

LEHRBUCH

Dominik Bullach
Johannes Funk

Vorbereitungskurs Staatsexamen Mathematik

Aufgabenbereiche Algebra und Analysis
mit umfassenden Lösungen



Springer Spektrum

Vorbereitungskurs Staatsexamen Mathematik

Dominik Bullach · Johannes Funk

Vorbereitungskurs Staatsexamen Mathematik

Aufgabenbereiche Algebra und Analysis
mit umfassenden Lösungen



Springer Spektrum

Dominik Bullach
München, Deutschland

Johannes Funk
München, Deutschland

ISBN 978-3-658-18340-0
DOI 10.1007/978-3-658-18341-7

ISBN 978-3-658-18341-7 (eBook)

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

Springer Spektrum
© Springer Fachmedien Wiesbaden GmbH 2017
Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung, die nicht ausdrücklich vom Urheberrechtsgesetz zugelassen ist, bedarf der vorherigen Zustimmung des Verlags. Das gilt insbesondere für Vervielfältigungen, Bearbeitungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.
Die Wiedergabe von Gebrauchsnamen, Handelsnamen, Warenbezeichnungen usw. in diesem Werk berechtigt auch ohne besondere Kennzeichnung nicht zu der Annahme, dass solche Namen im Sinne der Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten wären und daher von jedermann benutzt werden dürften.
Der Verlag, die Autoren und die Herausgeber gehen davon aus, dass die Angaben und Informationen in diesem Werk zum Zeitpunkt der Veröffentlichung vollständig und korrekt sind. Weder der Verlag noch die Autoren oder die Herausgeber übernehmen, ausdrücklich oder implizit, Gewähr für den Inhalt des Werkes, etwaige Fehler oder Äußerungen. Der Verlag bleibt im Hinblick auf geografische Zuordnungen und Gebietsbezeichnungen in veröffentlichten Karten und Institutionsadressen neutral.

Planung: Ulrike Schmickler-Hirzebruch
Textgestaltung: Micaela Krieger-Hauwede

Gedruckt auf säurefreiem und chlorfrei gebleichtem Papier

Springer Spektrum ist Teil von Springer Nature
Die eingetragene Gesellschaft ist Springer Fachmedien Wiesbaden GmbH
Die Anschrift der Gesellschaft ist: Abraham-Lincoln-Str. 46, 65189 Wiesbaden, Germany

*Für Mama, Max und Julia.
(J. F.)*

*Meinem Bruder als Ansporn,
meiner Oma als Dank,
der Mathematik als Verneigung.
(D. B.)*

Vorwort

Liebe Leserin, lieber Leser!

Dieses Buch ist aus einem Manuskript gewachsen, das wir zu unserer eigenen Examensvorbereitung erstellt haben. Unser Ziel dabei war es, die nötige Theorie kompakt zusammenzustellen und anhand von Original-Prüfungsaufgaben typische Strategien beispielhaft aufzuzeigen und einzuüben. Was einmal klein angefangen hat, ist nun zu einem umfangreichen Buch ausgewachsen, mit dem wir dieses Wissen weitergeben wollen.

Was erwartet mich? – oder: Staatsexamen für Anfänger

Das fachliche Staatsexamen in Mathematik besteht aus den beiden vierstündigen Prüfungen „Analysis“ und „Algebra, Lineare Algebra und Elemente der Zahlentheorie“. Dabei werden jeweils drei Themen (Aufgabengruppen) zur Auswahl gestellt, von denen eines vollständig bearbeitet werden muss.

Ein Thema des Analysis-Examens besteht typischerweise aus jeweils zwei Aufgaben der Funktionentheorie und der gewöhnlichen Differentialgleichungen sowie einer Aufgabe zur reellen Analysis, während im Algebra-Examen üblicherweise neben einer Aufgabe der Linearen Algebra vier Aufgaben aus den Bereichen Gruppen-, Ring- und Körpertheorie gestellt werden.

Wie lerne ich am besten? – oder: Aufbau des Buchs

Das Buch gliedert sich in zwei Teile, die auch unserer Vorstellung einer sinnvollen Vorbereitung auf das Staatsexamen entsprechen: Im Teil I werden die notwendigen Sätze und Definitionen, die zur Bearbeitung von Aufgaben unerlässlich sind, wiederholt und anhand ausgewählter, thematisch passender Aufgaben eingeübt. Wir haben dabei versucht, die Aufgaben didaktisch zu sortieren und dafür zu sorgen, dass nur das Wissen des jeweiligen Kapitels benötigt wird – hin und wieder kommen wir jedoch nicht ohne Vorgriffe auf andere Stoffgebiete aus.

In Teil II folgen dann vollständige Jahrgänge, bei denen wir die Aufgaben aus den Staatsexamina der letzten Jahre ohne Änderungen übernommen haben. Man sollte nach Durcharbeiten des ersten Teils in der Lage sein, diese als eine Art „Ernstfalltest“ selbstständig zu bearbeiten.

Die Aufgaben haben wir soweit möglich in Originalform übernommen, in Teil I jedoch die Notation behutsam angepasst.

Dieses Buch ist kein Lehrbuch im klassischen Sinne: Die benötigte Theorie wird jeweils nur überblicksartig angerissen und sollte eigentlich bereits vertraut sein. Wer hier Lücken in seinem Wissen feststellt, sollte eines der einschlägigen Lehrbücher zur Hand nehmen, die eine ausführlichere und vollständigere Darstellung bieten. Einige Vorschläge dafür finden sich im Literaturverzeichnis.

Obwohl wir uns bemüht haben, stets vollständige Lösungen der Aufgaben zu geben, sind doch der besseren Lesbarkeit wegen und um den Rahmen dieses Buches nicht zu sprengen, hin und wieder Details ausgespart. Hier raten wir dazu, in der Prüfungssituation des Examens im Zweifelsfall immer ausführlicher zu sein.

Jede Aufgabe besitzt ein Kürzel der folgenden Bauart:

F12T3A4 ↔ Aufgabe 4 im 3. Thema des Examens vom Frühjahr 2012

Um bestimmte Aufgaben zu finden, gibt es am Ende des Buches ein eigenes Aufgabenverzeichnis.

Danksagungen – oder: Habt ihr das ganz alleine geschrieben?

Über das letzte Jahr hinweg gab es eine ganze Reihe von Leuten, die Korrektur gelesen haben, an Aufgaben mitüberlegt haben oder sich einfach nur die neuesten Entwicklungen rund um das Buch anhören mussten. Ihnen allen sind wir zu Dank verpflichtet.

Einige unserer Kommilitonen haben das Manuskript bereits während des Entstehungsprozesses für ihre Examensvorbereitung genutzt. Für das kontinuierliche Feedback, ohne das dieses Buch nicht die jetzige Qualität und Verständlichkeit hätte, danken wir Philipp Brader, Elias Codreanu, Robert Doll, Thomas Eder, Christian Geishauser, Christina Leuchter, Sandra Meier, Julia Oswald, Ida Schmid, Isabella Schmidt, Isabella von Solemacher, Marietta Wagner und Tobias Zehetner.

Weitere Testleser einzelner Teile waren die Kollegen Thomas Götzer und Martin Hofer, für deren Verbesserungsvorschläge und ausführliche Kaffepausen wir sehr dankbar sind.

Danken wollen wir auch unseren Dozenten Dr. Ralf Gerkmann und Dr. Heribert Zenk, die durch ihre Vorlesungen unsere Art, Mathematik zu treiben, geprägt haben. Sie standen uns außerdem bei Fragen, die im Laufe dieses Projekts aufgetreten sind, stets zur Verfügung.

Dieses Buch wäre außerdem nie möglich gewesen ohne die Unterstützung unserer Lektorin Ulrike Schmickler-Hirzebruch, die vom ersten Moment an an das Projekt geglaubt hat, sowie ihrer Assistentin Barbara Gerlach. Vielen Dank!

Wir hoffen, mit diesem Buch zur Verbesserung des Notendurchschnitts im Mathematik-Examen, dem Abbau der Angst vor eben jenem und der Steigerung des Bruttosozialprodukts beitragen zu können. Für Rückmeldungen und Verbesserungsvorschläge, Erfahrungsberichte und Fanpost sind wir jederzeit dankbar.

München, im April 2017

Dominik Bullach und Johannes F. Funk

Inhaltsverzeichnis

Vorwort

vii

I. Themen des Staatsexamens	1
1. Algebra: Gruppentheorie	2
1.1. Grundlagen der Gruppentheorie	2
1.2. Gruppenoperationen	14
1.3. Direkte und semidirekte Produkte	30
1.4. Sylowsätze und ihre Anwendungen	38
1.5. Auflösbare Gruppen	55
1.6. Die Symmetrische Gruppe S_n	62
2. Algebra: Ringtheorie	75
2.1. Ringe und Ideale	75
2.2. Rechnen in Restklassenringen	97
2.3. Chinesischer Restsatz und simultane Kongruenzen	106
2.4. Quadrate und Legendre-Symbol	120
2.5. Irreduzibilität von Polynomen	130
3. Algebra: Körper- und Galois-Theorie	149
3.1. Algebraische Körpererweiterungen	149
3.2. Normale und separable Erweiterungen	154
3.3. Einheitswurzeln	166
3.4. Galois-Theorie	175
3.5. Endliche Körper	206
3.6. Konstruktionen mit Zirkel und Lineal	218
4. Lineare Algebra	224
4.1. Vektorräume und Basen	224
4.2. Diagonalisierbarkeit	234
4.3. Jordan-Normalform	240
5. Analysis reeller Variablen	252
5.1. Analysis einer reellen Variablen	252
5.2. Analysis mehrerer reeller Variablen	255
6. Analysis: Funktionentheorie	270
6.1. Komplexe Differenzierbarkeit	270
6.2. Potenz- und Laurentreihen	279
6.3. Identitätssatz	300
6.4. Wichtige Sätze der Funktionentheorie	311
6.5. Integralrechnung im Komplexen	326

6.6. Der Satz von Rouché	358
6.7. Biholomorphe Abbildungen	370
7. Analysis: Differentialgleichungen	391
7.1. Elementare Lösungsmethoden skalarer Differentialgleichungen	391
7.2. Existenz- und Eindeutigkeitssätze	406
7.3. Lineare Systeme von Differentialgleichungen	425
7.4. Skalare Differentialgleichungen höherer Ordnung	450
7.5. Ebene autonome Systeme	462
7.6. Stabilitätsuntersuchungen	475
II. Prüfungsaufgaben	491
8. Algebra: Aufgabenlösungen nach Jahrgängen	492
Frühjahr 2015	492
Herbst 2015	497
Frühjahr 2016	506
Herbst 2016	525
Frühjahr 2017	541
9. Analysis: Aufgabenlösungen nach Jahrgängen	560
Frühjahr 2015	560
Herbst 2015	578
Frühjahr 2016	597
Herbst 2016	623
Frühjahr 2017	647
Literatur	669
Aufgabenverzeichnis Algebra	670
Aufgabenverzeichnis Analysis	673
Index Algebra	675
Index Analysis	677

Teil I

Themen des Staatsexamens

1. Algebra: Gruppentheorie

1.1. Grundlagen der Gruppentheorie

Definition 1.1. Eine nicht-leere Menge G heißt **Gruppe**, falls eine Verknüpfung $\cdot: G \times G \rightarrow G$ mit den folgenden Eigenschaften existiert:

- (1) Die Verknüpfung ist **assoziativ**, d. h. es gilt $g \cdot (h \cdot k) = (g \cdot h) \cdot k$ für alle $g, h, k \in G$,
- (2) es gibt ein **Neutralelement**, d. h. ein Element $e \in G$ mit $g \cdot e = e \cdot g = g$ für alle $g \in G$,
- (3) jedes Element besitzt ein **Inverses**, d. h. für alle $g \in G$ gibt es ein $h \in G$ mit $g \cdot h = h \cdot g = e$.

Das Verknüpfungssymbol \cdot wird oft auch weggelassen, außerdem werden Gruppen auch additiv geschrieben, d. h. anstatt von \cdot wird das Symbol $+$ verwendet. Das Inverse wird üblicherweise als g^{-1} bzw. $-g$ notiert, zudem sind für das Neutralelement entsprechend die Bezeichnungen 1 bzw. 0 gebräuchlich. Falls zusätzlich $g \cdot h = h \cdot g$ für alle $g, h \in G$ einer Gruppe G gilt, so wird diese als **abelsch** oder **kommutativ** bezeichnet.

Eine Gruppe in der Gruppe wird erwartbarerweise Untergruppe genannt. Eine exakte Definition lautet folgendermaßen:

Definition 1.2. Sei G eine Gruppe. Eine Menge $U \subseteq G$ wird **Untergruppe** von G genannt, falls

- (1) $e \in U$, wobei e das Neutralelement von G ist,
- (2) $u \cdot v \in U$ für alle $u, v \in U$, wobei \cdot die Gruppenverknüpfung von G bezeichnet,
- (3) $u^{-1} \in U$ für alle $u \in U$, wobei u^{-1} das Inverse von u in G ist.

Wenn U eine Untergruppe von G ist, so verwendet man dafür auch die Kurzschreibweise $U \leq G$.

Als Nächstes schicken wir die zugehörige strukturerhaltende Abbildung hinterher:

Definition 1.3. Seien G und H Gruppen. Eine Abbildung $\phi: G \rightarrow H$ heißt **Gruppenhomomorphismus**, falls $\phi(ab) = \phi(a)\phi(b)$ für alle $a, b \in G$ erfüllt ist.

Der **Kern** des Homomorphismus $\phi: G \rightarrow H$ ist $\ker \phi = \{g \in G \mid \phi(g) = e\}$, wobei e das Neutralelement von H bezeichnet. Wie bei linearen Abbildungen ist ϕ genau dann injektiv, wenn sein Kern nur aus dem Neutralelement von G besteht.

Aufgabe (Frühjahr 2015, T3A1)

Gegeben seien eine Gruppe G und drei Untergruppen $U_1, U_2, V \subseteq G$ mit der Eigenschaft $V \subseteq U_1 \cup U_2$. Zeigen Sie, dass $V \subseteq U_1$ oder $V \subseteq U_2$ gilt.

Lösungsvorschlag zur Aufgabe (Frühjahr 2015, T3A1)

Nehmen wir das Gegenteil an, d.h. $V \not\subseteq U_1$ und $V \not\subseteq U_2$. Dann gibt es $x, y \in V$ mit $x \notin U_1$ und $y \notin U_2$. Dies bedeutet $x, x^{-1} \in U_2$ und $y, y^{-1} \in U_1$. Auch das Element xy liegt in V und muss daher in U_1 oder U_2 liegen. Wäre $xy \in U_1$, so wäre auch $xxy^{-1} = x \in U_1$, was nicht sein kann. Andererseits führt auch $xy \in U_2$ zum Widerspruch $x^{-1}xy = y \in U_2$. Also muss unsere Annahme falsch gewesen sein.

Gruppen- und Elementordnung

Ist G eine Gruppe und $S \subseteq G$ eine Teilmenge, so bezeichnen wir mit $\langle S \rangle$ die (bezüglich Inklusion) kleinste Untergruppe von G , die S enthält. Wichtig ist dabei der Spezialfall einer einelementigen Menge $S = \{g\}$, denn dann ist $\langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$. Gruppen dieser Bauart werden als *zyklisch* bezeichnet.

Definition 1.4. Sei G eine Gruppe. Die *Ordnung* eines Elementes $g \in G$ ist definiert als $\text{ord } g = |\langle g \rangle|$. Die *Ordnung* der Gruppe G ist $|G|$.

Proposition 1.5. Sei G eine Gruppe mit Neutralenlement e und sei $g \in G$. Die folgenden Aussagen sind jeweils äquivalent:

Für endliche Ordnung:

- (1) $n = \text{ord } g$,
- (2) n ist die minimale Zahl mit $g^n = e$,
- (3) $g^m = e \Leftrightarrow n \mid m$,
- (4) $\langle g \rangle \cong \mathbb{Z}/n\mathbb{Z}$.

Für unendliche Ordnung:

- (1') $\text{ord } g = \infty$,
- (2') für alle $m \in \mathbb{N}$ ist $g^m \neq e$,
- (3') $\langle g \rangle \cong \mathbb{Z}$.

Aus dem Satz von Lagrange 1.7 folgt zudem, dass in einer endlichen Gruppe die Elementordnung stets die Gruppenordnung teilen muss. Daraus erhält man direkt:

Proposition 1.6 (kleiner Fermat). Sei G eine endliche Gruppe, dann gilt $g^{|G|} = e$ für jedes $g \in G$.

Umgekehrt gibt es im Allgemeinen nicht zu jedem Teiler d der Gruppenordnung n auch ein Element der Ordnung d . Richtig ist dieser Umkehrschluss jedoch im

Spezialfall zyklischer Gruppen: Sei $G = \langle g \rangle$ und d ein Teiler von $n = \text{ord } g$, dann ist $g^{n/d}$ ein Element der Ordnung d in G und $\langle g^{n/d} \rangle$ ist die eindeutige Untergruppe der Ordnung d von G , welche alle Elemente der Ordnung d von G enthält. Jede Untergruppe von G hat diese Form, insbesondere sind also Untergruppen zyklischer Gruppen selbst wieder zyklisch.

Anleitung: Euler'sche φ -Funktion

Die Anzahl der Elemente der Ordnung d in einer zyklischen Gruppe endlicher Ordnung n kann mithilfe der **Euler'schen φ -Funktion** bestimmt werden. Diese ist definiert als

$$\varphi(d) = |\{m \in \mathbb{N} \mid m \leq d, \text{ggT}(d, m) = 1\}|.$$

Falls $d \mid n$, gibt es dann genau $\varphi(d)$ Elemente der Ordnung d in G . Eine effektive Berechnung ist mithilfe der folgenden beiden Eigenschaften möglich:

- (1) Sind $l, m \in \mathbb{N}$ teilerfremd, so gilt $\varphi(l \cdot m) = \varphi(l) \cdot \varphi(m)$.
- (2) Für eine Primzahl p und $m \in \mathbb{N}$ ist $\varphi(p^m) = (p - 1)p^{m-1}$.

Aufgabe (Herbst 2010, T3A2)

- a** Zeigen Sie: Jede endlich erzeugte Untergruppe von $(\mathbb{Q}, +)$ ist zyklisch.
- b** Geben Sie eine echte nichtzyklische Untergruppe von $(\mathbb{Q}, +)$ an.

Lösungsvorschlag zur Aufgabe (Herbst 2010, T3A2)

- a** Sei $U = \langle \frac{r_1}{s_1}, \dots, \frac{r_n}{s_n} \rangle$ eine endlich erzeugte Untergruppe von \mathbb{Q} . Wir bilden den Hauptnenner der Erzeuger, d. h. die Zahl

$$s = \prod_{i=1}^n s_i.$$

Dann gilt für alle $i \in \{1, \dots, n\}$, dass $\frac{r_i s}{s_i}$ eine ganze Zahl ist und somit

$$\frac{r_i}{s_i} = \frac{r_i s}{s_i} \cdot \frac{1}{s} \in \left\langle \frac{1}{s} \right\rangle.$$

Also ist U eine Untergruppe der zyklischen Gruppe $\subseteq \langle \frac{1}{s} \rangle$ und muss damit selbst zyklisch sein.

b Betrachte die Menge

$$\mathbb{Z}_{(2)} = \left\{ \frac{r}{s} \in \mathbb{Q} \mid 2 \nmid s \right\},$$

wobei $\frac{r}{s}$ jeweils vollständig gekürzt sein soll. Diese Menge ist eine additive Untergruppe von \mathbb{Q} , denn $0 = \frac{0}{1} \in \mathbb{Z}_{(2)}$ und für $\frac{r}{s}, \frac{r'}{s'} \in \mathbb{Z}_{(2)}$ ist auch

$$\frac{r}{s} + \frac{r'}{s'} = \frac{rs' + r's}{ss'} \in \mathbb{Z}_{(2)},$$

denn weil 2 eine Primzahl ist, folgt aus $2 \nmid s$ und $2 \nmid s'$, dass $2 \nmid ss'$. Dabei spielt auch keine Rolle, ob der Bruch noch gekürzt werden kann. Außerdem ist $\frac{-r}{s} \in \mathbb{Z}_{(2)}$.

Angenommen, $\mathbb{Z}_{(2)}$ wäre zyklisch, d. h. $\mathbb{Z}_{(2)} = \langle \frac{r}{s} \rangle$ für eine gewisse rationale Zahl $\frac{r}{s} \in \mathbb{Q}$. Wegen $\frac{r}{3s} \in \mathbb{Z}_{(2)}$ muss es ein $m \in \mathbb{Z}$ geben, sodass

$$m \cdot \frac{r}{s} = \frac{r}{3s} \Leftrightarrow mr \cdot 3s = r \cdot s \Leftrightarrow 3m = 1.$$

Eine ganze Zahl m mit dieser Eigenschaft gibt es jedoch nicht.

Aufgabe (Frühjahr 2012, T2A2)

Es seien G eine endliche Gruppe und p eine Primzahl. Begründen Sie, dass die Anzahl der Elemente der Ordnung p in G durch $p - 1$ teilbar ist, d. h.

$$|\{a \in G \mid \text{ord}(a) = p\}| = (p - 1) \cdot k \quad \text{für ein } k \in \mathbb{N}.$$

Hinweis Betrachten Sie die Mengen $M_a = \{a, a^2, \dots, a^{p-1}\}$ für $a \in G$ mit $\text{ord}(a) = p$.

Lösungsvorschlag zur Aufgabe (Frühjahr 2012, T2A2)

Ein Element $a \in G$ der Ordnung p liegt in genau einer Untergruppe der Ordnung p von G : Da $\langle a \rangle$ eine Untergruppe der Ordnung p ist, liegt a zumindest in einer solchen. Ist $U \subseteq G$ eine weitere Untergruppe der Ordnung p mit $a \in U$, so haben wir automatisch $\langle a \rangle \subseteq U$. Wegen $|\langle a \rangle| = p = |U|$ folgt $\langle a \rangle = U$.

Es gibt $\varphi(p) = p - 1$ viele Elemente der Ordnung p in der Untergruppe $\langle a \rangle$. Wegen $\text{ord } e = 1$ sind diese Elemente der Ordnung p also $\langle a \rangle \setminus \{e\} = M_a$. Sei k die Anzahl der verschiedenen Untergruppen der Ordnung p von G , dann ist die Gesamtzahl der Elemente der Ordnung p in G gerade $k \cdot (p - 1)$.

Aufgabe (Frühjahr 2011, T1A2)

Sei G eine endliche Gruppe. Die Ordnung von $g \in G$ bezeichnen wir mit $\text{ord } g$. Es seien $a, b, c \in G$ mit folgenden Eigenschaften: Die Gruppe G wird von $\{a, b, c\}$ erzeugt, das Element a erzeugt das Zentrum von G , und es gilt

$$bcb^{-1}c^{-1} = a.$$

- a** Berechnen Sie $b^n cb^{-n} c^{-1}$ für alle $n \in \mathbb{N}_0$.
- b** Zeigen Sie, dass $\text{ord } a \mid \text{ord } b$.
- c** Zeigen Sie, dass $b^{\text{ord } a}$ im Zentrum von G liegt.
- d** Folgern Sie hieraus $\text{ord } b \mid (\text{ord } a)^2$.

Hinweis Das Zentrum einer Gruppe G ist die Menge aller $x \in G$ mit $xg = gx$ für alle $g \in G$.

Lösungsvorschlag zur Aufgabe (Frühjahr 2011, T1A2)

- a** Wir beweisen per vollständiger Induktion, dass für alle $n \in \mathbb{N}_0$ die Gleichung $b^n cb^{-n} c^{-1} = a^n$ gilt. Für $n = 0$ haben wir

$$b^0 cb^0 c^{-1} = cc^{-1} = 1 = a^0$$

und $bcb^{-1}c^{-1} = a$ (der Fall $n = 1$) gilt laut Angabe. Setzen wir die Aussage daher für ein n als bereits bewiesen voraus. Man berechnet nun

$$b^{n+1} cb^{-(n+1)} c^{-1} = b \cdot (b^n cb^{-n} c^{-1}) \cdot cb^{-1} c^{-1} \stackrel{(I.V.)}{=} ba^n cb^{-1} c^{-1}.$$

Da a das Zentrum erzeugt, liegt insbesondere a^n im Zentrum von G . Also ist weiter

$$ba^n cb^{-1} c^{-1} = a^n(bcb^{-1}c^{-1}) = a^n \cdot a = a^{n+1}.$$

- b** Unter Zuhilfenahme von Teil **a** entdeckt man, dass

$$a^{\text{ord } b} = b^{\text{ord } b} cb^{-\text{ord } b} c^{-1} = 1 \cdot c \cdot 1 \cdot c^{-1} = c \cdot c^{-1} = 1$$

gilt. Gemäß Proposition 1.5 folgt daraus $\text{ord } a \mid \text{ord } b$.

- c** Wiederum hilft Teil **a** weiter:

$$b^{\text{ord } a} cb^{-\text{ord } a} c^{-1} = a^{\text{ord } a} = 1 \quad \Leftrightarrow \quad b^{\text{ord } a} c = cb^{\text{ord } a}$$

Das bedeutet, dass $b^{\text{ord } a}$ mit c vertauscht. Da $b^{\text{ord } a}$ und b sowieso vertauschen und dies wegen $a \in Z(G)$ auch auf a und $b^{\text{ord } a}$ zutrifft, vertauscht

$b^{\text{ord } a}$ mit allen Erzeugern von G . Daraus folgt, dass $b^{\text{ord } a}$ sogar mit allen Elementen aus G vertauscht, d. h. $b^{\text{ord } a} \in Z(G)$.

- d) Wegen $|Z(G)| = |\langle a \rangle| = \text{ord } a$ und $b^{\text{ord } a} \in Z(G)$ haben wir laut dem kleinen Satz von Fermat 1.6, dass

$$1 = \left(b^{\text{ord } a} \right)^{\text{ord } a} = b^{(\text{ord } a)^2}.$$

Aus dieser Gleichung folgt $\text{ord } b \mid (\text{ord } a)^2$ nach den allgemeinen Eigenschaften der Elementordnung.

Aufgabe (Frühjahr 1978, T5A3)

Man beweise, dass eine Gruppe genau dann endlich ist, wenn sie nur endlich viele Untergruppen hat.

Lösungsvorschlag zur Aufgabe (Frühjahr 1978, T5A3)

„ \Rightarrow “: Da man aus einer endlichen Menge auch nur endlich viele Teilmengen bilden kann, kann eine endliche Gruppe auch nur endlich viele Untergruppen haben.

„ \Leftarrow “: Angenommen, eine solche Gruppe besäße ein Element g unendlicher Ordnung. Es wäre dann $\langle g \rangle \cong \mathbb{Z}$ eine Untergruppe mit unendlich vielen Untergruppen. Dies kann nicht sein. Es haben also alle Gruppenelemente endliche Ordnung. Hätte die Gruppe unendlich viele Elemente, könnte man nun auf folgende Weise unendlich viele Untergruppen konstruieren: Man wähle ein Gruppenelement g_1 und definiere die endliche Gruppe $U_1 = \langle g_1 \rangle$. Anschließend wähle man $g_2 \in G \setminus \{g_1\}$ und setze $U_2 = \langle g_2 \rangle$ etc. Dies liefert eine nicht-abbrechende Kette von Untergruppen – im Widerspruch dazu, dass es davon nur endlich viele gibt.

Nebenklassen und Normalteiler

Sei G eine Gruppe und $U \subseteq G$ eine Untergruppe. Eine *Linksnebenklasse* von U in G ist dann eine Menge der Form

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

wobei das Element $g \in G$ als *Repräsentant* der Nebenklasse bezeichnet wird. Im Umgang mit Nebenklassen ist es wichtig, im Hinterkopf zu behalten, dass dieser Repräsentant in aller Regel nicht eindeutig ist, sondern folgende Aussagen äquivalent sind:

- (i) $gU = hU$,
- (ii) $gU \cap hU \neq \emptyset$,
- (iii) $g \in hU$,
- (iv) $h^{-1}g \in U$.

Die Menge aller Linksnebenklassen von U in G wird als G/U notiert. Die Mächtigkeit $|G/U|$ wird meist als $(G : U)$ geschrieben und als *Index* von U in G bezeichnet.

Satz 1.7 (Lagrange). Sei G eine endliche Gruppe und U eine Untergruppe von G . Dann ist $|G| = (G : U) \cdot |U|$.

Man möchte nun gern auf G/U ebenfalls eine Gruppenstruktur definieren, indem man $gU \cdot hU = (gh)U$ setzt. Dazu muss jedoch sichergestellt werden, dass diese Definition von der Wahl der Repräsentanten g und h unabhängig ist.¹ Es stellt sich heraus, dass dies genau dann der Fall ist, wenn U ein *Normalteiler* von G ist.

Definition 1.8. Sei G eine Gruppe. Eine Untergruppe $N \subseteq G$ heißt *Normalteiler*, falls eine der folgenden äquivalenten Bedingungen erfüllt ist:

- (1) $gN = Ng$ für alle $g \in G$,
- (2) $gNg^{-1} = N$ für alle $g \in G$,
- (3) $gNg^{-1} \subseteq N$ für alle $g \in G$.

Um auszudrücken, dass N Normalteiler von G ist, verwendet man die Schreibweise $N \trianglelefteq G$.

Nützliche Aussagen:

- Jede Untergruppe U mit $(G : U) = 2$ ist ein Normalteiler von G .
- Normalteiler sind genau die Kerne von Homomorphismen: Ist $\phi: G \rightarrow H$ ein Gruppenhomomorphismus, so ist $\ker \phi \trianglelefteq G$. Umgekehrt ist jeder Normalteiler $N \trianglelefteq G$ Kern von $\pi: G \rightarrow G/N, g \mapsto gN$.

Aufgabe (Frühjahr 2014, T3A1)

Wir betrachten die komplexen (2×2) -Matrizen

$$E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad A = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}, \quad B = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad \text{und} \quad C = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

Weiter sei $G = \{\pm E, \pm A, \pm B, \pm C\}$.

- a Zeigen Sie, dass G bezüglich der Matrixmultiplikation eine Gruppe ist, die sog. *Quaternionengruppe*.
- b Bestimmen Sie alle Untergruppen von G .
- c Welche Untergruppen sind Normalteiler von G ?

¹ Man spricht dann davon, dass die Verknüpfung *wohldefiniert* ist.

Lösungsvorschlag zur Aufgabe (Frühjahr 2014, T3A1)

- a** Dass Matrixmultiplikation assoziativ ist, ist bekannt, außerdem, dass die Einheitsmatrix E das Neutralelement bezüglich dieser Verknüpfung ist. Um die Existenz von Inversen zu sehen, rechnet man zunächst nach, dass $A^2 = B^2 = C^2 = -E$. Für alle $M \in G \setminus \{E\}$ ist also $M^{-1} = -M$. Noch nerviger ist die Abgeschlossenheit unter Multiplikation nachzuweisen, hier rechnet man am besten $AB = C$ sowie $BC = A$ und $AC = -B$ nach und klappert dann die anderen Fälle ab. Je nach Laune könnte man hier noch eine Verknüpfungstabelle angeben.
- b** Wegen $|G| = 8$ muss für eine Untergruppe U von G nach dem Satz von Lagrange $|U| \in \{1, 2, 4, 8\}$ gelten. Dabei folgt aus $|U| = 1$ natürlich $U = \{E\}$ und $|U| = 8$ bedeutet $U = G$. Falls $|U| = 2$, so ist U zyklisch nach Proposition 1.13, wird also von einem Element der Ordnung 2 erzeugt. Davon gibt es nur eines in G , nämlich $-E$, wie man vermutlich während des Rechnens in Teil **a** bemerkt hat.

Die übrigen Elemente $\pm A, \pm B, \pm C$ haben samt und sonders Ordnung 4, erzeugen also die drei Untergruppen $\langle A \rangle, \langle B \rangle$ und $\langle C \rangle$ der Ordnung 4. Gäbe es eine weitere, nicht-zyklische Untergruppe der Ordnung 4, so müsste diese zumindest abelsch und damit isomorph zu $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ sein (Proposition 1.13 und Satz 1.12). Sie würde daher insbesondere 3 verschiedene Elemente der Ordnung 2 enthalten. Wie bereits erwähnt, ist aber $-E$ das einzige Element der Ordnung 2 in G .

- c** Die Untergruppen $\langle A \rangle, \langle B \rangle$ und $\langle C \rangle$ haben Index 2 und sind daher Normalteiler von G , ebenso die trivialen Gruppen $\{E\}$ und G . Tatsächlich ist auch $N = \{E, -E\}$ ein Normalteiler: Sei $M \in G \setminus N$, dann ist laut Teil **a** $M^{-1} = -M$ und $M^2 = -E$. Es folgt

$$M(\pm E)(-M) = M \cdot (\mp M) = \pm E \in N,$$

sodass $M \cdot N \cdot M^{-1} \subseteq N$ ist. Für $M \in N$ ist $M \cdot N \cdot M^{-1} \subseteq N$ klar, also gilt diese Inklusion für sämtliche $M \in G$, sodass N ein Normalteiler von G ist.

Faktorgruppen

Ist N ein Normalteiler von G , so wird wie oben bereits erwähnt G/N mittels der Verknüpfung $gN \cdot hN = (gh)N$ zu einer Gruppe, der *Faktorgruppe* G modulo N . Das Neutralelement dieser Gruppe ist die Nebenklasse N .

Satz 1.9 (Homomorphiesatz). Seien G und H Gruppen sowie $N \trianglelefteq G$ ein Normalteiler. Ist $\phi: G \rightarrow H$ ein Homomorphismus mit $N \subseteq \ker \phi$, so gibt es einen eindeutig bestimmten Homomorphismus $\bar{\phi}: G/N \rightarrow H$, sodass das nebenstehende Diagramm kommutiert und Folgendes erfüllt ist:

$$\begin{array}{ccc} G & \xrightarrow{\phi} & H \\ \pi \downarrow & \nearrow \exists! \bar{\phi} & \\ G/N & & \end{array}$$

(1) $\bar{\phi}$ ist genau dann injektiv, wenn $\ker \phi = N$,
(2) $\bar{\phi}$ ist genau dann surjektiv, wenn ϕ surjektiv ist.

Insbesondere induziert ϕ einen Isomorphismus $\bar{\phi}: G/\ker \phi \cong \text{im } \phi$.

Satz 1.10 (Isomorphiesätze). Sei G eine Gruppe.

- (1) Ist $U \subseteq G$ eine Untergruppe und $N \trianglelefteq G$ ein Normalteiler, so ist das Komplexprodukt $UN \subseteq G$ eine Untergruppe, $N \trianglelefteq UN$ und $U \cap N \trianglelefteq U$ sind Normalteiler, und es gilt

$$U/(U \cap N) \cong UN/N.$$

- (2) Sind $N, M \trianglelefteq G$ zwei Normalteiler mit $N \subseteq M \subseteq G$, so gilt auch $N \trianglelefteq M$ und $M/N \trianglelefteq G/N$ sowie

$$(G/N)/(M/N) \cong G/M.$$

Aufgabe (Frühjahr 2013, T2A1)

Zeigen Sie, dass alle Elemente der Faktorgruppe \mathbb{Q}/\mathbb{Z} endliche Ordnung besitzen. Bestimmen Sie die Elemente endlicher Ordnung in den Faktorgruppen \mathbb{R}/\mathbb{Z} und \mathbb{R}/\mathbb{Q} .

Lösungsvorschlag zur Aufgabe (Frühjahr 2013, T2A1)

Sei $\frac{a}{b} + \mathbb{Z}$ ein beliebiges Element aus \mathbb{Q}/\mathbb{Z} , wobei $\frac{a}{b}$ ein vollständig gekürzter Bruch ist. Dann ist $b \cdot (\frac{a}{b} + \mathbb{Z}) = a + \mathbb{Z} = \mathbb{Z}$, also ist die Ordnung von $\frac{a}{b} + \mathbb{Z}$ ein Teiler von b und damit insbesondere endlich.

Sei $r + \mathbb{Z}$ ein Element aus \mathbb{R}/\mathbb{Z} der Ordnung $n < \infty$. Es gilt dann

$$n \cdot (r + \mathbb{Z}) = \mathbb{Z} \Leftrightarrow nr \in \mathbb{Z}.$$

Also gibt es ein $m \in \mathbb{Z}$ mit $nr = m$ und es folgt $r = \frac{m}{n} \in \mathbb{Q}$. Umgekehrt hat jedes Element aus \mathbb{Q}/\mathbb{Z} nach dem oben Gezeigten endliche Ordnung, sodass die Elemente endlicher Ordnung in \mathbb{R}/\mathbb{Z} genau \mathbb{Q}/\mathbb{Z} sind. Genauso zeigt man, dass ein Element $r + \mathbb{Q}$ aus \mathbb{R}/\mathbb{Q} der Ordnung $n < \infty$ die Bedingung $nr \in \mathbb{Q}$ erfüllen muss. Daraus folgt dann bereits $r \in \mathbb{Q}$, d. h. $r + \mathbb{Q} = \mathbb{Q}$ und das einzige Element endlicher Ordnung in \mathbb{R}/\mathbb{Q} ist das Neutralelement.

Aufgabe (Frühjahr 2014, T2A3)

Sei G eine Gruppe. Für $h \in G$ definieren wir den Gruppenautomorphismus

$$\phi_h: G \rightarrow G, \quad g \mapsto hgh^{-1}.$$

Die Automorphismen ϕ_h mit $h \in G$ nennt man *innere Automorphismen* von G . Wir definieren

$$\text{Inn}(G) = \{\phi_h \mid h \in G\} \subseteq \text{Aut}(G)$$

und das Zentrum von G ,

$$Z(G) = \{x \in G \mid xy = yx \text{ für alle } y \in G\}.$$

- a** Zeigen Sie, dass $\text{Inn}(G)$ ein Normalteiler in $\text{Aut}(G)$ ist.
- b** Zeigen Sie, dass die Abbildung

$$\phi: G \rightarrow \text{Inn}(G), \quad h \mapsto \phi_h$$

einen Gruppenisomorphismus $G/Z(G) \rightarrow \text{Inn}(G)$ induziert.

- c** Beschreiben Sie alle Automorphismen der zyklischen Gruppe $\mathbb{Z}/7\mathbb{Z}$ mit sieben Elementen und begründen Sie, weshalb in $\mathbb{Z}/7\mathbb{Z}$ nur die Identität ein innerer Automorphismus ist.

Lösungsvorschlag zur Aufgabe (Frühjahr 2014, T2A3)

- a** Zunächst zeigen wir, dass es sich bei $\text{Inn}(G)$ um eine Untergruppe von $\text{Aut}(G)$ handelt. Dazu bemerken wir $\text{id}_G = \phi_e \in \text{Inn}(G)$, wobei e das Neutralelement von G bezeichnet. Außerdem ist $\phi_h^{-1} = \phi_{h^{-1}} \in \text{Inn}(G)$ für alle $h \in G$, denn für alle $g \in G$ gilt

$$(\phi_h \circ \phi_{h^{-1}})(g) = \phi_h(h^{-1}gh) = hh^{-1}ghh^{-1} = g = \text{id}_G(g).$$

Da g beliebig gewählt war, folgt daraus $\phi_h \circ \phi_{h^{-1}} = \text{id}_G$. Um $\phi_h^{-1} = \phi_{h^{-1}}$ zu schließen, kann man entweder genauso die umgekehrte Gleichung $\phi_{h^{-1}} \circ \phi_h = \text{id}_G$ zeigen, oder man verwendet, dass $\text{Aut}(G)$ eine Gruppe ist und deshalb das (Rechts-)Inverse eindeutig ist.

Als letzten Teil der Untergruppedefinition zeigen wir $\phi_{h_1} \circ \phi_{h_2} = \phi_{h_1 h_2}$ für alle $h_1, h_2 \in G$. Sei dazu $g \in G$, dann berechnet man

$$\phi_{h_1 h_2}(g) = (h_1 h_2)g(h_1 h_2)^{-1} = h_1 h_2 g h_2^{-1} h_1^{-1} = \phi_{h_1}(\phi_{h_2}(g)) = (\phi_{h_1} \circ \phi_{h_2})(g).$$

Sei nun $\sigma \in \text{Aut}(G)$. Wir zeigen $\sigma \text{Inn}(G) \sigma^{-1} \subseteq \text{Inn}(G)$, daraus folgt

$\text{Inn}(G) \trianglelefteq \text{Aut}(G)$. Sei $\phi_h \in \text{Inn}(G)$ und $g \in G$, dann gilt

$$\begin{aligned} (\sigma \circ \phi_h \circ \sigma^{-1})(g) &= \sigma(h\sigma^{-1}(g)h^{-1}) = \\ &= \sigma(h) \cdot (\sigma \circ \sigma^{-1})(g) \cdot \sigma(h^{-1}) = \sigma(h) \cdot g \cdot (\sigma(h))^{-1} = \phi_{\sigma(h)}(g). \end{aligned}$$

Da g beliebig gewählt war, gilt $\sigma\phi_h\sigma^{-1} = \phi_{\sigma(h)} \in \text{Inn}(G)$.

- b** Die Abbildung ϕ ist nach Definition von $\text{Inn}(G)$ surjektiv, außerdem ist sie ein Homomorphismus, denn für $h_1, h_2 \in G$ haben wir bereits in **a** gesehen, dass $\phi(h_1h_2) = \phi_{h_1h_2} = \phi_{h_1} \circ \phi_{h_2} = \phi(h_1) \circ \phi(h_2)$.

Zu zeigen bleibt daher $\ker \phi = Z(G)$, dann folgt die Aussage aus dem Homomorphiesatz.

„ \supseteq “: Sei $h \in Z(G)$ und $g \in G$, dann gilt

$$\phi(h)(g) = hg^{-1} = hh^{-1}g = g = \text{id}_G(g),$$

also ist $\phi(h) = \text{id}_G$, was gerade $h \in \ker \phi$ bedeutet.

„ \subseteq “: Sei $h \in \ker \phi$ und $g \in G$, dann ist $g = \text{id}_G(g) = \phi(h)(g) = hgh^{-1}$, also $gh = hg$ nach Umstellen der Gleichung. Da $g \in G$ beliebig war, folgt $h \in Z(G)$.

- c** Sei $\sigma \in \text{Aut}(\mathbb{Z}/7\mathbb{Z})$. Da $\mathbb{Z}/7\mathbb{Z}$ zyklisch ist, ist σ als Abbildung bereits eindeutig durch $\sigma(\bar{1})$ fest gelegt. Als Automorphismus ist σ insbesondere surjektiv, sodass wegen $\text{im } \sigma = \langle \sigma(\bar{1}) \rangle = \mathbb{Z}/7\mathbb{Z}$ dann $\sigma(\bar{1})$ ein Erzeuger von $\mathbb{Z}/7\mathbb{Z}$ sein muss. Nun ist $\mathbb{Z}/7\mathbb{Z}$ eine Gruppe von Primzahlordnung, sodass alle Gruppenelemente außer $\bar{1}$ Ordnung 7 haben und folglich Erzeuger der Gruppe sind. Dies bedeutet $\sigma(\bar{1}) \in \mathbb{Z}/7\mathbb{Z}^\times$. Sei $\bar{x} \in \mathbb{Z}/7\mathbb{Z}$, dann gilt

$$\sigma(\bar{x}) = \sigma(\bar{1} + \dots + \bar{1}) = \bar{x} \cdot \sigma(\bar{1}).$$

Wir zeigen nun umgekehrt, dass die Abbildung $\tau: \mathbb{Z}/7\mathbb{Z} \rightarrow \mathbb{Z}/7\mathbb{Z}, \bar{x} \mapsto n \cdot \bar{x}$ für alle $n \in \{1, \dots, 6\}$ ein Automorphismus ist. Dass τ ein Homomorphismus ist, ist klar. Weiter ist $\ker \tau$ eine Untergruppe von $\mathbb{Z}/7\mathbb{Z}$ und kann daher nur Ordnung 1 oder 7 haben. Wegen $\tau(\bar{1}) = \bar{n} \neq \bar{0}$ ist $\ker \tau \neq \mathbb{Z}/7\mathbb{Z}$, weswegen nur Ordnung 1 in Frage kommt. Aus $\tau(\bar{0}) = \bar{0}$ folgt daher $\ker \tau = \{\bar{0}\}$, d.h. τ ist injektiv. Als Abbildung zwischen gleichmächtigen (endlichen) Mengen ist τ damit auch bereits surjektiv.

Da $\mathbb{Z}/7\mathbb{Z}$ abelsch ist, ist $Z(\mathbb{Z}/7\mathbb{Z}) = \mathbb{Z}/7\mathbb{Z}$ und aus Teil **b** folgt, dass $\text{Inn}(\mathbb{Z}/7\mathbb{Z})$ die triviale Gruppe ist, d.h. $\text{Inn}(\mathbb{Z}/7\mathbb{Z}) = \{\text{id}\}$.

Endlich erzeugte abelsche Gruppen

Die Klassifikation endlich erzeugter abelscher Gruppen bis auf Isomorphie ist mithilfe des nächsten Satzes besonders einfach.

Satz 1.11 (Elementarteilersatz). Sei G eine endlich erzeugte abelsche Gruppe. Dann gibt es eindeutig bestimmte Zahlen $r, s \in \mathbb{N}$ sowie $\varepsilon_1, \dots, \varepsilon_s \in \mathbb{N}$ mit $\varepsilon_1 \mid \varepsilon_2 \mid \dots \mid \varepsilon_s$ und

$$G \cong \mathbb{Z}/\varepsilon_1\mathbb{Z} \oplus \dots \oplus \mathbb{Z}/\varepsilon_s\mathbb{Z} \oplus \mathbb{Z}^r.$$

Die $\varepsilon_1, \dots, \varepsilon_s$ heißen **Elementarteiler** von G , die Zahl r heißt **Rang** von G .

Unter Zuhilfenahme des Chinesischen Restsatzes gewinnt man leicht die folgende äquivalente Darstellung:

Satz 1.12 (Hauptsatz über endlich erzeugte abelsche Gruppen). Sei G eine endlich erzeugte abelsche Gruppe. Dann gibt es eindeutig bestimmte Zahlen $r, s \in \mathbb{N}$ sowie (nicht notwendigerweise verschiedene) Primzahlen p_1, \dots, p_s und $n_1, \dots, n_s \in \mathbb{N}$ mit

$$G \cong \mathbb{Z}/p_1^{n_1}\mathbb{Z} \oplus \dots \oplus \mathbb{Z}/p_s^{n_s}\mathbb{Z} \oplus \mathbb{Z}^r.$$

Weitere nützliche Aussagen sind:

Proposition 1.13. Sei G eine Gruppe und p eine Primzahl.

- (1) Ist $|G| = p$, so ist G zyklisch.
- (2) Ist $|G| = p^2$, so ist G abelsch.

Mit diesem Wissen lassen sich Gruppen kleiner Ordnung relativ einfach bestimmen:

Ord.	abelsch	nicht–abelsch
1	$\{e\}$	–
2	$\mathbb{Z}/2\mathbb{Z}$	–
3	$\mathbb{Z}/3\mathbb{Z}$	–
4	$\mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	–
5	$\mathbb{Z}/5\mathbb{Z}$	–
6	$\mathbb{Z}/6\mathbb{Z}$	S_3
7	$\mathbb{Z}/7\mathbb{Z}$	–
8	$\mathbb{Z}/8\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	D_4, Q
9	$\mathbb{Z}/9\mathbb{Z}, \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$	–
10	$\mathbb{Z}/10\mathbb{Z}$	D_5
11	$\mathbb{Z}/11\mathbb{Z}$	–
12	$\mathbb{Z}/12\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$	$D_6, A_4, \mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$

Dabei bezeichnet S_n jeweils die symmetrische Gruppe, D_n die Diedergruppe der Ordnung $2n$, A_n die alternierende Gruppe, \mathcal{Q} die Quaternionengruppe und $\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$ das semidirekte Produkt der beiden Gruppen $\mathbb{Z}/3\mathbb{Z}$ und $\mathbb{Z}/4\mathbb{Z}$ (vgl. auch den Abschnitt über semidirekte Produkte bzw. zu symmetrischen Gruppen).

1.2. Gruppenoperationen

Das Konzept einer Gruppenoperation ist im Prinzip, Äpfel und Birnen miteinander zu multiplizieren. Soll heißen: Wir wollen sinnvoll definieren, was es heißt, ein Element einer Gruppe G mit einem Element einer Menge X zu verknüpfen. Dabei kann die Menge X zwar ebenfalls eine Gruppe sein, aber auch überhaupt keine algebraische Struktur tragen wie z. B. $X = \{1, 2, 3\}$.

Was zunächst etwas fremdartig anmutet, ist im Prinzip ein bekanntes Konzept, denn ist K ein Körper und V ein K -Vektorraum, so haben wir dort mit der Skalarmultiplikation eine Verknüpfung von Körperelementen und Vektoren – in naiver Sichtweise erst einmal vollkommen unterschiedliche Objekte.

Definition 1.14. Sei G eine Gruppe und X eine beliebige Menge. Eine **Gruppenoperation** von G auf X ist eine Abbildung $\cdot: G \times X \rightarrow X$, sodass für $g, h \in G$ die Gleichungen

$$e \cdot x = x \quad \text{und} \quad (gh) \cdot x = g \cdot (h \cdot x)$$

für alle $x \in X$ erfüllt sind. Dabei bezeichnet e das Neutralelement von G .

Gruppenoperationen lassen sich aus bestimmten Homomorphismen gewinnen und umgekehrt lassen sich aus Gruppenoperationen Homomorphismen in Permutationsgruppen konstruieren, was unter anderem in Aufgaben zu den Sylowsätzen nützlich ist (vgl. Seite 44).

Proposition 1.15. Sei G eine Gruppe und X eine Menge.

(1) Ist $\cdot: G \times X \rightarrow X$ eine Gruppenoperation, so ist die Abbildung

$$G \rightarrow \text{Per}(X), \quad g \mapsto \tau_g \quad \text{mit } \tau_g: X \rightarrow X, \quad x \mapsto g \cdot x,$$

ein Gruppenhomomorphismus.

(2) Sei umgekehrt $\phi: G \rightarrow \text{Per}(X)$ ein Gruppenhomomorphismus. Dann definiert $\cdot: G \times X \rightarrow X, g \cdot x = \phi(g)(x)$ eine Gruppenoperation.

Dazu sei auch bemerkt, dass für eine n -elementige Menge X stets $\text{Per}(X) \cong S_n$ gilt.

Definition 1.16 (Bahnen und Stabilisatoren). Sei G eine Gruppe, X eine beliebige Menge und $\cdot: G \times X \rightarrow X$ eine Gruppenoperation.

(1) Die **Bahn** eines Elements $x \in X$ ist die Menge

$$G(x) = \{g \cdot x \mid g \in G\} \subseteq X.$$

(2) Der **Stabilisator** oder auch die **Isotropiegruppe** von $x \in X$ ist die Menge

$$\text{Stab}_G(x) = \{g \in G \mid g \cdot x = x\} \subseteq G.$$

Dabei handelt es sich um eine Untergruppe von G .

Die Menge aller Bahnen einer Gruppe bildet eine Zerlegung von X , d. h. zwei Bahnen sind entweder disjunkt oder bereits gleich und die Vereinigung aller Bahnen bildet wieder ganz X .

Existiert ein $a \in X$ mit $G(a) = X$, so nennt man die Operation **transitiv**. Im diesem Fall existiert also nur eine einzige Bahn, sodass die Gleichung $G(a) = X$ sogar für ein beliebiges $a \in X$ gilt.

Zwischen den Bahnen und den Stabilisatoren besteht ein weiterer bedeutender Zusammenhang. Es gilt für $g_1, g_2 \in G$ und $x \in X$ die Äquivalenz

$$\begin{aligned} g_1 \cdot x = g_2 \cdot x &\Leftrightarrow (g_2^{-1}g_1) \cdot x = x \Leftrightarrow g_2^{-1}g_1 \in \text{Stab}_G(x) \\ &\Leftrightarrow g_1 \text{Stab}_G(x) = g_2 \text{Stab}_G(x). \end{aligned}$$

Zwei Elemente in $G(x)$ stimmen also genau dann überein, wenn die zugehörigen Nebenklassen von $\text{Stab}_G(x)$ übereinstimmen. Damit gibt es genauso viele verschiedene Elemente in $G(x)$ wie es Nebenklassen von $\text{Stab}_G(x)$ in G gibt. Da die zweite Anzahl nichts anderes als der Index $(G : \text{Stab}_G(x))$ ist, haben wir soeben das folgende Lemma bewiesen.

Lemma 1.17. Sei G eine Gruppe, X eine beliebige, endliche Menge. Dann gilt

$$|G(x)| = (G : \text{Stab}_G(x)),$$

d. h. die Länge einer Bahn entspricht dem Index des zugehörigen Stabilisators. Insbesondere sind die Bahnlängen Teiler von $|G|$, falls G eine endliche Gruppe ist.

Aus den beiden Ergebnissen lässt sich eine Aussage über die Anzahl der Fixpunkte einer Operation treffen. Unter einem **Fixpunkt** versteht man dabei ein $x \in X$ mit $g \cdot x = x$ für alle $g \in G$. Fixpunkte sind damit genau die Elemente aus X , deren Bahnen Länge 1 haben.

Satz 1.18 (Bahnengleichung). Sei G eine Gruppe, die auf einer endlichen Menge X operiert. Sei weiter R ein Repräsentantensystem der Menge aller

Bahnen mit Länge > 1 und F die Menge der Fixpunkte der Operation.
Dann gilt

$$|X| = |F| + \sum_{x \in R} (G : \text{Stab}_G(x)).$$

Aufgabe (Herbst 2010, T3A1)

Eine Gruppe der Ordnung 91 operiere auf einer Menge mit 71 Elementen. Zeigen Sie: Die Operation hat einen Fixpunkt.

Lösungsvorschlag zur Aufgabe (Herbst 2010, T3A1)

Wir bezeichnen die Gruppe mit G und die Menge mit X . Sei weiter R ein Repräsentantensystem der Bahnen mit Länge > 1. Laut der Bahnengleichung gilt (mit den Bezeichnungen aus Satz 1.18):

$$|X| = |F| + \sum_{x \in R} (G : \text{Stab}_G(x)) \Leftrightarrow 71 = |F| + \sum_{x \in R} (G : \text{Stab}_G(x))$$

Für $x \in R$ ist $(G : \text{Stab}_G(x))$ ein Teiler der Gruppenordnung 91. Dabei ist $(G : \text{Stab}_G(x)) = 1$ ausgeschlossen, da x sonst ein Fixpunkt wäre – Widerspruch zur Definition von R . $(G : \text{Stab}_G(x)) = 91$ ist nicht möglich, da die Bahn von x sonst $91 > 71 = |X|$ Elemente hätte. Also ist $(G : \text{Stab}_G(x)) \in \{7, 13\}$. Nehmen wir ferner an, dass $|F| = 0$ ist. Es gibt dann Zahlen $m, n \in \mathbb{N}_0$, sodass

$$|X| = |F| + 13m + 7n \Leftrightarrow 71 = 13m + 7n. \quad (\star)$$

Betrachten wir diese Gleichung modulo 7, so ergibt sich

$$1 \equiv 6m \pmod{7} \Leftrightarrow 1 \equiv -m \pmod{7} \Leftrightarrow m \equiv -1 \equiv 6 \pmod{7}.$$

Da 6 die kleinste natürliche Zahl mit $m \equiv 6 \pmod{7}$ ist, haben wir damit $m \geq 6$. Da aber bereits $13 \cdot 6 = 78 > 71$ gilt, existiert keine Lösung der Gleichung (\star) über den natürlichen Zahlen. Somit muss $|F| \neq 0$ sein und es gibt mindestens einen Fixpunkt.

Aufgabe (Herbst 2013, T3A4)

Sei p eine Primzahl, $e, n \in \mathbb{N}$ und G eine Untergruppe von $\text{GL}_n(\mathbb{F}_p)$ mit p^e Elementen. Zeigen Sie: Es gibt einen Spaltenvektor $0 \neq v \in \mathbb{F}_p^n$ mit $\gamma \cdot v = v$ für alle $\gamma \in G$.

Hinweis Betrachten Sie die Bahnlängen von G auf \mathbb{F}_p^n .

Lösungsvorschlag zur Aufgabe (Herbst 2013, T3A4)

Wir lassen G mittels

$$G \times \mathbb{F}_p^n \rightarrow \mathbb{F}_p^n, \quad (\gamma, v) \mapsto \gamma v$$

auf \mathbb{F}_p^n operieren. Betrachte die zugehörige Bahnengleichung

$$|\mathbb{F}_p^n| = |F| + \sum_{r \in R} (G : \text{Stab}_G(r)),$$

wobei F die Menge der Fixpunkte dieser Operation und R ein Repräsentantenstystem der Bahnen von Länge > 1 bezeichnet. Jeder der Summanden $(G : \text{Stab}_G(r))$ ist nach dem Satz von Lagrange ein Teiler von $|G| = p^e$ und deshalb selbst eine p -Potenz. Nach Definition von R ist zudem $(G : \text{Stab}_G(r)) > 1$, sodass

$$|F| = |\mathbb{F}_p^n| - \sum_{r \in R} (G : \text{Stab}_G(r))$$

von p geteilt wird. Da der Nullvektor ein Fixpunkt der Operation ist, ist F nicht-leer. Daraus bereits folgt $|F| \geq p$, sodass es neben dem Nullvektor einen weiteren Vektor $v \in F$ geben muss. Nach Definition der Operation ist dann $\gamma v = v$ für alle $\gamma \in G$.

Aufgabe (Herbst 2013, T2A2)

Die endliche Gruppe G operiere (von links) auf der endlichen Menge X . Für jedes $\sigma \in G$ bezeichne $\iota(\sigma) := |\{x \in X \mid \sigma x = x\}|$ die Anzahl der Fixpunkte von σ . Zeigen Sie, dass sich die Anzahl der Bahnen der Operation zu

$$|G \setminus X| = \frac{1}{|G|} \sum_{\sigma \in G} \iota(\sigma)$$

berechnet.

Hinweis Bestimmen Sie die Kardinalität der Teilmenge

$$Z := \{(\sigma, x) \in G \times X \mid \sigma x = x\} \subseteq G \times X$$

auf zwei verschiedene Arten.

Lösungsvorschlag zur Aufgabe (Herbst 2013, T2A2)

Es bezeichne $\text{Stab}_G(x)$ den Stabilisator von x in G und $G(x)$ die Bahn von x . Dem Hinweis folgend bestimmen wir die Kardinalität von Z :

$$\begin{aligned} |Z| &= |\{(\sigma, x) \in G \times X \mid \sigma x = x\}| = \\ &= \left| \bigcup_{\sigma \in G} \{(\sigma, x) \mid x \in X, \sigma \cdot x = x\} \right| = \sum_{\sigma \in G} \iota(\sigma) \end{aligned} \quad (*)$$

Dabei wurde im letzten Schritt verwendet, dass es sich um eine disjunkte Vereinigung handelt. Analog ergibt sich

$$\begin{aligned} |Z| &= |\{(\sigma, x) \in G \times X \mid \sigma \in \text{Stab}_G(x)\}| = \\ &= \left| \bigcup_{x \in X} \{(\sigma, x) \mid \sigma \in G, \sigma \in \text{Stab}_G(x)\} \right| = \sum_{x \in X} |\text{Stab}_G(x)|. \end{aligned}$$

Aufgrund von Lemma 1.17 gilt für $x \in X$

$$(G : \text{Stab}_G(x)) = |G(x)| \Leftrightarrow |\text{Stab}_G(x)| = \frac{|G|}{|G(x)|}.$$

Sei nun R ein Repräsentantensystem der Bahnen, dann erhalten wir

$$\begin{aligned} \sum_{x \in X} |\text{Stab}_G(x)| &= \sum_{x \in X} \frac{|G|}{|G(x)|} = |G| \cdot \sum_{r \in R} \sum_{x \in G(r)} \frac{1}{|G(x)|} = \\ &= |G| \cdot \sum_{r \in R} \sum_{x \in G(r)} \frac{1}{|G(r)|} = |G| \cdot \sum_{r \in R} \frac{|G(r)|}{|G(r)|} = \\ &= |G| \cdot \sum_{r \in R} 1 = |G| \cdot |R| = |G| \cdot |G \setminus X|. \end{aligned}$$

Gleichsetzen mit $(*)$ liefert dann

$$\sum_{\sigma \in G} \iota(\sigma) = |G| \cdot |G \setminus X| \Leftrightarrow |G \setminus X| = \frac{1}{|G|} \sum_{\sigma \in G} \iota(\sigma).$$

Konjugation und Klassengleichung

Eine wichtige Operation einer Gruppe G auf sich selbst ist die **Konjugation**, also die Abbildung

$$G \times G \rightarrow G, \quad (g, h) \mapsto ghg^{-1}.$$

Ist $h \in G$ ein Fixpunkt dieser Operation, so gilt für alle $g \in G$

$$ghg^{-1} = h \Leftrightarrow gh = hg,$$

d. h. das Element h kommutiert mit allen Elementen der Gruppe. Man bezeichnet die Menge dieser Fixpunkte als **Zentrum** von G , notiert als $Z(G)$. Das Zentrum ist stets ein Normalteiler der jeweiligen Gruppe. Der Stabilisator eines Elements h ist im Spezialfall der Konjugation gegeben durch

$$C(h) = \{g \in G \mid ghg^{-1} = h\} = \{g \in G \mid gh = hg\}.$$

Dies ist somit die Menge aller Elemente, die mit h kommutieren, genannt **Zentralisator** von h in G . Die Bahnengleichung wird mit diesen neuen Notationen zu

$$|G| = |Z(G)| + \sum_{h \in R} (G : C(h))$$

und meist als **Klassengleichung** bezeichnet. Dabei steht R wie zuvor für ein Repräsentantensystem der Bahnen mit Länge > 1 .

Eine elementare Folgerung aus der Klassengleichung ist das folgende Lemma:

Lemma 1.19. Für p -Gruppen (also Gruppen G mit Ordnung p^n für eine Primzahl p und $n \in \mathbb{N}$) ist das Zentrum $Z(G)$ nicht trivial, d. h. $|Z(G)| > 1$.

Der Index $(G : C(h))$ ist für jedes $h \in G$ nämlich ein Teiler von $|G| = p^n$, also wiederum eine Potenz von p . Falls $h \notin Z(G)$, so ist zudem $C(h) \subsetneq G$, sodass $(G : C(h)) > 1$. Falls $|Z(G)| = 1$ wäre, so würde die Klassengleichung also

$$p^n = 1 + \sum_{h \in R} (G : C(h)) \Leftrightarrow 1 = p^n - \sum_{h \in R} (G : C(h))$$

lauten. Dadurch hätten wir aber 1 als Summe von Potenzen von p ausgedrückt, sodass p ein Teiler von 1 wäre. Dies ist natürlich nicht der Fall.

Aufgabe (Frühjahr 2012, T1A1)

Das Zentrum einer Gruppe G ist die Menge $Z(G) = \{a \in G \mid \forall b \in G : a \cdot b = b \cdot a\}$. Bestimmen Sie das Zentrum der orthogonalen Gruppe $\mathcal{O}(2, \mathbb{R}) = \{A \in \mathrm{GL}_2(\mathbb{R}) \mid A^t A = \mathbb{E}_2\}$ über den reellen Zahlen.

Lösungsvorschlag zur Aufgabe (Frühjahr 2012, T1A1)

Sei $\begin{pmatrix} e & f \\ g & h \end{pmatrix} \in \mathcal{O}(2, \mathbb{R})$ eine Matrix aus dem Zentrum von $\mathcal{O}(2, \mathbb{R})$. Da auch die Matrizen $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ und $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ in der orthogonalen Gruppe liegen, kommutiert die vorgegebene Matrix insbesondere mit diesen beiden Matrizen.

zen, was folgende Gleichungen liefert:

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} g & h \\ e & f \end{pmatrix} \stackrel{!}{=} \begin{pmatrix} f & e \\ h & g \end{pmatrix} = \begin{pmatrix} e & f \\ g & h \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Man liest daraus $g = f$ und $e = h$ ab. Weiterhin muss gelten:

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \cdot \begin{pmatrix} e & f \\ f & e \end{pmatrix} = \begin{pmatrix} e & f \\ -f & -e \end{pmatrix} \stackrel{!}{=} \begin{pmatrix} e & -f \\ f & -e \end{pmatrix} = \begin{pmatrix} e & f \\ f & e \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Man erhält $f = -f$, also $f = 0$. Da wir eine Matrix aus $\mathcal{O}(2, \mathbb{R})$ suchen, muss wegen

$$\begin{pmatrix} e & 0 \\ 0 & e \end{pmatrix} \cdot \begin{pmatrix} e & 0 \\ 0 & e \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

zusätzlich $e^2 = 1$ sein. Es kommen somit nur die Matrizen

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

in Frage und man überprüft unmittelbar, dass diese auch mit allen Matrizen in $\mathcal{M}(2, \mathbb{R})$ vertauschen, also insbesondere denen aus $\mathcal{O}(2, \mathbb{R})$.

Aufgabe (Herbst 2001, T1A1)

Es sei p eine Primzahl und G eine Gruppe der Ordnung $p^n, n \geq 2$. $C(g)$ sei der Zentralisator eines Elements $g \in G$. Zeigen Sie:

$$|C(g)| > p.$$

Lösungsvorschlag zur Aufgabe (Herbst 2001, T1A1)

Sei $g \in G$. Ist $h \in Z(G)$, so gilt insbesondere $gh = hg$. Also ist $Z(G) \subseteq C(g)$. Da das Zentrum von p -Gruppen nicht-trivial ist, nach dem Satz von Lagrange also mindestens p Elemente hat, folgt $|C(g)| \geq p$. Nehmen wir nun an, es gilt $|C(g)| = p$. Dann muss bereits $Z(G) = C(g)$ sein, insbesondere also $g \in Z(G)$. Daraus folgt aber $gh = hg$ für alle $h \in G$, also ist $C(g) = G$ und somit $|G| = |C(g)| = p$, im Widerspruch zu $|G| = p^n$ mit $n \geq 2$.

Aufgabe (Frühjahr 2000, T3A2)

Zeigen Sie, dass eine endliche Gruppe mit einem Normalteiler, dessen Ordnung gleich dem kleinsten Primteiler ihrer Ordnung ist, ein nicht-triviales Zentrum hat.

Hinweis Man betrachte die Operation der Gruppe auf dem Normalteiler durch Konjugation.

Lösungsvorschlag zur Aufgabe (Frühjahr 2000, T3A2)

Sei G die Gruppe und N der besagte Normalteiler. Dem Hinweis folgend, lassen wir G durch Konjugation auf N operieren. Diese Operation ist wohldefiniert, da aufgrund der Normalteiler-Eigenschaft $g \cdot n = gng^{-1} \in N$ ist. Betrachten wir nun die zugehörige Bahnengleichung:

$$|N| = |F| + \sum_{g \in R} (G : \text{Stab}_G(g))$$

Dabei bezeichnet F die Fixpunktmenge der Operation, $\text{Stab}_G(g)$ den Stabilisator von g in G und R ein Repräsentantensystem der Bahnen von Länge > 1 . Wegen $1 \in F$ ist auf jeden Fall $|F| \geq 1$. Nehmen wir nun $R \neq \emptyset$ an, dann gibt es ein $g \in G$ mit $(G : \text{Stab}_G(g)) \geq 2$. Nach dem Satz von Lagrange ist $(G : \text{Stab}_G(g))$ ein Teiler von $|G|$, nach Voraussetzung also mindestens gleich $|N|$. Damit erhalten wir

$$|N| = |F| + \sum_{g \in R} (G : \text{Stab}_G(g)) \geq 1 + |N|,$$

was ein Widerspruch ist. Folglich gilt $R = \emptyset$ und damit $N = F$. Das bedeutet, dass für vorgegebenes $n \in N$ und jedes $g \in G$ dann

$$gng^{-1} = n \Leftrightarrow gn = ng \Leftrightarrow n \in Z(G)$$

gilt. Also liegt N im Zentrum $Z(G)$ von G , das insbesondere nicht-trivial sein muss.

Die genau gleiche Idee führt auch in der nächsten Aufgabe zum Erfolg.

Aufgabe (Frühjahr 2010, T3A4)

Es sei p eine Primzahl, G eine endliche p -Gruppe und N ein Normalteiler in G der Ordnung p . Zeigen Sie, dass N im Zentrum von G liegt.

Lösungsvorschlag zur Aufgabe (Frühjahr 2010, T3A4)

Wir betrachten die Operation

$$G \times N \rightarrow N, \quad g \cdot n = gng^{-1}$$

durch Konjugation von G auf N . Diese ist wohldefiniert, da N Normalteiler ist und somit $g \cdot n = gng^{-1} \in N$ für $g \in G$ erfüllt ist. Es gilt gemäß der Klassengleichung

$$|N| = |F| + \sum_{g \in R} (G : \text{Stab}_G(g)),$$

wobei wiederum F die Fixpunktmenge der Operation, $\text{Stab}_G(g)$ der Stabilisator von g in G und R ein Repräsentantensystem der Bahnen der Länge > 1 ist. Nehmen wir an, es gibt ein $g \in N$, das kein Fixpunkt ist, d. h. es gilt $|G(g)| > 1$. Laut Satz von Lagrange ist $(G : \text{Stab}_G(g))$ ein Teiler von $|G|$, muss also mindestens p sein. Damit aber folgt

$$p \geq 1 + p,$$

ein Widerspruch. Damit ist jedes $n \in N$ ein Fixpunkt, d. h. es gilt für alle $g \in G, n \in N$

$$g \cdot n = g \Leftrightarrow gng^{-1} = n \Leftrightarrow gn = ng$$

und somit $n \in Z(G)$.

Aufgabe (Herbst 2010, T2A3)

Die Automorphismengruppe $\text{Aut}(G)$ einer Gruppe G sei zyklisch. Zeigen Sie, dass G abelsch ist.

Lösungsvorschlag zur Aufgabe (Herbst 2010, T2A3)

Sei e das Neutralelement von G . Für jedes $g \in G$ definiere $\sigma_g: G \rightarrow G, a \mapsto gag^{-1}$. Es ist σ_g offensichtlich ein Gruppenhomomorphismus, der wegen

$$a \in \ker(\sigma_g) \Leftrightarrow \sigma_g(a) = e \Leftrightarrow gag^{-1} = e \Leftrightarrow a = g^{-1}g = e$$

injektiv ist. Außerdem ist σ_g surjektiv, denn als Urbild eines beliebigen $a \in G$ kann man $g^{-1}ag$ wählen. Definiere nun eine Abbildung

$$\phi: G \rightarrow \text{Aut}(G), \quad g \mapsto \sigma_g.$$

Auch ϕ ist ein Gruppenhomomorphismus, denn für $g, h, a \in G$ gilt

$$\begin{aligned}\phi(gh)(a) &= \sigma_{gh}(a) = (gh) \cdot a \cdot (gh)^{-1} = gh \cdot a \cdot h^{-1}g^{-1} = \\ &= g \cdot (hah^{-1}) \cdot g^{-1} = \sigma_g(\sigma_h(a)) = (\phi(g) \circ \phi(h))(a)\end{aligned}$$

und damit $\phi(gh) = \phi(g) \cdot \phi(h)$. Der Kern von ϕ ist gerade das Zentrum von G :

$$\sigma_g = \text{id} \Leftrightarrow \forall a \in G : gag^{-1} = a \Leftrightarrow \forall a \in G : ga = ag \Leftrightarrow g \in Z(G)$$

Nach dem Homomorphiesatz ist daher $G/Z(G)$ zu einer Untergruppe von $\text{Aut}(G)$ isomorph, ist also ebenfalls zyklisch. Aus diesem Grund gibt es ein $a \in G$ mit

$$G/Z(G) = \langle aZ(G) \rangle = \langle a \rangle Z(G).$$

Seien nun $g, h \in G$ beliebig, dann finden wir $n, m \in \mathbb{Z}$ und $z, z' \in Z(G)$ mit

$$g = a^n \cdot z \quad \text{und} \quad h = a^m \cdot z'.$$

Da Elemente des Zentrums nach Definition mit allen anderen Gruppenelementen vertauschen, erhalten wir

$$\begin{aligned}g \cdot h &= (a^n \cdot z) \cdot (a^m \cdot z') = z \cdot a^n \cdot a^m \cdot z' = z \cdot a^{n+m} \cdot z' = \\ &= z' \cdot a^{m+n} \cdot z = z' \cdot a^m \cdot a^n \cdot z = (z' \cdot a^m) \cdot (z \cdot a^n) = h \cdot g.\end{aligned}$$

Also ist G abelsch.

Aufgabe (Herbst 2008, T1A2)

Sei G eine endliche Gruppe.

- a** Sei $Z(G)$ das Zentrum von G . Zeigen Sie: Ist $G/Z(G)$ zyklisch, so ist G abelsch.
- b** Es operiere G transitiv auf einer Menge $|M| > 2$. Zeigen Sie, dass es ein $g \in G$ gibt mit $gm \neq m$ für alle $m \in M$.

Lösungsvorschlag zur Aufgabe (Herbst 2008, T1A2)

- a** Seien $g, h \in G$ und $a \in G$ so gewählt, dass die Nebenklasse $aZ(G)$ die Gruppe $G/Z(G)$ erzeugt. Zu zeigen ist die Gleichung $gh = hg$. Da $aZ(G)$ ein Erzeuger von $G/Z(G)$ ist, existieren $m, n \in \mathbb{N}$ mit $gZ(G) = a^m Z(G)$ und $hZ(G) = a^n Z(G)$. Insbesondere erhalten wir so Darstellungen

$$g = a^m z \quad \text{und} \quad h = a^n z' \quad \text{für } z, z' \in Z(G).$$

Die Elemente z und z' liegen im Zentrum und kommutieren somit mit jedem Element der Gruppe. Daraus folgt die Gleichung

$$gh = a^m z a^n z' = a^{m+n} z z' = a^n a^m z z' = a^n z' a^m z = hg.$$

- b** Die folgende Lösung ist etwas technisch und kommt selbst dem geübten Leser wohl nicht sofort in den Sinn – sie ist dennoch die Mühe wert, denn Aufgaben diesen Typs sind schon wiederholt aufgetaucht!

1. Schritt: Widerspruchsannahme. Nehmen wir an, ein solches Element existiert nicht. Das bedeutet, dass es für alle $g \in G$ ein Element $m \in M$ gibt mit $gm = m$. Es gilt dann $g \in \text{Stab}_G(m)$, wobei $\text{Stab}_G(m)$ den Stabilisator von m bezeichnet. Damit ist

$$G = \bigcup_{m \in M} \text{Stab}_G(m).$$

2. Schritt: G ist Vereinigung von Konjugierten eines Stabilisators. Wir betrachten nun die Stabilisatoren näher. Da die Gruppenoperation transitiv ist, existiert ein $a \in M$ mit $G(a) = M$. Ist also $m \in M$ beliebig, so existiert ein $h \in G$ mit $m = h \cdot a$. Es gilt dann

$$\begin{aligned} g \in \text{Stab}_G(m) &\Leftrightarrow g \cdot m = m \Leftrightarrow g \cdot h \cdot a = h \cdot a \\ &\Leftrightarrow (h^{-1}gh) \cdot a = a \Leftrightarrow h^{-1}gh \in \text{Stab}_G(a) \Leftrightarrow g \in h\text{Stab}_G(a)h^{-1}. \end{aligned}$$

Alle Stabilisatoren sind also zueinander konjugiert und wir können die Vereinigungsmenge von oben auch als Vereinigung über die Konjugierten des Stabilisators $\text{Stab}_G(a)$ schreiben:

$$G = \bigcup_{h \in G} h\text{Stab}_G(a)h^{-1}. \quad (*)$$

3. Schritt: Mächtigkeit der Konjugierten. $\text{Stab}_G(a)$ ist eine echte Untergruppe von G , denn im Fall $\text{Stab}_G(a) = G$ wäre $(G : \text{Stab}_G(a)) = |\text{Stab}_G(a)| = 1$ und a wäre ein Fixpunkt – wegen $G(a) = M$ würde daraus $M = \{a\}$ folgen, im Widerspruch zu $|M| > 2$. Da die Konjugation mit einem Element ein Automorphismus ist, gilt $|h\text{Stab}_G(a)h^{-1}| = |\text{Stab}_G(a)|$ für $h \in G$. Laut dem Satz von Lagrange gilt ferner $|\text{Stab}_G(a)| = \frac{|G|}{(G : \text{Stab}_G(a))}$.

4. Schritt: Anzahl der Konjugierten: Wir zeigen nun, dass die Anzahl der verschiedenen zu $\text{Stab}_G(a)$ konjugierten Untergruppen kleiner oder gleich dem Index $(G : \text{Stab}_G(a))$ ist. Seien dazu $g_1, g_2 \in G$ mit $g_1\text{Stab}_G(a) = g_2\text{Stab}_G(a)$. Dann existiert ein $h \in \text{Stab}_G(a)$ mit $g_1 = g_2h$ und somit folgt

$$g_1\text{Stab}_G(a)g_1^{-1} = g_2h\text{Stab}_G(a)h^{-1}g_2^{-1} = g_2\text{Stab}_G(a)g_2^{-1}.$$

Die Konjugation von $\text{Stab}_G(a)$ mit Elementen aus der gleichen Nebenklasse von $\text{Stab}_G(a)$ in G liefert somit die gleiche konjugierte Untergruppe. Damit existieren maximal so viele verschiedene Untergruppen, wie es verschiedene Nebenklassen gibt – deren Anzahl ist $(G : \text{Stab}_G(a))$.

5. Schritt: Widerspruch zur Elementezahl von G : Wir versuchen, einen Widerspruch zur Elementezahl von G zu erlangen. Bis jetzt wissen wir, dass die Anzahl von Konjugierten kleiner gleich $(G : \text{Stab}_G(a))$ ist und die einzelnen Konjugierten jeweils $\frac{|G|}{(G : \text{Stab}_G(a))}$ Elemente enthalten. Das liefert für die Elementezahl der Vereinigung leider nur die Abschätzung $\leq |G|$. Befassen wir uns also näher mit den zu $\text{Stab}_G(a)$ konjugierten Untergruppen. Jede davon enthält neben dem Neutralelement e noch $|\text{Stab}_G(a)| - 1$ weitere Elemente. Damit haben wir

$$\begin{aligned} \left| \bigcup_{h \in G} h\text{Stab}_G(a)h^{-1} \right| &\leq \underbrace{(G : \text{Stab}_G(a))}_{\text{Anzahl Konjugierte}} \cdot \underbrace{(|\text{Stab}_G(a)| - 1)}_{\text{Elemente außer } e} + \underbrace{1}_e = \\ &= (G : \text{Stab}_G(a)) \cdot \left(\frac{|G|}{(G : \text{Stab}_G(a))} - 1 \right) + 1 = \\ &= |G| - (G : \text{Stab}_G(a)) + 1 < |G|, \end{aligned}$$

wobei die letzte Ungleichung wiederum aus $(G : \text{Stab}_G(a)) > 1$ folgt.

Fazit: Damit kann eine Vereinigung der Form $(*)$ nicht existieren und wir haben schlussendlich einen Widerspruch erhalten – ein $g \in G$ mit der geforderten Eigenschaft muss also existieren.

Gruppenoperationen und Lineare Algebra

Aufgaben zu Gruppenoperationen, zu deren Lösung Wissen aus der Linearen Algebra nötig ist, wurden in den letzten Jahren zunehmend häufiger gestellt. Für einen Überblick der nötigen Theorie und weitere Aufgaben dieses Stils sei auf das entsprechende Kapitel verwiesen.

Aufgabe (Frühjahr 2015, T2A4)

- a** Die Gruppe G operiere transitiv auf einer Menge Ω mit $|\Omega| > 1$. Man zeige: Hat jedes Element aus G mindestens einen Fixpunkt, dann ist G eine Vereinigung der Konjugierten hUh^{-1} , $h \in G$ mit einer echten Untergruppe U von G .
- b** Für $n > 1$ sei $G = \text{GL}_n(\mathbb{C})$ die Gruppe der invertierbaren $n \times n$ -Matrizen über den komplexen Zahlen. Man gebe eine echte Untergruppe U von G an, so dass G die Vereinigung der Konjugierten von U ist.

Hinweis

Betrachten Sie die Operation auf den 1-dimensionalen Unterräumen von \mathbb{C}^n .

Lösungsvorschlag zur Aufgabe (Frühjahr 2015, T2A4)

- a** Dies ist genau der erste Teil von H08T1A2 **b** (vgl. Seite 23), sodass wir hier nur eine kurze Skizze des Beweises wiedergeben. Gibt es für jedes $g \in G$ ein $m \in \Omega$ mit $g \cdot m = m$, so gilt $g \in \text{Stab}_G(m)$ und damit

$$G = \bigcup_{m \in \Omega} \text{Stab}_G(m).$$

Im nächsten Schritt folgert man daraus, dass die Operation transitiv ist, es also ein $a \in \Omega$ mit $G(a) = \Omega$ gibt, dass alle Stabilisatoren zu $\text{Stab}_G(a)$ konjugiert sind. Somit wird obige Vereinigungsmenge zu

$$G = \bigcup_{h \in G} h \text{Stab}_G(a) h^{-1}.$$

Es bleibt lediglich zu zeigen, dass $\text{Stab}_G(a) \neq G$. Angenommen, es gilt $G = \text{Stab}_G(a)$, dann wäre

$$|\Omega| = |G(a)| = (G : \text{Stab}_G(a)) = 1$$

im Widerspruch zu $|\Omega| > 1$.

- b** Wir bestimmen zunächst eine geeignete Operation. Betrachte dazu die Menge \mathcal{U} der 1-dimensionalen Untervektorräume von \mathbb{C}^n sowie die Abbildung

$$\cdot : G \times \mathcal{U} \rightarrow \mathcal{U}, \quad (A, U) \mapsto A \cdot U = \{Av \mid v \in U\}.$$

Dass diese wohldefiniert ist, folgt daraus, dass $v \mapsto Av$ ein Isomorphismus ist, da die Matrix A invertierbar ist. Somit hat das Bild die gleiche Dimension wie U . Wir zeigen, dass es sich dabei um eine Gruppenoperation handelt: Es gilt zunächst für $U \in \mathcal{U}$, $A, B \in \text{GL}_n(\mathbb{C})$

$$\mathbb{E}_n U = \{\mathbb{E}_n v \mid v \in U\} = U$$

sowie

$$\begin{aligned} (AB) \cdot U &= \{(AB)v \mid v \in U\} = \{A(Bv) \mid v \in U\} = \{Aw \mid w \in BU\} \\ &= A \cdot B \cdot U. \end{aligned}$$

Um zu zeigen, dass \cdot transitiv ist, betrachte den Untervektorraum $W = \langle e_1 \rangle$, wobei im folgenden e_i jeweils den i -ten Einheitsvektor bezeichnet. Wir zeigen $G(W) = \mathcal{U}$. Sei dazu V ein beliebiger eindimensionaler Untervektorraum. Es ist dann $V = \langle v \rangle$ für ein $v \in \mathbb{C}^n \setminus \{0\}$. Dieser Vektor lässt sich mit anderen (w_2, \dots, w_n) zu einer Basis von \mathbb{C}^n ergänzen. Schreiben

wir dann diese Vektoren als Spalten in eine Matrix $A = (v \mid w_2 \mid \dots \mid w_m)$, so ist $A \in \mathrm{GL}_n(\mathbb{C})$. Weiter gilt

$$A \cdot W = \{A(\lambda e_1) \mid \lambda \in \mathbb{C}\} = \{\lambda(Ae_1) \mid \lambda \in \mathbb{C}\} = \{\lambda v \mid \lambda \in \mathbb{C}\} = \langle v \rangle.$$

Und somit $V \in G(W)$. Damit ist die Operation transitiv.

Nun müssen wir noch zeigen, dass jedes $A \in G$ einen Fixpunkt hat. Das charakteristische Polynom von A zerfällt über \mathbb{C} auf jeden Fall in Linearfaktoren, da \mathbb{C} algebraisch abgeschlossen ist. Sei also $\lambda \in \mathbb{C}$ eine Nullstelle des charakteristischen Polynoms, d.h. ein Eigenwert von A und v ein zugehöriger Eigenvektor. Dann gilt für den eindimensionalen Untervektorraum $U = \langle v \rangle$

$$A \cdot U = \{Au \mid u \in U\} = \{\lambda u \mid \lambda \in \mathbb{C}\} = U.$$

Damit ist U ein Fixpunkt zu A .

Laut Teil **a** ist eine Untergruppe mit den gewünschten Eigenschaften durch den Stabilisator eines Element gegeben. Bestimmen wir also $\mathrm{Stab}_G(W)$. Es gilt für $A \in G$

$$\begin{aligned} A \in \mathrm{Stab}_G W &\Leftrightarrow A \cdot W = W \Leftrightarrow \{A(\mu e_1) \mid \mu \in \mathbb{C}\} = \{\lambda e_1 \mid \lambda \in \mathbb{C}\} \\ &\Leftrightarrow \exists \lambda \in \mathbb{C}^\times : Ae_1 = \lambda e_1. \end{aligned}$$

Eine gesuchte Untergruppe ist also die Menge

$$U = \{A \in \mathrm{GL}_n(\mathbb{C}) \mid Ae_1 = \lambda e_1 \text{ für ein } \lambda \in \mathbb{C}^\times\}.$$

Dass es sich dabei um eine Untergruppe handelt, ist schnell nachgerechnet. Dass U die gewünschte Eigenschaft besitzt, folgt aus Teil **a**. Zum Schluss ist U eine echte Teilmenge von $\mathrm{GL}_n(\mathbb{C})$, da beispielsweise die Matrix $(e_2 \mid e_1 \mid e_3 \mid \dots \mid e_n)$ nicht in U enthalten ist.

*Alternative ohne Teil **a**:* Sei D die Menge der oberen Dreiecksmatrizen in $\mathrm{GL}_n(\mathbb{C})$. Es handelt sich dabei um eine echte Untergruppe (vgl. Aufgabe F13T2A2 auf Seite 227) von G . Ist ferner $A \in G$ eine beliebige Matrix, so zerfällt ihr charakteristisches Polynom in Linearfaktoren, da wir über dem algebraisch abgeschlossenen Körper \mathbb{C} arbeiten. Die Matrix A ist also ähnlich zu einer Matrix in Jordan-Normalform, die eine obere Dreiecksmatrizen ist, d.h. es gibt ein $T \in G$, sodass TAT^{-1} eine obere Dreiecksmatrix ist. Das wiederum bedeutet $A \in TDT^{-1}$. Somit ist G die Vereinigung aller Konjugierten von D .

Aufgabe (Herbst 2012, T2A1)

Seien $n, m > 0$ natürliche Zahlen. Mit $M_{n,m}(\mathbb{Q})$ bezeichnen wir die Menge der $(n \times m)$ -Matrizen mit rationalen Einträgen. Seien $GL_n(\mathbb{Q})$ und $GL_m(\mathbb{Q})$ die allgemeinen linearen Gruppen in den Dimensionen n und m über \mathbb{Q} .

- a** Zeigen Sie, dass die Gruppe $GL_n(\mathbb{Q}) \times GL_m(\mathbb{Q})$ vermöge

$$(GL_n(\mathbb{Q}) \times GL_m(\mathbb{Q})) \times M_{n,m}(\mathbb{Q}) \rightarrow M_{n,m}(\mathbb{Q}), \quad ((S, T), A) \mapsto SAT^{-1}$$

auf $M_{n,m}(\mathbb{Q})$ operiert, aber nicht effektiv. (Dabei heißt eine Gruppenoperation $G \times X \rightarrow X$ einer Gruppe G auf einer Menge X effektiv, wenn aus $\forall x \in X : g \cdot x = x$ für ein Gruppenelement $g \in G$ schon $g = 1$ folgt.)

- b** Zeigen Sie, dass diese Operation genau $r + 1$ Bahnen besitzt, dabei ist $r = \min(m, n)$.

Hinweis Verwenden Sie den Rang einer Matrix.

Lösungsvorschlag zur Aufgabe (Herbst 2012, T2A1)

- a** Wir zeigen zunächst die definierenden Eigenschaften einer Operation. Seien dazu $S_1, S_2 \in GL_n(\mathbb{Q})$, $T_1, T_2 \in GL_m(\mathbb{Q})$ und $A \in M_{n,m}(\mathbb{Q})$. Es gilt

$$(\mathbb{E}_n, \mathbb{E}_m) \cdot A = \mathbb{E}_n A \mathbb{E}_m^{-1} = A$$

sowie

$$\begin{aligned} (S_1 S_2, T_1 T_2) \cdot A &= (S_1 S_2) A (T_1 T_2)^{-1} = S_1 S_2 A T_2^{-1} T_1^{-1} \\ &= S_1 ((S_2, T_2) \cdot A) T_1^{-1} = (S_1, T_1) \cdot (S_2, T_2) \cdot A. \end{aligned}$$

Wir zeigen noch, dass diese Operation nicht effektiv ist: Betrachte dazu das Element

$$(2\mathbb{E}_n, 2\mathbb{E}_m) \in GL_n(\mathbb{Q}) \times GL_m(\mathbb{Q}).$$

Es gilt für beliebiges $A \in M_{n,m}(\mathbb{Q})$

$$(2\mathbb{E}_n, 2\mathbb{E}_m) \cdot A = 2\mathbb{E}_n A \frac{1}{2}\mathbb{E}_m^{-1} = A, \quad \text{aber } (2\mathbb{E}_n, 2\mathbb{E}_m) \neq (\mathbb{E}_n, \mathbb{E}_m).$$

- b** Wir verwenden den Hinweis und zeigen, dass zwei Matrizen genau dann in der gleichen Bahn liegen, wenn sie den gleichen Rang haben.

Seien zunächst $A, B \in M_{n,m}(\mathbb{Q})$ Elemente einer Bahn. Dann gibt es $S \in GL_n(\mathbb{Q})$, $T \in GL_m(\mathbb{Q})$ mit $B = SAT^{-1}$. Da S und T invertierbar sind, haben diese vollen Rang. Insbesondere folgt daraus $\text{rk}(B) = \text{rk}(SAT^{-1}) = \text{rk}(A)$. Also haben A und B den gleichen Rang.

Sind umgekehrt $A, B \in M_{n,m}(\mathbb{Q})$ Matrizen von gleichem Rang, so können diese durch Zeilen- und Spaltenumformungen auf die gleiche normierte Zeilenstufenform gebracht werden. Da diese Umformungen durch Multiplikation mit sogenannten Elementarmatrizen (von links bzw. rechts) realisiert werden können, erhält man invertierbare Matrizen $S_1, S_2 \in \mathrm{GL}_n(\mathbb{C})$ und $T_1, T_2 \in \mathrm{GL}_m(\mathbb{C})$, sodass

$$S_2 B T_2 = S_1 A T_1 \Leftrightarrow B = S_2^{-1} S_1 A T_1 T_2^{-1} = (S_2^{-1} S_1) A (T_2 T_1^{-1})^{-1}.$$

Somit liegt B in der gleichen Bahn wie A .

Da $\mathrm{rk}(A) \leq \min(n, m) = r$ gilt, gibt es für den Rang die $r + 1$ Möglichkeiten $\mathrm{rk}(A) \in \{0, 1, \dots, r\}$. Dementsprechend gibt es höchstens $r + 1$ Bahnen. Andererseits ist klar, dass in $M_{n,m}(\mathbb{Q})$ für jedes $k \in \{0, 1, \dots, r\}$ eine Matrix von Rang k existiert, also haben wir Gleichheit.

Aufgabe (Frühjahr 2013, T1A5)

Sei M die Menge der 3×3 -Matrizen mit Einträgen aus \mathbb{C} , deren charakteristisches Polynom $(X - 1)^3$ ist.

- a** Zeigen Sie: $\mathrm{GL}(3, \mathbb{C})$ operiert durch Konjugation, d. h. mittels $P * A = PAP^{-1}$ für $P \in \mathrm{GL}(3, \mathbb{C})$ und $A \in M$, auf M .
- b** Bestimmen Sie die Anzahl der Bahnen unter dieser Operation.

Lösungsvorschlag zur Aufgabe (Frühjahr 2013, T1A5)

- a** Wir zeigen zunächst, dass die Abbildung wohldefiniert ist, das heißt, dass $PAP^{-1} \in M$ gilt. Sei dazu $P \in \mathrm{GL}(3, \mathbb{C})$ beliebig und $A \in M$ mit $\chi_A = (X - 1)^3$. Dann gilt

$$\begin{aligned}\chi_{PAP^{-1}} &= \det(PAP^{-1} - X\mathbb{E}_3) = \det(PAP^{-1} - PX\mathbb{E}_3P^{-1}) = \\ &= \det(P(A - X\mathbb{E}_3)P^{-1}) = \det(P)\det(A - X\mathbb{E}_3)\det(P^{-1}) \\ &= \det(P)\chi_A\det(P)^{-1} = \chi_A\end{aligned}$$

Somit hat auch PAP^{-1} das charakteristische Polynom $(X - 1)^3$ und es gilt $PAP^{-1} \in M$. (Alternativ hätte man auch den Satz zitieren können, dass ähnliche Matrizen gleiches charakteristisches Polynom haben).

Zeigen wir nun noch die definierenden Eigenschaften einer Gruppenoperation: Seien dazu $P_1, P_2 \in G$ und $A \in M$. Es gilt

$$\mathbb{E}_3 * A = \mathbb{E}_3 A \mathbb{E}_3 = A$$

und

$$\begin{aligned} (P_1 P_2) * A &= (P_1 P_2) A (P_1 P_2)^{-1} = (P_1 P_2) A (P_2^{-1} P_1^{-1}) = \\ &= P_1 (P_2 A P_2^{-1}) P_1^{-1} = P_1 * P_2 * A. \end{aligned}$$

- b** Für jede Matrix aus M zerfällt das charakteristische Polynom in Linearfaktoren. Damit kann jede solche Matrix auf Jordan-Normalform gebracht werden, d. h. es gibt eine Matrix $P \in \mathrm{GL}(3, \mathbb{C})$, sodass PAP^{-1} in Jordan-Normalform vorliegt.

Eine solche Darstellung ist eindeutig bis auf die Anordnung der Jordanblöcke. Die Matrizen aus M haben den dreifachen Eigenwert 1, sodass alle Blöcke Eigenwert 1 haben müssen. Jede Matrix aus M ist damit ähnlich zu einer Jordan-Normalform mit einem Jordanblock der Größe 3, einer Kombination aus einem Jordanblock der Größe eins und einem der Größe zwei oder drei Jordanblöcken der Größe 1. (Beachte, dass es für die zweite Möglichkeit zwar zwei verschiedene Matrizen gibt, die sich aber nur in der Anordnung der Blöcke unterscheiden und deshalb in derselben Bahn liegen). Insgesamt haben wir somit begründet, dass die Menge

$$R = \left\{ \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \right\}$$

ein Repräsentantsystem der Bahnen ist. Daraus folgt insbesondere, dass es genau drei verschiedene Bahnen gibt.

1.3. Direkte und semidirekte Produkte

Das Konzept des semidirekten Produktes wird in den meisten Büchern (und Vorlesungen) etwas stiefmütterlich behandelt, sofern es überhaupt besprochen wird. Wir geben daher zunächst eine ausführliche Motivation.

Komplexprodukt

In diesem Abschnitt werden wir den Begriff des *Komplexprodukts* benötigen. Ist G eine Gruppe und sind $N, M \subseteq G$ Untergruppen, so ist dieses als die Menge

$$NM = \{nm \in G \mid n \in N, m \in M\}$$

definiert. Laut dem 1. Isomorphiesatz 1.10 (1) ist das Komplexprodukt zweier Untergruppen wieder eine Untergruppe, falls eine der beiden Untergruppen ein Normalteiler ist.

Sei G eine Gruppe mit Neutralelement e und seien $N, M \subseteq G$ Untergruppen mit $G = NM$ und $N \cap M = \{e\}$. Dann besitzt jedes $g \in G$ eine eindeutige Darstellung als $g = nm$ mit $n \in N$ und $m \in M$: Ist nämlich $n_1m_1 = n_2m_2$ für $n_1, n_2 \in N$ und $m_1, m_2 \in M$, so bedeutet dies

$$n_1m_1 = n_2m_2 \Leftrightarrow n_2^{-1}n_1 = m_2m_1^{-1} \in N \cap M = \{e\},$$

sodass also $n_2^{-1}n_1 = e = m_2m_1^{-1}$ bzw. $n_1 = n_2$ und $m_1 = m_2$ gelten muss. Mit der Eindeutigkeit der Darstellung haben wir gezeigt, dass die Abbildung

$$\sigma: G \rightarrow N \times M, \quad nm \mapsto (n, m)$$

eine wohldefinierte Bijektion ist.

Direktes Produkt

Damit σ zu einem Gruppenhomomorphismus wird, müssen wir zusätzlich fordern, dass N und M beide Normalteiler von G sind. In diesem Fall nennt man G ein *inneres direktes Produkt* von N und M .

Sind $n \in N$ und $m \in M$ vorgegeben, so gilt nämlich laut der Normalteilereigenschaft, dass

$$m^{-1}nm \in N \quad \text{und} \quad nm^{-1} \in M,$$

also folgt $(m^{-1}nm)n^{-1} = m^{-1}(nm)n^{-1} \in N \cap M = \{e\}$, sodass

$$m^{-1}nmn^{-1} = e \Leftrightarrow nm = mn.$$

Nun ist der Nachweis der Homomorphismus-Eigenschaft nur noch Routine:

$$\begin{aligned} \sigma((n_1m_1)(n_2m_2)) &= \sigma((n_1n_2)(m_1m_2)) = \\ &= (n_1n_2, m_1m_2) = (n_1, m_1) \cdot (n_2, m_2) = \sigma(n_1m_1) \cdot \sigma(n_2m_2) \end{aligned}$$

Dies bedeutet, dass G isomorph zu $N \times M$ ist, dem *äußeren direkten Produkt* von N und M .

Semidirektes Produkt

Im vorherigen Absatz haben unsere speziellen Voraussetzungen dazu geführt, dass die Gruppe G bereits eindeutig durch die Normalteiler N und M bestimmt ist. Diese Eindeutigkeit geht verloren, falls man sich damit zufrieden gibt, dass G nur ein *inneres semidirektes Produkt* von N und M ist, d. h. nur eine der beiden Untergruppen ein Normalteiler ist.

Beispiel 1.20. Als Beispiel dafür betrachten wir die symmetrische Gruppe S_3 und die Gruppe $\mathbb{Z}/6\mathbb{Z}$. Beide Gruppen besitzen mit A_3 bzw. $\langle \bar{2} \rangle$ einen Normalteiler der Ordnung 3. Mithilfe der zweielementigen Untergruppen $\langle (1 2) \rangle$ bzw. $\langle \bar{3} \rangle$ finden wir dann

$$S_3 = \langle (1 2) \rangle A_3 \quad \text{und} \quad \mathbb{Z}/6\mathbb{Z} = \langle \bar{3} \rangle \langle \bar{2} \rangle,$$

denn die Komplexprodukte sind Untergruppen, da jeweils einer der Faktoren ein Normalteiler ist, und haben Ordnung 6. Die gewählten Untergruppen sind als Gruppen gleicher Primzahlordnung paarweise isomorph, jedoch können die nicht-abelsche Gruppe S_3 und die zyklische Gruppe $\mathbb{Z}/6\mathbb{Z}$ nicht isomorph sein. ■

Sei also nun G eine Gruppe, sodass $N \trianglelefteq G$ ein Normalteiler, $M \subseteq G$ eine Untergruppe und $G = NM$ ist sowie $N \cap M = \{e\}$ gilt. Auch unter diesen Voraussetzungen handelt es sich bei der Abbildung σ von oben um eine Bijektion. Diese Abbildung induziert somit eine Gruppenstruktur auf $N \times M$, bezüglich der σ zu einem Homomorphismus wird. Die zugehörige Verknüpfungsvorschrift $*$ sieht jedoch anders aus als gewohnt. Sind nämlich (n_1, m_1) und $(n_2, m_2) \in N \times M$ vorgegeben, so gilt $m_1 n_1 m_1^{-1} \in N$, da N ein Normalteiler ist, und es folgt

$$\begin{aligned} (n_1, m_1) * (n_2, m_2) &= \sigma(n_1 m_1) * \sigma(n_2 m_2) = \sigma(n_1 m_1 n_2 m_2) = \sigma(n_1 (m_1 n_2 m_1^{-1}) m_1 m_2) \\ &= (n_1 (m_1 n_2 m_1^{-1}), m_1 m_2). \end{aligned}$$

Den „Korrekturterm“ in der ersten Komponente kann man so interpretieren, dass er infolge des Homomorphismus

$$\phi: M \rightarrow \text{Aut}(N), \quad m \mapsto \left\{ n \mapsto mn m^{-1} \right\}$$

entsteht, d. h. ϕ ordnet jedem $m \in M$ den Automorphismus $\phi(m)$ mit $\phi(m)(n) = mn m^{-1}$ für $n \in N$ zu. Damit schreibt sich die neue Verknüpfung als

$$*: (N \times M) \times (N \times M) \rightarrow N \times M, \quad (n_1, m_1) * (n_2, m_2) = (n_1 \phi(m_1)(n_2), m_1 m_2).$$

Um deutlich zu machen, dass wir die Menge $N \times M$ mit der neuen Gruppenverknüpfung meinen, schreiben wir dafür $N \rtimes_{\phi} M$. Auch wenn die Abbildung ϕ nicht exakt die gleiche Form hat wie in unserem Fall, handelt es sich bei $N \rtimes_{\phi} M$ um eine Gruppe der Ordnung $|N| \cdot |M|$. Wir halten die Konstruktion daher allgemein fest.

Definition 1.21. Seien N, M Gruppen und $\phi: M \rightarrow \text{Aut}(N)$ ein Homomorphismus. Dann wird die Menge $N \times M$ mit der Verknüpfung

$$(n_1, m_1) * (n_2, m_2) = (n_1 \phi(m_1)(n_2), m_1 m_2)$$

zu einer Gruppe. Diese heißt *äußeres semidirektes Produkt* von N und M und wird als $N \rtimes_{\phi} M$ notiert.

Eseisbrücke für die Verknüpfung in semidirekten Produkten

Das n_2 will sich mit dem n_1 paaren, dabei funk jedoch das m_1 mittels ϕ dazwischen. Das m_2 ist daher schlauer und schleicht sich oben rum am n_2 vorbei.

$$(n_1, m_1) * (n_2, m_2) = (n_1 \phi(m_1)(n_2), m_1 m_2)$$

Der folgende Satz fasst die bisherigen Ergebnisse der Klassifikation von inneren direkten bzw. semidirekten Produkten zusammen.

Satz 1.22. Sei G eine Gruppe und seien $N, M \subseteq G$ Untergruppen.

- (1) Ist G inneres direktes Produkt von N und M , d.h. sind N und M Normalteiler mit $G = NM$ und $N \cap M = \{e\}$, so ist G isomorph zum äußeren direkten Produkt $N \times M$.
- (2) Ist G inneres semidirektes Produkt von N und M , d.h. ist N ein Normalteiler und es gilt $G = NM$ sowie $N \cap M = \{e\}$, so ist G isomorph zum äußeren semidirekten Produkt $N \rtimes_{\phi} M$, wobei der Homomorphismus ϕ durch

$$\phi: M \rightarrow \text{Aut}(N), \quad m \mapsto \{n \mapsto mn m^{-1}\}$$

gegeben ist.

Vor diesem Hintergrund lässt sich auch unsere Beobachtung aus Beispiel 1.20 erklären: S_3 und $\mathbb{Z}/6\mathbb{Z}$ sind beide isomorph zu einem äußeren semidirekten Produkt von $\mathbb{Z}/3\mathbb{Z}$ und $\mathbb{Z}/2\mathbb{Z}$, allerdings zu verschiedenen Homomorphismen $\mathbb{Z}/2\mathbb{Z} \rightarrow \text{Aut}(\mathbb{Z}/3\mathbb{Z})$.

Konstruktion nicht-abelscher Gruppen

Interessant ist, dass im Fall $\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ das direkte und das semidirekte Produkt zusammen fallen. Wir bestimmen die Fälle, in denen dies auftritt, genauer.

Proposition 1.23. Seien N, M Gruppen, wobei N abelsch ist. Das semidirekte Produkt $N \rtimes_{\phi} M$ ist genau dann abelsch, wenn M abelsch und der Homomorphismus $\phi: M \rightarrow \text{Aut}(N)$ trivial ist, d.h. $\phi(m) = \text{id}_N$ für alle $m \in M$ gilt. In diesem Fall ist $N \rtimes_{\phi} M = N \times M$.

In den Aufgaben wird in aller Regel das semidirekte Produkt zweier zyklischer Gruppen benötigt. Aus diesem Grund sind die Aussagen der nächsten Proposition besonders hilfreich.

Proposition 1.24. Sei $G = \langle g \rangle$ eine zyklische Gruppe der Ordnung n .

- (1) Ist H eine weitere Gruppe und $h \in H$ ein Element, sodass $\text{ord } h$ ein Teiler von $\text{ord } g = n$ ist, so existiert ein eindeutig bestimmter Homomorphismus $\phi: G \rightarrow H$ mit $\phi(g) = h$.
- (2) Die Abbildung

$$(\mathbb{Z}/n\mathbb{Z})^\times \rightarrow \text{Aut}(G), \quad \bar{r} \mapsto \{g \mapsto g^r\}$$

ist ein Isomorphismus.

In Verbindung mit Proposition 1.24 (2) sind insbesondere die Struktursätze für die Einheitengruppe $(\mathbb{Z}/n\mathbb{Z})^\times$ nützlich (vgl. Satz 2.8). Beispielsweise ist diese zyklisch, falls n die Potenz einer ungeraden Primzahl ist. In jedem Fall hat $(\mathbb{Z}/n\mathbb{Z})^\times$ die Ordnung $\varphi(n)$.

Anleitung: Konstruktion nicht-abelscher Gruppen

Ziel ist es, eine nicht-abelsche Gruppe der Ordnung n zu konstruieren.

- (1) Finde Zahlen l und m , sodass $n = lm$ gilt und $\varphi(m)$ und l einen gemeinsamen Teiler haben.
- (2) Sind wir in der Lage, einen nicht-trivialen Homomorphismus $\phi: \mathbb{Z}/l\mathbb{Z} \rightarrow \text{Aut}(\mathbb{Z}/m\mathbb{Z})$ zu finden, so ist nach Proposition 1.23 durch $\mathbb{Z}/m\mathbb{Z} \rtimes_\phi \mathbb{Z}/l\mathbb{Z}$ eine nicht-abelsche Gruppe der Ordnung $ml = n$ gegeben. Dazu gehen wir folgendermaßen vor:
 - (a) Nach Proposition 1.24 (2) ist $\text{Aut}(\mathbb{Z}/m\mathbb{Z}) \cong (\mathbb{Z}/m\mathbb{Z})^\times$ und letztere Gruppe ist in vielen Fällen zyklisch, z. B. wenn m eine Primzahl ist. Aufgrund der Wahl von l und m in Schritt (1) existiert dann ein Element $a \in \text{Aut}(\mathbb{Z}/m\mathbb{Z})$ mit einer Ordnung, die l teilt.
 - (b) Nutzen wir nun Proposition 1.24 (1), um einen Homomorphismus $\psi: \mathbb{Z}/l\mathbb{Z} \rightarrow \text{Aut}(\mathbb{Z}/m\mathbb{Z})$ mit $\psi(\bar{1}) = a$ für das Element a aus (2a) zu definieren. Der Homomorphismus ist genau dann nicht-trivial, wenn $a \neq \text{id}$ ist. In diesem Fall folgt mit Proposition 1.23, dass das zugehörige semidirekte äußere Produkt nicht abelsch ist.

Aufgabe (Frühjahr 2013, T3A1)

Man konstruiere eine nicht-abelsche Gruppe der Ordnung 2013.

Hinweis Verwenden Sie ein geeignetes semidirektes Produkt.

Lösungsvorschlag zur Aufgabe (Frühjahr 2013, T3A1)

Wir bemerken zunächst, dass $2013 = 3 \cdot 11 \cdot 61$ ist. Unser Ziel ist, im Folgenden einen nicht-trivialen Homomorphismus $\phi: \mathbb{Z}/33\mathbb{Z} \rightarrow \text{Aut}(\mathbb{Z}/61\mathbb{Z})$ zu definieren. Dazu verwenden wir, dass nach Proposition 1.24 (2)

$$\text{Aut}(\mathbb{Z}/61\mathbb{Z}) \cong (\mathbb{Z}/61\mathbb{Z})^\times \cong \mathbb{Z}/60\mathbb{Z}$$

eine zyklische Gruppe der Ordnung $60 = 2^2 \cdot 3 \cdot 5$ ist. Wegen $3 \mid 60$ gibt es ein Element $a \in \text{Aut}(\mathbb{Z}/61\mathbb{Z})$ mit $\text{ord } a = 3$. Da 3 ein Teiler von $33 = \text{ord}(\bar{1})$ ist, gibt es nach Proposition 1.24 (1) einen eindeutigen Homomorphismus

$$\psi: \mathbb{Z}/33\mathbb{Z} \rightarrow \text{Aut}(\mathbb{Z}/61\mathbb{Z}) \quad \text{mit} \quad \psi(\bar{1}) = a.$$

Dieser ist nicht-trivial, denn es gilt $a \neq \text{id}$ wegen $\text{ord } a = 3$ und somit $\psi(\bar{1}) \neq \text{id}$. Gemäß Proposition 1.23 ist dann $\mathbb{Z}/61\mathbb{Z} \rtimes_\phi \mathbb{Z}/33\mathbb{Z}$ eine nicht-abelsche Gruppe der Ordnung $33 \cdot 61 = 2013$ ist.

Aufgabe (Herbst 2012, T3A1)

Geben Sie drei nicht-isomorphe Gruppen der Ordnung 2012 konkret an und beweisen Sie, dass diese nicht isomorph sind!

Lösungsvorschlag zur Aufgabe (Herbst 2012, T3A1)

Die Primfaktorzerlegung von 2012 ist $2^2 \cdot 503$. Die einzigen abelschen Gruppen der Ordnung 2012 sind nach Satz 1.11 also

$$G_1 = \mathbb{Z}/2012\mathbb{Z} \quad \text{und} \quad G_2 = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/1006\mathbb{Z},$$

wobei diese beiden Gruppen nicht isomorph sind, denn für jedes Element $(\bar{a}, \bar{b}) \in G_2$ gilt

$$1006 \cdot (\bar{a}, \bar{b}) = (\bar{0}, \bar{0}),$$

sodass jedes Element in G_2 höchstens Ordnung 1006 hat. Insbesondere gibt es kein Element der Ordnung 2012 in G_2 , weshalb G_2 nicht zyklisch und folglich nicht zur zyklischen Gruppe G_1 isomorph sein kann.

Eine dritte Gruppe der Ordnung 2012 konstruieren wir als semidirektes Produkt. Finden wir einen nicht-trivialen Homomorphismus $\phi: \mathbb{Z}/4\mathbb{Z} \rightarrow \text{Aut}(\mathbb{Z}/503\mathbb{Z})$, so ist nach Proposition 1.23 das semidirekte Produkt $G_3 = \mathbb{Z}/4\mathbb{Z} \rtimes_{\phi} \mathbb{Z}/503\mathbb{Z}$ nicht abelsch und kann daher nicht isomorph zu den abelschen Gruppen G_1 und G_2 sein. Da 503 eine Primzahl ist, gilt

$$\text{Aut}(\mathbb{Z}/503\mathbb{Z}) \cong (\mathbb{Z}/503\mathbb{Z})^{\times} \cong \mathbb{Z}/502\mathbb{Z}. \quad (*)$$

Da 2 ein Teiler von 502 ist, besitzt die zyklische Gruppe $\text{Aut}(\mathbb{Z}/503\mathbb{Z})$ ein Element der Ordnung 2, das wir mit a bezeichnen. Als Element der Ordnung 2 ist $a \neq \text{id}$, denn nur id hat Ordnung 1 in $\text{Aut}(\mathbb{Z}/503\mathbb{Z})$. Zudem ist die Ordnung von a ein Teiler von 4, der Ordnung von $\bar{1}$ in $\mathbb{Z}/4\mathbb{Z}$, und nach Proposition 1.24 (1) gibt es einen Homomorphismus

$$\psi: \mathbb{Z}/4\mathbb{Z} \rightarrow \text{Aut}(\mathbb{Z}/503\mathbb{Z}) \quad \text{mit} \quad \psi(\bar{1}) = a.$$

Wegen $a \neq \text{id}$ ist dieser nicht-trivial, sodass ψ nicht-trivial ist.

Aufgabe (Frühjahr 2001, T2A2)

Sei G eine Gruppe der Ordnung 63.

- a** Man zeige, dass G einen nichttrivialen Normalteiler hat.
- b** Man konstruiere zwei nicht isomorphe nicht-abelsche Gruppen der Ordnung 63 (als semidirektes Produkt).

Lösungsvorschlag zur Aufgabe (Frühjahr 2001, T2A2)

- a** Es sei v_7 die Anzahl der 7-Sylowgruppen von G . Die Sylowsätze besagen, dass $v_7 \mid 9$ und $v_7 \equiv 1 \pmod{7}$ gelten muss. Aus der ersten Bedingung erhält man $v_7 \in \{1, 3, 9\}$, wovon nur $v_7 = 1$ auch die zweite Bedingung erfüllt. Es gibt also nur eine 7-Sylowgruppe und diese ist daher ein (nicht-trivialer) Normalteiler von G .

- b** Wir konstruieren Produkte der Form

$$G_1 = \mathbb{Z}/7\mathbb{Z} \rtimes_{\phi} \mathbb{Z}/9\mathbb{Z} \quad \text{und} \quad G_2 = \mathbb{Z}/7\mathbb{Z} \rtimes_{\psi} (\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z})$$

und bestimmen dazu zunächst geeignete Homomorphismen $\phi: \mathbb{Z}/9\mathbb{Z} \rightarrow \text{Aut}(\mathbb{Z}/7\mathbb{Z})$ und $\psi: \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \rightarrow \text{Aut}(\mathbb{Z}/7\mathbb{Z})$.

Es ist $\text{Aut}(\mathbb{Z}/7\mathbb{Z}) \cong (\mathbb{Z}/7\mathbb{Z})^\times \cong \mathbb{Z}/6\mathbb{Z}$. Um einen Homomorphismus nach $\text{Aut}(\mathbb{Z}/7\mathbb{Z})$ anzugeben, genügt es also, einen Homomorphismus nach $\mathbb{Z}/6\mathbb{Z}$ anzugeben. Nach Proposition 1.24 (1) gibt es einen Gruppenhomomorphismus

$$\phi: \mathbb{Z}/9\mathbb{Z} \longrightarrow \mathbb{Z}/6\mathbb{Z} \quad \text{mit} \quad \phi(\bar{1}) = \bar{2},$$

denn die Ordnung $\text{ord}(\bar{1}) = 9$ in $\mathbb{Z}/9\mathbb{Z}$ ist ein Vielfaches von $\text{ord}(\bar{2}) = 3$ in $\mathbb{Z}/6\mathbb{Z}$.

Als zyklische Gruppe hat $\mathbb{Z}/6\mathbb{Z}$ genau eine Untergruppe der Ordnung 3, nämlich $\langle \bar{2} \rangle$. Auf diese bilden wir nun die erste Komponente von $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ ab. Konkret geschieht dies durch den Gruppenhomomorphismus

$$\psi: \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \rightarrow \mathbb{Z}/6\mathbb{Z}, \quad (\bar{a}, \bar{b}) \mapsto 2\bar{a}.$$

Mithilfe der beiden Homomorphismen ϕ und ψ können wir die semidirekten Produkte G_1 und G_2 konstruieren. Da diese nicht-trivial sind, sind G_1 und G_2 nicht abelsch.

Es bleibt zu zeigen, dass die beiden Gruppen nicht isomorph zueinander sind. Nehmen wir also an, es gäbe einen Isomorphismus $\theta: G_1 \rightarrow G_2$. Wir bemerken zunächst, dass

$$P = \{\bar{0}\} \times \mathbb{Z}/9\mathbb{Z} \subseteq G_1$$

eine Untergruppe von G_1 mit $P \cong \mathbb{Z}/9\mathbb{Z}$ ist. Es ist daher auch $\theta(P) \subseteq G_2$ eine zyklische Untergruppe der Ordnung 9. Da $\theta(P)$ eine 3-Sylowgruppe von G_2 ist, ist sie konjugiert zu

$$Q = \{\bar{0}\} \times (\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z})$$

und da Konjugation einen Automorphismus definiert, bedeutet dies

$$\mathbb{Z}/9\mathbb{Z} \cong \theta(P) \cong Q \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}.$$

Das kann aber nicht sein, denn $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ ist nicht zyklisch. Der Widerspruch zeigt, dass G_1 und G_2 nicht isomorph sind.

1.4. Sylowsätze und ihre Anwendungen

Ein ähnlich starker Satz wie der Hauptsatz über endlich erzeugte abelsche Gruppen 1.12 existiert für nicht-abelsche Gruppen nicht. Stattdessen machen aber die Sylowsätze detaillierte Aussagen über die Existenz und Anzahl bestimmter Untergruppen.

Definition 1.25. Sei G eine endliche Gruppe der Ordnung $|G| = p^r m$, wobei $r, m \in \mathbb{N}$ und p eine Primzahl mit $p \nmid m$ ist. Eine p -Untergruppe ist eine Untergruppe, deren Ordnung eine p -Potenz ist. Eine p -Sylowgruppe von G ist eine maximale p -Untergruppe von G , d. h. eine Untergruppe der Ordnung p^r .

Im Allgemeinen garantiert der Satz von Lagrange, dass die Ordnung jeder Untergruppe stets die Gruppenordnung teilt. Anders als beispielsweise bei zyklischen Gruppen existiert jedoch in nicht-abelschen Gruppen nicht zu jedem Teiler der Gruppenordnung zwangsläufig eine Untergruppe mit entsprechender Ordnung. Der folgende Satz stellt aber zumindest für p -Untergruppen die Existenz sicher.

Satz 1.26 (Nullter Sylowsatz). Sei G eine endliche Gruppe, p eine Primzahl und p^k eine p -Potenz, die $|G|$ teilt. Dann existiert eine Untergruppe U von G mit $|U| = p^k$.

Satz 1.27 (Sylowsätze). Sei G eine endliche Gruppe der Ordnung $|G| = p^r m$, wobei $r, m \in \mathbb{N}$ sind und p eine Primzahl mit $p \nmid m$ ist. Dann gilt:

- (1) Jede p -Untergruppe von G liegt in einer p -Sylowgruppe.
- (2) Sind P und P' zwei p -Sylowgruppen, so existiert ein $g \in G$ mit $P = gP'g^{-1}$ (vulgo: Je zwei p -Sylowgruppen sind zueinander konjugiert).
- (3) Für die Anzahl ν_p der p -Sylowgruppen in G gilt

$$\nu_p \mid m \quad \text{und} \quad \nu_p \equiv 1 \pmod{p}.$$

Aus dem Zweiten Sylowsatz ergibt sich ein wichtiger Zusammenhang zur Normalteiler-Eigenschaft einer p -Sylow-Untergruppe P : Da die Konjugation mit einem Gruppenelement ein Automorphismus ist, gilt $|gPg^{-1}| = |P|$ für $g \in G$ und somit ist gPg^{-1} wiederum eine p -Sylowgruppe. Gilt nun $\nu_p = 1$, so haben wir $gPg^{-1} = P$ für alle $g \in G$ und P ist Normalteiler von G . Existieren hingegen mindestens zwei verschiedene p -Sylowgruppen $P \neq P'$, so gibt es wiederum nach Satz 1.27 (2) ein $g \in G$ mit $P' = gPg^{-1}$ und P ist kein Normalteiler. Wir halten also fest:

Proposition 1.28. Sei G eine Gruppe. Eine p -Sylowgruppe P von G ist genau dann ein Normalteiler von G , wenn P die einzige p -Sylowgruppe ist.

Aufgabe (Frühjahr 2000, T2A1)

Entscheiden Sie, für welche $n = 2, 3, 4$ die symmetrische Gruppe S_n eine nicht-triviale normale Sylowuntergruppe besitzt.

Lösungsvorschlag zur Aufgabe (Frühjahr 2000, T2A1)

1. Fall: $n = 2$. Hier kommt wegen $|S_2| = 2$ nur eine 2-Sylowgruppe in Betracht. Diese muss aber zugleich 2 Elemente besitzen und damit bereits ganz S_2 sein. Die Antwort ist im Fall $n = 2$ also negativ.

2. Fall: $n = 3$. Hier kommen wegen $|S_3| = 3! = 2 \cdot 3$ nur 2- oder 3-Sylowgruppen in Betracht. Wegen $3^2 \nmid 6$ hat eine 3-Sylowgruppe in S_3 Ordnung 3. Betrachte nun die alternierende Gruppe A_3 . Es ist $|A_3| = \frac{1}{2}|S_3| = 3$, also ist A_3 eine 3-Sylowgruppe. Wegen $(S_3 : A_3) = 2$ ist A_3 ein Normalteiler von S_3 , sodass wir damit eine nicht-triviale normale Sylowuntergruppe gefunden haben.

Alternative: Zeige mit dem Dritten Sylowsatz, dass es nur eine 3-Sylowgruppe gibt und wende Proposition 1.28 an.

3. Fall: $n = 4$. Es gilt $S_4 = 4! = 24 = 2^3 \cdot 3$ und wir können wiederum 2- oder 3-Sylowgruppen betrachten. Der Dritte Sylowsatz liefert keine eindeutige Aussage, sodass wir zu Fuß zeigen, dass es jeweils mehrere 2- und 3-Sylowgruppen in S_4 gibt.

Für die 3-Sylowgruppen: Diese haben 3 Elemente. Nun sind aber durch

$$U_1 = \langle (1\ 2\ 3) \rangle = \{\text{id}, (1\ 2\ 3), (1\ 3\ 2)\}$$

und $U_2 = \langle (1\ 2\ 4) \rangle = \{\text{id}, (1\ 2\ 4), (1\ 4\ 2)\}$

zwei dreielementige Untergruppen gegeben, die verschieden sind. Damit ist $v_3 > 1$ und es gibt keine normale 3-Sylowgruppe in S_4 .

Für die 2-Sylowgruppen: Diese Gruppen müssen $2^3 = 8$ Elemente besitzen. Alle Elemente von G der Ordnung 2, 4 oder 8 erzeugen jeweils eine 2-Untergruppe, welche gemäß dem Ersten Sylowsatz alle in 2-Sylowgruppen enthalten sein müssen. Nach der Formel von Seite 63 gibt es in S_4

$$\binom{4}{2} (2-1)! = \frac{4!}{2! \cdot 2!} = 6 \text{ 2-Zykel} \quad \text{und} \quad \binom{4}{4} (4-1)! = 3! = 6 \text{ 4-Zykel},$$

welche Elemente der Ordnung 2 bzw. 4 sind. Da dies zusammen aber bereits mehr Elemente sind, als in einer 2-Sylowgruppe liegen, muss es auch hiervon mehrere geben. Folglich enthält auch die S_4 keine normale p -Sylowgruppe.

Aufgabe (Frühjahr 2001, T3A2)

Zeigen Sie

$$N_G(N_G(P)) = N_G(P)$$

für eine p -Sylowuntergruppe P der endlichen Gruppe G . ($N_G(U)$ ist der Normalisator der Untergruppe U in G).

Lösungsvorschlag zur Aufgabe (Frühjahr 2001, T3A2)

Es sei daran erinnert, dass der Normalisator von U die größte Untergruppe in G ist, bezüglich derer U ein Normalteiler ist. Konkret ist diese gegeben durch

$$N_G(U) = \{g \in G \mid gUg^{-1} = U\}.$$

Der Normalisator ist zudem gerade der Stabilisator von U bei Operation von G auf der Menge der Untergruppen der Ordnung $|U|$ mittels Konjugation.

Beginnen wir mit der Inklusion „ \supseteq “: Sei $g \in N_G(P)$, dann ist aufgrund der Untergruppeneigenschaften $gN_G(P)g^{-1} = N_G(P)$ und somit $g \in N_G(N_G(P))$.

Für die Richtung „ \subseteq “ sei $g \in N_G(N_G(P))$, d. h. es gelte $gN_G(P)g^{-1} = N_G(P)$. Es gilt dann auch wegen $P \subseteq N_G(P)$

$$gPg^{-1} \subseteq gN_G(P)g^{-1} = N_G(P).$$

Da Konjugation ein Automorphismus ist, haben wir $|P| = |gPg^{-1}|$, sodass auch gPg^{-1} eine p -Sylowgruppe von G ist. Tatsächlich handelt es sich bei P und gPg^{-1} sogar um p -Sylowgruppen von $N_G(P)$.

Nach Definition von $N_G(P)$ ist P ein Normalteiler von $N_G(P)$, folglich ist P die einzige p -Sylowgruppe von $N_G(P)$ und es muss $P = gPg^{-1}$ gelten. Das bedeutet gerade $g \in N_G(P)$.

Nicht-einfache Gruppen

In den folgenden Aufgaben geht es darum, zu zeigen, dass eine Gruppe bestimmter Ordnung einen nicht-trivialen Normalteiler besitzt, d. h. einen Normalteiler ungleich G und ungleich $\{e\}$. Eine solche Gruppe bezeichnet man als *nicht-einfach*.

Proposition 1.28 liefert zusammen mit dem Dritten Sylowsatz ein hilfreiches Kriterium dafür, ob eine der Sylowgruppen ein Normalteiler ist.

Anleitung: Finden von Normalteilern I (Elemente zählen)

Sei G eine Gruppe. Ziel ist es, zu zeigen, dass es einen Primteiler p der Ordnung von G gibt, sodass die zugehörige p -Sylowgruppe ein Normalteiler ist.

- (1) Betrachte einen Primteiler p von $|G|$, der nur einmal in der Primfaktorzerlegung von $|G|$ vorkommt, und sei ν_p die Anzahl der p -Sylowgruppen. Da p eine Primzahl ist, sind laut dem Satz von Lagrange alle Elemente außer dem Neutralelement Erzeuger der p -Sylowgruppe. Das bedeutet, dass zwei verschiedene p -Sylowgruppen nur das Neutralelement gemeinsam haben können. Die Anzahl der Elemente der Ordnung p ist also

$$\nu_p \cdot (p - 1)$$

- (2) Verfahren ebenso mit den anderen Primteilern.
- (3) Tritt ein Primfaktor q mehrfach in der Primfaktorzerlegung von $|G|$ auf, so stellt es sich als deutlich schwieriger heraus, die Anzahl der verschiedenen Elemente in den q -Sylowgruppen zu bestimmen. Immerhin kann man aber die Elementanzahl der q -Sylowgruppe einmal addieren, weil aufgrund der Teilerfremdheit von p und q die Elemente der q -Sylowgruppen in keiner der oben gezählten p -Sylowgruppen enthalten sind. (Achtung, Neutralelement nicht doppelt zählen!)
- (4) Addiere bei Bedarf 1 für das Neutralelement.
- (5) Berechne schließlich die Gesamtzahl. Geht diese über $|G|$ hinaus, so muss eine der Anzahlen 1 sein und die zugehörige Sylowgruppe ist ein Normalteiler, G also nicht-einfach. (Juhu!)

Der dritte Schritt kann gegebenenfalls übersprungen werden, wenn schon vorher die Ordnung von G überschritten ist.

Aufgabe (Herbst 2008, T3A3)

G bezeichne eine Gruppe der Ordnung p^2q , wobei p und q Primzahlen mit $p < q$ sind. Zeigen Sie:

- a** Ist G einfach, so folgt mit dem Satz von Sylow: $q = p + 1$.
- b** G ist nicht-einfach.
- c** Frage: Ist G auch dann nicht-einfach, wenn $p = q$ ist?

Lösungsvorschlag zur Aufgabe (Herbst 2008, T3A3)

a Der Dritte Sylowsatz liefert

$$\nu_p \in \{1, q\} \quad \text{und} \quad \nu_q \in \{1, p, p^2\}.$$

Wäre eine der beiden Anzahlen 1, so hätte G einen nicht-trivialen Normalteiler. Auch den Fall $\nu_q = p$ können wir ausschließen. Es gilt wegen $p < q$ nämlich $p \not\equiv 1 \pmod{q}$. Insgesamt folgt somit $\nu_p = q$ und $\nu_q = p^2$.

Mit der Kongruenzaussage des Dritten Sylowsatzes erhalten wir

$$p^2 \equiv 1 \pmod{q} \Leftrightarrow p^2 - 1 \equiv 0 \pmod{q} \Leftrightarrow (p+1)(p-1) \equiv 0 \pmod{q}.$$

Da q eine Primzahl ist, handelt es sich bei $\mathbb{Z}/q\mathbb{Z}$ um einen Körper, und wir dürfen $p \equiv \pm 1 \pmod{q}$ folgern. Den ersten Fall hatten wir oben bereits ausgeschlossen. Aus dem zweiten folgt wegen $p > 0$ zunächst $p = -1 + kq$ für ein $k \geq 1$. Wäre nun $k > 1$, so wäre $p > q - 1$ und somit $p \geq q$ im Widerspruch zur Annahme $p < q$. Wir erhalten insgesamt

$$p = -1 + q \Leftrightarrow q = p + 1.$$

b Nehmen wir widerspruchshalber an, G wäre einfach. Dann gilt aufgrund von Teil **a**, dass $q = p + 1$ ist. Somit muss aber mindestens eine der beiden Primzahlen gerade sein. Da dies nur auf 2 zutrifft, bedeutet das $p = 2, q = 3$. Untersuchen wir also einfach eine Gruppe G mit $|G| = 2^2 \cdot 3 = 12$. Wie schon zuvor festgestellt, gilt dann aufgrund des Dritten Sylowsatzes, dass $\nu_2 = 3$ und $\nu_3 = 4$.

Wir zählen Elemente:

- Die 3-Sylowgruppen haben wegen $3^2 \nmid 12$ Ordnung 3, sodass jede davon das Neutralelement sowie zwei Elemente der Ordnung 3 enthält. Die Elemente der Ordnung 3 sind Erzeuger, somit können zwei verschiedene 3-Sylowgruppen nur das Neutralelement gemeinsam haben. Insgesamt besitzt die Gruppe daher $4 \cdot 2 = 8$ Elemente der Ordnung 3.
- Eine 2-Sylowgruppe hat wegen $4^2 \mid 12, 4^3 \nmid 12$ hier Ordnung 4 und enthält zusätzlich zum Neutralelement drei nicht-triviale Elemente, deren Ordnungen Teiler von 4 sind. Da es mehr als eine 2-Sylowgruppe in G gibt, muss es noch mindestens ein anderes nicht-triviales Element geben, dessen Ordnung 4 teilt.

Zählen wir noch das Neutralelement hinzu, so müsste G also mindestens

$$8 + (3 + 1) + 1 = 13 > 12$$

Elemente besitzen. Widerspruch!

- c** Hier hat G die Ordnung p^3 . Wir betrachten das Zentrum $Z(G)$ von G , welches ein Normalteiler von G ist. Laut Lemma 1.19 gilt $\{e\} \subsetneq Z(G)$ für das Zentrum einer p -Gruppe. Falls $Z(G) \subsetneq G$, so ist also das Zentrum $Z(G)$ ein nicht-trivialer Normalteiler und G ist nicht-einfach.

Gilt andernfalls $Z(G) = G$, so ist G abelsch. In diesem Fall ist jede Untergruppe auch Normalteiler und auch in diesem Fall ist G nicht-einfach, da es nach dem Nullten Sylowsatz 1.26 eine Untergruppe der Ordnung p gibt.

Aufgabe (Herbst 2004, T3A1)

Sei G eine Gruppe der Ordnung p^2q , wobei p und q Primzahlen bezeichnen. Zeigen Sie, dass G einen nicht-trivialen Normalteiler hat.

Lösungsvorschlag zur Aufgabe (Herbst 2004, T3A1)

Wie immer betrachten wir die Anzahlen der jeweiligen Sylowgruppen. Aufgrund der Teilbarkeitsaussagen im Dritten Sylowsatz gilt zunächst

$$\nu_p \mid q \quad \Rightarrow \quad \nu_p \in \{1, q\} \quad \text{und} \quad \nu_q \mid p^2 \quad \Rightarrow \quad \nu_q \in \{1, p, p^2\}.$$

1. Fall: $\nu_p = 1$ oder $\nu_q = 1$

Hier existiert genau eine p - (bzw. q)-Sylowgruppe. Diese ist Normalteiler und wegen $1 < p^2 < p^2q$ (bzw. $1 < q < p^2q$) ist diese nicht-trivial.

2. Fall: $\nu_p = q$ und $\nu_q = p$

Aus $\nu_p \equiv 1 \pmod{p}$ und $\nu_p \neq 1$ folgt, dass es ein $k \in \mathbb{N}$ gibt, sodass $\nu_p = 1 + kp$. Insbesondere ist $\nu_p > p$. Somit erhalten wir

$$q = \nu_p > p.$$

Damit folgt aber $p \not\equiv 1 \pmod{q}$. Dieser Widerspruch zur Kongruenzaussage des Dritten Sylowsatzes zeigt, dass dieser Fall nicht eintreten kann.

3. Fall: $\nu_p = q$ und $\nu_q = p^2$

Wir zählen Elemente: Die q -Sylowgruppen haben Primzahlordnung. Damit enthalten sie jeweils das Neutralelement und $q - 1$ Elemente der Ordnung q .

Jedes der nicht-trivialen Elemente erzeugt somit bereits die ganze Untergruppe, sodass zwei verschiedene Untergruppen nur das Neutralerelement gemeinsam haben. Existieren p^2 verschiedene q -Sylowgruppen, so gibt es insgesamt $p^2 \cdot (q - 1)$ Elemente der Ordnung q . Damit bleiben in der Gruppe aber insgesamt nur noch

$$p^2 \cdot q - p^2 \cdot (q - 1) = p^2$$

Elemente übrig. Da jede p -Sylowgruppe p^2 Elemente enthält, kann es davon also nur maximal eine geben. Wir erhalten einen Widerspruch zur Annahme $\nu_q \neq 1$. Auch dieser Fall kann also nicht eintreten.

Insgesamt ist $\nu_p = 1$ oder $\nu_q = 1$, sodass ein nicht-trivialer Normalteiler existiert.

Anleitung: Finden von Normalteilern II (Operation)

Sei G eine Gruppe und p ein Primteiler von $|G|$. Wir setzen voraus, dass bekannt ist, dass $\nu_p \in \{1, q\}$ für ein $q \in \mathbb{N}$.

- (1) Annahme: $\nu_p = q$ (sonst wäre die p -Sylowuntergruppe ein Normalteiler und wir wären fertig). Wir bezeichnen die Menge der p -Sylowgruppen mit Syl_p .
- (2) Betrachte die Operation von G auf Syl_p gegeben durch

$$\cdot : (g, P) \mapsto gPg^{-1}$$

sowie den laut Proposition 1.15 daraus resultierenden Homomorphismus

$$\phi: G \rightarrow \text{Per}(\text{Syl}_p), \quad g \mapsto \tau_g, \quad \tau_g(P) = gPg^{-1}.$$

- (3) Der Kern dieses Homomorphismus ist stets ein Normalteiler. Um zu zeigen, dass dieser nicht-trivial ist, führt man zwei Widerspruchsbeweise:
 - (a) Wäre $\ker \phi = \{e\}$, so wäre $|\text{im } \phi| = |G|$ und somit müsste $|G|$ ein Teiler von $|\text{Per}(\text{Syl}_p)| = q!$ sein. Mit Glück ist dies nicht der Fall.
 - (b) Wäre $\ker \phi = G$, so wäre $\tau_g = \text{id}$ für alle $g \in G$. Damit folgt aber $gPg^{-1} = P$ und da die p -Sylowgruppe somit ein Normalteiler wäre, müsste $\nu_p = 1$ gelten – im Widerspruch zu $\nu_p \neq 1$.

Aufgabe (Herbst 2013, T1A2)

Sei G eine Gruppe der Ordnung $750 = 2 \cdot 3 \cdot 5^3$. Mit Syl_5 bezeichnen wir die Menge der 5-Sylowgruppen von G und mit ν_5 bezeichnen wir die Mächtigkeit von Syl_5 .

- a** Begründen Sie, dass $\nu_5 \in \{1, 6\}$.
- b** Begründen Sie, dass G im Fall $\nu_5 = 1$ nicht einfach ist.
- c** Begründen Sie, dass

$$\cdot : G \times \text{Syl}_5 \rightarrow \text{Syl}_5, \quad (g, P) \mapsto gPg^{-1}$$

eine transitive Operation von G auf Syl_5 ist.

- d** Begründen Sie, dass G im Fall $\nu_5 = 6$ nicht einfach ist.

Hinweis Betrachten Sie den Kern des Homomorphismus $\lambda: G \rightarrow S_6$, der durch die Operation aus **c** gegeben ist.

Lösungsvorschlag zur Aufgabe (Herbst 2013, T1A2)

- a** Wir verwenden den Dritten Sylowsatz und erhalten

$$\nu_5 \mid 6 \quad \Rightarrow \quad \nu_5 \in \{1, 2, 3, 6\}.$$

Wegen

$$1 \equiv 1 \pmod{5}, \quad 2 \not\equiv 1 \pmod{5}, \quad 3 \not\equiv 1 \pmod{5}, \quad 6 \equiv 1 \pmod{5}$$

bleibt davon nur $\nu_5 \in \{1, 6\}$ übrig.

- b** Im Fall $\nu_5 = 1$ ist die einzige 5-Sylowgruppe P_5 ein Normalteiler. Als maximale 5-Untergruppe hat diese 5^3 Elemente ($5^4 \nmid 750$) und somit gilt $P_5 \neq G$ sowie $P_5 \neq \{e\}$. Dies zeigt, dass P_5 ein nicht-trivialer Normalteiler ist.
- c** Da Konjugation ein Automorphismus ist, gilt $|gPg^{-1}| = |P|$ für beliebiges $g \in G$. Somit ist $g \cdot P$ wiederum eine 5-Sylowgruppe, sodass die Abbildung aus der Angabe tatsächlich nach Syl_5 abbildet, also wohldefiniert ist.

Wir überprüfen die Eigenschaften einer Gruppen-Operation: Seien dazu $g, h \in G$ und $P \in \text{Syl}_5$ und e das Neutralelement von G . Es gilt

$$(gh) \cdot P = (gh)P(gh)^{-1} = ghPh^{-1}g^{-1} = g(h \cdot P)g^{-1} = g \cdot (h \cdot P)$$

sowie

$$e \cdot P = ePe^{-1} = P.$$

Um zu zeigen, dass die Operation transitiv ist, beweisen wir, dass je zwei 5-Sylowgruppen in der gleichen Bahn liegen. Seien dazu $P, P' \in \text{Syl}_5$ beliebige 5-Sylowgruppen. Da nach dem Zweiten Sylowsatz alle 5-Sylowgruppen zueinander konjugiert sind, existiert ein $g \in G$ mit $P' = gPg^{-1} = g \cdot P$, also gilt $P' \in G(P)$.

- d** Wir konstruieren zunächst diesen Homomorphismus: Mittels der Gruppenoperation \cdot kann man durch

$$G \rightarrow \text{Per}(\text{Syl}_5), \quad g \mapsto \tau_g \quad \tau_g(P) = gPg^{-1}$$

jedem Gruppenelement eine Permutation von Syl_5 zuordnen (und diese Zuordnung definiert einen Homomorphismus).

Aufgrund der Annahme $|\text{Syl}_5| = v_5 = 6$ gibt es einen Isomorphismus $\text{Per}(\text{Syl}_5) \xrightarrow{\sim} S_6$. Nach Komposition mit dem Homomorphismus $G \rightarrow \text{Per}(\text{Syl}_5)$ von oben haben wir deshalb einen Homomorphismus

$$\lambda: G \rightarrow S_6.$$

Wir behaupten, dass $\ker \lambda$ nicht-trivial ist, denn dann ist $\ker \lambda$ ein nicht-trivialer Normalteiler.

Wäre $\ker \lambda = \{e\}$, so wäre λ injektiv. Nun ist aber $|S_6| = 6! = 720$ und $|G| = 750 > 720$, sodass es keine injektive Abbildung $G \rightarrow S_6$ geben kann.

Wäre andererseits $\ker \lambda = G$, dann würde das bedeuten, dass $\lambda(g) = \tau_g = \text{id}$ für alle $g \in G$ ist. Folglich wäre $gPg^{-1} = \tau_g(P) = P$ für beliebiges $g \in G, P \in \text{Syl}_5$ und jede Sylowgruppe daher ein Normalteiler. Das ist nur möglich, falls $v_5 = 1$ – Widerspruch zur Annahme $v_5 = 6$.

Bestimmung von Isomorphie-Typen

Das Ziel der folgenden Aufgaben ist es, für eine Gruppe G eine vollständige Liste von Gruppen anzugeben, zu denen G isomorph sein kann. Dabei werden wir häufig den Begriff des Komplexprodukts aus dem letzten Kapitel verwenden. Um die Ordnung solcher Komplexprodukte zu bestimmen, verwenden wir den 1. Isomorphiesatz 1.10 (1), welcher

$$M \diagup M \cap N \cong MN \diagup N$$

für einen Normalteiler $N \trianglelefteq G$ und eine Untergruppe $M \subseteq G$ einer Gruppe G liefert. Aus der Isomorphie ergibt sich für endliches G laut dem Satz von Lagrange:

$$\frac{|M|}{|M \cap N|} = \frac{|MN|}{|N|} \quad \Leftrightarrow \quad |MN| = \frac{|M| \cdot |N|}{|M \cap N|}.$$

Anleitung: Isomorphie-Typ von Gruppen mittels Sylowsätzen bestimmen

Sei G eine endliche Gruppe, sodass die Primfaktorzerlegung von $|G|$ höchstens Quadrate (aber keine höheren Potenzen) enthält. Oft funktioniert Folgendes:

- (1) Zeige, dass alle Sylowuntergruppen Normalteiler sind.
- (2) Zeige, dass G das innere direkte Produkt seiner Sylowuntergruppen ist (bilde hierzu ggf. schrittweise innere direkte Produkte).
- (3) Da das innere direkte Produkt stets isomorph zum äußeren direkten Produkt ist, lässt sich G als äußeres direktes Produkt seiner Sylowuntergruppen schreiben.
- (4) Eine Gruppe der Ordnung p^2 ist isomorph zu $\mathbb{Z}/p^2\mathbb{Z}$ oder $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$, jede Gruppe der Ordnung p ist isomorph zu $\mathbb{Z}/p\mathbb{Z}$. Wende dies sowie den Chinesischen Restsatz wiederholt an, um die gewünschte Liste zu erhalten.

Aufgabe (Herbst 2015, T1A3)

Bestimmen Sie bis auf Isomorphie sämtliche endliche Gruppen G der Ordnung $143 = 11 \cdot 13$.

Lösungsvorschlag zur Aufgabe (Herbst 2015, T1A3)

Der Dritte Sylowsatz liefert für die Anzahl ν_{11} der 11-Sylowgruppen bzw. die Anzahl ν_{13} der 13-Sylowgruppen, dass

$$\nu_{11} \mid 13 \quad \Rightarrow \quad \nu_{11} \in \{1, 13\} \quad \text{und} \quad \nu_{13} \mid 11 \quad \Rightarrow \quad \nu_{13} \in \{1, 11\}.$$

Wegen

$$1 \equiv 1 \pmod{11}, \quad 13 \equiv 2 \pmod{11}, \quad 1 \equiv 1 \pmod{13}, \quad 11 \not\equiv 1 \pmod{13}$$

erhält man daraus $\nu_{11} = \nu_{13} = 1$.

Sei nun P_{11} die einzige 11-Sylowgruppe bzw. P_{13} die einzige 13-Sylowgruppe. Beide sind laut Proposition 1.28 Normalteiler von G , sodass das Komplexprodukt $P_{11}P_{13}$ eine Untergruppe von G ist. Weiter ist $P_{11} \cap P_{13}$ sowohl eine Untergruppe von P_{11} als auch von P_{13} , sodass $|P_{11} \cap P_{13}|$ sowohl 11 als auch 13 teilen muss. Auf diese Weise folgt $|P_{11} \cap P_{13}| = 1$. Nach der Formel von oben ist nun

$$|P_{11}P_{13}| = \frac{|P_{11}||P_{13}|}{|P_{11} \cap P_{13}|} = 143 = |G|,$$

sodass bereits $G = P_{11}P_{13}$ gelten muss. Damit ist G das innere direkte Produkt von P_{11} und P_{13} und gemäß Satz 1.22 folgt

$$G = P_{11} \cdot P_{13} \cong P_{11} \times P_{13}.$$

Da die Ordnungen von P_{11} und P_{13} jeweils Primzahlen sind, sind sie isomorph zu zyklischen Gruppen und wir erhalten weiter mit dem Chinesischen Restsatz:

$$G \cong P_{11} \times P_{13} \cong \mathbb{Z}/11\mathbb{Z} \times \mathbb{Z}/13\mathbb{Z} \cong \mathbb{Z}/143\mathbb{Z}$$

Die einzigen Gruppen der Ordnung 143 sind also zyklische Gruppen.

Aufgabe (Frühjahr 2010, T2A1)

Zeigen Sie, dass es bis auf Isomorphie genau zwei Gruppen der Ordnung 99 gibt.

Lösungsvorschlag zur Aufgabe (Frühjahr 2010, T2A1)

Sei G eine Gruppe der Ordnung 99. Wir betrachten die Anzahlen der 3- und der 11-Sylowgruppen in G . Wir erhalten

$$\nu_3 \mid 11 \Rightarrow \nu_3 \in \{1, 11\} \quad \text{und} \quad \nu_{11} \mid 9 \Rightarrow \nu_{11} \in \{1, 3, 9\}.$$

Weiter ist

$$1 \equiv 1 \pmod{3}, \quad 11 \equiv 2 \not\equiv 1 \pmod{3}, \quad 1 \equiv 1 \pmod{11}, \quad 3 \not\equiv 1 \pmod{11}, \\ 9 \not\equiv 1 \pmod{11}$$

und somit kann nur $\nu_3 = \nu_{11} = 1$ sein. Bezeichnen wir die beiden Sylowgruppen von G als P_3 und P_{11} , so ist $|P_3| = 3^2$ bzw. $|P_{11}| = 11$.

Wegen $\nu_3 = \nu_{11} = 1$ sind P_3 und P_{11} Normalteiler von G . Zudem gilt $P_3 \cap P_{11} = \{e\}$, denn die Ordnung jedes Elements im Schnitt müsste sowohl 11 als auch 9 teilen und muss damit bereits 1 sein. Zuletzt ist $G = P_3 \cdot P_{11}$, denn „ \supseteq “ ist klar und mit der Formel von oben gilt:

$$|P_3 \cdot P_{11}| = \frac{|P_3| \cdot |P_{11}|}{|P_3 \cap P_{11}|} = 99 = |G|.$$

Insgesamt ist G somit das innere direkte Produkt von P_3 und P_{11} . Da das innere direkte Produkt isomorph zum äußeren direkten Produkt ist (siehe Satz 1.22), erhält man

$$G = P_3 \cdot P_{11} \cong P_3 \times P_{11}.$$

Nun ist P_3 eine Gruppe von Primzahlquadrat-Ordnung, also abelsch. Damit wissen wir aber aus dem Hauptsatz für endlich erzeugte abelsche Gruppen 1.12, dass

$$P_3 \cong \mathbb{Z}/9\mathbb{Z} \quad \text{oder} \quad P_3 \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}.$$

Wir erhalten für G die beiden Möglichkeiten

$$G \cong \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z} \quad \text{oder} \quad G \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z}.$$

Diese beiden Gruppen sind *nicht* isomorph zueinander: Mit $(\bar{1}, \bar{1})$ enthält die erste Gruppe ein Element der Ordnung 99, während für ein beliebiges Element g der zweiten Gruppe gilt, dass

$$33 \cdot g = 33 \cdot (g_1, g_2, g_3) = (33 \cdot g_1, 33 \cdot g_2, 33 \cdot g_3) = (\bar{0}, \bar{0}, \bar{0})$$

und die Ordnung jedes Element damit ein Teiler von 33 ist.

Aufgabe (Herbst 2002, T3A1)

Es sei $p \in \mathbb{N}$ eine Primzahl ≥ 5 derartig, dass auch $q = p + 2$ eine Primzahl ist, z. B. $p = 17$ und $q = 19$.

- a** Es sei G eine Gruppe der Ordnung $p^2 \cdot q^2$. Bestimmen Sie Anzahlen und Ordnungen der Sylow-Untergruppen von G .
- b** Bestimmen Sie alle Isomorphietypen von Gruppen der Ordnung $104329 = 323^2$.

Lösungsvorschlag zur Aufgabe (Herbst 2002, T3A1)

- a** Sei ν_p die Anzahl der p -Sylowgruppen von G , dann gilt laut dem Dritten Sylowsatz, dass

$$\nu_p \mid q^2 \quad \Rightarrow \quad \nu_p \in \{1, q, q^2\}$$

und wegen $q = p + 2$ ist $q \equiv 2 \pmod{p}$ sowie $q^2 \equiv 4 \pmod{p}$. Laut Angabe ist außerdem $4 < p$, sodass $4 \neq 1 \pmod{p}$. Also ist nur $\nu_p = 1$ möglich. Für die zweite Anzahl ν_q gilt analog

$$\nu_q \mid p^2 \quad \Rightarrow \quad \nu_q \in \{1, p, p^2\}$$

und $p \equiv -2 \pmod{q}$ sowie $p^2 \equiv 4 \pmod{q}$. Wegen $q \geq 7$ sind auch hier p und p^2 nicht kongruent zu 1, sodass nur die Möglichkeit $\nu_q = 1$ bleibt.

Es gibt also nur jeweils eine p - bzw. q -Sylowgruppe und diese haben die Ordnungen p^2 bzw. q^2 .

b Zunächst bemerken wir, dass $323 = 17 \cdot 19$ ist – das Beispiel aus der Einleitung. Damit gilt $|G| = 17^2 \cdot 19^2$ und wir können Teil **a** anwenden.

Es gibt also eine 17-Sylowgruppe der Ordnung 17^2 und eine 19-Sylowgruppe der Ordnung 19^2 , welche wir mit P_{17} bzw. P_{19} bezeichnen. Außerdem bemerken wir, dass G das innere direkte Produkt der beiden Gruppen ist (der Nachweis verläuft völlig analog zu obigen Aufgaben). Da das innere zum äußeren direkten Produkt isomorph ist, erhalten wir

$$G \cong P_{17} \times P_{19}.$$

Es sind P_{17} und P_{19} beides Gruppen von Primzahlquadratordnung, sodass sie abelsch sind. Es gilt somit

$$P_{17} \cong (\mathbb{Z}/17\mathbb{Z})^2 \quad \text{oder} \quad P_{17} \cong \mathbb{Z}/17^2\mathbb{Z}$$

und eine analoge Aussage für P_{19} . Damit muss G zu einer der folgenden vier Gruppen isomorph sein:

$$\begin{array}{ll} G_1 = \mathbb{Z}/17^2\mathbb{Z} \times \mathbb{Z}/19^2\mathbb{Z} & G_2 = (\mathbb{Z}/17\mathbb{Z})^2 \times \mathbb{Z}/19^2\mathbb{Z} \\ G_3 = \mathbb{Z}/17^2\mathbb{Z} \times (\mathbb{Z}/19\mathbb{Z})^2 & G_4 = (\mathbb{Z}/17\mathbb{Z})^2 \times (\mathbb{Z}/19\mathbb{Z})^2 \end{array}$$

Den Nachweis, dass diese Gruppen nicht isomorph sind, kann man analog zu Aufgabe F10T2A1 (Seite 48) führen.

Aufgabe (Herbst 2004, T2A1)

Seien p, q Primzahlen mit $p < q$. Zeigen Sie:

- a** Im Fall $p \nmid (q - 1)$ ist jede Gruppe der Ordnung pq abelsch.
- b** Jede abelsche Gruppe der Ordnung pq ist zyklisch.
- c** Im Fall $p \mid (q - 1)$ gibt es eine nicht-abelsche Gruppe der Ordnung pq .

Lösungsvorschlag zur Aufgabe (Herbst 2004, T2A1)

a Wir wenden den Dritten Sylowsatz an und erhalten zunächst für die Anzahl der p -Sylowgruppen wegen $\nu_p \mid q$, dass $\nu_p \in \{1, q\}$. Wäre nun $q \equiv 1 \pmod p$, so würde folgen, dass $q - 1 \equiv 0 \pmod p$, d. h. $p \mid (q - 1)$ im Widerspruch zur Voraussetzung. Es gilt also $\nu_p \not\equiv 1 \pmod p$, also $\nu_p = 1$.

Für die Anzahl ν_q der q -Sylowgruppen erhalten wir genauso zuerst $\nu_q \in \{1, p\}$, wegen $p < q$ gilt hier, dass $p \not\equiv 1 \pmod q$ und somit erhalten wir auch hier $\nu_q = 1$.

Damit gibt es genau eine p -Sylowgruppe P_1 mit p Elementen und genau eine q -Sylowgruppe P_2 mit q Elementen. Insbesondere sind beide Untergruppen Normalteiler von G . Da beide zudem Primzahlordnung haben, sind P_1 und P_2 zyklisch. Wie zuvor ist G somit das innere direkte Produkt von P_1 und P_2 und wir erhalten

$$G \cong P_1 \times P_2.$$

G ist daher als direktes Produkt zweier abelscher Gruppen selbst abelsch.

b Aus dem Chinesischen Restsatz folgt

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

Somit ist G zyklisch.

c Wir konstruieren eine solche Gruppe mittels eines semidirekten äußeren Produkts wie auf Seite 34 beschrieben. Wir betrachten dazu zunächst die Gruppen $\mathbb{Z}/p\mathbb{Z}$ und $\mathbb{Z}/q\mathbb{Z}$. Es gilt

$$\text{Aut}(\mathbb{Z}/q\mathbb{Z}) \cong (\mathbb{Z}/q\mathbb{Z})^\times \cong \mathbb{Z}/(q-1)\mathbb{Z}. \quad (*)$$

Um einen Homomorphismus $\mathbb{Z}/p\mathbb{Z} \rightarrow \mathbb{Z}/(q-1)\mathbb{Z}$ zu definieren, genügt es, das Bild von $\bar{1}$ anzugeben. Da $\mathbb{Z}/(q-1)\mathbb{Z}$ zyklisch ist und p laut Voraussetzung ein Teiler der Gruppenordnung ist, existiert ein Element $\bar{k} \in \mathbb{Z}/(q-1)\mathbb{Z}$, das Ordnung p hat. Somit existiert ein eindeutig bestimmter Homomorphismus

$$\psi: \mathbb{Z}/p\mathbb{Z} \rightarrow \mathbb{Z}/(q-1)\mathbb{Z} \quad \text{mit} \quad \psi(\bar{1}) = \bar{k}.$$

Dieser ist nicht-trivial, da bereits das Einselement nicht auf $\bar{0}$ abgebildet wird. Aufgrund der Isomorphie $(*)$ existiert auch ein nicht-trivialer Homomorphismus $\phi: \mathbb{Z}/p\mathbb{Z} \rightarrow \text{Aut}(\mathbb{Z}/q\mathbb{Z})$. Wir können somit ein semidirektes äußeres Produkt

$$G = \mathbb{Z}/p\mathbb{Z} \rtimes_\phi \mathbb{Z}/q\mathbb{Z}$$

definieren. Dieses ist eine nicht-abelsche Gruppe der Ordnung pq .

Sylowsätze und semidirektes Produkt

Wir haben im letzten Kapitel Proposition 1.23 verwendet, um spezielle nicht-abelsche Gruppen zu konstruieren. Da die Proposition eine Äquivalenzaussage macht, sagt sie umgekehrt aber auch aus, wann ein semidirektes Produkt abelsch ist und damit dem direkten Produkt entspricht. Dies ist in manchen Aufgaben zu den Sylowsätzen nützlich.

Anleitung: Isomorphie-Typ von Gruppen mittels Sylowsätzen und semidirektem Produkt bestimmen

Sei G eine Gruppe.

- (1) Verwende die Sylowsätze, um die Anzahlen der jeweiligen Sylowgruppen von G einzuschränken. Optimalerweise ist dann
 - eine Sylowgruppe oder ein Produkt von Sylowgruppen ein Normalteiler N von G und
 - N abelsch und von bekanntem Isomorphietyp, da z. B. die Ordnung von N eine Primzahl ist.
- (2) In aller Regel wird es nun eine Sylowgruppe P von G geben, die $G = NP$ und $N \cap P = \{e\}$ aus Ordnungsgründen erfüllt, von der man aber nicht weiß, ob sie ein Normalteiler ist. Nach Satz 1.22 (2) ist G isomorph zu einem semidirekten Produkt $P \rtimes_{\phi} N$ mit einem Homomorphismus $\phi: P \rightarrow \text{Aut}(N)$.
- (3) Kann man ausschließen, dass es einen nicht-trivialen Homomorphismus $\phi: P \rightarrow \text{Aut}(N)$ gibt, so ist $G \cong P \times N$ nach Proposition 1.23. Dazu kann man meist eine der beiden gleichwertigen Vorgehensweisen befolgen:
 - Ist $a \in P$, dann muss die Ordnung von $\phi(a)$ ein Teiler der Ordnung von a sein. Sind $|P|$ und $|\text{Aut}(N)|$ teilerfremd (verwende ggf. Proposition 1.24 (2)), so muss $\phi(a) = \text{id}_N$ sein. Da a beliebig gewählt war, folgt $\phi(a) = \text{id}_N$ für alle $a \in P$, d. h. ϕ ist trivial.
 - Es ist $\phi(P)$ eine Untergruppe von $\text{Aut}(N)$, d. h. $|\phi(P)|$ muss $|\text{Aut}(N)|$ teilen. Gleichzeitig ist laut Homomorphiesatz $P / \ker \phi \cong \phi(P)$, sodass $|\phi(P)|$ auch ein Teiler von $|P|$ ist. Haben P und $\text{Aut}(N)$ teilerfremde Ordnungen, so muss $\phi(P) = \{\text{id}_N\}$ sein, d. h. ϕ ist trivial.

Aufgabe (Herbst 2000, T1A1)

Sei G eine Gruppe mit 2001 Elementen. Zeigen Sie:

- a** Die p -Sylowgruppen sind für $p = 23$ und $p = 29$ normal.
- b** Auch die 3-Sylowgruppe von G ist normal.
- c** Die Gruppe G istzyklisch.

Lösungsvorschlag zur Aufgabe (Herbst 2000, T1A1)

- a** Es gilt $2001 = 3 \cdot 23 \cdot 29$. Wir verwenden zunächst den Dritten Sylowsatz und erhalten für die Anzahl der 23-Sylowgruppen ν_{23}

$$\nu_{23} \mid 3 \cdot 29 \quad \Rightarrow \quad \nu_{23} \in \{1, 3, 29, 3 \cdot 29\}.$$

Wegen

$$3 \not\equiv 1 \pmod{23}, \quad 29 \equiv 6 \pmod{23} \text{ und } 3 \cdot 29 \equiv 3 \cdot 6 \equiv 18 \pmod{23}$$

ist nur $\nu_{23} = 1$ möglich. Dies bedeutet bereits, dass die einzige 23-Sylowgruppe von G ein Normalteiler ist.

Eine völlig analoge Rechnung zeigt $\nu_{29} = 1$, also ist auch die 29-Sylowgruppe ein Normalteiler von G .

b Wir schränken die Anzahl ν_3 der 3-Sylowgruppen zunächst ein:

$$\nu_3 \mid 23 \cdot 29 \Rightarrow \nu_3 \in \{1, 23, 29, 23 \cdot 29\},$$

$$23 \equiv 2 \pmod{3}, \quad 29 \equiv 2 \pmod{3}, \quad 23 \cdot 29 \equiv 2 \cdot 2 \equiv 4 \equiv 1 \pmod{3},$$

somit kann $\nu_3 = 1$ oder $\nu_3 = 23 \cdot 29 = 667$ sein.

Sei P_{23} die einzige 23-Sylowgruppe und P_{29} die einzige 29-Sylowgruppe. Wir zeigen nun, dass G das innere direkte Produkt von P_{23} , P_{29} und einer beliebigen 3-Sylowgruppe P_3 ist. Setze dazu $N = P_{23} \cdot P_{29}$. Da nach Teil **a** sowohl P_{23} als auch P_{29} ein Normalteiler ist, ist N ebenfalls ein Normalteiler von G .

N hat als inneres direktes Produkt von P_{23} und P_{29} die Ordnung $23 \cdot 29$. Es folgt $N \cap P_3 = \{e\}$, da die Ordnungen von P_3 und N teilerfremd sind. Es bleibt noch zu zeigen, dass $G = NP_3$ gilt. Dazu berechnen wir:

$$|NP_3| = \frac{|N| \cdot |P_3|}{|N \cap P_3|} = \frac{23 \cdot 29 \cdot 3}{1} = 23 \cdot 29 \cdot 3 = |G|.$$

Zusammen mit $NP_3 \subseteq G$ erhalten wir daraus $NP_3 = G$. Insgesamt ist also G tatsächlich ein inneres semidirektes Produkt von N und P_3 . Damit ist G isomorph zum äußeren semidirekten Produkt dieser Untergruppen, d. h.

$$G \cong N \rtimes_\phi P_3$$

für einen geeigneten Homomorphismus $\phi: P_3 \rightarrow \text{Aut}(N)$. Wir zeigen, dass dafür nur die triviale Abbildung in Frage kommt. Es gilt

$$\text{Aut}(N) \cong \text{Aut}(\mathbb{Z}/23\mathbb{Z} \times \mathbb{Z}/29\mathbb{Z}) \cong (\mathbb{Z}/23\mathbb{Z} \times \mathbb{Z}/29\mathbb{Z})^\times.$$

Also hat $\text{Aut}(N)$ die Ordnung $\varphi(23 \cdot 29) = 22 \cdot 28$. Ist $a \in P_3$, so ist $\text{ord } a$ ein Teiler von 3 und auch die Ordnung von $\phi(a)$ muss 3 teilen. Wegen $3 \nmid 22 \cdot 28$ kommt dafür nur 1 in Frage, und es gilt $\phi(a) = \text{id}$ für alle $a \in P_3$. Damit ist ϕ trivial und G ist sogar das direkte äußere Produkt von N und P_3 , d. h.

$$G \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/(23 \cdot 29)\mathbb{Z}. \tag{*}$$

Somit ist G aber abelsch, d. h. jede Untergruppe ist Normalteiler. Insbesondere gilt das für die – beliebig gewählte – 3-Sylowgruppe P_3 .

- c** Aus der Isomorphie (\star) und dem Chinesischen Restsatz folgt unmittelbar

$$G \cong \mathbb{Z}/2001\mathbb{Z}.$$

Aufgabe (Frühjahr 2003, T3A1)

Zeigen Sie, dass jede Gruppe der Ordnung 255 zyklisch ist!

Lösungsvorschlag zur Aufgabe (Frühjahr 2003, T3A1)

Sei G eine Gruppe der Ordnung $255 = 3 \cdot 5 \cdot 17$. Wir betrachten die Anzahlen der 3-, 5- und 17-Sylowgruppen. Es gilt

$$\nu_3 \mid 5 \cdot 17 \quad \Rightarrow \quad \nu_3 \in \{1, 5, 17, 5 \cdot 17\}$$

Wegen

$$5 \not\equiv 1 \pmod{3}, \quad 17 \not\equiv 1 \pmod{3} \quad \text{und} \quad 5 \cdot 17 \equiv 2 \cdot 2 \equiv 1 \pmod{3}$$

verbleibt $\nu_3 \in \{1, 85\}$. Mit einer analogen Rechnung findet man $\nu_5 \in \{1, 51\}$ sowie $\nu_{17} = 1$. Zumindest hier gilt sofort $\nu_{17} = 1$ und die einzige 17-Sylowgruppe P_{17} ist ein Normalteiler von G .

Nehmen wir an, dass sowohl $\nu_3 = 85$ als auch $\nu_5 = 51$ gilt. Da jede 3-Sylowgruppe 2 Elemente der Ordnung 3 enthält und jeweils zwei Gruppen sich nur im Neutralelement schneiden, liefern diese $85 \cdot 2 = 170$ Elemente. Ebenso liefern die 5-Sylowgruppen $4 \cdot 51 = 204$ Elemente. Insgesamt ist damit bereits die Zahl der Elemente von G überschritten. Damit muss (mindestens) eine der beiden Anzahlen 1 sein.

1. Fall: $\nu_3 = 1$. Wir betrachten die Menge

$$N = P_3 \cdot P_{17},$$

wobei P_3 die 3-Sylowgruppe, P_{17} die 17-Sylowgruppe ist. Bei beiden Sylowgruppen handelt es sich um Normalteiler von G , sodass auch N ein Normalteiler von G ist. Wie in vorangegangenen Aufgaben zeigt man, dass N das innere direkte Produkt von P_3 und P_{17} ist und erhält mit dem Chinesischen Restsatz

$$N \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/17\mathbb{Z} \cong \mathbb{Z}/51\mathbb{Z}.$$

Ist nun P_5 eine beliebige 5-Sylowgruppe, so gilt $P_5 \cap N = \{e\}$, da die Ordnungen von N und P_5 teilerfremd sind. Ferner ist

$$|P_5 \cdot N| = \frac{|P_5| \cdot |N|}{|P_5 \cap N|} = |P_5| \cdot |N| = 255 = |G|$$

und zusammen mit $P_5N \subseteq G$ folgt $P_5N = G$. Wegen Satz 1.22 (2) gibt es einen Homomorphismus $\phi: P_5 \rightarrow \text{Aut}(N)$, sodass $G \cong N \rtimes_{\phi} P_5$ gilt. Untersuchen wir nun die Gruppe $\text{Aut}(N)$ näher. Mit 1.24 (2) erhalten wir

$$\text{Aut}(N) \cong (\mathbb{Z}/51\mathbb{Z})^{\times}.$$

Damit haben P_5 und $\text{Aut}(N)$ wegen $|P_5| = 5$ und

$$|\text{Aut}(N)| = \varphi(51) = \varphi(3) \cdot \varphi(17) = 2 \cdot 16 = 32$$

teilerfremde Ordnungen. Ist $a \in P_5$, so ist $\text{ord } \phi(a)$ ein Teiler von 5 und von 32, was nur für $\text{ord } \phi(a) = 1$ möglich ist. Der Homomorphismus ϕ muss also trivial sein, sodass G sogar direktes Produkt von N und P_5 ist. Wir erhalten mit dem Chinesischen Restsatz

$$G \cong P_5 \times N \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/51\mathbb{Z} \cong \mathbb{Z}/255\mathbb{Z}.$$

2. Fall: $\nu_5 = 1$. Das Verfahren hier verläuft analog: Betrachte den Normalteiler

$$N = P_5 \cdot P_{17} \trianglelefteq G.$$

In diesem Fall ist G das innere semidirekte Produkt von N und einer beliebigen 3-Sylowgruppe von G . Damit gilt $G \cong N \rtimes_{\psi} P_3$ für einen Homomorphismus $\psi: P_3 \rightarrow \text{Aut}(N)$. Nach analoger Argumentation wie oben berechnet man $|\text{Aut}(N)| = \varphi(5) \cdot \varphi(17) = 64$ und aus der Teilerfremdheit von $|P_3|$ und $|N|$ folgt, dass ψ trivial ist, was wiederum $G \cong \mathbb{Z}/255\mathbb{Z}$ bedeutet.

1.5. Auflösbare Gruppen

Definition 1.29. Eine Gruppe G heißt **auflösbar**, falls G eine **abelsche Normalreihe** besitzt, d. h. es gibt ein $r \in \mathbb{N}_0$ und eine Kette von Untergruppen $G_i \subseteq G$ der Form

$$\{e\} = G_0 \trianglelefteq G_1 \trianglelefteq \dots \trianglelefteq G_r = G,$$

sodass G_i/G_{i-1} für $i \in \{1, \dots, r\}$ jeweils eine abelsche Gruppe ist.

Man kann sich leicht überlegen, dass jede abelsche Gruppen auflösbar ist. Ist nämlich G abelsch, so definiert

$$\{e\} \trianglelefteq G$$

eine Normalreihe. Der Faktor $G/\{e\}$ ist isomorph zu G und damit abelsch.

Folgender Satz ist Grundlage für viele Aufgaben – er führt die Auflösbarkeitsbedingung auf kleinere Gruppen zurück.

Satz 1.30. Sei G eine Gruppe und $N \trianglelefteq G$ ein Normalteiler. G ist genau dann auflösbar, wenn N und G/N auflösbar sind.

Von elementarer Bedeutung für spätere Anwendungen ist die Auflösbarkeit der symmetrischen Gruppe S_n . Man überlegt sich leicht, dass diese für $n \leq 3$ auflösbar ist. Die Auflösbarkeit der S_4 wird Inhalt der ersten Aufgabe sein. Für $n \geq 5$ enthält die Gruppe mit A_n einen einfachen, nicht-abelschen Normalteiler und damit kann S_n gemäß Satz 1.30 nicht auflösbar sein.

Im echten Leben werden so gut wie alle Gruppen auflösbar sein – so kann man beispielsweise zeigen, dass alle Gruppen ungerader Ordnung auflösbar sind. Außerdem ist jede Untergruppe einer auflösbaren Gruppe wieder auflösbar.

Exkurs: Auflösbarkeit von Gruppen – Wozu?

Ein tiefergehendes Verständnis für die Bedeutung des Begriffs der Auflösbarkeit ist nur im Zusammenhang mit der Galois-Theorie möglich. Stellt man sich nämlich die Frage der Existenz von allgemeinen Lösungsformeln für Polynomgleichungen höheren Grades (wie wir sie mit der Mitternachtsformel für quadratische Polynome kennen), so erlaubt der Begriff der Auflösbarkeit die Formulierung dieses Problems auf gruppentheoretische Weise.

Eine Körpererweiterung $L|K$ bezeichnet man als **Radikalerweiterung**, wenn es ein $r \in \mathbb{N}_0$ und ein Kette von Körpererweiterungen der Form

$$L = K_r \supsetneq \dots \supsetneq K_1 \supsetneq K_0 = K$$

gibt, wobei für $i \in \{1, \dots, r\}$ die Gleichung $K_i = K_{i-1}(\alpha_i)$ für ein Element $\alpha_i \in E$ und $\alpha_i^{e_i} \in K_i$ gilt (also ist α_i eine e_i -te Wurzel aus dem vorangegangenen Körper). Liegt nun der Zerfällungskörper eines Polynoms $f \in K[x]$ in einer solchen Radikalerweiterung, so sind alle Nullstellen als verschachtelte Wurzel-Ausdrücke darstellbar und wir nennen das Polynom f **durch Radikale auflösbar**.

Die Verbindung zwischen dem Auflösbarkeitsbegriff der Gruppentheorie und dem eben definierten liefert nun die Galois-Theorie: Sei K ein Körper mit Charakteristik 0 und L der Zerfällungskörper eines Polynoms $f \in K[x]$, sowie $G_{L|K}$ die Galois-Gruppe von f über K . Ist $G_{L|K}$ eine auflösbare Gruppe, so gibt es eine abelsche Normalreihe der Form

$$\{e\} = G_0 \trianglelefteq G_1 \trianglelefteq \dots \trianglelefteq G_r = G.$$

Diese korrespondiert zu einer Kette von Zwischenkörpern

$$L = K_0 \supseteq K_1 \supseteq \dots \supseteq K_r = K,$$

wobei die Körpererweiterungen jeweils normal sind. Es stellt sich heraus, dass dies eine notwendige und hinreichende Bedingung dafür ist, dass die untere Kette eine Radikalerweiterung beschreibt. Man erhält so die folgende Aussage.

Satz 1.31. Sei K ein Körper mit $\text{char } K = 0$. Dann ist $f \in K[X]$ genau dann durch Radikale auflösbar, wenn seine Galois-Gruppe $\text{Gal}(f)$ auflösbar ist.

Da es Polynome gibt, deren Galois-Gruppe isomorph zu S_5 ist, kann es keine allgemeine Lösungsformel für Polynome von Grad ≥ 5 geben.

Aufgabe (Herbst 2003, T2A1)

- a** Definieren Sie die alternierende Gruppe A_n .
- b** Warum ist A_n für $n \geq 2$ eine Untergruppe vom Index 2 in S_n ?
- c** Zeigen Sie, dass die Gruppe S_4 auflösbar ist.

Lösungsvorschlag zur Aufgabe (Herbst 2003, T2A1)

- a** Sei $n \in \mathbb{N}$ und S_n die symmetrische Gruppe vom Grad n . Die Menge A_n ist die Untergruppe von S_n , die aus den Permutationen mit positivem Signum besteht:

$$A_n = \{\sigma \in S_n \mid \text{sgn}(\sigma) = +1\}$$

Hierbei bezeichnet $\text{sgn}: S_n \rightarrow \{\pm 1\}$ den Signumshomomorphismus.

- b** Die Signumsfunktion ist für $n \geq 2$ surjektiv: Es gilt nämlich $\text{sgn id} = +1$ und $\text{sgn}(1 2) = -1$. Für den ihren Kern gilt

$$\sigma \in \ker \text{sgn} \iff \text{sgn}(\sigma) = 1 \iff \sigma \in A_n.$$

Somit liefert der Homomorphiesatz

$$S_n / A_n \cong \{\pm 1\}.$$

Insbesondere bedeutet dies laut dem Satz von Lagrange

$$(S_n : A_n) = |S_n / A_n| = 2.$$

- c** Wir zeigen, dass durch

$$\{\text{id}\} \trianglelefteq V_4 \trianglelefteq A_4 \trianglelefteq S_4$$

eine Normalreihe gegeben ist, deren Faktoren abelsch sind. Zeigen wir zunächst, dass jede der angegebenen Untergruppen jeweils Normalteiler der folgenden Untergruppe ist. Die Aussage $\{\text{id}\} \trianglelefteq V_4$ ist klar.

Für die nächste Normalteiler-Eigenschaft sei $\sigma \in A_4$ und $\tau \in V_4$. Der Zykel $\sigma\tau\sigma^{-1}$ hat denselben Zerlegungstyp wie τ . Da aber V_4 genau aus den Doppeltranspositionen in S_4 und der Identität besteht, und es sich bei $\sigma\tau\sigma^{-1}$ im Fall $\tau \neq \text{id}$ wiederum um eine Doppeltransposition handelt, gilt nach Lemma 1.36 insbesondere $\sigma\tau\sigma^{-1} \in V_4$ für beliebiges $\sigma \in A_4$. Damit ist V_4 ein Normalteiler von S_4 . Zuletzt gilt aufgrund von Teil **b**, dass $(S_4 : A_4) = 2$, und somit ist A_4 ein Normalteiler von S_4 .

Beweisen wir nun noch, dass die Faktoren abelsch sind: Für die beiden Faktoren S_4/A_4 und A_4/V_4 folgt dies daraus, dass diese laut dem Satz von Lagrange Ordnung 2 bzw. 3 haben und somit als Gruppen von Primzahlordnung sogar zyklisch, insbesondere also abelsch sind. Für den ersten Faktor $V_4/\{\text{id}\} \cong V_4$ bemerken wir, dass dieser als Gruppe von Primzahlquadratordnung ebenso abelsch ist.

Anleitung: Auflösbarkeit unter Verwendung der Sylowsätze

Sei G eine endliche Gruppe.

- (1) Finde mithilfe der Sylowsätze einen Normalteiler N in G und zeige, dass dieser auflösbar ist. Das ist z. B. der Fall, wenn N Primzahl- bzw. Primzahlquadratordnung hat, da N dann zyklisch (bzw. abelsch) und somit auflösbar ist.
- (2) Berechne die Ordnung der Faktorgruppe G/N mit dem Satz von Lagrange. Ggf. reicht dies wie bei (1) schon, um zu zeigen, dass die Faktorgruppe auflösbar ist. Ansonsten beginne wieder bei (1), mit G/N statt G .
- (3) Die Auflösbarkeit von G folgt letzten Endes aus Satz 1.30.

Aufgabe (Herbst 2000, T3A1)

- a** Geben Sie die Definitionen der Begriffe „Normalteiler“ und „auflösbare Gruppe“ an.
- b** Sei G eine Gruppe der Ordnung 100. Zeigen Sie:
- (i) G ist auflösbar.
 - (ii) Hat G einen Normalteiler der Ordnung 4, so ist G abelsch.

Hinweis Es darf verwendet werden, dass Gruppen der Ordnung p^2 abelsch sind, wenn p eine Primzahl ist.

Lösungsvorschlag zur Aufgabe (Herbst 2000, T3A1)

- a** Ein Normalteiler ist eine Untergruppe N von G mit $gN = Ng$ für alle $g \in G$. Für die Definition von auflösbarer Gruppe siehe Definition 1.29.
- b** (i): Wir nutzen zunächst den Dritten Sylowsatz und berechnen die Anzahl ν_p der p -Sylowgruppen. Es gilt mit $100 = 2^2 \cdot 5^2$:

$$\nu_2 \mid 25 \Rightarrow \nu_2 \in \{1, 5, 25\} \quad \text{und} \quad \nu_5 \mid 4 \Rightarrow \nu_5 \in \{1, 2, 4\}$$

sowie

$$1 \equiv 5 \equiv 25 \pmod{2}, \quad 1 \equiv 1 \pmod{5}, \quad 2 \not\equiv 1 \pmod{5}, \quad 4 \not\equiv 1 \pmod{5}.$$

Es folgt insgesamt $\nu_2 \in \{1, 5, 25\}$ und $\nu_5 = 1$. Zumindest die 5-Sylowgruppe P_5 ist also ein Normalteiler, mit dem wir arbeiten können. Wegen $5^2 \mid 100$ und $5^3 \nmid 100$ gilt $|P_5| = 5^2$, sodass P_5 abelsch und damit auflösbar ist. Für die Faktorgruppe gilt laut dem Satz von Lagrange

$$|G/P_5| = (G : P_5) = \frac{|G|}{|P_5|} = \frac{100}{25} = 4.$$

Da auch die Faktorgruppe somit Primzahlquadratordnung hat, ist auch diese abelsch, damit auflösbar. Mit Satz 1.30 folgt, dass auch G auflösbar ist.

(ii): Bezeichnen wir den Normateiler mit N . Wir zeigen, dass G ein inneres direktes Produkt der beiden Normalteiler N und P_5 ist. Da die Ordnungen der beiden Gruppen teilerfremd sind, gilt $P_5 \cap N = \{e\}$. Die Gleichung $G = P_5N$ folgt aus $P_5N \subseteq G$ und

$$|P_5N| = \frac{|N| \cdot |P_5|}{|N \cap P_5|} = \frac{100}{1} = |G|.$$

Somit ist G isomorph zum äußeren direkten Produkt der beiden Gruppen:

$$G \cong P_5 \times N$$

Da P_5 und N Primzahlquadratordnung haben, sind die beiden Gruppen abelsch, damit auch ihr direktes Produkt.

Aufgabe (Frühjahr 2015, T1A3)

Sei G eine Gruppe der Ordnung 105. Zeigen Sie:

- a** G hat einen Normalteiler N mit $|N| = 5$ oder $|N| = 7$.
- b** G ist auflösbar.

Lösungsvorschlag zur Aufgabe (Frühjahr 2015, T1A3)

- a** Es gilt $105 = 3 \cdot 5 \cdot 7$. Nach dem Dritten Sylowsatz gilt

$$\nu_5 \mid 21 \Rightarrow \nu_5 \in \{1, 3, 7, 21\} \quad \text{und} \quad \nu_7 \mid 15 \Rightarrow \nu_7 \in \{1, 3, 5, 15\}.$$

Weiter gilt

$$\begin{aligned} 1 &\equiv 1 \pmod{5}, \quad 3 \not\equiv 1 \pmod{5}, \quad 7 \equiv 2 \not\equiv 1 \pmod{5}, \quad 21 \equiv 1 \pmod{5}, \\ 1 &\equiv 1 \pmod{7}, \quad 3 \not\equiv 1 \pmod{7}, \quad 5 \not\equiv 1 \pmod{7}, \quad 15 \equiv 1 \pmod{7}. \end{aligned}$$

Und wir erhalten insgesamt $\nu_7 \in \{1, 15\}$ sowie $\nu_5 \in \{1, 21\}$. Nehmen wir nun an, dass $\nu_5 \neq 1$ und $\nu_7 \neq 1$, d. h. $\nu_5 = 21$ und $\nu_7 = 15$.

Die 5-Sylowgruppen haben 5 Elemente: das Neutralelement sowie 4 Elemente der Ordnung 5. Da jedes der Elemente der Ordnung 5 bereits die ganze 5-Sylowgruppe erzeugt, schneiden sich je zwei der 5-Sylowgruppen nur im Neutralelement. Somit existieren $4 \cdot 21 = 84$ Elemente der Ordnung 5. Das gleiche Argument liefert $6 \cdot 15 = 90$ Elemente der Ordnung 7. Damit müsste G aber zusammen mit dem Neutralelement

$$90 + 84 + 1 = 175 > 105$$

Elemente besitzen – Widerspruch. Eine der beiden Anzahlen muss also 1 sein – die zugehörige Sylowgruppe ist dann ein Normalteiler.

- b** 1. Fall. Es gibt eine normale 5-Sylowgruppe, d. h. einen Normalteiler N von G mit $|N| = 5$.

Da N Primzahlordnung hat, ist die Gruppe zyklisch, also abelsch und somit auflösbar. Für die Faktorgruppe G/N gilt

$$|G/N| = \frac{|G|}{|N|} = \frac{105}{5} = 21.$$

Wir untersuchen in G/N die Anzahl der 7-Sylowgruppen $\bar{\nu}_7$. Man erhält

$$\bar{\nu}_7 \mid 3 \Rightarrow \bar{\nu}_7 \in \{1, 3\}, \quad 1 \equiv 1 \pmod{7}, \quad 3 \not\equiv 1 \pmod{7}.$$

Somit ist die 7-Sylowgruppe P in G/N ein Normalteiler. Wir können also die Faktorgruppe $(G/N)/P$ betrachten. Für diese gilt nun

$$\left| (G/N)/P \right| = \frac{|G/N|}{|P|} = \frac{21}{7} = 3.$$

Damit ist die Faktorgruppe $(G/N)/P$ zyklisch, also auflösbar. Ebenso ist auch P auflösbar. Damit ist laut Satz 1.30 die Gruppe G/N auflösbar. Nochmalige Anwendung von Satz 1.30 liefert, dass G auflösbar ist.

2. Fall. Es gibt eine normale 7-Sylowgruppe, d. h. einen Normalteiler N von G mit $|N| = 7$. Da auch hier N Primzahlordnung hat, ist N zyklisch und somit auflösbar. Für die Faktorgruppe G/N erhält man $|G/N| = (G : N) = 15$. An dieser Stelle verfährt man entweder analog zu oben (d. h. man zeigt, dass in G/N wiederum die 5-Sylowgruppe ein Normalteiler ist, und folgert, dass somit G/N auflösbar ist) oder man weiß, dass Gruppen der Ordnung 15 stets zyklisch sind (der Allgemeinfall ist in H04T2A1 abgedeckt), weshalb sofort folgt, dass G/N auflösbar ist.

Aufgabe (Frühjahr 2015, T3A2)

Seien p, q, r Primzahlen mit $p < q < r$ und $pq < r + 1$. Zeigen Sie, dass jede Gruppe der Ordnung pqr auflösbar ist.

Lösungsvorschlag zur Aufgabe (Frühjahr 2015, T3A2)

Betrachten wir zunächst die Anzahl der r -Sylowgruppen ν_r . Es gilt gemäß dem Dritten Sylowsatz

$$\nu_r \mid pq \quad \Rightarrow \quad \nu_r \in \{1, p, q, pq\}.$$

Weiter gilt wegen $p < q < r$, dass

$$p \not\equiv 1 \pmod{r}, \quad q \not\equiv 1 \pmod{r}$$

und im Falle $pq \equiv 1 \pmod{r}$ würde folgen $pq = kr + 1$ für ein $k \in \mathbb{N}$ (der Fall $pq = 1$ ist ausgeschlossen, da p und q Primzahlen sind). Dies ist wegen $pq < r + 1$ jedoch nicht möglich. Folglich gilt $\nu_r = 1$ und die einzige r -Sylowgruppe, im Folgenden als P_r bezeichnet, ist ein Normalteiler der Gruppe G . Des Weiteren ist P_r als Gruppe von Primzahlordnung zyklisch, also auflösbar. Betrachten wir die Faktorgruppe G/P_r . Mit dem Satz von Lagrange folgt

$$|G/P_r| = \frac{pqr}{r} = pq.$$

Für die Anzahl ν_q der q -Sylowgruppen in G/P_r gilt

$$\nu_q \mid p \quad \Rightarrow \quad \nu_q \in \{1, p\}.$$

Wegen $p < q$ ist $p \not\equiv 1 \pmod{p}$. Somit ist die einzige p -Sylowgruppe in G/P_r ein Normalteiler. Bezeichnen wir diese mit P_q , so gilt wiederum nach dem Satz von Lagrange

$$\left| (G/P_r)/P_q \right| = \frac{pq}{q} = p.$$

An dieser Stelle wenden wir zweimal Satz 1.30 an: Als Gruppe von Primzahlordnung ist $(G/P_r)/P_q$ auflösbar. Da auch P_q auflösbar ist, folgt die Auflösbarkeit von G/P_r . Da neben dieser Faktorgruppe auch die Untergruppe P_r auflösbar ist, folgt schlussendlich die Auflösbarkeit von G .

1.6. Die Symmetrische Gruppe S_n

Sei X eine beliebige Menge, dann bezeichnen wir mit $\text{Per}(X)$ die Gruppe der bijektiven Abbildungen $X \rightarrow X$ und nennen sie die **Permutationsgruppe** von X . Der wichtigste Spezialfall davon ist die Permutationsgruppe der Menge $\{1, \dots, n\}$, welche gewöhnlich als S_n notiert wird und **Symmetrische Gruppe** heißt. Symmetrische Gruppen wurden historisch lange vor allgemeinen Gruppen studiert, was sich rückwirkend durch den Satz von Cayley legitimieren lässt:

Satz 1.32 (Cayley). Jede Gruppe der Ordnung n ist zu einer Untergruppe von S_n isomorph.

Der Satz von Cayley ist eine direkte Folgerung von Proposition 1.15 (1), indem man die Gruppe G auf sich selbst durch Linkstranslation operieren lässt. Falls der Leser nun bereits die Hoffnung hegt, alle Aufgaben über abstrakte Gruppen unter Verwendung des Satzes von Cayley einfach in der konkreten Gruppe S_n lösen zu können, muss an dieser Stelle darauf hingewiesen werden, dass S_n als Gruppe der Ordnung $n!$ im Allgemeinen sehr viel größer ist und daher dort das Problem meist eher schwieriger zu lösen ist.

Definition 1.33. Sei $n \in \mathbb{N}$ und $\sigma \in S_n$, dann heißt $\text{supp } (\sigma) = \{k \in \{1, \dots, n\} \mid \sigma(k) \neq k\}$ der **Träger** von σ . Zwei Permutationen $\sigma, \tau \in S_n$ heißen **disjunkt**, falls ihre Träger disjunkt sind.

Als erste praktische Anwendung des Begriffs des Trägers fällt die Aussage ab, dass disjunkte Permutationen kommutieren, d. h. sind $\sigma, \tau \in S_n$ disjunkt, so gilt $\sigma\tau = \tau\sigma$.

Wir wollen uns nun überlegen, wie viele k -Zykel es in der S_n gibt. Dazu bemerken wir zunächst, dass es $\binom{n}{k}$ Möglichkeiten gibt, den Träger eines k -Zykels in der S_n zu bilden. Aus den k Ziffern des Trägers kann man $k!$ verschiedene geordnete Ketten bilden, die jedoch den Zykel noch nicht eindeutig bestimmen, denn beispielsweise

beschreiben $(1\ 2\ \dots\ n)$ und $(n\ 1\ 2\ \dots\ n-1)$ die gleiche Abbildung. Berücksichtigt wird dies, indem wir deren Anzahl noch durch k teilen, sodass wir insgesamt

$$\binom{n}{k} \cdot (k-1)!$$

k -Zykel in S_n finden. Als nächstes sammeln wir Ergebnisse zur vereinfachten Berechnung der Ordnung von Permutationen:

Proposition 1.34. Seien $n, r \in \mathbb{N}$ und $2 \leq k \leq n$ sowie $2 \leq k_1, \dots, k_r \leq n$.

- (1) Jeder k -Zykel in S_n hat Ordnung k .
- (2) Sind $\sigma_1, \dots, \sigma_r \in S_n$ disjunkte k_i -Zykel, so hat das Produkt $\sigma_1 \cdot \dots \cdot \sigma_r$ die Ordnung $\text{kgV}(k_1, \dots, k_r)$.

Es sei auch an den *Signumshomomorphismus* $\text{sgn}: S_n \rightarrow \{\pm 1\}$ erinnert, welcher sich am einfachsten mithilfe der folgenden Aussagen charakterisieren lässt:

Proposition 1.35. Sei $n \in \mathbb{N}$ und $2 \leq k \leq n$.

- (1) Jede Permutation in S_n lässt sich als Produkt disjunkter Zykel darstellen.
- (2) Ist $\sigma \in S_n$ ein k -Zykel, so gilt für diesen $\text{sgn}(\sigma) = (-1)^{k-1}$.

Der Kern des Signumshomomorphismus ist die *Alternierende Gruppe* A_n , welche als Kern eines Homomorphismus ein Normalteiler von S_n ist. Für $n \geq 5$ besitzt A_n selbst jedoch keinen nicht-trivialen Normalteiler, ist also eine einfache Gruppe. Die Ordnung der A_n kann man für $n \geq 2$ mithilfe des Homomorphiesatzes berechnen, denn dieser liefert $S_n/A_n \cong \{\pm 1\}$, woraus man $|A_n| = \frac{1}{2}|S_n| = \frac{n!}{2}$ erhält. Im Fall $n = 1$ ist schlicht $A_1 = S_1$.

Ist $\sigma \in S_n$ und $\sigma = \sigma_1 \cdot \dots \cdot \sigma_r$ eine Darstellung von σ als Produkt disjunkter Zykel σ_i der Länge k_i mit $2 \leq k_1 \leq \dots \leq k_r$, so nennt man (k_1, \dots, k_r) den *Zerlegungstyp* von σ .

Lemma 1.36. Zwei Permutationen sind genau dann konjugiert zueinander, wenn sie den gleichen Zerlegungstyp besitzen.

Aufgabe (Herbst 2013, T3A3)

- a** Eine Permutation σ sei das Produkt zweier disjunkter Zykel der teilerfremden Längen k und l . Welche Ordnung hat σ ?
- b** Sei $a(n)$ die größte Elementordnung in der symmetrischen Gruppe S_n . Man zeige $\lim_{n \rightarrow \infty} \frac{a(n)}{n} = \infty$.

Lösungsvorschlag zur Aufgabe (Herbst 2013, T3A3)

- a** Sei $\sigma = \rho\tau$ für zwei disjunkte Zykel ρ bzw. τ . Entscheidende Beobachtung ist, dass disjunkte Zykel miteinander kommutieren. Für jedes $m \in \mathbb{N}$ gilt daher

$$\sigma^m = (\rho\tau)^m = \rho^m\tau^m.$$

Also ist auch

$$\sigma^{\text{kgV}(k,l)} = \rho^{\text{kgV}(k,l)}\tau^{\text{kgV}(k,l)} = \text{id} \cdot \text{id} = \text{id}.$$

Das bedeutet $\text{ord } \sigma \mid \text{kgV}(k,l)$. Umgekehrt folgt aus

$$\text{id} = \sigma^{\text{ord } \sigma} = \rho^{\text{ord } \sigma}\tau^{\text{ord } \sigma},$$

dass bereits $\tau^{\text{ord } \sigma} = \text{id} = \rho^\sigma$, denn obige Gleichung bedeutet $\tau^{-\text{ord } \sigma} = \rho^{\text{ord } \sigma}$ und wären diese Abbildungen nicht die Identität, wäre dies ein Widerspruch dazu, dass τ und ρ disjunkte Zykel sind. Wir haben daher $\text{ord } \sigma = k \mid \text{ord } \sigma$ und $\text{ord } \rho = l \mid \text{ord } \sigma$. Daraus folgt $\text{kgV}(l,k) \mid \text{ord } \sigma$. Insgesamt muss deshalb $\text{kgV}(l,k) = \text{ord } \sigma$ gelten. Da k und l nach Voraussetzung teilerfremd sind, gilt $\text{kgV}(k,l) = kl$.

- b** Sei $n \in \mathbb{N}$ vorgegeben, dann gibt es in S_n disjunkte Zykel der Länge $\lfloor \frac{n-1}{2} \rfloor$ und $\lfloor \frac{n+1}{2} \rfloor$. Da $\lfloor \frac{n-1}{2} \rfloor$ und $\lfloor \frac{n+1}{2} \rfloor$ benachbarte Zahlen sind, sind sie stets teilerfremd und das Produkt von Zyklern dieser Länge hat nach Teil

a die Ordnung

$$\lfloor \frac{n-1}{2} \rfloor \cdot \lfloor \frac{n+1}{2} \rfloor \geq \frac{n-2}{2} \cdot \frac{n}{2} = \frac{n^2 - 2n}{4}.$$

Demnach gilt:

$$\lim_{n \rightarrow \infty} \frac{a(n)}{n} \geq \lim_{n \rightarrow \infty} \frac{n^2 - 2n}{4n} = \lim_{n \rightarrow \infty} \frac{n-2}{4} = \infty.$$

Aufgabe (Herbst 2015, T2A2)

Wieviele Elemente der Ordnung 15 gibt es in der symmetrischen Gruppe S_8 ?

Lösungsvorschlag zur Aufgabe (Herbst 2015, T2A2)

Jedes Element von S_8 hat eine Darstellung als Produkt disjunkter Zykeln. Die Ordnung eines solchen Elements ergibt sich dann als kleinstes gemeinsames Vielfaches der Zyklellängen. Da in S_8 nur Zyklellängen ≤ 8 auftreten können, ist die einzige Möglichkeit ein Produkt aus einem 3- und einem 5-Zykel. Für

die Wahl des 3-Zykels hat man $\binom{8}{3}2!$ Möglichkeiten. Danach ist der Träger des 5-Zykels bereits festgelegt, denn dieser muss aus den verbleibenden 5 Ziffern bestehen. Insgesamt erhält man auf diese Weise

$$\binom{8}{3}2! \cdot \binom{5}{5}4! = 2688$$

Elemente der Ordnung 15 in S_n .

Aufgabe (Herbst 2013, T2A5)

Sei S_5 die Permutationsgruppe von 5 Ziffern. Wie viele Elemente in S_5 haben die Ordnung 4? Wie viele Untergruppen von S_5 haben 4 Elemente?

Lösungsvorschlag zur Aufgabe (Herbst 2013, T2A5)

Jedes Element aus S_5 lässt sich als Produkt disjunkter Zykel schreiben. Die Ordnung des Elements entspricht dann dem kleinsten gemeinsamen Vielfachen der in dieser Zerlegung auftretenden Zykluslängen. Bei einem Element der Ordnung 4 können die auftretenden Zykluslängen daher nur 4 bzw. 4 und 2 sein. Da in S_5 nur 5 Ziffern zur Verfügung stehen, scheidet die zweite Möglichkeit aus. Daher muss jedes Element der Ordnung 4 in S_5 ein 4-Zykel sein. Ihre Anzahl ist

$$\binom{5}{4}(4-1)! = 5 \cdot 3! = 30.$$

Sei nun $U \subseteq S_5$ eine Untergruppe der Ordnung 4. Jede Gruppe von Primzahlordnung ist abelsch, deshalb muss $U \cong \mathbb{Z}/4\mathbb{Z}$ oder $U \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ sein. Im ersten Fall wird U von einem Element der Ordnung 4 erzeugt, jedoch ist dieser Erzeuger nicht eindeutig: U enthält $\varphi(4) = 2 \cdot (2-1) = 2$ Elemente der Ordnung 4. Umgekehrt bedeutet dies, dass je zwei Elemente der Ordnung 4 die gleiche Untergruppe erzeugen. Also gibt es $\frac{30}{2} = 15$ zyklische Untergruppen $U \subseteq S_5$.

Betrachte nun den Fall $U \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Eine solche Untergruppe wird von zwei Elementen der Ordnung 2 erzeugt. Die Elemente der Ordnung 2 in S_5 sind genau die 2-Zykel und die Doppeltranspositionen.

Unterscheide nun die folgenden Fälle:

1. Fall: Die Gruppe U wird von zwei 2-Zykeln σ und τ erzeugt. Hier müssen die 2-Zykel disjunkt sein, denn sonst ist $\sigma\tau$ ein 3-Zykel. Für σ gibt es $\binom{5}{2} = 10$ Wahlmöglichkeiten, für τ gibt es $\binom{3}{2} = 3$ Möglichkeiten. Da $\langle\sigma, \tau\rangle = \langle\tau, \sigma\rangle$, müssen wir das Produkt nach halbieren, d. h. die Anzahl ist $\frac{10 \cdot 3}{2} = 15$.

2. Fall: Die Gruppe U wird von einem 2-Zykel σ und einer Doppeltransposition $\tau\rho$ erzeugt. Sei $\omega \neq \text{id}$ das vierte Element aus U , dann ist auch

$$U = \langle \sigma, \tau\rho \rangle = \langle \sigma, \omega \rangle = \langle \omega, \tau\rho \rangle.$$

Das bedeutet: Ist ω ein 2-Zykel, so sind wir im 1. Fall, ist ω dagegen eine Doppeltransposition, so sind wir im 3. Fall.

3. Fall: Die Gruppe U wird von zwei Doppeltranspositionen $\sigma\tau$ und $\rho\omega$ erzeugt. Hier liegt U in A_5 , und wegen $|A_5| = 60$ sind dies glücklicherweise genau die 2-Sylowgruppen von A_5 .

Wir betrachten zunächst das einfachere Problem, die Untergruppen der Ordnung 4 in $A_4 \subseteq A_5$ zu bestimmen. In S_4 gibt es nur drei Doppeltranspositionen, welche zusammen die Klein'sche Vierergruppe

$$V_4 = \{\text{id}, (12)(34), (13)(24), (14)(23)\}$$

bilden. Diese ist insbesondere die einzige 2-Sylowgruppe von A_4 und somit ein Normalteiler von A_4 . Daraus folgt für den Normalisator von V_4 in A_4 , dass $N_{A_4}(V_4) = A_4$ gilt. Wenn wir nun nach A_5 zurückkehren, normalisiert A_4 natürlich weiterhin V_4 , d. h. $A_4 \subseteq N_{A_5}(V_4)$. Insbesondere wird $|N_{A_5}(V_4)|$ von $12 = |A_4|$ geteilt und ist ein Teiler von $60 = |A_5|$. Wäre $|N_{A_5}(V_4)|$ echt größer als 12, so würden diese beiden Teilbarkeitsbeziehungen bereits $|N_{A_5}(V_4)| = 60$ und damit $N_{A_5}(V_4) = A_5$ erzwingen. In diesem Fall wäre aber V_4 ein nicht-trivialer Normalteiler von A_5 im Widerspruch dazu, dass A_5 einfach ist.

Also ist $|N_{A_5}(V_4)| = 12$ und Lemma 1.17 liefert uns für die Anzahl ν_2 der 2-Sylowgruppen von A_5 , dass

$$\nu_2 = |A_5(V_4)| = (A_5 : N_{A_5}(V_4)) = \frac{|A_5|}{|N_{A_5}(V_4)|} = \frac{60}{12} = 5.$$

Insgesamt gibt es also $15 + 15 + 5 = 35$ Untergruppen der Ordnung 4.

Aufgabe (Herbst 2012, T3A2)

Zeigen Sie, dass für jedes $n \in \mathbb{N}$ der Zentralisator des n -Zyklus $(1\ 2\ 3\ \dots\ n)$ in der symmetrischen Gruppe S_n die zyklische Gruppe $\langle(1\ 2\ 3\ \dots\ n)\rangle$ ist.

Lösungsvorschlag zur Aufgabe (Herbst 2012, T3A2)

Variante 1: Sei $\sigma = (1\ 2\ \dots\ n) \in S_n$. Dann zeigt man per Induktion, dass

$$\sigma^k(l) = l + k \pmod{n}$$

für alle $l, k \in \{1, \dots, n\}$ gilt. Ist nun $\tau \in C_{S_n}(\sigma)$, so gilt $\tau\sigma = \sigma\tau$, d.h.

$$\tau(l+1) = \tau(\sigma(l)) = (\tau\sigma)(l) = (\sigma\tau)(l) = \sigma(\tau(l)) = \tau(l) + 1$$

für alle $l \in \{1, \dots, n\}$ und daraus gewinnt man per Induktion

$$\tau(l) = \tau(1) + (l - 1).$$

An dieser expliziten Darstellung sieht man, dass τ mit der Abbildung $\sigma^{\tau(1)-1}$ übereinstimmt. Dies zeigt $C_{S_n}(\sigma) \subseteq \langle \sigma \rangle$. Die umgekehrte Inklusion ist klar.

Variante 2: Wir lassen S_n auf sich selbst mittels Konjugation operieren. Dann ist gerade $\text{Stab}_{S_n}(\sigma) = C_{S_n}(\sigma)$. Nach Lemma 1.17 gilt

$$(S_n : \text{Stab}_{S_n}(\sigma)) = |S_n(\sigma)| \Leftrightarrow \frac{|S_n|}{|C_{S_n}|} = |S_n(\sigma)|,$$

wobei $S_n(\sigma)$ die Bahn von σ bezeichnet. Außerdem besteht die Konjugationsklasse eines Elements aus S_n nach Lemma 1.36 genau aus den Elementen mit dem gleichen Zerlegungstyp. In unserem Fall sind das die n -Zykel. Davon gibt es

$$\binom{n}{n} (n-1)! = (n-1)!$$

viele, das kombiniert sich mit der Gleichung von oben zu

$$|C_{S_n}(\sigma)| = \frac{|S_n|}{|S_n(\sigma)|} = \frac{n!}{(n-1)!} = n.$$

Wegen $\langle \sigma \rangle \subseteq C_{S_n}(\sigma)$ und $|\langle \sigma \rangle| = \text{ord } \sigma = n$ folgt daher $\langle \sigma \rangle = C_{S_n}(\sigma)$.

Aus Aufgabe H12T3A2 lässt sich folgern, dass das Zentrum der symmetrischen Gruppe S_n für $n \geq 3$ trivial ist. Da das Zentrum der Schnitt über alle Zentralisatoren ist, gilt nämlich insbesondere

$$Z(S_n) \subseteq \langle (1 \ 2 \ 3 \ \dots \ n) \rangle.$$

Ist $\sigma \in Z(S_n)$ mit $\sigma \neq \text{id}$, so gibt es also ein $k \in \{1, \dots, n-1\}$ mit $\sigma = (1 \ 2 \ 3 \ \dots \ n)^k$. Induktiv kann man nun $\sigma^k(1) = k+1$ zeigen, woraus

$$((1 \ 2) \circ \sigma)(1) = (1 \ 2)(k+1) = \begin{cases} 1 & \text{falls } k = 1, \\ k+1 & \text{sonst.} \end{cases}$$

folgt. Wegen

$$(\sigma \circ (1 \ 2))(1) = \sigma(2) = \begin{cases} 1 & \text{falls } k = n-1, \\ k+2 & \text{sonst.} \end{cases}$$

ist dann $\sigma(1 \ 2) \neq (1 \ 2)\sigma$ für $n \geq 3$, sodass $\sigma \notin Z(S_n)$. Dies zeigt, dass $Z(S_n) = \{\text{id}\}$ sein muss.

Aufgabe (Frühjahr 2011, T3A2)

Zeigen Sie: Ist G eine endliche Gruppe, so existiert eine natürliche Zahl n derart, dass G isomorph ist zu einer Untergruppe der alternierenden Gruppe A_n .

Lösungsvorschlag zur Aufgabe (Frühjahr 2011, T3A2)

Sei $|G| = m$, dann liefert der Satz von Cayley eine Einbettung $G \hookrightarrow S_m$. Es genügt daher, eine Einbettung von S_m in eine alternierende Gruppe A_n anzugeben. Betrachte dazu die Abbildung

$$\phi : S_m \rightarrow S_{m+2}, \quad \sigma \mapsto \begin{cases} \sigma \cdot (m+1, m+2) & \text{falls } \operatorname{sgn}(\sigma) = -1, \\ \sigma & \text{falls } \operatorname{sgn}(\sigma) = +1. \end{cases}$$

ϕ bildet nach A_{m+2} ab: Sei dazu $\sigma \in S_m$. Ist $\operatorname{sgn}(\sigma) = -1$, so gilt

$$\operatorname{sgn}(\phi(\sigma)) = \operatorname{sgn}(\sigma) \cdot \operatorname{sgn}((m+1, m+2)) = (-1) \cdot (-1) = 1.$$

Im Fall $\operatorname{sgn}(\sigma) = 1$ ist ohnehin $\operatorname{sgn}(\phi(\sigma)) = \operatorname{sgn}(\sigma) = 1$. In jedem Fall ist also $\phi(\sigma) \in A_{m+2}$.

Als nächstes überprüfen wir, dass es sich bei ϕ um einen Homomorphismus handelt. Seien dazu $\sigma, \tau \in S_m$.

1. Fall: $\operatorname{sgn}(\sigma) = \operatorname{sgn}(\tau) = +1$. In diesem Fall ist $\phi(\sigma\tau) = \sigma\tau = \phi(\sigma)\phi(\tau)$.
2. Fall: $\operatorname{sgn}(\sigma) = \operatorname{sgn}(\tau) = -1$. Die Transposition $(m+1, m+2)$ ist disjunkt zu σ bzw. τ , kommutiert also mit diesen und es ist

$$\begin{aligned} \phi(\sigma)\phi(\tau) &= \sigma(m+1, m+2)\tau(m+1, m+2) = \sigma\tau(m+1, m+2)^2 \\ &= \sigma\tau = \phi(\sigma\tau), \end{aligned}$$

wobei im letzten Schritt verwendet wurde, dass $\operatorname{sgn}(\sigma\tau) = \operatorname{sgn}(\sigma) \cdot \operatorname{sgn}(\tau) = (-1)^2 = 1$ gilt.

3. Fall: σ und τ haben verschiedenes Signum. O. B. d. A. ist hier $\operatorname{sgn}(\sigma) = -1$ und $\operatorname{sgn}(\tau) = 1$. In diesem Fall ist $\operatorname{sgn}(\sigma\tau) = -1$ und es gilt

$$\phi(\sigma\tau) = \sigma\tau(m+1, m+2) = \sigma(m+1, m+2)\tau = \phi(\sigma)\phi(\tau).$$

Zuletzt bestimmen wir noch den Kern von ϕ . Sei $\sigma \in \ker \phi$, dann ist $\phi(\sigma) = \text{id}$ und insbesondere $\phi(\sigma)(m+1) = m+1$, also muss $\phi(\sigma) = \sigma$ sein. Daraus folgt aber bereits $\text{id} = \phi(\sigma) = \sigma$. Setze also $n = m+2$, dann ist ϕ eine Einbettung von S_m in A_n .

Aufgabe (Herbst 2011, T3A1)

Sei $n \geq 5$. Man bestimme alle Normalteiler der symmetrischen Gruppe S_n . Dabei darf (und sollte) ohne Beweis benutzt werden, dass für $n \geq 5$ die alternierende Gruppe A_n einfach ist.

Lösungsvorschlag zur Aufgabe (Herbst 2011, T3A1)

Dass S_n , A_n und $\{\text{id}\}$ Normalteiler von S_n sind, ist hinlänglich bekannt. Nehmen wir nun an, dass es einen echten Normalteiler $N \trianglelefteq S_n$ mit $N \neq \{\text{id}\}$ und $N \neq A_n$ gibt.

Zunächst bemerken wir, dass auch $A_n \cap N$ ein Normalteiler von S_n wäre, da der Schnitt zweier Normalteiler wieder ein Normalteiler ist. Tatsächlich wäre $A_n \cap N$ sogar ein Normalteiler von A_n . Da A_n laut Angabe einfach ist, muss $A_n \cap N = A_n$ oder $A_n \cap N = \{\text{id}\}$ gelten.

Im ersten Fall wäre $A_n \subseteq N$, wegen $A_n \neq N$ sogar $A_n \subsetneq N$. In diesem Fall wäre aber

$$(S_n : N) = \frac{|S_n|}{|N|} < \frac{|S_n|}{|A_n|} = (S_n : A_2) = 2,$$

also $(S_n : N) = 1$ bzw. $S_n = N$. Wir nehmen deshalb im Folgenden $A_n \cap N = \{\text{id}\}$ an.

Sei nun $\sigma \in N$ mit $\sigma \neq \text{id}$. Wir zeigen, dass mindestens noch ein weiteres Element $\neq \text{id}$ in N liegt. Angenommen, es ist $N = \{\text{id}, \sigma\}$. Sei $\tau \in S_n$ mit $\tau \notin N$. Da N ein Normalteiler ist, gilt $\tau\sigma\tau^{-1} \in \{\text{id}, \sigma\}$. Wäre $\tau\sigma\tau^{-1} = \text{id}$, so würde folgen

$$\tau\sigma = \tau \Leftrightarrow \sigma = \text{id}$$

im Widerspruch zu $\sigma \neq \text{id}$. Wäre dagegen $\tau\sigma\tau^{-1} = \sigma$, so wäre

$$\tau\sigma = \sigma\tau.$$

Dies gilt sogar für $\tau \in N$, also wäre $\sigma \in Z(S_n)$. Allerdings gilt für das Zentrum von S_n , dass $Z(S_n) = \{\text{id}\}$ für $n \geq 3$. Also erhalten wir auch in diesem Fall einen Widerspruch.

Es gibt somit mindestens ein weiteres Element $\tau \in N$ mit $\tau \neq \text{id}$ und $\tau \neq \sigma$. Wegen $\sigma, \tau \notin A_n$, muss $\text{sgn}(\sigma) = \text{sgn}(\tau) = -1$ sein. Wegen

$$\text{sgn}(\sigma\tau) = \text{sgn}(\sigma) \cdot \text{sgn}(\tau) = (-1) \cdot (-1) = 1$$

und genauso $\text{sgn}(\sigma^2) = 1$ haben wir aber $\sigma\tau, \sigma^2 \in N \cap A_n = \{\text{id}\}$. Also folgt

$$\sigma\tau = \text{id} = \sigma^2 \Leftrightarrow \tau = \sigma$$

im Widerspruch zu $\sigma \neq \tau$. Insgesamt kann es solch einen Normalteiler mit $N \neq A_n$ und $N \neq \{\text{id}\}$ also nicht geben.

Aufgabe (Frühjahr 2010, T1A1)

Sei G eine endliche einfache Gruppe und H eine echte Untergruppe vom Index $k > 2$ in G . Zeigen Sie, dass die Gruppenordnung $|G|$ von G ein Teiler von $k!/2$ ist.

Lösungsvorschlag zur Aufgabe (Frühjahr 2010, T1A1)

Wir lassen G auf der Menge G/H mittels Translation operieren, d. h. mittels

$$G \times G/H \rightarrow G/H, \quad g \cdot (x + H) = gx + H.$$

Obwohl G/H im Allgemeinen keine Gruppe ist, ist dies trotzdem wie gewohnt eine Gruppenoperation und induziert einen Homomorphismus $\phi: G \rightarrow \text{Per}(G/H) \cong S_k$.

Wäre dieser Homomorphismus trivial, hieße das, dass für alle $g, x \in G$ gelten würde

$$gx + H = H \Leftrightarrow gx \in H.$$

Insbesondere gilt dies für $x = e$ mit dem Neutralelement e von G , also wäre $g \in H$ für alle g und somit $G = H$ im Widerspruch dazu, dass H eine echte Untergruppe von G ist. Es ist daher $\ker \phi \subsetneq G$. Da Kerne von Homomorphismen immer Normalteiler sind und G laut Voraussetzung eine einfache Gruppe ist, muss $\ker \phi = \{e\}$ sein. Dies bedeutet, dass ϕ injektiv ist und $G \cong \text{im } \phi$ gilt.

Tatsächlich muss sogar $\text{im } \phi \subseteq A_k$ gelten, denn $\ker(\text{sgn} \circ \phi)$ ist ebenfalls ein Normalteiler von G und daher muss $\ker(\text{sgn} \circ \phi) = G$ oder $\ker(\text{sgn} \circ \phi) = \{e\}$ sein. Im zweiten Fall wäre $(\text{sgn} \circ \phi): G \rightarrow \{\pm 1\}$ injektiv, was wegen

$$|G| = |H| \cdot (G : H) = |H| \cdot k > 2$$

unmöglich ist. Also ist $\ker(\text{sgn} \circ \phi) = G$, was $\text{im } \phi \subseteq A_k$ bedeutet. Nach dem Satz von Lagrange folgt daraus

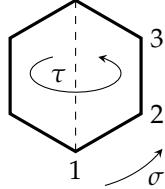
$$|G| = |\text{im } \phi| \quad \text{teilt} \quad |A_k| = \frac{k!}{2}.$$

Die Diedergruppe

Wir wenden uns nun der **Diedergruppe** D_n zu und motivieren zunächst, wieso es sich dabei um die Symmetriegruppe des regelmäßigen n -Ecks handelt.

Sei dazu $G \subseteq \text{Per}(\mathbb{R}^2)$ die Gruppe der Kongruenzabbildungen des n -Ecks. Diese operiert auf der Eckenmenge $E_n = \{1, \dots, n\}$ des n -Ecks, was nach Proposition 1.15 (1) einen Homomorphismus $\phi: G \rightarrow S_n$ liefert. Dieser ist injektiv, denn ist $\sigma \in \ker \phi$, so ist σ eine Kongruenzabbildung, die alle Ecken fest lässt und daher

schon die identische Abbildung. Wir haben folglich eine Einbettung von G in S_n , sodass G zu einer Untergruppe von S_n isomorph ist, die wir mit D_n bezeichnen.



Seien σ speziell die Rotation um $\frac{2\pi}{n}$ und τ die achsensymmetrische Spiegelung des n -Ecks an der Achse durch die Ecke 1. Anschaulich ist klar, dass σ und τ Kongruenzabbildungen des n -Ecks sind, also in D_n liegen, und Ordnung n bzw. 2 haben.

Betrachte nun die Bahn der Ecke 1. Durch k Hintereinanderausführungen der Rotation σ kann diese erste Ecke auf die Ecke k abgebildet werden, d. h. die Bahn der ersten Ecke ist die gesamte Eckemenge E_n . Nur die Spiegelung τ und id lassen die erste Ecke fest, d. h. der Stabilisator dieser Ecke ist $\{\text{id}, \tau\}$. Nach Lemma 1.17 haben wir nun

$$|D_n(1)| = (D_n : \text{Stab}_{D_n}(1)) \Leftrightarrow n = \frac{|D_n|}{2} \Leftrightarrow |D_n| = 2n.$$

Da τ die Ecke 1 festlässt, während jede Rotation τ^k sie weiterdreht, muss weiter $\langle \sigma \rangle \cap \langle \tau \rangle = \{\text{id}\}$ sein, sodass $\langle \sigma, \tau \rangle$ ebenfalls eine Gruppe der Ordnung $2n$ ist. Zusammen gibt das $D_n = \langle \sigma, \tau \rangle$. Zusammenfassend lässt sich zeigen:

Satz 1.37. Sei $n \geq 2$ eine natürliche Zahl. Dann gibt es bis auf Isomorphie genau eine Gruppe G mit den folgenden Eigenschaften:

- (1) $|G| = 2n$,
- (2) es gibt Elemente $\sigma, \tau \in G$ mit $\text{ord}(\sigma) = n$ und $\text{ord}(\tau) = 2$, für die $\sigma\tau = \tau\sigma^{n-1}$ gilt,
- (3) $G = \langle \sigma, \tau \rangle$.

Diese Gruppe wird n -te **Diedergruppe** genannt und mit D_n bezeichnet.

Im Fall $n = 2$ spricht man anstatt von D_2 in aller Regel von der **Klein'schen Vierergruppe** V_4 . Diese ist als Gruppe der Ordnung $4 = 2^2$ abelsch und da sie von zwei Elementen der Ordnung 2 erzeugt wird, ist $V_4 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Aufgabe (Herbst 2001, T2A1)

Für $3 \leq n$ sei D_n die Diedergruppe der Ordnung $2n$, es sei H die Quaternionengruppe der Ordnung 8, und S_3 sei die symmetrische Gruppe auf 3 Elementen.

- a** Zeigen Sie: Die drei Gruppen $D_8, D_4 \times \mathbb{Z}_2$ und $H \times \mathbb{Z}_2$ sind paarweise nicht isomorph.
- b** Bestimmen Sie für jede der drei Gruppen aus **a** die Anzahl der zyklischen Untergruppen der Ordnung 4 und geben Sie jeweils die Menge dieser Untergruppen an.
- c** Zeigen Sie: Die Gruppen D_6 und $S_3 \times \mathbb{Z}_2$ sind isomorph.

Lösungsvorschlag zur Aufgabe (Herbst 2001, T2A1)

- a** Nach Definition gibt es in D_8 ein Element der Ordnung 8, D_4 und H haben jedoch nur Elemente der Ordnung höchstens 4, sodass Elemente aus $D_4 \times \mathbb{Z}_2$ bzw. $H \times \mathbb{Z}_2$ ebenfalls höchstens Ordnung 4 haben können. Diese beiden Gruppen können daher nicht zu D_8 isomorph sein.

Weiterhin hat H genau ein Element der Ordnung 2, nämlich -1 , sodass es in $H \times \mathbb{Z}_2$ genau die drei Elemente $(-1, \bar{0}), (-1, \bar{1})$ und $(1, \bar{1})$ der Ordnung 2 gibt. Sind σ, τ die Erzeuger von D_4 , so gibt es in D_4 hingegen die 5 Elemente $\tau, \tau\sigma, \tau\sigma^2, \tau\sigma^3, \sigma^2$ der Ordnung 2, sodass es in $D_4 \times \mathbb{Z}_2$ mindestens die 5 Elemente

$$(\tau, \bar{0}), (\tau\sigma, \bar{0}), (\tau\sigma^2, \bar{0}), (\tau\sigma^3, \bar{0}), (\sigma^2, \bar{0})$$

der Ordnung 2 gibt. Also können auch $D_4 \times \mathbb{Z}_2$ und $H \times \mathbb{Z}_2$ nicht isomorph zueinander sein.

- b** Ist $D_8 = \langle \sigma, \tau \rangle$ mit $\text{ord}(\sigma) = 8$, so sind die einzigen Elemente der Ordnung 4 in D_8 genau σ^2 und σ^6 , welche beide die zyklische Gruppe $\langle \sigma^2 \rangle \subseteq D_8$ erzeugen.

In $H = \langle i, j, k \rangle$ gibt es als Elemente der Ordnung 4 gerade $\pm i, \pm j, \pm k$, die Untergruppen der Ordnung 4 in $H \times \mathbb{Z}_2$ sind daher

$$\langle (i, \bar{0}) \rangle, \langle (j, \bar{0}) \rangle, \langle (k, \bar{0}) \rangle \text{ sowie } \langle (i, \bar{1}) \rangle, \langle (j, \bar{1}) \rangle, \langle (k, \bar{1}) \rangle.$$

Schließlich gibt es in $D_4 = \langle \sigma, \tau \rangle$ als Untergruppe der Ordnung 4 nur $\langle \sigma \rangle$ und in $D_4 \times \mathbb{Z}_2$ sind die zyklischen Untergruppen der Ordnung 4 dann gegeben durch

$$\langle (\sigma, \bar{0}) \rangle, \langle (\sigma, \bar{1}) \rangle.$$

- c** Wir überprüfen die Kriterien aus Satz 1.37: (1) $|S_3 \times \mathbb{Z}_2| = 12 = |D_6|$.
(2) Seien $a = (123)$ und $b = (12)$, dann haben diese Elemente Ordnung 3 bzw. 2 und es gilt

$$(ab)^2 = [(123) \circ (12)]^2 = [(13)]^2 = \text{id} \Leftrightarrow ab = b^{-1}a^{-1} = ba^2$$

Folglich haben die Elemente $\sigma = (a, \bar{1})$ und $\tau = (b, \bar{0})$ die Ordnungen 6 bzw. 2 und es ist

$$\sigma\tau = (ab, \bar{1} + \bar{0}) = (ba^2, \bar{1}) = \tau(a^2, \bar{1}) = \tau(a^3 \cdot a^2, \bar{1}) = \tau\sigma^5$$

wie gewünscht.

- (3) Es ist $\tau \notin \langle \sigma \rangle$, da diese Untergruppe nur Elemente enthält, die in der ersten Komponente ein Element aus $\langle (123) \rangle$ stehen haben, also id oder

einen 3-Zykel. Somit hat $\langle \sigma, \tau \rangle$ mindestens 7 Elemente (nämlich $\langle \sigma \rangle$ und τ). Da als Untergruppenordnungen jedoch nur Teiler der Gruppenordnung 12 in Frage kommen, muss $\langle \sigma, \tau \rangle$ sogar 12 Elemente enthalten und es folgt somit $\langle \sigma, \tau \rangle = S_3 \times \mathbb{Z}_2$.

Aufgabe (Frühjahr 2012, T1A2)

Zeigen Sie, dass in der symmetrischen Gruppe S_5 alle Untergruppen der Ordnung 8 zur Diedergruppe D_4 (der Symmetriegruppe eines Quadrates) isomorph sind.

Lösungsvorschlag zur Aufgabe (Frühjahr 2012, T1A2)

Die Untergruppen der Ordnung 8 sind genau die 2-Sylowgruppen von S_5 . Diese sind zueinander konjugiert und deshalb isomorph zueinander. Weil S_5 die D_4 als Untergruppe enthält, müssen also alle 2-Sylowgruppen von S_5 zu D_4 isomorph sein.

Aufgabe (Frühjahr 2010, T1A5)

Sei D_6 die Diedergruppe der Ordnung 12, sei A_4 die alternierende Gruppe und sei G die von a und b erzeugte Gruppe, wobei a die Ordnung 3 und b die Ordnung 4 hat und $bab^{-1} = a^2$ gilt. Zeigen Sie, dass diese 3 Gruppen paarweise nicht isomorph sind.

Lösungsvorschlag zur Aufgabe (Frühjahr 2010, T1A5)

(1) $A_4 \not\cong G$: Die alternierende Gruppe enthält die Klein'sche Vierergruppe V_4 als Normalteiler und deshalb einzige 2-Sylowgruppe. Die Gruppe G besitzt die Gruppe $\langle b \rangle \cong \mathbb{Z}/4\mathbb{Z}$ als 2-Sylowgruppe. Nach den Sylowsätzen sind alle Sylowgruppen konjugiert zueinander, als auch isomorph. Wären A_4 und V_4 isomorph, müssten deshalb sämtliche 2-Sylowgruppen isomorph sein. Wegen

$$V_4 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \not\cong \mathbb{Z}/4\mathbb{Z} \cong \langle b \rangle$$

ist dies jedoch nicht der Fall.

(2) $G \not\cong D_6$: Die Gruppe D_6 wird von zwei Elementen $\sigma, \tau \in D_6$ erzeugt, wobei $\text{ord } \sigma = 6$, $\text{ord } \tau = 2$ und $\tau\sigma = \sigma^{-1}\tau$ ist. Es ist dann

$$\begin{aligned} (\sigma^3\tau)^2 &= \sigma^3\tau\sigma^3\tau = \sigma^3 \cdot \sigma^{-1}\tau \cdot \sigma^2\tau = \\ &= \sigma^2 \cdot \sigma^{-1}\tau \cdot \sigma\tau = \sigma \cdot \sigma^{-1}\tau\tau = \text{id} \cdot \text{id} = \text{id} \end{aligned}$$

und es gilt $\sigma^3\tau \neq \text{id}$, da andernfalls $\sigma^3 = \tau^{-1}$ wäre und somit $D_6 = \langle \sigma, \tau \rangle = \langle \sigma \rangle$ nur 6 Elemente hätte. Außerdem ist $\sigma^3\tau \neq \tau$, da auch $\sigma^3 \neq \text{id}$ wegen $\text{ord } \sigma = 6$. Wir haben damit gezeigt, dass $\langle \tau \rangle \cap \langle \sigma^3\tau \rangle = \{\text{id}\}$, sodass

$$\langle \tau, \sigma^3\tau \rangle \cong \langle \tau \rangle \times \langle \sigma^3\tau \rangle \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \cong V_4$$

als inneres direktes Produkt. Insbesondere ist $\langle \tau, \sigma^3\tau \rangle$ eine Gruppe der Ordnung 4, also 2-Sylowgruppe. Da diese nicht zyklisch ist, die 2-Sylowgruppen von G jedoch schon, kann D_6 nicht zu G isomorph sein.

(3) $A_4 \not\cong D_6$: Wie bereits erwähnt besitzt A_4 nur eine 2-Sylowgruppe. Wir zeigen nun, dass D_6 mehr als eine 2-Sylowgruppe besitzt, sodass A_4 und D_6 ebenfalls nicht isomorph sein können.

Jedes Element der Form $\sigma^n\tau$ mit $n \in \{1, \dots, 5\}$ hat Ordnung 2, denn es gilt

$$(\sigma^n\tau)^2 = \sigma^n\tau\sigma^n\tau = \dots = \sigma^n\sigma^{-n}\tau\tau = \text{id}$$

und $\sigma^n\tau \neq \text{id}$, da sonst $\tau = \sigma^n \in \langle \sigma \rangle$ wäre und das wie oben ausgeführt nicht sein kann. Also besitzt D_6 mindestens 5 Elemente der Ordnung 2, die unmöglich in nur einer 2-Sylowgruppe liegen können. Nach den Sylowsätzen liegt jedoch jedes Element der Ordnung 2 in einer 2-Sylowgruppe.

2. Algebra: Ringtheorie

2.1. Ringe und Ideale

Beschäftigt man sich mit den ganzen Zahlen \mathbb{Z} , so erscheint es unzufriedenstellend, diese nur isoliert als die Gruppe $(\mathbb{Z}, +)$ oder das Monoid (\mathbb{Z}, \cdot) zu betrachten. Stattdessen ist es natürlicher, die ganzen Zahlen als eine Menge mit *zwei* inneren Verknüpfungen $+$ und \cdot aufzufassen. Die ganzen Zahlen werden so zum Prototypen einer neuen Kategorie, zu der als zweiter bedeutender Vertreter der Polynomring $K[X]$ über einem Körper K gehört.

Definition 2.1. Ein *Ring* ist eine Menge R mit zwei Verknüpfungen

$$+: R \times R \rightarrow R, \quad \text{und} \quad \cdot: R \times R \rightarrow R,$$

sodass

- (1) $(R, +)$ eine kommutative Gruppe ist,
- (2) (R, \cdot) ein kommutatives Monoid ist,
- (3) das Distributivgesetz gilt, d. h. für alle $r, s, t \in R$ die Gleichung

$$(r + s)t = tr + st$$

erfüllt ist. Das Neutralelement von $(R, +)$ bezeichnen wir mit 0, das von (R, \cdot) mit 1.

Ist R ein Ring, so ist ein *Teilring* oder *Unterring* von R eine Teilmenge $S \subseteq R$ mit

- (1) $1 \in S$,
- (2) $a - b \in S$,
- (3) $ab \in S$

für beliebige $a, b \in S$.

Obwohl wir von den ganzen Zahlen ausgegangen sind, ist die Definition eines Rings genügend allgemein, sodass Ringe nicht immer alle Eigenschaften haben, die für uns im Umgang mit den ganzen Zahlen selbstverständlich sind. Die nächste Definition benennt einige dieser Merkmale deshalb.

Definition 2.2. Sei R ein Ring.

- (1) Ein Element $r \in R$ heißt *Einheit*, falls es ein $s \in R$ gibt, sodass $rs = 1$ ist.
Die Menge aller Einheiten von R notiert man als R^\times und nennt sie die *Einheitengruppe* von R .
- (2) Ein Element $r \in R$ heißt *Nullteiler*, falls es ein $s \in R \setminus \{0\}$ gibt, sodass $rs = 0$ ist und *nilpotent*, falls es ein $n \in \mathbb{N}$ mit $r^n = 0$ gibt.

(3) Ist 0 der einzige Nullteiler in R , so heißt R **Integritätsbereich** oder **Integritätsring**. Eine äquivalente Charakterisierung dafür ist, dass für Elemente $r, s \in R$ aus der Gleichung $rs = 0$ bereits $r = 0$ oder $s = 0$ folgt.

Definition 2.3. Ein Ring R heißt **Körper**, falls $R^\times = R \setminus \{0\}$.

Aufgabe (Frühjahr 2015, T3A3)

Ein Ring R mit Eins heißt *idempotent*, wenn $a \cdot a = a$ für alle $a \in R$ gilt. Beweisen Sie:

- a** $-1 = 1$ in einem idempotenten Ring R .
- b** Jeder idempotente Ring ist kommutativ.
- c** Jeder idempotente Integritätsbereich ist isomorph zu \mathbb{F}_2 , dem Körper mit zwei Elementen.

Lösungsvorschlag zur Aufgabe (Frühjahr 2015, T3A3)

- a** Da auch -1 idempotent ist, haben wir

$$-1 = (-1) \cdot (-1) = 1.$$

- b** Seien $a, b \in R$. Man berechnet:

$$\begin{aligned} a + b &= (a + b)^2 = a^2 + ab + ba + b^2 = a + ab + ba + b \\ \Leftrightarrow 0 &= ab + ba \quad \Leftrightarrow ab = -ba \end{aligned}$$

Da $-1 = 1$ nach Teil **a**, folgt daraus $ab = ba$.

- c** Sei $a \in R$ mit $a \neq 0$. Da R ein Integritätsbereich ist, folgt aus

$$a^2 = a \quad \Leftrightarrow \quad a(a - 1) = 0,$$

dass $a = 1$. Also ist $R = \{0, 1\}$. Insbesondere ist R ein Körper und als Körper mit zwei Elementen isomorph zu \mathbb{F}_2 nach Satz 3.25.

Anleitung: Endliche Integritätsbereiche

Ist R ein endlicher Integritätsbereich, so ist R bereits ein Körper. Zum Nachweis dieser Aussage, der gerne explizit oder implizit in Staatsexamensaufgaben abgefragt wird, gibt es zwei Standardargumente:

(1) Sei $a \in R$ ein Element mit $a \neq 0$. Betrachte die Abbildung

$$\tau_a: R \rightarrow R, \quad r \mapsto ar,$$

welche injektiv aufgrund der Integritätsbereichsbedingung ist. Da τ_a eine Abbildung zwischen endlichen und gleichmächtigen Mengen ist, muss sie bereits bijektiv sein. Insbesondere hat 1 ein Urbild $b \in R$, d.h. $1 = \tau_a(b) = ab$ und a ist invertierbar.

(2) Sei $a \in R$ ein Element mit $a \neq 0$. Da R endlich ist, können die Potenzen von a nicht alle verschieden sein, sodass es $n, m \in \mathbb{N}$ mit $n < m$ und $a^n = a^m$ geben muss. Aus dieser Gleichung folgt

$$a^n(1 - a^{m-n}) = 0.$$

Da R ein Integritätsbereich ist, muss $1 - a^{m-n} = 0$ oder $a^n = 0$ sein. Im ersten Fall ist a eine Einheit, im zweiten Fall zeigt man mittels Induktion, dass $a = 0$ sein muss.

Aufgabe (Frühjahr 2013, T3A3)

Beweisen Sie, dass jeder endliche Integritätsbereich ein Körper ist.

Hinweis Man betrachte eine durch Multiplikation gegebene Abbildung.

Lösungsvorschlag zur Aufgabe (Frühjahr 2013, T3A3)

Zu zeigen ist, dass jedes Element $a \in R$ mit $a \neq 0$ eine Einheit ist. Definiere dazu die Abbildung

$$\varphi_a: R \rightarrow R, \quad r \mapsto ra.$$

Diese Abbildung ist injektiv, denn sind $r, s \in R$ Elemente mit $\varphi_a(r) = \varphi_a(s)$, so bedeutet dies

$$ra = sa \quad \Leftrightarrow \quad ra - sa = 0 \quad \Leftrightarrow \quad (r - s)a = 0.$$

Da R nach Voraussetzung ein Integritätsbereich ist, folgt daraus, dass $r - s = 0$ oder $a = 0$ ist. Wir hatten $a \neq 0$ gewählt, sodass $r - s = 0$ sein muss, was äquivalent zu $r = s$ ist. Also ist φ_a eine injektive Abbildung zwischen zwei gleichmächtigen (endlichen) Mengen und daher auch surjektiv. Insbesondere gibt es ein $b \in R$ mit

$$\varphi_a(b) = 1 \quad \Leftrightarrow \quad ab = 1.$$

Aufgabe (Frühjahr 2010, T3A2)

R sei ein endlicher kommutativer Ring mit Einselement. Zeigen Sie, dass jedes Element aus R entweder Einheit oder Nullteiler ist.

Lösungsvorschlag zur Aufgabe (Frühjahr 2010, T3A2)

Sei $r \in R$ beliebig vorgegeben. Da R endlich ist, können die Potenzen r, r^2, \dots nicht alle verschieden sein, d. h. es muss verschiedene $m, n \in \mathbb{N}$ geben mit $r^m = r^n$. O. B. d. A. sei $m < n$, dann gilt:

$$r^m = r^n \Leftrightarrow r^m - r^n = 0 \Leftrightarrow r^m(1 - r^{n-m}) = 0.$$

Da R nicht unbedingt ein Integritätsbereich ist, können wir nicht folgern, dass einer der Faktoren 0 ist. Wir unterscheiden stattdessen zwei Fälle:

1. Fall: $1 - r^{n-m} = 0$: Es folgt $r \cdot r^{n-m-1} = r^{n-m} = 1$ und r ist eine Einheit.
2. Fall: $1 - r^{n-m} \neq 0$: Hier ist r^m ein Nullteiler. Wir zeigen nun per Induktion über m , dass daraus folgt, dass auch r ein Nullteiler ist.

Der Fall $m = 1$ ist klar. Nehmen wir an, die Aussage gilt für $m \in \mathbb{N}$ und betrachten den Fall $m + 1$. Ist r^{m+1} ein Nullteiler, dann gibt es ein $s \neq 0$ mit

$$r^{m+1} \cdot s = 0 \Leftrightarrow r \cdot r^m \cdot s = 0.$$

Ist nun auch $r^m \cdot s \neq 0$, so ist r ein Nullteiler und die Behauptung stimmt. Ansonsten folgt aus $r^m \cdot s = 0$ und $s \neq 0$, dass r^m ein Nullteiler ist – laut der Induktionvoraussetzung folgt daraus, dass r ein Nullteiler ist.

Ideale

Um das von den ganzen Zahlen gewohnte Konzept der eindeutigen Primfaktorzerlegung in allgemeinere Ringe hinüber zu retten, ist die erste Idee, die besonderen Eigenschaften von Primzahlen zu abstrahieren und anschließend nach abstrakteren Elementen mit diesen Eigenschaften zu suchen.

Definition 2.4. Sei R ein Integritätsbereich und $p \in R$ mit $p \neq 0$ und $p \notin R^\times$:

- (1) p heißt **Primelement**, falls für $x, y \in R$ die Implikation

$$p \mid xy \Rightarrow p \mid x \text{ oder } p \mid y$$

erfüllt ist.

- (2) p heißt **irreduzibles Element**, falls für $x, y \in R$ die Implikation

$$p = xy \Rightarrow x \in R^\times \text{ oder } y \in R^\times$$

erfüllt ist.



Abbildung 2.1: Veranschaulichung des Unterschieds zwischen einem Ideal $\mathfrak{a} \subseteq R$ (links) und einem Unterring $S \subseteq R$ (rechts). Im Unterschied zum Unterring wird beim Ideal gefordert, dass auch die Verknüpfung mit einem Ringelement *auf der Seite* des Ideals wieder im Ideal liegen soll.

Im Fall der ganzen Zahlen \mathbb{Z} fallen die obigen Eigenschaften zusammen und beschreiben gerade die Primzahlen (vgl. dazu auch Proposition 2.10). In Ringen der Form $\mathbb{Z}[\sqrt{d}]$ für ein $d \in \mathbb{Z}$ ist das jedoch nicht immer der Fall, wie wir sehen werden.

