Involutorische Geometrien

Wilhelm Blaschke zum 75. Geburtstag

Von Erich Ellers und Helmut Karzel in Hamburg

In der Geometrie treten häufig Mengen auf, die mit zwei Strukturen versehen sind, mit einer geometrischen und einer Gruppenstruktur. Dabei sind die beiden Strukturen durch Verträglichkeitsbedingungen miteinander verknüpft. Beispiele bilden alle affinen und euklidischen Geometrien. Die Gruppenstruktur ist hier durch die Gruppe der Ortsvektoren gegeben.

Wie kann man diesen Sachverhalt axiomatisch kennzeichnen? Wir führen hier zwei Möglichkeiten an (§ 1). Die eine wird durch die bereits in [6] angegebene Definition des (verallgemeinerten) *Gruppenraums* $D(G)$ beschrieben (der hier gebrauchte Begriff des Gruppenraums ist eine Verallgemeinerung einer Definition von R. Baer [2][1]), die in ihren Ursprüngen auf die kinematische Abbildung von Blaschke [4] und Grünwald [5] zurückgeht. Vergleiche hierzu die Einleitung von [6]). Die zweite Möglichkeit wird durch die Definition der *Inzidenzgruppe* dargelegt. Diese Definition ist der der topologischen Gruppe nachgebildet.

Die hier benutzten geometrischen Strukturen sind stets projektive Räume mit einer Dimension größer als 1. Für diesen Fall gilt, daß jede projektive Inzidenzgruppe auch als Gruppenraum deutbar ist (Satz 1).

In [6] sind die *elliptischen* Gruppenräume $D(G)$ behandelt worden, die gekennzeichnet waren durch die folgenden Eigenschaften der Teilmenge $D \in G$ (vgl. [6] S. 174):

A. *Für jedes $x \in D$ gilt $x^2 = 1$.*

B. *D ist invariant, d.h. mit $x \in D$ gilt auch $axa^{-1} \in D$ für alle $a \in G$.*

C. *D enthält mindestens zwei Elemente a, b mit $(ab)^2 \neq 1$.*

Es ergab sich in [6], daß ein elliptischer Gruppenraum $D(G)$ stets die Dimension 3 hat und daß die Gruppe G isomorph mit der Bewegungs-

---

[1]) Baer zeigt in [2]: $D(G)$ ist genau dann ein Gruppenraum mit $D = \{a \in G; a^2 = 1,\ a \neq 1\}$, wenn G die Bewegungsgruppe einer ebenen elliptischen Geometrie der Charakteristik $\neq 2$ ist.

gruppe einer ebenen elliptischen Geometrie ist. Der zugehörige Koordinatenkörper hat die Charakteristik 2 oder $\neq 2$, je nachdem, ob $1 \in D$ oder $1 \notin D$ gilt.

Hier soll die Frage untersucht werden: Welche Gruppenräume $D(G)$ bzw. welche Gruppen G werden durch die Eigenschaften A, B und die Negation

C′. *Für alle* $a,b \in D$ *gilt* $(ab)^2 = 1$.

von C gekennzeichnet? (Die Eigenschaften A und B sind übrigens eine Folge von C′.) Aus der Forderung C′ ergibt sich leicht (weil die Teilmenge D nach Satz 2 aus [6] ein Erzeugendensystem von G ist), daß die Gruppe G des Gruppenraumes $D(G)$ kommutativ ist und sogar den Exponenten 2 (d.h. für alle $x \in G$ gilt $x^2 = 1$) hat. Da auch die zyklischen Geometrien unter den Begriff Gruppenraum fallen (G ist hierbei eine zyklische Gruppe) (vgl. [6] § 2), wollen wir (nach diesem Vorbild) die Gruppenräume $D(G)$, bei denen alle Elemente $x \in G$ mit $x \neq 1$ involutorisch sind, *involutorische Geometrien* nennen.

Unsere Aufgabe besteht also darin, alle involutorischen Geometrien vollständig zu beschreiben und zu erfassen. Als Lösung erhalten wir, daß sich jede involutorische Geometrie $D(G)$ durch eine Cliffordalgebra der Charakteristik 2 darstellen läßt (Hauptsatz am Ende dieser Note). Jede Zahl der Gestalt $2^n - 1$ mit $n > 1$ kommt als Dimension einer involutorischen Geometrie vor.

Faßt man die hier gewonnenen Resultate mit denen von [6] zusammen, so erhält man nunmehr einen vollständigen Überblick über alle Gruppenräume, die durch die Eigenschaften A und B gekennzeichnet sind. Alle Gruppenräume $D(G)$ mit den Eigenschaften A, B zerfallen nämlich in drei disjunkte Klassen:

1. Elliptische Gruppenräume der Charakteristik $\neq 2$ (gekennzeichnet durch C und $1 \notin D$). Hier gilt: $\dim(D(G)) = 3$, $G \cong 0_3^+(K,F)$, wobei K ein kommutativer Körper der Charakteristik $\neq 2$ ist und F eine ternäre nullteilige quadratische Form.

2. Elliptische Gruppenräume der Charakteristik 2 (gekennzeichnet durch C und $1 \in D$). Hier gilt: $\dim(D(G)) = 3$, $G \cong 0_3(K,Q)$, wobei K ein kommutativer Körper der Charakteristik 2 ist und Q eine ternäre nullteilige und nichtquasilineare quadratische Form über K.

3. Involutorische Geometrien (gekennzeichnet durch C′). Hier gilt: Die Dimension von $D(G)$ ist eine natürliche Zahl der Gestalt $2^n - 1$ mit $n > 1$, $G \cong C^*/K^*$, wobei C eine Cliffordalgebra ist, die gleichzeitig ein kommutativer Körper der Charakteristik 2 ist und einen Grad 2^n mit $n > 1$ über dem Grundkörper K hat.

