \mathbb{F}_2^{23}$ entsteht aus G_{24}, indem man die letzte Koordinate aller Codeworte streicht.

Satz III.10.43. *Es gilt*

(i) G_{24} *ist ein selbstdualer* $(24, 12, 8)$*-Code.*

(ii) G_{23} *ist ein perfekter* $(23, 12, 7)$*-Code.*

Beweis (Turyn).

(i) Wir benutzen die Bezeichnungen aus Beispiel III.10.42. Addiert man die 1., 3. und 4. Zeile von G bzw. $\widetilde{G}$, so erhält man $\mathbb{F}_2(1, \ldots, 1) \subseteq C \cap \widetilde{C}$. Wir zeigen, dass $C \cap \widetilde{C}$ nicht größer ist. Seien dafür

$x, y \in \mathbb{F}_2^4$ mit $xG = y\widetilde{G}$. Dann ist $(x,y)\binom{G}{\widetilde{G}} = 0$. Der Gauß-Algorithmus führt zu

$$\binom{G}{\widetilde{G}} \sim \left(\begin{array}{cccccccc} 1&1&.&1&.&.&.&1\\ .&1&1&.&1&.&.&1\\ .&.&1&1&.&1&.&1\\ .&.&.&1&1&.&1&1\\ \hline .&.&.&.&1&1&.&.\\ .&.&.&1&1&.&.&.\\ .&.&1&1&.&.&.&.\\ .&1&1&.&.&.&.&. \end{array}\right) \sim \left(\begin{array}{cccccccc} 1&1&.&1&.&.&.&1\\ .&1&1&.&1&.&.&1\\ .&.&1&1&.&1&.&1\\ .&.&.&1&1&.&1&1\\ \hline .&.&.&.&1&1&.&.\\ .&.&.&.&.&.&1&1\\ .&.&.&.&.&1&.&1\\ .&.&.&.&1&.&.&1 \end{array}\right) \sim \left(\begin{array}{cccccccc} 1&1&.&1&.&.&.&1\\ .&1&1&.&1&.&.&1\\ .&.&1&1&.&1&.&1\\ .&.&.&1&1&.&1&1\\ \hline .&.&.&.&1&1&.&.\\ .&.&.&.&.&1&.&1\\ .&.&.&.&.&.&1&1\\ .&.&.&.&.&.&.&. \end{array}\right)$$

Also hat $\binom{G}{\widetilde{G}}$ Rang 7 und es folgt $C \cap \widetilde{C} = \mathbb{F}_2(1,\dots,1)$. Die Codeworte der Form $(c,0,c)$, $(0,d,d)$ und (e,e,e) mit $c,d \in C$ und $e \in \widetilde{C}$ bilden ein Erzeugendensystem von G_{24}. Im Fall $(c,0,c)+(0,d,d) = (e,e,e)$ ist $c = e = d = c+d = 0$. Dies zeigt

$$\dim G_{24} = \dim C + \dim C + \dim \widetilde{C} = 4+4+4 = 12.$$

Da C und $\widetilde{C}$ mit $\widehat{H_7}$ selbstdual sind, sind die Vektoren $(c,0,c)$, $(0,d,d)$ und (e,e,e) paarweise orthogonal. Also ist auch G_{24} selbstdual.

Je zwei Zeilen c und d von G (oder $\widetilde{G}$) haben Gewicht 4. Wegen $cd^{\mathrm{t}} = 0$ haben c und d eine gerade Anzahl von Einsen gemeinsam. In der Summe $c+d$ heben sich die gemeinsamen Einsen gegenseitig auf. Daraus folgt, dass $w(c+d)$ durch 4 teilbar ist. Für eine weitere Zeile e von G ist nun auch $w(c+d+e)$ durch 4 teilbar usw. Insgesamt ist $4 \mid w(c)$ für alle $c \in C \cup \widetilde{C}$. Mit dem gleichen Argument folgt $4 \mid w(x)$ für alle $x \in G_{24}$, da auch G_{24} selbstdual ist. Insbesondere ist $d(G_{24}) \geq 4$. Nehmen wir an, es existiert $x = (c+e, d+e, c+d+e) \in G_{24}$ mit $d(x) = 4$. Da jede der drei Komponenten gerades Gewicht hat, muss einer der drei Komponenten 0 sein. Dann ist $e \in C \cap \widetilde{C} = \mathbb{F}_2(1,\dots,1)$ und man erhält leicht einen Widerspruch. Daher ist $d(G_{24}) \geq 8$. Für $c \in C$ mit $w(c) = 4$ ist umgekehrt $w((c,0,c)) = 8 \leq d(G_{24})$.

(ii) Wegen $d(G_{24}) = 8$ ist die Projektion $G_{24} \to G_{23}$ injektiv. Also ist G_{23} ein $(23,12,d)$-Code mit $d \geq 7$. Streicht man die letzte Koordinate aus $(c,0,c) \in G_{24}$ mit $c = (1,1,0,1,0,0,0,1) \in C$, so erhält man ein Codewort mit Gewicht 7. Dies zeigt $d = 7$. Die Hamming-Schranke hat nun die Form

$$\sum_{i=0}^{3} \binom{23}{i} = 1 + 23 + 23\cdot 11 + 23\cdot 11\cdot 7 = 1 + 23\cdot 89 = 2048 = 2^{23-12},$$

d. h. G_{23} ist perfekt. □

Definition III.10.44. Der lineare Code $G_{12} \leq \mathbb{F}_3^{12}$ mit Erzeuger-Matrix

$$\begin{pmatrix} 1&.&.&.&.&.&1&1&1&1&1&.\\ .&1&.&.&.&.&.&1&-1&-1&1&-1\\ .&.&1&.&.&.&1&.&1&-1&-1&-1\\ .&.&.&1&.&.&-1&1&.&1&-1&-1\\ .&.&.&.&1&.&-1&-1&1&.&1&-1\\ .&.&.&.&.&1&1&-1&-1&1&.&-1 \end{pmatrix}$$

heißt *erweiterter ternärer Golay-Code* G_{12}. Durch Streichen der letzten Koordinate erhält man den *ternären Golay-Code* G_{11}.

Satz III.10.45. *Es gilt*

(i) G_{12} *ist ein selbstdualer* $(12, 6, 6)$*-Code.*

(ii) G_{11} *ist ein perfekter* $(11, 6, 5)$*-Code.*

Beweis.

(i) Sei M die in Definition III.10.44 angegebene Erzeuger-Matrix von G_{12}. Da M Rang 6 hat, ist G_{12} ein $(12, 6)$-Code. Offenbar hat jede Zeile von M Gewicht 6. Man überprüft außerdem, dass die Zeilen von M paarweise orthogonal sind. Daher ist G_{12} selbstdual. Für $c = (x_1, \ldots, x_{12}) \in C$ gilt somit $w(c) = x_1^2 + \ldots + x_{12}^2 = cc^{\mathrm{t}} \equiv 0 \pmod 3$. Zwei verschiedene Zeilen c und d von M unterscheiden sich an genau zwei Stellen auf den ersten sechs Koordinaten. Auf den letzten sechs Koordinaten unterscheiden sich c und d mindestens an den beiden Positionen der Nullen. Jede Linearkombination x von c und d hat daher Gewicht $w(x) = 6$ wegen $3 \mid w(x)$. Also besitzt x genau zwei Nullen auf den letzten sechs Koordinaten. Eine Linearkombination von drei verschiedenen Zeilen von M hat folglich mindestens Gewicht 6. Jede Linearkombination von mehr als drei Zeilen hat bereits mindestens vier von Null verschiedene Einträge auf den ersten sechs Koordinaten. Dies zeigt $d(G_{12}) = 6$.

(ii) Wegen $d(G_{12}) = 6$ ist die Projektion $G_{12} \to G_{11}$ injektiv. Also ist G_{11} ein $(11, 6, 5)$-Code. Die Hamming-Schranke hat die Form

$$1 + \binom{11}{1} 2 + \binom{11}{2} 4 = 1 + 22 + 220 = 243 = 3^5 = 3^{11-6},$$

d. h. G_{11} ist perfekt. □

Bemerkung III.10.46.

(i) VAN LINT, TIETÄVÄINEN haben bewiesen, dass jeder lineare perfekte Code zu einem der folgenden Codes äquivalent ist:

- der triviale $(n, n, 0)$-Code $\mathbb{F}_q^n$.
- der triviale $(n, 0, n)$-Code $\{0\}$.
- der binäre $(2n + 1, 1, 2n + 1)$-Wiederholungscode $W_{2n+1} = \mathbb{F}_2(1, \ldots, 1)$.
- der $(n, n - m, 3)$-Hamming-Code H_n, wobei $n = \frac{q^m-1}{q-1}$.
- der binäre Golay-Code G_{23}.
- der ternäre Golay-Code G_{11}.

Die Klassifikation nicht-linearer Codes über beliebigen Alphabeten ist jedoch noch offen (vgl. Aufgabe III.53).

(ii) Der Code G_{24} wurde von den Voyager-Raumsonden benutzt, um Bilder vom Jupiter zur Erde zu senden. Die Automorphismengruppe $\mathrm{Aut}(G_{24})$ ist zur sporadisch einfachen *Mathieugruppe* M_{24} der Ordnung 244.823.040 isomorph. Der 2020 an Covid verstorbene John Conway bezeichnete M_{24} als „the most remarkable of all finite groups“.

(iii) Codes mit vorgegebenen Parametern kann man in der Datenbank `http://codetables.de/` nachschlagen. Man findet dort beispielsweise einen $(32, 14, 8)_2$-Code, während die Existenz eines $(32, 14, 9)_2$-Codes noch offen ist.

Definition III.10.47. Sei $C \subseteq \mathbb{F}_q^n$ ein Code und $w_i := |\{c \in C : w(c) = i\}|$ für $i = 0, \ldots, n$. Man nennt

$$W_C(X) := \sum_{c \in C} X^{w(c)} = w_0 + w_1 X + \ldots + W_n X^n \in \mathbb{Z}[X]$$

die *erzeugende Funktion* von C.

Bemerkung III.10.48. Aus $W_C(X)$ lässt sich offenbar $|C| = w_0 + \ldots + w_n$, sowie $d(C) = \min\{i \geq 1 : w_i \neq 0\}$ ablesen.

Satz III.10.49 (MacWilliams-Identität)**.** *Sei $C \leq \mathbb{F}_q^n$ ein linearer Code der Dimension k. Dann ist*

$$W_{C^\perp}(X) = q^{-k}\big(1 + (q-1)X\big)^n W_C\Big(\frac{1-X}{1+(q-1)X}\Big).$$

Beweis. Sei $V := \mathbb{F}_q^n$. Da $(\mathbb{F}_q, +)$ abelsch ist, existiert ein nicht-trivialer Homomorphismus $\chi\colon \mathbb{F}_q \to \mathbb{C}^\times$. Für $v \in V$ ist $C \to \mathbb{C}^\times$, $c \mapsto \chi(cv^{\mathrm{t}})$ ein Charakter von C. Für $c \in C$ sei

$$\alpha(c) := \sum_{v \in V} \chi(cv^{\mathrm{t}}) X^{w(v)} \in \mathbb{C}[X].$$

Nach der ersten Orthogonalitätsrelation (Satz II.13.22) gilt

$$\sum_{c \in C} \alpha(c) = \sum_{v \in V} X^{w(v)} \sum_{c \in C} \chi(cv^{\mathrm{t}}) = \sum_{v \in C^\perp} |C| X^{w(v)} = q^k W_{C^\perp}(X).$$

Wir schreiben nun $v = (v_1, \ldots, v_n)$ und $w(v_i) = 1$ falls $v_i \neq 0$ und $w(v_i) = 0$. Dann ist

$$\begin{aligned}\alpha(c) &= \sum_{v \in V} \chi(c_1 v_1) \ldots \chi(c_n v_n) X^{w(v_1)+\ldots+w(v_n)} = \prod_{i=1}^n \sum_{a \in \mathbb{F}_q} \chi(a c_i) X^{w(a)} \\ &= (1-X)^{w(c)}(1+(q-1)X)^{n-w(c)} = \big(1-(q-1)X\big)^n \Big(\frac{1-X}{1+(q-1)X}\Big)^{w(c)}.\end{aligned}$$

Insgesamt erhält man

$$q^k W_{C^\perp}(X) = \sum_{c \in C} \alpha(c) = \big(1-(q-1)X\big)^n W_C\Big(\frac{1-X}{1+(q-1)X}\Big). \qquad \square$$

Beispiel III.10.50. Der Code $C = H_7^\perp$ besteht nach Beispiel III.10.35 aus folgenden Codewörtern:

0000000	1000111	0101011	1101100
0011101	1011010	0110110	1110001

Daher ist $W_C(X) = 1 + 7X^4$. Die MacWilliams-Identität liefert

$$\begin{aligned}W_{H_7}(X) &= \frac{1}{8}(1+X)^7\Big(1 + 7\frac{(1-X)^4}{(1+X)^4}\Big) = \frac{1}{8}(1+X)^3\big((1+X)^4 + 7(1-X)^4\big) \\ &= (1+3X+3X^2+X^3)(1-3X+6X^2-3X^3+X^4) \\ &= 1 + 7X^3 + 7X^4 + X^7.\end{aligned}$$

Definition III.10.51. Ein Code $C \subseteq A^n$ heißt *zyklisch*, falls $(c_2, c_3, \ldots, c_n, c_1) \in C$ für alle $(c_1, \ldots, c_n) \in C$ gilt.

Satz III.10.52. *Sei $\mathcal{C}$ die Menge der linearen zyklischen Codes $C \leq \mathbb{F}_q^n$. Sei $\mathcal{D}$ die Menge der normierten Teiler von $X^n - 1 \in \mathbb{F}_q[X]$. Für $c = (c_0, \ldots, c_{n-1}) \in C \in \mathcal{C}$ sei $c(X) := \sum_{i=0}^{n-1} c_i X^i \in \mathbb{F}_q[X]$. Dann existiert ein $\alpha \in \mathcal{D}$ mit*

$$(\alpha)/(X^n - 1) = \{c(X) + (X^n - 1) : c \in C\}$$

und $\dim C = n - \deg \alpha$. Die Abbildung $\mathcal{C} \to \mathcal{D}$, $C \to \alpha$ ist eine Bijektion.

Beweis. Sei $I := (X^n - 1) \trianglelefteq \mathbb{F}_q[X]$. Für $c, d \in C \in \mathcal{C}$ gilt

$$\begin{aligned} c(X) + d(C) &= \sum_{i=0}^{n-1} (c_i + d_i) X^i = (c + d)(X), \\ X(c(X) + I) &= \sum_{i=0}^{n-1} c_i X^{i+1} + I = c_{n-1} + c_0 X + \ldots + c_{n-2} X^{n-2} + I \\ &= (c_{n-1}, c_0, \ldots, c_{n-2})(X). \end{aligned}$$

Dies zeigt $C(X) := \{c(X) + I : c \in C\} \trianglelefteq \mathbb{F}_q[X]/I$. Nach dem Korrespondenzsatz existiert genau ein Ideal $J \trianglelefteq \mathbb{F}_q[X]$ mit $C(X) = J/I$. Da $\mathbb{F}_q[X]$ ein Hauptidealring ist, existiert genau ein normiertes Polynom $\alpha \in \mathbb{F}_q[X]$ mit $J = (\alpha)$. Da die Abbildung $c \mapsto c(X)$ injektiv ist, gilt

$$\dim C = \dim(J/I) = \dim(\mathbb{F}_q[X]/I) - \dim(\mathbb{F}_q[X]/(\alpha)) = n - \deg \alpha.$$

Wegen $X^n - 1 \in J$ gilt $\alpha \mid X^n - 1$, d. h. $\alpha \in \mathcal{D}$. Die Abbildung $\mathcal{C} \to \mathcal{D}$ ist also injektiv. Ist umgekehrt $\alpha \in \mathcal{D}$ gegeben, so kann man $(\alpha)/I$ wie oben als zyklischen Code interpretieren. Daher ist $\mathcal{C} \to \mathcal{D}$ auch surjektiv. □

Definition III.10.53. In der Situation von Satz III.10.52 nennt man α das *Erzeuger-Polynom* und $\beta := \frac{X^n - 1}{\alpha}$ das *Kontroll-Polynom* von C. Es gilt $\dim C = \deg \beta$.

Bemerkung III.10.54. Sei $\alpha = a_d X^d + a_{d-1} X^{d-1} + \ldots + a_0$ das Erzeuger-Polynom von C, wobei $a_d = 1$. Dann ist $\alpha, X\alpha, \ldots, X^{n-d-1}\alpha$ eine Basis von $(\alpha)/(X^n - 1)$. Somit ist

$$\begin{pmatrix} a_0 & \cdots & a_d & & 0 \\ & \ddots & & \ddots & \\ 0 & & a_0 & \cdots & a_d \end{pmatrix} \in \mathbb{F}_q^{(n-d) \times n}$$

eine Erzeuger-Matrix von C. Sei nun $\beta = b_{n-d} X^{n-d} + \ldots + b_0$ das Kontroll-Polynom von C. Wegen $\alpha\beta = X^n - 1$ ist $\sum_i a_i b_{k-i} = 0$ für $k = 1, \ldots, n-1$. Daher ist

$$\begin{pmatrix} b_{n-d} & \cdots & b_0 & & 0 \\ & \ddots & & \ddots & \\ 0 & & b_{n-d} & \cdots & b_0 \end{pmatrix} \in \mathbb{F}_q^{d \times n}$$

eine Kontroll-Matrix von C. Daher ist $C^\perp$ zyklisch mit Erzeuger-Polynom $X^{n-d} + b_0^{-1} b_1 X^{n-d-1} + \ldots + b_0^{-1} = b_0^{-1} X^{n-d} \beta(X^{-1})$ (bis auf Normierung wird die Reihenfolge der Koeffizienten umgekehrt).

Beispiel III.10.55. Die Erzeuger-Polynome $\alpha = 1$ und $\alpha = X^n - 1$ führen zu den trivialen Codes $\mathbb{F}_q^n$ und 0. Für $\alpha = X - 1$ erhält man den Paritätscode P_n. Der komplementäre Faktor $\frac{X^n-1}{X-1} = 1 + X + \ldots + X^{n-1}$ gehört zum Wiederholungscode W_n. Für interessantere Beispiele ist die Primfaktorzerlegung von $X^n - 1$ nützlich.

Definition III.10.56. Für teilerfremde Zahlen $a, d \in \mathbb{N}$ sei $\mathrm{ord}_d(a)$ die Ordnung von $a + d\mathbb{Z}$ in $(\mathbb{Z}/d\mathbb{Z})^\times$.

Satz III.10.57. *Sei $q \neq 1$ eine Potenz der Primzahl p und $n = p^k m \in \mathbb{N}$ mit $p \nmid m$. Dann gilt*

$$X^n - 1 = \prod_{d \mid m} \Phi_d^{p^k} = \prod_{d \mid m} \prod_{i=1}^{\varphi(d)/\mathrm{ord}_d(q)} \Phi_{d,i}^{p^k},$$

wobei $\Phi_{d,i} \in \mathbb{F}_q[X]$ paarweise verschiedene irreduzible Polynome vom Grad $\mathrm{ord}_d(q)$ sind.

Beweis. Da $X^n - 1 = (X^m - 1)^{p^k}$ in $\mathbb{F}_q[X]$ gilt, können wir $n = m$ annehmen. Die Kreisteilungspolynome $\Phi_d \in \mathbb{Z}[X]$ liegen nach Reduktion modulo p in $\mathbb{F}_p[X] \subseteq \mathbb{F}_q[X]$. Damit ist die erste Gleichung bewiesen. Sei $N := \mathrm{ord}_n(q)$. Wegen $q^N = 1 \pmod{n}$ existiert eine primitive n-te Einheitswurzel $\zeta \in \mathbb{F}_{q^N}^\times$. Offenbar sind $\zeta, \zeta^2, \ldots, \zeta^n$ die Nullstellen von $X^n - 1$. Mit Induktion nach n folgt

$$\Phi_n = \prod_{\mathrm{ggT}(s,n)=1} (X - \zeta^s)$$

wie in $\mathbb{Q}[X]$. Die irreduziblen Teiler von Φ_n in $\mathbb{F}_q[X]$ entsprechen den Bahnen von $\mathrm{Gal}(\mathbb{F}_{q^N}|\mathbb{F}_q) = \langle F \rangle$ auf $\{\zeta^s : \mathrm{ggT}(s,n) = 1\}$, wobei $F(x) = x^q$ der Frobenius-Automorphismus ist. Wir suchen daher die Bahnen der Multiplikationsoperation von $\langle q + n\mathbb{Z} \rangle$ auf $(\mathbb{Z}/n\mathbb{Z})^\times$. Dies sind genau die Nebenklassen von $\langle q + n\mathbb{Z} \rangle$; sie haben also Länge N. Auf diese Weise entstehen die $\varphi(n)/N$ irreduziblen Polynome $\Phi_{n,i}$ vom Grad N. □

Satz III.10.58. *Sei q eine Primzahlpotenz, $n \in \mathbb{N}$ teilerfremd zu q und $d := \mathrm{ord}_n(q)$, sodass $n = q^d - 1$ gilt. Dann existiert ein zyklischer $(n, d, q^{d-1}(q-1))$-Code C mit $W_C(X) = 1 + nX^{d(C)}$.*

Beweis. Nach Satz III.10.57 existiert ein irreduzibler Teiler β von Φ_n vom Grad d. Sei C der zyklische Code mit Kontroll-Polynom β und Erzeuger-Polynom $\alpha := \frac{X^n-1}{\beta}$. Wegen $\mathrm{ggT}(n, q) = 1$ sind die Primfaktoren von $X^n - 1$ paarweise verschieden. Insbesondere sind α und β teilerfremd. Nehmen wir an es existieren $0 \leq i < j < n$ mit $X^i\alpha \equiv X^j\alpha \pmod{I}$, wobei $I := (X^n - 1)$. Dann ist β ein Teiler von $X^k - 1$ mit $k := j - i < n$. Folglich teilt β auch $\mathrm{ggT}(X^k - 1, X^n - 1) = X^{\mathrm{ggT}(k,n)} - 1$. Dann müsste β aber zweimal in der Primfaktorzerlegung von $X^n - 1$ auftreten. Dieser Widerspruch zeigt $X^i\alpha \not\equiv X^j\alpha \pmod{I}$. Wegen $|C| = q^d = n + 1$ folgt

$$C(X) = (\alpha)/I = \{0, X^i\alpha + I : i = 0, \ldots, n-1\}.$$

Insbesondere haben alle nicht-trivialen Codewörter das gleiche Gewicht. Sei $c \in C$ mit $c_i \neq 0$. Schreibe $C = \langle c \rangle \oplus D$ als direkte Summe von Vektorräumen. Für jedes $c' \in D$ existieren genau $q - 1$ Elemente $\lambda \in \mathbb{F}_q$, sodass $\lambda c + c'$ an der Koordinate i nicht verschwindet. Also gibt es genau $|D|(q-1) = q^{d-1}(q-1)$ Codewörter c mit $c_i \neq 0$. Dies zeigt

$$d(C) = \frac{1}{|C| - 1} \sum_{c \in C \setminus \{0\}} w(c) = \frac{1}{n} \sum_{i=1}^{n} q^{d-1}(q-1) = q^{d-1}(q-1).$$

Damit ergibt sich auch die erzeugende Funktion $W_C(X)$. □

Beispiel III.10.59. Für $n = 7$, $q = 2$ und $d = 3$ ist die Bedingung $n = q^d - 1$ aus Satz III.10.58 erfüllt. Es gibt also einen zyklischen $(7, 3, 4)$-Code C. Wegen $\Phi_7 = (X^3 + X + 1)(X^3 + X^2 + 1)$ in $\mathbb{F}_2[X]$ können wir $\beta = X^3 + X^2 + 1$ als Kontroll-Polynom wählen. Die entsprechende Kontrollmatrix ist

$$\begin{pmatrix} 1 & 1 & . & 1 & . & . & . \\ . & 1 & 1 & . & 1 & . & . \\ . & . & 1 & 1 & . & 1 & . \\ . & . & . & 1 & 1 & . & 1 \end{pmatrix}$$

nach Bemerkung III.10.54. Dies ist nach Aufgabe III.54 eine Erzeuger-Matrix von H_7 (vgl. Beispiel III.10.50). Daher ist C zu $H_7^\perp$ äquivalent.

Satz III.10.60. *Seien $k \leq n \leq q$ und $A \subseteq \mathbb{F}_q$ mit $|A| = n$. Dann ist*

$$C := \big\{(\gamma(a) : a \in A) : \gamma \in \mathbb{F}_q[X],\ \deg \gamma < k\big\} \subseteq \mathbb{F}_q^n$$

ein $(n, k, n - k + 1)$-Code; also ein MDS-Code. Im Fall $A = \langle a \rangle$ ist C zyklisch.

Beweis. Der P der k-dimensionale $\mathbb{F}_q$-Vektorraum aller $\gamma \in \mathbb{F}_q[X]$ mit $\deg \gamma < k$. Jedes solche $\gamma \neq 0$ besitzt höchstens $k - 1$ Nullstellen. Wegen $k \leq n$ ist die Abbildung $P \to C$, $\gamma \mapsto (\gamma(a) : a \in A)$ ein Monomorphismus von Vektorräumen. Insbesondere ist C ein (n, k)-Code mit $d(C) \geq n-(k-1) = n-k+1$. Aus der Singleton-Schranke folgt $d(C) = n - k + 1$, d. h. C ist ein MDS-Code. Sei nun $A = \langle a \rangle$ und $(\gamma(1), \ldots, \gamma(a^{n-1})) \in C$. Setze $\rho(X) := \gamma(aX) \in \mathbb{F}_q[X]$. Dann ist $\deg \rho = \deg \gamma < k$ und $(\gamma(a), \gamma(a^2), \ldots, \gamma(1)) = (\rho(1), \ldots, \rho(a^{n-1})) \in C$. Daher ist C zyklisch. □

Bemerkung III.10.61. Die in Satz III.10.60 für $A = \langle a \rangle$ konstruierten Codes sind nach Reed und Solomon benannt. Sie werden unter anderem für Compact Discs (CD) und QR-Codes (zweidimensionale Barcodes) benutzt. Im Gegensatz zu den bisher behandelten Codes benötigen sie große Alphabete (für CDs benutzt man $q = 2^8$).

Aufgaben

Varietäten

Aufgabe III.1 (2 Punkte)**.** Sei K ein beliebiger Körper (nicht unbedingt algebraisch abgeschlossen) und $I \lhd K[X_1, \ldots, X_n]$. Zeigen Sie, dass ein Punkt $(x_1, \ldots, x_n) \in \overline{K}^n$ mit $\alpha(x_1, \ldots, x_n) = 0$ für alle $\alpha \in I$ existiert.

Aufgabe III.2 (2 + 2 + 2 Punkte)**.** Seien $A \in \mathrm{A}(K^n)$ und $B \in \mathrm{A}(K^m)$. Zeigen Sie:

(a) $A \times B \in \mathrm{A}(K^{n+m})$.

(b) Sind A und B irreduzibel, so auch $A \times B$.

(c) $\dim(A \times B) = \dim(A) + \dim(B)$.

Aufgabe III.3 (2 Punkte)**.** Seien $R \subseteq S$ Integritätsbereiche, sodass S ein endlich erzeugter R-Modul ist. Zeigen Sie, dass R genau dann ein Körper ist, wenn S ein Körper ist.

Aufgabe III.4 (2 Punkte)**.** Geben Sie einen neuen Beweis für Zariskis Lemma mit Hilfe der Noether-Normalisierung und Aufgabe III.3.

Aufgabe III.5 (2 Punkte)**.** Zeigen Sie, dass jede offene Teilmenge des K^n bzgl. der Zariski-Topologie leer oder unendlich ist.

Aufgabe III.6 (2 Punkte)**.** Sei $\leq_l$ die lexikografische Monomordnung auf $R := K[X_1, \ldots, X_n]$. Zeigen Sie, dass auch

$$\alpha < \beta \ :\Longleftrightarrow\ \deg \alpha < \deg \beta \vee (\deg \alpha = \deg \beta \wedge \alpha <_l \beta).$$

eine Monomordnung auf R definiert.

Aufgabe III.7 (3 Punkte)**.** Seien $\beta_1, \ldots, \beta_k \in K[X_1, \ldots, X_n] \setminus \{0\}$ und $I = (\beta_1, \ldots, \beta_k)$. Für alle $\alpha \in K[X_1, \ldots, X_n]$ gelte $\alpha \in I$ genau dann, wenn jeder Rest bei der Division von α durch $\beta_1, \ldots, \beta_k$ verschwindet. Zeigen Sie, dass $\beta_1, \ldots, \beta_k$ eine Gröbnerbasis von I ist.
Bemerkung: Dies ist die Umkehrung von Satz III.2.58.

Aufgabe III.8 (2 Punkte)**.** Sei B eine Gröbnerbasis von $I \trianglelefteq K[X_1, \ldots, X_n]$ bzgl. der lexikografischen Monomordnung und $1 \leq i \leq n$. Dann ist $B \cap K[X_i, \ldots, X_n]$ eine Gröbnerbasis des Eliminationsideals $I \cap K[X_i, \ldots, X_n]$.

Aufgabe III.9 (2 Punkte)**.** Seien $I = (\beta_1, \ldots, \beta_k)$ und $J = (\gamma_1, \ldots, \gamma_l)$ Ideale in $R := K[X_1, \ldots, X_n]$. Sei Y eine neue Variable. Zeigen Sie

$$I \cap J = (\beta_1 Y, \ldots, \beta_k Y, \gamma_1(Y-1), \ldots, \gamma_l(Y-1)) \cap R.$$

Bemerkung: Der Durchschnitt $I \cap J$ ist damit auf ein Eliminationsideal zurückgeführt, welches mit Aufgabe III.8 berechnet werden kann.

Aufgabe III.10 (2 + 2 Punkte)**.** Konstruieren Sie eine Gröbnerbasis von

$$I = (2XY^2 + 3X + 4Y^2, Y^2 - 2Y - 2) \trianglelefteq \mathbb{C}[X, Y].$$

Entscheiden Sie, ob $2X^3Y^3 + 4Y^2 \in I$ gilt.

Aufgabe III.11 (2 Punkte)**.** Konstruieren Sie die reduzierte Gröbnerbasis von $(XY - Y^2, X^2 - 1) \trianglelefteq \mathbb{C}[X, Y]$.

Aufgabe III.12 (2 Punkte)**.** Sei B die reduzierte Gröbnerbasis von $I \trianglelefteq K[X_1, \ldots, X_n]$. Zeigen Sie, $1 \in I \iff B = \{1\}$.

Modulare Darstellungen

Aufgabe III.13 (2+2 Punkte)**.** Sei A eine K-Algebra und V ein A-Modul. Wir definieren $\mathrm{J}^0(V) := V$, $\mathrm{Soc}(V)^0 := 0$ und

$$\mathrm{J}^{n+1}(V) := \mathrm{J}(\mathrm{J}^n(V)), \qquad \mathrm{Soc}^n(V)/\mathrm{Soc}^{n-1}(V) := \mathrm{Soc}(V/\mathrm{Soc}^{n-1}(V))$$

für $n \geq 0$. Sei $0 = V_0 \leq \ldots \leq V_k = V$, sodass V_i/V_{i-1} für $i = 1, \ldots, k$ halbeinfach ist. Zeigen Sie:

(a) $V_i \leq \mathrm{Soc}^i(V)$ und $\mathrm{J}^i(V) \leq V_{k-i}$ für $i = 0, \ldots, k$.

(b) $\mathrm{J}^i(V) = 0 \iff \mathrm{Soc}^i(V) = V$.

Bemerkung: Das kleinste $l \in \mathbb{N}_0$ mit $\mathrm{J}^l(V) = 0$ nennt man die *Loewylänge* von V. Sie misst wie weit ein Modul von einem halbeinfachen Modul entfernt ist.

Aufgabe III.14 (2 Punkte)**.** Sei K ein Körper und V ein endlich-dimensionaler K-Vektorraum. Zeigen Sie, dass $V^{\otimes n} := V \otimes \ldots \otimes V$ (n Faktoren) durch

$$\sigma(v_1 \otimes \ldots \otimes v_n) := v_{\sigma^{-1}(1)} \otimes \ldots \otimes v_{\sigma^{-1}(n)}$$

zu einem KS_n-Modul wird.

Aufgabe III.15 (3 Punkte)**.** Sei K ein beliebiger Körper und $G \cong C_n$. Zeigen Sie, dass KG höchstens n unzerlegbare Moduln bis auf Isomorphie besitzt.
Hinweis: Man kann die Weierstraß-Normalform benutzen.

Aufgabe III.16 (3 Punkte)**.** Sei K ein unendlicher Körper der Charakteristik $p > 0$ und $G \cong C_p^2$. Zeigen Sie, dass KG unendlich viele nicht-isomorphe unzerlegbare Moduln der Dimension 2 besitzt.

Aufgabe III.17 (2+2 Punkte)**.** Sei $H \leq G$ und U, V KH-Moduln. Konstruieren Sie einen Vektorraum-Monomorphismus $\mathrm{Hom}_{KH}(U,V) \to \mathrm{Hom}_{KG}(U^G, V^G)$. Zeigen Sie, dass die Vektorräume im Allgemeinen nicht isomorph sind.

Aufgabe III.18 (3 Punkte)**.** Sei K ein algebraisch abgeschlossener Körper der Charakteristik $p > 0$. Sei $N \trianglelefteq G$ mit $p \nmid |G : N|$. Sei V ein einfacher KG-Modul und $U \leq V_N$ ein einfacher KN-Modul. Zeigen Sie, dass U^G halbeinfach ist und die Vielfachheit von V als Kompositionsfaktor von U^G mit dem Verzweigungsindex übereinstimmt.
Hinweis: Man kann Aufgabe II.62 benutzen.

Aufgabe III.19 (3 + 3 Punkte)**.** Sei P ein projektiv-unzerlegbarer KG-Modul und $S := \mathrm{Soc}(P)$. Sei $N \trianglelefteq G$ und T ein einfacher Untermodul von S_N. Sei Q ein projektiv-unzerlegbarer KN-Modul mit $\mathrm{Soc}(Q) \simeq T$. Zeigen Sie:

(a) Es existiert ein $e \leq |G_T : N|$ mit

$$P_N \simeq \bigtimes_{gG_T \in G/G_T} (g \otimes Q)^e.$$

(b) Sei $W \in \Gamma(G_U, U)$ und R ein projektiv-unzerlegbarer KG_U-Modul mit $\mathrm{Soc}(R) \simeq W$. Dann ist R^G projektiv-unzerlegbar mit $\mathrm{Soc}(R^G) \simeq W^G$.

Aufgabe III.20 (4 Punkte)**.** Sei K ein Körper und A die Algebra aller Matrizen der Form

$$\begin{pmatrix} a & b & . & . \\ . & c & . & . \\ . & . & c & d \\ . & . & . & a \end{pmatrix} \in K^{4\times 4}.$$

Zeigen Sie, dass $\left(\begin{smallmatrix} 1 & 1 \\ 1 & 1 \end{smallmatrix}\right)$ die Cartan-Matrix von A ist.

Kategorien

Aufgabe III.21 (2+2 Punkte)**.** Sei G eine Gruppe und $\mathcal{C}$ die Kategorie zu G wie in Beispiel III.5.4(iv).

(a) Zeigen Sie, dass die Kongruenzen von $\mathcal{C}$ den Normalteilern von G entsprechen.

(b) Leiten Sie den Homomorphiesatz für Gruppen aus Satz III.5.12 ab.

Aufgabe III.22 (2 Punkte)**.** Zeigen Sie, dass ein Funktor der Form $\mathbf{Rng} \to \mathbf{Cat}$, $R \mapsto {}_R\mathbf{mod}$ existiert.

Aufgabe III.23 (2 Punkte)**.** Seien $\mathcal{C}$, $\mathcal{D}$ Kategorien und $\Phi\colon \mathcal{C} \to \mathcal{D}$ ein Funktor. Zeigen Sie, dass Φ genau dann ein Isomorphismus ist, wenn Φ voll und treu ist und $\Phi\colon \mathrm{Ob}(\mathcal{C}) \to \mathrm{Ob}(\mathcal{D})$ surjektiv ist.

Aufgabe III.24 (3 Punkte)**.** Entscheiden Sie, welche der folgenden Funktoren voll oder treu ist:

(a) $\mathrm{Hom}(A, .) : \mathbf{Grp} \to \mathbf{Set}$.

(b) $\mathrm{GL}(n,.) : \mathbf{Rng} \to \mathbf{Grp}$.

(c) $\Phi_K : \mathbf{grp} \to \mathbf{Rng}$, $G \mapsto KG$ für einen Körper K.

Aufgabe III.25 (3 Punkte)**.** Sei K ein Körper. Konstruieren Sie eine Äquivalenz ${}_K\mathbf{mod} \approx {}_K\mathbf{mod}^o$.

Aufgabe III.26 $(2+2+2$ Punkte$)$**.**

(a) Konstruieren Sie einen Funktor $\Phi\colon \mathbf{Grp} \to \mathbf{Ab}$, $G \mapsto G/G'$ (vgl. Aufgabe I.31).

(b) Zeigen Sie, dass Φ links-adjungiert zum Vergiss-Funktor $\mathbf{Ab} \to \mathbf{Grp}$ ist.

(c) Zeigen Sie, dass *kein* Funktor der Form $\mathbf{Grp} \to \mathbf{Ab}$, $G \mapsto \mathrm{Z}(G)$ existiert.

Morita-Theorie

Aufgabe III.27 (2 Punkte)**.** Seien M und N Linksmoduln über einem kommutativen Ring R. Zeigen Sie, dass $M \otimes_{\mathbb{Z}} N$ mit dem in Aufgabe II.52 definierten Tensorprodukt übereinstimmt.

Aufgabe III.28 $(2+2$ Punkte$)$**.** Seien $(M_i)_{i\in I}$ und $(N_j)_{j\in J}$ Familien von R-S-Bimoduln bzw. R-T-Bimoduln. Zeigen Sie:

(a) Es existiert ein S-T-Isomorphismus

$$\mathrm{Hom}_R\Big(\coprod_{i\in I} M_i, \bigtimes_{j\in J} N_j\Big) \simeq \bigtimes_{i\in I}\bigtimes_{j\in J} \mathrm{Hom}(M_i, N_j).$$

(b) Ist M ein endlich erzeugter R-S-Bimodul, so existiert ein S-T-Isomorphismus

$$\mathrm{Hom}_R\Big(M, \coprod_{j\in J} N_j\Big) \simeq \coprod_{j\in J} \mathrm{Hom}_R(M, N_j).$$

Aufgabe III.29 $(1+3+3$ Punkte$)$**.** Seien R und S Ringe. Eine Folge

$$\ldots \to A_{-1} \xrightarrow{f_{-1}} A_0 \xrightarrow{f_0} A_1 \to \ldots$$

von R-S-Homomorphismen heißt *exakt* an Position i, falls $f_{i-1}(A_{i-1}) = \mathrm{Ker}(f_i)$ gilt. Sei

$$\sigma\colon 0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$$

eine beliebige Folge von R-S-Homomorphismen. Zeigen Sie:

(a) Genau dann ist σ exakt an Position A (bzw. C), wenn f injektiv (bzw. g surjektiv) ist.