Viele Ringe gestatten nun dennoch keine eindeutige Zerlegung in diese verallgemeinerten „Primzahlen“, beispielsweise haben wir über dem Ring $\mathbb{Z}[\sqrt{-5}]$ die beiden Zerlegungen

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{5})$$

von 6 in irreduzible Elemente. Um diesen Makel zu beheben, entwickelte Eduard Kummer eine Theorie *ideal er Zahlen*, welche Richard Dedekind zum Begriff des *Ideals* inspirierte. Tatsächlich gilt im Ring $\mathbb{Z}[\sqrt{-5}]$ keine eindeutige Primzahl- oder Primelementzerlegung, sondern eine eindeutige Primidealzerlegung.

Definition 2.5. Sei R ein Ring. Eine Menge $\mathfrak{a} \subseteq R$ wird **Ideal** genannt, falls

- (1) $0 \in \mathfrak{a}$,
- (2) $ar \in \mathfrak{a}$,
- (3) $a + b \in \mathfrak{a}$

für alle $a, b \in \mathfrak{a}$ und $r \in R$ erfüllt ist.

Eine Klasse besonders schöner Ideale sind die **Hauptideale**, welche gerade die Menge aller Vielfachen eines Elementes sind, d.h. die Menge $\{ar \mid r \in R\}$ für ein $a \in R$. In aller Regel wird diese Menge als (a) oder aR notiert. Das von mehreren Elementen a_1, \dots, a_n erzeugte Ideal ist dann entsprechend

$$(a_1, \dots, a_n) = a_1R + \dots + a_nR.$$

Neben den besonders schönen Idealen gibt es noch die besonders wichtigen Ideale:

Definition 2.6. Sei R ein Ring.

- (1) Ein Ideal $\mathfrak{p} \subsetneq R$ heißt **Primideal**, falls für $x, y \in R$ die Implikation

$$xy \in \mathfrak{p} \Rightarrow x \in \mathfrak{p} \text{ oder } y \in \mathfrak{p}$$

erfüllt ist.

- (2) Ein Ideal $\mathfrak{m} \subsetneq R$ heißt **maximales Ideal**, falls für jedes Ideal $\mathfrak{a} \subseteq R$ die Implikation

$$\mathfrak{m} \subseteq \mathfrak{a} \subseteq R \Rightarrow \mathfrak{a} = \mathfrak{m} \text{ oder } \mathfrak{a} = R$$

erfüllt ist.

Ideale ermöglichen auch die Konstruktion der Restklassenringe, auf die wir im nächsten Abschnitt ausführlicher eingehen werden. Wir kommen jedoch nicht umhin, die dort entwickelte Theorie bereits teilweise vorweg zu nehmen.

Satz 2.7. Sei R ein Ring.

- (1) Ein Ideal $\mathfrak{p} \subseteq R$ ist genau dann prim, wenn R/\mathfrak{p} ein Integritätsbereich ist.
- (2) Ein Ideal $\mathfrak{m} \subseteq R$ ist genau dann maximal, wenn R/\mathfrak{m} ein Körper ist.

Unmittelbare Folgerung aus Satz 2.7 ist, dass jedes maximale Ideal auch prim ist, denn jeder Körper ist insbesondere ein Integritätsbereich.

Aufgabe (Herbst 2014, T1A2)

Es sei R ein kommutativer Ring mit Eins, der nicht der Nullring ist. Sei \mathfrak{p} ein Primideal von R . Betrachten Sie die Teilmenge

$$\mathfrak{p}R[X] := \left\{ \sum_{i=1}^r a_i f_i(X) \mid r \in \mathbb{N}, a_i \in \mathfrak{p} \text{ und } f_i(X) \in R[X] \right\}$$

im Polynomring $R[X]$.

- a** Zeigen Sie, dass $\mathfrak{p}R[X]$ ein Ideal von $R[X]$ ist.
- b** Geben Sie einen Isomorphismus $R[X]/\mathfrak{p}R[X] \rightarrow (R/\mathfrak{p})[X]$ an (mit Beweis).
- c** Zeigen Sie, dass $\mathfrak{p}R[X]$ ein Primideal, aber kein maximales Ideal von $R[X]$ ist.

Lösungsvorschlag zur Aufgabe (Herbst 2014, T1A2)

- a** Wegen $0 \in \mathfrak{p}$ ist auch $0 \in \mathfrak{p}R[X]$. Sei nun $\sum_{i=1}^r a_i f_i \in \mathfrak{p}R[X]$ und $g \in R[X]$. Dann ist auch

$$g \cdot \sum_{i=1}^r a_i f_i = \sum_{i=1}^r a_i \cdot g \cdot f_i = \sum_{i=1}^r a_i \tilde{f}_i \in \mathfrak{p}R[X],$$

wobei $\tilde{f}_i = g f_i$ für jedes $i \in \{1, \dots, r\}$ ist. Ist nun zusätzlich $\sum_{i=1}^s b_i g_i \in \mathfrak{p}R[X]$, so ist

$$\sum_{i=1}^r a_i f_i + \sum_{i=1}^s b_i g_i = \sum_{i=1}^{r+s} c_i h_i \in \mathfrak{p}R[X],$$

mit

$$c_i = \begin{cases} a_i & \text{für } 1 \leq i \leq r, \\ b_{i-r} & \text{für } r+1 \leq i \leq r+s, \end{cases} \quad h_i = \begin{cases} f_i & \text{für } 1 \leq i \leq r, \\ g_{i-r} & \text{für } r+1 \leq i \leq r+s. \end{cases}$$

- b** Es bezeichne \bar{a} jeweils die Restklasse von $a \in R$ in R/\mathfrak{p} . Wir definieren die Abbildung

$$\varphi: R[X] \rightarrow (R/\mathfrak{p})[X], \quad \sum_{i=0}^n a_i X^i \mapsto \sum_{i=0}^n \bar{a}_i X^i,$$

welche ein Homomorphismus ist. Außerdem ist diese surjektiv, da $R \rightarrow R/\mathfrak{p}$, $r \mapsto \bar{r}$ surjektiv ist. Nach dem Homomorphiesatz 2.11 genügt es daher zu zeigen, dass $\ker \varphi = \mathfrak{p}R[X]$ erfüllt ist, denn dann ist die induzierte Abbildung

$$\bar{\varphi}: R[X]/\mathfrak{p}R[X] \rightarrow (R/\mathfrak{p})[X], \quad p + \mathfrak{p}R[X] \mapsto \varphi(p)$$

ein Isomorphismus. Die Inklusion $\mathfrak{p}R[X] \subseteq \ker \varphi$ ist klar, da für jedes $a \in \mathfrak{p}$ die zugehörige Restklasse $\bar{a} = 0$ ist. Sei daher umgekehrt $p \in R[X]$ mit $\varphi(p) = \bar{0}$ vorgegeben. Schreibe $p = \sum_{i=0}^n a_i X^i$ mit Koeffizienten $a_i \in R$ für alle $i \in \{0, \dots, n\}$, dann haben wir

$$\varphi(p) = \sum_{i=0}^n \bar{a}_i X^i = \bar{0}.$$

Koeffizientenvergleich ergibt $\bar{a}_i = \bar{0}$ für alle $i \in \{0, \dots, n\}$, was gleichbedeutend zu $a_i \in \mathfrak{p}$ für alle $i \in \{0, \dots, n\}$ ist. Dies zeigt $p = \sum_{i=0}^n a_i X^i \in \mathfrak{p}R[X]$.

c Da \mathfrak{p} ein Primideal ist, ist R/\mathfrak{p} laut Satz 2.7 ein Integritätsbereich und als Polynomring über einem Integritätsbereich ist auch $(R/\mathfrak{p})[X]$ wieder ein Integritätsbereich. Nach Teil **b** gilt $R[X]/\mathfrak{p}R[X] \cong (R/\mathfrak{p})[X]$, also ist $R[X]/\mathfrak{p}R[X]$ ebenfalls ein Integritätsbereich, sodass $\mathfrak{p}R[X]$ ein Primideal von $R[X]$ ist.

Andererseits ist $(R/\mathfrak{p})[X]$ kein Körper, da dort beispielsweise das Polynom X aus Gründen nicht invertierbar ist. Folglich ist $R[X]/\mathfrak{p}R[X]$ ebenfalls kein Körper und das Ideal $\mathfrak{p}R[X]$ nicht maximal.

Einheiten

Wie man leicht überprüft, bilden die invertierbaren Element eines Ringes R eine Gruppe, die sogenannte *Einheitengruppe* R^\times . Ist S ein weiterer Ring, so hat man $(R \times S)^\times = R^\times \times S^\times$. Um die Einheitengruppen der Ringe $\mathbb{Z}/n\mathbb{Z}$ vollständig zu klassifizieren, ist es daher nach dem Chinesischen Restsatz 2.13 ausreichend, die Einheitengruppen der Ringe $\mathbb{Z}/p^n\mathbb{Z}$ für eine Primzahl p und $n \in \mathbb{N}$ zu bestimmen. Diese Leistung erbringt der nächste Satz.

Satz 2.8. Sei $n \in \mathbb{N}$ und p eine Primzahl.

- (1) $(\mathbb{Z}/n\mathbb{Z})^\times$ ist eine Gruppe der Ordnung $\varphi(n)$.
- (2) Ist p ungerade, so gilt $(\mathbb{Z}/p^n\mathbb{Z})^\times \cong \mathbb{Z}/(p^{n-1}(p-1))\mathbb{Z}$.
- (3) Für $n \geq 2$ ist $(\mathbb{Z}/2^n\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-2}\mathbb{Z}$.

Zur expliziten Berechnung von multiplikativen Inversen in Restklassenringen beachte auch den Kasten auf Seite 103. Nebenergebnis des dort beschriebenen Verfahrens ist die folgende Charakterisierung:

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{\bar{a} \in \mathbb{Z}/n\mathbb{Z} \mid \text{ggT}(a, n) = 1\}.$$

Eine weitere und besonders für die Zahlentheorie wichtige Klasse von Ringen sind die Ringe der Form $\mathbb{Z}[\sqrt{d}]$ für eine quadratfreie Zahl $d \in \mathbb{Z}$. Zur Untersuchung der Einheitengruppe dieser Ringe benutzt man die sog. *Normabbildung*

$$N: \mathbb{Z}[\sqrt{d}] \rightarrow \mathbb{Z}, \quad a + b\sqrt{d} \mapsto a^2 - db^2.$$

Diese hat die nützliche Eigenschaft, multiplikativ zu sein und Einheiten auf Einheiten abzubilden. Neben den Einheiten ist die Normabbildung auch zur Untersuchung von Primelementen und irreduziblen Elementen hilfreich.

Gebrauchsanweisung zur Norm

Gegeben sei ein Ring $\mathbb{Z}[\sqrt{d}]$, wobei $d \in \mathbb{Z}$ eine quadratfreie Zahl ist.

- (1) Definiere die Normabbildung $N: \mathbb{Z}[\sqrt{d}] \rightarrow \mathbb{Z}$. In unserem Fall ist diese durch $N(a + b\sqrt{d}) = a^2 - db^2$ gegeben. Falls $d < 0$, hat diese auch die Darstellung $N(z) = z\bar{z}$, woran man besonders leicht die Multiplikativität sieht.
- (2) Die Normabbildung hat die nützliche Eigenschaft, dass z genau dann eine Einheit in $\mathbb{Z}[\sqrt{d}]$ ist, wenn $N(z)$ eine Einheit in \mathbb{Z} , also ± 1 , ist (vgl. H10T1A3 **a** oder F10T2A3 **a**).
- (3) Nach (2) sind die Einheiten $z = a + b\omega$ von $\mathbb{Z}[\sqrt{d}]$ genau die Lösungen der Gleichung $N(z) = \pm 1$. Um diese sogenannte *Pell-Fermat-Gleichung*

$$a^2 - b^2d = n.$$

zu behandeln, verwendet man meist eine der folgenden beiden Strategien:

- (a) Im Fall, dass $d < 0$ ist, muss die rechte Seite positiv sein. Wir kehren zurück zum Spezialfall $n = 1$:
Triff die Annahme $b \neq 0$, sodass $b^2 \geq 1$ ist. Dies führt auf die Ungleichung $1 = a^2 - b^2d \geq a^2 - d$. Falls $d \leq -2$, ist dies bereits ein Widerspruch, sodass $b = 0$ sein muss. Für $d = -1$ hat man zusätzlich die Möglichkeiten $b \in \{\pm 1\}$. Nun muss man nur noch den Fall $b = 0$ betrachten.
- (b) Reduziere die Gleichung modulo einer geeigneten Primzahl und verwende die Strategie aus dem Kasten auf Seite 126, um die Existenz von Lösungen auszuschließen.
- (4) Auch im Zusammenhang mit irreduziblen Elementen ist die Norm nützlich, denn ist $z = xy$, so ist $N(z) = N(x)N(y)$. Falls $N(z)$ eine Primzahl ist, folgt daher aus (2) sofort, dass z irreduzibel ist. In allen anderen Fällen macht man die Annahme, dass x und y keine Einheiten sind, also $N(x) \neq \pm 1 \neq N(y)$ gilt, und überprüft wie in (3), ob für die verbleibenden Möglichkeiten die Pell-Fermat-Gleichung lösbar ist.
- (5) In euklidischen Ringen ist jedes irreduzible Elemente auch prim (vgl. Proposition 2.10), daher kann dort die Strategie aus (4) für den Nachweis der Primelementeigenschaft verwendet werden. Umgekehrt zeigt man, dass ein Ring nicht faktoriell ist, indem man ein Element findet, das nach (4) irreduzibel, aber dennoch nicht prim ist.

Aufgabe (Frühjahr 2012, T2A3)

Bestimmen Sie alle Teiler von 6 im Ring $\mathbb{Z}[\sqrt{-6}] = \{a + \sqrt{-6} \cdot b \mid a, b \in \mathbb{Z}\}$.

Lösungsvorschlag zur Aufgabe (Frühjahr 2012, T2A3)

Sei $\alpha = a + b\sqrt{-6} \in \mathbb{Z}[\sqrt{-6}]$ ein Teiler von 6, d. h. es gelte $6 = \alpha\beta$ für ein $\beta \in \mathbb{Z}[\sqrt{-6}]$. Wir wenden auf diese Gleichung die Normabbildung

$$N: \mathbb{Z}[\sqrt{-6}] \rightarrow \mathbb{Z}, \quad z \mapsto z\bar{z}$$

an und erhalten

$$36 = N(6) = N(\alpha\beta) = N(\alpha) \cdot N(\beta).$$

Damit haben wir $N(\alpha) \in \{1, 2, 3, 4, 6, 9, 12, 18, 36\}$. Wir benutzen nun die Argumentation aus (3)(a) im Kasten für die Gleichung

$$N(\alpha) = a^2 + 6b^2.$$

Ist $b = 0$, so heißt das $N(\alpha) = a^2$. Das ist nur für $N(\alpha) \in \{1, 4, 9, 36\}$ möglich. Für $N(\alpha) = 4$ ergibt sich $\alpha = \pm 2$ und dementsprechend $\beta = \pm 3$, im Fall $N(\alpha) = 9$ tauschen nur die Bezeichnungen. Die Fälle $N(\alpha) \in \{1, 36\}$ liefern die trivialen Teiler ± 1 und ± 6 .

Setzen wir nun also $b \neq 0$ voraus. Dann ist

$$N(\alpha) = a^2 + 6b^2 \geq 0 + 6 \cdot 1 = 6,$$

sodass die Fälle $N(\alpha) \in \{1, 2, 3, 4\}$ unmöglich sind. Auch die Fälle $N(\alpha) \in \{9, 12, 18, 36\}$ sind unmöglich, denn in diesem Fall wäre $N(\beta) \in \{1, 2, 3, 4\}$. Aus $6 = \alpha\beta$ und $b \neq 0$ folgt jedoch, dass auch der Imaginärteil von β nicht verschwinden kann, sodass das gleiche Argument wie oben auch $N(\beta) \notin \{1, 2, 3, 4\}$ zeigt.

Im Fall $N(\alpha) = 6$ muss $a = 0$ sein, sodass $b = \pm 1$, also $\alpha = \pm\sqrt{-6}$. Wegen $N(\beta) = 6$ daher auch $\beta = \pm\sqrt{-6}$.

Insgesamt erhalten wir damit die Kandidaten $\pm 1, \pm 2, \pm 3, \pm\sqrt{-6}, \pm 6$. Wegen

$$6 = 1 \cdot 6 = (-1) \cdot (-6) = 2 \cdot 3 = (-2) \cdot (-3) = \sqrt{-6} \cdot (-\sqrt{-6})$$

sind dies tatsächlich jeweils Teiler von 6.

Aufgabe (Herbst 2014, T3A4)

Sei $\omega \in \mathbb{C} \setminus \mathbb{Q}$ mit $\omega^2 \in \mathbb{Z}$ gegeben. Zeigen Sie:

- a** $\mathbb{Z}[\omega] := \{a + b\omega \mid a, b \in \mathbb{Z}\}$ ist ein Unterring von \mathbb{C} .
- b** Für $z = a + b\omega \in \mathbb{Z}[\omega]$ sei $z^* = a - b\omega$. Dann ist die *Normabbildung*

$$N : \mathbb{Z}[\omega] \longrightarrow \mathbb{Z}, \quad z \mapsto z\bar{z}$$

multiplikativ, d.h. für $z_1, z_2 \in \mathbb{Z}[\omega]$ gilt $N(z_1 z_2) = N(z_1)N(z_2)$.

- c** Ein Element $z \in \mathbb{Z}[\omega]$ ist genau dann eine Einheit, wenn $|N(z)| = 1$ ist.
- d** Der Ring $\mathbb{Z}[\sqrt{26}]$ besitzt unendlich viele Einheiten.

Lösungsvorschlag zur Aufgabe (Herbst 2014, T3A4)

- a** Offensichtlich ist $1 \in \mathbb{Z}[\omega]$. Seien $z_1, z_2 \in \mathbb{Z}[\omega]$. Schreibe $z_1 = a_1 + b_1\omega$ und $z_2 = a_2 + b_2\omega$, dann ist

$$\begin{aligned} z_1 - z_2 &= (a_1 + b_1\omega) - (a_2 + b_2\omega) = (a_1 - a_2) + (b_1 - b_2)\omega \in \mathbb{Z}[\omega], \\ z_1 \cdot z_2 &= (a_1 + b_1\omega) \cdot (a_2 + b_2\omega) = \\ &= (a_1 a_2 + b_1 b_2 \omega^2) + (a_1 b_2 + b_1 a_2)\omega \in \mathbb{Z}[\omega]. \end{aligned}$$

Damit sind alle Bedingungen dafür, dass $\mathbb{Z}[\omega]$ ein Unterring von \mathbb{C} ist, erfüllt.

- b** Seien $z_1, z_2 \in \mathbb{Z}[\omega]$ vorgegeben. Man berechnet:

$$N(z_1 z_2) = (z_1 z_2) \cdot (\overline{z_1 z_2}) = z_1 z_2 \overline{z_1 z_2} = (z_1 \overline{z_1}) \cdot (z_2 \overline{z_2}) = N(z_1) \cdot N(z_2)$$

- c** Ist $z \in \mathbb{Z}[\omega]$ eine Einheit, so gibt es ein Element $z^{-1} \in \mathbb{Z}[\omega]$ mit $z \cdot z^{-1} = 1$. Unter Verwendung von Teil **b** ist dann

$$N(z) \cdot N(z^{-1}) = N(z z^{-1}) = N(1) = 1 \cdot 1 = 1.$$

Da $N(z)$ ganzzahlig ist, bedeutet das $N(z) \in \{\pm 1\}$. Insbesondere $|N(z)| = 1$. Sei umgekehrt $|N(z)| = 1$ vorausgesetzt, dann ist

$$\pm 1 = N(z) = z\bar{z},$$

also ist z eine Einheit (mit Inversem \bar{z} oder $-z$) in $\mathbb{Z}[\omega]$.

d Wegen

$$-1 = 25 - 26 = (5 - \sqrt{26})(5 + \sqrt{26}) = N(5 + \sqrt{26})$$

ist $5 + \sqrt{26}$ nach Teil **c** eine Einheit in $\mathbb{Z}[\omega]$. Nun ist $5 + \sqrt{26} > 1$, deshalb ist die Folge $\{(5 + \sqrt{26})^n\}_{n \in \mathbb{N}}$ streng monoton steigend, besteht also insbesondere aus paarweise verschiedenen Gliedern. Da die Einheiten eines Rings eine Gruppe bilden, liegen diese Potenzen wieder in $\mathbb{Z}[\omega]^\times$, sodass dieser Ring unendlich viele Einheiten haben muss.

Aufgabe (Frühjahr 2010, T2A3)

Betrachten Sie die Gauß'schen Zahlen

$$\mathbb{Z}[i] = \{a + ib \in \mathbb{C} \mid a, b \in \mathbb{Z}\}$$

mit der Normabbildung $N: \mathbb{Z}[i] \rightarrow \mathbb{N}_0$, $N(z) := z\bar{z}$. \bar{z} steht dabei für die zu z komplex-konjugierte Zahl.

- a** Zeigen Sie: $z \in (\mathbb{Z}[i])^\times \Leftrightarrow N(z) = 1$.
- b** Sei $q \in \mathbb{Z}[i]$ so gewählt, dass $N(q)$ eine ungerade Primzahl ist. Zeigen Sie: q ist ein Primelement in $\mathbb{Z}[i]$ und für alle $\varepsilon \in (\mathbb{Z}[i])^\times$ gilt: $q \neq \varepsilon\bar{q}$.

Lösungsvorschlag zur Aufgabe (Frühjahr 2010, T2A3)

- a** „ \Rightarrow “: Sei $z \in \mathbb{Z}[i]$ eine Einheit, dann gibt es ein $w \in \mathbb{Z}[i]$, sodass $zw = 1$. Anwenden der Norm liefert:

$$1 = N(1) = N(zw) = N(z) \cdot N(w)$$

Da $N(z)$ eine nicht-negative ganze Zahl ist, muss bereits $N(z) = 1$ sein.

„ \Leftarrow “: Laut Voraussetzung ist $1 = N(z) = z\bar{z}$, d.h. $z^{-1} = \bar{z}$. Ist $z = a + ib$ mit $a, b \in \mathbb{Z}$, so liegt offensichtlich auch $\bar{z} = a - ib$ in $\mathbb{Z}[i]$. Also enthält $\mathbb{Z}[i]$ das multiplikative Inverse von z , sodass z eine Einheit in $\mathbb{Z}[i]$ ist.

- b** Sei p eine ungerade Primzahl und $N(q) = p$. Da $\mathbb{Z}[i]$ ein euklidischer Ring ist, genügt es zu zeigen, dass q irreduzibel in $\mathbb{Z}[i]$ ist. Sei dazu eine Faktorisierung $q = ab$ mit $a, b \in \mathbb{Z}[i]$ gegeben. Anwenden der Norm liefert

$$p = N(q) = N(ab) = N(a) \cdot N(b)$$

und da p eine Primzahl ist, muss $N(a) = p$ oder $N(b) = p$ sein. Als Konsequenz ist $N(b) = 1$ oder $N(a) = 1$ und laut Teil **a** bedeutet das, dass a oder b eine Einheit ist. Also ist q irreduzibel und damit auch prim.

Angenommen, es gibt eine Einheit $\varepsilon \in \mathbb{Z}[i]^\times$, sodass $q = \varepsilon\bar{q}$ erfüllt ist.
Schreibe $\varepsilon = x + iy$, dann gilt laut Teil **a**, dass

$$1 = N(\varepsilon) = \varepsilon\bar{\varepsilon} = (x + iy)(x - iy) = x^2 + y^2.$$

Nehmen wir an, dass $x \neq 0$ und $y \neq 0$. Dann ist $x^2, y^2 \geq 1$, d.h.

$$1 = x^2 + y^2 \geq 1 + 1 = 2,$$

was offensichtlich nicht sein kann. Also ist entweder $x = 0$ und damit $y^2 = 1$ oder $y = 0$ und damit $x^2 = 1$. Also erhalten wir

$$(x, y) \in \{(0, 1), (0, -1), (1, 0), (-1, 0)\} \Leftrightarrow \varepsilon \in \{i, -i, 1, -1\}.$$

Oben hatten wir angenommen, dass $q = \varepsilon\bar{q}$. Sei $q = c + id$ mit $c, d \in \mathbb{Z}$, dann impliziert dies

$$p = N(q) = q\bar{q} = \varepsilon\bar{\varepsilon} = \varepsilon(c^2 - d^2 - 2icd).$$

Wegen $p \in \mathbb{N}$ muss der Imaginärteil der rechten Seite verschwinden. Ist $\varepsilon = \pm 1$, so beträgt dieser $\mp 2cd$. Daraus folgt jedoch $c = 0$ oder $d = 0$ und damit $p = \varepsilon\bar{\varepsilon}^2 = \pm c^2$ oder $p = \pm d^2$ im Widerspruch dazu, dass p eine Primzahl ist.

Ist $\varepsilon = \pm i$, so ist der Realteil der rechten Seite $\pm 2cd$ und die Gleichung erzwingt $p = \pm 2cd$ obwohl p ungerade sein soll. Beide Fälle führen also zu Widersprüchen, weswegen die Annahme $q = \varepsilon\bar{q}$ falsch gewesen sein muss.

Aufgabe (Herbst 2010, T1A3)

Sei $\omega \in \mathbb{C}$ eine primitive dritte Einheitswurzel. Der Ring $R = \mathbb{Z}[\omega]$ ist ein euklidischer Ring mit Normabbildung $N : R \rightarrow \mathbb{N}_0$ definiert durch

$$N(a + b\omega) = (a + b\omega)(a + b\omega^2) = a^2 - ab + b^2, \quad a, b \in \mathbb{Z}.$$

Zeigen Sie:

- a** Ein Element $y \in R$ ist genau dann eine Einheit in R , wenn $N(y) = 1$.
- b** Sei $p \in \mathbb{Z}$ eine Primzahl. Dann ist $p = a^2 - ab + b^2$ für geeignete $a, b \in \mathbb{Z}$ genau dann, wenn das Ideal $(p) \subseteq R$ kein Primideal ist.
- c** Sei $p \in \mathbb{Z}$ eine Primzahl und $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ der endliche Körper mit p Elementen. Das Ideal $(p) \subseteq R$ ist genau dann ein Primideal, wenn das Polynom $X^2 + X + 1 \in \mathbb{F}_p[X]$ irreduzibel ist.

Lösungsvorschlag zur Aufgabe (Herbst 2010, T1A3)

- a** „ \Rightarrow “: Wir zeigen zunächst, dass die Normabbildung multiplikativ ist. Dazu bemerken wir, dass aus $\omega^3 = 1$ insbesondere $|\omega|^3 = 1$ folgt. Da $|\omega|$ eine positive reelle Zahl ist, folgt $|\omega| = 1$. Gleichzeitig ist $\omega\bar{\omega} = |\omega|^2$, sodass

$$\omega\bar{\omega} = 1 = \omega^3 \quad \Rightarrow \quad \bar{\omega} = \omega^2.$$

Dies zeigt $N(a + b\omega) = (a + b\omega)(a + b\bar{\omega}) = (a + b\omega)\overline{(a + b\omega)}$ und die Behauptung folgt aus der Multiplikativität der komplexen Konjugation.

Sei nun $y \in R$ eine Einheit, dann folgt

$$1 = N(yy^{-1}) = N(y) \cdot N(y^{-1})$$

aus der Multiplikativität und $N(y)$ muss eine Einheit in \mathbb{Z} sein. Das bedeutet $N(y) \in \{-1, +1\}$. Allerdings ist $N(y)$ stets nicht-negativ, denn laut dem oben Bewiesenen ist $N(y) = y\bar{y} = |y|^2$. Also muss $N(y) = 1$ sein.

„ \Leftarrow “: Es sei umgekehrt $N(y) = 1$ für $y = a + b\omega \in \mathbb{Z}[\omega]$ vorausgesetzt, d. h.

$$N(y) = (a + b\omega)(a + b\omega^2) = 1.$$

Offensichtlich ist $(a + b\omega^2)$ das Inverse von y in $\mathbb{Z}[\omega]$, d. h. y ist invertierbar in $\mathbb{Z}[\omega]$.

- b** „ \Rightarrow “: Sei p eine Primzahl, die eine Darstellung als $p = a^2 - ab + b^2$ mit $a, b \in \mathbb{Z}$ besitzt. Es ist dann

$$p = a^2 - ab + b^2 = N(a + b\omega) = (a + b\omega)(a + b\omega^2) \in (p).$$

Nach Teil **a** können nun $a + b\omega$ und $a + b\omega^2$ keine Einheiten sein, denn beide haben Norm $p \neq 1$. Somit ist p reduzibel in $\mathbb{Z}[\omega]$ und da $\mathbb{Z}[\omega]$ laut Angabe euklidisch ist, kann p nach Proposition 2.10 kein Primelement sein. Es folgt, dass (p) kein Primideal ist.

„ \Leftarrow “: Sei umgekehrt (p) kein Primideal. Laut Angabe ist $\mathbb{Z}[\omega]$ ein euklidischer Ring, sodass p nach Proposition 2.10 nicht irreduzibel sein kann. Es gibt also Nicht-Einheiten $x, y \in \mathbb{Z}[\omega]$ mit

$$p = xy \quad \Rightarrow \quad p^2 = N(p) = N(x) \cdot N(y).$$

Da x und y keine Einheiten sind, ist nach Teil **a** $N(x) \neq 1 \neq N(y)$, sodass diese Gleichung nur erfüllt sein kann, falls $p = N(x) = N(y)$. Schreibe x als $a + b\omega$, dann bedeutet dies gerade

$$p = N(x) = N(a + b\omega) = a^2 - ab + b^2.$$

c Wir zeigen zunächst folgende Isomorphie:

$$\mathbb{F}_p[X]/(X^2 + X + 1) \cong \mathbb{Z}[\omega]/(p).$$

Betrachte dazu den Homomorphismus

$$\phi: \mathbb{Z}[\omega] \rightarrow \mathbb{F}_p[X]/(X^2 + X + 1), \quad \sum_{i=0}^n a_i \omega^i \mapsto \sum_{i=0}^n \bar{a}_i X^i + (X^2 + X + 1).$$

Dieser ist surjektiv, denn ist $f + (X^2 + X + 1)$ mit $f = \sum_{i=0}^n \bar{a}_i X^i \in \mathbb{F}_p[X]$ vorgegeben, so ist $\sum_{i=0}^n a_i \omega^i$ ein Urbild von $f + (X^2 + X + 1)$ unter ϕ .

Weiter ist $(p) \subseteq \ker \phi$ wegen $\text{char } \mathbb{F}_p = p$. Sei umgekehrt ein Element $\alpha(\omega) = \sum_{i=0}^n a_i \omega^i \in \ker \phi$ vorgegeben, dann bedeutet $\phi(\alpha(\omega)) = 0$ gerade, dass $\phi(\alpha)$ im Ideal $(X^2 + X + 1) \subseteq \mathbb{F}_p[X]$ liegt. Dies ist genau dann der Fall, wenn es ein Polynom $g \in \mathbb{Z}[X]$ gibt, sodass das Polynom

$$\alpha(X) - g \cdot (X^2 + X + 1)$$

durch p teilbar ist. Weil $X^2 + X + 1$ gerade das dritte Kreisteilungspolynom ist, ist $\omega^2 + \omega + 1 = 0$, also folgt durch Einsetzen von ω , dass $\alpha(\omega)$ durch p teilbar ist. Dies zeigt $\ker \phi \subseteq (p)$.

Der Homomorphiesatz liefert dann die gewünschte Isomorphie.

Da $\mathbb{Z}[\omega]$ und $\mathbb{F}_p[X]$ euklidische Ringe sind, ist in ihnen jedes Primideal auch ein maximales Ideal. Also ist

$$\begin{aligned} (p) \subseteq \mathbb{Z}[\omega] \text{ prim} &\Leftrightarrow \mathbb{Z}[\omega]/(p) \text{ ist Körper} \\ &\Leftrightarrow \mathbb{F}_p[X]/(X^2 + X + 1) \text{ ist Körper} \\ &\Leftrightarrow (X^2 + X + 1) \subseteq \mathbb{F}_p[X] \text{ ist maximal} \end{aligned}$$

und Letzteres ist genau dann der Fall, wenn $X^2 + X + 1$ irreduzibel in $\mathbb{F}_p[X]$ ist.

Die ganzen Zahlen \mathbb{Z} sind sicherlich der für jeden von uns vertrauteste Ring, welcher eine Reihe schöner Eigenschaften wie die eindeutige Primfaktorzerlegung oder die Möglichkeit der Division mit Rest hat. Diese Eigenschaften lassen sich nicht auf jeden Ring übertragen, weshalb wir nun Bezeichnungen für diejenigen Ringe einführen, für die das möglich ist.

Definition 2.9. Sei R ein Integritätsbereich.

- (1) Gibt es eine Abbildung $|\cdot|: R \setminus \{0\} \rightarrow \mathbb{N}$, sodass es für beliebige $x, y \in R$ mit $y \neq 0$ immer $q, r \in R$ mit

$$x = qy + r \quad \text{und } |r| < |y| \text{ oder } r = 0$$

gibt, so heißt R ein *euklidischer Ring*. Die Abbildung $|\cdot|$ wird als *Höhenfunktion* bezeichnet.

- (2) Falls jedes Ideal in R ein Hauptideal ist, wird R als *Hauptidealring* bezeichnet.
(3) Lässt sich jedes $a \in R$ mit $a \neq 0$ und $a \notin R^\times$ bis auf Assoziiertheit und Reihenfolge als Produkt irreduzibler Elemente schreiben, so ist R ein *faktorieller Ring*.

Nachfolgend seien zusammenfassend einige Resultate zu diesen Begriffen genannt:

- (1) Jeder euklidische Ring ist ein Hauptidealring.
- (2) Jeder Hauptidealring ist ein faktorieller Ring.
- (3) Ist K ein Körper, so ist $K[X]$ ein Hauptidealring.
- (4) Ist A ein faktorieller Ring, so ist $A[X]$ ein faktorieller Ring.
- (5) In einem Hauptidealring ist jedes Primideal auch maximal.

Proposition 2.10. Sei R ein faktorieller Ring und $p \in R \setminus \{0\}$ keine Einheit. Die folgenden Aussagen sind gleichwertig:

- (1) p ist ein Primelement,
- (2) p ist ein irreduzibles Element,
- (3) (p) ist ein Primideal von R .

Aufgabe (Frühjahr 2012, T3A4)

Sei R ein Integritätsring. Zeigen Sie: Ist $R[X]$ ein Hauptidealring, so ist R ein Körper.

Lösungsvorschlag zur Aufgabe (Frühjahr 2012, T3A4)

Es ist $R[X]/(X) \cong R$ und da R nach Voraussetzung Integritätsbereich ist, ist (X) laut Satz 2.7 ein Primideal. In einem Hauptidealring ist jedes Primideal auch maximal, sodass $R \cong R[X]/(X)$ ein Körper ist.

Aufgabe (Frühjahr 2014, T3A3)

Wir betrachten die Teilmenge $R = \{a + bi\sqrt{2} \mid a, b \in \mathbb{Z}\}$ von \mathbb{C} .

- a** Zeigen Sie, dass R ein Unterring von \mathbb{C} ist.
- b** Beweisen Sie, dass R ein euklidischer Ring ist bezüglich der Normfunktion $d(\alpha) := |\alpha|^2$.
- c** Geben Sie alle möglichen Faktorisierungen von $8 - i\sqrt{2}$ in irreduzible Elemente von R an (bis auf Reihenfolge).

Lösungsvorschlag zur Aufgabe (Frühjahr 2014, T3A3)

- a** Offensichtlich ist $1 \in \mathbb{Z}[i\sqrt{2}]$. Seien $z_1, z_2 \in \mathbb{Z}[i\sqrt{2}]$. Schreibe $z_1 = a_1 + b_1i\sqrt{2}$ und $z_2 = a_2 + b_2i\sqrt{2}$, dann ist

$$z_1 - z_2 = (a_1 + b_1i\sqrt{2}) - (a_2 + b_2i\sqrt{2}) = (a_1 - a_2) + (b_1 - b_2)i\sqrt{2},$$

$$z_1 \cdot z_2 = (a_1 + b_1i\sqrt{2}) \cdot (a_2 + b_2i\sqrt{2}) = (a_1a_2 - 2b_1b_2) + (a_1b_2 + b_1a_2)i\sqrt{2}.$$

Damit sind auch die Bedingungen $z_1 - z_2, z_1z_2 \in \mathbb{Z}[i\sqrt{2}]$ erfüllt und $\mathbb{Z}[i\sqrt{2}]$ ist ein Unterring von \mathbb{C} .

- b** Seien $x = a + b\sqrt{-2}, y = c + d\sqrt{-2} \in R$ mit $y \neq 0$ vorgegeben. Wir müssen Elemente $q, r \in R$ finden mit $x = qy + r$ und $d(r) < d(y)$ oder $r = 0$. Dazu berechnen wir zunächst in \mathbb{C}

$$\frac{x}{y} = \frac{a + b\sqrt{-2}}{c + d\sqrt{-2}} = \frac{(a + b\sqrt{-2})(c - d\sqrt{-2})}{(c + d\sqrt{-2})(c - d\sqrt{-2})} = \frac{(ac + 2bd) + (bc - ad)\sqrt{-2}}{c^2 + 2d^2}.$$

Durch Auf- oder Abrunden erhalten wir nun ganze Zahlen r, s mit

$$\left| r - \frac{(ac + 2bd)}{c^2 + 2d^2} \right| \leq \frac{1}{2} \quad \text{und} \quad \left| s - \frac{bc - ad}{c^2 + 2d^2} \right| \leq \frac{1}{2}.$$

Setze dann $q = r + s\sqrt{-2}$ und $r = x - qy$, so gilt offensichtlich die erste geforderte Gleichung und außerdem $r = 0$ oder

$$\frac{d(r)}{d(y)} = \frac{|x - qy|^2}{|y|^2} = \left| \frac{x}{y} - q \right|^2 \leq (\frac{1}{2})^2 + 2(\frac{1}{2})^2 = \frac{3}{4} < 1$$

und damit $d(r) < d(y)$ wie gewünscht.

- c** Laut Teil **b** ist R ein euklidischer, also insbesondere faktorieller, Ring. Daher ist die gesuchte Zerlegung eindeutig bis auf Multiplikation mit Einheiten. Wir bestimmen also in einem ersten Schritt eine konkrete Zerlegung und dann die Menge der Einheiten, um die restlichen zu erhalten.

Seien $x = a_1 + b_1\sqrt{-2}$ und $y = a_2 + b_2\sqrt{-2}$ irreduzible Elemente aus R mit $8 - \sqrt{-2} = xy$. Wegen $d(8 - \sqrt{-2}) = 64 + 2 = 66$ sind $d(x)$ und $d(y)$ Teiler von 66. Beispielsweise überlegt man sich

$$11 = 9 + 2 = 3^2 + \sqrt{2}^2 = d(3 + \sqrt{-2})$$

und macht den Ansatz $x = 3 + \sqrt{-2}$. Die Bedingung $xy = 8 - \sqrt{-2}$ liefert dann die Gleichungen

$$3a_2 - 2b_2 = 8 \quad \text{und} \quad 3b_2 + a_2 = -1,$$

aus denen man $a_2 = 2$ und $b_2 = -1$ gewinnt. Tatsächlich ist dann auch $8 - \sqrt{-2} = (3 + \sqrt{-2})(2 - \sqrt{-2})$. Da $d(3 + \sqrt{-2}) = 11$ eine Primzahl ist, muss $3 + \sqrt{-2}$ irreduzibel sein. Den zweiten Faktor kann man dagegen noch weiter in $-\sqrt{-2}(1 + \sqrt{-2})$ zerlegen, wobei dies nun ebenfalls eine Faktorisierung in irreduzible Elemente ist, da die Faktoren Primzahlen als Norm haben. Wir erhalten deshalb

$$8 - \sqrt{-2} = -\sqrt{-2}(1 + \sqrt{-2})(3 + \sqrt{-2}).$$

Zur Bestimmung der Einheiten in R : Sei $z \in R^\times$ eine Einheit, dann gilt

$$z \cdot z^{-1} = 1 \quad \Rightarrow \quad |z|^2 \cdot |z^{-1}|^2 = |z \cdot z^{-1}|^2 = 1.$$

Also ist $N(z) = |z|^2$ eine invertierbare reelle Zahl. Schreibe $z = c + id\sqrt{2}$, dann ist $N(z) = c^2 + 2d^2$, also eine positive ganze und invertierbare Zahl. Es bleibt daher nur $N(z) = 1$.

Angenommen, $d \neq 0$, dann ist $d^2 \geq 1$ und wir haben

$$1 = N(z) = c^2 + 2d^2 \geq 0 + 2 \cdot 1 = 2,$$

was unsinnig ist. Es folgt $d = 0$, d. h. $z = c \in \mathbb{Z}$ und $N(z) = a^2$ impliziert $z \in \{\pm 1\}$. Dies zeigt $R^\times = \{\pm 1\}$. Zusätzlich zu der Zerlegung oben gibt es daher noch die Zerlegungen

$$\begin{aligned} 8 - \sqrt{-2} &= \sqrt{-2}(-1 - \sqrt{-2})(3 + \sqrt{-2}) \\ 8 - \sqrt{-2} &= \sqrt{-2}(1 + \sqrt{-2})(-3 - \sqrt{-2}) \\ 8 - \sqrt{-2} &= -\sqrt{-2}(-1 - \sqrt{-2})(-3 - \sqrt{-2}). \end{aligned}$$

Aufgabe (Herbst 2012, T1A4)

Sei $R = \mathbb{Z} \left[\frac{1+\sqrt{-7}}{2} \right] \subseteq \mathbb{C}$ gegeben. Sie dürfen ohne Beweis verwenden, dass R bezüglich der Normfunktion

$$N : R \longrightarrow \mathbb{N}_0, z \mapsto z\bar{z},$$

ein euklidischer Ring ist.

- a** Bestimmen Sie alle Einheiten von R .
- b** Zerlegen Sie 3, 5 und 7 in Primfaktoren in R .

Lösungsvorschlag zur Aufgabe (Herbst 2012, T1A4)

- a** Sei $\omega = \frac{1+\sqrt{-7}}{2}$ und $x = a + b\omega$ eine Einheit in R . Dann gibt es ein Inverses $x^{-1} \in R$, sodass $xx^{-1} = 1$ und wir haben, dass notwendigerweise $1 = N(1) = N(x)N(x^{-1})$ gelten muss. Da der Wertebereich der Normfunktion laut Angabe die natürlichen Zahlen sind, folgt daraus sogar

$$1 = N(x) = x\bar{x} = (a + \frac{b}{2})^2 + (\frac{b}{2}\sqrt{-7})^2 = a^2 + ab + 2b^2.$$

Fassen wir diese Gleichung als quadratische Gleichung in a auf, so können wir die Lösungen

$$a_{\pm} = \frac{-b \pm \sqrt{b^2 - 4(2b^2 - 1)}}{2} = -\frac{b}{2} \pm \frac{1}{2}\sqrt{-7b^2 + 4}$$

hinschreiben. Da wir nach einer ganzzahligen Lösung suchen, muss

$$-7b^2 + 4 \geq 0 \Leftrightarrow 4 \geq 7b^2$$

erfüllt sein. Ist $b \neq 0$, so ist $b^2 \geq 1$ und die Ungleichung ist bereits nicht mehr erfüllt. Also muss $b = 0$ sein und der Term oben reduziert sich zu $a_{\pm} = \pm 1$. Dass umgekehrt ± 1 Einheiten sind, ist klar. Also ist $R^\times = \{\pm 1\}$.

- b** Die Primfaktorzerlegung von 7 ist natürlich $-\sqrt{-7}^2$, dazu bemerke man, dass

$$\sqrt{-7} = 2\omega - 1 \in \mathbb{Z}[\omega].$$

Da $N(\sqrt{-7}) = 7$ eine Primzahl ist, ist $\sqrt{-7}$ irreduzibel in R . Laut Angabe handelt es sich bei R um einen euklidischen Ring, deshalb ist $\sqrt{-7}$ dort auch prim.

Die Primzahlen 3 und 5 bleiben dagegen prim. Um dies zu zeigen, gibt es zwei verschiedene Möglichkeiten, die wir an jeweils einer der beiden Zahlen illustrieren.

1. Möglichkeit: Angenommen, es gäbe Zahlen $\alpha = a_1 + a_2\omega, \beta = b_1 + b_2\omega \in R$ mit $\alpha\beta = 3$. Dann folgt wegen der Multiplikativität der Normabbildung

$$9 = N(3) = N(\alpha\beta) = N(\alpha)N(\beta),$$

also sind $N(\alpha)$ und $N(\beta)$ Teiler von 9. Im Fall, dass $N(\alpha)$ oder $N(\beta)$ gleich 1 ist, ist α oder β laut Teil **a** eine Einheit. Eine echte Zerlegung erhalten wir also nur für den Fall $N(\alpha) = N(\beta) = 3$. Die Mitternachtsformel liefert

$$a^2 + ab + 2b^2 = 3 \Leftrightarrow a_{1,2} = \frac{-b \pm \sqrt{b^2 - 4(b^2 - 3)}}{2} = -\frac{b}{2} \pm \frac{1}{2}\sqrt{-7b^2 + 12}.$$

Ganz analog zu Teil **a** ist diese Zahl überhaupt nur für $|b| \leq 1$ reell. Für $|b| = 1$ ist der Radikand 5, und für $b = 0$ gleich 12, sodass die Gleichung keine ganzzahlige Lösung besitzt und 3 irreduzibel ist.

2. Möglichkeit: Man bemerkt, dass $\omega^2 - \omega + 2 = 0$ erfüllt ist. Analog zu Aufgabe H10T1A3 **c** (Seite 88) erhält man deshalb einen Isomorphismus

$$\mathbb{Z}[\omega]/(5) \cong \mathbb{F}_5[X]/(X^2 - X + 2).$$

Da $X^2 - X + 2$ in \mathbb{F}_5 keine Nullstellen hat und somit irreduzibel ist, ist der Ring $\mathbb{Z}[\omega]/(5)$ ein Integritätsbereich (sogar ein Körper), also ist 5 ein Primelement.

Aufgabe (Frühjahr 2012, T1A3)

Die Teilmenge

$$R = \{q \in \mathbb{Q} \mid \exists a, b \in \mathbb{Z} : q = \frac{a}{b} \text{ und } 2 \nmid b \text{ und } 3 \nmid b\}$$

des Körpers der rationalen Zahlen ist ein Unterring, der die ganzen Zahlen enthält.

- a** Bestimmen Sie die Einheiten-Gruppe R^\times .
- b** Zeigen Sie, dass 2 und 3 Primelemente von R sind.
- c** Zeigen Sie, dass jedes Primelement zu 2 oder zu 3 assoziiert ist.

Hinweis Zwei Elemente $x, y \in R$ sind zueinander *assoziiert*, wenn es eine Einheit u gibt mit $x = u \cdot y$.

Lösungsvorschlag zur Aufgabe (Frühjahr 2012, T1A3)

- a** Wir behaupten, dass $R^\times = \left\{ \frac{a}{b} \in R \mid 2 \nmid a, 3 \nmid a \right\}$ ist. Sei dazu $\frac{a}{b} \in R^\times$ vorgegeben. Es gibt dann $\frac{c}{d} \in R$, sodass

$$\frac{a}{b} \cdot \frac{c}{d} = 1 \Leftrightarrow ac = bd.$$

Nach Definition von R werden b und d weder von 2 noch 3 geteilt. Also haben wir $2, 3 \nmid ac$ und es folgt $2, 3 \nmid a$ und $2, 3 \nmid c$. Setzen wir umgekehrt voraus, dass $\frac{a}{b} \in R$ mit $2 \nmid a$ und $3 \nmid a$, so ist $\frac{b}{a} \in R$ und wegen $\frac{a}{b} \cdot \frac{b}{a} = 1$ ist $\frac{a}{b}$ eine Einheit.

- b** Sei $p \in \{2, 3\}$ und $\frac{a}{b} \in R$. Es liegt $\frac{a}{b}$ genau dann in pR , wenn $p \mid a$. Ist nämlich $\frac{a}{b} = p \cdot \frac{c}{d}$, so bedeutet dies $ad = pcb$. Wegen $p \nmid d$ folgt $p \mid a$, da p eine Primzahl ist.

Für die umgekehrte Richtung sei $\frac{a}{b} \in R$ mit $p \mid a$ vorgegeben. Schreibe $a = p \cdot c$, dann ist $\frac{a}{b} = p \cdot \frac{c}{b}$ und $\frac{c}{b}$ liegt in R , da $p \nmid b$.

Wir zeigen nun, dass R/pR ein Körper ist. Sei dazu $\alpha \in R/pR$ mit $\alpha \neq 0$ vorgegeben. Es gibt $\frac{a}{b} \in R$, sodass $\alpha = \frac{a}{b} + pR$ und die Bedingung $\alpha \neq 0$ bedeutet $\frac{a}{b} \notin pR$. Nach dem oben Bewiesenen also $p \nmid a$. Nach Teil **a** heißt das $\frac{a}{b} \in R^\times$, setze also $\beta = \frac{b}{a} + pR$, dann ist $\alpha \cdot \beta = 1 + pR$. Dies zeigt, dass R/pR ein Körper ist. Es folgt, dass pR ein maximales Ideal ist, also insbesondere ein Primideal und somit p ein Primelement ist.

- c** Sei $q \in R$ ein Primelement, dann ist $qR \subseteq R$ ein Primideal. Betrachte die Menge $qR \cap \mathbb{Z}$, welche wiederum ein Primideal ist, wie man leicht zeigt. Die Primideale von \mathbb{Z} sind genau die Ideale $p\mathbb{Z}$ mit einer Primzahl p und (0) . Schreibe $q = \frac{a}{b}$, dann ist $a = b \cdot \frac{a}{b} \in qR \cap \mathbb{Z}$, sodass $qR \cap \mathbb{Z} \neq (0)$.

Also ist $qR \cap \mathbb{Z} = p\mathbb{Z}$ für eine Primzahl p . Wäre $p \notin \{2, 3\}$, so würde qR mit p nach Teil **a** eine Einheit in R enthalten, sodass $qR = R$. Dies steht im Widerspruch zu $qR \subsetneq R$ prim. Also ist $p \in \{2, 3\}$ und aus $p \in qR \cap \mathbb{Z} \subseteq qR$ folgt $pR \subseteq qR$. Nach Teil **b** ist das Ideal pR maximal, also muss sogar $pR = qR$ sein. Da p und q das gleiche Ideal erzeugen, müssen sie assoziiert zueinander sein.

Zum Abschluss eine Aufgabe, in der nochmal (fast) alle Begriffe dieses Abschnitts auftreten.

Aufgabe (Frühjahr 2000, T1A3)

Bestimmen Sie die Anzahl der Ideale, der Primideale, der Einheiten, der Nullteiler und der nilpotenten Elemente im Ring $\mathbb{Z}/2000\mathbb{Z}$.

Lösungsvorschlag zur Aufgabe (Frühjahr 2000, T1A3)

Sei $R = \mathbb{Z}/2000\mathbb{Z}$.

Ideale: Nach Satz 2.12 haben wir eine bijektive Korrespondenz zwischen den Idealen in R und den Idealen in \mathbb{Z} , die das Ideal $2000\mathbb{Z}$ enthalten. Da \mathbb{Z} ein Hauptidealring ist, genügt es also, alle $a \in \mathbb{Z}$ zu bestimmen, für die

$$2000\mathbb{Z} \subseteq a\mathbb{Z} \Leftrightarrow a \mid 2000 = 2^4 \cdot 5^3$$

gilt. Es gibt $5 \cdot 4$ Möglichkeiten für die Wahl der Exponenten in der Primfaktorzerlegung von a , also ist die gesuchte Anzahl 20.

Primideale: Die oben beschriebene Korrespondenz bildet Primideale auf Primideale ab, d. h. die Primideale in R entsprechen in eindeutiger Weise den Primteilern 2 und 5 von 2000. Es gibt folglich zwei verschiedene Primideale in R .

Einheiten: Die Anzahl der Einheiten lässt sich mithilfe der Euler'schen φ -Funktion berechnen:

$$\varphi(2000) = \varphi(2^4 \cdot 5^3) = \varphi(2^4) \cdot \varphi(5^3) = 2^3 \cdot 4 \cdot 5^2 = 800$$

Nullteiler: Wir weisen zunächst folgende Äquivalenz nach: $\bar{0} \neq \bar{x} \in R$ ist ein Nullteiler genau dann, wenn $\text{ggT}(x, 2000) \neq 1$.

„ \Leftarrow “: Sei $y = \frac{2000}{\text{ggT}(x, 2000)}$, dann ist $0 < y < 2000$, d. h. $\bar{y} \neq \bar{0}$. Sei $x = k \cdot \text{ggT}(x, 2000)$ für ein $k \in \mathbb{Z}$, dann ist

$$\bar{y} \cdot \bar{x} = \overline{\frac{2000}{\text{ggT}(x, 2000)} \cdot k \cdot \text{ggT}(x, 2000)} = \overline{2000k} = \bar{0}$$

also ist \bar{x} ein Nullteiler.

„ \Rightarrow “: Nach Voraussetzung ist \bar{x} Nullteiler, d. h. es gibt ein $\bar{0} \neq \bar{y} \in R$, sodass

$$\bar{x} \cdot \bar{y} = \bar{0} \Leftrightarrow 2000 \mid xy.$$

Da $\bar{y} \neq \bar{0}$, teilt 2000 nicht y , sodass mindestens einer der Primfaktoren von 2000 in x auftaucht und somit $\text{ggT}(2000, x) \neq 1$ gilt.

Die Anzahl der Nullteiler ist also durch die Anzahl derjenigen natürlichen Zahlen kleiner gleich 2000 gegeben, die nicht teilerfremd zu 2000 sind. Diese lässt sich mithilfe der Euler'schen φ -Funktion zu

$$2000 - \varphi(2000) = 2000 - 800 = 1200$$

bestimmen.

nilpotente Elemente: Wir zeigen zunächst: Es gibt genau dann ein $n \in \mathbb{N}$ mit $\bar{x}^n = \bar{0}$, wenn $10 \mid x$.

„ \Rightarrow “: Es gelte $\bar{x}^n = \bar{0}$, dann folgt $2000 \mid x^n$ und die Primfaktoren 2 und 5 müssen jeweils bereits x teilen. Also $10 \mid x$.

„ \Leftarrow “: Sei umgekehrt $x = 10k$, dann ist

$$x^4 = (10k)^4 = 10^4 \cdot k^4 = 2000 \cdot (5k^4) \equiv 0 \pmod{2000}$$

d. h. $\bar{x}^4 = \bar{0}$ und \bar{x} ist nilpotent.

Wir haben damit gezeigt, dass die nilpotenten Elemente in R gerade durch

$$\bar{0}, \bar{10}, \bar{20}, \dots, \bar{1990}$$

gegeben sind. Die gesuchte Anzahl ist daher 200.

2.2. Rechnen in Restklassenringen

Sei R ein Ring und $\mathfrak{a} \subseteq R$ ein Ideal. Wir wollen analog zur Konstruktion der Faktorgruppen aus der Gruppentheorie nun auf der Menge $R/\mathfrak{a} = \{r + \mathfrak{a} \mid r \in R\}$ eine Ringstruktur definieren. Wie dort sind dabei zwei Nebenklassen $x + \mathfrak{a}$ und $y + \mathfrak{a}$ genau dann gleich, wenn es ein $x - y \in \mathfrak{a}$ gilt. Man schreibt dann auch

$$x \equiv y \pmod{\mathfrak{a}}$$

Im Fall $R = \mathbb{Z}$ ist jedes Ideal ein Hauptideal, also $\mathfrak{a} = (a)$ für ein $a \in \mathbb{Z}$, sodass wir zusätzlich folgende Charakterisierungen erhalten

$$x \equiv y \pmod{a} \Leftrightarrow x - y \in (a) \Leftrightarrow a \mid x - y.$$

Der „einfachste“ Repräsentant der Nebenklasse $x + (a)$ ist somit der Rest bei Division von x durch a , weshalb man bei solchen Ringen auch von *Restklassenringen* oder *Faktorringen* spricht.

Mittels folgender Definitionen für Addition bzw. Multiplikation

$$\begin{aligned} (x + \mathfrak{a}) + (y + \mathfrak{a}) &= (x + y) + \mathfrak{a} \\ (x + \mathfrak{a}) \cdot (y + \mathfrak{a}) &= (x \cdot y) + \mathfrak{a} \end{aligned}$$

ist auf R/\mathfrak{a} eine Ringstruktur definiert. Diese Verknüpfungen sind wohldefiniert, hängen also nicht von der Wahl des Repräsentanten einer Nebenklasse ab.

Tipp: Wahl von Repräsentanten

Durch geschickte Wahl des Repräsentanten einer Nebenklasse kann man sich das Leben sehr viel einfacher machen. Beispielsweise liefern die Rechnungen im Restklassenring $\mathbb{Z}/12\mathbb{Z}$

$$11^2 \cdot 13 = 121 \cdot 13 = 1573 = 131 \cdot 12 + 1 \equiv 1 \pmod{12}$$

$$11^2 \cdot 13 \equiv (-1)^2 \cdot 1 \equiv 1 \pmod{12}$$

beide das gleiche Ergebnis, die zweite ist jedoch deutlich einfacher auszuführen.

Aufgabe (Frühjahr 2015, T1A2)

Sei $m \geq 3$ eine ungerade ganze Zahl. Zeigen Sie die folgende Kongruenz:

$$1^m + 2^m + 3^m + \dots + (m-3)^m + (m-2)^m + (m-1)^m \equiv 0 \pmod{m}$$

Lösungsvorschlag zur Aufgabe (Frühjahr 2015, T1A2)

Es ist $m-1 \equiv -1 \pmod{m}$ und, da m ungerade ist, ist $(-1)^m = -1$. Also gilt:

$$\begin{aligned} 1^m + 2^m + 3^m + \dots + m + \dots + (m-3)^m + (m-2)^m + (m-1)^m &\equiv \\ \equiv 1^m + 2^m + 3^m + \dots + m + \dots + (-3)^m + (-2)^m + (-1)^m &\equiv \\ \equiv 1 + 2^m + 3^m + \dots + m + \dots + (-1) \cdot 3^m + (-1) \cdot 2^m + (-1) &\equiv \\ \equiv 0 \pmod{m} \end{aligned}$$

Man beachte dabei, dass die „Paarbildung“ aufgeht, da m ungerade ist.

Aufgabe (Frühjahr 2011, T1A3)

Sei p eine ungerade Primzahl. Zeigen Sie, dass

$$2^2 \cdot 4^2 \cdot \dots \cdot (p-3)^2 \cdot (p-1)^2 \equiv (-1)^{\frac{1}{2}(p+1)} \pmod{p}.$$

Hinweis Ohne Beweis darf der Wilson'sche Satz verwendet werden: Eine natürliche Zahl $n \geq 2$ ist genau dann eine Primzahl, wenn $(n-1)! + 1$ durch n teilbar ist.

Lösungsvorschlag zur Aufgabe (Frühjahr 2011, T1A3)

Wir sortieren zunächst die Faktoren um:

$$\begin{aligned} & 2^2 \cdot 4^2 \cdot \dots \cdot (p-3)^2 \cdot (p-1)^2 = \\ & = (p-1) \cdot 2 \cdot (p-3) \cdot \dots \cdot 4 \cdot (p-3) \cdot 2 \cdot (p-1) \equiv \\ & \equiv (-1) \cdot 2 \cdot (-3) \cdot \dots \cdot ((p-4)) \cdot (p-3) \cdot ((p-2)) \cdot (p-1) \pmod{p} \end{aligned}$$

Von den insgesamt $p-1$ Faktoren hat nun genau die Hälfte ein negatives Vorzeichen. Sammeln wir diese, steht dort

$$(-1)^{\frac{p-1}{2}} \cdot 1 \cdot 2 \cdot 3 \cdot \dots \cdot (p-4) \cdot (p-3) \cdot (p-2) \cdot (p-1) = (-1)^{\frac{p-1}{2}} \cdot (p-1)!$$

und nach dem Satz von Wilson ist $(p-1)! \equiv -1 \pmod{p}$, sodass also insgesamt gilt:

$$2^2 \cdot 4^2 \cdot \dots \cdot (p-3)^2 \cdot (p-1)^2 \equiv (-1)^{\frac{p-1}{2}} \cdot (-1) = (-1)^{\frac{p+1}{2}} \pmod{p}.$$

Aufgabe (Frühjahr 2014, T2A1)

Es seien die Polynome $p(X) = X^{500} - 2X^{301} + 1$ und $q(X) = X^2 - 1$ in $\mathbb{Q}[X]$ gegeben. Berechnen Sie den Rest der Division von $p(X)$ durch $q(X)$.

Lösungsvorschlag zur Aufgabe (Frühjahr 2014, T2A1)

Wir rechnen im Restklassenring $\mathbb{Q}[X]/(q)$. Dort ist $X^2 \equiv 1 \pmod{q}$, d.h. es ist

$$p(X) = (X^2)^{250} - 2X \cdot (X^2)^{150} + 1 \equiv 1^{250} - 2X \cdot 1^{150} + 1 \equiv -2X + 2 \pmod{q}$$

und Rest der Division von $p(X)$ durch $q(X)$ ist also $-2X + 2$.

Aufgabe (Frühjahr 2012, T3A3)

Für welche $a, b \in \mathbb{Q}$ ist das Polynom $(X-1)^2$ ein Teiler von $f(X) := aX^{30} + bX^{15} + 1$?

Lösungsvorschlag zur Aufgabe (Frühjahr 2012, T3A3)

Wir beweisen folgende Behauptung:

$$aX^{30} + bX^{15} + 1 \equiv 0 \pmod{(X-1)^2} \Leftrightarrow a = 1 \text{ und } b = -2$$

„ \Leftarrow “: Rechnen wir modulo $X-1$, so ist $X \equiv 1 \pmod{(X-1)}$. Also auch $X^{15} - 1 \equiv 1 - 1 \equiv 0 \pmod{(X-1)}$. Daraus folgt

$$X^{30} - 2X^{15} + 1 = (X^{15} - 1)^2 \equiv 0 \pmod{(X-1)^2}.$$

„ \Rightarrow “: Setzen wir nun $f \equiv 0 \pmod{(X-1)^2}$ voraus, so hat f insbesondere eine Nullstelle bei 1, sodass

$$0 = f(1) = a + b + 1 \Leftrightarrow a + b = -1 \quad (\star)$$

Da 1 nach Voraussetzung jedoch sogar eine doppelte Nullstelle ist, muss für die formale Ableitung f' gelten:

$$0 = f'(1) = 30a + 15b = 15a + 15(a + b) \stackrel{(\star)}{=} 15a - 15 \Leftrightarrow a = 1.$$

Einsetzen in (\star) liefert dann $b = -2$.

Für Aufgaben im Stile der folgenden Aufgaben gibt es leider kein Vorgehen, das immer zielführend ist, sondern man muss jeweils die konkrete Form der vorgegebenen Gleichung ausnutzen. Meist ist es jedoch hilfreich, die Gleichung über einem Faktorring $\mathbb{Z}/n\mathbb{Z}$ zu betrachten. Man beachte in diesem Zusammenhang auch die im Abschnitt über Quadrate behandelten Methoden.

Aufgabe (Frühjahr 2015, T2A1)

Man bestimme alle Paare von Primzahlen p, q mit $p^2 - 2q^2 = 1$.

Lösungsvorschlag zur Aufgabe (Frühjahr 2015, T2A1)

Es ist

$$p^2 - 2q^2 = 1 \Leftrightarrow p^2 = 2q^2 + 1,$$

also ist p^2 ungerade und p muss ebenfalls ungerade sein, sodass $p \equiv 1 \pmod{4}$ oder $p \equiv 3 \pmod{4}$. In beiden Fällen folgt $p^2 \equiv 1 \pmod{4}$ und somit

$$2q^2 = p^2 - 1 \equiv 0 \pmod{4}.$$

Das bedeutet $4 \mid 2q^2$, sodass q^2 gerade sein muss. Also ist $q = 2$ und Einsetzen ergibt

$$p^2 = 2 \cdot 2^2 + 1 = 9 \Leftrightarrow p = 3.$$

Aufgabe (Herbst 2015, T3A1)

Seien $x, y, z \in \mathbb{Z}$ mit $x^2 + y^2 = z^2$. Zeigen Sie, dass das Produkt xyz durch 60 teilbar ist.

Lösungsvorschlag zur Aufgabe (Herbst 2015, T3A1)

Wir gehen schrittweise vor.

1. Schritt: $3 \mid xyz$

Modulo 3 gibt es die Quadrate

$$0 \equiv 0^2 \pmod{3} \quad \text{und} \quad 1 \equiv 1^2 \equiv 2^2 \pmod{3}.$$

Wegen $1+1 \not\equiv 1 \pmod{3}$ kann nicht $x \equiv y \equiv z \equiv 1 \pmod{3}$ sein und mindestens eines der x^2, y^2, z^2 muss durch 3 teilbar sein. Da 3 prim ist, ist bereits eines der x, y, z durch 3 teilbar.

2. Schritt: $5 \mid xyz$

Wie im ersten Schritt findet man mittels Ausprobieren, dass 0, 1 und -1 die Quadrate modulo 5 sind. Ist $x \not\equiv 0 \not\equiv y \pmod{5}$, so ist die einzige mögliche Kombination aus x^2 und y^2 , die ein Quadrat ergibt,

$$z^2 = x^2 + y^2 \equiv 1 - 1 \equiv 0 \pmod{5}.$$

Es folgt, dass mindestens eines der x^2, y^2, z^2 durch 5 teilbar ist, und, da 5 eine Primzahl ist, muss bereits eines der x, y, z durch 5 teilbar sein.

3. Schritt: $4 \mid xyz$

Da 4 keine Primzahl ist, kann daraus, dass 4 eines der Quadrate teilt, nicht gefolgert werden, dass 4 auch eine der Zahlen selbst teilt. Deshalb betrachten wir die Gleichung modulo 8. Hier gibt es die Quadrate 0, 1 und 4. Ist eines der x^2, y^2, z^2 kongruent zu 0 modulo 8, so tritt der Primteiler 2 in einer der drei Zahlen mindestens zweimal auf, d.h. xyz ist durch 4 teilbar. Ist keines der x^2, y^2, z^2 durch 8 teilbar, so handelt es sich um keine Lösung von

$$x^2 + y^2 = z^2:$$

$$1 + 1 = 2$$

ist kein Quadrat modulo 8,

$$1 + 4 = 5$$

ist kein Quadrat modulo 8,

$$4 + 4 \equiv 0 \pmod{8}$$

wurde bereits behandelt.

Insgesamt wurde also gezeigt, dass das Produkt xyz durch $3 \cdot 5 \cdot 4 = 60$ teilbar ist.

Aufgabe (Herbst 2015, T1A1)

Bestimmen Sie sämtliche Lösungen der Gleichung $x^6 - 2x + 4 = 0$ im Ring $\mathbb{Z}/64\mathbb{Z}$.

Hinweis Führen Sie eine Fallunterscheidung je nach Bild von x in $\mathbb{Z}/2\mathbb{Z}$ durch und beachten Sie, dass $64 = 2^6$.

Lösungsvorschlag zur Aufgabe (Herbst 2015, T1A1)

Sei $\alpha \in \mathbb{Z}$ eine Lösung von $x^6 - 2x + 4 \equiv 0 \pmod{64}$. Es ist dann $\alpha^6 \equiv 2\alpha - 4 \pmod{64}$, d. h. es gibt ein $l \in \mathbb{Z}$ mit

$$\alpha^6 = 2\alpha - 4 + 64l.$$

Insbesondere $2 \mid \alpha^6$ und da 2 prim ist, muss 2 bereits ein Teiler von α sein. Es gibt also ein $\beta \in \mathbb{Z}$ mit $\alpha = 2\beta$ und es folgt:

$$(2\beta)^6 - 2(2\beta) + 4 = 64\beta^6 - 4\beta + 4 \equiv -4(\beta - 1) \equiv 0 \pmod{64}$$

Es muss daher $\beta - 1$ ein Vielfaches von 16 sein. Sei daher $k \in \mathbb{Z}$, sodass

$$\beta - 1 = 16k \Leftrightarrow \alpha = 32k + 2.$$

In $\mathbb{Z}/64\mathbb{Z}$ erhalten wir die möglichen Lösungen $\bar{2}$ und $\bar{34}$. Tatsächlich gilt

$$\bar{2}^6 - \bar{2} \cdot \bar{2} + \bar{4} = \bar{4} - \bar{4} = 0,$$

$$\bar{34}^6 - \bar{2} \cdot \bar{34} + \bar{4} = \bar{4} - \bar{4} = 0.$$

Also handelt es sich bei $\bar{2}$ und $\bar{34}$ um sämtliche Lösungen der angegebenen Gleichung.

Anleitung: Erweiterter Euklidischer Algorithmus

Sei R ein euklidischer Ring mit Höhenfunktion $|\cdot|: R \setminus \{0\} \rightarrow \mathbb{N}$. Der *euklidische Algorithmus* ist ein Verfahren, mit dem der größte gemeinsame Teiler d zweier Elemente $a, b \in R$ sowie Elemente $x, y \in R$ mit $ax + by = d$ bestimmt werden können.

- (1) Starte mit den folgenden beiden Zeilen:

$$\begin{array}{r|ccc} 1 & - & a & 1 \\ 2 & - & b & 0 \end{array} \quad \begin{array}{c} 0 \\ 1 \end{array}$$

- (2) Dividiere nun in jedem Schritt a_k durch a_{k-1} mit Rest, d.h. finde r_k und q_k , sodass $a_k = q_k a_{k-1} + r_k$ und $|r_k| < |a_{k-1}|$ und führe die beiden Zeilen aus (1) gemäß dem folgenden Schema weiter:

$$\begin{array}{r|ccc} k-1 & q_{k-1} & a_{k-1} & x_{k-1} \\ k & q_k & a_k & x_k \\ k+1 & q_{k+1} & r_k & x_{k-1} - q_k x_k \end{array} \quad \begin{array}{r|cc} y_{k-1} \\ y_k \\ y_{k-1} - q_k y_k \end{array}$$

- (3) Die letzten beiden Zeilen werden folgendermaßen aussehen:

$$\begin{array}{r|ccccc} l-1 & q_{l-1} & a_{l-1} & x_{l-1} & y_{l-1} \\ l & q_l & 0 & - & - \end{array}$$

Setze dann $d = a_{l-1}$ sowie $x = x_{l-1}$ und $y = y_{l-1}$.

Eine unmittelbare Anwendung des Algorithmus ist die Berechnung von Inversen in Restklassenringen.

Anleitung: Berechnen von multiplikativen Inversen

Sei R ein euklidischer Ring, beispielsweise \mathbb{Z} oder $K[X]$ für einen Körper K , und $(p) \subseteq R$ ein Ideal. Wir berechnen das multiplikative Inverse von $q \in R$ in $R/(p)$.

(1) Bestimme mithilfe des euklidischen Algorithmus $x, y \in R$ mit

$$xp + yq = 1.$$

(2) Modulo (p) ergibt sich wegen $p = 0 + (p)$ dann

$$yq + (p) = 1 + (p) \Leftrightarrow (q + (p))^{-1} = y + (p).$$

An dieser Stelle schieben wir noch den allgegenwärtigen Homomorphiesatz ein, diesmal für Ringe:

Satz 2.11 (Homomorphiesatz). Sei $\varphi: R \rightarrow S$ ein Homomorphismus von Ringen und $\mathfrak{a} \subseteq R$ ein Ideal mit $\mathfrak{a} \subseteq \ker \varphi$. Dann gibt es einen eindeutigen Ringhomomorphismus $\bar{\varphi}: R/\mathfrak{a} \rightarrow S$, sodass das folgende Diagramm kommutiert:

$$\begin{array}{ccc} R & \xrightarrow{\varphi} & S \\ \pi \downarrow & \nearrow \bar{\varphi} & \\ R/\mathfrak{a} & & \end{array}$$

Der Homomorphismus $\bar{\varphi}$ ist dabei genau dann
 (1) injektiv, wenn $\mathfrak{a} = \ker \varphi$,
 (2) surjektiv, wenn φ surjektiv ist.

Insbesondere induziert φ einen Isomorphismus $R/\ker \varphi \cong \text{im } \varphi$.

Aufgabe (Frühjahr 2015, T1A4)

Sei J das von $X^3 - 7$ erzeugte Ideal in $\mathbb{Q}[X]$.

- a Beweisen Sie, dass $\mathbb{Q}[X]/J$ ein Körper ist, und bestimmen Sie den Grad der Körpererweiterung $\mathbb{Q}[X]/J \supseteq \mathbb{Q}$.
- b Bestimmen Sie ein Polynom $P \in \mathbb{Q}[X]$, für das $P + J$ multiplikatives Inverses von $(X^2 + 1) + J$ in $\mathbb{Q}[X]/J$ ist.

Lösungsvorschlag zur Aufgabe (Frühjahr 2015, T1A4)

- a Das Polynom $X^3 - 7$ ist irreduzibel nach dem Eisensteinkriterium mit $p = 7$ und damit ein Primelement, da $\mathbb{Q}[X]$ als Polynomring über einem Körper ein Hauptidealring ist. Folglich ist J ein Primideal. In einem Hauptidealring ist jedes Primideal bereits maximal (vgl. Aussage (5) auf Seite 90), sodass J ein maximales Ideal und $\mathbb{Q}[X]/J$ ein Körper ist.

Sei nun $\alpha \in \mathbb{C}$ eine Nullstelle von $X^3 - 7$. Wir zeigen im Folgenden mit dem Homomorphiesatz, dass $\mathbb{Q}/(J)$ isomorph zum Körper $\mathbb{Q}(\alpha)$ ist. Da $X^3 - 7$ normiert und irreduzibel über \mathbb{Q} ist, ist dann $X^3 - 7$ das Minimalpolynom von α über \mathbb{Q} , und die Erweiterung $\mathbb{Q}(\alpha)|\mathbb{Q}$ hat den Grad 3. Betrachte den Einsetzungshomomorphismus

$$\varphi: \mathbb{Q}[X] \rightarrow \mathbb{Q}(\alpha), \quad f \mapsto f(\alpha).$$

$$\begin{array}{ccc} \mathbb{Q}[X] & \xrightarrow{\varphi} & \mathbb{Q}(\alpha) \\ \downarrow & \nearrow \tilde{\varphi} & \\ \mathbb{Q}[X]/J & & \end{array}$$

Sei $f \in J$ vorgegeben, d.h. $f = g \cdot (X^3 - 7)$ für ein $g \in \mathbb{Q}[X]$. Da α Nullstelle von $X^3 - 7$ ist, ist dann auch $f(\alpha) = 0$, sodass $f \in \ker \varphi$. Ist umgekehrt $f \in \ker \varphi$, so gilt $f(\alpha) = 0$.

Nun ist $X^3 - 7$ das Minimalpolynom von α über \mathbb{Q} und muss daher f teilen, sodass $f \in J$. Insgesamt haben wir $\ker \varphi = J$.

Dass φ surjektiv ist, folgt daraus, dass $\mathbb{Q}(\alpha)$ eine \mathbb{Q} -Basis der Form $\{1, \alpha, \alpha^2\}$ hat und somit jedes Element $\beta \in \mathbb{Q}(\alpha)$ eine Darstellung der Form $\beta = a_0 + a_1\alpha + a_2\alpha^2 = f(\alpha)$ für $f = a_0 + a_1X + a_2X^2 \in \mathbb{Q}[X]$ besitzt.

Der Homomorphiesatz liefert nun $\mathbb{Q}[X]/J \cong \mathbb{Q}(\alpha)$ und der gesuchte Körpererweiterungsgrad ist der Grad des Minimalpolynoms von α über \mathbb{Q} , also 3.

- b** Das „Kochrezept“ hierzu wurde im Kasten auf Seite 103 dargestellt: Aus dem euklidischen Algorithmus bekommt man

$$(X - 7) \cdot (X^3 - 7) + (-X^2 + 7X + 1) \cdot (X^2 + 1) = 50$$

und modulo J erhält man daraus

$$(X^2 + 1) \cdot \frac{1}{50}(-X^2 + 7X + 1) + J = 1 + J.$$

Ein Polynom mit der gesuchten Eigenschaft ist also $\frac{1}{50}(-X^2 + 7X + 1)$.

Satz 2.12 (Korrespondenzsatz für Ringe). Sei R ein Ring, $\mathfrak{a} \subseteq R$ ein Ideal und $\pi: R \rightarrow R/\mathfrak{a}$ der kanonische Epimorphismus. Dann sind durch

$$\begin{array}{ccc} \{ \text{Ideale } \mathfrak{b} \text{ von } R \text{ mit } \mathfrak{a} \subseteq \mathfrak{b} \} & \xrightleftharpoons[\hspace{-1cm}]{} & \{ \text{Ideale } \bar{\mathfrak{b}} \text{ von } R/\mathfrak{a} \} \\ \mathfrak{b} & \longmapsto & \pi(\mathfrak{b}) \\ \pi^{-1}(\bar{\mathfrak{b}}) & \longleftarrow & \bar{\mathfrak{b}} \end{array}$$

zueinander inverse Bijektionen gegeben. Dabei werden Primideale auf Primideale abgebildet.

2.3. Chinesischer Restsatz und simultane Kongruenzen

Es gibt mehrere mathematische Aussagen unterschiedlicher Allgemeinheit, die als Chinesischer Restsatz bekannt sind. Wir formulieren zunächst die allgemeine Aussage und betrachten anschließend den wichtigen Spezialfall für die ganzen Zahlen.

Satz 2.13 (Chinesischer Restsatz). Sei R ein Ring und seien $\mathfrak{a}_1, \dots, \mathfrak{a}_n \subseteq R$ Ideale mit $\mathfrak{a}_i + \mathfrak{a}_j = R$ für $i, j \in \{1, \dots, n\}$ mit $i \neq j$. Dann ist die Abbildung

$$R / \bigcap_{i=1}^n \mathfrak{a}_i \longrightarrow R / \mathfrak{a}_1 \times \dots \times R / \mathfrak{a}_n,$$

$$a + \bigcap_{i=1}^n \mathfrak{a}_i \mapsto (a + \mathfrak{a}_1, \dots, a + \mathfrak{a}_n)$$

ein Isomorphismus von Ringen.

Zwei Ideale $\mathfrak{a}_1, \mathfrak{a}_2 \subseteq R$ für die die Bedingung $\mathfrak{a}_1 + \mathfrak{a}_2 = R$ aus dem Chinesischen Restsatz gilt, nennt man auch *relativ prim* oder *koprim* zueinander.

Aufgabe (Herbst 2014, T2A1)

Es sei R ein kommutativer Ring mit Eins. Ein Element $e \in R$ ist *idempotent* genau dann, wenn $e^2 = e$ ist (zum Beispiel sind 0 und 1 idempotent). Zeigen Sie:

- a Wenn e idempotent ist, dann ist auch $1 - e$ idempotent, und $e \cdot (1 - e) = 0$.
- b Ist e idempotent, dann sind die Ideale eR und $(1 - e)R$ relativ prim.
- c Genau dann ist R isomorph zu einem direkten Produkt von zwei Ringen, die beide keine Nullringe sind, wenn es in R ein idempotentes Element $e \notin \{0, 1\}$ gibt.

Lösungsvorschlag zur Aufgabe (Herbst 2014, T2A1)

- a Man berechnet:

$$\begin{aligned}(1 - e)^2 &= 1^2 - 2 \cdot 1 \cdot e + e^2 = 1 - 2e + e = 1 - e \\ e \cdot (1 - e) &= e - e^2 = e - e = 0\end{aligned}$$

- b Es ist $1 = e + (1 - e) \in eR + (1 - e)R$, also ist $eR + (1 - e)R = R$, was gerade bedeutet, dass die Ideale eR und $(1 - e)R$ relativ prim zueinander sind.

c „ \Leftarrow “: Unter Verwendung von **a** ist

$$eR \cdot (1 - e)R = e(1 - e)R = (0).$$

Nach Teil **b** sind die Ideale eR und $(1 - e)R$ koprimit zueinander, sodass wir den Chinesischen Restsatz anwenden können:

$$R \cong R/(0) = R/eR \cdot (1 - e)R \cong R/eR \times R/(1 - e)R$$

Angenommen, es ist $R/eR = \{0\}$, dann müsste $eR = R$ sein. Insbesondere gäbe es ein $r \in R$ mit $er = 1$, also wäre e eine Einheit und könnte gekürzt werden, sodass aus der Gleichung $e^2 = e$ dann $e = 1$ folgt. Dies steht aber im Widerspruch zu $e \neq 1$.

Genauso zeigt man, dass die Annahme $R/(1 - e)R = \{0\}$ auf den Widerspruch $e = 0$ führt.

„ \Rightarrow “: Setzen wir nun umgekehrt voraus, dass es Ringe $A, B \neq 0$ und einen Isomorphismus

$$\varphi: R \rightarrow A \times B$$

gibt. Setze $e = \varphi^{-1}(1, 0)$, dann gilt

$$e^2 = (\varphi^{-1}(1, 0))^2 = \varphi^{-1}(1^2, 0^2) = \varphi^{-1}(1, 0) = e,$$

also ist e idempotent. Da φ^{-1} bijektiv ist, ist außerdem

$$0 = \varphi^{-1}(0, 0) \neq \varphi^{-1}(1, 0) = e$$

$$1 = \varphi^{-1}(1, 1) \neq \varphi^{-1}(1, 0) = e,$$

wobei in der zweiten Zeile verwendet wurde, dass $(1, 1)$ das Einselement in $A \times B$ ist und deshalb $\varphi^{-1}(1, 1) = 1$ gelten muss.

Aufgabe (Herbst 2013, T1A4)

Wir betrachten den Ring $R = \mathbb{Q}[X]/(X^{10} - 1)$.

a Bestimmen Sie ein kartesisches Produkt von Körpern, das zu R isomorph ist.

Hinweis Der chinesische Restsatz kann hilfreich sein.

b Wie viele Ideale besitzt R ?

Lösungsvorschlag zur Aufgabe (Herbst 2013, T1A4)

- a** Sei Φ_n jeweils das n -te Kreisteilungspolynom, dann gilt laut Satz 3.17 (2)

$$X^{10} - 1 = \prod_{d|10} \Phi_d = \Phi_1 \cdot \Phi_2 \cdot \Phi_5 \cdot \Phi_{10}.$$

Da die Kreisteilungspolynome irreduzibel (und damit insbesondere teilerfremd) sind, erhalten wir aus dem Chinesischen Restsatz

$$\begin{aligned} R &= \mathbb{Q}[X]/(X^{10} - 1) = \mathbb{Q}[X]/(\Phi_1 \cdot \Phi_2 \cdot \Phi_5 \cdot \Phi_{10}) \cong \\ &\cong \mathbb{Q}[X]/(\Phi_1) \times \mathbb{Q}[X]/(\Phi_2) \times \mathbb{Q}[X]/(\Phi_5) \times \mathbb{Q}[X]/(\Phi_{10}). \end{aligned}$$

Dies ist ein Produkt von Körpern, da die Kreisteilungspolynome über \mathbb{Q} wie bereits erwähnt irreduzibel sind, sodass der Aufgabenstellung eigentlich bereits Genüge getan ist. Mithilfe des Einsetzungshomomorphismus $X \mapsto \xi_n$ für eine primitive n -te Einheitswurzel folgt noch

$$R \cong \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q}(\xi_5) \times \mathbb{Q}(\xi_{10}).$$

- b** Wir behandeln die Fragestellung in etwas größerer Allgemeinheit. Sei $R = \prod_{i=1}^n K_i$ ein Produkt von Körpern K_i . Betrachte für $i \in \{1, \dots, n\}$ die Abbildung

$$\pi_i: R \rightarrow K_i, \quad (a_1, \dots, a_n) \mapsto a_i,$$

welche offensichtlich ein Epimorphismus ist. Ist nun $\mathfrak{a} \subseteq R$ ein Ideal, so ist deshalb auch $\pi_i(\mathfrak{a}) \subseteq K_i$ ein Ideal. Weiter haben wir

$$\mathfrak{a} = \pi_1(\mathfrak{a}) \times \dots \times \pi_n(\mathfrak{a}). \quad (*)$$

Die Körper K_i besitzen jeweils nur die Ideale (0) und K_i ; Ist nämlich $I \subseteq K_i$ ein Ideal und $r \in I$ mit $r \neq 0$, so gilt auch $r^{-1}r = 1 \in I$, also ist $I = K_i$. Somit kann man an $(*)$ ablesen, dass R genau 2^n Ideale besitzt. In unserem Fall sind das nach Teil **a** also $2^4 = 16$ Ideale.

Da es sich bei \mathbb{Z} um einen Hauptidealring handelt, lässt sich im Spezialfall $R = \mathbb{Z}$ die Voraussetzung des Chinesischen Restsatzes als

$$(a) + (b) = \mathbb{Z} \Leftrightarrow \text{ggT}(a, b) = 1$$

umformulieren. Sind nämlich a und b zwei teilerfremde ganze Zahlen, so gibt es nach dem *Lemma von Bézout* Zahlen $x, y \in \mathbb{Z}$, sodass

$$ax + by = 1 \quad (*)$$

und folglich $(a) + (b) = (1)$. Umgekehrt folgt auch aus $1 \in (a) + (b)$ die Existenz einer Gleichung (\star) . Ein gemeinsamer Teiler von a, b muss daher auch ein Teiler von 1 sein, weswegen $\text{ggT}(a, b) = 1$ sein muss.

Zusammenfassend gilt für \mathbb{Z} der Chinesische Restsatz in der folgenden Formulierung:¹

Satz 2.14 (Chinesischer Restsatz für \mathbb{Z}). Seien $n_1, \dots, n_k \in \mathbb{Z}$ paarweise teilerfremd. Setze $n = \prod_{i=1}^k n_i$, dann ist die Abbildung

$$\mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/n_1\mathbb{Z} \times \dots \times \mathbb{Z}/n_k\mathbb{Z}, \quad a + n\mathbb{Z} \mapsto (a + n_1\mathbb{Z}, \dots, a + n_k\mathbb{Z})$$

ein Isomorphismus.

Der Chinesische Restsatz lässt sich nun auf Systeme simultaner Kongruenzen anwenden, d. h. auf Systeme der Form

$$a \equiv a_1 \pmod{n_1}$$

⋮

$$a \equiv a_k \pmod{n_k}$$

mit $a_i, n_i \in \mathbb{Z}$ für $1 \leq i \leq k$ und ein $k \in \mathbb{N}$. Sind die n_i paarweise teilerfremd, so gehört nach dem Chinesischen Restsatz zu dem Element

$$(a_1, \dots, a_k) \in \mathbb{Z}/n_1\mathbb{Z} \times \dots \times \mathbb{Z}/n_k\mathbb{Z}$$

genau ein Urbild in $\mathbb{Z}/(\prod_{i=1}^k n_i)\mathbb{Z}$, also eine bis auf Vielfache von $\prod_{i=1}^k n_i$ eindeutige Lösung des Systems von Kongruenzen.

Zu erwähnen bleibt noch der Fall, dass die n_i nicht paarweise teilerfremd sind, denn in diesem Fall kann der Chinesische Restsatz nicht ohne Weiteres angewendet werden. Jedoch können die n_i selbst in teilerfremde Faktoren $p_{ij}^{v_{ij}}$ zerlegt werden. Auf diese Weise kann eine Kongruenz mod n_i mithilfe des Chinesischen Restsatzes in Kongruenzen mod $p_{ij}^{v_{ij}}$ zerlegt werden. Tritt nun einer dieser Faktoren in mehreren n_i auf, so können die zugehörigen Kongruenzen auf Widerspruchsfreiheit geprüft werden. Sind die Kongruenzen konsistent, so sollte man nur diejenige für die höchste auftretende Potenz des jeweiligen Faktors beibehalten.

Beispiele 2.15. **a** Das System

$$a \equiv 0 \pmod{9}$$

$$a \equiv 1 \pmod{15}$$

¹ Der Satz ist außerdem gültig, wenn man \mathbb{Z} durch einen Polynomring $K[X]$ und die teilerfremden Zahlen durch teilerfremde Polynome ersetzt.

ist äquivalent zum System

$$a \equiv 0 \pmod{9}$$

$$a \equiv 1 \pmod{3}$$

$$a \equiv 1 \pmod{5}$$

und kann daher keine Lösung haben, denn aus der ersten Kongruenz folgt insbesondere $3 | a$, d.h. $a \equiv 0 \pmod{3}$.

b Das System

$$a \equiv 0 \pmod{9}$$

$$a \equiv 0 \pmod{15}$$

ist äquivalent zum System

$$a \equiv 0 \pmod{9}$$

$$a \equiv 0 \pmod{3}$$

$$a \equiv 0 \pmod{5}$$

und, da aus $9 | a$ insbesondere $3 | a$ folgt, ist die zweite Kongruenz redundant. ■

Wir sehen uns nun zwei verschiedene Methoden an, solche Systeme von Kongruenzen zu lösen.

Anleitung: Lösen simultaner Kongruenzen I

Gegeben sei ein System $a \equiv a_i \pmod{n_i}$ für $i \in \{1, \dots, l\}$.

- (1) Stelle sicher, dass die n_i teilerfremd sind.
- (2) Löse zunächst die ersten beiden Kongruenzen: Da n_1 und n_2 teilerfremd sind, gibt es $x, y \in \mathbb{Z}$, sodass

$$xn_1 + yn_2 = 1. \quad (*)$$

Diese Zahlen x und y können mithilfe des erweiterten euklidischen Algorithmus (Seite 103) bestimmt werden. Sei nun

$$\phi: \mathbb{Z}/n_1 n_2 \mathbb{Z} \rightarrow \mathbb{Z}/n_1 \mathbb{Z} \times \mathbb{Z}/n_2 \mathbb{Z}, \quad \bar{a} \mapsto (\bar{a}_1, \bar{a}_2)$$

der Isomorphismus aus dem Chinesischen Restsatz. Aus $(*)$ folgt

$$\phi(\overline{xn_1}) = (\bar{0}, \bar{1}) \quad \phi(\overline{yn_2}) = (\bar{1}, \bar{0}),$$

also ist

$$\phi(\overline{a_1 yn_2 + a_2 xn_1}) = \bar{a}_1 \cdot \phi(\overline{yn_2}) + \bar{a}_2 \cdot \phi(\overline{xn_1}) = (\bar{a}_1, \bar{a}_2).$$

Setze $z_2 = a_1 yn_2 + a_2 xn_1$.

- (3) Gehe nun induktiv vor: Eine Lösung z_{m-1} der ersten $m - 1$ Kongruenzen sei bereits konstruiert. Setze $M = \prod_{i=1}^{m-1} n_i$, dann sind M und n_m teilerfremd und eine Lösung z_m des Systems

$$z_m \equiv z_{m-1} \pmod{M} \quad \text{und} \quad z_m \equiv a_m \pmod{n_m}$$

kann wie in (2) bestimmt werden. Da $n_i \mid M$ für $i \in \{1, \dots, m-1\}$, ist dann $z_m \equiv z_{m-1} \equiv a_i \pmod{n_i}$. Insgesamt ist damit z_m eine Lösung der ersten m Kongruenzen.

- (4) Probe: Überprüfe, dass $a = z_l$ eine Lösung des ursprünglichen Systems ist.

Aufgabe (Frühjahr 2011, T2A1)

Bestimmen Sie alle ganzzahligen Lösungen des folgenden Systems:

$$\begin{aligned}x &\equiv 1 \pmod{2} \\x &\equiv 2 \pmod{3} \\x &\equiv 3 \pmod{5}\end{aligned}$$

Lösungsvorschlag zur Aufgabe (Frühjahr 2011, T2A1)

Wir lösen zunächst die ersten beiden Kongruenzen: Sei $\phi: \mathbb{Z}/6\mathbb{Z} \rightarrow \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ der Isomorphismus aus dem Chinesischen Restsatz. Aus der Gleichung

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

folgt

$$\phi(-\bar{2}) = (-\bar{2}, \bar{1} - \bar{3}) = (\bar{0}, \bar{1}) \quad \text{und} \quad \phi(\bar{3}) = (\bar{1} + \bar{2}, \bar{3}) = (\bar{1}, \bar{0}).$$

Daraus erhält man, dass

$$\phi(-\bar{1}) = \phi(\bar{1} \cdot \bar{3} + \bar{2} \cdot (-\bar{2})) = (\bar{1}, \bar{0}) + \bar{2} \cdot (\bar{0}, \bar{1}) = (\bar{1}, \bar{2}).$$

Also ist -1 eine Lösung der ersten beiden Kongruenzen. Betrachte nun das System

$$\begin{aligned}x &\equiv -1 \pmod{6}, \\x &\equiv 3 \pmod{5}.\end{aligned}$$

Ist $\psi: \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \rightarrow \mathbb{Z}/30\mathbb{Z}$ der Isomorphismus aus dem Chinesischen Restsatz, so folgt aus

$$1 \cdot 6 + (-1) \cdot 5 = 1,$$

dass $\psi(\bar{6}) = (\bar{0}, \bar{1})$ und $\psi(-\bar{5}) = (\bar{1}, \bar{0})$. Daraus erhält man, dass

$$\phi(\bar{2}\bar{3}) = \phi(-\bar{1} \cdot (-\bar{5}) + \bar{3} \cdot \bar{6}) = -(\bar{1}, \bar{0}) + \bar{3} \cdot (\bar{0}, \bar{1}) = (-\bar{1}, \bar{3}).$$

Also ist 23 eine Lösung des neuen Systems von Kongruenzen und man überprüft unmittelbar, dass 23 auch eine Lösung des ursprünglichen Systems aus der Aufgabenstellung ist. Diese Lösung ist eindeutig modulo $2 \cdot 3 \cdot 5$, d. h. die Menge aller ganzzahligen Lösungen ist durch $23 + 30\mathbb{Z}$ gegeben.

Aufgabe (Herbst 2014, T1A5)

Bestimmen Sie die kleinste natürliche Zahl, die bei Division durch n den Rest $n - 1$ hat, für alle $n \in \{2, 3, 4, 5, 6\}$.

Lösungsvorschlag zur Aufgabe (Herbst 2014, T1A5)

Die Aufgabenstellung lässt sich auch so formulieren, dass das System

$$\begin{aligned} a &\equiv 1 \pmod{2} \\ a &\equiv 2 \pmod{3} \\ a &\equiv 3 \pmod{4} \\ a &\equiv 4 \pmod{5} \\ a &\equiv 5 \pmod{6} \end{aligned}$$

gelöst werden soll. Diese Kongruenzen sind jedoch nicht unabhängig voneinander, denn beispielsweise gilt laut dem Chinesischen Restsatz, dass

$$a \equiv 5 \pmod{2 \cdot 3} \Leftrightarrow a \equiv 5 \equiv 1 \pmod{2} \quad \text{und} \quad a \equiv 5 \equiv 2 \pmod{3},$$

wobei die rechten beiden Kongruenzen gerade den ersten beiden Zeilen des Systems entsprechen. Außerdem folgt aus $4 \mid (a - 3)$ insbesondere, dass $2 \mid (a - 3)$, d. h.

$$a \equiv 3 \pmod{4} \Rightarrow a \equiv 3 \equiv 1 \pmod{2}$$

Es genügt also, das überschaubarere System

$$a \equiv 2 \pmod{3}$$

$$a \equiv 3 \pmod{4}$$

$$a \equiv 4 \pmod{5}$$

zu lösen. Sei $\phi: \mathbb{Z}/12\mathbb{Z} \rightarrow \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ der Isomorphismus aus dem Chinesischen Restsatz. Aus der Gleichung

$$(-1) \cdot 3 + 1 \cdot 4 = 1$$

folgt, dass $\phi(-\bar{3}) = (\bar{0}, \bar{1})$ und $\phi(\bar{4}) = (\bar{1}, \bar{0})$. In der Konsequenz also auch

$$\phi(-\bar{1}) = \phi(\bar{2} \cdot \bar{4} + \bar{3} \cdot (-\bar{3})) = (\bar{2}, \bar{3}).$$

Also ist -1 eine Lösung der ersten beiden Kongruenzen. Als nächstes lösen wir das System

$$a \equiv -1 \pmod{12},$$

$$a \equiv 4 \pmod{5}.$$

Sei dazu $\psi: \mathbb{Z}/60\mathbb{Z} \rightarrow \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ der Isomorphismus aus dem Chinesischen Restsatz. Aus der Gleichung

$$(-2) \cdot 12 + 5 \cdot 5 = 1$$

folgt, dass $\psi(\bar{25}) = (\bar{1}, \bar{0})$ und $\psi(-\bar{24}) = (\bar{0}, \bar{1})$. Folglich ist auch

$$\psi(-\bar{1}) = \psi(-\bar{121}) = \psi(-\bar{25} + \bar{4} \cdot (-\bar{24})) = (-\bar{1}, \bar{4}).$$

Man überprüft unmittelbar, dass -1 eine Lösung der ursprünglichen Kongruenz ist und somit $-1 + 60\mathbb{Z}$ die Menge aller Lösungen ist. Die kleinste natürliche Zahl in dieser Menge ist 59.

Anleitung: Lösen simultaner Kongruenzen II

Gegeben sei ein System $a \equiv a_i \pmod{n_i}$ für $i \in \{1, \dots, l\}$.

- (1) Stelle sicher, dass die n_i paarweise teilerfremd sind.
- (2) Setze $n'_i = \prod_{j \neq i} n_j$.
- (3) Berechne für jedes n'_i ein Inverses m_i modulo n_i , d.h. ein Element m_i mit $n'_i \cdot m_i \equiv 1 \pmod{n_i}$ (z.B. mit dem Verfahren auf Seite 103).
- (4) Setze $a = \sum_{i=1}^l a_i n'_i m_i$ und überprüfe, dass a tatsächlich eine Lösung des Systems ist.

Die explizite Umkehrabbildung zum Isomorphismus aus dem Chinesischen Restsatz ist dann

$$\mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_l\mathbb{Z} \longrightarrow \mathbb{Z}/\prod_{i=1}^l n_i\mathbb{Z}, \quad (\bar{a}_1, \dots, \bar{a}_l) \mapsto \sum_{i=1}^l \bar{a}_i n'_i m_i$$

Aufgabe (Herbst 2012, T1A5)

- a** Die Anzahl der Tänzer in einem Ballsaal liegt zwischen 100 und 200. Stellt man sie in 11-er Reihen auf, so bleibt ein Tänzer allein. Stellt man sie dagegen in 5-er Reihen auf, so bleiben drei übrig. Und stellt man sie in 3-er Reihen auf, so bleiben zwei Tänzer allein. Wieviele Tänzer sind es genau?
- b** Geben Sie explizit einen Ring-Isomorphismus

$$\varphi: \mathbb{Z}/57\mathbb{Z} \rightarrow \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/19\mathbb{Z}$$

und seine Umkehrung φ^{-1} an.

Lösungsvorschlag zur Aufgabe (Herbst 2012, T1A5)

- a** Zu lösen ist das System

$$\begin{aligned} a &\equiv 1 \pmod{11} \\ a &\equiv 3 \pmod{5} \\ a &\equiv 2 \pmod{3}. \end{aligned}$$

Wir verwenden das neue Verfahren und berechnen zunächst die n'_i :

$$n'_1 = 15 \quad n'_2 = 33 \quad n'_3 = 55$$

Als Nächstes bestimmen wir die m_i :

$$\begin{aligned} 15 \cdot 3 &\equiv 4 \cdot 3 = 12 \equiv 1 \pmod{11} & \Rightarrow m_1 &= 3 \\ 33 \cdot 2 &\equiv 3 \cdot 2 \equiv 1 \pmod{5} & \Rightarrow m_2 &= 2 \\ 55 &\equiv 1 \pmod{3} & \Rightarrow m_3 &= 1 \end{aligned}$$

Also setzen wir

$$a = 1 \cdot 15 \cdot 3 + 3 \cdot 33 \cdot 2 + 2 \cdot 55 \cdot 1 = 353.$$

Diese Lösung ist eindeutig modulo $3 \cdot 5 \cdot 11 = 165$, also ist $353 - 165 = 188$ die gesuchte Lösung im Bereich zwischen 100 und 200 und entspricht der Zahl der Tänzer.

b Der gefragte Ringisomorphismus ist

$$\varphi: \mathbb{Z}/57\mathbb{Z} \rightarrow \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/19\mathbb{Z}, \quad x + 57\mathbb{Z} \mapsto (x + 3\mathbb{Z}, x + 19\mathbb{Z}).$$

Zur Konstruktion von φ^{-1} gehen wir wie oben vor. Hier ist $n'_1 = 19$ und $n'_2 = 3$. Weiter ist $m_1 = 1$ und $m_2 = 13$, denn

$$19 \equiv 1 \pmod{3} \quad \text{und} \quad 3 \cdot 13 = 39 \equiv 1 \pmod{19}.$$

Also ist

$$\varphi^{-1}: \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/19\mathbb{Z} \rightarrow \mathbb{Z}/57\mathbb{Z}, \quad (x + 3\mathbb{Z}, y + 19\mathbb{Z}) \mapsto 19x + 39y + 57\mathbb{Z}$$

ein Kandidat für die Umkehrabbildung. Zum Test:

$$\begin{aligned} (\varphi \circ \varphi^{-1})(x + 3\mathbb{Z}, y + 19\mathbb{Z}) &= \varphi(19x + 39y + 57\mathbb{Z}) = \\ &= (19x + 3\mathbb{Z}, 39y + 19\mathbb{Z}) = (x + 3\mathbb{Z}, y + 19\mathbb{Z}) \\ (\varphi^{-1} \circ \varphi)(z + 57\mathbb{Z}) &= \varphi^{-1}(z + 3\mathbb{Z}, z + 19\mathbb{Z}) = (19z + 39z + 57\mathbb{Z}) = \\ &= (58z + 57\mathbb{Z}) = (z + 57\mathbb{Z}) \end{aligned}$$

Aufgabe (Frühjahr 2005, T3A3)

Geben Sie explizit einen Ring-Isomorphismus

$$\varphi: \mathbb{Z}/1000\mathbb{Z} \longrightarrow \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/125\mathbb{Z}$$

und seine Umkehrung φ^{-1} an.

Lösungsvorschlag zur Aufgabe (Frühjahr 2005, T3A3)

Der gefragte Isomorphismus ist der Homomorphismus aus dem Chinesischen Restsatz:

$$\varphi: \mathbb{Z}/1000\mathbb{Z} \longrightarrow \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/125\mathbb{Z}, \quad a + 1000\mathbb{Z} \mapsto (a + 8\mathbb{Z}, a + 125\mathbb{Z})$$

Zur Bestimmung der Umkehrabbildung:

$$\begin{aligned} n'_1 &= 125 & n'_2 &= 8 \\ 125 \cdot 5 &= 25^2 \equiv 1^2 \equiv 1 \pmod{8} & \Rightarrow & m_1 = 5 \\ 8 \cdot 47 &= 376 \equiv 1 \pmod{125} & \Rightarrow & m_2 = 47 \end{aligned}$$

Also bekommen wir als Kandidat für die inverse Abbildung

$$\begin{aligned} \varphi^{-1}: \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/125\mathbb{Z} &\rightarrow \mathbb{Z}/1000\mathbb{Z}, \\ (a_1 + 8\mathbb{Z}, a_2 + 125\mathbb{Z}) &\mapsto 625a_1 + 376a_2 + 1000\mathbb{Z} \end{aligned}$$

und man überprüft, dass tatsächlich $\varphi \circ \varphi^{-1} = \text{id}$ sowie $\varphi^{-1} \circ \varphi = \text{id}$ gilt.

Aufgabe (Herbst 2001, T2A2)

Betrachtet sei folgendes System von zwei Kongruenzen in $\mathbb{Q}[X]$:

$$\begin{aligned} f &\equiv X - 1 \pmod{X^2 - 1} \\ f &\equiv X + 1 \pmod{X^2 + X + 1}. \end{aligned}$$

Bestimmen Sie eine konkrete Lösung und die Menge aller Lösungen des Systems.

Lösungsvorschlag zur Aufgabe (Herbst 2001, T2A2)

Wir bemerken zunächst, dass die Polynome $X^2 - 1$ und $X^2 + X + 1$ teilerfremd sind, denn die Zerlegung von $X^2 - 1$ in irreduzible Faktoren ist

$$X^2 - 1 = (X - 1)(X + 1)$$

und, da $X^2 + X + 1$ keine Nullstelle bei ± 1 hat, kann keiner dieser Faktoren ein Teiler sein. Wir können also wie gewohnt mit dem Chinesischen Restsatz arbeiten.

Hier ist $n'_1 = X^2 + X + 1$ und $n'_2 = X^2 - 1$.

Aus dem euklidischen Algorithmus erhält man

$$1 = \frac{1}{3}(X-1)(X^2-1) - \frac{1}{3}(X-2)(X^2+X+1),$$

also ist $m_1 = -\frac{1}{3}(X-2)$ und $m_2 = \frac{1}{3}(X-1)$. Damit erhalten wir als konkrete Lösung

$$\begin{aligned} f &= (X-1)(X^2+X+1)\left(-\frac{1}{3}\right)(X-2) + (X+1)(X^2-1)\frac{1}{3}(X-1) = \\ &= \frac{1}{3}(2X^3 - 2X^2 + X - 1) \end{aligned}$$

und die Lösungsmenge des Systems ist $f + \mathfrak{a}$ mit dem Ideal

$$\mathfrak{a} = (X^2-1) \cap (X^2+X+1) = (X^2-1) \cdot (X^2+X+1) = (X^4 + X^3 - X - 1).$$

Aufgabe (Frühjahr 2012, T1A4)

Gegeben ist das Polynom $P = X^2 + 3 \cdot X + 1 \in \mathbb{Z}[X]$. Bestimmen Sie

- a** die Nullstellen von P modulo 5,
- b** die Nullstellen von P modulo 11,
- c** die Nullstellen von P modulo 11^2 ,
- d** die Nullstellen von P modulo 605.

Lösungsvorschlag zur Aufgabe (Frühjahr 2012, T1A4)

- a** Hier kann man einfach durchprobieren:

$$\begin{aligned} 0^2 + 3 \cdot 0 + 1 &\equiv 1 \pmod{5} \\ 1^2 + 3 \cdot 1 + 1 &= 5 \equiv 0 \pmod{5} \\ 2^2 + 3 \cdot 2 + 1 &= 11 \equiv 1 \pmod{5} \\ 3^2 + 3 \cdot 3 + 1 &= 19 \equiv 4 \pmod{5} \\ 4^2 + 3 \cdot 4 + 1 &\equiv (-1)^2 + 3 \cdot (-1) + 1 = -1 \equiv 4 \pmod{5} \end{aligned}$$

Also ist 1 die einzige Nullstelle von P modulo 5.

- b** Auch hier probiert man durch und sieht, dass 2 und 6 die Nullstellen von P modulo 11 sind.
- c** Ist a eine Nullstelle modulo 11^2 , so ist a insbesondere Nullstelle modulo 11. Das bedeutet unter Verwendung von Teil **b**:

$$a = 2 + k \cdot 11 \quad \text{oder} \quad a = 6 + k \cdot 11$$

für ein $k \in \mathbb{Z}$. Da es genügt, a modulo 11^2 eindeutig zu bestimmen, können wir $0 \leq k \leq 10$ annehmen. Einsetzen liefert nun

$$\begin{aligned} P(2 + 11k) &= (2 + 11k)^2 + 3 \cdot (2 + 11k) + 1 = 4 + 44k + 121k^2 + 6 + 33k + 1 \\ &= 121k^2 + 77k + 11 \equiv 77k + 11 \equiv 11(7k + 1) \pmod{11^2}. \end{aligned}$$

Weiterhin ist nun

$$11(7k + 1) \equiv 0 \pmod{11^2} \Leftrightarrow 7k + 1 \equiv 0 \pmod{11}.$$

Durch Testen der Werte $0 \leq k \leq 10$ überzeugt man sich schnell davon, dass die einzige Lösung dieser Gleichung $k = 3$ ist und zu $a = 2 + 3 \cdot 11 = 35$ führt. Ebenso verfährt man im zweiten Fall:

$$\begin{aligned} P(6 + k \cdot 11) &= (6 + 11k)^2 + 3 \cdot (6 + 11k) + 1 \\ &= 36 + 132k + 121k^2 + 18 + 33k + 1 = 121k^2 + 165k + 55 \\ &\equiv 165k + 55 = 11 \cdot (15k + 5) \pmod{11^2} \end{aligned}$$

Und betrachtet wiederum

$$\begin{aligned} 11 \cdot (15k + 5) \equiv 0 \pmod{11^2} &\Leftrightarrow 15k + 5 \equiv 0 \pmod{11} \\ &\Leftrightarrow 3k + 1 \equiv 0 \pmod{11}. \end{aligned}$$

Die einzige Lösungen dieser Gleichung im relevanten Bereich ist $k = 7$ mit der zugehörigen Nullstelle $a = 83$.

Insgesamt haben wir modulo 11^2 die Nullstellen 35 und 83 gefunden.

d Nach dem Chinesischen Restsatz haben wir den Isomorphismus

$$\varphi: \mathbb{Z}/605\mathbb{Z} \rightarrow \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/11^2\mathbb{Z}, \quad a + 605\mathbb{Z} \mapsto (a + 5\mathbb{Z}, a + 11^2\mathbb{Z}).$$

Da $\bar{a} \in \mathbb{Z}/605\mathbb{Z}$ genau dann eine Nullstelle von P ist, wenn $\varphi(\bar{a})$ eine Nullstelle von P in $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/11^2\mathbb{Z}$ ist, genügt es also nach Teil **a** und **c**, die Urbilder von (1, 35) und (1, 83) unter φ zu konstruieren.

Wir befolgen nun das Kochrezept von Seite 110. Es gilt

$$(-24) \cdot 5 + 121 = 1$$

und somit $\varphi(121) = (1, 0)$ und $\varphi(-120) = (0, 1)$. Damit erhalten wir

$$(1, 35) = \varphi(121 - 35 \cdot 120) = \varphi(-4079) = \varphi(156),$$

$$(1, 83) = \varphi(121 - 83 \cdot 120) = \varphi(-9839) = \varphi(446).$$

Damit sind die Nullstellen von P modulo 605 durch 156 und 446 gegeben.

Aufgabe (Herbst 2012, T3A4)

Wie viele Lösungen hat die Gleichung

$$X^2 + 46X + 1 \equiv 0$$

in $\mathbb{Z}/2012\mathbb{Z}$?

Hinweis 503 ist eine Primzahl.

Lösungsvorschlag zur Aufgabe (Herbst 2012, T3A4)

Nach dem Chinesischen Restsatz gibt es einen Isomorphismus

$$\mathbb{Z}/2012\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/503\mathbb{Z},$$

sodass sich die Lösungen der Gleichung in $\mathbb{Z}/2012\mathbb{Z}$ als Kombinationen der Lösungen in $\mathbb{Z}/4\mathbb{Z}$ bzw. $\mathbb{Z}/503\mathbb{Z}$ ergeben. In $\mathbb{Z}/4\mathbb{Z}$ gilt

$$X^2 + 46X + 1 \equiv 0 \pmod{4} \Leftrightarrow X^2 + 2X + 1 \equiv 0 \pmod{4}.$$

Durch Ausprobieren² findet man die Lösungen 1 und -1 . Betrachten wir nun die Gleichung über $\mathbb{Z}/503\mathbb{Z}$:

$$\begin{aligned} X^2 + 46X + 1 \equiv 0 \pmod{503} &\Leftrightarrow (X + 23)^2 - 23^2 + 1 \equiv 0 \pmod{503} \\ &\Leftrightarrow (X + 23)^2 \equiv 528 \equiv 25 \pmod{503} \end{aligned}$$

Da 503 laut Angabe eine Primzahl ist, handelt es sich bei $\mathbb{Z}/503\mathbb{Z}$ um einen Körper. In einem Körper kann ein Element a höchstens zwei Wurzeln haben, denn das Polynom $X^2 - a$ hat höchstens zwei Nullstellen. Also dürfen wir aus obiger Kongruenz tatsächlich

$$X + 23 \equiv \pm 5 \pmod{503}$$

schließen. Damit hat $X^2 + 46X + 1$ die Nullstellen

$$\{(1, -18), (-1, -18), (1, -28), (-1, -28)\} \subseteq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/503\mathbb{Z} \cong \mathbb{Z}/2012\mathbb{Z},$$

d. h. vier an der Zahl.

² Man wäre an dieser Stelle vielleicht versucht, $X^2 + 2X + 1 = (X + 1)^2$ zu schreiben und daraus zu schließen, dass -1 einzige (doppelte) Nullstelle ist. Allerdings ist $\mathbb{Z}/4\mathbb{Z}$ nicht nullteilerfrei und Einsetzen von 1 liefert $2 \cdot 2 = 4 \equiv 0 \pmod{4}$, also ebenfalls eine Lösung.

2.4. Quadrate und Legendre-Symbol

Sei p eine Primzahl und $q = p^n$ für ein $n \in \mathbb{N}$. Wir interessieren uns dafür, wie viele Quadrate es in der Einheitengruppe \mathbb{F}_q^\times gibt, d.h. Elemente der Form a^2 für ein $a \in \mathbb{F}_q$. Um diese Frage zu beantworten, betrachten wir den Homomorphismus

$$\tau : \mathbb{F}_q^\times \rightarrow \mathbb{F}_q^\times, \quad a \mapsto a^2,$$

dessen Bild genau die Menge der Quadrate ist, welche wir fortan als \mathcal{Q} bezeichnen. Nach dem Homomorphiesatz gilt $\mathcal{Q} = \text{im } \tau \cong \mathbb{F}_q^\times / \ker \tau$.

$$\begin{array}{ccc} \mathbb{F}_p^\times & \xrightarrow{\tau} & \mathcal{Q} \\ \downarrow & \nearrow \cong & \\ \mathbb{F}_p^\times / \{\pm 1\} & & \end{array}$$

Die Elemente im Kern von τ sind genau die Nullstellen von $X^2 - 1$, folglich kann es höchstens zwei solche Elemente geben. Für $p = 2$ ist das nur 1 , für ungerade Primzahlen sind das ± 1 , denn dann ist $1 \neq -1$.

Zusammenfassend können wir festhalten, dass für $p = 2$

$$|\mathcal{Q}| = \left| \mathbb{F}_q^\times / \{1\} \right| = |\mathbb{F}_q^\times| = q - 1$$

und für ungerades p

$$|\mathcal{Q}| = \left| \mathbb{F}_q^\times / \{1, -1\} \right| = \frac{q-1}{2}$$

gilt. Falls nicht nur nach der Anzahl der Quadrate in der Einheitengruppe, sondern in \mathbb{F}_q gefragt ist, so müssen wir noch das Quadrat 0 mitzählen und erhalten die Anzahlen q bzw. $\frac{q+1}{2}$. Insbesondere ist für gerades q jedes Element in \mathbb{F}_q ein Quadrat.

Aufgabe (Herbst 2014, T3A2)

Wie viele Quadrate gibt es im Ring $\mathbb{Z}/2014\mathbb{Z}$?

Lösungsvorschlag zur Aufgabe (Herbst 2014, T3A2)

Nach dem Chinesischen Restsatz gilt

$$\mathbb{Z}/2014\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/19\mathbb{Z} \times \mathbb{Z}/53\mathbb{Z},$$

sodass es genügt, die Quadrate auf der rechten Seite zu zählen. Auf der rechten Seite haben die Quadrate die Form (a^2, b^2, c^2) , also ist die gesuchte Anzahl die Zahl aller Kombinationen von Quadraten aus $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/19\mathbb{Z}$ und $\mathbb{Z}/53\mathbb{Z}$.

Da 2, 19 und 53 jeweils Primzahlen sind, handelt es sich bei den genannten Ringen um Körper, sodass wir wie oben skizziert vorgehen können: In $\mathbb{Z}/2\mathbb{Z}$ ist klar, dass sowohl 0 als 1 Quadrate sind. Sei daher p eine ungerade

Primzahl. Betrachte den Homomorphismus

$$\tau : \mathbb{F}_p^\times \rightarrow \mathcal{Q}, \quad a \mapsto a^2,$$

wobei \mathcal{Q} die Menge der Quadrate in \mathbb{F}_p^\times bezeichnet. Da $p \geq 3$ ist, ist $\bar{1} \neq -\bar{1}$ und somit sind $\bar{1}$ und $-\bar{1}$ zwei verschiedene Elemente im Kern von τ . Andererseits ist jedes $a \in \ker \tau$ eine Nullstelle von $X^2 - \bar{1}$, wovon es im Körper \mathbb{F}_p nur höchstens zwei geben kann. Dies zeigt $\ker \tau = \{\pm \bar{1}\}$ und der Homomorphiesatz liefert $\mathcal{Q} \cong \mathbb{F}_p / \{\pm \bar{1}\}$. Insbesondere gilt $|\mathcal{Q}| = \frac{p-1}{2}$.

In unserem Fall können wir uns jedoch nicht mit der Anzahl der Quadrate in der Einheitengruppe \mathbb{F}_p^\times begnügen, sondern wir müssen noch 0 hinzuzählen, um die Anzahl der Quadrate in \mathbb{F}_p zu erhalten.

Insgesamt ergibt sich die gesuchte Zahl an möglichen Kombinationen in unserem Fall als

$$2 \cdot \frac{19+1}{2} \cdot \frac{53+1}{2} = 2 \cdot 10 \cdot 27 = 540.$$

Aufgabe (Herbst 2013, T2A4)

Sei K ein endlicher Körper. Sei $a \in K$. Zeigen Sie, dass es Elemente $x, y \in K$ gibt, so dass $x^2 + y^2 = a$ gilt.

Hinweis Wie viele Quadrate gibt es in K ?

Lösungsvorschlag zur Aufgabe (Herbst 2013, T2A4)

Sei $|K| = q$ und $\mathcal{Q} = \{\alpha^2 \mid \alpha \in K\}$ die Menge der Quadrate in K . Wie oben bestimmt man $|\mathcal{Q}|$.

Für gerades q ist $K = \mathcal{Q}$, d. h. a ist ein Quadrat und es gibt $x \in K$ mit $a = x^2 = x^2 + 0^2$. Also ist $(x, 0)$ eine Lösung der Gleichung in der Aufgabenstellung.

Sei nun q ungerade. Wir zeigen, dass für ein $x \in K$ das Element $a - x^2$ ein Quadrat ist. Nehmen wir an, das ist nicht der Fall. Dann gilt $a - x^2 \neq y^2$ für beliebige $x, y \in K$, also sind die Mengen $a - \mathcal{Q}$ und \mathcal{Q} disjunkt. Wir zeigen nun, dass durch $K \rightarrow K : \alpha \mapsto a - \alpha$ eine Bijektion gegeben ist. Für den Nachweis der Injektivität seien $\alpha, \beta \in K$ vorgegeben mit $a - \alpha = a - \beta$. Es folgt $\alpha = \beta$. Als Abbildung zwischen endlichen, gleichmächtigen Mengen ist diese Abbildung damit bereits bijektiv. Es folgt $|a - \mathcal{Q}| = |\mathcal{Q}|$. Laut unserer Annahme ist $a - \mathcal{Q} \cap \mathcal{Q} = \emptyset$, also

$$|(a - \mathcal{Q}) \cup \mathcal{Q}| = |a - \mathcal{Q}| + |\mathcal{Q}| = \frac{q+1}{2} + \frac{q+1}{2} = q + 1 > q = |K|.$$

Dies kann jedoch nicht sein, da die Menge in K enthalten ist. Folglich gibt es $x^2, y^2 \in Q$, sodass

$$a - x^2 = y^2 \quad \in (a - Q) \cap Q \quad \Leftrightarrow \quad a = x^2 + y^2.$$

Aufgabe (Frühjahr 2008, T1A5)

- a** Bestimmen Sie die Anzahl der Zahlen $a \in \mathbb{N}$, so dass

$$1 \leq a < 42$$

$$x^2 \equiv a \pmod{42} \text{ für ein } x \in \mathbb{Z}.$$

- b** Welche Einheiten des Rings $\mathbb{Z}/42\mathbb{Z}$ kommen als quadratische Reste vor?

Lösungsvorschlag zur Aufgabe (Frühjahr 2008, T1A5)

- a** Nach dem Chinesischen Restsatz ist

$$\mathbb{Z}/42\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$$

und es genügt, die Quadrate auf der rechten Seite zu zählen. Wir haben bereits gesehen, dass die Anzahl der Quadrate in einem Körper mit q Elementen für ungerades q genau $\frac{q+1}{2}$ beträgt und für gerades q gleich q ist. Also gibt es auf der rechten Seite

$$2 \cdot 2 \cdot 4 = 16$$

Quadrate. Allerdings sollen wir laut Aufgabenstellung das Quadrat 0 nicht mitzählen, sodass die gesuchte Anzahl 15 ist.

- b** In $(\mathbb{Z}/2\mathbb{Z})^\times = \{\bar{1}\}$ und $(\mathbb{Z}/3\mathbb{Z})^\times = \{\bar{1}, \bar{2}\}$ ist $\bar{1}$ jeweils das einzige Quadrat. In $(\mathbb{Z}/7\mathbb{Z})^\times$ gibt es die Quadrate $\bar{1}, \bar{2}, \bar{4}$. Gesucht sind nun also die Urbilder von $(\bar{1}, \bar{1}, \bar{1}), (\bar{1}, \bar{1}, \bar{2})$ und $(\bar{1}, \bar{1}, \bar{4})$. Für das erste Element ist das einfach $\bar{1}$, für die anderen beiden sind die Urbilder nach dem auf Seite 114 beschriebenen Verfahren durch

$$21 \cdot 1 \cdot 1 + 14 \cdot (-1) \cdot 1 + 6 \cdot (-1) \cdot 2 \equiv -5 \equiv 37 \pmod{42}$$

$$21 \cdot 1 \cdot 1 + 14 \cdot (-1) \cdot 1 + 6 \cdot (-1) \cdot 4 \equiv -17 \equiv 25 \pmod{42}$$

gegeben. Also sind die in $(\mathbb{Z}/42\mathbb{Z})^\times$ auftretenden Quadrate $\bar{1}, \bar{25}$ und $\bar{37}$.

Das Legendre-Symbol

Es sei p eine ungerade Primzahl. Ist $a \in \mathbb{F}_p^\times$ ein Quadrat, d.h. $a = b^2$ für ein $b \in \mathbb{F}_p^\times$, so gilt wegen $|\mathbb{F}_p^\times| = p - 1$, dass

$$a^{\frac{p-1}{2}} = (b^2)^{\frac{p-1}{2}} = b^{p-1} = 1.$$

Folglich ist jedes Quadrat eine Nullstelle des Polynoms $X^{\frac{p-1}{2}} - 1$. Dieses Polynom kann höchstens $\frac{p-1}{2}$ Nullstellen in \mathbb{F}_p^\times haben. Da dies genau der Anzahl der Quadrate in \mathbb{F}_p^\times entspricht, sind die Nullstellen von $X^{\frac{p-1}{2}} - 1$ also genau die Quadrate. Eine äquivalente Formulierung wäre, dass $a \in \mathbb{F}_p^\times$ genau dann ein Quadrat ist, wenn $a^{\frac{p-1}{2}} = 1$ gilt.³

Ist a kein Quadrat, so ist immer noch $a^{p-1} = 1$, sodass $a^{\frac{p-1}{2}} = -1$ erfüllt sein muss. Wir haben daher mit

$$\mathbb{F}_p^\times \rightarrow \{\pm 1\}, \quad a \mapsto a^{\frac{p-1}{2}}$$

einen Homomorphismus gefunden, der uns sagt, ob ein Element ein Quadrat ist oder nicht. Dies übertragen wir nun auf die Ringe $\mathbb{Z}/p\mathbb{Z}$. Dazu sagen wir, eine Zahl $a \in \mathbb{Z}$ ist ein *quadratischer Rest modulo p*, falls es ein $x \in \mathbb{Z}$ mit $x^2 \equiv a \pmod{p}$ gibt. Andernfalls heißt a ein *quadratischer Nicht-Rest modulo p*.

Definition 2.16. Für eine Primzahl $p \in \mathbb{Z}$ ist das *Legendre-Symbol* definiert als

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{falls } x^2 \equiv a \pmod{p} \text{ lösbar ist und } a \not\equiv 0 \pmod{p}, \\ -1 & \text{falls } x^2 \equiv a \pmod{p} \text{ nicht lösbar ist,} \\ 0 & \text{falls } a \equiv 0 \pmod{p}. \end{cases}$$

Aus der gruppentheoretischen Interpretation des Legendre-Symbols zu Beginn ergibt sich unmittelbar das folgende Ergebnis.

Proposition 2.17 (Rechenregeln für das Legendre-Symbol). Sei p eine ungerade Primzahl und $a, b \in \mathbb{Z}$. Es gelten die folgenden Rechenregeln:

$$(1) \quad a \equiv b \pmod{p} \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$$

$$(2) \quad \left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$$

$$(3) \quad \left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right)$$

³ Man spricht hierbei vom *Euler-Kriterium*.

Dass das Legendre-Symbol effizient berechenbar ist, beruht jedoch v. a. auf dem **Quadratischen Reziprozitätsgesetz**. Dieses wurde erstmals von Gauß bewiesen und gehört zu den bedeutendsten Resultaten der Zahlentheorie.

Satz 2.18 (Quadratisches Reziprozitätsgesetz). Seien $p \neq q$ ungerade Primzahlen. Dann gilt

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \cdot \left(\frac{q}{p}\right).$$

Im Quadratischen Reziprozitätsgesetz hatten wir den Fall $p = 2$ ausgeschlossen – eine Lücke, die der folgende Satz behebt.

Proposition 2.19 (Ergänzungssätze). Sei p eine ungerade Primzahl. Dann gelten:

$$\begin{aligned} \left(\frac{-1}{p}\right) &= (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{falls } p \equiv 1 \pmod{4}, \\ -1 & \text{falls } p \equiv 3 \pmod{4}. \end{cases} \\ \left(\frac{2}{p}\right) &= (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & \text{falls } p \equiv \pm 1 \pmod{8}, \\ -1 & \text{falls } p \equiv \pm 3 \pmod{8}. \end{cases} \end{aligned}$$

Wir haben nun alle Rechenregeln beisammen, um Legendre-Symbole effizient berechnen zu können.

Anleitung: Berechnung von Legendre-Symbolen

Sei p eine Primzahl und $n \in \mathbb{Z}$.

- (1) Zerlege n in Primfaktoren, d. h. finde eine Darstellung $n = \pm \prod_{i=1}^m q_i^{v_i}$ mit Primzahlen q_i und natürlichen Zahlen v_i .
- (2) Nach Proposition 2.17 (3) ist dann

$$\left(\frac{n}{p}\right) = \left(\frac{\pm 1}{p}\right) \cdot \prod_{i=1}^m \left(\frac{q_i}{p}\right)^{v_i}.$$

Es genügt dabei, die Exponenten v_i modulo 2 zu reduzieren, denn gerade Exponenten liefern $(\pm 1)^2$ und damit keinen Beitrag (vgl. Beispiel 2.20).

- (3) Die einzelnen Faktoren $\left(\frac{q_i}{p}\right)$ berechnet man, indem man das Quadratische Reziprozitätsgesetz 2.18 anwendet und anschließend den „Nenner“ mittels Proposition 2.17 (1) reduziert. Dies wiederholt man so lange, bis man Proposition 2.19 oder das Euler-Kriterium 2.17 (2) anwenden kann.

Beispiel 2.20. Wir illustrieren die oben beschriebene Vorgehensweise exemplarisch:

$$\begin{aligned} \left(\frac{12}{29}\right) &= \left(\frac{2^2 \cdot 3}{29}\right) \stackrel{2.17(3)}{=} \left(\frac{2}{29}\right)^2 \cdot \left(\frac{3}{29}\right) = (\pm 1)^2 \cdot \left(\frac{3}{29}\right) = \\ &= \left(\frac{3}{29}\right) \stackrel{2.18}{=} (-1)^{14} \cdot \left(\frac{29}{3}\right) \stackrel{2.17(1)}{=} \left(\frac{-1}{3}\right) \stackrel{2.19}{=} (-1)^{\frac{3-1}{2}} = -1 \end{aligned}$$

■

Aufgabe (Frühjahr 2006, T2A2)

Für welche Primzahlen $p = 10n + k$ mit $n \geq 0$ und $k \in \{1, 3, 7, 9\}$ ist 5 ein quadratischer Rest, für welche ein quadratischer Nicht-Rest?

Lösungsvorschlag zur Aufgabe (Frühjahr 2006, T2A2)

Wir berechnen das zugehörige Legendre-Symbol:

$$\left(\frac{5}{p}\right) \stackrel{2.18}{=} (-1)^{2 \cdot \frac{p-1}{2}} \cdot \left(\frac{p}{5}\right) = \left(\frac{10n+k}{5}\right) \stackrel{2.17(1)}{=} \left(\frac{k}{5}\right)$$

Also genügt es zu prüfen, ob jeweils $k \in \{1, 3, 7, 9\}$ ein Quadrat modulo 5 ist. Dazu berechnen wir

$$\begin{aligned} \left(\frac{1}{5}\right) &= 1, \\ \left(\frac{3}{5}\right) &= (-1)^2 \cdot \left(\frac{5}{3}\right) = \left(\frac{-1}{3}\right) \stackrel{2.19}{=} -1, \\ \left(\frac{7}{5}\right) &= \left(\frac{2}{5}\right) \stackrel{2.19}{=} (-1)^{\frac{24}{8}} = -1, \\ \left(\frac{9}{5}\right) &= \left(\frac{3}{5}\right)^2 = (\pm 1)^2 = 1. \end{aligned}$$

Folglich ist 5 ein quadratischer Rest modulo Primzahlen der Form $10n + 1$ sowie $10n + 9$ und ein quadratischer Nicht-Rest modulo Primzahlen der Form $10n + 3$ sowie $10n + 7$.

Aufgabe (Frühjahr 2011, T3A1)

Zeigen Sie: Eine ungerade Primzahl p ist Teiler einer Zahl $n^2 + 1$ mit $n \in \mathbb{N}$ genau dann, wenn $p \equiv 1 \pmod{4}$ gilt.

Lösungsvorschlag zur Aufgabe (Frühjahr 2011, T3A1)

Es gelten die Äquivalenzen

$$p \mid (n^2 + 1) \Leftrightarrow n^2 + 1 \equiv 0 \pmod{p} \Leftrightarrow n^2 \equiv -1 \pmod{p},$$

also genügt es zu zeigen, dass $p \equiv 1 \pmod{4}$ genau dann gilt, wenn -1 ein Quadrat modulo p ist. Letzteres ist genau dann erfüllt, wenn für das Legendre-Symbol gilt, dass

$$\left(\frac{-1}{p}\right) = 1 \stackrel{2.19(1)}{\Leftrightarrow} (-1)^{\frac{p-1}{2}} = 1.$$

Die letzte Gleichung ist genau dann erfüllt, wenn $\frac{p-1}{2}$ eine gerade Zahl ist, d. h. für

$$2 \mid \left(\frac{p-1}{2}\right) \Leftrightarrow 4 \mid (p-1) \Leftrightarrow p-1 \equiv 0 \pmod{4} \Leftrightarrow p \equiv 1 \pmod{4}.$$

Anleitung: Nicht-Lösbarkeit quadratischer Gleichungen

Eine häufige Anwendung des Legendre-Symbols besteht darin, die Existenz einer ganzzahligen Lösung einer Gleichung der Form

$$x^2 + ny^k = a$$

für gewisse Zahlen $n, a \in \mathbb{Z}$ und $k \in \mathbb{N}_0$ auszuschließen. Dazu geht man folgendermaßen vor:

- (1) Wähle einen Primteiler p von n und reduziere obige Gleichung modulo p . Man erhält, dass

$$x^2 \equiv a \pmod{p},$$

d. h. a ist ein quadratischer Rest modulo p .

- (2) Berechne das Legendre-Symbol $\left(\frac{a}{p}\right)$. Ist das Ergebnis -1 , so hat man einen Widerspruch gefunden und es kann keine ganzzahlige Lösung geben.

Aufgabe (Frühjahr 2005, T3A4)

Hat die Gleichung

$$x^2 + 91y = 5$$

eine ganzzahlige Lösung? Begründen Sie Ihre Antwort.

Lösungsvorschlag zur Aufgabe (Frühjahr 2005, T3A4)

Nehmen wir an, dass es eine Lösung $(x, y) \in \mathbb{Z}^2$ gibt. Wir bemerken $91 = 7 \cdot 13$, sodass dann insbesondere

$$5 \equiv x^2 \pmod{7}$$

erfüllt ist, d. h. 5 ist ein Quadrat modulo 7. Dementsprechend müsste auch das zugehörige Legendre-Symbol 1 sein. Dieses berechnet sich jedoch zu

$$\left(\frac{5}{7}\right) = (-1)^{2 \cdot 3} \left(\frac{7}{5}\right) = \left(\frac{2}{5}\right) \stackrel{2.19}{=} (-1)^{\frac{24}{3}} = -1.$$

Also ist 5 doch kein Quadrat modulo 7 und die Annahme, dass es eine ganzzahlige Lösung gibt, muss falsch gewesen sein.

Aufgabe (Frühjahr 2013, T1A1)

Sei

$$S = \{n \in \mathbb{Z} \mid \text{es gibt } x, y \in \mathbb{Z} \text{ mit } n = x^2 - 23y^2\}.$$

Zeigen Sie folgende Aussagen:

- a** Die Primzahl 97 ist kein Element von S .

Hinweis Sie können zum Beispiel das Quadratische Reziprozitätsgesetz verwenden.

- b** Sind $a, b \in S$, dann ist auch $a \cdot b \in S$.

Lösungsvorschlag zur Aufgabe (Frühjahr 2013, T1A1)

- a** Angenommen, es ist $97 \in S$. Dann gibt es $x, y \in \mathbb{Z}$ mit $97 = x^2 - 23y^2$, sodass insbesondere $97 \equiv x^2 \pmod{23}$. Also ist 97 ein quadratischer Rest modulo 23. Andererseits berechnet sich das entsprechende Legendre-Symbol zu

$$\left(\frac{97}{23}\right) = \left(\frac{5}{23}\right) = (-1)^{2 \cdot 11} \cdot \left(\frac{23}{5}\right) = \left(\frac{3}{5}\right),$$

wobei wir im ersten Schritt $97 \equiv 5 \pmod{23}$ und im zweiten Schritt das Quadratische Reziprozitätsgesetz verwendet haben. Für das letzte Symbol gilt weiter

$$\left(\frac{3}{5}\right) \equiv 3^{\frac{5-1}{2}} = 3^2 = 9 \equiv -1 \pmod{5},$$

d. h. insgesamt $\left(\frac{97}{23}\right) = -1$, sodass 97 kein quadratischer Rest modulo 23 ist. Widerspruch.

- b) Seien beliebige Elemente $a = x^2 - 23y^2$ und $b = u^2 - 23v^2$ aus S vorgegeben. Die Rechnung

$$\begin{aligned} a \cdot b &= (x^2 - 23y^2) \cdot (u^2 - 23v^2) = \\ &= (x - \sqrt{23}y)(x + \sqrt{23}y)(u - \sqrt{23}v)(u + \sqrt{23}v) = \\ &= (x - \sqrt{23}y)(u - \sqrt{23}v)(x + \sqrt{23}y)(u + \sqrt{23}v) = \\ &= ((ux + 23vy) - \sqrt{23}(yu + vx))((ux + 23vy) + \sqrt{23}(yu + vx)) = \\ &= (ux + 23vy)^2 - 23(yu + vx)^2 \end{aligned}$$

zeigt dann, dass $ab \in S$.

Aufgabe (Herbst 2012, T1A2)

Gibt es ein $x \in \mathbb{Z}$ so, dass die Gleichung

$$x^{101} - (x+1)^{101} + x^2 - 47 \equiv 0 \pmod{101}$$

erfüllt ist?

Lösungsvorschlag zur Aufgabe (Herbst 2012, T1A2)

Nehmen wir an, es gibt ein solches $x \in \mathbb{Z}$. Es ist 101 eine Primzahl, sodass $\mathbb{Z}/101\mathbb{Z}$ ein Körper ist. Laut dem *freshman's dream* (vgl. Seite 206) gilt also $(a+b)^{101} = a^{101} + b^{101}$ für beliebige $a, b \in \mathbb{Z}/101\mathbb{Z}$ und somit

$$\begin{aligned} 0 &\equiv x^{101} - (x+1)^{101} + x^2 - 47 \equiv x^{101} - x^{101} - 1^{101} + x^2 - 47 \equiv \\ &\equiv x^2 - 48 \pmod{101} \end{aligned}$$

(Alternativ kann man auch verwenden, dass in einem endlichen Körper \mathbb{F}_q mit q Elementen für alle $a \in \mathbb{F}_q$ auch $a^q = a$ gilt, um auf das gleiche Ergebnis zu kommen).

Die neu erhaltene Gleichung zeigt, dass 48 ein quadratischer Rest modulo 101 ist. Allerdings berechnet sich das zugehörige Legendre-Symbol zu

$$\begin{aligned} \left(\frac{48}{101}\right) &= \left(\frac{2^4 \cdot 3}{101}\right) = \left(\frac{2}{101}\right)^4 \cdot \left(\frac{3}{101}\right) = (\pm 1)^4 \cdot \left(\frac{3}{101}\right) = \\ &= \left(\frac{3}{101}\right) \stackrel{2.18}{=} (-1)^{50} \cdot \left(\frac{101}{3}\right) = \left(\frac{-1}{3}\right) \stackrel{2.19}{=} -1. \end{aligned}$$

Die Rechnung zeigt, dass 48 kein quadratischer Rest modulo 48 ist. Widerspruch.

Aufgabe (Herbst 2004, T3A2)

- a** Sei p eine Primzahl und $a, b \in \mathbb{Z}$ mit $p \nmid a$. Zeigen Sie, dass die Kongruenz

$$x^2 - ay^2 \equiv b \pmod{p}$$

eine Lösung in ganzen Zahlen $x, y \in \mathbb{Z}$ hat.

Hinweis Zählen Sie die Elemente der Form $ay^2 + b$ in \mathbb{F}_p .

- b** Beweisen Sie, dass die Gleichung

$$x^2 - 43y^2 = 29$$

keine Lösung in ganzen Zahlen $x, y \in \mathbb{Z}$ hat.

Lösungsvorschlag zur Aufgabe (Herbst 2004, T3A2)

- a** Sei zunächst $p = 2$. Wegen $p \nmid a$ ist dann $a \equiv 1 \pmod{2}$ und die Kongruenz wird zu

$$x^2 - y^2 \equiv b \pmod{2}.$$

Für $b \equiv 0 \pmod{2}$ ist $(x, y) = (0, 0)$ eine Lösung und für $b \equiv 1 \pmod{2}$ ist $(x, y) = (1, 0)$ eine Lösung. In beiden Fällen existiert also eine Lösung. Sei daher im Weiteren p eine ungerade Primzahl. Betrachte

$$\mathcal{Q} = \{\bar{\alpha}^2 \mid \bar{\alpha} \in \mathbb{F}_p\}.$$

Es ist dann $|\mathcal{Q}| = \frac{p+1}{2}$. Die Abbildung

$$\tau_{\bar{a}, \bar{b}} : \mathbb{F}_p \rightarrow \mathbb{F}_p, \quad \bar{\alpha} \mapsto \bar{a}\bar{\alpha} + \bar{b}$$

ist eine Bijektion: Als Abbildung zwischen zwei endlichen, gleichmächtigen Mengen genügt es, Injektivität zu prüfen. Seien daher $\bar{\alpha}, \bar{\beta}$ mit $\tau_{\bar{a}, \bar{b}}(\bar{\alpha}) = \tau_{\bar{a}, \bar{b}}(\bar{\beta})$ vorgegeben. Dann gilt

$$\bar{a}\bar{\alpha} + \bar{b} = \bar{a}\bar{\beta} + \bar{b} \Leftrightarrow \bar{a}\bar{\alpha} = \bar{a}\bar{\beta} \Leftrightarrow \bar{\alpha} = \bar{\beta},$$

wobei im letzten Schritt einging, dass wegen $p \nmid a$ auch $\bar{a} \in \mathbb{F}_p^\times$ gilt. Folglich ist $\tau_{\bar{a}, \bar{b}}$ eine Bijektion, sodass

$$\frac{p+1}{2} = |\mathcal{Q}| = |\tau_{\bar{a}, \bar{b}}(\mathcal{Q})| = |\{\bar{a}\bar{\alpha}^2 + \bar{b} \mid \bar{\alpha} \in \mathbb{F}_p\}|.$$

Angenommen, es ist $\mathcal{Q} \cap \tau_{\bar{a}, \bar{b}}(\mathcal{Q}) = \emptyset$. Dann ist

$$|\mathcal{Q} \cup \tau_{\bar{a}, \bar{b}}(\mathcal{Q})| = |\mathcal{Q}| + |\tau_{\bar{a}, \bar{b}}(\mathcal{Q})| = \frac{p+1}{2} + \frac{p+1}{2} = p+1 > p = |\mathbb{F}_p|,$$

was offensichtlich ein Widerspruch ist. Der Schnitt der beiden Mengen muss daher nicht leer sein, d.h. es gibt $\bar{x}, \bar{y} \in \mathbb{F}_p$ mit

$$\bar{x}^2 = \bar{a}\bar{y}^2 + \bar{b} \Leftrightarrow \bar{x}^2 - \bar{a}\bar{y}^2 = \bar{b}.$$

Fassen wir die letzte Gleichung statt als Gleichung in \mathbb{F}_p als Kongruenz ganzer Zahlen x, y, a, b auf, so ergibt sich die Behauptung.

- b** Wir bemerken zunächst, dass 43 eine Primzahl ist. Gäbe es eine Lösung $(x, y) \in \mathbb{Z}^2$ der angegebenen Gleichung, so wäre wegen

$$x^2 \equiv 29 \pmod{43}$$

die Zahl 29 ein quadratischer Rest modulo 43. Folgende Rechnung für das Legendre-Symbol

$$\begin{aligned} \left(\frac{29}{43} \right) &= (-1)^{14 \cdot 21} \cdot \left(\frac{43}{29} \right) = \left(\frac{14}{29} \right) = \left(\frac{2}{29} \right) \cdot \left(\frac{7}{29} \right) = \\ &= (-1) \cdot (-1)^{3 \cdot 14} \cdot \left(\frac{29}{7} \right) = -\left(\frac{1}{7} \right) = -1 \end{aligned}$$

zeigt jedoch, dass 29 kein Quadrat modulo 43 ist.

2.5. Irreduzibilität von Polynomen

Sei R ein Integritätsbereich und $R[X]$ der Polynomring über R (der dann wiederum ein Integritätsbereich ist). Wir erinnern zunächst daran, dass ein Polynom $f \neq 0$ aus $R[X]$ **irreduzibel** heißt, wenn f keine Einheit ist, und für jede Zerlegung von f in Polynome $f = g \cdot h$ folgt, dass g oder h eine Einheit ist.

Polynome über Körpern. Wir betrachten zunächst den Fall, dass $f \in K[X]$ ein Polynom von Grad ≤ 3 ist, wobei $K[X]$ der Polynomring über einem Körper K ist. Die Einheiten in $K[X]$ sind genau die Elemente aus $K^\times = K \setminus \{0_K\}$. Ist f also reduzibel, so müssten die Faktoren $g, h \in K[X]$ einer Zerlegung $f = gh$ mindestens Grad 1 haben. Aufgrund der Formel $\text{grad}(gh) = \text{grad } g + \text{grad } h$ muss einer der beiden Faktoren zudem genau Grad 1 haben. Dieser Faktor liefert als Linearfaktor somit eine Nullstelle im Grundkörper. Dies zeigt, dass jedes reduzible Polynom von Grad 3 oder kleiner mindestens eine Nullstelle in K hat und begründet damit das folgende Lemma.

Lemma 2.21. Sei $K[X]$ der Polynomring über einem Körper K . Ist $f \in K[X]$ ein Polynom von Grad 3 oder 2, so ist f genau dann irreduzibel, wenn es in K keine Nullstellen besitzt.

Für höhere Grade ist diese Aussage falsch, da diese beispielsweise auch quadratische Faktoren enthalten können, die keine Nullstellen liefern. Ein Beispiel hierfür ist das Polynom $(X^2 + 1)^2$, das über \mathbb{R} keine Nullstellen besitzt, aber offensichtlich in zwei quadratische Faktoren zerfällt.

Wenn es um die Suche rationaler Nullstellen ganzzahliger Polynome geht, ist die Situation besonders komfortabel (vgl. dazu auch F11T2A2, Seite 142):

Lemma 2.22 (Rationale Nullstellen). Sei $f = \sum_{i=0}^n a_i X^i$ ein Polynom in $\mathbb{Z}[X]$. Dann gilt für jede vollständig gekürzte Nullstelle $\frac{p}{q} \in \mathbb{Q}$

$$q \mid a_n \quad \text{und} \quad p \mid a_0.$$

Polynome über Ringen und Quotientenkörpern. Man beachte, dass aus der Irreduzibilität eines Polynoms in $\mathbb{Q}[X]$ im Allgemeinen *nicht* folgt, dass das Polynom auch in $\mathbb{Z}[X]$ irreduzibel ist. Als Gegenbeispiel betrachte $f = 4X + 2$. Das Polynom ist in $\mathbb{Q}[X]$ irreduzibel, weil dort jedes Element aus \mathbb{Q} eine Einheit ist und somit jedes Polynom von Grad 1 irreduzibel ist. In $\mathbb{Z}[X]$ ist jedoch $f = 2(2X + 1)$ eine Zerlegung in zwei Nicht-Einheiten.

Obige Aussage wird dagegen richtig, wenn wir zusätzlich voraussetzen, dass das untersuchte Polynom teilerfremde Koeffizienten hat. Man bezeichnet es dann als *primitiv*. Beispielsweise sind normierte Polynome stets primitiv. Ein Ergebnis von Gauß lautet, dass das Produkt zweier primitiver Polynome wieder primitiv ist.

Einen grundlegenden Zusammenhang zwischen dem Polynomring über R und seinem Quotientenkörper liefert der folgende Satz.

Satz 2.23 (Gauß). Sei R ein Ring, K sein Quotientenkörper.

- (1) Jedes nicht-konstante Polynom $f \in R[X]$, das in $R[X]$ irreduzibel ist, ist auch in $K[X]$ irreduzibel.
- (2) Ist f primitiv, so ist f genau dann in $R[X]$ irreduzibel, wenn es in $K[X]$ irreduzibel ist.

In diesem Zusammenhang ebenfalls nützlich:

Lemma 2.24. Sei R ein faktorieller Ring mit Quotientenkörper K und seien $f, g, h \in K[X]$ normierte Polynome mit $f = gh$. Ist $f \in R[X]$, dann gilt auch $g, h \in R[X]$.

Polynome in mehreren Variablen. Ist R ein faktorieller Ring, so bezeichnet $R[X, Y] = R[X][Y]$ den Polynomring über R in den beiden Variablen X und Y . Die Elemente von $R[X, Y]$ können als Polynome in Y aufgefasst werden, deren Koeffizienten wiederum Polynome in X sind. Dabei können die Rollen von X und Y genauso gut vertauscht werden.

Falls R faktoriell ist, so ist auch der Polynomring $R[X, Y]$ nach Aussage (4) auf Seite 90 faktoriell, sodass die nachfolgenden Kriterien auch für diesen gelten.

Zwei Kriterien für Irreduzibilität

Satz 2.25 (Eisenstein-Kriterium). Sei R ein faktorieller Ring, K sein Quotientenkörper und $f = \sum_{k=0}^n a_k X^k$ ein Polynom vom Grad > 0 . Gibt es ein Primelement $p \in R$ mit

$$p \nmid a_n, \quad p \mid a_i \text{ für } i \in \{0, \dots, n-1\}, \quad p^2 \nmid a_0,$$

so ist f in $K[X]$ irreduzibel.

Satz 2.26 (Reduktionskriterium). Sei R ein faktorieller Ring, $p \in R$ ein Primelement und $f = \sum_{k=0}^n a_k x^k \in R[X]$ ein nicht-konstantes Polynom, dessen höchster Koeffizient nicht von p geteilt wird. Weiter sei $\pi : R \rightarrow R/(p)$ der kanonische Epimorphismus. Ist $\pi(f) = \sum_{k=0}^n \pi(a_k) x^k$ irreduzibel in $R/(p)[X]$, so ist f irreduzibel in $K[X]$ (wobei K den Quotientenkörper von R bezeichnet).

Am häufigsten wendet man das Reduktionskriterium für $R = \mathbb{Z}$ und eine Primzahl p an. Für die Untersuchung der Irreduzibilität in $\mathbb{Z}/p\mathbb{Z}[X]$ ist zudem Lemma 2.21 nützlich, denn ob ein Polynom eine Nullstelle in $\mathbb{Z}/p\mathbb{Z}$ besitzt lässt sich einfach durch sukzessives Einsetzen aller Elemente feststellen. Dies führt dazu, dass man die irreduziblen (und normierten) Polynome kleinen Grades zumindest in den Fällen $p \in \{2, 3\}$ direkt auflisten kann.

Aufgabe (Frühjahr 2010, T3A1)

Berechnen Sie alle rationalen Nullstellen des Polynoms

$$f = X^5 + X^4 - 2.$$

Begründen Sie insbesondere, dass es über die von Ihnen angegebenen Nullstellen hinaus keine weiteren rationalen Nullstellen gibt.

Lösungsvorschlag zur Aufgabe (Frühjahr 2010, T3A1)

Laut Lemma 2.22 kommen nur Teiler von 2 in Frage. Durch Ausprobieren findet man $f(1) = 0$. Wir können daher den Linearfaktor $(X - 1)$ ausklammern:

$$\begin{aligned} f &= X^5 + X^4 - 2 = (X - 1)X^4 + 2X^4 - 2 = (X - 1)X^4 + 2(X^4 - 1) \\ &= (X - 1)X^4 + 2(X^2 - 1)(X^2 + 1) = (X - 1)X^4 + 2(X - 1)(X + 1)(X^2 + 1) \\ &= (X - 1) \left(X^4 + 2(X + 1)(X^2 + 1) \right) = (X - 1)(X^4 + 2X^3 + 2X^2 + 2X + X) \end{aligned}$$

Das Polynom $X^4 + 2X^3 + 2X^2 + 2X + 2$ ist nach dem Eisenstein-Kriterium irreduzibel in $\mathbb{Q}[X]$, besitzt also keine rationalen Nullstellen, denn eine Nullstelle würde einen Teiler vom Grad 1 bedeuten. Also ist 1 die einzige Nullstelle von f in \mathbb{Q} .

Aufgabe (Herbst 2012, T3A5)

Zerlegen Sie das Polynom $X^5 - 7X^3 + 503X^2 + 12X - 2012$ in $\mathbb{Q}[X]$ in irreduzible Faktoren!

Lösungsvorschlag zur Aufgabe (Herbst 2012, T3A5)

Wir gehen naiv an diese Aufgabe heran und untersuchen f zunächst auf Nullstellen: Da f normiert ist, müssen diese Teiler des konstanten Terms sein. Es gilt $2012 = 2^2 \cdot 503$. Wir sehen nun

$$2^5 - 7 \cdot 2^3 + 503 \cdot 2^2 + 12 \cdot 2 - 2012 = 32 - 56 + 2012 - 24 - 2012 = 0.$$

Somit ist 2 eine Nullstelle des Polynoms. Zudem ist wegen

$$f(-2) = -32 + 56 + 2012 - 24 - 2012 = 0$$

auch -2 eine Nullstelle des Polynoms ist. Dementsprechend berechnen wir nun

$$\begin{array}{r} (X^5 - 7X^3 + 503X^2 + 12X - 2012) : (X^2 - 4) = X^3 - 3X + 503 \\ \underline{- X^5 + 4X^3} \\ \hline - 3X^3 + 503X^2 + 12X \\ \underline{3X^3} \quad \underline{- 12X} \\ \hline 503X^2 \quad - 2012 \\ \underline{- 503X^2} \quad \underline{+ 2012} \\ \hline 0 \end{array}$$

Somit gilt

$$X^5 - 7X^3 + 503X^2 + 12X - 2012 = (X + 2)(X - 2)(X^3 - 3X + 503).$$

Die ersten beiden Faktoren sind als Polynome von Grad 1 irreduzibel. Für den letzten Faktor genügt es zu zeigen, dass dieser keine Nullstellen hat. Wiederum kommen dafür aber nur ± 503 sowie ± 1 in Betracht. Es gilt

$$503^3 - 3 \cdot 503 + 503 = 503^3 - 2 \cdot 503 = 503(503^2 - 2) \neq 0$$

und

$$(-503)^3 - 3(-503) + 503 = -503^3 + 4 \cdot 503 = 503(4 - 503^2) \neq 0.$$

Somit ist das Polynom $X^3 - 3X + 503$ über \mathbb{Q} nullstellenfrei und damit irreduzibel.

Anleitung: Irreduzibilität mittels Koeffizientenvergleich

Sei $f \in K[X]$ ein Polynom von Grad 4 oder höher. Es genügt dann nicht mehr, die Nullstellenfreiheit von f über K nachzuweisen, da hier auch quadratische Faktoren in Frage kommen können.

- (1) Prüfe zunächst, ob f Nullstellen hat. Wenn ja, so ist das Polynom in dem Fall reduzibel (eine Zerlegung erhält man dann mittels Polynomdivision bzw. Ausklammern). Wenn nein, so enthält eine Zerlegung von f zumindest keinen Linearfaktor.
- (2) Bestimme mittels Gradargumenten alle restlichen Möglichkeiten, welche Grade Teiler von f haben könnten.
- (3) Leite aus den Kombinationen aus (2) durch Aufstellen einer Gleichung jeweils Gleichungen für die Koeffizienten der Faktoren in einer Zerlegung ab.
- (4) Aus dem Gleichungssystem aus (3) ergibt sich optimalerweise ein Widerspruch, sodass eine derartige Zerlegung nicht möglich (und f letzten Endes irreduzibel) ist, oder aber eine Lösung, die eine Zerlegung in Faktoren liefert.

Aufgabe (Herbst 2003, T2A5)

Zeigen Sie die Irreduzibilität der folgenden Polynome über \mathbb{Z} :

- a** $f = X^p + pX - 1$ für jede Primzahl p
- b** $f = X^4 - 42X^2 + 1$

Lösungsvorschlag zur Aufgabe (Herbst 2003, T2A5)

- a** Für diese Teilaufgabe kommt ein interessanter Trick zum Zuge. Ist $f(X) \in \mathbb{Q}[X]$ ein Polynom, sodass $f(X+c)$ für ein $c \in \mathbb{Q}$ irreduzibel ist, so ist auch $f(X)$ irreduzibel. Nehmen wir nämlich an, dass f reduzibel wäre, es also es eine Zerlegung der Form $f(X) = g(X)h(X)$ gibt. Dann wäre aber $f(X+c) = g(X+c)h(X+c)$ eine Zerlegung von $f(X+c)$ in Polynome, die nicht verschwinden – Widerspruch. Also folgt aus der Irreduzibilität von $f(X+1)$ auch, dass $f(X)$ irreduzibel ist. Unter Verwendung des binomischen Lehrsatzes gilt nun

$$\begin{aligned} f(X+1) &= (X+1)^p + p(X+1) - 1 = \sum_{k=0}^p \binom{p}{k} X^k + pX + p - 1 = \\ &= X^p + \sum_{k=1}^{p-1} \binom{p}{k} X^k + pX + p. \end{aligned}$$

Wir wenden nun das Eisenstein-Kriterium an: Es gilt

$$\binom{p}{k} = \frac{p!}{k!(p-k)!},$$

sodass für $1 \leq k < p$ der Faktor p im Zähler einmal, im Nenner nicht vorkommt. Da p eine Primzahl ist, folgt daraus $p \mid \binom{p}{k}$. Somit teilt p den Leitkoeffizienten von $f(X+1)$ nicht, alle anderen Koeffizienten einmal und den konstanten Term nicht doppelt. Gemäß dem Eisenstein-Kriterium ist $f(X+1)$ irreduzibel in $\mathbb{Q}[X]$ und laut der Vorbemerkung gilt dies auch für $f(X)$ selbst. Da f primitiv ist, folgt, dass es auch über \mathbb{Z} irreduzibel ist.

- b** Man prüft zunächst leicht, dass ± 1 keine Nullstellen von f sind. Damit kommt nur eine Zerlegung von f in zwei Polynome von Grad 2 in Betracht. Wiederum können wir voraussetzen, dass diese normiert sind. Dann muss es also eine Zerlegung der Form

$$X^4 - 42X^2 + 1 = (X^2 + bX + c)(X^2 + eX + f)$$

mit $b, c, e, f \in \mathbb{Z}$ geben. Koeffizientenvergleich liefert die Gleichungen

$$e + b = 0, \quad be + c + f = -42, \quad bf + ec = 0, \quad cf = 1.$$

Die erste Gleichung impliziert $e = -b$. Aus der letzten Gleichung folgt $c = \pm 1$ und daraus $c = f = 1$ oder $c = f = -1$. Im ersten Fall wird die zweite Gleichung zu

$$-b^2 = -44 \quad \Leftrightarrow \quad b^2 = 44 \quad \Rightarrow \quad b \notin \mathbb{Z}.$$

Im zweiten Fall folgt analog

$$-b^2 = -40 \Leftrightarrow b^2 = 40 \Rightarrow b \notin \mathbb{Z}.$$

Somit zerfällt f auch nicht in zwei Polynome von Grad 2 und muss daher über \mathbb{Z} irreduzibel sein.

Aufgabe (Frühjahr 2013, T3A4)

- a** Sei \mathbb{F}_3 der Körper mit drei Elementen. Man bestimme alle normierten, irreduziblen Polynome von Grad ≤ 2 in $\mathbb{F}_3[X]$.
- b** Ist $X^4 + 9X^2 - 2X + 2$ in $\mathbb{Q}[X]$ irreduzibel?

Lösungsvorschlag zur Aufgabe (Frühjahr 2013, T3A4)

- a** Alle normierten Polynome von Grad 1 sind irreduzibel. Dies sind in $\mathbb{F}_3[X]$ die Polynome

$$X, \quad X + 1, \quad X + 2.$$

Für die Polynome von Grad 2 verwenden wir, dass diese genau dann irreduzibel sind, wenn sie nullstellenfrei über \mathbb{F}_3 sind. Die folgende Liste zeigt alle normierten Polynome von Grad 2, wobei die eingeklammerten eine Nullstelle haben:

$$(X^2), \quad X^2 + 1, \quad (X^2 + 2), \quad (X^2 + X), \quad (X^2 + X + 1), \quad X^2 + X + 2, \\ (X^2 + 2X), \quad (X^2 + 2X + 1), \quad X^2 + 2X + 2.$$

- b** Wir verwenden Reduktion modulo 3. Das zugehörige Bild des Polynoms f ist

$$\bar{f} = X^4 + X + 2 \in \mathbb{F}_3[X].$$

Dieses hat in $\mathbb{F}_3[X]$ keine Nullstelle. Somit muss eine Zerlegung einen irreduziblen quadratischen Faktor enthalten. Wegen des konstanten Terms kommen aus der Auflistung in Teil **a** nur zwei Kombinationen in Betracht. Für diese gilt

$$(X^2 + 1)(X^2 + X + 2) = X^4 + X^3 + X + 2 \neq \bar{f}$$

und

$$(X^2 + 1)(X^2 + 2X + 2) = X^4 + 2X^3 + 2X + 2 \neq \bar{f}.$$

Somit enthält \bar{f} auch keinen quadratischen Faktor und ist damit irreduzibel in $\mathbb{F}_3[X]$. Mit dem Reduktionskriterium 2.26 folgt, dass f in $\mathbb{Z}[X]$ irreduzibel ist, und da f primitiv ist, ist es auch irreduzibel in $\mathbb{Q}[X]$.

Aufgabe (Frühjahr 2005, T1A4)

Untersuchen Sie (mit Beweis) auf Irreduzibilität:

- a** $f(X) = X^4 - X^3 - 9X^2 + 4X + 2$ und $g(X) = X^4 + 2X^3 + X^2 + 1$ in $\mathbb{Q}[X]$.
- b** $f(X, Y) = Y^6 + XY^5 + 2X^2Y^2 - X^3Y + X^2 + X$ in $\mathbb{Q}[X, Y]$.

Lösungsvorschlag zur Aufgabe (Frühjahr 2005, T1A4)

- a** Das Polynom ist primitiv. Es genügt also, Irreduzibilität über \mathbb{Z} zu untersuchen. Man sieht schnell, dass keiner der Teiler des konstanten Gliedes ($\pm 1, \pm 2$) eine Nullstelle von f ist, sodass f über \mathbb{Z} (und damit über \mathbb{Q}) nullstellenfrei ist und keinen Linearfaktor enthält. Damit kommt nur eine Zerlegung in zwei Polynome von Grad 2 in Frage. Da f normiert ist, können wir annehmen, dass dies auch für die beiden Faktoren gilt. Wir machen also den Ansatz

$$X^4 - X^3 - 9X^2 + 4X + 2 = (X^2 + aX + b)(X^2 + cX + d)$$

für $a, b, c, d \in \mathbb{Z}$. Aus der Gleichung $bd = 2$ folgt wiederum $b \in \{\pm 1, \pm 2\}$. Die weiteren Gleichungen aus dem Koeffizientenvergleich sind

$$a + c = -1, \quad b + d + ac = -9, \quad ad + bc = 4.$$

Für $b = -1$ folgt zunächst $d = -2$. Die erste Gleichung impliziert zudem $a = -1 - c$. Setzt man beides in die zweite Gleichung ein, so erhält man

$$\begin{aligned} -1 - 2 + (-1 - c)c &= -9 &\Leftrightarrow & -c^2 - c - 3 = -9 \\ \Leftrightarrow c^2 + c - 6 &= 0 &\Leftrightarrow & c \in \{2, -3\}. \end{aligned}$$

Im Fall $c = 2$ folgt dann $a = -3$. Die dritte Gleichung ist wegen $-3 \cdot (-2) + (-1) \cdot 2 = 4$ ebenfalls erfüllt. Wir haben somit die Zerlegung

$$f(X) = (X^2 - 3X - 1)(X^2 + 2X - 2)$$

gefunden. Insbesondere ist f über \mathbb{Q} *nicht* irreduzibel.

Das Polynom g hingegen ist irreduzibel, wie wir mit dem Reduktionskriterium zeigen. Reduktion modulo 2 liefert das Polynom $X^4 + X^2 + 1$, das leider nicht irreduzibel ist. Reduktion modulo 3 jedoch ergibt das Polynom

$$\bar{g} = X^4 + \bar{2}X^3 + X^2 + \bar{1} \in \mathbb{F}_3[X],$$

das zumindest keine Nullstellen in \mathbb{F}_3 hat, wie man leicht nachrechnet. Nun zeigt man, dass die normierten irreduziblen Polynome von Grad 2 in $\mathbb{F}_3[X]$ genau

$$X^2 + 1, \quad X^2 + X - 1, \quad X^2 - X - 1$$

sind. Es müsste also \bar{g} das Produkt zweier dieser Polynome sein. Da \bar{g} das konstante Glied $+1$ hat, kommen nur 4 Möglichkeiten in Betracht, die wir ausschließen:

$$\begin{aligned} (X^2 + 1)(X^2 + 1) &= X^4 + 2X^2 + 1 \\ (X^2 + X - 1)(X^2 + X - 1) &= X^4 + 2X^3 + 2X^2 + X + 1 \\ (X^2 - X - 1)(X^2 - X - 1) &= X^4 + X^3 + 2X^2 + 2X + 1 \\ (X^2 + X - 1)(X^2 - X - 1) &= X^4 + 1 \end{aligned}$$

Somit ist \bar{g} in $\mathbb{F}_3[X]$ irreduzibel, und damit ist laut Satz 2.26 auch g in $\mathbb{Q}[X]$ irreduzibel.

- b** Wir fassen f als Polynom in der Variablen Y und mit Koeffizienten aus dem Ring $\mathbb{Q}[X]$ auf. Das Element X ist in $\mathbb{Q}[X]$ ein Primelement. Um dies zu sehen, bemerke beispielsweise, dass $\mathbb{Q}[X]/(X) \cong \mathbb{Q}$ ein Integritätsbereich ist, sodass (X) ein Primideal ist. Ferner gilt

$$X \nmid 1, \quad X \mid X, \quad X \mid 2X^2, \quad X \mid -X^3, \quad X \mid (X^2 + X), \quad X^2 \nmid (X^2 + X).$$

Somit sind alle Voraussetzungen des Eisenstein-Kriteriums erfüllt und f ist über dem Quotientenkörper $\mathbb{Q}(X)$ irreduzibel. Als normiertes und somit primitives Polynom ist f auch irreduzibel in $\mathbb{Q}[X][Y] = \mathbb{Q}[X, Y]$.

Aufgabe (Frühjahr 2002, T2A1)

Sei $f = a_4X^4 + a_3X^3 + a_2X^2 + a_1X + a_0$ ein Polynom mit ganzzahligen Koeffizienten. Seien alle a_i ungerade. Man zeige, dass f irreduzibel über \mathbb{Q} ist.

Lösungsvorschlag zur Aufgabe (Frühjahr 2002, T2A1)

Es ist $a_0 \equiv a_1 \equiv a_2 \equiv a_3 \equiv a_4 \equiv 1 \pmod{2}$, da die Koeffizienten nach Voraussetzung ungerade sind. Wir zeigen, dass das Polynom

$$\bar{f} = X^4 + X^3 + X^2 + X + \bar{1} \in \mathbb{F}_2[X],$$

welches die Reduktion von f modulo 2 ist, irreduzibel in $\mathbb{F}_2[X]$ ist. Die Irreduzibilität von f in \mathbb{Q} folgt dann aus dem Reduktionskriterium.

Es ist $\bar{f}(\bar{0}) = \bar{1} = \bar{f}(\bar{1})$, also hat \bar{f} keine Nullstelle in \mathbb{F}_2 . Zu überprüfen bleibt, ob \bar{f} einen irreduziblen Teiler von Grad 2 hat. In $\mathbb{F}_2[X]$ gibt es nur ein irreduzibles Polynom von Grad 2, nämlich $X^2 + X + \bar{1}$. Es ist

$$(X^2 + X + \bar{1})^2 = X^4 + X^2 + \bar{1} \neq f,$$

sodass also \bar{f} auch nicht das Quadrat von $X^2 + X + \bar{1}$ ist. Damit hat \bar{f} keinen Teiler von Grad 2 und ist irreduzibel.

Aufgabe (Herbst 2011, T3A5)

Untersuchen Sie die folgenden Polynome auf Irreduzibilität. Hierbei ist \mathbb{F}_2 der endliche Körper mit 2 Elementen.

- a** $X^5 + X^2 + 1$ in $\mathbb{F}_2[X]$
- b** $X^5 + X^2Y^3 + X^3 + Y^3 + X^2 + 1$ in $\mathbb{Q}[X, Y]$

Lösungsvorschlag zur Aufgabe (Herbst 2011, T3A5)

- a** Man sieht unmittelbar, dass das Polynom, das wir im Folgenden als f bezeichnen, keine Nullstelle in \mathbb{F}_2 hat. Daher kommt nur eine Zerlegung der Form

$$\begin{aligned} X^5 + X^2 + 1 &= (X^3 + bX^2 + cX + d)(X^2 + eX + f) = \\ &= X^5 + (b+e)X^4 + (f+be+c)X^3 + (bf+ce+d)X^2 + (cf+de)X + df \end{aligned}$$

für $b, c, d, e, f \in \mathbb{F}_2$ in Frage. Aus $df = 1$ folgt $d = f = 1$ (beachte $1 = -1$ in \mathbb{F}_2). Daraus folgt $c + e = 0 \Leftrightarrow c = e$. Aus der Gleichung für den Term vierten Grades folgt zudem $b = e = c$. Nehmen wir nun an, dass $c = 0$ gilt. Dann folgt $b = c = e = 0$. Jedoch ist

$$(X^3 + 1)(X^2 + 1) = X^5 + X^3 + X^2 + 1 \neq f.$$

Im Fall $c = 1$ erhält man $b = c = e = 1$ und dann aber

$$(X^3 + X^2 + X + 1)(X^2 + X + 1) = X^5 + X^3 + X^2 + 1 \neq f.$$

Damit ist auch eine solche Zerlegung nicht möglich und das Polynom f ist irreduzibel.

- b** Es ist

$$\begin{aligned} X^5 + X^2Y^3 + X^3 + Y^3 + X^2 + 1 &= X^3(X^2 + 1) + (X^2 + 1)Y^3 + X^2 + 1 = \\ &= (X^2 + 1)(X^3 + Y^3 + 1). \end{aligned}$$

Da \mathbb{Q} ein Integrätsbereich ist, gilt $\mathbb{Q}[X, Y]^\times = \mathbb{Q}^\times$ und die Einheiten sind Elemente aus \mathbb{Q} . Keiner der beiden Faktoren ist also eine Einheit und das angegebene Polynom ist damit nicht irreduzibel.

Aufgabe (Frühjahr 2006, T1A2)

Sei $f(X, Y) = X^{17} + Y^{41}(X^3 + X + 1) - Y \in \mathbb{C}[X, Y]$.

- a** Man zeige, dass f als Polynom in X über dem Koeffizientenring $\mathbb{C}[Y]$ irreduzibel ist.

Hinweis Eisenstein-Kriterium.

- b** Man zeige, dass f ein irreduzibles Element im Ring $\mathbb{C}[X, Y]$ ist.

Lösungsvorschlag zur Aufgabe (Frühjahr 2006, T1A2)

- a** Es ist

$$f(X, Y) = X^{17} + Y^{41}X^3 + Y^{41}X + (Y^{41} - Y).$$

Wie in früheren Aufgaben zeigt man, dass Y in $\mathbb{C}[Y]$ ein Primelement ist. Wegen

$$Y \nmid 1, \quad Y \mid Y^{41}, \quad Y \mid Y^{41} - Y, \quad Y^2 \nmid Y^{41} - Y.$$

ist f als Polynom in X über $\mathbb{C}(Y)$ irreduzibel. Da f normiert ist, handelt es sich bei f um ein primitives Polynom, sodass f auch irreduzibel über $\mathbb{C}[Y]$ ist.

- b** Diese Aufgabe ist seltsam: Teil **a** besagt gerade, dass f ein irreduzibles Element in $\mathbb{C}[Y][X]$ ist. Wegen $\mathbb{C}[X, Y] = \mathbb{C}[Y][X]$ ist das jedoch bereits die Aussage.

Aufgabe (Frühjahr 2008, T2A4)

Sei $a \in \mathbb{Z}$ beliebig. Zeigen Sie: Es gibt unendlich viele ganze $b \in \mathbb{Z}$, so dass das Polynom $f(X) = X^3 + aX + b \in \mathbb{Q}[X]$ irreduzibel ist.

Lösungsvorschlag zur Aufgabe (Frühjahr 2008, T2A4)

Beschäftigen wir uns zunächst mit dem Fall $a \notin \{0, \pm 1\}$. Dann besitzt a einen Primteiler p . Wähle nun eine andere Primzahl q , sodass $q \neq p$. Dann sind alle Polynome der Form

$$X^3 + aX + pq^n$$

für $n \in \mathbb{N}$ wegen

$$p \nmid 1, \quad p \mid a, \quad p \mid pq^n, \quad p^2 \nmid pq^n$$

nach dem Eisenstein-Kriterium irreduzibel.

Im Fall $a = 0$ verfährt man analog, hier funktioniert $b = pq^n$ für beliebige, verschiedene Primzahlen p, q . In jedem Fall gibt es, da die Zahlen der Form pq^n für $n \in \mathbb{N}$ verschieden sind, unendlich viele solcher Elemente.

Betrachten wir zu guter Letzt noch den Fall $a = \pm 1$. Hier greifen wir auf das Reduktionskriterium zurück und zeigen, dass f irreduzibel ist, solange b ungerade ist. Das Bild von f in $\mathbb{F}_2[X]$ lautet dann

$$\bar{f} = X^3 + X + \bar{1}.$$

Wegen $\bar{f}(\bar{0}) = \bar{1}, \bar{f}(\bar{1}) = \bar{1}$ ist \bar{f} als nullstellenfreies Polynom dritten Grades irreduzibel in $\mathbb{F}_2[X]$ und somit in $\mathbb{Q}[X]$. Da es unendlich viele ungerade Zahlen gibt, folgt auch hier die Aussage.

Aufgabe (Frühjahr 2010, T1A3)

Sei \mathbb{F}_2 der Körper mit zwei Elementen und sei $K = \mathbb{F}_2[X]/(X^2 + X + 1)$.

- a** Zeigen Sie, dass K ein Körper ist.
- b** Sei $f(X) \in \mathbb{F}_2[X]$ ein normiertes Polynom von Grad ≤ 5 mit $f(0) \neq 0, f(1) \neq 0$ und $f(a) \neq 0$, wobei $a \in K$ eine Nullstelle von $X^2 + X + 1$ ist. Zeigen Sie, dass $f(X)$ irreduzibel ist.
- c** Zeigen Sie, dass $X^5 + 5X^4 + 3X^3 + X + 1$ in $\mathbb{Q}[X]$ irreduzibel ist.

Lösungsvorschlag zur Aufgabe (Frühjahr 2010, T1A3)

- a** Es genügt, zu zeigen, dass $(X^2 + X + 1)$ ein maximales Ideal ist. Da $\mathbb{F}_2[X]$ ein Hauptidealring ist, ist dies genau dann der Fall, wenn das Polynom $g = X^2 + X + 1$ in $\mathbb{F}_2[X]$ irreduzibel ist. Tatsächlich ist $g(0) = g(1) = 1 \neq 0$, sodass g keine Nullstellen in \mathbb{F}_2 hat und damit als Polynom vom Grad ≤ 3 irreduzibel ist.
- b** Laut Voraussetzung besitzt f keine Nullstelle in \mathbb{F}_2 , sodass f in ein Polynom von Grad 2 und eines von Grad 3 zerfallen müsste, falls es reduzibel wäre. Wir können annehmen, dass beide Faktoren irreduzibel sind (sonst gäbe es eine Zerlegung mit einem Linearfaktor, was wir bereits ausgeschlossen haben).

Wie inzwischen bekannt ist, ist aber $X^2 + X + 1$ das einzige irreduzible Polynom von Grad 2 in $\mathbb{F}_2[X]$. Wäre f also reduzibel, so müsste insbesondere $X^2 + X + 1$ ein Teiler von f sein. Damit wäre jede Nullstelle dieses Faktors auch eine Nullstelle von f . Weil aber laut Angabe $f(a) \neq 0$ für eine Nullstelle von $X^2 + X + 1$ gilt, ist dies nicht der Fall. Somit muss f irreduzibel sein.

- c** Wir wenden das Reduktionskriterium und Teil **b** an. Dazu bemerken wir zunächst, dass das Bild des angegebenen Polynoms in $\mathbb{F}_2[X]$ durch

$$h = X^5 + X^4 + X^3 + X + 1$$

gegeben ist. Die erste Voraussetzung zeigt man durch einfaches Nachrechnen: $h(1) = h(0) = 1 \neq 0$. Sei nun $a \in K$ eine Nullstelle von $X^2 + X + 1$. Dann gilt $a^2 + a + 1 = 0$. Wir erhalten

$$h(a) = a^5 + a^4 + a^3 + a + 1 = a^3(a^2 + a + 1) + a + 1 = a + 1.$$

Aus $h(a) = 0$ würde somit aber $a = -1 = 1$ folgen, was wir jedoch bereits ausgeschlossen hatten. Somit ist $h(a) \neq 0$ für eine Nullstelle a von $X^2 + X + 1$ und mit Teil **b** folgt die Irreduzibilität von h in $\mathbb{F}_2[X]$. Aus dem Reduktionskriterium folgt daraus wiederum, dass das angegebene Polynom in $\mathbb{Q}[X]$ irreduzibel ist.

Aufgabe (Frühjahr 2011, T2A2)

- a** Sei $P = \sum_{i=0}^n a_i X^i \in \mathbb{Z}[X]$ ein Polynom mit $a_n \neq 0$. Zeigen Sie: Ist $\frac{p}{q}$ eine rationale Nullstelle von P , und sind p und q teilerfremde ganze Zahlen, dann gilt $q \mid a_n$ und $p \mid a_0$.

- b** Bestimmen Sie die rationalen Nullstellen und deren Vielfachheiten von

$$P = X^4 - 2X^3 + 3X^2 - 4X + 2$$

und zerlegen Sie P in irreduzible reelle Polynome.

- c** Sei $Q_a = X^3 + 2X + a$. Bestimmen Sie alle $a \in \mathbb{R}$, sodass P und Q_a teilerfremd in $\mathbb{R}[X]$ sind.

Lösungsvorschlag zur Aufgabe (Frühjahr 2011, T2A2)

- a** Ist $\frac{p}{q}$ eine rationale Nullstelle, so gilt

$$\sum_{i=0}^n a_i \left(\frac{p}{q}\right)^i = 0 \quad \Leftrightarrow \quad \sum_{i=0}^n a_i p^i q^{n-i} = 0.$$

wobei wir die Gleichung im zweiten Schritt mit q^n multipliziert haben. Reduzieren wir die letzte Gleichung modulo p (bzw. modulo q), so erhalten wir

$$a_0 q^n \equiv 0 \pmod{p} \quad \text{bzw.} \quad a_n p^n \equiv 0 \pmod{q}$$

und damit $p \mid a_0 q^n$. Da p und q teilerfremd sind, folgt hieraus $p \mid a_0$. Analog erhält man aus der zweiten Kongruenz $q \mid a_n$.

- b** Laut Teil **a** kommen als Nullstellen nur Teiler von 2, also $\pm 1, \pm 2$, in Frage. Eine schnelle Rechnung zeigt

$$P(1) = 1 - 2 + 3 - 4 + 2 = 0, \quad P(-1) = 1 + 2 + 3 + 4 + 2 \neq 0,$$

$$P(2) = 16 - 16 + 12 - 8 + 2 \neq 0, \quad P(-2) = 16 + 16 + 12 + 8 + 2 \neq 0.$$

Um zu überprüfen, ob 1 eine doppelte Nullstelle ist, berechnen wir die erste Ableitung

$$P' = 4X^3 - 6X^2 + 6X - 4, \quad P'(1) = 4 - 6 + 6 - 4 = 0.$$

Somit ist 1 tatsächlich eine doppelte Nullstelle. Polynomdivision liefert nun

$$\begin{array}{r} (X^4 - 2X^3 + 3X^2 - 4X + 2) : (X^2 - 2X + 1) = X^2 + 2 \\ \underline{- X^4 + 2X^3 - X^2} \\ 2X^2 - 4X + 2 \\ \underline{- 2X^2 + 4X - 2} \\ 0 \end{array}$$

Damit erhalten wir für P die Zerlegung

$$P = (X - 1)^2(X^2 + 2).$$

Der doppelte Linearfaktor ist als Polynom vom Grad 1 irreduzibel. Für die Irreduzibilität des hinteren Faktors genügt es, zu bemerken, dass dieser vom Grad 2 ist und über \mathbb{R} wegen $x^2 + 2 \geq 2$ für alle $x \in \mathbb{R}$ nullstellenfrei ist. Somit ist die angegebene Zerlegung diejenige von P in irreduzible Faktoren.

c Wir untersuchen die irreduziblen Faktoren einzeln. Zunächst gilt

$$Q_a = X^3 + 2X + a \equiv 1 + 2 + a \equiv a + 3 \pmod{(X - 1)}.$$

Nun gilt $(X - 1) | Q_a$ genau dann, wenn $a + 3 = 0$. Analog ist

$$Q_a = X^3 + 2X + a \equiv -2X + 2X + a \equiv a \pmod{(X^2 + 2)}$$

und somit gilt $(X^2 + 2) | Q_a$ genau dann, wenn $a = 0$. Insgesamt sind die Polynome für alle $\mathbb{R} \setminus \{-3, 0\}$ teilerfremd.

Aufgabe (Frühjahr 2007, T2A3)

Sei $R[X]$ der Polynomring über einem faktoriellen Ring R . Beweisen Sie das sogenannte Gauß'sche Lemma:

Seien $0 \neq f, g \in R[X]$. Sind f und g primitiv, so auch ihr Produkt fg . (Ein Polynom $f \neq 0$ heißt primitiv, wenn seine Koeffizienten teilerfremd sind.)

Lösungsvorschlag zur Aufgabe (Frühjahr 2007, T2A3)

Nehmen wir an, es gibt einen gemeinsamen, echten Teiler der Koeffizienten von fg . Insbesondere werden diese dann von einem Primelement p in R geteilt. Da (p) ein Primideal ist, handelt es sich bei $R/(p)$ um einen Integritätsbereich. Nun betrachten wir den Homomorphismus

$$\phi: R[X] \rightarrow R/(p)[X], \quad \sum_{k=0}^n a_k X^k \mapsto \bar{a}_k X^k,$$

wobei \bar{a}_k die Nebenklasse $a_k + (p)$ bezeichnet. Mit $R/(p)$ ist auch $R/(p)[X]$ ein Integritätsbereich. Nun gilt aber $\phi(f), \phi(g) \neq 0$, da jeweils mindestens einer der Koeffizienten nicht durch p teilbar, also nicht kongruent zu 0 mod p ist. Zugleich gilt aber $\phi(f)\phi(g) = \phi(fg) = 0$, da in diesem Polynom alle Koeffizienten kongruent zu 0 mod p sind. Damit handelt es sich bei $\phi(f)$ aber um einen Nullteiler $\neq 0$. Dies ist in einem Integritätsbereich nicht möglich.

Aufgabe (Frühjahr 2015, T2A3)

Sei p eine Primzahl und $a \in \mathbb{Z}$ keine p -te Potenz in \mathbb{Z} . Man zeige, dass das Polynom $X^p - a$ über \mathbb{Q} irreduzibel ist.

Hinweis Betrachte die Nullstellen von $X^p - a$ in \mathbb{C} und untersuche den konstanten Term eines echten Teilers von $X^p - a$ auf Ganzzahligkeit.

Lösungsvorschlag zur Aufgabe (Frühjahr 2015, T2A3)

Als primitives Polynom ist $X^p - a$ nach Proposition 2.23 genau dann irreduzibel über \mathbb{Q} , wenn es bereits über \mathbb{Z} irreduzibel ist. Wir nehmen nun deshalb an, dass es einen echten Teiler f von $X^p - a$ in $\mathbb{Z}[X]$ gibt und betrachten den konstanten Term $c \in \mathbb{Z}$ dieses Teilers.

Sei ξ eine primitive p -te Einheitswurzel. Die Nullstellen von $X^p - a$ in \mathbb{C} sind gerade $\xi^i \sqrt[p]{a}$ mit $1 \leq i \leq p$, d. h.

$$X^p - a = \prod_{i=1}^p (X - \xi^i \sqrt[p]{a})$$

und der Teiler f ist das Produkt von k dieser Faktoren für ein $1 \leq k < p$. Es gibt deshalb eine k -elementige Teilmenge $I \subsetneq \{1, \dots, p\}$, sodass

$$f = \prod_{i \in I} (X - \xi^i \sqrt[p]{a}).$$

Dies bedeutet für den konstanten Term gerade $c = (-1)^k \prod_{i \in I} \xi^i \sqrt[p]{a}$. Nun ist

$$|c| = \left| \prod_{i \in I} \xi^i \sqrt[p]{a} \right| = \prod_{i \in I} |\xi^i| \cdot |\sqrt[p]{a}| = |\sqrt[p]{a}|^{|I|} = \sqrt[p]{|a|^{|I|}} = \sqrt[p]{|a|^k}$$

und damit dies eine ganze Zahl ergibt, muss a^k eine p -te Potenz sein. Wir zeigen, dass das nicht möglich ist.

Wäre die Vielfachheit aller Primfaktoren in der Primfaktorzerlegung von a ein ganzzahliges Vielfaches von p , so wäre a eine p -te Potenz. Da letzteres laut Angabe nicht der Fall ist, gibt es einen Primfaktor q von a , dessen Vielfachheit $\nu_q(a)$ in der Primfaktorzerlegung von a nicht von p geteilt wird. Da hingegen a^k eine p -te Potenz ist, muss die Vielfachheit von q in der Zerlegung von a^k ein Vielfaches von p sein. Nun ist die Vielfachheit des Faktors q in a^k gerade $k \cdot \nu_q(a)$. Da die Primzahl p jedoch $\nu_q(a)$ nicht teilt, muss $p \mid k$ gelten und wir haben einen Widerspruch zu $1 \leq k < p$. Also muss die Annahme, dass $X^p - a$ über \mathbb{Z} zerfällt, falsch gewesen sein.

Aufgabe (Herbst 2001, T3A5)

a Zeigen Sie:

Es gibt kein Polynom $P(X) \in \mathbb{Z}[X]$, sodass $P(7) = 5$ und $P(9) = 4$ gilt.

b Zeigen Sie für $a, b \geq 3$, $a, b \in \mathbb{Z}$:

$$X(X-3)(X-a)(X-b)+1 \quad \text{ist irreduzibel in } \mathbb{Z}[X].$$

Lösungsvorschlag zur Aufgabe (Herbst 2001, T3A5)

a Nehmen wir an, es gibt ein solches Polynom $P(X) \in \mathbb{Z}[X]$ mit $P(9) = 4$ und $P(7) = 5$. Es gilt $(X-Y) \mid P(X) - P(Y)$ in $\mathbb{Z}[X, Y]$, denn es ist $X \equiv Y \pmod{X-Y}$ und somit

$$P(X) - P(Y) \equiv 0 \pmod{X-Y}.$$

Einsetzen von $X = 9$ und $Y = 7$ liefert dann

$$2 = 9 - 7 \quad \text{teilt} \quad P(9) - P(7) = 4 - 5 = -1.$$

Dies ist in \mathbb{Z} nicht möglich.

b Sei $f = X(X-3)(X-a)(X-b)+1$. Es hat f keine Nullstellen in \mathbb{Z} , denn diese müssten laut 2.22 den konstanten Koeffizienten 1 teilen. Die einzigen Kandidaten für eine Nullstelle sind also $+1$ und -1 . Andererseits sieht man

$$|f(1) - 1| = |-2(1-a)(1-b)| \geq 2 \cdot 2 \cdot 2 = 8$$

$$|f(-1) - 1| = |-4(1+a)(1+b)| \geq 4 \cdot 4 \cdot 4 = 64,$$

sodass weder 1 noch -1 Nullstellen sein können. Nehmen wir nun an, es gibt Polynome $g, h \in \mathbb{Z}[X]$ von Grad 2, sodass $f = g \cdot h$. Da f normiert ist, müssen auch g und h normiert sein. Also ist $g - h$ ein Polynom von Grad ≤ 1 . Weiter ist

$$g(0) \cdot h(0) = f(0) = 1 = f(3) = g(3) \cdot h(3),$$

also sind $g(0), h(0), g(3), h(3)$ jeweils $+1$ oder -1 , in jedem Fall aber

$$g(0) = h(0) \quad \text{und} \quad g(3) = h(3).$$

Damit hat $g - h$ mindestens die beiden verschiedenen Nullstellen 0 und 3. Da $g - h$ höchstens Grad 1 hat, muss es das Nullpolynom sein. Dies

bedeutet $g = h$ und $f = g^2$. Anders ausgedrückt:

$$\begin{aligned} X(X-3)(X-a)(X-b) + 1 &= g^2 \\ X(X-3)(X-a)(X-b) &= g^2 - 1 = (g-1)(g+1) \end{aligned}$$

Als Polynomring über einem faktoriellen Ring ist $\mathbb{Z}[X]$ faktoriell, d.h. die linke Seite der letzten Gleichung lässt sich als eindeutige Zerlegung in irreduzible Faktoren auffassen.

1. Fall: $X \mid (g-1)$. Dann muss sich $(g+1)$ aus Gründen aus zwei der Faktoren $(X-3)$, $(X-a)$ und $(X-b)$ zusammensetzen. Nach Annahme ist $g(0) - 1 = 0$, d.h. $g(0) + 1 = 2$. Vergleich des letzten Koeffizienten möglicher Zerlegungen von $g+1$ zeigt, dass dann eine der Gleichungen

$$3a = 2, \quad 3b = 2 \quad \text{oder} \quad ab = 2$$

erfüllt sein müsste. Wegen $a, b \geq 3$ ist dies jedoch nicht möglich.

2. Fall: $X \mid (g+1)$. Dann ist $g(0) + 1 = 0$, sodass $g(0) - 1 = -2$. Wie im obigen Fall betrachtet man den konstanten Term möglicher Zerlegungen von $g+1$ in die Terme $(X-3)$, $(X-a)$ und $(X-b)$. Dabei ergeben sich folgende Gleichungen

$$3a = -2 \quad 3b = -2 \quad ab = -2,$$

die wegen $a, b \geq 3$ ebenfalls nicht erfüllt sein können.

Insgesamt haben wir damit nachgewiesen, dass f kein Quadrat in $\mathbb{Z}[X]$ sein kann. Es ist daher f ein Polynom von Grad 4, das weder einen Teiler von Grad 1 noch von Grad 2 hat. Somit ist f irreduzibel.

Aufgabe (Frühjahr 2000, T1A1)

Weisen Sie für eine Primzahl p die Äquivalenz folgender Aussagen nach:

- a** $f = X^2 + 2X + 2$ ist irreduzibel über dem Körper mit p^3 Elementen.
- b** $p \equiv 3 \pmod{4}$.

Lösungsvorschlag zur Aufgabe (Frühjahr 2000, T1A1)

Für $p = 2$ ist

$$f = X^2 + \bar{2}X + \bar{2} = X^2 \in \mathbb{F}_{2^3}$$

reduzibel, also ist in diesem Fall die Äquivalenz erfüllt. Sei daher im Folgenden p eine ungerade Primzahl. Wir führen die Irreduzibilität von f in \mathbb{F}_{p^3} zunächst auf die Irreduzibilität über \mathbb{F}_p zurück.

Behauptung 1: Es ist f genau dann irreduzibel über \mathbb{F}_{p^3} , wenn f irreduzibel in $\mathbb{F}_p[X]$ ist.

„ \Rightarrow “: Ist klar, denn gäbe es eine echte Zerlegung von f über \mathbb{F}_p , so wäre dies insbesondere eine Zerlegung über \mathbb{F}_{p^3} und damit wäre f auch in \mathbb{F}_{p^3} reduzibel.

„ \Leftarrow “: Nach Voraussetzung ist f irreduzibel über $\mathbb{F}_p[X]$, d. h. ist α eine Nullstelle von f in einem algebraischen Abschluss von \mathbb{F}_p , so ist f das Minimalpolynom von α und es folgt $[\mathbb{F}_p(\alpha) : \mathbb{F}_p] = 2$. Wäre nun f reduzibel in $\mathbb{F}_{p^3}[X]$, so müsste f dort in Linearfaktoren zerfallen, d. h. $\alpha \in \mathbb{F}_{p^3}$. Insbesondere wäre $\mathbb{F}_p(\alpha)$ ein Teilkörper von \mathbb{F}_{p^3} , sodass also nach der Gradformel

$$2 = [\mathbb{F}_p(\alpha) : \mathbb{F}_p] \quad \text{teilt} \quad [\mathbb{F}_{p^3} : \mathbb{F}_p] = 3$$

gilt, was offensichtlich nicht sein kann. Folglich muss f irreduzibel über \mathbb{F}_{p^3} sein.

Behauptung 2: Genau dann ist f irreduzibel in $\mathbb{F}_p[X]$, wenn $p \equiv 3 \pmod{4}$.

Als Polynom von Grad 2 ist f genau dann irreduzibel in $\mathbb{F}_p[X]$, wenn f keine Nullstelle in \mathbb{F}_p besitzt. Sei $\alpha \in \overline{\mathbb{F}_p}$ eine Nullstelle von f in einem algebraischen Abschluss von \mathbb{F}_p . Dann gilt

$$(\alpha + 1)^2 = \alpha^2 + \bar{2}\alpha + \bar{1} = f(\alpha) - \bar{1} = -\bar{1}.$$

Liegt α in \mathbb{F}_p , so ist also $-\bar{1}$ ein Quadrat in \mathbb{F}_p . Gibt es umgekehrt ein Element $\beta \in \mathbb{F}_p$ mit $\beta^2 = -\bar{1}$, so gilt

$$f(\beta - \bar{1}) = (\beta - 1)^2 + \bar{2}(\beta - \bar{1}) + 2 = \beta^2 - 2\beta + \bar{1} + 2\beta - \bar{2} + 2 = -\bar{1} + \bar{1} = \bar{0},$$

sodass f eine Nullstelle in \mathbb{F}_p besitzt. Wir haben damit gezeigt, dass f genau dann irreduzibel über \mathbb{F}_p ist, wenn $-\bar{1}$ kein Quadrat in \mathbb{F}_p ist. Letzteres ist genau dann der Fall, wenn für das Legendre-Symbol gilt, dass

$$\left(\frac{-1}{p} \right) = -1 \quad \Leftrightarrow \quad (-1)^{\frac{p-1}{2}} = -1.$$

Dabei haben wir 2.19 verwendet. Damit die letzte Bedingung erfüllt ist, muss der Exponent ungerade sein, sodass dies wiederum äquivalent ist zu

$$\frac{p-1}{2} \equiv 1 \pmod{2} \quad \Leftrightarrow \quad p-1 \equiv 2 \pmod{4} \quad \Leftrightarrow \quad p \equiv 3 \pmod{4}.$$

3. Algebra: Körper- und Galois-Theorie

3.1. Algebraische Körpererweiterungen

Eine *Körpererweiterung* $L|K$ ist ein Paar von Körpern K bzw. L mit $K \subseteq L$. Ein *Zwischenkörper* dieser Erweiterung ist ein Körper M mit $K \subseteq M \subseteq L$.

Definition 3.1. Sei $L|K$ eine Körpererweiterung.

- (1) Die Dimension von L als K -Vektorraum wird *Grad* von L über K genannt und mit $[L : K]$ bezeichnet.
- (2) Falls $[L : K]$ endlich bzw. unendlich ist, so heißt $L|K$ endliche bzw. unendliche Körpererweiterung.

Lemma 3.2 (Gradformel). Es sei $L|K$ eine Körpererweiterung und M ein Zwischenkörper. Dann gilt

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

Insbesondere ist $L|K$ genau dann endlich, wenn die Erweiterungen $L|M$ und $M|K$ beide endlich sind.

Definition 3.3. Sei $L|K$ eine Körpererweiterung.

- (1) Ein Element $\alpha \in L$ heißt *algebraisch* über K , wenn es ein Polynom $f \in K[X]$ mit $f(\alpha) = 0$ gibt und andernfalls *transzendent* über K .
- (2) Ist jedes Element aus L algebraisch über K , so heißt $L|K$ algebraische Körpererweiterung.

Aufgabe (Frühjahr 2003, T1A3)

Sei K eine algebraische Erweiterung des Körpers k und R ein Ring mit $k \subset R \subset K$. Folgt dann, dass R ein Körper ist?

Lösungsvorschlag zur Aufgabe (Frühjahr 2003, T1A3)

Wir zeigen, dass R tatsächlich bereits ein Körper sein muss. Sei $r \in R$ ein Element mit $r \neq 0$. Es ist dann r invertierbar in K , d. h. $r^{-1} \in K$ und da $K|k$ algebraisch ist, gibt es eine Gleichung

$$r^{-n} + a_{n-1}r^{-n+1} + \dots + a_1r^{-1} + a_0 = 0$$

mit Koeffizienten a_i aus k . Multiplizieren mit r^{n-1} liefert dann

$$r^{-1} + a_{n-1} + \dots + a_1 r^{n-2} + a_0 r^{n-1} = 0.$$

$$\Leftrightarrow r^{-1} = -(a_{n-1} + \dots + a_1 r^{n-2} + a_0 r^{n-1}) \in R$$

Also sind alle Elemente aus $R \setminus \{0\}$ invertierbar in R und R ist ein Körper.

Die nächste Aussage lässt sich umgangssprachlich als „algebraisch über algebraisch ist algebraisch“ zusammenfassen.

Proposition 3.4. Sei $L|K$ eine Körpererweiterung und M ein Zwischenkörper. Ist $\alpha \in L$ algebraisch über M und $M|K$ algebraisch, so ist α auch algebraisch über K . Somit ist $L|K$ genau dann algebraisch, wenn $L|M$ und $M|K$ algebraisch sind.

Dass $\alpha \in L$ algebraisch über K ist, ist äquivalent dazu, dass der Einsetzungshomomorphismus

$$\varphi_\alpha: K[X] \rightarrow L, \quad f \mapsto f(\alpha)$$

nicht injektiv ist. Da $K[X]$ ein Hauptidealring ist, gibt es ein nicht-konstantes Polynom $f \in K[X]$ mit $\ker \varphi_\alpha = (f)$. Stellen wir zusätzlich die Forderung, dass f ein normiertes Polynom ist, so ist dieses eindeutig mit dieser Eigenschaft. Wir bezeichnen es als **Minimalpolynom** von α über K .

Anhand dieser Definition des Minimalpolynoms sieht man sofort, dass jedes Polynom $g \in K[X]$ mit $g(\alpha) = 0$ vom Minimalpolynom von α über K geteilt wird.

Proposition 3.5. Sei $L|K$ eine Körpererweiterung, $\alpha \in L$ algebraisch über K und $f \in K[X]$ ein Polynom. Dann sind äquivalent:

- (1) f ist das Minimalpolynom von α über K ,
- (2) f ist ein normiertes und irreduzibles Polynom mit $f(\alpha) = 0$,
- (3) f ist normiert und das Polynom minimalen Grades mit $f(\alpha) = 0$,
- (4) f ist normiert und erzeugt den Kern des Einsetzungshomomorphismus $\varphi_\alpha: K[X] \rightarrow L$.

Eine wichtige Klasse von Erweiterungen sind die **einfachen** Erweiterungen, also Erweiterungen $L|K$, bei denen es ein $\alpha \in L$ mit $L = K(\alpha)$ gibt. In Aufgabe F03T1A3 auf Seite 149 haben wir gesehen, dass $K[\alpha] = K(\alpha)$ gilt, falls α algebraisch über K ist und, dass $K(\alpha)$ bereits von $1, \alpha, \dots, \alpha^{n-1}$ über K erzeugt wird, wobei n den Grad des Minimalpolynoms von α über K bezeichnet. Wären $1, \alpha, \dots, \alpha^{n-1}$ über K linear abhängig, so gäbe es $a_0, \dots, a_{n-1} \in K$, die nicht alle 0 sind, mit

$$a_0 + a_1 \alpha + \dots + a_{n-1} \alpha^{n-1} = 0.$$

In diesem Fall wäre dann $f = \sum_{i=0}^{n-1} a_i X^i$ ein Polynom von Grad $\leq n-1$, das α als Nullstelle hat. Dies ist ein Widerspruch dazu, dass n als Grad des Minimalpolynoms von α über K der minimale Grad ist, den ein Polynom aus $K[X]$ mit Nullstelle α haben kann.

Wir haben daher gezeigt, dass $\{1, \alpha, \dots, \alpha^{n-1}\}$ eine K -Basis von $K(\alpha)$ ist, sodass

$$[K(\alpha) : K] = n.$$

Proposition 3.6. Sei $L|K$ eine Körpererweiterung. Dann sind gleichwertig:

- (1) $L|K$ ist eine endliche Erweiterung,
- (2) $L|K$ ist endlich erzeugt und algebraisch,
- (3) L wird über K von endlich vielen algebraischen Elementen erzeugt.

Aufgabe (Herbst 2014, T1A3)

Es sei $K \subseteq L$ eine Körpererweiterung, und es seien $\alpha, \beta \in L$, so dass $\alpha + \beta$ und $\alpha\beta$ beide algebraisch sind. Zeigen Sie, dass dann auch α und β algebraisch über K sind.

Lösungsvorschlag zur Aufgabe (Herbst 2014, T1A3)

α und β sind jeweils Nullstellen des Polynoms

$$(X - \alpha)(X - \beta) = X^2 - (\alpha + \beta)X + \alpha\beta \in K(\alpha + \beta, \alpha\beta)[X]$$

und damit algebraisch über $K(\alpha + \beta, \alpha\beta)$. Nach Proposition 3.6 ist die Erweiterung $K(\alpha + \beta, \alpha\beta)|K$ algebraisch, weswegen nach Proposition 3.4 die Elemente α und β auch algebraisch über K sind.

Anleitung: Berechnung von Körpererweiterungsgraden

In vielen Aufgaben wird es nötig sein, Körpererweiterungsgrade zu bestimmen. Wir sammeln hier deshalb einige in diesem Zusammenhang häufig verwendeten Techniken.

- (1) Der Körpererweiterungsgrad $[K(\alpha) : K]$ mit einem über K algebraischen Element α entspricht dem Grad des Minimalpolynoms von α über K .
- (2) Erweiterungsgrade der Form $[K(\alpha, \beta) : K]$ können eventuell schrittweise bestimmt werden: Die Grade $n = [K(\alpha) : K]$ und $m = [K(\beta) : K]$ lassen sich nach (1) bestimmen und sind nach der Gradformel aus Lemma 3.2 jeweils Teiler von $[K(\alpha, \beta) : K]$, sodass dieser größer oder gleich dem $\text{kgV}(n, m)$ sein muss.

Andererseits ist das Minimalpolynom von β über $K(\alpha)$ ein Teiler des Minimalpolynoms von β über K , sodass $[K(\alpha)(\beta) : K(\alpha)] = [K(\alpha, \beta) : K(\alpha)]$ ein Teiler von $m = [K(\beta) : K]$ ist. Die Gradformel beschert uns somit die Abschätzung $[K(\alpha, \beta) : K] \leq n \cdot m$.

Falls n und m teilerfremd sind, liefern uns diese beiden Abschätzungen sofort $[K(\alpha, \beta) : K] = n \cdot m$. Andernfalls kann man versuchen, das Minimalpolynom von α über $K(\beta)$ bzw. von β über $K(\alpha)$ genauer zu bestimmen.

- (3) Möchte man an einer gewissen Stelle $\mathbb{Q}(\alpha) = L$ (also $[L : \mathbb{Q}(\alpha)] = 1$) ausschließen, so bietet sich oft folgendes Argument an: Ist $\alpha \in \mathbb{R}$, so ist auch $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$. Falls also $L \not\subseteq \mathbb{R}$ ist, hat man bereits einen Widerspruch erhalten.

Aufgabe (Herbst 2015, T2A4)

Sei $L|K$ eine Körpererweiterung und seien $\alpha, \beta \in L$ algebraisch über K . Sei f das Minimalpolynom von α über K und g das Minimalpolynom von β über K . Zeigen Sie, dass f irreduzibel über $K(\beta)$ ist genau dann, wenn g irreduzibel über $K(\alpha)$ ist.

Lösungsvorschlag zur Aufgabe (Herbst 2015, T2A4)

Sei $n = \text{grad } f = [K(\alpha) : K]$ und $m = \text{grad } g = [K(\beta) : K]$.

„ \Rightarrow “: Nach Voraussetzung ist f irreduzibel über $K(\beta)$ und somit das Minimalpolynom von α über $K(\beta)$, sodass $[K(\alpha, \beta) : K(\beta)] = n$ gilt. Daher erhält man unter Verwendung der Gradformel aus Lemma 3.2

$$[K(\alpha, \beta) : K(\alpha)] = \frac{[K(\alpha, \beta) : K]}{[K(\alpha) : K]} = \frac{[K(\alpha, \beta) : K(\beta)] \cdot [K(\beta) : K]}{[K(\alpha) : K]} = \frac{n \cdot m}{n} = m.$$

Das bedeutet, dass das Minimalpolynom von β über $K(\alpha)$ den Grad m haben muss. Da dies genau der Grad von g ist und g normiert ist, handelt es sich bei g um eben jenes Minimalpolynom. Insbesondere ist g irreduzibel über $K(\alpha)$.

„ \Leftarrow “: Vollkommen analog.

Aufgabe (Frühjahr 2015, T3A4)

Im Folgenden ist jeweils $L|K$ eine Körpererweiterung und ein Element $\alpha \in L$ gegeben. Bestimmen Sie jeweils das Minimalpolynom von α über dem Grundkörper K (mit Nachweis!).

- a** $K = \mathbb{Q}, L = \mathbb{C}$ und $\alpha = \sqrt{2} + \sqrt{3}$.
- b** $K = \mathbb{F}_3, L = \overline{\mathbb{F}_3}$ ein algebraischer Abschluss von \mathbb{F}_3 und α eine Nullstelle von $X^6 + 1$.
- c** $K = \mathbb{Q}(\zeta + \zeta^{-1}), L = \mathbb{Q}(\zeta)$ und $\alpha = \zeta \in \mathbb{C}$ eine primitive p -te Einheitswurzel, wobei $p \geq 3$ eine Primzahl bezeichne.

Lösungsvorschlag zur Aufgabe (Frühjahr 2015, T3A4)

- a** Wir berechnen zunächst

$$\begin{aligned}\alpha &= \sqrt{2} + \sqrt{3} \Rightarrow \alpha^2 = 2 + 2\sqrt{6} + 3 \Rightarrow \alpha^2 - 5 = 2\sqrt{6} \\ &\Rightarrow \alpha^4 - 10\alpha^2 + 25 = 24 \Rightarrow \alpha^4 - 10\alpha^2 + 1 = 0\end{aligned}$$

und wissen somit, dass $f = X^4 - 10X^2 + 1$ zumindest ein normiertes Polynom ist, das α als Nullstelle besitzt. Es bleibt zu zeigen, dass dieses irreduzibel über \mathbb{Q} ist.

Nach Lemma 2.22 wäre eine rationale Nullstelle ganzzahlig und ein Teiler von 1. Man überprüft jedoch unmittelbar, dass ± 1 keine Nullstellen von f sind. Wäre f dennoch reduzibel über \mathbb{Q} so müsste f in zwei quadratische Polynome zerfallen. Wegen Lemma 2.24 können wir sogar annehmen, dass diese beiden Faktoren in $\mathbb{Z}[X]$ liegen. Es gäbe also eine Darstellung der Form

$$\begin{aligned}X^4 - 10X^2 + 1 &= (X^2 + bX + c)(X^2 + eX + f) = \\ &= X^4 + (b+e)X^3 + (c+f+be)X^2 + (bf+ce)X + cf.\end{aligned}$$

Koeffizientenvergleich liefert die Gleichungen

$$(I) \quad b + e = 0, \quad (II) \quad c + f + be = -10, \quad (III) \quad bf + ce = 0, \quad (IV) \quad cf = 1.$$

Die letzte Gleichung (IV) impliziert über \mathbb{Z} bereits $c, f \in \{\pm 1\}$. Gleichung (I) bedeutet $b = -e$. Setzen wir beides in Gleichung (II) ein, so erhalten wir

$$c + f - b^2 = -10 \Leftrightarrow b^2 = 10 + c + f$$

und damit $b^2 \in \{8, 10, 12\}$. Da jedoch keine dieser Zahlen ein Quadrat in \mathbb{Z} ist, lässt sich die Gleichung nicht lösen. Damit ist f irreduzibel über \mathbb{Q} und somit das Minimalpolynom.

- b** Im Ring $\mathbb{F}_3[X]$ gilt (vgl. Seite 206), dass

$$(X^2 + \bar{1})^3 = X^6 + \bar{1}.$$

Somit ist α bereits eine Nullstelle von $g = X^2 + 1$. Da g keine Nullstellen in \mathbb{F}_3 besitzt, ist es dort irreduzibel und somit das Minimalpolynom zu α über \mathbb{F}_3 .

c ζ ist eine Nullstelle von

$$g = (X - \zeta)(X - \zeta^{-1}) = X^2 - (\zeta + \zeta^{-1})X + 1 \in \mathbb{Q}(\zeta + \zeta^{-1})[X].$$

Das Minimalpolynom f von ζ über K muss daher ein Teiler von g sein, weswegen $[L : K] = \text{grad } f \leq 2$ gilt. Wäre $\text{grad } f = 1$, so wäre $[L : K] = 1$, d.h. $L = K$. Allerdings liegt für $p \geq 3$ jede primitive p -te Einheitswurzel nicht in \mathbb{R} , denn

$$\zeta^p = 1 \Rightarrow |\zeta|^p = 1 \Rightarrow |\zeta| = 1$$

hat über \mathbb{R} nur die Lösungen ± 1 . Im Gegensatz dazu ist $\zeta + \zeta^{-1}$ immer reell: Aus $1 = |\zeta|^2 = \zeta \cdot \bar{\zeta}$ folgt $\zeta^{-1} = \bar{\zeta}$ und somit

$$\overline{\zeta + \bar{\zeta}} = \zeta + \bar{\zeta}.$$

Also ist $\zeta + \bar{\zeta}$ invariant unter komplexer Konjugation und muss in \mathbb{R} liegen. Daher ist K ein Teilkörper der reellen Zahlen. Wäre $L = K$, so wäre auch $\zeta \in K \subseteq \mathbb{R}$ im Widerspruch zu $\zeta \notin \mathbb{R}$.

Insgesamt haben wir gezeigt, dass $\text{grad } f = 1$ nicht möglich ist, sodass $\text{grad } f = 2$ sein muss. Es sind f und g also normierte Polynome gleichen Grades, weswegen $f \mid g$ sogar den Schluss $f = g$ zulässt.

3.2. Normale und separable Erweiterungen

Jeder Körper K besitzt einen Erweiterungskörper \bar{K} mit der Eigenschaft, dass die Erweiterung $\bar{K}|K$ algebraisch ist und jedes nicht-konstante Polynom aus $K[X]$ über \bar{K} in Linearfaktoren zerfällt. Ein solcher Erweiterungskörper heißt *algebraischer Abschluss* von K .

Um ein einzelnes nicht-konstantes Polynom $f \in K[X]$ zu untersuchen ist es dagegen zielführender, sich den *kleinsten* Erweiterungskörper von K anzusehen, über dem f in Linearfaktoren zerfällt. Dieser heißt Zerfällungskörper von f über K und ist ein deutlich handhabbareres Objekt als der algebraische Abschluss \bar{K} von K .

Definition 3.7. Sei K ein Körper und $f \in K[X]$ ein nicht-konstantes Polynom. Ein Erweiterungskörper L von K wird **Zerfällungskörper** von f über K genannt, falls

- (1) f über L in Linearfaktoren zerfällt, d. h. es gibt $\alpha_1, \dots, \alpha_n \in L$ und $c \in K^\times$ mit

$$f = c \prod_{i=1}^n (X - \alpha_i),$$

- (2) L über K von Nullstellen von f erzeugt wird.

Fixiert man einen algebraischen Abschluss \bar{K} von K , so lässt sich ein Zerfällungskörper von f über K leicht angeben. Sind nämlich $\alpha_1, \dots, \alpha_n \in \bar{K}$ die Nullstellen von f , dann ist

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

der eindeutige Zerfällungskörper von f über K in \bar{K} . Verändert man die Wahl des algebraischen Abschlusses, so erhält man mittels der beschriebenen Konstruktion einen weiteren Zerfällungskörper von f über K , der jedoch zu L isomorph ist. Da jeder Zerfällungskörper von f über K in einem algebraischen Abschluss von K liegt, hat jeder Zerfällungskörper von f diese Form.

Aufgabe (Frühjahr 2007, T3A5)

Gegeben sei das Polynom $f = X^4 - 3 \in \mathbb{Q}[X]$.

- a Beweisen Sie, dass $L = \mathbb{Q}(\sqrt[4]{3}, i)$ Zerfällungskörper von f ist.
- b Bestimmen Sie den Grad der Körpererweiterung $L|\mathbb{Q}$.
- c Beweisen Sie: $a = \sqrt[4]{3} + i$ ist ein primitives Element von L über \mathbb{Q} .

Lösungsvorschlag zur Aufgabe (Frühjahr 2007, T3A5)

- a Die Nullstellen von f sind durch die Elemente

$$\pm\sqrt[4]{3}, \pm i\sqrt[4]{3}$$

gegeben. Wir zeigen $L = \mathbb{Q}(\sqrt[4]{3}, i\sqrt[4]{3})$. Die Inklusion „ \supseteq “ ist klar. Für die andere Richtung bemerke, dass laut Definition $\sqrt[4]{3} \in L$ gilt und außerdem $i = \frac{i\sqrt[4]{3}}{\sqrt[4]{3}} \in \mathbb{Q}(\sqrt[4]{3}, i\sqrt[4]{3})$ gilt.

- b Laut der Gradformel 3.2 gilt:

$$[L : \mathbb{Q}] = [L : \mathbb{Q}(\sqrt[4]{3})] \cdot [\mathbb{Q}(\sqrt[4]{3}) : \mathbb{Q}]$$

Um den zweiten Grad zu bestimmen, bemerken wir, dass es sich bei f um ein normiertes Polynom handelt, das $f(\sqrt[4]{3}) = 0$ erfüllt und laut dem Eisensteinkriterium 2.25 irreduzibel ist. Also ist f das Minimalpolynom von $\sqrt[4]{3}$ über \mathbb{Q} und es gilt $[\mathbb{Q}(\sqrt[4]{3}) : \mathbb{Q}] = \text{grad } f = 4$.

Weiter ist $g = x^2 + 1$ das Minimalpolynom von i über $\mathbb{Q}(\sqrt[4]{3})$: Das Polynom g ist normiert und hat i als Nullstelle. Da $\mathbb{Q}(\sqrt[4]{3})$ ein Teilkörper der reellen Zahlen ist, hat g über diesem keine Nullstellen, ist wegen $\text{grad } g = 2$ also irreduzibel. Es folgt

$$[L : \mathbb{Q}] = [L : \mathbb{Q}(\sqrt[4]{3})] \cdot [\mathbb{Q}(\sqrt[4]{3}) : \mathbb{Q}] = 2 \cdot 4 = 8.$$

c Wir zeigen $\mathbb{Q}(\sqrt[4]{3}, i) = \mathbb{Q}(\sqrt[4]{3} + i)$.

Die Inklusion „ \supseteq “ ist klar. Für „ \subseteq “ berechnen wir zunächst mit $a = \sqrt[4]{3} + i$:

$$\begin{aligned} (a - i)^4 &= 3 \quad\Leftrightarrow\quad a^4 - 4a^3i + 6a^2i^2 - 4ai^3 + i^4 = 3 \\ \Leftrightarrow \quad a^4 - 4a^3i - 6a^2 + 4ai + 1 &= 3 \quad\Leftrightarrow\quad -4a^3i + 4ai = -a^4 + 6a^2 + 2. \end{aligned}$$

Es gilt $-4a^3 + 4a = 4a(-a^2 + 1) = 4a(1 + a)(1 - a) \neq 0$ und somit erhalten wir

$$i = \frac{-a^4 + 6a^2 + 2}{-4a^3 + 4a} \in \mathbb{Q}(a) = \mathbb{Q}(\sqrt[4]{3} + i)$$

Daraus folgt natürlich $\sqrt[4]{3} = a - i \in \mathbb{Q}(a)$ und damit insgesamt die gewünschte Gleichung.

Aufgabe (Herbst 2002, T1A3)

- a** Zerlegen Sie das Polynom $f := X^6 + 4X^4 + 4X^2 + 3 \in \mathbb{Q}[X]$ in irreduzible Faktoren.
- b** Bestimmen Sie den Zerfällungskörper von f über \mathbb{Q} und $[Z : \mathbb{Q}]$.

Lösungsvorschlag zur Aufgabe (Herbst 2002, T1A3)

- a** Da nur gerade Potenzen von X in f auftreten, klammern wir zunächst X^2 aus:

$$\begin{aligned} f &= X^6 + X^4 + X^2 + 3X^4 + 3X^2 + 3 = \\ &= X^2(X^4 + X^2 + 1) + 3(X^4 + X^2 + 1) = (X^2 + 3)(X^4 + X^2 + 1) \end{aligned}$$

Den zweiten Faktor zerlegen wir noch mittels quadratischer Ergänzung und der dritten binomischen Formel:

$$\begin{aligned} X^4 + X^2 + 1 &= X^4 + 2X^2 + 1 - X^2 = (X^2 + 1)^2 - X^2 = \\ &= (X^2 + X + 1)(X^2 - X + 1). \end{aligned}$$

Somit gilt insgesamt

$$f = (X^2 + 3)(X^2 + X + 1)(X^2 - X + 1).$$

Wir zeigen noch, dass diese drei Faktoren tatsächlich irreduzibel sind: Für den ersten Faktor folgt dies aus dem Eisenstein-Kriterium mit $p = 3$. Da die anderen beiden (ebenfalls) Grad zwei haben, genügt es hier zu zeigen, dass diese keine rationale Nullstellen haben. Dafür kämen laut Lemma 2.22 nur Teiler des konstanten Gliedes in Frage, da es sich jeweils um ein normiertes Polynom mit ganzzahligen Koeffizienten handelt. Man überprüft jedoch leicht, dass weder im zweiten noch im dritten Faktor ± 1 eine Nullstelle ist.

- b** Wir berechnen zunächst alle Nullstellen von f . Unter Zuhilfenahme der Mitternachtsformel ergeben sich die Nullstellen

$$\{\alpha_1, \dots, \alpha_6\} = \left\{ \pm\sqrt{-3}, \frac{-1 \pm \sqrt{-3}}{2}, \frac{1 \pm \sqrt{-3}}{2} \right\}.$$

Alle Nullstellen lassen sich durch rationale Operationen aus der ersten darstellen, somit gilt $\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6) = \mathbb{Q}(\alpha_1)$. Daraus folgt, dass

$$Z = \mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(i\sqrt{3})$$

ein Zerfällungskörper von f ist.

Um dessen Erweiterungsgrad über \mathbb{Q} zu bestimmen, bestimmen wir das Minimalpolynom von $i\sqrt{3}$ über \mathbb{Q} . Mit $X^2 + 3$ ist zumindest ein normiertes Polynom gefunden, das $i\sqrt{3}$ als Nullstelle hat. Laut dem Eisenstein-Kriterium ist dieses außerdem irreduzibel. Es folgt $[Z : \mathbb{Q}] = \text{grad}(X^2 + 3) = 2$.

Aufgabe (Herbst 2001, T3A4)

Sei $\alpha = \sqrt{2 + \sqrt[3]{2}} \in \mathbb{R}$ die positive Quadratwurzel von $2 + \sqrt[3]{2}$.

- a** Bestimmen Sie das Minimalpolynom f von α über \mathbb{Q} und den Grad $[\mathbb{Q}(\alpha) : \mathbb{Q}]$.
b Geben Sie alle Nullstellen von f in \mathbb{C} an. Ist $\mathbb{Q}(\alpha)$ ein Zerfällungskörper von f ?

Lösungsvorschlag zur Aufgabe (Herbst 2001, T3A4)

a Wir berechnen:

$$\begin{aligned}\alpha &= \sqrt[3]{2 + \sqrt[3]{2}} \Rightarrow \alpha^2 - 2 = \sqrt[3]{2} \Rightarrow (\alpha^2 - 2)^3 = 2 \\ \Leftrightarrow \alpha^6 - 6\alpha^4 + 12\alpha^2 - 8 &= 2 \Leftrightarrow \alpha^6 - 6\alpha^4 + 12\alpha^2 - 10 = 0\end{aligned}$$

Somit ist $f(X) = X^6 - 6X^4 + 12X^2 - 10$ ein normiertes Polynom mit α als Nullstelle. Zudem ist dieses nach dem Eisenstein-Kriterium mit $p = 2$ irreduzibel, also das Minimalpolynom von α über \mathbb{Q} . Daraus folgt

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = \text{grad } f = 6.$$

b Ist β eine Nullstelle von $f(x)$, so gilt gemäß der Äquivalenzen aus Teil **a**, dass $(\beta^2 - 2)^3 = 2$. Deshalb muss gelten, dass

$$\beta^2 - 2 = \sqrt[3]{2} \quad \text{oder} \quad \beta^2 - 2 = \zeta \sqrt[3]{2} \quad \text{oder} \quad \beta^2 - 2 = \zeta^2 \sqrt[3]{2},$$

wobei ζ eine primitive dritte Einheitswurzel bezeichnet. Man erhält die Lösungen

$$\{\beta_1, \dots, \beta_6\} = \left\{ \pm \sqrt{2 + \sqrt[3]{2}}, \pm \sqrt{2 + \zeta \sqrt[3]{2}}, \pm \sqrt{2 + \zeta^2 \sqrt[3]{2}} \right\}.$$

Somit haben wir 6 verschiedene Nullstellen von f gefunden, wegen $\text{grad } f = 6$ kann es keine weiteren geben.

$\mathbb{Q}(\alpha)$ ist *kein* Zerfällungskörper von f . Wäre dies der Fall, so müsste $\mathbb{Q}(\alpha)$ alle Nullstellen von f enthalten. Es gilt aber beispielsweise $\beta_3 \in \mathbb{C} \setminus \mathbb{R}$ und $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$.

Normale Erweiterungen

Definition 3.8. Eine algebraische Körpererweiterung $L|K$ heißt *normal*, wenn sie eine der folgenden, äquivalenten Bedingungen erfüllt:

- (1) Jedes irreduzible Polynom aus $K[X]$, das in L eine Nullstelle besitzt, zerfällt über L bereits in Linearfaktoren.
- (2) Es gibt ein nicht-konstantes Polynom $f \in K[X]$, sodass L der Zerfällungskörper von f über K ist.

- (3) Für einen algebraischen Abschluss \bar{L} von L gilt die Gleichung $\text{Hom}_K(L, \bar{L}) = \text{Aut}_K(L)$, d. h. jeder K -Homomorphismus $L \rightarrow \bar{L}$ beschränkt sich zu einem K -Automorphismus von L .¹

Ist $L|K$ eine Körpererweiterung mit $[L : K] = 2$, so ist sie stets normal. Um dies zu sehen, betrachte ein irreducibles Polynom f mit Nullstelle $\alpha \in L$. Es ist dann

$$\text{grad } f = [K(\alpha) : K] \leq [L : K] = 2.$$

Da es eine Nullstelle $\alpha \in L$ gibt, haben wir über L auch eine Darstellung $f = (X - \alpha) \cdot g$ für ein Polynom $g \in L[X]$. Aus Gradgründen ist g konstant oder ein Linearfaktor, sodass wir Bedingung (1) aus Definition 3.8 nachgewiesen haben.

In der Gruppentheorie hatten wir eine ganz ähnliche Aussage (siehe Seite 8): Ist G eine Gruppe und U eine Untergruppe mit $(G : U) = 2$, so ist U ein Normalteiler von G . Diese Analogie zur Aussage oben ist kein Zufall, sondern lässt sich mithilfe der Galois-Theorie erklären (siehe Satz 3.20).

- Beispiele 3.9.** **a** Die Erweiterung $\mathbb{Q}(\sqrt[4]{2})|\mathbb{Q}$ ist nicht normal, denn das irreducibile Polynom $X^4 - 2$ hat in $\mathbb{Q}(\sqrt[4]{2})$ eine Nullstelle. Da aber auch $i\sqrt[4]{2}$ eine Nullstelle ist, die nicht im reellen Körper $\mathbb{Q}(\sqrt[4]{2})$ liegt, zerfällt $X^4 - 2$ über $\mathbb{Q}(\sqrt[4]{2})$ nicht in Linearfaktoren.
- b** Ist ζ_3 eine dritte Einheitswurzel, so ist die Erweiterung $\mathbb{Q}(\zeta_3, \sqrt[3]{2})|\mathbb{Q}$ normal, denn der Körper $\mathbb{Q}(\zeta_3, \sqrt[3]{2})$ ist der Zerfällungskörper von $X^3 - 2$ über \mathbb{Q} .

■

Separabilität

Definition 3.10. Sei $L|K$ eine Körpererweiterung.

- (1) Ein nicht-konstantes Polynom $f \in K[X]$ heißt **separabel**, wenn f in einem algebraischen Abschluss von K nur einfache Nullstellen hat.
- (2) Ein Element $a \in L$ heißt **separabel** über K , wenn a algebraisch und sein Minimalpolynom über K separabel im Sinne von Teil (1) ist.
- (3) Die gesamte Körpererweiterung $L|K$ heißt **separabel**, wenn jedes Element aus L separabel über K ist.

Ob ein Polynom $f \in K[X]$ separabel ist, lässt sich besonders einfach anhand seiner **formalen Ableitung** fest stellen. Für $f = \sum_{i=0}^n a_i X^i$ meint man damit das Polynom $f' = \sum_{i=1}^n a_i i X^{i-1}$.

¹ vgl. Seite 165 für die Definition eines K -Homomorphismus.

Lemma 3.11. Sei K ein Körper.

- (1) Ein Element $\alpha \in \bar{K}$ ist genau dann mehrfache Nullstelle eines Polynoms $f \in K[X]$, wenn $f(\alpha) = f'(\alpha) = 0$.
- (2) Ein nicht-konstantes Polynom $f \in K[X]$ ist genau dann separabel, wenn f und f' teilerfremd sind.
- (3) Ein irreduzibles Polynom $f \in K[X]$ ist genau dann separabel, wenn $f' \neq 0$.

Falls K ein Körper der Charakteristik 0 ist, so ist $f' \neq 0$ für jedes nicht-konstante Polynom $f \in K[X]$ automatisch erfüllt. Dies zeigt bereits die Hälfte der nächsten Aussage.

Proposition 3.12. Jede algebraische Körpererweiterung eines Körpers der Charakteristik 0 und jede algebraische Erweiterung eines endlichen Körpers ist separabel.

Man spricht bei Körpern, deren Erweiterungen stets separabel sind, auch von *vollkommenen* oder *perfekten Körpern*. Da es sich bei der Mehrzahl der geläufigen Körper um perfekte Körper handelt, wird man nicht-separablen Erweiterungen nur selten begegnen. Eine bekannte Ausnahme bildet die Erweiterung aus Aufgabe F14T1A5.

Proposition 3.13. Eine Körpererweiterung $L|K$ ist genau dann separabel, wenn für jeden Zwischenkörper M der Erweiterung auch die Erweiterungen $L|M$ und $M|K$ separabel sind.

Aufgabe (Frühjahr 2014, T1A5)

Es seien p eine Primzahl, \mathbb{F}_p der Körper mit p Elementen und $\mathbb{F}_p(t)$ der Quotientenkörper des Polynomrings $\mathbb{F}_p[t]$. Wie üblich sei $\mathbb{F}_p(t^p)$ der kleinste Teilkörper, der t^p enthält.

- a Zeigen Sie, dass das Polynom $X^p - t^p \in \mathbb{F}_p(t^p)[X]$ irreduzibel ist.
- b Zeigen Sie, dass die Körpererweiterung $\mathbb{F}_p(t)|\mathbb{F}_p(t^p)$ endlich und normal, aber nicht separabel ist.

Lösungsvorschlag zur Aufgabe (Frühjahr 2014, T1A5)

- a Wir wenden das Eisenstein-Kriterium an. Im Ring $\mathbb{F}_p[t^p]$ ist das Element t^p ein Primelement: Betrachte den Homomorphismus $\phi : \mathbb{F}_p[t^p] \rightarrow \mathbb{F}_p$ mit $\phi(t^p) = 0$ und $\phi|_{\mathbb{F}_p} = \text{id}$. Es ist klar, dass ϕ surjektiv ist und der Kern durch das Ideal (t^p) gegeben ist. Mit dem Homomorphiesatz für Ringe folgt die Isomorphie

$$\mathbb{F}_p[t^p]/(t^p) \cong \mathbb{F}_p.$$

Weil \mathbb{F}_p ein Körper ist, ist damit das Ideal (t^p) ein Primideal. Insbesondere folgt daraus, dass das Element t^p prim ist. Nun gilt $t^p \nmid 1, t^p \mid t^p$ und $t^{2p} \nmid t^p$, also ist das angegebene Polynom irreduzibel über $\mathbb{F}_p(t^p)[X]$ nach dem Eisenstein-Kriterium.

- b** Es ist klar, dass $\mathbb{F}_p(t) = \mathbb{F}_p(t^p)(t)$ gilt. Der Grad der Erweiterung ist also der Grad des Minimalpolynoms von t über $\mathbb{F}_p(t^p)$. Laut Teil **a** ist $f = X^p - t^p$ ein über $\mathbb{F}_p(t^p)$ irreduzibles Polynom, ferner gilt $f(t) = t^p - t^p = 0$ und f ist normiert. Wir erhalten

$$[\mathbb{F}_p(t) : \mathbb{F}_p(t^p)] = \text{grad } f = p < \infty,$$

was die Endlichkeit der Erweiterung beweist.

Um zu zeigen, dass die Erweiterung normal ist, weisen wir nach, dass $\mathbb{F}_p(t)$ der Zerfällungskörper von f ist. Es gilt

$$(X^p - t^p) = (X - t)^p,$$

mit *freshman's dream*, sodass f über $\mathbb{F}_p(t)$ in Linearfaktoren zerfällt. Die Erweiterung wird zudem von der einzigen Nullstelle t über $\mathbb{F}_p(t^p)$ erzeugt. Damit ist $\mathbb{F}_p(t)$ Zerfällungskörper von f und die Erweiterung folglich normal.

Das Element t ist eine p -fache Nullstelle seines Minimalpolynoms, sodass das Minimalpolynom von t und damit die gesamte Erweiterung nicht separabel ist.

Aufgabe (Herbst 2012, T2A2)

Sei $n \in \mathbb{N}_0$ eine natürliche Zahl. Zeigen Sie, dass das Polynom $f(X) = \sum_{k=0}^n \frac{X^k}{k!}$ keine mehrfachen Nullstellen in den komplexen Zahlen besitzt.

Lösungsvorschlag zur Aufgabe (Herbst 2012, T2A2)

Angenommen, es gibt eine mehrfache Nullstelle $\alpha \in \mathbb{C}$, d. h. $f(\alpha) = 0$ und $f'(\alpha) = 0$ nach Lemma 3.11 (1). Dann wäre auch

$$\begin{aligned} 0 = f'(\alpha) &= \sum_{k=1}^n \frac{k}{k!} \alpha^{k-1} = \sum_{k=1}^n \frac{1}{(k-1)!} \alpha^{k-1} = \sum_{k=0}^{n-1} \frac{1}{k!} \alpha^k = f(\alpha) - \frac{1}{n!} \alpha^n = -\frac{1}{n!} \alpha^n \\ &\Leftrightarrow \alpha = 0 \end{aligned}$$

Andererseits ist $f(0) = \sum_{k=0}^n \frac{1}{k!} 0^k = 1 \neq 0$. Also kann es eine solche Nullstelle nicht geben.

Aufgabe (Herbst 2010, T1A5)

Sei $K|k$ eine Körpererweiterung und $0 \neq \alpha \in K$ mit $K = k[\alpha]$. Weiter sei eine Potenz α^e (e eine positive ganze Zahl) von α in k enthalten. Sei n die minimale positive ganze Zahl mit $\alpha^n \in k$. Zeigen Sie:

- a** Ist $\alpha^m \in k$ für ein $m > 0$, so ist m ein Vielfaches von n .
- b** Ist $K|k$ eine separable Erweiterung, so ist die Charakteristik von k kein Teiler von n .

Lösungsvorschlag zur Aufgabe (Herbst 2010, T1A5)

- a** Da n minimal ist, können wir $m \geq n$ annehmen und Division mit Rest durch n durchführen. Das bedeutet, wir finden nicht-negative ganze Zahlen k, r mit $m = k \cdot n + r$ und $r < n$. Es ist nun also

$$\alpha^m = \alpha^{kn} \cdot \alpha^r \Leftrightarrow \alpha^r = \alpha^m \cdot ((\alpha^n)^k)^{-1} \in k.$$

Falls $r \neq 0$, so ist dies ein Widerspruch zur Minimalität von n . Folglich muss $m = kn$ sein, d.h. m ist Vielfaches von n .

- b** Sei $K|k$ separabel und $\text{char}(k) = p$ ein Teiler von n . Es gibt also ein $l \in \mathbb{Z}$ mit $n = l \cdot p$. Jede Zwischenerweiterung einer separablen Körpererweiterung ist nach Proposition 3.13 separabel, sodass auch $k(\alpha^l)|k$ separabel sein muss. Dies ist gleichbedeutend dazu, dass α^l separabel über k sein muss, d.h. das Minimalpolynom f von α^l über k hat nur einfache Nullstellen (in einem algebraischen Abschluss von k). Betrachte nun das Polynom $X^p - \alpha^n \in k[X]$, welches sich in $k(\alpha^l)[X]$ mithilfe des *freshman's dream* folgendermaßen zerlegen lässt:

$$X^p - \alpha^n = X^p - \alpha^{l \cdot p} = (X - \alpha^l)^p$$

Das Minimalpolynom f von α^l teilt $X^p - \alpha^n$, setzt sich also aus den Faktoren $X - \alpha^l$ zusammen. Die einzige Möglichkeit, dass f nur einfache Nullstellen hat, ist also $f = X - \alpha^l$. Dies bedeutet aber, dass $\alpha^l \in k$, was ein Widerspruch zur Minimalität von n ist. Es kann daher α^l nicht separabel über k sein, sodass auch $K|k$ nicht separabel sein kann.

Der Widerspruch zeigt, dass $\text{char}(k)$ kein Teiler von n sein kann.

Aufgabe (Herbst 2000, T1A2)

Seien a, b, c positive natürliche Zahlen. Man zeige:

- a** Das Polynom $X^a + Y^b$ ist im Polynomring $\mathbb{C}[X, Y]$ durch kein Quadrat eines Primpolynoms teilbar.
- b** Das Polynom $X^a + Y^b + Z^c$ ist irreduzibel in $\mathbb{C}[X, Y, Z]$.

Lösungsvorschlag zur Aufgabe (Herbst 2000, T1A2)

- a** Angenommen, $f = X^a + Y^b$ hat einen mehrfachen irreduziblen Faktor in $\mathbb{C}[X, Y]$, dann hat f insbesondere einen mehrfachen Faktor in $\mathbb{C}(X)[Y]$ und somit eine mehrfache Nullstelle in einem algebraischen Abschluss $\overline{\mathbb{C}(X)}$. Sei also $\alpha \in \overline{\mathbb{C}(X)}$ eine mehrfache Nullstelle von f , dann muss

$$f'(\alpha) = b\alpha^{b-1} = 0$$

gelten. Ist $b = 1$, so ist dies schon ein Widerspruch. Ist $b > 1$, so muss wegen $\text{char } \mathbb{C} = 0$ bereits $\alpha = 0$ sein. Jedoch ist $f(0) = X^a \neq 0$. Folglich kann f keinen mehrfachen Faktor haben.

- b** Sei P ein beliebiger Primfaktor von $X^a + Y^b$. Da das Polynom $X^a + Y^b$ nach Teil **a** keinen doppelten irreduziblen Faktor hat, wird es insbesondere nicht zweifach von P geteilt. Somit liefert das Eisensteinkriterium 2.25, dass das Polynom

$$g = Z^c + (X^a + Y^b) \in \mathbb{C}(X, Y)[Z]$$

irreduzibel ist. Da g primitiv ist, ist g nach dem Satz von Gauß 2.23 auch in $\mathbb{C}[X, Y, Z]$ irreduzibel.

Endliche separable Erweiterungen sind auch deshalb besonders schön, weil sie stets einfach sind, wie der nächste Satz zeigt.

Satz 3.14 (Satz vom primitiven Element). Sei $L|K$ eine endliche, separable Körpererweiterung. Dann existiert ein primitives Element der Erweiterung $L|K$, d. h. ein Element $\alpha \in L$ mit $L = K(\alpha)$.

Der Beweis des Satzes vom primitiven Element liefert sogar einen Ansatz für die Berechnung eines solchen primitiven Elements. Für eine Körpererweiterung $K(\alpha, \beta)$ lässt sich durch den Ansatz $\gamma = a\alpha + b\beta$ für geeignete $a, b \in K^\times$ stets ein Element mit $K(\alpha, \beta) = K(\gamma)$ finden – hin und wieder sind jedoch andere Ansätze, wie z. B. $\gamma = \alpha\beta$, einfacher umzusetzen.

Aufgabe (Frühjahr 2000, T2A3)

- a** Man bestimme ein primitives Element für die Körpererweiterung $\mathbb{Q}(\sqrt[3]{2}, \sqrt[4]{5})|\mathbb{Q}$.
- b** Seien x und y Unbestimmte über dem Körper \mathbb{F}_p von p Elementen. Man zeige: Die Körpererweiterung $\mathbb{F}_p(X, Y)|\mathbb{F}_p(X^p, Y^p)$ besitzt kein primitives Element.

