Endliche Inzidenzgruppen

KURT REIDEMEISTER zum 70. Geburtstag gewidmet

Von ERICH ELLERS und HELMUT KARZEL in Hamburg

Eine *Inzidenzgruppe* ist eine Menge G, die mit einer Gruppenstruktur und der Struktur eines projektiven Raumes der Dimension größer als 1 versehen ist und in der jede Linkstranslation $a^*: x \to ax (a, x \in G)$ von G auf sich eine Kollineation des projektiven Raumes ist.

Der Begriff Inzidenzgruppe umfaßt genau alle Kollineationsgruppen G, die genau einfach transitiv auf den Punkten eines projektiven Raumes Π operieren[1]).

Die Lösung des Problems, alle Inzidenzgruppen anzugeben, ist bisher für die Klasse der kommutativen Inzidenzgruppen (vgl. [5], [6], [1]) und die Klasse der elliptischen Gruppenräume (vgl. [4], [2]) gelungen. Hier soll dieses Problem für die Klasse aller endlichen desarguesschen Inzidenzgruppen gelöst werden.

Wie wir bereits früher gezeigt haben (vgl. [2]), entspricht jeder desarguesschen Inzidenzgruppe G eindeutig ein *normaler Fastkörper* (F, K), d.i. ein Fastkörper F, der einen Teilschiefkörper K enthält, so daß F ein Linksvektorraum über K und $K^* \lhd F^*$ ist[2]). Denn als desarguesschem projektivem Raum ist G ein Linksvektorraum F über einem Schiefkörper K zugeordnet. Neben der bereits in F vorhandenen Vektoraddition läßt sich mit Hilfe der Inzidenzgruppe eine Multiplikation in F erklären. Hierzu zeichnen wir einen Koordinatenvektor $\mathfrak{e}$ des Punktes 1 von G aus, bezeichnen mit $\varphi: F^* \to G$ die Abbildung, die jeden von Null verschiedenen Vektor $\mathfrak{a}$ aus F auf den durch $\mathfrak{a}$ repräsentierten

---

[1]) Zu zwei Punkten a, b einer Inzidenzgruppe G gibt es genau eine Linkstranslation, nämlich $(ba^{-1})^*$, die a in b überführt. Also operiert die Gruppe der Linkstranslationen, die zu G isomorph ist, genau einfach transitiv auf den Punkten von G. Ist umgekehrt G eine Kollineationsgruppe, die genau einfach transitiv auf den Punkten eines projektiven Raumes Π operiert, so zeichnen wir einen Punkt $P \in \Pi$ aus und identifizieren jedes Gruppenelement $a \in G$ mit dem Punkt $a(P) \in \Pi$. Auf diese Weise erhalten wir eine Inzidenzgruppe, denn die Abbildung $a^*: x = x(P) \to ax = ax(P) = a(x(P))$ ist eine Kollineation von Π.

[2]) F^* bzw. K^* bezeichnet die multiplikative Gruppe von F bzw. K. $K^* \lhd F^*$ bedeutet, daß K^* ein Normalteiler von F^* ist.

Punkt aus G abbildet, und ordnen jedem Vektor $\mathfrak{a} \neq 0$ aus F die semilineare Abbildung $\mathfrak{a}^*$ zu, die in G die Linkstranslation $(\varphi(\mathfrak{a}))^* : x \to \varphi(\mathfrak{a})x$ induziert und dabei den Vektor $\mathfrak{e}$ auf den Vektor $\mathfrak{a}$ abbildet. Definieren wir $\mathfrak{a} \cdot \mathfrak{b} = \mathfrak{a}^*(\mathfrak{b})$ für $\mathfrak{a} \neq 0$ und $0 \cdot \mathfrak{b} = 0$, so wird F hierdurch zu einem Fastkörper, der den mit der Menge $K\mathfrak{e}$ identifizierten Schiefkörper K als Teilmenge enthält. Es gilt $K^* \lhd F^*$; denn für $\lambda \in K^*$, $\mathfrak{a} \in F^*$ erhält man $\mathfrak{a}\lambda\mathfrak{a}^{-1} = \mathfrak{a}^*(\lambda\mathfrak{a}^{-1}) = \lambda^{\mathfrak{a}^*}\mathfrak{a}^*(\mathfrak{a}^{-1}) = \lambda^{\mathfrak{a}^*} \in K^*$ (hierbei ist $\lambda \to \lambda^{\mathfrak{a}^*}$ der Automorphismus von K der semilinearen Abbildung $\mathfrak{a}^*$). Also ist (F, K) ein normaler Fastkörper, aus dem man die Inzidenzgruppe G als Faktorgruppe F^*/K^* zurückerhält.

In natürlicher Weise kann man aus jedem beliebigen normalen Fastkörper (F, K) mit Rang $[F : K] > 2$ eine desarguessche Inzidenzgruppe G gewinnen, indem man die Faktorgruppe F^*/K^* bildet und die Elemente von F^*/K^* mit den Punkten des projektiven Raumes identifiziert, der dem Vektorraum F über K zugeordnet ist.

Die Frage nach allen endlichen desarguesschen Inzidenzgruppen ist also gleichwertig mit dem algebraischen Problem, alle endlichen normalen Fastkörper (F, K) mit Rang $[F : K] > 2$ anzugeben. Bei der Lösung dieses Problems werden wir uns auf das Resultat von Zassenhaus [10] stützen, daß jeder endliche Fastkörper F, dessen Rang über seinem Primkörper größer als 2 ist, ein Dickson-Veblenscher Fastkörper ist.

Wir werden also von einem endlichen Dickson-Veblenschen Fastkörper M ausgehen (in § 1 werden diese durch eine axiomatische Definition eingeführt und einige ihrer Eigenschaften hergeleitet) und nach den Teilkörpern L — wir werden sie *normale Teilkörper* nennen — von M fragen, für die (M, L) ein normaler Fastkörper ist. Jeder normale Teilkörper L von M hat die Eigenschaft, daß L^* ein zyklischer Normalteiler von M^* ist[3]). Daher werden wir in § 2 alle zyklischen Normalteiler von M^* bestimmen. Mit Hilfe dieses Resultats lassen sich dann alle normalen Teilkörper L von M angeben (§ 3) und damit alle endlichen desarguesschen Inzidenzgruppen (§ 4).

Die desarguesschen Inzidenzgruppen kann man in zwei Klassen einteilen, je nachdem ob alle Linkstranslationen von G von linearen Abbildungen im zugehörigen Vektorraum induziert werden, oder ob es mindestens eine Linkstranslation gibt, deren korrespondierende semilineare Abbildungen nicht linear sind. Demgemäß werden wir die Inzidenzgruppen der ersten Klasse *linear*, die der zweiten *nichtlinear* nennen. Ist (F, K) der zu einer Inzidenzgruppe G gehörige normale Fastkörper, so ist G genau dann linear, wenn K ein *zentraler* Teilkörper von F ist,

---

[3]) Da L ein endlicher Körper ist und $L^* \lhd M^*$ gilt, ist L^* ein zyklischer Normalteiler von M^*.

d.h. wenn K^* im Zentrum von F^* liegt; denn wie bereits gezeigt wurde, gilt $a\lambda a^{-1} = \lambda^{a^*} \in K^*$ für $\lambda \in K^*$, $a \in F^*$.

