Prom. Nr. 2377

Über die endlichen klein-desarguesschen Zahlsysteme

VON DER

EIDGENÖSSISCHEN TECHNISCHEN HOCHSCHULE
IN ZÜRICH

ZUR ERLANGUNG DER WÜRDE EINES

DOKTORS DER MATHEMATIK

GENEHMIGTE

PROMOTIONSARBEIT

VORGELEGT VON

Walter Strickler

von Zürich und Richterswil

Referent: Herr Prof. Dr. P. Bernays
Korreferent: Herr Prof. Dr. H. Hopf

Zürich 1955
Dissertationsdruckerei Leemann AG

Leer - Vide - Empty

MEINEN ELTERN

Leer - Vide - Empty

Einleitung

In seiner Abhandlung „Über endliche Geometrien" (Annales Academiae Scientiarum Fennicae, Series A, I. Mathematica-Physica, 72) hat sich *R. Stettler* (u. a.) mit solchen Geometrien auseinandergesetzt, bei denen außer den Hilbertschen Inzidenzaxiomen noch eine schwächere Fassung des Desarguesschen Satzes gefordert wird; und zwar handelt es sich um denjenigen Spezialfall dieses Satzes, bei dem nicht nur die zwei entsprechenden Dreieckseiten, sondern auch die Verbindungsgeraden entsprechender Ecken der Dreiecke einander parallel sind. Eine solche Geometrie wird eine „klein-desarguessche" genannt. Auf diese Geometrien wandte *R. Stettler* die Hilbertsche Methode der Einführung einer Streckenrechnung an (s. *Hilbert*, Grundlagen der Geometrie). Bei Zugrundelegung des Desarguesschen Satzes bilden die Strecken einen Schiefkörper (s. *Hilbert*, Grundlagen der Geometrie). Bei der erwähnten schwächeren Fassung trifft dies nicht mehr zu: Bezüglich der Addition bilden die Strecken ebenfalls eine abelsche Gruppe; dagegen läßt sich das assoziative Gesetz der Multiplikation und das eine der beiden distributiven Gesetze nicht beweisen. Nachweisen hingegen lassen sich die zu Beginn des § 1 dieser Abhandlung aufgeführten Eigenschaften I. bis III.

Ein Beispiel einer solchen nicht-desarguesschen Geometrie wurde bereits 1907 von *O. Veblen* und *J. H. Maclagan-Wedderburn* publiziert („Non-Desarguesian and non Pascalian Geometries", Transactions of the Amer. math. Soc., vol. 8, pp. 379—388). Dieses Modell besteht nur aus endlich vielen Elementen.

Bei vorliegender Arbeit handelt es sich darum, obigen Streckenkalkül, wobei wir die Menge der Strecken als endlich voraussetzen wollen, algebraisch zu untersuchen. Die Gesamtheit der erwähnten

Eigenschaften wird hierbei als Axiomensystem aufgefaßt. Da auf die ursprüngliche geometrische Bedeutung der Systeme kein Bezug genommen wird, wollen wir allgemeiner statt von „Strecken" von „Elementen" sprechen, und ein solches System werde „endliches klein-desarguessches Zahlsystem" oder zur Abkürzung gewöhnlich „System Z" genannt und ein beliebiger Vertreter im allgemeinen mit „Z" bezeichnet.

Die vorliegende Arbeit stützt sich im übrigen auf keine Resultate der Stettlerschen, hingegen wurden in dieser (in § 5) einige Sätze der ersteren bereits bewiesen.

§ 1. Das Axiomensystem

Die endlichen klein-desarguesschen Zahlsysteme, deren Untersuchung der Zweck vorliegender Abhandlung sein soll, weisen folgende Eigenschaften auf:

Sie besitzen zwei Kompositionen, eine Addition und eine Multiplikation, die beide immer eindeutig ausführbar sind. Zudem sind folgende Bedingungen erfüllt:

I. Bezüglich der Addition bilden die Elemente eine abelsche Gruppe.

II. 1. Für alle a gilt
$$a\,0 = 0\,a = 0$$

2. Es existiert ein Einselement $\varepsilon \neq 0$, so daß für alle a
$$\varepsilon\, a = a\, \varepsilon = a$$

3. Zu jedem $a \neq 0$ und b gibt es ein und nur ein x_1 bzw. y_1 derart, daß
$$a\, x_1 = b \quad \text{und} \quad y_1\, a = b$$

III. Es gilt das Linksdistributivgesetz
$$a\,(b+c) = a\,b + a\,c$$

IV. Es gibt nur endlich viele Elemente.

In diesem Paragraphen soll obiges Axiomensystem nach der Unabhängigkeit der Axiome untereinander untersucht werden.

(Daß dieses widerspruchfrei ist, erhellt unmittelbar aus der Tatsache, daß seine Eigenschaften auch den Galoisfeldern zukommen.)

Wir werden nun zeigen, daß unser Axiomensystem sich reduzieren läßt. Von der Reduktion werden die Axiome der Gruppe II. betroffen, und zwar kann Axiom II. 1. eliminiert werden, während die beiden übrigen durch je eine schwächere Fassung ersetzt werden können. Zum Nachweis der Möglichkeit der Abschwächung von Axiom II. 3. werden die beiden übrigen Axiome dieser Gruppe nicht herangezogen. Das gleiche gilt für den Beweis der Abschwächung von Axiom II. 2. Hieraus folgert man, daß die drei Reduktionen gleichzeitig vorgenommen werden dürfen.

Satz 1. Axiom II. 3. läßt sich durch die folgende schwächere Fassung ersetzen: Aus $ab=ab'$ bzw. $ca=c'a$ folgt für $a\neq 0$ $b=b'$ bzw. $c=c'$. (M. a. W.: Wenn die Division ausführbar ist, dann ist sie es eindeutig.)

Beweis. Wir müssen zeigen, daß aus dieser schwächeren Fassung Axiom II. 3. folgt: Zum Nachweis der Lösbarkeit von $ax=b$ für $a\neq 0$ ziehen wir die Funktion $y=ax$ heran. Wenn x Z durchläuft, so durchläuft y wegen unserer Voraussetzung ebenfalls diesen Bereich, nimmt also insbesondere den Wert b an. Analog wird die Lösbarkeit von $ya=b$ bewiesen.

Satz 2. In Axiom II. 2. braucht nur die Existenz eines vorderen und hinteren Einselementes gefordert zu werden; die Gleichheit der beiden läßt sich beweisen.

Beweis. Es sei ε das vordere, ε' das hintere Einselement. Dann ist

$$\begin{aligned} & \varepsilon x = x \quad \text{für bel. } x\in Z, \\ \text{insbesondere} \quad & \varepsilon\varepsilon' = \varepsilon'. \\ \text{Ferner ist} \quad & x\varepsilon' = x, \\ \text{insbesondere} \quad & \varepsilon\varepsilon' = \varepsilon, \\ \text{woraus} \quad & \varepsilon' = \varepsilon \quad \text{folgt.} \end{aligned}$$

Zum Beweis von Satz 3 benötigen wir folgenden

Hilfssatz: In Z gibt es keine Nullteiler; und diese Tatsache ist von Axiom II. 1. unabhängig.

Beweis. Wäre $a\,b = 0$ für $a, b \neq 0$,

so würde aus $a\,(b+c) = d$

und $a\,(b+c) = a\,b + a\,c = a\,c = d$

ein Widerspruch mit Axiom II. 3. (nebst I.) entstehen.

Satz 3. Axiom II. 1. läßt sich aus den übrigen Axiomen beweisen.

Beweis. Wenn die Lösung von $a\,x = 0$ oder von $y\,a = 0 \neq 0$ wäre für gewisse $a \neq 0$, so hätten wir Nullteiler, im Widerspruch zum Hilfssatz.

Es bleibt noch $0 \cdot 0 = 0$ zu beweisen: Wenn $a \neq 0$, so erhält man unter Anwendung des bereits Bewiesenen unseres Satzes und des distributiven Gesetzes

$$0 \cdot 0 = 0\,(a - a) = 0\,a + 0\,(-a) = 0$$

Wir können nun unseren Zahlsystemen folgendes Axiomensystem zugrunde legen:

A. Bezüglich der Addition bilden die Elemente eine abelsche Gruppe.

M. 1. Aus $a\,b = a\,b'$ bzw. $c\,a = c'\,a$ folgt für $a \neq 0$ $b = b'$ bzw. $c = c'$.

2. Es gibt ein vorderes und ein hinteres Einselement „ε“ und „ε'“ der Multiplikation, wobei eines $\neq 0$, so daß für alle a $\varepsilon\,a = a$ bzw. $a\,\varepsilon' = a$.