Lösungsvorschlag zur Aufgabe (Frühjahr 2000, T2A3)

- a** Sei $\alpha = \sqrt[3]{2} \cdot \sqrt[4]{5}$. Wir zeigen, dass $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt[3]{2}, \sqrt[4]{5})$ gilt. Die Richtung „ \subseteq “ ist klar. Für die andere Richtung betrachte

$$\alpha^4 = 2 \cdot \sqrt[3]{2} \cdot 5 = 10\sqrt[3]{2}.$$

Damit ist $\sqrt[3]{2} = \frac{1}{10}\alpha^4 \in \mathbb{Q}(\alpha)$ und es folgt $\sqrt[4]{5} = \frac{\alpha}{\sqrt[3]{2}} \in \mathbb{Q}(\alpha)$. Insgesamt haben wir damit Gleichheit.

- b** Das Polynom $T^p - X^p \in \mathbb{F}_p(X^p, Y^p)[T]$ ist irreduzibel nach Eisenstein mit X^p (vgl. Aufgabe F14T1A5), daher ist $[\mathbb{F}_p(X^p, Y^p)(X) : \mathbb{F}_p(X^p, Y^p)] = p$. Genauso ist $T^p - Y^p \in \mathbb{F}_p(X, Y^p)[T]$ nach Eisenstein irreduzibel, sodass $[\mathbb{F}_p(X^p, Y^p)(Y, X) : \mathbb{F}_p(X^p, Y^p)(X)] = p$. Nach der Gradformel folgt

$$[\mathbb{F}_p(X^p, Y^p)(X, Y) : \mathbb{F}_p(X^p, Y^p)] = p^2.$$

Angenommen, es gibt ein primitives Element $\alpha \in \mathbb{F}_p(X, Y)$, dann müsste das Minimalpolynom von α (in $\mathbb{F}_p(X^p, Y^p)[T]$) Grad p^2 haben. Schreiben wir andererseits

$$\alpha = \sum_{i=0}^n \sum_{j=0}^m a_{ij} X^i Y^j,$$

so sieht man, dass bereits

$$\alpha^p = \left(\sum_{i=0}^n \sum_{j=0}^m a_{ij} X^i Y^j \right)^p = \sum_{i=0}^n \sum_{j=0}^m a_{ij}^p (X^i)^p (Y^j)^p \in \mathbb{F}_p(X^p, Y^p)$$

gilt. Das Polynom $T^p - \alpha^p$ liegt also in $\mathbb{F}_p(X^p, Y^p)[T]$ und hat α als Nullstelle, sodass das Minimalpolynom von α ein Teiler dieses Polynoms ist und folglich höchstens Grad p haben kann.

Sei $\sigma: K \rightarrow K'$ ein Körperhomomorphismus und $f = \sum_{i=0}^n a_i X^i \in K[X]$ ein Polynom mit Nullstelle $\alpha \in K$. Es gilt dann

$$0 = \sigma(0) = \sigma(f(\alpha)) = \sigma \left(\sum_{i=0}^n a_i \alpha^i \right) = \sum_{i=0}^n \sigma(a_i) \sigma(\alpha)^i,$$

d. h. $\sigma(\alpha)$ ist Nullstelle des Polynoms $f^\sigma = \sum_{i=0}^n \sigma(a_i)X^i \in K'[X]$. Wenn wir im Folgenden versuchen, den Homomorphismus σ auf einen Erweiterungskörper L von σ fortzusetzen, so muss sich diese Eigenschaft natürlich auf eine eventuelle Fortsetzung übertragen. Tatsächlich gilt in gewisser Weise sogar die Umkehrung.

Satz 3.15 (Fortsetzungssatz). Sei $L|K$ ein Körper, $\alpha \in L$ mit Minimalpolynom $f \in K[X]$ und $\sigma: K \rightarrow L'$ ein Körperhomomorphismus mit einem weiteren Körper L' . Dann gilt:

$$\begin{array}{ccc} L & & L' \\ | & & | \\ K(\alpha) & \dashrightarrow^{\tau} & \sigma(K)(\beta) \\ | & & | \\ K & \xrightarrow{\sigma} & \sigma(K) \end{array}$$

- (1) Ist $\tau: K(\alpha) \rightarrow L'$ eine Fortsetzung von σ , d. h. $\tau|_K = \sigma$, so ist $\tau(\alpha)$ eine Nullstelle von f^σ .
- (2) Ist $\beta \in L'$ eine Nullstelle von f^σ , so gibt es einen Homomorphismus $\tau: K(\alpha) \rightarrow L'$ mit $\tau(\alpha) = \beta$ und $\tau|_K = \sigma$.

Wichtigster Spezialfall der in Satz 3.15 beschriebenen Konstruktion sind Fortsetzungen der Identität id_K , welche auch als *K-Homomorphismen* bezeichnet werden. Die Menge der *K-Homomorphismen* von L nach L' bezeichnen wir als $\text{Hom}_K(L, L')$. Entsprechend ist dann $\text{Aut}_K(L)$ die Menge der *K-Automorphismen*, also der bijektiven *K-Homomorphismen* von L nach L .

Aufgabe (Frühjahr 2001, T3A1)

$K|\mathbb{Q}$ sei eine endliche Körpererweiterung vom Grad n . Zeigen Sie, dass es genau n verschiedene Körpermonomorphismen von K nach \mathbb{C} gibt und dass die Anzahl s derjenigen mit nicht-reellem Bild gerade ist. Mit $n = r + s$ weisen Sie $r = 0$ oder $s = 0$ für den Fall nach, dass $K|\mathbb{Q}$ galoissch ist, und geben Sie Beispiele für beide Fälle.

Lösungsvorschlag zur Aufgabe (Frühjahr 2001, T3A1)

Die Erweiterung $K|\mathbb{Q}$ ist endlich (laut Angabe) und separabel, da \mathbb{Q} wegen $\text{char } \mathbb{Q} = 0$ nach Proposition 3.13 ein perfekter Körper ist. Nach dem Satz vom primitiven Element existiert somit ein $\alpha \in K$ mit $K = \mathbb{Q}(\alpha)$. Ist f das Minimalpolynom von α , so gilt $\text{grad } f = [K : \mathbb{Q}] = n$. Das Minimalpolynom von α ist separabel, hat also n verschiedene Nullstellen $\alpha_1, \dots, \alpha_n$ in \mathbb{C} . Der Fortsetzungssatz 3.15 liefert somit n verschiedene \mathbb{Q} -Homomorphismen

$$\tau_i : K \rightarrow \mathbb{C} \quad \text{mit} \quad \psi_i(\alpha) = \alpha_i$$

für $i \in \{1, \dots, n\}$. Da jeder Homomorphismus von Körpern injektiv ist, handelt es sich dabei um Körpermonomorphismen.

Wir zeigen noch, dass es keine weiteren gibt. Sei dazu $\rho : K \rightarrow \mathbb{C}$ ein beliebiger Körperhomomorphismus. Aus $\rho(1) = 1$ folgert man leicht per Induktion $\rho(m) = m$ für $m \in \mathbb{Z}$ und daraus wiederum $\rho(q) = q$ für $q \in \mathbb{Q}$. Es handelt sich bei ρ also in jedem Fall um einen \mathbb{Q} -Homomorphismus. Sei nun $\beta = \rho(\alpha)$. Es gilt

$$f(\beta) = \sum_{k=0}^n a_k \beta^k = \sum_{k=0}^n a_k \rho(\alpha)^k = \rho \left(\sum_{k=0}^n a_k \alpha^k \right) = \rho(0) = 0.$$

Somit ist β eine Nullstelle von f , stimmt also mit einem α_i für $i \in \{1, \dots, n\}$ überein. Da ρ durch das Bild von α bereits eindeutig bestimmt ist, folgt $\rho = \tau_i$.

Das Bild von τ_i ist genau $K(\alpha_i)$ für $i \in \{1, \dots, n\}$. Ist also $\alpha_i \in \mathbb{R}$, so ist auch das Bild $K(\alpha_i)$ eine Teilmenge von \mathbb{R} , wohingegen Nullstellen $\alpha_i \in \mathbb{C} \setminus \mathbb{R}$ auch ein Bild $K(\alpha_i) \not\subseteq \mathbb{R}$ liefern. Da f ein Polynom mit reellen Koeffizienten ist, treten nicht-reelle Nullstellen in komplex-konjugierten Paaren auf. Insbesondere ist also die Anzahl der nicht-reellen Nullstellen und somit auch der Homomorphismen mit nicht-reellem Bild gerade.

Nehmen wir nun an, die Erweiterung $K|\mathbb{Q}$ ist galoissch, also insbesondere normal. Aus Definition 3.8 (iii) folgt, dass jedes τ_i ein \mathbb{Q} -Automorphismus ist, also gilt $K = \tau_i(K)$ für $i \in \{1, \dots, n\}$. Gilt $K \subseteq \mathbb{R}$, so folgt $\tau_i(K) \subseteq \mathbb{R}$ für alle $i \in \{1, \dots, n\}$ und $s = 0$. Andernfalls gilt $\tau_i(K) \not\subseteq \mathbb{R}$ für alle $i \in \{1, \dots, n\}$, und damit $r = 0$.

Gemäß dem eben Bewiesenen ist $\mathbb{Q}(\sqrt{2})|\mathbb{Q}$ ein Beispiel für den Fall $s = 0$ und $\mathbb{Q}(i)|\mathbb{Q}$ ein Beispiel für $r = 0$ (beides lässt sich auch leicht nachrechnen).

3.3. Einheitswurzeln

Gegenstand unserer Untersuchungen in diesem Abschnitt sind die Nullstellen des Polynoms $X^n - 1$ in einem Körper K für ein $n \in \mathbb{N}$. Man prüft leicht nach, dass diese eine Gruppe bilden, die wir mit $\mu_n(K)$ bezeichnen und die Gruppe der n -ten **Einheitswurzeln** von K nennen.

Im Fall eines algebraisch abgeschlossenen Körpers \bar{K} hat das Polynom $X^n - 1$ genau n Nullstellen in K . Ist $\text{char } \bar{K}$ kein Teiler von n , so ist das Polynom separabel und die Nullstellen sind alle verschieden. Verbunden mit der Tatsache, dass jede endliche Untergruppe der Einheitengruppe eines Körpers zyklisch ist, haben wir bewiesen:

Proposition 3.16. Sei $n \in \mathbb{N}$ und \bar{K} ein algebraisch abgeschlossener Körper, dann ist $\mu_n(\bar{K})$ eine zyklische Gruppe. Im Fall $\text{char } \bar{K} \nmid n$ (also insbesondere, wenn $\text{char } \bar{K} = 0$) hat $\mu_n(\bar{K})$ die Ordnung n .

Ein Erzeuger von $\mu_n(\overline{K})$ heißt **primitive n -te Einheitswurzel**. Im Fall $\overline{K} = \mathbb{C}$ kann man auf kanonische Weise eine solche primitive n -te Einheitswurzel angeben, nämlich $\xi_n = e^{2\pi i/n}$.

Veranschaulicht man sich n -ten Einheitswurzeln von \mathbb{C} graphisch in der Gauß'schen Zahlenoberfläche, so liegen diese in regelmäßigen Abständen über den Einheitskreis verteilt. Man spricht deshalb bei $\mathbb{Q}(\mu_n(\mathbb{C})) = \mathbb{Q}(\xi_n)$ vom n -ten **Kreisteilungskörper** oder auch **zyklotomischen Körper**. Das Minimalpolynom von ξ_n heißt entsprechend n -tes **Kreisteilungspolynom** und wird mit Φ_n bezeichnet.

Satz 3.17. Sei $n \in \mathbb{N}$ und Φ_n das n -te Kreisteilungspolynom.

- (1) Φ_n ist ein Polynom von Grad $\varphi(n)$ mit ganzzahligen Koeffizienten.
- (2) Es gilt die Formel $X^n - 1 = \prod_{d|n} \Phi_d$.

Die Aussage in Satz 3.17 (2) erweist sich als äußerst nützlich für die Berechnung von Kreisteilungspolynomen. Beispielsweise sieht man unmittelbar $\Phi_1 = X - 1$ und falls p eine Primzahl ist, so ist unter Verwendung der geometrischen Reihe

$$X^p - 1 = \Phi_p \cdot \Phi_1 \quad \Leftrightarrow \quad \Phi_p = \frac{X^p - 1}{X - 1} = X^{p-1} + \dots + X + 1.$$

Aufgabe (Frühjahr 2000, T3A3)

Sei $\xi = e^{\frac{2\pi i}{5}}$.

- a** Zeigen Sie, dass $\alpha = \xi + \xi^{-1}$ einer normierten quadratischen Gleichung mit Koeffizienten aus \mathbb{Z} genügt.
- b** Stellen Sie α^{-1} als Polynom in α dar und zeigen Sie $0 < \alpha < 1$.

Lösungsvorschlag zur Aufgabe (Frühjahr 2000, T3A3)

- a** Zunächst folgt aus $\xi^5 = 1$, dass $\xi^{-1} = \xi^4$ und $\xi^{-2} = \xi^3$. Außerdem gilt

$$\Phi_5(\xi) = 1 + \xi + \xi^2 + \xi^3 + \xi^4 = 0,$$

wobei Φ_5 das fünfte Kreisteilungspolynom bezeichnet. Es gilt nun

$$\begin{aligned} \alpha^2 &= \xi^2 + \xi^{-2} + 2 = \xi^2 + \xi^3 + 2 = -(\xi + \xi^4 + 1) + 2 = -\alpha + 1 \\ &\Leftrightarrow \alpha^2 + \alpha - 1 = 0. \end{aligned}$$

b Nach Aufgabenteil **a** gilt

$$1 = \alpha^2 + \alpha = \alpha \cdot (\alpha + 1),$$

d. h. $\alpha^{-1} = \alpha + 1$. Unter Benutzung der Euler-Identität gilt

$$\begin{aligned}\alpha &= \xi + \xi^{-1} = \cos\left(\frac{2\pi}{5}\right) + i \sin\left(\frac{2\pi}{5}\right) + \cos\left(-\frac{2\pi}{5}\right) + i \sin\left(-\frac{2\pi}{5}\right) = \\ &= 2 \cos\left(\frac{2\pi}{5}\right).\end{aligned}$$

Da die cos-Funktion auf dem Intervall $[0, \frac{\pi}{2}]$ streng monoton fallend ist, folgt aus

$$\frac{\pi}{3} = \frac{2\pi}{6} < \frac{2\pi}{5} < \frac{2\pi}{4} = \frac{\pi}{2},$$

dass auch die Ungleichung

$$\frac{1}{2} = \cos\left(\frac{\pi}{6}\right) > \cos\frac{2\pi}{5} > \cos\frac{\pi}{2} = 0$$

erfüllt ist.

Aufgabe (Herbst 2003, T1A2)

Beweisen Sie

$$\cos \frac{2\pi}{5} = \frac{\sqrt{5}-1}{4}.$$

Lösungsvorschlag zur Aufgabe (Herbst 2003, T1A2)

Sei $\xi = e^{2\pi i/5}$, dann ist $\cos \frac{2\pi}{5} = \frac{1}{2}(\xi + \xi^{-1})$. Sei $\alpha = \cos \frac{2\pi}{5}$. Man berechnet nun ähnlich wie in der vorhergehenden Aufgabe

$$\begin{aligned}\alpha^2 &= \frac{1}{4}(\xi^2 + \xi^{-2} + 2) = \frac{1}{4}(\xi^2 + \xi^3 + 2) = -\frac{1}{4}(\xi + \xi^4 + 1 - 2) = -\frac{1}{4}(2\alpha - 1) \\ &\Leftrightarrow 4\alpha^2 + 2\alpha - 1 = 0.\end{aligned}$$

Die Lösungen dieser quadratischen Gleichung sind nach der Mitternachtsformel

$$\frac{-2 \pm \sqrt{4+16}}{2 \cdot 4} = \frac{-1 \pm \sqrt{5}}{4}.$$

Wegen $\cos \frac{2\pi}{5} = \cos 72^\circ > 0$ ist dann $\cos \frac{2\pi}{5} = \frac{-1+\sqrt{5}}{4}$.

Aufgabe (Herbst 2010, T2A4)

Für $1 \leq m \in \mathbb{N}$ betrachte man das Polynom $f_m = X^{2m} + X^m + 1 \in \mathbb{Z}[X]$.

Zeigen Sie:

- a** Jede komplexe Nullstelle von f_m ist eine Einheitswurzel.
- b** f_m ist genau dann irreduzibel über \mathbb{Q} , wenn $m = 3^k$ für ein $k \in \mathbb{N}_0$ gilt.

Lösungsvorschlag zur Aufgabe (Herbst 2010, T2A4)

- a** Nach der Formel oben ist $X^2 + X + 1$ das dritte Kreisteilungspolynom, deshalb gilt laut Satz 3.17 (2):

$$X^3 - 1 = \prod_{d|3} \Phi_d = (X - 1)(X^2 + X + 1)$$

Dabei bezeichnet jeweils Φ_d das d -te Kreisteilungspolynom. Einsetzen von X^m liefert

$$X^{3m} - 1 = (X^m - 1) \cdot (X^{2m} + X^m + 1).$$

Dies zeigt, dass jede Nullstelle von $X^{2m} + X^m + 1$ auch eine Nullstelle von $X^{3m} - 1$ und damit eine Einheitswurzel ist.

- b** Obige Polynomgleichung kann umgeschrieben werden zu:

$$\prod_{d|3m} \Phi_d = X^{3m} - 1 = (X^{2m} + X^m + 1) \cdot (X^m - 1) = (X^{2m} + X^m + 1) \cdot \prod_{d|m} \Phi_d$$

Jeder Teiler von m ist insbesondere ein Teiler von $3m$, deshalb können die entsprechenden Kreisteilungspolynome gekürzt werden:

$$(X^{2m} + X^m + 1) = \prod_{\substack{d|3m \\ d|m}} \Phi_d$$

Das Polynom $f_m = X^{2m} + X^m + 1$ ist also genau dann irreduzibel, wenn das rechte Produkt nur aus einem Polynom besteht. (Denn Kreisteilungspolynome sind stets irreduzibel über \mathbb{Q}). Äquivalent dazu ist, dass es genau eine Zahl d gibt mit $d | 3m$ und $d \nmid m$. Falls $m = 3^k$ für ein $k \in \mathbb{N}_0$ gilt, so ist $m = 3^{k+1}$ und nur $d = 3$ erfüllt beide Bedingungen.

Falls m keine Potenz von 3 ist, können wir $m = l \cdot 3^k$ mit $3 \nmid l$ und $k \in \mathbb{N}_0$ schreiben. Es gilt nun

$$3^{k+1} | 3 \cdot (l3^k), \quad 3^{k+1} \nmid (l3^k), \quad l3^{k+1} | 3(l3^k), \quad l3^{k+1} \nmid (l3^k).$$

Falls $l \neq 1$ ist, gibt es also mindestens zwei verschiedene Zahlen d mit $d | 3m$ und $d \nmid m$.

Aufgabe (Herbst 2012, T2A3)

Seien p eine Primzahl und ζ eine primitive p -te Einheitswurzel in \mathbb{C} . Sei $R = \mathbb{Z}[\zeta]$ der von ζ erzeugte Unterring von \mathbb{C} . Sei $a \in \mathbb{Z}$ eine ganze Zahl. Zeigen Sie, dass

$$\mathbb{Z}/\left(\sum_{l=0}^{p-1} a^l\right) \rightarrow R/(a - \zeta), \quad n + \left(\sum_{l=0}^{p-1} a^l\right) \mapsto n + (a - \zeta)$$

ein wohldefinierter Ringisomorphismus ist und folgern Sie daraus, dass $2 - \zeta$ genau dann ein Primelement in R ist, wenn $2^p - 1$ eine Primzahl ist.

Lösungsvorschlag zur Aufgabe (Herbst 2012, T2A3)

Sei Φ_p das p -te Kreisteilungspolynom und definiere die Abbildung

$$\pi: \mathbb{Z} \rightarrow R/(a - \zeta), \quad n \mapsto n + (a - \zeta).$$

Diese Abbildung ist ein Homomorphismus mit $(\Phi_p(a)) \subseteq \ker \pi$, denn es gilt $a \equiv \zeta \pmod{a - \zeta}$ und somit

$$\pi(\Phi_p(a)) = \Phi_p(a) + (a - \zeta) = \Phi_p(\zeta) + (a - \zeta) = 0 + (a - \zeta).$$

Nach dem Homomorphiesatz 2.11 induziert π einen wohldefinierten Homomorphismus $\bar{\pi}: \mathbb{Z}/(\Phi_p(a)) \rightarrow R/(a - \zeta)$, das ist genau die Abbildung aus der Angabe.

Um zu zeigen, dass $\bar{\pi}$ bijektiv ist, geben wir die Umkehrabbildung an. Jedes Element in R ist ein Polynom in ζ , wegen $\Phi_p(\zeta) = 0$ erzeugen bereits die Potenzen $1, \zeta, \dots, \zeta^{p-2}$ den Ring R über \mathbb{Z} . Betrachte nun die Abbildung

$$\varphi: R \rightarrow \mathbb{Z}/\Phi_p(a)\mathbb{Z}, \quad \sum_{i=0}^{p-2} c_i \zeta^i \mapsto \sum_{i=0}^{p-2} c_i a^i + (\Phi_p(a)),$$

welche ein Homomorphismus mit $\varphi(a - \zeta) = a - a + (\Phi_p(a)) = 0 + (\Phi_p(a))$ ist, d. h. $(a - \zeta) \subseteq \ker \varphi$. Nach dem Homomorphiesatz 2.11 induziert deshalb auch φ einen Homomorphismus $\bar{\varphi}: R/(a - \zeta) \rightarrow \mathbb{Z}/\Phi_p(a)\mathbb{Z}$.

Man überprüft nun unmittelbar, dass $\bar{\pi} \circ \bar{\varphi} = \text{id}$ sowie $\bar{\varphi} \circ \bar{\pi} = \text{id}$ erfüllt ist. Dies zeigt, dass $\bar{\pi}$ eine Umkehrabbildung besitzt und deshalb ein Isomorphismus sein muss.

Nun ist $a - \zeta$ genau dann ein Primelement in R , wenn $(a - \zeta)$ ein Primideal ist, was wiederum genau dann der Fall ist, wenn $R/(a - \zeta) \cong \mathbb{Z}/(\Phi_p(a))$ ein Integritätsbereich ist. Letzteres ist genau dann der Fall, wenn $\Phi_p(a)$ eine

Primzahl ist. Unter Verwendung der geometrischen Reihe ist

$$\Phi_p(2) = \sum_{l=0}^{p-1} 2^l = \frac{2^p - 1}{2 - 1} = 2^p - 1.$$

Aufgabe (Frühjahr 2013, T3A5)

Für $n \in \mathbb{N}$ bezeichne $\zeta_n := e^{2\pi i/n}$ und $k_n := \text{kgV}\{1, \dots, n\}$ das kleinste gemeinsame Vielfache der Zahlen $1, \dots, n$. Zeigen Sie, für alle $n \in \mathbb{N}$, die folgenden Formeln über die Grade von Körpererweiterungen:

- a** $[\mathbb{Q}(\zeta_1, \dots, \zeta_n) : \mathbb{Q}] = \varphi(k_n)$, wobei φ die Euler'sche φ -Funktion bezeichnet.
- b** $[\mathbb{Q}(\sqrt[m]{2}, \dots, \sqrt[n]{2}) : \mathbb{Q}] = k_n$.

Lösungsvorschlag zur Aufgabe (Frühjahr 2013, T3A5)

- a** Es genügt nach Satz 3.17 (1) zu zeigen, dass $\mathbb{Q}(\zeta_1, \dots, \zeta_n) = \mathbb{Q}(\zeta_{k_n})$. Zunächst ist jedes ζ_s für $s \in \{1, \dots, n\}$ auch eine k_n -te Einheitswurzel, da wegen $s \mid k_n$ auch $\zeta_s^{k_n} = 1$ gilt. Also ist schon mal $\mathbb{Q}(\zeta_1, \dots, \zeta_n) \subseteq \mathbb{Q}(\zeta_{k_n})$. Sei nun $\mu_{k_n} \subseteq \mathbb{C}$ die Gruppe der k_n -ten Einheitswurzeln. Betrachte die Untergruppe

$$U = \langle \zeta_1, \dots, \zeta_n \rangle \subseteq \mu_{k_n}.$$

Da $\langle \zeta_s \rangle \subseteq U$ für alle $s \in \{1, \dots, n\}$ gilt, ist jedes solche s nach dem Satz von Lagrange ein Teiler von $|U|$. Somit ist $|U|$ ein Vielfaches von $1, \dots, n$ und muss die Abschätzung $|U| \geq k_n$ erfüllen. Wegen $U \subseteq \mu_{k_n}$ muss bereits $|U| = k_n$ und damit $U = \mu_{k_n}$ sein. Insbesondere ist $\zeta_{k_n} \in U \subseteq \mathbb{Q}(\zeta_1, \dots, \zeta_n)$. Insgesamt haben wir $\mathbb{Q}(\zeta_1, \dots, \zeta_n) = \mathbb{Q}(\zeta_{k_n})$ wie erhofft.

- b** Das Polynom $f_m = X^m - 2$ ist für jedes $m \in \mathbb{N}$ nach dem Eisensteinkriterium irreduzibel und deshalb das Minimalpolynom von $\sqrt[m]{2}$, sodass $[\mathbb{Q}(\sqrt[m]{2}) : \mathbb{Q}] = m$ gilt. Sei $s \in \{1, \dots, n\}$. Aus der Gradformel folgt, dass $s = [\mathbb{Q}(\sqrt[s]{2}) : \mathbb{Q}]$ ein Teiler von $[\mathbb{Q}(\sqrt[2]{2}, \dots, \sqrt[n]{2}) : \mathbb{Q}]$ ist. Also muss schon mal $[\mathbb{Q}(\sqrt[2]{2}, \dots, \sqrt[n]{2}) : \mathbb{Q}] \geq k_n$ sein. Sei $k_n = s \cdot l$, dann ist

$$\sqrt[s]{2} = 2^{\frac{1}{s}} = 2^{\frac{l}{ls}} = 2^{\frac{l}{k_n}} = \left(\sqrt[k_n]{2}\right)^l \in \mathbb{Q}(\sqrt[k_n]{2}).$$

Daraus folgt $\mathbb{Q}(\sqrt[2]{2}, \dots, \sqrt[n]{2}) \subseteq \mathbb{Q}(\sqrt[k_n]{2})$, sodass

$$[\mathbb{Q}(\sqrt[2]{2}, \dots, \sqrt[n]{2}) : \mathbb{Q}] \leq [\mathbb{Q}(\sqrt[k_n]{2}) : \mathbb{Q}] = k_n.$$

Beide Abschätzungen zusammen ergeben $[\mathbb{Q}(\sqrt[2]{2}, \dots, \sqrt[n]{2}) : \mathbb{Q}] = k_n$.

Galois-Theorie der Kreisteilungskörper

Die Kreisteilungskörper haben eine besonders schöne Galois-Theorie, weswegen der Leser ihnen im entsprechenden Abschnitt wieder begegnen wird. Wir formulieren das entsprechende Resultat der Vollständigkeit wegen an dieser Stelle, während die Anwendung zum größten Teil in den Aufgaben im Abschnitt über Galois-Theorie zu finden sein wird.

Satz 3.18. Sei $n \in \mathbb{N}$ und ξ_n eine primitive n -te Einheitswurzel. Dann ist $\mathbb{Q}(\xi_n)|\mathbb{Q}$ eine Galois-Erweiterung und die Abbildung

$$(\mathbb{Z}/n\mathbb{Z})^\times \longrightarrow G_{\mathbb{Q}(\xi_n)|\mathbb{Q}}, \quad \bar{r} \mapsto \{\xi_n \mapsto \xi_n^r\}$$

ist ein Isomorphismus von Gruppen. Beachte dazu auch Proposition 2.8.

Aufgabe (Herbst 2000, T3A4)

Sei $n > 2$ eine ganze Zahl und φ die Euler'sche φ -Funktion.

- a Zeigen Sie, dass $\mathbb{Q}[\cos \frac{2\pi}{n}]|\mathbb{Q}$ eine Galois-Erweiterung vom Grad $\frac{\varphi(n)}{2}$ ist.
- b Bestimmen Sie das neunte Kreisteilungspolynom über \mathbb{Q} .
- c Bestimmen Sie das Minimalpolynom von $\cos \frac{2\pi}{9}$ über \mathbb{Q} .

Lösungsvorschlag zur Aufgabe (Herbst 2000, T3A4)

- a Sei $\xi_n = e^{2\pi i/n} = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}$ eine primitive n -te Einheitswurzel. Dann ist $\cos \frac{2\pi}{n} = \frac{1}{2}(\xi_n + \overline{\xi_n})$. Zudem gilt

$$1 = |\xi_n|^2 = \xi_n \cdot \overline{\xi_n} \quad \Leftrightarrow \quad \overline{\xi_n} = \xi_n^{-1}.$$

Sei $\alpha = \cos \frac{2\pi}{n}$, dann haben wir also

$$\xi_n \alpha = \frac{1}{2} \cdot \xi_n \cdot (\xi_n + \xi_n^{-1}) = \frac{1}{2}(\xi_n^2 + 1) \quad \Leftrightarrow \quad \xi_n^2 - 2\alpha \xi_n + 1 = 0.$$

Also ist das Minimalpolynom von ξ_n über $\mathbb{Q}(\alpha)$ höchstens von Grad 2, sodass $[\mathbb{Q}(\xi_n) : \mathbb{Q}(\alpha)] \leq 2$. Gleichzeitig muss jedoch $\mathbb{Q}(\xi_n) \neq \mathbb{Q}(\alpha)$ sein, denn wegen $\alpha = \cos \frac{2\pi}{n} \in \mathbb{R}$ muss auch $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$ sein. Wäre auch $\mathbb{Q}(\xi_n) \subseteq \mathbb{R}$, so müsste insbesondere $\xi_n \in \mathbb{R}$ sein. Wegen $|\xi_n| = 1$ hieße das $\xi_n \in \{\pm 1\}$, was wegen $n > 2$ nicht der Fall ist. Also ist $[\mathbb{Q}(\xi_n) : \mathbb{Q}(\alpha)] = 2$

und die Gradformel liefert

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = \frac{[\mathbb{Q}(\xi_n) : \mathbb{Q}]}{\mathbb{Q}(\xi_n) : \mathbb{Q}(\alpha)} = \frac{\varphi(n)}{2}.$$

Die Erweiterung $\mathbb{Q}(\xi_n)|\mathbb{Q}$ ist nach Satz 3.18 galoissch und hat eine abelsche Galois-Gruppe, sodass jede Untergruppe ein Normalteiler ist. Nach dem Hauptsatz der Galois-Theorie 3.20 ist daher jede Zwischenerweiterung galoissch, insbesondere also die Erweiterung $\mathbb{Q}(\alpha)|\mathbb{Q}$.

b Unter Verwendung der Formel aus Satz 3.17 haben wir

$$\begin{aligned} X^9 - 1 &= \Phi_9 \cdot \Phi_3 \cdot \Phi_1 = \Phi_9 \cdot (X^3 - 1) \\ \Leftrightarrow \quad \Phi_9 &= \frac{X^9 - 1}{X^3 - 1} = \frac{(X^3)^3 - 1}{X^3 - 1} = \Phi_3(X^3) = X^6 + X^3 + 1. \end{aligned}$$

c Sei wieder $\alpha = \cos \frac{2\pi}{9}$, dann wissen wir aus Teil **a**, dass das Minimalpolynom den Grad $\frac{\varphi(9)}{2} = \frac{6}{2} = 3$ haben muss und die Gleichung $\alpha = \frac{1}{2}(\xi_9 + \xi_9^{-1})$ gilt. Nach Teil **b** ist außerdem $\xi_9^6 + \xi_9^3 + 1 = 0$. Wir berechnen daher:

$$\begin{aligned} \alpha^3 &= \frac{1}{8}(\xi_9^2 + \xi_9^{-2} + 2)(\xi_9 + \xi_9^{-1}) = \frac{1}{8}(\xi_9^3 + \xi_9 + 2\xi_9 + \xi_9 + \xi_9^{-3} + 2\xi_9^{-1}) = \\ &= \frac{1}{8}(\xi_9^6 + \xi_9^{-3} + 3\xi_9 + 3\xi_9^{-3}) = \frac{1}{8}(-1 + 6\alpha) \end{aligned}$$

Durch Umstellen erhält dieser Gleichung erhält man $\alpha^3 - \frac{3}{4}\alpha + \frac{1}{8} = 0$. Da das Polynom $X^3 - \frac{3}{4}X - \frac{1}{8}$ normiert ist, α als Nullstelle hat und den richtigen Grad besitzt, muss es das Minimalpolynom von α über \mathbb{Q} sein.

Aufgabe (Frühjahr 2013, T1A2)

Sei $f = X^2 - 2 \in \mathbb{Q}[X]$. Sei weiter $f_0 = X$ und für $n \geq 1$ sei $f_n = f_{n-1}(f) = f(f_{n-1})$ das n -fach iterierte Polynom f , also

$$f_1 = X^2 - 2, \quad f_2 = (X^2 - 2)^2 - 2, \quad f_3 = ((X^2 - 2)^2 - 2)^2 - 2 \quad \text{usw.}$$

Zeigen Sie:

- a** Alle Polynome f_n sind irreduzibel.
- b** Sei $z_n = e^{\pi i / 2^{n+1}}$ eine primitive 2^{n+2} -te Einheitswurzel. Für k ungerade ist $2 \cos \frac{k\pi}{2^{n+1}} = z_n^k + z_n^{-k}$ eine Nullstelle von f_n .
- c** Die Galois-Gruppe von f_2 über \mathbb{Q} ist abelsch.

Lösungsvorschlag zur Aufgabe (Frühjahr 2013, T1A2)

- a** Das Polynom $f_0 = X$ ist natürlich irreduzibel. Für $f_1 = X^2 - 2$ folgt die Irreduzibilität aus dem Eisenstein-Kriterium mit $p = 2$. Dieses wollen wir auch für die weiteren Folgenglieder verwenden, weshalb wir folgende Aussage beweisen:

Behauptung: Für $n \geq 1$ hat f_n die Form $f_n = g_n + 2$, wobei g_n ein Polynom mit verschwindendem konstanten Koeffizienten und $g_n \equiv X^{2^n} \pmod{2}$ ist.

Induktionsanfang: Die Behauptung ist für $f_1 = X^2 - 2$ erfüllt.

Induktionsgeschritt: Nehmen wir an, für n ist die Aussage bewiesen. Es ist dann $f_n = g_n + 1$ für ein Polynom g_n wie oben und $f_n \equiv X^{2^n} \pmod{2}$. Daraus folgt

$$f_{n+1} = f(f_n) = f(g_n + 2) = (g_n + 2)^2 - 2 = g_n^2 + 4g_n + 2.$$

Bei $g_{n+1} = g_n^2 + 4g_n$ handelt es sich um ein Polynom mit konstantem Glied 0, sodass die erste Behauptung erfüllt ist. Weiterhin erhalten wir

$$f_{n+1} \equiv f_n^2 - 2 \equiv (X^{2^k})^2 \equiv X^{2^{k+1}} \pmod{2}.$$

Damit ist f_n für jedes $n \geq 2$ ein Eisenstein-Polynom mit $p = 2$ und daher irreduzibel über \mathbb{Q} .

- b** Wir beweisen die Aussage nun per vollständiger Induktion über n .

Induktionsanfang: Es gilt $z_1^2 = z_0 = e^{\pi i/2} = i$, daher berechnet sich für ungerades k

$$\begin{aligned} f_1(z_1^k + z_1^{-k}) &= (z_1^k + z_1^{-k})^2 - 2 = z_1^{2k} + z_1^{-2k} + 2 \cdot z_n^k \cdot z_n^{-k} - 2 = \\ &= i^k + i^{-k} + 2 - 2 = i^k + \left(\frac{1}{i}\right)^k = i^k + (-i)^k = i^k - i^k = 0. \end{aligned}$$

Induktionsgeschritt:

$$\begin{aligned} f_{n+1}(z_{n+1}^k + z_{n+1}^{-k}) &= f_n(f((z_{n+1}^k + z_{n+1}^{-k}))) = f_n((z_{n+1}^k + z_{n+1}^{-k})^2 - 2) = \\ &= f_n((z_{n+1}^2)^k + (z_{n+1}^2)^{-k} + 2 \cdot z_{n+1}^k \cdot z_{n+1}^{-k} - 2) = f_n(z_n^k + z_n^{-k} + 2 - 2) = \\ &= f_n(z_n^k + z_n^{-k}) \stackrel{(I.V.)}{=} 0. \end{aligned}$$

Dabei haben wir die für $n \in \mathbb{N}$ gültige Gleichung

$$z_{n+1}^2 = \left(e^{\pi i/2^{n+2}}\right)^2 = e^{2\pi/2^{n+1}} = z_n$$

verwendet.

c Das Polynom f_2 hat Grad 4 und nach Teil **b** sind durch

$$2\cos\left(\frac{\pi}{8}\right), \quad 2\cos\left(\frac{3\pi}{8}\right), \quad 2\cos\left(\frac{5\pi}{8}\right), \quad 2\cos\left(\frac{7\pi}{8}\right)$$

vier verschiedene Nullstellen von f_2 gegeben. Diese liegen außerdem alle in $\mathbb{Q}(z_2)$, also liegt auch der Zerfallungskörper von f_2 in $\mathbb{Q}(z_2)$ und die Galois-Gruppe von f_2 ist nach Proposition 3.22 eine Faktorgruppe von $G_{\mathbb{Q}(z_2)|\mathbb{Q}}$. Die Galois-Gruppe der zyklotomischen Erweiterung ist laut Satz 3.18 zyklisch, also insbesondere abelsch. Da jede Faktorgruppe einer abelschen Gruppe wieder abelsch ist, ist daher $\text{Gal}(f)$ abelsch.

3.4. Galois-Theorie

Evariste Galois ist sicherlich eine der bedeutendsten Personen für die Mathematik gewesen. Bevor er im Alter von nur 20 Jahren bei einem Pistolenduell starb, ist es ihm gelungen, den Grundstein der Theorie zu legen, die heute ihm zu Ehren seinen Namen trägt.

Der Grundgedanke der Galois-Theorie besteht darin, einer Körpererweiterung $L|K$ die Gruppe ihrer K -Automorphismen $\text{Aut}_K(L)$ zuzuordnen, d. h. die Gruppe der bijektiven Körperhomomorphismen $\sigma: L \rightarrow L$ mit $\sigma|_K = \text{id}_K$. Auf diese Weise ist es möglich, Fragestellungen der Körpertheorie mithilfe von Methoden der Gruppentheorie zu beantworten.

Definition 3.19. Eine Körpererweiterung $L|K$ heißt *galoissch* oder *Galois-Erweiterung*, falls sie normal und separabel ist. In diesem Fall heißt $G_{L|K} := \text{Aut}_K(L)$ dann *Galois-Gruppe* von $L|K$.

Das Erstaunliche ist nun, dass die Forderungen, die wir an eine Galois-Erweiterung gestellt haben, dazu führen, dass sich viele ihrer Eigenschaften in ihrer Galois-Gruppe widerspiegeln.

Die Voraussetzung, dass eine Galois-Erweiterung $L|K$ normal ist, stellt sicher, dass $\text{Aut}_K(L) = \text{Hom}_K(L, \bar{L})$ gilt (vgl. Definition 3.8). Für einen endlichen separablen Erweiterungskörper von K ist die Zahl seiner K -Homomorphismen in einen algebraischen Abschluss durch den Erweiterungsgrad über K gegeben. Setzt man dies zusammen, so erhält man

$$|G_{L|K}| = [L : K].$$

Ferner können wir einer Untergruppe $H \subseteq G_{L|K}$ einen Körper zuordnen, nämlich den sogenannten *Fixkörper*

$$L^H = \{a \in L \mid \sigma(a) = a \text{ für alle } \sigma \in H\}$$

von H . Auch hier besteht ein Zusammenhang zwischen Erweiterungsgrad und Gruppenordnung. Es gilt nämlich

$$(G_{L|K} : H) = [L^H : K].$$

Wir sind nun in der Lage, das Hauptresultat der Galois-Theorie zu formulieren.

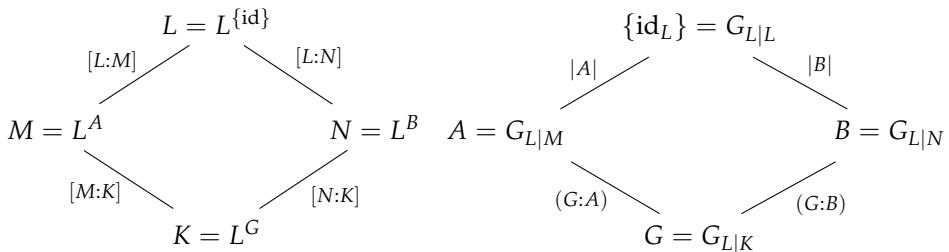
Satz 3.20 (Hauptsatz der Galois-Theorie). Sei $L|K$ eine endliche Galois-Erweiterung mit Galois-Gruppe $G = G_{L|K}$. Dann sind durch

$$\begin{array}{ccc} \{ \text{Untergruppen von } G \} & \xleftrightarrow{\hspace{2cm}} & \{ \text{Zwischenkörper von } L|K \} \\ H \longmapsto L^H & & \\ G_{L|M} \longleftarrow M & & \end{array}$$

zueinander inverse, inklusionsumkehrende Bijektionen gegeben. Dabei ist $L^H|K$ genau dann normal (und damit galoissch), wenn $H \trianglelefteq G$ ein Normalteiler ist.

Es sei an dieser Stelle betont, dass der Hauptsatz in der obigen Formulierung allein für *endliche* Erweiterungen gültig ist. Es gibt zwar eine Verallgemeinerung auf den Fall unendlicher Körpererweiterungen, doch diese geht deutlich über den im Staatsexamen verlangten Stoff hinaus.

Als Zusammenfassung und Merkhilfe der bisherigen Ergebnisse stellen wir exemplarisch das Körper- bzw. Gruppendiagramm einer Galois-Erweiterung $L|K$ mit genau zwei Zwischenkörpern M, N nebeneinander. Nach dem Hauptsatz der Galois-Theorie 3.20 besitzt die Galois-Gruppe $G_{L|K}$ zwei Untergruppen A, B sowie die triviale Untergruppe $\{\text{id}_L\}$. Die Beziehung zwischen den Untergruppen und Zwischenkörpern ist wie folgt:



Beispiel 3.21. Wir geben an dieser Stelle ein illustrierendes Beispiel und betrachten dazu die Erweiterung $L|\mathbb{Q}$ mit $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

L ist Zerfällungskörper des Polynoms $(X^2 - 2)(X^2 - 3) \in \mathbb{Q}[X]$, sodass $L|\mathbb{Q}$ normal ist. Außerdem hat \mathbb{Q} Charakteristik 0, folglich ist jede algebraische Erweiterung von \mathbb{Q} separabel. Insbesondere trifft dies auf $L|\mathbb{Q}$ zu, sodass es sich hierbei

um eine Galois-Erweiterung handelt. Weiterhin überzeugt man sich leicht davon, dass $[L : K] = 4$ ist, wir es also mit einer endlichen Galois-Erweiterung zu tun haben.

Um nun die Galois-Gruppe dieser Erweiterung explizit bestimmen zu können, greifen wir etwas vor und verwenden die Vorgehensweise auf Seite 185. Ein \mathbb{Q} -Automorphismus von L muss nämlich $\sqrt{2}$ auf eine Nullstelle von $X^2 - 2$ und $\sqrt{3}$ auf eine Nullstelle von $X^2 - 3$ abbilden. Diese Überlegung liefert die Abbildungsvorschriften

$$\text{id}_L, \quad \sigma = \begin{cases} \sqrt{2} \mapsto -\sqrt{2} \\ \sqrt{3} \mapsto \sqrt{3} \end{cases} \quad \tau = \begin{cases} \sqrt{2} \mapsto \sqrt{2} \\ \sqrt{3} \mapsto -\sqrt{3} \end{cases} \quad \sigma\tau = \begin{cases} \sqrt{2} \mapsto -\sqrt{2} \\ \sqrt{3} \mapsto -\sqrt{3} \end{cases}$$

von denen wir noch zeigen müssen, dass sie \mathbb{Q} -Automorphismen σ, τ und $\sigma\tau$ von L definieren. Dazu verwenden wir den Fortsetzungssatz 3.15, welcher im ersten Schritt die Existenz der beiden Homomorphismen

$$\text{id}_{\mathbb{Q}(\sqrt{2})} : \mathbb{Q}(\sqrt{2}) \rightarrow \mathbb{Q}(\sqrt{2}) \quad \text{und} \quad \mathbb{Q}(\sqrt{2}) \rightarrow \mathbb{Q}(\sqrt{2}), \quad a + b\sqrt{2} \mapsto a - b\sqrt{2}$$

als Fortsetzung von $\text{id}_{\mathbb{Q}}$ sicherstellt. Durch eine zweite Fortsetzung dieser beiden Homomorphismen auf $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ bekommt man die oben beschriebenen Abbildungen $\text{id}_L, \sigma, \tau, \sigma\tau$. Die Galois-Gruppe $G_{L|\mathbb{Q}}$ hat wegen $[L : K] = 4$ genau vier Elemente, sodass dies bereits alle sind.

Zur Bestimmung der Fixkörper geht man folgendermaßen vor: Sei $\alpha \in L$ beliebig vorgegeben. Da $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ eine \mathbb{Q} -Basis von L ist, gibt es $a, b, c, d \in \mathbb{Q}$, sodass

$$\alpha = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$$

gilt. Also ist

$$\begin{aligned} \alpha \in L^{(\sigma)} &\Leftrightarrow \sigma(\alpha) = \alpha \Leftrightarrow \sigma(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \\ &\Leftrightarrow a + b(-\sqrt{2}) + c\sqrt{3} + d(-\sqrt{6}) = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \Leftrightarrow 2(b\sqrt{2} + d\sqrt{6}) = 0 \\ &\Leftrightarrow b\sqrt{2} + d\sqrt{6} = 0 \end{aligned}$$

Dies bedeutet

$$\alpha = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} = a + c\sqrt{3} \in \mathbb{Q}(\sqrt{3})$$

Umgekehrt ist $\mathbb{Q}(\sqrt{3}) \subseteq L^{(\sigma)}$ klar, sodass Gleichheit folgt.

Genauso bestimmt man auch die übrigen Fixkörper. Man erhält dann die folgenden beiden Diagramme:

$$\begin{array}{ccc}
 & L = L^{\{\text{id}\}} & \\
 & | 2 & \\
 \mathbb{Q}(\sqrt{3}) = L^{\langle\sigma\rangle} & \mathbb{Q}(\sqrt{6}) = L^{\langle\sigma\tau\rangle} & \mathbb{Q}(\sqrt{2}) = L^{\langle\tau\rangle} \\
 & | 2 & \\
 & \mathbb{Q} = L^{\{\text{id}_L, \sigma, \tau, \sigma\tau\}} &
 \end{array}$$

$$\begin{array}{ccc}
 & \{\text{id}_L\} = G_{L|L} & \\
 & | 2 & \\
 \langle\sigma\rangle = G_{L|\mathbb{Q}(\sqrt{3})} & \langle\sigma\tau\rangle = G_{L|\mathbb{Q}(\sqrt{6})} & \langle\tau\rangle = G_{L|\mathbb{Q}(\sqrt{2})} \\
 & | 2 & \\
 & \{\text{id}_L, \sigma, \tau, \sigma\tau\} = G_{L|K} &
 \end{array}$$

■

Neben dem Hauptsatz könnten auch die folgenden Resultate hilfreich sein.

Proposition 3.22. Sei $L|K$ eine endliche Galois-Erweiterung und E ein Zwischenkörper, sodass auch $E|K$ galoissch ist. Die Einschränkungsabbildung

$$G_{L|K} \rightarrow G_{E|K}, \quad \sigma \mapsto \sigma|_E$$

ist ein surjektiver Gruppenhomomorphismus mit Kern $G_{L|E}$ und induziert daher laut dem Homomorphiesatz einen Isomorphismus

$$G_{E|K} \xrightarrow{\cong} G_{L|K}/G_{L|E}.$$

Für die nächste Aussage sei daran erinnert, dass das **Kompositum** zweier Zwischenkörper E, E' einer Körpererweiterung $L|K$ als $E \cdot E' = E(E') = E'(E)$ definiert ist. Beispielsweise ist $\mathbb{Q}(\sqrt{2}) \cdot \mathbb{Q}(\sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

Proposition 3.23. Sei $L|K$ eine Körpererweiterung mit Zwischenkörpern E, E' , sodass $E|K$ und $E'|K$ endliche Galois-Erweiterungen sind. Dann gilt:

(1) Die Erweiterung $E \cdot E'|K$ ist endlich sowie galoissch und die Abbildung

$$G_{EE'|E} \rightarrow G_{E'|E \cap E'}, \quad \sigma \mapsto \sigma|_{E'}$$

ist ein Isomorphismus.

(2) Der Homomorphismus

$$G_{EE'|K} \rightarrow G_{E|K} \times G_{E'|K}, \quad \sigma \mapsto (\sigma|_E, \sigma|_{E'})$$

ist injektiv. Gilt $E \cap E' = K$, so ist er sogar ein Isomorphismus.

Bestimmung der Struktur von Galois-Gruppen

Anleitung: Isomorphietyp von Galois-Gruppen bestimmen

Sei $L|K$ eine endliche Galois-Erweiterung. Will man den Isomorphietyp von $G_{L|K}$ bestimmen, so könnten folgende Schritte hilfreich sein:

- (1) Bestimme die Ordnung der Galois-Gruppe. Diese beträgt $[L : K]$.
- (2) Welche Gruppen der Ordnung $[L : K]$ gibt es? Für kleine Ordnungen sind dies nicht allzu viele.
- (3) Überprüfe charakteristische Merkmale der Gruppen aus (2):
 - Welche Elementordnungen sind möglich? Gibt es beispielsweise ein Element der Ordnung $[L : K]$ in $G_{L|K}$, so muss die Galois-Gruppe zyklisch sein.
 - Ist die Gruppe abelsch? Gibt es $\sigma, \tau \in G_{L|K}$ mit $\sigma\tau \neq \tau\sigma$, so kann die Galois-Gruppe nicht abelsch sein.
 - Welche Normalteiler hat die Gruppe? In einer abelschen Gruppe ist jede Untergruppe ein Normalteiler. Wäre $G_{L|K}$ abelsch, so müsste also jede Zwischenerweiterung $M|K$ normal sein.
 - Welche Untergruppenstruktur hat die Gruppe? Eine zyklische Gruppe hat z. B. zu jedem Teiler d der Gruppenordnung genau eine Untergruppe von Index d . Nach dem Hauptsatz der Galois-Theorie bedeutet dies, dass es genau einen Erweiterungskörper M von K mit $[M : K] = d$ geben müsste, falls $G_{L|K}$ zyklisch ist.

Aufgabe (Frühjahr 2015, T1A5)

Sei $f \in \mathbb{Q}[X]$ ein irreduzibles Polynom vom Grad $n \geq 1$ und sei K ein Zerfällungskörper von f . Sei weiterhin $G = G_{K|\mathbb{Q}}$ die zugehörige Galois-Gruppe.

- a** Beweisen Sie: Falls G eine abelsche Gruppe ist, hat sie die Ordnung n .
- b** Sei $K = \mathbb{Q}(\sqrt{2}, i)$, wobei $i \in \mathbb{C}$ die imaginäre Einheit mit $i^2 = -1$ ist. Bestimmen Sie ein irreduzibles Polynom $f \in \mathbb{Q}[X]$, dessen Zerfällungskörper K ist. Beweisen Sie, dass $G = G_{K|\mathbb{Q}}$ abelsch, aber nicht zyklisch ist.

Lösungsvorschlag zur Aufgabe (Frühjahr 2015, T1A5)

- a** Sei $\alpha \in K$ eine Nullstelle von f . Da f nach Voraussetzung irreduzibel ist, ist f (evtl. nach Normierung) das Minimalpolynom von α , sodass $[\mathbb{Q}(\alpha) : \mathbb{Q}] = n$ gilt. Weiter ist G abelsch, sodass jede Untergruppe $G_{K|\mathbb{Q}(\alpha)}$

von G ein Normalteiler ist und deshalb nach dem Hauptsatz der Galois-Theorie 3.20 jede Zwischenerweiterung galoissch ist. Insbesondere ist somit $\mathbb{Q}(\alpha)|\mathbb{Q}$ eine normale Erweiterung.

Weil f nach Konstruktion eine Nullstelle in $\mathbb{Q}(\alpha)$ besitzt, müssen bereits alle Nullstellen von f in $\mathbb{Q}(\alpha)$ liegen. Nun wird K über \mathbb{Q} von den Nullstellen von f erzeugt, also muss $K \subseteq \mathbb{Q}(\alpha)$ gelten. Wegen $\alpha \in K$ ist auch die umgekehrte Inklusion klar, sodass $K = \mathbb{Q}(\alpha)$ und

$$|G| = [K : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}] = n$$

gilt.

- b** Wir zeigen zunächst $K = \mathbb{Q}(\sqrt{2} + i)$. Die Inklusion „ \supseteq “ ist klar, für „ \subseteq “ bemerken wir, dass

$$\frac{1}{2}(\sqrt{2} + i)^2 - \frac{1}{2} = \frac{1}{2}(2 + 2i\sqrt{2} - 1 - 1) = i\sqrt{2} \in \mathbb{Q}(\sqrt{2} + i)$$

gilt und somit auch

$$i\sqrt{2}(\sqrt{2} + i) = 2i - \sqrt{2} \in \mathbb{Q}(\sqrt{2} + i).$$

Es folgt

$$\frac{1}{3}[i(\sqrt{2} + i) + (2i - \sqrt{2})] = i \in \mathbb{Q}(\sqrt{2} + i)$$

und $(\sqrt{2} + i) - i = \sqrt{2} \in \mathbb{Q}(\sqrt{2} + i)$, woraus die gewünschte Gleichheit folgt.

Sei $\alpha = \sqrt{2} + i$. Wir bestimmen das zugehörige Minimalpolynom. Es gilt

$$\begin{aligned} \alpha - i &= \sqrt{2} \Rightarrow \alpha^2 - 2i\alpha - 1 = 2 \Leftrightarrow \alpha^2 - 3 = 2i\alpha \\ &\Rightarrow \alpha^4 - 6\alpha^2 + 9 = -4\alpha^2 \Leftrightarrow \alpha^4 - 2\alpha^2 + 9 = 0, \end{aligned}$$

also ist $f = X^4 - 2X^2 + 9 \in \mathbb{Q}[X]$ ein normiertes Polynom mit α als Nullstelle. Außerdem hat f auch minimalen Grad mit dieser Eigenschaft, denn wegen $\mathbb{Q}(\sqrt{2}) \subseteq K$ muss $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]$ den Erweiterungsgrad $[K : \mathbb{Q}]$ teilen. Ersterer stimmt mit dem Grad von $X^2 - 2$ überein, da dieses Polynom irreduzibel nach Eisenstein und normiert ist und $\sqrt{2}$ als Nullstelle hat, d. h. das Minimalpolynom von $\sqrt{2}$ über \mathbb{Q} ist.

Wegen $i \notin \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{R}$ ist außerdem $\mathbb{Q}(\sqrt{2}) \subsetneq K$, wir haben also gezeigt, dass $[K : \mathbb{Q}]$ eine gerade Zahl echt größer 2 ist. Damit muss das Minimalpolynom von α mindestens Grad 4 haben. Da f Grad 4 hat und alle weiteren Bedingungen erfüllt, ist dieser Grad genau 4 und f ist das gesuchte Minimalpolynom.

G ist eine Gruppe der Ordnung $[K : \mathbb{Q}] = 4$, sodass G als Gruppe von Primzahlquadratordnung abelsch sein muss. Allerdings kann G nicht zyklisch sein, denn in diesem Fall gäbe es nur eine Untergruppe der Ordnung 2 (und damit von Index 2), sodass es nur eine quadratische Zwischenerweiterung von $K|\mathbb{Q}$ geben würde. Mit $\mathbb{Q}(\sqrt{2})$ und $\mathbb{Q}(i)$ gibt es aber mindestens zwei verschiedene solcher quadratischer Zwischenkörper.

Aufgabe (Herbst 2015, T2A5)

Sei $\xi = \sqrt{2 + \sqrt{2}} \in \mathbb{R}$.

- a** Berechnen Sie das Minimalpolynom m von ξ über \mathbb{Q} .
- b** Zeigen Sie, dass die Körpererweiterung $\mathbb{Q}(\sqrt{2 + \sqrt{2}})|\mathbb{Q}$ galoissch ist und berechnen Sie die Galois-Gruppe.

Lösungsvorschlag zur Aufgabe (Herbst 2015, T2A5)

- a** Wir berechnen

$$\xi^2 = 2 + \sqrt{2} \Rightarrow (\xi^2 - 2)^2 = 2 \Leftrightarrow \xi^4 - 4\xi^2 + 2 = 0,$$

also ist $m = X^4 - 4X^2 + 2 \in \mathbb{Q}[X]$ ein normiertes Polynom mit Nullstelle ξ . Laut dem Eisenstein-Kriterium, angewandt mit $p = 2$, ist m irreduzibel über \mathbb{Q} , also das Minimalpolynom von ξ über \mathbb{Q} .

- b** Mittels Substitution bestimmt man die Nullstellen von m als $\xi, -\xi, \omega, -\omega$, wobei $\omega = \sqrt{2 - \sqrt{2}} \in \mathbb{R}$. Der Zerfällungskörper von m ist dann $\mathbb{Q}(\xi, -\xi, \omega, -\omega)$. Wir zeigen nun $\mathbb{Q}(\xi, -\xi, \omega, -\omega) = \mathbb{Q}(\xi)$. Die Inklusion „ \supseteq “ ist dabei klar. Für die umgekehrte Inklusion suchen wir nach einer Relation zwischen ξ und ω . Wir berechnen daher

$$\omega\xi = \sqrt{(2 - \sqrt{2})(2 + \sqrt{2})} = \sqrt{2}$$

und schließen daraus $\omega = \frac{\sqrt{2}}{\xi}$. Wegen $\sqrt{2} = \xi^2 - 2 \in \mathbb{Q}(\xi)$ gilt somit auch $\omega \in \mathbb{Q}(\xi)$. Dies zeigt „ \subseteq “. Damit ist $\mathbb{Q}(\xi)$ Zerfällungskörper von m über \mathbb{Q} und die Erweiterung $\mathbb{Q}(\xi)|\mathbb{Q}$ ist normal. Da \mathbb{Q} ein perfekter Körper ist, ist sie auch separabel, insgesamt also galoissch.

Es gilt nun

$$|G_{\mathbb{Q}(\xi)|\mathbb{Q}}| = [\mathbb{Q}(\xi) : \mathbb{Q}] = \text{grad } m = 4,$$

also ist $G_{\mathbb{Q}(\xi)|\mathbb{Q}}$ als Gruppe von Primzahlquadratordnung abelsch und somit isomorph zu $\mathbb{Z}/4\mathbb{Z}$ oder zu $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Wir zeigen nun, dass

die Galois-Gruppe ein Element der Ordnung 4 enthält und somit zyklisch ist. Betrachte dazu den \mathbb{Q} -Automorphismus

$$\sigma : \mathbb{Q}(\xi) \rightarrow \mathbb{Q}(\xi) \quad \text{mit} \quad \sigma(\xi) = \omega.$$

Dass es diesen Automorphismus σ gibt, wird vom Fortsetzungssatz 3.15 sicher gestellt. Man berechnet nun

$$\begin{aligned} \sigma(\omega) &= \sigma\left(\frac{\sqrt{2}}{\xi}\right) = \sigma\left(\frac{\xi^2 - 2}{\xi}\right) = \frac{\sigma(\xi)^2 - 2}{\sigma(\xi)} = \frac{\omega^2 - 2}{\omega} = \\ &= \frac{(2 - \sqrt{2}) - 2}{\sqrt{2} - \sqrt{2}} = -\sqrt{2} \cdot \frac{\sqrt{2 + \sqrt{2}}}{\sqrt{(2 - \sqrt{2})(2 + \sqrt{2})}} = -\sqrt{2} \frac{\xi}{\sqrt{2}} = -\xi. \end{aligned}$$

Also ist $\sigma^2(\xi) = \sigma(\omega) = -\xi$ und es muss $\sigma^2 \neq \text{id}_{\mathbb{Q}(\xi)}$ sein. Dies zeigt, dass die Ordnung von σ größer als 2 sein muss. Da die Ordnung von σ zudem ein Teiler der Gruppenordnung 4 sein muss, folgt bereits $\text{ord } \sigma = 4$. Folglich erzeugt σ die Galois-Gruppe, d. h.

$$G_{\mathbb{Q}(\xi)|\mathbb{Q}} = \langle \sigma \rangle \cong \mathbb{Z}/4\mathbb{Z}.$$

Aufgabe (Frühjahr 2012, T3A2)

Sei $p \neq 2$ eine Primzahl, $\zeta := \exp(2\pi i/p) \in \mathbb{C}$ und $\sqrt[p]{p} \in \mathbb{R}_{>0}$. Weiter sei L der Zerfällungskörper des Polynoms $f = X^p - p$ in \mathbb{C} und M der Zerfällungskörper des Polynoms $g = X^{p^2} - 1$ in \mathbb{C} . Zeigen Sie:

- a** $L = \mathbb{Q}(\zeta, \sqrt[p]{p})$.
- b** $[L : \mathbb{Q}] = [M : \mathbb{Q}]$.
- c** Die Galois-Gruppe $G_{L|\mathbb{Q}}$ ist nicht abelsch.
- d** Die Körper L und M sind nicht isomorph.

Lösungsvorschlag zur Aufgabe (Frühjahr 2012, T3A2)

- a** ζ ist primitive p -te Einheitswurzel, also sind durch $\zeta^k \sqrt[p]{p}$ für $0 \leq k \leq p-1$ verschiedene Nullstellen von f gegeben. Dies sind genau p Nullstellen, sodass dies bereits alle sein müssen und L von diesen über \mathbb{Q} erzeugt wird:

$$L = \mathbb{Q}(\sqrt[p]{p}, \zeta \sqrt[p]{p}, \dots, \zeta^{p-1} \sqrt[p]{p}).$$

Es folgt insbesondere $\mathbb{Q}(\zeta, \sqrt[p]{p}) \subseteq L$. Da der Körper $\mathbb{Q}(\zeta, \sqrt[p]{p})$ auch die übrigen Nullstellen von f enthält, bekommt man dadurch auch die umgekehrte Inklusion, d. h. $L = \mathbb{Q}(\zeta, \sqrt[p]{p})$.

- b** Die Nullstellen von g sind gerade die p^2 -ten Einheitswurzeln. Sei ξ eine primitive p^2 -te Einheitswurzel, dann ist also $M = \mathbb{Q}(\xi)$ und $[M : \mathbb{Q}]$ ist der Grad des p^2 -ten Kreisteilungspolynoms:

$$[M : \mathbb{Q}] = \varphi(p^2) = p \cdot (p - 1)$$

f ist irreduzibel nach dem Eisensteinkriterium, sodass f das Minimalpolynom von $\sqrt[p]{p}$ über \mathbb{Q} ist und $[\mathbb{Q}(\sqrt[p]{p}) : \mathbb{Q}] = p$ folgt. Das Minimalpolynom von ζ über $\mathbb{Q}(\sqrt[p]{p})$ ist ein Teiler des p -ten Kreisteilungspolynoms Φ_p , d. h. $[L : \mathbb{Q}(\sqrt[p]{p})] \leq \varphi(p) = p - 1$, sodass $[L : \mathbb{Q}] \leq p \cdot (p - 1)$. Aus $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(p) = p - 1$ und den Inklusionen $\mathbb{Q}(\zeta) \subseteq L$ sowie $\mathbb{Q}(\sqrt[p]{p}) \subseteq L$ folgt nach der Gradformel, dass sowohl p als auch $p - 1$ Teiler von $[L : \mathbb{Q}]$ sind. Da p und $p - 1$ teilerfremd sind, ist $\text{kgV}(p, p - 1) = p \cdot (p - 1)$ und es muss $[L : \mathbb{Q}] = p \cdot (p - 1)$ sein.

Insbesondere ist damit gezeigt:

$$[L : \mathbb{Q}] = p \cdot (p - 1) = [M : \mathbb{Q}].$$

- c** Angenommen, $G_{L|\mathbb{Q}}$ ist abelsch. Dann wäre jede Untergruppe ein Normalteiler, d. h. jede Zwischenerweiterung von $L|\mathbb{Q}$ wäre normal. Insbesondere würde dies für $K = \mathbb{Q}(\sqrt[p]{p})$ zutreffen. Allerdings hat das irreduzible Polynom $f = X^p - p$ eine Nullstelle in K , nämlich $\sqrt[p]{p}$, ohne dass f über K vollständig in Linearfaktoren zerfällt. Tatsächlich ist $\zeta \sqrt[p]{p}$ eine Nullstelle von f , die wegen $\zeta = \cos(2\pi/p) + i \sin(2\pi/p) \notin \mathbb{R}$ (beachte $p \nmid 2 \Rightarrow \frac{2\pi}{p} \notin \pi\mathbb{Z}$) nicht reell ist und somit auch nicht in $K \subseteq \mathbb{R}$ liegen kann. Folglich ist $K|\mathbb{Q}$ keine normale Erweiterung und $G_{L|\mathbb{Q}}$ kann nicht abelsch sein.
- d** Nach Satz 3.18 ist $G_{M|\mathbb{Q}} \cong (\mathbb{Z}/p^2\mathbb{Z})^\times$, insbesondere ist $G_{M|\mathbb{Q}}$ abelsch. Gäbe es nun einen Isomorphismus $\phi: M \rightarrow L$, so wäre auch die Abbildung

$$\phi^*: G_{L|\mathbb{Q}} \rightarrow G_{M|\mathbb{Q}}, \quad \sigma \mapsto \phi^{-1} \circ \sigma \circ \phi$$

ein Isomorphismus. Denn zunächst folgt aus $\phi(1) = 1$ induktiv, dass $\phi|_{\mathbb{Z}} = \text{id}_{\mathbb{Z}}$ und somit auch $\phi|_{\mathbb{Q}} = \text{id}_{\mathbb{Q}}$. Also bildet ϕ^* tatsächlich nach $G_{M|\mathbb{Q}}$ ab. Weiterhin folgt aus $\phi^{-1}\sigma\phi = \text{id}_M$ durch Multiplizieren mit ϕ bzw. ϕ^{-1} bereits $\sigma = \text{id}_L$, d. h. $\ker \phi^* = \{\text{id}_L\}$ und ϕ^* ist injektiv. Da die beiden Galois-Gruppen die gleiche Ordnung haben, folgt daraus auch die Surjektivität.

Wir haben somit einen Widerspruch erhalten, denn die abelsche Gruppe $G_{M|\mathbb{Q}}$ kann unmöglich zur nicht-abelschen Gruppe $G_{L|\mathbb{Q}}$ isomorph sein. Folglich können auch L und M nicht isomorph sein.

Aufgabe (Herbst 2013, T3A1)

Sei $r \geq 1$. Die komplexen Zahlen $\alpha_1, \alpha_2, \dots, \alpha_r$ seien alle algebraisch von Grad 2 über \mathbb{Q} . Setze $K = \mathbb{Q}(\alpha_1, \dots, \alpha_r)$. Zeigen Sie, dass K eine Galois-Erweiterung von \mathbb{Q} ist. Sei $G = \text{Gal}(K/\mathbb{Q})$ und C_2 eine Gruppe der Ordnung 2. Geben Sie einen natürlichen injektiven Gruppenhomomorphismus $G \rightarrow C_2^r$ an.

Lösungsvorschlag zur Aufgabe (Herbst 2013, T3A1)

Sei f_i jeweils das Minimalpolynom von α_i . Setze $f = \prod_{i=1}^r f_i$, dann ist K der Zerfällungskörper von f : Jedes f_i zerfällt in $\mathbb{Q}(\alpha_i) \subseteq K$ in Linearfaktoren, da f_i ein Polynom von Grad 2 ist und Nullstelle α_i hat. Folglich zerfällt f in K . Weiter wird K über \mathbb{Q} von den Nullstellen von f erzeugt, sodass es sich um den Zerfällungskörper handeln muss.

Außerdem ist \mathbb{Q} als Körper der Charakteristik 0 perfekt, sodass $K|\mathbb{Q}$ auch separabel und somit galoissch ist.

Die Erweiterungen $\mathbb{Q}(\alpha_i)|\mathbb{Q}$ sind als Erweiterungen von Grad 2 automatisch normal und damit ebenfalls galoissch. Ist $\sigma \in G_{K|\mathbb{Q}}$, so ist daher $\sigma|_{\mathbb{Q}(\alpha_i)}$ ein Automorphismus von $\mathbb{Q}(\alpha_i)$ und wir haben eine wohldefinierte Abbildung

$$\varphi: G_{K|\mathbb{Q}} \rightarrow G_{\mathbb{Q}(\alpha_1)|\mathbb{Q}} \times \dots \times G_{\mathbb{Q}(\alpha_r)|\mathbb{Q}}, \quad \sigma \mapsto (\sigma|_{\mathbb{Q}(\alpha_1)}, \dots, \sigma|_{\mathbb{Q}(\alpha_r)})$$

Diese Abbildung ist ein Gruppenhomomorphismus und injektiv, denn ist $\sigma \in \ker \varphi$, so bedeutet dies insbesondere $\sigma(\alpha_i) = \alpha_i$. Da die α_i den Körper K als \mathbb{Q} -Vektorraum erzeugen, ist jede \mathbb{Q} -lineare Abbildung $K \rightarrow K$ bereits durch die Bilder der α_i festgelegt. Im vorliegenden Fall bedeutet das gerade $\sigma = \text{id}_K$, d. h. φ ist injektiv.

Da es bis auf Isomorphie nur eine Gruppe der Ordnung 2 gibt und $|G_{\mathbb{Q}(\alpha_i)}| = [\mathbb{Q}(\alpha_i) : \mathbb{Q}] = \deg f_i = 2$ gilt, haben wir $G_{\mathbb{Q}(\alpha_i)} \cong C_2$. Also induziert φ einen injektiven Homomorphismus

$$\phi: G_{K|\mathbb{Q}} \xrightarrow{\varphi} G_{\mathbb{Q}(\alpha_1)|\mathbb{Q}} \times \dots \times G_{\mathbb{Q}(\alpha_r)|\mathbb{Q}} \xrightarrow{\cong} C_2^r.$$

Alternative

Induktion über r . Verwende im Induktionsschritt Proposition 3.23.

Explizite Bestimmung einer Galois-Gruppe

Sei $L|K$ eine endliche Galois-Erweiterung und $f = \sum_{k=0}^n a_k X^k \in K[X]$ ein (nicht zwangsläufig irreduzibles) Polynom, das eine Nullstelle α in L hat. Ist $\sigma \in G_{L|K}$, so gilt

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

d. h. σ bildet jede Nullstelle von f wieder auf eine Nullstelle von f ab. Umgekehrt muss auch das Urbild jeder Nullstelle wieder eine Nullstelle sein, denn da σ ein K -Automorphismus ist, trifft dies auch auf σ^{-1} zu, sodass auch $\sigma^{-1}(\alpha)$ eine Nullstelle von f ist.

Dies hilft nun dabei, K -Automorphismen explizit zu bestimmen.

Anleitung: Explizite Bestimmung von K -Automorphismen

Sei $L|K$ eine endliche Galois-Erweiterung und seien $\alpha_1, \dots, \alpha_n \in L$, sodass $L = K(\alpha_1, \dots, \alpha_n)$. Will man $G_{L|K}$ explizit bestimmen, kann man beispielsweise folgendermaßen vorgehen:

- (1) Finde Polynome f_1, \dots, f_n möglichst kleinen Grades, die $\alpha_1, \dots, \alpha_n$ als Nullstelle haben.
Nach dem Satz vom primitiven Element 3.14 gibt es *ein* $\beta \in L$ mit $L = K(\beta)$, sodass es genügen würde, das Minimalpolynom von β zu bestimmen. Sowohl β als auch dessen Minimalpolynom zu finden, kann sich jedoch im konkreten Fall als sehr schwierig herausstellen.
- (2) Die Nullstellen eines f_i müssen wieder auf Nullstellen von f_i abgebildet werden. Dies liefert Bedingungen an die Bilder der $\alpha_1, \dots, \alpha_n$ unter einem K -Automorphismus.
- (3) Jede Relation zwischen den $\alpha_1, \dots, \alpha_n$ kann weiter helfen.
- (4) Da $\alpha_1, \dots, \alpha_n$ Erzeuger von L als K -Vektorraum sind, ist jedes $\sigma \in G_{L|K}$ bereits durch $\sigma(\alpha_1), \dots, \sigma(\alpha_n)$ eindeutig festgelegt.
- (5) Begründe, z. B. mithilfe des Fortsetzungssatzes 3.15, dass es zu den gefundenen Abbildungsvorschriften tatsächlich K -Homomorphismen gibt.

Aufgabe (Frühjahr 2010, T3A5)

Das Polynom

$$f = X^4 - 2aX^2 + b \in \mathbb{Q}[X]$$

sei irreduzibel, und L bezeichne seinen Zerfällungskörper in \mathbb{C} . Ferner sei

$$K := \mathbb{Q}(\sqrt{a^2 - b}).$$

Beweisen Sie:

- a** Ist $[L : \mathbb{Q}] = 4$, so ist $\sqrt{b} \in K$.
- b** Ist $\sqrt{b} \in \mathbb{Q}$, so ist $G_{L|\mathbb{Q}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
- c** Ist $\sqrt{b} \in K \setminus \mathbb{Q}$, so ist $G_{L|\mathbb{Q}} \cong \mathbb{Z}/4\mathbb{Z}$.
- d** $\sqrt{2} + \sqrt{3}$ ist ein primitives Element der Körpererweiterung $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$.
- e** Welche Struktur hat die Galois-Gruppe $G_{\mathbb{Q}(\sqrt{2}, \sqrt{3})|\mathbb{Q}}$?

Lösungsvorschlag zur Aufgabe (Frühjahr 2010, T3A5)

- a** Die Nullstellen von f berechnen sich (mittels Substitution und Mitternachtsformel) zu

$$\sqrt{a + \sqrt{a^2 - b}}, \quad -\sqrt{a + \sqrt{a^2 - b}}, \quad \sqrt{a - \sqrt{a^2 - b}}, \quad -\sqrt{a - \sqrt{a^2 - b}}.$$

Sei $\xi = \sqrt{a + \sqrt{a^2 - b}}$ und $\omega = \sqrt{a - \sqrt{a^2 - b}}$, dann ist f sowohl das Minimalpolynom von ξ als auch von ω , da f nach Voraussetzung irreduzibel ist. Es folgt

$$[\mathbb{Q}(\xi) : \mathbb{Q}] = 4 \quad \text{und} \quad [\mathbb{Q}(\omega) : \mathbb{Q}] = 4.$$

Wegen $\omega, \xi \in L$ ist $\mathbb{Q}(\xi) \subseteq L$ und $\mathbb{Q}(\omega) \subseteq L$. Zusammen mit $[L : \mathbb{Q}] = 4$ und obigen Erweiterungsgraden liefert die Gradformel $[L : \mathbb{Q}(\xi)] = 1 = [L : \mathbb{Q}(\omega)]$, d. h. $L = \mathbb{Q}(\xi) = \mathbb{Q}(\omega)$.

Wegen $\xi^2 - a = \sqrt{a^2 - b} \in L$ ist auf jeden Fall $K \subseteq L$. Weiter ist

$$\xi^2 \omega^2 = (a + \sqrt{a^2 - b})(a - \sqrt{a^2 - b}) = a^2 - (a^2 - b) = b,$$

sodass $\xi \omega = \pm \sqrt{b}$ in L liegt. Um $\sqrt{b} \in K$ zu zeigen, zeigen wir, dass jedes $\sigma \in G_{L|K}$ auch \sqrt{b} fixiert. Sei also $\sigma \in G_{L|K}$, d. h. es gelte $\sigma(\sqrt{a^2 - b}) = \sqrt{a^2 - b}$. Dann folgt

$$\sigma(\xi)^2 = \sigma(\xi^2) = \sigma(a + \sqrt{a^2 - b}) = a + \sqrt{a^2 - b} = \xi^2$$

und analog

$$\sigma(\omega)^2 = \sigma(\omega^2) = \sigma(a - \sqrt{a^2 - b}) = a - \sqrt{a^2 - b} = \omega^2.$$

Also ist $\sigma(\xi) = \pm\xi$, und $\sigma(\omega) = \pm\omega$. Da ξ die Erweiterung $L|\mathbb{Q}$ erzeugt, ist σ durch Angabe von $\sigma(\xi)$ bereits eindeutig festgelegt, sprich: Ist $\sigma(\xi) = \xi$, so ist $\sigma = \text{id}_L$. Ist andererseits $\sigma(\xi) = -\xi$, so kann nicht $\sigma(\omega) = \omega$ gelten, denn ω erzeugt ebenfalls die Erweiterung $L|\mathbb{Q}$, sodass aus $\sigma(\omega) = \omega$ ebenfalls $\sigma = \text{id}_L$ folgen würde. Es muss daher $\sigma(\omega) = -\omega$ sein. In beiden Fällen folgt

$$\sigma(\sqrt{b}) = \sigma(\pm\xi\omega) = \pm\sigma(\xi)\sigma(\omega) = \pm\xi\omega = \sqrt{b}.$$

Also liegt \sqrt{b} im Fixkörper $L^{G_{L|\mathbb{Q}}} = K$.

Wir werden in den Aufgabenteilen **b** und **c** brauchen, dass die in **a** behauptete Aussage sogar eine Äquivalenz ist. Gilt nämlich $\sqrt{b} \in K$, so ist

$$\xi\omega = \pm\sqrt{b} \Leftrightarrow \omega = \pm\sqrt{b}\xi^{-1} \in \mathbb{Q}(\xi).$$

Also wird auch in diesem Fall L bereits von ξ allein erzeugt und es gilt $[L : \mathbb{Q}] = [\mathbb{Q}(\xi) : \mathbb{Q}] = \text{grad } f = 4$.

- b** Sei $\sigma \in G_{L|\mathbb{Q}}$. Wir zeigen $\sigma^2 = \text{id}_L$, denn das bedeutet, dass jedes Element in $G_{L|\mathbb{Q}}$ höchstens Ordnung 2 hat. Da wir in Teil **a** bereits gesehen haben, dass

$$|G_{L|\mathbb{Q}}| = [L : \mathbb{Q}] = 4$$

beträgt und es nur zwei Gruppen der Ordnung 4, nämlich $\mathbb{Z}/4\mathbb{Z}$ und $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, gibt, muss dann $G_{L|\mathbb{Q}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ sein.

Da σ eine Nullstelle von f wieder auf eine Nullstelle abbilden muss, ist $\sigma(\xi) \in \{\xi, -\xi, \omega, -\omega\}$. Durch Angabe von $\sigma(\xi)$ wird σ bereits eindeutig festgelegt, also folgt aus $\sigma(\xi) = \xi$ und $\sigma(\xi) = -\xi$ jeweils, dass $\sigma^2 = \text{id}_L$ erfüllt ist.

Nach Voraussetzung ist $\sqrt{b} \in \mathbb{Q}$, also ist $\sigma(\sqrt{b}) = \sqrt{b}$ und es folgt

$$\omega\xi = \pm\sqrt{b} = \sigma(\pm\sqrt{b}) = \sigma(\omega\xi) = \sigma(\omega)\sigma(\xi)$$

Falls $\sigma(\xi) = \omega$, so muss also $\sigma(\omega) = \xi$ sein, sodass

$$\sigma^2(\xi) = \sigma(\omega) = \xi \Rightarrow \sigma^2 = \text{id}_L.$$

Vollkommen analog folgt aus $\sigma(\xi) = -\omega$, dass $\sigma(\omega) = -\xi$ und

$$\sigma^2(\xi) = \sigma(-\omega) = -\sigma(\omega) = \xi \Rightarrow \sigma^2 = \text{id}_L.$$

Es gibt daher kein Element der Ordnung 4 in $G_{L|\mathbb{Q}}$, weshalb diese nichtzyklisch sein kann.

- c** Falls $\sqrt{b} \notin \mathbb{Q}$, so muss es ein $\sigma \in G_{L|\mathbb{Q}}$ geben mit $\sigma(\sqrt{b}) \neq \sqrt{b}$. Wir haben bereits gesehen, dass sowohl aus $\sigma(\xi) = \xi$ als auch aus $\sigma(\xi) = -\xi$ folgt, dass $\sigma(\sqrt{b}) = \sqrt{b}$. Die verbleibenden Möglichkeiten für $\sigma(\xi)$ sind $\pm\omega$. Sei also $\varepsilon \in \{+1, -1\}$ mit $\sigma(\xi) = \varepsilon\omega$. Dann folgt aus

$$\xi\omega = \pm\sqrt{b} \neq \sigma(\pm\sqrt{b}) = \sigma(\xi)\sigma(\omega) = \varepsilon\omega\sigma(\omega),$$

dass $\sigma(\omega) \neq \varepsilon\xi$. Andererseits ist $\sigma(\omega) \neq \omega$ und $\sigma(\omega) \neq -\omega$, denn da auch ω die Erweiterung $L|\mathbb{Q}$ erzeugt, würde sonst wie in Teil **a** $\sigma(\xi) = \xi$ bzw. $\sigma(\xi) = -\xi$ folgen. Es bleibt also nur noch $\sigma(\omega) = -\varepsilon\xi$. Dies bedeutet

$$\sigma(\xi) = \varepsilon\omega, \quad \sigma^2(\xi) = -\varepsilon^2\xi = -\xi, \quad \sigma^3(\xi) = -\varepsilon\omega, \quad \sigma^4(\xi) = \varepsilon^2\xi = \xi$$

und somit beträgt die Ordnung von σ vier. Da dies der Gruppenordnung von $G_{L|\mathbb{Q}}$ entspricht, ist σ ein Erzeuger von $G_{L|\mathbb{Q}}$ und es folgt $G_{L|\mathbb{Q}} \cong \mathbb{Z}/4\mathbb{Z}$.

- d** Die Inklusion $\mathbb{Q}(\sqrt{2} + \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$ ist klar. Für die umgekehrte Inklusion bemerken wir, dass

$$\frac{1}{2}[(\sqrt{2} + \sqrt{3})^2 - 5] = \frac{1}{2}[(2 + 2\sqrt{6} + 3) - 5] = \sqrt{6} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$$

und somit

$$\begin{aligned} \sqrt{6} \cdot (\sqrt{2} + \sqrt{3}) - 2(\sqrt{2} + \sqrt{3}) &= 2\sqrt{3} + 3\sqrt{2} - 2(\sqrt{2} + \sqrt{3}) \\ &= \sqrt{2} \in \mathbb{Q}(\sqrt{2} + \sqrt{3}). \end{aligned}$$

Es folgt $\sqrt{3} = (\sqrt{2} + \sqrt{3}) - \sqrt{2} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$. Dies zeigt $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2} + \sqrt{3})$, insgesamt also Gleichheit.

- e** Sei $\alpha = \sqrt{2} + \sqrt{3}$. Wir berechnen das Minimalpolynom von α :

$$\begin{aligned} \alpha^2 &= 2 + 2\sqrt{6} + 3 \Rightarrow (\alpha^2 - 5)^2 = 4 \cdot 6 \Leftrightarrow \alpha^4 - 10\alpha^2 + 25 = 24 \\ &\Leftrightarrow \alpha^4 - 10\alpha^2 + 1 = 0 \end{aligned}$$

Also ist $f = X^4 - 10X^2 + 1$ zumindest ein normiertes Polynom mit Nullstelle α . Um zu zeigen, dass f das Minimalpolynom von α ist, weisen wir $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4 = \text{grad } f$ nach. Die Abschätzung „ \leq “ folgt daraus, dass das Minimalpolynom von α ein Teiler von f ist, also höchstens Grad 4 hat. Unter Verwendung von Teil **d** gilt

$$\mathbb{Q}(\sqrt{2}) \subsetneq \mathbb{Q}(\alpha) \quad \text{und} \quad \mathbb{Q}(\sqrt{3}) \subsetneq \mathbb{Q}(\alpha).$$

Da $\mathbb{Q}(\sqrt{2})$ und $\mathbb{Q}(\sqrt{3})$ quadratische Erweiterungen von \mathbb{Q} sind, ist $[\mathbb{Q}(\alpha) : \mathbb{Q}] > 2$. Außerdem ist $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ nach der Gradformel sogar ein Teiler von $[\mathbb{Q}(\alpha) : \mathbb{Q}]$. Dies zeigt $[\mathbb{Q}(\alpha) : \mathbb{Q}] \geq 4$. Somit ist f tatsächlich das Minimalpolynom von α .

Zu zeigen bleibt, dass $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ der Zerfällungskörper von f ist. Es ist $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ auf jeden Fall der Zerfällungskörper von $(X^2 - 2)(X^3 - 2)$, also ist die Erweiterung $\mathbb{Q}(\sqrt{2}, \sqrt{3})|\mathbb{Q}$ normal. Da f eine Nullstelle in $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$ besitzt, müssen dort schon alle Nullstellen liegen. Daraus folgt bereits, dass $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ der Zerfällungskörper von f über \mathbb{Q} ist.

Es sind nun alle Voraussetzungen von Teil **a** erfüllt. Wegen $\sqrt{1} = 1 \in \mathbb{Q}$, folgt also aus Teil **b**, dass $G_{\mathbb{Q}(\sqrt{2}, \sqrt{3})|\mathbb{Q}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Die Galois-Gruppe eines Polynoms

Es sei K ein Körper und $f \in K[X]$ ein nicht-konstantes und separables Polynom. Falls $\text{char}(K) = 0$, so ist diese Voraussetzung beispielsweise für jedes irreduzible Polynom erfüllt. Sei weiter L der Zerfällungskörper von f , dann ist $L|K$ eine Galois-Erweiterung. Die Galois-Gruppe $G_{L|K}$ heißt auch *Galois-Gruppe von f* und wird oft als $\text{Gal}(f)$ notiert.

Wir haben bereits gesehen, dass ein Element σ der Galois-Gruppe die Nullstellen eines Polynoms wieder auf Nullstellen abbildet. Da der Zerfällungskörper L von den Nullstellen von f über K erzeugt wird, ist σ durch seine Wirkung auf diesen Nullstellen bereits eindeutig festgelegt. Es liegt daher nahe, σ als Permutation der Nullstellen aufzufassen.

Satz 3.24. Sei K ein Körper, $f \in K[X]$ ein separables Polynom von Grad $n > 0$ sowie L der Zerfällungskörper von f über K . Sind $\alpha_1, \dots, \alpha_n \in L$ die Nullstellen von f , so definiert

$$G_{L|K} \rightarrow \text{Per}(\{\alpha_1, \dots, \alpha_n\}) \cong S_n, \quad \sigma \mapsto \sigma|_{\{\alpha_1, \dots, \alpha_n\}}$$

einen injektiven Gruppenhomomorphismus. Insbesondere lässt sich $G_{L|K}$ als Untergruppe der symmetrischen Gruppe S_n auffassen.

Aufgabe (Herbst 2011, T2A4)

Sei $\alpha \in \mathbb{C}$ eine Nullstelle des Polynoms $f = X^3 - 3X + 1 \in \mathbb{Q}[X]$. Zeigen Sie:

- a** Das Polynom f ist irreduzibel über \mathbb{Q} .

- b** Zeigen Sie, dass auch $\alpha^2 - 2$ eine Nullstelle von f ist. Folgern Sie, dass $\mathbb{Q}(\alpha)$ der Zerfällungskörper von f über \mathbb{Q} ist und dass die Galois-Gruppe von f über \mathbb{Q} isomorph zu $\mathbb{Z}/3\mathbb{Z}$ ist.
- c** Es gilt $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$.

Lösungsvorschlag zur Aufgabe (Herbst 2011, T2A4)

- a** Da f ein Polynom mit ganzzahligen Koeffizienten ist, genügt es nach dem Satz von Gauß 2.23, die Irreduzibilität in $\mathbb{Z}[X]$ nachzuweisen. Als Polynom von Grad 3 ist f dort genau dann irreduzibel, wenn es keine ganzzahlige Nullstelle hat. Eine solche Nullstelle müsste den konstanten Koeffizienten von f teilen, kann also nur -1 oder $+1$ sein. Jedoch ist

$$f(1) = -1 \neq 0 \quad \text{und} \quad f(-1) = 3 \neq 0.$$

Also gibt es keine ganzzahlige Nullstelle und f ist irreduzibel in $\mathbb{Z}[X]$.

- b** Wir berechnen mithilfe des binomischen Lehrsatzes und $\alpha^3 = 3\alpha - 1$:

$$\begin{aligned} f(\alpha^2 - 2) &= (\alpha^2 - 2)^3 - 3(\alpha^2 - 2) + 1 = \\ &= \alpha^6 - 3 \cdot 2 \cdot \alpha^4 + 3 \cdot 4 \cdot \alpha^2 - 8 - 3\alpha^2 + 6 + 1 = \\ &= (3\alpha - 1)^2 - 6\alpha(3\alpha - 1) + 12\alpha^2 - 3\alpha^2 - 1 \\ &= 9\alpha^2 - 6\alpha + 1 - 18\alpha^2 + 6\alpha + 9\alpha^2 - 1 = 0 \end{aligned}$$

Angenommen, es wäre $\alpha^2 - 2 = \alpha$, dann wäre $X^2 - X - 2$ ein Polynom von kleinerem Grad als f , das α als Nullstelle hat. Jedoch ist f das Minimalpolynom von α über \mathbb{Q} , sodass das nicht sein kann. Somit hat f bereits zwei verschiedene Nullstellen in $\mathbb{Q}(\alpha)$ und muss dort in Linearfaktoren zerfallen. Sei $\beta \in \mathbb{Q}(\alpha)$ die dritte Nullstelle von f , dann ist $\mathbb{Q}(\alpha) = \mathbb{Q}(\alpha, \alpha^2 - 2, \beta)$, also handelt es sich bei $\mathbb{Q}(\alpha)$ um den Zerfällungskörper von f .

Daraus folgt insbesondere, dass $\mathbb{Q}(\alpha)|\mathbb{Q}$ eine normale Erweiterung ist. Wegen $\text{char}(\mathbb{Q})$ ist sie auch separabel, also galoissch. Es gilt weiter

$$|G_{\mathbb{Q}(\alpha)|\mathbb{Q}}| = [\mathbb{Q}(\alpha) : \mathbb{Q}] = \text{grad } f = 3$$

und da jede Gruppe von Primzahlordnung zyklisch ist, folgt $G_{\mathbb{Q}(\alpha)|\mathbb{Q}} \cong \mathbb{Z}/3\mathbb{Z}$.

- c** Nehmen wir an, es gibt ein $w \in \mathbb{Q}(\alpha)$ mit $w \notin \mathbb{R}$. Betrachte die komplexe Konjugation

$$\iota: \mathbb{Q}(\alpha) \rightarrow \mathbb{C}, \quad x \mapsto \bar{x}.$$

Da $\mathbb{Q}(\alpha)|\mathbb{Q}$ laut Teil **b** eine normale Erweiterung ist, beschränkt sich ι zu einem Automorphismus von $\mathbb{Q}(\alpha)$, d.h. $\iota \in G_{\mathbb{Q}(\alpha)|\mathbb{Q}}$. Wegen $w \notin \mathbb{R}$ ist außerdem $\iota(w) = \bar{w} \neq w$, sodass $\text{ord } \iota > 1$. Jedoch ist

$$\iota^2(v) = \iota(\bar{v}) = v \quad \text{für alle } v \in \mathbb{Q}(\alpha).$$

Also folgt $\text{ord } \iota = 2$. Da Elementordnungen die Gruppenordnung teilen müssen, muss 2 ein Teiler von $|G_{\mathbb{Q}(\alpha)|\mathbb{Q}}| = 3$ sein. Widerspruch.

Aufgabe (Herbst 2003, T2A2)

Sei K ein Teilkörper von \mathbb{C} , der über \mathbb{Q} von endlichem Grad n ist. Zeigen Sie: Ist n ungerade und K normal über \mathbb{Q} , so gilt $K \subseteq \mathbb{R}$.

Lösungsvorschlag zur Aufgabe (Herbst 2003, T2A2)

Da $K|\mathbb{Q}$ nach Voraussetzung normal ist, beschränkt sich die komplexe Konjugation zu einem \mathbb{Q} -Automorphismus von K , welchen wir mit ι bezeichnen. Weiterhin ist \mathbb{Q} ein perfekter Körper, sodass $K|\mathbb{Q}$ auch separabel, d.h. eine endliche Galois-Erweiterung ist. Für den Fixkörper $K^{\langle \iota \rangle} = K \cap \mathbb{R}$ der komplexen Konjugation gilt somit gemäß Galoistheorie

$$[K : K \cap \mathbb{R}] = |G_{K|K \cap \mathbb{R}}| = |\langle \iota \rangle| = \text{ord}(\iota).$$

Nehmen wir nun $K \not\subseteq \mathbb{R}$ an, so gibt es ein nicht-reelles Element $x + iy \in K$ und es ist $\iota(x + iy) = x - iy \neq x + iy$, d.h. die Ordnung von ι kann nicht 1 sein. Da andererseits für jedes $u + iv \in \mathbb{C}$ gilt, dass $\iota^2(u + iv) = \iota(x - iy) = x + iy$, ist $\iota^2 = \iota$, was gerade $\text{ord}(\iota) = 2$ bedeutet. Somit haben wir $[K : K \cap \mathbb{R}] = 2$ und nach der Gradformel teilt 2 den Erweiterungsgrad $[K : \mathbb{Q}] = n$. Widerspruch. Es kann also n nur ungerade sein, wenn bereits $K \subseteq \mathbb{R}$ erfüllt ist.

Aufgabe (Herbst 2013, T1A5)

Es sei $f = X^3 + X - 1 \in \mathbb{Q}[X]$, weiter sei $a \in \mathbb{C}$ eine Nullstelle von f .

- a** Zeigen Sie: f ist irreduzibel.
- b** Geben Sie den Grad $[L : \mathbb{Q}]$ des Zerfällungskörpers L von f über \mathbb{Q} an.
- c** Geben Sie den Isomorphietyp der Galois-Gruppe $G_{L|\mathbb{Q}}$ an.
- d** Geben Sie $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{Q}$ an mit

$$a^4 - 2a^3 = \lambda_1 \cdot 1 + \lambda_2 \cdot a + \lambda_3 \cdot a^2.$$

Lösungsvorschlag zur Aufgabe (Herbst 2013, T1A5)

- a** Das reduzierte Polynom $\bar{f} = X^3 + X + \bar{1} \in \mathbb{F}_2[X]$ hat keine Nullstellen in \mathbb{F}_2 und ist daher als Polynom dritten Grades über diesem Körper irreduzibel. Nach dem Reduktionskriterium 2.26 ist dann auch $f \in \mathbb{Q}[X]$ irreduzibel.
- b** Wegen $f(0) = -1 < 0$ und $f(1) = 1 > 0$ gibt es laut Zwischenwertsatz eine reelle Nullstelle $b \in]0, 1[$. Diese ist die einzige reelle Nullstelle, denn die Ableitung $f' = 3X^2 + 1$ hat keine reelle Nullstelle, während zwischen zwei Nullstellen von f nach dem Satz von Rolle jeweils eine Nullstelle von f' liegen muss. Damit hat f noch eine nicht-reelle Nullstelle $a \in \mathbb{C} \setminus \mathbb{R}$. Da f ein Polynom mit reellen Koeffizienten ist, ist somit auch \bar{a} eine (d. h. die dritte verbleibende) Nullstelle von f .

f ist irreduzibel und normiert, ist also das Minimalpolynom von b über \mathbb{Q} , d. h. $[\mathbb{Q}(b) : \mathbb{Q}] = 3$. Allerdings ist $\mathbb{Q}(b) \subseteq \mathbb{R}$, sodass $a, \bar{a} \notin \mathbb{Q}(b)$.

Schreibe $f = (X - b) \cdot g$ für ein Polynom $g \in \mathbb{Q}(a)[X]$. Das Polynom g muss irreduzibel sein, da es sonst wegen $\text{grad } g = 2$ in Linearfaktoren zerfallen würde, was gerade $a \in \mathbb{Q}(b)$ bedeuten würde. Also ist g das Minimalpolynom von a bzw. \bar{a} über $\mathbb{Q}(b)$ und wir haben $[\mathbb{Q}(a, b) : \mathbb{Q}(b)] = 2$. Da $L = \mathbb{Q}(a, b)$ der Zerfällungskörper von f ist, erhalten wir aus der Gradformel

$$[L : \mathbb{Q}] = [L : \mathbb{Q}(b)] \cdot [\mathbb{Q}(b) : \mathbb{Q}] = 2 \cdot 3 = 6.$$

- c** Wegen $\text{grad } f = 3$ gibt es nach Satz 3.24 einen injektiven Homomorphismus $G_{L|\mathbb{Q}} \hookrightarrow S_3$. Da $|G_{L|\mathbb{Q}}| = [L : \mathbb{Q}] = 6 = |S_3|$ gilt, ist dieser Homomorphismus bereits ein Isomorphismus.
- d** Aus $f(a) = 0$ folgt $a^3 = 1 - a$ und somit

$$a^4 - 2a^3 = a(1 - a) - 2(1 - a) = a - a^2 - 2 + 2a = -a^2 + 3a - 2.$$

Aufgabe (Frühjahr 2014, T2A4)

Seien $a, b \in \mathbb{Q}$ und sei K der Zerfällungskörper des Polynoms

$$P = X^3 + aX + b \in \mathbb{Q}[X].$$

Wir nehmen an, dass P keine Nullstellen in \mathbb{Q} hat. Zeigen Sie:

- a** P ist irreduzibel in $\mathbb{Q}[X]$ und hat keine mehrfachen Nullstellen in K .
- b** Die Galois-Gruppe $G := G_{K|\mathbb{Q}}$ ist eine Untergruppe von S_3 .

- c** G hat entweder 3 oder 6 Elemente.
- d** Sei $\delta = (\alpha_1 - \alpha_2)(\alpha_2 - \alpha_3)(\alpha_3 - \alpha_1)$, wobei $\alpha_1, \alpha_2, \alpha_3$ die Nullstellen von P sind. Dann gilt für $\sigma \in G$ stets $\sigma(\delta) = \delta$ oder $\sigma(\delta) = -\delta$.
- e** Gilt $\sigma(\delta) = \delta$ für alle $\sigma \in G$, dann ist G zyklisch und hat Ordnung 3. Andernfalls ist $G = S_3$.

Lösungsvorschlag zur Aufgabe (Frühjahr 2014, T2A4)

- a** Das Polynom $P(X)$ hat laut Angabe keine Nullstellen in \mathbb{Q} , weshalb die Irreduzibilität bereits mit Lemma 2.21 daraus folgt, dass $P(X)$ den Grad 3 hat. Weiterhin ist jedes irreduzible Polynom aus $\mathbb{Q}[X]$ separabel über \mathbb{Q} , weil \mathbb{Q} ein perfekter Körper ist. Dies bedeutet, dass P keine mehrfachen Nullstellen in einem algebraischen Abschluss von \mathbb{Q} besitzt und somit insbesondere auch keine mehrfachen Nullstellen in K hat.
- b** Der Zerfällungskörper von $P(X)$ wird über \mathbb{Q} von den Nullstellen $\alpha_1, \alpha_2, \alpha_3$ erzeugt, d. h. $K = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3)$. Also wird jedes Element σ der Galois-Gruppe G bereits durch seine Wirkung auf die $\alpha_1, \alpha_2, \alpha_3$ eindeutig festgelegt. Weiterhin gilt

$$\begin{aligned} P(\sigma(\alpha_i)) &= \sigma(\alpha_i)^3 + a\sigma(\alpha_i) + b = \sigma(\alpha_i)^3 + \sigma(a\alpha_i) + \sigma(b) = \\ &= \sigma(P(\alpha_i)) = \sigma(0) = 0 \end{aligned}$$

für jedes $i \in \{1, \dots, 3\}$. Also bildet jedes σ die Menge der Nullstellen von $P(X)$ in sich selbst ab. Anders ausgedrückt: σ **permutiert** die drei Nullstellen von f und wir können σ als Element von S_3 auffassen.

- c** $P(X)$ ist als normiertes und irreduzibles Polynom das Minimalpolynom von α_1 , sodass also

$$[\mathbb{Q}(\alpha_1) : \mathbb{Q}] = \text{grad}(P(X)) = 3.$$

Nach der Gradformel ist folglich 3 ein Teiler von $[K : \mathbb{Q}]$. Für die Galois-Erweiterung $K|\mathbb{Q}$ ist außerdem $[K : \mathbb{Q}] = |G|$. Nach Teil **b** können wir G als Untergruppe von S_3 auffassen und nach dem Satz von Lagrange teilt also $|G|$ die Ordnung $|S_3| = 6$. Es folgt nun

$$3 \text{ teilt } |G| \text{ und } |G| \text{ teilt } 6 \Rightarrow |G| \in \{3, 6\}.$$

- d** Jedes $\sigma \in G$ vertauscht nur die Reihenfolge der $\alpha_1, \alpha_2, \alpha_3$, also wird δ bis auf das Vorzeichen festgehalten.
- e** Gibt es ein $\sigma \in G$ mit $\sigma(\delta) = -\delta$, so kann σ nicht Ordnung 1 haben. Wegen $\sigma^3(\delta) = -\delta$ ist auch Ordnung 3 unmöglich. Da Elementordnungen

die Gruppenordnung teilen müssen, kann G nicht Ordnung 3 haben und nach Teil **c** muss somit $|G| = 6$ sein. Wegen $|S_3| = 6$ folgt bereits $G = S_3$.

Betrachten wir nun den Fall $\sigma(\delta) = \delta$ für alle $\sigma \in G$. Angenommen, es gäbe ein Element der Ordnung 2 in G . Die Elemente der Ordnung 2 in S_3 sind genau die Permutationen $(1\ 2), (1\ 3), (2\ 3)$. Für diese gilt jedoch

$$\begin{aligned}(1\ 2)\delta &= (\alpha_2 - \alpha_1)(\alpha_1 - \alpha_3)(\alpha_3 - \alpha_2) = -\delta \\ (1\ 3)\delta &= (\alpha_3 - \alpha_2)(\alpha_2 - \alpha_1)(\alpha_1 - \alpha_3) = -\delta \\ (2\ 3)\delta &= (\alpha_1 - \alpha_3)(\alpha_3 - \alpha_2)(\alpha_2 - \alpha_1) = -\delta\end{aligned}$$

Also liegt nach Voraussetzung kein Element der Ordnung 2 in G und G kann nicht S_3 sein. Nach **c** hat daher G genau 3 Elemente und ist als Gruppe von Primzahlordnung zyklisch.

Aufgabe (Frühjahr 2011, T2A4)

Bestimmen Sie zwei irreduzible Polynome $f, g \in \mathbb{Q}[X]$, so dass die Galois-Gruppen $\text{Gal}(f)$ und $\text{Gal}(g)$ gleich viele Elemente haben, aber nicht isomorph sind.

Lösungsvorschlag zur Aufgabe (Frühjahr 2011, T2A4)

Hier gibt es viele Möglichkeiten, solche zwei Polynome anzugeben. Wir führen den Beweis für die kleinstmögliche Ordnung solcher Galois-Gruppen, nämlich 4 (für kleinere Ordnungen gibt es nämlich nur die zyklischen Gruppen dieser Ordnung).

Wir bestimmen zunächst das Minimalpolynom von $\alpha = \sqrt{2} + i$:

$$\begin{aligned}\alpha - i &= \sqrt{2} \quad \Rightarrow \quad \alpha^2 - 2i\alpha - 1 = 2 \quad \Leftrightarrow \quad \alpha^2 - 3 = 2i\alpha \\ &\Rightarrow \quad \alpha^4 - 6\alpha^2 + 9 = -4\alpha^2 \quad \Leftrightarrow \quad \alpha^4 - 2\alpha^2 + 9 = 0\end{aligned}$$

Damit ist $f = X^4 - 2X^2 + 9$ ein normiertes Polynom aus $\mathbb{Q}[X]$, das α als Nullstelle hat. Zum Nachweis, dass f das Minimalpolynom von α über \mathbb{Q} ist, ist noch $4 = \text{grad } f = [\mathbb{Q}(\alpha) : \mathbb{Q}]$ zu zeigen. Da das Minimalpolynom von α über \mathbb{Q} ein Teiler von f ist, gilt schon mal $[\mathbb{Q}(\alpha) : \mathbb{Q}] \leq 4$.

Für „ \geq “ zeigt man zuerst $\sqrt{2}, i \in \mathbb{Q}(\alpha)$. Diese Gleichung haben wir in F15T1A5 (Seite 179) bereits nachgerechnet. Also ist wegen $i \notin \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{R}$ und $\sqrt{2}, i \in \mathbb{Q}(\sqrt{2} + i)$ der Körper $\mathbb{Q}(\sqrt{2})$ ein *echter* Teilkörper von $\mathbb{Q}(\alpha)$. Folglich muss

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] > [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$$

gelten. Dabei haben wir benutzt, dass das Minimalpolynom von $\sqrt{2}$ über \mathbb{Q} durch $X^2 - 2$ gegeben ist. Laut Gradformel ist $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ sogar ein Teiler von $[\mathbb{Q}(\alpha) : \mathbb{Q}]$. Dies zeigt

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] \geq 4$$

Wir haben nachgewiesen, dass f das Minimalpolynom von α über \mathbb{Q} , d.h. insbesondere irreduzibel über \mathbb{Q} ist. Sei L der Zerfällungskörper von f . Dann ist auf jeden Fall $\mathbb{Q}(\alpha) \subseteq L$. Wir haben oben gesehen, dass $i, \sqrt{2} \in \mathbb{Q}(\alpha)$, also liegen auch die anderen Nullstellen von f , nämlich $-\alpha, \bar{\alpha}$ und $-\bar{\alpha}$, in $\mathbb{Q}(\alpha)$. Es folgt $L = \mathbb{Q}(\alpha)$.

Als Konsequenz ist $L|\mathbb{Q}$ eine normale Erweiterung, wegen $\text{char}(\mathbb{Q}) = 0$ sogar galoissch. Die zugehörige Galois-Gruppe hat Ordnung 4, ist also abelsch. Wäre sie zyklisch, gäbe es genau einen quadratischen Zwischenkörper, der zu der einzigen Untergruppe von $G_{L|\mathbb{Q}}$ von Index 2 korrespondiert. Allerdings sind $\mathbb{Q}(i), \mathbb{Q}(\sqrt{2})$ mindestens zwei verschiedene quadratische Zwischenerweiterungen.

Es ist nun verhältnismäßig einfach, eine zyklische Galois-Erweiterung von Grad 4 anzugeben: Betrachte das fünfte Kreisteilungspolynom

$$\Phi_5 = X^4 + X^3 + X^2 + X + 1 \in \mathbb{Q}[X].$$

Bekanntlich ist dieses irreduzibel über \mathbb{Q} und hat Zerfällungskörper $\mathbb{Q}(\xi_5)$ mit einer fünften primitiven Einheitswurzel $\xi_5 \in \mathbb{C}$. Außerdem ist

$$G_{\mathbb{Q}(\xi_5)|\mathbb{Q}} \cong (\mathbb{Z}/5\mathbb{Z})^\times \cong \mathbb{Z}/4\mathbb{Z}$$

zyklisch. Insbesondere $|G_{\mathbb{Q}(\alpha)|\mathbb{Q}}| = 4 = |G_{\mathbb{Q}(\xi_5)|\mathbb{Q}}|$, aber $G_{\mathbb{Q}(\alpha)|\mathbb{Q}} \not\cong G_{\mathbb{Q}(\xi_5)|\mathbb{Q}}$.

Aufgabe (Frühjahr 2003, T1A4)

Sei f ein Polynom vom Grad n mit Koeffizienten in einem Körper k . Der Zerfällungskörper K von f über k habe den Grad $n!$ über k . Zeigen Sie, dass f irreduzibel ist, und dass die Galois-Gruppe von f über k die symmetrische Gruppe S_n ist.

Lösungsvorschlag zur Aufgabe (Frühjahr 2003, T1A4)

Für $n = 1$ ist die Behauptung klar, sei also $n \geq 2$. Angenommen, f ist reduzibel. Wir zeigen durch vollständige Induktion über r : Sind $\alpha_1, \dots, \alpha_n \in K$ die (nicht notwendigerweise verschiedenen) Nullstellen von f , so ist $[k : k(\alpha_1, \dots, \alpha_r)] < \frac{n!}{(n-r)!}$ für jedes $r \in \{1, \dots, n\}$.

Induktionsanfang $r = 1$: Da f nach Voraussetzung reduzibel ist, ist das Minimalpolynom von α_1 über k ein echter Teiler von f und daher echt kleineren Grades als f . Somit ist $[k : k(\alpha_1)] < n = \frac{n!}{(n-1)!}$. Setzen wir die Aussage also für ein r als bereits bewiesen voraus.

Induktionsschritt $r \mapsto r + 1$: Über $k(\alpha_1, \dots, \alpha_r)$ kann man f schreiben als

$$f = g \cdot \prod_{i=1}^r (X - \alpha_i)$$

mit einem Polynom $g \in k(\alpha_1, \dots, \alpha_r)[X]$. Es ist dann α_{r+1} eine Nullstelle von g (ob α_{r+1} bereits unter den ersten r Nullstellen auftaucht, spielt dabei keine Rolle). Folglich ist das Minimalpolynom von α_{r+1} über $k(\alpha_1, \dots, \alpha_r)$ ein Teiler von g und hat höchstens Grad $n - r$. Unter Verwendung der Gradformel und der Induktionsvoraussetzung erhalten wir dann

$$\begin{aligned} [k(\alpha_1, \dots, \alpha_{r+1}) : k] &= [k(\alpha_1, \dots, \alpha_{r+1}) : k(\alpha_1, \dots, \alpha_r)] \cdot [k(\alpha_1, \dots, \alpha_r) : k] < \\ &< (n - r) \cdot \frac{n!}{(n-r)!} = \frac{n!}{(n-(r+1))!} \end{aligned}$$

wie gewünscht. Aus der damit bewiesenen Behauptung folgt nun $[K : k] = [k(\alpha_1, \dots, \alpha_n) : k] < n!$ im Widerspruch zur Voraussetzung und somit muss f irreduzibel sein.

Elemente der Galois-Gruppe $G_{K|k}$ permutieren die Nullstellen $\{\alpha_1, \dots, \alpha_n\}$, können also als Elemente von S_n aufgefasst werden. Da S_n und $G_{K|k}$ die gleiche Gruppenordnung haben, muss es sich bei $G_{K|k}$ also bereits um die volle S_n handeln.

Primitive Elemente

Wir erinnern an dieser Stelle daran, dass ein *primitives Element* einer Körpererweiterung $L|K$ ein Element $\alpha \in L$ ist, für das $L = K(\alpha)$ gilt.

Aufgabe (Frühjahr 2015, T3A5)

Sei $E|K$ eine Galois-Erweiterung mit zyklischer Galois-Gruppe und $[E : K] = p^n$ für eine Primzahl p und $n \geq 1$. Weiter sei $K \subset F \subset E$ ein Zwischenkörper mit $[F : K] = p^{n-1}$. Zeigen Sie: Jedes Element von $E \setminus F$ ist ein primitives Element von E über K .

Lösungsvorschlag zur Aufgabe (Frühjahr 2015, T3A5)

Da die Galois-Gruppe $G_{E|K}$ zyklisch ist, gibt es zu jeder Potenz p^i mit $0 \leq i \leq n$ genau eine Untergruppe $U_i \subseteq G_{E|K}$ mit $|U_i| = p^i$. Jede dieser

Untergruppen enthält genau diejenigen Elemente aus $G_{E|K}$, deren Ordnung ein Teiler von p^i ist. Man erhält also eine aufsteigende Kette

$$\{\text{id}_E\} = U_0 \subseteq U_1 \subseteq \dots \subseteq U_n = G_{E|K},$$

die nach dem Hauptsatz der Galoistheorie zu der eindeutigen absteigenden Kette der Zwischenerweiterungen von $E|K$ korrespondiert:

$$E = K_n \supseteq K_{n-1} \supseteq \dots \supseteq K_1 \supseteq K_0 = K$$

Wichtig festzustellen ist dabei, dass jeder Zwischenkörper von $E|K$ mit einem der K_i übereinstimmt. Sei also nun $\alpha \in E \setminus F$. Es kann dann $K(\alpha)$ nicht in F liegen, wegen der Kettenanordnung muss also F ein echter Teilkörper von $K(\alpha)$ sein. Da aber der Erweiterungsgrad $[K(\alpha) : F]$ ein Teiler von $[E : F] = p$ sein muss und 1 ausgeschlossen ist, muss $[K(\alpha) : F] = p$ sein. Aus der Gradformel folgt dann

$$[E : K(\alpha)] = \frac{[E : F]}{[K(\alpha) : F]} = \frac{p}{p} = 1 \quad \Leftrightarrow \quad E = K(\alpha).$$

Aufgabe (Herbst 2013, T2A3)

- a** Zeigen Sie, dass die alternierende Gruppe A_4 keine Untergruppe der Ordnung 6 besitzt.
- b** Sei K ein Körper, der eine galoissche Erweiterung mit Galois-Gruppe A_4 besitzt. Zeigen Sie, dass eine endliche Körpererweiterung $K \subseteq F$ mit $[F : K] = 4$ existiert, sodass $F = K(\alpha)$ für alle $\alpha \in F \setminus K$ gilt.

Lösungsvorschlag zur Aufgabe (Herbst 2013, T2A3)

- a** Angenommen, es gibt eine Untergruppe $N \subseteq A_4$ mit $|N| = 6$. Nach dem Satz von Lagrange ist dann $(A_4 : N) = 2$, sodass N ein Normalteiler von A_4 und A_4/N eine Gruppe der Ordnung 2 ist. Für alle $\sigma \in A_4$ gilt daher

$$(\sigma N)^2 = N \quad \Leftrightarrow \quad \sigma^2 N = N \quad \Leftrightarrow \quad \sigma^2 \in N.$$

Insbesondere also

$$(1 \ 2 \ 3)^2 = (1 \ 3 \ 2) \in N \quad (2 \ 3 \ 4)^2 = (2 \ 4 \ 3) \in N \quad (1 \ 4 \ 2)^2 = (1 \ 2 \ 4) \in N.$$

Jedes dieser Elemente erzeugt eine andere Untergruppe der Ordnung 3. Wir zählen nun Elemente (vgl. Seite 41) und sehen, dass N mindestens

$$3 \cdot 2 + 1 = 7$$

Elemente enthalten müsste. Widerspruch.

- b** Sei L der Erweiterungskörper mit Galois-Gruppe A_4 aus der Angabe. Es gibt mindestens eine Untergruppe U der Ordnung 3 in A_4 , beispielsweise $U = \langle (123) \rangle$. Nach dem Hauptsatz der Galoistheorie ist dann der zugehörige Fixkörper L^U ein Zwischenkörper von $L|K$ mit

$$[L^U : K] = (A_4 : U) = \frac{12}{3} = 4.$$

Sei nun $\alpha \in L^U \setminus K$. Der Erweiterungsgrad $[K(\alpha) : K]$ ist dann ein Teiler von $[L^U : K] = 4$. Wegen $\alpha \notin K$ ist $K \subsetneq K(\alpha)$ und somit $[K(\alpha) : K] > 1$. Nehmen wir an, es ist $[K(\alpha) : K] = 2$. Nach der Gradformel folgt

$$[L : K(\alpha)] = \frac{[L : K]}{[K(\alpha) : K]} = \frac{12}{2} = 6.$$

Damit ist $G_{L|K(\alpha)}$ eine Untergruppe der Ordnung 6 von A_4 . Nach Teil **a** gibt es eine solche Untergruppe jedoch nicht. Es kann deshalb unmöglich $[K(\alpha) : K] = 2$ sein, und es verbleibt nur noch $[K(\alpha) : K] = 4$. Dies bedeutet $[L^U : K(\alpha)] = 1$, d.h. $L^U = K(\alpha)$. Wir haben insgesamt nachgewiesen, dass L^U die gewünschte Eigenschaft besitzt.

Aufgabe (Frühjahr 2014, T1A2)

Es sei $L \supseteq K$ eine endliche Galois-Erweiterung. Zeigen Sie, dass für $\alpha \in L$ folgende Aussagen äquivalent sind:

- a** Es gilt $L = K(\alpha)$.
- b** Für alle $g \in G_{L|K}$ mit $g \neq \text{id}_L$ gilt $g(\alpha) \neq \alpha$.

Lösungsvorschlag zur Aufgabe (Frühjahr 2014, T1A2)

„ \Rightarrow “: Sei $L = K(\alpha)$ und $[K(\alpha) : K] = n$, dann ist durch $1, \alpha, \dots, \alpha^{n-1}$ eine K -Basis von L gegeben, sodass jedes Element $g \in G_{L|K}$ bereits durch seine Wirkung auf α eindeutig festgelegt ist. Also folgt aus $g \neq \text{id}_L$ auch $g(\alpha) \neq \text{id}_L(\alpha) = \alpha$.

„ \Leftarrow “: Wegen $\alpha \in L$ ist $K(\alpha) \subseteq L$ und nach dem Hauptsatz der Galois-Theorie ist $K(\alpha)$ der Fixkörper einer Untergruppe von $G_{L|K}$. Nach Voraussetzung wird aber α nur von id_L fixiert, sodass also $K(\alpha)$ der Fixkörper von $\{\text{id}_L\}$ sein muss. Da auch L diese Eigenschaft besitzt und die Zuordnung eindeutig ist, folgt daraus $L = K(\alpha)$.

Aufgabe (Frühjahr 2013, T2A5)

Sei $L|K$ eine endliche, galoissche Körpererweiterung. Sei $L' \supseteq K$ eine beliebige weitere Körpererweiterung von K . Zeigen Sie: Gibt es genau einen Körperhomomorphismus² $\phi: L \rightarrow L'$ mit $\phi|_K = \text{id}_K$, so ist schon $K = L$.

Lösungsvorschlag zur Aufgabe (Frühjahr 2013, T2A5)

Angenommen, es ist $K \neq L$, dann ist insbesondere $|G_{L|K}| = [L : K] \geq 2$. Wir können deshalb $\sigma, \tau \in G_{L|K}$ mit $\sigma \neq \tau$ wählen. Dann sind

$$\phi \circ \sigma: L \rightarrow L' \quad \text{und} \quad \phi \circ \tau: L \rightarrow L'$$

Homomorphismen mit $(\phi \circ \sigma)|_K = \text{id}_K$ und $(\phi \circ \tau)|_K = \text{id}_K$. Außerdem sind diese beiden Abbildungen verschieden, denn wäre für alle $x \in L$ die Gleichung

$$(\phi \circ \sigma)(x) = (\phi \circ \tau)(x) \iff \phi(\sigma(x)) = \phi(\tau(x))$$

erfüllt, so würde $\sigma(x) = \tau(x)$ für alle $x \in L$ folgen, da ϕ als Homomorphismus von Körpern injektiv ist. Dies bedeutet $\sigma = \tau$ – im Widerspruch zu $\sigma \neq \tau$. Also gibt es mehr als einen K -Homomorphismus $L \rightarrow L'$. Wir erhalten einen Widerspruch, weswegen die Annahme $K \neq L$ falsch gewesen sein muss.

Galois-Theorie und Sylowsätze**Aufgabe (Frühjahr 2004, T1A3)**

Sei k ein Körper, der keine Galois-Erweiterung vom Grad 3 hat. Kann k dann eine Galois-Erweiterung vom Grad 225 haben?

Lösungsvorschlag zur Aufgabe (Frühjahr 2004, T1A3)

Angenommen, es gibt eine Galois-Erweiterung $K|k$ von Grad 225. Sei G die zugehörige Galois-Gruppe, welche die Ordnung $225 = 15^2 = 3^2 \cdot 5^2$ hat. Für die Anzahl v_5 der 5-Sylowgruppen gilt

$$v_5 \mid 9 \quad \text{und} \quad v_5 \equiv 1 \pmod{5} \Rightarrow v_5 = 1.$$

² Die Originalaufgabe sprach von einem Ringhomomorphismus. Jeder Ringhomomorphismus zwischen zwei Körpern ist jedoch laut Definition ein Körperhomomorphismus.

Sei P_5 die einzige 5-Sylowgruppe, dann ist diese ein Normalteiler von G . Folglich ist $K^{P_5}|k$ eine Galois-Erweiterung von $\text{Grad}(G : P_5) = 9$. Sei $H = G_{K^{P_5}|k}$ die zugehörige Galois-Gruppe, dann besitzt diese nach Satz 1.26 eine Untergruppe U der Ordnung 3. Außerdem ist H als Gruppe von Primzahlquadratordnung abelsch, sodass U auch ein Normalteiler von H ist. Es folgt, dass $(K^{P_5})^U|k$ eine Galois-Erweiterung von $\text{Grad}(H : U) = 3$ ist. Widerspruch.

Aufgabe (Herbst 2012, T2A4)

Sei p eine Primzahl. Sei K ein Körper der Charakteristik 0.

- a** Sei E eine (endliche) galoissche Körpererweiterung von K . Zeigen Sie, dass $E|K$ einen Zwischenkörper $F|K$ besitzt, so dass der Grad $[E : F]$ eine p -Potenz ist und der Grad $[F : K]$ nicht von p geteilt wird. (Die Zahl 1 ist eine p -Potenz für jede Primzahl p .)
- b** Besitze K die Eigenschaft, dass der Grad $[L : K]$ jeder nicht trivialen endlichen Körpererweiterung $L|K$ von p geteilt wird. Zeigen Sie, dass dann der Grad einer jeden endlichen Körpererweiterung über K eine p -Potenz ist.

Lösungsvorschlag zur Aufgabe (Herbst 2012, T2A4)

- a** Sei $[E : K] = n$. Die Galois-Gruppe $G_{E|K}$ hat dann ebenfalls Ordnung n . Schreibe $n = m \cdot p^r$ mit $m \in \mathbb{N}$, $r \in \mathbb{N}_0$ und $p \nmid m$, dann gibt es nach Satz 1.26 eine p -Sylowgruppe $H \subseteq G_{E|K}$, d.h. eine Untergruppe mit $|H| = p^r$. Setze $F = E^H$, dann gilt

$$[E : F] = |G_{E|E^H}| = |H| = p^r \quad \text{und} \quad [F : K] = \frac{[E : K]}{[E : F]} = \frac{n}{p^r} = m$$

wie gewünscht.

- b** Angenommen, es gibt einen Erweiterungskörper L von K , sodass $[L : K]$ keine p -Potenz ist. Wir betrachten eine normale Hülle $N|L$ von L . Deren Erweiterungsgrad ist ein Vielfaches von $[L : K]$, hat also die Form $p^r m$ mit $r \in \mathbb{N}_0$ und $m \in \mathbb{N}$, $m \neq 1$ und $p \nmid m$. Da $N|K$ eine normale und separable Erweiterung ist (wegen $\text{char } K = 0$ ist K perfekt), gibt es dann mit Teil **a** einen (nicht-trivialen) Zwischenkörper $F \subseteq N$ mit $[N : F] = p^r$ und $[F : K] = m$. Wegen $m \neq 1$ ist die Erweiterung $F|K$ nicht-trivial, hat aber auch einen Grad, der nicht von p geteilt wird. Widerspruch zur Voraussetzung.

Aufgabe (Herbst 2014, T1A1)

Es seien $L \supseteq K$ eine endliche Galois-Erweiterung und p eine Primzahl, die den Körpergrad $[L : K]$ teilt.

- a** Zeigen Sie, dass es einen Zwischenkörper $K \subseteq Z \subseteq L$ gibt, so dass

$$[L : Z] = p^m \quad \text{und} \quad p \nmid [Z : K]$$

für ein $m \in \mathbb{N}$ gilt.

- b** Bestimmen Sie im Fall $K = \mathbb{Q}, L = \mathbb{Q}(\zeta_7)$ mit einer primitiven siebten Einheitswurzel ζ_7 und $p = 3$ einen solchen Zwischenkörper, indem Sie ein primitives Element α dafür angeben.

Lösungsvorschlag zur Aufgabe (Herbst 2014, T1A1)

- a** Sei $G_{L|K}$ die Galois-Gruppe von $L|K$ und $[L : K] = k \cdot p^m$ mit $k, m \in \mathbb{N}$ und $p \nmid k$. Es hat $G_{L|K}$ Ordnung $[L : K]$, also gibt es laut Satz 1.26 eine Untergruppe $H \subseteq G_{L|K}$ mit $|H| = p^m$. Sei L^H der Fixkörper von H , dann gilt

$$[L : L^H] = |G_{L|L^H}| = |H| = p^m \quad \text{und} \quad [L^H : K] = (G_{L|K} : H) = \frac{kp^m}{p^m} = k.$$

Setze also $Z = L^H$.

- b** Es ist $[L : K] = \varphi(7) = 6$, also ist ein Körper $Z \subseteq L$ mit

$$[L : Z] = 3 \quad \text{und} \quad [Z : \mathbb{Q}] = 2$$

gesucht. Wir suchen daher nach einer Untergruppe $H \subseteq G_{L|K}$ mit $|H| = 3$. Dazu verwenden wir den bekannten Isomorphismus (vgl. auch die nachfolgende Aufgabe)

$$G_{L|K} \rightarrow (\mathbb{Z}/7\mathbb{Z})^\times \cong \mathbb{Z}/6\mathbb{Z}, \quad \tau_k : \{\zeta \mapsto \zeta^k\} \mapsto \bar{k}.$$

$\mathbb{Z}/6\mathbb{Z}$ ist eine zyklische Gruppe, besitzt also genau eine solche Untergruppe der Ordnung 3. Man sieht anhand von

$$\bar{2} \neq \bar{0}, \quad \bar{2} + \bar{2} \neq \bar{0}, \quad \bar{2} + \bar{2} + \bar{2} = \bar{0}$$

schnell ein, dass $\bar{2}$ Ordnung 3 in $\mathbb{Z}/6\mathbb{Z}$ hat. Setze also $H = \langle \tau_2 \rangle$, wobei τ_2 durch $\zeta \mapsto \zeta^2$ festgelegt ist. Wir suchen nun nach dem Fixkörper L^H .

Dazu wählen wir ζ, \dots, ζ^6 als K -Basis von L und ein beliebiges Element

$$\beta = a_1\zeta + a_2\zeta^2 + a_3\zeta^3 + a_4\zeta^4 + a_5\zeta^5 + a_6\zeta^6 \in L^H.$$

Die Forderung $\tau_2(\beta) = \beta$ liefert

$$\begin{aligned} & a_1\zeta^2 + a_2\zeta^4 + a_3\zeta^6 + a_4\zeta^8 + a_5\zeta^{10} + a_6\zeta^{12} \\ &= a_1\zeta + a_2\zeta^2 + a_3\zeta^3 + a_4\zeta^4 + a_5\zeta^5 + a_6. \end{aligned}$$

Unter Verwendung von $\zeta^7 = 1$ liefert Koeffizientenvergleich, dass

$$\begin{aligned} a_1 &= a_2, \quad a_2 = a_4, \quad a_3 = a_6, \quad a_4 = a_1, \quad a_5 = a_3, \quad a_6 = a_5 \\ \Leftrightarrow \quad a_1 &= a_2 = a_4 \quad \text{und} \quad a_3 = a_5 = a_6, \end{aligned}$$

also vereinfacht sich obige Darstellung zu

$$\beta = a_1(\zeta + \zeta^2 + \zeta^4) + a_3(\zeta^3 + \zeta^5 + \zeta^6).$$

Nun bemerken wir noch

$$\begin{aligned} (\zeta + \zeta^2 + \zeta^4)^2 &= (\zeta + \zeta^2)^2 + 2(\zeta + \zeta^2)\zeta^4 + \zeta^8 = \\ &= \zeta^2 + 2\zeta^3 + \zeta^4 + 2\zeta^5 + 2\zeta^6 + \zeta = \\ &= \Phi_7(\zeta) - 1 + \zeta^3 + \zeta^5 + \zeta^6 = \\ &= \zeta^3 + \zeta^5 + \zeta^6 - 1, \end{aligned}$$

wobei $\Phi_7 = X^6 + \dots + X + 1$ das siebte Kreisteilungspolynom bezeichnet. Sei $\alpha = \zeta + \zeta^2 + \zeta^4$, dann haben wir $\zeta^3 + \zeta^5 + \zeta^6 = \alpha^2 + 1$ und somit $\beta \in \mathbb{Q}(\alpha)$ nachgewiesen. Da β beliebig aus L^H gewählt war, folgt $L^H \subseteq \mathbb{Q}(\alpha)$. Umgekehrt ist $\tau_2(\alpha) = \alpha$ klar, also gilt auch $\mathbb{Q}(\alpha) \subseteq L^H$ und es folgt $L^H = \mathbb{Q}(\alpha)$.

Aufgabe (Herbst 2015, T3A4)

Es sei $p \geq 3$ eine Primzahl und $a \in \mathbb{Q}$ eine rationale Zahl, so dass $X^p - a$ irreduzibel über \mathbb{Q} ist. Ferner sei $\zeta \in \mathbb{C}$ eine primitive p -te Einheitswurzel, $\alpha \in \mathbb{C}$ eine beliebige Nullstelle von $X^p - a$ und $Z := \mathbb{Q}(\alpha, \zeta)$.

- a** Zeigen Sie, dass Z ein Zerfällungskörper von $X^p - a$ ist und $[Z : \mathbb{Q}] = p(p-1)$ gilt.
- b** Zeigen Sie, dass $G_{Z|\mathbb{Q}}$ eine p -Sylowgruppe H besitzt, die ein Normalteiler ist, und dass

$$G_{Z|\mathbb{Q}}/H \cong \left(\mathbb{Z}/p\mathbb{Z}\right)^\times = \mathbb{Z}/p\mathbb{Z} \setminus \{0\}$$

gilt.

- c** Bestimmen Sie einen Gruppenisomorphismus $G_{Z|\mathbb{Q}(\alpha)} \xrightarrow{\cong} (\mathbb{Z}/p\mathbb{Z})^\times$.
- d** Zeigen Sie, dass $G_{Z|\mathbb{Q}}$ mehr als eine 2-Sylowgruppe besitzt.

Lösungsvorschlag zur Aufgabe (Herbst 2015, T3A4)

a Sei Z ein Zerfällungskörper von $X^p - a$. Da α Nullstelle von $X^p - a$ ist, ist auf jeden Fall $\alpha \in Z$. Daher muss auch $\alpha^{-1} \in Z$ sein. Weiterhin ist $\alpha\xi$ eine Nullstelle von $X^p - a$ und liegt deshalb ebenfalls in Z . Außerdem ist $\xi = \alpha^{-1} \cdot \alpha\xi \in Z$, sodass $\mathbb{Q}(\alpha, \xi) \subseteq Z$. Da $X^p - a$ über $\mathbb{Q}(\alpha, \xi)$ bereits vollständig in Linearfaktoren zerfällt, ist umgekehrt auch $Z \subseteq \mathbb{Q}(\alpha, \xi)$ und wir erhalten Gleichheit.

Wegen $\mathbb{Q}(\alpha) \subseteq Z$ und $\mathbb{Q}(\xi) \subseteq Z$ wird nun $[Z : \mathbb{Q}]$ sowohl von $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \text{grad}(X^p - a) = p$ als auch von $[\mathbb{Q}(\xi) : \mathbb{Q}] = \varphi(p) = p - 1$ geteilt. Wegen $\text{ggT}(p, p - 1) = 1$ ist also $[Z : \mathbb{Q}]$ ein Vielfaches von $p \cdot (p - 1)$. Andererseits ist das Minimalpolynom von α über $\mathbb{Q}(\xi)$ ein Teiler von $X^p - a$, hat folglich höchstens Grad p . Somit ist

$$[Z : \mathbb{Q}] = [\mathbb{Q}(\xi)(\alpha) : \mathbb{Q}(\xi)] \cdot [\mathbb{Q}(\xi) : \mathbb{Q}] \leq (p - 1) \cdot p$$

und es muss bereits $[Z : \mathbb{Q}] = p \cdot (p - 1)$ sein.

b Sei $G = G_{Z|\mathbb{Q}}$. Laut dem Sylowsatz 1.27 (3) gilt für die Anzahl ν_p der p -Sylowgruppen von G :

$$\nu_p \equiv 1 \pmod{p} \quad \text{und} \quad \nu_p \mid (p - 1).$$

Aus der zweiten Bedingung folgt insbesondere $\nu_p \leq (p - 1)$, sodass nur $\nu_p = 1$ beide Bedingungen erfüllt. Sei H die p -Sylowgruppe von G , dann ist H als einzige p -Sylowgruppe insbesondere ein Normalteiler von G . Laut dem Hauptsatz der Galois-Theorie 3.20 korrespondiert H zu einem eindeutigen (!) Zwischenkörper K von $Z|\mathbb{Q}$ mit $G_{Z|K} = H$. Insbesondere ist $[Z : K] = |H| = p$ und da nach Teil **a** die Gleichung

$$[Z : \mathbb{Q}(\xi)] = \frac{[Z : \mathbb{Q}]}{[\mathbb{Q}(\xi) : \mathbb{Q}]} = \frac{p(p - 1)}{p - 1} = p$$

erfüllt ist, muss $K = \mathbb{Q}(\xi)$ sein. Die Galois-Theorie (genauer Proposition 3.22) liefert uns nun weiterhin

$$G_{Z|\mathbb{Q}} / G_{Z|\mathbb{Q}(\xi)} \cong G_{\mathbb{Q}(\xi)|\mathbb{Q}} \cong (\mathbb{Z}/p\mathbb{Z})^\times,$$

wobei die letzte Isomorphie aus Satz 3.18 stammt.

- c** Da die Erweiterung $Z|\mathbb{Q}$ von α und ξ erzeugt wird, ist jedes $\sigma \in G_{Z|\mathbb{Q}(\alpha)}$ durch das Bild von ξ eindeutig festgelegt, da laut Definition $\sigma(\alpha) = \alpha$ gelten muss. Das Minimalpolynom von ξ über $\mathbb{Q}(\alpha)$ ist ein Teiler des p -ten Kreisteilungspolynoms Φ_p . Wegen

$$[\mathbb{Q}(\alpha)(\xi) : \mathbb{Q}(\alpha)] = \frac{[Z : \mathbb{Q}]}{[\mathbb{Q}(\alpha) : \mathbb{Q}]} = \frac{p(p-1)}{p} = p-1 = \text{grad } \Phi_p$$

ist Φ_p bereits das Minimalpolynom von ξ über $\mathbb{Q}(\alpha)$. Jedes $\sigma \in G_{Z|\mathbb{Q}(\alpha)}$ bildet nun ξ auf eine andere Nullstelle von Φ_p ab, also eine andere p -te Einheitswurzel. Da die Gruppe der p -ten Einheitswurzeln von ξ erzeugt wird, gibt es ein $k \in \{1, \dots, p\}$ mit $\sigma(\xi) = \xi^k$. Betrachte nun die Abbildung

$$\psi : (\mathbb{Z}/p\mathbb{Z})^\times \rightarrow G_{Z|\mathbb{Q}(\alpha)}, \quad \bar{r} \mapsto \{\xi \mapsto \xi^r\},$$

dabei bezeichnen wir mit $\{\xi \mapsto \xi^r\}$ diejenige eindeutig bestimmte Abbildung $\sigma \in G_{Z|\mathbb{Q}(\alpha)}$ mit $\sigma(\xi) = \xi^r$. Man beachte, dass ψ wegen $\xi^p = 1$ wohldefiniert ist. Wir rechnen nun nach, dass es sich bei ψ um einen Homomorphismus handelt:

$$\psi(\bar{l} \cdot \bar{k}) = \psi(\bar{l}\bar{k}) = \{\xi \mapsto \xi^{lk}\} = \{\xi \mapsto \xi^k \mapsto \xi^{lk}\} = \psi(\bar{l}) \circ \psi(\bar{k}).$$

Liegt weiterhin \bar{k} im Kern von ψ , so ist $\psi(\bar{k}) = \text{id}_Z = \{\xi \mapsto \xi^1\}$, sodass $\bar{k} = \bar{1}$. Folglich ist ψ injektiv und als Abbildung zwischen zwei gleichmächtigen (endlichen) Mengen auch surjektiv. Somit ist ψ ein Isomorphismus

$$(\mathbb{Z}/p\mathbb{Z})^\times \xrightarrow{\sim} G_{Z|\mathbb{Q}(\alpha)}.$$

- d** Sei $r \in \mathbb{N}$ maximal mit $2^r \mid p(p-1)$. Da p ungerade ist, muss $(p-1)$ von 2^r geteilt werden. Insbesondere ist also 2^r ein Teiler der Ordnung von $G_{Z|\mathbb{Q}(\alpha)}$. Da diese Gruppe nach Teil **c** zyklisch ist, gibt es eine Untergruppe S von $G_{Z|\mathbb{Q}(\alpha)}$ mit $|S| = 2^r$.

Wenn wir annehmen, dass es genau eine 2-Sylowgruppe in $G_{Z|\mathbb{Q}}$ gibt, dann muss S diese einzige 2-Sylowgruppe sein, denn es ist $S \subseteq G_{Z|\mathbb{Q}(\alpha)} \subseteq G_{Z|\mathbb{Q}}$ und S hat die richtige Ordnung.

Laut Galoiskorrespondenz gilt für den Fixkörper dann $\mathbb{Q}(\alpha) \subseteq Z^S$, d. h. $\alpha \in Z^S$ und $X^p - a$ hat eine Nullstelle in Z^S . Weiterhin ist die Erweiterung $Z^S|\mathbb{Q}$ normal, denn S ist als einzige 2-Sylowgruppe Normalteiler in $\text{Gal}(Z|\mathbb{Q})$. Es müsste also $X^p - a$ über Z^S vollständig in Linearfaktoren zerfallen. Da Z als Zerfällungskörper der kleinste Körper mit dieser

Eigenschaft ist, müsste $Z = Z^S$ sein. Dies ist jedoch ein Widerspruch zu $[Z : Z^S] = 2^r \neq 1$. Folglich muss unsere Annahme, dass es nur eine 2-Sylowgruppe gibt, falsch gewesen sein.

Aufgabe (Frühjahr 2012, T3A5)

Sei $L|K$ eine endliche Galois-Erweiterung, $G := G_{L|K}$ die zugehörige Galois-Gruppe, $\alpha \in L$ und f das (normierte) Minimalpolynom von α über K . Zeigen Sie, dass gilt:

$$f^{[L:K(\alpha)]} = \prod_{\sigma \in G} (X - \sigma(\alpha)).$$

Lösungsvorschlag zur Aufgabe (Frühjahr 2012, T3A5)

Sei $\sigma \in G$. Wir betrachten ein Element ρ der Nebenklasse $\sigma G_{L|K(\alpha)}$: Es ist $\rho = \sigma\tau$ für $\tau \in G_{L|K(\alpha)}$ und daher $\rho(\alpha) = \sigma(\tau(\alpha)) = \sigma(\alpha)$. Also folgt

$$(X - \sigma(\alpha))^{|\sigma G_{L|K(\alpha)}|} = \prod_{\rho \in \sigma G_{L|K(\alpha)}} (X - \rho(\alpha)).$$

Sei nun $\sigma_1, \dots, \sigma_n$ ein Repräsentantensystem von $G/G_{L|K(\alpha)}$, dann sind die $\sigma_i(\alpha)$ nach obiger Überlegung paarweise verschieden: Wäre $\sigma_i(\alpha) = \sigma_j(\alpha)$ für gewisse $i \neq j$, so gäben σ_i und σ_j eingeschränkt auf $K(\alpha)$ die gleiche Abbildung, sodass $(\sigma_i \sigma_j^{-1})|_K = \text{id}_K$. Dies bedeutet $\sigma_i \sigma_j^{-1} \in G_{L|K(\alpha)}$, also $\sigma_i G_{L|K(\alpha)} = \sigma_j G_{L|K(\alpha)}$ – im Widerspruch dazu, dass σ_i und σ_j Repräsentanten verschiedener Nebenklassen sind.

Da weiterhin jedes $\sigma_i(\alpha)$ eine Nullstelle von f sein muss, haben wir

$$n = (G : G_{L|K(\alpha)}) = \frac{[L : K]}{[L : K(\alpha)]} = [K(\alpha) : K]$$

verschiedene Nullstellen von f gefunden. Wegen $\text{grad } f = [K(\alpha) : K]$ müssen das bereits alle sein und wir erhalten:

$$\begin{aligned} f(X)^{[L:K(\alpha)]} &= \left(\prod_{i=1}^n (X - \sigma_i(\alpha)) \right)^{[L:K(\alpha)]} = \prod_{i=1}^n (X - \sigma_i(\alpha))^{[L:K(\alpha)]} \\ &\prod_{i=1}^n \prod_{\rho \in \sigma_i G_{L|K(\alpha)}} (X - \rho(\alpha)) = \prod_{\sigma \in G} (X - \sigma(\alpha)) \end{aligned}$$

3.5. Endliche Körper

Bevor wir uns den bereits in der Überschrift angekündigten endlichen Körpern widmen, kehren wir kurz zurück in die Ringtheorie, um den Begriff der Charakteristik nachträglich einzuführen. Sei dazu R ein Ring mit Einselement 1_R . Durch die Zuordnung

$$\varphi: \mathbb{Z} \rightarrow R, \quad n \mapsto n \cdot 1_R$$

ist ein Ringhomomorphismus gegeben. Da \mathbb{Z} ein Hauptidealring ist, gibt es ein $n \in \mathbb{Z}$ mit $\ker \varphi = n\mathbb{Z}$, welches als *Charakteristik* von R bezeichnet und als $\text{char } R = n$ notiert wird. Nach dem Homomorphiesatz ist $\text{im } \varphi \cong \mathbb{Z}/n\mathbb{Z}$. Ist nun R ein Integritätsbereich, so gilt dies auch für $\text{im } \varphi$, also muss in diesem Fall n eine Primzahl oder 0 sein.

Falls $R = K$ ein endlicher Körper ist, so wäre $\text{im } \varphi \cong \mathbb{Z}$ natürlich unsinnig, denn dann würde R eine unendliche Menge enthalten. Dies bedeutet, dass ein endlicher Körper nur Charakteristik p für eine Primzahl p haben kann und $\mathbb{Z}/p\mathbb{Z}$ enthält. Hier gilt sogar der stärkere Zusammenhang:

Satz 3.25 (Existenz und Eindeutigkeit endlicher Körper). (1) Ist p eine Primzahl und $n \in \mathbb{N}$, so gibt es einen Körper der Ordnung p^n , den wir als \mathbb{F}_{p^n} bezeichnen.
(2) Ist K ein Körper der Ordnung $|K| = q$ und $p = \text{char } K$, so gibt es $n \in \mathbb{N}$ mit $q = p^n$ und $K \cong \mathbb{F}_{p^n}$.

Für das Verständnis endlicher Körper ist hilfreich, dass \mathbb{F}_q^\times immer eine zyklische Gruppe ist. Insbesondere gilt $a^{q-1} = 1$ bzw. $a^q = a$ für alle $a \in \mathbb{F}_q^\times$. Letztere Gleichung gilt sogar für 0 , sodass jedes $a \in \mathbb{F}_q$ eine Nullstelle des Polynoms $X^q - X$ ist. Umgekehrt kann $X^q - X$ nur höchstens q Nullstellen in \mathbb{F}_q haben, also ist \mathbb{F}_q gerade die Nullstellenmenge von $X^q - X$ und der Zerfällungskörper von $X^q - X$ über \mathbb{F}_p .

Im Zusammenhang mit endlichen Körpern ist außerdem der *Frobenius-Homomorphismus* wichtig, nämlich die Abbildung

$$\mathbb{F}_{p^n} \rightarrow \mathbb{F}_{p^n}, \quad a \mapsto a^p.$$

Dem aufmerksamen Leser wird aufgefallen sein, dass daraus, dass diese Abbildung ein Homomorphismus ist,

$$(a + b)^{p^r} = a^{p^r} + b^{p^r} \quad \text{für alle } a, b \in \mathbb{F}_{p^n} \text{ und } r \in \mathbb{N}$$

folgt. Da dies die Form der binomischen Formel ist, von deren Gültigkeit wir alle träumen, ist diese Formel auch als *freshman's dream* bekannt.

Aufgabe (Frühjahr 2003, T3A2)

Sei K ein Körper mit vier Elementen. Bestimmen Sie eine Additions- und eine Multiplikationstafel von K .

Lösungsvorschlag zur Aufgabe (Frühjahr 2003, T3A2)

Da K ein Körper ist, gibt es auf jeden Fall ein Einselement 1 und eine Nullelement 0 in K . Wegen $|K| = 2^2$ muss $\text{char } K = 2$ sein, sodass $2a = 0$ bzw. $a = -a$ für alle $a \in K$ gelten muss. Sei $\alpha \in K \setminus \{0, 1\}$, dann stimmt $\alpha + 1$ mit keinem der Elemente in $\{0, 1, \alpha\}$ überein, sodass $K = \{0, 1, \alpha, \alpha + 1\}$ gilt. Mit diesem Wissen lässt sich die Additionstabelle von K vollständig ausfüllen:

+	0	1	α	$\alpha + 1$
0	0	1	α	$\alpha + 1$
1	1	0	$\alpha + 1$	α
α	α	$\alpha + 1$	0	1
$\alpha + 1$	$\alpha + 1$	α	1	0

Ein Großteil der Multiplikationstafel ergibt sich bereits aus den Relationen $0 \cdot x = 0$ sowie $1 \cdot x = x$ für alle $x \in K$. Für die restlichen verwenden wir, dass K die Nullstellenmenge von $X^4 - X = X(X - 1)(X^2 + X + 1)$ ist. Ein $\alpha \neq 0, 1$ muss daher $\alpha^2 + \alpha + 1 = 0$ erfüllen, also $\alpha^2 = \alpha + 1$ und $\alpha(\alpha + 1) = 1$. Zuletzt bemerken wir $(\alpha + 1)^2 = \alpha^2 + 1 = \alpha$ und bekommen letztlich:

.	0	1	α	$\alpha + 1$
0	0	0	0	0
1	0	1	α	$\alpha + 1$
α	0	α	$\alpha + 1$	1
$\alpha + 1$	0	$\alpha + 1$	1	α

Aufgabe (Frühjahr 2015, T2A5)

Sei p eine Primzahl und $q = p^n, n > 0$. Weiter sei K ein Körper der Charakteristik p . Zeigen Sie, dass die Nullstellen des Polynoms $f(X) = X^q - X$ einen Unterkörper von K bilden.

Lösungsvorschlag zur Aufgabe (Frühjahr 2015, T2A5)

Sei $N = \{a \in K \mid f(a) = 0\}$. Zu zeigen ist für $a, b \in N$, dass

- (i) $1 \in N$, (ii) $a - b \in N$, (iii) $ab \in N$, (iv) $a^{-1} \in N$ (falls $a \neq 0$).

(i): Es gilt $f(1) = 1^q - 1 = 0$ und somit $1 \in N$.

(ii): Seien $a, b \in N$, dann gilt unter Verwendung des *freshman's dream*:

$$f(a - b) = (a - b)^{p^n} - (a - b) = a^{p^n} - b^{p^n} - a + b = f(a) - f(b) = 0,$$

also $a - b \in N$.

(iii): Hier erhalten wir aus $f(a) = 0$, dass $a^q = a$ bzw. $b^q = b$, sodass

$$f(ab) = (ab)^{p^n} - ab = a^{p^n}b^{p^n} - ab = ab - ab = 0$$

und damit $ab \in N$.

(iv): Unter der Annahme $a \neq 0$ folgt aus $a^{p^n} = a$ die Gleichung

$$1_K = a^{p^n-1} = aa^{p^n-2} \Leftrightarrow a^{-1} = a^{p^n-2}.$$

Da N laut (iii) unter Bildung von Produkten abgeschlossen ist, gilt $a^{-1} = a^{p^n-2} \in N$.

Nun wollen wir uns noch mit den Zwischenkörpern einer Erweiterung $\mathbb{F}_{p^n}|\mathbb{F}_p$ beschäftigen. Folgende Proposition gibt zunächst Aufschluss über die „Schachtelung“ der oben konstruierten Körper.

Proposition 3.26. Seien p eine Primzahl, $\overline{\mathbb{F}_p}$ ein algebraischer Abschluss von \mathbb{F}_p und $n, m \in \mathbb{N}$. Es gilt

$$\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n} \Leftrightarrow m \mid n$$

und $[\mathbb{F}_{p^n} : \mathbb{F}_p] = n$.

Der bezüglich Inklusion kleinste Körper in \mathbb{F}_{p^n} ist demzufolge \mathbb{F}_p . Allgemein spricht man bei dem kleinsten Teilkörper eines Körpers K vom **Primkörper** von K , welcher gerade der Schnitt aller Unterkörper von K ist.

Aufgabe (Herbst 2003, T2A3)

Es seien p und q Primzahlen. Warum zerfällt das Polynom

$$f = X^{p^q} - X$$

über dem Körper \mathbb{F}_p mit p Elementen in p verschiedene Faktoren vom Grad 1 und in $\frac{p^q-p}{q}$ verschiedene irreduzible Faktoren von Grad q ?

Hinweis Die Faktoren müssen nicht angegeben werden! Zum Einstieg in die Aufgabe überlege man, dass die Nullstellen von f einen Körper bilden.

Lösungsvorschlag zur Aufgabe (Herbst 2003, T2A3)

Der Beweis des Hinweises ist gerade die vorangegangene Aufgabe.

Ferner ist $f' = -1$, also $\text{ggT}(f, f') = 1$ und das Polynom f ist separabel, hat also p^q verschiedene Nullstellen. Insgesamt ist N damit ein Erweiterungskörper von \mathbb{F}_p mit p^q Elementen.

Ist $a \in N$, so folgt aus $f(a) = 0$, dass das Minimalpolynom von a über \mathbb{F}_p ein Teiler von f ist. Ist umgekehrt $g \in \mathbb{F}_p$ ein irreduzibler (normierter) Teiler von f und $a \in N$ mit $g(a) = 0$, so ist g Minimalpolynom von a über \mathbb{F}_p . Zusammenfassend: Die irreduziblen Faktoren von f sind genau die Minimalpolynome der Elemente aus N .

Für die p Elemente in \mathbb{F}_p haben die zugehörigen Minimalpolynome Grad 1, wir erhalten also p Faktoren von f mit Grad 1.

Für die Erweiterung $N|\mathbb{F}_p$ gilt nach Proposition 3.26, dass $[N : \mathbb{F}_p] = q$. Da q eine Primzahl ist, gibt es deshalb keine echten Zwischenkörper von $N|\mathbb{F}_p$. Ist $a \in N \setminus \mathbb{F}_p$, so muss daher bereits $\mathbb{F}_p(a) = N$ gelten und das Minimalpolynom von a über \mathbb{F}_p hat den Grad q . Es gibt $p^q - p$ solcher Elemente, von denen jeweils q Elemente das gleiche Minimalpolynom haben, denn \mathbb{F}_p ist als endlicher Körper perfekt, sodass jedes irreduzible Polynom aus $\mathbb{F}_p[X]$ separabel ist und deshalb nur einfache Nullstellen hat. Also hat f noch $\frac{p^q - p}{q}$ irreduzible Faktoren von Grad q .

Aufgabe (Herbst 2013, T2A1)

- a** Zeigen Sie, dass das Polynom $f = X^4 + X + 1 \in \mathbb{F}_2[X]$ irreduzibel ist.
- b** Sei α eine Nullstelle des Polynoms f aus Teilaufgabe **a** in einem algebraischen Abschluss $\overline{\mathbb{F}}_2$ von \mathbb{F}_2 . Zeigen Sie, dass $\mathbb{F}_2(\alpha) = \mathbb{F}_{16}$ gilt, dass $\alpha \in \mathbb{F}_{16}^\times$ gilt, und dass α ein Erzeuger der multiplikativen Gruppe \mathbb{F}_{16}^\times von \mathbb{F}_{16} ist.

Lösungsvorschlag zur Aufgabe (Herbst 2013, T2A1)

- a** Das Polynom f hat keine Nullstellen in \mathbb{F}_2 . Wäre es dennoch reduzibel, müsste es in zwei irreduzible Polynome von Grad 2 zerfallen. Allerdings

ist $X^2 + X + 1$ das einzige solche Polynom in $\mathbb{F}_2[X]$. Wegen

$$(X^2 + X + 1)^2 = X^4 + X^2 + 1 \neq f(X)$$

ist f daher irreduzibel.

- b** f ist irreduzibel, normiert, hat α als Nullstelle und ist somit das Minimalpolynom von α über \mathbb{F}_2 . Es folgt $[\mathbb{F}(\alpha) : \mathbb{F}] = 4$, d.h. $|\mathbb{F}(\alpha)| = 2^4$. Da es bis auf Isomorphie nur einen Körper mit 16 Elementen gibt, muss bereits $\mathbb{F}(\alpha) = \mathbb{F}_{16}$ gelten.

Es ist $f(0) = 1$, sodass $\alpha \neq 0$ gelten muss. Dies bedeutet gerade $\alpha \in \mathbb{F}_{16}^\times$. Damit α ein Erzeuger von \mathbb{F}_{16}^\times ist, muss α Ordnung $|\mathbb{F}_{16}^\times| = 15$ haben. Dazu genügt es nachzuweisen, dass $\alpha^{\frac{15}{3}} = \alpha^5 \neq 1$ und $\alpha^{\frac{15}{5}} = \alpha^3 \neq 1$ gilt. Man berechnet:

$$\alpha^5 = \alpha \cdot \alpha^4 = \alpha \cdot (-\alpha - 1) = -\alpha^2 - \alpha.$$

Wäre $\alpha^5 = 1$, so hieße das $\alpha^2 + \alpha + 1 = 0$ und α wäre eine Nullstelle von $X^2 + X + 1$. Als Minimalpolynom von α ist jedoch f das Polynom kleinsten Grades, das α als Nullstelle hat. Genauso würde aus $\alpha^3 = 1$ folgen, dass $X^3 - 1$ Nullstelle α hat – nach dem gleichen Argument ebenfalls ein Widerspruch.

Aufgabe (Frühjahr 2008, T1A4)

Sei E ein endlicher Körper mit 81 Elementen.

- a** Wie viele Untergruppen besitzt die multiplikative Gruppe E^\times ?
b Sei F Primkörper von E . Wie viele Elemente $z \in E$ mit $E = F(z)$ gibt es?

Lösungsvorschlag zur Aufgabe (Frühjahr 2008, T1A4)

- a** Die Gruppe E^\times ist eine zyklische Gruppe der Ordnung $|E| - 1 = 80$. Sie besitzt also für jeden Teiler ihrer Ordnung genau eine Untergruppe. Wegen $80 = 2^4 \cdot 5$ sind dies $5 \cdot 2 = 10$ an der Zahl.
b Wegen $81 = 3^4$ ist $E \cong \mathbb{F}_{3^4}$ und die Kette aller Zwischenkörper ist durch

$$\mathbb{F}_3 \subseteq \mathbb{F}_{3^2} \subseteq \mathbb{F}_{3^4}$$

gegeben.

Sei nun $\alpha \in \mathbb{F}_{3^4}$, dann ist $\mathbb{F}_3(\alpha) \in \{\mathbb{F}_3, \mathbb{F}_{3^2}, \mathbb{F}_{3^4}\}$. Falls $\alpha \in \mathbb{F}_{3^2}$, so ist $\mathbb{F}_3(\alpha) \subseteq \mathbb{F}_{3^2}$, also insbesondere $\mathbb{F}_3(\alpha) \neq \mathbb{F}_{3^4}$. Um $\mathbb{F}_3(\alpha) = \mathbb{F}_{3^4}$ zu erreichen, muss daher auf jeden Fall $\alpha \in \mathbb{F}_{3^4} \setminus \mathbb{F}_{3^2}$ sein.

Ist umgekehrt $\alpha \in \mathbb{F}_{3^4} \setminus \mathbb{F}_{3^2}$, so würde aus $\mathbb{F}_3(\alpha) = \mathbb{F}_3$ oder $\mathbb{F}_3(\alpha) = \mathbb{F}_{3^2}$ folgen, dass $\alpha \in \mathbb{F}_{3^2}$. Da wir von oben alle Teilkörper von \mathbb{F}_{3^4} kennen, bleibt nur $\mathbb{F}_3(\alpha) = \mathbb{F}_{3^4}$.

Die gesuchte Anzahl an primitiven Elementen ist daher

$$|\mathbb{F}_{3^4} \setminus \mathbb{F}_{3^2}| = 81 - 9 = 72.$$

Aufgabe (Herbst 2000, T1A3)

Sei $K = \mathbb{F}_{2^{2000}}$ der Körper mit 2^{2000} Elementen.

- a** Wie viele Teilkörper besitzt K ?
- b** Wie viele erzeugende Elemente hat die Erweiterung $K|\mathbb{F}_2$?

Hinweis Die bei der Berechnung auftretenden Potenzen von 2 müssen nicht „ausgerechnet“ werden.

Lösungsvorschlag zur Aufgabe (Herbst 2000, T1A3)

- a** Die Zahl 2000 hat die Primfaktorzerlegung $2^4 \cdot 5^3$ und somit $5 \cdot 4 = 20$ Teiler. Dies ist laut Proposition 3.26 die Anzahl der Teilkörper.
- b** Für ein Element $\alpha \in K$ gilt $K = \mathbb{F}_2(\alpha)$ offenbar genau dann, wenn α in keinem echten Teilkörper der Erweiterung enthalten ist. Ist nämlich $\alpha \in \mathbb{F}_{2^d}$ für $d < 2000$, so ist auch $\mathbb{F}_2(\alpha) \subseteq \mathbb{F}_{2^d}$ und damit insbesondere $\mathbb{F}_2(\alpha) \neq K$. Umgekehrt bedeutet $\mathbb{F}_2(\alpha) \neq K$, dass $\mathbb{F}_2(\alpha)$ ein echter Zwischenkörper ist und insbesondere α in einem solchen liegt.

Damit ist die Anzahl der erzeugenden Elemente gegeben durch

$$\left| \mathbb{F}_{2^{2000}} \setminus \bigcup_{\substack{d|2000 \\ d < 2000}} \mathbb{F}_{2^d} \right|.$$

Ist nun d ein echter Teiler von $2000 = 2^4 \cdot 5^3$, dann ist $d = 2^k \cdot 5^l$ mit $k \leq 4, l \leq 3$ und $(k, l) \neq (0, 0)$. Ist $l \leq 3$, so ist d ein Teiler von $2^3 \cdot 5^3 = 1000$ und ist $k \leq 2$, so ist d ein Teiler von $2^4 \cdot 5^2 = 400$. Im ersten Fall ist $\mathbb{F}_{2^d} \subseteq \mathbb{F}_{2^{1000}}$, im zweiten Fall $\mathbb{F}_{2^d} \subseteq \mathbb{F}_{2^{400}}$. Die Anzahl der primitiven Elemente ist daher durch

$$\begin{aligned} |\mathbb{F}_{2^{2000}} \setminus (\mathbb{F}_{2^{1000}} \cup \mathbb{F}_{2^{400}})| &= |\mathbb{F}_{2^{2000}}| - |\mathbb{F}_{2^{1000}} \cup \mathbb{F}_{2^{400}}| = \\ &= 2^{2000} - |\mathbb{F}_{2^{1000}}| - |\mathbb{F}_{2^{400}}| + |\mathbb{F}_{2^{1000}} \cap \mathbb{F}_{2^{400}}| = \\ &= 2^{2000} - 2^{1000} - 2^{400} + |\mathbb{F}_{2^{1000}} \cap \mathbb{F}_{2^{400}}| \end{aligned}$$

gegeben. Sei $a \in \mathbb{F}_{2^{1000}} \cap \mathbb{F}_{2^{400}}$, dann ist $\mathbb{F}_2(a) = \mathbb{F}_{2^d}$ für ein $d \in \mathbb{N}_0$ mit $d \mid 1000$ und $d \mid 400$, also $d \mid \text{ggT}(400, 1000) = 200$. Folglich ist \mathbb{F}_{2^d} , und damit auch a , im Körper $\mathbb{F}_{2^{200}}$ enthalten. Umgekehrt ist natürlich $\mathbb{F}_{2^{200}} \subseteq \mathbb{F}_{2^{1000}} \cap \mathbb{F}_{2^{400}}$. Wir erhalten daher für die gesuchte Anzahl

$$2^{2000} - 2^{1000} - 2^{400} + 2^{200}.$$

Aufgabe (Herbst 2010, T3A5)

Sei $P = X^4 + X + 2 \in \mathbb{F}_3[X]$ und $K = \mathbb{F}_3[X]/(P)$. Weiter sei α das Bild von X in K .

- a** Zeigen Sie, dass K ein Körper mit 81 Elementen ist.
- b** Bestimmen Sie explizit alle Teilkörper von K . Hierbei heißt „explizit“: Die Angabe einer \mathbb{F}_3 -Basis, wobei die Basiselemente Polynome in α vom Grad ≤ 3 sind.

Hinweis Betrachten Sie $\alpha^{10} \in K$.

Lösungsvorschlag zur Aufgabe (Herbst 2010, T3A5)

- a** Wir zeigen, dass P irreduzibel ist. Zunächst sieht man durch Einsetzen, dass P keine Nullstelle in \mathbb{F}_3 hat. Wäre P dennoch irreduzibel, so müsste P in zwei Polynome von Grad 2 zerfallen. Nun sind die Polynome zweiten Grades in $\mathbb{F}_3[X]$ aber nur (vgl. F13T3A4)

$$X^2 + 1, \quad X^2 + X + 2, \quad X^2 + 2X + 2.$$

Da der konstante Term von P gleich 2 ist, kommen nur Produkte in Frage, die das erste Polynom einmal als Faktor enthalten. Durchrechnen dieser Möglichkeiten zeigt, dass keines der Produkte P ergibt. Somit ist P irreduzibel.

Als Polynomring über einem Körper ist $\mathbb{F}_3[X]$ ein Hauptidealring. P ist als irreduzibles Element daher auch prim, sodass (P) ein Primideal und damit bereits ein maximales Ideal ist. Dies wiederum bedeutet, dass K ein Körper ist.

Wir zeigen mit dem Homomorphiesatz, dass $K \cong \mathbb{F}_3(\beta)$ gilt, wobei $\beta \in \overline{\mathbb{F}_3}$ eine Nullstelle von P ist. P ist dann als normiertes, irreduzibles Polynom zugleich das Minimalpolynom von β über \mathbb{F}_3 und es ist $[\mathbb{F}_3(\beta) : \mathbb{F}_3] = 4$. Definiere nun den Einsetzungshomomorphismus

$$\phi: \mathbb{F}_3[X] \rightarrow \mathbb{F}_3(\beta), \quad g \mapsto g(\beta).$$

Wegen $[\mathbb{F}_3(\beta) : \mathbb{F}_3] = 4$ wissen wir, dass $1, \beta, \beta^2$ und β^3 eine \mathbb{F}_3 -Basis von $\mathbb{F}_3(\beta)$ bilden. Also hat jedes Element aus $\mathbb{F}_3(\beta)$ eine Darstellung als $a_0 + a_1\beta + a_2\beta^2 + a_3\beta^3$ mit $a_0, a_1, a_2, a_3 \in \mathbb{F}_3$ und ist damit das Bild von $f = a_0 + a_1X + a_2X^2 + a_3X^3$. Dies zeigt, dass ϕ surjektiv ist.

Wir zeigen weiter $\ker \phi = (P)$. Die Richtung „ \supseteq “ ist klar, da $P(\beta) = 0$. Ist umgekehrt $g \in \ker \phi$, d. h. $g(\beta) = 0$, dann wird g vom Minimalpolynom von β geteilt, sodass $g \in (P)$.

Nach dem Homomorphiesatz induziert ϕ somit einen Isomorphismus $K \cong \mathbb{F}_3(\beta)$. Wegen $[\mathbb{F}_3(\beta) : \mathbb{F}_3] = 4$ hat K damit $3^4 = 81$ Elemente.

- b** Wir bestimmen zunächst die Anzahl der Teilkörper: Nach Teil **a** ist K isomorph zu einem Erweiterungskörper von Grad 4 über \mathbb{F}_3 , also zu \mathbb{F}_{3^4} . Diese Erweiterung hat genau einen echten Zwischenkörper vom Grad 2 (nämlich \mathbb{F}_{3^2}), sodass auch K neben den trivialen Teilkörpern nur einen Teilkörper von Erweiterungsgrad 2 besitzt.

Dem Hinweis folgend betrachten wir zunächst $\alpha^{10} = X^{10} + (P)$ und vermuten, dass α^{10} bereits die gesuchte Erweiterung zweiten Grades erzeugt. Dazu muss das Minimalpolynom von α^{10} über \mathbb{F}_3 Grad 2 haben, weswegen wir den Ansatz $f = X^2 + aX + b$ mit $a, b \in \mathbb{F}_3$ für das Minimalpolynom machen und b und c so bestimmen, dass $f(\alpha) = 0$ gilt. Unter wiederholter Ausnutzung von $\alpha^4 = 1 - \alpha$ und dem *freshman's dream* bekommen wir:

$$\begin{aligned}\alpha^{20} + a\alpha^{10} + b &= (1 - \alpha)^5 + a\alpha^2(1 - \alpha)^2 + b = \\ &= (a - 1)\alpha^2 + (a - 1)\alpha^3 + (a - 1)\alpha + (a + b).\end{aligned}$$

Aus $f(\alpha) = 0$ erhält man daher mittels Koeffizientenvergleich $a = 1$ und $b = -1$. Somit ist $f = X^2 + X - 1$ ein normiertes Polynom, das α^{10} als Nullstelle hat, außerdem ist es irreduzibel über \mathbb{F}_3 , da dort nullstellenfrei. Somit ist $\mathbb{F}_3(\alpha^{10})$ tatsächlich der eindeutige Zwischenkörper von K von Grad 2 über \mathbb{F}_3 .

Laut Aufgabenstellung müssen wir α^{10} noch als Polynom in α von Grad höchstens 3 ausdrücken. Dies erledigen wir mittels der folgenden Rechnung:

$$\alpha^{10} = \alpha^2(1 - \alpha)^2 = \alpha^2 - 2\alpha^3 + (1 - \alpha) = \alpha^3 + \alpha^2 - \alpha + 1.$$

Die zugehörige \mathbb{F}_3 -Basis des Zwischenkörpers von Grad 2 ist nun $\{1, \alpha^3 + \alpha^2 - \alpha + 1\}$. Der triviale Teilkörper \mathbb{F}_3 hat die Basis $\{1\}$, der Teilkörper K hat als vierdimensionaler \mathbb{F}_3 -Vektorraum die Basis $\{1, \alpha, \alpha^2, \alpha^3\}$.

Aufgabe (Herbst 2000, T2A3)

- a** Sei $p \neq 2$ eine Primzahl. Zeigen Sie, dass der Körper \mathbb{F}_{p^2} mit p^2 Elementen eine primitive 8-te Einheitswurzel enthält.
- b** Zeigen Sie, dass das Polynom $X^4 + 1$ über \mathbb{Q} irreduzibel und über jedem endlichen Körper reduzibel ist.

Lösungsvorschlag zur Aufgabe (Herbst 2000, T2A3)

- a** Sei $K = \mathbb{F}_{p^2}$ der angegebene Körper und K^\times seine Einheitengruppe. Wir wissen, dass K^\times zyklisch von Ordnung $p^2 - 1$ ist. Wenn wir zeigen könnten, dass 8 ein Teiler von $p^2 - 1$ ist, so ist die Aussage wahr: Da K^\times zyklisch ist, existiert dann eine Untergruppe dieser Ordnung und diese Untergruppe ist wiederum zyklisch. Ihr Erzeuger ist also eine primitive 8-te Einheitswurzel.

Wir zeigen daher nun $8 \mid (p^2 - 1)$. Da p ungerade ist, ist p kongruent zu 1, 3, 5 oder 7 modulo 8. In jedem der Fälle ist

$$1 \equiv 3^2 \equiv 5^2 \equiv 7^2 \pmod{8},$$

also $p^2 - 1 \equiv 0 \pmod{8}$.

- b** *Irreduzibilität über \mathbb{Q} :* Sei $\zeta \in \mathbb{C}$ eine primitive achte Einheitswurzel, dann ist $\zeta^4 = -1$, denn aus $(\zeta^4)^2 = \zeta^8 = 1$ folgt $\zeta^4 \in \{\pm 1\}$ und $\zeta^4 = 1$ würde $\text{ord } \zeta = 8$ widersprechen. Dies zeigt, dass ζ eine Nullstelle von $X^4 + 1$ ist. Das achte Kreisteilungspolynom Φ_8 hat den Grad $\varphi(8) = 4$. Da dies dem Grad von $X^4 + 1$ entspricht und beide Polynome normiert sind, folgt $\Phi_8 = X^4 + 1$. Insbesondere ist $X^4 + 1$ irreduzibel über \mathbb{Q} .

Reduzibilität über endlichen Körpern: Ziel ist nun, Teil **a** anzuwenden. Betrachten wir zunächst den Fall $\text{char } K = 2$. In diesem Fall erhalten wir mittels *freshman's dream* problemlos die Zerlegung

$$X^4 + 1 = (X^2 + 1)^2 = (X + 1)^4.$$

Ist anderseits $\text{char } K = p \neq 2$, so existiert laut Teil **a** im Körper \mathbb{F}_{p^2} eine primitive achte Einheitswurzel ζ . Wie oben sieht man, dass $\zeta^4 = -1$ und somit ζ eine Nullstelle des angegebenen Polynoms sein muss.

Angenommen, das Polynom $X^4 + 1$ wäre irreduzibel über \mathbb{F}_p , dann wäre es das Minimalpolynom von ζ über \mathbb{F}_p und wir bekämen

$$4 = [\mathbb{F}_p(\zeta) : \mathbb{F}_p] \leq [\mathbb{F}_{p^2} : \mathbb{F}_p] = 2,$$

was unmöglich sein kann.

Galois-Theorie endlicher Körper

Endliche Erweiterungen endlicher Körper sind stets galoissch: Als Erweiterungen über einem endlichen (und damit perfekten) Körpers sind sie separabel, und als Zerfällungskörper eines Polynoms der Form $X^q - X$ für eine Primzahlpotenz q auch normal.

Die Galois-Theorie endlicher Körper ist besonders einfach, wie der nächste Satz zeigt.

Satz 3.27. Sei K ein endlicher Körper der Charakteristik p und $L|K$ eine endliche Körpererweiterung. Die Galois-Gruppe $G_{L|K}$ wird vom **Frobenius-Homomorphismus** erzeugt, d. h.

$$G_{L|K} = \langle \varphi \rangle \quad \text{für } \varphi: L \rightarrow L, \alpha \mapsto \alpha^p.$$

Insbesondere handelt es sich also um eine zyklische Gruppe der Ordnung n .

Aufgabe (Frühjahr 2013, T2A4)

Sei $K = \mathbb{F}_5(\alpha)$ mit $\alpha^4 = 3$.

- a** Zeigen Sie, dass $K|\mathbb{F}_5$ eine Galois-Erweiterung ist und bestimmen Sie die Galois-Gruppe dieser Erweiterung.
- b** Bestimmen Sie den Verband der Zwischenkörper von K über \mathbb{F}_5 , d. h. alle Zwischenkörper geordnet nach Inklusionen.
- c** Bestimmen Sie die Anzahl der primitiven Elemente der Erweiterung K über \mathbb{F}_5 .

Lösungsvorschlag zur Aufgabe (Frühjahr 2013, T2A4)

- a** Wegen $\alpha^4 - 3 = 0$ ist α algebraisch über \mathbb{F}_5 und K somit eine endliche Erweiterung von \mathbb{F}_5 . Insbesondere ist K selbst endlich und Zerfällungskörper des Polynoms $X^{5^n} - X$ mit $n = [K : \mathbb{F}_5]$ über \mathbb{F}_5 .

Weiter ist \mathbb{F}_5 als endlicher Körper perfekt, sodass $K|\mathbb{F}_5$ auch separabel ist. Insgesamt ist damit $K|\mathbb{F}_5$ galoissch.

Die Galois-Gruppe ist laut Satz 3.27 durch $G_{K|\mathbb{F}_5} = \langle \varphi \rangle \cong \mathbb{Z}/n\mathbb{Z}$ gegeben, wobei

$$\varphi: K \rightarrow K, \quad a \mapsto a^5$$

der Frobenius-Homomorphismus ist. Wir bestimmen noch $n = [K : \mathbb{F}_5]$:

Das Element α ist Nullstelle des Polynoms $f = X^4 - 3$. Dieses hat in \mathbb{F}_5 keine Nullstelle, wie Einsetzen zeigt. Angenommen, es zerfällt in zwei

irreduzible quadratische Polynome $X^2 + bX + c$ und $X^2 + dX + e$ mit $b, c, d, e \in \mathbb{F}_5$. Wir erhalten

$$\begin{aligned}(X^2 + bX + c)(X^2 + dX + e) \\ = X^4 + (b+d)X^3 + (bd+c+e)X^2 + (cd+be)X + ce\end{aligned}$$

und damit die Gleichungen

$$(I) \quad b + d = 0, \quad (II) \quad bd + c + e = 0, \quad (III) \quad cd + be = 0, \quad (IV) \quad ce = -3.$$

Die erste Gleichung liefert $b = -d$, einsetzen in (III) ergibt

$$cd - ed = 0 \quad \Leftrightarrow \quad d(c - e) = 0 \quad \Leftrightarrow \quad d = 0 \text{ oder } c = e.$$

Der Fall $c = e$ liefert mit Gleichung (IV) $c^2 = -3 = 2$. Da es ist in \mathbb{F}_5 jedoch nur die Quadrate 0, 1 und 4 gibt, ist das nicht möglich. Im Fall $d = 0$ erhalten wir aus Gleichung (II) $c = -e$ und damit mit (IV) $c^2 = 3$. Auch das ist in \mathbb{F}_5 unmöglich. Damit enthält f auch keinen quadratischen Faktor, ist irreduzibel über \mathbb{F}_5 und das Minimalpolynom von α über \mathbb{F}_5 , sodass $n = [K : \mathbb{F}_5] = 4$.

- b** Aus $[K : \mathbb{F}_5] = 4$ folgt $|K| = 5^4$ und Satz 3.25 liefert $K \cong \mathbb{F}_{5^4}$. Nach Proposition 3.26 ist der Verband der Zwischenkörper daher

$$\mathbb{F}_5 \subseteq \mathbb{F}_{5^2} \subseteq \mathbb{F}_{5^4} = K.$$

- c** Die primitiven Elemente sind wie in früheren Aufgaben genau die Elemente von $K \setminus \mathbb{F}_{5^2}$. Ihre Anzahl berechnet sich also zu

$$|\mathbb{F}_{5^4}| - |\mathbb{F}_{5^2}| = 5^4 - 5^2 = 600.$$

Aufgabe (Herbst 2003, T1A4)

Sei K ein Körper mit 81 Elementen, sei G die Gruppe aller Automorphismen von K . Bestimmen Sie:

- a** die Länge der Bahnen der Operation von G auf K , sowie
- b** die Anzahl der Bahnen gegebener Länge.

Lösungsvorschlag zur Aufgabe (Herbst 2003, T1A4)

- a** Der Primkörper von K hat 3 Elemente, wir bezeichnen ihn mit F . Ferner hat die Erweiterung $K|F$ laut Proposition 3.26 genau einen Zwischenkörper M vom Grad 2, also mit $3^2 = 9$ Elementen.

Betrachten wir nun die Automorphismen-Gruppe G . Ist $\sigma \in G$ ein Automorphismus, so muss laut der Definition von Körperhomomorphismen $\sigma(1) = 1$ sowie $\sigma(0) = 0$ gelten. Weiter folgt $\sigma(2) = \sigma(1+1) = 1+1 = 2$. Damit hält jeder Automorphismus den Primkörper P elementweise fest. Die Gruppe G ist also genau die Gruppe der F -Automorphismen, die Galois-Gruppe $G_{K|F}$ (beachte, dass die Erweiterung wie schon früher gesehen galoissch ist). Laut Satz 3.27 wird G daher vom Frobenius-Automorphismus $\varphi: K \rightarrow K$, $\alpha \rightarrow \alpha^3$ erzeugt. In unserem Fall ist $G_{K|F}$ eine Gruppe der Ordnung $[K : F] = 4$, also

$$G = \langle \varphi \rangle = \left\{ \text{id}, \varphi, \varphi^2, \varphi^3 \right\}.$$

Wir bestimmen nun die einzelnen Bahnen für Elemente $\alpha \in K$.

1. Fall: $\alpha \in F$. Da die Elemente von G allesamt F -Automorphismen sind, ist hier $G(\alpha) = \{\alpha\}$, wir erhalten hier 3 Bahnen der Länge 1 (also 3 Fixpunkte).

2. Fall: $\alpha \in M \setminus F$. Dann gilt $\alpha^9 = \alpha$ und somit

$$\text{id}(\alpha) = \alpha, \quad \varphi(\alpha) = \alpha^3, \quad \varphi^2(\alpha) = (\alpha^3)^3 = \alpha^9 = \alpha, \quad \varphi^3(\alpha) = \alpha^3.$$

Dabei ist $\alpha^3 \neq \alpha$, denn andernfalls wäre α Nullstelle von $X^3 - X$ und müsste bereits in \mathbb{F}_3 liegen. Damit erhalten wir die zweielementige Bahn $G(\alpha) = \{\alpha, \alpha^3\}$.

3. Fall: $\alpha \in K \setminus M$. Dann sind die Elemente $\alpha, \alpha^3, \alpha^9, \alpha^{27}$ alle verschieden und wir erhalten die vierelementige Bahn $G(\alpha) = \{\alpha, \alpha^3, \alpha^9, \alpha^{27}\}$.

Damit treten die Bahnlängen 1, 2 und 4 auf.

- b** Wir haben bereits festgestellt, dass es genau 3 einelementige Bahnen gibt. Die zweielementigen Bahnen sind genau die Bahnen der Elemente aus $\mathbb{F}_{3^2} \setminus \mathbb{F}_3$. Diese Menge enthält $9 - 3 = 6$ Elemente. Jeweils zwei davon liegen in der selben Bahn, sodass wir 3 Bahnen der Länge 2 erhalten. Die vierelementigen Bahnen sind die Bahnen der Elemente aus $\mathbb{F}_{3^4} \setminus \mathbb{F}_{3^2}$, dies sind $81 - 9 = 72$ Stück. Damit erhalten wir in diesem Fall $\frac{72}{4} = 18$ Bahnen der Länge 4.

3.6. Konstruktionen mit Zirkel und Lineal

Als letztem Inhalt der Körpertheorie beschäftigen wir uns noch mit der Konstruierbarkeit gewisser Punkte mit Zirkel und Lineal – es handelt sich dabei jedoch um ein Thema, das nur gelegentlich im Staatsexamen vorkommt.

Eine klassische Fragestellung ist, welche Punkte sich aus einer vorgegebenen Menge von Punkten mit Zirkel und Lineal konstruieren lassen. Man beschränkt sich dabei auf die folgenden elementaren Konstruktionsschritte:

- (1) Ziehen einer Verbindungsgerade durch zwei Punkte,
- (2) Abtragen von Streckenlängen,
- (3) Zeichnen eines Kreises um einen vorgegebenen Punkt, dessen Radiuslänge in Form der Entfernung zweier Punkte gegeben ist.

Wir identifizieren nun die reelle Ebene \mathbb{R}^2 mit \mathbb{C} und gehen mit algebraischen Methoden an dieses Problem heran. Dazu bezeichnen wir einen Punkt $z \in \mathbb{C}$ als *konstruierbar* aus einer Menge $M \subseteq \mathbb{C}$, falls man z durch obige elementare Konstruktionsschritte aus den Punkten in M konstruieren kann. Die Menge aller aus M konstruierbaren Punkte bezeichnen wir mit $\mathcal{K}(M)$.

Proposition 3.28. Sei $M \subseteq \mathbb{C}$ eine Teilmenge mit $\{0, 1\} \subseteq M$. Dann ist $\mathcal{K}(M)$ ein Körper.

Weitere nützliche Eigenschaften von $\mathcal{K}(M)$ sind, dass dieser invariant unter der komplexen Konjugation und quadratisch abgeschlossen ist. Dies kommt daher, dass die komplexe Kongation einer Spiegelung an der reellen Achse entspricht und somit als Konstruktion mit Zirkel und Lineal ausführbar ist. Ebenso lässt sich die Wurzel einer Zahl konstruieren. Formal: aus $z \in \mathcal{K}(M)$ folgt auch $\bar{z}, \sqrt{z} \in \mathcal{K}(M)$.

Ist \overline{M} die Menge der komplex Konjugierten der Elemente aus M , so enthält $\mathcal{K}(M)$ also $M \cup \overline{M}$. Als Körper der Charakteristik 0 enthält $\mathcal{K}(M)$ zudem den Primkörper \mathbb{Q} , deshalb gilt $\mathbb{Q}(M \cup \overline{M}) \subseteq \mathcal{K}(M)$.

Satz 3.29 (Konstruierbarkeit mit Zirkel und Lineal). Sei $M \subseteq \mathbb{C}$ eine Teilmenge mit $\{0, 1\} \subseteq M$ und $z \in \mathbb{C}$ ein Punkt. Dann sind äquivalent:

- (1) $z \in \mathcal{K}(M)$,
- (2) Es gibt einen Körperturm

$$\mathbb{Q}(M \cup \overline{M}) = L_0 \subseteq L_1 \subseteq \cdots \subseteq L_n,$$

sodass $z \in L_n$ und jeweils $[L_i : L_{i-1}] = 2$ für alle $i \in \{1, \dots, n\}$ gilt.

- (3) Es gibt eine Galoiserweiterung $L|\mathbb{Q}(M \cup \overline{M})$, sodass $z \in L$ und $[L : \mathbb{Q}(M \cup \overline{M})]$ eine Potenz von 2 ist.

Aus Satz 3.29 ergibt sich unmittelbar, dass für jeden aus M konstruierbaren Punkt der Grad des Minimalpolynoms über $\mathbb{Q}(M \cup \bar{M})$ eine Potenz von 2 ist. Mit diesem Kriterium lassen sich viele der klassischen Konstruierbarkeitsfragen wie beispielsweise die Dreiteilung des Winkels, die Quadratur des Kreises oder die Würfelverdopplung beantworten.

Aufgabe (Frühjahr 2005, T2A5)

Beweisen Sie mit Mitteln der Algebra, dass das regelmäßige Fünfeck mit Zirkel und Lineal konstruierbar ist, das regelmäßige Siebeneck aber nicht.

Lösungsvorschlag zur Aufgabe (Frühjahr 2005, T2A5)

Die Ecken des regelmäßigen Fünfecks bzw. Siebenecks sind genau die 5-ten bzw. 7-ten Einheitswurzeln. Wir müssen also zeigen, dass die fünfte primitive Einheitswurzel ζ_5 konstruierbar ist, die siebte primitive Einheitswurzel ζ_7 jedoch nicht.

Das Minimalpolynom von ζ_5 über \mathbb{Q} ist das fünfte Kreisteilungspolynom Φ_5 . Dieses hat Grad $\varphi(5) = 4 = 2^2$, also ist ζ nach Satz 3.29 aus der Menge $\{0, 1\}$ konstruierbar, denn $\mathbb{Q}(\zeta_5)|\mathbb{Q}$ ist eine Galoiserweiterung und $[\mathbb{Q}(\zeta_5) : \mathbb{Q}] = 2^2$.

Das Minimalpolynom von ζ_7 hat dagegen Grad $\varphi(7) = 6$. Für jeden Erweiterungskörper L von \mathbb{Q} mit $\zeta_7 \in L$ gilt daher, dass $[L : \mathbb{Q}]$ von $[\mathbb{Q}(\zeta_7) : \mathbb{Q}] = 6$ geteilt wird. Folglich kann $[L : \mathbb{Q}]$ keine Potenz von 2 sein und ζ_7 ist daher nicht aus $\{0, 1\}$ konstruierbar.

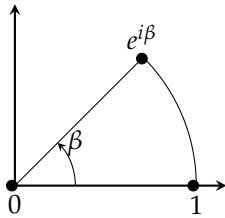
Aufgabe (Herbst 2012, T2A5)

Sei p eine Primzahl. Für jede nicht verschwindende ganze Zahl a sei $\nu_p(a)$ der Exponent von p in der Primfaktorzerlegung von a (also insbesondere genau dann 0, falls p kein Teiler von a ist). Ist b eine weitere nicht verschwindende ganze Zahl, so definieren wir $\nu_p(\frac{a}{b}) = \nu_p(a) - \nu_p(b)$.

- a** Sei $\frac{a}{b}$ ein vollständig gekürzter Bruch mit $a \neq 0$. Zeigen Sie, dass sich der Winkel $\frac{2\pi}{b}$ aus dem Winkel $\frac{2\pi a}{b}$ nur mit Zirkel und Lineal konstruieren lässt.
- b** Sei $r \in \mathbb{Q}^\times$ eine nicht verschwindende rationale Zahl. Zeigen Sie, dass sich der Winkel $2\pi r$ genau dann mit Zirkel und Lineal dritteln lässt, wenn $\nu_3(r) \geq 0$ gilt.

Lösungsvorschlag zur Aufgabe (Herbst 2012, T2A5)

- a** Da wir den Winkel $\alpha = \frac{2\pi}{b}$ aus dem Winkel $\beta = \frac{2\pi a}{b}$ konstruieren sollen, können wir o. B. d. A. davon ausgehen, dass wir die Punkte $0, 1, e^{i\beta}$ gegeben haben.



ben haben. Sei also $M = \{0, 1, e^{i\beta}\}$, dann müssen wir $e^{i\alpha} \in \mathcal{K}(M)$ zeigen.

Weil a und b nach Voraussetzung teilerfremd sind, gibt es laut dem Lemma von Bézout $x, y \in \mathbb{Z}$, sodass $1 = xa + yb$ erfüllt ist. Dies können wir verwenden, um

$$e^{i\alpha} = \left(e^{\frac{2\pi i}{b}}\right)^{xa+yb} = e^{\frac{2\pi i ax}{b}} \cdot e^{2\pi iy} = \left(e^{\frac{2\pi i a}{b}}\right)^x = \left(e^{i\beta}\right)^x \in \mathcal{K}(M)$$

zu erhalten, wobei eingeht, dass $\mathcal{K}(M)$ nach Proposition 3.28 ein Körper ist.

- b** Sei jeweils $\xi_k = e^{\frac{2\pi i}{k}}$ für $k \in \mathbb{N}$ eine primitive k -te Einheitswurzel. Wir benötigen folgende Aussagen: Sind $n, m \in \mathbb{N}$ teilerfremd, so gilt

$$\mathbb{Q}(\xi_{nm}) = \mathbb{Q}(\xi_n, \xi_m).$$

Die Inklusion „ \supseteq “ ist dabei klar, denn es ist $\xi_{nm}^n = \xi_m$ bzw. $\xi_{nm}^m = \xi_n$. Für die umgekehrte Inklusion weisen wir nach, dass die Gruppe U der Einheitswurzeln des Kompositums ein Element der Ordnung nm besitzt. Wegen $\xi_n, \xi_m \in U$ sind n und m jeweils Teiler von $|U|$, also ist auch $\text{kgV}(n, m)$ ein Teiler von $|U|$. Nun sind n und m teilerfremd, sodass gerade $\text{kgV}(n, m) = nm$ gilt. Da U zyklisch ist gibt es also ein Element der Ordnung nm in U , d. h. eine primitive nm -te Einheitswurzel.

Zur eigentlichen Aufgabe: Schreibe r als gekürzten Bruch $\frac{a}{b}$, dann dürfen wir wegen **a** o. B. d. A. annehmen, dass $a = 1$ und $b \in \mathbb{N}$. Es gilt $v_3(r) \geq 0$ also genau dann, wenn $3 \nmid b$. Wir müssen also zeigen: ξ_{3b} lässt sich genau dann aus $M = \{0, 1, \xi_b\}$ konstruieren, wenn $3 \nmid b$.

„ \Rightarrow “: Es gelte $3 \nmid b$. Unter Verwendung der oben bewiesenen Aussage und der Rechenregeln für die Euler'sche φ -Funktion (vgl. Seite 4) haben wir

$$[\mathbb{Q}(\xi_{3b}) : \mathbb{Q}(\xi_b)] = \frac{[\mathbb{Q}(\xi_{3b}) : \mathbb{Q}]}{[\mathbb{Q}(\xi_b) : \mathbb{Q}]} = \frac{\varphi(3b)}{\varphi(b)} = \frac{\varphi(3) \cdot \varphi(b)}{\varphi(b)} = \varphi(3) = 2.$$

Als Erweiterung von Grad 2 ist daher $\mathbb{Q}(\xi_{3b})|\mathbb{Q}(\xi_b)$ galoissch und aus Satz 3.29 (3) folgt, dass ξ_{3b} aus M konstruierbar ist.

„ \Leftarrow “: Es gelte diesmal $3 \mid b$, d. h. $b = 3^l c$ für $l, c \in \mathbb{N}$. In diesem Fall ist

$$\begin{aligned} [\mathbb{Q}(\xi_{3b}) : \mathbb{Q}(\xi_b)] &= \frac{[\mathbb{Q}(\xi_{3b}) : \mathbb{Q}]}{[\mathbb{Q}(\xi_b) : \mathbb{Q}]} = \frac{\varphi(3b)}{\varphi(b)} = \frac{\varphi(3^{l+1}) \cdot \varphi(c)}{\varphi(3^l) \cdot \varphi(c)} = \\ &= \frac{2 \cdot 3^l}{2 \cdot 3^{l-1}} = 3. \end{aligned}$$

Wäre ξ_{3b} konstruierbar aus M , so müsste es laut Satz 3.29 eine Galois-Erweiterung $L|\mathbb{Q}(\xi_b)$ mit $\xi_{3b} \in L$ geben, sodass $[L : \mathbb{Q}(\xi_b)]$ eine Potenz von 2 ist. Laut Gradformel wird $[L : \mathbb{Q}(\xi_b)]$ aber von $[\mathbb{Q}(\xi_{3b}) : \mathbb{Q}(\xi_b)] = 3$ geteilt, kann also keine Potenz von 2 sein. Folglich kann ξ_{3b} nicht in $\mathcal{K}(M)$ liegen.

Aufgabe (Herbst 2013, T3A2)

Sei $f = X^4 - X - 1 \in \mathbb{Q}[X]$.

- a** Zeigen Sie, dass f genau zwei reelle Nullstellen x_1 und x_2 hat.
- b** Zeigen Sie, dass f irreduzibel über \mathbb{Q} ist.
- c** Sei $g = X^3 + 4X - 1$, und $a \in \mathbb{C}$ komplex. Zeigen Sie, dass es genau dann komplexe Zahlen $b, c, d \in \mathbb{C}$ gibt mit $f = (X^2 + aX + b)(X^2 + cX + d)$, wenn $g(a^2) = 0$.
- d** Zeigen Sie, dass g irreduzibel über \mathbb{Q} ist.
- e** Sei $g(a^2) = 0$ für $a \in \mathbb{R}$ reell. Zeigen Sie, dass $a \in \mathbb{Q}[x_1, x_2]$.
- f** Zeigen Sie, dass x_1 oder x_2 nicht mit Zirkel und Lineal konstruierbar ist.

Lösungsvorschlag zur Aufgabe (Herbst 2013, T3A2)

- a** Es ist

$$f(-1) = 1 > 0, \quad f(0) = -1 < 0, \quad f(2) = 13 > 0,$$

also gibt es nach dem Zwischenwertsatz reelle Nullstellen $x_1 \in]-1, 0[$ und $x_2 \in]0, 2[$. Dass es keine weiteren reellen Nullstellen geben kann, sagt uns der Satz von Rolle: Zwischen zwei Nullstellen von f muss jeweils eine Nullstelle von f' liegen. Für die Ableitung $f' = 3X^3 - 1$ gibt jedoch über den reellen Zahlen

$$f'(X) = 0 \iff X^3 - \frac{1}{3} = 0 \iff X = \frac{1}{\sqrt[3]{3}}.$$

f' hat also nur eine reelle Nullstelle, weswegen f nur 2 reelle Nullstellen haben kann.

- b** Die Reduktion modulo 2 von f ist das Polynom $\bar{f} = X^4 + X + 1$. Dieses hat keine Nullstellen in \mathbb{F}_2 und auch keinen quadratischen Faktor, da das einzige irreduzible Polynom in $\mathbb{F}_2[X]$ das Polynom $X^2 + X + 1$ ist und $(X^2 + X + 1)^2 = X^4 + X^2 + 1 \neq \bar{f}$ gilt. Nach dem Reduktionskriterium ist daher f irreduzibel über \mathbb{Q} .

c Wir machen vorab einige Zwischenschritte und berechnen

$$(X^2 + aX + b)(X^2 + cX + d) = \\ = X^4 + (a+c)X^3 + (ac+b+d)X^2 + (bc+ad)X + bd.$$

Mittels Koeffizientenvergleich mit f erhält man daraus die Gleichungen

$$a + c = 0, \quad ac + b + d = 0, \quad bc + ad = -1, \quad bd = -1.$$

Aus der ersten Gleichung gewinnt man die Relation $a = -c$ und Einsetzen in die anderen Gleichungen führt zu

$$(I) \ a^2 = b + d, \quad (II) \ a = \frac{1}{b-d}, \quad (III) \ bd = -1.$$

„ \Rightarrow “: Nehmen wir an, es gibt Zahlen $b, c, d \in \mathbb{C}$, die die obigen Gleichungen erfüllen. Dann gilt

$$\begin{aligned} g(a^2) &= a^6 + 4a^2 - 1 = \left(\frac{b+d}{b-d}\right)^2 + 4a^2 - 1 = \\ &= \frac{b^2 + 2bd + d^2}{(b-d)^2} + 4a^2 - 1 = \\ &= 1 + \frac{4bd}{(b-d)^2} + 4a^2 - 1 = \\ &= -4a^2 + 4a^2 = 0. \end{aligned}$$

„ \Leftarrow “: Einsetzen zeigt $g(0) \neq 0$, sodass $a \neq 0$ ist. Aus der Gleichung (II) erhalten wir deshalb zuerst $b - d = \frac{1}{a}$. Addieren wir diese Gleichung zu (I), so erhalten wir

$$2b = a^2 + \frac{1}{a} \Leftrightarrow b = \frac{1}{2} \left(a^2 + \frac{1}{a} \right)$$

und Subtraktion der Gleichungen liefert

$$2d = a^2 - \frac{1}{a} \Leftrightarrow d = \frac{1}{2} \left(a^2 - \frac{1}{a} \right).$$

Wir überprüfen noch, dass mit dieser Wahl auch die dritte Gleichung erfüllt ist. Hier gilt

$$bd = \frac{1}{4} \left(a^2 + \frac{1}{a} \right) \left(a^2 - \frac{1}{a} \right) = \frac{1}{4} \left(a^4 - \frac{1}{a^2} \right).$$

Nun gilt wegen $g(a^2) = a^6 + 4a^2 - 1 = 0$, dass

$$a^6 + 4a^2 = 1 \Leftrightarrow a^2(a^4 + 4) = 1 \Leftrightarrow \frac{1}{a^2} = a^4 + 4$$

und damit

$$bd = \frac{1}{4} \left(a^4 - \frac{1}{a^2} \right) = \frac{1}{4} \left(a^4 - a^4 - 4 \right) = -1.$$

Eine gesuchte Zerlegung erhält man also, indem man b und d wie oben und $c = -a$ setzt.

- d** Als Polynom von Grad 3 ist g genau dann irreduzibel über \mathbb{Q} , wenn es dort keine Nullstellen hat. Da g zudem ein normiertes Polynom mit ganzzahligen Koeffizienten ist, müssen nach Lemma 2.22 alle rationalen Nullstellen von g bereits in \mathbb{Z} liegen. Diese müssen den letzten Koeffizienten teilen, sodass nur ± 1 in Frage kommt. Man überzeugt sich jedoch schnell von $g(\pm 1) \neq 0$. Also ist g irreduzibel in $\mathbb{Q}[X]$.
- e** Nach Teil **c** gibt es $a, b \in \mathbb{C}$, sodass $(X^2 + aX + b)$ ein Teiler von f ist. Insbesondere sind die Nullstellen von $X^2 + aX + b$ auch Nullstellen von f . Aus der Darstellung $X^2 + aX + b = (X - \alpha)(X + \beta)$ folgt $a = -(\alpha + \beta)$. Sind α und β genau die reellen Nullstellen x_1 und x_2 , so sind wir fertig. Der Fall einer reellen und einer komplexen Nullstelle kann nicht auftreten, da sonst $a \notin \mathbb{R}$ wäre. Sind α und β genau die beiden komplexen Nullstellen, so müssen in dem Faktor $X^2 + cX + d$ aus Teil **c** die beiden reellen Nullstellen stecken, d. h. $X^2 + cX + d = (X - x_1)(X - x_2)$. Es folgt $c = -(x_1 + x_2)$ und in **c** haben wir auch gesehen, dass

$$a = -c = x_1 + x_2 \in \mathbb{Q}[x_1, x_2].$$

- f** Wären x_1 und x_2 beide konstruierbar, so wäre nach Proposition 3.28 auch a^2 konstruierbar, denn in **e** haben wir gesehen, dass $a^2 \in \{x_1 + x_2, -(x_1 + x_2)\}$. Laut Satz 3.29 gibt es dann einen Erweiterungskörper L von \mathbb{Q} , sodass $[L : \mathbb{Q}]$ eine Potenz von 2 ist.

Das Polynom g ist laut Teil **d** irreduzibel über \mathbb{Q} und als normiertes Polynom mit Nullstelle a^2 das Minimalpolynom eben jenes Elements über \mathbb{Q} . Aus $a^2 \in L$ folgt auch $\mathbb{Q}(a^2) \subseteq L$ und die Gradformel liefert:

$$3 = \deg g = [\mathbb{Q}(a^2) : \mathbb{Q}] \text{ teilt } [L : \mathbb{Q}].$$

Dies ist jedoch ein Widerspruch dazu, dass $[L : \mathbb{Q}]$ eine Potenz von 2 ist.

4. Lineare Algebra

4.1. Vektorräume und Basen

Zentral für die Lineare Algebra ist der Begriff des *K-Vektorraums*, wobei K einen Körper bezeichnet. Dabei handelt es sich um eine nicht-leere Menge V , sodass $(V, +)$ eine abelsche Gruppe ist, die zusätzlich mit einer Skalarmultiplikation $\cdot : K \times V \rightarrow V$ ausgestattet ist, für die die Distributivgesetze gelten.

Genauer: Für alle $\lambda, \mu \in K$ sowie $v, w \in V$ gilt

- (i) $\lambda \cdot (\mu \cdot v) = (\lambda \cdot \mu) \cdot v,$
- (ii) $(\lambda + \mu) \cdot v = \lambda \cdot v + \mu \cdot v,$
- (iii) $\lambda \cdot (v + w) = \lambda \cdot v + \lambda \cdot w,$
- (iv) $1 \cdot v = v.$

Jeder Vektorraum besitzt eine *Basis* B , welche äquivalent charakterisiert werden kann als

- (1) linear unabhängiges Erzeugendensystem,
- (2) minimales Erzeugendensystem,
- (3) maximale linear unabhängige Menge,
- (4) jeder Vektor besitzt eine eindeutige Darstellung als Linearkombination von Vektoren aus B .

Dabei sind (2) und (3) nur für den Fall einer endlichen Basis gedacht.

Eine Basis ist nicht eindeutig, jedoch ist es ihre Mächtigkeit. Diese Zahl wird als *Dimension* bezeichnet und als $\dim_K V$ notiert.

Die Existenz einer Basis ist nun der Ausgangspunkt für die Entwicklung der weiteren Theorie: Beispielsweise stiftet die Wahl einer Basis im Fall $\dim_K V = n$ einen Isomorphismus $V \cong K^n$, der durch die Koordinatenabbildung gegeben ist. Insbesondere sind alle Vektorräume gleicher (endlicher) Dimension isomorph.

Weiterhin ermöglicht die Wahl einer Basis die Identifizierung von linearen Abbildungen und Matrizen. Seien dazu V und W Vektorräume der Dimension n bzw. m mit Basen $B = \{v_1, \dots, v_n\}$ und $B' = \{w_1, \dots, w_m\}$. Jede lineare Abbildung $L: V \rightarrow W$ ist durch die Bilder der Basisvektoren aus B bereits eindeutig bestimmt, sodass die gesamte Information über die lineare Abbildung bereits in der Matrix $(a_{ij}) \in \mathcal{M}_{m \times n}(K)$ mit

$$L(v_j) = \sum_{i=1}^m a_{ij} w_i$$

hinterlegt ist. Diese sogenannte **Darstellungsmatrix** hängt offensichtlich von der Wahl der Basen ab und wird als $[L]_{B,B'}$ notiert. Umgekehrt kann man einer Matrix $A \in \mathcal{M}_{m \times n}(K)$ durch $\phi_A^{B,B'} : V \rightarrow W, v \mapsto Av$ eine lineare Abbildung zuordnen. Auf diese Weise erhalten wir zueinander inverse Vektorraumisomorphismen

$$\begin{array}{ccc} \mathcal{M}_{m \times n}(K) & \xrightarrow{\hspace{1cm}} & \text{Hom}_K(V, W) \\ A & \longmapsto & \phi_A^{B,B'} \\ [L]_{B,B'} & \longleftarrow & L \end{array}$$

Falls die gewählten Basen nicht explizit angegeben sind, werden wir stillschweigend voraussetzen, dass dies die jeweiligen Standardbasen sind und dies auch in der Notation entsprechend unterdrücken.

Anleitung: Abzählen von Basen

In den nächsten Aufgaben wird es wiederholt nötig sein, die Anzahl der Basen bzw. Untervektorräume eines Vektorraums über einem endlichen Körper \mathbb{F}_q zu bestimmen. Sei dazu nun $V \cong \mathbb{F}_q^n$ ein \mathbb{F}_q -Vektorraum der Dimension n .

- (1) Der erste Vektor v_1 einer Basis ist ein beliebiger Vektor aus $\mathbb{F}_q^n \setminus \{0\}$, denn der Nullvektor ist zu jedem Vektor linear abhängig. Es gibt hier also $|\mathbb{F}_q^n \setminus \{0\}| = q^n - 1$ Möglichkeiten der Wahl.
- (2) Ist der k -te Basisvektor v_k bereits gewählt, so kann v_{k+1} aus allen Vektoren gewählt werden, die zu den bisher gewählten Basisvektoren linear unabhängig sind. Man kann also aus $\mathbb{F}_q^n \setminus \langle v_1, \dots, v_k \rangle$ wählen. Als Vektorraum der Dimension k ist $\langle v_1, \dots, v_k \rangle \cong \mathbb{F}_q^k$, daher haben wir $|\mathbb{F}_q^n \setminus \langle v_1, \dots, v_k \rangle| = q^n - q^k$ Wahlmöglichkeiten.
- (3) Die Anzahl der möglichen Basen ist nun durch das Produkt gegeben und beträgt

$$(q^n - 1) \cdot (q^n - q) \cdot \dots \cdot (q^n - q^{n-1}).$$

- (4) Was ist nun für $m \leq n$ die Anzahl der m -dimensionalen Untervektorräume von V ? Wie in den Schritten (1) und (2) beschrieben kann man

$$(q^n - 1) \cdot (q^n - q) \cdot \dots \cdot (q^n - q^{m-1})$$

Basen der Länge m wählen. Allerdings werden diese Basen im Allgemeinen keine unterschiedlichen Vektorräume erzeugen, denn nach der

gleichen Argumentation besitzt ein m -dimensionaler Vektorraum

$$(q^m - 1) \cdot (q^m - q) \cdot \dots \cdot (q^m - q^{m-1})$$

viele Basen. Dies entspricht also der Zahl der Basen, die jeweils den gleichen Untervektorraum erzeugen. Somit ist die Zahl der m -dimensionalen Vektorräume gleich

$$\frac{(q^n - 1) \cdot (q^n - q) \cdot \dots \cdot (q^n - q^{m-1})}{(q^m - 1) \cdot (q^m - q) \cdot \dots \cdot (q^m - q^{m-1})}.$$

Aufgabe (Herbst 2015, T1A2)

Sei \mathbb{F}_q der endliche Körper mit q Elementen.

- a** Zeigen Sie, dass für $n \geq 1$ die Anzahl der eindimensionalen \mathbb{F}_q -Untervektorräume von \mathbb{F}_q^n gleich $\frac{q^n - 1}{q - 1}$ ist.
- b** Zeigen Sie, dass die Anzahl der zweidimensionalen Untervektorräume von \mathbb{F}_q^3 gleich der Anzahl der eindimensionalen Untervektorräume von \mathbb{F}_q^3 ist.
- c** Wie viele Zerlegungen von \mathbb{F}_q^3 in direkte Summen von \mathbb{F}_q -Untervektorräumen $V_1 \oplus V_2$ gibt es mit $\dim_{\mathbb{F}_q}(V_1) = 2$?

Lösungsvorschlag zur Aufgabe (Herbst 2015, T1A2)

- a** Jeder eindimensionale Vektorraum von \mathbb{F}^n hat die Form $\langle v \rangle$ für ein $v \in \mathbb{F}_q^n$. Dieser Vektor v kann ein beliebiger Vektor aus $\mathbb{F}_q^n \setminus \{0\}$ sein, d. h. für dessen Wahl gibt es $q^n - 1$ Möglichkeiten. Allerdings erzeugen zwei solche Vektoren v und w genau dann den gleichen Untervektorraum, wenn sie linear abhängig sind:

$$\langle v \rangle = \langle w \rangle \Leftrightarrow \exists \lambda \in \mathbb{F}_q^\times : w = \lambda v.$$

Wegen $|\mathbb{F}_q^\times| = q - 1$ ergibt sich für die Anzahl der verschiedenen eindimensionalen Untervektorräume von \mathbb{F}_q^n daher $\frac{q^n - 1}{q - 1}$.

- b** Die Anzahl der verschiedenen zweidimensionalen Untervektorräume von \mathbb{F}_q^3 entspricht in Analogie zu Teil **a** der Anzahl der linear unabhängigen Mengen $\{v, w\}$ mit Vektoren $v, w \in \mathbb{F}_q^3$. Für die Wahl des ersten Vektors v gibt es $q^3 - 1$ Möglichkeiten, für den zweiten Vektor w dann $q^3 - q = |\mathbb{F}_q^3 \setminus \langle v \rangle|$ Möglichkeiten. Insgesamt also $(q^3 - 1)(q^3 - q)$ viele.

In einem zweidimensionalen \mathbb{F}_q -Vektorraum lassen sich nach der gleichen Argumentation jedoch $(q^2 - 1)(q^2 - q)$ Basen wählen, sodass die gesuchte Anzahl

$$\frac{(q^3 - 1)(q^3 - q)}{(q^2 - 1)(q^2 - q)} = \frac{(q^3 - 1)q}{q^2 - q} = \frac{q^3 - 1}{q - 1}$$

ist. Dies entspricht genau der Anzahl der eindimensionalen Untervektorräume aus Teil **a**.

- c** Nach Teil **b** gibt es $\frac{q^3 - 1}{q - 1}$ Möglichkeiten für die Wahl von V_1 . Für die Wahl von $v \in \mathbb{F}_q^3$ mit $V_2 = \langle v \rangle$ kommen dann prinzipiell $q^3 - q^2 = |\mathbb{F}_q^3 \setminus V_1|$ viele Vektoren in Frage. Allerdings erzeugen davon wiederum $q - 1$ viele den gleichen Untervektorraum, sodass es nur $\frac{q^3 - q^2}{q - 1} = q^2$ verschiedene Untervektorräume V_2 gibt. Die Anzahl der Zerlegungen $\mathbb{F}_q^3 = V_1 \oplus V_2$ berechnet sich dann zu $\frac{q^3 - 1}{q - 1} \cdot q^2$.

Aufgabe (Frühjahr 2013, T2A2)

Sei $q > 1$ eine Potenz einer Primzahl p , und sei \mathbb{F}_q ein Körper mit q Elementen. Sei n eine natürliche Zahl, und sei $G = GL_n(\mathbb{F}_q)$ die Gruppe der invertierbaren $(n \times n)$ -Matrizen über \mathbb{F}_q .

- a** Zeigen Sie, dass die Gruppe G von Ordnung

$$q^{\binom{n}{2}}(q^n - 1) \cdot (q^{n-1} - 1) \cdot \dots \cdot (q - 1)$$

ist.

- b** Zeigen Sie, dass die oberen Dreiecksmatrizen mit charakteristischem Polynom $(X - 1)^n$ eine Sylowsche p -Untergruppe von $GL_n(\mathbb{F}_q)$ bilden.

Lösungsvorschlag zur Aufgabe (Frühjahr 2013, T2A2)

- a** Eine Matrix $A \in \mathcal{M}_n(\mathbb{F}_q)$ ist genau dann invertierbar, wenn ihre Spalten linear unabhängig sind. Wir bestimmen daher die Anzahl der Möglichkeiten, n linear unabhängige Vektoren $v_1, \dots, v_n \in \mathbb{F}_q^n$ zu wählen.

Der erste Vektor kann beliebig aus $\mathbb{F}_q^n \setminus \{0\}$ gewählt werden, d. h. hier gibt es $q^n - 1$ Möglichkeiten der Wahl. Der zweite Vektor kann beliebig aus $\mathbb{F}_q^n \setminus \langle v_1 \rangle$ gewählt werden, sodass hier $q^n - q$ Vektoren zur Wahl stehen. Dieses Vorgehen setzt man fort und erhält als Produkt dieser jeweiligen

Wahlmöglichkeiten

$$\begin{aligned}
 & (q^n - 1) \cdot (q^n - q) \cdot \dots \cdot (q^n - q^{n-1}) = \\
 &= (q^n - 1) \cdot q(q^{n-1} - 1) \cdot \dots \cdot q^{n-1}(q - 1) = \\
 &= q^{\sum_{k=1}^{n-1} k} (q^n - 1) \cdot (q^{n-1} - 1) \cdot \dots \cdot (q - 1).
 \end{aligned}$$

Wir zeigen noch, dass $\sum_{k=1}^{n-1} k = \binom{n}{2}$ gilt: Für $n = 1$ ist per Konvention $\binom{1}{2} = 0 = \sum_{k=1}^0 k$. Für $n \geq 2$ gilt unter Verwendung der Summenformel für die ersten n natürlichen Zahlen („kleiner Gauß“), dass

$$\sum_{k=1}^{n-1} k = \frac{n(n-1)}{2} = \frac{n!}{2! \cdot (n-2)!} = \binom{n}{2}.$$

- b** Sei $A = (a_{ij}) \in G$ eine obere Dreiecksmatrix. Da die Determinante einer Dreiecksmatrix durch das Produkt der Diagonaleinträge gegeben ist, gilt für das charakteristische Polynom von A die Äquivalenz

$$\begin{aligned}
 \chi_A = \det(X \cdot \text{id}_{\mathbb{F}_q^3} - A) &= (X-1)^n \quad \Leftrightarrow \quad \prod_{i=1}^n (X - a_{ii}) = (X-1)^n \\
 &\Leftrightarrow \quad \forall i \in \{1, \dots, n\} : a_{ii} = 1,
 \end{aligned}$$

also müssen wir zeigen, dass die Menge

$$U = \{(a_{ij}) \in G \mid a_{ii} = 1 \text{ für } i \in \{1, \dots, n\}, a_{ij} = 0 \text{ für } i > j\}$$

aller oberen Dreiecksmatrizen mit 1 auf der Diagonalen eine p -Sylowgruppe von G ist. Wir zeigen zunächst die Untergruppeneigenschaften.

Dass die Einheitsmatrix in U liegt, ist klar. Seien nun $A = (a_{ij})$ und $B = (b_{ij})$ aus U und $AB = (c_{ij})$. Dann gilt

$$c_{ij} = \sum_{k=1}^n a_{ik} b_{kj}$$

und folglich $c_{ii} = \sum_{k=1}^n a_{ik} b_{ki} = a_{ii} b_{ii} = 1$ für alle $i \in \{1, \dots, n\}$, da $a_{ik} = 0$ für $i > k$ und $b_{ki} = 0$ für $i < k$. Also sind schon mal alle Diagonaleinträge von AB gleich 1. Weiterhin gilt für $i > j$, dass $c_{ij} = 0$, denn es ist $a_{ik} = 0$ für $i > k$ und $b_{kj} = 0$ für $k > j$, sodass ein Summand nur ungleich 0 ist, falls $i \leq k \leq j$ ist. Für $i > j$ ist dies jedoch unmöglich. Also handelt es sich bei AB auch um eine obere Dreiecksmatrix.

Da $\mathrm{GL}_n(\mathbb{F}_q)$ eine endliche Gruppe ist, gibt es nach Proposition 1.6 ein $m \in \mathbb{N}$ mit $\mathbb{E}_n = A^m = A \cdot A^{m-1}$. Also ist $A^{-1} = A^{m-1}$ und nach dem oben Gezeigten liegt daher auch die Inverse von A in U .

Nun bestimmen wir noch die Ordnung von U . In der ersten Spalte einer Matrix aus U sind bereits alle Einträge festgelegt (nämlich $(1, 0, \dots)$), in der zweiten Spalte ist ein Eintrag frei wählbar, in der dritten zwei usw. Insgesamt also

$$q \cdot q^2 \cdot \dots \cdot q^{n-1} = q^{\sum_{k=1}^{n-1} k} = q^{\binom{n}{2}}$$

viele. Da $|G| = q^{\binom{n}{2}} \prod_{k=1}^n (q^k - 1)$ ist und keiner der Faktoren des Produkts von p geteilt wird, ist U eine maximale p -Gruppe, d.h. eine p -Sylowgruppe.

Aufgabe (Frühjahr 2013, T1A3)

Sei $G = \mathrm{SL}_2(\mathbb{F}_7) = \{A \in \mathrm{GL}_2(\mathbb{F}_7) \mid \det(A) = 1\}$ und $H = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \mid a \in \mathbb{F}_7 \right\}$.

- a** Zeigen Sie, dass H eine Untergruppe der Ordnung 7 von G ist.
- b** Zeigen Sie, dass $\mathrm{SL}_2(\mathbb{F}_7)$ Ordnung 336 hat.
- c** Wie viele Untergruppen der Ordnung 7 gibt es in G ?

Lösungsvorschlag zur Aufgabe (Frühjahr 2013, T1A3)

- a** Dass die Einheitsmatrix in H liegt, ist klar. Seien nun

$$A = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \in H \quad \text{und} \quad B = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \in H$$

vorgegeben. Dann ist

$$AB = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+b \\ 0 & 1 \end{pmatrix} \in H$$

und

$$A^{-1} = \begin{pmatrix} 1 & -a \\ 0 & 1 \end{pmatrix} \in H,$$

also handelt es sich bei H um eine Untergruppe von G . Dass H Ordnung 7 hat, folgt direkt aus $|\mathbb{F}_7| = 7$.

b Betrachte die Determinantenabbildung

$$\det: \mathrm{GL}_2(\mathbb{F}_7) \rightarrow \mathbb{F}_7^\times,$$

welche ein Gruppenhomomorphismus und surjektiv ist, denn für beliebiges $a \in \mathbb{F}_7^\times$ ist beispielsweise $\begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix}$ ein Urbild. Der Kern der Determinantenabbildung ist gerade $\mathrm{SL}_2(\mathbb{F}_7)$, also gibt es nach dem Homomorphiesatz einen Isomorphismus

$$\mathrm{GL}_2(\mathbb{F}_7)/\mathrm{SL}_2(\mathbb{F}_7) \cong \mathbb{F}_7^\times$$

und der Satz von Lagrange liefert

$$\frac{|\mathrm{GL}_2(\mathbb{F}_7)|}{|\mathrm{SL}_2(\mathbb{F}_7)|} = |\mathbb{F}_7^\times| \Leftrightarrow |\mathrm{SL}_2(\mathbb{F}_7)| = \frac{|\mathrm{GL}_2(\mathbb{F}_7)|}{|\mathbb{F}_7^\times|} = \frac{|\mathrm{GL}_2(\mathbb{F}_7)|}{6}.$$

Wir müssen also nur noch die Zahl aller invertierbaren Matrizen $|\mathrm{GL}_2(\mathbb{F}_7)|$ bestimmen. Eine Matrix $A \in \mathcal{M}_2(\mathbb{F}_7)$ ist genau dann invertierbar, wenn ihre Spalten linear unabhängig sind. Es genügt daher, die Anzahl linear unabhängiger Mengen $\{v, w\}$ mit $v, w \in \mathbb{F}_7^2$ zu ermitteln.

Für die Wahl des ersten Vektors v gibt es nur die Einschränkung $v \neq 0$, also gibt es hier $|\mathbb{F}_7^2 \setminus \{(0, 0)\}| = 7^2 - 1 = 48$ Wahlmöglichkeiten. Der zweite Vektor w kann beliebig aus $\mathbb{F}_7^2 \setminus \langle v \rangle$ gewählt werden, das sind $7^2 - 7 = 42$ potentielle Vektoren. Wir erhalten daher insgesamt

$$|\mathrm{SL}_2(\mathbb{F}_7)| = \frac{|\mathrm{GL}_2(\mathbb{F}_7)|}{6} = \frac{48 \cdot 42}{6} = 8 \cdot 42 = 336.$$

c Es ist $336 = 2^4 \cdot 3 \cdot 7$, also ist nach den Anzahl der 7-Sylowgruppen ν_7 gefragt. Für diese gilt laut den Sylowsätzen, dass

$$\nu_7 \mid 2^4 \cdot 3 \Rightarrow \nu_7 \in \{1, 2, 3, 4, 6, 8, 12, 16, 24, 48\}.$$

Die einzigen Zahlen aus der Liste, die zusätzlich kongruent zu 1 mod 7 sind, sind 1 und 8. Angenommen, es ist $\nu_7 = 1$. In **a** haben wir gezeigt, dass H eine Untergruppe der Ordnung 7 ist, diese muss damit die einzige 7-Sylowgruppe sein. Außerdem wäre H als einzige 7-Sylowgruppe ein Normalteiler von G , sodass für jedes $A \in G$ und $B \in H$ dann $A^{-1}BA \in H$ erfüllt sein muss. Jedoch gilt für

$$A = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \quad \text{und} \quad B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

dass das Produkt

$$A^{-1}BA = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ -1 & 0 \end{pmatrix}$$

offensichtlich nicht in H liegt. Damit kann H kein Normalteiler sein und es muss $v_7 \neq 1$ gelten. Es folgt $v_7 = 8$.

Aufgabe (Herbst 2012, T1A1)

Sei p eine Primzahl und $q = p^l$ für ein $l > 0$ ($l \in \mathbb{N}$). Sei \mathbb{F}_q der endliche Körper mit q Elementen.

- a** Zeigen Sie, dass die Gruppe $G = \mathrm{SL}_2(\mathbb{F}_q)$ der 2×2 -Matrizen mit Einträgen in \mathbb{F}_q und Determinante 1 die Ordnung $q(q^2 - 1)$ hat.

Wir betrachten nun die Untergruppen

$$B = \left\{ \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \in \mathrm{SL}_2(\mathbb{F}_q) \mid a \in \mathbb{F}_q^\times, b \in \mathbb{F}_q \right\}$$

und

$$N^- = \left\{ \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{F}_q) \mid a \in \mathbb{F}_q \right\}$$

von G .

- b** Sei $\Omega = G/B$ die Menge der Linksnebenklassen von G bzgl. B . Bestimmen Sie die Ordnungen von N^- und B und die Anzahl $|\Omega|$ der Elemente aus Ω .
- c** Die Gruppe N^- operiert auf Ω durch Multiplikation von links. Zeigen Sie, dass diese Operation einen Fixpunkt besitzt.

Lösungsvorschlag zur Aufgabe (Herbst 2012, T1A1)

- a** Wir betrachten die Determinantenabbildung

$$\det: \mathrm{GL}_2(\mathbb{F}_q) \rightarrow \mathbb{F}_q^\times,$$

welche ein surjektiver Gruppenhomomorphismus ist und als Kern gerade $G = \mathrm{SL}_2(\mathbb{F}_q)$ hat. Folglich gilt unter Verwendung des Homomorphiesatzes und des Satzes von Lagrange, dass

$$|\mathrm{GL}_2(\mathbb{F}_q)/G| = |\mathbb{F}_q^\times| \Leftrightarrow |G| = \frac{|\mathrm{GL}_2(\mathbb{F}_q)|}{|\mathbb{F}_q^\times|} = \frac{|\mathrm{GL}_2(\mathbb{F}_q)|}{q-1}.$$

Wir bestimmen daher nun $|\mathrm{GL}_2(\mathbb{F}_q)|$. Da eine Matrix $A \in \mathcal{M}_2(\mathbb{F}_q)$ genau dann invertierbar ist, wenn ihre Spalten \mathbb{F}_q -linear unabhängig sind, zählen wir dafür die Möglichkeiten, eine Menge $\{v, w\}$ zweier linear unabhängiger Vektoren $v, w \in \mathbb{F}_q^2$ zu kreieren. Für die Wahl des ersten Vektors v stehen $|\mathbb{F}_q^2 \setminus \{(0, 0)\}| = q^2 - 1$ Vektoren zur Wahl, für den zweiten Vektor kann man aus $|\mathbb{F}_q^2 \setminus \langle v \rangle| = q^2 - q$ möglichen Vektoren wählen. Wir erhalten daher

$$|G| = \frac{|\mathrm{GL}_2(\mathbb{F}_q)|}{q-1} = \frac{(q^2-1)(q^2-q)}{q-1} = (q^2-1)q.$$

b Es ist $|N^-| = |\mathbb{F}_q| = q$ und $|B| = |\mathbb{F}_q^\times| \cdot |\mathbb{F}_q| = (q-1) \cdot q$, also ist

$$|\Omega| = \frac{|G|}{|B|} = \frac{q(q^2-1)}{q(q-1)} = q+1.$$

c Hier brauchen wir die Bahnengleichung 1.18. Diese hat im vorliegenden Fall die Form

$$|\Omega| = |F| + \sum_{x \in R} (N^- : \mathrm{Stab}_{N^-}(x)),$$

wobei F die Fixpunktmenge der Operation und R ein Repräsentantensystem der Bahnen von Länge > 1 bezeichnet. Nehmen wir an, es gilt $F = \emptyset$. Die auftretenden Summanden $(N^- : \mathrm{Stab}_{N^-}(x))$ sind jeweils Teiler von $|N^-| = q$ und müssen daher gleich q sein (da die Bahnengrößen nach Annahme alle echt größer 1 sind). Dies bedeutet aber, dass in

$$q+1 = |\Omega| = \sum_{x \in R} (N^- : \mathrm{Stab}_{N^-}(x))$$

die rechte Seite von q geteilt wird, während dies für die linke nicht der Fall ist. Wir erhalten einen Widerspruch, weswegen die Annahme $F = \emptyset$ falsch gewesen sein muss und es einen Fixpunkt $\omega \in F$ gibt.

Aufgabe (Frühjahr 2011, T2A3)

Sei $V := \mathbb{F}_2^2$ der zweidimensionale Vektorraum über dem Körper \mathbb{F}_2 mit zwei Elementen. Sei

$$G := \{v \mapsto Av + b \mid A \in \mathrm{GL}_2(\mathbb{F}_2), b \in V\}$$

die Gruppe der affinen Abbildungen von V .

- a** Geben Sie alle Matrizen in $\mathrm{GL}_2(\mathbb{F}_2)$ an.
- b** Zeigen Sie die folgenden Isomorphismen: $G \cong S_4$, $\mathrm{GL}_2(\mathbb{F}_2) \cong S_3$. (Hierbei bedeutet S_m die symmetrische Gruppe vom Grad m .)

Lösungsvorschlag zur Aufgabe (Frühjahr 2011, T2A3)

- a** Eine Matrix $A \in M_2(\mathbb{F}_2)$ ist genau dann invertierbar und liegt somit in $\text{GL}_2(\mathbb{F}_2)$, wenn ihre Spalten linear unabhängig sind. Wir wählen daher zunächst einen Vektor für die erste Spalte v aus

$$\mathbb{F}_2^2 \setminus \{(0,0)\} = \left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\}.$$

Für die zweite Spalte können wir nur noch einen Vektor aus $\mathbb{F}_2^2 \setminus \langle v \rangle$ wählen, wegen $\langle v \rangle = \{\lambda v \mid \lambda \in \mathbb{F}_2\} = \{(0,0), v\}$ stehen hier jeweils die anderen beiden Vektoren aus $\mathbb{F}_2^2 \setminus \{(0,0)\}$ zur Wahl. Diese Überlegungen liefern uns

$$\text{GL}_2(\mathbb{F}_2) = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \right\}.$$

- b** Sei $\tau \in G$ eine affine Abbildung, d. h. es gibt $A \in \text{GL}_2(\mathbb{F}_2)$ und $b \in \mathbb{F}_2^2$, sodass $\tau(v) = Av + b$ für alle $v \in \mathbb{F}_2^2$ erfüllt ist. Dann ist τ eine bijektive Abbildung, denn sind $v, w \in \mathbb{F}_2^2$ Vektoren mit $\tau(v) = \tau(w)$, so folgt

$$\begin{aligned} Av + b &= Aw + b \quad \Leftrightarrow \quad Av = Aw \\ \Leftrightarrow A^{-1}Av &= A^{-1}Aw \quad \Leftrightarrow \quad v = w, \end{aligned}$$

sodass τ injektiv ist. Für beliebiges $v \in \mathbb{F}_2^2$ kann man $w = A^{-1}(v - b)$ setzen und erhält

$$\tau(w) = A(A^{-1}(v - b)) + b = (v - b) + b = v,$$

also ist τ auch surjektiv. Wir haben damit $\tau \in \text{Per}(\mathbb{F}_2^2)$ gezeigt. Da τ beliebig aus G gewählt war, ist $G \subseteq \text{Per}(\mathbb{F}_2^2)$ und wegen $|\mathbb{F}_2^2| = 4$ ist $\text{Per}(\mathbb{F}_2^2) \cong S_4$. Außerdem gilt $|G| = 24$, denn für die Wahl von A in $v \mapsto Av + b$ gibt es nach Teil **a** 6 Möglichkeiten und für b gibt es $|\mathbb{F}_2^2| = 4$ Möglichkeiten. Also ist $|G| = 6 \cdot 4 = 24 = |S_4|$ und zusammen mit $G \subseteq \text{Per}(\mathbb{F}_2^2) \cong S_4$ haben wir $G \cong S_4$.

Um die Isomorphie $\text{GL}_2(\mathbb{F}_2) \cong S_3$ zu zeigen, ordnen wir jeder Matrix $A \in U = \text{GL}_2(\mathbb{F}_2)$ eine Abbildung auf $X = \mathbb{F}_2^2 \setminus \{(0,0)\}$ mittels

$$U \rightarrow \text{Per}(X), \quad A \mapsto \phi_A, \quad \text{wobei } \phi_A: X \rightarrow X, \quad v \mapsto Av$$

zu. Diese Abbildung ist wohldefiniert, denn weil $A \in U$ invertierbar ist, ist $\ker A = \{(0,0)\}$, sodass $Av \neq (0,0)$, falls $v \neq (0,0)$. Man zeigt auch

leicht, dass es sich um einen Homomorphismus handelt. Außerdem ist diese Abbildung injektiv, denn aus $\phi_A = \phi_B$ folgt insbesondere, dass

$$A \begin{pmatrix} 1 \\ 0 \end{pmatrix} = B \begin{pmatrix} 1 \\ 0 \end{pmatrix},$$

was bedeutet, dass die erste Spalte von A und B übereinstimmt. Durch Einsetzen von $(0, 1)$ sieht man analog, dass die zweite Spalte von A und B übereinstimmt, d.h. es gilt $A = B$.

Wir haben also eine Einbettung $U \hookrightarrow \text{Per}(X) \cong S_3$. Wegen $|U| = 6 = |S_3|$ ist diese bereits ein Isomorphismus.

4.2. Diagonalisierbarkeit

Sei V ein K -Vektorraum der Dimension n . Sieht man Endomorphismen von V als gleich an, wenn sie durch einen Basiswechsel ineinander überführt werden können, so wird dies auf der Seite der Matrizen durch eine Äquivalenzrelation auf $A \in \mathcal{M}_n(K)$ repräsentiert, die durch

$$A \sim B : \Leftrightarrow \exists T \in \text{GL}_n(K) : A = T^{-1}BT$$

definiert ist. Zwei Matrizen nennen wir *ähnlich*, falls sie in der gleichen Äquivalenzklasse dieser Relation liegen. Es liegt auf der Hand, dass es in vielen Situationen nützlich ist, einen möglichst einfachen Vertreter der jeweiligen Äquivalenzklasse zu wählen. Wann dies möglich ist und was in diesem Zusammenhang „möglichst einfach“ bedeutet, wird in diesem und im folgenden Abschnitt entwickelt.

Die Theorie kann äquivalent für Matrizen bzw. für Endomorphismen formuliert werden, da die Definitionen und Resultate weder von der Wahl einer Basis im Falle von Endomorphismen noch von der Wahl eines Vertreters der jeweiligen Äquivalenzklasse von Matrizen abhängen werden. Wir beschränken uns daher darauf, eine Formulierung zu geben, und hoffen, dass der Leser nicht verwirrt sein möge, falls doch ein Wechsel zwischen diesen Formulierungen stattfinden sollte.

Eigenräume

Definition 4.1. Sei V ein K -Vektorraum und $A \in \mathcal{M}_n(K)$ eine Matrix.

- (1) Ein Skalar $\lambda \in K$ heißt *Eigenwert* von A , falls es einen Vektor $v \in V$ mit $v \neq 0$ und $Av = \lambda v$ gibt. In diesem Fall heißt v dann *Eigenvektor* von A .

- (2) Der Untervektorraum aller Eigenvektoren (zusammen mit dem Nullvektor) zu einem Eigenwert $\lambda \in K$ notieren wir als

$$\text{Eig}(A, \lambda) = \{v \in V \mid Av = \lambda v\} \cup \{0\}$$

und nennen ihn den **Eigenraum** von A zum Eigenwert λ .

Sei $\lambda \in K$ ein Eigenwert der $n \times n$ -Matrix A . Man sieht unmittelbar, dass

$$\text{Eig}(A, \lambda) = \{v \in V \mid Av - \lambda v = 0\} = \ker(A - \lambda \mathbb{E}_n)$$

gilt. Da es einen Eigenvektor $v \neq 0$ zum Eigenwert λ gibt, bedeutet dies, dass $\ker(A - \lambda \mathbb{E}_n) \neq 0$ ist. Folglich ist $(A - \lambda \mathbb{E}_n)$ nicht invertierbar und es folgt $\det(A - \lambda \mathbb{E}_n) = 0$.

Ist umgekehrt $\lambda \in K$ ein Skalar, sodass $\det(A - \lambda \mathbb{E}_n) = 0$ gilt, so ist $\ker(A - \lambda \mathbb{E}_n) \neq 0$. Es gibt also einen Vektor $v \neq 0$ in $\ker(A - \lambda \mathbb{E}_n)$, sodass λ ein Eigenwert und v ein Eigenvektor von A ist. Dies gibt Anlass zur nächsten Definition.

Definition 4.2. Sei V ein endlich-dimensionaler K -Vektorraum und $A \in \mathcal{M}_n(K)$ eine Matrix, dann heißt

$$\chi_A = \det(A - X \cdot \mathbb{E}_n) \in K[X]$$

das **charakteristische Polynom** von A .

Ähnliche Matrizen haben das gleiche charakteristische Polynom und alle Begriffe lassen sich entsprechend für Endomorphismen $L: V \rightarrow V$ definieren, indem man die entsprechende Definition für die Darstellungsmatrix $[L]$ von L verwendet.

Oben haben wir gezeigt:

$$\lambda \in K \text{ ist Eigenwert von } A \Leftrightarrow \chi_A(\lambda) = 0$$

Aufgabe (Frühjahr 2014, T1A4)

Seien A, B komplexe $(n \times n)$ -Matrizen mit $AB = BA$.

- a** Man zeige, dass B jeden Eigenraum von A invariant lässt, d. h.:
Für jeden Eigenraum U von A gilt $Bu \in U$ für alle $u \in U$.
- b** Man zeige, dass A und B einen gemeinsamen Eigenvektor haben, d. h.:
Es gibt $0 \neq v \in \mathbb{C}^n$ und $\lambda, \mu \in \mathbb{C}$ mit $Av = \lambda v, Bv = \mu v$.
- c** Man zeige anhand eines Beispiels, dass die Aussage aus **b** ohne die Voraussetzung $AB = BA$ im Allgemeinen nicht gilt.

Lösungsvorschlag zur Aufgabe (Frühjahr 2014, T1A4)

- a** Sei $u \in U$ ein Eigenvektor von A zum Eigenwert λ . Dann gilt

$$A(Bu) = (AB)u = (BA)u = B(Au) = B(\lambda u) = \lambda(Bu),$$

d.h. Bu ist ebenfalls ein Eigenvektor zum Eigenwert λ .

- b** Nach Teil **a** gilt $B(U) \subseteq U$, d.h. wir können die Einschränkung $B|_U: U \rightarrow U$ betrachten. Da U wiederum ein \mathbb{C} -Vektorraum ist, zerfällt das charakteristische Polynom von $B|_U$ in Linearfaktoren und es gibt einen Eigenvektor $v \in U$ von $B|_U$. Dieser ist insbesondere ein Eigenvektor von B und nach Definition von U auch ein Eigenvektor von A .

- c** Betrachte die komplexen 2×2 -Matrizen

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \quad \text{und} \quad B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Es gilt

$$AB = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = BA$$

und man überprüft schnell, dass die Eigenwerte von A durch 1 und 0 gegeben sind. Die zugehörigen Eigenräume sind $\text{Eig}(A, 1) = \langle (1, 0) \rangle$ und $\text{Eig}(A, 0) = \langle (0, 1) \rangle$. Jedoch sieht man anhand

$$B \begin{pmatrix} x \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ x \end{pmatrix} \quad B \begin{pmatrix} 0 \\ x \end{pmatrix} = \begin{pmatrix} x \\ 0 \end{pmatrix},$$

für beliebiges $x \in \mathbb{C}^\times$, dass kein Eigenvektor von A ein Eigenvektor von B ist.

Diagonalisierbarkeit

Unser erstes Ziel besteht darin, Matrizen zu charakterisieren, die zu einer Matrix in Diagonalgestalt ähnlich sind. Das bedeutet, dass es eine Basis B gibt, bezüglich derer die Matrix M die Form

$$[M]_B = \begin{pmatrix} \lambda_1 & 0 & \cdots & \cdots & 0 \\ 0 & \ddots & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & & 0 \\ 0 & \cdots & \cdots & 0 & \lambda_n \end{pmatrix}$$

besitzt. Ist $B = \{v_1, \dots, v_n\}$, so bedeutet obige Gestalt, dass $Mv_i = \lambda_i v_i$ für $i \in \{1, \dots, n\}$ gilt. Also hat $[M]_B$ genau dann Diagonalgestalt, wenn B eine Basis aus Eigenvektoren ist. Sind λ_i die zugehörigen Eigenwerte, so ist dies äquivalent zu

$$K^n \cong \bigoplus_{i=1}^n \text{Eig}(M, \lambda_i).$$

Definition 4.3. Es seien K ein Körper, $n \in \mathbb{N}$, $M \in \mathcal{M}_n(K)$ und $\lambda_1, \dots, \lambda_m \in K$ die verschiedenen Eigenwerte von M .

- (1) Ist $\chi_M = \prod_{i=1}^m (X - \lambda_i)^{\nu(M, \lambda_i)}$ eine Zerlegung des charakteristischen Polynoms über $K[X]$ in Linearfaktoren, so heißt $\nu(M, \lambda_i)$ die *algebraische Vielfachheit* des Eigenwerts λ_i . Sie entspricht der Vielfachheit der Nullstelle λ_i von χ_M .
- (2) Die *geometrische Vielfachheit* eines Eigenwerts λ_i ist $\dim_K \text{Eig}(M, \lambda_i)$.

Wir bewegen uns nun weiter in Richtung einer Basis aus Eigenvektoren.

Lemma 4.4. Sei K ein Körper, $n \in \mathbb{N}$ und $M \in \mathcal{M}_n(K)$.