Unter den endlichen desarguesschen Inzidenzgruppen gibt es sowohl lineare als auch nichtlineare Inzidenzgruppen (§ 4). Zu den linearen Inzidenzgruppen gehören insbesondere die endlichen kommutativen desarguesschen Inzidenzgruppen. Diese sind sogar zyklisch und bei den zugehörigen normalen Fastkörpern (F, K) sind F und K endliche Körper.

Für einen vorgegebenen endlichen desarguesschen projektiven Raum Π lassen sich alle auf Π genau einfach transitiv operierenden Kollineationsgruppen angeben (§ 5). Alle endlichen Inzidenzgruppen haben die Eigenschaft, daß die Linkstranslationen auch auf den Hyperebenen genau einfach transitiv operieren (§ 6).

Zu bemerken ist noch, daß die ersten genau einfach transitiv operierenden Kollineationsgruppen G, die man betrachtet hatte, die sogenannten *zyklischen Geometrien* (vgl. [8], [3]) waren, bei denen G also eine zyklische Gruppe ist. Beispiele nichtzyklischer Kollineationsgruppen dieser Art hat später Zappa [9] angegeben. Rosati [7] konnte unlängst für die endlichen desarguesschen projektiven Ebenen alle genau einfach transitiv operierenden Kollineationsgruppen bestimmen.

§ 1. Dickson-Veblensche Fastkörper

Definition 1. *Ein Fastkörper* $M(+, \circ)$[4] *heißt Dickson-Veblenscher Fastkörper, wenn es eine dritte binäre Operation* $\cdot$ *gibt, so daß* $M(+, \cdot)$ *ein Schiefkörper ist und für jedes von Null verschiedene* a *aus* M *die Abbildung* $\varrho_a : x \to a^{-1}(a \circ x)$ *ein Automorphismus von* $M(+, \cdot)$ *ist; hierbei bezeichnet* a^{-1} *das Inverse von* a *im Schiefkörper* $M(+, \cdot)$[5].

Es sei $M(+, \circ)$ ein endlicher Dickson-Veblenscher Fastkörper. Die Abbildung $\varphi : a \to \varrho_a$ ist ein Homomorphismus der Gruppe $M^*(\circ)$ in die Automorphismengruppe von $M(+, \cdot)$. Aus dem Assoziativgesetz für und $\circ$ folgt nämlich:

$$a \circ (b \circ x) = a\varrho_a(b\varrho_b(x)) = (a\varrho_a(b))(\varrho_a\varrho_b(x)) = (a \circ b)\varrho_a\varrho_b(x)$$
$$= (a \circ b) \circ x = (a \circ b)\varrho_{a \circ b}(x),$$

d.h.

$$\varrho_{a \circ b} = \varrho_a\varrho_b. \tag{1}$$

[4]) Mit Fastkörper bezeichnen wir hier stets eine Menge, in der eine Addition und eine Multiplikation erklärt sind, so daß mit Ausnahme des rechtsseitigen Distributivgesetzes alle Schiefkörperaxiome erfüllt sind. Zassenhaus [10] nennt diese Fastkörper vollständige Fastkörper.

[5]) Ist $a \in M$, so bezeichnen wir mit a^n die n-te Potenz von a bezüglich der Multiplikation $\cdot$ und mit $a^{\overline{n}}$ die n-te Potenz von a bezüglich der Multiplikation $\circ$.

Also ist $\varphi(M^*) = \Gamma = \{\varrho_x;\ x \in M^*\}$ eine zyklische Gruppe, da sie Untergruppe der Automorphismengruppe des endlichen Körpers $M(+, \cdot)$ ist.

Es sei K_q der zu Γ gehörige Fixkörper von $M(+, \cdot)$, d. h. $K_q = \{x \in M(+, \cdot);\ \varrho(x) = x \text{ für alle } \varrho \in \Gamma\}$ und $q = |K_q|$. Dann wird Γ von dem Automorphismus $\varrho_0 : x \to x^q$ erzeugt. Bezeichnen wir mit n die Ordnung von Γ, so ist q^n die Anzahl der Elemente von M. $M(+, \circ)$ ist genau dann ein Körper (vgl. Satz 1), wenn Γ nur aus der Identität besteht.

Ist $U = \mathfrak{N}(\varphi) = \{x \in M^*;\ \varrho_x = 1\}$ der Kern des Homomorphismus φ, so gilt $|U| = m = \frac{q^n - 1}{n}$ und (wegen $u \circ x = u \cdot \varrho_u(x)$):

$$u \circ x = u \cdot x \quad \textit{für} \quad u \in U \quad \textit{und} \quad x \in M. \tag{2}$$

Hieraus folgt insbesondere, daß in U die Operationen $\circ$ und $\cdot$ übereinstimmen und daß daher die Einselemente von $M^*(\cdot)$ und $M^*(\circ)$ identisch sind. Infolgedessen ist U auch Untergruppe von $M^*(\cdot)$ und daher zyklisch. Ist ω eine Erzeugende von $M^*(\cdot)$, so wird U von ω^n erzeugt. Wegen (2) ist

$$M^* = U \cup U\omega \cup U\omega^2 \cup \cdots \cup U\omega^{n-1}$$

gleichzeitig eine Zerlegung von $M^*(\circ)$ und $M^*(\cdot)$ in Nebenklassen von U. Da ferner $\Gamma \cong M^*(\circ)/U$ ist, gibt es genau ein $\sigma < n$ mit $\varphi(\omega^\sigma) = \varrho_{\omega^\sigma} = \varrho_0$ $(\varrho_0 : x \to x^q)$. Somit ist $\omega^\sigma, (\omega^\sigma)^2, \ldots, (\omega^\sigma)^n$ [5]) ein Repräsentantensystem der Faktorgruppe $M^*(\circ)/U$. Nun gilt aber $(\omega^\sigma)^\beta = \omega^{\sigma\frac{q^\beta - 1}{q-1}}$. Also müssen die Zahlen $\sigma\frac{q^\beta - 1}{q-1}$ für $\beta = 1, 2, \ldots, n$ alle Restklassen mod n durchlaufen und $\sigma\frac{q^n - 1}{q-1} \equiv 0 \bmod n$ sein. Hieraus folgt aber $(\sigma, n) = 1$ und

$$\frac{q^\beta - 1}{q-1} \not\equiv 0 \bmod n \quad \textit{für} \quad 0 < \beta < n \quad \textit{und} \quad \frac{q^n - 1}{q-1} \equiv 0 \bmod n. \tag{3}$$