D. Es gilt das linksdistributive Gesetz

$$a\,(b+c) = a\,b + a\,c$$

E. Es gibt nur endlich viele Elemente.

Aus diesen Axiomen kann man nun also die Axiome II. 3. und II. 2. von Seite 6 beweisen und hierauf mit Benützung des ersteren Axiom II. 1.

Wir wollen nun von einigen der Axiome zeigen, daß sie von den andern unabhängig sind, sich also aus ihnen nicht beweisen lassen. Wir verfahren hiezu wie üblich, indem wir Modelle konstruieren, bei denen sämtliche Axiome erfüllt sind, mit Ausnahme desjenigen, dessen Unabhängigkeit bewiesen werden soll. Wir wollen uns hierbei auf die Axiome M. 1, 2. und E. beschränken.

Die Unabhängigkeit von Axiom E. von den übrigen erhellt ohne weiteres aus der Tatsache, daß bei unendlichen Körpern Axiom E. nicht erfüllt ist, hingegen sämtliche übrigen.

Nun wollen wir die Unabhängigkeit von Axiom M. 2. nachweisen. Zu diesem Zwecke konstruieren wir ein Modell von vier Elementen $0, e, r, e+r$, für die das Axiom M. 2. nicht gültig ist, hingegen alle übrigen. (Die Multiplikation ist bei diesem Modell kommutativ, woraus das andere Distributivgesetz gefolgert werden kann.)

Additionstabelle

$+$	e	r	$e+r$
e	0	$e+r$	r
r	$e+r$	0	e
$e+r$	r	e	0

Multiplikationstabelle

$\cdot$	e	r	$e+r$
e	e	$e+r$	r
r	$e+r$	r	e
$e+r$	r	e	$e+r$

Daß das Axiom M. 1. von den übrigen Axiomen unabhängig ist, folgt daraus, daß der Restklassenring modulo n für jedes zerlegbare n ein Modell für A., M. 2., D. und E. mit Ungültigkeit von M. 1. liefert.

Zum Schluß dieses Paragraphen sollen noch zwei Sätze bewiesen werden, die später Verwendung finden werden.

Satz 4. Für zwei beliebige Elemente a, b gilt stets

$$-(a\,b) = a\,(-b)$$

Beweis. Aus $$a\,b + a\,(-b) = a\,(b-b) = 0$$

folgt $$-(a\,b) = a\,(-b)$$

Satz 5. Die Gleichung

$$a\,x - b\,x = c \tag{1}$$

ist dann und nur dann eindeutig lösbar, wenn $a \neq b$.

Beweis. Zum Beweis, daß die Bedingung hinreichend ist, zeigen wir, daß die Funktion

$$y = a\,x - b\,x \tag{2}$$

den Wert c für genau ein x_0 annimmt. Diese nimmt jeden Wert nur einmal an. Wäre nämlich für $x_1 \neq x_2$

$$y_1 = a\,x_1 - b\,x_1$$
$$y_1 = a\,x_2 - b\,x_2$$

so würde durch Subtraktion der beiden Gleichungen und durch eine einfache Umformung

$$a\,(x_1 - x_2) = b\,(x_1 - x_2)$$

folgen. Nach Axiom M. 1. würde dies $a = b$ bedeuten, was der Voraussetzung widersprechen würde. Wenn x in (2) Z durchläuft, wird nach dem vorigen jeder Wert von Z angenommen, insbesondere also auch c.

Daß die Bedingung notwendig ist, ist noch leichter einzusehen: Für $a = b$ nimmt die Funktion (2) nur den Wert null an, weshalb (1) für $c \neq 0$ unlösbar und für $c = 0$, da Z aus mindestens zwei Elementen besteht, mehrdeutig lösbar ist.

§ 2. Die Untersysteme A, Δ und Π

Unter einem Untersystem von Z wollen wir auch hier, wie es ja bei den bekannten algebraischen Bereichen in analoger Weise der Fall ist, eine (echte oder unechte) Teilmenge von Z verstehen, die ebenfalls ein System Z ist. Unter diesen Untersystemen gibt es drei, welche beachtenswerte Eigenschaften aufweisen und deshalb in diesem Paragraphen behandelt werden sollen.

Zunächst soll ein allgemeiner Satz über Untersysteme von Z bewiesen werden:

Satz 1. Wenn bei einer Teilmenge U von Z die Addition und die Multiplikation ihrer Elemente nicht aus diesem Bereich herausführen, so handelt es sich um ein Untersystem von Z.

Beweis. In dieser Menge ist mit jedem ihrer Elemente auch die zugehörige additive zyklische Gruppe enthalten und deshalb auch die Null und jedes Additionsinverse eines Elementes. Die Elemente erfüllen somit Axiom A. Es muß nun nur noch gezeigt werden — die übrigen Axiome sind trivialerweise auch erfüllt —, daß auch das Einselement in U liegt: Aus Axiom M. 1. kann, analog dem Beweis von Satz 1 von § 1, ohne Benützung von ε gefolgert werden, daß in U für $a \neq 0$ jede Gleichung $a\,x = b$ lösbar ist, insbesondere also $a\,x = a$.

a) Das Untersystem A

Wir betrachten die Gesamtheit A der Elemente a mit der assoziativen Eigenschaft

$$(x\,y)\,a = x\,(y\,a),$$

wobei $a \in A$ und x, y beliebige Elemente von Z bedeuten.

Zunächst leuchtet unmittelbar ein, daß für die Elemente der Menge A das assoziative Gesetz der Multiplikation gilt.

Satz 2. Die Menge A bildet ein (assoziatives) Untersystem von Z. (Wenn A keine echte Untermenge von Z ist, so ist Z assoziativ bezüglich der Multiplikation.)

Beweis. Nach Satz 1 genügt es zu zeigen, daß mit a_1 und a_2 immer auch $a_1 + a_2$ und $a_1 a_2$ zu A gehören.

Das erstere beweist man wie folgt:

$$(x\,y)\,(a_1 + a_2) = (x\,y)\,a_1 + (x\,y)\,a_2 =$$
$$x\,(y\,a_1) + x\,(y\,a_2) = x\,(y\,a_1 + y\,a_2) = x\,(y\,(a_1 + a_2))$$

Somit ist $$(x\,y)\,(a_1 + a_2) = x\,(y\,(a_1 + a_2))$$

Nun wird gezeigt, daß mit a_1 und a_2 auch $a_1 a_2$ zu A gehört:

$$(x\,y)\,(a_1\,a_2) = ((x\,y)\,a_1)\,a_2) = (x\,(y\,a_1))\,a_2$$
$$= x\,((y\,a_1)\,a_2) = x\,(y\,(a_1\,a_2))$$

Somit ist $$(x\,y)\,(a_1\,a_2) = x\,(y\,(a_1\,a_2))$$

Folgerung. Die beiden Gleichungen

$$\begin{aligned} a_1\,x &= a_2 \\ y\,a_1 &= a_2 \end{aligned} \qquad (a_i \in A)$$

sind für $a_1 \neq 0$ in A eindeutig lösbar.

Hieraus und aus der Assoziativität der Multiplikation in A folgt

Satz 3. Die von null verschiedenen Elemente von A bilden eine multiplikative Gruppe.

Folgerung. In A ist das Rechtsinverse der Multiplikation zugleich Linksinverses.

Satz 4. Die Menge A ist nie leer; denn 0 und ε liegen immer darin.

Zerlegung von Z nach A. Z läßt sich nach Restklassen eines Untersystems zerlegen, analog wie sich ein Ring nach Restklassen eines Unterringes, etwa eines Ideals, zerlegen läßt. Nach A gibt es aber noch eine weitere Zerlegung der Form

$$Z^* = u_1 A^* + \cdots + u_m A^*$$

(Z^*, A^* = Menge Z bzw. A ohne Nullelement).