§ 1. Gruppenräume und Inzidenzgruppen

Wie in [6] ordnen wir einer Gruppe G mit Hilfe einer Teilmenge D von G eine *geometrische Struktur* $D(G)$ wie folgt zu:

R 1. *Jedes Element $a \in G$ stellt sowohl einen Punkt als auch eine Hyperebene dar* (während wir den a zugeordneten Punkt auch mit a bezeichnen, symbolisiere $\langle a \rangle$ die zugeordnete Hyperebene).

R 2. *Zwei verschiedenen Elementen aus G entsprechen verschiedene Punkte und verschiedene Hyperebenen.*

R 3. *Inzident heißt ein Punkt a und eine Hyperebene $\langle b \rangle$ genau dann, wenn $ab \in D$ gilt.*

Ist $D(G)$ ein projektiver Raum mit $\dim(D(G)) > 1$, so nennen wir $D(G)$ einen *Gruppenraum*.

Nach dem Vorbild des Begriffs der topologischen Gruppe definieren wir hier:

Eine Menge G heißt *Inzidenzgruppe*, wenn folgendes gilt:

G 1. *G ist eine Gruppe.*

G 2. *G ist mit einer geometrischen Struktur versehen, deren Punkte die Elemente von G sind.*

G 3. *Die beiden Strukturen sind verträglich, d.h. die Translationen*

$$\begin{cases} G \to G \\ x \to xa \end{cases} \qquad \begin{cases} G \to G \\ x \to ax \end{cases}$$

sind für jedes $a \in G$ Automorphismen der geometrischen Struktur.

Ist die geometrische Struktur insbesondere ein endlichdimensionaler projektiver Raum, dessen Dimension größer als 1 ist (die Translationen sind dann Projektivitäten), so heißt G *projektive Inzidenzgruppe*.

Satz 1. *In jeder projektiven Inzidenzgruppe G gibt es eine Teilmenge D von G, so daß $D(G)$ ein Gruppenraum ist, dessen geometrische Struktur mit der von G übereinstimmt. Hierbei genügt D der Eigenschaft:*

(1) *Zu jedem $a \in G$ gibt es ein $a' \in G$ mit $aDa' = D$.*

Ist umgekehrt $D(G)$ ein Gruppenraum und genügt D der Bedingung (1), *so ist G hinsichtlich der durch $D(G)$ gegebenen geometrischen Struktur eine projektive Inzidenzgruppe.*

Beweis. Es sei G eine projektive Inzidenzgruppe. Wir betrachten eine beliebige aber fest ausgewählte Hyperebene. Mit D bezeichnen wir die Gesamtheit der Gruppenelemente, die mit dieser Hyperebene inzidieren. Auf Grund der Verträglichkeitseigenschaft G 3 füllt jede der Punktgesamtheiten aD und Da mit $a \in G$ eine Hyperebene aus. Als erstes zeigen wir:

Hat die projektive Inzidenzgruppe die Dimension n, so gibt es zu n Punkten $a_1, \ldots, a_n$ stets eine Hyperebene der Gestalt Db (und eine der Gestalt $b'D$), die mit ihnen inzidiert.

Die Hyperebenen $a_1^{-1}D, a_2^{-1}D, \ldots, a_n^{-1}D$ haben einen nicht leeren Durchschnitt. Es sei etwa $c \in a_1^{-1}D \cap \ldots \cap a_n^{-1}D$, d.h. es gibt $d_i \in D$ mit $c = a_i^{-1}d_i$, $(i = 1, \ldots, n)$. Hieraus folgt $a_i = d_i c^{-1} \in Db$, wenn $c^{-1} = b$ gesetzt wird.

Zweitens wird bewiesen:

$$\text{Aus } Da = Db \quad \text{folgt} \quad a = b$$

oder gleichwertig hiermit:

$$\text{Aus } Da = D \quad \text{folgt} \quad a = 1\,.$$

Um das einzusehen, wählen wir n linear unabhängige Hyperebenen $D, c_2D, \ldots, c_nD$. Diese haben genau einen Punkt d gemein. Das gleiche gilt dann auf Grund von Eigenschaft G 3 für die Hyperebenen $Da, c_2Da, \ldots, c_nDa$, die nur den Punkt da gemein haben. Aus $Da = D$ folgt aber, daß $c_iDa = c_iD$ für $i = 2, \ldots, n$ ist. Also muß $d = da$ sein, d.h. $a = 1$.

Aus diesen Resultaten erkennt man, daß sich jede Hyperebene des projektiven Raumes in der Gestalt Da mit $a \in G$ darstellen läßt und daß die Zuordnung $a \leftrightarrow Da^{-1}$ die Gruppenelemente eineindeutig auf die Hyperebenen des Raumes abbildet. Man sieht also, daß jedes Gruppenelement a gleichzeitig einen Punkt und eine Hyperebene (bezeichnet durch $\langle a\rangle$) repräsentiert. Ist nun a ein Punkt und $\langle b\rangle$ eine Hyperebene, so inzidieren a und $\langle b\rangle$ genau dann, wenn $ab \in D$ ist. Also ist $D(G)$ ein Gruppenraum. Die Eigenschaft (1) folgt aus der Tatsache, daß sich die Hyperebene $c^{-1}D$ auch in der Form Dc' darstellen läßt.