(b) Sei M ein R-S-Modul. Ist σ exakt an Position A und B, so ist

$$0 \to \mathrm{Hom}_R(M, A) \xrightarrow{f\circ .} \mathrm{Hom}_R(M, B) \xrightarrow{g\circ .} \mathrm{Hom}_R(M, C)$$

exakt an $\mathrm{Hom}_R(M, A)$ und $\mathrm{Hom}_R(M, B)$.

(c) Sei M ein S-R-Modul. Ist σ exakt an Position B und C, so ist

$$A \otimes_S N \xrightarrow{f \otimes \mathrm{id}_N} B \otimes_S N \xrightarrow{g \otimes \mathrm{id}_N} C \otimes_S N \to 0$$

exakt an $B \otimes_S N$ und $C \otimes_S N$.

Aufgabe III.30 ($3 + 3$ Punkte)**.** Seien R und S Ringe.

(a) (*Fünferlemma*) Das folgende Diagramm von R-S-Homomorphismen sei kommutativ und die Zeilen seien exakt (soweit sinnvoll).

$$\begin{array}{ccccccccc}
A & \xrightarrow{f} & B & \xrightarrow{g} & C & \xrightarrow{h} & D & \xrightarrow{j} & E \\
\downarrow{\scriptstyle r} & & \downarrow{\scriptstyle s} & & \downarrow{\scriptstyle t} & & \downarrow{\scriptstyle u} & & \downarrow{\scriptstyle v} \\
A' & \xrightarrow{f'} & B' & \xrightarrow{g'} & C' & \xrightarrow{h'} & D' & \xrightarrow{j'} & E'
\end{array}$$

Außerdem seien r surjektiv, v injektiv und s und u bijektiv. Zeigen Sie, dass t bijektiv ist.

(b) (*Neunerlemma*) Das folgende Diagramm von R-S-Homomorphismen sei kommutativ, die Spalten seien exakt und die letzten beiden Zeilen seien exakt (soweit sinnvoll).

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & A_1 & \xrightarrow{f_1} & A_2 & \xrightarrow{f_2} & A_3 & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle g_1} & & \downarrow{\scriptstyle g_2} & & \downarrow{\scriptstyle g_3} & & \\
0 & \longrightarrow & B_1 & \xrightarrow{f_3} & B_2 & \xrightarrow{f_4} & B_3 & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle g_4} & & \downarrow{\scriptstyle g_5} & & \downarrow{\scriptstyle g_6} & & \\
0 & \longrightarrow & C_1 & \xrightarrow{f_5} & C_2 & \xrightarrow{f_6} & C_3 & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

Zeigen Sie, dass auch die erste Zeile exakt ist.

Aufgabe III.31 (2 Punkte)**.** Sei $(R, S, M, N, \mathfrak{R}, \mathfrak{S})$ ein Morita-Kontext mit surjektivem $\mathfrak{R}$. Konstruieren Sie einen S-R-Isomorphismus $N \to \mathrm{Hom}_S(M, S)$.
Bemerkung: Man ist also in der Situation von Beispiel III.6.33.

Zentral-einfache Algebren

Aufgabe III.32 (2 Punkte)**.** Seien A, B und C K-Algebren und $q_A \colon A \to C$, $q_B \colon B \to C$ Homomorphismen mit $q_A(a)q_B(b) = q_B(b)q_A(a)$ für alle $a \in A$, $b \in B$ und folgender universeller Eigenschaft:
Für Algebren-Homomorphismen $f_A \colon A \to D$, $f_B \colon B \to D$ mit $f_A(a)f_B(b) = f_B(b)f_A(a)$ für alle $a \in A$, $b \in B$ existiert genau ein Homomorphismus $f \colon C \to D$ mit $f \circ q_A = f_A$ und $f \circ q_B = f_B$. Zeigen Sie $C \cong A \otimes B$.
Bemerkung: Das Tensorprodukt ist also eine kommutative Variante des Koprodukts in der Kategorie K-**alg** der endlich-dimensionalen K-Algebren.

Aufgabe III.33 (2 Punkte)**.** Seien $K \subseteq M_i \subseteq L$ endliche Körpererweiterungen mit $M_1 \cap M_2 = K$. Sei $K \subseteq M_1$ eine Galois-Erweiterung. Zeigen Sie, dass die K-Algebra $M_1 \otimes_K M_2$ zum Komposition $M_1 M_2$ isomorph ist.

Aufgabe III.34 ($2 + 2$ Punkte)**.** Sei G eine endliche Gruppe, K ein Körper und $\gamma \in Z^2(G, K^\times)$. Auf dem K-Vektorraum $K_\gamma G := KG$ definieren wir eine Multiplikation

$$x \cdot y := \gamma(x, y)xy \qquad (x, y \in G).$$

Zeigen Sie:

(a) $K_\gamma G$ ist eine K-Algebra.

(b) Der Isomorphietyp von $K_\gamma G$ hängt nur von $\overline{\gamma} \in H^2(G, K^\times)$ ab.

Aufgabe III.35 ($1 + 2 + 2 + 2 + 2 + 2$ Punkte)**.** Sei $K \subseteq L$ eine Galois-Erweiterung mit zyklischer Galoisgruppe $G = \mathrm{Gal}(L|K) = \langle x \rangle \cong C_n$. Zeigen Sie:

(a) Die *Norm-Abbildung* $N\colon L^\times \to K^\times$, $a \mapsto \prod_{\sigma \in G} \sigma(a)$ ist ein Homomorphismus.

(b) Für $\lambda \in K^\times$ existiert $\gamma_\lambda \in Z^2(G, L^\times)$ mit

$$\gamma_\lambda(x^i, x^j) = \begin{cases} 1 & \text{falls } i + j < n, \\ \lambda & \text{falls } i + j \geq n, \end{cases}$$

wobei $0 \leq i, j < n$.

(c) $\gamma_\lambda \in B^2(G, L^\times) \iff \lambda \in N(L^\times)$.

(d) $H^2(G, L^\times) \cong K^\times / N(L^\times)$.

(e) Ist K endlich, so gilt $H^2(G, L^\times) = 1$.

(f) Satz II.8.7 folgt aus (e).

Bemerkung: Die entsprechenden Algebren $L_\gamma G$ nennt man *zyklisch*.

Aufgabe III.36 (2 Punkte)**.** Sei $n \in \mathbb{N}$ ungerade und $N\colon \mathbb{Q}_n^\times \to \mathbb{Q}^\times$ die Norm-Abbildung wie in Aufgabe III.35. Zeigen Sie $N(x) > 0$ für alle $x \in \mathbb{Q}_n^\times$.
Hinweis: $\zeta^{-1} = \overline{\zeta}$.

Aufgabe III.37 ($1 + 3 + 3 + 2$ Punkte)**.** Sei $\zeta := e^{2\pi \mathrm{i}/7} \in \mathbb{C}$, $\omega_1 := \zeta + \zeta^{-1}$, $\omega_2 := \zeta^2 + \zeta^{-2}$ und $\omega_3 := \zeta^3 + \zeta^{-3}$. Zeigen Sie:

(a) $\omega_1, \omega_2, \omega_3$ ist eine Normalbasis von $K := \mathbb{Q}(\omega) = \mathbb{Q}_7 \cap \mathbb{R}$ über $\mathbb{Q}$.

(b) $N(a\omega_1 + b\omega_2 + c\omega_3) = (a^3 + b^3 + c^3) + 3(a^2 b + ac^2 + b^2 c) - 4(a^2 c + ab^2 + bc^2) - abc$ für $a, b, c \in \mathbb{Q}$ mit der Norm-Abbildung aus Aufgabe III.35.

(c) $2 \notin N(K^\times)$.
Hinweis: Schreibe $x = \frac{1}{d}(a\omega_1 + b\omega_2 + c\omega_3)$ mit $d \in \mathbb{N}$ minimal. Betrachte $N(x)$ modulo 2.

(d) Es existiert eine 9-dimensionale $\mathbb{Q}$-Divisionsalgebra D mit $D \not\equiv D^o$.
Hinweis: Aufgabe III.35.
Bemerkung: Vergleich Aufgabe II.38.

Bewertungsringe

Aufgabe III.38 (2 Punkte)**.** Zeigen Sie, dass jeder lokale Hauptidealring R ein Bewertungsring einer ultrametrischen Bewertung auf $Q(R)$ ist.

Aufgabe III.39 (2 Punkte)**.** Sei K ein Körper mit ultrametrischer Bewertung ν. Sei $\alpha = \sum_{k=0}^{n} a_k X^k \in K[X]$ normiert mit Nullstelle $x \in K$. Zeigen Sie $\nu(x) \leq \max_{0 \leq k \leq n} \nu(a_k)$.
Bemerkung: Vergleich mit Satz A.2.2.

Aufgabe III.40 ($2 + 2 + 2$ Punkte)**.** Sei K ein Körper mit vollständiger ultrametrischer Bewertung. Zeigen Sie, dass eine Reihe $\sum_{n=1}^{\infty} x_n$ genau dann in K konvergiert, wenn $(x_n)_n$ eine Nullfolge ist. Ggf. gilt

$$\nu\Big(\sum_{n=1}^{\infty} x_n\Big) \leq \max_{n \in \mathbb{N}} \nu(x_n), \qquad \sum_{n=1}^{\infty} x_n = \sum_{n=1}^{\infty} x_{\pi(n)}$$

für alle $\pi \in \mathrm{Sym}(\mathbb{N})$.

Aufgabe III.41 (3 Punkte)**.** Sei $\epsilon = \frac{1}{7}$. Konstruieren Sie $x \in \mathbb{Q}$ mit $|x - 1| < \epsilon$, $\nu_5(x - 3) < \epsilon$ und $\mu_7(x - 4) < \epsilon$.

Aufgabe III.42 (3 Punkte)**.** (Eisenstein) Sei K ein Körper mit diskreter Bewertung und Bewertungsring R. Sei $\alpha = X^n + a_{n-1}X^{n-1} + \ldots + a_0 \in K[X]$ mit $a_0, \ldots, a_{n-1} \in \mathrm{J}(R)$ und $a_0 \notin \mathrm{J}(R)^2$. Zeigen Sie, dass α irreduzibel ist.

Aufgabe III.43 (3 Punkte)**.** Sei K ein Körper und ν die Bewertung von $K(X)$ aus Beispiel III.8.3. Zeigen Sie, dass die Vervollständigung von $K(X)$ zum Körper der formalen Laurentreihen $K((X))$ isomorph ist.

Aufgabe III.44 (3 Punkte)**.** Untersuchen Sie für welche $x \in \mathbb{Q}_{[p]}$ die Reihe $\sum_{n=0}^{\infty} \frac{x^n}{n!}$ konvergiert.

Aufgabe III.45 ($2 + 2 + 3$ Punkte)**.**

(a) Stellen Sie die p-adische Entwicklung von $-1 \in \mathbb{Z}_{[p]}$ auf.

(b) Konstruieren Sie eine primitive vierte Einheitswurzel in $\mathbb{Z}_{[5]}$ bis auf vier „Vorkommastellen“.
Hinweis: $\zeta^2 = -1$.

(c) Verifizieren Sie $\sum_{n=1}^{\infty} \frac{2^n}{n} = 0$ in $\mathbb{Q}_{[2]}$.

Aufgabe III.46 (2 Punkte)**.** Sei $p \in \mathbb{P}$ und $p \nmid n \in \mathbb{N}$. Zeigen Sie, dass $a, k \in \mathbb{N}$ mit $an = p^k - 1$ und

$$\frac{1}{n} = -a \sum_{i=0}^{\infty} p^{ki} \in \mathbb{Z}_{[p]}$$

existieren.

Aufgabe III.47 (3 Punkte)**.** Zeigen Sie, dass jeder Automorphismus auf $\mathbb{Q}_{[p]}$ stetig ist und folgern Sie $\mathrm{Aut}(\mathbb{Q}_{[p]}) = 1$.
Hinweis: Vergleich Aufgabe I.53.

Aufgabe III.48 $(3 + 3$ Punkte$)$**.**

(a) Zeigen Sie, dass die p-adische Entwicklung von $\alpha \in \mathbb{Z}_{[p]}$ genau dann endlich ist, wenn $\alpha \in \mathbb{N}_0$ gilt.

(b) Zeigen Sie, dass die p-adische Entwicklung von $\alpha \in \mathbb{Q}_{[p]}$ genau dann endlich oder periodisch ist, wenn $\alpha \in \mathbb{Q}$ gilt.

Aufgabe III.49 $(2 + 1 + 3$ Punkte$)$**.** Sei $p \in \mathbb{P}$, $K = \mathbb{Q}_{[p]}$ und $\overline{K}$ der algebraische Abschluss von K mit Bewertung $\tilde{\nu}_p$. Nehmen wir an, dass $\overline{K}$ vollständig ist. Zeigen Sie:

(a) $|\overline{K} : K| = \infty$.
Hinweis: Bemerkung III.8.42.

(b) Seien $x_1, \ldots \in \overline{K}$ linear unabhängig über K und $q_1, \ldots \in \mathbb{Q}$ mit folgenden Eigenschaften:

- $\tilde{\nu}_p(q_1 x_n) > \tilde{\nu}_p(q_2 x_2) > \ldots$ und $\lim_{n\to\infty} \tilde{\nu}_p(q_n x_n) = 0$.
- $\tilde{\nu}_p(q_{n+1} x_{n+1}) < \tilde{\nu}_p(s_n - y)$, wobei $s_n := \sum_{k=1}^{n} q_k x_k$ und y die übrigen Nullstellen des Minimalpolynoms μ_{s_n} durchläuft.

Dann ist s_n eine Cauchyfolge und $s := \lim_{n\to\infty} s_n = \sum_{n=1}^{\infty} q_n x_n \in \overline{K}$ existiert.

(c) Für $n \in \mathbb{N}$ gilt $s_n \in K(s)$. Dies liefert den Widerspruch $|K(s) : K| = \infty$. Also ist $\overline{K}$ nicht vollständig.
Hinweis: Folgerung III.8.44.

Galois-Theorie

Aufgabe III.50 (2 Punkte)**.** Sei V ein Modul über einem Schiefkörper R mit Basis B. Für $U \leq V$ definieren minimale Elemente $u \in U$ bzgl. B wie in Bemerkung III.9.8. Zeigen Sie, dass U durch minimale Elemente erzeugt wird.

Codierungstheorie

Aufgabe III.51 $(1 + 2 + 2$ Punkte$)$**.** Wir betrachten die (lineare) Codierungsfunktion $\gamma\colon \mathbb{F}_2^2 \to \mathbb{F}_2^5$ mit folgenden Werten

$$(0,0) \mapsto (0,0,0,0,0), \qquad (0,1) \mapsto (0,1,1,0,1),$$
$$(1,0) \mapsto (1,0,1,1,0), \qquad (1,1) \mapsto (1,1,0,1,1).$$

(a) Zeigen Sie, dass dieser Code einen Fehler korrigieren kann.

(b) Decodieren Sie damit folgende Nachricht:

11110 10100 01101 00110 10010 11101 00001 11011 10110 11001 01000 01001

und decodieren Sie das Ergebnis weiter mit dem ASCII-Code.

(c) Angenommen die Wahrscheinlichkeit eines falsch übertragenen Bits beträgt $p = 0{,}01$. Wie hoch ist die Wahrscheinlichkeit, dass Sie die Nachricht in (b) korrekt decodiert haben?

Aufgabe III.52 (3 + 3 Punkte)**.** Sei $H = H_{2^n}$ die in Beispiel III.10.9 konstruierte $2^n \times 2^n$-Hadamard-Matrix und C der Code aus Satz III.10.12. Zeigen Sie:

(a) Ersetzt man alle -1 durch 0, so wird C zu einem binären linearen Code.
Hinweis: Induktion nach n.

(b) Im Fall $n = 3$ ist C aus (a) zum erweiterten Hamming-Code $\widehat{H_7}$ äquivalent.

Aufgabe III.53 (3 Punkte)**.** Sei C ein nicht-trivialer perfekter Code der Länge $n \leq 1000$ mit Minimaldistanz d über einem Alphabet mit $q \leq 1000$ Elementen. Zeigen Sie (mit Computer), dass eine der folgenden Aussagen gilt:

(i) $n = d$ ist ungerade und $|C| = q = 2$ (Parameter von W_n).

(ii) $n = \frac{q^m-1}{q-1}$, $|C| = q^{n-m}$ und $d = 3$ mit $m \geq 2$ (Parameter von H_n).

(iii) $n = 11$, $|C| = q^6 = 3^6$ und $d = 5$ (Parameter von G_{11}).

(iv) $n = 23$, $|C| = q^{12} = 2^{12}$ und $d = 7$ (Parameter von G_{23}).

Hinweis: Beispiel III.10.24 und Beweis von Satz III.10.38.

Aufgabe III.54 (3 Punkte)**.** Zeigen Sie, dass der Code mit Erzeuger-Matrix

$$\begin{pmatrix} 1 & 1 & . & 1 & . & . & . \\ . & 1 & 1 & . & 1 & . & . \\ . & . & 1 & 1 & . & 1 & . \\ . & . & . & 1 & 1 & . & 1 \end{pmatrix}$$

zu H_7 äquivalent ist.
Hinweis: Berechnen Sie eine Kontroll-Matrix.

Aufgabe III.55 (1 + 2 + 3 Punkte)**.** Sei $C = G_{24}$ der erweiterte binäre Golay-Code. Zeigen Sie:

(a) $(1, \ldots, 1) \in C$.

(b) Es existieren $a, b \in \mathbb{N}_0$ mit $W_C(X) = 1 + aX^8 + bX^{12} + aX^{16} + X^{24}$ und $2a + b = 4094$.
Hinweis: Beweis von Satz III.10.43 und (a).

(c) $W_C(X) = 1 + 759X^8 + 2576X^{12} + 758X^{16} + X^{24}$.
Hinweis: MacWilliams-Identität.

Aufgabe III.56 (2 Punkte)**.** Bestimmen Sie die Primfaktorzerlegung von $X^{60} - 1$ in $\mathbb{F}_3[X]$.

Anhang

1 Quadratische Reste

Definition A.1.1.

(i) Sei p eine Primzahl und $n \in \mathbb{Z} \setminus p\mathbb{Z}$. Man nennt n einen *quadratischen Rest* modulo p, falls ein $k \in \mathbb{Z}$ mit $n \equiv k^2 \pmod{p}$ existiert. Anderenfalls nennt man n einen *quadratischen Nichtrest* modulo p. Für $n \in \mathbb{Z}$ definiert man das *Legendre-Symbol*

$$\left(\frac{n}{p}\right) := \begin{cases} 1 & \text{falls } n \text{ ein quadratischer Rest modulo } p \text{ ist,} \\ -1 & \text{falls } n \text{ ein quadratischer Nichtrest modulo } p \text{ ist,} \\ 0 & \text{falls } p \mid n \end{cases}$$

von n *nach* p.

(ii) Sei $n \in \mathbb{Z}$ und $a \in \mathbb{N}$ ungerade mit Primfaktorzerlegung $a = p_1 \dots p_k$ (der Fall $a = 1$ mit $k = 0$ ist zugelassen). Man nennt

$$\left(\frac{n}{a}\right) := \left(\frac{n}{p_1}\right) \dots \left(\frac{n}{p_k}\right)$$

das *Jacobi-Symbol* von n *nach* a.

Bemerkung A.1.2. Für ungerade $a, b \in \mathbb{N}$ beweist man in der Zahlentheorie[1] das sogenannte *quadratische Reziprozitätsgesetz*

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = (-1)^{\frac{a-1}{2}\frac{b-1}{2}}$$

mit den beiden *Ergänzungssätzen*

$$\left(\frac{-1}{a}\right) = (-1)^{\frac{a-1}{2}}, \qquad \left(\frac{2}{a}\right) = (-1)^{\frac{a^2-1}{8}}.$$

Wir geben im Folgenden einige Anwendungen.

Satz A.1.3 (Zolotarev)**.** *Sei $n \in \mathbb{N}$ ungerade und $k \in \mathbb{Z}$ teilerfremd zu n. Sei $\sigma \in \mathrm{Sym}(\mathbb{Z}/n\mathbb{Z})$ mit $\sigma(a + n\mathbb{Z}) = ka + n\mathbb{Z}$ für alle $a \in \mathbb{Z}$. Dann gilt* $\mathrm{sgn}(\sigma) = \left(\frac{k}{n}\right)$.

Beweis. Sei $n = p_1^{m_1} \dots p_s^{m_s}$ die Primfaktorzerlegung von n. Nach dem chinesischen Restsatz ist

$$\begin{aligned} \mathbb{Z}/n\mathbb{Z} &\to \mathbb{Z}/p_1^{m_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p_s^{m_s}\mathbb{Z} =: R, \\ a + n\mathbb{Z} &\mapsto (a + p_1^{m_1}\mathbb{Z}, \dots, a + p_s^{m_s}\mathbb{Z}) \end{aligned}$$

ein Ringisomorphismus. Sei $\sigma_i \in \mathrm{Sym}(\mathbb{Z}/p_i^{m_i}\mathbb{Z})$ mit $\sigma_i(a + p_i^{m_i}\mathbb{Z}) = ka + p_i^{m_i}\mathbb{Z}$ für $a \in \mathbb{Z}$. Sei $\hat{\sigma}_i \in \mathrm{Sym}(R)$ mit $\hat{\sigma}_i(a_1, \dots, a_s) = (a_1, \dots, \sigma_i(a_i), \dots, a_s)$ für alle $(a_1, \dots, a_s) \in R$. Wenn man $\mathbb{Z}/n\mathbb{Z}$ mit R identifiziert, ist $\sigma = \hat{\sigma}_1 \dots \hat{\sigma}_s$ und $\mathrm{sgn}(\hat{\sigma}_i) = \mathrm{sgn}(\sigma_i)^{n/p_i^{m_i}} = \mathrm{sgn}(\sigma_i)$, da n ungerade ist. Nach der Definition des Jacobi-Symbols können wir $n = p_1^{m_1} = p^m$ annehmen.

[1] Siehe Zahlentheorie-Skript

Nach Satz I.8.34 ist $(\mathbb{Z}/n\mathbb{Z})^\times \cong C_{p^{m-1}(p-1)}$. Da p ungerade ist, können wir k durch k^{p^m} ersetzen, ohne dass sich $\operatorname{sgn}(\sigma)$ oder $\left(\frac{k}{n}\right)$ ändert. Anschließend ist $q := |\langle\sigma\rangle|$ ein Teiler von $p-1$. Genau dann ist k ein Quadrat in $\mathbb{Z}/p\mathbb{Z}$, wenn q auch $\frac{p-1}{2}$ teilt. Also gilt

$$\left(\frac{k}{n}\right) = \left(\frac{k}{p}\right)^m = (-1)^{\frac{m(p-1)}{q}}.$$

Für $a \in \mathbb{Z} \setminus n\mathbb{Z}$ ist $ka \not\equiv a \pmod{n}$. Daher ist σ ein disjunktes Produkt von $\frac{n-1}{q}$ Zyklen der Länge q. Dies zeigt $\operatorname{sgn}(\sigma) = (-1)^{\frac{n-1}{q}}$. Die Behauptung folgt nun aus

$$\frac{n-1}{q} = (p^{m-1} + \ldots + p + 1)\frac{p-1}{q} \equiv m\frac{p-1}{q} \pmod{2}. \qquad \square$$

Bemerkung A.1.4. Beim Nachweis, dass quadratische Zahlkörper in Kreisteilungskörpern liegen (Satz I.12.23), trat eine merkwürdige Summe von Einheitswurzeln auf, deren Vorzeichen irrelevant war. Tatsächlich hat Gauß mehre Jahre gebraucht, um dieses Vorzeichen zu bestimmen. Wir geben einen modernen Beweis.

Definition A.1.5. Für eine ungerade Primzahl p sei $\zeta := e^{2\pi \mathrm{i}/p} \in \mathbb{C}$ und

$$G_p := \sum_{k=1}^{p} \zeta^{k^2} \in \mathbb{C}.$$

Man nennt G_p die (*quadratische*) *Gauß-Summe* bzgl. p.

Bemerkung A.1.6.

(i) Für jeden quadratischen Rest q modulo p hat die Gleichung $k^2 = q$ genau zwei Lösungen in $\mathbb{F}_p^\times$. Mit dem Jacobi-Symbol gilt daher

$$G_p = 1 + 2\sum_{\substack{1 \le q \le p-1 \\ \mathrm{QR}}} \zeta^q = \sum_{k=1}^{p}\left(\left(\frac{k}{p}\right)+1\right)\zeta^k = \sum_{k=1}^{p}\left(\frac{k}{p}\right)\zeta^k + \sum_{k=1}^{p}\zeta^k = \sum_{k=1}^{p}\left(\frac{k}{p}\right)\zeta^k.$$

(ii) Ersetzt man ζ durch eine andere primitive p-te Einheitswurzel, sagen wir ζ^a, so erhält man

$$\sum_{k=1}^{p}\left(\frac{k}{p}\right)\zeta^{ak} = \left(\frac{a}{p}\right)\sum_{k=1}^{p}\left(\frac{ak}{p}\right)\zeta^{ak} = \left(\frac{a}{p}\right)G_p$$

aus der Multiplikativität des Jacobi-Symbols. Die Gauß-Summe hängt also von der Wahl von ζ ab.

Satz A.1.7 (Gauss)**.** *Für jede ungerade Primzahl p gilt*

$$G_p = \begin{cases} \sqrt{p} & \text{falls } p \equiv 1 \pmod 4, \\ \sqrt{-p} & \text{falls } p \equiv -1 \pmod 4, \end{cases}$$

wobei $\sqrt{-p}$ die Wurzel mit positivem Imaginärteil bezeichnet.

Beweis. Nach Bemerkung A.1.6 gilt

$$G_p^2 = \left(\sum_{k=1}^{p} \left(\frac{k}{p}\right)\zeta^k\right)^2 = \sum_{k,l=1}^{p} \left(\frac{kl}{p}\right)\zeta^{k+l} = \sum_{k=1}^{p} \zeta^k \sum_{l=1}^{p-1} \left(\frac{l(k-l)}{p}\right) = \sum_{k=1}^{p} \zeta^k \sum_{l=1}^{p-1} \left(\frac{kl^{-1}-1}{p}\right),$$

wobei l^{-1} das Inverse von l modulo p bezeichnet. Für $k < p$ durchläuft $kl^{-1} - 1 \pmod p$ alle Restklassen außer $-1 + p\mathbb{Z}$. Mit $q := \frac{p-1}{2}$ und dem ersten Ergänzungssatz folgt

$$G_p^2 = -\left(\frac{-1}{p}\right)\sum_{k=1}^{p-1} \zeta^k + (p-1)\left(\frac{-1}{p}\right) = (-1)^q p =: p^*.$$

Für $H_p := \prod_{k=1}^{q}(\zeta^k - \zeta^{-k})$ gilt

$$\begin{aligned} H_p^2 &= (-1)^q \prod_{k=1}^{q}(\zeta^k - \zeta^{-k})(\zeta^{-k} - \zeta^k) = (-1)^q \prod_{k=1}^{q}(1-\zeta^{2k})(1-\zeta^{-2k}) \\ &= (-1)^q \prod_{k=1}^{p-1}(1-\zeta^k) = (-1)^q \Phi_p(1) = p^* \end{aligned}$$

(vgl. Beweis von Satz I.12.23). Also existiert ein Vorzeichen $\epsilon = \pm 1$ mit $G_p = \epsilon H_p$. Jeder Faktor $\zeta^k - \zeta^{-k}$ von H_p ist rein-imaginär mit positivem Imaginärteil.[2] Dies zeigt $H_p = \sqrt{p^*}$ für $q \equiv 0, 1 \pmod 4$ und $H_p = -\sqrt{p^*}$ für $q \equiv 2, 3 \pmod 4$. Eine Fallunterscheidung mit den Ergänzungssätzen liefert $H_p = \left(\frac{-2}{p}\right)\sqrt{p^*}$ in allen Fällen. Es bleibt $\epsilon = \left(\frac{-2}{p}\right)$ zu zeigen.

Betrachten wir das Polynom

$$\alpha := \prod_{k=1}^{q}(X^k - X^{p-k}) - \epsilon \sum_{k=1}^{p} \left(\frac{k}{p}\right) X^k \in \mathbb{Z}[X].$$

Wegen $\alpha(1) = 0 - 0 = 0$, $\alpha(\zeta) = H_p - \epsilon G_p = 0$ und $\alpha \in \mathbb{Z}[X]$ sind alle p-ten Einheitswurzeln Nullstellen von α. Die Division durch das normierte Polynom $X^p - 1$ liefert $\beta \in \mathbb{Z}[X]$ mit

$$\alpha = (X^p - 1)\beta \equiv (X-1)^p \beta \equiv 0 \pmod{(X-1)^p} \tag{A.1.1}$$

in $\mathbb{F}_p[X]$. Wir substituieren $Y := X - 1$ und berechnen mit der binomischen Formel $X^k - X^{p-k} = (1+Y)^k - (1+Y)^{p-k} \equiv 2kY \pmod{Y^2}$ in $\mathbb{F}_p[X]$ für $k = 1, \ldots, q$. Nach dem Euler-Kriterium[3] gilt daher

$$\prod_{k=1}^{q}(X^k - X^{p-k}) \equiv 2^q q! Y^q \equiv \left(\frac{2}{p}\right) q! \pmod{Y^{q+1}}. \tag{A.1.2}$$

Für den zweiten Summanden von α gilt

$$\sum_{k=1}^{p} \left(\frac{k}{p}\right) X^k = \sum_{k=1}^{p} \left(\frac{k}{p}\right) \sum_{l=0}^{k} \binom{k}{l} Y^l \equiv \sum_{l=0}^{q} \sum_{k=1}^{p} \binom{k}{l} \left(\frac{k}{p}\right) Y^l \pmod{Y^{q+1}},$$

denn $\binom{k}{l} = 0$ für $k < l$. Offenbar ist $\binom{k}{l} = \frac{k(k-1)\ldots(k-l+1)}{l!}$ ein Polynom in k vom Grad $l \leq q$ mit Koeffizienten in $\mathbb{F}_p$. Für $\mathbb{F}_p^\times = \langle t \rangle$ und $d \in \mathbb{N}_0$ gilt

$$\sum_{k=1}^{p} k^d \left(\frac{k}{p}\right) \equiv \sum_{k=1}^{p} k^{d+q} \equiv \sum_{k=1}^{p} (tk)^{d+q} \equiv t^{d+q} \sum_{k=1}^{p} k^d \left(\frac{k}{p}\right) \pmod p.$$

[2] Dies unterscheidet ζ von einer beliebigen primitiven Einheitswurzel.
[3] Siehe Zahlentheorie-Skript

Im Fall $d < q$ ist $t^{d+q} \neq 1$ und man erhält $\sum_{k=1}^{p} k^d \left(\frac{k}{p}\right) \equiv 0 \pmod{p}$. Für $d = q$ hingegen ist

$$\sum_{k=1}^{p} k^q \left(\frac{k}{p}\right) \equiv \sum_{k=1}^{p} k^{p-1} \equiv -1 \pmod{p}.$$

Also verbleibt

$$\sum_{k=1}^{p} \left(\frac{k}{p}\right) X^k \equiv \sum_{k=1}^{p} \binom{k}{q} \left(\frac{k}{p}\right) Y^q \equiv -\frac{1}{q!} Y^q \pmod{Y^{q+1}}. \tag{A.1.3}$$

Nun kombinieren wir (A.1.1), (A.1.2) und (A.1.3) zu

$$\left(\left(\frac{2}{p}\right) q! + \frac{\epsilon}{q!}\right) Y^q \equiv \alpha \equiv 0 \pmod{Y^{q+1}}.$$

Nach Wilson (Aufgabe I.9) gilt $(q!)^2 \equiv 1 \cdot \ldots \cdot q \cdot (-q)(-q-1)\ldots(-1) \equiv (-1)^q (p-1)! \equiv -(-1)^q \equiv -\left(\frac{1}{p}\right)$ (mod p). Wir erhalten

$$\epsilon \equiv -(q!)^2 \left(\frac{2}{p}\right) \equiv \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) \equiv \left(\frac{-2}{p}\right) \pmod{p}$$

wie behauptet. □

2 Nullstellenbereiche und Eigenwerte

Bemerkung A.2.1. Zur Untersuchung der Galoisgruppe eines Polynoms ist es nützlich die Lage der Nullstellen in der komplexen Ebene zu lokalisieren. Wir beweisen einige geometrische Aussagen dieser Art und geben Anwendungen für Matrizen.

Satz A.2.2. *Für jede Nullstelle $x \in \mathbb{C}$ von $\alpha = X^n + a_1 X^{n-1} + \ldots + a_n \in \mathbb{C}[X]$ gilt*

$$|x| < \max\{|a_i| : i = 1, \ldots, n\} + 1.$$

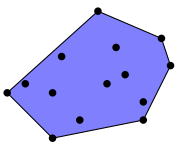
Beweis. Für $x \in \mathbb{C}$ mit $|x| \geq r := \max\{|a_i| : i = 1, \ldots, n\} + 1$ gilt

$$\begin{aligned} |\alpha(x)| &\geq |x|^n - |a_1||x|^{n-1} - \ldots - |a_n| \geq r|x|^{n-1} - |a_1||x|^{n-1} - \ldots - |a_n| \\ &\geq |x|^{n-1} - |a_2||x|^{n-2} - \ldots - |a_n| \geq \ldots \geq |x| - |a_n| \geq 1 \end{aligned}$$

nach der umgekehrten Dreiecksungleichung. □

Definition A.2.3. Eine Menge $C \subseteq \mathbb{C}$ heißt *konvex*, falls für $x, y \in C$ auch die Verbindungsstrecke $\{x + \lambda(y - x) : \lambda \in [0, 1]\}$ in C liegt. Die *konvexe Hülle* $\operatorname{conv}(S)$ einer Menge $S \subseteq \mathbb{C}$ ist der Durchschnitt aller konvexen Mengen, die S enthalten. Für $S = \{s_1, \ldots, s_n\}$ gilt

$$\operatorname{conv}(S) = \{\lambda_1 s_1 + \ldots + \lambda_n s_n : \lambda_1, \ldots, \lambda_n \in [0, 1],\ \lambda_1 + \ldots + \lambda_n = 1\}.$$



Satz A.2.4 (Gauss-Lucas)**.** *Sei $\alpha \in \mathbb{C}[X] \setminus \mathbb{C}$. Dann liegen die Nullstellen von α' in der konvexen Hülle der Nullstellen von α.*

Beweis. O. B. d. A. sei α normiert und $\alpha = (X - x_1) \ldots (X - x_n)$. Nach der Produktregel gilt

$$\frac{\alpha'}{\alpha} = \frac{1}{X - x_1} + \ldots + \frac{1}{X - x_n} \in \mathbb{C}(X).$$

Sei $y \in \mathbb{C}$ eine Nullstelle von α', die nicht in $C := \operatorname{conv}(x_1, \ldots, x_n)$ liegt. Die Vektoren $y - x_1, \ldots, y - x_n$ liegen dann in einem Kreissektor mit Winkel $< \pi$. Das Gleiche gilt für die Vektoren $\frac{1}{y - x_i} = \frac{\overline{y - x_i}}{|y - x_i|^2}$. Dies liefert den Widerspruch

$$0 = \frac{\alpha'(y)}{\alpha(y)} = \frac{1}{y - x_1} + \ldots + \frac{1}{y - x_n} \neq 0.$$ □

Folgerung A.2.5. *Sind alle Nullstellen von $\alpha \in \mathbb{C}[X]$ reell, so sind auch alle Nullstellen von α' reell.*

Bemerkung A.2.6. Für reelle Polynome lässt sich Folgerung A.2.5 mit dem Zwischenwertsatz aus der Analysis begründen (nach Lemma I.11.8 kann man annehmen, dass nur einfache Nullstellen vorliegen).

Satz A.2.7 (Sylvester). *Sei $\alpha \in \mathbb{R}[X]$ mit Nullstellen $\lambda_1, \ldots, \lambda_n \in \mathbb{C}$ (mit Vielfachheiten). Sei $\rho_k := \lambda_1^k + \ldots + \lambda_n^k$ für $k \in \mathbb{N}_0$ (vgl. Beispiel I.14.20). Genau dann sind alle λ_i reell, wenn die symmetrische Matrix*

$$A := (\rho_{i+j-2})_{i,j=1}^n \begin{pmatrix} \rho_0 & \rho_1 & \cdots & \rho_{n-1} \\ \rho_1 & \rho_2 & \cdots & \rho_n \\ \vdots & \vdots & & \vdots \\ \rho_{n-1} & \rho_n & \cdots & \rho_{2n-2} \end{pmatrix} \in \mathbb{R}^{n \times n}$$

positiv semidefinit ist.

