DEMBOWSKI, H. P.
Math. Zeitschr. Bd. 69, S. 59—89 (1958)

Verallgemeinerungen von Transitivitätsklassen endlicher projektiver Ebenen

Von
PETER DEMBOWSKI

Inhalt

Einleitung

Eine Gruppe von Kollineationen einer endlichen projektiven Ebene zerlegt sowohl die Menge der Punkte als auch die der Geraden in Transitivitätsklassen. Man überzeugt sich leicht, daß für jede solche Punktklasse $\mathfrak{P}$ und jede solche Geradenklasse $\mathfrak{g}$ gilt:

$$(*)\quad \begin{cases} \text{Auf jeder Geraden von } \mathfrak{g} \text{ liegen gleichviele Punkte von } \mathfrak{P}. \\ \text{Durch jeden Punkt von } \mathfrak{P} \text{ gehen gleichviele Geraden von } \mathfrak{g}. \end{cases}$$

Bei vielen Untersuchungen über Kollineationsgruppen endlicher projektiver Ebenen werden nun andere als diese Eigenschaften gar nicht benutzt; andererseits gibt es Klasseneinteilungen endlicher Ebenen mit den Eigenschaften (*), die nicht von einer Kollineationsgruppe herrühren. Es liegt daher nahe, allgemein Zerlegungen mit den Eigenschaften (*) zu untersuchen. Das wird in der vorliegenden Arbeit unternommen: Klasseneinteilungen der fraglichen Art nennen wir „taktische Zerlegungen".

Es zeigt sich, daß die für die Untersuchung fundamentalen Gleichungen („Grundgleichungen", S. 64) ohne Schwierigkeit für allgemeinere Strukturen

als endliche projektive Ebenen hergeleitet werden können, nämlich für die (endlichen) „λ-Ebenen", in denen je zwei Punkte λ Verbindungsgeraden und je zwei Geraden λ Schnittpunkte besitzen. Für diese Strukturen sind in der Literatur auch die Bezeichnungen „symmetrischer Blockplan" (PICKERT [12], S. 228), „symmetric block design" (HALL [7], S. 61) und „(v, k, λ)-configuration" (CHOWLA und RYSER [6], S. 93) üblich. Nur ausnahmsweise werden wir uns hier auf den Fall $\lambda = 1$ der endlichen projektiven Ebenen beschränken.

Das wesentliche Ergebnis des ersten Teiles der Arbeit ist der aus den Grundgleichungen leicht folgende Satz, daß die Anzahl der Punktklassen einer taktischen Zerlegung einer λ-Ebene gleich der ihrer Geradenklassen ist. Aus diesem Satz folgen viele Transitivitätseigenschaften von Kollineationsgruppen von λ-Ebenen; insbesondere ergeben sich Verallgemeinerungen von Resultaten von HALL und HOFFMAN (man vergleiche etwa [12], S. 304, 308) über zyklische Kollineationsgruppen endlicher projektiver Ebenen auf beliebige Gruppen und beliebige λ-Ebenen. Weiter läßt sich zeigen, daß eine Kollineationsgruppe einer λ-Ebene genau dann zweifach transitiv bezüglich der Punkte ist, wenn sie diese Eigenschaft auch bezüglich der Geraden hat.

Unter den Klassen einer taktischen Zerlegung Γ einer λ-Ebene $\mathfrak{E}$ läßt sich auf natürliche Weise eine Inzidenzrelation einführen, bezüglich welcher sie zu den Elementen einer neuen geometrischen Struktur werden, der „abgeleiteten Struktur $\mathfrak{E}/\Gamma$". Diese Struktur wird im zweiten Teile der Arbeit untersucht; insbesondere behandeln wir die naheliegende Frage, wann $\mathfrak{E}/\Gamma$ eine endliche projektive Ebene ist. Es zeigt sich überraschenderweise, daß das nur in dem trivialen Fall eintreten kann, daß $\lambda = 1$ (also $\mathfrak{E}$ selbst eine projektive Ebene) und Γ diejenige Zerlegung ist, deren sämtliche Klassen aus je einem Element bestehen. Auch wenn $\mathfrak{E}/\Gamma$ eine ausgeartete projektive Ebene ist, folgt $\lambda = 1$, vorausgesetzt, daß die Anzahl gleichartiger Γ-Klassen mindestens gleich vier ist. Die taktischen Zerlegungen, die solche abgeleitete Strukturen erzeugen, sind dadurch charakterisiert, daß eine ihrer Klassen aus n^2 Elementen besteht (n ist die Ordnung von $\mathfrak{E}$). Ist die Anzahl gleichartiger Klassen kleiner als vier, so gelten die Resultate nicht mehr allgemein. Gegenbeispiele erhält man unter anderen durch Betrachtung von Teilebenen und Ovalen endlicher projektiver Ebenen.

Durch jede taktische Zerlegung einer λ-Ebene werden in natürlicher Weise gewisse ganzzahlige Matrizen definiert, die im Falle der trivialen Zerlegung in lauter Klassen mit je einem Element gleich den bekannten Inzidenzmatrizen der Ebene sind. Aus den Grundgleichungen folgen leicht entsprechende Beziehungen zwischen diesen Matrizen („Matrix-Grundgleichungen", S. 80); die Untersuchung dieser Beziehungen bildet den Gegenstand des letzten Teiles der Arbeit. Es ergeben sich für die Existenz von taktischen Zerlegungen notwendige zahlentheoretische Bedingungen, die mit Hilfe verschiedener Methoden gewonnen werden. Aus einer elementaren Rangbetrachtung folgen zunächst Aussagen über die Anzahlen von Fixelementen von p-Gruppen von Kollineationen; z.B. kann die Anzahl der Fixpunkte einer projektiven Ebene bezüglich einer solchen Gruppe nur dann von der der Fixgeraden verschieden

sein, wenn p ein Teiler der Ordnung n der Ebene ist. Das wesentliche Hilfsmittel bei der weiteren Untersuchung ist die von HASSE und MINKOWSKI stammende Theorie der rationalen Kongruenz von quadratischen Formen. Der Hauptsatz dieser Theorie liefert mit den Matrixgleichungen eine fundamentale Beziehung zwischen Produkten von Hilbert-Symbolen [Gln. (H), S. 84], in die außer den Invarianten n und λ der gegebenen λ-Ebene noch die Anzahl der Γ-Klassen sowie die Anzahlen der Elemente der Γ-Klassen eingehen. Diese Beziehung enthält alle bisher bekannten Nichtexistenzsätze für endliche projektive Ebenen, insbesondere also den bekannten Satz von BRUCK und RYSER ([4], theorem 1, S. 88), aber auch die von CHOWLA und RYSER in [6] gegebenen Verallgemeinerungen auf λ-Ebenen. Sie liefert aber noch mehr; z.B. folgt die Nichtexistenz von nichttrivialen taktischen Zerlegungen mit lauter gleichmächtigen Klassen in vielen λ-Ebenen, z.B. in projektiven Ebenen der Ordnung 10.

Die Ergebnisse der vorliegenden Arbeit werden mit wenigen Ausnahmen durch ganz elementare Schlußweisen gewonnen, nämlich durch die für die Untersuchung endlicher Strukturen typischen abzählenden Methoden. Lediglich im letzten Abschnitt werden tieferliegende zahlentheoretische Hilfsmittel benutzt. Andererseits hat die hier entwickelte Theorie selbst interessante rein zahlentheoretische Konsequenzen: man kann mit ihrer Hilfe leicht mehrere Aussagen über die quadratischen Restcharaktere der Teiler von Zahlen des Typs $p^{2r}+p^r+1$ gewinnen.

Es sei hier erwähnt, daß einige Resultate des letzten Abschnittes der Arbeit kürzlich auch von D. R. HUGHES in [10] angekündigt worden sind.

Herrn Professor BAER, von dem die Anregung zu der Beschäftigung mit dem vorliegenden Problemkreis ausgegangen ist, bin ich für viele wertvolle Ratschläge und Hinweise zu großem Dank verpflichtet.

1. Taktische Zerlegungen von λ-Ebenen

1.1. Grundbegriffe

Unter einer *verallgemeinerten Inzidenzstruktur* verstehen wir ein Tripel $(\mathfrak{P}, \mathfrak{G}, I)$ von Mengen mit den Eigenschaften $\mathfrak{P} \cap \mathfrak{G} = \emptyset$, $I \subseteq \mathfrak{P} \times \mathfrak{G}$. Die Elemente von $\mathfrak{P}$ heißen *Punkte*, die von $\mathfrak{G}$ *Geraden*. Punkte werden stets mit großen, Geraden mit kleinen lateinischen Buchstaben bezeichnet. Ein Paar (P, g) von $\mathfrak{P} \times \mathfrak{G}$ heißt *inzident* oder *nichtinzident*, je nachdem ob es zu I gehört oder nicht. Statt $(P, g) \in I$ schreiben wir auch $P I g$ oder $g I P$, und diesen Sachverhalt drücken wir auch durch die Redeweisen „P liegt auf g", „g geht durch P" usw. aus.

Eine Gerade, die durch zwei verschiedene Punkte P und Q geht, heißt eine *Verbindungsgerade* von P und Q, ein Punkt, der auf zwei verschiedenen Geraden g und h liegt, ein *Schnittpunkt* von g und h. Im allgemeinen brauchen Schnittpunkte und Verbindungsgeraden vorgegebener Elementepaare weder zu existieren noch eindeutig zu sein. (Bei den von PICKERT in [12], S. 2 so bezeichneten „Inzidenzstrukturen" schlechthin wird Eindeutigkeit von Schnitt und Verbindung gefordert.)

In dieser Arbeit werden nur *endliche* verallgemeinerte Inzidenzstrukturen betrachtet, d.h. solche, bei denen $\mathscr{P}$ und $\mathscr{G}$ und damit auch I endliche Mengen sind. Die Attribute „endlich" und „verallgemeinert" werden wir künftig meist weglassen; das Wort „Inzidenzstruktur" soll aber niemals in dem Pickertschen, sondern stets in dem oben erklärten weiteren Sinne verstanden werden. Manchmal werden wir noch kürzer einfach „Struktur" sagen.

Eine Inzidenzstruktur heißt (nach CARMICHAEL [5]) *taktische Konfiguration*, wenn $|I \cap (P \times \mathscr{G})|$ für jeden Punkt P gleich derselben Zahl r und dual dazu $|I \cap (\mathscr{P} \times g)|$ für jede Gerade g gleich derselben Zahl k ist, d.h. wenn durch jeden Punkt genau r Geraden gehen und auf jeder Geraden genau k Punkte liegen. Dabei dürfen r und k durchaus auch gleich Null sein. Eine einfache Abzählung von $|I|$ ergibt

$$k\,|\mathscr{G}| = r\,|\mathscr{P}| \tag{1}$$

für jede taktische Konfiguration.