- (1) Eigenvektoren zu verschiedenen Eigenwerten sind linear unabhängig.
- (2) Für jeden Eigenwert $\lambda \in K$ von M gilt

$$1 \leq \dim_K \text{Eig}(M, \lambda) \leq \nu(M, \lambda).$$

Satz 4.5. Sei K ein Körper, $n \in \mathbb{N}$ und $M \in \mathcal{M}_n(K)$. Dann sind gleichwertig:

- (1) M ist diagonalisierbar.
- (2) Es gibt eine Basis von K^n aus Eigenvektoren von M .
- (3) Das charakteristische Polynom χ_M zerfällt in Linearfaktoren und für jeden Eigenwert $\lambda \in K$ von M gilt $\nu(M, \lambda) = \dim_K \text{Eig}(M, \lambda)$.

Anleitung: Matrizen diagonalisieren

Sei $A \in \mathcal{M}_n(K)$ eine Matrix.

- (1) Prüfe, ob die Bedingung (3) aus Satz 4.5 erfüllt ist.
- (2) Bestimme Basen aller Eigenräume.
- (3) Schreibe die Vektoren dieser Basen als Spalten in eine Matrix T . Dann hat $T^{-1}AT$ Diagonalgestalt.

Aufgabe (Frühjahr 2011, T1A1)

Sei $K := \mathbb{Q}(\sqrt[3]{5})$. Geben Sie eine Basis von K über \mathbb{Q} an und die Darstellungsmatrix des Endomorphismus

$$K \rightarrow K, \quad x \mapsto \sqrt[3]{5} \cdot x$$

bezüglich dieser Basis. Begründen Sie, warum diese Matrix über \mathbb{Q} nicht diagonalisierbar ist.

Lösungsvorschlag zur Aufgabe (Frühjahr 2011, T1A1)

Das Polynom $f = X^3 - 5$ ist normiert, irreduzibel über \mathbb{Q} nach dem Eisenstein-Kriterium und hat $\sqrt[3]{5}$ als Nullstelle. Folglich ist f das Minimalpolynom von $\sqrt[3]{5}$ über \mathbb{Q} , sodass $\dim_{\mathbb{Q}} K = [K : \mathbb{Q}] = 3$ gilt und eine \mathbb{Q} -Basis von K durch $\{1, \sqrt[3]{5}, \sqrt[3]{5}^2\}$ gegeben ist. Wegen

$$\begin{aligned}\sqrt[3]{5} \cdot 1 &= \sqrt[3]{5} = 0 \cdot 1 + 1 \cdot \sqrt[3]{5} + 0 \cdot \sqrt[3]{5}^2 \\ \sqrt[3]{5} \cdot \sqrt[3]{5} &= \sqrt[3]{5}^2 = 0 \cdot 1 + 0 \cdot \sqrt[3]{5} + 1 \cdot \sqrt[3]{5} \\ \sqrt[3]{5} \cdot \sqrt[3]{5}^2 &= 5 = 5 \cdot 1 + 0 \cdot \sqrt[3]{5} + 0 \cdot \sqrt[3]{5}^2\end{aligned}$$

ist die Darstellungsmatrix des angegebenen Endomorphismus

$$A = \begin{pmatrix} 0 & 0 & 5 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

Das charakteristische Polynom dieser Matrix ist f . Wie bereits erwähnt, ist f irreduzibel über \mathbb{Q} und zerfällt dort daher nicht in Linearfaktoren. Nach Satz 4.5 ist diese Matrix deshalb nicht diagonalisierbar über \mathbb{Q} .

Aufgabe (Herbst 2015, T3A3)

Betrachten Sie das Polynom $f(X) = X^2 + X + 1 \in \mathbb{F}_5[X]$.

- a** Zeigen Sie, dass $K := \mathbb{F}_5/(f(X))$ ein Körper mit 25 Elementen ist.
- b** Bestimmen Sie ein Element $w \in K$, mit $w^2 = 2$.
- c** Zeigen Sie, dass die Matrix

$$A := \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \in M(2 \times 2, \mathbb{F}_5)$$

über K diagonalisierbar ist.

Lösungsvorschlag zur Aufgabe (Herbst 2015, T3A3)

- a** Sei α eine Nullstelle von f in einem algebraischen Abschluss $\overline{\mathbb{F}_5}$. Dann hat der Einsetzungshomomorphismus

$$\phi: \mathbb{F}_5[X] \rightarrow \mathbb{F}_5[\alpha], \quad g(X) \mapsto g(\alpha)$$

Kern $\ker \phi = (f) \subseteq \mathbb{F}_5[X]$: Die Inklusion „ \supseteq “ ist klar, sei daher $g \in \ker \phi$. Man überzeugt sich schnell davon, dass f keine Nullstelle in \mathbb{F}_5 besitzt. Wegen $\deg f = 2$ ist daher f irreduzibel über \mathbb{F}_5 . Da f normiert ist, handelt es sich bei f um das Minimalpolynom von α über \mathbb{F}_5 . Nun haben wir vorausgesetzt, dass

$$\phi(g) = g(\alpha) = 0$$

ist. Es folgt $f \mid g$, d.h. $g \in (f)$. Aus dem Homomorphiesatz folgt, dass

$$K = \mathbb{F}_5[X]/(f) \cong \mathbb{F}_5[\alpha] = \mathbb{F}_5(\alpha)$$

ein Körper ist und wegen

$$[\mathbb{F}_5(\alpha) : \mathbb{F}_5] = \deg f = 2$$

handelt es sich bei K um einen zweidimensionalen \mathbb{F}_5 -Vektorraum. Also ist $K \cong \mathbb{F}_5^2$, weswegen $|K| = 5^2 = 25$ ist.

- b** Die Quadrate in \mathbb{F}_5 sind $0, 1$ und -1 , also gibt es kein solches Element w in \mathbb{F}_5 und wir müssen in K suchen.

Eine Basis von K als \mathbb{F}_5 -Vektorraum ist durch $\{1, \bar{X}\}$ gegeben. Es wird daher $a, b \in \mathbb{F}_5$ mit $w = a + b\bar{X}$ geben. Wir machen nun den Ansatz

$$\begin{aligned} 2 &= (a + b\bar{X})^2 \Leftrightarrow 2 = a^2 + 2ab\bar{X} + b^2\bar{X}^2 = \\ &= a^2 + 2ab\bar{X} + b^2(-\bar{X} - 1) = (a^2 - b^2) + (2ab - b^2)\bar{X}, \end{aligned}$$

wobei die Relation $f(\bar{X}) = 0$ verwendet wurde. Aus der linearen Unabhängigkeit von 1 und \bar{X} erhalten wir weiter die Gleichungen

$$2 = a^2 - b^2 \quad \text{und} \quad 0 = 2ab - b^2.$$

Aus der zweiten Gleichung folgt $0 = b(2a - b)$. Da K ein Integritätsbereich ist, muss $b = 0$ oder $2a - b = 0$ sein. Ersteres würde bedeuten, dass $2 = a^2$, doch so ein Element a gibt es – wie eingangs bemerkt – in \mathbb{F}_5 nicht. Also muss $2a - b = 0 \Leftrightarrow b = 2a$ gelten.

Die Quadrate in \mathbb{F}_5 sind $0, 1$ und -1 , die einzige Kombination dieser Zahlen, die $2 = a^2 - b^2$ erfüllt, ist

$$a^2 = 1 \quad \Rightarrow \quad a \in \{1, -1\} \quad \text{und} \quad b^2 = -1 \quad \Rightarrow \quad b \in \{2, 3\}.$$

Wir erhalten somit unter Berücksichtigung der Bedingung $b = 2a$ die beiden Lösungen $(a, b) \in \{(1, 2), (-1, 3)\}$. Tatsächlich gilt

$$(1 + 2\bar{X})^2 = 1 + 4\bar{X} + 4\bar{X}^2 = -3 + 4(1 + \bar{X} + \bar{X}^2) = 2 + 4f(\bar{X}) = 2$$

$$(-1 + 3\bar{X})^2 = (-1 - 2\bar{X})^2 = (-1)^2 \cdot (1 + 2\bar{X})^2 = 2$$

c Wir berechnen zunächst das charakteristische Polynom von A :

$$\begin{aligned}\chi_A &= \det(A - X\mathbb{E}_2) = \det \begin{pmatrix} 1-X & 2 \\ 3 & 4-X \end{pmatrix} = (1-X)(4-X) - 6 = \\ &= X^2 - (1+4)X + 4 - 1 = X^2 + 3\end{aligned}$$

Für das Element w aus Teil **a** gilt

$$\chi_A(w) = w^2 + 3 = 5 = 0,$$

also ist $\chi_A = (X - w)(X + w)$. Somit zerfällt das charakteristische Polynom von A über K in Linearfaktoren. Die algebraische Vielfachheit der beiden Eigenwerte ist 1 und da nach Lemma 4.4 (2) die geometrische Vielfachheit kleiner gleich der algebraischen Vielfachheit ist, muss auch diese 1 sein. Insgesamt sind damit die Voraussetzungen von Satz 4.5 erfüllt und A ist diagonalisierbar über K .

4.3. Jordan-Normalform

Die Bedingungen aus Satz 4.5 für Diagonalisierbarkeit bedeuten eine tatsächliche Einschränkung und sind im Allgemeinen nicht erfüllt. Wir entwickeln daher nun die Theorie einer allgemeineren Normalform, die bereits unter schwächeren Voraussetzungen angenommen werden kann.

Sei K ein Körper. Es ist $\mathcal{M}_n(K) \cong K^{n^2}$ ein K -Vektorraum der Dimension n^2 . Dies bedeutet, dass für eine Matrix $A \in \mathcal{M}_n(K)$ die Potenzen $A^0 = \mathbb{E}_n, A^1, \dots, A^{n^2}$ linear abhängig sein müssen. Es gibt folglich $a_0, \dots, a_{n^2-1} \in K$, sodass

$$A^{n^2} + a_{n^2-1}A^{n^2-1} + \dots + a_1A + a_0\mathbb{E}_n = 0$$

gilt. Betrachte dazu den Einsetzungshomomorphismus

$$\varphi_A: K[X] \rightarrow \mathcal{M}_n(K), \quad f = \sum_{i=0}^m a_i X^i \mapsto f(A) = \sum_{i=0}^m a_i A^i,$$

dann haben wir eben $\ker \varphi_A \neq 0$ gesehen. Es handelt sich bei $\ker \varphi_A \subseteq K[X]$ um ein Ideal und da $K[X]$ ein euklidischer Ring und somit ein Hauptidealring ist, gibt

es ein eindeutig bestimmtes normiertes Polynom minimalen Grades $\mu_A \in K[X]$, sodass $(\mu_A) = \ker \varphi_A$. Dieses Polynom heißt **Minimalpolynom** von A .

Im Gegensatz zum aus der Körpertheorie bekannten Minimalpolynom eines algebraischen Elements ist das Minimalpolynom einer Matrix im Allgemeinen *nicht* irreduzibel. Es gibt jedoch eine Verbindung der beiden Begriffe: Ist $L|K$ eine endliche Körpererweiterung und $a \in L$, so ist das Minimalpolynom des K -Vektorraumhomomorphismus $L \rightarrow L, x \mapsto ax$ (bzw. dessen Darstellungsmatrix in unserer Definition) genau das Körpertheoretische Minimalpolynom von a über K (vgl. dazu auch F11T1A1).

Satz 4.6 (Cayley-Hamilton). Sei $n \in \mathbb{N}$, K ein Körper und sei $A \in \mathcal{M}_n(K)$ mit charakteristischem Polynom χ_A und Minimalpolynom μ_A . Dann gilt $\chi_A(A) = 0$, d. h. $\mu_A | \chi_A$.

Wir versuchen nun, den Zusammenhang zur bisherigen Theorie herzustellen. Sei $\mu_A = \sum_{i=0}^m a_i X^i \in K[X]$ das Minimalpolynom von A . Wegen $\mu_A | \chi_A$ ist jede Nullstelle $\lambda \in K$ von μ_A eine Nullstelle von χ_A , d. h. λ ist ein Eigenwert von A . Ist umgekehrt $\lambda \in K$ ein Eigenwert von A und v ein zugehöriger Eigenvektor, so gilt

$$0 = \mu_A(A)v = \left(\sum_{i=0}^m a_i A^i \right) v = \sum_{i=0}^m a_i A^i v = \sum_{i=0}^m a_i \lambda^i = \mu_A(\lambda),$$

also ist λ eine Nullstelle von μ_A . Wir haben also gezeigt:

$$\lambda \in K \text{ ist Eigenwert von } A \Leftrightarrow \mu_A(\lambda) = 0$$

Aufgabe (Herbst 2010, T2A5)

Sei $A \in \mathcal{M}_{n,n}(\mathbb{Z})$ eine ganzzahlige $n \times n$ -Matrix mit $A^p = E$ für eine Primzahl p und $n \in \mathbb{N}$. Zeigen Sie, dass $\det(A - E)$ ganzzahlig und durch p teilbar ist. (E bezeichnet die Einheitsmatrix.)

Lösungsvorschlag zur Aufgabe (Herbst 2010, T2A5)

Dass $\det(A - E)$ ganzzahlig ist, ist klar, denn die Determinante ist ein Polynom in den Koeffizienten von $A - E$ und diese sind nach Voraussetzung ganzzahlig.

Betrachten wir zunächst den Fall, dass 1 ein Eigenwert von A ist. In diesem Fall ist 1 eine Nullstelle des charakteristischen Polynoms χ_A , sodass

$$\det(A - E) = \chi_A(1) = 0$$

auf jeden Fall durch p teilbar ist. Setzen wir daher nun voraus, dass 1 kein Eigenwert von A ist. Aus der Voraussetzung $A^p = E$ folgt, dass $A^p - E = 0$, d. h. A ist Nullstelle des Polynoms $X^p - 1$. Das Minimalpolynom μ_A von A

ist somit ein Teiler von $X^p - 1$. Die Zerlegung in irreduzible Faktoren von $X^p - 1$ über \mathbb{Z} ist nach Satz 3.17

$$X^p - 1 = \prod_{m|p} \Phi_m = \Phi_1 \cdot \Phi_p = (X - 1) \cdot (X^{p-1} + \dots + X + 1),$$

wobei Φ_m jeweils das m -te Kreisteilungspolynom bezeichnet. Nach Annahme ist 1 kein Eigenwert von A , sodass $\mu_A(1) \neq 0$. Also ist $X - 1$ kein Teiler von μ_A und es muss $\mu_A = \Phi_p$ gelten. Nach dem Satz von Cayley-Hamilton 4.6 ist μ_A ein Teiler von χ_A , d.h. es gibt ein Polynom $g \in \mathbb{Q}[X]$ mit $\chi_A = g \cdot \mu_A$. Da χ_A und μ_A beides primitive Polynome sind, folgt aus dem Lemma von Gauß sogar $g \in \mathbb{Z}[X]$ (vgl. hierzu Lemma 2.24). Also haben wir auch in \mathbb{Z} die Gleichung

$$\begin{aligned} \det(A - E) &= \chi_A(1) = g(1) \cdot \mu_A(1) = g(1) \cdot \Phi_p(1) = \\ &= g(1) \cdot (1^{p-1} + \dots + 1^1 + 1) = g(1) \cdot p. \end{aligned}$$

Also wird $\det(A - E)$ von p geteilt.

Aufgabe (Herbst 2005, T3A3)

Geben Sie alle Lösungen X der Gleichung

$$X^7 = \mathbb{1}_5$$

in der Gruppe $\mathrm{GL}_5(\mathbb{Q})$ an (mit Begründung).

Lösungsvorschlag zur Aufgabe (Herbst 2005, T3A3)

Sei $A \in \mathrm{GL}_5(\mathbb{Q})$ eine Lösung der angegebenen Gleichung. Dann ist $A^7 - \mathbb{E}_5 = 0$, d.h. das Minimalpolynom μ_A von A ist ein Teiler von $X^7 - 1$. Nun ist die Zerlegung dieses Polynoms in über $\mathbb{Q}[X]$ irreduzible Faktoren durch

$$X^7 - 1 = \prod_{n|7} \Phi_n = \Phi_1 \cdot \Phi_7 = (X - 1) \cdot (X^6 + X^5 + X^4 + X^3 + X^2 + X + 1)$$

gegeben, wobei Φ_n jeweils das n -te Kreisteilungspolynom bezeichnet. Damit ist

$$\mu_A \in \{(X - 1), \Phi_7, X^7 - 1\}.$$

Da μ_A nach dem Satz von Cayley-Hamilton 4.6 das charakteristische Polynom teilt, ist $\deg \mu_A \leq \deg \chi_A$. Weil $A \in \mathrm{GL}_5(\mathbb{Q})$ eine (5×5) -Matrix ist, hat χ_A den Grad 5. Somit kann nur $\mu_A = X - 1$ sein. Es folgt

$$0 = \mu_A(A) = A - \mathbb{E}_5 \Leftrightarrow A = \mathbb{E}_5.$$

Sei $\mu_A = \prod_{i=0}^m (X - \lambda_i)^{n_i}$ eine Zerlegung von μ_A über $K[X]$ mit paarweise verschiedenen Eigenwerten $\lambda_i \in K$ für $i \in \{1, \dots, m\}$. Nach Definition ist $\mu_A(A)$ die Nullmatrix, d. h. $\ker \mu_A = K^n$. Man kann nun weiter zeigen, dass

$$K^n = \ker \mu_A(A) = \bigoplus_{i=0}^m \ker(A - \lambda_i \mathbb{E}_n)^{n_i}.$$

Sind alle $n_i = 1$, so entspricht dies genau einer Zerlegung in Eigenräume. Wir haben also gezeigt:

Proposition 4.7. Sei K ein Körper, $n \in \mathbb{N}$ und $M \in \mathcal{M}_n(K)$. Dann sind die folgenden Aussagen gleichwertig:

- (1) A ist diagonalisierbar,
- (2) das Minimalpolynom μ_A von A zerfällt in Linearfaktoren und hat nur einfache Nullstellen.

Aufgabe (Frühjahr 2012, T3A1)

In der Gruppe $G := \mathrm{GL}_4(\mathbb{C})$ betrachten wir die Teilmenge

$$M := \left\{ B \in \mathrm{GL}_4(\mathbb{C}) \mid B^2 = \mathbb{E}_4 \right\}.$$

- a** Zeigen Sie, dass alle Matrizen $B \in M$ diagonalisierbar sind.
- b** Zeigen Sie, dass die Operation $G \times M \rightarrow M$, $(A, B) \mapsto ABA^{-1}$ von G auf M durch Konjugation wohldefiniert ist und die Menge M in genau 5 disjunkte Bahnen zerlegt.

Lösungsvorschlag zur Aufgabe (Frühjahr 2012, T3A1)

- a** Sei $B \in M$. Wegen $B^2 - \mathbb{E}_4 = 0$ ist das Minimalpolynom μ_B ein Teiler von $X^2 - 1 = (X - 1)(X + 1)$. Insbesondere hat μ_B nur einfache Nullstellen und zerfällt in Linearfaktoren. Nach Proposition 4.7 ist B daher diagonalisierbar.

- b** *Wohldefiniertheit:* Zu zeigen ist, dass $A \cdot B \in M$ für $A \in G, B \in M$. Es gilt

$$(A \cdot B)^2 = (ABA^{-1})^2 = ABA^{-1}ABA^{-1} = AB^2A^{-1} = A\mathbb{E}_4A^{-1} = \mathbb{E}_4$$

und somit $A \cdot B \in M$. Dass es sich bei der Abbildung um eine Operation handelt, ist klar.

Bahnen: Die Bahnen der Operation sind genau die Mengen (Äquivalenzklassen) aller Matrizen, die jeweils zueinander ähnlich sind. Nach Teil **a**

ist jede Matrix B aus M diagonalisierbar und wegen $\mu_B|(X^2 - 1)$ kann B nur die Eigenwerte 1 oder -1 haben. Damit ist B zu einer der Matrizen aus

$$R = \left\{ \mathbb{E}_4, \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \right. \\ \left. \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \right\}$$

ähnlich. Diese Matrizen sind jedoch nicht zueinander ähnlich, da sie verschiedene charakteristische Polynome haben. Also ist R tatsächlich ein Repräsentantensystem der Bahnen.

Falls μ_A mehrfache Nullstellen hat, so tauchen in der Zerlegung des Vektorraums K^n von oben Räume der Form $\ker(A - \lambda_i \mathbb{E}_n)^{n_i}$ auf, welche wir als Nächstes in den Griff bekommen wollen.

Definition 4.8. Sei K ein Körper, $n \in \mathbb{N}$ und $M \in \mathcal{M}_n(K)$. Ist $\lambda \in K$ ein Eigenwert von A , so nennen wir

$$\text{Eig}^i(A, \lambda) = \ker(A - \lambda \mathbb{E}_n)^i$$

den *verallgemeinerten Eigenraum* i -ter Stufe von A zum Eigenwert λ .

Wir sind nun so weit, die Jordan-Normalform zu formulieren. Dabei ist ein *Jordankästchen* (auch *Jordanblock*) der Größe m zum Eigenwert λ eine Matrix der Form

$$J(\lambda, m) = \begin{pmatrix} \lambda & 1 & 0 & \cdots & 0 \\ 0 & \ddots & & \ddots & \vdots \\ \vdots & \ddots & & & 0 \\ \vdots & & \ddots & & 1 \\ 0 & \cdots & \cdots & 0 & \lambda \end{pmatrix} \in \mathcal{M}_m(K)$$

und man sagt, eine Matrix A liegt in *Jordan-Normalform* vor, falls A die Form

$$A = \begin{pmatrix} J(\lambda_1, m_1) & & 0 \\ & \ddots & \\ 0 & & J(\lambda_r, m_r) \end{pmatrix}$$

besitzt.

Satz 4.9. Sei $A \in \mathcal{M}_n(K)$ eine Matrix, deren charakteristisches Polynom in Linearfaktoren zerfällt. Dann ist A ähnlich zu einer Matrix in Jordan-Normalform.

Proposition 4.10. Sei $A \in \mathcal{M}_n(K)$ eine Matrix, deren charakteristisches Polynom in Linearfaktoren zerfällt und $T \in \mathrm{GL}_n(K)$ eine Matrix, sodass $B = T^{-1}AT$ in Jordan-Normalform ist.

- (1) Die Zahl der Jordankästchen zum Eigenwert λ in B entspricht $\dim_K \mathrm{Eig}(A, \lambda)$.
- (2) Die Größe des größten Jordankästchen zum Eigenwert λ in B entspricht der Vielfachheit der Nullstelle λ von μ_A .
- (3) Die Anzahl der Jordankästchen der Größe m zum Eigenwert λ in B ist

$$2 \dim_K \mathrm{Eig}^m(A, \lambda) - \dim_K \mathrm{Eig}^{m+1}(A, \lambda) - \dim_K \mathrm{Eig}^{m-1}(A, \lambda).$$

Aufgabe (Frühjahr 2010, T2A2)

- a** Sei G eine endliche Gruppe und sei H eine echte Untergruppe von G (d.h. $H \neq G$). Zeigen Sie:

$$G \neq \bigcup_{x \in G} xHx^{-1}.$$

- b** Sei $G := GL(2, \mathbb{C})$ die Gruppe der invertierbaren komplexen 2×2 -Matrizen und sei $H < G$ die Untergruppe der oberen Dreiecksmatrizen, d.h.

$$H := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G \mid c = 0 \right\}.$$

Zeigen Sie:

$$G = \bigcup_{x \in G} xHx^{-1}.$$

Lösungsvorschlag zur Aufgabe (Frühjahr 2010, T2A2)

- a** Betrachte für vorgegebenes $x \in G$ die Abbildung

$$\tau_x: G \rightarrow G, \quad g \mapsto gx.$$

Diese ist injektiv, denn sind $g, h \in G$ Elemente mit $\tau_x(g) = \tau_x(h)$, so gilt

$$\tau_x(g) = \tau_x(h) \Leftrightarrow gx = hx \Leftrightarrow gxx^{-1} = hxx^{-1} \Leftrightarrow g = h.$$

Außerdem ist τ_x surjektiv, denn ist $g \in G$ beliebig, so ist $\tau_x(gx^{-1}) = gx^{-1}x = g$. Dies bedeutet einerseits

$$|xHx^{-1}| = |\tau_x(xHx^{-1})| = |xH| = |H|$$

für beliebiges $x \in G$ und andererseits, dass τ_x eine Bijektion

$$\{xHx^{-1} | x \in G\} \rightarrow G/H, \quad xHx^{-1} \mapsto \tau_x(xHx^{-1}) = xH$$

induziert. Als Konsequenz gibt es genau $|G/H| = (G : H)$ verschiedene Untergruppen der Form xHx^{-1} . Diese Untergruppen sind jedoch nicht disjunkt, denn sie enthalten zumindest alle das Neutralelement $1 = x \cdot 1 \cdot x^{-1}$. Zählen wir also nur die *verschiedenen* Elemente in der Vereinigung, so kommen wir auf

$$\begin{aligned} \left| \bigcup_{x \in G} xHx^{-1} \right| &= |\{1\}| + \left| \bigcup_{x \in G} xHx^{-1} \setminus \{1\} \right| \leq 1 + (G : H) \cdot (|H| - 1) = \\ &= 1 + (G : H)|H| - (G : H) = |G| + 1 - (G : H). \end{aligned}$$

Da H eine echte Untergruppe ist, ist $|H| < |G|$ und somit $(G : H) = \frac{|G|}{|H|} > 1$. Eingesetzt in obige Abschätzung ergibt dies

$$\left| \bigcup_{x \in G} xHx^{-1} \right| \leq |G| + 1 - (G : H) < |G|.$$

Folglich kann unmöglich $G = \bigcup_{x \in G} xHx^{-1}$ gelten.

- b** Die Inklusion „ \supseteq “ ist klar, sei daher $A \in G$ beliebig vorgegeben. Da wir über \mathbb{C} arbeiten, zerfällt das charakteristische Polynom von A auf jeden Fall in Linearfaktoren. Nach 4.9 ist daher A ähnlich zu einer Matrix in Jordan-Normalform B , d. h. es gibt eine Matrix $T \in G$, sodass $B = T^{-1}AT$ in Jordan-Normalform ist. Insbesondere ist B eine obere Dreiecksmatrix, sodass

$$T^{-1}AT = B \Leftrightarrow A = TBT^{-1}.$$

Insbesondere also $A \in THT^{-1} \subseteq \bigcup_{x \in G} xHx^{-1}$.

Aufgabe (Frühjahr 2015, T1A1)

Sei \mathbb{F}_2 der endliche Körper mit genau zwei Elementen 0 und 1. Auf dem dreidimensionalen \mathbb{F}_2 -Vektorraum $(\mathbb{F}_2)^3$ betrachten wir den Endomorphismus

$$\phi: (\mathbb{F}_2)^3 \rightarrow (\mathbb{F}_2)^3, \quad (x_1, x_2, x_3) \mapsto (x_3, x_2, x_1).$$

- a** Bestimmen Sie das charakteristische Polynom von ϕ . Bestimmen Sie alle Eigenwerte von ϕ in \mathbb{F}_2 . Bestimmen Sie für jeden Eigenwert von ϕ in \mathbb{F}_2 eine Basis des zugehörigen Eigenraums.
- b** Gibt es eine Basis von $(\mathbb{F}_2)^3$, bezüglich derer ϕ eine Jordan'sche Normalform hat? Begründen Sie Ihre Antwort. Wenn ja, bestimmen Sie die Jordan'sche Normalform von ϕ .

Lösungsvorschlag zur Aufgabe (Frühjahr 2015, T1A1)

- a** Die Darstellungsmatrix von ϕ bezüglich der Standardbasis $B = \{(1, 0, 0), (0, 1, 0), (0, 0, 1)\}$ ist

$$[\phi]_B = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}.$$

Somit berechnet sich das charakteristische Polynom von ϕ zu

$$\begin{aligned} \chi_\phi &= \det \begin{pmatrix} -X & 0 & 1 \\ 0 & 1-X & 0 \\ 1 & 0 & -X \end{pmatrix} = X^2(1-X) - (1-X) = \\ &= (1-X)(X^2-1) = (X-1)(X-1)^2 = (X-1)^3. \end{aligned}$$

Also hat ϕ nur den Eigenwert 1 in \mathbb{F}_2 . Der zugehörige Eigenraum ist

$$\text{Eig}(\phi, 1) = \ker(\phi - \text{id}_{\mathbb{F}_2^3}) = \ker \begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 1 \end{pmatrix} = \left\langle \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \right\rangle.$$

- b** Da χ_ϕ nach Teil **a** in Linearfaktoren zerfällt, ist $[\phi]_B$ nach Satz 4.9 zu einer Matrix in Jordan-Normalform ähnlich, d. h. es gibt eine Basis B' von \mathbb{F}_2^3 , bezüglich der ϕ Jordan-Normalform hat.

Wegen $\dim \text{Eig}(\phi, 1) = 2$ gibt es nach Proposition 4.10 (1) zwei Jordankästchen in $[\phi]_{B'}$. Die einzige Möglichkeit ist also, dass $[\phi]_{B'}$ ein Jordankästchen der Größe 1 und eines der Größe 2 hat. Somit ist

$$[\phi]_{B'} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

bis auf Vertauschung der beiden Jordankästchen.

Aufgabe (Herbst 2014, T2A5)

Die reelle (6×6) -Matrix A habe den sechsfachen Eigenwert 1 mit der geometrischen Vielfachheit 3. Es gelte weiterhin $A = E_6 + N$ mit der Einheitsmatrix E_6 und einer nilpotenten Matrix N mit Nilpotenzindex 3, d.h. $N^3 = 0$, aber $N^2 \neq 0$. Bestimmen Sie die Jordan-Normalform von A .

Lösungsvorschlag zur Aufgabe (Herbst 2014, T2A5)

Laut Angabe ist das charakteristische Polynom $\chi_A = (X - 1)^6$, sodass auch das Minimalpolynom von A eine Potenz von $(X - 1)$ sein muss. Weiter ist

$$(A - \mathbb{E}_6)^3 = N^3 = 0 \quad \text{und} \quad (A - \mathbb{E}_6)^2 = N^2 \neq 0,$$

d.h. das Minimalpolynom von A ist $\mu_A = (X - 1)^3$ und das größte Jordankästchen von A hat nach Proposition 4.10 (2) Größe 3. Weiter hat der Eigenwert 1 laut Angabe die geometrische Vielfachheit 3, es gibt also 3 Jordankästchen. Da A eine (6×6) -Matrix ist, muss es jeweils ein Jordankästchen der Größe 3, 2 und 1 geben. Wir erhalten somit

$$A \sim \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Aufgabe (Herbst 2013, T1A3)

Sei $A = \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$ eine Matrix über den komplexen Zahlen, hierbei gelte $\lambda \neq 0$. Man zeige, dass für alle $k \geq 1$ die Matrix A^k die Jordansche Normalform $\begin{pmatrix} \lambda^k & 1 \\ 0 & \lambda^k \end{pmatrix}$ hat.

Lösungsvorschlag zur Aufgabe (Herbst 2013, T1A3)

Wir zeigen zunächst per Induktion über k , dass

$$A^k = \begin{pmatrix} \lambda^k & k\lambda^{k-1} \\ 0 & \lambda^k \end{pmatrix} \quad \text{für alle } k \in \mathbb{N}$$

gilt. Im Fall $k = 1$ ist die Behauptung erfüllt. Setzen wir die Aussage daher für ein k als bereits bewiesen voraus. Dann ist

$$A^{k+1} = A^k \cdot A = \begin{pmatrix} \lambda^k & k\lambda^{k-1} \\ 0 & \lambda^k \end{pmatrix} \cdot \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix} = \begin{pmatrix} \lambda^{k+1} & (k+1)\lambda^k \\ 0 & \lambda^{k+1} \end{pmatrix}.$$

Dies schließt den Induktionsbeweis ab. Nun ist das charakteristische Polynom von A^k gegeben durch

$$\chi_{A^k} = \det(A^k - X\mathbb{E}_2) = (\lambda^k - X)^2 = (X - \lambda^k)^2,$$

sodass λ^k der einzige Eigenwert von A^k ist. Wegen $\lambda \neq 0$ ist

$$A^k - \lambda^k \mathbb{E}_2 = \begin{pmatrix} 0 & k\lambda^{k-1} \\ 0 & 0 \end{pmatrix} \neq 0$$

und damit ist χ_{A^k} gleichzeitig auch das Minimalpolynom von A^k . Nach 4.10 hat die Jordan-Normalform von A^k ein Jordankästchen der Größe 2 zum Eigenwert λ^k . Da A^k eine (2×2) -Matrix ist, entspricht dies bereits der Jordan-Normalform. Wir haben damit

$$A^k \sim \begin{pmatrix} \lambda^k & 1 \\ 0 & \lambda^k \end{pmatrix} \quad \text{gezeigt.}$$

Anleitung: Bestimmung der Jordan-Normalform

Sei K ein Körper und $A \in \mathcal{M}_n(K)$ eine Matrix. Gesucht ist eine Basis B , sodass A bezüglich B Jordan-Normalform hat. Interessanterweise ist dieser Basiswechsel nie in den Algebra-Aufgaben verlangt, aber bisweilen beim Lösen Linearer Differentialgleichungen vonnöten.

- (1) Prüfe, ob das charakteristische Polynom von A in Linearfaktoren zerfällt. In diesem Fall kann A nach Satz 4.9 auf Jordan-Normalform gebracht werden.
- (2) Bestimme die Jordan-Normalform mittels 4.10, also zu jedem der (nicht unbedingt verschiedenen) Eigenwerte $\lambda_1, \dots, \lambda_m$ die Anzahl $s(\lambda_i)$ der zugehörigen Jordankästchen sowie deren jeweilige Größe $k_j(\lambda_i)$ d.
- (3) Man frühstückt die Jordankästchen nun der Reihe nach ab. Wähle für das erste Kästchen einen Vektor $v_{k_1(\lambda_1)} \in \text{Eig}^{k_1(\lambda_1)}(\lambda_1) \setminus \text{Eig}^{k_1(\lambda_1)-1}(\lambda_1)$.
- (4) Man arbeitet rückwärts, indem man $v_{k_1(\lambda_1)-s} = (A - \lambda_1 \mathbb{E}_n)v_{k_1(\lambda_1)-s+1}$ für $s \in \{1, \dots, k_1(\lambda_1) - 1\}$ setzt.

- (5) Verfahre in der gleichen Weise mit den anderen Jordankästchen zum Eigenwert λ_1 , d.h. wähle einen Vektor $v_{k_1(\lambda_1)+k_2(\lambda_1)}$ aus $\text{Eig}^{k_1(\lambda_1)}(A, \lambda_1) \setminus \langle \text{Eig}^{k_1(\lambda_1)-1}(A, \lambda_1), M \rangle$, wobei M die Menge der schon bestimmten Vektoren ist und setze dann $v_{k_1(\lambda_1)+k_2(\lambda_1)-s} = (A - \lambda_1 \mathbb{E}_n)v_{k_2(\lambda_1)-s+1}$ für $s \in \{1, \dots, k_2(\lambda_1) - 1\}$ usw.
- (6) Gehe zum nächsten Eigenwert, indem (3)-(5) für den neuen Eigenwert durchgeführt werden.
- (7) Schreibe die Vektoren v_1, \dots, v_n als Spalten in die Transformationsmatrix T . Die Matrix $T^{-1}AT$ ist dann in Jordan-Normalform.

Beispiel 4.11. Zur Illustration der oben beschriebenen Vorgehensweise bestimmen wir die Jordan-Normalform samt Transformationsmatrizen für die Matrix

$$A = \begin{pmatrix} -1 & 1 & -1 \\ 0 & 0 & -1 \\ 1 & -1 & -1 \end{pmatrix}.$$

Diese Matrix taucht in der Aufgabe F16T3A5 des Analysis Examens (Seite 621) auf und muss dort auf Jordan-Normalform gebracht werden, um e^{tA} berechnen zu können.

(1): Zunächst bestimmen wir das charakteristische Polynom von A :

$$\begin{aligned} \chi_A &= \det \begin{pmatrix} -1 - X & 1 & -1 \\ 0 & -X & -1 \\ 1 & -1 & -1 - X \end{pmatrix} = -X(1 + X)^2 - 1 - X + (1 + X) = \\ &= -X(X + 1)^2 \end{aligned}$$

Die Eigenwerte sind also 0 und -1 , außerdem zerfällt das charakteristische Polynom in Linearfaktoren, sodass die Matrix A zu einer Matrix in Jordan-Normalform ähnlich ist.

(2): Der Eigenwert 0 hat algebraische Vielfachheit 1 und damit nach Lemma 4.4 (2) auch geometrische Vielfachheit 1. Das heißt, dass es einen Jordanblock der Größe 1 zum Eigenwert 0 gibt. Um zu bestimmen, wie viele Jordanblöcke es zum Eigenwert -1 gibt, berechnen wir den zugehörigen Eigenraum:

$$\text{Eig}(A, -1) = \ker \begin{pmatrix} 0 & 1 & -1 \\ 0 & 1 & -1 \\ 1 & -1 & 0 \end{pmatrix} = \ker \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & -1 \\ 1 & -1 & 0 \end{pmatrix} = \left\langle \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \right\rangle$$

Also hat $\text{Eig}(A, -1)$ Dimension 1, sodass es einen Jordanblock zum Eigenwert -1 gibt. Dieser muss dann notwendigerweise die Größe 2 haben. Wir erwarten also, dass A zur Matrix

$$\begin{pmatrix} -1 & 1 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

ähnlich ist.

(3): Der Jordanblock zum Eigenwert -1 hat Größe 2, daher müssen wir einen Vektor $v_2 \in \text{Eig}^2(A, -1) \setminus \text{Eig}(A, -1)$ wählen. Dazu berechnen wir zunächst:

$$\text{Eig}^2(A, -1) = \ker \begin{pmatrix} 0 & 1 & -1 \\ 0 & 1 & -1 \\ 1 & -1 & 0 \end{pmatrix}^2 = \ker \begin{pmatrix} -1 & 2 & -1 \\ -1 & 2 & -1 \\ 0 & 0 & 0 \end{pmatrix} = \left\langle \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix} \right\rangle$$

Setze also $v_2 = (1, 0, -1)$.

(4) Den Vektor v_1 berechnet man folgendermaßen:

$$v_1 = (A - (-1)\mathbb{E}_3)v_2 = \begin{pmatrix} 0 & 1 & -1 \\ 0 & 1 & -1 \\ 1 & -1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$$

(5) Dieser Schritt entfällt, da es nur einen Jordanblock zum Eigenwert -1 gibt.

(6): Für den Jordanblock zum Eigenwert 0 brauchen wir noch einen entsprechenden Eigenvektor, also Vektor aus dem Kern:

$$\begin{aligned} \ker A &= \ker \begin{pmatrix} -1 & 1 & -1 \\ 0 & 0 & -1 \\ 1 & -1 & -1 \end{pmatrix} = \ker \begin{pmatrix} -1 & 1 & -1 \\ 0 & 0 & 1 \\ 0 & 0 & -2 \end{pmatrix} = \\ &= \ker \begin{pmatrix} -1 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} = \left\langle \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \right\rangle \end{aligned}$$

Setze also $v_3 = (1, 1, 0)$.

(7) Die Transformationsmatrix mit ihrer Inversen lautet in unserem Fall nun

$$T = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & -1 & 0 \end{pmatrix} \quad T^{-1} = \begin{pmatrix} 1 & -1 & 1 \\ 1 & -1 & 0 \\ -1 & 2 & -1 \end{pmatrix}.$$

■

5. Analysis reeller Variablen

5.1. Analysis einer reellen Variablen

Wir erinnern an beiden wichtigsten Begriffe der Analysis einer reellen Variablen:

Definition 5.1. Sei $U \subseteq \mathbb{R}$ und $f: U \rightarrow \mathbb{R}$ eine Abbildung.

- (1) Die Funktion f heißt *stetig* in $a \in U$, wenn für jede Folge $(x_n)_{n \in \mathbb{N}}$ in U mit $\lim_{n \rightarrow \infty} x_n = a$ auch $\lim_{n \rightarrow \infty} f(x_n) = f(a)$ gilt.
- (2) Die Funktion f heißt *differenzierbar* in $a \in U$, wenn der Grenzwert

$$\lim_{h \rightarrow 0} \frac{f(a+h) - f(a)}{h}$$

existiert. Ist dies der Fall, so bezeichnen wir ihn als Ableitung $f'(a)$.

Zu der folgenden Definition der Konvergenz von Funktionenfolgen sei auch auf den entsprechenden Abschnitt im Teil zur Funktionentheorie verweisen (vgl. Seite 287).

Definition 5.2. Sei $U \subseteq \mathbb{R}$ und $(f_n)_{n \in \mathbb{N}}$ eine Folge von Funktionen $f_n: U \rightarrow \mathbb{R}$.

- (1) Man sagt, f_n konvergiert punktweise gegen die Funktion $f: U \rightarrow \mathbb{R}$, wenn es für jedes $x \in U$ und jedes $\varepsilon > 0$ ein $N \in \mathbb{N}$ gibt, sodass

$$|f_n(x) - f(x)| < \varepsilon \quad \text{für alle } n \geq N \text{ gilt.}$$

- (2) Die Folge f_n heißt gleichmäßig konvergent, wenn es für jedes $\varepsilon > 0$ ein $N \in \mathbb{N}$ gibt, sodass

$$|f_n(x) - f(x)| < \varepsilon \quad \text{für alle } n \geq N \text{ und } x \in U \text{ gilt.}$$

Der Unterschied der beiden Arten von Konvergenz besteht also darin, dass bei (1) N von x abhängen darf, während bei (2) die Ungleichung für alle $x \in U$ gelten muss. Diese Definitionen übertragen sich direkt auf komplexwertige Funktionenfolgen.

Eine wichtige Aussage in Verbindung mit Funktionenfolgen ist, dass sich bei gleichmäßig konvergenten Folgen Integration und Grenzwertbildung vertauschen lassen, d. h. es gilt für $a, b \in U$ und integrierbare f_n die Gleichung

$$\lim_{n \rightarrow \infty} \int_a^b f_n(x) dx = \int_a^b \lim_{n \rightarrow \infty} f_n(x) dx = \int_a^b f(x) dx.$$

Falls die f_n jeweils stetig sind und gleichmäßig gegen f konvergieren, so muss außerdem f ebenfalls stetig sein.

Aufgabe (Herbst 2010, T1A1)

Finden Sie heraus, ob die folgenden Aussagen über $f: [0, 1] \rightarrow \mathbb{R}$ wahr oder falsch sind. Bei wahren Aussagen geben Sie eine kurze Begründung, bei falschen Aussagen ein Gegenbeispiel an:

- a** Ist f differenzierbar, so ist f' stetig.
- b** Ist f differenzierbar, so ist f' beschränkt.
- c** Ist f stetig, so nimmt f auf jedem abgeschlossenen Teilintervall $[a, b] \subseteq [0, 1]$ alle Werte zwischen $f(a)$ und $f(b)$ an.
- d** Nimmt f auf jedem abgeschlossenen Teilintervall $[a, b] \subseteq [0, 1]$ alle Werte zwischen $f(a)$ und $f(b)$ an, so ist f stetig.
- e** Ist f stetig, so besitzt f eine Stammfunktion.
- f** Ist f stetig, so ist f integrierbar.

Lösungsvorschlag zur Aufgabe (Herbst 2010, T1A1)

- a** Falsch. Ein Gegenbeispiel ist durch

$$f: [0, 1] \rightarrow \mathbb{R}, \quad x \mapsto \begin{cases} x^2 \sin\left(\frac{1}{x^2}\right), & \text{falls } x \neq 0 \\ 0 & \text{falls } x = 0 \end{cases}$$

gegeben. Wir bestimmen die Ableitung. Für $x > 0$ berechnet sich die Ableitung mittels Ketten- und Produktregel zu

$$2x \sin\left(\frac{1}{x^2}\right) + x^2 \cos\left(\frac{1}{x^2}\right) \frac{-2}{x^3} = 2x \sin\left(\frac{1}{x^2}\right) - \frac{2}{x} \cos\left(\frac{1}{x^2}\right).$$

Um zu zeigen, dass f im Ursprung differenzierbar ist, verwenden wir die Definition der Differenzierbarkeit sowie $|\sin x| \leq 1$ für alle $x \in \mathbb{R}$ und

erhalten

$$\begin{aligned}|f'(0)| &= \lim_{h \rightarrow 0} \left| \frac{f(h) - f(0)}{h} \right| = \lim_{h \rightarrow 0} \left| \frac{h^2 \sin\left(\frac{1}{h^2}\right)}{h} \right| = \\ &= \lim_{h \rightarrow 0} \left| h \sin\left(\frac{1}{h^2}\right) \right| \leq \lim_{h \rightarrow 0} |h| = 0.\end{aligned}$$

Damit ist f auf ganz $[0, 1]$ differenzierbar mit Ableitung

$$f'(x) = \begin{cases} 2x \sin\left(\frac{1}{x^2}\right) - \frac{2}{x} \cos\left(\frac{1}{x^2}\right), & \text{falls } x \neq 0 \\ 0, & \text{falls } x = 0. \end{cases}$$

Wir zeigen, dass f' in 0 nicht stetig ist: Betrachte dazu die Folge $(x_n)_{n \in \mathbb{N}}$ mit $x_n = \frac{1}{\sqrt{2\pi n}}$. Für diese gilt $\lim_{n \rightarrow \infty} x_n = 0$, aber wegen $x_n \neq 0$

$$\begin{aligned}\lim_{n \rightarrow \infty} f'(x_n) &= \lim_{n \rightarrow \infty} \left(\frac{2}{\sqrt{2\pi n}} \sin(2\pi n) - \frac{\sqrt{2\pi n}}{2} \cos(2\pi n) \right) = \\ &\quad \lim_{n \rightarrow \infty} \left(-\frac{\sqrt{2\pi n}}{2} \right) = -\infty,\end{aligned}$$

sodass f' in 0 nicht stetig ist.

- b** *Falsch.* Dies zeigt ebenso unser Beispiel aus Teil **a**.
- c** *Richtig.* Sei nämlich c ein Wert zwischen $f(a)$ und $f(b)$. Laut dem Zwischenwertsatz gibt es dann ein $\tilde{c} \in [a, b]$ mit $f(\tilde{c}) = c$.
- d** *Falsch.* Man überlegt zunächst, dass eine Funktion, die einen Sprungpunkt hat, die angegebene Eigenschaft (die man, wie wir im Folgenden, als *Zwischenwert-Eigenschaft* bezeichnet) nicht erfüllt, sodass wir eine etwas komplizierte Funktion betrachten müssen. Sei also

$$f: [0, 1] \rightarrow \mathbb{R}, \quad x \mapsto \begin{cases} \sin\left(\frac{1}{x}\right) & \text{falls } x \neq 0, \\ 0 & \text{falls } x = 0. \end{cases}$$

Für Intervalle I , die nicht 0 enthalten, ist die Einschränkung $f|_I$ als Verketzung stetiger Funktionen selbst stetig, sodass dort laut Teil **c** die Zwischenwert-Eigenschaft erfüllt ist. Für das Intervall $[0, 0] = \{0\}$ ist die Aussage klar. Sei nun $J = [0, b]$ ein Intervall und sei c ein Wert zwischen $f(0)$ und $f(b)$. Dann liegt dieser insbesondere im Intervall $[-1, 1]$. Betrachte nun die

Punkte $c_k = \frac{2}{4k\pi + \pi}$ und $d_k = \frac{2}{4k\pi - \pi}$. Wegen $\lim_{k \rightarrow \infty} c_k = \lim_{k \rightarrow \infty} d_k = 0$ können wir k so wählen, dass $c_k, d_k \in J$ gilt. Es gilt ferner für dieses k

$$f(c_k) = \sin\left(2k\pi + \frac{\pi}{2}\right) = 1 \quad \text{und} \quad f(d_k) = \sin\left(2k\pi - \frac{\pi}{2}\right) = -1.$$

Wiederum ist f wegen $c_k, d_k \neq 0$ auf dem Intervall $[c_k, d_k]$ stetig, sodass dort laut dem Zwischenwertsatz insbesondere der Wert c angenommen wird.

Jedoch ist die Funktion f nicht stetig. Das beweist schon die oben angeführte Folge c_k , für diese gilt nämlich

$$\lim_{k \rightarrow \infty} f(c_k) = \lim_{k \rightarrow \infty} 1 = 1 \neq 0 = f(0) = f\left(\lim_{k \rightarrow \infty} c_k\right).$$

e *Richtig.* Ist nämlich f stetig, so existiert die Integralfunktion

$$F: [0, 1] \rightarrow \mathbb{R}, \quad x \mapsto \int_0^x f(t) dt$$

und für diese gilt laut dem Hauptsatz der Differential- und Integralrechnung $F' = f$, sodass F eine Stammfunktion zu f ist.

f *Richtig.* Jede stetige Funktion, die auf einer beschränkten Menge definiert ist, ist integrierbar.

5.2. Analysis mehrerer reeller Variablen

Eine Ableitung für reellwertige Funktionen mehrerer Variablen lässt sich dadurch definieren, dass man die Funktion nur entlang einer Geraden betrachtet und so eine Funktion in einer reeller Variablen erhält, auf die dann Definition 5.1 angewendet werden kann. Die folgende Definition präzisiert dies.

Definition 5.3. Sei $n \in \mathbb{N}$, $U \subseteq \mathbb{R}^n$ eine offene Teilmenge, $a \in U$, $v \in \mathbb{R}^n$ und $f: U \rightarrow \mathbb{R}$ eine Funktion. Sei weiter $\phi: I \rightarrow \mathbb{R}^n$ definiert durch $\phi(t) = a + tv$ (wobei $I \subseteq \mathbb{R}$ so gewählt ist, dass $\phi(I) \subseteq U$). Ist die Verkettung $f \circ \phi$ in 0 differenzierbar, so bezeichnet man

$$\partial_v f(a) = (f \circ \phi)'(0) = \lim_{t \rightarrow 0} \frac{f(a + tv) - f(a)}{t}$$

als *Richtungsableitung* von f in Richtung v .

Im Fall, dass v ein Einheitsvektor ist, spricht man von den *partiellen Ableitungen*. Der Begriff der partiellen Ableitung entspricht nicht der natürlichen Verallgemeinerung der Differenzierbarkeit auf höhere Dimensionen: Im Eindimensionalen besteht die Grundidee der Differenzierbarkeit darin, Funktionen mittels ihrer Tangenten, also durch affin-lineare Funktionen, anzunähern. Die Definition der totalen Differenzierbarkeit verallgemeinert dies und liefert so einen Differenzierbarkeitsbegriff, der die gewohnten Eigenschaften aus der Analysis I besitzt. Beispielsweise ist jede total differenzierbare Funktion auch stetig, während dies auf eine überall partiell differenzierbare Funktion nicht zutreffen muss.

Definition 5.4. Seien $n, m \in \mathbb{N}$, $U \subseteq \mathbb{R}^n$ offen und $f: U \rightarrow \mathbb{R}^m$ eine Funktion. Man nennt f in $a \in U$ (total) differenzierbar, wenn es eine lineare Abbildung $L: \mathbb{R}^n \rightarrow \mathbb{R}^m$ und eine Abbildung $q: U_a = \{x \in \mathbb{R}^n \mid a + x \in U\} \rightarrow \mathbb{R}^m$ gibt, sodass für alle $h \in U_a$

$$f(a + h) = f(a) + L(h) + q(h) \quad \text{und} \quad \lim_{h \rightarrow 0} \frac{q(h)}{\|h\|} = 0$$

gilt. Die Abbildung L nennt man *Ableitung von f an der Stelle a* und bezeichnet sie mit $f'(a)$.

Die Ableitung einer differenzierbaren Funktion in mehreren Variablen wird üblicherweise in Form der Darstellungsmatrix der linearen Abbildung L angegeben. Diese hat die Gestalt

$$(Df)(a) = \begin{pmatrix} \partial_{x_1} f_1(a) & \dots & \partial_{x_n} f_1(a) \\ \vdots & \ddots & \vdots \\ \partial_{x_1} f_m(a) & \dots & \partial_{x_n} f_m(a) \end{pmatrix}.$$

Dabei bezeichnet $\partial_{x_i} f_j$ jeweils die partielle Ableitung der j -Komponentenfunktion von f nach der i -ten Variable. Bei reellwertigen Funktionen $f: U \rightarrow \mathbb{R}$ schreibt man die Jacobi-Matrix, die dann nur aus einer Zeile besteht, häufig auch als Spaltenvektor und bezeichnet diesen als den *Gradienten* ∇f von f .

Zwischen den partiellen Ableitungen und der totalen Differenzierbarkeit besteht folgender Zusammenhang:

Satz 5.5 (Schwarz). Sei $U \subseteq \mathbb{R}^n$ offen und $f: U \rightarrow \mathbb{R}$ eine Abbildung. Existieren die k -ten partiellen Ableitungen von f und sind diese stetig, so ist f eine k -mal total differenzierbare Abbildung und es gilt

$$\partial_{x_i} \partial_{x_j} f(a) = \partial_{x_j} \partial_{x_i} f(a) \quad \text{für } a \in U \text{ und } i, j \in \{1, \dots, n\}.$$

Ist $f: U \rightarrow \mathbb{R}$ eine zweimal stetig partiell differenzierbare Funktion, so definieren wir zusätzlich die **Hesse-Matrix** als

$$(\mathcal{H}f)(a) = \begin{pmatrix} \partial_{x_1} \partial_{x_1} f(a) & \dots & \partial_{x_1} \partial_{x_n} f(a) \\ \vdots & \ddots & \vdots \\ \partial_{x_n} \partial_{x_1} f(a) & \dots & \partial_{x_n} \partial_{x_n} f(a) \end{pmatrix}.$$

Eine Folgerung aus dem Satz von Schwarz ist, dass die Hesse-Matrix stets eine symmetrische Matrix ist.

Aufgabe (Herbst 2013, T1A3)

Sei $f: \mathbb{R}^2 \rightarrow \mathbb{R}$ definiert durch

$$f(x, y) := \begin{cases} 0 & \text{für } y \leq 0 \text{ oder } y \geq x^2, \\ 1 & \text{für } 0 < y < x^2. \end{cases}$$

Beweisen Sie, dass f in $(0, 0)$ unstetig ist, aber dort sämtliche Richtungsableitungen existieren.

Lösungsvorschlag zur Aufgabe (Herbst 2013, T1A3)

Unstetigkeit: Definiere die Folge $(x_n, y_n)_{n \in \mathbb{N}}$ durch $(x_n, y_n) = (\frac{1}{n}, \frac{1}{2n^2})$. Es gilt dann $\lim_{n \rightarrow \infty} (x_n, y_n) = (0, 0)$. Außerdem gilt für alle $n \in \mathbb{N}$ die Ungleichung $0 < \frac{1}{2n^2} < \frac{1}{n^2}$ und somit ist $f(x_n, y_n) = 1$ für alle $n \in \mathbb{N}$. Folglich ist

$$\lim_{n \rightarrow \infty} f(x_n, y_n) = \lim_{n \rightarrow \infty} 1 = 1 \neq 0 = f\left(\lim_{n \rightarrow \infty} (x_n, y_n)\right).$$

Dies beweist, dass f in $(0, 0)$ nicht stetig ist.

Existenz aller Richtungsableitungen: Sei $v = (v_x, v_y) \in \mathbb{R}^2$ ein Vektor. Wir unterscheiden drei Fälle.

1. Fall: $v_x = 0$. Für $t \in \mathbb{R}$ gilt hier entweder $tv_y \leq 0$ oder $tv_y > 0 = tv_x$, also $f(0, tv_y) = 0$ und damit

$$\lim_{t \rightarrow 0} \frac{f(tv_x, tv_y) - f(0, 0)}{t} = \lim_{t \rightarrow 0} \frac{f(0, tv_y)}{t} = \lim_{t \rightarrow 0} \frac{0}{t} = 0.$$

2. Fall: $v_y = 0$. Hier erhalten wir

$$\lim_{t \rightarrow 0} \frac{f(tv_x, tv_y) - f(0, 0)}{t} = \lim_{t \rightarrow 0} \frac{f(tv_x, 0)}{t} = \lim_{t \rightarrow 0} \frac{0}{t} = 0.$$

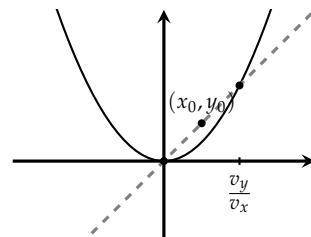
3. Fall: $v_x \neq 0, v_y \neq 0$. Die Abbildung $\phi(t) = t \cdot (v_x, v_y)$ definiert eine Gerade in \mathbb{R}^2 . Für Punkte $(x, y) \neq (0, 0)$ auf dieser Geraden gilt

$$\frac{y}{x} = \frac{tv_y}{tv_x} \Leftrightarrow y = \frac{v_y}{v_x} \cdot x$$

und auch für $(0, 0)$ ist diese Gleichung gültig. Wir berechnen die Schnittpunkte der Geraden mit $y = x^2$.

$$x^2 = \frac{v_y}{v_x} x \Leftrightarrow x \left(x - \frac{v_y}{v_x} \right) = 0 \Leftrightarrow x = 0 \quad \text{oder} \quad x = \frac{v_y}{v_x}$$

Nehmen wir zunächst an, dass $\frac{v_y}{v_x} > 0$. Betrachte nun den Punkt $x_0 = \frac{v_y}{2v_x}$. Einsetzen in die Geradengleichung liefert den y -Wert $y_0 = \frac{v_y^2}{2v_x^2}$. Zugleich ist $x_0^2 = \frac{v_y^2}{4v_x^2} < y_0$ und daher $f(x_0, y_0) = 0$. Da Gerade und Parabel stetig sind und keinen weiteren Schnittpunkt haben, folgt $y \geq x^2$ für alle $x \in]0; \frac{v_y}{v_x}[$.



Weiter gilt laut Definition von f aber auch im Fall $x \in]-\frac{v_y}{v_x}; 0]$, dass $f(x, y) = 0$. Für genügend kleines t gilt daher $f(tv_x, tv_y) = 0$ und es folgt

$$\lim_{t \rightarrow 0} \frac{f(tv_x, tv_y) - f(0, 0)}{t} = \lim_{t \rightarrow 0} \frac{0}{t} = 0.$$

Im Fall $\frac{v_y}{v_x} < 0$ verfährt man analog – hier ändern sich nur die zugehörigen Intervalle.

Damit haben wir schlussendlich gezeigt, dass alle Richtungsableitungen 0 sind, insbesondere also existieren.

Anleitung: Bestimmung lokaler Extrema

Gegeben sei eine zweimal differenzierbare Funktion $f: U \subseteq \mathbb{R}^n \rightarrow \mathbb{R}$, deren lokale Extremstellen gefunden werden sollen.

- (1) Berechne den Gradienten von f durch Bestimmung aller partiellen Ableitungen.
- (2) Berechne die *kritischen Punkte* von f . Dies sind diejenigen Punkte, an denen der Gradient mit dem Nullvektor übereinstimmt.

- (3) Berechne die Hesse-Matrix $(\mathcal{H}f)(a)$ für jeden kritischen Punkt $a \in U$ und bestimme ihre Definitheit:
- Ist $(\mathcal{H}f)(a)$ negativ definit, so handelt es sich um ein isoliertes lokales Maximum.
 - Ist $(\mathcal{H}f)(a)$ positiv definit, so handelt es sich um ein isoliertes lokales Minimum.
 - Ist $(\mathcal{H}f)(a)$ indefinit, so liegt ein Sattelpunkt (und damit kein Extremum) vor.

Zur Bestimmung der Definitheit der Hesse-Matrix ist folgender Zusammenhang hilfreich:

Proposition 5.6. Sei $A \in \mathcal{M}_n(\mathbb{R})$ eine symmetrische Matrix. Sind alle Eigenwerte von A positiv (bzw. negativ), so ist A positiv (bzw. negativ) definit. Existieren positive und negative Eigenwerte, so ist A indefinit.

Aufgabe (Frühjahr 2011, T3A5)

Sei

$$g: \mathbb{R}^2 \rightarrow \mathbb{R}, \quad g(x, y) = x^3 + 3xy^2 - 3xy$$

Bestimmen Sie alle kritischen Punkte von g und entscheiden Sie jeweils, ob es sich um ein (striktes) lokales Maximum oder Minimum oder um einen Sattelpunkt handelt.¹

Lösungsvorschlag zur Aufgabe (Frühjahr 2011, T3A5)

Wir berechnen zunächst den Gradienten von g :

$$(\nabla g)(x, y) = \begin{pmatrix} 3x^2 + 3y^2 - 3y \\ 6xy - 3x \end{pmatrix}$$

Die kritischen Punkte ergeben sich aus dem Gleichungssystem

$$\begin{aligned} 3x^2 + 3y^2 - 3y &= 0 \\ 6xy - 3x &= 0 \end{aligned} \Leftrightarrow \begin{aligned} 3x^2 + 3y^2 - 3y &= 0 \\ 3x(2y - 1) &= 0 \end{aligned}$$

Die zweite Gleichung liefert $x = 0$ oder $y = \frac{1}{2}$. Im ersten Fall ergibt sich

$$3y^2 - 3y = 0 \Leftrightarrow 3y(y - 1) = 0 \Leftrightarrow y = 0 \text{ oder } y = 1.$$

¹ Teil b der originalen Aufgabe beschäftigte sich mit der Stabilität von Ruhelagen in einem Differentialgleichungssystem. Wir haben an dieser Stelle darauf verzichtet.

Im zweiten erhalten wir

$$3x^2 + \frac{3}{4} - \frac{3}{2} = 0 \Leftrightarrow 3x^2 = \frac{3}{4} \Leftrightarrow x = \pm \frac{1}{2}.$$

Somit sind die kritischen Punkte $(0,0)$, $(0,1)$, $(\frac{1}{2}, \frac{1}{2})$ und $(-\frac{1}{2}, \frac{1}{2})$. Bestimmen wir nun die Hesse-Matrix von g :

$$(\mathcal{H}g)(x,y) = \begin{pmatrix} 6x & 6y-3 \\ 6y-3 & 6x \end{pmatrix}$$

Einsetzen der Punkte liefert

$$\begin{aligned} (\mathcal{H}g)(0,0) &= \begin{pmatrix} 0 & -3 \\ -3 & 0 \end{pmatrix} & (\mathcal{H}g)(0,1) &= \begin{pmatrix} 0 & 3 \\ 3 & 0 \end{pmatrix} \\ (\mathcal{H}g)\left(\frac{1}{2}, \frac{1}{2}\right) &= \begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix} & (\mathcal{H}g)\left(-\frac{1}{2}, \frac{1}{2}\right) &= \begin{pmatrix} -3 & 0 \\ 0 & -3 \end{pmatrix} \end{aligned}$$

Die Hesse-Matrix von $(\frac{1}{2}, \frac{1}{2})$ hat doppelten Eigenwert 3, ist also positiv definit. Die Hesse-Matrix von $(-\frac{1}{2}, \frac{1}{2})$ hat doppelten Eigenwert -3, ist also negativ definit. Für die ersten beiden Matrizen ergibt sich in beiden Fällen das charakteristische Polynom

$$\chi = X^2 - 9 = (X+3)(X-3),$$

sodass diese einen positiven und einen negativen Eigenwert haben, also indefinit sind. Damit handelt es sich bei $(0,0)$ und $(0,1)$ um einen Sattelpunkt, bei $(\frac{1}{2}, \frac{1}{2})$ um ein isoliertes lokales Minimum, und bei $(-\frac{1}{2}, \frac{1}{2})$ um ein isoliertes lokales Maximum.

Aufgabe (Frühjahr 2014, T3A1)

Es sei

$$u: \mathbb{R}^2 \rightarrow \mathbb{R}, \quad u(x,y) = (x^2 + 2y^2) \cos(x+y),$$

und $D = \{(x,y) \in \mathbb{R}^2 \mid x^2 + y^2 < \frac{1}{2}\}$. \overline{D} bezeichne den Abschluss dieser Menge.

- a** Berechnen Sie den Gradienten ∇u auf \mathbb{R}^2 .
- b** Zeigen Sie, dass u auf \overline{D} Maximum und Minimum annimmt, und bestimmen Sie das Minimum.

Hinweis Teil **a** wird hierzu nicht benötigt.

- c** Wir identifizieren \mathbb{R}^2 mit \mathbb{C} . Gibt es eine holomorphe Funktion $f: D \rightarrow \mathbb{C}$ mit $u = \operatorname{Re} f$?

Lösungsvorschlag zur Aufgabe (Frühjahr 2014, T3A1)

- a** Durch Berechnung der partiellen Ableitungen erhält man

$$(\nabla u)(x, y) = \begin{pmatrix} 2x \cos(x+y) - (x^2 + 2y^2) \sin(x+y) \\ 4y \cos(x+y) - (x^2 + 2y^2) \sin(x+y) \end{pmatrix}.$$

- b** Die Menge \overline{D} ist im Ball $B_1(0)$ enthalten und damit beschränkt, laut Definition auch abgeschlossen. Als abgeschlossene und beschränkte Teilmenge des \mathbb{R}^2 ist \overline{D} somit kompakt. Da die Funktion f stetig ist, nimmt diese also auf \overline{D} Minimum und Maximum an.

Wir zeigen, dass 0 das Minimum von f auf \overline{D} ist. Es gilt zunächst $f(0, 0) = 0$. Sei $(x, y) \in \overline{D}$ ein beliebiger weiterer Punkt mit $(x, y) \neq (0, 0)$. Es gilt für diesen $x^2, y^2 \leq x^2 + y^2 \leq \frac{1}{2}$ und somit $|x|, |y| \leq \frac{1}{\sqrt{2}} = \frac{\sqrt{2}}{2}$. Daraus folgt für $(x, y) \in \overline{D} \setminus \{(0, 0)\}$

$$|x + y| \leq |x| + |y| \leq \sqrt{2} < \frac{\pi}{2}.$$

Somit gilt $x + y \in]-\frac{\pi}{2}, \frac{\pi}{2}[$. Da die Cosinus-Funktion auf diesem Intervall positiv ist, folgt

$$f(x, y) = (x^2 + y^2) \cos(x + y) > 0 \cdot 0 = 0 = f(0, 0).$$

Und damit ist $0 = f(0, 0)$ das Minimum von f auf \overline{D} .

- c** Um Satz 6.6 anzuwenden, prüfen wir, ob es sich bei u um eine harmonische Funktion handelt. Die zweiten partiellen Ableitungen von u sind

$$\begin{aligned}\partial_x^2 u(x, y) &= 2 \cos(x+y) - 4x \sin(x+y) - (x^2 + y^2) \cos(x+y), \\ \partial_y^2 u(x, y) &= 4 \cos(x+y) - 8y \sin(x+y) - (x^2 + y^2) \cos(x+y).\end{aligned}$$

Wir sehen

$$\Delta u(x, y) = \partial_x^2 u(x, y) + \partial_y^2 u(x, y) \neq 0.$$

Somit ist u keine harmonische Funktion und kann nicht Realteil einer holomorphen Funktion sein.

Aufgabe (Herbst 2015, T2A1)

Wir betrachten die Funktion

$$\begin{aligned}f: D &= \{(x, y) \in \mathbb{R} \mid x \leq 0, y < 0\} \cup \{(0, 0)\} \rightarrow \mathbb{R}, \\ f(x, y) &= (y+1)e^x - e^y.\end{aligned}$$

- a** Geben Sie an, welche Punkte in \mathbb{R}^2 innere Punkte oder Randpunkte von D sind. Ist D offen oder abgeschlossen? Begründen Sie Ihrer Antwort.
- b** Bestimmen Sie Gradienten und Hessematrix von f in allen inneren Punkte von D .
- c** Welcher Punkt im Inneren von D ist eine lokale Extremstelle und von welchem Typ ist er? Begründen Sie Ihre Antwort.
- d** Welcher Randpunkt ist eine lokale Extremstelle von f ? Begründen Sie Ihre Antwort.

Lösungsvorschlag zur Aufgabe (Herbst 2015, T2A1)

- a** Die inneren Punkte von D sind gegeben durch die Menge

$$D^\circ = \{(x, y) \in \mathbb{R}^2 \mid x < 0, y < 0\},$$

Die Randpunkte sind

$$\partial D = \{(x, 0) \in \mathbb{R}^2 \mid x \leq 0\} \cup \{(0, y) \in \mathbb{R}^2 \mid y < 0\}.$$

Wäre D offen, so müsste gelten $D = D^\circ$, d.h. jeder Punkt müsste innerer Punkt sein. Wegen $(0, 0) \in D, (0, 0) \notin D^\circ$ ist dies nicht der Fall. Damit D abgeschlossen ist, müsste $D = D \cup \partial D$ gelten. Wegen $(-1, 0) \in \partial D, (-1, 0) \notin D$ ist auch dies nicht der Fall, sodass D weder offen noch abgeschlossen ist.

- b** Es gilt für $(x, y) \in D^\circ$

$$(\nabla f)(x, y) = \begin{pmatrix} (y+1)e^x \\ e^x - e^y \end{pmatrix} \quad \text{und} \quad (\mathcal{H}f)(x, y) = \begin{pmatrix} (y+1)e^x & e^x \\ e^x & -e^y \end{pmatrix}.$$

- c** Wir berechnen zuerst die kritischen Punkte

$$(\nabla f)(x, y) = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \Leftrightarrow \begin{array}{rcl} (y+1)e^x & = & 0 \\ e^x - e^y & = & 0 \end{array}$$

Wegen $e^x > 0$ für $x \in \mathbb{R}$ folgt aus der ersten Gleichung $y = -1$. Einsetzen in die zweite Gleichung ergibt wegen der Injektivität der Exponentialfunktion

$$e^x - e^{-1} = 0 \Leftrightarrow e^x = e^{-1} \Leftrightarrow x = -1.$$

Der einzige kritische Punkt ist somit $(-1, -1) \in D$. Die Hesse-Matrix an dieser Stelle ist

$$(\mathcal{H}f)(-1, -1) = \begin{pmatrix} 0 & e^{-1} \\ e^{-1} & -e^{-1} \end{pmatrix}.$$

Wir überprüfen, ob diese (semi-)definit oder indefinit ist, indem wir das charakteristische Polynom χ sowie die Eigenwerte ausrechnen:

$$\chi = -X(-e^{-1} - X) - e^{-2} = X^2 + e^{-1}X - e^{-2}.$$

Die Nullstellen sind

$$x_{1,2} = \frac{-e^{-1} \pm \sqrt{e^{-2} + 4e^{-2}}}{2} = \frac{-e^{-1} \pm \sqrt{5e^{-2}}}{2} = \frac{1}{2} \left(-e^{-1} \pm \sqrt{5}e^{-1} \right).$$

Offensichtlich ist von diesen Nullstellen eine positiv, die andere negativ. Die Matrix $(\mathcal{H}f)(-1, -1)$ ist somit indefinit und der zugehörige Punkt ist ein Sattelpunkt und somit *kein* Extremum. Also besitzt f in keinem inneren Punkt ein Extremum.

- d** Aufgrund der Definition von D kommen nur Randpunkte der Form $(0, y)$ in Betracht. Ist nun $(0, y)$ ein lokales Extremum von f , so muss es sich dabei insbesondere um ein lokales Extremum der Funktion

$$f_x: \mathbb{R}_0^- \rightarrow \mathbb{R}, \quad y \mapsto y + 1 - e^y$$

handeln. Ist $y < 0$, so muss dazu die Ableitung $f'_x(y) = 1 - e^y$ verschwinden. Es gilt aber für $y < 0$, dass $e^y < 1$ und somit $f'_x(y) \neq 0$ ist. Somit kommt nur der Punkt $y = 0$ in Frage. Dieser ist tatsächlich ein Randextremum: Es gilt $f(0, 0) = 0$. Wir zeigen zunächst, dass $y + 1 \leq e^y$ für alle $y \in \mathbb{R}$ gilt. Betrachte dazu die Funktion $g: \mathbb{R} \rightarrow \mathbb{R}$, $y \mapsto e^y - y - 1$. Es gilt $g(0) = 0$. Gäbe es eine weitere Nullstelle y' , so hätte die Ableitung g' eine Nullstelle zwischen 0 und y' . Jedoch ist

$$g'(y) = e^y - 1 = 0 \Leftrightarrow y = 0.$$

Also hat g keine weitere Nullstelle und es gilt $g(y) \leq 0$ oder $g(y) \geq 0$ für alle $y \in \mathbb{R}$. Wegen $g(1) = e$ ist letzteres der Fall und es folgt für $y \in \mathbb{R}$ $e^y \geq y + 1$. Dabei ist die Ungleichung für $y \neq 0$ strikt. Damit ist nun für $(x, y) \in D \setminus \{(0, 0)\}$

$$f(x, y) = (y + 1)e^x - e^y < e^y e^x - e^y = e^y(e^x - 1) \leq 0.$$

Definition 5.7. Eine Teilmenge $M \subseteq \mathbb{R}^n$ wird d -dimensionale **Untermannigfaltigkeit** genannt, wenn es für jeden Punkt $a \in M$ eine offene Umgebung U und $n - d$ stetig differenzierbare Funktionen $\varphi_1, \dots, \varphi_{n-d}: U \rightarrow \mathbb{R}$ gibt, so dass gilt

- (1) $U \cap M = \{x \in U \mid \varphi_1(x) = \dots = \varphi_{n-d}(x) = 0\}$.
- (2) $\dim \langle \nabla \varphi_1(x), \dots, \nabla \varphi_{n-d}(x) \rangle = n - d$ für alle $x \in U \cap M$. (Die Gradienten von $\varphi_1, \dots, \varphi_{n-d}$ sind also linear unabhängig.)

Satz 5.8 (Extrema unter Nebenbedingungen). Seien alle Bezeichnung so wie in der vorangegangenen Definition und $f: U \subseteq \mathbb{R}^n \rightarrow \mathbb{R}$ eine stetig differenzierbare Funktion. Ist $a \in U \cap M$ ein lokales Extremum von f auf der Untermannigfaltigkeit M , so gibt es reelle Zahlen $\lambda_1, \dots, \lambda_{n-d} \in \mathbb{R}$ (sog. *Lagrange-Multiplikatoren*), sodass die Gleichung

$$(\nabla f)(a) = \sum_{i=1}^{n-d} \lambda_i (\nabla \varphi_i)(a) \quad \text{erfüllt ist.}$$

Aufgabe (Herbst 2015, T3A5)

Gegeben sei der Ellipsenrand $E \subset \mathbb{R}^2$ durch

$$(x, y) \in E \Leftrightarrow x^2 + 2y^2 = 2$$

sowie die Funktion $f: \mathbb{R}^2 \rightarrow \mathbb{R}$ durch $f(x, y) = x^3 - 3y^4$.

Begründen Sie, warum f sein Maximum und Minimum auf E annimmt. Bestimmen Sie sodann den maximalen sowie den minimalen Wert, den $f(x, y)$ unter der Nebenbedingung $(x, y) \in E$ annimmt und diejenigen Stellen, an denen das globale Maximum und das globale Minimum angenommen wird.

Lösungsvorschlag zur Aufgabe (Herbst 2015, T3A5)

Um zu zeigen, dass Minimum und Maximum existieren, bemerken wir zunächst, dass f als Polynom stetig ist. Außerdem ist E kompakt: Es gilt $E \subseteq B_2(0) = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 < 4\}$, denn aus $(x, y) \in E$ folgt insbesondere

$$x^2 + y^2 \leq x^2 + 2y^2 = 2 < 2^2.$$

Somit ist E beschränkt. Als Urbild der abgeschlossenen Menge $\{2\}$ unter der stetigen Abbildung $(x, y) \mapsto x^2 + 2y^2$ ist die Menge auch abgeschlossen, und somit insgesamt kompakt. Als stetige Funktion nimmt f daher laut dem Maximumsprinzip auf der kompakten Menge E Minimum und Maximum an.

Bei E handelt es sich um eine eindimensionale Untermannigfaltigkeit. Ist nämlich $a \in E$, so definieren wir als offene Umgebung $U = \mathbb{R}^2$. Es gilt dann

$$U \cap M = \{p \in U \mid \varphi(x) := x^2 + 2y^2 - 2 = 0\} \quad \text{mit} \quad \nabla \varphi(x) = \begin{pmatrix} 2x \\ 4y \end{pmatrix}.$$

Der Gradient $(\nabla \varphi)(x)$ verschwindet außerdem für kein $x \in E$, da $(0, 0) \notin E$.

Laut dem Satz über Extrema unter Nebenbedingungen 5.8 ist es eine notwendige Bedingung für die Existenz eines lokalen Extremums, dass eine reelle

Zahl λ existiert, sodass

$$(\nabla f)(x, y) = \lambda(\nabla \varphi)(x, y)$$

gilt. Konkret ergibt sich

$$\begin{pmatrix} 3x^2 \\ -12y^3 \end{pmatrix} = \lambda \cdot \begin{pmatrix} 2x \\ 4y \end{pmatrix} \Leftrightarrow \begin{array}{lcl} 3x^2 & = & 2\lambda x \\ -12y^3 & = & 4\lambda y \end{array} \Leftrightarrow \begin{array}{lcl} x(3x - 2\lambda) & = & 0 \\ 4y(-3y^2 - \lambda) & = & 0 \end{array}$$

Aus der ersten Gleichung ergibt sich $x = 0$ oder $\lambda = \frac{3}{2}x$.

1. Fall: Im Fall $x = 0$ folgt aufgrund der Definition der Menge E , dass $2y^2 = 2 \Leftrightarrow y = \pm 1$ gilt. Für $(x, y) = (0, \pm 1)$ ist auch die zweite Gleichung erfüllt, sofern man $\lambda = -3$ setzt.

2. Fall: Im Fall $\lambda = \frac{3}{2}x$ ergibt sich die Gleichung

$$4y(-3y^2 - \frac{3}{2}x) = 0 \Leftrightarrow y = 0 \text{ oder } 3y^2 = -\frac{3}{2}x$$

Im ersten Fall erhalten wir aus der Gleichung von E , dass $x^2 = 2$, also $x = \pm\sqrt{2}$ ist. Im zweiten Fall würde folgen $2y^2 = -x$ und wiederum liefert Einsetzen in die Gleichung von E und Mitternachtsformel

$$x^2 - x = 2 \Leftrightarrow x^2 - x - 2 = 0 \Leftrightarrow x \in \{2, -1\}.$$

Im ersten Fall erhalten wir wegen der Gleichung $2y^2 = -x$ den Widerspruch $2y^2 = -2$. Für $x = -1$ liefert diese Gleichung

$$2y^2 = 1 \Leftrightarrow y = \pm \frac{1}{\sqrt{2}}.$$

Die zu untersuchenden Punkte sind also

$$(0, 1), \quad (0, -1), \quad (\sqrt{2}, 0), \quad (-\sqrt{2}, 0), \quad \left(-1, \frac{1}{\sqrt{2}}\right), \quad \left(-1, -\frac{1}{\sqrt{2}}\right).$$

Wir berechnen die Funktionswerte an diesen Stellen

$$\begin{array}{ll} f(0, 1) = 0^3 - 4 \cdot 1^4 = -1 & f(0, -1) = -1 \\ f(\sqrt{2}, 0) = 2\sqrt{2} & f(-\sqrt{2}, 0) = -2\sqrt{2} \\ f\left(-1, \frac{1}{\sqrt{2}}\right) = -1 - \frac{3}{8} = -\frac{11}{8} & f\left(-1, -\frac{1}{\sqrt{2}}\right) = -1 - \frac{3}{4} = -\frac{7}{4}. \end{array}$$

Das globale Minimum ist damit $-2\sqrt{2}$ an der Stelle $(-\sqrt{2}, 0)$, das Maximum ist $2\sqrt{2}$ für $(\sqrt{2}, 0)$.

Aufgabe (Herbst 2013, T2A3)

Welche der folgenden Aussagen sind richtig, welche falsch? Begründen Sie Ihre Antwort.

- a** Sei $f \in C^2(\mathbb{R}^2; \mathbb{R})$, und in $x_0 \in \mathbb{R}^2$ gelten $\nabla f(x_0) = 0$ und $D^2 f(x_0) = 0$. Dann hat f kein lokales Extremum in x_0 .
- b** Betrachten Sie das Vektorfeld $F(x) = (e^{x_1}, e^{x_2}, e^{x_3})^T$ auf \mathbb{R}^3 . Das Kurvenintegral über F ist wegen unabhängig.
- c** Die holomorphe Funktion $f: \mathbb{C} \rightarrow \mathbb{C}$ sei beschränkt längs der Gerade $\{z \in \mathbb{C} \mid z = t(1+i), t \in \mathbb{R}\}$. Dann ist f konstant.

Lösungsvorschlag zur Aufgabe (Herbst 2013, T2A3)

- a** *Falsch.* Betrachte die beliebig oft differenzierbare Funktion

$$f: \mathbb{R}^2 \rightarrow \mathbb{R}, \quad (x, y) \mapsto x^4 + y^4.$$

Für diese gilt

$$(\nabla f)(x, y) = \begin{pmatrix} 4x^3 \\ 4y^3 \end{pmatrix} \quad \text{und} \quad (\mathcal{H}f)(x, y) = \begin{pmatrix} 12x^2 & 0 \\ 0 & 12y^2 \end{pmatrix}.$$

Somit erhalten wir

$$(\nabla f)(0, 0) = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \quad \text{und} \quad (\mathcal{H}f)(0, 0) = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Dennoch ist $(0, 0)$ ein lokales Extremum. Es gilt $f(0, 0) = 0$ und für $(x, y) \neq (0, 0)$ gilt $f(x, y) = x^4 + y^4 > 0 = f(0, 0)$.

- b** *Richtig.* Bei dem Vektorfeld handelt es sich um das Gradientenfeld von

$$G: \mathbb{R}^3 \rightarrow \mathbb{R}, \quad \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \mapsto e^{x_1} + e^{x_2} + e^{x_3},$$

d. h. es gilt $(\nabla G)(x_1, x_2, x_3) = F(x_1, x_2, x_3)$. Wir erhalten mit der Kettenregel für einen beliebigen Weg $\gamma: [a, b] \rightarrow \mathbb{R}^3$

$$(G \circ \gamma)'(t) = (\nabla G)(\gamma(t)) \cdot \gamma'(t) = \langle f(\gamma(t)), \gamma'(t) \rangle$$

und somit

$$\begin{aligned} \int_{\gamma} \langle F, ds \rangle &= \int_a^b \langle (F \circ \gamma)(t), \gamma'(t) \rangle dt = \int_a^b (G \circ \gamma)'(t) dt = \\ &= \left[(G \circ \gamma)(t) \right]_a^b = (G \circ \gamma)(b) - (G \circ \gamma)(a) = G(\gamma(b)) - G(\gamma(a)). \end{aligned}$$

Dies beweist, dass der Wert des Integrals nur vom Anfangs- und Endpunkt $\gamma(a)$ bzw. $\gamma(b)$ und nicht vom Verlauf der Kurve abhängt.

- c** *Falsch.* Sei G die Menge aus der Angabe. Betrachte die Funktion

$$f: \mathbb{C} \rightarrow \mathbb{C}, \quad z \mapsto \sin\left[\frac{1}{2}(1-i)z\right]$$

Diese ist aufgrund der Kettenregel auf ganz \mathbb{C} holomorph. Zugleich gilt jedoch für $t \in \mathbb{R}$

$$\sin\left[\frac{1}{2}(1-i)(1+i)t\right] = \sin t \in [-1, 1].$$

Somit ist $f|_G$ beschränkt, wegen

$$f\left(\frac{\pi}{2} + \frac{\pi}{2}i\right) = \sin\left(\frac{\pi}{2}\right) = 1 \neq 0 = f(0) = 0$$

ist f jedoch nicht konstant.

Aufgabe (Frühjahr 2012, T2A3)

Sei $f: \mathbb{R}^2 \rightarrow \mathbb{R}$ zweimal stetig differenzierbar. Beweisen oder widerlegen Sie folgende Aussagen:

- a** $\lim_{|x| \rightarrow \infty} f(x) = 0 \Rightarrow f$ nimmt Maximum oder Minimum an.
- b** f beschränkt $\Rightarrow f$ nimmt Maximum oder Minimum an.
- c** f beschränkt und $\Delta f = \frac{\partial^2 f}{\partial x_1^2} + \frac{\partial^2 f}{\partial x_2^2} = 0 \Rightarrow f$ nimmt Maximum und Minimum an.

Hinweis Bei Teil **c** hilft Funktionentheorie.

Lösungsvorschlag zur Aufgabe (Frühjahr 2012, T2A3)

- a** *Richtig.* Im Fall $f \equiv 0$ ist die Aussage klar. Andernfalls existiert ein $(a, b) \in \mathbb{R}^2$ mit $f(a, b) = c \in \mathbb{R}^\times$. Wegen $\lim_{|x| \rightarrow \infty} f(x) = 0$ existiert außerdem ein $K > 0$, sodass $|f(x)| < |c|$ für alle $x \in \mathbb{R}^2$ mit $|x| > K$. Nun ist die Menge $B_K(0) = \{(x, y) \in \mathbb{R}^2 \mid |(x, y)| \leq K\}$ kompakt, somit nimmt $|f|$ als stetige Funktion dort ein Maximum an. Es gibt also ein $(u, v) \in B$ mit $f(u, v) = \max\{|f(x, y)| \mid (x, y) \in B\}$. Für alle $(x, y) \in \mathbb{R}^2 \setminus B$ gilt zudem

$$|f(u, v)| \geq |c| > |f(x, y)|.$$

Somit handelt es sich bei $f(u, v)$ um ein globales Maximum.

b Falsch. Betrachte die Funktion

$$f: \mathbb{R}^2 \rightarrow \mathbb{R}, \quad (x, y) \mapsto \arctan(x + y).$$

Aus der Gleichung $\arctan(\mathbb{R}) =]-\frac{\pi}{2}; \frac{\pi}{2}[$ folgt $f(\mathbb{R}^2) =]-\frac{\pi}{2}; \frac{\pi}{2}[$. Damit ist $\frac{\pi}{2}$ zwar ein Supremum der Wertemenge von f , jedoch nimmt f kein Maximum an, da die Tangensfunktion an der Stelle $\frac{\pi}{2}$ nicht definiert ist.

c Richtig. Die Funktion f ist wegen $\Delta f = 0$ harmonisch. Identifizieren wir also \mathbb{R}^2 mit \mathbb{C} , so existiert deshalb eine holomorphe Funktion $h: \mathbb{C} \rightarrow \mathbb{C}$ mit $\operatorname{Re} h = f$. Da $\operatorname{Re} h$ beschränkt ist, ist das Bild der Funktion h ein Streifen in der komplexen Ebene. Damit muss h laut dem kleinen Satz von Picard bereits konstant sein. Es gibt also $\alpha, \beta \in \mathbb{R}$ mit $h(z) = \alpha + i\beta$ für alle $z \in \mathbb{C}$. Daraus folgt $f(x, y) = \alpha$ für alle $(x, y) \in \mathbb{R}^2$. Somit ist α zugleich Minimum und Maximum der Funktion f .

Integralrechnung

Zur Berechnung von Integralen sind zwei Sätze besonders hilfreich: Mithilfe des Satzes von Fubini lässt sich die Integration schrittweise über die einzelnen Koordinaten ausführen (vgl. die folgende Aufgabe). Für komplexere Mengen bietet es sich an, den Integrationsbereich zu transformieren. Dies ist mittels des Transformationssatzes möglich.

Satz 5.9 (Transformationssatz). Es sei $M \subseteq \mathbb{R}^n$ eine offene Menge und $\phi: M \rightarrow \phi(M)$ ein Diffeomorphismus (d. h. eine bijektive stetig differenzierbare Abbildung mit stetig differenzierbarer Umkehrabbildung). Dann ist eine Funktion f auf $\phi(M)$ genau dann integrierbar, wenn $x \mapsto (f \circ \phi)(x)| \det \phi'(x)|$ auf M integrierbar ist und es gilt:

$$\int_{\phi(M)} f(x) dx = \int_M (f \circ \phi)(x) | \det \phi'(x) | dx.$$

Ferner ist das Volumen einer Menge B definiert als

$$\operatorname{vol} B = \int_B 1 dx.$$

Aufgabe (Frühjahr 2010, T3A3)

Man bestimme das Volumen des Bereichs

$$B = \{(x, y, z) \in \mathbb{R}^3 \mid x \geq 0, y \geq 0, z \geq 0, x + 2y + 3z \leq 1\}.$$

Lösungsvorschlag zur Aufgabe (Frühjahr 2010, T3A3)

Ein Punkt (x, y, z) liegt genau dann in B , wenn die drei Ungleichungen

$$0 \leq x \leq 1, \quad 0 \leq y \leq \frac{1}{2}(1-x) \quad \text{und} \quad 0 \leq z \leq \frac{1}{3}(1-x-2y)$$

erfüllt sind. Dies liefert die Grenzen der Integration. Wir berechnen also

$$\begin{aligned} \int_B 1 \mathrm{d}(x, y, z) &= \int_0^1 \int_0^{\frac{1}{2}-\frac{x}{2}} \int_0^{\frac{1}{3}(1-x-2y)} 1 \mathrm{d}(x, y, z) = \\ &= \int_0^1 \int_0^{\frac{1}{2}-\frac{x}{2}} \frac{1}{3}(1-x-2y) \mathrm{d}(x, y) = \\ &= \frac{1}{3} \int_0^1 \left[y - xy - y^2 \right]_{y=0}^{y=\frac{1}{2}-\frac{x}{2}} = \\ &= \frac{1}{3} \int_0^1 \frac{1}{2} - \frac{x}{2} - x \left(\frac{1}{2} - \frac{x}{2} \right) - \left(\frac{1}{2} - \frac{x}{2} \right)^2 \mathrm{d}x = \\ &= \frac{1}{3} \int_0^1 \frac{1}{2} - \frac{x}{2} - \frac{x}{2} + \frac{x^2}{2} - \frac{1}{4} + \frac{x}{2} - \frac{x^2}{4} \mathrm{d}x = \\ &= \frac{1}{3} \cdot \frac{1}{2} \int_0^1 \frac{1}{2} - x + \frac{1}{2}x^2 \mathrm{d}x = \\ &= \frac{1}{6} \left[\frac{1}{2}x - \frac{1}{2}x^2 + \frac{1}{6}x^3 \right]_{x=0}^{x=1} = \frac{1}{6} \cdot \left(\frac{1}{2} - \frac{1}{2} + \frac{1}{6} \right) = \frac{1}{6} \cdot \frac{1}{6} = \frac{1}{36}. \end{aligned}$$

6. Analysis: Funktionentheorie

6.1. Komplexe Differenzierbarkeit

Nachdem sich das vorangegangene Kapitel um die Differenzierbarkeit von Funktionen reeller Variablen gedreht hat, erarbeiten wir in diesem Abschnitt den Begriff der komplexen Differenzierbarkeit. Hierzu bieten sich dem Mathematiker zwei Wege an: einerseits lässt sich der in Definition 5.1 (2) angegebene Differenzenquotient auf komplexwertige Funktionen übertragen, andererseits lassen sich die komplexen Zahlen auch als zwei-dimensionaler \mathbb{R} -Vektorraum auffassen, sodass wir die Methoden der Analysis zweier reeller Variablen anwenden können.

Reelle Differenzierbarkeit

Ist $f: \mathbb{C} \rightarrow \mathbb{C}$ eine komplexe Funktion, so lässt sich diese durch die Zuordnung

$$(x, y) \mapsto (\operatorname{Re} f(x + iy), \operatorname{Im} f(x + iy))$$

als Funktion $\mathbb{R}^2 \rightarrow \mathbb{R}^2$ auffassen. Wir können dann die Definition 5.4 der Differenzierbarkeit aus der Analysis mehrerer reeller Variablen verwenden.

Definition 6.1. Sei $U \subseteq \mathbb{C}$ eine offene, nichtleere Teilmenge und $f: U \rightarrow \mathbb{C}$ eine Abbildung. Man bezeichnet f als *reell differenzierbar*, wenn f differenzierbar im Sinne von Definition 5.4 ist. Dies ist genau dann der Fall, wenn sämtliche partiellen Ableitungen von Real- und Imaginärteil existieren und stetig sind.

Beispiel 6.2. Sei $\iota: \mathbb{C} \rightarrow \mathbb{C}: z \mapsto \bar{z}$ die komplexe Konjugation, dann ist $\iota(x + iy) = x - iy$. Man erhält als Jacobi-Matrix der Funktion in $z = x + iy \in \mathbb{C}$

$$(\mathbf{D}\iota)(x, y) = \begin{pmatrix} \partial_x \operatorname{Re} \iota(z) & \partial_y \operatorname{Re} \iota(z) \\ \partial_x \operatorname{Im} \iota(z) & \partial_y \operatorname{Im} \iota(z) \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Da alle Einträge in dieser Matrix konstant sind, also insbesondere stetig, ist ι in jedem Punkt reell differenzierbar. ■

Komplexe Differenzierbarkeit

Definition 6.3. Sei $U \subseteq \mathbb{C}$ offen und $f : U \rightarrow \mathbb{C}$ eine Abbildung. Man bezeichnet f als *komplex differenzierbar* in $z_0 \in U$, wenn der Grenzwert

$$\lim_{z \rightarrow z_0} \frac{f(z) - f(z_0)}{z - z_0}$$

existiert und nennt diesen die *Ableitung* von f in z_0 , notiert als $f'(z_0)$.

Den Zusammenhang der beiden Differenzierbarkeits-Begriffe liefert folgender Satz.

Satz 6.4. Sei $a \in U$, $f : U \rightarrow \mathbb{C}$ eine Abbildung und $f = \operatorname{Re} f + i \operatorname{Im} f$ ihre Zerlegung in Real- und Imaginärteil. Folgende Aussagen sind äquivalent:

- (1) f ist in a komplex differenzierbar.
- (2) f ist in a reell differenzierbar und es gelten die *Cauchy-Riemannschen Differentialgleichungen*

$$\partial_x \operatorname{Re} f(a) = \partial_y \operatorname{Im} f(a) \quad \text{und} \quad \partial_y \operatorname{Re} f(a) = -\partial_x \operatorname{Im} f(a).$$

Eine komplex differenzierbare Funktion wird auch *holomorph* genannt. Die Jacobi-Matrix aus Beispiel 6.2 zeigt also, dass die komplexe Konjugation *nicht* holomorph ist, weil hier $\partial_x \operatorname{Re} \iota(z) \neq \partial_y \operatorname{Im} \iota(z)$ für alle $z \in \mathbb{C}$ ist.

Aufgabe (Frühjahr 2002, T2A1)

Gegeben seien die Funktionen

$$u : \mathbb{R}^2 \rightarrow \mathbb{R}, \quad u(x, y) = e^{-y}(x \cos x - y \sin x)$$

$$v : \mathbb{R}^2 \rightarrow \mathbb{R}, \quad v(x, y) = e^{-y}(y \cos x + x \sin x)$$

- a** Zeigen Sie, dass diese Funktionen die Cauchy-Riemannschen Differentialgleichungen erfüllen, und, dass deswegen die Funktion

$$f(z) = u(x, y) + iv(x, y), \quad z = x + iy \in \mathbb{C}$$

holomorph ist.

- b** Zeigen Sie für $z = iy$ mit $y \in \mathbb{R}$, dass

$$f(z) = ze^{iz},$$

und folgern Sie daraus $f(z) = ze^{iz}$ für alle $z \in \mathbb{C}$.

Lösungsvorschlag zur Aufgabe (Frühjahr 2002, T2A1)

- a** Man berechnet mithilfe der Produktregel die partiellen Ableitungen und erhält

$$\partial_x u(x, y) = e^{-y} \cos x - e^{-y} x \sin x - e^{-y} y \cos x$$

$$\partial_y u(x, y) = -e^{-y} x \cos x + e^{-y} y \sin x - e^{-y} \sin x$$

$$\partial_x v(x, y) = -e^{-y} \sin x + e^{-y} \sin x + e^{-y} x \cos x$$

$$\partial_y v(x, y) = -e^{-y} y \cos x + e^{-y} \cos x - e^{-y} x \sin x$$

Alle diese Ableitungen sind als punktweise Verknüpfung stetiger Funktionen stetig; somit ist f laut Satz 5.5 zumindest reell differenzierbar. Man sieht außerdem unmittelbar, dass die Cauchy-Riemannschen Differentialgleichungen für ein beliebiges $z = x + iy \in \mathbb{C}$ erfüllt sind.

- b** Sei also $z = 0 + iy$. Wir erhalten mit $iz = i^2y = -y$, dass

$$f(z) = u(0, y) + iv(0, y) = ie^{-y}(y \cos 0) = iye^{-y} = ze^{iz}.$$

Der zweite Teil der Behauptung folgt nun aus dem Identitätssatz. Sei dazu $g(z) = ze^{iz}$ für $z \in \mathbb{C}$. Wie eben gezeigt, stimmen die Funktionen f und g auf der Menge $i\mathbb{R} = \{iy \mid y \in \mathbb{R}\}$ überein. Diese Menge besitzt den Häufungspunkt 0 (vgl. hierzu den Abschnitt zum Identitätssatz), da beispielsweise die Folge $\frac{i}{n}$ für $n \in \mathbb{N}$ aus paarweise verschiedenen Gliedern besteht und $\lim_{n \rightarrow \infty} \frac{i}{n} = 0$ erfüllt. Ferner sind die Funktionen beide komplex differenzierbar (für f haben wir dies in **a** gezeigt, für g folgt die Aussage aus der Produkt- und Kettenregel) und auf dem Gebiet \mathbb{C} definiert. Somit gilt nach dem Identitätssatz

$$f(z) = g(z) = ze^{iz}$$

für alle $z \in \mathbb{C}$.

Holomorphe und harmonische Funktionen

Die Cauchy-Riemannschen Differentialgleichungen liefern ein Kriterium dafür, wann eine Funktion Realteil einer komplex differenzierbaren Funktion ist. In diesem Zusammenhang ist die folgende Definition wichtig:

Definition 6.5. Eine *harmonische* Funktion ist eine Funktion $u: \mathbb{R}^2 \rightarrow \mathbb{R}$, die die sogenannte *Laplace'sche Differentialgleichung*¹

$$\Delta u(x, y) = \partial_x^2 u(x, y) + \partial_y^2 u(x, y) = 0$$

für alle $(x, y) \in \mathbb{R}^2$ erfüllt.

Aufgabe (Herbst 2001, T3A1)

- a** Geben Sie ein Beispiel einer stetigen Funktion $f: \mathbb{C} \rightarrow \mathbb{C}$, die nur im Nullpunkt komplex differenzierbar ist (mit Begründung).
- b** Zeigen Sie, dass Real- und Imaginärteil einer holomorphen Funktion harmonisch sind.

Lösungsvorschlag zur Aufgabe (Herbst 2001, T3A1)

- a** Wir setzen $f(z) = |z|^2$. Es gilt dann $f(x + iy) = x^2 + y^2$ und wir erhalten in einem Punkt $z = x + iy$ als partielle Ableitungen des Real- und Imaginärteils

$$\begin{aligned}\partial_x \operatorname{Re} f(z) &= 2x & \partial_y \operatorname{Re} f(z) &= 2y \\ \partial_y \operatorname{Im} f(z) &= 0 & \partial_x \operatorname{Im} f(z) &= 0.\end{aligned}$$

Da alle diese Ableitungen als Polynome stetig sind, ist f zumindest reell differenzierbar, insbesondere also stetig.

Die Funktion f ist in z genau dann komplex differenzierbar, wenn die Cauchy-Riemannschen Differentialgleichungen gelten. Dies ist nach den obigen Rechnungen genau dann der Fall, wenn

$$2x = 0 \quad \text{und} \quad 2y = 0 \quad \Leftrightarrow \quad x = y = 0.$$

Somit ist f nur im Nullpunkt komplex differenzierbar, aber überall stetig.

- b** Sei f eine holomorphe Funktion, $u(x, y) = \operatorname{Re} f(x + iy)$ und $v(x, y) = \operatorname{Im} f(x + iy)$. Wir berechnen die zweiten partiellen Ableitungen des Realteils. Unter Verwendung der Cauchy-Riemannschen Differentialgleichungen erhalten wir für $a \in \mathbb{R}^2$, dass

$$\partial_x^2 u(a) = \partial_x \partial_x u(a) = \partial_x \partial_y v(a) \quad \text{und} \quad \partial_y^2 u(a) = \partial_y \partial_y u(a) = -\partial_y \partial_x v(a).$$

Da f als holomorphe Funktion unendlich oft differenzierbar ist (siehe (1) auf Seite 285), sind diese Ableitungen wiederum stetig differenzierbar. Damit folgt aus dem Satz von Schwarz, dass die partiellen Ableitungen

¹ Das Symbol Δ in der Formel steht für den Laplace'schen Differentialoperator, $\Delta = \partial_x^2 + \partial_y^2$.

vertauschbar sind und man erhält

$$\Delta u(a) = \partial_x^2 u(a) + \partial_y^2 u(a) = \partial_x \partial_y v(a) - \partial_x \partial_y v(a) = 0$$

und somit ist u harmonisch. Die Rechnung für v verläuft völlig analog.

Aufgabe (Frühjahr 2010, T1A4)

- a** Zeigen Sie, dass Real- und Imaginärteile holomorpher Funktionen harmonisch sind.
- b** Gibt es eine holomorphe Funktion $f: u + iv: \mathbb{C} \rightarrow \mathbb{C}$, deren Realteil $u(x+iy) = x^2 + y^2$ ist? Beweisen Sie ihre Antwort.

Lösungsvorschlag zur Aufgabe (Frühjahr 2010, T1A4)

- a** Siehe Aufgabe H01T3A1 **b** auf Seite 273.
- b** Wir berechnen die zweiten Ableitungen von u nach x und y . Es gilt

$$\partial_x^2 (x^2 + y^2) = \partial_x (2x) = 2, \quad \partial_y^2 (x^2 + y^2) = \partial_y (2y) = 2$$

und somit folgt für alle $(x, y) \in \mathbb{R}^2$

$$\Delta u(x, y) = 2 + 2 = 4 \neq 0.$$

Damit ist u keine harmonische Funktion und die ist Antwort negativ.

Wir halten dieses Ergebnis sowie die Tatsache, dass unter gewissen Voraussetzungen auch die Umkehrung gilt, noch in einer Proposition fest.

- Proposition 6.6.** (1) Ist $U \subseteq \mathbb{C}$ offen und $f: U \rightarrow \mathbb{C}$ eine komplex differenzierbare Funktion, so sind $\operatorname{Re} f$ und $\operatorname{Im} f$ harmonische Funktionen.
- (2) Ist umgekehrt $G \subseteq \mathbb{R}^2$ ein einfach zusammenhängendes Gebiet² und $u: G \rightarrow \mathbb{R}$ eine harmonische Funktion, so existiert eine holomorphe Funktion $f: \widehat{G} \rightarrow \mathbb{C}$ mit $\operatorname{Re} f(x+iy) = u(x, y)$. Hierbei bezeichnet \widehat{G} das Bild von G in \mathbb{C} .

² siehe Proposition 6.29 für den Begriff des einfach zusammenhängenden Gebiets

Aufgabe (Herbst 2011, T2A1)

- a** Sei $G \subseteq \mathbb{C}$ offen, $f : G \rightarrow \mathbb{C}$ holomorph und $G_\star = \{z \in \mathbb{C} \mid \bar{z} \in G\}$. Zeigen Sie, dass die Funktion

$$f_\star : G_\star \rightarrow \mathbb{C}, \quad f_\star(z) = \overline{f(\bar{z})}$$

ebenfalls holomorph ist.

- b** Für welche $a, b \in \mathbb{R}$ ist die Funktion $u : \mathbb{R}^2 \rightarrow \mathbb{R}, u(x, y) = ax^2 + by^2$ der Realteil einer holomorphen Funktion $f : \mathbb{C} \rightarrow \mathbb{C}$?

Lösungsvorschlag zur Aufgabe (Herbst 2011, T2A1)

- a** Aufgrund der Holomorphie ist f insbesondere reell differenzierbar. Auch für die komplexe Konjugation $\iota : z \mapsto \bar{z}$ haben wir dies bereits gesehen. Aus der Kettenregel für differenzierbare Abbildungen in zwei reellen Variablen folgt somit, dass f_\star zum mindesten reell differenzierbar ist. Zur Untersuchung der Gültigkeit der Cauchy-Riemannschen Differentialgleichungen bestimmen wir die Jacobi-Matrix von $f_\star = \iota \circ f \circ \iota$.

$$\begin{aligned} D(\iota \circ f \circ \iota)(z) &= (D\iota)((f \circ \iota)(z)) \cdot D(f \circ \iota)(z) = \\ &= (D\iota)((f \circ \iota)(z)) \cdot (Df)(\iota(z)) \cdot (D\iota)(z) \end{aligned}$$

Eine schnelle Rechnung oder ein Blick in Beispiel 6.2 liefert nun

$$\begin{aligned} D(\iota \circ f \circ \iota)(z) &= \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \cdot \begin{pmatrix} \partial_x \operatorname{Re} f(\bar{z}) & \partial_y \operatorname{Re} f(\bar{z}) \\ \partial_x \operatorname{Im} f(\bar{z}) & \partial_y \operatorname{Im} f(\bar{z}) \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \\ &= \begin{pmatrix} \partial_x \operatorname{Re} f(\bar{z}) & -\partial_y \operatorname{Re} f(\bar{z}) \\ -\partial_x \operatorname{Im} f(\bar{z}) & \partial_y \operatorname{Im} f(\bar{z}) \end{pmatrix}. \end{aligned}$$

Prüfen wir nun, ob die Cauchy-Riemannschen-Differentialgleichungen erfüllt sind. Für $z \in G_\star$ ist

$$\begin{aligned} \partial_x \operatorname{Re} f_\star(z) &= \partial_x \operatorname{Re} f(\bar{z}) \stackrel{(*)}{=} \partial_y \operatorname{Im} f(\bar{z}) = \partial_y \operatorname{Im} f_\star(z) \\ \partial_x \operatorname{Im} f_\star(z) &= -\partial_x \operatorname{Im} f(\bar{z}) \stackrel{(*)}{=} \partial_y \operatorname{Re} f(\bar{z}) = -\partial_y \operatorname{Re} f_\star(z) \end{aligned}$$

Hierbei wurde an den mit $(*)$ markierten Stellen verwendet, dass $\bar{z} \in G$ und deshalb f in \bar{z} holomorph ist. Tatsächlich erfüllt f_\star damit die Cauchy-Riemannschen Differentialgleichungen und ist holomorph.

- b** Gesucht sind die Paare $(a, b) \in \mathbb{R}^2$, für die u eine harmonische Funktion definiert. Wir berechnen die doppelten partiellen Ableitungen und erhalten

$$\partial_x^2 (ax^2 + by^2) = \partial_x(2ax) = 2a \quad \text{und} \quad \partial_y^2 (ax^2 + by^2) = \partial_y(2by) = 2b.$$

Die Laplace'sche Differentialgleichung wird zu

$$\Delta u(x, y) = 0 \Leftrightarrow 2a + 2b = 0 \Leftrightarrow a = -b.$$

Da \mathbb{C} ein einfach zusammenhängendes Gebiet ist, ist u genau dann der Realteil einer holomorphen Funktion, wenn $a = -b$.

Anleitung: Konstruktion einer holomorphen Funktion aus ihrem Realteil

Sei $u: \mathbb{R}^2 \rightarrow \mathbb{R}$ eine differenzierbare Funktion. Wir wollen eine holomorphe Funktion $f: \mathbb{C} \rightarrow \mathbb{C}$ konstruieren, sodass $f(x+iy) = u(x,y) + iv(x,y)$ für eine Funktion $v: \mathbb{R}^2 \rightarrow \mathbb{R}$ mit dem Anfangswert $v(x_0, y_0) = v_0$.

- (1) Überprüfe ggf. zunächst mit Proposition 6.6, ob u überhaupt Realteil einer holomorphen Funktion sein kann.
- (2) Gemäß den Cauchy-Riemannschen Differentialgleichungen gilt nun

$$\partial_x u(x, y) = \partial_y v(x, y) \quad \text{und} \quad \partial_y u(x, y) = -\partial_x v(x, y).$$

Durch Integration erhält man

$$v(x, y) = \int_{y_0}^y \partial_x u(x, \tilde{y}) d\tilde{y} + v(x, y_0) \quad (1)$$

und

$$v(x, y) = - \int_{x_0}^x \partial_y u(\tilde{x}, y) d\tilde{x} + v(x_0, y). \quad (2)$$

- (3) Werte den Ausdruck (2) bei (x, y_0) aus und setze in (1) ein
oder werte (1) bei (x_0, y) aus und setze in (2) ein.

Aufgabe (Frühjahr 2013, T2A1)

- a** Für welche $a, b \in \mathbb{R}$ ist das Polynom $u(x, y) = x^2 + 2axy + by^2$ der Realteil einer holomorphen Funktion auf \mathbb{C} ?
- b** Bestimmen Sie für jedes solche Paar (a, b) den Imaginärteil aller zugehörigen holomorphen Funktionen.

Lösungsvorschlag zur Aufgabe (Frühjahr 2013, T2A1)

- a** Es muss dafür die Laplace'sche Differentialgleichung gelten. Wir berechnen also die ersten beiden partiellen Ableitungen von u nach x und y und erhalten

$$\begin{aligned}\partial_x^2(x^2 + 2axy + by^2) &= \partial_x(2x + 2ay) = 2, \\ \partial_y^2(x^2 + 2axy + by^2) &= \partial_y(2ax + 2by) = 2b\end{aligned}$$

und somit

$$\Delta u(x, y) = 0 \Leftrightarrow 2 + 2b = 0 \Leftrightarrow b = -1.$$

Da \mathbb{R}^2 ein einfach zusammenhängendes Gebiet ist, liefert Proposition 6.6 (2), dass die Abbildung u für alle Paare der Form $(a, -1)$ mit $a \in \mathbb{R}$ der Realteil einer holomorphen Funktion ist.

- b** Sei $f = u + iv$ eine holomorphe Funktion mit der Funktion u als Realteil, außerdem sei $v(0, 0) = v_0$. Für den Imaginärteil v erhält man dann aufgrund der Cauchy-Riemannschen Differentialgleichungen

$$\partial_y v(x, y) = \partial_x u(x, y) = 2x + 2ay.$$

Wir integrieren nach y und erhalten

$$v(x, y) = 2xy + ay^2 + v(x, 0) \quad (1)$$

Mittels der zweiten Differentialgleichung erhalten wir weiter

$$-\partial_x v(x, y) = \partial_y v(x, y) = -(2ax - 2y).$$

Wiederum liefert Integration, diesmal nach x , dass

$$v(x, y) = -ax^2 + 2xy + v(0, y). \quad (2)$$

Wertet man (1) nun bei $(0, y)$ aus und setzt das Ergebnis in (2) ein, so erhält man

$$v(x, y) = (-ax^2 + 2xy) + (ay^2 + v(0, 0)) = -ax^2 + 2xy + ay^2 + v_0.$$

Aufgabe (Herbst 2014, T3A2)

Auf \mathbb{R}^2 sei die reellwertige Funktion $(x, y) \mapsto u(x, y) = (x - y)(x + y + 1)$ gegeben.

- a** Zeigen Sie, dass $u: \mathbb{R}^2 \rightarrow \mathbb{R}$ harmonisch ist.
- b** Bestimmen Sie alle Funktionen $v: \mathbb{R}^2 \rightarrow \mathbb{R}$, $(x, y) \mapsto v(x, y)$, so dass $f = u + iv$ holomorph ist und geben Sie f als Funktion von $z = x + iy \in \mathbb{C}$ an.

Lösungsvorschlag zur Aufgabe (Herbst 2014, T3A2)

- a** Wir vereinfachen zuerst die Funktion und erhalten

$$u(x, y) = x^2 + x - y^2 - y$$

Wie zuvor berechnet man routiniert

$$\Delta u(x, y) = \partial_x^2 u(x, y) + \partial_y^2 u(x, y) = 2 - 2 = 0.$$

Damit ist u eine harmonische Funktion.

- b** Es sei $v(0, 0) = v_0$. Durch die Cauchy-Riemannschen Differentialgleichungen erhalten wir

$$\partial_y v(x, y) = \partial_x u(x, y) = 2x + 1$$

und eine Integration nach y liefert

$$v(x, y) = 2xy + y + v(x, 0).$$

Weiter gilt mit der zweiten Differentialgleichung, dass

$$-\partial_x v(x, y) = \partial_y u(x, y) = -(-2y - 1) = 2y + 1,$$

sodass man daraus durch Integration nach x dann

$$v(x, y) = 2yx + x + v(0, y)$$

bekommt. Der erste Ausdruck liefert $v(0, y) = y + v(0, 0)$, was eingesetzt in den zweiten

$$v(x, y) = 2yx + x + y + v_0$$

ergibt und damit

$$\begin{aligned} f(x + iy) &= u(x, y) + iv(x, y) = (x - y)(x + y + 1) + i(x + 2xy + y + v_0) = \\ &= x^2 + x - y - y^2 + ix + 2ixy + iy + iv_0. \end{aligned}$$

Wir rechnen die Abbildung direkt aus, was in diesem Fall relativ entspannt möglich ist. Eine Alternative besteht in der Verwendung des Identitätssatzes (vgl. den Kasten auf Seite 303). Für $z = x + iy$ gilt:

$$\begin{aligned} f(z) &= x^2 + 2ixy + i^2y^2 + ix - y + x + iy + iv_0 = \\ &= (x + iy)^2 + i(x + iy) + (x + iy) + iv_0 = \\ &= z^2 + iz + z + iv_0. \end{aligned}$$

6.2. Potenz- und Laurentreihen

Der Übergang vom bekannten Begriff der *reellen* Potenzreihe zur *komplexen* Potenzreihe ist nahezu nahtlos – die Definitionen unterscheiden sich tatsächlich nur gering. Wir werden daher auch auf die bekannten Methoden im Umgang mit Reihen, insbesondere die Konvergenzkriterien, zurückgreifen.

Definition 6.7. Sei $(a_n)_{n \in \mathbb{N}_0}$ eine Folge komplexer Zahlen. Eine **Potenzreihe** mit Entwicklungspunkt $a \in \mathbb{C}$ ist eine Reihe der Form

$$\sum_{n=0}^{\infty} a_n(z - a)^n.$$

Besonders interessant sind natürlich diejenigen Reihen, denen sich ein endlicher Wert zuordnen lässt. Falls der Grenzwert $\lim_{k \rightarrow \infty} \sum_{n=0}^k a_n$ der Partialsummen einer Reihe der Form $\sum_{n=0}^{\infty} a_n$ existiert, so heißt diese **konvergent**.

Absolute Konvergenz liegt vor, wenn die zugehörige Reihe der Beträge $\sum_{n=0}^{\infty} |a_n|$ konvergiert. Absolute Konvergenz impliziert Konvergenz im ersten Sinne (das sieht man z. B. mit der Dreiecksungleichung des komplexen Absolutbetrags).

Die wohl einfachste – und für Anwendungen zugleich bedeutendste – Potenzreihe ist die sogenannte **geometrische Reihe**, gegeben durch

$$\sum_{n=0}^{\infty} z^n \quad \text{mit Partialsummen} \quad \sum_{n=0}^m z^n = \frac{1 - z^{m+1}}{1 - z}.$$

Mithilfe der Formel der Partialsummen auf der rechten Seite sieht man unmittelbar, dass die geometrische Reihe für $|z| < 1$ konvergiert und erhält den Grenzwert

$$\sum_{n=0}^{\infty} z^n = \frac{1}{1 - z}.$$

Im Fall $|z| \geq 1$ bilden die Summanden keine Nullfolge, die Reihe divergiert also. Die Menge der Punkte, in denen die geometrische Reihe konvergiert, ist somit genau die offene Kreisscheibe $B_1(0) = \{z \in \mathbb{C} \mid |z| < 1\}$.

Mit beliebigen Potenzreihen verhält es sich ähnlich wie mit der geometrischen Reihe: Ist $\sum_{n=0}^{\infty} a_n(z-a)^n$ eine Potenzreihe (mit Entwicklungspunkt $a \in \mathbb{C}$) und konvergiert die Reihe in $w \in \mathbb{C}$ mit $w \neq a$, so konvergiert sie auch in allen Punkten mit $|z-a| < |w-a|$. Dies führt zur Definition des **Konvergenzradius**.

Proposition 6.8. Sei $\sum_{n=0}^{\infty} a_n(z-a)^n$ eine Potenzreihe. Dann existiert eine eindeutig bestimmte Zahl $r \in \mathbb{R}_0^+$, sodass die Reihe auf der Kreisscheibe $B_r(a) = \{z \in \mathbb{C} \mid |z-a| < r\}$ konvergiert und auf $\{z \in \mathbb{C} \mid |z-a| > r\}$ divergiert. Man bezeichnet diese Zahl r als **Konvergenzradius** und $B_r(a)$ als **Konvergenzkreisscheibe**.

Auf dem Rand der Konvergenzkreisscheibe kann keine Aussage darüber getroffen werden, ob die Reihe dort konvergiert oder nicht. Hier gibt es Beispiele, die zeigen, dass in einem Punkt auf dem Rand der Konvergenzkreisscheibe sowohl Konvergenz als auch Divergenz auftreten kann.

Der Konvergenzradius kann mithilfe folgender beider Formeln direkt aus der Folge $(a_n)_{n \in \mathbb{N}_0}$ berechnet werden. Diese ergeben sich aus dem Wurzel- bzw. Quotientenkriterium für reelle Reihen.

Proposition 6.9. Sei $\sum_{n=0}^{\infty} a_n(z-a)^n$ eine Potenzreihe, und r der Konvergenzradius der Reihe.

- (1) Sei $L = \limsup_{n \rightarrow \infty} \sqrt[n]{|a_n|}$, dann gilt die sogenannte **Formel von Cauchy-Hadamard**:

$$r = \begin{cases} 0 & \text{falls } L = +\infty, \\ \frac{1}{L} & \text{falls } L \in]0, \infty[, \\ \infty & \text{falls } L = 0. \end{cases}$$

- (2) Existiert ein $N \in \mathbb{N}$, sodass $a_n \neq 0$ für $n > N$, so gilt alternativ

$$r = \lim_{n \rightarrow \infty} \left| \frac{a_n}{a_{n+1}} \right|.$$

Aufgabe (Herbst 2005, T2A1)

Beweisen Sie, dass die Potenzreihe

$$\sum_{n=0}^{\infty} \frac{(2n)!}{2^n (n!)^2} z^n$$

den Konvergenzradius $\frac{1}{2}$ hat.

Lösungsvorschlag zur Aufgabe (Herbst 2005, T2A1)

Die Formel von Cauchy-Hadamard liefert nur schwer das gewünschte Ergebnis. Stattdessen betrachten wir den Grenzwert

$$\lim_{n \rightarrow \infty} \left| \frac{a_n}{a_{n+1}} \right|.$$

Dieser ist wegen $a_n \neq 0$ für alle $n \in \mathbb{N}$ definiert und man erhält

$$\begin{aligned} \frac{a_n}{a_{n+1}} &= \frac{(2n)!}{2^n(n!)^2} \cdot \frac{2^{n+1}[(n+1)!]^2}{(2n+2)!} = \frac{2(n+1)^2}{(2n+2)(2n+1)} = \\ &= \frac{(n+1)^2}{(n+1)(2n+1)} = \frac{n+1}{2n+1}. \end{aligned}$$

Der Konvergenzradius ist somit

$$r = \lim_{n \rightarrow \infty} \left| \frac{a_n}{a_{n+1}} \right| = \frac{1}{2}.$$

Aufgabe (Herbst 2008, T3A4)

Die Koeffizienten der Potenzreihe $F(z) = \sum_{n=0}^{\infty} c_n z^n$ seien durch die Rekursionsformel

$$c_n = \sum_{k=1}^{n-1} c_k c_{n-k} \quad \text{für } n \geq 2$$

und die Anfangsbedingungen $c_0 = 0, c_1 = 1$ definiert.

- a** Zeigen Sie: $F(z) = z + F(z)^2$
- b** Bestimmen Sie den Konvergenzradius von $F(z)$.

Hinweis Benutzen Sie Teil **a**.

Lösungsvorschlag zur Aufgabe (Herbst 2008, T3A4)

- a** Wir hantieren etwas mit Summen und erhalten unter Verwendung des Cauchy-Produkts für Reihen (siehe (3) auf Seite 285), dass

$$F(z) - F(z)^2 = \sum_{n=0}^{\infty} c_n z^n - \left(\sum_{n=0}^{\infty} c_n z^n \right)^2 = \sum_{n=0}^{\infty} c_n z^n - \sum_{n=0}^{\infty} \left(\sum_{k=0}^n c_k c_{n-k} \right) z^n.$$

Durch Einsetzen der Anfangsbedingung $c_0 = 0$ sehen wir nun, dass in der Reihe $\sum_{k=0}^n c_k c_{n-k}$ sowohl der erste als auch der letzte Summand jeweils 0 ist, wir erhalten also für $n \geq 2$

$$\sum_{k=0}^n c_k c_{n-k} = \sum_{k=1}^{n-1} c_k c_{n-k}.$$

Im Fall $n = 0$ ist die Summe leer, im Fall $n = 1$ erhalten wir $\sum_{k=0}^1 c_k c_{1-k} = c_0 c_1 + c_1 c_0 = 0$.

Zudem ist wegen der zweiten Anfangsbedingung sowie der Rekursionsformel

$$\sum_{n=0}^{\infty} c_n z^n = 0 + 1z + \sum_{n=2}^{\infty} c_n z^n = z + \sum_{n=2}^{\infty} \left(\sum_{k=1}^{n-1} c_k c_{n-k} \right) z^n.$$

Die obige Differenz wird damit insgesamt zu

$$\begin{aligned} \sum_{n=0}^{\infty} c_n z^n - \sum_{n=0}^{\infty} \left(\sum_{k=0}^n c_k c_{n-k} \right) z^n &= \\ &= z + \sum_{n=2}^{\infty} \left(\sum_{k=1}^{n-1} c_k c_{n-k} \right) z^n - \sum_{n=2}^{\infty} \left(\sum_{k=1}^{n-1} c_k c_{n-k} \right) z^n = z. \end{aligned}$$

Wir haben also

$$F(z) - F(z)^2 = z \Leftrightarrow F(z) = z + F(z)^2.$$

- b** Sei $r \in [0, \infty[$ der Konvergenzradius von $F(z)$. Angenommen, es wäre $r > \frac{1}{4}$, dann gäbe es $\varepsilon > 0$, sodass $\omega = \frac{1}{4} + \varepsilon$ noch im Konvergenzkreis liegt. Da ω und die Koeffizienten c_n von $F(z)$ jeweils positive reelle Zahlen sind, müsste dann auch $F(\omega)$ eine positive reelle Zahl sein. Aus Teil **a** wissen wir jedoch, dass $F(\omega) = \omega + F(\omega)^2$ und Auflösen dieser quadratischen Gleichung liefert

$$\omega = \frac{1}{2} \pm \frac{1}{2} \sqrt{1 - 4\omega} = \frac{1}{2} \pm \frac{1}{2} \sqrt{-4\varepsilon},$$

was eindeutig in $\mathbb{C} \setminus \mathbb{R}$ liegt. Folglich muss für den Konvergenzradius die Abschätzung $r \leq \frac{1}{4}$ gelten.

Um zu sehen, dass $F(z)$ für $|z| < \frac{1}{4}$ tatsächlich konvergiert, beweisen wir zunächst mittels vollständiger Induktion über n , dass $c_n \leq \binom{2n}{n}$ für $n \geq 1$ gilt.

Der Fall $n = 1$ ist klar, für den Induktionsschritt verwenden wir die Formel von *Vandermonde*

$$\binom{l+m}{r} = \sum_{k=0}^r \binom{l}{k} \binom{m}{r-k}, \quad (*)$$

welche auch in der Formelsammlung steht. Setzen wir nun die Aussage für ein n als bereits bewiesen voraus, so haben wir

$$\begin{aligned} c_{n+1} &= \sum_{k=1}^n c_k c_{n+1-k} \leq \sum_{k=1}^n \binom{2k}{k} \binom{2(n+1-k)}{n+1-k} \leq \\ &\leq \sum_{k=0}^{n+1} \binom{2k}{k} \binom{2(n+1-k)}{n+1-k} \stackrel{(*)}{=} \binom{2(n+1)}{n+1}, \end{aligned}$$

was den Induktionsbeweis abschließt. Können wir nun zeigen, dass $\sum_{n=0}^{\infty} \binom{2n}{n} z^n$ für $|z| < \frac{1}{4}$ konvergiert, so handelt es sich nach der eben bewiesenen Behauptung dabei um eine konvergente Majorante für $F(z)$ in diesem Bereich. Dazu verwenden wir Proposition 6.9 (2):

$$\lim_{n \rightarrow \infty} \frac{(2n)!}{n! \cdot n!} \cdot \frac{(n+1)! \cdot (n+1)!}{(2n+2)!} = \lim_{n \rightarrow \infty} \frac{(n+1) \cdot (n+1)}{(2n+2) \cdot (2n+1)} = \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{4}.$$

Dies zeigt $r \geq \frac{1}{4}$ für den Konvergenzradius r von $F(z)$, also insgesamt $r = \frac{1}{4}$.

Die besondere Bedeutung der Potenzreihen für die Funktionentheorie liegt in der folgenden Aussage begründet.

Satz 6.10. Sei $U \subseteq \mathbb{C}$ offen. Eine Funktion $f: U \rightarrow \mathbb{C}$ ist genau dann holomorph auf U , wenn sich f in jedem Punkt von U als in einer Umgebung dieses Punktes konvergente Potenzreihe darstellen lässt, d. h. für jedes $a \in U$ gibt es eine komplexe Folge $(a_n)_{n \in \mathbb{N}_0}$ und ein $r > 0$, sodass

$$f(z) = \sum_{n=0}^{\infty} a_n (z - a)^n \quad \text{für alle } z \in B_r(a)$$

gilt und r der Konvergenzradius dieser Reihe ist. Die Folge $(a_n)_{n \in \mathbb{N}}$ lässt sich

(1) mittels *Taylor-Entwicklung* von f bestimmen, d. h. es gilt

$$a_n = \frac{1}{n!} f^{(n)}(a) \quad \text{für alle } n \in \mathbb{N}_0.$$

(2) mithilfe der *Cauchy-Integralformel* bestimmen, d.h. es gilt

$$a_n = \frac{1}{2\pi i} \int_{\partial B_r(a)} \frac{f(w)}{(w-a)^{n+1}} dw \quad \text{für alle } n \in \mathbb{N}_0$$

für $r > 0$ mit $B_r(a) \subseteq U$.

Funktionen, die sich lokal als Potenzreihen schreiben lassen, werden als *analytisch* bezeichnet. Der Satz besagt somit, dass kein Unterschied zwischen Funktionen $f: \mathbb{C} \rightarrow \mathbb{C}$ besteht, die holomorph bzw. analytisch sind.

Aufgabe (Herbst 2004, T2A2)

Beweisen Sie, dass durch

$$f(z) := \sum_{n=1}^{\infty} \frac{\cos n}{n^z}$$

in der Halbebene $\{z \in \mathbb{C} \mid \operatorname{Re} z > 1\}$ eine holomorphe Funktion f definiert ist.

Lösungsvorschlag zur Aufgabe (Herbst 2004, T2A2)

Per Definition ist $n^z = \exp(z \log n)$ für alle $n \in \mathbb{N}$ und $z \in \mathbb{C}$. Sei nun $z = x + iy \in \mathbb{C}$ mit $x > 1$, d.h. z liegt in der angegebenen Halbebene. Für eine beliebige komplexe Zahl $z = x + iy \in \mathbb{C}$ gilt nun

$$|e^z| = |e^{x+iy}| = |e^x| \cdot |e^{iy}| = |e^x| \cdot 1 = |e^{\operatorname{Re} z}| = e^{\operatorname{Re} z}.$$

Damit ist

$$|n^z| = |\exp(z \log n)| = \exp(\operatorname{Re} z \log n) = \exp(x \log n) = \exp(\log n^x) = n^x$$

für alle $n \in \mathbb{N}$. Die angegebene Reihe lässt sich folglich durch

$$\left| \sum_{n=1}^{\infty} \frac{\cos n}{n^z} \right| \leq \sum_{n=1}^{\infty} \left| \frac{\cos n}{n^z} \right| \leq \sum_{n=1}^{\infty} \left| \frac{1}{n^z} \right| = \sum_{n=1}^{\infty} \frac{1}{n^x}$$

abschätzen. Aus der Analysis 1 weiß man (oder auch nicht), dass die allgemeine harmonische Reihe $\sum_{n=0}^{\infty} \frac{1}{n^x}$ für $x > 1$ konvergiert, also haben wir eine konvergente Majorante gefunden und es handelt sich bei $\sum_{n=1}^{\infty} \frac{\cos n}{n^z}$ um eine auf ganz $\{z \in \mathbb{C} \mid \operatorname{Re} z > 1\}$ absolut konvergente Potenzreihe. Nach Satz 6.10 ist $f(z)$ dort holomorph.

Rechenregeln für Potenzreihen

- (1) *Gliedweises Differenzieren:* Sei $\sum_{n=0}^{\infty} a_n(z-a)^n$ eine Potenzreihe mit Konvergenzradius r . Dann ist die Funktion

$$f: B_r(a) \rightarrow \mathbb{C}, \quad z \mapsto \sum_{n=0}^{\infty} a_n(z-a)^n$$

komplex differenzierbar und die Ableitung ist durch

$$f': B_r(a) \rightarrow \mathbb{C}, \quad z \mapsto \sum_{n=1}^{\infty} n a_n(z-a)^{n-1}$$

gegeben. Außerdem haben die Potenzreihe und ihre formale Ableitung den gleichen Konvergenzradius und zusammen mit Satz 6.10 ergibt sich, dass jede holomorphe Funktion unendlich oft differenzierbar ist.

- (2) *Koeffizientenvergleich:* Wenn die Potenzreihen

$$\sum_{n=0}^{\infty} a_n(z-a)^n \quad \text{und} \quad \sum_{n=0}^{\infty} b_n(z-a)^n$$

in einer Umgebung $B_r(a)$ von a konvergieren und dort

$$\sum_{n=0}^{\infty} a_n(z-a)^n = \sum_{n=0}^{\infty} b_n(z-a)^n \quad \text{für alle } z \in B_r(a)$$

gilt, so ist $a_n = b_n$ für alle $n \in \mathbb{N}_0$.

- (3) *Produkt von Potenzreihen:* Seien

$$\sum_{n=0}^{\infty} a_n(z-a)^n \quad \text{und} \quad \sum_{n=0}^{\infty} b_n(z-a)^n$$

Potenzreihen mit Konvergenzradius $r > 0$. Dann ist

$$\left(\sum_{n=0}^{\infty} a_n(z-a)^n \right) \cdot \left(\sum_{n=0}^{\infty} b_n(z-a)^n \right) = \sum_{n=0}^{\infty} c_n(z-a)^n \quad \text{mit} \quad c_n = \sum_{k=0}^n a_k b_{n-k}$$

für alle $z \in B_r(a)$ und die rechte Reihe konvergiert für diese z auch. Man spricht hierbei vom *Cauchy-Produkt* von Reihen.

Aufgabe (Frühjahr 2008, T2A5)

Bestimmen Sie eine Potenzreihe $f(z) = \sum_{n=0}^{\infty} a_n z^n$ mit folgenden Eigenschaften (für z aus einer Umgebung von 0 aus \mathbb{C}):

$$\begin{cases} zf''(z) - f(z) = z^2 + z - 1 \\ f(0) = 1, f'(0) = 1. \end{cases}$$

Berechnen Sie zunächst a_0 und a_1 aus den Anfangswerten und a_2 und a_3 durch (formalen) Koeffizientenvergleich. Lesen Sie dann eine Rekursionsformel für a_n ($n \geq 4$) aus der Differentialgleichung ab. Geben Sie schließlich die a_n explizit an und berechnen Sie den Konvergenzradius der Reihe.

Lösungsvorschlag zur Aufgabe (Frühjahr 2008, T2A5)

Zunächst gilt nach Satz 6.10 (1), dass

$$a_0 = f(0) = 1 \quad \text{und} \quad a_1 = f'(0) = 1.$$

Die erste bzw. zweite formale Ableitung von f ist

$$f'(z) = \sum_{n=1}^{\infty} n a_n z^{n-1} \quad \text{und} \quad f''(z) = \sum_{n=2}^{\infty} n(n-1) a_n z^{n-2}.$$

Somit wird die erste Gleichung aus der Aufgabenstellung zu

$$\begin{aligned} z f''(z) - f(z) &= z \sum_{n=2}^{\infty} n(n-1) a_n z^{n-2} - \sum_{n=0}^{\infty} a_n z^n = \\ &= \sum_{n=2}^{\infty} n(n-1) a_n z^{n-1} - \sum_{n=0}^{\infty} a_n z^n = \sum_{n=1}^{\infty} (n+1)n a_{n+1} z^n - \sum_{n=0}^{\infty} a_n z^n = \\ &= \sum_{n=0}^{\infty} (n(n+1)a_{n+1} - a_n) z^n. \end{aligned}$$

Durch Koeffizientenvergleich mit $z^2 + z - 1$ (das ist (2) auf Seite 285) folgt

$$\begin{aligned} -1 &= -a_0 \\ 1 &= 2a_2 - a_1 \\ 1 &= 6a_3 - a_2 \\ 0 &= n(n+1)a_{n+1} - a_n \quad \text{für } n \geq 3 \end{aligned}$$

Einsetzen von $a_1 = 1$ in die zweite Gleichung ergibt $a_2 = 1$. Setzt man dies wiederum in die dritte Gleichung ein, bekommt man $a_3 = \frac{1}{3}$. Die in der Aufgabenstellung gefragte Rekursionsformel ergibt sich aus der vierten Gleichung, diese lautet umformuliert nämlich

$$a_n = \frac{1}{n(n-1)} a_{n-1} \quad \text{für } n \geq 4.$$

Intuitiv wird sich der Vorfaktor $\frac{1}{n(n-1)}$ zu einer Fakultät aufmultiplizieren, die jedoch erst bei $n = 4$ beginnt. Wir behaupten deshalb nun

$$a_n = \frac{3!}{n!} \cdot \frac{2!}{(n-1)!} \cdot a_3 = \frac{4}{n!(n-1)!} \quad \text{für } n \geq 4$$

und beweisen dies per Induktion über n . Der Induktionsanfang ist mit

$$a_4 = \frac{1}{4 \cdot 3} a_3 = \frac{1}{4 \cdot 3 \cdot 3} = \frac{2 \cdot 2}{(4 \cdot 3 \cdot 2) \cdot (3 \cdot 2)} = \frac{4}{4! \cdot 3!}$$

erledigt. Setzen wir daher die Aussage für ein n als bereits bewiesen voraus. Es ist nun

$$a_{n+1} = \frac{1}{(n+1)n} a_n = \frac{1}{(n+1)n} \cdot \frac{4}{n!(n-1)!} = \frac{4}{(n+1)!n!}.$$

Dies schließt den Induktionsbeweis ab. Zur Berechnung des Konvergenzradius verwenden wir Proposition 6.9 (2), denn für $n \geq 4$ ist

$$\frac{a_n}{a_{n+1}} = \frac{4}{n!(n-1)!} \cdot \frac{(n+1)!n!}{4} = (n+1)n$$

und da wir endlich viele Folgenglieder bei der Berechnung des Grenzwerts außer Acht lassen können, ergibt sich für den Konvergenzradius

$$r = \lim_{n \rightarrow \infty} \left| \frac{a_n}{a_{n+1}} \right| = \lim_{n \rightarrow \infty} (n+1)n = \infty.$$

Gleichmäßige Konvergenz von Funktionenfolgen

Satz 6.11 (Weierstraß'sches Majorantenkriterium). Sei $D \subseteq \mathbb{C}$ und $(f_n)_{n \in \mathbb{N}}$ eine Folge von Funktionen $D \rightarrow \mathbb{C}$. Weiter sei $(M_n)_{n \in \mathbb{N}}$ eine Folge nichtnegativer reeller Zahlen, sodass

- (1) $|f_n(z)| \leq M_n$ für alle $z \in D$ und $n \in \mathbb{N}$ gilt,
- (2) die Reihe $\sum_{n=0}^{\infty} M_n$ konvergiert.

Dann konvergiert die Reihe $\sum_{n=0}^{\infty} f_n(z)$ absolut und gleichmäßig auf D .

Ist $f(z) = \sum_{n=0}^{\infty} f_n(z)$ eine gleichmäßig konvergente Reihe stetiger Funktionen $f_n: D \rightarrow \mathbb{C}$, so ist f stetig. Daraus folgt, dass für eine konvergente Folge $(a_k)_{k \in \mathbb{N}}$ die Gleichung

$$\lim_{k \rightarrow \infty} \sum_{n=0}^{\infty} f_n(a_k) = \sum_{n=0}^{\infty} \lim_{k \rightarrow \infty} f_n(a_k)$$

gilt.

Aufgabe (Frühjahr 2007, T2A1)

Sei $\varepsilon > 0$. Zeigen Sie, dass die Reihe

$$f(z) := \sum_{n=1}^{\infty} e^{in^2 z}$$

für $\operatorname{Im} z \geq \varepsilon$ gleichmäßig konvergiert, und berechnen Sie $\lim_{y \rightarrow \infty} f(iy)$.

Lösungsvorschlag zur Aufgabe (Frühjahr 2007, T2A1)

Unter Verwendung der für alle $z \in \mathbb{C}$ gültigen Formel $|e^z| = e^{\operatorname{Re} z}$ erhalten wir

$$\left| e^{in^2 z} \right| = e^{\operatorname{Re}(in^2 z)} = e^{-n^2 \operatorname{Im} z} \leq e^{-n^2 \varepsilon}.$$

Weiter ist $e^{-\varepsilon} < e^0 = 1$, sodass

$$\sum_{n=0}^{\infty} (e^{-\varepsilon})^{n^2} \leq \sum_{n=0}^{\infty} (e^{-\varepsilon})^n < \infty.$$

Dabei folgt die erste Abschätzung daraus, dass die linke Reihe eine Teilreihe der rechten Reihe ist, und die zweite Abschätzung ist eine Folgerung daraus, dass die geometrische Reihe eine konvergente Majorante der rechten Reihe ist.

Aus der gleichmäßigen Konvergenz folgt, dass Grenzwertbildung und Reihenbildung vertauscht werden dürfen, d.h. es ist

$$\lim_{y \rightarrow \infty} f(iy) = \lim_{y \rightarrow \infty} \sum_{n=1}^{\infty} e^{-n^2 y} = \sum_{n=1}^{\infty} \lim_{y \rightarrow \infty} e^{-n^2 y} = \sum_{n=0}^{\infty} 0 = 0.$$

Aufgabe (Herbst 2014, T1A2)

- a** Definieren Sie den Begriff der gleichmäßigen Konvergenz für Folgen und Reihen von komplexwertigen Funktionen auf einer Teilmenge von \mathbb{C} .
- b** Es sei $\mathbb{E} := \{z \in \mathbb{C} : |z| < 1\}$ und $f: \mathbb{E} \rightarrow \mathbb{C}$ sei holomorph mit $f(0) = 0$.
 - (i) Zeigen Sie, dass die Reihe $\sum_{n=1}^{\infty} f(z^n)$ auf jeder in \mathbb{E} enthaltenen kompakten Menge gleichmäßig konvergiert.
 - (ii) Zeigen Sie, dass die Reihe $\sum_{n=1}^{\infty} f(z^n)$ i.A. nicht gleichmäßig auf \mathbb{E} konvergiert.

Lösungsvorschlag zur Aufgabe (Herbst 2014, T1A2)

- a** Für die Definition der gleichmäßigen Konvergenz einer Folge $(f_n)_{n \in \mathbb{N}}$ siehe Definition 5.2. Die Reihe $\sum_{n=0}^{\infty} f_n$ heißt dann entsprechend gleichmäßig konvergent, wenn die Folge $(S_n)_{n \in \mathbb{N}}$ von Partialsummen

$$S_n = \sum_{k=0}^n f_k$$

lokal gleichmäßig konvergent im Sinne von 5.2 ist.

- b** (i): Da f holomorph auf \mathbb{E} ist, können wir f dort in eine Potenzreihe entwickeln, d. h. es gibt eine Folge $(a_k)_{k \in \mathbb{N}_0}$ komplexer Zahlen, sodass

$$f(z) = \sum_{k=0}^{\infty} a_k z^k \quad \text{für alle } z \in \mathbb{E}$$

gilt. Wegen $f(0) = 0$ ist dabei $a_0 = 0$. Sei $s \in \mathbb{N}$ minimal mit $a_s \neq 0$, dann ist $f(z) = z^s \sum_{k=s}^{\infty} a_k z^{k-s}$ und durch $h(z) = \sum_{k=s}^{\infty} a_k z^{k-s}$ ist wiederum eine stetige Funktion definiert. Insbesondere gilt $f(z^n) = z^{sn} h(z^n)$.

Sei nun $D \subseteq \mathbb{E}$ eine kompakte Teilmenge, dann nimmt h auf D nach dem Maximumsprinzip sein Maximum an, d. h. es gibt ein $C > 0$, sodass

$$|f(z^n)| = |z^{sn} h(z^n)| \leq |z^{sn}| \cdot C \quad \text{für alle } z \in D$$

erfüllt ist. Genauso lässt sich $|z|^s$ auf D durch ein $q > 0$ abschätzen (denn $z \mapsto z^s$ definiert ja genauso eine holomorphe Funktion, die ein Maximum auf D annehmen muss). Damit ist also $|f(z^n)| \leq q^n C$ für alle $z \in D$ und $n \in \mathbb{N}$.

Wegen $D \subseteq \mathbb{E}$ muss außerdem $q < 1$ sein, sodass $\sum_{n=0}^{\infty} q^n C$ als geometrische Reihe konvergiert. Nach Satz 6.11 konvergiert die Reihe $\sum_{n=1}^{\infty} f(z^n)$ auf D dann gleichmäßig.

(ii): Betrachte $f: \mathbb{E} \rightarrow \mathbb{C}, z \mapsto z$. Angenommen, die Reihe $\sum_{n=1}^{\infty} z^n$ konvergiert gleichmäßig auf \mathbb{E} . Da besagte Reihe (punktweise) gegen $\frac{1}{1-z} - 1$ konvergiert und aus gleichmäßiger Konvergenz insbesondere punktweise Konvergenz resultiert, folgt in Verbindung mit der Eindeutigkeit des Grenzwerts, dass $\sum_{n=1}^{\infty} z^n$ gleichmäßig gegen $\frac{1}{1-z} - 1$ konvergieren muss. Genauer gesagt: Die Folge der Partialsummen $S_n = \sum_{k=0}^n z^k$ konvergiert

gleichmäßig gegen $\frac{1}{1-z} - 1$. Unter Verwendung der Formel für die Partialsummen der geometrischen Reihe ist nun

$$\delta_n(z) := \left| \frac{1}{1-z} - 1 - S_n \right| = \left| \frac{1}{1-z} - 1 - \left(\frac{1-z^{n+1}}{1-z} - 1 \right) \right| = \left| \frac{z^{n+1}}{1-z} \right|.$$

Es müsste nun für jedes $\varepsilon > 0$ ein $N \in \mathbb{N}$ geben, sodass $\delta_n(z) < \varepsilon$ für $n \geq N$ und alle $z \in \mathbb{E}$ gilt. Wegen $\lim_{z \rightarrow 1} \delta_n(z) = \lim_{z \rightarrow 1} \frac{z^{n+1}}{1-z} = \infty$ können wir jedoch immer $z \in \mathbb{E}$ wählen, sodass $\delta_n(z) > \varepsilon$. Daher kann $\sum_{n=1}^{\infty} z^n$ nicht gleichmäßig auf \mathbb{E} konvergieren.

Laurentreihen

Wir haben uns bisher ausschließlich mit holomorphen Funktionen befasst und diese innerhalb von Kreisgebieten $B_r(a)$ in Reihen entwickelt. Besitzt eine Funktion Singularitäten in einem solchen Kreisgebiet, so kann man versuchen, diese Singularitäten „auszuschneiden“. Möglicherweise ist die Funktion dann zumindest noch auf einem Ringgebiet der Form

$$K_{r,R}(a) = \{z \in \mathbb{C} \mid r < |z - a| < R\}$$

holomorph. Für diesen Fall gibt es ebenfalls eine Reihenentwicklung, die die bekannte Potenzreihendarstellung verallgemeinert.

Satz 6.12 (Laurentzerlegung). Seien $a \in \mathbb{C}$ und $0 \leq r < R \leq \infty$ reelle Zahlen, wobei auch $r = 0$ und $R = \infty$ zugelassen sind. Ist $f: K_{r,R}(a) \rightarrow \mathbb{C}$ holomorph, so gibt es eindeutig festgelegte holomorphe Funktionen

$$f_h: K_{r,\infty}(a) \rightarrow \mathbb{C} \quad \text{und} \quad f_n: B_R(a) \rightarrow \mathbb{C}$$

mit $f = f_h + f_n$ auf $K_{r,R}(a) = B_R(a) \cap K_{r,\infty}(a)$ und $\lim_{|z| \rightarrow \infty} |f_h(z)| = 0$. Man nennt f_h den **Haupt-** und f_n den **Nebenteil** von f .

Wir betrachten nun eine Laurentzerlegung einer Funktion $f: K_{r,R}(a) \rightarrow \mathbb{C}$, wobei wir der Einfachheit wegen $a = 0$ setzen. Da f_n auf $B_R(0)$ holomorph ist, gibt es eine komplexe Folge $(a_k)_{k \in \mathbb{N}_0}$, sodass $f_n(z) = \sum_{k=0}^{\infty} a_k z^k$ für alle $z \in B_R(0)$ erfüllt ist. Der Hauptteil ist für alle $z \in \mathbb{C}$ mit $|z| > r$ holomorph, also ist $z \mapsto f_h(\frac{1}{z})$ auf $B_{\frac{1}{r}}(0)$ holomorph, sodass es eine Darstellung

$$f_h\left(\frac{1}{z}\right) = \sum_{k=0}^{\infty} b_k z^k \quad \text{für } z \in B_{\frac{1}{r}}(0)$$

gibt. Wegen $\lim_{|z| \rightarrow \infty} |f_h(z)| = 0$ ist dabei $b_0 = 0$. Nun gilt also

$$f_h(z) = \sum_{k=1}^{\infty} b_k \left(\frac{1}{z}\right)^k$$

und wir finden für $z \in K_{r,R}(0)$ die Darstellung

$$f(z) = f_n(z) + f_h(z) = \sum_{k=0}^{\infty} a_k z^k + \sum_{k=1}^{\infty} b_k \left(\frac{1}{z}\right)^k = \sum_{k=-\infty}^{\infty} a_k z^k,$$

wobei wir $a_k = b_k$ für $k < 0$ setzen.

Proposition 6.13 (Laurententwicklung). Eine auf $K_{r,R}(a)$ holomorphe Funktion besitzt eine auf dem gesamten Definitionsbereich gültige Reihenentwicklung der Form

$$f(z) = \sum_{k=-\infty}^{\infty} a_k (z-a)^k,$$

welche *Laurentreihe* von f genannt wird. Dabei konvergiert die Teilsumme von $k = -\infty$ bis $k = -1$ lokal gleichmäßig absolut gegen den Hauptteil und die Teilsumme von $k = 0$ bis $k = \infty$ lokal gleichmäßig absolut gegen den Nebenteil von f . Für die Koeffizienten gilt

$$a_k = \frac{1}{2\pi i} \int_{\partial B_\rho(a)} \frac{f(\omega)}{(\omega-a)^{k+1}} d\omega$$

mit einem $r < \rho < R$ und $k \in \mathbb{Z}$.

Man überprüft unmittelbar, dass man im Spezialfall einer holomorphen Funktion $B_R(a)$ die bekannte Potenzreihenentwicklung zurückgewinnt. Außerdem folgt direkt aus der Formel zur Bestimmung der Koeffizienten, dass

$$a_{-1} = \frac{1}{2\pi i} \int_{\partial B_\rho(a)} f(\omega) d\omega = \text{Res}(f; a)$$

gilt.³

³ Die Definition des Residuums $\text{Res}(f; a)$ ist auf Seite 331 zu finden.

Anleitung: Laurententwicklungen bestimmen

Zur Bestimmung von Laurentreihen vermeidet man, wenn möglich, die Bestimmung der Koeffizienten über die Formel aus Satz 6.13, sondern versucht, auf bereits bekannte Potenzreihenentwicklungen zurückzugreifen. Dazu sollte man die folgenden Reihen (mit Entwicklungspunkt 0) parat haben:

$$\text{Geometrische Reihe: } \frac{1}{1-z} = \sum_{n=0}^{\infty} z^n \quad \text{für } |z| < 1,$$

$$\text{Exponentialreihe: } \exp(z) = \sum_{n=0}^{\infty} \frac{1}{n!} z^n \quad \text{für } z \in \mathbb{C},$$

$$\text{Sinusreihe: } \sin(z) = \sum_{n=0}^{\infty} (-1)^n \frac{z^{2n+1}}{(2n+1)!} \quad \text{für } z \in \mathbb{C},$$

$$\text{Kosinusreihe: } \cos(z) = \sum_{n=0}^{\infty} (-1)^n \frac{z^{2n}}{(2n)!} \quad \text{für } z \in \mathbb{C}.$$

Um diese bekannten Reihendarstellung verwenden zu können, könnte außerdem hilfreich sein:

- „Freund und Feind“: Entwickelt man um z_0 und enthält der Funktionsterm bereits den Faktor $(z - z_0)$ („Freund“), so entwickelt man zunächst den anderen Faktor („Feind“) in eine Reihe $\sum_{k=0}^{\infty} a_n(z - z_0)^n$ und kann dann den ersten Linearfaktor einfach mit der Reihe multiplizieren.
- Partialbruchzerlegung: Bei einer Funktion mit Polen, z. B. $\frac{1}{(z-a_1)(z-a_2)}$ kann man den Ansatz

$$\frac{1}{(z-a_1)(z-a_2)} = \frac{A}{z-a_1} + \frac{B}{z-a_2} = \frac{z(A+B) - (a_2A+a_1B)}{(z-a_1)(z-a_2)}$$

machen und die Koeffizienten $A, B \in \mathbb{C}$ aus den Gleichungen $A + B = 0$ und $a_2A + a_1B = -1$ bestimmen. Genauso verfährt man im Fall mehrerer Pole.

- Bei Polen höherer Ordnung kann gliedweises Differenzieren viel Arbeit ersparen, denn es ist

$$\frac{d^n}{dz^n} \left(\frac{1}{z-a} \right) = \frac{(-1)^n n!}{(z-a)^{n+1}}$$

- Für die Entwicklung in Ringgebieten $K_{r,R}(a)$ ist es häufig nützlich, die geometrische Reihe für das Argument $\frac{1}{r(z-a)}$ anzubringen, denn für $z \in K_{r,R}(a)$ ist $\left| \frac{1}{r(z-a)} \right| < 1$.

Aufgabe (Herbst 2010, T2A3)

Man bestimme die Laurent-Entwicklung von

$f(z) := \frac{z}{(z-1)(z-2)}$ in der Kreisscheibe $\{z \in \mathbb{C} \mid |z| < 1\}$ und in den Kreisringen $\{z \in \mathbb{C} \mid 1 < |z| < 2\}$ und $\{z \in \mathbb{C} \mid 2 < |z|\}$.

Hinweis Man verwende Partialbruchzerlegung.

Lösungsvorschlag zur Aufgabe (Herbst 2010, T2A3)

Dem Hinweis folgend verwenden wir zunächst Partialbruchzerlegung. Dazu machen wir den Ansatz

$$\frac{z}{(z-1)(z-2)} = \frac{A}{z-1} + \frac{B}{z-2} = \frac{z(A+B)-(B+2A)}{(z-1)(z-2)}$$

und finden die Gleichungen $-(B+2A) = 0$ sowie $A+B = 1$. Als Lösung erhält man $B = 2$ und $A = -1$. Also ist

$$f(z) = \frac{z}{(z-1)(z-2)} = \frac{-1}{z-1} + \frac{2}{z-2}.$$

Für $z \in B_1(0)$ gilt $|z| < 1$ bzw. $|z/2| < 1$, also können wir die geometrische Reihe verwenden und erhalten die dort gültige Reihendarstellung

$$\frac{-1}{z-1} + \frac{2}{z-2} = \frac{1}{1-z} - \frac{1}{1-\frac{z}{2}} = \sum_{k=0}^{\infty} z^k - \sum_{k=0}^{\infty} \left(\frac{z}{2}\right)^k = \sum_{k=0}^{\infty} (1-2^{-k})z^k.$$

Ist nun $z \in \mathbb{C}$ mit $1 < |z| < 2$, so ist immerhin $|z/2| < 1$ und $|1/z| < 1$, d. h. die geometrische Reihe liefert uns hier

$$\begin{aligned} \frac{-1}{z-1} + \frac{2}{z-2} &= -\frac{1}{z} \frac{1}{1-\frac{1}{z}} - \frac{1}{1-\frac{z}{2}} = -\frac{1}{z} \sum_{k=0}^{\infty} z^{-k} - \sum_{k=0}^{\infty} 2^{-k}z^k = \\ &= -\sum_{k=0}^{\infty} z^{-(k+1)} - \sum_{k=0}^{\infty} 2^{-k}z^k = -\sum_{k=1}^{\infty} z^{-k} - \sum_{k=0}^{\infty} 2^{-k}z^k. \end{aligned}$$

Im Fall $|z| > 2$ haben wir $|1/z| < \frac{1}{2}$ und $|2/z| < 1$, auch hier verwenden wir die geometrische Reihe:

$$\begin{aligned} \frac{-1}{z-1} + \frac{2}{z-2} &= -\frac{1}{z} \frac{1}{1-\frac{1}{z}} + \frac{2}{z} \frac{1}{1-\frac{2}{z}} = -\frac{1}{z} \sum_{k=0}^{\infty} z^{-k} + \frac{2}{z} \sum_{k=0}^{\infty} 2^k z^{-k} = \\ &= -\sum_{k=0}^{\infty} z^{-(k+1)} + \sum_{k=0}^{\infty} 2^{k+1} z^{-(k+1)} = -\sum_{k=1}^{\infty} z^k + \sum_{k=1}^{\infty} 2^k z^k = \sum_{k=1}^{\infty} (-1 + 2^k) z^{-k} \end{aligned}$$

Aufgabe (Herbst 2012, T3A5)

Mit $z_0 = 1 + i$ sei folgende rationale Funktion definiert:

$$f(z) = \frac{1}{(z-1)(z_0-z)^3} \quad (z \in \mathbb{C} \setminus \{1, z_0\}).$$

Bestimmen Sie (am einfachsten mit Hilfe der geometrischen Reihe) jeweils die Laurent-Reihen von f um $z = z_0$ bzw. um $z = 1$ mit ihren maximalen Konvergenzringen. Geben Sie jeweils die Hauptteile der Reihen an.

Lösungsvorschlag zur Aufgabe (Herbst 2012, T3A5)

Wir bestimmen zunächst die Laurent-Reihe um $z = 1$. Es ist

$$\frac{1}{z_0 - z} = \frac{1}{1+i-z} = \frac{1}{i-(z-1)} = \frac{1}{i} \cdot \frac{1}{1-\frac{z-1}{i}} = -i \cdot \sum_{k=0}^{\infty} \left(\frac{z-1}{i}\right)^k,$$

wobei wir freimütig $|\frac{z-1}{i}| < 1$ vorausgesetzt haben, um im letzten Schritt die geometrische Reihe zu erhalten. Bemerke nun, dass

$$\frac{d}{dz} \left(\frac{1}{z_0 - z} \right) = \frac{1}{(z_0 - z)^2} \quad \text{und} \quad \frac{d^2}{dz^2} \left(\frac{1}{z_0 - z} \right) = \frac{2}{(z_0 - z)^3}.$$

Nun können wir gliedweises Differenzieren verwenden (vgl. (1) auf Seite 285):

$$\frac{1}{(z_0 - z)^3} = \frac{-i}{2} \frac{d^2}{dz^2} \sum_{k=0}^{\infty} \left(\frac{z-1}{i}\right)^k = \frac{-i}{2} \sum_{k=2}^{\infty} (-i)^k \cdot k(k-1) \cdot (z-1)^{k-2}.$$

Wir erhalten also

$$\begin{aligned} \frac{1}{(z-1)(z_0-z)^3} &= (z-1)^{-1} \cdot \frac{-i}{2} \sum_{k=2}^{\infty} (-i)^k \cdot k(k-1) \cdot (z-1)^{k-2} = \\ &= \frac{-i}{2} \sum_{k=2}^{\infty} (-i)^k \cdot k(k-1) \cdot (z-1)^{k-3} = \\ &= \frac{-i}{2} \sum_{k=-1}^{\infty} (-i)^{k+3} (k+3)(k+2)(z-1)^k = \\ &= \sum_{k=-1}^{\infty} \frac{1}{2} (-i)^k (k+3)(k+2)(z-1)^k \end{aligned}$$

Der Hauptteil dieser Reihe ist $\frac{2 \cdot 1}{-2i} \cdot \frac{1}{z-1} = \frac{i}{z-1}$ und der Konvergenzradius des Nebenteils ist nach Proposition 6.9 (2)

$$\lim_{k \rightarrow \infty} \frac{(k+3)(k+2)}{(k+4)(k+3)} = 1.$$

Da der Hauptteil auf $\mathbb{C} \setminus \{1\}$ konvergiert, ist der maximale Konvergenzring $B_1(1) \setminus \{1\} = K_{0,1}(1)$.

Zur Bestimmung der Laurentreihe im Fall $z = z_0$ verfahren wir genauso:

$$\begin{aligned} \frac{1}{(z-1)(z_0-z)^3} &= (z_0-z)^{-3} \cdot \frac{1}{(z_0-1)-(z_0-z)} = \\ &= (z_0-z)^{-3} \cdot \frac{1}{i} \cdot \frac{1}{1-\frac{z_0-z}{i}} = \\ &= -i(z_0-z)^{-3} \cdot \sum_{k=0}^{\infty} \left(\frac{z_0-z}{i}\right)^k = -i \sum_{k=0}^{\infty} (-i)^k (z_0-z)^{k-3} = \\ &= \sum_{k=-3}^{\infty} (-i) \cdot (-i)^{k+3} \cdot (z-z_0)^k = \sum_{k=-3}^{\infty} (-i)^k (z-z_0)^k \end{aligned}$$

Auch hier ist der Konvergenzradius 1 und der Hauptteil dieser Reihe ist $\frac{-i}{(z-z_0)^3} + \frac{-1}{(z-z_0)^2} + \frac{i}{(z-z_0)}$. Der maximale Konvergenzring ist daher $B_1(z_0) \setminus \{z_0\} = K_{0,1}(z_0)$.

Aufgabe (Frühjahr 2007, T1A4)

Geben Sie die Laurent-Entwicklung für $f(z) = \frac{1}{z^2+1}$ in den folgenden Ringgebieten an:

$$R := \{z \in \mathbb{C} \mid 0 < |z-i| < 2\} \quad \text{und} \quad \tilde{R} := \{z \in \mathbb{C} \mid |z| > 1\}.$$

Lösungsvorschlag zur Aufgabe (Frühjahr 2007, T1A4)

Wegen $z^2 + 1 = (z-i)(z+i)$ enthält der Nenner im ersten Fall den „Freund“ $(z-i)$. Wir entwickeln daher zunächst den „Feind“:

$$\frac{1}{z+i} = \frac{1}{(z-i)+2i} = \frac{1}{2i} \frac{1}{1-\left(-\frac{z-i}{2i}\right)} = \frac{1}{2i} \sum_{k=0}^{\infty} \left(-\frac{z-i}{2i}\right)^k.$$

Dabei haben wir im letzten Schritt verwendet, dass wegen $|z - i| < 2$ die Ungleichung $\left|\frac{z-i}{2i}\right| < 1$ gilt und die geometrische Reihe angewendet werden kann. Nun erhalten wir

$$\begin{aligned} f(z) &= (z - i)^{-1} \frac{1}{2i} \sum_{k=0}^{\infty} \left(-\frac{z-i}{2i}\right)^k = \sum_{k=0}^{\infty} (-1)^k \left(\frac{1}{2i}\right)^{k+1} (z-i)^{k-1} = \\ &= \sum_{k=-1}^{\infty} (-1)^{k+1} \left(\frac{i}{2}\right)^{k+2} (z-i)^k = \frac{1}{4} \sum_{k=-1}^{\infty} (-1)^k \left(\frac{i}{2}\right)^k (z-i)^k \end{aligned}$$

Für die zweite Laurententwicklung müssen wir um 0 entwickeln. Dazu bemerken wir, dass für $z \in \tilde{R}$ die Ungleichung $|1/z^2| < 1$ erfüllt ist. Somit liefert die geometrische Reihe hier

$$f(z) = \frac{1}{z^2} \cdot \frac{1}{1 - \left(\frac{-1}{z^2}\right)} = \frac{1}{z^2} \cdot \sum_{k=0}^{\infty} \left(\frac{-1}{z^2}\right)^k = \sum_{k=0}^{\infty} (-1)^k z^{-(2k+2)} = \sum_{k=1}^{\infty} (-1)^{k-1} z^{-2k}.$$

Klassifikation von Singularitäten anhand von Laurentreihen

Definition 6.14. Sei $U \subseteq \mathbb{C}$ offen und $f: U \rightarrow \mathbb{C}$ eine holomorphe Funktion. Dann werden die Punkte in $\mathbb{C} \setminus U$ als *Singularitäten* von f bezeichnet. Eine Singularität $a \in \mathbb{C} \setminus U$ heißt *isolierte Singularität*, falls es eine offene Umgebung $V \subseteq \mathbb{C}$ gibt, sodass $(\mathbb{C} \setminus U) \cap V = \{a\}$ erfüllt ist.

Eine isolierte Singularität a nennt man

- (1) *hebbar*, wenn auf $U \cup \{a\}$ eine *holomorphe Fortsetzung* von f existiert, d. h. eine holomorphe Funktion $\hat{f}: U \cup \{a\} \rightarrow \mathbb{C}$ mit $\hat{f}(z) = f(z)$ für $z \in U$,
- (2) eine *Polstelle* der Ordnung n , falls $\lim_{z \rightarrow a} |(z-a)^k f(z)| = \infty$ für alle $k \in \{0, 1, \dots, n-1\}$ ist und $\lim_{z \rightarrow a} (z-a)^n f(z)$ existiert,
- (3) eine *wesentliche Singularität*, wenn sie weder hebbar noch eine Polstelle ist.

Ein weiteres nützliches Kriterium dafür, dass $\frac{f}{g}$ einen Pol der Ordnung k in a hat, ist, dass es eine offene Umgebung $V \subseteq \mathbb{C}$ von a gibt, sodass $f: V \rightarrow \mathbb{C}$ und $g: V \rightarrow \mathbb{C}$ holomorph sind, $f(a) \neq 0$, $g(z) \neq 0$ für $z \in V \setminus \{a\}$ und g hat eine Nullstelle der Ordnung k in a . Letzteres bedeutet, dass $g(z) = (z-a)^k h(z)$ für alle $z \in V$ und $h(a) \neq 0$.

Satz 6.15 (Riemannscher Hebbarkeitssatz). Eine isolierte Singularität a einer Funktion f ist genau dann hebbar, wenn f in einer punktierten Umgebung von a beschränkt ist.

Die Laurentreihen einer Entwicklung um die fragliche Singularität erlaubt es, deren Typ direkt anhand der Koeffizienten zu bestimmen.

Satz 6.16. Sei $U \subseteq \mathbb{C}$ und $f: U \rightarrow \mathbb{C}$ eine Funktion mit isolierter Singularität $a \in \mathbb{C} \setminus U$ und auf dem Kreisring $K_{r,R}(a) \subseteq U$ gültiger Laurent-Entwicklung

$$f(z) = \sum_{k=-\infty}^{\infty} a_k(z-a)^k.$$

- (1) Die Singularität a ist genau dann hebbbar, wenn $a_k = 0$ für alle $k < 0$ gilt.
- (2) a ist eine Polstelle der Ordnung n dann und nur dann, wenn $a_{-n} \neq 0$ und $a_k = 0$ für alle $k < -n$ gilt.
- (3) Genau dann ist a eine wesentliche Singularität, wenn $a_k \neq 0$ für unendlich viele $k \leq 0$ erfüllt ist.

Den nächsten Satz könnte man so zusammenfassen, dass Funktionen in der Nähe von wesentlichen Singularitäten „verrückt spielen“.

Satz 6.17 (Casorati-Weierstraß). Sei $f: U \rightarrow \mathbb{C}$ eine holomorphe Funktion mit einer wesentlichen Singularität in $a \in \mathbb{C}$. Dann ist das Bild jeder offenen Umgebung von a dicht in \mathbb{C} .

Dies liefert eine weitere Möglichkeit, wesentliche Singularitäten zu klassifizieren:

Proposition 6.18. Die isolierte Singularität a einer holomorphen Funktion $f: U \rightarrow \mathbb{C}$ ist genau dann wesentlich, wenn zwei konvergente Folgen $(u_n)_{n \in \mathbb{N}}, (v_n)_{n \in \mathbb{N}}$ mit $\lim_{n \rightarrow \infty} u_n = \lim_{n \rightarrow \infty} v_n$ existieren, deren Bildfolgen gegen verschiedene Werte konvergieren, also $\lim_{n \rightarrow \infty} f(u_n) \neq \lim_{n \rightarrow \infty} f(v_n)$.

Wäre die Singularität a hebbbar, so müssten nämlich beide Bildfolgen gegen den Wert der holomorphen Fortsetzung konvergieren. Wäre a hingegen ein Pol, so müssten beide Bildfolgen divergieren. Umgekehrt kann die Existenz solcher Folgen aus dem Satz von Casorati-Weierstraß gefolgert werden, da in einer immer kleiner werdenden Umgebung von a Werte gewählt werden können, die einem beliebig vorgegebenen Wert beliebig nahe kommen.

Aufgabe (Herbst 2008, T1A1)

Bestimmen Sie für die folgenden Funktionen f im Punkt a die Art der Singularität von f in a . Geben Sie bei hebbaren Singularitäten den Grenzwert von f in a , bei Polen den Hauptteil und bei wesentlichen Singularitäten das Residuum an.

a) $f: \mathbb{C} \setminus \{\pm i\} \rightarrow \mathbb{C}, \quad f(z) = \frac{z^3 - 5z + 6i}{z^2 + 1}, \quad a = i,$

b $f: \mathbb{C} \setminus 2\pi i \mathbb{Z} \rightarrow \mathbb{C}, \quad f(z) = \frac{1}{\exp(z) - 1}, \quad a = 2\pi i,$

c $f: \mathbb{C}^\times \rightarrow \mathbb{C}, \quad f(z) = \cos\left(\frac{1}{z}\right), \quad a = 0,$

Lösungsvorschlag zur Aufgabe (Herbst 2008, T1A1)

a Wir bemerken, dass

$$i^3 - 5i + 6i = -i - 5i + 6i = 0$$

gilt, sodass man aus dem Polynom $z^3 - 5z + 6i$ den Faktor $(z - i)$ herausfaktorisieren kann. Dazu sieht man entweder

$$\begin{aligned} z^3 - 5z + 6i &= z^3 + z - 6z + 6i = z(z^2 + 1) - 6(z - i) = \\ &= z(z + i)(z - i) - 6(z - i) = (z - i)(z(z + i) - 6) \end{aligned}$$

oder man führt einfach eine Polynomdivision durch. Folglich ist

$$\lim_{z \rightarrow i} f(z) = \lim_{z \rightarrow i} \frac{z^3 - 5z + 6i}{z^2 + 1} = \lim_{z \rightarrow i} \frac{z(z + i) - 6}{z + i} = \frac{2i^2 - 6}{2i} = \frac{-4}{i} = 4i,$$

sodass es sich bei i um eine hebbare Singularität von f handelt.

b Aufgrund der Periodizität der Exponentialfunktion können wir genauso gut $a = 0$ betrachten. Es ist

$$e^z - 1 = \sum_{k=0}^{\infty} \frac{z^k}{k!} - 1 = \sum_{k=1}^{\infty} \frac{z^k}{k!} = z \sum_{k=1}^{\infty} \frac{z^{k-1}}{k!} = z \sum_{k=0}^{\infty} \frac{z^k}{(k+1)!}$$

und für die letzte Summe $g(z) = \sum_{k=0}^{\infty} \frac{z^k}{(k+1)!}$ gilt $g(0) = 1$. Somit hat $f(z) = \frac{1}{e^z - 1} = \frac{1}{zg(z)}$ bei 0 einen Pol erster Ordnung. Der Hauptteil bei 0 ist $\frac{1}{z} \cdot g(0) = \frac{1}{z}$, somit ist der Hauptteil bei $2\pi i$ aufgrund der angesprochenen Periodizität durch $\frac{1}{(z - 2\pi i)}$ gegeben.

c Hier verwenden wir die Kosinusreihe und erhalten

$$\cos\left(\frac{1}{z}\right) = \sum_{k=0}^{\infty} (-1)^k \frac{\left(\frac{1}{z}\right)^{2k}}{(2k)!} = \sum_{k=-\infty}^0 (-1)^k \frac{z^{2k}}{(-2k)!}.$$

Da für alle geraden $k < 0$ der jeweilige Koeffizient $a_k = (-1)^{k/2} \frac{1}{(-k)!} \neq 0$ ist, ist 0 eine wesentliche Singularität von f . Allerdings taucht der Summand z^{-1} nicht auf (nur gerade Exponenten), sodass für das zugehörige Residuum

$$\text{Res}(f; 0) = a_{-1} = 0$$

gilt.

Aufgabe (Frühjahr 2009, T2A5)

Bestimmen Sie Formeln zur rekursiven Berechnung der Koeffizienten der Laurentreihe um $z = 0$ für die Funktion

$$f(z) = \frac{1}{e^z - 1}$$

und berechnen Sie die drei ersten Koeffizienten (die von $z^{-1}, 1, z$) explizit.

Lösungsvorschlag zur Aufgabe (Frühjahr 2009, T2A5)

Zunächst sehen wir, dass

$$e^z - 1 = \sum_{k=0}^{\infty} \frac{z^k}{k!} - 1 = \sum_{k=1}^{\infty} \frac{z^k}{k!} = z \sum_{k=1}^{\infty} \frac{z^{k-1}}{k!} = z \sum_{k=0}^{\infty} \frac{z^k}{(k+1)!}$$

gilt. Wertet man die letzte Summe $g(z) = \sum_{k=0}^{\infty} \frac{z^k}{(k+1)!}$ bei 0 aus, so erhält man $g(0) = 1$. Somit hat $f(z) = \frac{1}{e^z - 1} = \frac{1}{zg(z)}$ bei 0 einen Pol erster Ordnung. Wir machen daher den Ansatz $f(z) = \sum_{k=-1}^{\infty} a_k z^k$, dann muss unter Verwendung der Exponentialreihe gelten:

$$1 = f(z) \cdot (e^z - 1) = \left(\sum_{k=-1}^{\infty} a_k z^k \right) \cdot \left(\sum_{k=1}^{\infty} \frac{1}{k!} z^k \right) = \sum_{k=-\infty}^{\infty} \left(\sum_{n=1}^{k+1} a_{k-n} \frac{1}{n!} \right) z^k$$

Koeffizientenvergleich ergibt daher

$$1 = \sum_{n=1}^1 \frac{a_{-n}}{n!} = a_{-1} \quad \text{und} \quad 0 = \sum_{n=1}^{k+1} \frac{a_{k-n}}{n!} \quad \text{für } k > 0,$$

wobei wir das Produkt von Reihen auf Seite 285 verwendet haben.

Für $k = 1$ bzw. $k = 2$ ergibt die rechte Gleichung

$$\begin{aligned} 0 &= \frac{a_{1-1}}{1!} + \frac{a_{1-2}}{2!} = a_0 + \frac{a_{-1}}{2} \quad \Leftrightarrow \quad a_0 = -\frac{1}{2}a_{-1} = -\frac{1}{2}, \\ 0 &= \frac{a_{2-1}}{1!} + \frac{a_{2-2}}{2!} + \frac{a_{2-3}}{3!} = a_1 + \frac{1}{2}a_0 + \frac{1}{6}a_{-1} \\ \Leftrightarrow \quad a_1 &= -\frac{1}{2}a_0 - \frac{1}{6}a_{-1} = \frac{1}{4} - \frac{1}{6} = \frac{1}{12}. \end{aligned}$$

Die Rekursionformel für die übrigen Koeffizienten bestimmt sich aus

$$0 = \sum_{n=1}^{k+1} \frac{a_{k-n}}{n!} \quad \Leftrightarrow \quad a_{k-1} = - \sum_{n=2}^{k+1} \frac{a_{k-n}}{n!} = - \sum_{n=-1}^{k-2} \frac{a_n}{(k-n)!}$$

zu $a_k = - \sum_{n=-1}^{k-1} \frac{a_n}{(k+1-n)!}$ für $k > 1$.

6.3. Identitätssatz

Der Identitätssatz ist einer der Sätze, die verdeutlichen, dass der Begriff der Holomorphie wesentlich stärker als der der reellen Differenzierbarkeit ist. Er besagt, dass Funktionen, die nur auf einer kleinen Menge übereinstimmen, bereits auf ihrem gesamten Definitionsbereich identisch sind. Wir geben zunächst eine explizite Formulierung des Satzes.

Satz 6.19 (Identitätssatz). Sei $G \subseteq \mathbb{C}$ ein Gebiet und seien $f, g: G \rightarrow \mathbb{C}$ holomorphe Abbildungen. Folgende Aussagen sind äquivalent:

- (1) Es gilt $f|_N = g|_N$ für eine Menge $N \subseteq G$, die einen Häufungspunkt in G besitzt.
- (2) Es gibt einen Punkt $a \in G$ mit $f^{(n)}(a) = g^{(n)}(a)$ für $n \in \mathbb{N}_0$.
- (3) $f = g$.

Ein **Gebiet** ist dabei eine nicht-leere, offene und zusammenhängende Teilmenge von \mathbb{C} . Man beachte, dass der Satz falsch wird, wenn die Funktionen nicht auf einer solchen Menge definiert sind (vgl. H06T3A2 auf Seite 310).

Zur Erinnerung: Einen Punkt $a \in G$ nennt man **Häufungspunkt** der Menge N , wenn in jeder beliebigen offenen Umgebung V von a mindestens ein Punkt von N ungleich a liegt. Man weist dies in der Regel nach, indem man eine Folge $(z_n)_{n \in \mathbb{N}}$ mit $z_n \in N$, aber $z_n \neq a$ für fast alle $n \in \mathbb{N}$ angibt, die gegen a konvergiert. Dann liegen nach Definition der Konvergenz sogar unendlich viele Punkte von N in jeder Umgebung von a . In einer offenen Menge ist jeder Punkt ein Häufungspunkt.

Eng verwandt zum Häufungspunkt einer *Menge* ist der Begriff des Häufungspunkts einer *Folge*, welcher der Grenzwert einer Teilfolge ist. Diese beiden Begriffe sollten jedoch nicht verwechselt werden.

Zum Identitätssatz findet man mehrere äquivalente Formulierungen. Hin und wieder wird bei (1) auch die vermeintlich stärkere Forderung gestellt, dass N eine *nicht-diskrete* Teilmenge ist, also eine Menge, die selbst einen Häufungspunkt enthält (man beachte den Unterschied zum Satz oben, bei dem der Häufungspunkt nur im Gebiet, auf dem f und g definiert sind, liegen muss). Tatsächlich sind beide Formulierungen äquivalent: Sei nämlich N eine Menge mit Häufungspunkt $a \in G$, $f|_N = g|_N$ und $(z_n)_{n \in \mathbb{N}}$ eine Folge wie im letzten Absatz. Aufgrund der Stetigkeit von f und g erhält man dann auch

$$f(a) = f\left(\lim_{n \rightarrow \infty} z_n\right) = \lim_{n \rightarrow \infty} f(z_n) = \lim_{n \rightarrow \infty} g(z_n) = g\left(\lim_{n \rightarrow \infty} z_n\right) = g(a),$$

sodass f und g sogar auf der Menge $N \cup \{a\}$ übereinstimmen, die den Häufungspunkt a enthält.

Aufgabe (Frühjahr 2004, T1A2)

Sei $f : \mathbb{C} \setminus \{-i\} \rightarrow \mathbb{C}$ definiert durch

$$f(z) := \sin\left(\frac{1}{1-iz}\right)$$

- a** Zeigen Sie, dass f holomorph ist und Nullstellen in den Punkten $-i + i \frac{1}{k\pi}$ mit $k \in \mathbb{N}$ besitzt, aber nicht identisch Null ist.
- b** Warum widerspricht das Ergebnis aus **a** nicht dem Identitätssatz?
- c** Bestimmen Sie den Konvergenzradius der Potenzreihenentwicklung von f um 0.

Lösungsvorschlag zur Aufgabe (Frühjahr 2004, T1A2)

- a** Die Abbildung $z \mapsto 1 - iz$ ist als Polynom auf ganz \mathbb{C} holomorph, zudem gilt $1 - iz \neq 0$ für $z \neq -i$, sodass nach der Quotientenregel auch die Abbildung $z \mapsto \frac{1}{1-iz}$ auf $\mathbb{C} \setminus \{-i\}$ holomorph ist. Da die Sinus-Funktion auf ganz \mathbb{C} holomorph ist, folgt mit der Kettenregel die Holomorphie von f .

Wir berechnen für $k \in \mathbb{N}$:

$$f\left(-i + \frac{i}{k\pi}\right) = \sin\left(\frac{1}{1 - i(-i + \frac{i}{k\pi})}\right) = \sin\left(\frac{1}{1 - 1 + \frac{1}{k\pi}}\right) = \sin(k\pi) = 0.$$

Um zu zeigen, dass f nicht die Nullabbildung ist, betrachte

$$f\left(-i + \frac{2i}{\pi}\right) = \sin\left(\frac{1}{1 - i(-i + \frac{2i}{\pi})}\right) = \sin\left(\frac{1}{\frac{1}{2} + \frac{1}{\pi}}\right) = \sin\left(\frac{\pi}{2}\right) = 1 \neq 0.$$

- b** Die Menge $\mathbb{C} \setminus \{-i\}$ ist ein Gebiet und die Funktionen f sowie $z \mapsto 0$ sind holomorph. Sie stimmen auf der Menge $N = \{-i + \frac{i}{k\pi} \mid k \in \mathbb{N}\}$ überein. Das Problem ist der Häufungspunkt der Menge: N hat nur den Häufungspunkt $-i$, dieser ist nicht im Definitionsbereich von f enthalten, sodass nicht alle Voraussetzungen des Identitätssatzes erfüllt sind.
- c** Sei $r \geq 0$ der Konvergenzradius der Potenzreihenentwicklung von f um 0. Wäre $r > 1$, so würde $-i$ in der Konvergenzkreisscheibe $B_r(0)$ liegen, sodass besagte Potenzreihe eine holomorphe Fortsetzung von f auf $B_r(0)$ wäre. Da jedoch der Grenzwert

$$\lim_{k \rightarrow \infty} f\left(-i + i \frac{1}{\frac{\pi}{2} + k\pi}\right) = \lim_{k \rightarrow \infty} \sin\left(\frac{\pi}{2} + k\pi\right) = \lim_{k \rightarrow \infty} (-1)^k$$

nicht existiert, kann die Singularität bei $-i$ nicht hebbbar sein. Also muss $r \leq 1$ gelten.

Andererseits liegt $B_1(0)$ vollständig im Definitionsbereich von f , sodass sich f dort nach Satz 6.10 in eine Potenzreihe entwickeln lässt. Zusammen ergibt das, dass der Konvergenzradius der Potenzreihenentwicklung von f um 0 gerade 1 betragen muss.

Aufgabe (Herbst 2014, T1A1)

Es sei $G \subseteq \mathbb{C}$ ein nicht-leeres Gebiet und $f, g: G \rightarrow \mathbb{C}$ seien holomorph mit $f' = gf$.

Zeigen Sie: Hat f eine Nullstelle in G , so ist $f(z) = 0$ für alle $z \in G$.

Lösungsvorschlag zur Aufgabe (Herbst 2014, T1A1)

Sei $a \in G$ eine Nullstelle von f . Wir zeigen

$$f^{(n)}(a) = 0. \quad \text{für alle } n \in \mathbb{N}_0. \quad (\star)$$

Wir beweisen die Aussage durch Induktion über n :

Induktionsanfang: Für $n = 0$ gilt $f(a) = 0$, da a laut unserer Voraussetzung Nullstelle von f ist.

Induktionsschritt: Nehmen wir an, dass $f^{(n)}(a) = 0$ für $n \in \mathbb{N}_0$ bereits bewiesen ist. Es folgt:

$$f^{(n+1)}(a) = (gf)^{(n)}(a) = \sum_{k=0}^n \binom{n}{k} g^{(k)} f^{(n-k)}(a) \stackrel{(I.V.)}{=} 0.$$

Hierbei haben wir an der Stelle (I.V.) die Induktionsvoraussetzung $f^{(n-k)}(a) = 0$ für $k \in \{0, \dots, n\}$ und bei der zweiten Umformung die sogenannte *Leibniz'sche Regel* verwendet. Letztere ist eine Verallgemeinerung der Produktregel, die sich gegebenenfalls via Induktion beweisen ließe oder aus der Formelsammlung entnommen werden kann.

Insgesamt folgt damit $(*)$. Definieren wir nun $h : G \rightarrow \mathbb{C}$, $z \mapsto 0$, so gilt

$$h^{(n)}(a) = 0 = f^{(n)}(a) \quad \text{für alle } n \in \mathbb{N}_0.$$

Da G ein Gebiet ist und f sowie h beide holomorph sind, lässt sich die Aussage (2) des Identitätssatzes anwenden und wir erhalten

$$f(z) = h(z) = 0 \quad \text{für alle } z \in G.$$

Holomorphe Abbildungen als Funktion von z

Einige Aufgaben fordern, eine Abbildung, die als Term der Variablen x sowie y gegeben ist, als Funktion von $z = x + iy$ auszudrücken. Anstatt dies explizit zu berechnen, bietet sich folgendes Vorgehen an:

Anleitung: Funktionen in Abhängigkeit von z angeben

Sei $f : G \rightarrow \mathbb{C}$ eine holomorphe Funktion wie eben beschrieben, wobei G ein Gebiet ist.

- (1) Berechne $f(x)$ für ein reelles $x \in \mathbb{R}$ (oder für iy mit $y \in \mathbb{R}$). Definiere die entsprechende komplexe Funktion $g(z)$ durch Ersetzen von x mit z .
- (2) Aufgrund ihrer Konstruktion stimmen f und g auf der Menge \mathbb{R} (bzw. $i\mathbb{R}$) überein. Zeige, dass diese einen Häufungspunkt in der Definitionsmenge G hat.
- (3) Folgere mit dem Identitätssatz, dass f auf dem gesamten Gebiet durch den Term von g gegeben ist.

Aufgabe (Herbst 2003, T3A1)

Bestimmen Sie diejenige holomorphe Abbildung $f: \mathbb{C} \rightarrow \mathbb{C}$, die die harmonische Funktion $u(x, y) = x^3y - xy^3$ als Realteil hat und die Bedingung $f(0) = 3i$ erfüllt. Drücken Sie f als Funktion der komplexen Variablen $z = x + iy$ aus.

Lösungsvorschlag zur Aufgabe (Herbst 2003, T3A1)

Wir verwenden die Cauchy-Riemannschen Differentialgleichungen. Dazu bestimmen wir zunächst die Ableitung von $\operatorname{Re} f = u$ nach x und y

$$\partial_x u(x, y) = 3x^2y - y^3 \quad \partial_y u(x, y) = x^3 - 3xy^2$$

Bezeichnen wir den Imaginärteil der Funktion f mit v , so muss $\partial_y v = \partial_x u$ und $\partial_x v = -\partial_y u$ gelten. Wir integrieren also $\partial_x u$ nach y (bzw. $\partial_y u$ nach x) und erhalten

$$\begin{aligned} v(x, y) &= v(x, 0) + \int_0^y \partial_x u(x, \tilde{y}) d\tilde{y} = v(x, 0) + \frac{3}{2}x^2y^2 - \frac{1}{4}y^4 \\ v(x, y) &= v(0, y) + \int_0^x -\partial_y u(\tilde{x}, y) d\tilde{x} = v(0, y) - \left(\frac{1}{4}x^4 - \frac{3}{2}x^2y^2 \right) \end{aligned}$$

Aus der zweiten Gleichung folgt $v(x, 0) = -\frac{1}{4}x^4 + v(0, 0) = -\frac{1}{4} + 3$ unter Verwendung der Anfangsbedingung $f(0) = 3i$. Zusammensetzen liefert dann

$$v(x, y) = -\frac{1}{4}x^4 + \frac{3}{2}x^2y^2 - \frac{1}{4}y^4 + 3$$

Wir erhalten somit insgesamt die holomorphe Funktion f , gegeben durch

$$f(x + iy) = u(x, y) + iv(x, y) = x^3y - xy^3 + i \left(-\frac{1}{4}x^4 + \frac{3}{2}x^2y^2 - \frac{1}{4}y^4 + 3 \right).$$

Um f in Abhängigkeit von $z \in \mathbb{C}$ zu schreiben, verwenden wir nun den Identitätssatz. Dazu bestimmen wir zunächst die Gestalt von f für reelle Zahlen. Für $x \in \mathbb{R}$ gilt

$$f(x) = i \left(-\frac{1}{4}x^4 + 3 \right) = -\frac{i}{4}x^4 + 3i.$$

Betrachten wir also die Funktion $g: \mathbb{C} \rightarrow \mathbb{C}$, $z \mapsto -\frac{i}{4}z^4 + 3i$. Wir haben bereits gesehen, dass

$$f|_{\mathbb{R}} = g|_{\mathbb{R}}.$$

Wir zeigen noch, dass \mathbb{R} einen Häufungspunkt in \mathbb{C} besitzt. Sei dazu die Folge $(z_n)_{n \in \mathbb{N}}$ definiert durch $z_n = \frac{1}{n}$. Es gilt $z_n \neq 0$ für $n \in \mathbb{N}$ und $\lim_{n \rightarrow \infty} z_n = 0$. Somit hat \mathbb{R} einen Häufungspunkt bei 0. Die Definitionsmenge C von f und g ist offen und zusammenhängend, also ein Gebiet. Mit dem Identitätssatz erhalten wir $f = g$, also gilt

$$f(z) = g(z) = -\frac{i}{4}z^4 + 3i \quad \text{für alle } z \in \mathbb{C}.$$

Existenz von Funktionen

In den folgenden Aufgaben sind Bedingungen gegeben und nach der Existenz einer holomorphen Funktion gefragt, die diese erfüllt. Meist sind dabei die Funktionswerte für eine bestimmte Folge angegeben. Man versucht dann, aus dieser die Funktion zu rekonstruieren (optimalerweise auf einer Art Schmierzettel-Rechnung, vgl. die erste Aufgabe), und untersucht anschließend, ob diese Funktion eine eventuelle zweite Bedingung erfüllt bzw. auf dem angegebenen Definitionsbereich definiert werden kann.

Aufgabe (Herbst 2010, T1A5)

- a** Formulieren Sie den Identitätssatz für holomorphe Funktionen.
- b** Für $r > \frac{1}{2}$ sei $D_r := \{z \in \mathbb{C} : |z| < r\}$. Für welche r gibt es eine holomorphe Funktion $f : D_r \rightarrow \mathbb{C}$ mit $f\left(\frac{1}{n}\right) = \frac{1}{n-1}$ für $n = 2, 3, 4, \dots$?

Vorüberlegung auf dem Schmierzettel

Es ist klar, dass die Lösung von Teil **b** auf den Identitätssatz hinauslaufen wird. Überlegen wir aber erst, wie eine solche Funktion aussehen könnte: hierzu setzen wir $\xi = \frac{1}{n}$, also $n = \frac{1}{\xi}$ und erhalten

$$f(\xi) = f\left(\frac{1}{n}\right) = \frac{1}{n-1} = \frac{1}{\frac{1}{\xi}-1} = \frac{\xi}{1-\xi}.$$

Es handelt sich also um $f(z) = \frac{z}{1-z}$. Wir haben damit für $r \leq 1$ eine Funktion gefunden, für $r > 1$ muss eine andere Funktion mit dieser übereinstimmen. Da aber f für $z = 1$ „explodiert“, kann es eine solche Funktion gar nicht geben.

Lösungsvorschlag zur Aufgabe (Herbst 2010, T1A5)

- a** Siehe Satz 6.19.
- b** Wir betrachten zunächst den Fall $r \in]\frac{1}{2}; 1]$ und behaupten, dass es in diesem Fall eine holomorphe Funktion gibt, die die gewünschte Eigenschaft besitzt. Dazu setzen wir

$$f_r: D_r \rightarrow \mathbb{C}, \quad z \mapsto \frac{z}{1-z}.$$

Die Funktion f ist auf dem angegebenen Definitionsbereich als Quotient zweier holomorpher Funktionen holomorph, da der Nenner auf D_r nicht verschwindet. Zudem gilt für $n \geq 2$

$$f_r\left(\frac{1}{n}\right) = \frac{\frac{1}{n}}{1 - \frac{1}{n}} = \frac{1}{n-1}, \quad (*)$$

wie gefordert.

Kommen wir zu $r > 1$. Nehmen wir an, dass eine auf D_r definierte holomorphe Funktion g existiert, die die angegebenen Bedingungen erfüllt. Wir zeigen, dass diese auf D_1 mit der soeben definierten Funktion f_1 übereinstimmen muss.

Zunächst definiert D_1 eine Kreisscheibe in \mathbb{C} und ist somit offen und zusammenhängend, d. h. ein Gebiet. Weiter gilt gemäß $(*)$, dass

$$f_1(z) = g(z) \quad \text{für } z \in N = \left\{ \frac{1}{n} \mid n \in \mathbb{N}, n \geq 2 \right\}.$$

Die Menge N besitzt einen Häufungspunkt bei 0. Es ist nämlich $z_n = \frac{1}{n}$ für $n \geq 2$ eine Folge mit $z_n \in N, z_n \neq 0$ und $\lim_{n \rightarrow \infty} z_n = 0$. Dieser liegt in D_1 , sodass sich der Identitätssatz anwenden lässt. Es folgt $g|_{D_1} = f_1$.

Es gilt aber für die Folge $y_n = 1 - \frac{1}{n}$ für $n \in \mathbb{N}$ wegen $y_n \in D_1$ und aufgrund von Stetigkeit, dass

$$\lim_{n \rightarrow \infty} g(y_n) = \lim_{n \rightarrow \infty} f_1(y_n) = \lim_{n \rightarrow \infty} n - 1 = \infty.$$

Damit muss g in 1 eine nicht-hebbare Singularität haben – Widerspruch zur Holomorphie auf D_r . Für $r > 1$ existiert also keine Funktion mit der geforderten Eigenschaft.

Aufgabe (Herbst 2011, T3A2)

Sei $\Omega \subset \mathbb{C}$ ein Gebiet mit $0 \in \Omega$. Untersuchen Sie, ob es holomorphe Funktionen $f, g, h: \Omega \rightarrow \mathbb{C}$ mit den folgenden Eigenschaften gibt:

- a** $f\left(\frac{1}{n^{2011}}\right) = 0$ für alle $n \in \mathbb{N}$ mit $\frac{1}{n^{2011}} \in \Omega$, aber $f \not\equiv 0$.
- b** $g^{(k)}(0) = (k!)^2$ für alle $k \in \mathbb{N}_0 := \{0, 1, 2, \dots\}$.
- c** $h\left(\frac{1}{2n}\right) = h\left(\frac{1}{2n-1}\right) = \frac{1}{n}$ für alle $n \in \mathbb{N}$ mit $\frac{1}{2n}, \frac{1}{2n-1} \in \Omega$.

Lösungsvorschlag zur Aufgabe (Herbst 2011, T3A2)

- a** Wir zeigen, dass es eine solche Funktion *nicht* gibt, da aus der angegebenen Bedingung bereits folgt, dass f konstant 0 ist. Setze dazu $\tilde{f}: \Omega \rightarrow \mathbb{C}$, $z \mapsto 0$ und

$$N = \left\{ \frac{1}{n^{2011}} \mid n \in \mathbb{N}, \frac{1}{n^{2011}} \in \Omega \right\}.$$

Laut Voraussetzung stimmen f und \tilde{f} auf ganz N überein. Da Ω eine offene Menge ist, also insbesondere eine offene Umgebung der 0 enthält, liegt die Folge $(z_n)_{n \in \mathbb{N}} = (\frac{1}{n^{2011}})_{n \in \mathbb{N}}$ wegen $\lim_{n \rightarrow \infty} z_n = 0$ ab einem genügend großen Index in N . Sie erfüllt zudem $z_n \neq 0$ für alle $n \in \mathbb{N}$, sodass 0 ein Häufungspunkt von N ist, der in Ω liegt. Laut dem Identitätssatz folgt

$$f(z) = \tilde{f}(z) = 0 \text{ für } z \in \Omega.$$

Jede Funktion, die die erste Bedingung erfüllt, muss damit konstant 0 sein.

- b** Nehmen wir an, eine solche Funktion existiert. Laut Satz 6.10 (1) besitzt g eine Darstellung als Potenzreihe der Form

$$g(z) = \sum_{k=0}^{\infty} \frac{g^{(k)}(0)}{k!} z^k = \sum_{k=0}^{\infty} k! z^k.$$

Wir berechnen den Konvergenzradius r dieser Reihe mit der Formel aus dem Quotientenkriterium und erhalten

$$r = \lim_{n \rightarrow \infty} \left| \frac{a_n}{a_{n+1}} \right| = \lim_{n \rightarrow \infty} \left| \frac{n!}{(n+1)!} \right| = \lim_{n \rightarrow \infty} \left| \frac{1}{n+1} \right| = 0.$$

Somit konvergiert die obige Potenzreihe auf keiner Umgebung von 0, sodass eine solche Funktion g in 0 nicht holomorph ist.

c Auch hier zeigen wir, dass eine solche Funktion nicht existiert. Sei dazu h eine Funktion, die die erste Bedingung $h\left(\frac{1}{2n}\right) = \frac{1}{n}$ erfüllt. Wir setzen $\tilde{h} : \Omega \rightarrow \mathbb{C}$, $z \mapsto 2z$ und bemerken, dass wegen

$$\tilde{h}\left(\frac{1}{2n}\right) = \frac{1}{n} = h\left(\frac{1}{2n}\right)$$

die Funktionen h und \tilde{h} auf der Menge

$$N = \left\{ \frac{1}{2n} \mid n \in \mathbb{N}, \frac{1}{2n} \in \Omega \right\}$$

übereinstimmen. Die Menge N hat einen Häufungspunkt bei 0 (es gilt $z_n \neq 0$ und $\lim_{n \rightarrow \infty} z_n = 0$ für die Folge $(z_n)_{n \in \mathbb{N}} = (\frac{1}{2n})_{n \in \mathbb{N}}$). Dieser liegt in Ω und beide Funktionen sind auf dem Gebiet Ω definiert. Der Identitätssatz liefert somit

$$h(z) = 2z \quad \text{für } z \in \Omega.$$

Dies ist aber unvereinbar mit der zweiten Bedingung, denn z. B. gilt

$$h\left(\frac{1}{2 \cdot 1 - 1}\right) = h(1) = 2 \neq 1.$$

Somit existiert keine Funktion $h : \Omega \rightarrow \mathbb{C}$, die *beide* Bedingungen erfüllt.

Aufgabe (Herbst 2011, T2A2)

Beantworten Sie die folgenden zwei Fragen zur Funktionentheorie jeweils mit einer kurzen Begründung.

- a** Sei $f : \mathbb{C} \rightarrow \mathbb{C}$ holomorph mit $f^{(n)}(0) = n$ für alle $n \in \mathbb{N}_0$. Welchen Wert besitzt das Kurvenintegral $\frac{1}{2\pi i} \int_{|z-1|=R} \frac{f(z)}{z-1} dz$ für $R > 0$, wobei $|z-1| = R$ den positiv durchlaufenen Kreis um 1 mit Radius R bezeichnet?
- b** Gibt es eine holomorphe Funktion $f : \mathbb{C} \rightarrow \mathbb{C}$ mit $f\left(\frac{1}{n}\right) = \frac{n}{2n-1}$ für alle $n \in \mathbb{N}$?

Lösungsvorschlag zur Aufgabe (Herbst 2011, T2A2)

- a** Laut der Cauchy-Integralformel gilt

$$\frac{1}{2\pi i} \int_{|z-1|=R} \frac{f(z)}{z-1} dz = f(1).$$

Scheinbar genügt es nun, den Wert $f(1)$ zu bestimmen – was leider schwieriger als erwartet ist, da wir f nicht explizit angegeben haben. Wir „rekonstruieren“ diese mithilfe ihrer Reihenentwicklung um 0:

$$\begin{aligned} f(z) &= \sum_{n=0}^{\infty} \frac{f^{(n)}(0)}{n!} z^n = \sum_{n=0}^{\infty} \frac{n}{n!} z^n = \sum_{n=1}^{\infty} \frac{z^n}{(n-1)!} = \\ &= z \sum_{n=1}^{\infty} \frac{z^{n-1}}{(n-1)!} = z \sum_{n=0}^{\infty} \frac{z^n}{n!} = z \exp z. \end{aligned}$$

Damit ist der Wert des Integrals $f(1) = \exp(1) = e$.

- b** Nehmen wir an, eine solche Funktion existiert. Sei $B_2(0) = \{z \in \mathbb{C} \mid |z| < 2\}$. Wir betrachten die Funktion

$$g: B_2(0) \rightarrow \mathbb{C}, \quad z \mapsto \frac{1}{2-z}.$$

und zeigen mit dem Identitätssatz, dass die Einschränkung von f auf $B_2(0)$ mit g übereinstimmen muss. Zunächst ist $B_2(0)$ ein Gebiet. Setze außerdem $N = \left\{ \frac{1}{n} \mid n \in \mathbb{N} \right\}$. Wie zuvor zeigt man, dass N einen Häufungspunkt bei 0 hat. Es gilt außerdem

$$g\left(\frac{1}{n}\right) = \frac{1}{2 - \frac{1}{n}} = \frac{n}{2n-1} = f\left(\frac{1}{n}\right).$$

Mit dem Identitätssatz folgt

$$f(z) = g(z) \quad \text{für } z \in B_2(0).$$

Betrachte nun aber die Folge $(y_n)_{n \in \mathbb{N}}$ gegeben durch $y_n = 2 - \frac{1}{n}$. Es gilt $y_n \in B_2(0)$ für alle $n \in \mathbb{N}$. Zudem ist

$$\lim_{n \rightarrow \infty} f(y_n) = \lim_{n \rightarrow \infty} g(y_n) = \lim_{n \rightarrow \infty} n = \infty,$$

sodass f bei 2 eine nicht hebbare Singularität haben muss. Damit existiert keine auf \mathbb{C} definierte holomorphe Funktion, die die geforderte Bedingung erfüllt.

Aufgabe (Frühjahr 2001, T3A1)

Es bezeichne $\mathbb{E} := \{z \in \mathbb{C} \mid |z| < 1\}$ die komplexe Einheitskreisscheibe. Sei $f: \mathbb{E} \rightarrow \mathbb{C}$ eine holomorphe Funktion mit der Eigenschaft $f(z) = f(z^2)$ für alle $z \in \mathbb{E}$. Zeigen Sie, dass f konstant ist.

Lösungsvorschlag zur Aufgabe (Frühjahr 2001, T3A1)

Um den Identitätssatz anzuwenden, definieren wir zunächst eine konstante Funktion. Sei dazu $\omega \in \mathbb{E} \setminus \{0\}$ beliebig. Wir setzen

$$g : \mathbb{E} \rightarrow \mathbb{C}, \quad z \mapsto c := f(\omega).$$

Es gilt nun $f(\omega^{2^n}) = f(\omega)$ für $n \in \mathbb{N}$. Wir beweisen dies durch vollständige Induktion. Für $n = 1$ ist dies die Voraussetzung an f . Ist die Gleichung für $n \in \mathbb{N}$ bewiesen, so gilt wegen $|\omega^{2^n}| = |\omega|^2 < 1$ auch $\omega^{2^n} \in \mathbb{E}$. Daher ist

$$f(\omega^{2^{n+1}}) = f\left(\left[\omega^{2^n}\right]^2\right) = f(\omega^{2^n}) \stackrel{(I.V.)}{=} f(\omega),$$

wobei an der Stelle (I.V.) die Induktionsvoraussetzung verwendet wurde. Somit stimmen f und g auf der Menge $N = \{\omega^{2^n} \mid n \in \mathbb{N}\}$ überein. Wir zeigen, dass diese einen Häufungspunkt in \mathbb{E} hat. Sei dazu die Folge $(z_n)_{n \in \mathbb{N}}$ gegeben durch $z_n = \omega^{2^n}$. Es gilt $z_n \neq 0$ für alle $n \in \mathbb{N}$, sowie $\lim_{n \rightarrow \infty} z_n = 0$ wegen $|\omega| < 1$, also ist $0 \in \mathbb{E}$ ein Häufungspunkt der Menge N . Da \mathbb{E} ein Gebiet ist, folgt mit dem Identitätssatz

$$f(z) = g(z) = c \quad \text{für } z \in \mathbb{E}.$$

Aufgabe (Herbst 2006, T3A2)

Sei $U \subseteq \mathbb{C}$ eine offene Teilmenge. Zeigen Sie unter Verwendung des Identitätssatzes, dass U genau dann zusammenhängend ist, wenn für je zwei holomorphe Funktionen $f, g: U \rightarrow \mathbb{C}$ die Implikation gilt:

$$f \cdot g \equiv 0 \quad \Rightarrow \quad f \equiv 0 \text{ oder } g \equiv 0$$

Lösungsvorschlag zur Aufgabe (Herbst 2006, T3A2)

„ \Rightarrow “: Nehmen wir zunächst an, dass U zusammenhängend, also ein Gebiet ist. Seien $f, g: U \rightarrow \mathbb{C}$ holomorphe Funktionen mit $f \cdot g \equiv 0$.

Angenommen, f ist nicht die Nullfunktion. Dann gibt es ein $a \in U$ mit $f(a) \neq 0$ und, da f stetig ist, gibt es eine offene Umgebung U_a von a mit $f(u) \neq 0$ für $u \in U_a$. Wegen $(fg)(u) = f(u)g(u) = 0$ muss jedoch $g(u) = 0$ für $u \in U_a$ gelten. Damit stimmt g auf einer offenen Teilmenge von U mit der konstanten Funktion $U \rightarrow \mathbb{C}, z \mapsto 0$ überein. Da jeder Punkt einer offenen Menge ein Häufungspunkt ist, folgt mit dem Identitätssatz $g \equiv 0$.

„ \Leftarrow “: Wir führen einen indirekten Beweis. Nehmen wir also an, dass U nicht zusammenhängend ist. Dann gibt es in U offene, disjunkte und nicht-leere Teilmengen $U_1, U_2 \subseteq U$ mit

$$U = U_1 \cup U_2.$$

Wir definieren die beiden Funktionen

$$f: U \rightarrow \mathbb{C}, \quad z \mapsto \begin{cases} 1 & \text{falls } z \in U_1, \\ 0 & \text{falls } z \in U_2 \end{cases} \quad \text{und}$$

$$g: U \rightarrow \mathbb{C}, \quad z \mapsto \begin{cases} 0 & \text{falls } z \in U_1, \\ 1 & \text{falls } z \in U_2. \end{cases}$$

Da U_1 und U_2 disjunkt sind, sind diese Abbildungen wohldefiniert. Zudem sind sie holomorph, da es für jedes $z \in U$ eine offene Umgebung gibt, auf der die Funktionen durch eine konstante Abbildung gegeben sind (d. h. dort insbesondere eine Darstellung als Potenzreihe besitzen). Zudem ist $f \cdot g \equiv 0$. Es gilt nämlich für beliebiges $z \in U$, dass

$$(fg)(z) = \begin{cases} f(z)g(z) = 1 \cdot 0 = 0 & \text{falls } z \in U_1, \\ f(z)g(z) = 0 \cdot 1 = 0 & \text{falls } z \in U_2. \end{cases}$$

Jedoch ist weder $f \equiv 0$ noch $g \equiv 0$, da keine der Teilmengen U_1, U_2 leer ist. Ist also U nicht zusammenhängend, so ist die Implikation falsch. Die Aussage folgt durch Kontraposition.

6.4. Wichtige Sätze der Funktionentheorie

Ganze Funktionen

Eine *ganze Funktion* ist eine holomorphe Funktion, die auf der gesamten Menge der komplexen Zahlen definiert ist. Wie die beiden nächsten Sätze zeigen, erlauben diese beiden Eigenschaften bereits eine recht genaue Beschreibung einer solchen Funktion.

Satz 6.20 (Liouville). Sei $f: \mathbb{C} \rightarrow \mathbb{C}$ eine ganze Funktion. Ist f beschränkt, d. h. gibt es ein $M \in \mathbb{R}^+$ mit $|f(z)| \leq M$ für alle $z \in \mathbb{C}$, so ist f konstant.

Eine noch weitreichendere Aussage macht der kleine Satz von Picard – er gibt explizit an, wie das Bild einer ganzen Funktion aussehen kann.

Satz 6.21 (Kleiner Satz von Picard). Sei $f: \mathbb{C} \rightarrow \mathbb{C}$ eine holomorphe Funktion. Dann gilt eine der folgenden Aussagen:

- (1) $f(\mathbb{C}) = \mathbb{C}$,
- (2) $f(\mathbb{C}) = \mathbb{C} \setminus \{a\}$ für ein $a \in \mathbb{C}$ oder
- (3) $f(\mathbb{C}) = \{a\}$ für ein $a \in \mathbb{C}$, also f ist konstant.

Anleitung: Anwendungen des Satzes von Liouville

Um den Satz von Liouville anwenden zu können, sind gelegentlich folgende „Vorbereitungen“ hilfreich:

- (1) Sind aus dem Definitionsbereich nur einzelne Punkte ausgenommen, so lässt sich mit dem Riemann'schen Hebbarkeitssatz häufig argumentieren, dass die Funktion eine holomorphe Fortsetzung auf \mathbb{C} hat, die beschränkt ist und auf die somit der Satz von Liouville angewendet werden kann.
- (2) Abschätzungen für den Realteil (bzw. Imaginärteil) einer ganzen Funktion f lassen sich verwenden, indem man die Funktion e^f (bzw. e^{-if}) betrachtet: Für diese gilt nämlich wegen $|e^{ix}| = 1$ für $x \in \mathbb{R}$, dass

$$\left| e^{f(z)} \right| = \left| e^{\operatorname{Re} f(z) + i \operatorname{Im} f(z)} \right| = \left| e^{\operatorname{Re} f(z)} \right| \left| e^{i \operatorname{Im} f(z)} \right| = e^{\operatorname{Re} f(z)}.$$

Ist also $\operatorname{Re} f$ beschränkt, so gilt dies auch für die ganze Funktion e^f .

Aufgabe (Herbst 2014, T3A5)

Für die holomorphen Funktionen $f: \mathbb{C} \rightarrow \mathbb{C}$ und $g: \mathbb{C} \rightarrow \mathbb{C}$ gelte $|f(z)| \leq |g(z)|$ für alle $z \in \mathbb{C}$. Zeigen Sie: Es gibt ein $\lambda \in \mathbb{C}$ mit $|\lambda| \leq 1$, sodass $f(z) = \lambda g(z)$ für alle $z \in \mathbb{C}$.

Lösungsvorschlag zur Aufgabe (Herbst 2014, T3A5)

Sei $N = \{z \in \mathbb{C} \mid g(z) = 0\}$ die Nullstellenmenge von g . Nehmen wir zunächst an, dass N eine nicht-diskrete Menge ist. Dann ist laut dem Identitätssatz $g(z) = 0$ für alle $z \in \mathbb{C}$ und die Ungleichung aus der Angabe impliziert $f(z) = 0$ für alle $z \in \mathbb{C}$. In diesem Fall ist die geforderte Ungleichung also sogar für beliebige $\lambda \in \mathbb{C}$ erfüllt (insbesondere z.B. für $\lambda = 1$).

Betrachten wir nun den Fall, dass N diskret ist. Zunächst gilt für alle $z \notin N$ die Ungleichung

$$|f(z)| \leq |g(z)| \Leftrightarrow \left| \frac{f(z)}{g(z)} \right| \leq 1.$$

Da N diskret ist, sind alle Singularitäten von $\frac{f}{g}$ isoliert. Darüber hinaus bleibt die Funktion wegen der Ungleichung in jeder Umgebung einer solchen Singularität beschränkt. Damit sind laut dem Riemannschen Hebbarkeitssatz alle Singularitäten hebbbar, d.h. die Abbildung $\frac{f}{g}$ besitzt eine holomorphe Fortsetzung $h: \mathbb{C} \rightarrow \mathbb{C}$ mit $|h(z)| \leq 1$. Als ganze und beschränkte Funktion ist h laut dem Satz von Liouville konstant. Folglich gibt es ein $\lambda \in \mathbb{C}$ mit $|\lambda| \leq 1$, sodass

$$\frac{f(z)}{g(z)} = \lambda \Leftrightarrow f(z) = \lambda g(z)$$

für alle $z \notin N$ erfüllt ist. Für die Punkte $z \in N$ folgt wie oben $f(z) = g(z) = 0$, sodass auch in diesem Fall die Gleichung gültig ist.

Aufgabe (Herbst 2010, T3A2)

Sei

$$A = \{0\} \cup \left\{ \frac{1}{n} \mid n \in \mathbb{N} \right\}.$$

Zeigen Sie: Jede auf ganz $\mathbb{C} \setminus A$ definierte, beschränkte, holomorphe Funktion ist konstant.

Lösungsvorschlag zur Aufgabe (Herbst 2010, T3A2)

Sei f eine auf $\mathbb{C} \setminus A$ definierte, beschränkte und holomorphe Funktion. Betrachten wir zunächst die Singularitäten von f an den Stellen $\frac{1}{n}$ für $n \in \mathbb{N}$, welche isolierte Singularitäten sind.

Da f beschränkt ist, sind diese laut dem Riemannschen Hebbarkeitssatz hebbbar und wir erhalten eine holomorphe Fortsetzung $\tilde{f}: \mathbb{C} \setminus \{0\} \rightarrow \mathbb{C}$. Für diese ist nun 0 eine isolierte Singularität (beachte, dass das für f noch nicht der Fall war), sodass wir aus dem gleichen Argument eine holomorphe Fortsetzung $\tilde{f}: \mathbb{C} \rightarrow \mathbb{C}$ erhalten, die beschränkt und damit laut dem Satz von Liouville 6.20 konstant ist. Damit muss aber insbesondere f konstant sein.

Der Satz von der Gebietstreue

Gemäß der topologischen Definition von Stetigkeit ist das *Urbild* einer offenen Menge unter einer stetigen Abbildung stets wieder offen. Jedoch muss das *Bild* einer offenen Menge im Allgemeinen nicht wieder offen sein. Beispielsweise ist im Fall der stetigen Abbildung

$$f: \mathbb{R} \rightarrow \mathbb{R}, \quad x \mapsto x^2,$$

die Menge $f(\mathbb{R}) = [0, \infty[$ abgeschlossen. Anders ist die Situation für holomorphe Funktionen:

Satz 6.22 (Gebietstreue). Es sei $D \subseteq \mathbb{C}$ und $f: D \rightarrow \mathbb{C}$ eine nicht-konstante holomorphe Funktion. Ist $G \subseteq D$ ein Gebiet, so ist auch $f(G)$ ein Gebiet.

Aufgabe (Frühjahr 2011, T3A4)

- a Sei $U = \{z \in \mathbb{C} \mid |z| < 2\}$ und $f: U \rightarrow \mathbb{C}$ holomorph mit $f(0) = 0$ und $f(1) = 1$. Zeigen Sie, dass es ein $z \in U$ gibt mit $f(z) \in \mathbb{R}$ und $f(z) > 1$.
- b Bleibt die Aussage in a richtig, wenn man
 - (i) auf die Voraussetzung $f(0) = 0$ verzichtet,
 - (ii) U durch eine beliebige offene Teilmenge von \mathbb{C} mit $0 \in U$ und $1 \in U$ ersetzt?

Lösungsvorschlag zur Aufgabe (Frühjahr 2011, T3A4)

- a Die Menge U ist ein Gebiet und wegen $f(0) \neq f(1)$ ist f nicht konstant, sodass aufgrund der Gebietstreue auch die Bildmenge $f(U)$ ein Gebiet, insbesondere also offen, ist. Wegen $f(1) = 1$ gilt $1 \in f(U)$, und damit muss eine Umgebung $B_\varepsilon(1)$ für ein $\varepsilon > 0$ in U enthalten sein. Insbesondere gilt $1 + \frac{\varepsilon}{2} \in f(U)$, also gibt es ein $z \in U$ mit $f(z) = 1 + \frac{\varepsilon}{2}$.
- b (i) Nein. Die anderen Voraussetzungen werden beispielsweise von der konstanten Funktion $z \mapsto 1$ erfüllt, jedoch gibt es für diese kein $z \in U$, sodass $f(z) > 1$.
 (ii) Nein. Definiere beispielsweise $U = B_{\frac{1}{2}}(1) \cup B_{\frac{1}{2}}(0)$. Wegen $B_{\frac{1}{2}}(1) \cap B_{\frac{1}{2}}(0) = \emptyset$ ist die Funktion

$$f: U \rightarrow \mathbb{C}, \quad z \mapsto \begin{cases} 0 & \text{falls } z \in B_{\frac{1}{2}}(0) \\ 1 & \text{falls } z \in B_{\frac{1}{2}}(1) \end{cases}$$

wohldefiniert und holomorph mit $f(0) = 0, f(1) = 1$. Zugleich gilt auch hier $f(z) \leq 1$ für alle $z \in U$.

Aufgabe (Herbst 2007, T2A2)

- a** Formulieren Sie den Satz von Liouville und beweisen Sie ihn mit Hilfe der Koeffizientenabschätzung von Cauchy.
- b** Sei $f: \mathbb{C} \rightarrow \mathbb{C}$ holomorph und sei $(a, b) \in \mathbb{R}^2$ mit $(a, b) \neq (0, 0)$. Zeigen Sie: Ist die Funktion $a \operatorname{Re} f + b \operatorname{Im} f: \mathbb{C} \rightarrow \mathbb{R}$ nach oben beschränkt, so ist f konstant.

Lösungsvorschlag zur Aufgabe (Herbst 2007, T2A2)

- a** Für die Formulierung des Satzes siehe Satz 6.20.

Sei nun $f: \mathbb{C} \rightarrow \mathbb{C}$ eine ganze Funktion und $M \in \mathbb{R}^+$ mit $|f(z)| \leq M$ für $z \in \mathbb{C}$. Außerdem sei $\sum_{n=0}^{\infty} a_n z^n$ die Potenzreihenentwicklung von f um 0. Laut der Formel Satz 6.10 (2) gilt für die Koeffizienten

$$a_n = \frac{1}{2\pi i} \int_{\partial B_r(0)} \frac{f(w)}{w^{n+1}} dw \quad \text{für } r \in \mathbb{R}^+.$$

Nun erhalten wir für $r > 0$ jedoch

$$\begin{aligned} |a_n| &= \left| \frac{1}{2\pi i} \int_{\partial B_r(0)} \frac{f(w)}{w^{n+1}} dw \right| \leq \frac{1}{2\pi} \int_{\partial B_r(0)} \frac{|f(w)|}{r^{n+1}} dw \\ &\leq \frac{1}{2\pi} \int_{\partial B_r(0)} \frac{M}{r^{n+1}} dw = \frac{M}{r^n}. \end{aligned}$$

Da es sich bei f um eine ganze Funktion handelt, liegt für beliebiges $r > 0$ der Ball $B_r(0)$ im Definitionsbereich. Wir können somit den Grenzübergang $r \rightarrow \infty$ durchführen und erhalten für $n \geq 1$, dass

$$|a_n| = \lim_{r \rightarrow \infty} \frac{M}{r^n} = 0.$$

Somit erhalten wir $f(z) = a_0$. Insbesondere ist f konstant.

- b** Bemerke zunächst, dass für $z \in \mathbb{C}$ die Gleichung

$$\begin{aligned} (a - ib)f(z) &= (a - ib)(\operatorname{Re} f(z) + i \operatorname{Im} f(z)) = \\ &= (a \operatorname{Re} f(z) + b \operatorname{Im} f(z)) + i(-b \operatorname{Re} f(z) + a \operatorname{Im} f(z)) \end{aligned}$$

gilt. Daraus folgt, dass $|e^{(a-ib)f(z)}| = e^{a \operatorname{Re} f(z) + b \operatorname{Im} f(z)}$. Nach Voraussetzung ist nun die ganze Funktion $e^{(a-ib)f}$ beschränkt, sodass diese nach dem Satz von Liouville konstant ist.

Angenommen, die Funktion f wäre nicht konstant. Wegen $a - ib \neq 0$ ist dann auch $(a - ib)f$ eine nicht-konstante Funktion, sodass $(a - ib)f(\mathbb{C})$ nach dem Satz von der Gebietstreue 6.22 ein Gebiet ist. Eine weitere

Anwendung des Satzes von der Gebietstreue liefert dann, dass auch $\exp((a - ib)f(\mathbb{C}))$ ein Gebiet ist. Dies ist jedoch ein Widerspruch dazu, dass die Funktion $e^{(a-ib)f}$ konstant ist.

Aufgabe (Herbst 2012, T2A2)

- a** Sei $f: \mathbb{C} \rightarrow \mathbb{C}$ eine ganze Funktion mit der Eigenschaft, dass $|f(z)| \geq \pi$ für alle $z \in \mathbb{C}$ gilt. Zeigen Sie, dass $f(z) = f(\pi)$ für alle $z \in \mathbb{C}$ gilt.
- b** Sei $f: \mathbb{C} \rightarrow \mathbb{C}$ eine ganze Funktion mit der Eigenschaft, dass $f(z+1) = f(z) = f(z+i)$ für alle $z \in \mathbb{C}$. Zeigen Sie, dass f konstant ist.

Lösungsvorschlag zur Aufgabe (Herbst 2012, T2A2)

- a** Wir bemerken zunächst, dass $f(z) = f(\pi)$ für $z = \pi$ stets erfüllt ist. Um die Gleichheit auch für $z \in \mathbb{C} \setminus \{\pi\}$ zu zeigen, beweisen wir, dass f konstant ist.
 - 1. Möglichkeit:** Die brutale Holzhammer-Methode geht folgendermaßen: Zumindest die beiden Punkte 0 und 1 liegen nicht im Bild $f(\mathbb{C})$. Laut dem kleinen Satz von Picard muss f damit bereits konstant sein.
 - 2. Möglichkeit:** Die Funktion f hat wegen $|f(z)| \geq \pi$ für $z \in \mathbb{C}$ keine Nullstellen. Betrachte also die Abbildung $g = \frac{1}{f}$, die ebenfalls ganz ist. Diese erfüllt nun $|g(z)| \leq \frac{1}{\pi}$, ist also beschränkt. Laut dem Satz von Liouville ist g – und damit auch f – konstant.
- b** Aufgrund der Periodizitätsbedingung in der Angabe lassen sich sämtliche Funktionswerte auf solche im Bereich $Q = \{a + ib \mid a, b \in [0, 1]\} \subseteq \mathbb{C}$ zurückführen. Wir behaupten daher $f(\mathbb{C}) = f(Q)$.

Die Richtung „ \supseteq “ ist klar. Für die andere sei $x + iy \in \mathbb{C}$ beliebig. Sei $x_0 = \lfloor x \rfloor$ die zu x nächstkleinere ganze Zahl, $y_0 = \lfloor y \rfloor$ die zu y nächstkleinere ganze Zahl. Dann gilt $x - x_0 \in [0, 1]$ und $y - y_0 \in [0, 1]$. Durch wiederholte Anwendung der Relation oben erhält man nun

$$\begin{aligned} f(x + iy) &= f(x - 1 + iy) = \dots = f(x - x_0 + iy) = \\ &= f(x - x_0 + i(y - 1)) = \dots = f(x - x_0 + i(y - y_0)) \in f(Q) \end{aligned}$$

und damit die behauptete Gleichung.

Da Q kompakt ist, ist auch $f(Q)$ kompakt, also beschränkt und abgeschlossen. Wäre f nicht-konstant, so müsste $f(\mathbb{C}) = f(Q)$ nach dem Satz von der Gebietstreue 6.22 allerdings offen sein. Da \mathbb{C} zusammenhängend ist, sind die einzigen Teilmengen von \mathbb{C} , die offen und abgeschlossen sind,

die leere Menge und \mathbb{C} selbst. Jedoch ist $f(\mathbb{C}) \neq \emptyset$ wegen $f(0) \in f(\mathbb{C})$ und $f(\mathbb{C}) = \mathbb{C}$ ist nicht möglich, da \mathbb{C} nicht beschränkt ist.

Der Widerspruch zeigt, dass f konstant sein muss.

Maximum- und Minimumprinzip

Satz 6.23 (Maximum- und Minimumprinzip). Sei G ein Gebiet und $f: G \rightarrow \mathbb{C}$ eine holomorphe Funktion.

- (1) Nimmt $|f|$ auf G ein Maximum an, d.h. gibt es ein $a \in G$ mit $|f(a)| \geq |f(z)|$ für alle $z \in G$, so ist f konstant.
- (2) Ist f eine nicht-konstante holomorphe Funktion und besitzt f in $a \in G$ ein Betragssminimum, so ist bereits $f(a) = 0$.

Aufgabe (Herbst 2013, T1A1)

Konstruieren Sie jeweils eine nicht-konstante holomorphe Funktion $f: \mathbb{C} \rightarrow \mathbb{C}$ mit den angegebenen Eigenschaften oder begründen Sie, warum es eine solche Funktion nicht geben kann.

- a** f bildet \mathbb{C} auf die offene Kreisscheibe $D = \{u + iv \mid (u - 1)^2 + v^2 < 4\}$ ab.
- b** $f(z) = 0$ gilt genau für $z = k$ mit $k \in \mathbb{Z}$.
- c** f erfüllt $f(0) = 2$ und $|f(z)| \leq 1$ für $|z| = 1$.

Lösungsvorschlag zur Aufgabe (Herbst 2013, T1A1)

- a** Eine solche Funktion kann nicht existieren. Sie wäre eine ganze Funktion, deren Bild durch $f(\mathbb{C}) = D = B_2(1)$ gegeben ist. Damit ist das Bild der Funktion beschränkt und laut dem Satz von Liouville (Satz 6.20) ist f damit konstant.
- b** Betrachten wir $f: \mathbb{C} \rightarrow \mathbb{C}$ mit $f(z) = \sin(\pi z)$. Es handelt sich dabei als Verkettung holomorpher Funktionen um eine holomorphe Abbildung. Zudem ist

$$f(k\pi) = \sin(k\pi) = 0$$

für $k \in \mathbb{Z}$. Andererseits gilt

$$\begin{aligned} \sin(z) = 0 &\Leftrightarrow \frac{1}{2i} (e^{iz} - e^{-iz}) = 0 \Leftrightarrow e^{iz} = e^{-iz} \\ &\Leftrightarrow e^{2iz} = 1 \Leftrightarrow z = k\pi \text{ für ein } k \in \mathbb{Z}. \end{aligned}$$

Damit hat auch jede Nullstelle von f die Form $z = k$ für $k \in \mathbb{Z}$, die Nullstellen sind also *genau* von der vorgegebenen Form.

- c** Angenommen, es gibt eine nicht-konstante Funktion f mit dieser Eigenschaft. Wäre f auf der offenen Einheitskreisscheibe \mathbb{E} konstant, so wäre f nach dem Identitätssatz auf dem gesamten Definitionsbereich konstant. Wir dürfen daher annehmen, dass f auf \mathbb{E} nicht konstant ist.

f nimmt als stetige Funktion ein Maximum auf der kompakten Menge $\overline{\mathbb{E}}$ an. Sei $z_0 \in \overline{\mathbb{E}}$ mit $|f(z_0)| = \max_{z \in \overline{\mathbb{E}}} |f(z)|$. Würde $z_0 \in \mathbb{E}$ liegen, so wäre $|f(z_0)|$ ein Maximum von f auf \mathbb{E} , sodass f nach dem Maximumsprinzip 6.23 konstant auf \mathbb{E} wäre. Folglich muss $z_0 \in \overline{\mathbb{E}} \setminus \mathbb{E} = \partial\mathbb{E}$ gelten.

Wegen $|f(0)| = 2 > |f(z_0)|$ für $z_0 \in \partial\mathbb{E}$ kann jedoch auch das nicht sein. Der Widerspruch zeigt, dass es eine derartige Funktion nicht geben kann.

Das verwendete Argument im Teil **c** der letzten Aufgabe lässt sich verallgemeinern:

Proposition 6.24 (Maximum- und Minimumsprinzip für beschränkte Gebiete). Sei $G \subseteq \mathbb{C}$ ein beschränktes Gebiet, $f: \overline{G} \rightarrow \mathbb{C}$ eine stetige und auf G holomorphe Funktion. Dann gilt:

- (1) $|f|$ nimmt auf dem Rand ∂G ein Maximum an, d. h. es gibt ein $a \in \partial G$ mit $|f(a)| \geq |f(z)|$ für alle $z \in \overline{G}$.
- (2) f hat in G eine Nullstelle oder $|f|$ nimmt auf ∂G ein Minimum an.

Aufgabe (Frühjahr 2001, T3A2)

- a** Formulieren Sie das Maximum- und Minimumsprinzip für holomorphe Funktionen.
- b** Es sei $f: \overline{\mathbb{E}} \rightarrow \mathbb{C}$ eine stetige und auf \mathbb{E} holomorphe Funktion, die in $\overline{\mathbb{E}}$ keine Nullstelle besitzt und deren Betrag auf $\partial\mathbb{E}$ konstant ist. Beweisen Sie, dass f konstant ist.
- c** Es sei $f: \overline{\mathbb{E}} \rightarrow \mathbb{C}$ eine stetige und auf \mathbb{E} holomorphe Funktion, deren Realteil auf $\partial\mathbb{E}$ konstant ist. Beweisen Sie, dass f konstant ist.

Lösungsvorschlag zur Aufgabe (Frühjahr 2001, T3A2)

- a** Siehe Satz 6.23.
- b** Sei $c \in \mathbb{R}^+$ der Wert, der von $|f|$ auf dem Rand angenommen wird. Nach dem Maximumsprinzip für beschränkte Gebiete gilt $|f(z)| \leq c$ für $z \in \mathbb{E}$. Da f keine Nullstelle auf \mathbb{E} hat, können wir auch das Minimumsprinzip für beschränkte Gebiete anwenden und erhalten ebenso $|f(z)| \geq c$ für

$z \in \mathbb{E}$. Damit erhalten wir $|f(z)| = c$ für $z \in \mathbb{E}$. Insbesondere ist $0 \in \mathbb{E}$ ein Betragsmaximum, also ist f konstant laut dem Maximumsprinzip in Satz 6.23 (1).

- c** Sei $c \in \mathbb{R}^+$ mit $\operatorname{Re} f(z) = c$ für $z \in \partial\mathbb{E}$. Betrachte die auf \mathbb{E} holomorphe und auf $\overline{\mathbb{E}}$ stetige Funktion $g(z) = e^{f(z)}$. Für $z \in \partial\mathbb{E}$ gilt

$$\left|e^{f(z)}\right| = e^{\operatorname{Re} f(z)} = e^c.$$

Damit ist $|g|$ konstant auf $\partial\mathbb{E}$, also ist g laut Teil **b** konstant. Wie in Aufgabe H07T2A2 auf Seite 315 folgert man hieraus, dass auch f konstant sein muss.

Aufgabe (Frühjahr 2011, T2A2)

Sei G ein beschränktes nicht-leeres Gebiet in \mathbb{C} und seien $f, g: \overline{G} \rightarrow \mathbb{C}$ stetige Funktionen, deren Einschränkungen auf G holomorph sind. Zeigen Sie: Gilt $|f(z)| = |g(z)|$ für alle $z \in \partial G$ und haben f und g keine Nullstellen in \overline{G} , so gibt es ein $\lambda \in \mathbb{C}$ mit $|\lambda| = 1$, sodass $f = \lambda g$.

Lösungsvorschlag zur Aufgabe (Frühjahr 2011, T2A2)

Da f und g auf \overline{G} keine Nullstellen haben, können wir die holomorphen Funktionen $\frac{f}{g}$ und $\frac{g}{f}$ betrachten. Aus dem Maximumsprinzip für beschränkte Gebiete 6.24 und $|f(z)| = |g(z)|$ für $z \in \partial G$ folgt, dass $\left|\frac{f(z)}{g(z)}\right| \leq 1$ und $\left|\frac{g(z)}{f(z)}\right| \leq 1$. Das bedeutet aber, dass $\left|\frac{f(z)}{g(z)}\right| = 1$ für alle $z \in G$.

Damit ist jeder Punkt im Inneren von G ein lokales Maximum – und die Funktion $\frac{f}{g}$ ist laut dem Maximumsprinzip konstant. Also ist $\frac{f(z)}{g(z)} = \lambda$ für ein $\lambda \in \mathbb{C}$. Wegen $\left|\frac{f(z)}{g(z)}\right| = 1$ muss diese Konstante $|\lambda| = 1$ erfüllen und wir erhalten wir gewünscht $f = \lambda g$.

Aufgabe (Herbst 2012, T1A1)

Sei $G \subseteq \mathbb{C}$ ein Gebiet, $f: G \rightarrow \mathbb{C}$ eine holomorphe Funktion und $(z_n)_n$ eine Folge in G mit paarweise verschiedenen Gliedern. Entscheiden Sie, ob die folgenden Aussagen richtig oder falsch sind. Bei richtigen Aussagen verweisen sie auf einen passenden Satz der Funktionentheorie, bei falschen geben Sie ein Gegenbeispiel.

- a** Ist $f(z_n) = 0$ für alle n , so ist $f(z) = 0$.

- b** Hat $(z_n)_n$ einen Häufungspunkt und gilt $f(z_n) = 0$ für alle n , so ist $f(z) \equiv 0$.
- c** Hat $(z_n)_n$ einen Häufungspunkt in G und gilt $f(z_n) = 0$ für alle n , so ist $f(z) \equiv 0$.
- d** Ist f auf G beschränkt, so ist f konstant.
- e** Ist $G = \mathbb{C} \setminus \{0\}$ und f auf G beschränkt, so ist f konstant.
- f** Ist $G = \mathbb{C}$ und f auf G beschränkt, so ist f konstant.

Lösungsvorschlag zur Aufgabe (Herbst 2012, T1A1)

a *Falsch.* Ein Gegenbeispiel ist $f: \mathbb{C} \rightarrow \mathbb{C}$, $z \mapsto \sin z$ mit der Folge $z_n = n\pi$. Es gilt $f(z_n) = f(0) = 0$, aber wegen $f(\frac{\pi}{2}) = 1$ ist $f \not\equiv 0$.

b *Falsch.* Betrachte dazu $G = \mathbb{C} \setminus \{0\}$ sowie die Funktion $f: G \rightarrow \mathbb{C}$, $z \mapsto \sin \frac{1}{z}$ mit der Folge $z_n = \frac{1}{n\pi}$. Es gilt dann

$$f(z_n) = \sin(n\pi) = 0.$$

Ferner ist $\lim_{n \rightarrow \infty} z_n = 0$ und die Glieder der Folge sind paarweise verschieden, sodass $(z_n)_n$ bei 0 einen Häufungspunkt hat. Dennoch ist $f \not\equiv 0$, denn $f(\frac{2}{\pi}) = \sin(\frac{\pi}{2}) = 1 \neq 0$.

c *Richtig.* Hier können wir endlich auf den Identitätssatz verweisen, denn aus der Tatsache, dass $(z_n)_n$ paarweise verschiedene Folgenglieder und einen Häufungspunkt in G hat, folgt insbesondere, dass die Menge $N = \{z_n \mid f(z_n) = 0\}$ einen Häufungspunkt in G hat.

d *Falsch.* Betrachte dazu das Gebiet $G = \{z \in \mathbb{C} \mid |z| < 1\}$ und die Funktion $f: G \rightarrow \mathbb{C}$, $z \mapsto z$. Es gilt für alle $z \in G$

$$|f(z)| = |z| < 1,$$

also ist f auf G beschränkt. Wegen $f(0) = 0 \neq \frac{1}{2} = f(\frac{1}{2})$ ist f aber nicht konstant.

e *Richtig.* Die Funktion f ist auf einer Umgebung von 0 beschränkt, sodass es sich hierbei laut dem Riemannschen Hebbarkeitssatz um eine hebbare Singularität von f handelt und eine holomorphe Fortsetzung $\tilde{f}: \mathbb{C} \rightarrow \mathbb{C}$ existiert. Diese ist beschränkt, also laut dem Satz von Liouville konstant und damit ist auch f konstant.

f *Richtig.* Dies ist genau die Aussage des Satzes von Liouville 6.20.

Aufgabe (Frühjahr 2012, T1A2)

Fragen zur Funktionentheorie:

- a** Gibt es eine holomorphe Funktion $f: \{z \in \mathbb{C} : |z| < 2\} \rightarrow \mathbb{C}$, sodass $f(\frac{1}{2}) = 2$ ist und $|f(z)| = 1$ für alle $z \in \mathbb{C}$ mit $|z| = 1$ gilt?
- b** Gibt es eine holomorphe Funktion $g: \mathbb{C} \rightarrow \mathbb{C}$, sodass für alle $x + iy \in \mathbb{C}$ gilt: $(\operatorname{Im} g)(x + iy) = x^2 - y^2$?
- c** Gibt es eine offene Umgebung $U \subseteq \mathbb{C}$ von 0 und eine holomorphe Funktion $h: U \rightarrow \mathbb{C}$, sodass $h^{(n)}(0) = (-1)^n(2n)!$ für alle $n \in \mathbb{N}_0$ gilt?

Lösungsvorschlag zur Aufgabe (Frühjahr 2012, T1A2)

- a** *Nein.* Kurz lässt sich dies mit dem Maximumsprinzip für beschränkte Gebiete begründen (Proposition 6.24). Wir führen hier das dahinter liegende Argument nochmals aus: Wir betrachten dazu die Einschränkung von f auf die abgeschlossene Einheitskreisscheibe $\bar{\mathbb{E}}$. Diese ist stetig und auf \mathbb{E} holomorph. Da $\bar{\mathbb{E}}$ abgeschlossen und beschränkt ist, muss f dort ein Maximum annehmen.

Nehmen wir nun an, dass dieses Maximum im Inneren des Einheitskreises liegt. Dann wäre $f|_{\mathbb{E}}$ laut dem Maximumsprinzip konstant. Zusammen mit der ersten Bedingung der Angabe folgt dann $f(z) = 2$ für $z \in \mathbb{E}$. Aufgrund der Stetigkeit folgt damit auch für $a \in \partial\mathbb{E}$, dass

$$f(a) = f(\lim_{z \rightarrow a} z) = \lim_{z \rightarrow a} f(z) = \lim_{z \rightarrow a} 2 = 2$$

im Widerspruch zur Bedingung $|f(z)| = 1$ für $z \in \partial\mathbb{E}$. Somit muss also das Maximum auf dem Kreisrand $\partial\mathbb{E}$ liegen. Daraus erhalten wir jedoch einen Widerspruch zu

$$\left| f\left(\frac{1}{2}\right) \right| = 2 > 1 = |f(z)|$$

für beliebiges $z \in \partial\mathbb{E}$. Eine Funktion, die die angegebenen Forderungen erfüllt, kann also nicht existieren.

- b** Da \mathbb{C} ein einfach zusammenhängendes Gebiet ist, genügt es laut Proposition 6.6, zu überprüfen, ob die angegebene Funktion harmonisch ist. Wir berechnen

$$\partial_x \operatorname{Im} g = 2x, \quad \partial_x^2 \operatorname{Im} g = 2 \quad \text{sowie} \quad \partial_y \operatorname{Im} g = -2y, \quad \partial_y^2 \operatorname{Im} g = -2$$

und erhalten damit tatsächlich $\Delta(\operatorname{Im} g) = 0$. Damit ist $\operatorname{Im} g$ harmonisch und es existiert eine solche Funktion.⁴

- c** Angenommen, eine solche holomorphe Funktion existiert. Betrachten wir eine Potenzreihenentwicklung von h mit Entwicklungspunkt 0. Diese hat gemäß Satz 6.10 (1) die Form

$$h(z) = \sum_{n=0}^{\infty} \frac{h^{(n)}(0)}{n!} z^n = \sum_{n=0}^{\infty} \frac{(-1)^n (2n)!}{n!} z^n.$$

Wir untersuchen den Konvergenzradius dieser Reihe. Wegen $\frac{(-1)^n (2n)!}{n!} \neq 0$ für $n \in \mathbb{N}$ können wir die Formel aus Proposition 6.9 (2) verwenden und erhalten

$$r = \lim_{n \rightarrow \infty} \frac{(-1)^n (2n)!}{n!} \cdot \frac{(n+1)!}{(-1)^{n+1} (2n+2)!} = \lim_{n \rightarrow \infty} -\frac{n+1}{(2n+2)(2n+1)} = 0.$$

Damit konvergiert die Reihe leider auf keiner Umgebung der 0. Eine gesuchte Umgebung U existiert also nicht.