Beweis (Nathanson). Für $x = (x_1, \ldots, x_n) \in \mathbb{R}^n$ sei $\beta := \sum_{i=1}^n x_i Y^{i-1} \in \mathbb{R}[Y]$. Dann gilt

$$xAx^{\mathrm{t}} = \sum_{i,j=1}^n \rho_{i+j-2} x_i x_j = \sum_{i,j,k=1}^n \lambda_k^{i+j-2} x_i x_j = \sum_{k=1}^n \beta(\lambda_k)^2.$$

Sind alle λ_k reell, so folgt $\beta(\lambda_k) \in \mathbb{R}$ und $xAx^{\mathrm{t}} \geq 0$, d. h. A ist positiv semidefinit. Sei nun o. B. d. A. $\lambda_1 \notin \mathbb{R}$. Wegen $\alpha \in \mathbb{R}[X]$ können wir $\lambda_2 = \overline{\lambda_1}$ annehmen. Seien $\lambda_1, \ldots, \lambda_s$ paarweise verschieden mit $\{\lambda_1, \ldots, \lambda_n\} = \{\lambda_1, \ldots, \lambda_s\}$. Durch Interpolation erhält man ein eindeutig bestimmtes Polynom $\beta = \sum_{i=1}^s x_i Y^{i-1} \in \mathbb{C}[Y]$ mit

$$\beta(\lambda_1) = \mathrm{i} = -\beta(\lambda_2) = \overline{\beta(\overline{\lambda_1})}$$

und $\beta(\lambda_k) = 0$ für $k = 3, \ldots, s$. Wegen

$$(\beta - \overline{\beta})(\lambda_k) = \beta(\lambda_k) - \overline{\beta(\overline{\lambda_k})} = 0$$

für $k = 1, \ldots, s$ gilt $\beta = \overline{\beta} \in \mathbb{R}[Y]$, d. h. $x_1, \ldots, x_s \in \mathbb{R}$. Sei $m \in \mathbb{N}$ die Vielfachheit der Nullstelle λ_1 (bzw. λ_2). Für $x = (x_1, \ldots, x_s, 0, \ldots, 0)$ folgt dann

$$xAx^{\mathrm{t}} = \sum_{k=1}^n \beta(\lambda_k)^2 = m(\mathrm{i}^2 + (-\mathrm{i})^2) = -2m < 0.$$

Also ist A nicht positiv semidefinit. □

Bemerkung A.2.8. Die Gleichung $xAx^{\mathrm{t}} = \sum \beta(\lambda_k)^2$ im Beweis zeigt, dass A genau dann invertierbar (bzw. positiv definit) ist, wenn die Nullstellen paarweise verschieden (und reell) sind.

Satz A.2.9 (Descartes' Vorzeichenregel). *Genau dann besitzt $\alpha = X^n + a_1 X^{n-1} + \ldots + a_n \in \mathbb{R}[X]$ lauter positive reelle Nullstellen, falls die Koeffizienten $a_1, \ldots, a_n$ alternierend sind, d. h. $a_i(-1)^i > 0$ für $i = 1, \ldots, n$.*

Beweis. Sei $a_i(-1)^i > 0$ für $i = 1, \ldots, n$. Für $x < 0$ gilt dann

$$\alpha(x) = (-1)^n(|x|^n + |a_1||x|^{n-1} + \ldots + |a_n|) \neq 0.$$

Seien umgekehrt $x_1, \ldots, x_n > 0$ die Nullstellen von α. Nach Vieta ist

$$a_k(-1)^k = \sigma_k(x_1, \ldots, x_n) > 0.$$ □

Folgerung A.2.10. *Eine symmetrische Matrix $A \in \mathbb{R}^{n \times n}$ mit charakteristischem Polynom $\chi_A = X^n + a_1 X^{n-1} + \ldots + a_n$ ist genau dann positiv definit, falls $a_i(-1)^i > 0$ für $i = 1, \ldots, n$ gilt.*

Beweis. Als symmetrische Matrix besitzt A nur reelle Eigenwerte. Bekanntlich ist A genau dann positiv definit, wenn alle Eigenwerte positiv sind. □

Satz A.2.11 (Sturm)**.** *Seien $\alpha_0 \in \mathbb{R}[X] \setminus \mathbb{R}$, $\alpha_1 := \alpha_0'$ und*

$$\alpha_{k-1} = \alpha_k \beta_k - \alpha_{k+1} \qquad (\textit{Division mit Rest})$$

für $k = 1, \ldots, n+1$ mit $\beta_k \in \mathbb{R}[X]$, $\deg \alpha_{k+1} < \deg \alpha_k$ und $\alpha_n \neq 0 \neq \alpha_{n+1}$. Für $x \in \mathbb{R}$ sei $v(x)$ die Anzahl der Vorzeichenwechsel in der Folge $\alpha_0(x), \ldots, \alpha_n(x)$ ohne Berücksichtigung von Nullen. Für $a < b$ mit $f(a)f(b) \neq 0$ ist dann $v(a) - v(b)$ die Anzahl der verschiedenen reellen Nullstellen von α_0 im Intervall $[a, b]$.

Beweis. Nach dem euklidischen Algorithmus ist α_n bis auf Normierung der ggT von α_0 und α_1. Nach Voraussetzung ist $\alpha_n(a)\alpha_n(b) \neq 0$. Man kann also mit der Folge $\widetilde{\alpha}_k := \alpha_k/\alpha_n$ arbeiten ohne $v(a)$ oder $v(b)$ zu verändern. Wir lassen x gedanklich von a nach b laufen und beobachten, wie sich $v(x)$ dabei verändert. Solange keines der $\widetilde{\alpha}_k$ bei x verschwindet, verändern sich die Vorzeichenwechsel nicht. Sei nun $x \in \mathbb{R}$ eine Nullstelle von α_0 mit Vielfachheit m. Nach Konstruktion ist dann $\widetilde{\alpha}_k(x) \neq 0$ für $k \geq 1$. Außerdem existiert $\gamma \in \mathbb{R}[X]$ mit $\alpha_0 = (X-x)^m\gamma$ und $\gamma(x) \neq 0$. Wegen $\alpha_1 = \alpha_0' = m(X-x)^{m-1}\gamma + (X-x)^m\gamma'$ existieren $\sigma, \tau \in \mathbb{R}[X]$ mit

$$\widetilde{\alpha}_0 = (X-x)\sigma, \qquad \widetilde{\alpha}_1 = m\sigma + (X-x)\tau, \qquad \sigma(x) \neq 0.$$

Für $y = x - \epsilon$ mit $\epsilon > 0$ gilt dann

$$\widetilde{\alpha}_0(y)\widetilde{\alpha}_1(y) = -\epsilon\sigma(y)(m\sigma(y) - \epsilon\tau(y)) = -\epsilon m\sigma(y)^2 + \epsilon^2\sigma(y)\tau(y).$$

Wegen $\lim_{\epsilon\to 0} \sigma(y)^2 = \sigma(x)^2 > 0$ und $\lim_{\epsilon\to 0} \epsilon\sigma(y)\tau(y) = 0$ kann man ϵ so klein wählen, dass $\widetilde{\alpha}_0(y)\widetilde{\alpha}_1(y) < 0$ gilt. Analog ist $\widetilde{\alpha}_0(y)\widetilde{\alpha}_1(y) > 0$ für $y = x + \epsilon$ mit ϵ klein genug. Die Anzahl der Vorzeichenwechsel in der Folge $\widetilde{\alpha}_k(x)$ reduziert sich daher um 1.

Sei nun $\widetilde{\alpha}_k(x)$ mit $k \geq 1$. Wegen $\widetilde{\alpha}_n = 1$ ist $k < n$. Nach Konstruktion sind $\widetilde{\alpha}_{k-1}$, $\widetilde{\alpha}_k$ und $\widetilde{\alpha}_{k+1}$ paarweise teilerfremd und

$$\widetilde{\alpha}_{k-1} = \widetilde{\alpha}_k\beta_k - \widetilde{\alpha}_{k+1}.$$

Daraus folgt $\widetilde{\alpha}_{k-1}(x) = -\widetilde{\alpha}_{k+1}(x) \neq 0$. Sowohl links als auch rechts von x gibt es somit genau einen Vorzeichenwechsel in der Folge $(\widetilde{\alpha}_{k-1}(x), \widetilde{\alpha}_k(x), \widetilde{\alpha}_{k+1}(x))$. Somit bleibt $v(x)$ an dieser Stelle unverändert. □

Beispiel A.2.12. Man kann die Sätze A.2.2 und A.2.11 kombinieren, um alle reellen Nullstellen eines reellen Polynoms zu bestimmen. Wir betrachten $\alpha = X^3 - X^2 + 1$. Nach Satz A.2.2 liegen alle Nullstellen im Einheitskreis mit Radius 2. Insbesondere liegen die reellen Nullstellen im Intervall $[-2, 2]$. Mit dem euklidischen Algorithmus berechnen wir die Folge aus dem Satz von Sturm:

$$\alpha_0 = X^3 - X^2 + 1, \qquad \alpha_1 = 3X^2 - 2X, \qquad \alpha_2 = \alpha_1\Big(\frac{1}{3}X - \frac{1}{9}\Big) - \alpha_0 = -\frac{7}{9}.$$

Es folgt $(\alpha_0(-2), \alpha_1(-2), \alpha_2(-2)) = (-11, 16, -\frac{7}{9})$ und $(\alpha_0(2), \alpha_1(2), \alpha_2(2)) = (5, 8, -\frac{7}{9})$. Daher besitzt α genau $v(-2) - v(2) = 2 - 1 = 1$ reelle Nullstelle.

Satz A.2.13 (Murty)**.** *Sei $\alpha = X^n + a_1X^{n-1} + \ldots + a_n \in \mathbb{Z}[X]$ und $\alpha(k) \in \mathbb{P}$ für eine natürliche Zahl $k \geq \max\{|a_i| : i = 1, \ldots, n\} + 2$. Dann ist α irreduzibel in $\mathbb{Q}[X]$.*

Beweis. Sei $m := \max\{|a_i| : i = 1, \ldots, n\}$. Für jede Nullstelle $x \in \mathbb{C}$ von α gilt $|x| < m + 1$ nach Satz A.2.2. Nach Gauß' Lemma können wir $\alpha = \beta\gamma$ mit normierten $\beta, \gamma \in \mathbb{Z}[X] \setminus \mathbb{Z}$ annehmen. Wegen $\beta(k)\gamma(k) = \alpha(k) \in \mathbb{P}$ dürfen wir $\beta(k) = \pm 1$ voraussetzen. Nach dem Fundamentalsatz der Algebra gilt $\beta = (X - x_1) \ldots (X - x_s)$ für gewisse Nullstellen $x_1, \ldots, x_s \in \mathbb{C}$ von α. Obige Abschätzung liefert nun den Widerspruch

$$|\beta(k)| = \prod_{i=1}^{s} |k - x_i| \geq \prod_{i=1}^{s} (k - |x_i|) > \prod_{i=1}^{s} (k - (m+1)) \geq 1. \qquad \square$$

Satz A.2.14 (Gershgorin). *Für jeden Eigenwert $\lambda \in \mathbb{C}$ von $(a_{ij}) \in \mathbb{C}^{n \times n}$ existiert ein $i \in \{1, \ldots, n\}$ mit $|\lambda - a_{ii}| \leq \sum_{j \neq i} |a_{ij}|$.*

Beweis. Sei $x = (x_1, \ldots, x_n) \in \mathbb{C}^n$ ein Eigenvektor zum Eigenwert λ. Sei $|x_i| = \max\{|x_j| : j = 1, \ldots, n\} > 0$. Nach Normierung können wir $x_i = 1$ und $|x_j| \leq 1$ für $j \neq i$ annehmen. Nach der Dreiecksungleichung gilt dann

$$|\lambda - a_{ii}| = |\lambda x_i - a_{ii} x_i| = \Big|\sum_{j=1}^{n} a_{ij} x_j - a_{ii} x_i\Big| = \Big|\sum_{j \neq i} a_{ij} x_j\Big| \leq \sum_{j \neq i} |a_{ij}|. \qquad \square$$

Bemerkung A.2.15.

(i) Da A^{t} die gleichen Eigenwerte wie A besitzt, kann man Satz A.2.14 auch auf die Spalten von A anwenden.

(ii) Wendet man Satz A.2.14 auf die Begleitmatrix von $\alpha = X^n + a_1 X^{n-1} + \ldots + a_n \in \mathbb{C}[X]$ an, so erhält man

$$|x| \leq \max\big\{|a_n|, |a_{n-1}| + 1, \ldots, |a_1| + 1\big\}$$

für jede Nullstelle $x \in \mathbb{C}$ von α (beachte $1 \geq |x + a_1| \geq |x| - |a_1|$). Dies verbessert Satz A.2.2.

(iii) Für jede Matrix $A \in K^{n \times n}$ über einem Körper K ist bekanntlich $\mathrm{tr}(A)$ die Summe der Eigenwerte (in einem Zerfällungskörper). Die folgenden Sätze garantieren die Existenz von Matrizen mit vorgegebener Hauptdiagonale und Eigenwerten.

Satz A.2.16 (Fillmore). *Sei K ein Körper, $A \in K^{n \times n} \setminus K1_n$ und $d_1, \ldots, d_n \in K$ mit $\mathrm{tr}(A) = d_1 + \ldots + d_n$. Dann ist A zu einer Matrix mit Hauptdiagonale $d_1, \ldots, d_n$ ähnlich.*

Beweis. Induktion nach n: Wegen $A \notin K1_n$ ist $n \geq 2$ und nicht jeder Vektor ist ein Eigenvektor für A. Also existiert $b_1 \in K^n$, sodass b_1 und Ab_1 linear unabhängig sind. Wir ergänzen $b_1, b_2 := Ab_1 - d_1 b_1$ zu einer Basis $b_1, \ldots, b_n$ von K^n. Bezüglich dieser Basis hat A die Form $\left(\begin{smallmatrix} d_1 & * \\ * & A_1 \end{smallmatrix}\right)$ mit $A_1 \in K^{(n-1)\times(n-1)}$. Im Fall $n = 2$ sind wir fertig, denn $\mathrm{tr}(A_1) = \mathrm{tr}(A) - d_1 = d_2$. Sei nun $n \geq 3$. Ist $A_1 \in K1_{n-1}$, so ersetzen wir b_3 durch $b_1 + b_3$. Wegen $A(b_1 + b_3) = a_1 b_1 + b_2 + Ab_3$ ist anschließend $a_{23} = 1$ und $A_1 \notin K1_{n-1}$. Nach Induktion existiert $S \in \mathrm{GL}(n-1, K)$, sodass SA_1S^{-1} Hauptdiagonale $d_2, \ldots, d_n$ hat. Nun hat

$$\begin{pmatrix} 1 & 0 \\ 0 & S \end{pmatrix} \begin{pmatrix} d_1 & * \\ * & A_1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & S^{-1} \end{pmatrix} = \begin{pmatrix} d_1 & * \\ * & SA_1S^{-1} \end{pmatrix}$$

Hauptdiagonale $d_1, \ldots, d_n$. $\square$

Satz A.2.17 (MIRSKY). *Sei K ein Körper und $d_1, \ldots, d_n, \lambda_1, \ldots, \lambda_n \in K$ mit $d_1+\ldots+d_n = \lambda_1+\ldots+\lambda_n$. Dann existiert eine Matrix $A \in K^{n\times n}$ mit Hauptdiagonale $d_1, \ldots, d_n \in K$ und Eigenwerten $\lambda_1, \ldots, \lambda_n \in K$.*

Beweis. Im Fall $n = 1$ erfüllt $A = (d_1) = (\lambda_1)$ die Behauptung. Sei $n \geq 2$ und $A = (a_{ij}) \in K^{n\times n} \setminus K1_n$ eine obere Dreiecksmatrix mit Diagonale $\lambda_1, \ldots, \lambda_n$. Dann hat A Eigenwerte $\lambda_1, \ldots, \lambda_n$. Die Behauptung folgt nun aus Fillmore, da ähnliche Matrizen die gleichen Eigenwerte haben. □

Satz A.2.18.

(i) (SCHUR) *Ist $A \in \mathbb{C}^{n\times n}$ hermitesch mit Hauptdiagonale $d_1 \geq \ldots \geq d_n$ und Eigenwerten $\lambda_1 \geq \ldots \geq \lambda_n$, so gilt*

$$\sum_{i=1}^{k} d_i \leq \sum_{i=1}^{k} \lambda_i \qquad (1 \leq k \leq n)$$

mit Gleichheit im Fall $k = n$.

(ii) (HORN) *Sind reelle Zahlen $d_1 \geq \ldots \geq d_n$ und $\lambda_1 \geq \ldots \geq \lambda_n$ mit $\sum_{i=1}^{k} d_i \leq \sum_{i=1}^{k} \lambda_i$ für $1 \leq k \leq n$ und $\sum_{i=1}^{n} d_i = \sum_{i=1}^{n} \lambda_i$ gegeben, so existiert eine symmetrische Matrix mit Hauptdiagonale $d_1, \ldots, d_n$ und Eigenwerten $\lambda_1, \ldots, \lambda_n$.*

Beweis (CHAN-LI).

(i) Nach dem Spektralsatz existiert eine unitäre Matrix $S := (s_{ij})$ mit $A = (a_{ij}) = \overline{S}^{\mathrm{t}} \operatorname{diag}(\lambda_1, \ldots, \lambda_n)S$. Für $1 \leq k \leq n$ gilt

$$\sum_{i=1}^{k} d_i = \sum_{i=1}^{k} a_{ii} = \sum_{i=1}^{k}\sum_{j=1}^{n} \overline{s_{ji}} s_{ji} \lambda_j = \sum_{j=1}^{n} \lambda_j \sum_{i=1}^{k} |s_{ji}|^2. \tag{A.2.1}$$

Da S unitär ist, gilt $t_j := \sum_{i=1}^{k} |s_{ji}|^2 \leq 1$ mit Gleichheit falls $k = n$. Es folgt $\sum_{j=1}^{n} t_j = \sum_{i=1}^{k}\sum_{j=1}^{n} |s_{ji}|^2 = k$ und

$$\begin{aligned}\sum_{i=1}^{k}(d_i - \lambda_i) &= \sum_{j=1}^{n} \lambda_j t_j - \sum_{j=1}^{k} \lambda_j + \lambda_k \overbrace{\big(k - \sum_{i=1}^{n} t_i\big)}^{=0} \\ &= \sum_{j=1}^{k} \underbrace{(\lambda_j - \lambda_k)}_{\geq 0} \underbrace{(t_j - 1)}_{\leq 0} + \sum_{i=k+1}^{n} t_i \underbrace{(\lambda_i - \lambda_k)}_{\leq 0} \leq 0.\end{aligned}$$

Also ist $\sum_{i=1}^{k} d_i \leq \sum_{i=1}^{k} \lambda_i$ und $\sum_{i=1}^{n} d_i = \operatorname{tr}(A) = \sum_{i=1}^{n} \lambda_i$.

(ii) Induktion nach n: Im Fall $n = 1$ erfüllt $(d_1) = (\lambda_1)$ die Behauptung. Sei $n = 2$. Dann gilt $\lambda_1 \geq d_1 \geq d_2 = \lambda_1 + \lambda_2 - d_1 \geq \lambda_2$. Im Fall $\lambda_1 = \lambda_2$ können wir $d_1 1_2$ wählen. Im Fall $\lambda_1 > \lambda_2$ ist

$$S := \frac{1}{\sqrt{\lambda_1 - \lambda_2}} \begin{pmatrix} \sqrt{d_1 - \lambda_2} & -\sqrt{\lambda_1 - d_1} \\ \sqrt{\lambda_1 - d_1} & \sqrt{d_1 - \lambda_2} \end{pmatrix} \in \mathrm{O}(2, \mathbb{R}).$$

Für $A = (a_{ij}) = S^{\mathrm{t}} \operatorname{diag}(\lambda_1, \lambda_2)S$ gilt

$$a_{11} = \frac{1}{\lambda_1 - \lambda_2}\big((d_1 - \lambda_2)\lambda_1 + (\lambda_1 - d_1)\lambda_2\big) = d_1$$

nach (A.2.1). Es folgt $a_{22} = \lambda_1 + \lambda_2 - d_1 = d_2$. Sei nun $n \geq 3$ und

$$\lambda_2' := \lambda_1 + \lambda_2 - d_1 \geq \lambda_2.$$

Nach Induktion existiert $S \in \mathrm{O}(2, \mathbb{R})$, sodass $S^{\mathrm{t}} \operatorname{diag}(\lambda_1, \lambda_2) S$ Hauptdiagonale (d_1, λ_2') hat. Da die Folgen $(\lambda_2', \lambda_3, \ldots, \lambda_n)$ und $(d_2, \ldots, d_n)$ die gleichen Voraussetzungen erfüllen, existiert nach Induktion ein $T \in \mathrm{O}(n-1, \mathbb{R})$, sodass $T^{\mathrm{t}} \operatorname{diag}(\lambda_2', \ldots, \lambda_n) T$ Hauptdiagonale $d_2, \ldots, d_n$ hat. Für $U := (S \oplus 1_{n-2})(1_1 \oplus T) \in \mathrm{O}(n, \mathbb{R})$ hat

$$U^{\mathrm{t}} \operatorname{diag}(\lambda_1, \ldots, \lambda_n) U = \begin{pmatrix} 1 & 0 \\ 0 & T^{\mathrm{t}} \end{pmatrix} \begin{pmatrix} d_1 & * & & & 0 \\ * & \lambda_2' & & & \\ & & \lambda_3 & & \\ & & & \ddots & \\ 0 & & & & \lambda_n \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & T \end{pmatrix}$$

Hauptdiagonale $(d_1, \ldots, d_n)$. □

3 Kreisteilungspolynome

Bemerkung A.3.1. In diesem Abschnitt geben wir vier Anwendungen von Kreisteilungspolynomen: Spezialfälle von Dirichlets Primzahlsatz, Ganzheitsbasen von $\mathbb{Q}_n$, die Peirce-Zerlegung von $\mathbb{F}_q C_n$ und die Existenz von sogenannten Zsigmondy-Primzahlen.

Definition A.3.2. Ein *Primteiler* von $\alpha \in \mathbb{Z}[X]$ ist eine Primzahl p, die $\alpha(n)$ für ein $n \in \mathbb{Z}$ teilt. Die Menge der Primteiler von α sei $\Pi(\alpha)$.

Satz A.3.3. *Für $\alpha \in \mathbb{Z}[X] \setminus \mathbb{Z}$ gilt:*

(i) Für unendlich viele $n \in \mathbb{N}$ ist $\alpha(n)$ keine Primzahl.

(ii) α besitzt unendlich viele Primteiler.

Beweis.

(i) O. B. d. A. sei der führende Koeffizient von α positiv (anderenfalls ersetze α durch $-\alpha$). Wegen $\alpha \notin \mathbb{Z}$ gilt $\lim_{x\to\infty} \alpha(x) = \infty$. Sei p ein Primteiler von $\alpha(n)$. Für $k \in \mathbb{N}$ gilt $\alpha(n + pk) \equiv \alpha(n) \equiv 0 \pmod{p}$. Daher sind unendlich viele Werte der Form $\alpha(n + pk)$ keine Primzahlen.

(ii) Sei $\alpha = a_d X^d + \ldots + a_0$. Im Fall $a_0 = 0$ ist $p \mid \alpha(p)$ für jede Primzahl p. Sei also $a_0 \neq 0$. Wegen $\alpha(a_0 X) = a_0(a_0^{d-1} a_d X^{d-1} + \ldots + 1)$ dürfen $a_0 = 1$ annehmen. Wegen $d \geq 1$ hat α mindestens einen Primteiler. Angenommen $p_1, \ldots, p_s$ sind die einzigen Primteiler von α. Dann existiert $\beta \in \mathbb{Z}[X] \setminus \mathbb{Z}$ mit $\alpha(p_1 \ldots p_s X) = p_1 \ldots p_s \beta(X) + 1$. Offenbar existiert $n \in \mathbb{N}$ mit $p_1 \ldots p_s \beta(n) + 1 \neq \pm 1$. Jeder Primteiler dieser Zahl wäre neuer Primteiler von α. □

Bemerkung A.3.4. In Lemma I.12.15 haben wir gesehen, dass fast alle Primteiler von Φ_n kongruent zu 1 modulo n sind. Mit Satz A.3.3 folgt nun Satz I.12.17. Die nächsten Sätze verallgemeinern dieses Prinzip.

Satz A.3.5. *Für $n \geq 1$ existieren unendlich viele Primzahlen $p \equiv 1 + 2^{n-1} \pmod{2^n}$.*

Beweis. O. B. d. A. sei $n \geq 2$. Nach Lemma I.12.15 sind alle ungeraden Primteiler von

$$\alpha := \Phi_{2^{n-1}} \overset{I.12.10}{=} X^{2^{n-2}} + 1$$

kongruent zu 1 modulo 2^{n-1}. Angenommen α besitzt nur endlich viele Primteiler $p \equiv 1 + 2^{n-1} \pmod{2^n}$. Sei q deren Produkt ($q = 1$ zugelassen). Nach dem chinesischen Restsatz existiert ein $m \in \mathbb{N}$ mit $m \equiv 0 \pmod{q}$ und $m \equiv 5 \pmod{2^{n+1}}$. Wegen $\alpha(m) \equiv \alpha(0) \equiv 1 \pmod{q}$ sind alle ungeraden Primteiler von $\alpha(m)$ kongruent zu 1 modulo 2^n. Andererseits ist

$$\alpha(m) \equiv \alpha(5) = 5^{2^{n-2}} + 1 = (1 + 4)^{2^{n-2}} + 1 \equiv 2 + 2^n \pmod{2^{n+1}}.$$

Dann wäre aber $\frac{1}{2}\alpha(m) \equiv 1 + 2^{n-1} \pmod{2^n}$ das Produkt von Primzahlen $p \equiv 1 \pmod{2^n}$. □

Satz A.3.6 (SCHUR). *Seien $a, n \in \mathbb{N}$ mit $a^2 \equiv 1 \pmod{n}$. Gibt es eine Primzahl $p \geq \frac{1}{2}\varphi(n)$ mit $p \equiv a \pmod{n}$, so gibt es unendlich viele solche Primzahlen.*

Beweis. O. B. d. A. sei $n \geq 3$ und $k := \varphi(n)/2$. Nach Satz I.12.17 können wir $a \not\equiv 1 \pmod{n}$ annehmen. Sei $\zeta \in \mathbb{C}$ eine primitive n-te Einheitswurzel und $\sigma \in G := \mathrm{Gal}(\mathbb{Q}_n|\mathbb{Q})$ mit $\sigma(\zeta) = \zeta^a$. Nach Voraussetzung ist $\sigma^2 = 1$. Für $\tau \in G \setminus \langle\sigma\rangle$ können die Polynome $(X-\zeta)(X-\zeta^a)$ und $(X-\tau(\zeta))(X-\tau(\zeta)^a)$ an höchstens endlich vielen Stellen übereinstimmen. Daher existiert ein $z \in \mathbb{Z}$ („groß genug"), sodass $\eta := (z-\zeta)(z-\zeta^a)$ ein primitives Element von $\mathbb{Q}_n^\sigma$ ist. Sei $1 = \tau_1, \ldots, \tau_k \in G$ ein Repräsentantensystem für die Nebenklassen von $\langle\sigma\rangle$ in G. Dann ist

$$\alpha := (-1)^k \prod_{i=1}^{k} (X - \tau_i(\eta)) \in \mathbb{Q}_n^G[X] = \mathbb{Q}[X].$$

Da ζ und η ganz-algebraisch sind, gilt sogar $\alpha \in \mathbb{Z}[X]$. Sei $D := \prod_{i<j}(\tau_j(\eta) - \tau_i(\eta))^2 \in \mathbb{Z}$ die Diskriminante von α.

Schritt 1: Für $p \in \Pi(\alpha)$ gilt $p \mid n$, $p \mid D$ oder $p \equiv a^i \pmod{n}$ mit $i \in \{0,1\}$.
Sei $m \in \mathbb{N}$ und p ein Primteiler von $\alpha(m)$ mit $p \nmid n$ und $p \nmid D$. Sei R der Ganzheitsring von $\mathbb{Q}_n$. Wegen $1/p \notin R$ existiert ein maximales Ideal $P \trianglelefteq R$ mit $p \in P$ (Satz II.2.7). Dann ist $K := R/P$ ein Körper der Charakteristik p und $P \cap \mathbb{Z} = p\mathbb{Z}$. In K gilt $(m - \tau_1(\eta)) \ldots (m - \tau_k(\eta)) = 0$. Sei daher $m \equiv \tau_l(\eta) \pmod{P}$ für ein $1 \leq l \leq k$. Wegen $p \nmid n$ ist auch ζ^p eine primitive n-te Einheitswurzel. Daher existiert $1 \leq j \leq k$ mit $(z - \tau_l(\zeta^p))(z - \tau_l(\zeta^p)^a) = \tau_j(\eta)$. Mit dem Frobenius-Homomorphismus und Fermat-Euler erhält man

$$\tau_j(\eta) \equiv \big(z^p - \tau_l(\zeta)^p\big)\big(z^p - \tau_l(\zeta^a)^p\big) \equiv \tau_l(\eta)^p \equiv m^p \equiv m \equiv \tau_l(\eta) \pmod{P}.$$

Im Fall $j \neq l$ ist $\tau_j(\eta) - \tau_l(\eta)$ ein Faktor von D und man erhält $D \in P \cap \mathbb{Z} = p\mathbb{Z}$. Dann wäre aber $p \mid D$. Also ist $j = l$ und $(z - \zeta^p)(z - \zeta^{ap}) = \eta$. Dies zeigt $p \equiv a^i \pmod{p}$ für $i \in \{0,1\}$.

Schritt 2: Jede Primzahl $p \equiv a^i \pmod{p}$ ist ein Primteiler von α.
Wie in Schritt 1 gilt

$$\eta^p \equiv (z - \zeta^p)(z - \zeta^{ap}) \equiv (z - \zeta^{a^i})(z - \zeta^{a^{i+1}}) \equiv \eta \pmod{P}.$$

Daher ist η eine Nullstelle von $X^p - X$ in K. Andererseits besitzt $X^p - X$ nur die p Nullstellen im Primkörper $\mathbb{F}_p \subseteq K$. Also existiert $m \in \mathbb{Z}$ mit $\eta \equiv m \pmod{P}$. Es folgt $\alpha(m) \in P \cap \mathbb{Z} = p\mathbb{Z}$.

Schritt 3: Es existieren $m \in \mathbb{N}$, $p \in \mathbb{P}$ mit $p \equiv a \pmod{n}$, $p \mid \alpha(m)$ und $p^2 \nmid \alpha(m)$.
Nach Voraussetzung existiert eine Primzahl $p \equiv a \pmod{n}$ mit $p > k$. Nach Schritt 2 existiert $m \in \mathbb{N}$ mit $p \mid \alpha(m)$. Wir nehmen $p^2 \mid \alpha(m)$ an. Schreibe $\alpha = \sum a_i X^i$. Dann gilt

$$\alpha(m+p) = \sum a_i (m+p)^i \equiv \sum a_i (m^i + i m^{i-1} p) \equiv \alpha(m) + p\alpha'(m) \equiv p\alpha'(m) \pmod{p^2}.$$

Im Fall $p \nmid \alpha'(m)$ können wir m durch $m + p$ ersetzen und sind fertig. Sei also $p \mid \alpha'(m)$. Nach Lemma I.11.8 ist m eine mehrfache Nullstelle von α in K. Daher existieren ein $1 \leq s < t \leq k$ mit $\tau_s(\eta) \equiv \tau_t(\eta) \pmod{P}$. Indem wir P durch $\tau_t^{-1}(P) \trianglelefteq R$ ersetzen, können wir $t = 1$ annehmen. Dies bedeutet

$$z\big(\tau_s(\zeta) + \tau_s(\zeta)^a - \zeta - \zeta^a\big) \equiv \tau_s(\zeta)^{1+a} - \zeta^{1+a} \pmod{P}.$$

Nehmen wir $\tau_s(\zeta) + \tau_s(\zeta)^a \equiv \zeta + \zeta^a \pmod{P}$ an. Dann folgt $\tau_s(\zeta)^{1+a} \equiv \zeta^{1+a} \pmod{P}$ und

$$\tau_s((X-\zeta)(X-\zeta^a)) \equiv (X-\zeta)(X-\zeta^a) \pmod{P}.$$

Dies zeigt $\tau_s(\zeta) \equiv \zeta^{a^i} \pmod{P}$ für ein $i \in \{0,1\}$. Wegen $\tau_s \notin \langle\sigma\rangle$ ist andererseits $\tau_s(\zeta) \neq \zeta^{a^i}$. Folglich besitzt auch $X^n - 1$ eine mehrfache Nullstelle in K. Andererseits ist $(X^n-1)' = nX^{n-1}$ zu $X^n - 1$ teilerfremd (beachte $p \nmid n$). Dieser Widerspruch zeigt $\tau_s(\zeta)+\tau_s(\zeta)^a \not\equiv \zeta+\zeta^a \pmod{P}$. Also ist z modulo P und auch modulo p eindeutig durch l bestimmt. Für l gibt es höchstens $k-1$ Möglichkeiten. Wegen $p > k-1$ existiert eine Restklasse $r + p\mathbb{Z}$, sodass für $z \in r + p\mathbb{Z}$ stets $p^2 \nmid \alpha(m)$ oder $p^2 \nmid \alpha(m+p)$ gilt.

Schritt 4: Jeder Primteiler von $\alpha(0)$ ist kongruent zu 1 modulo n.
Mit dem chinesischen Restsatz können wir erreichen, dass z durch n teilbar ist ohne die Restklasse $r + p\mathbb{Z}$ zu verlassen. Nach Definition von α gilt $\alpha(0) = \Phi_n(z)$. Wegen $n \geq 3$ treten die primitiven n-ten Einheitswurzeln in Paaren der Form ζ^i, ζ^{-i} auf. Daher hat Φ_n Absolutglied 1 und es folgt $\Phi_n(z) = \Phi_n(0) \equiv 1 \pmod{n}$. Nach Lemma I.12.15 ist nun jeder Primteiler von $\alpha(0)$ kongruent zu 1 modulo n.

Schritt 5: Widerspruch.
Seien m und p wie in Schritt 3. Angenommen es gibt nur endlich viele Primzahlen in $a + n\mathbb{Z}$. Dann gibt es auch nur endlich viele Primteiler von α, die nicht in $1 + n\mathbb{Z}$ liegen (Schritt 1). Sei q das Produkt dieser Primteiler ohne p. Nach dem chinesischen Restsatz existiert $c \in \mathbb{Z}$ mit $c \equiv m \pmod{p^2}$ und $c \equiv 0 \pmod{nq}$. Es folgt $\alpha(c) \equiv \alpha(m) \pmod{p^2}$ und $\alpha(c) \equiv \alpha(0) \pmod{nq}$. Also ist p ein Primteiler von $\alpha(c)$ mit Vielfachheit 1. Alle weiteren Primteiler von $\alpha(c)$ liegen in $1 + n\mathbb{Z}$, denn $\alpha(0)$ besitzt nur solche Primteiler (Schritt 4). Dies ergibt den Widerspruch $a \equiv p \equiv \alpha(c) \equiv \alpha(0) \equiv 1 \pmod{n}$. □

Folgerung A.3.7. *In jeder primen Restklasse modulo* 24 *liegen unendlich viele Primzahlen.*

Beweis. Für $a + 24\mathbb{Z} \in (\mathbb{Z}/24\mathbb{Z})^\times \cong C_2^3$ gilt $a^2 \equiv 1 \pmod{24}$. Nach Satz I.12.17 können wir $a \not\equiv 1 \pmod{24}$ annehmen. Nach Satz A.3.6 genügt es aus jeder solchen Restklasse eine Primzahl $p \geq \frac{1}{2}\varphi(24) = 4$ anzugeben. Tatsächlich sind die kleinsten Vertreter $a \in \{5, 7, 11, 13, 17, 19, 23\}$ bereits Primzahlen. □

Bemerkung A.3.8. Wegen $11 + 24\mathbb{Z} \subseteq 3 + 8\mathbb{Z}$, $5 + 24\mathbb{Z} \subseteq 5 + 8\mathbb{Z}$ und $7 + 24\mathbb{Z} \subseteq 7 + 8\mathbb{Z}$ enthält auch jede prime Restklasse modulo 8 unendlich viele Primzahlen.

Satz A.3.9 (Bauer)**.** *Für jedes $n \in \mathbb{N}$ existieren unendlich viele Primzahlen $p \equiv -1 \pmod{n}$.*

Beweis. O. B. d. A. sei $n \geq 3$ und $k := \varphi(n)/2$. Wir argumentieren wie im Beweis von Satz A.3.6 mit $a = -1$. Dann ist $\eta = (z - \zeta)(z - \bar{\zeta}) \in \mathbb{R}$ eine einfache Nullstelle von $\alpha \in \mathbb{Z}[X]$. Folglich muss α bei η das Vorzeichen wechseln. Also existieren $x, y \in \mathbb{Z}$ mit $\alpha(x/y) < 0$ und $y > 0$. Wir definieren $\beta := y^k \alpha(X/y) \in \mathbb{Z}[X]$. Mit α ist auch β normiert. Außerdem ist $\beta(x) < 0$. Schließlich sei

$$\gamma := -\frac{1}{\beta(x)}\beta(x - \beta(x)X).$$

Das Absolutglied von γ ist $\gamma(0) = -1$. In allen anderen Koeffizienten lässt sich $\beta(x)$ kürzen, sodass $\gamma \in \mathbb{Z}[X]$ folgt. Der führende Koeffizient ist $(-\beta(x))^{k-1} > 0$. Insbesondere ist $\gamma(m) > 1$ für m „groß genug“. Nehmen wir an, dass γ nur endlich viele Primteiler $p \not\equiv 1 \pmod{n}$ besitzt. Sei q deren Produkt ($q = 1$ zugelassen). Jeder Primteiler p von $\gamma(mnq) > 0$ erfüllt dann $p \equiv 1 \pmod{n}$, denn $\gamma(mnq) \equiv \gamma(0) \equiv -1 \pmod{q}$. Andererseits ist aber $\gamma(mnq) \equiv -1 \pmod{n}$. Dieser Widerspruch zeigt, dass γ unendlich viele Primteiler $p \not\equiv 1 \pmod{n}$ besitzt. Wegen $\gamma(m) \mid \beta(x - \beta(x)m)$ ist $\Pi(\gamma) \subseteq \Pi(\beta)$. Sei nun p ein Primteiler von $\beta(m)$ mit $p \nmid y$. Dann existiert ein $m' \in \mathbb{N}$ mit $ym' \equiv m \pmod{p}$. Es folgt

$$y^k \alpha(m') = \beta(ym') \equiv \beta(m) \equiv 0 \pmod{p}.$$

Dies impliziert $p \mid \alpha(m')$. Also hat auch α unendlich viele Primteiler $p \not\equiv 1 \pmod{n}$. Aus Schritt 1 im Beweis von Satz A.3.6 wissen wir andererseits, dass fast alle (bis auf endlich viele) Primteiler von α die Kongruenz $p \equiv \pm 1 \pmod{n}$ erfüllen. Es muss daher unendlich viele Primteiler $p \equiv -1 \pmod{n}$ geben. □

Definition A.3.10. Sei $K \subseteq L$ eine Galois-Erweiterung mit $\mathrm{Gal}(L|K) = \{\sigma_1, \ldots, \sigma_n\}$. Sei $x_1, \ldots, x_n$ eine K-Basis von L und $M := (\sigma_i(x_j))_{1 \le i,j \le n}$. Die *Diskriminante* von $x_1, \ldots, x_n$ bzgl. K ist

$$D(x_1, \ldots, x_n) := \det(M)^2.$$

Bemerkung A.3.11.

