Zahlenbereiche – Algebra für Lehramtsstudierende

Jakob Scholbach

10. Februar 2021

Inhaltsverzeichnis

Kapitel 0

Vorbemerkung

Dies sind im Entstehen begriffene Vorlesungsnotizen einer Vorlesung für Lehramtsstudierende an der Universität Münster. Grundlegende Vorkenntnisse aus der Linearen Algebra und in geringerem Maße auch aus der Analysis, wie sie jeweils im ersten und zweiten Semester erworben werden, sind für das Verständnis des Stoffes hier notwendig.

- Das Ausrufezeichen-Symbol (!) weist auf Punkte hin, die im Nacharbeiten der Vorlesung beachtet werden können und sollten; oft sind dort einige kleinere Aspekte eines Begriffs zu wiederholen.
- Die drei Punkte am Rand stehen für Inhalte, die in der Vorlesung erklärt werden.
- Das Videozeichen am Rand verweist auf die Videoaufzeichnungen der Vorlesung. 04.11.20

Kapitel 1

Einleitung

Die reellen Zahlen $\mathbf{R}$ bilden einen Zahlenbereich, der uns aus anschaulich und aus dem Gebrauch in den verschiedensten Gebieten innerhalb und außerhalb der Mathematik gut vertraut ist. Aus der Analysis-Vorlesung ist uns bekannt, dass die reellen Zahlen folgende Eigenschaften haben: 04.11.20

- Sie bilden einen Körper, d.h. reelle Zahlen können addiert und multipliziert werden, und diese beiden Operationen erfüllen die Körperaxiome, die das Rechnen mit reellen Zahlen leicht machen. Beispielsweise gilt
$$ab = ba \tag{1.1}$$
für zwei reelle Zahlen a und b.
- Sie lassen sich anordnen, d.h. es gibt eine "$\leqslant$"-Relation, die in sinnvoller Weise mit der Addition und Multiplikation harmoniert.
- Sie sind (z.B. im Gegensatz zu den rationalen Zahlen $\mathbf{Q}$) vollständig, d.h. jede nach unten beschränkte nicht-leere Teilmenge $M \subset \mathbf{R}$ hat ein Infimum. [1]

Alle grundlegenden Sätze der Analysis lassen sich allein mit Hilfe dieser Eigenschaften beweisen. Beispielsweise die Tatsache, dass jedes Polynom *ungeraden Grades*, z.B.
$$t^7 + 3t^6 - 12t + 1$$
(wenigstens) eine reelle Nullstelle hat.

Nach den reellen Zahlen sind die komplexen Zahlen
$$\mathbf{C} = \{a + ib, \text{ mit } a, b \in \mathbf{R}\}$$
das nächstgrößere Zahlensystem. Die komplexen Zahlen haben Anwendungen natürlich innerhalb der Mathematik, aber auch der Physik (z.B. der Wechselstromrechnung) und auch der Chemie (bei der Untersuchung von Symmetrien von Molekülen). Was zeichnet die komplexen Zahlen aus?

- Sie sind ebenfalls ein Körper.
- Sie enthalten die reellen Zahlen, sind aber nicht wesentlich größer als diese (d.h. endlich-dimensional als $\mathbf{R}$-Vektorraum).
- *Jedes* komplexe Polynom, z.B.
$$t^4 - it^3 + 3t^2 + 4$$
hat (wenigstens) eine komplexe Nullstelle. Man sagt hierzu: $\mathbf{C}$ *ist algebraisch abgeschlossen.*

[1] M heißt hierbei nach unten *beschränkt*, wenn es ein $x \in \mathbf{R}$ gibt mit $x \leqslant m$ für alle $m \in M$. Ein solches x heißt auch *untere Schranke* von M. Man sagt, M hat ein *Infimum*, wenn es ein $m \in \mathbf{R}$ gibt mit der Eigenschaft dass alle unteren Schranken x von M die Bedingung $x \leqslant m$ erfüllen.

Der letzte Punkt ist der sog. *Fundamentalsatz der Algebra* (Theorem 2.6). Diese Eigenschaft unterscheidet $\mathbf{R}$, wo bekanntlich das Polynom $t^2 + 1$ keine Nullstelle hat, von $\mathbf{C}$. Wir werden dies nutzen, um zu zeigen, dass die komplexen Zahlen i.W. den einzigen Zahlenbereich bilden, der diese drei Eigenschaften hat.

Was kommt nun? Um neue, größere Zahlenbereiche zu erhalten, müssen wir nach der obigen Charakterisierung wenigstens eine der Forderungen fallen lassen. In dieser Vorlesung werden wir nur Zahlenbereiche studieren, die nicht wesentlich größer als $\mathbf{R}$ sind, d.h. deren $\mathbf{R}$-Dimension nach wie vor endlich ist. Die *Quaternionen* $\mathbf{H}$ sind ein solcher Zahlenbereich. Ihre Elemente haben die Form

$$a + ib + jc + kd,$$

wobei $a, b, c, d \in \mathbf{R}$ und i, j, k drei Pendants der imaginären Einheit (in $\mathbf{C}$) sind. Die Kommutativität der Multiplikation (1.1) gilt in $\mathbf{H}$ *nicht* mehr: beispielsweise ist

$$ij = k,$$

jedoch

$$ji = -k.$$

Dennoch sind die Quaternionen ein sinnvolles Zahlensystem, welches wir nach den komplexen Zahlen kennenlernen werden (§3). Sie werden z.B. in der Berechnung von räumlichen Darstellungen in der Computer-Grafik eingesetzt, spielen aber auch in verschiedenen Bereichen der Mathematik, z.B. den sog. Shimura-Varietäten eine grundlegende Rolle. Auch die Quaternionen lassen sich axiomatisch charakterisieren (Theorem 3.30).

Als Schlusspunkt unserer Erkundungen werden wir die Oktonionen $\mathbf{O}$ kennenlernen. Der Name rührt daher, dass sie als $\mathbf{R}$-Vektorraum 8-dimensional sind. Ein kleiner Vorgeschmack, was uns erwartet gibt das folgende Zitat von Baez [Bae02]:

> "Die reellen Zahlen $\mathbf{R}$ sind der verlässliche Ernährer der Familie, der vollständige angeordnete Körper, auf den wir uns verlassen. Die komplexen Zahlen $\mathbf{C}$ sind der etwas schrillere, aber respektierte kleinere Bruder: nicht angeordnet, aber algebraisch abgeschlossen. Die Quaternionen $\mathbf{H}$ sind, da sie nicht kommutativ sind, der exzentrische Cousin, der bei Familienfeiern gern gemieden wird. Die Oktonionen $\mathbf{O}$ jedoch sind der verrückte alte Onkel, den niemand vom Dachboden herunter lässt: sie sind nicht assoziativ."

Dieser verrückte alte Onkel hat jedoch bei allerhand interessanten mathematischen Strukturen seine Hände im Spiel, daher lohnt es sich, ihn doch einmal vom Dachboden zu bitten!

Kapitel 2

Die komplexen Zahlen

Nach den reellen Zahlen sind die komplexen Zahlen der "nächstgrößere" Zahlenbereich. Wir wiederholen kurz die grundlegenden Eigenschaften der komplexen Zahlen und beweisen anschließend den Fundamentalsatz der Algebra (Theorem 2.6). Nachdem wir uns einiges grundlegendes algebraisches Handwerkszeug verschafft haben, beweisen wir anschließend dass die reellen und die komplexen Zahlen die einzigen Zahlenbereiche sind, die folgende Anforderungen erfüllen (Theorem 2.27):

- Sie enthalten die reellen Zahlen.
- Sie sind ein Körper.
- Sie sind nicht "zu groß", d.h. jede Zahl lässt sich als endliche $\mathbf{R}$-Linearkombination darstellen.

2.1 Grundlegende Eigenschaften

Definition 2.1. Die *komplexen Zahlen* $\mathbf{C}$ sind die Menge

$$\mathbf{C} = \{(a, b), \text{ mit } a, b \in \mathbf{R}\}.$$

Die Addition und Multiplikation komplexer Zahlen sind definiert durch

$$\begin{aligned}(a_1, b_1) + (a_2, b_2) &:= (a_1 + a_2, b_1 + b_2)\\ (a_1, b_1) \cdot (a_2, b_2) &:= (a_1 a_2 - b_1 b_2, a_1 b_2 + a_2 b_1).\end{aligned}$$

Wir schreiben ein solches Paar in aller Regel als

$$a + ib := (a, b).$$

In dieser Schreibweise gilt also

$$(a_1 + ib_1)(a_2 + ib_2) = (a_1 a_2 - b_1 b_2) + i(a_1 b_2 + a_2 b_1).$$

Insbesondere gilt also die fundamentale Gleichung

$$i^2 (:= ii) = -1.$$

Wir fassen die reellen Zahlen $\mathbf{R}$ als die Teilmenge $\{(a, 0), a \in \mathbf{R}\} = \{a + i0\} \subset \mathbf{C}$ auf. Der *Realteil* bzw. *Imaginärteil* ist definiert als

$$\Re(a + ib) := a, \Im(a + ib) := b.$$

Aus der Grundvorlesung ist bekannt, der elementare Beweis ist eine gute Wiederholung der Körperaxiome.

Satz 2.2. Die komplexen Zahlen bilden einen Körper.

In Richtung der geometrischen Eigenschaften von $\mathbf{C}$ benutzen wir die folgenden Standardbegriffe:

Definition 2.3. Die *komplexe Konjugation* ist die Abbildung

$$\overline{?} : \mathbf{C} \to \mathbf{C}, z = a + ib \mapsto \overline{z} := a - ib.$$

Der *Betrag* ist die Abbildung

$$|?| : \mathbf{C} \to \mathbf{R}^{\geqslant 0}, z = a + ib \mapsto |z| := \sqrt{z\overline{z}} = \sqrt{a^2 + b^2}.$$

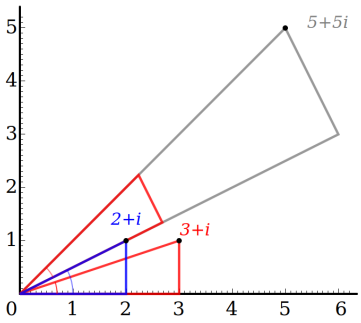
Aus der Grundvorlesung bekannt ist folgende geometrische Beschreibung der Addition und Multiplikation:

- Die Addition ist die übliche Vektoraddition im $\mathbf{R}^2$.
- Die Multiplikation erfüllt folgende Eigenschaften (und ist durch diese eindeutig bestimmt): es gilt für $z_1, z_2 \in \mathbf{C}$

  $$|z_1 z_2| = |z_1||z_2|.$$

  Seien $z_1, z_2 \in \mathbf{C}$ mit $|z_1| = |z_2| = 1$. Bezeichne mit φ_i den Winkel zwischen der positiven x-Achse und dem Strahl der vom Ursprung ausgeht und durch z_i verläuft. Sei $\varphi := \varphi_1 + \varphi_2$. Dann ist $z_1 z_2$ der eindeutige Schnittpunkt des Einheitskreises $S^1 := \{z \in \mathbf{C}, |z| = 1\}$ mit dem Strahl der mit der positiven x-Achse den Winkel φ bildet.

  Die folgende Illustration stammt von Wikimedia[1]



2.2 Der Fundamentalsatz der Algebra

Bekanntermaßen hat nicht jedes reelle Polynom eine reelle Nullstelle. Zum Beispiel hat

$$f(t) = t^2 + 1$$

keine reelle Nullstelle, denn $f(x)$ ist für alle reellen Zahlen x positiv. Fragen wir nach Nullstellen innerhalb der komplexen Zahlen, so ändert sich das: dieses Polynom hat genau zwei komplexe Nullstellen, nämlich i und $-i$. Der Fundamentalsatz der Algebra besagt eine wesentlich stärkere Aussage, nämlich dass nicht nur dieses Polynom, sondern sogar jedes nicht-konstante reelle Polynom und sogar, noch allgemeiner, jedes nicht-konstante komplexe Polynom, eine komplexe Nullstelle hat. Dies ist insofern bemerkenswert, als der Übergang von $\mathbf{R}$ zu $\mathbf{C}$ ja darin besteht, dass zu $\mathbf{R}$ eine "neue" Zahl i hinzugefügt wird mit der Eigenschaft $i^2 = -1$. Wenn wir nur i hinzufügen, d.h. die Menge $\mathbf{R} \sqcup \{i\}$ betrachten, bildet dies natürlich(!) keinen Körper. Wir können den Körper $\mathbf{C}$ als den kleinsten Körper auffassen, der $\mathbf{R}$ und i enthält. (Eine genaue Präzisierung des Wortes "kleinsten" in dieser Aussage ist möglich, doch wir belassen es hier bei dieser eher informellen Feststellung.)

[1] By IkamusumeFan - Own work, CC BY-SA 4.0, https://commons.wikimedia.org/w/index.php?curid=42024950.

Definition 2.4. Sei K ein Körper und

$$f(t) = a_0 + a_1 t + \cdots + a_n t^n = \sum_{k=0}^{n} a_k t^k$$

ein *Polynom*. Wir bezeichnen dann mit $\deg f$ (*Grad* von f) die größte Zahl n derart, dass $a_n \neq 0$ ist. Die a_k heißen *Koeffizienten*, der Koeffizient a_n heißt *Leitkoeffizient* von f. Das Polynom f heißt *normiert*, falls $a_n = 1$ ist.

Die Menge der Polynome mit Koeffizienten in K wird mit $K[t]$ bezeichnet. (Grundlegende Eigenschaften der Addition und Multiplikation von Polynomen werden in Übungsaufgabe 2.2 studiert.)

Bemerkung 2.5. Wir betrachten oft nur normierte Polynome, um den Leitkoeffizienten nicht immer separat beachten zu müssen. Dies ist keine wesentliche Einschränkung, denn

$$f(t) = a_n \left(\sum_{k=0}^{n} \frac{a_k}{a_n} t^k \right),$$

und innerhalb der Klammern steht ein normiertes Polynom. Die Nullstellen (wofür wir uns im folgenden besonders interessieren) dieses Polynoms sind(!) die gleichen wie die Nullstellen von f.

Theorem 2.6. (*Fundamentalsatz der Algebra*) Jedes Polynom Bo 11.11.20

$$f(t) = a_0 + a_1 t + \cdots + a_n t^n$$

mit Grad $\deg f \geqslant 1$ mit komplexen Koeffizienten (d.h. $a_k \in \mathbf{C}$) hat eine komplexe Nullstelle, d.h. es gibt ein $z \in \mathbf{C}$ mit

$$f(z) = 0.$$

Dieser Satz wurde erstmals von C.F. Gauss bewiesen. Der folgende, vollständig elementare Beweis stammt von de Oliveira [Oli11].

Beweis. Die Dreiecksungleichung $|z| \geqslant |z + w| - |w|$ (!) für zwei beliebige komplexe Zahlen z, w liefert

$$|f(z)| \geqslant |a_n||z|^n - \sum_{k=0}^{n-1} |a_k||z|^k.$$

Da $a_n \neq 0$ folgt hieraus $|f(z)| \to \infty$ für $|z| \to \infty$. Da die Funktion $z \mapsto |f(z)|$ stetig ist, gibt es folglich ein $z_0 \in \mathbf{C}$ derart dass

$$|f(z)| \geqslant |f(z_0)|$$

für alle $z \in \mathbf{C}$. (Betrachte $z_1 \in \mathbf{C}$ beliebig. Wähle $R > 0$ so, dass $|f(z)| > |f(z_1)|$ für alle z mit $|z| > R$. Die Abbildung $f|_{\{z \in \mathbf{C}, |z| \leqslant R\}}$ ist eine stetige Funktion auf einer kompakten Teilmenge von $\mathbf{R}^2$. Nach dem Satz von Bolzano–Weierstraß nimmt diese Funktion daher ihr Minimum in einem z_0 an. Es gilt $|z_1| \leqslant R$, d.h. $|f(z_0)| \leqslant |f(z_1)|$. Damit ist auch $|f(z_0)| \leqslant |f(z)|$ für alle $z \in \mathbf{C}$.)

Wir können (indem wir $f(z)$ durch $f(z - z_0)$ ersetzen) $z_0 = 0$ annehmen. Also folgt

$$|f(z)|^2 - |f(0)|^2 \geqslant 0 \tag{2.7}$$

für alle $z \in \mathbf{C}$. Außerdem gilt $f(z) = f(0) + z^k g(z)$ für ein $k \in \{1, \ldots, n\}$ und ein Polynom g mit $g(0) \neq 0$. Wir setzen in der Ungleichung (2.7) $z = r\zeta$ mit $r \in \mathbf{R}^{\geqslant 0}$ und $\zeta \in \mathbf{C}$ ein und erhalten (beachte $|w|^2 = w\overline{w}$ für $w \in \mathbf{C}$):

$$2r^k \Re(\overline{f(0)} \zeta^k g(r\zeta)) + r^{2k} |\zeta^k g(r\zeta)|^2 \geqslant 0.$$

Für alle $r > 0$ (und alle $\zeta \in \mathbf{C}$) erhalten wir nach Division durch r^k:

$$2\Re(\overline{f(0)} \zeta^k g(r\zeta)) + r^k |\zeta^k g(r\zeta)|^2 \geqslant 0.$$

Die linke Seite ist (für fixiertes ζ) eine stetige Funktion in r, durch Bilden von $\lim_{r\searrow 0}$ erhalten wir für alle $\zeta \in \mathbf{C}$

$$2\Re(\overline{f(0)}g(0)\zeta^k) \geqslant 0. \tag{2.8}$$

Setze $\alpha := 2\overline{f(0)}g(0)$.Wir erhalten also

$$\Re(\alpha\zeta^k) \geqslant 0$$

für alle $\zeta \in \mathbf{C}$.

Bezeichne, wie üblich, $S^1 := \{z \in \mathbf{C}, |z| = 1\}$ den Einheitskreis. Wir verwenden nun, dass die Abbildung

$$S^1 \to S^1, \zeta \mapsto \zeta^k$$

surjektiv ist (Übungsaufgabe 2.1; der Originalbeweis von Oliveira vermeidet dieses Argument zugunsten eines elementareren, aber eher ad-hoc mäßigen Argument). Es gilt also $\{\alpha\zeta^k | \zeta \in S^1\} = \alpha \cdot S^1 = \{s \in \mathbf{C}, |s| = |\alpha|\}$, d.h. der um den Faktor $|\alpha|$ gestreckte (bzw. gestauchte) Einheitskreis. Falls $|\alpha| \neq 0$, so haben nicht alle Punkte s auf diesem Kreis die Eigenschaft $\Re(s) \geqslant 0$. Also ist $|\alpha| = 0$, d.h. $\alpha = 0$, d.h. (wegen $g(0) \neq 0$) folgt $f(0) = 0$. □

Folgerung 2.9. Jedes komplexe *normierte* Polynom $f(t)$ mit $\deg f = n$ zerfällt als Produkt von n *linearen* 18.11.20 Polynomen, d.h. es gibt $z_1, \ldots, z_n \in \mathbf{C}$ mit der Eigenschaft dass folgendes gilt:

$$f(t) = (t - z_1)(t - z_2) \cdot \cdots \cdot (t - z_n).$$

Diese Zerlegung in Linearfaktoren ist bis auf die Reihenfolge eindeutig, d.h. für eine ähnliche Zerlegung

$$f(t) = (t - z_1')(t - z_2') \cdot \cdots \cdot (t - z_n')$$

gibt es eine Bijektion $\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\}$ mit $z_k = z'_{\sigma(k)}$ für alle k.

Bemerkung 2.10.

- Die z_k sind gerade die Nullstellen von f: für $z \in \mathbf{C}$ gilt $f(z) = \prod(z - z_k)$. Dies ist 0 genau dann, wenn (wenigstens) einer der Faktoren 0 ist (Übungsaufgabe 2.14).
- Es ist möglich, dass ein oder mehrere z_k mehrfach auftauchen, zum Beispiel für

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

  können wir $z_1 = z_2 = 1$, $z_3 = -2$ wählen.
- Aufgrund der obigen Zerlegung in Faktoren bezeichnet man das Finden der Nullstellen eines Polynoms gelegentlich auch als *Faktorisierung* des Polynoms.

Beweis. Wir zeigen folgende Behauptung: ist $g(t)$ ein Polynom vom Grad n (mit komplexen Koeffizienten) und $z \in \mathbf{C}$ eine Nullstelle, d.h. $g(z) = 0$, so gibt es ein Polynom $h(t)$ vom Grad $n - 1$ derart, dass

$$g(t) = (t - z)h(t)$$

gilt. Dieses Argument wenden wir n mal an, wobei wir jedes Mal Theorem 2.6 benutzen, um sicherzustellen dass die Polynome (angefangen mit f selbst) jeweils eine Nullstelle haben.

Diese *Polynomdivision* ist elementare Algebra, wir beweisen sie per Induktion über den Grad von g. Falls $\deg g = 1$, d.h. $g(t) = a_1 t + a_0$ so erhalten wir aus $g(z) = a_1 z + a_0 = 0$:

$$g(t) = (t - z)\frac{a_1}{a_0}$$

falls $a_0 \neq 0$. Falls $a_0 = 0$ und damit auch $z = 0$, so erhalten wir $g(t) = (t - 0)a_1$.

Für den Induktionsschritt sei $g(t) = a_0 + a_1 t + \cdots + a_n t^n$. Dann ist

$$g_1(t) := g(t) - (t - z)a_n t^{n-1}$$

ein Polynom vom Grad $\leqslant n-1$, da der t^n-Term sich aufhebt. Außerdem ist $g_1(z) = g(z) - 0 = 0$, d.h. z ebenfalls Nullstelle von g_1. Damit gibt es laut Induktionsvoraussetzung ein Polynom $h_1(t)$ vom Grad $\leqslant n-2$ derart, dass $g_1(z) = (t-z)h_1(t)$. Es ergibt sich die Induktionsbehauptung:

$$g(t) = g_1(t) + (t-z)a_n t^{n-1} = (t-z)\left(h_1(t) + a_n t^{n-1}\right).$$

Um die Eindeutigkeit (bis auf Permutation) einzusehen: für

$$\prod_{k=1}^{n}(t-z_k) = \prod_{k=1}^{n}(t-z'_k)$$

ist z_1 eine Nullstelle des Polynoms auf der rechten Seite, d.h. $z_1 = z'_r$ für ein geeignetes r. Es gilt dann

$$(t-z_1)\left(\prod_{k\neq 1}(t-z_k) - \prod_{k\neq r}(t-z'_k)\right) = 0.$$

Aus Übungsaufgabe 2.5 folgt $g(t) := \prod_{k\neq 1}(t-z_k) = \prod_{k\neq r}(t-z'_k)$. Wir wenden dieses Argument auf $g(t)$ an (beachte $\deg g = n-1$) und erhalten die Behauptung per Induktion über n. □

Theorem 2.11. Sei $K \supset \mathbf{C}$ ein Körper, derart dass

$$\dim_{\mathbf{C}} K < \infty.$$

Dann ist $K = \mathbf{C}$.