Aufgabe (Frühjahr 2010, T2A1)

Sei $f: \mathbb{C} \rightarrow \mathbb{C}$ eine ganze Funktion. Entscheiden Sie, ob die folgenden Behauptungen wahr sind. Begründen Sie Ihre Antwort jeweils mit einem *kurzen* Beweis oder einem Gegenbeispiel.

- a** Wenn $f(z) \in \mathbb{R}$ für alle $z \in \mathbb{C}$, dann ist f konstant.
- b** Wenn $f\left(\frac{1}{n}\right) = \frac{i}{n}$ ist für alle $n \in \mathbb{N}$, dann ist $f(z) = iz$ für alle $z \in \mathbb{C}$.
- c** Wenn f eine nicht-konstante Polynomfunktion ist, dann gibt es eine stückweise stetig differenzierbare Kurve $\gamma: [0, 1] \rightarrow \mathbb{C}$ mit $\int_{\gamma} f(z) dz = 2\pi i$.
- d** Die Funktion $\frac{1}{f}$ hat in 0 keinen Pol.
- e** Die Funktion $r \mapsto \int_{|z|=r} f(z) dz$ ist konstant auf $]0, \infty[$.
- f** Die Potenzreihe $\sum_{n=0}^{\infty} \frac{1}{n!} f^{(n)}(1)(z-1)^n$ konvergiert für alle $z \in \mathbb{C}$.

Lösungsvorschlag zur Aufgabe (Frühjahr 2010, T2A1)

- a** *Richtig.* Es gilt $\operatorname{Im} f(z) = 0$ für alle $z \in \mathbb{C}$ und somit auch $\partial_x \operatorname{Im} f = \partial_y \operatorname{Im} f = 0$. Mit den Cauchy-Riemann-Differentialgleichungen erhalten

⁴ Für Neugierige: Es handelt sich um Funktionen der Form $g(z) = iz^2 + c$ für $c \in \mathbb{C}$.

wir

$$\partial_x \operatorname{Re} f = \partial_y \operatorname{Im} f = 0 \quad \text{und} \quad \partial_y \operatorname{Re} f = -\partial_x \operatorname{Im} f = 0.$$

Somit ist auch $\operatorname{Re} f$ konstant und wir erhalten $f(z) = a$ für ein $a \in \mathbb{R}$.

Alternative: Das Bild $f(\mathbb{C})$ müsste ein Gebiet sein. Eine Teilmenge von \mathbb{R} ist jedoch nie offen in \mathbb{C} .

- b** *Richtig.* Die Menge $N = \{\frac{1}{n} \mid n \in \mathbb{N}\}$ hat einen Häufungspunkt bei Null, da die Folge $\frac{1}{n}$ aus paarweise verschiedenen Gliedern besteht und $\lim_{n \rightarrow \infty} \frac{1}{n} = 0$ erfüllt. Dieser Häufungspunkt liegt (natürlich) in \mathbb{C} , einem Gebiet. Auf N stimmen die holomorphen Funktionen f und $z \mapsto iz$ überein und mit dem Identitätssatz 6.19 folgt $f(z) = iz$ für alle $z \in \mathbb{C}$.
- c** *Richtig.* Wir konstruieren eine Kurve γ , die die Anforderungen erfüllt. Als Polynomfunktion besitzt f eine Stammfunktion F . Damit ist das angegebene Integral wegunabhängig und es gilt $\int_{\gamma} f(z) dz = F(\gamma(1)) - F(\gamma(0))$. Wir können o.B.d.A. annehmen, dass $F(0) = 0$ gilt (ansonsten könnten wir die Stammfunktion F durch die Stammfunktion $F(z) - F(0)$ ersetzen).

Nun ist $F(z) - 2\pi i$ ein Polynom vom Grad ≥ 2 , da f nicht-konstant ist, und hat damit laut dem Fundamentalsatz der Algebra genau zwei Nullstellen. Ist z_0 eine dieser Nullstellen, so gilt $F(z_0) - 2\pi i = 0$, also $F(z_0) = 2\pi i$. Wir setzen $\gamma(t) = tz_0$ für $t \in [0, 1]$. Dann gilt

$$\int_{\gamma} f(z) dz = F(\gamma(1)) - F(\gamma(0)) = F(z_0) - F(0) = 2\pi i.$$

- d** *Falsch.* Betrachte die ganze Funktion $f(z) = z$. Dann hat die Funktion $\frac{1}{f}$ wegen

$$\lim_{z \rightarrow 0} \left| \frac{1}{z} \right| = \infty \quad \text{und} \quad \lim_{z \rightarrow 0} z \frac{1}{z} = 1 < \infty$$

einen Pol erster Ordnung in 0.

- e** *Richtig.* Sei $r \in]0, \infty[$. Da f auf ganz \mathbb{C} holomorph ist, gilt laut dem Cauchy-Integralsatz 6.28

$$\int_{|z|=r} f(z) dz = 0.$$

Insbesondere ist die in der Aufgabenstellung angegebene Zuordnung damit konstant.

- f** *Richtig.* Es handelt sich bei der angegebene Reihe um die Potenzreihenentwicklung zum Entwicklungspunkt 1. Da f eine ganze Funktion ist, also keine Singularitäten hat, hat diese den Konvergenzradius ∞ .

Aufgabe (Frühjahr 2012, T2A2)

Bestimmen Sie alle holomorphen Funktionen $f, g, h: \mathbb{C} \rightarrow \mathbb{C}$ mit der Eigenschaft

- a** $f(z) = -f(\bar{z}), z \in \mathbb{C}$, bzw.
- b** $\operatorname{Re} g(z) = \sin(\operatorname{Im} g(z)), z \in \mathbb{C}$, und $g(0) = 2\pi i$, bzw.
- c** $h'(z) = z^2 h(z), z \in \mathbb{C}$.

Lösungsvorschlag zur Aufgabe (Frühjahr 2012, T2A2)

- a** Wir zeigen, dass dies nur für die Nullfunktion möglich ist. Sei dazu $x \in \mathbb{R}$ beliebig. Wir erhalten hier

$$f(x) = -f(\bar{x}) = -f(x) \Leftrightarrow f(x) = 0.$$

Somit stimmt f auf der reellen Achse mit der Funktion $z \mapsto 0$ überein. Bereits in anderen Aufgaben hatten wir gesehen, dass \mathbb{R} einen Häufungspunkt bei der 0 hat. Somit folgt laut dem Identitätssatz $f(z) = 0$ für alle $z \in \mathbb{C}$.

- b** Es gilt aufgrund der Gleichung aus der Angabe für $z \in \mathbb{C}$

$$|\operatorname{Re} g(z)| = |\sin(\operatorname{Im} g(z))| \leq 1.$$

Somit ist wie in einer früheren Aufgabe der Realteil beschränkt. Damit ist die Funktion $e^{g(z)}$ eine ganze und beschränkte Funktion, was wiederum impliziert, dass g konstant ist. Zusammen mit der Bedingung $g(0) = 2\pi i$ ergibt sich $g(z) = 2\pi i$ für alle $z \in \mathbb{C}$. Tatsächlich erfüllt diese auch

$$\operatorname{Re} g(z) = 0 = \sin(2\pi) = \sin(\operatorname{Im} g(z)).$$

- c** Sei $h(z) = \sum_{n=0}^{\infty} a_n z^n$ die Potenzreihendarstellung von h um 0. Laut Angabe gilt dann

$$h'(z) = \sum_{n=1}^{\infty} a_n n z^{n-1} = \sum_{n=0}^{\infty} a_n z^{n+2} = z^2 h(z).$$

Koeffizientenvergleich der beiden Reihen ergibt

$$a_1 = 0, \quad a_2 = 0, \quad n a_n = a_{(n-1)-2} = a_{n-3} \quad \text{für } n \geq 2.$$

Mittels Induktion zeigen wir nun, dass

$$a_{3k} = \frac{a_0}{3^k \cdot k!}, \quad a_{3k+1} = 0, \quad a_{3k+2} = 0$$

für alle $k \in \mathbb{N}_0$ gilt. Der Induktionsanfang wurde bereits oben erledigt, setzen wir daher die Aussage für ein k als bereits bewiesen voraus. Dann ist

$$a_{3(k+1)+1} \stackrel{(*)}{=} a_{3k+1} \stackrel{(I.V.)}{=} 0, \quad a_{3(k+1)+2} \stackrel{(*)}{=} a_{3k+2} \stackrel{(I.V.)}{=} 0,$$

wobei an der Stelle $(*)$ die Rekursionsformel und an der Stelle $(I.V.)$ die Induktionsvoraussetzung angewendet wurde. In ähnlicher Weise erhält man außerdem

$$3(k+1) \cdot a_{3(k+1)} \stackrel{(*)}{=} a_{3k} \Leftrightarrow a_{3(k+1)} = \frac{a_{3k}}{3(k+1)} \stackrel{(I.V.)}{=} \frac{a_0}{3^{k+1} \cdot (k+1)!}.$$

Folglich ist

$$h(z) = \sum_{n=0}^{\infty} a_n z^n = \sum_{k=0}^{\infty} a_{3k} z^{3k} = \sum_{k=0}^{\infty} \frac{a_0}{k!} \left(\frac{z^3}{3}\right)^k = a_0 \exp(z^3/3).$$

Aufgabe (Herbst 2007, T3A1)

Drei Kurzaufgaben zur Funktionentheorie:

- a** Begründen Sie, dass die Funktion $f(z) = \frac{1}{z^2 - 2z + 2}$ eine konvergente Potenzreihen-Entwicklung um $z = 0$ besitzt und geben Sie deren Konvergenzradius an.
- b** Bestimmen Sie alle holomorphen Funktionen $f: \mathbb{C} \setminus \{0\} \rightarrow \mathbb{C}$ mit $|f(z)| \geq \frac{1}{|z|}$ für alle $z \neq 0$.
- c** Bestimmen Sie alle ganzen Funktionen $f: \mathbb{C} \rightarrow \mathbb{C}$ mit $f \circ f = f$.

Lösungsvorschlag zur Aufgabe (Herbst 2007, T3A1)

- a** Die Nullstellen des Nenners von f erhalten wir durch die Rechnung

$$z^2 - 2z + 2 = 0 \Leftrightarrow z = \frac{2 \pm \sqrt{4 - 8}}{2} = 1 \pm i.$$

Die Funktion ist also laut der Quotientenregel holomorph auf $\mathbb{C} \setminus \{1 \pm i\}$. Wegen $|1+i| = \sqrt{2}$ liegt insbesondere der Ball $B_{\sqrt{2}}(0)$ im Definitionsbereich. Auf diesem Bereich besitzt die Reihe nach dem Entwicklungssatz 6.10 eine Darstellung als konvergente Potenzreihe (insbesondere ist der Konvergenzradius $\geq \sqrt{2}$). Zugleich kann der Radius nicht größer als $\sqrt{2}$ sein, da die Reihe wegen $\lim_{z \rightarrow 1+i} |f(z)| = \infty$ bei $1+i$ eine nicht-hebbare Singularität besitzt.

b Wegen $|f(z)| \geq \frac{1}{|z|} > 0$ hat f keine Nullstellen. Wegen

$$|f(z)| \geq \frac{1}{|z|} \Leftrightarrow \left| \frac{1}{zf(z)} \right| \leq 1$$

ist die holomorphe Funktion $g: \mathbb{C} \setminus \{0\} \rightarrow \mathbb{C}, z \mapsto \frac{1}{zf(z)}$ nach oben beschränkt. Ferner ist 0 eine hebbare Singularität, da g in einer Umgebung der 0 beschränkt bleibt. Betrachten wir also die holomorphe Fortsetzung $\tilde{g}: \mathbb{C} \rightarrow \mathbb{C}$. Diese ist laut dem Satz von Liouville 6.20 konstant. Damit ist $g(z) = c$ für ein $c \in \mathbb{C}$ mit $|c| \leq 1$. Dies wiederum ergibt

$$g(z) = c \Leftrightarrow \frac{1}{zf(z)} = c \Leftrightarrow f(z) = \frac{1}{cz}$$

für $|c| \leq 1$.

c Zunächst bemerken wir, dass natürlich jede konstante Funktion die angegebene Gleichung erfüllt. Nehmen wir an, dass f nicht konstant ist. Wir zeigen, dass f dann bereits die Identitätsabbildung $\text{id}: z \mapsto z$ sein muss. Aufgrund der Gebietstreue muss $G = f(\mathbb{C})$ wiederum ein Gebiet sein. Sei $w_0 \in G$ beliebig und $v_0 \in \mathbb{C}$ mit $f(v_0) = w_0$. Dann gilt

$$f(w_0) = f(f(v_0)) = f(v_0) = w_0.$$

Somit stimmen f und id auf dem Gebiet G überein. Als offene Menge enthält G einen Häufungspunkt, sodass mit dem Identitätssatz 6.19 folgt, dass $f(z) = z$ für alle $z \in \mathbb{C}$. Die geforderte Gleichung $f \circ f = f$ wird also nur von konstanten Funktionen und der Identität erfüllt.

6.5. Integralrechnung im Komplexen

Anders als für zwei reelle Zahlen gibt es verschiedene Verbindungswege zwischen zwei komplexen Zahlen $a, b \in \mathbb{C}$. Möchte man nun „von a nach b “ integrieren, so muss man daher zusätzlich einen Integrationsweg angeben, d. h. eine Kurve, die die beiden Punkte verbindet und entlang derer das Integral berechnet werden soll.

Definition 6.25. Eine **Kurve** ist eine stetig differenzierbare Abbildung $\gamma: [a, b] \rightarrow U$, wobei $U \subseteq \mathbb{C}$ und $[a, b] \subseteq \mathbb{R}$. Das **Kurvenintegral** einer Funktion $f: U \rightarrow \mathbb{C}$ entlang der Kurve γ ist definiert als

$$\int_{\gamma} f(z) dz = \int_a^b (f \circ \gamma)(t) \gamma'(t) dt.$$

Glücklicherweise ist es nur selten nötig, derartige Integrale zu Fuß zu berechnen, da verschiedene Sätze dies erleichtern. Wir führen nun zunächst den Begriff

der Windungszahl einer Kurve ein und geben anschließend ein Beispiel für die explizite Berechnung eines Kurvenintegrals anhand ihrer Definition.

Definition 6.26. Sei $\gamma: [a, b] \rightarrow \mathbb{C}$ eine geschlossene Kurve und $z_0 \in \mathbb{C} \setminus \text{im } \gamma$. Die **Windungszahl** (auch **Umlaufzahl**) von γ in z_0 ist definiert als

$$n(\gamma, z_0) = \frac{1}{2\pi i} \int_{\gamma} \frac{1}{z - z_0} dz.$$

Beispiel 6.27. Sei $a \in \mathbb{C}$ und $r > 0$ sowie $n \in \mathbb{N}$. Betrachte die Kurve

$$\gamma_n: [0, 2\pi] \rightarrow \mathbb{C}, \quad t \mapsto a + re^{int},$$

welche den Kreis $\partial B_r(a)$ parametrisiert, weswegen auch oft $\int_{\partial B_r(a)} f dz$ für $\int_{\gamma_1} f dz$ geschrieben wird. Die Umlaufzahl von γ in a ist dann

$$n(\gamma, a) = \frac{1}{2\pi i} \int_{\gamma} \frac{1}{z - a} dz = \frac{1}{2\pi i} \int_0^{2\pi} \frac{1}{e^{int}} \cdot ine^{int} dt = \frac{1}{2\pi i} \int_0^{2\pi} n idt = n,$$

was auch dem Ergebnis entspricht, das wir von dem anschaulichen Konzept einer Windungszahl erwarten würden. ■

Die Berechnung der Windungszahl gestaltet sich meist deutlich schwieriger als in Beispiel 6.27, deshalb könnten folgende Ergebnisse hilfreich sein:

- (1) Die Windungszahl einer geschlossenen Kurve ist stets ganzzahlig.
- (2) Die Windungszahl ist auf Zusammenhangskomponenten konstant.

Cauchy-Integralsatz und Cauchy-Integralformel

Satz 6.28 (Cauchy-Integralsatz). Sei G ein einfach zusammenhängendes Gebiet, $f: G \rightarrow \mathbb{C}$ eine holomorphe Funktion. Dann gilt für jede geschlossene, in G verlaufende Kurve γ

$$\int_{\gamma} f(z) dz = 0.$$

Für den Begriff „einfach zusammenhängend“ existiert eine Vielzahl von äquivalenten Definitionen, der folgende Satz listet die wichtigsten auf.

Proposition 6.29. Sei $G \subseteq \mathbb{C}$ ein Gebiet. Dann sind äquivalent:

- (1) G ist einfach zusammenhängend.
- (2) G ist (homotop) einfach zusammenhängend, d. h. jede geschlossene Kurve ist nullhomotop in G , lässt sich stetig auf einen Punkt zusammenziehen.
- (3) $\mathbb{C} \setminus G$ besitzt keine beschränkte Zusammenhangskomponente.

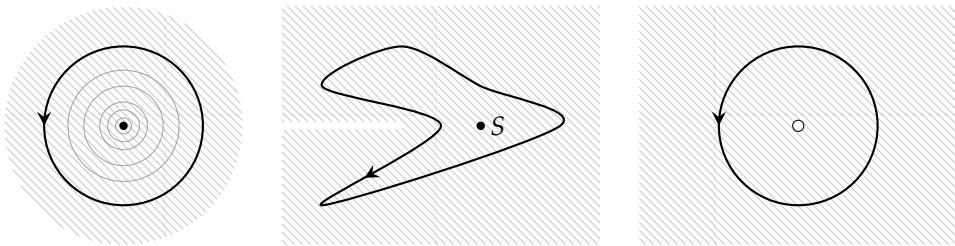


Abbildung 6.1: Der Ball links ist einfach zusammenhängend, da sich eine beliebige Kurve auf einen Punkt zusammenziehen lässt. Gleiches gilt für die geschlitzte Ebene (diese ist sternförmig, da jeder Punkt der Menge geradlinig mit S verbunden werden kann). Die punktierte Ebene rechts ist nicht einfach zusammenhängend: die eingezeichnete Kurve kann nicht auf einen Punkt in der Menge zusammengezogen werden, ohne sie „über das Loch zu ziehen“ und die Menge dabei zu verlassen.

- (4) Für jede holomorphe Funktion $f: G \rightarrow \mathbb{C}$ und jede geschlossene Kurve γ gilt der Cauchy-Integralsatz wie in Satz 6.28 formuliert.
- (5) Jede holomorphe Funktion $f: G \rightarrow \mathbb{C}$ besitzt eine Stammfunktion.

Punktierte Mengen wie $\mathbb{C} \setminus \{0\}$ sind also nicht einfach zusammenhängend. Dagegen sind Sterngebiete und geschlitzte Ebenen Beispiele für einfach zusammenhängende Mengen.

Satz 6.30 (Cauchy-Integralformel). Sei $U \subseteq \mathbb{C}$ offen und $f: U \rightarrow \mathbb{C}$ holomorph. Ist $\overline{B_r(a)} \subseteq U$, so gilt für jeden Punkt $w \in B_r(a)$ und jedes $n \in \mathbb{N}$

$$\frac{1}{n!} f^{(n)}(w) = \frac{1}{2\pi i} \int_{\partial B_r(a)} \frac{f(z)}{(z-w)^{n+1}} dz.$$

Die Cauchy-Integralformel gilt außerdem in der folgenden, allgemeineren Version:

Satz 6.31 (verallgemeinerte Cauchy-Integralformel). Sei $U \subseteq \mathbb{C}$ offen, $f: U \rightarrow \mathbb{C}$ holomorph, $\gamma: [a, b] \rightarrow \mathbb{C}$ eine geschlossene Kurve in U und $a \in \mathbb{C} \setminus \text{im } \gamma$ sowie $n \in \mathbb{N}$. Dann gilt

$$\frac{n(\gamma, w)}{n!} f^{(n)}(w) = \frac{1}{2\pi i} \int_{\gamma} \frac{f(z)}{(z-w)^{n+1}} dz.$$

Aufgabe (Frühjahr 2012, T3A1)

Berechnen Sie die folgenden Integrale, wobei $\gamma(t) = 2e^{it}$ für $t \in [0, 2\pi]$.

a $\int_{\gamma} \frac{z}{(9-z^2)(z+i)} dz, \quad \textbf{b} \int_{\gamma} \frac{5z-2}{z(z-1)} dz, \quad \textbf{c} \int_{\gamma} \frac{e^{-z}}{(z-1)^2} dz.$

Lösungsvorschlag zur Aufgabe (Frühjahr 2012, T3A1)

a Wir schreiben die Funktion als

$$\frac{z}{(9-z^2)(z+i)} = \frac{\frac{z}{9-z^2}}{z+i} = \frac{g(z)}{z+i}$$

mit $g : \mathbb{C} \setminus \{3, -3\} \rightarrow \mathbb{C}, z \mapsto \frac{z}{9-z^2}$ laut der Quotientenregel holomorph auf $B_3(0)$. Wir erhalten mit der Cauchy-Integralformel

$$\begin{aligned} \int_{\gamma} \frac{z}{(9-z^2)(z+i)} dz &= \int_{\gamma} \frac{g(z)}{z - (-i)} dz = 2\pi i g(-i) = \\ &= 2\pi i \frac{-i}{9 - (-i)^2} = 2\pi i \frac{-i}{10} = \frac{2\pi}{10} = \frac{\pi}{5}. \end{aligned}$$

b Da der Integrand zwei Singularitäten besitzt, die bei der Integration umlaufen werden, zerlegen wir die Funktion zunächst in Partialbrüche. Dazu machen wir den Ansatz

$$\frac{5z-2}{z(z-1)} = \frac{A}{z} + \frac{B}{z-1} \Leftrightarrow \frac{5z-2}{z(z-1)} = \frac{A(z-1) + Bz}{z(z-1)}.$$

Man erhält die Gleichungen $A + B = 5$ und $-A = -2$ und somit $A = 2$ und $B = 3$. Somit ist

$$\frac{5z-2}{z(z-1)} = \frac{2}{z} + \frac{3}{z-1}.$$

Die Zähler sind als konstante Funktionen holomorph auf ganz \mathbb{C} , also liefert die Cauchy-Integralformel

$$\begin{aligned} \int_{\gamma} \frac{5z-2}{z(z-1)} dz &= \int_{\gamma} \left(\frac{2}{z} + \frac{3}{z-1} \right) dz = \int_{\gamma} \frac{2}{z} dz + \int_{\gamma} \frac{3}{z-1} dz = \\ &= 2\pi i \cdot 2 + 2\pi i \cdot 3 = 10\pi i. \end{aligned}$$

c Die Funktion $g: \mathbb{C} \rightarrow \mathbb{C}$, $z \mapsto e^{-z}$ ist holomorph mit $g'(z) = -e^{-z}$. Mit der Cauchy-Integralformel 6.30 für $n = 1$ erhält man also

$$\int_{\gamma} \frac{e^{-z}}{(z-1)^2} dz = \int_{\gamma} \frac{g(z)}{(z-1)^2} dz = 2\pi i g'(1) = 2\pi i (-e^{-1}) = -\frac{2\pi i}{e}.$$

Aufgabe (Frühjahr 2013, T2A2)

Sei $f: \mathbb{C} \rightarrow \mathbb{C}$ eine ganze Funktion, $n \in \mathbb{N}_0$ und $\gamma: [0, 2\pi] \rightarrow \mathbb{C}$ die Kurve mit $\gamma(t) = e^{-it}$. Weiterhin bezeichne $P_n(z) = \sum_{j=0}^n a_j z^j$ das n -te Taylorpolynom von f mit Entwicklungspunkt $z_0 = 0$. Zeigen Sie, dass für alle $w \in \mathbb{C}$ mit $|w| > 1$ gilt:

$$P_n(w) = \frac{w^{n+1}}{2\pi i} \int_{\gamma} \frac{f(z)}{z^{n+1}(z-w)} dz.$$

Hinweis Man schreibe den im Integranden auftretenden Faktor als $\frac{1}{z-w} = -\frac{1}{w[1-(z/w)]}$ und verwende dann die geometrische Reihe.

Lösungsvorschlag zur Aufgabe (Frühjahr 2013, T2A2)

Wir berechnen, dem Hinweis folgend,

$$\begin{aligned} \frac{w^{n+1}}{2\pi i} \int_{\gamma} \frac{f(z)}{z^{n+1}(z-w)} dz &= \frac{w^{n+1}}{2\pi i} \int_{\gamma} \frac{-f(z)}{z^{n+1}w(1-\frac{z}{w})} dz = \\ &= -\frac{w^n}{2\pi i} \int_{\gamma} \frac{f(z)}{z^{n+1}} \cdot \frac{1}{1-\frac{z}{w}} dz \\ &= -\frac{w^n}{2\pi i} \int_{\gamma} \frac{f(z)}{z^{n+1}} \sum_{k=0}^{\infty} \left(\frac{z}{w}\right)^k dz \end{aligned}$$

An dieser Stelle teilen wir die Summe auf und betrachten zunächst die Summanden mit $k \geq n+1$: Sei $\varepsilon > 0$ so gewählt, dass $|w| > 1 + \varepsilon$, dann ist $q := |\frac{z}{w}| < 1$ für alle $z \in B_{1+\varepsilon}(0)$, sodass die geometrische Reihe $\sum_{k=0}^{\infty} q^k$ eine konvergente Majorante für $\sum_{k=0}^{\infty} \left(\frac{z}{w}\right)^k$ ist. Folglich definiert

$$\frac{f(z)}{z^{n+1}} \sum_{k=n+1}^{\infty} \left(\frac{z}{w}\right)^k = \frac{f(z)}{w^{n+1}} \sum_{k=0}^{\infty} \frac{z^k}{w^k}$$

eine holomorphe Funktion auf $B_{1+\varepsilon}(0)$ und laut dem Cauchy-Integralsatz 6.28 gilt

$$\int_{\gamma} \frac{f(z)}{z^{n+1}} \sum_{k=n+1}^{\infty} \left(\frac{z}{w}\right)^k dz = 0.$$

Für die restlichen Summanden verwenden wir die Cauchy-Integralformel 6.30 und erhalten

$$\begin{aligned}
 \frac{-w^n}{2\pi i} \int_{\gamma} \frac{f(z)}{z^{n+1}} \sum_{k=0}^n \left(\frac{z}{w}\right)^k dz &= \frac{-w^n}{2\pi i} \sum_{k=0}^n \int_{\gamma} \frac{f(z)}{z^{n+1}} \left(\frac{z}{w}\right)^k dz = \\
 &= \frac{-w^n}{2\pi i} \sum_{k=0}^n \int_{\gamma} \frac{f(z)}{z^{n+1-k}} \frac{1}{w^k} dz = \\
 &= \frac{-1}{2\pi i} \sum_{k=0}^n \int_{\gamma} \frac{w^{n-k} f(z)}{z^{n+1-k}} dz = \\
 &= \frac{-1}{2\pi i} \sum_{k=0}^n 2\pi i \cdot n(\gamma, w) \cdot \frac{f^{(n-k)}(w)}{(n-k)!} w^{n-k} = \\
 &= \sum_{k=0}^n \frac{f^{(n-k)}(w)}{(n-k)!} w^{n-k} = \sum_{k=0}^n \frac{f^{(k)}}{k!} w^k = P_n(w).
 \end{aligned}$$

Dabei wurde verwendet, dass die Umlaufzahl von γ um 0 gleich -1 ist.

Der Residuensatz

Bereits bei der Cauchy-Integralformel sowie dem Cauchy-Integralsatz deutet sich an, dass der Wert eines Integrals über eine geschlossene Kurve nur vom Verhalten des Integranden in unmittelbarer Nähe seiner Singularitäten abhängt. Diese Idee liegt dem Begriff des Residuums zu Grunde.

Definition 6.32. Sei $U \subseteq \mathbb{C}$ offen und $f: U \rightarrow \mathbb{C}$ eine holomorphe Funktion, die in $a \in \mathbb{C}$ eine isolierte Singularität hat. Das **Residuum** von f an der Stelle a ist definiert als

$$\text{Res}(f; a) = \frac{1}{2\pi i} \int_{\partial B_\varepsilon(a)} f(z) dz,$$

wobei der Radius $\varepsilon > 0$ des Integrationsweges so klein zu wählen ist, dass a die einzige Singularität in der Menge $B_\varepsilon(a)$ ist (nur dann ist das Residuum wohldefiniert).

Wir leiten eine Reihe von Möglichkeiten her, solche Residuen zu berechnen.

Residuen und Laurent-Reihen. Sei $a \in \mathbb{C}$ und $f: \mathbb{C} \setminus \{a\} \rightarrow \mathbb{C}$ eine holomorphe Funktion. Außerdem sei $f(z) = \sum_{n=-\infty}^{\infty} a_n z^n$ die auf $K_{r,R}(a)$ gültige Laurentreihenentwicklung von f um a . Es gilt dann

$$\text{Res}(f; a) = \frac{1}{2\pi i} \int_{\partial B_{r+\varepsilon}(a)} f(\omega) d\omega = \frac{1}{2\pi i} \int_{\partial B_{r+\varepsilon}(a)} \frac{a_{-1}}{z-a} dz \stackrel{(6.30)}{=} a_{-1},$$

denn die Terme $\frac{1}{(z-a)^k}$ besitzen für $k \neq 1$ Stammfunktionen und liefern daher keinen Beitrag zum Integral.

Im allgemeineren Fall, dass f mehrere isolierte Singularitäten besitzt und sich mehr als eine davon in $B_r(a)$ befindet, so ist durch den Koeffizienten a_{-1} entsprechend eine Summe von Residuen gegeben. Um dies zu verstehen, benötigt man jedoch bereits den Residuensatz 6.33.

Polstellen. Eine weitere Möglichkeit für den Fall, dass f in a einen Pol n -ter Ordnung hat, ergibt sich mit der Cauchy-Integralformel. Es existiert dann nämlich eine holomorphe Funktion $g: U \rightarrow \mathbb{C}$ mit $f(z) = (z - a)^{-n}g(z)$ und somit gilt

$$\begin{aligned}\operatorname{Res}(f; a) &= \frac{1}{2\pi i} \int_{\partial B_\varepsilon(a)} f(z) dz = \frac{1}{2\pi i} \int_{\partial B_\varepsilon(a)} \frac{g(z)}{(z - a)^n} dz = \\ &= \frac{1}{2\pi i} \frac{2\pi i}{(n-1)!} g^{(n-1)}(a) = \frac{g^{(n-1)}(a)}{(n-1)!}.\end{aligned}$$

Spezialfall: Pole erster Ordnung. Zuletzt betrachten wir eine Funktion f der Form $f = g/h$ wobei g in a keine, h in a eine Nullstelle erster Ordnung hat. Es gilt dann $h(z) = (z - a)\tilde{h}(z)$ für eine holomorphe Funktion \tilde{h} mit $\tilde{h}(a) \neq 0$. Weiter ist $\frac{g}{h}$ holomorph auf $\overline{B_\varepsilon(a)}$ und es folgt mit der Cauchy-Integralformel

$$\begin{aligned}\operatorname{Res}(f; a) &= \frac{1}{2\pi i} \int_{\partial B_\varepsilon(a)} \frac{g(z)}{h(z)} dz = \frac{1}{2\pi i} \int_{\partial B_\varepsilon(a)} \frac{g(z)}{(z - a)\tilde{h}(z)} dz \stackrel{(6.30)}{=} \\ &= \frac{1}{2\pi i} 2\pi i \frac{g(a)}{\tilde{h}(a)} = \frac{g(a)}{\tilde{h}(a)} = \lim_{z \rightarrow a} (z - a) \frac{g(z)}{h(z)}.\end{aligned}$$

Man erhält ferner unter Verwendung der Produktregel

$$h'(z) = (z - a)\tilde{h}'(z) + \tilde{h}(z)$$

und damit $\tilde{h}(a) = h'(a)$, also mit obiger Formel auch $\operatorname{Res}(f; a) = \frac{g(a)}{h'(a)}$.

Anleitung: Berechnung von Residuen

Gegeben sei eine Funktion $f: U \rightarrow \mathbb{C}$, die in $a \in \mathbb{C}$ eine isolierte Singularität hat. Zur Berechnung des Residuums unterscheide folgende Fälle:

- (1) Ist a eine hebbare Singularität, so verschwindet der Hauptteil der Laurent-Reihe von f um a und es gilt $\operatorname{Res}(f; a) = a_{-1} = 0$.
- (2) Ist a ein einfacher Pol, gilt also $f = g/h$, wobei h in a eine Nullstelle erster Ordnung hat, so ist

$$\operatorname{Res}(f; a) = \frac{g(a)}{h'(a)} = \lim_{z \rightarrow a} (z - a) f(z).$$

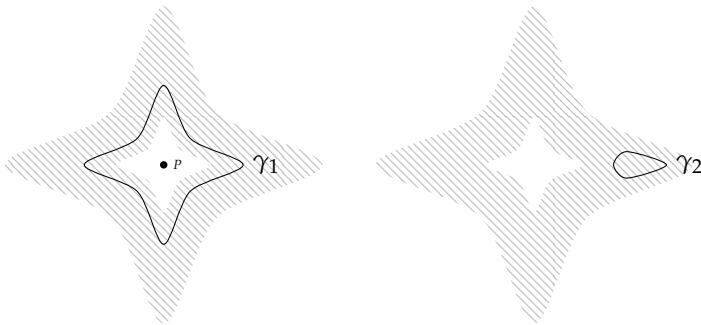


Abbildung 6.2: Die Kurve γ_1 ist in der schraffierten Menge nicht nullhomolog, da die Umlaufzahl des Punktes P , der nicht in der Menge liegt, 1 ist. Die Kurve γ_2 hingegen ist nullhomolog.

(3) Ist a ein Pol n -ter Ordnung, so gilt

$$\text{Res}(f; a) = \frac{g^{(n-1)}(a)}{(n-1)!} \quad \text{mit} \quad g(z) = (z-a)^n f(z).$$

(4) Ist a eine wesentliche Singularität, so entwickle f in eine Laurentreihe. Es genügt natürlich, dabei nur den Koeffizienten a_{-1} zu bestimmen.

Bevor wir den Residuensatz formulieren, führen wir noch einen Begriff ein. Einen Weg γ nennt man *nullhomolog* in U , wenn $n(\gamma, z) = 0$ für alle $z \in \mathbb{C} \setminus U$ gilt. Anschaulich bedeutet dies, dass das Gebiet, das von γ umrandet wird, vollständig in U liegt. Im Fall $U = \mathbb{C}$ ist dies offensichtlich stets der Fall.

Satz 6.33 (Residuensatz). Sei $U \subseteq \mathbb{C}$ offen und $S \subseteq U$ eine Menge, die keinen Häufungspunkt in U besitzt. Die Funktion $f: U \setminus S \rightarrow \mathbb{C}$ sei holomorph. Dann gilt für jeden geschlossenen, in U nullhomologen Weg $\gamma: [a, b] \rightarrow U \setminus S$

$$\int_{\gamma} f(z) dz = 2\pi i \sum_{z \in S} n(\gamma, z) \text{Res}(f; z).$$

Ist f eine holomorphe Funktion, die nur endlich viele isolierte Singularitäten a_0, \dots, a_n hat, so lässt sich im Residuensatz $S = \{a_0, \dots, a_n\}$ und $U = (\mathbb{C} \setminus S) \cup S = \mathbb{C}$ setzen. Da in \mathbb{C} jeder Weg nullhomolog ist, reduzieren sich die Anforderungen somit auf den Nachweis, dass $\gamma(t) \in U \setminus S$ für $t \in [a, b]$ erfüllt ist.

Aufgabe (Frühjahr 2007, T2A2)

Welche Werte kann das Integral

$$\int_{\gamma} \frac{dz}{z(z-1)}$$

annehmen, wenn γ alle geschlossenen Integrationswege in $\mathbb{C} \setminus \{0, 1\}$ durchläuft?

Lösungsvorschlag zur Aufgabe (Frühjahr 2007, T2A2)

Die Abbildung $f: \mathbb{C} \setminus \{0, 1\}$, $z \mapsto \frac{1}{z(z-1)}$ ist holomorph laut der Quotientenregel. Wir wenden den Residuensatz auf $U = \mathbb{C}$ und $S = \{0, 1\}$ an. Da jeder Weg in \mathbb{C} nullhomolog ist, sind bereits alle Voraussetzungen des Residuensatzes erfüllt und wir erhalten

$$\int_{\gamma} \frac{1}{z(z-1)} dz = 2\pi i \left(n(\gamma, 1) \operatorname{Res}(f; 1) + n(\gamma, 0) \operatorname{Res}(f; 0) \right).$$

Berechnen wir also die entsprechenden Residuen. Es ist klar, dass es sich bei 0 und 1 um Pole erster Ordnung handelt. Mit Formel (2) von Seite 332 ergibt sich

$$\operatorname{Res}(f; 0) = \lim_{z \rightarrow 0} z \frac{1}{z(z-1)} = -1 \quad \text{und} \quad \operatorname{Res}(f; 1) = \lim_{z \rightarrow 1} (z-1) \frac{1}{z(z-1)} = 1.$$

Somit gilt

$$\int_{\gamma} f(z) dz = 2\pi i \left(n(\gamma, 1) - n(\gamma, 0) \right).$$

Insbesondere sind die Werte ganzzahlige Vielfachen von $2\pi i$. Alle diese Werte werden auch angenommen, denn ist $k \in \mathbb{Z}$, so hat der Weg $\gamma: [0, 1] \rightarrow \mathbb{C}$, $t \mapsto \frac{1}{2}e^{2\pi i k t}$ die Umlaufzahlen $n(\gamma, 0) = k$, $n(\gamma, 1) = 0$ und erfüllt $|\gamma(t)| = \frac{1}{2}$, also $\gamma(t) \notin \{0, 1\}$ für $t \in [0, 1]$.

Aufgabe (Frühjahr 2014, T2A3)

Berechnen Sie für $\gamma: [0, 2\pi] \rightarrow \mathbb{C}$, $t \mapsto 2e^{it}$ und für $\eta: [0, 2\pi] \mapsto i + e^{-it}$ die Kurvenintegrale: **a** $\int_{\gamma} \frac{e^{iz^2} - 1}{z^2} dz$; **b** $\int_{\eta} \frac{e^z}{(z-i)^3} dz$; **c** $\int_{\gamma} e^{\frac{1}{z}} dz$.

Lösungsvorschlag zur Aufgabe (Frühjahr 2014, T2A3)

Die Wege γ und η beschreiben die Kreisränder $\partial B_2(0)$ (bzw. $\partial B_1(i)$), wobei bei letzterem das Integral im Uhrzeigersinn, also in negativer Richtung, durchlaufen wird.

- a** Die Singularität des Integranden ist $0 \in B_2(0)$. Wir können die Cauchy-Integralformel anwenden: die Funktion $g(z) = e^{iz^2} - 1$ ist auf \mathbb{C} holomorph mit $g'(z) = 2ize^{iz^2}$. Wir erhalten also

$$\int_{\partial B_2(0)} \frac{e^{iz} - 1}{z^2} dz = \frac{2\pi i}{1!} g'(0) = 0.$$

- b** Bei der Singularität handelt es sich um einen dreifachen Pol bei $i \in B_1(i)$. Wir verwenden den Residuensatz und bezeichnen den Integranden als f . Es gilt für $g(z) = (z - i)^3 f(z) = e^z$, dass

$$\text{Res}(f; i) = \frac{1}{2!} g''(i) = \frac{1}{2} e^i.$$

Nun berechnen wir noch die Umlaufzahl. Hier gilt

$$\begin{aligned} n(\eta, i) &= \frac{1}{2\pi i} \int_{\eta} \frac{1}{z - i} dz = \frac{1}{2\pi i} \int_0^{2\pi} \frac{1}{i + e^{-it} - i} \cdot (-i)e^{-it} dt \\ &= \frac{-i}{2\pi i} \int_0^{2\pi} \frac{e^{-it}}{e^{-it}} dt = \frac{-1}{2\pi} \int_0^{2\pi} 1 dt = -1. \end{aligned}$$

Wir erhalten insgesamt

$$\int_{\eta} f(z) dz = 2\pi i \cdot n(\eta, i) \text{Res}(f; i) = 2\pi i \cdot (-1) \cdot \frac{1}{2} e^i = -\pi i e^i.$$

- c** Wie man vielleicht inzwischen weiß, hat die Abbildung $f: \mathbb{C} \setminus \{0\} \rightarrow \mathbb{C}, z \mapsto \exp\left(\frac{1}{z}\right)$ hat bei 0 eine wesentliche Singularität. Wir entwickeln die Funktion daher zunächst in eine Laurent-Reihe:

$$\exp\left(\frac{1}{z}\right) = \sum_{k=0}^{\infty} \frac{1}{k!} \left(\frac{1}{z}\right)^k = \sum_{k=0}^{\infty} \frac{1}{k!} z^{-k}.$$

Der Koeffizient der (-1) -ten Potenz ist 1, dementsprechend gilt $\text{Res}(f; 0) = 1$. Für die Umlaufzahl erhalten wir mit der Cauchy-Integralformel

$$n(\gamma, 0) = \frac{1}{2\pi i} \int_{\gamma} \frac{1}{z} dz = 1.$$

Nun ist f auf $U = \mathbb{C} \setminus \{0\}$ holomorph, die geschlossene Kurve γ ist in $U \cup \{0\} = \mathbb{C}$ nullhomolog und erfüllt $\gamma(t) \neq 0$ für $t \in [0, 2\pi]$. Der Residuensatz liefert also

$$\int_{\gamma} f(z) dz = 2\pi i \cdot n(\gamma, 0) \text{Res}(f; 0) = 2\pi i \cdot 1 \cdot 1 = 2\pi i.$$

Aufgabe (Herbst 2014, T2A2)

- a** Bestimmen Sie die Laurentreihen-Entwicklung mit Entwicklungspunkt $z_0 = 0$ von

$$f(z) = \frac{1}{(z-1)(z+1)} + \frac{\sin z}{z^2}$$

im Gebiet $\{z \in \mathbb{C} \mid 0 < |z| < 1\}$.

- b** Bestimmen Sie alle isolierten Singularitäten von f und deren Typ.

- c** Berechnen Sie

$$\int_{|z-1|=\frac{3}{2}} f(z) dz.$$

Lösungsvorschlag zur Aufgabe (Herbst 2014, T2A2)

- a** Der Übersichtlichkeit halber betrachten wir die Summanden getrennt und erhalten zunächst mit der geometrischen Reihe (beachte $|z| < 1$)

$$\frac{1}{(z-1)(z+1)} = \frac{-1}{1-z^2} = -\sum_{k=0}^{\infty} z^{2k}.$$

Die Sinus-Reihe liefert weiter

$$\frac{\sin z}{z^2} = z^{-2} \sin z = z^{-2} \sum_{k=0}^{\infty} (-1)^k \frac{z^{2k+1}}{(2k+1)!} = \sum_{k=0}^{\infty} (-1)^k \frac{z^{2k-1}}{(2k+1)!}.$$

Damit ist insgesamt

$$f(z) = \sum_{k=0}^{\infty} \left(-z^{2k} + (-1)^k \frac{z^{2k-1}}{(2k+1)!} \right).$$

b Die Funktion ist an den Stellen ± 1 und 0 nicht definiert. Offensichtlich sind dies alles isolierte Singularitäten. Weiter gilt

$$\lim_{z \rightarrow 1} |f(z)| = \infty, \quad \lim_{z \rightarrow 1} (z-1)f(z) = \lim_{z \rightarrow 1} \left(\frac{1}{z+1} + \frac{(z-1)\sin z}{z^2} \right) = \frac{1}{2}.$$

Analog folgt

$$\lim_{z \rightarrow -1} |f(z)| = \infty, \quad \lim_{z \rightarrow -1} (z+1)f(z) = \lim_{z \rightarrow -1} \left(\frac{1}{z-1} + \frac{(z+1)\sin z}{z^2} \right) = -\frac{1}{2}.$$

Somit sind 1 und -1 Pole 1. Ordnung. Für $z_0 = 0$ zeigt die obige Laurent-Reihe, deren Koeffizienten wir mit $(a_n)_{n \in \mathbb{Z}}$ bezeichnen, dass $a_{-1} = 1 \neq 0$ und $a_k = 0$ für $k < -1$ gilt, sodass die Funktion auch dort einen Pol 1. Ordnung hat.

c Die beiden Singularitäten 1 und 0 liegen im Bereich $B_{\frac{3}{2}}(1)$. Wir werden den Residuensatz verwenden. Dazu bemerken wir zunächst, dass unter Verwendung der Formeln (2) und (4) aus dem Kasten auf Seite 332 gilt

$$\text{Res}(f; 1) = \lim_{z \rightarrow 1} (z-1)f(z) = \frac{1}{2}, \quad \text{Res}(f; 0) = a_{-1} = 1.$$

Laut Definition des Kurvenintegrals werden diese beiden Nullstellen einmal umlaufen; die Funktion ist auf $U = \mathbb{C} \setminus \{\pm 1, 0\}$ holomorph und γ ist (natürlich) nullhomolog in $U \cup \{\pm 1, 0\} = \mathbb{C}$. Der Residuensatz ist also anwendbar und liefert uns das Ergebnis

$$\int_{|z-1|=\frac{3}{2}} f(z) dz = 2\pi i \left(\frac{1}{2} + 1 \right) = 3\pi i.$$

Aufgabe (Herbst 2013, T1A2)

Zwei Funktionen f und g seien in einer Umgebung eines Punktes $z_0 \in \mathbb{C}$ holomorph und es gelte $f(z_0) \neq 0, g(z_0) = 0$ und $g'(z_0) \neq 0$. Beweisen Sie, dass dann

$$\text{Res}\left(\frac{f}{g}; z_0\right) = \frac{f(z_0)}{g'(z_0)}$$

ist. Berechnen Sie unter Benutzung dieses Ergebnisses das Integral

$$I = \int_{|z|=1} \frac{e^z}{\sin z} dz.$$

Lösungsvorschlag zur Aufgabe (Herbst 2013, T1A2)

Sei $g(z) = \sum_{n=0}^{\infty} a_n(z - z_0)^n$ die Potenzreihenentwicklung von g in genannter Umgebung von z_0 . Laut Angabe ist $a_0 = g(0) = 0$ und $a_1 = g'(0) \neq 0$. Somit ist

$$g(z) = \sum_{n=1} a_n(z - z_0)^n = (z - z_0) \sum_{n=0} a_{n+1}(z - z_0)^n.$$

Setze $\tilde{g}(z) = \sum_{n=0}^{\infty} a_{n+1}(z - z_0)^n$, dann ist $g(z) = (z - z_0)\tilde{g}(z)$ und $\tilde{g}(z_0) = a_1 \neq 0$.

Es gilt laut Definition für hinreichend kleines $\varepsilon > 0$

$$\text{Res}\left(\frac{f}{g}; z_0\right) = \frac{1}{2\pi i} \int_{\partial B_\varepsilon(z_0)} \frac{f(z)}{g(z)} dz.$$

Daher erhalten wir mit der Cauchy-Integralformel

$$\frac{1}{2\pi i} \int_{\partial B_\varepsilon(z_0)} \frac{f(z)}{g(z)} dz = \frac{1}{2\pi i} \int_{\partial B_\varepsilon(z_0)} \frac{f(z)}{(z - z_0)\tilde{g}(z)} dz = \frac{f(z_0)}{\tilde{g}(z_0)}.$$

Wir sind fertig, wenn wir $\tilde{g}(z_0) = g'(z_0)$ zeigen können. Laut der Produktregel gilt

$$g'(z) = (z - z_0)\tilde{g}'(z) + \tilde{g}(z) \quad \text{also } g'(z_0) = \tilde{g}(z_0).$$

Für den zweiten Teil der Aufgabe überprüfen wir zunächst die Voraussetzungen der soeben bewiesenen Aussage. Wir setzen dazu $f(z) = e^z$ und $g(z) = \sin z$. Es gilt

$$f(0) = 1 \neq 0, \quad g(0) = \sin 0 = 0, \quad g'(0) = \cos 0 = 1 \neq 0$$

und die beiden Funktionen sind auf ganz \mathbb{C} holomorph. Damit erhalten wir

$$\text{Res}\left(\frac{f}{g}; 0\right) = \frac{f(0)}{g'(0)} = \frac{1}{1} = 1.$$

Zudem sind die Nullstellen der Sinus-Funktion gegeben durch $k\pi$ für $k \in \mathbb{Z}$. Ist aber $k \neq 0$, so folgt $|k\pi| > |3k| > 1$ und $k\pi \notin B_1(0)$. Die einzige Singularität, die vom Integrationsweg umlaufen wird, ist damit 0 und der Residuensatz liefert

$$\int_{|z|=1} \frac{e^z}{\sin z} dz = 2\pi i (1 \cdot 1) = 2\pi i.$$

Aufgabe (Frühjahr 2004, T1A1)

- a** Bestimmen Sie die Art der Singularität der folgenden beiden Funktionen $f, g: \mathbb{C} \setminus \{0\} \rightarrow \mathbb{C}$ im Nullpunkt:

$$f(z) = \frac{1}{z^2} \sin(z^2), \quad g(z) = z \cos \frac{1}{z}.$$

- b** Berechnen Sie das Integral

$$\int_{\gamma} g(z) dz$$

über den positiv orientierten Rand γ des Rechtecks mit den Eckpunkten $1 - i, 1 + 3i, -4 + 3i, -4 - i$.

Lösungsvorschlag zur Aufgabe (Frühjahr 2004, T1A1)

- a** Wir berechnen die Reihendarstellung der Funktionen um $z_0 = 0$. Es gilt

$$f(z) = \frac{1}{z^2} \sin(z^2) = z^{-2} \sum_{k=0}^{\infty} (-1)^k \frac{(z^2)^{2k+1}}{(2k+1)!} = \sum_{k=0}^{\infty} (-1)^k \frac{z^{4k}}{(2k+1)!}.$$

Somit verschwindet der Hauptteil der Laurent-Reihendarstellung und 0 ist eine hebbare Singularität der Funktion.

Für die zweite Funktion erhalten wir

$$g(z) = z \cos \frac{1}{z} = z \sum_{k=0}^{\infty} (-1)^k \frac{z^{-2k}}{(2k)!} = \sum_{k=0}^{\infty} (-1)^k \frac{z^{-2k+1}}{(2k)!}.$$

Da in dieser Reihe unendlich viele Potenzen von z mit negativem Exponenten als Summand auftreten, handelt es sich bei 0 um eine wesentliche Singularität der Funktion g .

- b** Der Weg ist nullhomolog in \mathbb{C} . Damit gilt laut dem Residuensatz

$$\int_{\gamma} g(z) dz = 2\pi i \cdot n(\gamma, 0) \cdot \operatorname{Res}(g; 0).$$

In der Reihendarstellung aus Teil **a** erhalten wir den Koeffizienten von z^{-1} für $k = 1$. Es ist also

$$\operatorname{Res}(g; 0) = -\frac{1}{2!} = -\frac{1}{2}.$$

Da der Weg positiv orientiert, also $n(\gamma, 0) = 1$ ist, folgt

$$\int_{\gamma} g(z) dz = -\pi i.$$

Berechnung reeller Integrale mittels Residuensatz

In diesem Abschnitt entwickeln wir das *Residuenkalkül*, welches die Anwendung komplexer Methoden zur Berechnung bestimmter reeller Integrale meint. Diese Integrale können meist nicht durch die Angabe einer Stammfunktion berechnet werden, sodass man auf andere Verfahren angewiesen ist.

Proposition 6.34. Seien p und q Polynome mit $\text{grad } q \geq \text{grad } p + 2$. Außerdem setzen wir voraus, dass q keine reellen Nullstellen hat. Dann existiert das uneigentliche Riemann-Integral

$$\int_{-\infty}^{\infty} \frac{p(x)}{q(x)} dx.$$

Anleitung: Reelle Integrale und Residuensatz I (rationale Funktionen)

Gegeben sei ein Integral der Form

$$\int_{-\infty}^{\infty} \frac{p(x)}{q(x)} dx,$$

wobei p und q Polynome mit $\text{grad } q \geq \text{grad } p + 2$ sind und q nullstellenfrei über \mathbb{R} ist. Ziel ist die Berechnung des Wertes des Integrals, das laut Proposition 6.34 existiert.

- (1) Bestimme die komplexen Nullstellen des Nenners und deren Vielfachheit. Gib sodann die komplexe Funktion $f(z) = \frac{p(z)}{q(z)}$ mit zugehörigem Definitionsbereich an.
- (2) Definiere für $R > 0$ den Weg $\gamma_1 * \gamma_2$ als Konkatenation der beiden Wege

$$\gamma_1: [-R, R] \rightarrow \mathbb{C}, \quad t \mapsto t, \quad \text{und} \quad \gamma_2: [0, \pi] \rightarrow \mathbb{C}, \quad t \mapsto Re^{it}.$$

- (3) Gib die Menge S der Polstellen an, die vom Weg $\gamma_1 * \gamma_2$ umlaufen werden, und berechne die Residuen von f an diesen Stellen.

(4) Mit dem Residuensatz ist nun

$$\begin{aligned} \lim_{R \rightarrow \infty} \int_{\gamma_1} f(z) dz + \lim_{R \rightarrow \infty} \int_{\gamma_2} f(z) dz &= \lim_{R \rightarrow \infty} \int_{\gamma_1 * \gamma_2} f(z) dz = \\ &= 2\pi i \sum_{z \in S} n(\gamma_1 * \gamma_2, z) \operatorname{Res}(f; z), \end{aligned}$$

wobei die Summe über die relevanten Polstellen gebildet wird.

- (5) Zeige zu guter Letzt mittels geeigneter Abschätzungen, dass der Grenzwert $\lim_{R \rightarrow \infty} \int_{\gamma_2} f(z) dz = 0$ ist. Dazu verwende die Definition des Kurvenintegrals aus Definition 6.25 sowie Abschätzungen folgender Art:
- Für integrierbare Funktionen gilt $|\int f(z) dz| \leq \int |f(z)| dz$.
 - Die (gewöhnliche) Dreiecksungleichung

$$|x + y| \leq |x| + |y| \quad (\triangle)$$

(c) Die umgekehrte Dreiecksungleichung

$$|x - y| \geq ||x| - |y|| \quad \text{bzw.} \quad |x + y| = |x - (-y)| \geq ||x| - |y|| \quad (\nabla)$$

Erhalte dann eine von R abhängige Abschätzung des Integranden. Die Multiplikation mit der Länge des Integrationswegs ergibt dann eine Abschätzung des gesamten Integrals, die für $R \rightarrow \infty$ gegen 0 geht.

(6) Übrig bleibt

$$\int_{-\infty}^{\infty} f(z) dz = \lim_{R \rightarrow \infty} \int_{\gamma_1} f(z) dz = 2\pi i \sum_{z \in S} n(\gamma_1 * \gamma_2, z) \operatorname{Res}(f; z).$$

Aufgabe (Frühjahr 2014, T3A3)

a Berechnen Sie das Integral

$$\int_0^\infty \frac{r^2}{1+r^4} dr.$$

b Berechnen Sie das Integral

$$\int_{\mathbb{R}^3} \frac{dx}{1+|x|^4}.$$

Dabei bezeichnet $|x| := \sqrt{x_1^2 + x_2^2 + x_3^2}$ die euklidische Norm von $x \in \mathbb{R}^3$.

Lösungsvorschlag zur Aufgabe (Frühjahr 2014, T3A3)

- a) Das Integral existiert laut Proposition 6.34, da der Grad des Nennerpolynoms um zwei größer als der des Zählerpolynoms ist und der Nenner keine reellen Nullstellen besitzt. Ferner ist der Integrand als gerade Funktion achsensymmetrisch zur y -Achse, also gilt

$$\int_0^\infty \frac{r^2}{1+r^4} dr = \frac{1}{2} \int_{-\infty}^\infty \frac{r^2}{1+r^4} dr.$$

Wir bestimmen zunächst die komplexen Nullstellen des Nenners. Für $k \in \mathbb{Z}$ gilt

$$z^4 + 1 = 0 \Leftrightarrow z^4 = -1 = e^{i\pi+2k\pi i} \Leftrightarrow z \in \left\{ e^{\frac{i\pi}{4}}, e^{\frac{3i\pi}{4}}, e^{\frac{5i\pi}{4}}, e^{\frac{7i\pi}{4}} \right\} = D$$

Sei nun $R > 1$. Wir betrachten die holomorphe Funktion $f: \mathbb{C} \setminus D \rightarrow \mathbb{C}$, $z \mapsto \frac{z^2}{1+z^4}$ sowie die beiden Wege

$$\gamma_1: [-R, R] \rightarrow \mathbb{C}, \quad t \mapsto t \quad \text{und} \quad \gamma_2: [0, \pi] \rightarrow \mathbb{C}, \quad t \mapsto Re^{it}.$$

Die Konkatenation $\gamma_1 * \gamma_2$ liefert einen Weg, der in der oberen Halbebene verläuft. Wegen $R > 1$ umläuft dieser alle Pole von f , die positiven Imaginärteil haben. Dies sind $e^{\frac{i\pi}{4}}$ und $e^{\frac{3i\pi}{4}}$. Berechnen wir die Residuen an den entsprechenden Stellen: Da die Singularitäten jeweils einfache Nullstellen des Nennerpolynoms sind, können wir (2) von Seite 332 anwenden. Die Ableitung des Nenners ist gegeben durch $4z^3$. Dementsprechend ist

$$\operatorname{Res}\left(f; e^{\frac{i\pi}{4}}\right) = \frac{\left(e^{\frac{i\pi}{4}}\right)^2}{4\left(e^{\frac{i\pi}{4}}\right)^3} = \frac{1}{4e^{\frac{3i\pi}{4}}} = \frac{1}{4}e^{-\frac{i\pi}{4}}$$

sowie

$$\operatorname{Res}\left(f; e^{\frac{3i\pi}{4}}\right) = \frac{\left(e^{\frac{3i\pi}{4}}\right)^2}{4\left(e^{\frac{3i\pi}{4}}\right)^3} = \frac{1}{4e^{\frac{5i\pi}{4}}} = \frac{1}{4}e^{-\frac{3i\pi}{4}}.$$

Bereits jetzt liefert uns der Residuensatz

$$\begin{aligned} \int_{\gamma_1 * \gamma_2} f(z) dz &= 2\pi i \left(\frac{1}{4} e^{-\frac{i\pi}{4}} + \frac{1}{4} e^{-3\frac{i\pi}{4}} \right) = \\ &= \frac{1}{2} \pi i \left[\cos\left(-\frac{\pi}{4}\right) + i \sin\left(-\frac{\pi}{4}\right) + \cos\left(-\frac{3\pi}{4}\right) + i \sin\left(-\frac{3\pi}{4}\right) \right] = \\ &= \frac{1}{2} \pi i \left[\cos\left(\frac{\pi}{4}\right) - i \sin\left(\frac{\pi}{4}\right) - \cos\left(\frac{3\pi}{4}\right) - i \sin\left(\frac{3\pi}{4}\right) \right] = \\ &= \frac{1}{2} \pi i \left[-2i \sin\left(\frac{\pi}{4}\right) \right] = \pi \sin\left(\frac{\pi}{4}\right) = \frac{\pi}{\sqrt{2}}. \end{aligned}$$

Als Nächstes zeigen wir

$$\lim_{R \rightarrow \infty} \int_{\gamma_2} f(z) dz = 0.$$

Es gilt für $R > 1$ wegen $|e^{it}| = 1$ für $t \in \mathbb{R}$, dass

$$\begin{aligned} \left| \int_{\gamma_2} f(z) dz \right| &= \left| \int_0^\pi \frac{R^2(e^{it})^2}{1+R^4(e^{it})^4} Rie^{it} dt \right| \leq \int_0^\pi \frac{|R^2(e^{it})^2|}{|1+R^4(e^{it})^4|} |Rie^{it}| dt \stackrel{(\nabla)}{\leq} \\ &\quad \int_0^\pi \frac{R^3}{|1-|R^4|||(e^{it})^4||} dt = \int_0^\pi \frac{R^3}{|1-R^4|} dt = \frac{\pi R^3}{R^4-1}. \end{aligned}$$

Wir sehen

$$\lim_{R \rightarrow \infty} \left| \int_{\gamma_2} f(z) dz \right| \leq \lim_{R \rightarrow \infty} \frac{\pi R^3}{R^4-1} = 0 \quad \Rightarrow \quad \lim_{R \rightarrow \infty} \int_{\gamma_2} f(z) dz = 0.$$

Damit folgt aber schließlich für das zu bestimmende Integral

$$\begin{aligned} \frac{1}{2} \int_{-\infty}^{\infty} \frac{r^2}{1+r^4} dr &= \frac{1}{2} \lim_{R \rightarrow \infty} \int_{\gamma_1 * \gamma_2} f(z) dz - \frac{1}{2} \lim_{R \rightarrow \infty} \int_{\gamma_2} f(z) dz = \\ &= \frac{\pi}{2\sqrt{2}} - \frac{1}{2} \cdot 0 = \frac{\pi}{2\sqrt{2}}. \end{aligned}$$

- b** Wir verwenden hier den Transformationssatz mit der Kugel-Koordinaten-Abbildung. Sei $M = [0, \infty[\times] -\frac{\pi}{2}, \frac{\pi}{2}[\times [0, 2\pi[$ und

$$\phi: M \rightarrow \mathbb{R}^3, \quad (r, \vartheta, \varphi) \mapsto (r \cos \vartheta \cos \varphi, r \cos \vartheta \sin \varphi, r \sin \vartheta).$$

Bekanntlich ist ϕ ein Diffeomorphismus mit $|\det \phi'(r\vartheta, \varphi)| = r^2 \cos \vartheta$ (Formelsammlung!). Nun gilt

$$\begin{aligned}\frac{1}{1 + |\phi(r, \vartheta, \varphi)|^4} &= \frac{1}{1 + (r^2 \cos^2 \vartheta \cos^2 \varphi + r^2 \cos^2 \vartheta \sin^2 \varphi + r^2 \sin^2 \vartheta)^2} = \\ &= \frac{1}{1 + r^4 (\cos^2 \vartheta (\cos^2 \varphi + \sin^2 \varphi) + \sin^2 \vartheta)^2} = \\ &= \frac{1}{1 + r^4 (\cos^2 \vartheta + \sin^2 \vartheta)^2} = \frac{1}{1 + r^4}.\end{aligned}$$

Wir erhalten damit

$$\begin{aligned}\int_{\mathbb{R}^3} \frac{1}{1 + |x|^4} dx &= \int_M \frac{|\det \phi'(r, \vartheta, \varphi)|}{1 + |\phi(r, \vartheta, \varphi)|^4} d(r, \vartheta, \varphi) = \\ &= \int_0^\infty \left(\int_{-\frac{\pi}{2}}^{\frac{\pi}{2}} \left(\int_0^{2\pi} \frac{r^2 \cos \vartheta}{1 + r^4} d\varphi \right) d\vartheta \right) dr = \int_0^\infty \left(\int_{-\frac{\pi}{2}}^{\frac{\pi}{2}} 2\pi \frac{r^2 \cos \vartheta}{1 + r^4} d\vartheta \right) dr = \\ &= 2\pi \int_0^\infty \frac{r^2}{1 + r^4} \left(\int_{-\frac{\pi}{2}}^{\frac{\pi}{2}} \cos \vartheta d\vartheta \right) dr = 4\pi \int_0^\infty \frac{r^2}{1 + r^4} dr \stackrel{\text{a}}{=} \frac{2\pi^2}{\sqrt{2}}.\end{aligned}$$

Dabei haben wir in der letzten Zeile

$$\int_{-\frac{\pi}{2}}^{\frac{\pi}{2}} \cos \vartheta d\vartheta = \left[\sin \vartheta \right]_{-\frac{\pi}{2}}^{\frac{\pi}{2}} = \sin\left(\frac{\pi}{2}\right) - \sin\left(-\frac{\pi}{2}\right) = 2$$

verwendet.

Aufgabe (Frühjahr 2013, T1A3)

- a** Bestimmen Sie Lage und Ordnung der Pole der meromorphen Funktion

$$f(z) = \frac{1}{1 + 2z^2 + z^4}.$$

- b** Berechnen Sie

$$\int_{-\infty}^{\infty} \frac{1}{1 + 2x^2 + x^4} dx$$

mit Hilfe des Residuensatzes.

- c** Geben Sie die Laurent-Reihe in einem der Pole an.

Lösungsvorschlag zur Aufgabe (Frühjahr 2013, T1A3)

a Es gilt

$$f(z) = \frac{1}{1+2z^2+z^4} = \frac{1}{(z^2+1)^2} = \frac{1}{(z-i)^2(z+i)^2}.$$

Somit hat f in i und $-i$ jeweils einen Pol zweiter Ordnung.

b Das Integral existiert, da der Nenner keine reellen Nullstellen hat und der Nennergrad um mehr als 2 größer als der Zählergrad ist. Wir definieren die beiden Wege $\gamma_1: [-R, R] \rightarrow \mathbb{C}$, $t \mapsto t$ und $\gamma_2: [0, \pi] \rightarrow \mathbb{C}$, $t \mapsto Re^{it}$. Die von $\gamma_1 * \gamma_2$ umlaufene Polstelle ist i . Das Residuum berechnet sich für $g(z) = (z-i)^2 f(z) = \frac{1}{(z+i)^2}$ mit $g'(z) = \frac{-2(z+i)}{(z+i)^4}$ zu

$$\text{Res}(f; i) = \frac{1}{1!} g'(i) = \frac{-2 \cdot 2i}{(2i)^4} = \frac{-4i}{16} = \frac{-i}{4}.$$

Und damit ist laut dem Residuensatz

$$\int_{\gamma_1 * \gamma_2} f(z) dz = 2\pi i \cdot \frac{-i}{4} = \frac{\pi}{2}.$$

Sei nun $R > 1$. Wir erhalten

$$\begin{aligned} \left| \int_{\gamma_2} f(z) dz \right| &= \left| \int_{\gamma} \frac{1}{(z^2+1)^2} dz \right| \leq \int_0^\pi \frac{|Re^{it}|}{|R^2 e^{2it} + 1|^2} dt \\ &\stackrel{(\nabla)}{\leq} \int_0^\pi \frac{R}{|R^2 - 1|} dt = \frac{\pi R}{R^2 - 1} \end{aligned}$$

Somit gilt

$$\lim_{R \rightarrow \infty} \left| \int_{\gamma_2} f(z) dz \right| \leq \lim_{R \rightarrow \infty} \frac{\pi R}{R^2 - 1} = 0 \quad \Rightarrow \quad \lim_{R \rightarrow \infty} \int_{\gamma_2} f(z) dz = 0.$$

Dies wiederum bedeutet

$$\int_{-\infty}^{\infty} \frac{1}{1+2x^2+x^4} dx = \lim_{R \rightarrow \infty} \int_{\gamma_1} f(z) dz = \frac{\pi}{2}.$$

c Da die Funktion symmetrisch ist, macht es von der Schwierigkeit her keinen Unterschied, welcher Pol verwendet wird. Wir wählen $z_0 = i$. Mit der Zerlegung aus Teil **a** gilt zunächst

$$f(z) = (z-i)^{-2} \frac{1}{(z+i)^2}.$$

Um den hinteren Teil in eine Reihe der Form $\sum_{k=0}^{\infty} a_k(z-i)^k$ zu entwickeln, verwenden wir zunächst die geometrische Reihe:

$$\begin{aligned}\frac{1}{z+i} &= \frac{1}{z-i+i+i} = \frac{1}{(z-i)+2i} = \frac{1}{2i} \frac{1}{1-\frac{(-z+i)}{2i}} = \frac{1}{2i} \sum_{k=0}^{\infty} \left(\frac{-z+i}{2i}\right)^k = \\ &= \frac{1}{2i} \sum_{k=0}^{\infty} \left(\frac{-1}{2i}\right)^k (z-i)^k = \frac{1}{2i} \sum_{k=0}^{\infty} \left(\frac{i}{2}\right)^k (z-i)^k\end{aligned}$$

Nun gilt mittels gliedweisem Differenzieren

$$\frac{1}{(z+i)^2} = -\frac{d}{dz} \left(\frac{1}{z+i}\right) = -\frac{1}{2i} \sum_{k=1}^{\infty} k \left(\frac{i}{2}\right)^k (z-i)^{k-1}.$$

Somit erhalten wir insgesamt

$$\begin{aligned}f(z) &= -\frac{1}{2i} (z-i)^{-2} \sum_{k=1}^{\infty} k \left(\frac{i}{2}\right)^k (z-i)^{k-1} = -\frac{1}{2i} \sum_{k=1}^{\infty} k \left(\frac{i}{2}\right)^k (z-i)^{k-3} = \\ &= -\frac{1}{2i} \sum_{k=-2}^{\infty} (k+3) \left(\frac{i}{2}\right)^{k+3} (z-i)^k = \frac{1}{16} \sum_{k=-2}^{\infty} (k+3) \left(\frac{i}{2}\right)^k (z-i)^k.\end{aligned}$$

Anleitung: Reelle Integrale und Residuensatz II (Funktionen mit Sinus oder Kosinus)

Gegeben sei ein Integral (i. d. R. von 0 bis 2π) über eine von Sinus- und Kosinusfunktionen abhängige gebrochene Funktion, deren Nenner keine reelle Nullstelle besitzt.

- (1) Ersetze den Sinus oder Kosinus mittels einer der Identitäten

$$\cos t = \frac{1}{2} (e^{it} + e^{-it}) \quad \text{oder} \quad \sin t = \frac{1}{2i} (e^{it} - e^{-it}).$$

- (2) Ergänze im Integral den Faktor $\frac{\gamma'(t)}{i\gamma(t)} = \frac{ie^{it}}{ie^{it}} = 1$, wobei γ der Weg $\gamma: [0, 2\pi] \rightarrow \mathbb{C}$, $t \mapsto e^{it}$ ist.
- (3) Laut der Definition des Kurvenintegrals (vgl. 6.25) lässt sich das Integral nun in ein Kurvenintegral über den Rand des Einheitskreises umschreiben. Bestimme die zugehörige Funktion im Integranden.
- (4) Ermittle mittels des Residuensatzes den Wert dieses Integrals.

Aufgabe (Herbst 2010, T1A4)

Zeigen Sie mithilfe des Residuensatzes, dass

$$I := \int_0^{2\pi} \frac{dt}{5 + 3 \cos t} = \frac{\pi}{2}$$

ist.

Lösungsvorschlag zur Aufgabe (Herbst 2010, T1A4)

Wegen $|\cos t| \leq 1$ hat die Funktion $f: [0, 2\pi] \rightarrow \mathbb{R}$, $t \mapsto \frac{1}{5+3\cos t}$ keine Polstellen und ist somit als stetige Funktion auf einem beschränkten Intervall integrierbar.

Wir verwenden die Identität $\cos t = \frac{1}{2}(e^{it} + e^{-it})$ und erhalten

$$\int_0^{2\pi} \frac{1}{5 + 3 \cos t} dt = \int_0^{2\pi} \frac{1}{5 + \frac{3}{2}(e^{it} + e^{-it})} dt = \int_0^{2\pi} \frac{1}{5 + \frac{3}{2}(e^{it} + e^{-it})} \cdot \frac{ie^{it}}{ie^{it}} dt.$$

Mit der Kurve $\gamma: [0, 2\pi] \rightarrow \mathbb{C}$, $t \mapsto e^{it}$ wird die letzte Gleichung zu

$$\begin{aligned} \int_0^{2\pi} \frac{1}{5 + \frac{3}{2}(\gamma(t) + \frac{1}{\gamma(t)})} \cdot \frac{\gamma'(t)}{i\gamma(t)} dt &= \int_0^{2\pi} \frac{-i\gamma'(t)}{5\gamma(t) + \frac{3}{2}(\gamma(t)^2 + 1)} dt = \\ &= \int_{\gamma} \frac{-i}{5z + \frac{3}{2}(z^2 + 1)} dz. \end{aligned}$$

Die Nullstellen des Nenners bestimmt man mittels

$$\frac{3}{2}z^2 + 5z + \frac{3}{2} = 0 \Leftrightarrow z = \frac{-5 \pm \sqrt{5^2 - 4 \cdot \frac{3}{2} \cdot \frac{3}{2}}}{3} = \frac{-5 \pm 4}{3}.$$

Damit sind die Nullstellen des Nenners -3 und $-\frac{1}{3}$. Diese sind somit einfache Polstellen der Funktion

$$f: \mathbb{C} \setminus \left\{ -3, -\frac{1}{3} \right\} \rightarrow \mathbb{C}, \quad z \mapsto \frac{-i}{5z + \frac{3}{2}(z^2 + 1)}.$$

Da $n(\gamma, -3) = 0$ ist ergibt sich mit dem Residuensatz

$$I = \int_{\gamma} \frac{-i}{5z + \frac{3}{2}(z^2 + 1)} dz = 2\pi i \cdot n\left(\gamma, -\frac{1}{3}\right) \cdot \text{Res}\left(f; -\frac{1}{3}\right).$$

Wir berechnen das nötige Residuum und benutzen dazu die Ableitung $3z + 5$ des Nenners:

$$\text{Res}\left(f; -\frac{1}{3}\right) = \frac{-i}{3 \cdot \left(-\frac{1}{3}\right) + 5} = \frac{-i}{4}$$

und somit

$$I = 2\pi i \cdot \frac{-i}{4} = \frac{\pi}{2}.$$

Aufgabe (Frühjahr 2003, T2A3)

Berechnen Sie für $a \in \mathbb{R}, a > 1$ das Integral

$$\int_0^{2\pi} \frac{d\varphi}{a + \cos \varphi}.$$

Lösungsvorschlag zur Aufgabe (Frühjahr 2003, T2A3)

Auch hier sei zunächst bemerkt, dass das Integral existiert, da der Nenner keine Nullstellen hat.

Mittels $\cos t = \frac{1}{2}(e^{it} + e^{-it})$ erhalten wir für die Kurve $\gamma : [0, 2\pi] \rightarrow \mathbb{C}$, $t \mapsto e^{it}$

$$\begin{aligned} \int_0^{2\pi} \frac{1}{a + \cos \varphi} d\varphi &= \int_0^{2\pi} \frac{1}{a + \frac{1}{2}(e^{it} + e^{-it})} dt = \int_0^{2\pi} \frac{2}{2a + (e^{it} + e^{-it})} \cdot \frac{ie^{it}}{ie^{it}} dt = \\ &= \int_0^{2\pi} \frac{2}{2a + (\gamma(t) + \gamma(t)^{-1})} \cdot \frac{\gamma'(t)}{i\gamma(t)} dt = \int_0^{2\pi} \frac{-2i\gamma'(t)}{2a\gamma(t) + (\gamma(t)^2 + 1)} dt = \\ &= \int_{\gamma} \frac{-2i}{2za + z^2 + 1} dz. \end{aligned}$$

Untersuchen wir den Nenner des Integranden auf Nullstellen!

$$z^2 + 2az + 1 = 0 \Leftrightarrow z = \frac{-2a \pm \sqrt{4a^2 - 4}}{2} = -a \pm \sqrt{a^2 - 1}.$$

Beide Polstellen sind wegen $a^2 - 1 > 0$ reell (beachte $a > 1$). Wegen

$$z_1 = -a - \sqrt{a^2 - 1} < -a < -1$$

ist aber $z_1 \notin B_1(0)$. Zumindest z_2 liegt jedoch in $B_1(0)$: Wegen $\sqrt{a^2 - 1} <$

$\sqrt{a^2} = a$ ist $z_2 < -a + a = 0$. Ferner ist

$$\begin{aligned} -a + \sqrt{a^2 - 1} > -1 &\Leftrightarrow \sqrt{a^2 - 1} > a - 1 \Leftrightarrow a^2 - 1 > a^2 - 2a + 1 \\ &\Leftrightarrow a > 1 \end{aligned}$$

und die letzte Gleichung gilt laut Voraussetzung. Insgesamt gilt $-1 < z_2 < 0$ und damit $z_2 \in B_1(0)$. Der Residuensatz liefert sodann

$$\int_{\gamma} \frac{-2i}{2za + z^2 + 1} dz = 2\pi i \cdot n(\gamma, z_2) \cdot \operatorname{Res}(f; z_2).$$

Berechnen wir noch das fragliche Residuum! Hier gilt unter Verwendung der Nenner-Ableitung $2z + 2a = 2(z + a)$, dass

$$\operatorname{Res}(f; z_2) = \frac{-2i}{2(z_2 + a)} = \frac{-i}{\sqrt{a^2 - 1}}.$$

Und somit erhalten wir

$$\int_0^{2\pi} \frac{d\varphi}{a + \cos \varphi} = 2\pi i \cdot \frac{-i}{\sqrt{a^2 - 1}} = \frac{2\pi}{\sqrt{a^2 - 1}}.$$

Für die folgende Aufgabe benötigen wir noch die Definition des Residuums im „Punkt“ ∞ . Man setzt hier analog zur Definition 6.32

$$\operatorname{Res}(f; \infty) = -\frac{1}{2\pi i} \int_{\gamma} f(z) dz$$

für eine Kurve γ mit hinreichend großem Radius, sodass keine andere Singularität umlaufen wird. Eine für die explizite Berechnung besser geeignete Formel ist

$$\operatorname{Res}(f; \infty) = \operatorname{Res}\left(\frac{-1}{z^2} f\left(\frac{1}{z}\right); 0\right),$$

die man mittels Substitution $z \mapsto \frac{1}{z}$ aus der Definition erhält.

Aufgabe (Herbst 2003, T1A3)

- a Bestimmen Sie die Residuen der Funktion

$$f(z) = \frac{1}{z^3 - z^5}$$

in allen Singularitäten sowie im Punkt ∞ .

b Berechnen Sie das Integral

$$\int_C \frac{dz}{z^4 + 1},$$

wobei C die positiv durchlaufene Kreislinie $(x - 1)^2 + y^2 = 1, z = x + iy$ bezeichne.

Lösungsvorschlag zur Aufgabe (Herbst 2003, T1A3)

a Es gilt

$$f(z) = -\frac{1}{z^3} \cdot \frac{1}{z-1} \cdot \frac{1}{z+1}.$$

Somit hat f jeweils eine einfache Polstelle bei 1 und -1 sowie eine dreifache bei 0 . Gemäß dem im Kasten auf Seite 332 beschriebenen Verfahren berechnen wir für $g(z) = z^3 f(z) = \frac{1}{1-z^2}$ die Ableitungen

$$g'(z) = \frac{2z}{(1-z^2)^2} \quad \text{und} \quad g''(z) = \frac{2(1-z^2)^2 + 8z^2(1-z^2)}{(1-z^2)^4}.$$

Die Formel liefert sodann

$$\operatorname{Res}(f; 0) = \frac{1}{2!} g''(0) = \frac{1}{2} \cdot 2 = 1.$$

Für die beiden Residuen bei ± 1 gilt

$$\operatorname{Res}(f; 1) = \lim_{z \rightarrow 1} (z-1) \frac{-1}{z^3(z-1)(z+1)} = -\frac{1}{2} \quad \text{und analog}$$

$$\operatorname{Res}(f; -1) = \frac{1}{2}.$$

Zur Berechnung von $\operatorname{Res}(f; \infty)$ bemerken wir, dass die Funktion $\frac{-1}{z^2} f\left(\frac{1}{z}\right)$ wegen

$$\lim_{z \rightarrow 0} \frac{-1}{z^2} f\left(\frac{1}{z}\right) = \lim_{z \rightarrow 0} \frac{-1}{z^2} \frac{1}{\frac{1}{z^3} - \frac{1}{z^5}} = \lim_{z \rightarrow 0} \frac{-1}{z^2} \cdot \frac{z^5}{z^2 - 1} = \lim_{z \rightarrow 0} \frac{-z^3}{z^2 - 1} = 0$$

eine hebbare Singularität bei 0 hat. Somit gilt

$$\operatorname{Res}(f; \infty) = \operatorname{Res}\left(\frac{-1}{z^2} f\left(\frac{1}{z}\right); 0\right) = 0.$$

b Dies ist eine uns bereits bekannte Funktion. Wir haben die Menge der Nullstellen bereits zu

$$D = \left\{ e^{\frac{i\pi}{4}}, e^{\frac{3i\pi}{4}}, e^{\frac{5i\pi}{4}}, e^{\frac{7i\pi}{4}} \right\}$$

bestimmt (vgl. F14T3A3, Seite 341). Bei der Kurve C handelt es sich um den Rand des Kreises $B_1(1)$. Für Elemente $z \in B_1(1)$ gilt $\operatorname{Re} z > 0$. Somit kommen nur $e^{\frac{i\pi}{4}}$ und $e^{\frac{7i\pi}{4}}$ als umlaufene Singularitäten in Frage. Diese liegen auch tatsächlich im Integrationsbereich, es gilt nämlich

$$\left| e^{\frac{i\pi}{4}} - 1 \right| = \left| i \sin\left(\frac{\pi}{4}\right) + \cos\left(\frac{\pi}{4}\right) - 1 \right| = \sqrt{2 - \sqrt{2}} < 1$$

und ebenso $\left| e^{\frac{7i\pi}{4}} - 1 \right| < 1$. Man berechnet die relevanten Residuen zu

$$\operatorname{Res}\left(f; e^{\frac{i\pi}{4}}\right) = \frac{1}{4(e^{\frac{i\pi}{4}})^3} = \frac{e^{-\frac{3i\pi}{4}}}{4} \quad \text{und} \quad \operatorname{Res}\left(f; e^{\frac{7i\pi}{4}}\right) = \frac{1}{4(e^{\frac{7i\pi}{4}})^3} = \frac{e^{\frac{3i\pi}{4}}}{4}.$$

Somit erhalten wir mit

$$\begin{aligned} \int_{\gamma} \frac{1}{z^4 + 1} dz &= 2\pi i \left(\frac{e^{-\frac{3i\pi}{4}}}{4} + \frac{e^{\frac{3i\pi}{4}}}{4} \right) = \frac{\pi i}{2} \left(2 \cos\left(\frac{3\pi}{4}\right) \right) = \\ &= \frac{\pi i}{2} (-\sqrt{2}) = -\frac{\pi i}{\sqrt{2}}. \end{aligned}$$

Anleitung: Reelle Integrale und Residuensatz III (Sinus- und Kosinusfunktion und rationale Funktion)

Seien p und q Polynome mit $\operatorname{grad} q \geq \operatorname{grad} p + 1$, und $q(x) \neq 0$ für $x \in \mathbb{R}$. Berechnet werden soll ein Integral der Form

$$\int_{-\infty}^{\infty} \sin x \frac{p(x)}{q(x)} dx \quad \text{oder} \quad \int_{-\infty}^{\infty} \cos x \frac{p(x)}{q(x)} dx.$$

(1) Bei dem Integral handelt es sich um den Real- oder Imaginärteil des Integrals

$$\int_{-\infty}^{\infty} e^{ix} \frac{p(x)}{q(x)} dx = \lim_{R \rightarrow \infty} \int_{\gamma_R} e^{iz} \frac{p(z)}{q(z)} dz$$

für den Weg $\gamma_R: [-R, R] \rightarrow \mathbb{C}, t \mapsto t$.

(2) Gib einen Weg δ_R an, sodass $\gamma_R * \delta_R$ ein geschlossener Weg ist. Ist $\text{grad } q \geq \text{grad } p + 2$, so tut es der bereits bekannte Halbbogen. Ansonsten liefert ein Rechteckweg bessere Abschätzungen in (4).

(3) Berechne das Integral

$$\lim_{R \rightarrow \infty} \int_{\gamma_R * \delta_R} e^{iz} \frac{p(z)}{q(z)} dz$$

mit dem Residuensatz.

(4) Zeige, dass der Integralwert des Weges δ_R aus (2) für $R \rightarrow \infty$ gegen 0 konvergiert. Der Wert des gesuchten Integrals stimmt somit mit dem Real- bzw. Imaginärteil des Ergebnisses aus (3) überein.

Aufgabe (Herbst 2013, T3A3)

Sei $a > 0$ und sei $f: \mathbb{R} \rightarrow \mathbb{R}$, $x \mapsto \frac{\cos x}{a^2 + x^2}$.

a Zeigen Sie: $\int_{-\infty}^{\infty} |f(x)| dx < \infty$.

b Beweisen Sie mit Hilfe des Residuensatzes:

$$\int_{-\infty}^{\infty} \frac{\cos x}{a^2 + x^2} dx = \frac{\pi}{a} e^{-a}.$$

Lösungsvorschlag zur Aufgabe (Herbst 2013, T3A3)

a Wir geben eine integrierbare Majorante an. Betrachte dazu die Abschätzung

$$\int_{-\infty}^{\infty} \left| \frac{\cos x}{a^2 + x^2} \right| dx \leq \int_{-\infty}^{\infty} \frac{1}{a^2 + x^2} dx.$$

Das Integral auf der rechten Seite existiert, da die Differenz zwischen Zähler- und Nennergrad 2 beträgt und der Nenner keine reellen Nullstellen hat.

b Zunächst gilt für den Weg $\gamma_R: [-R, R] \rightarrow \mathbb{C}$, $t \mapsto t$

$$\int_{-\infty}^{\infty} \frac{\cos x}{a^2 + x^2} dx = \operatorname{Re} \int_{-\infty}^{\infty} \frac{e^{it}}{a^2 + t^2} dt = \lim_{R \rightarrow \infty} \operatorname{Re} \int_{\gamma_R} \frac{e^{iz}}{z^2 + a^2} dz.$$

Für die Nullstellen des Nenners gilt

$$z^2 + a^2 = 0 \Leftrightarrow (z - ia)(z + ia) = 0 \Leftrightarrow z = \pm ia.$$

Betrachten wir also im Folgenden die holomorphe Funktion

$$f: \mathbb{C} \setminus \{\pm ia\} \rightarrow \mathbb{C}, \quad z \mapsto \frac{e^{iz}}{z^2 + a^2}$$

sowie den Weg $\delta: [0, \pi] \rightarrow \mathbb{C}$, $t \mapsto Re^{it}$. Die einzige von $\gamma_R * \delta$ umlaufene Polstelle ist $+ia$. Das zugehörige Residuum berechnet sich zu

$$\text{Res}(f; ia) = \frac{e^{i(ia)}}{2(ia)} = \frac{e^{-a}}{2ia}.$$

Mit dem Residuensatz folgt nun

$$\int_{\gamma_R * \delta} \frac{e^{iz}}{z^2 + a^2} dz = 2\pi i \frac{e^{-a}}{2ia} = \frac{\pi}{a} e^{-a}.$$

Wir schätzen nun das Integral über δ ab. Hier ergibt sich für $R > a$

$$\begin{aligned} \left| \int_{\delta} \frac{e^{iz}}{z^2 + a^2} dz \right| &\leq \int_{\delta} \left| \frac{e^{iz}}{z^2 + a^2} \right| dz = \int_0^\pi \frac{|\exp(iRe^{it})|}{|R^2 e^{2it} + a^2|} |iRe^{it}| dt \\ &\stackrel{(\nabla)}{\leq} \int_0^\pi \frac{R}{|R^2 - a^2|} dt = \frac{\pi R}{R^2 - a^2}. \end{aligned}$$

Dabei haben wir für die vorletzte Abschätzung die für $t \in [0, \pi]$ gültige Gleichung

$$\begin{aligned} |\exp(iRe^{it})| &= |\exp(iR(\cos t + i \sin t))| = |\exp(iR \cos t) \exp(-R \sin t)| = \\ &= |\exp(-R \sin t)| \leq 1 \end{aligned}$$

verwendet. Damit ergibt sich aber

$$\lim_{R \rightarrow \infty} \left| \int_{\delta_R} f(z) dz \right| \leq \lim_{R \rightarrow \infty} \frac{\pi R}{R^2 - a^2} = 0 \Rightarrow \lim_{R \rightarrow \infty} \int_{\delta_R} f(z) dz = 0$$

und somit

$$\begin{aligned} \lim_{R \rightarrow \infty} \int_{-R}^R \frac{\cos t}{t^2 + a^2} dt &= \operatorname{Re} \lim_{R \rightarrow \infty} \int_{\gamma_R} \frac{e^{iz}}{z^2 + a^2} dz = \operatorname{Re} \lim_{R \rightarrow \infty} \int_{\gamma_R * \delta_R} \frac{e^{iz}}{z^2 + a^2} dz = \\ &= \operatorname{Re} \frac{\pi}{a} e^{-a} = \frac{\pi}{a} e^{-a} \end{aligned}$$

Aufgabe (Herbst 2013, T2A2)

Benutzen Sie den Residuensatz, um das uneigentliche reelle Integral

$$\int_0^\infty \frac{x \sin x}{x^2 + c^2} dx$$

für $c \in \mathbb{R}, c \neq 0$, zu berechnen. Geben Sie insbesondere Integrationspfade explizit an und weisen Sie nach, dass die Werte der entsprechenden Kurvenintegrale gegen das gesuchte Integral konvergieren.

Lösungsvorschlag zur Aufgabe (Herbst 2013, T2A2)

Der Integrand ist achsensymmetrisch zur y -Achse. Es gilt

$$\int_0^\infty \frac{x \sin x}{x^2 + c^2} dx = \frac{1}{2} \int_{-\infty}^\infty \frac{x \sin x}{x^2 + c^2} dx = \frac{1}{2} \operatorname{Im} \int_{-\infty}^\infty \frac{xe^{ix}}{x^2 + c^2} dx = \frac{1}{2} \lim_{r \rightarrow \infty} \operatorname{Im} \int_{\gamma_r} \frac{ze^{iz}}{z^2 + c^2} dz$$

für den Weg $\gamma_r : [-r, r] \rightarrow \mathbb{C}$, $t \mapsto t$. Die Nullstellen des Nenners im Komplexen sind gegeben durch $\pm ic$, sodass wir im Folgenden die Funktion

$$f: \mathbb{C} \setminus \{\pm ic\} \rightarrow \mathbb{C}, \quad z \mapsto \frac{ze^{iz}}{z^2 + c^2}$$

betrachten. Als Integrationspfad wählen wir das geschlossene Rechteck mit den Ecken $r, r+is, -r+is, -r$, wobei $s \in \mathbb{R}^+$ so gewählt sei, dass $s > c$ gilt. Bezeichnen wir den Weg mit γ , so ist $n(\gamma, ic) = 1$ und $n(\gamma, -ic) = 0$. Wir berechnen also nur das benötigte Residuum

$$\operatorname{Res}(f; ic) = \frac{ice^{i^2 c}}{2ic} = \frac{e^{-c}}{2}.$$

Damit ist schon mal

$$\int_{\gamma} f(z) dz = 2\pi i \frac{e^{-c}}{2} = \frac{\pi i}{e^c}.$$

Kommen wir zur Abschätzung der Integrale.

Vertikale Wege: $\gamma_1: [0, s] \rightarrow \mathbb{C}, t \mapsto r + it$.

Hier gilt

$$\begin{aligned} |f(r+it)| &= \frac{|r+it||e^{i(r+it)}|}{|(r+it)^2+c^2|} = \frac{|r+it||e^{-t+ir}|}{|(r+it)+ic||(r+it)-ic|} \\ &\stackrel{(\Delta)}{\leq} \frac{(|r|+|it|)|e^{-t}||e^{ir}|}{|r+i(t+c)||r+i(t-c)|} \leq \frac{r+s}{r^2}. \end{aligned}$$

Dabei wurde im Nenner verwendet, dass

$$|r+i(t \pm c)| = \sqrt{r^2 + (t \pm c)^2} \geq \sqrt{r^2} = r.$$

Die gleiche Abschätzung ergibt sich für $\gamma_3: [0, s] \rightarrow \mathbb{C}, t \mapsto -r + i(s-t)$.

Für die Integrale $\int_{\gamma_1} f(z) dz$ und $\int_{\gamma_3} f(z) dz$ ist somit $\frac{s(r+s)}{r^2}$ eine Abschätzung nach oben.

Horizontaler Weg: $\gamma_2: [-r, r] \rightarrow \mathbb{C}, t \mapsto (-t) + is$.

Hier erhalten wir

$$|f(-t+is)| = \frac{|-t+is||e^{i(-t+is)}|}{|(-t+is)^2+c^2|} = \frac{|-t+is||e^{-s-it}|}{|(-t+is)+ic|(-t+is)-ic|} \stackrel{(\Delta)}{\leq} \frac{r+s}{r^2}.$$

Hierbei haben wir beim letzten Schritt verwendet, dass

$$|-s-it| \cdot |e^{-s-it}| = |-s-it| \cdot |e^{-s}| \cdot |e^{-it}| \stackrel{(\Delta)}{\leq} (|t|+|s|) \cdot 1 \cdot 1 \leq r+s.$$

Somit gilt insgesamt

$$\lim_{r \rightarrow \infty} \int_{\gamma_1 * \gamma_2 * \gamma_3} f(z) dz = 0.$$

Dies bedeutet

$$\int_0^\infty \frac{x \sin x}{x^2+c^2} dx = \frac{1}{2} \operatorname{Im} \int_{\gamma} \frac{ze^{iz}}{z^2+c^2} dz = \frac{\pi}{2e^c}.$$

Zuletzt betrachten wir noch eine Möglichkeit, reelle Integrale zu berechnen, die nicht entlang der gesamten reellen Achse verlaufen. Diese Möglichkeit hat den Vorteil, dass nur ein Residuum betrachtet werden muss.

Anleitung: Berechnung von reellen Integralen IV (Pizzastück)

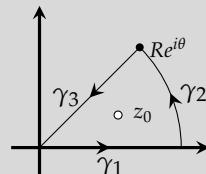
Zu berechnen ist ein Integral der Form

$$I = \int_0^\infty f(x)dx.$$

Anstatt eines Halbkreises lässt sich hier ein Kreissektor als Weg wählen.

- (1) Bestimme die Singularitäten der Funktion in Polarkoordinaten. Bezeichne mit $z_0 = r_0 e^{i\theta}$ die Singularität mit kleinstem Winkel θ .
- (2) Definiere den Weg $\Gamma_R = \gamma_1 * \gamma_2 * \gamma_3$ durch

$$\begin{aligned}\gamma_1 &: [0, R] \rightarrow \mathbb{C}, t \mapsto t, \\ \gamma_2 &: [0, 2\theta] \rightarrow \mathbb{C}, t \mapsto Re^{it}, \\ \gamma_3 &: [0, R] \rightarrow \mathbb{C}, t \mapsto (R - t)e^{2i\theta}.\end{aligned}$$



- (3) Das Integral über γ_3 lässt sich durch die Substitution $t \mapsto R - t$ in ein Vielfaches des Integrals über γ_1 überführen. Das Integral über γ_2 geht für $R \rightarrow \infty$ gegen 0. Es gilt somit für ein $c \in \mathbb{C}$

$$\int_{\Gamma_R} f(z)dz = \lim_{R \rightarrow \infty} \int_{\gamma_1} f(z)dz + \lim_{R \rightarrow \infty} c \int_{\gamma_3} f(z)dz = (1 + c)I.$$

- (4) Bestimme das Residuum $\text{Res}(f; z_0)$ und mit dem Residuensatz das Integral über Γ_R .
- (5) Löse die so entstandene Gleichung nach I auf. Dabei ist es oft sinnvoll, von den Beziehungen

$$\sin z = \frac{1}{2i} (e^{iz} - e^{-iz}) \quad \text{und} \quad \cos z = \frac{1}{2} (e^{iz} + e^{-iz}).$$

Aufgabe (Frühjahr 2011, T2A3)

Zeigen Sie, dass für alle $n \in \mathbb{N} = \{1, 2, \dots\}$ gilt:

$$\int_{-\infty}^{\infty} \frac{1}{1 + x^{2n}} dx = \frac{\pi}{n \sin(\frac{\pi}{2n})}.$$

Lösungsvorschlag zur Aufgabe (Frühjahr 2011, T2A3)

Sei $f(z) = \frac{1}{1+z^{2n}}$. Der Nenner des Integranden hat keine reelle Nullstelle und sein Grad ist um zwei größer als der des Zählers. Somit existiert das Integral. Aufgrund der Symmetrie des Integranden gilt

$$\int_{-\infty}^{\infty} \frac{1}{1+x^{2n}} dx = 2 \int_0^{\infty} \frac{1}{1+x^{2n}} dx,$$

wobei wir das Integral auf der rechten Seite fortan als I bezeichnen. Ist $e^{i\theta}$ eine Nullstelle des Nenners, so gilt

$$z^{2n} = -1 \Leftrightarrow e^{2in\theta} = e^{i\pi} \Leftrightarrow 2in\theta = i\pi + 2k\pi i \quad (k \in \mathbb{Z})$$

also haben die Nullstellen die Form $z = e^{\frac{\pi i + 2k\pi i}{2n}}$ für $k \in \{0, \dots, 2n-1\}$. Wir betrachten also die Singularität $z_0 = e^{\pi i/2n}$ und den Weg Γ_R definiert durch die Stücke

$$\begin{aligned} \gamma_1 &: [0, R] \rightarrow \mathbb{C}, t \mapsto t, \quad \gamma_2: [0, \frac{2\pi i}{2n}] \rightarrow \mathbb{C}, t \mapsto Re^{it}, \\ \gamma_3 &: [0, R] \rightarrow \mathbb{C}, t \mapsto (R-t)e^{2i\pi/2n}. \end{aligned}$$

Nun gilt mit der Substitution $t \mapsto R-t$

$$\begin{aligned} \int_{\gamma_3} \frac{1}{1+z^{2n}} dz &= \int_0^R \frac{1}{1+(R-t)^{2n}e^{2\pi i}} \cdot (-e^{2\pi i/2n}) dt = \\ &= -e^{2\pi i/2n} \int_0^{-R} \frac{-1}{1+t^{2n}} dt = -e^{2\pi i/2n} \int_0^R \frac{1}{1+t^{2n}} dt. \end{aligned}$$

Somit ist $\lim_{R \rightarrow \infty} \int_{\gamma_1} f(z) dz = -e^{2\pi i/2n} I$. Außerdem gilt für $R > 1$

$$\begin{aligned} \left| \int_{\gamma_2} \frac{1}{1+z^{2n}} dz \right| &\leq \int_0^{2\pi/2n} \left| \frac{1}{1+R^{2n}e^{2nit}} \right| dt \stackrel{(\nabla)}{\leq} \int_0^{2\pi/2n} \frac{1}{R^{2n}-1} dt \\ &= \frac{2\pi}{2n(R^{2n}-1)} \xrightarrow{R \rightarrow \infty} 0. \end{aligned}$$

Nun ist z_0 eine Polstelle erster Ordnung von f , dementsprechend ist

$$\text{Res}(f; z_0) = \frac{1}{2ne^{(\pi i/2n)(2n-1)}} = \frac{1}{-2ne^{-\pi i/2n}}.$$

Damit erhalten wir mit dem Residuensatz

$$\int_{\Gamma_R} \frac{1}{1+z^2} dz = 2\pi i n(\Gamma_R, z_0) \operatorname{Res}(f; z_0) = \frac{-\pi i}{ne^{-\pi i/2n}}.$$

Damit ist, da das Integral über γ_2 für $R \rightarrow \infty$ verschwindet,

$$(1 - e^{2\pi i/2n})I = \lim_{R \rightarrow \infty} \left(\int_{\gamma_1} f(z) dz + \int_{\gamma_3} f(z) dz \right) = \frac{-\pi i}{ne^{-\pi i/2n}}.$$

Unter Verwendung von $e^{iz} - e^{-iz} = 2i \sin z$ folgt daraus

$$I = \frac{-\pi i}{ne^{-\pi i/2n}(1 - e^{2\pi i/2n})} = \frac{-\pi i}{-n(e^{\pi i/2n} - e^{-\pi i/2n})} = \frac{\pi i}{2in \sin(\frac{\pi}{2n})}.$$

Insgesamt erhalten wir

$$\int_{-\infty}^{\infty} \frac{1}{1+x^{2n}} dx = 2 \frac{\pi i}{2in \sin(\frac{\pi}{2n})} = \frac{\pi}{n \sin(\frac{\pi}{2n})}.$$

6.6. Der Satz von Rouché

Das vorrangige Ziel dieses Abschnitts wird es sein, Nullstellen holomorpher Funktionen zu zählen. Dabei ist der Satz von Rouché hilfreich, der eine Folgerung aus dem Residuensatz ist. Qualitativ macht er folgende Aussage: Verändern wir eine holomorphe Funktion f um eine verhältnismäßig kleine Störfunktion g , d. h. $|g(z)| < |f(z)|$ für Punkte z einer bestimmten Menge, so kann sich zwar die Lage der Nullstellen verändern, nicht jedoch ihre Anzahl.

Satz 6.35 (Rouché). Sei $U \subseteq \mathbb{C}$ eine nicht-leere offene Teilmenge, $f, g: U \rightarrow \mathbb{C}$ seien holomorphe Funktionen. Weiter sei $\gamma: [a, b] \rightarrow U$ eine in U nullhomologe geschlossene Kurve, die jeden Punkt in ihrem Inneren genau einmal umläuft, und es gelte

$$|g(z)| < |f(z)| \quad \text{für alle } z \in \text{Spur } \gamma.$$

Dann haben f und $f + g$

- (1) auf Spur γ keine Nullstelle,
- (2) im Inneren der Kurve γ gleich viele Nullstellen (mit Vielfachheit gezählt).

Anleitung: Zählen von Nullstellen in Kreis- und Ringgebieten

Für reelle Zahlen $r, R > 0$ und $a \in \mathbb{C}$ definieren wir $B_r(a) = \{z \in \mathbb{C} \mid |z - a| < r\}$ und $K_{r,R}(a) = \{z \in \mathbb{C} \mid r < |z - a| < R\}$. Gegeben sei eine holomorphe Funktion $p: B_r(a) \rightarrow \mathbb{C}$.

- (1) Finde eine Zerlegung $p = f + g$ mit holomorphen Funktionen $f, g: B_r(a) \rightarrow \mathbb{C}$, sodass

$$|g(z)| < |f(z)| \quad \text{für alle } z \in \partial B_r(a)$$

gilt. Diese Zerlegung sollte so gewählt werden, dass sich die Nullstellen von f leicht bestimmen lassen.

- Dabei wählt man f meist so, dass sich $|f(z)|$ für $z \in \partial B_r(a)$ direkt angeben lässt, z. B. ein Monom $c_n z^n$ im Fall $a = 0$ für ein Polynom. Andernfalls kann man versuchen, mithilfe der umgekehrten Dreiecksungleichung eine untere Schranke für $|f(z)|$ anzugeben.
 - Anschließend kann man $|g(z)|$ mithilfe der Dreiecksungleichung nach oben abschätzen. Mit etwas Glück ist diese kleiner als die untere Schranke für $|f(z)|$, d. h. man bekommt $|g(z)| < |f(z)|$ für $z \in B_r(a)$.
- (2) Parametrisiere $\partial B_r(a)$ durch $\gamma: [0, 2\pi] \rightarrow \mathbb{C}, t \mapsto re^{it} + a$ und zeige, dass γ die Voraussetzungen des Satzes von Rouché erfüllt.
- (3) Nach dem Satz von Rouché hat p auf $B_r(a)$ genauso viele Nullstellen wie f .
- (4) Ist nach der Anzahl der Nullstellen in einem Ringgebiet $K_{r,R}(a)$ gefragt, bestimme die Anzahl der Nullstellen in $B_r(a)$ und $B_R(a)$ wie in (1)–(3). Nach Satz 6.35 (1) hat p auf $\partial B_r(a)$ keine Nullstellen, d. h. die Anzahl der Nullstellen in $K_{r,R}(a) = B_R(a) \setminus \overline{B_r(a)}$ ist die Differenz der bestimmten Anzahlen.
- (5) Bei Polynomen ist es außerdem hilfreich, im Hinterkopf zu behalten, dass die Anzahl der Nullstellen in \mathbb{C} gleich dem Grad ist (Fundamentalsatz der Algebra). Hat man also beispielsweise alle Nullstellen in $B_r(a)$ lokalisiert, so kann außerhalb keine mehr zu finden sein.

Aufgabe (Herbst 2003, T2A1)

Wie viele Nullstellen hat die Gleichung $z^4 - 5z + 1 = 0$

- a** im Kreisgebiet $\{z \mid |z| < 1\}$,
- b** im Ringgebiet $\{z \mid 1 < |z| < 2\}$,
- c** im Außengebiet $\{z \mid |z| > 2\}$?

Lösungsvorschlag zur Aufgabe (Herbst 2003, T2A1)

- a** Sei $B_1(0) = \{z \in \mathbb{C} \mid |z| < 1\}$. Wir definieren

$$\gamma_1: [0, 2\pi] \rightarrow \mathbb{C}, \quad t \mapsto e^{it}$$

und berechnen an dieser Stelle einmal ausführlich die Windungszahl an jedem Punkt. Da $\mathbb{C} \setminus \overline{B_1(0)}$ unbeschränkt ist, verschwindet die Windungszahl dort. Da die Windungszahl auf jeder Zusammenhangskomponente von $\mathbb{C} \setminus \text{Spur}(\gamma_1)$ konstant ist, genügt es, die Windungszahl von γ_1 um 0 zu berechnen, um sie für alle Punkte in $B_1(0)$ zu bestimmen. Diese ist

$$\begin{aligned} n(\gamma_1, 0) &= \frac{1}{2\pi i} \int_{\gamma_1} \frac{1}{z} dz = \frac{1}{2\pi i} \int_0^{2\pi} \frac{\gamma'_1(t)}{\gamma_1(t)} dt = \frac{1}{2\pi i} \int_0^{2\pi} \frac{ie^{it}}{e^{it}} dt = \\ &= \frac{1}{2\pi i} \int_0^{2\pi} idt = \frac{2\pi i}{2\pi i} = 1. \end{aligned}$$

Insgesamt ist damit

$$n(\gamma_1, a) = \frac{1}{2\pi i} \int_{\gamma_1} \frac{1}{z-a} dz = \begin{cases} 1 & \text{für } a \in B_1(0), \\ 0 & \text{für } a \in \mathbb{C} \setminus \overline{B_1(0)} \end{cases}$$

d. h. γ_1 ist nullhomolog in der offenen Menge \mathbb{C} und umläuft jeden Punkt in seinem Inneren genau einmal, wobei das Innere gerade $B_1(0)$ ist. Seien nun weiter

$$f: \mathbb{C} \rightarrow \mathbb{C}, \quad z \mapsto -5z \quad \text{und} \quad g: \mathbb{C} \rightarrow \mathbb{C}, \quad z \mapsto z^4 + 1,$$

dann gilt $|f(z)| = 5|z| = 5$ für alle $z \in \partial B_1(0)$ und

$$|g(z)| = |z^4 + 1| \leq |z^4| + 1 = 1 + 1 = 2 \quad \text{für alle } z \in \partial B_1(0).$$

Insbesondere also $|g(z)| < |f(z)|$ für alle $z \in \partial B_1(0) = \text{Spur } \gamma_1$. Nach dem Satz von Rouché 6.35 (2) haben daher f und $f+g$ in $B_1(0)$ gleich viele Nullstellen. Da f nur die einfache Nullstelle 0 in $B_1(0)$ hat, hat also $f(z) + g(z) = z^4 - 5z + 1$ ebenfalls nur eine Nullstelle in $B_1(0)$.

- b** Nach Satz 6.35 (1) hat $f+g$ keine Nullstelle auf $\partial B_1(0)$, also können wir die Anzahl der Nullstellen von $f+g$ auf $B_2(0) = \{z \in \mathbb{C} \mid |z| < 2\}$ bestimmen und die Anzahl der Nullstellen in $B_1(0)$ aus Teil **a** abziehen, um die Anzahl der Nullstellen im angegebenen Ringgebiet zu erhalten.

Definiere

$$\gamma_2: [0, 2\pi] \rightarrow \mathbb{C}, \quad t \mapsto 2e^{it},$$

dann ist γ_2 ebenfalls nullhomolog in \mathbb{C} und umläuft jeden Punkt in seinem Inneren genau einmal. Betrachte nun

$$h: \mathbb{C} \rightarrow \mathbb{C}, \quad z \mapsto z^4 \quad \text{und} \quad k: \mathbb{C} \rightarrow \mathbb{C}, \quad z \mapsto -5z + 1,$$

dann gilt $|h(z)| = |z^4| = 2^4 = 16$ für alle $z \in \text{Spur } \gamma_2$ und

$$|k(z)| = |-5z + 1| \leq 5|z| + 1 = 10 + 1 = 11 \quad \text{für alle } z \in \text{Spur } \gamma_2,$$

insbesondere also $|k(z)| < |h(z)|$ für alle $z \in \text{Spur } \gamma_2 = \partial B_2(0)$. Da h eine vierfache Nullstelle in 0 hat, hat nach dem Satz von Rouché auch $(h+k)(z) = z^4 - 5z + 1$ vier Nullstellen in $B_2(0)$.

Die Anzahl der Nullstellen im Ringgebiet $\{z \in \mathbb{C} \mid 1 < |z| < 2\}$ beträgt nach obiger Argumentation dann $4 - 1 = 3$.

- c** Da $z^4 - 5z + 1$ ein Polynom von Grad 4 ist, hat es genau vier Nullstellen in \mathbb{C} . In **b** haben wir gesehen, dass diese bereits in $B_2(0)$ liegen, also gibt es im Außengebiet $\{z \in \mathbb{C} \mid |z| > 2\}$ keine weiteren Nullstellen.

Aufgabe (Herbst 2014, T2A3)

Es sei $h: \mathbb{C} \rightarrow \mathbb{C}$ holomorph mit $|h(z)| \leq 2$ für alle $|z| = 2$ und $f: \mathbb{C} \rightarrow \mathbb{C}$ sei definiert durch

$$f(z) = h(z)^3 + 4z^2 - z + 1 \quad \text{für alle } z \in \mathbb{C}.$$

- a** Bestimmen Sie die Zahl der Nullstellen (gezählt mit Vielfachheit) von f im Gebiet $\{z \in \mathbb{C} \mid |z| < 2\}$.
- b** Sei nun $h(z) = \frac{z}{2}$ für alle $z \in \mathbb{C}$. Bestimmen Sie die Zahl der Nullstellen von f in $\{z \in \mathbb{C} \mid 1 < |z| < 2\}$.

Lösungsvorschlag zur Aufgabe (Herbst 2014, T2A3)

- a** Sei $B_2(0) = \{z \in \mathbb{C} \mid |z| < 2\}$. Wir verwenden die umgekehrte Dreiecksungleichung:

$$|4z^2 - z| \geq \left| |4z^2| - |z| \right| = |4 \cdot 2^2 - 2| = 14 \quad \text{für alle } z \in \partial B_2(0)$$

Weiter ist $|h(z)^3 + 1| \leq |h(z)|^3 + 1 \leq 2^3 + 1 = 9$ für alle $z \in \partial B_2(0)$. Es gilt also $|h(z)^3 + 1| < |4z^2 - z|$ für alle $z \in \partial B_2(0)$. Nach dem Satz von Rouché hat f daher in $B_2(0)$ genauso viele Nullstellen wie das Polynom $4z^2 - z = 4z(z - \frac{1}{4})$ dort hat, nämlich 2.

b Für $z \in \partial B_2(0)$ gilt $|\frac{z}{2}| = \frac{2}{2} = 1 \leq 2$, also besitzt f in $B_2(0)$ nach Teil **a** zwei Nullstellen. Wir bestimmen nun die Zahl der Nullstellen von f in $\overline{B_1(0)}$, dann ist die gesuchte Anzahl die Differenz.

Für $z \in \partial B_1(0)$ gilt $|4z^2| = 4$, außerdem

$$\left| \frac{1}{8}z^3 - z + 1 \right| \leq \left| \frac{1}{8}z^3 \right| + |z| + 1 = \frac{1}{8} + 1 + 1 < 4,$$

d. h. $\left| \frac{1}{8}z^3 - z + 1 \right| < |4z^2|$ für alle $z \in \partial B_1(0)$. Nach dem Satz von Rouché hat f daher in $B_1(0)$ genauso viele Nullstellen wie das Polynom $4z^2$. Das sind zwei. Da f in $B_2(0)$ ebenfalls nur zwei Nullstellen besitzt, kann es keine Nullstelle im Ringgebiet $\{z \in \mathbb{C} \mid 1 < |z| < 2\}$ geben.

Aufgabe (Frühjahr 2012, T2A1)

Wie viele Lösungen (mit Vielfachheit gezählt) hat die Gleichung

$$z^5 - z^4 + z^3 - z^2 + 6z = 1$$

in $\{z \in \mathbb{C} \mid |z| < 1\}$ bzw. in $\{z \in \mathbb{C} \mid 1 < |z| < 3\}$ bzw. in $\{z \in \mathbb{C} \mid |z| > 3\}$?

Lösungsvorschlag zur Aufgabe (Frühjahr 2012, T2A1)

Die Lösungen obiger Gleichung stimmen mit den Nullstellen des Polynoms $p(z) = z^5 - z^4 + z^3 - z^2 + 6z - 1$ überein.

Wir bestimmen zunächst die Anzahl der Nullstellen von p in $B_1(0) = \{z \in \mathbb{C} \mid |z| < 1\}$. Dazu bemerken wir, dass für alle $z \in \partial B_1(0)$ die Abschätzung

$$|z^5 - z^4 + z^3 - z^2 - 1| \leq |z^5| + |z^4| + |z^3| + |z^2| + 1 = 1 + 1 + 1 + 1 + 1 = 5$$

erfüllt ist. Wegen $|6z| = 6$ für alle $z \in \partial B_1(0)$ gilt also

$$|z^5 - z^4 + z^3 - z^2 - 1| < |6z| \quad \text{für alle } z \in \partial B_1(0).$$

Somit können wir den Satz von Rouché anwenden und erhalten, dass das Polynom p in $B_1(0)$ genauso viele Nullstellen hat wie $6z$, d. h. genau eine.

Im Falle $z \in \partial B_3(0)$ haben wir die Abschätzung

$$\begin{aligned} |-z^4 + z^3 - z^2 + 6z - 1| &\leq |z^4| + |z^3| + |z^2| + |6z| + 1 = \\ &= 3^4 + 3^3 + 3^2 + 6 \cdot 3 + 1 = 136. \end{aligned}$$

Wegen $|z^5| = 3^5 = 243$ für alle $z \in \partial B_3(0)$ bedeutet dies

$$|-z^4 + z^3 - z^2 + 6z - 1| < |z^5| \quad \text{für alle } z \in \partial B_3(0),$$

d. h. p hat in $B_3(0)$ genauso viele Nullstellen wie z^5 dort hat, nämlich fünf. Da p nach dem Satz von Rouché auf $\partial B_1(0)$ keine Nullstelle hat, ist die Zahl der Nullstellen in $\{z \in \mathbb{C} \mid 1 < |z| < 3\} = B_3(0) \setminus \overline{B_1(0)}$ damit $5 - 1 = 4$.

Als Polynom von Grad 5 hat p genau fünf Nullstellen in \mathbb{C} , da diese bereits alle in $B_3(0)$ liegen, kann sich keine mehr im Außengebiet $\{z \in \mathbb{C} \mid |z| > 3\}$ befinden.

Aufgabe (Frühjahr 2015, T1A1)

In dieser Aufgabe bezeichne $B_r(a) := \{z \in \mathbb{C} \mid |z - a| < r\}$ den offenen Ball von Radius $r > 0$ um $a \in \mathbb{C}$. Ferner sei $f: \mathbb{C} \rightarrow \mathbb{C}$ durch $f(z) := 6z^6 - 2z^2 + 1$ gegeben.

a Formulieren Sie den Satz von Rouché für ganze Funktionen.

b Zeigen Sie, dass $B_4(1) \subseteq f(B_1(0)) \subseteq B_8(1)$ gilt.

Hinweis Für den Nachweis der ersten Inklusion könnte der in **a** formulierte Satz hilfreich sein.

c Entscheiden Sie mit Beweis, ob $f(B_1(0)) \cap \mathbb{R} = f(B_1(0) \cap \mathbb{R})$ gilt.

Lösungsvorschlag zur Aufgabe (Frühjahr 2015, T1A1)

a Siehe Satz 6.35. Um eine Formulierung für ganze Funktionen zu erhalten, setze $U = \mathbb{C}$. Außerdem kann dann dann die Bedingung weggelassen werden, dass der Weg nullhomolog ist.

b Wir zeigen zunächst die zweite Inklusion. Sei $z \in B_1(0)$, dann gilt

$$|f(z) - 1| = |6z^6 - 2z^2| \leq 6|z|^6 + 2|z|^2 < 6 + 2 = 8,$$

d. h. $f(z) \in B_8(1)$. Sei nun $w \in B_4(1)$. Um die erste Inklusion zu zeigen, müssen wir $z_0 \in B_1(0)$ finden, sodass $f(z_0) = w$ gilt. Dazu definieren wir

$$g: \mathbb{C} \rightarrow \mathbb{C}, \quad z \mapsto 6z^6 \quad \text{und} \quad h: \mathbb{C} \rightarrow \mathbb{C}, \quad z \mapsto -2z^2 + 1 - w$$

Wegen $w \in B_4(1)$ gilt für alle $z \in \partial B_1(0)$, dass

$$|h(z)| = |-2z^2 + 1 - w| \leq 2|z|^2 + |1 - w| = 2 + |1 - w| < 2 + 4 = 6.$$

Außerdem ist $|g(z)| = |6z^6| = 6$ für alle $z \in \partial B_1(0)$. Also $|h(z)| < |g(z)|$ für alle $z \in \partial B_1(0)$. Da g mit 0 eine sechsfache Nullstelle in $B_1(0)$ hat, hat $g + h$ nach dem Satz von Rouché ebenfalls sechs Nullstellen in $B_1(0)$. Es gibt also $z_0 \in B_1(0)$, sodass

$$\begin{aligned}(g + h)(z_0) &= 0 \Leftrightarrow 6z_0^6 - 2z_0^2 + 1 - w = 0 \\ &\Leftrightarrow 6z_0^6 - 2z_0^2 + 1 = w \Leftrightarrow f(z_0) = w\end{aligned}$$

- c** Wir widerlegen die Aussage. Sei $x \in B_1(0) \cap \mathbb{R} =]-1, 1[$, dann ist $6x^6 + 1 \geq 0$, sodass

$$f(x) = 6x^6 - 2x^2 + 1 \geq -2x^2 \geq -2$$

Also kann $-\frac{5}{2}$ nicht in $f(B_1(0) \cap \mathbb{R})$ liegen. Wegen

$$-\frac{5}{2} \in B_4(1) \cap \mathbb{R} \stackrel{\text{b}}{\subseteq} f(B_1(0)) \cap \mathbb{R}$$

ist daher $f(B_1(0)) \cap \mathbb{R} \not\subseteq f(B_1(0) \cap \mathbb{R})$.

Anleitung: Imaginärteil von Nullstellen

Manchmal ist nicht nur die Anzahl der Nullstellen einer holomorphen Funktion f gefragt, sondern auch, wie viele davon reell sind bzw. positiven Imaginärteil haben.

- (1) Die Existenz einer reellen Nullstelle kann man häufig mit dem Zwischenwertsatz beantworten, indem man diesen auf die Einschränkung $f|_{\mathbb{R}}$ anwendet. Auch weitere Hilfsmittel aus der reellen Analysis wie die Betrachtung der Ableitung oder der Satz von Rolle können hilfreich sein.
- (2) Echt-komplexe Nullstellen treten bei Polynomen mit reellen Koeffizienten immer in komplex-konjugierten Paaren auf. Ist nämlich $w \in \mathbb{C} \setminus \mathbb{R}$ eine Nullstelle des Polynoms f , so ist

$$f(\bar{w}) = \overline{f(w)} = 0,$$

d. h. auch \bar{w} ist eine Nullstelle von f . Insbesondere ist die Zahl der Nullstellen mit positivem Imaginärteil gleich der der Nullstellen mit negativem Imaginärteil.

Aufgabe (Frühjahr 2013, T1A2)

Bestimmen Sie mit Hilfe des Satzes von Rouché die Anzahl der Nullstellen der Funktion $f(z) = e^z + 3z^5$ in der offenen Kreisscheibe $E = \{z \in \mathbb{C} \mid |z| < 1\}$. Zeigen Sie weiter, dass genau zwei dieser Nullstellen positiven Imaginärteil haben und eine Nullstelle in \mathbb{R} liegt.

Lösungsvorschlag zur Aufgabe (Frühjahr 2013, T1A2)

Sei

$$\gamma: [0, 2\pi] \rightarrow \mathbb{C}, \quad t \mapsto e^{it},$$

dann ist γ nullhomolog in \mathbb{C} und umläuft jeden Punkt in E genau einmal. Definiere weiter

$$g: \mathbb{C} \rightarrow \mathbb{C}, \quad z \mapsto 3z^5,$$

dann gilt für alle $z \in \text{Spur } \gamma$, dass $|g(z)| = 3|z|^5 = 3$. Außerdem ist

$$|\exp(z)| = |e^z| = |e^{i\operatorname{Im}(z)+\operatorname{Re}(z)}| = |e^{i\operatorname{Im}(z)}| \cdot |e^{\operatorname{Re}(z)}| = 1 \cdot |e^{\operatorname{Re}(z)}|$$

und für $z \in \partial B_1(0)$ folgt aus $|z| = 1$ insbesondere, dass $\operatorname{Re} z \leq 1$ und die Monotonie der reellen Exponentialfunktion liefert $e^{\operatorname{Re} z} \leq e < 3$. Zusammen also

$$|\exp(z)| < 3 = |g(z)| \quad \text{für alle } z \in \partial B_1(0).$$

Nach dem Satz von Rouché haben daher $f = \exp + g$ und g gleich viele Nullstellen in $B_1(0)$. Da g eine fünffache Nullstelle bei 0 hat, sind dies fünf.

Nehmen wir an, f besitzt eine doppelte Nullstelle $\omega \in \mathbb{C}$. Für eine solche Nullstelle müsste auch die erste Ableitung verschwinden, d.h.

$$\begin{aligned} f(\omega) = f'(\omega) = 0 &\Rightarrow f(\omega) - f'(\omega) = 0 \Leftrightarrow e^\omega + 3\omega^5 - e^\omega - 15\omega^4 = 0 \\ &\Leftrightarrow 3\omega^4(\omega - 5) = 0 \Leftrightarrow \omega \in \{0, 5\}. \end{aligned}$$

Einsetzen zeigt jedoch, dass weder 0 noch 5 eine Nullstelle von f ist. Folglich hat f nur einfache Nullstellen, sodass diese insbesondere verschieden sein müssen.

Betrachte die Einschränkung $f|_{\mathbb{R}} : \mathbb{R} \rightarrow \mathbb{R}$ auf die reelle Achse. Wegen

$$f|_{\mathbb{R}}(-1) = \frac{1}{e} - 3 < 1 - 3 = -2 < 0 \quad \text{und} \quad f|_{\mathbb{R}}(0) = 1 + 0 = 1 > 0$$

besitzt f nach dem Zwischenwertsatz mindestens eine reelle Nullstelle in $] -1, 0 [$. Da $f'|_{\mathbb{R}} = e^x + 15x^4$ für alle $x \in \mathbb{R}$ positiv ist, ist $f|_{\mathbb{R}}$ streng monoton steigend und kann daher nur eine reelle Nullstelle haben.

Sei nun $\omega \in \mathbb{C}$ eine Nullstelle von f . Für das komplexe konjugierte $\bar{\omega}$ gilt

$$\begin{aligned} e^{\bar{\omega}} &= e^{\operatorname{Re} \omega} \cdot e^{-i\operatorname{Im} \omega} = \\ &= e^{\operatorname{Re} \omega} \cdot (\cos(-\operatorname{Im} \omega) + i \sin(-\operatorname{Im} \omega)) = \\ &= e^{\operatorname{Re} \omega} \cdot (\cos(\operatorname{Im} \omega) - i \sin(\operatorname{Im} \omega)) = e^{\operatorname{Re} \omega} \cdot \overline{e^{i \operatorname{Im} \omega}} = \\ &= \overline{e^{\operatorname{Re} \omega} \cdot e^{i \operatorname{Im} \omega}} = \\ &= \overline{e^\omega}. \end{aligned}$$

Also ist auch

$$0 = \bar{0} = \overline{f(\omega)} = \overline{e^\omega + 3\omega^5} = e^{\bar{\omega}} + 3\bar{\omega}^5 = f(\bar{\omega}).$$

Das bedeutet, dass für jede Nullstelle von f auch das jeweilige komplexe Konjugierte eine Nullstelle ist. Als Folge müssen die vier echt-komplexen Nullstellen in ein Paar Nullstellen mit positivem Imaginärteil und ein Paar mit negativem Imaginärteil zerfallen.

Aufgabe (Herbst 2012, T1A4)

Bestimmen Sie die Anzahl der Nullstellen des Polynoms $p(z) = 2z^5 - 6z^2 + z + 1$ im Ringgebiet $1 \leq |z| \leq 2$. Sind darunter auch reelle Nullstellen?

Lösungsvorschlag zur Aufgabe (Herbst 2012, T1A4)

Wir bestimmen zunächst die Anzahl der Nullstellen in $B_2(0) = \{z \in \mathbb{C} \mid |z| < 2\}$. Für alle $z \in \partial B_2(0)$ gilt

$$|-6z^2 + z + 1| \leq 6|z|^2 + |z| + 1 = 24 + 2 + 1 = 27$$

und $|2z^5| = 2 \cdot 2^5 = 64$, also ist $|-6z^2 + z + 1| < |2z^5|$ für alle $z \in \partial B_2(0)$ erfüllt und nach dem Satz von Rouché stimmt die Zahl der Nullstellen von p in $B_2(0)$ mit der Zahl der Nullstellen von $2z^5$ in $B_2(0)$ überein. Dies sind fünf.

Für $z \in \partial B_1(0)$ gilt die Abschätzung

$$|2z^5 + z + 1| \leq |2z^5| + |z| + 1 = 2 + 1 + 1 = 4$$

sowie $|-6z^2| = 6$, d.h. $|2z^5 + z + 1| < |-6z^2|$. Nach dem Satz von Rouché hat daher p in $B_1(0)$ genauso viele Nullstellen wie $-6z^2$, nämlich zwei. Außerdem hat p nach dem Satz von Rouché auf dem Rand $\partial B_1(0)$ keine Nullstellen, sodass p auf $\overline{B_1(0)}$ zwei Nullstellen hat.

Die Zahl der Nullstellen in $\{z \in \mathbb{C} \mid 1 < |z| < 2\} = B_2(0) \setminus \overline{B_1(0)}$ ist deshalb $5 - 2 = 3$. Da auch auf dem Rand von $B_2(0)$ keine Nullstellen liegen können, entspricht das auch der Anzahl der Nullstellen im abgeschlossenen Ringgebiet $\{z \in \mathbb{C} \mid 1 < |z| \leq 2\}$.

Sei $w \in \mathbb{C} \setminus \mathbb{R}$ eine komplexe Nullstelle von p und \bar{w} ihr komplex Konjugiertes. Es ist dann $w \neq \bar{w}$ und es gilt

$$p(\bar{w}) = 2\bar{w}^5 - 6\bar{w}^2 + \bar{w} + 1 = \overline{2w^5 - 6w^2 + w + 1} = \overline{p(w)} = \bar{0} = 0,$$

sodass auch \bar{w} eine Nullstelle von p sein muss. Dies zeigt, dass die echtkomplexen Nullstellen von p in komplex konjugierten Paaren auftreten. Da p jedoch eine ungerade Anzahl von Nullstellen in $\{z \in \mathbb{C} \mid 1 < |z| \leq 2\}$ besitzt, muss darunter mindestens eine reelle Nullstelle sein.

Aufgabe (Frühjahr 2015, T3A3)

Es seien f und g holomorph auf $K_2(0)$ und $f(\zeta) \neq 0$ für alle $\zeta \in \partial\mathbb{D}$ und für jedes $\zeta \in \partial\mathbb{D}$ sei $g(\zeta)/f(\zeta)$ reell und positiv. Zeigen Sie, dass f und g in \mathbb{D} dieselbe Anzahl von Nullstellen (mit Vielfachheiten gezählt) besitzen.⁵

Lösungsvorschlag zur Aufgabe (Frühjahr 2015, T3A3)

Da nach Voraussetzung $f(z) \neq 0$ und $\frac{g(z)}{f(z)}$ für alle $z \in \partial K_2(0)$ reell und positiv ist, können wir die Funktion

$$h: \partial K_2(0) \rightarrow \mathbb{R}_+, \quad a \mapsto \frac{g(a)}{f(a)}$$

definieren. Diese ist als Quotient stetiger Funktionen mit nullstellenfreiem Nenner stetig und nimmt deshalb auf der kompakten Menge $\partial K_2(0)$ ein Minimum an. Es gibt also ein $c_1 \in \mathbb{R}$, sodass $\frac{g(z)}{f(z)} \geq c_1$ für alle $z \in \partial K_2(0)$ erfüllt ist. Nun ist weiter $|\frac{g(z)}{f(z)}| = \frac{|g(z)|}{|f(z)|}$ für alle $z \in \partial K_2(0)$, da dort der Bruch $\frac{g(z)}{f(z)}$ reell und positiv ist. Deshalb gilt für eben diese $z \in \partial K_2(0)$ die Abschätzung

$$\begin{aligned} |f(z) + g(z)| &= \left| f(z) \left(1 + \frac{g(z)}{f(z)} \right) \right| = |f(z)| \cdot \left(1 + \frac{|g(z)|}{|f(z)|} \right) \geq \\ &\geq |f(z)|(1 + c_1) > |f(z)|. \end{aligned}$$

⁵ Die Bezeichnungen $K_r(0) = \{z \in \mathbb{C} \mid |z| < r\}$ und $\mathbb{D} = K_1(0)$ waren für die gesamte Aufgabengruppe definiert.

Nach dem Satz von Rouché haben daher $f + g$ und $g = (f + g) + (-f)$ gleich viele Nullstellen in \mathbb{D} . Zu zeigen bleibt nun, dass auch f genauso viele Nullstellen wie $f + g$ in \mathbb{D} hat.

Sei wiederum $z \in \partial K_2(0)$ und betrachten wir zunächst den Fall, dass $g(z) \neq 0$ ist. Die Funktion h nimmt auf der kompakten Menge $\partial K_2(0)$ auch ein Maximum an, d.h. es gibt ein $c_2 \in \mathbb{R}_+$, sodass

$$\frac{g(z)}{f(z)} \leq c_2 \quad \Leftrightarrow \quad \frac{f(z)}{g(z)} \geq \frac{1}{c_2}$$

für alle $z \in \partial K_2(0)$ erfüllt ist. Also folgt

$$|f(z) + g(z)| = |g(z)| \cdot \left| \frac{f(z)}{g(z)} + 1 \right| \geq |g(z)| \cdot \left(1 + \frac{1}{c_2} \right) > |g(z)|.$$

Falls $g(z) = 0$ ist, so lautet die Ungleichung $|f(z)| > 0$ und ist ebenfalls erfüllt, da f nullstellenfrei auf $\partial K_2(0)$ ist. Also gilt die Ungleichung $|f(z) + g(z)| > |g(z)|$ sogar für alle $z \in \partial K_2(0)$ und nach dem Satz von Rouché haben $f + g$ und $(f + g) + (-g) = f$ gleiche viele Nullstellen in \mathbb{D} .

Aufgabe (Herbst 2011, T1A3)

- a** Es sei $P(z) := \sum_{k=0}^n a_k z^k$ mit $a_n \neq 0$ ein Polynom vom Grad $n \geq 1$ und $m \in \{1, \dots, n\}$. Für ein $r > 0$ gelte

$$\sum_{k=0}^n |a_k| \cdot r^k < 2|a_m| \cdot r^m.$$

Zeigen Sie, dass P genau m Nullstellen im offenen Ball $B_r(0)$ und genau $n - m$ Nullstellen in $\mathbb{C} \setminus \overline{B_r(0)}$ hat (jeweils mit Vielfachheiten gezählt). Belegen Sie durch ein Beispiel, dass dies im Allgemeinen falsch ist, wenn man nur $\sum_{k=0}^n |a_k| \cdot r^k \leq 2|a_m| \cdot r^m$ voraussetzt.

- b** Zeigen Sie, dass

$$\int_{|z|=2} \frac{1}{z^5 + 12z^2 + i} dz = \int_{|z|=1} \frac{1}{z^5 + 12z^2 + i} dz$$

gilt.

Hinweis Wenden Sie **a** an.

Lösungsvorschlag zur Aufgabe (Herbst 2011, T1A3)

- a** Die Voraussetzungen führen dazu, dass für alle $z \in \partial B_r(0)$ die Abschätzung

$$\begin{aligned} |P(z) - a_m z^m| &= \left| \sum_{\substack{k=0 \\ k \neq m}}^n a_k z^k \right| \stackrel{(\Delta)}{\leq} \sum_{\substack{k=0 \\ k \neq m}}^n |a_k| |z|^k = \sum_{k=0}^n |a_k| r^k - |a_m| r^m < \\ &< 2|a_m|r^m - |a_m|r^m = |a_m|r^m \end{aligned}$$

gilt. Also können wir den Satz von Rouché anwenden und erhalten, dass $P(z)$ genauso viele Nullstellen in $B_r(0)$ hat wie $a_m z^m$. Das sind m viele. Da $P(z)$ als Polynom von Grad n genau n Nullstellen in \mathbb{C} besitzt und nach Satz 6.35 (1) keine davon auf $\partial B_r(0)$ liegt, müssen $n - m$ davon in $\mathbb{C} \setminus \overline{B_r(0)}$ liegen.

Als Gegenbeispiel für den zweiten Teil der Aufgabe betrachten wir das Polynom $P(z) = z^2 + z$. Für $r = 1$ gilt dann

$$1^2 + 1 = 2 \leq 2 \cdot 1^2,$$

d. h. falls die Behauptung wahr wäre, müsste P zwei Nullstellen in $B_1(0)$ haben. Allerdings liegt nur eine Nullstelle von $P(z) = z(z+1)$ in $B_1(0)$.

- b** Wir verwenden Teil **a**. Eine geeignete Abschätzung der obigen Form erhält man für $m = 2$ und $r = 1$ bzw. $r = 2$. Es ist nämlich

$$1^5 + 12 \cdot 1^2 + |i| = 14 < 24 = 2 \cdot 12 \cdot 1^2 \quad \text{und}$$

$$2^5 + 12 \cdot 2^2 + |i| = 81 < 96 = 2 \cdot 12 \cdot 2^2,$$

also hat das Polynom $z^5 + 12z^2 + i$ in $B_1(0)$ und $B_2(0)$ jeweils zwei Nullstellen (mit Vielfachheit gezählt). Seien $a_1, a_2 \in B_1(0)$ diese (möglicherweise gleichen) Nullstellen, dann entsprechen diese den Polstellen der Funktion

$$f : B_2(0) \setminus \{a_1, a_2\} \rightarrow \mathbb{C}, \quad z \mapsto \frac{1}{z^5 + 12z^2 + i}.$$

Falls $a_1 \neq a_2$, so ist nach dem Residuensatz

$$\int_{|z|=2} f dz = 2\pi i \cdot \operatorname{Res}(f; a_1) + 2\pi i \cdot \operatorname{Res}(f; a_2) = \int_{|z|=1} f dz$$

und falls $a_1 = a_2$, so ist

$$\int_{|z|=2} f dz = 2\pi i \cdot \text{Res}(f; a_1) = \int_{|z|=1} f dz.$$

In jedem Fall also $\int_{|z|=2} f dz = \int_{|z|=1} f dz$.

6.7. Biholomorphe Abbildungen

Abbildungen, die holomorph sind und eine holomorphe Umkehrfunktion haben, werden als *biholomorph* (gelegentlich auch als *konform*) bezeichnet. Während in der reellen Analysis die Umkehrfunktion einer differenzierbaren Funktion nicht unbedingt selbst differenzierbar sein muss, gilt im Komplexen:

Proposition 6.36. Seien $U, V \subseteq \mathbb{C}$ und $f: U \rightarrow V$ eine Abbildung. Ist f bijektiv und holomorph, so ist auch die Umkehrfunktion f^{-1} eine holomorphe Funktion. Insbesondere ist f bijektiv.

Vielfältige Fragen über die Existenzbiholomorpher Abbildungen lassen sich mit dem folgenden Satz beantworten. Dabei bezeichnet $\mathbb{E} = \{z \in \mathbb{C} \mid |z| < 1\}$ – wie im gesamten Abschnitt – die Einheitskreisscheibe.

Satz 6.37 (Riemann'scher Abbildungssatz). Sei $G \subsetneq \mathbb{C}$ ein einfach zusammenhängendes Gebiet. Dann existiert eine biholomorphe Abbildung $G \rightarrow \mathbb{E}$.

Der Begriff des einfachen Zusammenhangs spielt in der Funktionentheorie allgemein eine zentrale Rolle, wir verweisen hierzu auf Proposition 6.29. Da das Bild einer einfach zusammenhängenden Menge unter einer biholomorphen Abbildung wieder einfach zusammenhängend ist, gilt auch die Umkehrung von Satz 6.37, d. h. es existiert genau dann eine biholomorphe Abbildung $G \rightarrow \mathbb{E}$, wenn $G \subsetneq \mathbb{C}$ einfach zusammenhängend ist.

Aufgabe (Frühjahr 2014, T2A5)

Entscheiden Sie, bei welchem der drei Paare von offenen Teilmengen von \mathbb{C} es eine biholomorphe Abbildung zwischen den beiden Mengen gibt.

- a** $\mathbb{C} \setminus \{2\}$ und $\mathbb{E} := \{z \in \mathbb{C} \mid |z| < 1\}$,
- b** $\mathbb{C} \setminus]-\infty; 0]$ und $\mathbb{H} := \{z \in \mathbb{C} \mid \operatorname{Re}(z) > 0\}$,
- c** $S := \{z \in \mathbb{C} \mid -1 < \operatorname{Im}(z) < 1\}$ und \mathbb{C} .

Lösungsvorschlag zur Aufgabe (Frühjahr 2014, T2A5)

- a** Eine solche Abbildung existiert *nicht*. Als offene Kreisscheibe um 0 mit Radius 1 ist \mathbb{E} ein einfach zusammenhängendes Gebiet. Ist nun $f: \mathbb{C} \setminus \{2\} \rightarrow \mathbb{E}$ eine biholomorphe Abbildung, so müsste auch $f^{-1}(\mathbb{E}) = \mathbb{C} \setminus \{2\}$ einfach zusammenhängend sein. Dies ist nicht der Fall, denn es gilt $\mathbb{C} \setminus (\mathbb{C} \setminus \{2\}) = \{2\}$ und somit hat $\mathbb{C} \setminus (\mathbb{C} \setminus \{2\})$ eine beschränkte Zusammenhangskomponente.

Alternative: Mit Verwendung des Riemannschen Hebbarkeitssatzes und des Satzes von Liouville lässt sich zeigen, dass f konstant ist, vgl. hierzu Teil **b** der nächsten Aufgabe (H06T3A1).

- b** Eine solche Abbildung *existiert*. Es gilt $\mathbb{C} \setminus (\mathbb{C} \setminus]-\infty; 0]) =]-\infty; 0]$, sodass die linke Menge genau eine unbeschränkte Zusammenhangskomponente hat und damit einfach zusammenhängend ist. Gleiches gilt für die Menge \mathbb{H} , wie man analog zeigt. Damit gibt es laut dem Riemannschen Abbildungssatz 6.37 biholomorphe Abbildungen $f: \mathbb{C} \setminus]-\infty; 0] \rightarrow \mathbb{E}$ und $g: \mathbb{H} \rightarrow \mathbb{E}$. Die Abbildung $g^{-1} \circ f: \mathbb{C} \setminus]-\infty; 0] \rightarrow \mathbb{H}$ ist dann wiederum biholomorph als Verkettung biholomorpher Abbildungen.
- c** Eine solche Abbildung existiert *nicht*. Angenommen, es gäbe eine biholomorphe Abbildung $f: \mathbb{S} \rightarrow \mathbb{C}$. Dann wäre die Abbildung $f^{-1}: \mathbb{C} \rightarrow \mathbb{S}$ eine ganze Abbildung mit $f^{-1}(\mathbb{C}) = \mathbb{S}$. Die Punkte $2i$ und $3i$ liegen wegen $\operatorname{Im} 2i, \operatorname{Im} 3i > 1$ nicht in \mathbb{S} , sodass f laut dem kleinen Satz von Picard 6.21 konstant ist – Widerspruch zur Bijektivität.

Alternative: Statt Verwendung des Satzes von Picard lässt sich der Satz von Liouville auf e^{if} anwenden, um zu zeigen dass f konstant ist.

Aufgabe (Herbst 2006, T3A1)

Sei $\mathbb{D} = \{z \in \mathbb{C} \mid |z| < 1\}$. Sind die folgenden Aussagen wahr oder falsch? Geben Sie jeweils eine kurze Begründung an!

- a** Es gibt eine biholomorphe Abbildung $f: \mathbb{C} \rightarrow \mathbb{D}$.
- b** Es gibt eine biholomorphe Abbildung $f: \mathbb{C} \setminus \{0\} \rightarrow \mathbb{D} \setminus \{0\}$.
- c** Es gibt eine biholomorphe Abbildung $f: \mathbb{C} \setminus [1, \infty) \rightarrow \mathbb{D}$.

Lösungsvorschlag zur Aufgabe (Herbst 2006, T3A1)

- a** *Falsch.* Die Abbildung f wäre eine ganze Funktion, die für $z \in \mathbb{C}$ die Abschätzung $|f(z)| < 1$ erfüllt, also wäre f nach dem Satz von Liouville konstant. Damit kann f aber weder injektiv noch surjektiv sein.

- b** *Falsch.* Die Menge $U = B_{\frac{1}{2}}(0) \setminus \{0\}$ ist eine offene, punktierte Umgebung von 0. Wegen $f(U) \subseteq \mathbb{D} \setminus \{0\}$ ist das Bild von U unter f beschränkt. Die Singularität 0 ist laut dem Riemannschen Hebbarkeitssatz also hebbbar und es existiert eine holomorphe Fortsetzung $\tilde{f}: \mathbb{C} \rightarrow \overline{\mathbb{D}}$. Analog zu Teil **a** folgt nun, dass eine solche Funktion konstant sein muss. Damit ist aber auch f konstant – Widerspruch zur Biholomorphie.
- c** *Richtig.* Die Menge $\mathbb{C} \setminus [1, \infty[$ ist ein einfach zusammenhängendes Gebiet. Die einzige Zusammenhangskomponente von $\mathbb{C} \setminus (\mathbb{C} \setminus [1, \infty[)$ ist nämlich $[1, \infty[$ und damit unbeschränkt. Somit garantiert der Riemannsche Abbildungssatz die Existenz einer solchen Funktion.

Riemann'sche Zahlenkugel und Möbius-Transformationen

Die komplexen Zahlen sind mittels stereographischer Projektion homöomorph zu einer Kugel ohne einen Punkt (vgl. Abbildung 6.3). Gelegentlich ist es von Vorteil, \mathbb{C} um diesen ausgesparten Punkt künstlich zu erweitern, welchen man dann als „ ∞ “ bezeichnet. Aus den komplexen Zahlen wird so die *Riemann'sche Zahlenkugel* $\widehat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$.

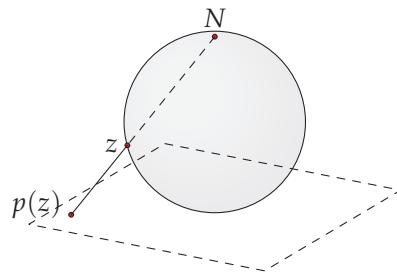


Abbildung 6.3: Um einen Punkt z auf der Kugel mittels stereographischer Projektion in die Gauß'sche Ebene abzubilden, zeichne die Gerade durch z und den Nordpol N der Kugel. Der Schnittpunkt dieser Geraden mit der Ebene ist der Bildpunkt $p(z)$.

Definition 6.38. Seien $a, b, c, d \in \mathbb{C}$ mit $ad - bc \neq 0$, so definieren wir für $c \neq 0$ die Abbildung

$$\varphi_{a,b,c,d}: \widehat{\mathbb{C}} \rightarrow \widehat{\mathbb{C}}, \quad z \mapsto \begin{cases} \frac{az+b}{cz+d} & \text{für } z \in \mathbb{C} \setminus \left\{-\frac{d}{c}\right\}, \\ \infty & \text{für } z = -\frac{d}{c}, \\ \frac{a}{c} & \text{für } z = \infty, \end{cases}$$

und für $c = 0$ setzen wir

$$\varphi_{a,b,0,d} : \widehat{\mathbb{C}} \rightarrow \widehat{\mathbb{C}}, \quad z \mapsto \begin{cases} \frac{az+b}{d} & \text{für } z \in \mathbb{C}, \\ \infty & \text{für } z = \infty. \end{cases}$$

Die so entstandene Abbildung nennt man *Möbius-Transformation*.

Die Bedingung $ad - bc \neq 0$ stellt sicher, dass Zähler und Nenner nicht zugleich Null sind. Zudem kann dadurch eine Zuordnung

$$\mathrm{GL}_2(\mathbb{C}) \rightarrow \{\varphi_{a,b,c,d} \mid a, b, c, d \in \mathbb{C}, ad - bc \neq 0\}, \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \varphi_{a,b,c,d}$$

definiert werden. Diese ist ein surjektiver Homomorphismus, insbesondere entspricht die Verkettung zweier Möbiustransformationen der Multiplikation der zugehörigen Matrizen. Dabei definieren zwei Matrizen genau dann die gleiche Abbildung, wenn sie skalare Vielfache voneinander sind.

Proposition 6.39. Die Möbius-Transformationen sind genau diebiholomorphen Abbildungen von $\widehat{\mathbb{C}}$ nach $\widehat{\mathbb{C}}$.

Eine wesentliche Abbildungseigenschaft der Möbius-Transformationen ist die *Kreistreue*. Eine sogenannte *verallgemeinerte Kreislinie* ist eine Kreislinie in \mathbb{C} oder eine Gerade in \mathbb{C} vereinigt mit dem Punkt ∞ . Das Bild einer solchen Kreislinie unter einer Möbius-Transformation ist stets wieder eine solche:

Proposition 6.40 (Kreistreue). Seien $\varphi: \widehat{\mathbb{C}} \rightarrow \widehat{\mathbb{C}}$ eine Möbius-Transformation, $L \subseteq \widehat{\mathbb{C}}$ eine verallgemeinerte Kreislinie sowie K_1 und K_2 die beiden Zusammenhangskomponenten von $\widehat{\mathbb{C}} \setminus L$. Wir bezeichnen die beiden Zusammenhangskomponenten von $\widehat{\mathbb{C}} \setminus \varphi(L)$ mit M_1 und M_2 , wobei $\varphi(a) \in M_1$ für ein $a \in K_1$. Dann gilt

$$\varphi(K_1) = M_1 \quad \text{und} \quad \varphi(K_2) = M_2.$$

Aufgabe (Frühjahr 2009, T1A1)

Gegeben sei die Funktion $f(z) = \frac{z+1}{2z}, z \in \mathbb{C} \setminus \{0\}$.

- a** Man bestimme das Bild der Einheitskreislinie unter f .
- b** Man bestimme das Bild der punktierten offenen Kreisscheibe $\{z \in \mathbb{C} \mid 0 < |z| < 1\}$ unter f .

Lösungsvorschlag zur Aufgabe (Frühjahr 2009, T1A1)

- a** Man berechnet für die Randpunkte $i, \pm 1$ leicht

$$f(-1) = 0, \quad f(1) = 1, \quad \text{und} \quad f(i) = \frac{i+1}{2i} = \frac{1}{2} - \frac{1}{2}i$$

und sieht (am besten anhand einer Skizze), dass die Bilder den Kreis $\partial B_{\frac{1}{2}}(\frac{1}{2})$ definieren. Allgemein berechnet man für beliebiges $z \in \mathbb{C}$ mit $|z| = 1$

$$\left| \frac{z+1}{2z} - \frac{1}{2} \right| = \left| \frac{1}{2z} \right| = \frac{1}{2|z|} = \frac{1}{2}.$$

Dies beweist $f(\partial \mathbb{E}) \subseteq \partial B_{\frac{1}{2}}(\frac{1}{2})$. Gleichheit folgt daraus, dass Möbius-Transformationen Kreislinien auf Kreislinien abbilden. (Gäbe es nämlich ein $a \in \mathbb{C} \setminus \mathbb{E}$ mit $f(a) \in K$, so würde die inverse Möbius-Transformation $\partial B_{\frac{1}{2}}(\frac{1}{2})$ auf eine Menge abbilden, die keine Kreislinie ist.)

- b** Die Abbildung f ist die natürliche Einschränkung der Möbius-Transformation

$$\varphi: \widehat{\mathbb{C}} \rightarrow \widehat{\mathbb{C}}, \quad z \mapsto \begin{cases} \frac{z+1}{2z} & \text{falls } z \in \mathbb{C} \setminus \{0\}, \\ \frac{1}{2} & \text{falls } z = \infty, \\ \infty & \text{falls } z = 0 \end{cases}$$

auf $\mathbb{C} \setminus \{0\}$. Diese bildet die Menge $\{z \in \mathbb{C} \mid |z| < 1\}$ auf eine der beiden Zusammenhangskomponenten von $\widehat{\mathbb{C}} \setminus \partial B_{\frac{1}{2}}(\frac{1}{2})$ ab. Dabei handelt es sich um

$$\left\{ z \in \mathbb{C} \mid \left| z - \frac{1}{2} \right| > \frac{1}{2} \right\} \cup \{\infty\} \quad \text{und} \quad \left\{ z \in \mathbb{C} \mid \left| z - \frac{1}{2} \right| < \frac{1}{2} \right\}.$$

Wegen $\varphi(0) = \infty$ muss es sich bei $\varphi(\mathbb{E})$ um die linke Menge handeln. Die Einschränkung auf $\mathbb{C} \setminus \{0\}$ erfüllt somit

$$f(\mathbb{E}) = \varphi|_{\mathbb{C} \setminus \{0\}}(\mathbb{E}) = \left\{ z \in \mathbb{C} \mid \left| z - \frac{1}{2} \right| > \frac{1}{2} \right\}.$$

Aufgabe (Frühjahr 2003, T1A5)

Sei $\widehat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$ die kompaktifizierte komplexe Ebene, und sei $f: \widehat{\mathbb{C}} \rightarrow \widehat{\mathbb{C}}$ die durch $w = f(z) := z/(z - i)$ gegebene gebrochen-lineare Funktion.

- a** Bestimmen Sie die Fixpunkte von f , die Umkehrabbildung f^{-1} und die Bilder bzw. Urbilder von $0, 1, i$ und ∞ .
- b** Skizzieren Sie das Bild der rechten Halbebene $\mathbb{H}_1 = \{z \in \mathbb{C} \mid \operatorname{Re} z \geq 0\}$, der oberen Halbebene $\mathbb{H}_2 = \{z \in \mathbb{C} \mid \operatorname{Im} z \geq 0\}$, und des offenen Einheitskreises $\mathbb{E} = \{z \in \mathbb{C} \mid |z| < 1\}$.

Lösungsvorschlag zur Aufgabe (Frühjahr 2003, T1A5)

a Fixpunkte: Wir lösen die Gleichung $f(z) = z$. Es gilt für $z \neq i$, dass

$$\frac{z}{z-i} = z \Leftrightarrow z = z^2 - iz \Leftrightarrow z^2 - (i+1)z = 0 \Leftrightarrow z(z - (i+1)) = 0$$

und wir erhalten die beiden Fixpunkte $z_1 = 0$ und $z_2 = i+1$.

Bilder: Es gilt

$$\begin{aligned} f(0) &= 0, & f(i) &= \infty, & f(\infty) &= 1, \\ f(1) &= \frac{1}{1-i} = \frac{1+i}{(1-i)(1+i)} = \frac{1}{2} + \frac{1}{2}i. \end{aligned}$$

Urbilder: Die meisten Urbilder lassen sich direkt aus den Bildern ablesen. Dementsprechend ist

$$f^{-1}(0) = 0, \quad f^{-1}(1) = \infty, \quad \text{und} \quad f^{-1}(\infty) = i.$$

Das Urbild von i berechnet man explizit oder man verwendet die Umkehrfunktion (siehe gleich) mit $f^{-1}(i) = \frac{1}{2} + \frac{1}{2}i$.

Bestimmung von f^{-1} : Sei $w \neq 1$, dann ist

$$\begin{aligned} \frac{z}{z-i} = w &\Leftrightarrow z = w(z-i) \Leftrightarrow (1-w)z = -iw \\ &\Leftrightarrow z = \frac{-iw}{1-w} = \frac{w}{-iw+i}. \end{aligned}$$

Die beiden nötigen Sonderfälle haben wir bereits bei den Urbildern abgehandelt und erhalten so

$$f^{-1}: \widehat{\mathbb{C}} \rightarrow \widehat{\mathbb{C}}, \quad z \mapsto \begin{cases} \frac{z}{-iz+i} & \text{für } z \in \mathbb{C} \setminus \{1\}, \\ \infty & \text{für } z = 1, \\ i & \text{für } z = \infty. \end{cases}$$

Alternative: Man verwendet Matrizenkalkül. Der angegebenen Möbius-Transformation lässt sich wie auf Seite 373 beschrieben die Matrix

$$A = \begin{pmatrix} 1 & 0 \\ 1 & -i \end{pmatrix} \quad \text{mit} \quad A^{-1} = \frac{1}{-i} \begin{pmatrix} -i & 0 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -i & i \end{pmatrix}$$

zuordnen. Die Umkehrfunktion von f ist damit durch $\varphi_{1,0,-i,i}$ gegeben.

b Sehen wir uns jeweils an, was auf dem Rand der betroffenen Mengen geschieht. Alle Ränder sind Kreise oder Geraden, sodass auch deren Bilder wieder Kreise oder Geraden sind. Da diese durch drei Punkte eindeutig bestimmt sind, genügt die Berechnung dreier willkürlicher Punkte.

1. Fall: Für die Elemente $0, i$ und $-i$ des Randes der rechten Halbebene gilt

$$f(0) \stackrel{\text{a}}{=} 0, \quad f(i) \stackrel{\text{a}}{=} \infty \quad \text{und} \quad f(-i) = \frac{-i}{-2i} = \frac{1}{2}.$$

Damit muss es sich bei $f(\partial\mathbb{H}_1)$ um die reelle Achse handeln. Tatsächlich gilt für beliebiges iy mit $y \in \mathbb{R}$

$$\operatorname{Im} f(iy) = \operatorname{Im} \frac{iy}{iy - i} = \operatorname{Im} \frac{y}{y - 1} = 0.$$

Aufgrund von Proposition 6.40 muss damit f die Menge \mathbb{H}_1 auf die obere oder untere Halbebene abbilden. Aus Teil **a** ist die Gleichung $f(1) = \frac{1}{2} + \frac{1}{2}i$ bekannt, sodass es sich bei $f(\mathbb{H}_1)$ um die obere Halbebene \mathbb{H}_2 handeln muss.

2. Fall: Für die Elemente $0, 1$ und -1 des Randes der oberen Halbebene gilt

$$f(0) \stackrel{\text{a}}{=} 0, \quad f(1) \stackrel{\text{a}}{=} \frac{1}{2} + \frac{1}{2}i \quad \text{und} \quad f(-1) = \frac{-1}{-1 - i} = \frac{1}{2} - \frac{1}{2}i.$$

Eine kurze Skizze legt nahe, dass alle diese Punkte auf dem Kreis um $\frac{1}{2}$ mit Radius $\frac{1}{2}$ liegen. Sei also $x \in \mathbb{R}$, dann ist

$$\left| f(x) - \frac{1}{2} \right| = \left| \frac{x}{x-i} - \frac{1}{2} \right| = \left| \frac{2x - (x-i)}{2(x-i)} \right| = \left| \frac{x+i}{2(x-i)} \right| = \frac{\sqrt{x^2+1}}{2\sqrt{x^2+1}} = \frac{1}{2}.$$

Damit gilt $f(\partial\mathbb{H}_2) = \partial B_{\frac{1}{2}}\left(\frac{1}{2}\right)$. Wegen $f(i) = \infty \in \widehat{\mathbb{C}} \setminus B_{\frac{1}{2}}\left(\frac{1}{2}\right)$ gilt damit $f(\mathbb{H}_2) = \widehat{\mathbb{C}} \setminus B_{\frac{1}{2}}\left(\frac{1}{2}\right)$.

3. Fall: Für die Elemente $1, i$ und $-i$ der Einheitskreislinie gilt

$$f(1) \stackrel{\text{a}}{=} \frac{1}{2} + \frac{1}{2}i, \quad f(i) \stackrel{\text{a}}{=} \infty \quad \text{und} \quad f(-i) \stackrel{\text{b}}{=} \frac{1}{2}.$$

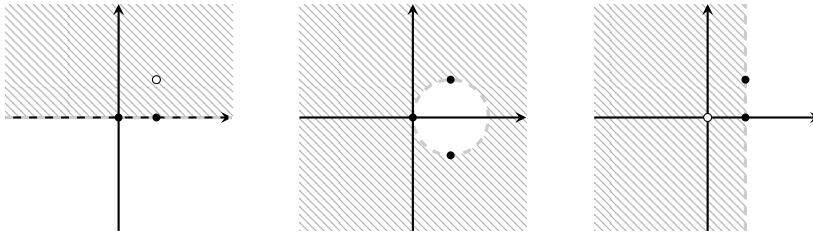
Aufgrund des zweiten Wertes muss es sich bei $f(\mathbb{E})$ um eine Gerade handeln, nämlich $\{z \in \mathbb{C} \mid \operatorname{Re} z = \frac{1}{2}\}$. Dies kann man für $z \in \partial\mathbb{E}$, also

$|z| = 1$, explizit nachrechnen:

$$\begin{aligned}\operatorname{Re} f(z) &= \frac{x+iy}{x+iy-i} = \operatorname{Re} \frac{x+iy}{x+i(y-1)} = \operatorname{Re} \frac{(x+iy)(x-i(y-1))}{x^2+(y-1)^2} = \\ &= \frac{x^2+y^2-y}{x^2+y^2-2y+1} = \frac{1-y}{2-2y} = \frac{1}{2}\end{aligned}$$

Wegen $f(0) = 0$ folgt $f(\mathbb{E}) = \{z \in \mathbb{C} \mid \operatorname{Re} z < \frac{1}{2}\}$.

Die verlangten Skizzen sehen dementsprechend wie folgt aus:



In der Zeichnung finden sich neben den Rändern der Bereiche (gestrichelt) auch die berechneten Punkte auf den Rändern bzw. in den Mengen.

Aufgabe (Frühjahr 2004, T2A1)

Sei D der Durchschnitt der beiden offenen Kreisscheiben $D_1 = \{z \in \mathbb{C} \mid |z - i| < 1\}$ und $D_2 = \{z \in \mathbb{C} \mid |z - 1| < 1\}$. Bestimmen Sie das Bild von D unter der Möbius-Transformation

$$f(z) = \frac{z}{z - (1 + i)}$$

Lösungsvorschlag zur Aufgabe (Frühjahr 2004, T2A1)

Wir berechnen zunächst das Bild unter den beiden Kreisscheiben. Die drei Punkte $0, -1 + i, 1 + i$ liegen auf ∂D_1 . Wegen $f(1 + i) = \infty$ ergibt das Bild auf jeden Fall eine Gerade. Für die weiteren Punkte gilt

$$f(0) = 0 \quad \text{und} \quad f(-1 + i) = \frac{-1 + i}{-2} = \frac{1}{2} - \frac{1}{2}i.$$

Es muss sich also um die Gerade $\{x + iy \in \mathbb{C} \mid x + y = 0\}$ handeln. Um einen expliziten (und „wasserdichten“) Nachweis zu führen, berechnen wir

zunächst für $z = x + iy \in \mathbb{C} \setminus \{1 + i\}$

$$\begin{aligned} f(z) &= \frac{x + iy}{x + iy - (1 + i)} = \frac{x + iy}{(x - 1) + i(y - 1)} = \frac{(x + iy)((x - 1) - i(y - 1))}{(x - 1)^2 + (y - 1)^2} = \\ &= \frac{x^2 - x + y^2 - y}{(x - 1)^2 + (y - 1)^2} + i \frac{-y + x}{(x - 1)^2 + (y - 1)^2}. \end{aligned}$$

Für $z \in \partial D_1$ gilt nun $|z - i| = 1$, also $x^2 + (y - 1)^2 = 1$ und damit

$$\operatorname{Re} f(z) + \operatorname{Im} f(z) = \frac{x^2 + (y - 1)^2 - 1}{(x - 1)^2 + (y - 1)^2} = 0.$$

Aufgrund der Kreistreue gilt nun entweder $f(D_1) = \{x + iy \in \mathbb{C} \mid x + y < 0\}$ oder $f(D_1) = \{x + iy \mid x + y > 0\}$. Wegen

$$f(i) = \frac{i}{i - (1 + i)} = \frac{i}{-1} = -i$$

ist ersteres der Fall.

Ebenso verfahren wir für den zweiten Kreis: Es sind $1 + i, 1 - i, 0$ Elemente von ∂D_2 . Für diese gilt

$$f(1 + i) = \infty, \quad f(0) = 0 \quad \text{und} \quad f(1 - i) = \frac{1 - i}{-2i} = \frac{i + 1}{2} = \frac{1}{2} + \frac{1}{2}i.$$

Und diesmal behaupten wir, dass es sich bei der Bildmenge $f(\partial D_2)$ um die Gerade $\{x + iy \in \mathbb{C} \mid x - y = 0\}$ handelt. Wir betrachten Punkte $z \in \partial D_2$. Für diese gilt $|z - 1| = 1$, also $(x - 1)^2 + y^2 = 1$.

$$\operatorname{Re} f(z) - \operatorname{Im} f(z) = \frac{x^2 - 2x + y^2}{(x - 1)^2 + (y - 1)^2} = \frac{(x - 1)^2 + y^2 - 1}{(x - 1)^2 + (y - 1)^2} = 0.$$

Und wegen $f(1) = i$ gilt hier $f(D_2) = \{x + iy \in \mathbb{C} \mid x - y < 0\}$.

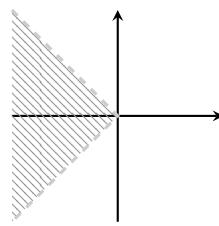
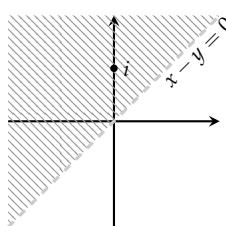
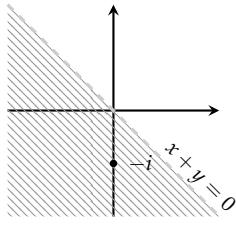
Wir behaupten nun die Gleichung

$$f(D_1 \cap D_2) = f(D_1) \cap f(D_2).$$

„ \subseteq “: Ist $z \in f(D_1 \cap D_2)$, so ist $z = f(d)$ für ein $d \in D_1 \cap D_2$, also insbesondere $z = f(d) \in f(D_1)$ und $z = f(d) \in f(D_2)$.

„ \supseteq “: Ist $z \in f(D_1) \cap f(D_2)$, so ist $z = f(d_1)$ für ein $d_1 \in D_1$ und $z = f(d_2)$ für ein $d_2 \in D_2$. Da f injektiv ist, folgt aus $f(d_1) = z = f(d_2)$ jedoch $d_1 = d_2$, also $d_1 \in D_1 \cap D_2$ und somit $z \in f(D_1 \cap D_2)$. Wir erhalten

$$f(D) = f(D_1) \cap f(D_2) = \{x + iy \in \mathbb{C} \mid x + y < 0 \text{ und } x - y < 0\}.$$



(Die Abbildung zeigt schraffierte die Bildmengen $f(D_1)$, $f(D_2)$ und $f(D)$. Sie war nicht verlangt.)

Aufgabe (Frühjahr 2007, T2A3)

Betrachten Sie die Möbius-Transformation

$$f(z) = \frac{z-i}{z+i}$$

- a** Zeigen Sie, dass $f: \mathbb{C} \setminus \{-i\} \rightarrow \mathbb{C} \setminus \{1\}$ biholomorph ist, und bestimmen Sie die Umkehrabbildung $g(z)$.
- b** Beschreiben und skizzieren Sie die Höhenlinien $|f(z)| = \text{const}$ von f .

Lösungsvorschlag zur Aufgabe (Frühjahr 2007, T2A3)

- a** Gemäß Proposition 6.36 genügt es zu zeigen, dass f bijektiv und holomorph ist. Die Holomorphie auf $\mathbb{C} \setminus \{-i\}$ folgt aus der Quotientenregel.
Injectivität: Seien $z_1, z_2 \in \mathbb{C}$ mit $f(z_1) = f(z_2)$. Wir erhalten

$$\begin{aligned} \frac{z_1-i}{z_1+i} = \frac{z_2-i}{z_2+i} &\Leftrightarrow (z_1-i)(z_2+i) = (z_1+i)(z_2-i) \Leftrightarrow \\ iz_1 - iz_2 &= iz_2 - iz_1 \Leftrightarrow 2iz_1 = 2iz_2 \Leftrightarrow z_1 = z_2. \end{aligned}$$

Surjektivität: Sei $w \in \mathbb{C} \setminus \{1\}$ vorgegeben. Wir suchen ein $z \in \mathbb{C} \setminus \{-i\}$ mit $f(z) = w$. Es gilt

$$\frac{z-i}{z+i} = w \Leftrightarrow z-i = w(z+i) \Leftrightarrow z-wz = (w+1)i \Leftrightarrow z = \frac{(w+1)i}{1-w}.$$

Aus der Annahme $z = -i$ folgt nach kurzer Rechnung der Widerspruch $i = -i$, also ist $z \in \mathbb{C} \setminus \{-i\}$ und damit tatsächlich ein Urbild zu w . Aus dieser Rechnung erhalten wir auch sofort die Umkehrabbildung

$$g: \mathbb{C} \setminus \{1\} \rightarrow \mathbb{C} \setminus \{-i\}, \quad z \mapsto \frac{iz+i}{-z+1}.$$

b Sei $c \in \mathbb{R}_0^+$. Wir erhalten für $z = x + iy \in \mathbb{C} \setminus \{-i\}$

$$\begin{aligned} \left| \frac{z-i}{z+i} \right| = c &\Leftrightarrow \sqrt{\frac{x^2 + (y-1)^2}{x^2 + (y+1)^2}} = c \\ &\Leftrightarrow x^2 + y^2 - 2y + 1 = c^2 x^2 + c^2 y^2 + 2c^2 y + c^2 \\ &\Leftrightarrow (1 - c^2)x^2 + (1 - c^2)y^2 - 2(1 + c^2)y + 1 - c^2 = 0. \end{aligned}$$

Im Fall $c \neq 1$ können wir durch $(1 - c^2)$ teilen und erhalten so mit der Abkürzung $\gamma_c = \frac{1+c^2}{1-c^2}$ und mittel quadratischer Ergänzung

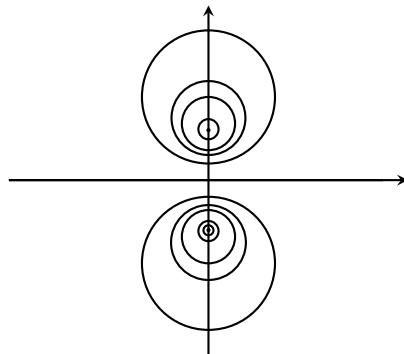
$$\begin{aligned} x^2 + y^2 - 2y \left(\frac{1+c^2}{1-c^2} \right) + 1 &= 0 \\ x^2 + (y - \gamma_c)^2 - \gamma_c^2 + 1 &= 0 \quad \Leftrightarrow \quad x^2 + (y - \gamma_c)^2 = \gamma_c^2 - 1 \\ &\Leftrightarrow |z - i\gamma_c| = \sqrt{\gamma_c^2 - 1}. \end{aligned}$$

Für den letzten Schritt sei bemerkt, dass aus $|1 - c^2| \leq |1 + c^2|$ folgt, dass $\gamma_c^2 \geq 1$. Die Höhenlinien für c sind in diesem Fall also Kreise um $i\gamma_c$ mit Radius $\sqrt{\gamma_c^2 - 1}$.

Für den Fall $c = 1$ wird die obige Gleichung zu

$$-4y = 0 \quad \Leftrightarrow \quad y = 0.$$

Die zugehörige Höhenlinie im Fall $c = 1$ ist also die reelle Achse.



Die Abbildung zeigt die Höhenlinien für $c \in \{2, 3, 4, 10, 20, 100\}$ (unten), $c \in \left\{ \frac{1}{100}, \frac{1}{4}, \frac{1}{3}, \frac{1}{2}, 1 \right\}$ (oben) sowie für $c = 1$ (reelle Achse).

Konstruktionbiholomorpher Abbildungen

In Aufgabe F03T1A5 a haben wir gesehen, dass die Bestimmung von Fixpunkten von Möbius-Transformationen auf eine quadratische Gleichung führt. Eine Möbius-Transformation hat also maximal zwei Fixpunkte oder ist bereits die Identität. Daraus folgt auch, dass eine Möbius-Transformation bereits durch die Bilder von drei Punkten eindeutig bestimmt ist: Sind nämlich für $j \in \{1, 2, 3\}$ Punkte $z_j, w_j \in \widehat{\mathbb{C}}$ gegeben und σ, τ Transformationen mit $\sigma(z_j) = \tau(z_j) = w_i$ für $j \in \{1, 2, 3\}$, so wäre $\sigma \circ \tau^{-1}$ eine Möbius-Transformation mit $(\sigma \circ \tau^{-1})(w_j) = w_j$, woraus $\sigma \circ \tau^{-1} = \text{id}$, also $\sigma = \tau$ folgt.

Doppelverhältnisse und Möbius-Transformationen. Seien vier verschiedene komplexe Zahlen $z, z_1, z_2, z_3 \in \mathbb{C}$ vorgegeben. Wir definieren ihr sogenanntes *Doppelverhältnis* als

$$DV(z, z_1, z_2, z_3) = \frac{z - z_1}{z - z_3} \cdot \frac{z_2 - z_3}{z_2 - z_1}.$$

Mittels entsprechender Grenzwertbildung lässt sich diese Definition auch auf den Fall ausdehnen, dass eines der Elemente ∞ ist. Es gilt beispielsweise

$$DV(z, z_1, z_2, \infty) = \lim_{|z_3| \rightarrow \infty} \frac{z - z_1}{z - z_3} \cdot \frac{z_2 - z_3}{z_2 - z_1} = \lim_{|z_3| \rightarrow \infty} \frac{z_2 - z_3}{z - z_3} \cdot \frac{z - z_1}{z_2 - z_1} = \frac{z - z_1}{z_2 - z_1}.$$

Eine wesentliche Bedeutung für die Theorie der Möbius-Transformationen bekommt das Doppelverhältnis dadurch, dass das Doppelverhältnis von vier Punkten in $\widehat{\mathbb{C}}$ mit dem Doppelverhältnis der zugehörigen Bilder unter einer Möbius-Transformation übereinstimmt – dies liefert einen Ansatz zur Bestimmung einer solchen Transformation durch drei vorgegebene Funktionswerte.

Anleitung: Möbius-Transformation durch drei Punkte

Seien für $j \in \{1, 2, 3\}$ Werte $z_j, w_j \in \widehat{\mathbb{C}}$ gegeben. Gesucht ist eine Möbius-Transformation $\widehat{\mathbb{C}} \rightarrow \widehat{\mathbb{C}}$ mit $f(z_j) = w_j$.

- (1) Löse die Doppelverhältnisgleichung

$$\frac{z - z_1}{z - z_3} \cdot \frac{z_2 - z_3}{z_2 - z_1} = \frac{w - w_1}{w - w_3} \cdot \frac{w_2 - w_3}{w_2 - w_1}$$

nach w auf.

- (2) Setze $f(z) = w$. Definiere dann noch das Bild der Nennernullstelle und für ∞ gemäß Definition 6.38.

Aufgabe (Herbst 2001, T3A2)

Es seien folgende Punkte in der komplexen Ebene \mathbb{C} gegeben:

$$z_1 = 0, z_2 = i, z_3 = -i \quad \text{sowie} \quad w_1 = -i/2, w_2 = i, w_3 = -i.$$

- a** Bestimmen Sie die Möbius-Transformation mit $f(z_i) = w_i$ für $i = 1, 2, 3$.
- b** Bestimmen Sie das Bild des Einheitskreises und seines Randes unter f .
- c** Bestimmen Sie die zu f inverse Abbildung.

Lösungsvorschlag zur Aufgabe (Herbst 2001, T3A2)

- a** Wir lösen die Doppelverhältnis-Gleichung

$$\frac{z}{z+i} \cdot \frac{i+i}{i} = \frac{w+\frac{i}{2}}{w+i} \cdot \frac{i+i}{i+\frac{i}{2}} \Leftrightarrow \frac{2z}{z+i} = \frac{w+\frac{i}{2}}{w+i} \cdot \frac{4}{3}$$

nach w auf und erhalten $w = \frac{2z-i}{iz+2}$. Der Nenner ist für $z = 2i$ nicht definiert, hier ist der Funktionswert ∞ . Für $z = \infty$ erhalten wir andererseits den Wert $\frac{2}{i} = -2i$. Also ist

$$f = \varphi_{2,-i,i,2} : \widehat{\mathbb{C}} \rightarrow \widehat{\mathbb{C}}, \quad z \mapsto \begin{cases} \frac{2z-i}{iz+2} & \text{falls } z \in \mathbb{C} \setminus \{2i\}, \\ \infty & \text{falls } z = 2i \\ -2i, & \text{falls } z = \infty. \end{cases}$$

Man überprüft unmittelbar, dass diese die geforderten Gleichungen erfüllt.

- b** Aus der Angabe folgt bereits $i, -i \in f(\partial\mathbb{E})$. Wir bestimmen noch ein drittes Element:

$$f(1) = \frac{2-i}{i+2} = \frac{(2-i)(2-i)}{5} = \frac{3}{5} - \frac{4}{5}i.$$

Wegen $|\frac{3}{5} - \frac{4}{5}i| = 1$ liegt auch dieser Punkt auf dem Rand des Einheitskreises. Tatsächlich gilt für beliebiges $z = x+iy \in \mathbb{C}$ mit $|z| = x^2 + y^2 = 1$, dass

$$\begin{aligned} \left| \frac{2z-i}{iz+2} \right| &= \left| \frac{2(x+iy)-i}{i(x+iy)+2} \right| = \left| \frac{2x+(2y-1)i}{(-y+2)+ix} \right| = \frac{\sqrt{4x^2+4y^2-4y+1}}{\sqrt{y^2-4y+4+x^2}} = \\ &= \frac{\sqrt{-4y+5}}{\sqrt{-4y+5}} = 1. \end{aligned}$$

Dies beweist $f(\partial\mathbb{E}) = \partial\mathbb{E}$ (wobei die Inklusion „ \supseteq “ wiederum aus der Kreistreu von Möbius-Transformationen folgt). Die Einheitskreisscheibe wird somit entweder auf \mathbb{E} oder auf $\widehat{\mathbb{C}} \setminus \overline{\mathbb{E}}$ abgebildet. Wegen $f(0) = -\frac{i}{2} \in \mathbb{E}$ ist ersteres der Fall.

- c** Wiederum könnte man das selbe Verfahren wie in Teil **a** anwenden und dabei nur Bild- und Urbildwerte vertauschen. Alternativ betrachtet man die Matrix

$$A = \begin{pmatrix} 2 & -i \\ i & 2 \end{pmatrix} \quad \text{mit} \quad A^{-1} = \frac{1}{3} \begin{pmatrix} 2 & i \\ -i & 2 \end{pmatrix}.$$

Die inverse Abbildung ist damit gegeben durch

$$f^{-1}(z) = \varphi_{2,i,-i,2}(z) = \begin{cases} \frac{2z+i}{-iz+2} & \text{für } z \in \mathbb{C} \setminus \{-2i\} \\ \infty & \text{für } z = -2i, \\ 2i & \text{für } z = \infty. \end{cases}$$

Anleitung: Konstruktion von Möbius-Transformationen

Gegeben seien zwei Gebiete G_1, G_2 , die aufeinander biholomorph abgebildet werden sollen. Wir gehen davon aus, dass die Ränder von G_1 und G_2 verallgemeinerte Kreislinien sind.

- (1) Wähle drei Punkte auf dem Rand von G_1 und drei Punkte auf dem Rand von G_2 .
Tipp: Mutige sparen sich Rechenarbeit, indem sie, wo möglich, den Punkt ∞ verwenden.
- (2) Bestimme die Möbius-Transformation, die die Punkte aus (1) paarweise aufeinander abbildet (vgl. hierzu Seite 381).
- (3) Überprüfe für einen Punkt aus G_1 , ob dieser von der Möbius-Transformation aus (2) nach G_2 oder nach $\widehat{\mathbb{C}} \setminus \overline{G_2}$ abgebildet wird. Ist ersteres der Fall, so ist die Einschränkung der Möbius-Transformation eine Abbildung mit der gewünschten Eigenschaft. Im zweiten Fall tausche in der Konstruktion (1) zwei Bildpunkte miteinander. Die dann entstehende Abbildung hat die gewünschten Eigenschaften.

Aufgabe (Frühjahr 2006, T2A1)

- a** Formulieren Sie den Riemann'schen Abbildungssatz.
b Finden Sie eine Funktion der Form $z \mapsto \frac{az+b}{cz+d}$, die die rechte Halbebene

$$H = \{z \in \mathbb{C} \mid \operatorname{Re}(z) > 0\}$$

biholomorph auf die offene Einheitskreisscheibe

$$D = \{z \in \mathbb{C} \mid |z| < 1\}$$

abbildet (mit Beweis).

Lösungsvorschlag zur Aufgabe (Frühjahr 2006, T2A1)

- a** Siehe Satz 6.37.
b Wir konstruieren eine Möbiustransformation, die ∂H auf ∂D abbildet. Dazu bestimmen wir $f : \widehat{\mathbb{C}} \rightarrow \widehat{\mathbb{C}}$ mit

$$f(0) = 1 \quad f(i) = -i \quad f(\infty) = -1.$$

Wir gehen wie oben beschrieben vor und lösen zunächst

$$\begin{aligned} DV(z, 0, i, \infty) &= \frac{w-1}{w+1} \cdot \frac{-i+1}{-i-1} \Leftrightarrow \frac{z}{i} = \frac{w-1}{w+1} \cdot i \Leftrightarrow z = -\frac{w-1}{w+1} \\ &\Leftrightarrow zw + z = -w + 1 \Leftrightarrow zw + w = -z + 1 \Leftrightarrow w = \frac{-z+1}{z+1}. \end{aligned}$$

Wir definieren dementsprechend die Möbius-Transformation

$$f : \widehat{\mathbb{C}} \rightarrow \widehat{\mathbb{C}}, \quad z \mapsto \begin{cases} \frac{-z+1}{z+1} & \text{für } z \in \mathbb{C} \setminus \{-1\} \\ \infty & \text{für } z = -1 \\ -1 & \text{für } z = \infty \end{cases}$$

Zunächst betrachten wir, was im Grenzfall $z = iy$ für $y \in \mathbb{R}$ geschieht:

$$|f(z)| = \left| \frac{-iy-1}{iy+1} \right| = \frac{\sqrt{1+y^2}}{\sqrt{1+y^2}} = 1$$

Zusammen mit der Definition im Fall $z = \infty$ ergibt sich

$$f(i\mathbb{R} \cup \{\infty\}) \subseteq \{z \in \mathbb{C} \mid |z| = 1\}$$

Somit bildet die Möbius-Transformation f die verallgemeinerte Kreislinie $i\mathbb{R} \cup \{\infty\}$ auf die Einheitskreislinie ab. Damit bildet f auch die

Zusammenhangskomponenten des Komplements aufeinander ab. Wegen $f(1) = \frac{0}{2} = 0 \in D$ muss $f(H) = D$ gelten. Die Einschränkung $f|_H$ liefert also eine biholomorphe Abbildung, wie sie gewünscht war.

Aufgabe (Herbst 2010, T1A3)

Konstruieren Sie eine gebrochen-rationale Abbildung (Möbius-Transformation) f , die die Kreisscheibe $K := \{z \in \mathbb{C} \mid |z+1| < 2\}$ auf die obere Halbebene $H := \{w \in \mathbb{C} \mid \operatorname{Im}(w) > 0\}$ abbildet. Ist eine solche Abbildung eindeutig bestimmt?

Lösungsvorschlag zur Aufgabe (Herbst 2010, T1A3)

Wir wählen drei Punkte auf dem Rand von K und drei Punkte auf dem Rand von H , beispielsweise

$$z_1 = -3, z_2 = 1, z_3 = -1 + 2i \in \partial K \quad \text{und} \quad w_1 = -1, w_2 = 0, w_3 = 1 \in \partial H.$$

Nun lösen wir die Doppelverhältnisgleichung

$$\frac{z+3}{z+(1-2i)} \cdot \frac{1+1-2i}{1+3} = \frac{w+1}{w-1} \cdot \frac{-1}{1}$$

nach w auf und erhalten

$$w = \frac{(-1-i)z + (1+i)}{(3-i)z + (5-7i)}.$$

Für die Nullstelle des Nenners ergibt sich $z_0 = -\frac{5-7i}{3-i} = -\frac{11}{5} + \frac{8}{5}i$. Ferner gilt sogar

$$\left| -\frac{11}{5} + \frac{8}{5}i + 1 \right| = \left| -\frac{6}{5} + \frac{8}{5}i \right| = \sqrt{\frac{36}{25} + \frac{64}{25}} = 2,$$

sodass diese auf ∂K liegt. Definieren wir also die Möbius-Transformation

$$f: \widehat{\mathbb{C}} \rightarrow \widehat{\mathbb{C}}, \quad z \mapsto \begin{cases} \frac{(-1-i)z + (1+i)}{(3-i)z + (5-7i)} & \text{falls } z \in \mathbb{C} \setminus \{z_0\}, \\ \infty & \text{falls } z = z_0, \\ \frac{-1-i}{3-i} = \frac{-(1+2i)}{5} & \text{falls } z = \infty. \end{cases}$$

Diese bildet nach Konstruktion die Kreislinie ∂K nach ∂H ab. Damit wird K auf

$$H = \{z \in \mathbb{C} \mid \operatorname{Im} z > 0\} \quad \text{oder} \quad \{z \in \mathbb{C} \mid \operatorname{Im} z < 0\}$$

abgebildet. Wegen

$$f(-1) = \frac{1+i+1+i}{-3+i+5-7i} = \frac{2+2i}{2-6i} = \frac{-1+2i}{5} \in H$$

ist ersteres der Fall.

Die Einschränkung $f|_K$ liefert damit eine Abbildung mit den verlangten Eigenschaften.

Eine solche Abbildung ist *nicht* eindeutig bestimmt. Zwar ist eine Abbildung durch die drei Punkte eindeutig bestimmt. Wenn bei den obigen Bedingungen jedoch für w_3 anstelle von 1 das Element $-2 \in \partial H$ gewählt worden wäre, so hätte man die Abbildung

$$g: \mathbb{C} \rightarrow \mathbb{C}, \quad z \mapsto \frac{-2i(z-1)}{(1+2i)z+(3-2i)}$$

erhalten, die ebenfalls K biholomorph auf H abbildet. Wegen $f(0) \neq g(0)$ ist jedoch $f \neq g$.

Aufgabe (Herbst 2010, T2A1)

Gegeben sei die Möbius-Transformation $h(z) = \frac{1}{z-1}$. Sei $\mathbb{E} \subseteq \mathbb{C}$ die offene Einheitskreisscheibe und $K \subseteq \mathbb{C}$ die abgeschlossene Kreisscheibe $\{z \in \mathbb{C} \mid |z - \frac{1}{2}| \leq \frac{1}{2}\}$. Mit $\partial\mathbb{E}$ und ∂K werde der Rand von \mathbb{E} bzw. K bezeichnet.

- a** Man zeige, dass $h(\partial\mathbb{E})$ und $h(\partial K)$ parallele Geraden sind.
- b** Man gebe die Gerade $h(\partial\mathbb{E})$ und $h(\partial K)$ jeweils explizit in der Form $ax + by = c$ an, wobei x und y Real- bzw. Imaginärteil von $z \in \mathbb{C}$ sind.
- c** Man bestimme $h(\mathbb{E} \setminus K)$ explizit durch Ungleichungen der Form $ax + by \geqslant c$ und skizziere die Menge $\mathbb{E} \setminus K$ und $h(\mathbb{E} \setminus K)$.

Lösungsvorschlag zur Aufgabe (Herbst 2010, T2A1)

- a** Eine Möbius-Transformation muss jede Kreislinie entweder auf eine Gerade oder auf eine Kreislinie abbilden. Wir setzen drei Punkte aus $\partial\mathbb{E}$ ein und erhalten

$$h(-1) = -\frac{1}{2}, \quad h(i) = \frac{1}{i-1} = -\frac{1}{2} - \frac{1}{2}i, \quad \text{sowie } h(-i) = \frac{1}{-i-1} = -\frac{1}{2} + \frac{1}{2}i.$$

Wir zeigen, dass der Realteil aller Zahlen im Bild von ∂E gleich $-\frac{1}{2}$ ist, dann folgt aus der Kreistreue, dass $h(\partial E) = \{z \in \mathbb{C} \mid \operatorname{Re} z = -\frac{1}{2}\}$. Es gilt für $z = x + iy \in \mathbb{C}$ mit $|z| = 1, z \neq 1$, dass

$$\begin{aligned}\operatorname{Re} \frac{1}{z-1} &= \operatorname{Re} \frac{1}{(x-1)+iy} = \operatorname{Re} \frac{(x-1)-iy}{(x-1)^2+y^2} = \frac{x-1}{x^2-2x+1+y^2} = \\ &= \frac{x-1}{-2x+2} = -\frac{1}{2}.\end{aligned}$$

Analog verfahren wir mit dem zweiten Kreis:

$$h(0) = -1, \quad h\left(\frac{1}{2} + \frac{1}{2}i\right) = -1 - i, \quad \text{und} \quad h\left(\frac{1}{2} - \frac{1}{2}i\right) = -1 + i.$$

Und entsprechend gilt hier mittels quadratischer Ergänzung

$$\begin{aligned}\operatorname{Re} \frac{1}{z-1} &= \operatorname{Re} \frac{1}{(x+iy)-1} = \operatorname{Re} \frac{(x-1)-iy}{(x-1)^2+y^2} = \frac{x-1}{x^2-2x+1+y^2} = \\ &= \frac{x-1}{(x-\frac{1}{2})^2-x+\frac{3}{4}+y^2} = \frac{x-1}{\frac{1}{4}-x+\frac{3}{4}} = -1.\end{aligned}$$

Somit handelt es sich bei beiden Mengen um Geraden, die parallel zur x -Achse sind.

b Wir haben beide Gleichungen in Teil **a** bereits hergeleitet:

$$h(\partial E) = \{x+iy \in \mathbb{C} \mid 2x = -1\} \quad \text{und} \quad h(\partial K) = \{x+iy \in \mathbb{C} \mid x = -1\}.$$

c Wir zeigen zunächst

$$h(E \setminus K) = h(E) \setminus h(K).$$

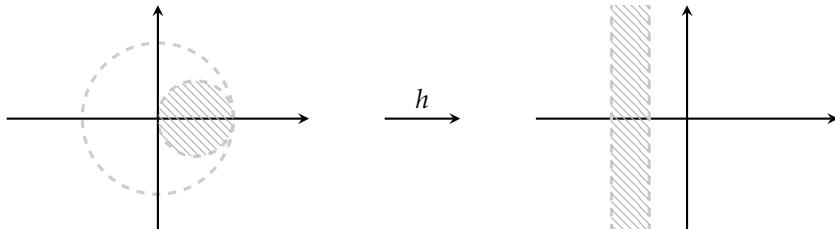
„ \subseteq “: Sei $w \in h(E \setminus K)$, also $w = h(z)$ für ein $z \in E, z \notin K$. Dann ist w jedenfalls auch Element von $h(E)$. Angenommen, es wäre $w = h(\hat{z})$ für ein $\hat{z} \in K$. Dann wäre aufgrund der Injektivität von h aber $z = \hat{z} \in K$ – Widerspruch. Also ist w in der rechten Menge enthalten.

„ \supseteq “: Sei $w \in h(E) \setminus h(K)$, also $w = h(z)$ für ein $z \in E$, aber $h(\hat{z}) \neq w$ für alle $\hat{z} \in K$. Dann gilt insbesondere $z \notin K$, also ist $w = h(z) \in h(E \setminus K)$.

Wir bestimmen die Bilder $h(E)$ und $h(K)$. Da diese wieder Zusammenhangskomponenten von $\mathbb{C} \setminus \partial E$ bzw. $\mathbb{C} \setminus \partial K$ sein müssen, kommt für die erste Menge nur $\{z \in \mathbb{C} \mid \operatorname{Re} z > -\frac{1}{2}\}$ oder $\{z \in \mathbb{C} \mid \operatorname{Re} z < -\frac{1}{2}\}$ infrage. Wegen $h(0) = -1$ muss es sich bei $h(E)$ um die zweite Mengen handeln.

Eine analoge Überlegung liefert wegen $h(\frac{1}{2}) = -2$ die Gleichung $h(K) = \{z \in \mathbb{C} \mid \operatorname{Re} z < -1\}$. Wir erhalten damit

$$h(\mathbb{E} \setminus K) = \left\{ x + iy \in \mathbb{C} \mid x > -1 \text{ und } x < -\frac{1}{2} \right\}.$$



Übersicht: Wichtige biholomorphe Abbildungen

Je nach Form der gegebenen Mengen, die biholomorph aufeinander abgebildet werden sollen, bieten sich verschiedene Abbildungen an:

- (1) Kreise und Halbebenen (also verallgemeinerte Kreislinien) lassen sich mittels Möbiustransformationen aufeinander abbilden.
- (2) Die Exponentialfunktion kann dazu genutzt werden, Streifen der Form $\{z \in \mathbb{C} \mid a < \operatorname{Im} z < b\}$ auf die Mengen $\{re^{i\theta} \mid r \in \mathbb{R}^\times, a < \theta < b\}$ abzubilden.
- (3) Mithilfe der Abbildung $z \mapsto z^2$ kann ein Quadrant auf eine Halbebene oder eine Halbebene auf eine geschlitzte Ebene abgebildet werden (allgemein gilt: Abbildungen der Form $z \mapsto z^n$ ver-n-fachen den „Öffnungswinkel“).
- (4) Drehungen um den Winkel θ (gegen den Uhrzeigersinn) lassen sich durch Multiplikation mit der Konstanten $e^{2\pi i\theta}$ erreichen.
- (5) Manchmal ist es nötig, die Einheitskreisscheibe auf sich selbst abzubilden, um eine bestimmte Anfangsbedingung zu erfüllen. Die biholomorphen Abbildungen $\varphi: \mathbb{E} \rightarrow \mathbb{E}$ mit $\varphi(a) = 0$ für ein $a \in \mathbb{E}$ sind genau die Abbildungen

$$\varphi(z) = \zeta \frac{z - a}{\bar{a}z - 1}, \quad \text{wobei } a \in \mathbb{E}, \zeta \in \partial \mathbb{E}.$$

Im Fall $\varphi(0) = 0$ vereinfachen sich diese Abbildungen zu $z \mapsto \zeta z$.

Aufgabe (Frühjahr 2009, T1A3)

Gegeben sei das Gebiet $G := \mathbb{C} \setminus \{iy \mid y \geq 0\}$. Auf welches der folgenden Gebiete lässt sich G biholomorph abbilden?

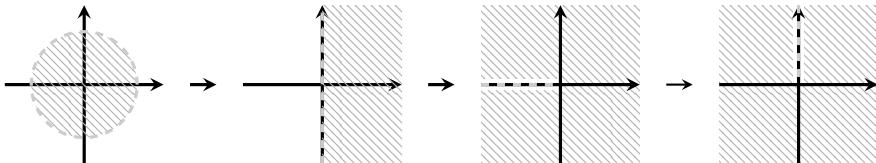
- a** $\{w \in \mathbb{C} \mid |z| < 1\}$;
- b** $\{w \in \mathbb{C} \mid |z| > 1\}$.

Man gebe im Falle der Existenz jeweils eine solche Abbildung an.

Lösungsvorschlag zur Aufgabe (Frühjahr 2009, T1A3)

- a** Die Menge G ist ein sternförmiges Gebiet und somit einfach zusammenhängend. Bei der angegebenen Menge handelt es sich um die Einheitskreisscheibe, sodass laut dem Riemannschen Abbildungssatz eine solche biholomorphe Abbildung existiert.

Zur Konstruktion der Abbildung gehen wir in mehreren Schritten vor, wie die folgende Abbildung veranschaulicht.



Wir transformieren zunächst den Einheitskreis mittels einer Möbius-Transformation auf die rechte Halbebene $\mathbb{H} = \{z \in \mathbb{C} \mid \operatorname{Re} z > 0\}$. Man wählt sich hierzu wie oben drei Punkte auf dem Rand und erhält

$$f : \mathbb{D} \rightarrow \mathbb{H}, \quad z \mapsto \frac{z-1}{z+1}.$$

Die Halbebene \mathbb{H} bilden wir nun in einem zweiten Schritt auf die geschlitzte Ebene $\mathbb{C} \setminus [-\infty, 0]$ ab. Wir zeigen hierzu, dass

$$g : \mathbb{H} \rightarrow \mathbb{C} \setminus [-\infty, 0], \quad z \mapsto z^2$$

eine biholomorphe Abbildung ist. Die Holomorphie ist als Polynomfunktion klar. Zunächst sei bemerkt, dass für $z \in \mathbb{H}$ gilt, dass $z^2 \notin [-\infty, 0]$ (sonst müsste $\operatorname{Re} z = 0$ gelten.)

Für die *Injectivität* betrachte $z_1 \neq z_2 \in \mathbb{H}$ mit $g(z_1) = g(z_2)$. Es folgt

$$z_1^2 = z_2^2 \Leftrightarrow z_1^2 - z_2^2 = 0 \Leftrightarrow (z_1 + z_2)(z_1 - z_2) = 0$$

Nehmen wir an, es wäre $z_1 + z_2 = 0$, also $z_1 = -z_2$. Wegen $z_1 \in \mathbb{H}$ würde aber folgen $\operatorname{Re} z_2 = -\operatorname{Re} z_1 < 0$, also $z_2 \notin \mathbb{H}$ – Widerspruch. Also muss $z_1 = z_2$ gelten.

Für die *Surjektivität* sei $w \in \mathbb{C} \setminus]-\infty, 0]$ vorgegeben. Schreibe $w = re^{i\varphi}$ mit $r = |w|$ und $\varphi \in]-\pi, \pi[$. Dann gilt (wegen $\cos x > 0$ für $x \in]-\frac{\pi}{2}, \frac{\pi}{2}[$)

$$\operatorname{Re} \sqrt{re^{i\frac{\varphi}{2}}} = \sqrt{r} \cdot \cos\left(\frac{\varphi}{2}\right) > 0 \quad \text{und} \quad \left(\sqrt{re^{\frac{\varphi}{2}}}\right)^2 = re^{i\varphi} = w.$$

Zu guter Letzt fehlt nur noch eine Drehung um 90° im Uhrzeigersinn. Dies bewerkstelligt die Abbildung

$$h : \mathbb{C} \setminus]-\infty, 0] \rightarrow \mathbb{C} \setminus \{iy \mid y \geq 0\}, \quad z \mapsto -iz.$$

Für diese ist die Biholomorphie klar.

Insgesamt erhalten wir die gesuchte Abbildung durch $\psi = h \circ g \circ f$. Explizit gilt

$$\psi : \mathbb{E} \rightarrow G, \quad z \mapsto -i \left(\frac{z-1}{z+1} \right)^2.$$

Die inverse Abbildung $G \rightarrow \mathbb{E}$ erhält man durch Berechnung von $f^{-1} \circ g^{-1} \circ h^{-1}$:

$$\varphi(z) = f^{-1}(g^{-1}(h^{-1}(z))) = f^{-1}(g^{-1}(iz)) = f^{-1}(\sqrt{iz}) = \frac{\sqrt{iz} + 1}{-\sqrt{iz} + 1}$$

- b** Eine solche Abbildung existiert nicht. Wir haben bereits bemerkt, dass G einfach zusammenhängend ist, also auch das Bild von G unter einerbiholomorphen Abbildung einfach zusammenhängend sein muss. Wir zeigen, dass dies für $\{w \in \mathbb{C} \mid |z| > 1\}$ nicht der Fall ist. Hierzu lässt sich beispielsweise bemerken, dass das Komplement $\mathbb{C} \setminus \{w \in \mathbb{C} \mid |z| > 1\} = \overline{\mathbb{E}}$ beschränkt ist.

7. Analysis: Differentialgleichungen

Definition 7.1. Seien $n, m \in \mathbb{N}$ natürliche Zahlen, $D \subseteq \mathbb{R} \times \mathbb{R}^{nm}$ eine Menge und $f: D \rightarrow \mathbb{R}^m$ eine Funktion. Eine Gleichung der Form

$$x^{(n)} = f(t, x, x', \dots, x^{(n-1)})$$

heißt m -dimensionale *explizite gewöhnliche Differentialgleichung* n -ter Ordnung. Eine Lösung dieser Gleichung ist eine n -mal differenzierbare Funktion $\lambda: I \rightarrow \mathbb{R}^m$ mit einem Intervall $I \subseteq \mathbb{R}$, die $(t, \lambda(t), \lambda'(t), \dots, \lambda^{(n-1)}(t)) \in D$ und

$$f\left(t, \lambda(t), \lambda'(t), \dots, \lambda^{(n-1)}(t)\right) = \lambda^{(n)}(t) \quad \text{für alle } t \in I \text{ erfüllt.}$$

Wird neben der eigentlichen Differentialgleichnung noch gefordert, dass

$$x(t_0) = x_0, \dots, x'(t_0) = x_1, \dots, x^{(n-1)}(t_0) = x_{n-1}$$

für Werte $(t_0, x_0, \dots, x_{n-1}) \in D$ erfüllt sein soll, so spricht man von einem *Anfangswertproblem*. Eine Lösung $\lambda: I \rightarrow \mathbb{R}^m$ muss dann noch $t_0 \in I$ und $\lambda^{(k)}(t_0) = x_k$ für $k \in \{0, \dots, n-1\}$ erfüllen.

Ein wichtiger Spezialfall dieser Definition sind Gleichungen, bei denen die Funktion f nicht von t abhängt. Solche Gleichungen bezeichnet man als *autonom*.

7.1. Elementare Lösungsmethoden skalarer Differentialgleichungen

Wir beschreiben in diesem Abschnitt gängige Methoden, skalare Differentialgleichungen zu lösen. Leider werden sehr selten Aufgaben gestellt, die sich auf das reine Lösen beschränken, weshalb wir etwas im Stoff vorgreifen müssen und Sätze über die Existenz und Eindeutigkeit solcher Lösungen anwenden werden.

Differentialgleichungen mit getrennten Variablen

Satz 7.2 (Trennen der Variablen). Seien $I, J \subseteq \mathbb{R}$ offene Intervalle, $t_0 \in I$, $x_0 \in J$ und $g: I \rightarrow \mathbb{R}$ sowie $h: J \rightarrow \mathbb{R}$ stetig. Dann hat das Anfangswertproblem

$$x' = g(t)h(x), \quad x(t_0) = x_0$$

- (1) im Fall $h(x_0) = 0$ zumindest die konstante Lösung $\lambda: I \rightarrow \mathbb{R}$, $t \mapsto x_0$.
- (2) im Fall $h(x_0) \neq 0$ lokal eine eindeutige Lösung, d. h. es gibt ein offenes Intervall $I' \subseteq I$ mit $t_0 \in I'$, sodass es auf I' eine eindeutige Lösung λ gibt. Diese lässt sich durch Auflösen von

$$\int_{x_0}^{\lambda(t)} \frac{1}{h(x)} dx = \int_{t_0}^t g(\tau) d\tau$$

nach $\lambda(t)$ bestimmen.

Aufgabe (Herbst 2013, T3A1)

Gegeben sei die parameterabhängige Differentialgleichung

$$\dot{x} = x^\alpha \quad \text{mit} \quad x(0) = 1.$$

Bestimmen Sie die maximalen Lösungen dieser Differentialgleichung für $\alpha = 1$ und $\alpha = 2$.

Lösungsvorschlag zur Aufgabe (Herbst 2013, T3A1)

Wir bestimmen zunächst eine Lösung λ zum Parameter $\alpha = 1$ mittels Trennen der Variablen:

$$\int_1^{\lambda(t)} \frac{1}{x} dx = \int_0^t 1 d\tau \quad \Leftrightarrow \quad \ln \lambda(t) = t \quad \Leftrightarrow \quad \lambda(t) = e^t.$$

Da diese Lösung bereits auf ganz \mathbb{R} definiert ist, kann sie nicht weiter fortgesetzt werden und ist deshalb maximal (Eindeutigkeit war nicht zu zeigen).

Ebenso verfahren wir im Fall $\alpha = 2$:

$$\int_1^{\mu(t)} \frac{1}{x^2} dx = \int_0^t 1 d\tau \quad \Leftrightarrow \quad -\frac{1}{\mu(t)} + 1 = t \quad \Leftrightarrow \quad \mu(t) = \frac{1}{1-t}.$$

Diese Lösung ist auf $\mathbb{R} \setminus \{1\}$ definiert. Da 0 im Definitionssintervall liegen soll, wählen wir $I =]-\infty, 1[$ als solches. Da die untere Grenze dieses Intervalls

$-\infty$ ist und

$$\lim_{t \rightarrow 1^-} |\mu(t)| = \infty$$

gilt, handelt es sich bei $\mu: I \rightarrow \mathbb{R}$ um die maximale Lösung des obigen Anfangswertproblems (vgl. Satz 7.13).

Aufgabe (Herbst 2013, T2A4)

Betrachten Sie die Differentialgleichung

$$y' = t^2 \sqrt{1 + 2y}.$$

- a Geben Sie die Lösung der zugehörigen Anfangswertaufgabe mit Anfangswert $y(0) = 0$ auf dem Intervall $[0, \infty)$ an. Warum ist sie dort eindeutig?
- b Betrachten Sie die o. g. Differentialgleichung zum Anfangswert $y(0) = -1/2$. Geben Sie zwei verschiedene Lösungen dieser Anfangswertaufgabe explizit an.

Lösungsvorschlag zur Aufgabe (Herbst 2013, T2A4)

- a Wir lösen das Anfangswertproblem mittels Trennen der Variablen:

$$\begin{aligned} \int_0^{\lambda(t)} \frac{1}{\sqrt{1+2y}} dy &= \int_0^t \tau^2 d\tau \quad \Leftrightarrow \quad \left[\sqrt{1+2y} \right]_0^{\lambda(t)} = \left[\frac{1}{3}\tau^3 \right]_0^t \\ \Leftrightarrow \quad \sqrt{1+2\lambda(t)} - 1 &= \frac{1}{3}t^3 \quad \Leftrightarrow \quad \lambda(t) = \frac{1}{2} \left(\left(\frac{1}{3}t^3 + 1 \right)^2 - 1 \right). \end{aligned}$$

Wir überprüfen durch Einsetzen in die Gleichung, ob wir tatsächlich eine Lösung gefunden haben. Für $t \in [0, \infty[$ gilt

$$\begin{aligned} t^2 \sqrt{1+2\lambda(t)} &= t^2 \sqrt{1+\left(\frac{1}{3}t^3+1\right)^2-1} = t^2 \cdot \left(\frac{1}{3}t^3+1\right) = \\ &= \left(\left(\frac{1}{3}t^3+1\right) \cdot t^2\right) = \lambda'(t). \end{aligned}$$

Die Lösung ist auf $[0, \infty[$ definiert und dort eindeutig, denn die partielle Ableitung der rechten Seite der Differentialgleichung nach y ist

$$\partial_y t^2 \sqrt{1+2y} = \frac{t^2}{\sqrt{1+2y}}.$$

Diese existiert auf dem Intervall $] -\frac{1}{2}, \infty[$ und ist dort stetig, sodass die rechte Seite der Gleichung dort nach Proposition 7.10 lokal Lipschitz-stetig

bezüglich y ist. Also genügt die Differentialgleichung den Voraussetzungen des Globalen Existenz- und Eindeutigkeitssatzes 7.12, sodass es insbesondere auf $[0, \infty[$ eine eindeutige maximale Lösung gibt. Da λ auf diesem Intervall definiert ist, muss es sich bei λ um diese eindeutige maximale Lösung handeln.

- b** Wiederum bestimmen wir eine Lösung mittels Trennen der Variablen:

$$\int_{-\frac{1}{2}}^{\lambda(t)} \frac{1}{\sqrt{1+2y}} dy = \int_0^t \tau^2 d\tau \Leftrightarrow \sqrt{1+2\lambda(t)} = \frac{1}{3}t^3$$

$$\Leftrightarrow \lambda(t) = \frac{1}{2}\left(\frac{1}{9}t^6 - 1\right)$$

Wir überprüfen kurz, ob wir auch tatsächlich eine Lösung gefunden haben:

$$t^2 \sqrt{1+2\lambda(t)} = t^2 \sqrt{1+\frac{1}{9}t^6 - 1} = t^2 \cdot \frac{1}{3}t^3 = \frac{1}{3}t^3 \cdot t^2 = \lambda'(t).$$

Da der zweite Faktor der rechten Seite der Differentialgleichung jedoch bei $y = -\frac{1}{2}$ verschwindet, gibt es eine weitere Lösung zum Anfangswert $y(0) = -\frac{1}{2}$, nämlich

$$\mu: \mathbb{R} \rightarrow \mathbb{R}, \quad t \mapsto -\frac{1}{2}.$$

Aufgabe (Frühjahr 2015, T3A1)

Seien $f, g: \mathbb{R} \rightarrow \mathbb{R}$ stetig. Wir betrachten das Anfangswertproblem

$$\dot{x}(t) = g(t)f(x(t)), \quad x(t_0) = x_0, \tag{1}$$

wobei $t_0, x_0 \in \mathbb{R}$.

- a** Geben Sie ein Beispiel eines Anfangswertproblems der Form (1) an, sowie ein zugehöriges Intervall, so dass es zwei verschiedene Lösungen besitzt.
b Wir nehmen nun zusätzlich an, dass $f, g: \mathbb{R} \rightarrow (0, \infty)$. Zeigen Sie, dass das Problem (1) dann lokal eindeutig lösbar ist.

Hinweis Es sind hier Existenz und Eindeutigkeit zu zeigen.

Lösungsvorschlag zur Aufgabe (Frühjahr 2015, T3A1)

- a** Etwas vorausschauend auf den Globalen Existenz- und Eindeutigkeitssatz 7.12 wissen wir, dass Funktionen zu wählen sind, sodass die rechte Seite nicht lokal Lipschitz-stetig ist.

Wir wählen daher $g: \mathbb{R} \rightarrow \mathbb{R}, t \mapsto 1$ sowie $f: \mathbb{R} \rightarrow \mathbb{R}, x \mapsto \sqrt{|x|}$ und

betrachten das Anfangswertproblem

$$\dot{x}(t) = \sqrt{|x(t)|}, \quad x(0) = 0.$$

Eine erste Lösung bekommen wir mit $\lambda_1: \mathbb{R} \rightarrow \mathbb{R}, t \mapsto 0$, eine andere bestimmen wir mittels Trennen der Variablen:

$$\int_0^{\lambda_2(t)} \frac{1}{\sqrt{|x|}} dx = \int_0^t 1 d\tau \Leftrightarrow \pm 2\sqrt{|\lambda_2(t)|} = t \Leftrightarrow \lambda_2(t) = \pm \frac{1}{4}t^2$$

Dabei haben wir für die erste Äquivalenz das Integral

$$\int_0^y \frac{1}{\sqrt{|x|}} dx = \pm 2\sqrt{|y|} = \begin{cases} 2\sqrt{y} & \text{falls } y \geq 0, \\ -2\sqrt{-y} & \text{falls } y < 0 \end{cases}$$

verwendet. Dies liefert eine weitere Lösung

$$\lambda_2: \mathbb{R} \rightarrow \mathbb{R}, \quad t \mapsto \begin{cases} \frac{1}{4}t^2 & \text{für } t \geq 0 \\ -\frac{1}{4}t^2 & \text{für } t \leq 0. \end{cases}$$

Wir überprüfen noch, dass λ in 0 tatsächlich differenzierbar ist:

$$\lim_{\omega \rightarrow 0} \frac{\lambda(\omega) - \lambda(0)}{\omega} = \lim_{\omega \rightarrow 0} \frac{\operatorname{sgn}(\omega) \frac{1}{4}\omega^2}{\operatorname{sgn}(\omega)|\omega|} = \lim_{\omega \rightarrow 0} \frac{1}{4}|\omega| = 0.$$

Man kann nun die Ableitung als $\lambda'(x) = \frac{1}{2}|x|$ schreiben, somit ist auch

$$\sqrt{|\lambda(x)|} = \sqrt{\frac{1}{4}x^2} = \frac{1}{2}|x| = \lambda'(x)$$

für alle $x \in U$ wie erwünscht erfüllt.

b Hierzu müssen wir Satz 7.2 (2) (teilweise) beweisen. Definiere dazu

$$G: \mathbb{R} \rightarrow \mathbb{R}, \quad t \mapsto \int_{t_0}^t g(\tau) d\tau \quad \text{und} \quad F: \mathbb{R} \rightarrow \mathbb{R}, \quad x \mapsto \int_{x_0}^x \frac{1}{f(\omega)} d\omega.$$

Wegen $F'(x) = \frac{1}{f(x)} > 0$ für alle $x \in \mathbb{R}$ ist F auf ganz \mathbb{R} streng monoton steigend, deshalb injektiv und auf ganz \mathbb{R} umkehrbar. Sei $V = F(\mathbb{R})$, dann existiert also die Umkehrabbildung $F^{-1}: V \rightarrow \mathbb{R}$ und ist stetig differenzierbar. Wegen $0 \in G(\mathbb{R}) \cap F(\mathbb{R})$ ist $G^{-1}(V) \neq \emptyset$ und offen, sodass wir ein Intervall $I \subseteq G^{-1}(V)$ wählen können. Definiere nun

$$\lambda: I \rightarrow \mathbb{R}, \quad t \mapsto F^{-1}(G(t)),$$

dann ist λ stetig differenzierbar und unter Verwendung der Umkehrregel bekommt man

$$\lambda'(t) = (F^{-1})'(G(t)) \cdot G'(t) = \frac{1}{F'(F^{-1}(G(t)))} g(t) = g(t) \cdot f(\lambda(t)),$$

sowie $\lambda(t_0) = F^{-1}(G(t_0)) = F^{-1}(0) = x_0$, d. h. λ ist eine Lösung von (1). Diese Lösung ist eindeutig auf I , denn ist $\mu: I \rightarrow \mathbb{R}$ eine weitere Lösung von (1), so folgt mit Substitution:

$$G(t) = \int_{t_0}^t g(\tau) d\tau = \int_{t_0}^t \frac{\mu'(\tau)}{f(\mu(\tau))} d\tau = \int_{x_0}^{\mu(t)} \frac{1}{f(\omega)} d\omega = F(\mu(t)).$$

Weil F auf seinem gesamten Definitionsbereich umkehrbar ist, bedeutet das

$$\mu(t) = F^{-1}(G(t)) = \lambda(t).$$

Exakte Differentialgleichungen

Definition 7.3. Sei $G \subseteq \mathbb{R}^2$ ein Gebiet und $f, g: G \rightarrow \mathbb{R}$ stetig. Die Differentialgleichung

$$f(t, x) + g(t, x)x' = 0$$

heißt *exakt*, falls es eine stetig differenzierbare Funktion $F: G \rightarrow \mathbb{R}$ gibt, sodass

$$\partial_t F(t, x) = f(t, x) \quad \text{und} \quad \partial_x F(t, x) = g(t, x)$$

für alle $(t, x) \in G$ erfüllt ist. Eine solche Funktion F heißt *Stammfunktion* der Differentialgleichung.

Man sieht einer Differentialgleichung meist nicht an, ob sie exakt ist. Glücklicherweise gibt uns die nächste Proposition dafür ein praktikables Kriterium an die Hand.

Proposition 7.4 (Exaktheitstest). Sei $G \subseteq \mathbb{R}^2$ ein einfach zusammenhängendes Gebiet und seien $f, g: G \rightarrow \mathbb{R}$ stetig differenzierbar. Die Differentialgleichung

$$f(t, x) + g(t, x)x' = 0$$

ist genau dann exakt auf G , wenn die *Integrabilitätsbedingung*

$$\partial_x f(t, x) = \partial_t g(t, x)$$

für alle $(t, x) \in G$ erfüllt ist.

Lässt man in 7.4 die Forderung fallen, dass G einfach zusammenhängend ist, so liefert die Integrierbarkeitsbedingung zumindest noch eine notwendige Bedingung. Existiert nämlich eine Stammfunktion F , so gilt nach dem Satz von Schwarz

$$\partial_x f(t, x) = \partial_x(\partial_t F(t, x)) = \partial_t(\partial_x F(t, x)) = \partial_t g(t, x).$$

Aus dem nächsten Satz geht hervor, auf welche Weise sich die Lösung einer exakten Differentialgleichung aus ihrer Stammfunktion bestimmen lässt.

Satz 7.5 (Bedeutung einer Stammfunktion für die Lösungsbestimmung). Sei $G \subseteq \mathbb{R}^2$ ein Gebiet, $I \subseteq \mathbb{R}$ ein (nicht-leeres) Intervall, $f: G \rightarrow \mathbb{R}$ und $g: G \rightarrow \mathbb{R}$ stetig. Für eine exakte Differentialgleichung

$$f(t, x) + g(t, x)x' = 0$$

mit Stammfunktion F sind äquivalent:

- (1) $\lambda: I \rightarrow \mathbb{R}$ ist eine Lösung dieser Differentialgleichung,
- (2) $\lambda: I \rightarrow \mathbb{R}$ ist eine stetig differenzierbare Funktion mit $(t, \lambda(t)) \in G$ und für alle $t \in I$ ist $F(t, \lambda(t))$ konstant.

Anleitung: Lösungsverfahren für exakte Differentialgleichungen

Sei $G \subseteq \mathbb{R}^2$ ein einfach zusammenhängendes Gebiet, $f, g: G \rightarrow \mathbb{R}$ stetig differenzierbar und $(\tau, \xi) \in G$. Wir betrachten das Anfangswertproblem

$$f(t, x) + g(t, x)x' = 0, \quad x(\tau) = \xi.$$

- (1) Prüfe mittels Proposition 7.4, ob die Differentialgleichung exakt ist.
- (2) Bestimmung einer Stammfunktion:
 - (i) Sei $(x_0, t_0) \in G$ Integration liefert

$$\int_{t_0}^t f(\tau) d\tau = F(t, x) - F(t_0, x) \quad \text{und} \quad \int_{x_0}^x g(\omega) d\omega = F(t, x) - F(t, x_0).$$

- (ii) Werte die erste Gleichung bei x_0 aus und setze in die zweite ein, oder werte die zweite Gleichung bei t_0 aus und setze anschließend in die erste ein.
- (iii) Die Konstante $F(t_0, x_0)$ kann frei gewählt werden, denn sie verändert die relevanten Eigenschaften der Stammfunktion nicht.

- (3) Löse nun

$$F(t, \lambda(t)) = F(\tau, \xi)$$

nach der Funktion $\lambda(t)$ auf und bestimme ihren Definitionsbereich. Nach Satz 7.5 ist λ dann eine Lösung des Anfangswertproblems.

Leider sind die meisten Differentialgleichungen nicht exakt. Man kann jedoch versuchen, sie „exakt zu machen“.

Definition 7.6. Sei $G \subseteq \mathbb{R}^2$ ein Gebiet und seien $f, g: G \rightarrow \mathbb{R}$ stetig partiell differenzierbar. Gibt es für die Differentialgleichung

$$f(t, x) + g(t, x)x' = 0$$

eine stetig differenzierbare Funktion $m: G \rightarrow \mathbb{R} \setminus \{0\}$, sodass die Gleichung

$$m(t, x)f(t, x) + m(t, x)g(t, x)x' = 0$$

exakt ist, so heißt m ein *integrierender Faktor* oder *Euler'scher Multiplikator* dieser Differentialgleichung.

Da ein integrierender Faktor nach Definition nie den Wert 0 annimmt, ist eine Funktion genau dann eine Lösung der ursprünglichen Differentialgleichung, wenn sie eine der neuen exakten ist. Es stellt sich nun die Frage, wann und wie man einen solchen integrierenden Faktor findet. Leider können wir dazu kein allgemein gültiges Rezept anbieten, sondern nur eine Vorgehensweise skizzieren, die in den meisten Fällen zum Ziel führt.

Sei G ein einfach zusammenhängendes Gebiet. Nach Proposition 7.4 ist $m(t, x)$ genau dann ein integrierender Faktor, wenn

$$\partial_x(m(t, x)f(t, x)) = \partial_t(m(t, x)g(t, x))$$

erfüllt ist. Nach der Produktregel ist diese Gleichung äquivalent zu

$$\begin{aligned} \partial_x m(t, x)f(t, x) + m(t, x)\partial_x f(t, x) &= \partial_t m(t, x)g(t, x) + m(t, x)\partial_t g(t, x) \\ \Leftrightarrow g(t, x)\partial_t m(t, x) - f(t, x)\partial_x m(t, x) &= m(t, x)[\partial_x f(t, x) - \partial_t g(t, x)]. \end{aligned}$$

Macht man den Ansatz $m = M(u)$, dass die Funktion m also als Verkettung zweier anderer Funktionen $u: G \rightarrow D \subseteq \mathbb{R}$ und $M: D \rightarrow \mathbb{R}$ entsteht, so wird diese Gleichung unter Verwendung der Kettenregel zu

$$\begin{aligned} g(t, x)M'(u)\partial_t u - f(t, x)M'(u)\partial_x u &= M(u)[\partial_x f(t, x) - \partial_t g(t, x)] \\ \Leftrightarrow \frac{M'(u)}{M(u)} &= \frac{\partial_x f(t, x) - \partial_t g(t, x)}{g(t, x)\partial_t u - f(t, x)\partial_x u} \end{aligned}$$

Falls man Glück hat und die rechte Seite nur von u abhängt, so ist dies eine Differentialgleichung für M mit getrennten Variablen, die sich lösen lässt. Wir beschreiben die Vorgehensweise nochmals konkret:

Anleitung: Bestimmung eines integrierenden Faktors

Sei $G \subseteq \mathbb{R}^2$ ein einfach zusammenhängendes Gebiet und seien $f, g: G \rightarrow \mathbb{R}$ stetig partiell differenzierbar. Gesucht ist ein integrierender Faktor $m(t, x)$ von

$$f(t, x) + g(t, x)x' = 0.$$

- (1) Wähle eine Funktion $u(t, x)$ und berechne

$$H(t, x) = \frac{\partial_x f(t, x) - \partial_t g(t, x)}{g(t, x)\partial_t u(t, x) - f(t, x)\partial_x u(t, x)}.$$

Gängige Ansätze für $u(t, x)$ sind

$$u(t, x) = t, \quad u(t, x) = x, \quad u(t, x) = t \pm x, \quad u(t, x) = tx.$$

- (2) Falls $H(t, x)$ für den gewählten Ansatz für u eine Funktion ausschließlich in u ist, so berechne $M(u) = e^{\int H(u)du}$. Es ist dann durch

$$m(t, x) = M(u(t, x))$$

ein integrierender Faktor obiger Differentialgleichung gegeben.

Aufgabe (Frühjahr 2011, T2A4)

Gegeben sei die Differentialgleichung

$$e^{-t}(t+x) - e^{-t}(x-t)x' = 0.$$

- a** Untersuchen Sie, ob die Differentialgleichung exakt ist oder ob wenigstens ein integrierender Faktor existiert
- b** Bestimmen Sie jeweils die maximal fortgesetzte Lösung der Differentialgleichung, die der folgenden Anfangsbedingung genügt:
 - (i) $x(1) = 0$
 - (ii) $x(-1) = 1$

Lösungsvorschlag zur Aufgabe (Frühjahr 2011, T2A4)

- a** Die Differentialgleichung ist auf dem einfach zusammenhängenden Gebiet \mathbb{R}^2 definiert. Wir überprüfen die Integrabilitätsbedingung:

$$\partial_x(e^{-t}(t+x)) = e^{-t} \neq e^{-t}(x-t) + e^{-t} = \partial_t(-e^{-t}(x-t)).$$

Damit ist die Differentialgleichung nach Proposition 7.4 nicht exakt. Wir versuchen nun, einen integrierenden Faktor mit dem oben beschriebenen Verfahren zu finden und machen dazu den Ansatz $u(t, x) = t$. Es ist dann

$$H(t, x) = \frac{e^{-t} - e^{-t}(x-t) - e^{-t}}{-e^{-t}(x-t)} = \frac{-e^{-t}(x-t)}{-e^{-t}(x-t)} = 1$$

eine konstante Funktion in u . Wir berechnen daher

$$M(u) = e^{\int 1 \mathrm{d}u} = e^u \quad \text{sowie} \quad m(t, x) = M(u(t, x)) = e^t$$

und erhalten nach Multiplikation mit $m(t, x)$ die neue Gleichung

$$(t+x) - (x-t)x' = 0. \quad (\star)$$

Die Integrabilitätsbedingung zeigt, dass diese tatsächlich exakt ist.

- b** Um eine Stammfunktion für (\star) zu bestimmen, berechnen wir

$$\begin{aligned} F(t, x) &= F(0, x) + \int_0^t (\tau + x) \mathrm{d}\tau = F(0, x) + \frac{1}{2}t^2 + xt \\ F(t, x) &= F(t, 0) + \int_0^x (-\omega + t) \mathrm{d}\omega = F(t, 0) - \frac{1}{2}x^2 + tx. \end{aligned}$$

Aus der ersten Gleichung erhält man $F(t, 0) = F(0, 0) + \frac{1}{2}t^2$ und Einsetzen in die zweite liefert:

$$F(t, x) = F(0, 0) + \frac{1}{2}t^2 - \frac{1}{2}x^2 + tx$$

Wir setzen der Einfachheit wegen $F(0, 0) = 0$.

(i): Wir suchen eine Funktion λ , für die

$$\begin{aligned} F(t, \lambda(t)) &= F(1, 0) \Leftrightarrow \frac{1}{2}t^2 + t\lambda(t) - \frac{1}{2}\lambda(t)^2 = \frac{1}{2} \\ &\Leftrightarrow -\lambda(t)^2 + 2t\lambda(t) + t^2 - 1 = 0 \end{aligned}$$

gilt. Die Mittelnachtsformel liefert

$$\lambda(t) = t \pm \sqrt{2t^2 - 1}$$

und aus der Bedingung $\lambda(1) = 0$ folgt, dass $\lambda(t) = t - \sqrt{2t^2 - 1}$ sein muss. Diese Funktion ist auf dem Intervall $I =]\frac{1}{2}\sqrt{2}, +\infty[$ stetig differenzierbar, also ist nach Satz 7.5 durch

$$\lambda: I \rightarrow \mathbb{R}, \quad t \mapsto t - \sqrt{2t^2 - 1}$$

eine Lösung gegeben. Wegen

$$\lim_{t \searrow \frac{1}{2}\sqrt{2}} \lambda'(t) = \lim_{t \searrow \frac{1}{2}\sqrt{2}} 1 - \frac{2t}{\sqrt{2t^2 - 1}} = -\infty$$

lässt sich diese nicht stetig differenzierbar fortsetzen.

(ii): Wiederum fordern wir für eine Lösung μ , dass

$$\begin{aligned} F(t, \mu(t)) = F(-1, 1) &\Leftrightarrow \frac{1}{2}t^2 + t\mu(t) - \frac{1}{2}\mu(t)^2 = \frac{1}{2} - 1 - \frac{1}{2} \\ &\Leftrightarrow -\mu(t)^2 + 2t\mu(t) + t^2 + 2 = 0 \end{aligned}$$

und bekommen aus der Mitternachtsformel, dass

$$\mu(t) = t \pm \sqrt{2t^2 + 2}.$$

Wegen $\mu(-1) = 1$ muss $\mu(t) = t + \sqrt{2t^2 + 2}$ sein und nach Satz 7.5 handelt es sich bei $\mu: \mathbb{R} \rightarrow \mathbb{R}, t \mapsto t + \sqrt{2t^2 + 2}$ um eine Lösung der Differentialgleichung, die auf ganz \mathbb{R} definiert, also auch maximal fortgesetzt ist.

Aufgabe (Frühjahr 2015, T1A4)

Bestimmen Sie eine reelle Lösung $y: I \rightarrow \mathbb{R}$ des Anfangswertproblems

$$y(x)y'(x) + y(x)^2 + 2x + 5 = 0, \quad y(-4) = -2.$$

Wie groß kann das Intervall I maximal gewählt werden?

Hinweis Eine Möglichkeit der Lösung besteht darin, zunächst einen integrierenden Faktor $m: \mathbb{R} \rightarrow]0; \infty[$ zu bestimmen, welcher nur von der Variablen x abhängt. Wir bezeichnen hierbei m als integrierenden Faktor, wenn die Differentialgleichung nach Multiplikation mit m exakt wird.

Lösungsvorschlag zur Aufgabe (Frühjahr 2015, T1A4)

Nachdem man geprüft hat, dass die Differentialgleichung nicht exakt ist, folgen wir dem oben beschriebenen Verfahren und machen den Ansatz $u(x, y) = x$. Dann ist

$$H(x, y) = \frac{2y - 0}{y} = 2$$

eine konstante Funktion in u . Integration liefert

$$M(u) = e^{\int 2 \mathrm{d}u} = e^{2u}.$$

Wir multiplizieren die Gleichung also mit

$$m(x, y)M(u(x, y)) = e^{2x}$$

und erhalten

$$e^{2x}y(x)y'(x) + e^{2x} \left(y(x)^2 + 2x + 5 \right) = 0$$

Diese Differentialgleichung ist exakt, denn

$$\partial_y(e^{2x}(y^2 + 2x + 5)) = e^{2x} \cdot (2y) = 2e^{2x} \cdot y = \partial_x(e^{2x}y)$$

Als Nächstes bestimmen wir eine Stammfunktion der Differentialgleichung. Dazu berechnen wir

$$\begin{aligned} F(x, y) &= F(0, y) + \int_0^x e^{2\tau}(y^2 + 2\tau + 5) \mathrm{d}\tau = \\ &= F(0, y) + \frac{1}{2}e^{2x}(y^2 + 5) - \frac{1}{2}(y^2 + 5) + e^{2x}x - \frac{1}{2}e^{2x} + \frac{1}{2}, \\ F(x, y) &= F(x, 0) + \int_0^y e^{2x}w \mathrm{d}w = F(x, 0) + \frac{1}{2}y^2e^{2x}, \end{aligned}$$

wobei wir partielle Integration für die Berechnung von

$$\int 2xe^{2x} \mathrm{d}x = e^{2x}x - \int e^{2x} \mathrm{d}x = e^{2x}x - \frac{1}{2}e^{2x}$$

verwendet haben. Die zweite Gleichung gibt $F(0, y) = F(0, 0) + \frac{1}{2}y^2$ und eingesetzt haben wir:

$$F(x, y) = F(0, 0) + \frac{1}{2}e^{2x}(y^2 + 2x + 4) + 3.$$

Wir setzen $F(0, 0) = -3$, dann bekommen wir

$$F(x, y) = \frac{1}{2}e^{2x}(y^2 + 2x + 4)$$

als Stammfunktion obiger Differentialgleichung. Wir suchen nun ein maximales Intervall $I \subseteq \mathbb{R}$ und eine Funktion $\lambda: I \rightarrow \mathbb{R}$, sodass

$$\begin{aligned} F(x, \lambda(x)) = F(-4, -2) &\Leftrightarrow \frac{1}{2}e^{2x}(\lambda(x)^2 + 2x + 4) = \frac{1}{2}e^{-8}(4 + (-8) + 4) = 0 \\ &\Leftrightarrow \lambda(x)^2 + 2x + 4 = 0 \Leftrightarrow \lambda(x) = \pm\sqrt{-2x - 4}. \end{aligned}$$

Aus der Anfangswertbedingung $\lambda(-4) = -2$ folgt, dass $\lambda(x) = -\sqrt{-2(x+2)}$ sein muss. Das maximale Existenzintervall dieser Lösung ist $I =]-\infty, -2[$, denn die linke Seite ist bereits unendlich und wie oben zeigt man, dass der Grenzwert $\lim_{x \rightarrow -2} \lambda'(x)$ nicht existiert.

Variation der Konstanten

Betrachte das Anfangswertproblem

$$x'(t) = a(t)x(t) + b(t), \quad x(\tau) = \xi,$$

wobei I ein offenes Intervall mit $\tau \in I$, $\xi \in \mathbb{R}$ und $a, b: I \rightarrow \mathbb{R}$ stetige Abbildungen sind. Im Fall, dass $b(t) = 0$ für alle $t \in I$ gilt, spricht man von einer *homogenen* linearen Differentialgleichung und verifiziert durch direktes Nachrechnen, dass

$$\lambda_h(t) = \xi e^{\int_{\tau}^t a(s)ds}$$

eine auf I definierte Lösung des Problems ist. Um die inhomogene Differentialgleichung zu lösen, verwendet man die Lösungsmethode der **Variation der Konstanten**, d.h. man macht den Ansatz $\lambda(t) = c(t)\lambda_h(t)$ für eine Funktion $c(t)$ mit $c(\tau) = 1$. Einsetzen in die Differentialgleichung ergibt

$$c'(t)\xi e^{\int_{\tau}^t a(s)ds} + c(t)\xi e^{\int_{\tau}^t a(s)ds}a(t) = a(t)c(t)\xi e^{\int_{\tau}^t a(s)ds} + b(t)$$

und Auflösen liefert

$$c'(t)e^{\int_{\tau}^t a(s)ds}\xi = b(t) \Leftrightarrow \xi c'(t) = b(t)e^{-\int_{\tau}^t a(s)ds}.$$

Die zugehörige Integralgleichung lautet unter Berücksichtigung von $c(\tau) = 1$:

$$\xi c(t) = \xi + \int_{\tau}^t e^{-\int_r^t a(r)dr} b(s)ds.$$

Eine Lösung des Anfangswertproblems ist daher

$$\lambda: I \rightarrow \mathbb{R}, \quad t \mapsto e^{\int_{\tau}^t a(s)ds}\xi + e^{\int_{\tau}^t a(s)ds} \int_{\tau}^t e^{-\int_r^s a(r)dr} b(s)ds.$$

Variableentransformation

Manchmal lassen sich Differentialgleichungen, die sich mit den bisher besprochenen Verfahren nicht lösen lassen, durch eine Transformation in eine lösbarer Form bringen. Dazu führt man eine neue Variable ein und drückt die Differentialgleichung in der neuen Variable aus. Anstelle einer theoretischen Formulierung erläutern wir lediglich die pragmatische Vorgehensweise.

Anleitung: Variableentransformation

Gegeben sei ein Anfangswertproblem der Form

$$x' = f(t, x), \quad x(t_0) = x_0.$$

- (1) Führe eine neue Variable $u(t)$ ein. Bestimme ihre Ableitung, setze dann $x'(t) = f(t, x)$ ein und drücke die rechte Seite durch $u(t)$ aus. Bestimme zudem den neuen Anfangswert $u(t_0)$.
- (2) Bestimme eine Lösung μ des so erhaltenen Anfangswertproblems.
- (3) Eine Lösung λ der ursprünglichen Gleichung erhält man durch Rücktransformation, also durch Auflösen der Gleichung für $u(t)$ nach $x(t) = \lambda(t)$.
- (4) Überprüfe, dass λ eine Lösung der ursprünglichen Differentialgleichung $x' = f(t, x)$ ist, und bestimme das Existenzintervall.

Beispiele 7.7. **a** *Homogene Differentialgleichungen:* Gilt für die Differentialgleichung $x' = f(t, x)$ die Gleichung $f(\sigma t, \sigma x) = f(t, x)$ für $\sigma \in \mathbb{R}^\times$, so ergibt die Substitution $y = \frac{x}{t}$ die Differentialgleichung

$$y' = \frac{f(1, y) - y}{t},$$

die sich mittels Trennen der Variablen lösen lässt.

- b** Eine Differentialgleichung der Form $x' = g(\alpha t + \beta x + \gamma)$ lässt sich mithilfe der Substitution $y = \alpha t + \beta x + \gamma$ zu

$$y' = \alpha + \beta g(y)$$

transformieren. ■

Aufgabe (Herbst 2008, T1A4)

Lösen Sie die folgenden Anfangswertprobleme und geben Sie jeweils den maximalen Definitionsbereich der Lösung an:

a $y' = \frac{y^2 - t^2}{2ty}$, $y\left(\frac{1}{2}\right) = \frac{1}{2}$, **b** $y' - \frac{t}{t^2 - 1}y = \sqrt{t^2 - 1}$, $y(\sqrt{2}) = \sqrt{2}$.

Lösungsvorschlag zur Aufgabe (Herbst 2008, T1A4)

a Wir bemerken, dass die Differentialgleichung wegen

$$\frac{(\sigma y)^2 - (\sigma t)^2}{2(\sigma t)(\sigma y)} = \frac{\sigma^2(y^2 - t^2)}{\sigma^2(2yt)} = \frac{y^2 - t^2}{2yt}$$

für $\sigma \neq 0$ homogen ist. Wir führen deshalb die Substitution $u(t) = \frac{y(t)}{t}$ durch und erhalten die Differentialgleichung

$$\begin{aligned} u' &= \frac{y't - y}{t^2} = \frac{\frac{y^2 - t^2}{2y} - y}{t^2} = \frac{y^2 - t^2 - 2y^2}{2yt^2} = \\ &= \frac{-y^2 - t^2}{2yt^2} = -\frac{t^2(u^2 + 1)}{2yt^2} = -\frac{u^2 + 1}{2ut}. \end{aligned}$$

Der neue Startwert ist dann

$$u\left(\frac{1}{2}\right) = \frac{y\left(\frac{1}{2}\right)}{\frac{1}{2}} = 1.$$

Nun können wir eine Lösung der neuen Differentialgleichung durch Trennen der Variablen bestimmen:

$$\begin{aligned} \int_1^{\mu(t)} \frac{2u}{u^2 + 1} du &= - \int_{\frac{1}{2}}^t \frac{1}{\tau} d\tau \quad\Leftrightarrow\quad \ln(\mu(t)^2 + 1) - \ln 2 = -\ln t + \ln \frac{1}{2} \\ \Leftrightarrow \ln(\mu(t)^2 + 1) &= -\ln t \quad\Leftrightarrow\quad \mu(t)^2 + 1 = \frac{1}{t} \quad\Leftrightarrow\quad \mu(t) = \pm\sqrt{\frac{1}{t} - 1}. \end{aligned}$$

Aufgrund der Anfangsbedingung kommt nur die positive Lösung in Frage. Eine Lösung λ der ursprünglichen Differentialgleichung ergibt sich aus

$$\mu(t) = \frac{\lambda(t)}{t} \quad\Leftrightarrow\quad \lambda(t) = t\sqrt{\frac{1}{t} - 1}.$$

Die Lösung λ ist auf $]0, 1[$ definiert und wegen

$$\lim_{t \searrow 0} |\lambda(t)| = 0 \quad \text{und} \quad \lim_{t \nearrow 1} |\lambda(t)| = 0$$

ist diese auch maximal, denn sie kann auf beiden Seiten nicht stetig differenzierbar fortgesetzt werden (beachte den Definitionsbereich $\mathbb{R}^+ \times \mathbb{R}^+$).

