Jürgen Timm

Die Lösung eines Problems von Havel

Archivum Mathematicum, Vol. 5 (1969), No. 1, 25--28

Persistent URL: http://dml.cz/dmlcz/104678

DIE LÖSUNG EINES PROBLEMS VON HAVEL

Jürgen Timm, Hamburg

Eingegangen am 30. August 1968

In [3]*) benutzte Havel Veblen-Wedderburn-Systeme mit Rechtskürzregel zur Konstruktion affiner Ebenen. Dabei wurde die Frage aufgeworfen, ob es derartige Systeme gibt, die weder assoziativ noch distributiv sind. Diese Frage wird hier positiv beantwortet und zwar werden wir mit einer Verallgemeinerung des Verfahrens von Dickson [1] und Zassenhaus [5] ein solches System über den rationalen Cayley-Zahlen konstruieren.**)

Wir beginnen mit der

Definition: Eine doppelte binäre Struktur $\boldsymbol{S}(+,.)$ heißt *Veblen-Wedderburn-System mit Rechtskürzregel*, falls***)

V1: $\boldsymbol{S}(+)$ eine (abelsche) Gruppe, 0 das neutrale Element und $S^* = S\text{-}\{0\}$

V2: $\boldsymbol{S}^*(.)$ eine Loop, 1 das neutrale Element

V3: $\forall a, b, c \in \boldsymbol{S}$: $(a + b)\, c = ac + bc$

V4: $\forall a \in \boldsymbol{S}\ \forall b \in \boldsymbol{S}^*\ \exists\, b^{-1} \in \boldsymbol{S}^*$: $(ab)\, b^{-1} = a$ und $b^{-1}b = 1$ (Rechtskürzregel)

V5: $a, b, c \in \boldsymbol{S}$ mit $a \neq b$ gilt: $xa - xb = c$ ist eindeutig nach x auflösbar.

Im Folgenden sei stets $\boldsymbol{Q}(+,.)$ der Körper der rationalen Zahlen, $\boldsymbol{H}(+,.)$ der rationale Quaternionen-Schiefkörper und $\boldsymbol{S}(+,.)$ der Alternativkörper der rationalen Cayleyzahlen.*) Mit kleinen griechischen Buchstaben bezeichnen wir Elemente aus $\boldsymbol{Q}$, mit kleinen lateinischen solche aus $\boldsymbol{H}$ und mit großen lateinischen Buchstaben die Elemente von $\boldsymbol{S}$.

Bekanntlich kann man $\boldsymbol{S}$ als zweidimensionalen Vektorraum über $\boldsymbol{H}$ auffassen. Entsprechend denken wir uns zu jedem $A \in \boldsymbol{S}$ Komponenten $a_1, a_2 \in \boldsymbol{H}$ gegeben, so daß $A = \langle a_1, a_2 \rangle$. Die Multiplikation „." in $\boldsymbol{S}$

*) Die Zahlen in eckigen Klammern verweisen auf das Literaturverzeichnis am Ende der Arbeit.

**) Der Verfasser konnte in [4] zeigen, daß es nicht-assoziative und nicht-distributive $\mathfrak{S}$-Systeme gibt. Diese Systeme besitzen zwar auch die Rechtskürzregel, dagegen verlangt man bei ihnen das andere Distributivgesetz. In den in [4] angegebenen Beispielen ist stets die zweite Kürzregel verletzt, so daß man aus ihnen auch durch Dualisierung keine Beispiele für Strukturen der hier gesuchten Art erhält.

***) Vergl. etwa [2] § 20.3.

*) Man kann (nach isomorpher Einbettung und anschließender Identifizierung) annehmen, daß $\boldsymbol{Q} \subset \boldsymbol{H} \subset \boldsymbol{S}$.

wird dann durch $\langle a_1, a_2\rangle . \langle b_1, b_2\rangle = \langle a_1 b_1 - \bar{b}_2 a_2,\ b_2 a_1 + a_2 \bar{b}_1\rangle$ beschrieben. Bekanntlich kann man jedem $A \in \mathbf{S}$ die rationale Zahl $N(A) := a_1\bar{a}_1 + a_2\bar{a}_2$ zuordnen, die $N(A) = 0 \Leftrightarrow A = 0$ sowie $N(AB) = N(A)\,N(B)$ erfüllt. Für $A \neq 0$ läßt sich $N(A)$ eindeutig in der Form $N(A) = 2^{k(A)}\, b(A)$ darstellen, wo $k(A)$ eine ganze Zahl und $b(A)$ einen ausgekürzten Bruch bedeutet, in dessen Zähler und Nenner der Faktor 2 nicht auftritt. Man erhält dann den sehr einfachen Hilfssatz

L 1: $k(AB) = k(A) + k(B)$, $k(\alpha) \equiv 0 \bmod 2$, $k(A^{-1}) = -k(A)$.