Beweis. Bezeichne $n := \dim_{\mathbf{C}} K$ (nach Voraussetzung ist dies eine natürliche Zahl). Sei $x \in K$. Wir werden zeigen, dass $x \in \mathbf{C}$ liegt.

Die Elemente

$$1 = x^0, x, x^2, x^3, \ldots, x^n \in K$$

sind $n+1$ Elemente im $\mathbf{C}$-Vektorraum K. Damit müssen sie $\mathbf{C}$-linear abhängig sein, d.h. es gibt $a_0, \ldots, a_n \in \mathbf{C}$, so dass nicht alle $a_k = 0$ sind mit

$$a_0 x^0 + a_1 x + \cdots + a_n x^n = 0.$$

Es gibt ein $k > 0$ mit $a_k \neq 0$: andernfalls würde aus dieser Gleichung auch $a_0 = 0$ folgen, d.h. alle $a_k = 0$. Also ist $x \in K$ eine Nullstelle des Polynoms $f(t) := \sum_{k=0}^{n} a_k t^k$. Sei $d := \deg f$ der Grad von f. Es gilt $d > 0$. Nach Folgerung 2.9 ist aber $f(t) = \prod_{k=1}^{d}(t-z_k)$ für gewisse $z_k \in \mathbf{C}$. Es gilt also

$$0 = f(x) = \prod_{k}(x-z_k).$$

Rechts steht ein Produkt von d Elementen in K, und ein solches Produkt ist genau dann 0, wenn wenigstens einer der Faktoren 0 ist (Übungsaufgabe 2.14). Also folgt hier $x = z_k$ für ein $1 \leqslant k \leqslant d$, d.h. $x \in \mathbf{C}$. □

Bemerkung 2.12. Ohne die Bedingung $\dim_{\mathbf{C}} K < \infty$ ist die Aussage von Theorem 2.11 falsch: beispielsweise ist der sog. *Funktionenkörper*

$$\mathbf{C}(t) := \left\{ \frac{p(t)}{q(t)} | p, q \text{ komplexe Polynome, } q(t) \neq 0 \right\}$$

ein Körper (mit $\dim_{\mathbf{C}} \mathbf{C}(t) = \infty$).

Situationen wie in Theorem 2.11 kommen in der Folge immer wieder vor. Wir verwenden daher folgende Sprechweise:

Definition 2.13. Seien k und K ein Körper (z.B. $\mathbf{R}$ oder $\mathbf{C}$) mit

$$k \subset K.$$

Man nennt dann K eine *Körpererweiterung* von k. Es ist(!) insbesondere K dann auch ein k-Vektorraum. Die Dimension von K als *k-Vektorraum* nennen wir *Grad* der Körpererweiterung. Wir sind in der Folge v.a. an dem Fall interessiert, dass dieser Grad endlich ist. Solche Körpererweiterungen heißen *endliche Körpererweiterung*.

Bemerkung 2.14.
- Der Grad, definiert als $\dim_k K$ darf nicht verwechselt werden mit $\dim_K K$ (d.h. die Dimension von K als K-Vektorraum): letztere ist stets 1.
- $\mathbf{R} \subset \mathbf{C}$ ist eine Körpererweiterung.

  Ihr Grad ist 2, denn $\{1, i\}$ ist eine Basis von $\mathbf{C}$ als $\mathbf{R}$-Vektorraum.

- Die Aussage von Theorem 2.11 bedeutet in dieser Sprechweise also gerade, dass $\mathbf{C}$ keine endlichen Körpererweiterungen (abgesehen natürlich von $\mathbf{C} \subset \mathbf{C}$) besitzt.

Definition 2.15. Man bezeichnet einen Körper k als *algebraisch abgeschlossen*, wenn jedes nicht-konstante Polynom mit Koeffizienten in k eine Nullstelle hat.

Theorem 2.6 besagt also, dass $\mathbf{C}$ algebraisch abgeschlossen ist. Der Beweis von Folgerung 2.9 und Theorem 2.11 benutzt nur diese Eigenschaft von $\mathbf{C}$ (und nicht die konkrete Konstruktion von $\mathbf{C}$). Demzufolge erhalten wir:

Folgerung 2.16. Sei k ein algebraisch abgeschlossener Körper und $K \supset k$ eine endliche Körpererweiterung. Dann ist $k = K$.

2.3 Körpererweiterungen der reellen Zahlen

Unser nächstes Ziel ist der Beweis von Theorem 2.27. Beispielsweise besagt der Satz, dass es keinen Zahlenbereich (hiermit ist an dieser Stelle gemeint: Körper) geben kann, der als $\mathbf{R}$-Vektorraum drei-dimensional ist, d.h. aus Ausdrücken der Form

$$a + ib + jc$$

wobei $a, b, c \in \mathbf{R}$ und i, j zwei "hyperimaginäre" Zahlen sind. Um den Satz präzise zu formulieren, führen wir zunächst einige algebraische Grundbegriffe ein.

Definition 2.17.
- Eine *reelle Algebra* oder kurz *Algebra* ist ein $\mathbf{R}$-Vektorraum V, zusammen mit einer Abbildung (genannt *Multiplikation*)
$$V \times V \to V$$
Wir notieren diese Abbildung mit $(v, w) \mapsto vw$. Diese Abbildung muss folgende Eigenschaften erfüllen ($v, w, u \in V$ sind hierbei beliebige Elemente, sowie $\lambda, \mu \in \mathbf{R}$):
  - Die Multiplikation ist eine bilineare Abbildung, d.h. es gilt das Distributivitätsgesetz
$$v(\lambda w + \mu u) = \lambda vw + \mu vu, (\lambda v + \mu w)u = \lambda vu + \mu wu.$$
  - Es gibt ein Element $1 \in V$, genannt *Eins-Element*, so dass
$$v1 = 1v = v.$$
(Ein solches Element ist automatisch eindeutig: wäre $1'$ ein anderes Eins-Element, so gilt $1 = 1 \cdot 1' = 1'$.) Wir fordern (um den langweiligen Fall $V = \{0\}$ auszuschließen), dass
$$1 \neq 0$$
- Wir nennen V eine *assoziative Algebra*, wenn das Assoziativitätsgesetz gilt:
$$(vw)u = v(wu).$$
- Wir nennen V eine *kommutative Algebra*, wenn das Kommutativitätsgesetz gilt:
$$vw = wv.$$

Beispiel 2.18.
- Die reellen Polynome $\mathbf{R}[t]$ (Übungsaufgabe 2.2) bilden eine assoziative, kommutative Algebra.
- Die komplexen Zahlen $\mathbf{C}$ sind ebenfalls eine assoziative, kommutative Algebra.
- Die $n \times n$-Matrizen (mit der Matrizenmultiplikation versehen) bilden eine assoziative, aber für $n \geqslant 2$ *nicht* kommutative Algebra.
- Wir werden in §3 die Quaternionen $\mathbf{H}$ kennenlernen, welche ebenfalls assoziativ, aber nicht kommutativ sind. Es gilt $\dim_{\mathbf{R}} \mathbf{H} = 4$.
- In Übungsaufgabe 3.2 wird eine 4-dimensionale, kommutative, jedoch nicht assoziative Algebra konstruiert.
- Die Oktonionen (§4) $\mathbf{O}$ bilden eine 8-dimensionale, weder assoziative, noch kommutative Algebra.

Wir brauchen immer mal wieder auch einige spezielle Eigenschaften von Elementen bezüglich der Multiplikation:

Definition 2.19. Sei V eine assoziative Algebra. Sei $v \in V$ beliebig.

- Ein Element w heißt *multiplikatives Inverses* von v, wenn
$$wv = vw = 1$$
gilt. Ein solches Element wird oft auch mit v^{-1} bezeichnet, denn es ist automatisch eindeutig: falls w' ein weiteres multiplikatives Inverses ist, so gilt
$$w = w1 = w(vw') = (wv)w' = 1w' = w'.$$
- Ein *Schiefkörper* (der $\mathbf{R}$ enthält) ist eine assoziative $\mathbf{R}$-Algebra V mit der Eigenschaft, dass jedes $v \in V$, $v \neq 0$ ein multiplikatives Inverses besitzt.
- $v \in V$, $v \neq 0$ heißt *Nullteiler*, falls es ein $w \in V \backslash \{0\}$ gibt mit
$$vw = 0.$$

Beispiel 2.20.
- Jeder Körper ist also ein Schiefkörper. Genauer: ein Schiefkörper ist genau dann ein Körper, wenn er kommutativ ist.
- Wir lernen in §**??** die Quaternionen kennen. Sie sind ein Schiefkörper (aber kein Körper).
- Falls V ein Schiefkörper ist, so hat V keine Nullteiler, denn aus $vw = 0$ und $v \neq 0$ folgt
$$0 = v^{-1}0 = v^{-1}vw = 1w = w.$$
- Die Matrizen $\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$ (für beliebiges $a \neq 0$) sind Nullteiler in $\mathrm{Mat}_{2\times 2}(\mathbf{R})$, denn
$$\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = 0.$$

Definition 2.21. Seien V und W zwei Algebren. Ein *Algebren-Homomorphismus* oder kurz *Homomorphismus*

25.11.20

$$f : V \to W$$
ist eine $\mathbf{R}$-lineare Abbildung derart, dass
$$f(v_1 v_2) = f(v_1) f(v_2) \tag{2.22}$$

und

$$f(1_V) = 1_W$$

gilt. Hierbei ist die Multiplikation auf der linken Seite in V zu verstehen, rechts die in W; 1_V bzw. 1_W bezeichnet ein Eins-Element.

Ein solcher Algebren-Homomorphismus f heißt *Algebren-Isomorphismus* oder kurz *Isomorphismus*, wenn es einen (Algebren-)Homomorphismus

$$g : W \to V$$

gibt so dass $g \circ f = \mathrm{id}_V$ (d.h. $g(f(v)) = v$ für alle $v \in V$) und $f \circ g = \mathrm{id}_W$.

Beispiel 2.23. Die komplexe Konjugation

$$\overline{?} : \mathbf{C} \to \mathbf{C}, z \mapsto \overline{z}$$

ist ein Algebren-Homomorphismus, denn die Abbildung ist $\mathbf{R}$-linear und erfüllt (2.22), d.h. es gilt

$$\overline{z_1 z_2} = \overline{z_1}\ \overline{z_2},$$

(!) wie man mit einer expliziten Rechnung(!) leicht nachprüft. Dieser Homomorphismus ist sogar ein Isomorphismus, denn es gilt $z = \overline{\overline{z}}$, d.h. die Abbildung $z \mapsto \overline{z}$ ist ihr eigenes Inverses.

Wie in Übungsaufgabe 2.6 präzisiert wird, gibt es nur zwei Algebren-Isomorphismen $\mathbf{C} \to \mathbf{C}$.

Bemerkung 2.24. Ein Homomorphismus f ist ein Isomorphismus genau dann, wenn er bijektiv ist: in diesem Fall ist die Umkehrabbildung f^{-1} nämlich automatisch selbst ein Homomorphismus. Beispielsweise prüft man (2.22) wie folgt nach: $f^{-1}(w_1 w_2) = f^{-1}(w_1) f^{-1}(w_2)$ ist, da f bijektiv ist, äquivalent zu

$$f(f^{-1}(w_1 w_2)) \stackrel{!}{=} f(f^{-1}(w_1) f^{-1}(w_2)).$$

Die linke Seite ist $w_1 w_2$. Ebenso rechts, wobei wir hier benutzen, dass f die Bedingung (2.22) erfüllt:

$$w_1 w_2 = f(f^{-1}(w_1)) f(f^{-1}(w_2)) = f(f^{-1}(w_1) f^{-1}(w_2)).$$

Lemma 2.25. Sei K ein Schiefkörper (z.B. ein Körper), W eine assoziative Algebra und $f : K \to W$ ein Homomorphismus von Algebren. Dann ist f stets injektiv.

Damit ist nach Bemerkung 2.24 f genau dann ein Isomorphismus wenn f surjektiv ist.

Beweis. Aus der linearen Algebra (dies ist eine allgemeine Tatsache über lineare Abbildungen) ist bekannt: die Injektivität folgt aus $\ker f = 0$. Der Klarheit halber schreiben wir $\mathbf{0} \in W$ für den Nullvektor und $0 \in \mathbf{R}$ für die Zahl Null. Für jeden Vektor $w \in W$ gilt $\mathbf{0}w = (01_W)w = 0(1_W w) = 0w = \mathbf{0}$. Hier benutzen wir (nur) die allgemeinen Algebra-Axiome, nämllich die $\mathbf{R}$-Linearität der Multiplikation, die Assoziativität, die Definition eines Eins-Elements sowie nochmal die $\mathbf{R}$-Linearität.

Sei also $v \in K$ mit $f(v) = \mathbf{0}$. Angenommen $v \neq 0$. Dann gilt

$$1_W = f(1_K) = f(vv^{-1}) = f(v) f(v^{-1}) = \mathbf{0} f(v^{-1}) = \mathbf{0}.$$

Dies ist ein Widerspruch zur Forderung $1 \neq \mathbf{0}$ (Definition 2.17). □

Beispiel 2.26. Sei V eine Algebra. Die Abbildung

$$\mathbf{R} \to V, \lambda \mapsto \lambda 1$$

(!) ist ein Algebrenhomomorphismus(!) und demzufolge (Lemma 2.25) injektiv. Wir können (und werden) daher die reellen Zahlen als Unteralgebra von V auffassen. Für eine reelle Zahl λ bedeutet das Element "$\lambda \in V$" also genau genommen $\lambda 1$.

Theorem 2.27. Sei $\mathbf{R} \subset K$ eine *endliche* Körpererweiterung mit Grad $n (< \infty)$. Dann ist entweder
(1) $n = 1$. In diesem Fall gilt $K = \mathbf{R}$.

(2) $n = 2$. In diesem Fall gibt es einen Algebren-Isomorphismus

$$\mathbf{C} \xrightarrow{\cong} K.$$

Um dies zu beweisen, beginnen wir zunächst mit der Frage nach der Faktorisierung *reeller* Polynome, d.h. der Frage, wie wir reelle Polynome als Produkte "einfacher(er)" reeller Polynome schreiben können. Diese Frage beantwortet der nächste Satz. Zu seiner Vorbereitung ein kleines Lemma:

Lemma 2.28. Sei $f(t) = \sum_{k=0}^{n} a_k t^k$ ein reelles Polynom. Seien $z_1, \ldots, z_n$ die Nullstellen von f, d.h. $f(t) = \prod_k (t - z_k)$. Dann gilt: ist $z \in \mathbf{C}$ unter den z_k, dann ist auch $\overline{z}$ (das komplex Konjugierte) unter den z_k.

Beweis. Es gilt (die Gleichung * gilt wegen $a_k \in \mathbf{R}$!)

$$f(\overline{z}) = \sum a_k (\overline{z})^k \overset{*}{=} \sum \overline{a_k} (\overline{z})^k = \sum \overline{a_k z^k} = \overline{f(z)} = \overline{0} = 0,$$

also ist $\overline{z}$ ebenfalls eine Nullstelle von f. □

Satz 2.29. Sei $f(t)$ ein reelles normiertes Polynom vom Grad $n \geqslant 1$. Dann gibt es Zahlen $r, s \in \mathbf{N}$, $a_1, \ldots, a_r, b_1, \ldots b_s, c_1, \ldots, c_s, \in \mathbf{R}$ sowie $m_1, \ldots, m_r, n_1, \ldots, n_s \in \mathbf{N}\backslash\{0\}$ derart, dass $\sum_{k=1}^{r} m_k + 2\sum_{k=1}^{s} n_k = n$, $b_k^2 - 4c_k < 0$ und (vor allem!)

$$f(t) = \prod_{k=1}^{r} (t - a_k)^{m_k} \prod_{k=1}^{s} (t^2 - b_k t + c_k)^{n_k}.$$

Beweis. Das reelle Polynom f können wir auch auffassen als ein (besonderes) komplexes Polynom. Laut Folgerung 2.9 zerfällt das Polynom f dann als Produkt der Form $f(t) = \prod_{k=1}^{n} (t - z_k)$ mit geeigneten $z_k \in \mathbf{C}$.

Wir bezeichnen diejenigen Nullstellen z_k, die in $\mathbf{R}$ liegen, mit $a_1, \ldots, a_r$. Laut Lemma 2.28 tauchen die übrigen Nullstellen in Paaren auf, d.h. für jede echt komplexe (d.h. nicht in $\mathbf{R}$ liegende) Nullstelle z ist auch $\overline{z}$ eine Nullstelle. Für eine derartige Nullstelle ist

$$q(t) := (t - z)(t - \overline{z}) = t^2 - \underbrace{(z + \overline{z})}_{=:b} t + \underbrace{z\overline{z}}_{=:c}$$

ein *reelles*(!) Polynom. Es gilt dann $b^2 - 4c < 0$, denn sonst hätte(!) $q(t)$ eine reelle Nullstelle. □ 

Bemerkung 2.30. Analog zu Folgerung 2.9 gilt zusätzlich folgendes: diese Darstellung ist bis auf die Reihenfolge der Faktoren *eindeutig*, d.h. wenn

$$f(t) = \prod_{k=1}^{r'} (t - a'_k)^{m'_k} \prod_{k=1}^{s'} (t^2 - b'_k t - c'_k)^{n'_k}$$

mit $a'_k, \ldots$ etc. mit den gleichen Bedingungen wie eben, so gilt $r = r'$, $s = s'$ und für eine geeignete Permutation $\rho : \{1, \ldots, r\} \to \{1, \ldots, r'(= r)\}$ sowie $\sigma : \{1, \ldots, s\} \to \{1, \ldots, s'(= s)\}$ gilt $a'_{\rho(k)} = a_k$, $n'_{\rho(k)} = n_k$, $b'_{\sigma(k)} = b_k$ usw. Der Beweis verläuft ähnlich zu der in Folgerung 2.9.

Eine weitere Vorbereitung für den Beweis von Theorem 2.27 ist folgende Aussage:

Lemma 2.31. Sei $K \supset \mathbf{R}$ eine endliche Körpererweiterung und $v \in K\backslash\mathbf{R}$. Dann gibt es $b, c \in \mathbf{R}$ mit

$$v^2 = bv + c.$$

Beweis. Genau wie im Beweis von Theorem 2.11 (ersetze im ersten Schritt dort $\mathbf{C}$ durch $\mathbf{R}$) sieht man, dass es ein reelles Polynom $f(t)$ gibt, so dass $f(v) = 0$ gilt. Betrachte eine Faktorisierung von f als Produkt linearer und quadratischer Polynome wie in Satz 2.29: $f(t) = \prod (t - a_k)^{n_k} \prod (t^2 - b_k t - c_k)^{m_k}$. Da $f(v) = 0$, muss einer der Faktoren $v - a_k$ bzw. $v^2 - b_k v - c_k$ gleich 0 sein: in einem Körper (so wie K) ist ein Produkt $\prod_{i=1}^{n} \lambda_i$ genau dann 0 (mit $\lambda_i \in K$), wenn (wenigstens) eins der $\lambda_i = 0$ ist (Übungsaufgabe 2.14).

Da $v \notin \mathbf{R}$ und $a_k \in \mathbf{R}$, ist es nicht möglich, dass $v - a_k = 0$. Es tritt also der andere Fall ein, d.h. v ist Nullstelle eines reellen quadratischen Polynoms. Dies zeigt die Behauptung. □

Nun beweisen wir Theorem 2.27.

Beweis. Sei $V = \mathbf{R} + \mathbf{R}v$ der $\mathbf{R}$-Untervektorraum (in K), der von 1 und v erzeugt wird. Laut Lemma 2.31 gibt es $b, c \in \mathbf{R}$ mit $v^2 = bv + c$. Setze $d := \frac{b}{2}$. Für zwei beliebige Elemente $x_1 + y_1 v$, $x_2 + y_2 v \in V$ gilt:

$$(x_1 + y_1 v)(x_2 + y_2 v) = (x_1 x_2 + y_1 y_2 c) + (x_1 y_2 + y_1 x_2 + y_1 y_2 b)v.$$

Dies liegt wieder in V (!). Also ist V, versehen mit der Multiplikation von K, eine (kommutative, assoziative) Algebra.

Setze $w := v - d$. Dies liegt (in V aber) nicht in $\mathbf{R}$, denn sonst wäre $v \in \mathbf{R}$. Dann gilt $w^2 = r$, wobei $r := c + d^2 \in \mathbf{R}$. Dann ist $r < 0$: andernfalls wäre $\sqrt{r} \in \mathbf{R}$ und demnach $v = \pm\sqrt{r} \in \mathbf{R}$. Wegen $r < 0$ gibt es also $s \in \mathbf{R}$ mit $s^2 = -\frac{1}{r}$. Setzen wir schließlich $u := sw \in K \backslash \mathbf{R}$, so erhalten wir

$$u^2 = -1.$$

Die Abbildung

$$\varphi : \mathbf{C} \to V, x + iy \mapsto x + wy$$

ist ein Algebren-Homomorphismus: dies prüft(!) man durch direktes Nachrechnen mittels $u^2 = -1$ nach. Nach Konstruktion ist φ surjektiv und damit, laut Lemma 2.25, ein Isomorphismus.

Wir zeigen nun $K = V$: wir haben einen Algebrenisomorphismus $\varphi : \mathbf{C} \xrightarrow{\cong} V$ und sein Inverses $\varphi^{-1} : V \xrightarrow{\cong} \mathbf{C}$. Da $\mathbf{C}$ algebraisch abgeschlossen ist, ist es auch V: sei $f(t) = \sum a_k t^k \in V[t]$ ein Polynom mit Koeffizienten in V. Bezeichne mit $\varphi^{-1}(f)(t) := \sum \varphi^{-1}(a_k) t^k \in \mathbf{C}[t]$. Es hat eine Nullstelle $z \in \mathbf{C}$ und es gilt also $\varphi^{-1}(f)(t) = (t - z)g(t)$ mit einem geeigneten Polynom $g = \sum b_k t^k \in \mathbf{C}[t]$. Hieraus folgt, da φ ein Algebren-Homomorphismus ist: $f(t) = \varphi(\varphi^{-1}(f))(t) = (t - \varphi(z))\varphi(g)(t)$, wobei $\varphi(g) := \sum \varphi(b_k) t^k$. Also hat f die Nullstelle $\varphi(z)$, d.h. V ist algebraisch abgeschlossen.