- b** Wir bestimmen die Lösung mittels Variation der Konstanten. Dazu berechnen wir zunächst

$$\int_{\sqrt{2}}^t \frac{s}{s^2 - 1} ds = \left[\frac{1}{2} \ln(s^2 - 1) \right]_{\sqrt{2}}^t = \frac{1}{2} \ln(t^2 - 1) = \ln \sqrt{t^2 - 1}$$

und setzen dies nun in die Lösungsformel aus dem Abschnitt über Variation der Konstanten ein:

$$\begin{aligned} \lambda(t) &= e^{\ln \sqrt{t^2 - 1}} \sqrt{2} + e^{\ln \sqrt{t^2 - 1}} \int_{\sqrt{2}}^t e^{-\ln \sqrt{s^2 - 1}} \sqrt{s^2 - 1} ds = \\ &= \sqrt{t^2 - 1} \sqrt{2} + \sqrt{t^2 - 1} \int_{\sqrt{2}}^t \frac{1}{\sqrt{s^2 - 1}} \cdot \sqrt{s^2 - 1} ds = \\ &= \sqrt{t^2 - 1} \sqrt{2} + \sqrt{t^2 - 1} \int_{\sqrt{2}}^t 1 ds = \\ &= \sqrt{t^2 - 1} \sqrt{2} + (t - \sqrt{2}) \sqrt{t^2 - 1} = t \sqrt{t^2 - 1}. \end{aligned}$$

Diese Lösung ist auf $\mathbb{R} \setminus]-1, 1[$ definiert. Da das Lösungsintervall den Startwert $\sqrt{2}$ enthalten soll, wählen wir als Definitionsbereich $I =]1, \infty[$. Dabei handelt es sich auch schon um das maximale Existenzintervall, denn die rechte Grenze ist unendlich und an der linken ist die Differentialgleichung selbst ebenfalls nicht definiert.

7.2. Existenz- und Eindeutigkeitssätze

Hat man eine Differentialgleichung gelöst, so fragt man sich oft, ob es sich bei dieser Lösung um die einzige handelt. Ist man dagegen nicht in der Lage, eine Lösung anzugeben, so wäre von Interesse, ob es überhaupt eine Lösung gibt. Wir sind somit in der Existenz- und Eindeutigkeitstheorie gelandet.

Satz 7.8 (Peano). Sei $D \subseteq \mathbb{R}^{n+1}$ offen und $f: D \rightarrow \mathbb{R}^n$ eine stetige Funktion. Dann besitzt jedes Anfangswertproblem der Form

$$x' = f(t, x), \quad x(\tau) = \xi, \quad \text{für } (\tau, \xi) \in D$$

eine lokale Lösung, d. h. es gibt ein $\varepsilon > 0$, sodass das Anfangswertproblem auf dem Intervall $[\tau - \varepsilon, \tau + \varepsilon]$ mindestens eine Lösung besitzt.

Bereits im vorigen Abschnitt sind uns Differentialgleichungen begegnet, bei denen unter den Voraussetzungen des Satzes von Peano mehrere Lösungen existieren. (Gewöhnliche) Stetigkeit allein reicht als Bedingung daher nicht aus, um Eindeutigkeit zu erreichen. Wir benötigen daher einen stärkeren Begriff von Stetigkeit.

Definition 7.9. Sei $D \subseteq \mathbb{R} \times \mathbb{R}^n$ eine Teilmenge und $f: D \rightarrow \mathbb{R}^n$, $(t, x) \mapsto f(t, x)$ eine Funktion.

(1) Gibt es eine *Lipschitzkonstante*, d. h. eine Konstante $L > 0$ mit

$$\|f(t, x) - f(t, y)\| \leq L\|x - y\| \quad \text{für alle } (t, x), (t, y) \in D,$$

so heißt f *global Lipschitz-stetig bzgl. x* auf D .

(2) Gibt es für jedes Paar $(t, x) \in D$ eine Umgebung U , sodass $f|_{U \cap D}$ global Lipschitz-stetig ist, so heißt f *lokal Lipschitz-stetig bzgl. x* auf D .

Um eine Intuition für Lipschitz-Stetigkeit zu bekommen, bietet es sich an, den einfacheren Fall einer von t unabhängigen Funktion $f: \mathbb{R} \rightarrow \mathbb{R}$ zu betrachten. In diesem Fall ist f genau dann global Lipschitz-stetig, wenn es eine Konstante $L > 0$ gibt, sodass für alle $x, y \in \mathbb{R}$ mit $x \neq y$ der Differenzenquotient beschränkt ist:

$$\frac{|f(x) - f(y)|}{|x - y|} \leq \frac{L|x - y|}{|x - y|} = L$$

Anschaulich bedeutet das, dass die Steigung der Sekanten zwischen den Punkten $(x, f(x))$ und $(y, f(y))$ beschränkt ist. Insbesondere ist im Grenzfall die Steigung der Tangenten beschränkt, d. h. falls f differenzierbar ist, so muss die Ableitung beschränkt sein. Diese Überlegung legt bereits nahe, dass es nicht viele Funktionen geben wird, die *global Lipschitz-stetig* sind.

Der praktische Nachweis der lokalen Lipschitz-Bedingung lässt sich meist wiederum mithilfe der Ableitung führen, wie man leicht am obigen Beispiel sieht. Ist nämlich f' stetig, so ist f' nach dem Maximumsprinzip auf jedem abgeschlossenen Intervall beschränkt. Da es für jedes Paar $x, y \in \mathbb{R}$ mit $x \neq y$ nach dem Mittelwertsatz ein $z \in]x, y[$ mit

$$\frac{f(x) - f(y)}{x - y} = f'(z)$$

gibt, ist also auch die Steigung der Sekanten zwischen zwei Punkten des Graphen f lokal beschränkt und f ist lokal Lipschitz-stetig. Die nächste Proposition behandelt dies in voller Allgemeinheit.

Proposition 7.10 (Differenzierbarkeit und Lipschitz-Stetigkeit). Sei $D \subseteq \mathbb{R} \times \mathbb{R}^n$ ein Gebiet und $f: D \rightarrow \mathbb{R}^n$, $(t, x) \mapsto f(t, x)$ stetig partiell differenzierbar nach x . Dann ist f lokal Lipschitz-stetig bzgl. x auf D .

Als Ergebnis der bisherigen Vorarbeit können wir nun den folgenden Satz ernten.

Satz 7.11 (Picard-Lindelöf, qualitative Fassung). Sei $D \subseteq \mathbb{R} \times \mathbb{R}^n$ offen und $f: D \rightarrow \mathbb{R}^n$, $(t, x) \mapsto f(t, x)$ eine stetige und bzgl. x lokal Lipschitz-stetige Funktion. Dann besitzt für $(\tau, \xi) \in D$ jedes Anfangswertproblem

$$x' = f(t, x), \quad x(\tau) = \xi,$$

eine eindeutig bestimmte lokale Lösung, d. h. es gibt ein $\varepsilon > 0$, sodass das Anfangswertproblem auf dem Intervall $[\tau - \varepsilon, \tau + \varepsilon]$ genau eine Lösung besitzt.

Aufgabe (Frühjahr 2004, T1A4)

Welche der drei Differentialgleichungen

a $y' = |y|$, **b** $y' = \sqrt{|y|}$, **c** $y' = y^2$

besitzen eine Lösung bzw. eine eindeutig bestimmte Lösung φ mit $\varphi(0) = 0$?

Lösungsvorschlag zur Aufgabe (Frühjahr 2004, T1A4)

- a** Die Betragsfunktion ist global Lipschitz-stetig mit Lipschitzkonstante 1, denn aus der umgekehrten Dreiecksungleichung folgt für alle $x, y \in \mathbb{R}$, dass

$$||x| - |y|| \leq |x - y|$$

erfüllt ist. Insbesondere ist $f: \mathbb{R}^2 \rightarrow \mathbb{R}$, $(x, y) \mapsto |y|$ eine stetige und bzgl. y lokal Lipschitz-stetige Funktion, die auf einem Gebiet definiert ist. Der Satz von Picard-Lindelöf 7.11 gewährleistet daher die Existenz einer lokal eindeutigen Lösung von $y' = f(x, y)$ zum Anfangswert $y(0) = 0$.

- b** Die Funktion $g: \mathbb{R}^2 \rightarrow \mathbb{R}$, $(x, y) \mapsto \sqrt{|y|}$ ist auf dem gesamten Definitionsbereich stetig und hat einen offenen Definitionsbereich, also können wir nach dem Satz von Peano 7.8 zumindest sicher sein, dass $y' = g(x, y)$ eine lokale Lösung zum Anfangswert $y(0) = 0$ hat. Allerdings ist diese nie eindeutig, denn in jeder Umgebung $U \subseteq \mathbb{R}$ von 0 haben wir sowohl die Nulllösung

$$\nu: U \rightarrow \mathbb{R}, \quad x \mapsto 0,$$

als auch eine weitere Lösung, die man durch Trennen der Variablen bekommt (vgl. dazu Aufgabe F15T3A1 auf Seite 394):

$$\lambda: U \rightarrow \mathbb{R}, \quad x \mapsto \begin{cases} \frac{1}{4}x^2 & \text{für } x \geq 0, \\ -\frac{1}{4}x^2 & \text{für } x \leq 0. \end{cases}$$

c Definiere $h: \mathbb{R}^2 \rightarrow \mathbb{R}$, $(x, y) \mapsto y^2$, dann ist $\partial_y h(x, y) = 2y$ auf ganz \mathbb{R}^2 stetig, d. h. h ist eine auf dem gesamten Definitionsbereich (einem Gebiet) partiell stetig nach y differenzierbare Funktion und somit nach Proposition 7.10 dort lokal Lipschitz-stetig. Der Satz von Picard-Lindelöf 7.11 stellt daher die Existenz einer eindeutigen lokalen Lösung von $y' = h(x, y)$ zum Anfangswert $y(0) = 0$ sicher.

Der Beweis des Satzes von Picard-Lindelöf liefert außerdem ein Iterationsverfahren zur Lösung von Anfangswertproblemen.

Anleitung: Picard-Iteration

Seien $a, b \in \mathbb{R}$ mit $a < b$ und $f: [a, b] \times \mathbb{R}^n \rightarrow \mathbb{R}$, $(t, x) \mapsto f(t, x)$ eine stetige und global Lipschitz-stetige Funktion. Wir betrachten das Anfangswertproblem

$$x' = f(t, x), \quad x(\tau) = \xi \quad \text{mit } (\tau, \xi) \in [a, b] \times \mathbb{R}^n.$$

(1) Definiere einen Integraloperator $T: \mathcal{C}([a, b], \mathbb{R}^n) \rightarrow \mathcal{C}([a, b], \mathbb{R}^n)$ durch

$$(Tg)(t) := \xi + \int_{\tau}^t f(s, g(s)) ds.$$

(2) Man kann nun zeigen, dass es sich bei dem Integraloperator T um eine Kontraktion handelt, sodass dieser nach dem Banach'schen Fixpunktsatz genau einen Fixpunkt $\lambda_{\infty} \in \mathcal{C}([a, b], \mathbb{R}^n)$ besitzt. Dieser Fixpunkt ist eine Lösung des obigen Anfangswertproblems (siehe F13T2A5).

(3) Wir definieren induktiv die Funktionenfolge $(\lambda_k)_{k \in \mathbb{N}_0}$ durch

$$\lambda_0(t) = \xi, \quad \lambda_{k+1} = (T\lambda_k)(t).$$

Laut (2) konvergiert diese gegen die Lösung λ_{∞} .

Aufgabe (Frühjahr 2013, T2A5)

Eine Version des Banach'schen Fixpunktsatzes lautet: Seien (X, d) metrischer Raum, $\emptyset \neq A \subset X$ und $T: A \rightarrow X$ mit

- (1) $T(A) \subset A$ (2) A abgeschlossen (3) T Kontraktion (4) (X, d) vollständig.

Dann besitzt T genau einen Fixpunkt.

- a** Erklären Sie die in der Formulierung des Satzes auftretenden Voraussetzungen
- (i) T ist eine Kontraktion
 - (ii) der metrische Raum (X, d) ist vollständig.

- b** Beweisen Sie die Eindeutigkeit des Fixpunktes.

Seien $D \subset \mathbb{R} \times \mathbb{R}^n$ offen, $f: D \rightarrow \mathbb{R}^n$ und $(t_0, x_0) \in D$. Im Folgenden betrachten wir das Anfangswertproblem

$$x' = f(t, x), \quad x(t_0) = x_0.$$

- c** Formulieren Sie die Picard-Lindelöf Bedingung an f , d.h. die Voraussetzungen an f , unter denen mit dem Satz von Picard-Lindelöf auf die (lokale) Existenz und Eindeutigkeit einer Lösung des Anfangswertproblems geschlossen werden kann.

- d** Erläutern Sie kurz, wie man die Existenz einer Lösung des Anfangswertproblems unter der Voraussetzung der Picard-Lindelöf Bedingung aus dem Banach'schen Fixpunktsatz schließen kann. Gehen Sie hierbei insbesondere darauf ein, wie das Anfangswertproblem in eine äquivalente Fixpunktgleichung umformuliert werden kann und warum die Picard-Lindelöf Bedingung den Nachweis der Kontraktionseigenschaft ermöglicht.

Lösungsvorschlag zur Aufgabe (Frühjahr 2013, T2A5)

- a** (i): Die Abbildung T heißt *Kontraktion*, falls es eine Konstante $\Theta \in]0, 1[$ gibt, sodass für alle $x, y \in A$ die Abschätzung

$$d(T(x), T(y)) \leq \Theta d(x, y)$$

erfüllt ist.

(ii): Ein metrischer Raum (X, d) wird *vollständig* genannt, wenn jede Cauchy-Folge in (X, d) konvergiert.

- b** Seien $a, b \in A$ Fixpunkte von T , d.h. es gelte $T(a) = a$ und $T(b) = b$. Dann gilt

$$d(a, b) = d(T(a), T(b)) \leq \Theta d(a, b).$$

Wäre $d(a, b) \neq 0$, so könnten wir den Term rechts und links kürzen und bekämen $1 \leq \Theta$. Dies ist ein Widerspruch zu $\Theta \in]0, 1[$. Also gilt $d(a, b) = 0$ und nach der Definition einer Metrik folgt daraus $a = b$.

- c** Die Funktion f muss stetig und lokal Lipschitz-stetig bezüglich x sein (vgl. Satz 7.11). Letzteres bedeutet, dass es für jedes $(t, x) \in D$ eine Umgebung $U \subseteq D$ von (t, x) und eine Konstante $L > 0$ gibt, sodass dort

$$\|f(t, x_1) - f(t, x_2)\| \leq L \|x_1 - x_2\| \quad \text{für alle } (t, x_1), (t, x_2) \in U$$

erfüllt ist (vgl. Definition 7.9).

d Sei $\lambda: [a, b] \rightarrow \mathbb{R}$ eine Lösung des Anfangswertproblems. Definiere einen Integraloperator

$$T: \mathcal{C}([a, b], \mathbb{R}^n) \rightarrow \mathcal{C}([a, b], \mathbb{R}^n), \quad g \mapsto x_0 + \int_{t_0}^t f(s, g(s)) ds,$$

dann gilt

$$\begin{aligned} T(\lambda)(t) &= x_0 + \int_{t_0}^t f(s, \lambda(s)) ds = x_0 + \int_{t_0}^t \lambda'(s) ds = \\ &= x_0 + \lambda(t) - \lambda(t_0) = x_0 + \lambda(t) - x_0 = \lambda(t), \end{aligned}$$

d. h. λ ist ein Fixpunkt von T . Ist umgekehrt $\mu: [a, b] \rightarrow \mathbb{R}$ ein Fixpunkt von T , so gilt

$$\mu'(t) = (T(\mu))'(t) = \frac{d}{dt} \left(x_0 + \int_{t_0}^t f(s, \mu(s)) ds \right) = f(t, \mu(t))$$

und

$$\mu(t_0) = (T(\mu))(t_0) = x_0 + \int_{t_0}^{t_0} f(s, \mu(s)) ds = x_0,$$

also ist μ eine Lösung des Anfangswertproblems. Wir haben damit gezeigt, dass die Lösungen des Anfangswertproblems genau die Fixpunkte des Operators T sind. Wir wollen nun den Banach'schen Fixpunktsatz auf T anwenden. Dazu müssen wir zunächst prüfen, ob es sich bei T um eine Kontraktion handelt.

Sei nun f lokal Lipschitz-stetig bzgl. x , d. h. a und b seien so gewählt, dass es eine Konstante $L > 0$ mit

$$\|f(t, x) - f(t, y)\| \leq L \|x - y\| \quad \text{für alle } (t, x), (t, y) \in [a, b] \times D'$$

gibt, wobei $[a, b] \times D' \subseteq D$ ist. Verwenden wir die Supremumsnorm

$$\|g\|_\infty = \sup_{t \in [a, b]} \|g(t)\|,$$

so gilt nun für zwei Funktionen $g, h \in \mathcal{C}([a, b], \mathbb{R})$, dass

$$\|T(g) - T(h)\|_\infty = \sup_{t \in [a, b]} \left\| \int_{t_0}^t f(s, g(s)) - f(s, h(s)) ds \right\|.$$

Das darin auftretende Integral können wir wie folgt weiter abschätzen:

$$\begin{aligned} \left\| \int_{t_0}^t f(s, g(s)) - f(s, h(s)) ds \right\| &\leq \int_{t_0}^t \|f(s, g(s)) - f(s, h(s))\| ds \\ &\leq |t - t_0| \cdot \sup_{s \in [t_0, t]} \|f(s, g(s)) - f(s, h(s))\| \leq |t - t_0| \cdot L \cdot \sup_{s \in [t_0, t]} \|g(s) - h(s)\| \\ &\leq L \cdot (b - a) \cdot \|g - h\|_\infty \end{aligned}$$

Die Abschätzung schreibt sich also insgesamt als

$$\|T(g) - T(h)\|_\infty \leq L(b - a)\|g - h\|_\infty.$$

Verkleinert man nun ggf. $[a, b]$, sodass $(b - a) < \frac{1}{L}$ gilt, so haben wir eine Konstante $\Theta = L(b - a) < 1$ mit

$$\|T(g) - T(h)\|_\infty \leq \Theta\|g - h\|_\infty$$

gefunden und T ist eine Kontraktion. Da es sich bei $(C([a, b], \mathbb{R}), \|\cdot\|_\infty)$ um einen vollständigen metrischen Raum handelt, gibt es nach dem Banachschen Fixpunktsatz einen eindeutigen Fixpunkt, d. h. eine eindeutige Lösung $\lambda: [a, b] \rightarrow \mathbb{R}$.

Aufgabe (Frühjahr 2015, T2A4)

Man löse das Anfangswertproblem

$$x' = x + t, \quad x(0) = -1$$

- a** mit der Methode der Variation der Konstanten,
- b** mittels der Picard-Lindelöf-Iteration $(\alpha_n)_{n \in \mathbb{N}_0}$, beginnend mit $\alpha_0(t) \equiv -1$.

Lösungsvorschlag zur Aufgabe (Frühjahr 2015, T2A4)

- a** Die Lösungsformel der Variation der Konstanten lautet hier

$$\lambda(t) = (-1)e^{\int_0^t 1 ds} + e^{\int_0^t 1 ds} \int_0^t e^{-\int_0^s 1 dr} \cdot s ds = -e^t + e^t \int_0^t s e^{-s} ds.$$

Wir berechnen nun das Integral mittels partieller Integration:

$$\int_0^t s e^{-s} ds = [-s e^{-s}]_0^t - \int_0^t -e^{-s} ds = -t e^{-t} - [e^{-s}]_0^t = -t e^{-t} - e^{-t} + 1.$$

Also ergibt sich als Lösung die Abbildung $\lambda: \mathbb{R} \rightarrow \mathbb{R}$ mit

$$\lambda(t) = -e^t + e^t(-te^{-t} - e^{-t} + 1) = -t - 1.$$

- b** Wir sehen uns zunächst an, was in den ersten Schritten der Picard-Lindelöf-Iteration hier passiert:

$$\alpha_0(t) = -1,$$

$$\alpha_1(t) = -1 + \int_0^t (-1+s) \, ds = -1 - t + \frac{1}{2}t^2,$$

$$\alpha_2(t) = -1 + \int_0^t \left(-1 + \frac{1}{2}s^2 \right) \, ds = -1 - t + \frac{1}{6}t^3.$$

Dies gibt Anlass zu der Vermutung, dass $\alpha_n(t) = -1 - t + \frac{1}{(n+1)!}t^{n+1}$ ist.

Dies beweisen wir nun mittels vollständiger Induktion. Den Induktionsanfang haben wir bereits erledigt, widmen wir uns also dem Induktions schritt:

$$\begin{aligned} \alpha_{n+1}(t) &= -1 + \int_0^t \alpha_n(s) + s \, ds \stackrel{(I.V.)}{=} -1 + \int_0^t -1 + \frac{1}{(n+1)!}s^{n+1} \, ds = \\ &= -1 - t + \frac{1}{(n+2)!}t^{n+2}. \end{aligned}$$

Um zu sehen, dass $(\alpha_n)_{n \in \mathbb{N}_0}$ gegen die Lösungsfunktion aus Teil **a** konvergiert, müssen wir zeigen, dass die Folge $(\frac{1}{n!}t^n)_{n \in \mathbb{N}}$ für festes (aber beliebiges) t gegen 0 konvergiert. Dazu bemerken wir, dass die Exponentialreihe $\sum_{n=0}^{\infty} \frac{1}{n!}t^n$ konvergiert und daher $(\frac{1}{n!}t^n)_{n \in \mathbb{N}}$ eine Nullfolge sein muss.

Insgesamt haben wir also $\lim_{n \rightarrow \infty} \alpha_n(t) = -1 - t = \lambda(t)$ für beliebiges $t \in \mathbb{R}$ nachgewiesen.

Aufgabe (Herbst 2015, T2A3)

Betrachten Sie das Anfangswertproblem

$$y' = y^2, \quad y(0) = 1. \tag{3}$$

- a** Wir betrachten die Picard-Iteration mit der Startfunktion $y_0(x) = 1$. Zeigen Sie durch vollständige Induktion, dass die n -te Iterierte die Gestalt

$$y_n(x) = 1 + x + \dots + x^n + x^{n+1}r_n(x)$$

besitzt, wobei r_n ein Polynom ist. Finden Sie damit eine Potenzreihe, die (3) löst.

- b** In welchem Intervall $I \subseteq \mathbb{R}$ konvergiert diese Reihe?
- c** Bestimmen Sie die maximale Lösung des Anfangswertproblems (3). Auf welchem Intervall ist sie definiert?

Lösungsvorschlag zur Aufgabe (Herbst 2015, T2A3)

- a** Für $n = 0$ ist die Behauptung offensichtlich erfüllt. Setzen wir die Aussage daher für ein n als bereits bewiesen voraus. Es ist dann

$$y_{n+1}(x) = 1 + \int_0^x y_n^2(s) ds = 1 + \int_0^x (1 + s + \dots + s^{n+1} r_n(s))^2 ds.$$

Um das Integral berechnen zu können, zeigen wir zunächst folgende Hilfsbehauptung per Induktion:

$$(1 + x + \dots + x^k)^2 = 1 + 2x + \dots + (k+1)x^k + kx^{k+1} + (k-1)x^{k+2} + \dots + x^{2k}$$

Für $k = 0$ ist die Behauptung wahr. Gehen wir zum Induktionsschritt über.

$$\begin{aligned} (1 + \dots + x^{k+1})^2 &= (1 + \dots + x^k)^2 + 2(1 + \dots + x^k)x^{k+1} + x^{2(k+1)} = \\ &\stackrel{(I.V.)}{=} \left(1 + \dots + (k+1)x^k + kx^{k+1} + (k-1)x^{k+2} + \dots + x^{2k}\right) + \\ &\quad + 2(1 + \dots + x^k)x^{k+1} + x^{2(k+1)} = \\ &= 1 + \dots + (k+1)x^k + (k+2)x^{k+1} + (k+1)x^{k+2} + \dots + 2x^{2k+1} + x^{2(k+1)} \end{aligned}$$

Damit ist die Behauptung bewiesen. Der Einfachheit halber fassen wir die höheren Terme zu einem Polynom p_k zusammen und schreiben nur

$$(1 + \dots + x^k)^2 = 1 + 2x + \dots + kx^{k-1} + p_k x^k.$$

Für obiges Integral ergibt sich nun

$$\begin{aligned} &\int_0^x (1 + s + \dots + s^{n+1} r_n(s))^2 ds = \\ &= \int_0^x (1 + s + \dots + s^n)^2 + 2(1 + s + \dots + s^n)r_n s^{n+1} + r_n^2 s^{2(n+1)} ds = \\ &= \int_0^x \left(1 + 2s + \dots + (n+1)s^n + p_{n+1}s^{n+1}\right) + \\ &\quad + s^{n+1} \left(2r_n(1 + \dots + s^n) + r_n^2 s^{n+1}\right) ds = \\ &= x + \dots + x^{n+1} + \int_0^x p_{n+1}s^{n+1} + s^{n+1} \left(2r_n(1 + \dots + s^n) + r_n^2 s^{n+1}\right) ds. \end{aligned}$$

Das letzte Integral ergibt ein Polynom, dessen Monome alle mindestens Grad $n + 2$ haben. Wir kürzen diesen Term daher einfach mit $r_{n+1}x^{n+2}$ ab und erhalten

$$y_{n+1}(x) = 1 + \int_0^x y_n^2(s)ds = 1 + x + x^2 + \dots + x^{n+1} + r_{n+1}x^{n+2}.$$

Damit ist die erste Aussage bewiesen.

Ignoriert man für einen Moment den Term r_nx^{n+1} , so sieht der Ausdruck verdächtig nach der geometrischen Reihe aus. Setzen wir $y(x) = \sum_{i=0}^{\infty} x^i$, so gilt für $|x| < 1$, dass $y(x) = \frac{1}{1-x}$ ist und somit tatsächlich

$$y'(x) = \frac{0 - 1 \cdot (-1)}{(1-x)^2} = \left(\frac{1}{1-x}\right)^2 = y(x)^2.$$

b Die geometrische Reihe konvergiert für $x \in]-1, 1[$.

c Wir zeigen, dass $\lambda:]-\infty, 1[\rightarrow \mathbb{R}, x \mapsto \frac{1}{1-x}$ die maximale Lösung des Anfangswertproblems ist. Dazu greifen wir etwas vor und verwenden bereits die nachfolgenden Sätze.

Zunächst ist $f: \mathbb{R}^2 \rightarrow \mathbb{R}, (x, y) \mapsto y^2$ eine auf einem Gebiet definierte und bezüglich y stetig differenzierbare Funktion. Diese ist nach Proposition 7.10 lokal Lipschitz-stetig, sodass es nach dem Globalen Existenz- und Eindeutigkeitssatz 7.12 eine eindeutige maximale Lösung des Anfangswertproblems $y' = f(x, y)$ mit $y(0) = 1$ gibt.

Bedingung (1)(i) von Satz 7.13 wird von λ bereits erfüllt, also brauchen wir nur das Verhalten von λ an der oberen Grenze betrachten:

$$\lim_{x \rightarrow 1^-} |\lambda(x)| = \lim_{x \rightarrow 1^-} \frac{1}{|1-x|} = \infty$$

Damit ist (2)(ii) erfüllt und es handelt sich bei λ tatsächlich um die maximale Lösung.

Der Satz von Picard-Lindelöf liefert in der qualitativen Fassung lediglich die Existenz und Eindeutigkeit einer lokalen Lösung. Diese existiert im konkreten Fall jedoch oft sogar auf einem größeren Intervall oder kann fortgesetzt werden. Da dies aus Sicht des Theoretikers unbefriedigend ist, verfeinern wir die Aussage des Satzes von Picard-Lindelöf.

Satz 7.12 (Globaler Existenz- und Eindeutigkeitssatz). Sei $D \subseteq \mathbb{R} \times \mathbb{R}^n$ ein Gebiet und $f: D \rightarrow \mathbb{R}^n$, $(t, x) \mapsto f(t, x)$ eine stetige und bzgl. x lokal Lipschitz-stetige Funktion. Dann gibt es für jedes $(\tau, \xi) \in D$ ein eindeutig bestimmtes Intervall $I =]a, b[$ mit $\tau \in I$, sodass

- (1) das Anfangswertproblem

$$x'(t) = f(t, x), \quad x(\tau) = \xi,$$

auf dem Lösungsintervall I genau eine Lösung $\lambda: I \rightarrow \mathbb{R}^n$ besitzt,

- (2) jede weitere Lösung $\mu: J \rightarrow \mathbb{R}^n$ des Anfangswertproblems eine Einschränkung der Lösung λ aus (1) ist und $J \subseteq I$ gilt.

Die Lösungsfunktion aus (1) heißt **maximale Lösung** des Anfangswertproblems und wird gelegentlich mit $\lambda_{(\tau, \xi)}$ bezeichnet.

Die Lösungskurven zweier maximaler Lösungen sind immer disjunkt oder bereits gleich: Seien $\lambda: I \rightarrow \mathbb{R}^n$ und $\mu: J \rightarrow \mathbb{R}^n$ zwei maximale Lösungen einer Differentialgleichung $x' = f(t, x)$, die die Voraussetzungen des Globalen Existenz- und Eindeutigkeitssatzes erfüllt. Gibt es ein $t_0 \in I \cap J$ mit $\lambda(t_0) = \mu(t_0)$, so sind λ und μ beide Lösungen des Anfangswertproblems

$$x' = f(t, x), \quad x(t_0) = \lambda(t_0) = \mu(t_0)$$

und aus der Eindeutigkeitsaussage folgt $\lambda = \mu$.

Neben der Existenz einer maximalen Lösung ist natürlich von Interesse, wie man diese erkennt. Hier hilft das Randverhalten weiter.

Satz 7.13 (Randverhalten maximaler Lösungen). Sei $D \subseteq \mathbb{R} \times \mathbb{R}^n$ ein Gebiet und $f: D \rightarrow \mathbb{R}^n$, $(t, x) \mapsto f(t, x)$ eine stetige und bzgl. x lokal Lipschitz-stetige Funktion. Zu $(\tau, \xi) \in D$ sei $\lambda:]a, b[\rightarrow \mathbb{R}^n$ eine Lösung des Anfangswertproblems

$$x' = f(t, x), \quad x(\tau) = \xi.$$

λ ist genau dann die maximale Lösung des Anfangswertproblems, wenn jeweils eine der Bedingungen aus (1) und (2) erfüllt ist:

- (1) (i) $a = -\infty$,
- (ii) $a > -\infty$ und $\limsup_{t \searrow a} \|\lambda(t)\| = \infty$,
- (iii) $a > -\infty$, $\partial D \neq \emptyset$ und $\lim_{t \searrow a} \text{dist}(\partial D, (t, \lambda(t))) = 0$.

- (2) (i) $b = \infty$,
(ii) $b < \infty$ und $\limsup_{t \nearrow b} \|\lambda(t)\| = \infty$,
(iii) $b < \infty$, $\partial D \neq \emptyset$ und $\lim_{t \nearrow b} \text{dist}(\partial D, (\lambda(t))) = 0$.

Die in der Formulierung des Satzes verwendete **Abstandsfunktion** einer Menge $M \subseteq \mathbb{R}^n$ ist dabei definiert als

$$\text{dist}(p, M) = \inf_{m \in M} \|p - m\| \quad \text{für } p \in \mathbb{R}^n.$$

Aufgabe (Herbst 2012, T3A2)

- a** Formulieren Sie den Existenz- und Eindeutigkeitssatz von Picard-Lindelöf.
b Sei $\alpha \in \mathbb{R}, \alpha > 0$. Zeigen Sie, dass das Anfangswertproblem

$$y' = |y|^\alpha, \quad y(0) = 0$$

genau im Fall $\alpha \geq 1$ eine eindeutige Lösung auf $[0, \infty)$ besitzt.

Lösungsvorschlag zur Aufgabe (Herbst 2012, T3A2)

- a** Siehe Satz 7.11.
b Wir definieren $f_\alpha: \mathbb{R}^2 \rightarrow \mathbb{R}, (t, y) \mapsto |y|^\alpha$ und zeigen, dass diese Funktion für $\alpha \geq 1$ die Voraussetzungen des Globalen Existenz- und Eindeutigkeitssatzes erfüllt. Dass \mathbb{R}^2 ein Gebiet und f_α stetig ist, ist klar. Zu zeigen bleibt die (lokale) Lipschitz-Stetigkeit.
Sei zunächst $\alpha = 1$. Hier lässt sich globale Lipschitz-Stetigkeit anhand der Definition zeigen, denn für alle $x, y \in \mathbb{R}$ gilt aufgrund der umgekehrten Dreiecksungleichung die Abschätzung

$$||x| - |y|| \leq |x - y| = 1 \cdot |x - y|.$$

Sei nun $\alpha > 1$. Die stetige Differenzierbarkeit nach y von $f: \mathbb{R}^2 \rightarrow \mathbb{R}, (t, y) \mapsto |y|^\alpha$ für $y \neq 0$ ist klar, da die Funktion dort mit $(t, y) \mapsto y^\alpha$ bzw. $(t, y) \mapsto (-y)^\alpha$ übereinstimmt. Die Differenzierbarkeit in 0 überprüfen wir anhand der Definition:

$$\lim_{h \rightarrow 0} \frac{f_\alpha(0 + h) - f_\alpha(0)}{h} = \lim_{h \rightarrow 0} \frac{|h|^\alpha}{h} = \lim_{h \rightarrow 0} \text{sgn}(h)|h|^{\alpha-1}$$

Wegen $\alpha > 1$ ist $\alpha - 1 > 0$, sodass der Ausdruck $|h|^{\alpha-1}$ für $h = 0$ definiert ist. Somit ist

$$\lim_{h \rightarrow 0} \operatorname{sgn}(h)|h|^{\alpha-1} = 0$$

und f_α ist auch in 0 differenzierbar mit $\partial_y f_\alpha(0) = 0$. Insgesamt ist damit

$$\partial_y f_\alpha: \mathbb{R}^2 \rightarrow \mathbb{R}, \quad (t, y) \mapsto \begin{cases} \alpha y^{\alpha-1} & \text{für } y > 0, \\ 0 & \text{für } y = 0, \\ \alpha(-y)^{\alpha-1} & \text{für } y < 0. \end{cases}$$

stetig. Diese Abbildung lässt sich als $\partial_y f_\alpha(t, y) = \alpha|y|^{\alpha-1}$ schreiben und ist damit als Komposition stetiger Funktionen selbst ebenfalls stetig. Somit ist f_α für $\alpha > 1$ stetig partiell nach y differenzierbar und daher nach Proposition 7.10 lokal Lipschitz-stetig.

Der Globale Existenz- und Eindeutigkeitssatz liefert dann für $\alpha \geq 1$ eine eindeutige maximale Lösung $\lambda: I \rightarrow \mathbb{R}$ von $y' = f_\alpha(t, y)$ zum Anfangswert $y(0) = 0$ auf einem Definitionssintervall $I \subseteq \mathbb{R}$ mit $0 \in I$.

Betrachte die Nullfunktion $v: \mathbb{R} \rightarrow \mathbb{R}, t \mapsto 0$. Diese ist offensichtlich eine Lösung besagten Anfangswertproblems und erfüllt zudem (1)(i) und (2)(i) von Satz 7.13, sodass es sich bei v um die eindeutige maximale Lösung handelt. Nach dem Globalen Existenz- und Eindeutigkeitssatz 7.12 (2) ist jede Lösung auf $[0, \infty[$ eine Einschränkung von v und somit insbesondere eindeutig.

Im Fall $\alpha < 1$ ist die Nullfunktion ebenfalls eine Lösung des Anfangswertproblems. Eine zweite Lösung bekommen wir hier jedoch durch Trennen der Variablen (der Einfachheit wegen für $y \geq 0$):

$$\int_0^{\lambda(t)} y^{-\alpha} dy = \int_0^t 1 d\tau \Leftrightarrow \left[\frac{1}{1-\alpha} y^{1-\alpha} \right]_0^{\lambda(t)} = t \Leftrightarrow \frac{1}{1-\alpha} \lambda(t)^{1-\alpha} = t$$

Man beachte dabei, dass wegen $1 - \alpha > 0$ das Einsetzen der Integrationsgrenze 0 möglich ist. Auflösen der Gleichung liefert nun

$$\lambda(t) = \sqrt[1-\alpha]{(1-\alpha)t}$$

und diese Funktion ist für $t \in [0, \infty[$ tatsächlich eine Lösung des Anfangswertproblems, denn dort ist $\lambda(t) = |\lambda(t)|$ und somit:

$$\lambda'(t) = \frac{1}{1-\alpha} \cdot ((1-\alpha)t)^{\frac{1}{1-\alpha}-1} \cdot (1-\alpha) = ((1-\alpha)t)^{\frac{1-1+\alpha}{1-\alpha}} = \lambda(t)^\alpha = |\lambda(t)|^\alpha$$

sowie $\lambda(0) = 0$.

Anleitung: Abschätzungen maximaler Lösungen

Gegeben sei eine Differentialgleichung $x' = f(t, x)$, die die Voraussetzungen des Globalen Existenz- und Eindeutigkeitssatzes erfüllt. Gesucht sind eine obere bzw. untere Schranke für eine maximale Lösung $\lambda: I \rightarrow \mathbb{R}$ zum Anfangswert $\lambda(\tau) = \xi$, da direkt danach gefragt ist oder man den Fall (1)(ii) bzw. (2)(ii) im Satz über das Randverhalten maximaler Lösungen 7.13 ausschließen möchte.

- (1) Bestimme die stationären Lösungen der Differentialgleichung: Jede Nullstelle x_0 mit $f(t, x_0) = 0$ liefert eine konstante Lösung

$$\mu : \mathbb{R} \rightarrow \mathbb{R}, \quad t \mapsto x_0,$$

die die eindeutige maximale Lösung zum Anfangswert $x(0) = x_0$ ist, da sie auf ganz \mathbb{R} definiert ist.

- (2) Ist $\lambda(\tau) = \xi < x_0$, so muss $\lambda(t) < x_0$ für alle $t \in I$ gelten: Gäbe es nämlich $t_1 \in I$ mit $\lambda(t_1) \geq x_0$, so würde man nach dem Zwischenwertsatz ein $t_2 \in I$ finden, sodass $\lambda(t_2) = x_0 = \mu(t_2)$. Da die Graphen maximaler Lösungen entweder disjunkt oder gleich sind, würde daraus bereits $\lambda(t) = \mu(t)$ für alle $t \in I$ folgen, was ein Widerspruch zu $\lambda(\tau) < x_0$ ist.

Genauso kann man aus $\lambda(\tau) = \xi > x_0$ auch $\lambda(t) > x_0$ für alle $t \in I$ folgern.

- (3) Hilfreich kann es außerdem sein, $f(t, \lambda(t))$ abzuschätzen, denn es gilt laut dem Hauptsatz der Differential- und Integralrechnung

$$\lambda(t) - \lambda(\tau) = \int_{\tau}^t \lambda'(s) ds = \int_{\tau}^t f(s, \lambda(s)) ds$$

und aus $m \leq f(t, \lambda(t)) \leq M$ für alle $t \in I$ folgt

$$(t - \tau)m = \int_{\tau}^t m ds \leq \int_{\tau}^t f(s, \lambda(s)) ds \leq \int_{\tau}^t M ds = (t - \tau)M$$

bzw. $|f(t, \lambda(t))| \leq C$ für alle $t \in I$ liefert die Abschätzung

$$\left| \int_{\tau}^t f(s, \lambda(s)) ds \right| \leq \int_{\tau}^t |f(s, \lambda(s))| ds \leq |t - \tau| \cdot C.$$

Aufgabe (Frühjahr 2012, T1A5)

Für $\xi \in \mathbb{R}$ sei das Anfangswertproblem

$$x' = \arctan(x), \quad x(0) = \xi$$

gegeben. Beweisen Sie die folgenden Aussagen:

- a** Das Anfangswertproblem besitzt genau eine maximale Lösung $\lambda_\xi: I_\xi \rightarrow \mathbb{R}$.
- b** λ_ξ besitzt genau dann eine Nullstelle, wenn $\xi = 0$ ist.
- c** Für alle $t \in I_\xi$ gilt:

$$\xi - \frac{\pi}{2}|t| \leq \lambda_\xi(t) \leq \xi + \frac{\pi}{2}|t|.$$
- d** $I_\xi = \mathbb{R}$.

Lösungsvorschlag zur Aufgabe (Frühjahr 2012, T1A5)

- a** Definiere $f: \mathbb{R}^2 \rightarrow \mathbb{R}, (t, x) \mapsto \arctan(x)$, dann ist die Funktion f auf einem Gebiet definiert und bekanntlich stetig. Weiterhin ist

$$\partial_x f(t, x) = \frac{1}{1+x^2},$$

sodass f auf dem gesamten Definitionsbereich stetig partiell differenzierbar nach x ist. Nach Proposition 7.10 ist daher f lokal Lipschitz-stetig und nach dem Globalen Existenz- und Eindeutigkeitssatz 7.12 gibt es eine eindeutige maximale Lösung des Anfangswertproblems $x' = f(t, x)$ mit $x(0) = \xi$ und Definitionssintervall I_ξ .

- b** Es ist $\tan 0 = \frac{\sin 0}{\cos 0} = 0$, d.h. $\arctan 0 = 0$. Folglich ist die Nullfunktion $v: \mathbb{R} \rightarrow \mathbb{R}, t \mapsto 0$ eine Lösung der Differentialgleichung. Da sie auf ganz \mathbb{R} definiert ist, handelt es sich bei ihr nach dem Satz über das Randverhalten maximaler Lösungen (Satz 7.13) um die eindeutige maximale Lösung zum Anfangswert $x(0) = 0$.

Hat λ_ξ eine Nullstelle t_0 , so bedeutet dies, dass sich die Lösungskurven von λ_ξ und v in dieser Nullstelle schneiden. Nun ist aber v eine maximale Lösung der Gleichung zur Anfangsbedingung $x(0) = 0$ und somit müssen laut dem Globalen Existenz- und Eindeutigkeitssatz λ_ξ und v identisch sein. Insbesondere ist $\xi = \lambda_\xi(0) = 0$.

- c** Es gilt

$$|\lambda'_\xi(t)| = |\arctan \lambda_\xi(t)| \leq \frac{\pi}{2} \quad \text{für alle } t \in I_\xi,$$

also ist auch

$$|\lambda_\xi(t) - \lambda_\xi(0)| = \left| \int_0^t \lambda'_\xi(s) ds \right| \leq \left| \int_0^t \frac{\pi}{2} ds \right| = |t| \cdot \frac{\pi}{2}$$

und umformuliert ergibt dies mit $\lambda_\xi(0) = \xi$

$$\xi - \frac{\pi}{2}|t| \leq \lambda_\xi(t) \leq \xi + \frac{\pi}{2}|t| \quad \text{für alle } t \in I_\xi.$$

- d** Wir gehen die Bedingungen aus Satz 7.13 durch. Da der Rand von \mathbb{R}^2 leer ist, kann weder (1)(iii) noch (2)(iii) erfüllt sein. Hat I_ξ eine endliche untere Grenze a , so gilt unter Verwendung von Teil **c**:

$$\lim_{t \rightarrow a} |\lambda_\xi(t)| \leq \lim_{t \rightarrow a} \left| \xi \pm \frac{\pi}{2}|t| \right| = \left| \xi \pm \frac{\pi}{2}|a| \right| < \infty.$$

Also kann (1)(ii) und analog (w)(ii) unmöglich eintreten. Es bleibt daher nur noch (1)(i) und (2)(i), d. h. $I_\xi = \mathbb{R}$.

Aufgabe (Frühjahr 2012, T2A4)

Gegeben sei das Anfangswertproblem

$$\dot{x} = x(x-2)e^{\cos x}, x(0) = 1.$$

Zeigen Sie:

- a** Das Anfangswertproblem hat eine eindeutige maximale Lösung $x: I \rightarrow \mathbb{R}$ auf einem offenen Intervall $I \subseteq \mathbb{R}$. Welche stationären Lösungen hat die Differentialgleichung?
- b** Die maximale Lösung x aus **a** existiert auf ganz \mathbb{R} und ist monoton fallend und beschränkt.
- c** Die Grenzwerte $\lim_{t \rightarrow \pm\infty} x(t)$ existieren in \mathbb{R} . Bestimmen Sie diese Grenzwerte.

Lösungsvorschlag zur Aufgabe (Frühjahr 2012, T2A4)

- a** Definiere $f: \mathbb{R}^2 \rightarrow \mathbb{R}, (t, x) \mapsto x(x-2)e^{\cos x}$, dann ist f auf einem Gebiet definiert und stetig, außerdem gilt

$$\partial_x f(t, x) = (x-2)e^{\cos x} + x e^{\cos x} + x(x-2)e^{\cos x} \sin x.$$

Somit ist f auf dem ganzen Definitionsbereich stetig partiell differenzierbar nach x . Mit Proposition 7.10 und dem Globalen Existenz- und Eindeutigkeitssatz 7.12 folgt die Existenz einer eindeutigen maximalen Lösung $x: I \rightarrow \mathbb{R}$.

Die stationären Lösungen der Differentialgleichung sind durch die Nullstellen von f gegeben. Da der Faktor $e^{\cos x}$ stets positiv ist, sind dies also

$$\mu_1: \mathbb{R} \rightarrow \mathbb{R}, \quad t \mapsto 0 \quad \text{und} \quad \mu_2: \mathbb{R} \rightarrow \mathbb{R}, \quad t \mapsto 2.$$

b Die stationären Lösungen aus Teil **a** sind auf ganz \mathbb{R} definiert und daher maximale Lösungen. Wegen der Anfangswertbedingung $x(0) = 1$ stimmt x weder mit μ_0 noch mit μ_2 überein. Da sich die Graphen verschiedener maximaler Lösungen nicht schneiden können, bedeutet das, dass $0 < x(t) < 2$ für alle $t \in I$ gelten muss. Da der Rand von \mathbb{R}^2 zudem leer ist, ist das einzige mögliche Randverhalten von x in Satz 7.13 dann (1)(i) und (2)(i), d. h. $I = \mathbb{R}$. Die beiden Schranken von $x(t)$ liefern weiterhin $x(t) - 2 < 0$ und $x(t) > 0$ für alle $t \in I$, d. h.

$$x'(t) = x(t)(x(t) - 2)e^{\cos x(t)} < 0$$

für alle $t \in I$. Dies bedeutet gerade, dass x auf ganz \mathbb{R} monoton fallend ist.

c Die Grenzwerte existieren, da x nach Teil **b** beschränkt und monoton fallend ist. Nehmen wir an, es gibt eine obere Schranke $c < 2$, sodass $x(t) \leq c$ für alle $t \in \mathbb{R}$. Dies bedeutet, dass

$$x'(t) = x(t)(x(t) - 2)e^{\cos x(t)} \leq c(c - 2)e^1 < 0$$

ist. Für alle $t \geq 0$ ist daher

$$x(t) = x(0) + \int_0^t x'(s)ds \leq 1 + tc(c - 2)e^t \xrightarrow{t \rightarrow \infty} -\infty,$$

d. h. x ist nach unten nicht beschränkt. Widerspruch zu **b**. Auf die gleiche Weise führt man die Annahme, dass es eine untere Schranke $d > 0$ mit $x(t) \geq d$ für alle $t \in I$ gibt, zum Widerspruch. Wir erhalten daher aufgrund der Monotonie

$$\lim_{t \rightarrow \infty} x(t) = 0 \quad \text{und} \quad \lim_{t \rightarrow -\infty} x(t) = 2.$$

Im Unterschied zu den bisher vorgestellten Existenz- und Eindeutigkeitssätzen zeichnet sich der folgende – und letzte – dadurch aus, dass er neben der Existenz einer maximalen Lösung auch das Definitionsintervall dieser maximalen Lösung explizit angibt.

Satz 7.14 (Existenz- und Eindeutigkeitssatz bei linear beschränkter rechter Seite). Seien $a, b \in \mathbb{R} \cup \{\pm\infty\}$ mit $a < b$ und $f:]a, b[\times \mathbb{R}^n \rightarrow \mathbb{R}^n$, $(t, x) \mapsto f(t, x)$ eine stetige und bezüglich x lokal Lipschitz-stetige Funktion, die *linear beschränkt* ist, d. h. eine Abschätzung der Form

$$\|f(t, x)\| \leq \rho(t)\|x\| + \sigma(t) \quad \text{für alle } (t, x) \in]a, b[\times \mathbb{R}^n$$

mit stetigen Funktionen $\rho, \sigma:]a, b[\rightarrow [0, +\infty[$ erfüllt. Dann existiert für jedes $(\tau, \xi) \in D$ eine eindeutige maximale Lösung $\lambda_{(\tau, \xi)}$ des Anfangswertproblems

$$x' = f(t, x), \quad x(\tau) = \xi$$

auf dem ganzen Intervall $]a, b[$.

Aufgabe (Herbst 2010, T3A3)

Sei

$$f(t, x) := \frac{t^2}{(e^x - x)^2}.$$

- a** Zeigen Sie, dass $e^x \neq x$ für alle $x \in \mathbb{R}$ ist, also dass f auf ganz \mathbb{R}^2 definiert ist.
- b** Zeigen Sie, dass das Anfangswertproblem

$$\dot{x}(t) = f(t, x), \quad x(0) = 0,$$

eine auf ganz \mathbb{R} definierte Lösung hat.

Lösungsvorschlag zur Aufgabe (Herbst 2010, T3A3)

- a** Lösungen der Gleichung $e^x = x$ sind genau die Nullstellen der Funktion

$$g: \mathbb{R} \rightarrow \mathbb{R}, \quad x \mapsto e^x - x.$$

Es ist $g'(0) = e^0 - 1 = 0$ und $g''(0) = e^0 = 1 > 0$, also hat g ein Minimum an der Stelle 0. Wegen $g''(x) = e^x > 0$ für alle $x \in \mathbb{R}$ ist dies ein globales Minimum. Es gilt also $g(x) \geq g(0) = 1$ für alle $x \in \mathbb{R}$. Damit kann g keine Nullstelle haben und es ist $e^x \neq x$ für alle $x \in \mathbb{R}$.

- b** Nach Teil **a** ist $f(t, x)$ auf ganz \mathbb{R}^2 definiert und dort stetig. Gleichermaßen gilt für

$$\partial_x f(t, x) = \frac{-2t^2(e^x - x)(e^x - 1)}{(e^x - x)^4},$$

sodass $f(t, x)$ nach Proposition 7.10 auf dem gesamten Definitionsbereich lokal Lipschitz-stetig ist. In Teil **a** haben wir gezeigt, dass $e^x - x \geq 1$ für alle $x \in \mathbb{R}$. Folglich ist

$$f(t, x) = \frac{t^2}{(e^x - x)^2} \leq t^2 = 0 \cdot |x| + t^2$$

für alle $(t, x) \in \mathbb{R}^2$. Somit ist $f(t, x)$ linear beschränkt auf ganz \mathbb{R}^2 , sodass das Anfangswertproblem $x' = f(t, x), x(0) = 0$ nach Satz 7.14 eine eindeutige maximale und auf ganz \mathbb{R} definierte Lösung besitzt.

Aufgabe (Frühjahr 2014, T2A1)

Es sei $f: \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}$, $(t, x) \mapsto \frac{xt}{\sqrt{x^2+1}}$. Zeigen Sie:

- a** Das Anfangswertproblem

$$x' = f(t, x), \quad x(0) = 1$$

hat eine eindeutige Lösung $\lambda: I \rightarrow \mathbb{R}$.

- b** Für das maximale Lösungsintervall gilt: $I = \mathbb{R}$.
- c** Für alle $t \geq 0$ ist $\lambda(t) \in [1, 1 + \frac{t^2}{2}]$.

Lösungsvorschlag zur Aufgabe (Frühjahr 2014, T2A1)

- a** Bei $\mathbb{R} \times \mathbb{R}$ handelt es sich um ein Gebiet. Außerdem ist f auf dem gesamten Definitionsbereich stetig und da

$$\partial_x f(t, x) = \frac{t\sqrt{x^2+1} - xt \cdot \frac{2x}{2\sqrt{x^2+1}}}{x^2+1}$$

auf ganz $\mathbb{R} \times \mathbb{R}$ definiert und stetig ist, ist f nach Proposition 7.10 auf dem gesamten Definitionsbereich lokal Lipschitz-stetig. Der Globale Existenz- und Eindeutigkeitssatz 7.12 gewährleistet daher die Existenz einer eindeutigen maximalen Lösung $\lambda: I \rightarrow \mathbb{R}$ auf einem Definitionssintervall $I \subseteq \mathbb{R}$ mit $0 \in I$.

- b** Für alle $x \in \mathbb{R}$ gilt $x^2 + 1 \geq 1$, also

$$|f(t, x)| = \left| \frac{xt}{\sqrt{x^2+1}} \right| \leq |xt| = |t| \cdot |x|.$$

Damit ist $f(t, x)$ linear beschränkt auf ganz \mathbb{R} und nach Satz 7.14 ist λ auf ganz \mathbb{R} definiert.

- c** Die Nullfunktion $v: \mathbb{R} \rightarrow \mathbb{R}$, $t \mapsto 0$ ist eine Lösung zum Anfangswert $x(0) = 0$. Diese erfüllt (1)(i) und (2)(i) von 7.13, ist also die maximale Lösung zu diesem Anfangswert.

Angenommen, es gibt ein $t \in I$ mit $\lambda(t) \leq 0$. Wegen $\lambda(0) = 1 > 0$ gibt es dann laut Zwischenwertsatz ein $\tau \in [t, 0[$ mit $\lambda(\tau) = 0$. Dies bedeutet aber, dass sich die Lösungskurven der beiden maximalen Lösungen v und λ schneiden, was unmöglich ist. Also ist $\lambda(t) \geq 0$ für alle $t \in I$. Für $t \geq 0$ folgt daraus

$$\lambda'(t) = \frac{\lambda(t)t}{\sqrt{\lambda(t)^2+1}} \geq 0,$$

d. h. λ ist auf $[0, \infty[$ monoton steigend und es muss $\lambda(t) \geq \lambda(0) = 1$ für alle $t \geq 0$ gelten. Weiterhin gilt

$$\lambda'(t) = f(t, \lambda(t)) = \frac{\lambda(t)t}{\sqrt{\lambda^2(t) + 1}} \leq \frac{\lambda(t)t}{\sqrt{\lambda(t)^2}} = t.$$

Integrieren beider Seiten ergibt

$$\lambda(t) - \lambda(0) = \int_0^t \lambda'(s) ds \leq \int_0^t s ds = \frac{1}{2}t^2 \quad \Leftrightarrow \quad \lambda(t) \leq 1 + \frac{1}{2}t^2.$$

Insgesamt haben wir $1 \leq \lambda(t) \leq 1 + \frac{1}{2}t^2$ für alle $t \geq 0$ nachgewiesen.

7.3. Lineare Systeme von Differentialgleichungen

In diesem Abschnitt¹ beschäftigen wir uns mit Differentialgleichungen der Form

$$x'(t) = A(t)x(t) + g(t), \quad t \in I, \tag{*}$$

wobei I ein Intervall, $A(t)$ eine $(n \times n)$ -Matrix mit stetig von t abhängigen Einträgen und g eine stetige Funktion ist. Im Fall $g \equiv 0$ bezeichnet man solche Gleichungen als *homogene lineare Gleichungen*, ansonsten also *inhomogen*. Eine Lösung x ist dabei eine vektorwertige Funktion, d. h. eine Abbildung $\lambda: I \rightarrow \mathbb{R}^n$ für ein geeignetes Intervall $I \subseteq \mathbb{R}$.

Eine Gleichung der Form (*) besitzt stets eine eindeutige Lösung. Dies folgt aus dem Globalen Existenz- und Eindeutigkeitssatz bei linear beschränkter rechter Seite (Satz 7.14). Der Definitionsbereich der Gleichung ist $I \times \mathbb{R}^n$ und damit ein Gebiet. Betrachte die Funktion $f(t, x) = A(t)x + g(t)$. Ist $t \in I$, so gilt für eine beliebige Norm $\|\cdot\|$ und zugehörige induzierte Matrix-Norm $\|\cdot\|$, dass

$$\|f(t, x)\| = \|A(t)x + g(t)\| \stackrel{(\Delta)}{\leq} \|A(t)x\| + \|g(t)\| \leq \|A(t)\| \cdot \|x\| + \|g(t)\|.$$

Die Zuordnungen $t \mapsto \|A(t)\|$ und $t \mapsto \|g(t)\|$ sind stetig, da $A(t)$ und $g(t)$ stetig von t abhängen und die Norm ebenfalls eine stetige Abbildung definiert. Die i -te Komponente der Funktion f ist gegeben durch $f_i(t, x) = \sum_{j=1}^n a_{ij}(t)x_j + g_i(t)$ und ist stetig differenzierbar nach x_i , da die Einträge $a_{ij}(t)$ stetig von t abhängen. Damit ist f laut Proposition 7.10 lokal Lipschitz-stetig bezüglich x und alle Voraussetzungen von Satz 7.14 sind erfüllt. Es folgt die Existenz einer eindeutigen maximalen Lösung auf ganz I .

Eine grundlegende Erkenntnis für die Theorie solcher Systeme ist das *Superpositionsprinzip* für homogene Differentialgleichungen: Sind μ_1 und μ_2 Lösungen einer

¹ Mehrere Aufgaben werden grundlegende Ergebnisse aus der Stabilitätstheorie benötigen. Wir verweisen dazu insbesondere auf Satz 7.29.

homogenen Gleichung der Form (\star) , so sind auch $\mu_1 + \mu_2$ und $\lambda\mu_1$ für $\lambda \in \mathbb{R}$ Lösungen der Gleichungen, wie man unmittelbar nachrechnet.

Satz 7.15 (Lösungsraum linearer Differentialgleichungen). Sei $n \in \mathbb{N}$, $I \subseteq \mathbb{R}$ ein Intervall und $A: I \rightarrow \mathcal{M}_n(\mathbb{R})$ sowie $g: I \rightarrow \mathbb{R}$ stetige Abbildungen.

- (1) Die Lösungsmenge \mathcal{L} des homogenen Systems $x'(t) = A(t)x(t)$ wird mit der punktweisen Addition und skalaren Multiplikation zu einem n -dimensionalen Vektorraum.
- (2) Die Lösungsmenge des inhomogenen Systems $x'(t) = A(t)x(t) + g(t)$ bildet einen affinen Raum, hat also die Struktur

$$\mu_p + \mathcal{L},$$

wobei μ_p eine spezielle (sog. *partikuläre* Lösung) des inhomogenen Systems und \mathcal{L} der n -dimensionale Lösungsraum des homogenen Systems aus (1) ist.

Von besonderem Interesse ist natürlich die Angabe einer Basis des Lösungsraumes, d. h. die Angabe von n Funktionen, die linear unabhängig sind und den gesamten Lösungsraum erzeugen. Eine solche Basis wird **Fundamentalsystem** der Differentialgleichung genannt. Häufig schreibt man ihre Elemente als Spalten in eine Matrix, die dann als **Fundamentalmatrix** bezeichnet wird.

Satz 7.16. Sei $k \in \mathbb{N}$ und seien μ_1, \dots, μ_k Lösungen eines homogenen Systems von Differentialgleichungen. Dann sind äquivalent:

- (1) Die Funktionen μ_1, \dots, μ_k sind linear unabhängig.
- (2) Die Vektoren $\mu_1(t), \dots, \mu_k(t)$ sind für jedes $t \in I$ linear unabhängig.
- (3) Die Vektoren $\mu_1(t), \dots, \mu_k(t)$ sind für ein $t \in I$ linear unabhängig.

Eine einfache Möglichkeit, die lineare Unabhängigkeit von Lösungen zu prüfen, bietet die **Wronski-Determinante**. Diese ist für die Lösungen μ_1, \dots, μ_n eines Systems der Form (\star) definiert als

$$\omega(t) = \det(\mu_1(t) \mid \dots \mid \mu_n(t)).$$

Ist $\omega(t) \neq 0$ für ein $t \in I$, so sind die Vektoren $\mu_1(t), \dots, \mu_n(t)$ linear unabhängig und laut Satz 7.16 sind auch die Lösungen selbst linear unabhängig.

Systeme mit konstanten Koeffizienten

In den meisten Fällen sind im Staatsexamen alle auftretenden Koeffizienten eines Systems konstant. Hier kann ein explizites Rechenschema zur Bestimmung einer

Fundamentalmatrix angegeben werden. Wir betrachten im Folgenden für eine $(n \times n)$ -Matrix A ein System der Form

$$x' = Ax + g(t),$$

wobei wie zuvor $g: \mathbb{R} \rightarrow \mathbb{R}^n$ eine stetige Abbildung bezeichnet.

Eine zentrale Rolle werden die Eigenwerte von A spielen. Um deren Bedeutung zu verstehen, sei $\lambda \in \mathbb{R}$ ein Eigenwert von A und v ein zugehöriger Eigenvektor. Für $\mu(t) = e^{\lambda t}v$ und $t \in \mathbb{R}$ berechnet man

$$\mu'(t) = \lambda e^{\lambda t}v = (\lambda v)e^{\lambda t} = Ave^{\lambda t} = A\mu(t)$$

und sieht, dass μ eine Lösung der homogenen Differentialgleichung ist. Im Fall, dass A diagonalisierbar ist, liefert dies bereits ein erstes Verfahren zur Berechnung einer Fundamentalmatrix.

Anleitung: Bestimmung von Fundamentalmatrizen I (diagonalisierbares A)

Gegeben sei eine diagonalisierbare $(n \times n)$ -Matrix A und die Differentialgleichung $x' = Ax$, für die ein Fundamentalsystem bestimmt werden soll.

- (1) Berechne die Eigenwerte von A und Basen für die zugehörigen Eigenräume. Da A diagonalisierbar ist, ergeben sich so insgesamt n verschiedene Eigenvektoren, die linear unabhängig sind.
- (2) Definiere für jeden Eigenwert λ von A die Funktionen

$$e^{\lambda t}v_1, \dots, e^{\lambda t}v_k,$$

wobei v_1, \dots, v_k linear unabhängige Eigenvektoren zum Eigenwert λ sind (k ist also die geometrische, und zugleich algebraische, Vielfachheit von λ).

- (3) Man erhält so insgesamt n verschiedene Lösungen der Gleichung. Ferner sind die Spalten der Wronski-Matrix an der Stelle $t = 0$ durch die Eigenvektoren gegeben. Da diese linear unabhängig sind, ist $\omega(0) \neq 0$ und die Funktionen bilden ein Fundamentalsystem.

Aufgabe (Frühjahr 2007, T2A5)

Gegeben sei das Differentialgleichungssystem $\dot{x} = A(\alpha)x$ auf \mathbb{R}^2 mit

$$A(\alpha) = \begin{pmatrix} \alpha + 2 & 1 \\ -2 & \alpha - 1 \end{pmatrix}, \quad \alpha \in \mathbb{R}.$$

- a** Bestimmen Sie in Abhängigkeit von $\alpha \in \mathbb{R}$ ein Fundamentalsystem des Systems.

- b** Geben Sie jeweils die Menge aller $\alpha \in \mathbb{R}$ an, sodass $(0,0)$ ein stabiler bzw. asymptotisch stabiler Gleichgewichtspunkt des Systems $\dot{x} = A(\alpha)x$ ist.

Lösungsvorschlag zur Aufgabe (Frühjahr 2007, T2A5)

- a** Das charakteristische Polynom ist

$$\begin{aligned}\chi_{A(\alpha)} &= (\alpha + 2 - X)(\alpha - 1 - X) + 2 = \alpha^2 + \alpha - 2\alpha X - X + X^2 = \\ &= \alpha(\alpha + 1 - X) - X(\alpha + 1 - X) = (\alpha - X)(\alpha + 1 - X).\end{aligned}$$

Damit hat $A(\alpha)$ die beiden verschiedenen Eigenwerte α und $\alpha + 1$. Berechnen wir die zugehörigen Eigenräume:

$$\begin{aligned}\text{Eig}(A, \alpha) &= \ker \begin{pmatrix} 2 & 1 \\ -2 & -1 \end{pmatrix} = \ker \begin{pmatrix} 2 & 1 \\ 0 & 0 \end{pmatrix} = \left\langle \begin{pmatrix} 1 \\ -2 \end{pmatrix} \right\rangle, \\ \text{Eig}(A, \alpha + 1) &= \ker \begin{pmatrix} 1 & 1 \\ -2 & -2 \end{pmatrix} = \ker \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} = \left\langle \begin{pmatrix} 1 \\ -1 \end{pmatrix} \right\rangle\end{aligned}$$

Da geometrische und algebraische Vielfachheit bei beiden Eigenwerten jeweils 1 sind, ist A diagonalisierbar und wir behaupten, dass durch $\{\mu_1, \mu_2\}$ mit

$$\mu_1(t) = e^{\alpha t} \begin{pmatrix} 1 \\ -2 \end{pmatrix} = \begin{pmatrix} e^{\alpha t} \\ -2e^{\alpha t} \end{pmatrix}, \quad \mu_2(t) = e^{(\alpha+1)t} \begin{pmatrix} 1 \\ -1 \end{pmatrix} = \begin{pmatrix} e^{(\alpha+1)t} \\ -e^{(\alpha+1)t} \end{pmatrix}$$

ein Fundamentalsystem gegeben ist. Wir weisen dies noch explizit nach. Zunächst gilt

$$\mu'_1(t) = \begin{pmatrix} \alpha e^{\alpha t} \\ -2\alpha e^{\alpha t} \end{pmatrix} = \begin{pmatrix} \alpha + 2 & 1 \\ -2 & \alpha - 1 \end{pmatrix} \begin{pmatrix} e^{\alpha t} \\ -2e^{\alpha t} \end{pmatrix} \quad \text{und}$$

$$\mu'_2(t) = \begin{pmatrix} (\alpha + 1)e^{(\alpha+1)t} \\ -(\alpha + 1)e^{(\alpha+1)t} \end{pmatrix} = \begin{pmatrix} \alpha + 2 & 1 \\ -2 & \alpha - 1 \end{pmatrix} \begin{pmatrix} e^{(\alpha+1)t} \\ -e^{(\alpha+1)t} \end{pmatrix}.$$

Somit sind die Funktionen μ_1 und μ_2 Lösungen der Differentialgleichung. Ferner sind sie wegen

$$\omega(0) = \det \begin{pmatrix} e^{\alpha \cdot 0} & e^{(\alpha+1) \cdot 0} \\ -2e^{\alpha \cdot 0} & -e^{(\alpha+1) \cdot 0} \end{pmatrix} = \det \begin{pmatrix} 1 & 1 \\ -2 & -1 \end{pmatrix} = 1 \neq 0$$

linear unabhängig und bilden damit ein Fundamentalsystem des Systems.

b Wir verwenden Satz 7.29. Im Fall $\alpha > -1$ ist mindestens einer der Eigenwerte von $A(\alpha)$ positiv, und $(0,0)$ somit eine instabile Ruhelage. Im Fall $\alpha < -1$ sind beide Eigenwerte reell und negativ, also ist $(0,0)$ hier asymptotisch stabil. Bleibt der Fall $\alpha = -1$. Hier ist ein Eigenwert negativ, der andere 0. Da für letzteren aber algebraische und geometrische Vielfachheit übereinstimmen, handelt es sich dann bei $(0,0)$ um eine stabile Ruhelage.

Im Gros der Fälle wird A jedoch nicht diagonalisierbar sein. Das Problem liegt dann darin, dass „zu wenige“ linear unabhängige Eigenvektoren zur Verfügung stehen, also das Vorgehen aus dem obigen Kasten nicht n Funktionen liefert. Auch in diesem Fall lässt sich jedoch ein allgemeines Schema angeben.

Anleitung: Bestimmung von Fundamentalmatrizen II (nicht-diagonalisierbares A)

Gegeben sei eine nicht-diagonalisierbare $(n \times n)$ -Matrix A und die Differentialgleichung $x' = Ax$, für die ein Fundamentalsystem bestimmt werden soll.

- (1) Berechne die Eigenwerte von A .
- (2) Bestimme für jeden Eigenwert λ gemäß dem Vorgehen im Kasten auf Seite 249 k linear unabhängige (verallgemeinerte) Eigenvektoren, wobei k die algebraische Vielfachheit von λ bezeichnet.
- (3) Definiere nun für jeden Eigenwert λ die k Funktionen

$$e^{\lambda t}v_1, \quad (v_2 + tv_1)e^{\lambda t}, \quad \dots, \quad e^{\lambda t} \left(v_k + \dots + t^{k-1}v_1 \right).$$

- (4) Die Wronski-Determinante an der Stelle $t = 0$ besteht aus (verallgemeinerten) Eigenvektoren, ist also invertierbar und die Funktionen bilden somit ein Fundamentalsystem.

Aufgabe (Herbst 2003, T1A3)

Bestimmen Sie ein Fundamentalsystem zu $y' = Ay$ mit

$$A = \begin{pmatrix} 1 & 1 & 1 \\ -1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}.$$

Lösungsvorschlag zur Aufgabe (Herbst 2003, T1A3)

Mit der Sarrus-Regel erhält man das charakteristische Polynom

$$\begin{aligned}\chi_A &= (1 - X)(-X)^2 + 1 - 1 - (-X) - (1 - X) - X = \\ &= (1 - X)X^2 - (1 - X) = (1 - X)(X^2 - 1) = -(X - 1)^2(X + 1).\end{aligned}$$

Somit hat A die Eigenwerte $\lambda_1 = 1$ (mit algebraischer Vielfachheit 2) und $\lambda_2 = -1$ (mit algebraischer Vielfachheit 1).

Für den Eigenraum zum Eigenwert λ_1 erhalten wir

$$\text{Eig}(A, 1) = \ker \begin{pmatrix} 0 & 1 & 1 \\ -1 & -1 & 1 \\ 1 & 1 & -1 \end{pmatrix} = \ker \begin{pmatrix} 1 & 0 & -2 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix} = \left\langle \begin{pmatrix} 2 \\ -1 \\ 1 \end{pmatrix} \right\rangle.$$

Analog ergibt sich

$$\text{Eig}(A, -1) = \ker \begin{pmatrix} 2 & 1 & 1 \\ -1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix} = \ker \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix} = \left\langle \begin{pmatrix} 0 \\ -1 \\ 1 \end{pmatrix} \right\rangle.$$

Damit hat der Eigenwert 1 geometrische Vielfachheit 1, diese stimmt nicht mit der algebraischen überein und A ist laut Satz 4.5 (3) nicht diagonalisierbar. Wir berechnen den verallgemeinerten Eigenraum zweiter Stufe zum Eigenwert 1

$$\begin{aligned}\text{Eig}^2(A, 1) &= \ker(A - 1 \cdot \mathbb{E}_3)^2 = \ker \begin{pmatrix} 0 & 1 & 1 \\ -1 & -1 & 1 \\ 1 & 1 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 & 1 \\ -1 & -1 & 1 \\ 1 & 1 & -1 \end{pmatrix} = \\ &= \ker \begin{pmatrix} 0 & 0 & 0 \\ 2 & 1 & -3 \\ -2 & -1 & 3 \end{pmatrix} = \ker \begin{pmatrix} 2 & 1 & -3 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = \left\langle \begin{pmatrix} -1 \\ 2 \\ 0 \end{pmatrix}, \begin{pmatrix} 3 \\ 0 \\ 2 \end{pmatrix} \right\rangle.\end{aligned}$$

Der erste Vektor liegt nicht in $\text{Eig}(A, 1)$, sodass wir diesen als verallgemeinerten Eigenvektor verwenden und den zugehörigen Eigenvektor berechnen:

$$\begin{pmatrix} 0 & 1 & 1 \\ -1 & -1 & 1 \\ 1 & 1 & -1 \end{pmatrix} \begin{pmatrix} -1 \\ 2 \\ 0 \end{pmatrix} = \begin{pmatrix} 2 \\ -1 \\ 1 \end{pmatrix} \in \text{Eig}(A, 1)$$

Damit sind wir in der Lage, ein Fundamentalsystem anzugeben. Wir definieren dazu die drei Abbildungen

$$\begin{pmatrix} 0 \\ -e^{-t} \\ e^{-t} \end{pmatrix}, \quad \begin{pmatrix} 2e^t \\ -e^t \\ e^t \end{pmatrix}, \quad \text{und} \quad \left[\begin{pmatrix} -1 \\ 2 \\ 0 \end{pmatrix} + t \begin{pmatrix} 2 \\ -1 \\ 1 \end{pmatrix} \right] e^t = \begin{pmatrix} (2t-1)e^t \\ (-t+2)e^t \\ te^t \end{pmatrix}.$$

Diese Abbildungen sind Lösungen der Gleichung, was man unmittelbar nachrechnet, und linear unabhängig laut Satz 7.16, denn es ist

$$\omega(0) = \det \begin{pmatrix} 0 & 2 & -1 \\ -1 & -1 & 2 \\ 1 & 1 & 0 \end{pmatrix} = 4 \neq 0.$$

Aufgabe (Frühjahr 2012, T3A5)

Gegeben sei die Matrix

$$A = \begin{pmatrix} 1 & -1 & 1 \\ 1 & -1 & 0 \\ 1 & 0 & -1 \end{pmatrix}.$$

Man bestimme ein Fundamentalsystem des homogenen Differentialgleichungssystems $x' = Ax$.

Lösungsvorschlag zur Aufgabe (Frühjahr 2012, T3A5)

Da diese Aufgabe völlig analog zur vorhergehenden verläuft, skizzieren wir hier nur die Zwischenergebnisse kurz.

Mittels des charakteristischen Polynoms $\chi_A = -(X-1)(X+1)^2$ erhält man die Eigenwerte $\lambda_1 = 1$ (einfach) und $\lambda_2 = -1$ (doppelt). Die Eigenräume sowie der benötigte verallgemeinerte Eigenraum berechnen sich zu

$$\text{Eig}(A, 1) = \left\langle \begin{pmatrix} 2 \\ 1 \\ 1 \end{pmatrix} \right\rangle, \quad \text{Eig}(A, -1) = \left\langle \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} \right\rangle,$$

$$\text{Eig}^2(A, -1) = \left\langle \begin{pmatrix} 1 \\ 2 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ -2 \end{pmatrix} \right\rangle.$$

Man verwendet (beispielsweise) den ersten erzeugenden Vektor des verallgemeinerten Eigenraums und erhält $(A + \mathbb{E}_3)(1, 2, 0) = (0, 1, 1)$. Ein Fundamentalsystem ist nun gegeben durch

$$e^t \begin{pmatrix} 2 \\ 1 \\ 1 \end{pmatrix}, \quad e^{-t} \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}, \quad \text{und} \quad e^{-t} \left[\begin{pmatrix} 1 \\ 2 \\ 0 \end{pmatrix} + t \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} \right] = e^{-t} \begin{pmatrix} 1 \\ 2+t \\ t \end{pmatrix},$$

wie man wie zuvor überprüft.

Aufgabe (Frühjahr 2005, T1A3)

Bestimmen Sie ein Fundamentalsystem von Lösungen zu

$$\frac{d}{dt} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 1 & 1 & -1 \\ 0 & -1 & 2 \\ -2 & -1 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix}.$$

Welche Lösungen bleiben für $t \rightarrow +\infty$ beschränkt?

Lösungsvorschlag zur Aufgabe (Frühjahr 2005, T1A3)

Das charakteristische Polynom der Koeffizientenmatrix A ist

$$\chi_A = -(X+1)(X-1)^2.$$

Damit ergeben sich -1 als einfacher und $+1$ als doppelter Eigenwert. Es ergeben sich die Eigenräume

$$\text{Eig}(A, +1) = \left\langle \begin{pmatrix} -1 \\ 2 \\ 2 \end{pmatrix} \right\rangle \quad \text{und} \quad \text{Eig}(A, -1) = \left\langle \begin{pmatrix} 1 \\ -2 \\ 0 \end{pmatrix} \right\rangle.$$

Somit ist A nicht diagonalisierbar. Es ergibt sich jedoch für den verallgemeinerten Eigenraum zum Eigenwert 1

$$\ker(A - \mathbb{E}_3)^2 = \ker \begin{pmatrix} 2 & -1 & 2 \\ -4 & 2 & -4 \\ 0 & 0 & 0 \end{pmatrix} = \left\langle \begin{pmatrix} 1 \\ 2 \\ 0 \end{pmatrix}, \begin{pmatrix} -1 \\ 0 \\ 1 \end{pmatrix} \right\rangle.$$

Wir berechnen ferner $(A - \mathbb{E}_3)(1, 0, -1) = (-1, 2, 2) \in \text{Eig}(A, +1)$ und behaupten nun, dass $\{\mu_1, \mu_2, \mu_3\}$ mit

$$\begin{aligned}\mu_1(t) &= e^{-t} \begin{pmatrix} 1 \\ -2 \\ 0 \end{pmatrix}, \quad \mu_2(t) = e^t \begin{pmatrix} -1 \\ 2 \\ 2 \end{pmatrix}, \quad \text{und} \\ \mu_3(t) &= e^t \left[\begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix} + t \begin{pmatrix} -1 \\ 2 \\ 2 \end{pmatrix} \right] = e^t \begin{pmatrix} 1-t \\ 2t \\ -1+2t \end{pmatrix}\end{aligned}$$

ein Fundamentalsystem ist. Zur Überprüfung rechnet man nach, dass die Funktionen Lösungen sind, und zeigt mit der Wronski-Determinante, dass sie linear unabhängig sind.

Alle Lösungen der Differentialgleichung sind Linearkombinationen dieser Lösungen. Da die letzten beiden für $t \rightarrow \infty$ divergieren, kommen als beschränkte Lösungen nur Lösungen der Form $c\mu_1$ für $c \in \mathbb{R}$ in Frage.

Eine Systematisierung der beiden bisher vorgestellten Methoden ist das sogenannte Matrix-Exponential. Dies ist für eine Matrix A definiert als

$$e^A = \sum_{k=0}^{\infty} \frac{A^k}{k!}.$$

Wir fassen einige wichtige Rechenregeln für das Matrix-Exponential der Gestalt e^{tA} für ein $t \in \mathbb{R}$ zusammen, von denen viele direkte Analogien zum skalaren Fall sind.

Proposition 7.17. Seien $A, B \in \mathcal{M}_{n(\mathbb{R})}$ und $t \in \mathbb{R}$.

- (1) Es ist $e^{0 \cdot A} = \mathbb{E}_n$ und $(e^{tA})^{-1} = e^{-tA}$.
- (2) Gilt $AB = BA$, so ist $e^{tA}e^{tB} = e^{t(A+B)}$.
- (3) Gilt $B = TAT^{-1}$ für eine invertierbare Matrix T , so ist $e^{tB} = Te^{tA}T^{-1}$.
- (4) Für Diagonalmatrizen und Jordan-Blöcke der Größe ν gelten

$$e^{t \begin{pmatrix} \lambda_1 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & \lambda_n \end{pmatrix}} = \begin{pmatrix} e^{t\lambda_1} & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & e^{t\lambda_n} \end{pmatrix}$$

bzw.

$$e^{\begin{pmatrix} \lambda & 1 & & 0 \\ & \ddots & \ddots & \\ t & & \ddots & 1 \\ & 0 & & \lambda \end{pmatrix}} = \begin{pmatrix} e^{\lambda t} & te^{\lambda t} & \frac{t^2}{2!}e^{\lambda t} & \dots & \frac{t^{v-1}}{(v-1)!}e^{\lambda t} \\ \vdots & \ddots & \ddots & & \vdots \\ & \ddots & \ddots & \frac{t^2}{2!}e^{\lambda t} & \\ 0 & & \ddots & te^{\lambda t} & e^{\lambda t} \end{pmatrix}$$

Anleitung: Bestimmung des Matrix-Exponentials

Sei A eine reelle $(n \times n)$ -Matrix, für die e^{tA} bestimmt werden soll.

- (1) Berechne die Eigenwerte und zugehörigen Eigenräume von A und prüfe mit Satz 4.5, ob A diagonalisierbar ist.
 - (a) Falls ja, berechne eine Transformationsmatrix T , sodass $D = T^{-1}AT$ eine Diagonalmatrix ist.
 - (b) Falls nein, so kann A auf jeden Fall über \mathbb{C} in Jordan-Normalform gebracht werden. Bestimme also eine Transformationsmatrix T , sodass $J = T^{-1}AT$ in Jordan-Normalform vorliegt.

Für die beiden Verfahren sei auf die Kästen auf Seite 237 bzw. Seite 249 verwiesen.

- (2) Berechne mit Proposition 7.17 (4) die Matrizen e^{tJ} bzw. e^{tD} .
- (3) Verwende Proposition 7.17 (3), um e^{tA} auszurechnen.

Für jedes $\tau \in \mathbb{R}$ bezeichnet man diejenige Fundamentalmatrix, die an der Stelle τ mit der Einheitsmatrix \mathbb{E}_n übereinstimmt, als **Übergangsmatrix** und notiert sie als $\Lambda(t, \tau)$. Es gilt für eine beliebige Fundamentalmatrix $\Phi(t)$ die Formel

$$\Lambda(t, \tau) = \Phi(t)\Phi(\tau)^{-1}.$$

Ist $\Phi(t) = e^{tA}$, so vereinfacht sich der Ausdruck entsprechend zu

$$\Lambda(t, \tau) = e^{tA}e^{-\tau A} = e^{(t-\tau)A}.$$

Damit sind wir in der Lage, eine einfache Formel zur Lösung von Anfangswertproblemen anzugeben.

Anleitung: Lösen von Anfangswertproblemen

Gegeben sei ein Intervall $I \subseteq \mathbb{R}$, $\tau \in I$, $\xi \in \mathbb{R}^n$, eine stetige Abbildung $g: I \rightarrow \mathbb{R}^n$ sowie das Anfangswertproblem

$$\dot{x} = Ax + g(t), \quad x(\tau) = \xi.$$

- (1) Berechne eine Fundamentalmatrix $\Phi(t)$ für die homogene Differentialgleichung $\dot{x} = Ax$.

- (2) Berechne die Übergangsmatrix $\Lambda(t, \tau) = \Phi(t)\Phi(\tau)^{-1}$.

Im Fall einer inhomogenen Gleichung muss zudem die allgemeine Übergangsmatrix $\Lambda(t, s)$ für $s \in I$ bestimmt werden.

- (3) Die Lösung des homogenen Anfangswertproblems ist gegeben durch

$$\mu(t) = \Lambda(t, \tau)\xi \quad \text{für } t \in I.$$

- (4) Die Lösung des inhomogenen Anfangswertproblems erhält man durch **Variation der Konstanten**:

$$\mu(t) = \Phi(t) \left[\Phi^{-1}(\tau)\xi + \int_{\tau}^t \Phi^{-1}(s)g(s)ds \right] = \Lambda(t, \tau)\xi + \int_{\tau}^t \Lambda(t, s)g(s)ds.$$

Das Integral über den Vektor $\Phi^{-1}(s)g(s)$ (bzw. $\Lambda(t, s)g(s)$) ist dabei komponentenweise zu berechnen.

Es sei an dieser Stelle erwähnt, dass die Berechnung eines Fundamentalsystems durch Angabe von e^{tA} aufwendiger ist als die bisher besprochenen Vorgehensweisen – jedoch kann hier die Inverse der Fundamentalmatrix einfach als $e^{(-t)A}$ angegeben werden. Als **Faustregel**: Handelt es sich um eine homogene Differentialgleichung, so ist die Angabe eines Fundamentalsystems mittels des Vorgehens auf Seite 429 schneller, bei inhomogenen Systemen ist es vorteilhafter, e^{tA} wie eben dargestellt zu berechnen.

Aufgabe (Frühjahr 2011, T3A1)

Seien

$$A = \begin{pmatrix} 0 & 0 & -1 \\ 0 & -1 & 0 \\ 1 & 0 & 2 \end{pmatrix}, \quad b: \mathbb{R} \rightarrow \mathbb{R}^3, b(t) = \begin{pmatrix} -t \\ e^{-t} \\ 1+t \end{pmatrix}.$$

- a** Berechnen Sie ein Fundamentalsystem für die Differentialgleichung $\dot{x} = Ax$.

b Berechnen Sie die maximale Lösung des Anfangswertproblems

$$\dot{x} = Ax + b(t), \quad x(0) = \begin{pmatrix} 1 \\ 3 \\ -2 \end{pmatrix}.$$

Lösungsvorschlag zur Aufgabe (Frühjahr 2011, T3A1)

a Wir berechnen e^{tA} . Aus dem charakteristischen Polynom $\chi_A = -(X+1)(X-1)^2$ ergeben sich die Eigenwerte $\lambda_1 = -1$ (einfach) und $\lambda_2 = 1$ (doppelt). Die zugehörigen Eigenräume sind gegeben durch

$$\text{Eig}(A, 1) = \left\langle \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix} \right\rangle \quad \text{und} \quad \text{Eig}(A, -1) = \left\langle \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \right\rangle.$$

Damit ist die Matrix wiederum nicht diagonalisierbar. Wir berechnen den verallgemeinerten Eigenraum zweiter Stufe und erhalten

$$\text{Eig}^2(A, 1) = \ker \begin{pmatrix} 0 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 0 \end{pmatrix} = \left\langle \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \right\rangle.$$

Rückwärts-Einsetzen ergibt

$$(A - \mathbb{E}_3) \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} -1 \\ 0 \\ 1 \end{pmatrix} \in \text{Eig}(A, 1)$$

und damit die Transformationsmatrix

$$T = \begin{pmatrix} -1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \quad \text{mit} \quad T^{-1} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

Wie erwartet, liegt nun

$$J = T^{-1}AT = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & -1 \\ 0 & -1 & 0 \\ 1 & 0 & 2 \end{pmatrix} \begin{pmatrix} -1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$$

in Jordan-Normalform vor.

Somit ergibt sich mit Proposition 7.17 (3):

$$\begin{aligned}\Phi(t) = e^{tA} &= \begin{pmatrix} -1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} e^t & te^t & 0 \\ 0 & e^t & 0 \\ 0 & 0 & e^{-t} \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} = \\ &= \begin{pmatrix} -1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} te^t & 0 & e^t + te^t \\ e^t & 0 & e^t \\ 0 & e^{-t} & 0 \end{pmatrix} = \begin{pmatrix} e^t - te^t & 0 & -te^t \\ 0 & e^{-t} & 0 \\ te^t & 0 & e^t + te^t \end{pmatrix}.\end{aligned}$$

b Hier ist Variation der Konstanten anzuwenden. Wir verwenden die Formel

$$\mu(t) = \Phi(t) \left[\Phi^{-1}(0) \begin{pmatrix} 1 \\ 3 \\ -2 \end{pmatrix} + \int_0^t \Phi^{-1}(s) \begin{pmatrix} -s \\ e^{-s} \\ 1+s \end{pmatrix} ds \right].$$

Mit $\Phi^{-1}(s) = (e^{sA})^{-1} = e^{-sA}$ ergibt sich für das hintere Integral

$$\begin{aligned}&\int_0^t \begin{pmatrix} e^{-s} + se^{-s} & 0 & se^{-s} \\ 0 & e^s & 0 \\ -se^{-s} & 0 & e^{-s} - se^{-s} \end{pmatrix} \begin{pmatrix} -s \\ e^{-s} \\ 1+s \end{pmatrix} ds = \\ &= \int_0^t \begin{pmatrix} 0 \\ 1 \\ e^{-s} \end{pmatrix} ds = \begin{pmatrix} 0 \\ t \\ -e^{-t} + 1 \end{pmatrix}.\end{aligned}$$

Damit erhält man für die gesamte Lösung mit $\Phi^{-1}(0) = \mathbb{E}_3$:

$$\mu(t) = \begin{pmatrix} e^t - te^t & 0 & -te^t \\ 0 & e^{-t} & 0 \\ te^t & 0 & e^t + te^t \end{pmatrix} \begin{pmatrix} 1 \\ t+3 \\ -e^{-t} - 1 \end{pmatrix} = \begin{pmatrix} e^t + t \\ (t+3)e^{-t} \\ -e^t - t - 1 \end{pmatrix}.$$

Das sollten wir aber nun überprüfen. Es gilt $\mu(0) = (1, 3, -2)$ und

$$\mu'(t) = \begin{pmatrix} e^t + 1 \\ e^{-t} - (t+3)e^{-t} \\ -e^t - 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 & -1 \\ 0 & -1 & 0 \\ 1 & 0 & 2 \end{pmatrix} \begin{pmatrix} e^t + t \\ (t+3)e^{-t} \\ -e^t - t - 1 \end{pmatrix} + \begin{pmatrix} -t \\ e^{-t} \\ 1+t \end{pmatrix}$$

#passt.

Aufgabe (Herbst 2015, T1A4)

Es sei $A: \mathbb{R} \rightarrow \mathbb{R}^{n \times n}$ eine stetige, matrixwertige Funktion. Betrachten Sie die zugehörige Differentialgleichung

$$\dot{x} = A(t)x. \quad (1)$$

- a** Es seien $x_1(t), \dots, x_n(t), t \in \mathbb{R}$, Lösungen von (1). Ferner seien für ein $t_0 \in \mathbb{R}$ die Vektoren $x_1(t_0), \dots, x_n(t_0)$ im \mathbb{R}^n linear unabhängig. Zeigen Sie, dass dann für alle $t_1 \in \mathbb{R}$ die Vektoren $x_1(t_1), \dots, x_n(t_1)$ im \mathbb{R}^n linear unabhängig sind.

Hinweis Benutzen Sie das Superpositionsprinzip für lineare homogene Differentialgleichungen oder benutzen Sie die Differentialgleichung für Wronski-Determinanten.

- b** Erklären Sie die Begriffe Fundamentalmatrix und Übergangsmatrix (auch Transitionsmatrix oder Hauptfundamentalmatrix genannt). Wie erhält man aus **a** eine Fundamentalmatrix und wie lässt sich die Lösung von (1) mit Anfangswert $x(t_0) = x_0 \in \mathbb{R}^n, t_0 \in \mathbb{R}$, mithilfe der Übergangsmatrix ausdrücken?
- c** Zeigen Sie: Sind $\Phi_1(t), \Phi_2(t), t \in \mathbb{R}$, Fundamentalmatrizen, so existiert eine Matrix $C \in \mathbb{R}^{n \times n}$ mit

$$\Phi_1(t) = \Phi_2(t)C, \quad t \in \mathbb{R}.$$

Lösungsvorschlag zur Aufgabe (Herbst 2015, T1A4)

- a** Seien $a_1, \dots, a_n \in \mathbb{R}$ so, dass

$$a_1x_1(t_1) + \dots + a_nx_n(t_1) = 0$$

erfüllt ist. Nach dem Superpositionsprinzip für lineare homogene Differentialgleichungen ist dann auch

$$\mu(t) = a_1x_1(t) + \dots + a_nx_n(t)$$

eine Lösung von $\dot{x} = A(t)x$. Als lineare Differentialgleichung besitzt diese Differentialgleichung zu jedem Anfangswert eine eindeutige maximale Lösung. Wegen

$$\mu(t_1) = a_1x_1(t_1) + \dots + a_nx_n(t_1) = 0$$

hat die Lösungskurve von $\mu(t)$ einen gemeinsamen Punkt mit der Nulllösung $\nu: \mathbb{R} \rightarrow \mathbb{R}^n$. Da es sich bei letzterer um die eindeutige maximale Lösung zum Anfangswert $x(t_1) = 0$ handelt, folgt $\mu = \nu$ auf dem Definitionsbereich von μ . Insbesondere gilt

$$\mu(t_0) = a_1x_1(t_0) + \dots + a_nx_n(t_0) = 0.$$

Da die Vektoren $x_1(t_0), \dots, x_n(t_0)$ nach Voraussetzung linear unabhängig sind, folgt $a_1 = \dots = a_n = 0$. Dies bedeutet gerade, dass auch die Vektoren $x_1(t_1), \dots, x_n(t_1)$ linear unabhängig sind.

- b** Eine $(n \times n)$ -Matrix $\Phi(t)$, deren Spalten aus linear unabhängigen Lösungen einer n -dimensionalen Differentialgleichung nennt man *Fundamentalmatrix*. Die Matrix $\Lambda(t, \tau) = \Phi(t)\Phi^{-1}(\tau)$ nennt man in diesem Fall *Übergangsmatrix*. Die Lösung von (1) zum Anfangswert $x(t_0) = x_0$ schreibt sich dann als

$$\lambda_{(t_0, x_0)}(t) = \Lambda(t, t_0)x_0.$$

- c** Nach Teil **b** gilt

$$\lambda_{(t_0, x_0)} = \Phi_1(t)\Phi_1^{-1}(t_0)x_0 = \Phi_2(t)\Phi_2^{-1}(t_0)x_0$$

für alle $x_0 \in \mathbb{R}^n$ und $t_0, t \in \mathbb{R}$. Daher folgt

$$\Phi_1(t)\Phi_1^{-1}(t_0) = \Phi_2(t)\Phi_2^{-1}(t_0) \Leftrightarrow \Phi_1(t) = \Phi_2(t)\Phi_2^{-1}(t_0)\Phi_1(t_0).$$

Setze also $C = \Phi_2^{-1}(t_0)\Phi_1(t_0)$.

Komplexe Eigenwerte

In aller Regel wird man darauf abzielen, reelle Lösungen anzugeben, sollte das angegebene System reell sein. Ein Problem ist das, wenn Eigenwerte (und damit auch die zugehörigen Eigenvektoren) komplex sind. In jedem Fall müssen komplexe Eigenwerte reeller Matrizen als komplex-konjugierte Paare auftreten, so dass auch die zugehörigen Lösungen im Fundamentalsystem komplex-konjugiert zueinander sind. Nun gilt aber für eine beliebige komplexe Zahl $z \in \mathbb{C}$

$$\operatorname{Re} z = \frac{1}{2}z + \frac{1}{2}\bar{z} \quad \text{und} \quad \operatorname{Im} z = \frac{1}{2i}z - \frac{1}{2i}\bar{z}.$$

Damit sind auch Real- und Imaginärteil einer solchen Lösung wieder (reelle!) Lösungen der DGL. Anstatt des komplex-konjugierten Paares kann im Fundamentalsystem also schlicht der Real- und Imaginärteil *einer* der Lösungen verwendet werden. Die folgenden Aufgaben demonstrieren dies.

Aufgabe (Herbst 2012, T1A2)

Sei

$$A = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \in M(2 \times 2, \mathbb{R}).$$

Geben sie ein Fundamentalsystem reeller Lösungen des linearen Gleichungssystems

$$\dot{y} = Ay$$

an und untersuchen Sie, ob es stabile Lösungen besitzt. Berechnen Sie auch die Lösung, die der Anfangsbedingung $y(0) = (2, 0)^T$ genügt, und begründen Sie, warum diese Lösung eindeutig ist.

Lösungsvorschlag zur Aufgabe (Herbst 2012, T1A2)

Es gilt

$$\chi_A = (1 - X)^2 + 1 = X^2 - 2X + 2.$$

Die Nullstellen sind gegeben durch

$$\lambda_{1,2} = \frac{2 \pm \sqrt{-4}}{2} = 1 \pm i.$$

Berechnen wir einen zugehörigen Eigenraum:

$$\text{Eig}(A, 1+i) = \ker \begin{pmatrix} -i & -1 \\ 1 & -i \end{pmatrix} = \ker \begin{pmatrix} 1 & -i \\ 0 & 0 \end{pmatrix} = \left\langle \begin{pmatrix} 1 \\ -i \end{pmatrix} \right\rangle.$$

Eine Lösung ist nun die Funktion $\mu(t) = \begin{pmatrix} 1 \\ -i \end{pmatrix} e^{(1+i)t}$, die wir gemäß der Bemerkung oben in Real- und Imaginärteil zerlegen:

$$\begin{aligned} \mu(t) &= \begin{pmatrix} 1 \\ -i \end{pmatrix} e^{(1+i)t} = \begin{pmatrix} 1 \\ -i \end{pmatrix} e^t e^{it} = \begin{pmatrix} 1 \\ -i \end{pmatrix} e^t (\cos t + i \sin t) = \\ &= \begin{pmatrix} e^t \cos t \\ e^t \sin t \end{pmatrix} + i \begin{pmatrix} e^t \sin t \\ -e^t \cos t \end{pmatrix}. \end{aligned}$$

Wir zeigen nun, dass es sich dabei wirklich um ein Fundamentalsystem handelt: Zunächst gilt

$$\frac{d}{dt} \begin{pmatrix} e^t \cos t \\ e^t \sin t \end{pmatrix} = \begin{pmatrix} -e^t \sin t + e^t \cos t \\ e^t \cos t + e^t \sin t \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} e^t \cos t \\ e^t \sin t \end{pmatrix}$$

und

$$\frac{d}{dt} \begin{pmatrix} e^t \sin t \\ -e^t \cos t \end{pmatrix} = \begin{pmatrix} e^t \cos t + e^t \sin t \\ e^t \sin t - e^t \cos t \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} e^t \sin t \\ -e^t \cos t \end{pmatrix}.$$

Zum Nachweis, dass die beiden Lösungen linear unabhängig sind, berechnen wir die Wronski-Determinante:

$$\omega(0) = \det(\mu_1(0) \mid \mu_2(0)) = \det \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = -1 \neq 0$$

Voller Stolz präsentieren wir also das reelle Fundamentalsystem

$$\left\{ \begin{pmatrix} e^t \cos t \\ e^t \sin t \end{pmatrix}, \begin{pmatrix} e^t \sin t \\ -e^t \cos t \end{pmatrix} \right\}.$$

Um das Anfangswertproblem zu lösen, verwenden wir die Formel (3) aus dem Kasten auf Seite 435 und erhalten

$$\begin{aligned} \lambda(t) &= \Phi(t)\Phi^{-1}(0) \begin{pmatrix} 2 \\ 0 \end{pmatrix} = \begin{pmatrix} e^t \cos t & e^t \sin t \\ e^t \sin t & -e^t \cos t \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 2 \\ 0 \end{pmatrix} = \\ &= \begin{pmatrix} e^t \cos t & e^t \sin t \\ e^t \sin t & -e^t \cos t \end{pmatrix} \begin{pmatrix} 2 \\ 0 \end{pmatrix} = \begin{pmatrix} 2e^t \cos t \\ 2e^t \sin t \end{pmatrix}. \end{aligned}$$

Dass diese Lösung der geforderten Anfangsbedingung entspricht, sieht man unmittelbar.

Es handelt sich bei $\dot{y} = Ay$ um eine Differentialgleichung mit linear beschränkter rechter Seite: Die Zuordnung $x \mapsto Ax$ ist als lineare Abbildung stetig differenzierbar (und damit Lipschitz-stetig) und es gilt für eine beliebige Norm $\|\cdot\|$ mit induzierter Matrix-Norm $\|\cdot\|$, dass

$$\|Ay\| \leq \|A\| \cdot \|y\|.$$

Damit existiert für jedes Anfangswertproblem eine eindeutige, auf ganz \mathbb{R} definierte Lösung.

Da die Eigenwerte positiven Realteil besitzen, sind sämtliche Lösungen instabil laut Satz 7.29.

Aufgabe (Herbst 2011, T1A4)

Berechnen Sie die Lösung des Anfangswertproblems

$$\dot{x}(t) = \begin{pmatrix} 0 & -1 & 1 \\ 1 & 0 & 3 \\ 0 & 0 & -1 \end{pmatrix} x(t) + \begin{pmatrix} -4 \\ -2 \\ 2 \end{pmatrix} e^t, \quad x(0) = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}.$$

Lösungsvorschlag zur Aufgabe (Herbst 2011, T1A4)

Diese Aufgabe wird auf Variation der Konstanten hinauslaufen. Dazu berechnen wir zunächst ein Fundamentalsystem der homogenen Differentialgleichung. Die Koeffizientenmatrix A hat das charakteristische Polynom

$$\det \begin{pmatrix} -X & -1 & 1 \\ 1 & -X & 3 \\ 0 & 0 & -1-X \end{pmatrix} = -X^2(X+1) - (X+1) = -(X+1)(X^2+1).$$

und die Eigenwerte $\lambda_1 = -1$ sowie $\lambda_{2,3} = \pm i$. Weiter mit den Eigenräumen:

$$\text{Eig}(A, -1) = \left\langle \begin{pmatrix} -2 \\ -1 \\ 1 \end{pmatrix} \right\rangle \quad \text{und} \quad \text{Eig}(A, i) = \left\langle \begin{pmatrix} i \\ 1 \\ 0 \end{pmatrix} \right\rangle.$$

Für λ_2 erhalten wir eine komplexe Lösung, die wir wie zuvor zerlegen

$$e^{it} \begin{pmatrix} i \\ 1 \\ 0 \end{pmatrix} = (\cos t + i \sin t) \begin{pmatrix} i \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} -\sin t \\ \cos t \\ 0 \end{pmatrix} + i \begin{pmatrix} \cos t \\ \sin t \\ 0 \end{pmatrix}.$$

und damit die Fundamentalmatrix

$$\Phi(t) = \begin{pmatrix} -2e^{-t} & -\sin t & \cos t \\ -e^{-t} & \cos t & \sin t \\ e^{-t} & 0 & 0 \end{pmatrix}.$$

erhalten. Eine etwas langwierige, aber wenig aufregende, Rechnung liefert

$$\Phi^{-1}(t) = \begin{pmatrix} 0 & 0 & e^t \\ -\sin t & \cos t & -2\sin t + \cos t \\ \cos t & \sin t & 2\cos t + \sin t \end{pmatrix}.$$

Schlussendlich setzen wir in die Formel aus der Variation der Konstanten ein:

$$\begin{aligned} \mu(t) &= \Phi(t) \left[\Phi^{-1}(0) \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} + \int_0^t e^s \Phi^{-1}(s) \begin{pmatrix} -4 \\ -2 \\ 2 \end{pmatrix} ds \right] = \\ &= \begin{pmatrix} -2e^{-t} & -\sin t & \cos t \\ -e^{-t} & \cos t & \sin t \\ e^{-t} & 0 & 0 \end{pmatrix} \left[\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 2 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} + \int_0^t \begin{pmatrix} 2e^{2s} \\ 0 \\ 0 \end{pmatrix} ds \right] = \end{aligned}$$

und weiter

$$\begin{aligned}\mu(t) &= \begin{pmatrix} -2e^{-t} & -\sin t & \cos t \\ -e^{-t} & \cos t & \sin t \\ e^{-t} & 0 & 0 \end{pmatrix} \left[\begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} + \begin{pmatrix} [e^{2s}]_0^t \\ 0 \\ 0 \end{pmatrix} \right] = \\ &= \begin{pmatrix} -2e^{-t} & -\sin t & \cos t \\ -e^{-t} & \cos t & \sin t \\ e^{-t} & 0 & 0 \end{pmatrix} \begin{pmatrix} e^{2t} \\ 2 \\ 3 \end{pmatrix} = \begin{pmatrix} -2e^t - 2\sin t + 3\cos t \\ -e^t + 2\cos t + 3\sin t \\ e^t \end{pmatrix}\end{aligned}$$

Nicht-konstante Koeffizienten

Im Fall, dass die Einträge der Matrix $A(t)$ tatsächlich von t abhängen, sind die bisher verwendeten Methoden nicht mehr zielführend. Oftmals besteht ein Lösungsansatz darin, die beiden Gleichungen getrennt von einander zu lösen (was z. B. möglich ist, wenn es sich um Dreiecksmatrizen handelt).

Aufgabe (Frühjahr 2014, T2A2)

Gegeben sei die matrixwertige Funktion $A:]-1, 1[\rightarrow \mathbb{R}^{2 \times 2}, t \mapsto \begin{pmatrix} 2t & t \\ 0 & \frac{2t}{t^2-1} \end{pmatrix}$.

Zeigen Sie, dass das Anfangswertproblem

$$x'(t) = A(t)x(t), \quad x(0) = \begin{pmatrix} 2 \\ 1 \end{pmatrix}$$

eine eindeutige maximale Lösung besitzt und berechnen Sie diese.

Lösungsvorschlag zur Aufgabe (Frühjahr 2014, T2A2)

Die Existenz und Eindeutigkeit der Lösung folgt aus dem Globalen Existenz- und Eindeutigkeitssatz für Differentialgleichungen mit linear beschränkter rechter Seite. Sei dazu $\|\cdot\|$ eine Norm und $\|\|\cdot\|\|$ die induzierte Matrix-Norm. Dann definiert $t \mapsto \|\|A(t)\|\|$ eine stetige Zuordnung (als Verkettung zweier stetiger Abbildungen) und es gilt

$$\|x'(t)\| \leq \|\|A(t)\|\| \cdot \|x(t)\|.$$

Da ferner die DGL auf dem Gebiet $] -1, 1[\times \mathbb{R}^2$ definiert ist und die Abbildung $(t, x) \mapsto A(t)x$ stetig differenzierbar ist, sind alle Voraussetzungen des Satzes erfüllt. Die Lösung des gegebenen Anfangswertproblems ist also eindeutig und existiert auf ganz $] -1, 1[$.

Der wesentliche Schritt bei der expliziten Lösung besteht darin, zu erkennen, dass die Gleichung für $x_2(t)$ unabhängig von $x_1(t)$ ist. Wir können uns also zunächst ganz dieser Gleichung mittels Trennen der Variablen widmen:

$$\begin{aligned} x'_2(t) = \frac{2t}{t^2 - 1} x_2(t) &\Leftrightarrow \int_1^{\mu(t)} \frac{1}{x} dx = \int_0^t \frac{2\tau}{\tau^2 - 1} d\tau \\ [\ln|x|]_1^{\mu(t)} = [\ln|\tau^2 - 1|]_0^t &\Leftrightarrow \ln|\mu(t)| = \ln|t^2 - 1| \Leftrightarrow \mu(t) = \pm(t^2 - 1). \end{aligned}$$

Unter Berücksichtigung der Anfangswertbedingung $x_2(0) = 1$ erhält man die Lösung $x_2:]-1, 1[\rightarrow \mathbb{R}, t \mapsto 1 - t^2$. Für die erste Gleichung ist nun noch

$$x'_1(t) = 2tx_1(t) + tx_2(t) = 2tx_1(t) + t - t^3.$$

zu lösen. Hierfür verwenden wir die Formel der Variation der Konstanten für den eindimensionalen Fall (Seite 403) mit der Anfangsbedingung $x_1(0) = 2$:

$$\begin{aligned} x_1(t) &= 2e^{\int_0^t 2s ds} + e^{\int_0^t 2s ds} \int_0^t e^{-\int_0^s 2r dr} (s - s^3) ds = \\ &= 2e^{t^2} + e^{t^2} \int_0^t e^{-s^2} (s - s^3) ds = 2e^{t^2} + e^{t^2} \left(\int_0^t s e^{-s^2} ds - \int_0^t s^3 e^{-s^2} ds \right). \end{aligned}$$

Die beiden Integrale berechnen wir, indem wir beim zweiten Integral partielle Integration auf die Faktoren s^2 und se^{-s^2} anwenden:

$$\int_0^t s e^{-s^2} ds - \int_0^t s^2 se^{-s^2} ds = \int_0^t s e^{-s^2} ds - \left[-\frac{1}{2}s^2 e^{-s^2} \right]_0^t - \int_0^t s e^{-s^2} ds = \frac{1}{2}t^2 e^{-t^2}.$$

Damit erhalten wir als Lösung für die erste Komponente

$$x_1(t) = 2e^{t^2} + \frac{1}{2}e^{t^2} t^2 e^{-t^2} = 2e^{t^2} + \frac{1}{2}t^2.$$

Und eine kurze Rechnung zeigt leicht, dass die Gleichungen

$$x'_1(t) = 4te^{t^2} + t = 2tx_1(t) + tx_2(t)$$

sowie $x_1(0) = 2$ erfüllt sind, und x_1 damit die gesuchte Lösung ist. Insgesamt ist damit die Lösung des Systems gegeben durch

$$\mu:]-1, 1[\rightarrow \mathbb{R}^2, \quad t \mapsto \begin{pmatrix} 2e^{t^2} + \frac{1}{2}t^2 \\ 1 - t^2 \end{pmatrix}.$$

Phasenportraits linearer Differentialgleichungen

Die Veranschaulichung der Lösungen von ebenen (d. h. zweidimensionalen) Systemen stellt uns vor ein gewisses Problem: Die Graphen solcher Lösungen sind Teilmengen des \mathbb{R}^3 und daher nur schwer zu skizzieren. Eine Möglichkeit, dieses Problem zu umgehen, bietet das Konzept der *Trajektorien*. Dabei handelt es sich um die Bildmengen einer Lösung. Diese verlaufen nur im \mathbb{R}^2 , da die t -Komponente nicht erfasst wird. Ein *Phasenportrait* enthält alle Trajektorien eines Systems (diese bilden stets eine Zerlegung der Definitionsmenge des Systems).

Beispiel 7.18. Wir illustrieren das Vorgehen beim Skizzieren eines solchen Phasenportraits zunächst anhand der linearen Differentialgleichung

$$\dot{x} = Ax = \begin{pmatrix} 1 & 1 \\ 4 & -2 \end{pmatrix} x$$

raten dazu, die im Text nur geschilderten Schritte explizit auszuführen. Als charakteristisches Polynom erhält man $\chi_A = X^2 + X - 6$ mit den Eigenwerten $\lambda_1 = 2$ und $\lambda_2 = -3$. Als zugehörige Eigenvektoren berechnet man leicht $v_1 = (1, 1)$ und $v_2 = (-1, 4)$. Die beiden Lösungen

$$\mu_1(t) = \begin{pmatrix} 1 \\ 1 \end{pmatrix} e^{2t} \quad \text{und} \quad \mu_2(t) = \begin{pmatrix} -1 \\ 4 \end{pmatrix} e^{-3t}$$

bilden damit ein Fundamentalsystem von Lösungen der Gleichung. Da 0 kein Eigenwert der Matrix ist, ist A invertierbar und $(0, 0)$ ist die einzige Ruhelage. Die Trajektorie von μ_1 ist

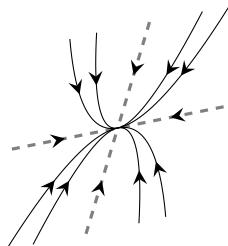
$$\{\mu_1(t) \mid t \in \mathbb{R}\} = \{v_1 e^{2t} \mid t \in \mathbb{R}\} = \{\lambda v \mid \lambda \in \mathbb{R}^+\}.$$

Es handelt sich also um eine *Halbgerade* mit Richtungsvektor v_1 . Die Lösung $-\mu_1$ liefert die komplementäre Halbgerade. Ebenso bildet auch die Lösung μ_2 eine Halbgerade im Phasenportrait. Für $t \rightarrow \infty$ strebt die Lösung μ_2 gegen den Ursprung, die Lösung μ_1 von ihm weg. Dies ermöglicht es, entsprechende Pfeile einzuziehen.

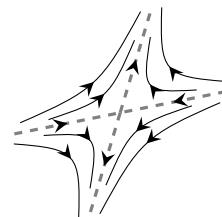
Ist nun eine beliebige Lösung vorgegeben, so hat diese die Gestalt

$$a \begin{pmatrix} 1 \\ 1 \end{pmatrix} e^{2t} + b \begin{pmatrix} -1 \\ 4 \end{pmatrix} e^{-3t}$$

für geeignete $a, b \in \mathbb{R}$. Wir betrachten wiederum das Grenzverhalten: Für $t \rightarrow \infty$ verschwindet der hintere Summand, wir nähern uns also der Richtung des ersten Eigenvektors an, während für $t \rightarrow -\infty$ der vordere Summand verschwindet und wir uns der Richtung des zweiten Eigenvektors annähern. Insgesamt erhalten wir ein Phasenportrait, das in Abbildung 7.1 rechts oben steht und *Sattel* genannt wird. ■

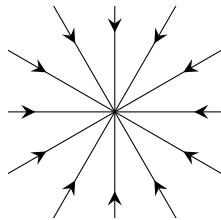
**Senke (bzw. Quelle)**

$$\lambda_1, \lambda_2 < 0$$

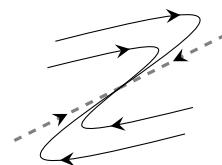
(instabile Quelle, falls $\lambda_1, \lambda_2 > 0$)**Sattel**

$$\lambda_1 < 0 < \lambda_2$$

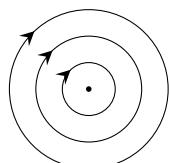
(immer instabil)

**Stern**

$$\lambda_1 = \lambda_2 < 0, \text{ geom. Vielfachheit } 2$$

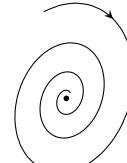
(instabil, falls $\lambda_1 = \lambda_2 > 0$)
**Eintangentialer Knoten**

$$\lambda_1 = \lambda_2 < 0, \text{ geom. Vielfachheit } 1$$

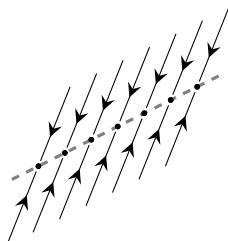
(instabil, falls $\lambda_1 = \lambda_2 > 0$)
**Wirbel**

$$\lambda_1, \lambda_2 \notin \mathbb{R},$$

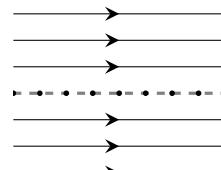
$$\operatorname{Re} \lambda_1, \lambda_2 = 0$$

**Strudel**

$$\lambda_1, \lambda_2 \notin \mathbb{R}, \operatorname{Re} \lambda_1, \lambda_2 < 0$$

(instabil, falls $\operatorname{Re} \lambda_1, \lambda_2 > 0$)**Liniensenken**

$$\lambda_1 = 0, \lambda_2 < 0$$

(instabile Linienquellen, falls $\lambda_2 > 0$)

$$\lambda_1 = \lambda_2 = 0, \text{ geom. Vielfachheit } 1$$

(stets instabil)

Abbildung 7.1: Klassifizierung der Ruhelagen der Linearen Differentialgleichung $\dot{x} = Ax$ anhand der (ggf. komplexen) Eigenwerte λ_1, λ_2 des charakteristischen Polynoms χ_A . Gestrichelte Linien zeigen in Richtung der Eigenvektoren.

Für lineare Systeme lassen sich die auftretenden Phasenportraits anhand der Eigenwerte des charakteristischen Polynoms vollständig klassifizieren. Abbildung 7.1 zeigt diese Übersicht. In der folgenden Aufgaben illustrieren wir noch, wie man auf einige der Phasenportraits kommt.

Aufgabe (Herbst 2001, T2A1)

Skizzieren Sie die Phasenportraits der ebenen autonomen Systeme $\dot{x} = Ax$ für die drei Matrizen

$$\mathbf{a} \quad A = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, \quad \mathbf{b} \quad A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \mathbf{c} \quad A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}.$$

Lösungsvorschlag zur Aufgabe (Herbst 2001, T2A1)

- a** Da A in Diagonalform vorliegt, sind die Eigenwerte 1 und 2, mit den Einheitsvektoren e_1 bzw. e_2 als Eigenvektoren. Alle Lösungen haben damit die Form

$$a \begin{pmatrix} 1 \\ 0 \end{pmatrix} e^t + b \begin{pmatrix} 0 \\ 1 \end{pmatrix} e^{2t}$$

für $a, b \in \mathbb{R}$. Setzt man einen der beiden Parameter gleich 0, so erhält man als Trajektorien die beiden Koordinatenachsen, die beide für $t \rightarrow \infty$ vom Ursprung weglauen. Beliebige Lösungen laufen für $t \rightarrow -\infty$ zum Ursprung hin, da der hintere Summand „schneller“ gegen 0 strebt, geschieht dies parallel zum Vektor e_1 , für $t \rightarrow \infty$ hat der hintere Summand dagegen den stärkeren Einfluss und die Kurven verlaufen zunehmend parallel zu e_2 (im Englischen dies die sogenannte „fast eigendirection“). Man erhält somit eine *Quelle*.

- b** Das charakteristische Polynom $X^2 - 1$ liefert die Eigenwerte ± 1 und man berechnet die Eigenvektoren $v_1 = (1, 1)$ sowie $v_2 = (-1, 1)$. Die allgemeine Lösung hat somit die Form

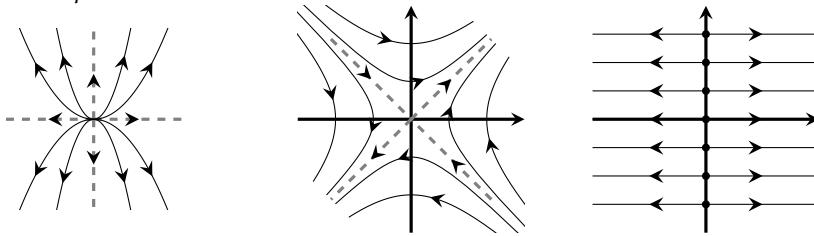
$$a \begin{pmatrix} 1 \\ 1 \end{pmatrix} e^t + b \begin{pmatrix} -1 \\ 1 \end{pmatrix} e^{-t}$$

mit Parametern $a, b \in \mathbb{R}$. Setzen wir $b = 0$, so erhält man wie im Beispiel oben zwei Halbgeraden entlang des Vektors $(1, 1)$, die für $t \rightarrow \infty$ vom Ursprung weglauen. Für $a = 0$ ergeben sich entsprechend zwei Halbgeraden entlang $(-1, 1)$, die auf den Ursprung zulaufen. Für allgemeine Lösungen stellen wir fest, dass diese sich für beliebige Wahl der Parameter für $t \rightarrow \infty$ der Richtung v_1 nähern, da der zweite Teil verschwindet und für $t \rightarrow -\infty$ parallel zu v_2 verlaufen. Damit erhält man einen *Sattel*.

- c Die Matrix A liegt wiederum in Diagonalform vor, mit Eigenwerten 1 und 0 und Eigenvektoren e_1 bzw. e_2 . Da der zweite Eigenwert 0 ist, sind jedoch alle Vielfachen von e_2 zugleich Ruhelagen der Gleichung, sodass die y -Achse aus Ruhelagen besteht. Die allgemeine Lösung lautet dementsprechend

$$a \begin{pmatrix} 1 \\ 0 \end{pmatrix} e^t + b \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

Diese Trajektorien bilden verschobene Halbgeraden mit den Richtungsvektor $(1, 0)$ und verlaufen somit parallel zur x -Achse und für $t \rightarrow -\infty$ auf den Punkt $(0, b)$ zu, für $t \rightarrow \infty$ von ihm weg. Es handelt sich somit um Liniенquellen.



Aufgabe (Herbst 2010, T3A4)

Bestimmen Sie alle Lösungen von

$$\begin{aligned}\dot{x} &= 8x + 10y \\ \dot{y} &= -5x - 6y\end{aligned}$$

und skizzieren Sie das Phasenportrait.

Lösungsvorschlag zur Aufgabe (Herbst 2010, T3A4)

Die angegebenen Gleichungen sind äquivalent zu

$$\begin{pmatrix} \dot{x} \\ \dot{y} \end{pmatrix} = \begin{pmatrix} 8 & 10 \\ -5 & -6 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}.$$

Sei A die Koeffizientenmatrix. Wir berechnen ein Fundamentalsystem von Lösungen. Dazu beobachten wir zunächst, dass das charakteristische Polynom hier gegeben ist durch

$$\chi_A = \det \begin{pmatrix} 8 - X & 10 \\ -5 & -6 - X \end{pmatrix} = X^2 - 2X + 2.$$

Mit der Mitternachtsformel erhält man die Eigenwerte $1 \pm i$. Wir berechnen nun zunächst eine komplexe Lösung des Systems und dazu einen der Eigenräume:

$$\begin{aligned}\text{Eig}(A, 1+i) &= \ker \begin{pmatrix} 7-i & 10 \\ -5 & -7-i \end{pmatrix} = \ker \begin{pmatrix} (7-i)(7+i) & 10(7+i) \\ -5 & -7-i \end{pmatrix} = \\ &= \ker \begin{pmatrix} 50 & 70+10i \\ 5 & 7+i \end{pmatrix} = \ker \begin{pmatrix} 5 & 7+i \\ 0 & 0 \end{pmatrix} = \left\langle \begin{pmatrix} 7+i \\ -5 \end{pmatrix} \right\rangle\end{aligned}$$

Eine (komplexe) Lösung ist nun gegeben durch

$$\lambda(t) = \begin{pmatrix} 7+i \\ -5 \end{pmatrix} e^{(1+i)t}.$$

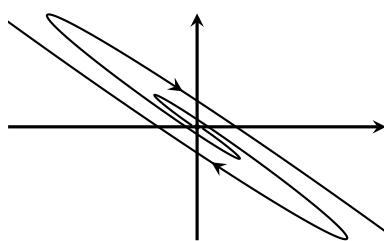
Der Real- und Imaginärteil dieser Funktion sind dann reelle Lösungen der Gleichung. Wir berechnen diese explizit:

$$\begin{aligned}\lambda(t) &= \begin{pmatrix} 7+i \\ -5 \end{pmatrix} e^{(1+i)t} = \begin{pmatrix} 7+i \\ -5 \end{pmatrix} e^t \cdot (\cos t + i \sin t) = \\ &= \begin{pmatrix} 7e^t \cos t - e^t \sin t \\ -5e^t \cos t \end{pmatrix} + i \begin{pmatrix} 7e^t \sin t + e^t \cos t \\ -5e^t \sin t \end{pmatrix}\end{aligned}$$

Definieren wir den Realteil als μ_1 und den Imaginärteil als μ_2 , so ist schnell nachgerechnet, dass diese tatsächlich Lösungen der ursprünglichen Gleichungen sind. Für die Wronski-Determinante an der Stelle 0 ergibt sich

$$\omega(0) = \det \begin{pmatrix} 7 & 1 \\ -5 & 0 \end{pmatrix} = 5 \neq 0,$$

sodass die Lösungen linear unabhängig sind und damit ein Fundamentalsystem bilden. Alle Lösungen der Differentialgleichung haben also die Form $a\mu_1 + b\mu_2$ mit $a, b \in \mathbb{R}$.



Zum Phasenportait: Da A invertierbar ist, ist die einzige Ruhelage $(0,0)$. Beide Eigenwerte hatten positiven Realteil, sodass es sich um eine instabile Ruhelage handelt. Anhand der Terme der Lösungen (oder mithilfe der Klassifizierung auf Seite 446) erkennt man nun, dass es sich um einen instabilen Strudel handelt.

7.4. Skalare Differentialgleichungen höherer Ordnung

Lineare Gleichungen höherer Ordnung mit konstanten Koeffizienten

Die Theorie der linearen Differentialgleichungen höherer Ordnung, also von Gleichungen der Form

$$y^{(n)} + a_{n-1}y^{(n-1)} + \dots + a_1y' + a_0y = 0,$$

ist eng mit der Theorie von Linearen Systemen von Differentialgleichungen verbunden. Um dies zu sehen, führen wir die neuen Variablen

$$u_0 = y, \quad u_1 = y', \quad \dots, \quad u_{n-1} = y^{(n-1)}$$

ein. Die obige Gleichung ist dann äquivalent zum System

$$\begin{aligned} u'_0 &= y' &= & u_1 \\ \vdots &= \vdots &= & \vdots \\ u'_n &= y^{(n)} &= -a_{n-1}u_{n-1} - \dots - a_0u_0 \end{aligned},$$

welches auch als

$$\begin{pmatrix} u'_0 \\ \vdots \\ u'_{n-1} \end{pmatrix} = \begin{pmatrix} 0 & 1 & \dots & 0 \\ \vdots & & & \vdots \\ -a_0 & -a_1 & \dots & -a_{n-1} \end{pmatrix} \begin{pmatrix} u_0 \\ \vdots \\ u_{n-1} \end{pmatrix}$$

geschrieben werden kann. Zwischen den Lösungen der ursprünglicher Gleichung und entstandenem System besteht nun folgender Zusammenhang: Ist μ eine Lösung der ursprünglichen Gleichung, so definiert $(\mu, \mu', \dots, \mu^{(n-1)})$ eine Lösung des Systems. Ist umgekehrt $(\lambda_0, \dots, \lambda_{n-1})$ eine Lösung des Systems, so ist λ_0 eine Lösung der ursprünglichen Gleichung.

Aufgrund dieser Korrespondenz lassen sich viele Begriffe aus der Theorie Linearer Systeme direkt übertragen. Beispielsweise bildet auch die Lösungsmenge einer Gleichung n -ter Ordnung einen n -dimensionalen Vektorraum \mathcal{L} , dessen Basis ebenfalls als *Fundamentalsystem* bezeichnet wird. Im Fall von inhomogenen Gleichungen hat die Lösungsmenge die Form $\mathcal{L} + \mu_p$, wobei \mathcal{L} die Lösungsmenge des zugehörigen homogenen Systems und μ_p eine *partikuläre* Lösung ist.

Hat die Gleichung konstante Koeffizienten, so kann ein Fundamentalsystem mittels des *charakteristischen Polynoms* der Differentialgleichung angegeben werden. Dies ist das Polynom

$$\chi = X^n + a_{n-1}X^{n-1} + \dots + a_1X + a_0.$$

Dabei handelt es sich um das charakteristische Polynom der Koeffizientenmatrix von oben.

Satz 7.19 (Fundamentalsystem). Gegeben sei eine homogene lineare Differentialgleichung n -ter Ordnung mit charakteristischem Polynom χ . Ist ρ eine k -fache reelle Nullstelle von χ , so sind die k Funktionen

$$e^{\rho t}, \quad te^{\rho t}, \quad \dots, \quad t^{k-1}e^{\rho t}$$

linear unabhängige Lösungen der Differentialgleichung. Ist $\rho + i\sigma$ mit $\sigma \neq 0$ (und damit auch $\rho - i\sigma$) eine m -fache komplexe Nullstelle der Gleichung, so sind die $2m$ Funktionen

$$\begin{aligned} e^{\rho t} \cos \sigma t, \quad te^{\rho t} \cos \sigma t, \quad \dots, \quad t^{m-1}e^{\rho t} \cos \sigma t, \\ e^{\rho t} \sin \sigma t, \quad te^{\rho t} \sin \sigma t, \quad \dots, \quad t^{m-1}e^{\rho t} \sin \sigma t \end{aligned}$$

linear unabhängige Lösungen. Indem man sämtliche Nullstellen von χ durchgeht, erhält man so n linear unabhängige Lösungen, also ein Fundamentalsystem der Gleichung.

Aufgabe (Frühjahr 2008, T2A2)

- a Bestimmen Sie alle reellen Lösungen des Differentialgleichungssystems

$$y_1'' = 3y_2, \quad y_2'' = 27y_1,$$

indem Sie zunächst eine der beiden unbekannten Funktionen eliminieren.

- b Schreiben Sie das System aus a um in ein System $u' = Au$ erster Ordnung mit einer (4×4) -Matrix A .
- c Geben Sie vier Funktion $\mathbb{R} \rightarrow \mathbb{R}^4$ an, die denselben Vektorraum aufspannen wie die Spalten von e^{xA} .

Hinweis Dabei macht es zu viel Mühe, e^{xA} auszurechnen.

Lösungsvorschlag zur Aufgabe (Frühjahr 2008, T2A2)

- a Aus der ersten Gleichung folgt $y_2 = \frac{1}{3}y_1''$ und somit durch Einsetzen in die zweite

$$27y_1 = y_2'' = \frac{1}{3}y_1^{(4)} \Leftrightarrow y_1^{(4)} - 81y_1 = 0.$$

Damit haben wir nun eine lineare Differentialgleichung höherer Ordnung erhalten, die das charakteristische Polynom

$$X^4 - 81 = (X^2 - 9)(X^2 + 9) = (X + 3)(X - 3)(X + 3i)(X - 3i)$$

hat. Ein Fundamentalsystem ist nach Satz 7.19 dann gegeben durch

$$\{e^{3x}, e^{-3x}, \sin(3x), \cos(3x)\}.$$

Einsetzen in die Gleichung oben liefert nun die jeweils zugehörige Lösung für y_2 :

$$\left\{ \begin{pmatrix} e^{3x} \\ 3e^{3x} \end{pmatrix}, \begin{pmatrix} e^{-3x} \\ 3e^{-3x} \end{pmatrix}, \begin{pmatrix} \sin(3x) \\ -3\sin(3x) \end{pmatrix}, \begin{pmatrix} \cos(3x) \\ -3\cos(3x) \end{pmatrix} \right\}.$$

- b** Wir definieren die Variablen $u_1 = y_1, u_2 = y'_1, u_3 = y_2, u_4 = y'_2$. Es gilt dann natürlich $u'_1 = u_2$ und $u'_3 = u_4$. Ferner liefern die Gleichungen

$$u'_2 = y''_1 = 3y_2 = 3u_3 \quad \text{und} \quad u'_4 = y''_2 = 27y_1 = 27u_1.$$

Das äquivalente System lautet also

$$u' = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 1 \\ 27 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} u_1 \\ u_2 \\ u_3 \\ u_4 \end{pmatrix}.$$

- c** Der Vektorraum, der von den Spalten von e^{xA} aufgespannt wird, ist genau der Lösungsraum des in Teil **b** definierten linearen Systems. Nun besteht zwischen den Lösungen des Systems aus Teil **a** und denjenigen des Systems aus Teil **b** eine bijektive Korrespondenz mittels

$$(y_1, y_2) \mapsto (y_1, y'_1, y_2, y'_2)$$

(vgl. die Definition von u). Diese liefert aus dem in Teil **a** bestimmten Fundamentalsystem das Fundamentalsystem

$$\begin{pmatrix} e^{3x} \\ 3e^{3x} \\ 3e^{3x} \\ 9e^{3x} \end{pmatrix}, \begin{pmatrix} e^{-3x} \\ -3e^{-3x} \\ 3e^{-3x} \\ -9e^{-3x} \end{pmatrix}, \begin{pmatrix} \sin(3x) \\ 3\cos(3x) \\ -3\sin(3x) \\ 9\cos(3x) \end{pmatrix}, \begin{pmatrix} \cos(3x) \\ -3\sin(3x) \\ -3\cos(3x) \\ 9\cos(3x) \end{pmatrix}.$$

Aufgabe (Frühjahr 2009, T3A2)

Bestimmen Sie die maximale Lösung des Anfangswertproblems

$$\begin{aligned} \ddot{x} &= x + 3y \\ \dot{y} &= \dot{x} \\ x(0) &= 5, \quad \dot{x}(0) = 0, \quad y(0) = 1 \end{aligned}$$

Lösungsvorschlag zur Aufgabe (Frühjahr 2009, T3A2)

Wir formen das System zunächst in ein System um, das nur Ableitungen erster Ordnung enthält. Dafür definieren wir $u_1 = x, u_2 = \dot{x}, u_3 = y$. Dann ist das angegebene System äquivalent zu

$$\begin{pmatrix} \dot{u}_1 \\ \dot{u}_2 \\ \dot{u}_3 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 3 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} u_1 \\ u_2 \\ u_3 \end{pmatrix}$$

mit der Anfangswertbedingung $u(0) = (5, 0, 1)$. Das lineare System erster Ordnung lösen wir, indem wir zunächst das charakteristische Polynom der Koeffizientenmatrix A bestimmen:

$$\chi_A = \det \begin{pmatrix} -X & 1 & 0 \\ 1 & -X & 3 \\ 0 & 1 & -X \end{pmatrix} = -X^3 + 4X = -X(X^2 - 4).$$

Damit haben wir die drei verschiedenen Eigenwerte $\lambda_1 = 0, \lambda_{2,3} = \pm 2$. Die entsprechenden Eigenräume sind

$$\text{Eig}(A, 0) = \left\langle \begin{pmatrix} -3 \\ 0 \\ 1 \end{pmatrix} \right\rangle, \quad \text{Eig}(A, 2) = \left\langle \begin{pmatrix} 1 \\ 2 \\ 1 \end{pmatrix} \right\rangle, \quad \text{Eig}(A, -2) = \left\langle \begin{pmatrix} 1 \\ -2 \\ 1 \end{pmatrix} \right\rangle.$$

Also ist

$$\Phi(t) = \begin{pmatrix} -3 & e^{2t} & e^{-2t} \\ 0 & 2e^{2t} & -2e^{-2t} \\ 1 & e^{2t} & e^{-2t} \end{pmatrix}$$

eine Fundamentalmatrix des Systems. Um die Lösung anzugeben, berechnet man zunächst

$$\Phi(0)^{-1} = \begin{pmatrix} -3 & 1 & 1 \\ 0 & 2 & -2 \\ 1 & 1 & 1 \end{pmatrix}^{-1} = \frac{1}{8} \begin{pmatrix} -2 & 0 & 2 \\ 1 & 2 & 3 \\ 1 & -2 & 3 \end{pmatrix}$$

und weiter mit der Formel aus der Variation der Konstanten

$$\begin{aligned} \mu(t) &= \Phi(t)\Phi(0)^{-1} \begin{pmatrix} 5 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} -3 & e^{2t} & e^{-2t} \\ 0 & 2e^{2t} & -2e^{-2t} \\ 1 & e^{2t} & e^{-2t} \end{pmatrix} \frac{1}{8} \begin{pmatrix} -2 & 0 & 2 \\ 1 & 2 & 3 \\ 1 & -2 & 3 \end{pmatrix} \begin{pmatrix} 5 \\ 0 \\ 1 \end{pmatrix} = \\ &= \begin{pmatrix} -3 & e^{2t} & e^{-2t} \\ 0 & 2e^{2t} & -2e^{-2t} \\ 1 & e^{2t} & e^{-2t} \end{pmatrix} \begin{pmatrix} -1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 3 + e^{2t} + e^{-2t} \\ 2e^{2t} - 2e^{-2t} \\ -1 + e^{2t} + e^{-2t} \end{pmatrix}. \end{aligned}$$

Re-Substitution ergibt damit die Lösung

$$\begin{pmatrix} x(t) \\ y(t) \end{pmatrix} = \begin{pmatrix} 3 + e^{2t} + e^{-2t} \\ -1 + e^{2t} + e^{-2t} \end{pmatrix}.$$

Wir überprüfen dies. Wegen

$$\dot{x} = 2e^{2t} - 2e^{-2t}, \quad \ddot{x} = 4e^{2t} + 4e^{-2t}, \quad \dot{y} = 2e^{2t} - 2e^{-2t}$$

gelten sowohl $\dot{x} = \dot{y}$ als auch $\ddot{x} = x + 3y$ und mit

$$x(0) = 5, \quad \dot{x}(0) = 0, \quad y(0) = 1$$

ist auch die Anfangswertbedingung erfüllt.

Aufgabe (Herbst 2010, T2A5)

Man berechne die allgemeine Lösung der Differentialgleichung

$$x'' + 2x' + 4x = \sin t.$$

Hinweis Eine partikuläre Lösung ergibt sich aus dem Ansatz $x(t) = a \cos t + b \sin t$.

Lösungsvorschlag zur Aufgabe (Herbst 2010, T2A5)

Das charakteristische Polynom dieser Differentialgleichung lautet

$$X^2 + 2X + 4.$$

Dessen Nullstellen berechnen sich zu

$$\lambda_{1,2} = \frac{-2 \pm \sqrt{-12}}{2} = -1 \pm i\sqrt{3}.$$

Laut Satz 7.19 erhält man das Fundamentalsystem

$$\left\{ e^{-t} \cos(\sqrt{3}t), e^{-t} \sin(\sqrt{3}t) \right\}.$$

Um eine partikuläre Lösung zu finden, folgen wir dem Hinweis und berechnen zunächst die beiden nötigen Ableitungen

$$x'(t) = -a \sin t + b \cos t \quad \text{und} \quad x''(t) = -a \cos t - b \sin t.$$

Einsetzen in die Ausgangsgleichung liefert nun

$$(-a \cos t - b \sin t) + 2(-a \sin t + b \cos t) + 4(a \cos t + b \sin t) = \sin t \Leftrightarrow \\ (3a + 2b) \cos t + (3b - 2a) \sin t = \sin t \Leftrightarrow 3a + 2b = 0 \text{ und } 3b - 2a = 1.$$

Aus dem letzten Gleichungssystem ergibt sich $b = -\frac{3}{2}a$ und damit

$$-\frac{9}{2}a - 2a = 1 \Leftrightarrow -\frac{13}{2}a = 1 \Leftrightarrow a = -\frac{2}{13}$$

Dies wiederum bedeutet $b = \frac{3}{13}$. Die allgemeine Lösung der DGL lautet somit

$$\mu(t) = ae^{-t} \cos(\sqrt{3}t) + be^{-t} \sin(\sqrt{3}t) - \frac{2}{13} \cos t + \frac{3}{13} \sin t$$

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

Neben der Angabe von Fundamentalsystemen beschäftigen wir uns – wir zuvor – nun noch mit dem Lösen von Anfangswertproblemen. Aufgrund der Strukturähnlichkeit zur linearen Differentialgleichungssystemen ist es keine Überraschung, dass uns dabei erneut die Variation der Konstanten begegnet.

Proposition 7.20 (Variation der Konstanten). Gegeben sei eine Differentialgleichung

$$y^{(n)} + a_{n-1}y^{(n-1)} + \dots + a_1y' + a_0 = 0$$

mit Anfangswerten $y(t_0) = y_0, y'(t_0) = y_1, \dots, y^{(n-1)}(t_0) = y_{n-1}$. Die Lösung dieses Anfangswertproblems ist

$$(\mu_1(t), \dots, \mu_n(t)) \left[W(t_0)^{-1} \begin{pmatrix} y_0 \\ \vdots \\ y_{n-1} \end{pmatrix} + \int_{t_0}^t W^{-1}(s) \begin{pmatrix} 0 \\ \vdots \\ 0 \\ b(s) \end{pmatrix} ds \right].$$

Hierbei ist μ_1, \dots, μ_n ein Fundamentalsystem der homogenen Differentialgleichung und

$$W(t) = \begin{pmatrix} \mu_1(t) & \dots & \mu_n(t) \\ \vdots & & \vdots \\ \mu_1^{(n-1)}(t) & \dots & \mu_n^{(n-1)}(t) \end{pmatrix}$$

ist die sogenannte **Wronski-Matrix**.

Alternativ zu diesem Lösungsverfahren kann es manchmal einfacher sein, zunächst die allgemeine Lösung einer Differentialgleichung zu bestimmen, um dann die Parameter dem Anfangswertproblem entsprechend zu bestimmen. Hierzu benötigen wir für inhomogene Gleichungen ein Vorgehen, mit dem sich eine partikulären Lösung bestimmen lässt:

Anleitung: Finden partikulärer Lösungen

Es sei eine Differentialgleichung höherer Ordnung sowie ein zugehöriges Fundamentalsystem gegeben. Eine partikuläre Lösung kann oft mithilfe eines Ansatzes aus der folgenden Tabelle bestimmt werden.

Rechte Seite der DGL	Parameter	Ansatz
(1) $e^{\alpha t}$	α	$Ct^k e^{\alpha t}$
(2) $p_l(t)e^{\alpha t}$	α	$t^k r_l(t)e^{\alpha t}$
(3) $A \sin(\beta t) + B \cos(\beta t)$	$\pm \beta i$	$t^k (C \sin(\beta t) + D \cos(\beta t))$
(4) $(p_l(t) \sin(\beta t) + q_l(t) \cos(\beta t))e^{\alpha t}$	$\alpha \pm i\beta$	$t^k (r_l(t) \sin(\beta t) + s_l(t) \cos(\beta t))e^{\alpha t}$

- (1) Falls das konkrete α Nullstelle des charakteristischen Polynoms ist, so bezeichnet k die Vielfachheit der Nullstelle (man spricht dann davon, dass *Resonanz* vorliegt). Andernfalls setze $k = 0$.

Hinweis Dabei sind im Ansatz (3) bzw. (4) stets sin und cos zu verwenden, auch wenn nur eine der beiden Funktionen in der Gleichung auftritt. Die Symbole p_l, q_l, r_l und s_l bezeichnen jeweils Polynome vom Grad l .

- (2) Bestimme nun für den gewählten Ansatz alle auftretenden Ableitungen.
(3) Setze diese in die ursprüngliche Differentialgleichung ein, um die Unbestimmten im Ansatz zu berechnen.

Beispiel 7.21. Wir illustrieren das Vorgehen an der Gleichung

$$x'' + 2x' + 4x = \sin t$$

aus H10T2A5 (wo der Ansatz aber angegeben war). Es handelt sich um (3) in der Tabelle mit $\beta = 1$. Das charakteristische Polynom ist $X^2 + 2X + 4$. Da $\pm i$ keine Nullstellen des charakteristischen Polynoms sind (wie man schnell überprüft), haben wir $k = 0$ und ein geeigneter Ansatz ist

$$C \sin t + D \cos t.$$

■

Aufgabe (Herbst 2004, T2A3)

Bestimmen Sie die allgemeine Lösung der inhomogenen linearen Differentialgleichung $y'' - 4y' - 5y = f$ für

a $f(t) = 8e^t$, **b** $6e^{-t}$.

Lösungsvorschlag zur Aufgabe (Herbst 2004, T2A3)

Wir geben zunächst ein Fundamentalsystem der homogenen Differentialgleichung an. Diese hat das charakteristische Polynom

$$X^2 - 4X - 5 = (X - 5)(X + 1).$$

Damit ist $\{e^{5t}, e^{-t}\}$ ein solches Fundamentalsystem.

- a** Arbeiten wir mit der Tabelle, so liegt hier Zeile (1) mit $\alpha = 1$ vor. Da 1 keine Nullstelle des charakteristischen Polynoms ist, machen wir den Ansatz $y_p(t) = Ce^t$ mit zu bestimmendem $C \in \mathbb{R}$. Es ist

$$y'_p(t) = y''_p(t) = Ce^t.$$

Einsetzen in die Gleichung liefert

$$Ce^t - 4Ce^t - 5Ce^t = 8e^t \Leftrightarrow -8Ce^t = 8e^t.$$

Wir setzen also $C = -1$ und erhalten die partikuläre Lösung $y_p(t) = -e^t$. Die allgemeine Lösung ist damit

$$y(t) = ae^{5t} + be^{-t} - e^t \quad \text{mit } a, b \in \mathbb{R}.$$

- b** Hier ist $\alpha = -1$ und es handelt sich dabei um eine einfache Nullstelle des charakteristischen Polynoms, sodass wir hier den Ansatz $y_p(t) = Cte^{-t}$ machen. Die Ableitungen lauten

$$y'_p(t) = Ce^{-t} - Cte^{-t}, \quad y''_p(t) = -2Ce^{-t} + Cte^{-t}.$$

Einsetzen in die Gleichung liefert

$$-2Ce^{-t} + Cte^{-t} - 4(Ce^{-t} - Cte^{-t}) - 5Cte^{-t} = 6e^{-t} \Leftrightarrow -6Ce^{-t} = 6e^{-t}.$$

Diesmal wählen wir also $C = -1$ und erhalten die partikuläre Lösung $y_p(t) = -te^{-t}$. Die allgemeine Lösung lautet daher

$$y(t) = ae^{5t} + be^{-t} - te^{-t} \quad \text{mit } a, b \in \mathbb{R}.$$

Aufgabe (Herbst 2015, T2A2)

Betrachten Sie die Differentialgleichung

$$y''' - 2y'' + y' = e^{2x}.$$

- a** Bestimmen Sie ein Fundamentalsystem für die zugehörige homogene Differentialgleichung.
- b** Bestimmen Sie mit einem geeigneten Ansatz eine spezielle Lösung der inhomogenen Gleichung und geben Sie damit die allgemeine Lösung an.
- c** Bestimmen Sie die Lösung des zugehörigen Anfangswertproblems mit

$$y(0) = y'(0) = y''(0) = 0.$$

Lösungsvorschlag zur Aufgabe (Herbst 2015, T2A2)

- a** Das charakteristische Polynom der homogenen Differentialgleichung lautet

$$\chi = X^3 - 2X^2 + X = X(X^2 - 2X + 1) = X(X - 1)^2.$$

Ein Fundamentalsystem ist daher

$$\{e^{0x}, e^x, xe^x\} = \{1, e^x, xe^x\}.$$

- b** Wiederum liegt Fall (1) der Tabelle auf Seite 456 vor, diesmal mit $\alpha = 2$. Da 2 keine Nullstelle des charakteristischen Polynoms ist, machen wir also den Ansatz $y_p(x) = Ce^{2x}$ für ein zu bestimmendes $C \in \mathbb{R}$. Es gilt

$$y'_p(x) = 2Ce^{2x}, \quad y''_p(x) = 4Ce^{2x}, \quad y'''_p(x) = 8Ce^{2x}.$$

Eingesetzt in die Gleichung ergibt dies

$$8Ce^{2x} - 8Ce^{2x} + 2Ce^{2x} = e^{2x} \Leftrightarrow 2Ce^{2x} = e^{2x} \Leftrightarrow C = \frac{1}{2}.$$

Damit ist $y_p(x) = \frac{1}{2}e^{2x}$ eine partikuläre Lösung und die allgemeine Lösung des Systems ist gegeben durch

$$y(x) = a + be^x + cxe^x + \frac{1}{2}e^{2x} \quad \text{mit } a, b, c \in \mathbb{R}.$$

- c** Es sind nur noch die Parameter der allgemeinen Lösung geeignet zu wählen, deshalb bestimmen wir zunächst die ersten beiden Ableitungen der allgemeinen Lösung:

$$y'(x) = be^x + cxe^x + ce^x + e^{2x}, \quad y''(x) = be^x + cxe^x + 2ce^x + 2e^{2x}.$$

Einsetzen der Anfangswerte ergibt die Gleichungen

$$(I) \quad a + b + \frac{1}{2} = 0, \quad (II) \quad b + c + 1 = 0, \quad (III) \quad b + 2c + 2 = 0.$$

Subtrahiert man die zweite Gleichung von der dritten, so erhält man sofort $c = -1$, dies liefert $b = 0$ und damit $a = -\frac{1}{2}$, also insgesamt

$$y(x) = -\frac{1}{2} - xe^x + \frac{1}{2}e^{2x}.$$

Aufgabe (Herbst 2012, T3A1)

Bestimmen Sie jeweils für $\omega_0 = 1$ und $\omega_0 = \sqrt{2}$ die allgemeine reelle Lösung der Differentialgleichung

$$\ddot{y} + 2y = 2 \cos \omega_0 t.$$

Lösungsvorschlag zur Aufgabe (Herbst 2012, T3A1)

Wir betrachten zunächst die homogene Differentialgleichung $\ddot{y} + 2y = 0$ mit charakteristischem Polynom

$$X^2 + 2 = (X + i\sqrt{2})(X - i\sqrt{2}).$$

Dies liefert uns gemäß Satz 7.19 das Fundamentalsystem

$$\left\{ \sin \sqrt{2}t, \cos \sqrt{2}t \right\}.$$

Für $\omega_0 = 1$ ist $i\omega_0$ keine Nullstelle des charakteristischen Polynoms, sodass keine Resonanz vorliegt. Ein möglicher Ansatz ist somit

$$\mu_p(t) = C \sin t + D \cos t.$$

Für die zweite Ableitung erhält man $\mu_p''(t) = -C \sin t - D \cos t$. Einsetzen in die Ausgangsgleichung liefert dann die Gleichung

$$-C \sin t - D \cos t + 2C \sin t + 2D \cos t = 2 \cos t \Leftrightarrow C \sin t + D \cos t = \cos t.$$

Durch Wahl von $C = 0$ und $D = 2$ erhalten wir die partikuläre Lösung $\mu(t) = 2 \cos t$ und somit die allgemeine Lösung

$$a \sin(\sqrt{2}t) + b \cos(\sqrt{2}t) + 2 \cos t \quad \text{für } a, b \in \mathbb{R}.$$

Für $\omega_0 = \sqrt{2}$ ist $i\sqrt{2}$ eine einfache Nullstelle des charakteristischen Polynoms.
Wir verwenden daher den Ansatz

$$\mu_p(t) = Ct \sin \sqrt{2}t + Dt \cos \sqrt{2}t.$$

Zunächst berechnet man

$$\begin{aligned}\mu'_p(t) &= (C - \sqrt{2}Dt) \sin \sqrt{2}t + (D + \sqrt{2}Ct) \cos \sqrt{2}t, \\ \mu''_p(t) &= (2\sqrt{2}C - 2Dt) \cos \sqrt{2}t - (2\sqrt{2}D + 2Ct) \sin \sqrt{2}t.\end{aligned}$$

Einsetzen in die Differentialgleichung liefert

$$2\sqrt{2}C \cos \sqrt{2}t + 2\sqrt{2}D \sin \sqrt{2}t = 2 \cos \sqrt{2}t.$$

Da $D = 0$ und $C = \frac{\sqrt{2}}{2}$ diese Gleichung lösen, ist die allgemeine Lösung im Fall $\omega_0 = \sqrt{2}$ gegeben durch

$$a \sin(\sqrt{2}t) + b \cos(\sqrt{2}t) + \frac{\sqrt{2}}{2} t \sin \sqrt{2}t \quad \text{für } a, b \in \mathbb{R}.$$

Nicht-konstante Koeffizienten

Im Fall, dass die Koeffizienten der Differentialgleichung nicht konstant sind, sondern von t (bzw. x) abhängen, lässt sich die Gleichung manchmal mit einer Substitution in eine Form bringen, die sich mit den bereits behandelten Methoden lösen lässt.

Aufgabe (Frühjahr 2013, T2A4)

- a) Bestimmen Sie alle reellen Lösungen der Differentialgleichung

$$u'' = -u' - \frac{5}{2}u.$$

- b) Gegeben sei die Differentialgleichung

$$xy''(x) + \frac{1+\sqrt{x}}{2}y'(x) + \frac{5}{8}y(x) = 0 \quad \text{für } x > 0.$$

Durch die Substitution $y(t^2) = u(t)$ ($t > 0$) geht die Differentialgleichung in eine lineare Differentialgleichung mit konstanten Koeffizienten über. Wie lautet diese? Geben Sie die allgemeine reelle Lösung der ursprünglichen Differentialgleichung an.

Lösungsvorschlag zur Aufgabe (Frühjahr 2013, T2A4)

- a** Das charakteristische Polynom der Gleichung lautet $X^2 + X + \frac{5}{2}$ und hat die Nullstellen $-\frac{1}{2} \pm \frac{3}{2}i$. Ein Fundamentalsystem ist deshalb

$$e^{-\frac{1}{2}t} \sin\left(\frac{3}{2}t\right), e^{-\frac{1}{2}t} \cos\left(\frac{3}{2}t\right).$$

- b** Es gilt

$$u'(t) = \frac{d}{dt}y(t^2) = 2ty'(t^2), \quad u''(t) = \frac{d}{dt}2ty'(t^2) = 4t^2y''(t^2) + 2y'(t^2).$$

Aus der Differentialgleichung erhalten wir nun für $x = t^2$ den Ausdruck

$$t^2y''(t^2) = -\frac{1+\sqrt{t^2}}{2}y'(t^2) - \frac{5}{8}y(t^2)$$

und dadurch

$$\begin{aligned} u''(t) &= 4\left(-\frac{1+\sqrt{t^2}}{2}y'(t^2) - \frac{5}{8}y(t^2)\right) + 2y'(t^2) = \\ &= -2y'(t^2) - 2ty'(t^2) - \frac{5}{2}y(t^2) + 2y'(t^2) = \\ &= -u'(t) - \frac{5}{2}u(t). \end{aligned}$$

Dies ist genau die Differentialgleichung aus Teil **a** mit dem dort angegebenen Fundamentalsystem. Die allgemeine Lösung der ursprünglichen Gleichung lautet dementsprechend

$$y(x) = u(\sqrt{x}) = ae^{-\frac{1}{2}\sqrt{x}} \sin\left(\frac{3}{2}\sqrt{x}\right) + be^{-\frac{1}{2}\sqrt{x}} \cos\left(\frac{3}{2}\sqrt{x}\right), \text{ für } a, b \in \mathbb{R}.$$

Aufgabe (Herbst 2011, T3A1)

Bestimmen Sie für die Differentialgleichung

$$y'' + \frac{4}{x}y' - \frac{10}{x^2}y = 0$$

alle reellen Lösungen $y(x)$ auf dem Intervall $]0, \infty[$. Benutzen Sie dazu die Substitution $y(x) = z(\ln x)$ mit $z: \mathbb{R} \rightarrow \mathbb{R}$ oder eine andere Methode Ihrer Wahl.

Lösungsvorschlag zur Aufgabe (Herbst 2011, T3A1)

Sei y eine Lösung. Für die angegebene Substitution erhält man dann

$$y'(x) = z'(\ln x) \cdot \frac{1}{x}, \quad y''(x) = z''(\ln x) \cdot \frac{1}{x^2} - z'(\ln x) \cdot \frac{1}{x^2}.$$

Durch Einsetzen in die Differentialgleichung folgt

$$z''(\ln x) \cdot \frac{1}{x^2} - z'(\ln x) \cdot \frac{1}{x^2} + \frac{4}{x} z'(\ln x) \cdot \frac{1}{x} - \frac{10}{x^2} z(\ln x) = 0.$$

Multiplizieren mit x^2 ergibt

$$z''(\ln x) + 3z'(\ln x) - 10z(\ln x) = 0.$$

Nun hat die Gleichung

$$z'' + 3z' - 10z = 0$$

das charakteristische Polynom $X^2 + 3X - 10 = (X - 2)(X + 5)$ mit den Nullstellen 2 und -5 , sodass $\{e^{2x}, e^{-5x}\}$ ein Fundamentalraum der Gleichung bildet. Damit hat jede Lösung der Gleichung die Form

$$y(x) = z(\ln x) = ae^{2\ln x} + be^{-5\ln x} = ax^2 + bx^{-5} \quad \text{für } a, b \in \mathbb{R}.$$

Umgekehrt sieht man leicht, dass alle solche Funktionen auch Lösungen der Differentialgleichung sind.

7.5. Ebene autonome Systeme

Dieser Abschnitt behandelt zweidimensionale (oder ebene) Systeme von Differentialgleichungen erster Ordnung. Die linearen Systeme bieten hier nichts wirklich Neues, denn sie lassen sich mit den Methoden aus Abschnitt 7.3 abhandeln. Für nicht-lineare Systeme ergeben sich jedoch einige neue Ansätze. Im gesamten Abschnitt beschäftigen wir uns mit einem auf einer Menge $D \subseteq \mathbb{R}^2$ gegebenen Differentialgleichungssystem der Form

$$\dot{x} = f(x, y), \quad \dot{y} = g(x, y), \tag{*}$$

mit stetigen Funktionen $f, g: D \rightarrow \mathbb{R}$, sodass $(x, y) \mapsto (f(x, y), g(x, y))$ Lipschitzstetig ist.

Erhaltungsgrößen und Hamiltonsche Systeme

Definition 7.22. Gegeben sei wiederum ein System der Form (\star) . Eine Funktion $E: D \rightarrow \mathbb{R}$, die für $(x, y) \in D$ die Gleichung

$$\partial_x E(x, y) \cdot f(x, y) + \partial_y E(x, y) \cdot g(x, y) = 0$$

erfüllt, heißt *Erstes Integral* oder *Erhaltungsgröße* des Systems.

Ist E eine Erhaltungsgröße und $\mu: I \rightarrow \mathbb{R}^2$ eine Lösung der Differentialgleichung, so gilt

$$\frac{d}{dt} E(\mu(t)) = \langle \nabla E(\mu(t)), \mu'(t) \rangle = \left\langle \begin{pmatrix} \partial_x E(\mu(t)) \\ \partial_y E(\mu(t)) \end{pmatrix}, \begin{pmatrix} f(\mu(t)) \\ g(\mu(t)) \end{pmatrix} \right\rangle = 0,$$

also ist E konstant entlang der Trajektorie von μ , was den Namen Erhaltungsgröße erklärt.

Ein Spezialfall von Definition 7.22 sind sogenannte Hamilton'sche Systeme.

Definition 7.23. Gegeben sei ein System der Form (\star) . Eine *Hamilton-Funktion* des Systems ist eine differenzierbare Funktion $H: D \rightarrow \mathbb{R}$ mit

$$\partial_x H(x, y) = -g(x, y) \quad \text{und} \quad \partial_y H(x, y) = f(x, y) \quad \text{für } (x, y) \in D.$$

Leider sind ebene Systeme im Allgemeinen nicht hamiltonsch – die folgende Proposition liefert hierzu ein Kriterium.

Proposition 7.24 (Integrabilitätsbedingung für hamiltonsche Systeme). Sei ein System der Form (\star) gegeben, dessen Definitionsmenge D ein einfach zusammenhängendes Gebiet ist. Es existiert genau dann eine Hamilton-Funktion für das System, wenn für alle $(x, y) \in D$ die Gleichung

$$\partial_x f(x, y) + \partial_y g(x, y) = 0,$$

erfüllt ist.

Aufgabe (Herbst 2010, T2A3)

Für das Differentialgleichungssystem

$$\begin{pmatrix} \dot{x}_1 \\ \dot{x}_2 \end{pmatrix} = \begin{pmatrix} x_2 \\ x_1 \end{pmatrix}$$

bestimme man ein nicht-konstantes Erstes Integral, d.h. eine nicht-konstante Funktion $E: \mathbb{R}^2 \rightarrow \mathbb{R}$, die längs der Lösungskurven $\begin{pmatrix} x_1(t) \\ x_2(t) \end{pmatrix}$ konstant ist.

Lösungsvorschlag zur Aufgabe (Herbst 2010, T2A3)

Das System ist auf dem einfach zusammenhängenden Gebiet \mathbb{R}^2 definiert. Die Integrabilitätsbedingung lautet

$$\partial_{x_1}(x_2) + \partial_{x_2}(x_1) = 0 + 0 = 0,$$

also ist das System hamiltonsch. Wir bestimmen nun eine Hamiltonfunktion H (denn diese ist stets ein Erstes Integral). H muss die Gleichungen

$$\partial_{x_1}H(x_1, x_2) = -x_1 \quad \text{und} \quad \partial_{x_2}H(x_1, x_2) = x_2$$

erfüllen. Wir integrieren diese beiden Gleichungen zunächst nach x_1 bzw. x_2 und erhalten:

$$\begin{aligned} H(x_1, x_2) - H(0, x_2) &= \int_0^{x_1} -\omega_1 d\omega_1 = -\frac{1}{2}x_1^2, \\ H(x_1, x_2) - H(x_1, 0) &= \int_0^{x_2} \omega_2 d\omega_2 = \frac{1}{2}x_2^2 \end{aligned}$$

Aus der ersten Gleichung folgt $H(x_1, 0) = H(0, 0)$, sodass

$$H(x_1, x_2) = \frac{1}{2}x_2^2 - \frac{1}{2}x_1^2 + H(0, 0).$$

Die Konstante $H(0, 0)$ spielt dabei keine Rolle, wir setzen daher $H(0, 0) = 0$. Für eine Trajektorie $(x_1(t), x_2(t))$ gilt nun

$$\begin{aligned} \frac{d}{dt}H(x_1(t), x_2(t)) &= \frac{d}{dt} \left(\frac{1}{2}x_2(t)^2 - \frac{1}{2}x_1(t)^2 \right) = \\ &= x_2(t)\dot{x}_2(t) - x_1(t)\dot{x}_1(t) = x_2(t)x_1(t) - x_1(t)x_2(t) = 0. \end{aligned}$$

Also ist H längs der Lösungskurven konstant.

Aufgabe (Frühjahr 2005, T1A2)

Gegeben sei das gewöhnliche Differentialgleichungssystem²

$$\dot{x} = y, \quad \dot{y} = -x + x^2.$$

Bestimmen Sie ein erstes Integral des Systems.

² Die ursprüngliche Aufgabenstellung enthielt auch die Frage nach Ruhelagen, deren Linearisierung und die Stabilität der Linearisierung. Da dies jedoch wenig Spannendes bringt, haben wir sie hier unterlassen. Für Interessierte: Die Ruhelagen sind $(0, 0)$ und $(1, 0)$ - die Linearisierung der ersten Ruhelage ist stabil, die zweite instabil.

Lösungsvorschlag zur Aufgabe (Frühjahr 2005, T1A2)

Wir untersuchen zunächst, ob das System hamiltonsch ist. Der Definitionsbereich ist \mathbb{R}^2 , also einfach zusammenhängend. Die Integrabilitätsbedingung ist hier

$$\partial_x(y) + \partial_y(-x + x^2) = 0 + 0 = 0.$$

Also haben wir Glück. Wir bestimmen eine Hamiltonfunktion nun durch doppelte Integration:

$$\begin{aligned} H(x, y) - H(0, y) &= \int_0^x \omega^2 - \omega d\omega = \frac{1}{3}x^3 - \frac{1}{2}x^2 \\ H(x, y) - H(x, 0) &= \int_0^y \omega d\omega = \frac{1}{2}y^2 \end{aligned}$$

Auswerten der ersten Gleichung bei $y = 0$ und Einsetzen in die zweite liefert

$$H(x, y) = \frac{1}{3}x^3 - \frac{1}{2}x^2 + \frac{1}{2}y^2 + H(0, 0)$$

mit einer frei wählbaren Konstante $H(0, 0)$.

Aufgabe (Herbst 2008, T3A3)

Betrachtet wird das ebene System

$$\begin{aligned} \dot{x} &= y \\ \dot{y} &= -\sin x \end{aligned}$$

um den Gleichgewichtspunkt $(0, 0)$.

- a** Finden sie ein stetig differenzierbares $H = H(x, y)$, das auf den Lösungen des Systems konstant ist.

Hinweis Suchen Sie ein H mit $\dot{x} = H_y, \dot{y} = -H_x$. Warum ist H dann konstant auf den Lösungen des Systems?

- b** Begründen Sie anschaulich, warum die Lösungskurven $(x(t), y(t))$ in der Nähe von $(0, 0)$ geschlossen sind.

Hinweis Untersuchen Sie H auf Extrema.

Lösungsvorschlag zur Aufgabe (Herbst 2008, T3A3)

- a** Man überprüft schnell, dass die Integrabilitätsbedingung erfüllt ist und begibt sich direkt auf die Suche nach einer Hamilton-Funktion. Mittels doppelter Integration oder etwas Probieren findet man

$$H(x, y) = \frac{1}{2}y^2 - \cos x \quad \text{mit} \quad \partial_x H(x, y) = \sin x, \quad \partial_y H(x, y) = y.$$

Ist $(x(t), y(t))$ eine Lösung des Systems, so gilt

$$\begin{aligned} \frac{d}{dt}H(x(t), y(t)) &= \frac{d}{dt}\left(\frac{1}{2}y^2(t) - \cos x(t)\right) = y(t)y'(t) + \sin x(t)x'(t) = \\ &= y(t)(-\sin x(t)) + \sin x(t)y(t) = 0. \end{aligned}$$

Damit ist H entlang der Trajektorien von Lösungen konstant.

- b** Der Gradient von H ist gegeben durch

$$(\nabla H)(x, y) = \begin{pmatrix} \sin x \\ y \end{pmatrix}$$

und verschwindet in den Punkten $(k\pi, 0)$ mit $k \in \mathbb{Z}$. Die Hesse-Matrix ist

$$(\mathcal{H}H)(x, y) = \begin{pmatrix} \cos x & 0 \\ 0 & 1 \end{pmatrix}.$$

Im Punkt $(0, 0)$ ist $(\mathcal{H}H)(x, y) = \mathbb{E}_2$, also positiv definit, sodass $(0, 0)$ ein striktes lokales Minimum von H ist. Anschaulich gesehen bildet H in der Nähe von $(0, 0)$ also einen Krater mit tiefstem Punkt $(0, 0)$. Die Niveaumengen

$$N_c = \{(x, y) \in \mathbb{R}^2 \mid H(x, y) = c\}$$

sind in der Nähe der Ruhelage $(0, 0)$ daher in etwa kreisförmig und geschlossen. Jede dieser Niveaumengen ist eine disjunkte Vereinigung von Trajektorien. Trajektorien können allgemein nur die Form einer Ruhelage, geschlossenen Kurve oder doppelpunktfreien Kurve ohne ihre Endpunkte annehmen. Falls also nicht die gesamte Menge N_c einer Trajektorie entspricht, müsste sie in Kurven ohne ihre Endpunkte zerfallen. Anschaulich gesprochen bleibt dabei jedoch immer ein Punkt „übrig“, der auf keiner Trajektorie liegt. Dieser wäre dann wieder eine Ruhelage. Da wir unsere Betrachtungen nur auf eine Umgebung von $(0, 0)$ beschränken, ist $(0, 0)$ dort die einzige Ruhelage. Also muss die gesamte Menge N_c bereits von einer (geschlossenen) Trajektorie eingenommen werden.

Das genaue Phasenportrait der Gleichung findet sich auf Seite 612.

Anleitung: Phasenportraits mittels Erhaltungsgröße

Gegeben sei ein ebenes autonomes System

$$\begin{pmatrix} \dot{x} \\ \dot{y} \end{pmatrix} = f(x, y)$$

mit Erstem Integral E , dessen Phasenportrait skizziert werden soll.

- (1) Bestimme die Ruhelagen der Differentialgleichung, d. h. alle Punkte (x_0, y_0) mit $f(x_0, y_0) = (0, 0)$.
- (2) Da Erste Integrale entlang der Lösungskurven konstant sind, erfüllen Lösungen $(x(t), y(t))$, die auf die Ruhelage zu bzw. von ihr weglauen, die Gleichung

$$E(x(t), y(t)) = E(x_0, y_0).$$

Vereinfache diese Gleichung und zeichne die entsprechenden Niveaumengen in ein Koordinatensystem ein.

- (3) Der Tangentialvektor im Punkt (x, y) einer Trajektorie ist jeweils durch $f(x, y)$ gegeben. Auf diese Weise lassen sich Richtungspfeile bestimmen.
- (4) Die Trajektorien der übrigen Lösungen nähern sich (bei nicht allzu verrückten Systemen) den soeben bestimmten Trajektorien an.

Aufgabe (Frühjahr 2004, T3A5)

Betrachtet wird das autonome Differentialgleichungssystem im \mathbb{R}^2

$$\begin{aligned} \dot{x} &= x \\ \dot{y} &= x^2 - y. \end{aligned}$$

- a** Zeigen Sie, dass das System genau einen Gleichgewichtspunkt besitzt, und untersuchen Sie dessen Stabilität.
- b** Bestimmen Sie eine Funktion $\varphi: \mathbb{R}^2 \rightarrow \mathbb{R}$, sodass die Phasenkurven des Systems auf den Niveaumengen $\{(x, y) \in \mathbb{R}^2 \mid \varphi(x, y) - c = 0\}$ mit $c \in \mathbb{R}$ liegen.
- c** Skizzieren Sie das Phasenporträt, hierin insbesondere die Lösungskurven (mit Richtungspfeilen), die auf den Gleichgewichtspunkt zu bzw. von ihm weglauen. Von welchem Typ (Knoten, Sattel usw.) ist der Gleichgewichtspunkt?

Lösungsvorschlag zur Aufgabe (Frühjahr 2004, T3A5)

- a** Die Ruhelagen sind genau die Nullstellen der rechten Seite und bestimmen sich daher aus

$$x = 0 \quad x^2 - y = 0.$$

Die einzige Ruhelage ist damit $(0, 0)$. Bezeichnet f die rechte Seite der Gleichung, so ist

$$(Df)(x, y) = \begin{pmatrix} 1 & 0 \\ 2x & -1 \end{pmatrix} \quad \text{und} \quad (Df)(0, 0) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Die Matrix $(Df)(0, 0)$ hat die Eigenwerte 1 und -1 , damit ist $(0, 0)$ nach Satz 7.30 eine instabile Ruhelage.

- b** Die Integrabilitätsbedingung lautet hier

$$\frac{d}{dx}(x) + \frac{d}{dy}(x^2 - y) = 1 - 1 = 0,$$

sodass wir uns auf die Suche nach einer Hamilton-Funktion machen können. Man erhält durch doppelte Integration oder etwas Überlegen

$$H(x, y) = -\frac{1}{3}x^3 + xy.$$

Wie wir gesehen haben, ist eine Hamilton-Funktion auf Lösungskurven konstant, sodass $\varphi = H$ die gewünschte Eigenschaft besitzt.

- c** 1. Schritt: Ruhelagen. Siehe Teil **a**.

2. Schritt: Lösungen, die auf Ruhelagen zulaufen. Für jede Lösung $(x(t), y(t))$, die auf die Ruhelage $(0, 0)$ zu bzw. von ihr weg läuft, gilt

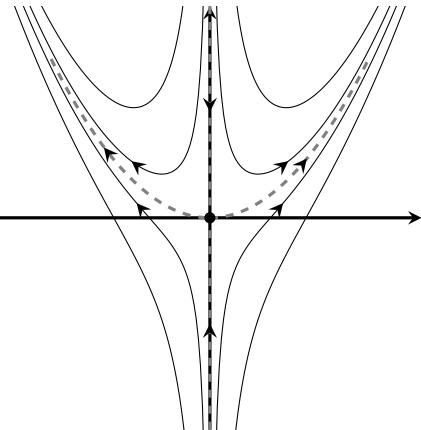
$$H(x(t), y(t)) = H(0, 0) = 0.$$

Solche Lösungen sind also in der Menge $M = \{(x, y) \in \mathbb{R}^2 \mid H(x, y) = 0\}$ enthalten. Nun haben wir

$$H(x, y) = 0 \Leftrightarrow x \left(-\frac{1}{3}x^2 + y \right) = 0 \Leftrightarrow x = 0 \quad \text{oder} \quad y = \frac{1}{3}x^2,$$

also ist M die Vereinigung der y -Achse und der Parabel mit der Gleichung $y = \frac{1}{3}x^2$.

In den Punkten $(0, y)$ mit $y \in \mathbb{R}$ gilt $\dot{x} = 0, \dot{y} = -y$. Auf der positiven y -Achse zeigen die Pfeile damit nach unten, auf der negativen nach oben.



Auf der Parabel haben wir $\dot{y} = \frac{2}{3}x^2 > 0$. Im I. Quadranten (also $x > 0$) ist damit $\dot{x} > 0$ und $\dot{y} > 0$, also zeigen die Pfeile nach „rechts oben“, im II. Quadranten zeigen sie wegen $x < 0$ nach „links oben“. Die restlichen Kurven zeichnet man nun so ein, dass sie sich der Form der auf $(0,0)$ zulaufenden Ruhelagen annähern. Auf diese Weise erhält man nebenstehendes Phasenportrait.

Aufgabe (Frühjahr 2009, T3A3)

Gegeben sei die skalare Differentialgleichung zweiter Ordnung

$$\ddot{x} = 2x - 4x^3.$$

- a** Bestimmen Sie alle stationären Lösungen dieser Differentialgleichung.
- b** Bestimmen Sie eine Erhaltungsgröße (ein erstes Integral für diese Differentialgleichung).
- c** Zeigen Sie, dass alle maximalen Lösungen der Gleichung auf ganz \mathbb{R} existieren.
- d** Skizzieren Sie das Phasenportrait für diese Differentialgleichung. Begründen Sie mit dessen Hilfe, welche der stationären Punkte stabil, welche instabil sind. Besitzt die Differentialgleichung nicht konstante, periodische Lösungen?

Lösungsvorschlag zur Aufgabe (Frühjahr 2009, T3A3)

- a** Ist $\mu(t) \equiv \xi_0$ eine stationäre Lösung, so muss $\dot{\mu}(t) = 0$ gelten. Also muss ξ_0 eine Nullstelle der rechten Seite der Gleichung sein. Nun ist

$$2x - 4x^3 = 0 \Leftrightarrow -2x(2x^2 - 1) = 0 \Leftrightarrow x \in \left\{ 0, \frac{1}{\sqrt{2}}, -\frac{1}{\sqrt{2}} \right\}.$$

Die stationären Lösungen sind also die konstanten Abbildungen

$$\mathbb{R} \rightarrow \mathbb{R}, t \mapsto 0, \quad \mathbb{R} \rightarrow \mathbb{R}, t \mapsto \frac{1}{\sqrt{2}}, \quad \mathbb{R} \rightarrow \mathbb{R}, t \mapsto -\frac{1}{\sqrt{2}}.$$

b Das äquivalente, zweidimensionale System lautet

$$\dot{x} = y, \quad \dot{y} = 2x - 4x^3.$$

Wegen

$$\partial_x(y) + \partial_y(2x - 4x^3) = 0 + 0 = 0$$

ist die Gleichung hamiltonsch. Ohne große Mühe berechnet man die Hamilton-Funktion

$$H(x, y) = \frac{1}{2}y^2 - x^2 + x^4.$$

Diese ist eine Erhaltungsgröße im dem Sinne, dass für eine Lösung λ der Differentialgleichung zweiter Ordnung $H(\lambda(t), \lambda'(t))$ konstant ist.

c Sei $\lambda: I \rightarrow \mathbb{R}^2$ mit $I =]a, b[$ eine maximale Lösung und $t_0 = \frac{a+b}{2}$. Setze $c = H(\lambda(t_0))$, dann gilt für alle $t \in I$ die Gleichung $c = H(\lambda(t))$. Es folgt:

$$\begin{aligned} c &= H(\lambda_1(t), \lambda_2(t)) = \frac{1}{2}\lambda_2(t)^2 - \lambda_1(t)^2 + \lambda_1(t)^4 = \\ &= \frac{1}{2}\lambda_2(t)^2 + \lambda_1(t)^2 + (1 - \lambda_1(t)^2) - 1 \geq \\ &\geq \frac{1}{2}(\lambda_2(t)^2 + \lambda_1(t)^2) - 1 \end{aligned}$$

Folglich ist $\|\lambda(t)\| \leq 2(1 + c)$ für alle $t \in I$. Da der Rand des Definitionsbereichs der Differentialgleichung leer und λ beschränkt ist, muss λ nach Satz 7.13 auf ganz \mathbb{R} definiert sein.

d Das Phasenporträt muss aufgrund der Struktur der Differentialgleichung punktsymmetrisch zum Ursprung sein: Ist nämlich $\lambda(t) = (\lambda_1(t), \lambda_2(t))$ eine Lösung des ebenen Systems, so überprüft man, dass auch durch

$$\mathbb{R} \rightarrow \mathbb{R}, \quad t \mapsto (-\lambda_1(t), -\lambda_2(t))$$

eine Lösung des Systems gegeben ist. Es genügt daher, den Verlauf der Trajektorien für $x \geq 0$ näher zu untersuchen.

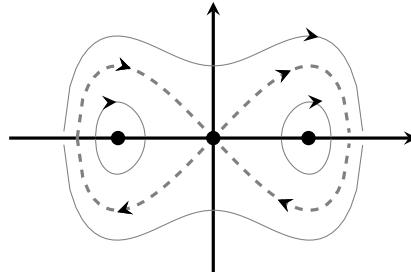
Zunächst bestimmen wir die Niveaumengen von H in diesem Bereich. Für vorgegebenes $c \in \mathbb{R}$ gilt

$$H(x, y) = c \Leftrightarrow \frac{1}{2}y^2 - x^2 + x^4 = c \Leftrightarrow y = \pm \sqrt{2x^2 - 2x^4 + 2c}.$$

Wir berechnen noch den Schnittpunkt mit der x -Achse:

$$-2x^4 + 2x^2 + 2c = 0 \Leftrightarrow x^2 = \frac{1}{2} \pm \frac{1}{2}\sqrt{1 + 4c}.$$

Man kann nun ein paar Werte für c einsetzen, die erhaltenen Schnittpunkte im Koordinatensystem eintragen und in etwa „wurzelförmig“ miteinander verbinden. Spiegelt man das Ganze am Ursprung, sollte in etwa Folgendes dabei herauskommen:



Die Ruhelagen $\pm \frac{1}{\sqrt{2}}$ werden von benachbarten Trajektorien umlaufen, sind also stabil. Im ersten Quadranten ist $\dot{x} = y > 0$, im vierten erhalten wir $\dot{x} = y < 0$. Außerdem ist für kleines x auch $\dot{y} = 2x - 4x^3 > 0$, sodass die Pfeile im ersten Quadranten in der Nähe von $(0,0)$ vom Ursprung wegzeigen müssen, im vierten zum Ursprung hin. Die Pfeile für $x < 0$ ergeben sich aus der Symmetrie. Insgesamt ist $(0,0)$ eine instabile Ruhelage.

Polarcoordinaten

Gelegentlich kommt es vor, dass die Aufgabenstellung die Transformation einer Differentialgleichung in Polarkoordinaten verlangt. Ein Punkt $(x(t), y(t)) \in \mathbb{R}^2$ in kartesischen Koordinaten hat in Polarkoordinaten die Form

$$(x(t), y(t)) = (r(t) \cos \theta(t), r(t) \sin \theta(t)),$$

wobei $r(t) = \|(x(t), y(t))\|$ und $\theta(t) = \arctan \frac{y(t)}{x(t)}$, falls $x(t) \neq 0$. Die Variablentransformation kann dann wie im Kasten auf Seite 404 beschrieben durchgeführt werden.

Aufgabe (Frühjahr 2006, T1A4)

Auf $\mathbb{R}^2 \setminus \{(0,0)\}$ sei folgendes Vektorfeld gegeben

$$f \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} -y \\ x \end{pmatrix} + (1 - \sqrt{x^2 + y^2}) \begin{pmatrix} x \\ y \end{pmatrix}.$$

Für alle Lösungen $\alpha:]a, \infty[\rightarrow \mathbb{R}^2 \setminus \{(0,0)\}$ der Differentialgleichung $\begin{pmatrix} x' \\ y' \end{pmatrix} = f \begin{pmatrix} x \\ y \end{pmatrix}$ zeige man: $\lim_{t \rightarrow +\infty} \|\alpha(t)\| = 1$.

Hinweis Man leite zunächst eine Differentialgleichung her, der die Funktion $r(t) = \|\alpha(t)\|$ genügt.

Lösungsvorschlag zur Aufgabe (Frühjahr 2006, T1A4)

Sei $\alpha(t)$ eine Lösung der Gleichung zu einem Anfangswert $\alpha(\tau) = (\xi_1, \xi_2)$ mit $(\xi_1, \xi_2) \neq (0, 0)$. Wegen

$$\|\alpha(t)\| = \sqrt{x^2(t) + y^2(t)}$$

handelt es sich bei $r(t)$ um die uns bereits bekannte Radius-Funktion. Für diese gilt

$$r'(t) = \frac{2x(t)x'(t) + 2y(t)y'(t)}{2\sqrt{x^2(t) + y^2(t)}} = \frac{1}{r(t)} \cdot [x(t)x'(t) + y(t)y'(t)].$$

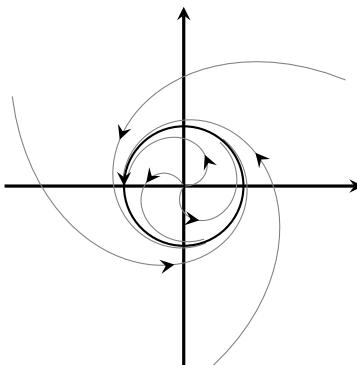
Setzen wir die Differentialgleichung ein, so erhalten wir

$$\begin{aligned} r'(t) &= \frac{1}{r(t)} [x(t)(-y(t) + (1 - r(t))x(t)) + y(t)(x(t) + (1 - r(t))y(t))] = \\ &= \frac{(1 - r(t))(x^2(t) + y^2(t))}{r(t)} = \frac{(1 - r(t))r(t)}{r(t)} = 1 - r(t). \end{aligned}$$

Diese Differentialgleichung für r kann man beispielsweise mittels Variation der Konstanten zur Anfangsbedingung $r(\tau) = r_0$ lösen. Man erhält als Ergebnis die Funktion $\rho(t) = (r_0 - 1)e^{\tau-t} + 1$.

Da die Differentialgleichung für r die Voraussetzungen des Globalen Existenz- und Eindeutigkeitssatzes 7.12 erfüllt, muss $\|\alpha(t)\|$ für jede Lösung α der ursprünglichen Differentialgleichung eine Einschränkung von ρ sein. Laut Aufgabenstellung soll außerdem α den Bildbereich $\mathbb{R}^2 \setminus \{(0, 0)\}$ haben, sodass $r_0 \neq 0$. Es folgt:

$$\lim_{t \rightarrow \infty} \|\alpha(t)\| = \lim_{t \rightarrow \infty} \rho(t) = \lim_{t \rightarrow \infty} (r_0 - 1)e^{\tau-t} + 1 = 1.$$



Aufgabe (Frühjahr 2010, T2A5)

Betrachten Sie das System gewöhnlicher Differentialgleichungen

$$\begin{aligned}\dot{x}_1 &= -x_2 + x_1 \left(\lambda - (x_1^2 + x_2^2)^2 \right) \\ \dot{x}_2 &= x_1 + x_2 \left(\lambda - (x_1^2 + x_2^2)^2 \right)\end{aligned}$$

mit einem positiven Parameter $\lambda > 0$.

- a** Bestimmen Sie mithilfe von Polarkoordinaten $x_1 = r \cos \theta, x_2 = r \sin \theta$ alle periodischen Lösungen sowie deren (minimale) Periode $T > 0$.
- b** Bestimmen Sie für jede Lösung des Systems den Grenzwert $\lim_{t \rightarrow \infty} \|x(t)\|$.

Lösungsvorschlag zur Aufgabe (Frühjahr 2010, T2A5)

- a** Wir definieren die neuen Variablen $r(t) = \sqrt{x_1^2(t) + x_2^2(t)}$ und $\theta(t) = \arctan \frac{y(t)}{x(t)}$, dann erhält man durch Variablentransformation die neuen Differentialgleichungen

$$r'(t) = r(t)(\lambda - r^4(t)) \quad \text{und} \quad \theta'(t) = 1.$$

Ist μ eine periodische Lösung der ursprünglichen Differentialgleichung, so ist $\rho(t) = \|\mu(t)\|$ ebenfalls periodisch und eine Lösung der neuen Differentialgleichung für r . Sei T die Periodenlänge von ρ . Nach dem Maximumsprinzip hat ρ ein Maximum auf dem Intervall $[0, T]$ und da der Wertevorrat von ρ bereits durch $\rho([0, T])$ gegeben ist, handelt es sich dabei auch um ein globales Maximum. Insbesondere gibt es ein $\tau \in [0, T]$ mit $\rho'(\tau) = 0$. Aus der Differentialgleichung folgt nun

$$\rho(\tau) \in \{0, \sqrt[4]{\lambda}, -\sqrt[4]{\lambda}\}.$$

Da die Differentialgleichung die Voraussetzungen des Globalen Existenz- und Eindeutigkeitssatzes erfüllt, sind die eindeutigen Lösungen zu diesem Anfangswert die konstanten Lösungen

$$\mathbb{R} \rightarrow \mathbb{R}, t \mapsto 0, \quad \mathbb{R} \rightarrow \mathbb{R}, t \mapsto \sqrt[4]{\lambda}, \quad \mathbb{R} \rightarrow \mathbb{R}, t \mapsto -\sqrt[4]{\lambda}.$$

Also muss ρ mit einer dieser Lösungen übereinstimmen. Wegen $\rho(t) = \|\mu(t)\| \geq 0$ scheidet dabei die dritte Möglichkeit aus. Falls ρ die Nullfunktion ist, so ist μ ebenfalls die (pseudo-)periodische Nullfunktion.

Für den Fall $\rho(t) = \sqrt[4]{\lambda}$ schließlich bestimmen wir noch die zugehörige Winkelfunktion aus der zweiten Differentialgleichung:

$$\theta'(t) = 1 \Leftrightarrow \theta(t) = t - t_0$$

für ein $t_0 \in \mathbb{R}$. Damit erhalten wir die Funktion

$$\mu: \mathbb{R} \rightarrow \mathbb{R}^2, t \mapsto \left(\sqrt[4]{\lambda} \cos(t - t_0), \sqrt[4]{\lambda} \sin(t - t_0) \right),$$

welche auch tatsächlich die anfängliche Differentialgleichung löst. Die Periodenlänge dieser Lösung ist $T = 2\pi$.

- b** Sei wieder $\mu: \mathbb{R} \rightarrow \mathbb{R}$ eine Lösung der Differentialgleichung und $\rho(t) = \|\mu(t)\|$. Dann ist laut **a** die Funktion ρ eine Lösung von

$$r' = r(\lambda - r^4), \quad r(0) = r_0.$$

Falls $r_0 = 0$, so haben wir bereits gesehen, dass ρ die Nullfunktion sein muss, sodass $\lim_{t \rightarrow \infty} \rho(t) = 0$. Falls $r_0 = \sqrt[4]{\lambda}$, so ist $\rho(t) = \sqrt[4]{\lambda}$ für alle $t \in \mathbb{R}$, sodass hier $\lim_{t \rightarrow \infty} \rho(t) = \sqrt[4]{\lambda}$. Wir können daher $r_0 \notin \{0, \sqrt[4]{\lambda}\}$ voraussetzen, wobei wir zunächst den Fall $0 < r_0 < \sqrt[4]{\lambda}$ betrachten.

Da der Globale Existenz- und Eindeutigkeitssatz auf die Differentialgleichung für r anwendbar ist, muss $0 < \rho(t) < \sqrt[4]{\lambda}$ für alle $t \in \mathbb{R}$ gelten (vgl. (2) im Kasten auf Seite 419). Es folgt, dass

$$\rho'(t) = \rho(t)(\lambda - \rho^4(t)) > 0 \quad \text{für alle } t \in \mathbb{R},$$

also ist ρ streng monoton steigend. Da ρ weiterhin durch $\sqrt[4]{\lambda}$ beschränkt ist, existiert der Grenzwert $\lim_{t \rightarrow \infty} \rho(t)$ schon mal und ist ebenfalls höchstens gleich $\sqrt[4]{\lambda}$. Angenommen, es ist $\lim_{t \rightarrow \infty} \rho(t) = c$ mit $c < \sqrt[4]{\lambda}$, dann haben wir $\rho(t) < c$ für alle $t \in \mathbb{R}$ und

$$\begin{aligned} \rho(t) &= \rho(0) + \int_0^t \rho'(\tau) d\tau = \rho(0) + \int_0^t \rho(\tau)(\lambda - \rho^4(\tau)) d\tau \geq \\ &\geq \rho(0) - \int_0^t \rho(0)(\lambda - c^4) d\tau = \rho(0)(1 + (\lambda - c^4)t) \xrightarrow{t \rightarrow \infty} \infty \end{aligned}$$

im Widerspruch dazu, dass ρ beschränkt ist. Also muss $\lim_{t \rightarrow \infty} \rho(t) = \sqrt[4]{\lambda}$ gelten. Für den Fall $r_0 > \sqrt[4]{\lambda}$ zeigt man in gleicher Weise, dass ebenfalls $\lim_{t \rightarrow \infty} \rho(t) = \sqrt[4]{\lambda}$ erfüllt ist.

7.6. Stabilitätsuntersuchungen

Differentialgleichungen können sich sehr schnell als zu schwierig herausstellen, um sie explizit zu lösen. In solchen Situationen ist man daran interessiert, zumindest qualitative Aussagen über das Verhalten von Lösungen einer solchen Differentialgleichung zu machen. Eine natürliche Fragestellung ist dabei, wie sich eine kleine Änderung des Startwertes auf die zugehörige Lösung auswirkt.

Wir benennen nun zunächst die in dieser Situation auftretenden Formen des Verhaltens von Lösungen. Zur Veranschaulichung der Begriffe sei auf die Abbildungen 7.2 und 7.3 verwiesen.

Definition 7.25. Sei $n \in \mathbb{N}$, $V \subseteq \mathbb{R} \times \mathbb{R}^n$ offen und zusammenhängend, $f: V \rightarrow \mathbb{R}^n$ stetig sowie lokal Lipschitz-stetig bezüglich x . Eine Lösung

$$\mu:]a, \infty[\rightarrow \mathbb{R}^n \quad \text{von} \quad x' = f(t, x)$$

heißt

- (1) *stabil*, falls es zu jedem $\varepsilon > 0$ und jedem $\tau > a$ ein $\delta > 0$ gibt, sodass für jeden Anfangswert $\xi \in \mathbb{R}^n$ mit $\|\xi - \mu(\tau)\| < \delta$ die maximale Lösung $\lambda(t)$ zum Anfangswert $\lambda(\tau) = \xi$ für alle $t \geq \tau$ existiert und die Abschätzung

$$\|\lambda(t) - \mu(t)\| < \varepsilon \quad \text{für alle } t \geq \tau$$

erfüllt. Ansonsten heißt μ *instabil*.

- (2) *attraktiv*, wenn es zu jedem $\tau > a$ ein $\eta > 0$ gibt, sodass für jeden Anfangswert $\xi \in \mathbb{R}^n$ mit $\|\xi - \mu(t)\| < \eta$ die maximale Lösung $\lambda(t)$ zum Anfangswert $\lambda(\tau) = \xi$ für alle $t \geq \tau$ existiert und

$$\lim_{t \rightarrow \infty} \|\lambda(t) - \mu(t)\| = 0$$

erfüllt.

- (3) *asymptotisch stabil*, falls μ stabil und attraktiv ist.

Proposition 7.26 (Attraktivität und Stabilität bei skalaren Differentialgleichungen). Sei $D \subseteq \mathbb{R}^2$ ein Gebiet und $f: D \rightarrow \mathbb{R}$ stetig und bezüglich x lokal Lipschitz-stetig. Ist eine Lösung von

$$x' = f(t, x)$$

attraktiv, so ist sie auch stabil, d. h. asymptotisch stabil.

Wir werden in Kürze sehen, dass auch für lineare Systeme eine entsprechende Aussage gilt.

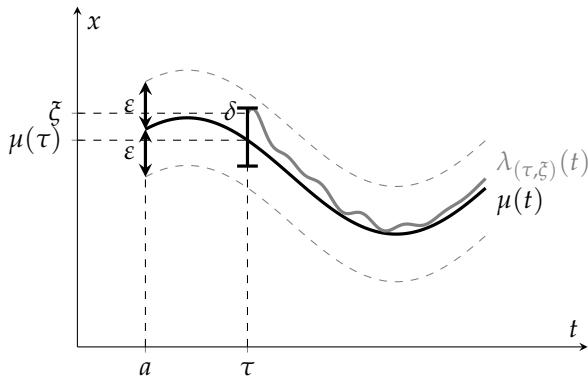


Abbildung 7.2: Illustration der Definition von Stabilität. Eingezeichnet ist eine Lösung $\mu(t)$ sowie eine Lösung für einen leicht veränderten Anfangswert ξ . Die graue Lösung verläuft innerhalb eines ε -Schlauchs um $\mu(t)$.³

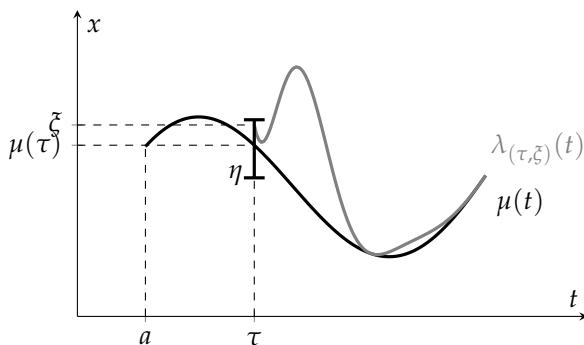


Abbildung 7.3: Illustration der Definition von Attraktivität. Eingezeichnet ist eine Lösung $\mu(t)$ sowie eine Lösung für einen leicht veränderten Anfangswert ξ , die gegen $\mu(t)$ konvergiert.⁴

Direkt anhand der Definition nachzuweisen, ob eine gegebene Lösung stabil bzw. attraktiv ist, ist recht mühsam. Glücklicherweise gibt es hier handlichere Kriterien, die das Leben eines Stabilitätstheoretikers sehr viel einfacher machen.

Stabilitätsuntersuchung linearer Differentialgleichungssysteme

Beschäftigt man sich mit linearen (Differential-)Gleichungssystemen, so lassen sich Aussagen über ein inhomogenes System oft auf das zugehörige homogene System zurückführen. Dies ist auch bei Stabilitätsfragen der Fall.

³ Abbildung in Anlehnung an [Aul04], S. 312.

⁴ Abbildung in Anlehnung an [Aul04], S. 316.

Proposition 7.27 (Einheitliches Stabilitätsverhalten aller Lösungen). Es sei $n \in \mathbb{N}$ und $A:]a, \infty[\rightarrow \mathcal{M}_n(\mathbb{R})$ sowie $g:]a, \infty[\rightarrow \mathbb{R}^n$ seien stetig. Wir betrachten das inhomogene Differentialgleichungssystem

$$x' = A(t) \cdot x(t) + g(t).$$

- (1) Eine Lösung des inhomogenen Systems ist genau dann stabil bzw. attraktiv, wenn die Nulllösung des homogenen Differentialgleichungssystems

$$x' = A(t) \cdot x(t)$$

stabil bzw. attraktiv ist.

- (2) Jede attraktive Lösung des inhomogenen Systems ist stabil, d. h. asymptotisch stabil.

Da also insbesondere das Stabilitätsverhalten *aller* Lösungen einer linearen Differentialgleichung gleich ist, können wir die jeweilige Eigenschaft der Differentialgleichung zuweisen und von einem stabilen, instabilen oder asymptotisch stabilen System sprechen. Wir formulieren nun ein erstes Kriterium für Stabilität bzw. Attraktivität.

Satz 7.28. Sei $n \in \mathbb{N}$, $A:]a, \infty[\rightarrow \mathcal{M}_n(\mathbb{R})$ stetig und $\Lambda(t, \tau)$ die Übergangsmatrix von $x' = A(t)x$. Alle Lösungen dieser Differentialgleichung sind genau dann

- (1) stabil, falls es für alle $T_0 > a$ ein $\beta > 0$ gibt mit $\|\Lambda(t, T_0)\| \leq \beta$ für alle $t \geq T_0$.
(2) attraktiv, wenn $\lim_{t \rightarrow \infty} \Lambda(t, T_0) = 0$ für jedes $T_0 > a$ gilt.

In beiden Fällen genügt es, die Bedingung für eine einzelne Anfangszeit $T_0 > a$ zu überprüfen.

Aufgabe (Herbst 2014, T2A4)

Gegeben sei das Differentialgleichungssystem

$$y'(t) = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & -1 \\ 0 & 0 & -1 \end{pmatrix} y(t).$$

a Bestimmen Sie ein Fundamentalsystem für dieses Differentialgleichungssystem.

b Bestimmen Sie die Lösung dieses Differentialgleichungssystems mit dem Anfangswert

$$y(0) = \begin{pmatrix} 1 \\ 2 \\ 1 \end{pmatrix}.$$

c Ist die Nulllösung für dieses Differentialgleichungssystem stabil?

Lösungsvorschlag zur Aufgabe (Herbst 2014, T2A4)

- a** Da es sich um ein lineares Differentialgleichungssystem handelt, ist ein Fundamentalsystem durch e^{tA} gegeben, wobei A obige Matrix bezeichnet. Um e^{tA} zu berechnen, zeigen wir zunächst per Induktion über n , dass $A^n = (-1)^n A^2$ für alle $n \geq 2$ gilt.

Der Induktionsanfang $n = 2$ ist unmittelbar klar, setzen wir die Aussage also für ein n als bereits bewiesen voraus. Nun gilt

$$\begin{aligned} A^2 &= \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & -1 \\ 0 & 0 & -1 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & -1 \\ 0 & 0 & -1 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix} \\ A^{n+1} &= A^n \cdot A \stackrel{(*)}{=} (-1)^n A^2 \cdot A = (-1)^n \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & -1 \\ 0 & 0 & -1 \end{pmatrix} = \\ &= (-1)^n \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 0 & -1 \end{pmatrix} = (-1)^n \cdot (-A^2) = (-1)^{n+1} A^2, \end{aligned}$$

wobei an der Stelle (*) die Induktionsvoraussetzung verwendet wurde. Dies zeigt die Behauptung. Mithilfe der eben bewiesenen Aussage können wir berechnen:

$$\begin{aligned} e^{tA} &= \sum_{k=0}^{\infty} \frac{1}{k!} A^k t^k = \mathbb{E} + At + \sum_{k=2}^{\infty} \frac{1}{k!} (-1)^k A^2 t^k = \\ &= \mathbb{E} + At + A^2 \sum_{k=2}^{\infty} \frac{1}{k!} (-t)^k = \mathbb{E} + At + A^2 \cdot (e^{-t} + t - 1) = \\ &= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} + \begin{pmatrix} 0 & 0 & 0 \\ t & 0 & -t \\ 0 & 0 & -t \end{pmatrix} + \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & (e^{-t} + t - 1) \\ 0 & 0 & (e^{-t} + t - 1) \end{pmatrix} = \\ &= \begin{pmatrix} 1 & 0 & 0 \\ t & 1 & e^{-t} - 1 \\ 0 & 0 & e^{-t} \end{pmatrix} \end{aligned}$$

- b** Die Übergangsmatrix ist hier durch $\Lambda(t, \tau) = e^{(t-\tau)A}$ gegeben, in unserem Fall also $\Lambda(t, 0) = e^{(t-0)A} = e^{tA}$. Also ist die gesuchte Lösung zum

Anfangswert $\xi = (1, 2, 1)$ gegeben durch

$$\begin{aligned}\lambda(t) &= \Lambda(t, 0)\xi = \begin{pmatrix} 1 & 0 & 0 \\ t & 1 & e^{-t} - 1 \\ 0 & 0 & e^{-t} \end{pmatrix} \begin{pmatrix} 1 \\ 2 \\ 1 \end{pmatrix} = \\ &= \begin{pmatrix} 1 \\ t + 2 + e^{-t} - 1 \\ e^{-t} \end{pmatrix} = \begin{pmatrix} 1 \\ e^{-t} + t + 1 \\ e^{-t} \end{pmatrix}\end{aligned}$$

c Sei $T_0 \in \mathbb{R}$. Wir verwenden die Spaltensummennorm und stellen fest, dass

$$\lim_{t \rightarrow \infty} \|\Lambda(t, T_0)\|_1 \geq \lim_{t \rightarrow \infty} 1 + |t - T_0| = \infty.$$

Also kann $\|\Lambda(t, T_0)\|_1$ für kein T_0 beschränkt sein und nach Satz 7.28 (1) ist die Nulllösung für dieses Differentialgleichungssystem nicht stabil.

Ein besonders praktikables Kriterium für Stabilität liefert der nächste Satz.

Satz 7.29 (Eigenwertbedingung für Stabilität). Sei $n \in \mathbb{N}$ und $A \in \mathcal{M}_n(\mathbb{R})$ mit Eigenwerten $\lambda_1, \dots, \lambda_m \in \mathbb{C}$. Alle Lösungen von $x' = Ax$ sind genau dann

- (1) stabil, wenn $\operatorname{Re} \lambda_1, \dots, \operatorname{Re} \lambda_m \leq 0$ und für jedes $j \in \{1, \dots, m\}$ mit $\operatorname{Re} \lambda_j = 0$ die algebraische und geometrische Vielfachheit von λ_j übereinstimmen.
- (2) asymptotisch stabil, falls $\operatorname{Re} \lambda_1, \dots, \operatorname{Re} \lambda_m < 0$.

Aufgabe (Frühjahr 2009, T2A2)

Es sei

$$A = \begin{pmatrix} -5 & 0 & 3 \\ 0 & -1 & 0 \\ 3 & 0 & -5 \end{pmatrix}.$$

- a** Zeigen Sie, dass die Ruhelage 0 für das System $x' = Ax$ asymptotisch stabil ist.
b Weiterhin sei $b : \mathbb{R} \rightarrow \mathbb{R}^3$ stetig. Zeigen Sie, dass jede Lösung y der Gleichung $y' = Ay + b(t)$ asymptotisch stabil ist, indem Sie zeigen, dass für zwei Lösungen y und \tilde{y} immer gilt:

$$\lim_{t \rightarrow \infty} \|\tilde{y}(t) - y(t)\| = 0.$$

Lösungsvorschlag zur Aufgabe (Frühjahr 2009, T2A2)

- a** Wir berechnen das charakteristische Polynom von A :

$$\begin{aligned}\chi_A &= \det \begin{pmatrix} -5-X & 0 & 3 \\ 0 & -1-X & 0 \\ 3 & 0 & -5-X \end{pmatrix} = -(X+5)^2(X+1) + 9(1+X) \\ &= -(X+1)[X^2 + 10X + 25 - 9] = -(X+1)[X(X+2) + 8(X+2)] = \\ &= -(X+1)(X+2)(X+8)\end{aligned}$$

Die Eigenwerte von A sind also $-1, -2, -8$. Diese sind alle reell und negativ, also ist 0 nach 7.29 (2) eine asymptotisch stabile Ruhelage von $x' = Ax$.

- b** Sei $\Lambda(t, 0)$ die Übergangsmatrix von $x' = Ax$, dann hat jede Lösung y von $x' = Ax + b(t)$ die Form (vgl. den Kasten auf Seite 435)

$$y(t) = \Lambda(t, 0)y(0) + \int_0^t \Lambda(t, s)b(s)ds.$$

Es folgt

$$\|\tilde{y}(t) - y(t)\| = \|\Lambda(t, 0)[\tilde{y}(0) - y(0)]\| \leq \|\Lambda(t, 0)\| \cdot \|\tilde{y}(0) - y(0)\|.$$

Nach Teil **a** ist 0 eine asymptotisch stabile Ruhelage von $x' = Ax$, sodass nach Proposition 7.27 alle Lösungen von $x' = Ax$ asymptotisch stabil sind. Wir können daher Satz 7.28 (2) verwenden und erhalten

$$\lim_{t \rightarrow \infty} \|\tilde{y}(t) - y(t)\| \leq \|\tilde{y}(0) - y(0)\| \cdot \lim_{t \rightarrow \infty} \|\Lambda(t, 0)\| = 0.$$

Aufgabe (Frühjahr 2014, T1A2)

Betrachten Sie die folgende Differentialgleichung:

$$\begin{pmatrix} \dot{x} \\ \dot{y} \end{pmatrix} = \begin{pmatrix} -\frac{5}{4} & \frac{1}{4} \\ -\frac{1}{4} & -\frac{3}{4} \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

- a** Bestimmen Sie die Stabilitätseigenschaften der Ruhelage $(0, 0)$.
b Skizzieren Sie das Phasenporträt.

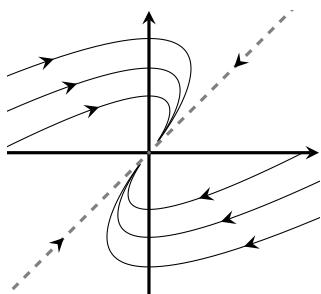
Lösungsvorschlag zur Aufgabe (Frühjahr 2014, T1A2)

- a Wir bestimmen zunächst das charakteristische Polynom der Koeffizientenmatrix

$$\chi = \det \begin{pmatrix} -\frac{5}{4} - X & \frac{1}{4} \\ -\frac{1}{4} & -\frac{3}{4} - X \end{pmatrix} = X^2 + 2X + 1 = (X + 1)^2$$

χ hat eine doppelte Nullstelle bei -1 , also hat die Matrix oben auch nur den Eigenwert -1 , welcher offensichtlich negativen Realteil hat. Nach Satz 7.29 ist deshalb $(0, 0)$ eine asymptotisch stabile Ruhelage.

- b Es ist $(1, 1)$ ein Eigenvektor zum Eigenwert -1 . Damit enthält das Phasenportrait zwei Halbgeraden als Trajektorien, die $(1, 1)$ als Richtungsvektor haben und für $t \rightarrow \infty$ jeweils auf den Ursprung zulaufen.



Auch die anderen Lösungen streben für $t \rightarrow \infty$ gegen den Ursprung, wie man weiß oder Abbildung 7.1 entnimmt, handelt es sich zudem um einen eintangentialen Knoten, sodass wir nebenstehendes Phasenportrait erhalten.

Stabilitätsuntersuchung von Ruhelagen

Während wir im vorigen Abschnitt noch Stabilität beliebiger Lösungen linearer Differentialgleichungen betrachtet haben, beschränken wir uns nun auf konstante Lösungen autonomer Systeme. Diese werden auch als *Ruhelagen* oder *stationäre Punkte* bezeichnet und bestimmen sich für eine Differentialgleichung $x' = g(x)$ als Nullstellen der Funktion $g(x)$.

Das Eigenwertkriterium 7.29 lässt sich ausschließlich auf lineare autonome Differentialgleichungen anwenden. Ist jedoch eine nicht-lineare Differentialgleichung $x' = g(x)$ gegeben, so können wir diese *linearisieren*. Ähnlich wie bei einer linearen Näherung einer Funktion als Gerade geschieht dies unter Zuhilfenahme der Ableitung. Konkret untersucht man dazu die einfachere Differentialgleichung $x' = (Dg)(\xi)x$ für eine Ruhelage ξ .

Satz 7.30 (Linearisierte asymptotische Stabilität). Sei $D \subseteq \mathbb{R}^n$ offen und zusammenhängend, $g: D \rightarrow \mathbb{R}^n$ eine stetig differenzierbare Funktion und $\xi \in D$ mit $g(\xi) = 0$. Es bezeichnen $\lambda_1, \dots, \lambda_m \in \mathbb{C}$ die Eigenwerte der Jacobi-Matrix $(Dg)(\xi)$.

- (1) Gilt $\operatorname{Re} \lambda_1, \dots, \operatorname{Re} \lambda_m < 0$, so ist ξ eine asymptotisch stabile Ruhelage der autonomen Differentialgleichung $x' = g(x)$.
- (2) Gibt es ein $j \in \{1, \dots, m\}$ mit $\operatorname{Re} \lambda_j > 0$, so ist ξ eine instabile Ruhelage von $x' = g(x)$.

Beachte, dass anders als im linearen Fall keine Aussage mehr möglich ist, falls der Realteil eines Eigenwertes 0 ist – mit einer Methode, um dieses Problem zu umgehen, beschäftigen wir uns im nächsten Abschnitt.

Aufgabe (Frühjahr 2015, T2A5)

Gegeben sei das ebene autonome System

$$\begin{aligned} x' &= -e^x - 2y + 1 \\ y' &= 2x - y. \end{aligned}$$

Man bestimme alle Ruhepunkte des Systems und untersuche diese auf Stabilität.

Lösungsvorschlag zur Aufgabe (Frühjahr 2015, T2A5)

Sei $(x, y) \in \mathbb{R}^2$ eine Ruhelage des Systems, dann muss gelten

$$-e^x - 2y + 1 = 0 \quad \text{und} \quad 2x - y = 0.$$

Aus der zweiten Gleichung folgt $y = 2x$, eingesetzt in die erste liefert das

$$-e^x - 4x + 1 = 0.$$

0 ist offensichtlich Lösung dieser Gleichung. Wir zeigen nun, dass es keine weitere geben kann. Nehmen wir an, es gibt $x_0 \in \mathbb{R}$ mit $x_0 \neq 0$ und

$$-e^{x_0} - 4x_0 + 1 = 0,$$

dann müsste die Ableitung der Funktion $x \mapsto -e^x - 4x + 1$ nach dem Satz von Rolle eine Nullstelle zwischen 0 und x_0 haben. Die Ableitung ist jedoch

$$-e^x - 4 < 0 \quad \text{für alle } x \in \mathbb{R}.$$

Also haben wir gezeigt, dass die einzige Lösung obiger Gleichung $x = 0$ ist. Einsetzen in die zweite Gleichung liefert $y = 2 \cdot 0 = 0$. Also ist $(0, 0)$ die einzige Ruhelage des Systems.

Die Jacobi-Matrix des Systems lautet

$$\begin{pmatrix} -e^x & -2 \\ 2 & -1 \end{pmatrix}$$

und hat an der Stelle $(0, 0)$ das charakteristische Polynom

$$\det \begin{pmatrix} -1 - X & -2 \\ 2 & -1 - X \end{pmatrix} = (1 + X)^2 + 4 = X^2 + 2X + 5.$$

Die Eigenwerte der Jacobi-Matrix bei $(0, 0)$ sind daher

$$\lambda_{\pm} = \frac{-2 \pm \sqrt{4 - 4 \cdot 5}}{2} = -1 \pm 2i.$$

Es gilt $\operatorname{Re} \lambda_{\pm} = -1 < 0$, also ist $(0, 0)$ eine asymptotisch stabile Ruhelage.

Aufgabe (Frühjahr 2012, T1A4)

Es sei $f : \mathbb{R}^2 \rightarrow \mathbb{R}^2$

$$\begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} \sin(\pi(x^2 + y^2)) \\ x + \sqrt{3}y \end{pmatrix}$$

- a** Bestimmen Sie alle Ruhelösungen des ebenen autonomen Differentialgleichungssystems

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = f \begin{pmatrix} x \\ y \end{pmatrix}$$

- b** Ist die Ruhelösung $(\frac{\sqrt{3}}{2}, -\frac{1}{2})$ stabil oder instabil?

Lösungsvorschlag zur Aufgabe (Frühjahr 2012, T1A4)

- a** Die Ruhelagen bestimmen sich als Nullstellen von f . Es gelte also

$$\sin(\pi(x^2 + y^2)) = 0 \quad \text{und} \quad x + \sqrt{3}y = 0,$$

dann ist $x = -\sqrt{3}y$ und einsetzen in die erste Gleichung liefert

$$\sin(\pi(3y^2 + y^2)) = 0 \quad \Leftrightarrow \quad 4y^2\pi \in \pi\mathbb{Z}.$$

Es gibt folglich ein $k \in \mathbb{N}_0$, sodass

$$4y^2 = k \Leftrightarrow |y| = \frac{1}{2}\sqrt{k}$$

und folglich $x = -\sqrt{3}y = \mp\frac{1}{2}\sqrt{3k}$. Umgekehrt überzeugt man sich schnell davon, dass $(\mp\frac{1}{2}\sqrt{3k}, \pm\frac{1}{2}\sqrt{k})$ für jedes $k \in \mathbb{N}_0$ eine Nullstelle von f ist. Also ist die Menge der Ruhelösungen gegeben durch

$$\left\{ \left(-\frac{1}{2}\sqrt{3k}, \frac{1}{2}\sqrt{k} \right) \mid k \in \mathbb{N}_0 \right\} \cup \left\{ \left(\frac{1}{2}\sqrt{3k}, -\frac{1}{2}\sqrt{k} \right) \mid k \in \mathbb{N}_0 \right\}.$$

- b** Wir wollen linearisieren und berechnen daher zunächst die Jacobi-Matrix von f :

$$(Df)(x, y) = \begin{pmatrix} \cos(\pi(x^2 + y^2)) \cdot 2\pi x & \cos(\pi(x^2 + y^2)) \cdot 2\pi y \\ 1 & \sqrt{3} \end{pmatrix}$$

Es ist dann

$$(Df)\left(\frac{\sqrt{3}}{2}, -\frac{1}{2}\right) = \begin{pmatrix} \cos(\pi) \cdot \pi\sqrt{3} & \cos(\pi) \cdot \pi \cdot (-1) \\ 1 & \sqrt{3} \end{pmatrix} = \begin{pmatrix} -\pi\sqrt{3} & \pi \\ 1 & \sqrt{3} \end{pmatrix}$$

und das charakteristische Polynom dieser Matrix ist

$$\det \begin{pmatrix} -\pi\sqrt{3} - X & \pi \\ 1 & \sqrt{3} - X \end{pmatrix} = (X + \pi\sqrt{3})(X - \sqrt{3}) - \pi = X^2 + \sqrt{3}(\pi - 1)X - 4\pi.$$

Die Nullstellen dieses Polynoms bestimmen wir mittels Mitternachtsformel:

$$\lambda_{\pm} = \frac{-\sqrt{3}}{2}(\pi - 1) \pm \frac{1}{2}\sqrt{3(\pi - 1)^2 + 16\pi}$$

Der Radikand ist nicht-negativ, also sind die Eigenwerte von $(Df)\left(\frac{\sqrt{3}}{2}, -\frac{1}{2}\right)$ auf jeden Fall reell. Weiter gilt

$$\begin{aligned} \lambda_+ > 0 &\Leftrightarrow \frac{\sqrt{3}}{2}(1 - \pi) + \frac{1}{2}\sqrt{3(1 - \pi)^2 + 16\pi} > 0 \\ &\Leftrightarrow \sqrt{3(1 - \pi)^2 + 16\pi} > -\sqrt{3}(1 - \pi) \Leftrightarrow 3(1 - \pi)^2 + 16\pi > 3(1 - \pi)^2 \\ &\Leftrightarrow 16\pi > 0 \end{aligned}$$

Die letzte Aussage ist offensichtlich wahr, also ist $\lambda_+ > 0$. Nach Satz 7.30 (2) ist deshalb $(\frac{\sqrt{3}}{2}, -\frac{1}{2})$ eine instabile Ruhelage.

Aufgabe (Herbst 2011, T2A5)

Die Gleichung des mathematischen Pendels mit Reibung lautet

$$y''(t) + \varepsilon y'(t) + \sin(y(t)) = 0, \quad t \geq 0,$$

wobei $\varepsilon > 0$.

- a** Überführen Sie diese Gleichung in das zugehörige System erster Ordnung der Form $v'(t) = f(v(t))$ für den Vektor $v = (y, y')$.
- b** Bestimmen Sie die kritischen Punkte des Systems aus **a**.
- c** Untersuchen Sie die kritischen Punkte auf Stabilität und Instabilität.

Lösungsvorschlag zur Aufgabe (Herbst 2011, T2A5)

- a** Schreibe $v_1 = y, v_2 = y'$, dann ist

$$\begin{aligned} v'_1 &= y' = v_2 \\ v'_2 &= y'' = -\varepsilon y' - \sin y = -\varepsilon v_2 - \sin v_1 \end{aligned}$$

Setze also

$$f: \mathbb{R}^2 \rightarrow \mathbb{R}^2, \quad v = (v_1, v_2) \mapsto (v_2, -\varepsilon v_2 - \sin v_1).$$

- b** Die kritischen Punkte entsprechen den Lösungen der Nullstellen-Gleichung $f(v_1, v_2) = (0, 0)$. Die erste Komponente liefert sofort v_2 und für die zweite folgt daraus

$$-\varepsilon v_2 - \sin v_1 = 0 \Leftrightarrow \sin v_1 = 0 \Leftrightarrow v_1 \in \pi\mathbb{Z}.$$

Die kritischen Punkte sind also durch die Menge $\{(k\pi, 0) \mid k \in \mathbb{Z}\}$ gegeben.

- c** Wir berechnen zunächst die Jacobi-Matrix von f allgemein und an der Stelle $(v_1, v_2) = (k\pi, 0)$ für $k \in \mathbb{Z}$ und erhalten

$$(Df)(v_1, v_2) = \begin{pmatrix} 0 & 1 \\ -\cos v_1 & -\varepsilon \end{pmatrix} \quad \text{bzw. } (Df)(k\pi, 0) = \begin{pmatrix} 0 & 1 \\ -\cos k\pi & -\varepsilon \end{pmatrix}.$$

Die zweite Matrix hat für $k \in \mathbb{Z}$ das charakteristische Polynom

$$\det \begin{pmatrix} -X & 1 \\ -\cos k\pi & -\varepsilon - X \end{pmatrix} = X(X + \varepsilon) + \cos k\pi = X^2 + \varepsilon X + (-1)^k.$$

Die Nullstellen dieses Polynoms sind

$$\begin{aligned}\lambda_{1,\pm} &= -\frac{\varepsilon}{2} \pm \frac{1}{2}\sqrt{\varepsilon^2 + 4} && \text{für ungerades } k, \\ \lambda_{2,\pm} &= -\frac{\varepsilon}{2} \pm \frac{1}{2}\sqrt{\varepsilon^2 - 4} && \text{für gerades } k.\end{aligned}$$

Die Eigenwerte $\lambda_{1,\pm}$ sind auf jeden Fall reell. Außerdem ist

$$\lambda_{1,+} = -\frac{\varepsilon}{2} + \frac{1}{2}\sqrt{\varepsilon^2 + 4} > -\frac{\varepsilon}{2} + \frac{1}{2}\sqrt{\varepsilon^2} = -\frac{\varepsilon}{2} + \frac{\varepsilon}{2} = 0.$$

Also sind alle Ruhelagen der Form $(0, (k+1)\pi)$ nach Satz 7.30 instabil.

Für gerades k unterscheiden wir die Fälle $\varepsilon < 2$ und $\varepsilon \geq 2$. Falls $\varepsilon < 2$ ist, so ist $\varepsilon^2 - 4$ negativ, d. h. $\sqrt{\varepsilon^2 - 4}$ ist rein imaginär. Es folgt

$$\operatorname{Re} \lambda_{2,\pm} = -\frac{\varepsilon}{2} < 0.$$

Ist andererseits $\varepsilon \geq 2$, so ist $\sqrt{\varepsilon^2 - 4}$ reell und es gilt

$$\operatorname{Re} \lambda_{2,\pm} = -\frac{\varepsilon}{2} \pm \frac{1}{2}\sqrt{\varepsilon^2 - 4} \leq -\frac{\varepsilon}{2} + \frac{1}{2}\sqrt{\varepsilon^2 - 4} < -\frac{\varepsilon}{2} + \frac{1}{2}\sqrt{\varepsilon^2} = -\frac{\varepsilon}{2} + \frac{\varepsilon}{2} = 0.$$

Also hat in beiden Fällen $(Df)(0, k\pi)$ für gerades k nur Eigenwerte mit negativem Realteil. Es handelt sich daher hierbei um asymptotisch stabile Ruhelagen.

Stabilitätsuntersuchung mittels Lyapunov-Funktionen

Unbefriedigend an Satz 7.30 ist, dass dieser keine Aussage mehr erlaubt, falls ein Eigenwert mit Realteil 0 auftritt. In solchen Fällen kann oft die *direkte Methode von Lyapunov* einen Ausweg bieten. Anstoß der Entwicklung dieser Methode war die Beobachtung Lyapunovs, dass physikalische Ruhelagen die Energie minimieren, woraufhin er nach einem Typ von Funktion suchte, der das Konzept der physikalischen Energie verallgemeinert.

Definition 7.31. Sei $n \in \mathbb{N}$, $D \subseteq \mathbb{R}^n$ offen und zusammenhängend, $f: D \rightarrow \mathbb{R}^n$ lokal Lipschitz-stetig und $\langle \cdot, \cdot \rangle$ das Standard-Skalar-Produkt auf \mathbb{R}^n . Eine stetig differenzierbare Funktion $V: D \rightarrow \mathbb{R}$ heißt *Lyapunov-Funktion* der Differentialgleichung $x' = f(x)$, falls

$$\langle \nabla V(x), f(x) \rangle \leq 0$$

für alle $x \in D$ erfüllt ist.

Eine Lyapunov-Funktion für eine vorgegebene Differentialgleichung $x' = f(x)$ zu finden, ist ein nicht-triviales Problem. Ist $f(x)$ skalar, d. h. $f: D \rightarrow \mathbb{R}$ eine stetige Funktion mit einem offenen Intervall $D \subseteq \mathbb{R}$, so ist dies jedoch recht entspannt möglich. Sei dazu $F(x)$ eine Stammfunktion von $f(x)$, dann gilt

$$-F'(x) \cdot f(x) = -[f(x)]^2 \leq 0$$

für alle $x \in D$. Folglich ist durch $V(x) = -F(x)$ eine Lyapunov-Funktion von $x' = f(x)$ gegeben.

Satz 7.32 (direkte Methode von Lyapunov). Sei $n \in \mathbb{N}$, $D \subseteq \mathbb{R}^n$ offen und zusammenhängend, $f: D \rightarrow \mathbb{R}^n$ lokal Lipschitz-stetig und $V: D \rightarrow \mathbb{R}$ eine Lyapunov-Funktion zu $x' = f(x)$. Sei weiter $\xi \in D$ mit $f(\xi) = 0$.

(1) Gilt $V(\xi) = 0$ und $V(x) > 0$ für alle $x \in D \setminus \{\xi\}$, so ist ξ eine stabile Ruhelage von $x' = f(x)$.

(2) Gilt $V(\xi) = 0$ und $V(x) > 0$ für alle $x \in D \setminus \{\xi\}$ sowie

$$\langle \nabla V(x), f(x) \rangle < 0 \quad \text{für alle } x \in D \setminus \{\xi\},$$

so ist ξ eine asymptotisch stabile Ruhelage von $x' = f(x)$.

(3) Gilt $V(\xi) = 0$ sowie

$$\langle \nabla V(x), f(x) \rangle < 0 \quad \text{für alle } x \in D \setminus \{\xi\}$$

und gibt es in jeder Umgebung U von ξ ein $u \in U$ mit $V(u) < 0$, so ist ξ eine instabile Ruhelage von $x' = f(x)$.

Aufgabe (Herbst 2011, T1A5)

Betrachten Sie die Differentialgleichung

$$\begin{aligned}\dot{x} &= -3x + y + 2y^3 \\ \dot{y} &= -4x\end{aligned}$$

und zeigen Sie die asymptotische Stabilität der Ruhelage $(x^*, y^*) = (0, 0)$ sowohl durch Untersuchung der Linearisierung in (x^*, y^*) als auch durch Verwendung der Lyapunov-Funktion

$$V(x, y) = 4x^2 - 2xy + y^2 + y^4.$$

Lösungsvorschlag zur Aufgabe (Herbst 2011, T1A5)

Sei $g : \mathbb{R}^2 \rightarrow \mathbb{R}^2, (x, y) \mapsto (-3x + y + 2y^3, -4x)$, dann ist

$$(Dg)(x, y) = \begin{pmatrix} -3 & 1+6y^2 \\ -4 & 0 \end{pmatrix}.$$

Wir bestimmen nun die Eigenwerte von $(Dg)(0, 0)$:

$$\chi = \det \begin{pmatrix} -3 - X & 1 \\ -4 & -X \end{pmatrix} = X(X + 3) + 4 = X^2 + 3X + 4$$

Die Nullstellen des charakteristischen Polynoms sind

$$\lambda_{\pm} = -\frac{3}{2} \pm \frac{1}{2}\sqrt{-7}.$$

Die Eigenwerte von $(Dg)(0, 0)$ haben also beide Realteil $-\frac{3}{2} < 0$. Aus Satz 7.30 folgt daher, dass $(0, 0)$ eine asymptotisch stabile Ruhelage ist.

Laut Aufgabenstellung ist durch $V(x, y) = 4x^2 - 2xy + y^2 + y^4$ eine Lyapunov-Funktion obiger Differentialgleichung gegeben. Wir überprüfen die Bedingungen aus Satz 7.32 (2). Es ist $V(0, 0) = 0$ und

$$\begin{aligned} V(x, y) &= 4x^2 - 2xy + y^2 + y^4 = 3x^2 + [x^2 - 2xy + y^2] + y^4 = \\ &= 3x^2 + (x - y)^2 + y^4 > 0 \end{aligned}$$

für alle $(x, y) \in \mathbb{R}^2 \setminus \{(0, 0)\}$, außerdem

$$\begin{aligned} \langle \nabla V(x, y), g(x) \rangle &= \langle (8x - 2y, -2x + 2y + 4y^3), (-3x + y + 2y^2, -4x) \rangle = \\ &= (8x - 2y)(-3x + y + 2y^2) + (-2x + 2y + 4y^3)(-4x) = \\ &= -4x \cdot \left[(-2x + 2y + 4y^3) - 2(-3x + y + 2y^2) \right] \\ &\quad - 2y(-3x + y + 2y^2) = \\ &= -4x \cdot 4x + 6xy - 2y^2 - 4y^4 = \\ &= -7x^2 - (9x^2 - 6xy + y^2) - y^2 - 4y^4 = \\ &= -7x^2 - (3x - y)^2 - y^2 - 4y^4 < 0 \end{aligned}$$

für alle $(x, y) \in \mathbb{R}^2 \setminus \{(0, 0)\}$. Daher zeigt auch die direkte Methode von Lyapunov, dass es sich bei $(0, 0)$ um eine asymptotisch stabile Ruhelage handelt.

Aufgabe (Frühjahr 2014, T1A1)

Zeigen Sie die asymptotische Stabilität der Ruhelage $(0,0)$ der in \mathbb{R}^2 gegebenen Differentialgleichung

$$\dot{x} = -x^3 + y^5, \dot{y} = -xy^4 - y^3.$$

Führt Linearisierung zum Ziel?

Lösungsvorschlag zur Aufgabe (Frühjahr 2014, T1A1)

Sei $g : \mathbb{R}^2 \rightarrow \mathbb{R}^2$, $(x, y) \mapsto (-x^3 + y^5, -xy^4 - y^3)$, dann berechnet sich die Jacobi-Matrix zu

$$(Dg)(x, y) = \begin{pmatrix} -3x^2 & 5y^4 \\ -y^4 & -4xy^3 - 3y^2 \end{pmatrix}$$

und es ist $(Dg)(0,0)$ die Nullmatrix. Da die Nullmatrix den doppelten Eigenwert 0 hat, kann aus Satz 7.30 keine Aussage über die Stabilität der Ruhelage $(0,0)$ gewonnen werden. Wir versuchen daher stattdessen unser Glück mit der direkten Methode von Lyapunov. Dazu bemerken wir zunächst, dass

$$x(-x^3 + y^5) + y(-xy^4 - y^3) = -x^4 + xy^5 - xy^5 - y^4 = -x^4 - y^4 \leq 0$$

für alle $(x, y) \in \mathbb{R}^2$ gilt. Also ist durch

$$V : \mathbb{R}^2 \rightarrow \mathbb{R}, (x, y) \mapsto \frac{1}{2}x^2 + \frac{1}{2}y^2$$

eine Lyapunov-Funktion unserer Differentialgleichung gegeben, denn es ist

$$\begin{aligned} \langle \nabla V(x, y), g(x, y) \rangle &= \\ &= \langle \left(\partial_x (\frac{1}{2}x^2 + \frac{1}{2}y^2), \partial_y (\frac{1}{2}x^2 + \frac{1}{2}y^2) \right), (-x^3 + y^5, -xy^4 - y^3) \rangle \\ &= \langle (x, y), (-x^3 + y^5, -xy^4 - y^3) \rangle \\ &= x(-x^3 + y^5) + y(-xy^4 - y^3) \\ &= -x^4 - y^4 \\ &\leq 0 \end{aligned}$$

für alle $(x, y) \in \mathbb{R}^2$. Im Falle $(x, y) \neq (0,0)$ gilt die Ungleichung sogar strikt. Weiter ist $V(0,0) = 0$ und $V(x, y) = \frac{1}{2}x^2 + \frac{1}{2}y^2 > 0$ für alle $(x, y) \in \mathbb{R}^2 \setminus \{(0,0)\}$, sodass $(0,0)$ nach Satz 7.32 (2) eine asymptotisch stabile Ruhelage ist.

Anleitung: Zusammenfassung zur Stabilitätsuntersuchung

Es seien an dieser Stelle noch einmal die verschiedenen Methoden der Stabilitätsuntersuchung aufgelistet:

- (1) Für Differentialgleichungen der Form $x' = A(t)x + g(t)$ mit einer zeitabhängigen Matrix A und einer stetigen Abbildung g liefert Satz 7.28 eine äquivalente Charakterisierung der Stabilität aller Lösungen anhand der Übergangsmatrix.
- (2) Für eine zeitunabhängige Matrix A lässt sich die Stabilität aller Lösungen von $x' = Ax + g(t)$ nach Satz 7.29 vollständig anhand der Eigenwerte von A klassifizieren.
- (3) Die Stabilitätseigenschaften einer *Ruhelage* ξ von $x' = g(x)$ lassen sich oft mittels Linearisierung (Satz 7.30) bestimmen, indem man die Eigenwerte von $(Dg)(\xi)$ bestimmt. Allerdings liefert diese Methode keine Aussage, falls es einen Eigenwert mit Realteil 0 gibt.
- (4) Ist man in der Lage, eine Lyapunov-Funktion zu $x' = g(x)$ zu bestimmen, so kann man sein Glück mit der Direkten Methode von Lyapunov (Satz 7.32) versuchen.

Teil II

Prüfungsaufgaben

8. Algebra: Aufgabenlösungen nach Jahrgängen

Prüfungstermin: Frühjahr 2015

Thema Nr. 1 (Aufgabengruppe)

Aufgabe 1 → S. 247

Sei \mathbb{F}_2 der endliche Körper mit genau zwei Elementen 0 und 1. Auf dem dreidimensionalen \mathbb{F}_2 -Vektorraum $(\mathbb{F}_2)^3$ betrachten wir den Endomorphismus

$$\phi: (\mathbb{F}_2)^3 \rightarrow (\mathbb{F}_2)^3, \quad (x_1, x_2, x_3) \mapsto (x_3, x_2, x_1).$$

- a** Bestimmen Sie das charakteristische Polynom von ϕ . Bestimmen Sie alle Eigenwerte von ϕ in \mathbb{F}_2 . Bestimmen Sie für jeden Eigenwert von ϕ in \mathbb{F}_2 eine Basis des zugehörigen Eigenraums. (8 Punkte)
- b** Gibt es eine Basis von $(\mathbb{F}_2)^3$, bezüglich derer ϕ eine Jordan'sche Normalform hat? Begründen Sie Ihre Antwort. Wenn ja, bestimmen Sie die Jordan'sche Normalform von ϕ . (8 Punkte)

Aufgabe 2 → S. 98

Sei $m \geq 3$ eine ungerade ganze Zahl. Zeigen Sie die folgende Kongruenz:

$$1^m + 2^m + 3^m + \cdots + (m-3)^m + (m-2)^m + (m-1)^m \equiv 0 \pmod{m}$$

(4 Punkte)

Aufgabe 3 → S. 60

Sei G eine Gruppe der Ordnung 105. Zeigen Sie:

- a** G hat einen Normalteiler N mit $|N| = 5$ oder $|N| = 7$. (6 Punkte)
- b** G ist auflösbar. (6 Punkte)

Aufgabe 4 → S. 104

Sei J das von $X^3 - 7$ erzeugte Ideal in $\mathbb{Q}[X]$.

- a** Beweisen Sie, dass $\mathbb{Q}[X]/J$ ein Körper ist, und bestimmen Sie den Grad der Körpererweiterung $\mathbb{Q}[X]/J \supseteq \mathbb{Q}$. (6 Punkte)
- b** Bestimmen Sie ein Polynom $P \in \mathbb{Q}[X]$, für das $P + J$ multiplikatives Inverses von $(X^2 + 1) + J$ in $\mathbb{Q}[X]/J$ ist. (6 Punkte)

Aufgabe 5 → S. 179

Sei $f \in \mathbb{Q}[X]$ ein irreduzibles Polynom vom Grad $n \geq 1$. Sei K ein Zerfällungskörper von f . Sei $G = \text{Gal}(K/\mathbb{Q})$ die zugehörige Galois-Gruppe.

- a** Beweisen Sie: Falls G eine abelsche Gruppe ist, hat sie die Ordnung n . (8 Punkte)
- b** Sei $K = \mathbb{Q}(\sqrt{2}, i)$, wobei $i \in \mathbb{C}$ die imaginäre Einheit mit $i^2 = -1$ ist. Bestimmen Sie ein irreduzibles Polynom $f \in \mathbb{Q}[X]$, dessen Zerfällungskörper K ist. Beweisen Sie, dass $G = \text{Gal}(K/\mathbb{Q})$ abelsch, aber nicht zyklisch ist. (8 Punkte)

Thema Nr. 2
(Aufgabengruppe)

Aufgabe 1 → S. 100

Man bestimme alle Paare von Primzahlen p, q mit $p^2 - 2q^2 = 1$. (10 Punkte)

Aufgabe 2 → S. 496

Es sei $f(X) \in K[X]$ ein nicht konstantes Polynom ohne mehrfache Nullstellen in einem Zerfällungskörper. Man zeige, dass $f(X)$ ein Teiler des Polynoms $f(X + f(X))$ ist. (10 Punkte)

Aufgabe 3 → S. 145

Sei p eine Primzahl und $a \in \mathbb{Z}$ keine p -te Potenz in \mathbb{Z} . Man zeige, dass das Polynom $X^p - a$ über \mathbb{Q} irreduzibel ist.

Hinweis Betrachte die Nullstellen von $X^p - a$ in \mathbb{C} und untersuche den konstanten Term eines echten Teilers von $X^p - a$ auf Ganzzahligkeit. (12 Punkte)

Aufgabe 4 → S. 25

- a** Die Gruppe G operiere transitiv auf einer Menge Ω mit $|\Omega| > 1$. Man zeige: Hat jedes Element aus G mindestens einen Fixpunkt, dann ist G eine Vereinigung der Konjugierten hUh^{-1} , $h \in G$ mit einer echten Untergruppe U von G .
(8 Punkte)

- b** Für $n > 1$ sei $G = \mathrm{GL}_n(\mathbb{C})$ die Gruppe der invertierbaren $n \times n$ -Matrizen über den komplexen Zahlen. Man gebe eine echte Untergruppe U von G an, so dass G die Vereinigung der Konjugierten von U ist.

Hinweis Betrachte die Operation auf den 1-dimensionalen Unterräumen von \mathbb{C}^n .

(10 Punkte)

Aufgabe 5 → S. 208

Sei p eine Primzahl und $q = p^n, n > 0$. Weiter sei K ein Körper der Charakteristik p . Zeigen Sie, dass die Nullstellen des Polynoms $f(X) = X^q - X$ einen Unterkörper von K bilden.
(10 Punkte)

Thema Nr. 3

(Aufgabengruppe)

Aufgabe 1 → S. 3

Gegeben seien eine Gruppe G und drei Untergruppen $U_1, U_2, V \subseteq G$ mit der Eigenschaft $V \subseteq U_1 \cup U_2$. Zeigen Sie, dass $V \subseteq U_1$ oder $V \subseteq U_2$ gilt. (8 Punkte)

Aufgabe 2 → S. 61

Seien p, q, r Primzahlen mit $p < q < r$ und $pq < r + 1$. Zeigen Sie, dass jede Gruppe der Ordnung pqr auflösbar ist.
(12 Punkte)

Aufgabe 3 → S. 76

Ein Ring R mit Eins heißt *idempotent*, wenn $a \cdot a = a$ für alle $a \in R$ gilt. Beweisen Sie:

- a** $-1 = 1$ in R .
(4 Punkte)
- b** Jeder idempotente Ring ist kommutativ.
(4 Punkte)
- c** Jeder idempotente Integritätsbereich ist isomorph zu \mathbb{F}_2 , dem Körper mit zwei Elementen.
(4 Punkte)

Aufgabe 4 → S. 152

Im Folgenden ist jeweils L/K eine Körpererweiterung und ein Element $\alpha \in L$ gegeben. Bestimmen Sie jeweils das Minimalpolynom von α über dem Grundkörper K (mit Nachweis!).

- a** $K = \mathbb{Q}, L = \mathbb{C}$ und $\alpha = \sqrt{2} + \sqrt{3}$. (4 Punkte)
- b** $K = \mathbb{F}_3, L = \overline{\mathbb{F}_3}$ ein algebraischer Abschluss von \mathbb{F}_3 und α eine Nullstelle von $X^6 + 1$. (6 Punkte)
- c** $K = \mathbb{Q}(\zeta + \zeta^{-1}), L = \mathbb{Q}(\zeta)$ und $\alpha = \zeta \in \mathbb{C}$ eine p -te Einheitswurzel. wobei $p \geq 3$ eine Primzahl bezeichne. (6 Punkte)

Aufgabe 5 → S. 196

Es sei eine Galoiserweiterung E/K mit zyklischer Galois-Gruppe gegeben, so dass $[E : K] = p^n$ gilt mit einer Primzahl p und $n \geq 1$. Weiter sei $K \subset F \subset E$ ein Zwischenkörper mit $[F : K] = p^{n-1}$. Zeigen Sie: Jedes Element von $E \setminus F$ ist ein primitives Element von E über K . (12 Punkte)

Lösungen zu Thema Nr. 1

Alle Lösungen aus diesem Thema wurden bereits in früheren Kapiteln dieses Buches behandelt.

Lösungen zu Thema Nr. 2

Lösungsvorschlag zur Aufgabe (Frühjahr 2015, T2A2)

Zu zeigen ist $f(X + f) \equiv 0 \pmod{f}$. Sei dazu $f = \sum_{k=0}^n a_k X^k$ mit $n \in \mathbb{N}$ und $a_k \in K$, dann ist wegen $X + f \equiv X \pmod{f}$ auch

$$f(X + f) = \sum_{k=0}^n a_k (X + f)^k \equiv \sum_{k=0}^n a_k X^k \equiv f \equiv 0 \pmod{f}.$$

Lösungen zu Thema Nr. 3

Alle Lösungen aus diesem Thema wurden bereits in früheren Kapiteln dieses Buches behandelt.

Prüfungstermin: Herbst 2015

Thema Nr. 1 (Aufgabengruppe)

Aufgabe 1 → S. 102

Bestimmen Sie sämtliche Lösungen der Gleichung $x^6 - 2x + 4 = 0$ im Ring $\mathbb{Z}/64\mathbb{Z}$.
Hinweis Führen Sie eine Fallunterscheidung je nach Bild von x in $\mathbb{Z}/2\mathbb{Z}$ durch und beachten Sie, dass $64 = 2^6$. (8 Punkte)

Aufgabe 2 → S. 226

Sei \mathbb{F}_q der endliche Körper mit q Elementen.