Unter einer *taktischen Zerlegung* einer endlichen verallgemeinerten Inzidenzstruktur $(\mathscr{P}, \mathscr{G}, I)$ verstehen wir eine Klasseneinteilung von $\mathscr{P} \cup \mathscr{G}$ in Punkt- und Geradenklassen (keine Klasse soll Punkte *und* Geraden enthalten) derart, daß für jedes Paar $\mathfrak{P}, \mathfrak{g}$ ungleichartiger Klassen die durch $I' = (\mathfrak{P} \times \mathfrak{g}) \cap I$ definierte Teilstruktur $(\mathfrak{P}, \mathfrak{g}, I')$ von $(\mathscr{P}, \mathscr{G}, I)$ eine taktische Konfiguration wird. Punktklassen taktischer Zerlegungen werden stets durch große, Geradenklassen durch kleine deutsche Buchstaben bezeichnet, und die bei (1) eingeführten Zahlen r und k werden für die durch eine taktische Zerlegung definierte taktische Konfiguration $(\mathfrak{P}, \mathfrak{g}, I')$ mit $(\mathfrak{g}\,\mathfrak{P})$ bzw. $(\mathfrak{P}\,\mathfrak{g})$ bezeichnet, d.h. auf jeder Geraden der Klasse $\mathfrak{g}$ liegen $(\mathfrak{P}\,\mathfrak{g})$ Punkte der Klasse $\mathfrak{P}$, und durch jeden Punkt der Klasse $\mathfrak{P}$ gehen $(\mathfrak{g}\,\mathfrak{P})$ Geraden der Klasse $\mathfrak{g}$.

Die Bedeutung des Begriffes der taktischen Zerlegung beruht auf dem nachfolgenden Satz 1. Wir definieren zunächst: Eine *Kollineation* einer Inzidenzstruktur $(\mathscr{P}, \mathscr{G}, I)$ ist eine Permutation σ von $\mathscr{P} \cup \mathscr{G}$ mit $\mathscr{P}^\sigma = \mathscr{P}$, $\mathscr{G}^\sigma = \mathscr{G}$, $I^\sigma = I$. Dabei ist unter $(P, g)^\sigma$ natürlich das Paar (P^σ, g^σ) zu verstehen. Die sämtlichen Kollineationen von $(\mathscr{P}, \mathscr{G}, I)$ bilden eine Gruppe; jede Untergruppe dieser Gruppe heißt eine *Kollineationsgruppe* von $(\mathscr{P}, \mathscr{G}, I)$.

Satz 1. *Die Ttransitivitätsklassen jeder Kollineationsgruppe einer beliebigen endlichen verallgemeinerten Inzidenzstruktur bilden eine taktische Zerlegung.*

Beweis. Zunächst ist klar, daß die Transitivitätsklassen (oder „Transitivitätsgebiete" oder „Transitivitätsbereiche"; für die Definition dieses und anderer Begriffe aus der Theorie der Permutationsgruppen vergleiche man etwa WIELANDT [15]) entweder nur Punkte oder nur Geraden enthalten. Sei $\mathfrak{P}$ eine Punkttransitivitätsklasse und $\mathfrak{g}$ eine Geradentransitivitätsklasse. Wir müssen zeigen, daß die von $\mathfrak{P}$ und $\mathfrak{g}$ gebildete Teilstruktur eine taktische Konfiguration ist. Dazu genügt es aus Dualitätsgründen, zu beweisen, daß jede Gerade von $\mathfrak{g}$ gleichviele Punkte von $\mathfrak{P}$ trägt. Das aber folgt sofort aus der für alle Kollineationen σ gültigen trivialen Tatsache, daß m Punkte $P_1, P_2, \ldots, P_m$ genau dann auf einer Geraden g liegen, wenn ihre Bilder $P_1^\sigma, P_2^\sigma, \ldots, P_m^\sigma$ auf g^σ liegen.

In der vorliegenden Arbeit werden taktische Zerlegungen einer speziellen Klasse von Inzidenzstrukturen untersucht, die wir jetzt definieren: Eine *λ-Ebene* ist eine taktische Konfiguration $\mathfrak{E} = (\mathscr{P}, \mathscr{G}, I)$ mit $r = k \neq 0$ sowie

$$|I \cap (P \times \mathscr{G}) \cap (Q \times \mathscr{G})| = \lambda < k$$

für jedes Paar verschiedener Punkte P, Q. Die Gesamtzahl der Punkte von $\mathfrak{E}$, die wegen (1) und $r = k$ auch gleich der der Geraden ist, wird mit v bezeichnet. Man kann zeigen (vgl. etwa [12], S. 288), daß für jede λ-Ebene weiterhin

$$|I \cap (\mathscr{P} \times g) \cap (\mathscr{P} \times h)| = \lambda$$

gilt; in einer λ-Ebene haben je zwei verschiedene Punkte also genau λ Verbindungsgeraden und je zwei verschiedene Geraden genau λ Schnittpunkte. Ferner besteht die Beziehung

$$k(k-1) = \lambda(v-1). \tag{2}$$

Unter der *Ordnung* einer λ-Ebene $\mathfrak{E}$ verstehen wir die Zahl $n = k - \lambda$. Im Falle $n = 1$ ist die Struktur von $\mathfrak{E}$ durch die Angabe von v eindeutig bestimmt: aus (2) folgt $k = v - 1$ und $\lambda = v - 2$, und die Punkte und Geraden lassen sich so numerieren, daß $I = \mathscr{P} \times \mathscr{G} - \{(P_1, g_1), (P_2, g_2), \ldots, (P_v, g_v)\}$ wird. Wir wollen daher den Fall $n = 1$ von nun an ausschließen und unter einer λ-Ebene stets eine solche mit $n \geq 2$ verstehen. Es gilt sodann stets $0 < \lambda < k - 1 < v - 1$. Aus (2) folgt weiter die später benötigte Beziehung

$$k^2 = (n + \lambda)^2 = n + \lambda v. \tag{3}$$

Wir bemerken noch, daß die λ-Ebenen mit $\lambda = 1$ gerade die (nichtausgearteten) endlichen projektiven Ebenen sind.

Jede λ-Ebene besitzt taktische Zerlegungen, nämlich einmal die, deren sämtliche Klassen aus je einem Element bestehen, und zum anderen die aus nur zwei Klassen (der aller Punkte und der aller Geraden) bestehende Zerlegung. Diese beiden Typen von taktischen Zerlegungen wollen wir *triviale Zerlegungen* nennen.

Man könnte meinen, daß jede taktische Zerlegung gemäß Satz 1 von einer Kollineationsgruppe erzeugt wird. Daß das nicht der Fall ist, zeigt schon das Beispiel der trivialen Zerlegung mit nur zwei Klassen bei einer endlichen projektiven Ebene über einem echten Fastkörper. Jede solche Ebene besitzt nämlich eine ausgezeichnete Gerade, für die als Achse der kleine Satz des DESARGUES gilt; diese Gerade muß bei jeder Kollineation festbleiben, da die Ebene sonst — nach HALL [7], S. 25 — eine Moufang-Ebene (Definition in [12], S. 186), also wegen der Endlichkeit sogar desarguessch und somit keine Ebene über einem *echten* Fastkörper wäre. Aber auch nichttriviale taktische Zerlegungen brauchen nicht von Kollineationsgruppen herzurühren, wie folgendes Beispiel zeigt: Es sei $\mathfrak{E}$ eine beliebige nicht-desarguessche endliche projektive Ebene der Ordnung n, ferner (Z, a) ein inzidentes Paar von $\mathfrak{E}$ derart, daß $\mathfrak{E}$ nicht (Z, a)-transitiv ist. (Vgl. BAER [1]. Ein solches Paar existiert

immer, da die Ebene sonst desarguessch wäre.) Wir numerieren die Punkte $\neq Z$ von a und die Geraden $\neq a$ durch Z irgendwie von 1 bis n: $P_1, P_2, \ldots, P_n$; $g_1, g_2, \ldots, g_n$ und definieren folgende Punkt- und Geradenklassen: $\mathfrak{P}_i = \{P_i\}$, $\mathfrak{g}_i = \{g_i\}$, $\mathfrak{P}_{n+i} = \{\text{Punkte} \neq Z \text{ von } g_i\}$, $\mathfrak{g}_{n+i} = \{\text{Geraden} \neq a \text{ durch } P_i\}$, $i = 1, 2, \ldots, n$; und $\mathfrak{P}_{2n+1} = \{Z\}$, $\mathfrak{g}_{2n+1} = \{a\}$. Man verifiziert ohne Schwierigkeit, daß so eine taktische Zerlegung von $\mathfrak{E}$ definiert wird. Diese kann aber nicht von einer Kollineationsgruppe herrühren, denn eine solche müßte aus zentralen Kollineationen mit Zentrum Z und Achse a bestehen und transitiv auf den Punkten $\neq Z$ jeder der Geraden g_i sein. Das aber würde heißen, daß die Ebene doch (Z, a)-transitiv wäre, entgegen unserer Voraussetzung.

Im folgenden bezeichnen wir taktische Zerlegungen meist durch das Symbol Γ, dementsprechend reden wir auch von den „Γ-Klassen" einer λ-Ebene. Für den Fall, daß die Zerlegung gemäß Satz 1 von einer Kollineationsgruppe herrührt, werden wir das Symbol Γ auch zur Bezeichnung dieser Gruppe verwenden; das wird nirgends zu Mißverständnissen führen.