Ist m' das Produkt aller Primteiler p von $m = \frac{q^n - 1}{n}$ mit $p \nmid \sigma$, so gilt (wegen $(\sigma, n) = 1$) auch $(\sigma + m'n, mn) = 1$. Daher ist $\omega^{\sigma + m'n}$ eine Erzeugende von $M^*(\cdot)$. Da $\omega^{m'n} \in U$ ist, gelten nach (2) die Gleichungen

$$\omega^{\sigma + m'n} = \omega^{m'n} \cdot \omega^\sigma = \omega^{m'n} \circ \omega^\sigma$$

und

$$\varphi(\omega^{\sigma + m'n}) = \varphi(\omega^{m'n})\,\varphi(\omega^\sigma) = \varphi(\omega^\sigma) = \varrho_0.$$

Damit ist gezeigt:

(4) *Es gibt eine Erzeugende ω von $M^*(\cdot)$ mit $\varrho_\omega = \varrho_0$.*

Nun können wir den folgenden Satz beweisen:

Satz 1. *Die multiplikative Gruppe $M^*(\circ)$ eines endlichen Dickson-Veblenschen Fastkörpers der Ordnung q^n besitzt zwei Erzeugende a und b, die den Relationen*

$$a^{\underline{m}} = 1, \quad b^{\underline{n}} = a^{\underline{t}}, \quad b \circ a \circ b^{\underline{-1}} = a^{\underline{q}} \tag{5}$$

genügen, wobei für die Zahlen m, n, t und q die folgenden Bedingungen gelten:

$$(q-1)t = m > 0, \tag{6}$$

$$q^\nu \not\equiv 1 \bmod m \quad \text{für} \quad 1 \leqq \nu < n, \quad q^n \equiv 1 \bmod m, \tag{7}$$

$$(n, t) = (q-1, t) \leqq 2. \tag{8}$$

Beweis. Es sei ω eine Erzeugende von $M^*(\cdot)$ mit $\varrho_\omega = \varrho_0$ (vgl. (4)); ferner sei $a = \omega^n$ und $b = \omega$. Dann ist a eine Erzeugende von U, also gilt $a^{\underline{\alpha}} = a^\alpha \neq 1$ für $0 < \alpha < m$ und $a^m = 1$, und $1, b, b^{\underline{2}}, \ldots, b^{\underline{n-1}}$ ist einRepräsentantensystem der Faktorgruppe $M^*(\circ)/U$. Daher gilt sogar auf Grund von (2):

(9) *Jedes $x \in M^*(\circ)$ läßt sich eindeutig in der Form $x = a^{\underline{\alpha}} \circ b^{\underline{\beta}} = a^\alpha \cdot b^{\underline{\beta}}$ mit $0 \leqq \alpha < m = \frac{q^n - 1}{n}$ und $0 \leqq \beta < n$ darstellen.*

Aus (2) erhält man weiterhin:

$$\begin{aligned} b \circ a \circ b^{\underline{-1}} &= b \circ (a \cdot b^{\underline{-1}}) = b\varrho_b(a)\,\varrho_b(b^{\underline{-1}}) = \varrho_b(a)(b \circ b^{\underline{-1}}) \\ &= \varrho_b(a) = a^q = a^{\underline{q}}. \end{aligned}$$

Da die Ordnung von $\Gamma \cong M^*(\circ)/U$ gleich n ist, gilt $b^{\underline{n}} \in U$, also gibt es ein t mit $b^{\underline{n}} = a^t$ und $0 \leqq t < m$. Andrerseits ist $a^t = \omega^{nt}$ und $b^{\underline{n}} = \omega^{\underline{n}} = \omega^{\frac{q^n-1}{q-1}}$. Die Zahlen nt und $\frac{q^n-1}{q-1}$ sind beide positiv und kleiner als $nm = q^n - 1$. Also gilt $nt = \frac{q^n-1}{q-1}$, d. h. $m = (q-1)t$. Damit sind (5) und (6) bewiesen.

Da $mn = q^n - 1$ ist, ist die Ordnung von q (wir bezeichnen sie mit s) in der primen Restklassengruppe mod m ein Teiler von n. Aus $m \mid (q^s - 1)$ folgt $q^s - 1 \geqq m = \frac{q^n-1}{n}$ und hieraus $n \geqq 1 + q^s + \cdots + q^{s\left(\frac{n}{s}-1\right)}$. Für jede natürliche Zahl $q > 1$ ist stets $2s \leqq q^s$. Also gilt:

$$n \geqq 1 + q^s + \cdots + q^{s\left(\frac{n}{s}-1\right)} \geqq 1 + 2s\left(\frac{n}{s} - 1\right) = 1 + 2n - 2s,$$

d. h. $2s > n$. Dies ist wegen $s \mid n$ nur für $s = n$ möglich, also ist auch (7) richtig.

Für den Beweis der Relation (8) benötigen wir die folgenden Hilfssätze:

(10) *Ist p eine Primzahl mit $p|n$, so folgt $p|q-1$.*

Beweis. Es sei p ein Primteiler von n mit $p\nmid q-1$ und p^δ die höchste in n aufgehende p-Potenz. Aus $p|n$ und $n|q^n-1$ folgt $(p,q)=1$ und hieraus $q^{p^{\delta-1}(p-1)} \equiv 1 \bmod p^\delta$. Ist p_0 der größte Primteiler von n mit $p_0\nmid q-1$, so folgt $p_0\nmid p-1$ und daher $q^{\frac{n}{p_0}} \equiv 1 \bmod p^\delta$. Nach (3) ist ferner $q^n-1=\left(q^{\frac{n}{p_0}}-1\right)\left(1+q^{\frac{n}{p_0}}+\cdots+q^{\frac{n}{p_0}(p_0-1)}\right) \equiv 0 \bmod n$ $(q-1)$ und für jeden Primteiler r von $q-1$ gilt $r\nmid 1+q^{\frac{n}{p_0}}+\cdots+q^{\frac{n}{p_0}(p_0-1)}$. Daher folgt $q^{\frac{n}{p_0}} \equiv 1 \bmod n$ $(q-1)$, was (3) widerspricht.

(11) *Ist $q \equiv 3 \bmod 4$, so ist 4 kein Teiler von n.*

Für den Beweis von (11) dürfen wir voraussetzen, daß n gerade ist; 2^ν sei die höchste in n aufgehende 2-Potenz. Nach (10) gilt dann: Ist p ein Primteiler von n, so teilt p die Zahl $q^{\frac{n}{2}}-1$, aber, falls $p \neq 2$ ist, nicht $q^{\frac{n}{2}}+1$. Hieraus folgt, da $2^{\nu+1}$ (wegen $q \equiv 3 \bmod 4$) die höchste in $n(q-1)$ aufgehende 2-Potenz ist:

$$q^{\frac{n}{2}} \equiv 1 \bmod n(q-1)2^{-\nu-1}.$$

Ist $\nu > 1$ (d.h. 4 teilt n), so gilt außerdem $q^{\frac{n}{2}} \equiv 1 \bmod 2^{\nu+1}$ [6]). Für $\nu > 1$ folgt also $q^{\frac{n}{2}} \equiv 1 \bmod n(q-1)$. Da diese Kongruenz der Aussage (3) widerspricht, ist $\nu \leqq 1$, also 4 kein Teiler von n.