(i) Durch die Quadratbildung hängt $D := D(x_1, \ldots, x_n)$ weder von der Reihenfolge der x_i noch von der Reihenfolge der σ_i ab. Insbesondere gilt $\sigma_i(D) = D$ für $i = 1, \ldots, n$ und es folgt $D \in L^{\mathrm{Gal}(L|K)} = K$.

(ii) Für alle $\lambda = (\lambda_1, \ldots, \lambda_n) \in K^n \setminus \{0\}$ gilt $M\lambda = (\sigma_i(\lambda_1 x_1 + \ldots + \lambda_n x_n))_i \neq 0$. Daher ist M invertierbar und $D(x_1, \ldots, x_n) \neq 0$.

(iii) Ist $K = \mathbb{Q}$ und $x_1, \ldots, x_n$ eine Ganzheitsbasis von L, so ist D ganz-algebraisch, also $D \in \mathbb{Z}$. Ist $y_1, \ldots, y_n$ eine weitere Ganzheitsbasis von L, so existiert ein $S = (s_{ij}) \in \mathrm{GL}(n, \mathbb{Z})$ mit $Sx = y$. Mit $M := (\sigma_i(x_j))_{i,j}$ folgt

$$\begin{aligned} D(y_1, \ldots, y_n) &= \det\big((\sigma_i(y_j))_{i,j}\big)^2 = \det\Big(\Big(\sum_{k=1}^{n} s_{jk}\sigma_i(x_k)\Big)_{i,j}\Big)^2 \\ &= \det(MS^{\mathrm{t}})^2 = \det(M)^2 \det(S)^2 = D(x_1, \ldots, x_n). \end{aligned}$$

Die Diskriminante ist also eine Invariante des Ganzheitsrings $\mathbb{Z}_L$.

Beispiel A.3.12. Nach dem Satz vom primitiven Element besitzt jede Galois-Erweiterung $K \subseteq L$ eine Basis der Form $1, x, \ldots, x^{n-1}$. Nun ist $(\sigma_i(x^{j-1}))_{1 \le i,j \le n}$ eine Vandermonde-Matrix mit Determinante $\prod_{i<j}(\sigma_j(x) - \sigma_i(x))$. Daher ist $D(1, x, \ldots, x^{n-1}) = D_\mu$ die Diskriminante des Minimalpolynoms μ von x. Der nächste Satz hat daher Bezug zu Aufgabe I.68.

Satz A.3.13 (Stickelberger)**.** *Für jede Ganzheitsbasis $x_1, \ldots, x_n$ eines Zahlkörpers ist $D(x_1, \ldots, x_n)$ kongruent zu 0 oder 1 modulo 4.*

Beweis. Sei K der besagte Zahlkörper und $\mathrm{Gal}(K|\mathbb{Q}) = \{\sigma_1, \ldots, \sigma_n\}$ sowie $M = (\sigma_i(x_j))_{i,j}$. Für eine Permutation $\tau \in S_n$ sei $s_\tau := \sigma_1(x_{\tau(1)}) \ldots \sigma_n(x_{\tau(n)}) \in K$. Sei $S_+ := \sum_{\tau \in A_n} s_\tau$ und $S_- := \sum_{\tau \in S_n \setminus A_n} s_\tau$. Nach der Leibniz-Formel gilt $\det M = S_+ - S_-$ und

$$D(x_1, \ldots, x_n) = \det(M)^2 = (S_+ - S_-)^2 = (S_+ + S_-)^2 - 4S_+S_- \in \mathbb{Z}.$$

Da jedes σ_i die s_τ permutiert, gilt $S_+ + S_- \in \mathbb{Z}$. Daher ist $S_+S_- \in \mathbb{Q} \cap \mathbb{Z}_K = \mathbb{Z}$ und es folgt $D(x_1, \ldots, x_n) \equiv (S_+ + S_-)^2 \equiv 0, 1 \pmod{4}$. □

Lemma A.3.14. *Sei $p \in \mathbb{P}$, $n \in \mathbb{N}$ und ζ eine primitive p^n-te Einheitswurzel. Sei $k := \varphi(p^n)$. Dann gilt*

$$D(1, \zeta, \ldots, \zeta^{k-1}) = (-1)^{\binom{k}{2}} p^{p^{n-1}(np-n-1)}.$$

Beweis. Sei $m := p^n$ und $G := \mathrm{Gal}(\mathbb{Q}_m|\mathbb{Q}) = \{\sigma_1, \ldots, \sigma_k\}$. Bekanntlich ist $1, \zeta, \ldots, \zeta^{k-1}$ eine $\mathbb{Q}$-Basis von $\mathbb{Q}(\zeta) = \mathbb{Q}_m$. Nach Beispiel A.3.12 ist

$$D := D(1, \zeta, \ldots, \zeta^{k-1}) = D_{\Phi_m} = \prod_{1 \le i < j \le k} (\sigma_i(\zeta) - \sigma_j(\zeta))^2 = (-1)^{\binom{k}{2}} \prod_{i \ne j} (\sigma_i(\zeta) - \sigma_j(\zeta)).$$

Die Produktregel für $\Phi_m = \prod_{i=1}^k (X - \sigma_i(\zeta))$ liefert $\Phi'_m = \sum_i \prod_{j \ne i} (X - \sigma_j(\zeta))$ und

$$\sigma_l(\Phi'_m(\zeta)) = \Phi'_m(\sigma_l(\zeta)) = \prod_{j \ne l} (\sigma_l(\zeta) - \sigma_j(\zeta)),$$

für $l = 1, \ldots, k$. Mit der Norm-Abbildung $N\colon \mathbb{Q}_m \to \mathbb{Q}$, $x \mapsto \prod_{l=1}^k \sigma_l(x)$ folgt

$$D = (-1)^{\binom{k}{2}} \prod_{l=1}^k \sigma_l(\Phi'_m(\zeta)) = (-1)^{\binom{k}{2}} N(\Phi'_m(\zeta)).$$

Nach Beispiel I.12.10 ist $(1 - X^{p^{n-1}})\Phi_m = 1 - X^m$. Ableiten und Einsetzen von ζ ergibt

$$(1 - \gamma)\Phi'_m(\zeta) = -m\zeta^{m-1} = -m\zeta^{-1}$$

mit der primitiven p-ten Einheitswurzel $\gamma := \zeta^{p^{n-1}}$. Nun ist $N(-\zeta^{-1}) = N(-\zeta)^{-1} = \Phi_m(0) = 1$ und $N(1 - \gamma) = \Phi_p(1)^{p^{n-1}} = p^{p^{n-1}}$, da die Einschränkung $G \to \mathrm{Gal}(\mathbb{Q}_p|\mathbb{Q})$ surjektiv ist. Wegen $N(xy) = N(x)N(y)$ für $x, y \in \mathbb{Q}_n$ erhält man insgesamt

$$\begin{aligned} D &= (-1)^{\binom{k}{2}} N\Big(\frac{-m\zeta^{-1}}{1 - \gamma}\Big) = (-1)^{\binom{k}{2}} m^k p^{-p^{n-1}} \\ &= (-1)^{\binom{k}{2}} p^{np^{n-1}(p-1) - p^{n-1}} = (-1)^{\binom{k}{2}} p^{p^{n-1}(np-n-1)}. \end{aligned}$$

□

Bemerkung A.3.15. In der Situation von Lemma A.3.14 gilt $k = p^{n-1}(p-1) \equiv 0 \pmod 2$ außer im Fall $p^n = 2$. Dies zeigt

$$\begin{aligned} (-1)^{\binom{k}{2}} = (-1)^{\frac{k^2-k}{2}} = -1 &\iff k^2 - k \equiv 2 \pmod 4 \iff k \equiv 2 \pmod 4 \\ &\iff p \equiv 3 \pmod 4,\ n \equiv 1 \pmod 2. \end{aligned}$$

Lemma A.3.16. *Seien $\mathbb{Q} \subseteq K$ und $\mathbb{Q} \subseteq L$ Galois-Erweiterungen mit $K \cap L = \mathbb{Q}$. Seien $x_1, \ldots, x_n \in K$ und $y_1, \ldots, y_m \in L$ Ganzheitsbasen von K bzw. L mit teilerfremden Diskriminanten D_K und D_L. Dann ist $\{x_i y_j : i = 1, \ldots, n,\ j = 1, \ldots, m\}$ eine Ganzheitsbasis von KL mit Diskriminante $D_K^m D_L^n$.*

Beweis. Nach Satz I.10.15 ist $\mathbb{Q} \subseteq KL$ eine Galois-Erweiterung mit

$$G := \mathrm{Gal}(KL|\mathbb{Q}) = \mathrm{Gal}(KL|L) \times \mathrm{Gal}(KL|K) \cong \mathrm{Gal}(K|\mathbb{Q}) \times \mathrm{Gal}(L|\mathbb{Q}).$$

Mit $\mathrm{Gal}(KL|L) = \{\sigma_1, \ldots, \sigma_n\}$ und $\mathrm{Gal}(KL|K) = \{\tau_1, \ldots, \tau_m\}$ gilt $G = \{\sigma_i\tau_j : 1 \le i \le n, 1 \le j \le m\}$. Nach dem Beweis des Gradsatz ist außerdem $B := \{x_i y_j : 1 \le i \le n, 1 \le j \le m\}$ eine Basis von KL. Für $M_K := (\sigma_i(x_j))_{i,j}$ und $M_L := (\tau_i(y_j))_{i,j}$ ist das Kronecker-Produkt $M_K \otimes M_L$ die Matrix zur Diskriminante von B. Nach Aufgabe II.69 gilt

$$\det(M_K \otimes M_L)^2 = \det(M_K)^{2m} \det(M_L)^{2n} = D_K^m D_L^n.$$

Es bleibt zu zeigen, dass B eine Ganzheitsbasis ist. Sicher liegt B im Ganzheitsring $\mathbb{Z}_{KL}$. Sei umgekehrt $\alpha = \sum a_{ij} x_i y_j \in \mathbb{Z}_{KL}$ mit $a_{ij} \in \mathbb{Q}$ für alle i, j. Wir müssen $a_{ij} \in \mathbb{Z}$ zeigen. Für $j = 1, \dots, m$ sei $\beta_j := \sum_i a_{ij} x_i \in K$. Dann ist

$$M_L(\beta_j)_j = \Big(\sum_{j=1}^{m} \tau_i(y_j)\beta_j\Big)_i = \Big(\tau_i\Big(\sum_{j=1}^{m} \beta_j y_j\Big)\Big)_i = (\tau_1(\alpha), \dots, \tau_m(\alpha)) \in \mathbb{Z}_{KL}^m.$$

Für die zu M_L komplementäre Matrix $\widetilde{M_L} \in \mathbb{Z}_{KL}^{m \times m}$ gilt $\widetilde{M_L} M_L = \det(M_L) 1_m$ und $\det(M_L)\beta_i \in \mathbb{Z}_{KL}$. Wegen $\det(M_L)^2 = D_L$ ist auch $D_L \beta_i \in \mathbb{Z}_{KL} \cap K = \mathbb{Z}_K = \mathbb{Z}[x_1, \dots, x_n]$ für $i = 1, \dots, n$. Dies zeigt $D_L a_{ij} \in \mathbb{Z}$ für alle i, j. Analog gilt $D_K a_{ij} \in \mathbb{Z}$. Aus $\operatorname{ggT}(D_K, D_L) = 1$ erhält man $a_{ij} \in \mathbb{Z}$ wie gewünscht. □

Satz A.3.17. *Sei $n \in \mathbb{N}$ und $\zeta \in \mathbb{C}$ eine primitive n-te Einheitswurzel. Dann ist $1, \zeta, \dots, \zeta^{\varphi(n)-1}$ eine Ganzheitsbasis von $\mathbb{Q}_n$.*

Beweis. Sei $R := \mathbb{Z}_{\mathbb{Q}_n}$ und $k := \varphi(n)$.

Fall 1: $n = p^s$ mit $p \in \mathbb{P}$.
Sicher ist $\mathbb{Z}[\zeta] \subseteq R$. Sei umgekehrt $a := \sum_{i=0}^{k-1} a_i \zeta^i \in R$ mit $a_i \in \mathbb{Q}$. Sei $\operatorname{Gal}(\mathbb{Q}_n|\mathbb{Q}) = \{\sigma_1, \dots, \sigma_k\}$ und $\operatorname{tr}\colon \mathbb{Q}_n \to \mathbb{Q}$, $x \mapsto \sum_{i=1}^{k} \sigma_i(x)$ die Spur-Abbildung. Für $M := (\sigma_i(\zeta^{j-1}))_{1 \le i,j \le k}$ gilt

$$T := M^{\mathrm{t}} M = \Big(\sum_{l=1}^{k} \sigma_l(\zeta^{i-1})\sigma_l(\zeta^{j-1})\Big)_{i,j} = \big(\operatorname{tr}(\zeta^{i+j-2})\big)_{i,j}$$

und

$$T(a_i)_i = \Big(\sum_{l=0}^{k-1} \operatorname{tr}(\zeta^{i+l-1}) a_l\Big)_i = (\operatorname{tr}(\zeta^{i-1} a))_i \in \mathbb{Q}^k \cap R^k = \mathbb{Z}^k.$$

Durch Multiplikation mit der komplementären Matrix erhält man $\det(T) a_i \in \mathbb{Z}$ für $i = 0, \dots, k-1$ wie im Beweis von Lemma A.3.16. Andererseits ist $\det T = \det(M)^2 = D(1, \zeta, \dots, \zeta^{k-1})$ bis auf Vorzeichen eine p-Potenz nach Lemma A.3.14. Es genügt daher $pR \cap \mathbb{Z}[\zeta] \subseteq p\mathbb{Z}[\zeta]$ zu beweisen.

Für $i \in \mathbb{Z}$ mit $p \nmid i$ sei $\epsilon_i := \frac{1-\zeta^i}{1-\zeta} = \sum_{j=0}^{i-1} \zeta^j \in R$. Dann gilt

$$p \overset{I.12.10}{=} \Phi_n(1) = \prod_{\substack{1 \le i \le n \\ p \nmid i}} (1 - \zeta^i) = (1-\zeta)^k \prod_{\substack{1 \le i \le n \\ p \nmid i}} \epsilon_i.$$

Für $j \in \mathbb{N}$ mit $ij \equiv 1 \pmod{n}$ ist

$$\epsilon_i^{-1} = \frac{1-\zeta^{ij}}{1-\zeta^i} = \sum_{l=0}^{j-1} \zeta^{il} \in R.$$

Dies zeigt $\epsilon := \prod \epsilon_i \in R^\times$ und $p = \epsilon \lambda^k$ mit $\lambda := 1 - \zeta$. Offenbar ist $\mathbb{Z}[\lambda] \subseteq \mathbb{Z}[\zeta]$ und induktiv zeigt man $\mathbb{Z}[\zeta] \subseteq \mathbb{Z}[\lambda]$ (zum Beispiel ist $\zeta^2 = \lambda^2 - 2\lambda + 1$). Sei $a := \sum_{i=0}^{k-1} a_i \lambda^i \in pR \cap \mathbb{Z}[\lambda]$. Wir zeigen $p \mid a_i$ durch Induktion nach i. Wegen $\lambda \mid p \mid a$ ist $\lambda \mid a_0$ und $a_0 \in \lambda R \cap \mathbb{Z}$. Offenbar ist $p \in \lambda R \cap \mathbb{Z} \trianglelefteq \mathbb{Z}$. Im Fall $\mathbb{Z} \subseteq \lambda R$ wäre $R = \lambda R = \lambda^k R = pR$ und $1/p \in R$. Dieser Widerspruch zeigt $a_0 \in \lambda R \cap \mathbb{Z} = p\mathbb{Z}$. Ist die Behauptung für alle $i < k-1$ bereits bewiesen, so ist λ ein Teiler von $\epsilon \lambda^{k-i-1} = p/\lambda^{i+1}$ und damit auch von

$$\frac{1}{\lambda^{i+1}}\Big(a - \sum_{j=0}^{i} a_j \lambda^j\Big) = \sum_{j=i+1}^{k-1} a_j \lambda^{j-i-1}.$$

Es folgt $\lambda \mid a_{i+1}$ und $p \mid a_{i+1}$ wie oben. Insgesamt ist $a \in p\mathbb{Z}[\lambda] = p\mathbb{Z}[\zeta]$ wie behauptet.

Fall 2: $n \in \mathbb{N}$ beliebig.
Sei $n = p_1^{a_1} \dots p_l^{a_l}$ die Primfaktorzerlegung von n. Bekanntlich ist $\zeta_i := \zeta^{n/p_i^{a_i}}$ eine primitive $p_i^{a_i}$-te Einheitswurzel und $\mathbb{Q}_n = \mathbb{Q}(\zeta) = \mathbb{Q}(\zeta_1) \dots \mathbb{Q}(\zeta_l) = \mathbb{Q}_{p_1^{a_1}} \dots \mathbb{Q}_{p_l^{a_l}}$. Nach Satz I.12.14 ist außerdem $\mathbb{Q}(\zeta_1) \dots \mathbb{Q}(\zeta_{l-1}) \cap \mathbb{Q}(\zeta_l) = \mathbb{Q}$. Nach Fall 1 ist $1, \zeta_i, \dots, \zeta_i^{\varphi(p_i^{a_i})}$ eine Ganzheitsbasis von $\mathbb{Q}_{p_i^{a_i}}$. Nach Lemma A.3.14 sind die entsprechenden Diskriminanten für verschiedene p_i teilerfremd. Durch Induktion nach l erhält man aus Lemma A.3.16 eine Ganzheitsbasis von $\mathbb{Q}_n$ bestehend aus Potenzen von ζ. Für $s \geq k$ lässt sich $\zeta^s = \zeta^s - \zeta^{s-k}\Phi_n(\zeta)$ als $\mathbb{Z}$-Linearkombination kleinerer ζ-Potenzen ausdrücken. Daher ist $1, \zeta, \dots, \zeta^{k-1}$ bereits eine Ganzheitsbasis. □

Bemerkung A.3.18. Aus Lemma A.3.14 und Lemma A.3.16 kann man eine explizite (aber äußerst unübersichtliche) Formel für D_{Φ_n} gewinnen. Insbesondere haben n und D_{Φ_n} die gleichen Primteiler.

Satz A.3.19 (Kronecker)**.** *Sei $\alpha \in \mathbb{Z}[X] \setminus \{X\}$ irreduzibel. Für alle Nullstellen $x \in \mathbb{C}$ von α gelte $|x| \leq 1$. Dann ist α ein Kreisteilungspolynom.*

Beweis (Greiter). Die Nullstellen $x_1, \dots, x_n \in \mathbb{C}$ von α sind paarweise verschieden, da α irreduzibel ist (Satz I.11.20) und ungleich 0 wegen $\alpha \neq X$. Die Begleitmatrix $A \in \mathbb{Z}^{n \times n}$ von α hat Eigenwerte $x_1, \dots, x_n$ (Lemma II.10.4) und ist daher diagonalisierbar. Sei also $S = (s_{ij}) \in \mathrm{GL}(n, \mathbb{C})$ mit $SAS^{-1} = D = \mathrm{diag}(x_1, \dots, x_n)$ und $S^{-1} = (s'_{ij})$. Für $k \in \mathbb{N}$ ist der Eintrag von $A^k = S^{-1}D^kS$ an Position (i, j) beschränkt durch

$$\Big|\sum_{l=1}^{n} s'_{il} x_l^k s_{lj}\Big| \leq \sum_{l=1}^{n} |s'_{il} s_{lj}|.$$

Da die Matrizen A^k ganzzahlig sind, ist die Menge $\{A^k : k \in \mathbb{N}\}$ endlich. Also existieren $k < l$ mit $A^k = A^l$ und $A^{l-k} = 1 = D^{l-k}$. Dies zeigt $x_i^{l-k} = 1$ für $i = 1, \dots, n$. Als irreduzibler Teiler von $X^{l-k} - 1$ muss α ein Kreisteilungspolynom sein. □

Satz A.3.20. *Mit den Bezeichnungen aus Satz III.10.57 ist*

$$\mathbb{F}_q C_n \cong \bigtimes_{d \mid m} \bigtimes_{i=1}^{\varphi(d)/\mathrm{ord}_d(q)} \mathbb{F}_q[X]/(\Phi_{d,i})^{p^k}$$

die Peirce-Zerlegung von $\mathbb{F}_q C_n$. Für $d \mid m$ gibt es $\varphi(d)/\mathrm{ord}_d(q)$ nicht-isomorphe einfache $\mathbb{F}_q C_n$-Moduln der Dimension $\mathrm{ord}_d(q)$ (über $\mathbb{F}_q$). Die entsprechenden projektiv-unzerlegbaren Moduln haben Dimension $\mathrm{ord}_d(q)^{p^k}$.

Beweis. Für $G = \langle x \rangle \cong C_n$ ist die Abbildung $\mathbb{F}_q[X] \to \mathbb{F}_q G$, $X \mapsto g$ ein Ringepimorphismus mit Kern $(X^n - 1)$. Aus dem chinesischen Restsatz für Ringe folgt mit Satz III.10.57 die angegebene Zerlegung (vgl. Aufgabe II.63). Sei $R := \mathbb{F}_q[X]/(\Phi_{d,i})^{p^k}$. Nach dem zweiten Isomorphiesatz ist $M_{d,i} := \mathbb{F}_q[X]/(\Phi_{d,i})$ ein einfacher R-Modul. Außerdem ist

$$\begin{aligned} M_{d,i} &\to (\Phi_{d,i})^a/(\Phi_{d,i})^{a+1}, \\ \alpha + (\Phi_{d,i}) &\mapsto \alpha\Phi_{d,i}^a + (\Phi_{d,i})^{a+1} \end{aligned}$$

ein Isomorphismus von R-Moduln für $a = 1, \dots, p^k - 1$. Die Kompositionsfaktoren des regulären R-Moduls sind daher isomorph. Nach Satz II.8.25 muss R ein Block von $\mathbb{F}_q C_n$ sein. Die $\mathbb{F}_q C_n$-Untermoduln

von R haben die Form $(\Phi_{d,i})^a/(\Phi_{d,i})^{p^k}$. Insbesondere ist R projektiv-unzerlegbar. Die Dimensionen ergeben sich aus den Graden der $\Phi_{d,i}$. □

Beispiel A.3.21. Im Fall $n \mid q-1$ haben alle irreduziblen Darstellungen von C_n über $\mathbb{F}_q$ Grad 1 (wie über $\mathbb{C}$).

Folgerung A.3.22. *Sei $n \in \mathbb{N}$ und $q \neq 1$ eine Primzahlpotenz. Genau dann ist Φ_n irreduzibel in $\mathbb{F}_q[X]$, wenn $g := \mathrm{ggT}(n, q^2) \leq 2$ und $|\langle q + \frac{n}{g}\mathbb{Z}\rangle| = \varphi(n)$.*

Beweis. Im Fall $g = 1$ folgt die Behauptung aus Satz III.10.57. Im Fall $g = 2$ ist $n = 2m$ mit $2 \nmid m$. Dann gilt $\Phi_n = \Phi_m(-X) = \Phi_m$ in $\mathbb{F}_2[X] \subseteq \mathbb{F}_q[X]$. Wieder gilt die Behauptung nach Satz III.10.57. Sei nun $g > 2$ und $n = p^k m$ mit $p \mid q$ und $p \nmid m$. Dann gilt

$$\Phi_n \mid X^n - 1 = \prod_{d \mid m} \Phi_d^{p^k}.$$

Für $d \mid n$ ist $\varphi(d) \leq \varphi(n)$ nach Aufgabe I.51. Wegen

$$\deg \Phi_n = \varphi(n) = \varphi(p^k)\varphi(m) > \varphi(m) \geq \varphi(d) = \deg \Phi_d$$

kann Φ_n nicht irreduzibel sein. □

Beispiel A.3.23.

(i) Die Bedingung in Folgerung A.3.22 impliziert, dass Φ_n nur dann irreduzibel in $\mathbb{F}_q[X]$ sein kann, wenn $(\mathbb{Z}/n\mathbb{Z})^\times$ zyklisch ist. Nach Folgerung I.8.35 muss n dafür die Form $4, p^k, 2p^k$ für eine ungerade Primzahl p haben. Daher ist Φ_{12} reduzibel modulo p für jede Primzahl p (vgl. Beispiel I.8.57).

(ii) Für $q = 2$ gilt

$$\begin{aligned}\Phi_{21} &= \frac{X^{21}-1}{\Phi_1\Phi_3\Phi_7} = \frac{X^{21}-1}{(X-1)(X^2+X+1)(X^6+\ldots+1)} \\ &= X^{12}+X^{11}+X^9+X^8+X^6+X^4+X^3+X+1 = \Phi_{21,1}\Phi_{21,2} \\ &= (X^6+X^4+X^2+X+1)(X^6+X^5+X^4+X^2+1) \in \mathbb{F}_2[X].\end{aligned}$$

Lemma A.3.24. *Für $n \in \mathbb{N}$ gilt*

$$\boxed{\Phi_n = \prod_{d \mid n} (X^{n/d} - 1)^{\mu(d)}}$$

mit der Möbius-Funktion μ.

Beweis. Die Möbius-Inversion Satz I.2.42 gilt auch, wenn man $(\mathbb{C}, +)$ durch die abelsche Gruppe $(\mathbb{Q}(X)^\times, \cdot)$ ersetzt (gleicher Beweis). Für $f(n) := \Phi_n$ gilt $F(n) = \prod_{d \mid n} f(d) = X^n - 1$. Dies zeigt die Behauptung. □

Bemerkung A.3.25.

(i) Ist $n = p_1^{a_1} \dots p_s^{a_s}$ die Primfaktorzerlegung von $n \in \mathbb{N}$ und $q := p_1 \dots p_s$, so gilt

$$\Phi_n = \prod_{d|n} (X^{\frac{n}{d}} - 1)^{\mu(d)} = \prod_{d|q} \big((X^{\frac{n}{q}})^{\frac{q}{d}} - 1\big)^{\mu(d)} = \Phi_q(X^{\frac{n}{q}})$$

nach Lemma A.3.24. Dies reduziert die Berechnung von Φ_n auf quadratfreie n. Für $p \in \mathbb{P}$ mit $p \nmid n$ gilt

$$\Phi_{pn} = \prod_{d|n} (X^{\frac{pn}{d}} - 1)^{\mu(d)} (X^{\frac{pn}{pd}} - 1)^{\mu(pd)} = \prod_{d|n} \frac{\big((X^p)^{\frac{n}{d}} - 1\big)^{\mu(d)}}{(X^{\frac{n}{d}} - 1)^{\mu(d)}} = \frac{\Phi_n(X^p)}{\Phi_n}.$$

Schließlich ist $\Phi_p = X^{p-1} + X^{p-2} + \ldots + 1$ für $p \in \mathbb{P}$.

(ii) Berechnet man $\Phi_1, \Phi_2, \ldots, \Phi_{104}$, so stellt man fest, dass alle Koeffizienten 0 oder ± 1 sind. Überraschenderweise ist dies im Allgemeinen falsch.

Satz A.3.26 (Suzuki)**.** *Jede ganze Zahl ist Koeffizient eines Kreisteilungspolynoms.*

Beweis. Sei $s > 2$ ungerade. Für genügend große $m \in \mathbb{N}$ existieren nach Tschebyschow[1] Primzahlen $p_1 < \ldots < p_s$ zwischen m und $2m$. Insbesondere gilt $p_1 + p_2 > 2m \geq p_s$. Sei $n := p_1 \dots p_s$. Jeder Teiler von n hat die Form $d = p_{i_1} \dots p_{i_k}$ mit $k \geq 0$. Im Fall $k < s - 1$ ist

$$(X^{n/d} - 1)^{\mu(d)} \equiv -1 \pmod{X^{p_s+1}}.$$

Die Anzahl der Teiler mit $k < s - 1$ beträgt $2^s - s - 1 \equiv 0 \pmod 2$. Mit Lemma A.3.24 folgt

$$(X-1)\Phi_n \equiv \prod_{i=1}^{s} (X^{p_i} - 1) \equiv X^{p_1} + \ldots + X^{p_s} - 1 \pmod{X^{p_s+1}}.$$

Nun ist $(X-1)(X^{p_s} + X^{p_s-1} + \ldots + X + 1) = X^{p_s+1} - 1 \equiv -1 \pmod{X^{p_s+1}}$ und man erhält

$$\begin{aligned} \Phi_n &\equiv -(X^{p_1} + \ldots + X^{p_s} - 1)(X^{p_s} + X^{p_s-1} + \ldots + X + 1) \\ &\equiv (1-s)X^{p_s} + (2-s)X^{p_s-1} + (2-s)X^{p_s-2} + \ldots \pmod{X^{p_s+1}}, \end{aligned}$$

denn $p_{s-1} \leq p_s - 2$. Also sind bereits $-1, -2, \ldots$ Koeffizienten von Kreisteilungspolynomen. Wir können sicherlich $p_1 > 2$ annehmen, sodass n ungerade ist. Seien $\zeta_1, \ldots, \zeta_t \in \mathbb{C}$ die primitiven n-ten Einheitswurzeln mit $t = \varphi(n) \equiv 0 \pmod 2$. Dann sind $-\zeta_1, \ldots, -\zeta_t$ die primitiven $2n$-ten Einheitswurzeln. Also gilt

$$\begin{aligned} \Phi_{2n} &= \prod_{i=1}^{t} (X + \zeta_i) = (-1)^t \prod_{i=1}^{t} (-X - \zeta_i) = \Phi_n(-X) \\ &\equiv (s-1)X^{p_s} + (2-s)X^{p_s-1} + (s-2)X^{p_s-2} + \ldots \pmod{X^{p_s+1}}. \end{aligned}$$

Also sind auch $1, 2, \ldots$ Koeffizienten von Kreisteilungspolynomen. Schließlich ist 0 ein Koeffizient von $\Phi_4 = X^2 + 1$. □

[1] Siehe Zahlentheorie-Skript

Definition A.3.27. Seien $a, n \in \mathbb{N} \setminus \{1\}$. Eine Primzahl p heißt *Zsigmondy-Primzahl* bzgl. a^n, falls $p \mid a^n - 1$ und $p \nmid a^k - 1$ für $k = 1, \ldots, n-1$. Dies bedeutet, dass a die multiplikative Ordnung n modulo p hat.

Lemma A.3.28. *Sei $n = p^s m \in \mathbb{N}$ mit $p \in \mathbb{P}$ und $s \geq 1$. Dann gilt $\Phi_n(a) > a^{p^{s-1}(p-2)}$ für $a \in \mathbb{N} \setminus \{1\}$.*

Beweis. Wegen $s \geq 1$ ist $n \geq p \geq 2$. Sei $\zeta = e^{2\pi \mathrm{i}/n} \in \mathbb{C}$. Dann gilt zunächst

$$\Phi_n(a) = \prod_{\substack{1 \leq k \leq n \\ \mathrm{ggT}(n,k)=1}} (a - \zeta^k) = \prod_{\substack{1 \leq k \leq n/2 \\ \mathrm{ggT}(n,k)=1}} |a - \zeta^k|^2 > 0.$$

Für $b := a^{p^{s-1}}$ gilt $b^p - 1 \geq b^{p-2}(b^2 - 1)$. Wie in Bemerkung A.3.25 folgt

$$\begin{aligned}\Phi_n(a) &= \prod_{d \mid m} \frac{(a^{n/d} - 1)^{\mu(d)}}{(a^{n/(pd)} - 1)^{\mu(d)}} = \frac{\Phi_m(a^{p^s})}{\Phi_m(a^{p^{s-1}})} = \frac{\Phi_m(b^p)}{\Phi_m(b)} = \prod_{\mathrm{ggT}(k,m)=1} \frac{|b^p - \zeta^k|}{|b - \zeta^k|} \\ &> \Big(\frac{b^p - 1}{b+1}\Big)^{\varphi(m)} \geq (b^{p-2}(b-1))^{\varphi(m)} \geq b^{p-2}.\end{aligned}$$

□

Lemma A.3.29. *Seien $a, n \geq 2$. Sei p ein Primteiler von $\Phi_n(a)$ und $n = p^s m$ mit $p \nmid m$ sowie $s \geq 0$.*

(i) Genau dann ist p eine Zsigmondy-Primzahl bzgl. a^n, wenn $s = 0$.

(ii) Ist $s \geq 1$, so ist $m \mid p - 1$. Insbesondere ist p dann der größte Primteiler von n.

(iii) Ist $s \geq 1$ und $p^2 \mid \Phi_n(a)$, so ist $p = n = 2$.

Beweis.

(i) Im Fall $s \geq 1$ ist $1 \equiv a^n \equiv (a^p)^{n/p} \equiv a^{n/p}$ nach Fermat. Also ist p keine Zsigmondy-Primzahl. Nehmen wir nun umgekehrt an, dass p keine Zsigmondy-Primzahl ist. Dann muss die Ordnung von a modulo p ein echter Teiler von n sein. Insbesondere existiert ein Primteiler q von n mit $a^{n/q} \equiv 1 \pmod{p}$. Sei $c := a^{n/q}$. Aus $\Phi_n(a) \mid \frac{a^n - 1}{a^{n/q} - 1}$ folgt

$$0 \equiv \Phi_n(a) \equiv \frac{a^n - 1}{a^{n/q} - 1} \equiv \frac{c^q - 1}{c - 1} = 1 + c + \ldots + c^{q-1} \equiv q \pmod{p},$$

d. h. $p = q \mid n$.

(ii) Das obige Argument zeigt, dass die Ordnung von a modulo p die Form n/p^t mit $t \geq 1$ hat. Damit ist $\frac{n}{p^t} \mid p - 1$, also $s = t$ und $m \mid p - 1$.

(iii) Sei zunächst $p > 2$ und $d := c - 1 = a^{n/p} - 1$. Dann gilt $p \mid d$ und

$$\frac{a^n - 1}{a^{n/p} - 1} = \frac{(1+d)^p - 1}{d} = p + \sum_{k=2}^{p} \binom{p}{k} d^{k-1} \equiv p \pmod{p^2}.$$

Also ist $p^2 \nmid \Phi_n(a)$. Sei nun $p = 2$ und $n > 2$. Dann ist $n = 2^s$ nach (ii) und a ist ungerade wegen $2 = p \mid a^n - 1$. Wie oben folgt

$$\frac{a^n - 1}{a^{n/p} - 1} = \frac{c^2 - 1}{c - 1} = c + 1 = a^{2^{s-1}} + 1 \equiv 2 \pmod{4}.$$

Dies zeigt $4 \nmid \Phi_n(a)$. □

Satz A.3.30 (ZSIGMONDY)**.** *Für $a, n \geq 2$ existiert stets eine Zsigmondy-Primzahl bzgl. a^n außer in den folgenden Fällen:*

(i) $n = 2$, $a = 2^k - 1$ *für* $k \geq 2$.

(ii) $n = 6$, $a = 2$.

Beweis. Besitzt $\Phi_n(a)$ mehr als einen Primteiler, so existiert eine Zsigmondy-Primzahl nach Lemma A.3.29. Sei also $\Phi_n(a) = p^k$, wobei p der größte Primteiler von n ist. Für $n = 2$ ist $p = 2$ und $2^k = \Phi_2(a) = a + 1$. Sei also $n \geq 3$. Nach Lemma A.3.29 ist $\Phi_n(a) = p$. Im Fall $p = 2$ wäre $n = 2^s \geq 4$ und $\Phi_n(a) = a^{2^{s-1}} + 1 > 2 = p$. Also ist $p > 2$ und $n = p^s m$ mit $m \mid p - 1$. Nach Lemma A.3.28 gilt

$$p = \Phi_n(a) > a^{p^{s-1}(p-2)} \geq 2^{p-2} = 2^{p-3} + 2^{p-4} + \ldots + 1 + 1 \geq p - 1.$$

Dies liefert $p = 3$, $a = 2$ und $s = 1$. Also ist $n \in \{3, 6\}$. Für $a^n = 2^3$ ist 7 eine Zsigmondy-Primzahl. Somit bleibt nur der Ausnahmefall $n = 6$. □

Bemerkung A.3.31.

(i) Für $n = 2$ und $a = 2^k - 1$ ist

$$a^n - 1 = 2^{2k} - 2^{k+1} = 2^k(a - 1)$$

und es gibt keine Zsigmondy-Primzahl. Das Gleiche gilt für $(n, a) = (6, 2)$ wegen $2^6 - 1 = 63 = 3^2 \cdot 7 = (2^2 - 1)^2(2^3 - 1)$.

(ii) Sei $q > 1$ eine Primzahlpotenz. Bekanntlich ist $q^n - 1$ ein Teiler von $|\mathrm{GL}(n, q)|$. Mit Zsigmondy und Cauchy kann man also auf die Existenz von invertierbaren Matrizen mit „großer“ Primzahlordnung schließen.

4 Frobenius-Normalform ohne Moduln

Bemerkung A.4.1.

(i) Die meisten Bücher zur Linearen Algebra verzichten auf die Frobenius-Normalform von Matrizen, obwohl man diese auch mit elementaren Mitteln beweisen kann. Ein solcher Zugang wird in diesem Abschnitt vorgestellt.

(ii) Im Folgenden sei V stets ein endlich-dimensionaler Vektorraum über einem beliebigen Körper K. Für $f \in \mathrm{End}(V)$ sei χ_f das charakteristische Polynom und μ_f das Minimalpolynom von f. Nach Cayley-Hamilton gilt $\mu_f \mid \chi_f$.

(iii) Für einen f-invarianten Unterraum $U \leq V$ ist das Minimalpolynom der Einschränkung $f_{|U}$ ein Teiler von μ_f. Außerdem operiert f auch auf V/U und das entsprechende Minimalpolynom teilt ebenfalls μ_f. Im Fall $U = \langle f^i(v) : i \geq 0\rangle$ für ein festes $v \in V$ bezeichnen wir das Minimalpolynom von $f_{|U}$ mit μ_v.

Satz A.4.2. *Sei $f \in \mathrm{End}(V)$ und $\mu_f = \gamma_1^{a_1} \dots \gamma_k^{a_k}$ die Primfaktorzerlegung von μ_f in $K[X]$. Dann ist*

$$V = \mathrm{Ker}\big(\gamma_1^{a_1}(f)\big) \oplus \ldots \oplus \mathrm{Ker}\big(\gamma_k^{a_k}(f)\big)$$

eine Zerlegung in f-invariante Unterräume. Außerdem ist $\gamma_i^{a_i}$ das Minimalpolynom der Einschränkung von f auf $\mathrm{Ker}\big(\gamma_i^{a_i}(f)\big)$.

