I.L. Kantor, A.S. Solodownikow

Hyperkomplexe Zahlen

Übersetzung: W. Hintzsche
1978 BSB B.G. Teubner Verlagsgesellschaft Leipzig
MSB: Nr. 95
Abschrift und LaTex-Satz: 2022 https://mathematikalpha.de

Inhaltsverzeichnis

Vorwort

Gegenstand dieses Büchleins sind verschiedene Systeme von "Zahlen", die aus den reellen Zahlen durch Hinzufügen einer Reihe "imaginärer Einheiten" aufgebaut werden können. Ein klassisches Beispiel eines solchen Systems ist das System der komplexen Zahlen.
Eine der wichtigsten Eigenschaften komplexer Zahlen wird durch die Identität

$$|zz'| = |z| \cdot |z'| \tag{1}$$

ausgedrückt (der absolute Betrag eines Produktes ist gleich dem Produkt der absoluten Beträge). Wenn man $z = a_1 + a_2 i$ und $z' = b_1 + b_2 i$ setzt, dann wird (1) in der Form

$$(a_1b_1 - a_2b_2)^2 + (a_1b_2 + a_2b_1)^2 = (a_1^2 + a_2^2)(b_1^2 + b_2^2)$$

geschrieben. Von rechts nach links gelesen lautet diese Identität so:
Das Produkt der Summe zweier Quadrate mit der Summe zweier Quadrate ist wiederum die Summe zweier Quadrate.

Existieren noch ähnliche Identitäten mit mehr als 2 Quadraten?
Wie beschreibt man alle solche Identitäten?

Schon L. Euler zeigte ein Beispiel einer Identität für 4 Quadrate; später wurde eine Identität für 8 Quadrate gefunden. Es gelang jedoch erst am Ende des 19. Jahrhunderts, die vollständige Lösung der Frage zu erhalten.
Man kann annehmen, dass jede Identität für n Quadrate mit der Formel (1) zusammenhängt, in der z und z' bereits keine komplexen Zahlen mehr sind, sondern "Zahlen" der allgemeineren Form

$$a_1 + a_2 i + a_3 j + ... + a_n l$$

wobei i,j,...,l imaginäre Einheiten sind. Indem man die Lage der Dinge etwas vereinfacht, kann man sagen, dass dies tatsächlich so ist. Das Aufstellen der Verbindung zwischen den Identitäten für n Quadrate und der Formel (1) für einige Systeme "hyperkomplexer" Zahlen bildet eine der Grundlinien im Aufbau dieses Büchleins.

Eine Frage, der in diesem Büchlein viel Platz eingeräumt wurde, ist die Frage nach der Division hyperkomplexer Zahlen.
Es verhält sich so, dass in jedem System hyperkomplexer Zahlen stets drei der vier "arithmetischen" Operationen definiert sind: die Addition, die Subtraktion und die Multiplikation. Was die Division anbetrifft, erfordert die Frage nach der Möglichkeit dieser Operation für ein gegebenes System hyperkomplexer Zahlen eine gesonderte Betrachtung.

Man muss überhaupt sagen, dass hyperkomplexe Systeme, in denen die Division möglich ist, eine große Seltenheit bilden. Es versteht sich, dass Systeme reeller Zahlen (wie auch komplexer Zahlen) Beispiele von Systemen mit Division darstellen. Es gibt aber außer ihnen auch andere Beispiele.

Die bemerkenswertesten unter ihnen sind das System der sogenannten Quaternionen und das System der Oktaven. Das Problem des Auffindens aller hyperkomplexen Systeme mit Division ist bis zur heutigen Zeit noch nicht in erschöpfender Weise gelöst worden. Einige Varianten dieses Problems werden im vorliegenden Büchlein betrachtet.

Das erste Kapitel dieses Buches macht den Leser mit verschiedenen Beispielen hyperkomplexer Zahlen, darunter die Quaternionen und die Oktaven, bekannt; für diese und andere ist die Formel (1) richtig, und diese und andere bilden ein "System mit Division".

Das dritte Kapitel ist der außergewöhnlichen Rolle gewidmet, die die drei Systeme der komplexen Zahlen, der Quaternionen und der Oktaven in Bezug auf die oben gestellten Fragen spielen. Das zweite Kapitel trägt einen Hilfscharakter. In ihm werden auf elementarem Niveau die grundlegenden Begriffe der linearen Algebra dargelegt.

Das Büchlein ist für die außerschulische Mathematikarbeit gedacht und einfach für alle, die sich für Mathematik interessieren.
Das erste und das zweite Kapitel sind im wesentlichen Schülern höherer Klassen zugänglich, die Lektüre der anderen Teile mag ziemlich intensive Bemühungen erfordern. In allen Fällen werden keine Vorkenntnisse vom Leser verlangt.

1 Hyperkomplexe Zahlen

1.1 Komplexe Zahlen

1.1.1 Einleitung

In der elementaren Algebra wird zusammen mit den reellen Zahlen auch das umfangreichere System der komplexen Zahlen betrachtet. Der Grund, der dazu zwingt, die komplexen Zahlen zu betrachten, ist mit der Lösung quadratischer Gleichungen verbunden. Er besteht darin, dass man einige quadratische Gleichungen, zum Beispiel

$$x^2 + 1 = 0 \tag{1}$$

nicht lösen kann, wenn man sich nur auf die reellen Zahlen beschränkt (denn es existiert keine solche reelle Zahl a, so dass a^2 gleich -1 ist).

Die Geschichte der komplexen Zahlen beginnt mit dem 16.Jahrhundert. Die italienischen Mathematiker Girolamo Cardano und Raffael Bombelli führten beim Lösen quadratischer Gleichungen das Symbol $\sqrt{-1}$ die formale Lösung der Gleichungen (1), aber auch den Ausdruck $b\sqrt{-1}$, die formale Lösung der Gleichung

$$x^2 + b^2 = 0$$

ein.
Ausdrücke der noch allgemeineren Form $a + b\sqrt{-1}$ kann man dann als formale Lösung der Gleichung

$$(x - a)^2 + b^2 = 0 \tag{2}$$

betrachten.
Später wurden die Ausdrücke $a + b\sqrt{-1}$ als imaginäre und danach als komplexe Zahlen bezeichnet und $a + bi$ geschrieben.

Das Symbol i zur Bezeichnung von $\sqrt{-1}$ führte L. Euler im 18. Jahrhundert ein. Diese Zahlen erweisen sich bereits zur Lösung einer beliebigen quadratischen Gleichung als ausreichend.
Wenn die Diskriminante der quadratischen Gleichung nicht negativ ist, dann sind, wie bekannt ist, die Wurzeln einer solchen Gleichung reelle Zahlen; wenn die Diskriminante negativ ist, wird die Gleichung notwendig die Form (2) haben.

Man nennt einen Ausdruck der Form

$$a + bi$$

komplexe Zahl, wobei a und b reelle Zahlen sind und dem Symbol i die Eigenschaft $i^2 = -1$ zugeschrieben wird. Wir bemerken, dass die komplexen Zahlen, insbesondere alle reellen Zahlen (man erhält sie bei $b = 0$), aber auch alle rein imaginären Zahlen bi (man erhält sie bei $a = 0$) enthalten.
Indem wir der Kürze halber eine komplexe Zahl mit dem Buchstaben z bezeichnen, werden wir weiter schreiben

$$z = a + bi$$

Die Zahl a wird Realteil, die Zahl bi Imaginärteil der komplexen Zahl z genannt; das Symbol i bezeichnet die imaginäre Einheit.

Die Bezeichnung "imaginär" darf man nicht wörtlich auffassen, sie hat sich aus den Zeiten (16.-17. Jahrhundert) her erhalten, in denen man die komplexen Zahlen als etwas Unreales ansah und sie von einer Aureole tiefen Geheimnisses umgeben waren. Für die heutige Mathematik sind die komplexen Zahlen eine völlig natürliche Sache (ebenso wie die reellen Zahlen nichts "Imaginäres" mehr).

1.1.2 Die Grundrechenarten für komplexe Zahlen

Addition, Subtraktion und Multiplikation komplexer Zahlen werden ganz natürlich auf folgende Weise definiert:

$$\begin{aligned}(a+bi)+(c+di) &= (a+c)+(b+d)i\\ (a+bi)-(c+di) &= (a-c)+(b-d)i\\ (a+bi)(c+di) &= ac+adi+bci+bdi^2=(ac-bd)+(ad+bc)i\end{aligned}$$

Beim Definieren der Multiplikation berücksichtigten wir die Tatsache, dass $i^2=-1$ ist.

Wir bemerken zugleich, dass wir aus der Gleichung, die die Multiplikation der komplexen Zahlen definiert, für $b=0$ die Regel der Multiplikation einer reellen Zahl mit einer komplexen Zahl erhalten:

$$a(c+yi)=ac+adi$$

Es ist nicht schwierig zu überprüfen, dass die Gesetze, denen die oben definierten Operationen für komplexe Zahlen unterworfen sind, die gleichen Gesetze sind wie die der Grundrechenarten für reelle Zahlen. Die Addition besitzt kommutative und assoziative Eigenschaften:

$$z_1+z_2=z_2+z_1 \qquad , \qquad (z_1+z_2)+z_3=z_1+(z_2+z_3)$$

ebenso verhält es sich mit der Multiplikation:

$$z_1z_2=z_2z_1 \qquad , \qquad (z_1z_2)z_3=z_1(z_2z_3)$$

schließlich gilt das Distributivgesetz, das eine Verbindung zwischen diesen zwei Grundrechenarten aufstellt:

$$z_1(z_2+z_3)=z_1z_2+z_1z_3 \tag{3}$$

Wir überprüfen zum Beispiel die Gültigkeit der Gleichung (3). Es mögen $z_1=a_1+b_1i$, $z_2=a_2+b_2i$ und $z_3=a_3+b_3i$ sein. Wir haben

$$\begin{aligned}z_1(z_2+z_3) &= (a_1+b_1i)((a_2+a_3)+(b_2+b_3)i)\\ &= (a_1(a_2+a3)-b_1(b_2+b_3))+(a_1(b_2+b_3)+b_1(a_2+a_3))i \qquad \text{und}\\ z_1z_2+z_1z_3 &= (a_1+b_1i)(a_2+b_2i)+(a_1+b_1i)(a_3+b_3i)\\ &= (a_1a_2-b_1b_2+a_1a_3-b_1b_3)+(a_1b_2+b_1a_2+a_1b_3+b_1a_3)i\end{aligned}$$

Durch Vergleichen der Resultate beider Rechnungen überzeugt man sich davon, dass sie übereinstimmen.

1.1.3 Konjugiert komplexe Zahlen

Wir gehen jetzt auf andere Eigenschaften des Systems der komplexen Zahlen ein. Jeder komplexen Zahl

$$z=a+bi$$

kann man eine andere komplexe Zahl $a - bi$ zuordnen, die man konjugiert komplexe Zahl zu z nennt und mit $\overline{z}$ bezeichnet. Auf solche Weise gilt nach Definition

$$\overline{z} = a - bi$$

Man kann sich leicht davon überzeugen, dass die Formeln

$$\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2} \qquad \text{und} \qquad \overline{z_1 z_2} = \overline{z_1}\ \overline{z_2}$$

gelten. Anders ausgedrückt ist die konjugiert komplexe Zahl einer Summe gleich der Summe der konjugiert komplexen Summanden und die konjugiert komplexe Zahl eines Produkts gleich dem Produkt der konjugiert komplexen Faktoren. Den Nachweis überlassen wir dem Leser.

Durch Addieren und Multiplizieren der Zahlen z und $\overline{z}$ finden wir

$$z + \overline{z} = 2a \qquad \text{und} \qquad z\overline{z} = a^2 + b^2$$

d.h., die Summe und das Produkt von konjugiert komplexen Zahlen stellen immer reelle Zahlen dar.

1.1.4 Der absolute Betrag einer komplexen Zahl. Identität für zwei Quadrate

Die nichtnegative reelle Zahl $\sqrt{a^2 + b^2}$ wird absoluter Betrag der komplexen Zahl z genannt und mit $|z|$ bezeichnet:

$$|z| = a^2 + b^2$$

Folglich gilt

$$z\overline{z} = |z|^2$$

Aus der letzten Gleichung geht eine bemerkenswerte Folgerung hervor. Es mögen z_1 und z_2 zwei komplexe Zahlen sein. Wir haben

$$|z_1 z_2|^2 = (z_1 z_2)\overline{(z_1 z_2)} = z_1 z_2 \overline{z_1}\ \overline{z_2} = z_1\overline{z_1} \cdot z_2\overline{z_2} = |z_1|^2 \cdot |z_2|^2$$

folglich ist

$$|z_1 z_2|^2 = |z_1|^2 |z_2|^2 \qquad , \qquad |z_1 z_2| = |z_1||z_2| \tag{4,5}$$

Der absolute Betrag eines Produktes ist so gleich dem Produkt der absoluten Beträge. Dies ist eine außerordentlich wichtige Eigenschaft der komplexen Zahlen. Im § 16 wird ihr eine spezielle Bezeichnung gegeben (die Eigenschaft der Normiertheit).
Wir werden gleich sehen, wie die Gleichung (4) in einer ähnlichen Schreibweise aussieht. Wenn

$$z_1 = a_1 + b_1 i \qquad , \qquad z_2 = a_2 + b_2 i$$

ist, dann gilt

$$z_1 z_2 = (a_1 a_2 - b_1 b_2) + (a_1 b_2 + a_2 b_1)i$$

und Gleichung (4) nimmt, von rechts nach links geschrieben, die Form

$$(a_1^2 + b_1^2)(a_2^2 + b_2^2) = (a_1 a_2 - b_1 b_2)^2 + (a_1 b_2 + a_2 b_1)^2$$

an. Wir haben eine recht interessante Identität erhalten. Wenn wir eine gewisse Unklarheit der Formulierung einräumen, dann können wir sie so lesen: Das Produkt einer Summe aus zwei Quadraten mit einer Summe aus zwei Quadraten ist wiederum eine Summe aus zwei

Quadraten.

Natürlich taucht die Frage auf: Existiert eine analoge Identität für eine größere Zahl von Quadraten? Die Frage ist, wie wir weiter sehen werden, durchaus nicht einfach; im Verlauf von vielen Jahren beschäftigte sie die Mathematiker.
Im vorliegenden Büchlein wird sie einen der hervorragenden Plätze einnehmen.
Im § 3 formulieren wir sie noch klarer und im Kapitel 3 zeigen wir, wie sie gelöst wird.

1.1.5 Division von komplexen Zahlen

Bis jetzt haben wir die Frage nach der Division der komplexen Zahlen noch nicht berührt. Darüber wollen wir jetzt reden. Es mögen z' und z zwei komplexe Zahlen sein, außerdem möge $z \neq 0$ sein. Der Quotient z' durch z ist nach Definition die Lösung der Gleichung

$$zx = z' \tag{6}$$

Durch Multiplizieren beider Seiten der Gleichung mit $\overline{z}$ erhalten wir $\overline{z}zx = \overline{z}z'$ oder $|z|^2x = \overline{z}z'$. Wenn wir jetzt beide Seiten mit der reellen Zahl $1/|z|^2$ multiplizieren, so erhalten wir

$$x = \frac{1}{|z|^2}\overline{z}z' \tag{7}$$

Durch Einsetzen kann man sich leicht davon überzeugen, dass die gefundene Größe x tatsächlich der Gleichung (6) genügt.

Wir veranschaulichen uns die Division durch ein Beispiel. Es soll $z' = 5 - i$ durch $z = 2 - 3i$ geteilt werden. Nach Formel (7) haben wir

$$\frac{z'}{z} = \frac{1}{2^2 + 3^2}(2 + 3i)(5 - i) = \frac{1}{13}(13 + 13i) = 1 + i$$

1.2 Andere Arithmetiken für die Zahlen $a + bi$

1.2.1 Aufgabenstellung

Wir haben aus Ausdrücken der Form $a+bi$ ein Zahlensystem aufgebaut, indem wir die Addition und die Multiplikation solcher Ausdrücke durch die Formeln

$$(a + bi) + (c + di) = (a + c) + (b + d)i \tag{1}$$

und

$$(a + bi)(c + di) = (ac - bd) + (ad + be)i \tag{2}$$

definierten.
Die Formel (1) wirkt völlig natürlich. Die Form der Formel (2) ruft hingegen diesen Eindruck nicht hervor. Wir werden sehen, ob man nicht mit den Ausdrücken $a + bi$ ein hinreichend vernünftiges Zahlensystem aufbauen kann, wobei die Additionsvorschrift (1) erhalten bleiben soll, aber (2) durch irgendein neues Multiplikationsgesetz ersetzt werden soll.

Wie könnte dieses neue Gesetz aussehen? In bedeutendem Maße hängt dies davon ab, mit welchen Eigenschaften wir die neue Multiplikation versehen wollen.
Wir sehen, dass es unsinnig wäre, sie durch die Formel

$$(a + bi) \cdot (c + di) = ac^2 + bdi$$

einzuführen, weil wir dann zum Beispiel für $b = 0$, $d = 0$ die ziemlich eigentümliche Gleichung

$$a \cdot c = ac^2$$

erhalten würden. Wir nennen diejenigen Forderungen, die wir gesammelt haben, um sie an die neue Multiplikation zu stellen:

1) Die Multiplikation einer reellen Zahl a, die als Element des neuen Zahlensystems betrachtet wird ($a = a + 0i$), mit jeder Zahl $z = b + ci$ soll das gleiche Resultat wie im Falle komplexer Zahlen ergeben, d.h.,

$$(a + 0i)(b + ci) = ab + aci \qquad \text{und} \qquad (b + ci)(a + 0i) = ab + aci$$

Insbesondere bedeutet dies, dass die neue Multiplikation für reelle Zahlen mit der üblichen übereinstimmen muss:

$$(a + 0i)(b + 0i) = ab + 0i$$

Da dasselbe auch für die Addition richtig ist (aus (1) folgt $(a + 0i) + (b + 0i) = (a + b) + 0i$, sind die reellen Zahlen mit ihrer natürlichen Arithmetik in das neue Zahlensystem einbegriffen.

2) Es soll die Gleichung

$$(az_1) \cdot (bz_2) = (ab) \cdot (z_1 z_2)$$

erfüllt werden, wobei a und b beliebige reelle Zahlen sind. Zum Beispiel ist

$$(2i)(3i) = 6i^2$$

3) Sowohl für den ersten Faktor als auch für den zweiten Faktor soll die Eigenschaft der Distributivität, die die Multiplikation mit der Addition verbindet, erfüllt sein:

$$z_1(z_2 + z_3) = z_1 z_2 + z_1 z_2 \qquad \text{und} \qquad (z_1 + z_2)z_3 = z_1 z_3 + z_2 z_3$$

Natürlich erlauben es diese Forderungen noch nicht, das neue Gesetz der Multiplikation vollständig aufzuschreiben, aber dennoch folgt aus ihnen einiges. Und zwar

$$(a + bi)(c + di) = a(c + di) + (bi)(c + di) = ac + adi + bci + bdi^2$$

Wir müssen jetzt, um ein Resultat niederschreiben zu können, nur noch festlegen, wem i^2 gleich ist. Wenn wir $i^2 = -1$ annehmen, dann kommen wir zur Multiplikation der komplexen Zahlen.

Dies ist aber durchaus nicht die einzige Möglichkeit. Im Prinzip ist es doch nur erforderlich, dass das Produkt $i \cdot i$ dem von uns betrachteten Zahlensystem angehörte, d.h., dass es eine Zahl der Form $p + qi$ ist.
Wenn p und q festgelegt sind, dann können wir schließlich die Form des Multiplikationsgesetzes angeben:

$$(a + bi)(c + di) = (ac + bdp) + (ad + bc + bdq)i \tag{8}$$

Der Gegenstand unserer Untersuchung wurde auf diese Weise definiert. Jetzt kann man die "hinführenden" Überlegungen vergessen, die uns zur Formel (3) brachten, und kann einfach sagen, dass ein System von Zahlen der Form $a + bi$ mit dem Additionsgesetz (1) und dem Multiplikationsgesetz (3) betrachtet wird, wobei p und q zwei feste reelle Zahlen sind (die sich sozusagen aus der "Arithmetik" des gegebenen Zahlensystems ergeben).

Wenn wir die Formel (3) aufmerksam betrachten, überzeugen wir uns ziemlich leicht davon, dass die neue Multiplikation die Eigenschaft der Kommutativität ($z_1z_2 = z_2z_1$) besitzt. Das ist ein recht unerwartetes Resultat, wenn man berücksichtigt, dass unter den Forderungen, die an die Multiplikation gestellt wurden, eine solche Eigenschaft nicht vorkam!
Erfüllt wird auch die Eigenschaft der Assoziativität $[(z_1z_2)z_3 = z_1(z_2z_3)]$, obwohl die Überprüfung dieser Tatsache etwas mehr Geduld erfordert.
Wir erhalten

$$\begin{aligned}
[(a+bi)(c+di)](e+fi) &= [(ac+bdp)+(ad+bc+bdq)i](e+fi)\\
&= ((ac+bdp)e+(ad+be+bdq)fp)\\
&\quad +(ac+bdp)f+(ad+bc+bdq)e+(ad+bc+bdq)fg)i
\end{aligned}$$

und

$$\begin{aligned}
(a+bi)[(e+di)(e+fi)] &= (a+bi)[(ce+dfp)+(cf+de+dfq)i\\
&= (a(ce+dfp)+(b(cf+de+dfq)p)\\
&\quad +(a(cf+de+dfq)+(b(ce+dfp)+b(cf+de+dfq)i
\end{aligned}$$

Durch Vergleichen der Ergebnisse der beiden Rechnungen kann man sich leicht von ihrer Übereinstimmung überzeugen. (Um die Überprüfung zu vereinfachen, haben wir gleiche Ausdrücke mit der gleichen Zahl gerader Linien unterstrichen.)

1.2.2 Rückführung auf drei Systeme

Man könnte vermuten, dass wir eine unendliche Menge von Zahlensystemen gefunden haben, da zwei beliebige reelle Zahlen p und q in Formel (3) eingehen. Dies verhält sich aber nicht ganz so. Wir werden gleich sehen, dass sich jedes System auf eins der drei reduziert:

I) Zahlen $a + bi$, wobei $i^2 = -1$ (komplexe Zahlen);

II) Zahlen $a + bi$, wobei $i^2 = 1$ (sogenannte binäre Zahlen);

III) Zahlen $a + bi$, wobei $i^2 = 0$ (sogenannte duale Zahlen).

Die Rückführung eines beliebigen Falles auf einen von diesen drei erfolgt auf folgende Weise. Aus der Gleichung $i^2 = p + qi$ geht $i^2 - qi = p$ oder

$$\left(i - \frac{q}{2}\right)^2 = p + \frac{q^2}{4} \tag{4}$$

hervor. Möglich sind drei Fälle:
I. $p + q^2/4$ ist eine negative Zahl, d.h.,

$$p + \frac{q^2}{4} = -k^2$$

wobei k irgendeine von Null verschiedene reelle Zahl ist. Dann ist

$$\left(i - \frac{q}{2}\right)^2 = -k^2 \qquad \text{und} \qquad \left(-\frac{q}{2k} + \frac{1}{k}i\right)^2 = -1 \tag{5}$$

Wenn wir die Zahl; die in Klammern steht, mit J bezeichnen, erhalten wir

$$J^2 = -1$$

Dabei ist $i = q/2 + kJ$, so dass jede Zahl $a + bi$ in der Form

$$a + bi = a + b\left(\frac{q}{2} + kJ\right) = \left(a + \frac{b}{2}q\right) + bkJ$$

geschrieben werden kann. Anders ausgedrückt, die Zahl $a + bi$ lässt eine Darstellung in der Form $a' + b'J$ zu, wobei $J^2 = -1$ ist.
Das bedeutet, dass wir es in der Tat mit komplexen Zahlen zu tun haben.

II. $p + q^2/4$ ist eine positive Zahl, d.h.

$$p + \frac{q^2}{4} = k^2$$

Dann erhalten wir anstelle von (5)

$$\left(-\frac{q}{2k} + \frac{1}{k}i\right)^2 = 1$$

Wenn wir diesmal die Zahl, die in Klammern steht, mit E bezeichnen, erhalten wir

$$E^2 = 1$$

Auf diese Weise lässt jede Zahl $a + bi$ unseres Systems eine Darstellung in der Form $a' + b'E$ zu, jetzt ist aber $E^2 = 1$. Das Multiplikationsgesetz solcher Zahlen ist

$$(a' + b'E)(c' + d'E) = (a'c' + b'd') + (a'd' + b'd')E$$

Wir erhalten also für $p + q^2/4 > 0$ das System der binären Zahlen.

III. $p + q^2/4 = 0$. In diesem Fall erhalten wir, wenn wir die Zahl $i - q/2$ mit Ω bezeichnen

$$\Omega^2 = 0$$

Eine beliebige Zahl $a + bi$ unseres Systems kann umgeformt werden zu $(a + b/2q) + b\Omega$, d.h., in die Form $\tilde{a} + \tilde{b}\Omega$. Das Multiplikationsgesetz sieht so aus

$$(\tilde{a} + \tilde{b}\Omega)(\tilde{c} + \tilde{d}\Omega) = \tilde{a}\tilde{c} + (\tilde{a}\tilde{d} + \tilde{b}\tilde{c})\Omega$$

Dies ist das System der dualen Zahlen.

Wir fassen zusammen. Wir zeigten, dass jedes System von Zahlen $a + bi$ mit den Regeln der Grundrechenarten (1) und (3) stets eines der nachfolgenden drei ist:

I. komplexe Zahlen $a + bJ$, $J^2 = -1$;
II. binäre Zahlen $a + bE$, $E^2 = 1$;
III. duale Zahlen $a + b\Omega$, $\Omega^2 = 0$.

Wir haben die Eigenschaften der komplexen Zahlen ausführlich genug untersucht. Die dualen und die binären Zahlen sind weniger interessant. Der Hauptunterschied zu den komplexen Zahlen besteht darin, dass man die dualen und binären Zahlen im allgemeinen nicht durcheinander dividieren kann.
Übrigens ist es hier nötig, noch einmal den Sinn des Wortes "Division" zu erklären. Wenn ein bestimmtes Multiplikationsgesetz gegeben ist, dann bedeutet z_1 durch z_2 ($z_2 \neq 0$) zu dividieren, die Gleichung

$$z_2 x = z_1$$

zu lösen.

Wir zeigen, dass es im System der binären Zahlen nicht möglich ist, zum Beispiel die Zahl $z_1 = 1$ (d.h. $1 + 0E$) durch $z_2 = 1 + E$ zu dividieren. In der Tat, wenn die Gleichung

$$(1 + E)x = 1 + 0E$$

eine Lösung besitzen würde, dann würden wir, wenn wir beide Seiten der Gleichung mit $1 - E$ multiplizierten, $(1 - E)^2 x = 1 - E$, d.h., $0 = 1 - E$, eine unrichtige Gleichung, erhalten.
Ebenso kann man im System der dualen Zahlen zum Beispiel nicht 1 durch 2 dividieren. Tatsächlich gilt für beliebiges $x = a + b\Omega$

$$x \cdot \Omega = a\Omega \neq 1$$

Natürlich stellt die Unmöglichkeit der Division das Recht der binären und der dualen Zahlen in Zweifel, als "Zahlen" bezeichnet zu werden, denn in der Hauptsache besteht der Begriff einer Zahl doch gerade darin, dass man Zahlen addieren, multiplizieren und dividieren kann.

In der Mathematik spielen jedoch auch solchen Systeme von "Zahlen" (ähnlich den binären und den dualen Zahlen) eine große Rolle, bei denen nur die Grundrechenarten Addition, Subtraktion und Multiplikation definiert sind, während die Division nicht immer ausführbar ist (d.h. nicht für alle $z_1, z_2 \neq 0$).
In jenen Fällen, in denen die Division für jedes $z_1, z_2 \neq 0$ erfüllt wird, spricht man von einem System mit Division. In diesem Büchlein werden wir in der Hauptsache Systeme mit Division betrachten.

1.3 Quaternionen

1.3.1 Einleitende Überlegungen

Die Erfahrung beim Aufbau des Systems der komplexen (sowie auch der binären und dualen) Zahlen bringt uns auf den Gedanken, weiterzugehen und Zahlen der Form

$$z = a + bi + cj$$

zu betrachten, wobei a, b und c beliebige reelle Zahlen und i und j gewisse Symbole sind. Als Additionsregel für Zahlen solcher Form ist es offensichtlich vernünftig

$$(a + bi + cj) + (a' + b'i + c'j) = (a + a') + (b + b')i + (c + c')j$$

zu nehmen; über die Multiplikationsregel müssen wir noch nachdenken.
Es versteht sich, dass wir von dieser Regel erwarten, dass sie nicht zu allzu eigentümlichen Ergebnissen führt. Beispielsweise wäre es wünschenswert, dass für reelle Zahlen die neue Multiplikation mit der gewöhnlichen übereinstimmt

$$(a + 0i + 0j)(b + 0i + 0j) = ab + 0i + 0j$$

Im vorigen Paragraphen wurden diejenigen natürlichen Forderungen aufgezählt, die gegenüber neuen Multiplikationen erhoben werden. Wir wiederholen sie sinngemäß noch einmal:

1) Das Produkt einer reellen Zahl $k = k + 0i + 0j$ mit einer beliebigen Zahl $z = a + bi + cj$ muss gleich $ka + kbi + kcj$ sein.

2) Es muss die Gleichung

$$(az_1)(bz_2) = (ab)(z_1z_2)$$

erfüllt sein, wobei a und b beliebige reelle Zahlen sind.

3) Das Distributivgesetz muss sowohl in der Form

$$z_1(z_2 + z_3) = z_1z_2 + z_1z_3$$

als auch in der Form

$$(z_1 + z_2)z_3 = z_1z_3 + z_2z_3$$

erfüllt sein.
Es bereitet keine Mühe, sich ein Multiplikationsgesetz auszudenken, das allen aufgezählten Forderungen genügt. Man kann zum Beispiel

$$(a + bi + bj)(a' + b'i + c'j) = aa' + (ab' + ba')i + (ac' + ca')j$$

annehmen, Bei einer solchen Multiplikationsregel werden sogar das Kommutativgesetz und das Assoziativgesetz erfüllt ($z_1z_2 = z_2z_1$) und $(z_1z_2)z_3 = z_1(z_2z_3)$; jedoch fehlt offensichtlich die Möglichkeit der Division! Man kann zum Beispiel 1 nicht durch i dividieren, denn die Gleichung

$$(0 + i + 0j)x = 1 + 0i + 0j$$

besitzt keine Lösung.

Dies ist aber nicht zufällig so. Man kann zeigen, dass bei jeder Multiplikationsregel für die Zahlen $a + bi + cj$, die den Bedingungen 1), 2) und 3) genügt, man wenigstens ein Paar Zahlen z_1, z_2 (wobei $z_2 \neq 0$ ist) derart finden kann, dass z_1 nicht durch z_2 dividiert werden kann.
So ist es nicht möglich, aus Zahlen der Form $a + bi + cj$ ein System mit Division aufzubauen!

Es zeigt sich jedoch, wenn man noch ein Symbol k hinzufügt und die Zahlen der Form

$$a + bi + cj + dk \tag{1}$$

betrachtet, dann ist es möglich, ein System mit Division zu erhalten.
Genauer gesagt, man kann die Multiplikation für die Zahlen (1) so einführen, dass mit den Forderungen 1), 2) und 3) auch die zur Multiplikation entgegengesetzte Grundrechenart, die Division, erfüllt wird. Das interessanteste Beispiel eines solchen Systems sind die Quaternionen ("Vierer"-Zahlen).

1.3.2 Definitionen der Quaternionen

Zahlen der Form (1) mit dem Additionsgesetz

$$(a + bi + cj + dk) + (a' + b'i + c'j + d'k) = (a + a') + (b + b')i + (c + c')j + (d + d')k$$

und einem sehr eigenartigen Multiplikationsgesetz nennt man Quaternionen. Um dieses Multiplikationsgesetz zu beschreiben, genügt es, alle möglichen paarweisen Produkte der Zahlen i, j und k zu kennen. Wir setzen durch Definition

$$i^2 = -1, \quad j^2 = -1, \quad k^2 = -1$$

$$ij = k, \quad ji = -k, \quad jk = i, \quad kj = -i, \quad ki = j, \quad ik = -j \tag{2}$$

Die Abbildung 1, in der die Quaternionen i, j und k als drei im Uhrzeigersinn angeordnete Punkte eines Kreises dargestellt sind, hilft, sich diese "Multiplikationstafel" zu merken.

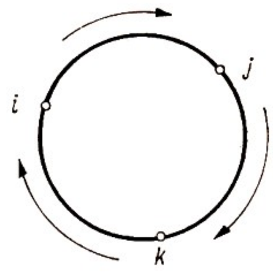


Abb.1

Das Produkt zweier beliebiger Zahlen aus dem Tripel i, j und k ist gleich der dritten Zahl, wenn die Bewegung vom ersten Faktor zum zweiten im Uhrzeigersinn erfolgt, und ist gleich der dritten Zahl mit negativem Vorzeichen, wenn die Bewegung entgegen dem Uhrzeigersinn erfolgt.
Wir wir sehen, ist die kommutative Eigenschaft der Multiplikation hier nicht erfüllt. Das Produkt hängt von der Reihenfolge der Faktoren ab!

Die Multiplikation beliebiger Quaternionen wird mit Hilfe der oben eingeführten Tafel und unter Berücksichtigung der Forderungen 1)-3) ausgeführt. Es möge

$$q = a + bi + cj + dk \qquad \text{und} \qquad q' = a' + b'i + c'j + d'k$$

sein. Nach der Regel der Multiplikation einer Summe mit einer Summe (die aus 3) hervorgeht, erhalten wir

$$\begin{aligned} qq' &= aa' + a(b'i) + a(c'j) + a(d'k) + (bi)a' + (bi)(b'i) + (bi)(c'j) + (bi)(d'k) \\ &\quad + (cj)a' + (cj)(b'i) + (cj)(c'j) + (cj)(d'k) + (dk)a' + (dk)(b'i) + (dk)(c'j) + (dk)(d'k) \end{aligned}$$

Wir haben eine Summe von 16 Summanden erhalten. Durch Umformen jedes Summanden mit Hilfe der Forderungen 1) und 2) und der Multiplikationstafel (zum Beispiel $(bi)(c'j) = bc'(ij)' = bc'k$) gelangen wir zum Resultat:

$$\begin{aligned} qq' &= (aa' - bb' - cc' - dd') + (ab' + ba' + cd' - dc')i \\ &\quad + (ac' + ca' + db' - bd')j + (ad' + da' + bc' - cb')k \end{aligned} \tag{3}$$

1.3.3 Assoziativgesetz für die Multiplikation der Quaternionen

Obwohl die Multiplikation der Quaternionen nicht dem Kommutativgesetz unterworfen ist, sind alle Rechnungen mit Quaternionen nicht so schwierig, wie es auf den ersten Blick erscheinen mag. Das liegt daran, dass die Multiplikation der Quaternionen das Assoziativgesetz erfüllt:

$$(q_1 q_2)q_3 = q_1(q_2 q_3) \tag{4}$$

Wir werden die Richtigkeit dieser Gleichung überprüfen. Da jede Quaternion q_α $(\alpha = 1, 2, 3)$ sich als Summe von vier Summanden ($q_\alpha = a_\alpha + b_\alpha i + c_\alpha j + d_\alpha k$) darstellt, ist die linke Seite von (4) gleich der Summe von $4 \times 4 \times 4 = 64$ Summanden der Form

$$(u_1 u_2)u_3 \tag{5}$$

wobei u_1 ein beliebiger der vier Summanden der Quaternion q_1, u_2 ein beliebiger der Summanden von q_2 und u_3 ein beliebiger der Summanden von q_3 ist. Analog ist die rechte Seite von (4) gleich der Summe von 64 entsprechenden Summanden

$$u_1(u_2 u_3) \tag{6}$$

Deshalb ist die Gleichung (4) bewiesen, wenn wir zeigen, dass jeder Summand (5) gleich dem entsprechenden Summanden (6) ist. Folglich genügt es zum Beweis der Gleichung (4), wenn als q_1, q_2 und q_3 die Quaternionen a, bi, cj und dk (in jeder Kombination) genommen werden. Weil man den Zahlenfaktor vor 1, i, j und k weglassen kann, ist es hinreichend, die Gleichung (4) für die Fälle zu überprüfen, in denen q_1, q_2 und q_3 beliebige der Quaternionen 1, i, j oder k sind; zum Beispiel ist es hinreichend, anstelle von

$$((bi)(cj))(b'i) = (bi)((cj)(b'i))$$

die Gleichungen

$$(ij)i = i(ji)$$

zu beweisen. In denjenigen Fällen, in denen eine der Quaternionen q_1, q_2 oder q_3 gleich 1 ist, ist die Gleichung (4) offensichtlich. Deshalb läuft die Aufgabe auf eine Überprüfung dieser Gleichung für die Fälle hinaus, in denen q_1, q_2 und q_3 beliebige der Quaternionen i, j und k sind. Im ganzen unterliegen auf diese Weise 27 Gleichungen der Überprüfung. Wir schreiben als Beispiele einige von ihnen auf:

$$(ii)i = i(ii), \quad (ii)j = i(ij), \quad (ij)i = i(ji), \quad (ij)k = i(jk)$$

Die Richtigkeit jeder der 27 Gleichungen folgt leicht aus der Multiplikationstafel (2).

Die Multiplikation der Quaternionen ist also assoziativ. Später werden wir sehen, dass das System der Quaternionen in vielen der wichtigsten Beziehungen dem System der komplexen Zahlen ähnlich ist. So haben wir uns eben von der Assoziativität der Multiplikation der Quaternionen überzeugt.
Die Ähnlichkeit von Quaternionen und komplexen Zahlen ist jedoch bedeutend größer. Erstens ist es, wie bereits erwähnt wurde, möglich, Quaternionen durcheinander zu dividieren.

Zweitens kann man auf natürliche Weise für Quaternionen den Begriff des absoluten Betrags so einführen, dass die Regel "der absolute Betrag eines Produktes ist gleich dem Produkt der absoluten Beträge" erfüllt wird. Der aufgezeigten Ähnlichkeit liegt die Existenz der Operation des Konjugierens im System der Quaternionen zugrunde, die übereinstimmende Eigenschaften mit der gleichen Operation bei komplexen Zahlen besitzt.

1.3.4 Konjugierte Quaternionen

In Analogie zu den komplexen Zahlen führen wir folgende Definition ein.

Gegeben sei die Quaternion

$$q = a + bi + ci + dk$$

Die Quaternion

$$\overline{q} = a - bi - cj - dk \tag{7}$$

wird zu ihr konjugiert genannt.
Es ist offensichtlich, dass die Summe konjugierter Quaternionen eine reelle Zahl ist. Ebenso ist auch das Produkt $q\overline{q}$ eine reelle Zahl, was sofort aus der Formel (3) für die Multiplikation folgt:

$$(a + bi + cj + dk)(a - bi - cj - dk) = a^2 + b^2 + c^2 + d^2 \tag{8}$$

Indem wir die Analogie mit den komplexen Zahlen fortführen, werden wir die reelle Zahl

$$\sqrt{a^2 + b^2 + c^2 + d^2}$$

den absoluten Betrag der Quaternion q nennen und vereinbaren, den absoluten Betrag von q mit $|g|$ zu bezeichnen. Dann wird die letzte Gleichung so geschrieben

$$q\overline{q} = |q|^2$$

also genau die gleiche Formel wie für die komplexen Zahlen.

Bemerkung. Wenn q' eine rein imaginäre Quaternion

$$q' = bi + cj + dk$$

ist, dann folgt aus Gleichung (8)

$$q'^2 = -(b^2 + c^2 + d^2) \leq 0$$

Umgekehrt ist, wenn das Quadrat irgendeiner Quaternion eine reelle Zahl kleiner oder gleich Null ist, diese Quaternion rein imaginär[1].
Auf diese Weise können die Quaternionen $bi + cj + dk$, und nur sie, durch die Bedingung charakterisiert werden, dass ihre Quadrate reelle Zahlen kleiner oder gleich 0 darstellen. Damit kann man eine andere Beschreibung der Operation des Konjugierens geben: für jede Quaternion q mit der eindeutigen Darstellung $a+q'$, wobei q' eine Quaternion ist, deren Quadrat eine reelle Zahl kleiner oder gleich 0 ist, gilt für die konjugierte Quaternion $\overline{q} = a - q'$. Diese Bemerkung werden wir später im § 17 brauchen.

Die direkte Überprüfung zeigt, dass die Operation des Konjugierens die folgenden Eigenschaften besitzt:

$$\overline{q_1 + q_2} = \overline{q_1} + \overline{q_2} \tag{9}$$

(die Konjugierte einer Summe ist gleich der Summe der Konjugierten) und

$$\overline{q_1 q_2} = \overline{q_1}\ \overline{q_2} \tag{10}$$

(die Konjugierte eines Produktes ist gleich dem Produkt der Konjugierten in umgekehrter Reihenfolge). Diese Gleichungen sind, wie sich der Leser erinnern wird, auch für den Fall der komplexen Zahlen gültig.
Man muss nur im Auge behalten, dass man bei den komplexen Zahlen anstelle von $\overline{z_2}\ \overline{z_1}$ auch $\overline{z_1}\ \overline{z_2}$ schreiben kann (da das Produkt nicht von der Reihenfolge der Faktoren abhängt), während im allgemeinen für die Quaternionen $\overline{q_2}\ \overline{q_1}$ nicht gleich $\overline{q_1}\ \overline{q_2}$ ist. Um sich von der Gültigkeit der Gleichung (10) zu überzeugen, genügt es, sie für jeden der Fälle zu überprüfen, in denen anstelle von q_1, und q_2 i, j und k genommen wird.
Die Überprüfung lässt sich leicht mit Hilfe der Tafel (2) durchführen. Zum Beispiel ist

$$\overline{ii} = \overline{-1} = -1, \qquad \text{aber auch } \overline{i}\ \overline{i} = (-i)(-i) = i^2 = -1$$

$$\overline{ij} = \overline{k} = -k, \qquad \text{aber auch } \overline{j}\ \overline{i} = (-j)(-i) = ji = -k \quad \text{usw.}$$

[1] In der Tat, für die Quaternion $q = a + q' = a + bi + cj + dk$ erhalten wir

$$q^2 = (a + q')(a + q') = a^2 + q'^2 + 2aq' = a^2 - b^2 - c^2 - d^2 + 2aq'$$

Wenn dieser Ausdruck eine reelle Zahl darstellt und $a \neq 0$ ist, dann ist $q' = 0$. Dann ist aber $q = a$, und folglich kann nicht $q \leq 0$ sein.

1.3.5 Ausführbarkeit der Division im System der Quaternionen

Zunächst wenden wir unsere Aufmerksamkeit auf den bestehenden Unterschied in der Fragestellung nach der Division der Quaternionen und der Division der komplexen Zahlen.
Für die komplexen Zahlen wird, wie sich der Leser erinnert, als Quotient von z_1 und z_2 die Lösung der Gleichung $z_2 x = z_1$ bezeichnet. Für die Quaternionen aber hängt das Produkt von der Reihenfolge der Faktoren ab, deshalb ist es notwendig, anstelle einer Gleichung zwei zu betrachten:

$$q_2 x = q_1 \qquad \text{und} \qquad x q_2 = q_1 \tag{11,11'}$$

Demgemäß werden wir die Lösung der ersten Gleichung den linken Quotient von q_1 durch q_2 nennen und ihn mit x_l bezeichnen, die Lösung der zweiten hingegen rechter Quotient x_r (im Falle der komplexen Zahlen stimmen beide Quotienten offensichtlich überein).

Um die Gleichungen (11) und (11') zu lösen, wenden wir das gleiche Verfahren wie auch im Falle der komplexen Zahlen an. Wir multiplizieren beide Seiten der Gleichung (11) von links zuerst mit $\overline{q_2}$ und dann mit $1/|q_2|^2$. Wir erhalten

$$x = \frac{1}{|q_2|^2}\overline{q_2}q_1$$

Durch Einsetzen in Gleichung (11) überzeugen wir uns, dass dieser Ausdruck tatsächlich die Lösung ist. Auf diese Weise ist

$$x_l = \frac{1}{|q_2|^2}\overline{q_2}q_1$$

Analog findet man x_r

$$x_r = \frac{1}{|q_2|^2}q_1\overline{q_2}$$

Als Beispiel ermitteln wir den linken und den rechten Quotienten der Division von k durch $1 + i + k$:

$$\begin{aligned} x_l &= \frac{1}{3}(1 - i - k)k = \frac{1}{3}(k + j + 1) \\ x_r &= \frac{1}{3}k(1 - i - k) = \frac{1}{3}(k - j + 1) \end{aligned}$$

Somit haben wir zwei der wichtigsten Eigenschaften des Systems der Quaternionen ermittelt:

1) Für die Multiplikation der Quaternionen gilt das Assoziativgesetz;
2) Die Quaternionen sind ein System mit Division.

1.3.6 Der absolute Betrag eines Produktes

Eine weitere wichtige Eigenschaft der Quaternionen besteht darin, dass der absolute Betrag eines Produktes gleich ist dem Produkt der absoluten Beträge.
Der Beweis ist genau der gleiche wie im Falle der komplexen Zahlen; in ihm wird die Formel

$$\overline{q_1 q_2} = \overline{q_2}\ \overline{q_1}$$

und die Eigenschaft der Assoziativität für die Multiplikation der Quaternionen verwendet. Hier dieser Beweis:

$$|q_1 q_2|^2 = (q_1 q_2)\overline{(q_1 q_2)} = (q_1 q_2)(\overline{q_2}\ \overline{q_1}) = q_1(q_2\overline{q_2})\overline{q_1} = |q_1|^2|q_2|^2$$

1.3.7 Identität für vier Quadrate, Allgemeine Aufgabenstellung über die Summe von Quadraten

Wenn man die von uns erhaltene Gleichung

$$|q_1q_2|^2 = |q_1|^2|q_2|^2 \tag{12}$$

ausführlich schreibt, führt sie zu einer interessanten Identität. Es möge

$$q_1 = a + bi + cj + dk \qquad \text{und} \qquad q_2 = a' + b'i + c'j + d'k$$

sein; dann ist q_1q_2 der Ausdruck, der auf der rechten Seite von Gleichung (3) steht. Folglich nimmt die Formel (12), von rechts nach links gelesen, die Form

$$\begin{aligned}&(a^2 + b^2 + c^2 + d^2)(a'^2 + b'^2 + c'^2 + d'2^2) = \\ &= (aa' - bb' - cc' - dd')^2 + (ab' + ba' + cd' - dc')^2 \\ &+ (ac + ca' + db' - ba')^2 + (ad' + da' + bc' - cb')^2\end{aligned} \tag{13}$$

an. Wir erinnern daran, dass uns im Falle der komplexen Zahlen die Gleichung

$$|z_1z_2|^2 = |z_1]^2|z_2|^2$$

zur analogen Identität

$$(a^2 + b^2)(a'^2 + b'^2) = (aa' - bb')^2 + (ab' + ba')^2 \tag{14}$$

führte, der wir eine solche Deutung gaben: das Produkt einer Summe von zwei Quadraten mit einer Summe von zwei Quadraten ist erneut eine Summe von zwei Quadraten. Eine analoge Deutung gestattet offensichtlich auch die Identität (13):
Das Produkt einer Summe von vier Quadraten mit einer Summe von vier Quadraten ist erneut eine Summe von vier Quadraten. Wenn man von den komplexen Zahlen und den Quaternionen abstrahiert, ist es natürlich, jetzt diese Frage zu stellen:

Für welche n kann man die Identität "das Produkt einer Summe von n Quadraten mit einer Summe von n Quadraten ist gleich einer Summe von n Quadraten" finden?

Für $n = 1$ folgt sofort die Lösung:

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

aber dies ist sehr einfach. Für $n = 2$ und $n = 4$ ist die Antwort, wie wir sehen, auch positiv. Das ist aber von vornherein durchaus nicht klar!
Wie verhält es sich aber mit $n = 3$, mit $n = 5, 6$ usw.?

Wie wir bereits bemerkten, erhielt diese Frage lange Zeit keine endgültige Lösung. Eine erschöpfende Antwort wurde im Jahre 1898 durch den deutschen Mathematiker A. Hurwitz erhalten, der einen erstaunlichen Satz bewies:

Die Identität des uns interessierenden Typs ist nur für $n = 1, 2, 4, 8$ möglich und für alle anderen n unmöglich.

Damit beim Leser nicht irgendeine Unklarheit in der Aufgabenstellung über die Summe von Quadraten zurückbleibt, werden wir sie jetzt genauer formulieren.
Es mögen $a_1, a_2, ..., a_n$ und $b_1, b_2, ..., b_n$ zwei Folgen sein. Wir werden eine Summe Form zweiten Grades nennen, wenn ihre Summanden so aufgebaut sind, dass jeder von ihnen das Produkt

eines Elements der ersten Folge mit einem Element der zweiten Folge ist und mit einem beliebigen (reellen) Zahlenfaktor verbunden ist. Zum Beispiel ist der Ausdruck

$$a_1b_1 + 8a_1b_2 - 2a_3b_5 + 3a_3b_n$$

eine Form zweiten Grades. Die genaue Formulierung der Aufgabe über die Summe von Quadraten besteht in folgendem.
Es ist erforderlich zu beantworten:

Wie muss die, Zahl n sein und wie müssen die n Formen zweiten Grades, die wir der Kürze halber mit Φ_1, Φ_2, ..., Φ_n, bezeichnen, ausgewählt werden, damit die Identität

$$(a_1^2 + a_2^2 + ... + a_n^2)(b_1^2 + b_2^2 + ... + b_n^2) = \Phi_1^2 + \Phi_2^2 + ... + \Phi_n^2 \qquad (*)$$

gilt. Die von uns früher gezeigten Identitäten für die komplexen Zahlen und die Quaternionen waren offensichtlich gerade von diesem Typ. Für komplexe Zahlen ist

$$(a_1^2 + a_2^2)(b_1^2 + b_2^2) = (a_1b_1 - a_2b_2)^2 + (a_1b_2 + a_2b_1)^2$$

und für Quaternionen

$$\begin{aligned}
&(a_1^2 + a_2^2 + a_3^2 + a_4^2)(b_1^2 + b_2^2 + b_3^2 + b_4^2) = \\
&= (a_1b_1 - a_2b_2 - a_3b_3 - a_4b_4)^2 + (a_1b_2 + a_2b_1 + a_3b_4 - a_4b_3)^2 \\
&+ (a_1b_3 + a_3b_1 + a_4b_2 - a_2b_4)^2 + (a_1b_4 + a_4b_1 + a_2b_3 - a_3b_2)^2
\end{aligned}$$

In Übereinstimmung mit der allgemeinen Aufgabenstellung haben wir die Bezeichnungen in den Identitäten (13) und (14) geändert.
Im § 6 werden wir auf der Basis eines weiteren Zahlensystems (der sogenannten Oktaven) die Identität (*) für $n = 8$ konstruieren.

So umfasst das Verzeichnis der Werte n in der Identität (*) die Zahlen 1, 2, 4 und 8. Der oben erwähnte Satz von Hurwitz, der behauptet, dass andere Werte von n nicht möglich sind, wird in Kapitel 3 bewiesen, nachdem wir alle dafür notwendigen Fakten kennengelernt haben.

1.4 Quaternionen und Vektoralgebra

Die Entdeckung der Quaternionen in der Mitte des 19. Jahrhunderts gab den Anstoß für die verschiedenartigsten Untersuchungen auf dem Gebiet der Mathematik und der Physik. Insbesondere entstand durch die Quaternionen ein außerordentlich fruchtbares Gebiet der Mathematik - die Vektoralgebra.
Wir werden in diesem Paragraphen über die Verbindungen sprechen, die zwischen den Rechnungen mit Quaternionen und den Operationen mit Vektoren im dreidimensionalen Raum existieren.

1.4.1 Skalarer und vektorieller Teil eines Quaternions

Wir erinnern den Leser an einige aus der Geometrie bekannte Sätze. Wenn man in einem gewöhnlichen Raum ein rechtwinkliges Koordinatensystem einführt und mit i, j und k Vektoren der Länge 1 bezeichnet, die vom Koordinatenursprung in Richtung der Koordinatenachsen ausgehen (Abb. 2), dann wird jede Summe der Form

$$bi + cj + dk$$

wobei b, c und d reelle Zahlen sind, genau einen Vektor darstellen. Dieser Vektor verläuft vom Koordinatenursprung O zum Punkt M mit den Koordinaten b, c, d.

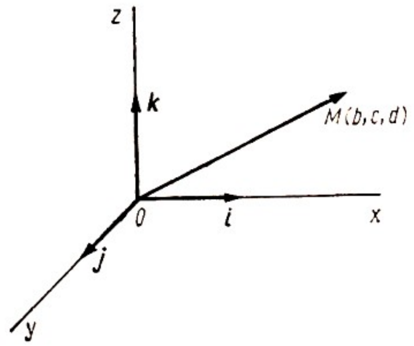


Abb.2

Auf die Quaternionen zurückkommend, bemerken wir, dass jede Quaternion

$$q = a + bi + cj + dk$$

formal die Summe der reellen Zahl a und des Vektors $bi + cj + dk$ darstellt. Die Zahl a werden wir den skalaren Teil (oder Realteil) und den Ausdruck $bi + cj + dk$ den vektoriellen (oder imaginären) Teil der Quaternion q nennen. Wir werden jetzt zwei rein vektorielle Quaternionen (Vektoren)

$$q_1 = b_1 i + c_1 j + d_i k \qquad \text{und} \qquad q_2 = b_2 j + c_2 j + d_2 k$$

betrachten. Wenn wir sie nach der Regel der Multiplikation der Quaternionen miteinander multiplizieren, so erhalten wir

$$q_1 q_2 = -(b_1 b_2 + c_1 c_2 + d_1 d_2) + (c_1 d_2 - d_1 c_2)i + (d_1 b_2 - b_1 d_2)j + (b_1 c_2 - c_1 b_2)k \tag{1}$$

Wir schreiben den skalaren Teil und den vektoriellen Teil der Quaternion $q_1 q_2$ einzeln:

skalarer Teil $-(b_1 b_2 + c_1 c_2 + d_1 d_2)$ (2)
vektorieller Teil $(c_1 d_2 - d_1 c_2)i + (d_1 b_2 - b_1 d_2)j + (b_1 c_2 - c_1 b_2)k$ (3)

1.4.2 Das Skalarprodukt

Jeder der Ausdrücke (2) und (3) besitzt eine bestimmte geometrische Bedeutung. Die Summe $b_1 b_2 + c_1 c_2 + d_1 d_2$ ist, wie wir sofort zeigen werden, gleich $|q_1||q_2| \cos\varphi$, d.h., dem Produkt der Längen der Vektoren q_1 und q_2 (oder, was das gleiche bedeutet, der absoluten Beträge der Quaternionen q_1 und q_2) mit dem Kosinus des eingeschlossenen Winkels.
Ein solches Produkt wird in der Mathematik sehr häufig betrachtet. Es trägt den besonderen Namen Skalarprodukt der Vektoren q_1 und q_2 und wird gewöhnlich mit (q_1,q_2) bezeichnet. Wir betonen, dass das Skalarprodukt eine (reelle) Zahl und kein Vektor ist.
Auf diese Weise haben wir durch Definition

$$(q_1,q_2) = |q_1||q_2| \cos\varphi$$

Wir wollen noch die Formel

$$(q_1,q_2) = b_1 b_2 + c_1 c_2 + d_1 d_2$$

beweisen.
In der Abb. 3 ist ein Dreieck dargestellt, das durch die Vektoren q_1 und q_2 gebildet wird. Eine seiner Ecken befindet sich im Koordinatenursprung, die zwei anderen Ecken sind die Punkte M_1 und M_2 (die Endpunkte der Vektoren q_1 und q_2), deren Koordinaten entsprechend b_1, c_1, d_1 und b_2, c_2, d_2 sind.