Um den zweiten Teil von Satz 1 zu beweisen, haben wir nur die Verträglichkeitseigenschaft G 3 nachzuweisen:

Nach [6] S. 170 ist die Punktabbildung $x \to xa$ ein Automorphismus von $D(G)$. Daß auch $x \to ax$ ein Automorphismus von $D(G)$ ist, folgern wir aus (1): eine Hyperebene $\langle x\rangle$ wird auf $\langle xa'\rangle$ abgebildet. Ist nämlich $xy \in D$, so folgt $axya' \in D$, d.h. aus der Inzidenz von x und $\langle y\rangle$ folgt die Inzidenz von ax und $\langle ya'\rangle$.

§ 2. Involutorische Geometrien

Wir nennen einen Gruppenraum $D(G)$ *involutorische Geometrie*, wenn G den Exponenten 2 hat, d.h. wenn $a^2 = 1$ für jedes $a \in G$ gilt.

Von nun an sollen nur noch involutorische Geometrien betrachtet werden.

Wie in [6] § 1 gezeigt worden ist, erhält man einen isomorphen Gruppenraum, wenn man D durch $D' = aD$ ersetzt. Daher bedeutet es keine Einschränkung der Allgemeinheit, wenn wir hier zusätzlich fordern, daß das Einselement 1 von G in D liegt $(1 \in D)$.

Unter dieser Voraussetzung stellt die Abbildung $a \leftrightarrow \langle a^{-1} \rangle$ ein Nullsystem dar (weil $D^{-1} \subset D$ und $1 \in D$), wie ebenfalls in [6] gezeigt worden ist. Dies bedeutet aber:

(2) *Die Dimension $D(G)$ ist endlich und ungerade.*

Für Dimensionen ≥ 3 ist dies bekannt[2]). Daß die Dimensionen 2 nicht auftreten kann, folgt ebenfalls bereits aus den Voraussetzungen $D^{-1} \subset D$ und $1 \in D$ (hier benötigt man nicht die Voraussetzung, daß G den Exponenten 2 hat): Wäre nämlich $\dim(D(G)) = 2$, so würden im Widerspruch zu den ebenen Inzidenzaxiomen für $a \in D$, $a \neq 1$[3]) die zwei verschiedenen Punkte 1 und a (wegen $D^{-1} \subset D$) sowohl mit der Geraden $\langle 1 \rangle$ als auch mit der Geraden $\langle a^{-1} \rangle$ inzidieren.

Aus der Existenz eines Nullsystems und (2) folgt somit[2]):

(3) *$D(G)$ besitzt als Koordinatenbereich einen kommutativen Körper.*

Um die Struktur des Raumes $D(G)$ näher zu untersuchen, führen wir einige Abkürzungen ein.

Definition. Ist M eine Teilmenge von G, so bezeichnet $\overline{M}$ den kleinsten projektiven Unterraum von $D(G)$, der sämtliche Punkte $x \in M$ enthält und $[M]$ die von den Elementen aus M erzeugte Untergruppe von G.

Ist $c \in G$, so bezeichnet c^* die Translation[4])

(4) $$c^*: \begin{cases} a \to ca = c^*(a) \\ \langle a \rangle \to \langle ca \rangle = c^*\langle a \rangle \end{cases} \quad \text{für jedes } a \in G.$$

Offenbar gilt:

Die Gesamtheit aller Projektivitäten c^* mit $c \in G$ bildet eine zu G isomorphe Gruppe G^*.

(5) *Bei der Kollineation c^* ist das Bild des von $M \subset G$ aufgespannten Raumes $\overline{M}$ der Raum $\overline{cM}$, der von der Menge cM aufgespannt wird, d.h. $c^*(\overline{M}) = c\overline{M} = \overline{cM}$.*

Es sei U eine Untergruppe von G. Nach (5) gilt:

(6) *Aus $a \in U$ und $x \in \overline{U}$ folgt $ax \in \overline{U}$.*

---

[2]) Vgl. z.B. [3], S. 108.

[3]) D enthält mindestens zwei Elemente; andernfalls wäre $\dim D(G) = 1$. Vgl. [6], Satz 1.

[4]) Da G kommunativ ist, stimmen Links- und Rechtstranslationen überein.

Aus (6) folgt unmittelbar: Für jedes $x \in \bar{U}$ gilt $\overline{Ux} \subset \bar{U}$, d.h.:

$$\text{(7)} \qquad \textit{Aus } x \in \bar{U} \textit{ folgt } \bar{U} = \overline{[U, x]}.$$

Sind jetzt x und y zwei Punkte des Raumes $\bar{U}$, so gilt nach (7):

$$\bar{U} = \overline{[U, x]} = \overline{[U, x, y]} \quad \text{und} \quad xy \in \bar{U}, \quad \text{weil} \quad xy \in [U, x, y].$$

Damit haben wir bewiesen:

Satz 2. *Ist U eine Untergruppe von G, so ist auch die Menge $\bar{U}$ eine Untergruppe von G.*

Eine unmittelbare Folge von Satz 2 ist

Satz 3. *Mit N ist auch die Menge $\bar{N}$ eine Nebengruppe in G.*

Ein Teilraum T von $D(G)$ heißt *ausgezeichnet*, wenn es eine Nebengruppe N in G gibt mit $\bar{N} = T$.