Zum *Beweis* nehmen wir zuerst irgend ein Element u_1 von Z^* und bilden $u_1 A^*$. Dann greifen wir ein Element u_2 heraus, das nicht in $u_1 A^*$ liegen soll und bilden die Menge $u_2 A^*$. Auf diese Weise fahren wir fort, bis jedes Element von Z in mindestens einer der Mengen $u_i A^*$ sich befindet. — Nun muß noch gezeigt werden, daß der Durchschnitt der $u_i A^*$ gleich null ist: Wenn etwa der Durchschnitt $u_1 A^* \cap u_2 A^*$ von null verschieden wäre und somit eine Beziehung $u_1 a_1 = u_2 a_2$ $(a_i \in A^*)$ bestehen würde, so würde hieraus

$$u_2 = u_1 a_1 a_2^{-1}$$

folgen, weshalb u_2 zur Klasse $u_1 A^*$ gehören würde.

b) Das Untersystem Δ

Das zweite Untersystem, dem wir uns nun zuwenden wollen, ist ein Körper, weshalb wir es Körper Δ nennen wollen und seine Elemente (mit Ausnahme der Null) mit griechischen Buchstaben bezeichnen werden.

Wir betrachten vorerst die Gesamtheit $\mathfrak{D}$ der Elemente von Z, für die das zweite distributive Gesetz in der folgenden Form gilt:

$$(x+y)\,d = x\,d + y\,d,$$

wobei x und y beliebige Elemente aus Z und d ein Element aus $\mathfrak{D}$ bedeuten sollen.

Satz 5. Die Menge $\mathfrak{D}$ bildet eine Untergruppe der additiven Gruppe von Z.

Beweis. Auf Grund einer Überlegung, wie sie beim Beweise von Satz 1 angestellt wurde, genügt es zu zeigen, daß die Summe je zweier Elemente nicht aus dem Bereich herausführt.

$$\begin{aligned}(x+y)\,d_1 &= x\,d_1 + y\,d_1 \\ (x+y)\,d_2 &= x\,d_2 + y\,d_2\end{aligned} \qquad (d_i \in \mathfrak{D})$$

Addition der beiden Gleichungen liefert

$$(x+y)\,d_1+(x+y)\,d_2 = x\,d_1+y\,d_1+x\,d_2+y\,d_2,$$

und durch Ausklammern auf beiden Seiten ergibt sich

$$(x+y)\,(d_1+d_2) = x\,(d_1+d_2)+y\,(d_1+d_2)$$

Satz 6. Der Durchschnitt Δ von A und $\mathfrak{D}$ ist ein Körper (und somit ein Untersystem von A).

Beweis. Die Elemente von Δ bilden, wie leicht einzusehen, eine Untergruppe der additiven Gruppe von Z. Es gilt zudem ($\delta_i \in \Delta$)

$$\begin{aligned}(x+y)\,(\delta_1\,\delta_2) &= ((x+y)\,\delta_1)\,\delta_2 = (x\,\delta_1+y\,\delta_1)\,\delta_2\\ &= (x\,\delta_1)\,\delta_2+(y\,\delta_1)\,\delta_2 = x\,(\delta_1\,\delta_2)+y\,(\delta_1\,\delta_2),\end{aligned}$$

womit gezeigt ist, daß unter der Bedingung $\delta_1, \delta_2 \in \Delta$ $\delta_1\,\delta_2$ nicht nur zu A, sondern auch zu $\mathfrak{D}$ und somit auch zu Δ gehört. Wir haben somit bewiesen, daß Δ ein Ring (ohne Nullteiler) ist. Ein endlicher, nullteilerfreier Ring ist aber bekanntlich ein Galoisfeld.

Satz 7. Die Menge Δ enthält immer Elemente, da 0 und ε dazu gehören.

Anwendung. Das Gleichungssystem

$$\begin{aligned}x\,\delta_1+y\,b_1 &= c_1\\ x\,\delta_2+y\,b_2 &= c_2\end{aligned}$$

ist für $\delta_i \in \Delta \neq 0$, b_i, $c_i \in Z$ und $b_1\,\delta_1^{-1}-b_2\,\delta_2^{-1} \neq 0$ eindeutig lösbar. Man kann es auflösen, indem man die erste der Gleichungen von rechts her mit δ_1^{-1} und die zweite von rechts her mit δ_2^{-1} multipliziert. Durch Subtraktion der beiden Gleichungen voneinander ergibt sich eine Gleichung für y, die sich leicht auflösen läßt.

Die Bedeutung des Körpers Δ wird im nächsten Paragraphen klar werden.

c) Das Untersystem Π

Unter dem Primkörper eines Körpers versteht man den eindeutig bestimmten Durchschnitt aller Unterkörper (welcher geläufigermaßen auch ein Körper ist und keine echten Unterkörper enthält). Auf gleiche Weise wie bei Körpern kann auch bei den

Systemen Z die Existenz eines „Primsystems" nachgewiesen werden, was auf der Tatsache beruht, daß auch hier der Durchschnitt irgend welcher Untersysteme wiederum ein solches ist. Über die Struktur dieses Untersystems gibt der nachstehende Satz Auskunft:

Satz 8. Das Primsystem von Z ist mit dem Primkörper Π' von Δ identisch (weshalb wir auch beim System Z von einem Prim*körper* sprechen wollen).

Der *Beweis* dieses Satzes erhellt aus der Tatsache, daß der Durchschnitt *aller* Untersysteme von Z zunächst die Elemente 0 und ε, und somit alle Elemente von Π' enthalten muß.

Die Ordnung von Π wollen wir die *Charakteristik* von Z nennen und mit p bezeichnen. Mittelst $b = b\,\varepsilon$, $b\,0 = 0$ und dem distributiven Gesetz erkennt man

Satz 9. Die Ordnung (der additiven zyklischen Gruppe) jedes Elementes von Z, mit Ausnahme der Null, ist gleich p.

Ferner folgt aus $b\,n = b\,m$ ($b \neq 0$, n, m natürliche Zahlen) stets $n \equiv m \pmod{p}$ und umgekehrt.

Es sei noch festgestellt, daß Π als Unterkörper von Δ natürlich auch dessen Eigenschaften in Hinsicht auf Z aufweist, d. h. also die Eigenschaften von A und der Gruppe $\mathfrak{D}$. Über die Struktur der Primkörper sei auf die Literatur über Körper verwiesen.

Bemerkung. Die Existenz eines Primkörpers in Z kann auch direkt nachgewiesen werden; und zwar läßt sich die Methode nachbilden, die in der Körpertheorie zur Bestimmung der Struktur des Primkörpers angewendet wird (siehe etwa *van der Waerden*, Moderne Algebra I).

§ 3. Basisdarstellung, Ordnung von Z

In diesem Paragraphen soll gezeigt werden, daß sich die Elemente von Z durch eine Basis darstellen lassen. Zu diesem Zwecke wollen wir den Begriff der linearen Abhängigkeit der Elemente von Z in bezug auf den Körper Δ einführen, wie er von der linearen Algebra her bekannt ist: m Elemente u_i sollen linear unabhängig

in bezug auf Δ genannt werden, wenn eine Summe der Form $\sum_1^m u_i \delta_i$, wobei die δ_i immer rechts stehen sollen, nur gleich null sein kann, wenn sämtliche δ_i verschwinden; im andern Falle sollen sie linear abhängig heißen. (In Z ist außer dem Nullelement jedes einzelne Element linear unabhängig, da wir keine Nullteiler haben.) Da Z von endlicher Ordnung ist, gibt es eine Maximalzahl von linear unabhängigen Elementen. Aus diesem Grunde gibt es in Z eine Basisdarstellung über dem Körper Δ. Nämlich, es sei $u_i\,(i=1,\ldots,m)$ ein maximales System von linear unabhängigen Elementen. Wenn nun u_0 ein beliebiges Element von Z ist, so sind die $(u_0, u_1, \ldots, u_m)$ linear abhängig, d. h. es besteht eine Beziehung $u_0\delta_0 + \sum_{i=1}^m u_i \delta_i = 0$ derart, daß nicht alle δ verschwinden. Insbesondere ist dann δ_0 von null verschieden, da sonst wegen der linearen Unabhängigkeit der u_i auch die $\delta_i\,(i \neq 0)$ gleich null wären. Wir können somit obige Gleichung nach u_0 auflösen:

$$u_0\delta_0 = -\sum_1^m u_i\delta_i = \sum_1^m u_i(-\delta_i)$$

$$u_0 = (\sum_1^m u_i(-\delta_i))\delta_0^{-1} = \sum_1^m (u_i(-\delta_i))\delta_0^{-1} = \sum_1^m u_i((-\delta_i)\delta_0^{-1})$$

Aus $$u_0 = \sum_1^m u_i\delta_i' = \sum_1^m u_i\delta_i''$$

folgt $$\sum_1^m u_i(\delta_i' - \delta_i'') = 0,$$

und daraus wegen der linearen Unabhängigkeit der u_i, daß $\delta_i' = \delta_i''$, womit die Eindeutigkeit der Darstellung bewiesen ist. Wir haben somit den

Satz 1. Z besitzt eine Basisdarstellung über Δ.