Bewies: Während die erste Behauptung aus der Gleichung $N(AB) = N(A)\,N(B)$ folgt und zusammen mit $k(1) = 0$ die letzte Gleichung der Behauptung impliziert, folgt die mittlere Gleichung aus der Tatsache, daß (wegen $\alpha \in \mathbf{Q}$) $N(\alpha) = \alpha^2$ ist, also keine ungerade Primzahlpotenz enthalten kann.

Als Nächstes definieren wir die Abbildung Ψ: $\begin{cases} \mathbf{S} \longrightarrow \mathbf{S} \\ \langle a_1, a_2\rangle \to \langle a_1, -a_2\rangle \end{cases}$ und behaupten

L 2: Ψ ist ein Automorphismus von $\mathbf{S}$ $(+,.)$ und $k(\Psi(A)) = k(A)$.

Beweis: Ψ ist trivialerweise ein additiver Automorphismus und es gilt $\Psi(AB) = \langle a_1 b_1 - b_2 a_2,\ -b_2 a_1 \perp a_2 b_1\rangle = \Psi(A)\,\Psi(B)$. Schließlich ist $N(\langle a_1, a_2\rangle) = a_1 a_1 + a_2 a_2 = N(\langle a_1, -a_2\rangle)$ also auch $k(\Psi(A)) = k(A)$.

Wir führen nun eine neue binäre Operation „o" in $\mathbf{S}$ ein indem wir verlangen:

$$A \circ B := \begin{cases} 0, \text{ falls } B = 0 \\ \Psi(A)^{k(B)} . B \text{ sonst.} \end{cases}$$

Das Hauptresultat lautet nun

Satz: $\mathbf{S}(+,\circ)$ *ist ein nicht-assoziatives und nicht-distributives Veblen-Wedderburn-System mit Rechtskürzregel.*

Der Übersichtlichkeit halber beweisen wir den Satz in einer Folge von kleinen Hilfssätzen:

L 3: $\mathbf{S}^*(\circ)$ ist rechtseindeutig lösbar.

Beweis: Gegeben sei eine Gleichung $A \circ X = B$ mit $A, B \in \mathbf{S}^*$. Für jede Lösung X dieser Gleichung muß $k(\Psi^{k(X)}(A) . X) = k(A) + k(X) = k(B)$ oder $k(X) = k(A) - k(B)$ sein.

Fall 1: $k(A) - k(B)$ ist gerade. Dann ist $A \circ X = AX = B$ in $\mathbf{S}(+,.)$ eindeutig lösbar.

Fall 2: $k(A) - k(B)$ ist ungerade. Dann ist $A \circ X = \Psi(A)\,X = B$ wiederum in $\mathbf{S}^*(.)$ eindeutig lösbar.

L 4: $\mathbf{Q}$ liegt im Zentrum von $\mathbf{S}(\circ)$.

Beweis: Jeder Automorphismus von $S(+,.)$ läßt Q elementweise fest. Also ist $\alpha \circ B = \alpha \,.\, B$. Weiter ist $\Psi^{k(\alpha)} = \mathrm{id.}$, denn Ψ ist involutorisch und $k(\alpha) \equiv 0 \bmod 2$ (siehe **L 1**). Deshalb ist $B \circ \alpha = B \,.\, \alpha$. Schließlich liegt Q im Zentrum von $S(.)$ Also ist auch $B \circ \alpha = \alpha \circ B$.

L 5: In $S(+,\circ)$ gilt das Distributivgesetz $(A + B) \circ C = A \circ C + B \circ C$.

Beweis folgt unmittelbar aus der Tatsache, daß Ψ ein Automorphismus von $S(+,.)$ ist (**L 2**).

L 6: $\forall A,\ B \in S$ mit $A \neq B$ ist die durch $\Phi(X) := X \circ A - X \circ B$ definierte Funktion eine Q-lineare Abbildung des Q-Vektorraums S in sich.

Beweis: $\Phi(X + Y) = (X + Y) \circ A - (X + Y) \circ B = X \circ A - X \circ B + Y \circ A - Y \circ B = \Phi(X) + \Phi(Y)$ (s. **L 5**).

$$\Phi(X\alpha) = \begin{cases} -\Psi^{k(B)}(X\alpha)\, B = -\Psi^{k(B)}(X)\, \alpha B = -\Psi^{k(B)}(X) B\alpha = \\ = \Phi(X)\, \alpha \quad \text{für } A = 0 \\ \Psi^{k(A)}(X\alpha)\, A = \Psi^{k(A)}(X)\, A\alpha = \Phi(X)\, \alpha \quad \text{für } B = 0 \\ \Psi^{k(A)}(X)\, A\alpha - \Psi^{k(B)}(X)\, B\alpha = \Phi(X)\, \alpha \quad \text{sonst.} \end{cases}$$

L 7: Die in **L 6** definierte Abbildung Φ ist sogar ein Vektorraumautomorphismus von S über Q.