Satz 4. *Der Durchschnitt zweier ausgezeichneter Teilräume ist ausgezeichnet oder leer.*

Beweis. Der Punkt x liege in den Nebengruppen $a\bar{U}$ und $b\bar{V}$. Dann gilt $x^*(a\bar{U}) = \bar{U}$ und $x^*(b\bar{V}) = \bar{V}$. Denn aus $x \in a\bar{U}$ und $x \in b\bar{V}$ folgt $a\bar{U} = x\bar{U}$ und $b\bar{V} = x\bar{V}$. Nun ist aber der Durchschnitt der beiden Untergruppen $\bar{U}$ und $\bar{V}$, die gleichzeitig Teilräume sind, sowohl Untergruppe als auch linearer Teilraum. Hieraus erkennt man $a\bar{U} \cap b\bar{V} = x(\bar{U} \cap \bar{V})$.

Satz 5. *Zu jeder Untergruppe U von G gibt es eine Untergruppe V von G mit $\bar{V} = \bar{U}$ und* $\operatorname{Ord}(V) = \dim \bar{U} + 1$.

Beweis. Wir konstruieren rekursiv folgende Untergruppen:

$$\begin{aligned} V_0 &= [1] \\ V_1 &= [1, a_1], && \text{falls} \quad a_1 \in \bar{U} \quad \text{und} \quad a_1 \notin \bar{V}_0 \\ V_n &= [V_{n-1}, a_n], && \text{falls} \quad a_n \in \bar{U} \quad \text{und} \quad a_n \notin \overline{V_{n-1}} \end{aligned}$$

und behaupten: Alle Punkte x mit $x \in V_i$ sind linear unabhängig. Den Beweis führen wir durch vollständige Induktion. Für $i = 0$ ist die Aussage trivial. Da die Gruppe G den Exponenten 2 hat, gilt $V_n = V_{n-1} \cup a_n V_{n-1}$ für die oben konstruierten V_n. Nehmen wir nun an, daß die Punkte $x \in V_{n-1}$ linear unabhängig sind, so trifft das auch für die Punkte $y \in a_n V_{n-1}$ zu. Nach Satz 4 und der Konstruktion der V_i gilt $\overline{V_{n-1}} \cap \overline{a_n V_{n-1}} = \emptyset$. Also müssen nach dem Dimensionssatz die Punkte $x \in V_{n-1} \cup a_n V_{n-1}$ linear unabhängig sein.

Da die Gruppe G den Exponenten 2 hat, ist die Ordnung jeder endlichen Untergruppe eine Zweierpotenz. Daher ergibt sich sofort aus Satz 5:

Satz 6. *Als Dimension jedes ausgezeichneten Raumes (insbesondere des gesamten Raumes) kommen nur Zahlen der Form* $2^n - 1$ *in Frage.*

§ 3. Darstellung der involutorischen Geometrien durch Cliffordalgebren

Unter einer *Algebra* $\mathfrak{A} = \{\mathfrak{a}, \mathfrak{b}, \ldots\}$ verstehen wir hier eine Menge mit folgenden Eigenschaften:

1. $\mathfrak{A}$ *ist ein endlichdimensionaler Vektorraum über einem Körper* $K = \{\alpha, \beta, \ldots\}$.
2. *In* $\mathfrak{A}$ *ist eine assoziative Multiplikation erklärt, die dem linksseitigen Distributivgesetz*

(8) $$\mathfrak{a}(\mathfrak{b} + \mathfrak{c}) = \mathfrak{a}\mathfrak{b} + \mathfrak{a}\mathfrak{c}$$

genügt und für die ferner gilt

(9) $$\alpha(\mathfrak{a}\mathfrak{b}) = (\alpha\mathfrak{a})\mathfrak{b}.$$

Diese Definition stimmt weitgehend mit der üblichen (vgl. z.B. [7] S. 53) überein. Wir verzichten hier nur auf das rechtsseitige Distributivgesetz und ersetzen die Regel $(\alpha\mathfrak{a})\mathfrak{b} = \mathfrak{a}(\alpha\mathfrak{b}) = \alpha(\mathfrak{a}\mathfrak{b})$ durch die schwächere Forderung (9).

Nun soll jeder involutorischen Geometrie $D(G)$ eine Algebra $\mathfrak{A}$ zugeordnet werden. Nach (3) wissen wir bereits, daß der projektive Raum $D(G)$ einen kommutativen Koordinatenkörper K besitzt. Also läßt sich $D(G)$ durch einen Vektorraum $\mathfrak{A}$ über K darstellen. Hierbei ist jedem $a \in G$ der Teilraum $K\mathfrak{a}$ von $\mathfrak{A}$ zugeordnet:

(10) $$a \leftrightarrow K\mathfrak{a}.$$

Für die nun folgende Definition der Multiplikation benötigen wir noch die Zuordnung

(11) $\mathfrak{e}$ *sei ein fester der* $1 \in G$ *entsprechender Vektor.*

Die Projektivität a^* [vgl. (4)] läßt sich in $\mathfrak{A}$ durch eine semilineare Abbildung darstellen. Jedem $\mathfrak{a} \in \mathfrak{A}$, $\mathfrak{a} \neq 0$, ordnen wir eineindeutig die semilineare Abbildung $\mathfrak{a}^*$ zu, die durch folgende Vorschriften gekennzeichnet ist:

(12) *Ist* $a \leftrightarrow K\mathfrak{a}$, *so sei* $\mathfrak{a}^*$ *eine Darstellung von* a^*.

(13) $$\mathfrak{a}^* : \mathfrak{e} \to \mathfrak{a}.$$

Die Forderung (13) ist erfüllbar, weil $a^*(1) = a$ und $1 \leftrightarrow K\mathfrak{e}$ gilt.