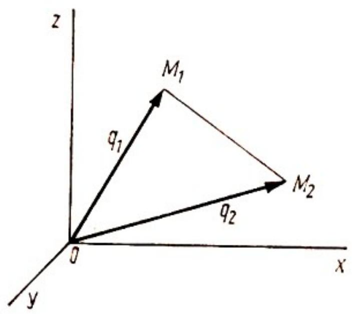


Abb.3

Wir haben
$$(OM_1)^2 = b_1^2 + c_1^2 + d_1^2 \qquad , \qquad (OM_2)^2 = b_2^2 + c_2^2 + d_2^2$$
und
$$(M_1M_2)^2 = (b_1 - b_2)^2 + (c_1 - c_2)^2 + (d_1 - d_2)^2$$
woraus folgt
$$(M_1M_2)^2 = (OM_1)^2 + (OM_2)^2 - 2(b_1b_2 + c_1c_2 + d_1d_2)$$
Nach dem bekannten Kosinussatz ist aber
$$(M_1M_2)^2 = (OM_1)^2 + (OM_2)^2 - 2OM_1 \cdot OM_2 \cdot \cos\varphi$$
wobei φ der Winkel an der Ecke O ist, d.h., der Winkel zwischen den Vektoren q_1 und q_2. Durch Vergleichen der hingeschriebenen Gleichungen erhalten wir
$$OM_1 \cdot OM_2 \cdot \cos\varphi = b_1b_2 + c_1c_2 + d_1d_2$$
was zu beweisen war.
Folglich ist der Realteil des Produktes der vektoriellen Quaternionen q_1 und q_2 gleich dem mit dem Minuszeichen versehenen Skalarprodukt von q_1 und q_2.

Wir bemerken: wenn die Vektoren q_1 und q_2 senkrecht aufeinander stehen, so ist ihr Skalarprodukt gleich Null ($\varphi = \pi/2$, $\cos\varphi = 0$); folglich ist auch der Realteil des Produktes der Quaternionen q_1q_2 gleich Null. In diesem Falle wird die Quaternion q_1q_2 zu einem "reinen" Vektor.
Die Umkehrung ist natürlich auch richtig: wenn die Quaternion q_1q_2 ein "reiner" Vektor ist, dann ist das Skalarprodukt von q_1 und q_2 gleich Null, folglich ist $\cos\varphi = 0$ und die Vektoren q_1 und q_2 stehen senkrecht aufeinander.
Es bleibt noch zu bemerken, wenn q_1 und q_2 senkrecht aufeinander stehen, ist $q_1q_2 = -q_2q_1$. Dies ist sofort aus Formel (1) ersichtlich, wenn man berücksichtigt, dass der Realteil von q_1q_2 gleich Null ist.

1.4.3 Das Vektorprodukt

Die geometrische Bedeutung des vektoriellen Teils des Produktes q_1q_2 zu bestimmen, d.h. des Ausdrucks, der auf der rechten Seite der Gleichung (3) steht, ist etwas schwieriger. Dieser Ausdruck wird Vektorprodukt des Vektors q_1 mit dem Vektor q_2 genannt und mit $q_1 \times q_2$ bezeichnet:
$$q_1 \times q_2 = (c_1d_2 - d_1c_2)i + (d_1b_2 - b_1d_2)j + (b_1c_2 - c_1b_2)k$$
Es zeigt sich, dass der Vektor $q_1 \times q_2$ senkrecht auf jedem der Vektoren q_1 und q_2 steht und seine Länge gleich $|q_1| \cdot |q_2| \sin\varphi$ ist oder, was das gleiche ist, dem Flächeninhalt S des

Parallelogramms, das durch die Vektoren q_1 und q_2 aufgespannt wird.

Um zu beweisen, dass die Vektoren $q_1 \times q_2$ und q_1 senkrecht aufeinander stehen, genügt es, wie wir wissen, zu überprüfen, dass der Realteil des Produktes dieser Quaternionen gleich Null ist oder dass ihr Produkt ein "reiner" Vektor ist. Aufgrund von (1) und (4) gilt aber $q_1 \times q_2 = q_1 q_2 + (q_1,q_2)$, deshalb ist[2]

$$q_1(q_2 \times q_3) - q_1(q_1 q_2 + (q_1,q_2)) = q_1^2 q_2 + (q_1,q_2)q_1 = -|q_1|^2 q_2 + (q_1,q_2)q_1$$

Rechts steht die Summe zweier Vektoren, d.h, erneut ein Vektor. Dass die Vektoren $q_1 \times q_2$ und q_2 senkrecht aufeinander stehen, wird analog bewiesen.

Wir bestimmen jetzt die Länge des Vektors $q_1 \times q_2$. Sein Quadrat ist gleich

$$(c_1 d_2 - d_1 c_2)^2 + (d_1 b_2 - b_1 d_2)^2 + (b_1 c_2 - c_1 b_2)^2$$

oder (nach identischer Umformung)

$$(b_1^2 + c_1^2 + d_1^2)(b_2^2 + c_2^2 + d_2^2) - (b_1 b_1 + c_1 c_2 + d_1 d_2)^2$$

Der letzte Ausdruck ist gleich

$$|q_1|^2 |q_2|^2 - (q_1,q_2)^2$$

oder, wenn man sich die Definition des Skalarprodukts in Erinnerung ruft, gleich

$$|q_1|^2 |q_2|^2 - |q_1|^2 |q_2|^2 \cos^2\varphi \qquad \text{bzw.} \qquad |q_1|^2 |q_2|^2 \sin^2\varphi$$

Folglich ist das Quadrat der Länge des Vektors $q_1 \times q_2$ gleich

$$|q_1|^2 |q_2|^2 \sin^2\varphi$$

d.h. S^2, was zu beweisen war.

Die von uns aufgezeigten Eigenschaften des Vektors $q_1 \times q_2$, nämlich das Senkrechtstehen auf q_1 und q_2 sowie seine Länge S, bestimmen ihn noch nicht vollständig.

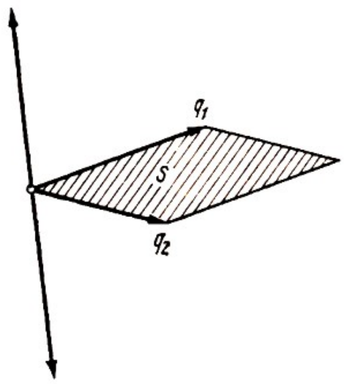


Abb.4

[2] Im Verlauf der Rechnung haben wir q_1^2 durch die Zahl $-|q_1|^2$ ersetzt. Dies kann man aufgrund der Gleichung (1) tun. Aus (1) folgt

$$q_1^2 = -(b_1^2 + c_1^2 + d_1^2) + 0i + 0j + 0k = -|q_1|^2$$

Genau zwei einander entgegengesetzte Vektoren (Abb. 4) besitzen solche Eigenschaften. Welcher von ihnen ist aber $q_1 \times q_2$? Die letzte charakteristische Eigenschaft, die die Beschreibung des Vektors $q_1 \times q_2$ abschließt, besteht in folgendem: die Vektoren q_1, q_2 und $q_1 \times q_2$ sind im Raum ähnlich wie i, j und k orientiert.

Damit wollen wir sagen, wenn man von der Spitze des Vektors $q_1 \times q_2$, auf die Ebene der Vektoren q_1 und q_2 sieht, so erfolgt die Drehung von q_1 nach q_2 um den kleinsten Winkel in der gleichen Richtung (d.h. im Uhrzeigersinn oder entgegengesetzt), in der man von der Spitze des Vektors k die Drehung von i nach j um den kleinsten Winkel sehen kann (Abb. 5)[3].

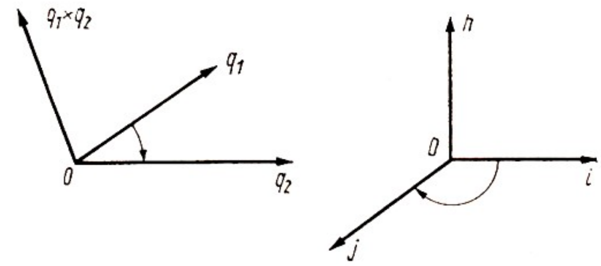


Abb.5

Folglich gilt für die Multiplikation rein vektorieller Quaternionen die Formel

$$q_1 q_2 = -(q_1, q_2) + q_1 \times q_2$$

wobei (q_1, q_2) das skalare und $q_1 \times q_2$ das vektorielle Produkt der Vektoren q_1 und q_2 ist. Wir sehen daher, dass das Skalarprodukt und das Vektorprodukt sich so darstellen, als wären sie "Bruchstücke" des Produktes der Quaternionen.

Die Operationen der skalaren und der vektoriellen Multiplikation zusammen mit der Addition von Vektoren und der Multiplikation eines Vektors mit einer Zahl liegen einem ganzen Gebiet der Mathematik zugrunde, der Vektoralgebra, die sowohl in der Mathematik selbst, als auch in der Physik (besonders in der Mechanik) zahlreiche Anwendungen besitzt. Verschiedene dieser Anwendungen sind dem Leser wahrscheinlich bekannt.

Die Arbeit ist das Skalarprodukt des Vektors der Kraft mit dem Vektor des Weges u.ä.m. Wir bemerken, dass, genaugenommen, die Vektoralgebra bedeutend später als die ersten Arbeiten über die Theorie der Quaternionen auftrat.
Die Arbeiten des Schöpfers der Theorie der Quaternionen, des englischen Mathematikers W. Hamilton, gehen bis in die fünfziger Jahre des vergangenen Jahrhunderts zurück, während die Hauptsätze der Vektoralgebra erst in den achtziger Jahren des vergangenen Jahrhunderts in den Arbeiten des amerikanischen Mathematikers und Physikers J. W. Gibbs formuliert wurden.

1.4.4 Geometrische Deutung der Multiplikation einer beliebigen Quaternion mit einer rein vektoriellen Quaternion

Da die Multiplikation der Quaternionen zwei Formen der Vektormultiplikation (skalare und vektorielle) in sich vereinigt, werden die Quaternionen zu einem bemerkenswerten Hilfsmittel bei der Lösung einiger Aufgaben der Geometrie und der Mechanik. Etwas weiter unten werden

[3] Hier eine kurze Erklärung dieses Sachverhaltes. Wir stellen uns vor, dass sich die Spitzen der Vektoren i und j, wenn man sie im Raum verschiebt, den Spitzen der Vektoren q_1 und q_2 (entsprechend) nähern. In der Ausgangslage ist das Tripel i, j, $i \times j$ ähnlich orientiert wie i, j, k (da $i \times j = k$). Da sich während des Verschiebens die Orientierung nicht ändern kann, muss das Endtripel q_1, q_2, $q_1 \times q_2$, die gleiche Orientierung wie i, j, k haben.

wir als Beispiel eine sehr schwierige Aufgabe anführen, deren Lösung man mit Hilfe der Quaternionen besonders einfach und elegant erhält.

Wir müssen jedoch dazu zuerst über die geometrische Bedeutung der Multiplikation einer beliebigen Quaternion mit einer rein vektoriellen Quaternion sprechen. Es möge

$$q = a + bi + cj + dk$$

eine beliebige Quaternion sein, deren absoluter Betrag gleich 1 ist, d.h.

$$a^2 + b^2 + c^2 + d^2 = 1$$

Wir setzen

$$q = a + q' \qquad \text{mit} \qquad q'' = bi + cj + dk$$

Weil $|a^2| + |q']^2 = 1$ gilt, existiert ein solcher Winkel φ, dass

$$a = \cos\varphi \qquad \text{und} \qquad |q'| = \sin\varphi$$

ist. Offensichtlich ist $q' = |q'|p$, wobei p ein Vektor der Länge 1 ist. Folglich ist

$$q = \cos\varphi + p\sin\varphi$$

Wir betonen noch einmal, dass jede Quaternion mit einem absoluten Betrag gleich 1 in einer solchen Form (wobei p ein Vektor der Länge 1 ist) dargestellt werden kann. Wir multiplizieren jetzt von rechts die Quaternion q mit irgendeiner vektoriellen Quaternion v, wobei wir uns auf den Fall beschränken, dass der Vektor v senkrecht auf p steht. Wir erhalten

$$qu = (\cos\varphi + p\sin\varphi)v = v\cos\varphi + pv\sin\varphi$$

Da p und v senkrecht aufeinander stehen, besitzt das Produkt pv einen verschwindenden Realteil; der vektorielle Teil wird gleich $p \times v$ sein, d.h., ein Vektor der Länge $|p| \cdot |v| \sin\sin\pi/2 = |v|$, der senkrecht auf p und v steht und in Bezug auf p und v auf die gleiche Weise orientiert ist, wie der Vektor k in Bezug auf i und j.
Wir werden diesen Vektor mit $\tilde{v}$ bezeichnen. Man kann sagen, dass $\tilde{v}$ aus v durch Drehung des Vektors p[4] um $\pi/2$ erhalten wurde. Also ist

$$qv = v\cos\varphi + \overline{v}\sin\varphi$$

Es genügt jetzt ein Blick auf Abb. 6, um zu verstehen, dass der Vektor qv aus v durch Drehung um die Achse des Vektors p um den Winkel φ erhalten wurde.

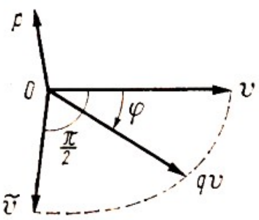


Abb.6

[4] Der Begriff "Drehung um p" ist zweideutig, da man in zwei Richtungen drehen kann. Von nun an betrachten wir eine Drehung (um p) stets in der Richtung, in der sich die kürzeste Drehung von i nach j (um k) vollzieht.

Folglich stellt, wenn p irgendein Vektor der Länge 1 und v ein beliebiger Vektor ist, der senkrecht auf p steht, die Multiplikation von v von links mit der Quaternion

$$q = \cos\varphi + p\sin\varphi$$

die Drehung des Vektors v um die Achse p um den Winkel dar. Bis zu einem gewissen Grad kann man diese Tatsache als geometrische Deutung der Multiplikation (von links) mit der Quaternion q betrachten; enttäuschend ist, dass man den Vektor v nicht willkürlich, sondern nur senkrecht auf p stehend wählen kann.

1.4.5 Darstellung einer beliebigen Drehung im Raum mit Hilfe der Quaternionen

Man kann, wie sich erweist, auch die Drehung eines jeden Vektors v um die Achse p in Quaternionenform schreiben; man muss jedoch dazu mehr Operationen auf v ausüben: anstelle der Multiplikation von links mit q wird der kompliziertere Ausdruck

$$qvq^{-1}$$

benötigt. Hier bedeutet q^{-1} die Quaternion, die zu q invers ist, d.h., eine solche, für die gilt $qq^{-1} = 1$. Man kann leicht sehen, dass

$$q^{-1} = \cos\varphi - p\sin\varphi$$

gilt; in der Tat ist

$$(\cos\varphi + p\sin\varphi)(\cos\varphi - p\sin\varphi) = \cos^2\varphi - p^2\sin^2\varphi = \cos^2\varphi + \sin^2\varphi = 1$$

Wir werden zeigen, dass man den Vektor qvq^{-1} aus v durch Drehung um die Achse p um den Winkel 2φ erhält!

Zunächst möge v senkrecht auf p stehen. Wir haben

$$qvq^{-1} = qv(\cos\varphi - p\sin\varphi) = qv\cos\varphi - (qv)p\sin\varphi$$

Wie wir aber bereits wissen, ist qv erneut ein Vektor, der senkrecht auf p steht; deshalb ist $(qv)p = -p(qv)$. Die Quaternion $p(qv)$ ist, wie wir früher sahen, der Vektor, den man aus qv durch Drehung um die Achse p um den Winkel $\pi/2$ (Abb. 7) erhalten kann.

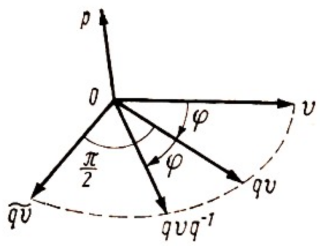


Abb.7

Wir bezeichnen ihn wie früher mit $\tilde{qv}$. Folglich ist

$$qvq^{-1} = qv\cos\varphi + \tilde{qv}\sin\varphi$$

Der Ausdruck, der auf der rechten Seite steht, stellt den Vektor dar, der aus qv durch Drehung um p um den Winkel φ erhalten wurde.

Wenn man noch berücksichtigt, dass der Vektor qv selbst aus v durch dieselbe Drehung erhalten wurde, zeigt sich, dass man qvq^{-1} aus v durch Drehung um p um den Winkel 2φ erhält.

Um den allgemeinen Fall zu betrachten, bemerken wir: Wenn ein Vektor v proportional p ist (d.h. $v = \lambda p$), dann gelten offensichtlich $qv = vq$ und $qvq^{1-} = vqq^{-1} = v$.
Es möge jetzt v ein beliebiger Vektor sein. Wir zerlegen ihn in zwei Bestandteile

$$v = v_1 + v_2$$

wobei v_1 ein Vektor ist, der senkrecht auf p steht und v_2 proportional p ist. Dann ist

$$qvq^{-1} = qv_1q^{-1} + qv_2q^{-1} = qv_1q^{-1} + v_2$$

Daraus ist ersichtlich, dass der Bestandteil v_1 sich um den Winkel 2φ um p dreht, der Bestandteil v_2 aber unverändert bleibt. Als Ergebnis dreht sich der ganze Vektor v um den Winkel 2φ um die Achse p.

Wir haben so bewiesen, dass jeder Vektor v bei einer Drehung um die Achse p um den Winkel 2φ in qvq^{-1} übergeht, wobei

$$q = \cos\varphi + p\sin\varphi$$

ist. Deshalb sagen wir, dass die beschriebene Drehung der Quaternion q entspricht.

1.4.6 Die „Addition“ von Drehungen

Wir hatten früher versprochen, die Anwendung der Quaternionen an einem Beispiel, einer schwierigen Aufgabe aus der Geometrie, zu beschreiben. Wir tun dies jetzt. Die Aufgabe, von der die Rede sein wird, behandelt die Zusammensetzung von Drehungen (im Raum).

Die Drehung möge um den Winkel $2\varphi_1$ um irgendeine Achse, die durch den Einheitsvektor p_1 charakterisiert ist, ausgeführt werden; danach möge eine andere Drehung um den Winkel $2\varphi_2$ um die Achse, die durch den Einheitsvektor p_2 charakterisiert ist, ausgeführt werden.
Als Ergebnis erhalten wir eine bestimmte neue Drehung, das Resultat der aufeinanderfolgenden Ausführung der zwei angegebenen. Es fragt sich, wie man die Achse und den Winkel der resultierenden Drehung findet?

Bei der ersten Drehung geht der beliebige Vektor v, wie wir wissen, in $v_1 = q_1vq_1^{-1}$ über, wobei $q_1 = \cos\varphi_1 + p_1\sin\varphi_1$ ist. Bei der zweiten Drehung geht v_1 in

$$v_2 = q_2v_1q_2^{-1} = q_2(q_1vq_1^1)q_2^{-1} = (q_2q_1)v(q_2q_1)^{-1}$$

über (wir bemerken, dass $(q_2q_1)^{-1}$ gleich $q_1^{-1}q_2^{-1}$ ist, weil $(q_2q_1)(q_1{-}1q_2^{-1}) = 1$ ist). Als Ergebnis der aufeinanderfolgenden Ausführung zweier Drehungen geht der Vektor v in

$$v_2 = (q_2q_1)v)q_2q_1)^{-1}$$

über. Auf diese Weise erhält man als Resultat von zwei aufeinanderfolgenden Drehungen, die den Quaternionen q_1 und q_2 entsprechen, eine dritte Drehung, die der Quaternion q_2q_1 entspricht.

Es bereitet keine Schwierigkeit, die Quaternion q_2q_1 zu berechnen, da die Multiplikationsregel für Quaternionen bekannt ist. Wenn wir q_2q_1 gefunden haben, bringen wir diese Quaternion in die Form

$$q_2q_1 = \cos\psi + p\sin\psi \tag{6}$$

wobei p ein Vektor mit der Länge 1 ist. Dann ist die resultierende Drehung die Drehung um die Achse p um den Winkel 2φ. Wie wir sehen, haben wir die Antwort mit Hilfe der Quaternionen sehr einfach erhalten!

Wir betrachten ein Beispiel. Die erste Drehung möge um den Winkel $\pi/2$ um die z-Achse ausgeführt werden, die zweite hingegen um die y-Achse um den gleichen Winkel. Der ersten Drehung entspricht die Quaternion

$$q_1 = \cos\frac{\pi}{4} + i\sin\frac{\pi}{4} = \frac{\sqrt{2}}{2}(1+i)$$

der zweiten die Quaternion

$$q_2 = \frac{\sqrt{2}}{2}(1+j)$$

Im gegebenen Fall ist

$$q_2q_1 = \frac{1}{2}(1+i)(1+j) = \frac{1}{2}(1+i+j-k)$$

Um diese Quaternion in die Form (5) zu bringen, stellen wir fest, dass ihr Realteil gleich $0{,}5 = \cos(\pi/3)$ ist. Davon ausgehend schreiben wir

$$q_2q_1 = \cos\frac{\pi}{3}\left[\frac{1}{\sqrt{3}}(i+j-k)\right]\sin\frac{\pi}{3}$$

so verläuft die resultierende Drehung um den Winkel $2\pi/3$ um den Vektor $p = (i+j-k)/\sqrt{3}$.

1.5 Hyperkomplexe Zahlen

1.5.1 Definition eines hyperkomplexen Zahlensystems

Die von uns betrachteten komplexen, binären und dualen Zahlen sowie die Quaternionen werden durch den allgemeineren Begriff des hyperkomplexen (überkomplexen) Zahlensystems zusammengefasst.
Jetzt, da wir die einfachsten Beispiele solcher Systeme kennen, wird es uns leichter fallen, die allgemeine Definition eines hyperkomplexen Zahlensystems zu verstehen.

Für eine feste natürliche Zahl n betrachten wir Ausdrücke der Form

$$a_0 + a_1i_1 + a_2i_2 + ... + a_ni_n \tag{1}$$

wobei $a_0, a_1, a_2, ..., a_n$ beliebige reelle Zahlen und $i_1, i_2, ..., i_n$ bestimmte Symbole sind (die wir manchmal imaginäre Einheiten nennen werden). Vor allem vereinbaren wir, dass die Gleichheit zweier solcher Ausdrücke

$$a_0 + a_1i_1 + a_2i_2 + ... + a_ni_n = b_0 + b_1i_1 + b_2i_2 + ... + b_ni_n$$

bedeutet, dass

$$a_0 = b_0, a_1 = b_1, ..., a_n = b_n$$

ist. Für eine abgekürzte Schreibweise der Ausdrücke (1) werden wir die halbfetten Buchstaben **a**, **b**, **c**, **u**, **v**, **w**, ... verwenden, wobei wir nur für Ausdrücke der Form

$$a_0 + 0i_1 + 0i_2 + ... + 0i_n$$

eine Ausnahme machen, indem diese manchmal einfach mit a_0 bezeichnet werden.[5]

Wir werden für die Ausdrücke (1) die Grundrechenarten Addition, Subtraktion und Multiplikation erklären. Die Addition und die Subtraktion werden definiert durch die Formeln

$$(a_0 + a_1\mathbf{i}_1 + ... + a_n\mathbf{i}_n) + (b_0 + b_1\mathbf{i}_1 + ... + b_n\mathbf{i}_n) = (a_0 + b_0) + (a_1 + b_1)\mathbf{i}_1 + ... + (a_n + b_n)\mathbf{i}_n)$$

und

$$(a_0 + a_1\mathbf{i}_1 + ... + a_n\mathbf{i}_n) - (b_0 + b_1\mathbf{i}_1 + ... + b_n\mathbf{i}_n) = (a_0 - b_0) + (a_1 - b_1)\mathbf{i}_1 + ... + (a_n - b_n)\mathbf{i}_n)$$

die Multiplikation hingegen wird auf folgende Weise eingeführt.
Es wird eine "Multiplikationstafel" gegeben, d.h., es wird gezeigt, wem alle möglichen Produkte

$$\mathbf{i}_\alpha\mathbf{i}_\beta$$

gleich sind, wobei α und β beliebige Zahlen von 1 bis n sind. Im ganzen gibt es offensichtlich $n \times n = n^2$ solcher Produkte. Jedes Produkt $\mathbf{i}_\alpha\mathbf{i}_\beta$ muss erneut einen Ausdruck der Form (1) darstellen, d.h.

$$\mathbf{i}_\alpha\mathbf{i}_\beta = p_0 + p_1\mathbf{i}_1 + ... + p_n\mathbf{i}_n \tag{2}$$

wobei $p_0, p_1, ..., p_n$ bestimmte reelle Zahlen sind. Jeder Kombination der Indizes α, β entspricht natürlich ein eigener Koeffizientensatz $p_0, p_1, ..., p_n$.
Um die Abhängigkeit dieser Koeffizienten von α, β zu unterstreichen, schreiben wir in (2) $p_{\alpha,\beta i}$ anstelle von p_i; damit wird (2) möglicherweise unübersichtlicher, aber dafür umfasst die Gleichung

$$\mathbf{i}_\alpha\mathbf{i}_\beta = p_{\alpha\beta,0} + p_{\alpha\beta,1}\mathbf{i}_1 + ... + p_{\alpha\beta,n}\mathbf{i}_n \tag{2}$$

gleich alle Fälle. Der Satz Zahlen $p_{\alpha\beta,i}$ ergibt gerade die Multiplikationstafel.
Im ganzen muss es $n^2(n+1)$ dieser Zahlen geben, denn für jede Kombination α, β läuft i von 0 bis n.
Im Falle der komplexen Zahlen zum Beispiel ergibt sich die Multiplikationstafel aus der einzigen Gleichung

$$\mathbf{i} \cdot \mathbf{i} = -1 + 0\mathbf{i}$$

Im Falle der Quaternionen ergibt sich die Tafel aus neun Gleichungen und kann auf folgende Weise geschrieben werden:

	i	**j**	**k**
i	-1	**k**	-**j**
j	-**k**	-1	**i**
k	**j**	-**i**	-1

[5] Durch die von nun an konsequent benutzte Schreibweise ergeben sich gelegentlich verschiedene Schriftbilder für die gleichen Sachverhalte, so wird für die imaginäre Einheit i der komplexen Zahlen zukünftig **i** geschrieben werden u.ä.m. (A.d.R.)

Es ist verständlich, dass jedes Quadrat der Tafel eine der Gleichungen (3) vertritt: zum Beispiel

$$\mathbf{i} \cdot \mathbf{j} = \mathbf{k} = 0 + 0\mathbf{i} + 0\mathbf{j} + 1\mathbf{k}$$

Nachdem die Multiplikationstafel gegeben ist, erklären wir das Produkt

$$(a_0 + a_1\mathbf{i}_1 + ... + a_n\mathbf{i}_n) \cdot -(b_0 + b_1\mathbf{i}_1 + ... + b_n\mathbf{i}_n)$$

durch die übliche Regel der Multiplikation einer Summe mit einer Summe (wir multiplizieren jeden Summanden der ersten Summe mit jedem Summanden der zweiten und addieren die Resultate), wobei wir Produkte der Form $(a_\alpha\mathbf{i}_\alpha)(\beta_\beta\mathbf{i}_\beta)$ in $\alpha_\alpha\beta_\beta(\mathbf{i}_\alpha\mathbf{i}_\beta)$ umformen und $\mathbf{i}_\alpha\mathbf{i}_\beta$ nach Formel (3) ersetzen; danach fassen wir gleichartige Glieder zusammen. Als Ergebnis erhält man erneut einen Ausdruck der Form (1).

Die Menge aller Ausdrücke der Form (1), für die die Operation der Addition und der Multiplikation, wie oben gezeigt, eingeführt wurde, wird hyperkomplexes System der Dimension $n+1$ genannt, die Ausdrücke (1) selbst aber hyperkomplexe Zahlen. Wie aus der oben angeführten Beschreibung folgt, ist ein hyperkomplexes System einer gegebenen Dimension vollständig durch seine Multiplikationstafel definiert.

Wir erwähnen einige Eigenschaften der Multiplikation, die in jedem hyperkomplexen System erfüllt sind.

1) Die Multiplikation einer reellen Zahl a, die als hyperkomplexe Zahl $a + 0\mathbf{i}_1 + ... + 0\mathbf{i}_n$, betrachtet wird; mit der beliebigen Zahl $b_0 + b_1\mathbf{i}_1 + ... + b_n\mathbf{i}_n$ reduziert sich auf die Multiplikation aller Koeffizienten $b_0, b_1, ..., b_n$ mit a:

$$(a + 0\mathbf{i}_1 + ... + 0\mathbf{i}_n)(b_0 + b_1\mathbf{i}_1 + ... + b_n\mathbf{i}_n) = ab_0 + ab_1\mathbf{i}_1 + ... + ab_n\mathbf{i}_n$$

und

$$(b_0 + b_1\mathbf{i}_1 + ... + b_n\mathbf{i}_n)(a + 0\mathbf{i}_1 + ... + 0\mathbf{i}_n) = ab_0 + ab_1\mathbf{i}_1 + ... + ab_n\mathbf{i}_n$$

Insbesondere gelten

$$1 \cdot \mathbf{v} = \mathbf{v} \qquad \text{und} \qquad \mathbf{v} \cdot 1 = \mathbf{v}$$

wobei $\mathbf{v}$ eine beliebige hyperkomplexe Zahl ist.

2) Wenn $\mathbf{u}$ und $\mathbf{v}$ hyperkomplexe Zahlen sind sowie a und b beliebige reelle Zahlen sind, dann ist

$$(a\mathbf{u})(d\mathbf{v}) = (ab)(\mathbf{uv})$$

3) Es gelten beide Varianten (linke und rechte) des Distributivgesetzes:

$$\mathbf{u}(\mathbf{v} + \mathbf{w}) = \mathbf{uv} + \mathbf{uw} \qquad \text{und} \qquad (\mathbf{v} + \mathbf{w})\mathbf{u} = \mathbf{vu} + \mathbf{wu}$$

Die Eigenschaften 1), 2) und 3) folgen offensichtlich aus dem Multiplikationsverfahren. Wir unterstreichen noch einmal, dass sie in jedem hyperkomplexen System gelten.

1.5.2 Kommutative und assoziative Systeme. Systeme mit Division

Im Gegensatz zu den oben gezeigten Eigenschaften werden andere "gute" Eigenschaften der Operation der Multiplikation wie

$$\mathbf{uv} = \mathbf{vu} \qquad \text{(Kommutativgesetz)}$$

und

$$(\mathbf{uv})\mathbf{w} = \mathbf{u}(\mathbf{vw}) \qquad \text{(Assoziativgesetz)}$$

bei weitem nicht in jedem hyperkomplexen System erfüllt. Wenn für je zwei Zahlen **u** und **v**, die einem gegebenen System angehören, die Gleichung

$$\mathbf{uv} = \mathbf{vu}$$

gilt, dann wird ein solches System kommutativ genannt. Die früher von uns betrachteten Systeme der komplexen, binären und dualen Zahlen sind kommutativ; das System der Quaternionen ist demgegenüber nicht kommutativ.

Es ist nicht schwer zu verstehen, was die Bedingung der Kommutativität in den Termen der Multiplikationstafel (3) bedeuten. Da im Falle eines kommutativen Systems

$$\mathbf{i}_\alpha \mathbf{i}_\beta = \mathbf{i}_\beta \mathbf{i}_\alpha$$

(für alle α und β von 1 bis n) sein muss, ist

$$p_{\alpha\beta,0} + p_{\alpha\beta,1}\mathbf{i}_1 + ... + p_{\alpha\beta,n}\mathbf{i}_n = p_{\beta\alpha,0} + p_{\beta\alpha,1}\mathbf{i}_1 + ... + p_{\beta\alpha,n}\mathbf{i}_n$$

und folglich

$$p_{\alpha\beta,0} = p_{\beta\alpha,0}, \quad p_{\alpha\beta,1} = p_{\beta\alpha,1}, \quad ..., \quad p_{\alpha\beta,n} = p_{\beta\alpha,n}$$

(für alle α und β von 1 bis n).
Umgekehrt ist, wenn diese Gleichungen erfüllt sind, ein gegebenes System offensichtlich kommutativ. So ist die Beziehung (4) zwischen den Zahlen $p_{\alpha\beta,i}$ der Multiplikationstafel eine notwendige und hinreichende Bedingung für die Kommutativität.

Wenn für je drei Zahlen **u**, **v** und **w** aus einem gegebenen hyperkomplexen System die Gleichung

$$(\mathbf{uv})\mathbf{w} = \mathbf{u}(\mathbf{vw})$$

erfüllt ist, wird das System assoziativ genannt.[6]

Die Bedingung der Assoziativität ist ebenfalls an bestimmte Beziehungen zwischen den Zahlen $p_{\alpha\beta,i}$ geknüpft, deren Auffindung wir dem Leser überlassen.
Wie wir wissen, sind die Systeme der komplexen, binären und dualen Zahlen sowie auch der Quaternionen assoziativ. Ein einfaches Beispiel eines nichtassoziativen Systems bilden die Zahlen der Form $a + b\mathbf{i} + c\mathbf{j}$ mit der Multiplikationstafel

$$\mathbf{i}^2 = 0, \quad \mathbf{j}^2 = 0, \quad \mathbf{ji} = 0, \quad \mathbf{ij} = \mathbf{i}$$

In diesem Falle ist

$$(\mathbf{ii})\mathbf{j} \neq \mathbf{i}(\mathbf{ij})$$

Für alle hyperkomplexen Zahlen kann man die Grundrechenarten Addition, Subtraktion und Multiplikation erklären. Eine Division ist nur in sehr wenigen hyperkomplexen Systemen möglich.

[6] Wir merken an, dass die von uns gegebene Definition eines hyperkomplexen Systems nicht in der geschichtlichen Tradition steht. Gewöhnlich ist der Begriff der Assoziativität in der Definition eines hyperkomplexen Systems enthalten.

Übrigens müssen wir hier einmal genau sagen, was man unter der Möglichkeit der Division versteht. Man sagt, dass ein gegebenes hyperkomplexes System ein System mit Division ist (oder dass in ihm die Division möglich ist), wenn jede der Gleichungen

$$\mathbf{vx} = \mathbf{u} \qquad \text{und} \qquad \mathbf{xv} = \mathbf{u}$$

eine und nur eine Lösung für jedes **u**, **v** mit $\mathbf{v} \neq 0$ besitzt. Die Lösung der ersten Gleichung wird linker Quotient von **u** durch **v**, die Lösung der zweiten rechter Quotient genannt. Im allgemeinen stimmen der linke und der rechte Quotient nicht überein.

Beispiele von Systemen mit Division sind die komplexen Zahlen und die Quaternionen. Die Dimension des ersten dieser Systeme ist gleich 2, die Dimension des zweiten ist gleich 4.
Eine merkwürdige Tatsache, über die wir später noch sprechen werden, wurde erst unlängst festgestellt: hyperkomplexe Systeme mit Division können nur die Dimension 2, 4 oder 8 besitzen.

Daraus ist ersichtlich, dass man in der großen Zahl hyperkomplexer Systeme solche mit Division nur sehr selten antrifft. Insbesondere ist jedes hyperkomplexe System, das aus Zahlen der Form $a + b\mathbf{i} + c\mathbf{j}$ mit einer beliebigen Multiplikationstafeln besteht, ein System ohne Division (die Dimension eines solchen Systems ist gleich 3).

1.6 Das Verdopplungsverfahren. Oktaven

Wir werden jetzt von noch einem bemerkenswerten System hyperkomplexer Zahlen, die Oktaven genannt werden sprechen. Ebenso wie für die komplexen Zahlen und die Quaternionen sind für die Oktaven nicht nur Addition, Subtraktion und Multiplikation definiert, sondern auch die Division.
Außerdem erlaubt es die Betrachtung der Oktaven bei der Aufgabe über die Summe von Quadraten, die am Ende von § 3 gestellt wurde, einen Schritt weiterzugehen und die Identität (*) für $n = 8$ zu erhalten.

Wie die Bezeichnung Oktaven (achtfache Zahlen) selbst zeigt, sind dies Ausdrücke, die aus acht Gliedern bestehen. Zur Beschreibung solcher Ausdrücke muss man notwendigerweise sieben "imaginäre Einheiten" $\mathbf{i}_1, i_2, ..., \mathbf{i}_7$ haben. Also sind Oktaven Ausdrücke der Form

$$a_0 + a_1\mathbf{i}_1 + a_2\mathbf{i}_2 + a_3\mathbf{i}_3 + a_4\mathbf{i}_4 + a_5\mathbf{i}_5 + a_6\mathbf{i}_6 + a_7\mathbf{i}_7$$

wobei $a_0, a_1, a_2, ..., a_6$ und a_7 beliebige reelle Zahlen sind.

Das Multiplikationsgesetz der Oktaven ist ziemlich kompliziert, deshalb werden wir es nicht gleich definieren. Dafür werden wir ein Verfahren beschreiben, das es erlaubt, auf sehr natürlichem Weg die Oktaven aufzubauen, indem wir von den Quaternionen ausgehen.
Wir werden dieses Verfahren Verdopplung[7] nennen und die Oktaven als "verdoppelte" Quaternionen definieren.

Das Verdopplungsverfahren besitzt übrigens nicht nur eine Beziehung zu den Oktaven: Wir werden sehen, dass man die Quaternionen selbst durch Verdopplung der komplexen Zahlen erhält und die komplexen Zahlen ihrerseits durch Verdopplung der reellen Zahlen.

[7] Oft wird es Cayley-Dickson-Verfahren genannt, nach den Mathematikern A. Cayley, dem Schöpfer des Systems der Oktaven, und L. E. Dickson, der als erster dieses Verfahren betrachtete.

1.6.1 Ein anderer Zugang zur Definition der Quaternionen

Wir werden mit einer bestimmten Analyse des Systems der Quaternionen beginnen. Eine beliebige Quaternion

$$\mathbf{q} = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$$

kann man unter Ausnutzung dessen, dass $\mathbf{ij} = \mathbf{k}$ ist, in der Form

$$\mathbf{q} = (a + b\mathbf{i}) + (c + d\mathbf{i})\mathbf{j} \qquad \text{oder} \qquad \mathbf{q} = \mathbf{z}_1 + \mathbf{z}_2\mathbf{j}$$

darstellen, wobei $\mathbf{z}_1 = a + b\mathbf{i}$ und $\mathbf{z}_2 = c + d\mathbf{i}$ ist. Wir werden sehen, wie sich bei einer solchen Art der Darstellung der Quaternionen ihr Multiplikationsgesetz schreiben lässt.

Es möge zusammen mit $\mathbf{q}$ noch eine Quaternion

$$\mathbf{r} = \mathbf{w}_1 + \mathbf{w}_2\mathbf{j}$$

gegeben sein. Durch Multiplikation von $\mathbf{q}$ mit $\mathbf{r}$ erhalten wir

$$\begin{aligned}\mathbf{qr} &= (\mathbf{z}_1 + \mathbf{z}_2\mathbf{i})(\mathbf{w}_1 + \mathbf{w}_2\mathbf{j}) = \mathbf{z}_1\mathbf{w}_1 + \mathbf{z}_1(\mathbf{w}_2\mathbf{j}) + (\mathbf{z}_2\mathbf{j})\mathbf{w}_1 + (\mathbf{z}_2\mathbf{j})(\mathbf{w}_2\mathbf{j}) \\ &= \mathbf{z}_1\mathbf{w}_1 + \mathbf{z}_1\mathbf{w}_2\mathbf{j} + \mathbf{z}_2\mathbf{j}\mathbf{w}_1 + \mathbf{z}_2\mathbf{j}\mathbf{w}_2\mathbf{j} \end{aligned} \tag{4}$$

(die Klammern in den Produkten haben wir weggelassen, weil die Multiplikation der Quaternionen assoziativ ist). Wir bemerken jetzt, da $\mathbf{ij} = -\mathbf{ji}$ ist, gilt $(a + b\mathbf{i})\mathbf{j} = \mathbf{j}(a - b\mathbf{i})$, d.h.

$$\mathbf{zj} = \mathbf{j}\overline{\mathbf{z}}$$

Außerdem ist es leicht zu überprüfen, dass je zwei Elemente $\mathbf{z}$ und $\mathbf{w}$ der Form $a+b\mathbf{i}$ kommutativ sind:

$$\mathbf{zw} = \mathbf{wz}$$

Damit kann man den zweiten und den dritten Summanden auf der rechten Seite von (1) entsprechend in der Form $\mathbf{w}_2\mathbf{z}_1\mathbf{j}$ und $\mathbf{z}_2\overline{\mathbf{w}}_1\mathbf{j}$ schreiben, anstelle des vierten Summanden aber $\mathbf{z}_2\overline{\mathbf{w}}_2\mathbf{j}^2$ oder $-\overline{\mathbf{w}}_2\mathbf{z}_2$. Folglich ist

$$\mathbf{qr} = (\mathbf{z}_1\mathbf{w}_1 - \overline{\mathbf{w}_2}\mathbf{z}_2) + (\mathbf{w}_2\mathbf{z}_1 + \mathbf{z}_2\overline{\mathbf{w}}_1)\mathbf{j} \tag{2}$$

Wenn wir zur Darstellung einer Quaternion die Form $\mathbf{q} = \mathbf{z}_1 + \mathbf{z}_2\mathbf{j}$ benutzen, werden wir ein wichtiges Moment bemerken. Da $\mathbf{i}^2 = -1$ ist, kann man alle Quaternionen $a + b\mathbf{i}$, insbesondere $\mathbf{z}_1$ und $\mathbf{z}_2$ als komplexe Zahlen deuten. Zusammen mit Formel (2) führt uns dies zu einer solchen Schlussfolgerung.

Man kann die Quaternionen als Ausdrücke der Form $\mathbf{z}_1 + \mathbf{z}_2\mathbf{j}$ definieren, wobei $\mathbf{z}_1$ und $\mathbf{z}_2$ beliebige komplexe Zahlen sind und $\mathbf{j}$ ein bestimmtes Symbol. Dabei ist das Multiplikationsgesetz solcher Ausdrücke durch die Formel (2) gegeben.
Das ist eine wesentliche Feststellung. Sie hilft uns, das Verdopplungsverfahren der hyperkomplexen Zahlen zu verstehen.

1.6.2 Verdopplung eines hyperkomplexen Systems. Definition der Oktaven

Wir führen eine Reihe von Definitionen ein. Es möge ein hyperkomplexes System $\mathscr{U}$ gegeben sein, das aus Zahlen der Form

$$\mathbf{u} = a_0 + a_1\mathbf{i}_1 + a_2\mathbf{i}_2 + ... + a_n\mathbf{i}_n$$

mit einem bestimmten Multiplikationsgesetz besteht. Wir vereinbaren, das Element

$$\overline{\mathbf{u}} = a_0 - a_1\mathbf{i}_1 - a_2\mathbf{i}_2 - ... - a_n\mathbf{i}_n$$

konjugiert zu **u** zu nennen. Verdopplung des Systems $\mathscr{U}$ wird ein neues hyperkomplexes System $\mathscr{U}^2$ mit doppelt so großer Dimension (wie $\mathscr{U}$) genannt, das auf folgende Weise aufgebaut wird.

Seine Elemente stellen Ausdrücke der Form

$$\mathbf{u}_1 + \mathbf{u}_2\mathbf{e} \tag{3}$$

dar, wobei u_1 und u_2 beliebige Elemente aus $\mathscr{U}$ sind und **e** ein bestimmtes Symbol ist. Die Addition der Elemente aus $\mathscr{U}$ erfolgt auf natürliche Weise

$$(\mathbf{u}_1 + \mathbf{u}_2\mathbf{e}) + (\mathbf{v}_1 + \mathbf{v}_2\mathbf{e}) = (\mathbf{u}_1 + \mathbf{v}_1) + (\mathbf{u}_2 + \mathbf{v}_2)\mathbf{e} \tag{4}$$

die Multiplikation hingegen wird durch die Formel

$$(\mathbf{u}_1 + \mathbf{u}_2\mathbf{e})(\mathbf{v}_1 + \mathbf{v}_2\mathbf{e}) = (\mathbf{u}_1\mathbf{v}_1 - \overline{\mathbf{v}}_2\mathbf{u}_2) + (\mathbf{v}_2\mathbf{u}_1 + \mathbf{u}_2\overline{\mathbf{v}}_1) \tag{5}$$

definiert (der Strich bedeutet die Konjugation in $\mathscr{U}$).

Den Leser mag es befremden, dass wir beim Definieren des Systems $\mathscr{U}^{(2)}$ erstens auf die gewohnte Schreibweise der hyperkomplexen Zahlen und zweitens auf die Angabe der Multiplikation mit Hilfe einer Tafel verzichteten. Die Zahlen aus $\mathscr{U}$ müssten in der Form

$$a_0 + a_1\mathbf{i}_1 + a_2\mathbf{i}_2 + ... + a_n\mathbf{i}_n + a_{n+1}\mathbf{i}_{n+1} + ... + a_{2n+1}\mathbf{i}_{2n+1} \tag{6}$$

geschrieben werden, jedoch bevorzugen wir die kürzere Schreibweise (3), da man jedem Ausdruck (6) zwei Elemente des hyperkomplexen Ausgangssystems zuordnen kann:

$$\mathbf{u}_1 = a_0 + a_1\mathbf{i}_1 + ... + a_n\mathbf{i}_n \qquad , \qquad \mathbf{u}_2 = a_{n+1} + a_{n+2}\mathbf{i}_1 + ... + a_{2n+1}\mathbf{i}_n$$

und folglich auch den Ausdruck (3) (er könnte als "Code" für die hyperkomplexen Zahlen (6) gelten). Umgekehrt, wenn ein Ausdruck der Form (3) gegeben ist, so kann man durch ihn (6) bilden.

Die kurze Schreibweise (3) besitzt im Vergleich mit (6) einen wesentlichen Vorteil. Statt die Multiplikation in $\mathscr{U}^{(2)}$ mit Hilfe einer Tafel anzugeben, können wir sie in der überschaubaren Form (5) schreiben. Natürlich kann man der Formel (5) die Multiplikationstafel für die "imaginären Einheiten" $\mathbf{i}_1, \mathbf{i}_2, ..., \mathbf{i}_{2n+1}$ entnehmen.

Wir werden uns in allgemeiner Form nicht mit dieser Tafel beschäftigen, für den uns am meisten interessierenden Fall der Oktaven werden wir sie weiter unten vollständig angeben.

Wir haben damit das Verdopplungsverfahren definiert. Als Beispiel mag der Übergang von den komplexen Zahlen zu den Quaternionen dienen. Das, was am Anfang dieses Paragraphen getan wurde, bedeutet faktisch, dass das System der Quaternionen die Verdopplung des Systems der komplexen Zahlen ist. Man kann auch leicht überprüfen (dem Leser wird empfohlen, dies selbständig zu tun), dass man die komplexen Zahlen durch Verdopplung der reellen erhält.

Das Hauptziel dieses Paragraphen ist, wie wir bereits sagten, der Aufbau des Systems der Oktaven. Die Definition der Oktaven kann jetzt in einigen Worten formuliert werden: das System der Oktaven ist die Verdopplung des Systems der Quaternionen.
Alle Eigenschaften des Systems der Oktaven erhält man auf natürliche Weise aus der gegebenen Definition. Im nächsten Punkt beginnen wir mit der ausführlichen Untersuchung dieser Eigenschaften.

1.6.3 Die Multiplikationstafel im System der Oktaven

Oktaven sind also gemäß Definition Ausdrücke der Form

$$\mathbf{q}_1 + \mathbf{q}_2\mathbf{e}$$

wobei $\mathbf{q}_1$ und $\mathbf{q}_2$ beliebige Quaternionen sind. Das Multiplikationsgesetz besitzt folgende Form

$$(\mathbf{q}_1 + \mathbf{q}_2 e)(\mathbf{r}_1 + \mathbf{r}_2 e) = (\mathbf{q}_1\mathbf{r}_1 - \bar{\mathbf{r}}_2\mathbf{q}_2) + (\mathbf{r}_2\mathbf{q}_1 + \mathbf{q}_2\bar{\mathbf{r}}_1)e \tag{7}$$

Wir werden vor allem sehen, wie eine solche Definition der Oktaven mit der Darstellung in der Form

$$a_0 + a_1\mathbf{i}_1 + a_2\mathbf{i}_2 + a_3\mathbf{i}_3 + a_4\mathbf{i}_4 + a_5\mathbf{i}_5 + a_6\mathbf{i}_6 + a_7\mathbf{i}_7 \tag{8}$$

verknüpft ist, genauer gesagt, wir werden die Multiplikationstafel für die imaginären Einheiten $\mathbf{i}_1, ..., \mathbf{i}_7$ bilden. Die Quaternionen $\mathbf{q}_1$ und $\mathbf{q}_2$ die der Schreibweise (8) entsprechen, sind

$$\mathbf{q}_1 = a_0 + a_1\mathbf{i} + a_2\mathbf{j} + a_3\mathbf{k} \qquad \text{und} \qquad \mathbf{q}_2 = a_4 + a_5\mathbf{i} + a_6\mathbf{j} + a_7\mathbf{k}$$

Wir vereinbaren, der größeren Einheitlichkeit halber anstelle von (8) zu schreiben

$$a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} + A\mathbf{E} + B\mathbf{I} + C\mathbf{J} + D\mathbf{K}$$

wobei a, b, c, d, A, B, C, D die früheren $a_0, a_1, ..., a_7$ sind und $\mathbf{i}, \mathbf{j}, \mathbf{k}, \mathbf{E}, \mathbf{I}, \mathbf{J}, \mathbf{K}$ die neuen Bezeichnungen für die "imaginären Einheiten" $\mathbf{i}_1, ..., \mathbf{i}_7$. In diesen Bezeichnungen werden die Quaternionen q_1 und q_2 zu

$$\mathbf{q}_1 = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \qquad \text{und} \qquad \mathbf{q}_2 = A + B\mathbf{i} + C\mathbf{j} + D\mathbf{k}$$

Aus (7) ergibt sich, wie wir bereits bemerkten, die Multiplikationstafel für die Einheiten $\mathbf{i}, \mathbf{j}, \mathbf{k}, \mathbf{E}, \mathbf{I}, \mathbf{J}, \mathbf{K}$.
Wenn wir zum Beispiel in der Formel (7) $\mathbf{q}_2 = \mathbf{r}_2 = 0$ setzen, erhalten wir

$$(\mathbf{q}_1 + 0\mathbf{e})(\mathbf{r}_1 + 0\mathbf{e}) = \mathbf{q}_1\mathbf{r}_1 + 0\mathbf{e}$$

auf diese Weise werden die Oktaven q_1 und r_1 wie Quaternionen multipliziert. Daraus folgt, dass die Multiplikationstafel für die Einheiten **i**, **j** und **k** genau dieselbe ist wie im Falle der Quaternionen:

$$\mathbf{i}^2 = -1, \quad \mathbf{j}^2 = -1, \quad \mathbf{k}^2 = -1$$
$$\mathbf{ij} = \mathbf{k}, \quad \mathbf{ji} = -\mathbf{k}, \quad \mathbf{jk} = \mathbf{i}, \quad \mathbf{kj} = -\mathbf{i}, \quad \mathbf{ki} = \mathbf{j}, \quad \mathbf{ik} = -\mathbf{j}$$

Die niedergeschriebenen Gleichungen geben die Ausdrücke für nur 9 Produkte von insgesamt 49 wieder (in unserem Falle haben wir 7 Einheiten und folglich $7 \times 7 = 49$ paarweise Produkte). Es besteht keine Notwendigkeit, die übrigen 40 Produkte niederzuschreiben, da es eine ziemlich einfache Methode gibt, sich die ganze Tafel zu merken. Sie besteht in der Angabe der folgenden sieben Triaden:

$$\mathbf{i} \;\; \mathbf{j} \;\; \mathbf{k} \qquad \boxed{\begin{array}{ccc} \mathbf{I} & \mathbf{J} & \mathbf{-k} \\ \mathbf{I} & \mathbf{-j} & \mathbf{K} \\ \mathbf{-i} & \mathbf{J} & \mathbf{K} \end{array}} \qquad \boxed{\begin{array}{ccc} \mathbf{i} & \mathbf{E} & \mathbf{I} \\ \mathbf{j} & \mathbf{E} & \mathbf{J} \\ \mathbf{k} & \mathbf{E} & \mathbf{K} \end{array}}$$

Es ist nicht schwer, sich diese Triaden zu merken: Jede Triade im ersten Rahmen erhält man aus der Triade der Symbole **i**, **j**, **k**, wenn man vor eins das Minuszeichen setzt und die zwei anderen durch die entsprechenden großgeschriebenen Symbole - ersetzt; jede der Triaden im zweiten Rahmen enthält E und zwei gleichartige Symbole.

Um die Multiplikationstafel zu erläutern, bezeichnen wir mit α, β, γ eine beliebige der angegebenen sieben Triaden (die Reihenfolge der Symbole in der Triade ist wesentlich). Dann ist

$$\alpha^2 = -1, \quad \beta^2 = -1, \quad \gamma^2 = -1$$
$$\alpha\beta = \gamma, \quad \beta\alpha = -\gamma, \quad \beta\gamma = \alpha, \quad \gamma\beta = -\alpha, \quad \gamma\alpha = \beta, \quad \alpha\gamma = -\beta$$

d.h., α, β und γ werden genauso multipliziert wie die Quaternionen **i**, **j** und **k**.

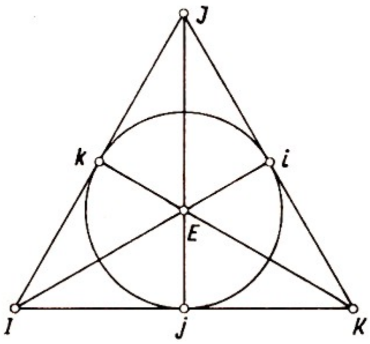


Abb.8

Als gute Illustration dieser Regel dient Abb. 8. Auf ihr ist ein Dreieck mit den Ecken **I**, **J** und **K** und den Seitenmittelpunkten **i**, **j** und k abgebildet; im Schnittpunkt der Seitenhalbierenden liegt der Buchstabe E.
Auf jeder Geraden befinden sich drei "imaginäre Einheiten". Außerdem betrachtet man die drei Einheiten **i**, **j**, **k** als einer "Geraden" zugehörig (die auf der Abbildung symbolisch durch einen Kreis dargestellt ist).

Auf der Abbildung sind also 7 "Geraden" und auf jeder von ihr liegen drei Einheiten. Um das Produkt von zwei beliebigen Einheiten zu finden, muss man die "Gerade" betrachten, die durch diese Einheiten bestimmt wird, und die dritte Einheit dieser "Geraden" mit dem Zeichen $+$ oder $-$ nehmen.

Es ist interessant, dass man die Einheiten $\mathbf{i}, \mathbf{j}, \mathbf{k}, \mathbf{E}, \mathbf{I}, \mathbf{J}, \mathbf{K}$ in dieser Zeichnung auf mehrere Arten darstellen kann. Es genügt, $\mathbf{i}, \mathbf{j}, \mathbf{k}$ als auf einer "Geraden" (einer beliebigen von den sieben) liegend zu nehmen, irgendeinen der übrigen Punkte mit **E** zu bezeichnen und dann **I**, **J**, **K** auf den Geraden **iE**, **jE**, **kE** anzuordnen; das Resultat führt uns erneut zu einem richtigen Bild.