Nun folgt der Beweis von (8):

Es sei p ein Primteiler von $q-1$ und p^μ die höchste in $q-1$ aufgehende p-Potenz. Ist $p^\mu \neq 2$, so gilt $p\nmid t=\frac{q^n-1}{n(q-1)}$ [6]). Ist $p^\mu = 2$, so gilt $2|t$ genau dann, wenn n gerade ist. Also erhalten wir $(q-1,t) \leqq 2$ und es gilt $(q-1,t)=2$ genau dann, wenn $q \equiv 3 \bmod 4$ und n gerade

---

[6]) Wir benötigen hier den folgenden Hilfssatz: Ist p ein Primteiler von $q-1$ und p^μ bzw. p^ν die höchste in $q-1$ bzw. n aufgehende p-Potenz, so gilt

$$q^n-1 \equiv 0 \bmod p^{\mu+\nu}$$

und

$$q^n-1 \begin{cases} \not\equiv 0 \bmod p^{\mu+\nu+1} & \text{für } p^\mu \neq 2 \text{ oder für } \nu = 0, \\ \equiv 0 \bmod p^{\mu+\nu+1} & \text{für } p^\mu = 2 \text{ und } \nu \geqq 1. \end{cases}$$

ist (vgl. [6]). Hieraus folgt aber nach (10) und (11): $(n, t) = (q-1, t) \leqq 2$. Damit ist (8) und die folgende Aussage bewiesen:

(12) *Es gilt* $(n, t) = (q-1, t) = 2$ *genau dann, wenn* $n \equiv 2 \bmod 4$ *und* $q \equiv 3 \bmod 4$ *ist.*

Aus Satz 1 folgt, daß das Zentrum von $M^*(\circ)$ von a^t erzeugt wird, also eine Untergruppe von U ist und die Ordnung $\frac{m}{t} = q-1$ hat. Daher gilt:

(13) *Das Zentrum von* $M(+, \circ)$ *ist der Körper* K_q.

Definition 2. *Sind q und n zwei natürliche Zahlen, so heißt das Paar $\{q, n\}$ Dickson-Veblensches Zahlenpaar, wenn folgende Eigenschaften erfüllt sind:*

1. *q ist eine Primzahlpotenz;*
2. *Jeder Primteiler von n ist auch Teiler von $q-1$;*
3. *Ist $q \equiv 3 \bmod 4$, so gilt $n \not\equiv 0 \bmod 4$.*

Aus den bisherigen Ausführungen geht hervor (vgl. (10) und (11)), daß jedem Dickson-Veblenschen Fastkörper ein Dickson-Veblensches Zahlenpaar zugeordnet ist. Wir wollen jetzt die Umkehrung beweisen:

Satz 2. *Zu jedem Dickson-Veblenschen Zahlenpaar $\{q, n\}$ gibt es genau einen Dickson-Veblenschen Fastkörper $M(+, \circ)$ mit q^n Elementen, dessen Zentrum aus genau q Elementen besteht.*

Beweis. Es sei $M(+, \cdot)$ der endliche Körper mit q^n Elementen und ω eine Erzeugende von $M^*(\cdot)$. Auf Grund der Voraussetzungen von Satz 2 kann man zeigen (vgl. [10]), daß $0, 1, \frac{q^2-1}{q-1}, \ldots, \frac{q^{n-1}-1}{q-1}$ ein Repräsentantensystem mod n ist. Daher ist

$$M^*(\cdot) = U \cup U\omega \cup U\omega^{\frac{q^2-1}{q-1}} \cup \cdots \cup U\omega^{\frac{q^{n-1}-1}{q-1}}$$

eine Zerlegung von $M^*(\cdot)$ in Nebenklassen, wobei U die von ω^n erzeugte Untergruppe bezeichnet. Jedem Element $a \in M^*$ ordnen wir einen Automorphismus ϱ_a von $M(+, \cdot)$ zu: Ist $a \in U\omega^{\frac{q^\beta-1}{q-1}}$, so sei $\varrho_a : x \to x^{q^\beta}$. Definieren wir nun in M^* eine neue Multiplikation $\circ$ durch $a \circ b = a\varrho_a(b)$, so ist $M(+, \circ)$ der gesuchte Dickson-Veblensche Fastkörper.

Daß es zu einem Dickson-Veblenschen Zahlenpaar (bis auf Isomorphie) nur einen Dickson-Veblenschen Fastkörper gibt, läßt sich aus (4) und (9) folgern.

§ 2. Zyklische Normalteiler der multiplikativen Gruppe eines Dickson-Veblenschen Fastkörpers

Um die zyklischen Normalteiler der multiplikativen Gruppe eines Dickson-Veblenschen Fastkörpers zu bestimmen, beweisen wir zunächst:

Satz 3. *Es sei G eine Gruppe mit den Erzeugenden a, b, die den Relationen* (5), (6) *und* (7) *genügen. Erzeugt $a^\alpha b^\beta$ [7]) einen zyklischen Normalteiler von G, so gilt $q^\beta \equiv 1 \bmod t$.*

Beweis. $a^\alpha b^\beta$ erzeuge einen zyklischen Normalteiler. Dann ist das Element $a^{-1}(a^\alpha b^\beta)a = a^{q^\beta - 1}(a^\alpha b^\beta)$ in der Form $(a^\alpha b^\beta)^k = a^{\alpha(1+q^\beta+\cdots+q^{\beta(k-1)})} b^{k\beta}$ darstellbar. Hieraus folgen mit Hilfe von (5), (6) und (7) die Kongruenzen $\beta(k-1) \equiv 0 \bmod n$ und

$$q^\beta - 1 \equiv \alpha q^\beta \frac{q^{\beta(k-1)} - 1}{q^\beta - 1} \bmod t.$$

Da $\beta(k-1)$ durch n teilbar ist, ist $q^{\beta(k-1)} - 1$ nach (7) durch $m = (q-1)t$ teilbar. Also können wir die letzte Kongruenz auch in der Form

$$q^\beta - 1 \equiv \alpha \frac{\sigma(q-1)t}{q^\beta - 1} \bmod t. \tag{14}$$

schreiben.

Auch das Element $b(a^\alpha b^\beta)b^{-1} = a^{\alpha(q-1)} a^\alpha b^\beta$ ist in der Form $(a^\alpha b^\beta)^{k'}$ darstellbar. Hieraus erhält man entsprechend $\beta(k'-1) \equiv 0 \bmod n$ und

$$\alpha(q-1) \equiv \alpha \frac{\sigma'(q-1)t}{q^\beta - 1} \bmod t. \tag{15}$$

Es sei p ein Primteiler von t und p^τ, $p^{\alpha'}$, p^ϱ, $p^{\beta'}$ jeweils die höchste in $t, \alpha, q-1, q^\beta - 1$ aufgehende p-Potenz. Aus (14) und (15) erhält man dann:

$$p^{\beta'} \equiv p^{\alpha'+\varrho+\tau-\beta'} \sigma \bmod p^\tau \tag{16}$$

und

$$p^{\alpha'+\varrho} \equiv p^{\alpha'+\varrho+\tau-\beta'} \sigma' \bmod p^\tau. \tag{17}$$

Sollte $\tau - \beta' > 0$ sein, so würde aus (17) folgen $\alpha' + \varrho \geqq \tau$, d.h. $\alpha' + \varrho + \tau - \beta' \geqq \tau + (\tau - \beta') > \tau$. Hieraus und aus (16) ergibt sich aber $\beta' \geqq \tau$ im Widerspruch zu unserer Annahme $\tau > \beta'$. Also gilt $\beta' \geqq \tau$ und daher $q^\beta \equiv 1 \bmod p^\tau$. Diese Aussage ist aber für alle Primteiler p von t richtig. Also gilt $q^\beta \equiv 1 \bmod t$, w. z. b. w.