Beweis. O. B. d. A. sei $k \geq 2$. Sei $\mu_f = \alpha\beta$ mit normierten, teilerfremden $\alpha, \beta \in K[X] \setminus K$ (zum Beispiel $\alpha = \gamma_1^{a_1}$ und $\beta = \gamma_2^{a_2} \dots \gamma_k^{a_k}$). Sei $V_\alpha := \mathrm{Ker}(\alpha(f))$ und $V_\beta := \mathrm{Ker}(\beta(f))$. Nach Folgerung I.8.21 existieren $\tilde{\alpha}, \tilde{\beta} \in K[X]$ mit $\alpha\tilde{\alpha} + \beta\tilde{\beta} = 1$. Dann ist

$$V = (\alpha\tilde{\alpha} + \beta\tilde{\beta})(f)(V) \subseteq \alpha(f)(V) + \beta(f)(V) \subseteq V_\beta + V_\alpha.$$

Für $v \in V_\alpha \cap V_\beta$ ist andererseits

$$v = \tilde{\alpha}(f)\big(\alpha(f)(v)\big) + \tilde{\beta}(f)\big(\beta(f)(v)\big) = 0.$$

Dies zeigt $V = V_\alpha \oplus V_\beta$. Für $v \in V_\alpha$ gilt $\alpha(f)\big(f(v)\big) = f\big(\alpha(f)(v)\big) = 0$, d. h. V_α ist f-invariant (analog V_β). Das Minimalpolynom α_1 der Einschränkung $f_{|V_\alpha}$ teilt α. Genauso ist β durch das Minimalpolynom β_1 von $f_{|V_\beta}$ teilbar. Wegen $V = V_\alpha \oplus V_\beta$ gilt andererseits $(\alpha_1\beta_1)(f) = 0$ und $\mu_f \mid \alpha_1\beta_1$. Dies zeigt $\alpha_1 = \alpha$ sowie $\beta_1 = \beta$. Die Behauptung ergibt sich nun durch Induktion nach k. □

Bemerkung A.4.3. Wählt man in der Situation von Satz A.4.2 eine geeignete Basis, so hat die Matrix von f Blockdiagonalform.

Lemma A.4.4. *Für $f \in \mathrm{End}(V)$ existiert ein $v \in V$ mit $\mu_v = \mu_f$.*

Beweis. Sei $V_i := \operatorname{Ker}(\gamma_i^{a_i}(f))$ wie in Satz A.4.2. Für $v \in V_i$ ist μ_v ein Teiler von $\gamma_i^{a_i}$ nach Bemerkung A.4.1. Da $\gamma_i^{a_i}$ das Minimalpolynom von $f_{|V_i}$ ist, muss ein $v_i \in V_i$ mit $\mu_{v_i} = \gamma_i^{a_i}$ existieren. Wir setzen $v := v_1 + \ldots + v_k$. Da V_i f-invariant ist, gilt $\mu_v(f)(v_i) = 0$ für $i = 1, \ldots, k$. Dies zeigt $\mu_i^{a_i} = \mu_{v_i} \mid \mu_v$ und es folgt $\mu_v = \mu_f$. □

Bemerkung A.4.5. Sei $\alpha \in K[X] \setminus K$ normiert vom Grad n und $B := B_\alpha$ die Begleitmatrix von α. Für $v := (1, 0, \ldots, 0)^{\mathrm{t}} \in K^n$ ist $v, Bv, \ldots, B^{n-1}v$ die Standardbasis von K^n. Daher gilt $\deg \mu_B \geq \deg \mu_v \geq n$. Nach Cayley-Hamilton ist andererseits $\deg \mu_B \leq n$. Lemma II.10.4 zeigt $\mu_B = \chi_B = \alpha$.

Lemma A.4.6. *Für $k \in \mathbb{N}$ und jedes normierte Polynom $\alpha \in K[X] \setminus K$ ist*

$$\begin{pmatrix} J_k(0) & & 0 \\ & \ddots & \\ 0 & & J_k(0) \end{pmatrix}$$

die Jordansche Normalform von $\alpha(B_{\alpha^k})$.

Beweis. Sei $n := \deg(\alpha^k) = k \deg \alpha = kd$. Für $A := B_{\alpha^k}$ und $N := \alpha(A)$ gilt $N^k = \alpha^k(A) = 0$ nach Bemerkung A.4.5. Daher besitzt N eine Jordansche Normalform J und diese besteht aus Blöcken der Form $J_l(0)$ mit $l \leq k$. Nach Lemma A.4.4 existiert $v \in K^n$ mit $\mu_v = \mu_A$, d. h. die Vektoren $v, Av, \ldots, A^{n-1}v$ sind linear unabhängig. Wegen $\deg(\alpha X^i) = d + i$ sind auch $Nv, NAv, \ldots, NA^{n-d-1}v$ linear unabhängig und zusätzlich im Bild von N. Dies zeigt $\operatorname{rk} N \geq n - d$ und $\dim \operatorname{Ker}(N) \leq d$ nach dem Rangsatz. Somit besitzt J höchstens d Jordanblöcke. Diese müssen folglich alle die Größe $k \times k$ haben. □

Satz A.4.7. *Für jede Matrix $A \in K^{n \times n}$ gilt:*

(i) Es existieren eindeutig bestimmte normierte Polynome $\alpha_1, \ldots, \alpha_k \in K[X] \setminus K$ mit $\alpha_k \mid \ldots \mid \alpha_1$, sodass A zu

$$\begin{pmatrix} B_{\alpha_1} & & 0 \\ & \ddots & \\ 0 & & B_{\alpha_k} \end{pmatrix} \qquad \text{(Frobenius-Normalform)}$$

ähnlich ist. Dabei ist $\mu_A = \alpha_1$ und $\chi_A = \alpha_1 \ldots \alpha_k$.

(ii) Es existieren irreduzible Polynome $\gamma_1, \ldots, \gamma_s \in K[X]$ und $a_1, \ldots, a_s \in \mathbb{N}$, sodass A zu

$$\begin{pmatrix} B_{\gamma_1^{a_1}} & & 0 \\ & \ddots & \\ 0 & & B_{\gamma_s^{a_s}} \end{pmatrix} \qquad \text{(Weierstrass-Normalform)}$$

ähnlich ist. Dabei sind die Potenzen $\gamma_1^{a_1}, \ldots, \gamma_s^{a_s}$ bis auf die Reihenfolge eindeutig bestimmt und $\chi_A = \gamma_1^{a_1} \ldots \gamma_s^{a_s}$.

Beweis. Sei $V = K^n$ und $f \in \operatorname{End}(V)$ mit $f(v) = Av$ für $v \in V$. Nach Lemma A.4.4 existiert $v \in V$ mit $\mu_v = \mu_f$. Wir setzen $U := \langle f^i(v) : i \geq 0 \rangle \leq V$. Die Matrix von $f_{|U}$ bzgl. $v, f(v), \ldots, f^{d-1}(v)$ ist dann B_{μ_f}.

Nehmen wir nun induktiv an, dass f-invariante Räume $U_i := \langle f^j(u_i) : j \geq 0 \rangle \leq V$ mit $U := U_1 \oplus \ldots \oplus U_l \leq V$ gegeben sind. Die Matrix von $f_{|U_i}$ sei B_{α_i} und α_i sei das Minimalpolynom von f auf $V/(U_1 + \ldots + U_{i-1})$ für $i = 1, \ldots, l$. Sicher ist dann $\alpha_l \mid \ldots \mid \alpha_1 = \mu_f$.

Sei $\alpha = \alpha_{l+1}$ das Minimalpolynom von f auf V/U. Offenbar ist $\alpha \mid \alpha_l$, sagen wir $\alpha_l = \alpha\gamma$ mit $\gamma \in K[X]$. Nach Lemma A.4.4 existiert $v \in V$ mit $\mu_{v+U} = \alpha$. Es existieren $\beta_1, \ldots, \beta_l \in K[X]$ mit

$$\alpha(f)v = \beta_1(f)u_1 + \ldots + \beta_l(f)u_l.$$

Multiplikation mit $\gamma(f)$ impliziert

$$U_1 + \ldots + U_{l-1} \ni \alpha_l(f)v = \gamma(f)\alpha(f)v = \gamma(f)\beta_1(f)u_1 + \ldots + \gamma(f)\beta_l(f)u_l$$

und $(\gamma\beta_l)(f)u_l = 0$. Dies zeigt $\gamma\alpha = \alpha_l \mid \gamma\beta_l$ und $\alpha \mid \beta_l$. Sei also $\beta_l = \alpha\delta$ für ein $\delta \in K[X]$. Nachdem wir v durch $v - \delta(f)u_l \in v + U$ ersetzt haben, gilt

$$\alpha(f)v = \beta_1(f)u_1 + \ldots + \beta_{l-1}(f)u_{l-1}.$$

Wir können diesen Prozess mit $i = l-1, \ldots, 1$ wiederholen und gelangen schließlich zu $\alpha(f)v = 0$ ohne die Nebenklasse $v+U$ zu verändern. Wir definieren $U_{l+1} := \langle f^i(f)v : i \geq 0\rangle \leq V$. Für $w = \beta(f)v \in U_{l+1} \cap U$ mit $\beta \in K[X]$ gilt $w + U = 0$ und $\alpha \mid \beta$ wegen $\mu_{v+U} = \alpha$. Dies zeigt $w = 0$ und $U + U_{l+1} = U \oplus U_{l+1}$. Die Matrix von $f_{|U_{l+1}}$ ist B_α. Die Existenz einer Frobenius-Normalform folgt jetzt durch Induktion nach $\dim V$.

Für die Eindeutigkeit konstruieren wir zunächst die Weierstraß-Normalform. Dafür zerlegen wir

$$V = \operatorname{Ker}\big(\gamma_1^{c_1}(f)\big) \oplus \ldots \oplus \operatorname{Ker}\big(\gamma_l^{c_l}(f)\big)$$

gemäß Satz A.4.2. Sei f_i die Einschränkung von f auf $\operatorname{Ker}\big(\gamma_i^{c_i}(f)\big)$. Dann ist $\mu_{f_i} = \gamma_i^{c_i}$. Die Frobenius-Normalform von f_i besteht also aus Blöcken der Form $B_{\gamma_i^a}$, wobei $a \leq c_i$. Die Anzahl dieser Blöcke ergibt sich mittels Lemma A.4.6 aus der (eindeutigen) Anzahl der Jordanblöcke $J_a(0)$ von $\gamma_i(f_i)$. Insgesamt erhält man daraus die eindeutige Weierstraß-Normalform von f.

Wir betrachten schließlich die f-invariante Zerlegung $V = U_1 \oplus \ldots \oplus U_k$ einer Frobenius-Normalform von f wie oben. Sei $\alpha_i = \gamma_{i1}^{a_{i1}} \ldots \gamma_{is}^{a_{is}}$ die Primfaktorzerlegung des Minimalpolynoms von $f_{|U_i}$. In der Weierstraß-Normalform von $f_{|U_i}$ müssen dann die Blöcke $B_{\gamma_{ij}^{a_{ij}}}$ mit $j = 1, \ldots, s$ auftreten. Da α_i auch das charakteristische Polynom von $f_{|U_i}$ ist, können auch keine weiteren Blöcke auftreten. Zusammen ergeben alle $B_{\gamma_{ij}^{a_{ij}}}$ die eindeutige Weierstraß-Normalform von f. Auf diese Weise sind auch $\alpha_1, \ldots, \alpha_k$ eindeutig bestimmt. □

5 Analytischer Beweis des Fundamentalsatz der Algebra

Bemerkung A.5.1. Wir haben den Fundamentalsatz der Algebra in Satz I.13.7 mit möglichst wenig Analysis bewiesen (der Zwischenwertsatz für reelle Polynome wurde benutzt). Wir führen nun einen kürzeren Beweis, der etwas mehr Analysis benutzt (aber ohne Funktionentheorie auskommt).

Satz A.5.2. *Jedes nicht-konstante Polynom $\alpha \in \mathbb{C}[X]$ besitzt eine Nullstelle.*

Beweis (Argand). Angenommen α besitzt keine Nullstelle. Da α nicht konstant ist, existiert ein $r > 0$ mit $|\alpha(x)| > |\alpha(0)|$ für alle $x \in \mathbb{C}$ mit $|x| > r$. Die stetige Funktion $\mathbb{C} \to \mathbb{R}$, $x \mapsto |\alpha(x)|$ (wobei man $\mathbb{C}$ als $\mathbb{R}^2$ auffasst) nimmt daher ihr Minimum auf der kompakten Menge $\{x \in \mathbb{C} : |x| \leq r\}$ an. Sei $|\alpha(x_0)| > 0$ dieses Minimum. Indem man α durch $\alpha(x_0)^{-1}\alpha(X + x_0)$ ersetzt, kann man $x_0 := 0$ und $\alpha(0) = 1$ annehmen. Sei $k \in \mathbb{N}$ mit $\alpha = 1 + aX^k + X^{k+1}\beta$ für $a \in \mathbb{C}^\times$ und $\beta \in \mathbb{C}[X]$. Sei $z \in \mathbb{C}$ eine k-te Wurzel aus $-a^{-1}$. Indem wir α durch $\alpha(zX)$ ersetzten, können wir $a = -1$ annehmen. Da auch $x \mapsto |\beta(x)|$ stetig ist (möglicherweise ist $\beta = 0$), existiert ein $0 < t < 1$ mit $t|\beta(t)| < 1$. Dann erhält man den Widerspruch

$$|\alpha(t)| \leq 1 - t^k + t^k t|\beta(t)| < 1. \qquad \square$$

Bemerkung A.5.3. In der linearen Algebra 1 beweist man den Spektralsatz für symmetrische Matrizen üblicherweise, indem man den Fundamentalsatz der Algebra für die Existenz von Eigenwerten benutzt. Dies ist ungünstig, da der Spektralsatz selbst keine komplexen Zahlen benötigt. Der folgende Beweis umgeht dieses Problem.

Satz A.5.4. *Jede symmetrische Matrix $A \in \mathbb{R}^n$ besitzt einen reellen Eigenwert.*

Beweis (Geck). Sei

$$\mu(A) := \inf\{v^{\mathrm{t}} A v : v \in \mathbb{R}^n,\ |v| = 1\}$$

und $B := A - \mu(A)1_n$. Für alle $v \in \mathbb{R}^n$ gilt $v^{\mathrm{t}} B v \geq 0$, d. h. B ist positiv semidefinit. Nehmen wir an, dass B sogar positiv definit ist. Mit dem Gram-Schmidt-Verfahren findet man eine Matrix $S \in \mathrm{GL}(n, \mathbb{R})$ mit $B = S^{\mathrm{t}} S$ (Sylvesters Trägheitssatz). Nach Definition von $\mu(A)$ existiert eine Folge normierter Vektoren $v_1, v_2, \ldots \in \mathbb{R}^n$ mit

$$\lim_{i\to\infty} |Sv_i|^2 = \lim_{i\to\infty} v_i^{\mathrm{t}} B v_i = 0.$$

Nun muss auch jede Koordinate von Sv_i gegen Null streben mit $i \to \infty$. Mit der Dreiecksungleichung erhält man den Widerspruch

$$1 = \lim_{i\to\infty} |v_i| = \lim_{i\to\infty} |S^{-1} S v_i| = 0.$$

Also ist $\det(B) = 0$ und es existiert ein $v \in \mathbb{R}^n$ mit $Bv = 0$. Nun ist v ein Eigenvektor von A zum Eigenwert $\mu(A)$. $\square$

6 Transzendente Erweiterungen

Definition A.6.1. Eine Körpererweiterung $K \subseteq L$ heißt *endlich erzeugt*, falls $x_1, \ldots, x_n \in L$ (nicht notwendig algebraisch) mit $L = K(x_1, \ldots, x_n)$ existieren.

Satz A.6.2. *Seien $K \subseteq M \subseteq L$ Körpererweiterungen. Ist L über K endlich erzeugt, so auch M.*

Beweis. Jedes endliche Erzeugendensystem von L enthält eine Transzendenzbasis von L über K. Für eine Transzendenzbasis T von M über K gilt dann $|T| = \operatorname{trg}(M|K) \leq \operatorname{trg}(L|K) < \infty$. Indem wir K durch $K(T)$ ersetzen, können wir annehmen, dass M algebraisch über K ist (sicher ist L dann immer noch endlich erzeugt). Sei B eine Transzendenzbasis von L über K. Wegen $|L : K(B)| < \infty$ genügt es $|M : K| \leq |L : K(B)|$ zu zeigen. Wegen

$$\begin{aligned}\operatorname{trg}(M(B)|M) &= \operatorname{trg}(M(B)|M) + \operatorname{trg}(M|K) = \operatorname{trg}(M(B)|K)\\ &= \operatorname{trg}(M(B)|K(B)) + \operatorname{trg}(K(B)|K) = \operatorname{trg}(K(B)|K) = |B|\end{aligned}$$

ist B algebraisch unabhängig über M. Seien $a_1, \ldots, a_n \in M$ linear unabhängig über K und $\sum_{i=1}^n \lambda_i a_i = 0$ mit $\lambda_1, \ldots, \lambda_n \in K(B)$. Multipliziert man die λ_i mit einem gemeinsamen Nenner, so erhält man Polynome $\delta_1, \ldots, \delta_n \in K[X_b : b \in B]$ mit $\sum \delta_i(B) a_i = 0$. Da B algebraisch unabhängig über M ist, folgt $\sum a_i \delta_i = 0$. Ein Koeffizientenvergleich ergibt $\delta_1 = \ldots = \delta_n = 0$, denn die a_i sind linear unabhängig über K. Da $K[X_b : b \in B]$ ein Integritätsbereich ist, gilt auch $\delta_1 = \ldots = \delta_n = 0$. Also sind $a_1, \ldots, a_n$ auch linear unabhängig über $K(B)$. Dies zeigt $|M : K| \leq |L : K(B)| < \infty$. □

Satz A.6.3 (Lüroth)**.** *Seien $K \subseteq L \subseteq M$ Körpererweiterungen und $x \in M$ mit $M = K(x)$. Dann existiert ein $a \in L$ mit $L = K(a)$.*

Beweis. Ist x algebraisch über K, so folgt die Behauptung aus Aufgabe II.19. Sei also x transzendent und o. B. d. A. $K \subsetneq L \subseteq M = K(X)$. Nach Lemma II.4.9 ist $K \subseteq L$ (absolut) transzendent. Daher ist

$$1 = \operatorname{trg}(K(X)|K) \overset{II.4.18}{=} \operatorname{trg}(K(X)|L) + \operatorname{trg}(L|K) \geq \operatorname{trg}(K(X)|L) + 1$$

und $L \subseteq K(X)$ ist algebraisch. Sei $\alpha \in L[Y]$ das Minimalpolynom von X über L. Da X transzendent über K ist, besitzt α einen Koeffizienten $a \in L \setminus K$. Wir arbeiten nun über den faktoriellen Ringen $R := K[X]$ und $R[Y]$. Wir schreiben $a = \frac{b}{c}$ mit teilerfremden $b, c \in R$. Sei $d \in R$, sodass $\tilde{\alpha} := d\alpha \in R[Y]$ primitiv ist. Dann ist d der führende Koeffizient von $\tilde{\alpha}$ und $c \mid d$. Wir definieren

$$\begin{aligned}\beta &:= cb(Y) - bc(Y) \in R[Y],\\ \gamma &:= \frac{\beta}{c} = b(Y) - ac(Y) \in K(a)[Y] \subseteq M[Y].\end{aligned}$$

Wegen $\gamma(X) = \beta(X) = 0$ ist $\alpha \mid \gamma$. Daher existiert $\delta \in K(X)[Y]$ mit $\tilde{\alpha}\delta = \beta$.

Wir zeigen $\delta \in K$ in drei Schritten. Sei $e \in R$, sodass $\tilde{\delta} := e\delta \in R[Y]$ primitiv ist. Nach Lemma II.5.24 ist auch $e\beta = \tilde{\alpha}\tilde{\delta}$ primitiv und es folgt $e \in R^\times = K^\times$. Also ist $\delta \in R[Y]$. Sei $\deg_X \beta$ der Grad von β als Polynom in X (mit Koeffizienten in $K[Y]$). Dann gilt

$$\deg_X \beta \leq \max\{\deg b, \deg c\} \leq \deg_X \tilde{\alpha}, \tag{A.6.1}$$

denn $\tilde{\alpha}$ besitzt zwei Koeffizienten, die durch c bzw. b teilbar sind. Daher ist sogar $\delta \in K[Y]$. Division mit Rest liefert $\sigma_b, \sigma_c, \tau_b, \tau_c \in K[Y]$ mit $b(Y) = \sigma_b\delta + \tau_b$, $c(Y) = \sigma_c\delta + \tau_c$ und $\deg \tau_b, \deg \tau_c < \deg \delta$. Wegen

$$\beta = cb(Y) - bc(Y) = c(\sigma_b\delta + \tau_b) - b(\sigma_c\delta + \tau_c) = \delta(c\sigma_b - b\sigma_c) + c\tau_b - b\tau_c$$

ist $\delta \mid c\tau_b - b\tau_c$. Ein Gradvergleich zeigt $c\tau_b - b\tau_c = 0$. Die Gleichung $c\tau_b = b\tau_c$ in $K(Y)[X]$ besagt $b \mid c \mid b$. Wegen $\mathrm{ggT}(b, c) = 1$ und $b/c = a \notin K$ geht dies nur, falls $\tau_b = \tau_c = 0$. Also ist $\delta \mid \mathrm{ggT}(b, c) = 1$, d. h. $\delta \in K$.

Da das Minimalpolynom von X über $K(a)$ ein Teiler von γ ist, gilt

$$\begin{aligned} |K(X) : L| = |L(X) : L| &= \deg \alpha = \deg \tilde{\alpha} = \deg(\tilde{\alpha}\delta) = \deg \beta = \deg \gamma \\ &\geq |K(a)(X) : K(a)| = |K(X) : K(a)| \overset{a \in L}{\geq} |K(X) : L|. \end{aligned}$$

Dies zeigt $L = K(a)$. □

Satz A.6.4 (Steinitz)**.** *Je zwei gleichmächtige überabzählbare algebraisch abgeschlossene Körper der gleichen Charakteristik sind isomorph.*

Beweis. Sei K ein überabzählbarer, algebraisch abgeschlossener Körper. Die Charakteristik von K bestimmt den Primkörper P von K bis auf Isomorphie. Sei B eine Transzendenzbasis von K über P. Dann ist K der algebraische Abschluss von $P(B)$. Nach Folgerung II.2.11 ist K bis auf Isomorphie durch $P(B)$ eindeutig bestimmt. Da jedes Element aus K Nullstelle eines Polynoms in $P(B)[X]$ ist, ist K eine abzählbare Vereinigung von Kopien von $P(B)$. Da K unendlich groß ist, müssen K und $P(B)$ gleichmächtig sein. Nach Bemerkung II.4.7 ist $P(K)$ zum Körper der rationalen Funktionen $P(X_b : b \in B)$ isomorph. Es genügt daher zu zeigen, dass $P(B)$ und B gleichmächtig sind. Bekanntlich ist P höchstens abzählbar. Jedes Element in $P(B)$ hat die Form $\alpha(C)/\beta(C)$, wobei α und β Polynome mit Koeffizienten in P sind und C eine endliche Teilmenge von B ist. Wäre B endlich, so wären $P(B)$ und K abzählbar. Also ist B unendlich. Sei

$$\mathcal{B} := \{C \subseteq B : |C| < \infty\}.$$

Dann $P(B)$ in einer Menge vom Typ $\bigcup_{C \in \mathcal{B}} P$ enthalten. Insbesondere sind $P(B)$ und $\mathcal{B}$ gleichmächtig. In der Mengenlehre[1] zeigt man, dass $\mathcal{B}$ und B gleichmächtig sind. Damit sind auch K und B gleichmächtig. Insgesamt ist K durch seine Mächtigkeit und Charakteristik bis auf Isomorphie eindeutig bestimmt. □

Beispiel A.6.5. Die abzählbaren algebraisch abgeschlossenen Körper $\overline{\mathbb{Q}}$ und $\overline{\mathbb{Q}(X)}$ sind nicht isomorph, da $\overline{\mathbb{Q}(X)}$ nicht über seinem Primkörper algebraisch ist.

Bemerkung A.6.6. Die (formale) Ableitung für Polynome lässt sich genauso gut für Potenzreihen und sogar Laurentreihen definieren (Aufgabe II.30). Die Summen- und Produktregel übertragen sich leicht. Aus der Produktregel folgt

$$\alpha' = \left(\frac{\alpha}{\beta}\beta\right)' = \left(\frac{\alpha}{\beta}\right)'\beta + \frac{\alpha\beta'}{\beta}$$

[1] Siehe Satz 8.11 in meinem Mengenlehre-Skript

für $\alpha, \beta \in K((X))$ und $\beta \neq 0$. Durch Umstellen erhält man die *Quotientenregel*

$$\Big(\frac{\alpha}{\beta}\Big)' = \frac{\alpha'\beta - \alpha\beta'}{\beta^2}.$$

Nach der universellen Eigenschaft lässt sich die Einbettung $K[X] \hookrightarrow K[[X]] \hookrightarrow K((X))$ zu genau einem Homomorphismus $K(X) \to K((X))$ fortsetzen (Aufgabe I.40). Wir betrachten im Folgenden $K(X)$ als Teilkörper von $K((X))$.

Definition A.6.7. Sei $\frac{\partial\alpha}{\partial X_k}$ die (partielle) Ableitung von $\alpha \in K(X_1, \dots, X_n)$ nach X_k.

Lemma A.6.8 (Mehrdimensionale Kettenregel)**.** *Für $\alpha \in K[X_1, \dots, X_n]$ und $\beta_1, \dots, \beta_n \in K(X_1, \dots, X_n)$ gilt*

$$\frac{\partial\alpha(\beta_1, \dots, \beta_n)}{\partial X_k} = \sum_{i=1}^{n} \frac{\partial\beta_i}{\partial X_k} \frac{\partial\alpha}{\partial X_i}(\beta_1, \dots, \beta_n).$$

Beweis. Wegen der Summenregel können wir annehmen, dass α ein Monom ist, etwa $\alpha = X_1^{a_1} \dots X_n^{a_n}$. Nach der Produktregel gilt

$$\frac{\partial\alpha(\beta_1, \dots, \beta_n)}{\partial X_k} = \sum_{i=1}^{n} a_i \frac{\partial\beta_i}{\partial X_k} \beta_1^{a_1} \dots \beta_i^{a_i - 1} \dots \beta_n^{a_n} = \sum_{i=1}^{n} \frac{\partial\beta_i}{\partial X_k} \frac{\partial\alpha}{\partial X_i}(\beta_1, \dots, \beta_n). \qquad \square$$

Satz A.6.9. *Sei* $\operatorname{char} K = 0$. *Genau dann ist $\alpha_1, \dots, \alpha_n \in K(X_1, \dots, X_n)$ eine Transzendenzbasis von $K(X_1, \dots, X_n)$ über K, wenn $\det(\partial\alpha_i/\partial X_j) \neq 0$.*

Beweis. Wegen $\operatorname{trg}(K(X_1, \dots, X_n)) = n$ ist $\alpha_1, \dots, \alpha_n$ genau dann eine Transzendenzbasis, wenn $\alpha_1, \dots, \alpha_n$ algebraisch unabhängig sind. Angenommen $\alpha_1, \dots, \alpha_n$ sind algebraisch abhängig. Dann existiert $\beta \in K[X_1, \dots, X_n] \setminus K$ mit $\beta(\alpha_1, \dots, \alpha_n) = 0$. Sei dabei $\deg\beta$ so klein wie möglich. Die Kettenregel liefert

$$\sum_{j=1}^{n} \frac{\partial\alpha_j}{\partial X_i} \frac{\partial\beta}{\partial X_j}(\alpha_1, \dots \alpha_n) = 0$$

für $i = 1, \dots, n$. Dies ist ein lineares Gleichungssystem in $K(X_1, \dots, X_n)$ mit Koeffizientenmatrix $(\partial\alpha_j/\partial X_i)$. Wegen $\beta \notin K$ und $\operatorname{char} K = 0$ existiert ein j mit $\partial\beta/\partial X_j \neq 0$. Da $\deg\beta$ minimal ist, gilt $\frac{\partial\beta}{\partial X_j}(\alpha_1, \dots \alpha_n) \neq 0$. Also hat das Gleichungssystem eine nicht-triviale Lösung und die Determinante der Koeffizientenmatrix muss 0 sein.

Seien nun $\alpha_1, \dots, \alpha_n$ algebraisch unabhängig über K. Wegen $\operatorname{trg}(K(X_1, \dots, X_n)) = n$ sind $X_i, \alpha_1, \dots, \alpha_n$ algebraisch abhängig für $1 \leq i \leq n$. Sei $\beta_i \in K[X_0, \dots, X_n] \setminus K$ mit $\beta_i(X_i, \alpha_1, \dots, \alpha_n) = 0$ und $\deg\beta_i$ minimal. Ableiten nach X_k ergibt

$$\delta_{ik} \frac{\partial\beta_i}{\partial X_0}(X_i, \alpha_1, \dots, \alpha_n) + \sum_{j=1}^{n} \frac{\partial\alpha_j}{\partial X_k} \frac{\partial\beta_i}{\partial X_j}(X_i, \alpha_1, \dots \alpha_n) = 0$$

für $i = 1, \dots, n$. Da $\alpha_1, \dots, \alpha_n$ algebraisch unabhängig sind, muss X_0 in jedem β_i auftauchen. Insbesondere ist $\partial\beta_i/\partial X_0 \neq 0$ mit kleinerem Grad als β_i. Nach Wahl von β_i ist $\frac{\partial\beta_i}{\partial X_0}(X_i, \alpha_1, \dots \alpha_n) \neq 0$ für $i = 1, \dots, n$. Dies liefert eine Matrixgleichung in $K[X_1, \dots, X_n]$:

$$\Big(\frac{\partial\beta_i}{\partial X_j}(X_i, \alpha_1, \dots, \alpha_n)\Big)\Big(\frac{\partial\alpha_i}{\partial X_j}\Big) = -\Big(\delta_{ij} \frac{\partial\beta_i}{\partial X_0}(X_i, \alpha_1, \dots, \alpha_n)\Big).$$

Da die Determinante der Diagonalmatrix auf der rechten Seite nicht verschwindet, muss $\det(\partial\alpha_i/\partial X_j) \neq 0$ gelten. □

Bemerkung A.6.10. Man nennt $(\partial\alpha_i/\partial X_j)$ die *Jacobi-Matrix* von $\alpha_1, \ldots, \alpha_n$.

Beispiel A.6.11. Seien $\alpha = XY$, $\beta = Y + Z$ und $\gamma = \frac{X^2}{Z}$. Die Determinante der Jacobi-Matrix ist

$$\det \begin{pmatrix} Y & X & 0 \\ 0 & 1 & 1 \\ \frac{2X}{Z} & 0 & -\frac{X^2}{Z^2} \end{pmatrix} = -\frac{X^2Y}{Z^2} + \frac{2X^2}{Z} = \frac{X^2(2Z-Y)}{Z^2} \neq 0.$$

Daher ist α, β, γ eine Transzendenzbasis von $K(X, Y, Z)$.

Definition A.6.12. Sei $\alpha \in K[X_1, \ldots, X_n]$, sodass der Grad von α in jedem X_i kleiner d ist. Man nennt

$$\Omega(\alpha) := \alpha(Y, Y^d, \ldots, Y^{d^{n-1}}) \in K[Y]$$

die *Kronecker-Transformation* von α.

Bemerkung A.6.13. Wegen der Eindeutigkeit der d-adischen Entwicklung ist die Kronecker-Transformation injektiv. Außerdem gilt $\Omega(\alpha \dot{+} \beta) = \Omega(\alpha) \dot{+} \Omega(\beta)$, falls wohldefiniert. Das folgende Kriterium erlaubt es, die Irreduzibilität von α im gewöhnlichen Polynomring $K[Y]$ zu überprüfen.

Satz A.6.14 (Kronecker-Kriterium)**.** *Ein Polynom $\alpha \in K[X_1, \ldots, X_n]$ ist genau dann irreduzibel, wenn für jede Faktorisierung $\Omega(\alpha) = \beta\gamma$ mit $\beta, \gamma \in K[Y] \setminus K$ das Polynom $\Omega^{-1}(\beta)\Omega^{-1}(\gamma)$ in einem X_i Grad $\geq d$ besitzt.*

Beweis. Sei α reduzibel, also $\alpha = \alpha_1\alpha_2$ mit $\alpha_1, \alpha_2 \in K[X_1, \ldots, X_n] \setminus K$. Der Grad von α_i in jedem X_j ist $< d$. Für $\beta := \Omega(\alpha_1)$, $\gamma := \Omega(\alpha_2)$ gilt $\Omega(\alpha) = \beta\gamma$ und $\Omega^{-1}(\beta)\Omega^{-1}(\gamma) = \alpha$.

Nehmen wir umgekehrt an, dass $\Omega(\alpha) = \beta\gamma$ gilt, wobei der Grad von $\Omega^{-1}(\beta)\Omega^{-1}(\gamma)$ in jedem X_i kleiner d ist. Wegen der Eindeutigkeit der Kronecker-Transformation muss dann $\alpha = \Omega^{-1}(\beta)\Omega^{-1}(\gamma)$ gelten. Also ist α reduzibel. □

Beispiel A.6.15. Sei $\alpha = X_1 + X_2 \in \mathbb{Q}[X_1, X_2]$ mit $d = 2$. Dann ist $\Omega(\alpha) = Y + Y^2 = Y(1 + Y)$, $\Omega^{-1}(Y) = X_1$ und $\Omega^{-1}(1 + Y) = 1 + X_1$. Da der Grad von X_1 in $X_1(1 + X_1) = X_1 + X_1^2$ gleich d ist, ist α irreduzibel.

7 Artin-Schreier-Theorie

Bemerkung A.7.1. Wir beginnen mit einer Verallgemeinerung von Lemma I.14.2.

Definition A.7.2. Für $n \in \mathbb{N}$ und einen Körper K sei $(K^\times)^n := \{x^n : x \in K^\times\} \leq K^\times$.

Satz A.7.3 (Kummer)**.** *Sei $n \in \mathbb{N}$ und K ein Körper, der eine primitive n-te Einheitswurzel enthält. Für $x \in K^\times$ sei K_x ein Zerfällungskörper von $X^n - x$. Dann ist die Abbildung $\langle x(K^\times)^n\rangle \mapsto K_x$ eine Bijektion zwischen der Menge der zyklischen Untergruppen von $K^\times/(K^\times)^n$ der Ordnung n und der Menge der K-Isomorphieklassen von Galois-Erweiterungen $K \subseteq L$ mit $\mathrm{Gal}(L|K) \cong C_n$.*

Beweis. Sei $\zeta \in K$ eine primitive n-te Einheitswurzel und $x \in K^\times$ und $|\langle x(K^\times)^n\rangle| = n$. Sei $y \in K_x$ mit $y^n = x$. Dann sind $\zeta y, \zeta^2 y, \ldots, \zeta^n y$ die paarweise verschiedenen Nullstellen von $X^n - x$. Nach Artin ist $K \subseteq K_x$ eine Galois-Erweiterung. Nach (dem Beweis von) Lemma I.14.2 ist

$$d := |K_x : K| = |K(y) : K|$$

ein Teiler von n. Das Minimalpolynom μ_y von y über K teilt $X^n - x$ und besitzt daher Nullstellen der Form $\zeta^i y$ mit $i \in \mathbb{Z}$. Das Absolutglied von μ_y hat somit die Form $\pm\zeta^i y^d$. Dies zeigt $y^d \in K$ und $x^d = (y^d)^n \in (K^\times)^n$. Wegen $|\langle x(K^\times)^n\rangle| = n$ gilt $d = n$. Nach Lemma I.14.2 ist $\mathrm{Gal}(L|K) \cong C_n$. Sei $x' \in K^\times$ mit $\langle x'(K^\times)^n\rangle = \langle x(K^\times)^n\rangle$. Dann existieren $m \in \mathbb{N}$ und $a \in K^\times$ mit $x' = x^m a^n$. Da $X^n - x'$ die Nullstellen $y^m a\zeta^i \in K_x$ für $i = 1, \ldots, n$ besitzt, ist K_x auch Zerfällungskörper von $X^n - x'$. Es folgt $K_{x'} \cong K_x$. Insgesamt ist damit die Wohldefiniertheit der angegebenen Abbildung $\langle x(K^\times)^n\rangle \mapsto K_x$ gezeigt.

Für die Surjektivität sei $K \subseteq L$ eine Galois-Erweiterung mit $\mathrm{Gal}(L|K) \cong C_n$. Nach Lemma I.14.2 ist L der Zerfällungskörper von $X^n - x$ für ein $x \in K$. Wegen $|L : K| = n$ ist $X^n - x$ irreduzibel und $x^d \notin K$ für $d < n$. Also ist $|\langle x(K^\times)^n\rangle| = n$. Seien schließlich $x, x' \in K^\times$ mit $|\langle x(K^\times)^n\rangle| = |\langle x'(K^\times)^n\rangle| = n$ und sei $\Gamma\colon K_x \to K_{x'}$ ein K-Isomorphismus. O. B. d. A. seien K_x und $K_{x'}$ Teilkörper des algebraischen Abschluss $\overline{K}$. Da $\Gamma(K_x) = K_{x'}$ ein Zerfällungskörper von $\Gamma(X^n - x) = X^n - x$ ist, gilt nun $K_x = K_{x'}$. Sei $\mathrm{Gal}(K_x|K) = \langle\sigma\rangle$. Seien $y \in K_x$ und $y' \in K_{x'}$ mit $y^n = x$ und $(y')^n = x'$. Dann sind $\sigma(y)/y$ und $\sigma(y')/y'$ primitive n-te Einheitswurzeln in K. O. B. d. A. sei $\sigma(y) = \zeta y$ und $\sigma(y') = \zeta^m y'$ für ein $m \leq n$. Wegen $K_x = K(y)$ existieren $\lambda_1, \ldots, \lambda_n \in K$ mit $y' = \sum_{i=1}^n \lambda_i y^i$. Es folgt

$$\sum_{i=1}^n \lambda_i \zeta^m y^i = \zeta^m y' = \sigma(y') = \sum_{i=1}^n \lambda_i \sigma(y)^i = \sum_{i=1}^n \lambda_i \zeta^i y^i.$$

Ein Koeffizientenvergleich ergibt $\lambda_i = 0$ für $i \neq m$. Also ist $y' = \lambda_m y^m$ und $x' = (y')^n = \lambda_m^n x^m \in x^m(K^\times)^n$. Dies zeigt $\langle x(K^\times)^n\rangle = \langle x'(K^\times)^n\rangle$ und die Abbildung $\langle x(K^\times)^n\rangle \mapsto K_x$ ist injektiv. □

Beispiel A.7.4. Kummers Satz lässt sich auf $K = \mathbb{Q}$ und $n = 2$ anwenden. Für $a, b \in \mathbb{Q}^\times$ gilt $\mathbb{Q}(\sqrt{a}) \cong \mathbb{Q}(\sqrt{b})$ genau dann, wenn $ab^{-1} \in (\mathbb{Q}^\times)^2$ (vgl. Aufgabe I.56).