1.2. Die Grundgleichungen

Es sei nun eine beliebige taktische Zerlegung einer beliebigen λ-Ebene der Ordnung n gegeben. Wir wollen eine Anzahl von Beziehungen herleiten, die zwischen den Zahlen $|\mathfrak{X}|$, $|\mathfrak{x}|$, $(\mathfrak{X}\mathfrak{x})$, $(\mathfrak{x}\mathfrak{X})$ und den Invarianten v, k, λ, n der Ebene immer bestehen müssen, nämlich die folgenden

Grundgleichungen:

(G 1) $$(\mathfrak{P}\mathfrak{g})\,|\mathfrak{g}| = (\mathfrak{g}\mathfrak{P})\,|\mathfrak{P}| \qquad \textit{für alle } \mathfrak{P}, \mathfrak{g}.$$

(G 2) $$\sum_{\mathfrak{x}} (\mathfrak{x}\mathfrak{P}) = \sum_{\mathfrak{X}} (\mathfrak{X}\mathfrak{g}) = k \qquad \textit{für alle } \mathfrak{P}, \mathfrak{g}.$$

(G 3) $$\sum_{\mathfrak{X}} |\mathfrak{X}| = \sum_{\mathfrak{x}} |\mathfrak{x}| = v.$$

(G 4a) $$\sum_{\mathfrak{x}} (\mathfrak{P}\mathfrak{x})(\mathfrak{x}\mathfrak{Q}) = \lambda\,|\mathfrak{P}| + n\,\delta(\mathfrak{P}, \mathfrak{Q}) \qquad \textit{für alle } \mathfrak{P}, \mathfrak{Q}.$$

(G 4b) $$\sum_{\mathfrak{X}} (\mathfrak{g}\mathfrak{X})(\mathfrak{X}\mathfrak{h}) = \lambda\,|\mathfrak{g}| + n\,\delta(\mathfrak{g}, \mathfrak{h}) \qquad \textit{für alle } \mathfrak{g}, \mathfrak{h}.$$

Dabei soll die Funktion δ wie üblich die Werte Eins oder Null annehmen, je nachdem ob ihre Argumente gleich oder verschieden sind.

(G 1) ist genau die Gl. (1) mit der auf S. 62 eingeführten Bezeichnungsweise. (G 2) und (G 3) folgen sofort aus den Tatsachen, daß jedes Element mit genau k andersartigen inzidiert und daß die Anzahl aller gleichartigen Elemente v ist. Also bleiben nur die Beziehungen (G 4) zu beweisen, und dazu genügt es aus Dualitätsgründen, nur (G 4a) herzuleiten.

Es sei Q ein beliebiger Punkt der Punktklasse $\mathfrak{Q}$ und g eine Gerade durch Q, die der Geradenklasse $\mathfrak{x}$ angehören möge. Auf g liegen $(\mathfrak{P}\mathfrak{x}) - \delta(\mathfrak{P}, \mathfrak{Q})$ von Q verschiedene Punkte der Punktklasse $\mathfrak{P}$, welche von $\mathfrak{Q}$ nicht verschieden zu sein braucht, und durch Q gehen $(\mathfrak{x}\mathfrak{Q})$ Geraden von $\mathfrak{x}$. Die Anzahl inzidenter Paare (P, x) mit $x \mathrel{I} Q \neq P \in \mathfrak{P}$ und $x \in \mathfrak{x}$ ist also gleich $[(\mathfrak{P}\mathfrak{x}) - \delta(\mathfrak{P}, \mathfrak{Q})](\mathfrak{x}\mathfrak{Q})$.

Durch Summation über alle Geradenklassen (diejenigen Geradenklassen $\mathfrak{y}$, die keine Geraden durch Q schicken, geben dabei wegen $(\mathfrak{y}\,\mathfrak{Q})=0$ keinen Beitrag) erhält man die Anzahl aller inzidenten Paare (P, z) mit $z\,\mathrm{I}\,Q \neq P \in \mathfrak{P}$. Diese ist aber, da jeder der $|\mathfrak{P}|-\delta(\mathfrak{P}, \mathfrak{Q})$ von Q verschiedenen Punkte von $\mathfrak{P}$ mit Q genau λ Verbindungsgeraden hat, auch gleich $\lambda[|\mathfrak{P}|-\delta(\mathfrak{P}, \mathfrak{Q})]$. Damit haben wir die Beziehung

$$\lambda[|\mathfrak{P}|-\delta(\mathfrak{P}, \mathfrak{Q})]=\sum_{\mathfrak{x}}[(\mathfrak{P}\,\mathfrak{x})-\delta(\mathfrak{P}, \mathfrak{Q})]\,(\mathfrak{x}\,\mathfrak{Q}),$$

aus der (G 4a) durch triviale Umformungen mit (G 2) folgt.

Für später brauchen wir noch die folgenden Gleichungen:

$$\sum_{\mathfrak{x}}(\mathfrak{P}\,\mathfrak{x})\,|\mathfrak{x}|=k\,|\mathfrak{P}|, \qquad \sum_{\mathfrak{X}}(\mathfrak{g}\,\mathfrak{X})\,|\mathfrak{X}|=k\,|\mathfrak{g}|; \tag{4}$$

man erhält sie sofort aus (G 1) durch Summation und Benutzung von (G 2).

1.3. Anzahl der Klassen einer taktischen Zerlegung

Aus den Grundgleichungen ergibt sich leicht der folgende wichtige Satz:

Satz 2. *Die Anzahl der Punktklassen einer taktischen Zerlegung einer λ-Ebene ist gleich der ihrer Geradenklassen.*

Beweis. Man setze $\mathfrak{P}=\mathfrak{Q}=\mathfrak{X}$ in (G 4a) und summiere über alle $\mathfrak{X}$, wegen (G 3) folgt

$$\sum_{\mathfrak{x},\mathfrak{X}}(\mathfrak{X}\,\mathfrak{x})\,(\mathfrak{x}\,\mathfrak{X})=\lambda v+nt, \tag{5}$$

wobei t die Anzahl der Punktklassen bezeichnet. Dual erhält man aus (G 4b), daß die in (5) links stehende Summe auch gleich $\lambda v+nt'$ ist, mit t' gleich der Anzahl der Geradenklassen. Also folgt $t=t'$, q.e.d.

Die Anzahl der Punktklassen einer taktischen Zerlegung Γ, d.h. also auch die der Geradenklassen, wird von nun an durch das Symbol $t=t(\Gamma)$ bezeichnet.

Aus den Sätzen 1 und 2 folgt bei $t(\Gamma)=1$ sofort:

Satz 3. *Eine Kollineationsgruppe einer λ-Ebene ist genau dann auf den Punkten transitiv, wenn sie auf den Geraden transitiv ist.*

Tiefer liegt der entsprechende Satz über zweifache Transitivität:

Satz 4. *Eine Kollineationsgruppe einer λ-Ebene ist genau dann auf den Punkten zweifach transitiv, wenn sie auf den Geraden zweifach transitiv ist.*

Beweis. Wir treffen zunächst folgende Verabredungen: Ist G eine beliebige Permutationsgruppe der Menge M, so werde die Untergruppe aller derjenigen Permutationen von G, die ein bestimmtes Element $x \in M$ festlassen, mit G_x bezeichnet. Weiter soll x^U die Menge aller x^σ mit $\sigma \in U \subseteq G$ bedeuten. Sodann gilt, wie wir hier ohne Beweis bemerken (man vergleiche etwa WIELANDT [*15*], S. 9):

$$|G|=|G_x|\,|x^G|. \tag{6}$$

Es sei nun Γ eine Kollineationsgruppe einer λ-Ebene $\mathfrak{E}$, die auf der Menge $\mathscr{P}$ der Punkte von $\mathfrak{E}$ zweifach transitiv ist. Sodann ist Γ sicher transitiv auf $\mathscr{P}$, also nach Satz 3 auch transitiv auf der Menge $\mathscr{G}$ der Geraden von $\mathfrak{E}$. Folglich ist $|P^\Gamma| = |g^\Gamma| = v$ für alle $P \in \mathscr{P}$, $g \in \mathscr{G}$. Nach (6) ist daher auch $|\Gamma_P| = |\Gamma_g|$. Anwendung von (6) auf die Gruppen Γ_P, Γ_g ergibt nun wegen $(\Gamma_P)_g = \Gamma_P \cap \Gamma_g = (\Gamma_g)_P$ die Beziehung

$$|P^{\Gamma_g}| = |g^{\Gamma_P}|. \tag{7}$$

Da Γ zweifach transitiv auf $\mathscr{P}$ ist, ist jede Γ_P noch transitiv auf den von P verschiedenen Punkten von $\mathscr{P}$, d.h. die taktische Zerlegung Γ_P hat zwei Punktklassen. Also hat sie nach Satz 2 auch zwei Geradenklassen; eine von diesen muß aus den k Geraden durch P, die andere aus den $v-k$ übrigen Geraden bestehen. Aus (7) folgt nun, daß für eine feste Gerade g die Zahl $|P^{\Gamma_g}|$ gleich k ist, wenn $P \mathrel{I} g$, und gleich $v-k$, wenn $P \mathrel{\not I} g$. Die Gruppe Γ_g zerlegt $\mathscr{P}$ also in zwei Punktklassen. Also folgt aus Satz 2, daß Γ_g die Menge $\mathscr{G}$ in zwei Geradenklassen zerlegt. Von diesen besteht eine aus g allein, also ist Γ_g transitiv auf den von g verschiedenen Geraden. Das bedeutet aber zusammen mit der Transitivität von Γ auf $\mathscr{G}$, daß Γ zweifach transitiv auf $\mathscr{G}$ ist. Da es aus Dualitätsgründen genügt, nur diesen Beweis zu liefern, ist Satz 4 damit bewiesen.

1.4. Beziehungen zwischen verschiedenen taktischen Zerlegungen

Wir kehren nun zu beliebigen taktischen Zerlegungen von λ-Ebenen zurück. Wir beweisen zunächst einige zahlentheoretische Eigenschaften der Zahlen $(\mathfrak{X}\mathfrak{x})$, $(\mathfrak{x}\mathfrak{X})$, $|\mathfrak{X}|$, $|\mathfrak{x}|$.