Wir wenden jetzt Satz 3 auf die multiplikative Gruppe $G = M^*(\circ)$ eines endlichen Dickson-Veblendschen Fastkörpers an. Hierzu nehmen wir an, daß $a^\alpha b^\beta$ einen zyklischen Normalteiler erzeugt. Nach (9) dürfen

[7]) Ist speziell G die multiplikative Gruppe eines Dickson-Veblenschen Fastkörpers, so verstehen wir hier unter x^y die Potenzbildung bezüglich der Operation $\circ$.

wir $0 \leqq \beta < n$ voraussetzen. Aus Satz 3 folgt dann $q^\beta \equiv 1 \bmod t$ und hieraus $q^\beta \equiv 1 \bmod \frac{(q-1)t}{(q-1,t)}$ oder nach (6) $q^\beta \equiv 1 \bmod \frac{m}{(q-1,t)}$. Auf Grund von (8) haben wir die zwei Fälle zu unterscheiden:

1. Ist $(n,t) = (q-1,t) = 1$, also $q^\beta \equiv 1 \bmod m$, so folgt nach (7) aber $n|\beta$, also $\beta = 0$, da $\beta < n$ vorausgesetzt war. Daher liegen alle zyklischen Normalteiler von $M^*(\circ)$ in $U = \{\bar{a}\}$.

2. Ist $(n,t) = (q-1,t) = 2$, also $q^\beta \equiv 1 \bmod \frac{m}{2}$, so folgt (wegen $2|q-1$) die Kongruenz $q^{2\beta} \equiv 1 \bmod m$. Wegen (7) gilt daher $n|2\beta$, d.h. $\beta = 0$ oder $\beta = \frac{n}{2}$, da $\beta < n$ ist. Aus $q^{\frac{n}{2}} \equiv 1 \bmod \frac{m}{2}$ folgt $\frac{m}{2} \leqq q^{\frac{n}{2}} - 1$, d.h. $\frac{q^n-1}{2n} \leqq q^{\frac{n}{2}} - 1$, da $mn = q^n - 1$ ist. Aus der letzten Ungleichung erhalten wir durch Umformen $q^{\frac{n}{2}} + 1 \leqq 2n$. Wegen $(n,t) = (q-1,t) = 2$ ist aber $n \geqq 2$ und $q \geqq 3$. Also ist die Ungleichung $q^{\frac{n}{2}} + 1 \leqq 2n$ nur für $q = 3$ und $n = 2$ richtig. Daher gilt: Ist $q \neq 3$ oder $n \neq 2$, so liegen alle zyklischen Normalteiler von $M^*(\circ)$ in $U = \{\bar{a}\}$. Ist $q = 3$ und $n = 2$, so folgt aus (5), daß $M^*(\circ)$ die Quaternionengruppe ist, da $|M^*| = q^n - 1 = 3^2 - 1 = 8$, $m = 4$ und $t = 2$ ist.

Zusammenfassend erhalten wir:

Satz 4. *Es sei $M(+,\circ)$ ein endlicher Dickson-Veblenscher Fastkörper. Ist $|M| \neq 9$, so sind die zyklischen Normalteiler von $M^*(\circ)$ genau die Untergruppen der zyklischen Gruppe $U = \{x \in M^*;\ \varrho_x = 1\}$. Ist $|M| = 9$ und $M(+,\circ)$ kein Körper, so ist $M^*(\circ)$ die Quaternionengruppe und jedes Element von $M^*(\circ)$ erzeugt einen zyklischen Normalteiler.*

§ 3. Normale Teilkörper endlicher Dickson-Veblenscher Fastkörper

Einen Fastkörper $M(+,\circ)$ haben wir *normal* über einem Teilkörper L genannt und L einen *normalen Teilkörper* von $M(+,\circ)$, wenn M ein Linksvektorraum über L ist und wenn $L^* \lhd M^*(\circ)$ gilt. Es sollen hier alle normalen Teilkörper L eines endlichen Dickson-Veblenschen Fastkörpers $M(+,\circ)$ bestimmt werden.

Hierzu beweisen wir:

Satz 5. *Es sei $M(+,\circ)$ ein endlicher Dickson-Veblenscher Fastkörper der Charakteristik p, $\{q,n\}$ das zugehörige Dickson-Veblensche Zahlenpaar, $U = \{x \in M^*;\ \varrho_x = 1\}$ und a eine Erzeugende von U. Dann gilt:*

I. *Ist L ein normaler Teilkörper von $M(+,\circ)$, so ist L^* eine Untergruppe von U, d.h. $|L^*|$ ist ein Teiler von $m = \frac{q^n-1}{n}$ und L^* wird erzeugt von a^s, wenn $s = \frac{q^n-1}{n|L^*|}$ ist.*

II. *Ist* $p^\sigma - 1$ *ein Teiler von* $m = \frac{q^n - 1}{n}$, *so gibt es genau einen normalen Teilkörper* L *von* $M(+, \circ)$ *mit* $|L| = p^\sigma$.

Beweis von I. Da L^* ein zyklischer Normalteiler von $M^*(\circ)$ ist, gilt $L^* \subset U$ nach Satz 4. Hieraus folgt, daß $|L^*|$ ein Teiler von $|U| = m = \frac{q^n - 1}{n}$ ist und daß L^* von a^s mit $s = \frac{q^n - 1}{n\,|L^*|}$ erzeugt wird.

Beweis von II. Wir setzen $s = \frac{m}{p^\sigma - 1}$, bezeichnen mit L^* die von a^s erzeugte Untergruppe von U und mit $L = L^* \cup \{0\}$. L hat genau p^s Elemente und ist hinsichtlich der Operationen $+$ und $\circ$ ein Körper, da U auch Untergruppe der multiplikativen Gruppe $M^*(\cdot)$ des Körpers $M(+, \cdot)$ ist und in U die Operationen $\cdot$ und $\circ$ übereinstimmen (vgl. (2)). Es gilt $L^* \lhd M^*(\circ)$, denn alle Untergruppen von U (vgl. Satz 4) sind Normalteiler. Schließlich ist $M(+, \circ)$ ein Linksvektorraum über L, denn aus (2) ergibt sich: Sind $\lambda, \mu \in L$ und $x \in M$, so gilt $\lambda + \mu \in L$ und $(\lambda + \mu) \circ x = (\lambda + \mu) \cdot x = \lambda \cdot x + \mu \cdot x = \lambda \circ x + \mu \circ x$. Also ist L ein normaler Teilkörper von $M(+, \circ)$. L ist eindeutig bestimmt, da L^* nach I. eine Untergruppe der zyklischen Gruppe U ist und U genau eine Untergruppe der Ordnung $p^\sigma - 1$ besitzt.