Laut Folgerung 2.16 hat V also keine nicht-trivialen endlichen Erweiterungen, d.h. es gilt $K = V$. □

3.12.20 **Bemerkung 2.32.** Der Körperisomorphismus im zweiten Fall ist nicht eindeutig, denn gegeben einen solchen Isomorphismus $\varphi : \mathbf{C} \to K$ ist auch $\overline{\varphi} : z \mapsto \varphi(\overline{z})$ ein Isomorphismus. (Hierbei benutzen wir die allgemeine Tatsache(!) , dass die Komposition zweier Homomorphismen wieder ein Homomorphismus ist.) Es gilt $\varphi(z) = \varphi(\overline{z})$ genau dann, wenn $z = \overline{z}$, d.h. wenn $z \in \mathbf{R}$. Insbesondere gilt $\varphi \neq \overline{\varphi}$.

Es lässt sich leicht aus Übungsaufgabe 2.6 folgern, dass (für einen gegebenen Isomorphismus φ) die beiden Abbildungen $\varphi, \overline{\varphi}$ die beiden einzigen Isomorphismen sind.

2.4 Übungsaufgaben

Übungsaufgabe 2.1. Sei $n \geqslant 1$ eine natürliche Zahl. Zeige mittels der in §2.1 wiederholten Eigenschaften, dass die Abbildung

$$S^1 \to S^1,$$
$$z \mapsto z^n$$

surjektiv ist.

Man bezeichnet die Menge $\{z \in \mathbf{C}, z^n = 1\}$ als die n-ten *Einheitswurzeln*. Wie viele Elemente hat diese Menge? Skizziere sie!

Übungsaufgabe 2.2. Sei K ein Körper. Sei

$$K[t] := \{p(t) \text{ Polynom mit Koeffizienten in } K\}.$$

Wir versehen diese Menge mit der aus der Schule bekannten Addition und Multiplikation, d.h. für $p(t) = a_0 t^0 + a_1 t + \cdots + a_n t^n$ und $q(t) = b_0 t^0 + b_1 t + \cdots + b_m t^m = 0$ ist

$$p + q := (a_0 + b_0)t^0 + (a_1 + b_1)t^1 + \cdots + (a_k + b_k)t^k$$

wobei $k := \max(n, m)$ und wir interpretieren $a_k := 0$ für $k > n$ (bzw. $b_k := 0$ für $k > m$).

$$p \cdot q := a_0 b_0 t^0 + (a_1 b_0 + a_0 b_1)t^1 + \cdots + a_n b_m t^{n+m}.$$

(Der Koeffizient bei t^k ist gegeben durch $\sum_{i=0}^{k} a_i b_{k-i}$.)

(1) Handelt es sich bei $K[t]$ um einen Körper? Gib an, welche Körperaxiome erfüllt sind, und (ggf.) welche nicht erfüllt sind.

Tipp: zeige $\deg(fg) = \deg f + \deg g$.

(2) Welche Dimension hat $K[t]$ als K-Vektorraum?

Übungsaufgabe 2.3. Gib die Faktorisierung von $f(t) = t^4 - 1$ als Produkt komplexer Linearfaktoren und als Produkt von reellen Polynomen vom Grad $\leqslant 2$ (Satz 2.29) an.

Übungsaufgabe 2.4. Ist die Determinante bzw. Spur

$$\det, \mathrm{tr} : \mathrm{Mat}_{n\times n}(\mathbf{R}) \to \mathbf{R}$$

ein Algebren-Homomorphismus?

Übungsaufgabe 2.5. Sei K ein Körper und $f(t), g(t)$ zwei Polynome mit Koeffizienten in K. Zeige: $f(t)g(t) = 0$ genau dann wenn $f(t)$ oder $g(t) = 0$ ist.

Tipp: benutze Übungsaufgabe 2.14.

Übungsaufgabe 2.6.

- Zeige, dass die einzigen Algebren-Homomorphismen

$$\mathbf{C} \overset{\cong}{\to} \mathbf{C}$$

die Identität und die komplexe Konjugation sind.

- Seien $\varphi : E \to F$ und $\psi : F \to G$ Homomorphismen zwischen drei Algebren. Zeige, dass auch die Komposition $\psi \circ \varphi : E \to G$ ein Algebrenhomomorphismus ist.

- Ist der Isomorphismsus $K \overset{\cong}{\to} \mathbf{C}$ in Theorem 2.27 eindeutig?

Übungsaufgabe 2.7. Sei K ein Körper. Zeige, dass es *kein* Element

$$x \in K$$

gibt mit der Eigenschaft, dass

$$x0 = 0x = 1$$

ist. Gib genau an, welche Axiome der Definition eines Körpers in diesem Beweis verwendet wurden, und welche nicht verwendet wurden.

Also: in einem Körper gibt es *kein* multiplikatives Inverses der 0. Insbesondere ist auch keine Division durch 0 möglich (denn dieses multiplikative Inverse wäre ja $x = \frac{1}{0}$).

Übungsaufgabe 2.8. Zeige, dass es *keine* Teilmenge

$$\mathbf{C}^{>0} \subset \mathbf{C}$$

gibt, die die folgenden Eigenschaften erfüllt:

- Für jedes $z \in \mathbf{C}$ gilt genau eine der folgenden drei Aussagen: a) $z \in \mathbf{C}^{>0}$, b) $-z \in \mathbf{C}^{>0}$, c) $z = 0$.

- Für $w, z \in \mathbf{C}^{>0}$ gilt $w + z, wz \in \mathbf{C}^{>0}$.

Wähle zwei Teilmengen $C_1, C_2 \subset \mathbf{C}$ und erkläre / illustriere, welche der obigen Bedingungen für die gewählten Teilmengen nicht erfüllt sind.

Inwiefern ist die obige Aussage ein Unterschied zu den reellen Zahlen?

Übungsaufgabe 2.9. In der folgenden Aufgabe fassen wir, wie üblich, $\mathbf{C}$ als die Zahlenebene $\mathbf{R}^2$ auf. Sei $\Delta \subset \mathbf{C}$ das Dreieck mit den Ecken $z_1, z_2, z_3 \in \mathbf{C}$. Zeige, dass der Flächeninhalt dieses Dreiecks mit dem Betrag des folgenden Ausdrucks übereinstimmt

$$\frac{1}{4}\begin{vmatrix} z_1 & \overline{z_1} & 1 \\ z_2 & \overline{z_2} & 1 \\ z_3 & \overline{z_3} & 1 \end{vmatrix}.$$

Hierbei bezeichnet $|\dots|$ die Determinante der angegebenen komplexen 3×3-Matrix.

Tipp: sei $z_k = (x_k, y_k) \in \mathbf{R}^2$. Zeige zunächst eine ähnliche Formel für die Fläche in Termen einer Matrix deren Einträge die x_k, y_k und 1 sind.

Übungsaufgabe 2.10. Das *Zentrum* einer assoziativen Algebra A ist definiert als

$$Z(A) := \{x \in A, xy = yx \text{ für alle } y \in A\}.$$

Zeige:

- $\mathbf{R} \subset Z(A)$. (Wie üblich ist mit $\mathbf{R}$ hier genauer die Teilmenge $\mathbf{R} \cdot 1 := \{\lambda \cdot 1 | \lambda \in \mathbf{R}\} \subset A$ gemeint.)
- $Z(A)$ ist, versehen mit der Addition und Multiplikation aus A, eine *kommutative* Algebra.
- $Z(A) = A$ genau dann, wenn A kommutativ ist.
- $Z(\mathrm{Mat}_{n\times n}(\mathbf{R}))$ besteht genau aus den Diagonalmatrizen, deren Einträge alle gleich sind. (Also in der obigen Schreibweise $Z(\mathrm{Mat}_{n\times n}(\mathbf{R})) = \mathbf{R} \cdot 1 = \mathbf{R}$.) Zeige dies durch Wahl einiger geeigneter Elemente y in der obigen Definition des Zentrums.

Übungsaufgabe 2.11. Sei $n \geqslant 1$ eine natürliche Zahl. Gib eine kommutative, assoziative Algebra V an, deren Dimension (als $\mathbf{R}$-Vektorraum) n ist.

Tipp: orientiere dich an der Algebra der dualen Zahlen (Übungsaufgabe 2.18).

Übungsaufgabe 2.12. Sei K ein Körper. Seien $f, g, h \in K[t]$ Polynome mit Koeffizienten in K. Wir sagen "g teilt f" (Schreibweise $g|f$), wenn es ein Polynom h gibt mit

$$g \cdot h = f.$$

Wir nennen nicht-konstantes Polynom f ein *irreduzibles Polynom*, wenn für alle $g \in K[t]$ mit $g|f$ gilt: $\deg g = 1$ oder $\deg g = \deg f$.

(1) Zeige: für $K = \mathbf{C}$ ist ein nicht-konstantes Polynom genau dann irreduzibel, wenn es linear ist, d.h. $f(t) = a_1 t + a_0$.

(2) Zeige: für $K = \mathbf{R}$ ist ein nicht-konstantes Polynom genau dann irreduzibel, wenn es entweder linear ist, oder wenn es quadratisch ist, aber keine reelle Nullstelle hat.

(3) Betrachte $K = \mathbf{Q}$. Ist $f(t) = t^2 - 2$ irreduzibel?

(4) Zeige: haben zwei Polynome $f, g \in K[t]$ *keinen* nicht-konstanten gemeinsamen Teiler, dann gibt es Polynome $r, s \in K[t]$ mit $fr + gs = 1$.

(5) Folgere aus (4): Sei f irreduzibel sowie $g, h \in K[t]$ beliebig. Zeige: aus $f|(gh)$ folgt entweder $f|g$ oder $f|h$.

(6) Zeige: jedes nicht-konstante Polynom $f \in K[t]$ lässt sich schreiben als

$$f = \prod_{k=1}^{r} g_k,$$

wobei $g_1, \dots, g_r \in K[t]$ irreduzible Polynome sind.

2.5 Präsenzaufgaben für die Übungen

Übungsaufgabe 2.13. Wie lautet die Definition eines Körpers? Gib wenigstens drei Beispiele eines Körpers an. Erläutere jeweils kurz, weshalb die Körperaxiome in diesen Beispielen gelten. Erkläre ferner, weshalb $\mathbf{N}$ (natürliche Zahlen), $\mathbf{Z}$, $\mathbf{R}\backslash\{0\}$ (jeweils mit den üblichen Rechenoperationen) keine Körper sind.

Übungsaufgabe 2.14. Sei K ein Körper und $x, y \in K$. Zeige (allein unter Benutzung der Axiome in der Definition eines Körpers): $xy = 0$ genau dann wenn $x = 0$ oder $y = 0$. Benenne explizit, welche Körperaxiome in diesem Beweis benutzt werden, und welche nicht benutzt werden.

Illustriere diese Tatsache geometrisch am Beispiel von $K = \mathbf{C}$.

Übungsaufgabe 2.15. Sei K ein Körper, V, W seien K-Vektorräume. Erkläre den Begriff einer Basis von V.

Sei $\{v_1, \ldots, v_n\}$ eine Basis von V. Seien $w_1, \ldots, w_n \in W$ beliebig. Zeige: es gibt genau eine $\mathbf{R}$-lineare Abbildung $f : V \to W$ mit $f(v_k) = w_k$. Wie sieht diese Abbildung f aus?

Erläutere, inwieweit die Aussage falsch ist, wenn die v_k lediglich linear unabhängig, bzw. lediglich ein Erzeugendensystem bilden.

Übungsaufgabe 2.16. Sei V eine assoziative Algebra und $x \in V$. Wir definieren

$$x^0 := 1$$

und induktiv, für $n \geqslant 1$:

$$x^n := x \cdot x^{n-1}.$$

Beispielsweise ist also $x^3 = x(xx)$.

Zeige: für $n, m \in \mathbf{N}$ gilt

$$x^n x^m = x^{n+m}.$$

Gib genau an, auf welche Tripel von Elementen die Assoziativität der Algebra angewendet wurde (d.h. mit welchen Elemente $a, b, c \in V$ die Gleichheit $a(bc) = (ab)c$ benutzt wurde).

Übungsaufgabe 2.17. Sei $\mathbf{R}[t]$ die Algebra der reellen Polynome. Zeige, dass für eine beliebige Algebra A die Abbildung

$$\mathrm{Hom}(\mathbf{R}[t], A) \to A, f \mapsto f(t)$$

eine Bijektion (bzw. sogar ein $\mathbf{R}$-Vektorraumisomorphismus) ist. Hierbei bezeichnet Hom die Menge der Algebrenhomomorphismen.

Übungsaufgabe 2.18. Die Algebra der *dualen Zahlen* ist folgendermaßen definiert: als Vektorraum ist es der 2-dimensionale Vektorraum $V := \mathbf{R}^2$. Wir wählen die Notation $e := (1, 0)$, $x := (0, 1) \in V$. Die Multiplikation ist die eindeutige $\mathbf{R}$-bilineare Abbildung, die folgende Regeln erfüllt:

$$e \cdot e = e, e \cdot x = x \cdot e = x, x \cdot x = 0.$$

- Gib eine explizite Formel für die Multiplikation beliebiger Elemente in V an.
- Bestimme die Nullteiler in V.
- Gib einen surjektiven Algebrenhomomorphismus $\mathbf{R}[t] \to V$ an.
- Zusatz: formuliere und beweise eine Aussage wie in Übungsaufgabe 2.17 für $\mathrm{Hom}(V, A)$.

Übungsaufgabe 2.19. Sei $a \in \mathbf{C}$ sowie $f(t) := t^n - a$. Wie viele Lösungen (mit $z \in \mathbf{C}$) hat die Gleichung

$$f(z) = 0?$$

Skizziere die Lösungsmenge für einige ausgewählte Paare (n, a).

Übungsaufgabe 2.20. Für eine komplexe Zahl $w \in \mathbf{C}$ bezeichnen wir mit L_w den Strahl, der von 0 durch w verläuft. Wir bezeichnen mit

$$\arg w \in [0, 2\pi)$$

den Winkel zwischen L_1 (d.h. der positiven x-Achse) und dem Strahl L_w.

- Gib $\arg(i)$, $\arg(\pm 1 + i)$ und $\arg(e^{2\pi i k/n})$ (für $k, n \in \mathbf{Z}$, $n \neq 0$) an.
- Seien $z_1, z_2 \in \mathbf{C}$ und beide $\neq 0$. Wir bezeichnen mit $\angle(z_1, 0, z_2)$ den Winkel *gegen den Uhrzeigersinn* zwischen den Strahlen L_{z_1} und L_{z_2}. Zeige

  $$\angle(z_1, 0, z_2) = \arg \frac{z_2}{z_1}.$$

  Berechne und skizziere dies für folgende Werte von (z_1, z_2): $(1 + i, 1 - i)$, $(1, i)$, $(i, 1)$.
- Formuliere und begründe eine ähnliche Aussage für den Winkel zwischen zwei Geraden.

Übungsaufgabe 2.21. Wir betrachten die Abbildung

$$(\ )' : \mathbf{C}[t] \to \mathbf{C}[t], f(t) = \sum_{k=0}^{n} a_k t^k \mapsto f'(t) := \sum_{k=1}^{n} a_k k t^{k-1}.$$

- Handelt es sich bei dieser Abbildung um einen Algebren-Homomorphismus?
- Sei

  $$f(t) = \prod_{k=1}^{n} (t - z_k)$$

  die Faktorisierung in lineare Faktoren. Bestimme $f'(t)$ in Termen der z_k.
- Sei $z_k \in \mathbf{C}$ eine Nullstelle von f. Dann ist $f(t)/(t - z_k)$ ebenfalls wieder ein Polynom. Wir nennen z_k eine *mehrfache Nullstelle* von f, wenn z_k ebenfalls eine Nullstelle von $f(t)/(t - z_k)$ ist.

  Sei nun $z \in \mathbf{C}$ beliebig. Zeige: z ist genau dann eine mehrfache Nullstelle von f, wenn $f(z) = 0$ und $f'(z) = 0$ gilt.

Übungsaufgabe 2.22. Sei $n \geqslant 1$ und B die Menge der reellen, oberen $n \times n$-Dreiecksmatrizen. Wir versehen B mit der üblichen Matrix-Multiplikation Handelt es sich bei B um eine Algebra? Ist sie kommutativ? Ist sie assoziativ?

Übungsaufgabe 2.23. Sei V eine assoziative Algebra mit $\dim_{\mathbf{R}} V = 2$.
(1) Zeige, dass V automatisch kommutativ ist.

(2) Zeige dass *genau* einer der beiden folgenden Fälle eintritt:

- Es gibt einen Algebren-Isomorphismus $V \cong \mathbf{C}$.
- Es gibt einen Algebren-Isomorphismus $V \cong W$, wobei W hier die Algebra der dualen Zahlen bezeichnet.
- Es gibt einen Algebren-Isomorphismus $V \cong \mathbf{R} \times \mathbf{R}$. Hierbei bezeichnet $\mathbf{R} \times \mathbf{R}$ die Algebra, deren Multiplikation durch $(x_1, x_2) \cdot (y_1, y_2) := (x_1 y_1, x_2 y_2)$ definiert ist.

Eine derart übersichtliche Klassifikation für assoziative Algebren gibt es in höheren Dimensionen nicht, wie man an der nicht kommutativen (jedoch assoziativen) 3-dimensionalen Algebra

$$B := \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} | a, b, d \in \mathbf{R} \right\}$$

sieht.

Übungsaufgabe 2.24. Sei V die Algebra der dualen Zahlen (siehe Übungsaufgabe 2.18). Seien

$$D := \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} | a, d \in \mathbf{R} \right\}$$

sowie

$$E := \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} | a, b \in \mathbf{R} \right\}$$

die Algebren, deren Multiplikation die übliche Matrizenmultiplikation ist. Bestätige zunächst, dass es sich bei D und E in der Tat um Algebren handelt.

Zu welcher der Algebren in Präsenzaufgabe 2 sind D und E isomorph?

Übungsaufgabe 2.25. Sei $f : V \to W$ ein Algebren-Isomorphismus von assoziativen Algebren. Die folgenden Aussagen lassen sich so umschreiben: eine Algebren-Eigenschaft von V (oder eines Elements $v \in V$) ist gleichbedeutend mit der entsprechenden Eigenschaft von W (bzw. von $f(v) \in W$).

Zeige einige der folgenden Aussagen. Stelle hierbei jeweils klar heraus, wo bzw. ob benutzt wurde, dass f a) ein Algebren-Homomorphismus, b) injektiv, c) surjektiv ist.

- v hat ein multiplikatives Inverses genau dann wenn $f(v)$ ein multiplikatives Inverses hat.
- V ist ein (Schief-)körper genau dann wenn W ein (Schief-)körper ist.
- v ist Nullteiler in V genau dann, wenn $f(v)$ Nullteiler in W ist.

Kapitel 3

Die Quaternionen

Theorem 2.11 und seine Folgerung Theorem 2.27 sagen uns: fordern wir für ein "Zahlensystem" K folgende Eigenschaften:

- es enthält die reellen Zahlen, ist aber nicht wesentlich größer, d.h.

$$\dim_{\mathbf{R}} K < \infty,$$

- es erfüllt die "üblichen" Rechenregeln, d.h. es handelt sich um einen Körper

so gibt es außer den reellen und komplexen Zahlen keine weiteren Möglichkeiten.

Im weiteren Verlauf dieser Vorlesung werden wir die Bedingungen an ein Zahlensystem abschwächen und untersuchen, wie Zahlensysteme mit schwächeren Eigenschaften aussehen können. Die erste Aussage in dieser Richtung ist Theorem 3.30: wenn wir zulassen, dass die Multiplikation nicht notwendig das Kommutativitätsgesetz

$$ab = ba$$

erfüllt, und ansonsten alle Forderungen in der obigen Liste aufrecht erhalten, erhalten wir noch genau ein weiteres neues Zahlensystem, die Quaternionen.

3.1 Definition und grundlegende Rechenregeln

Die Definition der Quaternionen ist eine Abwandlung einer möglichen Definition der komplexen Zahlen. Zur Erinnerung: $\mathrm{Mat}_{2\times 2}(K)$ bezeichnet die Algebra der 2×2-Matrizen mit Einträgen in einem Körper K. Es ist eine assoziative, jedoch *nicht* kommutative Algebra.

Lemma 3.1. Sei $\mathcal{C} \subset \mathrm{Mat}_{2\times 2}(\mathbf{R})$ die Teilmenge der Matrizen der Form

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$$

mit $a, b \in \mathbf{R}$. Diese Teilmenge (versehen mit der üblichen Matrizenmultiplikation) ist eine Algebra und die Abbildung

$$\begin{aligned} \mathcal{C} &\xrightarrow{\varphi} \mathbf{C}, \\ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} &\mapsto a + ib \end{aligned}$$

ist ein Algebren-Isomorphismus.

Beweis. Es handelt sich bei $\mathcal{C}$ um eine Algebra, da Produkte und $\mathbf{R}$-Linearkombinationen von Matrizen der obigen Form wieder diese Form haben. Dies ist sofort(!) klar für $\mathbf{R}$-Linearkombinationen. Für Produkte ist es eine explizite kleine Rechnung:

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix}\begin{pmatrix} c & -d \\ d & c \end{pmatrix} = \begin{pmatrix} ac-bd & -ad-bc \\ bc+ad & ac-bd \end{pmatrix} \in \mathcal{C}.$$

Es handelt sich bei φ um einen Algebren-Homomorphismus, denn

$$\begin{aligned} \varphi\left(\begin{pmatrix} a & -b \\ b & a \end{pmatrix}\right)\varphi\left(\begin{pmatrix} c & -d \\ d & c \end{pmatrix}\right) &= (a+ib)(c+id) \\ &= (ac-bd)+i(ad+bc) \\ &= \varphi(\begin{pmatrix} ac-bd & -ad-bc \\ bc+ad & ac-bd \end{pmatrix}) \\ &= \varphi(\begin{pmatrix} a & -b \\ b & a \end{pmatrix}\begin{pmatrix} c & -d \\ d & c \end{pmatrix}). \end{aligned}$$

Die Abbildung φ ist offensichtlich bijektiv und damit (Bemerkung 2.24) ein Isomorphismus. □

Diesen Zugang zu den komplexen Zahlen nutzen wir nun, etwas abgewandelt, um die Quaternionen zu konstruieren:

Definition und Lemma 3.2. Sei

$$\mathbf{H} \subset \mathrm{Mat}_{2\times 2}(\mathbf{C})$$

die Teilmenge der Matrizen der Form

$$\begin{pmatrix} w & -z \\ \overline{z} & \overline{w} \end{pmatrix}$$

(wie üblich bezeichnet $\overline{z}$ das komplex Konjugierte von z.) Diese Teilmenge, versehen mit der üblichen Matrizen-Multiplikation bildet eine assoziative Algebra, die sog. Algebra der *Quaternionen*.