Korollar. Z besitzt eine Basisdarstellung über jedem Unterkörper von Δ, insbesondere über Π.

Ferner gilt

Satz 2. Z ist ein Vektorraum über Δ, wenn die Elemente von Δ rechts geschrieben werden.

Zum *Beweis* brauchen wir nur zu verifizieren, daß die fünf Vektorraumaxiome erfüllt sind (s. etwa *van der Waerden*, Moderne Algebra I):

1. Das Produkt $u\delta$ eines Elementes u von Z mit einem Element δ von Δ gehört stets zu Z.
2. $(u+v)\delta = u\delta + v\delta$
3. $u(\delta_1+\delta_2) = u\delta_1 + u\delta_2$
4. $u(\delta_1\delta_2) = (u\delta_1)\delta_2$
5. Alle Elemente von Z sind eindeutig darstellbar als Linearformen $\sum_1^m u_i\delta_i$ mit Hilfe von m festen Basiselementen $u_1, \ldots, u_m$.

Auf Grund der Vektorraumeigenschaft läßt sich die Basis wie folgt transformieren:

$$u_j' = \sum_{i=1}^{m} u_i \delta_{ij} \qquad (j = 1, \ldots, m)$$

wobei die Determinante $|\delta_{ij}|$ von null verschieden sein muß.

Ferner bilden die Transformationen, die eine Basis in eine andere überführen, eine Gruppe, und zwar ist es die allgemeine lineare Gruppe $GL(m, \Delta)$, deren Ordnung

$$(q^m-1)(q^m-q)\ldots(q^m-q^{m-1})$$

beträgt, wobei q die Ordnung von Δ und m der Rang von Z über Δ bedeutet (s. etwa *van der Waerden*, Gruppen von linearen Transformationen).

Es sei noch bemerkt, daß mit $(u_1, \ldots, u_m)$ auch $(b\,u_1, \ldots, b\,u_m)$, wobei b ein von null verschiedenes, sonst aber willkürliches Element aus Z bedeutet, eine Basis ist, da die $b\,u_i$ wegen

$$\sum_1^m b\,u_i\delta_i = b\sum_1^m u_i\delta_i$$

linear unabhängig sind.

Wegen der vorherigen Bemerkung läßt sich leicht zeigen, daß (genau) ein Basiselement in Δ liegen kann. Hieraus folgt die Tatsache, daß ein System Z mit zweigliedriger Basis als einfache Erweiterung von Δ aufgefaßt werden kann, d. h. durch Adjunktion eines einzigen Elementes zu Δ erzeugt wird.

Es folgt nun etwas über die *Ordnung* von Z und seiner Untersysteme. Nach dem Korollar von Satz 1 folgt durch eine elementare kombinatorische Überlegung

Satz 3. Die Ordnung von Z ist eine Potenz der Charakteristik, wobei der Exponent gleich der Maximalzahl linear unabhängiger Elemente von Z über Π ist. (Diese Maximalzahl werde auch hier als Rang von Z über Π bezeichnet.)

Da die Untersysteme von Z denselben Primkörper haben, so ist deren Ordnung auch eine Potenz von p. Für das Untersystem A gilt zudem noch folgendes:

Satz 4. Wenn p^n die Ordnung von Z und p^l diejenige von A bedeutet, so muß l Teiler von n sein.

Beweis. Wir betrachten die Zerlegung von Z, wie sie auf Seite 12 ausgeführt wurde. Da das Nullelement dort weggelassen wird, gilt zwischen der Ordnung von Z und derjenigen von A die Beziehung

$$p^n - 1 = m'(p^l - 1)$$

(m' = Anzahl der Klassen). $p^n - 1$ muß also durch $p^l - 1$ ohne Rest teilbar sein, und dies ist nur möglich, wenn $n\,l$ als Faktor enthält. (Beweis: $n = q\,l + r$, $0 \leqq r < l$, $p^n - 1 = p^r(p^{ql} - 1) + p^r - 1$, $p^l - 1 \mid p^{ql} - 1$; also $p^l - 1 \mid p^r - 1$; somit $r = 0$.)

Folgerung. Bei allen nicht-assoziativen Systemen Z mit Primzahlrang über Π fällt A mit Π, und da $\Pi \subset \Delta \subset A$, auch mit Δ zusammen.

Man sieht leicht ein, daß sich A nach Δ analog wie Z nach A zerlegen läßt und daß deshalb zwischen den Ordnungen von A und Δ die analoge Beziehung bestehen muß:

Satz 5. Der Rang von Δ über Π ist ein Teiler des Ranges von A über Π und somit auch desjenigen von Z über Π.

Ein System Z mit verschiedenen A, Δ und Π hat somit eine Ordnung von mindestens $2^{2.2.2} = 256$.

Zum Schluß dieses Paragraphen soll noch eine hinreichende Bedingung für ein Untersystem von Z angegeben werden, damit Z über ihm eine Basisdarstellung besitzt:

Satz 6. Z besitzt eine Basisdarstellung über dem Untersystem Z', bei rechtsseitiger Stellung der Koeffizienten, wenn die Ordnung von Z' $p^{n/m''}$ beträgt und m'' linear unabhängige Elemente über Z' existieren (p = Charakteristik von Z, n = Rang von Z über Π).

Beweis. Es seien $u_i\,(i=1,\ldots,m'')$ linear unabhängige Elemente über Z'. Durch $c=\sum_i u_i b_i\,(b_i \in Z')$ sei ein (eventuell nicht willkürliches) Element dargestellt. Wegen der linearen Unabhängigkeit der u_i folgt aus

$$c = \sum_i u_i b_i = \sum_i u_i b_i'$$

$$b_i = b_i',$$

weshalb die Darstellung eindeutig ist. Die Gesamtheit

$$\{\sum_i u_i x_i\} \quad (x_i \in Z')$$

hat die Ordnung

$$(p^{n/m''})^{m''} = p^n,$$

weshalb sie sämtliche Elemente von Z umfaßt.

Bemerkung. Wenn die Koeffizienten rechts stehen, geschieht bei jeder Basisdarstellung die Addition komponentenweise. Dies schließt man aus dem distributiven Gesetz.

§ 4. Zwei spezielle Sätze, und über spezielle Systeme Z

In dem bekannten von *Veblen* und *Maclagan-Wedderburn* benutzten (allerdings assoziativen) Modell eines Systems Z (Transact. Americ. Math. Soc., vol. 8, S. 379)*) sind die Elemente des Primkörpers mit allen Elementen des Systems vertauschbar. Für solche Systeme gilt folgendes:

Satz 1. Damit alle Elemente von Z mit allen Elementen des Primkörpers vertauschbar sind, d. h. damit $b\alpha = \alpha b$ für sämtliche $b \in Z$ und sämtliche $\alpha \in \Pi$ gilt, ist notwendig und hinreichend, daß Z auch bei linksseitiger Multiplikation der Elemente von Π über diesem einen Vektorraum bildet.

*) Das System wurde zuerst von *L. E. Dickson* (in der im nachfolgenden Literaturhinweis (S. 32) kurz besprochenen Abhandlung) aufgestellt.

Beweis. Die im Satz erwähnte Vektorraumbedingung bedeutet, daß folgende zusätzlichen Forderungen erfüllt sein müssen:

1. Es existiert eine Basisdarstellung der Form $\sum_i \alpha_i u_i$ $(\alpha_i \in \Pi)$.
2. Es gilt das distributive Gesetz $(\alpha+\beta)b = \alpha b + \beta b$ für alle $b \in Z$ und alle $\alpha, \beta \in \Pi$.
3. Es gilt das assoziative Gesetz $(\alpha\beta)b = \alpha(\beta b)$ für alle $b \in Z$ und alle $\alpha, \beta \in \Pi$.

Die restlichen Vektorraumaxiome sind erfüllt, wie man leicht nachprüfen kann.