1.6.4 Die Konjugation im System der Oktaven. Der absolute Betrag einer Oktave

Es möge

$$\mathbf{u} = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} + A\mathbf{E} + B\mathbf{I} + C\mathbf{J} + D\mathbf{K} \tag{9}$$

eine beliebige Oktave sein. Die Oktave

$$\overline{\mathbf{u}} = a - b\mathbf{i} - c\mathbf{j} - d\mathbf{k} - A\mathbf{E} - B\mathbf{I} - C\mathbf{J} - D\mathbf{K}$$

werden wir konjugiert zu **u** nennen. Wenn man anstelle von (9) die kürzere Schreibweise

$$\mathbf{u} = \mathbf{q}_1 + \mathbf{q}_2\mathbf{e}$$

verwendet, wobei

$$\mathbf{q}_1 = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \qquad \text{und} \qquad \mathbf{q}_2 = A + B\mathbf{i} + C\mathbf{j} + D\mathbf{k}$$

ist, dann erhält man für die konjugierte Oktave den Ausdruck

$$\overline{\mathbf{u}} = \overline{\mathbf{q}_1} - \mathbf{q}_2\mathbf{e}$$

Wir berechnen jetzt das Produkt einer beliebigen Oktave $\mathbf{u}$ mit ihrer konjugierten Oktave $\overline{\mathbf{u}}$. Wir werden sehen, dass dieses Produkt, wie auch im Falle der komplexen Zahlen oder der Quaternionen, gleich einer reellen Zahl ist (d.h. einer Oktave der Form $a + 0\mathbf{i} + 0\mathbf{j} + ... + 0\mathbf{K}$). Es ergibt sich

$$\mathbf{u}\overline{\mathbf{u}} = (\mathbf{q}_1 + \mathbf{q}_2 e)(\overline{\mathbf{q}_1} - \mathbf{q}_2 e) = (\mathbf{q}_1\overline{\mathbf{q}_1} + \overline{\mathbf{q}_2}\mathbf{q}_2) + (-\mathbf{q}_2\mathbf{q}_1 + \mathbf{q}_2\mathbf{q}_1)\mathbf{e}$$

Unter Berücksichtigung, dass für Quaternionen $\mathbf{q}\overline{\mathbf{q}} = \overline{\mathbf{q}}\mathbf{q} = |\mathbf{q}|^2$ gilt, finden wir damit

$$\mathbf{u}\overline{\mathbf{u}} = \mathbf{q}_1\overline{\mathbf{q}_1} + \mathbf{q}_2\overline{\mathbf{q}_2} = |\mathbf{q}_1|^2 + |\mathbf{q}^2|^2 \tag{10}$$

Die Quadratwurzel aus dem Ausdruck

$$|\mathbf{q}_1|^2 + |\mathbf{q}^2|^2$$

wird absoluter Betrag oder Norm der Oktave $\mathbf{u}$ genannt und mit $|\mathbf{u}|$ bezeichnet. Wir bemerken, dass für eine Oktave $\mathbf{u}$, die in der Form (9) gegeben ist, das Quadrat ihres absoluten Betrages gleich

$$a^2 + b^2 + c^2 + d^2 + A^2 + B^2 + C^2 + D^2 \tag{11}$$

ist. Auf diese Weise haben wir nach Definition des absoluten Betrags

$$\mathbf{u}\overline{\mathbf{u}} = |\mathbf{u}|^2 \tag{12}$$

Zu dieser Gleichung kann man eine andere hinzufügen

$$\overline{\mathbf{u}}\mathbf{u} = |\mathbf{u}|^2$$

die aus der Tatsache hervorgeht, dass das Quadrat des absoluten Betrages der Oktave $\mathbf{u}$ mit dem Quadrat des absoluten Betrages der konjugierten Oktave $\overline{\mathbf{u}}$ übereinstimmt (das auch gleich (11) ist).

1.6.5 Der absolute Betrag eines Produkts von Oktaven

Das System der Oktaven besitzt viele Gemeinsamkeiten mit den Systemen der komplexen Zahlen und der Quaternionen. Eine der Gemeinsamkeiten besteht in der wichtigen Eigenschaft, dass der absolute Betrag des Produkts von je zwei Oktaven gleich dem Produkt der absoluten Beträge dieser Oktaven ist

$$|\mathbf{u}\mathbf{v}| = |\mathbf{u}||\mathbf{v}| \tag{13}$$

oder, was äquivalent ist,

$$|\mathbf{u}\mathbf{v}|^2 = |\mathbf{u}|^2|\mathbf{v}|^2 \tag{14}$$

Den Beweis der Gleichung (14) kann man durch direkte Berechnung führen. Wir berechnen $|\mathbf{u}\mathbf{v}|^2$ und $|\mathbf{u}|^2|\mathbf{v}|^2$ einzeln. Da

$$\mathbf{u}\mathbf{v} = (\mathbf{q}_1 + \mathbf{q}_2\mathbf{e})(\mathbf{r}_1 + \mathbf{r}_2\mathbf{e}) = (\mathbf{q}_1\mathbf{r}_2 - \overline{\mathbf{r}_2}\mathbf{q}_2) + (\mathbf{r}_2\mathbf{q}_1 + \mathbf{q}_2\overline{\mathbf{r}_1})\mathbf{e}$$

ist, erhalten wir durch Anwenden von Formel (10)

$$|\mathbf{uv}|^2 = (\mathbf{q}_1\mathbf{r}_1 - \overline{\mathbf{r}_2}\mathbf{q}_2)\overline{(\mathbf{q}_1\mathbf{r}_1 - \overline{\mathbf{r}_2}\mathbf{q}_2)} + (\mathbf{r}_2\mathbf{q}_1 + \mathbf{q}_2\overline{\mathbf{r}_1})\overline{(\mathbf{r}_2\mathbf{q}_1 + \mathbf{q}_2\overline{\mathbf{r}_1})}$$

oder unter Berücksichtigung der Eigenschaft der Konjugation für Quaternionen

$$|\mathbf{uv}|^2 = (\mathbf{q}_1\mathbf{r}_1 - \overline{\mathbf{r}_2}\mathbf{q}_2)(\overline{\mathbf{r}_1}\overline{\mathbf{q}_1} - \overline{\mathbf{q}_2}\mathbf{r}_2) + (\mathbf{r}_2\mathbf{q}_1 + \mathbf{q}_2\overline{\mathbf{r}_1})(\overline{\mathbf{q}_1}\overline{\mathbf{r}_2} + \mathbf{r}_1\overline{\mathbf{q}_2})$$

Andererseits gilt

$$|\mathbf{u}|^2|\mathbf{v}|^2 = (\mathbf{q}_1\overline{\mathbf{q}_1} + \mathbf{q}_2\overline{\mathbf{q}_2})(\mathbf{r}_1\overline{\mathbf{r}_1} + \mathbf{r}_2\overline{\mathbf{r}_2})$$

Durch Vergleichen beider Ausdrücke finden wir, dass sie sich durch die Summe der vier Summanden

$$S = \mathbf{r}_2\mathbf{q}_1\mathbf{r}_1\overline{\mathbf{q}_2} + \mathbf{q}_2\overline{\mathbf{r}_1}\overline{\mathbf{q}_1}\overline{\mathbf{r}_2} - \mathbf{q}_1\mathbf{r}_1\overline{\mathbf{q}_2}\mathbf{r}_2 - \overline{\mathbf{r}_2}\mathbf{q}_2\overline{\mathbf{r}_1}\overline{\mathbf{q}_1}$$

unterscheiden. Deshalb bleibt noch zu beweisen, dass für je vier Quaternionen $\mathbf{p}_1, \mathbf{q}_2, \mathbf{r}_1, \mathbf{r}_2$ stets $S = 0$ ist.
Wir beginnen mit der offensichtlichen Bemerkung, dass $S = 0$ ist, wenn $\mathbf{r}_2$ eine reelle Zahl ist. Andererseits ist, wenn r_2 eine rein imaginäre Quaternion ist (und folglich $\overline{\mathbf{r}_2} = -\mathbf{r}_2$),

$$S = \mathbf{r}_2(\mathbf{q}_1\mathbf{r}_1\overline{\mathbf{q}_2} + \mathbf{q}_2\overline{\mathbf{r}_1}\overline{\mathbf{q}_1}) - (\mathbf{q}_1\mathbf{r}_1\overline{\mathbf{q}_2} + \mathbf{q}_2\overline{\mathbf{r}_1}\overline{\mathbf{q}_1})r_2$$

Der Ausdruck in Klammern ist selbst die Summe zweier konjugierter Quaternionen und deshalb gleich einer reellen Zahl; wir bezeichnen sie mit c. Dann ist

$$S = \mathbf{r}_2 c - c\mathbf{r}_2 = 0$$

Man muss jetzt eine offensichtliche Eigenschaft des Ausdrucks S berücksichtigen. Wenn er für $\mathbf{r}_2 = a$ und $\mathbf{r}_2 = b$ gleich 0 ist, so verschwindet er auch bei $\mathbf{r}_2 = a + b$. Weil sich jede Quaternion $\mathbf{r}_2$ als Summe einer reellen Zahl und einer rein imaginären Quaternion darstellen lässt, wobei für beide Summanden $S = 0$ ist, ist damit S identisch Null.

1.6.6 Eine Identität für acht Quadrate

Die im vorhergehenden Punkt aufgestellte Gleichung

$$|\mathbf{uv}|^2 = |\mathbf{u}|^2|\mathbf{v}|^2 \tag{15}$$

stellt einen neuen Beitrag zur Lösung der Aufgabe über die Summe von Quadraten, die am Ende von § 3 gestellt wurde, dar, weil sie in der ausführlichen Schreibweise (wenn man sie von rechts nach links liest) selbst eine Identität darstellt: das Produkt einer Summe von acht Quadraten mit einer Summe von acht Quadraten ist wiederum eine Summe von acht Quadraten.
In der Tat, es möge

$$\begin{aligned}
\mathbf{u} &= a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} + A\mathbf{E} + B\mathbf{I} + C\mathbf{J} + D\mathbf{K} \\
\mathbf{v} &= a' + b'\mathbf{i} + c'\mathbf{j} + d'\mathbf{k} + A'\mathbf{E} + B'\mathbf{I} + C'\mathbf{J} + D'\mathbf{K} \quad \text{und} \\
\mathbf{uv} &= \Phi_0 + \Phi_1\mathbf{i} + \Phi_2\mathbf{j} + \Phi_3\mathbf{k} + \Phi_4\mathbf{E} + \Phi_5\mathbf{I} + \Phi_6\mathbf{J} + \Phi_7\mathbf{K}
\end{aligned}$$

sein. Dann nimmt Gleichung (15) die Form

$$(a^2 + ... + D^2)(a'^2 + ... + D'^2) = \Phi_0^2 + \Phi_1^2 + ... + \Phi_7^2$$

an. Es versteht sich, dass man hier $\Phi_0, \Phi_1, ..., \Phi_7$ unter Benutzung des Multiplikationsgesetzes der Oktaven durch Ausdrücke in a,...,D, a', ...,D' ersetzt. Nachdem diese umfangreiche Arbeit getan ist, gelangen wir zur folgenden Identität:

$$\begin{aligned}(a^2+b^2{+}c^2+d^2+A^2+B^2+C^2+D^2)\cdot(a'^2+b'^2+c'^2+d'^2+A'^2+B'^2+C'^2+D'^2) =\\ &= (aa'-bb'-cc'-dd'-AA'-BB'-CC'-DD')^2\\ &+ (ab'+ba'+cd'+dc'-A'B+B'A+C'D-D'C)^2\\ &+ (ac'+ca'-bd'+db'-A'C+C'A-B'D+D'B)^2\\ &+ (ad'+da'+bc'+cb'-A'D+D'A+B'C-C'B)^2\\ &+ (A'a-B'b-C'c-D'd+Aa'+Bb'+Cc'+Dd')^2\\ &+ (A'b+B'a+C'd-D'c-Ab'+Ba'-Cd'+Dc')^2\\ &+ (A'c+C'a-B'd+D'b-Ac'+Ca'+Bd'-Db')^2\\ &+ (A'd+D'a+B'c-C'b-Ad'+Da'-Bc'+Cb')^2\end{aligned}$$

Es ist interessant zu bemerken, dass gerade die Suche nach der Identität für 8 Quadrate den Schöpfer des Systems der Oktaven, den englischen Mathematiker A. Cayley, zu deren Entdeckung führte.

1.6.7 Nichtassoziativität der Multiplikation von Oktaven. Die Eigenschaft der Alternativität

Wir sagten oben, dass viele Eigenschaften der Oktaven mit den Eigenschaften der Quaternionen und der komplexen Zahlen übereinstimmen.
Wir wenden nun die Aufmerksamkeit einem wesentlichen Unterschied zwischen diesen Systemen zu. Während die Multiplikation der komplexen Zahlen und der Quaternionen assoziativ ist, wird das Assoziativgesetz bei der Multiplikation der Oktaven nicht erfüllt. Zum Beispiel gilt

$$(\mathbf{ij})\mathbf{E} \neq \mathbf{i}(\mathbf{jE})$$

weil

$$(\mathbf{ij})E = \mathbf{kE} = \mathbf{k} \qquad \text{und} \qquad \mathbf{i}(\mathbf{jE}) = \mathbf{iJ} = -\mathbf{K}$$

ist. Die Ungültigkeit des Assoziativgesetzes für die Oktaven bedeutet durchaus nicht, dass für je drei Oktaven u, v, w gilt

$$(\mathbf{uv})\mathbf{w} \neq \mathbf{u}(\mathbf{vw})$$

Man kann beweisen, dass die folgenden zwei Formeln gelten

$$(\mathbf{uv})\mathbf{v} = \mathbf{u}(\mathbf{vv}) \qquad , \qquad \mathbf{v}(\mathbf{vu}) = (\mathbf{vv})\mathbf{u} \tag{16,17}$$

wobei **u** und **v** zwei beliebige Oktaven sind. Man kann die Formeln (16) und (17) als eine gewisse abgeschwächte Variante der Assoziativität betrachten. Für Systeme, in denen diese Formeln gelten, existiert eine spezielle Bezeichnung; man nennt solche Systeme alternativ.

Indem wir uns dem Beweis der Formeln (16) und (17) zuwenden, bemerken wir, dass man an ihrer Stelle

$$(\mathbf{uv})\bar{\mathbf{v}} = \mathbf{u}(\mathbf{v}\bar{\mathbf{v}}) \qquad \text{und} \qquad \bar{\mathbf{v}}(\mathbf{vu}) = (\bar{\mathbf{v}}\mathbf{v})\mathbf{u} \tag{16',17'}$$

beweisen kann, da man, indem man in diesen Gleichungen **v** durch $-\mathbf{v}+2a$ (wobei a der Realteil der Oktave **v** ist) ersetzt, leicht (16) und (17) erhält. Wir werden die Formel (16') beweisen; die Formel (17') erhält man analog. Es möge

$$\mathbf{u} = \mathbf{q}_1 + \mathbf{q}_2\mathbf{e} \qquad \text{und} \qquad \mathbf{v} = \mathbf{r}_1 + \mathbf{r}_2\mathbf{e}$$

sein. Wir haben dann

$$
\begin{aligned}
(\mathbf{uv})\bar{\mathbf{v}} &= ((\mathbf{q}_1 + \mathbf{q}_2\mathbf{e})(\mathbf{r}_1 + \mathbf{r}_2\mathbf{e}))(\bar{\mathbf{r}}_1 - \mathbf{r}_2\mathbf{e}) \\
&= (\mathbf{q}_1\mathbf{r}_1 - \bar{\mathbf{r}}_2\mathbf{q}_2)\bar{\mathbf{r}}_1 + \bar{\mathbf{r}}_2(\mathbf{r}_2\mathbf{q}_1 + \mathbf{q}_2\bar{\mathbf{r}}_1)) + ((-\mathbf{r}_2)(\mathbf{q}_1\mathbf{r}_1 - \bar{\mathbf{r}}_2\mathbf{q}_2) + (\mathbf{r}_2\mathbf{q}_1 + \mathbf{q}_2\bar{\mathbf{r}}_1)\mathbf{r}_1)\mathbf{e} \\
&= (|\mathbf{r}_1|^2 + |\mathbf{r}_2|^2)\mathbf{q}_1 + (|\mathbf{r}_1|^2 + |\mathbf{r}_2|^2)\mathbf{q}_2\mathbf{e} = (|\mathbf{r}_1|^2 + |\mathbf{r}_2|^2)(\mathbf{q}_1 + \mathbf{q}_2\mathbf{e}) = |\mathbf{v}|^2\mathbf{u}
\end{aligned}
$$

Andererseits ist

$$|\mathbf{v}\bar{\mathbf{v}}| = |\mathbf{v}|^2$$

deshalb gilt $\mathbf{u}(\mathbf{v}\bar{\mathbf{v}}) = |\mathbf{v}|^2\mathbf{u}$. Daraus folgt (16').

1.6.8 Die Oktaven sind ein System mit Division

Eine weitere wichtige Eigenschaft des Systems der Oktaven, die diese den komplexen Zahlen und den Quaternionen näherbringt, ist die Möglichkeit der Division. Es mögen $\mathbf{u}$ und $\mathbf{v}$ beliebige Oktaven sein, wobei $\mathbf{v} \neq 0$ ist.
Wir erinnern uns daran, dass der linke Quotient $\mathbf{u}$ durch $\mathbf{v}$ die Lösung der Gleichung

$$\mathbf{vx} = \mathbf{u} \tag{18}$$

ist, der rechte Quotient hingegen die Lösung der Gleichung

$$\mathbf{xv} = \mathbf{u} \tag{19}$$

Wir werden zunächst die Gleichung (18) lösen. Indem wir genauso verfahren wie im Falle der Quaternionen, multiplizieren wir beide Seiten von (18) von links mit $\bar{\mathbf{v}}$. Wir erhalten

$$\bar{\mathbf{v}}(\mathbf{vx}) = \bar{\mathbf{v}}\mathbf{u}$$

oder unter Berücksichtigung von (17')

$$|\mathbf{v}|^2 x = \bar{\mathbf{v}}\mathbf{u}$$

Daraus folgt

$$\mathbf{x} = \frac{1}{|\mathbf{v}|^2}\bar{\mathbf{v}}\mathbf{u}$$

Die direkte Überprüfung (wiederum unter Verwendung von Formel (17')) zeigt, dass der gefundene Wert $\mathbf{x}$ der Gleichung (18) genügt. Also ist der linke Quotient $\mathbf{u}$ durch $\mathbf{v}$ gleich

$$\mathbf{x}_l = \frac{1}{|\mathbf{v}|^2}\bar{\mathbf{v}}\mathbf{u}$$

Analog wird bewiesen, dass der rechte Quotient gleich

$$\mathbf{x}_r = \frac{1}{|\mathbf{v}|^2}\mathbf{u}\bar{\mathbf{v}}$$

ist; dabei muss man Formel (16) verwenden. Auf diese Weise sehen wir, dass die Oktaven ein System mit Division darstellen.

1.7 Algebren

1.7.1 Einführende Überlegungen

Wir kommen noch einmal auf den allgemeinen Begriff eines hyperkomplexen Systems zurück. Gemäß der in § 5 gegebenen Definition ist ein hyperkomplexes System der Dimension $n+1$ die Menge der Ausdrücke der Form

$$a_0 + a_1\mathbf{i}_1 + a_2\mathbf{i}_2 + ... + a_n\mathbf{i}_n$$

(der hyperkomplexen Zahlen) mit der natürlichen Additionsregel und einer bestimmten Multiplikationsregel. Die letztere besteht darin, dass eine Tafel der Form

$$\mathbf{i}_\alpha\mathbf{i}_\beta = p_{\alpha\beta,0} + p_{\alpha\beta,1}\mathbf{i}_1 + ... + p_{\alpha\beta,n}\mathbf{i}_n \tag{1}$$

(Multiplikationstafel der "imaginären Einheiten" $\mathbf{i}_1, \mathbf{i}_2, ..., \mathbf{i}_n$) angegeben wird, aus der das Produkt zweier hyperkomplexer Zahlen nach der Regel der Multiplikation einer Summe mit einer Summe bestimmt wird, wobei nachfolgend die Summanden $(a_\alpha\mathbf{i}_\alpha)(b_\beta\mathbf{i}_\beta)$ in der Form $a_\alpha b_\beta(\mathbf{i}_\alpha\mathbf{i}_\beta)$ geschrieben werden und die Produkte $\mathbf{i}_\alpha\mathbf{i}_\beta$ gemäß Formel (1) ersetzt werden.

Wir betrachten den Fall, dass alle Zahlen $p_{\alpha\beta,0}$ (die "freien Glieder" in den Gleichungen (1)) gleich Null sind. Dann ist das Produkt von je zwei imaginären Einheiten $\mathbf{i}_\alpha$, $\mathbf{i}_\beta$ erneut eine Kombination imaginärer Einheiten.

Wir bezeichnen mit (A) die Menge aller hyperkomplexer Zahlen der Form

$$\mathbf{a} = a_1\mathbf{i}_1 + a_2\mathbf{i}_2 + ... + a_n\mathbf{i}_n \tag{2}$$

(ohne die freien Glieder). Es ist völlig klar, dass die Summe von zwei derartigen Zahlen wiederum eine Zahl der Form (2) ist.

Aus dem oben bezüglich der Produkte $\mathbf{i}_\alpha\mathbf{i}_\beta$ Gesagten folgt, dass auch die Multiplikation zweier Zahlen der Form (2) erneut eine Zahl der Form (2) ergibt. Die Menge (A) besitzt also die Eigenschaft, dass beide Operationen - die Addition und die Multiplikation - nicht aus dieser Menge herausführen.
Diese Eigenschaft erlaubt es, (A) auch als selbständiges System mit zwei Operationen, der Addition und der Multiplikation, zu betrachten. Es ist jedoch im allgemeinen kein hyperkomplexes System in der Bedeutung, die wir diesem Wort zuschrieben (von den Fällen, in denen man das System (A) trotzdem als hyperkomplexes betrachten kann, werden wir etwas später sprechen).

Der Hauptunterschied des Systems (A) zu einem hyperkomplexen reduziert sich auf folgendes. Jedes hyperkomplexe System muss ein bestimmtes besonderes Element $\mathbf{e}$ der Art enthalten, dass

$$\mathbf{e}\cdot\mathbf{a} = \mathbf{a}\cdot\mathbf{e} = \mathbf{a}$$

für ein beliebiges Element $\mathbf{a}$ aus dem gegebenen System gilt (dieses Element $\mathbf{e}$ ist $1 + 0\mathbf{i}_1 + ... + 0\mathbf{i}_n$). Im allgemeinen existiert indessen im System (A) kein Element mit einer solchen Eigenschaft.
Es gibt noch einen Unterschied, der eng mit dem ersten verbunden ist:

In einem hyperkomplexen System kann man vom Produkt einer reellen Zahl k mit einem beliebigen Element $\mathbf{a}$ des gegebenen Systems sprechen (nach der Definition ist dies das Produkt

der Elemente $k = k + 0\mathbf{i}_1 + ... + 0\mathbf{i}_n$ und **a**); im System (A) dagegen besitzt das Produkt $k\mathbf{a}$ keinen Sinn.
Man kann jedoch diesen letzteren Unterschied leicht aufheben. Dazu genügt es, die Operation der Multiplikation einer reellen Zahl mit den Elementen von (A) durch

$$k(a_1\mathbf{i}_1 + a_2\mathbf{i}_2 + ... + a_n\mathbf{i}_n) = ka_1\mathbf{i}_1 + ka_2\mathbf{i}_2 + ... + ka_n\mathbf{i}_n$$

einzuführen. Mit einer solchen Operation versehen, verwandelt sich die Menge (A) (in ihr gibt es bereits die Addition und die Multiplikation) in ein Objekt, das die spezielle Bezeichnung Algebra der Dimension n oder einfach Algebra[8] trägt.

1.7.2 Definition einer Algebra

Wir werden jetzt die genaue Definition einer Algebra angeben. Eine Algebra der Dimension n wird eine Menge von Ausdrücken der Form

$$a_1\mathbf{i}_1 + a_2\mathbf{i}_2 + ... + a_n\mathbf{i}_n \tag{2}$$

genannt (wobei $a_1, a_2, ..., a_n$ beliebige reelle Zahlen und $\mathbf{i}_1, ..., \mathbf{i}_n$ bestimmte Symbole sind), die mit folgenden Operationen versehen ist:

1) der Multiplikation mit reellen Zahlen, die nach der Formel

$$k(a_1\mathbf{i}_1 + a_2\mathbf{i}_2 + ... + a_n\mathbf{i}_n) = ka_1\mathbf{i}_1 + ka_2\mathbf{i}_2 + ... + ka_n\mathbf{i}_n \tag{3}$$

ausgeführt wird;

2) der Addition

$$(a_1\mathbf{i}_1+a_2\mathbf{i}_2+...+a_n\mathbf{i}_n)+(b_1\mathbf{i}_1+b_2\mathbf{i}_2+...+b_n\mathbf{i}_n) = (a_1+b_1)\mathbf{i}_1+(a_2+b_2)\mathbf{i}_2+...+(a_n+b_n)\mathbf{i}_n \tag{4}$$

3) der Multiplikation, die durch eine Tafel der Form

$$\mathbf{i}_\alpha\mathbf{i}_\beta = p_{\alpha\beta,1}\mathbf{i}_1 + p_{\alpha\beta,2}\mathbf{i}_2 + ... + p_{\alpha\beta,n}\mathbf{i}_n \tag{5}$$

gegeben ist, wobei α, β beliebige Zahlen von 1 bis n sind (die Tafel wird zum Auffinden der Produkte

$$(a_1\mathbf{i}_1 + a_2\mathbf{i}_2 + ... + a_n\mathbf{i}_n)(b_1\mathbf{i}_1 + b_2\mathbf{i}_2 + ... + b_n\mathbf{i}_n)$$

genauso verwendet wie im Falle eines hyperkomplexen Systems).

Aus der oben gegebenen Definition einer Algebra ist ersichtlich, dass eine Algebra der Dimension n vollständig durch ihre "Multiplikationstafel" (5) bestimmt ist, d.h. durch einen bestimmten Satz von n^3 Zahlen $p_{\alpha\beta,\gamma}$. Im Prinzip sind diese Zahlen keinen Bedingungen unterworfen; jeder Satz von ihnen ergibt eine bestimmte Algebra.

1.7.3 Hyperkomplexe Systeme als Spezialfall einer Algebra

Obwohl wir zur größeren Klarheit der Darlegung den Begriff der Algebra aus dem Begriff eines hyperkomplexen Systems "entnahmen", muss man deutlich herausstellen, dass der Begriff der Algebra umfassender ist.

[8] Auf diese Weise besitzt das Wort "Algebra" zwei Bedeutungen: Algebra als Gebiet der Mathematik und Algebra als mathematisches Objekt mit den definierten Eigenschaften.

Anders ausgedrückt, kann man jedes hyperkomplexe System als Algebra der entsprechenden Dimension betrachten. Wir erklären dies ausführlicher.

Es möge eine Algebra $\mathscr{A}$, die aus den Elementen

$$a_1\mathbf{i}_1 + a_2\mathbf{i}_2 + ... + a_n\mathbf{i}_n$$

besteht, mit der Multiplikationstafel

$$\mathbf{i}_\alpha\mathbf{i}_\beta = p_{\alpha\beta,1}\mathbf{i}_1 + p_{\alpha\beta,2}\mathbf{i}_2 + ... + p_{\alpha\beta,n}\mathbf{i}_n$$

(α, β sind beliebige Zahlen von 1 bis n) gegeben sein, wobei die Einheit $\mathbf{i}_1$ die spezielle Eigenschaft

$$\mathbf{i}_1\mathbf{i}_\alpha = \mathbf{i}_\alpha \qquad \text{und} \qquad \mathbf{i}_\alpha\mathbf{i}_1 = \mathbf{i}_\alpha \tag{6}$$

für alle i von 1 bis n besitzt. Wir betrachten zusammen mit ihr ein hyperkomplexes System, das aus den Elementen

$$a_1 + a_2\mathbf{i}_2 + ... + a_n\mathbf{i}_n$$

mit einer Multiplikationstafel

$$\mathbf{i}_\alpha\mathbf{i}_\beta = p_{\alpha\beta,1} + p_{\alpha\beta,2}\mathbf{i}_2 + ... + p_{\alpha\beta,n}\mathbf{i}_n$$

(α, β sind beliebige Zahlen von 2 bis n) besteht; dieses hyperkomplexe System werden wir als mit der Algebra $\mathscr{A}$ übereinstimmend nachweisen.

Unter Verwendung der Multiplikationstafel kann man das Produkt von je zwei Elementen der gegebenen Algebra finden:

$$(a_1\mathbf{i}_1 + a_2\mathbf{i}_2 + ... + a_n\mathbf{i}_n)(b_1\mathbf{i}_1 + b_2\mathbf{i}_2 + ... + b_n\mathbf{i}_n) = c_1\mathbf{i}_1 + c_2\mathbf{i}_2 + ... + c_n\mathbf{i}_n$$

Wenn man jetzt in der niedergeschriebenen Gleichung $\mathbf{i}_1$ "wegnimmt", erhält man die Beziehung

$$(a_1 + a_2\mathbf{i}_2 + ... + a_n\mathbf{i}_n)(b_1 + b_2\mathbf{i}_2 + ... + b_n\mathbf{i}_n) = c_1 + c_2\mathbf{i}_2 + ... + c_n\mathbf{i}_n$$

die aufgrund von (6) das Multiplikationsgesetz im entsprechenden hyperkomplexen System ausdrückt. Auf solche Weise verwandelt sich jede Algebra mit der Bedingung (6) durch "Wegstreichen" des Symbols $\mathbf{i}_1$ aus der Schreibweise aller Elemente in ein hyperkomplexes System der gleichen Dimension.
Mehr noch, da die Zahlen $p_{\alpha\beta,\gamma}$ für $\alpha > 1$, $\beta > 1$ in der vorhergehenden Überlegung beliebig waren, kann man auf dem gezeigten Wege jedes hyperkomplexes System erhalten.

Zur Illustration betrachten wir ein Beispiel. Es möge eine zweidimensionale Algebra $\mathscr{A}$ mit der folgenden Multiplikationstafel gegeben sein:

$$\mathbf{i}_1\mathbf{i}_1 = \mathbf{i}_1, \quad \mathbf{i}_1\mathbf{i}_2 = \mathbf{i}_2, \quad \mathbf{i}_2\mathbf{i}_1 = \mathbf{i}_2, \quad \mathbf{i}_2\mathbf{i}_2 = -\mathbf{i}_1$$

Die Gleichung (6) wird hier offensichtlich erfüllt. Das Multiplikationsgesetz in $\mathscr{A}$ sieht folgendermaßen aus:

$$(a_1\mathbf{i}_1 + a_2\mathbf{i}_2)(b_1\mathbf{i}_1 + b_2\mathbf{i}_2) = (a_1b_1 - a_2b_2)\mathbf{i}_1 + (a_1b_2 + a_2b_1)\mathbf{i}_2$$

Wenn man $\mathbf{i}_1$ "wegstreicht", verwandelt sich die Multiplikationstafel in

$$\mathbf{i}_2\mathbf{i}_2 = -1$$

das Multiplikationsgesetz nimmt die Form

$$(a_1 + a_2\mathbf{i}_2)(b_1 + b_2\mathbf{i}_2) = (a_1b_1 - a_2b_2) + (a_1b_2 + a_2b_1)\mathbf{i}_2$$

an, woraus sofort klar wird, dass die betrachtete Algebra völlig mit dem System der komplexen Zahlen übereinstimmt.

1.7.4 Kommutative, assoziative Algebren. Algebren mit Division

Im § 5 führten wir eine Reihe Termini zur Bezeichnung bestimmter Eigenschaften hyperkomplexer Systeme ein. Diese Terminologie wird ohne jegliche Veränderung auf die Algebren übertragen.
Und zwar wird eine Algebra kommutativ genannt, wenn für je zwei Elemente **a** und **b** der Algebra $\mathscr{A}$ die Gleichung

$$\mathbf{ab} = \mathbf{ba}$$

gilt. Wenn für je drei Elemente **a**, **b** und **c** die Gleichung

$$(\mathbf{ab})\mathbf{c} = \mathbf{a}(\mathbf{bc})$$

gilt, wird die Algebra assoziativ[9] genannt. Weiter sagt man, wenn jede der Gleichungen

$$\mathbf{ax} = \mathbf{b} \qquad \text{und} \qquad \mathbf{ya} = \mathbf{b} \tag{7,8}$$

wobei **a** und **b** beliebige Elemente der Algebra $\mathscr{A}$ sind und $\mathbf{a} \neq 0$ ist, eine eindeutige Lösung besitzt, dass $\mathscr{A}$ eine Algebra mit Division ist.
Das Element **x**, das aus Gleichung (7) bestimmt wird, nennt man in diesem Falle den linken Quotient, das Element **y**, das aus (8) bestimmt wird, den rechten Quotient von **b** durch **a**.

Es ist nicht schwer zu sehen, dass in jeder Algebra mit Division folgendes gilt: Wenn das Produkt **ab** gleich Null ist, dann ist wenigstens einer der Faktoren **a** oder **b** gleich Null.
In der Tat ist $\mathbf{b} = 0$ wenn $a \neq 0$ ist, da $\mathbf{x} = 0$ die einzige Lösung der Gleichung $\mathbf{ax} = 0$ ist.
Später werden wir beweisen (siehe § 9), dass auch die Umkehrung richtig ist.

Wenn eine Algebra $\mathscr{A}$ die Eigenschaft besitzt, dass aus dem Verschwinden des Produkts **ab** folgt, dass wenigstens einer der Faktoren **a** oder **b** verschwindet, dann ist $\mathscr{A}$ eine Algebra mit Division.
Wenn in einer Algebra $\mathscr{A}$ ein solches Element **e** existiert, dass

$$\mathbf{ae} = \mathbf{a} \qquad \text{und} \qquad \mathbf{ea} = \mathbf{a}$$

für jedes $a \in \mathscr{A}$ gilt, dann wird dieses Element Einselement der Algebra $\mathscr{A}$ genannt; man spricht in diesem Falle auch davon, dass $\mathscr{A}$ eine Algebra mit Einselement ist.
Jedes hyperkomplexe System ist, wie schon bemerkt wurde, eine Algebra mit Einselement.
Das einfachste Beispiel einer Algebra mit Einselement ist die eindimensionale Algebra mit der Multiplikationstafel

$$\mathbf{i}_1\mathbf{i}_1 = \mathbf{i}_1$$

Das Multiplikationsgesetz hat in dieser Algebra die Form

$$(a_1)(b_1\mathbf{i}_1) = a_1 b_1 \mathbf{i}_1$$

d.h. es führt zur Multiplikation der reellen Zahlen. In Übereinstimmung damit werden wir die gezeigte Algebra als Algebra der reellen Zahlen bezeichnen.

[9] In der Anfangsphase der Entwicklung der Theorie der Algebra empfand man die Bedingung der Assoziativität als so natürlich, dass sie in die Definition einer Algebra eingeschlossen wurde; unter dem Terminus "Algebra" wurde eine "assoziative Algebra" verstanden.

1.7.5 Beispiele

Wir werden einige Beispiele von Algebren betrachten, die keine hyperkomplexen Systeme darstellen.

Beispiel 4. Nullalgebra der Dimension n.
Die Multiplikationstafel hat in dieser Algebra eine äußerst einfache Form:

$$\mathbf{i}_\alpha \mathbf{i}_\beta = 0$$

(für alle Zahlen α, β von 1 bis n). Daraus folgt sofort, dass das Produkt von je zwei Elementen auch gleich Null ist.

Beispiel 2. Wir betrachten die zweidimensionale Algebra mit der Multiplikationstafel

$$\mathbf{i}_1\mathbf{i}_1 = \mathbf{i}_1, \qquad \mathbf{i}_1\mathbf{i}_2 = \mathbf{i}_2, \qquad \mathbf{i}_2\mathbf{i}_1 = -\mathbf{i}_2, \qquad \mathbf{i}_2\mathbf{i}_2 = \mathbf{i}_1$$

Das Multiplikationsgesetz ist dann

$$(a_1\mathbf{i}_1 + a_2\mathbf{i}_2)(b_1\mathbf{i}_1 + b_2\mathbf{i}_2) = (a_1b_1 + a_2b_2)\mathbf{i}_1 + (a_1b_2 - a_2b_1)\mathbf{i}_2$$

Obwohl in dieser Algebra die Multiplikation an die Multiplikation der komplexen Zahlen erinnert, stimmt sie nicht mit der Algebra der komplexen Zahlen überein. Wir schlagen dem Leser vor, selbst zu überprüfen, dass es in dieser Algebra kein Einselement gibt (daher kann sie auch kein hyperkomplexes System sein).

Eine schwierigere Übung ist die Überprüfung der interessanten Tatsache, dass die betrachtete Algebra eine Algebra mit Division ist.

Beispiel 3. Die Algebra dreidimensionaler Vektoren mit der vektoriellen Multiplikation. Diese Algebra besteht aus Elementen der Form

$$b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$$

die gemäß der Tafel

$$\begin{aligned} \mathbf{i}^2 = \mathbf{0}, \qquad \mathbf{j}^2 = \mathbf{0}, \qquad \mathbf{k}^2 = \mathbf{0} \\ \mathbf{ij} = \mathbf{k}, \quad \mathbf{ji} = -\mathbf{k}, \quad ,\mathbf{jk} = \mathbf{i}, \quad \mathbf{kj} = -\mathbf{i}, \quad \mathbf{ki} = \mathbf{j}, \quad \mathbf{ik} = -\mathbf{j} \end{aligned}$$

multipliziert werden. Auf diese Weise erhalten wir

$$(b\mathbf{i} + c\mathbf{j} + d\mathbf{k})(b'\mathbf{i} + c'\mathbf{j} + d'\mathbf{k}) = (cd' - dc')\mathbf{i} + (db' - bd')\mathbf{j} + (bc' - cb')\mathbf{k} \tag{9}$$

Wenn man im gewöhnlichen Raum ein rechtwinkliges Koordinatensystem einführt und unter **i**, **j**, **k** Vektoren der Länge 1 versteht, die die Richtung der Koordinatenachsen haben (Abb. 9), dann stellt der Ausdruck

$$\mathbf{q} = b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$$

selbst (bei der üblichen geometrischen Bedeutung der Summe von Vektoren und des Produkts eines Vektors mit einer Zahl) einen bestimmten Vektor im Raum dar.
Die Operation (9) wird als vektorielle Multiplikation bezeichnet (geometrische Bedeutung siehe § 4). Sie spielt in der Geometrie und der Physik eine wichtige Rolle.

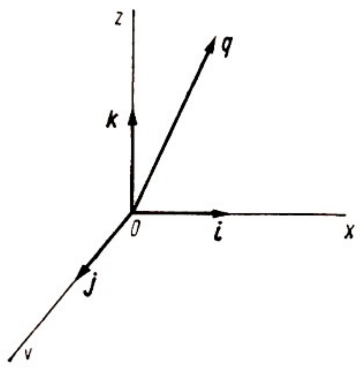


Abb.9

1.7.6 Ein wichtiges Beispiel: die Algebra quadratischer Matrizen n-ter Ordnung

Die Dimension dieser Algebra ist gleich n^2. Die entsprechenden imaginären Einheiten könnten mit $\mathbf{i}_1, \mathbf{i}_2, ..., \mathbf{i}_{n^2}$ bezeichnet werden.
Bequemer ist jedoch ein anderes Prinzip der Indizierung: anstelle des Index α, der die Werte von 1 bis n^2 durchläuft, ist es zweckmäßiger, einen "Index" zu nehmen, der aus zwei Zahlen α und β besteht, von denen jede die Werte von 1 bis n durchläuft (offensichtlich ist die Anzahl verschiedener Paare α, β genau n^2).

Wir führen auf diese Weise für die imaginären Einheiten die Bezeichnung $\mathbf{i}_{\alpha\beta}$ ein. Die Reihenfolge der imaginären Einheiten kann man nach Belieben festlegen; der Eindeutigkeit halber werden wir sie in solcher Reihenfolge darlegen

$$\mathbf{i}_{11}, \mathbf{i}_{12}, ..., \mathbf{i}_{1n}, \mathbf{i}_{21}, \mathbf{i}_{22}, ..., \mathbf{i}_{2n}, \mathbf{i}_{31}, ..., \mathbf{i}_{n1}, \mathbf{i}_{n2}, ..., \mathbf{i}_{nn}$$

Die Elemente unserer Algebra sind also Ausdrücke folgender Form

$$\begin{aligned} A = & a_{11}\mathbf{i}_{11} + a_{12}\mathbf{i}_{12} + ... + a_{1n}\mathbf{i}_{1n} \\ & + a_{21}\mathbf{i}_{21} + a_{22}\mathbf{i}_{22} + ... + a_{2n}\mathbf{i}_{2n} \\ & + ... \\ & + a_{n1}\mathbf{i}_{n1} + a_{n2}\mathbf{i}_{n2} + ... + a_{nn}\mathbf{i}_{nn} \end{aligned} \tag{10}$$

In dieser Schreibweise wird die Tatsache besonders klar, dass jedes Element A unserer Algebra durch die Anordnung

$$\begin{pmatrix} a_{11} & a_{12} & ... & a_{1n} \\ a_{21} & a_{22} & ... & a_{2n} \\ ... & ... & & ... \\ a_{n1} & a_{n2} & ... & a_{nn} \end{pmatrix}$$

die aus n^2 Zahlen besteht, definiert wird. Solche Anordnungen tragen die Bezeichnung Matrizen, genauer, quadratische Matrizen n-ter Ordnung (Ordnung wird die Zahl der Zeilen oder Spalten des quadratischen Schemas genannt). Im weiteren werden wir anstelle von (10) kurz

$$A = \begin{pmatrix} a_{11} & a_{12} & ... & a_{1n} \\ a_{21} & a_{22} & ... & a_{2n} \\ ... & ... & & ... \\ a_{n1} & a_{n2} & ... & a_{nn} \end{pmatrix}$$

schreiben und annehmen, dass die Elemente unserer Algebra Matrizen sind.

Wir definieren jetzt die Multiplikationstafel der Einheiten $\mathbf{i}_{\alpha\beta}$; in ihr sind alle Charakteristika der Matrizenalgebren enthalten. Wir setzen

$$\mathbf{i}_{\alpha 1}\mathbf{i}_{1\beta} = \mathbf{i}_{\alpha\beta}, \quad \mathbf{i}_{\alpha 2}\mathbf{i}_{2\beta} = \mathbf{i}_{\alpha\beta}, \quad ..., \quad \mathbf{i}_{\alpha n}\mathbf{i}_{n\beta} = \mathbf{i}_{\alpha\beta} \tag{11}$$

oder kürzer

$$\mathbf{i}_{\alpha\lambda}\mathbf{i}_{\lambda\beta} = \mathbf{i}_{\alpha\beta}$$

(α, β und λ sind beliebige Zahlen von 1 bis n); alle übrigen Produkte der imaginären Einheiten sind nach Definition gleich Null. Damit ist die Multiplikationstafel vollständig angegeben. Man kann übrigens die ganze Multiplikationstafel in der knapperen Form

$$\mathbf{i}_{\alpha\lambda}\mathbf{i}_{\mu\beta} = \delta_{\lambda\mu}\mathbf{i}_{\alpha\beta} \tag{12}$$

schreiben, wobei das Symbol $\delta_{\lambda\mu}$ definitionsgemäß gleich 1 ist, wenn $\lambda = \mu$ und gleich 0 ist, wenn $\lambda \neq \mu$.

Wir werden jetzt sehen, wie das Produkt von je zwei Elementen A und B unserer Algebra geschrieben wird, d.h., wir berechnen

$$\begin{pmatrix} a_{11}\mathbf{i}_{11} + ... + a_{1n}\mathbf{i}_{1n} \\ a_{21}\mathbf{i}_{21} + ... + a_{2n}\mathbf{i}_{2n} \\ ... \\ a_{n1}\mathbf{i}_{n1} + ... + a_{nn}\mathbf{i}_{nn} \end{pmatrix} \begin{pmatrix} b_{11}\mathbf{i}_{11} + ... + b_{1n}\mathbf{i}_{1n} \\ b_{21}\mathbf{i}_{21} + ... + b_{2n}\mathbf{i}_{2n} \\ ... \\ b_{n1}\mathbf{i}_{n1} + ... + b_{nn}\mathbf{i}_{nn} \end{pmatrix}$$

Als Resultat muss man ein bestimmtes Element **C** erhalten:

$$\mathbf{C} = \begin{pmatrix} c_{11}\mathbf{i}_{11} + c_{12}\mathbf{i}_{12} + ... + c_{1n}\mathbf{i}_{1n} \\ c_{21}\mathbf{i}_{21} + c_{22}\mathbf{i}_{22} + ... + c_{2n}\mathbf{i}_{2n} \\ ... \\ c_{n1}\mathbf{i}_{n1} + c_{n2}\mathbf{i}_{n2} + ... + c_{nn}\mathbf{i}_{nn} \end{pmatrix}$$

Wir betrachten einen beliebigen Summanden $c_{\alpha\beta}\mathbf{i}_{\alpha\beta}$ in **C**. Wie die Multiplikationstafel (11) zeigt, entsteht dieser Summand nur durch die Multiplikation von

$$a_{\alpha 1}\mathbf{i}_{\alpha 1} \text{ mit } b_{1\beta}\mathbf{i}_{1\beta}, a_{\alpha 2}\mathbf{i}_{\alpha 2} \text{ mit } b_{2\beta}\mathbf{i}_{2\beta}, ..., a_{\alpha n}\mathbf{i}_{\alpha n} \text{ mit } b_{n\beta}\mathbf{i}_{n\beta}$$

folglich ist er gleich

$$(a_{\alpha 1}b_{1\beta} + a_{\alpha 2}b_{2\beta} + ... + a_{\alpha n}b_{n\beta})\mathbf{i}_{\alpha\beta}$$

Also ist

$$c_{\alpha\beta} = a_{\alpha 1}b_{1\beta} + a_{\alpha 2}b_{2\beta} + ... + a_{\alpha n}b_{n\beta}$$

Es ist durchaus nicht schwierig, sich diese Formel zu merken:
Man nimmt die α-te Zeile der Matrix **A**

$$a_{\alpha 1}a_{\alpha 2}...a_{\alpha n}$$

und die β-te Spalte der Matrix B

$$\begin{matrix} b_{1\beta} \\ b_{2\beta} \\ ... \\ b_{n\beta} \end{matrix}$$

multipliziert dann jede Zahl der Zeile mit der entsprechenden Zahl der Spalte und addiert alle diese Produkte; als Ergebnis erhält man die Zahl $c_{\alpha\beta}$ aus der Matrix C.

Die Regel, die wir gerade aufgestellt haben, erlaubt es, aus je zwei Matrizen A und B eine dritte Matrix C aufzubauen; man nennt sie naturgemäß Produkt der Matrizen A und B. Um die Elemente A und B unserer Algebra zu multiplizieren, muss man also das Produkt der entsprechenden Matrizen A und B finden.

Als Beispiel berechnen wir das Produkt der Matrizen

$$A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \quad \text{und} \quad B = \begin{pmatrix} 6 & -4 \\ -3 & 3 \end{pmatrix}$$

Wir bekommen

$$AB = \begin{pmatrix} 1 \cdot 6 + 2 \cdot (-3) & 1 \cdot (-4) + 2 \cdot 3 \\ 3 \cdot 6 + 4 \cdot (-3) & 3 \cdot (-4) + 4 \cdot 3 \end{pmatrix} = \begin{pmatrix} 0 & 2 \\ 6 & 0 \end{pmatrix}$$

Die auf diesem Wege entwickelte Multiplikation der Matrizen spielt in der Mathematik eine außerordentlich wichtige Rolle. Der Rahmen des vorliegenden Büchleins erlaubt es nicht, uns ausführlicher mit der Untersuchung dieser Operation zu beschäftigen.

Wir wollen uns auf die Feststellung einer wichtigen Eigenschaft der Multiplikation der Matrizen beschränken. Wir werden zeigen, dass die Multiplikation der Matrizen assoziativ ist oder, anders ausgedrückt, dass die Matrizenalgebra eine assoziative Algebra ist. Für den Beweis ist es hinreichend zu überprüfen, dass die Gleichung

$$(AB)C = A(BC)$$

richtig ist, wenn für A, B und C drei beliebige "imaginäre Einheiten" der Matrizenalgebra genommen werden (siehe die analoge Überlegung beim Beweis der Assoziativität der Multiplikation der Quaternionen im § 3). Anders gesagt, man braucht nur zu überprüfen, dass

$$(\mathbf{i}_{\alpha\lambda}\mathbf{i}_{\mu\beta})\mathbf{i}_{\nu\gamma} = \mathbf{i}_{\alpha\lambda}(\mathbf{i}_{\mu\beta}\mathbf{i}_{\nu\gamma})$$

gilt. Die linke Seite ist aber gemäß (12) gleich $(\delta_{\lambda\mu}\mathbf{i}_{\alpha\beta})\mathbf{i}_{\nu\gamma}$, oder, erneut aufgrund von (12), gleich $\delta_{\lambda\mu}\delta\beta\nu\mathbf{i}_{\alpha\gamma}$.
Analog findet man die rechte Seite: sie ist gleich $\mathbf{i}_{\alpha\lambda}(\delta_{\beta\nu}\mathbf{i}_{\mu\gamma})$ oder $\delta\beta\nu\delta_{\lambda\mu}\mathbf{i}_{\alpha\gamma}$. In beiden Fällen erhält man ein und dasselbe Resultat.

1.7.7 Charakteristische Eigenschaften der Multiplikation in einer beliebigen Algebra

[10] Aus der Definition einer Algebra gehen direkt die folgenden Eigenschaften der Multiplikation hervor:

1) $(\mathbf{a}+\mathbf{b})\mathbf{c} = \mathbf{ac}+\mathbf{bc}, \quad \mathbf{a}(\mathbf{b}+\mathbf{c}) = \mathbf{ab}+\mathbf{ac}$

2) $k\mathbf{a}\cdot\mathbf{b} = k(\mathbf{ab}), \quad \mathbf{a}\cdot k\mathbf{b} = k(\mathbf{ab})$

Diese Eigenschaften sind in einem gewissen Sinne für die Multiplikation bestimmend. Genauer, es gilt der folgende Satz:

[10] Der Inhalt dieses Punktes hat erläuternden Charakter und wird von uns nur in den §§ 16 und 18 benötigt.

In der Menge $\mathscr{A}$ aller Ausdrücke der Form

$$a_1\mathbf{i}_1 + a_2\mathbf{i}_2 + ... + a_n\mathbf{i}_n$$

seien die Multiplikation mit einer Zahl, (3), die Addition, (4), sowie eine weitere bestimmte Operation[11] $\mathbf{a} \circ \mathbf{b}$, die die oben gezeigten Eigenschaften 1) und 2) besitzt, definiert:

1) $(\mathbf{a} + \mathbf{b}) \circ \mathbf{c} = \mathbf{a} \circ \mathbf{c} + \mathbf{b} \circ \mathbf{c}, \quad \mathbf{a} \circ (\mathbf{b} + \mathbf{c}) = \mathbf{a} \circ \mathbf{b} + \mathbf{a} \circ \mathbf{c}$

2) $k\mathbf{a} \circ \mathbf{b} = k(\mathbf{a} \circ \mathbf{b}), \quad \mathbf{a} \circ k\mathbf{b} = k(\mathbf{a} \circ \mathbf{b})$

Dann ist die Menge $\mathscr{A}$ eine Algebra, in der $\mathbf{a} \circ \mathbf{b}$ die Rolle der Multiplikation spielt.
Um diesen Satz zu beweisen, müssen wir uns vergewissern, dass die Operation $\mathbf{a} \circ \mathbf{b}$ die Multiplikation in der Bedeutung ist, wie in der Definition einer Algebra festgelegt wurde. Wir betrachten den Ausdruck $\mathbf{i}_\alpha \circ \mathbf{i}_\beta$. Dieser ist ein bestimmtes Element der Menge $\mathscr{A}$, d.h.,

$$\mathbf{i}_\alpha \circ \mathbf{i}_\beta = p_{\alpha\beta,1}\mathbf{i}_1 + p_{\alpha\beta,2}\mathbf{i}_2 + ... + p_{\alpha\beta,n}\mathbf{i}_n \tag{13}$$

Aus den Eigenschaften 1) und 2) folgt, dass

$$\mathbf{a} \circ \mathbf{b} = (a_1\mathbf{i}_1 + ... + a_n\mathbf{i}_n) \circ (b_1\mathbf{i}_1 + ... + b_n\mathbf{i}_n) = \sum_{\alpha,\beta}[(a_\alpha\mathbf{i}_\alpha) \circ (b_\beta\mathbf{i}_\beta)] = \sum_{\alpha,\beta} a_\alpha b_\beta(\mathbf{i}_\alpha) \circ \mathbf{i}_\beta)$$

gilt [zum Nachweis der ersten Gleichheit verwendeten wir die Eigenschaft 1), für die zweite Gleichheit verwendeten wir 2)].
Danach braucht man zur Berechnung von $\mathbf{a} \circ \mathbf{b}$ nur noch anstelle von $\mathbf{i}_\alpha \circ \mathbf{i}_\beta$ das entsprechende Element (13) zu setzen, die Zahl $a_\alpha b_\beta$ mit diesem Element zu multiplizieren und danach entsprechende Glieder einzuführen. Dies ist aber genau dasselbe Verfahren, mit dessen Hilfe die Multiplikation der Elemente in einer beliebigen Algebra $\mathscr{A}$ definiert wurde.

[11] An dieser Stelle bedeutet "ist eine bestimmte Operation gegeben" nur die Tatsache, dass je zwei Elementen $\mathbf{a}$ und $\mathbf{b}$ ein drittes Element, das mit $\mathbf{a} \circ \mathbf{b}$ bezeichnet wird, zugeordnet wird.

2 n-dimensionale Vektoren

Wir wenden uns noch einmal zurück zur Definition einer Algebra der Dimension n. In dieser Definition besteht das schwierigste Moment unbestreitbar im Vorhandensein der Multiplikation. Bleibt noch irgend etwas übrig, wenn man von dieser Eigenschaft absieht?

Man sieht leicht, dass, obwohl nicht viel, doch noch etwas übrigbleibt. Es bleibt die Gesamtheit der Elemente übrig, die eindeutig in der Form

$$a_1\mathbf{i}_1 + a_2\mathbf{i}_2 + ... + a_n\mathbf{i}_n$$

dargestellt werden mit der natürlichen Additionsregel der Elemente untereinander

$$(a_1\mathbf{i}_1{+}a_2\mathbf{i}_2 + ... + a_n\mathbf{i}_n) + (b_1\mathbf{i}_1 + b_2\mathbf{i}_2 + ... + b_n\mathbf{i}_n) = \\ = (a_1 + b_1)\mathbf{i}_1 + (a_2 + b_2)\mathbf{i}_2 + ... + (a_n + b_n)\mathbf{i}_n$$

und mit der ebenso natürlichen Multiplikationsregel der Elemente mit einer reellen Zahl

$$k(a_1\mathbf{i}_1 + a_2\mathbf{i}_2 + ... + a_n\mathbf{i}_n) = ka_1\mathbf{i}_1 + ka_2\mathbf{i}_2 + ... + ka_n\mathbf{i}_n)$$

Ist es möglich, nur auf der Grundlage dieses Materials irgendeine inhaltsreiche Theorie zu entwickeln? Es erweist sich, dass dies möglich ist.
Mehr noch, es existiert ein ganzes Gebiet der Mathematik, dem nur die oben gezeigten Operationen zugrunde liegen. Dieses Gebiet wird lineare Algebra genannt. Es ist sehr inhaltsreich und wird oft sowohl in der Mathematik selbst als auch in ihren zahlreichen Anwendungen benutzt. In diesem Kapitel werden wir den Leser mit einigen Tatsachen aus der linearen Algebra bekanntmachen. Sie bilden die Basis, auf der die Untersuchung der Theorie der Algebren im Kapitel 3 fortgesetzt wird.