Beweis. Wiederum mit einer kleinen Rechnung, ähnlich wie oben (und zusätzlich $\overline{zw} = \overline{z}\,\overline{w}$) prüft man nach, dass Produkte von Quaternionen wieder Quaternionen sind. $\mathbf{R}$-Linearkombinationen von Quaternionen sind Quaternionen. Die Multiplikation in $\mathrm{Mat}_{2\times 2}(\mathbf{C})$ ist assoziativ, folglich auch die Multiplikation in $\mathbf{H}$. □

Die Quaternionen enthalten die komplexen Zahlen: genauer ist die Abbildung

$$\mathbf{C} \to \mathbf{H}, z \mapsto \begin{pmatrix} z & 0 \\ 0 & \overline{z} \end{pmatrix}$$

ein injektiver Algebren-Homomorphismus(!) . Insbesondere sind die Zahlen $1, i \in \mathbf{C}$ auf natürliche Weise Quaternionen, d.h. aufgefasst als die Matrizen

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

Wir bezeichnen noch

$$j := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},\ k := \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}.$$

Die Elemente

$$1, i, j, k \in \mathbf{H}$$

bilden offensichtlich eine Basis von $\mathbf{H}$ als $\mathbf{R}$-Vektorraum. Es gilt also $\dim_{\mathbf{R}} \mathbf{H} = 4$.

Die Multiplikation in $\mathbf{H}$ ist *nicht* kommutativ, d.h. $\mathbf{H}$ ist keine kommutative Algebra (Übungsaufgabe 3.1), es gilt nämlich

$$ij = k, ji = -k.$$

Wie wir bald sehen werden hat die Nicht-Kommutativität hat einige bemerkenswerte Folgerungen, die z.B. im krassen Gegensatz zu den üblichen Eigenschaften von komplexen Polynomen stehen. Zunächst einige weitere Grundbegriffe:

Definition und Lemma 3.3. Der *Realteil*, *Imaginärteil*, *Konjugation*, *Skalarprodukt*, *Norm*, *Determinante* und *Spur* sind die Abbildungen

$$\begin{aligned}
&\Re : \mathbf{H} \to \mathbf{R}, a + ib + jc + kd \mapsto a,\\
&\Im : \mathbf{H} \to \mathbf{H}, a + ib + jc + kd \mapsto ib + jc + kd,\\
&\overline{?} : \mathbf{H} \to \mathbf{H}, x \mapsto \Re x - \Im x,\\
&\langle -, - \rangle : \mathbf{H} \times \mathbf{H} \to \mathbf{R}, (x = a + ib + jc + kd, x' = a' + ib' + jc' + kd') \mapsto \langle x, x' \rangle := \Re(x\overline{x'}) = aa' + bb' + cc' + dd',\\
&| - | : \mathbf{H} \to \mathbf{R}^{\geqslant 0}, q \mapsto \sqrt{\langle q, q \rangle}\\
&\det : \mathbf{H} \to \mathbf{R}, x = \begin{pmatrix} w & -z \\ \overline{z} & \overline{w} \end{pmatrix} \mapsto \langle x, x \rangle = w\overline{w} + z\overline{z} = |w|^2 + |z|^2\\
&\mathrm{tr} : \mathbf{H} \to \mathbf{R}, \begin{pmatrix} w & -z \\ \overline{z} & \overline{w} \end{pmatrix} \mapsto w + \overline{w} = 2\Re(w).
\end{aligned}$$

Das Skalarprodukt ist eine positiv definite, symmetrische Bilinearform (wobei $\mathbf{H}$ als $\mathbf{R}$-Vektorraum aufgefasst wird).

Die Norm erfüllt die Regeln für alle $x, y \in \mathbf{H}$

$$|\overline{x}| = |x|, |xy| = |x||y|. \tag{3.4}$$

Die zweite Formel heißt *Produktregel*.

Jedes Quaternion $x \in \mathbf{H}$ erfüllt eine quadratische Gleichung mit Koeffizienten in $\mathbf{R}$, nämlich

$$x^2 - \mathrm{tr}x \cdot x + \det x = 0. \tag{3.5}$$

Beweis. Die Aussage über das Skalarprodukt ist bekannt aus der linearen Algebra, wo man allgemeiner zeigt, dass ($e_i \in \mathbf{R}^n$ ist der Standardbasisvektor)

$$\langle -, - \rangle : \mathbf{R}^n \times \mathbf{R}^n \to \mathbf{R}, (\sum_{i=1}^{n} a_i e_i, \sum_{i=1}^{n} a'_i e_i) \mapsto \sum a_i a'_i$$

ein positiv definites Skalarprodukt ist. Wir nutzen hier den Fall $n = 4$. Wegen der Positiv-Definitheit ist $|q|$ in der Tat wohldefiniert.

Im Beweis der Produktformel benutzen wir die Formel

$$\overline{xx'} = \overline{x'}\overline{x},$$

siehe Übungsaufgabe 3.1 (beachte die Reihenfolge der Faktoren!).

Hieraus folgt (für $x \in \mathbf{H}$):

$$\langle x, x \rangle := \Re(x\overline{x}) = \frac{1}{2}(x\overline{x} + \overline{x\overline{x}}) = \frac{1}{2}(x\overline{x} + \overline{\overline{x}\overline{x}}) = x\overline{x},$$

d.h. $x\overline{x} \in \mathbf{R} \subset \mathbf{H}$.

Beachte: hieraus und aus der Symmetrie der Bilinearform $\langle -, - \rangle$ folgt:

$$x\overline{x} = \overline{x}x = \langle x, x \rangle.$$

Es gilt daher

$$|xy|^2 1 = \langle xy, xy \rangle 1 = (\overline{xy})(xy) = \overline{y}(\overline{x}x)y = \langle x, x \rangle \overline{y}y = \langle x, x \rangle \langle y, y \rangle = |x|^2|y|^2 1.$$

Da die Abbildung $\mathbf{R} \to \mathbf{H}, \lambda \mapsto \lambda 1$ ein *injektiver* Algebren-Homomorphismus ist, folgt $|xy|^2 = |x|^2|y|^2$ und damit (beachte, dass $|x| \geqslant 0$ etc.) die Behauptung $|xy| = |x||y|$.

Die behauptete quadratische Gleichung ist ein Spezialfall des Satzes von Cayley-Hamilton. Zur Erinnerung: für $A \in \mathrm{Mat}_{n \times n}(K)$, wobei K ein Körper ist, besagt dieser

$$\chi_A(A) = 0,$$

wobei $\chi_A \in K[t]$ das *charakteristische Polynom* ist. Wir wenden dies auf $K = \mathbf{C}$ und $n = 2$ an. (In diesem Fall kann man den Satz durch direktes Nachrechnen sofort bestätigen(!)) Es gilt $\chi_A(t) = t^2 - \mathrm{tr}At + \det A$, hieraus folgt Behauptung, da die obige Definition von det und tr gerade die Einschränkung der üblichen Determinante und Spur von komplexen 2×2-Matrizen ist. □

Folgerung 3.6. Die Quaternionen bilden einen Schiefkörper. Das multiplikative Inverse eines Elements $x \in \mathbf{H}$, $x \neq 0$ ist gegeben durch

$$x^{-1} = \frac{1}{|x|^2}\overline{x}.$$

Beweis. In der Tat:

$$x \underbrace{\frac{1}{|x|^2}}_{\in \mathbf{R}^{>0}} \overline{x} = \frac{1}{|x|^2} x\overline{x} = \frac{1}{|x|^2}|x|^2 = 1$$

und ebenso auch $\frac{1}{|x|^2}\overline{x}x = 1$. □

3.2 Nullstellen von Polynomen innerhalb der Quaternionen

10.12.20

In diesem Abschnitt betrachten wir einige bemerkenswerte Eigenschaften von Lösungen von Polynomen innerhalb der Quaternionen. Man sollte die folgende Aussage mit Folgerung 2.9 kontrastieren: ein komplexes Polynom $f(t) \in \mathbf{C}[t]$ mit $\deg f = n$ hat höchstens n Nullstellen (und genau n wenn wir sie entsprechend ihrer Vielfachheiten zählen).

Satz 3.7. Sei $a \in \mathbf{H}$. Das Polynom $t^n - a$ hat Nullstellen in jeder Ebene $V \subset \mathbf{H}$ (d.h. jedem 2-dimensionalen $\mathbf{R}$-Untervektorraum), die 0, 1, und a enthält.

Die Menge dieser Nullstellen, d.h. $\{x \in \mathbf{H}, x^n - a = 0\}$, ist endlich falls

- $a = 0$ (und n beliebig). In diesem Fall ist $x = 0$ die einzige Nullstelle.
- $n = 1$ und $a \in \mathbf{R}, a \neq 0$. In diesem Fall ist $x = a$ die einzige Nullstelle in $\mathbf{H}$.
- $n = 2$ und $a \in \mathbf{R}, a > 0$. In diesem Fall sind die reellen Nullstellen dieses Polynoms auch gleichzeitig die Nullstellen in $\mathbf{H}$.
- $\Im a \neq 0$ (und n beliebig). In diesem Fall hat das Polynom genau n Nullstellen.

Ansonsten ist die Menge dieser Nullstellen *unendlich*.

Bevor wir dies beweisen, führen wir eine allgemeine Sprechweise ein:

Definition 3.8. Sei V eine Algebra. Eine Teilmenge $W \subset V$ heißt *Unteralgebra* von V, wenn folgende Bedingungen erfüllt sind:

- W ist ein Untervektorraum von V,
- $1 \in W$,
- für $v, v' \in W$ ist auch $vv' \in W$.

Beispiel 3.9.

- Jede Unteralgebra $W \subset V$ einer Algebra ist selbst wieder (nach Definition!) eine Algebra.
- $\mathbf{R}$ ist eine Unteralgebra von $\mathbf{C}$.

- $\mathbf{C}$, aufgefasst als die Menge der Quaternionen der Form

$$\begin{pmatrix} a+ib & 0 \\ 0 & a-ib \end{pmatrix} \in \mathbf{H}$$

ist ebenfalls eine Unteralgebra von $\mathbf{H}$. Letzteres prüft man durch eine explizite Rechnung (vgl. auch Übungsaufgabe 3.1) nach.

- Für jedes $x \in \mathbf{H}$ sei $A := \langle 1, x\rangle$ der von 1 und x erzeugte $\mathbf{R}$-Untervektorraum. Dieser Untervektorraum ist automatisch eine Unteralgebra. Hierzu genügt es (wegen der $\mathbf{R}$-Linearität der Multiplikation) zu sehen, dass $x^2 \in A$ gilt. Dies folgt aus (3.5).

U.a. um Unteralgebren der Quaternionen zu verstehen, ist folgendes Lemma nützlich:

Lemma 3.10. Sei V eine assoziative Algebra mit $n := \dim_{\mathbf{R}} V < \infty$. Wir setzen voraus, dass V keine Nullteiler hat (Definition 2.19). Dann hat jedes $x \in V$, $x \neq 0$ ein Inverses. Folglich ist V ein Schiefkörper.

Falls überdies V kommutativ ist, so ist V ein Körper und es besteht ein Algebren-Isomorphismus

$$V \cong \mathbf{R}$$

oder

$$V \cong \mathbf{C}.$$

Beweis. Wir argumentieren wie im Beweis von Theorem 2.11: Die Elemente

$$1 = x^0, x, x^2, x^3, \ldots, x^n \in V$$

sind $n+1$ Elemente im $\mathbf{R}$-Vektorraum V. Damit müssen sie $\mathbf{R}$-linear abhängig sein, d.h. es gibt $a_0, \ldots, a_n \in \mathbf{R}$, nicht alle gleich 0, mit

$$a_0x^0 + a_1x + \cdots + a_nx^n = 0.$$

Sei $k \geqslant 0$ der niedrigste Index so dass $a_k \neq 0$, d.h. es gilt

$$a_kx^k + \cdots + a_nx^n = (a_k + \cdots + a_nx^{n-k})x^k = 0.$$

(Wir benutzen rechts die Assoziativität von V in Form von $x^rx^s = x^{r+s}$, Übungsaufgabe 2.16.) Da V keine Nullteiler hat, folgt aus $x \neq 0$ auch $x^k \neq 0$(!) , und damit aus der vorigen Gleichheit $a_k + \cdots + a_nx^{n-k} = 0$. Dies liefert

$$-a_k^{-1}(a_{k+1} + \cdots + a_nx^{n-k-1}) \cdot x = 1.$$

Außerdem gilt

$$x \cdot a_k^{-1}(a_{k+1} + \cdots + a_nx^{n-k-1}) = a_k^{-1}(a_{k+1} + \cdots + a_nx^{n-k-1}) \cdot x,$$

denn $xa = ax$ für $a \in \mathbf{R}$(!) und $xx^n = x^{n+1} = x^nx$ (s.o.). Dies zeigt, dass x ein multiplikatives Inverses hat.

Die Aussage im kommutativen Fall ist dann eine Wiederholung von Theorem 2.27. □

Eine weitere Vorbereitung betrifft die Frage, welche Unteralgebren von $\mathbf{H}$ isomorph zu den komplexen Zahlen sind:

Lemma 3.11. Seien $x, y \in \mathbf{H}$. Dann sind äquivalent:

(1) Es gibt eine Teilalgebra $A \subset \mathbf{H}$ (d.h. eine Teilmenge, mit $0, 1 \in A$, so dass Produkte und Summen von Elementen in A wieder in A liegen), mit $x, y \in A$ und einen Algebra-Isomorphismus $A \xrightarrow{\varphi} \mathbf{C}$.

(2) $1, x, y$ sind $\mathbf{R}$-linear abhängig.

(3) $xy = yx$.

Beweis. (1) $\Rightarrow$ (2): da $\dim_{\mathbf{R}} \mathbf{C} = 2$, sind die Elemente $\{\varphi(1) = 1, \varphi x, \varphi y\}$ $\mathbf{R}$-linear abhängig. Da φ ein $\mathbf{R}$-linearer(!) Isomorphismus ist, sind auch $\{1, x, y\}$ in A, und damit auch in $\mathbf{H}$ linear abhängig.

(2) $\Rightarrow$ (3): sei $\lambda \cdot 1 + \mu x + \nu y = 0$ eine lineare Abhängigkeit, d.h. $\lambda, \mu, \nu \in \mathbf{R}$ und nicht alle drei Koeffizienten seien 0. Falls $\nu \neq 0$, so gilt also $y = -\frac{\lambda + \mu x}{\nu}$ und damit

$$xy = -x\frac{\lambda + \mu x}{\nu} = -\frac{x\lambda + x\mu x}{\nu} = -\frac{\lambda x + \mu x^2}{\nu} = yx.$$

Analog zeigt man dies für $\mu \neq 0$. Falls $\mu = \nu = 0$ gilt, so folgt $\lambda \cdot 1 = 0$, hieraus $\lambda = 0$, im Widerspruch dazu, dass nicht alle drei Koeffizienten 0 sind.

(3) $\Rightarrow$ (1): Sei $B := \{a + bx + cy + dxy | a, b, c, d \in \mathbf{R}\} \subset \mathbf{H}$. Dann ist B eine Unteralgebra. Um dies zu sehen, genügt es zu prüfen, dass die Produkte der vier Erzeuger $\{1, x, y, xy\}$ jeweils wieder in B liegen: Es gilt $yx = xy \in B$ nach Voraussetzung (3). Wegen (3.5) (und $(xy)^2 = x^2y^2$, wegen (3))) gilt $x^2, y^2, (xy)^2 \in B$. Ebenfalls aus (3.5) folgt $x^2y \in \langle 1, x\rangle y \subset B$ und ebenso sieht man auch $yxy = xyy = xy^2 \in B$. Ebenfalls aus diesen Berechnungen folgt, dass B kommutativ ist. Als Unteralgebra von $\mathbf{H}$ ist B assoziativ und hat keine Nullteiler. Natürlich gilt $\dim_{\mathbf{R}} B \leqslant \dim_{\mathbf{R}} \mathbf{H} = 4 < \infty$, d.h. wir erhalten aus Lemma 3.10 entweder einen (Algebren-)Isomorphismus $B \cong \mathbf{R}$ oder $B \cong \mathbf{C}$. Im zweiten Fall sind wir direkt fertig, d.h. $A := B$. Im ersten Fall gilt also $x, y \in \mathbf{R}$, und wir können ein beliebiges Element $z \in \mathbf{H}\backslash B$ wählen und die Algebra $A := \{a + bz | a, b \in \mathbf{R}\}$ erfüllt dann die Behauptung. □

Beweis. (von Satz 3.7). Laut Beispiel 3.9 ist eine solche Ebene V automatisch eine Unter*algebra*. Laut Lemma 3.11 gibt es einen Algebren-Isomorphismus

$$\varphi : V \xrightarrow{\cong} \mathbf{C}.$$

Sei $b := \varphi(a) \in \mathbf{C}$. Das Polynom $t^n - b$ hat n komplexe Nullstellen $z_1, \ldots, z_n$ (falls $b \neq 0$ sind diese alle verschieden, ansonsten ist 0 eine n-fache Nullstelle). Damit sind $\varphi^{-1}(z_k) \in V \subset \mathbf{H}$ Nullstellen des Polynoms $t^n - a$, d.h. $(\varphi^{-1}(z_k))^n - a = 0$.

(1) Falls $a = 0$ so folgt aus der Produktformel: für eine Nullstelle x gilt $0 = |x^n| = |x|^n$, damit $|x| = 0$ und damit $x = 0$. In diesem Fall gibt es also nur die Nullstelle $x = 0$.

(2) Falls $\Im a = 0$, d.h. $a \in \mathbf{R} \subset \mathbf{H}$, aber $a \neq 0$. Es gibt dann unendlich viele verschiedene Ebenen V, die 0, 1 und a enthalten. Falls $n > 2$ und $a \neq 0$ oder falls $n = 2$ und $a < 0$ so enthält jede dieser Ebenen eine Nullstelle, die *nicht* in $\mathbf{R}(\subset V)$ liegt. Damit erhalten wir dann unendlich viele Nullstellen. Hierzu nutzen wir nochmals den Isomorphismus φ; beachte, dass $\varphi|_{\mathbf{R}} = \mathrm{id}$. In der obigen Notation gilt insbesondere $b = a$. Die Nullstellen von $t^n - a$, die in $\mathbf{C}\backslash\mathbf{R}$ liegen, sind via φ in Bijektion zu den Nullstellen von $t^n - a$, die in $V\backslash\mathbf{R}$ liegen. Ersteres Polynom hat für $n > 2$ (und $a \neq 0$) oder für $n = 2$ und $a < 0$ Nullstellen in $\mathbf{C}\backslash\mathbf{R}$.

(3) Für $n = 1$ (und $a \in \mathbf{R}$, $a \neq 0$ beliebig) oder $n = 2$ (und $a \in \mathbf{R}$, $a > 0$) hat das Polynom nur reelle Nullstellen: sei $x \in \mathbf{H}$ eine Nullstelle. Es gibt eine zu $\mathbf{C}$ isomorphe Unteralgebra $V \subset \mathbf{H}$, die x enthält (Lemma 3.11). Die Nullstellen von $t^n - a$ in V (diese enthalten insbesondere x) sind in Bijektion zu den Nullstellen von $t^n - a$ in $\mathbf{C}$. Hier hat das Polynom (unter den genannten Bedingungen an n und a) aber nur Nullstellen in $\mathbf{R}$. Damit sind die Nullstellen in $\mathbf{H}$ automatisch reell.

(4) Sei nun $\Im a \neq 0$ und $x \in \mathbf{H}$ eine Nullstelle, d.h. $x^n = a$. Sei $A = \langle 1, a\rangle \subset \mathbf{H}$. Wir werden zeigen:

$$x \in A. \tag{3.12}$$

Dies liefert die Behauptung, denn $\dim_{\mathbf{R}} A = 2$ (wegen $a \notin \mathbf{R}$). Damit gibt es einen Algebren-Isomorphismus $\varphi : A \xrightarrow{\cong} \mathbf{C}$. Das Polynom $t^n - \varphi(a)$ hat genau n Nullstellen in $\mathbf{C}$, damit hat $t^n - a$ ebenfalls genau n Nullstellen in A (und damit wegen der Behauptung auch in $\mathbf{H}$). Um (3.12) zu sehen, betrachte die Unteralgebra $B := \langle 1, x\rangle \subset \mathbf{H}$. Falls $x \in \mathbf{R}$ ist (3.12) klar. Ansonsten ist B ebenfalls eine 2-dimensionale Unter-Algebra. Wegen $a = x^n \in B$ (da B Unteralgebra!) gilt $A \subset B$ und damit aus Dimensionsgründen $A = B$, d.h. $x \in A$. □

Wir beenden dieses Thema mit der Erwähnung des "Fundamentalsatzes der Algebra" für Quaternionen. Wir werden den Satz nicht beweisen, da dies tieferliegende Methoden z.B. aus der algebraischen Topologie erfordert. Zur Formulierung: wir nennen ein *Monom* einen Ausdruck der Form 16.12.20

$$a_1 t^{n_1} a_2 t^{n_2} a_3 \dots a_r t^{n_r} a_{r+1},$$

wobei die $a_k \in \mathbf{H}\backslash\{0\}$. Der *Grad* eines solchen Monoms ist definiert als $n := \sum n_k$. Ein *Polynom mit Koeffizienten in* $\mathbf{H}$ ist definiert als eine endliche Summe von Monomen.

Theorem 3.13. Sei $p(t)$ ein Polynom mit Koeffizienten in $\mathbf{H}$. Wir nehmen an $p = m + q$, wobei m ein *Monom* (im Gegensatz zu einem Polynom) vom Grad $n > 0$ und q ein Polynom vom Grad $< n$ ist. Dann hat p eine Nullstelle (in $\mathbf{H}$).

Bemerkung 3.14. Die Voraussetzung, dass im Grad n nur ein Monom (und kein Polynom) auftaucht, ist notwendig. Z.B. hat $p(t) = it - ti + 1$ *keine* Nullstelle in $\mathbf{H}$ (vgl. **??**).

3.3 Geometrische Eigenschaften

Definition 3.15. Die *n-Sphäre* ist

$$S^n := \{(x_1, \dots, x_{n+1}) \in \mathbf{R}^{n+1}, \sum_{k=1}^{n+1} x_k^2 = 1\}.$$

Für $n = 0$ ist $S^0 = \{\pm 1\}$ (versehen mit der Multiplikation) eine Gruppe. Die wichtige Rolle der

$$S^1 = \{z \in \mathbf{C}, |z| = 1\}$$

im Kontext der Geometrie der komplexen Zahlen haben wir in §2, beispielsweise beim Beweis des Fundamentalsatzes der Algebra (Theorem 2.6, Übungsaufgabe 2.1) kennen gelernt.