- a Zeigen Sie, dass für $n \geq 1$ die Anzahl der eindimensionalen \mathbb{F}_q -Untervektorräume von \mathbb{F}_q^n gleich $\frac{q^n - 1}{q - 1}$ ist. (4 Punkte)
- b Zeigen Sie, dass die Anzahl der zweidimensionalen Untervektorräume von \mathbb{F}_q^3 gleich der Anzahl der eindimensionalen Untervektorräume von \mathbb{F}_q^3 ist. (4 Punkte)
- c Wie viele Zerlegungen von \mathbb{F}_q^3 in direkte Summen von \mathbb{F}_q -Untervektorräumen $V_1 \oplus V_2$ gibt es mit $\dim_{\mathbb{F}_q}(V_1) = 2$? (4 Punkte)

Aufgabe 3 → S. 47

Bestimmen Sie bis auf Isomorphie sämtliche endliche Gruppen G der Ordnung $143 = 11 \cdot 13$. (8 Punkte)

Aufgabe 4 → S. 501

Sei $P(X)$ das Polynom $X^3 - X + 2 \in \mathbb{Z}[X]$. Zeigen Sie die folgenden Behauptungen:

- a Das Bild von $P(X)$ in $\mathbb{F}_3[X]$ ist irreduzibel. (2 Punkte)
- b Das Polynom $P(X)$ ist irreduzibel in $\mathbb{Q}[X]$. (2 Punkte)
- c Das Polynom $P(X)$ hat genau eine reelle Nullstelle. (4 Punkte)
- d Die Galois-Gruppe des Zerfällungskörpers L von $P(X)$ über \mathbb{Q} ist isomorph zu S_3 . (4 Punkte)

Aufgabe 5 → S. 502

Sei $\zeta_5 \in \mathbb{C}$ eine primitive fünfte Einheitswurzel, $\zeta_7 \in \mathbb{C}$ eine primitive siebte Einheitswurzel und $u = \zeta_7 + \zeta_7^{-1}$. Zeigen Sie:

- a** $[\mathbb{Q}(\zeta_7) : \mathbb{Q}(u)] = 2$, (4 Punkte)
 - b** $[\mathbb{Q}(u) : \mathbb{Q}] = 3$, (4 Punkte)
 - c** $[\mathbb{Q}(u, \zeta_5) : \mathbb{Q}] = 12$. (6 Punkte)
 - d** Die Galois-Gruppe $\text{Gal}(\mathbb{Q}(u, \zeta_5)/\mathbb{Q})$ ist isomorph zu $\mathbb{Z}/12\mathbb{Z}$. (6 Punkte)
-

Thema Nr. 2
(Aufgabengruppe)

Aufgabe 1 → S. 503

Bestimmen Sie alle Matrizen A in $\text{GL}_2(\mathbb{C})$, die mit der Matrix

$$X = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

kommutieren. (6 Punkte)

Aufgabe 2 → S. 64

Wieviele Elemente der Ordnung 15 gibt es in der symmetrischen Gruppe S_8 ?

(14 Punkte)

Aufgabe 3 → S. 504

Sei $(a_n)_{n \geq 0}$ die wie folgt rekursiv definierte Folge ganzer Zahlen

$$a_0 = 0, \quad a_{n+1} = a_n^2 + 1 \text{ für } n \geq 0.$$

Sei $N \in \mathbb{Z}$. Zeigen Sie: Ist N ein Teiler von a_n , dann teilt N auch a_{kn} für alle $k \geq 2$.

(14 Punkte)

Aufgabe 4 → S. 152

Sei $K \subset L$ eine Körpererweiterung und seien $\alpha, \beta \in L$ algebraisch über K . Sei f das Minimalpolynom von α über K und g das Minimalpolynom von β über K . Zeigen Sie, dass f irreduzibel über $K(\beta)$ ist genau dann, wenn g irreduzibel über $K(\alpha)$ ist. (12 Punkte)

Aufgabe 5 → S. 181

Sei $\xi = \sqrt{2 + \sqrt{2}} \in \mathbb{R}$.

- a** Berechnen Sie das Minimalpolynom $m(X)$ von ξ über \mathbb{Q} . (6 Punkte)
- b** Zeigen Sie, dass die Körpererweiterung $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2 + \sqrt{2}})$ Galois'sch ist und berechnen Sie die Galois-Gruppe. (8 Punkte)
-

Thema Nr. 3

(Aufgabengruppe)

Aufgabe 1 → S. 101

Seien $x, y, z \in \mathbb{Z}$ mit $x^2 + y^2 = z^2$. Zeigen Sie, dass das Produkt xyz durch 60 teilbar ist. (12 Punkte)

Aufgabe 2 → S. 504

Sei $n \geq 2$ eine natürliche Zahl. Es bezeichne $\varphi(n)$ den Wert der Euler'schen φ -Funktion bei n . Zeigen Sie, dass es genau $\varphi(n)$ verschiedene injektive Gruppenhomomorphismen $f: \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Q}/\mathbb{Z}$ gibt. (15 Punkte)

Aufgabe 3 → S. 239

Betrachten Sie das Polynom $f(X) = X^2 + X + 1 \in \mathbb{F}_5[X]$.

- a** Zeigen Sie, dass $K = \mathbb{F}_5[X]/(f(X))$ ein Körper mit 25 Elementen ist. (4 Punkte)
- b** Bestimmen Sie ein Element $w \in K$, mit $w^2 = 2$. (6 Punkte)
- c** Zeigen Sie, dass die Matrix

$$A := \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \in M(2 \times 2, \mathbb{F}_5)$$

über K diagonalisierbar ist. (5 Punkte)

Aufgabe 4 → S. 203

Es sei $p \geq 3$ eine Primzahl und $a \in \mathbb{Q}$ eine rationale Zahl, so dass $X^p - a$ irreduzibel über \mathbb{Q} ist. Ferner sei $\xi \in \mathbb{C}$ eine primitive p -te Einheitswurzel, $\alpha \in \mathbb{C}$ eine beliebige Nullstelle von $X^p - a$ und $Z := \mathbb{Q}(\alpha, \xi)$.

- a** Zeigen Sie, dass Z ein Zerfällungskörper von $X^p - a$ ist und $[Z : \mathbb{Q}] = p(p-1)$ gilt. (5 Punkte)

- b** Zeigen Sie, dass $\text{Gal}(Z|\mathbb{Q})$ eine p -Sylowgruppe H besitzt, die ein Normalteiler ist, und dass

$$\text{Gal}(Z|\mathbb{Q})/H \simeq (\mathbb{Z}/p\mathbb{Z})^\times = \mathbb{Z}/p\mathbb{Z} \setminus \{0\}$$

gilt. (5 Punkte)

- c** Bestimmen Sie einen Gruppenisomorphismus $\text{Gal}(Z|\mathbb{Q}(\alpha)) \xrightarrow{\sim} (\mathbb{Z}/p\mathbb{Z})^\times$. (5 Punkte)

- d** Zeigen Sie, dass $\text{Gal}(Z|\mathbb{Q})$ mehr als eine 2-Sylowgruppe besitzt. (3 Punkte)

Lösungen zu Thema Nr. 1

Lösungsvorschlag zur Aufgabe (Herbst 2015, T1A4)

- a** Wegen $\text{grad } P(X) = 3$ genügt es zu zeigen, dass $P(X)$ keine Nullstellen in \mathbb{F}_3 hat. Dazu berechnen wir

$$P(\bar{0}) = \bar{2}, \quad P(\bar{1}) = \bar{1} - \bar{1} + \bar{2} = \bar{2}, \quad P(\bar{2}) = -\bar{1} + \bar{1} + \bar{2} = \bar{2}.$$

- b** Das folgt direkt aus dem Reduktionskriterium 2.26.

- c** Es gilt

$$P(-1) = 2 > 0, \quad P(-2) = -8 + 2 + 2 = -4 < 0.$$

Damit hat P aufgefasst als Polynomfunktion $p: \mathbb{R} \rightarrow \mathbb{R}$, $x \mapsto P(x)$ laut dem Zwischenwertsatz eine Nullstelle im Intervall $]-2, -1[$. Um auszuschließen, dass es weitere Nullstellen gibt, betrachten wir die erste Ableitung $p'(x) = 3x^2 - 1$. Für diese gilt

$$p'(x) = 0 \Leftrightarrow x = \pm c \quad \text{für } c = \sqrt{\frac{1}{3}}.$$

Damit ist p für $x < -c$ streng monoton steigend, sodass in diesem Bereich nur eine Nullstelle (die oben gefundene) vorkommen kann. Im Bereich $-c < x < c$ ist p wegen $p'(x) < 0$ streng monoton fallend. Jedoch erhalten wir hier wegen $p(-c) > 0$ keine weitere Nullstelle. Für $x > c$ ist p wiederum monoton steigend, sodass sich auch hier keine Nullstelle ergibt. Insbesondere hat P keine weitere reelle Nullstelle.

- d** Gemäß Satz 3.24 ist $\text{Gal}(f) = G_{L|\mathbb{Q}}$ zumindest isomorph zu einer Untergruppe von S_3 . Wir zeigen, dass $|\text{Gal}(f)| = [L : \mathbb{Q}] > 3$ ist, wobei L ein Zerfällungskörper von f ist. Sei α die reelle Nullstelle aus Teil **c**. Dann ist $\mathbb{Q}(\alpha)$ ein Zwischenkörper von $L|\mathbb{Q}$ mit Erweiterungsgrad 3. Nehmen wir nun an, $L = \mathbb{Q}(\alpha)$. Dann wäre $L \subseteq \mathbb{R}$, im Widerspruch dazu, dass laut Teil **c** zwei der Nullstellen nicht-reell sind. Damit ist $\text{Gal}(f)$ isomorph zu einer Untergruppe von S_3 , deren Ordnung größer als 3 ist. Dies ist nur für $\text{Gal}(f) \cong S_3$ möglich.

Lösungsvorschlag zur Aufgabe (Herbst 2015, T1A5)

- a** Wegen $\zeta_7 = e^{\frac{2\pi i k}{7}}$ für ein $k \in \{1, \dots, 6\}$ ist

$$u = \zeta_7 + \zeta_7^{-1} = 2 \cos\left(\frac{2\pi k}{7}\right)$$

und somit $\mathbb{Q}(u) \subseteq \mathbb{R}$. Insbesondere folgt wegen $\zeta_7 \notin \mathbb{R}$ auch $[\mathbb{Q}(\zeta_7) : \mathbb{Q}] > 1$. Betrachten wir nun

$$f = (X - \zeta_7)(X - \zeta_7^{-1}) = X^2 - (\zeta_7 + \zeta_7^{-1})X - 1 = X^2 - uX - 1 \in \mathbb{Q}(u)[X],$$

so stellen wir fest, dass f ein Polynom mit $f(\zeta_7) = 0$ ist, und somit $[\mathbb{Q}(\zeta_7) : \mathbb{Q}(u)] \leq 2$. Insgesamt folgt aus beiden Ungleichungen die Behauptung.

- b** Nach Definition ist das Minimalpolynom von ζ_7 das siebte Kreisteilungspolynom Φ_7 ist. Es gilt daher laut Satz 3.17, dass

$$[\mathbb{Q}(\zeta_7) : \mathbb{Q}] = \text{grad } \Phi_7 = \varphi(7) = 6.$$

Mit der Gradformel und Teil **a** folgt nun

$$[\mathbb{Q}(u) : \mathbb{Q}] = \frac{[\mathbb{Q}(\zeta_7) : \mathbb{Q}]}{[\mathbb{Q}(\zeta_7) : \mathbb{Q}(u)]} = \frac{6}{2} = 3.$$

- c** Der Körper $\mathbb{Q}(u)$ ist laut Teil **b** ein Zwischenkörper der Erweiterung von Grad 3 über \mathbb{Q} . Der Körper $\mathbb{Q}(\zeta_5)$ ist ein Zwischenkörper, für dessen Grad

$$[\mathbb{Q}(\zeta_5) : \mathbb{Q}] = \text{grad } \Phi_5 = \varphi(5) = 4$$

gilt. Insgesamt wird laut der Gradformel also der Erweiterungsgrad sowohl von 4 als auch von 3 geteilt und ist somit ein Vielfaches von $\text{kGV}(3, 4) = 12$. Zugleich ist aber Φ_5 ein Polynom in $\mathbb{Q}(u)[X]$ mit $\Phi_5(\zeta_5) = 0$. Das Minimalpolynom von ζ_5 über diesem Körper muss also ein Teiler von Φ_5 sein und insbesondere vom Grad ≤ 4 sein. Damit gilt auch

$$[\mathbb{Q}(u, \zeta_5) : \mathbb{Q}] = [\mathbb{Q}(u, \zeta_5) : \mathbb{Q}(u)] \cdot [\mathbb{Q}(u) : \mathbb{Q}] \leq 4 \cdot 3 = 12.$$

Beide Abschätzungen zusammen ergeben die gewünschte Gleichheit.

- d** Nach Satz 3.18 ist $\mathbb{Q}(\zeta_7)|\mathbb{Q}$ eine Galois-Erweiterung mit zyklischer Galois-Gruppe. Insbesondere ist jede Untergruppe ein Normalteiler, sodass jede Zwischenerweiterung nach dem Hauptsatz der Galois-Theorie 3.20 daher jede Zwischenerweiterung galoissch ist. Folglich ist auch $\mathbb{Q}(u) |\mathbb{Q}$ eine

Galois-Erweiterung. Da $|G_{\mathbb{Q}(u)|\mathbb{Q}}| = [\mathbb{Q}(u) : \mathbb{Q}] = 3$ eine Primzahl ist, ist außerdem $G_{\mathbb{Q}(u)|\mathbb{Q}} \cong \mathbb{Z}/3\mathbb{Z}$.

Aus Satz 3.18 folgt genauso, dass $\mathbb{Q}(\zeta_5) \mid \mathbb{Q}$ eine Galois-Erweiterung mit Galois-Gruppe $G_{\mathbb{Q}(\zeta_5)|\mathbb{Q}} \cong \mathbb{Z}/4\mathbb{Z}$ ist. Nach Satz 3.23 ist daher auch $\mathbb{Q}(u, \zeta_5) \mid \mathbb{Q}$ galoissch und es gibt einen injektiven Homomorphismus

$$G_{\mathbb{Q}(u, \zeta_5)|\mathbb{Q}} \hookrightarrow G_{\mathbb{Q}(u)|\mathbb{Q}} \times G_{\mathbb{Q}(\zeta_5)|\mathbb{Q}} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \cong \mathbb{Z}/12\mathbb{Z}.$$

Unter Verwendung von Teil **b** ist $|G_{\mathbb{Q}(u, \zeta_5)|\mathbb{Q}}| = 12$, sodass dieser Homomorphismus bereits ein Isomorphismus sein muss.

Lösungen zu Thema Nr. 2

Lösungsvorschlag zur Aufgabe (Herbst 2015, T2A1)

Wir machen den Ansatz

$$\begin{aligned} AX = XA &\Leftrightarrow \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \Leftrightarrow \\ &\begin{pmatrix} a & a+b \\ c & c+d \end{pmatrix} = \begin{pmatrix} a+c & b+d \\ c & d \end{pmatrix} \end{aligned}$$

und erhalten daraus die Gleichungen

$$a = a + c, \quad a + b = b + d, \quad c = c, \quad c + d = d.$$

Die erste (und die letzte) Gleichung ist äquivalent zu $c = 0$, die zweite Gleichung zu $a = d$. Die Menge, der Matrizen, die mit X kommutieren, ist daher durch

$$\left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \mid a \in \mathbb{C}^\times, b \in \mathbb{C} \right\} \subseteq \mathrm{GL}_2(\mathbb{C})$$

gegeben.

Lösungsvorschlag zur Aufgabe (Herbst 2015, T2A3)

Nach Berechnung der ersten paar Werte stellt man folgende Behauptung für $n \in \mathbb{N}$ und $l \geq 0$ auf:

$$a_{n+l} \equiv a_l \pmod{N}.$$

Im Fall $l = 0$ ist die Aussage natürlich klar. Für den Induktionsschritt setzen wir die Aussagen für $l \geq 0$ voraus und erhalten

$$a_{n+(l+1)} \equiv a_{n+l}^2 + 1 \stackrel{(I.V.)}{\equiv} a_l^2 + 1 \equiv a_{l+1} \pmod{N}.$$

Daraus erhalten wir für beliebiges $k \geq 2$, dass $a_{kn} \equiv a_n \pmod{N}$ – wie man zur Not durch eine weitere Induktion zeigt. Insgesamt folgt für $k \geq 2$

$$a_{kn} \equiv a_n \equiv 0 \pmod{N}$$

und damit ist N ein Teiler von a_{kn} .

Lösungen zu Thema Nr. 3

Lösungsvorschlag zur Aufgabe (Herbst 2015, T3A2)

Ein Homomorphismus $f: \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Q}/\mathbb{Z}$ ist durch das Bild von $\bar{1}$ bereits eindeutig bestimmt. Laut Proposition 1.24 existiert für jedes Element $q + \mathbb{Z}$ mit $\text{ord}(q + \mathbb{Z}) \mid n$ ein solcher Homomorphismus.

Wir zeigen nun zunächst, dass ein solcher Homomorphismus genau dann injektiv ist, wenn das Element $q + \mathbb{Z} = f(\bar{1})$ die Ordnung n hat.

„ \Rightarrow “: Da f ein Homomorphismus ist, muss die Ordnung von $q + \mathbb{Z}$ auf jeden Fall $\text{ord } \bar{1} = n$ teilen. Nehmen wir an, es gibt einen Teiler $k < n$, so dass $k \cdot f(\bar{1}) = 0$. Dann wäre jedoch $f(\bar{k}) = k \cdot f(\bar{1}) = 0$ und damit $\bar{k} \in \ker f$, aber $\bar{k} \neq \bar{0}$, im Widerspruch dazu, dass f injektiv ist.

„ \Leftarrow “: Angenommen, $q + \mathbb{Z}$ hat die Ordnung n . Dann gilt:

$$f(\bar{b}) = 0 \Leftrightarrow b f(\bar{1}) = 0 \Leftrightarrow b(q + \mathbb{Z}) = 0 \Leftrightarrow b \mid n \Leftrightarrow \bar{b} = 0.$$

Es genügt also, zu zeigen, dass es in \mathbb{Q}/\mathbb{Z} genau $\varphi(n)$ Elemente der Ordnung n gibt. Wir zeigen dazu, dass genau die Elemente der Form $\frac{a}{n} + \mathbb{Z}$ mit $\text{ggT}(a, n) = 1$ Ordnung n haben.

„ \Rightarrow “: Sei $\frac{a}{n} + \mathbb{Z} \in \mathbb{Q}/\mathbb{Z}$. Dann ist zunächst $n\frac{a}{n} = a \in \mathbb{Z}$, also ist $\text{ord } \frac{a}{n} + \mathbb{Z}$ ein Teiler von n . Sei k ein echter Teiler von n , dann ist $n = k \cdot n'$ für $n' \neq \pm 1$ und somit

$$k\frac{a}{n} = k\frac{a}{kn'} = \frac{a}{n'} \notin \mathbb{Z},$$

denn wegen $\text{ggT}(a, n) = 1$ ist n' kein Teiler von a .

„ \Leftarrow “: Sei $\frac{r}{s} + \mathbb{Z}$ ein Element der Ordnung n , wobei wir o. B. d. A. annehmen, dass der Bruch $\frac{r}{s}$ vollständig gekürzt ist. Es ist dann $n \cdot \frac{r}{s} \in \mathbb{Z}$, also $n = sk$ für ein $k \in \mathbb{Z}$. Damit haben wir $\frac{r}{s} = \frac{kr}{n}$. Nehmen wir nun an, es gibt einen echten gemeinsamen Teiler $d \neq \pm 1$ von kr und n . Dann kürzen wir den Bruch mit dieser Zahl und erhalten $\frac{n}{d} \cdot \frac{kr}{n} \in \mathbb{Z}$, im Widerspruch zu Ordnung $\text{ord}(\frac{r}{s} + \mathbb{Z}) = n$.

Insgesamt haben wir damit die $\varphi(n)$ Elemente der Form $\frac{a}{n} + \mathbb{Z}$ mit $\text{ggT}(a, n) = 1$ und laut dem ersten Teil gibt es genau so viele injektive Homomorphismen f .

Prüfungstermin: Frühjahr 2016

Thema Nr. 1 (Aufgabengruppe)

Aufgabe 1 → S. 511

Es sei f ein Endomorphismus des Euklidischen Vektorraums \mathbb{R}^n , und es sei M die Matrix von f bezüglich der kanonischen Basis von \mathbb{R}^n . Zeigen Sie, dass die folgenden Aussagen zueinander äquivalent sind:

- a** f ist eine Orthogonalprojektion auf einen Unterraum der Dimension k .
- b** Die Matrix M ist idempotent (d. h. $M^2 = M$), symmetrisch und hat Spur k .

(12 Punkte)

Aufgabe 2 → S. 513

Es sei $n \geq 1$ eine natürliche Zahl. Zeigen Sie, dass $\sum_{k=1}^n k^2$ genau dann durch n teilbar ist, wenn n weder durch 2 noch durch 3 teilbar ist.

Hinweis $\sum_{k=1}^n k^2 = \frac{1}{6} \cdot n \cdot (n+1) \cdot (2n+1)$. (8 Punkte)

Aufgabe 3 → S. 513

Es sei $(A, +)$ eine abelsche Gruppe, und es sei (H, \cdot) eine Gruppe mit einem Normalteiler $N \trianglelefteq H$ vom Index 2. Zeigen Sie:

- a** Sind $x, y \in H \setminus N$, dann ist $xy \in N$.
- b** Die auf $A \times H$ definierte Verknüpfung

$$(a, x) \circledast (b, y) := \begin{cases} (a+b, xy), & \text{falls } x \in N, \\ (a-b, xy), & \text{falls } x \in H \setminus N, \end{cases}$$

ist assoziativ.

Im Folgenden darf ohne Beweis verwendet werden, dass $A \times H$ mit dieser Verknüpfung eine Gruppe mit neutralem Element $(0_A, 1_H)$ bildet.

- c** Ist $x \in H \setminus N$ ein Element der Ordnung 2, und ist $a \in A$, dann hat (a, x) in der Gruppe $(A \times H, \circledast)$ die Ordnung 2.
- d** Es gibt eine Gruppe der Ordnung 42, die weder ein Element der Ordnung 6 noch ein Element der Ordnung 14 enthält. (16 Punkte)

Aufgabe 4 → S. 514

Es seien $1 < D \in \mathbb{Z}$ und $R = \mathbb{Z}[\sqrt{-D}]$.

- a** Zeigen Sie: Die Einheitengruppe von R ist $R^* = \{\pm 1\}$.

Ferner sei $D := 13$.

- b** Zeigen Sie, dass 2 und $1 + \sqrt{-13}$ in R irreduzibel sind.

- c** Zeigen Sie, dass $2 \in R$ kein Primelement ist.

Hinweis Man benutze die Normabbildung $N(a + b\sqrt{-D}) = a^2 + Db^2$.

(12 Punkte)

Aufgabe 5 → S. 515

Für eine primitive Einheitswurzel in \mathbb{C} gilt die Formel

$$\zeta_5 := e^{\frac{2\pi i}{5}} = \frac{\sqrt{5}-1}{4} + i\sqrt{\frac{\sqrt{5}+5}{8}};$$

diese Formel kann im Folgenden ohne Beweis verwendet werden.

- a** Bestimmen Sie das Minimalpolynom von $\alpha := \sqrt{\frac{\sqrt{5}+5}{8}}$ über \mathbb{Q} .

- b** Zeigen Sie: $i \notin \mathbb{Q}(\zeta_5)$.

(12 Punkte)

Thema Nr. 2
(Aufgabengruppe)

Aufgabe 1 → S. 516

- a** Sei p eine Primzahl und \mathbb{F}_p der Körper mit p Elementen. Die Menge

$$G = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mid a, b \in \mathbb{F}_p, a \neq 0 \right\}$$

ist eine Untergruppe der $\mathrm{GL}_2(\mathbb{F}_p)$ (Nachweis nicht erforderlich). Zeigen Sie, dass G auflösbar ist.

- b** Sei nun G eine beliebige Gruppe der Ordnung $p(p-1)$. Zeigen Sie, dass es genau eine Untergruppe H von G der Ordnung p gibt. Zeigen Sie weiter, dass G genau dann auflösbar ist, wenn G/H auflösbar ist.

- c** Sei $C = (\mathbb{Z}/61\mathbb{Z}) \times A_5$ das direkte Produkt der zyklischen Gruppe der Ordnung 61 und der alternierenden Gruppe A_5 . Ist C auflösbar? Begründen Sie Ihre Antwort. (14 Punkte)

Aufgabe 2 → S. 517

Sei

$$R := \mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}, \quad i^2 = -1,$$

der Ring der ganzen Gaußschen Zahlen. Sei

$$I := \mathbb{Z} \cdot 25 + \mathbb{Z}(7+i) = \{25x + y(7+i) \mid x, y \in \mathbb{Z}\}.$$

Die Menge I ist ein Ideal in R (Nachweis nicht erforderlich).

- a** Zeigen Sie, dass $\varphi: \mathbb{Z} \rightarrow R/I, a \mapsto a + I$ surjektiv ist und bestimmen Sie den Kern von φ .
- b** Zeigen Sie, dass die Gruppe $(R/I)^\times$ der Einheiten von R/I zyklisch von der Ordnung 20 ist.
- c** Wie viele verschiedene Erzeuger von $(R/I)^\times$ gibt es? Begründen Sie Ihre Antwort. (12 Punkte)

Aufgabe 3 → S. 518

Sei

$$f(x) = x^4 - 6x^2 - 14 \in \mathbb{Q}[x].$$

- a** Zeigen Sie, dass $K = \mathbb{Q}(\sqrt{3 + \sqrt{23}}, \sqrt{-14})$ der Zerfällungskörper von f ist.
- b** Zeigen Sie: $[K : \mathbb{Q}] = 8$. (12 Punkte)

Aufgabe 4 → S. 518

Sei

$$f(x) := x^3 - x - 1 \in \mathbb{Q}[x]$$

und $a \in \mathbb{C}$ eine Nullstelle von f . Sei $b := 2a^2 - a - 2$.

- a** Zeigen Sie, dass f irreduzibel über \mathbb{Q} ist.
- b** Zeigen Sie, dass $b \neq 0$ gilt.
- c** Bestimmen Sie das Minimalpolynom von a^2 über \mathbb{Q} . (12 Punkte)

Aufgabe 5 → S. 519

Es sei $M_4(\mathbb{Q})$ der Ring der 4×4 -Matrizen mit Einträgen in \mathbb{Q} . Sei

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 \\ -1 & -2 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 2 & 2 & 2 & -1 \end{pmatrix} \in M_4(\mathbb{Q}).$$

- a** Bestimmen Sie das charakteristische Polynom $\chi_A(x)$ sowie die Eigenwerte von A . Ist A diagonalisierbar?
- b** Berechnen Sie das Ideal $J_A = \{g \in \mathbb{Q}[X] \mid g(A) = 0\}$. (10 Punkte)
-

Thema Nr. 3 (Aufgabengruppe)

Aufgabe 1 → S. 520

Sei K ein Körper, $n \in \mathbb{N}$, und $K^{n \times n}$ der K -Vektorraum der $n \times n$ -Matrizen. Ferner sei $\mathrm{GL}_n(K)$ die Gruppe der invertierbaren Matrizen aus $K^{n \times n}$.

- a** Sei $A \in K^{n \times n}$, und V der von den Matrizen A^0, A^1, A^2, \dots erzeugte Unterraum von $K^{n \times n}$. Man zeige, dass $\dim V \leq n$.

Hinweis Satz von Cayley-Hamilton.

- b** Sei K ein endlicher Körper. Man zeige, dass jedes Element aus $\mathrm{GL}_n(K)$ höchstens die Ordnung $|K|^n - 1$ hat.

Hinweis Für $A \in \mathrm{GL}_n(K)$ vergleiche man die von A erzeugte Untergruppe von $\mathrm{GL}_n(K)$ mit V . (12 Punkte)

Aufgabe 2 → S. 521

Seien $m, n \in \mathbb{N}$ natürliche Zahlen ≥ 1 . Man zeige:

- a** $X^m - 1$ ist ein Teiler von $X^n - 1$ in $\mathbb{Q}[X]$ genau dann, wenn m ein Teiler von n ist.
- b** $X^m + 1$ ist ein Teiler von $X^n + 1$ in $\mathbb{Q}[X]$ genau dann, wenn m ein Teiler von n und n/m ungerade ist.
- c** Genau dann ist $X^n + 1$ irreduzibel in $\mathbb{Q}[X]$, wenn n eine Potenz von 2 ist.

Hinweis Für eine Zweierpotenz n ist $(X + 1)^n + 1$ ein Eisenstein-Polynom.

(12 Punkte)

Aufgabe 3 → S. 522

Sei p eine Primzahl, die die Ordnung der endlichen Gruppen G teilt. Weiter sei P eine zyklische p -Sylowgruppe von G . Man zeige:

- a** P enthält genau eine Untergruppe der Ordnung p .
- b** Es gelte $|P \cap x^{-1}Px| > 1$ für alle $x \in G$. Man zeige, dass G einen Normalteiler N hat mit $|N| = p^e$ mit $e \in \mathbb{N}$. (10 Punkte)

Aufgabe 4 → S. 523

Sei R ein Integritätsbereich und $I \subseteq R$ ein Primideal, so dass der Index $[R : I]$ der additiven Gruppen endlich ist. Zeigen Sie, dass I ein maximales Ideal von R ist.

(11 Punkte)

Aufgabe 5 → S. 523

Sei $f(X) = X^4 - 2X^2 - 2 \in \mathbb{Q}[X]$.

- a** Zeigen Sie, dass

$$\alpha_1 = \sqrt{1 + \sqrt{3}}, \quad \alpha_2 = \sqrt{1 - \sqrt{3}}, \quad \alpha_3 = -\alpha_1, \quad \alpha_4 = -\alpha_2$$

die Nullstellen von f in \mathbb{C} sind.

- b** Zeigen Sie, dass $\mathbb{Q}(\alpha_1) \neq \mathbb{Q}(\alpha_2)$ (als Teilkörper von \mathbb{C}).
- c** Zeigen Sie, dass $\mathbb{Q}(\sqrt{3}) = \mathbb{Q}(\alpha_1) \cap \mathbb{Q}(\alpha_2)$.
- d** Zeigen Sie, dass die Körpererweiterungen $\mathbb{Q}(\sqrt{3}) \subset \mathbb{Q}(\alpha_1)$ und $\mathbb{Q}(\sqrt{3}) \subset \mathbb{Q}(\alpha_2)$ galoissch sind.
- e** Sei K der Zerfällungskörper von f über \mathbb{Q} . Zeigen Sie, dass $\mathbb{Q}(\sqrt{3}) \subset K$ galoissch ist und bestimmen Sie den Isomorphietyp der Galois-Gruppe.

(15 Punkte)

Lösungen zu Thema Nr. 1

Lösungsvorschlag zur Aufgabe (Frühjahr 2016, T1A1)

Sei $\langle \cdot, \cdot \rangle$ ein Skalarprodukt auf einem euklidischen Vektorraum V . Eine **Orthogonalprojektion** auf einen Untervektorraum $U \subseteq V$ ist eine lineare Abbildung $\pi_U: V \rightarrow U$, sodass

$$\langle \pi_U(v) - v, u \rangle = 0 \quad \text{für alle } v \in V \text{ und } u \in U$$

erfüllt ist.

„ \Rightarrow “: Wir zeigen zunächst, dass $f^2 = f$, das zeigt dann gerade $M^2 = M$. Sei dazu U der Unterraum der Dimension k mit $f = \pi_U$ und sei $v \in V$ beliebig vorgegeben. Nach Definition gilt dann $f(v) \in U$, insbesondere also $f^2(v) - f(v) \in U$. Da sich $\langle \cdot, \cdot \rangle$ zu einem Skalarprodukt auf U beschränkt, dort also auch eine nicht-ausgeartete Bilinearform definiert, folgt aus

$$\langle f^2(v) - f(v), u \rangle = 0 \quad \text{für alle } u \in U,$$

dass bereits $f^2(v) - f(v) = 0$ gelten muss. Weil $v \in V$ ebenfalls beliebig war, zeigt dies $f^2 = f$.

Wir zeigen als nächstes, dass M symmetrisch ist. Dies ist genau dann der Fall, wenn $\langle Mv, w \rangle = \langle v, Mw \rangle$ für alle $v, w \in V$ erfüllt ist. Dazu bemerke zunächst, dass $f(v)$ und $f(w)$ in U liegen, sodass

$$\langle f(v) - v, f(w) \rangle = 0 = \langle f(w) - w, f(v) \rangle$$

gilt. Da $\langle \cdot, \cdot \rangle$ als Skalarprodukt eine symmetrische Bilinearform ist, haben wir nun die folgenden Äquivalenzen:

$$\begin{aligned} \langle f(v), w \rangle &= \langle v, f(w) \rangle \Leftrightarrow \langle w, f(v) \rangle = \langle v, f(w) \rangle \\ \Leftrightarrow \langle f(w), f(v) \rangle - \langle f(w) - w, f(v) \rangle &= \langle f(v), f(w) \rangle - \langle f(v) - v, f(w) \rangle \\ \Leftrightarrow \langle f(v), f(w) \rangle &= \langle f(v), f(w) \rangle \end{aligned}$$

Dies zeigt, dass f selbst-adjungiert ist, die Darstellungsmatrix M von f also symmetrisch ist. Es fehlt noch nachzuweisen, dass $\text{Tr } M = k$ ist. Sei $v \in U$, dann gilt für alle $u \in U$, dass

$$\langle f(v) - v, u \rangle = 0.$$

Weil $f(v) - v$ selbst in U liegt, folgt $f(v) - v = 0$ wie oben. Dies zeigt $f|_U = \text{id}_U$, d.h. $U \subseteq \text{Eig}_1(f)$. Nach dem Dimensionssatz für lineare Abbildungen gilt weiter

$$V \cong \text{im } f \oplus \ker f = U \oplus \ker f.$$

Wählt man eine Basis von U und einer von $\ker M$, so bilden diese demnach zusammen eine Basis von V und f hat in dieser Basis die Darstellungsmatrix

$$\begin{pmatrix} 1 & 0 & \dots & \dots & \dots & 0 \\ 0 & \ddots & & & & \vdots \\ \vdots & & 1 & & & \vdots \\ \vdots & & & 0 & & \vdots \\ \vdots & & & & \ddots & \vdots \\ 0 & \dots & \dots & \dots & \dots & 0 \end{pmatrix}$$

mit genau k Einträgen 1 für die k Basisvektoren von U . Da sich die Spur bei einem Basiswechsel nicht ändert, folgt $\text{Tr } M = k$.

„ \Leftarrow “: Sei nun umgekehrt f eine lineare Abbildung mit idempotenter und symmetrischer Darstellungsmatrix M . Sei $U = \text{im } f$ und $u = f(v) \in \text{im } f$, dann gilt

$$f(u) = f^2(v) = f(v) = u, \quad (\star)$$

da M idempotent ist. Weil M symmetrisch ist, ist außerdem f selbst-adjungiert. Daraus folgt, dass für alle $v \in V$ und $u \in U$ die Gleichung

$$\langle f(v), u \rangle = \langle v, f(u) \rangle \stackrel{(\star)}{=} \langle v, u \rangle \Leftrightarrow \langle f(v) - v, u \rangle = 0$$

gilt. Nach Definition ist daher f eine Orthogonalprojektion auf U und es bleibt zu zeigen, dass $\dim U = \text{Tr } M$. Wir haben

$$V \cong \text{im } f \oplus \ker f = U \oplus \ker f.$$

Oben haben wir außerdem bereits $f|_U = \text{id}_U$ gezeigt. Zusammen ergibt das wieder, dass M eine Diagonalgestalt wie oben besitzt, wobei die Anzahl der Einträge 1 der Dimension von U entspricht. Diese Anzahl ist gerade $\text{Tr } M$.

Lösungsvorschlag zur Aufgabe (Frühjahr 2016, T1A2)

„ \Leftarrow “: Wir nehmen zunächst an, dass n ungerade und nicht durch 3 teilbar ist. Es dann auf jeden Fall $n + 1$ gerade, also durch 2 teilbar. Falls $n \equiv 1 \pmod{3}$, so ist $2n + 1 \equiv 0 \pmod{3}$ und falls $n \equiv 2 \pmod{3}$, so ist $n + 1 \equiv 0 \pmod{3}$. Das Produkt $(n+1)(2n+1)$ ist daher auf jeden Fall durch 2 und 3 teilbar, also durch 6 teilbar. Es folgt, dass $m = \frac{(n+1)(2n+1)}{6}$ eine ganze Zahl ist, und laut dem Hinweis ist

$$\sum_{k=1}^n k^2 = n \cdot m.$$

Dies zeigt, dass $\sum_{k=1}^n k^2$ durch n teilbar ist.

„ \Rightarrow “: Sei umgekehrt $\sum_{k=1}^n k^2$ durch n teilbar, dann gibt es ein $m \in \mathbb{Z}$ mit $\sum_{k=1}^n k^2 = n \cdot m$. Laut dem Hinweis folgt

$$\frac{1}{6} \cdot (n+1) \cdot (2n+1) = nm \Leftrightarrow (n+1)(2n+1) = 6nm.$$

Betrachtet man diese Gleichung modulo 2, steht da $(n+1) \cdot 1 \equiv 0 \pmod{2}$, also $n \equiv 1 \pmod{2}$, und betrachtet man die Gleichung modulo 3, wird daraus $(n+1) \cdot (-n+1) \equiv 0 \pmod{3}$. Da $\mathbb{Z}/3\mathbb{Z}$ ein Integritätsbereich ist, ist letzteres genau dann der Fall, wenn $n \equiv -1 \pmod{3}$ oder $n \equiv 1 \pmod{3}$. Insbesondere ist n weder durch 2 noch durch 3 teilbar.

Lösungsvorschlag zur Aufgabe (Frühjahr 2016, T1A3)

- a** Wegen $(H : N) = 2$ gibt es neben N nur eine weitere Nebenklasse in H/N . Da $x, y \notin N$, müssen x und y beide in dieser Nebenklasse liegen, d.h. $yN = xN$. Daraus erhält man schon mal $x^{-1}y \in N$. Nun ist auch $x^{-1} \notin N$, denn andernfalls würde $x \in N$ aufgrund der Untergruppeneigenschaft von N folgen. Wenden wir also das gleiche Argument auf y und $x' = x^{-1}$ an, so erhalten wir $xy \in N$.
- b** Man kann hier natürlich alle vier auftretenden Fälle zu Fuß abklappern. Oder man macht Folgendes: Als Gruppe der Ordnung 2 ist H/N isomorph zu $(\{\pm 1\}, \cdot)$, Komposition mit der Projektion $H \rightarrow H/N$ liefert einen Homomorphismus

$$\sigma: H \rightarrow \{\pm 1\}, \quad x \mapsto \begin{cases} 1 & \text{falls } x \in N, \\ -1 & \text{falls } x \notin N. \end{cases}$$

Die Verknüpfungsvorschrift wird damit zu $(a, x) \circledast (b, y) = (a + \sigma(x)b, xy)$. Seien nun also $(a, x), (b, y), (c, z) \in A \times H$ vorgegeben. Dann berechnet man

$$\begin{aligned} & (a, x) \circledast ((b, y) \circledast (c, z)) = \\ &= (a, x) \circledast (b + \sigma(y)c, xyz) = (a + \sigma(x)(b + \sigma(y)c), xyz) = \\ &= (a + \sigma(x)b + \sigma(xy)c, xyz) = (a + \sigma(x)b, xy) \circledast (c, z) = \\ &= ((a, x) \circledast (b, y)) \circledast (c, z). \end{aligned}$$

- c** Da x Ordnung 2 hat, ist $x \neq 1$ und somit $(a, x) \neq (0, 1)$. Wegen

$$(a, x)^2 = (a - a, x^2) = (0, 1)$$

folgt daraus, dass (a, x) Ordnung 2 in $A \times H$ hat.

- d** Sei $A = \mathbb{Z}/21\mathbb{Z}$ und $H = \{\pm 1\}$ mit dem Normalteiler $N = \{1\}$, dann ist $A \times H$ mit der Verknüpfung \circledast eine Gruppe der Ordnung 42. Angenommen, es gibt ein Element $(a, x) \in A \times H$ der Ordnung 14. Wegen $|H| = 2$ kann x nur Ordnung 1 oder 2 haben. Da (a, x) Ordnung 14 haben soll, folgt aus Teil **c**, dass x Ordnung 1 hat, d. h. $x = 1$. Somit gilt

$$(a, x)^n = (a, 1)^n = (na, 1) \quad \text{für alle } n \in \mathbb{N},$$

sodass $\text{ord}(a, 1) = \text{ord } a$. Wegen $14 \nmid 21$ gibt es jedoch kein Element der Ordnung 14 in A . Der Fall eines Elementes der Ordnung 6 lässt sich vollkommen analog behandeln.

Lösungsvorschlag zur Aufgabe (Frühjahr 2016, T1A4)

- a** Ein Element $x = a + b\sqrt{-D}$ ist genau dann eine Einheit, falls $N(x) = a^2 + Db^2 = 1$ gilt. Nehmen wir an, dass $b \neq 0$, dann ist $b^2 \geq 1$, d. h.

$$1 = N(x) = a^2 + Db^2 \geq D > 1,$$

was unmöglich sein kann. Also ist $b = 0$ und $a^2 = 1$. Es folgt $x = 1$ oder $x = -1$.

- b** Nehmen wir an, es gibt $x, y \in R$ mit $2 = xy$ und $x, y \notin R^*$. Insbesondere ist dann $N(x) \neq 1 \neq N(y)$ und aus der Gleichung

$$4 = N(2) = N(xy) = N(x) \cdot N(y)$$

erhält man als einzige mögliche Lösung $N(x) = 2 = N(y)$. Schreibe $x = a + b\sqrt{-13}$, dann führt die Annahme $b \neq 0$ auf die Ungleichung

$$2 = a^2 + 13b^2 \geq 13.$$

Da dies ein Widerspruch ist, muss $b = 0$ sein. Allerdings hat die resultierende Gleichung $a^2 = 2$ keine Lösung in \mathbb{Z} , sodass die ursprüngliche Annahme falsch gewesen sein muss. Folglich ist 2 irreduzibel in R . Genau so verfährt man im zweiten Fall: Angenommen, es gibt Nicht-Einheiten $x, y \in R$ mit $1 + \sqrt{-13} = xy$, so hätten wir

$$14 = N(1 + \sqrt{-13}) = N(xy) = N(x)N(y),$$

woraus wir o. B. d. A. $N(x) = 7$ und $N(y) = 2$ schließen können. Allerdings haben wir oben bereits gesehen, dass $N(y) = 2$ zu einem Widerspruch führt.

- c** Wäre 2 ein Primelement, so würde aus $14 = (1 + \sqrt{-13})(1 - \sqrt{-13})$ folgen, dass 2 ein Teiler von $1 + \sqrt{-13}$ oder $1 - \sqrt{-13}$ sein müsste. Es gäbe also ein $x \in R$ mit $2x = (1 + \sqrt{-13})$ oder $2x = (1 - \sqrt{-13})$. In beiden Fällen folgt durch Anwenden der Norm jedoch

$$4 \cdot N(x) = N(2x) = N(1 \pm \sqrt{-13}) = 14.$$

Bekanntlich ist aber 4 kein Teiler von 14.

Lösungsvorschlag zur Aufgabe (Frühjahr 2016, T1A5)

- a** Wir berechnen:

$$\begin{aligned} \alpha^2 = \frac{\sqrt{5} + 5}{8} &\Rightarrow 8\alpha^2 - 5 = \sqrt{5} \Rightarrow (8\alpha^2 - 5)^2 = 5 \\ &\Rightarrow 64\alpha^4 - 80\alpha^2 + 20 = 0. \end{aligned}$$

Somit ist $16X^4 - 20X^2 + 5$ schon mal ein Polynom, das α als Nullstelle hat. Glücklicherweise ist dieses Polynom nach dem Eisensteinkriterium mit $p = 5$ auch irreduzibel. Da die Irreduzibilität durch Normierung nicht verloren geht, ist $X^4 - \frac{5}{4}X^2 + \frac{5}{16}$ das gesuchte Minimalpolynom.

- b** Angenommen, es ist $i \in \mathbb{Q}(\zeta_5)$. Dann wäre wegen $\operatorname{Im} \zeta_5^1 = -\operatorname{Im} \zeta_5$ auch

$$\alpha = \frac{-i}{2}(e^{2\pi i/5} - e^{-2\pi i/5}) = \frac{-i}{2}(\zeta_5 - \zeta_5^{-1}) \in \mathbb{Q}(\zeta_5).$$

Es folgt $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\zeta_5)$. Nach Teil **a** gilt $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$, für den Kreisteilungskörper $\mathbb{Q}(\zeta_5)$ gilt ebenfalls $[\mathbb{Q}(\zeta_5) : \mathbb{Q}] = \varphi(5) = 4$. Deshalb haben wir unter Verwendung der Gradformel:

$$[\mathbb{Q}(\zeta_5) : \mathbb{Q}(\alpha)] = \frac{[\mathbb{Q}(\zeta_5) : \mathbb{Q}]}{[\mathbb{Q}(\alpha) : \mathbb{Q}]} = \frac{4}{4} = 1,$$

was $\mathbb{Q}(\zeta_5) = \mathbb{Q}(\alpha)$ bedeutet. Allerdings ist wegen $\alpha \in \mathbb{R}$ auch $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$, während $\zeta_5 \notin \mathbb{R}$ ist. Die Annahme $i \in \mathbb{Q}(\zeta_5)$ muss daher falsch gewesen sein.

Lösungen zu Thema Nr. 2

Lösungsvorschlag zur Aufgabe (Frühjahr 2016, T2A1)

- a** Betrachte die Determinantenabbildung $\det: G \rightarrow \mathbb{F}_p^\times$, welche einen Gruppenhomomorphismus definiert. Sei $A \in G$ und seien $a, b \in \mathbb{F}_p$ mit

$$A = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix},$$

dann ist $\det(A) = a$. Folglich ist die Determinantenabbildung surjektiv. Sei $N = \ker \det$, dann liefert der Homomorphiesatz einen Isomorphismus $G/N \cong \mathbb{F}_p^\times$. Da \mathbb{F}_p^\times abelsch ist, ist der Quotient G/N auflösbar. Um Satz 1.30 anwenden zu können, müssen wir noch zeigen, dass N ebenfalls auflösbar ist. Dazu bestimmen wir zunächst N : Sei $A \in N$ mit $a, b \in \mathbb{F}_p$ wie oben, dann gilt

$$A \in N \Leftrightarrow \det(N) = 1 \Leftrightarrow a = 1,$$

also ist

$$N = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \mid b \in \mathbb{F}_p \right\}.$$

Man kann nun direkt überprüfen, dass N abelsch ist oder zeigt, dass

$$N \rightarrow \mathbb{F}_p, \quad \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \mapsto b$$

ein Isomorphismus ist. Auf jeden Fall ist N auflösbar.

- b** Laut dem Dritten Sylowsatzes gilt für die Anzahl ν_p der p -Sylowgruppen von G , dass $\nu_p \equiv 1 \pmod{p}$ und $\nu_p | p - 1$. Die zweite Bedingung liefert insbesondere $\nu_p \leq p - 1$, weswegen nur $\nu_p = 1$ beide Bedingungen erfüllt.

Sei H die einzige p -Sylowgruppe, dann ist diese ein Normalteiler von G . Außerdem ist N als Gruppe von Primzahlordnung zyklisch und somit auflösbar. Aus Satz 1.30 folgt daher, dass G genau dann auflösbar ist, wenn G/H auflösbar ist.

- c** Zufälligerweise ist $|C| = 61 \cdot 60$ und 61 ist eine Primzahl. Dabei ist $H = \mathbb{Z}/61\mathbb{Z} \times \{\text{id}\}$ die eindeutige Untergruppe der Ordnung 61 von G . Nach Teil **b** ist daher C genau dann auflösbar, wenn $C/H \cong A_5$ auflösbar ist. Da die alternierende Gruppe A_5 nicht auflösbar ist, kann also auch C nicht auflösbar sein.

Lösungsvorschlag zur Aufgabe (Frühjahr 2016, T2A2)

- a** Sei $x + I \in R/I$ beliebig vorgegeben mit $x = a + bi$. Es ist dann

$$x + I = a + bi + I = (a - 7b) + b(7 + i) + I = a - 7b + I,$$

d.h. $\varphi(a - 7b) = x + I$, sodass φ surjektiv ist. Sei nun $a \in \ker \varphi \subseteq \mathbb{Z}$, dann gilt $\varphi(a) = \bar{0}$, d.h. $a \in I$. Es gibt also $x, y \in \mathbb{Z}$, sodass

$$a = 25x + y(7 + i) = (25x + 7y) + yi.$$

Da a eine ganze Zahl ist, muss der Imaginärteil auf der rechten Seite verschwinden, was gerade $y = 0$ bedeutet. Also ist $a = 25x$ und liegt in $25\mathbb{Z}$. Umgekehrt liegt $25\mathbb{Z}$ natürlich im Kern von φ , sodass $\ker \varphi = 25\mathbb{Z}$. Da a eine ganze Zahl ist, muss der Imaginärteil auf der rechten Seite verschwinden, was gerade $y = 0$ bedeutet. Also ist $a = 25x$ und liegt in $25\mathbb{Z}$. Umgekehrt liegt $25\mathbb{Z}$ natürlich im Kern von φ , sodass $\ker \varphi = 25\mathbb{Z}$.

- b** Nach Teil **a** und dem Homomorphiesatz gilt $R/I \cong \mathbb{Z}/25\mathbb{Z}$. Unter Verwendung von Satz 2.8 (2) gilt daher

$$(R/I)^\times \cong (\mathbb{Z}/25\mathbb{Z})^\times \cong \mathbb{Z}/20\mathbb{Z}.$$

- c** Die Anzahl der verschiedenen Erzeuger einer Gruppe der Ordnung n ist die Anzahl der Elemente der Ordnung n dieser Gruppe und damit $\varphi(n)$. In unserem Fall sind das also

$$\varphi(20) = \varphi(4 \cdot 5) = \varphi(4) \cdot \varphi(5) = 2 \cdot 4 = 8.$$

Lösungsvorschlag zur Aufgabe (Frühjahr 2016, T2A3)

- a Wir berechnen die Nullstellen von f mit der Substitution $u = x^2$

$$x^4 - 6x^2 - 14 = 0 \Leftrightarrow u^2 - 6u - 14 = 0 \Leftrightarrow u = 3 \pm \sqrt{23}.$$

Somit sind die vier Nullstellen gegeben durch

$$\pm\sqrt{3 + \sqrt{23}}, \pm\sqrt{3 - \sqrt{23}}.$$

Damit ist $Z = \mathbb{Q}(\sqrt{3 + \sqrt{23}}, \sqrt{3 - \sqrt{23}})$ ein Zerfällungskörper von f . Wir zeigen $Z = K$. Betrachte dazu

$$\sqrt{3 + \sqrt{23}} \cdot \sqrt{3 - \sqrt{23}} = \sqrt{9 - 23} = \sqrt{-14}.$$

Damit liegt einerseits $\sqrt{3 - \sqrt{23}} = \frac{\sqrt{-14}}{\sqrt{3 + \sqrt{23}}}$ in K , anderseits liegt $\sqrt{-14}$ in Z . Insgesamt haben wir damit $Z = K$ und K ist Zerfällungskörper von f .

- b Sei nun $\alpha = \sqrt{3 + \sqrt{23}}$. Das Polynom f ist normiert, irreduzibel über \mathbb{Q} laut dem Eisenstein-Kriterium mit $p = 2$ und hat α als Nullstelle. Damit ist

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = \text{grad } f = 4.$$

Das Polynom $g = X^2 + 14 \in \mathbb{Q}(\alpha)[X]$ hat die Nullstelle $\sqrt{-14}$. Das Minimalpolynom von $\sqrt{-14}$ über $\mathbb{Q}(\alpha)$ ist damit ein Teiler von g und wir erhalten $[\mathbb{Q}(\alpha, \sqrt{-14}) : \mathbb{Q}(\alpha)] \leq 2$. Wäre der Grad 1, so wäre $\mathbb{Q}(\alpha, \sqrt{-14}) = \mathbb{Q}(\alpha)$. Nun ist der Körper auf der rechten Seite wegen $\alpha \in \mathbb{R}$ aber ein Teilkörper der reellen Zahlen, während der Körper auf der linken Seite mit $\sqrt{-14}$ ein Element von $\mathbb{C} \setminus \mathbb{R}$ enthält – Widerspruch. Der Erweiterungsgrad beträgt deswegen 2 und die Gradformel liefert uns

$$[K : \mathbb{Q}] = [\mathbb{Q}(\alpha, \sqrt{-14}) : \mathbb{Q}(\alpha)] \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}] = 4 \cdot 2 = 8.$$

Lösungsvorschlag zur Aufgabe (Frühjahr 2016, T2A4)

- a Wir verwenden das Reduktionskriterium und zeigen, dass das Bild $\bar{f} = x^3 + x + \bar{1}$ irreduzibel in $\mathbb{F}_2[X]$ ist. Dazu genügt es zu überprüfen, dass \bar{f} keine Nullstellen in \mathbb{F}_2 besitzt. Wegen $f(\bar{0}) = \bar{1}$ und $f(\bar{1}) = \bar{1}$ ist das der Fall.

- b** Als irreduzibles und normiertes Polynom mit Nullstelle a ist f das Minimalpolynom von a über \mathbb{Q} . Wäre $b = 0$, so wäre $x^2 - \frac{1}{2}x - 1$ ein Polynom von kleinerem Grad als f , das a als Nullstelle hat, im Widerspruch dazu, dass f das Minimalpolynom von a ist. Also muss $b \neq 0$ sein.
- c** Sei g das Minimalpolynom von a^2 über \mathbb{Q} , dann ist $\text{grad } g = [\mathbb{Q}(a^2) : \mathbb{Q}]$. Wegen $a^2 \in \mathbb{Q}(a)$ und $[\mathbb{Q}(a) : \mathbb{Q}] = \text{grad } f = 3$ ist nach 3.2 dann $\text{grad } g$ ein Teiler von 3. Wäre $\text{grad } g = 1$, so wäre $a^2 \in \mathbb{Q}$. Dies kann jedoch nicht sein, da sonst $X^2 - a^2$ ein Polynom in $\mathbb{Q}[X]$ mit Nullstelle a wäre, das kleineren Grad als f hat. Also wissen wir schon mal, dass wir nach einem Polynom von Grad 3 suchen müssen, wenn wir g finden wollen.

Wir berechnen unter Verwendung von $f(a) = 0$, also $a^3 = a + 1$:

$$\begin{aligned}(a^2)^3 &= (a^3)^2 = (a + 1)^2 = a^2 + 2a + 1 = a(a^3 - 1) + 2a + 1 = a^4 + a + 1 \\ &= a^4 + a^2 - a^2 + a + 1 = a^4 + a(a + 1) - a^2 + 1 = 2a^4 - a^2 + 1\end{aligned}$$

Also ist das Polynom $x^3 - 2x^2 + x - 1$ ein Kandidat für g . Da dieses Polynom normiert ist und den richtigen Grad, nämlich 3, hat, handelt sich dabei tatsächlich um g .

Lösungsvorschlag zur Aufgabe (Frühjahr 2016, T2A5)

- a** Wir erhalten mit dem Laplace'schen Entwicklungssatz, angewendet auf die 3. Zeile

$$\begin{aligned}\chi_A &= \det \begin{pmatrix} -X & 1 & 0 & 0 \\ -1 & -2 - X & 0 & 0 \\ 0 & 0 & -1 - X & 0 \\ 2 & 2 & 2 & -1 - X \end{pmatrix} = \\ &= 1 \cdot (-1 - X) \det \begin{pmatrix} -X & 1 & 0 & 0 \\ -1 & -2 - X & 0 & 0 \\ 2 & 2 & -1 - X & 0 \end{pmatrix} = (X + 1)^4.\end{aligned}$$

A hat damit den vierfachen Eigenwert -1 . Damit A diagonalisierbar ist, müsste $\text{Eig}(A, -1) = \ker(A + \mathbb{E}_4)$ vierdimensional sein, also ganz \mathbb{Q}^4 sein. Dies ist nur möglich, wenn $A + \mathbb{E}_4$ die Nullmatrix ist. Wegen

$$A + \mathbb{E}_4 = \begin{pmatrix} 1 & 1 & 0 & 0 \\ -1 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 2 & 2 & 2 & 0 \end{pmatrix}$$

ist A also nicht diagonalisierbar (alternativ berechne $\text{Eig}(A, -1)$ wie gewohnt).

b Das gesuchte Ideal wird vom Minimalpolynom von A erzeugt (vgl. Seite 241). Dieses ist laut dem Satz von Cayley-Hamilton ein Teiler des charakteristischen Polynoms. Es kommen daher nur Potenzen von $X + 1$ in Frage. Wir haben oben bereits gesehen, dass $A + \mathbb{E}_4$ nicht die Nullmatrix ergibt. Weiter gilt

$$(A + \mathbb{E}_4)^2 = \begin{pmatrix} 1 & 1 & 0 & 0 \\ -1 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 2 & 2 & 2 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 & 0 \\ -1 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 2 & 2 & 2 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Damit ist $(X + 1)^2$ das Minimalpolynom von A und wir haben

$$J_A = ((X + 1)^2).$$

Lösungen zu Thema Nr. 3

Lösungsvorschlag zur Aufgabe (Frühjahr 2016, T3A1)

a Sei χ_A das charakteristische Polynom von A . Der Grad von χ_A ist n . Nach dem Satz von Cayley-Hamilton 4.6 ist $\chi_A(A) = 0$, somit erhalten wir eine Darstellung der Form

$$\begin{aligned} a_n A^n + \dots + a_1 A + a_0 \mathbb{E}_n &= 0 \\ \Leftrightarrow A^n &= \frac{-1}{a_n} (a_{n-1} A^{n-1} + \dots + a_1 A + a_0 \mathbb{E}_n). \end{aligned}$$

Daraus ergibt sich nun per vollständiger Induktion, dass jede Potenz der Form A^m für $m \geq n$ als Linearkombination von $\{\mathbb{E}_n, \dots, A^{n-1}\}$ darstellen lässt: Für $m = n$ haben wir dies bereits begründet. Für den Induktions-schritt betrachte

$$\begin{aligned} A^{m+1} &= AA^m \stackrel{(I.V.)}{=} A (b_{n-1} A^{n-1} + \dots + b_0 \mathbb{E}_n) = b_{n-1} A^n + \dots + b_0 A = \\ &= b_{n-1} \left(\frac{-1}{a_n} (a_{n-1} A^{n-1} + \dots + a_0 \mathbb{E}_n) \right) + b_{n-2} A^{n-2} + \dots + b_0 A. \end{aligned}$$

Insgesamt haben wir damit

$$V = \langle A^0, A^1, A^2, \dots \rangle \subseteq \langle A^0, A^1, \dots, A^n \rangle$$

und deshalb $\dim V \leq n$.

- b** Sei $A \in \mathrm{GL}_n(K)$. Die von A erzeugte Untergruppe ist gegeben durch

$$\langle A \rangle = \{A^k \mid k \in \mathbb{Z}\}.$$

Sei $k \geq 0$, so gilt $A^k \in V$ laut der Definition von V . Um zu zeigen, dass auch die Matrix A^{-k} in V liegt, bemerke, dass mit K auch $\mathrm{GL}_n(K)$ endlich ist. Damit ist $A^m = AA^{m-1} = \mathbb{E}_n$ für ein $m \in \mathbb{N}$ und damit $A^{-1} = A^{m-1}$, also auch $A^{-k} = (A^{-1})^k = (A^{m-1})^k \in V$. Damit haben wir $\langle A \rangle \subseteq V \setminus \{0\}$. Der Untervektorraum V hat wegen $\dim V \leq n$ höchstens $|K|^n$ Elemente, also ist

$$\mathrm{ord} A = |\langle A \rangle| \leq |V \setminus \{0\}| = |K|^n - 1.$$

Lösungsvorschlag zur Aufgabe (Frühjahr 2016, T3A2)

- a** Division mit Rest ergibt Zahlen $q, r \in \mathbb{N}$ mit $n = qm + r$. Wir zeigen, dass $X^n - 1 \equiv 0 \pmod{(X^m - 1)}$ genau dann gilt, wenn $r = 0$ ist. Betrachte hierzu zunächst

$$X^n - 1 \equiv X^{qm+r} - 1 \equiv 1^q \cdot X^r - 1 \equiv X^r - 1 \pmod{(X^m - 1)}.$$

Wegen $\mathrm{grad} X^r - 1 < \mathrm{grad} X^m - 1$ ist $X^r - 1$ der eindeutige Rest der Division von $X^n - 1$ durch $X^m - 1$ und es ist $X^m - 1$ genau dann ein Teiler von $X^n - 1$, wenn $X^r - 1 = 0$, also $r = 0$ gilt.

- b** Hier haben wir wiederum für $n = qm + r$,

$$X^n + 1 \equiv X^{qm+r} + 1 \equiv (-1)^q X^r + 1 \pmod{(X^m + 1)}.$$

Nach gleicher Begründung ist $X^m + 1$ genau dann ein Teiler von $X^n + 1$, wenn $(-1)^q X^r + 1 = 0$ ist. Aus Gradgründen ist dies genau dann der Fall, wenn $r = 0$ und $(-1)^q = -1$, also q ungerade ist.

- c** Ist n keine Potenz von zwei, so hat n einen ungeraden Teiler d und somit eine Darstellung der Form $n = dm$ für ein $m \in \mathbb{N}$. Da somit aber m ein Teiler von n und $n/m = d$ ungerade ist, hat $X^n + 1$ laut Teil **b** den Teiler $X^m + 1$ und ist somit nicht irreduzibel.

Nehmen wir an, n ist eine Zweierpotenz. Wir zeigen, dem Hinweis entsprechend, zunächst, dass dann $(X + 1)^n + 1$ irreduzibel nach dem Eisenstein-Kriterium ist. Mit dem binomischen Lehrsatz erhalten wir

$$(X + 1)^n + 1 = \sum_{k=0}^n \binom{n}{k} X^k + 1 = X^n + \sum_{k=1}^{n-1} \binom{n}{k} X^k + 2.$$

Also ist der letzte Koeffizient durch zwei, nicht aber durch 2^2 teilbar. Mit dem *freshman's dream* angewendet auf die Zweierpotenz n erhalten wir

$$(X + 1)^n + 1 \equiv X^n + 2 \equiv X^n \pmod{2},$$

sodass außer dem Leitkoeffizienten alle Koeffizienten durch 2 teilbar sind. Also handelt es sich bei $(X + 1)^n + 1$ tatsächlich um ein Eisenstein-Polynom mit $p = 2$. Nehmen wir nun an, dass $X^n - 1 = fg$ eine Zerlegung in Nicht-Einheiten $f, g \in \mathbb{Q}[X]$ wäre, dann ist

$$(X + 1)^n - 1 = f(X + 1)g(X + 1)$$

eine Zerlegung von $(X + 1)^n + 1$ in Nicht-Einheiten, im Widerspruch dazu, dass dieses Polynom wie eben gezeigt irreduzibel ist. Also kann es eine solche Zerlegung von $X^n - 1$ nicht geben.

Lösungsvorschlag zur Aufgabe (Frühjahr 2016, T3A3)

- a** Da P eine p -Sylowgruppe ist, ist p ein Teiler ihrer Ordnung. Damit folgt die Aussage daraus, dass in zyklischen Gruppen für jeden Teiler der Gruppenordnung genau eine Untergruppe entsprechender Ordnung existiert.
- b** Betrachte die Menge

$$N = \bigcap_{x \in G} x^{-1}Px.$$

Für beliebiges $x \in G$ sind die Konjugierten $x^{-1}Px$ wiederum p -Sylowgruppen von G , also handelt es sich dabei insbesondere um Untergruppen von G , sodass auch N eine Untergruppe von G ist. Zudem ist laut Voraussetzung $|N| > 1$ und da N auch eine Untergruppe von P ist, muss laut dem Satz von Lagrange $|N| = p^e$ für ein $e \in \mathbb{N}$ gelten. Wir zeigen noch, dass es sich bei N um einen Normalteiler handelt. Sei dazu $x^{-1}px \in N$ und $g \in G$, dann gilt

$$g(x^{-1}px)g^{-1} = gx^{-1}pxg^{-1} = \left(gx^{-1}\right)p\left(gx^{-1}\right)^{-1} \in N.$$

Lösungsvorschlag zur Aufgabe (Frühjahr 2016, T3A4)

Da I ein Primideal ist, ist R/I nach Satz 2.7 (1) ein Integritätsbereich, der wegen $[R : I] < \infty$ endlich ist. Mittels einer der Methoden aus dem Kasten auf Seite 76 zeigt man, dass R/I bereits ein Körper sein muss, sodass I nach Satz 2.7(2) ein maximales Ideal ist.

Lösungsvorschlag zur Aufgabe (Frühjahr 2016, T3A5)

a Es gilt

$$(1 \pm \sqrt{3})^2 - 2(1 \pm \sqrt{3}) - 2 = 1 \pm 2\sqrt{3} + 3 - 2 \mp 2\sqrt{3} - 2 = 0,$$

sodass α_1 und α_2 Nullstellen von f sind. Da f ein gerades Polynom ist, folgt daraus auch, dass α_3 und α_4 Nullstellen von f sind.

b Wegen $\sqrt{3} > 1$ ist $\alpha_2 \notin \mathbb{R}$, während $\mathbb{Q}(\alpha_1) \subseteq \mathbb{R}$ gilt. Damit ist $\alpha_2 \notin \mathbb{Q}(\alpha_1)$.

c Die Inklusion „ \subseteq “ folgt aus

$$\sqrt{3} = \sqrt{1 + \sqrt{3}}^2 - 1 = -\sqrt{1 - \sqrt{3}}^2 + 1 \in \mathbb{Q}(\alpha_1) \cap \mathbb{Q}(\alpha_2).$$

Für die Inklusion „ \supseteq “ sei $\beta \in \mathbb{Q}(\alpha_1) \cap \mathbb{Q}(\alpha_2)$. Bemerke zunächst, dass der Körper $\mathbb{Q}(\alpha_1)$ ein Teilkörper der reellen Zahlen ist, also muss auch β reell sein.

Das Polynom f ist normiert, irreduzibel nach dem Eisenstein-Kriterium mit $p = 2$ und hat α_1 und α_2 als Nullstelle, ist also das Minimalpolynom von α_1 und α_2 . Damit erhalten wir

$$[\mathbb{Q}(\alpha_1) : \mathbb{Q}] = [\mathbb{Q}(\alpha_2) : \mathbb{Q}] = \text{grad } f = 4.$$

Somit besitzt β als Element von $\mathbb{Q}(\alpha_2)$ eine Darstellung der Form

$$\beta = a + b\alpha_2 + c\alpha_2^2 + d\alpha_2^3 = a + b\sqrt{1 - \sqrt{3}} + c(1 - \sqrt{3}) + d\sqrt{(1 - \sqrt{3})^3}$$

für $a, b, c, d \in \mathbb{Q}$. $\beta \in \mathbb{R}$ ist daher nur möglich, falls $b = d = 0$ gilt. Daraus folgt sogleich $\beta \in \mathbb{Q}(\sqrt{3})$.

d Der Grad der Erweiterung $\mathbb{Q}(\sqrt{3})|\mathbb{Q}$ ist 2, wie man routiniert zeigt. Somit liefert die Gradformel

$$[\mathbb{Q}(\alpha_1) : \mathbb{Q}(\sqrt{3})] = [\mathbb{Q}(\alpha_2) : \mathbb{Q}(\sqrt{3})] = \frac{4}{2} = 2.$$

Als Erweiterungen von Grad zwei sind die beiden Erweiterungen damit normal. Ferner handelt es sich bei $\mathbb{Q}(\sqrt{3})$ um einen Körper der Charakteristik 0, sodass die Erweiterungen auch separabel, insgesamt also galoissch sind.

- e Wiederum ist die Erweiterung natürlich separabel, ferner ist K laut Definition Zerfällungskörper von f und damit auch normal. Der Zerfällungskörper K enthält $\mathbb{Q}(\alpha_1)$ und $\mathbb{Q}(\alpha_2)$ und ist der kleinste Körper mit dieser Eigenschaft. Somit handelt es sich bei K um das Kompositum $\mathbb{Q}(\alpha_1) \cdot \mathbb{Q}(\alpha_2)$. Mit Proposition 3.23 (2) erhalten wir, da $\mathbb{Q}(\alpha_1) \cap \mathbb{Q}(\alpha_2) = \mathbb{Q}(\sqrt{3})$ laut Teil c gilt,

$$G_{K|\mathbb{Q}(\sqrt{3})} \cong G_{\mathbb{Q}(\alpha_1)|\mathbb{Q}(\sqrt{3})} \times G_{\mathbb{Q}(\alpha_2)|\mathbb{Q}(\sqrt{3})} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Prüfungstermin: Herbst 2016

Thema Nr. 1 (Aufgabengruppe)

Aufgabe 1 → S. 529

Seien N ein auflösbarer Normalteiler einer endlichen Gruppe G und H eine weitere auflösbare Untergruppe von G . Zeigen Sie, dass

$$\{nh \mid n \in N, h \in H\}$$

wieder eine auflösbare Untergruppe von G ist.

(12 Punkte)

Aufgabe 2 → S. 529

Seien p eine Primzahl und $k \leq p - 2$. Zeigen Sie, dass die Einheitsmatrix I_k die einzige Matrix $A \in \mathrm{GL}_k(\mathbb{Q})$ mit der Eigenschaft $A^p = I_k$. (12 Punkte)

Aufgabe 3 → S. 529

Sei R ein kommutativer Ring mit Einselement. Zu jedem $a \in R$ existiere ein $b \in R$ mit $a^2 \cdot b = a$.

- a** Zeigen Sie, dass R reduziert ist, das heißt, 0 das einzige nilpotente Element in R ist.
- b** Zeigen Sie weiter, dass jedes Primideal \mathfrak{p} in R maximal ist. (12 Punkte)

Aufgabe 4 → S. 530

Sei $a \in \mathbb{N}_0$. Wir definieren eine Folge (x_n) , $n \in \mathbb{N}_0$ durch

$$x_n = a^{2^n} + 1.$$

- a** Sei $n < m$. Zeigen Sie, dass x_n ein Teiler von $x_m - 2$ ist.
- b** Berechnen Sie den größten gemeinsamen Teiler von x_n und x_m .
- c** Folgern Sie, dass es unendlich viele Primzahlen gibt. (12 Punkte)

Aufgabe 5 → S. 531

Sei $f(X)$ ein separables Polynom über \mathbb{Q} , welches in der Form $f(X) = h(X^2)$ mit $h(X) \in \mathbb{Q}[X]$ und $n = \deg h(X) \geq 2$ geschrieben werden kann. Zeigen Sie,

dass die Galoissche Gruppe (eines Zerfällungskörpers) von $f(X)$ nicht die volle symmetrische Gruppe der Nullstellen sein kann. (12 Punkte)

Thema Nr. 2 (Aufgabengruppe)

Aufgabe 1 → S. 531

Sei $H := \{z \in \mathbb{C} \mid \operatorname{Im} z > 0\}$ die obere Halbebene und $\operatorname{SL}_2(\mathbb{R})$ die Gruppe der reellen 2×2 -Matrizen mit Determinante 1. Die Abbildung

$$\varrho: \operatorname{SL}_2(\mathbb{R}) \times H \rightarrow H, \quad \left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}, z \right) \mapsto \frac{az + b}{cz + d}$$

definiert eine Gruppenoperation von $\operatorname{SL}_2(\mathbb{R})$ auf H .

- a** Geben Sie die Bahnen von ϱ an.
- b** Geben Sie den Stabilisator von $i \in H$ an. (6 + 2 Punkte)

Aufgabe 2 → S. 532

Seien A, B abelsche Gruppen und $\phi: B \rightarrow \operatorname{Aut}(A)$ ein Homomorphismus von B in die Gruppe der Automorphismen von A . Das *semidirekte Produkt* $A \rtimes_{\phi} B$ ist die folgendermaßen definierte Gruppe:

$$\begin{aligned} A \rtimes_{\phi} B &:= \{(a, b) \mid a \in A, b \in B\} \\ (a_1, b_1) \cdot (a_2, b_2) &:= (a_1 \phi(b_1)(a_2), b_1 b_2) \end{aligned}$$

- a** Zeigen Sie, dass $A \rtimes_{\phi} B$ genau dann abelsch ist, wenn ϕ trivial ist, also $\phi(b) = \operatorname{id}_A$ für alle $b \in B$ gilt.
- b** Konstruieren Sie eine nichtabelsche Gruppe der Ordnung 2015. (6 + 10 Punkte)

Aufgabe 3 → S. 533

Im Folgenden sei K jeweils der angegebene Körper. Entscheiden Sie jeweils, ob die Matrix A über K diagonalisierbar ist, und begründen Sie Ihre Antwort.

$$\textbf{a} \quad A = \begin{pmatrix} 2 & 1 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}, K = \mathbb{C}$$

$$\textbf{b} \quad A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, K = \mathbb{R}$$

c $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, K = \mathbb{F}_5$

d $A = \begin{pmatrix} X+1 & 1 \\ X-1 & 2X-1 \end{pmatrix}, K$ ist der rationale Funktionenkörper $\mathbb{R}(X)$.

(2 + 2 + 3 + 3 Punkte)

Aufgabe 4 → S. 534

Sei $p > 2$ eine Primzahl. Wir betrachten den Körper $K = \mathbb{Q}(\zeta_p, \alpha_p) \subset \mathbb{C}$ mit $\alpha_p = \sqrt[p]{p} \in \mathbb{R}$ und $\zeta_p = e^{\frac{2\pi i}{p}}$. Zeigen Sie:

- a** Die Körpererweiterung $K|\mathbb{Q}$ ist galois'sch.
- b** $[K : \mathbb{Q}] = p(p-1)$.
- c** Die Teilerweiterung $\mathbb{Q}(\alpha_p)|\mathbb{Q}$ ist nicht normal und daher ist die Galois-Gruppe $\text{Gal}(K|\mathbb{Q})$ nicht abelsch.
- d** $\text{Gal}(K|\mathbb{Q})$ hat einen Normalteiler der Ordnung p . (2 + 6 + 6 + 2 Punkte)

Aufgabe 5 → S. 535

Sei p eine Primzahl. Wir betrachten in $\mathbb{F}_p[X]$ die Polynome $P_1 = X^2 + X + 1$ und $P_2 = X^3 + X^2 + X + 1$. Bestimmen Sie die Lösungsmenge $L \subset \mathbb{F}_p[X]$ des Kongruenzsystems

$$F \equiv X - 1 \pmod{P_1} \quad \text{und} \quad F \equiv 1 \pmod{P_2} \quad F \in \mathbb{F}_p[X].$$

(10 Punkte)

Thema Nr. 3
(Aufgabengruppe)**Aufgabe 1** → S. 536

Sei K ein Körper, V ein endlich dimensionaler K -Vektorraum und $\phi: V \rightarrow V$ ein Endomorphismus von V , dessen charakteristisches Polynom in Linearfaktoren zerfällt. Beweisen Sie, dass die folgenden Bedingungen äquivalent sind:

- a** Alle Eigenräume von ϕ sind eindimensional.
- b** Zu jedem Eigenwert von ϕ existiert in der Jordanschen Normalform genau ein Jordanblock.
- c** Das Minimalpolynom und das charakteristische Polynom von ϕ sind gleich.

(12 Punkte)

Aufgabe 2 → S. 537

Sei $p \geq 3$ eine ungerade Primzahl und \mathbb{F}_{p^2} der Körper mit p^2 Elementen. Beweisen Sie:

- a** Die Abbildung $f: \mathbb{F}_{p^2} \rightarrow \mathbb{F}_{p^2}$, die durch $f(a) = a^p$ gegeben ist, ist ein Isomorphismus von Ringen.
- b** Durch die Vorschrift $g(a) = a + a^p$ ist eine Abbildung $g: \mathbb{F}_{p^2} \rightarrow \mathbb{F}_p$ gegeben, und diese ist ein surjektiver Gruppenhomomorphismus.
- c** Durch die Vorschrift $h(a) = a^{p+1}$ ist eine Abbildung $h: \mathbb{F}_{p^2}^\times \rightarrow \mathbb{F}_p^\times$ gegeben, und diese ist ein surjektiver Gruppenhomomorphismus. (4 + 4 + 4 Punkte)

Aufgabe 3 → S. 538

Es sei G eine Gruppe der Ordnung $|G| = 7^2 \cdot 8$. Mit Syl_7 bezeichnen wir die Menge der 7-Sylowgruppen und mit n_7 die Anzahl der 7-Sylowgruppen von G . Zeigen Sie mithilfe der folgenden Schritte, dass G nicht einfach ist.

- a** Begründen Sie, dass $n_7 \in \{1, 8\}$ gilt.
- b** Begründen Sie, dass G im Fall $n_7 = 1$ nicht einfach ist.
- c** Begründen Sie, dass

$$\cdot: G \times \text{Syl}_7 \rightarrow \text{Syl}_7, \quad (g, P) \mapsto gPg^{-1}$$

eine transitive Operation von G auf Syl_7 ist.

- d** Begründen Sie, dass G auch im Fall $n_7 = 8$ nicht einfach ist.

(2 + 2 + 2 + 6 Punkte)

Aufgabe 4 → S. 539

In einem assoziativen Ring R mit Einselement gelte für jedes Element $x \in R$ entweder $x^2 = 1$ oder $x^n = 0$ für ein $n \geq 1$.

- a** Beweisen Sie, dass die Einheitengruppe von R kommutativ ist.
- b** Beweisen Sie, dass für jedes Element $x \in R$ entweder x oder $1 - x$ eine Einheit ist.
- c** Beweisen Sie, dass R ein kommutativer Ring ist. (3 + 3 + 6 Punkte)

Aufgabe 5 → S. 539

Finden Sie zwei Polynome $f, g \in \mathbb{Q}[x]$ gleichen Grades, sodass $\text{Gal}(f)$ und $\text{Gal}(g)$ gleich viele Elemente haben, aber $\text{Gal}(f)$ abelsch und $\text{Gal}(g)$ nicht abelsch ist.

(12 Punkte)

Lösungen zu Thema Nr. 1

Lösungsvorschlag zur Aufgabe (Herbst 2016, T1A1)

Da N ein Normalteiler ist, ist das Komplexprodukt NH eine Untergruppe von G und N ist insbesondere Normateiler von NH . Nach dem 1. Isomorphismensatz 1.10 (1) ist dann $NH/N \cong H/N \cap H$. Da N laut Angabe auflösbar ist, genügt es nach Satz 1.30 zu zeigen, dass $H/N \cap H$ auflösbar ist. Auch H ist auflösbar, daher können wir Satz 1.30 erneut anwenden (diesmal andersrum) und erhalten, dass der Quotient $H/H \cap N$ auflösbar ist.

Lösungsvorschlag zur Aufgabe (Herbst 2016, T1A2)

Es ist klar, dass die Einheitsmatrix die geforderte Eigenschaft besitzt. Sei also $A \in \mathrm{GL}_k(\mathbb{Q})$ eine weitere Matrix mit $A^k = I_k$. Dann ist A eine Nullstelle des Polynoms $X^p - 1$ und das Minimalpolynom von A muss ein Teiler dieses Polynoms sein. Sei Φ_n jeweils das n -te Kreisteilungspolynom, dann ist

$$X^p - 1 = \Phi_1 \cdot \Phi_p$$

die eindeutige Zerlegung in irreduzible normierte Faktoren. Das Minimalpolynom von A kann jedoch nicht von Φ_p geteilt werden: Als $k \times k$ -Matrix hat das charakteristische Polynom von A Grad k . Laut dem Satz von Cayley-Hamilton ist das Minimalpolynom von A ein Teiler des charakteristischen Polynoms von A , hat also insbesondere maximal Grad k , während hingegen

$$\mathrm{grad} \Phi_p = \varphi(p) = p - 1 > p - 2 \geq k$$

gilt. Damit muss $\Phi_1 = X - 1$ das Minimalpolynom von A sein und wir erhalten

$$\Phi_1(A) = 0 \Leftrightarrow A - I_k = 0 \Leftrightarrow A = I_k.$$

Lösungsvorschlag zur Aufgabe (Herbst 2016, T1A3)

- a) Sei $a \in R$. Wir zeigen per Induktion über n , dass für alle $n \in \mathbb{N}$ aus $a^n = 0$ bereits $a = 0$ folgt. Für $n = 1$ ist die Aussage offensichtlich wahr. Für den Induktionsschritt nehmen wir an, dass $a^{n+1} = 0$ gilt. Es existiert ein $b \in R$, sodass die Gleichung $a^2b = a$ gilt. Daraus erhält man

$$a^n = a^{n-1} \cdot a = a^{n-1}a^2b = a^{n+1}b = 0.$$

Nach Induktionsvoraussetzung folgt daher $a = 0$.

- b** Wir zeigen, dass R/\mathfrak{p} ein Körper ist. Sei $\bar{a} \in R/\mathfrak{p}$ mit $\bar{a} \neq \bar{0}$. Nach Voraussetzung gibt es $b \in R$, sodass die Gleichung $a^2b = a$ in R erfüllt ist. Man erhält daraus in R/\mathfrak{p} :

$$\bar{a}^2 \cdot \bar{b} = \bar{a} \Leftrightarrow \bar{a}(\bar{a}\bar{b} - 1) = \bar{0}$$

Da \mathfrak{p} Primideal ist, ist R/\mathfrak{p} ein Integritätsbereich. Weiter war nach Wahl $\bar{a} \neq 0$, sodass aus der Gleichung oben $\bar{a}\bar{b} - \bar{1} = \bar{0}$ und damit $\bar{a}\bar{b} = \bar{1}$ folgt. Dies bedeutet gerade, dass \bar{a} eine Einheit und somit R/\mathfrak{p} ein Körper ist.

Lösungsvorschlag zur Aufgabe (Herbst 2016, T1A4)

- a** Sei $n \in \mathbb{N}$. Wir zeigen die Aussage per vollständiger Induktion über $m > n$. Den Induktionsanfang müssen wir daher für $m = n + 1$ machen: Es gilt

$$x_{n+1} - 2 = a^{2^{n+1}} - 1 = (a^{2^n} - 1)(a^{2^n} + 1) = (a^{2^n} - 1) \cdot x_n.$$

Dies zeigt, dass $x_{n+1} - 2$ von x_n geteilt wird. Setzen wir die Aussage also für ein m als bereits bewiesen voraus und zeigen die Aussage für $m + 1$: Wir haben

$$x_{m+1} - 2 = a^{2^{m+1}} - 1 = (a^{2^m} - 1)(a^{2^m} + 1) = (x_m - 2) \cdot x_m.$$

Laut Induktionsvoraussetzung ist $x_n \mid (x_m - 2)$ erfüllt, deshalb auch $x_n \mid (x_{m+1} - 2)$.

- b** Sei d ein gemeinsamer Teiler von x_n und x_m . Da laut Teil **a** x_n ein Teiler von $x_m - 2$ ist, muss auch d die Zahl $x_m - 2$ teilen. Insbesondere ist d ein Teiler von

$$2 = x_m - (x_m - 2).$$

Daraus folgt, dass d ein Teiler von 2 sein muss, also $d \in \{1, 2\}$. Ist nun $a \in \mathbb{N}_0$ gerade, so ist x_n ungerade für alle $n \in \mathbb{N}_0$, also ist der größte gemeinsame Teiler in diesem Fall 1. Ist hingegen a ungerade, so ist x_n gerade für alle $n \in \mathbb{N}_0$ und der größte gemeinsame Teiler von x_n und x_m ist 2.

- c** Sei a ungerade. Wähle jeweils einen Primteiler p_n von x_n , dann hat die Folge $(p_n)_{n \in \mathbb{N}}$ paarweise verschiedene Glieder: Angenommen, es gibt $n, m \in \mathbb{N}$ mit $n < m$ und $p_n = p_m$, dann ist p_n ein gemeinsamer Primteiler von x_n und x_m . In **b** haben wir jedoch gesehen, dass x_n und x_m teilerfremd sind.

Wir haben also mit $(p_n)_{n \in \mathbb{N}}$ eine unendliche Folge von Primzahlen konstruiert.

Lösungsvorschlag zur Aufgabe (Herbst 2016, T1A5)

Das Polynom f hat $2n$ Nullstellen, diese sind verschieden (da f separabel ist) und wegen $f(-X) = h((-X)^2) = h(X^2) = f(X)$ ist das Negative jeder Nullstelle jeweils wiederum eine Nullstelle. Wir schreiben die Nullstellen als

$$\alpha_1, \quad \alpha_2 = -\alpha_1, \quad \alpha_3, \quad \dots, \quad \alpha_{2n-1}, \quad \alpha_{2n} = -\alpha_{2n-1}.$$

Laut Satz 3.24 existiert ein injektiver Homomorphismus $\phi: \text{Gal}(f) \rightarrow S_{2n}$, wobei $\text{Gal}(f)$ die Galois-Gruppe (eines Zerfällungskörpers) von f bezeichnet. Nehmen wir an, ϕ ist sogar ein Isomorphismus. Wegen $n \geq 2$ ist $(1\ 3) \in S_{2n}$. Das Urbild $\sigma = \phi^{-1}((1\ 3))$ dieser Transposition ist ein \mathbb{Q} -Automorphismus, der nur α_1 und α_3 vertauscht, also

$$\sigma(\alpha_1) = \alpha_3 \text{ und } \sigma(\alpha_i) = \alpha_i \text{ für } i \in \{2, 4, 5, \dots, 2n\}$$

erfüllt. Ein solches Element kann es jedoch nicht geben: Da σ ein \mathbb{Q} -Automorphismus ist, gilt $\sigma(-1) = -1$. Damit erhalten wir aber

$$\sigma(\alpha_2) = \sigma(-\alpha_1) = -\sigma(\alpha_1) = -\alpha_3 = \alpha_4.$$

Wegen $\sigma(\alpha_2) = \alpha_4 \neq \alpha_2$ ist das ein Widerspruch.

Lösungen zu Thema Nr. 2

Lösungsvorschlag zur Aufgabe (Herbst 2016, T2A1)

- a) Sei $G = \text{SL}_2(\mathbb{R})$. Wir behaupten, dass es nur eine Bahn gibt, die Operation also transitiv ist. Dazu zeigen wir

$$G(i) = H.$$

Die Inklusion „ \subseteq “ ist klar laut Definition der Gruppenoperation. Sei umgekehrt $x + iy \in H$ mit $x \in \mathbb{R}$ und $y \in \mathbb{R}^+$. Wir bestimmen eine Matrix $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathbb{R})$ mit $\varrho(A, i) = x + iy$. Es gilt unter Verwendung von $ad - bc = \det A = 1$

$$\begin{aligned} \varrho(A, i) &= \frac{ai + b}{ci + d} = \frac{(ai + b)(-ci + d)}{(ci + d)(-ci + d)} = \\ &= \frac{(ac + bd) + i(ad - bc)}{c^2 + d^2} = \frac{(ac + bd) + i}{c^2 + d^2}. \end{aligned}$$

Da nur die Existenz solcher Zahlen zu zeigen ist, dürfen wir der Einfachheit halber $c = 0$ setzen. Damit $\text{Im } \varrho(A, i) = y$ gilt, muss $\frac{1}{d^2} = y$ sein, wir wählen also weiter $y = \frac{1}{\sqrt{y}}$. Wegen $\det A = ad = 1$ muss dann $a = \frac{1}{d} = \sqrt{y}$ gelten. Für b erhalten wir zuletzt

$$\frac{ac + bd}{d^2} = x \Leftrightarrow \frac{bd}{d^2} = x \Leftrightarrow b = xd = \frac{x}{\sqrt{y}}.$$

Wir überprüfen dieses Ergebnis. A ist eine Matrix in G , und tatsächlich gilt

$$\varrho\left(\begin{pmatrix} \sqrt{y} & \frac{x}{\sqrt{y}} \\ 0 & \frac{1}{\sqrt{y}} \end{pmatrix}, i\right) = \frac{i\sqrt{y} + \frac{x}{\sqrt{y}}}{\frac{1}{\sqrt{y}}} = x + iy.$$

Insgesamt haben wir für beliebiges $x + iy \in H$ gezeigt, dass $x + iy \in G(i)$ und somit haben wir Gleichheit. Es gibt damit nur eine Bahn, nämlich H .

b Wir zeigen

$$\text{Stab}_G(i) = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a, b \in \mathbb{R}, a^2 + b^2 = 1 \right\}$$

(vgl. die erste Inklusion dazu, wie man darauf kommt).

„ \subseteq “: Sei $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{Stab}_G(i)$. Dann gilt $\varrho(A, i) = i$ und somit

$$\frac{ai + b}{ci + d} = i \Leftrightarrow ai + b = di - c \Leftrightarrow a = d \text{ und } b = -c.$$

Wegen $\det A = 1$ muss zudem $a^2 + b^2 = 1$ erfüllt sein. Damit ist A ein Element der Menge auf der rechten Seite der Gleichung.

„ \supseteq “: Seien $a, b \in \mathbb{R}$ mit $a^2 + b^2 = 1$, dann gilt

$$\varrho\left(\begin{pmatrix} a & b \\ -b & a \end{pmatrix}, i\right) = \frac{ai + b}{-bi + a} = \frac{(ai + b)(a + bi)}{(a - bi)(a + bi)} = \frac{-ab + ab + i(a^2 + b^2)}{a^2 + b^2} = i.$$

Lösungsvorschlag zur Aufgabe (Herbst 2016, T2A2)

a „ \Rightarrow “: Nehmen wir an, dass $A \rtimes_{\phi} B$ abelsch ist. Sei $b \in B$ beliebig und e_A das Neutralelement von A , e_B das von B . Dann gilt für alle $a \in A$

$$(e_A, b) \cdot (a, b) = (a, b) \cdot (e_A, b) \Leftrightarrow (e_A \phi(b)(a), b^2) = (a \phi(b)(e_A), b^2).$$

Da $\phi(b)$ ein Automorphismus ist, gilt $\phi(b)(e_A) = e_A$. Damit liefert Ver-
gleich der ersten Komponente

$$\phi(b)(a) = a$$

für alle $a \in A$, also $\phi(b) = \text{id}_A$.

„ \Leftarrow “: Nehmen wir an, es gilt $\phi(b) = \text{id}_A$ für alle $b \in B$. Dann erhalten wir für beliebiges $(a_1, b_1), (a_2, b_2) \in A \rtimes_\phi B$

$$\begin{aligned} (a_1, b_1) \cdot (a_2, b_2) &= (a_1\phi(b_1)(a_2), b_1b_2) = (a_1a_2, b_1b_2) \stackrel{(*)}{=} \\ &= (a_2a_1, b_2b_1) = (a_2\phi(b_2)(a_1), b_2b_1) = (a_2, b_2) \cdot (a_1, b_1). \end{aligned}$$

Dabei wurde an der Stelle $(*)$ verwendet, dass A und B abelsch sind.
Insgesamt zeigt die Gleichung, dass $A \rtimes_\phi B$ abelsch ist.

- b** Es ist $2015 = 65 \cdot 31$. Wir setzen nun $A = \mathbb{Z}/65\mathbb{Z}$ und $B = \mathbb{Z}/31\mathbb{Z}$. Das Element $\bar{1} \in A$ hat die Ordnung 65. Ferner gilt

$$\text{Aut}(B) \cong (\mathbb{Z}/31\mathbb{Z})^\times \cong \mathbb{Z}/30\mathbb{Z}$$

und da 5 ein Teiler von 30 ist, existiert in $\mathbb{Z}/30\mathbb{Z}$ ein Element der Ordnung 5, und aufgrund der Isomorphismen besitzt auch $\text{Aut}(B)$ ein Element der Ordnung 5, das wir mit ψ bezeichnen. Wegen $5 \mid 65$ gibt es einen Homomorphismus $\phi: A \rightarrow \text{Aut}(B)$ mit $\phi(\bar{1}) = \psi$. Dieser Homomorphismus ist wegen $\text{ord } \phi(\bar{1}) = 5 \neq 1$ nicht trivial. Damit ist laut Teil **a** das Produkt $A \rtimes_\phi B$ eine nicht-abelsche Gruppe, die die Ordnung $|A \times B| = 65 \cdot 31 = 2015$ hat.

Lösungsvorschlag zur Aufgabe (Herbst 2016, T2A3)

- a** Die Matrix liegt in Jordan-Normalform vor. Wäre A diagonalisierbar, müsste sie daher bereits Diagonalgestalt haben, denn die Jordan-Normalform ist bis auf Reihenfolge der Jordanblöcke eindeutig. Aus diesem Grund ist A nicht diagonalisierbar über \mathbb{C} .
- b** Das charakteristische Polynom ist hier $\chi_A = X^2 + 1$ und da dieses über \mathbb{R} nicht in Linearfaktoren zerfällt, ist A *nicht* diagonalisierbar.
- c** Auch hier ist das charakteristische Polynom natürlich $\chi_A = X^2 + \bar{1}$. Jedoch erhalten wir hier die Zerlegung $\chi_A = (X - \bar{2})(X - \bar{3})$, so dass χ_A in Linearfaktoren zerfällt. Ferner ist die geometrische Vielfachheit kleiner oder gleich der algebraischen und größer gleich 1. Da die algebraische Vielfachheit beider Eigenwerte 1 ist, muss auch die geometrische jeweils 1 betragen. Die Matrix ist somit diagonalisierbar.

- d** Das charakteristische Polynom (mit der Variable Y) lautet hier

$$\begin{aligned}\chi_A(Y) &= (X+1-Y)(2X-1-Y) - (X-1) = Y^2 - 3XY + 2X^2 = \\ &= (Y-X)(Y-2X).\end{aligned}$$

Damit hat auch hier χ_A zwei verschiedene, einfache Nullstellen und A ist nach dem gleichen Argument wie in Teil **c** diagonalisierbar.

Lösungsvorschlag zur Aufgabe (Herbst 2016, T2A4)

- a** Da \mathbb{Q} als Körper der Charakteristik 0 perfekt ist, ist die Erweiterung zumindest separabel. Um zu zeigen, dass sie auch normal ist, zeigen wir, dass K der Zerfällungskörper des Polynoms $f = X^p - p \in \mathbb{Q}[X]$ ist. Die p verschiedenen Nullstellen dieses Polynoms sind gegeben durch $\zeta_p^k \alpha_p$ mit $k \in \{1, \dots, p\}$. Alle diese Nullstellen liegen in K , ferner wird K bereits von den Nullstellen α_p und $\zeta_p \alpha_p$ erzeugt. Damit ist K tatsächlich der Zerfällungskörper von f und die Erweiterung ist normal.
- b** Zunächst ist f irreduzibel aufgrund des Eisenstein-Kriteriums, hat α_p als Nullstelle und ist normiert, also das Minimalpolynom von α_p . Damit ist $[\mathbb{Q}(\alpha_p) : \mathbb{Q}] = \text{grad } f = p$.

Das Minimalpolynom von ζ_p über \mathbb{Q} ist das p -te Kreisteilungspolynom Φ_p , welches $\text{Grad } \varphi(p) = p-1$ hat. ζ_p als Nullstelle. Aus diesem Grund ist $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p-1$.

Aufgrund der Gradformel haben wir

$$[K : \mathbb{Q}] = [K : \mathbb{Q}(\alpha_p)] \cdot [\mathbb{Q}(\alpha_p) : \mathbb{Q}] = [K : \mathbb{Q}(\zeta_p)] \cdot [\mathbb{Q}(\zeta_p) : \mathbb{Q}],$$

also ist $[K : \mathbb{Q}]$ ein Vielfaches von p und $p-1$. Wegen $p > 2$ sind diese beiden Zahlen teilerfremd, sodass wir $[K : \mathbb{Q}] \geq p(p-1)$ erhalten. Andererseits ist Φ_p auch ein Polynom aus $\mathbb{Q}(\alpha_p)[X]$ mit $\Phi_p(\zeta_p) = 0$, also hat das Minimalpolynom von ζ_p über $\mathbb{Q}(\alpha_p)$ maximal den Grad $p-1$. Deshalb gilt

$$[K : \mathbb{Q}] = [K : \mathbb{Q}(\alpha_p)] \cdot [\mathbb{Q}(\alpha_p) : \mathbb{Q}] \leq p(p-1).$$

Insgesamt haben wir $[K : \mathbb{Q}] = p(p-1)$ gezeigt.

- c** Wir haben bereits gesehen, dass f irreduzibel ist und eine Nullstelle in $\mathbb{Q}(\alpha_p)$ hat. Wäre die Erweiterung normal, so müssen bereits alle Nullstellen in $\mathbb{Q}(\alpha_p)$ liegen. Tatsächlich ist aber beispielsweise die Nullstelle $\zeta_p \alpha_p \in \mathbb{C} \setminus \mathbb{R}$, während $\mathbb{Q}(\alpha_p) \subseteq \mathbb{R}$ gilt. Damit zerfällt f über $\mathbb{Q}(\alpha_p)$ nicht in Linearfaktoren und die Erweiterung ist nicht normal.

Angenommen, $\text{Gal}(K|\mathbb{Q})$ wäre abelsch. Dann wäre jede Untergruppe ein Normalteiler, insbesondere die Untergruppe $\text{Gal}(K|\mathbb{Q}(\alpha_p))$. Deren zugehöriger Fixkörper ist $\mathbb{Q}(\alpha_p)$. Laut dem Hauptsatz der Galois-Theorie wäre damit die Erweiterung $\mathbb{Q}(\alpha_p)|\mathbb{Q}$ normal – Widerspruch zum ersten Teil der Aufgabe.

- d**
1. *Möglichkeit:* Die Gruppe $\text{Gal}(K|\mathbb{Q})$ hat Ordnung $p(p-1)$. Eine Untergruppe der Ordnung p ist damit eine p -Sylowgruppe. Sei deren Anzahl ν_p . Wir erhalten mit dem Dritten Sylowsatz $\nu_p \equiv 1 \pmod{p}$, also $\nu_p = 1 + kp$ für ein $k \in \mathbb{N}_0$. Zugleich muss aber wegen $\nu_p \mid p-1$ auch $\nu_p < p$ gelten, weshalb wir $k=0$ und somit $\nu_p = 1$ folgern können. Da es nur eine einzige p -Sylowgruppe gibt, ist diese ein Normalteiler.
 2. *Möglichkeit:* Die Erweiterung $\mathbb{Q}(\zeta_p)|\mathbb{Q}$ ist eine Erweiterung vom Grad $p-1$ und ist als zyklotomische Erweiterung normal, sodass die korrespondierende Untergruppe $U = \text{Gal}(K|\mathbb{Q}(\zeta_p))$ ein Normalteiler von $\text{Gal}(K|\mathbb{Q})$ ist. Die Ordnung von U berechnet sich nach dem Zusatz zum Hauptsatz der Galois-Theorie zu

$$|U| = [K : \mathbb{Q}(\zeta_p)] = \frac{[K : \mathbb{Q}]}{[\mathbb{Q}(\zeta_p) : \mathbb{Q}]} = \frac{p(p-1)}{p-1} = p.$$

Lösungsvorschlag zur Aufgabe (Herbst 2016, T2A5)

Wegen

$$P_2 - XP_1 = X^3 + X^2 + X + 1 - X^3 - X^2 - X = 1$$

sind die beiden angegebenen Polynome teilerfremd. Nach dem Chinesischen Restsatz haben wir einen Isomorphismus

$$\begin{aligned}\phi: \mathbb{F}_p[X]/(P_1P_2) &\rightarrow \mathbb{F}_p[X]/(P_1) \times \mathbb{F}_p[X]/(P_2), \\ f + (P_1P_2) &\mapsto (f + (P_1), f + (P_2)).\end{aligned}$$

und die Lösungsmenge der angegebenen Kongruenz ist das Urbild von $(X-1, 1)$ unter ϕ . Mit der Relation von oben erhalten wir

$$\begin{aligned}\phi(1 + XP_1 + (P_1P_2)) &= (1 + P_1, 0 + P_2) \quad \text{und} \\ \phi(1 - P_2 + (P_1P_2)) &= (0 + P_1, 1 + P_2).\end{aligned}$$

Damit ist

$$\phi((X-1)(1+XP_1) + (1-P_2)) = (X-1, 1).$$

Wir berechnen:

$$\begin{aligned}
 (X - 1)(1 + XP_1) + (1 - P_2) &= \\
 &= (X - 1)(X^3 + X^2 + X + 1) + (-X^3 - X^2 - X) = \\
 &= X^4 + X^3 + X^2 + X - X^3 - X^2 - X - 1 - X^3 - X^2 - X = \\
 &= X^4 - X^3 - X^2 - X - 1
 \end{aligned}$$

Die Lösungsmenge des obigen Kongruenzsystems ist somit

$$\mathcal{L} = X^4 - X^3 - X^2 - X - 1 + (P_1P_2).$$

Lösungen zu Thema Nr. 3

Lösungsvorschlag zur Aufgabe (Herbst 2016, T3A1)

„**a** \Leftrightarrow **b**“: Folgt aus Proposition 4.10 (1).

„**b** \Rightarrow **c**“: Seien $\lambda_1, \dots, \lambda_m$ die Eigenwerte von ϕ und schreibe das Minimalpolynom von ϕ als $\mu = \prod_{i=1}^m (X - \lambda_i)^{v_i}$ mit $v_i \in \mathbb{N}$. Laut Proposition 4.10 (2) ist v_i jeweils die Größe des größten Jordanblocks zum Eigenwert λ_i . Nach (2) gibt es nur jeweils einen Jordanblock, dieser ist dann insbesondere der größte zum jeweiligen Eigenwert, d. h. es gibt genau einen Jordanblock der Größe v_i zum Eigenwert λ_i . Die Jordanblöcke müssen zusammen die Darstellungsmatrix von ϕ ausfüllen, d. h. ihre gesamte Breite muss

$$\sum_{i=1}^m v_i = \dim_K V$$

betragen. Daraus folgt $\text{grad } \mu = \dim_K V$. Da dies genau der Grad des charakteristischen Polynoms χ von ϕ ist, beide normiert sind und laut dem Satz von Cayley-Hamilton 4.6 außerdem $\mu \mid \chi$ gilt, folgt bereits $\mu = \chi$.

„**c** \Rightarrow **b**“: Aus $\mu = \chi$ folgt insbesondere $\text{grad } \mu = \text{grad } \chi$. Wegen $\text{grad } \chi = \dim_K V$ gilt daher $\sum_{i=1}^m v_i = \dim_K V$, wobei $\mu = \prod_{i=1}^m (X - \lambda_i)^{v_i}$ wie zuvor. Das bedeutet: Nimmt man nur die jeweils größten Jordanblöcke zu jedem Eigenwert, so füllen diese bereits die gesamte Breite der Darstellungsmatrix von ϕ . Es kann daher nur zu jedem Eigenwert genau einen Jordanblock geben.

Lösungsvorschlag zur Aufgabe (Herbst 2016, T3A2)

- a** Es gilt natürlich $f(1) = 1$. Seien nun $a, b \in \mathbb{F}_{p^2}$. Dann gilt

$$\begin{aligned} f(ab) &= (ab)^p = a^p b^p = f(a)f(b), \\ f(a+b) &= (a+b)^p = a^p + b^p = f(a) + f(b). \end{aligned}$$

Dabei folgt die zweite Gleichung durch Anwendung des *freshman's dream*, da \mathbb{F}_{p^2} Charakteristik p hat. Damit ist f ein Körper-Homomorphismus und als solcher injektiv. Als injektiver Homomorphismus zwischen endlichen, gleichmächtigen Mengen ist f bijektiv.

- b** Wir zeigen zunächst, dass g wohldefiniert ist, dass also $g(a) \in \mathbb{F}_p$ für alle $a \in \mathbb{F}_{p^2}$ gilt. Ist $a \in \mathbb{F}_{p^2}$, so gilt $a^{p^2} = a$ und somit

$$g(a)^p = (a + a^p)^p = a^p + a^{p^2} = a^p + a = g(a).$$

Damit ist $g(a)$ eine Nullstelle von $X^p - X$, woraus $g(a) \in \mathbb{F}_p$ folgt. Für $a, b \in \mathbb{F}_{p^2}$ gilt unter Verwendung des *freshman's dream*

$$g(a+b) = (a+b) + (a+b)^p = a + a^p + b + b^p = g(a) + g(b),$$

sodass g ein Gruppenhomomorphismus ist. Zum Nachweis der Surjektivität betrachte, dass für $a \in \mathbb{F}_p$ gilt

$$g(a) = a + a^p = 2a.$$

Wegen $p \geq 3$ ist $2 \neq 0$, also ist 2 invertierbar und wir erhalten für beliebiges $a \in \mathbb{F}_p$

$$a = 2 \cdot 2^{-1}a = g(2^{-1}a).$$

- c** Für $a \in \mathbb{F}_{p^2}^\times$ gilt

$$h(a)^p = (a^{p+1})^p = a^{p^2+p} = a^{p^2}a^p = aa^p = a^{p+1} = h(a)$$

und somit wie oben $h(a) \in \mathbb{F}_p$. Wäre $h(a) = 0$, so wäre $a = 0$ im Widerspruch zu $a \in \mathbb{F}_{p^2}^\times$. Somit ist $h(a) \in \mathbb{F}_p^\times$. Die Rechnung

$$h(ab) = (ab)^{p+1} = a^{p+1}b^{p+1} = h(a)h(b)$$

für $a, b \in \mathbb{F}_{p^2}^\times$ zeigt, dass h ein Gruppenhomomorphismus ist. Zum Nachweis der Surjektivität sei $a \in \mathbb{F}_p^\times$ vorgegeben. Wir suchen dann ein $b \in \mathbb{F}_{p^2}^\times$

mit $h(b) = a$, d.h. mit $b^{p+1} = a$. Elemente mit dieser Eigenschaft sind genau die Nullstellen des Polynoms $X^{p+1} - a \in \mathbb{F}_p[X]$. Sei daher $c \in \overline{\mathbb{F}_p}$ eine Nullstelle dieses Polynoms in einem algebraischen Abschluss $\overline{\mathbb{F}_p}$ von \mathbb{F}_p . Wegen

$$c^{p^2-1} = (c^{p+1})^{p-1} = a^{p-1} = 1$$

ist c Nullstelle von $X^{p^2-1} - 1$. Die Nullstellen dieses Polynoms sind wiederum genau die Elemente von $\mathbb{F}_{p^2}^\times$. Also liegt c in $\mathbb{F}_{p^2}^\times$.

Lösungsvorschlag zur Aufgabe (Herbst 2016, T3A3)

- a** Der Dritte Sylowsatz liefert sofort

$$n_7 \mid 8 \quad \Rightarrow \quad n_7 \in \{1, 2, 4, 8\}$$

und wegen $2 \not\equiv 1 \pmod{7}$ und $4 \not\equiv 1 \pmod{7}$ folgt $n_7 \in \{1, 8\}$.

- b** Ist $n_7 = 1$, so existiert nur eine 7-Sylowgruppe. Diese ist dann ein Normalteiler der Ordnung 7^2 und wegen $1 < 7^2 < |G|$ ist diese nicht trivial.

- c** Da Konjugation mit einem Element einen Automorphismus von G definiert, gilt $|gPg^{-1}| = |P|$ für beliebige $g \in G, P \in \text{Syl}_7$. Damit ist $g \cdot P$ wiederum eine 7-Sylowgruppe, die Abbildung ist also wohldefiniert. Zudem gilt für $P \in \text{Syl}_7, g \in G$, dass

$$e \cdot P = ePe^{-1} = P,$$

$$(gh) \cdot P = (gh)P(gh)^{-1} = ghPh^{-1}g^{-1} = g \cdot (hPh^{-1}) = g \cdot h \cdot P.$$

Laut dem Zweiten Sylowsatz sind zudem je zwei Sylowgruppen zueinander konjugiert. Sind also $P, P' \in \text{Syl}_7$, so gibt es ein $g \in G$ mit $P' = gPg^{-1}$, und damit liegen P' und P in derselben Bahn – die Operation ist also transitiv.

- d** Nehmen wir $n_7 = |\text{Syl}_7| = 8$ an. Die Operation liefert uns nach Proposition 1.15 einen Homomorphismus

$$\phi: G \rightarrow \text{Per}(\text{Syl}_7) \cong S_8, \quad g \mapsto \tau_g \quad \text{mit} \quad \tau_g(P) = gPg^{-1}.$$

Wir zeigen, dass der Kern dieses Homomorphismus ein nicht-trivialer Normalteiler von G ist. Nehmen wir zunächst widerspruchshalber an, dass $\ker \phi = \{e\}$. Dann wäre ϕ injektiv. Der Homomorphismus $\phi: G \rightarrow \phi(G) \subseteq \text{Per}(\text{Syl}_7)$ wäre damit ein Isomorphismus und G isomorph zu

einer Untergruppe von $\text{Per}(\text{Syl}_7)$. Das ist wegen $7^2 \cdot 8 \nmid 8!$ jedoch ein Widerspruch zum Satz von Lagrange.

Nehmen wir nun an, dass $\ker \phi = G$. Dann wäre $\phi(g) = \text{id}_{\text{Per}(\text{Syl}_7)}$ für alle $g \in G$ und damit $\tau_g(P) = P$, also $gPg^{-1} = P$ für alle $g \in G$ und $P \in \text{Syl}_7$. Damit müsste aber P ein Normalteiler von G sein - was wegen $n_7 \neq 1$ ausgeschlossen ist.

Insgesamt ist $\ker \phi$ ein Normalteiler von G , der nicht-trivial ist, und G ist nicht einfach.

Lösungsvorschlag zur Aufgabe (Herbst 2016, T3A4)

- a** Sei $r \in R^\times$. Gäbe es $n \in \mathbb{N}$, sodass $r^n = 0$, so wäre $1 = r^{-n} \cdot r^n = 0$. Widerspruch. Also gilt $r^2 = 1$ und somit $r^{-1} = r$ für alle $r \in R^\times$.

Seien nun $x, y \in R^\times$. Dann gilt:

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

- b** Nehmen wir an, dass x keine Einheit ist. Dann muss $x^n = 0$ für ein $n \geq 1$ sein, denn im Fall $x^2 = 1$ wäre x eine Einheit. Die geometrische Reihe liefert nun

$$1 + x + \dots + x^{n-1} = \frac{1 - x^n}{1 - x} = \frac{1}{1 - x}.$$

Insbesondere ist $1 - x$ eine Einheit.

- c** Seien $x, y \in R$. Sind x und y beides Einheiten, so vertauschen diese nach Teil **a**. Nehmen wir also an, dass o. B. d. A. das Element y keine Einheit ist. Nach Teil **b** ist dann $1 - y$ eine Einheit. Unter Verwendung von Teil **a** gilt also

$$x(1 - y) = (1 - y)x \Leftrightarrow x - xy = x - yx \Leftrightarrow xy = yx.$$

Lösungsvorschlag zur Aufgabe (Herbst 2016, T3A5)

Vorüberlegung: Erst bei Ordnung 6 finden wir mit S_3 überhaupt eine nicht-abelsche Gruppe. Aus anderen Aufgaben weiß man vielleicht noch, dass ein Polynom dritten Grades, das nur eine reelle Nullstelle hat, diese Galois-Gruppe hat. Ein Polynom, dass eine abelsche Galois-Gruppe hat, ist das siebte Kreisteilungspolynom mit Grad 6. Beachte nun noch, dass beide Polynome gleichen Grad haben sollen, aber *nicht* irreduzibel sein müssen.

Definiere zunächst $f = (X^3 + 3X + 3)^2$, dann ist f ein Polynom von Grad 6. Die Nullstellen von f stimmen mit denen von $\bar{f} = X^3 + 3X + 3$ überein, sodass diese den gleichen Zerfällungskörper und die gleiche Galois-Gruppe besitzen. Nun hat \bar{f} genau eine reelle Nullstelle, denn wegen $\bar{f}(-1) = -1$ und $\bar{f}(0) = 3$ existiert laut dem Zwischenwertsatz ein $\alpha \in]-1, 0[$ mit $\bar{f}(\alpha) = 0$. Hätte \bar{f} eine weitere reelle Nullstelle, so müsste zwischen dieser und α laut dem Satz von Rolle eine Nullstelle der ersten Ableitung \bar{f}' liegen. Dies ist wegen $\bar{f}' = 3X^2 + 3$ unmöglich, da die Ableitung keine reellen Nullstellen besitzt. Damit ist α die einzige reelle Nullstelle, die anderen beiden Nullstellen bilden ein komplex-konjugiertes Paar $\beta, \bar{\beta} \in \mathbb{C} \setminus \mathbb{R}$.

Nun wissen wir, dass die Galois-Gruppe von \bar{f} isomorph zu einer Untergruppe von S_3 ist. Ihre Ordnung entspricht dem Erweiterungsgrad des Zerfällungskörpers von f über \mathbb{Q} . Das Polynom \bar{f} ist laut dem Eisensteinkriterium 2.25 mit $p = 3$, normiert und damit wegen $\bar{f}(\alpha) = 0$ das Minimalpolynom von α , sodass die Ordnung von $\text{Gal}(\bar{f})$ Vielfaches von 3, also 3 oder 6 ist. Im Ersteren Fall wäre $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$ bereits der Zerfällungskörper von \bar{f} , was wegen $\beta \in \mathbb{C} \setminus \mathbb{R}$ nicht möglich ist. Daher haben wir

$$\text{Gal}(f) = \text{Gal}(\bar{f}) \cong S_3.$$

Betrachten wir nun das siebte Kreisteilungspolynom $g = \Phi_7$ mit $\text{grad } g = \varphi(7) = 6$. Die Nullstellen von g sind gegeben durch ζ_7^k für $k \in \{1, \dots, 7\}$ und $\zeta = e^{2\pi i/7}$. Ferner wissen wir $\text{Gal}(g) \cong \mathbb{Z}/6\mathbb{Z}$ aus Satz 3.18. Damit ist $\text{Gal}(g)$ zyklisch, also insbesondere abelsch.

Prüfungstermin: Frühjahr 2017

Thema Nr. 1 (Aufgabengruppe)

Aufgabe 1 → S. 545

Sei $L|\mathbb{Q}$ eine endliche Galois'sche Körpererweiterung. Die Norm eines Elements $x \in L$ sei gegeben als

$$N(x) = \prod_{\sigma \in G_{L|\mathbb{Q}}} \sigma(x).$$

- a** Zeigen Sie, dass $N(x) \in \mathbb{Q}$ für alle $x \in L$ und $N(xy) = N(x) \cdot N(y)$ für alle $x, y \in L$.
- b** Sei speziell $L = \mathbb{Q}[\sqrt{5}]$. Zeigen Sie, dass $N(r + s\sqrt{5}) = r^2 - 5s^2$ für $r, s \in \mathbb{Q}$.
- c** Betrachten Sie in L den Teilring $\mathbb{Z}[\sqrt{5}] = \{r + s\sqrt{5} \mid r, s \in \mathbb{Z}\}$. Zeigen Sie, dass für $x \in \mathbb{Z}[\sqrt{5}]$ gilt, dass x genau dann eine Einheit in $\mathbb{Z}[\sqrt{5}]$ ist, wenn $N(x) \in \{\pm 1\}$ gilt.
- d** Zeigen Sie, dass 11 kein Primelement in $\mathbb{Z}[\sqrt{5}]$ ist. (12 Punkte)

Aufgabe 2 → S. 546

Betrachten Sie die Körpererweiterung $L = \mathbb{Q}(\sqrt{2}, \sqrt{2+\sqrt{3}}) \subseteq \mathbb{C}$. Sei $\alpha = \sqrt{2+\sqrt{3}} \in L$.

- a** Zeigen Sie, dass $\alpha - \sqrt{2-\sqrt{3}} = \sqrt{2}$ gilt.
- b** Bestimmen Sie das Minimalpolynom von α über \mathbb{Q} .
- c** Bestimmen Sie das Minimalpolynom von α über $\mathbb{Q}(\sqrt{2})$.
- d** Bestimmen Sie $G_{L|\mathbb{Q}}$. (12 Punkte)

Aufgabe 3 → S. 548

Zeigen Sie, dass es keine einfache Gruppe der Ordnung 300 gibt.

Hinweis Nehmen Sie an, es gäbe so eine Gruppe und lassen Sie diese auf ihren 5-Sylowgruppen operieren. (12 Punkte)

Aufgabe 4 → S. 549

Sei $N \in \mathbb{N}$ eine natürliche Zahl $N \geq 3$.

- a** Zeigen Sie: Gilt $2^{N-1} \not\equiv 1 \pmod{N}$, ist N keine Primzahl.
- b** Zeigen Sie, dass die Umkehrung der Aussage nicht gilt, indem Sie das Beispiel $N = 341 = 11 \cdot 31$ betrachten. (12 Punkte)

Aufgabe 5 → S. 549

Es seien p eine Primzahl, $\overline{\mathbb{F}_p}$ ein algebraischer Abschluss des endlichen Körpers \mathbb{F}_p mit p Elementen. Für $r \in \mathbb{N}$ bezeichne $\mathbb{F}_{p^r} \subseteq \overline{\mathbb{F}_p}$ den Zwischenkörper mit p^r Elementen. Zeigen Sie

- a** Ist $n \in \mathbb{N}$ und A eine $(n \times n)$ -Matrix mit Koeffizienten in \mathbb{F}_p , sodass das charakteristische Polynom χ_A von A irreduzibel über \mathbb{F}_p ist, so ist A über dem Körper \mathbb{F}_{p^n} diagonalisierbar.
- b** Für $p = 5$ ist die Matrix

$$A = \begin{pmatrix} -1 & 3 & -1 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

nicht über \mathbb{F}_{125} diagonalisierbar, aber über \mathbb{F}_{25} . (12 Punkte)

Thema Nr. 2 (Aufgabengruppe)

Aufgabe 1 → S. 550

Wie viele Elemente der Ordnung 11 gibt es in einer einfachen Gruppe der Ordnung 660? (12 Punkte)

Aufgabe 2 → S. 551

- a** Sei G eine multiplikativ geschriebene Gruppe der Ordnung n und $g \in G$. Weiter gelte $g^{n/p} \neq 1$ für jeden Primteiler p von n gilt. Zeigen Sie: g erzeugt G .
- b** Zeigen Sie: $4^{3^m} \equiv 1 + 3^{m+1} \pmod{3^{m+2}}$ für alle $m \geq 0$.
- c** Zeigen Sie, dass die Restklasse von 2 für jedes $e \geq 1$ die Einheitengruppe des Rings $\mathbb{Z}/3^e\mathbb{Z}$ erzeugt. (12 Punkte)

Aufgabe 3 → S. 552

Sei K ein endlicher Körper mit seiner multiplikativen Gruppe (K^\times, \cdot) und sei weiter $H := \{a^2 \mid a \in K^\times\}$. Zeigen Sie:

- a** H ist eine Untergruppe von (K^\times, \cdot) ,
- b** $H = K^\times$, falls $\text{char } K = 2$,
- c** H hat Index 2 in K^\times , falls $\text{char } K > 2$.

(12 Punkte)

Aufgabe 4 → S. 553

Sei $f = X^3 + 2X + 2 \in \mathbb{Q}[X]$ und sei $\alpha \in \mathbb{C}$ eine Nullstelle von f .

- a** Zeigen Sie: $\{1, \alpha, \alpha^2\}$ eine Basis des \mathbb{Q} -Vektorraums $\mathbb{Q}(\alpha)$ ist.
- b** Schreiben Sie $(\alpha + 1)^{-1}$ als Linearkombination mit rationalen Koeffizienten bezüglich dieser Basis. (12 Punkte)

Aufgabe 5 → S. 554

Sei $K|\mathbb{Q}$ eine Galois-Erweiterung vom Grad 55 mit nicht-abelscher Galois-Gruppe. Zeigen Sie: Es gibt genau einen echten Zwischenkörper L von $K|\mathbb{Q}$, sodass $L|\mathbb{Q}$ eine Galois-Erweiterung ist. Bestimmen Sie $[L : \mathbb{Q}]$. (12 Punkte)

Thema Nr. 3
(Aufgabengruppe)**Aufgabe 1** → S. 555

Sei K ein Körper der Charakteristik $p > 0$ und sei

$$G = \text{SL}_n(K) = \{A \in \text{Mat}(n \times n, K) \mid \det A = 1\}$$

die Gruppe der invertierbaren $(n \times n)$ -Matrizen mit Einträgen aus K und Determinante 1. Wir betrachten die Abbildung

$$F: \text{Mat}(n \times n, K) \rightarrow \text{Mat}(n \times n, K), \quad F((a_{ij})) = (a_{ij}^p).$$

Zeigen Sie $F(G) \subseteq G$ und dass $F|_G: G \rightarrow G$ ein Homomorphismus von Gruppen ist. Folgern Sie daraus, dass $H = \{g \in G \mid F(g) = g\}$ eine Untergruppe von G ist, und bestimmen Sie diese Untergruppe. (12 Punkte)

Aufgabe 2 → S. 556

Man zeige:

- a** S_5 hat genau sechs 5-Sylowuntergruppen.
- b** S_6 hat eine zu S_5 isomorphe und transitiv auf $\{1, 2, 3, 4, 5, 6\}$ operierende Untergruppe.
- c** S_6 hat zwei zu S_5 isomorphe Untergruppen, die nicht zueinander konjugiert sind. (12 Punkte)

Aufgabe 3 → S. 558

Sei $R = \mathbb{Z}[\sqrt{-3}]$ und $S = \mathbb{Z}[i] = \mathbb{Z}[\sqrt{-1}]$. Man zeige, dass es keinen Ringhomomorphismus $\phi: R \rightarrow S$ gibt.

Hinweis Ringhomomorphismen $R \rightarrow S$ bilden definitionsgemäß 1_R auf 1_S ab.
(12 Punkte)

Aufgabe 4 → S. 558

Sei K ein Körper, $n \geq 1$ und $\mu_A(X) \in K[X]$ das Minimalpolynom einer Matrix $A \in \text{Mat}(n \times n, K)$. Sei $f(X) \in K[X]$ ein Polynom, das zu $\mu_A(X)$ teilerfremd ist. Man zeige, dass die Matrix $f(A)$ invertierbar ist. (12 Punkte)

Aufgabe 5 → S. 559

Sei K ein endlicher Körper mit q Elementen. Man zeige, dass das Polynom $X^2 + X + 1$ genau dann irreduzibel über K ist, wenn $q \equiv -1 \pmod{3}$. (12 Punkte)

Lösungen zu Thema Nr. 1

Lösungsvorschlag zur Aufgabe (Frühjahr 2017, T1A1)

- a** Sei $\tau \in G_{L|\mathbb{Q}}$, dann ist $\tau G_{L|\mathbb{Q}} = G_{L|\mathbb{Q}}$ und es gilt für jedes $x \in L$, dass

$$\begin{aligned}\tau(N(x)) &= \tau\left(\prod_{\sigma \in G_{L|\mathbb{Q}}} \sigma(x)\right) = \prod_{\sigma \in G_{L|\mathbb{Q}}} \tau(\sigma(x)) = \\ &= \prod_{\sigma \in \tau G_{L|\mathbb{Q}}} \sigma(x) = \prod_{\sigma \in G_{L|\mathbb{Q}}} \sigma(x) = N(x).\end{aligned}$$

Da τ beliebig aus $G_{L|\mathbb{Q}}$ war, wird $N(x)$ von der gesamten Gruppe $G_{L|\mathbb{Q}}$ fixiert, d.h. $N(x)$ liegt im Fixkörper $L^{G_{L|\mathbb{Q}}} = \mathbb{Q}$. Sei zusätzlich $y \in L$, dann gilt

$$\begin{aligned}N(xy) &= \prod_{\sigma \in G_{L|\mathbb{Q}}} \sigma(xy) = \prod_{\sigma \in G_{L|\mathbb{Q}}} \sigma(x) \cdot \sigma(y) = \\ &= \left(\prod_{\sigma \in G_{L|\mathbb{Q}}} \sigma(x) \right) \cdot \left(\prod_{\sigma \in G_{L|\mathbb{Q}}} \sigma(y) \right) = N(x) \cdot N(y).\end{aligned}$$

- b** Das Minimalpolynom von $\sqrt{5}$ über \mathbb{Q} ist $f = X^2 - 5$, denn dieses Polynom ist normiert, irreduzibel nach Eisenstein und hat $\sqrt{5}$ als Nullstelle. Daraus folgt

$$|G_{L|\mathbb{Q}}| = [L : \mathbb{Q}] = \text{grad } f = 2$$

sowie, dass $\{1, \sqrt{5}\}$ eine \mathbb{Q} -Basis von L ist. Jedes Element in L hat also eine Darstellung als $r + s\sqrt{5}$ für gewisse $r, s \in \mathbb{Q}$. Sei $G_{L|\mathbb{Q}} = \{\text{id}_L, \sigma\}$. Da ein \mathbb{Q} -Automorphismus eine Nullstelle von f wieder auf eine Nullstelle von f abbilden muss, muss $\sigma(\sqrt{5}) \in \{\pm\sqrt{5}\}$ gelten. Da $\{1, \sqrt{5}\}$ eine \mathbb{Q} -Basis von L ist, wird σ durch das Bild $\sigma(\sqrt{5})$ bereits eindeutig bestimmt. Im Fall $\sigma \neq \text{id}_L$ muss daher $\sigma(\sqrt{5}) = -\sqrt{5}$ sein. Damit haben wir:

$$\begin{aligned}N(r + s\sqrt{5}) &= \prod_{\tau \in G_{L|\mathbb{Q}}} \tau(r + s\sqrt{5}) = \text{id}_L(r + s\sqrt{5}) \cdot \sigma(r + s\sqrt{5}) = \\ &= (r + s\sqrt{5})(r - s\sqrt{5}) = r^2 - 5s^2.\end{aligned}$$

- c** „ \Rightarrow “ : Sei $x \in \mathbb{Z}[\sqrt{5}]^\times$, dann gibt es ein $y \in \mathbb{Z}[\sqrt{5}]$ mit $xy = 1$ und man berechnet

$$1 \stackrel{\text{b}}{=} N(1) = N(xy) \stackrel{\text{a}}{=} N(x) \cdot N(y).$$

Da $x = r + s\sqrt{5}$ mit $r, s \in \mathbb{Z}$, ist $N(x) = r^2 - 5s^2$ eine ganze Zahl. Also zeigt obige Gleichung, dass $N(x) \in \mathbb{Z}^\times = \{\pm 1\}$.

„ \Leftarrow “: Sei umgekehrt $N(x) \in \{\pm 1\}$ für $x = r + s\sqrt{5} \in \mathbb{Z}[\sqrt{5}]$ vorausgesetzt, dann folgt aus

$$\pm 1 = N(x) = (r + s\sqrt{5})(r - s\sqrt{5}),$$

dass $y = \pm(r - s\sqrt{5})$ ein multiplikatives Inverses von x in $\mathbb{Z}[\sqrt{5}]$ hat. Insbesondere gilt $x \in \mathbb{Z}[\sqrt{5}]^\times$.

d Wäre 11 ein Primelement in $\mathbb{Z}[\sqrt{5}]$, so würde aus der Gleichung

$$11 = 16 - 5 = (4 + \sqrt{5}) \cdot (4 - \sqrt{5})$$

folgen, dass 11 ein Teiler von $(4 + \sqrt{5})$ oder $(4 - \sqrt{5})$ ist. Gäbe es allerdings ein $x \in \mathbb{Z}[\sqrt{5}]$ mit $11x = 4 \pm \sqrt{5}$, so liefert Anwenden der Norm:

$$11 = N(4 \pm \sqrt{5}) = N(11x) = N(11) \cdot N(x) = 11^2 \cdot N(x) \Leftrightarrow N(x) = \frac{1}{11}$$

Dies widerspricht jedoch $N(x) \in \mathbb{Z}$. Also kann 11 kein Primelement in $\mathbb{Z}[\sqrt{5}]$ sein.

Lösungsvorschlag zur Aufgabe (Frühjahr 2017, T1A2)

a Wir berechnen zunächst:

$$\begin{aligned} \left(\alpha - \sqrt{2 - \sqrt{3}}\right)^2 &= \alpha^2 - 2\alpha\sqrt{2 - \sqrt{3}} + (2 - \sqrt{3}) = \\ &= (2 + \sqrt{3}) - 2\sqrt{(2 + \sqrt{3})(2 - \sqrt{3})} + (2 - \sqrt{3}) = \\ &= -2 \cdot \sqrt{1 + 4} = 2 \end{aligned}$$

Aus der Rechnung folgt $\alpha - \sqrt{2 - \sqrt{3}} \in \{\pm\sqrt{2}\}$. Wegen

$$\sqrt{2 - \sqrt{3}} < \sqrt{2 + \sqrt{3}} \Leftrightarrow 0 < \sqrt{2 + \sqrt{3}} - \sqrt{2 - \sqrt{3}}$$

ist $\alpha - \sqrt{2 + \sqrt{3}} = \sqrt{2}$.

b Wir rechnen wieder:

$$\alpha^2 = 2 + \sqrt{3} \Rightarrow (\alpha^2 - 2)^2 = 3 \Leftrightarrow \alpha^4 - 4\alpha^2 + 1 = 0$$

Somit ist $f = X^4 - 4X^2 + 1$ unser Kandidat für das Minimalpolynom von α über \mathbb{Q} . Sei g das Minimalpolynom, dann folgt aus $f(\alpha) = 0$ schon mal $g \mid f$ und damit $\deg g \leq 4$. Wir zeigen nun $\deg g = 4$, indem wir $[\mathbb{Q}(\alpha) : \mathbb{Q}] \geq 4$ nachweisen. Es sind dann nämlich f und g normierte Polynome gleichen Grades, sodass aus $g \mid f$ bereits $g = f$ folgt.

Bemerke zunächst

$$\begin{aligned}\alpha \cdot \sqrt{2 - \sqrt{3}} &= 1 \quad \Rightarrow \quad \sqrt{2 - \sqrt{3}} = \alpha^{-1} \in \mathbb{Q}(\alpha) \\ \alpha^2 &= 2 + \sqrt{3} \quad \Rightarrow \quad \sqrt{3} = \alpha^2 - 2 \in \mathbb{Q}(\alpha).\end{aligned}$$

Aus Teil **a** folgt außerdem $\sqrt{2} \in \mathbb{Q}(\alpha)$. Wir haben somit $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\alpha)$ und $\mathbb{Q}(\sqrt{3}) \subseteq \mathbb{Q}(\alpha)$. Wegen $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ folgt aus der Gradformel, dass $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ von 2 geteilt wird. Wäre $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2$, so hätten wir

$$\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{3}).$$

Jedoch ist $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$, denn sonst gäbe es $r, s \in \mathbb{Q}$ mit $\sqrt{3} = r + s\sqrt{2}$ und es würde folgen

$$3 = (r + s\sqrt{2})^2 = r^2 + 2s^2 + 2rs\sqrt{2}.$$

Die lineare Unabhängigkeit von 1 und $\sqrt{2}$ über \mathbb{Q} beschert uns $2rs = 0$. Im Fall $s = 0$ hätten wir $3 = r^2$, obwohl 3 kein Quadrat in \mathbb{Q} ist, und im Fall $r = 0$ hätten wir $3 = 2s^2$, obwohl $\frac{3}{2}$ kein Quadrat in \mathbb{Q} ist. Daher kann nicht $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2$ sein, sondern der Erweiterungsgrad muss mindestens gleich dem nächst größeren Vielfachen von 2, nämlich 4, sein.

- c** Sei h das Minimalpolynom von α über $\mathbb{Q}(\sqrt{2})$. Mit den Ergebnissen aus Teil **b** haben wir

$$\deg h = [\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt{2})] = \frac{[\mathbb{Q}(\alpha) : \mathbb{Q}]}{[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]} = \frac{4}{2} = 2.$$

Ein passendes Polynom von Grad 2 liefert uns die Gleichung aus Teil **a**:

$$\alpha - \frac{1}{\alpha} = \sqrt{2} \quad \Rightarrow \quad \alpha^2 - \sqrt{2}\alpha - 1 = 0.$$

Es ist daher $h = X^2 - \sqrt{2}X - 1$.

- d** Natürlich ist $L = \mathbb{Q}(\alpha)$. Wegen $|G_{L|\mathbb{Q}}| = [L : \mathbb{Q}] = 4$ ist $G_{L|\mathbb{Q}} \cong \mathbb{Z}/4\mathbb{Z}$ oder $G_{L|\mathbb{Q}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Wäre $G_{L|\mathbb{Q}} \cong \mathbb{Z}/4\mathbb{Z}$, so hätte $G_{L|\mathbb{Q}}$ nur genau eine Untergruppe von Index 2 und damit die Erweiterung $L|\mathbb{Q}$ nur genau einen quadratischen Zwischenkörper. Wir haben allerdings in Teil **b**

gesehen, dass $L|\mathbb{Q}$ mit $\mathbb{Q}(\sqrt{2})$ und $\mathbb{Q}(\sqrt{3})$ mindestens zwei verschiedene quadratische Zwischenkörper besitzt. Folglich ist $G_{L|\mathbb{Q}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Möchte man die Automorphismen in $G_{L|\mathbb{Q}}$ explizit bestimmen, so kann man das mithilfe des Fortsetzungssatzes tun: Ein \mathbb{Q} -Automorphismus von $L = \mathbb{Q}(\alpha)$ muss α wieder auf eine Nullstelle des Minimalpolynoms f abbilden. Die vier Automorphismen von $G_{L|\mathbb{Q}}$ sind daher anhand der Abbildungsvorschriften

$$\text{id}: \alpha \mapsto \alpha, \quad \sigma_1: \alpha \mapsto -\alpha, \quad \sigma_2: \alpha \mapsto \sqrt{2-\sqrt{3}}, \quad \sigma_3: \alpha \mapsto -\sqrt{2-\sqrt{3}}$$

eindeutig bestimmt.

Lösungsvorschlag zur Aufgabe (Frühjahr 2017, T1A3)

Sei G eine Gruppe der Ordnung $300 = 2^2 \cdot 3 \cdot 5^2$ und v_5 die Anzahl ihrer 5-Sylowgruppen. Laut dem Dritten Sylowsatz gilt dann

$$v_5 \mid (2^2 \cdot 3) \quad \Rightarrow \quad v_5 \in \{1, 2, 3, 4, 6, 12\},$$

sowie $v_5 \equiv 1 \pmod{5}$, was $v_5 \in \{1, 6\}$ liefert. Angenommen, G wäre eine einfache Gruppe. Dann muss $v_5 \neq 1$ sein, denn in diesem Fall wäre die einzige 5-Sylowgruppe ein nicht-trivialer Normalteiler. Folglich muss $v_5 = 6$ sein. Lassen wir nun G mittels

$$G \times \text{Syl}_5 \rightarrow \text{Syl}_5, \quad (g, P) \mapsto gPg^{-1}$$

auf der Menge seiner 5-Sylowgruppen Syl_5 operieren, so liefert dies laut Proposition 1.15 (1) einen Homomorphismus $\phi: G \rightarrow S_6$.

Wäre $\ker \phi = \{e\}$, so wäre ϕ injektiv und wir hätten $G \cong \phi(G) \subseteq S_6$. Nach dem Satz von Lagrange müsste insbesondere $|G| = 300$ ein Teiler von $|S_6| = 720$ sein.

Wäre $\ker \phi = G$, so wäre der Homomorphismus ϕ trivial, d. h. $\phi(g) = \text{id}$ für alle $g \in G$, was gleichbedeutend zu $gPg^{-1} = P$ für alle $g \in G$ und alle 6-Sylowgruppen P ist. Das ist jedoch gerade die Bedingung dafür, dass P ein Normalteiler von G ist, was wiederum unmöglich ist, da G einfach ist.

Es bleibt nur, dass $\ker \phi \neq \{e\}$ und $\ker \phi \neq G$. Dies zeigt aber, dass $\ker \phi$ ein nicht-trivialer Normalteiler von G ist. Widerspruch dazu, dass G einfach ist.

Lösungsvorschlag zur Aufgabe (Frühjahr 2017, T1A4)

- a** Wir zeigen die Aussage per Kontraposition. Sei $p \geq 3$ eine Primzahl, dann hat die Einheitengruppe $(\mathbb{Z}/p\mathbb{Z})^\times$ die Ordnung $\varphi(p) = p - 1$. Wegen $p \geq 3$ ist 2 teilerfremd zu p , sodass 2 eine Einheit modulo p ist, und aus dem kleinen Satz von Fermat folgt

$$2^{p-1} \equiv 1 \pmod{p}.$$

- b** Laut dem Chinesischen Restsatz ist die Abbildung

$$\phi: \mathbb{Z}/341\mathbb{Z} \rightarrow \mathbb{Z}/11\mathbb{Z} \times \mathbb{Z}/31\mathbb{Z}, \quad a \mapsto (a \pmod{11}, a \pmod{31})$$

ein Isomorphismus. Es genügt daher zu zeigen, dass $2^{340} \equiv 1 \pmod{11}$ und $2^{340} \equiv 1 \pmod{31}$. Dies rechnen wir nach:

$$2^{340} = (2^{10})^{34} \stackrel{\text{a}}{\equiv} 1 \pmod{11}$$

$$2^{340} = 2^{330} \cdot 2^{10} \stackrel{\text{a}}{\equiv} 1 \cdot (32)^2 \equiv 1 \cdot 1^2 \equiv 1 \pmod{31}$$

Lösungsvorschlag zur Aufgabe (Frühjahr 2017, T1A5)

- a** Sei $a \in \overline{\mathbb{F}_p}$ eine Nullstelle von χ_A , dann ist χ_A als irreduzibles und normiertes Polynom das Minimalpolynom von a über \mathbb{F}_p . Es folgt

$$[\mathbb{F}_p(a) : \mathbb{F}_p] = \text{grad } \chi_A = n,$$

sodass $\mathbb{F}_p(a) = \mathbb{F}_{p^n}$. Aus dem Kapitel über endliche Körper ist bekannt, dass $\mathbb{F}_{p^n}|\mathbb{F}_p$ eine normale Erweiterung ist, daher folgt aus $a \in \mathbb{F}_{p^n}$ für die Nullstelle a von χ_A , dass χ_A über \mathbb{F}_{p^n} in Linearfaktoren zerfällt. Zudem ist die Erweiterung $\mathbb{F}_{p^n}|\mathbb{F}_p$ nach Proposition 3.12 separabel, weswegen χ_A nur einfache Nullstellen in \mathbb{F}_{p^n} hat. Da die geometrische Vielfachheit jeweils höchstens gleich der algebraischen Vielfachheit ist, müssen sie in diesem Fall bereits gleich sein und alle Voraussetzungen dafür, dass A diagonalisierbar über \mathbb{F}_{p^n} ist, sind erfüllt.

b Wir berechnen zunächst das charakteristische Polynom von A :

$$\begin{aligned}\chi_A &= \det \begin{pmatrix} -1-X & 3 & -1 \\ 0 & -X & 1 \\ 1 & 0 & -X \end{pmatrix} = \\ &= -X^2(X+1) + 3 - X = -X^3 - X^2 - X + 3.\end{aligned}$$

Man sieht, dass 1 eine Nullstelle dieses Polynoms ist. Mittels Polynomdivision gewinnt man

$$\chi_A = -(X-1)(X^2+2X+3).$$

Der zweite Faktor hat in \mathbb{F}_5 keine Nullstellen und ist deswegen in $\mathbb{F}_5[X]$ irreduzibel. Nehmen wir an, A ist über \mathbb{F}_{125} diagonalisierbar. Dann zerfällt χ_A über \mathbb{F}_{125} in Linearfaktoren. Sei $a \in \mathbb{F}_{125}$ eine Nullstelle des zweiten Faktors. Es gilt dann für den Zwischenkörper $\mathbb{F}_5(a)$

$$[\mathbb{F}_5(a) : \mathbb{F}_5] = 2 \quad \text{teilt} \quad 3 = [\mathbb{F}_{125} : \mathbb{F}_5],$$

was einen Widerspruch bedeutet. Andererseits zerfällt χ_A über \mathbb{F}_{25} in Linearfaktoren: Sei $a \in \overline{\mathbb{F}_5}$ eine Nullstelle des zweiten Faktors. Dann ist $\mathbb{F}_5(a)$ ein Körper mit 25 Elementen, also ist $\mathbb{F}_5(a) = \mathbb{F}_{25}$. Da Erweiterungen vom Grad 2 stets normal sind, zerfällt also der zweite Faktor (und damit χ_A) über \mathbb{F}_{25} in Linearfaktoren.

Das charakteristische Polynom χ_A hat keine doppelten Nullstellen, denn im zweiten Faktor tritt 1 nicht als Nullstelle auf und da $\mathbb{F}_{25}|\mathbb{F}_5$ separabel ist, ist auch a keine doppelte Nullstelle. Aus analoger Argumentation wie in Teil **a** stimmen also für alle Eigenwerte die algebraische und geometrische Vielfachheit überein und A ist über \mathbb{F}_{25} diagonalisierbar.

Lösungen zu Thema Nr. 2

Lösungsvorschlag zur Aufgabe (Frühjahr 2017, T2A1)

Sei G eine einfache Gruppe mit $|G| = 660 = 11 \cdot 5 \cdot 2^2 \cdot 3$. Jedes Element der Ordnung 11 von G erzeugt eine Untergruppe der Ordnung 11, also eine 11-Sylowgruppe P . Nehmen wir an, es gibt eine weitere 11-Sylowgruppe P' mit $g \in P$, so folgt daraus $P = \langle g \rangle \subseteq P'$ und da P und P' gleiche Ordnung haben, erhalten wir $P = P'$. Das bedeutet, jedes Element der Ordnung 11 liegt in genau einer 11-Sylowgruppe. Wir bestimmen daher nun die Anzahl ν_{11} der 11-Sylowgruppen von G .

Nach dem Dritten Sylowsatz ist $\nu_{11} \mid 5 \cdot 2^2 \cdot 3$ und daher

$$\nu_{11} \in \{1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60\}.$$

Die zweite Bedingung $\nu_{11} \equiv 1 \pmod{1}$ liefert $\nu_{11} \in \{1, 12\}$. Wäre $\nu_{11} = 1$, so wäre die 11-Sylowgruppe ein Normalteiler von G , was nicht möglich ist, da G laut Voraussetzung eine einfache Gruppe ist, also keinen nicht-trivialen Normalteiler besitzt. Somit muss $\nu_{11} = 12$ gelten.

Da in jeder 11-Sylowgruppe das Neutralelement sowie 10 Element der Ordnung 11 liegen, besitzt G insgesamt

$$12 \cdot 10 = 120$$

Elemente der Ordnung 11.

Lösungsvorschlag zur Aufgabe (Frühjahr 2017, T2A2)

- a** Wir zeigen, dass $\text{ord } g = n$, denn dann ist $|\langle g \rangle| = \text{ord } g = n$, sodass aus $\langle g \rangle \subseteq G$ bereits $G = \langle g \rangle$ folgen muss.

Wir wissen, dass $\text{ord } g$ ein Teiler der Gruppenordnung n sein muss. Angenommen, es ist $\text{ord } g$ ein echter Teiler, d.h. es gibt ein $k \geq 2$ mit $n = k \cdot \text{ord } g$. Wegen $k \geq 2$ hat k einen Primteiler p und wir haben $\frac{n}{p} = \frac{k}{p} \cdot \text{ord } g$, wobei $\frac{k}{p}$ eine ganze Zahl ist. Es folgt

$$g^{n/p} = g^{\frac{k}{p} \cdot \text{ord } g} = \left(g^{\text{ord } g}\right)^{k/p} = 1^{k/p} = 1$$

im Widerspruch zur Voraussetzung.

- b** Wir zeigen die Aussage stupide durch vollständige Induktion über m .

Induktionsanfang $m = 0$: Es gilt $4^{3^0} = 4^1 = 1 + 3^1$, also ist die Aussage für diesen Fall erfüllt.

Induktionsschritt $m \mapsto m + 1$: Nach Induktionsvoraussetzung gibt es ein $k \in \mathbb{Z}$ mit

$$4^{3^m} = 1 + 3^{m+1} + k3^{m+2}.$$

Unter Verwendung von $(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$ berechnet man

nun

$$\begin{aligned} 4^{3^m+1} &= (1 + 3^{m+1} + k3^{m+2})^3 = \\ &= (1 + 3^{m+1})^3 \\ &\quad + 3(1 + 3^{m+1})^2 \cdot k3^{m+2} + 3(1 + 3^{m+1}) \cdot (k3^{m+2})^2 + (k3^{m+2})^3 \equiv \\ &\equiv (1 + 3^{m+1})^3 \mod 3^{m+3}. \end{aligned}$$

Und der Spaß geht noch weiter:

$$\begin{aligned} (1 + 3^{m+1})^3 &\equiv 1^3 + 3 \cdot 3^{m+1} + 3 \cdot (3^{m+1})^2 + (3^{m+1})^3 \equiv \\ &\equiv 1 + 3^{m+2} \mod 3^{m+3}. \end{aligned}$$

Insgesamt also $4^{3^m+1} \equiv 1 + 3^{m+2} \mod 3^{m+3}$ wie gewünscht.

- c** Die Einheitengruppe $(\mathbb{Z}/3^e\mathbb{Z})^\times$ ist eine Gruppe der Ordnung $\varphi(3^e) = 2 \cdot 3^{e-1}$. Wir wollen nun Aufgabenteil **a** mit $n = 2 \cdot 3^{e-1}$ anwenden und berechnen daher:

$$2^{n/3} = 2^{2 \cdot 3^{e-2}} = 4^{3^{e-2}} \stackrel{\text{b}}{\equiv} 1 + 3^{e-1} \not\equiv 1 \mod 3^e$$

Um auch $2^{n/2} \not\equiv 1 \mod 3^e$ zu sehen, betrachten wir $2^{n/2}$ zunächst modulo 3:

$$2^{n/2} = 2^{3^{e-1}} \equiv (-1)^{3^{e-1}} \equiv -1 \equiv 2 \mod 3$$

Dabei ging ein, dass 3^{e-1} immer ungerade ist. Wäre nun $2^{n/2} \equiv 1 \mod 3^e$, so wäre insbesondere $2^{n/2} \equiv 1 \mod 3$ im Widerspruch zur obigen Rechnung, also ist $2^{n/2} \not\equiv 1 \mod 3$.

Anwendung von Teil **a** liefert nun $\langle 2 \rangle = (\mathbb{Z}/3^e\mathbb{Z})^\times$.

Lösungsvorschlag zur Aufgabe (Frühjahr 2017, T2A3)

- a** Bei H handelt es sich um das Bild der Abbildung $\tau: K^\times \rightarrow H, a \mapsto a^2$. Da Bildmengen von Homomorphismen stets Untergruppen sind, folgt die Aussage aus der Gleichung

$$\tau(ab) = (ab)^2 = a^2b^2 = \tau(a)\tau(b) \quad \text{für } a, b \in K^\times.$$

Alternative: Man kann die Untergruppen-Eigenschaften auch direkt prüfen.

b Sei τ wie in Teil **a** definiert. In Charakteristik 2 gilt

$$a \in \ker \tau \Leftrightarrow a^2 = \bar{1} \Leftrightarrow a^2 - \bar{1} = 0 \Leftrightarrow (a - \bar{1})^2 = 0 \Leftrightarrow a = \bar{1}.$$

Also ist der Kern von τ trivial und τ ist eine Bijektion zwischen K^\times und H . Daraus folgt insbesondere $|H| = |K^\times|$ und zusammen mit $H \subseteq K^\times$ ergibt dies $H = K^\times$.

c Ist $\text{char } K > 2$, so gilt $-1 \neq 1$ und wir erhalten

$$a^2 = 1 \Leftrightarrow a^2 - 1 = 0 \Leftrightarrow (a + 1)(a - 1) = 0 \Leftrightarrow a \in \{1, -1\}.$$

Damit ist $\ker \tau = \{\pm 1\}$ und der Homomorphiesatz liefert

$$\left| K^\times / \{\pm 1\} \right| = |H| \Leftrightarrow |K^\times| = 2|H|.$$

Dies ergibt

$$(K^\times : H) = \frac{2|H|}{|H|} = 2.$$

Lösungsvorschlag zur Aufgabe (Frühjahr 2017, T2A4)

a Das normierte Polynom f ist laut dem Eisenstein-Kriterium mit $p = 2$ irreduzibel, also das Minimalpolynom von α . Wir zeigen nun, dass $\{1, \alpha, \alpha^2\}$ ein linear unabhängiges Erzeugendensystem von $\mathbb{Q}(\alpha)$ ist.

Zum Nachweis der linearen Unabhängigkeit nehmen wir an, es gibt $a_0, a_1, a_2 \in \mathbb{Q}$ mit $a_2\alpha^2 + a_1\alpha + a_0 = 0$. Wäre $a_1 \neq 0$ und $a_2 \neq 0$, so wäre $g = a_2X^2 + a_1X + a_0$ ein Polynom vom Grad ≤ 2 , das die Nullstelle α hat – im Widerspruch dazu, dass f das Minimalpolynom von α ist. Aus $a_1 = a_2 = 0$ und der Gleichung folgt auch $a_0 = 0$ und somit die lineare Unabhängigkeit von $\{1, \alpha, \alpha^2\}$.

Jedes Element $\beta \in \mathbb{Q}(\alpha)$ hat die Form $\beta = g(\alpha)$ für ein Polynom $g \in \mathbb{Q}[X]$. Division mit Rest von g durch f liefert $g = rq + h$ für Polynome $q, h \in \mathbb{Q}[X]$ mit $\text{grad } h \leq 2$. Schreibe $h = a_2X^2 + a_1X + a_0$, so gilt

$$\beta = r(\alpha)f(\alpha) + h(\alpha) = h(\alpha) = a_2\alpha^2 + a_1\alpha + a_0$$

und β ist eine \mathbb{Q} -Linearkombination von $\{1, \alpha, \alpha^2\}$. Damit ist $\{1, \alpha, \alpha^2\}$ ein Erzeugendensystem von $\mathbb{Q}(\alpha)$.

b Es gilt:

$$\begin{aligned} 0 = f(\alpha) &\Leftrightarrow 1 = \alpha^3 + 2\alpha + 3 \Leftrightarrow 1 = (\alpha + 1)(\alpha^2 - \alpha + 3) \\ &\Leftrightarrow \frac{1}{\alpha + 1} = \alpha^2 - \alpha + 3 \end{aligned}$$

Alternative: Der Ansatz $(a_2\alpha^2 + a_1\alpha + a_0)(\alpha + 1) = 1$ mit rationalen Koeffizienten $a_0, a_1, a_2 \in \mathbb{Q}$ liefert aufgrund der linearen Unabhängigkeit von $1, \alpha, \alpha^2$ ein lineares Gleichungssystem für a_0, a_1, a_2 , das gelöst werden kann.

Lösungsvorschlag zur Aufgabe (Frühjahr 2017, T2A5)

Sei $G_{K|\mathbb{Q}}$ die Galois-Gruppe der Erweiterung $K|\mathbb{Q}$. Laut Angabe hat diese die Ordnung $55 = 5 \cdot 11$. Gemäß dem Hauptsatz der Galois-Theorie korrespondieren die Zwischenkörper der Erweiterung $K|\mathbb{Q}$ eindeutig zu den Untergruppen der Galois-Gruppe und für einen Zwischenkörper L ist $L|\mathbb{Q}$ genau dann normal (und somit galoissch), wenn die zugehörige Untergruppe ein Normalteiler von $G_{K|\mathbb{Q}}$ ist.

Da die Ordnung einer Untergruppe von $G_{K|\mathbb{Q}}$ laut dem Satz von Lagrange ein Teiler von 55 sein muss, kommen für nicht-triviale Untergruppen nur die Ordnungen 5 oder 11 in Betracht. Bei diesen Untergruppen handelt es sich genau um die Sylowgruppen von $G_{K|\mathbb{Q}}$, sodass wir ihre Anzahl mit dem Dritten Sylowsatz bestimmen können.

Aus diesem folgt, dass $G_{K|\mathbb{Q}}$ genau eine 11-Sylowgruppe P_{11} hat, die deshalb ein Normalteiler ist. Laut der Vorbemerkung ist für den korrespondierenden Zwischenkörper L die Erweiterung $L|\mathbb{Q}$ galoissch und es gilt

$$[L : \mathbb{Q}] = (G_{K|\mathbb{Q}} : P_{11}) = \frac{55}{11} = 5.$$

Außerdem kann $G_{K|\mathbb{Q}}$ eine oder elf 5-Sylowgruppen besitzen. Nehmen wir zunächst an, dass es nur eine 5-Sylowgruppe P_5 gibt. Diese wäre dann ein Normalteiler von $G_{K|\mathbb{Q}}$. Da ferner die Ordnungen von P_{11} und P_5 teilerfremd sind, haben diese trivialen Schnitt und die Ordnung des Komplexprodukts ist

$$|P_5 P_{11}| = \frac{|P_5| \cdot |P_{11}|}{P_5 \cap P_{11}} = 5 \cdot 11,$$

was $P_5 P_{11} = G_{K|\mathbb{Q}}$ impliziert. $G_{K|\mathbb{Q}}$ ist also inneres direktes Produkt von P_5 und P_{11} und daher isomorph zu $P_5 \times P_{11}$. Nun sind P_5 und P_{11} als Gruppen

von Primzahlordnung jedoch zyklisch, also ist ihr Produkt abelsch – Widerspruch zur Voraussetzung, dass $G_{K|Q}$ eine nicht-abelsche Gruppe ist. Somit ist keine der 5-Sylowgruppen ein Normalteiler von $G_{K|Q}$ und es gibt keine weitere normale Zwischenerweiterung.

Lösungen zu Thema Nr. 3

Lösungsvorschlag zur Aufgabe (Frühjahr 2017, T3A1)

Sei $A = (a_{ij}) \in G$ eine Matrix, dann ist zu zeigen, dass $\det F(A) = 1$ erfüllt ist. Dazu verwenden wir die Leibniz-Formel für die Determinante:

$$\det F(A) = \sum_{\sigma \in S_n} \operatorname{sgn} \sigma \prod_{i=1}^n a_{i, \sigma(i)}^p = \sum_{\sigma \in S_n} \operatorname{sgn} \sigma \left(\prod_{i=1}^n a_{i, \sigma(i)} \right)^p$$

Ist $p > 2$, so ist p ungerade und es gilt $(\operatorname{sgn} \sigma)^p = (\pm 1)^p = (\pm 1) = \operatorname{sgn} \sigma$ für alle $\sigma \in S_n$. Falls $p = \operatorname{char} K = 2$, so ist $1 = -1$ in K und es gilt ebenfalls $(\operatorname{sgn} \sigma)^p = \operatorname{sgn} \sigma$. Zusammen mit *freshman's dream* kann man den Ausdruck von oben also weiter zu

$$\det F(A) = \sum_{\sigma \in S_n} (\operatorname{sgn} \sigma)^p \prod_{i=1}^n a_{i, \sigma(i)}^p = \left(\sum_{\sigma \in S_n} \operatorname{sgn} \sigma \prod_{i=1}^n a_{i, \sigma(i)} \right)^p = (\det A)^p = 1$$

umschreiben. Sei nun $B = (b_{ij}) \in G$ eine weitere Matrix, dann gilt

$$F(AB) = \left(\left(\sum_{k=1}^n a_{ik} b_{kj} \right)^p \right) = \left(\sum_{k=1}^n a_{ik}^p b_{kj}^p \right) = F(A) \cdot F(B),$$

also definiert F tatsächlich einen Gruppenhomomorphismus $G \rightarrow G$.

Wir zeigen als Nächstes, dass H eine Untergruppe von G ist. Sei dazu $\mathbb{E}_n = (\delta_{ij})$ mit dem **Kronecker-Delta** δ_{ij} (also $\delta_{ij} = 0$, falls $i \neq j$ und $\delta_{ij} = 1$, falls $i = j$) die Einheitsmatrix, dann ist

$$F(\mathbb{E}_n) = (\delta_{ij}^p) = (\delta_{ij}) = \mathbb{E}_n,$$

sodass $\mathbb{E}_n \in H$. Falls $A, B \in H$ sind, so ist auch

$$F(AB) = F(A) \cdot F(B) = A \cdot B,$$

da F ein Homomorphismus ist. In gleicher Weise erhält man

$$F(A^{-1}) = F(A)^{-1} = A^{-1}.$$

Dies zeigt, dass mit A und B auch $A \cdot B$ sowie A^{-1} in H liegen. Insgesamt haben wir damit gezeigt, dass H eine Untergruppe von G ist. Es gilt nun

$$A \in H \Leftrightarrow F(A) = A \Leftrightarrow a_{ij}^p = a_{ij} \text{ für alle } (i, j) \in \{1, \dots, n\}^2,$$

also sind alle Koeffizienten von A Nullstellen des Polynoms $X^p - X \in K[X]$. Aus dem Kapitel über endliche Körper ist bekannt, dass die Nullstellenmenge dieses Polynoms genau der Primkörper $P \cong \mathbb{F}_p$ von K ist.

Lösungsvorschlag zur Aufgabe (Frühjahr 2017, T3A2)

- a** Sei ν_5 die Anzahl der 5-Sylowgruppen von S_5 , dann liefert der Dritte Sylowsatz, dass

$$\nu_5 \mid (2^3 \cdot 3) \Rightarrow \nu_5 \in \{1, 2, 3, 4, 6, 8, 12, 24\}$$

und mit der zusätzlichen Bedingung $\nu_5 \equiv 1 \pmod{5}$ bleibt nur $\nu_5 \in \{1, 6\}$. Angenommen, es wäre $\nu_5 = 1$, dann gäbe es nur eine 5-Sylowgruppe in S_5 , bestehend aus id und 4 Elementen der Ordnung 5. Jedoch ist jeder 5-Zykel ein Element der Ordnung 5 und davon gibt es nach der Formel von Seite 63 genau

$$\binom{5}{5} (5-1)! = 4! = 24.$$

Da jedes davon in einer 5-Sylowgruppe liegt, muss es mehr als eine Sylowgruppe geben. Es bleibt daher nur $\nu_5 = 6$.

- b** Wir lassen S_5 per Konjugation auf der Menge Syl_5 seiner 5-Sylowgruppen operieren. Dies liefert gemäß Proposition 1.15 (1) einen Homomorphismus

$$\phi: S_5 \rightarrow S_6.$$

Wir zeigen nun, dass ϕ injektiv ist, denn dann ist $S_5 \cong \phi(S_5)$ und da S_5 laut dem Zweiten Sylowsatz transitiv auf Syl_5 operiert, operiert $\phi(S_5)$ transitiv auf $\{1, \dots, 6\}$.

Sei $\sigma \in \ker \phi$, dann gilt $\sigma P \sigma^{-1} = P$ für alle $P \in \text{Syl}_5$, d.h. σ liegt in $\bigcap_{P \in \text{Syl}_5} N_{S_5}(P)$, dem Schnitt über alle Normalisatoren. Laut 1.17 gilt

$$|N_{S_5}(P)| = \frac{|S_5|}{|S_5(P)|} = \frac{120}{6} = 20$$

für alle $P \in \text{Syl}_5$, wobei wir verwendet haben, dass S_5 transitiv auf Syl_5 operiert und deshalb für die Bahn $|S_5(P)| = v_5 = 6$ gilt. Wegen $\ker \phi \subseteq N_{S_5}(P)$ muss daher $|\ker \phi|$ ein Teiler von 20 sein.

Angenommen, $|\ker \phi|$ wird von 5 geteilt, dann gibt es nach dem Nullten Sylowsatz 1.26 ein Element der Ordnung 5 in $\ker \phi$, also einen 5-Zykel. Da $\ker \phi$ ein Normalteiler ist, müsste $\ker \phi$ dann die gesamte Konjugationsklasse dieses 5-Zykels enthalten, also alle 5-Zykeln. Wir haben oben gesehen, dass deren Anzahl 24 ist. Wegen $|\ker \phi| \leq 20$ können diese also nicht alle in $\ker \phi$ enthalten sein. Also wird $|\ker \phi|$ nicht von 5 geteilt und, da $|\ker \phi|$ ein Teiler von 20 ist, haben wir $|N| \leq 4$.

Analog liefert die Annahme, dass $|\ker \phi|$ von 2 geteilt wird, dass $\ker \phi$ einen 2-Zykel oder eine Doppeltransposition und damit alle Permutationen diesen Zerlegungstyps enthalten muss. Davon gibt es aber

$$\binom{5}{2} = 10 \quad \text{bzw.} \quad \frac{1}{2} \cdot \binom{5}{2} \cdot \binom{3}{2} = 15,$$

also ebenfalls zu viele. Es bleibt also nur noch $|\ker \phi| = 1$, d.h. $\ker \phi = \{\text{id}\}$.

c Betrachte die Untergruppe

$$U = \{\sigma \in S_6 \mid \sigma(6) = 6\} \cong S_5.$$

Angenommen, es gibt ein $\tau \in S_6$ mit $\phi(S_5) = \tau U \tau^{-1}$. Sei $a = \tau(6)$, dann würde für alle Elemente $\tau \rho \tau^{-1} \in \tau U \tau^{-1} = \phi(S_5)$ gelten, dass

$$\tau \rho \tau^{-1}(a) = \tau \rho(6) = \tau(6) = a.$$

Dies widerspricht aber der Tatsache, dass $\phi(S_5)$ transitiv auf $\{1, \dots, 6\}$ operiert, es also beispielsweise ein $\iota \in \phi(S_5)$ mit $\iota(6) = 1$ geben muss.

Lösungsvorschlag zur Aufgabe (Frühjahr 2017, T3A3)

Angenommen, es gibt einen Ringhomomorphismus $\phi: \mathbb{Z}[\sqrt{-3}] \rightarrow \mathbb{Z}[i]$. Aus $\phi(1) = 1$ folgt zunächst induktiv, dass $\phi(m) = m$ für alle $m \in \mathbb{Z}$. Sei nun $\xi = \phi(\sqrt{-3})$, dann gilt

$$\xi^2 = \phi(\sqrt{-3})^2 = \phi(\sqrt{-3}^2) = \phi(-3) = -3.$$

Wegen $\xi \in \mathbb{Z}[i]$ gibt es $a, b \in \mathbb{Z}$ mit $\xi = a + ib$, sodass

$$-3 = (a + ib)^2 = a^2 - b^2 + 2abi.$$

Da -3 eine reelle Zahl ist, muss der Imaginärteil verschwinden, sodass $2ab = 0$ sein muss, d.h. $a = 0$ oder $b = 0$. Falls $a = 0$, so wird obige Gleichung zu $-3 = -b^2$. Diese Gleichung hat jedoch keine ganzzahlige Lösung. Genauso würde man für $b = 0$ die unsinnige Gleichung $-3 = a^2$ erhalten.

Der Widerspruch zeigt, dass es ein solches Element ξ in $\mathbb{Z}[i]$ und damit auch den Homomorphismus $\phi: \mathbb{Z}[\sqrt{-3}] \rightarrow \mathbb{Z}[i]$ nicht geben kann.

Lösungsvorschlag zur Aufgabe (Frühjahr 2017, T3A4)

Da μ_A und f teilerfremd sind, existieren laut dem Lemma von Bézout Polynome $g, h \in K[X]$, sodass

$$g\mu_A + fh = 1$$

erfüllt ist. Setzen wir die Matrix A in diese Gleichung ein, so erhalten wir

$$\mathbb{E}_n = g(A)\mu_A(A) + f(A)h(A) = f(A)h(A)$$

wegen $\mu_A(A) = 0$. Somit ist $f(A)^{-1} = h(A)$ und $f(A)$ ist insbesondere invertierbar.

Lösungsvorschlag zur Aufgabe (Frühjahr 2017, T3A5)

Sei $f = X^2 + X + 1 \in \mathbb{F}_q[X]$. Ist q eine Potenz von 3, ist $\text{char } K = 3$, sodass $f(1) = 0$. Insbesondere ist f nicht irreduzibel über \mathbb{F}_q für $\text{char } K = 3$ bzw. $q \equiv 0 \pmod{3}$.

Für $\text{char } K \neq 3$ hat man $f(1) = 3 \neq 0$, sodass 1 in diesem Fall keine Nullstelle hat. Inspiriert von Satz 3.17 (2) hat man jedoch die Gleichung

$$X^3 - 1 = (X - 1)(X^2 + X + 1),$$

denn f ist das dritte Kreisteilungspolynom. Ist f also reduzibel, so gibt es eine Nullstelle $a \in \mathbb{F}_q$ von f , für die somit $a^3 = 1$ gelten muss. Daraus folgt, dass die Ordnung von a in \mathbb{F}_q^\times ein Teiler von 3 ist. Wegen $a \neq 1$ muss tatsächlich $\text{ord } a = 3$ sein. Ist umgekehrt $a \in \mathbb{F}_q^\times$ ein Element der Ordnung 3, so gilt

$$0 = a^3 - 1 = (a - 1)(a^2 + a + 1)$$

und wegen $a \neq 1$ ist $f(a) = 0$. Wir haben also gezeigt, dass f genau dann reduzibel über \mathbb{F}_q ist, wenn es ein Element der Ordnung 3 in \mathbb{F}_q^\times gibt. Da \mathbb{F}_q^\times eine zyklische Gruppe ist, ist dies genau dann der Fall, wenn 3 die Gruppenordnung $q - 1$ teilt, was

$$q - 1 \equiv 0 \pmod{3} \Leftrightarrow q \equiv 1 \pmod{3}$$

bedeutet. Zusammenfassend:

„ \Rightarrow “: Sei f irreduzibel über \mathbb{F}_q , dann muss $q \not\equiv 0 \pmod{3}$, denn sonst hätte f wie ganz zu Beginn gesehen die Nullstelle 1 und wäre somit reduzibel. Wäre $q \equiv 1 \pmod{3}$, so wäre f nach der Äquivalenz oben ebenfalls reduzibel. Es bleibt daher nur $q \equiv -1 \pmod{3}$.

„ \Leftarrow “: Sei umgekehrt $q \equiv -1 \pmod{3}$, dann ist insbesondere $\text{char } K \neq 3$ und die Äquivalenz oben liefert, dass f irreduzibel über \mathbb{F}_q ist.

9. Analysis: Aufgabenlösungen nach Jahrgängen

Prüfungstermin: Frühjahr 2015

Thema Nr. 1 (Aufgabengruppe)

Aufgabe 1 → S. 363

In dieser Aufgabe bezeichne $B_r(a) := \{z \in \mathbb{C} \mid |z - a| < r\}$ für $a \in \mathbb{C}$ und $r > 0$. Ferner sei $f: \mathbb{C} \rightarrow \mathbb{C}$ durch $f(z) := 6z^6 - 2z^2 + 1$ gegeben.

- a** Formulieren Sie den Satz von Rouché für ganze Funktionen. (1 Punkt)
 - b** Zeigen Sie, dass $B_4(1) \subseteq f(B_1(0)) \subseteq B_8(1)$ gilt.
- Hinweis** Für den Nachweis der ersten Inklusion könnte der in **a** formulierte Satz hilfreich sein. (3 Punkte)
- c** Entscheiden Sie mit Beweis, ob $f(B_1(0)) \cap \mathbb{R} = f(B_1(0) \cap \mathbb{R})$ gilt. (2 Punkte)

Aufgabe 2 → S. 565

Es sei $Q := \{z \in \mathbb{C} \mid \operatorname{Re}(z) < 0 \text{ und } \operatorname{Im}(z) > 0\}$ der offene zweite Quadrant der komplexen Zahlenebene. Bestimmen Sie mit Begründung alle Abbildungen $f: Q \rightarrow \mathbb{C}$, die Q biholomorph auf die offene Einheitskreisscheibe $\mathbb{E} := \{z \in \mathbb{C} \mid |z| < 1\}$ abbilden mit $f(-1 + i) = 0$. (6 Punkte)

Aufgabe 3 → S. 567

- a** Bestimmen Sie die allgemeine reelle Lösung der Differentialgleichung

$$x''(t) + 2x'(t) + x(t) = \cos(2t), \quad t \in \mathbb{R}.$$

Für welche $(a; b) \in \mathbb{R}^2$ ist die maximale Lösung des zugehörigen Anfangswertproblems $x(0) = a, x'(0) = b$ beschränkt? Begründen Sie Ihre Antworten.

(3 Punkte)

- b** Geben Sie (mit Begründung) alle Paare $(c; d) \in \mathbb{R}^2$ an, für welche die zu gehörige Differentialgleichung

$$x''(t) + cx'(t) + dx(t) = \cos(2t), \quad t \in \mathbb{R},$$

keine beschränkte reelle maximale Lösung besitzt. (3 Punkte)

Aufgabe 4 → S. 402

Bestimmen Sie eine reelle Lösung $y : I \rightarrow \mathbb{R}$ des Anfangswertproblems

$$y(x)y'(x) + y(x)^2 + 2x + 5 = 0, \quad y(-4) = -2.$$

Wie groß kann das Intervall I maximal gewählt werden? (6 Punkte)

Hinweis Eine Möglichkeit der Lösung besteht darin, zunächst einen integrierenden Faktor $u : \mathbb{R} \rightarrow]0; \infty[$ zu bestimmen, welcher nur von der Variablen x abhängt. Wir bezeichnen hierbei u als integrierenden Faktor, wenn die Differentialgleichung nach Multiplikation mit u exakt wird. (6 Punkte)

Aufgabe 5 → S. 569

Bestimmen Sie (mit Nachweis) für jedes $a \in \mathbb{R}$ das globale Minimum der Funktion

$$f : H \rightarrow \mathbb{R}, \quad f(x, y) := x^2 - ax + y^2, \quad \text{wobei } H := \{(x, y) \in \mathbb{R}^2 \mid x + y \geq 1\},$$

falls f ein solches Minimum besitzt. Geben Sie in diesen Fällen alle Stellen an, an denen das Minimum angenommen wird. (6 Punkte)

Thema Nr. 2
(Aufgabengruppe)

Aufgabe 1 → S. 570

- a** Definiere $U := \{z \in \mathbb{C} : 2|\operatorname{Re}(z)| + 3|\operatorname{Im}(z)| + \frac{1}{1+|z|^2} < \frac{11}{2}\}$. Gibt es eine holomorphe Funktion $h : \mathbb{C} \rightarrow U$ und Punkte $v, w \in \mathbb{C}$ mit $h(v) = \frac{i}{2}$ und $h(w) = 1 - i$? Begründung! (2 Punkte)

- b** Sei $\Omega \subseteq \mathbb{C}$ eine nicht-leere offene Menge und $z_0 \in \Omega$. Seien $f : \Omega \rightarrow \mathbb{C}$ und $g : \Omega \rightarrow \mathbb{C}$ holomorphe Funktionen mit $f(z_0) = f^{(1)}(z_0) = 0, g(z_0) = g^{(1)}(z_0) = 0$ und $g^{(2)}(z_0) \neq 0$. Zeigen Sie:

$$\lim_{z \rightarrow z_0} \frac{f(z)}{g(z)} = \frac{f^{(2)}(z_0)}{g^{(2)}(z_0)}.$$

(2 Punkte)

- c** Definiere $F: \mathbb{C} \setminus \{0\} \rightarrow \mathbb{C}$ durch

$$F(z) := \frac{1 - \cos(z)}{z^2}, \quad z \neq 0.$$

Ist die isolierte Singularität 0 von F hebbbar? Begründung! (2 Punkte)

Aufgabe 2 → S. 572

Sei $U := \{z \in \mathbb{C} : \operatorname{Re}(z) > 0\}$.

- a** Zeigen Sie, dass

$$\operatorname{Log}(z+i) - \operatorname{Log}(z-i) = \operatorname{Log}\left(\frac{z+i}{z-i}\right), \quad z \in U,$$

gilt, wobei $\operatorname{Log} : \Omega_- \rightarrow \mathbb{C}$, mit $\Omega_- := \mathbb{C} \setminus \{x + i0 : x \in]-\infty, 0]\}$, der Hauptzweig des Logarithmus ist. (3 Punkte)

- b** Für jedes $z \in U$ sei $[1, \frac{z}{2}]$ die gerade Strecke in \mathbb{C} von $1+0i$ nach $\frac{z}{2}$. Definiere $f: U \rightarrow \mathbb{C}$ durch die Wegintegrale

$$f(z) := \int_{[1, \frac{z}{2}]} \frac{1}{1+\xi^2} d\xi, \quad z \in U.$$

Zeigen Sie:

$$f(z) = \frac{\pi}{4} + \frac{i}{2} \operatorname{Log}\left(\frac{z+2i}{z-2i}\right), \quad z \in U.$$

(3 Punkte)

Aufgabe 3 → S. 573

- a** Sei $K := \{z \in \mathbb{C} : |z| \leq 1\}$ und r eine reelle Zahl mit $r > e$. Zeigen Sie, dass die Gleichung

$$rze^z = 1$$

genau eine Lösung in K besitzt.

Hinweis Die Verwendung des Satzes von Rouché könnte hier hilfreich sein.

(2 Punkte)

- b** Sei γ die positiv orientierte Kreislinie mit Mittelpunkt 0 und Radius 3. Definiere die Funktion $f: \mathbb{R} \rightarrow \mathbb{C}$ durch die Wegintegrale

$$f(t) := \frac{1}{2\pi i} \int_{\gamma} \frac{e^{zt}}{z^2(z^2 + 2z + 2)} dz, \quad t \in \mathbb{R}.$$

Zeigen Sie, dass f eine reell-wertige C^∞ -Funktion auf \mathbb{R} mit $f(0) = 0$ ist.

(4 Punkte)

Aufgabe 4 → S. 412

Man löse das Anfangswertproblem $x' = x + t, x(0) = -1$

- a** mit der Methode der Variation der Konstanten; (3 Punkte)
- b** mittels der Picard-Lindelöf-Iteration $(\alpha_n)_{n \in \mathbb{N}_0}$, beginnend mit $\alpha_0(t) = -1$. (3 Punkte)

Aufgabe 5 → S. 482

Gegeben sei das ebene autonome System

$$\begin{aligned}x' &= -e^x - 2y + 1 \\y' &= 2x - y.\end{aligned}$$

Man bestimme alle Ruhelpunkte des Systems und untersuche diese auf Stabilität. (6 Punkte)

Thema Nr. 3
(Aufgabengruppe)

In dieser Aufgabengruppe bezeichne $K_r(0) := \{z \in \mathbb{C} : |z| < r\}$ die offene Kreisscheibe um 0 mit Radius $r > 0$. Ferner sei $\mathbb{D} := K_1(0)$.

Aufgabe 1 → S. 394

Seien $f, g: \mathbb{R} \rightarrow \mathbb{R}$ stetig. Wir betrachten das Anfangswertproblem

$$\dot{x}(t) = g(t)f(x(t)), \quad x(t_0) = x_0, \tag{1}$$

wobei $t_0, x_0 \in \mathbb{R}$.

- a** Geben Sie ein Beispiel eines Anfangswertproblems der Form (1) an, sowie ein zugehöriges Intervall, so dass es zwei verschiedene Lösungen besitzt. (3 Punkte)

- b** Wir nehmen nun zusätzlich an, dass $f, g: \mathbb{R} \rightarrow (0, \infty)$. Zeigen Sie, dass das Problem (1) dann lokal eindeutig lösbar ist. (3 Punkte)

Hinweis Es sind hier Existenz und Eindeutigkeit zu zeigen.

Aufgabe 2 → S. 574

Gegeben sei das Anfangswertproblem

$$\begin{bmatrix} \dot{x} \\ \dot{y} \end{bmatrix} = \begin{bmatrix} e^t & 1 \\ 1 & e^t \end{bmatrix} \cdot \begin{bmatrix} x \\ y \end{bmatrix}, \quad \begin{bmatrix} x(0) \\ y(0) \end{bmatrix} = \begin{bmatrix} x_0 \\ y_0 \end{bmatrix}$$

Man zeige, dass die eindeutige Lösung von der Form

$$\begin{bmatrix} x(t) \\ y(t) \end{bmatrix} = e^{\begin{bmatrix} f(t) & g(t) \\ g(t) & f(t) \end{bmatrix}} \cdot \begin{bmatrix} x_0 \\ y_0 \end{bmatrix}$$

ist und bestimme die Funktionen $f, g: \mathbb{R} \rightarrow \mathbb{R}$.

(6 Punkte)

Aufgabe 3 → S. 367

Es seien f und g holomorph auf $K_2(0)$ und $f(\zeta) \neq 0$ für alle $\zeta \in \partial\mathbb{D}$ und für jedes $\zeta \in \partial\mathbb{D}$ sei $g(\zeta)/f(\zeta)$ reell und positiv. Zeigen Sie, dass f und g in \mathbb{D} dieselbe Anzahl von Nullstellen (mit Vielfachheiten gezählt) besitzen. (6 Punkte)

Aufgabe 4 → S. 575

- a** Es sei f holomorph in $\mathbb{D} \setminus \{0\}$ mit einem Pol 1. Ordnung in $z = 0$. Weiter seien $\alpha \in (0, 2\pi)$, $\varepsilon > 0$ und $\gamma_\varepsilon : [0, \alpha] \rightarrow \mathbb{C}$, $\gamma_\varepsilon(t) = \varepsilon e^{it}$ für $t \in [0, \alpha]$. Zeigen Sie:

$$\lim_{\varepsilon \rightarrow 0} \int_{\gamma_\varepsilon} f(\xi) d\xi = i\alpha \operatorname{res}(0, f).$$

Hier bezeichne $\operatorname{res}(0, f)$ das Residuum von f im Punkt $z = 0$. (4 Punkte)

- b** Die stetige Funktion $f : \overline{\mathbb{D}} \rightarrow \mathbb{C}$ sei holomorph in \mathbb{D} . Ferner seien m_1 und m_2 reell und positiv, derart, dass für alle $\zeta \in \partial\mathbb{D}$ gilt

$$|f(\zeta)| \leq m_1 \text{ falls } \operatorname{Im} \zeta \geq 0 \quad \text{und} \quad |f(\zeta)| \leq m_2 \text{ falls } \operatorname{Im} \zeta \leq 0.$$

Beweisen Sie, dass $|f(0)| \leq \sqrt{m_1 m_2}$. (2 Punkte)

Hinweis Betrachten Sie die Funktion $f(z)f(-z)$.

Aufgabe 5 → S. 576

- a** Zeigen Sie: Es gibt keine holomorphe Funktion $f : \mathbb{D} \setminus \{0\} \rightarrow \mathbb{C}$ mit der Eigenschaft $f(z)^3 = z$ für alle $z \in \mathbb{D} \setminus \{0\}$. (3 Punkte)

Hinweis Wenden Sie zunächst den Riemannschen Hebbarkeitssatz an.

- b** Gibt es eine holomorphe Funktion $f : \mathbb{C} \rightarrow \mathbb{C} \setminus \{0\}$, die den beiden Bedingungen $|f(z)| = 2$ für alle $z \in \partial\mathbb{D}$ und

$$\frac{1}{2\pi} \int_0^{2\pi} f(e^{it}) dt = 1$$

genügt? (3 Punkte)

Hinweis Maximumsprinzip für $\frac{1}{f}$ bzw. Minimumsprinzip für f .

Lösungen zu Thema Nr. 1

Lösungsvorschlag zur Aufgabe (Frühjahr 2015, T1A2)

Sei $f: Q \rightarrow \mathbb{E}$ eine biholomorphe Abbildung mit $f(-1+i) = 0$ und $g: Q \rightarrow \mathbb{E}$ eine weitere biholomorphe Abbildung mit $g(-1+i) = 0$. Dann ist

$$g \circ f^{-1}: \mathbb{E} \rightarrow \mathbb{E}$$

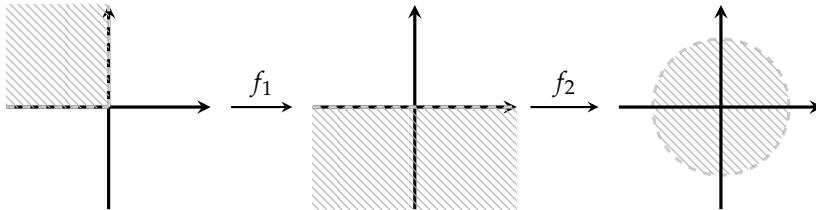
ebenfalls eine biholomorphe Abbildung mit $(g \circ f^{-1})(0) = 0$. Abbildungen dieser Art sind vollständig bekannt, es gibt nämlich ein $\xi \in \mathbb{C}$ mit $|\xi| = 1$, sodass

$$(g \circ f^{-1})(w) = g(f^{-1}(w)) = \xi w \quad \text{für alle } w \in \mathbb{E}.$$

Aufgrund der Bijektivität von f folgt daraus für $w = f(z)$ die Gleichung $g(z) = \xi f(z)$ für alle $z \in Q$. Wir bestimmen nun also solch eine Abbildung f , dann ist die Menge aller biholomorphen Abbildungen $g: Q \rightarrow \mathbb{E}$ mit $g(-1+i) = 0$ gegeben durch

$$\{g: Q \rightarrow \mathbb{E} \mid \exists \xi \in \partial \mathbb{E} : \forall z \in Q : g(z) = \xi f(z)\}.$$

Zur Konstruktion der Abbildung f gehen wir in mehreren Schritten vor, wie die folgende Abbildung veranschaulicht.



Um zunächst den zweiten Quadranten auf die untere Halbebene $\mathbb{H} = \{z \in \mathbb{C} \mid \operatorname{Im} z < 0\}$ abzubilden, bemerken wir, dass für $z = x + iy \in Q$ gilt, dass

$$z^2 = x^2 - y^2 + i2xy.$$

Wegen $x < 0$ und $y > 0$ ist somit $\operatorname{Im} z^2 = 2xy < 0$ und z^2 liegt in \mathbb{H} . Wir zeigen nun, dass

$$f_1: Q \rightarrow \mathbb{H}, \quad z \mapsto z^2$$

eine biholomorphe Abbildung ist. Die Holomorphie ist als Polynomfunktion klar. Für die *Injektivität* betrachte $z_1, z_2 \in Q$ mit $g_1(z_1) = g_1(z_2)$. Es folgt

$$z_1^2 = z_2^2 \quad \Leftrightarrow \quad z_1^2 - z_2^2 = 0 \quad \Leftrightarrow \quad (z_1 + z_2)(z_1 - z_2) = 0$$

Nehmen wir an, es wäre $z_1 + z_2 = 0$, also $z_1 = -z_2$. Wegen $z_1 \in Q$ würde aber folgen $\operatorname{Re} z_2 = -\operatorname{Re} z_1 > 0$, also $z_2 \notin Q$ – Widerspruch. Also muss $z_1 = z_2$ gelten.

Für die *Surjektivität* sei $w \in \mathbb{H}$ vorgegeben. Schreibe $w = re^{i\varphi}$ mit $r = |w|$ und $\varphi \in]\pi; 2\pi[$. Dann gilt wegen $\cos x < 0$ und $\sin x > 0$ für $x \in]\frac{\pi}{2}, \pi[$

$$\operatorname{Re} \sqrt{r} e^{i\frac{\varphi}{2}} = \sqrt{r} \cdot \cos\left(\frac{\varphi}{2}\right) < 0 \quad \text{und} \quad \operatorname{Im} \sqrt{r} e^{i\frac{\varphi}{2}} = \sqrt{r} \cdot \sin\left(\frac{\varphi}{2}\right) > 0$$

sowie $\left(\sqrt{r} e^{i\frac{\varphi}{2}}\right)^2 = r e^{i\varphi} = w$. Also ist $\sqrt{r} e^{i\frac{\varphi}{2}}$ ein Urbild von w in Q .

Im nächsten Schritt bilden wir nun \mathbb{H} auf \mathbb{E} ab. Dafür bestimmt man beispielsweise aus den Punkten

$$z_1 = -1, \quad z_2 = 0, \quad z_3 = 1, \quad w_1 = -1, \quad w_2 = i, \quad w_3 = 1$$

mithilfe des Doppelverhältnisses die Möbiustransformation

$$f_2: \mathbb{H} \rightarrow \mathbb{E}, \quad z \mapsto \frac{z+i}{iz+1}.$$

Als Komposition ergibt sich dann

$$f_2 \circ f_1(z) = \frac{z^2 + i}{iz^2 + 1}.$$

Wegen $(f_2 \circ f_1)(-1+i) = \frac{-i}{3}$ brauchen wir noch eine weitere Abbildung $f_3: \mathbb{E} \rightarrow \mathbb{E}$ mit $g(\frac{-i}{3}) = 0$. Dazu nimmt man beispielsweise

$$f_3: \mathbb{E} \rightarrow \mathbb{E}, \quad z \mapsto \frac{3z+i}{iz-3}.$$

Um $f_3 \circ f_2$ zu bestimmen, verwenden wir Matrizenkalkül: Wegen

$$\begin{pmatrix} 3 & i \\ i & -3 \end{pmatrix} \cdot \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix} = \begin{pmatrix} 2 & 4i \\ -2i & -4 \end{pmatrix} = 2 \cdot \begin{pmatrix} 1 & 2i \\ -i & -2 \end{pmatrix}$$

ist $(f_3 \circ f_2)(z) = \frac{z+2i}{-iz-2}$. Insgesamt erhalten wir daher

$$f(z) = (f_3 \circ f_2 \circ f_1)(z) = \frac{z^2 + 2i}{-iz^2 - 2}.$$

Lösungsvorschlag zur Aufgabe (Frühjahr 2015, T1A3)

- a Das charakteristische Polynom der homogenen Differentialgleichung ist

$$p = X^2 + 2X + 1 = (X + 1)^2.$$

Dieses hat eine doppelte Nullstelle -1 , also ist nach Satz 7.19 durch

$$\{e^{-t}, te^{-t}\}$$

ein Fundamentalsystem der homogenen Differentialgleichung gegeben. Um eine partikuläre Lösung λ_p des inhomogenen Systems zu finden, machen wir den Ansatz (vgl. die Tabelle auf Seite 456)

$$\lambda_p(t) = c_1 \cos 2t + c_2 \sin 2t.$$

Einsetzen ergibt

$$\begin{aligned} \cos 2t &\stackrel{!}{=} \lambda_p''(t) + 2\lambda_p'(t) + \lambda_p(t) = \\ &= -4c_1 \cos 2t - 4c_2 \sin 2t + 2(-2c_1 \sin 2t + 2c_2 \cos 2t) \\ &\quad + (c_1 \cos 2t + c_2 \sin 2t) = \\ &= (-3c_1 + 4c_2) \cos 2t + (-3c_2 - 4c_1) \cos 2t. \end{aligned}$$

Mittels Koeffizientenvergleich liest man daraus die Gleichungen

$$1 = -3c_1 + 4c_2 \quad \text{und} \quad 0 = -4c_1 - 3c_2$$

ab. Die zweite Gleichung liefert $c_1 = -\frac{3}{4}c_2$ und eingesetzt in die erste ergibt das

$$1 = \frac{9}{4}c_2 + 4c_2 = \frac{25}{4}c_2 \quad \Leftrightarrow \quad c_2 = \frac{4}{25}.$$

Daraus folgt dann $c_1 = -\frac{3}{25}$ und man erhält

$$\lambda_p(t) = -\frac{3}{25} \cos 2t + \frac{4}{25} \sin 2t.$$

Die allgemeine Lösung der Differentialgleichung hat dann die Form

$$\lambda(t) = c_3 e^{-t} + c_4 t e^{-t} - \frac{3}{25} \cos 2t + \frac{4}{25} \sin 2t$$

mit gewissen Koeffizienten $c_3, c_4 \in \mathbb{R}$. Damit λ beschränkt bleibt, muss $c_3 = c_4 = 0$ sein, d. h.

$$a = \lambda(0) = -\frac{3}{25} \quad \text{und} \quad b = \lambda'(0) = \frac{8}{25}.$$

b Damit alle reellen Lösungen unbeschränkt sind, muss die partikuläre Lösung der Gleichung unbeschränkt sein. Aufgrund der Tabelle auf Seite 456 vermuten wir, dass dies nur dann der Fall ist, wenn Resonanz vorliegt. Dazu müsste in diesem Fall $2i$ eine Nullstelle des charakteristischen Polynoms der Gleichung sein. Die entsprechende Gleichung lautet

$$(2i)^2 + 2ic + d = 0 \Leftrightarrow -4 + 2ic + d = 0 \Leftrightarrow c = 0 \text{ und } d = 4.$$

Behauptung: Die Gleichung hat genau dann keine beschränkte reelle Lösung, wenn $c = 0$ und $d = 4$ gilt.

Im Fall $c = 0$ und $d = 4$ hat das charakteristische Polynom die Eigenwerte $\pm 2i$, als Ansatz für eine partikuläre Lösung wählt man somit

$$\lambda_p(t) = tc_1 \cos(2t) + tc_2 \sin(2t).$$

Eine weitgehend analoge Rechnung zu oben liefert dann $\lambda_p(t) = \frac{1}{4}t \sin(2t)$. Damit ist die allgemeine Lösung der Gleichung gegeben durch

$$a \cos 2t + b \sin 2t + \frac{1}{4}t \sin 2t \quad \text{für } a, b \in \mathbb{R}.$$

Da der letzte Summand unbeschränkt ist, sind somit für $a, b \in \mathbb{R}$ alle Lösungen unbeschränkt.

Betrachten wir nun den Fall, dass $c \neq 0$ und $d \neq 0$ ist. Wir zeigen, dass es dann eine partikuläre Lösung in derselben Form wie in Teil **a** gibt. Der Ansatz $\lambda_p(t) = c_1 \cos(2t) + c_2 \sin(2t)$ liefert durch Einsetzen in die Gleichung analog zu vorher

$$\cos 2t = (da_1 + 2ca_2 - 4a_1) \cos(2t) + (da_2 - 2ca_1 - 4a_2) \sin(2t).$$

Daraus bekommt man das Gleichungssystem

$$\begin{aligned} 1 &= (d - 4)a_1 + 2c a_2 \\ 0 &= -2c a_1 + (d - 4)a_2. \end{aligned}$$

Die Determinante der Koeffizientenmatrix ist nun gegeben durch

$$\det \begin{pmatrix} d - 4 & 2c \\ -2c & d - 4 \end{pmatrix} = (d - 4)^2 + 4c^2.$$

Wegen $d \neq 4$ oder $c \neq 0$ ist diese positiv, also ist das Gleichungssystem eindeutig lösbar und wir erhalten eine partikuläre Lösung, die beschränkt ist.

Lösungsvorschlag zur Aufgabe (Frühjahr 2015, T1A5)

1. Schritt: kritische Punkte und isolierte Minima: Wir bestimmen zunächst den Gradienten von f :

$$(\nabla f)(x, y) = \begin{pmatrix} 2x - a \\ 2y \end{pmatrix}$$

Die kritischen Punkte sind genau diejenigen Punkte, an denen $(\nabla f)(x, y)$ verschwindet, d. h. die Lösungen der Gleichungen

$$2x - a = 0 \quad \text{und} \quad 2y = 0.$$

Auflösen ergibt den kritischen Punkt $(\frac{a}{2}, 0)$. Wegen

$$\frac{a}{2} + 0 \geq 1 \quad \Leftrightarrow \quad a \geq 2$$

ist dieser nur im Fall $a \geq 2$ in H enthalten. Tatsächlich ist in diesem Fall $f(\frac{a}{2}, 0)$ ein globales Minimum, denn es gilt für $(x, y) \in H$

$$f(x, y) = x^2 - ax + y^2 = (x - \frac{a}{2})^2 - \frac{a^2}{4} + y^2 \geq -\frac{a^2}{4} = \frac{a^2}{4} - \frac{a^2}{2} + 0 = f(\frac{a}{2}, 0).$$

2. Schritt: Randextrema: Für $a < 2$ liegt P nicht in H . In diesem Fall könnte es stattdessen ein Minimum auf dem Rand geben. Wir betrachten daher f eingeschränkt auf den Rand

$$\partial H = \{(x, y) \in \mathbb{R}^2 \mid x + y = 1\}.$$

Für einen Randpunkt $(x, y) \in \partial H$ ist $y = 1 - x$, d. h. dort ist

$$f_{|\partial H}(x, y) = g(x) = x^2 - ax + (1 - x)^2 = 2x^2 - (a + 2)x + 1.$$

Wo (und ob) diese Funktion ein Extremum besitzt, sehen wir an der ersten Ableitung:

$$g'(x_0) = 0 \quad \Leftrightarrow \quad 4x_0 - (a + 2) = 0 \quad \Leftrightarrow \quad x_0 = \frac{1}{4}(a + 2).$$

Der zugehörige y -Wert ist dann $y_0 = 1 - \frac{1}{4}(a + 2) = \frac{2-a}{4}$. Der Funktionswert berechnet sich zu

$$\begin{aligned} f(x_0, y_0) &= \left(\frac{a+2}{4}\right)^2 - a\left(\frac{a+2}{4}\right) + \left(\frac{2-a}{4}\right)^2 = \\ &= \frac{(a+2)^2}{16} - \frac{4a(a+2)}{16} + \frac{(2-a)^2}{16} = \frac{-2a^2 - 8a + 8}{16} = \\ &= -\frac{a^2 + 4a - 4}{8} = -\frac{a^2 + 4a + 4}{8} + \frac{8}{8} = -\frac{1}{8}(a+2)^2 + 1. \end{aligned}$$

Wir verwenden nun quadratische Ergänzung, um $f(x, y) \geq f(x_0, y_0)$ für beliebiges $(x, y) \in H$ zu zeigen. Wir berechnen:

$$\begin{aligned} f(x, y) &= x^2 - ax + y^2 = \\ &= \left(x - \frac{a+2}{4}\right)^2 + \frac{a+2}{2}x - \frac{(a+2)^2}{16} - ax + \left(y - \frac{2-a}{4}\right)^2 + \frac{2-a}{2}y - \left(\frac{2-a}{4}\right)^2 \geq \\ &\geq \frac{a+2}{2}x - \frac{(a+2)^2}{16} - ax + \frac{2-a}{2}y - \left(\frac{2-a}{4}\right)^2 \geq \\ &\geq \frac{2-a}{2}x + \frac{2-a}{2}y - \frac{a^2+4a+4}{16} - \frac{a^2-4a+4}{16} = \\ &= \frac{2-a}{2}(x+y) - \frac{2a^2+8}{16}. \end{aligned}$$

Nun wissen wir, dass $x+y \geq 1$ ist und wegen $a < 2$ ist $\frac{2-a}{2}$ positiv, sodass wir daraus $\frac{2-a}{2}(x+y) \geq \frac{2-a}{2}$ schlussfolgern können. Damit erhalten wir die Abschätzung

$$f(x, y) \geq \frac{2-a}{2} - \frac{2a^2+8}{16} = 1 - \frac{4a}{8} - \frac{a^2+4}{8} = 1 - \frac{1}{8}(a+2)^2 = f(x_0, y_0).$$

Tatsächlich ist also $f(x_0, y_0) = -\frac{1}{8}(a+2)^2 + 1$ ein globales Minimum von f . Die obige Abschätzung ist für $(x, y) \neq (x_0, y_0)$ sogar strikt, sodass (x_0, y_0) die einzige Stelle ist, an der das Minimum angenommen wird.

Lösungen zu Thema Nr. 2

Lösungsvorschlag zur Aufgabe (Frühjahr 2015, T2A1)

- a** Angenommen, es gibt eine solche Funktion h . Es gilt $3,4 \notin U$, denn

$$2 \cdot 4 + \frac{1}{1+4^2} > 2 \cdot 3 + \frac{1}{1+3^2} > 6 = \frac{12}{2} > \frac{11}{2}.$$

Laut Angabe ist $h(\mathbb{C}) \subseteq U$, also insbesondere $3,4 \notin h(\mathbb{C})$. Nach dem kleinen Satz von Picard muss daher h bereits konstant sein, also kann nicht $h(v) = \frac{i}{2} \neq 1 - i = h(w)$ gelten.

- b** Da f und g auf Ω holomorph sind, können wir beide Funktionen in Potenzreihen um $z_0 \in \Omega$ entwickeln:

$$f(z) = \sum_{k=0}^{\infty} a_k (z - z_0)^k \quad \text{und} \quad g(z) = \sum_{k=0}^{\infty} b_k (z - z_0)^k.$$

Für die Koeffizienten gilt $a_k = \frac{1}{k!} f^{(k)}(z_0)$ bzw. $b_k = \frac{1}{k!} g^{(k)}(z_0)$, sodass aus der Angabe

$$\begin{aligned} a_0 &= f(z_0) = 0, & a_1 &= f'(z_0) = 0, \\ b_0 &= g(z_0) = 0, & b_1 &= g'(z_0) = 0, & b_2 &= \frac{1}{2}g^{(2)}(z_0) \neq 0 \end{aligned}$$

folgt. Somit können wir

$$\begin{aligned} f(z) &= \sum_{k=2}^{\infty} a_k (z - z_0)^k = (z - z_0)^2 \sum_{k=0}^{\infty} a_{k+2} (z - z_0)^k \\ \text{und } g(z) &= (z - z_0)^2 \sum_{k=0}^{\infty} b_{k+2} (z - z_0)^k \end{aligned}$$

schreiben. Nun ist also

$$\begin{aligned} \lim_{z \rightarrow z_0} \frac{f(z)}{g(z)} &= \lim_{z \rightarrow z_0} \frac{(z - z_0)^2 \sum_{k=0}^{\infty} a_{k+2} (z - z_0)^k}{(z - z_0)^2 \sum_{k=0}^{\infty} b_{k+2} (z - z_0)^k} = \\ &= \lim_{z \rightarrow z_0} \frac{\sum_{k=0}^{\infty} a_{k+2} (z - z_0)^k}{\sum_{k=0}^{\infty} b_{k+2} (z - z_0)^k} = \frac{a_2}{b_2} = \frac{\frac{1}{2}f^{(2)}(z_0)}{\frac{1}{2}g^{(2)}(z_0)} = \frac{f^{(2)}(z_0)}{g^{(2)}(z_0)}. \end{aligned}$$

c Unter Verwendung der Kosinus-Reihe ist

$$\begin{aligned} F(z) &= \frac{1}{z^2} \cdot (1 - \cos z) = \frac{1}{z^2} \left(1 - \sum_{k=0}^{\infty} (-1)^k \frac{z^{2k}}{(2k)!} \right) = \\ &= -\frac{1}{z^2} \sum_{k=1}^{\infty} (-1)^k \frac{z^{2k}}{(2k)!} = \sum_{k=1}^{\infty} (-1)^{k+1} \frac{z^{2k-2}}{(2k)!} = \\ &= \sum_{k=0}^{\infty} (-1)^k \frac{z^{2k}}{(2(k+1))!} \end{aligned}$$

An dieser Laurentreihen-Entwicklung sieht man, dass der Hauptteil verschwindet und es sich folglich bei 0 um eine hebbare Singularität handelt.

Lösungsvorschlag zur Aufgabe (Frühjahr 2015, T2A2)

- a** Der Hauptzweig des Logarithmus ist definiert als $\text{Log}(re^{i\varphi}) = \ln r + i\varphi$. Sei nun $x \in]0, \infty[$. Es ist dann $x+i = \sqrt{1+x^2}e^{i\varphi}$ und $x-i = \sqrt{1+x^2}e^{-i\varphi}$ mit $\varphi = \arctan \frac{1}{x}$. Damit gilt

$$\begin{aligned}\text{Log}(x+i) - \text{Log}(x-i) &= \ln \sqrt{1+x^2} + i\varphi - (\ln \sqrt{1+x^2} - i\varphi) = 2i\varphi = \\ &= \text{Log} e^{2i\varphi} = \text{Log} \frac{\sqrt{1+x^2}e^{i\varphi}}{\sqrt{1+x^2}e^{-i\varphi}} = \text{Log} \frac{x+i}{x-i}.\end{aligned}$$

Somit gilt die Gleichheit zumindest auf der positiven reellen Achse. Da es sich bei $]0, \infty[$ um eine nicht-diskrete Menge handelt, folgt die Aussage aus dem Identitätssatz.

- b** Man zeigt zunächst, dass die Partialbruchzerlegung

$$\frac{1}{1+\xi^2} = \frac{i/2}{\xi+i} - \frac{i/2}{\xi-i}$$

wahr ist. Damit berechnet man nun

$$\begin{aligned}f(z) &= \frac{i}{2} \int_{[1, \frac{z}{2}]} \frac{1}{\xi+i} d\xi - \frac{i}{2} \int_{[1, \frac{z}{2}]} \frac{1}{\xi-1} d\xi = \\ &= \frac{i}{2} [\text{Log}(\xi+i)]_1^{z/2} - \frac{i}{2} [\text{Log}(\xi-1)]_1^{z/2} = \\ &= \frac{i}{2} (\text{Log}(\frac{z}{2}+i) - \text{Log}(\frac{z}{2}-i) - \text{Log}(1+i) + \text{Log}(1-i)) = \\ &\stackrel{\text{a}}{=} \frac{i}{2} \text{Log} \left(\frac{z+2i}{z-2i} \right) - \frac{i}{2} \text{Log} \left(\frac{1+i}{1-i} \right)\end{aligned}$$

Den zweiten Summanden berechnen wir getrennt:

$$\frac{1+i}{1-i} = \frac{(1+i)^2}{(1-i)(1+i)} = \frac{1+2i+i^2}{1-i^2} = \frac{2i}{2} = i$$

Es ist $i = e^{i\pi/2}$ und somit $\text{Log}(i) = \ln 1 + i\frac{\pi}{2} = i\frac{\pi}{2}$. Also ist insgesamt

$$f(z) = \frac{i}{2} \text{Log} \left(\frac{z+2i}{z-2i} \right) - \frac{i}{2} \cdot i \frac{\pi}{2} = \frac{i}{2} \text{Log} \left(\frac{z+2i}{z-2i} \right) + \frac{\pi}{4}.$$

Lösungsvorschlag zur Aufgabe (Frühjahr 2015, T2A3)

a Für alle $z \in \partial K$ gilt $|z| = 1$ und damit die Abschätzung

$$|rze^z| = r \cdot |e^z| = r \cdot e^{\operatorname{Re} z}.$$

Aus $|z| = 1$ folgt insbesondere $|\operatorname{Re}(z)| \leq 1$, d. h. $-1 \leq \operatorname{Re} z \leq 1$. Also gilt weiter

$$r \cdot e^{\operatorname{Re} z} \geq r \cdot e^{-1} > e \cdot e^{-1} = 1 = |-1|.$$

Aus dem Satz von Rouché 6.35 folgt nun, dass rze^z und $rze^z - 1$ gleich viele Nullstellen in K haben. Wegen

$$|rze^z| = 0 \Leftrightarrow r|z| \cdot e^{\operatorname{Re}(z)} = 0 \Leftrightarrow |z| = 0 \Leftrightarrow z = 0$$

ist dies genau eine Nullstelle. Daher gibt es genau ein $z \in K$ mit

$$rze^z - 1 = 0 \Leftrightarrow rze^z = 1.$$

b Es gilt

$$z^2 + 2z + 2 = (z+1)^2 + 1 = (z+1)^2 - i^2 = (z+1-i)(z+1+i).$$

Definiere nun für jedes $t \in \mathbb{R}$ die Funktion

$$g_t: \mathbb{C} \setminus \{0, -1+i, -1-i\}, \quad z \mapsto \frac{e^{zt}}{z^2(z+1-i)(z+1+i)}.$$

Wir wollen im Folgenden (natürlich) den Residuensatz anwenden, weswegen wir zunächst die Residuen von f berechnen. Wegen

$$\lim_{z \rightarrow 0} |g_t(z)| = \lim_{z \rightarrow 0} |zg_t(z)| = \infty \quad \text{und} \quad \lim_{z \rightarrow 0} z^2 g_t(z) = \frac{1}{2} \neq \infty$$

hat g_t bei 0 ein Pol zweiter Ordnung. Daher ist

$$\begin{aligned} \operatorname{Res}(g_t; 0) &= \left(\frac{d}{dz} z^2 g_t(z) \right)_{|z=0} = \left(\frac{te^{zt}(z^2 + 2z + 2) - (2z + 2)e^{zt}}{(z^2 + 2z + 2)^2} \right)_{|z=0} = \\ &= \frac{2t - 2}{4} = \frac{t-1}{2}. \end{aligned}$$

Genauso sieht man anhand von

$$\lim_{z \rightarrow -1-i} |g_t(z)| = \infty, \quad \lim_{z \rightarrow -1-i} (z+1+i)g_t(z) = \frac{e^{t(-1-i)}}{(-1-i)^2(-2i)} = \frac{1}{4}e^{-t-it}$$

sowie

$$\lim_{z \rightarrow -1+i} |g_t(z)| = \infty, \quad \lim_{z \rightarrow -1+i} (z + 1 - i) g_t(z) = \frac{e^{t(-1+i)}}{(-1+i)^2 \cdot 2i} = \frac{1}{4} e^{-t+it},$$

dass die beiden anderen Singularitäten Pole erster Ordnung mit $\operatorname{Res}(g_t; -1-i) = \frac{1}{4} e^{-t-it}$ und $\operatorname{Res}(g_t; -1+i) = \frac{1}{4} e^{-t+it}$ sind.

Wir erhalten also

$$\begin{aligned} f(t) &= \frac{1}{2\pi} \int_{\gamma} g_t(z) dz = \operatorname{Res}(g_t; 0) + \operatorname{Res}(g_t; -1-i) + \operatorname{Res}(g_t; -1+i) = \\ &= \frac{t-1}{2} + \frac{1}{4} e^{-t-it} + \frac{1}{4} e^{-t+it} = \frac{t-1}{2} + \frac{1}{4} e^{-t} (e^{-it} + e^{it}) = \\ &= \frac{t-1}{2} + \frac{1}{4} e^{-t} \cdot 2 \cos t = \frac{t-1}{2} + \frac{1}{2} e^{-t} \cdot \cos t. \end{aligned}$$

Dabei folgt die vorletzte Gleichung mithilfe der Euler-Identität aus

$$e^{it} + e^{-it} = \cos t + i \sin t + \cos(-t) + i \sin(-t) = 2 \cos t.$$

An der obigen Darstellung erkennt man direkt, dass f eine reellwertige \mathcal{C}^∞ -Funktion ist. Zudem ist

$$f(0) = -\frac{1}{2} + \frac{1}{2} e^0 \cos 0 = 0.$$

Lösungen zu Thema Nr. 3

Lösungsvorschlag zur Aufgabe (Frühjahr 2015, T3A2)

Sei

$$A(t) = \begin{pmatrix} e^t & 1 \\ 1 & e^t \end{pmatrix}.$$

Es gilt nun, falls $M: I \rightarrow \mathcal{M}_{n \times n}(\mathbb{R})$ eine Matrix-wertige Funktion mit $M(t) \cdot M'(t) = M'(t) \cdot M(t)$ ist, dass dann $e^{M(t)} = M'(t) \cdot e^{M(t)}$ gilt (Kettenregel für Matrizen). Setze $M(t) = \int_0^t A(s) ds$, dann überprüft man $M(t) \cdot A(t) = A(t) \cdot M(t)$. Es gilt also

$$\frac{d}{dt} e^{M(t)} = M'(t) e^{M(t)} = A(t) e^{M(t)}.$$

Somit liefern beide Spalten von $e^{M(t)}$ Lösungen der angegebenen Differentialgleichung. Diese sind außerdem linear unabhängig, denn $e^{M(t)}$ ist invertierbar

(die Inverse ist $e^{-M(t)}$), sodass $\det e^{M(t)} \neq 0$. Also ist $e^{M(t)}$ eine Fundamentalmatrix der Differentialgleichung und jede Lösung des Anfangswertproblems ist gegeben durch

$$e^{M(t)} \left(e^{M(0)} \right)^{-1} \begin{pmatrix} x_0 \\ y_0 \end{pmatrix} = e^{M(t)} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} x_0 \\ y_0 \end{pmatrix} = e^{M(t)} \begin{pmatrix} x_0 \\ y_0 \end{pmatrix}.$$

Daher ist

$$\begin{pmatrix} f(t) & g(t) \\ g(t) & f(t) \end{pmatrix} = M(t) = \begin{pmatrix} e^t - 1 & t \\ t & e^t - 1 \end{pmatrix}.$$

Lösungsvorschlag zur Aufgabe (Frühjahr 2015, T3A4)

- a** Sei $f(z) = \sum_{k=-1}^{\infty} a_k z^k$ eine auf $\mathbb{D} \setminus \{0\}$ gültige Laurent-Reihenentwicklung von f um 0. Der Nebenteil $h(z) = \sum_{k=0}^{\infty} a_k z^k$ definiert dann eine ganze Funktion. Da \mathbb{C} einfach zusammenhängend ist, besitzt h eine Stammfunktion $H: \mathbb{C} \rightarrow \mathbb{C}$ und wir haben

$$\int_{\gamma_\varepsilon} h(\xi) d\xi = H(\gamma_\varepsilon(\alpha)) - H(\gamma_\varepsilon(0)) = H(\varepsilon e^{i\alpha}) - H(\varepsilon).$$

Da H als holomorphe Funktion stetig ist, ist weiter

$$\lim_{\varepsilon \rightarrow 0} H(\varepsilon e^{i\alpha}) - H(\varepsilon) = H(0) - H(0) = 0,$$

also verschwindet das Integral über h . Für den Hauptteil berechnen wir

$$\int_{\gamma_\varepsilon} \frac{a_{-1}}{\xi} d\xi = \int_0^\alpha \frac{a_{-1} i \varepsilon e^{it}}{\varepsilon e^{it}} dt = \int_0^\alpha i a_{-1} dt = i a_{-1} \alpha = i \alpha \operatorname{Res}(0; f).$$

Zusammen ergibt dies

$$\lim_{\varepsilon \rightarrow 0} \int_{\gamma_\varepsilon} f(\xi) d\xi = \lim_{\varepsilon \rightarrow 0} \int_{\gamma_\varepsilon} \frac{a_{-1}}{\xi} + h(\xi) d\xi = i \alpha \operatorname{Res}(0; f).$$

- b** Sei $\zeta \in \partial\mathbb{D}$. Ist $\operatorname{Im} \zeta \geq 0$, so ist $\operatorname{Im} -\zeta \leq 0$, sodass $|f(\zeta)| \leq m_1$ und $|f(-\zeta)| \leq m_2$ ist. Im Fall $\operatorname{Im} \zeta \leq 0$ folgt analog $|f(\zeta)| \leq m_2$ und $|f(-\zeta)| \leq m_1$. In beiden Fällen gilt damit

$$|f(\zeta)f(-\zeta)| \leq m_1 m_2.$$

Da $f(z)f(-z)$ auf \mathbb{D} holomorph und auf $\overline{\mathbb{D}}$ stetig ist, nimmt sie nach dem Maximumsprinzip für beschränkte Mengen auf $\partial\mathbb{D}$ ein Betragsmaximum

an. Also gilt für alle $z \in \mathbb{D}$ die Abschätzung

$$|f(z)f(-z)| \leq m_1 m_2.$$

Insbesondere also $|f(0)|^2 = |f(0)f(0)| \leq m_1 m_2$ und somit $|f(0)| \leq \sqrt{m_1 m_2}$.

Lösungsvorschlag zur Aufgabe (Frühjahr 2015, T3A5)

- a** Für alle $z \in \mathbb{D} \setminus \{0\}$ gilt laut Angabe

$$|f(z)|^3 = |z| < 1 \Rightarrow |f(z)| = |z|^{1/3} < 1 \quad (\in \mathbb{R}),$$

somit ist 0 nach dem Riemannschen Hebbarkeitssatz eine hebbare Singularität von f . Sei $g: \mathbb{D} \rightarrow \mathbb{C}$ eine holomorphe Fortsetzung von f , dann folgt aus der Stetigkeit von $z \mapsto z^3$, dass

$$g(0)^3 = \lim_{z \rightarrow 0} g(z)^3 = \lim_{z \rightarrow 0} f(z)^3 = \left(\lim_{z \rightarrow 0} f(z) \right)^3 = \left(\lim_{z \rightarrow 0} z \right)^3 = 0,$$

also $g(0) = 0$. Holomorphe Funktionen sind unendlich oft stetig differenzierbar. Aus der Kettenregel erhält man daher

$$\frac{d}{dz} g^3(z) = 3g(z)^2 \cdot g'(z)$$

und damit $\left(\frac{d}{dz} g^3 \right)(0) = 3g(0)^2 g'(0) = 0$. Andererseits muss aufgrund der Stetigkeit auch

$$\left(\frac{d}{dz} g^3 \right)(0) = \lim_{z \rightarrow 0} \frac{d}{dz} g^3(z) = \lim_{z \rightarrow 0} \frac{d}{dz} f^3(z) = \lim_{z \rightarrow 0} \frac{d}{dz} z = \lim_{z \rightarrow 0} 1 = 1$$

sein. Widerspruch.

- b** Nach dem Minimumsprinzip für beschränkte Gebiete hat f eine Nullstelle in \mathbb{D} oder $f|_{\overline{\mathbb{D}}}$ nimmt auf $\partial\mathbb{D}$ ein Betragsminimum an. Da nach Voraussetzung $f(z) \neq 0$ für alle $z \in \mathbb{C}$ gilt, muss es also $\xi \in \partial\mathbb{D}$ geben, sodass

$$|f(z)| \geq |f(\xi)| = 2 \quad \text{für alle } z \in \overline{\mathbb{D}}$$

gilt. Das Maximumsprinzip für beschränkte Gebiet besagt, dass $f|_{\overline{\mathbb{D}}}$ auf $\partial\mathbb{D}$ auch sein Betragsmaximum annimmt, d. h. es gibt $\zeta \in \partial\mathbb{D}$, sodass

$$|f(z)| \leq |f(\zeta)| = 2 \quad \text{für alle } z \in \overline{\mathbb{D}}.$$

Beide Abschätzungen zusammen ergeben $|f(z)| = 2$ für alle $z \in \mathbb{D}$. Insbesondere hat $|f(z)|$ ein Minimum in 0. Aus dem Minimumsprinzip erhält man nun, dass f konstant auf \mathbb{D} (und damit nach Identitätssatz auf ganz \mathbb{C}) sein muss. Es folgt

$$1 = \frac{1}{2\pi} \int_0^{2\pi} f(e^{it}) dt = \frac{1}{2\pi} f(0) \int_0^{2\pi} dt = \frac{1}{2\pi} f(0) \cdot 2\pi = f(0).$$

Allerdings ist $|f(0)| = 2 \neq 1$. Widerspruch, also kann es eine solche Funktion f nicht geben.

Prüfungstermin: Herbst 2015

Thema Nr. 1 (Aufgabengruppe)

Aufgabe 1 → S. 584

Es sei \mathbb{D} die offene komplexe Einheitskreisscheibe. Darüber hinaus seien f und g auf einer Umgebung von $\overline{\mathbb{D}}$ holomorphe Funktionen, die keine Nullstelle in \mathbb{D} besitzen. Zeigen Sie: Gilt $|f| = |g|$ auf $\partial\mathbb{D}$, so gibt es eine Konstante c mit $|c| = 1$, so dass $f = cg$ auf $\overline{\mathbb{D}}$.

Hinweis Man nehme zunächst an, dass auch auf $\partial\mathbb{D}$ keine Nullstellen von g liegen. (6 Punkte)

Aufgabe 2 → S. 585

- a** Existiert eine Folge von Punkten in der offenen oberen komplexen Halbebene, die alle Punkte von \mathbb{R} und keine anderen Häufungswerte hat? Geben Sie eine ausführlich begründete Antwort. (3 Punkte)
- b** Zeigen Sie, dass es eine Folge von Punkten in der offenen komplexen Einheitskreisscheibe gibt, die genau die Punkte der (komplexen) Einheitskreislinie als Häufungswerte hat, und weisen Sie nach, dass diese Eigenschaften tatsächlich erfüllt sind. (3 Punkte)

Aufgabe 3 → S. 586

Beweisen Sie, dass jedes Polynom mit komplexen Koeffizienten vom Grad $n \geq 1$, $p(z) = a_0 + a_1z + \dots + a_{n-1}z^{n-1} + z^n$, genau n Nullstellen in \mathbb{C} besitzt (mit Vielfachheit gezählt) mithilfe

- a** des Satzes von Rouché, (2 Punkte)
- b** des Null- und Polstellen zählenden Integrals, indem Sie den Quotienten

$$\frac{p'(z)}{p(z)} =: \frac{n}{z}(1 + g(z))$$

betrachten und die so definierte Funktion g geeignet abschätzen. (4 Punkte)

Aufgabe 4 → S. 438

Es sei $A: \mathbb{R} \rightarrow \mathbb{R}^{n \times n}$ eine stetige, matrixwertige Funktion. Betrachten Sie die zugehörige Differentialgleichung

$$\dot{x} = A(t)x. \quad (1)$$

- a** Es seien $x_1(t), \dots, x_n(t), t \in \mathbb{R}$, Lösungen von (1). Ferner seien für ein $t_0 \in \mathbb{R}$ die Vektoren $x_1(t_0), \dots, x_n(t_0)$ im \mathbb{R}^n linear unabhängig. Zeigen Sie, dass dann für alle $t_1 \in \mathbb{R}$ die Vektoren $x_1(t_1), \dots, x_n(t_1)$ im \mathbb{R}^n linear unabhängig sind.

(2 Punkte)

Hinweis Benutzen Sie das Superpositionsprinzip für lineare homogene Differentialgleichungen oder benutzen Sie die Differentialgleichung für Wronski-Determinanten.

(2 Punkte)

- b** Erklären Sie die Begriffe Fundamentalmatrix und Übergangsmatrix (auch Transitionsmatrix oder Hauptfundamentalmatrix genannt). Wie erhält man aus Teil **a** eine Fundamentalmatrix und wie lässt sich die Lösung von **a** mit Anfangswert $x(t_0) = x_0 \in \mathbb{R}^n, t_0 \in \mathbb{R}$, mithilfe der Übergangsmatrix ausdrücken?

(2 Punkte)

- c** Zeigen Sie: Sind $\Phi_1(t), \Phi_2(t), t \in \mathbb{R}$, Fundamentalmatrizen, so existiert eine Matrix $C \in \mathbb{R}^{n \times n}$ mit

$$\Phi_1(t) = \Phi_2(t)C, t \in \mathbb{R}.$$

(2 Punkte)

Aufgabe 5 → S. 587

Betrachten Sie die Differentialgleichung

$$\ddot{y}(t) + 2c\dot{y}(t) + y(t) = 0 \quad (2)$$

mit einer Konstanten $c > 0$.

- a** Zeigen Sie, dass in allen drei Fällen $c^2 - 1 > 0, c^2 - 1 = 0$ und $c^2 - 1 < 0$ die Differentialgleichung asymptotisch stabil ist.

(2 Punkte)

- b** Sei $y(t)$ Lösung von (2) zum Anfangswert $(y(t_0), \dot{y}(t_0)) = (y_0, y_1) \in \mathbb{R}^2, t_0 \in \mathbb{R}$. Bestimmen Sie $\lim_{t \rightarrow \infty} y(t)$.

(2 Punkte)

- c** Bestimmen Sie im Fall $c^2 - 1 < 0$ die Lösung zu den Anfangsbedingungen

$$y(0) = 1, \dot{y}(0) = 0.$$

Hierbei ist die Abkürzung $a := \sqrt{1 - c^2}$ nützlich.

(2 Punkte)

Thema Nr. 2
(Aufgabengruppe)

Aufgabe 1 → S. 262

Wir betrachten die Funktion

$$f: D = \{(x, y) \in \mathbb{R}^2 : x \leq 0, y < 0\} \cup \{(0, 0)\} \rightarrow \mathbb{R}, \\ f(x, y) := (y+1)e^x - e^y$$

- a Geben Sie an, welche Punkte in \mathbb{R}^2 innere Punkte oder Randpunkte von D sind. Ist D offen oder abgeschlossen? Begründen Sie Ihrer Antwort. (1 Punkt)
- b Bestimmen Sie Gradienten und Hessematrix von f in allen inneren Punkte von D . (2 Punkte)
- c Welcher Punkt im Inneren von D ist eine lokale Extremstelle und von welchem Typ ist er? Begründen Sie Ihre Antwort. (1 Punkt)
- d Welcher Randpunkt ist eine lokale Extremstelle von f ? Begründen Sie Ihre Antwort. (2 Punkte)

Aufgabe 2 → S. 458

Betrachten Sie die Differentialgleichung

$$y''' - 2y'' + y' = e^{2x}.$$

- a Bestimmen Sie ein Fundamentalsystem für die zugehörige homogene Differentialgleichung. (2 Punkte)
- b Bestimmen Sie mit einem geeigneten Ansatz eine spezielle Lösung der inhomogenen Gleichung und geben Sie damit die allgemeine Lösung an. (2 Punkte)
- c Bestimmen Sie die Lösung des zugehörigen Anfangswertproblems mit $y(0) = y'(0) = y''(0) = 0$. (2 Punkte)

Aufgabe 3 → S. 414

Betrachten Sie das Anfangswertproblem

$$y' = y^2, \quad y(0) = 1. \tag{3}$$

- a Wir betrachten die Picard-Iteration mit der Startfunktion $y_0(x) = 1$. Zeigen Sie durch vollständige Induktion, dass die n -te Iterierte die Gestalt

$$y_n(x) = 1 + x + \dots + x^n + x^{n+1}r_n(x)$$

besitzt, wobei r_n ein Polynom ist. Finden Sie damit eine Potenzreihe, die (3) löst. (4 Punkte)

- b** In welchem Intervall $I \subseteq \mathbb{R}$ konvergiert diese Reihe? (1 Punkt)
- c** Bestimmen Sie die maximale Lösung des Anfangswertproblems (3). Auf welchem Intervall ist sie definiert? (1 Punkt)

Aufgabe 4 → S. 589

- a** Zeigen Sie, dass es keine biholomorphe Abbildung $f: \mathbb{C} \rightarrow \mathcal{D} := \{z \in \mathbb{C} : \operatorname{Re} z \geq 0\}$ gibt. (3 Punkte)
- b** Sei $\Omega \subseteq \mathbb{C}$ ein nichtleeres Gebiet. Bestimmen Sie alle holomorphen Funktionen $f: \Omega \rightarrow \Omega$, die der Gleichung $f \circ f = f$ genügen. (3 Punkte)

Aufgabe 5 → S. 590

Auf dem Gebiet

$$\Omega := \{z \in \mathbb{C} : |\operatorname{Re} z| < \pi\}$$

betrachten wir die meromorphe Funktion

$$f(z) := \frac{1}{(z + \frac{\pi}{2}) \cdot \cos z}.$$

- a** Bestimmen Sie alle Singularitäten von f in Ω und geben Sie jeweils den Typ an. (1 Punkt)
- b** Berechnen Sie die Residuen von f in allen Polstellen. (2 Punkte)
- c** Hat die Funktion f eine Stammfunktion? (1 Punkt)
- d** Bestimmen Sie $c \in \mathbb{C}$, so dass die Funktion $f(z) + c \frac{1}{z - \frac{\pi}{2}}$ auf Ω eine Stammfunktion besitzt. (2 Punkte)

Begründen Sie jeweils alle Antworten auf die Teilaufgaben.

Thema Nr. 3
(Aufgabengruppe)

Aufgabe 1 → S. 591

Gegeben sei die Funktion

$$f: \mathbb{C} \setminus \{0, -1, -1+i\} \rightarrow \mathbb{C} \quad f(z) = \frac{z}{(z^2 + z)(z + 1 - i)^2}.$$

$\gamma(r)$ bezeichne den Weg entlang der Kreislinie mit Mittelpunkt 0 und Radius $r > 0$ mit einem Umlauf in positiver Richtung. Bestimmen Sie für alle Werte $r \in \mathbb{R}^+ \setminus \{1, \sqrt{2}\}$ den Wert des Integrales

$$W(r) := \int_{\gamma(r)} f(z) dz.$$

(6 Punkte)

Aufgabe 2 → S. 592

- a Geben Sie die Definitionen für die Begriffe "isolierte Singularität", "hebbare Singularität", "Polstelle" sowie "wesentliche Singularität" an. (2 Punkte)
- b Bestimmen Sie Lage und Art aller isolierten Singularitäten der Funktion $h: \mathcal{D} \rightarrow \mathbb{C}$ gegeben durch

$$h(z) = \frac{z}{z-2} \exp\left(\sin\left(\frac{z-1}{z^2-z}\right)\right),$$

wobei $\mathcal{D} \subseteq \mathbb{C}$ den maximal möglichen Definitionsbereich der Funktion bezeichnet.

Achten Sie jeweils bei Ihrer Entscheidung über die Art der Singularitäten auf eine ausführliche Begründung! (4 Punkte)

Aufgabe 3 → S. 594

Wir betrachten die Differentialgleichung

$$f' = f(f-1)(f+1)$$

für eine reellwertige Funktion f in einer reellen Veränderlichen.

- a Zeigen Sie unter Nennung geeigneter Sätze, dass diese Differentialgleichung für jedes $f_0 \in \mathbb{R}$ eine eindeutige maximale Lösung f mit $f(0) = f_0$ besitzt. (1 Punkt)

- b** Sei nun $f_0 < 1$. Zeigen Sie, dass für keine reelle Zahl a mit $a > 1$ ein t im Definitionsbereich von f existiert, so dass $f(t) = a$ gilt. (2 Punkte)
- c** Sei $f_0 > 1$. Zeigen Sie, dass für jede reelle Zahl a mit $a > 1$ ein t im Definitionsbereich von f mit $f(t) = a$ existiert. (3 Punkte)

Aufgabe 4 → S. 596

- a** Es sei $f: \mathbb{C} \rightarrow \mathbb{C}$ eine ganze Funktion. Für ein $M \in \mathbb{R}^+$ und ein $\alpha \in \mathbb{R}$ gelte:

$$|f(z)| \leq M|z|^\alpha \quad \forall z \in \mathbb{C}.$$

Zeigen Sie: $f^{(n)}(0) = 0$ für alle $n \in \mathbb{N}_0$ mit $n > \alpha$, hierbei bezeichne $f^{(n)}$ die n -te Ableitung von f , $f^{(0)} = f$. (3 Punkte)

- b** Es sei $n_0 \in \mathbb{N}_0$, $p: \mathbb{C} \rightarrow \mathbb{C}$ eine ganze Funktion mit $p^{(n)}(0) = 0$ für alle $n > n_0$. Zeigen Sie: p ist ein Polynom vom Grad n_0 . (2 Punkte)
- c** f erfülle die Voraussetzungen von Aufgabenteil **a**. Zeigen Sie: f ist entweder konstant oder hat mindestens eine Nullstelle. (1 Punkt)

Aufgabe 5 → S. 264

Gegeben sei der Ellipsenrand $E \subset \mathbb{R}^2$ durch $(x, y) \in E \Leftrightarrow x^2 + 2y^2 = 2$ sowie die Funktion $f: \mathbb{R}^2 \rightarrow \mathbb{R}$ durch $f(x, y) = x^3 - 3y^4$.

Begründen Sie, warum f sein Maximum und Minimum auf E annimmt. Bestimmen Sie sodann den maximalen sowie den minimalen Wert, den $f(x, y)$ unter der Nebenbedingung $(x, y) \in E$ annimmt und diejenigen Stellen, an denen das globale Maximum und das globale Minimum angenommen wird. (6 Punkte)

Lösungen zu Thema Nr. 1

Lösungsvorschlag zur Aufgabe (Herbst 2015, T1A1)

Wir nehmen zunächst an, dass g keine Nullstellen auf $\partial\mathbb{D}$ hat. Dies bedeutet auch, dass f keine Nullstellen auf $\partial\mathbb{D}$ hat. Somit ist auch

$$\frac{f}{g}: \overline{\mathbb{D}} \rightarrow \mathbb{C}$$

eine wohldefinierte, holomorphe Funktion, die auf $\overline{\mathbb{D}}$ keine Nullstellen hat. Diese nimmt nach dem Minimums- bzw. Maximumsprinzip für beschränkte Gebiete daher ihr Betragsminimum bzw. -maximum auf $\partial\mathbb{D}$ an. Laut Angabe ist

$$|f(z)| = |g(z)| \Leftrightarrow \left| \frac{f(z)}{g(z)} \right| = 1 \quad \text{für alle } z \in \partial\mathbb{D},$$

also fallen Minimum und Maximum von $\frac{f}{g}$ zusammen, sodass $\left| \frac{f}{g} \right|$ bereits konstant auf $\overline{\mathbb{D}}$ sein muss. Insbesondere ist $0 \in \mathbb{D}$ ein lokales Maximum, sodass laut dem Maximumsprinzip auch $\frac{f}{g}$ konstant ist. Also gibt es $c \in \mathbb{C}$, sodass

$$\frac{f(z)}{g(z)} = c \Leftrightarrow f(z) = cg(z) \quad \text{für alle } z \in \overline{\mathbb{D}}$$

gilt. Zudem gilt $1 = \left| \frac{f(1)}{g(1)} \right| = |c|$.

Betrachten wir nun den Fall, dass g eine Nullstelle ξ auf $\partial\mathbb{D}$ besitzt. Es ist dann auch $|f(\xi)| = |g(\xi)| = 0$, sodass $f(\xi) = 0$. Weil f und g keine Nullstellen in \mathbb{D} haben, sind sie nicht die Nullfunktion, sodass 0 eine Nullstelle von endlicher Ordnung ist. Also gibt es holomorphe Funktionen $f_1, g_1: \overline{\mathbb{D}} \rightarrow \mathbb{C}$ mit

$$f(z) = (z - \xi)^n f_1(z) \quad \text{und} \quad g(z) = (z - \xi)^m g_1(z)$$

für alle $z \in \overline{\mathbb{D}}$ und $f_1(\xi) \neq 0 \neq g_1(\xi)$. Sei o. B. d. A. $n \leq m$. Für $z \in \partial\mathbb{D} \setminus \{\xi\}$ gilt also

$$|(z - \xi)^n f_1(z)| = |(z - \xi)^m g_1(z)| \Leftrightarrow |f_1(z)| = |(z - \xi)^{m-n} g_1(z)|.$$

Angenommen, es ist $n < m$. Dann folgt aus der Stetigkeit von f_1 , dass

$$|f_1(\xi)| = \lim_{z \rightarrow \xi} |f_1(z)| = \lim_{z \rightarrow \xi} |(z - \xi)^{m-n} g_1(z)| = 0$$

im Widerspruch zu $f_1(\xi) \neq 0$. Somit muss $n = m$ gelten und wir erhalten, dass $\frac{f(z)}{g(z)} = \frac{(z - \xi)^n f_1(z)}{(z - \xi)^n g_1(z)}$ eine hebbare Singularität in ξ hat und $\lim_{z \rightarrow \xi} \frac{f(z)}{g(z)} \neq 0$

gilt. Da ξ als beliebige Nullstelle von g vorgegeben war, kann $\frac{f}{g}$ in allen Singularitäten auf $\partial\mathbb{D}$ in dieser Weise holomorph fortgesetzt werden. Für die holomorphe Fortsetzung kann nun wie in Teil **a** verfahren werden, da ihr Nenner keine Nullstellen in $\partial\mathbb{D}$ mehr hat.

Lösungsvorschlag zur Aufgabe (Herbst 2015, T1A2)

- a** Eine solche Folge gibt es (!). Da \mathbb{Q} abzählbar ist, gibt es eine Folge $(a_n)_{n \in \mathbb{N}}$, die alle rationalen Zahlen durchläuft. Da andererseits \mathbb{Q} dicht in \mathbb{R} liegt, liegen in der Umgebung jeder reellen Zahl unendlich viele rationale Zahlen, sodass jede reelle Zahl ein Häufungspunkt der Folge a_n ist. Betrachte nun die Folge

$$(b_n)_{n \in \mathbb{N}} \quad \text{mit} \quad b_n = a_n + \frac{i}{n}.$$

Da $\frac{1}{n} > 0$ für alle $n \in \mathbb{N}$ gilt, verläuft diese Folge in der oberen Halbebene.

Ist nun $r \in \mathbb{R}$, so gibt es eine Teilfolge $(a_n)_{n \in I}$ von $(a_n)_{n \in \mathbb{N}}$, die gegen r konvergiert. Die Folge $(b_n)_{n \in I}$ konvergiert dann ebenfalls gegen r , d. h. r ist ein Häufungspunkt von $(b_n)_{n \in \mathbb{N}}$.

Andererseits kann kein anderer Punkt $z \in \mathbb{C} \setminus \mathbb{R}$ ein Häufungspunkt von $(b_n)_{n \in \mathbb{N}}$ sein. Gilt $\operatorname{Im} z < 0$, so wähle $0 < \varepsilon < -\operatorname{Im} z$. Dann ist $B_\varepsilon(z) \cap \{b_n \mid n \in \mathbb{N}\} = \emptyset$, d. h. z kann kein Häufungspunkt von $(b_n)_{n \in \mathbb{N}}$ sein. Betrachte nun den Fall $\operatorname{Im} z > 0$. Wähle $0 < \varepsilon < \operatorname{Im} z$, dann gibt es ein $N \in \mathbb{N}$, sodass für $n \geq N$ die Ungleichung

$$\frac{1}{n} < \operatorname{Im} z - \varepsilon \quad \Leftrightarrow \quad \operatorname{Im} z - \frac{1}{n} > \varepsilon$$

erfüllt ist. Wegen $|z - b_n| > |\operatorname{Im} z - \operatorname{Im} b_n| = |\operatorname{Im} z - \frac{1}{n}| > \varepsilon$ für $n \geq N$ liegen also die Folgenglieder b_n nicht in $B_\varepsilon(z)$. Somit können höchstens endlich viele Folgenglieder von $(b_n)_{n \in \mathbb{N}}$ in $B_\varepsilon(z)$ liegen, was bedeutet, dass z kein Häufungspunkt der Folge $(b_n)_{n \in \mathbb{N}}$ sein kann.

Wir haben gezeigt: $z \in \mathbb{C}$ ist genau dann Häufungspunkt von $(b_n)_{n \in \mathbb{N}}$, wenn $\operatorname{Im} z = 0$, also z eine reelle Zahl ist.

- b** Wir benutzen die Darstellung der komplexen Einheitskreislinie $\partial\mathbb{D}$ als

$$\partial\mathbb{D} = \left\{ e^{i\alpha} \mid \alpha \in \mathbb{R} \right\}.$$

Sei $(a_n)_{n \in \mathbb{N}}$ wiederum die rationale Folge, die jede reelle Zahl als Häufungspunkt hat. Dann hat die Folge $(e^{ia_n})_{n \in \mathbb{N}}$ jeden Punkt der komplexen Einheitskreislinie als Häufungspunkt, da $\exp(i\mathbb{R}) = \partial\mathbb{D}$ gilt und die

Exponentialfunktion stetig ist. Leider verläuft diese Folge auf der Einheitskreislinie selbst, d. h. nicht in der offenen Einheitskreisscheibe. Dies reparieren wir, indem wir den Radius gegen 1 konvergieren lassen: Die Folge $(c_n)_{n \in \mathbb{N}}$ mit

$$c_n = \left(1 - \frac{1}{n}\right) e^{ia_n}$$

sollte dann eine Folge mit den gewünschten Eigenschaften sein. Der Nachweis verläuft wie in Teil **a**.

Lösungsvorschlag zur Aufgabe (Herbst 2015, T1A3)

a Sei $r > 1$ eine reelle Zahl und $z \in \partial B_r(0)$, dann gilt die Abschätzung

$$|p(z) - z^n| = \left| \sum_{k=0}^{n-1} a_k z^k \right| \leq \sum_{k=0}^{n-1} |a_k| \cdot |z|^k = \sum_{k=0}^{n-1} |a_k| \cdot r^k < r^{n-1} \sum_{k=0}^{n-1} |a_k| = r^{n-1} C$$

mit $C = \sum_{k=0}^{n-1} |a_k|$. Wählt man also $r > C$, so gilt

$$|p(z) - z^n| < r^{n-1} C < r^n = |z|^n.$$

Nach dem Satz von Rouché hat daher $p(z) = (p(z) - z^n) + z^n$ in $B_r(0)$ genauso viele Nullstellen (mit Vielfachheit gezählt) wie das Polynom z^n . Da z^n eine n -fache Nullstelle in 0 hat, sind das genau n . Da r beliebig groß gewählt werden kann, hat $p(z)$ genau n Nullstellen in \mathbb{C} .

b Es ist

$$p'(z) = a_1 + 2a_2 z + \dots + (n-1)a_{n-1} z^{n-2} + n z^{n-1}$$

und somit

$$\begin{aligned} \frac{p'(z)}{p(z)} &= \frac{a_1 + 2a_2 z + \dots + (n-1)a_{n-1} z^{n-2} + n z^{n-1}}{a_0 + a_1 z + \dots + a_{n-1} z^{n-1} + z^n} = \\ &= \frac{n}{z} \left(\frac{a_1 z + 2a_2 z^2 + \dots + (n-1)a_{n-1} z^{n-1} + n z^n}{na_0 + na_1 z + \dots + na_{n-1} z^{n-1} + nz^n} \right) = \\ &= \frac{n}{z} \left(1 + \frac{-na_0 + (n-1)a_1 z + (n-2)a_2 z^2 + \dots + (-1)a_{n-1} z^{n-1}}{na_0 + na_1 z + \dots + na_{n-1} z^{n-1} + nz^n} \right) = \\ &= \frac{n}{z} \cdot (1 + g(z)). \end{aligned}$$

Da der Grad des Polynoms im Nenner von $g(z)$ höher als der Grad des Polynoms im Zähler ist, gilt $\lim_{|z| \rightarrow \infty} g(z) = 0$. Somit ist

$$\begin{aligned}\lim_{r \rightarrow \infty} \left| \int_{\partial B_r(0)} \frac{ng(z)}{z} dz \right| &\leq \lim_{r \rightarrow \infty} 2\pi r \cdot n \cdot \max_{z \in \partial B_r(0)} \left| \frac{g(z)}{z} \right| = \\ &= \lim_{r \rightarrow \infty} 2\pi r \cdot n \cdot \frac{1}{r} \cdot \max_{z \in \partial B_r(0)} |g(z)| = \\ &= 2\pi n \lim_{r \rightarrow \infty} \max_{z \in \partial B_r(0)} |g(z)| = 0.\end{aligned}$$

Also liefert das Nullstellen zählende Integral

$$\begin{aligned}\lim_{r \rightarrow \infty} \frac{1}{2\pi i} \int_{\partial B_r(0)} \frac{p'(z)}{p(z)} dz &= \lim_{r \rightarrow \infty} \frac{1}{2\pi i} \int_{\partial B_r(0)} \frac{n}{z} \cdot (1 + g(z)) dz = \\ &= \frac{1}{2\pi i} \lim_{r \rightarrow \infty} \left(\int_{\partial B_r(0)} \frac{n}{z} dz + \int_{\partial B_r(0)} \frac{ng(z)}{z} dz \right) = \\ &= \frac{1}{2\pi i} \lim_{r \rightarrow \infty} \int_{\partial B_r(0)} \frac{n}{z} dz = \\ &= \frac{1}{2\pi i} \lim_{r \rightarrow \infty} 2\pi i \cdot n = n\end{aligned}$$

Dabei wurde im vorletzten Schritt die Cauchy-Integralformel verwendet.