Satz A.7.5 (HILBERTs Satz 90)**.** *Sei $K \subseteq L$ eine Galois-Erweiterung mit zyklischer Galoisgruppe $G = \langle \sigma \rangle$ und $a \in L$.*

(i) Genau dann gilt $\prod_{\tau \in G} \tau(a) = 1$, wenn $a = \frac{b}{\sigma(b)}$ für ein $b \in L^\times$.

(ii) Genau dann gilt $\sum_{\tau \in G} \tau(a) = 0$, wenn $a = b - \sigma(b)$ für ein $b \in L$ gilt.

Beweis. Sei $|G| = n$.

(i) Für $a = \frac{b}{\sigma(b)}$ ist sicher $N(a) := \prod_{\tau \in G} \tau(a) = 1$. Sei umgekehrt $N(a) = 1$. Nach Lemma I.14.1 ist

$$\Gamma := \mathrm{id}_L + a\sigma + a\sigma(a)\sigma^2 + \ldots + a\sigma(a)\ldots\sigma(a)^{n-2}\sigma^{n-1} \neq 0.$$

Sei also $c \in L$ mit $b := \Gamma(c) \in L^\times$. Dann gilt

$$a\sigma(b) = a\sigma(c) + a\sigma(a)\sigma^2(c) + \ldots + N(a)\sigma^n(c) = a\sigma(c) + a\sigma(a)\sigma^2(c) + \ldots + c = b.$$

(ii) Für $a = b - \sigma(b)$ ist sicher $S(a) := \sum_{\tau \in G} \tau(a) = 0$. Sei umgekehrt $S(a) = 0$. Nach Lemma I.14.1 existiert ein $c \in L$ mit $S(c) \in L^G \setminus \{0\} = K \setminus \{0\}$. Nach Normierung gilt $S(c) = 1$. Für

$$b := a\sigma(c) + (a + \sigma(a))\sigma^2(c) + \ldots + (a + \ldots + \sigma^{n-2}(a))\sigma^{n-1}(c)$$

gilt dann

$$\sigma(b) = \sigma(a)\sigma^2(c) + \ldots + \underbrace{(\sigma(a) + \ldots + \sigma^{n-1}(a))}_{=S(a)-a=-a}c = \sigma(a)\sigma^2(c) + \ldots - ac = b - aS(c) = b - a. \quad \square$$

Bemerkung A.7.6. Der folgende Satz ist eine Version von Kummers Lemma in Primzahlcharakteristik.

Satz A.7.7. *Sei $K \subseteq L$ eine Körpererweiterung vom Grad $p = \mathrm{char}\, K > 0$. Genau dann ist $K \subseteq L$ eine Galois-Erweiterung, falls L Zerfällungskörper eines Polynoms $X^p - X - a \in K[X]$ ist.*

Beweis. Sei L Zerfällungskörper von $\alpha := X^p - X - a \in K[X]$ und $x \in L$ eine Nullstelle von α. Wegen

$$\alpha(x+1) = (x+1)^p - x - 1 - a = x^p - x - a + 1 - 1 = \alpha(x) = 0.$$

hat α paarweise verschiedene Nullstellen $x, x+1, \ldots, x+p-1$. Nach Artin ist $K \subseteq L$ eine Galois-Erweiterung.

Sei nun umgekehrt $K \subseteq L$ eine Galois-Erweiterung mit $G := \mathrm{Gal}(L|K) = \langle \sigma \rangle$. Wegen $\sum_{\tau \in G} \tau(1) = p = 0$ existiert nach Hilberts Satz 90 ein $x \in L$ mit $1 = x - \sigma(x)$. Insbesondere ist $x \notin L^G = K$ und $L(x) = K$. Wegen

$$a := \sigma(x^p - x) = \sigma(x)^p - \sigma(x) = (x-1)^p - x + 1 = x^p - x \in L^G = K$$

ist L Zerfällungskörper von $X^p - X - a \in K[X]$. $\square$

Lemma A.7.8. *Sei K ein Körper der Charakteristik $p > 0$ und $a \in K \setminus \{b^p : b \in K\}$. Dann ist $X^{p^k} - a$ für jedes $k \in \mathbb{N}$ irreduzibel in $K[X]$.*

Beweis. Sei $\alpha := X^{p^k} - a \in K[X]$ reduzibel, etwa $\alpha = \beta\gamma$ mit o. B. d. A. normierten $\beta, \gamma \in K[X] \setminus K$. Für eine Nullstelle x von α in einem Zerfällungskörper gilt dann

$$\beta \mid \alpha = X^{p^k} - a = X^{p^k} - x^{p^k} = (X - x)^{p^k}.$$

Daher ist $\beta = (X - x)^s$ mit $0 < s < p^k$. Sei $s = p^l t$ mit $p \nmid t$ und $l < k$. Dann ist

$$\beta = (X^{p^l} - x^{p^l})^t = X^s - tx^{p^l} X^{p^l(t-1)} + \dots$$

mit $-tx^{p^l} \in K$. Wegen $p \nmid t$ ist auch $x^{p^l} \in K$. Also ist $a = (x^{p^l})^{p^{k-l}} \in \{b^p : b \in K\}$. □

Lemma A.7.9. *Sei K ein Körper, in dem X^2+1 irreduzibel ist. Außerdem sei in einem Zerfällungskörper von $X^2 + 1$ jedes Element ein Quadrat. Dann ist* $\operatorname{char} K = 0$ *und jede Summe von Quadraten in K wieder ein Quadrat.*

Beweis. Sei L ein Zerfällungskörper von $X^2 + 1$ und $x \in L$ mit $x^2 = -1$. Es genügt zu zeigen, dass die Summe von zwei Quadraten ein Quadrat ist. Für $a, b \in K$ existieren $c, d \in K$ mit $a + bx = (c + dx)^2 = c^2 - d^2 + 2cdx$. Also ist $a = c^2 - d^2$ und $b = 2cd$. Dies zeigt

$$a^2 + b^2 = (c^2 - d^2)^2 + (2cd)^2 = (c^2 + d^2)^2.$$

Im Fall $\operatorname{char} K = p > 0$ wäre $-1 = 1^2 + \dots + 1^2$ ($p-1$ Summanden) ein Quadrat. Also ist $\operatorname{char} K = 0$. □

Satz A.7.10 (Artin-Schreier)**.** *Sei $K \subsetneq L$ eine endliche Körpererweiterung und L algebraisch abgeschlossen. Dann ist $|L : K| = 2$ und* $\operatorname{char} K = 0$*. Außerdem existiert ein $z \in L$ mit $L = K(z)$ und $z^2 = -1$.*

Beweis. Wir zeigen zunächst, dass K vollkommen ist. Sei dazu $\operatorname{char} K = p > 0$ und $a \in K$. Ist a keine p-te Potenz (also nicht im Bild des Frobenius-Homomorphismus), so ist $\alpha := X^{p^k} - a$ für alle $k \in \mathbb{N}$ irreduzibel in $K[X]$ nach Lemma A.7.8. Andererseits besitzt α eine Nullstelle x im algebraisch abgeschlossenen Körper L. Dies liefert den Widerspruch

$$p^k = |K(x) : K| \leq |L : K| < \infty \qquad \forall k \in \mathbb{N}.$$

Also ist K vollkommen und $K \subseteq L$ separabel. Nach Aufgabe II.23 ist $K \subseteq L$ normal und daher eine Galois-Erweiterung. Sei $G := \operatorname{Gal}(L|K)$.

Fall 1: $p := |L : K| = |G| \in \mathbb{P}$.
Sei $G = \langle\sigma\rangle$. Nehmen wir zunächst $\operatorname{char} K = p$ an. Nach Satz A.7.7 ist $L = K(x)$ mit $a := x^p - x \in K$. Da L algebraisch abgeschlossen ist, existiert ein $y \in L$ mit $y^p - y = ax^{p-1}$. Wir schreiben $y = y_0 + y_1 x + \dots + y_{p-1}x^{p-1}$ mit $y_0, \dots, y_{p-1} \in K$. Dann ist

$$ax^{p-1} = y^p - y = \sum_{i=0}^{p-1} (y_i^p x^{ip} - y_i x^i) = \sum_{i=0}^{p-1} (y_i^p (x + a)^i - y_i x^i) = (y_{p-1}^p - y_{p-1})x^{p-1} + \dots.$$

Ein Koeffizientenvergleich liefert $a = y_{p-1}^p - y_{p-1}$. Dann wäre aber y_{p-1} Nullstelle von $X^p - X - a$ und man hätte den Widerspruch $L = K(x) = K(y_{p-1}) = K$. Also ist $\operatorname{char} K \neq p$ und $X^p - 1 \neq (X - 1)^p$ in $K[X]$. Der algebraisch abgeschlossene Körper L besitzt folglich eine primitive p-te Einheitswurzel ζ. Wegen $X^p - 1 = (X-1)(X^{p-1} + \dots + 1)$ ist $|K(\zeta) : K| \leq p-1$ und andererseits $|K(\zeta) : K| \,\big|\, |L : K| = p$. Dies zeigt $\zeta \in K$. Nach Lemma I.14.1 existiert ein $b \in L$ mit

$$x := b + \zeta\sigma(b) + \zeta^2\sigma^2(b) + \dots + \zeta^{p-1}\sigma^{p-1}(b) \neq 0.$$

Wegen $\sigma(x) = \zeta^{-1}x \neq x$ ist $L = K(x)$. Außerdem gilt $x^p = \zeta^{-p}x^p = \sigma(x)^p = \sigma(x^p) \in L^G = K$. Wir wählen $y \in L$ mit $y^p = x$. Dann ist $\sigma(y)^{p^2} = \sigma(y^{p^2}) = \sigma(x^p) = x^p = y^{p^2}$, d. h. $\sigma(y) = zy$ mit $z^{p^2} = 1$. Es gilt $z^p \in \langle\zeta\rangle \subseteq K$. Im Fall $z^p = 1$ wäre

$$x = y^p = \sigma(y)^p = \sigma(y^p) \in L^G = K.$$

Also ist z eine primitive p^2-te Einheitswurzel. Wegen $(\sigma(z)z^{-1})^p = \sigma(z^p)z^{-p} = 1$ existiert ein $k \in \mathbb{Z}$ mit $\sigma(z) = z^{1+pk}$. Aus $\sigma(y) = zy$ folgt nun

$$y = \sigma^p(y) = \sigma^{p-1}(zy) = \ldots = z\sigma(z)\ldots\sigma^{p-1}(z)y = z^{1+(1+pk)+\ldots+(1+pk)^{p-1}}y$$

und

$$0 \equiv \sum_{i=0}^{p-1}(1+pk)^i \equiv \sum_{i=0}^{p-1}(1+ipk) \equiv p + \frac{p(p-1)}{2}pk \pmod{p^2}.$$

Also ist $p = 2$ und k ungerade. Wegen $\sigma(z) = z^{1+2k} = z^3 \neq z$ ist $L = K(z)$ mit $z^2 = -1$. Da L algebraisch abgeschlossen ist, ist jedes Element in L ein Quadrat. Lemma A.7.9 zeigt $\operatorname{char} K = 0$ und wir sind fertig.

Fall 2: $|L : K| \notin \mathbb{P}$.
Nehmen wir zunächst an, dass $|G|$ einen ungeraden Primteiler p besitzt. Nach Cauchy existiert ein $\sigma \in G$ der Ordnung p. Für K^σ anstelle von K liefert Fall 1 nun einen Widerspruch. Also ist $|G|$ eine 2-Potenz. Nach Sylow besitzt G eine Untergruppe H der Ordnung 4. Indem wir K durch L^H ersetzen, können wir $|G| = |L : K| = 4$ annehmen. Dann existiert ein $\sigma \in G$ der Ordnung 2. Fall 1 mit K^σ anstelle von K zeigt $L = K^\sigma(z)$ mit $z^2 = -1$. Nun kann man Fall 1 aber auch mit $K(z)$ anstelle von K anwenden. Dies liefert $L = K(z, w)$ mit $w^2 = -1 = z^2$. Dann ist aber $w = \pm z \in K(z)$. Widerspruch. □

Beispiel A.7.11. Die Erweiterung $\mathbb{R} \subseteq \mathbb{C}$ erfüllt die Voraussetzung von Artin-Schreier.

Folgerung A.7.12. *Sei K ein algebraisch abgeschlossener Körper und $H \leq \operatorname{Aut}(K)$ mit $|H| < \infty$. Dann ist $|H| \leq 2$ und im Fall $\operatorname{char} K > 0$ sogar $H = 1$.*

Beweis. Nach Artin ist $K^H \subseteq K$ eine Galois-Erweiterung. Artin-Schreier zeigt $|H| = |K : K^H| \leq 2$ und $K = K^H$ falls $\operatorname{char} K > 0$. □

Bemerkung A.7.13. Die komplexe Konjugation ist bei weitem nicht der einzige Automorphismus auf $\mathbb{C}$ der Ordnung 2. Tatsächlich gibt es unendlich viele Konjugationsklassen von Elementen der Ordnung 2 in $\operatorname{Aut}(\mathbb{C})$.[1]

[1] siehe [B. Schnor, *Involutions in the Group of Automorphisms of an Algebraically Closed Field*, J. Algebra 152 (1992), 520–524]

8 Proendliche Gruppe

Bemerkung A.8.1. Wir haben in Definition III.9.33 die Krull-Topologie auf Galoisgruppen von (unendlichen) Galois-Erweiterungen definiert. Wir zeigen in diesem Abschnitt wie man abstrakte Gruppen mit topologischen Eigenschaften als Galoisgruppen charakterisieren kann. Für solche (proendliche) Gruppen beweisen wir Verallgemeinerungen der Sätze von Lagrange und Sylow.

Definition A.8.2. Sei M eine nichtleere Menge. Eine Familie von Teilmengen $\mathcal{F} \subseteq \mathcal{P}(M)$ heißt *Filter* von M, falls gilt:

- $\varnothing \neq \mathcal{F} \neq \mathcal{P}(M)$.
- $A, B \in \mathcal{F} \Longrightarrow A \cap B \in \mathcal{F}$.
- $A \supseteq B \in \mathcal{F} \Longrightarrow A \in \mathcal{F}$.

Ist $\mathcal{F}$ maximal bzgl. Inklusion, so nennt man $\mathcal{F}$ einen *Ultrafilter*.

Bemerkung A.8.3. Die erste Bedingung in Definition A.8.2 ist äquivalent zu $\varnothing \notin \mathcal{F}$ und $M \in \mathcal{F}$.

Beispiel A.8.4.

(i) Für jede Teilmenge $\varnothing \neq A \subseteq M$ ist

$$\mathcal{F}(A) := \{B \subseteq M : A \subseteq B\}$$

ein Filter. Für $x \in M$ sei $\mathcal{F}(x) := \mathcal{F}(\{x\})$.

(ii) Die Menge Ω aller Filter, die einen gegebenen Filter $\mathcal{F}$ enthalten ist durch $\subseteq$ geordnet. Man sieht leicht, dass die Vereinigung einer total geordneten Teilmenge von Ω wieder ein Filter ist. Nach Zorns Lemma existiert also stets ein Ultrafilter, der $\mathcal{F}$ enthält.

Lemma A.8.5. *Für jeden Filter $\mathcal{F}$ von $M \neq \varnothing$ sind folgende Aussagen äquivalent:*

(1) $\mathcal{F}$ ist ein Ultrafilter.

(2) Für alle $A \subseteq M$ gilt entweder $A \in \mathcal{F}$ oder $M \setminus A \in \mathcal{F}$.

(3) Für alle $A_1, \ldots, A_n \subseteq M$ mit $A_1 \cup \ldots \cup A_n \in \mathcal{F}$ existiert ein i mit $A_i \in \mathcal{F}$.

Beweis.

(1)⇒(2): Sei

$$\mathcal{G} := \big\{B \subseteq M : \exists F \in \mathcal{F} : A \cap F \subseteq B\big\}.$$

Ist $\varnothing \in \mathcal{G}$, so existiert ein $F \in \mathcal{F}$ mit $F \subseteq M \setminus A$. Dann gilt auch $M \setminus A \in \mathcal{F}$. Anderenfalls ist $\mathcal{G}$ ein Filter, der $\mathcal{F}$ enthält. Da $\mathcal{F}$ ein Ultrafilter ist, gilt $A = A \cap M \in \mathcal{G} = \mathcal{F}$.

(2)⇒(3): Nehmen wir $A_i \notin \mathcal{F}$ für $i = 1, \ldots, n$ an. Nach (2) gilt $M \setminus A_i \in \mathcal{F}$ für $i = 1, \ldots, n$. Da $\mathcal{F}$ ein Filter ist, folgt der Widerspruch

$$\varnothing = \Big(\bigcup_{i=1}^{n} A_i\Big) \cap \Big(M \setminus \bigcup_{i=1}^{n} A_i\Big) = \Big(\bigcup_{i=1}^{n} A_i\Big) \cap \bigcap_{i=1}^{n} (M \setminus A_i) \in \mathcal{F}.$$

(3)⇒(1): Angenommen $\mathcal{F}$ ist kein Ultrafilter. Dann existiert ein Filter $\mathcal{G} \supsetneq \mathcal{F}$ und ein $A \in \mathcal{G} \setminus \mathcal{F}$. Wegen $A \cup (M \setminus A) \in \mathcal{F}$ folgt $M \setminus A \in \mathcal{F} \subseteq \mathcal{G}$ aus (3). Nun wäre aber $\varnothing = A \cap (M \setminus A) \in \mathcal{G}$. □

Definition A.8.6. Sei M ein topologischer Raum (vgl. Lemma III.9.34).

- Man nennt M einen *Hausdorff-Raum*, falls für je zwei verschiedene Punkte $x, y \in M$ disjunkte offene Mengen $U_x, U_y \subseteq M$ mit $x \in U_x$ und $y \in U_y$ existieren (*Trennungsaxiom*).
- Man nennt $K \subseteq M$ *kompakt*, wenn sich aus jeder Überdeckung $K \subseteq \bigcup_{i \in I} U_i$ mit offenen Mengen U_i eine „Teilüberdeckung“ $K \subseteq \bigcup_{j \in J} U_j$ mit $|J| < \infty$ auswählen lässt. Ist M selbst kompakt, so spricht man von einem kompakten topologischen Raum.
- Man nennt $Z \subseteq M$ *zusammenhängend*, falls für je zwei offene Mengen $U, V \subseteq M$ mit $Z = (U \cap Z) \dot\cup (V \cap Z)$ gilt: $Z \subseteq U$ oder $Z \subseteq V$. Besitzt jede zusammenhängende Teilmenge von M höchstens ein Element, so nennt man M *total unzusammenhängend*.
- Eine Abbildung $f\colon A \to B$ zwischen topologischen Räumen A und B heißt *stetig*, wenn für jede offene Menge $U \subseteq B$ auch $f^{-1}(U)$ offen ist. Ist f bijektiv und f, f^{-1} stetig, so nennt man f einen *Homöomorphismus*.

Bemerkung A.8.7.

(i) Jeder metrische Raum (M, d) ist ein Hausdorff-Raum, denn für verschiedene $x, y \in M$ sind die offenen ϵ-Kugeln um x und y mit $\epsilon := \frac{1}{2} d(x, y)$ nach der Dreiecksungleichung disjunkt.

(ii) Ist $K \subseteq M$ kompakt und $A \subseteq K$ abgeschlossen, so ist auch A kompakt, denn ist $A \subseteq \bigcup_{i \in I} U_i$ eine offene Überdeckung, so auch $K \subseteq (M \setminus A) \cup \bigcup_{i \in I} U_i$.

(iii) Eine Abbildung $f\colon A \to B$ ist genau dann stetig, wenn Urbilder abgeschlossener Mengen abgeschlossen sind, denn $A \setminus f^{-1}(C) = f^{-1}(B \setminus C)$ für alle $C \subseteq B$.

(iv) Die Komposition von stetigen Abbildungen ist offensichtlich stetig.

(v) Ist $f\colon A \to B$ stetig und $K \subseteq A$ kompakt, so ist auch $f(K)$ kompakt, denn ist $f(K) \subseteq \bigcup_{i \in I} U_i$ eine offene Überdeckung, so auch $K \subseteq \bigcup_{i \in I} f^{-1}(U_i)$.

(vi) Im Gegensatz zu Homomorphismen ist die Umkehrabbildung einer bijektiven stetigen Abbildung nicht automatisch stetig. Betrachte zum Beispiel $A = B = \mathbb{N}$ mit der diskreten Topologie auf A (jede Teilmenge ist offen) und der trivialen Topologie auf B (nur $\varnothing$ und B sind offen). Dann ist $f\colon A \to B$, $a \mapsto a$ stetig, aber f^{-1} nicht.

Lemma A.8.8. *Jede kompakte Teilmenge eines Hausdorff-Raums ist abgeschlossen.*

Beweis. Sei K kompakt im Hausdorff-Raum M. Sei $x \in M \setminus K$. Für alle $a \in K$ existieren disjunkte offene Mengen $U_a, V_a \subseteq M$ mit $a \in U_a$ und $x \in V_a$. Wegen der Kompaktheit existieren $a_1, \ldots, a_n \in K$ mit $K \subseteq U_{a_1} \cup \ldots \cup U_{a_n}$. Nun ist $V_{a_1} \cap \ldots \cap V_{a_n}$ eine offene Menge in $M \setminus K$, die x enthält. Also ist $M \setminus K$ offen und K ist abgeschlossen. □

Folgerung A.8.9. *Sei A ein kompakter Raum und B ein Hausdorff-Raum. Dann ist jede stetige Bijektion $A \to B$ ein Homöomorphismus.*

Beweis. Sei $f\colon A \to B$ eine stetige Bijektion und $U \subseteq A$ abgeschlossen. Nach Bemerkung A.8.7 sind U und $f(U)$ kompakt. Nach Lemma A.8.8 ist $f(U)$ abgeschlossen. Daher ist f^{-1} stetig. □

Definition A.8.10. Ein Filter $\mathcal{F}$ eines topologischen Raums M *konvergiert* gegen $x \in M$, falls alle offenen Teilmengen in $\mathcal{F}(x)$ auch in $\mathcal{F}$ liegen.

Lemma A.8.11. *Ein topologischer Raum M ist genau dann kompakt, wenn jeder Ultrafilter von M gegen einen Punkt konvergiert.*

Beweis. Sei M kompakt. Angenommen ein Ultrafilter $\mathcal{F}$ von M konvergiert gegen keinen Punkt. Für alle $x \in M$ existieren dann eine offene Menge $U_x \notin \mathcal{F}$ mit $x \in U_x$. Da M kompakt ist, existiert eine endliche Menge $X \subseteq M$ mit $M = \bigcup_{x \in X} U_x$. Dies widerspricht Lemma A.8.5.

Nehmen wir nun an, dass M nicht kompakt ist. Dann existiert eine offene Überdeckung $M = \bigcup_{i \in I} U_i$ ohne endliche Teilüberdeckung. Folglich ist

$$\left\{A \subseteq M : \exists i_1, \ldots, i_n \in I : M \setminus A \subseteq U_{i_1} \cup \ldots \cup U_{i_n}\right\}$$

ein Filter, der in einem Ultrafilter $\mathcal{F}$ liegt. Angenommen $\mathcal{F}$ konvergiert gegen x. Sei $i \in I$ mit $x \in U_i$. Dann wäre $\varnothing = U_i \cap (M \setminus U_i) \in \mathcal{F}$. □

Definition A.8.12. Sei G eine Gruppe und zugleich ein topologischer Raum.

- Man erhält die *Produkt-Topologie* auf $G \times G$, indem man offenen Mengen als beliebige Vereinigungen von Produkten der Form $U \times V$ mit offenen Mengen $U, V \subseteq G$ definiert.
- Man nennt G *topologisch*, falls die Abbildung $G \times G \to G$, $(x, y) \mapsto xy^{-1}$ bzgl. der entsprechenden Topologien stetig ist.
- Eine topologische Gruppe G heißt *proendlich*, falls G kompakt und total unzusammenhängend ist.

Satz A.8.13. *Für jede Galois-Erweiterung $K \subseteq L$ ist $\mathrm{Gal}(L|K)$ proendlich bzgl. der Krull-Topologie.*

Beweis. Sei $G := \mathrm{Gal}(L|K)$ und $\varphi\colon G \times G \to G$, $(x, y) \mapsto xy^{-1}$. Sei $\mathcal{N}$ die Menge der offenen Normalteiler in G wie in Definition III.9.33. Jede offene Menge $U \subseteq G$ hat die Form $U = \bigcup_{i \in I} g_i N_i$ mit $g_i \in G$ und $N_i \in \mathcal{N}$ für $i \in I$. Dann ist

$$\varphi^{-1}(U) = \bigcup_{i \in I} \varphi^{-1}(g_i N_i) = \bigcup_{i \in I} \bigcup_{x \in G} (g_i x N_i, x N_i)$$

offen und φ ist stetig. Also ist G eine topologische Gruppe.

Sei nun $Z \subseteq G$ zusammenhängend. Angenommen es existieren verschiedene $x, y \in Z$. Nach Bemerkung III.9.32 gilt $\bigcap_{N \in \mathcal{N}} N = 1$. Daher existiert ein $N \in \mathcal{N}$ mit $x^{-1}y \notin N$. Nun wären aber $U := xN$ und $V := \bigcup_{gN \neq xN} gN$ disjunkte offene Mengen mit $x \in U$, $y \in V$ und $Z = (Z \cap U) \cup (Z \cap V)$. Also ist G total unzusammenhängend.

Für den Beweis der Kompaktheit von G genügt es zu zeigen, dass jeder Ultrafilter $\mathcal{F}$ gegen einen Punkt konvergiert (Lemma A.8.11). Für jedes $x \in L$ existiert eine endliche Galois-Erweiterung $K \subseteq M$ mit

$x \in M$. Dabei hat $N := \mathrm{Gal}(L|M)$ endlichen Index in G. Nach Lemma A.8.5 gilt $gN \in \mathcal{F}$ für ein $g \in G$. Sei auch $K \subseteq \tilde{M}$ eine endliche Galois-Erweiterung mit $x \in \tilde{M}$ und $\tilde{N} := \mathrm{Gal}(L|\tilde{M})$. Sei $\tilde{g}\tilde{N} \in \mathcal{F}$. Da $\mathcal{F}$ ein Filter ist, gilt $gN \cap \tilde{g}\tilde{N} \neq \varnothing$. Für $\sigma \in gN \cap \tilde{g}\tilde{N}$ gilt $\sigma^{-1}g(x) = x = \sigma^{-1}h(x)$ und $g(x) = h(x)$. Auf diese Weise erhält man eine wohldefinierte Abbildung $\gamma\colon L \to L$, $x \mapsto g(x)$. Man zeigt leicht $\gamma \in G$. Sei $\gamma \in gN$. Dann gilt $gN = \gamma N$. Wie oben existiert ein $h \in G$ mit $hN \in \mathcal{F}$. Für $x \in L^N$ gilt dabei $h(x) = \gamma(x)$. Dies zeigt $h^{-1}\gamma \in N$ und $gN = hN \in \mathcal{F}$. Also konvergiert $\mathcal{F}$ gegen γ. □

Lemma A.8.14. *Für jede proendliche Gruppe G gilt*

(i) Für $x \in G$ sind die Abbildungen $G \to G$, $g \mapsto xg$, $G \to G$, $g \mapsto gx$ und $G \to G$, $g \mapsto g^{-1}$ Homöomorphismen.

(ii) Jede endliche Teilmenge von G ist abgeschlossen.

(iii) G ist ein Hausdorff-Raum.

(iv) Eine Untergruppe $H \leq G$ ist genau dann offen, wenn H abgeschlossen ist und $|G : H| < \infty$.

(v) Jede offene, abgeschlossene Teilmenge $U \subseteq G$ mit $1 \in U$ enthält einen offenen Normalteiler.

(vi) Der Durchschnitt aller offenen Normalteiler von G ist trivial.

Beweis.

(i) Jede offene Menge in $G \times G$ ist eine Vereinigung von Mengen der Form $U \times V$ mit $U, V \subseteq G$ offen. Das Urbild von $U \times V$ unter der Abbildung $\varphi\colon G \to G \times G$, $g \mapsto (g, x^{-1})$ ist entweder leer oder U. Daher ist φ stetig. Nach Definition ist auch $\psi\colon G \times G \to G$, $(g, h) \mapsto gh^{-1}$ stetig. Also ist $\psi \circ \varphi\colon G \to G$, $g \mapsto gx$ stetig. Analog sind auch $\varphi\colon G \to G \times G$, $g \mapsto (1, g)$ und $\psi \circ \varphi\colon G \to G$, $g \mapsto g^{-1}$ stetig. Dies zeigt, dass auch $\varphi\colon G \to G \times G$, $g \mapsto (x, g^{-1})$ und $\psi \circ \varphi\colon G \to G$, $g \mapsto xg$ stetig sind. Es ist klar, dass in allen Fällen auch die Umkehrabbildungen stetig sind.

(ii) Seien $x, y \in G$ verschieden. Da $\{x, y\}$ nicht zusammenhängend ist, existiert eine offene Menge $U_y \subseteq G$ die y, aber nicht x enthält. Nun ist $\{x\} = \bigcap_{y \in G \setminus \{x\}} G \setminus U_y$ abgeschlossen. Als endliche Vereinigung von einelementigen Teilmengen ist jede endliche Teilmenge abgeschlossen.

(iii) Seien $x, y \in G$ verschieden. Nach (ii) ist $\{xy^{-1}\}$ abgeschlossen. Daher existiert eine offene Menge $U \subseteq G$ mit $1 \in U$ und $xy^{-1} \notin U$. Da das Urbild von U unter $G \times G \to G$, $(g, h) \mapsto gh^{-1}$ offen ist, existieren offene Mengen $V, W \subseteq G$ mit $1 \in V \cap W$ und $VW^{-1} \subseteq U$. Aus $x^{-1}y \notin VW^{-1}$ folgt $xV \cap yW = \varnothing$ mit $x \in xV$ und $y \in yW$. Nach (i) sind xV und yW offen.

(iv) Sei H offen. Dann ist $G \setminus H = \bigcup_{g \in G \setminus H} gH$ offen, d. h. H ist abgeschlossen. Da die offene Überdeckung $G = \bigcup_{g \in G} gH$ eine offene Teilüberdeckung besitzt, ist $|G : H| < \infty$. Sei umgekehrt H abgeschlossen mit $|G : H| < \infty$. Dann ist $G \setminus H$ als endliche Vereinigung von abgeschlossenen Nebenklassen abgeschlossen. Also ist H offen.

(v) Sei $x \in U$. Da $G \times G \to G$, $(g, h) \mapsto gh$ stetig ist, existieren offene Mengen $L_x, R_x \subseteq G$ mit $1 \in L_x \cap R_x =: S_x$ und $L_x R_x \subseteq Ux^{-1}$. Nun gilt $S_x S_x \subseteq Ux^{-1}$. Da G kompakt ist, ist auch die abgeschlossene Menge U kompakt. Aus der offenen Überdeckung $U \subseteq \bigcup_{x \in U} S_x x$ kann man eine endliche Teilüberdeckung $U \subseteq \bigcup_{i=1}^{n} S_{x_i} x_i$ auswählen. Jetzt ist auch $S := S_{x_1} \cap \ldots \cap S_{x_n}$ offen und $1 \in S$. Außerdem gilt

$$SU \subseteq \bigcup_{i=1}^{n} S S_{x_i} x_i \subseteq \bigcup_{i=1}^{n} U x_i^{-1} x_i \subseteq U.$$

Wegen $1 \in U$ folgt $S \subseteq U$. Sei schließlich $T := S \cap S^{-1}$ und $H := \bigcup_{i=1}^{\infty} T^i$. Man zeigt leicht, dass H eine Untergruppe von G ist. Wegen $T^i = \bigcup_{t \in T^{i-1}} tT$ sind T^i und H offen. Aus $SU \subseteq U$ folgt $H \subseteq U$. Nach (iv) ist $|G : H| < \infty$. Daher hat auch der Kern $N := H_G$ endlichen Index (Aufgabe I.17). Wegen $|G : \mathrm{N}_G(H)| \leq |G : H| < \infty$ ist N als endlicher Durchschnitt von Konjugierten von H offen mit $N \subseteq U$.

(vi) Sei $1 \neq x \in G$. Da $\{1, x\}$ unzusammenhängend ist, existiert eine offene, abgeschlossene Teilmenge $U_x \subseteq G$ mit $1 \in U_x$ und $x \notin U_x$. Nach (v) existiert ein offener Normalteiler $N_x \trianglelefteq G$ mit $N_x \subseteq U_x$. Daher ist $\bigcap_{x \in G \setminus \{1\}} N_x = 1$. □

Satz A.8.15 (Leptin)**.** *Jede proendliche Gruppe ist die Galoisgruppe einer Galois-Erweiterung bzgl. der Krull-Topologie.*

Beweis. Nach Lemma A.8.14 existiert eine Familie $\mathcal{N}$ von offenen Normalteilern mit $\bigcap_{N \in \mathcal{N}} N = 1$ und $|G : N| < \infty$ für alle $N \in \mathcal{N}$. Daher operiert G treu auf der disjunkten Vereinigung $\Omega := \dot{\bigcup}_{N \in \mathcal{N}} G/N$ durch Linksmultiplikation. Sei K ein beliebiger Körper und $L := K(X_\omega : \omega \in \Omega)$. Durch Permutation der X_ω operiert G auf L. Sei $M := L^G$ und $\Gamma \colon G \to \mathrm{Gal}(L|M)$ der kanonische Monomorphismus. Für $\omega = gN \in \Omega$ hat die Bahn von X_ω unter G Länge $|G : N| < \infty$. Daher ist X_ω Nullstelle des separablen Polynoms $\prod_{\delta \in {}^G\omega}(Y - X_\delta) \in M[Y]$. Dies zeigt, dass $M \subseteq L$ eine separable Körpererweiterung ist.

Sei $x \in L$ beliebig. Dann existiert eine endliche Teilmenge $\Delta_x \subseteq \Omega$ mit

$$M(x) \subseteq M(X_\delta : \delta \in \Delta_x) =: M(\Delta_x).$$

O. B. d. A. sei ${}^G\Delta_x = \Delta_x$. Dann induziert G eine endliche Automorphismengruppe auf $M(\Delta_x)$. Nach Satz II.3.10 ist $M \subseteq M(\Delta_x)$ eine Galois-Erweiterung. Nach Satz III.9.28 ist daher $M \subseteq L = \bigcup_{x \in L} M(\Delta_x)$ eine Galois-Erweiterung.

Sei $M \subseteq M_1$ eine beliebige endliche Galois-Erweiterung. Nach Artin gilt $M_1 = M(x)$ für ein $x \in L$. Dies zeigt

$$H := \Gamma^{-1}\big(\mathrm{Gal}(L|M(\Delta_x))\big) \subseteq \Gamma^{-1}\big(\mathrm{Gal}(L|M_1)\big) =: H_1.$$

Wegen $|\Delta_x| < \infty$ ist H der Durchschnitt von endlichen vielen $N \in \mathcal{N}$. Insbesondere ist H offen. Als Vereinigung von Nebenklassen nach H ist auch H_1 offen. Für $\sigma \in \mathrm{Gal}(L|M)$ ist $\Gamma^{-1}(\sigma\mathrm{Gal}(L|M_1))$ entweder leer oder eine Nebenklasse nach H_1. Dies zeigt, dass Γ stetig ist. Folglich ist $\Gamma(G)$ kompakt nach Bemerkung A.8.7 und daher abgeschlossen in $\mathrm{Gal}(L|M)$ nach Lemma A.8.8, denn $\mathrm{Gal}(L|M)$ ist ein Hausdorff-Raum nach Lemma A.8.14. Der Satz von Krull zeigt $\Gamma(G) = \mathrm{Gal}(L|L^{\Gamma(G)}) = \mathrm{Gal}(L|M)$, d. h. Γ ist eine Bijektion. Wegen Folgerung A.8.9 ist Γ ein Homöomorphismus. □

Folgerung A.8.16. *In jeder proendlichen Gruppe ist jede offene Teilmenge eine Vereinigung von Nebenklassen nach offenen Normalteilern.*

Beweis. Nach Leptin ist jede proendliche Gruppe eine Galoisgruppe und man kann die Definition der Krull-Topologie (Definition III.9.33) benutzen. □

Lemma A.8.17. *Sei G proendlich und $\mathcal{N}$ die Menge der offenen Normalteiler von G. Für jede abgeschlossene Untergruppe $H \leq G$ gilt $H = \bigcap_{N \in \mathcal{N}} HN$.*

Beweis. Sicher ist $H \subseteq HN$ für alle $N \in \mathcal{N}$. Sei umgekehrt $x \in G \setminus H$. Wegen $xH \cap \bigcap_{N\in\mathcal{N}} N = xH \cap \{1\} = \varnothing$ ist $G = (G \setminus xH) \cup \bigcup_{N\in\mathcal{N}} G \setminus N$ eine offene Überdeckung. Da G kompakt ist, existieren $N_1, \ldots, N_k \in \mathcal{N}$ mit $G = (G \setminus xH) \cup G \setminus (N_1 \cap \ldots \cap N_k)$. Für $N := N_1 \cap \ldots \cap N_k \in \mathcal{N}$ gilt $xH \subseteq G \setminus N$. Dies zeigt $x \notin HN$. □

Definition A.8.18.

- Sei Π die Menge aller Abbildungen $\mathbb{P} \to \mathbb{N}_0 \cup \{\infty\}$. Wir schreiben $\pi \in \Pi$ als formales Produkt $\pi = \prod_{p\in\mathbb{P}} p^{\pi(p)}$. Für $\pi_i \in \Pi$ mit $i \in I$ sei

$$\begin{aligned} \pi_i \mid \pi_j \ &:\Longleftrightarrow\ \forall p \in \mathbb{P} : \pi_i(p) \leq \pi_j(p), \\ \prod_{i\in I} \pi_i &= \prod_{p\in\mathbb{P}} p^{\sum_{i\in I} \pi_i(p)}, \\ \mathrm{kgV}(\pi_i : i \in I) &= \prod_{p\in\mathbb{P}} p^{\sup\{\pi_i(p) : i\in I\}} \end{aligned}$$

  mit der naheliegenden Regel $k + \infty = \infty$ für $k \in \mathbb{N}_0 \cup \{\infty\}$.