Für die Geometrie der Quaternionen übernimmt S^3 eine ähnlich wichtige Rolle, wegen

$$S^3 = \{x \in \mathbf{H}, |x| = 1\}.$$

Insbesondere zeigen diese beiden Identifikationen (sowie die Produktformel (3.4)), dass S^1 und S^3 Gruppen sind, d.h. für $n = 1, 3$ gibt es eine Multiplikationsabbildung

$$S^n \times S^n \to S^n, \tag{3.16}$$

so dass die Gruppenaxiome (Existenz eines neutralen Elements, Existenz von Inversen, Assoziativität der Multiplikation) gelten. Überdies ist diese Multiplikationsabbildung stetig (sogar differenzierbar). Dieses Muster setzt sich jedoch *nicht* fort: ein tiefliegender Satz von Adams [**Adams:Non-existence**] besagt, dass $S^0 := \{\pm 1\}$, S^1 und S^3 unter den Sphären S^n die *einzigen* Gruppen sind, deren Multiplikation stetig ist. Ein Beweis dieser Aussage ist weit jenseits unserer Reichweite in dieser Vorlesung. Unser Ziel in diesem Abschnitt ist es, die geometrischen Eigenschaften der Quaternionen in Bezug auf Drehungen im Raum genauer zu verstehen.

Aus der linearen Algebra bekannt sind die folgenden Gruppen. Für uns interessant sind im folgenden vor allem SU(2) und O(3).

Definition 3.17. Die folgenden Gruppen heißen *orthogonale Gruppe*, *spezielle orthogonale Gruppe*, *unitäre Gruppe* sowie *spezielle unitäre Gruppe*:

$$\begin{aligned} \mathrm{O}(n) &:= \{A \in \mathrm{Mat}_{n\times n}(\mathbf{R}), AA^T = \mathrm{id}\}, \\ \mathrm{SO}(n) &:= \{A \in \mathrm{O}(n), \det A = 1\}, \\ \mathrm{U}(n) &:= \{A \in \mathrm{Mat}_{n\times n}(\mathbf{C}), A\overline{A}^T = \mathrm{id}\}, \\ \mathrm{SU}(n) &:= \{A \in \mathrm{U}(n), \det A = 1\}. \end{aligned}$$

(Hierbei bezeichnet $\overline{A}$ die Matrix, die aus element-weisem Konjugieren entsteht und T bezeichnet die transponierte Matrix; id bezeichnet die $n \times n$-Identitätsmatrix.)

In niedrigen Dimensionen kann man die Elemente von $\mathrm{SO}(n)$ und $\mathrm{O}(n)$ laut Übungsaufgabe 3.8 explizit wie folgt beschreiben:

$$\mathrm{SO}(2) = \left\{ R_\alpha := \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} | \alpha \in \mathbf{R} \right\}.$$

Linksmultiplikation mit einer solchen Matrix liefert eine Abbildung

$$\mathbf{R}^2 \to \mathbf{R}^2, x \mapsto R_\alpha \cdot x,$$

die durch Drehung (gegen den Uhrzeigersinn) um den Winkel α gegeben ist. Drehungen (um den Ursprung) in $\mathbf{R}^2$ werden durch Elemente von S^1 gegeben, wobei die Komposition zweier Drehungen gerade der (komplexen) Multiplikation von Elementen in S^1 entspricht.

Lemma 3.18. Die Abbildung

$$\varphi : S^1 \to \mathrm{SO}(2), z \mapsto \begin{pmatrix} \Re z & -\Im z \\ \Im z & \Re z \end{pmatrix}$$

ist ein Gruppenisomorphismus von abelschen Gruppen. (Hierbei ist die Gruppenoperation in S^1 die Multiplikation, die in $\mathrm{SO}(2)$ die Matrix-Multiplikation.)

Der Beweis dieses Lemmas ist eine Übungsaufgabe (Übungsaufgabe 3.8). Er orientiert sich am Beweis der folgenden Aussage:

Lemma 3.19. Die beiden folgenden Teilmengen von $\mathrm{Mat}_{2\times 2}(\mathbf{C})$ stimmen überein:

$$\mathrm{SU}(2) = \{x \in \mathbf{H}, \det x = 1\}.$$

Vermöge der üblichen Identifikation $\mathbf{R}^4 \cong \mathbf{H}$ (gegeben durch $e_1 \mapsto 1$, $e_2 \mapsto i$, $e_3 \mapsto j$, $e_4 \mapsto k$) besteht außerdem eine Gleichheit

$$S^3 = \{x \in \mathbf{H}, \det x = 1\}.$$

Beweis. Zunächst zur ersten Gleichheit: "$\subseteq$": für $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SU}(2)$ gilt (wegen $A\overline{A}^T = \mathrm{id}$) $A^{-1} = \overline{A}^T = \begin{pmatrix} \overline{a} & \overline{c} \\ \overline{b} & \overline{d} \end{pmatrix}$. Andererseits gilt für jede 2×2-Matrix mit Determinante 1: $A^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$, also $d = \overline{a}$, $c = -\overline{b}$, d.h. $A = \begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix} \in \mathbf{H}$.

(!) "$\supseteq$": umgekehrt, für eine solche Matrix A prüft man(!) durch explizites Nachrechnen

$$A\overline{A}^T = \det A \cdot \mathrm{id}.$$

Hieraus folgt die umgekehrte Inklusion "$\supseteq$".

Zur zweiten Behauptung: nach Definition gilt für $x = \begin{pmatrix} w & -z \\ \overline{z} & \overline{w} \end{pmatrix}$: $\det x = w\overline{w} + z\overline{z} = |w|^2 + |z|^2$, wobei hier $|-|$ der Absolutbetrag einer komplexen Zahl ist. Mittels des obigen Standard-Isomorphismus $\mathbf{R}^4 \overset{\varphi}{\cong} \mathbf{H}$ übersetzt sich dies gerade in $\det(x) = \sum_{n=1}^4 x_n^2$, wobei $w = x_1 + ix_2$, $z = x_3 + ix_4$. Es gilt also $|x|^2 := \sum_{n=1}^4 x_n^2 = \det x$, d.h. wir erhalten die zweite Behauptung. □

Definition 3.20. Für $x \in \mathbf{H}$, $x \neq 0$ bezeichnen wir die folgende Abbildung als *Konjugation*:

$$\Im\mathbf{H} \xrightarrow{h_x} \Im\mathbf{H},$$
$$u \mapsto xux^{-1} \quad (= \frac{1}{|x|^2} xu\overline{x})$$

(Beachte, dass die Abbildung in der Tat Werte in $\Im\mathbf{H}$ annimmt, denn es gilt

$$\Re(x(ux^{-1}) = \Re((ux^{-1})x) = \Re(u),$$

wobei wir die Tatsache

$$\Re(xy) = \langle x, y\rangle = \langle y, x\rangle = \Re(yx) \tag{3.21}$$

für $x, y \in \mathbf{H}$ benutzt haben, siehe den Beweis von Definition und Lemma 3.3.)

Wir werden i.d.R. die üblichen Identifikationen

$$\mathbf{R}^3 \cong \Im\mathbf{H}, \mathbf{R}^4 \cong \mathbf{H}$$

vornehmen. Auf diese Weise werden wir h_x auch als Abbildung

$$h_x : \mathbf{R}^3 \to \mathbf{R}^3$$

bzw. auch als reelle 3×3-Matrix ansehen.

Unser Ziel in diesem Abschnitt ist das folgende Theorem. Hierbei ist die Gruppenstruktur auf S^3 durch die Multiplikation von Quaternionen gegeben (siehe (3.16)) und $S^3 \times S^3$ wird zu einer Gruppe durch komponentenweise Multiplikation, d.h. 13.1.21

$$(z_1, z_2)(w_1, w_2) := (z_1 w_1, z_2 w_2).$$

Theorem 3.22. Die Abbildungen

$$\begin{aligned} \mathrm{SU}(2) = S^3 &\xrightarrow{\varphi} \mathrm{SO}(3), \\ x &\mapsto (h_x : \Im\mathbf{H} \ni t \mapsto xtx^{-1} = xt\overline{x} \in \Im\mathbf{H}) \end{aligned}$$

$$\begin{aligned} \mathrm{SU}(2) \times \mathrm{SU}(2) = S^3 \times S^3 &\xrightarrow{\psi} \mathrm{SO}(4), \\ (x, y) &\mapsto (\mathbf{H} \ni t \mapsto xt\overline{y} \in \mathbf{H}) \end{aligned}$$

sind surjektive Gruppenhomomorphismen. Die Kerne haben jeweils zwei Elemente, nämlich

$$\begin{aligned} \ker\varphi &= \{\pm 1_{\mathbf{H}}\} \\ \ker\psi &= \{\pm(1_{\mathbf{H}}, 1_{\mathbf{H}})\}. \end{aligned} \tag{3.23}$$

Hierbei bezeichnet $1_{\mathbf{H}}$ das Einselement (welches unter dem obigen Isomorphismus auf den Vektor $(1,0,0,0) \in \mathbf{R}^4$ abgebildet wird.)

Mit anderen Worten: da die Elemente von SO(3) gerade die Drehungen (um den Ursprung) im $\mathbf{R}^3$ angeben, lassen sich die Quaternionen (von Norm 1) nutzen, um alle Drehungen zu beschreiben und die Komposition von Drehungen entspricht der Multiplikation von Quaternionen. Überdies gibt es nur eine geringe Ambiguität, d.h. bis auf den Faktor ± 1 ist die Beschreibung von Drehungen mittels Quaternionen auf die obige Weise auch eindeutig.

Um den Nutzen von letzterer Eigenschaft zu sehen, betrachten wir (anstatt $\varphi : S^3 \to \mathrm{SO}(3)$) die Abbildung

$$\mu : S^1 \times S^1 \times S^1 \cong \mathrm{SO}(2) \times \mathrm{SO}(2) \times \mathrm{SO}(2) \to \mathrm{SO}(3),$$

$$(z, z', z'') \mapsto (A, A', A'') \mapsto \begin{pmatrix} 1 & & \\ & \cos\alpha & -\sin\alpha \\ & \sin\alpha & \cos\alpha \end{pmatrix} \cdot \begin{pmatrix} \cos\alpha' & & -\sin\alpha' \\ & 1 & \\ \sin\alpha' & & \cos\alpha' \end{pmatrix} \cdot \begin{pmatrix} \cos\alpha'' & -\sin\alpha'' & \\ \sin\alpha'' & \cos\alpha'' & \\ & & 1 \end{pmatrix}.$$

Hierbei ist $A = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}$ etc. Die erste 3×3-Matrix gibt eine Drehung in der y-z-Ebene in $\mathbf{R}^3$ an, die die x-Achse festhält. Die zweite hält analog die y-Achse fest, die dritte die z-Achse. Man kann zeigen, dass diese Abbildung *surjektiv* ist, d.h. jede Drehung in $\mathbf{R}^3$ lässt sich als Komposition von Drehungen um die x-, y- und z-Achse durchführen.

Betrachte die Restriktion von μ, wo $\alpha' = -\frac{\pi}{2}$ auf die Matrix $A' = \begin{pmatrix} & & 1 \\ & 1 & \\ -1 & & \end{pmatrix}$, d.h. die Abbildung,

die $(A, A'') \in \mathrm{SO}(2) \times \mathrm{SO}(2)$ auf folgende Matrix abbildet:

$$\begin{pmatrix} 1 & & \\ & \cos\alpha & -\sin\alpha \\ & \sin\alpha & \cos\alpha \end{pmatrix} \cdot \begin{pmatrix} & & 1 \\ & 1 & \\ -1 & & \end{pmatrix} \cdot \begin{pmatrix} \cos\alpha'' & -\sin\alpha'' & \\ \sin\alpha'' & \cos\alpha'' & \\ & & 1 \end{pmatrix}$$
$$\stackrel{*}{=} \begin{pmatrix} & & 1 \\ \sin\alpha\cos\alpha'' + \cos\alpha\sin\alpha'' & \cos\alpha\cos\alpha'' - \sin\alpha\sin\alpha'' & \\ \sin\alpha\sin\alpha'' - \cos\alpha\cos\alpha'' & \sin\alpha\cos\alpha'' + \cos\alpha\sin\alpha'' & \end{pmatrix}$$
$$= \begin{pmatrix} & & 1 \\ \sin(\alpha+\alpha'') & \cos(\alpha+\alpha'') & \\ -\cos(\alpha+\alpha'') & \sin(\alpha+\alpha'') & \end{pmatrix}.$$

(!) (Die Gleichung * bestätigt man schnell (!) mittels einer elementaren Rechnung.) Insbesondere ist das Bild dieser Einschränkung von μ nicht 2-dimensional, sondern nur 1-dimensional (da das Bild nur von $\alpha'' + \alpha$ abhängt). Andererseits ist $\mathrm{SO}(2) \times \mathrm{SO}(2) = S^1 \times S^1$ zwei-dimensional, d.h. die Abbildung μ hat nicht die schöne Eigenschaft (wie φ oben!), dass jeweils genau 2 Elemente das gleiche Bild haben. In physikalischen Anwendungen, z.B. bei der Navigation von Raumschiffen, spielt dieses Problem eine praktische Rolle (sog. *gimbal lock*): hier entspricht die Möglichkeit der Multiplikation von 3 Matrizen gerade der Benutzung von drei Rotationsfreiheitsgraden (durch entsprechende Triebwerke). Die obige Rechnung besagt, dass ein Raumschiff in gewissen (isolierten) Positionen nur noch einen Freiheitsgrad in der Navigation hat.

Nach diesem Ausflug wenden wir uns dem Beweis von Theorem 3.22 zu.

Lemma 3.24. Die Abbildungen φ und ψ nehmen in der Tat Werte in $\mathrm{SO}(3)$ bzw. $\mathrm{SO}(4)$ an.

Beweis. Wir zeigen zunächst, dass es sich um orthogonale Abbildungen handelt. Fixiere $x, y \in S^3$ und schreibe kurz $\psi := \psi(x, y)$. A priori ist ψ eine lineare Abbildung $\psi : \mathbf{H} \to \mathbf{H}$. Wir prüfen die Orthogonalitätsbedingung: für $t, t' \in \mathbf{H}$ gilt

$$\langle \psi(t), \psi(t') \rangle = \langle t, t' \rangle.$$

In der Tat:

$$\begin{aligned} \langle \psi(t), \psi(t') \rangle &= \langle xt\overline{y}, xt'\overline{y} \rangle \\ &= \Re(xt\overline{y}\overline{xt'\overline{y}}) \\ &\stackrel{*}{=} \Re(xt \underbrace{\overline{y}y}_{=|y|^2=1} \overline{t'}\overline{x}) \\ &\stackrel{**}{=} \Re(xt\overline{t'}\overline{x}) \\ &= \Re(t\overline{t'} \underbrace{\overline{x}x}_{=1}) \\ &= \langle t, t' \rangle. \end{aligned}$$

Bei * wurde die Produktformel benutzt, bei ** die obige Gleichung (3.21). In Matrizenschreibweise haben wir gezeigt: ψ nimmt Werte in $\mathrm{O}(4)$ an.

Es gilt

$$\mathrm{O}(4) = \mathrm{SO}(4) \sqcup \mathrm{O}^-(4),$$

wobei $\mathrm{O}^-(4) := \{A \in \mathrm{O}(4), \det A = -1\}$. Es gilt $\psi(1_{\mathbf{H}}, 1_{\mathbf{H}}) = \mathrm{id}$, insbesondere liegt ein Element von $\mathrm{SO}(4)$ im Bild von ψ. Die Komposition

$$S^3 \times S^3 \stackrel{\psi}{\to} \mathrm{O}(4) \stackrel{\det}{\to} \{\pm 1\}$$

ist eine *stetige Abbildung*, da dies sowohl auf die Determinante als auch auf ψ zutrifft; letztere ist ja Einschränkung einer bilinearen und damit stetigen Abbildung $\mathbf{R}^4 \times \mathbf{R}^4 \to \mathrm{Mat}_{4\times 4}(\mathbf{R})$. Angenommen es gäbe ein $(x, y) \in S^3 \times S^3$ mit $\psi(x, y) \in \mathrm{O}^-(4)$. Der topologische Raum S^3 ist wegzusammenhängend, d.h. es gibt eine stetige Abbildung $\gamma : [0, 1] \to S^3$ mit $\gamma(0) = 1_{\mathbf{H}} (\in S^3)$ und $\gamma(1) = x$. Ebenso gibt es auch einen Weg δ, der $1_{\mathbf{H}}$ mit y verbindet. Die Komposition

$$[0, 1] \stackrel{\gamma\times\delta}{\to} S^3 \times S^3 \stackrel{\psi}{\to} \mathrm{O}(4) \stackrel{\det}{\to} \{\pm 1\}$$

ist also eine *stetige* Abbildung, die 0 auf $\det \mathrm{id} = 1$ abbildet, und 1 auf -1. Da die Funktion aber nur die Werte $+1$ und -1 annimmt, ist dies ein Widerspruch zum Zwischenwertsatz!

Dies zeigt die Behauptung für ψ. Für φ argumentiert man entweder analog oder nutzt die Tatsache $\varphi(x) = \psi(x, x)$. □

Lemma 3.25. φ und ψ sind Gruppenhomomorphismen mit Kernen wie in (3.23) behauptet.

Beweis. Es gilt

$$\begin{aligned}\big(\psi(x,y) \circ \psi(x',y')\big)(t) &= \psi(x,y)(x't\overline{y'}) \\ &= xx't\overline{y'}\overline{y} \\ &\overset{*}{=} (xx')t\overline{yy'} \\ &= \psi(xx', yy')(t).\end{aligned}$$

Bei * haben wir die Formel aus Übungsaufgabe 3.1 verwendet.

Sei nun $x \in \ker \varphi$, d.h. $t = xtx^{-1}$ für alle $t \in \Im\mathbf{H}$. Da diese Gleichung (unabhängig von x) auch für $t \in \mathbf{R}$ gilt, gilt diese Gleichung also für alle $t \in \mathbf{H}$, d.h. $x \in Z(\mathbf{H})$ (das Zentrum). Laut Übungsaufgabe 3.15 ist $Z(\mathbf{H}) = \mathbf{R}$. Andererseits ist $x \in S^3$, d.h. $x \in S^3 \cap \mathbf{R} \cdot e_1 = \{\pm e_1\} = \{\pm 1_{\mathbf{H}}\}$.

Sei $(x, y) \in \ker \psi$, d.h. $t = xt\overline{y}$ für alle $t \in \mathbf{H}$. Insbesondere folgt mit $t = 1$: $x = \overline{y}^{-1} = y$, d.h. $x \in \ker \varphi = \{\pm 1\}$. □

Um die Surjektivität von φ und ψ zu zeigen, verwenden wir folgende Aussage, deren Beweis eine Übungsaufgabe ist (Übungsaufgabe 3.11):

Satz 3.26. (*Satz von Cartan*) Sei $a \in \mathbf{R}^n$, mit $|a|^2 (:= \sum_{k=1}^n a_k^2) = 1$. Wir betrachten die *Spiegelungen*

$$s_a : \mathbf{R}^n \to \mathbf{R}^n, x \mapsto x - 2\langle a, x\rangle a.$$

Die Gruppe $\mathrm{O}(n)$ wird von diesen Spiegelungen erzeugt.

Der Name "Spiegelung" rührt daher, dass das orthogonale Komplement von a, d.h. die Hyperebene $\{x \in \mathbf{R}^n, \langle x, a\rangle = 0\}$ unter s_a elementweise festgelassen wird. Außerdem gilt $s_a(a) = -a$, d.h. s_a ist in der Tat die Spieglung an der Geraden die durch a aufgespannt wird.

Lemma 3.27. Für $x, y \in \mathbf{H}$ gilt folgende *Dreifach-Produktformel*

$$yxy = 2\langle \overline{x}, y\rangle y - \langle y, y\rangle \overline{x}. \tag{3.28}$$

Beweis. Wir haben $\langle x, y\rangle = \frac{1}{2}(x\overline{y} + y\overline{x})$ (entweder durch explizites Nachrechnen oder wegen der Bilinearität von $\langle -, -\rangle$)). Rechtsmultiplikation mit y liefert die Behauptung wegen $\overline{y}y = \langle y, y\rangle$. □

Wir wenden die Spiegelungen nun auf $\mathbf{H} \cong \mathbf{R}^4$ an. Aus (3.28) folgt

$$s_a(x) = -a\overline{x}a$$

für alle $a \in S^3$ und $x \in \mathbf{H}$. Insbesondere gilt $s_e(x) = -\overline{x}$. Bezeichne für $a \in S^3$

$$p_a : \mathbf{H} \to \mathbf{H}, x \mapsto axa.$$

Dann folgt aus der obigen Gleichung (für $a, b \in S^3$)

$$s_a \circ s_b = p_a \circ p_{\overline{b}}.$$

Insbesondere gilt $p_a = s_a \circ s_e$.

Wir nutzen dies und die obige Beschreibung der Erzeuger von $\mathrm{O}(4)$ (Satz 3.26) und halten fest: die Gruppe $\mathrm{O}(\mathbf{H}) = \mathrm{O}(4)$ wird von den Elementen p_a (für $a \in S^3$) und s_e erzeugt.

Folgerung 3.29. Die Abbildungen φ und ψ sind surjektiv.

Beweis. Wir beginnen mit der Surjektivität von ψ. Jedes $f \in \mathrm{SO}(4)$ ist Produkt von Elementen der Form $p_{a_1} \circ \cdots \circ p_{a_n}$ mit gewissen $a_1, \ldots, a_n \in S^3$. In der Tat: nach dem vorigen Satz ist zunächst f eine Komposition von Abbildungen der Form s_a und s_a^{-1}, wobei $a \in S^3$. Wegen $s_a^2 = \mathrm{id}$ gilt $s_a^{-1} = s_a$, d.h. $f = s_{a_1} \circ \cdots \circ s_{a_n}$ für gewisse $a_1, \ldots, a_n \in S^3$. Es gilt $\det(s_a) = -1$, demnach $\det f = (-1)^n$. Wegen $f \in \mathrm{SO}(4)$ ist n also gerade. Nach obiger Gleichung ist f ein Produkt der p_{a_k} bzw. $p_{\overline{a_k}}$. (Man kann darüber hinaus zeigen, dass man $n = 4$ wählen kann, aber dies wird in der Folge nicht gebraucht).