Nennen wir $\{p^{\tau n}, p^\tau, p^\sigma\}$ ein *normales Zahlentripel*, wenn $\{p^\tau, n\}$ ein Dickson-Veblensches Zahlenpaar und wenn $p^\sigma - 1$ ein Teiler von $\frac{p^{\tau n} - 1}{n}$ ist, so können wir Satz 5 auch die folgende Fassung geben:

Satz 5′. *Ist* (M, L) *ein endlicher normaler Dickson-Veblenscher Fastkörper und* K_q *das Zentrum von* M, *so ist* $\{|M|, |K_q|, |L|\}$ *ein normales Zahlentripel. Ist umgekehrt* $\{p^{\tau n}, p^\tau, p^\sigma\}$ *ein normales Zahlentripel, so gibt es genau einen normalen Dickson-Veblenschen Fastkörper* (M, L), *so daß* $|M| = p^{\tau n}$, $|L| = p^\sigma$ *ist und das Zentrum von* M *genau* p^τ *Elemente enthält.*

Aus Satz 5 soll eine Folgerung gezogen werden. Hierzu benötigen wir den Hilfssatz:

(18) *Es sei* $\{q, n\}$ *ein Dickson-Veblensches Zahlenpaar mit* $q = p^\tau$ (p *Primzahl*). *Ferner sei* σ *eine natürliche Zahl und* σ_0 *durch* $\sigma = \sigma_0(\sigma, \tau)$ *definiert.* $p^\sigma - 1$ *ist genau dann ein Teiler von* $m = \frac{q^n - 1}{n}$, *wenn* $\sigma_0 | n$ *und* $(\sigma_0, p^{(\sigma,\tau)} - 1) = 1$ *gilt.*

Beweis. Es gilt:

a) Jede der Zahlen $(p^{(\sigma,\tau)} - 1, \sigma_0)$, $(p^{(\sigma,\tau)} - 1,\ 1 + p^{(\sigma,\tau)} + \cdots + p^{(\sigma,\tau)(\sigma_0 - 1)})$ und $(p^\tau - 1,\ 1 + p^{(\sigma,\tau)} + \cdots + p^{(\sigma,\tau)(\sigma_0 - 1)})$ ist durch dieselben Primzahlen teilbar.

Zusammen mit (10) ergibt sich aus a):

b) Aus $(p^{(\sigma,\tau)}-1, \sigma_0) = 1$ folgt $(n, 1 + p^{(\sigma,\tau)} + \cdots + p^{(\sigma,\tau)(\sigma_0-1)} = 1$.

Die Zahl

$$\frac{p^{n\tau}-1}{p^{\sigma}-1} = \frac{p^{n\tau}-1}{(p^{(\sigma,\tau)}-1)(1+p^{(\sigma,\tau)}+\cdots+p^{(\sigma,\tau)(\sigma_0-1)})}$$

ist dann und nur dann ganz, wenn σ_0 ein Teiler von n ist. Sie ist, falls sie ganz ist, durch n teilbar, wenn $(p^{(\sigma,\tau)}-1, \sigma_0) = 1$ gilt; denn n ist ein Teiler von $\frac{p^{n\tau}-1}{p^{\tau}-1}$ (vgl. (6)) und wegen b) gilt

$$(n, 1 + p^{(\sigma,\tau)} + \cdots + p^{(\sigma,\tau)(\sigma_0-1)}) = 1.$$

Damit haben wir bewiesen: Aus $\sigma_0 | n$ und $(p^{(\sigma,\tau)}-1, \sigma_0) = 1$ folgt $p^{\sigma}-1 \Big| \frac{p^{n\tau}-1}{n}$.

Wir gehen nun von der Annahme aus, daß σ_0 ein Teiler von n, $p^{\sigma}-1$ ein Teiler von $m = \frac{p^{n\tau}-1}{n}$ und daß $(p^{(\sigma,\tau)}-1, \sigma_0) \neq 1$ ist. Es gilt:

c) Ist π ein Primteiler von $(p^{(\sigma,\tau)}-1, \sigma_0)$, so auch von $\frac{p^{\sigma}-1}{p^{(\sigma,\tau)}-1}$, und wegen $(p^{\sigma}-1, p^{\tau}-1) = p^{(\sigma,\tau)}-1$:

d) Aus $p^{\sigma}-1 | m$ folgt $\frac{p^{\sigma}-1}{p^{(\sigma,\tau)}-1} \Big| t = \frac{p^{n\tau}-1}{n(p^{\tau}-1)}$.

Aus unserer Annahme und auf Grund von c), d) und (8) erhalten wir: $(p^{(\sigma,\tau)}-1, \sigma_0) = (n, t) = 2$ und hieraus nach (12): $n \equiv q - 1 \equiv 2 \bmod 4$. Also sind $p^{\sigma}-1$ und $p^{n\tau}-1$ (wegen $\sigma = \sigma_0(\sigma, \tau)$) durch dieselbe 2-Potenz teilbar. Dann kann aber $m = \frac{p^{n\tau}-1}{n}$ (wegen $2|n$) nicht durch $p^{\sigma}-1$ teilbar sein im Widerspruch zu unserer Annahme.

Aus Satz 5 und (18) können wir jetzt folgern:

(19) *Ist L ein normaler Teilkörper von $M(+, \circ)$ und umfaßt L das Zentrum K_q von $M(+, \circ)$, so gilt $L = K_q$.*

Beweis. Es sei p die Charakteristik von $M(+, \circ)$, $|L| = p^{\sigma}$ und $q = p^{\tau}$. Dann folgt aus Satz 5, daß $p^{\sigma}-1$ ein Teiler von $m = \frac{q^n-1}{n}$ ist, und hieraus nach (18), daß $\sigma_0 | n$ und $(\sigma_0, p^{(\sigma,\tau)}-1) = 1$ gilt. Aus $K_q \subset L$ erhalten wir $\tau | \sigma$, d.h. $(\sigma, \tau) = \tau$. Also gelten wegen $p^{(\sigma,\tau)} = p^{\tau} = q$ die Aussagen $(\sigma_0, q-1) = 1$ und $\sigma_0 | n$. Zusammen mit (10) ergibt sich hieraus $\sigma_0 = 1$, d.h. $\sigma = \tau$, also $L = K_q$.

Mit Satz 5 sind alle normalen Teilkörper eines endlichen Dickson-Veblenschen Fastkörper $M(+, \circ)$ bestimmt. Die zentralen Teilkörper von $M(+, \circ)$ sind genau alle Teilkörper des Zentrums K_q. Gibt es in $M(+, \circ)$ auch normale Teilkörper L, die nicht zentral sind? Nach (19) wissen wir, daß L nicht das Zentrum K_q umfassen kann, sondern mit

K_q einen Durchschnitt besitzen muß, der in L und K_q echt enthalten ist. Mit Hilfe von (18) können wir für einen vorgegebenen endlichen Dickson-Veblenschen Fastkörper $M(+, \circ)$ alle normalen Teilkörper L, die nicht zentral sind, angeben.