2.8 Der n-dimensionale Vektorraum A_n

2.8.1 Grundlegende Definitionen

Definition 1. Wir werden ein Objekt der Form

$$a_1\mathbf{i}_1 + a_2\mathbf{i}_2 + ... + a_n\mathbf{i}_n \tag{1}$$

einen n-dimensionalen Vektor nennen, wobei $a_1, a_2, ..., a_n$ beliebige reelle Zahlen und

$$\mathbf{i}_1, \mathbf{i}_2, ..., \mathbf{i}_n$$

einfach n verschiedene Symbole sind, denen wir keine spezielle Bedeutung zuschreiben.
Wir erklären, warum der Ausdruck (1) "Vektor" genannt wird. Es ist so, dass man bei $n = 2$ einen Ausdruck der Form

$$a_1\mathbf{i}_1 + a_2\mathbf{i}_2 \tag{2}$$

erhält, und wenn man $\mathbf{i}_1$ und $\mathbf{i}_2$ als zwei fixierte Vektoren in der gewöhnlichen Ebene ansieht, dann wird der oben aufgeschriebene Ausdruck auch einem bestimmten Vektor in der Ebene[12] entsprechen (Abb. 10).

[12]Wir gehen vom gewöhnlichen geometrischen Verständnis der Summe von Vektoren und des Produktes eines Vektors mit einer Zahl aus. Wir erinnern daran, dass die Summe von Vektoren nach der "Parallelogrammregel" bestimmt wird und die Multiplikation eines Vektors mit einer Zahl k seine Verlängerung um das k-fache ist mit einer anschließenden Richtungsumkehrung, falls $k < 0$ ist.

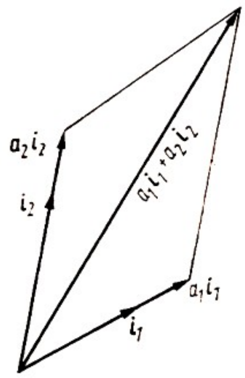


Abb.10

Mehr noch, wenn die Vektoren $\mathbf{i}_1$ und $\mathbf{i}_2$ nicht auf einer Geraden liegen, kann jeder Vektor der Ebene (eindeutig) in einer solchen Form dargestellt werden.

Definition 2. Zwei n-dimensionale Vektoren

$$a_1\mathbf{i}_1 + a_2\mathbf{i}_2 + ... + a_n\mathbf{i}_n \qquad \text{und} \qquad b_1\mathbf{i}_1 + b_2\mathbf{i}_2 + ... + b_n\mathbf{i}_n$$

betrachtet man dann und nur dann als gleich, wenn

$$a_1 = b_1, a_2 = b_2, ..., a_n = b_n$$

ist.
Als Motiv für eine solche Definition dient die oben bereits erwähnte Tatsache, nämlich die Gleichwertigkeit der Darstellung eines beliebigen Vektors in der Ebene in der Form (2), wenn die "Basis"-Vektoren $\mathbf{i}_1, \mathbf{i}_2$ so ausgewählt wurden, dass sie nicht auf einer Geraden liegen.

Definition 3. Die Addition n-dimensionaler Vektoren erfolgt nach der Regel

$$(a_1\mathbf{i}_1+a_2\mathbf{i}_2 + ... + a_n\mathbf{i}_n) + (b_1\mathbf{i}_1 + b_2\mathbf{i}_2 + ... + b_n\mathbf{i}_n) =$$
$$= (a_1 + b_1)\mathbf{i}_1 + (a_2 + b_2)\mathbf{i}_2 + ... + (a_n + b_n)\mathbf{i}_n$$

die Multiplikation eines n-dimensionalen Vektors mit einer reellen Zahl nach der Regel

$$k(a_1\mathbf{i}_1 + a_2\mathbf{i}_2 + ... + a_n\mathbf{i}_n) = ka_1\mathbf{i}_1 + ka_2\mathbf{i}_2 + ... + ka_n\mathbf{i}_n)$$

Diese Definition wurde verständlicherweise durch die Analogie mit den geometrischen Vektoren angeregt.

Zur abgekürzten Bezeichnung n-dimensionaler Vektoren werden wir die halbfetten Buchstaben **a**, **b**, **e** usw. verwenden. Die Gleichheit der Vektoren **a** und **b** wird in gewöhnlicher Weise

$$\mathbf{a} = \mathbf{b}$$

geschrieben. Es ist leicht zu sehen, dass die oben definierte Vektoraddition die Eigenschaften

$$\mathbf{a} + \mathbf{b} = \mathbf{b} + \mathbf{a} \qquad \text{und} \qquad \text{(Kommutativität)}$$

$$(\mathbf{a} + \mathbf{b}) + \mathbf{c} = \mathbf{a} + (\mathbf{b} + \mathbf{c}) \qquad \text{(Assoziativität)}$$

besitzt und für die Multiplikation eines Vektors mit einer Zahl die folgenden Beziehungen gelten:

$$k(l\mathbf{a}) = (kl)\mathbf{a} \quad , \quad (k + l)\mathbf{a} = k\mathbf{a} + l\mathbf{a}$$

Die Gesamtheit aller n-dimensionalen Vektoren werden wir n-dimensionalen Vektorraum nennen und mit A_n bezeichnen. Der Vektor der Form

$$0\mathbf{i}_1 + 0\mathbf{i}_2 + ... + 0\mathbf{i}_n$$

wird Nullvektor genannt und mit **0** bezeichnet. Offensichtlich gelten

$$\mathbf{a} + \mathbf{0} = \mathbf{a} \qquad \text{und} \qquad \mathbf{0a} = \mathbf{0}$$

für jeden Vektor **a**. Wir werden von nun an den Nullvektor einfach Null nennen.

2.8.2 Der Begriff der linearen Abhängigkeit

Gewöhnlich wird man es bei der Untersuchung irgendeiner Frage nicht mit einem einzelnen Vektor zu tun haben, sondern mit einem ganzen System n-dimensionaler Vektoren. In diesem Falle werden sie in der Regel durch ein und denselben Buchstaben (sagen wir durch **a**) mit verschiedenen Indizes bezeichnet.

Beispiel.

$$\begin{aligned} \mathbf{a}_1 &= -5\mathbf{i}_1 + 3\mathbf{i}_2 + 5\mathbf{i}_3 + 3\mathbf{i}_4 \\ \mathbf{a}_2 &= -\mathbf{i}_1 + \mathbf{i}_2 + 4\mathbf{i}_3 + 3\mathbf{i}_4 \\ \mathbf{a}_3 &= \mathbf{i}_1 + 0\mathbf{i}_2 + 3\mathbf{i}_3 - 2\mathbf{i}_4 \end{aligned} \tag{3}$$

Das ist ein System von drei 4-dimensionalen Vektoren.

Es möge $\mathbf{a}_1, \mathbf{a}_2, ..., \mathbf{a}_m$ irgendein System n-dimensionaler Vektoren sein. Wir nehmen die beliebigen Zahlen $k_1, k_2, ..., k_m$ und bilden den Vektor

$$\mathbf{a} = k_1\mathbf{a}_1 + k_2\mathbf{a}_2 + ... + k_m\mathbf{a}_m$$

Jeder Vektor **a** von dieser Form wird Linearkombination der gegebenen Vektoren $\mathbf{a}_1, \mathbf{a}_2, ..., \mathbf{a}_m$ genannt und die Zahlen $k_1, k_2, ..., k_m$ die Koeffizienten dieser Linearkombination.

Beispiel. Gesucht ist die Linearkombination

$$\mathbf{a}_1 - 3\mathbf{a}_2 + 2\mathbf{a}_3$$

der Vektoren $\mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_3$ aus dem oben angeführten System (3). Durch Addition der Vektoren

$$\begin{aligned} \mathbf{a}_1 &= -5\mathbf{i}_1 + 3\mathbf{i}_2 + 5\mathbf{i}_3 + 3\mathbf{i}_4 \\ -3\mathbf{a}_2 &= 3\mathbf{i}_1 - 3\mathbf{i}_2 - 12\mathbf{i}_3 - 9\mathbf{i}_4 \\ 2\mathbf{a}_3 &= 2\mathbf{i}_1 + 0\mathbf{i}_2 + 6\mathbf{i}_3 - 4\mathbf{i}_4 \end{aligned}$$

erhalten wir

$$\mathbf{a}_1 - 3\mathbf{a}_2 + 2\mathbf{a}_3 = 0\mathbf{i}_1 + 0\mathbf{i}_2 - 1\mathbf{i}_3 - 10\mathbf{i}_4$$

Wenn der Vektor **a** eine Linearkombination der Vektoren $\mathbf{a}_1, \mathbf{a}_2, ..., \mathbf{a}_m$ ist, dann sagt man
"**a** wird durch $\mathbf{a}_1, \mathbf{a}_2, ..., \mathbf{a}_m$ linear dargestellt"
oder
"**a** wird in $\mathbf{a}_1, \mathbf{a}_2, ..., \mathbf{a}_m$ zerlegt."

Wir werden meist den letzten Ausdruck verwenden, Wir führen noch eine wichtige Definition ein.

Definition 4. Ein System von Vektoren

$$\mathbf{a}_1, \mathbf{a}_2, ..., \mathbf{a}_p \tag{4}$$

wird linear abhängig genannt, wenn eine bestimmte Linearkombination dieser Vektoren gleich dem Nullvektor ist

$$s_1\mathbf{a}_1 + s_2\mathbf{a}_2 + ... + s_p\mathbf{a}_p = \mathbf{0} \tag{5}$$

wobei mindestens einer der Koeffizienten $s_1, s_2, ..., s_p$ von Null verschieden ist. Im entgegengesetzten Fall (d.h. wenn keine Linearkombination solcher Art existiert) wird das System (4) linear unabhängig genannt.

Aus der Definition geht direkt hervor, dass ein System, das aus einem Vektor besteht, nur in dem Falle linear abhängig ist, wenn dieser Vektor der Nullvektor ist (tatsächlich folgt aus $s_1\mathbf{a}_1 = \mathbf{0}$ und $s_1 \neq 0$, $\mathbf{a}_1 \neq \mathbf{0}$).

Im Falle eines Systems von zwei Vektoren bedeutet die lineare Abhängigkeit, dass man die Zahlen s_1 und s_2, von denen mindestens eine von Null verschieden ist, derart ermitteln muss, dass

$$s_1\mathbf{a}_1 + s_2\mathbf{a}_2 = \mathbf{0}$$

ist. Es möge zum Beispiel $s_1 \neq 0$ sein. Dann folgt aus der niedergeschriebenen Gleichung

$$\mathbf{a}_1 = k\mathbf{a}_2$$

(wobei $k = -s_2/s_1$ ist). Zwei Vektoren, die durch eine solche Abhängigkeit verbunden sind, werden zueinander proportional genannt.

Es sei jetzt ein linear abhängiges System von p Vektoren gegeben, wobei p eine beliebige Zahl ist. Wir setzen der Eindeutigkeit halber voraus, dass in Gleichung (5) der Koeffizient s_1 von Null verschieden ist. Dann folgt aus dieser Gleichung

$$\mathbf{a}_1 = k_2\mathbf{a}_2 + k_3\mathbf{a}_3 + ... + k_p\mathbf{a}_p$$

d.h., der Vektor $\mathbf{a}_1$ wird durch die übrigen Vektoren des Systems linear dargestellt. Diese Überlegung zeigt, dass ein linear abhängiges System entweder aus einem Vektor besteht (und dann ist dieser $\mathbf{0}$ oder dass einer der Vektoren des Systems durch die übrigen Vektoren linear ausgedrückt wird.

2.8.3 Eine andere Definition der linearen Abhängigkeit

Im weiteren wird es für uns bequemer sein, eine ändere Formulierung des Begriffs der linearen Abhängigkeit zu verwenden.
Das System (4) ist linear abhängig, wenn man irgendeinen Vektor des Systems linear durch die ihm vorhergehenden Vektoren des Systems ausdrücken kann oder wenn $\mathbf{a}_1 = \mathbf{0}$ ist.

Wir werden zeigen, dass diese Formulierung der ursprünglichen äquivalent ist. In der Tat, wenn $\mathbf{a}_1 = \mathbf{0}$ ist, dann ist das System linear abhängig, da in diesem Falle die Linearkombination

$$1 \cdot \mathbf{a}_1 + 0\mathbf{a}_2 + ... + 0\mathbf{a}_p$$

gleich Null ist, wobei der erste Koeffizient von Null verschieden ist. Wenn einer der Vektoren des Systems linear durch die vorhergehenden ausgedrückt wird

$$\mathbf{a}_i = k_1\mathbf{a}_1 + ... + k_{i-1}\mathbf{a}_{i-1}$$

dann ist in diesem Falle das System auch linear abhängig, denn die Linearkombination

$$k_1\mathbf{a}_1 + ... + k_{i-1}\mathbf{a}_{i-1} - 1\mathbf{a}_i + 0\mathbf{a}_{i+1} + ... + 0\mathbf{a}_p$$

ist gleich Null, wobei der Koeffizient von $\mathbf{a}_i$ von Null verschieden ist. Umgekehrt möge das System linear abhängig sein, d.h., es gilt (5), wobei mindestens einer der Koeffizienten $s_1, s_2, ..., s_p$ nicht gleich Null ist.
Wir betrachten den letzten von Null verschiedenen Koeffizienten. Wenn dieser s_1 ist, dann gilt $s_1\mathbf{a}_1 = \mathbf{0}$, folglich ist $\mathbf{a}_1 = \mathbf{0}$. Wenn der betrachtete Koeffizient s_i ist, wobei $i > 1$ ist, dann erhalten wir durch Hinzufügen des Vektors $-s_i\mathbf{a}_i$ zu beiden Seiten der Gleichung und Multiplikation beider Seiten $-1/s_i$ eine Gleichung der Form

$$\mathbf{a}_i = k_1\mathbf{a}_1 + ... + k_{i-1}\mathbf{a}_{i-1}$$

d.h., wir kommen zur Zerlegung des Vektors $\mathbf{a}_i$ in die ihm vorhergehenden Vektoren des Systems.

2.8.4 Die Ausgangsbasis

Den Vektor

$$1\mathbf{i}_1 + 0\mathbf{i}_2 + ... + 0\mathbf{i}_n$$

bezeichnet man natürlicherweise kurz mit $\mathbf{i}_1$. Auf diese Weise wird das Symbol $\mathbf{i}_1$, dem wir früher keine spezielle Bedeutung zuordneten, jetzt mit einem Vektor identifiziert. Analog wird der Vektor

$$0\mathbf{i}_1 + 1\mathbf{i}_2 + ... + 0\mathbf{i}_n$$

mit $\mathbf{i}_2$ identifiziert usw., schließlich wird der Vektor

$$0\mathbf{i}_n + 0\mathbf{i}_2 + ... + 1\mathbf{i}_n$$

mit $\mathbf{i}_n$ identifiziert. Die auf diesem Wege definierten Vektoren

$$\mathbf{i}_1, \mathbf{i}_2, ...; \mathbf{i}_n$$

besitzen die Eigenschaft, dass man jeden Vektor aus A_n in sie zerlegen kann. In der Tat, betrachten wir einen beliebigen Vektor $\mathbf{a} \in A_n$. Er besitzt die Gestalt einer formalen Summe

$$a_1\mathbf{i}_1 + a_2\mathbf{i}_2 + ... + a_n\mathbf{i}_n \tag{6}$$

Wenn wir die oben angegebenen Definitionen 2 und 3 berücksichtigen, dann können wir Schreiben

$$a_1\mathbf{i}_1 + a_2\mathbf{i}_2 + ... + a_n\mathbf{i}_n = a_1(1\mathbf{i}_1 + 0\mathbf{i}_2 + ... + 0\mathbf{i}_n) + a_2(0\mathbf{i}_n + 1\mathbf{i}_2 + ... + 0\mathbf{i}_n) + ... + a_n(0\mathbf{i}_n + 0\mathbf{i}_2 + ... + 1\mathbf{i}_n)$$

Daraus ist ersichtlich, dass der Vektor $\mathbf{a}$ eine Linearkombination der Vektoren $\mathbf{i}_1, \mathbf{i}_2, ..., \mathbf{i}_n$ mit den Koeffizienten $a_1, a_2, ..., a_n$ ist. Auf diese Weise kann man jetzt die formale Summe (6) als echte Linearkombination betrachten. Die Vektoren $\mathbf{i}_1, \mathbf{i}_2, ..., \mathbf{i}_n$ bilden eine sogenannte Basis des Raumes A_n. Die genaue Bedeutung dieses Wortes wird im folgenden Paragraphen definiert werden.
Wir bemerken, dass es unendlich viele Basen gibt und dass unter diesen sich die Basis $\mathbf{i}_1, \mathbf{i}_2, ..., \mathbf{i}_n$ durch nichts besonderes auszeichnet.

2.9 Eine Basis des Raumes A_n

2.9.1 Definition einer Basis

Eine Basis des Raumes A_n ist ein System einer endlichen Anzahl von Vektoren

$$\mathbf{a}_1, \mathbf{a}_2, ..., \mathbf{a}_p \tag{1}$$

das die zwei Eigenschaften besitzt:
1) Jeder Vektor $\mathbf{a} \in A_n$ erlaubt eine Zerlegung in die Basis

$$\mathbf{a} = k_1\mathbf{a}_1 + ... + k_p\mathbf{a}_p \tag{2}$$

2) Diese Zerlegung ist eindeutig; anders ausgedrückt, wenn es neben (2) noch eine Zerlegung

$$\mathbf{a} = l_1\mathbf{a}_1 + ... + l_p\mathbf{a}_p$$

des Vektors **a** gibt, dann gilt

$$k_1 = l_1, k_2 = l_2, ..., k_p = l_p$$

Wir beweisen eine Eigenschaft jeder Basis: Vektoren, die eine Basis bilden, sind linear unabhängig.
Wir nehmen an, dass die Vektoren (1) linear abhängig sind. Definitionsgemäß bedeutet dies, dass eine bestimmte Linearkombination dieser Vektoren gleich Null ist

$$s_1\mathbf{a}_1 + s_2\mathbf{a}_2 + ... + s_p\mathbf{a}_p = \mathbf{0} \tag{3}$$

wobei unter den Zahlen $s_1, s_2, ..., s_p$ mindestens eine von Null verschieden ist. Durch Addition der Gleichungen (2) und (3) erhalten wir

$$\mathbf{a} = (k_1 + s_1)\mathbf{a}_1 + (k_2 + s_2)\mathbf{a}_2 + ... + (k_p + s_p)\mathbf{a}_p$$

d.h. eine andere Zerlegung von **a** in die Vektoren (1). Dies widerspricht aber der Definition einer Basis.

2.9.2 Eine Methode zur Gewinnung anderer Basen

Als Beispiel einer Basis mag das System

$$\mathbf{i}_1, \mathbf{i}_2, ..., \mathbf{i}_n$$

dienen, das aus den ursprünglichen Basisvektoren gebildet wurde; die Bedingungen 1) und 2) werden für sie offensichtlich erfüllt. Dies ist aber durchaus nicht die einzige Basis des Raumes A_n.
Man kann zum Beispiel aus einer beliebigen Basis viele andere mit Hilfe der folgenden Operationen erhalten:

1. Multiplikation irgendeines Vektors der Basis mit einer Zahl, die von Null verschieden ist. So erhalten wir durch Multiplikation des ersten der Vektoren (1) mit einer beliebigen Zahl $k \neq 0$ das neue System

$$k\mathbf{a}_1, \mathbf{a}_2, ..., \mathbf{a}_p \tag{1'}$$

das offensichtlich auch eine Basis darstellt.

2. Hinzufügen eines anderen Basisvektors zu einem der Basisvektoren. Zum Beispiel erhalten wir, wenn wir $\mathbf{a}_2$ zu $\mathbf{a}_1$ addieren, das neue System

$$\mathbf{a}_1 + \mathbf{a}_2, \mathbf{a}_2, ..., \mathbf{a}_p \tag{1''}$$

das auch eine Basis ist. In der Tat, es möge $\mathbf{a}$ ein beliebiger Vektor sein. Dann gilt Gleichung (2), aus der

$$\mathbf{a} = k_1(\mathbf{a}_1 + \mathbf{a}_2) + (k_2 - k_1)\mathbf{a}_2 + k_3\mathbf{a}_3 + ... + k_p\mathbf{a}_p$$

folgt, d.h. dass der Vektor $\mathbf{a}$ in die Vektoren (1") zerlegt wird.
Weiter geht aus der Eindeutigkeit der Zerlegung von $\mathbf{a}$ in die Basis (1) leicht die Eindeutigkeit der Zerlegung in (1") hervor. Folglich ist (1") wieder eine Basis des Raumes $\mathbf{A}_n$.

Es erhebt sich eine natürliche Frage: Wie findet man alle Basen des Raumes A_n?
Die Antwort müsste man aus der Sicht des Verfahrens her erwägen, das es erlaubt, aus irgendeiner Basis alle übrigen zu erhalten. In bestimmten Sinne ist eine solche Antwort im folgenden Satz enthalten, in dem unter "elementaren Umformungen" die oben definierten Operationen 1 und 2 verstanden werden. Man kann von jeder Basis mit Hilfe einer endlichen Zahl elementarer Umformungen zu jeder anderen Basis übergehen.

Wenn man insbesondere als Ausgangsbasis die Basis nimmt, die aus den ursprünglichen Basisvektoren $\mathbf{i}_1$,$\mathbf{i}_2, ..., \mathbf{i}_n$ gebildet wird, und sie allen möglichen elementaren Umformungen (in beliebiger Anzahl) unterwirft, dann erhält man alle Basen des Raumes A_n.
Den Beweis des oben formulierten Satzes führen wir nicht an (obwohl er nicht schwierig ist). Übrigens gilt unser Interesse nicht so sehr diesem Satz selbst, sondern einer Folgerung aus ihm, nämlich:

Jede Basis des Raumes A_n besteht aus n Vektoren. Tatsächlich ist in der ursprünglichen Basis $\mathbf{i}_1, \mathbf{i}_2, ..., \mathbf{i}_n$ die Zahl der Vektoren gleich n. Dann folgt aber aus dem oben Gesagten, dass auch in jeder anderen Basis die Zahl der Vektoren gleich n ist. Weiter unten wird ein unabhängiger Beweis dieses Satzes angegeben.

2.9.3 Die Anzahl der Basisvektoren

Unser nächstliegendes Ziel ist der Beweis des folgenden Satzes.

Satz 1. Jede Basis des Raumes A_n besteht aus n Vektoren.

Da die ursprüngliche Basis $\mathbf{i}_1, \mathbf{i}_2, ..., \mathbf{i}_n$ aus n Vektoren besteht, ist es für unsere Absicht hinreichend zu zeigen, dass je zwei Basen aus ein und derselben Anzahl von Vektoren bestehen. Dem Beweis dieser Tatsache stellen wir eine Bemerkung voran.

Bemerkung. Das System von Vektoren

$$\mathbf{a}_1, \mathbf{a}_2, ..., \mathbf{a}_p$$

möge derart sein, dass jeder Vektor $\mathbf{a} \in A_n$ in es zerlegt werden kann. Wir vereinbaren, ein solches System vollständig zu nennen.
Wenn wir zu einem vollständigen System als ersten Vektor irgendeinen Vektor $\mathbf{b} \neq 0$ hinzunehmen, dann erhalten wir das neue System

$$\mathbf{b}, \mathbf{a}_1, \mathbf{a}_2, ..., \mathbf{a}_p$$

das linear abhängig ist (weil aufgrund der Vollständigkeit eine Gleichung der Form

$$\mathbf{b} - k_1\mathbf{a}_1 - k_2\mathbf{a}_2 - ... - k_p\mathbf{a}_p = \mathbf{0}$$

gilt). Gemäß § 8 kann man in diesem System einen Vektor $\mathbf{a}_i$ finden, der eine Zerlegung in die ihm vorhergehenden Vektoren zulässt.
Wir verabreden, einen solchen Vektor $\mathbf{a}_i$ "überflüssig" zu nennen. Durch Streichen des "überflüssigen" Vektors erhalten wir erneut ein System von p Vektoren.

Wir zeigen, dass dieses System, das dem ursprünglichen System ähnlich ist, vollständig ist. Dies ist fast offensichtlich. Man kann einen beliebigen Vektor $\mathbf{a}$ in $\mathbf{a}_1, \mathbf{a}_2, ..., \mathbf{a}_p$ zerlegen; wenn man in dieser Zerlegung den "überflüssigen" Vektor $\mathbf{a}_i$ durch seine Zerlegung in $\mathbf{b}, \mathbf{a}_1, \mathbf{a}_2, ..., \mathbf{a}_p$ ersetzt, dann gelangt man zur Zerlegung des Vektors $\mathbf{a}$ in dem oben gezeigten System von p Vektoren. Das letztere System ist vollständig.

Der Beweis des Satzes erfolgt jetzt mit einigen Worten. Es mögen

$$\mathbf{a}_1, \mathbf{a}_2, ..., \mathbf{a}_p \qquad \text{und} \qquad \mathbf{b}_1, \mathbf{b}_2, ..., \mathbf{b}_q \tag{4,5}$$

zwei verschiedene Basen des Raumes A_n sein. Unser Ziel ist es, zu zeigen, dass $p = q$ gilt. Wir nehmen $p \neq q$ an. Aus Gründen der Eindeutigkeit nehmen wir $p < q$ an.
Wir fügen $\mathbf{b}_1$ als ersten Vektor dem System (4) zu und befreien das auf diese Weise erhaltene System von dem "überflüssigen" Vektor. Wir kommen zu dem neuen System

$$\mathbf{b}_1, \underbrace{......}_{p-1} \tag{4'}$$

das nach dem oben Bewiesenen vollständig ist. Zu dem System (4') fügen wir b_2 als ersten Vektor hinzu und befreien das auf diese Weise erhaltene System von dem "überflüssigen" Vektor. Wir kommen zum System

$$\mathbf{b}_2, \mathbf{b}_1, \underbrace{......}_{p-2}$$

das wiederum vollständig ist, usw.

Wir bemerken, dass keiner der hinzugenommenen Vektoren $\mathbf{b}_1, \mathbf{b}_2$, ... die Rolle des "überflüssigen" Vektors übernehmen kann, da diese Vektoren nach Voraussetzung derart sind, dass keiner von ihnen in die übrigen zerlegt werden kann (da (5) eine Basis ist). Auf diese Weise wird bei jedem Schritt einer der Vektoren $\mathbf{a}_1, \mathbf{a}_2, ..., \mathbf{a}_p$ gestrichen. Nach p Schritten sind alle Vektoren $\mathbf{a}_1, \mathbf{a}_2, ..., \mathbf{a}_p$ gestrichen, und wir kommen zum System

$$\mathbf{b}_p, \mathbf{b}_{p-1}, ..., \mathbf{b}_2, \mathbf{b}_1$$

das vollständig sein muss. Dies ist aber nicht möglich, weil zum Beispiel der Vektor $\mathbf{b}_{p-1}$ nicht in diesem System zerlegt werden kann.
Folglich sind wir, indem wir annehmen, dass $q > p$ ist, zu einem Widerspruch gekommen. Der Satz ist damit bewiesen.

2.9.4 Die Anzahl der Vektoren, die ein linear unabhängiges System bilden

Nach dem früher Bewiesenen müssen die Vektoren, die eine beliebige Basis bilden, linear unabhängig sein. Als triviale Folgerung erhalten wir daraus, dass im Raum A_n linear unabhängige Systeme existieren, die n Vektoren enthalten. Dann ist es aber natürlich, die Frage zu stellen:

Kann man im Raum A_n ein linear unabhängiges System aus mehr als n Vektoren aufbauen? Wir werden zeigen, dass man dies nicht kann.

Satz 2. Es möge im Raum A_n ein linear unabhängiges System von Vektoren

$$\mathbf{a}_1, \mathbf{a}_2, ..., \mathbf{a}_p$$

gegeben sein. Dann ist $p \leq n$. Wenn $p = n$ ist, dann ist das gegebene System eine Basis des Raumes A_n.

Beweis. Wir bezeichnen der Kürze halber das gegebene System mit S. Wir werden eine Basis des Raumes A_n aufbauen, indem wir zu dem System S Vektoren irgendeiner Basis

$$\mathbf{e}_1, \mathbf{e}_2, ..., \mathbf{e}_n$$

hinzufügen. Wir betrachten den Vektor $\mathbf{e}_1$.
Wenn er im System S zerlegt wird, schenken wir ihm keine Beachtung; wenn er nicht zerlegt wird, fügen wir ihn zum System S zu (als letzten Vektor).

In beiden Fällen bezeichnen wir das erhaltene System mit S' (es stimmt entweder mit S überein oder wird durch Hinzufügen des Vektors $\mathbf{e}_1$ zu S erhalten).

Danach gehen wir zum Vektor $\mathbf{e}_2$ über. Wenn er im System S' zerlegt wird, dann bleibt er unbeachtet; wenn er nicht zerlegt wird, dann fügen wir ihn zu S' hinzu. Das in beiden Fällen erhaltene System bezeichnen wir mit S'' (es stimmt entweder mit S' überein oder wird durch Hinzufügen des Vektors $\mathbf{e}_2$ zu S' erhalten). So fahren wir weiter fort.
Indem wir auf diese Weise alle Vektoren $\mathbf{e}_1, \mathbf{e}_2, ..., \mathbf{e}_n$ betrachten, erhalten wir das System $S^{(n)}$. Es besitzt folgende Eigenschaften:

1. Jeder Vektor $\mathbf{a} \in A_n$ wird in ihm zerlegt. Tatsächlich wird der Vektor $\mathbf{a}$ in $\mathbf{e}_1, \mathbf{e}_2, ..., \mathbf{e}_n$ zerlegt. Jeder dieser Vektoren wird aber seinerseits in die Vektoren des Systems $S^{(n)}$ zerlegt, wie aus dem Aufbauverfahren dieses Systems folgt.

2. Kein Vektor des Systems $S^{(n)}$ wird in vorhergehende Vektoren zerlegt (dies folgt wieder aus dem Aufbauverfahren von $S^{(n)}$), Das bedeutet, dass das System $S^{(n)}$ linear unabhängig ist.

3. Die Zerlegung eines beliebigen Vektors $\mathbf{a}$ im System $S^{(n)}$) ist eindeutig. Tatsächlich würden wir, wenn für $\mathbf{a}$ zwei verschiedene Zerlegungen existieren, durch Subtraktion der einen von der anderen eine lineare Abhängigkeit zwischen den Vektoren des Systems S erhalten.

Die Eigenschaften 1 und 3 erlauben es, den Schluss zu ziehen, dass das System $S^{(n)}$) eine Basis des Raumes A_n ist. Nach Satz 1 ist die Zahl der Vektoren in diesem System gleich n. Da das System $S^{(n)}$ die Ausgangsvektoren $\mathbf{a}_1, \mathbf{a}_2, ..., \mathbf{a}_n$ enthält, ist $p \leq n$; im Fall $p = n$ bilden die Ausgangsvektoren selbst eine Basis. Der Satz ist damit bewiesen.

2.9.5 Eine Folgerung aus Satz 2, die sich auf Algebren bezieht

Im § 7 hatten wir versprochen, einen solchen Satz zu beweisen:
Wenn eine Algebra $\mathscr{A}$ die Eigenschaft besitzt, dass aus dem Verschwinden des Produkts **ab** auch das Verschwinden mindestens eines der Faktoren **a** oder **b** folgt, dann ist $\mathscr{A}$ eine Algebra mit Division.

Zu jenem Zeitpunkt verfügten wir noch nicht über die notwendigen Mittel, um diesen Satz zu beweisen. Wir beweisen ihn jetzt.

Es möge erforderlich sein, die Gleichung

$$\mathbf{ax} = \mathbf{b} \tag{6}$$

zu lösen, wobei $\mathbf{a} \neq \mathbf{0}$ ist. Wir wählen im Vektorraum $\mathscr{A}$ irgendeine Basis

$$\mathbf{e}_1, \mathbf{e}_2, ..., \mathbf{e}_n \tag{7}$$

aus. Durch Multiplikation der Basisvektoren von links mit $\mathbf{a}$ erhalten wir n andere Vektoren

$$\mathbf{ae}_1, \mathbf{ae}_2, ..., \mathbf{ae}_n \tag{8}$$

Wir zeigen, dass diese wiederum eine Basis bilden. Gemäß Satz 2 ist es hinreichend zu zeigen, dass die Vektoren (8) linear unabhängig sind. Wir nehmen an, dass dies nicht der Fall ist. Dann existieren Zahlen $k_1, k_2, ..., k_n$, die nicht gleichzeitig Null sind, derart, dass

$$k_1\mathbf{ae}_1 + k_2\mathbf{ae}_2 + ... + k_n\mathbf{ae}_n = \mathbf{0}$$

gilt. Daraus folgt

$$\mathbf{a}(k_1\mathbf{e}_1 + k_2\mathbf{e}_2 + ... + k_n\mathbf{e}_n) = \mathbf{0}$$

Da nach Voraussetzung aus dem Verschwinden des Produktes folgt, dass einer der Faktoren Null ist, und weil in unserem Falle $\mathbf{a} \neq \mathbf{0}$ ist, haben wir

$$k_1\mathbf{e}_1 + k_2\mathbf{e}_2 + ... + k_n\mathbf{e}_n = \mathbf{0}$$

was der linearen Unabhängigkeit der Vektoren (7) widerspricht.
Also bilden die Vektoren (8) eine Basis. Wenn man den Vektor $\mathbf{b}$ in sie zerlegt, kann man schreiben

$$\mathbf{b} = s_1\mathbf{ae}_1 + s_2\mathbf{ae}_2 + ... + s_n\mathbf{ae}_n$$

oder

$$\mathbf{b} = \mathbf{a}(s_1\mathbf{e}_1 + s_2\mathbf{e}_2 + ... + s_n\mathbf{e}_n)$$

Daraus ist ersichtlich, dass das Element

$$\mathbf{x} = s_1\mathbf{e}_1 + s_2\mathbf{e}_2 + ... + s_n\mathbf{e}_n$$

eine Lösung der Gleichung (6) ist.
Diese Lösung ist eindeutig. Wenn $\mathbf{x}'$ eine andere Lösung ist, erhalten wir durch Subtraktion der Gleichung (6) von der Gleichung $\mathbf{ax}' = \mathbf{b}$

$$\mathbf{a}(\mathbf{x} - \mathbf{x}') = \mathbf{0}$$

woraus $\mathbf{x} - \mathbf{x}' = \mathbf{0}$ bzw. $\mathbf{x} = \mathbf{x}'$ folgt.

Analog werden die Existenz und die Eindeutigkeit der Lösung der Gleichung $\mathbf{xa} = \mathbf{b}$ bewiesen.

2.9.6 Die Vektorkoordinaten einer gegebenen Basis

Die letzte Frage, die wir in diesem Paragraphen berühren wollen, ist die Frage nach den Vektorkoordinaten einer gegebenen Basis des Raumes A_n.
Es möge

$$\mathbf{a}_1, \mathbf{a}_2, ..., \mathbf{a}_n$$

irgendeine Basis des Raumes A_n sein und

$$\mathbf{p} = k_1\mathbf{a}_1 + k_2\mathbf{a}_2 + ... + k_n\mathbf{a}_n$$

die Zerlegung eines beliebigen Vektors $\mathbf{p} \in A_n$ in dieser Basis. Dann werden die Zahlen $k_1, k_2, ..., k_n$ die Koordinaten des Vektors $\mathbf{p}$ in Bezug auf die gegebene Basis genannt. Die Gleichung

$$(k_1\mathbf{a}_1 + k_2\mathbf{a}_2 + ... + k_n\mathbf{a}_n) + (l_1\mathbf{a}_1 + l_2\mathbf{a}_2 + ... + l_n\mathbf{a}_n)(k_1 + l_1)\mathbf{a}_1 + (k_2 + l_2)\mathbf{a}_2 + ... + (k_n + l_n)\mathbf{a}_n$$

die aus den Eigenschaften der Vektoraddition und der Multiplikation eines Vektors mit einer Zahl hervorgeht, zeigt, dass bei der Vektoraddition die entsprechenden Koordinaten addiert werden (die erste mit der ersten, die zweite mit der zweiten usw.). Analog zeigt die Gleichung

$$k(k_1\mathbf{a}_1 + k_2\mathbf{a}_2 + ... + k_n\mathbf{a}_n) = kk_1\mathbf{a}_1 + kk_2\mathbf{a}_2 + ... + kk_n\mathbf{a}_n)$$

dass bei der Multiplikation eines Vektors $\mathbf{p}$ mit der Zahl k alle seine Koordinaten mit dieser Zahl multipliziert werden. Auf diese Weise bleiben in jeder Basis $\mathbf{a}_1, \mathbf{a}_2, ..., \mathbf{a}_n$ die Regeln der Vektoraddition und der Multiplikation eines Vektors mit einer Zahl genau dieselben wie in der Ausgangsbasis $\mathbf{i}_1, \mathbf{i}_2, ..., \mathbf{i}_n$.

2.10 Teilräume

Wir gehen kurz auf die Frage nach den Teilräumen des Raumes A_n ein. So werden die Mengen von Vektoren genannt, die einige spezifische Eigenschaften besitzen. Dank dieser Eigenschaften kann man jede dieser Mengen als selbständigen Raum A_n betrachten, wobei $p \leq n$ ist.

2.10.1 Definition eines Teilraumes

Es möge P eine bestimmte Menge von Vektoren aus A_n sein. Wir vereinbaren, diese Menge Teilraum des Raumes A_n zu nennen, wenn sie die folgenden Eigenschaften besitzt:

1) Aus $\mathbf{a} \in P$ und $\mathbf{b} \in P$ folgt $\mathbf{a} + \mathbf{b} \in P$;
2) Aus $\mathbf{a} \in P$ folgt $k\mathbf{a} \in P$, wobei k eine beliebige reelle Zahl ist.

Anders ausgedrückt ist ein Teilraum eine Menge von Vektoren, die zusammen mit beliebigen ihrer Vektoren $\mathbf{a}, \mathbf{b}, \mathbf{c}, ...$ auch alle Linearkombinationen $k\mathbf{a} + l\mathbf{b} + s\mathbf{c}...$ aus ihnen enthält.

Ein triviales Beispiel eines Teilraumes ist die Menge, die lediglich aus dem Nullvektor besteht. Dies ist der sogenannte Nullteilraum. Ein anderes triviales Beispiel ist der ganze Raum A_n. Jedoch gibt es außer diesen beiden Extremfällen auch noch andere Teilräume. Im folgenden Punkt zeigen wir, wie man einen beliebigen Teilraum des Raumes A_n aufbaut.

2.10.2 Der Teilraum als selbständiger Vektorraum

Wir setzen voraus, dass der Teilraum P verschieden vom Nullteilraum ist. Wir zeigen, dass man dann in P ein System von Vektoren auswählen kann, das eine Basis bildet.

Wir nehmen irgendeinen Vektor $\mathbf{a}_1 \in P$, der von Null verschieden ist. Wenn alle Vektoren aus P in $\mathbf{a}_1$ zerlegt werden, bleiben wir bei diesem. Wenn es in P noch Vektoren gibt, die nicht in $\mathbf{a}_1$ zerlegt werden, dann wählen wir einen Vektor $\mathbf{a}_1$ von ihnen aus und fügen ihn zu $\mathbf{a}_1$ hinzu. Wenn alle Vektoren aus P in $\mathbf{a}_1, \mathbf{a}_2$ zerlegt werden, bleiben wir bei diesen. Wenn es in P noch Vektoren gibt, die nicht in $\mathbf{a}_1, \mathbf{a}_2$ zerlegt werden können, wählen wir einen Vektor $\mathbf{a}_3$ von ihnen aus und fügen ihn zu $\mathbf{a}_1, \mathbf{a}_2$ hinzu usw. Indem wir diesen Prozess fortsetzen, bauen wir nacheinander die Vektoren

$$\mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_3$$

auf, wobei keiner von ihnen in die vorhergehenden zerlegt werden kann. Auf diese Weise erhalten wir bei jedem Schritt ein linear unabhängiges System von Vektoren. Aufgrund des Satzes 2 im vorhergehenden Paragraphen ist dieser Prozess nach höchstens n Schritten abgeschlossen. Wir erhalten dann das linear unabhängige System von Vektoren

$$\mathbf{a}_1, \mathbf{a}_2, ..., \mathbf{a}_p \qquad (p \leq n) \tag{1}$$

das dem Teilraum P angehört, und derart ist, dass:

1) für jeden Vektor aus P eine Zerlegung in ihm möglich ist;
2) diese Zerlegung eindeutig ist.

In der Tat würden wir, wenn für den Vektor $\mathbf{a}$ zwei verschiedene Zerlegungen existieren würden, durch Subtraktion der einen von der anderen zu dem Resultat kommen, dass eine bestimmte Linearkombination

$$s_1\mathbf{a}_1 + s_2\mathbf{a}_2 + ... + s_p\mathbf{a}_p$$

gleich Null ist, wobei mindestens einer der Koeffizienten $s_1, s_2, ..., s_p$ von Null verschieden ist; dies würde die lineare Abhängigkeit des Systems (1) bedeuten.
Folglich besteht der von uns betrachtet Teilraum P aus allen möglichen Vektoren der Form

$$k_1\mathbf{a}_1 + k_2\mathbf{a}_2 + ... + k_p\mathbf{a}_p$$

wobei die Darstellung eines beliebigen Vektors $\mathbf{a} \in P$ in solcher Form eindeutig ist. Dies erlaubt es uns, den Teilraum P als selbständigen p-dimensionalen Vektorraum A_n mit den ursprünglichen Basisvektoren $\mathbf{a}_1, \mathbf{a}_2, ..., \mathbf{a}_p$ zu betrachten. Es ist natürlich offensichtlich, dass in diesem Raum die früher bewiesenen Sätze gelten, insbesondere besteht jede Basis in ihm aus p Vektoren.

Die Zahl p wird Dimension des Teilraumes P genannt. Wie wir sahen, übertrifft sie n nicht; in dem Falle $p = n$ wird das System (1) zu einer Basis des ganzen Raumes A_n (siehe wiederum Satz 2 des vorhergehenden Paragraphen), und folglich stimmt P mit A_n überein.

Aus dem oben Gesagten geht eine offensichtliche Folgerung hervor, die wir besonders betonen wollen:
Jeder Teilraum P stimmt mit der Menge aller Linearkombinationen bestimmter p Vektoren $\mathbf{a}_1, \mathbf{a}_2, ..., \mathbf{a}_n$ überein.

2.10.3 Beispiele

Wir erläutern den Begriff des Teilraumes für den Fall eines dreidimensionalen Vektorraumes A_3. Es möge P ein Teilraum in A_3 sein, der nicht Nullteilraum ist. Eine Basis von P besteht aus nicht mehr als drei Vektoren, d.h., sie besitzt eine der Formen:

$$\mathbf{a}_1; \quad \mathbf{a}_1, \mathbf{a}_2; \quad \mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_3$$

Im ersten Fall besteht P aus allen Vektoren der Form $k\mathbf{a}_1$, d.h. aus allen Vektoren, die zu a_1 proportional sind (Abb. 11).

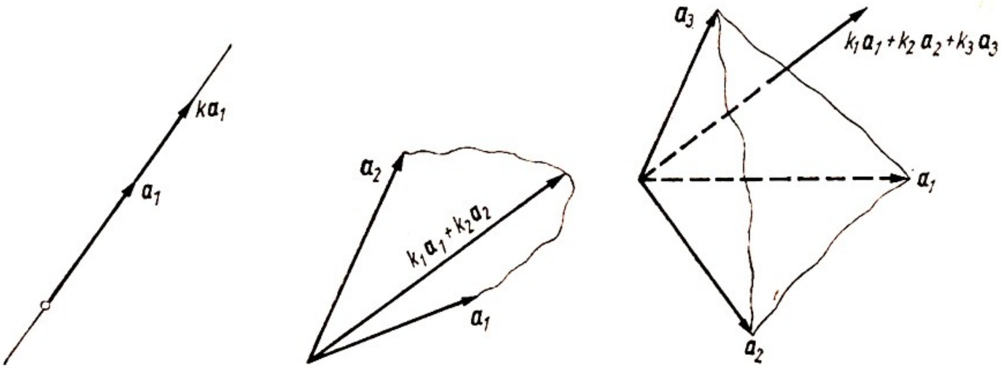


Abb.11, 12, 13

Im zweiten Fall ist P die Menge aller Vektoren der Form $k_1\mathbf{a}_1 + k_2\mathbf{a}_2$ folglich besteht P aus allen Vektoren, die in der gleichen Ebene wie auch $\mathbf{a}_1, \mathbf{a}_2$ liegen (Abb. 12).
Im dritten Falle ist P die Menge aller Vektoren der Form $k_1\mathbf{a}_1 + k_2\mathbf{a}_2 + k_3\mathbf{a}_3$, d.h. überhaupt aller Vektoren des Raumes A_n (Abb. 13).

2.11 Lemma über ein homogenes Gleichungssystem

Dieser Paragraph dient nur einem Hilfszweck. Wir schweifen für kurze Zeit von den Vektoren ab und wenden uns einem Gegenstand zu, der, wie es scheint, keine direkte Beziehung zu ihnen hat, den Systemen linearer Gleichungen.
Im Grunde genommen wird nur die Rede von den homogenen Gleichungen sein, genauer noch, von einem Lemma, das sich auf Systeme solcher Gleichungen bezieht. Im weiteren wird uns der Verweis auf dieses Lemma helfen, wichtige Sätze aufzustellen.

Wie bekannt ist, wird eine lineare Gleichung homogen genannt, wenn ihr absolutes Glied gleich Null ist. Etwas abweichend von der Schreibweise, wie sie in der elementaren Algebra eingeführt wurde, werden wir die Unbekannten in den Gleichungen mit ein und demselben Buchstaben x bezeichnen, jedoch mit verschiedenen Indizes: x_1 ist die erste Unbekannte, x_2 die zweite usw. Dann wird eine lineare homogene Gleichung mit n Unbekannten in der Form

$$a_1x_1 + a_2x_2 + ... + a_nx_n = 0$$

geschrieben.
Ein System, das aus homogenen Gleichungen besteht, wird selbst homogen genannt. In allgemeiner Form wird ein homogenes System aus m Gleichungen mit n Unbekannten in folgender

Weise geschrieben:

$$\begin{aligned} a_1x_1 + a_2x_2 + ... + a_nx_n &= 0 \qquad \text{1. Gleichung} \\ b_1x_1 + b_2x_2 + ... + b_nx_n &= 0 \qquad \text{2. Gleichung} \\ &... \\ d_1x_1 + d_2x_2 + ... + d_nx_n &= 0 \qquad \text{m. Gleichung} \end{aligned} \tag{1}$$

Wenn wir

$$x_1 = 0, x_2 = 0, ..., x_n = 0$$

annehmen, erhalten wir offensichtlich eine Lösung des homogenen Systems. Sie wird die triviale Lösung genannt. In vielen Fällen ist es wichtig zu wissen, ob ein gegebenes homogenes System auch noch eine nichttriviale Lösung besitzt. Das folgende Lemma gibt eine Teilantwort auf diese Frage.

Lemma. Ein homogenes System, in dem die Anzahl der Gleichungen kleiner als die Anzahl der Unbekannten ist, besitzt immer eine nichttriviale Lösung.

Den Beweis werden wir durch vollständige Induktion über m, der Anzahl der Gleichungen im System (1), führen. Wenn $m = 1$ ist, dann ist nur eine Gleichung gegeben, während die Anzahl der Unbekannten größer als 1 ist.
Es ist klar, dass diese Gleichung unbedingt eine nichttriviale Lösung besitzt. Wir nehmen an, dass die Behauptung des Satzes für Systeme, die aus $m - 1$ Gleichungen bestehen, richtig ist und beweisen dann, dass sie für Systeme von m Gleichungen richtig bleibt.

Es möge also das System (1) gegeben sein, in dem die Anzahl m der Gleichungen kleiner als die Anzahl n der Unbekannten ist. Wenn alle Zahlen $a_1, b_1, ..., d_1$ die Koeffizienten von x_1, gleich 0 sind, dann besitzt das System zweifellos eine nichttriviale Lösung; zum Beispiel kann man

$$x_1 = 0, x_2 = 0, ..., x_n = 0$$

nehmen. Wir nehmen jetzt an, dass es unter den gegebenen Koeffizienten von Null verschiedene gibt. Gegebenenfalls durch das Vertauschen der Plätze der ersten Gleichung mit einer der nachfolgenden kann man annehmen, dass $a_1 \neq 0$ ist. Wir nehmen an dem System folgende Umformungen vor.

Wir fügen die erste Gleichung, die mit $-b_1/a_1$ multipliziert wurde, zur zweiten Gleichung hinzu. Man erhält ein neues System, das offensichtlich mit dem Ausgangssystem gleichwertig ist. Die zweite Gleichung in ihm wird die Form

$$b'_2x_2 + ... + b'_nx_n = 0$$

haben (ein Glied mit x_1 kommt nicht vor). Weiter nehmen wir analoge Umformungen mit der dritten, vierten usw. (bis zur m-ten) Gleichung des Systems vor. Zu jeder von ihnen fügen wir das entsprechende Vielfache der ersten Gleichung hinzu. Als Ergebnis erhält man das System

$$\begin{aligned} a_1x_1 + a_2x_2 + ... + a_nx_n &= 0 \qquad \text{1. Gleichung} \\ b'_2x_2 + ... + b'_nx_n &= 0 \qquad \text{2. Gleichung} \\ &... \\ d'_2x_2 + ... + d'_nx_n &= 0 \qquad \text{m. Gleichung} \end{aligned} \tag{1'}$$

das mit dem Ausgangssystem gleichwertig ist. Der Teil dieses Systems (ohne die erste Gleichung) stellt ein homogenes System von $m-1$ Gleichungen mit $n-1$ Unbekannten dar. Weil $m < n$ ist, gilt

$$m-1 < n-1$$

Folglich ist in diesem System die Anzahl der Gleichungen kleiner als die Anzahl der Unbekannten. Für ein System aber, das aus $m-1$ Gleichungen besteht, ist die Behauptung des Lemmas infolge der Induktionsannahme richtig. Damit besitzt das eingerahmte System eine nichttriviale Lösung

$$x_2 = \alpha_2, x_3 = \alpha_3, ..., x_n = \alpha_n$$

Wenn wir den Wert x_1 hinzufügen, den man aus der ersten Gleichung des Systems (1') erhalten kann:

$$x_1 = -\frac{1}{a_1}(a_2\alpha_2 + ... + a_n\alpha_n)$$

dann erhalten wir eine nichttriviale Lösung des ganzen Systems (1'), folglich auch des Ausgangssystems (1). Das Lemma ist bewiesen.

2.12 Das Skalarprodukt

Allen Begriffen, die wir bis jetzt in diesem Kapitel untersucht haben, liegen zwei Operationen über Vektoren zugrunde: die Vektoraddition und die Multiplikation eines Vektors mit einer Zahl. Indessen ist, wenn wir die gewöhnlichen geometrischen Vektoren[13] im Auge haben, der Kreis der Begriffe, die mit ihnen verbunden sind, bedeutend größer.

Zum Beispiel besitzt jeder Vektor eine Länge, existieren senkrecht aufeinanderstehende Vektoren usw. Deshalb wird man naturgemäß versuchen, für den n-dimensionalen Fall eine vernünftige Methode zur Einführung solcher Begriffe wie Länge, das aufeinander Senkrechtstehen u.ä.m. zu finden. Das wird weiter unten getan werden.

2.12.1 Das Skalarprodukt gewöhnlicher geometrischer Vektoren

Es mögen in der Ebene zwei Vektoren **x** und **y** gegeben sein, die vom Ursprung 0 eines rechtwinkligen Koordinatensystems ausgehen. Die Koordinaten des ersten Vektors mögen x_1, x_2 die des zweiten y_1, y_2 sein. Also ist

$$\mathbf{x} = x_1\mathbf{i}_1 + x_2\mathbf{i}_2 \qquad , \qquad \mathbf{y} = y_1\mathbf{i}_1 + y_2\mathbf{i}_2$$

$\mathbf{i}_1$ und $\mathbf{i}_2$ Vektoren der Länge 1 sind, die die Richtung der Koordinatenachsen haben (Abb. 14).

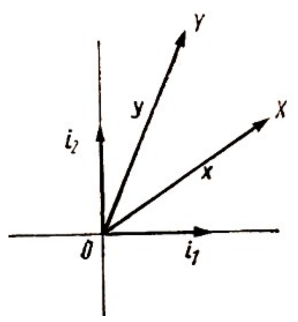


Abb.14

[13] Das heißt, gerichtete Strecken in der Ebene oder im Raum.

Wir bezeichnen die Spitzen der gegebenen Vektoren entsprechend mit X und Y. Der Punkt X hat die Koordinaten x_1, x_2, der Punkt Y hat die Koordinaten y_1, y_2. Aus der Formel für den Abstand zwischen zwei Punkten erhalten wir

$$(XY)^2 = (y_1 - x_1)^2 + (y_2 - x_2)^2, \qquad (OX)^2 = x_1^2 + x_2^2, \qquad (OY)^2 = y_1^2 + y_2^2$$

woraus

$$(OX)^2 + (OY)^2 - (XY)^2 = 2(x_1y_1 + x_2y_2) \tag{1}$$

folgt. Aus dieser Gleichung ist leicht zu ersehen (wenn man den Satz des Pythagoras berücksichtigt), dass eine notwendige und hinreichende Bedingung für das aufeinander Senkrechtstehen von **x** und **y**

$$x_1y_1 + x_2y_2 = 0$$

ist: Wir bemerken, wenn wir diese Überlegung nicht nur auf Vektoren einer Ebene, sondern im Raum anwenden, dann erhalten wir die Bedingung für das aufeinander Senkrechtstehen in analoger Form:

$$x_1y_1 + x_2y_2 + x_3y_3 = 0$$

Die Formel (1) bringt uns auf den Gedanken, mit jedem Vektorpaar **x** und **y** in der Ebene die Zahl

$$x_1y_1 + x_2y_2 \tag{2}$$

zu verbinden und im Raum die Zahl

$$x_1y_1 + x_2y_2 + x_3y_3 \tag{2'}$$

Diese Zahl nennt man in der Geometrie Skalarprodukt der Vektoren **x** und **y** und bezeichnet sie mit $(\mathbf{x}, \mathbf{y})$.
Wir bemerken, dass die Länge eines beliebigen Vektors **x** durch das Skalarprodukt ausgedrückt wird. Im Falle der Ebene ist nämlich

$$|\mathbf{x}| = \sqrt{x_1^2 + x_2^2}$$

im Falle des Raumes

$$|\mathbf{x}| = \sqrt{x_1^2 + x_2^2 + x_3^2}$$

so dass in beiden Fällen die Formel

$$|\mathbf{x}| = \sqrt{(\mathbf{x},\mathbf{x})}$$

gilt.

2.12.2 Eine allgemeinere Definition des Skalarproduktes

Das oben betrachtete Skalarprodukt von Vektoren in der Ebene und im Raum besitzt eine Reihe einfacher Eigenschaften. Hier sind einige davon:

1) $(\mathbf{x},\mathbf{x}) > 0$, wobei $(\mathbf{x}, \mathbf{x}) = 0$ nur für $\mathbf{x} = \mathbf{0}$ gilt;
2) $(\mathbf{x},\mathbf{y}) = (\mathbf{y},\mathbf{x})$;
3) $(\mathbf{x}, k\mathbf{y}) = k(\mathbf{x}, \mathbf{y})$; wobei k eine beliebige reelle Zahl ist;
4) $(\mathbf{x},\mathbf{y} + \mathbf{z}) = (\mathbf{x},\mathbf{y}) + (\mathbf{x},\mathbf{z})$.

Die ersten drei Eigenschaften gehen direkt aus der Definition des Skalarproduktes hervor. Der

Beweis der letzten Eigenschaft ist ein wenig komplizierter. Wir führen ihn für den Fall des Raumes an:

$$\begin{aligned}(\mathbf{x},\mathbf{y}+\mathbf{z}) &= x_1(y_1+z_1)+x_2(y_2+z_2)+x_3(y_3+z_3)\\ &= (x_1y_1+x_2y_2+x_3y_3)+(x_1z_1+x_2z_2+x_3z_3)=(\mathbf{x},\mathbf{y})+(\mathbf{x},\mathbf{z})\end{aligned}$$

Wir kommen jetzt zum zentralen Punkt in diesem Paragraphen.