Es sei Γ eine taktische Zerlegung der λ-Ebene $\mathfrak{E}$ der Ordnung n mit $t(\Gamma) \geq 2$, und es seien $\mathfrak{P}$, $\mathfrak{Q}$, $\mathfrak{g}$, $\mathfrak{h}$ vier verschiedene Γ-Klassen. Wir definieren D als den größten gemeinsamen Teiler der Zahlen $(\mathfrak{X}\mathfrak{g}) - (\mathfrak{X}\mathfrak{h})$, ferner d als den g.g.T. aller $(\mathfrak{x}\mathfrak{P}) - (\mathfrak{x}\mathfrak{Q})$, $D' =$ g.g.T. aller $(\mathfrak{g}\mathfrak{X}) - (\mathfrak{h}\mathfrak{X})$ und $d' =$ g.g.T. aller $(\mathfrak{P}\mathfrak{x}) - (\mathfrak{Q}\mathfrak{x})$. Sodann gilt:

Lemma 1. (a) *D und d, und im Falle $t(\Gamma) > 2$ auch D' und d', sind Teiler von n.*

(b) *Es gilt stets:*

$$\begin{cases} n \equiv \lambda(|\mathfrak{P}| - |\mathfrak{Q}|) \equiv k(|\mathfrak{P}| - |\mathfrak{Q}|) \bmod d' \\ n \equiv \lambda(|\mathfrak{g}| - |\mathfrak{h}|) \equiv k(|\mathfrak{g}| - |\mathfrak{h}|) \bmod D', \end{cases} \tag{8}$$

$$\begin{cases} \varepsilon\lambda(|\mathfrak{P}| - |\mathfrak{Q}|) \equiv \varepsilon k(|\mathfrak{P}| - |\mathfrak{Q}|) \equiv 0 \bmod d' \\ \varepsilon\lambda(|\mathfrak{g}| - |\mathfrak{h}|) \equiv \varepsilon k(|\mathfrak{g}| - |\mathfrak{h}|) \equiv 0 \bmod D' \end{cases} \tag{9}$$

mit $\varepsilon = \begin{cases} 1 & \text{wenn } t(\Gamma) > 2 \\ 2 & \text{wenn } t(\Gamma) = 2. \end{cases}$

(c) *Ist $t(\Gamma) = 2$, so sind $\mathfrak{P}$, $\mathfrak{Q}$, $\mathfrak{g}$, $\mathfrak{h}$ die einzigen Γ-Klassen, und es gilt*

$$n = [(\mathfrak{P}\mathfrak{g}) - (\mathfrak{P}\mathfrak{h})]\,[(\mathfrak{g}\mathfrak{P}) - (\mathfrak{g}\mathfrak{Q})]. \tag{10}$$

Beweis. Nach (G 4a) ist

$$n = \lambda|\mathfrak{P}| + n - \lambda|\mathfrak{P}| = \sum_{\mathfrak{x}} (\mathfrak{P}\,\mathfrak{x})\,[(\mathfrak{x}\,\mathfrak{P}) - (\mathfrak{x}\,\mathfrak{Q})] \equiv 0 \bmod d,$$

und analog folgt, daß D Teiler von n ist. Ist $t(\Gamma)>2$, so existiert außer $\mathfrak{P}$ und $\mathfrak{Q}$ noch eine weitere Punktklasse $\mathfrak{R}$; mit dieser erhält man

$$\lambda(|\mathfrak{P}| - |\mathfrak{Q}|) = \sum_{\mathfrak{x}} [(\mathfrak{P}\,\mathfrak{x}) - (\mathfrak{Q}\,\mathfrak{x})]\,(\mathfrak{x}\,\mathfrak{R}) \equiv 0 \bmod d'$$

[womit die erste Kongruenz (9) für $t>2$ bewiesen ist], und daraus folgt

$$n \equiv n + \lambda(|\mathfrak{P}| - |\mathfrak{Q}|) = \sum_{\mathfrak{x}} [(\mathfrak{P}\,\mathfrak{x}) - (\mathfrak{Q}\,\mathfrak{x})]\,(\mathfrak{x}\,\mathfrak{P}) \equiv 0 \bmod d'.$$

Also ist auch d' Teiler von n. Für D' läuft der Beweis dual. Damit ist (a) bewiesen.

Es sei nun $t(\Gamma)=2$. Sodann erhält man wie oben

$$\lambda(|\mathfrak{P}| - |\mathfrak{Q}|) + n = \sum_{\mathfrak{x}} [(\mathfrak{P}\,\mathfrak{x}) - (\mathfrak{Q}\,\mathfrak{x})]\,(\mathfrak{x}\,\mathfrak{P}) \equiv 0 \bmod d'$$

und

$$\lambda(|\mathfrak{P}| - |\mathfrak{Q}|) - n = \sum_{\mathfrak{x}} [(\mathfrak{P}\,\mathfrak{x}) - (\mathfrak{Q}\,\mathfrak{x})]\,(\mathfrak{x}\,\mathfrak{Q}) \equiv 0 \bmod d';$$

daraus folgt durch Addition und Subtraktion

$$2n = 2\lambda(|\mathfrak{P}| - |\mathfrak{Q}|) \equiv 0 \bmod d'.$$

Hieraus ergibt sich nun

$$2k(|\mathfrak{P}| - |\mathfrak{Q}|) = 2(n+\lambda)(|\mathfrak{P}| - |\mathfrak{Q}|) \equiv 0 \bmod d',$$

womit die erste Kongruenz (9) auch für $t(\Gamma)=2$ bewiesen ist. Der Beweis der zweiten Kongruenz (9) verläuft dual. Wegen $k=n+\lambda$ ist damit im Falle $t(\Gamma)>2$ auch (8) erledigt, es bleibt also (8) für $t(\Gamma)=2$ zu beweisen. Wie oben gezeigt, gilt $2n\equiv 0 \bmod d'$ und $\lambda(|\mathfrak{P}|-|\mathfrak{Q}|)+n\equiv 0 \bmod d'$, folglich ist $n\equiv\lambda(|\mathfrak{P}|-|\mathfrak{Q}|) \bmod d'$. Der verbleibende Teil von (8) folgt wieder aus $k=n+\lambda$. Damit ist (b) bewiesen.

Im Falle $t(\Gamma)=2$ gilt nach (G 4a), daß

$$n = (\mathfrak{P}\,\mathfrak{g})\,[(\mathfrak{g}\,\mathfrak{P}) - (\mathfrak{g}\,\mathfrak{Q})] + (\mathfrak{P}\,\mathfrak{h})\,[(\mathfrak{h}\,\mathfrak{P}) - (\mathfrak{h}\,\mathfrak{Q})]$$

ist. Andererseits ist $(\mathfrak{h}\,\mathfrak{P}) - (\mathfrak{h}\,\mathfrak{Q}) = -[(\mathfrak{g}\,\mathfrak{P}) - (\mathfrak{g}\,\mathfrak{Q})]$ wegen (G 2). Kombination dieser Beziehungen ergibt (10). Damit ist Lemma 1 vollständig bewiesen.

Lemma 2. *Ist Γ eine taktische Zerlegung einer beliebigen λ-Ebene mit $(\Gamma)\geq 2$, und sind $\mathfrak{P}$, $\mathfrak{Q}$, $\mathfrak{g}$, $\mathfrak{h}$ vier verschiedene Γ-Klassen, so gibt es unter den Zahlen $(\mathfrak{P}\,\mathfrak{x}) - (\mathfrak{Q}\,\mathfrak{x})$ und unter den Zahlen $(\mathfrak{g}\,\mathfrak{X}) - (\mathfrak{h}\,\mathfrak{X})$ mindestens je eine, und unter den Zahlen $(\mathfrak{x}\,\mathfrak{P}) - (\mathfrak{x}\,\mathfrak{Q})$ und $(\mathfrak{X}\,\mathfrak{g}) - (\mathfrak{X}\,\mathfrak{h})$ mindestens je zwei von Null verschiedene.*

Beweis. Wären z.B. alle $(\mathfrak{P}\,\mathfrak{x}) - (\mathfrak{Q}\,\mathfrak{x}) = 0$, so würden (8) und (9) „modulo Null" gelten, d.h. man könnte in (8) und (9) das Kongruenzzeichen durch das

Gleichheitszeichen ersetzen. Das würde in (9) wegen $\varepsilon\lambda \neq 0$ ergeben, daß $|\mathfrak{P}| = |\mathfrak{Q}|$ wäre, also würde aus (8) folgen, daß $n = 0$ ist, ein Widerspruch. Daß es unter den $(\mathfrak{x}\mathfrak{P}) - (\mathfrak{x}\mathfrak{Q})$ sogar zwei von Null verschiedene geben muß, folgt aus (G 2): es ist

$$\sum_{\mathfrak{x}} [(\mathfrak{x}\mathfrak{P}) - (\mathfrak{x}\mathfrak{Q})] = k - k = 0;$$

verschwinden in dieser Summe alle Glieder bis auf eines, so muß auch dieses letzte verschwinden, und das haben wir schon als unmöglich erkannt. Damit ist Lemma 2 bewiesen.

Das wesentliche Ergebnis des vorliegenden Paragraphen ist der folgende Satz, der es erlaubt, in der Menge aller taktischen Zerlegungen einer λ-Ebene auf natürliche Weise eine teilweise Ordnung einzuführen:

Satz 5. *Es seien Γ und Γ' zwei (nicht notwendig verschiedene) taktische Zerlegungen derselben λ-Ebene. Sodann sind die folgenden Aussagen gleichwertig:*

(i) *Zu jeder Γ-Punktklasse $\mathfrak{P}$ existiert eine Γ'-Punktklasse $\mathfrak{P}'$ derart, daß $\mathfrak{P} \subseteqq \mathfrak{P}'$.*

(ii) *Zu jeder Γ-Geradenklasse $\mathfrak{g}$ existiert eine Γ'-Geradenklasse $\mathfrak{g}'$ derart, daß $\mathfrak{g} \subseteqq \mathfrak{g}'$.*

Beweis. Es genügt zu zeigen, daß (ii) aus (i) folgt. Wäre das nicht der Fall, so gäbe es eine λ-Ebene mit zwei taktischen Zerlegungen Γ und Γ', für die (i), aber nicht (ii) gilt, d.h. es gäbe eine Γ-Geradenklasse $\mathfrak{g}$ und zwei verschiedene Γ'-Geradenklassen $\mathfrak{g}_1'$ und $\mathfrak{g}_2'$ derart, daß $\mathfrak{g} \cap \mathfrak{g}_i' \neq \emptyset$, für $i = 1, 2$. Wir werden diese Möglichkeit ad absurdum führen.

Wir zeigen zunächst, daß für diese Geradenklassen und beliebige Γ'-Punktklassen $\mathfrak{X}'$ die folgenden Aussagen äquivalent sind:

(a) $(\mathfrak{X}'\,\mathfrak{g}_1')' \neq 0$,

(b) $(\mathfrak{X}'\,\mathfrak{g}_2')' \neq 0$.

(c) Es existiert eine Γ-Punktklasse $\mathfrak{X} \subseteqq \mathfrak{X}'$ mit $(\mathfrak{X}\,\mathfrak{g}) \neq 0$.

Sei $i = 1$ oder 2 und $(\mathfrak{X}'\,\mathfrak{g}_i')' \neq 0$, ferner $g \in \mathfrak{g} \cap \mathfrak{g}_i'$. Auf g liegen Punkte von $\mathfrak{X}'$; sei P ein solcher und $\mathfrak{X}$ die durch ihn bestimmte Γ-Punktklasse. Wegen (i) ist sodann $\mathfrak{X} \subseteqq \mathfrak{X}'$; ferner ist $(\mathfrak{X}\,\mathfrak{g}) \neq 0$, da $g \in \mathfrak{g}$ und $g \mathrel{I} P \in \mathfrak{X}$. Also folgt (c) aus jeder der Aussagen (a), (b).