Wir beweisen zuerst, daß die Bedingungen 1. bis 3. notwendig sind (indem wir nachweisen, daß sie bei der Allgemeingültigkeit von $b\alpha = \alpha b$ $(b \in Z, \alpha \in \Pi)$ beweisbar sind):

Daß Bed. 1. erfüllt sein muß, ist trivial, da wegen

$$u_j \alpha_j = \alpha_j u_j$$
$$b = \sum_i u_i \alpha_i = \sum_i \alpha_i u_i$$

gilt. Ebenso einfach ist die Notwendigkeit von Bed. 2. nachzuweisen:

$$(\alpha+\beta)b = b(\alpha+\beta) = b\alpha + b\beta = \alpha b + \beta b$$

Die Notwendigkeit von Bed. 3. ergibt sich wie folgt:

$$(\alpha\beta)b = (\beta\alpha)b = b(\beta\alpha) = (b\beta)\alpha = \alpha(b\beta) = \alpha(\beta b)$$

Damit ist erwiesen, daß die im Satz erwähnte Vektorraumeigenschaft von Z notwendig ist, damit allgemein $b\alpha = \alpha b$ $(b \in Z, \alpha \in \Pi)$ gültig ist.

Um zu beweisen, daß die Bedingungen 1. bis 3. hinreichend sind, müssen wir zeigen, daß $b\alpha = \alpha b$ beweisbar ist, wenn diese Bedingungen vorausgesetzt werden: Wir benötigen hierzu nur Bed. 2:

$$b\alpha = b(\varepsilon+\varepsilon+\ldots) = b+b+\ldots = \varepsilon b + \varepsilon b + \ldots$$
$$= (\varepsilon+\varepsilon+\ldots)b = \alpha b,$$

wodurch auch der zweite Teil unserer Behauptung bewiesen ist.

Es folgt nun eine schwächere Bedingung für die Allgemeingültigkeit von $b\alpha = \alpha b$:

Satz 2. Damit in Z allgemein $b\alpha = \alpha b$ $(b \in Z, \alpha \in \Pi)$ gilt, ist die Allgemeingültigkeit von $(\alpha+\varepsilon)b = \alpha b + b$ notwendig und hinreichend.

Beweis. Da aus $b\alpha = \alpha b$ dieses distributive Gesetz und sogar $(\alpha+\beta)b = \alpha b + \beta b$ bewiesen werden kann, ist die Bedingung notwendig. Da jedes Element von Π in der Form $\alpha = \varepsilon\nu\,(0 \leqq \nu < p)$ geschrieben werden kann und die Behauptung für $\nu = 0$ offenbar richtig ist, können wir den Satz mit vollständiger Induktion nach ν beweisen:

$$b(\varepsilon\nu+\varepsilon) = b(\varepsilon\nu)+b = (\varepsilon\nu)b+b = (\varepsilon\nu+\varepsilon)b.$$

Wir wollen nun einige Sätze über vier spezielle Arten von Systemen Z beweisen.

a) Systeme Z, bei denen die Elemente von A mit sämtlichen von Z vertauschbar sind

Diese Systeme haben die Eigenschaft, daß bei der Basisdarstellung nach Δ die Koeffizienten mit den Basiselementen vertauscht werden können.

Satz 3. A fällt mit Δ zusammen.

Beweis. Wir müssen zeigen, daß

$$(x+y)a = xa+ya \qquad (x, y \in Z, a \in A)$$

gilt:

$$(x+y)a = a(x+y) = ax+ay = xa+ya$$

Es existiert ferner ein weiteres assoziatives und ein weiteres distributives Gesetz:

Satz 4. Es gilt $\qquad (a_1a_2)x = a_1(a_2x)$

Beweis.
$$(a_1a_2)x = x(a_1a_2) = (xa_1)a_2 = (a_1x)a_2 = a_1(xa_2) = a_1(a_2x)$$

Satz 5. Es ist $\qquad (a_1+a_2)x = a_1x+a_2x$

Beweis. $(a_1+a_2)x = x(a_1+a_2) = xa_1+xa_2 = a_1x+a_2x$

Bemerkung. Es besteht eine gewisse Symmetrie zwischen dem früheren assoziativen Gesetz von A $((xy)a = x(ya))$ und demjenigen von Satz 4: obige Beziehung bleibt richtig, wenn x und y durch Elemente aus A ersetzt werden und für a ein beliebiges Element aus Z gesetzt wird. Das Analoge gilt zwischen dem früheren distributiven

Gesetz für $\Delta((x+y)\delta = x\delta + y\delta)$, das ja hier auch für A gilt, und demjenigen von Satz 5.

b) Systeme vom Typus Veblen, Maclagan-Wedderburn (VW-Systeme)

Dieses Beispiel eines Systems Z wurde schon früher zitiert (§ 4). Es soll im folgenden einiges über dieses und gewisse etwas allgemeinere Systeme ausgesagt werden, wobei wir die Gültigkeit des assoziativen Gesetzes der Multiplikation nicht voraussetzen wollen. Ein solches System (kurz VW-System genannt) sei durch folgende zu den Axiomen eines Systems Z hinzutretende Eigenschaften charakterisiert:

1. Die Multiplikation eines Elementes mit einem solchen aus Δ ist kommutativ; die Multiplikation mit den übrigen Elementen ist entweder kommutativ oder antikommutativ.
2. Sämtliche Quadrate sind Elemente aus Δ.

Bemerkungen. 1. Die Multiplikation zweier von null verschiedenen Elemente ist dann und nur dann zugleich kommutativ und antikommutativ, wenn die Charakteristik zwei ist. (Das System ist dann kommutativ und nach § 5, Satz 2, deshalb zudem beidseitig distributiv.) Denn aus

$$bc = -(cb) = c(-b) = cb$$

folgt

$$b = -b$$

2. Die Relation $b^2 = \delta^2 (b \notin \Delta, \delta \in \Delta)$ ist unmöglich; denn sonst wäre $b(b+\delta) = \delta(b+\delta)$, $b+\delta \neq 0$, also $b = \delta$.

Satz 6. Die Produkte von drei gleichen Elementen sind assoziativ. (Wir können somit von dritten Potenzen sprechen.)

Der *Beweis* ist sehr einfach: infolge der zwei zusätzlichen Axiome ist

$$b \cdot b^2 = b^2 \cdot b$$

Es folgen noch zwei weitere Sätze über die Produkte gleicher Faktoren:

Satz 7. Die Produkte aus einer geraden Anzahl gleicher Elemente sind immer Elemente aus Δ.

Beweis. Wir wollen für die Produkte gleicher Faktoren die Potenzschreibweise benützen, obgleich diese vieldeutig ist und wollen zeigen, daß $b^{2n}\,(n>0)$ für jede Art der Zusammenfassung der Faktoren und jedes n zu Δ gehört. Der Beweis soll durch vollständige Induktion nach n geliefert werden. Für $n=1$ ist die Behauptung nach Zusatz-Axiom 2. richtig. Nehmen wir also an, sie stimme für jede Zahl kleiner n. Es sei

$$b^{2n} = b^m \cdot b^{2n-m} \qquad (0<m<2n)$$

Wir müssen drei Fälle unterscheiden.

1. Fall: m gerade.

Es ist dann auch $2n-m$ gerade, weshalb nach Induktionsvoraussetzung beide Faktoren und somit auch das Produkt in Δ liegen.

2. Fall: m ungerade $<2n-1$.

Es ist dann auch $2n-m$ ungerade. Es sei

$$b^{2n} = b^m\,(b^{n'} \cdot b^{2n-m-n'}) \qquad (0<n'<2n-m)$$

Wir müssen nun zwei Unterfälle unterscheiden:

1. Unterfall: n' ungerade.

Es ist dann $2n-m-n'$ gerade, und es ist

$$b^{2n} = b^m\,(b^{n'} \cdot b^{2n-m-n'}) = (b^m \cdot b^{n'})\,b^{2n-m-n'},$$

da der letzte Faktor nach Induktionsvoraussetzung zu Δ gehört. Da $m+n'$ $(<2n)$ auch eine gerade Zahl ist, liegt $b^m \cdot b^{n'}$ nach Induktionsvoraussetzung ebenfalls in Δ und somit auch das Produkt dieser beiden Elemente.

2. Unterfall: n' gerade.

Es ist dann $2n-m-n'$ ungerade, und es ist (Anwendung von Zusatz-Axiom 1!)

$$b^{2n} = b^m\,(b^{n'} \cdot b^{2n-m-n'}) =$$
$$b^m\,(b^{2n-m-n'} \cdot b^{n'}) = (b^m \cdot b^{2n-m-n'})\,b^{n'}$$

Beide Faktoren — und somit auch ihr Produkt — der rechten Seite dieser Gleichungskette liegen in Δ, da beide aus einer geraden

Anzahl gleicher Faktoren aufgebaut sind, weshalb auch in diesem Falle b^{2n} in Δ liegt.