Setze $a := a_1 a_2 \ldots a_n$ und $b := a_n a_{n-1} \ldots a_1$. Dann ist (da $S^3 = \{x \in \mathbf{H}, |x| = 1\}$ eine Gruppe ist) $a, b \in S^3$ und

$$f(x) = axb.$$

Sei nun $g \in \mathrm{SO}(\Im\mathbf{H}) = \mathrm{SO}(3)$. Betrachte die eindeutige lineare Abbildung

$$f : \mathbf{H} \to \mathbf{H}$$

die die Identität auf $\mathbf{R} \subset \mathbf{H}$ und auf $\Im\mathbf{H}$ mit g übereinstimmt. Es gilt $\det f = \det g = 1$. Es gibt also (wegen der Surjektivität von ψ) $a, b \in S^3$ mit $f(x) = axb$. Wegen $1 = f(1) = ab$ folgt $b = a^{-1} = \overline{a}$, d.h. $g(x) = axa^{-1}$ für alle $x \in \Im\mathbf{H}$. Also: $g = \varphi(a)$. □

3.4 Der Satz von Frobenius

20.1.21 Der folgende Satz von Frobenius ist eine Erweiterung von Theorem 2.27. Letzteres ist die parallele Aussage für Körper (im Gegensatz zu Schiefkörpern).

Theorem 3.30. (*Satz von Frobenius*) Sei K ein Schiefkörper mit $\mathbf{R} \subset K$ und

$$n := \dim_{\mathbf{R}} K < \infty.$$

Dann tritt genau eine der folgenden drei Möglichkeiten ein:

(1) $n = 1$. In diesem Fall gibt es einen Algebren-Isomorphismus $K \xrightarrow{\cong} \mathbf{R}$.

(2) $n = 2$. In diesem Fall gibt es einen Algebren-Isomorphismus $K \xrightarrow{\cong} \mathbf{C}$.

(3) $n = 4$. In diesem Fall gibt es einen Algebren-Isomorphismus $K \xrightarrow{\cong} \mathbf{H}$.

Beweis. (nach [Pal68]) Wie üblich fassen wir $\mathbf{R}$ als Teilalgebra von K via dem injektiven (Lemma 2.25) Algebren-Homomorphismus

$$\mathbf{R} \to K, r \mapsto r \cdot 1$$

auf.

Falls $n = 1$, so ist dieser automatisch auch noch surjektiv (da beides *endlich-dimensionale* $\mathbf{R}$-Vektorräume mit der gleichen Dimension sind), also ein Isomorphismus.

Bevor wir den Fall $n > 1$ betrachten, halten wir eine allgemeine Beobachtung fest: sei $x \in K$ und betrachte die Teilmenge

$$\mathbf{R}\langle x\rangle := \{\sum_{k=0}^{n} a_k x^k | n \geqslant 0, a_k \in \mathbf{R}\} \subset K.$$

Offensichtlich(!) ist $\mathbf{R}\langle x\rangle$ eine Unteralgebra von K. (Man nennt sie die von x in K *erzeugte Algebra*.) K (nach Voraussetzung) und damit auch $\mathbf{R}\langle x\rangle$ ist assoziativ. Dann ist $\mathbf{R}\langle x\rangle$ nach Lemma 3.10 ein Schiefkörper. Überdies ist $\mathbf{R}\langle x\rangle$ (möglicherweise im Gegensatz zu K) kommutativ, denn:

$$\begin{aligned}
(\sum a_k x^k)(\sum b_l x^l) &= \sum_{k,l} a_k x^k b_l x^l \\
&\overset{*}{=} \sum_{k,l} a_k b_l x^k x^l \\
&\overset{**}{=} \sum_{k,l} a_k b_l x^l x^k \\
&\overset{*}{=} \sum_{k,l} b_l x^l a_k x^k \\
&= (\sum b_l x^l)(\sum a_k x^k).
\end{aligned}$$

Wir haben hier (in *) benutzt, dass für jedes $a \in \mathbf{R}$ und jedes $y \in K$ gilt: $ay = ya$ (dies ist ein Spezialfall des Distributivitätsgesetzes). In ** haben wir die Gleichheit $x^n x^m = x^{n+m}$ benutzt, die in jeder assoziativen Algebra gilt (Übungsaufgabe 2.16). Also ist $\mathbf{R}\langle x\rangle$ ein Körper. Wir erhalten aus Theorem 2.27 (beachte, dass dies letztlich eine Folgerung aus dem Fundamentalsatz der Algebra ist!) entweder einen Isomorphismus $\mathbf{C} \cong \mathbf{R}\langle x\rangle$ oder einen Isomorphismus $\mathbf{R} \cong \mathbf{R}\langle x\rangle$. Ersteres tritt genau dann ein, wenn $x \in K\backslash\mathbf{R}$ gilt. Letzteres tritt genau dann ein, wenn $x \in \mathbf{R}$ gilt.

Sei nun $n > 1$. Dann können wir ein $x \in K\backslash\mathbf{R}$ wählen. Betrachte den oben diskutierten Körper + Isomorphismus

$$\mathbf{C} \cong \mathbf{R}\langle x\rangle.$$

Bezeichne mit $\underline{i} \in \mathbf{R}\langle x\rangle (\subset K)$ das Bild von $i \in \mathbf{C}$ unter diesem Isomorphismus. Es gilt also(!) $\underline{i}^2 = -1$. Wir betrachten K nun als $\mathbf{C}$-Vektorraum, vermöge der Multiplikation *von links*. Andererseits bezeichne

$$T : K \to K, t \mapsto t\underline{i}$$

die Multiplikation mit $\underline{i}$ *von rechts*. Es handelt sich hierbei um eine $\mathbf{C}$-lineare Abbildung, denn $T(\lambda t) = \lambda t\underline{i} = \lambda T(t)$. Es gilt dann $T^2 (:= T \circ T) = -\mathrm{id}_K$. Die einzigen möglichen (komplexen!) Eigenwerte von T sind also $\pm i$. Sei $K^{\pm} := \{t \in K, T(t) = \pm it\}$ der Eigenraum zum Eigenwert $\pm i$. Anders gesagt:

$$\begin{aligned} K^+ &= \{t \in K, T(t) = it\} \\ &= \{t \in K, t\underline{i} = \underline{i}t\} \\ K^- &= \{t \in K, \underline{i} = -\underline{i}t\}. \end{aligned}$$

Es gilt $K = K^+ \oplus K^-$: offensichtlich ist $K^+ \cap K^- = 0$ und jedes Element $x \in K$ erfüllt

$$x = \underbrace{\frac{x - \underline{i}x\underline{i}}{2}}_{\in K^+} + \underbrace{\frac{x + \underline{i}x\underline{i}}{2}}_{\in K^-}.$$

Nach Definition von $K^{\pm}$ gilt

$$\begin{aligned} x, y \in K^- &\Rightarrow xy \in K^+, \\ x, y \in K^+ &\Rightarrow xy \in K^+. \end{aligned} \tag{3.31}$$

Es gilt $K^+ = \mathbf{R}\langle x\rangle$: "$\supset$" gilt da $\mathbf{R}\langle x\rangle$ kommutativ ist. Sei umgekehrt $t \in K^+$, d.h. t kommutiert mit $\underline{i}$ und natürlich mit allen $r \in \mathbf{R}$. Damit kommutiert t auch mit allen Elementen von $\mathbf{R}\langle x\rangle$. Folglich ist die Teilmenge

$$\mathbf{R}\langle t, x\rangle := \left\{ \sum_{k,l \geqslant 0} a_{kl} t^k x^l \right\}$$

eine *kommutative Unteralgebra* von K und damit ein Körper. Er enthält den Körper $\mathbf{R}\langle x\rangle$. Nach Theorem 2.27 und aus Dimensionsgründen müssen beide Körper den Grad 2 haben und damit übereinstimmen. Folglich gilt $t \in \mathbf{R}\langle x\rangle$, d.h. $K^+ \subset \mathbf{R}\langle x\rangle$.

Falls $K^- = 0$, so gilt also $K = \mathbf{R}\langle x\rangle (\cong \mathbf{C})$. Es bleibt zu zeigen: falls $K^- \neq 0$, so ist $K \cong \mathbf{H}$. Wenn $K^- \neq 0$, so können wir $\alpha \in K^-, \alpha \neq 0$ wählen.

Die Rechts-Multiplikation

$$K \to K, x \mapsto x\alpha$$

ist ein Isomorphismus (nach Lemma 3.10), der K^- auf K^+ abbildet (wegen (3.31)). Aus diesem Isomorphismus erhalten wir

$$\dim_{\mathbf{C}} K^- = 1. \tag{3.32}$$

Wir zeigen nun:

$$\alpha^2 \in \mathbf{R},\ \alpha^2 < 0. \tag{3.33}$$

Wir haben die Inklusionen

$$K^+ = \mathbf{R}\langle x\rangle \subset K \supset \mathbf{R}\langle \alpha\rangle.$$

Hierbei sind sowohl ($\mathbf{C} \cong$)K^+ als auch $\mathbf{R}\langle\alpha\rangle$ Teilkörper von K. Ihre Dimension (als $\mathbf{R}$-Vektorraum) ist jeweils 2. Wie bereits oben für K können wir daher auch rechts einen Isomorphismus wählen und erhalten folgendes Bild:

$$\mathbf{C} \cong K^+ = \mathbf{R}\langle x\rangle \subset K \supset \mathbf{R}\langle\alpha\rangle \cong \mathbf{C}.$$

Also ist auch $K^+ \cap \mathbf{R}\langle\alpha\rangle$ ein Körper, genauer ein Teilkörper von $\mathbf{R}\langle\alpha\rangle$. Aus Dimensionsgründen kann dies nur entweder $\mathbf{R}\langle\alpha\rangle$ oder $\mathbf{R}$ sein. Im ersteren Fall wäre also $K^+ \cap \mathbf{R}\langle\alpha\rangle = \mathbf{R}\langle\alpha\rangle$, d.h. $\mathbf{R}\langle\alpha\rangle \subset K^+$, insbesondere $\alpha \in K^+$ im Widerspruch zur Wahl von α. Also gilt $K^+ \cap \mathbf{R}\langle\alpha\rangle = \mathbf{R}$ und damit insbesondere $\alpha^2 \in \mathbf{R}$.

Betrachte den oben erwähnten Isomorphismus $\rho : \mathbf{R}\langle\alpha\rangle \xrightarrow{\cong} \mathbf{C}$, sei $z := \rho(\alpha)$. Es gilt

$$z^2 = \rho(\alpha)^2 = \rho(\alpha^2) = \alpha^2 \in \mathbf{R},$$

denn $\alpha^2 \in \mathbf{R}$ und $\rho|_{\mathbf{R}} = \mathrm{id}$. Andererseits ist $z \notin \mathbf{R}$ (wegen $\alpha \notin \mathbf{R}$). Hieraus folgt $z \in \Im\mathbf{C}$, d.h. $z^2 = \alpha^2 < 0$.

Aus (3.33) folgt: ein geeignetes positives Vielfaches $\underline{j} = \lambda\alpha \in K^-$ (mit $\lambda \in \mathbf{R}^{>0}$) erfüllt $\underline{j}^2 = -1$. Setze $\underline{k} := \underline{i}\underline{j}$. Wir betrachten die eindeutige $\mathbf{R}$-lineare Abbildung

$$\varphi : \mathbf{H} \to K,$$

die $1 \mapsto 1$, $i \mapsto \underline{i}$, $j \mapsto \underline{j}$, $k \mapsto \underline{k}$ erfüllt.

Wegen (3.32) ist $\{\underline{j}, \underline{k}\}$ eine $\mathbf{R}$-Basis von K^-, also sind $1, \underline{i}, \underline{j}, \underline{k}$ eine Basis von K, d.h. φ ist ein Isomorphismus von $\mathbf{R}$-Vektorräumen. Es ist überdies ein Isomorphismus von Algebren. Hierzu genügt es zu zeigen
(!) $\varphi(x)\varphi(y) = \varphi(xy)$ für $x, y \in \{i, j, k\}$(!) . Für $x = i$, $y = j$ ist dies gerade die Definition von $\underline{k} = \varphi(k) = \varphi(ij)$. Für $x = j$, $y = i$ folgt dies aus $\underline{j} \in K^-$, d.h. $\underline{i}\underline{j} = -\underline{j}\underline{i}$. Falls x oder $y = k$ sind, so benutzen wir die Assoziativität in beiden Algebren, z.B.

$$\varphi(i)\varphi(k) = \underline{i}\underline{k} = \underline{i}(\underline{i}\underline{j}) = (\underline{i}\underline{i})\underline{j} = -\underline{j} = \varphi(-j) = \varphi(ik).$$

3.5 Übungsaufgaben

Übungsaufgabe 3.1. Bestätige folgende Multiplikationsregeln in $\mathbf{H}$:

$$ij = k, ji = -k.$$

Nutze dies und die Assoziativität der Multiplikation um eine Multiplikationstabelle zu vervollständigen:

	1	i	j	k
1				
i			k	
j		$-k$		
k				

Berechne

$$(a + ib + jc + kd)(a' + ib' + jc' + kd')$$

wobei a, a' etc. in $\mathbf{R}$.

Bestätige folgende Formel (Tipp: wie kann man den Rechenaufwand minimieren?) für $x, y \in \mathbf{H}$ und $\overline{x}$ die Konjugation von x im Sinne von Definition und Lemma 3.3

$$\overline{x \cdot y} = \overline{y} \cdot \overline{x}.$$

Übungsaufgabe 3.2. Sei V eine Algebra. Wie üblich bezeichnen wir die Addition in V mit $+$ und die Multiplikation mit $\cdot$. Definiere eine Abbildung

$$\star : V \times V \to V, x \star y := \frac{1}{2}(x \cdot y + y \cdot x).$$

Zeige, dass $(V, +, \star)$ eine kommutative Algebra ist (d.h. anstelle von $\cdot$ wird nun $\star$ als Multiplikation verwendet).

Wir betrachten nun spezieller die Algebra $(\mathbf{H}, +, \star)$. Bestimme $x \star y$ für $x, y \in \{1, i, j, k\}$. Ist $\mathbf{H}$, versehen mit $\star$ als Multiplikation assoziativ?

Übungsaufgabe 3.3. Seien $x, y \in \mathbf{H}$ derart, dass

$$xy \neq yx.$$

Zeige, dass für jede Unteralgebra $V \subset \mathbf{H}$ mit $x, y \in V$ schon gilt:

$$V = \mathbf{H}.$$

Tipp: wende den Satz von Frobenius an.

Übungsaufgabe 3.4. Welche der beiden Abbildungen sind Algebren-Homomorphismen?

$$\begin{aligned} \mathbf{H} &\xrightarrow{?} \mathbf{H}, \\ x &\mapsto \overline{x} \end{aligned}$$

$$\begin{aligned} \mathbf{C} &\to \mathbf{H}, \\ z &\mapsto \overline{z} \end{aligned}$$

wobei in der zweiten Abbildung $\overline{z}$ als Quaternion aufgefasst wird, d.h. als $\begin{pmatrix} \overline{z} & 0 \\ 0 & \overline{\overline{z}} \end{pmatrix} = \begin{pmatrix} \overline{z} & 0 \\ 0 & z \end{pmatrix}$. Gib jeweils detailliert an, welche der Eigenschaften eines Algebren-Homomorphismus erfüllt und welche ggf. nicht erfüllt sind.

Übungsaufgabe 3.5.

- Betrachte die Abbildung:

$$- \times - : \Im\mathbf{H} \times \Im\mathbf{H} \to \Im\mathbf{H}, (u, v) \mapsto u \times v := \frac{1}{2}(uv - vu).$$

  Bestätige, dass diese Abbildung in der Tat Werte in $\Im\mathbf{H}$ annimmt.

  Bemerkung: via der Standardidentifikation $\mathbf{R}^3 \cong \Im\mathbf{H}$, $e_1 \mapsto i, e_2 \mapsto j, e_3 \mapsto k$ ist diese Abbildung gerade das *Kreuzprodukt*.

- Zeige für $u, v \in \Im\mathbf{H}$

$$uv = u \times v - \langle u, v \rangle,$$

  wobei $\langle -, - \rangle$ das Skalarprodukt auf $\mathbf{H}$ ist.

- Seien $u, v \in \Im\mathbf{H}$. Zeige $uv = -vu$ genau dann, wenn $\langle u, v \rangle = 0$.

Übungsaufgabe 3.6. Sei $x \in \mathbf{H}$. Zeige, dass die Abbildung

$$\mathbf{H} \to \mathbf{H}, a \mapsto [a, x] := ax - xa$$

Werte in $\Im\mathbf{H} := \{\Im y, y \in \mathbf{H}\} \subset \mathbf{H}$ annimmt.

Folgere hieraus die Aussage in Bemerkung 3.14.

Übungsaufgabe 3.7. Unter einem *Gitter* verstehen wir das Bild einer Abbildung

$$\mathbf{Z}^n \to \mathbf{R}^n, x \mapsto Ax,$$

wobei $A \in \mathrm{GL}_n(\mathbf{R})$. Schreibe dann Γ_A für dieses Bild.

- Wir betrachten die Teilmenge
$$\Lambda := \mathbf{Z}^4 \cup (\mathbf{Z} + \frac{1}{2})^4 \subset \mathbf{R}^4$$
(d.h. $(x_1, \ldots, x_4)$ ist in Λ enthalten, wenn entweder alle $x_i \in \mathbf{Z}$ oder alle $x_i - \frac{1}{2} \in \mathbf{Z}$). Zeige, dass diese Teilmenge ein Gitter in $\mathbf{R}^4$ ist. Man nennt dies das sog. *D_4-Gitter*. Vervollständige hierzu die Matrix
$$A = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ * & * & * & * \\ * & * & * & * \\ * & * & * & * \end{pmatrix}.$$

- Wir verwenden die übliche Identifikation $\varphi : \mathbf{R}^4 \cong \mathbf{H}$, $e_1 \mapsto 1$, $e_2 \mapsto i$, $e_3 \mapsto j$, $e_4 \mapsto k$. Zeige, dass $\varphi(\Lambda)$ eine Unteralgebra von $\mathbf{H}$ ist. (An dieser Stelle, im Gegensatz zu unserer allgemeinen Definition in Definition 3.8, fordern wir für eine Unteralgebra nur, dass sie eine Untergruppe bezüglich der Addition, nicht jedoch ein $\mathbf{R}$-Untervektorraum sein soll. Alle anderen Bedingungen an eine Unteralgebra bleiben unverändert.) Man nennt diese Unteralgebra auch die *Hurwitz-Quaternionen*.

- Bestimme
$$\mu := \min_{\gamma \in \Lambda, \gamma \neq 0} |\gamma|.$$

- Wir betrachten die *Kugelpackung*, d.h. die Teilmenge
$$\{x \in \mathbf{R}^4, |x - \gamma| \leqslant \frac{\mu}{2} \text{ für ein } \gamma \in \Lambda\}.$$
Die *Dichte dieser Kugelpackung* ist definiert als
$$\frac{V_4(\mu)}{\mu^4 |\det A|}.$$
Hierbei ist $V_n(\mu)$ das Volumen des n-dimensionalen Balls mit Durchmesser μ, d.h. das Volumen von $\{x \in \mathbf{R}^n, |x| \leqslant \mu/2\}$.
Weshalb nennt man diese Zahl Dichte der Kugelpackung? Gib, mit Hilfe einer geeigneten Formel für V_n, die hier nicht bewiesen werden muss, die obige Dichte numerisch an.

Bemerkung: Es ist bekannt, dass das obige Gitter die dichteste Kugelpackung, die von einem Gitter in $\mathbf{R}^4$ ausgeht ist. Die Frage nach den dichtesten Kugelpackungen in $\mathbf{R}^n$ ist in Dimensionen 1, 2, 3, 8 und 24 vollständig verstanden, aber für allgemeine n weitgehend ungeklärt.

Übungsaufgabe 3.8. Bestätige die Aussage von Lemma 3.18:

- Zeige zunächst, dass es sich um einen Gruppenhomomorphismus handelt, d.h. dass $\varphi(zz') = \varphi(z)\varphi(z')$ gilt.
- Zeige dass $\ker \varphi = \{1\}$ und folgere die Injektivität von φ.
- Zeige die Surjektivität durch explizites Rechnen mithilfe der definierenden Gleichung $\mathrm{SO}(2) := \{A \in \mathrm{Mat}_{2\times 2} | AA^T = \mathrm{id}, \det A = 1\}$.

Übungsaufgabe 3.9. Bestimme die (unendliche!) Menge
$$\{x \in \mathbf{H}, x^2 = -1\}.$$

Übungsaufgabe 3.10. In dieser Aufgabe soll der Beweis von Theorem 3.30 nachvollzogen werden.

(1) Beschreibe die Unteralgebra $\mathbf{R}\langle x \rangle$ für $x = i + j (\in \mathbf{H})$ explizit.

(2) Gib einen expliziten Isomorphismus $\sigma : \mathbf{C} \xrightarrow{\cong} \mathbf{R}\langle x \rangle$ an.

(3) Bestimme $\underline{i} := \sigma(i)$.

(4) Gib die lineare Abbildung $\mathbf{H} \to \mathbf{H}$, $x \mapsto \underline{i}x$ sowie $x \mapsto x\underline{i}$ in Termen der Standard-Basis $1, i, j, k$ an.

(5) Bestimme die Eigenraumzerlegung für die Abbildung $T : x \mapsto x\underline{i}$.

(6) Wähle ein möglichst bequemes $\alpha \notin \mathbf{R}\langle i + j\rangle$ und gib den Isomorphismus

$$\varphi : \mathbf{H} \to \mathbf{H}$$

an, der im Beweis konstruiert wurde.

Übungsaufgabe 3.11. Zeige, dass jedes Element in $\mathrm{O}(n)$ ein Produkt von höchstens n Spiegelungen ist.

Tipp: führe einen Induktionsbeweis durch. Im Induktionsschritt betrachte (für $A \in \mathrm{O}(n)$): falls $A \neq \mathrm{id}$, betrachte $v \in \mathbf{R}^n$ mit $Av \neq v$, wähle $\lambda \in \mathbf{R}$ so dass für $u := \lambda(v - Av)$ gilt: $|u| = 1$. Betrachte die Komposition $s_u \circ f$.

Übungsaufgabe 3.12. Stelle die folgenden Abbildungen

$$\mathbf{H} \to \mathbf{H}, x \mapsto -x$$

$$\mathbf{H} \to \mathbf{H}, x \mapsto ix$$

jeweils als Komposition geeigneter s_a bzw. auch als Komposition geeigneter p_a (wobei jeweils $a \in S^3$) dar.

Übungsaufgabe 3.13.