Ist umgekehrt $\mathfrak{X} \subseteqq \mathfrak{X}'$ und $(\mathfrak{X}\,\mathfrak{g}) \neq 0$, so enthält jede Gerade von $\mathfrak{g}$ Punkte von $\mathfrak{X}$, also erst recht solche von $\mathfrak{X}'$; ist also $g_i \in \mathfrak{g} \cap \mathfrak{g}_i'$, so enthält g_i Punkte von $\mathfrak{X}'$. Daher ist $(\mathfrak{X}'\,\mathfrak{g}_i')' \neq 0$, $i = 1, 2$. Also folgen sowohl (a) als auch (b) aus (c), und die Äquivalenz von (a), (b), (c) ist bewiesen.

Nach Lemma 2 gibt es nun eine Γ'-Punktklasse $\mathfrak{P}'$, für die $(\mathfrak{P}'\,\mathfrak{g}_1')' \neq (\mathfrak{P}'\,\mathfrak{g}_2')'$ gilt. Eine dieser beiden Zahlen ist von Null verschieden, also wegen der Äquivalenz von (a) und (b) auch die andere. Wegen der Äquivalenz von (a) und (b) mit (c) folgt weiter die Existenz gewisser Γ-Punktklassen $\mathfrak{P}_j \subseteqq \mathfrak{P}'$, mit $j = 1, 2, \ldots, h$; $h \geqq 1$, für die $(\mathfrak{P}_j\,\mathfrak{g}) \neq 0$ gilt. Für alle von den $\mathfrak{P}_j$ verschiedenen Γ-Punktklassen $\mathfrak{X}$ gilt wegen (i) und (a), (b), (c) entweder $\mathfrak{X} \cap \mathfrak{P}' = \emptyset$

oder $(\mathfrak{X}\,\mathfrak{g}) = 0$. Ist nun $g_i \in \mathfrak{g} \cap \mathfrak{g}_i'$, $i = 1, 2$, so liegen auf g_1 wie auf g_2 genau $(\mathfrak{P}_j\,\mathfrak{g})$ Punkte von $\mathfrak{P}_j$, und aus den angegebenen Eigenschaften der $\mathfrak{P}_j$ folgt

$$(\mathfrak{P}'\,\mathfrak{g}_1')' = \sum_{j=1}^{h} (\mathfrak{P}_j\,\mathfrak{g}) = (\mathfrak{P}'\,\mathfrak{g}_2')',$$

im Widerspruch zur Voraussetzung $(\mathfrak{P}'\,\mathfrak{g}_1')' \neq (\mathfrak{P}'\,\mathfrak{g}_2')'$. Damit ist Satz 5 bewiesen.

Eine unmittelbare Konsequenz dieses Satzes ist nachstehende

Folgerung. *Stimmen zwei taktische Zerlegungen derselben λ-Ebene in den Punktklassen oder in den Geradenklassen überein, so sind sie identisch.*

2. Die abgeleitete Struktur $\mathfrak{E}/\Gamma$

2.1. Definitionen

Es sei $\mathfrak{E}$ eine λ-Ebene der Ordnung n und Γ eine taktische Zerlegung von $\mathfrak{E}$. Wir definieren: Zwei ungleichartige Γ-Klassen $\mathfrak{P}$ und $\mathfrak{g}$ bilden ein *inzidentes Paar* oder ein *nichtinzidentes Paar*, je nachdem ob $(\mathfrak{P}\,\mathfrak{g}) \neq 0$ oder $= 0$ ist. [Wegen (G 1) könnte man auch $(\mathfrak{g}\,\mathfrak{P}) \neq 0$ bzw. $(\mathfrak{g}\,\mathfrak{P}) = 0$ zur Definition benutzen.] Bezüglich der so definierten Inzidenzrelation werden die Γ-Klassen von $\mathfrak{E}$ zu den Elementen einer neuen endlichen verallgemeinerten Inzidenzstruktur; diese nennen wir die *nach Γ abgeleitete Struktur* von $\mathfrak{E}$ und bezeichnen sie mit $\mathfrak{E}/\Gamma$. Die Struktur $\mathfrak{E}/\Gamma$ besitzt $t(\Gamma)$ „Punkte" und ebensoviele „Geraden". Da wir bei den nachfolgenden Untersuchungen stets die zugrundeliegende λ-Ebene $\mathfrak{E}$ sowie die taktische Zerlegung Γ im Auge behalten wollen, werden wir die Elemente von $\mathfrak{E}/\Gamma$ nicht „Punkte" und „Geraden", sondern weiterhin „Punktklassen" und „Geradenklassen" nennen und dementsprechend auch von „Schnittklassen" und „Verbindungsklassen" reden.

Wir werden später sehen (vgl. das Beispiel S. 77), daß $\mathfrak{E}/\Gamma$ keineswegs wieder eine λ'-Ebene zu sein braucht. Insbesondere können verschiedene Γ-Klassen mit verschieden vielen andersartigen inzidieren, und verschiedene Paare von Punkt- bzw. Geradenklassen können verschieden viele Verbindungs- bzw. Schnittklassen besitzen. Um für das weitere eine bequeme Sprechweise zu besitzen, definieren wir die Zahlen $[\mathfrak{X}]$ bzw. $[\mathfrak{x}]$ als die Anzahlen von mit $\mathfrak{X}$ bzw. $\mathfrak{x}$ inzidenten Geraden- bzw. Punktklassen, und die Zahlen $[\mathfrak{X}, \mathfrak{Y}]$ bzw. $[\mathfrak{x}, \mathfrak{y}]$ als die Anzahlen von Verbindungsklassen von $\mathfrak{X}$ und $\mathfrak{Y}$ bzw. von Schnittklassen von $\mathfrak{x}$ und $\mathfrak{y}$, wobei natürlich $\mathfrak{X} \neq \mathfrak{Y}$ und $\mathfrak{x} \neq \mathfrak{y}$ sein soll. Es ist klar, daß $[\mathfrak{X}]$ und $[\mathfrak{x}]$ stets $\geqq 1$ sind. Daß auch $[\mathfrak{X}, \mathfrak{Y}]$ und $[\mathfrak{x}, \mathfrak{y}]$ stets $\geqq 1$ sind, ist leicht zu sehen: Eine Verbindungsgerade eines Punktes von $\mathfrak{X}$ mit einem Punkt von $\mathfrak{Y}$ spannt eine Verbindungsklasse von $\mathfrak{X}$ und $\mathfrak{Y}$ auf; und die Existenz von Schnittklassen folgt aus der dualen Überlegung. Für den Fall der Eindeutigkeit der Verbindungsklasse von $\mathfrak{X}$ und $\mathfrak{Y}$ bzw. der Schnittklasse von $\mathfrak{x}$ und $\mathfrak{y}$ wollen wir diese durch $\mathfrak{X}$ und $\mathfrak{Y}$ bzw. durch $\mathfrak{x}$ und $\mathfrak{y}$ eindeutig bestimmten Γ-Klassen mit $\mathfrak{X} + \mathfrak{Y}$ bzw. $\mathfrak{x} \cap \mathfrak{y}$ bezeichnen. Der Gebrauch dieser Symbole soll umgekehrt die Eindeutigkeit mit ausdrücken.

2.2. Der Hauptsatz

Wir werden nun zeigen, daß die Eindeutigkeit von Schnitt und Verbindung in $\mathfrak{E}/\Gamma$ ein recht selten auftretendes Phänomen ist:

Satz 6. *Sind Schnitte und Verbindungen in der abgeleiteten Struktur $\mathfrak{E}/\Gamma$ einer λ-Ebene $\mathfrak{E}$ nach einer taktischen Zerlegung Γ mit $t(\Gamma)>3$ eindeutig, so ist $\lambda=1$, also $\mathfrak{E}$ eine projektive Ebene. Ist auch $\mathfrak{E}/\Gamma$ eine (nichtausgeartete) projektive Ebene, so besteht jede Γ-Klasse aus einem Element, d.h. $\mathfrak{E}/\Gamma$ ist isomorph zu $\mathfrak{E}$.*

Dem Beweis schicken wir einige Hilfssätze voraus, aus denen wir außer Satz 6 noch andere Folgerungen werden ziehen können.

Lemma 3. *Es seien $\mathfrak{P}$, $\mathfrak{Q}$, $\mathfrak{g}$, $\mathfrak{h}$ vier verschiedene Klassen einer taktischen Zerlegung einer λ-Ebene. Dann gilt:*

Die folgenden Eigenschaften von $\mathfrak{P}$, $\mathfrak{Q}$ und $\mathfrak{g}$ sind äquivalent:		*Die folgenden Eigenschaften von $\mathfrak{g}$, $\mathfrak{h}$, und $\mathfrak{P}$ sind äquivalent:*	
(i)	$\mathfrak{g}=\mathfrak{P}+\mathfrak{Q}$	(i')	$\mathfrak{P}=\mathfrak{g}\cap\mathfrak{h}$
(ii)	$\lambda\,\lvert\mathfrak{P}\rvert=(\mathfrak{P}\,\mathfrak{g})\,(\mathfrak{g}\,\mathfrak{Q})$	(ii')	$\lambda\,\lvert\mathfrak{g}\rvert=(\mathfrak{g}\,\mathfrak{P})\,(\mathfrak{P}\,\mathfrak{h})$
(iii)	$\lambda\,\lvert\mathfrak{Q}\rvert=(\mathfrak{Q}\,\mathfrak{g})\,(\mathfrak{g}\,\mathfrak{P})$	(iii')	$\lambda\,\lvert\mathfrak{h}\rvert=(\mathfrak{h}\,\mathfrak{P})\,(\mathfrak{P}\,\mathfrak{g})$
(iv)	$\lambda\,\lvert\mathfrak{g}\rvert=(\mathfrak{g}\,\mathfrak{P})\,(\mathfrak{g}\,\mathfrak{Q})$.	(iv')	$\lambda\,\lvert\mathfrak{P}\rvert=(\mathfrak{P}\,\mathfrak{g})\,(\mathfrak{P}\,\mathfrak{h})$.