Bei einer beliebigen Verallgemeinerung des Begriffs des Skalarproduktes auf den n-dimensionalen Fall wäre es wünschenswert, dass die Eigenschaften 1)-4) Geltung behielten. In Anbetracht dessen verwenden wir die folgende Definition.

Definition. Wir sagen, dass im n-dimensionalen Vektorraum A_n ein Skalarprodukt erklärt ist, wenn je zwei Vektoren **x** und **y** eine bestimmte Zahl, die wir mit $(\mathbf{x},\mathbf{y})$ bezeichnen, so zugeordnet ist, dass die Eigenschaften 1)-4) erfüllt sind. Die Zahl $(\mathbf{x},\mathbf{y})$ werden wir Skalarprodukt des Vektors **x** mit dem Vektor **y** nennen.

2.12.3 Eine Methode zur Einführung des Skalarproduktes

Die angegebene Definition lässt eine Frage offen: Kann man nur auf eine Weise das Skalarprodukt im Raum A_n einführen?
Die Antwort darauf deuten bereits die Ausdrücke (2) und (2') an.

Und zwar wählen wir im Raum A_n irgendeine Basis

$$\mathbf{a}_1, \mathbf{a}_2, ..., \mathbf{a}_n$$

aus und ordnen je zwei Vektoren **x** und **y** die Zahl

$$(\mathbf{x},\mathbf{y}) = x_1y_1 + x_2y_2 + ... + x_ny_n \tag{3}$$

zu; hierbei sind $x_1, x_2, ..., x_n$ die Koordinaten des Vektors **x** und $y_1, y_2, ..., y_n$ die Koordinaten des Vektors **y** in der ausgewählten Basis, d.h.,

$$\mathbf{x} = x_1\mathbf{a}_1 + x_2\mathbf{a}_2 + ... + x_n\mathbf{a}_n \quad , \quad \mathbf{y} = y_1\mathbf{a}_1 + y_2\mathbf{a}_2 + ... + y_n\mathbf{a}_n$$

Wie nicht schwer zu zeigen ist, werden dann alle Eigenschaften 1)-4) erfüllt, und folglich ist $(\mathbf{x},\mathbf{y})$ das Skalarprodukt. Wenn man eine andere Basis

$$\mathbf{a}'_1, \mathbf{a}'_2, ..., \mathbf{a}'_n$$

auswählt und den Vektoren **x** und **y** die Zahl

$$(\mathbf{x},\mathbf{y})' = x'_1y'_1 + x'_2y'_2 + ... + x'_ny'_n$$

zuordnet (wobei $x'_1, x'_2, ..., x'_n$ und $y'_1, y'_2, ..., y'_n$ die Koordinaten der Vektoren **x** und **y** in der neuen Basis sind), dann wird im allgemeinen die Gleichung

$$(\mathbf{x},\mathbf{y}) = (\mathbf{x},\mathbf{y})'$$

nicht erfüllt. Daraus wird klar, dass man im Raum A_n viele verschiedene Skalarprodukte einführen kann.
Im weiteren wird gezeigt werden, dass die obige Methode der Einführung des Skalarproduktes allgemein ist, denn wie auch das Skalarprodukt im Raum gewählt wird, man wird stets eine solche Basis (und sogar nicht nur eine) finden, in der Formel (3) gilt.

2.12.4 Die Länge eines Vektors, orthogonale Vektoren

Nachdem die Definition des Skalarproduktes angegeben wurde, werden solche Begriffe wie die Länge eines Vektors und das aufeinander Senkrechtstehen zweier Vektoren in Analogie zu den zweidimensionalen und dreidimensionalen Fällen eingeführt.
Und zwar definieren wir die Länge oder Norm eines n-dimensionalen Vektors **x** durch die Formel

$$|\mathbf{x}| = \sqrt{(\mathbf{x}, \mathbf{x})}$$

(die Zahl, die unter dem Wurzelzeichen steht, ist aufgrund von Eigenschaft 1) des Skalarproduktes nicht negativ); senkrecht aufeinanderstehend oder orthogonal nennen wir die Vektoren **x** und **y**, deren Skalarprodukt gleich Null ist. In diesem Fall schreiben wir

$$\mathbf{x} \perp \mathbf{y}$$

Also bedeutet $\mathbf{x} \perp \mathbf{y}$, dass $(\mathbf{x}, \mathbf{y}) = 0$ gilt.

2.12.5 Ein Ausdruck für das Skalarprodukt in Vektorkoordinaten

Wir kehren jetzt zur Definition des Skalarproduktes zurück und ziehen aus den grundlegenden Eigenschaften 1)-4) einfachste Schlussfolgerungen. Vor allem werden wir feststellen, dass die folgenden zwei Eigenschaften, die 3) und 4) ergänzen, gelten:

3') $(k\mathbf{x}, \mathbf{y}) = k(\mathbf{x}, \mathbf{y})$;
4') $(\mathbf{x} + \mathbf{y},\mathbf{z}) = (\mathbf{x},\mathbf{z}) + (\mathbf{y},\mathbf{z})$.

Die Eigenschaft 3') ergibt sich aus der Kette der Gleichungen

$$(k\mathbf{x}, \mathbf{y}) = (\mathbf{y},k\mathbf{x}) = k(\mathbf{y},\mathbf{x}) = k(\mathbf{x},\mathbf{y})$$

von denen in jeder eine der Eigenschaften des Skalarproduktes benutzt wurde. Analog wird die Eigenschaft 4') bewiesen:

$$(\mathbf{x} + \mathbf{y},\mathbf{z}) = (\mathbf{z},\mathbf{x} + \mathbf{y}) = (\mathbf{z},\mathbf{x}) + (\mathbf{z},\mathbf{y}) = (\mathbf{x},\mathbf{z}) + (\mathbf{y},\mathbf{z})$$

Durch Kombination der Eigenschaften 3) und 3') erhalten wir

3") $(k\mathbf{x}, l\mathbf{y}) = kl(\mathbf{x}, \mathbf{y})$

Weiter folgt sofort aus 4) und 4'), dass

$$(\mathbf{x}_1 + \mathbf{x}_2 + ... + \mathbf{x}_p, \mathbf{y}_1 + \mathbf{y}_2 + ... + \mathbf{y}_p) = \sum_{i,j}(\mathbf{x}_i,\mathbf{y}_i)$$

gilt, d.h., die skalare Multiplikation einer Summe mit einer Summe ist der üblichen Regel unterworfen: Man muss jeden Summanden der ersten Summe mit jedem Summanden der zweiten Summe multiplizieren und die Resultate addieren. Daraus sowie auch aus der Eigenschaft 3') erhält man auch die Regel für die Multiplikation einer Linearkombination mit einer anderen:

$$(k_1\mathbf{x}_1 + k_2\mathbf{x}_2 + ... + k_p\mathbf{x}_p, l_1\mathbf{y}_1 + l_2\mathbf{y}_2 + ... + l_p\mathbf{y}_p) = \sum_{i,j} k_i l_j(\mathbf{x}_i,\mathbf{y}_i) \tag{4}$$

Aus dieser Formel erhalten wir sogleich den Ausdruck des Skalarproduktes $(\mathbf{x}, \mathbf{y})$ in den Vektorkoordinaten von **x** und **y**. Es möge eine bestimmte Basis

$$a_1, a_2, ..., a_n \tag{5}$$

im Raum A_n ausgewählt sein. Wir betrachten zwei beliebige Vektoren **x** und **y**. Wenn wir sie in der Basis (5) zerlegen, erhalten wir

$$\mathbf{x} = x_1\mathbf{a}_1 + x_2\mathbf{a}_2 + ... + x_n\mathbf{a}_n \qquad , \qquad \mathbf{y} = y_1\mathbf{a}_1 + y_2\mathbf{a}_2 + ... + y_n\mathbf{a}_n$$

Jetzt kann man zur Berechnung des Skalarproduktes $(\mathbf{x},\mathbf{y})$ die Formel (4) benutzen:

$$(\mathbf{x},\mathbf{y}) = \sum_{i,j} x_i y_j (\mathbf{a}_i,\mathbf{a}_j)$$

Die Größen

$$g_{ij} = (\mathbf{a}_i,\mathbf{a}_j)$$

sind konstante Zahlen, die nur von der ausgewählten Basis abhängen. Auf diese Weise erhält man, wenn eine bestimmte Basis festgelegt wurde, für das Skalarprodukt den Ausdruck

$$(x,y) = \sum_{i,j} g_{ij} x_i y_j \tag{6}$$

Dies ist ein sehr nützliches Resultat; mit seiner Hilfe können wir sofort eine Reihe wichtiger Sätze beweisen.

2.12.6 Die Existenz eines Vektors, der zu p gegebenen Vektoren orthogonal ist ($p < n$)

Wir nehmen an, dass wir den Vektor **y** festgelegt haben und den Vektor **x** so auswählen wollen, dass er **y** gegenüber orthogonal ist, d.h., dass $(\mathbf{x},\mathbf{y}) = 0$ sein möge.
Dann erhält man zur Bestimmung von $x_1, x_2, ..., x_n$ der Koordinaten des unbekannten Vektors **x**, aufgrund von (6) die Gleichung

$$\sum_{i,j} g_{ij} x_i y_j = 0$$

Da g_{ij} und y_j gegebene konstante Zahlen sind, nimmt die linke Seite der Gleichung nach dem Ordnen der Glieder die Form

$$a_1x_1 + a_2x_2 + ... + a_nx_n$$

an; folglich ist die erhaltene Gleichung linear und homogen in Bezug auf die Unbekannten $x_1, x_2, ..., x_n$.

Wenn der Vektor **x** nicht nur zu einem Vektor **y** orthogonal sein soll, sondern zu verschiedenen Vektoren

$$\mathbf{y}_1, \mathbf{y}_2, ..., \mathbf{y}_p$$

dann erhält man zur Bestimmung seiner Koordinaten nicht nur eine Gleichung, sondern ein System von p Gleichungen. Nach dem Lemma aus § 11 besitzt ein solches System sicher eine nichttriviale Lösung, wenn die Anzahl der Gleichungen kleiner ist als die Anzahl der Unbekannten. Daraus geht der folgende Satz hervor.

Satz. Wenn im Raum A_n die Vektoren

$$\mathbf{y}_1, \mathbf{y}_2, ..., \mathbf{y}_p$$

gegeben sind, wobei die Anzahl dieser Vektoren kleiner als n ist, dann existiert ein vom Nullvektor verschiedener Vektor derart, dass dieser Vektor zu jedem der gegebenen Vektoren orthogonal ist.[14]

[14] Der Nebensatz "der nicht der Nullvektor ist" in der Formulierung des Satzes ist wesentlich, da der Nullvektor jedem anderen Vektor **y** gegenüber orthogonal ist. Dies folgt aus der Gleichung $(\mathbf{0},\mathbf{y}) = (0\mathbf{y},\mathbf{y}) = 0(\mathbf{y},\mathbf{y}) = 0$.

Dieser Satz schließt zahlreiche Folgerungen ein. Wir werden hier nur eine davon betrachten; im weiteren spielt sie eine wichtige Rolle.

Folgerung. Wenn der Teilraum P des Raumes A_n nicht mit dem ganzen Raum A_n übereinstimmt, dann existiert ein Vektor $\mathbf{x} \in A_n$ mit $x \neq 0$, derart, dass dieser Vektor zu jedem Vektor aus P orthogonal ist (oder, wie wir kürzer sagen werden, der zum ganzen Teilraum P orthogonal ist).

Der Beweis ist fast offensichtlich. Wir wählen in P eine Basis aus den Vektoren

$$\mathbf{y}_1, \mathbf{y}_2, ..., \mathbf{y}_p$$

Da P nicht mit A_n übereinstimmt, ist $p < n$. Nach dem Bewiesenen findet man einen Vektor $\mathbf{x} \neq 0$, der zu jedem der Vektoren $\mathbf{y}_1, \mathbf{y}_2, ..., \mathbf{y}_p$ orthogonal ist. Dann ist $\mathbf{x}$ aber auch zu jeder Linearkombination dieser Vektoren orthogonal:

$$(\mathbf{x}, k_1\mathbf{y}_1 + k_2\mathbf{y}_2 + ... + k_p\mathbf{y}_p) = k_1(\mathbf{x},\mathbf{y}_1) + k_2(\mathbf{x},\mathbf{y}_2) + ... + k_p(\mathbf{x},\mathbf{y}_p) = 0$$

Folglich ist $\mathbf{x}$ zu jedem Vektor aus P orthogonal.

2.12.7 Zerlegung eines Vektors in zwei zueinander orthogonale Komponenten

Wir schließen diesen Paragraphen mit einer Behauptung ab, die in zweidimensionalen und dreidimensionalen Fällen eine geometrisch offensichtliche Tatsache ausdrückt; hier wird sie für einen Raum beliebiger Dimension bewiesen werden.

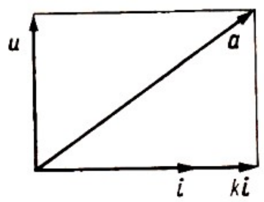


Abb.15

Es möge $\mathbf{i}$ irgendein Vektor sein, der vom Nullvektor verschieden ist. Dann kann man jeden Vektor $\mathbf{a}$ in zwei Summanden zerlegen, von denen einer $\mathbf{i}$ proportional ist, der andere aber orthogonal zu $\mathbf{i}$ (Abb. 15) ist:

$$\mathbf{a} = k\mathbf{i} + \mathbf{u} \qquad \text{mit} \quad \mathbf{u} \neq \mathbf{i}$$

Um diese Behauptung zu beweisen, ist es notwendig zu überprüfen, dass eine Zahl k existiert, für die der Vektor $\mathbf{a} - k\mathbf{i}$ orthogonal zu $\mathbf{i}$ ist. Dann erhalten wir, wobei wir diesen Vektor mit $\mathbf{u}$ bezeichnen, die verlangte Zerlegung für $\mathbf{a}$. Es ist also notwendig, dass

$$(\mathbf{a} - k\mathbf{i},\mathbf{i}) = 0$$

ist, oder, was das gleiche bedeutet,

$$(\mathbf{a},\mathbf{i}) = k(\mathbf{i}, \mathbf{i})$$

Daraus finden wir sofort die gesuchte Zahl k:

$$k = \frac{(\mathbf{a},\mathbf{i})}{(\mathbf{i},\mathbf{i})}$$

(man muss berücksichtigen; dass $(\mathbf{i}, \mathbf{i}) \neq 0$ gilt, weil der Vektor $\mathbf{i}$ nicht der Nullvektor ist).

2.13 Die orthonormierte Basis. Orthogonale Transformationen

2.13.1 Definition einer orthonormierten Basis

Wir wissen bereits, dass im Raum A_n eine unendliche Menge von Basen existiert. Bis zur Einführung des Skalarproduktes in A_n gab es keinen Grund für uns, irgendwelche davon besonders hervorzuheben.
Von dem Moment an jedoch, in dem das Skalarprodukt auftritt, beginnen einige Basen eine privilegierte Rolle zu spielen. Dies sind die sogenannten orthonormierten Basen.

Eine Basis

$$\mathbf{a}_1, \mathbf{a}_2, ..., \mathbf{a}_n$$

wird orthonormiert genannt, wenn je zwei Basisvektoren zueinander orthogonal sind

$$(\mathbf{a}_i,\mathbf{a}_j) = 0 \qquad (i,j = 1,..,n; i \neq j) \tag{1}$$

und die Länge jedes Basisvektors gleich 1 ist

$$(a_i, a_i) = 1 \qquad (i = 1,...,n) \tag{2}$$

Im gewöhnlichen dreidimensionalen Raum ist eine orthonormierte Basis ein beliebiges Tripel paarweise senkrecht aufeinanderstehender Einheitsvektoren (Abb. 16).

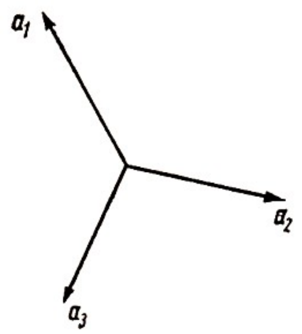


Abb.16

Wir bemerken, dass das Wort "orthonormiert" aus der Zusammenziehung der Worte "orthogonal" und "normiert" entstanden ist. Der Vektor **a** wird normiert oder Einheitsvektor genannt, wenn seine Länge gleich 1 ist.

Eine orthonormierte Basis ist deshalb bemerkenswert, weil man in ihr einen besonders einfachen Ausdruck für das Skalarprodukt erhält. Wir benutzen die im vorhergehenden Paragraphen bewiesene Formel

$$(\mathbf{x},\mathbf{y}) = \sum_{i,j} x_i y_j (\mathbf{a}_i,\mathbf{a}_j)$$

Wenn man berücksichtigt, dass die Basis orthonormiert ist, d.h., dass die Gleichungen (1) und (2) gelten, erhält man sofort

$$(x,y) = x_1y_1 + x_2y_2 + ... + x_ny_n \tag{3}$$

Auf diese Weise ist in einer orthonormierten Basis das Skalarprodukt gleich der Summe der Produkte gleichnamiger Koordinaten (der ersten mit der ersten, der zweiten mit der zweiten usw.).

2.13.2 Die Existenz orthonormierter Basen

Obwohl wir eine wichtige Eigenschaft einer orthonormierten Basis bestimmt haben, wissen wir die Hauptsache noch nicht. Existiert wenigstens eine orthonormierte Basis?
Wir werden sogleich beweisen, dass eine solche Basis existiert. Wir beginnen mit der folgenden Bemerkung.

Der Vektor $\mathbf{a}$ möge nicht normiert sein (jedoch sei $\mathbf{a} \neq \mathbf{0}$). Dann können wir nach der Formel

$$\mathbf{a}' = \frac{1}{|\mathbf{a}|}\mathbf{a}$$

aus ihm einen normierten Vektor $\mathbf{a}'$ erhalten: Tatsächlich ist

$$(\mathbf{a}',\mathbf{a}') = \frac{1}{|\mathbf{a}|^2}(\mathbf{a},\mathbf{a}) = 1$$

Der Übergang von $\mathbf{a}$ zu $\mathbf{a}'$ wird Normierung des Vektors $\mathbf{a}$ genannt.
Die Existenz einer orthonormierten Basis folgt leicht aus dem Satz, der im vorhergehenden Paragraphen bewiesen wurde.

Wir wählen einen beliebigen von Null verschiedenen Vektor $\mathbf{b}_1$ aus. Indem wir ihn normieren, erhalten wir den Einheitsvektor $\mathbf{a}_1$. Weiter wählen wir einen beliebigen von Null verschiedenen Vektor $\mathbf{b}_2$ aus, der orthogonal zu $\mathbf{a}_1$ ist: indem wir ihn normieren, erhalten wir $\mathbf{a}_2$.
Weiter wählen wir einen Vektor $\mathbf{b}_3 \neq \mathbf{0}$ aus, der zu $\mathbf{a}_1$ und $\mathbf{a}_2$ orthogonal ist. Indem wir ihn normieren, erhalten wir den Vektor $\mathbf{a}_3$ usw. bis wir zum Vektor $\mathbf{a}_n$ kommen, der orthogonal zu dem früher aufgebauten Vektoren $\mathbf{a}_1, \mathbf{a}_2$, ..., $\mathbf{a}_{n-1}$ ist. Das auf diesem Wege erhaltene System

$$\mathbf{a}_1, \mathbf{a}_2, ..., \mathbf{a}_n$$

ist aufgrund von Satz 2 aus § 9 eine Basis. In der Tat ist die Anzahl der Vektoren im System gleich n, und außerdem ist dieses System linear unabhängig. Im entgegengesetzten Fall, wenn man einen der Vektoren des Systems durch die ihm vorhergehenden zerlegen könnte, zum Beispiel

$$\mathbf{a}_3 = \alpha\mathbf{a}_1 + \beta\mathbf{a}_2,$$

würden wir, indem wir beide Seiten der Gleichung skalar mit dem Vektor $\mathbf{a}_3$ multiplizieren,

$$(\mathbf{a}_3, \mathbf{a}_3) = 0$$

erhalten, was nicht möglich ist, da $(\mathbf{a}_3, \mathbf{a}_3) = 1$ gilt.
Wir stellen fest, dass wir, nachdem wir die Existenz einer orthonormierten Basis bewiesen haben, das Versprechen erfüllt haben, das wir im vorhergehenden Paragraphen gegeben hatten. Wir haben gezeigt, dass wenigstens eine Basis existiert, in der das Skalarprodukt durch Formel (3) ausgedrückt wird.

2.13.3 Eine Methode zum Auffinden aller orthonormierten Basen

Bei der Untersuchung der orthonormierten Basen erhebt sich eine Reihe interessanter Fragen. Hier ist eine davon: Wie ergibt sich eine orthonormierte Basis aus einer anderen?

Im § 9 sprachen wir davon, dass man je zwei Basen des Raumes A_n auseinander durch eine Kette elementarer Umformungen erhält. Natürlich ist dieser Satz insbesondere auch für orthonormierte Basen richtig, aber für diese ist er nicht von besonderem Interesse, denn wir erhalten durch Anwenden der elementaren Umformung auf eine orthonormierte Basis in der Regel keine orthonormierte Basis mehr (obwohl man nach einigen elementaren Umformungen wiederum eine orthonormierte Basis erhalten kann).

Wir würden natürlich gern je zwei orthonormierte Basen durch eine Kette solcher Umformungen verbinden, um nach jeder von ihnen erneut eine orthonormierte Basis zu erhalten. Es zeigt sich, dass man dies auf folgende Weise tun kann.

Es möge $\mathbf{a}_1, \mathbf{a}_2, ..., \mathbf{a}_n$ eine orthonormierte Basis sein. Wir nennen jede der folgenden Operationen eine elementare orthogonale Transformation über einer Basis:

1. Die Multiplikation eines beliebigen Basisvektors mit -1. Es ist klar, dass man als Ergebnis einer solchen Transformation erneut eine orthonormierte Basis erhält.

2. Das Ersetzen irgendwelcher zwei Vektoren $\mathbf{a}_i, \mathbf{a}_j$ $(i \neq j)$ der gegebenen Basis durch die neuen Vektoren $\mathbf{a}'_i, \mathbf{a}'_j$ nach den Formeln

$$\mathbf{a}'_i = \cos\alpha\ \mathbf{a}_i - \sin\alpha\ \mathbf{a}_j \qquad \text{und} \qquad \mathbf{a}'_j = \sin\alpha\ \mathbf{a}_i - \cos\alpha\ \mathbf{a}_j$$

wobei α eine beliebige reelle Zahl ist.
Der folgende Satz, den wir hier ohne Beweis anführen, zeigt die Rolle der elementaren orthogonalen Transformationen.

Satz. Man kann mit Hilfe einer endlichen Anzahl elementarer orthogonaler Transformationen von jeder orthonormierten Basis zu jeder anderen orthonormierten Basis übergehen.

2.13.4 Orthogonale Transformationen

Dem Leser ist wahrscheinlich der Begriff der Transformation schon bekannt (einige Transformationen werden zum Beispiel im Geometrieunterricht der Schule untersucht). Im vorliegenden Fall wird von Transformationen des n-dimensionalen Vektorraumes A_n die Rede sein.

Wir sagen, dass eine Transformation des Raumes A_n gegeben ist, wenn die Vorschrift bekannt ist, vermittels der jedem Vektor $\mathbf{a} \in A_n$ ein anderer Vektor $\mathbf{a}' \in A_n$ entspricht. Das Vorhandensein einer solchen Vorschrift kann man durch die folgende Schreibweise wiedergeben:

$$\mathbf{a}' = F(\mathbf{a})$$

wobei das Symbol F zur Bezeichnung des Verfahrens dient, durch das man $\mathbf{a}'$ aus $\mathbf{a}$ erhält.

Die Transformation F wird linear genannt, wenn sie den folgenden zwei Bedingungen genügt:

1) $F(\mathbf{x} + \mathbf{y}) = F(\mathbf{x}) + F(\mathbf{y})$;
2) $F(k\mathbf{x}) = kF(\mathbf{x})$

wobei $\mathbf{x}$ und $\mathbf{y}$ zwei beliebige Vektoren und k eine beliebige Zahl ist.

Wenn wir die Vektoren $F(\mathbf{x})$ und $F(\mathbf{y})$ mit $\mathbf{x}'$ und $\mathbf{y}'$ bezeichnen, kann man diese Bedingungen so umschreiben: die Transformation F überführt das Vektortripel $\mathbf{x}, \mathbf{y}, \mathbf{x} + \mathbf{y}$ in $\mathbf{x}', \mathbf{y}', \mathbf{x}' + \mathbf{y}'$ und das Paar $\mathbf{x}, k\mathbf{x}$ in das Paar $\mathbf{x}', k\mathbf{x}'$.
Anders ausgedrückt, die Transformation ist linear, wenn sie weder die Summe von Vektoren, noch das Produkt eines Vektors mit einer Zahl "zerstört". Daraus folgt, dass die lineare Transformation auch die Linearkombinationen nicht zerstört

$$F(k_1\mathbf{x}_1 + k_2\mathbf{x}_2 + ... + k_n\mathbf{x}_n) = kF(\mathbf{x}_1) + k_2F(\mathbf{x}_2) + ... + k_nF(\mathbf{x}_n)$$

Wir nehmen an, dass ein Skalarprodukt im Raum A_n eingeführt ist. Dann kommt unter allen linearen Transformationen denen ein besonderes Interesse zu, die dieses Skalarprodukt "erhalten", d.h. die Eigenschaft

$$(F(\mathbf{x}), F(\mathbf{y})) = (\mathbf{x},\mathbf{y}) \qquad \text{für alle} \quad \mathbf{x},\mathbf{y} \in A_n$$

besitzen. Solche Transformationen werden orthogonal genannt.
Es ist klar, dass eine orthogonale Transformation auch die Länge jedes Vektors $\mathbf{x}$ erhält, d.h.

$$|F(\mathbf{x})| = |\mathbf{x}|$$

Dies folgt daraus, dass die Länge durch das Skalarprodukt ausgedrückt wird:

$$|\mathbf{x}| = \sqrt{(\mathbf{x},\mathbf{x})}$$

Die Erhaltung der Länge eines beliebigen Vektors kann man als Definition der orthogonalen Transformationen nehmen. Das wird daraus ersichtlich, dass das Skalarprodukt seinerseits durch die Länge ausgedrückt wird. In der Tat geht aus der offensichtlichen Gleichung

$$(\mathbf{x}+\mathbf{y}, \mathbf{x}+\mathbf{y}) = (\mathbf{x},\mathbf{x}) + (\mathbf{y},\mathbf{y}) + (\mathbf{x},\mathbf{y}) + (\mathbf{y},\mathbf{x})$$

die Gleichung

$$2(\mathbf{x},\mathbf{y}) = (\mathbf{x}+\mathbf{y},\mathbf{x}+\mathbf{y}) - (\mathbf{x},\mathbf{x}) - (\mathbf{y},\mathbf{y}) = |\mathbf{x}+\mathbf{y}|^2 - |\mathbf{x}|^2 - |\mathbf{y}|^2$$

hervor.
Die orthogonalen Transformationen besitzen eine Reihe wichtiger Eigenschaften. Wir zeigen eine davon. Es möge

$$\mathbf{a}_1, \mathbf{a}_2, ..., \mathbf{a}_n$$

eine orthonormierte Basis sein. Dann bilden die Vektoren

$$\mathbf{a}'_1 = F(\mathbf{a}_1), \mathbf{a}'_2 = F(\mathbf{a}_2), ..., \mathbf{a}'_n = F(\mathbf{a}_n)$$

auch eine orthonormierte Basis. Anders ausgedrückt, eine orthogonale Transformation überführt jede orthonormierte Basis wiederum in eine orthonormierte Basis. In der Tat, da die Transformation F orthogonal ist, gilt $(\mathbf{a}_i, \mathbf{a}_j) = (\mathbf{a}'_i, \mathbf{a}'_j)$ (i und j sind beliebige Indizes von 1 bis n); folglich genügen die Vektoren

$$\mathbf{a}'_1, \mathbf{a}'_2, ..., \mathbf{a}'_n, \qquad \text{die} \qquad \mathbf{a}_1, \mathbf{a}_2, ..., \mathbf{a}_n$$

ähnlich sind, den Beziehungen

$$(\mathbf{a}'_i, \mathbf{a}'_i) = 1 \qquad \text{und} \qquad (\mathbf{a}'_i, \mathbf{a}'_j) = 0 \quad \text{für} \quad i \neq j$$

Daraus geht hervor, dass sie eine orthonormierte Basis bilden (siehe die Überlegungen am Ende von 2).

2.13.5 Die zu einer orthogonalen Transformation inverse Transformation

Wir wollen zuerst die folgende Tatsache feststellen. Für eine orthogonale Transformation F besitzt die Gleichung

$$F(\mathbf{x}) = \mathbf{b} \tag{4}$$

für jedes $\mathbf{b} \in A_n$ eine eindeutige Lösung. Dies kann man auf folgende Weise beweisen.

Es möge $\mathbf{a}_1, \mathbf{a}_2, ..., \mathbf{a}_n$ eine orthonormierte Basis sein. Dann bilden die Vektoren $\mathbf{a}'_1 = F(\mathbf{a}_1)$, $\mathbf{a}'_2 = F(\mathbf{a}_2)$, ..., $\mathbf{a}'_n = F(\mathbf{a}_n)$, wie wir wissen, auch eine orthonormierte Basis. Wir stellen den Vektor $\mathbf{b}$ durch sie dar

$$b = k_1\mathbf{a}'_1 + k_2\mathbf{a}'_2 + ... + k_n\mathbf{a}'_n$$

und zeigen, dass der Vektor

$$a = k_1\mathbf{a}_1 + k_2\mathbf{a}_2 + ... + k_n\mathbf{a}_n$$

der Gleichung (4) genügt. Tatsächlich folgt aus der Linearität der Transformation F

$$F(\mathbf{a}) = k_1\mathbf{a}'_1 + k_2\mathbf{a}'_2 + ... + k_n\mathbf{a}'_n = \mathbf{b}$$

Damit ist die Lösbarkeit der Gleichung (4) bewiesen. Die Tatsache, dass die Lösung eindeutig ist, kann man ganz einfach beweisen.
Wenn $F(\mathbf{x}_1) = \mathbf{b}$ und $F(\mathbf{x}_2) = \mathbf{b}$, gelten, dann ist $F(\mathbf{x}_1) = F(\mathbf{x}_2)$ und folglich $F(\mathbf{x}_1 - \mathbf{x}_2) = \mathbf{0}$. Dann ist aber $|x_1 - x_2| = 0$, d.h. $\mathbf{x}_1 = \mathbf{x}_2$.

Wenn man jedem Vektor $\mathbf{b} \in A_n$ den Vektor $\mathbf{x}$, der eine Lösung von Gleichung (4) ist, zuordnet, erhalten wir eine neue Transformation, die die inverse Transformation zu **F** genannt wird und mit F^{-1} bezeichnet wird.

Der oben bewiesene Satz kann jetzt anders formuliert werden.
Zu jeder orthogonalen Transformation existiert stets eine inverse Transformation. Es erhebt sich natürlich die Frage: Wird die inverse Transformation wiederum orthogonal sein? Wir werden beweisen, dass dies so ist.

Die Linearität von F^{-1} folgt in offensichtlicher Weise aus der Linearität von F.
Wenn F das Tripel der Vektoren $\mathbf{x}$, $\mathbf{y}$, $\mathbf{x} + \mathbf{y}$ in das Tripel $\mathbf{x}'$, $\mathbf{y}'$, $\mathbf{x}' + \mathbf{y}'$ überführt, dann überführt F^{-1} umgekehrt $\mathbf{x}'$, $\mathbf{y}'$, $\mathbf{x}' + \mathbf{y}'$ in $\mathbf{x}$, $\mathbf{y}$, $\mathbf{x} + \mathbf{y}$; wenn F das Paar $\mathbf{x}$, $k\mathbf{x}$ in das Paar $\mathbf{x}'$, $k\mathbf{x}'$ überführt, dann überführt F^{-1} $\mathbf{x}'$, $k\mathbf{x}'$ in $\mathbf{x}$, $k\mathbf{x}$.

Weiter folgt aus der Gleichung

$$(\mathbf{x},\mathbf{y}) = (\mathbf{x}',\mathbf{y}')$$

die Gleichung

$$(F^{-1}(\mathbf{x}'), F^{-1}(\mathbf{y}')) = (\mathbf{x}', \mathbf{y}')$$

Damit ist die Transformation F^{-1} linear und erhält das Skalarprodukt.
Folglich ist sie orthogonal. Also ist die Transformation, die zu einer orthogonalen invers ist, wiederum orthogonal.

2.13.6 Wie viele verschiedene orthogonale Transformationen existieren?

Es erheben sich die natürlichen Fragen: Existieren überhaupt orthogonale Transformationen und wie groß ist ihre Anzahl? Der folgende Satz hilft uns, sie zu beantworten.

Es mögen zwei orthonormierte Basen

$$\mathbf{a}_1, \mathbf{a}_2, ..., \mathbf{a}_n \qquad \text{und} \qquad \mathbf{a}'_1, \mathbf{a}'_2, ..., \mathbf{a}'_n$$

gegeben sein. Dann existiert eine, zudem eindeutige, orthogonale Transformation, die die erste Basis in die zweite überführt.
Die gesuchte Transformation wird auf folgende Weise bestimmt: jedem Vektor

$$\mathbf{a} = k_1\mathbf{a}_1 + k_2\mathbf{a}_2 + ... + k_n\mathbf{a}_n$$

wird der Vektor

$$F(\mathbf{a}) = k_1\mathbf{a}'_1 + k_2\mathbf{a}'_2 + ... + k_n\mathbf{a}'_n$$

zugeordnet. Wir werden zeigen, dass diese Transformation orthogonal ist. Die Linearität der Transformation F ist offensichtlich. Es bleibt nur noch zu überprüfen, dass F das Skalarprodukt erhält.
Es mögen

$$\mathbf{x} = x_1\mathbf{a}_1 + ... + x_n\mathbf{a}_n \qquad \text{und} \qquad \mathbf{y} = y_1\mathbf{a}_1 + ... + y_n\mathbf{a}_n \tag{5}$$

zwei beliebige Vektoren aus A_n sein. Es gilt

$$F(\mathbf{x}) = x_1\mathbf{a}'_1 + ... + x_n\mathbf{a}'_n \qquad \text{und} \qquad F(\mathbf{y}) = y_1\mathbf{a}'_1 + ... + y_n\mathbf{a}'_n \tag{6}$$

Da die Basis $\mathbf{a}_1, ..., \mathbf{a}_n$ orthonormiert ist, folgt aus (5)

$$(\mathbf{x},\mathbf{y}) = x_1y_1 + x_2y_2 + ... + x_ny_n$$

Aber auch die Basis $\mathbf{a}'_1, ..., \mathbf{a}'_n$ ist orthonormiert, deshalb folgt aus (6)

$$(F(\mathbf{x}),F(\mathbf{y})) = x_1y_1 + x_2y_2 + ... + x_ny_n$$

Daher ist

$$(\mathbf{x},\mathbf{y}) = (F(\mathbf{x}),F(\mathbf{y}))$$

d.h., die Transformation F ist orthogonal.

Aus der Linearität der orthogonalen Transformation folgt leicht, dass es keine andere orthogonale Transformation geben kann, die die erste Basis in die zweite überführt. Tatsächlich muss aufgrund der Linearität die gesuchte Transformation so sein, wie wir sie bestimmt haben.

Aus dem von uns bewiesenen Satz kann man diese Schlussfolgerung ziehen. Zwischen der Menge aller orthonormierter Basen und der Menge aller orthogonalen Transformationen kann man eine umkehrbar eindeutige Zuordnung aufstellen.
Dazu muss man eine der orthonormierten Basen, die wir mit B_0 bezeichnen, festhalten und einer beliebigen anderen orthonormierten Basis B die orthogonale Transformation zuordnen, die B_0 in B überführt. Es gibt auf diese Weise "so viele" orthogonale Transformationen, wie es verschiedene orthonormierte Basen gibt.

3 Die Ausnahmestellung von vier Algebren

In der unendlichen Vielfalt aller Algebren nehmen einige Algebren eine Ausnahmestellung ein. Dies sind die Algebra $\mathscr{K}$ aller komplexen Zahlen, die Algebra $\mathscr{Q}$ der Quaternionen und die Algebra $\mathscr{O}$ der Oktaven.
Was unterscheidet nun gerade diese Algebren von allen übrigen? Auf diese Frage kann man verschiedenartig antworten. Das Gemeinsame aller Antworten führt jedoch zu folgendem:

Im Vergleich mit anderen Algebren stehen die drei gezeigten ihrer Ursprungsalgebra, der Algebra $\mathscr{D}$ aller reellen Zahlen, am nächsten. Diese Nähe äußert sich zum Beispiel darin, dass:

1. die Algebren $\mathscr{D}$, $\mathscr{K}$ und $\mathscr{Q}$ die einzigen Algebren mit Division sind, in denen die Multiplikation die Eigenschaft der Assoziativität besitzt. Dieser Satz trägt in etwas genauerer Formulierung die Bezeichnung Satz von Frobenius.

2. die Algebren $\mathscr{D}$, $\mathscr{K}$, $\mathscr{Q}$ und $\mathscr{O}$ die einzigen Algebren mit Division sind, in denen die Formeln

$$(\mathbf{uv})\mathbf{v} = \mathbf{u}(\mathbf{vv}) \qquad \text{und} \qquad \mathbf{v}(\mathbf{vu}) = (\mathbf{vv})\mathbf{u}$$

gelten (eine abgeschwächte Variante der Assoziativität, die Alternativität genannt wird). Diese Behauptung wird verallgemeinerter Satz von Frobenius genannt.

3. die Algebren $\mathscr{D}$, $\mathscr{K}$, $\mathscr{Q}$ und $\mathscr{O}$ die einzigen Algebren mit Einselementen sind, in denen man ein Skalarprodukt derart einführen kann, dass die Regel "die Norm eines Produktes ist gleich dem Produkt der Normen" erfüllt wird. Diese Tatsache bildet den Inhalt des Satzes von Hurwitz.

Kurzum, in der Hierarchie der Algebren stellt sich die Lage so dar. Als "Grundlage" dient die Algebra der reellen Zahlen.
Als ihr nächster Nachbar tritt die Algebra der komplexen Zahlen auf, in der die Multiplikation alle wichtigsten Eigenschaften der Multiplikation der reellen Zahlen besitzt. Die Multiplikation ist kommutativ, assoziativ, umkehrbar (anders ausgedrückt, die Division ist möglich) und für sie existiert ein Einselement. Dann folgt die Algebra der Quaternionen, wobei in ihr von den oben aufgezählten Eigenschaften nur die Kommutativität der Multiplikation verschwindet.

Noch weiter entfernt gelegen ist die Algebra der Oktaven, in der die Assoziativität durch eine abgeschwächte Form dieser Eigenschaft, die "Alternativität", ersetzt wird, jedoch wie bei der vorigen ist die Division möglich und ein Einselement existiert.

Alle übrigen Algebren besitzen nicht einmal mehr diese Eigenschaften. Natürlich folgt daraus nicht, dass die übrigen Algebren weniger interessant oder weniger wichtig sind, im vorliegenden Fall ist nur von der größeren oder kleineren Ähnlichkeit mit der Algebra der reellen Zahlen die Rede.
Zu allem Gesagten können wir noch eine Bemerkung hinzufügen.

Im Kapitel 1 wurde die Aufgabe über die Summe von Quadraten aufgestellt, die darin bestand, alle Identitäten des bestimmten Typs

$$(a_1^2 + a_2^2 + ... + a_n^2)(b_1^2 + b_2^2 + ... + b_n^2) = \Phi_1^2 + \Phi_2^2 + ... + \Phi_n^2 \tag{1}$$

aufzufinden (siehe § 3). Ausgehend von einer oben erwähnten Eigenschaft der Algebren $\mathscr{D}$, $\mathscr{K}$, $\mathscr{Q}$ und $\mathscr{O}$ (die Norm eines Produktes ist gleich dem Produkt der Normen) konstruierten wir im Kapitel 1 konkrete Beispiele solcher Identitäten für $n = 1,2,4,8$.

In diesem Kapitel wird gezeigt werden, dass die Zahl n in der Identität (1) nur diese vier Werte annehmen kann. Eine entscheidende Rolle im Beweis dieser Tatsache wird der Satz von Hurwitz spielen. Auf diese Weise werden auch in der Aufgabe über die Summe von Quadraten als hauptsächliche Mitwirkende eben die Algebren $\mathscr{D}$, $\mathscr{K}$, $\mathscr{Q}$ und $\mathscr{O}$ auftreten.

Dieses Kapitel ist der Präzisierung und dem Beweis aller oben aufgezählten Tatsachen gewidmet.

3.14 Isomorphe Algebren

Gemäß der Definition, die in § 7 gegeben wurde, besteht eine beliebige Algebra der Dimension n aus Elementen, die man gleichbedeutend in der Form

$$a_1\mathbf{i}_1 + a_2\mathbf{i}_2 + ... + a_n\mathbf{i}_n$$

darstellen kann und die in natürlicher Weise untereinander addiert werden und mit reellen Zahlen multipliziert werden. Mit anderen Worten, jede Algebra der Dimension n ist insbesondere ein n-dimensionaler Vektorraum.
Außerdem muss die Multiplikationstafel der (ursprünglichen) Basiselemente $\mathbf{i}_1, \mathbf{i}_2$, ..., $\mathbf{i}_n$ angegeben sein, d.h., der Tafel von n^2 Beziehungen der Form

$$\mathbf{i}_\alpha\mathbf{i}_\beta = k_{\alpha\beta,1}\mathbf{i}_1 + k_{\alpha\beta,2}\mathbf{i}_2 + ... + k_{\alpha\beta,n}\mathbf{i}_n \tag{1}$$

$(\alpha, \beta = 1,2,...,n)$, wobei $k_{\alpha\beta,\gamma}$ bestimmte reelle Zahlen sind. Nachdem die Regeln der Multiplikation der Basiselemente erklärt wurden, wird das Produkt beliebiger zwei Elemente

$$a_1\mathbf{i}_1 + a_2\mathbf{i}_2 + ... + a_n\mathbf{i}_n \qquad \text{und} \qquad b_1\mathbf{i}_1 + b_2\mathbf{i}_2 + ... + b_n\mathbf{i}_n$$

der Algebra nach der gewöhnlichen Regel der Multiplikation einer Summe mit einer Summe unter anschließender Benutzung der Beziehungen (1) hergeleitet.

Man kann daher sagen, dass eine beliebige Algebra der Dimension n ein n-dimensionaler Vektorraum A_n ist, in dem zusätzlich die Multiplikationstafel der Basiselemente, die Tafel (1), Gültigkeit hat. Es scheint, als würde sich daraus der Schluss aufdrängen, dass man zwei Algebren der Dimension n, die durch verschiedene Multiplikationstafeln bestimmt wurden, als verschiedene Algebren betrachten muss. Jedoch würde dieser Gesichtspunkt nicht ganz korrekt sein, hier den Grund dafür.

Es möge $\mathscr{A}$ eine Algebra der Dimension n mit der ursprünglichen Basis $\mathbf{i}_1, \mathbf{i}_2$, ..., $\mathbf{i}_n$ und der Multiplikationstafel (1) sein. Wenn wir im Vektorraum $\mathscr{A}$ zu einer anderen Basis $\mathbf{i}'_1, \mathbf{i}'_2$, ..., $\mathbf{i}'_n$ übergehen, erhalten wir natürlich auch eine andere Multiplikationstafel

$$\mathbf{i}'_\alpha\mathbf{i}'_\beta = l_{\alpha\beta,1}\mathbf{i}'_1 + l_{\alpha\beta,2}\mathbf{i}'_2 + ... + l_{\alpha\beta,n}\mathbf{i}'_n \tag{2}$$

$(\alpha, \beta = 1,2,...,n)$.
Wir stellen uns jetzt noch eine Algebra $\mathscr{A}'$ mit der Basis $\mathbf{i}'_1, \mathbf{i}'_2$, ..., $\mathbf{i}'_n$ und der Multiplikationstafel (2) vor. Muss man sie als neue Algebra ansehen?

Es versteht sich, dass dies formal so ist, im Grunde genommen ist $\mathscr{A}'$ aber dieselbe Algebra $\mathscr{A}$, nur auf eine andere Basis bezogen. Es ist deshalb natürlich, den Unterschied zwischen den Algebren $\mathscr{A}$ und $\mathscr{A}'$ als unwesentlich anzusehen.
Dieser Gesichtspunkt findet seinen Ausdruck im Begriff des Isomorphismus.

Definition. Zwei Algebren ein und derselben Dimension n werden einander ähnlich oder isomorph genannt, wenn man aus ihnen Basen mit gleichen Multiplikationstafeln auswählen kann.

Wie sich versteht, setzt die Übereinstimmung der Multiplikationstafeln durchaus nicht dieselbe Wahl der Bezeichnungen für die Basiselemente beider Algebren voraus; zum Beispiel können die Basiselemente der ersten Algebra mit $\mathbf{c}_1, \mathbf{c}_2, ..., \mathbf{c}_n$ bezeichnet werden und die der zweiten, sagen wir, mit $\mathbf{d}_1, \mathbf{d}_2, ..., \mathbf{d}_n$.
Es ist lediglich erforderlich, dass sich jedes Produkt $\mathbf{c}_\alpha \mathbf{c}_\beta$ in $\mathbf{c}_1, \mathbf{c}_2, ..., \mathbf{c}_n$ mit genau denselben Koeffizienten zerlegen lässt, in die auch das Produkt $\mathbf{d}_\alpha \mathbf{d}_\beta$ in $\mathbf{d}_1, \mathbf{d}_2, ..., \mathbf{d}_n$ zerlegt wird. Dies bedeutet, dass, wenn zum Beispiel

$$\mathbf{c}_3\mathbf{c}_2 = 3\mathbf{c}_1 - 7\mathbf{c}_5 \qquad \text{gilt, auch} \qquad \mathbf{d}_3\mathbf{c}_d = 3\mathbf{d}_1 - 7\mathbf{d}_5$$

sein muss.

In der Mathematik werden zwei isomorphe Algebren nicht als verschieden angesehen. Man betrachtet sie so, als wären sie zwei verschiedene Exemplare ein und derselben Algebra. In Verbindung damit wird, wenn man die Frage nach dem Auffinden aller Algebren stellt, die irgendeine bestimmte Eigenschaft besitzen, die Antwort in dieser Form gesucht:
Die gesuchte Algebra ist isomorph entweder dieser oder jener konkreten Algebra usw.

Im Kapitel I führten wir den Begriff eines hyperkomplexen Systems ein und danach den breiteren Begriff einer Algebra. Die Beziehung zwischen ihnen kann in vollem Maße erst jetzt aufgedeckt werden, da wir den Begriff des Isomorphismus besitzen.
Es wurde gezeigt (§ 7), dass man jedes hyperkomplexe System als Algebra betrachten kann, in der das erste Basiselement als Einselement der Algebra auftritt:

$$\mathbf{i}_1\mathbf{i}_\alpha = \mathbf{i}_\alpha\mathbf{i}_1 = \mathbf{i}_\alpha \qquad \text{für alle } \alpha$$

Jetzt können wir zu diesem Satz in bestimmtem Sinne die Umkehrung hinzufügen: Jede Algebra mit Einselement ist einem bestimmten hyperkomplexen System isomorph.

Tatsächlich, wenn eine Algebra mit dem Einselement 1 gegeben ist, dann erhalten wir durch Auswählen einer neuen Basis $\mathbf{i}'_1, \mathbf{i}'_2, ..., \mathbf{i}'_n$ aus ihr, so dass $\mathbf{i}'_1 = 1$ gilt, eine Multiplikationstafel, in der

$$\mathbf{i}'_1\mathbf{i}'_\alpha = \mathbf{i}'_\alpha\mathbf{i}'_1 = \mathbf{i}'_\alpha$$

für alle α gilt, d.h., die Multiplikationstafel in einem bestimmten hyperkomplexen System $\mathscr{M}$. Daraus folgt, dass die Ausgangsalgebra dem hyperkomplexen System $\mathscr{M}$ isomorph ist.

Zum Abschluss führen wir noch ein Beispiel an, das die Rolle des Begriffs des Isomorphismus illustriert. Ausgehend von den Resultaten, die wir in § 2 erhalten haben, können wir jetzt sagen, dass eine beliebige Algebra der Dimension 2, die ein Einselement besitzt, einem der drei hyperkomplexen Systeme isomorph ist: den komplexen, den binären oder den dualen Zahlen.

Gerade dies ist der Übergang zum genauen Sprachgebrauch für den Sachverhalt, den wir in § 2 durch die Worte "ein beliebiges System von Zahlen $a + bi$ reduziert sich auf eines der drei ..." ausdrückten. "Reduziert sich auf" bedeutet "ist isomorph"!

3.15 Unteralgebren

Im Kapitel I stießen wir mehrfach auf eine solche Erscheinung, dass eine Algebra als Teil einer anderen auftrat. Zum Beispiel ist die Algebra der reellen Zahlen ein Teil der Algebra

der komplexen Zahlen, die letztere stellt einen Teil der Algebra der Quaternionen dar, diese Algebra geht ihrerseits in die Algebra der Oktaven ein u.ä.m.
In ähnlichen Fällen wird anstelle des Wortes "Teil" der Terminus "Unteralgebra" gebraucht.

Definition. Eine Menge $\mathscr{P}$ von Elementen der Algebra $\mathscr{A}$ wird Unteralgebra der Algebra $\mathscr{A}$ genannt, wenn:

1) $\mathscr{P}$ ein Teilraum des Vektorraumes $\mathscr{A}$ ist;
2) $\mathscr{P}$ bezüglich der Multiplikation in der Algebra $\mathscr{A}$ abgeschlossen ist, d.h. wenn $\mathbf{a} \in \mathscr{P}$ und $\mathbf{b} \in \mathscr{P}$ ist, dann gilt $\mathbf{ab} \in \mathscr{P}$.

Die erste Forderung ist gleichbedeutend (§ 10) mit der, dass $\mathscr{P}$ die Menge aller Linearkombinationen

$$k_1\mathbf{a}_1 + k_2\mathbf{a}_2 + ... + k_p\mathbf{a}_p$$

bestimmter Vektoren $\mathbf{a}_1, ..., \mathbf{a}_p$ ist. Die letzteren können linear unabhängig ausgewählt werden; in diesem Falle bilden sie eine Basis des Teilraumes $\mathscr{P}$ (und ihre Anzahl überschreitet n nicht).

Damit die zweite Forderung erfüllt ist, ist es faktisch hinreichend, dass alle möglichen Produkte der Basiselemente

$$\mathbf{a}_\alpha \mathbf{a}_\beta \qquad (\alpha, \beta = 1{,}2{,}...; p)$$

wiederum $\mathscr{P}$ angehören, d.h.; dass die Gleichungen

$$\mathbf{a}_\alpha \mathbf{a}_\beta = k_{\alpha\beta,1}\mathbf{a}_1 + k_{\alpha\beta,2}\mathbf{a}_2 + ... + k_{\alpha\beta,p}\mathbf{a}_p \tag{1}$$

$(\alpha, \beta = 1,...,p)$ gelten.
Aus der oben gegebenen Definition wird direkt klar, dass man die Unteralgebra $\mathscr{P}$ als selbständige Algebra mit den ursprünglichen Basiselementen $\mathbf{a}_1, \mathbf{a}_2$, ..., $\mathbf{a}_n$ und der Multiplikationstafel (1) betrachten kann.

Wir führen einige Beispiele von Unteralgebren an.
1. In der Algebra der Quaternionen stellt der Teilraum mit der Basis 1, **j** eine Unteralgebra dar. Ein allgemeineres Beispiel: der Teilraum mit der Basis 1, **q**, wobei **q** irgendein Quaternion ist, das 1 nicht proportional ist. Jede solche Unteralgebra ist der Algebra der komplexen Zahlen isomorph.

2. In der Algebra der Oktaven stellt der Teilraum mit der Basis 1, **i**, **E**, **I** eine Unteralgebra dar. Diese Unteralgebra ist der Algebra der Quaternionen isomorph (in der gezeigten Basis ist die Multiplikationstafel dieselbe wie in der Basis 1, **i**, **j**, **k** der Algebra der Quaternionen).
Analoge Beispiele: Jeder Teilraum mit der Basis 1, **a**, **b**, **ab**, wobei **a** und **b** zwei beliebige imaginäre Einheiten der ursprünglichen Basis 1, **i**, **j**, **k**, **E**, **I**, **J**, **K** der Algebra der Oktaven sind.

3. In der Algebra der Matrizen der gegebenen Ordnung n stellt der Teilraum der Matrizen, in denen alle Elemente der ersten k Zeilen (k ist eine feste Zahl) gleich Null sind, eine Unteralgebra dar. Ein komplizierteres Beispiel: der Teilraum der "Schachbrett"- Matrizen, d.h., der Matrizen, deren Elemente $\mathbf{a}_{ij}$ gleich Null sind, wenn $\mathbf{i}+\mathbf{j}$ eine ungerade Zahl ist. Für $n = 3$ zum Beispiel werden das Matrizen der Form

$$\begin{pmatrix} * & 0 & * \\ 0 & * & 0 \\ * & 0 & * \end{pmatrix}$$

sein.

Die Überprüfung, dass die gezeigten Teilräume Unteralgebren darstellen, überlassen wir dem Leser.

3.16 Übertragung der Aufgabe über die Summe von Quadraten in die Sprache der Algebrentheorie. Normierte Algebren

Wir erinnern den Leser an die Formulierung der Aufgabe über die Summe von Quadraten, die im Kapitel 1 aufgestellt wurde.
Es ist erforderlich, zu klären, wie n beschaffen sein muss und wie die n Formen zweiten Grades

$$\begin{aligned}&\Phi_1(x_1, x_2, ..., x_n; y_1, y_2, ..., y_n),\\ &\Phi_2(x_1, x_2, ..., x_n; y_1, y_2, ..., y_n),\\ &...\\ &\Phi_n(x_1, x_2, ..., x_n; y_1, y_2, ..., y_n)\end{aligned}$$

ausgewählt sein müssen, damit die Identität

$$(x_1^2 + x_2^2 + ... + x_n^2)(y_1^2 + y_2^2 + ... + y_n^2) = \Phi_1^2 + \Phi_2^2 + ... + \Phi_n^2 \tag{*}$$

richtig ist.
Die Untersuchung bestimmter konkreter Algebren (der Algebren der komplexen Zahlen, der Quaternionen und der Oktaven) erlaubte es uns, im Kapitel 1 Beispiele der Identitäten (*) für $n = 2$, $n = 4$ und $n = 8$ aufzubauen.
Jedoch wurde dort nichts darüber gesagt, wie man eine beliebige Identität (*) aufbaut.
Mit dieser Frage werden wir uns nun beschäftigen.