3. Fall: $m = 2n - 1$.

Es ist dann

$$b^{2n} = b^{2n-1} \cdot b$$

Wir vertauschen nun die beiden Faktoren mit Hilfe des kommutativen bzw. antikommutativen Gesetzes:

$$b^{2n} = \pm b \cdot b^{2n-1}$$

Gemäß dem zweiten Fall liegt $b \cdot b^{2n-1}$ in Δ, also auch $\pm b \cdot b^{2n-1}$.

Unser Satz ist damit vollständig bewiesen.

Satz 8. Eine ungerade Potenz läßt sich immer in der Form

$$b^{2n+1} = b\,\delta \qquad (\delta \in \Delta)$$

darstellen.

Beweis. Für $n = 0$ ist die Behauptung offenbar richtig. Wir können somit vollständige Induktion nach n anwenden. Hieraus folgt

$$b^{2n+1} = b^{n'} \cdot b^{2n+1-n'} = b\,\delta \qquad (0 < n' < 2n+1),$$

da nach Satz 7 der gerade Faktor in Δ liegt und auf den andern die Induktionsvoraussetzung zutrifft.

Folgerungen. 1. Die Produkte aus einer ungeraden Anzahl gleicher, nicht in Δ liegender Elemente können nicht diesem Körper angehören.

2. Die Gleichungen vom Typus

$$\delta_1 x^{2n+1} = \delta_2 \qquad (\delta_i \in \Delta,\ \delta_1 \neq 0)$$

haben höchstens in Δ Lösungen, da x^{2n+1} (bei jeder Art der Zusammenfassung der Faktoren) in Δ liegen muß und als Basis dieser Potenz deshalb nur ein Element aus Δ in Frage kommt.

3. Die Gleichungen vom Typus

$$x^{2n} = c$$

sind für $c \notin \Delta$ im System unlösbar.

Satz 9. Das Produkt zweier Elemente ist gleich dem Produkt ihrer Additionsinversen, d. h.

$$b\,c = (-b)(-c)$$

Beweis. Bedenkt man, daß eine Beziehung $bc=(-b)c$ nur möglich ist, wenn Z die Charakteristik zwei hat und daß in diesem Falle der Satz trivial ist, so ergibt sich, falls die beiden Faktoren antikommutativ sind,

$$bc = -(cb) = c(-b) = -((-b)c) = (-b)(-c)$$

und im kommutativen Falle

$$bc = cb = -(c(-b)) = -((-b)c) = (-b)(-c)$$

Korrolar. Ersetzt man in Satz 9 b durch $-b$, so ergibt sich

$$(-b)c = -(bc)$$

Bemerkung. Satz 9 (samt Korrolar) gilt nicht für sämtliche Systeme Z. Im Abschnitt d) dieses Paragraphen ist nämlich von zwei Modellen von Systemen Z die Rede, bei denen er nicht stimmt.

Satz 10. Das Produkt von n Faktoren bleibt sich gleich oder ändert nur das Vorzeichen, wenn man dessen Faktoren durch ihre Additionsinversen ersetzt, und zwar trifft das erstere bei gerader, das letztere bei ungerader Faktorenzahl zu. (Verallgemeinerung von Satz 9.) Beide Fälle können in *eine* Formel zusammengefaßt werden:

$$\prod_1^n b_i = (-\varepsilon)^n \prod_1^n -b_i$$

Beweis. Für $n=1$ ist die Behauptung trivial, und für $n=2$ ist sie die Aussage des vorhergehenden Satzes. Wir beweisen den Satz durch vollständige Induktion nach n. Somit haben wir

$$\prod_1^n b_i = \prod_1^m b_i \prod_{m+1}^n b_i = (\pm \prod_1^m -b_i)(\pm \prod_{m+1}^n -b_i) \qquad (0<m<n)$$

Gilt beim linken Klammerausdruck das Pluszeichen (m gerade), so ist die Behauptung evident (Anwendung von § 1, Satz 4); gilt das Minuszeichen (m ungerade), so führt man diesen Fall durch Anwendung von Satz 9 auf den vorherigen zurück. Der Satz ist damit bewiesen.

c) Ein Satz über die assoziativen Systeme Z

Darunter wollen wir solche Systeme Z verstehen, bei denen die Multiplikation assoziativ ist. Wie schon früher bemerkt, ist bei

diesem Spezialfall das Untersystem A keine echte Teilmenge, weshalb die Aussagen über A (s. § 2) auch für die assoziativen Systeme Z gelten und umgekehrt.

Es soll nun hier für diese Systeme ein Satz über lineare Gleichungen Platz finden.

Satz 12. Ein lineares Gleichungssystem mit zwei Unbekannten

$$b_{00}x_0 + b_{01}x_1 = c_0$$
$$b_{10}x_0 + b_{11}x_1 = c_1$$

ist dann und nur dann eindeutig lösbar, wenn eine Ungleichung

$$b_{j+1,i}b_{ji}^{-1}b_{j,i+1} - b_{j+1,i+1} \neq 0 \qquad (b_{ji} \neq 0)$$

erfüllt ist. Die Indizes sind modulo zwei zu reduzieren.

Beweis. Wenn (mindestens) ein b verschwindet, ist die Richtigkeit der Behauptung ohne weiteres einzusehen. — Im andern Falle wird folgender Weg beschritten: Man versucht die eine der beiden Unbekannten mittels der bekannten (elementaren) Substitutionsmethode zu bestimmen. Dies führt auf eine Gleichung vom in § 1, Satz 5, behandelten Typus. Für jede Unbekannte hat man zwei Möglichkeiten für die Auflösung, was total vier Gleichungen ergibt. Aus obiger Ungleichung erhält man, wenn i und j durch 0 und 1 ersetzt werden, für jede der vier Gleichungen die im zitierten Satz enthaltene Ungleichung (Lösbarkeitsbedingung). Wenn somit eine dieser Ungleichungen erfüllt ist, erhält man eine Lösung für die eine Unbekannte (die andere ist dann wegen Axiom M. 1. ebenfalls bestimmt). Im andern Fall hat das Gleichungssystem keine Lösung, oder es ist vieldeutig lösbar.

d) Über eine weitere Klasse von Systemen Z

Daß die Elemente außerhalb Δ eines Systems Z, wenn dieses eine Erweiterung vom Range zwei über diesem Körper ist, einer Gleichung zweiten Grades mit Koeffizienten aus Δ genügen, ist leicht einzusehen. Bedeutender erscheint die Tatsache, daß Systeme Z vorkommen, bei denen diese Elemente, wobei deren Anzahl größer als zwei ist, alle *derselben* quadratischen Gleichung genügen.

Von solchen Systemen soll nun etwas ausgesagt werden — zwei weitere Sätze folgen am Schluß des letzten Paragraphen —, wobei

wir außer der Voraussetzung über den Rang von Z über Δ des weiteren noch fordern wollen, daß die Elemente von Δ mit sämtlichen von Z vertauschbar sind.

Das schon wiederholt genannte Modell von *Veblen* und *Maclagan-Wedderburn* hat diese Eigenschaften. Seine Elemente außerhalb Δ genügen der Gleichung $x^2 = -\varepsilon$. *R. Stettler* hat in § 7 seiner in der Einleitung zitierten Arbeit ein solches Beispiel angegeben (es hat wie das Vorherige die Ordnung neun), bei dem nicht nur das zweite distributive Gesetz, sondern auch das assoziative Gesetz der Multiplikation nicht allgemein gilt. Seine Elemente außerhalb Δ genügen der Gleichung $x^2 = \varepsilon - x$ *).