Beweis. Aus Dualitätsgründen genügt es, die Äquivalenz der Aussagen (i) bis (iv) zu beweisen. Ist $\mathfrak{g}=\mathfrak{P}+\mathfrak{Q}$, so ist insbesondere $\mathfrak{P}\neq\mathfrak{Q}$, und aus (G 4a) folgt $\lambda\,\lvert\mathfrak{P}\rvert=\sum_{\mathfrak{x}}(\mathfrak{P}\,\mathfrak{x})\,(\mathfrak{x}\,\mathfrak{Q})$. Da $\mathfrak{g}$ eindeutige Verbindungsklasse ist, gilt für alle $\mathfrak{x}\neq\mathfrak{g}$ entweder $(\mathfrak{P}\,\mathfrak{x})=0$ oder $(\mathfrak{x}\,\mathfrak{Q})=0$. Also folgt (ii). Ebenso folgt (iii) aus (i). Umgekehrt ergibt (G 4a) zusammen mit (ii) bzw. (iii), daß $\mathfrak{g}$ eindeutige Verbindungsklasse von $\mathfrak{P}$ und $\mathfrak{Q}$ ist. Damit ist die Gleichwertigkeit der Aussagen (i), (ii), (iii) bewiesen. Multiplikation von (ii) mit $\lvert\mathfrak{g}\rvert$ und Anwendung von (G 1) auf die rechte Seite ergibt nach Herauskürzen von $\lvert\mathfrak{P}\rvert$ die Gl. (iv), und analog folgt (ii) aus (iv). Damit ist alles bewiesen.

Für das weitere benötigen wir noch nachstehende

Folgerung. *Aus $\mathfrak{g}=\mathfrak{P}+\mathfrak{Q}$ und $\mathfrak{P}=\mathfrak{g}\cap\mathfrak{h}$ folgt $(\mathfrak{P}\,\mathfrak{h})=(\mathfrak{g}\,\mathfrak{Q})$.*

Das ergibt sich unmittelbar durch Vergleich von (iv) und (ii').

Lemma 4. *Sind Schnitte und Verbindungen in $\mathfrak{E}/\Gamma$ eindeutig und ist $t(\Gamma)>2$, so gibt es in $\mathfrak{E}/\Gamma$ ein nicht-ausgeartetes Dreieck.*

Beweis. Wäre das nicht der Fall, so müßten alle Punktklassen mit derselben Geradenklasse $\mathfrak{g}$ und alle Geradenklassen mit derselben Punktklasse $\mathfrak{P}$ inzident sein; und $\mathfrak{P}$ und $\mathfrak{g}$ wären die einzigen Γ-Klassen, die mit mehr als einer andersartigen inzidieren. Wegen $t(\Gamma)>2$ müßte es nun zwei Punktklassen $\mathfrak{X}$ und $\mathfrak{Y}$ geben, die mit keiner anderen Geradenklasse als $\mathfrak{g}$ inzident sind, d.h. es müßte gelten $(\mathfrak{g}\,\mathfrak{X})=(\mathfrak{g}\,\mathfrak{Y})=k$. Einerseits würde nun aus Lemma 3, (ii) folgen, daß $\lambda\,\lvert\mathfrak{X}\rvert=(\mathfrak{X}\,\mathfrak{g})\,(\mathfrak{g}\,\mathfrak{Y})=k\,(\mathfrak{X}\,\mathfrak{g})$, andererseits ergibt (G 4a), daß

$\lambda|\mathfrak{X}| = (\mathfrak{X}\,\mathfrak{g})\,(\mathfrak{g}\,\mathfrak{X}) - n = k\,(\mathfrak{X}\,\mathfrak{g}) - n$ ist. Das ist ein Widerspruch, der Lemma 4 beweist.

Das folgende Lemma 5 ist das Kernstück des Beweises von Satz 6:

Lemma 5. *Es sei Γ eine taktische Zerlegung der λ-Ebene $\mathfrak{E}$ der Ordnung n. Gibt es sodann eine Γ-Klasse, die mit allen gleichartigen Γ-Klassen eindeutige Verbindungs- bzw. Schnittklassen besitzt und die mit mindestens drei andersartigen Klassen inzidiert, von denen ihrerseits mindestens zwei außer mit der gegebenen noch mit einer weiteren inzident sind, so ist $\lambda = 1$ und die gegebene Γ-Klasse besteht entweder aus einem oder aus n^2 Elementen. Im letzteren Falle gibt es genau eine mit der gegebenen nicht inzidierende andersartige Klasse, und diese besteht aus einem Element.*

Beweis. Ohne Beschränkung der Allgemeinheit kann die gegebene Γ-Klasse als Punktklasse $\mathfrak{P}$ angenommen werden. Die Voraussetzungen über $\mathfrak{P}$ besagen dann:

(a) $[\mathfrak{P}, \dot{\mathfrak{X}}] = 1$ für alle $\mathfrak{X} \neq \mathfrak{P}$,

(b) $[\mathfrak{P}] > 2$.

(c) Es gibt zwei verschiedene Geradenklassen $\mathfrak{g}$ und $\mathfrak{h}$ mit $(\mathfrak{P}\,\mathfrak{g}) \neq 0 \neq (\mathfrak{P}\,\mathfrak{h})$ und $[\mathfrak{g}] > 1 < [\mathfrak{h}]$.

Das bedeutet, daß es in $\mathfrak{E}/\Gamma$ eine aus $\mathfrak{P}$ und zwei weiteren Punktklassen $\mathfrak{Q}$, $\mathfrak{R}$ sowie aus $\mathfrak{g}$, $\mathfrak{h}$ und einer weiteren Geradenklasse $\mathfrak{y}$ bestehende Konfiguration gibt, deren Inzidenzen in Fig. 1 illustriert sind:

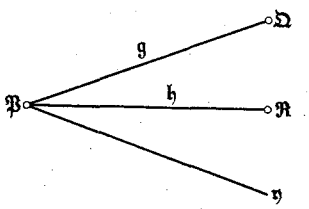

Fig. 1

Alle Schnitte und Verbindungen in dieser Konfiguration sind eindeutig: $\mathfrak{g} \cap \mathfrak{h} = \mathfrak{g} \cap \mathfrak{y} = \mathfrak{h} \cap \mathfrak{y} = \mathfrak{P}$, $\mathfrak{g} = \mathfrak{P} + \mathfrak{Q}$, $\mathfrak{h} = \mathfrak{P} + \mathfrak{R}$. Wegen der Folgerung von Lemma 3 ergibt sich aus diesen Beziehungen: $(\mathfrak{P}\,\mathfrak{h}) = (\mathfrak{g}\,\mathfrak{Q}) = (\mathfrak{P}\,\mathfrak{y}) = (\mathfrak{h}\,\mathfrak{R}) = (\mathfrak{P}\,\mathfrak{g})$; alle diese Zahlen sind also gleich derselben von Null verschiedenen Konstanten j, und es ist bewiesen:

Aus $(\mathfrak{P}\,\mathfrak{x})\,(\mathfrak{x}\,\mathfrak{X}) \neq 0$ folgt $(\mathfrak{P}\,\mathfrak{x}) = (\mathfrak{x}\,\mathfrak{X}) = j$.

Nun ist nach Lemma 3,(ii) einerseits $\lambda\,|\,\mathfrak{P}| = (\mathfrak{P}\,\mathfrak{g})\,(\mathfrak{g}\,\mathfrak{Q}) = j^2$, andererseits nach (G 4a) und (G 2) auch

$$\lambda\,|\,\mathfrak{P}| = \sum_{\mathfrak{x}} (\mathfrak{P}\,\dot{\mathfrak{x}})\,(\mathfrak{x}\,\mathfrak{P}) - n = j \sum_{\mathfrak{x}} (\mathfrak{x}\,\mathfrak{P}) - n = jk - n,$$

denn wegen (G 1) ist genau dann $(\mathfrak{x}\,\mathfrak{P}) = 0$, wenn $(\mathfrak{P}\,\mathfrak{x}) = 0$ ist. Also ergibt sich für j die quadratische Gleichung

$$j^2 - kj + n = 0.$$

Diese Gleichung hat die Lösungen $j = (k \pm q)/2$, wobei $q^2 = k^2 - 4n$ ist. Es muß also $k \equiv q \bmod 2$ und die Zahl $k^2 - 4n$ eine Quadratzahl sein.

Nun ist $q^2 = k^2 - 4n < k^2$, also $q \leqq k - 1$. Andererseits ist wegen $k = n + \lambda$ auch $q^2 = (k-2)^2 + 4(\lambda - 1) \geqq (k-2)^2$. Wäre nun $\lambda > 1$, so würde in der letzten Ungleichung nur das „Größer"-Zeichen gelten, und es ergäbe sich

$q \geqq k-1$, d.h. mit dem oben gewonnenen Ergebnis zusammen $q=k-1$. Das aber ist ein Widerspruch zu $k \equiv q \bmod 2$. Damit ist $\lambda=1$ bewiesen.

Es folgt nun weiter $q=k-2=n-1$, also $j=1$ oder $j=n$. Aus $\lambda|\mathfrak{P}| = |\mathfrak{P}|=j^2$ ergibt sich also $|\mathfrak{P}|=1$ oder $|\mathfrak{P}|=n^2$. Es bleibt zu zeigen, daß die Ebene im Falle $|\mathfrak{P}|=n^2$ genau eine Gerade enthält, auf der keine Punkte von $\mathfrak{P}$ liegen. Dazu benutzen wir die in 1.2. bewiesene Gleichung

$$\sum_{\mathfrak{x}} (\mathfrak{P}\,\mathfrak{x})\,|\mathfrak{x}| = k\,|\mathfrak{P}|. \tag{4}$$

Die linke Seite dieser Gleichung ist im vorliegenden Falle $j \sum_{(\mathfrak{P}\,\mathfrak{x})\neq 0} |\mathfrak{x}| = n \sum_{(\mathfrak{P}\,\mathfrak{x})\neq 0} |\mathfrak{x}|$, die rechte Seite ist $(n+1)\,n^2$. Es folgt $\sum_{(\mathfrak{P}\,\mathfrak{x})\neq 0} |\mathfrak{x}| = n(n+1)$, oder $\sum_{(\mathfrak{P}\,\mathfrak{x})=0} |\mathfrak{x}| = v-n(n+1)=1$. Also gibt es nur eine Geradenklasse $\mathfrak{g}$ mit $(\mathfrak{P}\,\mathfrak{g})=0$, und diese besteht aus genau einer Geraden. Damit ist Lemma 5 vollständig bewiesen.

Beweis von Satz 6. Wegen Lemma 4 folgt aus der Voraussetzung $t(\Gamma)>3$ die Existenz eines nichtausgearteten Dreiecks. Also ergibt sich: Entweder ist $\mathfrak{E}/\Gamma$ eine nichtausgeartete projektive Ebene, oder es gibt zwei ausgezeichnete Γ-Klassen $\mathfrak{P}$ und $\mathfrak{g}$ mit den in Fig. 2 angedeuteten Inzidenzverhältnissen, insbesondere also mit $[\mathfrak{P}]>2<[\mathfrak{g}]$, da $t(\Gamma)>3$.