Da $\lambda\mathfrak{a}^* : \mathfrak{e} \to \lambda\mathfrak{a}$ gilt, ist

$$(\lambda\mathfrak{a})^* = \lambda\mathfrak{a}^*. \tag{14}$$

Die Multiplikation in $\mathfrak{A}$ erklären wir durch:

$$\mathfrak{a} \cdot \mathfrak{b} = \mathfrak{a}^* \cdot \mathfrak{b}^*(\mathfrak{e}) \tag{15}$$

und

$$0 \cdot \mathfrak{a} = 0. \tag{16}$$

Hieraus erkennt man sofort:

$$(\mathfrak{a}\mathfrak{b})^* = \mathfrak{a}^* \cdot \mathfrak{b}^*. \tag{17}$$

Satz 7. *$\mathfrak{A}$ ist eine Algebra, die auch bezüglich der Multiplikation eine Gruppe bildet.*

Beweis. Assoziativgesetz: Auf Grund von (15) und (17) gilt

$$\mathfrak{a}(\mathfrak{b}\mathfrak{c}) = \mathfrak{a}^*(\mathfrak{b}\mathfrak{c})^*(\mathfrak{e}) = \mathfrak{a}^*(\mathfrak{b}^*\mathfrak{c}^*)(\mathfrak{e}) = (\mathfrak{a}^*\mathfrak{b}^*)\mathfrak{c}^*(\mathfrak{e}) = (\mathfrak{a}\mathfrak{b})^*\mathfrak{c}^*(\mathfrak{e}) = (\mathfrak{a}\mathfrak{b})\mathfrak{c}.$$

Einselement: $\mathfrak{e}\mathfrak{a} = \mathfrak{e}^*\mathfrak{a}^*(\mathfrak{e}) = \mathfrak{e}^*(\mathfrak{a}) = \mathfrak{a}$. Dies gilt, da $\mathfrak{e}^*$ die Identität in $D(G)$ induziert und weil nach (13) $\mathfrak{e}^*(\mathfrak{e}) = \mathfrak{e}$ ist.

Inverses: Da wegen $a^2 = 1$ die semilineare Abbildung $\mathfrak{a}^*\mathfrak{a}^*$ die Identität in $D(G)$ induziert, gilt:

$$\mathfrak{a}\mathfrak{a} = \mathfrak{a}^*\mathfrak{a}^*(\mathfrak{e}) = \gamma_{\mathfrak{a}}\mathfrak{e} \quad \text{mit} \quad \gamma_{\mathfrak{a}} \in K^* \tag{18}$$ [5])

und:

$$\mathfrak{a}^{-1} = \gamma_{\mathfrak{a}}^{-1}\mathfrak{a}, \tag{19}$$

denn es ist

$$(\gamma_{\mathfrak{a}}^{-1}\mathfrak{a})\mathfrak{a} = (\gamma_{\mathfrak{a}}^{-1}\mathfrak{a})^*\mathfrak{a}^*(\mathfrak{e}) = \gamma_{\mathfrak{a}}^{-1}\mathfrak{a}^*\mathfrak{a}^*(\mathfrak{e}) = \gamma_{\mathfrak{a}}^{-1}\gamma_{\mathfrak{a}}(\mathfrak{e}) = \mathfrak{e} \quad \text{[vgl. (14)]}.$$

Linksseitiges Distributivgesetz:

$$\mathfrak{a}(\mathfrak{b} + \mathfrak{c}) = \mathfrak{a}\mathfrak{b} + \mathfrak{a}\mathfrak{c}, \tag{20}$$

denn es ist

$$\begin{aligned}\mathfrak{a}(\mathfrak{b} + \mathfrak{c}) &= \mathfrak{a}^*(\mathfrak{b} + \mathfrak{c})^*(\mathfrak{e}) = \mathfrak{a}^*(\mathfrak{b} + \mathfrak{c}) = \mathfrak{a}^*(\mathfrak{b}) + \mathfrak{a}^*(\mathfrak{c}) \\ &= \mathfrak{a}^*\mathfrak{b}^*(\mathfrak{e}) + \mathfrak{a}^*\mathfrak{c}^*(\mathfrak{e}) = \mathfrak{a}\mathfrak{b} + \mathfrak{a}\mathfrak{c}\end{aligned}$$

[vgl. hierzu (15) und (13)].

Das Gesetz (9) folgt unmittelbar aus (14) und (15).

In $\mathfrak{A}$ sind also alle Schiefkörperaxiome bis auf das rechtsseitige Distributivgesetz erfüllt, d.h. $\mathfrak{A}$ ist ein Fastkörper.

[5]) Unter K^* verstehen wir wie üblich die Menge der von 0 verschiedenen Elemente von K.

Da $\mathfrak{A}$ ein Einselement enthält, ist die Teilmenge $\{\lambda\mathfrak{e} : \lambda \in K\}$ ein zu K isomorpher Körper; wir identifizieren daher $\lambda\mathfrak{e}$ mit λ. Aus dieser Identifizierung, Satz 7 und (18) ergibt sich der folgende Satz:

Satz 8. *Die einer involutorischen Geometrie zugeordnete Algebra $\mathfrak{A}$ hat die Eigenschaften:*

a) *$\mathfrak{A}$ enthält ein Einselement $\mathfrak{e} = 1$.*

b) *Für alle $\mathfrak{a} \in \mathfrak{A}$ gilt $\mathfrak{a}\mathfrak{a} = \gamma_\mathfrak{a} \in K^*$.*

c) *Der Rang von $\mathfrak{A}$ über K ist größer als 2.*

Jetzt gehen wir von einer Algebra aus, die die Eigenschaften a), b), c) hat. Diese enthält wegen b) den Grundkörper K und hat folgende weitere Eigenschaften:

(21) *$\mathfrak{A}^*$ bildet bezüglich der Multiplikation eine Gruppe.*

Zu zeigen ist nur, daß es zu jedem $\mathfrak{a} \in \mathfrak{A}^*$ ein Inverses $\mathfrak{a}^{-1}$ gibt. Aus der Forderung $\mathfrak{a}\mathfrak{a} = \gamma_\mathfrak{a} \in K^*$ ergibt sich aber $\gamma_\mathfrak{a}^{-1}\mathfrak{a} = \mathfrak{a}^{-1}$.