- Sei G eine proendliche Gruppe und $\mathcal{N}$ die Menge der offenen Normalteiler in G. Für eine abgeschlossene Untergruppe H definieren wir (motiviert durch Lemma A.8.17)

$$\begin{aligned} |G : H| &:= \mathrm{kgV}\big(|G : HN| : N \in \mathcal{N}\big), \\ |G| &:= |G : 1| \end{aligned}$$

  (beachte: $|G : HN| \leq |G : N| < \infty$ nach Lemma A.8.14).

Bemerkung A.8.19. Sei G eine proendliche Gruppe und $H \leq G$ abgeschlossen.

(i) Sei $|G : H| < \infty$. Nach Lagrange gilt $|G : HN| \,\big|\, |G : H|$ für alle $N \in \mathcal{N}$. Nach Lemma A.8.14 ist H offen und nach Folgerung A.8.16 existiert ein $N \in \mathcal{N}$ mit $N \subseteq H$. Daher stimmt $|G : H| = |G : HN|$ mit dem gewöhnlichen Index überein.

(ii) Eine Teilmenge $U \subseteq H$ nennt man *offen in* H, falls eine offene Menge $V \subseteq G$ mit $U = V \cap H$ existiert. Auf diese Weise wird H selbst zu einem topologischen Raum (*Relativ-Topologie*). Nach Bemerkung A.8.7 ist H kompakt und offenbar auch total unzusammenhängend. Für $\varphi\colon G\times G \to G$, $(x, y) \mapsto xy^{-1}$ gilt $\varphi^{-1}_{|H\times H}(U) = \varphi^{-1}(V) \cap H \times H$. Dies zeigt, dass H eine proendliche Gruppe. Für jede abgeschlossene Untergruppe A in H ist daher $|H : A|$ definiert. Nach Definition existiert eine offene Menge $U \subseteq G$ mit $H \setminus A = U \cap H$. Wegen $G \setminus A = (G \setminus H) \cup U$ ist A auch abgeschlossen in G.

Satz A.8.20 (Lagrange für proendliche Gruppen)**.** *Sei G eine proendliche Gruppe und $A, B \leq G$ abgeschlossen mit $A \leq B$. Dann gilt*

$$|G : A| = |G : B||B : A|.$$

Beweis. Die Aussage gilt bekanntlich für Untergruppen mit endlichem Index. Für $N \in \mathcal{N}$ ist daher

$$|G : AN| = |G : BN||BN : AN| = |G : BN||B : B \cap AN| = |G : BN||B : (B \cap N)A|$$

nach der Dedekind-Identität. Offenbar ist $B \cap N$ ein offener Normalteiler von B bzgl. der Relativ-Topologie (Bemerkung A.8.19). Dies zeigt

$$\begin{aligned}|G:A| &= \operatorname{kgV}\big(|G:AN| : N \in \mathcal{N}\big) \;\big|\; \operatorname{kgV}\big(|G:BN| : N \in \mathcal{N}\big) \operatorname{kgV}\big(|B:(B\cap N)A| : N \in \mathcal{N}\big) \\ &= |G:B||B:A|.\end{aligned}$$

Sei nun M ein offener Normalteiler in B. Nach Definition der Relativ-Topologie existiert eine offene Menge $U \subseteq G$ mit $M = U \cap B$. Nach Folgerung A.8.16 existiert ein $M_1 \in \mathcal{N}$ mit $M_1 \leq U$. Nun ist auch $B \cap N \cap M_1 \trianglelefteq B$ offen in B und in M enthalten. Es folgt

$$|G:BN||B:MA| \;\big|\; |G:B(N\cap M_1)||B:(B\cap N\cap M_1)A| = |G:A(N\cap M_1)| \;\big|\; |G:A|.$$

Dies zeigt $|G:B||B:A| \;\big|\; |G:A|$. □

Definition A.8.21. Sei G eine proendliche Gruppe und $H \leq G$ abgeschlossen. Man nennt H eine *p-Untergruppe* von G, falls $|H|$ ein Teiler von $p^\infty \in \Pi$ ist. Eine p-Untergruppe H heißt *p-Sylowgruppe* von G, falls $|G:H|$ nicht durch p teilbar ist.

Satz A.8.22 (Sylow für proendliche Gruppen)**.** *Sei G eine proendliche Gruppe und $p \in \mathbb{P}$. Dann besitzt G eine p-Sylowgruppe P und jede p-Untergruppe von G ist zu einer Untergruppe von P konjugiert. Insbesondere sind je zwei p-Sylowgruppen in G konjugiert.*

Beweis. Sei $\mathcal{P}$ die Menge aller abgeschlossenen Untergruppen $H \leq G$, sodass $|G:H|$ nicht durch p teilbar ist. Wegen $G \in \mathcal{P}$ ist $\mathcal{P}$ nichtleer und durch $\subseteq$ geordnet. Sei $\mathcal{Q} \subseteq \mathcal{P}$ total geordnet, $S := \bigcap_{Q\in\mathcal{Q}} Q \leq G$ und $N \in \mathcal{N}$. Dann ist $SN = \bigcup_{s\in S} sN$ offen und abgeschlossen nach Lemma A.8.14. Als abgeschlossene Teilmenge des kompakten Raums G ist auch $G\backslash SN$ kompakt (Bemerkung A.8.7). Die offene Überdeckung

$$G \setminus SN \subseteq G \setminus S = \bigcup_{Q\in\mathcal{Q}} G \setminus Q$$

besitzt also eine endliche Teilüberdeckung. Da $\mathcal{Q}$ total geordnet ist, existiert ein $Q \in \mathcal{Q}$ mit $Q \leq SN$. Nach Lagrange ist $|G:SN| \;\big|\; |G:Q|$ zu p teilerfremd. Da $N \in \mathcal{N}$ beliebig war, folgt $S \in \mathcal{P}$. Somit ist S eine untere Schranke für $\mathcal{Q}$. Nach Zorns Lemma besitzt $\mathcal{P}$ ein minimales Element P. Angenommen P ist keine p-Untergruppe. Dann existiert ein offener Normalteiler M von B, sodass $|P : P\cap M|$ keine p-Potenz ist. Wegen Folgerung A.8.16 existiert ein $N \in \mathcal{N}$ mit $P \cap N \leq M$. Insbesondere ist auch $|P : P\cap N|$ keine p-Potenz. Nach dem endlichen Sylowsatz existiert eine p-Sylowgruppe $\tilde{P}/(P\cap N) < P/(P\cap N)$. Als Vereinigung von Nebenklassen nach $P \cap N$ ist $\tilde{P}$ offen in P. Wegen $|P:\tilde{P}| < \infty$ ist $\tilde{P}$ auch abgeschlossen in P und in G (Bemerkung A.8.19), d. h. $\tilde{P} \in \mathcal{P}$. Nach Lagrange ist $|G:\tilde{P}| = |G:P||P:\tilde{P}|$ zu p teilerfremd im Widerspruch zur Wahl von P. Dies zeigt, dass P eine p-Sylowgruppe von G ist.

Sei jetzt $U \leq G$ eine p-Untergruppe. Für alle $N \in \mathcal{N}$ ist

$$T(N) := \{g \in G : gUg^{-1} \leq PN\} \neq \varnothing$$

nach dem endlichen Sylowsatz für G/N. Als Vereinigung von Nebenklassen nach N ist $T(N)$ offen. Nehmen wir $\bigcap_{N\in\mathcal{N}} T(N) = \varnothing$ an. Da G kompakt ist, existieren $N_1, \ldots, N_k \in \mathcal{N}$ mit $\bigcap_{i=1}^k T(N_i) = \varnothing$. Dies widerspricht jedoch $\varnothing \neq T(N_1 \cap \ldots \cap N_k) \subseteq \bigcap_{i=1}^k T(N_i)$. Also existiert ein $g \in \bigcap_{N\in\mathcal{N}} T(N)$. Aus Lemma A.8.17 folgt

$$gUg^{-1} = \bigcap_{N\in\mathcal{N}} gUNg^{-1} \leq \bigcap_{N\in\mathcal{N}} PN = P.$$

Für die letzte Aussage sei U eine p-Sylowgruppe von G und $g \in G$ mit $gUg^{-1} \leq P$. Dann ist $|G : gUg^{-1}| = |G : P||P : gUg^{-1}|$ zu p teilerfremd. Wie im Beweis von Satz A.8.20 ist andererseits

$$|P : gUg^{-1}| = \mathrm{kgV}\big(|P : (P \cap N)gUg^{-1}| : N \in \mathcal{N}\big) \,\big|\, \mathrm{kgV}\big(|P : P \cap N| : N \in \mathcal{N}\big) = |P|$$

eine p-Potenz. Dies zeigt $gUg^{-1} = P$. □

Beispiel A.8.23. Sei $2 < p \in \mathbb{P}$ und $G := \mathrm{Gal}(\mathbb{Q}_{p^\infty}|\mathbb{Q})$ wie in Beispiel III.9.30. Nach Satz A.8.13 ist G proendlich. Sei $\sigma \in G$ mit $\sigma(\zeta_{p^n}) = \zeta_{p^n}^{1+p}$ für alle $n \in \mathbb{N}$. Nach (dem Beweis von) Satz I.8.34 erzeugt die Einschränkung von σ auf $\mathbb{Q}_{p^n}$ eine p-Sylowgruppe von $\mathrm{Gal}(\mathbb{Q}_{p^n}|\mathbb{Q})$. Also ist $\mathbb{Q}_{p^n}^\sigma = \mathbb{Q}_p$ und $\mathbb{Q}_{p^\infty}^\sigma = \mathbb{Q}_p$. Sei $H = \mathrm{Gal}(\mathbb{Q}_{p^\infty}|\mathbb{Q}_p) \trianglelefteq G$ der Abschluss von $\langle\sigma\rangle$ in G. Dann gilt $|G : H| = |\mathrm{Gal}(\mathbb{Q}_p|\mathbb{Q})| = p - 1$. Sei $\mathbb{Q}_p \subseteq L$ eine endliche Galois-Erweiterung mit $L \subseteq \mathbb{Q}_{p^\infty}$. Es existiert ein $n \in \mathbb{N}$ mit $L \subseteq \mathbb{Q}_{p^n}$. Für $N := \mathrm{Gal}(\mathbb{Q}_{p^\infty}|L) \trianglelefteq H$ gilt

$$|H : N| = |L : \mathbb{Q}_p| \,\big|\, |\mathbb{Q}_{p^n} : \mathbb{Q}_p| = p^{n-1}.$$

Dies zeigt, dass H eine p-Sylowgruppe von G ist. Als unendliche Galoisgruppe ist H überabzählbar nach Satz III.9.29. Insbesondere ist $H > \langle\sigma\rangle$.

Bemerkung A.8.24. Für beliebige (unendliche) Gruppen G definiert man p-Sylowgruppen völlig anders. Man nennt $P \leq G$ eine p-Untergruppe, wenn P nur aus p-Elementen besteht. Eine bzgl. Inklusion maximale p-Untergruppe heißt p-Sylowgruppe. In dieser Allgemeinheit sind jedoch alle Teile des Sylowsatzes falsch.

9 Der Satz von Lindemann-Weierstraß

Definition A.9.1. Für $\alpha = \sum a_k X^k \in \mathbb{C}[X]$, $n \in \mathbb{N}_0$ und $x \in \mathbb{C}$ sei

$$\begin{aligned}\alpha^{(\Sigma)} &:= \sum_{k=0}^{\infty} \alpha^{(k)} \in \mathbb{C}[X],\\ \epsilon_n(x) &:= e^{-|x|} \sum_{k=1}^{\infty} \frac{x^k n!}{(n+k)!} \in \mathbb{C},\\ \alpha^*(x) &:= \sum a_k \epsilon_k(x) x^k \in \mathbb{C}.\end{aligned}$$

Bemerkung A.9.2. Wegen $\frac{(n+k)!}{n!k!} = \binom{n+k}{n} \geq 1$ ist

$$e^{|x|} = 1 + \sum_{k=1}^{\infty} \frac{|x|^k}{k!} > \sum_{k=1}^{\infty} \frac{|x|^k n!}{(n+k)!}$$

und $|\epsilon_n(x)| < 1$ für alle $n \in \mathbb{N}_0$ und $x \in \mathbb{C}$.

Lemma A.9.3. *Für $\alpha \in \mathbb{C}[X]$ und $x \in \mathbb{C}$ gilt $e^x \alpha^{(\Sigma)}(0) = \alpha^{(\Sigma)}(x) + \alpha^*(x) e^{|x|}$.*

Beweis. Da die Abbildungen $\alpha \mapsto \alpha^{(\Sigma)}$ und $\alpha \mapsto \alpha^*$ linear sind, können wir $\alpha = X^n$ mit $n \in \mathbb{N}_0$ annehmen. Dann gilt

$$\alpha^{(\Sigma)}(x) + \alpha^*(x) e^{|x|} = x^n + n x^{n-1} + \ldots + n! + x^n \sum_{k=1}^{\infty} \frac{x^k n!}{(n+k)!} = n! \sum_{k=0}^{\infty} \frac{x^k}{k!} = e^x \alpha^{(\Sigma)}(0). \qquad \square$$

Lemma A.9.4. *Sei $\alpha \in \mathbb{Z}[X]$, $n \in \mathbb{N}$, $\beta := \frac{X^n}{(n-1)!}\alpha$ und $\gamma := \frac{X^{n-1}}{(n-1)!}\alpha$. Dann gilt $\beta^{(\Sigma)}(0) \in n\mathbb{Z}$ und $\gamma^{(\Sigma)}(0) \in \alpha(0) + n\mathbb{Z}$.*

Beweis. O. B. d. A. sei $\alpha = X^m$ mit $m \in \mathbb{N}_0$. Dann gilt

$$\begin{aligned}\beta^{(\Sigma)}(0) &= \beta^{(n+m)}(0) = \frac{(n+m)!}{(n-1)!} \in n\mathbb{Z},\\ \gamma^{(\Sigma)}(0) &= \beta^{(n+m-1)}(0) = \frac{(n+m-1)!}{(n-1)!} \in \alpha(0) + n\mathbb{Z}.\end{aligned} \qquad \square$$

Satz A.9.5 (Lindemann-Weierstrass)**.** *Für paarweise verschiedene $a_1, \ldots, a_n \in \overline{\mathbb{Q}}$ sind $e^{a_1}, \ldots, e^{a_n}$ linear unabhängig über $\overline{\mathbb{Q}}$.*

Beweis. Nehmen wir an, es existieren $b_1, \ldots, b_n \in \overline{\mathbb{Q}} \setminus \{0\}$ mit

$$b_1 e^{a_1} + \ldots + b_n e^{a_n} = 0. \tag{A.9.1}$$

Sei $\mu_i \in \mathbb{Q}[X]$ das Minimalpolynom von b_i und sei L ein Zerfällungskörper von $\mu_1 \ldots \mu_n$. Sei $G := \mathrm{Gal}(L|\mathbb{Q})$ und $\alpha := b_1 X_1 + \ldots + b_n X_n \in L[X_1, \ldots, X_n]$. Dann ist

$$\beta := \prod_{\sigma \in G} \sigma(\alpha) = \sum_{\substack{i_1,\ldots,i_n \geq 0 \\ i_1+\cdots+i_n=|G|}} \lambda_{i_1,\ldots,i_n} X_1^{i_1} \ldots X_n^{i_n} \in L^G[X_1, \ldots, X_n] = \mathbb{Q}[X_1, \ldots, X_n]$$

und $\beta(e^{a_1}, \ldots, e^{a_n}) = 0$. Andererseits ist $\beta(e^{a_1}, \ldots, e^{a_n})$ eine rationale Linearkombination von Termen der Form $e^{i_1 a_1 + \ldots + i_n a_n}$ mit algebraischen Exponenten. Indem wir Terme mit gleichen Exponenten zusammenfassen, erhalten wir $b_1' e^{a_1'} + \ldots + b_m' e^{a_m'} = 0$ mit $a_1', \ldots, a_m' \in \overline{\mathbb{Q}}$ paarweise verschieden und $b_1', \ldots, b_m' \in \mathbb{Q}$. Wir sortieren die a_i lexikografisch $(\mathrm{Re}(a_1), \mathrm{Im}(a_1)) < \cdots < (\mathrm{Re}(a_n), \mathrm{Im}(a_n))$. Da $e^{|G|a_1}$ nur einmal in $\beta(e^{a_1}, \ldots, e^{a_n})$ auftritt (mit Koeffizienten $\prod \sigma(b_1) \neq 0$), können nicht alle b_i' verschwinden. Wir ersetzen daher a_i durch a_i' und b_i durch b_i'. Nach Multiplikation mit dem Hauptnenner gilt dann $b_1, \ldots, b_n \in \mathbb{Z} \setminus \{0\}$.

Sei nun $\mu_i \in \mathbb{Q}[X]$ das Minimalpolynom von a_i und L ein Zerfällungskörper von $\mu_1 \ldots \mu_n$ mit $G := \mathrm{Gal}(L|\mathbb{Q}) = \{\sigma_1, \ldots, \sigma_s\}$. Wir betrachten analog

$$0 = \prod_{\sigma \in G} \sum_{i=1}^{n} b_i e^{\sigma(a_i)} = \sum_{1 \leq k_1,\ldots,k_s \leq n} b_{k_1} \ldots b_{k_s} e^{\sigma_1(a_{k_1}) + \cdots + \sigma_s(a_{k_s})}. \tag{A.9.2}$$

Für $\tau \in G$ existiert eine Permutation $\pi \in S_s$ mit $\tau\sigma_i = \sigma_{\pi(i)}$ für $i = 1, \ldots, s$. Es folgt

$$\tau\Big(\sum_{i=1}^{s} \sigma_i(a_{k_i})\Big) = \sum_{i=1}^{s} \sigma_{\pi(i)}(a_{k_i}) = \sum_{i=1}^{s} \sigma_i(a_{k_{\pi^{-1}(i)}})$$

und $b_{k_1} \ldots b_{k_s} = b_{k_{\pi^{-1}(1)}} \ldots b_{k_{\pi^{-1}(s)}}$. Daher operiert G auf der Menge der Exponenten in (A.9.2) und je zwei Terme in der gleichen Bahn haben den gleichen Koeffizienten. Diese Eigenschaft bleibt erhalten, wenn wir Terme mit gleichen Exponenten zusammenfassen. Für $i = 1, \ldots, s$ wählen wir $m_i \in \{1, \ldots, n\}$ mit $(\mathrm{Re}(\sigma_i(a_{m_i})), \mathrm{Im}(\sigma_i(a_{m_i}))) < (\mathrm{Re}(\sigma_i(a_l)), \mathrm{Im}(\sigma_i(a_l)))$ für alle $l \neq m_i$. Da der Exponent $\sigma_1(a_{m_1}) + \cdots + \sigma_s(a_{m_s})$ nur einmal in (A.9.2) auftritt (mit Koeffizienten $b_{m_1} \ldots b_{m_s} \neq 0$), verschwinden nicht alle Terme in (A.9.2). Wir dürfen also a_i durch $\sigma_1(a_{k_1}) + \cdots + \sigma_s(a_{k_s})$ und b_i durch $b_{k_1} \ldots b_{k_s}$ ersetzen. Anschließend hat (A.9.1) die Form

$$\sum_{i=1}^{t} b_i \sum_{j=1}^{s_i} e^{a_{ij}} = 0,$$

wobei $\{a_{ij} : j = 1, \ldots, s_i\}$ für $i = 1, \ldots, t$ die Bahnen von G auf $\{a_1, \ldots, a_n\}$ sind. Indem wir diese Gleichung mit $\sum_{j=1}^{t_1} e^{-a_{1j}}$ multiplizieren und anschließend G-Bahnen erneut aufteilen, können wir $a_{11} = 0$ und $t_1 = 1$ annehmen (wegen $a_{1j} \neq a_{ik}$ für $i > 1$ können sich die Terme e^0 nicht gegenseitig aufheben). Nach Umbenennung erhalten wir

$$b_0 + \sum_{i=1}^{t} b_i \sum_{j=1}^{s_i} e^{a_{ij}} = 0 \tag{A.9.3}$$

mit $b_0, \ldots, b_t \in \mathbb{Z} \setminus \{0\}$ und $a_{ij} \neq 0$ für alle i, j. Weiterhin sei $n = s_1 + \cdots + s_t$.

Nach Satz II.11.14 existiert ein $c \in \mathbb{N}$, sodass ca_{ij} für alle i, j ganz-algebraisch ist. Dann folgt $\alpha := c^n \prod_{i,j}(X - a_{ij}) \in \mathbb{Z}[X]$ aus Bemerkung I.8.53. Wir wählen eine Primzahl $p > \max\{c, b_0, |\alpha(0)|\}$ und definieren

$$\gamma := \frac{(cX)^{p-1}}{(p-1)!}\alpha^p \in \mathbb{Q}[X].$$

Multiplikation von (A.9.3) mit $\gamma^{(\Sigma)}(0)$ ergibt

$$b_0\gamma^{(\Sigma)}(0) + \sum_{i=1}^{t} b_i \sum_{j=1}^{s_i} \gamma^{(\Sigma)}(a_{ij}) + \sum_{i=1}^{t} b_i \sum_{j=1}^{s_i} \gamma^*(a_{ij})e^{|a_{ij}|} = 0 \tag{A.9.4}$$

nach Lemma A.9.3. Aus Lemma A.9.4 und der Wahl von p folgt

$$b_0\gamma^{(\Sigma)}(0) \equiv b_0 c^{p-1}\alpha^p(0) \not\equiv 0 \pmod{p}.$$

Ferner gilt

$$\gamma_{ij} := \gamma(X + a_{ij}) = \frac{X^p}{(p-1)!}\big(c(X + a_{ij})\big)^{p-1}\Big(c^n \prod_{(k,l)\neq(i,j)} (X + a_{ij} - a_{kl})\Big)^p = \frac{X^p}{(p-1)!}\delta_{ij},$$

wobei $\delta_{ij} \in \mathbb{C}[X]$ ganz-algebraische Koeffizienten hat (Polynome in den ca_{kl}). Andererseits ist $\sum_{j=1}^{t_i} \gamma_{ij} \in L^G[X] = \mathbb{Q}[X]$ und aus Bemerkung I.8.53 folgt $\sum_{j=1}^{t_i} \gamma_{ij} = \frac{X^p}{(p-1)!}\delta_i$ mit $\delta_i := \sum_{j=1}^{t_i} \delta_{ij} \in \mathbb{Z}[X]$. Mit der Kettenregel gilt $\gamma'_{ij} = \gamma'(X + a_{ij})$ und Lemma A.9.4 liefert

$$\sum_{j=1}^{t_i} \gamma^{(\Sigma)}(a_{ij}) = \sum_{j=1}^{t_i} \gamma_{ij}^{(\Sigma)}(0) \in p\mathbb{Z}.$$

Die Summe der ersten beiden (ganzzahligen) Summanden in (A.9.4) ist also nicht durch p teilbar und daher betragsmäßig mindestens 1.

Für ein festes $x \in \mathbb{C}$ existiert eine Konstante $C \in \mathbb{R}$ mit

$$|\gamma^*(x)| \overset{A.9.2}{\leq} \frac{(c|x|)^{p-1}}{(p-1)!}\alpha(|x|)^p \leq \frac{C^p}{(p-1)!}.$$

Wenn p groß genug ist, folgt

$$\Big|\sum_{i=1}^{t} b_i \sum_{j=1}^{s_i} \gamma^*(a_{ij})e^{|a_{ij}|}\Big| < 1.$$

Dies widerspricht (A.9.4). □

Beispiel A.9.6. Für $a_1 = 0$ und $a_2 = 1$ erhält man die Transzendenz von e. Sei $x \in \overline{\mathbb{Q}} \setminus \{0\}$. Dann ist $\cos(x)e^0 - \frac{1}{2}e^{x\mathrm{i}} - \frac{1}{2}e^{-x\mathrm{i}} = 0$. Nach Lindemann-Weierstraß ist $\cos(x)$ transzendent. Wegen $\cos(\pi) = -1 \in \mathbb{Q}$ ist π transzendent. Sei nun $x \in \overline{\mathbb{Q}} \cap \mathbb{R} \setminus \{1\}$ und $x > 0$. Dann ist $xe^0 - e^{\log(x)} = 0$ und $\log(x)$ ist transzendent.

Folgerung A.9.7. *Genau dann sind $a_1, \ldots, a_n \in \overline{\mathbb{Q}}$ linear abhängig über $\mathbb{Q}$, wenn $e^{a_1}, \ldots, e^{a_n}$ algebraisch abhängig über $\mathbb{Q}$ sind.*

Beweis. Zuerst seien $a_1, \dots, a_n$ linear abhängig, sagen wir $\sum_{i=1}^n \lambda_i a_i = 0$ für $\lambda_1, \dots, \lambda_n \in \mathbb{Q}$ (nicht alle 0). Nach Multiplikation mit dem Hauptnenner können wir $\lambda_1, \dots, \lambda_n \in \mathbb{Z}$ annehmen. Nach Umnummerierung gilt $\lambda_1, \dots, \lambda_k > 0$, $\lambda_{k+1}, \dots, \lambda_l < 0$ und $\lambda_{l+1} = \dots = \lambda_n = 0$. Es folgt

$$\prod_{i=1}^{k} (e^{a_i})^{\lambda_i} \Big(\prod_{i=k+1}^{l} (e^{a_i})^{-\lambda_i} \Big)^{-1} = e^{\lambda_1 a_1 + \dots + \lambda_n a_n} = e^0 = 1.$$

Für das Polynom $\alpha := X_1^{\lambda_1} \dots X_k^{\lambda_k} - X_{k+1}^{-\lambda_{k+1}} \dots X_l^{-\lambda_l} \in \mathbb{Q}[X_1, \dots, X_n] \setminus \{0\}$ gilt also $\alpha(e^{a_1}, \dots, e^{a_n}) = 0$. Damit sind $e^{a_1}, \dots, e^{a_n}$ algebraisch abhängig über $\mathbb{Q}$.

Nun seien $e^{a_1}, \dots, e^{a_n}$ algebraisch abhängig über $\mathbb{Q}$. Dann existiert

$$\alpha = \sum_{i_1, \dots, i_n \geq 0} \lambda_{i_1, \dots, i_n} X_1^{i_1} \dots X_n^{i_n} \in \mathbb{Q}[X_1, \dots, X_n] \setminus \{0\}$$

mit $\alpha(e^{a_1}, \dots, e^{a_n}) = 0$. Also sind die Zahlen $e^{i_1 a_1 + \dots + i_n a_n}$ mit $\lambda_{i_1, \dots, i_n} \neq 0$ linear abhängig über $\mathbb{Q}$. Nach Lindemann-Weierstraß existieren Tupel $(i_1, \dots, i_n) \neq (j_1, \dots, j_n)$ mit $i_1 a_1 + \dots + i_n a_n = j_1 a_1 + \dots + j_n a_n$. Damit sind $a_1, \dots, a_n$ linear abhängig über $\mathbb{Q}$. □

Bemerkung A.9.8.

(i) Man kann den Satz von Lindemann-Weierstraß auch aus Folgerung A.9.7 herleiten. Seien dazu $a_1, \dots, a_n \in \overline{\mathbb{Q}}$ paarweise verschiedenen. Angenommen es existieren $b_1, \dots, b_n \in \overline{\mathbb{Q}} \setminus \{0\}$ mit $\sum_{i=1}^n b_i e^{a_i} = 0$. O. B. d. A. sei $a_1, \dots, a_k$ eine $\mathbb{Q}$-Basis von $\langle a_1, \dots, a_n \rangle$. Dann existieren $\lambda_{ij} \in \mathbb{Q}$ mit $a_i = \sum_{j=1}^k \lambda_{ij} a_j$ für $i = k+1, \dots, n$. Wähle $s \in \mathbb{N}$ mit $s\lambda_{ij} \in \mathbb{Z}$ für alle i, j. Sei $s_j := \min\{0, s_{k+1,j}, \dots, s_{n,j}\} \leq 0$ für $j = 1, \dots, k$. Dann ist

$$\gamma := X_1^{-s_1} \dots X_k^{-s_k} \Big(\sum_{i=1}^{k} b_i X_i^s + \sum_{i=k+1}^{n} b_i X_1^{s_{i,1}} \dots X_k^{s_{i,k}} \Big) \in \overline{\mathbb{Q}}[X_1, \dots, X_k].$$

Da $a_{k+1}, \dots, a_n$ paarweise verschieden sind, sind die Exponententupel $(s_{i,1}, \dots, s_{i,k})$ für $i = k+1, \dots, n$ paarweise verschieden. Da diese a_i auch zu $a_1, \dots, a_k$ verschieden sind, hat keines der Tupel die Form $(0, \dots, 0, s, 0, \dots, 0)$. Die Monome in der obigen Klammer sind daher paarweise verschieden. Dies zeigt $\gamma \neq 0$. Es gilt

$$\begin{aligned} \gamma(e^{a_1/s}, \dots, e^{a_k/s}) &= e^{-(a_1 s_1 + \dots + a_k s_k)/s} \Big(\sum_{i=1}^{k} b_i e^{a_i} + \sum_{i=k+1}^{n} b_i e^{a_1 \lambda_{i1} + \dots + a_k \lambda_{ik}} \Big) \\ &= e^{-(a_1 s_1 + \dots + a_k s_k)/s} \sum_{i=1}^{n} b_i e^{a_i} = 0. \end{aligned}$$

Nach Lemma II.4.6 sind $e^{a_1/s}, \dots, e^{a_k/s}$ algebraisch abhängig über $\overline{\mathbb{Q}}$. O. B. d. A. sei $e^{a_1/s}$ algebraisch über $\overline{\mathbb{Q}}(e^{a_2/s}, \dots, e^{a_k/s})$. Aus Satz II.4.18 folgt

$$\begin{aligned} \operatorname{trg}\big(\mathbb{Q}(e^{a_1/s}, \dots, e^{a_k/s}) | \mathbb{Q}\big) &\leq \operatorname{trg}\big(\overline{\mathbb{Q}}(e^{a_1/s}, \dots, e^{a_k/s}) | \mathbb{Q}\big) = \operatorname{trg}\big(\overline{\mathbb{Q}}(e^{a_1/s}, \dots, e^{a_k/s}) | \overline{\mathbb{Q}}\big) \\ &= \operatorname{trg}\big(\overline{\mathbb{Q}}(e^{a_2/s}, \dots, e^{a_k/s}) | \overline{\mathbb{Q}}\big) \leq k - 1. \end{aligned}$$

Also sind $e^{a_1/s}, \dots, e^{a_k/s}$ algebraisch abhängig über $\mathbb{Q}$. Nach Folgerung A.9.7 wären $a_1, \dots, a_k$ linear abhängig über $\mathbb{Q}$. Dieser Widerspruch zeigt, dass $e^{a_1}, \dots, e^{a_n}$ linear unabhängig über $\overline{\mathbb{Q}}$ sind.

(ii) Die Transzendenz des Logarithmus (Beispiel A.9.6) wurde von BAKER verallgemeinert: Seien $a_1, \ldots, a_n \in \overline{\mathbb{Q}} \setminus \{0, 1\}$, sodass $\log(a_1), \ldots, \log(a_n)$ linear unabhängig über $\mathbb{Q}$ sind. Dann sind $1, \log(a_1), \ldots, \log(a_n)$ linear unabhängig über $\overline{\mathbb{Q}}$ (insbesondere sind $\log(a_1), \ldots, \log(a_n)$ transzendent). Dies hängt nicht von der konkreten Wahl des komplexen Logarithmus ab. Nehmen wir beispielsweise an, dass $a = 2^{\sqrt{2}}$ algebraisch ist. Wegen $\log(a) = \sqrt{2}\log(2)$ sind $\log(a)$ und $\log(2)$ sind linear abhängig über $\overline{\mathbb{Q}}$. Nach Baker sind $\log(a)$ und $\log(2)$ auch linear abhängig über $\mathbb{Q}$. Dann wäre aber $\sqrt{2} = \frac{\log(a)}{\log(2)} \in \mathbb{Q}$. Dieser Widerspruch, zeigt die Transzendenz von $2^{\sqrt{2}}$.

(iii) Eine offene Vermutung von SCHANUEL besagt: Sind $a_1, \ldots, a_n \in \mathbb{C}$ linear unabhängig über $\mathbb{Q}$, so ist $\operatorname{trg}(\mathbb{Q}(a_1, \ldots, a_n, e^{a_1}, \ldots, e^{a_n})|\mathbb{Q}) \geq n$. Im Fall $a_1, \ldots, a_n \in \overline{\mathbb{Q}}$ erhält man Lindemann-Weierstraß und im Fall $e^{a_1}, \ldots, e^{a_n} \in \overline{\mathbb{Q}}$ folgt der Satz von Baker.

10 Freie Moduln mit unendlichem Rang

Satz A.10.1. *Sei R ein Hauptidealring und M ein freier R-Modul. Dann ist jeder Untermodul $N \leq M$ frei mit* $\operatorname{rk} N \leq \operatorname{rk} M$.

Beweis. Sei B eine Basis von M und $N_C := \langle C\rangle \cap N$ für $C \subseteq B$. Sei $\mathcal{M}$ die Menge aller Tripel (C, Γ, f) bestehend aus einer Teilmenge $C \subseteq B$, sodass N_C frei ist mit Basis Γ und $f\colon \Gamma \to C$ ist injektive Abbildung. Wegen $(\varnothing, \varnothing, \varnothing) \in \mathcal{M}$ ist $\mathcal{M}$ nichtleer und durch

$$(C, \Gamma, f) \leq (C', \Gamma', f') :\Longleftrightarrow C \subseteq C',\ \Gamma \subseteq \Gamma',\ f'_\Gamma = f$$

geordnet. Sei $\varnothing \neq \mathcal{N} \subseteq \mathcal{M}$ total geordnet und

$$(C, \Gamma) := \Big(\bigcup_{(D,\Delta,g)\in\mathcal{N}} D,\ \bigcup_{(D,\Delta,g)\in\mathcal{N}} \Delta \Big).$$

Offenbar ist dann N_C frei mit Basis Γ. Für $\gamma \in \Gamma$ existiert $(D, \Delta, g) \in \mathcal{N}$ mit $\gamma \in \Delta$. Wir definieren $f(\gamma) := g(\gamma)$. Offenbar ist dann $g\colon \Gamma \to C$ eine wohldefinierte injektive Abbildung. Also ist $(C, \Gamma, f) \in \mathcal{M}$ eine obere Schranke von $\mathcal{N}$. Nach Zorn existiert ein maximales Element $(C, \Gamma, f) \in \mathcal{M}$. Wir nehmen $C \neq B$ an und wählen $b \in B \setminus C$. Für $C' := C \cup \{b\}$ gilt

$$N_{C'}/N_C = N_{C'}/(N_{C'} \cap \langle C\rangle) \simeq (N_{C'} + \langle C\rangle)/\langle C\rangle \leq \langle C'\rangle/\langle C\rangle \simeq Rb \simeq R.$$

Im Fall $N_{C'} = N_C$ wäre $(C', \Gamma, f) \in \mathcal{M}$ im Widerspruch zur Maximalität von (C, Γ, f). Also ist $N_{C'} \neq N_C$. Da R ein Hauptidealring ist, existiert $\delta \in N_{C'}$ mit $N_{C'}/N_C = R(\delta + N_C)/N_C \simeq R$, d. h. $N_{C'} = R\delta + N_C$. Daher ist $\Gamma' := \Gamma \cup \{\delta\}$ ein Erzeugendensystem von $N_{C'}$. Seien $r_\gamma, r_\delta \in R$ mit

$$r_\delta \delta + \sum_{\gamma\in\Gamma} r_\gamma \gamma = 0.$$

Dann ist $r_\delta \delta \in N_C$ und aus $N_{C'}/N_C \simeq R$ folgt $r_\delta = 0$. Da Γ linear unabhängig ist, ist auch $r_\gamma = 0$ für alle $\gamma \in \Gamma$. Daher ist $N_{C'}$ frei mit Basis Γ'. Schließlich lässt sich $f\colon \Gamma \to C$ zu einer injektiven Abbildung $f'\colon \Gamma' \to C'$ mit $f'(\delta) = b$ fortsetzen. Also ist $(C', \Gamma', f') \in \mathcal{M}$ im Widerspruch zur Maximalität von (C, Γ, f). Dies zeigt $C = B$ und $N = N_B$ ist frei mit Basis Γ. Die Abbildung $f\colon \Gamma \to B$ zeigt $\operatorname{rk} N = |\Gamma| \leq |B| = \operatorname{rk} M$. □

Satz A.10.2 (Baer)**.** *Die abelsche Gruppe $\mathbb{Z}^\mathbb{N} = \prod_\mathbb{N} \mathbb{Z}$ ist nicht frei.*

Beweis (Schröer). Angenommen $G := \mathbb{Z}^\mathbb{N}$ ist frei mit Basis B. Sei $e_i \in G$ mit einer 1 an Position i und sonst nur Nullen. Wir schreiben $e_i = \sum_{b\in B} \lambda_{ib} b$ mit $\lambda_{ib} \in \mathbb{Z}$. Als abzählbare Vereinigung endlicher Mengen ist

$$C := \{b \in B : \exists i \in \mathbb{N} : \lambda_{ib} \neq 0\}$$

abzählbar. Damit ist auch $H := \langle C\rangle \leq G$ abzählbar. Andererseits ist G und damit auch B überabzählbar. Außerdem ist G/H frei mit Basis $B \setminus C$. Offenbar existieren überabzählbar viele $(a_1, a_2, \ldots) \in G$ mit

$a_i \geq 2$ für $i = 1, \ldots$. Daher kann findet man gewisse a_i mit $x := (a_1, a_1a_2, \ldots) \notin H$. Seien $\lambda_b \in \mathbb{Z}$ mit $x \equiv \sum_{b \in B \setminus C} \lambda_b b \pmod{H}$. Wegen $x \notin H$ existiert ein $b' \in B \setminus C$ mit $\lambda_{b'} \neq 0$. Wegen $e_1, e_2, \ldots \in H$ gilt

$$a_1 \ldots a_i(0, \ldots, 0, a_{i+1}, a_{i+1}a_{i+2}, \ldots) \equiv x \equiv \sum_{b \in B \setminus C} \lambda_b b \pmod{H}.$$

Ein Koeffizientenvergleich liefert den Widerspruch $a_1 \ldots a_i \mid \lambda_{b'}$ für alle $i \in \mathbb{N}$. □

11 Gruppendeterminanten

Definition A.11.1. Sei G eine endliche Gruppe und $R := \mathbb{C}[X_g : g \in G]$ der Polynomring in $|G|$ Unbekannten. Man nennt $\Theta(G) := \det((X_{gh^{-1}})_{g,h\in G}) \in R$ die *Determinante* von G.