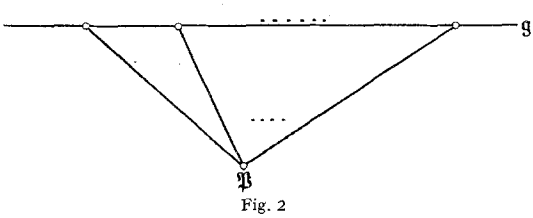

Fig. 2

In jedem Falle gibt es Γ-Klassen, die die Voraussetzungen von Lemma 5 erfüllen. Also ist $\lambda=1$ und $\mathfrak{E}$ eine projektive Ebene. Ist auch $\mathfrak{E}/\Gamma$ eine (nichtausgeartete) projektive Ebene, so kann keine Klasse mehr als ein Element enthalten, da es sonst nach Lemma 5 nur eine nicht mit ihr inzidente andersartige Γ-Klasse geben könnte. Das aber ist in einer nichtausgearteten projektiven Ebene nicht möglich. Damit ist Satz 6 bewiesen.

2.3. Ergänzungssätze

Während bisher die Frage im Vordergrund stand, unter welchen Umständen man aus der Voraussetzung der Eindeutigkeit von Schnitt und Verbindung in $\mathfrak{E}/\Gamma$ schließen kann, daß $\lambda=1$ ist, wollen wir nun $\lambda=1$ voraussetzen und untersuchen, was man über die Typen von taktischen Zerlegungen aussagen kann, deren abgeleitete Strukturen eindeutige Schnitte und Verbindungen haben. Wir werden zeigen (man vergleiche dazu die Definition von S. 63):

Satz 7. *Die nichttrivialen taktischen Zerlegungen Γ mit $t(\Gamma)>2$ einer projektiven Ebene der Ordnung n, deren abgeleitete Strukturen eindeutige Schnitte und Verbindungen haben, sind genau diejenigen, welche eine Klasse mit genau n^2 Elementen besitzen.*

Wir beweisen zunächst den folgenden Hilfssatz:

Lemma 6. *Erfüllt die taktische Zerlegung Γ der endlichen projektiven Ebene $\mathfrak{E}$ die Bedingungen*

(a) $t(\Gamma) = 3$,

(b) $[\mathfrak{X}] = [\mathfrak{x}] = 2$ *für alle* $\mathfrak{X}, \mathfrak{x}$,

(c) $[\mathfrak{X}, \mathfrak{Y}] = 1$ *für alle* $\mathfrak{X}, \mathfrak{Y}$, *oder*
$[\mathfrak{x}, \mathfrak{y}] = 1$ *für alle* $\mathfrak{x}, \mathfrak{y}$,

so besteht eine Γ-Klasse aus n^2 Elementen.

Die beiden Eigenschaften (c) sind natürlich gleichwertig.

Beweis. Aus den Voraussetzungen folgt zunächst, daß die abgeleitete Struktur $\mathfrak{E}/\Gamma$ ein nichtausgeartetes Dreieck ist. Wir bezeichnen die Punktklassen mit $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}$ und die Geradenklassen mit $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ derart, daß

$$(\mathfrak{A}\,\mathfrak{a}) = (\mathfrak{B}\,\mathfrak{b}) = (\mathfrak{C}\,\mathfrak{c}) = 0$$

ist (vgl. Fig. 3).

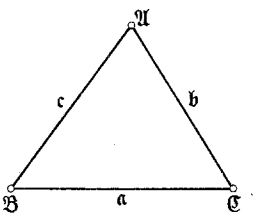

Fig. 3

Wir machen nun die Annahme

(*) $\qquad |\mathfrak{X}| > 1 < |\mathfrak{x}|$ für alle $\mathfrak{X}, \mathfrak{x}$.

Dann folgt zunächst, daß jede Γ-Klasse drei Elemente in allgemeiner Lage enthalten muß, denn wären z.B. alle Punkte einer Punktklasse $\mathfrak{X}$ mit einer Geraden g kollinear, so müßte g eine Geradenklasse für sich bilden. Gäbe es nämlich noch eine weitere Gerade h in der von g aufgespannten Geradenklasse, so könnte auf dieser höchstens ein Punkt von $\mathfrak{X}$ liegen; das aber kann nicht sein, da ja g mehr als einen Punkt von $\mathfrak{X}$ enthält. Es sei nun b eine beliebige Gerade von $\mathfrak{b}$ und ferner $A \in \mathfrak{A}$ derart, daß $A \nmid b$. Einen solchen Punkt gibt es, da $\mathfrak{A}$ drei Punkte in allgemeiner Lage enthält. Auf b liegen genau $(\mathfrak{C}\,\mathfrak{b})$ Punkte von $\mathfrak{C}$, und die Verbindungsgeraden dieser Punkte mit A, die wegen $\lambda = 1$ eindeutig sind, müssen zu $\mathfrak{b}$ gehören, da sie Punkte von $\mathfrak{A}$ und $\mathfrak{C}$ enthalten. Da sie alle durch denselben Punkt A gehen, folgt $(\mathfrak{b}\,\mathfrak{A}) \geq (\mathfrak{C}\,\mathfrak{b})$. Wegen Voraussetzung (c) ist nun die Folgerung von Lemma 3 anwendbar, sie ergibt $(\mathfrak{b}\,\mathfrak{A}) = (\mathfrak{C}\,\mathfrak{a})$. Also folgt $(\mathfrak{C}\,\mathfrak{a}) \geq (\mathfrak{C}\,\mathfrak{b})$, und aus Symmetriegründen muß sogar $(\mathfrak{C}\,\mathfrak{a}) = (\mathfrak{C}\,\mathfrak{b})$ gelten. Ebenso folgt $(\mathfrak{A}\,\mathfrak{b}) = (\mathfrak{A}\,\mathfrak{c})$, $(\mathfrak{B}\,\mathfrak{c}) = (\mathfrak{B}\,\mathfrak{a})$, und dual dazu $(\mathfrak{a}\,\mathfrak{B}) = (\mathfrak{a}\,\mathfrak{C})$, $(\mathfrak{b}\,\mathfrak{C}) = (\mathfrak{b}\,\mathfrak{A})$, $(\mathfrak{c}\,\mathfrak{A}) = (\mathfrak{c}\,\mathfrak{B})$. Wir zeigen nun, daß alle von Null verschiedenen $(\mathfrak{X}\,\mathfrak{x})$ und $(\mathfrak{x}\,\mathfrak{X})$ gleich derselben Konstanten r sind. Aus Symmetrie- und Dualitätsgründen braucht dazu nur noch z.B. $(\mathfrak{A}\,\mathfrak{c}) = (\mathfrak{B}\,\mathfrak{c})$ bewiesen zu werden. Das geht mit der Folgerung von Lemma 3 und den oben gefundenen Beziehungen: $(\mathfrak{A}\,\mathfrak{c}) = (\mathfrak{A}\,\mathfrak{b}) = (\mathfrak{c}\,\mathfrak{B}) = (\mathfrak{c}\,\mathfrak{A}) = (\mathfrak{B}\,\mathfrak{a}) = (\mathfrak{B}\,\mathfrak{c})$. Aus Lemma 4, (ii) folgt nun wegen $\lambda = 1$, daß $|\mathfrak{X}| = |\mathfrak{x}| = r^2$, also $3r^2 = n^2 + n + 1$, ferner aus (G 2) und Voraussetzung (b): $2r = n + 1$. Kombination dieser beiden Beziehungen aber ergibt $n = 1$, wonach alle Γ-Klassen aus nur einem Element bestehen würden, im Widerspruch zu (*). Also gibt es eine Klasse mit nur einem Element, z.B. die Klasse $\mathfrak{a}$. Alle nicht auf der einzigen Geraden

von $\mathfrak{a}$ liegenden Punkte gehören sodann zu nicht mit $\mathfrak{a}$ inzidenten Punktklassen. Da es genau n^2 solche Punkte und genau eine solche Punktklasse, nämlich $\mathfrak{A}$, gibt, folgt daraus die Behauptung des Lemma 6.

Beweis von Satz 7. Ist zunächst Γ eine taktische Zerlegung mit einer Klasse — o.B.d.A. einer Punktklasse $\mathfrak{P}$ —, die n^2 Elemente enthält, so folgt wie beim Beweis von Lemma 5 mit Benutzung von (4), daß es genau eine Geradenklasse $\mathfrak{g}$ gibt, die mit $\mathfrak{P}$ nicht inzidiert, und diese Geradenklasse besteht aus einem Element. Es ist nun klar, daß die von $\mathfrak{P}$ verschiedenen Punktklassen, die ja alle aus kollinearen Punkten bestehen müssen, sowohl unter sich als auch mit $\mathfrak{P}$ eindeutige Verbindungsklassen haben. Andernfalls nämlich müßte es außer der einzigen Geraden von $\mathfrak{g}$ noch andere Verbindungsgeraden von nicht zu $\mathfrak{P}$ gehörigen Punkten geben, was in einer projektiven Ebene nicht möglich ist.

Sei nun umgekehrt Γ eine nichttriviale taktische Zerlegung mit eindeutigen Schnitt- und Verbindungsklassen. Wegen $t(\Gamma)>2$ und Lemma 4 ist $\mathfrak{E}/\Gamma$ entweder vom Typ der Fig. 2 oder vom Typ der Fig. 3. Im ersteren Falle ist die Existenz einer Γ-Klasse mit n^2 Elementen durch Lemma 5, im letzteren durch Lemma 6 gesichert. Damit ist Satz 7 bewiesen.

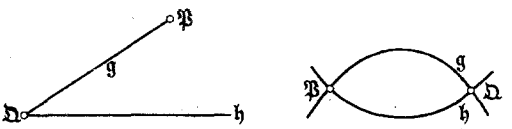

Fig. 4 a u. b

Satz 6 und 7 geben vollständige Auskunft über alle möglichen Typen von taktischen Zerlegungen Γ von projektiven Ebenen, deren abgeleitete Strukturen wieder (eventuell ausgeartete) projektive Ebenen sind, vorausgesetzt, daß $t(\Gamma)>2$ ist. Es liegt nun nahe, jetzt auch noch den Fall $t=2$ zu untersuchen (der Fall $t=1$ ist natürlich uninteressant) und festzustellen, unter welchen Umständen auch hier Schnitte und Verbindungen eindeutig sind. Für die abgeleitete Struktur $\mathfrak{E}/\Gamma$ sind offenbar nur noch zwei Typen möglich (vgl. Fig. 4), von denen der erste eindeutige Schnitte und Verbindungen hat.