Bei einem weiteren Modell dieses Typus der Ordnung neun (nach § 5, Satz 10, dem letzten dieser Ordnung) genügen die Elemente außerhalb Δ der Gleichung $x^2 = \varepsilon + x$. Wenn wir für seine Elemente eine Basisdarstellung wählen (Addition dann komponentenweise!), so hat die *Multiplikationstabelle* folgendes Aussehen:

$\cdot$	$-\varepsilon$	u	$-u$	$\varepsilon+u$	$\varepsilon-u$	$-\varepsilon+u$	$-\varepsilon-u$
$-\varepsilon$	ε	$-u$	u	$-\varepsilon-u$	$-\varepsilon+u$	$\varepsilon-u$	$\varepsilon+u$
u	$-u$	$\varepsilon+u$	$-\varepsilon-u$	$\varepsilon-u$	$-\varepsilon$	ε	$-\varepsilon+u$
$-u$	u	$-\varepsilon+u$	$\varepsilon-u$	$-\varepsilon$	$\varepsilon+u$	$-\varepsilon-u$	ε
$\varepsilon+u$	$-\varepsilon-u$	ε	$-\varepsilon$	$-\varepsilon+u$	u	$-u$	$\varepsilon-u$
$\varepsilon-u$	$-\varepsilon+u$	$-\varepsilon$	ε	$-u$	$-\varepsilon-u$	$\varepsilon+u$	u
$-\varepsilon+u$	$\varepsilon-u$	$-\varepsilon-u$	$\varepsilon+u$	ε	$-u$	u	$-\varepsilon$
$-\varepsilon-u$	$\varepsilon+u$	$\varepsilon-u$	$-\varepsilon+u$	u	ε	$-\varepsilon$	$-u$

Auch bei diesem Beispiel gilt das zweite distributive Gesetz und das assoziative Gesetz *nicht* allgemein. Wie schon unter Abschnitt b) bemerkt, gilt bei den letzteren beiden Modellen, im Gegensatz zu den VW-Systemen (s. Satz 9), auch $bc = (-b)(-c)$ nicht immer; dasselbe ist deshalb auch von $(-b)c = -(bc)$ zu sagen (da die erstere Beziehung sonst beweisbar wäre).

Es sollen nun zwei Sätze über solche Systeme (Bez. Z^*) bewiesen werden.

Satz 13. Wenn die Charakteristik größer als zwei ist, so sind sämtliche Körper, die in Z^* liegen, Unterkörper von Δ.

*) Diese Eigenschaft bemerkte Herr Prof. Dr. P. Bernays.

Beweis. Wenn $K \subset Z^*$ ein Körper der Ordnung p^s wäre, der nicht in Δ enthalten ist, dann müßten mindestens drei Elemente von K außerhalb Δ liegen. Nämlich, der Durchschnitt von K und Δ habe die Ordnung p^r, wobei $s > r \geqq 1$. Die Differenz $p^s - p^r$ ist dann für alle zulässigen Werte für p, r und s größer als drei. Da in einem Körper eine quadratische Gleichung aber höchstens zwei Lösungen haben kann, die Elemente von K außerhalb Δ aber nach Voraussetzung der „definierenden Gleichung" *) genügen müßten, ist obige Annahme widerlegt.

Folgerung. Δ ist der umfassendste Körper, über dem Z^* ein Vektorraum ist.

Satz 14. Bei Systemen Z^*, bei denen jedes Element außerhalb Δ derselben Gleichung $x^2 = \delta_1 + x\,\delta_2$ genügt, ist bei $\delta_2 \neq 0$ jedes Element außerhalb Δ ein Quadrat.

Beweis. Aus
$$x^2 = \delta_1 + x\,\delta_2$$
$$y^2 = \delta_1 + y\,\delta_2$$
folgt
$$x^2 - y^2 = x\,\delta_2 - y\,\delta_2$$

Wenn $\delta_2 \neq 0$, erkennt man mittels Axiom M. 1., daß obiger Ausdruck nur für $x = y$ verschwindet. Verschiedene Elemente außerhalb Δ haben deshalb immer verschiedene Quadrate, weshalb deren Anzahl mit der entsprechenden Elementenzahl übereinstimmt. Jedes Element außerhalb Δ ist deshalb ein Quadrat.

§ 5. Über die Existenz und Bestimmtheit der Systeme Z

Zu jeder Primzahlpotenz gibt es mindestens ein System Z dieser Ordnung, nämlich immer ein Galoisfeld (das ja ein spezielles System Z ist). Unter „eigentlichen" Systemen Z wollen wir solche verstehen, bei denen das zweite distributive Gesetz nicht allgemein gilt. Die andern sollen „uneigentliche" genannt werden.

Für das Folgende hat der nachstehende Satz eine gewisse Bedeutung, weshalb er an die Spitze gestellt werden soll.

*) Wir werden im nächsten Paragraphen zeigen, daß bei gegebener Ordnung durch diese Gleichung ein solches System Z eindeutig bestimmt ist.

Satz 1. Zu gegebener Ordnung ist der Vektorraum über Π, somit also die additive Gruppe eines Systems Z, eindeutig bestimmt.

Beweis. Durch Angabe des Grundkörpers und der Dimension ist ein Vektorraum bis auf Isomorphie eindeutig bestimmt (s. etwa *van der Waerden*, Moderne Algebra I). Wie in § 3 erwähnt, bildet Z über dem Primkörper Π einen Vektorraum. Π und die Dimension sind durch Angabe der Ordnung von Z eindeutig festgelegt somit also auch die additive Gruppe von Z.

Satz 2. Es gibt keine eigentlichen kommutativen Systeme Z.

Beweis. Die Kommutativität der Multiplikation hat die Gültigkeit des zweiten distributiven Gesetzes zur Folge:

$$(x+y)z = z(x+y) = zx+zy = xz+yz$$

Satz 3. Zu einer Primzahl gibt es nur *ein* System Z dieser Ordnung, nämlich nur das Galoisfeld.

Der *Beweis* folgt aus den Sätzen 7 und 8 von § 2 und Satz 3 von § 3.

Satz 4. Es gibt keine eigentlichen Systeme Z der Ordnung vier, sondern nur das Galoisfeld dieser Ordnung.

Beweis. Wir führen den Beweis, indem wir ein solches Modell zu konstruieren versuchen: Die Charakteristik muß zwei sein; somit besteht der Primkörper aus den Elementen 0 und ε. Der Rang von Z über Π ist zwei; wir haben es deshalb mit einer zweigliedrigen Basis zu tun. Die Elemente lassen sich somit wie folgt darstellen:

$$0,\ \varepsilon,\ r,\ \varepsilon+r$$

Nach Satz 1 ist die additive Gruppe eindeutig festgelegt. Daß ebenfalls nur *eine* Multiplikationsvorschrift möglich ist, sieht man bequem aus der nachstehenden Multiplikationstabelle:

$\cdot$	r	$\varepsilon+r$
r	$\varepsilon+r$	ε
$\varepsilon+r$	ε	r

(Zunächst: $r(\varepsilon+r) \neq 0, r, \varepsilon+r$, also $=\varepsilon$)

Darstellung des Modells: $k+lr \qquad (k, l \bmod 2)$

$1+r+r^2=0$

Satz 5. Das GF (8) ist das einzige assoziative System Z der Ordnung acht. (Es gibt somit keine eigentlichen.)

Beweis. Die (zyklische) multiplikative sowie nach Satz 1 auch die additive Gruppe sind eindeutig bestimmt. Das GF (8) ist deshalb das einzige System Z dieser Ordnung.

Bemerkung. Satz 5 läßt sich leicht verallgemeinern: Zu einer Primzahlpotenz, die Nachfolger einer Primzahl ist, gibt es außer dem Galoisfeld kein assoziatives System Z.

Aus den Sätzen 3 bis 5 und aus der Assoziativität des Modells von *Veblen* und *Maclagan-Wedderburn* folgert man

Satz 6. Die Ordnung neun ist die kleinste, zu der eigentliche assoziative Systeme Z gehören.

Bemerkung. Durch Probieren der Möglichkeiten kann man feststellen, daß das GF (8) das einzige System Z der Ordnung acht ist, was eine Verallgemeinerung von Satz 5 bedeutet. Auch Satz 6 läßt sich deshalb verschärfen (Weglassung von „assoziative").

Satz 7. Es gibt keine eigentlichen VW-Systeme der Ordnung 2^n.

Beweis. Systeme Z dieser Ordnung haben immer die Charakteristik zwei, und bei solchen ist jedes Element mit seinem Additionsinversen identisch. Ein VW-System dieser Art ist deshalb kommutativ und somit beidseitig distributiv.

Satz 8. Es gibt keine eigentlichen antikommutativen Systeme Z (das sind solche, bei denen jedes Produkt antikommutativ ist).

Beweis. Aus dem Spezialfall $\varepsilon^2 = -\varepsilon^2$ folgert man die Notwendigkeit der Charakteristik zwei, und hieraus folgt nach dem Beweis von Satz 7 die Behauptung.

Satz 9. Ist ein System Z als endlicher Vektorraum über $K \subseteq \Delta$ gegeben, so ist es durch Angabe der Produkte der Elemente des Vektorraumes mit dessen Basiselementen eindeutig bestimmt.