(22) *Der Kommutator* $[\mathfrak{a}, \mathfrak{b}] = \mathfrak{a}\mathfrak{b}\,\mathfrak{a}^{-1}\,\mathfrak{b}^{-1}$ *liegt in K^* für $\mathfrak{a}, \mathfrak{b} \in \mathfrak{A}^*$.*

Für die Rechnung, bei der mehrmals von b) Gebrauch gemacht wird, ist es einfacher, $\mathfrak{a}^{-1}\mathfrak{b}^{-1}\mathfrak{a}\mathfrak{b} \in K^*$ nachzuweisen.
$\mathfrak{a}^{-1}\mathfrak{b}^{-1}\mathfrak{a}\mathfrak{b} = (\mathfrak{b}\mathfrak{a})^{-1}\mathfrak{a}\mathfrak{b} = \gamma_{\mathfrak{b}\mathfrak{a}}^{-1}\mathfrak{b}\mathfrak{a}\mathfrak{a}\mathfrak{b} = \gamma_{\mathfrak{b}\mathfrak{a}}^{-1}\mathfrak{b}\gamma_\mathfrak{a}\mathfrak{b} = \gamma_{\mathfrak{b}\mathfrak{a}}^{-1}\gamma_\mathfrak{a}^{-1}(\gamma_\mathfrak{a}\mathfrak{b})\,(\gamma_\mathfrak{a}\mathfrak{b}) \in K^*$.

Satz 9. *Sind die Elemente $1, \mathfrak{a}, \mathfrak{b} \in \mathfrak{A}$ unabhängig über K, so gilt dies auch für die Elemente $1, \mathfrak{a}, \mathfrak{b}, \mathfrak{b}\mathfrak{a}$.*

Beweis. Aus $\mathfrak{b}\mathfrak{a} = -\alpha\mathfrak{a} + \beta\mathfrak{b} + \gamma$ würde nämlich

$$\mathfrak{b}\mathfrak{a} + \alpha\mathfrak{a} = \beta\mathfrak{b} + \gamma = \mathfrak{c} \neq 0 \tag{23}$$

folgen. Da der von $1, \mathfrak{b}$ aufgespannte Vektorraum $\mathfrak{L}$ die Dimension 2 hat und $\mathfrak{a} \notin \mathfrak{L}$, kann der von $\mathfrak{a}$ und $\mathfrak{b}\mathfrak{a}$ aufgespannte Vektorraum $\mathfrak{R}$ mit $\mathfrak{L}$ nur den Vektorraum $K\mathfrak{c}$ gemein haben. Multipliziert man (23) von links mit $\mathfrak{b}$, so ergibt sich:

$$\gamma_\mathfrak{b}\mathfrak{a} + \mathfrak{b}\alpha\mathfrak{a} = \mathfrak{b}\beta\mathfrak{b} + \mathfrak{b}\gamma = \mathfrak{b}\mathfrak{c}$$

oder

$$\gamma_\mathfrak{b}\mathfrak{a} + [\mathfrak{b}, \alpha]\alpha(\mathfrak{b}\mathfrak{a}) = [\mathfrak{b}, \beta]\beta\gamma_\mathfrak{b} + [\mathfrak{b}, \gamma]\gamma\mathfrak{b} = \mathfrak{b}\mathfrak{c}.$$

(Hierbei denken wir uns zur Vereinfachung der Rechnung die Definition des Kommutators $[\mathfrak{a}, \mathfrak{b}]$ auch auf den Fall ausgedehnt, daß $\mathfrak{a} = 0$ oder $\mathfrak{b} = 0$ ist und setzen dann $[\mathfrak{a}, \mathfrak{b}] = 1$.)

Da nach (22) alle Kommutatoren in K liegen, gilt:

$$\gamma_\mathfrak{b}\mathfrak{a} + [\mathfrak{b}, \alpha]\alpha(\mathfrak{b}\mathfrak{a}) \in \mathfrak{R},$$

$$[\mathfrak{b}, \beta]\beta\gamma_\mathfrak{b} + [\mathfrak{b}, \gamma]\gamma\mathfrak{b} \in \mathfrak{L},$$

also $\mathfrak{b}\mathfrak{c} \in \mathfrak{N} \cap \mathfrak{L} = K\mathfrak{c}$, d.h. $\mathfrak{b}\mathfrak{c} = \lambda\mathfrak{c}$ mit $\lambda \in K$ oder $\mathfrak{b} = \lambda \in K$. Folglich wären $1, \mathfrak{a}, \mathfrak{b}$ linear abhängig.