3.16.1 Die Verbindung zwischen der Identität (*) und einer bestimmten Algebra $\mathscr{A}$

Zu Beginn bemerken wir, dass mit jeder Identität (*) eine bestimmte Algebra verbunden ist. Diese Algebra wird auf folgende Weise bestimmt. Wir betrachten den n-dimensionalen Vektorraum, als dessen Elemente die Vektoren

$$x_1\mathbf{i}_1 + x_2\mathbf{i}_2 + ... + x_n\mathbf{i}_n \tag{1}$$

auftreten. Das Produkt von zwei beliebigen Elementen dieses Raumes

$$x = x_1\mathbf{i}_1 + x_2\mathbf{i}_2 + ... + x_n\mathbf{i}_n \qquad \text{und} \qquad y = y_1\mathbf{i}_1 + y_2\mathbf{i}_2 + ... + y_n\mathbf{i}_n$$

bestimmen wir durch die Formel

$$\mathbf{xy} = \Phi_1\mathbf{i}_1 + \Phi_2\mathbf{i}_2 + ... + \Phi_n\mathbf{i}_n \tag{2}$$

Aufgrund der "Linearität" der Formen Φ_1, Φ_2, ..., Φ_n in den Veränderlichen $x_1, x_2, ..., x_n$, aber auch in den Veränderlichen $y_1, y_2, ..., y_n$ ist klar, dass jede der weiter unten niedergeschriebenen Gleichungen erfüllt wird:

$$k\mathbf{x} \cdot \mathbf{y} = k(\mathbf{xy}) \qquad , \qquad \mathbf{x} \cdot k\mathbf{y} = k(\mathbf{xy})$$

$$(\mathbf{x}_1 + \mathbf{x}_2)\mathbf{y} = \mathbf{x}_1\mathbf{y} + \mathbf{x}_2\mathbf{y} \qquad , \qquad \mathbf{x}(\mathbf{y}_1 + \mathbf{y}_2) = \mathbf{xy}_1 + \mathbf{xy}_2$$

Daraus folgt, dass das Multiplikationsgesetz (2) tatsächlich eine bestimmte Algebra definiert (siehe § 7). Wir bezeichnen diese Algebra mit $\mathscr{A}$.
Wie aus dem oben Gesagten folgt, ist die Algebra $\mathscr{A}$ vollständig definiert, wenn nur die Identität (*) angegeben ist.

3.16.2 Normiertheit der Algebra

Wir werden jetzt sehen, welcher Eigenschaft der Algebra $\mathscr{A}$ die Tatsache entspricht, dass Φ_1, Φ_2, ..., Φ_n nicht einfach irgendwelche Formen zweiten Grades sind, sondern solche, für die die Identität (*) gilt.
Zu diesem Zweck geben wir in der Algebra $\mathscr{A}$ ein Skalarprodukt $(\mathbf{x}, \mathbf{y})$ an, das wir durch die Koordinaten der Vektoren **x** und **y** in der Basis $\mathbf{i}_1, \mathbf{i}_2, ..., \mathbf{i}_n$ definieren:

$$(\mathbf{x},\mathbf{y}) = x_1y_1 + x_2y_2 + ... + x_ny_n \tag{3}$$

Insbesondere gilt

$$(\mathbf{x},\mathbf{x}) = x_1^2 3 + x_2^2 + ... + x_n^2$$

Indem wir das Skalarprodukt auf die gezeigte Weise definieren, schreiben wir damit von vornherein der Basis $\mathbf{i}_1, \mathbf{i}_2, ..., \mathbf{i}_n$ die Rolle einer orthonormierten Basis zu, da

$$(\mathbf{i}_\alpha, \mathbf{i}_\alpha) = 1 \qquad , \qquad (\mathbf{i}_\alpha, \mathbf{i}_\beta) = 0$$

für alle $\alpha, \beta = 1,...n$, $\alpha \neq \beta$ gilt. Zur Erläuterung dieser Gleichungen bemerken wir, dass beim Vektor $\mathbf{i}_\alpha$ nur die α-te Koordinate von Null verschieden ist (sie ist gleich 1), und beim Vektor $\mathbf{i}_\beta$ nur die β-te.

Nachdem in der Algebra $\mathscr{A}$ ein Skalarprodukt definiert worden ist, kann man erneut die Identität (*) deuten. Der Ausdruck, der auf der rechten Seite der Identität steht, ist, wie man unschwer bemerkt, gleich (**xy**,**xy**), dem "skalaren Quadrat" des Elementes **xy**; die linke Seite stellt das Produkt zweier "skalarer Quadrate" dar: (**x**,**x**) und (**y**,**y**). Deshalb kann man anstelle von (*)

$$(\mathbf{xy},\mathbf{xy}) = (\mathbf{x},\mathbf{x})(\mathbf{y},\mathbf{y}) \tag{4}$$

schreiben. Übrigens, wenn man die Norm des Elementes **x** die durch die Formel

$$|\mathbf{x}| = \sqrt{(\mathbf{x},\mathbf{x})}$$

definiert wird, in die Betrachtung einführt, kann man die Gleichung (4) ihrerseits folgendermaßen schreiben:

$$|\mathbf{xy}| = |\mathbf{x}||\mathbf{y}| \tag{4'}$$

(die Norm eines Produktes ist gleich dem Produkt der Normen).
Wir verwenden jetzt die folgende

Definition. Eine Algebra $\mathscr{A}$ wird normiert genannt, wenn man in ihr ein Skalarprodukt auf die Art einführen kann, dass die Identität (4) erfüllt ist.

Beispiele normierter Algebren stellen die uns schon bekannten Algebren der komplexen Zahlen, der Quaternionen und der Oktaven dar. Ihre Normiertheit folgt daraus, dass in jeder dieser Algebren die Formel (4) gilt; man braucht dabei, damit alles genau der Definition einer normierten Algebra entspricht, nur ein Skalarprodukt zu finden, für das die Gleichung

$$|\mathbf{x}| = \sqrt{(\mathbf{x},\mathbf{x})}$$

erfüllt ist. Im Falle der Algebra der komplexen Zahlen wird ein solches Skalarprodukt durch die Formel

$$(\mathbf{z}, \mathbf{z}') = x_1y_1 + x_2y_2$$

definiert, wobei $\mathbf{z} = x_1 + y_1\mathbf{i}$ und $\mathbf{z}' = x_2 + y_2\mathbf{i}$ ist; für die Algebra der Quaternionen durch

$$(\mathbf{q}, \mathbf{q}') = x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4$$

wobei $\mathbf{q} = x_1 + x_2\mathbf{i} + x_3\mathbf{j} + x_4\mathbf{k}$ und $\mathbf{q'} = y_1 + y_2\mathbf{i} + y_3\mathbf{j} + y_4\mathbf{k}$ ist; in analoger Weise wird das Skalarprodukt in der Algebra der Oktaven definiert.

3.16.3 Schlussfolgerung

Wir haben also bewiesen, dass man jeder Identität (*) eine bestimmte normierte Algebra $\mathscr{A}$ zuordnen kann. Die Multiplikation beliebiger zwei Elemente

$$\mathbf{x} = x_1\mathbf{i}_1 + ... + x_i\mathbf{i}_n \qquad \text{und} \qquad \mathbf{y} = y_1\mathbf{i}_1 + ... + y_i\mathbf{i}_n$$

wird in dieser Algebra durch die Formel

$$\mathbf{xy} = \Phi_1\mathbf{i}_1 + ... + \Phi_n\mathbf{i}_n \tag{5}$$

definiert, das Skalarprodukt aber nach der Formel

$$(\mathbf{x},\mathbf{y}) = x_1y_1 + x_2y_2 + ...x_ny_n$$

In der Algebra $\mathscr{A}$ bilden die Elemente $\mathbf{i}_1, \mathbf{i}_2, ..., \mathbf{i}_n$ eine orthonormierte Basis. Dabei ist die Identität (*) nichts anderes als die Bedingung der Normiertheit der Algebra $\mathscr{A}$, in dieser Basis geschrieben.

Man kann leicht sehen, dass auch die umgekehrte Behauptung richtig ist, nämlich: Wenn eine beliebige normierte Algebra $\mathscr{A}$ gegeben ist und in ihr eine beliebige orthonormierte Basis $i_1, i_2, ..., i_n$ ausgewählt wurde, dann erhält man, wenn man das Multiplikationsgesetz in dieser Basis niederschreibt, n Formen $\Phi_1, \Phi_2, ..., \Phi_n$, und wenn man die Bedingung der Normiertheit der Algebra $\mathscr{A}$ niederschreibt, dann erhält man die Identität (*) mit diesen Formen auf der rechten Seite.
Wenn wir die Bilanz des Gesagten ziehen, kommen wir zu folgender Schlussfolgerung:

Alle Formen $\Phi_1, \Phi_2, ..., \Phi_n$, die der Identität (*) genügen, können auf folgendem Wege erhalten werden.
Man betrachtet eine beliebige normierte Algebra $\mathscr{A}$ und in ihr eine beliebige orthonormierte Basis $i_1, i_2, ..., i_n$ und schreibt danach das Multiplikationsgesetz der Algebra $\mathscr{A}$ in der Form (5).
Daraus ist ersichtlich, dass die Aufgabe der Aufzählung aller Identitäten (*) sich auf zwei Aufgaben reduziert:

1) Das Auffinden aller normierter Algebren.
2) Die Niederschrift des Multiplikationsgesetzes für jede dieser Algebren in jeder ihrer orthonormierten Basen.

Die erste dieser Aufgaben werden wir in den nächsten zwei Paragraphen betrachten. Auf der Basis ihrer Lösung wird ein Überblick über alle Identitäten (*) erhalten werden.

3.17 Normierte Algebren mit Einselement. Satz von Hurwitz

3.17.1 Die Formulierung des Satzes von Hurwitz

Im vorhergehenden Paragraphen gelangten wir bei der Erläuterung der Aufgabe über die Summe von Quadraten zur Notwendigkeit, alle möglichen normierten Algebren zu finden. Weiter unten wird ein Satz bewiesen, der erstmalig durch den deutschen Mathematiker A. Hurwitz im Jahre 1898 aufgestellt wurde.

Obwohl er noch nicht die vollständige Aufzählung aller normierten Algebren bringt, behebt er doch den Hauptteil der Schwierigkeiten, die mit der Lösung dieser Aufgabe verbunden sind.

Satz (von Hurwitz). Jede normierte Algebra mit Einselement ist isomorph einer der vier Algebren: der reellen Zahlen, der komplexen Zahlen, der Quaternionen oder der Oktaven.

Die Bedingung, dass die Algebra ein Einselement enthält, darf in der Formulierung des Satzes nicht weggelassen werden. Wie wir weiter sehen werden, existieren normierte Algebren, die keine Einselemente enthalten. Solche Algebren können keiner der vier im Satz angeführten Algebren isomorph sein, da es in jeder dieser vier Algebren ein Einselement gibt.

Es möge also $\mathscr{A}$ eine normierte Algebra mit Einselement sein. Wir erinnern uns, dass wir vereinbart hatten, eine Algebra normiert zu nennen, wenn man in ihr ein Skalarprodukt mit folgender Eigenschaft einführen kann:

$$(\mathbf{ab}, \mathbf{ab}) = (\mathbf{a}, \mathbf{a})(\mathbf{b}, \mathbf{b}) \tag{1}$$

Bevor wir zum Beweis des Satzes schreiten, wollen wir darauf hinweisen, dass er ziemlich lang sein wird. Deshalb legen wir zuerst das allgemeine Schema dar, das die Beweisidee aufdeckt und füllen danach das "Loch" in den durchgeführten Überlegungen.

3.17.2 Entwurf des Beweises

Wir bezeichnen das Einselement der Algebra $\mathscr{A}$ mit $\mathbf{1}$. Man kann jedes Element $\mathbf{a} \in \mathscr{A}$ gleichwertig als Summe von zwei Summanden[15] darstellen, von denen einer proportional $\mathbf{1}$ ist und der andere orthogonal zu $\mathbf{1}$ ist

$$\mathbf{a} = k\mathbf{1} + \mathbf{a}'$$

wobei k eine reelle Zahl ist und $\mathbf{a}' \perp \mathbf{1}$. Wir führen in der Algebra die folgende Operation der Konjugation ein. Das zu $\mathbf{a}$ konjugierte Element ist

$$\overline{\mathbf{a}} = k\mathbf{1} - \mathbf{a}'$$

Insbesondere ist $\overline{\mathbf{a}} = \mathbf{a}$, wenn das Element $\mathbf{a}$ proportional zu $\mathbf{1}$ ist; wenn $\mathbf{a}$ orthogonal zu $\mathbf{1}$ ist, dann gilt $\overline{\mathbf{a}} = -\mathbf{a}$. Offensichtlich ist auch, dass

$$\overline{\overline{\mathbf{a}}} = \mathbf{a} \qquad \text{und} \qquad \overline{\mathbf{a} + \mathbf{b}} = \overline{\mathbf{a}} + \overline{\mathbf{b}}$$

gelten. Nachdem die Konjugation in der Algebra $\mathscr{A}$ eingeführt wurde, können wir zur Darlegung der Idee schreiten, die dem Beweis des Satzes zugrunde liegt.

Es möge $\mathscr{U}$ irgendeine Unteralgebra der Algebra $\mathscr{A}$ sein, die $\mathbf{1}$ enthält und nicht mit der ganzen Algebra übereinstimmt. Wir wählen in $\mathscr{U}$ eine Basis aus den Elementen $\mathbf{1}, \mathbf{i}_1, \mathbf{i}_2, ..., \mathbf{i}_n$, wobei $\mathbf{i}_1, \mathbf{i}_2, ..., \mathbf{i}_n$ orthogonal zu $\mathbf{1}$ sind. Dann wird

$$a_0 - a_1\mathbf{i}_1 - ... - a_n\mathbf{i}_n$$

konjugiert zu einem beliebigen Element

$$a_0 + a_1\mathbf{i}_1 + ... + a_n\mathbf{i}_n$$

[15] An dieser Stelle sowie auch in den folgenden Überlegungen stützen wir uns auf die allgemeinen Eigenschaften des Skalarproduktes, die im § 12 betrachtet wurden.

aus $\mathscr{U}$ sein. Daraus ist ersichtlich, wenn das Element $\mathbf{u}$ zu $\mathscr{U}$ gehört, dann gehört das ihm konjugierte Element $\bar{\mathbf{u}}$ ebenfalls $\mathscr{U}$ an.
Gemäß dem Satz in § 12 existiert ein Vektor, der nicht der Nullvektor ist und der orthogonal zu $\mathscr{U}$ ist. Wenn man ihn mit einer geeigneten Zahl multipliziert, erhält man einen Einheitsvektor $\mathbf{e}$, der orthogonal zu $\mathscr{U}$ ist. Es wird gezeigt werden, dass die Menge der Elemente der Form

$$\mathbf{u}_1 + \mathbf{u}_2 e \qquad (\mathbf{u}_1 \in \mathscr{U}, \mathbf{u}_2 \in \mathscr{U}) \tag{2}$$

bezüglich der Multiplikation abgeschlossen ist, d.h., wiederum eine Unteralgebra bildet. Wir bezeichnen die letztere mit $\mathscr{U} + \mathscr{U}\mathbf{e}$ Wir werden beweisen, dass:

I) die Darstellung eines beliebigen Elementes aus $\mathscr{U} + \mathscr{U}\mathbf{e}$ in der Form (2) nur in einer einzigen Weise möglich ist;

II) für das Produkt der Elemente der Form (2) die Formel

$$(\mathbf{u}_1 + \mathbf{u}_2\mathbf{e})(\mathbf{v}_1 + \mathbf{v}_2\mathbf{e}) = (\mathbf{u}_1\mathbf{v}_1 - \bar{\mathbf{v}}_2\mathbf{u}_2) + (\mathbf{v}_2\mathbf{u}_1 + \mathbf{u}_2\bar{\mathbf{v}}_1)\mathbf{e} \tag{3}$$

gilt.
Wenn wir diese Tatsachen mit dem Verdopplungsverfahren, das in § 6 beschrieben wurde, vergleichen, kommen wir zu folgender Schlussfolgerung: die Unteralgebra $\mathscr{U} + \mathscr{U}\mathbf{e}$ ist isomorph der verdoppelten Unteralgebra $\mathscr{U}$.

Damit sind die hauptsächlichen Schwierigkeiten für den Beweis des Satzes überwunden. Bevor wir zur abschließenden Etappe des Beweises übergehen, machen wir noch eine Bemerkung bezüglich der Konjugation in der Algebra $\mathscr{A}$.

Da die Algebra $\mathscr{A}$ ein Einselement enthält, gibt es in ihr eine Unteralgebra, die aus Elementen der Form $k\mathbf{1}$ besteht. Diese Unteralgebra ist zur Algebra der reellen Zahlen isomorph; wir bezeichnen sie mit $\mathscr{D}$. Wenn man in den vorhergehenden Überlegungen als $\mathscr{U}$ die Unteralgebra $\mathscr{D}$ nimmt, dann wird $\mathbf{e}$ ein beliebiger Vektor der Länge 1, der orthogonal zu $\mathbf{1}$ ist. Aus Formel (3) folgt dann, dass

$$\mathbf{e}^2 = (\mathbf{0} + \mathbf{1e})(\mathbf{0} + \mathbf{1e}) = -1$$

gilt. Daraus kann man den Schluss ziehen, dass das Quadrat eines beliebigen Vektors $\mathbf{a}'$, der orthogonal zu $\mathbf{1}$ ist, gleich $\lambda\mathbf{1}$ mit $\lambda < 0$ ist. Man kann auch leicht die Umkehrung beweisen. Wenn das Quadrat irgendeines Elementes gleich $\lambda\mathbf{1}$ ist, wobei $lambda < 0$ ist, dann ist dieses Element orthogonal zu $\mathbf{1}$.[16]
Auf diese Weise sind die und nur die Elemente, die orthogonal zu $\mathbf{1}$ sind, dadurch charakterisiert, dass ihre Quadrate gleich $\lambda\mathbf{1}$ sind, wobei $\lambda < 0$ ist. Dies erlaubt es uns, die Konjugation in der Algebra $\mathscr{A}$ anders zu beschreiben. Für jedes Element $\mathbf{a} \in \mathscr{A}$, das eine eindeutige Darstellung in der Form

$$k\mathbf{1} + \mathbf{a}'$$

besitzt, wobei $\mathbf{a}'^2 = \lambda\mathbf{1}$ und $\lambda < 0$ gilt, ist $\overline{a} = k\mathbf{1} - \mathbf{a}'$.

[16] Tatsächlich ist das Quadrat eines beliebigen Elementes, das nicht orthogonal zu $\mathbf{1}$ ist, d.h., eines Elementes der Form $\mathbf{a} = k\mathbf{1} + \mathbf{a}'$, wobei $k \neq 0$ und $\mathbf{a}' \perp \mathbf{1}$ ist, gleich

$$(k\mathbf{1} + \mathbf{a}')(k\mathbf{1} + \mathbf{a}') = k^2\mathbf{1} + \mathbf{a}'^2 + 2k\mathbf{a}' = k^2\mathbf{1} + \mu\mathbf{1} + 2k\mathbf{a}'$$

Wenn dieser Ausdruck proportional zu $\mathbf{1}$ ist, dann gilt $\mathbf{a}' = \mathbf{0}$, folglich ist $\mathbf{a} = k\mathbf{1}$, das Quadrat eines solchen Elementes kann aber nicht gleich $\lambda\mathbf{1}$ sein, wobei $\lambda < 0$ ist.

Wir gehen zum abschließenden Teil des Beweises über. Er stellt die folgende, sehr leicht durchschaubare Überlegung dar. Wir betrachten erneut die Unteralgebra $\mathscr{D}$.
Wenn sie nicht mit der ganzen Algebra $\mathscr{A}$ übereinstimmt, kann man einen Einheitsvektor $\mathbf{e}$ finden, der orthogonal zu $\mathscr{D}$ ist. Wir betrachten dann die Unteralgebra $\mathscr{K} = \mathscr{D} + \mathscr{D}\mathbf{e}$. Sie stellt die Verdopplung von $\mathscr{D}$ dar und ist folglich der Algebra der komplexen Zahlen isomorph.

Aus dem, was oben über die Konjugation in der Algebra $\mathscr{A}$ gesagt wurde, folgt, dass die Konjugation für die Elemente aus $\mathscr{K}$ mit der gewöhnlichen Konjugation der komplexen Zahlen übereinstimmt.
Wenn die Unteralgebra $\mathscr{K}$ nicht mit der ganzen Algebra $\mathscr{A}$ übereinstimmt, dann kann man wieder einen Einheitsvektor $\mathbf{e}'$ finden, der orthogonal zu $\mathscr{K}$ ist.

Wir betrachten dann die Unteralgebra $\mathscr{Q} = \mathscr{K} + \mathscr{K}\mathbf{e}'$, die die Verdopplung von $\mathscr{K}$ darstellt. Sie ist der Algebra der Quaternionen isomorph. Aus der oben gegebenen Charakteristik der Konjugation in der Algebra $\mathscr{A}$ folgt erneut, dass die Konjugation für die Elemente aus $\mathscr{Q}$ mit der gewöhnlichen Konjugation in der Algebra der Quaternionen übereinstimmt.

Wenn die Unteralgebra $\mathscr{Q}$ nicht mit der ganzen Algebra $\mathscr{A}$ übereinstimmt, wählen wir erneut einen Einheitsvektor $\mathbf{e}''$ aus, der orthogonal zu $\mathscr{Q}$ ist, und betrachten die Unteralgebra $\mathscr{O} = \mathscr{Q} + \mathscr{Q}\mathbf{e}''$, die die Verdopplung von $\mathscr{Q}$ darstellt und folglich der Algebra der Oktaven isomorph ist (§ 6).
Es erweist sich, dass diese Unteralgebra notwendig mit $\mathscr{A}$ übereinstimmt, da, wie wir beweisen werden, eine beliebige Unteralgebra, die $\mathbf{1}$ enthält und nicht mit der ganzen Algebra $\mathscr{A}$ übereinstimmt, assoziativ ist. Da die Multiplikation der Oktaven nicht assoziativ ist, muss die Unteralgebra $\mathscr{O}$ mit der ganzen Algebra $\mathscr{A}$ übereinstimmen!

Wenn wir aus dem oben Gesagten die Bilanz ziehen, dann erhalten wir das Ergebnis: Wenn die Algebra $\mathscr{A}$ keiner der Algebren $\mathscr{D}$, $\mathscr{K}$ oder $\mathscr{Q}$ isomorph ist, dann ist sie der Algebra $\mathscr{O}$ isomorph.
Dies ist aber die Behauptung des Satzes. Also wird der Satz bewiesen sein, wenn wir die Richtigkeit der Behauptungen I und II überprüfen sowie die Behauptung III beweisen:

Jede Unteralgebra $\mathscr{U}$, die 1 enthält und nicht mit der ganzen Algebra $\mathscr{A}$ übereinstimmt, ist assoziativ.

3.17.3 Zwei Lemmata

Einleitend benötigen wir zwei Lemmata. Wir empfehlen dem Leser, sich zuerst mit ihrer Formulierung vertraut zu machen und sich den Beweis für die "zweite Lektüre" vorzubehalten.

Lemma 1. In jeder normierten Algebra $\mathscr{A}$ gilt die Identität

$$(\mathbf{a}_1\mathbf{b}_1, \mathbf{a}_2\mathbf{b}_2) + (\mathbf{a}_1\mathbf{b}_2, \mathbf{a}_2\mathbf{b}_1) = 2(\mathbf{a}_1,\mathbf{a}_2)(\mathbf{b}_1, \mathbf{b}_2) \tag{4}$$

Wir bemerken, dass diese Identität vier beliebige Elemente $\mathbf{a}_1, \mathbf{a}_2, \mathbf{b}_1, \mathbf{b}_2$ der Algebra $\mathscr{A}$ miteinander verbindet.

Beweis. Wir setzen in der grundlegenden Identität (1) an die Stelle des Elementes $\mathbf{a}$ die Summe $\mathbf{a}_1 + \mathbf{a}_2$. Wir erhalten

$$(\mathbf{a}_1\mathbf{b} + \mathbf{a}_2\mathbf{b}, \mathbf{a}_1\mathbf{b} + \mathbf{a}_2\mathbf{b}) = (\mathbf{a}_1 + \mathbf{a}_2,\mathbf{a}_1 + \mathbf{a}_2)(\mathbf{b},\mathbf{b})$$

oder

$$(\mathbf{a}_1\mathbf{b}, \mathbf{a}_1\mathbf{b}) + (\mathbf{a}_2\mathbf{b}, \mathbf{a}_2\mathbf{b}) + 2(\mathbf{a}_1\mathbf{b}, \mathbf{a}_2\mathbf{b}) = (\mathbf{a}_1,\mathbf{a}_1)(\mathbf{b},\mathbf{b}) + (\mathbf{a}_2, \mathbf{a}_2)(\mathbf{b}, \mathbf{b}) + 2(\mathbf{a}_1, \mathbf{a}_2)(\mathbf{b}, \mathbf{b})$$

Infolge der Identität (1) ist der erste und zweite Summand der linken Seite gleich dem entsprechenden ersten und zweiten Summanden der rechten Seite. Folglich gilt

$$(\mathbf{a}_1\mathbf{b}, \mathbf{a}_2\mathbf{b}) = (\mathbf{a}_1, \mathbf{a}_2)(\mathbf{b}, \mathbf{b}) \tag{5}$$

Um das geforderte Resultat zu erhalten, muss man in der Identität (5) $\mathbf{b}$ durch $\mathbf{b}_1+\mathbf{b}_2$ ersetzen. Wir haben dann

$$(\mathbf{a}_1\mathbf{b}_1 + \mathbf{a}_1\mathbf{b}_2, \mathbf{a}_2\mathbf{b}_1 + \mathbf{a}_2\mathbf{b}_2) = (\mathbf{a}_1, \mathbf{a}_2)(\mathbf{b}_1 + \mathbf{b}_2, \mathbf{b}_1 + \mathbf{b}_2)$$

oder

$$\begin{aligned}(\mathbf{a}_1\mathbf{b}_1 + \mathbf{a}_2\mathbf{b}_1) + (\mathbf{a}_1\mathbf{b}_2 + \mathbf{a}_2\mathbf{b}_2) + (\mathbf{a}_1\mathbf{b}_1 + \mathbf{a}_2\mathbf{b}_2) + (\mathbf{a}_1\mathbf{b}_2 + \mathbf{a}_2\mathbf{b}_1) &= \\ = (\mathbf{a}_1,\mathbf{a}_2)(\mathbf{b}_1, \mathbf{b}_1) + (\mathbf{a}_1,\mathbf{a}_2)(\mathbf{b}_2, \mathbf{b}_2) + 2(\mathbf{a}_1,\mathbf{a}_2)(\mathbf{b}_1, \mathbf{b}_2)&\end{aligned}$$

Aufgrund von (5) aber sind der erste und der zweite Summand der linken Seite gleich dem entsprechenden ersten und zweiten Summanden der rechten Seite. Durch Streichen gleicher Summanden kommen wir zur Identität (4).

Lemma 2. In einer normierten Algebra $\mathscr{A}$ mit Einselement gilt die Identität

$$(\mathbf{ab})\overline{\mathbf{b}} = (\mathbf{b}, \mathbf{b})\mathbf{a} \tag{6}$$

Anders ausgedrückt, das Element $(\mathbf{ab})\overline{\mathbf{b}}$ ist immer proportional $\mathbf{a}$, wobei der Proportionalitätsfaktor gleich dem Skalarprodukt $(\mathbf{b}, \mathbf{b})$ ist.

Beweis. Wir bemerken zunächst, dass es hinreichend ist, die Identität (6) für die Fälle zu beweisen, in denen $\mathbf{b} \perp \mathbf{1}$ ist. Tatsächlich, es möge $\mathbf{b}'$ ein beliebiges Element der Algebra $\mathscr{A}$ sein. Wir stellen es in der Form

$$\mathbf{b}' = k\mathbf{1} + \mathbf{b}$$

dar, wobei $\mathbf{b} \perp \mathbf{1}$ ist. Dann gilt $\overline{\mathbf{b}} = -\mathbf{b}$ und

$$(\mathbf{ab}')\overline{\mathbf{b}}' = (\mathbf{a}(k\mathbf{1} + \mathbf{b}))(k\mathbf{1} - \mathbf{b}) = k^2\mathbf{a} - (\mathbf{ab})\mathbf{b} = k^2\mathbf{a} + (\mathbf{ab})\overline{\mathbf{b}}$$

Wenn wir jetzt annehmen, dass die Formel (6) für den Vektor $\mathbf{b}$ gilt, dann erhalten wir[17]

$$(\mathbf{ab}')\overline{\mathbf{b}}' = k^2\mathbf{a} + (\mathbf{bb})\mathbf{a} = [k^2 + (\mathbf{b},\mathbf{b})]\mathbf{a} = (\mathbf{b}',\mathbf{b}')\mathbf{a})$$

d.h., wir erhalten, dass die Formel (6) für den Vektor $\mathbf{b}'$ gilt.
Wir werden also die Identität (6) unter der Voraussetzung beweisen, dass $\mathbf{b} \perp \mathbf{1}$ ist (oder, was dasselbe ist, $\overline{\mathbf{b}} = -\mathbf{b}$).

Zur Abkürzung der weiteren Formulierungen werden wir die Zahl $(\mathbf{b}, \mathbf{b})$ mit λ bezeichnen. Wir betrachten das Element

$$\mathbf{c} = (\mathbf{ab})\overline{\mathbf{b}} - \lambda\mathbf{a}$$

[17] Aus der Gleichung $\mathbf{b}' = k\mathbf{1} + \mathbf{b}$ erhalten wir

$$(\mathbf{b}',\mathbf{b}') = k^2(\mathbf{1},\mathbf{1}) + (\mathbf{b},\mathbf{b})$$

weiter muss man berücksichtigen, dass $(\mathbf{1},\mathbf{1}) = 1$ ist, wie leicht aus der grundlegenden Identität (1) für $\mathbf{a} = \mathbf{b} = \mathbf{1}$ folgt.

Wir müssen zeigen, dass $\mathbf{c} = \mathbf{0}$ ist, oder, was dasselbe bedeutet, dass $(\mathbf{c},\mathbf{c}) = 0$ ist. Aufgrund der Eigenschaften des Skalarproduktes haben wir

$$(\mathbf{c},\mathbf{c}) = (\mathbf{a},\mathbf{b})\overline{\mathbf{b}}, (\mathbf{ab})\overline{\mathbf{b}}) + \lambda^2(\mathbf{a},\mathbf{a}) - 2\lambda((\mathbf{ab})\overline{\mathbf{b}},\mathbf{a}) \tag{7}$$

Die rechte Seite besteht aus drei Summanden. Den ersten davon kann man leicht mit Hilfe der grundlegenden Identität (1) vereinfachen:

$$((\mathbf{ab})\overline{\mathbf{b}}, (\mathbf{ab})\overline{\mathbf{b}}) = (\mathbf{ab}, \mathbf{ab})(\overline{\mathbf{b}}, \overline{\mathbf{b}}) = (\mathbf{a}, \mathbf{a})(\mathbf{b}, \mathbf{b})^2 = \lambda^2(\mathbf{a}, \mathbf{a})$$

Zur Vereinfachung des dritten Summanden benutzen wir die Identität (4). Einleitend schreiben wir diese Identität in der Form

$$(\mathbf{a}_1\mathbf{b}_1, \mathbf{a}_2\mathbf{b}_2) = 2(\mathbf{a}_1, \mathbf{a}_2)(\mathbf{b}_1, \mathbf{b}_2) - (\mathbf{a}_1\mathbf{b}_2, \mathbf{a}_2\mathbf{b}_1)$$

Wenn wir hier

$$\mathbf{a}_1 = \mathbf{ab}, \qquad \mathbf{b}_1 = \overline{\mathbf{b}}, \qquad \mathbf{a}_2 = \mathbf{a}, \qquad \mathbf{b}_2 = \mathbf{1}$$

setzen, dann erhalten wir

$$((\mathbf{ab})\overline{\mathbf{b}}, \mathbf{a}) = 2(\mathbf{ab}, \mathbf{a})(\overline{\mathbf{b}}, \mathbf{1}) - (\mathbf{ab}, \mathbf{a}\overline{\mathbf{b}})$$

Der erste Summand der rechten Seite ist aufgrund von $\mathbf{b} \perp \mathbf{1}$ gleich Null, der zweite ist gleich

$$-(\mathbf{ab}, \mathbf{a}\overline{\mathbf{b}}) = (\mathbf{ab}, \mathbf{ab}) = (\mathbf{a}, \mathbf{a})(\mathbf{b}, \mathbf{b}) = \lambda(\mathbf{a}, \mathbf{a})$$

Abschließend erhalten wir

$$((\mathbf{ab})\overline{\mathbf{b}}, \mathbf{a}) = \lambda(\mathbf{a}, \mathbf{a})$$

Wenn wir uns Gleichung (7) zuwenden, können wir jetzt

$$(\mathbf{c}, \mathbf{c}) = \lambda^2(\mathbf{a}, \mathbf{a}) + \lambda^2(\mathbf{a}, \mathbf{a}) - 2\lambda(\mathbf{a}, \mathbf{a}) = 0$$

schreiben, was zu beweisen war.

Folgerung aus Lemma 2. Aus der Identität (6) leiten wir jetzt eine andere Identität ab, die in den weiteren Überlegungen eine sehr wichtige Rolle spielen wird. Wir setzen in (6) anstelle von $\mathbf{b}$ die Summe $\mathbf{x} + \mathbf{y}$. Wir erhalten

$$(\mathbf{a}(\mathbf{x} + \mathbf{y}))(\overline{\mathbf{x}},\overline{\mathbf{y}}) = (\mathbf{x} + \mathbf{y},\mathbf{x} + \mathbf{y})\mathbf{a}$$

oder

$$(\mathbf{ax})\overline{\mathbf{x}} + (\mathbf{ay})\overline{\mathbf{y}} + (\mathbf{ax})\overline{\mathbf{y}} + (\mathbf{ay})\overline{\mathbf{x}} = (\mathbf{x},\mathbf{x})\mathbf{a} + (\mathbf{y},\mathbf{y})\mathbf{a} + 2(\mathbf{x},\mathbf{y})\mathbf{a}$$

Aufgrund der Identität (6) aber sind der erste und zweite Summand der linken Seite gleich dem entsprechenden ersten und zweiten Summanden der rechten Seite, folglich ist

$$(\mathbf{ax})\overline{\mathbf{y}} + (\mathbf{ay}\overline{\mathbf{x}} = 2(\mathbf{x},\mathbf{y})\mathbf{a} \tag{8}$$

Dies ist die benötigte Identität.
Aus der Identität (6) erhalten wir für $\mathbf{a} = \mathbf{1}$

$$\mathbf{b}\overline{\mathbf{b}} = (\mathbf{b},\mathbf{b})\mathbf{1}$$

Diese Formel ergibt in Verbindung mit (6)

$$(\mathbf{ab})\overline{\mathbf{b}} = \mathbf{a}(\mathbf{b}\overline{\mathbf{b}})$$

Daraus folgt sofort

$$(\mathbf{ab})\mathbf{b} = \mathbf{a}(\mathbf{bb})$$

Durch analoge Überlegungen kann man die Formel

$$\mathbf{b}(\mathbf{ba}) = (\mathbf{bb})\mathbf{a}$$

erhalten. Die zwei letzten Formeln zeigen, dass die Algebra $\mathscr{A}$ alternativ ist.

3.17.4 Abschluss des Beweises

Wir kommen jetzt zum Beweis der Behauptungen I, II und III. Wir erinnern daran, dass in diesen Behauptungen $\mathscr{U}$ eine beliebige Unteralgebra der Algebra $\mathscr{A}$ bezeichnet, die **1** enthält und nicht mit der ganzen Algebra übereinstimmt, während e ein beliebiger Einheitsvektor ist, der orthogonal zu $\mathscr{U}$ ist.

Zu Beginn stellen wir fest, dass die Teilräume $\mathscr{U}$ und $\mathscr{U}e$ zueinander orthogonal sind, d.h., dass $\mathbf{u}_1 \perp \mathbf{u}_2\mathbf{e}$ für zwei beliebige Elemente $\mathbf{u}_1 \in \mathscr{U}$ und $\mathbf{u}_2 \in \mathscr{U}$ ist. Dazu benutzen wir das Lemma 1.
Wenn man in der Identität (4)

$$\mathbf{a}_1 = \mathbf{u}_1, \qquad \mathbf{b}_1 = \mathbf{u}_2, \qquad \mathbf{a}_2 = \mathbf{e}, \qquad \mathbf{b}_2 = \mathbf{1}$$

setzt, dann erhält man

$$(\mathbf{u}_1\mathbf{u}_2,\mathbf{e}) + (\mathbf{u}_1, \mathbf{u}_2\mathbf{e}) = 2(\mathbf{u}_1, \mathbf{e})(\mathbf{u}_2, \mathbf{1})$$

Man muss jetzt berücksichtigen, dass $\mathscr{U}$ eine Unteralgebra ist, und folglich gehört $\mathbf{u}_1\mathbf{u}_1$ zu $\mathscr{U}$. Also ist $\mathbf{u}_1 \perp \mathbf{e}$ und $\mathbf{u}_1\mathbf{u}_2 \perp \mathbf{e}$. Deshalb folgt aus der oben niedergeschriebenen Gleichung

$$(\mathbf{u}_1, \mathbf{u}_2\mathbf{e}) = 0$$

d.h. $\mathbf{u}_1 \perp \mathbf{u}_2\mathbf{e}$. Folglich sind die Teilräume $\mathscr{U}$ und $\mathscr{U}e$ zueinander orthogonal.
Daraus folgt leicht die Behauptung 1:

Die Darstellung jedes Elementes aus $\mathscr{U} + \mathscr{U}e$ in Form von $\mathbf{u}_1 + \mathbf{u}_2\mathbf{e}$ ist auf genau eine Art möglich. In der Tat, es möge

$$\mathbf{u}_1 + \mathbf{u}_2\mathbf{e} = \mathbf{u}_1' + \mathbf{u}_2'\mathbf{e}$$

sein. Dann gilt

$$\mathbf{u}_1 - \mathbf{u}_1' = (\mathbf{u}_2' - \mathbf{u}_2)\mathbf{e}$$

und folglich gehört das Element $\mathbf{v} = \mathbf{u} - \mathbf{u}'$ gleichzeitig den Teilräumen $\mathscr{U}$ und $\mathscr{U}e$ an. Nach dem früher Bewiesenen sind aber diese Teilräume zueinander orthogonal. Folglich ist $(\mathbf{v}, \mathbf{v}) = 0$ und damit $\mathbf{v} = \mathbf{0}$. Dies ergibt

$$\mathbf{u}_1 - \mathbf{u}_1' = \mathbf{0} \qquad \text{und} \qquad (\mathbf{u}'2 - \mathbf{u}_2)\mathbf{e} = \mathbf{0}$$

Weiter kann man leicht sehen, dass aufgrund der grundlegenden Identität (1) aus $\mathbf{ab} = \mathbf{0}$ folgt $\mathbf{a} = \mathbf{0}$ oder $\mathbf{b} = \mathbf{0}$.
Im gegebenen Fall ist das Produkt $(\mathbf{u}_2' - \mathbf{u}_2)\mathbf{e}$ gleich **0**, und da $\mathbf{e} \neq \mathbf{0}$ ist, muss $\mathbf{u}_2' - \mathbf{u}_2 = \mathbf{0}$ sein. Also ist $\mathbf{u}_1 = \mathbf{u}_1'$ und $\mathbf{u}_2 = \mathbf{u}_2'$. Die Behauptung I ist damit bewiesen.

Wir gehen jetzt zum Beweis der Behauptung II über. Wir müssen die Gültigkeit der Formel (3) überprüfen. Dazu beweisen wir, dass für zwei beliebige Elemente **u** und **v** aus der Unteralgebra $\mathscr{U}$ die Formeln

$$(\mathbf{ue})\mathbf{v} = (\mathbf{uv})\mathbf{e}, \quad \mathbf{u}(\mathbf{ve}) = (\mathbf{vu})\mathbf{e}, \quad (\mathbf{ue})(\mathbf{ve}) = -\bar{\mathbf{v}}\mathbf{u} \qquad (\alpha,\beta,\gamma)$$

gelten. Aus diesen Beziehungen geht die Formel (3) in offensichtlicher Weise hervor. Tatsächlich erhalten wir nach der gewöhnlichen Regel der Multiplikation einer Summe mit einer Summe

$$(\mathbf{u}_1 + \mathbf{u}_2\mathbf{e})(\mathbf{v}_1 + \mathbf{v}_2\mathbf{e}) = \mathbf{u}_1\mathbf{v}_1 + (\mathbf{u}_2\mathbf{e})(\mathbf{v}_2\mathbf{e}) + (\mathbf{u}_2\mathbf{e})\mathbf{v}_1 + \mathbf{u}_1(\mathbf{v}_2\mathbf{e})$$

und wenn wir die letzten drei Summanden der rechten Seite mit Hilfe der Formeln (α), (β) und (γ) umformen, dann erhalten wir

$$(\mathbf{u}_1 + \mathbf{u}_2\mathbf{e})(\mathbf{v}_1 + \mathbf{v}_2\mathbf{e}) = (\mathbf{u}_1\mathbf{v}_1 - \overline{\mathbf{v}}_2\mathbf{u}_2) + (\mathbf{v}_2\mathbf{u}_1 + \mathbf{u}_2\overline{\mathbf{v}}_1)\mathbf{e}$$

d.h. Formel (3). Zum Beweis von (α), (β) und (γ) gehen wir von der früher bewiesenen Identität (8) aus:

$$(\mathbf{ax})\overline{\mathbf{y}} + (\mathbf{ay})\overline{\mathbf{x}} = 2(\mathbf{x}, \mathbf{y})\mathbf{a} \tag{8}$$

Wenn wir in dieser Identität

$$\mathbf{a} = \mathbf{u}, \qquad \mathbf{x} = \mathbf{e}, \qquad \mathbf{y} = \overline{\mathbf{v}}$$

setzen und berücksichtigen, dass $\mathbf{v} \perp \mathbf{e}$ ist, dann erhalten wir

$$(\mathbf{ue})\mathbf{v} + (\mathbf{u}\overline{\mathbf{v}})\overline{\mathbf{e}} = \mathbf{0}$$

Wenn wir berücksichtigen, dass $\overline{\mathbf{e}} = -\mathbf{e}$ ist (da $\mathbf{e} \perp \mathbf{1}$ ist), erhalten wir die Formel (α). Um (β) zu beweisen, setzen wir in der Identität (8)

$$\mathbf{a} = \mathbf{1}, \qquad \mathbf{x} = \mathbf{u}, \qquad \mathbf{y} = \overline{\mathbf{ve}}$$

Wenn wir berücksichtigen, dass $\overline{\mathbf{ve}} = -\mathbf{ve}$ ist (da $\mathbf{ve} \perp \mathscr{U}$ ist und folglich $\mathbf{ve} \perp \mathbf{1}$ ist), dann erhalten wir

$$\mathbf{u}(\mathbf{ve}) - (\mathbf{ve})\overline{\mathbf{u}} = \mathbf{0}$$

Wenn wir jetzt die schon bewiesene Formel (α) benutzen, dann haben wir

$$\mathbf{u}(\mathbf{ve}) = (\mathbf{ve})\overline{\mathbf{u}} = (\mathbf{vu})\mathbf{e}$$

Zur Ableitung der Formel (γ) benutzen wir die folgende offensichtliche Bemerkung. Wenn diese Formel für $\mathbf{v} = \mathbf{c}$ und $\mathbf{v} = \mathbf{d}$ gilt, so ist sie auch für $\mathbf{v} = \mathbf{c} + \mathbf{d}$ richtig. Da man jedes Element $\mathbf{v}$ in Form einer Summe von zwei Summanden darstellen kann, von denen einer proportional zu $\mathbf{1}$ und der andere orthogonal zu $\mathbf{1}$ ist, wird aus der oben gemachten Bemerkung klar, dass es genügt, die Formel (γ) für zwei Fälle zu beweisen, für $\mathbf{v} = k\mathbf{1}$ und für $\mathbf{v} \perp \mathbf{1}$.

Wenn $\mathbf{v} = k\mathbf{1}$ ist, dann nimmt die Formel (γ) die Form

$$k(\mathbf{ue})\mathbf{e} = -k\mathbf{u}$$

an. Eine solche Formel gilt aber aufgrund der Identität (6). Es möge $\mathbf{v} \perp \mathbf{1}$ sein (und folglich $\overline{\mathbf{v}} = -\mathbf{v}$). Wenn wir in der Identität

$$\mathbf{a} = \mathbf{u}, \qquad \mathbf{x} = \mathbf{e}, \qquad \mathbf{y} = -\mathbf{ve}$$

setzen, so erhalten wir

$$(\mathbf{ue})(\mathbf{ve}) - (\mathbf{u}(\mathbf{ve}))\overline{\mathbf{e}} = -2(\mathbf{e}, \mathbf{ve})\mathbf{u}$$

Der Ausdruck $(\mathbf{e}, \mathbf{ve})$ ist aber aufgrund der Identität (5) gleich $(\mathbf{1}, \mathbf{v})(\mathbf{e},\mathbf{e})$, d.h. gleich Null. Weiterhin ist aufgrund von (β) der zweite Summand der linken Seite gleich

$$-((\mathbf{vu})\mathbf{e})\overline{\mathbf{e}} = -\mathbf{vu} = \overline{\mathbf{v}}\mathbf{u}$$

Daraus folgt

$$(\mathbf{ue})(\mathbf{ve}) = -\overline{\mathbf{v}}\mathbf{u}$$

was zu zeigen war.
Also sind alle drei Formeln (α), (β) und (γ) und zusammen mit ihnen auch die Behauptung II bewiesen.

Um den Beweis des Satzes abzuschließen, bleibt noch ein letzter Schritt. Es ist zu zeigen, dass (Behauptung III) jede Unteralgebra $\mathscr{U}$ der Algebra $\mathscr{A}$, die 1 enthält und nicht mit der ganzen Algebra $\mathscr{A}$ übereinstimmt, assoziativ ist, d.h., dass

$$(\mathbf{uv})\mathbf{w} = \mathbf{u}(\mathbf{vw})$$

für je drei Elemente $\mathbf{u}$, $\mathbf{v}$ und $\mathbf{w}$ aus $\mathscr{U}$ gilt. Dazu benutzen wir wiederum die Identität (8). Wenn wir darin $\mathbf{a} = \mathbf{ve}$, $\mathbf{x} = \overline{\mathbf{w}}$ und $\mathbf{y} = \overline{\mathbf{u}}\mathbf{e}$, setzen, so erhalten wir

$$((\mathbf{ve})\overline{\mathbf{w}})(-\overline{\mathbf{u}}\mathbf{e}) + (\mathbf{ve})(\overline{\mathbf{u}}\mathbf{e}))\mathbf{w} = \mathbf{0}$$

oder, wenn wir die Formeln (α) und (γ) anwenden,

$$\mathbf{u}(\mathbf{vw}) - (\mathbf{uv})\mathbf{w} = \mathbf{0}$$

Der Beweis des Satzes von Hurwitz ist damit vollständig abgeschlossen.

3.18 Eine Methode zum Aufbau einer beliebigen normierten Algebra und daraus hervorgehende Folgerungen für die Aufgabe über die Summe von Quadraten

3.18.1 Eine Methode zum Aufbau neuer normierter Algebren

Zu Beginn zeigen wir ein spezielles Verfahren, mit dessen Hilfe man, ausgehend von einer gegebenen normierten Algebra $\mathscr{A}$, viele andere normierte Algebren aufbauen kann. Es mögen A und B zwei orthogonale Transformationen in $\mathscr{A}$ sein (d.h., zwei Transformationen, die die Norm jedes Elementes $\mathbf{x} \in \mathscr{A}$ erhalten).

Wir definieren im Vektorraum der Algebra $\mathscr{A}$ eine neue Multiplikation, die wir mit Hilfe des Symbols "$\circ$" bezeichnen, durch die Formel

$$\mathbf{u} \circ \mathbf{v} = A(\mathbf{u})B(\mathbf{v}) \tag{4}$$

Wie aus dieser Definition ersichtlich ist, muss man, um das Produkt der Elemente $\mathbf{u}$ und $\mathbf{v}$ in der neuen Bedeutung zu erhalten, anstelle von $\mathbf{u}$ und $\mathbf{v}$ die Elemente $A(\mathbf{u})$ und $B(\mathbf{v})$ nehmen und sie im alten Sinne miteinander multiplizieren. Es ist nicht schwierig, sich davon zu überzeugen, dass für die neue Operation die folgenden Beziehungen gelten:

$$\mathbf{u} \circ (\mathbf{v}_1 + \mathbf{v}_2) = \mathbf{u} \circ \mathbf{v}_! + \mathbf{u} \circ \mathbf{v}_2 \quad , \quad \mathbf{u} \circ k\mathbf{v} = k(\mathbf{u} \circ \mathbf{v}) \quad \text{und}$$

$$(\mathbf{u}_1 + \mathbf{u}_2) \circ \mathbf{v} = \mathbf{u}_1 \circ \mathbf{v} + \mathbf{u}_2 \circ \mathbf{v} \quad , \quad k\mathbf{u} \circ \mathbf{v} = k(\mathbf{u} \circ \mathbf{v})$$

Die ersten zwei der niedergeschriebenen Gleichungen gehen aus der Linearität der Transformation B hervor, die beiden anderen aus der Linearität von A.
Diese Beziehungen zeigen, dass die neue Operation "$\circ$" tatsächlich eine Multiplikation ist (siehe § 7).

Den Vektorraum der Algebra $\mathscr{A}$, der mit der neuen Operation der Multiplikation versehen ist, bezeichnen wir mit $\mathscr{A}_0$. Auf diese Weise sind $\mathscr{A}$ und $\mathscr{A}_0$ ein und derselbe Vektorraum, jedoch mit verschiedenen Multiplikationen ausgestattet.

In der Algebra $\mathscr{A}$ ist nach Vereinbarung das Skalarprodukt $(\mathbf{x}, \mathbf{y})$ gegeben. Es erweist sich, dass in Bezug auf dieses Skalarprodukt die neue Algebra $\mathscr{A}_0$, wie die alte, auch normiert ist. Tatsächlich folgt aus Formel (1)

$$|\mathbf{u} \circ \mathbf{v}| = |A(\mathbf{u})B(\mathbf{v})| = |A(\mathbf{u})||B(\mathbf{v})| = |\mathbf{u}||\mathbf{v}|$$

Hier benutzten wir die Normiertheit der Ausgangsalgebra $\mathscr{A}$ sowie auch die Tatsache, dass die Transformationen A und B orthogonal sind,d.h., dass $|A(\mathbf{u})| = |\mathbf{u}|$ und $|B(\mathbf{v})| = |\mathbf{v}|$ gelten.

3.18.2 Konstruktion einer beliebigen normierten Algebra

Mit der oben gezeigten Methode kann man aus einer normierten Algebra $\mathscr{A}$ viele andere erhalten. Dazu muss man in der Formel (1) die eine oder andere orthogonale Transformation A und B einsetzen.
Uns sind vier bemerkenswerte normierte Algebren bekannt: die der reellen Zahlen, der komplexen Zahlen, der Quaternionen und der Oktaven.

Ist es nicht möglich, durch Anwenden der beschriebenen Methodik auf sie überhaupt alle normierten Algebren zu erhalten? Es erweist sich; dass man es kann.

Da nach dem Satz von Hurwitz alle normierten Algebren mit Einselement durch die vier gezeigten Algebren ausgeschöpft werden, müssen wir hierzu den folgenden Satz beweisen.

Satz. Jede normierte Algebra $\mathscr{A}_0$ kann aus einer bestimmten normierten Algebra $\mathscr{A}$ mit Einselement durch Einführen einer neuen Multiplikation nach Formel (1) erhalten werden (in dieser Formel bedeutet $\circ$ die Multiplikation in der Algebra $\mathscr{A}_0$).

Zum Beweis nehmen wir ein beliebiges Element $\mathbf{e} \in \mathscr{A}_0$, dessen Norm gleich 1 ist, und betrachten die Transformation der Algebra $\mathscr{A}_0$, bei der jedes ihrer Elemente $\mathbf{x}$ in $\mathbf{x} \circ \mathbf{e}$ übergeht. Diese Transformation (Multiplikation mit $\mathbf{e}$ von rechts) wird rechte Verschiebung um das Element $\mathbf{e}$ in der Algebra $\mathscr{A}_0$ genannt; wir bezeichnen sie kurz mit A. Wir führen also die Transformation

$$A(\mathbf{x}) = \mathbf{x} \circ \mathbf{e}$$

ein. Es ist nicht schwierig zu sehen, dass die Transformation A orthogonal ist. Tatsächlich folgt aus der Gleichung

$$|A(\mathbf{x})| = |\mathbf{x} \circ \mathbf{e}| = |\mathbf{x}||\mathbf{e}| = |\mathbf{x}|$$

dass die Transformation A die Norm eines beliebigen Elementes $\mathbf{x}$ erhält. In analoger Weise kann man die andere Transformation

$$B(\mathbf{x}) = \mathbf{e} \circ \mathbf{x}$$

die linke Verschiebung um das Element $\mathbf{e}$ in der Algebra $\mathscr{A}_0$ erklären und kann zeigen, dass sie auch orthogonal ist.
Aus der Orthogonalität der Transformation A und B geht (§ 13) die Existenz der inversen Transformationen A^{-1} und B^{-1} sowie auch deren Orthogonalität hervor.[18]

[18] Wir machen eine beiläufige Bemerkung. Die Existenz der Transformationen A^{-1} und B^{-1} bedeutet, dass jede der Gleichungen $\mathbf{x} \circ \mathbf{e} = \mathbf{a}$ und $\mathbf{e} \circ \mathbf{y} = \mathbf{a}$ eine eindeutige Lösung besitzt. Die Tatsache, dass $|\mathbf{e}| = 1$ ist, spielt hier natürlich keine Rolle; wichtig ist nur, dass $\mathbf{e} \neq \mathbf{0}$ ist.

Daraus kann man folgende Schlussfolgerung ziehen: Jede normierte Algebra ist eine Algebra mit Division.

Indem wir diese Transformationen benutzen, führen wir gleich ein neues Multiplikationsgesetz in den Vektorraum der Algebra $\mathscr{A}_0$ ein. Und zwar definieren wir das Produkt der Elemente **x** und **y** in neuer Bedeutung durch die Formel

$$\mathbf{xy} = A^{-1}(\mathbf{x}) \circ B^{-1}(\mathbf{y}) \tag{2}$$

Die auf diese Weise erhaltene neue Algebra bezeichnen wir mit $\mathscr{A}$. Die niedergeschriebene Gleichung drückt die neue Multiplikation durch die alte aus. Man kann aber aus ihr auch leicht den Ausdruck der alten Multiplikation durch die neue erhalten. Wenn wir

$$A^{-1}(\mathbf{x}) = \mathbf{u} \qquad \text{und} \qquad B^{-1}(\mathbf{y}) = \mathbf{v}$$

setzen, dann werden wir

$$A(\mathbf{u})B(\mathbf{v}) = \mathbf{u} \circ \mathbf{v}$$

erhalten. Auf diese Weise wird man, wenn man die Algebra $\mathscr{A}$ mit der Multiplikation **uv** als Ausgangsalgebra nimmt, die uns von vornherein gegebene Algebra $\mathscr{A}_0$ aus ihr durch Ersetzen der Multiplikation durch die Multiplikation $\mathbf{u} \circ \mathbf{v}$ nach der Formel

$$\mathbf{u} \circ \mathbf{v} = A(\mathbf{u})B(\mathbf{v})$$

erhalten.
Um den Beweis des Satzes abzuschließen, bleibt jetzt nur noch zu zeigen, dass die Algebra $\mathscr{A}$ ein Einselement besitzt. Wir werden beweisen, dass in der Algebra $\mathscr{A}$ das Element $\tilde{\mathbf{e}} = \mathbf{e} \circ \mathbf{e}$ die Rolle des Einselementes spielt. In der Tat, betrachten wir die zwei Produkte

$$\mathbf{x}\tilde{\mathbf{e}} \qquad \text{und} \qquad \tilde{\mathbf{e}}\mathbf{y}$$

Für das erste davon gilt

$$\mathbf{x}\tilde{\mathbf{e}} = A^{-1}(\mathbf{x}) \circ B^{-1}(\mathbf{e})$$

Nach Definition der inversen Transformation ist das Element $\mathbf{u} = B^{-1}(\tilde{\mathbf{e}})$ die (eindeutige) Lösung der Gleichung

$$B(\mathbf{u}) = \tilde{\mathbf{e}}$$

oder, was dasselbe ist, der Gleichung $\mathbf{e} \circ \mathbf{u} = \mathbf{e} \circ \mathbf{e}$. Daraus wird klar (aufgrund der Eindeutigkeit), dass dieses Element gleich **e** ist. Weiter bedeutet $\mathbf{v} = A^{-1}(\mathbf{x})$, dass $\mathbf{x} = A(\mathbf{v})$ ist, d.h. $\mathbf{v} \circ \mathbf{e} = \mathbf{x}$. Damit erhalten wir

$$\mathbf{x}\tilde{\mathbf{e}} = A^{-1}(\mathbf{x}) \circ B^{-1}(\tilde{\mathbf{e}}) = \mathbf{v} \circ \mathbf{e} = \mathbf{x}$$

Genauso finden wir, dass

$$\tilde{\mathbf{e}}\mathbf{y} = A^{-1}(\tilde{\mathbf{e}}) \circ B^{-1}(\mathbf{y}) = \mathbf{e} \circ B^{-1}(\mathbf{y}) = \mathbf{y}$$

gilt. Damit haben wir gezeigt, dass $\tilde{\mathbf{e}}$ die Einheit der Algebra ist. Der Satz ist vollständig bewiesen.