Beweis: Wir betrachten den Kern der Abbildung:
$\mathrm{Ker}\,\Phi = \{X \in S \mid \Phi(X) = 0\} = \{X \in S \mid X \circ A = X \circ B\}$. Nehmen wir an, daß $A,\ B \in S^*$ sind und daß es eine Lösung $X \neq 0$ der Gleichung $X \circ A = X \circ B$ gäbe, so müßte im Widerspruch zur Voraussetzung $A = B$ sein (**L 3**). Für $A,\ B \in S^*$ wird die Gleichung deshalb genau von $X = 0$ gelöst. Ist etwa $A = 0$ und $B \neq 0$, so wird die Gleichung $X \circ B = \Psi^{k(B)}(X)\, B = 0$ genau von $\Psi^{k(B)}(X) = 0$ gelöst (Nullteilerfreiheit von $S(+,.)$). Also ist in jedem Falle $\mathrm{Ker}\,\Phi = \{0\}$. S hat die endliche Dimension 8 über Q, also muß nach der Dimensionsformel der Vektorraum $\Phi(S)$ mit S übereinstimmen.

L 8: Für alle $A, B, C \in S$ mit $A \neq B$ ist die Gleichung $X \circ A - X \circ B = C$ eindeutig nach X auflösbar.

Beweis: folgt aus **L 7**, denn zu $C \in S$ existiert genau ein Urbild X mit $\Phi(X) = C$.

L 9: Für $B \in S^*$ erfüllt $\overset{\circ}{B}{}^{-1} := \Psi^{-k(B)}(B^{-1})$ für alle $A \in S$: $(A \circ B) \circ \overset{\circ}{B}{}^{-1} = A$ und $\overset{\circ}{B}{}^{-1} \circ B = 1$.

Beweis: Nach **L 1** und **L 2** ist $k(\overset{\circ}{B}{}^{-1}) = k(\Psi^{-k(B)}(B^{-1})) = k(B^{-1}) = -k(B)$. Also ist $(A \circ B) \circ B^{-1} = \Psi^{-k(B)}(\Psi^{k(B)}(A) \,.\, B)\, \Psi^{-k(B)}(B^{-1}) = A\Psi^{-k(B)}(B)\, \Psi^{-k(B)}(B^{-1}) = A$ und $\overset{\circ}{B}{}^{-1} \circ B = \Psi^{k(B)}(\Psi^{-k(B)}(B^{-1}))\, B = B^{-1} \,.\, B = 1$.

Beweis des Satzes: Da wir die Addition nicht abgeändert haben ist nach wie vor $S(+)$ eine abelsche Gruppe. Nach **L 5** gilt das eine Distributivgesetz, während $S^*(o)$ nach **L 3** und **L 8** eine Loop ist. **L 9** besagt die Gültigkeit der einen Kürzregel und **L 8** die distributive Auflösbarkeit. $S(+,o)$ ist also ein Veblen-Wedderburn-System mit Rechtskürzregel. Wir haben nur noch zu zeigen, daß $S(+,o)$ weder assoziativ noch distributiv ist. Dafür bezeichnen wir die Basiselemente von H wie üblich mit $1, i, j, k$. Es ist $N(\langle -i, 0\rangle) = 1$ und $N(\langle 1+i, 0\rangle) = 2$, daraus folgt $\langle 0, 1\rangle \circ (\langle 1+i, 0\rangle + \langle -i, 0\rangle) = \langle 0, 1\rangle$ aber $\langle 0, 1\rangle \circ \langle 1+i, 0\rangle + \langle 0, 1\rangle \circ \langle -i, 0\rangle = \langle 0, -1\rangle \cdot \langle 1+i, 0\rangle + \langle 0, 1\rangle \cdot \langle -i, 0\rangle = \langle 0, -1+2i\rangle$. $S(+,o)$ ist also nicht distributiv. Das Assoziativgesetz ist schon in $S(+,.)$ verletzt. Wir müssen nur zeigen, daß es durch den Übergang zu $S(+,o)$ nicht wieder hergestellt wird. Ein Gegenbeispiel liefert $(\langle i, 0\rangle \circ \langle j, 0\rangle) \circ \langle 0, 1\rangle = \langle 0, k\rangle \neq \langle 0, -k\rangle = \langle i, 0\rangle \circ (\langle j, 0\rangle \circ \langle 0, 1\rangle)$. Damit ist der Satz vollständig bewiesen.

LITERATURVERZEICHNIS

[1] E. Dickson, *On finite algebras* Nachr. Kgl. Ges. Wiss. Göttingen Math. Phys. Klasse (1905) 358—393.

[2] M. Hall, *The theory of groups* N. York 1959.

[3] V. Havel, *One characterization of special translation planes* Arch. math. Brno **3** (1967) 157—160.

[4] J. Timm, *Eine Klasse schwacher binärer Doppelstrukturen*, Abh. Math. Sem. d. Univ. Hamburg **33** (1969) 102—118.

[5] H. Zassenhaus, *Über endliche Fastkörper*, Abh. Math. Sem. d. Univ. Hamburg **11** (1936) 187—220.

Mathematisches Seminar
der Universität Hamburg
2 Hamburg 13
Rothenbaumchaussee 67