Satz 10. *Eine Algebra $\mathfrak{A}$ mit den Eigenschaften* a), b), c) *ist kommutativ.*

Beweis. Aus c) folgt: In $\mathfrak{A}$ gibt es zu jedem $\mathfrak{a} \in \mathfrak{A}$ mit $\mathfrak{a} \notin K$ ein $\mathfrak{b} \in \mathfrak{A}$, so daß $1, \mathfrak{a}, \mathfrak{b}$ über K unabhängig sind. Nach Satz 9 sind dann auch die Elemente $1, \mathfrak{a}, \mathfrak{b}, \mathfrak{b}\mathfrak{a}$ unabhängig. Wir berechnen das Produkt $(1 + \mathfrak{a})(1 + \mathfrak{b})$ auf verschiedene Weisen.

$$\begin{aligned}(1+\mathfrak{a})(1+\mathfrak{b}) &= 1 + \mathfrak{a} + [1+\mathfrak{a}, \mathfrak{b}](\mathfrak{b} + \mathfrak{b}\mathfrak{a}) \\ &= 1 + \mathfrak{a} + [1+\mathfrak{a}, \mathfrak{b}]\mathfrak{b} + [1+\mathfrak{a}, \mathfrak{b}]\mathfrak{b}\mathfrak{a},\end{aligned}$$

$$\begin{aligned}(1+\mathfrak{a})(1+\mathfrak{b}) &= [1+\mathfrak{a}, 1+\mathfrak{b}](1+\mathfrak{b})(1+\mathfrak{a}) \\ &= [1+\mathfrak{a}, 1+\mathfrak{b}]\{1 + \mathfrak{b} + [1+\mathfrak{b}, \mathfrak{a}]\mathfrak{a} \\ &\qquad + [1+\mathfrak{b}, \mathfrak{a}][\mathfrak{a}, \mathfrak{b}]\mathfrak{b}\mathfrak{a}\}.\end{aligned}$$

Koeffizientenvergleich ergibt:

$$\begin{array}{lrl}
\text{Für} & 1: & 1 = [1+\mathfrak{a}, 1+\mathfrak{b}], \\
,, & \mathfrak{a}: & 1 = [1+\mathfrak{a}, 1+\mathfrak{b}][1+\mathfrak{b}, \mathfrak{a}] = [1+\mathfrak{b}, \mathfrak{a}], \\
,, & \mathfrak{b}: & [1+\mathfrak{a}, \mathfrak{b}] = [1+\mathfrak{a}, 1+\mathfrak{b}] = 1, \\
,, & \mathfrak{b}\mathfrak{a}: & [1+\mathfrak{a}, \mathfrak{b}] = [1+\mathfrak{a}, 1+\mathfrak{b}][1+\mathfrak{b}, \mathfrak{a}][\mathfrak{a}, \mathfrak{b}].
\end{array}$$

Also gilt $[\mathfrak{a}, \mathfrak{b}] = 1$, d.h. $\mathfrak{a}\mathfrak{b} = \mathfrak{b}\mathfrak{a}$ für zwei beliebige Elemente $\mathfrak{a}, \mathfrak{b}$, die mit 1 zusammen linear unabhängig sind. Da mit $1, \mathfrak{a}, \mathfrak{b}$ auch $1, \mathfrak{a}, \lambda\mathfrak{b}$ (mit $\lambda \in K^*$) linear unabhängig sind, gilt $(\lambda\mathfrak{a})\mathfrak{b} = \lambda(\mathfrak{a}\mathfrak{b}) = \lambda(\mathfrak{b}\mathfrak{a}) = (\lambda\mathfrak{b})\mathfrak{a} = \mathfrak{a}(\lambda\mathfrak{b}) = (\mathfrak{a}\lambda)\mathfrak{b}$, d.h. $\mathfrak{a}\lambda = \lambda\mathfrak{a}$ für jedes $\lambda \in K$ und jedes $\mathfrak{a} \in \mathfrak{A}$ mit $\mathfrak{a} \notin K$.

Hieraus folgt sofort, daß K kommutativ ist:

$$(\mu\lambda)\mathfrak{a} = \mu(\lambda\mathfrak{a}) = (\lambda\mathfrak{a})\mu = \lambda(\mathfrak{a}\mu) = \lambda(\mu\mathfrak{a}) = (\lambda\mu)\mathfrak{a},$$

d.h.

$$\mu\lambda = \lambda\mu \quad \text{für} \quad \lambda, \mu \in K.$$

Schließlich seien $\mathfrak{a}, \mathfrak{b}$ zwei Elemente aus $\mathfrak{A}$, die zusammen mit 1 abhängig sind, aber nicht in K liegen. $\mathfrak{c} \in \mathfrak{A}$ sei so gewählt, daß $1, \mathfrak{a}, \mathfrak{c}$ unabhängig sind. Dann sind auch $1, \mathfrak{b}, \mathfrak{c}$ unabhängig. Nach Satz 9 sind $1, \mathfrak{b}, \mathfrak{b}\mathfrak{c}$ unabhängig und daher auch $1, \mathfrak{a}, \mathfrak{b}\mathfrak{c}$. Also gilt $\mathfrak{a}\mathfrak{b}\mathfrak{c} = \mathfrak{a}(\mathfrak{b}\mathfrak{c}) = (\mathfrak{b}\mathfrak{c})\mathfrak{a} = \mathfrak{b}(\mathfrak{c}\mathfrak{a}) = \mathfrak{b}\mathfrak{a}\mathfrak{c}$, d.h. $\mathfrak{a}\mathfrak{b} = \mathfrak{b}\mathfrak{a}$. Damit ist gezeigt, daß $\mathfrak{A}$ kommutativ ist.

Aus der Kommutativität von $\mathfrak{A}$ folgt das rechte Distributivgesetz, d.h. $\mathfrak{A}$ ist sogar ein Körper.

(24) *Der Grundkörper K von $\mathfrak{A}$ hat die Charakteristik* 2,

denn ist $\mathfrak{a} \in \mathfrak{A}$, $\mathfrak{a} \notin K$, so liegen $(\mathfrak{a} + 1)^2 = \mathfrak{a}^2 + 2\mathfrak{a} + 1$ und $\mathfrak{a}^2$ wegen b) in K, woraus $2 = 0$ folgt, da $\mathfrak{a} \notin K$.