Beweis. Wir beweisen die Bestimmtheit der Multiplikation zuerst für die Elemente der Form $u_k \beta_k$: Wenn $(\beta_i \in K)$

$$(\sum_i u_i \beta_{ij})\, u_k = \sum_i u_i \beta^i_{jk}$$

so ist

$$(\sum_i u_i \beta_{ij}).(u_k \beta_k) = ((\sum_i u_i \beta_{ij})\, u_k)\, \beta_k$$

$$= (\sum_i u_j \beta^i_{jk})\, \beta_k = \sum_i u_i (\beta^i_{jk} \beta_k)$$

Für beliebige Elemente aus Z ist nun der Satz wegen des distributiven Gesetzes evident.

Bemerkung. Natürlich können die im Satz 9 erwähnten Produkte nicht willkürlich definiert werden, da sie dem Axiom M. 1. genügen müssen. Hingegen sind bei willkürlicher Definition dieser Produkte sämtliche Axiome außer M. 1. erfüllt. Die Anzahl solcher Systeme zu einer gegebenen Ordnung läßt sich durch eine einfache kombinatorische Überlegung angeben, was dann eine (allerdings grobe) Abschätzung der Anzahl der Systeme Z zu einer bestimmten Ordnung nach oben ergäbe. (Als eines der Basiselemente ist hierbei ε zu wählen.) Diese Abschätzung läßt sich etwas verfeinern, wenn man die die Multiplikation definierenden Produkte so wählt, daß diese mit Axiom M. 1. nicht im Widerspruch stehen.

Obiger Satz ließe sich dazu verwenden, Systeme Z mit vorgeschriebener Ordnung zu suchen.

Beispiel. Gesucht Systeme Z der Ordnung neun. — Die Basis muß zweigliedrig sein, und wir können ε und ein Element r als Basiselemente wählen. Der Vektorraum und die Produkte mit ε sind eindeutig bestimmt, und die Produkte der Elemente mit r bestimmen das System eindeutig. Man könnte nun systematisch, mit oben erwähnter Einschränkung, diese Produkte definieren (es gibt etwa 35000 Möglichkeiten) und solange fortfahren, bis einmal Axiom M. 1. erfüllt ist.

Die nächsten zwei Sätze gelten für VW-Systeme, die wie folgt spezialisiert sind: Das Produkt zweier Elemente außerhalb Δ ist kommutativ, wenn die beiden Elemente im Sinne von § 3 linear abhängig sind; im andern Fall ist es antikommutativ. (Das Modell von *Veblen* und *Maclagan-Wedderburn* besitzt diese Eigenschaft.)

Satz 10. Ist ein (spezielles) VW-System als endlicher Vektorraum über $K \subseteq \Delta$ gegeben, so ist es durch Angabe der Produkte der Basiselemente eindeutig bestimmt.

Beweis. Wir beweisen die Behauptung nur für Produkte der Form

$$(\sum_i u_i \beta_i)\, u_j$$

Der allgemeine Fall ist dann hieraus nach Satz 9 zu entnehmen.

Da die Produkte bei diesen Systemen entweder kommutativ oder antikommutativ sind, haben wir die Alternative

$$(\sum_i u_i \beta_i)\, u_j = \pm (u_j \sum_i u_i \beta_i)$$

Weitere Umformung ergibt, wenn $u_1 = \varepsilon$,

$$\pm (u_j \sum_i u_i \beta_i) = \pm \sum_i (u_j u_i) \beta_i \,[= \pm (u_j \beta_1 + u_j{}^2 \beta_j) \mp \sum_{(i \neq 1, j)} (u_i u_j) \beta_i]$$

Der soeben bewiesene Satz soll in Satz 11 Anwendung finden.

Satz 11. Es gibt nur *ein* (spezielles) VW-System der Ordnung neun.

Beweis. Π und nach Satz 1 auch der Vektorraum über Π sind eindeutig bestimmt. Δ fällt mit Π zusammen. Die Basis ist zweigliedrig, und eines der beiden Basiselemente liege in Δ. Nach Satz 10 ist somit das System durch Definition des Quadrates des andern Basiselementes eindeutig bestimmt. Da Δ aus drei Elementen besteht, hat man drei Möglichkeiten der Definition zu untersuchen: 0 kommt nicht in Frage, da in Z keine Nullteiler möglich sind; $-\varepsilon$ ergibt das bekannte Modell von *Veblen* und *Maclagan-Wedderburn*. ε schließlich ist nach der zweiten Bemerkung auf Seite 21 nicht möglich.

Abschließend folgen noch zwei Sätze über die in § 4, d) behandelten speziellen Systeme Z.

Satz 12. Ein System vom Typus des § 4, d) ist durch dessen Ordnung und die definierende Gleichung eindeutig bestimmt.

Beweis. Durch die Ordnung ist die additive Gruppe des Systems nach Satz 1 eindeutig festgelegt. Die Quadrate sind durch die definierende Gleichung eindeutig bestimmt. Es erübrigt sich zu zeigen, daß das Produkt bc zweier verschiedener, nicht in Δ liegender Elemente ebenfalls eindeutig festgelegt ist: Die Basis des Vektorraumes werde in (ε, b) transformiert; dann ist $c = \delta_1 + b\,\delta_2$ und

$$b\,c = b\,(\delta_1 + b\,\delta_2) = b\,\delta_1 + b^2\,\delta_2$$

Satz 13. Die in § 4, d) angegebenen drei Modelle von Systemen Z^* sind die einzigen der Ordnung neun.

Beweis. Die übrigen quadratischen Gleichungen bestimmen keine Systeme Z; denn:

1. Bei $x^2 = -\varepsilon + x$ hat man den Widerspruch $\begin{cases} (-\varepsilon)u = -u \\ (-\varepsilon+u)u = -u \end{cases}$
2. „ $x^2 = -\varepsilon - x$ „ „ „ „ $(\varepsilon+u)u = u$
3. „ $x^2 = \varepsilon$ „ „ „ „ $\begin{cases} (-\varepsilon)u = -u \\ (\varepsilon+u)u = -u \end{cases}$

(Zur Berechnung der Produkte wird man sich der im Beweis des vorherigen Satzes angewandten Methode bedienen.) — Bei Gleichungen mit verschwindendem absolutem Glied stößt man noch leichter auf Widersprüche.

Literaturhinweis

Es sei hier auf die vor 50 Jahren erschienene Abhandlung „On finite algebras" von *L. E. Dickson* (Göttinger Nachrichten, 1905) aufmerksam gemacht, in der von zwei Verallgemeinerungen der Galoisfelder die Rede ist. Die eine betrifft die assoziativen Systeme Z, die andere die nicht-assoziativen Galoisfelder. Was über die ersteren ausgeführt wird, hat im Hinblick auf die vorliegende Arbeit besondere Bedeutung, weshalb hierüber kurz berichtet werden soll:

Der Verfasser nimmt die Aufgabe in Angriff, alle assoziativen Systeme Z aufzustellen. Er zeigt, daß ein eigentliches assoziatives System Z der Ordnung p^n dann und nur dann existiert, wenn $p^n - 1$ und n nicht teilerfremd sind. Für die Ordnungen p^2, mit ungerader Primzahl p, und p^3, wobei p von der Form $3l+1$ ist, stellt er explizite solche Systeme auf, darunter das von *Veblen* und *Maclagan-Wedderburn* (vgl. § 4) benutzte. Eine vollständige Aufstellung aller derartigen Systeme Z gelingt aber nur für diejenigen Werte von n und p, für die n ungerade ist und außerdem ein gewisser Satz über die Existenz eines Normalteilers in einer Gruppe der Ordnung $p^n - 1$ gilt. — In den axiomatischen Betrachtungen sticht das Resultat hervor, daß bei assoziativen Systemen Z die Kommutativität der Addition aus den übrigen Axiomen beweisbar ist. Der angeführte Beweis hiefür stammt von *J. H. Maclagan-Wedderburn.*

Lebenslauf

Mein Geburtsdatum ist der 21. August 1920. In Zürich besuchte ich die Volksschule sowie die Kantonale Handelsschule. Während der anschließenden praktischen Tätigkeit auf einer Großbank in Zürich besuchte ich das Abendgymnasium Juventus, um mich für die Aufnahme an die ETH vorzubereiten. Dann studierte ich an der ETH Mathematik. Anschließend betätigte ich mich einige Jahre als Vikar und Hilfslehrer an verschiedenen Mittelschulen. Hierauf arbeitete ich drei Jahre beim Eidgenössischen Statistischen Amt in Bern. Seit 1. Juni 1955 bin ich bei einer Lebensversicherung in Zürich angestellt.

Für die Anregung zu vorliegender Arbeit sowie für manche Diskussion bin ich Herrn Prof. Dr. *P. Bernays* zu Dank verpflichtet.