- Sei A eine endlich-dimensionale assoziative Algebra. Zeige, dass folgende Aussagen äquivalent sind:
  (1) A hat keine Nullteiler,
  (2) Jedes $a \in A\backslash\{0\}$ hat ein multiplikatives Inverses.
- Fixiere $\epsilon \in \mathbf{R}^{>0}$. Wir betrachten die Algebra $\mathbf{H}_\epsilon$, die als Vektorraum von der Basis $1, i, j, k$ aufgespannt wird und deren Multiplikationstabelle auf Basisvektoren $1, i, j, k$ wie folgt gegeben ist:

	1	i	j	k
1	1	i	j	k
i	i	$-1+\epsilon j$	k	$-j$
j	j	$-k$	-1	i
k	k	j	$-i$	-1

  D.h. die Multiplikation von $\mathbf{H}_\epsilon$ stimmt mit der gewöhnlichen Multiplikation in $\mathbf{H}$ überein, bis auf

$$i^2 = -1 + \epsilon j.$$

Zeige: $\mathbf{H}_\epsilon$ hat für genügend kleines ϵ keine Nullteiler. Zeige, dass i *kein* multiplikatives Inverses hat.

Die Algebra $\mathbf{H}_\epsilon$ zeigt, dass ohne die Assozativität die Implikation (1) $\Rightarrow$ (2) nicht gilt. Auch die umgekehrte Implikation gilt ohne Assoziativität nicht, dies sieht man z.B. anhand der Sedenionen (Übungsaufgabe 4.12, diese sind laut Übungsaufgabe 4.3 eine gut normierte *-Algebra und hat daher inbesondere multiplikative Inverse).

3.6 Präsenzaufgaben für die Übungen

Übungsaufgabe 3.14. Sei $x \in \Im\mathbf{H}$. Zeige

$$x^2 = -|x|^2.$$

Tipp: es ist möglich, dies direkt mittels $x = bi + cj + dk$ nachzuprüfen. Wie geht es auch ohne konkrete Rechnung?

Übungsaufgabe 3.15. Zeige für das Zentrum von $\mathbf{H}$:

$$Z(\mathbf{H}) = \mathbf{R}.$$

Bemerkung: das Zentrum einer assoziativen Algebra (im Sinne der Definition 2.17) enthält stets $\mathbf{R}$. Eine Algebra, deren Zentrum nicht größer ist, d.h. $Z(A) = \mathbf{R}$, heißt *zentrale Algebra*. In dieser Terminologie sind die Quaternionen also eine zentrale Algebra.

Welche andere zentrale Algebra kennst du?

Übungsaufgabe 3.16. Zeige die Implikation (1) $\Rightarrow$ (3) in Lemma 3.11 direkt (d.h. ohne den Zwischenschritt via (2)).

Übungsaufgabe 3.17. Zeige, dass es keinen Algebren-Isomorphismus

$$\mathbf{C} \times \mathbf{C} \to \mathbf{H}$$

gibt. Hierbei bezeichnet ist links die Algebra gemeint, deren Addition und Multiplikation komponentenweise definiert ist, d.h. $(z_1, z_2) \cdot (z_1', z_2') := (z_1 z_1', z_2 z_2')$.

Tipp: verwende Übungsaufgabe 2.25.

Übungsaufgabe 3.18. Sei $V = \{a + b(i + j) | a, b \in \mathbf{R}\}$. Zeige dass es sich bei $V \subset \mathbf{H}$ um eine Unteralgebra handelt und gib einen Algebren-Isomorphismus

$$V \cong \mathbf{C}$$

an.

Übungsaufgabe 3.19. Gilt die Gleichheit

$$\mathrm{U}(2) \stackrel{?}{=} \{x \in \mathbf{H}, x \neq 0\}$$

Gib an (und begründe), welche der beiden Inklusionen "$\subseteq$" und "$\supseteq$" gelten bzw. nicht gelten.

Übungsaufgabe 3.20. Sei $x \in \Im\mathbf{H}$. Zeige

$$x^2 = -|x|^2.$$

Tipp: es zwar ist möglich, dies direkt mittels $x = bi + cj + dk$ nachzuprüfen, aber wie geht es auch ohne konkrete Rechnung?

Übungsaufgabe 3.21. Eine Teilmenge $V \subset \mathbf{R}^n$ heißt *wegzusammenhängend*, wenn es für je zwei Punkte $x_0, x_1 \in V$ eine *stetige* Abbildung

$$\gamma : [0, 1] \to V$$

gibt mit $\gamma(0) = x_0$, $\gamma(1) = x_1$.

Für welche $n \geqslant 0$ ist S^n wegzusammenhängend?

Übungsaufgabe 3.22. In leichter Abwandlung von Definition 3.20 verwenden wir in dieser Aufgabe folgende Notation: für $x \in \mathbf{H}\backslash 0$ ist

$$h_x : \mathbf{H} \to \mathbf{H}, t \mapsto xtx^{-1}.$$

Zeige dass die Abbildung

$$\mathbf{H}\backslash 0 \to \mathrm{End}(\mathbf{H}), x \mapsto h_x$$

ein Gruppenhomomorphismus ist. Bestimme dessen Kern und Bild.

Übungsaufgabe 3.23. Definiere die Abbildungen $\Re$, $\Im$, $\overline{-}$, $|-|^2$ und $\langle -, - \rangle$ (vgl. Definition und Lemma 3.3) allein in Termen der Spiegelung

$$s_1 : \mathbf{H} \to \mathbf{H}.$$

Kapitel 4

Die Oktonionen

4.1 Definition

Die Oktonionen sind die natürliche Fortsetzung der Reihe

$$\mathbf{R} \subset \mathbf{C} \subset \mathbf{H}.$$

Wir definieren sie mit Hilfe der sog. Dickson-Konstruktion, für die wir zunächst einige Grundbegriffe einführen. 27.1.21

Definition 4.1. Eine **-Algebra* ist eine Algebra A (im Sinne von Definition 2.17) versehen mit einer *Involution*, d.h. einer $\mathbf{R}$-linearen Abbildung

$$* : A \to A$$

derart, dass folgende Bedingungen gelten (hierbei sind $a, b \in A$ beliebig)
(1) $a^{**} := (a^*)^* = a$,

(2) $(ab)^* = b^* a^*$,

(3) $1^* = 1$.
Die *-Algebra heißt *reell*, wenn $* = \mathrm{id}$, d.h. $a^* = a$ für alle $a \in A$.

Beispiel 4.2. Auf $\mathbf{R}$, $\mathbf{C}$, $\mathbf{H}$ ist die Konjugation jeweils eine Involution. Die Bedingungen sind jeweils trivial nachzuprüfen, bis auf (2) für $\mathbf{H}$, d.h. $\overline{xy} = \overline{y} \cdot \overline{x}$ für $x, y \in \mathbf{H}$, siehe hierzu Übungsaufgabe 3.1. Nach Definition ist $\mathbf{R}$ eine reelle $*$-Algebra, die übrigen jedoch nicht.

Jede reelle *-Algebra ist kommutativ: $ab = (ab)^* = b^* a^* = ba$.

Definition und Lemma 4.3. Sei $(A, *)$ eine *-Algebra. Die *Dickson-Konstruktion* ist die folgende *-Algebra $(A', *)$: als $\mathbf{R}$-Vektorraum

$$A' := A \oplus A.$$

Die Multiplikation von Elementen in A' ist gegeben durch

$$(a_1, b_1) \cdot (a_2, b_2) = (a_1 a_2 - b_2 b_1^*, a_1^* b_2 + a_2 b_1). \tag{4.4}$$

(Wir setzen nicht voraus, dass A kommutativ ist, insbesondere ist die Reihenfolge der Faktoren rechts wesentlich, siehe hierzu auch +!) Die Involution $*$ auf A' ist definiert als

$$(a, b)^* := (a^*, -b).$$

Mit diesen Definitionen ist $(A', *)$ in der Tat eine *-Algebra und die Inklusion

$$\iota : A \to A', a \mapsto (a, 0)$$

ist ein Homomorphismus von *-Algebren (d.h. ein Algebrenhomomorphismus und es gilt $\iota(a)^* = \iota(a^*)$).

Beweis. Das Nachprüfen der Axiome einer Algebra sowie der Bedingungen in Definition 4.1 ist eine gute Wiederholung(!) . □

Beispiel 4.5. Betrachte $A = \mathbf{R}$ (und $* = \mathrm{id}$). Also ist $\mathbf{R}' = \mathbf{R}^2$ mit der Multiplikation

$$(a_1, b_1) \cdot (a_2, b_2) = (a_1a_2 - b_2b_1, a_1b_2 + a_2b_1),$$

d.h.

$$\mathbf{R}' = \mathbf{C},$$

versehen mit $*$, der üblichen komplexen Konjugation.

Betrachte $A = \mathbf{C}$ (und $*$ der üblichen komplexen Konjugation). Dann ist $\mathbf{C}' = \mathbf{C}^2$ (als Vektorraum), mit der Multiplikation (mit $a_1 \in \mathbf{C}$ etc.)

$$(a_1, b_1) \cdot (a_2, b_2) = (a_1a_2 - b_2\overline{b_1}, \overline{a_1}b_2 + a_2b_1).$$

Die Abbildung

$$\mathbf{C}' \to \mathbf{H}, (a, b) \mapsto \begin{pmatrix} a & \overline{b} \\ -b & \overline{a} \end{pmatrix}$$

ist ein *Algebren*-Isomorphismus, denn das Produkt der Quaternionen

$$\begin{pmatrix} a_1 & \overline{b_1} \\ -b_1 & \overline{a_1} \end{pmatrix}\begin{pmatrix} a_2 & \overline{b_2} \\ -b_2 & \overline{a_2} \end{pmatrix} = \begin{pmatrix} a_1a_2 - \overline{b_1}b_2 & a_1\overline{b_2} + \overline{b_1}\overline{a_2} \\ -b_1a_2 - \overline{a_1}b_2 & -b_1\overline{b_2} + \overline{a_1}\ \overline{a_2} \end{pmatrix}$$

stimmt mit dem obigen Produkt überein. Unter diesem Isomorphismus stimmt die abstrakt definierte Abbildung * auf $\mathbf{C}'$ mit der Konjugation in $\mathbf{H}$ überein.

Definition 4.6. Die *Oktonionen* sind die folgende *-Algebra:

$$\mathbf{O} := \mathbf{H}',$$

d.h. die Dickson-Konstruktion der Quaternionen.

Bemerkung 4.7. Die Multiplikation in $\mathbf{O}$ lässt sich direkt anhand der Definition explizit ablesen, siehe Übungsaufgabe 4.5.

Wir erhalten also folgende Kette von Algebren

$$\mathbf{R} \mapsto \mathbf{R}' = \mathbf{C} \mapsto \mathbf{C}' = \mathbf{H} \mapsto \mathbf{H}' =: \mathbf{O} \mapsto \dots.$$

Die Dimension (als $\mathbf{R}$-Vektorraum) verdoppelt sich in jedem Schritt. Man kann diese Konstruktion immer wieder ausführen, d.h. erhält eine unendliche Kette von Algebren der Dimension $1, 2, 4, 8, 16, \dots$. Je höher die Dimensionen dieser Dickson-Konstruktionen jedoch werden, desto "schlechter" verhalten sich die Algebren. Daher betrachtet man die Algebren ab der Dimension 16 nur wenig (vgl. Übungsaufgabe 4.12). Diesen Verlust an "guten" Eigenschaften macht Satz 4.12 deutlich.

Wir verschaffen uns vorab einige grundlegende Rechenregeln innerhalb der Dickson-Konstruktion. Zur Abkürzung schreiben wir

$$\ell := (0, 1) \in A'.$$

Vermöge der injektiven Abbildung $\iota : A \to A'$ (s.o.) fassen wir Elemente in A auch als Elemente in A' auf.

Lemma 4.8. Innerhalb der Dickson-Konstruktion A' gelten folgende Rechenregeln (für alle $a, b \in A$):

$$\begin{aligned} a(\ell b) &= \ell(a^*b) \\ (a\ell)b &= (ab^*)\ell \\ (\ell a)(b\ell) &= -(ab)^*. \end{aligned} \tag{4.9}$$

Beweis. Dies zeigt man durch direktes Nachprüfen anhand der Definition. □

Lemma 4.10. Es gilt (für alle $a, b \in A$)

$$a\ell = \ell a^* \tag{4.11a}$$
$$(\ell a)b = \ell(ba) \tag{4.11b}$$
$$(\ell a)(\ell b) = -ba^*. \tag{4.11c}$$

Beweis. Die erste Gleichheit folgt aus (4.4) (vgl. auch (4.9))

$$a\ell = (a,0)(0,1) = (0,a) = (0,1)(a^*,0) = \ell a^*.$$

$$(\ell a)b \overset{(4.11a)}{=} (a^*\ell)b \overset{(4.9)}{=} (a^*b^*)\ell \overset{(4.11a)}{=} \ell(a^*b^*)^* = \ell(ba).$$

$$(\ell a)(\ell b) \overset{(4.11a)}{=} (\ell a)(b^*\ell) \overset{(4.9)}{=} -(ab^*)^* = -ba^*.$$

Satz 4.12. Sei A eine *-Algebra sowie A' ihre Dickson-Konstruktion.

(1) A' ist nie reell.

(2) A ist reell (und damit kommutativ) genau dann, wenn A' kommutativ ist.

(3) A ist kommutativ und assoziativ genau dann, wenn A' assoziativ ist.

Beweis. Die erste Aussage ist klar, denn das Element $(0,1) \in A'$ erfüllt $(0,1)^* = (0,-1)$. Generell ist nach Definition A eine Unteralgebra von A', d.h. ist z.B. A' kommutativ, dann auch A.

(2): dies ist eine direkte Folgerung von $(\ell a)\ell \overset{(4.11c)}{=} -a^*$, und damit

$$a^* = (\ell a)\ell^{-1} = -(\ell a)\ell.$$

Damit gilt $a = a^*$ genau dann, wenn $\ell a = a\ell$. Dies zeigt sofort die Richtung "$\Leftarrow$". Umgekehrt, genügt es die Kommutativitätsbedingung $xy = yx$ (für $x, y \in A'$) in 3 Fällen zu zeigen: a) $x = \ell$, $y \in A$ (obige Rechnung), b) $x = y = \ell$ (trivial), c) $x \in A$, $y = \ell$ (obige Rechnung).

(3): es gilt für $a, b \in A$

$$(\ell a)b - \ell(ab) \overset{(4.11b)}{=} \ell(ba) - \ell(ab) = \ell(ba - ab).$$

Dies zeigt sofort die Richtung $\Leftarrow$.

Zu "$\Rightarrow$": es gilt

$$(\ell a)(\ell b) - \ell(a(\ell b)) \overset{(4.9)}{=} -ba^* - \ell(\ell(a^*b)) \overset{(4.11c)}{=} -ba^* + a^*b.$$

Es genügt die Assoziativitätsbedingung $L_x \circ L_y = L_{xy}$ (für $x, y \in A'$) in den Fällen a) $x = \ell$, $y \in A$, $y = \ell$ b) $x = y = \ell$ und c) $x \in A$ zu prüfen; der allgemeine Fall folgt dann aus der Linearität der Multiplikation (Übungsaufgabe 4.4) sowie der Tatsache, dass jedes Element in A' von der Form $a + b\ell$ mit $a, b \in A$ ist. Der Teil a) und c) ist gerade die obige Rechnung. Der Fall b), d.h. $x = y = \ell$ ist ein Spezialfall von (4.11c). □

Satz 4.12 besagt, dass **O** *nicht* assoziativ ist, denn **H** ist zwar assoziativ, jedoch nicht kommutativ. (Man kann dies auch schon der Gleichung (4.11b) ablesen.) Um eine Aussage zu treffen, inwieweit die Assoziativität zumindest noch eingeschränkt gilt, führen wir folgende weitere Begriffe ein.

Definition 4.13. Eine *-Algebra heißt *gut normiert*, wenn für alle $a \in A$ gilt: $a + a^* \in \mathbf{R}$ sowie für alle $a \in A, a \neq 0$: $aa^* = a^*a \in \mathbf{R}^{>0}$.

Für eine gut normierte Algebra A definieren wir *Realteil* und *Imaginärteil*:

$$\Re(a) := \frac{a + a^*}{2} (\in \mathbf{R}), \Im(a) := \frac{a - a^*}{2} (\in A)$$

sowie die *Norm*:

$$|a| := \sqrt{aa^*} (\in \mathbf{R}^{\geq 0}).$$

Für $A = \mathbf{R}$, $\mathbf{C}$ oder $\mathbf{H}$ stimmen diese Begriffe mit den uns bereits bekannten (siehe u.a. Definition und Lemma 3.3) überein.

Nach Definition einer Algebra liegt $\mathbf{R}$ jeweils im Zentrum einer jeden Algebra A, d.h. $\lambda x = x\lambda$ für alle
3.2.21 $\lambda \in R$ und $x \in A$. In der Situation einer gut normierten *-Algebra gilt daher

$$xx^* = xx^* + x^2 - x^2 = x(x^* + x) - x^2 \overset{!}{=} (x^* + x)x - x^2 = x^*x + x^2 - x^2 = x^*x. \tag{4.14}$$

Mit anderen Worten: die Kommutativität $xx^* = x^*x$ folgt aus den übrigen Bedingungen an eine gut normierte *-Algebra. Dies sichert ein Minimum an Kommutativität; man vergleiche dies mit dem Begriff einer *normalen Matrix* (bzw. eines *normalen Endomorphismus*), d.h. Matrizen $M \in \mathrm{Mat}_{n\times n}(\mathbf{C})$, die die Eigenschaft

$$MM^* = M^*M$$

erfüllen.

Beispiel 4.15. $\mathrm{Mat}_{n\times n}(\mathbf{C})$, versehen mit der Abbildung $* : M \mapsto M^* := (\overline{M})^T$ (eintragsweise komplexe Konjugation und anschließend Transposition der Matrix), ist eine *-Algebra. Sie ist jedoch nicht gut normiert, denn i.A. sind weder $M + M^*$ noch MM^* von der Form $\lambda \cdot \mathrm{id}$ mit $\lambda \in \mathbf{R}$.

Als Abschwächung der Assoziativität führen wir folgende Variante ein:

Definition 4.16. Eine Algebra A heißt *alternativ*, wenn folgende Bedingungen (für beliebige $a, b \in A$) gelten:

$$(aa)b = a(ab), \quad (ab)a = a(ba), \quad (ba)a = b(aa).$$

Nun können wir eine Aussage über den "Verfall" der Assoziativität im Zuge der Dickson-Konstruktion treffen:

Satz 4.17. Sei A eine *-Algebra sowie A' ihre Dickson-Konstruktion. Dann gilt: A ist assoziativ und gut normiert genau dann, wenn A' alternativ ist und gut normiert.

Folgerung 4.18. Die Oktonionen sind

▌ alternativ, aber nicht assoziativ.

Beweis. (von Satz 4.17) Wir benutzen Übungsaufgabe 4.3: A ist gut normiert genau dann, wenn A' es ist. Wir müssen also (unter dieser Voraussetzung) zeigen:

$$A \text{ assoziativ genau dann wenn } A' \text{ alternativ.}$$

Die Richtung "⇒" kann man mit einer expliziten Rechnung erledigen: nach Definition gilt

$$\begin{aligned}
(a,b)\big((a,b),(a',b')\big) &= (a,b)(aa' - b'b^*, a^*b' + a'b) \\
&= (a(aa' - b'b^*) - (a^*b' + a'b)b^*, a^*(a^*b' + a'b) + (aa' - b'b^*)b) \\
&= (a^2a' \underbrace{-ab'b^* - a^*b'b^*}_{=-\underline{(a+a^*)}b'b^*} - a'\underline{bb^*}, (a^*)^2b' + \underbrace{\underline{a^*}a'b + \underline{aa'}b}_{=\underline{(a^*+a)}a'b} - b'b^*b)) \\
&= (a^2a' - b'b^*(a + a^*) - bb^*a', (a^*)^2b' + a'(a^* + a)b - b'b^*b)
\end{aligned}$$

Andererseits ist

$$\begin{aligned}
(a,b)^2(a',b') &= (a^2 - bb^*, a^*b + ab)(a',b') \\
&= ((a^2 - bb^*)a' - b'(a^*b + ab)^*, (a^2 - bb^*)^*b' + a'(a^*b + ab)) \\
&= (a^2a' - bb^*a' - b'b^*a - b'b^*a^*, (a^*)^2b' - bb^*b' + a'a^*b + a'ab).
\end{aligned}$$

Wegen (4.14) stimmen diese Ausdrücke überein. Hierbei benutzen wir jeweils, dass A gut normiert ist, die unterstrichenen Ausdrücke liegen daher in $\mathbf{R}$ und kommutieren damit mit allen Elementen von A. Die übrigen Bedingungen an eine alternative Algebra in Definition 4.16 zeigt man durch ähnliche Rechnungen. Die Umkehrung wird ebenfalls mit ähnlichen Rechnungen bewiesen, siehe Übungsaufgabe 4.2. □

4.2 Charakterisierungen der Oktonionen

Beim Studium der Quaternionen spielte die Produktformel

$$|xy| = |x||y|$$

(siehe (3.4)) eine wichtige Rolle. Der *Satz von Hurwitz* charakterisiert $\mathbf{R}$, $\mathbf{C}$, $\mathbf{H}$ und $\mathbf{O}$ als die einzigen Algebren, die mit einer (a priori abstrakt definierten) Norm mit einer ähnlichen Produktregel ausgestattet sind. Der genaue Begriff ist wie folgt:

Definition 4.19. Eine Algebra A heißt *Divisionsalgebra*, wenn sie keine Nullteiler hat, d.h. wenn aus $a, b \in A$ mit $ab = 0$ schon folgt: $a = 0$ oder $b = 0$.

Eine *normierte Divisionsalgebra* (oder auch, in anderen Quellen, eine *Kompositionsalgebra*) ist eine Algebra A, derart, dass es eine positiv definite symmetrische Bilinearform

$$\langle -, - \rangle : A \times A \to \mathbf{R}$$

gibt, derart, dass die zugehörige Abbildung (genannt *Norm*)

$$N : A \to \mathbf{R}^{\geqslant 0}, x \mapsto N(x) := \langle x, x \rangle$$

die Produktregel

$$N(xy) = N(x)N(y) \tag{4.20}$$

erfüllt.

Bemerkung 4.21.