Folglich können durch Einführung der neuen Multiplikation nach Formel (1) ohne Ausnahmen alle normierten Algebren aus den vier bekannten Algebren $\mathscr{D}$, $\mathscr{K}$, $\mathscr{Q}$ und $\mathscr{O}$ erhalten werden. Bis zu der jetzt bekannten Stufe kann man diese Tatsache als Methode der Beschreibung aller normierter Algebren betrachten.

3.18.3 Die Zahl n in der Identität (*)

Als Folgerungen aus dem Satz erhalten wir, dass die Dimension einer beliebigen normierten Algebra gleich einer der Zahlen 1, 2, 4 oder 8 ist (entsprechend den Dimensionen der Algebren der reellen Zahlen, der komplexen Zahlen, der Quaternionen und der Oktaven).
Wir erinnern jetzt daran, dass eine bestimmte Verbindung zwischen normierten Algebren und Identitäten der Form

$$(x_1^2 + x_2^2 + ... + x_n^2)(y_1^2 + y_2^2 + ... + y_n^2) = \Phi_1^2 + \Phi_2^2 + ... + \Phi_n^2 \qquad (*)$$

existiert. Diese Verbindung (siehe § 17) besteht darin, dass wir, wenn wir eine beliebige normierte Algebra der Dimension n nehmen, in ihr eine beliebige orthonormierte Basis auswählen und das Multiplikationsgesetz in dieser Basis niederschreiben, dann n Formen Φ_1, Φ_2, ..., Φ_n erhalten, die der Identität (*) genügen; mehr noch, auf solchem Wege können ohne Ausnahme alle Identitäten (*) erhalten werden. Unter Berücksichtigung dieser Verbindung werden wir die folgenden fundamentale Schlussfolgerung ziehen.

Die Zahl n in der Identität (*) kann nur einer der vier Zahlen 1, 2, 4 oder 8 gleich sein.

3.18.4 Überblick über alle Identitäten (*)

Natürlich kann man aus dem oben bewiesenen Satz etwas mehr ableiten, als nur die Schlussfolgerung über die Zahl der Quadrate in der Identität (*).
Tatsächlich haben wir, wenn wir das Verfahren des Aufbaus einer beliebigen normierten Algebra kennen, damit eine bestimmte Methode, eine Beschreibung aller Identitäten (*) zu geben.
Wir werden zeigen, dass man alle solche Identitäten auf folgendem Wege erhalten kann.

Für gegebenes n, das einer der Zahlen 2, 4 oder 8 gleich ist, muss man in der entsprechenden Algebra $\mathscr{K}$, $\mathscr{Q}$ oder $\mathscr{O}$ drei orthonormierte Basen

$$\mathbf{e}_1, \mathbf{e}_2, ..., \mathbf{e}_n; \quad \mathbf{k}_1, \mathbf{k}_2, ..., \mathbf{k}_n; \quad \mathbf{i}_1, \mathbf{i}_2, ..., \mathbf{i}_n$$

nehmen, einen beliebigen Vektor **x** durch die erste Basis darstellen, einen beliebigen Vektor **y** durch die zweite und ihr Produkt durch die dritte, d.h., man schreibt

$$\mathbf{x} = \sum_\alpha x_\alpha \mathbf{e}_\alpha, \qquad \mathbf{y} = \sum_\beta y_\beta \mathbf{k}_\beta, \qquad \mathbf{xy} = \sum_\gamma \Phi_\gamma \mathbf{i}_\gamma$$

Dann genügen die Formen[19] $\Phi_\gamma(x_1, ..., x_n; y_1, ..., y_n)$ der Identität (*), wobei auf solchem Wege jede Identität (*) erhalten werden kann.

Dass der gezeigte Weg immer auf Formen führt, die (*) genügen, folgt aus der Gleichung

$$\left(\sum_\alpha x_\alpha \mathbf{e}_\alpha\right)\left(\sum_\beta y_\beta \mathbf{k}_\beta\right) = \sum_\gamma \Phi_\gamma \mathbf{i}_\gamma$$

[19] Um tatsächlich Ausdrücke für die Formen Φ_j zu finden, muss man

$$\mathbf{xy} = \left(\sum_\alpha x_\alpha \mathbf{e}_\alpha\right)\left(\sum_\beta y_\beta \mathbf{k}_\beta\right) = \sum_{\alpha,\beta} x_\alpha y_\beta \mathbf{e}_\alpha \mathbf{k}_\beta$$

aufschreiben und jedes Produkt $\mathbf{e}_\alpha \mathbf{k}_\beta$ durch seine Zerlegung in $\mathbf{i}_1, ..., \mathbf{i}_n$ ersetzen.

Tatsächlich erhalten wir die Identität (*), wenn wir die Norm beider Seiten der Gleichungen nehmen.

Umgekehrt werden wir zeigen, dass jede Identität (*) auf die gezeigte Weise erhalten werden kann. Wir wissen bereits, dass man jede Identität (*) erhält, wenn man das Multiplikationsgesetz in der Form

$$\mathbf{x} \circ \mathbf{y} = A(\mathbf{x})B(\mathbf{y})$$

betrachtet (wobei A und B orthogonale Transformationen sind), und es in einer beliebigen orthonormierten Basis $\mathbf{i}_1, ..., \mathbf{i}_n$ schreibt. Mit anderen Worten, die Formen $\Phi_1, \Phi_2, ..., \Phi_n$, die in die gegebene Identität eingehen, werden aus der Gleichung

$$A\left(\sum_\alpha x_\alpha \mathbf{i}_\alpha\right) \overline{B}\left(\sum_\beta y_\beta \mathbf{i}_\beta\right) = \sum_\gamma \Phi_\gamma \mathbf{i}_\gamma \tag{3}$$

übernommen. Aufgrund der Linearität der Transformationen A und B aber haben wir

$$A\left(\sum_\alpha x_\alpha \mathbf{i}_\alpha\right) = \sum_\alpha x_\alpha A(\mathbf{i}_\alpha) \qquad , \qquad B\left(\sum_\beta y_\beta \mathbf{i}_\beta\right) = \sum_\beta y_\beta B(\mathbf{i}_\beta)$$

Wenn wir $A(\mathbf{i}_\alpha)$ mit $\mathbf{e}_\alpha$ und $B(\mathbf{i}_\beta)$ mit $\mathbf{k}_\beta$ bezeichnen, so kommen wir auf folgende Schreibweise der Gleichung (3):

$$\left(\sum_\alpha x_\alpha \mathbf{e}_\alpha\right)\left(\sum_\beta y_\beta \mathbf{k}_\beta\right) = \sum_\gamma \Phi_\gamma \mathbf{i}_\gamma$$

Wenn wir jetzt berücksichtigen, dass jeder der Sätze $\mathbf{e}_1, \mathbf{e}_2, ..., \mathbf{e}_n$ und $\mathbf{k}_1, \mathbf{k}_2, ..., \mathbf{k}_n$ eine orthonormierte Basis darstellt, so kommen wir zu dem Schluss, dass man den Satz von Formen $\Phi_1, \Phi_2, ..., \Phi_n$ so erhält, wie oben gezeigt wurde.

Für den besser vorgebildeten Leser führen wir jetzt denselben Überblick über die Identitäten (*) in anderen Termini an. Für gegebenes $n = 1, 2, 4, 8$ muss man irgendeinen bestimmten Satz $\Phi_1, \Phi_2, ..., \Phi_n$ nehmen und ihn auf folgende Weise verändern. Die Veränderlichen $x_1, x_2, ..., x_n$ in dem Ausdruck für Φ_n werden durch die Veränderlichen $x_1', x_2', ..., x_n'$ ersetzt, die mit Hilfe einer bestimmten orthogonalen Transformation A durch die $x_1, x_2, ..., x_n$ ausgedrückt werden. Analog wird die Operation über $y_1, y_2, ..., y_n$ mit Hilfe einer anderen orthogonalen Transformation B ausgeführt. Danach wird der erhaltene Satz von Formen $\Phi_1, \Phi_2, ..., \Phi_n$ einer dritten orthogonalen Transformation C unterworfen.

Wir vereinbaren, zwei Identitäten (*) als äquivalent zu betrachten, wenn man die eine von ihnen aus der anderen gerade durch das gezeigte Verfahren erhält. Dann ist der folgende Satz richtig.

Bei gegebenem $n = 1, 2, 4, 8$ existiert bis auf Äquivalenz nur eine Identität (*).

3.18.5 Beispiele normierter Algebren der Dimension 2 und 4 mit zugehörigen Identitäten (*)

Unter den normierten Algebren der Dimension 2 besitzt, wie wir wissen, nur eine ein Einselement. Das ist die Algebra $\mathscr{K}$ der komplexen Zahlen. Weil der Übergang zur konjugiert komplexen Zahl

$$\mathbf{x} \to \overline{\mathbf{x}}$$

eine orthogonale Transformation der Algebra $\mathscr{K}$ ist (da $|\bar{\mathbf{x}}| = |\mathbf{x}|$ ist), können wir noch mindestens drei neue Algebren aufbauen.
Dazu ersetzen wir die gewöhnliche Multiplikation $\mathbf{xy}$ der komplexen Zahlen durch die neuen Operationen

$$\mathbf{x}①\mathbf{y} = \bar{\mathbf{x}}\mathbf{y} \quad , \quad \mathbf{x}②\mathbf{y} = \mathbf{x}\bar{\mathbf{y}} \quad , \quad \mathbf{x}③\mathbf{y} = \bar{\mathbf{x}}\,\bar{\mathbf{y}} \tag{4}$$

Man erhält die drei neuen normierten Algebren $\mathscr{K}_1$, $\mathscr{K}_2$ und $\mathscr{K}_3$.
Als nützliche Übung schlagen wir dem Leser vor, zu beweisen, dass eine beliebige normierte Algebra der Dimension 2 isomorph einer der Algebren $\mathscr{K}$, $\mathscr{K}_1$, $\mathscr{K}_2$ und $\mathscr{K}_3$ ist,wobei unter diesen vier Algebren keine zwei einander isomorph sind.

Wir führen jetzt Beispiele von Identitäten (*) an, die mit den beschriebenen Algebren verbunden sind. Für die Algebra $\mathscr{K}_1$ erhalten wir mit der Basis $\mathbf{1}$, $\mathbf{i}$

$$\mathbf{x}①\mathbf{y} = \bar{\mathbf{x}}\mathbf{y} = (x_1 + x_2\mathbf{i})(y_1 + y_2\mathbf{i}) = (x_1y_1 + x_2y_2) + (y_1x_2 - x_2y_1)\mathbf{i}$$

Deshalb wird die entsprechende Identität

$$(x_1^2 + x_2^2)(y_1^2 + y_2^2) = (x_1y_1 + x_2y_2)^2 + (x_1y_2 - x_2y_1)^2$$

sein. Sie unterscheidet sich, wie wir sehen, etwas von der uns bereits bekannten Identität

$$(x_1^2 + x_2^2)(y_1^2 + y_2^2) = (x_1y_1 - x_2y_2)^2 + (x_1y_2 + x_2y_1)^2 \tag{5}$$

der der Algebra $\mathscr{K}$ entsprechenden in derselben Basis $\mathbf{1}$, $\mathbf{i}$. Eine Identität, die sich stärker von (5) unterscheidet, kann man erhalten, wenn man als Ausgangsalgebra $\mathscr{K}$ nimmt und in ihr als Basisvektoren die Elemente

$$\mathbf{e}_1 = \frac{1}{\sqrt{2}}(\mathbf{1} + \mathbf{i}) \qquad \text{und} \qquad \mathbf{e}_2 = \frac{1}{\sqrt{2}}(\mathbf{1} - \mathbf{i})$$

nimmt. Es ist nicht schwierig zu überprüfen, dass diese zwei Elemente eine orthonormierte Basis bilden. Wir schreiben das Multiplikationsgesetz in dieser Basis nieder:

$$(\mathbf{u}_1\mathbf{e}_1+\mathbf{u}_2\mathbf{e}_2)(\mathbf{v}_1\mathbf{e}_1+\mathbf{v}_2\mathbf{e}_2) = \frac{1}{\sqrt{2}}(u_1v_2+v_1u_2+u_1v_1-u_2v_2)\mathbf{e}_1+\frac{1}{\sqrt{2}}(u_1v_2+v_1u_2-u_1v_1+u_2v_2)\mathbf{e}_2$$

Die entsprechende Identität ist

$$\begin{aligned}(u_1^2 + u_2^2)(v_1^2 + v_2^2) &= \left[\frac{1}{\sqrt{2}}(u_1v_2 + v_1u_2 + u_1v_1 - u_2v_2)\right]^2 \\ &\quad + \left[\frac{1}{\sqrt{2}}(u_1v_2 + v_1u_2 - u_1v_1 + u_2v_2)\right]^2\end{aligned}$$

Wir wenden uns den normierten Algebren der Dimension 4 zu.
In diesem Falle ist die einzige Algebra mit Einselement, wie wir wissen, die Algebra $\mathscr{Q}$ der Quaternionen. Ebenso wie im Falle der komplexen Zahlen ist die Operation der Konjugation eine orthogonale Transformation der Algebra $\mathscr{Q}$.
Deshalb existieren noch mindestens drei normierte Algebren $\mathscr{Q}_1$, $\mathscr{Q}_2$ und $\mathscr{Q}_3$ der Dimension 4 mit einer Multiplikation, die durch die Formeln (4) definiert wird. Im vierdimensionalen Fall

jedoch existieren auch noch andere normierte Algebren, zum Beispiel Algebren mit Multiplikationen der Form

$$\mathbf{axyb}, \quad \mathbf{a\bar{x}yb}, \quad \mathbf{ax\bar{y}b}, \quad \mathbf{a\bar{x}\bar{y}b}$$

wobei **a** und **b** zwei feste Quaternionen sind. Man kann zeigen (wir überlassen dies dem Leser), dass jede normierte Algebra der Dimension 4 einer solchen Algebra isomorph ist.

Wir betrachten als Beispiel die erste der gezeigten Multiplikationen mit $\mathbf{a} = \mathbf{i}$, $\mathbf{b} = \mathbf{j}$. Wir erhalten die normierte Algebra $\mathscr{Q}$ mit dem Multiplikationsgesetz

$$\mathbf{x} \circ \mathbf{y} = (\mathbf{ix})(\mathbf{yj})$$

Wenn wir als Basiselemente $\mathbf{1}$, $\mathbf{i}$, $\mathbf{j}$, $\mathbf{k}$ nehmen, werden wir herausfinden, welche Identität (*) dieser Algebra entspricht. Wir erhalten

$$\begin{aligned}\mathbf{x} \circ \mathbf{y} &= (\mathbf{i}(x_0 + x_1\mathbf{i} + x_2\mathbf{j} + x_3\mathbf{k}))(y_0 + y_1\mathbf{i} + y_2\mathbf{j} + y_3\mathbf{k})\mathbf{j}) \\ &= (x_0\mathbf{i} - x_1 + x_2\mathbf{k} - x_3\mathbf{j})(y_0\mathbf{j} + y_1\mathbf{k} - y_2 - y_3\mathbf{i}) \\ &= (x_1y_2 - x_2y_1 + x_0y_3 + x_3y_0) + (-x_0y_2 - x_2y_0 + x_1y_3 - x_3y_1)\mathbf{i} \\ &\quad + (-x_1y_0 - x_0y_1 + x_3y_2 - x_2y_1)\mathbf{j} + (x_0y_0 - x_1y_1 - x_2y_2 - x_3y_3)\mathbf{k}\end{aligned}$$

Die entsprechende Identität ist

$$\begin{aligned}&(x_0^2 + x_1^2 + x_2^2 + x_3^2)(y_0^2 + y_1^2 + y_2^2 + y_3^2) = \\ &\quad = (x_1y_2 - x_2y_1 + x_0y_3 + x_3y_0)^2 + (-x_0y_2 - x_2y_0 + x_1y_3 - x_3y_1)^2 \\ &\quad + (-x_1y_0 - x_0y_1 + x_3y_2 - x_2y_1)^2 + (x_0y_0 - x_1y_1 - x_2y_2 - x_3y_3)^2\end{aligned}$$

Beispiele der Identität (*) für $n = 8$ (die von der "Standard"-Identität verschieden sind) führen wir hier, weil sie umfangreich sind, nicht an. Ihr Auffinden bereitet aber keine prinzipiellen Schwierigkeiten.

3.19 Satz von Frobenius

3.19.1 Formulierung des Satzes von Frobenius

Eine der klassischen Aufgaben der Theorie der Algebren ist das Auffinden aller Algebren mit Division. Ungeachtet ihres, wie es scheint, fundamentalen Charakters (aber auch ungeachtet dessen, dass sich eine Reihe von Fragen aus anderen Gebieten der Mathematik, zum Beispiel der Topologie, auf die Lösung dieser Aufgabe stützt) wurde diese Aufgabe in vollem Umfang bis in unsere Zeit nicht gelöst.

Ein wichtiges Resultat wurde erst vor nicht allzu langer Zeit erhalten. Es besteht darin, dass die Dimension jeder solcher Algebren gleich einer der Zahlen 1, 2, 4 oder 8 ist. Obwohl, wie hieraus ersichtlich, die Dimension von Algebren mit Division nicht allzu groß ist, gibt es trotzdem selbst jetzt noch keinen vollständigen Überblick über diese Algebren.

Wenn wir jedoch außer der Existenz der Division noch andere Forderungen natürlicher Art an die gesuchte Algebra stellen, dann wird natürlich unsere Aufgabe bedeutend leichter. Im Jahre 1878 bewies der deutsche Mathematiker G. Frobenius den folgenden bemerkenswerten Satz.

Satz (von Frobenius). Jede assoziative Algebra mit Division ist einer der drei Algebren isomorph: der Algebra der reellen Zahlen, der Algebra der komplexen Zahlen oder der Algebra der Quaternionen.

In der Folge wurde ein allgemeineres Ergebnis gefunden, das man verallgemeinerten Satz von Frobenius nennen kann.

Verallgemeinerter Satz von Frobenius. Jede alternative Algebra mit Division ist einer der vier Algebren isomorph: der Algebra der reellen Zahlen, der komplexen Zahlen, der Quaternionen oder der Oktaven.

Wir erinnern daran, dass eine Algebra alternativ genannt wird, wenn für je zwei Elemente **a** und **b** die Gleichungen

$$(\mathbf{ab})\mathbf{b} = \mathbf{a}(\mathbf{bb}) \qquad \text{und} \qquad (\mathbf{bb})\mathbf{a} = \mathbf{b}(\mathbf{ba})$$

richtig sind. Es ist offensichtlich, dass jede assoziative Algebra automatisch alternativ ist, deshalb geht der Satz von Frobenius aus dem verallgemeinerten Satz von Frobenius hervor (man muss berücksichtigen, dass die Algebra der Oktaven nicht assoziativ ist).

Um die beiden oben formulierten Sätze zu beweisen, zählen wir zuerst einige Eigenschaften einer assoziativen Algebra mit Division auf. Danach wird gezeigt, wie man aus diesen Eigenschaften den Satz von Frobenius ableitet. Der Beweis dieser Eigenschaften wird danach angegeben werden.
Im letzten Punkt des Paragraphen wird unter Verwendung des Satzes von Hurwitz der Beweis des verallgemeinerten Satzes von Frobenius angegeben.

3.19.2 Drei Behauptungen über Eigenschaften jeder assoziativen Algebra mit Division

Behauptung I. Die Algebra $\mathscr{A}$ enthält ein Einselement $\mathbf{1}$.

Behauptung II. Wenn das Element $\mathbf{a} \in \mathscr{A}$ nicht proportional zu $\mathbf{1}$ ist, dann bildet die Gesamtheit $\mathscr{K}_a$ der Elemente der Form

$$\alpha\mathbf{1} + \beta\mathbf{a}$$

eine Unteralgebra, die der Algebra der komplexen Zahlen isomorph ist.

Behauptung III. Wenn die Elemente $\mathbf{a}_1 \in \mathscr{A}$ und $\mathbf{a}_2 \in \mathscr{A}$ nicht gleichzeitig einer Unteralgebra $\mathscr{K}_a$ angehören, dann bildet die Gesamtheit $\mathscr{Q}_{a_1,a_2}$ der Elemente der Form

$$\alpha\mathbf{1} + \beta\mathbf{a}_1 + \gamma\mathbf{a}_2 + \delta\mathbf{a}_1\mathbf{a}_2$$

eine Unteralgebra, die der Algebra der Quaternionen isomorph ist.

Wir bemerken, dass in der Beweisführung der Behauptung III folgender Sachverhalt festgestellt wird: wenn $\mathbf{b}_1$ und $\mathbf{b}_2$ zwei Elemente sind, deren Quadrat gleich -1 ist, dann gilt

$$\mathbf{b}_1\mathbf{b}_2 + \mathbf{b}_2\mathbf{b}_1 = \lambda\mathbf{1} \tag{1}$$

wobei λ eine reelle Zahl ist.

3.19.3 Beweis des Satzes von Frobenius

Wenn wir von den Behauptungen I, II und III ausgehen, bereitet es keine Schwierigkeiten mehr, den Satz von Frobenius zu beweisen.

Es möge $\mathscr{A}$ eine assoziative Algebra mit Division sein. Gemäß der Behauptung I besitzt die Algebra $\mathscr{A}$ ein Einselement.

Die Elemente der Form $k\mathbf{1}$ bilden eine Unteralgebra $\mathscr{D}$, die der Algebra der reellen Zahlen isomorph ist. Wenn $\mathscr{D}$ nicht mit der ganzen Algebra $\mathscr{A}$ übereinstimmt, dann ist gemäß Behauptung II in $\mathscr{A}$ eine Unteralgebra $\mathscr{K}_a$ enthalten, die der Algebra der komplexen Zahlen isomorph ist.

Wenn $\mathscr{K}_a$ nicht mit der ganzen Algebra $\mathscr{A}$ übereinstimmt, dann ist gemäß Behauptung III in $\mathscr{A}$ eine Unteralgebra $\mathscr{Q}_{a,b}$ enthalten, die der Algebra der Quaternionen isomorph ist. In dem Fall, dass $\mathscr{Q}_{a,b}$ mit der ganzen Algebra $\mathscr{A}$ übereinstimmt, braucht man nichts mehr zu beweisen.

Wir nehmen deshalb an, dass ein Element **c** existiert, das nicht $\mathscr{Q}_{a,b}$ angehört, und zeigen, dass dann $\mathscr{A}$ keine Algebra mit Division sein kann.

Wir wählen in der Quaternionenalgebra $\mathscr{Q}_{a,b}$ eine Basis $\mathbf{1}$, **i**, **j**, **k** mit der "Standard"-Multiplikationstafel

$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1, \qquad \mathbf{ij} = -\mathbf{ji} = \mathbf{k}, \quad \mathbf{jk} = -\mathbf{kj} = \mathbf{i}, \quad \mathbf{ki} = -\mathbf{ik} = \mathbf{j}$$

aus. Das Element **c** stellen wir in der Form $p\mathbf{1} + q\mathbf{e}$ dar, wobei $\mathbf{e}^2 = -1$ ist (**e** ist die "imaginäre Einheit" der komplexen Algebra $\mathscr{K}_c$).
Wir formen jetzt das Element **ie** unter Benutzung der Assoziativität der Multiplikation in der Algebra $\mathscr{A}$ sowie der Beziehung (1) um. Wir erhalten

$$\mathbf{ie} = (\mathbf{jk})\mathbf{e} = \mathbf{j}(\mathbf{ke}) = \mathbf{j}(-\mathbf{ek} + \lambda'\mathbf{1}) = -(\mathbf{je})\mathbf{k} + \lambda'\mathbf{j} = -(-\mathbf{ej} + \lambda''\mathbf{1})k + \lambda'\mathbf{j} = \mathbf{ei} - \lambda''\mathbf{k} + \lambda'\mathbf{j}$$

und folglich

$$\mathbf{ie} - \mathbf{ei} = \lambda'\mathbf{j} - \lambda''\mathbf{k}$$

Andererseits gilt, wiederum aufgrund von (1), $\mathbf{ie} + \mathbf{ei} = \lambda'''\mathbf{1}$.
Wenn wir diese zwei Gleichungen addieren, finden wir, dass **ie** ein Element aus $\mathscr{Q}_{a,b}$ ist. Folglich ist $\mathbf{ic} = \mathbf{i}(p\mathbf{1} + q\mathbf{e})$ auch ein Element aus $\mathscr{Q}_{a,b}$. Wir sehen, dass die Multiplikation von **i** mit jedem Element, das nicht $\mathscr{Q}_{a,b}$ angehört, ein Element aus $\mathscr{Q}_{a,b}$ ergibt.

Aber auch in dem Fall, dass $\mathbf{c}' \in \mathscr{Q}_{a,b}$ ist das Produkt $\mathbf{ic}'$ ein Element aus $\mathscr{Q}_{a,b}$. Auf diese Weise ergibt das mit jedem Element der Algebra $\mathscr{A}$ multiplizierte Element **i** ein Element aus $\mathscr{Q}_{a,b}$.
Dies ist aber nicht möglich, wenn $\mathscr{A}$ eine Algebra mit Division ist (die Gleichung $\mathbf{ix} = \mathbf{c}$, wobei **e** nicht in $\mathscr{Q}_{a,b}$ enthalten ist, erweist sich als unlösbar). Damit ist (wenn man die Behauptungen I, II und III als richtig annimmt) der Satz von Frobenius bewiesen.

3.19.4 Beweis der Behauptungen I, II und III

Um den Beweis des Satzes von Frobenius abzuschließen, bleibt uns also nur noch, die Richtigkeit der Behauptungen I, II und III zu beweisen.

Beweis der Behauptung I.
Es möge **a** irgendein von Null verschiedenes Element der Algebra $\mathscr{A}$ sein. Wir betrachten die Gleichung

$$\mathbf{xa} = \mathbf{a}$$

Weil $\mathscr{A}$ eine Algebra mit Division ist, besitzt die niedergeschriebene Gleichung eine und zwar eindeutige Lösung. Wir bezeichnen diese Lösung (d.h. das gesuchte Element **x**) mit **e**. Folglich ist $\mathbf{ea} = \mathbf{a}$.

Wenn wir beide Seiten dieser Gleichung von links mit **b** multiplizieren, erhalten wir $\mathbf{b}(\mathbf{ea}) = \mathbf{ba}$ oder unter Berücksichtigung der Assoziativität der Algebra $\mathscr{A}$ $(\mathbf{be})\mathbf{a} = \mathbf{ba}$. Aufgrund der Eindeutigkeit der Lösung der Gleichung $\mathbf{xa} = \mathbf{ba}$ folgt daraus

$$\mathbf{be} = \mathbf{b}$$

Wenn wir jetzt die erhaltene Beziehung von rechts mit **c** multiplizieren und analog schließen, finden wir

$$\mathbf{ec} = \mathbf{c}$$

Da die Elemente **b** und **c** beliebig sind, bedeuten die letzten zwei Gleichungen, dass das Element **e** das Einselement der Algebra $\mathscr{A}$ ist. Im weiteren werden wir das Einselement der Algebra wie üblich mit $\mathbf{1}$ bezeichnen.

Beweis der Behauptung II.
Für unsere Aufgabe ist es hinreichend zu zeigen, dass das Element **a** der quadratischen Gleichung

$$\mathbf{a}^2 + s\mathbf{a} + t\mathbf{1} = \mathbf{0} \tag{2}$$

mit einer negativen Diskriminante genügt.[20] Wir betrachten die aufeinanderfolgenden Potenzen des Elementes **a**:

$$\mathbf{a}^0 = \mathbf{1}, \mathbf{a}^1, \mathbf{a}^2, \mathbf{a}^3, ..., \mathbf{a}^n$$

wobei n die Dimension der Algebra ist. Aus Satz 2, § 9, geht hervor, dass dieses System aus $n+1$ Vektoren linear abhängig ist, d.h., dass sich eine bestimmte Potenz in die vorhergehenden zerlegen lassen muss:

$$\mathbf{a}^m = k_{m-1}\mathbf{a}^{m-1} + ... + k_2\mathbf{a}^2 + k_1\mathbf{a} + k_0\mathbf{1}$$

Anders ausgedrückt, das Element **a** genügt einer Gleichung m-ten Grades

$$\mathbf{x}^m = k_{m-1}\mathbf{x}^{m-1} + ... + k_2\mathbf{x}^2 + k_1\mathbf{x} + k_0\mathbf{1} = \mathbf{0}$$

Dem Ausdruck, der auf der linken Seite dieser Gleichung steht, kann man das gewöhnliche Polynom m-ten Grades

$$x^m = k_{m-1}x^{m-1} + ... + k_2x^2 + k_1x + k_0$$

zuordnen. Wir bezeichnen es kurz mit $P(x)$. Wie bekannt ist, kann jedes Polynom mit reellen Koeffizienten in das Produkt von Polynomen ersten und zweiten Grades zerlegt werden.
Dabei kann man, wie sich versteht, annehmen, dass jeder Faktor zweiten Grades nicht mehr zerlegbar in das Produkt zweier Faktoren ersten Grades ist. Also ist

$$P(x) = P_1(x)P_2(x)...P_s(x) \tag{3}$$

wobei jeder der Faktoren der rechten Seite entweder ein Polynom ersten Grades oder ein nichtzerlegbares Polynom zweiten Grades ist.

[20] In der Tat, aus (2) folgt $\mathbf{a}^2 = -s\mathbf{a} - t\mathbf{1}$, also ist die Menge der Elemente der Form $\alpha\mathbf{1} + \beta\mathbf{a}$ bezüglich der Multiplikation abgeschlossen. Damit ist die betrachtete Menge ein hyperkomplexes System der Dimension 2. Gemäß § 2 ist für

$$\frac{s^2}{4} - t < 0$$

(Negativität der Diskriminante) ein solches System dem System der komplexen Zahlen isomorph.

Um die weiteren Überlegungen zu verstehen, muss sich der Leser die Bedeutung der Gleichung (3) deutlich vorstellen.

Jedes der Polynome $P_1(z), ..., P_s(x)$ stellt eine Summe der zwei oder drei Glieder

$$x + t \qquad \text{oder} \qquad x^2 + sx + t$$

dar. Die Gleichung (3) sagt aus, dass man, wenn man die Ausdrücke $P_1(x), ..., P_s(x)$ nach der Regel der Multiplikation einer Summe mit einer Summe miteinander multipliziert, danach die Formel

$$x^k \cdot x^l = x^{k+l}$$

verwendet und nach ähnlichen Gliedern ordnet, dann den Ausdruck $P(x)$ erhält. Die Regeln der Grundrechenarten für die Potenzen des Elementes **a** sind aber die gleichen wie für die Potenzen der Unbekannten x:

$$\mathbf{a}^k \cdot \mathbf{a}^l = \mathbf{a}^{k+l}$$

(da doch die Algebra $\mathscr{A}$ als assoziativ vorausgesetzt wurde). Daraus ist ersichtlich, dass die Gleichung (3) gültig bleibt, wenn man das Element **a** an die Stelle der Unbekannten x setzt:

$$P(\mathbf{a}) = P_1(\mathbf{a})P_2(\mathbf{a})...P_s(\mathbf{a})$$

Da aber $P(\mathbf{a}) = \mathbf{0}$ ist, gilt

$$P_1(\mathbf{a})P_2(\mathbf{a})...P_s(\mathbf{a}) = \mathbf{0} \tag{4}$$

Wir verwenden weiter, dass $\mathscr{A}$ eine Algebra mit Division ist. Aus dieser Tatsache geht hervor, wenn das Produkt mehrerer Elemente gleich Null ist, dann ist mindestens einer der Faktoren gleich 0 (tatsächlich, wenn $\mathbf{uv} = \mathbf{0}$ und $\mathbf{u} \neq \mathbf{0}$ ist, dann muss aufgrund der Eindeutigkeit der Lösung der Gleichung $\mathbf{ux} = \mathbf{0}$ $\mathbf{v} = \mathbf{0}$ sein).
In Anwendung auf (4) bedeutet dies, dass für einen bestimmten Index i

$$P_i(\mathbf{a}) = \mathbf{0}$$

ist, d.h., dass das Element **a** einer Gleichung ersten oder zweiten Grades genügt. Eine Gleichung ersten Grades kann man für **a** jedoch nicht erhalten, da dann

$$\mathbf{a} + t\mathbf{1} = \mathbf{0}$$

ist, d.h., das Element **a** ist proportional zu $\mathbf{1}$ entgegen der Bedingung des Lemmas.
Folglich genügt a einer bestimmten quadratischen Gleichung (2). Weil dabei das Polynom zweiten Grades $P_i(x)$ nicht zerlegbar ist, muss seine Diskriminante eine negative Zahl sein. Die Behauptung II ist bewiesen.

Beweis der Behauptung III.
Wir wählen in der Unteralgebra $\mathscr{K}_{a_1}$ ein solches Element $\mathbf{b}_1$ aus, dass $\mathbf{b}_1^2 = -1$ ist ($\mathbf{b}_1$ ist die "imaginäre Einheit" in der komplexen Algebra $\mathscr{K}_{a_1}$).
In analoger Weise wählen wir in der Unteralgebra $\mathscr{K}_{a_2}$, ein Element $\mathbf{b}_2$ aus, derart, dass $\mathbf{b}_2^2 = -1$ ist. Weil $\mathbf{b}_1$ und $\mathbf{b}_2$ sich von $\mathbf{a}_1$ und $\mathbf{a}_2$ (entsprechend) durch Summanden, die ein Vielfaches von $\mathbf{1}$ sind, unterscheiden, stimmt die Gesamtheit der Elemente der Form

$$\alpha\mathbf{1} + \beta\mathbf{a}_1 + \gamma\mathbf{a}_2 + \delta\mathbf{a}_1\mathbf{a}_2$$

mit der Gesamtheit der Elemente der Form

$$\alpha'\mathbf{1} + \beta'\mathbf{b}_1 + \gamma'\mathbf{b}_2 + \delta'\mathbf{b}_1\mathbf{b}_2$$

überein, anders ausgedrückt, $\mathscr{Q}_{a_1,a_2}$ stimmt mit $\mathscr{Q}_{b_1,b_2}$ überein.
Weiter kann man leicht sehen, wenn

$$\mathbf{e}_1 = \mathbf{b}_1 \qquad , \qquad \mathbf{e}_2 = k_1\mathbf{b}_1 + k_2\mathbf{b}_2$$

ist, wobei $k_2 \neq 0$ ist, dann ist die Menge $\mathscr{Q}_{e_1,e_2}$ dieselbe wie die Menge $\mathscr{Q}_{b_1,b_2}$ und folglich auch wie die Menge $\mathscr{Q}_{a_1,a_2}$.
Wir werden zeigen, dass man die Zahlen k_1 und k_2 so wählen kann, dass die Gleichungen

$$\mathbf{e}_1^2 = -1, \qquad \mathbf{e}_2^2 = -1, \qquad (\mathbf{e}_1\mathbf{e}_2)^2 = -1 \tag{5}$$

gelten (wobei die erste Gleichung für jede Wahl von k_1 und k_2 richtig ist). Zu diesem Zweck notieren wir, dass

$$(\mathbf{b}_1 + \mathbf{b}_2)^2 = \mathbf{b}_1^2 + \mathbf{b}_2^2 + (\mathbf{b}_1\mathbf{b}_2 + \mathbf{b}_2\mathbf{b}_1) = -2 \cdot \mathbf{1} + (\mathbf{b}_1\mathbf{b}_2 + \mathbf{b}_2\mathbf{b}_1)$$

gilt, andererseits aber muss sich das Quadrat des Elementes $\mathbf{b}_1 + \mathbf{b}_2$ in $\mathbf{1}$ und $\mathbf{b}_1 + \mathbf{b}_2$ zerlegen lassen:

$$(\mathbf{b}_1 + \mathbf{b}_2)^2 = p\mathbf{1} + q(\mathbf{b}_1 + \mathbf{b}_2)$$

Folglich haben wir

$$\mathbf{b}_1\mathbf{b}_2 + \mathbf{b}_2\mathbf{b}_1 = (p+2)\mathbf{1} + q(\mathbf{b}_1 + \mathbf{b}_2) \tag{6}$$

Analog gilt

$$(\mathbf{b}_1 + 2\mathbf{b}_2)^2 = \mathbf{b}_1^2 + 4\mathbf{b}_2^2 + 2(\mathbf{b}_1\mathbf{b}_2 + \mathbf{b}_2\mathbf{b}_1) = -5 \cdot \mathbf{1} + 2(\mathbf{b}_1\mathbf{b}_2 + \mathbf{b}_2\mathbf{b}_1)$$

und

$$(\mathbf{b}_1 + 2\mathbf{b}_2)^2 = p'\mathbf{1} + q'(\mathbf{b}_1 + 2\mathbf{b}_2)$$

Folglich ist

$$\mathbf{b}_1\mathbf{b}_2 + \mathbf{b}_2\mathbf{b}_1 = \frac{1}{2}(p'+5)\mathbf{1} + \frac{1}{2}q'(\mathbf{b}_1 + 2\mathbf{b}_2)$$

Wenn $q \neq 0$ wäre, dann würden wir, wenn wir beide Ausdrücke für $\mathbf{b}_1\mathbf{b}_2 + \mathbf{b}_2\mathbf{b}_1$ gleichsetzen, feststellen, dass $\mathbf{b}_1$ sich von $\mathbf{b}_2$ durch ein Element unterscheidet, das ein Vielfaches von $\mathbf{1}$ ist, d.h., $b_2 \in \mathscr{K}_{b_1}$, was nach der Voraussetzung ausgeschlossen ist. Folglich ist $q = 0$, und die Gleichung (6) ergibt

$$\mathbf{b}_1\mathbf{b}_2 + \mathbf{b}_2\mathbf{b}_1 = \lambda\mathbf{1} \tag{1}$$

Wenn also $\mathbf{b}_1$ und $\mathbf{b}_2$ zwei Elemente sind, deren Quadrate gleich -1 sind, dann ist die Gleichung (1) richtig.

Es ist jetzt nicht schwierig, die gesuchten Elemente $\mathbf{e}_1$ und $\mathbf{e}_2$ zu bestimmen. Wir betrachten dazu das Element

$$\mathbf{c} = \lambda\mathbf{b}_1 + 2\mathbf{b}_2$$

wobei λ der Gleichung (1) entnommen ist. Sein Quadrat ist gleich

$$\mathbf{c}^2 = -\lambda^2\mathbf{1} - 4 \cdot \mathbf{1} + 2\lambda(\mathbf{b}_1\mathbf{b}_2 + \mathbf{b}_2\mathbf{b}_1) = (\lambda^2 - 4) \cdot \mathbf{1} \tag{7}$$

deshalb muss $\lambda^2 - 4 < 0$ sein.[21]

[21]Wenn $\rho = \lambda^2 - 4 \geq 0$ wäre, dann würde aus $\mathbf{c}^2 = \rho\mathbf{1}$ folgen

$$(\mathbf{c} - \sqrt{\rho} \cdot \mathbf{1})(\mathbf{c} + \sqrt{\rho} \cdot \mathbf{1}) = \mathbf{0}$$

d.h, $\mathbf{c} = \sqrt{\rho}\mathbf{1}$ oder $\mathbf{c} = -\sqrt{\rho}\mathbf{1}$. Dies ist aber nicht möglich, weil $\mathbf{b}_1$ und $\mathbf{b}_2$ nicht in der gleichen komplexen Unteralgebra liegen.

Wir setzen

$$\mathbf{e}_2 = \frac{1}{\sqrt{4-\lambda^2}}\mathbf{c}$$

dann folgt aus (7), dass $\mathbf{e}_2^2 = -1$ ist, d.h., die zweite der Gleichungen (5). Um die dritte aufzustellen, bemerken wir zuerst, dass

$$\mathbf{e}_1\mathbf{e}_2 + \mathbf{e}_2\mathbf{e}_1 = 0 \tag{8}$$

ist. Dies folgt aus

$$\begin{aligned}
\mathbf{e}_1\mathbf{e}_2 + \mathbf{e}_2\mathbf{e}_1 &= \frac{1}{\sqrt{4-\lambda^2}}(\mathbf{b}_1(\lambda\mathbf{b}_1 + 2\mathbf{b}_2) + (\lambda\mathbf{b}_1 + 2\mathbf{b}_2)\mathbf{b}_1) \\
&= \frac{1}{\sqrt{4-\lambda^2}}(-2\lambda\cdot\mathbf{1} + 2((\mathbf{b}_1\mathbf{b}_2 + \mathbf{b}_2\mathbf{b}_1)) = 0
\end{aligned}$$

Mit (8) erhalten wir

$$(\mathbf{e}_1\mathbf{e}_2)^2 = (\mathbf{e}_1\mathbf{e}_2)(\mathbf{e}_1\mathbf{e}_2) = (\mathbf{e}_1\mathbf{e}_2)(-\mathbf{e}_2\mathbf{e}_1) = -(\mathbf{e}_1\mathbf{e}_2^2)\mathbf{e}_1 = \mathbf{e}_1^2 = -1 \tag{9}$$

was den Beweis der Gleichungen (5) abschließt.

Wir werden jetzt feststellen, dass die Menge $\mathscr{Q}_{e_1,e_2}$ der Elemente der Form

$$\alpha\mathbf{1} + \beta\mathbf{e}_1 + \gamma\mathbf{e}_2 + \delta\mathbf{e}_1\mathbf{e}_2$$

(die, wie wir bereits sagten, mit $\mathscr{Q}_{a_1,a_2}$ übereinstimmt) eine Unteralgebra der Algebra $\mathscr{A}$ ist. Dazu genügt es zu überprüfen, dass man das Produkt von zwei beliebigen Elementen aus dem Quadrupel

$$\mathbf{1}, \quad \mathbf{e}_1, \quad \mathbf{e}_2, \quad \mathbf{e}_1\mathbf{e}_2 \tag{10}$$

in diese vier Elemente zerlegen kann. Uns sind schon außer den folgenden alle Produkte bekannt:

$$\mathbf{e}_1(\mathbf{e}_1\mathbf{e}_2), \quad (\mathbf{e}_1\mathbf{e}_2)\mathbf{e}_1, \quad \mathbf{e}_2(\mathbf{e}_1\mathbf{e}_2), \quad (\mathbf{e}_1\mathbf{e}_2)\mathbf{e}_2$$

Jedes von ihnen lässt sich leicht berechnen:

$$\begin{aligned}
&\mathbf{e}_1(\mathbf{e}_1\mathbf{e}_2) = \mathbf{e}_1^2\mathbf{e}_2 = -\mathbf{e}_2 \\
&(\mathbf{e}_1\mathbf{e}_2)\mathbf{e}_1 = -(\mathbf{e}_2\mathbf{e}_1)\mathbf{e}_1 = -\mathbf{e}_2\mathbf{e}_1^2 = \mathbf{e}_2 \\
&\mathbf{e}_2(\mathbf{e}_1\mathbf{e}_2) = -\mathbf{e}_2(\mathbf{e}_2\mathbf{e}_1) = -\mathbf{e}_2^2\mathbf{e}_1 = \mathbf{e}_1 \\
&(\mathbf{e}_1\mathbf{e}_2)\mathbf{e}_2 = \mathbf{e}_1\mathbf{e}_2^2 = -\mathbf{e}_1
\end{aligned} \tag{11}$$

Die uns interessierende Menge $\mathscr{Q}_{e_1,e_2}$ ist also eine Unteralgebra.
Es bleibt noch zu überprüfen, dass diese Unteralgebra der Algebra der Quaternionen isomorph ist. Dazu beweisen wir erstens, dass das Quadrupel der Elemente (10) in dieser Unteralgebra eine Basis bildet, und zweitens, dass die Multiplikationstafel für diese Basis genau die gleiche wie die für die Basis **1**, **i**, **j**, **k** in der Algebra der Quaternionen ist.

Zum Beweis dessen, dass die Elemente (10) eine Basis bilden, bemerken wir, dass jedes Element der Unteralgebra $\mathscr{Q}_{e_1,e_2}$ durch sie dargestellt wird. Folglich bleibt nur noch zu beweisen, dass die betrachteten Elemente linear unabhängig sind oder (siehe § 8), dass keines der vier Elemente (10) durch die ihm vorhergehenden Elemente dieses Quadrupels dargestellt wird.

Das Element $\mathbf{e}_2$ wird aber nicht durch $\mathbf{e}_1, \mathbf{1}$ dargestellt (dies folgt aus der Tatsache, dass $\mathbf{e}_1$ und $\mathbf{e}_2$ nicht gleichzeitig einer Unteralgebra $\mathscr{K}_a$ angehören).
Es bleibt deshalb zu beweisen, dass $\mathbf{e}_1\mathbf{e}_2$ nicht durch $\mathbf{e}_2, \mathbf{e}_1, \mathbf{1}$ dargestellt wird, d.h., dass eine Gleichung der Form

$$\mathbf{e}_1\mathbf{e}_2 = p\mathbf{e}_2 + q\mathbf{e}_1 + r\mathbf{1} \tag{12}$$

nicht möglich ist. Wir nehmen an, dass eine solche Beziehung gilt.
Dann ist keine der Zahlen p und q gleich Null. (Wenn zum Beispiel $p = 0$ wäre, so würden wir durch Multiplizieren beider Seiten von (12) mit $\mathbf{e}_1$ von links erhalten, dass $\mathbf{e}_2$ durch $\mathbf{e}_1$ und $\mathbf{1}$ dargestellt werden kann, was nicht möglich ist.) Wenn wir beide Seiten von (12) von links mit $\mathbf{e}_1$ multiplizieren, erhalten wir

$$-\mathbf{e}_2 = p\mathbf{e}_1\mathbf{e}_2 - q\mathbf{1} + r\mathbf{e}_1 \qquad \text{oder} \qquad \mathbf{e}_1\mathbf{e}_2 = -\frac{1}{p}\mathbf{e}_2 - \frac{r}{p}\mathbf{e}_1 + \frac{q}{p}\mathbf{1}$$

Wenn wir von dem einen Ausdruck für $\mathbf{e}_1\mathbf{e}_2$ den anderen subtrahieren, erhalten wir

$$\left(p + \frac{1}{p}\right)\mathbf{e}_2 + \left(q + \frac{r}{p}\right)\mathbf{e}_1 + \left(r + \frac{q}{p}\right)\mathbf{1} = \mathbf{0}$$

In dieser Gleichung muss der Koeffizient von $\mathbf{e}_2$ gleich Null sein (sonst würden wir feststellen, dass $\mathbf{e}_2$ durch $\mathbf{e}_1$ und $\mathbf{1}$ dargestellt werden kann), was für kein reelles p möglich ist. Auf diese Weise bilden die Elemente $\mathbf{1}, \mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3$ wobei $\mathbf{e}_3 = \mathbf{e}_2\mathbf{e}_1$ ist, eine Basis der Unteralgebra $\mathscr{Q}_{e_1,e_2}$.
Um festzustellen, dass die Unteralgebra $\mathscr{Q}_{e_1,e_2}$, der Algebra $\mathscr{Q}$ der Quaternionen isomorph ist, bleibt noch ein letzter Schritt zu gehen, zu zeigen, dass die Multiplikationstafel für die Algebra $\mathscr{Q}_{e_1,e_2}$ in der Basis

$$\mathbf{1}, \mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3$$

genau die gleiche wie die für die Algebra $\mathscr{Q}$ in der Basis

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

ist. Dies ist aber direkt aus den Beziehungen (5), (8) und (11) ersichtlich.

3.19.5 Beweis des verallgemeinerten Satzes von Frobenius mit Hilfe des Satzes von Hurwitz

Wir werden zuerst eine Bemerkung bezüglich der Definition einer alternativen Algebra machen. Wir nannten die Erfüllung der Identitäten

$$(\mathbf{ab})\mathbf{b} = \mathbf{a}(\mathbf{bb}) \qquad \text{und} \qquad \mathbf{b}(\mathbf{ba}) = (\mathbf{bb})\mathbf{a}$$

Alternativität. Außer dieser Definition gibt es jedoch noch eine andere, die wir die zweite Definition der Alternativität nennen wollen. Sie besteht aus folgendem.

Es mögen $\mathbf{a}$ und $\mathbf{b}$ zwei beliebige Elemente der Algebra $\mathscr{A}$ sein. Wir werden alle möglichen Produkte betrachten, die aus ihnen gebildet wurden. Wenn jedes solches Produkt nicht von der Anordnung der Klammern abhängt, wird die Algebra $\mathscr{A}$ alternativ genannt.
Zum Beispiel bedeutet dies, dass

$$(\mathbf{ab})\mathbf{b} = \mathbf{a}(\mathbf{bb}) \qquad , \qquad (\mathbf{ab})(\mathbf{ba}) = (\mathbf{a}(\mathbf{bb}))\mathbf{a}$$

u.ä.m. ist.

Offensichtlich folgt aus der zweiten Definition der Alternativität die erste. Man kann zeigen, dass auch umgekehrt aus der ersten Definition die zweite folgt (diese Tatsache bildet den Inhalt eines Satzes von Artin, den wir hier nicht beweisen werden).

Zum Beweis des verallgemeinerten Satzes von Frobenius werden wir von der zweiten Definition der Alternativität ausgehen. Auf diese Weise werden wir, strenggenommen, den folgenden Satz beweisen:

Wenn eine Algebra $\mathscr{A}$ mit Division von der Art ist, dass jedes Produkt von zwei beliebigen Elementen **a** und **b** nicht von der Anordnung der Klammern abhängt, dann ist die Algebra $\mathscr{A}$ isomorph einer der vier Algebren: der Algebra der reellen Zahlen, der komplexen Zahlen, der Quaternionen oder der Oktaven.

Als wichtiges Moment des Beweises erscheint die Tatsache, dass die Behauptungen I, II und III über die Eigenschaften einer assoziativen Algebra mit Division auch im Falle einer alternativen Algebra mit Division richtig bleiben. Was die Behauptungen II und III betrifft, so braucht man in ihren oben angeführten Beweisen keine Zeile zu verändern.

In der Tat, wenn man diese Beweise aufmerksam durchsieht, so zeigt sich, dass die Assoziativität einer Algebra nur an zwei Stellen benutzt wurde: in der Formel $\mathbf{a}^n \cdot \mathbf{a}^m = \mathbf{a}^{n+m}$ für die Multiplikation von Potenzen und in der Beziehung $(\mathbf{e}_1\mathbf{e}_2)(\mathbf{e}_2\mathbf{e}_1) = (\mathbf{e}_1\mathbf{e}_2^2)\mathbf{e}_1$, die in der Kette der Gleichungen (9) gebraucht wurde.

Es ist klar, dass auch das übrige im Falle einer alternativen Algebra richtig bleibt. Der Beweis der Behauptung I muss für den alternativen Fall etwas verändert werden.
Indem wir das Element **e** aus Gleichung $\mathbf{xa} = \mathbf{a}$ bestimmen und beide Seiten der Gleichung $\mathbf{ea} = \mathbf{a}$ von links mit **e** multiplizieren, erhalten wir $\mathbf{e}(\mathbf{ea}) = \mathbf{ea}$ oder unter Berücksichtigung der Alternativität $(\mathbf{ee})\mathbf{a} = \mathbf{ea}$.
Daraus folgt, dass $\mathbf{ee} = \mathbf{e}$ ist.

Wiederum erhalten wir aufgrund der Alternativität $(\mathbf{be})\mathbf{e} = \mathbf{b}(\mathbf{ee})$ und $\mathbf{e}(\mathbf{ec}) = (\mathbf{ee})\mathbf{c}$ d.h., $(\mathbf{be})\mathbf{e} = \mathbf{be}$ und $\mathbf{e}(\mathbf{ec}) = \mathbf{ec}$.
Daraus folgen $\mathbf{be} = \mathbf{b}$ und $\mathbf{ec} = \mathbf{c}$. Folglich ist **e** das Einselement der Algebra.

Um jetzt den verallgemeinerten Satz von Frobenius zu beweisen, könnte man den gleichen Weg gehen wie auch bei Beweis des Satzes von Frobenius, d.h., zeigen, wenn die von uns betrachtete alternative Algebra $\mathscr{A}$ durch die Unteralgebra $\mathscr{Q}_{a,b}$ nicht ausgeschöpft wird, dann ist in ihr eine Unteralgebra enthalten, die der Algebra der Oktaven isomorph ist.
Danach würde nur noch zu beweisen sein, dass diese Unteralgebra mit der ganzen Algebra übereinstimmt. Ein solches Beweisverfahren ist möglich, jedoch würde es ziemlich lange Überlegungen erfordern.

Deshalb wählen wir einen anderen Weg, und zwar versuchen wir zu beweisen, dass die Algebra $\mathscr{A}$ normiert ist. Daraus wird nach dem Satz von Hurwitz das von uns benötigte Resultat folgen.

Wir führen auf folgende Weise in der Algebra $\mathscr{A}$ die Operation der Konjugation ein. Wenn ein Element **a** proportional zu $\mathbf{1}$ ist, dann gilt $\overline{\mathbf{a}} = \mathbf{a}$. Wenn a nicht proportional zu 1 ist, dann ist es, gemäß Behauptung II, in der komplexen Unteralgebra $\mathscr{K}_a$ enthalten.
In dieser Unteralgebra ist das zum Element **a** konjugierte Element $\overline{\mathbf{a}}$ enthalten, das wir auch als das Element in der Algebra $\mathscr{A}$ zu **a** konjugierte Element nehmen. Aus der Definition von

$\overline{\mathbf{a}}$ geht direkt hervor, dass $\overline{\overline{\mathbf{a}}} = \mathbf{a}$ ist, aber auch

$$\overline{k\mathbf{a}} = k\overline{\mathbf{a}} \tag{13}$$

wobei k eine beliebige reelle Zahl ist.

Für die Ableitung anderer Eigenschaften der Konjugation ist es notwendig, eine Frage zu klären. Das Element $\mathbf{a}$ möge nicht proportional zu $\mathbf{1}$ sein. Wir betrachten irgendeine Quaternionenunteralgebra $\mathscr{Q}_{a_1,a_2}$, die $\mathbf{a}$ enthält.
In dieser Unteralgebra gibt es für $\mathbf{a}$ auch ein konjugiertes Element $\tilde{\mathbf{a}}$. Wird es mit dem oben definierten Element übereinstimmen? Wir werden zeigen, dass dies der Fall ist.