Die jeweils kleinsten normalen Dickson-Veblenschen Fastkörper (M, L) der Ränge 2, 3 und 4, für die L nicht zentral ist, sind durch die folgenden normalen Zahlentripel $\{p^{\tau n}, p^{\tau}, p^{\sigma}\}$ gegeben (vgl. Satz 5′ und (18)):

$$\text{Rang } [M : L] = 2 : \{2^{2\cdot 3}, 2^2, 2^3\},$$
$$\text{Rang } [M : L] = 3 : \{2^{3\cdot 7}, 2^3, 2^7\},$$
$$\text{Rang } [M : L] = 4 : \{2^{4\cdot 3}, 2^4, 2^3\}.$$

§ 4. Bestimmung der endlichen desarguesschen Inzidenzgruppen

Nachdem wir im letzten Paragraphen alle endlichen normalen Fastkörper (M, L) mit Rang $[M : L] > 2$ angegeben haben, sind wir jetzt in der Lage alle endlichen desarguesschen Inzidenzgruppen zu bestimmen. Auf Grund der Erörterungen in der Einleitung wissen wir nämlich, daß wir jede desarguessche Inzidenzgruppe G als Faktorgruppe F^*/K^* erhalten können, wobei (F, K) ein normaler Fastkörper mit Rang $[F : K] > 2$ ist. Wir brauchen also nur die in den vorhergegangenen Paragraphen gewonnenen algebraischen Resultate in eine geometrische Sprechweise zu übersetzen.

Es sei (M, L) ein normaler Dickson-Veblenscher Fastkörper mit Rang $[M : L] > 2$ und $\{|M|, |K_q|, |L|\} = \{p^{\tau n}, p^{\tau}, p^{\sigma}\}$ das zugehörige normale Zahlentripel (vgl. Satz 5′). Da der Rang $[M : L] > 2$ ist, gilt $3\sigma \leqq \tau n$. Sind a und b die durch Satz 1 beschriebenen Erzeugenden von $M^*(\circ)$, so wird L^* nach Satz 5 von a^s mit $s = \frac{q^n - 1}{n|L^*|} = \frac{p^{\tau n} - 1}{n(p^{\sigma} - 1)}$ erzeugt. Infolgedessen wird die Gruppe $M^*(\circ)/L^*$, die die Mächtigkeit $\frac{p^{\tau n} - 1}{p^{\sigma} - 1}$ hat, von den zwei Elementen $A = L^*a$ und $B = L^*b$ erzeugt, die auf Grund von Satz 1 den folgenden Relationen genügen:

$$A^s = 1, \quad B^n = A^t, \quad BAB^{-1} = A^q$$
$$\text{mit} \quad s = \frac{p^{\tau n} - 1}{n(p^{\sigma} - 1)}, \quad t = \frac{p^{\tau n} - 1}{n(p^{\tau} - 1)} \quad \text{und} \quad q = p^{\tau}. \tag{20}$$

Also gilt:

Satz 6. *Jeder endlichen desarguesschen Inzidenzgruppe G entspricht genau ein normales Zahlentripel $\{p^{\tau n}, p^{\tau}, p^{\sigma}\}$ mit $\tau n \geqq 3\sigma$, so daß gilt: G besitzt zwei Erzeugende A und B, die den Relationen (20) genügen und G hat die Ordnung $\frac{p^{\tau n} - 1}{p^{\sigma} - 1}$. Ist umgekehrt $\{p^{\tau n}, p^{\tau}, p^{\sigma}\}$ ein normales Zahlentripel mit $\tau n \geqq 3\sigma$, so gibt es genau eine endliche Inzidenzgruppe G der*

Ordnung $\frac{p^{\tau n}-1}{p^{\sigma}-1}$ *mit zwei Erzeugenden A und B, die den Relationen* (20) *genügen.*

Der zweite Teil von Satz 6 folgt sofort aus dem zweiten Teil von Satz 5.

Mit Satz 6 sind also alle endlichen desarguesschen Inzidenzgruppen bestimmt.

Welche der endlichen Inzidenzgruppen G sind linear, welche nicht linear? Aus der Einleitung wissen wir, daß G genau dann *linear* ist, wenn in dem zu G gehörigen normalen Fastkörper (M, L) der Teilkörper L sogar *zentral* ist, wenn also $L \subset K_q$ gilt (vgl. § 3). Ist $|L| = p^{\sigma}$ und $|K_q| = q = p^{\tau}$, so ist $L \subset K_q$ gleichbedeutend mit $p^{\sigma} - 1 | p^{\tau} - 1$, d.h. mit $\sigma | \tau$. Hieraus erhalten wir:

Satz 7. *Eine endliche desarguessche Inzidenzgruppe G mit dem normalen Zahlentripel $\{p^{\tau n}, p^{\tau}, p^{\sigma}\}$* (vgl. Satz 6) *ist genau dann linear, wenn $\sigma | \tau$ gilt.*

Da es normale Dickson-Veblensche Fastkörper (M, L) gibt, für die L nicht zentral ist (vgl. § 3), existieren auch endliche nichtlineare Inzidenzgruppen.

Aus (20) erkennt man, daß eine endliche desarguessche Inzidenzgruppe G mit dem normalen Zahlentripel $\{p^{\tau n}, p^{\tau}, p^{\sigma}\}$ genau dann kommutativ ist, wenn $q - 1 = p^{\tau} - 1$ durch $s = \frac{p^{\tau n}-1}{n(p^{\sigma}-1)}$ teilbar ist. Hieraus folgt $n(p^{\sigma} - 1)(p^{\tau} - 1) \geqq p^{\tau n} - 1$. Diese Ungleichung ist aber wegen $\tau n \geqq 3\sigma$ nur für $n = 1$ richtig. $n = 1$ hat $t = 1$ und $s = \frac{p^{\tau}-1}{p^{\sigma}-1}$ zur Folge, d.h. G ist eine zyklische Gruppe. Da das normale Zahlentripel von G die Gestalt $\{p^{\tau}, p^{\tau}, p^{\sigma}\}$ hat, ist für den zu G korrespondierenden normalen Fastkörper (M, L) das Zentrum $K_{p^{\tau}}$ von M gleich M, d.h. M ist ein kommutativer Körper. Damit haben wir bewiesen:

Satz 8. *Jede endliche kommutative desarguessche Inzidenzgruppe ist zyklisch und der zugehörige normale Fastkörper (M, L) ist kommutativ*[8]*.*

§ 5. Genau einfach transitive Kollineationsgruppen eines endlichen projektiven Raumes

Ist ein endlicher projektiver desarguesscher Raum Π vorgegeben, so kann man die Aufgabe stellen, alle scharf einfach transitiv operierenden Kollineationsgruppen von Π zu finden. Mit Hilfe der bisher erhaltenen

[8]) Dieses Resultat folgt auch aus [5] und [6]. Dort ist allgemein bewiesen worden, daß jeder desarguesschen kommutativen Inzidenzgruppe G ein kommutativer normaler Fastkörper (F, K) entspricht, d.h. F und damit auch K sind kommutative Körper.