- Offenbar ist der Name gerechtfertigt, d.h. jede normierte Divisionsalgebra ist eine Divisionsalgebra. Außerdem folgt $N(1) = 1$.
- Sei A eine gut normierte alternative *-Algebra, z.B. $A = \mathbf{R}$, $\mathbf{C}$, $\mathbf{H}$ oder $\mathbf{O}$. Dann ist A eine normierte Divisionsalgebra via
$$\langle x, y \rangle := \frac{xy^* + yx^*}{2}.$$
Da A gut normiert ist, liegt dies in $\mathbf{R}$:
$$\frac{xy^* + yx^*}{2} = \frac{(x+y)(x+y)^* - xx^* - yy^*}{2} \in \mathbf{R}.$$
Die Bilinearform ist offensichtlich symmetrisch und ist positiv definit wegen $xx^* \in \mathbf{R}^{>0}$ für $x \neq 0$. Die Produktregel gilt wegen
$$N(xy) = (xy)(xy)^* = (xy)(y^*x^*) \overset{!}{=} x \underbrace{(yy^*)}_{\in \mathbf{R}^{\geqslant 0}} x^* = (xx^*)(yy^*) = N(x)N(y).$$
An der Stelle ! haben wir benutzt, dass x, y, x^* und y^* in der von x und y erzeugten Unteralgebra von A liegen. Diese Unteralgebra ist (da A alternativ ist) assoziativ (Übungsaufgabe 4.7), beachte hierbei, dass $x^* = (x + x^*) - x$ in dieser Unteralgebra liegt.

Definition 4.22. Sei A eine normierte Divisionsalgebra, versehen mit $\langle -, - \rangle$. Wir definieren dann

$$* : A \to A, x \mapsto x^* := 2\langle x, 1 \rangle - x.$$

(Anders gesagt: $x^* = s_1(x)$, wobei s_1 die Spiegelung an der Geraden $1 \cdot \mathbf{R} = \mathbf{R} \subset A$ ist, vgl. Satz 3.26.)

Bemerkung 4.23. Wir werden in Kürze sehen (Lemma 4.28 und Übungsaufgabe 4.9), dass eine normierte Divisionsalgebra mittels dieser Abbildung * eine gut normierte *-Algebra ist.

Wenn wir mit einer gut normierten *-Algebra $(A, *)$ beginnen, und dann $\langle x, y \rangle$ wie in Bemerkung 4.21 definieren erhalten wir auf obige Weise die gegebene Involution * zurück:

$$2\langle x, 1 \rangle - x := 2\frac{x1^* + 1x^*}{2} - x = x^*.$$

10.2.21 **Theorem 4.24.** (*Satz von Hurwitz*, 1898) Sei A eine normierte Divisionsalgebra. Dann ist A isomorph zu **R**, **C**, **H** bzw. **O**.

Obwohl laut Definition *nicht* vorausgesetzt wird, dass normierte Divisionsalgebren endlich-dimensional oder alternativ sind, folgen insbesondere diese Eigenschaften!

Dieses Theorem stammt aus einer Familie von ähnlichen, weiteren Theoremen, die hier nur kurz erwähnt seien:

Theorem 4.25.
- (*Satz von Zorn*, 1930) Bis auf Isomorphismus sind **R**, **C**, **H** und **O** die einzigen *alternativen* Divisionsalgebren.
- (Hopf, 1940) Die Dimension einer Divisionsalgebra ist 2^n.
- (Kervaire und Bott–Milnor, 1958) Die Dimension einer Divisionsalgebra ist 1, 2, 4 oder 8.

Der Satz von Zorn ist unter diesen der leichteste und lässt sich mit ähnlich elementaren rein algebraischen Überlegungen wie der Satz von Hurwitz zeigen, siehe z.B. [**EbbinghausEtAl:Numbers**]. Das Theorem von Hopf ist eine recht direkte Folgerung der Berechnung der sog. *Homologie* und *Kohomologie* von *projektiven Räumen*, d.h. topologischen Räumen der Form

$$\mathbf{P}^n := S^n/\{\pm 1\}.$$

Der Satz von Kervaire und Bott–Milnor ist wesentlich tiefliegender, und wird ebenfalls mit Mitteln der algebraischen Topologie bewiesen.

Man beachte, dass die letzteren beiden Aussagen nicht besagen, dass **R**, **C**, **H** und **O** (bis auf Isomorphismus) die einzigen Divisionsalgebren sind. Diese Aussage gilt *nicht*, denn Übungsaufgabe 3.13 zeigt, dass es z.B. 4-dimensionale nicht assoziative Divisionsalgebren gibt, die also insbesondere nicht isomorph zu **H** sind.

Wir beginnen nun einige Vorbereitungen für den Beweis von Theorem 4.24. Sei A im folgenen eine normierte Divisionsalgebra.

Lemma 4.26. Seien $x, y, z, u \in A$ beliebig. Dann gilt

$$\langle xy, xz\rangle = N(x)\langle y, z\rangle, \tag{4.27a}$$
$$\langle xz, yz\rangle = \langle x, y\rangle N(z), \tag{4.27b}$$
$$\langle xy, uz\rangle = 2\langle x, u\rangle\langle y, z\rangle - \langle xz, uy\rangle. \tag{4.27c}$$

Beweis. (4.27a): wir setzen in (4.20) $y + z$ ein:

$$N(xy) + N(xz) + 2\langle xy, xz\rangle = N(x)\left(N(y) + 2\langle y, z\rangle + N(z)\right),$$

einige Terme kürzen sich weg wegen $N(xy) = N(x)N(y)$ etc., und wir teilen durch 2.

(4.27c): wir setzen in (4.27a) (für x) $x + u$ ein und erhalten:

$$\langle xy, xz\rangle + \langle xy, uz\rangle + \langle uy, xz\rangle + \langle uy, uz\rangle \overset{(4.27a)}{=} \left(N(x) + 2\langle x, u\rangle + N(u)\right)\langle y, z\rangle.$$

Wiederum heben sich einige Terme weg, und wir erhalten die Behauptung. □

Lemma 4.28. Sei A eine normierte Divisionsalgebra und die Abbildung $* = s_1$ wie eben definiert. Dann gilt für alle $x, y, z \in A$:

$$\langle xy, z\rangle = \langle y, x^*z\rangle, \text{ sowie } \langle xy, z\rangle = \langle x, zy^*\rangle \tag{4.29a}$$
$$x^{**}(:= (x^*)^*) = x, \tag{4.29b}$$
$$(xy)^* = y^*x^*. \tag{4.29c}$$

Direkt klar nach Definition ist $1^* = 1$, insbesondere ist $(A, *)$ also eine *-Algebra.

Beweis. (4.29a): setze in (4.27c) $u = 1$ ein:

$$2\langle x, 1\rangle\langle y, z\rangle - \langle xz, y\rangle = \langle y, (2\langle x, 1\rangle - x)z\rangle = \langle y, x^*z\rangle.$$

Ebenso erhalten wir auch die zweite Gleichung, indem wir in (4.27c) $z = 1$ wählen:

$$\langle x, zy^*\rangle = \langle x, z(2\langle y, 1\rangle - y)\rangle = 2\langle y, 1\rangle\langle x, z\rangle - \langle x, zy\rangle \overset{(4.27c)}{=} \langle xy, z\rangle.$$

(4.29b): setze in (4.29a) $y = 1$, $z = t$ für beliebiges $t \in A$ ein und erhalte

$$\langle x, t\rangle = \langle x1, t\rangle \overset{(4.29a)}{=} \langle 1, x^*t\rangle \overset{(4.29a)}{=} \langle x^{**}1, t\rangle = \langle x^{**}, t, .\rangle$$

Da die Bilineaform $\langle -, -\rangle$ positiv definit und damit nicht entartet ist, folgt hieraus $x = x^{**}$.

(4.29c): Für alle $t \in A$ gilt folgende Gleichheit, wobei wir (4.29a) und (4.29b) anwenden:

$$\langle y^*x^*, t\rangle = \langle x^*, yt\rangle = \langle x^*t^*, y\rangle = \langle t^*, xy\rangle = \langle t^*, (xy)1\rangle = \langle t^*(xy)^*, 1\rangle = \langle (xy)^*, t\rangle.$$

Hieraus folgt wie eben die Behauptung. □

Die Gesamtbeweisstrategie für Theorem 4.24 ist die Idee, nach und nach größere Divisionsalgebren in A zu finden, und zu zeigen, dass diese, je größer sie werden, immer schlechtere Eigenschaften haben, was dazu führt, dass dieser Prozess schnell (d.h. bei Dimension 8) endet.

Satz 4.30. Sei A eine normierte Divisionsalgebra sowie

$$H \subsetneq A$$

eine echte Unteralgebra. Dann enthält A eine Unteralgebra Z, die zur Dickson-Konstruktion von H isomorph ist:

$$H' \cong Z \subset A.$$

Beweis. Da H ein *echter* Unterraum ist, gibt es ein Element $v \in A$ derart, dass

$$\langle a, v\rangle = 0$$

für alle $a \in H$ und $N(v) = 1$ gilt. In der Tat, da $\langle -, -\rangle$ nicht entartet ist, gibt es ein $v \neq 0$ mit der ersten Eigenschaft, Reskalieren sichert die zweite Eigenschaft. Es gilt dann $v^* = -v$.

Wir zeigen nun die folgenden Behauptungen, wobei $a, b, c, d \in H$:

$$\langle a + vb, c + vd\rangle = \langle a, c\rangle + \langle b, d\rangle, \tag{4.31a}$$

$$(a + vb)^* = a^* - vb \tag{4.31b}$$

$$b^*v = -b^*v^* \overset{(4.29c)}{=} -(vb)^* \overset{(4.31b)}{=} vb, \tag{4.31c}$$

$$(a + vb)(c + vd) = (ac - db^*) + v(cb + a^*d). \tag{4.31d}$$

(4.31a) folgt aus der Bilinearität von $\langle -, -\rangle$ und folgenden Rechnungen: $\langle a, vd\rangle = \langle ad^*, v\rangle = 0$, $\langle vb, c\rangle = \langle v, cb^*\rangle = 0$ sowie $\langle vb, vd\rangle = N(v)\langle b, d\rangle = \langle b, d\rangle$. (4.31b) folgt aus (4.29a): $(vb)^* = 2\langle vb, 1\rangle - vb = 2\langle b, v^*\rangle - vb = -vb$. (4.31d) folgt aus folgenden Berechnungen sowie der Nicht-Entartetheit von $\langle -, -\rangle$.

$$\langle a(vd), t\rangle \overset{(4.29a)}{=} \langle vd, a^*t\rangle \overset{(4.27c)}{=} 0 - \langle vt, a^*d\rangle \overset{(4.29a)}{=} \langle t, v(a^*d)\rangle$$

sowie

$$\langle (vb)c, t\rangle \overset{(4.29a)}{=} \langle vb, tc^*\rangle \overset{(4.31c)}{=} \langle b^*v, tc^*\rangle \overset{(4.27c)}{=} 0 - \langle b^*c^*, tv\rangle \overset{(4.29a)}{=} \langle (b^*c^*)v, t\rangle \overset{(4.31b)}{=} \langle v(cb), t\rangle$$

und

$$\langle (vb)(vd), t\rangle \overset{(4.29a)}{=} -\langle vb, t(vd)\rangle \overset{(4.27c)}{=} 0 + \langle v(vd), tb\rangle \overset{(4.29a)}{=} -\langle vd, v(tb)\rangle \overset{(4.27a)}{=} -N(v)\langle d, tb\rangle \overset{(4.29a)}{=} \langle -db^*, t\rangle.$$

Definieren wir nun $Z := H + vH := \{x + vy | x, y \in H\} (\subset A)$, so ist die Abbildung

$$H' \to Z, (x, y) \mapsto x + vy$$

ein Vektorraumisomorphismus, denn es gilt $H \cap vH = 0$ (andernfalls gäbe es $a \in A$ mit $1 = va$ mit $a \in H$, dann wäre $1 = \langle 1, 1\rangle = \langle va, 1\rangle \overset{(4.27c)}{=} \langle v, a^*\rangle = 0$ ein Widerspruch). Damit handelt es sich um eine surjektive Abbildung zwischen endlich-dimensionalen Vektorräumen der gleichen Dimension.

Die obigen Rechnungen zeigen, dass es sich überdies um einen Isomorphismus von *-Algebren handelt.□

Dies liefert nun schnell den Satz von Hurwitz:

Beweis. (von Theorem 4.24) Sei A eine normierte Divisionsalgebra. Es gilt $A_0 := \mathbf{R} \subset A$. Falls $\mathbf{R} \neq A$, so enthält A laut Satz 4.30 eine Algebra A_1, die zu $\mathbf{C} = \mathbf{R}'$ isomorph ist. Falls $A_1 \subsetneq A$ so enthält A eine Algebra A_2, die zu $A_1' \cong \mathbf{C}' = \mathbf{H}$ isomorph ist. Falls $A_2 \subsetneq A$, so gilt wiederum $A_3 \cong \mathbf{H}' = \mathbf{O} \subset A$.

Angenommen $A_3 \subsetneq A$, d.h. $A_4 \cong \mathbf{S} = \mathbf{O}' \subset A$. Hierbei sind $\mathbf{S}$ die Sedenionen. Laut Übungsaufgabe 4.12 gibt es in $\mathbf{S}$ jedoch Nullteiler, andererseits gibt es in der (normierten) Divisionsalgebra A keine Nullteiler. (Ein alternatives Argument, das die konkrete Rechnung in den Sedenionen aus Übungsaufgabe 4.12 vermeidet, ist auch möglich, siehe [CS03, S. 70].) Dieser Widerspruch zeigt: aus $A_3 (\cong \mathbf{O}) \subset A$ folgt bereits $A_3 = A$. □

4.3 Übungsaufgaben

Übungsaufgabe 4.1. Vervollständige die folgende Tabelle (mit Begründung)

	R	**C**	**H**	**O**
reell				
kommutativ				
assoziativ				
alternativ				
gut normiert				

Übungsaufgabe 4.2. Sei A eine Algebra. Der *Assoziator* ist die Abbildung

$$A \times A \times A \to A,$$

die ein Tripel abbildet auf

$$[x, y, z] := (xy)z - x(yz).$$

Offensichtlich gilt: A ist genau dann assoziativ, wenn der Assoziator verschwindet, d.h. $[x, y, z] = 0$ für alle $x, y, z \in A$.

Sei nun A eine *-Algebra und A' ihre Dickson-Konstruktion. Sei $x = (a, b)$ und $x' = (a', b') \in A'$.

(1) Berechne $[x, x^*, x']$ (d.h. den Assoziator in A') in Termen von Assoziatoren der Elemente a, a', b und b'.

(2) Gib hiermit einen erneuten Beweis von Satz 4.17 an.

Übungsaufgabe 4.3. Sei A eine *-Algebra und A' ihre Dickson-Konstruktion. Zeige: A ist gut normiert genau dann, wenn A' gut normiert ist.

Übungsaufgabe 4.4. Sei A eine Algebra. Betrachte, für $x \in A$ die *Linksmultiplikation* und *Rechtsmultiplikation*, definiert als

$$L_x : A \to A, y \mapsto xy$$
$$R_x : A \to A, y \mapsto yx.$$

Zeige: die Abbildung

$$L : A \to \mathrm{End}(A), x \mapsto L_x$$

ist eine lineare Abbildung. (Hierbei bezeichnet $\mathrm{End}(A)$ die $\mathbf{R}$-linearen Endomorphismen von A, d.h. die Algebrastruktur auf A spielt für $\mathrm{End}(A)$ keine Rolle).

Zeige: A ist assoziativ genau dann, wenn L ein Algebren-Homomorphismus ist. Hierbei ist die Multiplikation von $\mathrm{End}(A)$ die Komposition von Endomorphismen.

Übungsaufgabe 4.5. Wir bezeichnen die Basisvektoren von $\mathbf{H}$ wie folgt:

$$1, e_1 := i, e_2 := j, e_4 := k.$$

(Achtung: nicht e_3.) Vervollständige diese 4 Vektoren zu einer Basis $\{1, e_1, e_2, \ldots, e_7\}$ von $\mathbf{O}$ derart, dass folgende Regeln gelten:

$$\begin{aligned} e_i^2 &= -1, \\ e_i e_j &= -e_j e_i \quad \forall i \neq j, \\ e_i e_j = e_k &\Rightarrow e_{i+1} e_{j+1} = e_{k+1}, \\ e_i e_j = e_k &\Rightarrow e_{2i} e_{2j} = e_{2k}. \end{aligned}$$

Bei den letzteren beiden Gleichungen ist der Index jeweils modulo 7 zu verstehen, d.h. z.B. $e_1 e_2 = e_4$ impliziert $e_2 e_4 = e_1$.

Zeige außerdem, dass die obigen 4 Gleichungen, zusammen mit $e_1 e_2 = e_4$ die Multiplikation in $\mathbf{O}$ eindeutig charakterisieren.

Übungsaufgabe 4.6. Bestätige die Aussage in Lemma 4.8.

Übungsaufgabe 4.7. Sei A eine alternative Algebra sowie $x, y \in A$. Betrachte

$$\mathbf{R}\langle x, y\rangle := \bigcap V,$$

wobei der Durchschnitt über alle $\mathbf{R}$-Untervektorräume $V \subset A$ läuft die die folgenden Bedingungen erfüllen: a) $\mathbf{R} \subset V$, b) $L_x(V) \subset V$, c) $L_y(V) \subset V$. (Hier ist L_x die Linksmultiplikation mit x, siehe Übungsaufgabe 4.4).

Zeige: $\mathbf{R}\langle x, y\rangle$ ist eine assoziative Unteralgebra von A. Wir nennen sie die *von x und y erzeugte Unteralgebra*.

Übungsaufgabe 4.8. Zeige, dass jede 4-dimensionale Unteralgebra $A \subset \mathbf{O}$ isomorph zu den Quaternionen ist.

Tipp: es gibt (weshalb?) $x, y \in A$ derart, dass $\{1, x, y\}$ $\mathbf{R}$-linear unabhängig sind. Wende Übungsaufgabe 4.7 auf $\mathbf{R}\langle x, y\rangle \subset A$ an. Nutze Dimensionsargumente sowie den Satz von Frobenius.

Übungsaufgabe 4.9. Sei A eine normierte Divisionsalgebra. Zeige für $x, y \in A$:

$$\langle x, yx\rangle + \langle x^2, y\rangle = 2\langle x, y\rangle\langle 1, x\rangle.$$

Folgere die quadratische Gleichung (vgl. (3.5))

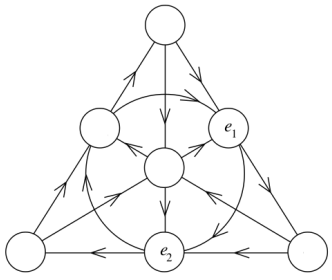
$$x^2 - 2\langle x, 1\rangle x + N(x) = 0.$$

Folgere, dass die Involution $* = s_1$ (Definition 4.22) A zu einer *gut normierten* *-Algebra macht.

4.4 Präsenzaufgaben für die Übungen

Übungsaufgabe 4.10. Gib (neben $\mathbf{R}, \mathbf{C}, \mathbf{H}$ und $\mathbf{O}$) weitere konkrete Beispiele von $*$-Algebren an.

Übungsaufgabe 4.11. Ausgehend von der Nomenklatur der Basisvektoren $1, e_1, \ldots, e_7$ wie in Übungsaufgabe 4.5, vervollständige das folgende Schaubild wie folgt: für jeden Pfeil, der ausgehend von e_i zu e_j verläuft, trage an der nächsten Ecke längs der Pfeilrichtung $e_i e_j$ ein.



Übungsaufgabe 4.12. Die *Sedenionen* sind definiert als

$$\mathbf{S} := \mathbf{O}'$$

d.h. die Dickson-Konstruktion angewendet auf die Oktonionen. Wir bezeichnen die Elemente $(0, 1)$ in der Kette der Dickson-Konstruktionen mit $i \in \mathbf{C}$, $j \in \mathbf{H}$, $\ell \in \mathbf{O}$ (wie üblich) und $e := (0, 1) \in \mathbf{S}$. Zeige

$$(i\ell + je)(j\ell + ie) = 0.$$

Mit anderen Worten: die Sedenionen haben Nullteiler und sind insbesondere *keine* Divisionsalgebra.

Übungsaufgabe 4.13. Zur Erinnerung: Die *Signatur* einer symmetrischen Bilinearform ist die Anzahl der positiven Eigenwerte. Die Signatur einer quadratischen Form ist die Signatur der zugehörigen symmetrischen Bilinearform. Bestimme die Signatur der Abbildung

$$A \to \mathbf{R}, x \mapsto |x|$$

wobei $A = \mathbf{R}$, $\mathbf{C}$, $\mathbf{H}$, bzw. $\mathbf{O}$.

Übungsaufgabe 4.14. Charakterisiere die Eigenschaft einer Algebra alternativ zu sein in Termen der Links- und Rechtsmultiplikation (vgl. Übungsaufgabe 4.4).

Übungsaufgabe 4.15.

- Zeige, dass jede gut normierte *-Algebra A auch eine Kompositionsalgebra ist, indem man
$$N(x) := xx^*$$
setzt.
- Sei $A = \mathbf{H}$, wie üblich mit der Involution * gegeben durch Konjugation. Zeige, dass sich die Grundbegriffe aus Definition und Lemma 3.3 (Realteil, Imaginärteil, etc.) ausschließlich mit Hilfe dieser Abbildung N (bzw. der hieraus abgeleiteten Bilinearform $\langle -, - \rangle$ definieren lassen.

Übungsaufgabe 4.16. Wie kann man die 4 Fälle im Satz von Hurwitz voneinander unterscheiden?

Literatur

[Bae02] John C. Baez. "The octonions". In: *Bull. Amer. Math. Soc. (N.S.)* 39.2 (2002), S. 145–205. ISSN: 0273-0979. DOI: 10.1090/S0273-0979-01-00934-X. URL: https://doi.org/10.1090/S0273-0979-01-00934-X.

[CS03] John H. Conway und Derek A. Smith. *On quaternions and octonions: their geometry, arithmetic, and symmetry*. A K Peters, Ltd., Natick, MA, 2003, S. xii+159. ISBN: 1-56881-134-9.

[Oli11] O.R.B. de Oliveira. "The Fundamental Theorem of Algebra: A most elementary proof". https://arxiv.org/pdf/1109.1459v1.pdf. 2011.

[Pal68] R. S. Palais. "The classification of real division algebras". In: *Amer. Math. Monthly* 75 (1968), S. 366–368. ISSN: 0002-9890. DOI: 10.2307/2313414. URL: https://doi.org/10.2307/2313414.

[SV00] Tonny A. Springer und Ferdinand D. Veldkamp. *Octonions, Jordan algebras and exceptional groups*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2000, S. viii+208. ISBN: 3-540-66337-1. DOI: 10.1007/978-3-662-12622-6. URL: https://doi.org/10.1007/978-3-662-12622-6.

Index

Todo

f, 48

finish, 46