Die zueinander konjugierten Elemente $\mathbf{a}$ und $\overline{\mathbf{a}}$ der Algebra der komplexen Zahlen genügen den Bedingungen

$$\mathbf{a} + \overline{\mathbf{a}} = (\text{reelle Zahl}) \cdot \mathbf{1} \qquad \text{und} \qquad \mathbf{a} \cdot \overline{\mathbf{a}} = (\text{reelle Zahl}) \cdot \mathbf{1} \tag{14,15}$$

Die konjugierten Elemente $\mathbf{a}$ und $\tilde{\mathbf{a}}$ in der Algebra der Quaternionen genügen den analogen Bedingungen:

$$\mathbf{a} + \tilde{\mathbf{a}} = (\text{reelle Zahl}) \cdot \mathbf{1} \qquad \text{und} \qquad \mathbf{a} \cdot \tilde{\mathbf{a}} = (\text{reelle Zahl}) \cdot \mathbf{1} \tag{14',15'}$$

Durch Subtrahieren der entsprechenden Gleichungen (14') und (15') von den Gleichungen (14) und (15) erhalten wir

$$\overline{\mathbf{a}} - \tilde{\mathbf{a}} = (\text{reelle Zahl}) \cdot \mathbf{1} \qquad \text{und} \qquad \mathbf{a}(\overline{\mathbf{a}} - \tilde{\mathbf{a}}) = (\text{reelle Zahl}) \cdot \mathbf{1}$$

Wenn $\overline{\mathbf{a}} \neq \tilde{\mathbf{a}}$ ist, dann geht aus diesen Beziehungen hervor, dass das Element $\mathbf{a}$ proportional zu $\mathbf{1}$ ist, was der Voraussetzung widerspricht. Auf diese Weise ist das Element, das zu $\mathbf{a}$ konjugiert ist, ein und dasselbe, unabhängig davon, ob wir $\mathbf{a}$ als Element einer komplexen Unteralgebra $\mathscr{K}_a$ (d.h. als eine komplexe Zahl) oder als Element irgendeiner Unteralgebra $\mathscr{Q}_{a_1,a_2}$ (d.h. als Quaternion) ansehen.

Wir bemerken zugleich, dass es sich beim absoluten Betrag des Elementes $\mathbf{a}$ ebenso verhält. Da (absoluter Betrag von $\mathbf{a})^2 = \mathbf{a}\overline{\mathbf{a}}$ sowohl im Falle der komplexen Zahlen als auch im Falle der Quaternionen gilt, hängt der absolute Betrag des Elementes $\mathbf{a}$ nicht davon ab, ob wir $\mathbf{a}$ als Element der komplexen Unteralgebra oder der Quaternionenunteralgebra betrachten.

Aus dem, was von uns bezüglich der Konjugation bewiesen wurde, folgt leicht, dass für zwei beliebige Elemente $\mathbf{a}$ und $\mathbf{b}$ der Algebra $\mathscr{A}$ die Gleichungen

$$\overline{\mathbf{a} + \mathbf{b}} = \overline{\mathbf{a}} + \overline{\mathbf{b}} \qquad \text{und} \qquad \overline{\mathbf{ab}} = \overline{\mathbf{b}}\,\overline{\mathbf{a}} \tag{16,17}$$

gelten. In der Tat, wenn $\mathbf{a}$ und $\mathbf{b}$ einer komplexen Unteralgebra angehören (d.h. $\mathscr{K}_a$ stimmt mit $\mathscr{K}_b$ überein), dann drücken die niedergeschriebenen Gleichungen die Eigenschaften der Konjugation in dieser Unteralgebra aus:
Wenn $\mathbf{b}$ nicht in $\mathscr{K}_a$ enthalten ist, sind diese Gleichungen wiederum richtig, ebenso die Eigenschaften der Konjugation in $\mathscr{Q}_{a,b}$.

Aus Formel (17) und aus $\overline{\overline{\mathbf{b}}} = \mathbf{b}$ geht hervor, dass das Element, das zu $\mathbf{a}\overline{\mathbf{b}}$ konjugiert ist, gleich $\mathbf{b}\overline{\mathbf{a}}$ ist; folglich gilt

$$\mathbf{a}\overline{\mathbf{b}} + \mathbf{b}\overline{\mathbf{a}} = (\text{reelle Zahl}) \cdot \mathbf{1}$$

Wir definieren in der Algebra $\mathscr{A}$ ein Skalarprodukt $(\mathbf{a}, \mathbf{b})$ mit Hilfe der Formel

$$\mathbf{a}\overline{\mathbf{b}} + \mathbf{b}\overline{\mathbf{a}} = 2(\mathbf{a},\mathbf{b}) \cdot \mathbf{1}$$

Dass der Ausdruck $(\mathbf{a},\mathbf{b})$ alle Eigenschaften des Skalarproduktes besitzt, lässt sich leicht überprüfen. Wir rufen diese Eigenschaften in Erinnerung:

1) $(\mathbf{a},\mathbf{a}) > 0$ wenn $\mathbf{a} \neq \mathbf{0}$ und $(\mathbf{0},\mathbf{0}) = 0$;
2) $(\mathbf{a},\mathbf{b}) = (\mathbf{b},\mathbf{a})$;
3) $(\mathbf{a}, k\mathbf{b}) = k(\mathbf{a}, \mathbf{b})$;
4) $(\mathbf{a},\mathbf{b}_1 + \mathbf{b}_2) = (\mathbf{a},\mathbf{b}_1) + (\mathbf{a},\mathbf{b}_2)$.

Im gegebenen Fall ist die Eigenschaft 2) offensichtlich. Die Eigenschaften 3) und 4) gehen direkt aus den Formeln (13) und (16) hervor.
Zum Beweis der Eigenschaft 1) muss man schreiben

$$(\mathbf{a},\mathbf{a}) \cdot \mathbf{1} = \mathbf{a}\overline{\mathbf{a}} = (\text{absoluter Betrag}\mathbf{a})^2 \cdot \mathbf{1} \tag{18}$$

und berücksichtigen, dass der absolute Betrag der komplexen Zahl $\mathbf{a}$ positiv ist, wenn $\mathbf{a} \neq \mathbf{0}$ ist und gleich Null, wenn $\mathbf{a} = \mathbf{0}$ ist. Wir bemerken, dass aus den Gleichungen (18) folgt

$$\sqrt{(\mathbf{a}, \mathbf{a})} = \text{ absoluter Betrag von } \mathbf{a}$$

d.h., die Norm des Elementes $\mathbf{a}$ in der Algebra $\mathscr{A}$ stimmt mit dem absoluten Betrag von $\mathbf{a}$ als komplexer Zahl (oder eines Quaternions) überein.

Weil je zwei Elemente $\mathbf{a}$ und $\mathbf{b}$ der Algebra $\mathscr{A}$ einer komplexen Unteralgebra oder einer Quaternionenunteralgebra angehören, gilt

$$(\text{absoluter Betrag von } \mathbf{ab})^2 = (\text{absoluter Betrag von } \mathbf{a})^2 \cdot (\text{absoluter Betrag von } \mathbf{b})^2$$

(da die Algebra der komplexen Zahlen ebenso wie auch die Algebra der Quaternionen normiert ist) oder

$$(\mathbf{ab}, \mathbf{ab}) = (\mathbf{a}, \mathbf{a})(\mathbf{b}, \mathbf{b})$$

Die Gleichung aber bedeutet gerade die Normiertheit der Algebra $\mathscr{A}$.
Weiterhin kommt der Satz von Hurwitz zur Geltung, gemäß dem die Algebra $\mathscr{A}$ einer der vier "Standard"-Algebren isomorph ist: der Algebra der reellen Zahlen, der komplexen Zahlen, der Quaternionen oder der Oktaven. Darin besteht aber gerade der verallgemeinerte Satz von Frobenius.

3.20 Kommutative Algebren mit Division

3.20.1 Formulierung des Resultats

Im vorhergehenden Paragraphen fanden wir alle Algebren mit Division, die zusätzlich der Bedingung der Assoziativität genügen.
Weiter unten wird eine Beschreibung aller Algebren mit Division unter der zusätzlichen Bedingung der Kommutativität gegeben. Vor allem kommen wir auf die folgende Tatsache zurück, die wir hier nicht beweisen werden.

Jede kommutative Algebra mit Division besitzt eine Dimension, die nicht größer als 2 ist![22]

Deshalb müssen wir zur Lösung der gestellten Aufgabe alle kommutativen Algebren der Dimension 2 mit Division ermitteln. Um die Antwort zu formulieren, führen wir die Bezeichnung $\mathscr{A}(\alpha, \beta, \gamma)$ ein für eine kommutative Algebra der Dimension 2 mit der Multiplikationstafel der Form

$$\begin{aligned} \mathbf{k}_1 \circ \mathbf{k}_1 &= \alpha \mathbf{k}_1 + \beta \mathbf{k}_2 \\ \mathbf{k}_2 \circ \mathbf{k}_2 &= -\alpha \mathbf{k}_1 - \beta \mathbf{k}_2 \\ \mathbf{k}_1 \circ \mathbf{k}_2 &= \beta \mathbf{k}_1 + \gamma \mathbf{k}_2 \end{aligned} \tag{1}$$

wobei die Zahlen α, β und γ folgenden Bedingungen genügen:

1) $\alpha\gamma - \beta^2 = \pm 1$;
2) $\beta \geq 0$;
3) $\alpha \geq 0$, wobei $\alpha = 0$ ist, wenn $\gamma \geq 0$ ist.

Satz. Jede kommutative Algebra $\mathscr{A}$ der Dimension 2 mit Division ist einer der Algebren $\mathscr{A}(\alpha, \beta, \gamma)$ isomorph. Alle Algebren $\mathscr{A}(\alpha, \beta, \gamma)$ sind Algebren mit Division und je zwei von ihnen sind untereinander nicht isomorph.

Der weitere Teil dieses Paragraphen ist dem Beweis dieses Satzes gewidmet.

3.20.2 Die Verbindung zwischen der Multiplikation in der Algebra $\mathscr{A}$ und der Multiplikation der komplexen Zahlen

Es möge also $\mathscr{A}$ eine kommutative Algebra mit Division sein. Wir bezeichnen die Multiplikation in der Algebra $\mathscr{A}$ mit $\mathbf{x} \diamond \mathbf{y}$.
Wir halten irgendein Element $\mathbf{a} \neq \mathbf{0}$ fest und betrachten die Transformation

$$\mathbf{x} \to \mathbf{a} \diamond \mathbf{x}$$

Diese Transformation ist offensichtlich linear. Wir bezeichnen sie mit A. Weil die gegebene Algebra eine Algebra mit Division ist, existiert zur Transformation A eine inverse Transformation A^{-1}.
Wir führen für die Elemente unserer Algebra das neue Multiplikationsgesetz

$$\mathbf{x} \cdot \mathbf{y} = A^{-1}(\mathbf{x}) \diamond A^{-1}(\mathbf{y}) \tag{2}$$

[22] Einen geistreichen Beweis dieses Satzes unter Verwendung topologischer Überlegungen fand der deutsche Mathematiker G. Hopf. Wir führen den Beweis für den Leser an, der mit den elementaren Begriffen der Topologie vertraut ist.

Es möge $\mathscr{A}$ eine kommutative Algebra der Dimension n mit Division sein. Wenn für je zwei Elemente $\mathbf{x}$ und $\mathbf{y}$ die Gleichung $\mathbf{x}^2 = \mathbf{y}^2$ gilt, dann haben wir aufgrund der Kommutativität $(\mathbf{x} - \mathbf{y})(\mathbf{x} + \mathbf{y}) = \mathbf{0}$. Wegen des Fehlens von Nullteilern bedeutet dies $\mathbf{x} = \mathbf{y}$ oder $\mathbf{x} = -\mathbf{y}$. Daraus ist ersichtlich, dass die Abbildung

$$\mathbf{x} \to \mathbf{x}^2$$

eine monomorphe und stetige Abbildung der Sphäre S^{n-1} in den projektiven Raum RP^{n-1} induziert. Bekanntlich gibt es eine solche Abbildung nur für $n = 2$.

Wir stellen fest, dass der von G. Hopf bewiesene Satz ein algebraischer ist. Deshalb muss es auch einen rein algebraischen Beweis dieses Satzes geben. Ein solcher Beweis wurde von dem holländischen Mathematiker T. A. Springer gefunden.

ein. Die Algebra mit der Multiplikation $\mathbf{x} \cdot \mathbf{y}$ ist wiederum eine Algebra mit Division (aus der eindeutigen Lösbarkeit der Gleichungen

$$\mathbf{a} \diamond \mathbf{x} = \mathbf{b} \qquad \text{und} \qquad \mathbf{x} \diamond \mathbf{a} = \mathbf{b}$$

geht die eindeutige Lösbarkeit der Gleichungen

$$\mathbf{a} \cdot \mathbf{x} = \mathbf{b} \qquad \text{und} \qquad \mathbf{x} \cdot \mathbf{a} = \mathbf{b}$$

hervor). In dieser Algebra spielt das Element $\mathbf{a} \diamond \mathbf{a}$ die Rolle des Einselementes. Die einzige Algebra mit Division aber, die ein Einselement besitzt, ist die Algebra der komplexen Zahlen (§ 2). Deshalb kann man die Elemente $\mathbf{x}$ und $\mathbf{y}$ als komplexe Zahlen behandeln und die Operation $\mathbf{x} \cdot \mathbf{y}$ als die gewöhnliche Multiplikation der komplexen Zahlen.

Indem wir $A^{-1}(\mathbf{x})$ mit $\mathbf{u}$ und $A^{-1}(\mathbf{y})$ mit v bezeichnen, schreiben wir (2) um in die Form

$$\mathbf{u} \diamond \mathbf{v} = A(\mathbf{u}) \cdot A(\mathbf{v})$$

Damit haben wir die Multiplikation in der Ausgangsalgebra $\mathscr{A}$ durch die Multiplikation in der Algebra der komplexen Zahlen ausgedrückt.

Wir gehen jetzt den nächsten Schritt. Wir betrachten die Multiplikation

$$\mathbf{u} \cdot \mathbf{v} = A(\mathbf{u} \circ \mathbf{v}) \tag{3}$$

und werden zeigen, dass Algebren mit den Multiplikationen

$$\mathbf{u} \diamond \mathbf{v} \qquad \text{und} \qquad \mathbf{u} \circ \mathbf{v}$$

einander isomorph sind. Dazu schreiben wir die Tafel der Multiplikation $\circ$ in irgendeiner Basis $\mathbf{e}_1, \mathbf{e}_2$ nieder und beweisen, dass sie dann genau mit der Tafel der Multiplikation $\diamond$ in der Basis $\mathbf{e}'_1 = A^{-1}(\mathbf{e}_1)$, $\mathbf{e}'_2 = A^{-1}(\mathbf{e}_2)$ übereinstimmt. In der Tat, es möge

$$\mathbf{e}_i \circ \mathbf{e}_j = \alpha \mathbf{e}_1 + \beta \mathbf{e}_2$$

sein. Dann gilt

$$\begin{aligned} \mathbf{e}'_i \circ \mathbf{e}'_j &= A(\mathbf{e}'_i) \cdot A(\mathbf{e}'_j) = \mathbf{e}_i \cdot \mathbf{e}_j = A^{-1}(\mathbf{e}_i \circ \mathbf{e}_j) = A^{-1}(\alpha \mathbf{e}_1 + \beta \mathbf{e}_2) \\ &= \alpha A^{-1}(\mathbf{e}_1) + \beta A^{-1}(\mathbf{e}_2) = \alpha \mathbf{e}'_1 + \beta \mathbf{e}'_2 \end{aligned}$$

was die Übereinstimmung der Multiplikationstafeln beweist.
Wir haben also gezeigt, dass die Ausgangsalgebra $\mathscr{A}$ der Algebra mit der Multiplikation (3) isomorph ist, wobei $\mathbf{u} \cdot \mathbf{v}$ das gewöhnliche Produkt komplexer Zahlen ist und A eine bestimmte lineare Transformation, für die die inverse Transformation A^{-1} existiert.

Andererseits ist offensichtlich, dass jede Algebra solcher Art eine kommutative Algebra mit Division ist. Auf solche Weise führte die Aufgabe.der Aufzählung aller Algebren mit Division der Dimension 2 dazu, unter den Algebren (3) alle untereinander nicht isomorphen auszusuchen.

3.20.3 Auffinden der Algebren $\mathscr{A}(\alpha,\beta,\gamma)$, die der Algebra $\mathscr{A}$ isomorph sind

Es ist notwendig, in der Algebra (3) eine solche Basis $\mathbf{k}_1, \mathbf{k}_2$ zu finden, in der die Multiplikationstafel die Form (1) besitzt (mit bestimmten Beschränkungen für α, β, γ). Wir schreiben zuerst die Multiplikationstafel der Algebra (3) in der Basis $\mathbf{e}_1 = \mathbf{1}$, $\mathbf{e}_2 = \mathbf{i}$ auf. Da

$$\begin{aligned}
\mathbf{e}_1 \circ \mathbf{e}_1 &= A(\mathbf{e}_1 \circ \mathbf{e}_1) = A(\mathbf{1}),\\
\mathbf{e}_2 \circ \mathbf{e}_2 &= A(\mathbf{e}_2 \circ \mathbf{e}_2) = A(\text{-}\mathbf{1}) = -A(\mathbf{1}),\\
\mathbf{e}_1 \circ \mathbf{e}_2 &= A(\mathbf{e}_1 \circ \mathbf{e}_2) = A(\mathbf{i})
\end{aligned}$$

gilt, werden wir, indem wir

$$A(\mathbf{1}) = a + b\mathbf{i} \qquad , \qquad A(\mathbf{i}) = c + d\mathbf{i}$$

setzen,

$$\begin{aligned}
\mathbf{e}_1 \circ \mathbf{e}_1 &= a\mathbf{e}_1 + b\mathbf{e}_2\\
\mathbf{e}_2 \circ \mathbf{e}_2 &= -a\mathbf{e}_1 - b\mathbf{e}_2\\
\mathbf{e}_1 \circ \mathbf{e}_2 &= c\mathbf{e}_1 + d\mathbf{e}_2
\end{aligned} \tag{4}$$

erhalten. Wir stellen die Frage, ob außer $\mathbf{e}_1, \mathbf{e}_2$ (d.h. außer $\mathbf{1}$, $\mathbf{i}$) in der Algebra $\mathscr{A}$ andere Basen existieren, für die die Multiplikationstafel ähnlich der Tafel (4) ist:

$$\begin{aligned}
\mathbf{k}_1 \circ \mathbf{k}_1 &= \alpha\mathbf{k}_1 + \beta\mathbf{k}_2\\
\mathbf{k}_2 \circ \mathbf{k}_2 &= -\alpha\mathbf{k}_1 - \beta\mathbf{k}_2\\
\mathbf{k}_1 \circ \mathbf{k}_2 &= \delta\mathbf{k}_1 + \gamma\mathbf{k}_2
\end{aligned} \tag{5}$$

Anders ausgedrückt, existieren Basen, für die

$$\mathbf{k}_1 \cdot \mathbf{k}_1 = -\mathbf{k}_2 \circ \mathbf{k}_2 \tag{6}$$

gilt. Weil Gleichung (6) gleichbedeutend mit $A(\mathbf{k}_1 \cdot \mathbf{k}_1) = -A(\mathbf{k}_2 \cdot \mathbf{k}_2)$ oder $A(\mathbf{k}_1 \cdot \mathbf{k}_1) = A(-\mathbf{k}_2 \cdot \mathbf{k}_2)$ ist, folgt aus der Existenz der inversen Transformation A^{-1}, dass $\mathbf{k}_1 \cdot \mathbf{k}_1 = -\mathbf{k}_2 \cdot \mathbf{k}_2$ ist, oder

$$\mathbf{k}_2 = \pm\mathbf{i}\mathbf{k}_1$$

Folglich sind

$$\mathbf{k}_1 = \mathbf{f} \qquad , \qquad \mathbf{k}_2 = \pm\mathbf{i}\mathbf{f} \tag{7}$$

alle Basen, für die die Multiplikationstafel die Form (5) besitzt, wobei $\mathbf{f}$ eine beliebige komplexe Zahl (nicht gleich Null) ist.

Es versteht, sich, dass eine unendliche Menge von Basen (7) existiert. Wir werden gleich zeigen, dass man unter ihnen unbedingt eine solche finden kann, in der die Bedingung

$$\beta = \delta$$

erfüllt ist. d.h., eine Basis, in der die Multiplikationstafel die Form (1) besitzt. Dazu nehmen wir als Ausgangsbasis $\mathbf{e}_1 = \mathbf{1}$, $\mathbf{e}_2 = \mathbf{i}$, die gesuchte Basis aber schreiben wir in der Form

$$\mathbf{k}_1 = \rho(\cos\varphi + \mathbf{i}\sin\varphi) \qquad , \qquad \mathbf{k}_2 = \pm\mathbf{i}\rho(\cos\varphi + \mathbf{i}\sin\varphi)$$

Um ρ und φ zu finden, müssen wir:

a) das Produkt $\mathbf{k}_1 \circ \mathbf{k}_1$, mit Hilfe der Formeln (4) berechnen und das erhaltene Element in $\mathbf{k}_1$ und $\mathbf{k}_2$ zerlegen;

b) auf die gleiche Weise das Produkt $\mathbf{k}_1 \circ \mathbf{k}_2$ berechnen und das erhaltene Element in $\mathbf{k}_2$ und k_2 zerlegen;

c) den Koeffizienten von k_2 in der ersten Zerlegung dem Koeffizienten von k_1 in der zweiten Zerlegung gleichsetzen.

Wir überlassen es dem Leser, diese Rechenarbeit auszuführen.
Das Resultat ist folgendes. ρ wird keine Beschränkung auferlegt und φ findet man aus der Bedingung

$$\tan\varphi = \frac{b-c}{a+d}$$

Offensichtlich bestimmt diese Bedingung einen Winkel φ bis auf Vielfache von πn und legt in der Ebene zwei Strahlen fest (Abb. 17), die eine Gerade l_1 bilden.

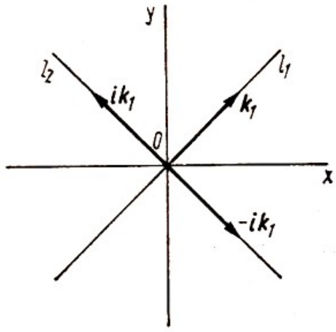
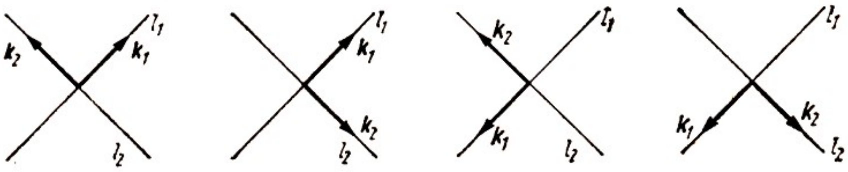


Abb.17

Auf dieser Geraden liegt der Vektor, der die komplexe Zahl k_1 darstellt (oder, wie wir sagen werden, den Vektor $\mathbf{k}_1$). Der andere Vektor $\mathbf{k}_2 = \pm\mathbf{i}\mathbf{k}_1$ liegt auf der zugehörigen Geraden l_2.
Die Länge beider Vektoren stimmt überein. Wir kommen also zur folgenden Beschreibung aller Basen $\mathbf{k}_1, \mathbf{k}_2$ in denen die Multiplikationstafel die Form (1) besitzt.

Der Basisvektor $\mathbf{k}_1$ wird auf der eindeutig bestimmten Geraden l_1 ausgewählt, der Basisvektor $\mathbf{k}_2$ auf der senkrecht daraufstehenden Geraden l_2; die Länge ρ der Vektoren muss gleich sein. Wir bemerken, dass bei gegebener Länge genau 4 der gesuchten Basen möglich sind.

Abb.18



Es bleibt jetzt noch zu sagen, wenn wir von der Basis $\mathbf{k}_1, \mathbf{k}_2$ zu einer anderen Basis $\lambda\mathbf{k}_1, \lambda\mathbf{k}_2$, übergehen, wobei λ eine positive reelle Zahl ist, dann werden alle Koeffizienten in der Multiplikationstafel (1) mit ρ multipliziert. Deshalb wird, wenn man der Basis die zusätzliche Bedingung

$$\alpha\gamma - \beta^2 = \pm 1$$

auferlegt, damit eindeutig der Wert von λ bestimmt. Dann bleiben von der oben gezeigten unendlichen Menge genau 4 Basen (siehe Abb. 18). Es existieren also genau 4 Basen

$$k_1 = \pm k \qquad , \qquad k_2 = \pm k$$

für die die Multiplikationstafel die Form

$$\begin{aligned} \mathbf{k}_1 \circ \mathbf{k}_1 &= \alpha\mathbf{k}_1 + \beta\mathbf{k}_2 \\ \mathbf{k}_2 \circ \mathbf{k}_2 &= -\alpha\mathbf{k}_1 - \beta\mathbf{k}_2 \\ \mathbf{k}_1 \circ \mathbf{k}_2 &= \delta\mathbf{k}_1 + \gamma\mathbf{k}_2 \end{aligned} \tag{1}$$

besitzt, wobei $\alpha\gamma - \beta^2 = \pm 1$ ist.

Wir gehen jetzt den letzten Schritt und zeigen, dass man unter den oben gezeigten vier Basen eine solche auswählen kann, in der $\alpha \geq 0$ und $\beta \geq 0$ ist, wobei $\gamma > 0$ ist, wenn $\alpha = 0$ ist.
In der Tat, wenn $\beta < 0$ für die Basis $\mathbf{k}_1, \mathbf{k}_2$ ist, dann erhalten wir, indem wir zur Basis $\mathbf{k}_1, -\mathbf{k}_2$ übergehen, eine neue Tafel, in der $\beta > 0$ ist.

Analog erhalten wir, wenn $\alpha < 0$ ist, durch Multiplizieren des ersten Basisvektors mit -1, eine Tafel, in der $\alpha > 0$ ist (dabei wird das Vorzeichen von β nicht verändert); wenn $\alpha = 0$ ist, dann ermöglicht es diese Transformation, das Vorzeichen von γ zu verändern.

Wir ziehen Bilanz. Für jede kommutative Algebra $\mathscr{A}$ der Dimension 2 mit Division existiert eine Basis, in der die Multiplikationstafel die Form (1) besitzt, wobei gilt

1) $\alpha\gamma - \beta^2 = \pm 1$,
2) $\beta \geq 0$,
3) $\alpha \geq 0$, wobei $\gamma > 0$ ist, wenn $\alpha = 0$ ist.

Diese Basis ist im allgemeinen die einzige. In einigen besonderen Fällen (wenn $\beta = 0$ oder $\alpha = \gamma = 0$ ist) gibt es zwei solcher Basen, die Tafel (1) aber wird für sie ein und dieselbe sein. Daraus ist ersichtlich, dass jede Algebra $\mathscr{A}$ genau eine Tafel (1) mit den oben gezeigten Beschränkungen für α, β und γ entspricht, d.h., die Algebra $\mathscr{A}$ ist isomorph einer und nur einer Algebra $\mathscr{A}(\alpha, \beta, \gamma)$.

Jede Algebra $\mathscr{A}(\alpha, \beta, \gamma)$ ist eine Algebra mit Division. Das folgt bereits aus der Tatsache, dass jede solche Algebra die Form

$$\mathbf{u} \circ \mathbf{v} = A(\mathbf{u} \circ \mathbf{v})$$

besitzt, wobei die Transformation A entsprechend den Formeln

$$A(\mathbf{k}_1) = \alpha\mathbf{k}_1 + \beta\mathbf{k}_2 \qquad \text{und} \qquad A(\mathbf{k}_2) = \beta\mathbf{k}_1 + \gamma\mathbf{k}_2$$

mit $\alpha\gamma - \beta^2 \neq 0$ wirkt. In der Tat geht aus der Bedingung

$$\frac{\alpha}{\beta} \neq \frac{\beta}{\gamma}$$

(die $\alpha\gamma - \beta^2 \neq 0$ äquivalent ist) hervor, dass

$$A(\mathbf{k}_1) \neq \lambda A(\mathbf{k}_2)$$

ist und damit, dass die Vektoren $A(\mathbf{k}_1)$ und $A(\mathbf{k}_2)$ eine Basis bilden. Daraus erhält man unschwer, dass zur Transformation **A** eine inverse Transformation A^{-1} existiert und daraus wiederum, dass eine Algebra mit der Multiplikation $\mathbf{u} \circ \mathbf{v}$ eine Algebra mit Division ist. Der Satz ist bewiesen.

4 Schlusswort

Ein großer Teil von dem, worüber in diesem Büchlein gesprochen wurde, bezieht sich auf die Anfangsetappe in der Entwicklung der Theorie der Algebren.
Wir wollen jetzt, obwohl nur sehr flüchtig, von einigen weiteren Ergebnissen dieser Theorie sprechen.

Die Entwicklung der Algebrentheorie beginnt mit den Arbeiten W. Hamiltons über Quaternionen, die im Jahre 1843 erschienen. Später wurde ihr Inhalt zusammen mit einer Reihe anderer Ergebnisse von ihm in den "Vorlesungen über Quaternionen" niedergelegt. Der Einfluss der Ideen Hamiltons war sehr bedeutsam.
Sie bereiteten den Boden für eine ganze Serie von Arbeiten über assoziative Algebren vor, die mit dem Beweis einer Reihe tiefliegender Sätze über den Bau solcher Algebren abgeschlossen wurden.

Um über diese Sätze zu berichten, präzisieren wir zuerst einen wichtigen Sachverhalt, den wir bis zu dieser Zeit überhaupt noch nicht berührt haben. Er ist mit den Größen $a_1, a_2, ..., a_n$ verbunden, die die Koeffizienten in dem Ausdruck

$$a_1\mathbf{i}_1 + a_2\mathbf{i}_2 + ... + a_n\mathbf{i}_n \tag{1}$$

für die Elemente einer n-dimensionalen Algebra darstellen. In unserer Darlegung werden diese Größen immer als reelle Zahlen vorausgesetzt.
In diesem Falle ist es üblich, von Algebren über dem Körper der reellen Zahlen zu sprechen. Neben diesen betrachtet man auch andere Algebren, deren Elemente Ausdrücke der Form (1) darstellen, wobei $a_1, a_2, ..., a_n$ beliebige komplexe Zahlen sind. Solche Algebren werden Algebren über dem Körper der komplexen Zahlen genannt.
Außer dem Körper der reellen und dem Körper der komplexen Zahlen gibt es viele andere Körper[23] (zum Beispiel den Körper der rationalen Zahlen) und dementsprechend viele andere Typen von Algebren.

Viele Ergebnisse in der Theorie der Algebren ändern sich stark in Abhängigkeit davon, welchem Körper die Koeffizienten $a_1, ..., a_n$ in den Ausdrücken (1) angehören, d.h., über welchem Körper die Algebra betrachtet wird.

Zum Beispiel existieren über dem Körper der reellen Zahlen, wie wir wissen, drei assoziative Algebren mit Division (und eine unendliche Menge nichtassoziativer Algebren solcher Art), während es nur eine komplexe Algebra mit Division gibt.
Das ist die eindimensionale Algebra, die aus den komplexen Zahlen selbst besteht.

Außer ihr existiert keine Algebra mit Division über dem Körper der komplexen Zahlen (selbst ohne die Bedingung der Assoziativität). Der Beweis dieser Tatsache ist nicht kompliziert, wir

[23] Die allgemeine Definition eines Körpers ist folgendermaßen. Es möge $\mathscr{P}$ eine bestimmte Menge von Objekten sein, über der man zwei Operationen ausführen kann. Eine von ihnen werden wir durch Vereinbarung Addition nennen und mit $a + b$ bezeichnen, die andere werden wir Multiplikation nennen und mit ab bezeichnen.

Die Menge $\mathscr{P}$ wird Körper genannt, wenn die beiden in ihr gegebenen Operationen kommutativ und assoziativ sind, das Distributivgesetz richtig ist, so wie auch die Subtraktion ausführbar ist (anders ausgedrückt, dass die Gleichung $a + x = b$ eindeutig lösbar ist) und die Division ausführbar ist. Die letztere bedeutet, dass die Gleichung $ax = b$ eindeutig lösbar ist, wenn $a \neq 0$ ist. Hier bedeutet 0 ein Element der Menge $\mathscr{P}$ von der Art, dass $a + 0 = a$ für alle $a \in \mathscr{P}$ ist (die Existenz eines solchen Elementes ist leicht zu beweisen). Unter dem Wort "Operation"versteht man in dieser Definition eine beliebige Regel, die je zwei Elementen $a \in \mathscr{P}$ und $b \in \mathscr{P}$ ein drittes Element $c \in \mathscr{P}$ zuordnet.

werden uns aber damit nicht aufhalten.

1. Ein Teilraum einer Algebra $\mathscr{A}$ wird Ideal genannt, wenn

$$\mathscr{A}\mathscr{U} \subset \mathscr{U} \qquad \text{und} \qquad \mathscr{U}\mathscr{A} \subset \mathscr{U}$$

gilt. Dies bedeutet, wie auch die Elemente **a** $\in \mathscr{A}$ und **u** $\in \mathscr{U}$ gewählt werden, die beiden Produkte **au** und **ua** gehören $\mathscr{U}$ an.
Anders ausgedrückt, das Produkt jedes Elementes, das aus dem Ideal genommen ist, mit jedem Element der Algebra gehört wiederum dem Ideal an.

Dabei ist es nicht üblich, die zwei Grenzfälle, dass der Teilraum $\mathscr{U}$ mit der ganzen Algebra $\mathscr{A}$ übereinstimmt und dass $\mathscr{U}$ aus einem einzigen Element **0** besteht, als Ideale anzusehen (man sagt übrigens manchmal, dass $\mathscr{A}$ und **0** uneigentlich Ideale sind).

Als Beispiel eines Ideals mag der Teilraum der Elemente der Form $b\Omega$ in der Algebra der dualen Zahlen dienen (d.h., der Zahlen $a+b\Omega$, wobei $\Omega^2 = 0$ ist). Ein anderes Beispiel ist der Teilraum der Elemente der Form $a(1+E)$ in der Algebra der binären Zahlen (der Zahlen $a+bE$, wobei $E^2 = 1$ ist).

2. Eine Algebra, die keine Ideale besitzt, wird einfach genannt.
Man kann sagen, dass der Begriff der einfachen Algebra den Begriff der Algebra mit Division abschwächt. Jede Algebra mit Division ist notwendig einfach. In der Tat, wenn es in einer Algebra ein Ideal $\mathscr{U}$ gibt, besitzt die Gleichung

$$\mathbf{ux} = \mathbf{b}$$

wobei **u** dem Ideal angehört und **b** ihm nicht angehört, keine Lösung. Deshalb kann eine solche Algebra keine Algebra mit Division sein.

Am Ende des 19. Jahrhunderts wurden die Forschungen, die die Theorie der Algebra betrafen, hauptsächlich auf die Untersuchung assoziativer Algebren konzentriert (wie wir bereits bemerkten, verstand man den Terminus "Algebra" stets als "assoziative Algebra").
Als Ergebnis entstand eine ziemlich klare Vorstellung von der Struktur einer assoziativen Algebra.

Das erste Resultat, das sich auf einfache Algebren bezieht, wurde im Jahre 1893 durch F. Molin erhalten; unabhängig davon erhielten G. Frobenius und E. Cartan das gleiche Ergebnis. Es zeigt sich, dass alle einfachen komplexen, assoziativen Algebren bis auf Isomorphie vollständige Matrizenalgebren einer beliebigen Ordnung n sind (d.h. Algebren aller quadratischen Matrizen der Ordnung n).

Ein allgemeinerer Satz, der für Algebren über einem beliebigen Körper $\mathscr{P}$ gilt, wurde im Jahre 1907 durch den amerikanischen Mathematiker J. Wedderburn bewiesen: Alle einfachen assoziativen Algebren über dem Körper $\mathscr{P}$ sind genau alle vollständigen Matrizenalgebren mit Elementen aus einer assoziativen Algebra mit Division über $\mathscr{P}$.

Gemäß diesem Satz bestehen zum Beispiel alle einfachen assoziativen Algebren über dem Körper $\mathscr{D}$ der reellen Zahlen aus drei Serien:

1) Matrizenalgebren mit reellen Zahlen als Elementen;

2) Matrizenalgebren mit komplexen Zahlen als Elementen (wir betonen, dass man diese Algebren als Algebren über dem Körper $\mathscr{D}$ betrachten muss), von denen die Algebra der komplexen

Zahlen selbst ein Spezialfall ist (für $n = 1$), deren Dimension gleich 2 ist; entsprechend besitzt die Algebra aller komplexen Matrizen der Ordnung n die Dimension $2n^2$;

3) Matrizenalgebren mit Quaternionen als Elementen (für Matrizen der Ordnung n ist die Dimension einer solchen Algebra gleich $4n^2$).

Den vorigen Satz über komplexe, einfache Algebren erhält man leicht aus dem Satz von Wedderburn, wenn man sich daran erinnert, dass die einzige komplexe Algebra mit Division die Algebra der komplexen Zahlen selbst ist.
Auf diese Weise wurden alle einfachen assoziativen Algebren gefunden. Gleichzeitig damit wurde (durch die gleichen Autoren) geklärt, dass die Struktur einfacher assoziativer Algebren in vielem die Struktur beliebiger assoziativer Algebren bestimmt. Um die letztere Behauptung genau zu formulieren, brauchen wir noch einige Definitionen.

3. Es mögen $\mathscr{U}_1$ und $\mathscr{U}_2$ zwei Algebren sein. Die neue Algebra $\mathscr{A}$ deren Elemente alle möglichen Paare

$$(\mathbf{u}_1, \mathbf{u}_2)$$

(mit $\mathbf{u}_1 \in \mathscr{U}_1$ und $\mathbf{u}_2 \in \mathscr{U}_2$) sind, wird die direkte Summe von $\mathscr{U}_1$ und $\mathscr{U}_2$ genannt, wobei folgende Gesetze der Addition und der Multiplikation erklärt sind:

$$(\mathbf{u}_1, \mathbf{u}_2) + (\mathbf{u}'_1, \mathbf{u}'_2) = (\mathbf{u}_1 + \mathbf{u}'_1, \mathbf{u}_2 + \mathbf{u}'_2)$$
$$(\mathbf{u}_1, \mathbf{u}_2) \cdot (\mathbf{u}'_1, \mathbf{u}'_2) = (\mathbf{u}_1\mathbf{u}'_1, \mathbf{u}_2\mathbf{u}'_2)$$

Es ist leicht zu sehen, dass die Elemente der Form $(\mathbf{u}_1, 0)$ eine Unteralgebra der Algebra $\mathscr{A}$ bilden, wobei diese Unteralgebra zu $\mathscr{U}_1$ isomorph ist; wir bezeichnen sie mit $\mathscr{A}_1$. Analog bilden die Elemente der Form $(0, \mathbf{u}_2)$ eine Unteralgebra $\mathscr{A}_2$, die zu $\mathscr{U}_2$ isomorph ist.
Beide gezeigte Unteralgebren sind Ideale; zum Beispiel folgt dies für die erste von ihnen aus den Gleichungen

$$(\mathbf{u}_1, 0)(\mathbf{u}'_1, \mathbf{u}'_2) = (\mathbf{u}_1\mathbf{u}'_1, 0) \qquad \text{und} \qquad (\mathbf{u}'_1, \mathbf{u}'_2)(\mathbf{u}_1, 0) = (\mathbf{u}'_1\mathbf{u}_1, 0)$$

Wir bemerken; dass die Unteralgebren $\mathscr{A}_1$ und $\mathscr{A}_2$ komplementär sind. So nennen wir zwei Unteralgebren, die die Eigenschaft besitzen, dass jedes Element der Algebra, und zwar in eindeutiger Weise, in der Form

$$\mathbf{a}_1 + \mathbf{a}_2 \quad \text{mit } \mathbf{a}_1 \in \mathscr{A}_1, \mathbf{a}_2 \in \mathscr{A}_2$$

dargestellt werden kann.
Analog der direkten Summe zweier Algebren wird die direkte Summe einer beliebigen Zahl von Algebren definiert. Elemente der direkten Summe der Algebren $\mathscr{U}_1$, $\mathscr{U}_2$, ..., $\mathscr{U}_k$ sind alle k-Tupel

$$(\mathbf{u}_1, \mathbf{u}_2, ..., \mathbf{u}_k) \quad \text{mit } \mathbf{u}_1 \in \mathscr{U}_1, ..., \mathbf{u}_k \in \mathscr{U}$$

Ein Beispiel einer direkten Summe ist die Algebra der Matrizen der Ordnung $p + q$, die die "blockförmig-diagonale" Form

$$\left(\begin{array}{c|c} A & 0 \\ \hline 0 & B \end{array}\right)$$

besitzt, wobei A und B beliebige Matrizen der entsprechenden Ordnung p und q sind. Es ist nicht schwer zu überprüfen, dass für Produkte solcher Matrizen die Formel

$$\left(\begin{array}{c|c} A & 0 \\ \hline 0 & B \end{array}\right)\left(\begin{array}{c|c} A' & 0 \\ \hline 0 & B' \end{array}\right) = \left(\begin{array}{c|c} AA' & 0 \\ \hline 0 & BB' \end{array}\right)$$

gilt, woraus ersichtlich ist, dass die gegebene Algebra isomorph zu der direkten Summe der Algebra aller Matrizen der Ordnung p und der Algebra aller Matrizen der Ordnung q ist.

Es ist interessant zu bemerken, dass die von uns am Anfang des Buches (siehe § 2) betrachtete Algebra der binären Zahlen isomorph zu der direkten Summe zweier Algebren reeller Zahlen ist. In der Tat, wir wählen als Basis die folgenden zwei Elemente der Algebra $\mathscr{A}$:

$$\mathbf{i}_1 = \frac{1-E}{\sqrt{2}} \qquad \text{und} \qquad \mathbf{i}_2 = \frac{1+E}{\sqrt{2}}$$

Offensichtlich ist

$$\mathbf{i}_1^2 = \mathbf{i}_1, \qquad \mathbf{i}_2^2 = \mathbf{i}_2, \qquad \mathbf{i}_1\mathbf{i}_2 = \mathbf{0}$$

Jedes Element $\mathbf{a} \in \mathscr{A}$ kann man gleichwertig darstellen in Form der Summe

$$a_1\mathbf{i}_1 + a_2\mathbf{i}_2$$

wobei für das Produkt zweier Elemente die Formel

$$(a_1\mathbf{i}_1 + a_2\mathbf{i}_2)(b_1\mathbf{i}_1 + b_2\mathbf{i}_2) = a_1b_1\mathbf{i}_1 + a_2b_2\mathbf{i}_2$$

gilt. Wenn wir das Element $\mathbf{a}$ dem Zahlenpaar $(\mathbf{a}_1, \mathbf{a}_2)$ zuordnen, so sehen wir, dass die Algebra $\mathscr{A}$ die direkte Summe zweier Algebren $\mathscr{D}$ (reeller Zahlen) ist.

4. Die direkte Summe einfacher Algebren wird halbeinfach genannt. Weil eine direkte Summe durch ihre Summanden bestimmt ist, kann man alle halbeinfachen assoziativen Algebren als bekannt annehmen, sobald alle einfachen assoziativen Algebren bekannt sind.

Zum Beispiel ist eine beliebige halbeinfache assoziative Algebra über dem Körper der komplexen Zahlen isomorph zur Algebra aller "blockförmig-diagonalen" Matrizen mit Blöcken der Ordnung $p_1, p_2, ..., p_k$ in der Diagonale (die Zahlen $p_1, p_2, ..., p_k$ sind fest). Insbesondere erhalten wir für $k = 3$ Matrizen der Form

$$\left(\begin{array}{c|c|c} A & 0 & 0 \\ \hline 0 & B & 0 \\ \hline 0 & 0 & C \end{array}\right)$$

5. Eine Algebra wird nilpotent genannt, wenn eine Zahl k existiert, so dass das Produkt von je k Elementen gleich Null ist, wobei die Klammern im Produkt willkürlich gesetzt werden. (Wir haben die Definition einer nilpotenten Algebra für den allgemeinen Fall angeführt, d.h. ohne die Bedingung der Assoziativität. Deshalb ist der letzte Zusatz über die willkürliche Reihenfolge der Multiplikation notwendig.)
Eine Unteralgebra einer bestimmten Algebra wird nilpotent genannt, wenn sie, als selbständige Algebra betrachtet, nilpotent ist.

Das einfachste Beispiel einer nilpotenten Algebra ist die Nullalgebra (das Produkt von je zwei Elementen ist gleich Null). Ein anderes Beispiel ist die Algebra mit der Basis i_1, i_2, i_3 und der Multiplikationstafel

$$\begin{cases} \mathbf{i}_1\mathbf{i}_2 = \mathbf{i}_3 \\ \text{die übrigen } \mathbf{i}_\alpha\mathbf{i}_\beta \text{ sind gleich } 0 \end{cases}$$

Wir bemerken, dass nilpotente Algebren in einem gewissem Sinne in ihren Eigenschaften entgegengesetzt zu halbeinfachen Algebren sind. Zum Beispiel besteht für eine nilpotente Algebra $\mathscr{A}$ eine bestimmte "Potenz" $\mathscr{A}^k$, d.h., die Menge aller Produkte von je k Elementen der Algebra $\mathscr{A}$, aus der Null (darin besteht die Definition einer nilpotenten Algebra), während im

Falle einer halbeinfachen Algebra jede Potenz mit der ganzen Algebra übereinstimmt.

Es ist nicht schwierig zu beweisen, wenn $\mathscr{V}_1$, und $\mathscr{V}_2$ zwei nilpotente Ideale einer beliebigen Algebra $\mathscr{A}$ sind, dann ist ihre Summe (d.h. die Gesamtheit der Elemente der Form $\mathbf{v}_1 + \mathbf{v}_2$, wobei $\mathbf{v}_1 \in \mathscr{V}_1$ und $\mathbf{v}_2 \in \mathscr{V}_2$ ist) wiederum ein nilpotentes Ideal.

Daraus kann man leicht ableiten, dass unter allen nilpotenten Idealen der Algebra $\mathscr{A}$ ein maximales existiert, d.h., ein solches, das alle anderen nilpotenten Ideale enthält. Jetzt können wir einen grundlegenden Satz in der Theorie der assoziativen Algebren formulieren.

Satz von Wedderburn. In jeder assoziativen Algebra $\mathscr{A}$ existiert eine halbeinfache Unteralgebra $\mathscr{U}$, die komplementär zu dem maximalen nilpotenten Ideal $\mathscr{V}$ ist.

Mit anderen Worten, jedes Element $\mathbf{a} \in \mathscr{A}$ wird gleichbedeutend in Form der Summe $\mathbf{u} + \mathbf{v}$ dargestellt, wobei der erste Summand der halbeinfachen Unteralgebra $\mathscr{U}$ angehört und der zweite dem maximalen nilpotenten Ideal $\mathscr{V}$; dem Element $\mathbf{a}$ wird gleichbedeutend das Paar $(\mathbf{u}, \mathbf{v})$ zugeordnet, wobei $\mathbf{u} \in \mathscr{U}$ und $\mathbf{v} \in \mathscr{V}$ ist.
Dabei gilt für das Produkt zweier beliebiger Elemente der Algebra $\mathscr{A}$ die Formel

$$(\mathbf{u}_1, \mathbf{v}_1)(\mathbf{u}_2, \mathbf{v}_2) = (\mathbf{u}_1\mathbf{u}_2, \mathbf{v}) \tag{2}$$

wobei

$$\mathbf{v} = \mathbf{u}_1\mathbf{v}_2 + \mathbf{v}_1\mathbf{u}_2 + \mathbf{v}_1\mathbf{v}_2 \in \mathscr{V}$$

ist (man muss berücksichtigen, dass $\mathscr{V}$ ein Ideal ist).

In dem Spezialfall, dass die Unteralgebra $\mathscr{U}$ auch ein Ideal ist, ist jedes der Produkte $\mathbf{u}_1\mathbf{v}_2$ und $\mathbf{v}_2\mathbf{u}_1$ gleich $\mathbf{0}$ (weil es gleichzeitig $\mathscr{U}$ und $\mathscr{V}$ angehören muss), und die Formel für die Multiplikation nimmt die Form

$$(\mathbf{u}_1, \mathbf{v}_1)(\mathbf{u}_2, \mathbf{v}_2) = (\mathbf{u}_1\mathbf{u}_2, \mathbf{v}_1\mathbf{v}_2)$$

an. In diesem Fall ist die Algebra $\mathscr{A}$ das direkte Produkt der Algebren $\mathscr{U}$ und $\mathscr{V}$.

Im allgemeinen Fall wird die Struktur der Algebra $\mathscr{A}$ nicht vollständig durch die Struktur der Algebra $\mathscr{U}$ und $\mathscr{V}$ einzeln bestimmt, weil das Element $\mathbf{v}$ in (2) nicht nur von $\mathbf{v}_1, \mathbf{v}_2$ abhängt, sondern auch noch von $\mathbf{u}_1, \mathbf{u}_2$.
Dennoch klärt der Umstand, dass man jede assoziative Algebra $\mathscr{A}$ als Menge der Paare $(\mathbf{u}, \mathbf{v})$ darstellen kann, wobei $\mathbf{u}$ eine bestimmte halbeinfache Algebra durchläuft und $\mathbf{v}$ eine nilpotente, und die Multiplikation dem Gesetz (2) unterworfen ist, deutlich die Struktur assoziativer Algebren.

Als Beispiel zum Satz von Wedderburn betrachten wir die Algebra der Matrizen der Ordnung $p + q$, bei denen die Elemente der letzten q Zeilen Null sind. Jede solche Matrix kann man in der Form

$$\left(\begin{array}{c|c} u & v \\ \hline 0 & 0 \end{array}\right)$$

schreiben, wobei u eine quadratische Matrix der Ordnung p und v eine rechteckige Matrix mit p Zeilen und q Spalten bedeutet. Es ist nicht schwierig zu zeigen, dass sich das maximale nilpotente Ideal $\mathscr{V}$ aus den Matrizen (3) für u ergibt (und eine Nullalgebra darstellt).
Als zu ihm komplementäre halbeinfache Unteralgebra $\mathscr{U}$ kann man die Menge der Matrizen (3) für $v = 0$ nehmen (im gegebenen Fall ist die Unteralgebra $\mathscr{U}$ einfach).

Um die Reichhaltigkeit des Satzes von Wedderburn zu unterstreichen, führen wir Beispiele

zweidimensionaler Algebren (natürlicherweise nichtassoziativer) an, für die die Behauptung des Satzes falsch ist.
Im ersten Beispiel besitzt die Multiplikationstafel die Form

$$\mathbf{e}_1\mathbf{e}_1 = \mathbf{e}_1 + \mathbf{e}_2, \qquad \mathbf{e}_2\mathbf{e}_2 = \mathbf{0}, \qquad \mathbf{e}_1\mathbf{e}_2 = \mathbf{e}_2, \qquad \mathbf{e}_2\mathbf{e}_1 = \mathbf{0}$$

Es ist leicht zu sehen, dass die Elemente der Form $k\mathbf{e}_2$ ein eindimensionales nilpotentes Ideal $\mathscr{N}$ bilden.
Dieses Ideal ist maximal, da der einzige es enthaltende Teilraum die ganze Algebra ist, die aber nicht nilpotent ist (jede Potenz des Elementes $\mathbf{e}_1$ ist von Null verschieden). Es ist leicht zu überprüfen, dass außer $\mathscr{N}$ keine andere Unteralgebra der gegebenen Algebra existiert. Damit existiert auch keine komplementäre Unteralgebra zu $\mathscr{N}$.

Die zweite Algebra besitzt folgende Multiplikationstafel:

$$\mathbf{e}_1\mathbf{e}_1 = \mathbf{e}_1, \qquad \mathbf{e}_2\mathbf{e}_2 = \mathbf{e}_2, \qquad \mathbf{e}_1\mathbf{e}_2 = \mathbf{e}_2, \qquad \mathbf{e}_2\mathbf{e}_1 = 0$$

In dieser Algebra gibt es überhaupt keine nilpotenten Ideale.
Wenn die Algebra dem Satz von Wedderburn "genügen" würde, wäre sie einfach oder halbeinfach. Das erste ist nicht der Fall, weil die Algebra ein Ideal enthält, das aus Elementen der Form $k\mathbf{e}_2$ besteht, das zweite ist auch nicht möglich, weil dieses Ideal das einzige ist.

Die Resultate, die in der Theorie assoziativer Algebren erhalten wurden, dienten als Modell für weitere Untersuchungen. Viele der nachfolgenden Arbeiten bewiesen, dass die Behauptung des Satzes von Wedderburn für andere Klassen von Algebren richtig ist (obwohl sie nicht für alle Algebren, wie wir gerade sahen, richtig sein kann), und zählten einfache Algebren dieser Klassen auf.

Es wurde bewiesen (M. Zorn), dass man den Satz von Wedderburn auf alternative Algebren verallgemeinern kann, d.h. auf eine umfassendere Klasse von Algebren als die der assoziativen. Wir bemerken, dass bei der Untersuchung einfacher alternativer Algebren eine interessante Tatsache aufgeklärt wurde. Obwohl auf den ersten Blick die Klasse solcher Algebren viel umfassender als die Klasse der einfachen assoziativen Algebren erscheint, erhält man im Falle des Körpers der komplexen Zahlen tatsächlich die erste Klasse aus der zweiten durch Hinzufügung von nur einer Algebra "komplexer" Oktaven; im Falle des Körpers der reellen Zahlen werden einige Algebren des gleichen Typs wie die Oktaven hinzugefügt.

Wir werden noch zwei Klassen von Algebren betrachten, für die der Satz von Wedderburn gilt. Dazu nehmen wir eine beliebige assoziative Algebra $\mathscr{A}$ und mit ihr bauen wir zwei neue Algebren $\mathscr{A}^+$ und $\mathscr{A}^-$ auf, die aus den gleichen Elementen mit den folgenden Multiplikationsgesetzen bestehen

in $\mathscr{A}^+$: $\mathbf{a} \diamond \mathbf{b} = \mathbf{ab} + \mathbf{ba}$,
in $\mathscr{A}^-$: $\mathbf{a} \circ \mathbf{b} = \mathbf{ab} - \mathbf{ba}$

In der Algebra $\mathscr{A}^+$ ist die Multiplikation kommutativ und, wie nicht schwer zu überprüfen ist, es wird die Identität

$$(\mathbf{b}^2 \diamond \mathbf{a}) \diamond \mathbf{b} = \mathbf{b}^2 \diamond (\mathbf{a} \diamond \mathbf{b}) \tag{3}$$

erfüllt. In der Algebra $\mathscr{A}^-$ ist die Multiplikation antikommutativ (d.h. $\mathbf{a} \circ \mathbf{b} = -\mathbf{b} \circ \mathbf{a}$) und es wird die Identität

$$\mathbf{a} \circ (\mathbf{b} \circ \mathbf{c}) + \mathbf{b} \circ (\mathbf{c} \circ \mathbf{a}) + \mathbf{c} \circ (\mathbf{a} \circ \mathbf{b}) = \mathbf{0} \tag{4}$$

erfüllt. Jede kommutative Algebra, für die (3) gilt, wird Jordansche Algebra genannt (nach dem deutschen Physiker P. Jordan).

Jede antikommutative Algebra, für die (4) gilt, wird Liesche Algebra genannt. Der norwegische Mathematiker Sophus Lie betrachtete am Ende des 19. Jahrhunderts zum ersten Mal in Verbindung mit der Theorie "stetiger Transformationsgruppen" diese Algebren, die dann nach ihm benannt wurden.
In der heutigen Mathematik spielen die Lieschen Algebren eine sehr wichtige Rolle und finden in fast jedem ihrer Gebiete Anwendung.

Die Klassifikation einfacher Jordanscher Algebren wurde durch den amerikanischen Mathematiker A. Albert erhalten; durch ihn Wurde auch die Richtigkeit des Satzes von Wedderburn für Jordansche Algebren bewiesen. Grundlegende Sätze über die Struktur von Lieschen Algebren wurden durch einen der bedeutendsten Mathematiker des 20. Jahrhunderts E. Cartan erhalten.

Durch ihn wurde insbesondere eine Klassifikation einfacher Liescher Algebren gefunden. Eine Erweiterung des Satzes von Wedderburn auf Liesche Algebren wurde durch E. Levi angegeben; dabei erwies es sich als erforderlich, den Begriff des nilpotenten Ideals in den allgemeineren Begriff des lösbaren Ideals zu verändern. Der Rahmen des vorliegenden Büchleins erlaubt es uns nicht, ausführlicher auf diese Fragen einzugehen.