Bemerkung A.11.2.

(i) Für $\pi \in \mathrm{Sym}(G)$ gilt $(X_{\pi(g)\pi(h)^{-1}})_{g,h} = P^{-1}(X_{gh^{-1}})P$, wobei $P = (\delta_{g\pi(h)})_{g,h}$ die Permutationsmatrix von π ist. Dies zeigt, dass $\Theta(G)$ nicht von der Reihenfolge der $g \in G$ abhängt.

(ii) Nach der Leibniz-Formel ist $\Theta(G)$ ein homogenes Polynom vom Grad n und normiert in X_1, d. h. jedes Mononom von $\Theta(G)$ hat Grad n und der Koeffizient von X_1^n ist 1. Da R nach Gauß ein faktorieller Ring ist, kann man nach der Primfaktorzerlegung von $\Theta(G)$ fragen.

Lemma A.11.3. *Sei K ein unendlicher Körper und $\alpha, \beta \in K[X_1, \ldots, X_n]$ mit $\alpha(x_1, \ldots, x_n) = \beta(x_1, \ldots, x_n)$ für alle $x_1, \ldots, x_n \in K$. Dann ist $\alpha = \beta$.*

Beweis. Für $n = 1$ hat $\alpha - \beta$ unendlich viele Nullstellen und es folgt $\alpha = \beta$ aus Satz I.8.29. Sei nun $n \geq 2$ und $\alpha - \beta = \sum_{k=0}^{d} \gamma_k X_n^k$ mit $\gamma_0, \ldots, \gamma_d \in K[X_1, \ldots, X_{n-1}]$. Für alle $x_1, \ldots, x_{n-1} \in K$ hat

$$\sum_{k=0}^{d} \gamma_k(x_1, \ldots, x_{n-1}) X_n^k \in K[X_n]$$

unendlich viele Nullstellen und es folgt wieder $\gamma_k(x_1, \ldots, x_{n-1}) = 0$. Durch Induktion nach n ist $\gamma_0 = \ldots = \gamma_d = 0$ und damit $\alpha = \beta$. □

Lemma A.11.4. *Das Polynom $\det\big((X_{ij})_{i,j}\big) \in \mathbb{C}[X_{ij} : 1 \leq i, j \leq n]$ ist irreduzibel.*

Beweis. Nach der Leibniz-Formel ist $\delta := \det(X_{ij})$ linear als Polynom in X_{kl} mit Koeffizienten über dem Integritätsbereich $\mathbb{C}[X_{ij} : (i, j) \neq (k, l)]$. Sei $\delta = \alpha\beta$ mit $\alpha, \beta \in \mathbb{C}[X_{ij} : 1 \leq i, j \leq n]$. Jedes X_{kl} tritt dann entweder in α oder in β auf, denn lineare Polynome sind stets irreduzibel. O. B. d. A. trete X_{11} in α auf. Angenommen X_{1k} tritt für ein $k > 1$ in β auf. Dann gilt

$$\delta = (\alpha_0 + \alpha_1 X_{11})(\beta_0 + \beta_1 X_{1k}) = \alpha_0\beta_0 + \alpha_1\beta_0 X_{11} + \alpha_0\beta_1 X_{1k} + \alpha_1\beta_1 X_{11}X_{1k},$$

wobei X_{11} nicht in α_0 und X_{1k} nicht in β_0 auftritt. Wegen $\alpha_1\beta_1 \neq 0$ kommt $X_{11}X_{1k}$ in δ vor. Dies widerspricht aber der Leibniz-Formel. Also kommen $X_{11}, \ldots, X_{1n}$ nur in α vor. Mit dem gleichen Argument kommen $X_{1j}, \ldots, X_{nj}$ nur in α vor, denn $X_{1j}X_{kj}$ kommt für $k > 1$ nicht in δ vor. Insgesamt ist $\beta \in \mathbb{C}$ und δ ist irreduzibel. □

Lemma A.11.5. *Seien $\Delta_1, \dots, \Delta_k$ die nicht-ähnlichen irreduziblen Darstellungen von G über $\mathbb{C}$. Dann ist die Abbildung*

$$\begin{aligned}\Delta_1 \oplus \dots \oplus \Delta_k \colon \mathbb{C}G &\to \bigtimes_{i=1}^{k} \mathbb{C}^{\deg \Delta_i \times \deg \Delta_i}, \\ x &\mapsto (\Delta_i(x))_i\end{aligned}$$

ein Isomorphismus von Algebren.

Beweis. Wegen $\dim \mathbb{C}G = |G| = \sum_{i=1}^{k} \deg(\Delta_i)^2$ genügt es zu zeigen, dass $\Delta_1 \oplus \dots \oplus \Delta_k$ injektiv ist. Sei also $x \in \bigcap_{i=1}^{k} \operatorname{Ker}(\Delta_i)$. Dann liegt x auch im Kern der regulären Darstellung. Insbesondere ist $x = x \cdot 1 = 0$. □

Lemma A.11.6. *Sei $\Delta \colon G \to \mathrm{GL}(d, \mathbb{C})$ eine irreduzible Darstellung von G und*

$$(\alpha_{ij})_{i,j} := \sum_{g \in G} X_g \Delta(g) \in R^{d \times d}.$$

Dann sind die Polynome α_{ij} linear unabhängig über $\mathbb{C}$.

Beweis. Seien $c_{ij} \in \mathbb{C}$ mit $\sum_{1 \le i,j \le n} c_{ij} \alpha_{ij} = 0$. Für alle $x_g \in \mathbb{C}$ $(g \in G)$ gilt $\sum_{1 \le i,j \le n} c_{ij} \alpha_{ij}(x_g) = 0$. Nach Lemma A.11.5 ist die Fortsetzung $\Delta \colon \mathbb{C}G \to \mathbb{C}^{d \times d}$ surjektiv. Für $1 \le k, l \le n$ existiert daher ein $x := \sum x_g g \in \mathbb{C}G$ mit $(\alpha_{ij}(x_g))_{i,j} = \Delta(x) = (\delta_{ik}\delta_{jl})$. Es folgt $c_{kl} = \sum_{1 \le i,j \le n} c_{ij} \alpha_{ij}(x_g) = 0$ für $k, l = 1, \dots, n$. □

Satz A.11.7 (Frobenius)**.** *Die Primfaktorzerlegung von $\Theta(G)$ in R hat die Form*

$$\Theta(G) = \prod_{\chi \in \mathrm{Irr}(G)} \theta_\chi^{\chi(1)},$$

wobei θ_χ irreduzibel und homogen vom Grad $\chi(1)$ ist.

Beweis. Sei $n := |G|$ und $\Gamma \colon \mathbb{C}G \to \mathbb{C}^{n \times n}$ die reguläre Darstellung von G. Für $x = \sum_{g \in G} x_g g \in \mathbb{C}G$ und $h \in G$ gilt $xh = \sum_{g \in G} x_{gh^{-1}} g$. Bzgl. der kanonischen Basis G gilt daher $\Gamma(x) = (x_{gh^{-1}})_{g,h \in G}$. Andererseits ist Γ ähnlich zu $\Delta_1^{d_1} \oplus \dots \oplus \Delta_k^{d_k}$, wobei $\Delta_1, \dots, \Delta_k$ die nicht-ähnlichen irreduziblen Darstellungen von G sind und $d_i := \deg \Delta_i$ (Bemerkung II.12.39). Insbesondere gilt $\det\big((x_{gh^{-1}})_{g,h}\big) = \prod_{i=1}^{k} \det\big(\Delta_i(x)\big)^{d_i}$ für alle $(x_g)_g \in \mathbb{C}^n$. Aus Lemma A.11.3 folgt

$$\Theta(G) = \prod_{i=1}^{k} \det\Big(\sum_{g \in G} X_g \Delta_i(g)\Big)^{d_i}.$$

Sei also $\theta_i := \det\big(\sum_{g \in G} X_g \Delta_i(g)\big) \in R$ für $i = 1, \dots, k$. Nach der Leibniz-Formel ist θ_i homogen vom Grad d_i und normiert in X_1. Sei $(\alpha_{st})_{s,t} = \sum_{g \in G} X_g \Delta_i(g)$. Nach Lemma A.11.6 sind die α_{st} linear unabhängig über $\mathbb{C}$ und linear in allen X_g. Die X_g spannen einen $\mathbb{C}$-Vektorraum $V \le R$ der Dimension n auf. Wir können daher α_{st} durch $\beta_1, \dots, \beta_{n-d_i^2}$ zu einer Basis von V ergänzen. Sei F eine beliebige Bijektion zwischen $\{\alpha_{st}, \beta_j : 1 \le s,t \le d_i, j = 1, \dots, n - d_i^2\}$ und $\{X_g : g \in G\}$. Dann setzt sich F zu einem Automorphismus der $\mathbb{C}$-Algebra R fort. Unter F wird θ_i auf $\det(X_{st})$ abgebildet, wobei die $X_{st} := F(\alpha_{st}) \in \{X_g : g \in G\}$ paarweise verschieden sind. Nach Lemma A.11.4 ist $\det(X_{st})$

irreduzibel in $\mathbb{C}[X_{st} : 1 \leq s,t \leq d_i]$. Eine Zerlegung von $\det(X_{st})$ in R wäre auch eine Zerlegung in $\mathbb{C}[X_{st}]$ (Gradvergleich). Daher sind $\det(X_{st})$ und θ_i auch in R irreduzibel.

Es verbleibt zu zeigen, dass θ_i und θ_j für $i \neq j$ nicht assoziiert sind. Da alle θ_i in X_1 normiert sind, genügt es $\theta_i \neq \theta_j$ zu zeigen (beachte $R^\times = \mathbb{C}$). Sei dafür χ_i der Charakter von Δ_i. Sei $g \in G \setminus \{1\}$. Indem wir $X_h = 0$ für $h \in G \setminus \{1, g\}$ setzen, wird θ_i zu $\det(X_1^{d_i} + \Delta_i(g)X_g)$. Wieder nach der Leibniz-Formel gilt

$$\det(X_1^{d_i} + \Delta_i(g)X_g) = X_1^{d_1} + \chi_i(g)X_1^{d_i-1}X_g + \gamma,$$

wobei der Grad von X_1 in γ kleiner als d_i ist. Aus $\chi_i \neq \chi_j$ folgt nun $\theta_i \neq \theta_j$. □

Beispiel A.11.8. Für $G = C_n$ erhält man die zyklische Determinante

$$\Theta(G) = |X_{i-j \pmod n}| = \begin{vmatrix} X_0 & X_{n-1} & \cdots & X_1 \\ X_1 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & X_{n-1} \\ X_{n-1} & X_{n-2} & \cdots & X_0 \end{vmatrix}.$$

Der Beweis von Satz A.11.7 zeigt

$$\Theta(G) = \prod_{\chi \in \mathrm{Irr}(G)} \Big(\sum_{g \in G} \chi(g) X_g \Big) = \prod_{i=0}^{n-1} \Big(\sum_{j=0}^{n-1} \zeta^{ij} X_j \Big),$$

wobei $\zeta = e^{2\pi \mathrm{i}/n} \in \mathbb{C}$. Setzt man $X_1 = 1$ und $X_i = 0$ für $i \neq 1$, so erhält man die Permutationsmatrix eines n-Zyklus mit Determinante $\zeta^{0+1+\ldots+n-1} = \zeta^{n(n-1)/2} = (-1)^{n-1}$.

12 Frobenius-Schur-Indikatoren

Bemerkung A.12.1. Im Folgenden sei G eine endliche Gruppe. Es kommt häufig vor, dass der Charakter einer Darstellung $\Delta\colon G \to \mathrm{GL}(n,\mathbb{C})$ nur reelle Werte annimmt, obwohl Δ zu keiner $\mathbb{R}$-Darstellung $G \to \mathrm{GL}(n,\mathbb{R})$ ähnlich ist. Wir führen in diesem Abschnitt eine Invariante von χ ein, die angibt, ob Δ zu einer $\mathbb{R}$-Darstellung ähnlich ist. Als Anwendung erhält man eine Formel für die Anzahl der Quadratwurzeln eines Gruppenelements.

Definition A.12.2. Sei V ein $\mathbb{C}G$-Modul und $W := V \otimes V$. Nach Satz III.3.19 definiert $f\colon W \to W$, $v \otimes w \mapsto w \otimes v$ einen Homomorphismus von $\mathbb{C}G$-Moduln. Insbesondere sind

$$S^2(V) := \mathrm{Ker}(f - \mathrm{id}_W), \qquad A^2(V) := \mathrm{Ker}(f + \mathrm{id}_W)$$

$\mathbb{C}G$-Moduln. Man nennt $S^2(V)$ das *symmetrische Quadrat* und $A^2(V)$ das *alternierende Quadrat* von V. Wegen $v \otimes w = \frac{1}{2}(v \otimes w + w \otimes v) + \frac{1}{2}(v \otimes w - w \otimes v)$ ist $W = S^2(V) \oplus A^2(V)$.

Lemma A.12.3. *Sei V ein $\mathbb{C}G$-Modul mit Charakter χ. Dann hat $S^2(V)$ den Charakter $\chi_s(g) := \frac{1}{2}(\chi(g)^2 + \chi(g^2))$ und $A^2(V)$ hat den Charakter $\chi_a(g) := \frac{1}{2}(\chi(g)^2 - \chi(g^2))$ für $g \in G$.*

Beweis. Sei $b_1, \ldots, b_n$ eine Basis von V und $gb_i = \sum_{j=1}^n \lambda_{ji} b_j$ für $g \in G$ und $\lambda_{ji} \in \mathbb{C}$. Dann ist $\chi(g) = \sum_{i=1}^n \lambda_{ii}$ und $\chi(g^2) = \sum_{i,j=1}^n \lambda_{ji}\lambda_{ji}$. Außerdem ist $\{b_i \otimes b_j - b_i \otimes b_j : i < j\}$ eine Basis von $A^2(V)$ und

$$g(b_s \otimes b_t - b_t \otimes b_s) = \sum_{i,j=1}^n (\lambda_{is}\lambda_{jt} - \lambda_{it}\lambda_{js}) b_i \otimes b_j = \sum_{i<j} (\lambda_{is}\lambda_{jt} - \lambda_{jt}\lambda_{is})(b_i \otimes b_j - b_j \otimes b_i).$$

Dies zeigt

$$\chi_a(g) = \frac{1}{2}\sum_{s \neq t} (\lambda_{ss}\lambda_{tt} + \lambda_{st}\lambda_{ts}) = \frac{1}{2}(\chi(g)^2 - \chi(g^2))$$

Die Formel für $\chi_s(g)$ folgt aus $V = S^2(V) \oplus A^2(V)$. □

Definition A.12.4. Für $\chi \in \mathrm{Irr}(G)$ nennt man

$$\epsilon(\chi) := \frac{1}{|G|}\sum_{g \in G} \chi(g^2)$$

den *Frobenius-Schur-Indikator* von χ.

Bemerkung A.12.5. Offenbar ist $\theta\colon G \to \mathbb{C}$, $g \mapsto |\{x \in G : x^2 = g\}|$ eine Klassenfunktion mit

$$(\chi, \theta) = \frac{1}{|G|}\sum_{g \in G} \sum_{\substack{x \in G \\ x^2 = g}} \chi(x^2) = \frac{1}{|G|}\sum_{x \in G} \chi(x^2) = \epsilon(\chi)$$

für $\chi \in \mathrm{Irr}(G)$. Daher gilt

$$\boxed{|\{x \in G : x^2 = g\}| = \sum_{\chi \in \mathrm{Irr}(G)} \epsilon(\chi)\chi(g)}$$

für $g \in G$.

Beispiel A.12.6.

(i) Ist $\chi(1) = 1$, so ist χ ein Homomorphismus und man erhält $\epsilon(\chi) = (\chi^2, \mathbb{1}_G) = (\chi, \overline{\chi}) = 1$ falls $\chi = \overline{\chi}$ und $\epsilon(\chi) = 0$ sonst. Insbesondere ist $\epsilon(\mathbb{1}_G) = 1$.

(ii) Ist $|G|$ ungerade, so ist $G \to G$, $g \mapsto g^2$ eine Bijektion. Es folgt $\theta = \mathbb{1}_G$, d. h. $\epsilon(\chi) = 0$ für $\chi \neq \mathbb{1}_G$.

(iii) Nach Aufgabe I.26 besitzt die Quaternionengruppe $G = Q_8$ genau eine Involution. Wegen $G/G' \cong C_2^2$ besteht $\mathrm{Irr}(G)$ aus vier reellen linearen Charaktere und einem Charakter χ vom Grad 2 (Lemma II.13.42). Nach Bemerkung A.12.5 gilt

$$2 = |\{x \in G : x^2 = 1\}| = 4 + 2\epsilon(\chi)$$

und $\epsilon(\chi) = -1$.

Satz A.12.7. *Für alle $\chi \in \mathrm{Irr}(G)$ gilt $\epsilon(\chi) \in \{-1, 0, 1\}$ und*

$$\epsilon(\chi) = (\chi_s - \chi_a, \mathbb{1}_G) = \begin{cases} 0 & \textit{falls } \overline{\chi} \neq \chi, \\ 1 & \textit{falls } (\chi_s, \mathbb{1}_G) = 1, \\ -1 & \textit{falls } (\chi_a, \mathbb{1}_G) = 1. \end{cases}$$

Beweis. Nach Lemma A.12.3 gilt $0 \leq (\chi_s, \mathbb{1}_G) + (\chi_a, \mathbb{1}_G) = (\chi^2, \mathbb{1}_G) = (\chi, \overline{\chi}) \leq 1$. Daraus folgt die Behauptung. □

Bemerkung A.12.8.

(i) Sei $V = \mathbb{C}^n$ ein $\mathbb{C}G$-Modul mit Standard-Skalarprodukt $[v, w] := v^{\mathrm{t}}\overline{w} = \sum_{i=1}^n v_i\overline{w_i}$ für $v, w \in V$ (positiv definite hermitesche Sesquilinearform). Dann definiert

$$\beta(v, w) := \sum_{g \in G} [gv, gw]$$

ein G-invariantes Skalarprodukt, d. h. $\beta(gv, gw) = \beta(v, w)$ für alle $v, w \in V$ und $g \in G$. Nach dem Gram-Schmidt-Verfahren besitzt V eine Orthonormalbasis $b_1, \ldots, b_n$ bzgl. β. Sei $\Delta\colon G \to \mathrm{GL}(n, \mathbb{C})$ die Darstellung von V bzgl. $b_1, \ldots, b_n$. Für die Standardbasis $e_1, \ldots, e_n \in \mathbb{C}^n$ gilt dann

$$e_i^{\mathrm{t}}\Delta(g)^{\mathrm{t}}\overline{\Delta(g)}e_j = \beta(gb_i, gb_j) = \beta(b_i, b_j) = \delta_{ij} \qquad (1 \leq i, j \leq n).$$

Also ist $\Delta(g)$ eine unitäre Matrix, d. h. $\Delta(g)^{\mathrm{t}}\overline{\Delta(g)} = 1_n$. Jede Darstellung ist somit zu einer *unitären Darstellung*

$$G \to \mathrm{GU}(n, \mathbb{C}) := \{A \in \mathrm{GL}(n, \mathbb{C}) : A^{\mathrm{t}}\overline{A} = 1_n\}$$

ähnlich.

(ii) Sei $\beta' \colon V \times V \to \mathbb{C}$ ebenfalls ein G-invariantes Skalarprodukt. Für $v, w \in V$ sei $\beta_v(w) := \beta(v, w)$. Offenbar ist $\gamma \colon V \to V^*$, $v \mapsto \beta_v$ linear. Wegen $\beta_v(v) > 0$ für $v \neq 0$ und $\dim V = \dim V^*$ ist γ ein Isomorphismus. Analog existiert ein Isomorphismus $\gamma' \colon V \to V^*$, $v \mapsto \beta'_v$. Daher ist $\sigma := \gamma^{-1} \circ \gamma' \in \mathrm{GL}(V)$ mit

$$\beta(\sigma(v), w) = \beta_{\sigma(v)}(w) = \gamma(\sigma(v))(w) = \gamma'(v)(w) = \beta'(v, w)$$

für alle $v, w \in V$. Für $g \in G$ folgt

$$\beta(\sigma(gv), gw) = \beta'(gv, gw) = \beta'(v, w) = \beta(\sigma(v), w) = \beta(g\sigma(v), gw).$$

Daher ist $\sigma(gv) = g\sigma(v)$ und $\sigma \in \mathrm{C}_{\mathrm{GL}(V)}(\Delta(G))$. Ist V einfach, so folgt $\sigma \in \mathbb{C}^\times \mathrm{id}_V$ aus Satz II.13.47, d. h. β ist bis auf einen konstanten Faktor eindeutig bestimmt.

(iii) Wir untersuchen nun, wann eine G-invariante Bilinearform auf V existiert.

Satz A.12.9. *Sei V ein irreduzibler $\mathbb{C}G$-Modul mit Charakter χ. Dann gilt*

(1) V besitzt eine nicht-triviale symmetrische G-invariante Bilinearform genau dann, wenn $\epsilon(\chi) = 1$.

(2) V besitzt eine nicht-triviale alternierende G-invariante Bilinearform genau dann, wenn $\epsilon(\chi) = -1$.

(3) V besitzt keine nicht-triviale G-invariante Bilinearform genau dann, wenn $\epsilon(\chi) = 0$.

Beweis. Nach der universellen Eigenschaft des Tensorprodukts (Satz III.3.19) entspricht jeder G-invarianten Bilinearform $V \times V \to \mathbb{C}$ ein $\mathbb{C}G$-Homomorphismus $V \otimes V \to \mathbb{C}$. Eine nicht-triviale Bilinearform existiert also genau dann, wenn $\mathbb{1}_G$ in $\chi^2 = \chi_s + \chi_a$ vorkommt. Kommt $\mathbb{1}_G$ in χ_s vor, so entspricht ein Homomorphismus $f \colon S^2(V) \to \mathbb{C}$ einer symmetrischen Bilinearform

$$V \times V \to \mathbb{C}, \qquad (v, w) \mapsto f(v \otimes w + w \otimes v).$$

Ist umgekehrt $\beta \colon V \times V \to \mathbb{C}$ eine nicht-triviale symmetrische G-invariante Bilinearform, so ist

$$S^2(V) \to \mathbb{C}, \qquad v \otimes w + w \otimes v \mapsto \beta(v, w) + \beta(w, v) = 2\beta(v, w)$$

ein nicht-trivialer Homomorphismus, d. h. $\mathbb{1}_G$ kommt in χ_s vor. Analog beweist man die Behauptung für alternierende Bilinearformen. □

Satz A.12.10. *Für $\chi \in \mathrm{Irr}(G)$ gilt $\epsilon(\chi) = 1$ genau dann, wenn ein $\mathbb{R}G$-Modul mit Charakter χ existiert.*

Beweis. Sei V ein $\mathbb{R}G$-Modul mit Charakter χ und Basis $b_1, \ldots, b_n$. Dann ist $\hat{V} := \mathbb{C} \otimes V = \mathbb{C}b_1 + \ldots + \mathbb{C}b_n$ ein $\mathbb{C}G$-Modul mit Charakter χ (Stichwort: Skalarerweiterung). Für $v = \sum_{i=1}^n v_i b_i$ und $w = \sum_{i=1}^n w_i b_i$ in $\hat{V}$ definiert $[v, w] := \sum_{i=1}^n v_i w_i$ eine symmetrische Bilinearform auf V. Offenbar definiert

$$\beta(v, w) := \sum_{g \in G} [gv, gw] \in \mathbb{C}$$

eine symmetrische G-invariante Bilinearform. Wegen $gb_1 \in V$ für $g \in G$ gilt $\beta(b_1, b_1) > 0$. Insbesondere ist β nicht-trivial. Aus Satz A.12.9 folgt $\epsilon(\chi) = 1$.

Sei umgekehrt $\epsilon(\chi) = 1$ und V ein $\mathbb{C}G$-Modul mit Charakter χ und Basis $b_1, \ldots, b_n$. Nach Satz A.12.7 ist $\overline{\chi} = \chi$. Für $g \in G$ sei $gb_k = \sum_{j=1}^{n} (\lambda_{jk} + \mathrm{i}\mu_{jk}) b_j$ mit $\lambda_{jk}, \mu_{jk} \in \mathbb{R}$ für $j, k = 1, \ldots, n$. Dann ist $\hat{V} := \mathbb{R}b_1 + \mathbb{R}\mathrm{i}b_1 + \ldots + \mathbb{R}b_n + \mathbb{R}\mathrm{i}b_n$ ein $\mathbb{R}G$-Modul mit Charakter

$$\hat{\chi}(g) = 2 \sum_{j=1}^{n} \lambda_{jj} = \chi(g) + \overline{\chi}(g) = 2\chi(g)$$

für $g \in G$. Es genügt daher zu zeigen, dass $\hat{V}$ nicht einfach ist. Sei $f \colon \hat{V} \to V$, $\lambda b_j + \mu \mathrm{i} b_j \mapsto (\lambda + \mathrm{i}\mu) b_j$ der kanonische Isomorphismus von $\mathbb{R}$-Vektorräumen. Für $v \in \hat{V}$ und $g \in G$ gilt $f(gv) = gf(v)$ (auch wenn V kein $\mathbb{R}G$-Modul ist). Nach Satz A.12.9 existiert eine nicht-triviale symmetrische G-invariante Bilinearform $\beta \colon V \times V \to \mathbb{C}$. Durch

$$\hat{\beta} \colon \hat{V} \times \hat{V} \to \mathbb{R}, \qquad (v, w) \mapsto \mathrm{Re}\big(\beta(f(v), f(w))\big)$$

erhält man eine symmetrische G-invariante Bilinearform auf $\hat{V}$. Da β nicht-trivial ist, existieren $v, w \in V$ mit $\beta(v, w) \neq 0$. Wegen $\beta(v + w, v + w) = \beta(v, v) + 2\beta(v, w) + \beta(w, w)$ existiert $v \in V$ mit $\beta(v, v) \neq 0$. Nach Normierung gilt $\beta(v, v) = 1$ und $\beta(\mathrm{i}v, \mathrm{i}v) = -1$. Für $\hat{v} := f^{-1}(v)$ und $\hat{w} := f^{-1}(v + \mathrm{i}v)$ gilt $\hat{\beta}(\hat{v}, \hat{v}) = 1$ und

$$\hat{\beta}(\hat{w}, \hat{w}) = \mathrm{Re}\big(\beta(v, v) + 2\mathrm{i}\beta(v, v) - \beta(v, v)\big) = 0.$$

Daher ist $\hat{\beta}$ nicht-trivial und $\{v \in \hat{V} : \hat{\beta}(v, v) = 0\}$ ist ein nicht-trivialer Untermodul von $\hat{V}$. Insbesondere ist $\hat{V}$ nicht einfach. □

Beispiel A.12.11. Nach Beispiel A.12.6 und Satz A.12.10 gibt es keine treue (und damit irreduzible) Darstellung der Form $Q_8 \to \mathrm{GL}(2, \mathbb{R})$, d. h. Q_8 ist zu keiner Untergruppe von $\mathrm{GL}(2, \mathbb{R})$ isomorph (vgl. Aufgabe I.26). Andererseits ist $D_8 \leq \mathrm{GL}(2, \mathbb{R})$. Nach Aufgabe II.66 lassen sich die Frobenius-Schur-Indikatoren daher nicht aus der Charaktertafel ablesen.

Bemerkung A.12.12.

(i) Sei V ein einfacher $\mathbb{C}G$-Modul mit Charakter χ und $\epsilon(\chi) = -1$. Dann existiert eine nicht-triviale alternierende G-invariante Bilinearform $\beta \colon V \times V \to \mathbb{C}$. Da V einfach ist, ist β nicht-ausgeartet, d. h. für alle $v \in V \setminus \{0\}$ existiert ein $w \in V$ mit $\beta(v, w) \neq 0$ (anderenfalls wäre $\{v \in V : \beta(v, V) = 0\}$ ein nicht-trivialer echter Untermodul von V). Durch Induktion nach $\dim V$ lässt sich zeigen, dass V eine sogenannte *symplektische* Basis der Form $b_1, c_1, \ldots, b_n, c_n$ mit $\beta(b_i, b_j) = 0 = \beta(c_i, c_j)$ und $\beta(b_i, c_j) = \delta_{ij}$ für $i, j = 1, \ldots, n$ besitzt.[1] Insbesondere ist $\chi(1) = \dim V = 2n$ gerade.

(ii) Für den Schur-Index von $\chi \in \mathrm{Irr}(G)$ gilt $m_{\mathbb{R}}(\chi) = 2 \iff \epsilon(\chi) = -1$ (siehe Beweis von Satz A.12.10).

Satz A.12.13. *Sei V ein einfacher $\mathbb{C}G$-Modul mit Charakter χ und Basis $b_1, \ldots, b_n$. Sei $\hat{V}$ der entsprechende $\mathbb{R}G$-Modul mit Basis $b_1, \mathrm{i}b_1, \ldots, b_n, \mathrm{i}b_n$ und Charakter $\chi + \overline{\chi}$. Dann gilt*

$$\mathrm{End}_{\mathbb{R}G}(\hat{V}) \cong \begin{cases} \mathbb{R}^{2\times 2} & \text{falls } \epsilon(\chi) = 1, \\ \mathbb{C} & \text{falls } \epsilon(\chi) = 0, \\ \mathbb{H} & \text{falls } \epsilon(\chi) = -1. \end{cases}$$

[1] Siehe Satz 7.5 in meinem Skript Kombinatorische Gruppentheorie.

Beweis. Im Fall $\epsilon(\chi) = 1$ zerfällt $\hat{V}$ in zwei isomorphe absolut irreduzible $\mathbb{R}G$-Moduln mit Charakter χ (vgl. Beweis Satz A.12.10). Lemma II.7.20 und Satz II.13.47 zeigen $\mathrm{End}_{\mathbb{R}G}(\hat{V}) \cong \mathbb{R}^{2\times 2}$. Sei nun $\epsilon(\chi) = 0$, d. h. $\overline{\chi} \neq \chi$. Dann ist $\hat{V}$ einfach und $\mathrm{End}_{\mathbb{R}G}(V)$ ist eine $\mathbb{R}$-Divisionsalgebra. Anderenfalls zerfällt $\hat{V}_{\mathbb{C}}$ in zwei nicht-isomorphe einfache Moduln mit Charakter χ bzw. $\overline{\chi}$. Aus Lemma III.7.54 und Lemma II.7.20 folgt

$$\dim_{\mathbb{R}} \mathrm{End}_{\mathbb{R}G}(\hat{V}) = \dim_{\mathbb{C}} \mathrm{End}_{\mathbb{C}G}(\hat{V}_{\mathbb{C}}) = \dim_{\mathbb{C}}(\mathbb{C} \times \mathbb{C}) = 2.$$

Nach Satz III.7.24 gilt $\mathrm{End}_{\mathbb{R}G}(\hat{V}) \cong \mathbb{C}$. Sei schließlich $\epsilon(\chi) = -1$. Dann zerfällt $\hat{V}_{\mathbb{C}}$ in zwei isomorphe einfache Moduln mit Charakter $\chi = \overline{\chi}$. Also ist $\dim_{\mathbb{R}} \mathrm{End}_{\mathbb{R}G}(\hat{V}) = 4$ und $\mathrm{End}_{\mathbb{R}G}(\hat{V}) \cong \mathbb{H}$ nach Satz III.7.24. □

GAP-Befehle

Viele Rechnungen lassen sich im kostenfreien Computeralgebrasystem GAP[2] durchführen:

Objekt	Code
Division a durch d mit Rest	`QuoInt(a,d); RemInt(a,d); a mod d;`
Euklidischer Algorithmus $\mathrm{ggT}(a,b) = ax + by$	`Gcd(a,b); Gcdex(a,b);`
$\mathrm{kgV}(a,b)$	`Lcm(a,b);`
$a \in \mathbb{P}$?	`IsPrime(a);`
Primfaktorzerlegung von a	`Factors(a);`
Lösung von $ax \equiv b \pmod{d}$	`a^-1*b mod d;`
Chinesischer Restsatz	`ChineseRem([d1,d2],[a1,a2]);`
ISBN Prüfziffer	`CheckDigitISBN(n);`
$\varphi(n)$	`Phi(n);`
$\mu(n)$	`MoebiusMu(n);`
Jacobi-Symbol $\left(\frac{a}{n}\right)$	`Jacobi(a,n);`
S_n	`SymmetricGroup(n);`
A_n	`AlternatingGroup(n);`
D_{2n}	`DihedralGroup(2*n);`
Zerlegung in disjunkte Zyklen	`(1,2,3)*(3,5,1);`
$\mathrm{sgn}(a)$	`SignPerm(a);`
$G := \langle a,b \rangle$ für Permutationen a,b	`G:=Group(a,b);`
$\lvert G \rvert$	`Order(G); Size(G);`
$\lvert \langle x \rangle \rvert$	`Order(x);`
G abelsch, zyklisch?	`IsAbelian(G); IsCyclic(G);`
$H \leq G$?	`IsSubgroup(G,H);`
$\lvert G : H \rvert$	`Index(G,H);`
Hg	`RightCoset(g,H);`
$\langle U,V \rangle$ für $U,V \leq G$	`ClosureGroup(U,V);`
UV für $U,V \subseteq G$	`SetX(U,V,PROD);`
$U \cap V$	`Intersection(U,V);`
$N \trianglelefteq G$?	`IsNormal(G,N);`
G/N	`G/N;`
kanonischer Epimorphismus $G \to G/N$	`NaturalHomomorphismByNormalSubgroup(G,N);`

[2] `https://www.gap-system.org/`

Objekt	Code
Isomorphietyp von G (falls sinnvoll)	`StructureDescription(G);`
$G \cong H$?	`IsIsomorphicGroup(G,H);`
$G \times H$	`DirectProduct(G,H);`
Bahnen der G-Menge M	`Orbits(G,M);`
Konjugationsklassen von G	`ConjugacyClasses(G); Orbits(G,G);`
$k(G)$	`NrConjugacyClasses(G);`
g und h konjugiert in G?	`IsConjugate(G,g,h);`
$\mathrm{C}_G(g)$, $\mathrm{C}_G(H)$	`Centralizer(G,g); Centralizer(G,H);`
$\mathrm{N}_G(H)$	`Normalizer(G,H);`
G_x	`Stabilizer(G,x);`
$\mathrm{Z}(G)$	`Center(G);`
$P \in \mathrm{Syl}_p(G)$	`P:=SylowSubgroup(G,p);`
G einfach, auflösbar?	`IsSimple(G); IsSolvable(G);`
nicht-auflösbare Gruppen G mit $\lvert G\rvert \leq 60$	`AllGroups([1..60],IsSolvable,false);`
Kompositionsreihe von G	`CompositionSeries(G);`
$\mathrm{Aut}(G)$	`AutomorphismGroup(G);`
$\mathrm{GL}(n,q)$, $\mathrm{SL}(n,q)$	`GL(n,q); SL(n,q);`
$\mathbb{Z}$	`Integers;`
$\mathbb{Q}$	`Rationals;`
$\mathbb{F}_q$	`GF(q);`
$\mathbb{Z}/n\mathbb{Z}$	`ZmodnZ(n);`
$R^\times$	`Units(R);`
$(a,b) \trianglelefteq R$	`Ideal(R,[a,b]);`
$a = X^2 + 3X - 1 \in K[X]$	`x:=X(K,"X"); a:=x^2+3*x-1;`
Koeffizienten von a	`CoefficientsOfUnivariatePolynomial(a);`
$a(y)$ für $y \in K$	`Value(a,y);`
Nullstellen von a in K	`RootsOfPolynomial(K,a);`
$\deg a$	`Degree(a);`
$\mathrm{ggT}(a,b) = ax + by$ in $K[X]$	`Gcd(a,b); GcdRepresentation(a,b);`
$a \in K[X]$ irreduzibel?	`IsIrreducible(a);`
Primfaktorzerlegung in $K[X]$	`Factors(a);`
$I_n(q)$ (Aufgabe I.61)	`IrreduciblePolynomialsNr(n,q);`
Ableitung a'	`Derivative(a);`
Minimalpolynom von $a \in L$ über K	`MinimalPolynomial(K,a);`
$K(a)$	`Field(K,a); Field(a);`
Zerfällungskörper von $a \in K[X]$	`SplittingField(a);`
$\sqrt{a}$	`Sqrt(a);`
primitive n-te Einheitswurzel z	`z:=E(n);`
Φ_n	`CyclotomicPolynomial(Rationals,n);`

Objekt	Code
$\mathbb{Q}_n$	`CyclotomicField(Rationals,n); CF(n);`
$\mathrm{Gal}(K\|P(K))$	`GaloisGroup(K);`
$\mathrm{Gal}(a)$ für $a \in \mathbb{Q}[X]$ als Permutationsgruppe	`TransitiveGroup(Degree(a),GaloisType(a));`
Diskriminante von $a \in \mathbb{Q}[X]$	`Discriminant(a);`
Smith-Normalform von A	`SmithNormalFormIntegerMat(A);`
Frobenius-Normalform von A	`S:=RationalCanonicalFormTransform(A);;`
	`S^-1*A*S;`
Normalbasis von K über $P(K)$	`NormalBase(K);`
Gruppenalgebra KG	`GroupRing(K,G);`
Augmentationsideal $I(KG)$	`AugmentationIdeal(KG);`
Jacobson-Radikal $\mathrm{J}(KG)$	`RadicalOfAlgebra(KG);`
Artin-Wedderburn-Zerlegung von KG	`WedderburnDecomposition(KG);`
irreduzible Darstellungen von G über K	`IrreducibleRepresentations(G,K);`
Charaktertafel von G	`Display(CharacterTable(G));`
Resultante von a, b bzgl. X	`Resultant(a,b,x);`
Division von a durch b, c in $K[X_1, \ldots, X_n]$	`PolynomialReduction(a,[b,c],MonomialLexOrdering);`
Gröbnerbasis von (b, c)	`GrobnerBasis([b,c],MonomialLexOrdering);`
reduzierte Gröbnerbasis	`ReducedGrobnerBasis([b,c],MonomialGrlexOrdering);`
H_7	`LoadPackage("guava"); C:=HammingCode(3,GF(2));`
G_{24}	`ExtendedBinaryGolayCode();`
$\dim C$	`Dimension(C);`
$d(C)$	`MinimumDistance(C);`
$C^\perp$	`DualCode(C);`
$W_C(X)$	`WeightDistribution(C);`
Erzeuger-Matrix	`GeneratorMat(C);`
Kontroll-Matrix	`CheckMat(C);`
zyklische Codes	`CyclicCodes(n,GF(q));`

Stichwortverzeichnis