Nachdem wir jeder involutorischen Geometrie eine Algebra zugeordnet haben, wollen wir umgekehrt zeigen, daß jeder Algebra $\mathfrak{A}$ mit den Eigenschaften a), b), c) eine involutorische Geometrie entspricht.

(25) $\mathfrak{A}^*/K^*$ *ist eine Inzidenzgruppe vom Exponenten* 2.

Da $\mathfrak{A}$ ein Vektorraum ist, entspricht $\mathfrak{A}$ in bekannter Weise ein projektiver Raum Π. Wir können daher die Elemente der Faktorgruppe $\mathfrak{A}^*/K^*$ mit den Punkten des projektiven Raumes Π identifizieren. Damit ist $\mathfrak{A}^*/K^*$ gleichzeitig Gruppe und projektiver Raum. Sie ist sogar eine Inzidenzgruppe, denn die Verträglichkeit ergibt sich wie folgt:

Die Algebra ist ein kommutativer Körper, daher ist $\mathfrak{x} \to \mathfrak{a}\mathfrak{x} = \mathfrak{x}\mathfrak{a}$ eine lineare Abbildung des Vektorraumes $\mathfrak{A}$ in sich und induziert folglich in $\mathfrak{A}^*/K^*$ eine Projektivität.

In der Inzidenzgruppe $\mathfrak{A}^*/K^*$ gibt es nach Satz 1 eine Teilmenge D, so daß $D(\mathfrak{A}^*/K^*)$ ein Gruppenraum ist. Dieser ist wegen (25) eine involutorische Geometrie. Hiermit ist gezeigt:

Satz 11. *Ist* $\mathfrak{A}$ *eine Algebra mit den Eigenschaften* a), b), c), *so gibt es in* $\mathfrak{A}^*/K^*$ *eine Teilmenge* D, *so daß* $D(\mathfrak{A}^*/K^*)$ *eine involutorische Geometrie ist.*

Aus Satz 5, Satz 6 und Satz 11 ergibt sich:

Satz 12. *Der Rang einer Algebra mit den Eigenschaften* a), b), c) *ist eine Zahl der Form* 2^n. *Es gibt* n *Elemente* $\mathfrak{a}_1, \ldots, \mathfrak{a}_n \in \mathfrak{A}$, *so daß alle* 2^n *Elemente der Form* $\mathfrak{a}_1^{\varepsilon_1} \mathfrak{a}_2^{\varepsilon_2} \ldots \mathfrak{a}_n^{\varepsilon_n}$ *mit* $\varepsilon_i = 1$ *oder* $= 0$ *eine Basis von* $\mathfrak{A}$ *bilden.*

Beweis. U sei eine Untergruppe von $\mathfrak{A}^*/K^*$ mit $\overline{U} = \mathfrak{A}^*/K^*$ und $\mathrm{Ord}(U) = \dim D(\mathfrak{A}^*/K^*) + 1 = 2^n$. Nach dem Basissatz für abelsche Gruppen gibt es in U eine Basis von n Elementen $\mathfrak{a}_1 K^*, \ldots, \mathfrak{a}_n K^*$. Da alle Punkte der Gestalt $(\mathfrak{a}_1 K^*)^{\varepsilon_1} \cdots (\mathfrak{a}_n K^*)^{\varepsilon_n}$ den Raum $D(\mathfrak{A}^*/K^*)$ aufspannen, sind die Koordinatenvektoren $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ von $\mathfrak{a}_1 K^*, \ldots, \mathfrak{a}_n K^*$ die gesuchten n Elemente aus $\mathfrak{A}$.

Als Zusammenfassung unserer Ergebnisse erhalten wir:

Hauptsatz. *Jede involutorische Geometrie* $D(G)$ *läßt sich durch eine Cliffordalgebra*[6] $\mathfrak{C}$ *darstellen, so daß* $G \cong \mathfrak{C}^*/K^*$ *ist. Hierbei ist* $\mathfrak{C}$ *ein kommutativer Körper der Charakteristik* 2 *vom Grade* 2^n *(mit* $n > 1$*) über* K. *Eine Cliffordalgebra mit diesen Eigenschaften ist bereits durch die Forderungen* a), b), c) *gekennzeichnet. Umgekehrt gibt es zu jeder Cliffordalgebra mit diesen Eigenschaften eine involutorische Geometrie.*

---

[6]) Zur Definition eines Cliffordalgebra für Körper der Charakteristik 2 vgl. z.B. [1].

Literatur

[1] C. Arf: Untersuchungen über quadratische Formen in Körpern der Charakteristik 2. J. reine angew. Math. 183, 148—167 (1941).

[2] R. Baer, The group of motions of a two dimensional elliptic geometry. Compositio math. 9, 244—288 (1951).

[3] R. Baer, Linear algebra and projective geometry. New York 1952.

[4] W. Blaschke, Euklidische Kinematik und nichteuklidische Geometrie. Zeitschrift für Math. u. Phys. 60, 61—91 u. 203—204 (1911).

[5] J. Grünwald. Ein Abbildungsprinzip, welches die ebene Geometrie und Kinematik mit der räumlichen Geometrie verknüpft. S.-B. Akad. Wien. math.-nat. Kl. IIa 80, 677—741 (1911).

[6] H. Karzel, Verallgemeinerte elliptische Geometrien und ihre Gruppenräume. Abh. Math. Sem. Univ. Hamburg 24, 167—188 (1960).

[7] B. L. van der Waerden, Moderne Algebra I. 3. Auflage, Berlin 1950.

Eingegangen am 1. 9. 1960