Resultate ist es leicht eine Lösung anzugeben. Wie in der Einleitung bemerkt wurde, ist der Begriff einer auf einem projektiven Raum Π scharf einfach transitiv operierenden Kollineationsgruppe G gleichwertig mit dem Begriff der Inzidenzgruppe. Da ein endlicher desarguesscher projektiver Raum Π durch die Anzahl seiner Punkte vollständig festgelegt ist, ist die gestellte Aufgabe also gleichwertig mit dem Problem, alle Inzidenzgruppen G zu bestimmen, deren Ordnung gleich der Anzahl der Punkte von Π ist.

Die Anzahl der Punkte von Π sei $1 + p^\sigma + \cdots + p^{\sigma(\delta-1)} = \frac{p^{\sigma\delta}-1}{p^\sigma-1}$. Ist G eine desarguessche endliche Inzidenzgruppe mit dem normalen Zahlentripel $\{\tilde{p}^{\tau n}, \tilde{p}^\tau, \tilde{p}^{\tilde{\sigma}}\}$ (vgl. Satz 6), so gilt $|G| = \frac{\tilde{p}^{\tau n}-1}{\tilde{p}^{\tilde{\sigma}}-1}$. Die Zahlen $\frac{p^{\sigma\delta}-1}{p^\sigma-1}$ und $\frac{\tilde{p}^{\tau n}-1}{\tilde{p}^{\tilde{\sigma}}-1}$ sind genau dann gleich, wenn $\tilde{p} = p$, $\tilde{\sigma} = \sigma$ und $\tau n = \sigma\delta$ gilt. Bezeichnen wir mit $\Phi(p, \sigma, \delta)$ die Menge der in τ und n positiv ganzzahligen Lösungen der Gleichung $\tau n = \sigma\delta$ mit der Nebenbedingung, daß $\{p^\tau, n\}$ ein Dicksonsches Zahlenpaar (vgl. Definition 2) ist, so gilt (vgl. Satz 6):

Satz 9. *Ist Π ein endlicher desarguesscher projektiver Raum, dessen Dimension größer als 1 ist, und ist $\frac{p^{\sigma\delta}-1}{p^\sigma-1}$ (p Primzahl) die Anzahl der Punkte von Π, so besitzt Π genau $|\Phi(p, \sigma, \delta)|$ nicht isomorphe genau einfach transitive Kollineationsgruppen. Zu jeder Lösung $\{\tau, n\}$ aus $\Phi(p, \sigma, \delta)$ gibt es genau eine genau einfach transitiv operierende Kollineationsgruppe G von Π, die durch das normale Zahlentripel (vgl. Satz 6) $\{p^{\tau n}, p^\tau, p^\sigma\}$ bestimmt ist.*

Die Menge $\Phi(p, \sigma, \delta)$ ist nicht leer, denn $\{\tau, n\} = \{\sigma\delta, 1\}$ liegt stets in $\Phi(p, \sigma, \delta)$. Dieser Lösung entspricht die zyklische Kollineationsgruppe.

§ 6. Transitivität der Hyperebenen

Zum Abschluß soll noch gezeigt werden, daß die Linkstranslationen einer endlichen Inzidenzgruppe G genau einfach transitiv auf den Hyperebenen von G operieren. Zu diesem Zweck denken wir uns eine Hyperebene H der Inzidenzgruppe G ausgezeichnet (jede Hyperebene fassen wir im folgenden stets als die Gesamtheit der mit ihr inzidierenden Punkte auf). $\mathfrak{M} = \{xH;\ x \in G\}$ sei die Menge aller Hyperebenen, die durch Linkstranslationen aus H hervorgehen und m die Kardinalzahl von $\mathfrak{M}$. Da die Gruppe der Linkstranslationen transitiv auf den Punkten von G operiert, inzidieren mit jedem Punkt von G gleich viele Hyperebenen aus $\mathfrak{M}$, deren Anzahl wir mit r bezeichnen. Ist $1 + n + \cdots + n^k$ die Ordnung der Inzidenzgruppe G, so liegen auf jeder Hyper-

ebene genau $1 + n + \cdots + n^{k-1}$ Punkte aus G. Demnach erhalten wir:

$$m = \frac{r(1 + n + \cdots + n^k)}{1 + n + \cdots + n^{k-1}} \leqq 1 + n + \cdots + n^k.$$

Da m eine natürliche Zahl $\leqq 1 + n + \cdots + n^k$ ist und die Zahlen $1 + n + \cdots + n^k$ und $1 + n + \cdots + n^{k-1}$ teilerfremd sind, folgt hieraus $r = 1 + n + \cdots + n^{k-1}$ und $m = 1 + n + \cdots + n^k$. Also liegen bereits alle Hyperebenen in $\mathfrak{M}$, d.h. die Linkstranslationen operieren genau einfach transitiv auf den Hyperebenen von G.

Aus diesem Ergebnis folgt (vgl. [2] Satz 4), daß jede endliche Inzidenzgruppe sogar als Gruppenraum $D(G)$ darstellbar ist, wobei wir unter einem *Gruppenraum* $D(G)$ eine Gruppe G verstehen, in der eine Teilmenge D so ausgezeichnet ist, daß die wie folgt definierte geometrische Struktur ein projektiver Raum ist: Jedes Element $x \in G$ fassen wir gleichzeitig als Punkt x und als Hyperebene $\langle x \rangle$ auf und erklären die Inzidenz zwischen einer Hyperebene $\langle x \rangle$ und einem Punkt y durch $xy \in D$. Also kennen wir mit allen endlichen desarguesschen Inzidenzgruppen auch alle endlichen desarguesschen Gruppenräume.

Literatur

[1] E. Ellers und H. Karzel, Involutorische Geometrien. Abh. Math. Sem. Univ. Hamburg 25 (1961) 93—104.

[2] —, Kennzeichnung elliptischer Gruppenräume. Abh. Math. Sem. Univ. Hamburg 26 (1963) 55—77.

[3] M. Hall, Cyclic projective planes. Duke Math. J. 14 (1947) 1079—1090.

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

[5] —, Kommutative Inzidenzgruppen. Arch. Math. 13 (1962) 535—538.

[6] —, Ebene Inzidenzgruppen. Arch. Math. 15 (1964) 10—17.

[7] L. A. Rosati, Piani proiettivi desarguesiani non ciclici. Boll. U. M. I. 12 (1957) 230—240.

[8] J. Singer, A theorem in finite projective geometry and some applications to number theory. Trans. Amer. Math. Soc. 43 (1938) 377—385.

[9] G. Zappa, Sui piani grafici finiti transitivi e quasi-transitivi. Ric. Mat. Napoli 2 (1953) 274—287.

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

Eingegangen am 24. 10. 1963