Lösungsvorschlag zur Aufgabe (Herbst 2015, T1A5)

- a Die gegebene Differentialgleichung zweiter Ordnung ist äquivalent zum linearen System

$$\begin{pmatrix} \dot{u} \\ \dot{v} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & -2c \end{pmatrix} \begin{pmatrix} u \\ v \end{pmatrix} = A \begin{pmatrix} u \\ v \end{pmatrix}.$$

Das charakteristische Polynom von A ist

$$\chi_A = \det \begin{pmatrix} -X & 1 \\ -1 & -X - 2c \end{pmatrix} = X(X + 2c) + 1 = X^2 + 2cX + 1$$

Die Eigenwerte sind also

$$\lambda_{\pm} = \frac{-2c \pm \sqrt{4c^2 - 4}}{2} = -c \pm \sqrt{c^2 - 1}.$$

Ist $c^2 - 1 \leq 0$, so folgt sofort $\operatorname{Re}(\lambda_{\pm}) = -c < 0$ und das System ist asymptotisch stabil. Im Fall $c^2 - 1 > 0$ ist zumindest $\operatorname{Re}(\lambda_-) = \lambda_- < -c < 0$. Zudem folgt aus der Monotonie der Wurzelfunktion, dass

$$c^2 > c^2 - 1 \quad \Rightarrow \quad c > \sqrt{c^2 - 1} \quad \Leftrightarrow \quad 0 > -c + \sqrt{c^2 - 1}$$

gilt. Also ist auch $\operatorname{Re}(\lambda_+) = \lambda_+ < 0$ und somit ist auch im Fall $c^2 - 1 > 0$ das System asymptotisch stabil.

- b** Die Lösung $y(t)$ hat die Form

$$y(t) = \Lambda(t, t_0) \begin{pmatrix} y(t_0) \\ \dot{y}(t_0) \end{pmatrix},$$

wobei $\Lambda(t, t_0)$ die Übergangsmatrix bezeichnet. Da das System nach Teil **a** asymptotisch stabil ist, gilt laut 7.28, dass $\lim_{t \rightarrow \infty} \Lambda(t, t_0) = 0$. Also folgt

$$\lim_{t \rightarrow \infty} y(t) = \lim_{t \rightarrow \infty} \Lambda(t, t_0) \begin{pmatrix} y(t_0) \\ \dot{y}(t_0) \end{pmatrix} = 0.$$

- c** Im Fall $c^2 - 1 < 0$ sind die Eigenwerte aus Teil **a** durch $\lambda_{\pm} = -c \pm ia$ gegeben. Ein Fundamentalsystem der Differentialgleichungssystem ist dann

$$\{e^{-ct} \cos at, e^{-ct} \sin at\}.$$

Jede Lösung λ hat daher die Form $\lambda(t) = Ae^{-ct} \cos at + Be^{-ct} \sin at$ mit $A, B \in \mathbb{R}$. Aufgrund der Bedingung $\lambda(0) = 1$ muss $A = 1$ sein. Wir berechnen weiter

$$\lambda'(t) = -ce^{-ct} \cos at - ae^{-ct} \sin at - cBe^{-ct} \sin at + aBe^{-ct} \cos at.$$

Aus der Bedingung $\lambda'(0) = 0$ erhalten wir daher

$$0 = -c + aB \quad \Leftrightarrow \quad B = \frac{c}{a}.$$

Die gesuchte Lösung ist damit

$$\lambda(t) = e^{-ct} \cos at + \frac{c}{a} e^{-ct} \sin at.$$

Lösungen zu Thema Nr. 2

Lösungsvorschlag zur Aufgabe (Herbst 2015, T2A4)

- a** Sei $f: \mathbb{C} \rightarrow \mathcal{D}$ eine holomorphe Funktion. Wegen $-1, -2 \notin \text{im } f \subseteq \mathcal{D}$ muss f nach dem kleinen Satz von Picard konstant sein. Da eine konstante Funktion auf jeden Fall nicht bijektiv ist, kann f also nicht biholomorph sein.
- b** Sei $w \in \text{im } f$, d. h. $w = f(z)$ für ein $z \in \mathbb{C}$. Dann gilt

$$f(w) = f(f(z)) \stackrel{(*)}{=} f(z) = w,$$

wobei an der Stelle $(*)$ die Gleichung $f \circ f = f$ verwendet wurde. Nehmen wir nun an, dass f nichtkonstant ist (für konstante Funktionen ist die Gleichung $f \circ f = f$ stets erfüllt). Da $\text{im } f = f(\Omega)$ dann nach dem Satz über die Gebietstreue 6.22 wieder ein (nicht-leeres) Gebiet ist, stimmt f auf einem Gebiet mit der Funktion $w \mapsto w$ überein. Laut Identitätssatz gilt dann bereits $f(z) = z$ für alle $z \in \Omega$. Also ist eine solche Funktion f entweder konstant oder die Identitätsabbildung.

Alternative: Gemäß Kettenregel ist

$$f'(f(z)) \cdot f'(z) = f'(z) \Leftrightarrow f'(z)(f'(f(z)) - 1) = 0$$

für alle $z \in \Omega$. Da Ω als Gebiet zusammenhängend und $f'(z)$ bzw $f'(z) - 1$ wiederum holomorphe Funktionen sind, folgt wie in H06T3A2, dass

$$f'(z) = 0 \quad \text{oder} \quad f'(f(z)) - 1 = 0$$

für alle $z \in \Omega$. Im ersten Fall folgt, dass f konstant ist, im zweiten Fall ist $f'(w) = 1$ für alle $w \in \text{im } \Omega$, d. h. $f(w) = w + c$ für ein $c \in \mathbb{C}$. Dabei gilt:

$$f(1) = (f \circ f)(1) \Leftrightarrow 1 + c = f(1 + c) = 1 + 2c \Leftrightarrow c = 0.$$

Wie oben (f nicht-konstant, da sonst $f' \equiv 0$ wäre), folgt aus dem Identitätssatz $f(z) = z$ für alle $z \in \Omega$.

Lösungsvorschlag zur Aufgabe (Herbst 2015, T2A5)

a Wir verwenden $\cos(z) = \sin(z + \frac{\pi}{2})$. Damit bekommen wir

$$(z + \frac{\pi}{2}) \cos z = (z + \frac{\pi}{2}) \sin(z + \frac{\pi}{2}) = (z + \frac{\pi}{2}) \sum_{n=0}^{\infty} (-1)^n \frac{(z + \frac{\pi}{2})^{2n+1}}{(2n+1)!} = \\ = (z + \frac{\pi}{2})^2 \sum_{n=0}^{\infty} (-1)^n \frac{(z + \frac{\pi}{2})^{2n}}{(2n+1)!} =: (z - \frac{\pi}{2})^2 g(z).$$

Es ist nun $g(-\frac{\pi}{2}) = \frac{0^0}{(0+1)!} = 1 \neq 0$. Aus der Darstellung $f(z) = \frac{1}{(z + \frac{\pi}{2})^2 g(z)}$ folgt daher, dass f in $-\frac{\pi}{2}$ einen Pol zweiter Ordnung hat. Um die restlichen Singularitäten bestimmen zu können, brauchen wir die Nullstellen der komplexen Kosinusfunktion:

$$\begin{aligned} \cos z = 0 &\Leftrightarrow \frac{1}{2}(e^{iz} + e^{-iz}) = 0 \Leftrightarrow e^{iz} = -e^{-iz} = e^{i\pi} \cdot e^{-iz} = e^{i(\pi-z)} \\ &\Leftrightarrow z \equiv \pi - z \pmod{2\pi\mathbb{Z}} \Leftrightarrow 2z \equiv \pi \pmod{2\pi\mathbb{Z}} \Leftrightarrow \\ &\Leftrightarrow z \equiv \frac{\pi}{2} \pmod{2\pi\mathbb{Z}} \end{aligned}$$

Die einzige andere Singularität von f in Ω ist daher $\frac{\pi}{2}$. Hier gilt

$$\begin{aligned} \cos z = \cos(-z) &= \sin(-z + \frac{\pi}{2}) = -\sin(z - \frac{\pi}{2}) = \\ &= -\sum_{n=0}^{\infty} (-1)^n \frac{(z - \frac{\pi}{2})^{2n+1}}{(2n+1)!} = (z - \frac{\pi}{2}) \cdot \sum_{n=0}^{\infty} (-1)^{n+1} \frac{(z - \frac{\pi}{2})^{2n}}{(2n+1)!} = \\ &=: (z - \frac{\pi}{2}) \cdot h(z). \end{aligned}$$

Die hintere Summe $h(z)$ hat wieder keine Nullstelle bei $\frac{\pi}{2}$, deshalb hat f einen Pol erster Ordnung in $\frac{\pi}{2}$.

b Mithilfe der Darstellung aus Teil **a** ist $\operatorname{Res}(f; \frac{\pi}{2}) = \frac{1}{h'(\frac{\pi}{2})} = -1$ und

$$\operatorname{Res}(f; -\frac{\pi}{2}) = \left(\frac{1}{g(z)} \right)' \Big|_{z=-\frac{\pi}{2}} = \frac{-g'(-\frac{\pi}{2})}{g^2(-\frac{\pi}{2})} = 0,$$

wobei wir verwendet haben, dass

$$g'(z) = \sum_{k=1}^{\infty} (-1)^k \cdot 2k \frac{(z + \frac{\pi}{2})^{2k-1}}{(2k+1)!}$$

keinen konstanten Koeffizienten hat.

c f hat genau dann eine Stammfunktion falls das Integral über jede beliebige geschlossene Kurve verschwindet (vgl. Proposition 6.29). Allerdings gilt laut Residuensatz, dass

$$\int_{\partial B_\epsilon(\frac{\pi}{2})} f(z) dz = 2\pi i \operatorname{Res}(f; \frac{\pi}{2}) = -2\pi i \neq 0.$$

d Sei $p(z) = f(z) + \frac{c}{(z - \frac{\pi}{2})}$. Setze $c = 1$, dann gilt

$$\operatorname{Res}(p; \frac{\pi}{2}) = \operatorname{Res}(f; -\frac{\pi}{2}) + \operatorname{Res}\left(\frac{c}{z - \frac{\pi}{2}}; -\frac{\pi}{2}\right) = -1 + c = -1 + 1 = 0.$$

Ist $\gamma: [0, 1] \rightarrow \Omega$ nun eine geschlossene Kurve, so gilt nach dem Residuensatz

$$\int_{\gamma} p(z) dz = n(\gamma, -\frac{\pi}{2}) \operatorname{Res}(p; -\frac{\pi}{2}) + n(\gamma, \frac{\pi}{2}) \operatorname{Res}(p; \frac{\pi}{2}) = 0 + 0 = 0.$$

Folglich besitzt p eine Stammfunktion auf Ω .

Lösungen zu Thema Nr. 3

Lösungsvorschlag zur Aufgabe (Herbst 2015, T3A1)

Wegen

$$\lim_{z \rightarrow 0} f(z) = \lim_{z \rightarrow 0} \frac{z}{z(z+1)(z+1-i)^2} = \lim_{z \rightarrow 0} \frac{1}{(z+1)(z+1-i)} = \frac{1}{1-i}$$

handelt es sich bei 0 um eine hebbare Singularität von f . Folglich ist $\operatorname{Res}(f; 0) = 0$. Dagegen ist wegen

$$\lim_{z \rightarrow -1} |f(z)| = \infty, \quad \lim_{z \rightarrow -1} (z+1)f(z) = \frac{-1}{-(-i)^2} = -1$$

die Singularität -1 eine Polstelle erster Ordnung. Obige Rechnung zeigt außerdem $\operatorname{Res}(f; -1) = -1$. Zu guter Letzt ist $-1+i$ wegen

$$\begin{aligned} \lim_{z \rightarrow -1+i} |f(z)| &= \lim_{z \rightarrow -1+i} |(z+1-i)f(z)| = \infty, \\ \lim_{z \rightarrow -1+i} (z+1-i)^2 f(z) &= \frac{-1+i}{i(-1+i)} = -i \end{aligned}$$

ein Pol zweiter Ordnung. Hier berechnet sich das Residuum zu

$$\operatorname{Res}(f; -1+i) = \frac{d}{dz} \left(\frac{z}{z^2+z} \right) \Big|_{z=-1+i} = \left(\frac{-1}{(z+1)^2} \right) \Big|_{z=-1+i} = \frac{-1}{-1} = 1.$$

Nach dem Residuensatz gilt nun

$$\begin{aligned} \int_{\gamma(r)} f(z) dz &= n(\gamma(r), 0) \operatorname{Res}(f; 0) + n(\gamma(r), -1) \operatorname{Res}(f; -1) \\ &\quad + n(\gamma(r), -1+i) \operatorname{Res}(f; -1+i). \end{aligned}$$

Für $r < 1$ wird nur die Singularität 0 von $\gamma(r)$ umlaufen, d.h. hier ist $n(\gamma(r), 0) = 1$ und $n(\gamma(r), -1) = 0 = n(\gamma(r), -1+i)$. Der Wert des Integrals ist damit

$$\int_{\gamma(r)} f(z) dz = 1 \cdot \operatorname{Res}(f; 0) = 0.$$

Für $r \in]1, \sqrt{2}[$ ist $0, -1 \in B_r(0)$, aber $-1+i \notin B_r(0)$, da $| -1+i | = \sqrt{1^2 + 1^2} = \sqrt{2}$. Also erhält man hier

$$\int_{\gamma(r)} f(z) dz = 2\pi i (1 \cdot \operatorname{Res}(f; 0) + 1 \cdot \operatorname{Res}(f; -1)) = -2\pi i.$$

Ist $r > \sqrt{2}$, so werden alle Singularitäten umlaufen. Man berechnet hier deshalb

$$\begin{aligned} \int_{\gamma(r)} f(z) dz &= 2\pi i (1 \cdot \operatorname{Res}(f; 0) + 1 \cdot \operatorname{Res}(f; -1) + 1 \cdot \operatorname{Res}(f; -1+i)) = \\ &= 2\pi i (1 - 1) = 0. \end{aligned}$$

Lösungsvorschlag zur Aufgabe (Herbst 2015, T3A2)

- a Eine Singularität a einer Funktion f heißt *isoliert*, falls es eine Umgebung $U \subseteq \mathbb{C}$ von a gibt, sodass in U (neben a) keine weitere Singularität von f liegt. Ist nun

$$f(z) = \sum_{n=-\infty}^{\infty} a_n (z-a)^n$$

eine Laurentreihen-Entwicklung von f um a , so heißt a

- (i) *hebbar*, falls $a_n = 0$ für alle $n < 0$,
- (ii) *Polstelle* der Ordnung k , falls $a_{-k} \neq 0$ und $a_n = 0$ für alle $n < -k$,
- (iii) *wesentliche Singularität*, falls a weder hebbar noch Polstelle ist.

b Es gilt

$$\lim_{z \rightarrow 2} |h(z)| = \infty, \quad \lim_{z \rightarrow 2} (z-2)h(z) = 2 \exp(\sin(\frac{1}{2})),$$

also handelt es sich bei $z = 2$ um eine Polstelle erster Ordnung. Weiter ist

$$\begin{aligned} \lim_{z \rightarrow 1} h(z) &= \lim_{z \rightarrow 1} \frac{z}{z-2} \exp\left(\sin\left(\frac{z-1}{z(z-1)}\right)\right) = \\ &= \lim_{z \rightarrow 1} \frac{z}{z-2} \exp\left(\sin\left(\frac{1}{z}\right)\right) = -\exp \sin 1 \in \mathbb{C}, \end{aligned}$$

sodass in 1 eine hebbare Singularität vorliegt. Nun fehlt nur noch die Klassifikation der Singularität in 0. Betrachte dazu die Folgen $(u_n)_{n \in \mathbb{N}}, (v_n)_{n \in \mathbb{N}}$ mit $u_n = \frac{1}{n\pi}$ und $v_n = \frac{2}{\pi + 4n\pi}$. Es gilt $\lim_{n \rightarrow \infty} u_n = \lim_{n \rightarrow \infty} v_n = 0$ und

$$\begin{aligned} \lim_{n \rightarrow \infty} \frac{1}{u_n - 2} \exp\left(\sin\left(\frac{1}{u_n} \frac{u_n - 1}{u_n - 1}\right)\right) &= \lim_{n \rightarrow \infty} \frac{\exp(\sin(n\pi))}{u_n - 2} = \\ &= \lim_{n \rightarrow \infty} \frac{1}{u_n - 2} = -\frac{1}{2}. \end{aligned}$$

Außerdem

$$\begin{aligned} \lim_{n \rightarrow \infty} \frac{1}{v_n - 2} \exp\left(\sin\left(\frac{1}{v_n} \frac{v_n - 1}{v_n - 1}\right)\right) &= \lim_{n \rightarrow \infty} \frac{\exp(\sin(\frac{\pi}{2}))}{v_n - 2} = \\ &= \lim_{n \rightarrow \infty} \frac{e}{v_n - 2} = -\frac{e}{2}. \end{aligned}$$

Also hat die Funktion $g: \mathbb{C} \setminus \{0\} \rightarrow \mathbb{C}, z \mapsto \frac{1}{z-2} \exp(\sin(\frac{z-1}{z^2-z}))$ eine wesentliche Singularität bei 0. Eine Laurentreihendarstellung um 0 von g mit Koeffizienten a_k erfüllt also $a_k \neq 0$ für unendlich viele $k < 0$. Bezeichnet b_n die Koeffizienten der Laurentreihenentwicklung von h , so ist

$$h(z) = \sum_{k=-\infty}^{\infty} b_k z^k = z \sum_{k=-\infty}^{\infty} a_k z^k = \sum_{k=-\infty}^{\infty} a_{k-1} z^k$$

Daraus folgt $b_k = a_{k-1}$ für alle $k \in \mathbb{Z}$ und somit muss auch h unendliche viele negative Koeffizienten besitzen, also eine wesentliche Singularität bei 0 haben.

Lösungsvorschlag zur Aufgabe (Herbst 2015, T3A3)

a Definiere eine Funktion

$$\Phi: \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}, \quad (t, f) \mapsto f(f-1)(f+1),$$

dann handelt es sich bei Φ um eine stetige und auf einem Gebiet definierte Funktion, die die rechte Seite der gegebenen Differentialgleichung beschreibt. Weiter ist

$$\partial_f \Phi(t, f) = \partial_f(f^3 - f) = 3f^2 - 1$$

ebenfalls stetig, sodass Φ lokal Lipschitz-stetig bezüglich f ist. Aus dem Globalen Existenz- und Eindeutigkeitssatz folgt nun, dass $f' = \Phi(t, f)$ eine eindeutige maximale Lösung zum Anfangswert $f(0) = f_0$ besitzt.

b Betrachte die konstante Funktion

$$\mu_1: \mathbb{R} \rightarrow \mathbb{R}, \quad t \mapsto 1.$$

Es ist μ_1 Lösung der Differentialgleichung $\Phi(t, f) = f'$ und da sie auf ganz \mathbb{R} definiert ist, handelt es sich dabei um die eindeutige maximale Lösung zum Anfangswert $f(0) = 1$.

Sei nun $\lambda: I \rightarrow \mathbb{R}$ die laut Teil **a** eindeutige Lösung zum Anfangswert $\lambda(0) = f_0 < 1$. Angenommen, es gibt ein $\tau \in I$ mit $\lambda(\tau) = a > 1$ für ein $\tau \in I$. Da λ stetig ist, gibt es nach dem Zwischenwertsatz dann ein $\tau_1 \in I$, sodass $f(\tau_1) = 1 = \mu_1(\tau_1)$. Da die Lösungskurven maximaler Lösungen entweder disjunkt oder schon gleich sind und λ die Einschränkung einer maximalen Lösung ist, folgt daraus bereits $\lambda(t) = \mu_1(t) = 1$ für alle $t \in I$. Dies ist jedoch ein Widerspruch zu $\lambda(0) = f_0 < 1$.

c Sei $\lambda:]a, b[\rightarrow \mathbb{R}$ die eindeutige maximale Lösung mit $\lambda(0) = f_0 > 1$. Wenn wir zeigen können, dass $\lim_{t \searrow a} \lambda(t) = 1$ und $\lim_{t \nearrow b} \lambda(t) = +\infty$ gilt, sind wir fertig, denn dann gibt es für jedes $\xi > 1$ reelle Zahlen $t_1, t_2 \in]a, b[$ mit

$$\lambda(t_1) \leq \xi \leq \lambda(t_2).$$

Nach dem Zwischenwertsatz wird dann der Wert ξ von f auf jeden Fall angenommen. Wir zeigen daher nun die Aussage über das Grenzwertverhalten.

Wie in Teil **a** zeigt man unter Verwendung der konstanten Lösung μ_1 , dass $\lambda(t) > 1$ für alle $t \in I$ gilt. Aus der Lösungsidentität folgt dann, dass

$$\lambda'(t) = \Phi(t, \lambda(t)) = \lambda(t)(\lambda(t) - 1)(\lambda(t) + 1) > 0$$

für alle $t \in I$ gilt. Also ist λ auf ganz I streng monoton steigend. Falls eine der Grenzen a oder b endlich ist, so folgt aus der Charakterisierung des Randverhaltens maximaler Lösungen 7.13, dass

$$\lim_{t \searrow a} |\lambda(t)| = \infty \quad \text{bzw.} \quad \lim_{t \nearrow b} |\lambda(t)| = \infty.$$

Da λ streng monoton steigend ist, muss sogar

$$\lim_{t \searrow a} \lambda(t) = -\infty \quad \text{bzw.} \quad \lim_{t \nearrow b} \lambda(t) = +\infty$$

gelten. Die linke Aussage ist unmöglich, denn λ ist durch 1 nach unten beschränkt, also muss $a = -\infty$ gelten. Ist die rechte Aussage erfüllt, so sind wir laut den Ausführungen oben fertig. Nehmen wir also im Folgenden an, dass $b = +\infty$ ist. Da λ streng monoton steigend ist, haben wir $\lambda(t) \geq \lambda(0) = f_0 > 1$ für alle $t \geq 0$, sodass

$$\begin{aligned} \lambda(t) &= \lambda(0) + \int_0^t \lambda'(\tau) d\tau = \lambda(0) + \int_0^t \lambda(\tau)(\lambda(\tau) - 1)(\lambda(\tau) + 1) d\tau \geq \\ &\geq \lambda(0) + \int_0^t f_0(f_0 - 1)(f_0 + 1) d\tau = \lambda(0) + f_0(f_0 - 1)(f_0 + 1)t \end{aligned}$$

für $t \geq 0$ gilt. Daraus folgt $\lim_{t \rightarrow \infty} \lambda(t) = \infty$ wie erhofft.

Für alle $t \leq 0$ gilt $1 < \lambda(t) < f_0$, sodass $\lambda(t)$ für $t \rightarrow -\infty$ gegen einen endlichen Wert $c \in [1, f_0[$ gehen muss. Angenommen, es ist $c > 1$, dann gilt $\lambda(t) \geq c$ für alle $t \in \mathbb{R}$ und für alle $t \leq 0$ haben wir die Abschätzung

$$\begin{aligned} \lambda(t) &= \lambda(0) + \int_0^t \lambda'(\tau) d\tau = f_0 - \int_t^0 \lambda'(\tau) d\tau = \\ &= f_0 - \int_t^0 \lambda(\tau)(\lambda(\tau) - 1)(\lambda(\tau) + 1) d\tau \leq \\ &\leq f_0 - \int_t^0 c(c - 1)(c + 1) d\tau = f_0 + c(c - 1)(c + 1)t \end{aligned}$$

Daraus jedoch $\lim_{t \rightarrow -\infty} \lambda(t) = -\infty$ im Widerspruch dazu, dass λ durch 1 nach unten beschränkt ist. Insgesamt muss $\lim_{t \rightarrow -\infty} \lambda(t) = 1$ gelten.

Lösungsvorschlag zur Aufgabe (Herbst 2015, T3A4)

- a** Sei $r > 0$. Laut Cauchy-Integralformel gilt

$$f^{(n)}(0) = \frac{n!}{2\pi i} \int_{\partial B_r(0)} \frac{f(z)}{z^{n+1}} dz.$$

Als Abschätzung erhält man daraus

$$|f^{(n)}(0)| \leq \frac{n!}{2\pi} \int_{\partial B_r(0)} \left| \frac{f(z)}{z^{n+1}} \right| dz \leq \frac{n!}{2\pi} \cdot 2\pi r \cdot \frac{Mr^\alpha}{r^{n+1}} = n! Mr^{\alpha-n}$$

Ist $n > \alpha$, so ist $\alpha - n < 0$ und damit $\lim_{r \rightarrow \infty} r^{\alpha-n} = 0$. Also bekommen wir

$$|f^{(n)}(0)| = \lim_{r \rightarrow \infty} n! Mr^{\alpha-n} = 0,$$

weswegen $f^{(n)}(0) = 0$ sein muss.

- b** Da p ganz ist, gibt es eine auf ganz \mathbb{C} gültige Potenzreihendarstellung

$$p(z) = \sum_{n=0}^{\infty} a_n z^n,$$

wobei die Koeffizienten durch $a_n = \frac{1}{n!} p^{(n)}(0)$ gegeben sind. Aus der Voraussetzung folgt also $a_n = 0$ für alle $n > n_0$ und somit

$$p(z) = \sum_{n=0}^{\infty} a_n z^n = \sum_{n=0}^{n_0} a_n z^n.$$

- c** Nach Aufgabenteil **a** gilt $f^{(n)}(0) = 0$ für alle $n > \alpha$. Setze $n_0 = \lfloor \alpha \rfloor$, dann gilt auch $f^{(n)}(0) = 0$ für $n > n_0$ und aus Aufgabenteil **b** folgt, dass f ein Polynom von Grad (höchstens) n_0 ist. Ist f ein Polynom von Grad 0, so ist f konstant. Ist dagegen $\text{grad } f \geq 1$, so hat f nach dem Fundamentalsatz der Algebra mindestens eine Nullstelle in \mathbb{C} .

Prüfungstermin: Frühjahr 2016

Thema Nr. 1 (Aufgabengruppe)

Aufgabe 1 → S. 603

- a** Finden Sie eine holomorphe Funktion $f: \mathbb{C} \setminus \{-1, 1\} \rightarrow \mathbb{C}$, welche in den Punkten -1 und 1 wesentliche Singularitäten mit den Residuen

$$\operatorname{Res}(f; -1) = -1, \quad \operatorname{Res}(f; 1) = 1$$

besitzt. Ist f durch diese Eigenschaft eindeutig bestimmt? (2 Punkte)

- b** Sei f die in **a** gefundene Funktion. Für $\alpha \in [0, \infty[$ sei γ_α der geschlossene Weg, der die Punkte

$$2 + \alpha i, -2 - i, -2 + i, 2 - \alpha i, 2 + \alpha i$$

in der angegebenen Reihenfolge durch Geradenstücke verbindet. Für welche Werte von α ist da komplexe Wegintegral

$$\int_{\gamma_\alpha} f(z) dz$$

definiert? Berechnen Sie das Integral für diese Werte von α . (4 Punkte)

Aufgabe 2 → S. 605

- a** Zeigen Sie für alle natürlichen Zahlen n

$$\sum_{k=1}^n (4k^3 - 6k^2) = n^4 - 2n^2 - n.$$

(3 Punkte)

- b** Zeigen Sie durch Induktion in n , dass für $G_r(k) := \prod_{l=0}^{r-1} (k+l)$ (also mit $G_0(k) = 1$) die Formeln

$$\sum_{k=1}^n G_r(k) = \frac{1}{r+1} G_{r+1}(n)$$

gelten, für alle $r \in \mathbb{N} \cup \{0\}$ und alle $n \in \mathbb{N}$. (3 Punkte)

Aufgabe 3 → S. 606

Sei $D := \{x \in \mathbb{R}^2 \mid |x| := \sqrt{x_1^2 + x_2^2} < 1\}$ und $f: D \rightarrow \mathbb{R}^2, f(x) := ((1 - |x|)^{-1}, |x|)$. Zeigen Sie:

- a** Das Anfangswertproblem

$$\dot{x} = f(x), \quad x(0) = 0$$

besitzt eine eindeutige bestimmte, maximale Lösung. (2 Punkte)

- b** Für diese maximale Lösung $x:]a, b[\rightarrow D$, wobei $-\infty \leq a < 0 < b \leq \infty$, ist $b \leq 1$, $x(b) = \lim_{t \rightarrow b} x(t)$ existiert und $|x(b)| = 1,0 < x_2(b) < 1/4$.

Hinweis Die Trajektorie der Lösung lässt sich als Graph einer Funktion darstellen und deren Ableitung lässt sich geeignet abschätzen. (4 Punkte)

Aufgabe 4 → S. 607

- a** Sei $f: \mathbb{R} \rightarrow \mathbb{R}$ stetig differenzierbar. Zeigen Sie, dass für jede Lösung der Differentialgleichung

$$\dot{x} = f(x)$$

genau eine der folgenden Aussagen zutrifft:

- (i) x ist streng monoton wachsend.
- (ii) x ist streng monoton fallend.
- (iii) x ist konstant. (4 Punkte)

- b** Bleibt die Aussage in **a** richtig, wenn $f: \mathbb{R} \rightarrow \mathbb{R}$ nur als stetig vorausgesetzt wird? (2 Punkte)

Aufgabe 5 → S. 608

- a** Für $n \in \mathbb{N}$ sei $f_n: [0, \infty[\rightarrow \mathbb{R}$, $f_n(x) := \frac{x}{n^2} e^{-\frac{x}{n}}$. Zeigen Sie, dass die Folge $(f_n)_{n \in \mathbb{N}}$ auf $[0, \infty[$ gleichmäßig gegen 0 konvergiert, und bestimmen Sie

$$\lim_{n \rightarrow \infty} \int_0^\infty f_n(x) dx.$$

(3 Punkte)

- b** Sei $f: [0, 1] \rightarrow \mathbb{R}$ stetig mit $f(0) = 0$. Bestimmen Sie

$$\lim_{n \rightarrow \infty} \int_0^1 f(x^n) dx.$$

(3 Punkte)

Thema Nr. 2
(Aufgabengruppe)

Aufgabe 1 → S. 609

Begründen Sie, dass das uneigentliche Riemann-Integral

$$I := \int_{-\infty}^{+\infty} \frac{2}{x^6 + 3} dx$$

existiert, und berechnen Sie I mithilfe des Residuensatzes. (1 + 5 Punkte)

Aufgabe 2 → S. 611

Zeigen Sie, dass das Differentialgleichungssystem erster Ordnung

$$\frac{dx}{dt} = y \quad , \quad \frac{dy}{dt} = -\sin(x)$$

auf dem Phasenraum \mathbb{R}^2

- a** für alle Anfangswerte $z_0 = (x_0, y_0) \in \mathbb{R}^2$ eine eindeutige Lösung $\phi_{z_0} : \mathbb{R} \rightarrow \mathbb{R}^2$ besitzt. (2 Punkte)
- b** Zeigen Sie, dass die Funktion $F: \mathbb{R}^2 \rightarrow \mathbb{R}, F(x, y) = y^2/2 - \cos(x)$ eine Erhaltungsgröße ist, also entlang der Lösungskurven ϕ_{z_0} konstant ist. (1 Punkt)
- c** Bestimmen Sie, ob die Gleichgewichtslage $0 \in \mathbb{R}^2$ stabil oder sogar asymptotisch stabil ist. (3 Punkte)

Aufgabe 3 → S. 613

Berechnen Sie, für welche Anfangswerte $x_0 \in \mathbb{R}^3$ die Lösung der linearen Differentialgleichung

$$\frac{dx}{dt} = Ax \quad \text{mit der Systemmatrix } A := \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}$$

für $t \rightarrow +\infty$ gegen die Ruhelage $r := \begin{pmatrix} 1 \\ -2 \\ 1 \end{pmatrix}$ konvergiert.

Hinweis Sie müssen nicht die allgemeine Lösung der Differentialgleichung bestimmen, um die Aufgabe zu lösen. (6 Punkte)

Aufgabe 4 → S. 613

Welche der folgenden Aussagen sind wahr, welche falsch? Beweisen Sie die Aussage oder geben Sie ein Gegenbeispiel an.

- a** Stetige Funktionen $f: [a, b] \rightarrow \mathbb{R}$ sind gleichmäßig stetig. (2 Punkte)
- b** Die Umkehrfunktion $f^{-1}: (c, d) \rightarrow (a, b)$ einer stetig differenzierbaren streng monotonen Funktion $f: (a, b) \rightarrow (c, d)$ ist ebenfalls stetig differenzierbar. (2 Punkte)
- c** Die Funktion $f: \mathbb{R} \rightarrow \mathbb{R}, f(x) = 1/(1+x^2)$ ist reell-analytisch, und ihre Potenzreihendarstellung bei $x = 0$ besitzt den Konvergenzradius 1. (2 Punkte)

Aufgabe 5 → S. 615

Gegeben sei die Potenzreihe $f(z) = \sum_{n=0}^{\infty} z^{2^n}$. Zeigen Sie:

- a** Der Konvergenzradius von f ist 1. (1 Punkt)
 - b** Für $k \in \mathbb{N}_0$ und $z \in \mathbb{C}$ mit $|z| < 1$ gilt $|f(z^{2^k})| \leq |f(z)| + k$. (1 Punkt)
 - c** Sei $k \in \mathbb{N}_0$ und ρ eine 2^k -te Einheitswurzel. Dann gilt $\lim_{t \rightarrow 1, 0 < t < 1} |f(t\rho)| = \infty$. (2 Punkte)
 - d** Für keinen Punkt z des Randes seines Konvergenzgebietes ist f auf eine offene Umgebung von z holomorph fortsetzbar. (2 Punkte)
-

Thema Nr. 3 (Aufgabengruppe)

Aufgabe 1 → S. 616

Es sei $f: \mathbb{C} \setminus \{0\} \rightarrow \mathbb{C}, z \mapsto \sin\left(\frac{1}{z}\right)$.

- a** Bestimmen Sie den Typ der isolierten Singularität von f bei 0. (2 Punkte)
- b** Es sei $\gamma: [0, 2\pi] \rightarrow \mathbb{C} \setminus \{0\}, t \mapsto e^{2it}$. Berechnen Sie $\int_{\gamma} f(z) dz$. (2 Punkte)
- c** Es sei $U := \{z \in \mathbb{C} : \frac{1}{2} < |z| < 2\}$. Zeigen Sie, dass es keine Folge von Polynomfunktionen $(p_n: \mathbb{C} \rightarrow \mathbb{C})_{n \in \mathbb{N}}$ gibt, sodass $(p_n|_U)_{n \in \mathbb{N}}$ lokal gleichmäßig gegen $f|_U$ konvergiert. (2 Punkte)

Aufgabe 2 → S. 617

- a** Zeigen Sie, dass $f: [0, \infty[\rightarrow \mathbb{R}, x \mapsto \frac{x}{1+x^3}$ stetig und integrierbar ist. (1 Punkt)

- b** Berechnen Sie $\int_0^\infty \frac{x}{1+x^3} dx$. (5 Punkte)

Hinweis Sie können einen geschlossenen Weg verwenden, der durch 0, R und $e^{\frac{2\pi i}{3}}$ geht, oder die Partialbruch-Zerlegung benutzen.

Aufgabe 3 → S. 619

Zeigen Sie:

- a** Ist $S := \{z \in \mathbb{C} : |\operatorname{Im}(z)| < 1\}$, so gibt es keine biholomorphe Abbildung $f: S \rightarrow \mathbb{C}$. (1.5 Punkte)

- b** Es gibt keine holomorphe Abbildung $f: \mathbb{C} \rightarrow \mathbb{C}$ mit $f(0) = 2i$ und $|f(z)| = 1$ für alle $z \in \mathbb{C}$ mit $|z| = 1$. (1.5 Punkte)

- c** Ist $U := \{z \in \mathbb{C} : 1 < |z| < 3\}$ und $f: U \rightarrow \mathbb{C}$ holomorph mit $f(-2) = 1$ und $f(2) = -1$, dann gibt es $z, w \in U$ mit $f(z), f(w) \in \mathbb{R}$ und $f(z) < -1, f(w) > 1$. (1.5 Punkte)

- d** Es gibt eine Folge $(z_n)_{n \in \mathbb{N}}$ in $\mathbb{C} \setminus \{0\}$ mit $z_n \xrightarrow{n \rightarrow \infty} 0$ und $e^{\frac{1}{z_n}} \xrightarrow{n \rightarrow \infty} i$. (1.5 Punkte)

Aufgabe 4 → S. 620

Zeigen Sie:

- a** Das Anfangswertproblem

$$\dot{x} = (x^2 - 1) \sin t \quad , \quad x(0) = 0$$

hat eine eindeutige auf ganz \mathbb{R} definierte, beschränkte Lösung. (3 Punkte)

- b** Zu jedem $\tau \in \mathbb{R}$ und $\xi \in \mathbb{R}^2$ existieren die maximalen Lösungen des Differentialgleichungssystems

$$\begin{aligned}\dot{x} &= -2y \\ \dot{y} &= 2x + 4x^3\end{aligned}$$

zur Anfangsbedingung $\begin{pmatrix} x(\tau) \\ y(\tau) \end{pmatrix} = \xi$ auf ganz \mathbb{R} . (3 Punkte)

Aufgabe 5 → S. 621

Es sei $A := \begin{pmatrix} -1 & 1 & -1 \\ 0 & 0 & -1 \\ 1 & -1 & -1 \end{pmatrix}$.

- a** Bestimmen Sie die Fundamentalmatrix e^{At} zu $\dot{x} = Ax$. (4 Punkte)
- b** Bestimmen Sie die Lösung von

$$\dot{x} = Ax, \quad x(1) = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$$

(1 Punkt)

- c** Zeigen Sie, dass die Ruhelage $\begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$ stabil ist. (1 Punkt)

Lösungen zu Thema Nr. 1

Lösungsvorschlag zur Aufgabe (Frühjahr 2016, T1A1)

a Wir definieren

$$f: \mathbb{C} \setminus \{-1, 1\} \rightarrow \mathbb{C}, \quad z \mapsto \sin\left(\frac{1}{z-1}\right) - \sin\left(\frac{1}{z+1}\right).$$

Auf ihrem Definitionsbereich ist die Funktion gemäß der Quotienten- und Kettenregel holomorph. Wir zeigen, dass die beiden Singularitäten ± 1 wesentlich sind, indem wir den Hauptteil der Laurent-Reihenentwicklung in diesen Punkten angeben. Entwickeln wir f zunächst auf der punktierten Umgebung $B_2(1) \setminus \{1\}$. Hier ist der zweite Summand holomorph, sodass dessen Hauptteil verschwindet. Für den ersten Summanden erhalten wir

$$\sin\left(\frac{1}{z-1}\right) = \sum_{k=0}^{\infty} (-1)^k \frac{(z-1)^{-(2k+1)}}{(2k+1)!}$$

und sehen an dieser Darstellung, dass der Hauptteil der Reihe nicht abbricht und $\text{Res}(f; 1) = 1$ gilt.

In analoger Weise genügt es, Hauptteil des zweiten Summanden auf dem Bereich $B_2(-1) \setminus \{-1\}$ zu betrachten. Wir erhalten mit

$$-\sin\left(\frac{1}{z+1}\right) = -\sum_{k=0}^{\infty} (-1)^k \frac{(z+1)^{-(2k+1)}}{(2k+1)!}$$

wiederum einen nicht-abbrechenden Hauptteil sowie $\text{Res}(f; -1) = -1$ wie gewünscht.

Eine Funktion ist durch diese Eigenschaften nicht eindeutig bestimmt. Beispielsweise kann einfach eine beliebige ganze Funktion addiert werden, ohne dass sich am Typ der Singularitäten oder an den Residuen etwas ändert.

b Das Integral existiert genau dann, wenn keine der Singularitäten auf γ_α liegt. Alle Punkte der geraden Verbindung von $-2 - i$ und $-2 + i$ haben Realteil -2 , also liegt hier sicher keine Singularität. Analoges gilt für die gerade Verbindung von $2 - \alpha i$ und $2 + \alpha i$. Das Geradenstück zwischen $2 + \alpha i$ und $-2 - i$ parametrisieren wir durch

$$\gamma: [0, 1] \rightarrow \mathbb{C}, \quad t \mapsto (1-t)(2 + \alpha i) + t(-2 - i) = (2 - 4t) + i(\alpha - \alpha t - t).$$

Es ist $\gamma(t) = 1$, wenn

$$2 - 4t = 1 \quad \text{und} \quad \alpha - \alpha t - t = 0$$

gilt. Die erste Gleichung liefert $t = \frac{1}{4}$ und Einsetzen in die zweite ergibt $\alpha = \frac{1}{3}$. Eine analoge Überlegung zeigt, dass $\gamma(t) = -1$ im Fall $t = \frac{3}{4}$ und $\alpha = 3$ gilt. Für den Weg

$$\delta: [0, 1] \rightarrow \mathbb{C}, \quad t \mapsto (1-t)(-2+i) + t(2-\alpha i) = -(2+4t) - i(1-t-\alpha t)$$

ergeben sich genau dieselben Werte für α und t , was zeigt, dass das Wegintegral für $\alpha \notin \{\frac{1}{3}, 3\}$ existiert.

Wir bestimmen im Folgenden die Umlaufzahlen intuitiv. Für $\alpha \in [0, \frac{1}{3}[$ werden beide Punkte einmal in negativer Richtung umlaufen, also haben wir hier mit dem Residuensatz

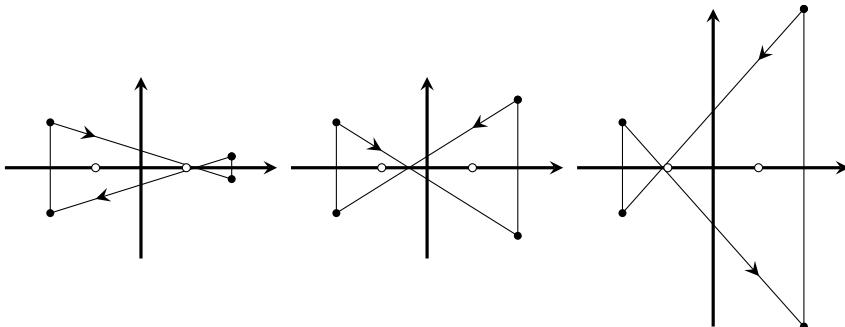
$$\int_{\gamma_\alpha} f(z) dz = 2\pi i((-1) \operatorname{Res}(f; 1) + (-1) \operatorname{Res}(f; -1)) = 2\pi i(-1 + 1) = 0.$$

Für $\alpha \in]\frac{1}{3}, 3[$ wird 1 in positiver, -1 in negativer Richtung umlaufen, sodass wir hier

$$\int_{\gamma_\alpha} f(z) dz = 2\pi i(1 \operatorname{Res}(f; 1) + -1 \operatorname{Res}(f; -1)) = 4\pi i$$

erhalten. Für $\alpha \in]3, \infty[$ werden beide Punkte schließlich in positiver Richtung umlaufen und wir haben

$$\int_{\gamma_\alpha} f(z) dz = 2\pi i(\operatorname{Res}(f; 1) + \operatorname{Res}(f; -1)) = 0.$$



Die Abbildungen zeigen die Kurven γ_α für $\alpha = \frac{1}{4}$, $\alpha = 1.5$ und $\alpha = 3.5$.

Lösungsvorschlag zur Aufgabe (Frühjahr 2016, T1A2)

- a** Wir zeigen die Aussage durch vollständige Induktion über n . Im Fall $n = 1$ ist

$$\sum_{k=1}^1 (4k^3 - 6k^2) = 4 \cdot 1^3 - 6 \cdot 1^2 = -2 = 1^4 - 2 \cdot 1^2 - 1,$$

die Aussage also wahr. Setzen wir die Aussage daher für ein n als bereits bewiesen voraus. Unter Verwendung des binomischen Lehrsatzes gilt dann:

$$\begin{aligned} \sum_{k=1}^{n+1} (4k^3 - 6k^2) &= 4(n+1)^3 - 6(n+1)^2 + \sum_{k=1}^n (4k^3 - 6k^2) = \\ &\stackrel{(I.V.)}{=} 4(n+1)^3 - 6(n+1)^2 + n^4 - 2n^2 - n = \\ &= 4(n^3 + 3n^2 + 3n + 1) - 4(n^2 + 2n + 1) - 2(n+1)^2 \\ &\quad + n^4 - 2n^2 + 1 - (n+1) = \\ &= (n^4 + 4n^3 + 6n^2 + 4n + 1) - 2(n+1)^2 - (n+1) = \\ &= (n+1)^4 - 2(n+1)^2 - (n+1) \end{aligned}$$

- b** Sei $r \in \mathbb{N}_0$ beliebig vorgegeben. Der Induktionsanfang lautet hier

$$G_r(1) = \prod_{l=0}^{r-1} (1+l) = \frac{1+r}{1+r} \prod_{l=0}^{r-1} (1+l) = \frac{1}{r+1} \prod_{l=0}^r (1+l) = \frac{1}{r+1} G_{r+1}(1).$$

Gehen wir daher zum Induktionsschritt über:

$$\begin{aligned} \sum_{k=1}^{n+1} G_r(k) &= G_r(n+1) + \sum_{k=1}^n G_r(k) = \\ &\stackrel{(I.V.)}{=} G_r(n+1) + \frac{1}{r+1} G_{r+1}(n) = \\ &= \prod_{l=0}^{r-1} (n+1+l) + \frac{1}{r+1} \prod_{l=1}^r (n+l) = \\ &= \frac{1}{r+1} \left((r+1) \prod_{l=0}^{r-1} (n+l+1) + n \prod_{l=1}^{r-1} (n+l+1) \right) = \\ &= \frac{1}{r+1} \prod_{l=0}^{r-1} (n+l+1) \cdot ((r+1)+n) = \\ &= \frac{1}{r+1} \prod_{l=0}^r (n+1+l) = \frac{1}{r+1} G_{r+1}(n+1) \end{aligned}$$

Lösungsvorschlag zur Aufgabe (Frühjahr 2016, T1A3)

- a** Die Menge D ist ein Gebiet mit $(0, 0) \in D$, wegen $\|x\| \neq 1$ für $(x_1, x_2) \in D$ ist f auf D stetig. Mit der umgekehrten Dreiecksungleichung folgt

$$\left| \|x\| - \|y\| \right| \stackrel{(\nabla)}{\leq} \|x - y\|,$$

also ist $\|\cdot\|: \mathbb{R}^2 \rightarrow \mathbb{R}$ Lipschitz-stetig. Daraus folgert man leicht, dass auch die Abbildung $x \mapsto 1 - \|x\|$ Lipschitz-stetig ist. Betrachte nun für $\|x\| < 1$ die Abbildung $x \mapsto \frac{1}{1 - \|x\|}$. Sei U eine offene und genügend kleine Umgebung eines Punktes $x_1 \in D$, sodass der Abschluss \bar{U} ebenfalls in D liegt. Dann ist \bar{U} beschränkt und abgeschlossen, also kompakt, sodass $x \mapsto (1 - \|x\|)^{-1}$ dort ein Maximum M annimmt. Wir erhalten für $x_2 \in \bar{U}$:

$$\|f(x_1) - f(x_2)\| = \left\| \frac{(1 - \|x_2\|) - (1 - \|x_1\|)}{(1 - \|x_2\|)(1 - \|x_1\|)} \right\| \leq L \cdot M^2 \|x_1 - x_2\|,$$

wobei L die Lipschitz-Konstante von $x \mapsto 1 - \|x\|$ beschreibt. Somit ist $x \mapsto \frac{1}{1 - \|x\|}$ zumindest lokal Lipschitz-stetig. Insgesamt haben wir damit gezeigt, dass die Komponentenfunktionen f_1 und f_2 von f Lipschitz-stetig sind. Seien L_1, L_2 die zugehörigen Lipschitz-Konstanten. Dann gilt

$$\|f(x_1, x_2)\| = \sqrt{f_1(x_1, x_2)^2 + f_2(x_1, x_2)^2} \leq \sqrt{L_1^2 + L_2^2} =: L$$

Also ist auch f selbst Lipschitz-stetig bezüglich x . Damit folgt aus dem Globalen Existenz- und Eindeutigkeitssatz, dass das angegebene Anfangswertproblem eine eindeutig bestimmte, maximale Lösung hat.

- b** Sei $I =]a, b[$ und $x = (x_1, x_2): I \rightarrow \mathbb{R}^2$ eine Lösung der Gleichung, dann gilt laut Definition einer Lösung insbesondere $\|(x_1(t), x_2(t))\| < 1$ für $t \in I$. Es ist $\|x(t)\| \geq |x_1(t)|$. Für die erste Komponente gilt die Abschätzung

$$x_1(t) = \int_0^t \frac{1}{1 - \|(x_1(s), x_2(s))\|} ds \geq \int_0^t 1 ds = t.$$

Wäre also $b > 1$, so wäre $1 \in I$ und $\|x_1(1)\| \geq 1$ – im Widerspruch dazu, dass laut Definition einer Lösung $x(t) \in D$ für alle $t \in I$ gelten muss.

Wir verwenden nun den Satz vom Randverhalten maximaler Lösungen: Wegen $x(t) \in D$ ist $\|x\|$ durch 1 beschränkt, $b = \infty$ hatten wir gerade ausgeschlossen, also kommt nur $\lim_{t \rightarrow b} \text{dist}(\|x(t)\|, \partial D) = 0$ in Frage. Zusammen mit $\partial D = \{x \in D \mid |x| = 1\}$ bedeutet dies gerade, dass $x(b) = \lim_{t \rightarrow b} x(t)$ existiert und $|x(b)| = 1$ gilt.

Für die letzte zu zeigende Aussage schreiben wir die Punkte der Trajektorie $\{(x_1(t), x_2(t)) \mid t \in I\}$ als Graph einer Funktion $x_2(x_1)$. Aus der Differentialgleichung folgt unter Verwendung der Kettenregel

$$\begin{aligned} \frac{dx_2}{dt}(x_1(t)) &= \frac{dx_2}{dx_1}(x_1(t)) \cdot \frac{dx_1}{dt}(t) \quad \Leftrightarrow \\ \Leftrightarrow \quad \frac{dx_2}{dx_1} &= \frac{dx_2}{dt} \cdot \left(\frac{dx_1}{dt} \right)^{-1} = \|(x_1, x_2)\| (1 - \|(x_1, x_2)\|). \end{aligned}$$

Die zugehörige Integralgleichung lautet

$$x_2(x_1) = \int_0^{x_1} \|(x_1, x_2)\| (1 - \|(x_1, x_2)\|) dx_1,$$

wobei der Integrand wegen $0 \leq \|(x_1, x_2)\| < 1$ nicht-negativ ist. Wir schätzen den Integranden geeignet nach oben ab: Betrachte dazu die Funktion $g(t) = t(1-t) = -t^2 + t$. Es gilt $g'(t) = 0$ genau für $t = \frac{1}{2}$, also hat diese bei $(\frac{1}{2}, \frac{1}{4})$ ein Maximum. Der Integrand ist nun gerade $g(\|(x_1, x_2)\|)$, also folgt für $x_1 \in]0, 1[$

$$x_2(x_1) \leq \int_0^{x_1} \frac{1}{4} dt = \frac{1}{4} x_1 < \frac{1}{4}.$$

Insbesondere haben wir also $0 < x_2(b) < \frac{1}{4}$.

Lösungsvorschlag zur Aufgabe (Frühjahr 2016, T1A4)

- a) Sei $\lambda: I \rightarrow \mathbb{R}$ eine Lösung der Differentialgleichung. Angenommen, die Ableitung λ' besitzt eine Nullstelle $\tau \in I$, d.h. $\lambda'(\tau) = 0$. Dann folgt

$$0 = \lambda'(\tau) = f(\lambda(\tau)),$$

sodass $\lambda(\tau)$ eine Nullstelle von f sein muss. Die konstante Funktion $t \mapsto \lambda(\tau)$ ist dann eine Lösung der Differentialgleichung, die auf ganz \mathbb{R} definiert ist. Da f stetig differenzierbar ist, ist der Globale Existenz- und Eindeutigkeitssatz auf die Differentialgleichung anwendbar, sodass $t \mapsto \lambda(\tau)$ die eindeutige maximale Lösung von

$$x' = f(x), \quad x(\tau) = \lambda(\tau)$$

ist. Nun ist λ ebenfalls eine Lösung dieser Differentialgleichung, weshalb λ eine Einschränkung dieser konstanten Lösung sein muss. Insbesondere ist λ selbst konstant.

Sei λ eine nicht-konstante Lösung, dann folgt aus dem gerade Gezeigten, dass die Ableitung λ' keine Nullstelle hat. Folglich muss für alle $t \in I$ entweder $\lambda(t) > 0$ oder $\lambda(t) < 0$ gelten. Das bedeutet gerade, dass λ entweder streng monoton steigend oder streng monoton fallend ist.

- b** Betrachte als Gegenbeispiel die Funktion $f: \mathbb{R} \rightarrow \mathbb{R}, x \mapsto \sqrt{|x|}$, welche stetig, aber nicht stetig differenzierbar in 0 ist. Das Anfangswertproblem $\dot{x} = f(x), x(0) = 0$ besitzt dann die Lösung

$$\lambda: \mathbb{R} \rightarrow \mathbb{R}, \quad t \mapsto \begin{cases} \frac{1}{4}t^2 & \text{für } t > 0, \\ 0 & \text{für } t \leq 0. \end{cases}$$

Auf diese Lösung trifft keine der drei Charakterisierungen aus Teil **a** zu, denn es ist $\lambda(-1) = \lambda(0)$, also ist λ nicht streng monoton, wegen $\lambda(2) = 1 \neq \lambda(0)$ aber auch nicht konstant.

Lösungsvorschlag zur Aufgabe (Frühjahr 2016, T1A5)

- a** Betrachte zunächst für $n \in \mathbb{N}$ die Ableitung

$$f'_n(x) = \frac{1}{n^2} e^{-\frac{x}{n}} + \frac{x}{n^2} \cdot \left(\frac{-1}{n}\right) e^{-\frac{x}{n}} = \frac{1}{n^2} e^{-\frac{x}{n}} \left(1 - \frac{x}{n}\right).$$

Die Ableitung verschwindet also genau dann, wenn $x = n$ gilt, und hat dort einen Vorzeichenwechsel von $+$ nach $-$. Folglich besitzt f_n ein globales Maximum bei n und es gilt für alle $x \in \mathbb{R}_0^+$ unter Verwendung von $f_n(x) \geq 0$, dass

$$|f_n(x)| = f_n(x) \leq f_n(n) = \frac{n}{n^2} e^{-\frac{n}{n}} = \frac{1}{ne}.$$

Für ein vorgegebenes $\varepsilon > 0$ wähle nun $N \in \mathbb{N}$ so groß, dass $N > \frac{1}{\varepsilon e}$, dann gilt für alle $n \geq N$ und $x \in [0, \infty[$, dass

$$|f_n(x)| \leq \frac{1}{ne} \leq \frac{1}{Ne} < \frac{\varepsilon e}{e} = \varepsilon.$$

Dies zeigt die gleichmäßige Konvergenz der Folge $(f_n)_{n \in \mathbb{N}}$ auf $[0, \infty[$ gegen 0. Als Konsequenz lassen sich Integration und Grenzwertübergang vertauschen:

$$\lim_{n \rightarrow \infty} \int_0^\infty f_n(x) dx = \int_0^\infty \lim_{n \rightarrow \infty} f_n(x) dx = \int_0^\infty 0 dx = 0.$$

b Ist $0 \leq q < 1$, so konvergiert $\sum_{k=0}^{\infty} q^n$ als geometrische Reihe, also muss $(q^n)_{n \in \mathbb{N}}$ gegen 0 konvergieren. Aufgrund der Stetigkeit von f folgt, dass

$$\lim_{n \rightarrow \infty} f(q^n) = f\left(\lim_{n \rightarrow \infty} q^n\right) = f(0) = 0.$$

Das bedeutet, die Folge $(f(x^n))_{n \in \mathbb{N}}$ konvergiert auf $[0, 1[$, und damit fast überall auf $[0, 1]$, punktweise gegen 0.

Die Folge $f(x^n)$ konvergiert im Allgemeinen jedoch nicht gleichmäßig auf $[0, 1[$ gegen 0, weshalb wir hier nicht analog zu Teil **a** argumentieren können. Wir verwenden daher den Satz über majorisierte Konvergenz. Dieser besagt, dass sich Grenzwertbildung und Integration auch dann vertauschen lassen, wenn die Funktionenfolge f_n fast überall punktweise gegen f konvergiert, und es eine integrierbare positive Funktion g gibt, so dass $|f(x)| \leq g(x)$ für $x \in I$ gilt.

Die erste Voraussetzung haben wir bereits gezeigt. Zusätzlich ist f als stetige Funktion auf dem kompakten Intervall $[0, 1]$ beschränkt, d. h. es gibt ein $c \in \mathbb{R}$, sodass $|f(x)| \leq c$ für alle $x \in [0, 1]$ gilt. Wegen $x^n \in [0, 1]$ für alle $x \in [0, 1]$ ist insbesondere auch $|f(x^n)| \leq c$ für alle $n \in \mathbb{N}$, also auch $|f(x)| \leq c$. Damit folgt mit dem eben zitierten Satz

$$\lim_{n \rightarrow \infty} \int_0^1 f(x^n) dx = \int_0^1 \lim_{n \rightarrow \infty} f(x^n) dx = \int_0^1 0 dx = 0.$$

Lösungen zu Thema Nr. 2

Lösungsvorschlag zur Aufgabe (Frühjahr 2016, T2A1)

Das Integral existiert, da das Nennerpolynom in \mathbb{R} nullstellenfrei ist und sein Grad um mehr als 2 größer als der des Zählerpolynoms ist. Für $R \in \mathbb{R}^+$ definiere die Wege

$$\gamma_1: [-R, R] \rightarrow \mathbb{C}, \quad t \mapsto t, \quad \gamma_2: [0, \pi] \rightarrow \mathbb{C}, \quad t \mapsto Re^{it}.$$

Diese Wege bilden zusammen einen geschlossenen, in \mathbb{C} nullhomologen Weg, der sein Inneres genau einmal umläuft. Nach dem Residuensatz gilt daher

$$\int_{\gamma_1 * \gamma_2} f(z) dz = 2\pi i \cdot \sum_{a \in M} \operatorname{Res}(f; a),$$

wobei $f(z) = \frac{2}{z^6 + 3}$ und M die Menge der von $\gamma_1 * \gamma_2$ umlaufenden Singularitäten von f bezeichnet. Ist z eine Nullstelle des Nenners, so gilt

$$|z|^6 = |z^6| = |-3| = 3 \Leftrightarrow |z| = \sqrt[6]{3}.$$

Also existiert ein $\varphi \in [0, 2\pi[,$ sodass $z = \sqrt[6]{3}e^{i\varphi}$. Die Äquivalenz

$$z^6 = -3 \Leftrightarrow 3e^{6i\varphi} = 3e^{i\pi} \Leftrightarrow 6i\varphi = i\pi + 2k\pi i \quad (k \in \mathbb{Z})$$

liefert somit die Nullstellen

$$\begin{aligned} z_1 &= \sqrt[6]{3}e^{i\pi/6}, & z_2 &= \sqrt[6]{3}e^{3i\pi/6}, & z_3 &= \sqrt[6]{3}e^{5i\pi/6}, \\ z_4 &= \sqrt[6]{3}e^{7i\pi/6}, & z_5 &= \sqrt[6]{3}e^{9i\pi/6}, & z_6 &= \sqrt[6]{3}e^{11i\pi/6}. \end{aligned}$$

Da nur z_1, z_2 und z_3 positiven Imaginärteil haben, werden nur diese drei Punkte von $\gamma_1 * \gamma_2$ umlaufen. Außerdem sind sämtliche Nullstellen einfache Nullstellen von $z^6 - 3$, also Pole 1. Ordnung von f . Die Residuen berechnen sich daher zu

$$\text{Res}(f; z_1) = \frac{2}{6z_1^5}, \quad \text{Res}(f; z_2) = \frac{2}{6z_2^5}, \quad \text{Res}(f; z_3) = \frac{2}{6z_3^5}.$$

Ihre Summe beträgt

$$\begin{aligned} &\frac{1}{3 \cdot \sqrt[6]{3}^5} \cdot \left(e^{-5\pi i/6} + e^{-15\pi i/6} + e^{-25\pi i/6} \right) = \\ &= \frac{1}{3 \cdot \sqrt[6]{3}^5} \cdot \left(e^{-5\pi i/6} + e^{-\pi i/2} + e^{-\pi i/6} \right) = \\ &= \frac{1}{3 \cdot \sqrt[6]{3}^5} \cdot \left(\cos\left(\frac{-5\pi}{6}\right) + i \sin\left(\frac{-5\pi}{6}\right) - i + \cos\left(\frac{-\pi}{6}\right) + i \sin\left(\frac{-\pi}{6}\right) \right) = \\ &= \frac{1}{3 \cdot \sqrt[6]{3}^5} \cdot (-2i). \end{aligned}$$

Man erhält daher

$$\int_{\gamma_1 * \gamma_2} f(z) dz = 2\pi i \cdot \frac{1}{3 \cdot \sqrt[6]{3}^5} \cdot (-2i) = \frac{4\pi}{3\sqrt[6]{3}^5}.$$

Nun fehlt noch die obligatorische Abschätzung für den oberen Integrationsweg. Es gilt für $R > \sqrt[6]{3}$:

$$\begin{aligned} \left| \int_{\gamma_2} f(z) dz \right| &\leq \int_0^\pi \left| \frac{2 \cdot i R e^{it}}{R^6 e^{6it} + 3} \right| dt \stackrel{(\nabla)}{\leq} \int_0^\pi \frac{2R}{|R^6 e^{6it} + 3|} dt = \\ &= \int_0^\pi \frac{2R}{R^6 - 3} dt = \frac{2\pi R}{R^6 - 3}. \end{aligned}$$

Diese zeigt, dass das Integral entlang γ_2 für $R \rightarrow \infty$ verschwindet. Jetzt muss nur noch alles zusammen gesetzt werden:

$$\int_{-\infty}^{\infty} f(x) dx = \lim_{R \rightarrow \infty} \left(\int_{\gamma_1 * \gamma_2} f(z) dz - \int_{\gamma_2} f(z) dz \right) = \frac{4\pi}{3\sqrt[6]{3^5}}.$$

Lösungsvorschlag zur Aufgabe (Frühjahr 2016, T2A2)

a Definiere die Funktion

$$f: \mathbb{R}^3 \rightarrow \mathbb{R}^2, \quad (t, x, y) \mapsto (y, -\sin(x)).$$

Diese ist lokal Lipschitz-stetig bezüglich der zweiten Komponente, da

$$\partial_{(x,y)} f(t, x, y) = \begin{pmatrix} 0 & 1 \\ \cos x & 0 \end{pmatrix}$$

stetige Einträge hat und deshalb stetig ist. Außerdem gilt für alle $(t, x, y) \in \mathbb{R}^3$ die Abschätzung

$$\begin{aligned} \|f(t, x, y)\| &= \|(y, -\sin x)\| \stackrel{(\Delta)}{\leq} \|(y, 0)\| + \|(0, -\sin x)\| = \\ &= \sqrt{y^2} + \sqrt{\sin(x)^2} \leq \sqrt{x^2 + y^2} + 1 = \|(x, y)\| + 1. \end{aligned}$$

Dies zeigt, dass f linear beschränkt ist, sodass das gegebene Differentialgleichungssystem eine auf ganz \mathbb{R} definierte eindeutige Lösung $\phi_{z_0}: \mathbb{R} \rightarrow \mathbb{R}^2$ zum Anfangswert $z_0 = (x_0, y_0) \in \mathbb{R}^2$ besitzt.

b Man berechnet

$$\nabla F(x, y) = \begin{pmatrix} \sin x \\ y \end{pmatrix}.$$

Sei $\phi_{z_0}(t)$ eine Lösung der Differentialgleichung, so gilt

$$\frac{d}{dt} F(\phi_{z_0}(t)) = \langle \nabla F(\phi_{z_0}(t)), \phi'_{z_0}(t) \rangle = \left\langle \begin{pmatrix} \sin x(t) \\ y(t) \end{pmatrix}, \begin{pmatrix} y(t) \\ -\sin x(t) \end{pmatrix} \right\rangle = 0.$$

c Betrachte die Funktion

$$H: D \rightarrow \mathbb{R}, \quad (x, y) \mapsto \frac{1}{2}y^2 - \cos x + 1,$$

wobei die Menge D definiert ist als

$$D = \{(x, y) \in \mathbb{R}^2 \mid -\pi < x < \pi\}.$$

Diese ist eine Lyapunov-Funktion für die gegebene Differentialgleichung, denn wie in Teil **b** ist $\langle \nabla H(x, y), f(t, x, y) \rangle = 0$ und es gilt

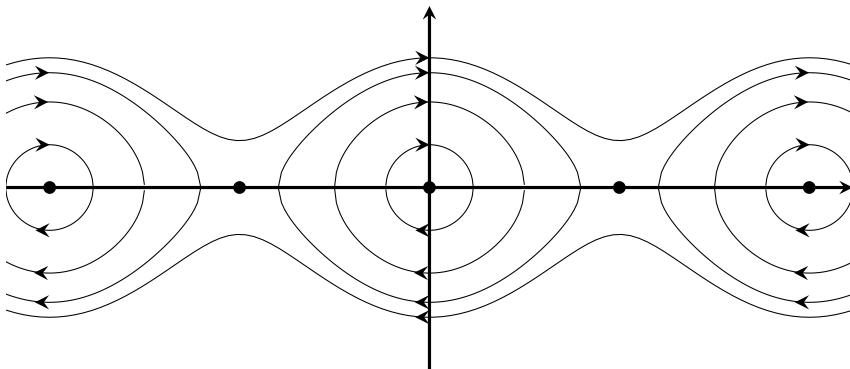
$$H(x, y) = \frac{1}{2}y^2 - \cos x + 1 \geq \frac{1}{2}y^2 - 1 + 1 \geq \frac{1}{2}y^2 \geq 0.$$

Dabei gilt $H(x, y) = 0$ genau dann, wenn $(x, y) = (0, 0)$, denn ist $y \neq 0$, so ist auf jeden Fall $H(x, y) \geq \frac{1}{2}y^2 > 0$, und ist $y = 0$, so ist

$$H(x, 0) = 0 \Leftrightarrow -\cos x - 1 = 0 \Leftrightarrow \cos x = 1 \Leftrightarrow x \in 2\pi\mathbb{Z}.$$

Da wir unsere Betrachtungen auf den Streifen D beschränkt haben, muss in diesem Fall $x = 0$ sein. Insgesamt zeigt dies, dass $(0, 0)$ ein stabiles Gleichgewicht ist. Jedoch kann $(0, 0)$ kein asymptotisch stabiles Gleichgewicht sein, denn für eine Lösung $\lambda: \mathbb{R} \rightarrow \mathbb{R}^2$ mit $\lim_{t \rightarrow \infty} \lambda(t) = 0$ muss wegen der Stetigkeit von F auch $\lim_{t \rightarrow \infty} F(\lambda(t)) = F(0, 0) = -1$ gelten. Nach Teil **b** ist F konstant entlang jeder Trajektorie, daher kann dies nur erfüllt sein, wenn λ bereits die konstante Nulllösung ist.

Das Phasenportrait sieht folgendermaßen aus:



Lösungsvorschlag zur Aufgabe (Frühjahr 2016, T2A3)

Wir bestimmen zunächst das charakteristische Polynom von A :

$$\chi_A = \det \begin{pmatrix} 1-X & 2 & 3 \\ 4 & 5-X & 6 \\ 7 & 8 & 9-X \end{pmatrix} = -X(X^2 - 15X - 18).$$

Die Eigenwerte von A sind daher 0 und

$$\lambda_{\pm} = \frac{15 \pm \sqrt{225 + 72}}{2} = \frac{15 \pm 3\sqrt{33}}{2}.$$

Dabei ist $\lambda_+ > 0$ und $\lambda_- < 0$. Da $r = (1, -2, 1)$ eine Ruhelage ist, muss dieser Vektor im Kern von A liegen. Außerdem ist A diagonalisierbar, da A drei verschiedene Eigenwerte hat und die algebraische und geometrische Vielfachheit daher beide jeweils 1 sind. Seien v_+ bzw. v_- Eigenvektoren zu den Eigenwerten λ_+ bzw. λ_- , dann haben alle Lösungen der Gleichung $\dot{x} = Ax$ die Form

$$ae^{\lambda_+ t}v_+ + be^{\lambda_- t}v_- + cr$$

für $a, b, c \in \mathbb{R}$. Ist $a \neq 0$, so divergiert die Lösung für $t \rightarrow \infty$. Wegen $\lim_{t \rightarrow \infty} e^{\lambda_- t} = 0$ konvergieren ansonsten die Lösungen gegen cr . Diejenigen Lösungen, die für $t \rightarrow \infty$ gegen r konvergieren, sind also genau die Lösungen der Form

$$b \cdot e^{\lambda_- t}v_- + r$$

für ein $b \in \mathbb{R}$ und die zugehörigen Anfangswerte für $t = 0$ sind $bv_- + r$. Den Hinweis interpretieren die Autoren so, dass v_- nicht explizit berechnet werden braucht.

Lösungsvorschlag zur Aufgabe (Frühjahr 2016, T2A4)

- a** *Richtig.* Laut Definition ist eine Funktion $f: [a, b] \rightarrow \mathbb{R}$ gleichmäßig stetig, wenn es für jedes $\varepsilon > 0$ ein $\delta > 0$ gibt, sodass

$$|f(x) - f(y)| < \varepsilon \quad \text{für alle } x, y \in [a, b] \quad \text{mit } |x - y| < \delta.$$

Sei nun $\varepsilon > 0$ und nehmen wir widerspruchshalber an, dass kein solches δ existiert. Dann gibt es für jedes $n \in \mathbb{N}$ Punkte $x_n, y_n \in [a, b]$ mit

$$|x_n - y_n| < \frac{1}{n} \quad \text{aber} \quad |f(x_n) - f(y_n)| \geq \varepsilon.$$

Wir betrachten im Folgenden die so erhaltenen Punkte als zwei Folgen $(x_n)_{n \in \mathbb{N}}$ und $(y_n)_{n \in \mathbb{N}}$. Beide Folgen sind beschränkt, da sie im Inter-

vall $[a, b]$ liegen. Nach dem Satz von Bolzano-Weierstraß enthält $(x_n)_{n \in \mathbb{N}}$ (und analog $(y_n)_{n \in \mathbb{N}}$) somit eine konvergente Teilfolge $(x_{n_k})_{k \in \mathbb{N}}$ (bzw. $(y_{n_k})_{k \in \mathbb{N}}$), deren Grenzwert wiederum in $[a, b]$ liegen muss, da dieses Intervall abgeschlossen ist. Wir notieren $x_0 = \lim_{k \rightarrow \infty} x_{n_k}$. Für $k \in \mathbb{N}$ gilt nun

$$|x_{n_k} - y_{n_k}| < \frac{1}{n_k} \Leftrightarrow x_{n_k} - \frac{1}{n_k} < y_{n_k} < x_{n_k} + \frac{1}{n_k}.$$

und somit $\lim_{k \rightarrow \infty} y_{n_k} = x_0$. Aufgrund der Stetigkeit von f gilt nun aber $\lim_{k \rightarrow \infty} f(x_{n_k}) = f(\lim_{k \rightarrow \infty} x_{n_k}) = f(x_0)$. Dies bedeutet aufgrund der Stetigkeit des Betrags

$$\lim_{k \rightarrow \infty} |f(x_{n_k}) - f(y_{n_k})| = \left| \lim_{k \rightarrow \infty} f(x_{n_k}) - \lim_{k \rightarrow \infty} f(y_{n_k}) \right| = |f(x_0) - f(y_0)| = 0 < \varepsilon,$$

wobei $y_0 = \lim_{k \rightarrow \infty} y_{n_k}$, und stellt damit einen Widerspruch zur Definition der Folgen x_n und y_n dar. Die Annahme war also falsch und es muss ein δ wie in der Definition existieren.

b Falsch. Betrachte dazu die Funktion

$$f:]-1, 1[\rightarrow]-1, 1[, \quad x \mapsto x^3 \quad \text{mit} \quad f^{-1}:]-1, 1[\rightarrow]-1, 1[, \quad x \mapsto \sqrt[3]{x}.$$

Wegen $f'(x) = 3x^2$ ist f zumindest für $x \neq 0$ auf jeden Fall streng monoton steigend. Im Punkt null gilt für beliebig kleines $\varepsilon > 0$, dass $f(-\varepsilon) < 0 < f(\varepsilon)$, sodass auch dort f streng monoton steigend ist. Zudem ist f als Polynom natürlich stetig differenzierbar. Dennoch gilt für die Folge $h_n = \frac{1}{n^3}$ mit $\lim_{n \rightarrow \infty} h_n = 0$

$$\lim_{n \rightarrow \infty} \frac{\sqrt[3]{h_n} - \sqrt[3]{0}}{h_n} = \frac{\frac{1}{n}}{\frac{1}{n^3}} = n^2 = \infty.$$

Somit ist f^{-1} an der Stelle 0 nicht differenzierbar.

Anmerkung Die Aussage stimmt, wenn man zusätzlich $f'(x) \neq 0$ für $x \in]a, b[$ voraussetzt – dann greift nämlich die Umkehrregel.

c Richtig. Unter Verwendung der geometrischen Reihe erhält man für alle $x \in \mathbb{R}$ mit $|x| < 1$ die Reihenentwicklung

$$f(x) = \frac{1}{1+x^2} = \frac{1}{1-(-x^2)} = \sum_{k=0}^{\infty} (-x^2)^k = \sum_{k=0}^{\infty} (-1)^k x^{2k}.$$

Diese Reihe divergiert für $x = 1$, daher beträgt ihr Konvergenzradius genau 1.

Lösungsvorschlag zur Aufgabe (Frühjahr 2016, T2A5)

- a** Sei r der Konvergenzradius von f . Da z^{2^n} für $z = 1$ keine Nullfolge ist, muss $r \leq 1$ sein. Für alle $z \in \mathbb{C}$ mit $|z| < 1$ ist $f(z) = \sum_{n=0}^{\infty} z^{2^n}$ eine Teilreihe der geometrischen Reihe, daher gilt

$$|f(z)| \leq \sum_{n=0}^{\infty} |z|^{2^k} \leq \sum_{n=0}^{\infty} |z|^n < \infty.$$

Also ist die geometrische Reihe eine konvergente Majorante, sodass $r \geq 1$ folgt. Zusammen ergibt das $r = 1$.

Alternative: Formel von Cauchy-Hadamard.

- b** Eine kurze Rechnung zeigt:

$$\begin{aligned} f(z^k) &= \sum_{n=0}^{\infty} (z^{2^k})^{2^n} = \sum_{n=0}^{\infty} z^{2^k \cdot 2^n} = \\ &= \sum_{n=0}^{\infty} z^{2^{k+n}} = \sum_{n=0}^{\infty} z^{2^n} - \sum_{n=0}^{k-1} z^{2^n} = f(z) - \sum_{n=0}^{k-1} z^{2^n} \end{aligned}$$

Laut Aufgabenstellung ist $|z| < 1$, also auch $|z|^{2^n} < 1$ für alle $n \in \mathbb{N}$. Man erhält deshalb aus obiger Gleichung unter Verwendung der Dreiecksungleichung die Abschätzung

$$|f(z^{2^k})| \leq |f(z)| + \sum_{n=0}^{k-1} |z|^{2^k} \leq |f(z)| + \sum_{n=0}^{k-1} 1 = |f(z)| + k.$$

- c** Aufgrund des Ergebnisses aus Teilaufgabe **b** haben wir

$$f(t^{2^k}) = |f((\rho t)^{2^k})| \leq |f(t\rho)| + k$$

für alle $t \in [0, 1[$. Es genügt deshalb zu zeigen, dass $\lim_{t \nearrow 1} f(t) = \infty$. Sei $N \in \mathbb{N}$ vorgegeben, dann gilt für alle $t \in [0, 1[$ die Abschätzung

$$f(t) = \sum_{n=0}^{\infty} t^{2^n} \geq \sum_{n=0}^{N-1} t^{2^n} \geq \sum_{n=0}^{N-1} t^{2^{N-1}} = Nt^{2^{N-1}}$$

und daher auch

$$\lim_{t \nearrow 1} f(t) \geq \lim_{t \nearrow 1} Nt^{2^{N-1}} = N.$$

Da $N \in \mathbb{N}$ beliebig gewählt war, muss bereits $\lim_{t \nearrow 1} f(t) = \infty$ sein.

- d** Angenommen, es gibt ein $z \in \mathbb{C}$ mit $|z| = 1$, sodass sich f holomorph auf eine Umgebung U von z fortsetzen lässt. Wir zeigen, dass in jeder Umgebung von z eine 2^k -te Einheitswurzel für ein gewisses $k \in \mathbb{N}$ liegt. Die Behauptung folgt dann aus Teil **c**.

Schreibe $z = e^{i\theta}$ und sei $w = e^{i\varphi} \in U$ mit $z \neq w$. Wähle $k \in \mathbb{N}$ so groß, dass

$$2^k \cdot \frac{\theta - \varphi}{2\pi} > 2$$

erfüllt ist. Dann gibt es nämlich ein $n \in \mathbb{N}$ mit

$$2^k \frac{\theta}{2\pi} < n < 2^k \frac{\varphi}{2\pi} \Leftrightarrow \theta < \frac{2\pi n}{2^k} < \varphi.$$

Es folgt, dass $\rho = e^{i \frac{2\pi n}{2^k}}$ ein 2^k -te Einheitswurzel in U ist.

Lösungen zu Thema Nr. 3

Lösungsvorschlag zur Aufgabe (Frühjahr 2016, T3A1)

- a** Unter Verwendung der Reihenentwicklung der Sinus-Funktion ist

$$f(z) = \sin(z^{-1}) = \sum_{k=0}^{\infty} (-1)^k \frac{(z^{-1})^{2k+1}}{(2k+1)!}.$$

Der Hauptteil der Laurentreihenentwicklung von f um 0 bricht also nicht ab, sodass 0 eine wesentliche Singularität von f ist.

- b** Die Funktion f hat nur die Singularität 0. Wir berechnen zunächst die Windungszahl von γ um 0:

$$\begin{aligned} n(\gamma, 0) &= \frac{1}{2\pi i} \int_{\gamma} \frac{1}{z} dz = \frac{1}{2\pi i} \int_0^{2\pi} \frac{1}{e^{2it}} \cdot 2ie^{2it} dt = \\ &= \frac{2i}{2\pi} \int_0^{2\pi} 1 dt = \frac{2i}{2\pi} \cdot 2\pi i = 2. \end{aligned}$$

Der Weg γ ist nullhomolog in \mathbb{C} , also können wir den Residuensatz anwenden. Das fehlende Residuum lässt sich an der Laurentreihenentwicklung von f aus Teil **a** ablesen, der Koeffizient vor z^{-1} berechnet sich nämlich mit $k = 0$ zu $\text{Res}(f; 0) = (-1)^0 \cdot \frac{1}{(0+1)!} = 1$.

$$\int_{\gamma} f(z) dz = 2\pi i \cdot n(\gamma, 0) \text{Res}(f; 0) = 4\pi i \cdot \text{Res}(f; 0) = 4\pi i.$$

- c** Nehmen wir an, es gibt eine solche Folge von Polynomen. Aus der gleichmäßigen Konvergenz folgt, dass sich Integration und Grenzwertbildung vertauschen lassen:

$$\int_{\gamma} f(z) dz = \int_{\gamma} \lim_{n \rightarrow \infty} p_n(z) dz = \lim_{n \rightarrow \infty} \int_{\gamma} p_n(z) dz.$$

Als Polynomfunktion ist jedes p_n holomorph auf \mathbb{C} , sodass nach dem Cauchy-Integralsatz

$$\int_{\gamma} p_n(z) dz = 0$$

für jedes $n \in \mathbb{N}$ gilt. Damit erhalten wir den Widerspruch

$$4\pi i \stackrel{\mathbf{b}}{=} \int_{\gamma} f(z) dz = \lim_{n \rightarrow \infty} \int_{\gamma} p_n(z) dz = \lim_{n \rightarrow \infty} 0 = 0.$$

Die Annahme muss daher falsch gewesen sein.

Lösungsvorschlag zur Aufgabe (Frühjahr 2016, T3A2)

- a** Die Funktion f ist Quotient zweier Polynomfunktionen, wobei der Nenner im Intervall $[0, \infty[$ nullstellenfrei ist. Deshalb ist f stetig. Da zusätzlich der Grad des Nennerpolynoms um 2 größer ist als der Grad des Zählerpolynoms, ist f integrierbar.
- b** Wir bestimmen zunächst die Singularitäten von f (in \mathbb{C}). Sei $z \in \mathbb{C}$ eine Nullstelle des Nenner, dann gilt

$$z^3 + 1 = 0 \Leftrightarrow z^3 = -1 \Rightarrow |z|^3 = 1 \Leftrightarrow |z| = 1.$$

Es gibt also ein $\varphi \in [0, 2\pi[,$ sodass $z = e^{i\varphi}$ gilt. Wegen $-1 = e^{i\pi}$ folgt aus

$$z^3 = -1 \Leftrightarrow z^{3i\varphi} = z^{\pi i} \Leftrightarrow 3i\varphi = \pi i + 2k\pi i \quad (k \in \mathbb{Z}),$$

dass die Singularitäten von f durch $z_1 = e^{i\pi/3}, z_2 = e^{i\pi} = -1$ und

$z_3 = e^{5\pi i/3}$ gegeben sind. Definiere nun für ein $R \in \mathbb{R}^+$ den Weg Γ als Verknüpfung von

$$\begin{aligned}\gamma_1: [0, R] &\rightarrow \mathbb{C}, t \mapsto t, & \gamma_2: [0, \frac{2\pi}{3}] \rightarrow \mathbb{C}, t \mapsto Re^{it}, \\ \gamma_3: [0, R] &\rightarrow \mathbb{C}, t \mapsto (R-t)e^{\frac{2\pi i}{3}}.\end{aligned}$$

Der Weg Γ ist nullhomolog in \mathbb{C} und umläuft von den Singularitäten von f nur z_1 einmal. Somit gilt nach dem Residuensatz

$$\int_{\Gamma} f(z) dz = 2\pi i \cdot \operatorname{Res}(f; z_1).$$

Dabei ist

$$\begin{aligned}\int_{\gamma_3} f(z) dz &= \int_{\gamma_3} \frac{z}{1+z^3} dz = \int_0^R \frac{(R-t)e^{2\pi i/3}}{1+(R-t)^3 e^{2\pi i}} \cdot (-e^{2\pi i/3}) dt = \\ &= -e^{4\pi i/3} \int_0^R \frac{(R-t)}{1+(R-t)^3} dt \stackrel{(*)}{=} -e^{4\pi i/3} \int_R^0 \frac{t}{1+t^3} \cdot (-1) dt = \\ &= -e^{4\pi i/3} \int_0^R \frac{t}{1+t^3} dt = -e^{4\pi i/3} \int_{\gamma_1} \frac{z}{1+z^3} dz = -e^{4\pi i/3} \int_{\gamma_1} f(z) dz,\end{aligned}$$

wobei an der Stelle $(*)$ die Substitution $t \mapsto R-t$ angewendet wurde. Weiterhin gilt für $R > 1$ die Abschätzung

$$\begin{aligned}\left| \int_{\gamma_2} f(z) dz \right| &\leq \int_0^{2\pi/3} \left| \frac{iR^2 e^{2it}}{1+R^3 e^{3it}} \right| dt = \int_0^{2\pi/3} \frac{R^2}{|1+R^3 e^{3it}|} dt \leq \\ &\stackrel{(\nabla)}{\leq} \int_0^{2\pi/3} \frac{R^2}{|1-R^3|} dt = \frac{2\pi}{3} \frac{R^2}{R^3-1} = \frac{2\pi}{3} \frac{1}{R-\frac{1}{R^2}} \xrightarrow{R \rightarrow \infty} 0\end{aligned}$$

unter Verwendung der umgekehrten Dreiecksungleichung bei (∇) . Daraus folgt $\lim_{R \rightarrow \infty} \int_{\gamma_2} f(z) dz = 0$ und somit

$$\begin{aligned}\lim_{R \rightarrow \infty} \int_{\Gamma} f(z) dz &= \lim_{R \rightarrow \infty} \left(\int_{\gamma_1} f(z) dz + \int_{\gamma_2} f(z) dz + \int_{\gamma_3} f(z) dz \right) = \\ &= \lim_{R \rightarrow \infty} \left(\int_{\gamma_1} f(z) dz + 0 + \left(-e^{4\pi i/3}\right) \int_{\gamma_1} f(z) dz \right) = \\ &= \lim_{R \rightarrow \infty} \left(1 - e^{4\pi i/3} \right) \int_{\gamma_1} f(z) dz = \left(1 - e^{4\pi i/3} \right) \int_0^{\infty} f(x) dx.\end{aligned}$$

Umstellen dieser Gleichung ergibt

$$\int_0^\infty f(x)dx = \frac{1}{1 - e^{4\pi i/3}} \lim_{R \rightarrow \infty} \int_{\Gamma} f(z)dz = \frac{2\pi i \operatorname{Res}(f; z_1)}{1 - e^{4\pi i/3}}.$$

Wir müssen also nur noch $\operatorname{Res}(f; z_1)$ berechnen. Bemerke dazu $\lim_{z \rightarrow z_1} |f(z)| = \infty$ und

$$\begin{aligned} \lim_{z \rightarrow z_1} (z - z_1)f(z) &= \frac{z_1}{(z_1 - z_2)(z_1 - z_3)} = \frac{e^{i\pi/3}}{(e^{i\pi/3} - e^{i\pi})(e^{i\pi/3} - e^{5i\pi/3})} = \\ &= \frac{e^{i\pi/3}}{e^{2i\pi/3}(1 - e^{2i\pi/3})(1 - e^{4i\pi/3})} = \frac{e^{-i\pi/3}}{1 + 1 - e^{2i\pi/3} - e^{4i\pi/3}} = \\ &= \frac{e^{-i\pi/3}}{2 - 2 \cos \frac{2\pi i}{3}} = \frac{e^{-i\pi/3}}{2(1 - (\frac{-1}{2}))} = \frac{1}{3}e^{-i\pi/3}. \end{aligned}$$

Somit ist z_1 ein Pol 1. Ordnung von f mit $\operatorname{Res}(f; z_1) = \frac{1}{3}e^{-i\pi/3}$. Schlussendlich:

$$\begin{aligned} \int_0^\infty f(x)dx &= \frac{2\pi i \operatorname{Res}(f; z_1)}{1 - e^{4\pi i/3}} = \frac{2\pi i}{3} \cdot \frac{e^{-i\pi/3}}{1 - e^{4\pi i/3}} = \frac{2\pi i}{3} \cdot \frac{1}{e^{i\pi/3} - e^{5\pi i/3}} = \\ &= \frac{2\pi i}{3} \cdot \frac{1}{e^{i\pi/3} - e^{-\pi i/3}} = \frac{2\pi i}{3 \cdot 2i \sin \frac{\pi}{3}} = \frac{\pi}{3 \cdot \frac{\sqrt{3}}{2}} = \frac{2}{9}\pi\sqrt{3}. \end{aligned}$$

Lösungsvorschlag zur Aufgabe (Frühjahr 2016, T3A3)

- a** Angenommen, es gibt eine solche biholomorphe Abbildung $S \rightarrow \mathbb{C}$. Es wäre dann auch $f^{-1}: \mathbb{C} \rightarrow S$ holomorph und bijektiv, jedoch liegen beispielsweise $2i$ und $-2i$ nicht in $S = \operatorname{im} f^{-1}$, sodass f^{-1} nach dem kleinen Satz von Picard konstant sein müsste. Eine konstante Funktion ist aber nicht injektiv und deshalb nicht bijektiv.
- b** Nach dem Maximumsprinzip für beschränkte Gebiete würde eine solche Funktion f auf dem Rand $\partial B_1(0)$ der Einheitskreisscheibe ein Betragssmaximum annehmen, d.h. es gäbe ein $z_0 \in \mathbb{C}$ mit $|z_0| = 1$ und $|f(z)| \leq |f(z_0)| = 1$ für alle $z \in \overline{B_1(0)}$. Dies verträgt sich jedoch nicht mit $|f(0)| = |2i| = 2 > 1$. Also kann es dieses f nicht geben.
- c** Der Satz von der Gebietstreue stellt sicher, dass $f(U) \subseteq \mathbb{C}$ wieder offen ist. Es gibt daher $\varepsilon, \varepsilon' > 0$, sodass die Umgebungen $B_\varepsilon(1)$ und $B_{\varepsilon'}(-1)$ von 1 bzw. -1 in $f(U)$ enthalten sind. Insbesondere gilt

$$-1 - \frac{\varepsilon'}{2} \in B_{\varepsilon'}(-1) \subseteq f(U) \quad \text{und} \quad 1 + \frac{\varepsilon}{2} \in B_\varepsilon(1) \subseteq f(U).$$

Es gibt daher $z, w \in U$ mit

$$f(z) = -1 - \frac{\varepsilon}{2} < -1 \quad \text{und} \quad f(w) = 1 + \frac{\varepsilon}{2} > 1.$$

- d** Betrachte die Folge $(z_n)_{n \in \mathbb{N}}$ gegeben durch $z_n = \frac{2}{\pi i + 4\pi n}$, dann gilt $\lim_{n \rightarrow \infty} z_n = 0$ und

$$\lim_{n \rightarrow \infty} e^{\frac{1}{z_n}} = \lim_{n \rightarrow \infty} e^{\frac{\pi i + 4\pi n}{2}} = \lim_{n \rightarrow \infty} e^{\frac{\pi i}{2} + 2\pi i n} = \lim_{n \rightarrow \infty} e^{\frac{\pi i}{2}} = i.$$

Lösungsvorschlag zur Aufgabe (Frühjahr 2016, T3A4)

- a** Definiere die Funktion

$$f: \mathbb{R}^2 \rightarrow \mathbb{R}, \quad (t, x) \mapsto (x^2 - 1) \sin(t),$$

dann schreibt sich die gegebene Differentialgleichung als $\dot{x} = f(t, x)$. Für die partielle Ableitung von f nach x berechnet man

$$\partial_x f(t, x) = 2x \sin(t).$$

Also ist f auf ganz \mathbb{R} partiell stetig differenzierbar nach x , sodass f dort lokal Lipschitz-stetig bezüglich x ist. Nach dem Globalen Existenz- und Eindeutigkeitssatz gibt es daher eine eindeutige maximale Lösung $\lambda: I \rightarrow \mathbb{R}$ von $\dot{x} = f(t, x)$ zum Anfangswert $x(0) = 0$.

Die Differentialgleichung besitzt die konstanten und auf ganz \mathbb{R} definierten Lösungen $t \mapsto 1$ und $t \mapsto -1$. Da sich Lösungskurven maximaler Lösungen nicht schneiden können, folgt aus $-1 < \lambda(0) = 0 < 1$, dass $-1 < \lambda(t) < 1$ für alle $t \in \mathbb{R}$ gilt. Gäbe es nämlich ein $t_1 \in I$, so dass $\lambda(t_1) > 1$ ist, so müsste es nach dem Zwischenwertsatz auch ein $t_2 \in I$ mit $\lambda(t_2) = 1$ geben. Damit hätten wir aber einen Schnittpunkt der Lösungskurven von λ und $t \mapsto 1$ gefunden, den es nicht geben darf.

Da weiterhin der Rand von \mathbb{R}^2 leer ist und wie gesehen $\lambda(t)$ beschränkt ist, muss λ nach der Charakterisierung des Randverhaltens maximaler Lösungen auf ganz \mathbb{R} definiert sein.

- b** Das Differentialgleichungssystem ist hamiltonsch, wie man sieht, indem man die Integrabilitätsbedingung überprüft:

$$\partial_x(-2y) + \partial_y(2x + 4x^3) = 0$$

Eine Hamilton-Funktion ist dann gegeben durch

$$H(x, y) = \int_0^y -2v dv - \int_0^x 2w + 4w^3 dw = -y^2 - x^2 - x^4.$$

Die Hamilton-Funktion ist längs jeder Trajektorie des Systems konstant, die Trajektorien sind also Teilmengen der Mengen

$$\begin{aligned} N(\xi) &= \{(x, y) \in \mathbb{R}^2 \mid H(x, y) = H(\xi)\} = \\ &= \{(x, y) \in \mathbb{R}^2 \mid 0 \leq y^2 + x^2 + x^4 = -H(\xi)\} \\ &\subseteq \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 \leq H(\xi)\} = B_{-H(\xi)}(0). \end{aligned}$$

Damit sind die Trajektorien in der kompakten Menge $B_{-H(\xi)}(0)$ enthalten, bleiben also insbesondere beschränkt. Zusammen mit der Tatsache, dass auch hier der Rand des Definitionsbereiches leer ist, bedeutet dies, dass die zugehörige Lösung auf ganz \mathbb{R} definiert sein muss.

Lösungsvorschlag zur Aufgabe (Frühjahr 2016, T3A5)

a) Zunächst bestimmen wir das charakteristische Polynom von A :

$$\chi_A = \det \begin{pmatrix} -1 - X & 1 & -1 \\ 0 & -X & -1 \\ 1 & -1 & -1 - X \end{pmatrix} = -X(X + 1)^2$$

Die Eigenwerte sind also 0 und -1 , außerdem zerfällt das charakteristische Polynom in Linearfaktoren, sodass die Matrix A zu einer Matrix in Jordan-Normalform ähnlich ist. Auf Seite 250 ist ausführlich beschrieben, wie man die Transformationsmatrizen

$$T = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & -1 & 0 \end{pmatrix} \quad \text{sowie} \quad T^{-1} = \begin{pmatrix} 1 & -1 & 1 \\ 1 & -1 & 0 \\ -1 & 2 & -1 \end{pmatrix}.$$

bestimmt. Es gilt nun

$$J = T^{-1}AT = \begin{pmatrix} -1 & 1 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

und laut Proposition 7.17 gilt $e^{At} = e^{T(T^{-1}AT)T^{-1}} = Te^{It}T^{-1}$. Man berechnet also

$$\begin{aligned} e^{At} &= \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & -1 & 0 \end{pmatrix} \cdot \begin{pmatrix} e^{-t} & te^{-t} & 0 \\ 0 & e^{-t} & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & -1 & 1 \\ 1 & -1 & 0 \\ -1 & 2 & -1 \end{pmatrix} = \\ &= \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & -1 & 0 \end{pmatrix} \cdot \begin{pmatrix} e^{-t} + te^{-t} & -e^{-t} - te^{-t} & e^{-t} \\ e^{-t} & -e^{-t} & 0 \\ -1 & 2 & -1 \end{pmatrix} = \\ &= \begin{pmatrix} te^{-t} + 2e^{-t} - 1 & -te^{-t} - 2e^{-t} + 2 & e^{-t} - 1 \\ te^{-t} + e^{-t} - 1 & -te^{-t} - e^{-t} + 2 & e^{-t} - 1 \\ te^{-t} & -te^{-t} & e^{-t} \end{pmatrix} \end{aligned}$$

b Die gesuchte Lösung ist

$$\begin{aligned} \lambda(t) &= e^{(t-1)A} \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} (t-1)e^{-(t-1)} + 2e^{-(t-1)} - 1 \\ (t-1)e^{-(t-1)} + e^{-(t-1)} - 1 \\ (t-1)e^{-(t-1)} \end{pmatrix} = \\ &= \begin{pmatrix} te^{-(t-1)} + e^{-(t-1)} - 1 \\ te^{-(t-1)} - 1 \\ (t-1)e^{-(t-1)} \end{pmatrix} = e^{-(t-1)} \begin{pmatrix} t+1 \\ t \\ t-1 \end{pmatrix} + \begin{pmatrix} -1 \\ -1 \\ 0 \end{pmatrix}. \end{aligned}$$

c Die Eigenwerte von A wurden bereits in Teil **a** bestimmt, diese sind -1 und 0 . Offensichtlich ist -1 negativ und da der Eigenwert 0 die algebraische Vielfachheit 1 hat, muss auch dessen geometrische Vielfachheit 1 sein. Nach dem Eigenwertkriterium für Stabilität linearer Systeme sind dann alle Lösungen von $\dot{x} = Ax$ stabil.

Prüfungstermin: Herbst 2016

Thema Nr. 1
(Aufgabengruppe)

Aufgabe 1 → S. 629

- a** Sei $U \subset \mathbb{C}$ offen und $f: U \rightarrow \mathbb{C}$ holomorph. Für ein $z_0 \in U$ gelte $|f(z)| \leq |z - z_0|^\alpha$ mit $\alpha > 1$. Zeigen Sie $f(z_0) = 0$ und $f'(z_0) = 0$. (2 Punkte)
- b** Sei $\lambda \in \mathbb{R}$ und sei $u: \mathbb{C} \rightarrow \mathbb{R}$ gegeben durch $u(z) = x^2 + \lambda y^2$ für $z = x + iy$. Bestimmen Sie alle λ , für die u Realteil einer ganzen Funktion $f: \mathbb{C} \rightarrow \mathbb{C}$ ist. Geben Sie für diese λ alle zugehörigen ganzen Funktionen an. (4 Punkte)

Aufgabe 2 → S. 630

Bestimmen Sie für jede der Singularitäten von f im Komplexen den Typ und berechnen Sie das Integral $\int_{|z|=4} f(z) dz$ für

$$\mathbf{a} \quad f(z) = \frac{\sin(z)}{e^z - e^\pi}, \quad \mathbf{b} \quad f(z) = \sin(e^{1/z}).$$

(3+3 Punkte)

Aufgabe 3 → S. 632

Gegeben sei das Anfangswertproblem

$$y' = -\tan(y)e^y, \quad y(0) = -1.$$

- a** Zeigen Sie, dass das Anfangswertproblem eine eindeutige Lösung auf $\mathbb{R}_+ = [0, \infty[$ hat. (3 Punkte)
- b** Bestimmen Sie $\lim_{x \rightarrow \infty} y(x)$. (3 Punkte)

Aufgabe 4 → S. 633

Wir betrachten die Funktion

$$F: \mathbb{R}^2 \rightarrow \mathbb{R}^2, \\ \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} e^x \cos(y + x^3) \\ e^x \sin(y + x^3) \end{pmatrix}$$

- a** Zeigen Sie, dass F beliebig oft differenzierbar ist. (1 Punkt)
- b** Berechnen Sie die Jacobi-Matrix DF . (1 Punkt)
- c** Berechnen die den Flächeninhalt der Menge

$$\Omega := \{F(x, y) \mid 0 \leq y \leq x \leq 1\} \subseteq \mathbb{R}^2.$$

(4 Punkte)

Aufgabe 5 → S. 634

Betrachten Sie das Differentialgleichungssystem

$$\begin{aligned}x' &= -x^3 + 2x^2y - xy^2, \\y' &= -2x^3 - y^3 + x^2y + 2y^4.\end{aligned}$$

Bestimmen Sie alle Ruhelagen und untersuchen Sie diese auf ihre Stabilität.

(6 Punkte)

Thema Nr. 2
(Aufgabengruppe)

Aufgabe 1 → S. 635

- a** Gegeben sei die Funktion $f(z) = z^2\bar{z}, z \in \mathbb{C}$. Bestimmen Sie alle Punkte, in denen die komplexe Ableitung $f'(z)$ existiert. (2 Punkte)
- b** Die Funktion $h(z) = \frac{z^8+z^4+2}{(z-1)^3(9z^2+12z+4)}$ sei für alle $z \in \mathbb{C}$ definiert, für die der Nenner nicht verschwindet. Bestimmen Sie für jede Singularität von h (in \mathbb{C}) den Typ.

Ist $z = \infty$ eine Singularität von h ? Falls ja, von welchem Typ? (2 Punkte)

- c** Sei D das Dreiecksgebiet in der komplexen Ebene, das durch die Punkte $0 + 0i, 1 + 0i$ und $1 + i$ aufgespannt wird. Sei weiter γ ein Weg, dessen Spur den Rand von D gegen den Uhrzeigersinn einmal durchläuft. Berechnen Sie das Wegintegral

$$\int_{\gamma} |z|^2 dz.$$

(2 Punkte)

Aufgabe 2 → S. 637

Welche der folgenden Aussagen sind wahr? Begründen Sei Ihre Antwort.

- a** Jede überall partiell differenzierbare Funktion $f: \mathbb{R}^2 \rightarrow \mathbb{R}$ ist stetig. (2 Punkte)

- b** Sei Ω ein Gebiet in \mathbb{C} und $f: \Omega \rightarrow \mathbb{C}$ eine holomorphe Funktion, und es gebe ein $z_0 \in \Omega$ mit

$$|f(z_0)| \leq |f(z)| \quad \forall z \in \Omega.$$

Dann ist f konstant. (2 Punkte)

- c** Die Funktion

$$f: \mathbb{R} \rightarrow \mathbb{R}, f(x) = \begin{cases} x^2 \sin(1/x) & \text{für } x > 0 \\ 0 & \text{für } x \leq 0 \end{cases}$$

ist auf ganz \mathbb{R} differenzierbar. (2 Punkte)

Aufgabe 3 → S. 638

- a** Zeigen Sie, dass für jedes $n = 1, 2, \dots$ gilt:

$$\int_0^{2\pi} (\cos(\theta))^{2n} d\theta = \frac{\pi(2n)!}{2^{2n-1}(n!)^2}.$$

(2 Punkte)

- b** Für jedes $R > 0$ sei der geschlossene Weg $\gamma_R = \gamma_1 + \gamma_2 + \gamma_3$ (der also zuerst γ_1 , dann γ_2 und zuletzt γ_3 durchläuft) definiert durch

$$\begin{aligned} \gamma_1(x) &= x, & x &\in [0, R] \\ \gamma_2(\theta) &= Re^{i\theta}, & \theta &\in [0, \frac{\pi}{4}] \\ \gamma_3(t) &= -te^{i\pi/4}, & t &\in [-R, 0]. \end{aligned}$$

Betrachten Sie das Wegintegral $\int_{\gamma_R} e^{iz^2} dz$, um zu zeigen, dass die uneigentlichen Integrale

$$\int_0^\infty \sin(x^2) dx \quad \text{und} \quad \int_0^\infty \cos(x^2) dx$$

gleich sind und den gemeinsamen Wert $\sqrt{\frac{\pi}{8}}$ haben.

Hinweis Sie dürfen ohne Beweis verwenden, dass $\int_0^\infty e^{-t^2} = \frac{\sqrt{\pi}}{2}$ und dass $\sin u \geq \frac{2u}{\pi}$ für alle $0 \leq u \leq \pi/2$ gilt. (4 Punkte)

Aufgabe 4 → S. 640

Sei auf \mathbb{R}^3 das Anfangswertproblem

$$\begin{pmatrix} x' \\ y' \\ z' \end{pmatrix} = \begin{pmatrix} yz \\ zx \\ xy \end{pmatrix} = v \begin{pmatrix} x \\ y \\ z \end{pmatrix}, \quad \begin{pmatrix} x(0) \\ y(0) \\ z(0) \end{pmatrix} = \begin{pmatrix} 1 \\ -1 \\ 1 \end{pmatrix}$$

gegeben und sei $u(t) = \begin{pmatrix} \alpha(t) \\ \beta(t) \\ \gamma(t) \end{pmatrix}, t \in J$ dessen maximale Lösung.

- a** Man zeige: Die Funktionen

$$E_1(x, y, z) = x^2 - y^2 \quad \text{und} \quad E_2(x, y, z) = y^2 - z^2$$

sind *erste Integrale* von v . (Ein erstes Integral ist eine Erhaltungsgröße, also eine differenzierbare Funktion E , deren Ableitung längs des Vektorfeldes v verschwindet, d.h. $E'(x, y, z)v(x, y, z) = 0$. Ein erstes Integral ist demnach auf Integralkurven konstant.) (2 Punkte)

- b** Man zeige: Für t nahe 0 gilt $\alpha(t) = -\beta(t) = \gamma(t)$.

Hinweis Es gilt $E_i(u(t)) = E_i(u(0))$ für alle $t, i = 1, 2$. (2 Punkte)

- c** Man bestimme die Lösung $u(t)$ und das maximale Definitionsintervall J . (2 Punkte)

Aufgabe 5 → S. 641

Gegeben sei die Funktion $f: \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}, (t, x) \mapsto |\cos x| + t^2$. Man zeige:

- a** Es gibt ein Intervall $]-\delta, \delta[$, auf dem das Anfangswertproblem $x' = f(t, x), x(0) = 0$ eine und nur eine Lösung besitzt. (2 Punkte)

- b** Ist $\alpha(t), t \in]a, b[$ mit $a < 0 < b$ eine Lösung des vorstehenden Anfangswertproblems, so ist $\tilde{\alpha}(s) = -\alpha(-s), s \in]-b, -a[$ ebenfalls eine Lösung. (2 Punkte)

- c** Sei $\alpha(t), -\infty \leq t^- < t < t^+ \leq +\infty$ die maximale Lösung des Anfangswertproblems.

- (i) Es gilt $t^- = -t^+$.

Hinweis Man verwende **b**.

- (ii) Es gilt $t^- = -\infty, t^+ = \infty$. (2 Punkte)

Thema Nr. 3
(Aufgabengruppe)

Aufgabe 1 → S. 643

Seien $f, g: \mathbb{C} \rightarrow \mathbb{C}$ holomorphe Funktionen mit $g \circ f = 0$. Zeigen Sie, dass $g = 0$ oder f konstant ist. (6 Punkte)

Aufgabe 2 → S. 643

Es sei $\alpha > 0$ ein gegebener Parameter. Betrachten Sie die Folge $(f_n)_{n \in \mathbb{N}}$ von Funktionen $f_n: \mathbb{R} \rightarrow \mathbb{R}$ mit

$$f_n(x) = \begin{cases} \frac{\sin^2(n^\alpha x)}{nx} & \text{falls } x \neq 0 \\ 0 & \text{falls } x = 0. \end{cases}$$

Beweisen Sie:

- a** Jede Funktion f_n ist stetig. (1 Punkt)
- b** Die Folge $(f_n)_{n \in \mathbb{N}}$ konvergiert punktweise gegen die Nullfunktion. (1 Punkt)
- c** Falls $\alpha < 1/2$, so konvergiert die Folge $(f_n)_{n \in \mathbb{N}}$ gleichmäßig.
- Hinweis** Es gilt $|\sin z| \leq |z|$ für alle $z \in \mathbb{R}$. (2 Punkte)
- d** Falls $\alpha \geq 1$, so konvergiert die Folge $(f_n)_{n \in \mathbb{N}}$ nicht gleichmäßig. (2 Punkte)

Aufgabe 3 → S. 644

Sei

$$S := \{z \in \mathbb{C} : 0 < \operatorname{Im} z < 6\pi\}$$

sowie

$$T := \{z = re^{i\varphi} \in \mathbb{C} \setminus \{0\} : r > 0, -\frac{\pi}{4} < \varphi < \frac{\pi}{4}\}.$$

Geben Sie ein biholomorphe Abbildung $\varphi: S \rightarrow T$ an mit

$$\lim_{\operatorname{Re} z \rightarrow \infty} \varphi(z) = \infty.$$

(6 Punkte)

Aufgabe 4 → S. 645

Sei $f: \mathbb{R} \times \mathbb{R}^n \rightarrow \mathbb{R}^n, (t, x) \mapsto f(t, x)$ eine stetige Funktion, die bezüglich der Koordinate x Lipschitz-stetig ist. Zeigen Sie, dass das Differentialgleichungssystem

$$\dot{x} = f(t, x)$$

genau dann autonom ist (d. h. $f(t, x)$ ist von t unabhängig), wenn mit jeder Lösung $\varphi:]a, b[\rightarrow \mathbb{R}^n$ der Differentialgleichung und jedem $\gamma \in \mathbb{R}$ auch $\varphi_\gamma:]a - \gamma, b - \gamma[\rightarrow \mathbb{R}^n$, $\varphi_\gamma(t) = \varphi(t + \gamma)$, eine Lösung ist. (6 Punkte)

Aufgabe 5 → S. 646

- a** Gegeben sei ein autonomes Differentialgleichungssystem $\dot{x} = f(x)$ mit einer stetig differenzierbaren Abbildung $f: \mathbb{R}^n \rightarrow \mathbb{R}^n$, die $f(0) = 0$ erfüllt.

- (i) Definieren Sie den Begriff der asymptotischen Stabilität der stationären Lösung 0 des Systems. (2 Punkte)
- (ii) Geben Sie ein hinreichendes Kriterium für die asymptotische Stabilität der stationären Lösung 0 an, welches die totale Ableitung $Df(0)$ von f in 0 verwendet. (1 Punkte)

- b** Prüfen Sie, ob die stationäre Lösung 0 des Systems

$$\begin{aligned}\dot{x}_1 &= x_1^2 x_2 + \sin x_2 \\ \dot{x}_2 &= 2(1 - e^{x_1}) - 3x_2 + x_1 x_2^2\end{aligned}$$

asymptotisch stabil ist. (3 Punkte)

Lösungen zu Thema Nr. 1

Lösungsvorschlag zur Aufgabe (Herbst 2016, T1A1)

- a** Einsetzen von $z = z_0$ in die Voraussetzung ergibt sofort $|f(z_0)| \leq 0$, also $f(z_0) = 0$.

Entwickeln wir f in einer Umgebung von z_0 in eine konvergente Potenzreihe $f(z) = \sum_{n=0}^{\infty} a_n(z - z_0)^n$, so ist $a_0 = f(z_0) = 0$. Sei $h(z) = \sum_{n=1}^{\infty} a_n(z - z_0)^{n-1}$, dann haben wir $f(z) = (z - z_0)h(z)$ und für alle $z \neq z_0$ gilt

$$|f(z)| = |(z - z_0)h(z)| \leq |z - z_0|^{\alpha} \Leftrightarrow |h(z)| \leq |z - z_0|^{\alpha-1}.$$

Da h als holomorphe Funktion stetig ist, folgt (beachte $\alpha - 1 > 0$)

$$|h(z_0)| = \lim_{z \rightarrow z_0} |h(z)| \leq \lim_{z \rightarrow z_0} |z - z_0|^{\alpha-1} = 0,$$

also ist $h(z_0) = 0$. Wegen $f'(z_0) = a_1 = h(z_0) = 0$ ist damit der Aufgabenstellung Genüge getan.

- b** Wir bestimmen λ so, dass u eine harmonische Funktion ist und berechnen zunächst

$$\partial_x^2 u(x + iy) = \partial_x(2x) = 2, \quad \partial_y^2 u(x + iy) = \partial_y(2\lambda y) = 2\lambda.$$

Daraus folgt für $x + iy \in \mathbb{C}$

$$(\Delta u)(x + iy) = 0 \Leftrightarrow 2 + 2\lambda = 0 \Leftrightarrow \lambda = -1.$$

Im Fall $\lambda = -1$ ist u also der Realteil einer ganzen Funktion f .

Den zugehörigen Imaginärteil v bestimmen wir wie auf Seite 276 beschrieben. Es muss aufgrund der Cauchy-Riemann-Differentialgleichungen gelten:

$$\partial_y v(x + iy) = \partial_x u(x + iy) = 2x \quad \text{und} \quad \partial_x v(x + iy) = -\partial_y u(x + iy) = 2y.$$

Durch Integration der zweiten Gleichung nach x erhalten wir

$$v(x, y) = 2xy + v(x, 0)$$

und Integration nach y liefert

$$v(x, y) = 2xy + v(0, y).$$

Wertet man die erste Gleichung bei $(0, y)$ aus, so erhält man

$$v(x, y) = 2xy + v(0, 0).$$

Schreibe $c = v(0, 0)$, so ist für $z = x + iy$

$$f(z) = x^2 - y^2 + i(2xy + c) = x^2 + 2ixy + i^2y^2 + ic = (x + iy)^2 + ic = z^2 + ic.$$

Umgekehrt ist für jedes $c \in \mathbb{R}$ eine Funktion dieser Form holomorph und hat u als Realteil.

Lösungsvorschlag zur Aufgabe (Herbst 2016, T1A2)

a) Die Nullstellen des Nenners haben die Form $z_k = \pi + 2k\pi i$ für $k \in \mathbb{Z}$. Keine dieser Nullstellen ist doppelt, da die Nennerableitung durch e^z gegeben ist und $e^{z_k} = e^\pi \neq 0$. Somit lässt sich der Nenner von f schreiben als $(z - z_k)g_k(z)$ für eine holomorphe Abbildung g_k mit $g_k(z_k) \neq 0$.

Betrachten wir zuerst $k \neq 0$: Wegen $\sin(z_k) \neq 0$ lässt sich f als $f(z) = (z - z_k)^{-1} \frac{\sin z}{g_k(z)}$ schreiben, wobei der zweite Faktor holomorph ist und nicht verschwindet. Also ist $\pi + 2k\pi i$ eine Polstelle erster Ordnung ist.

Im Fall $k = 0$ beachte, dass $\sin(\pi) = 0$, aber $\sin'(\pi) = \cos \pi \neq 0$, sodass der Zähler eine Darstellung der Form $\sin(z) = (z - \pi)h(z)$ für eine holomorphe Funktion h mit $h(\pi) \neq 0$ hat. Damit erhalten wir aber analog zu eben für $z \neq \pi$

$$f(z) = \frac{(z - \pi)h(z)}{(z - \pi)g_0(z)} = \frac{h(z)}{g(z)}.$$

Der Quotient $\frac{h}{g}$ ist holomorph auf $B_{2\pi}(\pi)$, sodass die Singularität π hebbare ist.

Zur Berechnung des Integrals: es gilt $\operatorname{Res}(f; \pi) = 0$, da π eine hebbare Singularität ist. Die restlichen Singularitäten liegen nicht im Integrationsbereich, da für $k \neq 0$

$$|\pi + 2k\pi i| \geq |\operatorname{Im}(\pi + 2k\pi i)| = |2k\pi| > 4$$

gilt. Somit ist $\int_{|z|=4} f dz = 0$.

b Die einzige Singularität der Funktion ist 0. Betrachten wir zunächst das Argument der Sinusfunktion. Hier gilt

$$e^{1/z} = e^{z^{-1}} = \sum_{k=0}^{\infty} \frac{(z^{-1})^k}{k!} = \sum_{k=0}^{\infty} \frac{z^{-k}}{k!}.$$

Da in dieser Reihenentwicklung um 0 unendlich viele Glieder mit negativem Exponenten auftreten, handelt es sich bei 0 um eine wesentliche Singularität. Laut dem Satz von Casorati-Weierstraß ist das Bild einer beliebig kleinen punktierten Umgebung von 0 unter $z \mapsto \exp(\frac{1}{z})$ daher dicht in \mathbb{C} und es muss Folgen $(u_n)_{n \in \mathbb{N}}$ und $(v_n)_{n \in \mathbb{N}}$ geben, sodass $\lim_{n \rightarrow \infty} u_n = \lim_{n \rightarrow \infty} v_n = 0$, aber

$$\lim_{n \rightarrow \infty} \exp\left(\frac{1}{u_n}\right) = \frac{\pi}{2} \quad \text{und} \quad \lim_{n \rightarrow \infty} \exp\left(\frac{1}{v_n}\right) = -\pi.$$

Für diese Folgen gilt nun aufgrund der Stetigkeit der Sinusfunktion

$$\lim_{n \rightarrow \infty} f(u_n) = \sin \frac{\pi}{2} = 1 \quad \text{und} \quad \lim_{n \rightarrow \infty} f(v_n) = \sin \pi = 0.$$

Damit ist auch die Singularität 0 der Funktion f wesentlich. Wir berechnen das Residuum, indem wir die Reihendarstellung von f betrachten:

$$f(z) = \sin\left(e^{\frac{1}{z}}\right) = \sin\left(\sum_{l=0}^{\infty} \frac{z^{-k}}{k!}\right) = \sum_{k=0}^{\infty} \frac{(-1)^k}{(2k+1)!} \left(\sum_{l=0}^{\infty} \frac{z^{-l}}{l!}\right)^{2k+1}$$

Wir zeigen zunächst, dass der Koeffizient vor z^{-1} in der Reihe $\left(\sum_{l=0}^{\infty} \frac{z^{-l}}{l!}\right)^n$ für $n \in \mathbb{N}$ gleich n ist. Für $n = 1$ ist dies klar. Setzen wir die Aussage für n als gültig voraus. Dann gilt

$$\begin{aligned} \left(\sum_{l=0}^{\infty} \frac{z^{-l}}{l!}\right)^{n+1} &= \left(\sum_{l=0}^{\infty} \frac{z^{-l}}{l!}\right)^n \cdot \left(\sum_{l=0}^{\infty} \frac{z^{-l}}{l!}\right) = \\ &= (1 + nz^{-1} + a_2 z^{-2} + \dots)(1 + z^{-1} + \frac{1}{2} z^{-2} + \dots) = \\ &= 1 + (n+1)z^{-1} + \dots \end{aligned}$$

und somit ist die Aussage auch für $n+1$ wahr. Wir erhalten daher:

$$\text{Res}(f; 0) = \sum_{k=0}^{\infty} (-1)^k \frac{(2k+1)}{(2k+1)!} = \sum_{k=0}^{\infty} \frac{(-1)^k}{(2k)!} = \cos 1.$$

Damit berechnet sich das gesuchte Integral mit dem Residuensatz zu

$$\int_{|z|=4} f(z) dz = 2\pi i \operatorname{Res}(f; 0) = 2\pi i \cos 1.$$

Lösungsvorschlag zur Aufgabe (Herbst 2016, T1A3)

- a** Sei $D = \mathbb{R} \times]-\frac{\pi}{2}, \frac{\pi}{2}[$ der Definitionsbereich der Gleichung. Die Funktion $f: \mathbb{R}^2 \rightarrow \mathbb{R}, f(x, y) = -\tan(y)e^y$ ist wegen

$$\partial_y f(x, y) = \frac{-e^y}{\cos^2 y} - \tan(y)e^y$$

auf ganz D stetig differenzierbar und somit lokal Lipschitz-stetig. Da D ein Gebiet ist, folgt aus dem Globalen Existenz- und Eindeutigkeitssatz, dass das Anfangswertproblem eine eindeutige maximale Lösung y auf einem Intervall $I =]a, b[$ mit $0 \in I$ besitzt.

Um zu zeigen, dass diese maximale Lösung auf ganz \mathbb{R} definiert ist, zeigen wir, dass die Lösung des Anfangswertproblems beschränkt bleibt: Angenommen, es gibt ein $x_0 \in I$ mit $y(x_0) > 0$. Laut dem Zwischenwertsatz gibt es wegen $y(0) = -1 < 0$ ein $x_1 \in]0, x_0[$ mit $y(x_1) = 0$. Damit sind aber sowohl die Abbildung y als auch die Nullfunktion $t \mapsto 0$ Lösungen der Differentialgleichung zur Anfangsbedingung $y(x_0) = 0$. Da die Nullfunktion auf ganz \mathbb{R} definiert ist, ist sie die maximale Lösung dieses Anfangswertproblems, sodass y eine Einschränkung Nullfunktion sein muss. Insbesondere ist y konstant – jedoch kann y wegen $y(0) \neq 0$ nicht die Nulllösung sein. Widerspruch.

Damit haben wir $y(x) < 0$ für $x \in I$. Wegen $f(x, y) > 0$ für $(x, y) \in \mathbb{R} \times]-\frac{\pi}{2}, 0[$ ist y streng monoton steigend, insbesondere ist also $y(x) \in]-1, 0[$ für alle $x \in [0, b[$. Folglich sind $\lim_{x \nearrow b} \operatorname{dist}((x, y(x)), \partial D) = 0$ und $\lim_{x \nearrow b} |y(x)| = \infty$ unmöglich. Laut der Charakterisierung des Randverhaltens maximaler Lösungen muss deshalb $b = -\infty$ gelten.

- b** Die Lösung $y(x)$ ist durch 0 nach oben beschränkt und monoton wachsend, damit existiert der Limes und erfüllt $\lim_{x \rightarrow \infty} y(x) \leq 0$. Nehmen wir widerspruchshalber an, es gibt eine kleinere obere Schranke $c < 0$. Dann gilt für $x \in \mathbb{R}_+$

$$y'(x) = -e^{y(x)} \tan y(x) > -e^c \tan c > 0.$$

Dies bedeutet jedoch

$$y(x) = y(0) + \int_0^x y'(t) dt \geq -1 + \int_0^x -e^c \tan c dt = -1 - xe^c \tan c \xrightarrow{x \rightarrow \infty} \infty$$

im Widerspruch dazu, dass y nach oben beschränkt ist.

Lösungsvorschlag zur Aufgabe (Herbst 2016, T1A4)

- a** Die Komponentenfunktionen von F entstehen durch punktweise Addition und Multiplikation der beliebig oft differenzierbaren Abbildungen $(x, y) \mapsto x$ bzw. $(x, y) \mapsto y$ sowie durch Verkettung mit Exponential- bzw. Sinus-/ Kosinusfunktion, die ebenfalls beliebig oft differenzierbar sind. Also sind die Komponenten und damit auch die Funktion F selbst beliebig oft differenzierbar.

- b** Es gilt

$$(DF)(x, y) = \begin{pmatrix} e^x \cos(y + x^3) - 3e^x \sin(y + x^3)x^2 & -e^x \sin(y + x^3) \\ e^x \sin(y + x^3) + 3e^x \cos(y + x^3)x^2 & e^x \cos(y + x^3) \end{pmatrix}.$$

- c** Sei $\Delta = \{(x, y) \mid 0 \leq y \leq x \leq 1\} \subseteq \mathbb{R}^2$. Es gilt $\Omega = F(\Delta)$. Außerdem ist $F|_{\Delta}$ injektiv, denn aus $F(x, y) = F(x', y')$ folgt wegen $e^x = |F(x, y)| = |F(x', y')| = e^{x'}$ sofort $x = x'$. Die Bedingung $\cos(y + x^3) = \cos(y' + x'^3)$ liefert weiter

$$y \equiv y' \pmod{2\pi}$$

und aufgrund der Definition von Δ bedeutet dies $y = y'$. Mit dem Transformationssatz erhalten wir damit

$$\text{vol}(\Omega) = \int_{\Omega} 1 d(x, y) = \int_{\Delta} |\det(DF)(x, y)| d(x, y).$$

Als Vorbereitung berechnet man in einer nicht allzu aufwendigen Rechnung

$$|\det(DF)(x, y)| = e^{2x}.$$

Nun gilt $(x, y) \in \Delta$ genau dann, wenn $0 \leq x \leq 1$ und $0 \leq y \leq x$ ist, also

$$\int_{\Delta} |\det DF(x, y)| d(x, y) = \int_0^1 \int_0^x e^{2x} dy dx = \int_0^1 [ye^{2x}]_{y=0}^{y=x} dx = \int_0^1 xe^{2x} dx.$$

Mittels partieller Integration erhalten wir schlussendlich

$$\begin{aligned}\int_0^1 xe^{2x} dx &= \left[\frac{1}{2} xe^{2x} \right]_0^1 - \int_0^1 e^{2x} dx = \\ &= \left[\frac{1}{2} xe^{2x} \right]_0^1 - \left[\frac{1}{2} e^{2x} \right]_0^1 = \frac{1}{2} e^2 - \frac{1}{2} e^2 + \frac{1}{2} = \frac{1}{2}.\end{aligned}$$

Lösungsvorschlag zur Aufgabe (Herbst 2016, T1A5)

Wir lösen zunächst

$$\begin{aligned}-x^3 + 2x^2y - xy^2 = 0 &\Leftrightarrow -x(x^2 - 2xy + y^2) = 0 \\ &\Leftrightarrow -x(x - y)^2 = 0.\end{aligned}$$

Daraus erhalten wir $x = 0$ oder $x = y$. Im ersten Fall liefert die zweite Gleichung $y = 0$ und damit die Ruhelage $(0, 0)$. Im zweiten Fall erhalten wir

$$-2x^3 - x^3 + x^3 + 2x^4 = 0 \Leftrightarrow x^4 - x^3 = 0 \Leftrightarrow x^3(x - 1) = 0$$

und somit erneut $(0, 0)$ oder $(1, 1)$. Tatsächlich zeigt Einsetzen, dass $(0, 0)$ und $(1, 1)$ Ruhelagen des Systems sind.

Um diese auf Stabilität zu untersuchen, versuchen wir zunächst Linearisierung. Bezeichnet f die Funktion der rechten Seite, so erhalten wir

$$(Df)(x, y) = \begin{pmatrix} -3x^2 + 4xy - y^2 & 2x^2 - 2xy \\ -6x^2 + 2xy & -3y^2 + x^2 + 8y^3 \end{pmatrix}.$$

Für die Stelle $(1, 1)$ ergibt sich

$$(Df)(1, 1) = \begin{pmatrix} 0 & 0 \\ -4 & 6 \end{pmatrix}.$$

Für diese berechnet man leicht die Eigenwerte 0 und 6. Da letzterer einen positiven Realteil hat, ist die Ruhelage $(1, 1)$ nach dem Kriterium für linearisierte Stabilität 7.30 instabil.

Da $(Df)(0, 0)$ die Nullmatrix ist, liefert Linearisierung hier keine Aussage. Wir machen folgenden Versuch: Es gilt für $(x, y) \in \mathbb{R}^2$

$$\left\langle \begin{pmatrix} x \\ y \end{pmatrix}, \begin{pmatrix} -x^3 + 2x^2y - xy^2 \\ -2x^3 - y^3 + x^2y + 2y^4 \end{pmatrix} \right\rangle =$$

$$-x^4 + 2x^3y - x^2y^2 - 2x^3y - y^4 + x^2y^2 + 2y^5 = -x^4 - y^4 + 2y^5.$$

Der letzte Term ist leider nicht auf ganz \mathbb{R}^2 negativ. Betrachten wir daher die Einschränkung des Systems auf die Menge $D = \{(x, y) \in \mathbb{R}^2 \mid y < \frac{1}{2}\}$. Für $(x, y) \in D$ mit $y \neq 0$ gilt nun

$$y < \frac{1}{2} \Rightarrow 2y^5 < y^4 \Rightarrow -y^4 + 2y^5 < 0 \Rightarrow -x^4 - y^4 + 2y^5 < 0.$$

Im Fall $y = 0$ gilt zumindest, falls $x \neq 0$, dass $-x^4 < 0$. Somit haben wir

$$\left\langle \begin{pmatrix} x \\ y \end{pmatrix}, \begin{pmatrix} -x^3 + 2x^2y - xy^2 \\ -2x^3 - y^3 + x^2y + 2y^4 \end{pmatrix} \right\rangle < 0$$

für alle $(x, y) \in D \setminus \{(0, 0)\}$ gezeigt. Nun ist (x, y) gerade der Gradient der Funktion $V: D \rightarrow \mathbb{R}, (x, y) \mapsto \frac{1}{2}x^2 + \frac{1}{2}y^2$. Bei V handelt es sich also um eine Lyapunov-Funktion für das auf D eingeschränkte System. Es gilt ferner $V(0, 0) = 0$ und $V(x, y) > 0$ für $(x, y) \neq (0, 0)$. Gemäß der direkten Methode von Lyapunov ist die Ruhelage $(0, 0)$ des auf D eingeschränkten Systems also asymptotisch stabil. Das trifft dann auch auf die entsprechende Ruhelage des auf \mathbb{R}^2 definierten Systems zu.

Lösungen zu Thema Nr. 2

Lösungsvorschlag zur Aufgabe (Herbst 2016, T2A1)

- a** Es ist für $z = x + iy \in \mathbb{C}$

$$f(z) = (x + iy)^2(x - iy) = (x + iy)(x^2 + y^2) = x^3 + xy^2 + i(x^2y + y^3).$$

Da f reell analytisch ist, ist f genau dann in z holomorph, wenn dort die Cauchy-Riemann-Differentialgleichungen gelten:

$$\partial_x \operatorname{Re} f(z) = \partial_y \operatorname{Im} f(z) \Leftrightarrow 3x^2 + y^2 = x^2 + 3y^2 \Leftrightarrow x^2 = y^2$$

sowie

$$\partial_y \operatorname{Re} f(z) = -\partial_x \operatorname{Im} f(z) \Leftrightarrow 2xy = -2xy \Leftrightarrow xy = 0.$$

Die zweite Gleichung liefert $x = 0$ oder $y = 0$, zusammen mit der ersten Gleichung folgt in jedem Fall $z = 0$. Da für $x = y = 0$ andererseits beide Gleichungen erfüllt sind, ist die Funktion genau im Ursprung holomorph.

- b** Aufgrund von

$$(z - 1)^3(9z^2 + 12z^2 + 4) = (z - 1)^3(3z + 2)^2$$

hat der Nenner von h die Nullstellen 1 und $-\frac{2}{3}$. Wir erhalten zunächst

$$h(z) = (z-1)^{-3}g_1(z) \quad \text{mit } g_1(z) = \frac{z^8+z^4+2}{(3z-2)^2}.$$

Die Funktion g_1 ist holomorph auf einer Umgebung von 0, ferner gilt $g_1(1) \neq 0$. Somit ist 1 eine Polstelle dritter Ordnung. Analog gilt

$$h(z) = \frac{1}{9} \left(z + \frac{2}{3}\right)^{-2} g_2(z) \quad \text{mit } g_2(z) = \frac{z^8+z^4+2}{(z-1)^3}.$$

Auch hier ist g_2 holomorph auf einer Umgebung von $-\frac{2}{3}$ und es gilt $g_2(-\frac{2}{3}) \neq 0$. Damit ist $-\frac{2}{3}$ eine Polstelle zweiter Ordnung.

Zur Untersuchung des Punktes ∞ betrachten wir die Funktion $f(\frac{1}{z})$. Es ist für $z \neq 0$

$$f\left(\frac{1}{z}\right) = \frac{z^{-8}+z^{-4}+2}{(\frac{1}{z}-1)^3(\frac{3}{z}-2)^2} = \frac{1+z^4+2z^8}{z^3(1-z)^3(3-2z)^2}.$$

Wiederum gilt hier

$$f\left(\frac{1}{z}\right) = z^{-3} \frac{1+z^4+2z^8}{(1-z)^3(3-2z)^2}$$

und der hintere Faktor ist auf einer Umgebung der 0 holomorph und verschwindet in 0 nicht. Somit ist 0 eine Polstelle dritter Ordnung von $f(\frac{1}{z})$ und dasselbe gilt für die Singularität ∞ von f .

- c** Wir bemerken, dass der Integrand nicht holomorph ist und Integralsätze hier keine große Hilfe sind. Wir berechnen das Integral zu Fuß: γ ist die Verknüpfung der Wege

$$\gamma_1(t) = t, \quad \gamma_2(t) = 1+it, \quad \gamma_3(t) = (1-t)(1+i),$$

wobei jeweils $t \in [0, 1]$ ist.

Mit $\gamma'_1(t) = 1$ gilt zunächst

$$\int_{\gamma_1} |z|^2 dz = \int_0^1 t^2 dt = \left[\frac{1}{3}t^3 \right]_0^1 = \frac{1}{3}.$$

Ferner ist für $\gamma'_2(t) = i$, also

$$\int_{\gamma_2} |z|^2 dz = \int_0^1 (1+t^2)i dt = i \left[t + \frac{1}{3}t^3 \right]_0^1 = \frac{4}{3}i.$$

Zu guter Letzt ist noch für $\gamma'_3(t) = -1 - i$

$$\begin{aligned}\int_{\gamma_3} |z|^2 dz &= (-1 - i) \int_0^1 (1-t)^2 + (1-t)^2 dt = \\ &= (-2 - 2i) \int_0^1 (1-t)^2 dt = (-2 - 2i) \left[-\frac{1}{3}(1-t)^3 \right]_0^1 = -\frac{2}{3} - \frac{2}{3}i\end{aligned}$$

Insgesamt erhalten wir

$$\int_{\gamma} |z|^2 dz = \frac{1}{3} + \frac{4}{3}i - \frac{2}{3} - \frac{2}{3}i = -\frac{1}{3} + \frac{2}{3}i.$$

Lösungsvorschlag zur Aufgabe (Herbst 2016, T2A2)

a *Falsch.* Betrachte die Abbildung

$$f: \mathbb{R}^2 \rightarrow \mathbb{R}, (x, y) \mapsto \begin{cases} \frac{xy}{x^2+y^2} & \text{falls } (x, y) \neq (0, 0) \\ 0 & \text{falls } (x, y) = (0, 0). \end{cases}$$

Diese ist überall partiell differenzierbar. In Punkten $(x, y) \neq (0, 0)$ folgt dies aus der totalen Differenzierbarkeit aufgrund des Quotientenkriteriums. Im Punkt $(0, 0)$ betrachten wir zunächst die Ableitung in x -Richtung. Hier gilt

$$\partial_x f(0, 0) = \lim_{t \rightarrow 0} \frac{f(t, 0) - f(0, 0)}{t} = \lim_{t \rightarrow 0} \frac{0}{t} = 0.$$

Für die y -Richtung erhalten wir

$$\partial_y f(0, 0) = \lim_{t \rightarrow 0} \frac{f(0, t) - f(0, 0)}{t} = \lim_{t \rightarrow 0} \frac{0}{t} = 0.$$

Insbesondere existieren beide partiellen Ableitungen auch in $(0, 0)$. Zum Nachweis der Unstetigkeit definiere die Folge $(x_n, y_n)_{n \in \mathbb{N}}$ durch $(x_n, y_n) = (\frac{1}{n}, \frac{1}{n})$. Es gilt

$$\lim_{n \rightarrow \infty} f(x_n, y_n) = \lim_{n \rightarrow \infty} \frac{\frac{1}{n^2}}{\frac{1}{n^2} + \frac{1}{n^2}} = \lim_{n \rightarrow \infty} \frac{1}{2} = \frac{1}{2} \neq 0 = f\left(\lim_{n \rightarrow \infty} (x_n, y_n)\right).$$

b *Falsch.* Die Aussage wäre richtig, falls f nullstellenfrei ist (vgl. Minimumsprinzip). Da dies nicht vorausgesetzt war, definieren wir auf dem Gebiet

$\Omega = B_1(0)$ die Funktion $f: \Omega \rightarrow \mathbb{C}$, $z \mapsto z^2$. Diese Funktion ist holomorph. Zugleich gilt natürlich für $z_0 = 0$

$$|f(z_0)| = 0 \leq |f(z)| \quad \forall z \in \Omega.$$

Andererseits ist aber f wegen $f(\frac{1}{2}) = \frac{1}{4} \neq 0 = f(0)$ nicht konstant.

- c** *Wahr.* Die Bereiche $x \neq 0$ sind uninteressant, da dort die Differenzierbarkeit aus der Produkt-/ Ketten- bzw. Quotientenregel folgt. Betrachten wir den Fall $x = 0$. Wir berechnen

$$\lim_{\substack{h \rightarrow 0 \\ h > 0}} \frac{f(h) - f(0)}{h} = \lim_{\substack{h \rightarrow 0 \\ h > 0}} \frac{h^2 \sin(1/h)}{h} = \lim_{\substack{h \rightarrow 0 \\ h > 0}} h \sin(1/h) = 0,$$

wobei die letzte Gleichheit aus $\sin(1/h) \in [-1, 1]$ für alle $h \in \mathbb{R}$ folgt. Fazit: Die Funktion f ist an der Stelle 0 differenzierbar mit $f'(0) = 0$.

Lösungsvorschlag zur Aufgabe (Herbst 2016, T2A3)

- a** Wegen $\cos \theta = \frac{1}{2}(e^{i\theta} + e^{-i\theta})$ gilt

$$\int_0^{2\pi} (\cos \theta)^{2n} d\theta = \int_0^{2\pi} \left(\frac{1}{2} e^{i\theta} + \frac{1}{2} e^{-i\theta} \right)^{2n} d\theta.$$

Bezeichnet nun γ den Weg $\gamma(t) = e^{it}$ für $t \in [0, 2\pi]$, so wird das Integral zu

$$\int_0^{2\pi} \left(\frac{1}{2} e^{it} + \frac{1}{2} e^{-it} \right)^{2n} \frac{\gamma'(t)}{ie^{it}} dt = \frac{1}{i2^{2n}} \int_\gamma \frac{1}{z} (z + z^{-1})^{2n} dz.$$

Der Integrand, den wir im Folgenden als $f(z)$ bezeichnen, hat nur eine Singularität bei 0. Wir berechnen das zugehörige Residuum. Der binomische Lehrsatz liefert zunächst

$$f(z) = \frac{1}{z} (z + z^{-1})^{2n} = \frac{1}{z} \sum_{k=0}^{2n} \binom{2n}{k} z^k z^{-2n+k} = \sum_{k=0}^{2n} \binom{2n}{k} z^{2k-2n-1}.$$

Der Koeffizient von z^{-1} ergibt sich für $k = n$ und es ist dementsprechend

$$\text{Res}(f; 0) = \binom{2n}{n} = \frac{(2n)!}{(2n-n)!n!} = \frac{(2n)!}{(n!)^2}.$$

Damit ist der Wert des Integrals laut Residuensatz

$$\frac{1}{i2^{2n}} \int_{\gamma} z \left(z + z^{-1} \right)^{2n} dt = \frac{1}{i2^{2n}} \cdot 2\pi i \cdot \frac{(2n)!}{(n!)^2} = \frac{\pi(2n)!}{2^{2n-1}(n!)^2}.$$

b Wir betrachten zunächst die Integrale getrennt:

$$\begin{aligned} \int_{\gamma_3} e^{iz^2} dz &= \int_{-R}^0 e^{i(-t)^2 e^{i\pi/2}} (-e^{i\pi/4}) dt = -e^{i\pi/4} \int_{-R}^0 e^{-t^2} dt = \\ &= -e^{i\pi/4} \int_R^0 (-1) e^{-t^2} dt = -e^{i\pi/4} \int_0^R e^{-t^2} dt. \end{aligned}$$

Dabei erhält man die vorletzte Gleichung durch die Substitution $t \mapsto -t$. Ferner ist für $R > 0$ mit der Ungleichung aus dem Hinweis

$$\begin{aligned} \left| \int_0^{\pi/4} e^{iRe^{i\theta}} iRe^{i\theta} d\theta \right| &\leq \int_0^{\pi/4} \left| e^{iRe^{i\theta}} \right| \cdot R d\theta = R \int_0^{\pi/4} e^{\operatorname{Re}(iRe^{i\theta})} d\theta = \\ &= R \int_0^{\pi/4} e^{-R \sin \theta} d\theta \leq R \int_0^{\pi/4} e^{-\frac{2R\theta}{\pi}} d\theta \leq \\ &\leq R \int_0^{\pi/4} e^{-\frac{2R}{\pi}} d\theta = \frac{R\pi}{4} e^{-\frac{2R}{\pi}} \xrightarrow{R \rightarrow \infty} 0. \end{aligned}$$

Laut dem Cauchy-Integralsatz verschwindet das Integral $\int_{\gamma} e^{iz^2} dz$, da der Integrand holomorph auf \mathbb{C} ist. Damit erhalten wir

$$0 = \int_{\gamma_1} e^{iz^2} dz + \int_{\gamma_2} e^{iz^2} dz + \int_{\gamma_3} e^{iz^2} dz.$$

Und da das Integral über γ_2 beim Grenzübergang $R \rightarrow \infty$ verschwindet, ist

$$\lim_{R \rightarrow \infty} \int_{\gamma_1} e^{iz^2} dz = - \lim_{R \rightarrow \infty} \int_{\gamma_3} e^{iz^2} dz.$$

Weiter erhalten wir wegen $e^{ix^2} = \cos(x^2) + i \sin(x^2)$ für $x \in \mathbb{R}$ unter Verwendung des Integrals aus der Angabe

$$\begin{aligned} \int_0^{\infty} \cos(x^2) dx + i \int_0^{\infty} \sin(x^2) dx &= e^{i\pi/4} \int_0^{\infty} e^{-t^2} dt = \left(\frac{\sqrt{2}}{2} + i \frac{\sqrt{2}}{2} \right) \frac{\sqrt{\pi}}{2} \\ \Leftrightarrow \quad \int_0^{\infty} \cos(x^2) dx + i \int_0^{\infty} \sin(x^2) dx &= \frac{\sqrt{\pi}}{2\sqrt{2}} + i \frac{\sqrt{\pi}}{2\sqrt{2}}. \end{aligned}$$

Vergleich von Real- und Imaginärteil liefert dann

$$\int_0^\infty \cos(x^2)dx = \frac{\sqrt{\pi}}{\sqrt{8}} = \int_0^\infty \sin(x^2)dx.$$

Lösungsvorschlag zur Aufgabe (Herbst 2016, T2A4)

- a** Man berechnet für $x, y, z \in \mathbb{R}$

$$\begin{aligned}\langle \nabla(E_1)(x,y,z), v(x,y,z) \rangle &= (2x \quad -2y \quad 0) \begin{pmatrix} yz \\ zx \\ xy \end{pmatrix} = 0, \\ \langle (\nabla E_2)(x,y,z), v(x,y,z) \rangle &= (0 \quad 2y \quad -2z) \begin{pmatrix} yz \\ zx \\ xy \end{pmatrix} = 0.\end{aligned}$$

- b** Dem Hinweis folgend bemerkt man zuerst $E_1(u(0)) = E_1(1, -1, 1) = 0 = E_2(1, -1, 1) = E_2(u(0))$. Dementsprechend folgt

$$\alpha^2(t) - \beta^2(t) = 0 = \beta^2(t) - \gamma^2(t).$$

Damit muss $\alpha(t) = \pm\beta(t)$ und $\beta(t) = \pm\gamma(t)$ sein. Im Punkt $t = 0$ gilt $\alpha(0) = -\beta(0) = \gamma(0)$ aufgrund der Anfangsbedingung. Wir zeigen nun, dass es eine Umgebung der 0 gibt, in der $\alpha(t) = -\beta(t)$ gilt. Der Nachweis von $-\beta(t) = \gamma(t)$ kann analog geführt werden. Die Gleichheit $\alpha(t) = -\beta(t) = \gamma(t)$ gilt dann im Schnitt dieser beiden Umgebungen.

Da α und β stetig sind, gibt es nach dem ε - δ -Kriterium zu jedem $\varepsilon > 0$ jeweils $\delta_1, \delta_2 > 0$, sodass für alle $|t| < \delta_1$ bzw. $|t| < \delta_2$ die Ungleichungen

$$|\alpha(0) - \alpha(t)| < \varepsilon \quad \text{und} \quad |\beta(0) - \beta(t)| < \varepsilon$$

erfüllt sind. Setze $\varepsilon = \frac{1}{2}$ und $\delta = \min\{\delta_1, \delta_2\}$, dann sind für $|t| < \delta$ beide Ungleichungen erfüllt. Nehmen wir an, es gibt ein solches $t \in]-\delta, \delta[$ mit $\alpha(t) = \beta(t)$, dann gilt

$$|\beta(0) - \beta(t)| = |-1 - \alpha(t)| = |1 + \alpha(t)| < \frac{1}{2}.$$

Dies widerspricht jedoch $|\alpha(0) - \alpha(t)| = |1 - \alpha(t)| < \frac{1}{2}$. Für alle $t \in]-\delta, \delta[$ muss daher $\alpha(t) = -\beta(t)$ erfüllt sein.

c Schränken wir die Differentialgleichung auf die Umgebung aus Teil **b** ein, so gilt dort

$$\alpha'(t) = \beta(t) \cdot \gamma(t) = -\alpha^2(t),$$

d. h. α ist Lösung der Differentialgleichung $x' = -x^2$ zum Anfangswert $x(0) = 1$. Diese Differentialgleichung lösen wir mittels Trennen der Variablen:

$$\int_1^{\alpha(t)} \frac{-1}{x^2} dx = \int_0^t 1 d\tau \Leftrightarrow \frac{1}{\alpha(t)} - 1 = t \Leftrightarrow \alpha(t) = \frac{1}{t+1}.$$

Unser Lösungskandidat ist daher

$$u(t) = \frac{1}{t+1} \cdot \begin{pmatrix} 1 \\ -1 \\ 1 \end{pmatrix}$$

und man überprüft, dass u tatsächlich die Differentialgleichung löst. Das maximale Definitionsintervall ist $J =]-1, \infty]$. Wegen

$$\lim_{t \searrow -1} \|u(t)\| = \infty$$

kann u auch nicht stetig über dieses Intervall hinaus fortgesetzt werden.

Lösungsvorschlag zur Aufgabe (Herbst 2016, T2A5)

a Der Definitionsbereich der Gleichung ist ein Gebiet, die rechte Seite ist stetig. Wir zeigen, dass f sogar Lipschitz-stetig bezüglich x ist. Seien dazu $(t, x), (t, y) \in \mathbb{R}^2$, wobei wir o. B. d. A. $x < y$ annehmen. Es gilt

$$|f(t, x) - f(t, y)| = \left| |\cos x| - |\cos y| \right| \stackrel{(\nabla)}{\leq} |\cos x - \cos y|.$$

Laut dem Mittelwertsatz der Differentialrechnung existiert nun ein $x_0 \in]x, y[$, sodass

$$\frac{\cos x - \cos y}{x - y} = \cos'(x_0) = -\sin(x_0) \Leftrightarrow \cos x - \cos y = -\sin(x_0)(x - y)$$

und damit

$$|f(t, x) - f(t, y)| \leq |\cos x - \cos y| = |\sin(x_0)| \cdot |x - y| \leq |x - y|$$

gilt. Damit ist f (sogar global) Lipschitz-stetig bezüglich x mit Lipschitz-Konstante 1. Laut dem Globalen Existenz- und Eindeutigkeitssatz 7.12 existiert damit ein Intervall $] -\delta, \delta[$, sodass das angegebene Anfangswertproblem eine eindeutige Lösung besitzt.

- b** Es gilt für $s \in] -b, -a[$ unter Verwendung der Achsensymmetrie des Kosinus:

$$\begin{aligned}\tilde{\alpha}'(s) &= \alpha'(-s) = f(-s, \alpha(-s)) = |\cos \alpha(-s)| + (-s)^2 = \\ &= |\cos(-\alpha(-s))| + s^2 = |\cos(\tilde{\alpha}(s))| + s^2 = f(s, \tilde{\alpha}(s)).\end{aligned}$$

Zudem ist $\tilde{\alpha}(0) = -\alpha(0) = 0$, also ist auch die Anfangsbedingung erfüllt.

Anmerkung Laut Teil **a** folgt mit der Eindeutigkeit der (maximalen) Lösung, dass $\alpha(s) = -\alpha(-s)$ für $s \in]a, b[$ gilt – wir haben soeben also gezeigt, dass die Lösung des Anfangswertproblems punktsymmetrisch zum Ursprung ist.

- c** (i) In Teil **b** hatten wir gesehen, dass das Anfangswertproblem eindeutig lösbar ist. Nun folgt daraus aber, wie eben bemerkt, $\alpha = \tilde{\alpha}$. Damit ist insbesondere $] -t^+, -t^- [=] t^-, t^+ [$ und daraus folgt die Behauptung.
(ii) Wir folgen dem Vorgehen von Seite 419 und erhalten für $s \in]t^-, t^+[$

$$\begin{aligned}|\alpha(s) - \alpha(0)| &= \left| \int_0^s f(t, \alpha(t)) dt \right| = \left| \int_0^s |\cos \alpha(t)| + t^2 dt \right| \leq \\ &\leq \int_0^s 1 + t^2 dt = \left[t + \frac{1}{3} t^3 \right]_0^s = s + \frac{1}{3} s^3.\end{aligned}$$

Umformuliert ergibt dies mit $\alpha(0) = 0$

$$-s - \frac{1}{3} s^3 \leq \alpha(s) \leq s + \frac{1}{3} s^3.$$

Nun ist der Rand des Definitionsbereichs der Gleichung leer, und wegen der Abschätzung ist $\lim_{s \rightarrow t^+} \alpha(s)$ endlich, falls t^+ endlich wäre. Damit bleibt gemäß der Charakterisierung maximaler Lösungen nur der Fall $t^+ = \infty$, und damit laut Teil (i) auch $t^- = -\infty$, übrig.

Lösungen zu Thema Nr. 3

Lösungsvorschlag zur Aufgabe (Herbst 2016, T3A1)

Sei f nicht-konstant, dann ist $U = f(\mathbb{C})$ nach dem Satz über die Gebietstreue 6.22 ein Gebiet. Laut Voraussetzung stimmt also $g|_U$ mit der Nullfunktion überein. Nach dem Identitätssatz muss daher g bereits selbst die Nullfunktion sein.

Lösungsvorschlag zur Aufgabe (Herbst 2016, T3A2)

- a** Sei $\alpha > 0$ und $n \in \mathbb{N}$. Auf der offenen Menge $\mathbb{R} \setminus \{0\}$ ist f_n definiert durch $x \mapsto \frac{\sin^2(n^\alpha x)}{nx}$ und somit als punktweise Verknüpfung stetiger Abbildungen stetig. Betrachten wir noch $x = 0$. Hier gilt unter Verwendung der Regel von l'Hospital

$$\lim_{x \rightarrow 0} \frac{\sin^2(n^\alpha x)}{nx} = \lim_{x \rightarrow 0} \frac{2 \sin(n^\alpha x) \cos(n^\alpha x) n^\alpha}{n} = \frac{0}{n} = 0.$$

Zusammen mit $f_n(0) = 0$ ergibt sich $\lim_{x \rightarrow 0} f_n(x) = f_n(0)$.

- b** Im Fall $x = 0$ ist wegen $f_n(0) = 0$ die Behauptung klar. Sei also $x \neq 0$. Dann gilt

$$\lim_{n \rightarrow \infty} |f_n(x)| = \lim_{n \rightarrow \infty} \left| \frac{\sin^2(n^\alpha x)}{nx} \right| \leq \lim_{n \rightarrow \infty} \left| \frac{1}{nx} \right| = 0$$

und damit auch $\lim_{n \rightarrow \infty} f_n(x) = 0$. Damit konvergiert die Funktionenfolge punktweise gegen die Nullfunktion.

- c** Sei $\varepsilon > 0$ beliebig. Wir müssen ein $N \in \mathbb{N}$ finden, sodass für alle $x \in \mathbb{R}$ und für alle $n \geq N$ die Ungleichung $|f_n(x)| < \varepsilon$ erfüllt ist. Wiederum ist dies im Fall $x = 0$ wegen $f_n(0) = 0$ klar. Für $x \neq 0$ treffen wir die Abschätzung

$$|f_n(x)| = \left| \frac{\sin(n^\alpha x) \sin(n^\alpha x)}{nx} \right| \stackrel{(*)}{\leq} \left| \frac{1 \cdot n^\alpha x}{nx} \right| = n^{\alpha-1} = \frac{1}{n^{1-\alpha}} < \frac{1}{n^{\frac{1}{2}}}.$$

Dabei haben wir an der Stelle $(*)$ den Hinweis aus der Aufgabenstellung verwendet. Setzen wir nun $N = \frac{1}{\varepsilon^2}$, so folgt aus $n \geq N$ für alle $x \neq 0$

$$|f_n(x)| < \frac{1}{N^{\frac{1}{2}}} = \varepsilon.$$

d Wir wählen $\varepsilon = \frac{1}{2}$. Würde f_n gleichmäßig gegen die Nullfunktion konvergieren, so gibt es ein $N \in \mathbb{N}$, sodass $|f_n(x)| < 1$ für $n \geq N$ und $x \in \mathbb{R}$. Für ein genügend großes $n \geq N$ gilt $x_0 = \frac{\pi}{2N^\alpha} \in]0, 1[$. Es gilt

$$f_n(x_0) = \frac{\sin^2(N^\alpha x_0)}{Nx_0} = \frac{\sin^2\left(\frac{N^\alpha \pi}{2N^\alpha}\right)}{\frac{\pi N}{2N^\alpha}} = \frac{2N^\alpha}{\pi N}.$$

Daraus folgt jedoch wegen $\alpha - 1 \geq 0$ für alle $n \geq N$ die Abschätzung

$$f_n(x_0) = \frac{2}{\pi} N^{\alpha-1} \geq \frac{2}{\pi} N^0 > \frac{2}{4} \cdot 1 = \frac{1}{2}$$

im Widerspruch zur Wahl von N .

Lösungsvorschlag zur Aufgabe (Herbst 2016, T3A3)

Die wesentliche Idee liegt hier in der Nutzung der komplexen Exponentialfunktion. Diese bildet nämlich (wie wir später zeigen werden) den Streifen $U = \{z \in \mathbb{C} \mid -\frac{\pi}{4} < \operatorname{Im} z < \frac{\pi}{4}\}$ auf die gewünschte Menge ab. Deshalb definieren wir zunächst $\psi_1: S \mapsto U, z \mapsto \frac{1}{12}z - \frac{i\pi}{4}$. Offensichtlich ist ψ_1 biholomorph. Tatsächlich bildet ψ_1 die Menge S auf U ab: Ist nämlich $z \in S$, so gilt

$$\begin{aligned} 0 < \operatorname{Im} z < 6\pi &\Leftrightarrow -3\pi < \operatorname{Im}(z - 3i\pi) < 3\pi \\ -\frac{\pi}{4} < \operatorname{Im}\left(\frac{1}{12}z - \frac{i\pi}{4}\right) &< \frac{\pi}{4}. \end{aligned}$$

Wir zeigen nun, dass $\psi_2: U \rightarrow T, z \mapsto e^z$ eine biholomorphe Abbildung ist. Sei $z \in U$, dann gilt

$$\psi_2(z) = e^{\operatorname{Re} z + i \operatorname{Im} z} = e^{\operatorname{Re} z} e^{i \operatorname{Im} z} \in T$$

und somit $\psi_2(U) \subseteq T$. Es ist bekannt, dass die Exponentialfunktion holomorph ist. Zum Nachweis der Injektivität seien $z_1, z_2 \in U$ mit $e^{z_1} = e^{z_2}$. Es folgt $z_1 = z_2 + 2k\pi i$ für ein $k \in \mathbb{Z}$. Wegen $-\frac{\pi}{4} < \operatorname{Im} z_1, \operatorname{Im} z_2 < \frac{\pi}{4}$ muss aber bereits $k = 0$ und somit $z_1 = z_2$ gelten. Zum Nachweis der Surjektivität sei $z \in T$, also $z = re^{i\varphi}$ mit $r > 0$ und $-\frac{\pi}{4} < \varphi < \frac{\pi}{4}$. Es gilt dann $\ln r + i\varphi \in U$ und

$$e^{\ln r + i\varphi} = z.$$

Insgesamt ist damit ψ_2 eine biholomorphe Abbildung wie behauptet und wir erhalten mit $\varphi = \varphi_2 \circ \varphi_1$ die biholomorphe Abbildung

$$\varphi: S \rightarrow T, \quad z \mapsto e^{\frac{1}{12}z - \frac{i\pi}{4}}.$$

Zudem gilt

$$\lim_{\operatorname{Re} z \rightarrow \infty} |\varphi(z)| = \lim_{\operatorname{Re} z \rightarrow \infty} e^{\operatorname{Re}(\frac{1}{12}z - \frac{i\pi}{4})} = \lim_{\operatorname{Re} z \rightarrow \infty} e^{\frac{1}{12}\operatorname{Re} z} = \infty$$

und somit ist der geforderte Grenzwert auch erfüllt.

Lösungsvorschlag zur Aufgabe (Herbst 2016, T3A4)

„ \Rightarrow “: Nehmen wir an, dass die Gleichung autonom ist. Dann ist $f(t, x) = f(t + \gamma, x)$ für alle $(t, x) \in \mathbb{R} \times \mathbb{R}^n$ und $\gamma \in \mathbb{R}$. Sei ferner φ eine Lösung und φ_γ wie in der Angabe. Dann gilt für $t \in]a - \gamma, b - \gamma[$, dass $t + \gamma \in]a, b[$ ist. Wir erhalten, da φ laut Annahme eine Lösung der Gleichung ist, mit der Kettenregel:

$$\dot{\varphi}_\gamma(t) = \dot{\varphi}(t + \gamma) = f(t + \gamma, \varphi(t + \gamma)) = f(t, \varphi_\gamma(t))$$

Also ist auch φ_γ eine Lösung der Gleichung.

„ \Leftarrow “: Seien alle Bezeichnungen wie zuvor. Wir müssen zeigen, dass für alle $\sigma, \tau \in \mathbb{R}, y \in \mathbb{R}^n$ die Gleichung $f(\tau, y) = f(\sigma, y)$ gilt. Betrachte zunächst die beiden Anfangswertprobleme

$$\dot{x} = f(t, x), \quad x(\tau) = y, \quad \text{bzw.} \quad \dot{x} = f(t, x), \quad x(\sigma) = y.$$

Da die Gleichung den Voraussetzungen des Globalen Existenz- und Eindeutigkeitssatzes genügt, besitzen diese eindeutige maximale Lösungen φ bzw. ψ . Laut Voraussetzung ist nun für $\gamma = \tau - \sigma$ auch φ_γ eine Lösung von $\dot{x} = f(t, x)$, und zwar zum Anfangswert $\varphi_\gamma(\sigma) = \varphi(\tau) = y$. Laut dem Globalen Existenz- und Eindeutigkeitssatz ist φ_γ somit eine Einschränkung von ψ . In einer Umgebung von σ gilt also

$$f(\sigma, y) = f(\sigma, \psi(\sigma)) = \dot{\psi}(\sigma) = \dot{\varphi}_\gamma(\sigma) = \dot{\varphi}(\tau) = f(\tau, \varphi(\tau)) = f(\tau, y).$$

Lösungsvorschlag zur Aufgabe (Herbst 2016, T3A5)

a (i) Die Nulllösung heißt asymptotisch stabil, wenn sie attraktiv und stabil ist. Dabei bedeutet stabil, dass es für jedes $\varepsilon > 0$ und zu jedem $\tau \in \mathbb{R}$ ein $\delta > 0$ gibt, sodass für jeden Anfangswert $\xi \in \mathbb{R}$ mit $\|\xi\| < \delta$ die maximale Lösung $\lambda_{(\tau,\xi)}(t)$ für alle $t \geq \tau$ existiert und die Abschätzung $\|\lambda_{(\tau,\xi)}(t)\| < \varepsilon$ für alle $t \geq \tau$ erfüllt. Ferner bedeutet attraktiv, dass diese maximale Lösung existiert und die Grenzwerteigenschaft $\lim_{t \rightarrow \infty} \|\lambda_{(\tau,\xi)}(t)\| = 0$ erfüllt.

(ii) Die stationäre Nulllösung ist asymptotisch stabil, wenn alle Eigenwerte der totalen Ableitung $(Df)(0)$ negativen Realteil haben.

b Wir bezeichnen die rechte Seite der Gleichung als $f(x_1, x_2)$ und berechnen zunächst

$$(Df)(x_1, x_2) = \begin{pmatrix} 2x_1x_2 & x_1^2 + \cos x_2 \\ -2e^{x_1} + x_2^2 & -3 + 2x_1x_2 \end{pmatrix}.$$

Entsprechend ist

$$(Df)(0) = \begin{pmatrix} 0 & 1 \\ -2 & -3 \end{pmatrix}$$

mit charakteristischem Polynom $X(X + 3) + 2 = X^2 + 3X + 2$. Dessen Nullstellen berechnen sich zu

$$\lambda_{1,2} = \frac{-3 \pm 1}{2}.$$

Die beiden Eigenwerte -1 und -2 sind beide negativ, also ist die stationäre Lösung 0 asymptotisch stabil.

Prüfungstermin: Frühjahr 2017

Thema Nr. 1 (Aufgabengruppe)

Aufgabe 1 → S. 652

Es sei f eine ganze Funktion mit der Eigenschaft, dass für alle $z \in \mathbb{C}$ mit $|z| \geq 3$ gilt, $|f'(z)| \leq 1 + e^{-|z|}$.

Zeigen Sie, dass es $a, b \in \mathbb{C}$ gibt, sodass $f(z) = az + b$ für alle $z \in \mathbb{C}$. (6 Punkte)

Aufgabe 2 → S. 652

- a Es sei

$$X = \{z \in \mathbb{C} \mid \operatorname{Im} z \geq 0\}$$

der Abschluss der oberen Halbebene. Zeigen Sie, dass durch

$$f(z) = \frac{1}{z^2 + iz - 2}$$

eine Funktion $f: X \rightarrow \mathbb{C}$ ohne Polstellen definiert ist. (1 Punkt)

- b Zeigen Sie, dass $|f|$ auf X ein globales Maximum hat. (2 Punkte)

- c Bestimmen Sie das globale Maximum von $|f|$ auf X und geben Sie alle Punkte an, an denen das globale Maximum angenommen wird. Begründen Sie, warum Ihre Antwort in der Tat das globale Maximum von $|f|$ auf X ist. (3 Punkte)

Aufgabe 3 → S. 653

- a Gibt es eine holomorphe Funktion $f: \mathbb{C} \rightarrow \mathbb{C}$ mit $f(1) = \pi$ und $f'(z) = |z|f(z)$ für alle $z \in \mathbb{C}$? (3 Punkte)

- b Zeigen Sie, dass es höchstens eine ganze Funktion f mit $f(0) = 2 + 3i$ gibt, sodass

$$f'(z) = \sin(z)f(z) + e^{z^2} \text{ für alle } z \in \mathbb{C}.$$

(3 Punkte)

Aufgabe 4 → S. 654

- a** Bestimmen Sie die Ableitung der Funktion

$$f: \mathbb{R} \rightarrow \mathbb{R}, x \mapsto f(x) = \int_0^{\sin x} e^{t^2} dt.$$

(2 Punkte)

- b** Bestimmen Sie die Ableitung der Funktion

$$g: \mathbb{R} \rightarrow \mathbb{R}, z \mapsto \int_0^{\sin z} \sqrt{t^4 + 3z^2} dt$$

am Punkt $z = \pi$.

(4 Punkte)

In beiden Aufgabenteilen muss klar ersichtlich sein, wie Sie zu Ihrem Ergebnis kommen.

Aufgabe 5 → S. 655

- a** Wir betrachten die Differentialgleichung

$$y' = \frac{6t}{1+3t^2} y + 5$$

Bestimmen Sie die maximale Lösung φ der Differentialgleichung zum Anfangswert $\varphi(0) = 2$. Vereinfachen Sie Ihre Antwort so weit wie möglich. (3 Punkte)

- b** Wir betrachten die Differentialgleichung

$$y' = \frac{1}{5}y^3 + t \arctan(t) - \frac{\pi t}{2}.$$

Zeigen Sie, dass für jede Lösung der Differentialgleichung mit $\lim_{t \rightarrow \infty} \varphi'(t) = 0$ auch der Grenzwert $\lim_{t \rightarrow \infty} \varphi(t)$ existiert, und bestimmen Sie diesen. Vereinfachen Sie Ihre Antwort so weit wie möglich. (3 Punkte)

Thema Nr. 2
(Aufgabengruppe)

Aufgabe 1 → S. 657

Für $n \in \mathbb{N}$ seien

$$f_n, g_n: [0, \infty[\rightarrow \mathbb{R}, \quad f_n(x) = x^n e^{-nx}, \quad g_n(x) = x^n e^{-x^n}.$$

- a** Sei $n \in \mathbb{N}$ beliebig, aber fest. Untersuchen Sie, ob die Funktionen f_n und g_n auf $[0, \infty[$ Maximum und Minimum annehmen. (2 Punkte)
- b** Zeigen Sie, dass $(f_n)_{n \in \mathbb{N}}$ und $(g_n)_{n \in \mathbb{N}}$ auf $[0, \infty[$ punktweise konvergieren. Bestimmen Sie die jeweilige Grenzfunktion f bzw. g . (2 Punkte)
- c** Welche der Funktionenfolgen $(f_n)_{n \in \mathbb{N}}$ und $(g_n)_{n \in \mathbb{N}}$ konvergieren auf $[0, \infty[$ gleichmäßig? (2 Punkte)

Aufgabe 2 → S. 658

Gegeben sei ein stetig differenzierbares Vektorfeld $f: \mathbb{R}^3 \rightarrow \mathbb{R}^3$ derart, dass die Differentialgleichung

$$x' = f(x) \quad (*)$$

die Erhaltungsgrößen

$$V, W: \mathbb{R}^3 \rightarrow \mathbb{R}, \quad V(x_1, x_2, x_3) = x_1^2 + x_2^2 + x_3^2, \quad W(x_1, x_2, x_3) = x_1^2 + x_2^2 + 2x_3$$

besitzt. Zeigen Sie:

- a** Alle maximalen Lösungen von $(*)$ existieren auf ganz \mathbb{R} . (1 Punkt)
- b** $\bar{x} = 0$ ist eine stabile, stationäre Lösung von $(*)$. (1 Punkt)
- c** Für jede Lösung $x: \mathbb{R} \rightarrow \mathbb{R}^3$ von $(*)$ ist $t \mapsto x_3(t)$ konstant. (2 Punkte)
- d** Es gibt ein Vektorfeld f mit den obigen Eigenschaften, für welches zusätzlich die maximale Lösung des Anfangswertproblems $x' = f(x), x(0) = (1, 0, 0)$ periodisch und nicht konstant ist. (2 Punkte)

Aufgabe 3 → S. 659

Sei $f: \mathbb{R}^2 \rightarrow \mathbb{R}^2, f(x) = (|x_2|^{1/2}, |x_1|^{1/2})$, und $D =]0, \infty[^2$. Zeigen Sie:

- a** Das Anfangswertproblem $x' = f(x), x(0) = x_0$ ist für jedes $x_0 \in D$ lokal eindeutig lösbar. (1 Punkt)
- b** Es gibt genau eine Lösung $x: [0, \infty[\rightarrow \mathbb{R}^2$ des Anfangswertproblems $\dot{x} = f(x), x(0) = 0$ mit $x(t) \in D$ für alle $t > 0$.

Hinweis Die Trajektorie einer solchen Lösungen ist der Graph einer Funktion, welche wieder eine Differentialgleichung erfüllt. (4 Punkte)

- c** Das Anfangswertproblem $\dot{x} = f(x), x(0) = 0$ ist nicht eindeutig lösbar. (1 Punkt)

Aufgabe 4 → S. 661

Sei $D = \{z \in \mathbb{C} \mid |z| < 1\}$.

- a) Bestimmen Sie alle holomorphen Funktionen $f: D \rightarrow \mathbb{C}$ mit

$$f(0) = 1 \text{ und } \forall z \in D : f'(z) = (f(z))^2.$$

(3 Punkte)

- b) Bestimmen Sie alle holomorphen Funktionen $g = u + iv: D \rightarrow \mathbb{C}$, u und v reellwertig, mit

$$u(0) = v(0) = 0 \text{ und } \forall z \in D : \sin u(z) + iv(z) \cos v(z) = 0.$$

(3 Punkte)

Aufgabe 5 → S. 662

Sei $U = \mathbb{R}^2 \setminus \{0\}$ und $f: U \rightarrow \mathbb{R}^2$ stetig differenzierbar mit folgenden Eigenschaften:

- (i) $\partial_{x_1} f_1 = \partial_{x_2} f_2$ und $\partial_{x_2} f_1 = -\partial_{x_1} f_2$.
- (ii) f ist auf $\{x \in U \mid x_1^2 + x_2^2 \leq 1\}$ unbeschränkt, und auf $\{x \in U \mid |x_1| \leq 1, x_2 = 0\}$ beschränkt.

Zeigen Sie, dass es eine Folge $(x_n)_{n \in \mathbb{N}}$ gibt mit $\lim_{n \rightarrow \infty} x_n = 0 = \lim_{n \rightarrow \infty} f(x_n)$.

(6 Punkte)

Thema Nr. 3 (Aufgabengruppe)

Aufgabe 1 → S. 663

Es seien $p: \mathbb{C} \rightarrow \mathbb{C}$ ein Polynom sowie $\gamma_{r,w}$ der positiv orientierte Rand der Kreisscheibe mit Radius $r > 0$ um $w \in \mathbb{C}$. Beweisen Sie für das komplexe Wegintegral:

$$\oint_{\gamma_{r,w}} \overline{p(z)} dz = 2\pi i r^2 \overline{p'(w)}.$$

(6 Punkte)

Aufgabe 2 → S. 664

Gegeben sei die lineare Differentialgleichung für $x: \mathbb{R} \rightarrow \mathbb{R}^3$

$$x'(t) = \begin{pmatrix} -1 & -1 \\ 4 & -1 \end{pmatrix} x(t).$$

- a** Zeigen Sie, dass der Ursprung ein asymptotisch stabiler Gleichgewichtspunkt der Differentialgleichung ist. (2 Punkte)
- b** Geben Sie einen Wert $x(0) \in \mathbb{R}^2$ an, sodass die euklidische Norm $\|x(t)\|$ der Lösung x keine monotone Funktion der Zeit $t \in \mathbb{R}$ ist. (2 Punkte)
- c** Bestimmen Sie ein $\rho > 0$, sodass für jede Lösung x die Funktion $f: \mathbb{R} \rightarrow \mathbb{R}$ mit $f(t) = x_1(t)^2 + \rho x_2(t)^2$ monoton in der Zeit $t \in \mathbb{R}$ ist. (2 Punkte)

Hinweis Zum Lösen der Aufgaben muss die allgemeine Lösung der Differentialgleichung nicht angegeben werden.

Aufgabe 3 → S. 665

Gegeben ist die Funktion $f: \mathbb{R}^2 \rightarrow \mathbb{R}^2$ mit $f(x, y) = x + y^2$. Bestimmen Sie für jedes $r > 0$ die Menge aller kritischen Punkte von f unter der Nebenbedingung $x^2 + y^2 = r^2$ und geben Sie mit Begründung an, ob es sich bei diesen um lokale Maxima oder Minima handelt. (6 Punkte)

Aufgabe 4 → S. 666

Im Folgenden sei $f: \mathbb{R}^2 \rightarrow \mathbb{R}^2$ eine integrierbare Funktion.

- a** Formulieren Sie den Transformationssatz für Integrale im Spezialfall, dass Sie das Integral von $f \circ T$ zurückführen auf das Integral über f , wobei die Transformation $T: \mathbb{R}^2 \rightarrow \mathbb{R}^2$ eine *lineare* Abbildung ist. (2 Punkte)
- b** Integrieren Sie die Funktion $f: \mathbb{R}^2 \rightarrow \mathbb{R}^2$,

$$f(x_1, x_2) = \frac{1}{(1 + (x_1 + x_2)^2)(1 + (2x_1 + 5x_2)^2)}$$

über \mathbb{R}^2 . (4 Punkte)

Aufgabe 5 → S. 667

Gegeben ist die Folge $(f_n)_{n \in \mathbb{N}}$ von Funktionen $f_n: \mathbb{R} \rightarrow \mathbb{R}$ mit

$$f_n(x) = \frac{1}{1 + n^2 x^2}.$$

Beweisen Sie:

- a** f_n konvergiert auf dem offenen Intervall $(0, 1)$ punktweise, aber nicht gleichmäßig gegen 0. (2 Punkte)
- b** $\lim_{n \rightarrow \infty} \int_0^1 f_n(x) dx = \frac{\pi}{2}$. (2 Punkte)
- c** Für jeden Parameter $\alpha \in (0, 1)$ ist $\lim_{n \rightarrow \infty} \int_0^1 x^\alpha f_n(x) dx = 0$. (2 Punkte)

Lösungen zu Thema Nr. 1

Lösungsvorschlag zur Aufgabe (Frühjahr 2017, T1A1)

Für alle $z \in \mathbb{C}$ gilt $e^{-|z|} \leq 1$ und somit die Abschätzung

$$|f'(z)| \leq 1 + e^{-|z|} \leq 2 \quad \text{für alle } z \in \mathbb{C} \setminus B_3(0). \quad (\star)$$

Aufgrund des Maximumsprinzip für beschränkte Gebiete gibt es außerdem ein $z_0 \in \partial B_3(0)$, sodass

$$|f'(z)| \leq |f(z_0)| \leq 2 \quad \text{für alle } z \in B_3(0),$$

wobei wir verwendet haben, dass auch z_0 die Abschätzung (\star) aus der Angabe erfüllt. Insgesamt ist damit f' beschränkt. Da mit f auch f' eine ganze Funktion ist, folgt mit dem Satz von Liouville, dass $f'(z) = a$ für alle $z \in \mathbb{C}$ und ein $a \in \mathbb{C}$ gilt. Als ganze Funktion hat f (bzw f') eine auf ganz \mathbb{C} gültige Potenzreihendarstellung der Form

$$f(z) = \sum_{k=0}^{\infty} a_k z^k \quad \text{bzw.} \quad f'(z) = \sum_{k=1}^{\infty} k a_k z^{k-1}.$$

Wegen $f'(z) = a$ für $z \in \mathbb{C}$ folgt $a_k = 0$ für $k > 2$ und $a_1 = a$. Damit wird f zu

$$f(z) = a_0 + az$$

und mit $b = a_0$ ist die geforderte Gleichung gezeigt.

Lösungsvorschlag zur Aufgabe (Frühjahr 2017, T1A2)

- a** Man berechnet

$$z^2 + iz - 2 = 0 \quad \Leftrightarrow \quad z = \frac{-i \pm \sqrt{-1+8}}{2} = \frac{-i \pm \sqrt{7}}{2}.$$

Da der Imaginärteil aller Nennernullstellen negativ ist, liegen diese nicht in X und f hat auf X keine Singularitäten.

b Wir berechnen für $z = x + iy$ mit $y \geq 0$ das Betragsquadrat des Nenners zu

$$\begin{aligned}
 |z^2 + iz - 2| &= |(x+iy)^2 + i(x+iy) - 2|^2 = \\
 &= (x^2 - y^2 - (y+2))^2 + (2xy + x)^2 = \\
 &= (x^2 - y^2)^2 - 2(x^2 - y^2)(y+2) + (y+2)^2 + 4x^2y^2 + 4x^2y + x^2 = \\
 &= x^4 - 2x^2y^2 + y^4 - 2yx^2 - 4x^2 + 2y^3 + 4y^2 + \\
 &\quad + y^2 + 4y + 4 + 4x^2y^2 + 4x^2y + x^2 = \\
 &= x^4 + 2x^2y^2 + y^4 + 2yx^2 - 3x^2 + y^3 + 5y^2 + 4y + 4 \geq \\
 &\geq x^4 - 3x^2 + 4 = (x^2 - \frac{3}{2})^2 + \frac{7}{4} \geq \frac{7}{4}
 \end{aligned}$$

Damit haben wir

$$|f(z)| \leq \frac{2}{\sqrt{7}} \quad \text{für alle } z \in X.$$

Wegen $|f(\sqrt{\frac{3}{2}})| = \frac{2}{\sqrt{7}}$ wird der minimale Wert auch angenommen, d. h. $\frac{2}{\sqrt{7}}$ ist ein globales Maximum von $|f|$ auf X .

c Nehmen wir an, dass $x + iy \in X$ ein Maximum des Betrags ist. Die obige Ungleichung ist für $y > 0$ oder $x^2 \neq \frac{3}{2}$ strikt, also kommen nur die beiden Punkte $\pm\sqrt{\frac{3}{2}}$ in Frage. Einsetzen zeigt, dass diese auch tatsächlich beide ein Extremum sind.

Lösungsvorschlag zur Aufgabe (Frühjahr 2017, T1A3)

a Angenommen, es gibt so eine ganze Funktion $f: \mathbb{C} \rightarrow \mathbb{C}$, dann wäre auch $f': \mathbb{C} \rightarrow \mathbb{C}$ ganz und insbesondere die Einschränkung $f'_{|\mathbb{C} \setminus \{0\}|}$ holomorph, müsste also auf ihrem Definitionsbereich die Cauchy-Riemann-Differentialgleichungen erfüllen. Unter Verwendung von $\partial_x|z| = \frac{x}{|z|}$ und $\partial_y|z| = \frac{y}{|z|}$ für $z \neq 0$ lautet die erste davon:

$$\begin{aligned}
 \partial_x \operatorname{Re} f'(z) &= \partial_x \operatorname{Re}(|z|f(z)) = \frac{x \operatorname{Re} f(z)}{|z|} + |z| \partial_x \operatorname{Re} f(z) = \\
 &\stackrel{!}{=} \frac{y \operatorname{Im} f(z)}{|z|} + |z| \partial_y \operatorname{Im} f(z) = \partial_y \operatorname{Im}(|z|f(z)) = \partial_y \operatorname{Re} f'(z)
 \end{aligned}$$

Da f selbst holomorph ist und die Cauchy-Riemann-Differentialgleichungen erfüllt, reduziert sich obige Gleichung für $z \neq 0$ auf

$$x \operatorname{Re} f(z) = y \operatorname{Im} f(z).$$

Verwendet man nun $f(1) = \pi$, um diese Gleichung bei 1 auszuwerten, erhält man $\pi = 0$. Der Widerspruch zeigt, dass f zumindest in 1 nicht holomorph sein kann. Insbesondere kann f keine ganze Funktion sein.

- b** Seien f_1 und f_2 zwei Funktionen mit den angegebenen Eigenschaften. Dann gilt für die ganze Funktion $g = f_1 - f_2$

$$g'(z) = f'_1(z) - f'_2(z) = \sin(z)(f_1(z) - f_2(z)) = \sin(z)g(z), \quad g(0) = 0.$$

Betrachte nun die Abbildung $h(z) = g(z)e^{\cos z}$. Auch diese ist eine ganze Funktion und es gilt für $z \in \mathbb{C}$

$$h'(z) = g'(z)e^{\cos z} - g(z)e^{\cos z} \sin z = \sin(z) \cdot g(z)e^{\cos z} - g(z)e^{\cos z} \sin(z) = 0.$$

Also ist h konstant, wegen $h(0) = 0$ ist somit $h(z) = 0$ für alle $z \in \mathbb{C}$. Da $e^z \neq 0$ für alle $z \in \mathbb{C}$ gilt, folgt daraus $g(z) = 0$ und somit $f_1 = f_2$.

Lösungsvorschlag zur Aufgabe (Frühjahr 2017, T1A4)

- a** Laut dem Hauptsatz der Differential- und Integralrechnung gilt

$$\frac{d}{dx} \int_0^x e^{t^2} dt = e^{x^2}.$$

Mit der Kettenregel folgt daraus

$$f'(x) = e^{\sin^2(x)} \cdot \cos x.$$

- b** Definiere zunächst die Funktion

$$\hat{g}(y, z) : \mathbb{R}^2 \rightarrow \mathbb{R}, \quad (y, z) \mapsto \int_0^{\sin z} \sqrt{t^4 + 3y^2} dy,$$

dann gilt nach der Kettenregel:

$$g'(z) = \frac{d}{dz} \hat{g}(z, z) = (\nabla \hat{g}) \cdot \begin{pmatrix} 1 \\ 1 \end{pmatrix}.$$

Wie berechnen daher (wie in **a**):

$$\partial_z \hat{g}(y, z) = \frac{d}{dz} \int_0^{\sin z} \sqrt{t^4 + 3y^2} dt = \sqrt{\sin^4(z)^4 + 3y^2} \cdot \cos z$$

Um $\partial_y \hat{g}(y, z)$ berechnen zu können, wenden wir zunächst den Satz über die Differenzierbarkeit von Parameterintegralen an: Es gilt

$$\partial_y \sqrt{t^4 + 3y^2} = \frac{3y}{\sqrt{t^4 + 3y^2}},$$

also ist die Funktion $(y, t) \mapsto \sqrt{t^4 + 3y^2}$ für $t \neq 0$ stetig partiell differenzierbar nach y , außerdem stetig in t . Da wir uns am Ende für die Ableitung von g an der Stelle $z = \pi$ interessieren, können wir uns außerdem auf $y \in [3, 4]$ beschränken. In diesem Fall ist nämlich

$$\partial_y \sqrt{t^4 + 3y^2} = \frac{3y}{\sqrt{t^4 + 3y^2}} \leq \frac{12}{\sqrt{0+27}},$$

d. h. der Integrand besitzt integrierbare Majorante. Wir können nun Ableitung und Integration vertauschen:

$$\partial_y \hat{g}(y, z) = \partial_y \int_0^{\sin z} \sqrt{t^4 + 3y^2} dt = \int_0^{\sin z} \partial_y \sqrt{t^4 + 3y^2} dt.$$

Wertet man $\partial_y \hat{g}(y, z)$ an der Stelle (π, π) aus, erhält man auf jeden Fall 0, da von 0 bis 0 integriert wird. Insgesamt folgt:

$$g'(\pi) = \partial_z \hat{g}(\pi, \pi) + (\partial_y \hat{g})(\pi, \pi) = (\sqrt{\sin^4(\pi)^4 + 3\pi^2} \cdot \cos \pi + 0) = -\pi\sqrt{3}.$$

Lösungsvorschlag zur Aufgabe (Frühjahr 2017, T1A5)

a Die Lösungsformel aus der Variation der Konstanten ergibt zunächst

$$2 \exp \left(\int_0^t \frac{6s}{1+3s^2} ds \right) + \exp \left(\int_0^t \frac{6s}{1+3s^2} ds \right) \int_0^s \exp \left(- \int_0^r \frac{6r}{1+3r^2} dr \right) 5ds.$$

Nun gilt

$$\int_0^t \frac{6s}{1+3s^2} ds = \left[\ln(1+3s^2) \right]_0^t = \ln(1+3t^2).$$

Damit erhalten wir

$$\varphi(t) = 2(1 + 3t^2) + (1 + 3t^2) \int_0^t \frac{5}{1 + 3s^2} ds.$$

Mittels Substitution erhalten wir für das hintere Integral

$$\begin{aligned} \int_0^t \frac{5}{1 + 3s^2} ds &= \int_0^{\sqrt{3}t} \frac{5}{\sqrt{3}(1 + s^2)} ds = \frac{5}{\sqrt{3}} \int_0^{\sqrt{3}t} \frac{1}{1 + s^2} ds = \\ &= \frac{5}{\sqrt{3}} [\arctan s]_0^{\sqrt{3}t} = \frac{5}{\sqrt{3}} \arctan(\sqrt{3}t). \end{aligned}$$

Die Lösung ist somit

$$\varphi(t) = 2 + 6t^2 + \frac{5}{\sqrt{3}} (1 + 3t^2) \arctan(\sqrt{3}t).$$

Man überprüft unmittelbar, dass diese Funktion das Anfangsproblem löst. Da φ auf ganz \mathbb{R} definiert ist, handelt es sich außerdem um die maximale Lösung.

b Wir bestimmen mit der Regel von l'Hospital:

$$\begin{aligned} \lim_{t \rightarrow \infty} t (\arctan t - \frac{\pi}{2}) &= \lim_{t \rightarrow \infty} \frac{\arctan t - \frac{\pi}{2}}{t^{-1}} = \\ &= \lim_{t \rightarrow \infty} \frac{(1 + t^2)^{-1}}{-t^{-2}} = \lim_{t \rightarrow \infty} \frac{-t^2}{1 + t^2} = -1. \end{aligned}$$

Ist nun $y(t)$ eine Lösung der Gleichung, so gilt

$$y(t)^3 = 5 \cdot [y'(t) - t(\arctan(t) - \frac{\pi}{2})]$$

und wegen $\lim_{t \rightarrow \infty} y'(t) = 0$ konvergiert die rechte Seite der Gleichung. Aufgrund der Stetigkeit von $t \mapsto \sqrt[3]{t}$ folgt daraus die Konvergenz von $y(t)$. Um den Grenzwert zu bestimmen, betrachte:

$$(\lim_{t \rightarrow \infty} y(t))^3 = \cdot \lim_{t \rightarrow \infty} y(t)^3 = 5[0 - (-1)] = 5 \Leftrightarrow \lim_{t \rightarrow \infty} y(t) = \sqrt[3]{5}.$$

Lösungsvorschlag zur Aufgabe (Frühjahr 2017, T2A1)

- a** Es gilt $f_n(0) = g_n(0) = 0$ für alle $n \in \mathbb{N}$ sowie $f_n(x), g_n(x) > 0$ für $x \in]0, \infty[$. Also ist 0 ein Minimum von f_n und g_n auf $[0, \infty[$. Zur Untersuchung auf Maxima berechne zunächst

$$f'_n(x) = nx^{n-1}e^{-nx} + x^n e^{-nx}(-n) = nx^{n-1}e^{-nx}(1-x).$$

Damit hat f'_n eine Nullstelle bei $x = 1$. Da der erste Faktor stets positiv ist, gilt $f'(x) > 0$ für $x < 1$ und $f'(x) < 0$ für $x > 1$, sodass an der Stelle $x = 1$ ein Maximum vorliegt. Der zugehörige Funktionswert berechnet sich zu $f_n(1) = e^{-n}$.

Analog verfahren wir für g_n und erhalten

$$g'_n(x) = nx^{n-1}e^{-x^n} + x^n e^{-x^n}(-nx^{n-1}) = nx^{n-1}e^{-x^n}(1-x^n).$$

Neben der schon behandelten Nullstelle bei 0, hat auch g'_n nur die Nullstelle $x = 1$ und aus dem gleichen Grund wie zuvor liegt dort ein Maximum mit Funktionswert $g_n(1) = e^{-1}$ vor.

- b** Wir zeigen zunächst, dass $(f_n)_{n \in \mathbb{N}}$ punktweise gegen die Nullfunktion konvergiert. Sei dazu $x \in [0, \infty[$. Die Abschätzungen aus Teil **a** zeigen, dass $xe^{-x} = f_1(x) \leq e^{-n} < 1$ gilt. Daher erhalten wir

$$\lim_{n \rightarrow \infty} f_n(x) = \lim_{n \rightarrow \infty} x^n e^{-nx} = \lim_{n \rightarrow \infty} (xe^{-x})^n \leq \lim_{n \rightarrow \infty} e^{-n^2} = 0.$$

Da das Maximum von g_n konstant bei e^{-1} lag, kann $(g_n)_{n \in \mathbb{N}}$ nicht gegen die Nullfunktion konvergieren. Wir zeigen stattdessen, dass $(g_n)_{n \in \mathbb{N}}$ punktweise gegen

$$g: [0, \infty[\rightarrow \mathbb{R}, \quad x \mapsto \begin{cases} e^{-1} & \text{falls } x = 1 \\ 0 & \text{sonst} \end{cases}$$

konvergiert. Für $x = 1$ ist dies klar. Für $x < 1$ gilt $\lim_{n \rightarrow \infty} x^n = 0$ und daher

$$\lim_{n \rightarrow \infty} g_n(x) = \lim_{n \rightarrow \infty} x^n e^{-x^n} \leq \lim_{n \rightarrow \infty} x^n = 0 = g(x).$$

Für $x > 1$ schließlich erhalten wir wegen $\lim_{n \rightarrow \infty} x^n = \infty$:

$$\lim_{n \rightarrow \infty} g_n(x) = \lim_{n \rightarrow \infty} x^n e^{-x^n} = \lim_{x \rightarrow \infty} xe^{-x} = 0 = g(x).$$

- c** Das Argument aus Teil **b** zeigt bereits, dass $(f_n)_{n \in \mathbb{N}}$ gleichmäßig konvergiert: Sei $\varepsilon > 0$. Wähle $N \in \mathbb{N}$ so groß, dass $e^{-N} < \varepsilon$. Es gilt dann für $x \in [0, \infty[$ und $n \geq N$

$$f_n(x) \leq f_n(1) = e^{-n} \leq e^{-N} < \varepsilon.$$

Würde die Folge $(g_n)_{n \in \mathbb{N}}$ gleichmäßig konvergieren, so würde aus der Stetigkeit von g_n auch die Stetigkeit der Grenzfunktion g folgen. Jedoch haben wir bereits in **b** gesehen, dass g nicht stetig ist.

Lösungsvorschlag zur Aufgabe (Frühjahr 2017, T2A2)

- a** Da f nach Voraussetzung stetig differenzierbar ist, ist f nach Proposition 7.10 auch lokal Lipschitz-stetig. Da die Differentialgleichung $x' = f(x)$ auf dem Gebiet \mathbb{R}^3 definiert ist, gibt es nach dem Globalen Existenz- und Eindeutigkeitssatz 7.12 eine eindeutige maximale Lösung $\lambda:]a, b[\rightarrow \mathbb{R}^3$ zu jedem Anfangswert $\lambda(\tau) = \xi$.

Nehmen wir an, es ist $a > -\infty$, dann muss wegen $\partial\mathbb{R}^2 = \emptyset$ laut Satz 7.13 die Bedingung $\lim_{t \searrow a} \|\lambda(t)\| = \infty$ gelten. Insbesondere wäre dann

$$\lim_{t \searrow a} v(\lambda(t)) = \lim_{t \searrow a} \|\lambda(t)\|^2 = \infty.$$

Jedoch ist v laut Angabe eine Erhaltungsgröße für die Differentialgleichung $x' = f(x)$, sodass

$$\lim_{t \searrow a} v(\lambda(t)) = \lim_{t \searrow a} v(\lambda(\frac{a+b}{2})) = v(\lambda(\frac{a+b}{2})) < \infty$$

gilt. Die einzige Möglichkeit ist daher $a = -\infty$ und genauso zeigt man $b = \infty$. Insgesamt ist dann λ auf ganz \mathbb{R} definiert.

- b** Wir zeigen die Stabilität der Nulllösung direkt anhand der Definition. Seien dazu $\varepsilon > 0$ und $\tau \in \mathbb{R}$ vorgegeben. Nach Teil **a** existiert für jeden Anfangswert $\xi \in \mathbb{R}^3$ die maximale Lösung $\lambda: \mathbb{R} \rightarrow \mathbb{R}^3$ zum Anfangswert $\lambda(\tau) = \xi$, also insbesondere diejenige zu den Anfangswerten ξ mit $\|\xi\| < \varepsilon$. Da v eine Erhaltungsgröße für $x' = f(x)$ ist, haben wir

$$\|\lambda(t) - 0\| = \|\lambda(t)\| = \sqrt{v(\lambda(t))} = \sqrt{v(\lambda(\tau))} = \sqrt{\|\xi\|^2} = \|\xi\| < \varepsilon$$

für alle $t \in \mathbb{R}$.

- c** Da $v(x(t))$ und $w(x(t))$ für jede Lösung $x: \mathbb{R} \rightarrow \mathbb{R}^3$ konstant sind, ist auch

$$x_3^2(t) - 2x_3(t) = v(x(t)) - w(x(t)) =: c$$

konstant. Diese quadratische Gleichung für $x_3(t)$ hat genau zwei diskrete Lösungen. Da $x_3(t)$ stetig ist, kann nur eine davon angenommen werden, d.h. $x_3(t)$ ist konstant.

- d** Sei $\lambda: \mathbb{R} \rightarrow \mathbb{R}^3$ die maximale Lösung der Differentialgleichung $x' = f(x)$ zum Anfangswert $x(0) = (1, 0, 0)$ mit dem zu bestimmenden Vektorfeld $f: \mathbb{R}^3 \rightarrow \mathbb{R}^3$. Nach Teil **c** folgt aus $\lambda_3(0) = 0$ sogar $\lambda_3(t) = 0$ für alle $t \in \mathbb{R}$. Wegen

$$v(\lambda(t)) = \lambda_1^2(t) + \lambda_2^2(t) = \text{const.}$$

für alle $t \in \mathbb{R}$ muss sich λ auf einer Kreisbahn bewegen. Ein mögliches λ ist daher die periodische und nicht-konstante Funktion

$$\lambda: \mathbb{R} \rightarrow \mathbb{R}^3, \quad t \mapsto (\cos t, \sin t, 0).$$

Die zugehörige Differentialgleichung ist

$$x'_1 = -x_2, \quad x'_2 = x_1, \quad x'_3 = 0,$$

was dem Vektorfeld

$$f: \mathbb{R}^3 \rightarrow \mathbb{R}^3, \quad (x_1, x_2, x_3) \mapsto (-x_2, x_1, 0)$$

entspricht.

Lösungsvorschlag zur Aufgabe (Frühjahr 2017, T2A3)

- a** Der Definitionsbereich der Gleichung ist mit $\mathbb{R} \times D$ ein Gebiet, die Funktion f ist als Verkettung stetiger Funktionen auf \mathbb{R}^2 stetig. Für $x, y > 0$ gilt ferner $f(x, y) = (x^{1/2}, y^{1/2})$ und damit

$$(Df)(x, y) = \begin{pmatrix} 0 & \frac{1}{2}x_2^{-1/2} \\ \frac{1}{2}x_1^{-1/2} & 0 \end{pmatrix}.$$

Da alle Einträge dieser Jacobi-Matrix stetig sind, ist $f|_D$ stetig differenzierbar, also Lipschitz-stetig. Deshalb folgt die Behauptung aus dem Globalen Existenz- und Eindeutigkeitssatz.

- b** Sei $x: [0, \infty[\rightarrow \mathbb{R}^2$ eine Lösung von $\dot{x} = f(x)$ mit $x(0) = 0$ und $x(t) \in D$ für $t > 0$. Laut dem Hinweis ist dann die Trajektorie dieser Lösung als

Graph einer Funktion darstellbar, d. h. es gibt eine Funktion $g: [0, \infty[\rightarrow \mathbb{R}$ mit $g(x_2(t)) = x_1(t)$ für alle $t \geq 0$. Es gilt dann nach der Kettenregel

$$\begin{aligned}\dot{x}_1(t) &= \frac{dg(x_2(t))}{dt} = g'(x_2(t)) \cdot \dot{x}_2(t) \\ \Leftrightarrow g'(x_2(t)) &= \frac{\dot{x}_1(t)}{\dot{x}_2(t)} = \left(\frac{x_2(t)}{x_1(t)} \right)^{1/2} = \left(\frac{x_2(t)}{g(x_2(t))} \right)^{1/2}.\end{aligned}$$

Die Funktion g ist also Lösung der Differentialgleichung $y' = \left(\frac{x_2}{y} \right)^{1/2}$ zu einem Anfangswert $y(x_2(\tau)) = x_1(\tau)$ für ein $\tau > 0$. Diese Differentialgleichung ist auf dem Gebiet D definiert, außerdem ist die rechte Seite wegen

$$\partial_y \left(\frac{x_2}{y} \right)^{1/2} = \frac{1}{2\sqrt{\frac{x_2}{y}}} \cdot \frac{-x_2}{y^2}$$

auf D partiell stetig differenzierbar, also nach Proposition 7.10 lokal Lipschitz-stetig bezüglich y . Nach dem Globalen Existenz- und Eindeutigkeitssatz besitzt das Anfangswertproblem daher eine eindeutige maximale Lösung. Diese Lösung bestimmen wir nun mittels Trennen der Variablen:

$$\begin{aligned}\int_{x_1(\tau)}^{g(x_2)} y^{1/2} dy &= \int_{\tau}^{x_2} \omega^{1/2} d\omega \quad \Leftrightarrow \\ \Leftrightarrow \frac{2}{3}(g(x_2)^{3/2} - x_1(\tau)^{2/3}) &= \frac{2}{3}(x_2^{3/2} - \tau^{3/2}) \\ \Leftrightarrow g(x_2) &= (x_2^{3/2} - \tau^{3/2} + x_1(\tau)^{3/2})^{2/3}\end{aligned}$$

Diese Lösung ist auf ganz $[0, \infty[$ definiert und deshalb die eindeutige maximale Lösung des Anfangswertproblems. Wir wollen ja eigentlich, dass $(x_1(0), x_2(0)) = (0, 0)$, also $g(0) = 0$. Einsetzen dieser Bedingung liefert $\tau = x_1(\tau)$, sodass $g(x_1) = x_2$.

Wir haben also gezeigt, dass für jede Lösung x mit den genannten Eigenschaften $x_1(t) = x_2(t)$ für alle $t \geq 0$ gelten muss. Die ursprüngliche Differentialgleichung reduziert sich daher für diese Lösung auf

$$\dot{x}_1(t) = \sqrt{x_1(t)}.$$

Diese Differentialgleichung ist wieder auf dem Gebiet D definiert und die rechte Seite dort stetig partiell differenzierbar nach x_1 . Laut Globalen Existenz und Eindeutigkeitssatz gibt es daher zu jedem Anfangswert eine eindeutige maximale Lösung. Wie oben berechnet man diese mittels

Trennen der Variablen zu

$$x_1(t) = \left(\frac{1}{2}(t - \tau) + \sqrt{x_1(\tau)}\right)^2.$$

Die Bedingung $x_1(0) = 0$ erzwingt $x_1(t) = \frac{1}{2}t^2$, also ist die eindeutige Lösung mit den gewünschten Eigenschaften die Abbildung

$$x : [0, \infty[\rightarrow D, \quad t \mapsto (\frac{1}{2}t^2, \frac{1}{2}t^2).$$

- c** Sei λ die Lösung aus Teil **b**. Dann ist λ eine Lösung des gegebenen Anfangswertproblems. Ferner ist aber auch $\mu(t) = 0$ eine Lösung, denn es ist

$$\frac{d\mu(t)}{dt} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} = \begin{pmatrix} |0|^{1/2} \\ |0|^{1/2} \end{pmatrix} = f(0).$$

Wegen $\lambda(t) \neq 0$ für alle $t > 0$ sind diese beiden Lösungen nicht identisch, das Anfangswertproblem ist also nicht eindeutig lösbar.

Lösungsvorschlag zur Aufgabe (Frühjahr 2017, T2A4)

- a** Wir beweisen per vollständiger Induktion, dass $f^{(n)}(0) = n!$ für $n \in \mathbb{N}$ gilt. Der Induktionsanfang ergibt sich direkt aus $f'(0) = f(0)^2 = 1$. Nehmen wir an, die Gleichung ist für $n \in \mathbb{N}$ erfüllt. Mithilfe der verallgemeinerten Produktregel (Leibniz'sche Regel) erhalten wir zunächst

$$f^{(n+1)}(z) = \frac{d}{dz^n} f'(z) = \frac{d}{dz^n} f(z)f(z) = \sum_{k=0}^n \binom{n}{k} f^{(k)}(z) f^{(n-k)}(z).$$

Einsetzen der Induktionsvoraussetzung liefert nun

$$\begin{aligned} f^{(n+1)}(0) &= \sum_{k=0}^n \binom{n}{k} f^{(k)}(0) f^{(n-k)}(0) = \sum_{k=0}^n \binom{n}{k} k!(n-k)! \\ &= \sum_{k=0}^n n! = (n+1)!. \end{aligned}$$

Somit ist

$$f(z) = \sum_{k=0}^{\infty} \frac{f^{(k)}(0)}{k!} z^k = \sum_{k=0}^{\infty} z^k = \frac{1}{1-z}.$$

Tatsächlich prüft man unmittelbar, dass diese Funktion die geforderten Bedingungen erfüllt.

- b** Laut Voraussetzung sind u und v reellwertig. Aus der angegebenen Gleichung und der Eindeutigkeit von Real- und Imaginärteil folgt also, dass für $z \in D$

$$\sin u(z) = 0 = v(z) \cos v(z)$$

gelten muss. Aus der ersten Gleichung folgt $u(z) \subseteq \{k\pi \mid k \in \mathbb{Z}\}$. Damit kann das Bild $g(D)$ jedoch nicht offen (also kein Gebiet) sein, denn für jedes $k \in \mathbb{Z}$ und $\varepsilon < \pi$ liegt $k\pi + \varepsilon$ nicht in der Menge. Laut dem Satz von der Gebietstreue muss g damit konstant sein. Zusammen mit dem Anfangswert erhalten wir $g(z) = 0$ für alle $z \in D$. Wiederum prüft man unmittelbar, dass diese Funktion die Bedingungen erfüllt.

Lösungsvorschlag zur Aufgabe (Frühjahr 2017, T2A5)

Wir betrachten die komplexe Funktion

$$g: \mathbb{C} \setminus \{0\} \rightarrow \mathbb{C}, \quad x + iy \mapsto f_1(x, y) + if_2(x, y).$$

Die Bedingung (i) entspricht genau den Cauchy-Riemannschen Differentialgleichungen für g , sodass g holomorph ist. Wir untersuchen nun den Typ der Singularität 0. Wäre 0 hebbbar, so gäbe es eine holomorphe Fortsetzung auf \mathbb{C} und diese würde auf der kompakten Menge $\overline{\mathbb{E}}$ ein Maximum annehmen – Widerspruch dazu, dass f auf $\overline{\mathbb{E}}$ unbeschränkt ist.

Zudem ist $z_n = \frac{1}{n}$ eine Folge in U_2 mit $\lim_{n \rightarrow \infty} z_n = 0$, entlang derer f laut Bedingung (ii) beschränkt bleibt, also ist

$$\lim_{z \rightarrow 0} f(z) \neq \infty.$$

Dies zeigt, dass 0 auch keine Polstelle von f ist. Deshalb muss 0 eine wesentliche Singularität sein.

Wir folgern nun die Existenz einer Folge mit den geforderten Eigenschaften aus dem Satz von Casorati-Weierstraß: Sei dazu $n \in \mathbb{N}$. Laut dem Satz ist das Bild von $B_{\frac{1}{n}}(0)$ dicht in \mathbb{C} , d. h. es gibt ein $z_n \in B_{\frac{1}{n}}(0)$, sodass $|f(z_n) - 0| < \frac{1}{n}$ gilt. Die komplexe Folge $(z_n)_{n \in \mathbb{N}}$ erfüllt nun $\lim_{n \rightarrow \infty} z_n = 0 = \lim_{n \rightarrow \infty} f(z_n)$. Definiere die Folge $(x_n)_{n \in \mathbb{N}}$ durch $x_n = (\operatorname{Re} z_n, \operatorname{Im} z_n)$, so hat diese die verlangten Eigenschaften.

Lösungen zu Thema Nr. 3

Lösungsvorschlag zur Aufgabe (Frühjahr 2017, T3A1)

Sei $p(z) = \sum_{k=0}^n a_k z^k$. Nach Definition ist die Kurve $\gamma_{r,w}$ gegeben durch

$$\gamma_{r,w}: [0, 2\pi] \rightarrow \mathbb{C}, \quad t \mapsto w + re^{it}.$$

Damit berechnen wir nun:

$$\begin{aligned} \int_{\gamma_{r,w}} \overline{p(z)} dz &= \int_{\gamma_{r,w}} \sum_{k=0}^n \overline{a_k} \cdot \bar{z}^k dz = \int_0^{2\pi} \left(\sum_{k=0}^n \overline{a_k} (\bar{\omega} + re^{-it})^k \right) \cdot ire^{it} dt = \\ &= \sum_{k=0}^n ir\bar{a}_k \int_0^{2\pi} (\bar{\omega} + re^{-it}) \cdot e^{it} dt = \\ &= \sum_{k=0}^n ir\bar{a}_k \int_0^{2\pi} \sum_{l=0}^k \binom{k}{l} \bar{\omega}^{k-l} \cdot (re^{-it})^l \cdot e^{it} dt = \\ &= \sum_{k=0}^n ir\bar{a}_k \sum_{l=0}^k \binom{k}{l} \bar{\omega}^{k-l} r^l \int_0^{2\pi} e^{-i(l-1)t} dt \end{aligned}$$

Wir berechnen das Integral zunächst für den Fall $l \neq 1$, denn in diesem Fall ist $l-1 \neq 0$, sodass

$$\int_0^{2\pi} e^{-i(l-1)t} dt = \left[\frac{i}{l-1} e^{-i(l-1)t} \right]_0^{2\pi} = 0.$$

In der Summe oben fallen alle Summanden mit $l \neq 1$ weg und übrig bleibt:

$$\sum_{k=0}^n ir\bar{a}_k \binom{k}{1} \bar{\omega}^{k-1} r \int_0^{2\pi} 1 dt = 2\pi ir^2 \sum_{k=0}^n \bar{a}_k k \bar{\omega}^{k-1} = 2\pi ir^2 \overline{p'(\omega)}$$

Lösungsvorschlag zur Aufgabe (Frühjahr 2017, T3A2)

- a** Das charakteristische Polynom der Koeffizientenmatrix ist $\chi_a = X^2 + 2X + 5$. Die Eigenwerte der Matrix sind daher

$$\lambda = \frac{-2 \pm \sqrt{4 - 20}}{2} = -1 \pm 2i.$$

Da alle Eigenwerte negativen Realteil haben, ist die Nulllösung laut Satz 7.29 asymptotisch stabil.

- b** Wir berechnen:

$$\begin{aligned}\frac{d}{dt} \|x(t)\|^2 &= \frac{d}{dt} (x_1^2(t) + x_2^2(t)) = 2x_1(t)\dot{x}_1(t) + 2x_2(t)\dot{x}_2(t) = \\ &= 2(x_1(-x_1 - x_2) + x_2(4x_1 - x_2)) = \\ &= (-x_1^2 + 3x_1x_2 - x_2^2)\end{aligned}$$

Wählen wir beispielweisweise $x(0) = (1, -\frac{3+\sqrt{5}}{2})$, so hat die Ableitung von $\|x(t)\|^2$ mindestens eine Nullstelle. Damit kann $\|x(t)\|^2$ nur monoton sein, falls $\|x(t)\|$ konstant ist, d. h. $\|x(t)\| = \|(1, -\frac{3+\sqrt{5}}{2})\|$ für alle $t \in \mathbb{R}$. Insbesondere ist diese Lösung x nicht attraktiv im Widerspruch dazu, dass nach **a** der Ursprung eine asymptotisch stabile Ruhelage ist, alle Lösungen also asymptotisch stabil sind. Der Betrag von $x(t)$ kann daher nicht konstant bleiben.

- c** Wir berechnen:

$$\begin{aligned}\frac{d}{dt} f(t) &= \frac{d}{dt} (x_1^2(t) + \rho x_2^2(t)) = 2x_1(t)\dot{x}_1(t) + 2\rho x_2(t)\dot{x}_2(t) = \\ &= 2(x_1(-x_1 - x_2) + \rho x_2(4x_1 - x_2)) = \\ &= 2(-x_1^2 + (-1 + 4\rho)x_1x_2 - \rho x_2^2)\end{aligned}$$

Wähle $\rho = \frac{1}{4}$, dann gilt also

$$\dot{f}(t) = -2(x_1^2 + \frac{1}{4}x_2^2) \leq 0,$$

d. h. die Funktion f ist monoton fallend.

Lösungsvorschlag zur Aufgabe (Frühjahr 2017, T3A3)

Die Menge $K = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = r^2\}$ ist die Nullstellenmenge der Funktion $\varphi(x, y) = x^2 + y^2 - r^2$. Diese ist eine stetig differenzierbare Funktion mit Gradienten

$$(\nabla \varphi)(x, y) = \begin{pmatrix} 2x \\ 2y \end{pmatrix}.$$

Dieser verschwindet nur im Punkt $(0, 0) \notin K$, also bildet K eine eindimensionale Untermannigfaltigkeit des \mathbb{R}^2 . Laut dem Satz über Extrema unter Nebenbedingungen ist (x, y) nur dann ein Extremum, wenn es ein $\lambda \in \mathbb{R}$ gibt, sodass

$$(\nabla \varphi)(x, y) = \lambda (\nabla f)(x, y) \Leftrightarrow \begin{pmatrix} 2x \\ 2y \end{pmatrix} = \lambda \begin{pmatrix} 1 \\ 2y \end{pmatrix}.$$

Die erste Gleichung liefert $\lambda = 2x$ und eingesetzt in die zweite Gleichung ergibt dies

$$2y = (2x)2y \Leftrightarrow 2y(1 - 2x) = 0 \Leftrightarrow y = 0 \text{ oder } x = \frac{1}{2}.$$

Im Fall $y = 0$ erhalten wir mittels der definierenden Gleichung von K , dass $x = \pm r$ sein muss. Nur im Fall $r \geq \frac{1}{2}$ liefert die zweite Lösung überhaupt einen Punkt in der Menge K , der sich dann zu

$$\frac{1}{4} + y^2 = r^2 \Leftrightarrow y = \pm \sqrt{r^2 - \frac{1}{4}}$$

berechnet. Die Menge der kritischen Punkte ist also

$$\begin{aligned} & \{(\pm r, 0)\} && \text{falls } r < \frac{1}{2} \\ & \{(\pm r, 0), \left(\frac{1}{2}, \pm \sqrt{r^2 - \frac{1}{4}}\right)\} && \text{falls } r \geq \frac{1}{2}. \end{aligned}$$

Um zu sehen, wo ein globales Extremum vorliegt, berechnen wir die zugehörigen Funktionswerte:

$$f(r, 0) = r, \quad f(-r, 0) = -r, \quad f\left(\frac{1}{2}, \pm \sqrt{r^2 - \frac{1}{4}}\right) = r^2 + \frac{1}{4}$$

Das Minimum ist damit $-r$ und wird an der Stelle $(-r, 0) \in K$ angenommen. Ferner gilt für alle $r > 0$

$$r^2 - r + \frac{1}{4} = \left(r - \frac{1}{2}\right)^2 > 0 \Leftrightarrow r^2 + \frac{1}{4} > r,$$

also ist das Maximum $r^2 + \frac{1}{4}$ und wird an den Stellen $(\frac{1}{2}, \pm \sqrt{r^2 - \frac{1}{4}})$ angenommen.

Alternative: Ohne den Satz über Extrema unter Nebenbedingungen kommt man aus, wenn man für K die Parametrisierung

$$\phi: [0, 2\pi] \rightarrow K, t \mapsto (r \cos t, r \sin t)$$

wählt. Die Verkettung $f \circ \phi$ ist eine reellwertige auf $[0, 2\pi]$ definierte Funktion und kann entsprechend mit den Mitteln der Analysis einer reeller Variablen auf Extrema untersucht werden. Es ergibt sich Hochpunkte bei $t = \arccos(\frac{1}{2r})$ und $t = 0$ sowie ein Tiefpunkt bei $t = \pi$. Einsetzen der Werte in $f \circ \phi$ gibt die Minima und Maxima und Einsetzen in ϕ die zugehörigen Stellen, an denen diese angenommen werden.

Lösungsvorschlag zur Aufgabe (Frühjahr 2017, T3A4)

- a** Sei T eine injektive lineare Abbildung $T: \mathbb{R}^2 \rightarrow \mathbb{R}^2$ und f wie angegeben. Die Voraussetzung, dass T ein Diffeomorphismus ist, ist genau dann erfüllt, wenn die Darstellungsmatrix A von T bezüglich der Standardbasis des \mathbb{R}^2 invertierbar ist, denn dann ist T bijektiv mit differenzierbarer Umkehrung $x \mapsto A^{-1}x$. Ferner ist dann $(DT)(x, y) = A$ sowie $T(\mathbb{R}^2) = \mathbb{R}^2$, aufgrund der Bijektivität. Der allgemeine Transformationssatz 5.9 liefert unter diesen Voraussetzungen

$$\int_{\mathbb{R}^2} (f \circ T)(x) dx = \int_{\mathbb{R}^2} f(x) |\det A|^{-1} dx = \frac{1}{|A|} \int_{\mathbb{R}^2} f(x) dx.$$

- b** Definiere

$$T: \mathbb{R}^2 \rightarrow \mathbb{R}^2, \quad \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \mapsto \begin{pmatrix} x_1 + x_2 \\ 2x_1 + 5x_2 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 2 & 5 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}.$$

Diese Darstellung zeigt, dass T linear ist, und da die Darstellungsmatrix Determinante 3 hat, handelt es sich um eine bijektive Transformation. Mit Teil **a** erhalten wir

$$\int_{\mathbb{R}^2} \frac{1}{1 + (x_1 + x_2)^2(1 + (2x_1 + 5x_2)^2)} dx = \frac{1}{3} \int_{\mathbb{R}^2} \frac{1}{(1 + x_1^2)(1 + x_2^2)} dx.$$

Mit dem Satz von Fubini und unter Verwendung von

$$\int_{-\infty}^{\infty} \frac{1}{1+x^2} dx = [\arctan x]_{-\infty}^{\infty} = 2 \lim_{x \rightarrow \infty} \arctan x = \pi$$

berechnet sich das hintere Integral zu

$$\begin{aligned} \frac{1}{3} \int_{\mathbb{R}} \int_{\mathbb{R}} \frac{1}{(1+x_1^2)(1+x_2^2)} dx_1 dx_2 &= \\ &= \frac{1}{3} \left(\int_{-\infty}^{\infty} \frac{1}{(1+x_2^2)} dx_2 \right) \cdot \left(\int_{-\infty}^{\infty} \frac{1}{(1+x_1^2)} dx_1 \right) = \\ &= \frac{1}{3} \cdot \pi \cdot \pi = \frac{\pi^2}{3}. \end{aligned}$$

Lösungsvorschlag zur Aufgabe (Frühjahr 2017, T3A5)

- a** Sei $x \in]0, 1[$ und $\varepsilon > 0$. Wähle $N \in \mathbb{N}$ so, dass $x^2 N > \frac{1}{\varepsilon}$ ist, dann gilt für $n \geq N$

$$|f_n(x)| = \frac{n}{1+n^2x^2} = \frac{1}{\frac{1}{n}+nx^2} \leq \frac{1}{nx^2} \leq \frac{1}{Nx^2} < \varepsilon.$$

Also konvergiert f_n punktweise gegen 0. Nehmen wir an, f_n konvergiert gleichmäßig gegen 0. Dann gibt es ein $N \in \mathbb{N}$, sodass für alle $n \geq N$ und $x \in]0, 1[$ die Ungleichung $|f_n(x)| < \frac{1}{2}$ erfüllt ist. Betrachte nun aber $\hat{x} = \frac{1}{N}$. Dann gilt für $n \geq N$

$$f_n(\hat{x}) = \frac{n}{1+\frac{n^2}{N^2}} \geq \frac{n}{2} > \frac{1}{2}.$$

- b** Mittels der Substitution $x \mapsto \frac{x}{n}$ erhalten wir

$$\int_0^1 \frac{n}{1+n^2x^2} dx = \int_0^n \frac{1}{1+x^2} dx = [\arctan(x)]_0^n = \arctan(n).$$

Daraus folgt wegen $\lim_{x \rightarrow \infty} \arctan(x) = \frac{\pi}{2}$ die Aussage.

- c** Die gleiche Substitution wie in Teil **b** liefert hier

$$\int_0^1 \frac{nx^\alpha}{1+n^2x^2} dx = \frac{1}{n^\alpha} \int_0^n \frac{x^\alpha}{1+x^2} dx = \frac{1}{n^\alpha} \left(\int_0^1 \frac{x^\alpha}{1+x^2} dx + \int_1^n \frac{x^\alpha}{1+x^2} dx \right).$$

Für alle $x \geq 1$ gilt $x^\alpha \leq x$, deshalb können wir das zweite Integral folgendermaßen abschätzen:

$$\int_1^n \frac{x^\alpha}{1+x^2} dx \leq \int_1^n \frac{x}{1+x^2} dx = \left[\frac{1}{2} \ln(1+x^2) \right]_1^n = \frac{1}{2} \ln(1+n^2) - \frac{1}{2} \ln 2.$$

Das andere auftretende Integral können wir ebenfalls abschätzen:

$$\int_0^1 \frac{x^\alpha}{1+x^2} dx \leq \int_0^1 \frac{1}{1} dx = 1.$$

Insgesamt erhält man daher

$$\lim_{n \rightarrow \infty} \int_0^1 \frac{nx^\alpha}{1+(nx)^2} dx \leq \lim_{n \rightarrow \infty} \frac{1}{n^\alpha} \left(1 - \frac{1}{2} \ln 2 + \frac{1}{2} \ln(1+n^2) \right) = 0,$$

wobei wir verwendet haben, dass aufgrund der Regel von L'Hospital der Grenzwert

$$\lim_{n \rightarrow \infty} \frac{\frac{1}{2} \ln(1+n^2)}{n^\alpha} = \lim_{n \rightarrow \infty} \frac{n}{1+n^2} \cdot \frac{1}{\alpha n^{\alpha-1}} = \lim_{n \rightarrow \infty} \frac{n^{2-\alpha}}{\alpha(1+n^2)} = 0$$

ist.

Literatur

- [Aul04] Bernd Aulbach. *Gewöhnliche Differenzialgleichungen*. 2. Aufl. München, Heidelberg: Spektrum, 2004.
- [Bos09] Siegfried Bosch. *Algebra*. 7. Aufl. Berlin, Heidelberg: Springer, 2009.
- [Bos14] Siegfried Bosch. *Lineare Algebra*. 5. Aufl. Berlin, Heidelberg: Springer, 2014.
- [FB06] Eberhard Freitag und Rolf Busam. *Funktionentheorie*. 4. Aufl. Heidelberg: Springer, 2006.
- [Fur95] Peter Furlan. *Das gelbe Rechenbuch* 3. Dortmund: Furlan, 1995.
- [Ger16] Ralf Gerkmann. *Algebra*. Vorlesungsskript. 2016.
- [Kle07] Israel Kleiner. *A History Of Abstract Algebra*. Boston: Birkhäuser, 2007.
- [Kra14] Martina Kraupner. *Algebra leicht(er) gemacht*. 2. Aufl. Berlin: De Gruyter Oldenbourg, 2014.
- [Lan05] Serge Lang. *Algebra*. Revised Third Edition. corrected printing. New York: Springer, 2005.
- [Zen15] Heribert Zenk. *Gewöhnliche Differenzialgleichungen und Funktionentheorie*. Vorlesungsskript. 2015.

Aufgabenverzeichnis Algebra

Frühjahr 1978	T1A2, 168	T2A1, 48
T5A3, 7	T1A4, 216	T2A2, 245
Frühjahr 2000	T2A1, 57	T2A3, 86
T1A1, 147	T2A2, 191	T3A1, 132
T1A3, 95	T2A3, 208	T3A2, 77
T2A1, 39	T2A5, 134	T3A4, 21
T2A3, 163	Frühjahr 2004	T3A5, 186
T3A2, 20	T1A3, 199	Herbst 2010
T3A3, 167	T2A1, 377	T1A3, 87
Herbst 2000	Herbst 2004	T1A5, 162
T1A1, 52	T2A1, 50	T2A3, 22
T1A2, 163	T3A1, 43	T2A4, 168
T1A3, 211	T3A2, 129	T2A5, 241
T2A3, 213	Frühjahr 2005	T3A1, 16
T3A1, 58	T1A4, 137	T3A2, 4
T3A4, 172	T2A5, 219	T3A5, 212
Frühjahr 2001	T3A3, 115	Frühjahr 2011
T2A2, 36	T3A4, 126	T1A1, 237
T3A1, 165	Herbst 2005	T1A2, 5
T3A2, 40	T3A3, 242	T1A3, 98
Herbst 2001	Frühjahr 2006	T2A1, 111
T1A1, 20	T1A2, 140	T2A2, 142
T2A1, 71	T2A2, 125	T2A3, 232
T2A2, 116	Frühjahr 2007	T2A4, 194
T3A4, 157	T2A3, 144	T3A1, 125
T3A5, 145	T3A5, 155	T3A2, 67
Frühjahr 2002	Frühjahr 2008	Herbst 2011
T2A1, 138	T1A4, 210	T2A4, 189
Herbst 2002	T1A5, 122	T3A1, 68
T1A3, 156	T2A4, 140	T3A5, 139
T3A1, 49	Herbst 2008	Herbst 2012
Frühjahr 2003	T1A2, 23	T1A1, 231
T1A3, 149	T3A3, 41	T1A2, 128
T1A4, 195	Frühjahr 2010	T1A4, 93
T3A1, 54	T1A1, 69	T1A5, 114
T3A2, 206	T1A3, 141	T2A1, 28
Herbst 2003	T1A5, 73	T2A2, 161

T2A3, 169	T3A4, 16	T2A5, 181, 499
T2A4, 200	Frühjahr 2014	T3A1, 101, 499
T2A5, 219	T1A2, 198	T3A2, 499
T3A1, 35	T1A4, 235	T3A3, 238, 499
T3A2, 66	T1A5, 160	T3A4, 202, 499
T3A4, 118	T2A1, 99	Frühjahr 2016
T3A5, 133	T2A3, 11	T1A1, 506
Frühjahr 2012	T2A4, 192	T1A2, 506
T1A1, 19	T3A1, 8	T1A3, 506
T1A2, 73	T3A3, 90	T1A4, 507
T1A3, 94	Herbst 2014	T1A5, 507
T1A4, 117	T1A1, 200	T2A1, 507
T2A2, 5	T1A2, 80	T2A2, 508
T2A3, 83	T1A3, 151	T2A3, 508
T3A1, 243	T1A5, 112	T2A4, 508
T3A2, 182	T2A1, 106	T2A5, 509
T3A3, 99	T2A5, 247	T3A1, 509
T3A4, 90	T3A2, 120	T3A2, 509
T3A5, 205	T3A4, 84	T3A3, 510
Frühjahr 2013	Frühjahr 2015	T3A4, 510
T1A1, 127	T1A1, 246, 492	T3A5, 510
T1A2, 173	T1A2, 98, 492	Herbst 2016
T1A3, 229	T1A3, 59, 492	T1A1, 525
T1A5, 29	T1A4, 104, 493	T1A2, 525
T2A1, 10	T1A5, 179, 493	T1A3, 525
T2A2, 227	T2A1, 100, 493	T1A4, 525
T2A4, 215	T2A2, 493	T1A5, 525
T2A5, 199	T2A3, 145, 493	T2A1, 526
T3A1, 35	T2A4, 25, 494	T2A2, 526
T3A3, 77	T2A5, 207, 494	T2A3, 526
T3A4, 136	T3A1, 2, 494	T2A4, 527
T3A5, 171	T3A2, 61, 494	T2A5, 527
Herbst 2013	T3A3, 76, 494	T3A1, 527
T1A2, 45	T3A4, 152, 495	T3A2, 528
T1A3, 248	T3A5, 196, 495	T3A3, 528
T1A4, 107	Herbst 2015	T3A4, 528
T1A5, 191	T1A1, 102, 497	T3A5, 528
T2A1, 209	T1A2, 226, 497	Frühjahr 2017
T2A2, 17	T1A3, 47, 497	T1A1, 541
T2A3, 197	T1A4, 497	T1A2, 541
T2A4, 121	T1A5, 498	T1A3, 541
T2A5, 65	T2A1, 498	T1A4, 542
T3A1, 184	T2A2, 64, 498	T1A5, 542
T3A2, 221	T2A3, 498	T2A1, 542
T3A3, 63	T2A4, 152, 498	T2A2, 542

T2A3, 543
T2A4, 543
T2A5, 543

T3A1, 543
T3A2, 543
T3A3, 544

T3A4, 544
T3A5, 544

Aufgabenverzeichnis Analysis

Frühjahr 2001	T2A1, 287	T3A4, 448
T3A1, 309	T2A2, 334	Frühjahr 2011
T3A2, 318	T2A3, 379	T2A2, 319
Herbst 2001	T2A5, 427	T2A3, 356
T2A1, 447	Herbst 2007	T2A4, 399
T3A1, 273	T2A2, 314	T3A1, 435
T3A2, 381	T3A1, 325	T3A4, 314
Frühjahr 2002	Frühjahr 2008	T3A5, 259
T2A1, 271	T2A2, 451	Herbst 2011
Frühjahr 2003	T2A5, 285	T1A3, 368
T1A5, 374	Herbst 2008	T1A4, 441
T2A3, 348	T1A1, 297	T1A5, 487
Herbst 2003	T1A4, 405	T2A1, 275
T1A3, 349, 429	T3A3, 465	T2A2, 308
T2A1, 359	T3A4, 281	T2A5, 484
T3A1, 304	Frühjahr 2009	T3A1, 461
Frühjahr 2004	T1A1, 373	T3A2, 307
T1A1, 338	T1A3, 388	Frühjahr 2012
T1A2, 301	T2A2, 479	T1A2, 321
T1A4, 408	T2A5, 299	T1A4, 483
T3A5, 467	T3A2, 452	T1A5, 420
Herbst 2004	T3A3, 469	T2A1, 362
T2A2, 284	Frühjahr 2010	T2A2, 324
T2A3, 457	T1A4, 274	T2A3, 267
Frühjahr 2005	T2A1, 322	T2A4, 421
T1A2, 464	T2A5, 472	T3A1, 329
T1A3, 432	T3A3, 268	T3A5, 431
Herbst 2005	Herbst 2010	Herbst 2012
T2A1, 280	T1A1, 253	T1A1, 319
Frühjahr 2006	T1A3, 385	T1A2, 440
T1A4, 471	T1A4, 347	T1A4, 366
T2A1, 384	T1A5, 305	T2A2, 316
Herbst 2006	T2A1, 386	T3A1, 459
T3A1, 371	T2A3, 292, 463	T3A2, 417
T3A2, 310	T2A5, 454	T3A5, 293
Frühjahr 2007	T3A2, 313	Frühjahr 2013
T1A4, 295	T3A3, 423	T1A2, 365

T1A3, 344	T2A1, 561	T3A1, 600
T2A1, 276	T2A2, 562	T3A2, 601
T2A2, 330	T2A3, 562	T3A3, 601
T2A4, 460	T2A4, 412, 563	T3A4, 601
T2A5, 409	T2A5, 482, 563	T3A5, 602
Herbst 2013	T3A1, 394, 563	Herbst 2016
T1A1, 317	T3A2, 563	T1A1, 623
T1A2, 337	T3A3, 367, 564	T1A2, 623
T1A3, 257	T3A4, 564	T1A3, 623
T2A2, 354	T3A5, 564	T1A4, 623
T2A3, 265	Herbst 2015	T1A5, 624
T2A4, 393	T1A1, 578	T2A1, 624
T3A1, 392	T1A2, 578	T2A2, 625
T3A3, 352	T1A3, 578	T2A3, 625
Frühjahr 2014	T1A4, 438, 579	T2A4, 626
T1A1, 488	T1A5, 579	T2A5, 626
T1A2, 480	T2A1, 261, 580	T3A1, 627
T2A1, 424	T2A2, 457, 580	T3A2, 627
T2A2, 443	T2A3, 413, 580	T3A3, 627
T2A3, 334	T2A4, 581	T3A4, 627
T2A5, 370	T2A5, 581	T3A5, 628
T3A1, 260	T3A1, 582	Frühjahr 2017
T3A3, 341	T3A2, 582	T1A1, 647
Herbst 2014	T3A3, 582	T1A2, 647
T1A1, 302	T3A4, 583	T1A3, 647
T1A2, 288	T3A5, 264, 583	T1A4, 648
T2A2, 336	Frühjahr 2016	T1A5, 648
T2A3, 361	T1A1, 597	T2A1, 648
T2A4, 477	T1A2, 597	T2A2, 649
T3A2, 278	T1A3, 598	T2A3, 649
T3A5, 312	T1A4, 598	T2A4, 650
Frühjahr 2015	T1A5, 598	T2A5, 650
T1A1, 363, 560	T2A1, 599	T3A1, 650
T1A2, 560	T2A2, 599	T3A2, 650
T1A3, 560	T2A3, 599	T3A3, 651
T1A4, 401, 561	T2A4, 600	T3A4, 651
T1A5, 561	T2A5, 600	T3A5, 651

Index Algebra

- abelsche Normalreihe, 55
- ähnlich, 234
- algebraisch, 149
- algebraischer Abschluss, 154
- Alternierende Gruppe, 63
- assoziiert, 94
- auflösbare Gruppe, 55
- Bahn, 15
- Bahnengleichung, 15
- Basis, 224
- Cayley, Satz von, 62
- Cayley-Hamilton, 241
- charakteristisches Polynom, 235
- Chinesischer Restsatz, 106
- Darstellungsmatrix, 225
- diagonalisierbar, 236
- Diedergruppe, 70
- Dimension, 224
- direktes Produkt, 31
- effektive Gruppenoperation, 28
- Eigenraum, 234
- Eigenvektor, 234
- Eigenwert, 234
- einfache Erweiterung, 150
- einfache Gruppe, 40
- Einheit, 75
- Einheitswurzel, 166
- Eisenstein-Kriterium, 132
- Elementarteilersatz, 13
- Euklidischer Algorithmus, 103
- Euler'sche φ -Funktion, 4
- Euler-Krtierium, 123
- Faktorgruppe, 9
- faktorieller Ring, 90
- Faktorring, 97
- Fixpunkt, 15
- formale Ableitung eines Polynoms, 159
- Fortsetzungssatz, 165
- freshman's dream, 206
- Frobenius-Homomorphismus, 206, 215
- Gauß, Lemma von, 131
- Gradformel, 149
- Gruppe, 2
- Gruppenhomomorphismus, 2
- Gruppenoperation, 14
- Höhenfunktion, 90
- Hauptideal, 79
- Hauptidealring, 90
- Hauptsatz über endlich erzeugte abelsche Gruppen, 13
- Homomorphiesatz
 - für Ringe, 104
 - von Gruppen, 10
- Ideal, 79
- idempotent, 76, 106
- Index, 8
- Integritätsbereich, 76
- irreduzibel, 78
 - Polynom, 130
- Isomorphiesätze, 10
- Isotropiegruppe, *siehe* Stabilisator
- Jordan-Normalform, 240
- K-Homomorphismus, 165
- Kern, 2

- Klassengleichung, 19
 Klein'sche Vierergruppe, 71
 kleiner Satz von Fermat, 3
 Komplexprodukt, 30
 Kompositum von Körpern, 178
 Konjugation, 18
 konstruierbar, 218
 koprim, 106
 Körper, 76
 Körpererweiterung, 149
 Körpererweiterungsgrad, 149
 Korrespondenzsatz für Ringe, 105
 Kreisteilungskörper, 167
 Kreisteilungspolynom, 167

 Lagrange, 8
 Legendre-Symbol, 123
 Lemma von Bézout, 108
 linear unabhängig, 224
 lineare Abbildung, 224

 Minimalpolynom
 eines Körperelements, 150
 von Matrizen, 241

 Nebenklasse, 7
 normal, 158
 Normalisator, 40
 Normalteiler, 8
 Nullteiler, 75

 Ordnung, 3
 Orthogonalprojektion, 511

 perfekter Körper, 160
 Permutationsgruppe, 62
 Primelement, 78
 Primideal, 80
 primitives Polynom, 131
 primitives Element, 196
 Satz vom, 163
 Primkörper, 208
 p -Untergruppe, 38

 Quadrat, 120
 Quadratischer Rest, 123
 Quadratisches Reziprozitätsgesetz,
 124
 Quaternionengruppe, 8, 71

 Reduktionskriterium, 132
 Restklassenring, 97
 Ring, 75

 semidirektes Produkt, 31
 separabel, 159
 Signumshomomorphismus, 63
 Stabilisator, 15
 Sylowgruppe, 38
 Sylowsätze, 38
 Symmetrische Gruppe, 62

 Teilring, 75
 Träger einer Permutation, 62
 transitive Gruppenoperation, 15
 transzendent, 149

 Untergruppe, 2
 Unterring, *siehe* Teilring

 Vektorraum, 224
 direkte Summe, 226
 Vielfachheit
 algebraische, 237
 geometrische, 237
 vollkommener Körper, 160

 wohldefiniert, 8

 Zentralisator, 19, 20
 Zentrum, 19
 Zerfällungskörper, 155
 Zerlegungstyp, 63
 Zwischenkörper, 149
 zyklisch, 3
 zyklotomischer Körper, 167

Index Analysis

- absolute Konvergenz, 279
- analytisch, *siehe* holomorph
- asymptotische Stabilität von Lösungen, 475
- Attraktivität von Lösungen, 475
- Banach'scher Fixpunktsatz, 409
- biholomorph, 370
- Casorati-Weierstaß, 297
- Cauchy-Hadamard, 280
- Cauchy-Integralformel, 328
- Cauchy-Integralsatz, 327
- Cauchy-Riemannsche Differentialgleichungen, 271
- charakteristisches Polynom einer Differentialgleichung, 450
- definit, 259
- Differenzierbarkeit, 252
- diskret, 301
- Doppelverhältnis, 381
- einfach zusammenhängend, 327
- Erhaltungsgröße, 463
- Erstes Integral, 463
- Euler'scher Multiplikator, *siehe* Integrierender Faktor
- Exakte Differentialgleichungen, 396
- Existenz- und Eindeutigkeitssatz bei linear beschränkter rechter Seite, 422
- Extremstellen, 258
- Extremum, Unter Nebenbedingung, 264
- Fundamentalmatrix, 426
- Fundamentalsystem, 426
- Ganze Funktion, 311
- Gebiet, 300
- Gebietstreue, 314
- geometrische Reihe, 279
- Globaler Existenz- und Eindeutigkeitssatz, 416
- Gradient, 256
- Häufungspunkt, 300
- harmonisch, 273
- Hauptteil, 290
- Hesse-Matrix, 257
- holomorph, 271
- holomorphe Fortsetzung, 296
- homogene Differentialgleichung, 404
- Identitätssatz, 300
- inhomogen, 425
- Integrabilitätsbedingung, 396
- Integrierender Faktor, 398
- komplexe Differenzierbarkeit, 271
- konform, *siehe* biholomorph
- Konvergenzkreisscheibe, 280
- Konvergenzradius, 280
- Kreistreue, 373
- Kurve, 326
- Lagrange-Multiplikator, 264
- Laplace'scher Differentialoperator, 273
- Laurentreihe, 291
- Lipschitz-Stetigkeit, 407
- Lyapunov-Funktion, 486

- Möbius-Transformation, 373
- Fixpunkte, 381
- Matrix-Exponential, 433
- Maximumprinzip, 317
- Minimumprinzip, 317
- Nebenteil, 290
- nicht-diskret, *siehe* diskret
- nullhomolog, 333
- partielle Ableitung, 256
- partikuläre Lösung, 450
- Phasenportrait, 445
- Picard-Iteration, 409
- Polstelle, 296
- Potenzreihe, 279
- reelle Differenzierbarkeit, 270
- Residuensatz, 333
- Residuum, 331
 - im Punkt ∞ , 349
- Richtungsableitung, 255
- Riemannsche Zahlenkugel, 372
- Riemannscher Abbildungssatz, 370
- Riemannscher Hebbareitssatz, 296
- Satz von
 - der Gebietstreue, 314
 - Fubini, 268
 - Liouville, 311
 - Peano, 406
 - Picard (kleiner), 312
 - Picard-Lindelöf, 408
 - Rouché, 358
 - Schwarz, 256
- Singularität, 296
- Stabilität von Lösungen, 475
 - direkte Methode von Lyapunov, 487
- Eigenwertbedingung, 479
- lineare Systeme, 476
- Linearisierung, 482
- Stetigkeit, 252
- Superpositionsprinzip, 425
- Taylor-Entwicklung, 283
- totale Differenzierbarkeit, 256
- Trajektorie, 445
- Transformationssatz, 268
- Trennen der Variablen, 392
- Übergangsmatrix, 434
- Umlaufzahl, *siehe* Windungszahl
- Untermannigfaltigkeit, 263
- Variablentransformation, 404
- Variation der Konstanten
 - für Differentialgleichungen höherer Ordnung, 455
 - für Lineare Systeme, 435
 - für skalaren Fall, 403
- verallgemeinerte Kreislinie, 373
- Weierstraß'sches
 - Majorantenkriterium, 287
- Windungszahl, 327
- Wronski-Determinante, 426
- Wronski-Matrix bei DGL höherer Ordnung, 455