Wir zeigen, daß in vielen Fällen auch für $t=2$ noch die Aussage des Satzes 7 von der Existenz einer Klasse mit n^2 Elementen erhalten bleibt.

Satz 8. *Sei Γ eine taktische Zerlegung einer projektiven Ebene der Primzahlordnung p derart, daß $t(\Gamma)=2$. Dann sind Schnitte und Verbindungen in $\mathfrak{E}/\Gamma$ eindeutig, und eine der Γ-Klassen enthält n^2 Elemente.*

Beweis. Es seien $\mathfrak{P}$, $\mathfrak{Q}$, $\mathfrak{g}$, $\mathfrak{h}$ die Γ-Klassen. Dann gilt nach Lemma 1, Gl. (10) und wegen $n=p$, daß eine der Zahlen $|(\mathfrak{P}\,\mathfrak{g})-(\mathfrak{P}\,\mathfrak{h})|$, $|(\mathfrak{g}\,\mathfrak{P})-(\mathfrak{g}\,\mathfrak{Q})|$ gleich p, die andere gleich 1 ist. O.B.d.A. nehmen wir $(\mathfrak{P}\,\mathfrak{g})-(\mathfrak{P}\,\mathfrak{h})=p$ und $(\mathfrak{g}\,\mathfrak{P})-(\mathfrak{g}\,\mathfrak{Q})=1$ an. Nach (G 2) ist dann $p=(\mathfrak{P}\,\mathfrak{g})-(\mathfrak{P}\,\mathfrak{h})=p+1-(\mathfrak{Q}\,\mathfrak{g})-(\mathfrak{P}\,\mathfrak{h})$, $(\mathfrak{P}\,\mathfrak{h})+(\mathfrak{Q}\,\mathfrak{g})=1$. Da sowohl $(\mathfrak{P}\,\mathfrak{h})$ wie $(\mathfrak{Q}\,\mathfrak{g})$ nicht negativ und ganzzahlig sind, muß eine dieser Zahlen verschwinden und die andere $=1$ sein. Es folgt, daß Schnitte und Verbindungen in $\mathfrak{E}/\Gamma$ eindeutig sind, d.h. $\mathfrak{E}/\Gamma$ ist vom Typ der Fig. 4a. Denn in einer Struktur vom Typ der Fig. 4b müssen alle $(\mathfrak{X}\,\mathfrak{x})$ und $(\mathfrak{x}\,\mathfrak{X})$ von Null verschieden sein, da jede Klasse mit jeder andersartigen inzidiert.

Ist nun $(\mathfrak{P}\mathfrak{h}) = 1$ und $(\mathfrak{Q}\mathfrak{g}) = 0$, so ist wegen (G 1) auch $(\mathfrak{g}\mathfrak{Q}) = 0$, und es folgt $(\mathfrak{g}\mathfrak{P}) = 1$, da $(\mathfrak{g}\mathfrak{P}) - (\mathfrak{g}\mathfrak{Q}) = 1$. Also ist $|\mathfrak{g}| = (\mathfrak{g}\mathfrak{P})(\mathfrak{P}\mathfrak{h}) = 1$ nach Lemma 3, und es folgt $|\mathfrak{g}| = 1$. Ist $(\mathfrak{P}\mathfrak{h}) = 0$ und $(\mathfrak{Q}\mathfrak{g}) = 1$, so folgt $(\mathfrak{h}\mathfrak{P}) = 0$ wegen (G 1), und daraus $(\mathfrak{g}\mathfrak{P}) = p + 1$ wegen (G 2). Nun folgt weiter $p + 1 = (\mathfrak{g}\mathfrak{Q}) + (\mathfrak{h}\mathfrak{Q}) = (\mathfrak{g}\mathfrak{P}) - 1 + (\mathfrak{h}\mathfrak{Q}) = p + (\mathfrak{h}\mathfrak{Q})$, also ist $(\mathfrak{h}\mathfrak{Q}) = 1$, und Lemma 3 ergibt nun wieder $|\mathfrak{h}| = (\mathfrak{h}\mathfrak{Q})(\mathfrak{Q}\mathfrak{g}) = 1$, also $|\mathfrak{h}| = 1$. In jedem Falle enthält also eine Γ-Klasse nur ein Element, woraus wie beim Beweis von Lemma 6 die Existenz einer Klasse mit n^2-Elementen folgt, q.e.d.

Wir zeigen als nächstes, daß im allgemeinen aus $t(\Gamma) = 2$ nicht $\lambda = 1$ zu folgen braucht. Dazu betrachte man einen beliebigen endlichen dreidimensionalen projektiven Raum $\mathfrak{R}$. Man überzeugt sich leicht, daß $\mathfrak{R}$ als λ-Ebene $\mathfrak{E}$ aufgefaßt werden kann, wenn man unter den Punkten von $\mathfrak{E}$ die Punkte von $\mathfrak{R}$ und unter den „Geraden" von $\mathfrak{E}$ die Ebenen von $\mathfrak{R}$ versteht, während Inzidenz in $\mathfrak{E}$ durch Inzidenz in $\mathfrak{R}$ erklärt ist. Für die so erhaltene λ-Ebene $\mathfrak{E}$ gilt $v = q^3 + q^2 + q + 1$, wobei q eine Primzahlpotenz ist, ferner $k = q^2 + q + 1$, $\lambda = q + 1$ und $n = q^2$. Insbesondere ist also $\lambda > 1$; aber es gibt eine taktische Zerlegung Γ mit $t(\Gamma) = 2$: Man betrachte einen festen Punkt P und definiere Punktklassen:

$$\mathfrak{P} = \{P\}, \quad \mathfrak{Q} = \{\text{Alle Punkte} \neq P\}$$

und „Geraden"klassen:

$$\mathfrak{g} = \{\text{Alle mit } P \text{ inzidenten Ebenen von } \mathfrak{R}\},$$

$$\mathfrak{h} = \{\text{Alle übrigen Ebenen von } \mathfrak{R}\}.$$

Es ist leicht zu sehen, daß diese Klasseneinteilung tatsächlich eine taktische Zerlegung von $\mathfrak{E}$ definiert. Die Werte der Zahlen $(\mathfrak{X}\mathfrak{x})$ und $(\mathfrak{x}\mathfrak{X})$ sind in folgendem Schema zusammengestellt:

$(\mathfrak{X}\mathfrak{x})$	$\mathfrak{g}$	$\mathfrak{h}$
$\mathfrak{P}$	1	0
$\mathfrak{Q}$	$q^2 + q$	$q^2 + q + 1$

$(\mathfrak{x}\mathfrak{X})$	$\mathfrak{P}$	$\mathfrak{Q}$
$\mathfrak{g}$	$q^2 + q + 1$	$q + 1$
$\mathfrak{h}$	0	q^2

Wir zeigen nun weiter, daß die Aussagen von Satz 8 für zusammengesetzte n nicht mehr allgemein richtig sind. Wir werden für die beiden in Fig. 4 illustrierten Typen von abgeleiteten Strukturen $\mathfrak{E}/\Gamma$ mit $t(\Gamma) = 2$ Beispiele angeben, bei denen jede Klasse mehr als ein Element enthält. Die beiden zu behandelnden Klassen von Beispielen rühren von Teilebenen bzw. von Ovalen endlicher projektiver Ebenen her.

2.4. Durch Teilebenen projektiver Ebenen definierte taktische Zerlegungen

Es sei $\mathfrak{E}$ eine endliche nichtausgeartete projektive Ebene der Ordnung n und $\mathfrak{E}'$ eine nichtausgeartete projektive Teilebene von $\mathfrak{E}$. Die Teilebene $\mathfrak{E}'$ ist dann ebenfalls endlich; ihre Ordnung bezeichnen wir mit m. Für diese

Situation gibt es viele Beispiele: Jede Ebene $\mathfrak{E}$ über einem Galois-Feld der Ordnung p^r, wo $r>1$, besitzt eigentliche Teilebenen der Ordnung p^d, mit $d|r$. Wir unterscheiden zwei Fälle:

(I) *Jeder Punkt von $\mathfrak{E}$ ist mit einer Geraden von $\mathfrak{E}'$ inzident.*

Wir definieren eine taktische Zerlegung Γ von $\mathfrak{E}$ folgendermaßen: $\mathfrak{P}=$ {Punkte von $\mathfrak{E}'$}, $\mathfrak{Q}=$ {alle übrigen Punkte}, $\mathfrak{g}=$ {Geraden von $\mathfrak{E}'$}, $\mathfrak{h}=$ {alle übrigen Geraden}. Es ist klar, daß die so definierte Klasseneinteilung eine taktische Zerlegung ist; die Werte der Zahlen $(\mathfrak{X}\mathfrak{x})$ und $(\mathfrak{x}\mathfrak{X})$ sind in nachstehendem Schema zusammengestellt:

$(\mathfrak{X}\mathfrak{x})$	$\mathfrak{g}$	$\mathfrak{h}$
$\mathfrak{P}$	$m+1$	1
$\mathfrak{Q}$	$n-m$	n

$(\mathfrak{x}\mathfrak{X})$	$\mathfrak{P}$	$\mathfrak{Q}$
$\mathfrak{g}$	$m+1$	1
$\mathfrak{h}$	$n-m$	n

Daß z.B. $(\mathfrak{P}\mathfrak{h})=1$ ist, folgt so: $(\mathfrak{P}\mathfrak{h})$ ist >0 nach Voraussetzung (I), und wäre $(\mathfrak{P}\mathfrak{h})>1$, so wäre jede $\mathfrak{h}$-Gerade Verbindungsgerade von Punkten von $\mathfrak{E}'$, gehörte also selbst zu $\mathfrak{E}'$, entgegen unserer Annahme.

Aus den Grundgleichungen folgt nun der bekannte Satz (vgl. BAER [2], theorem 5), daß $m^2=n$ sein muß: $|\mathfrak{P}|$ ist die Anzahl der Punkte der projektiven Ebene $\mathfrak{E}'$, also gleich m^2+m+1. Andererseits ist nach (G 4a) auch

$$|\mathfrak{P}| = \sum_{\mathfrak{x}} (\mathfrak{P}\mathfrak{x})(\mathfrak{x}\mathfrak{Q}) = m+1+n,$$

also folgt $m^2=n$. Umgekehrt hat jede Teilebene der Ordnung m mit $m^2=n$ die Eigenschaft (I). Die abgeleitete Struktur $\mathfrak{E}/\Gamma$ ist vom zweiten der in Fig. 4 dargestellten Typen.

(II) *Es gibt Punkte von $\mathfrak{E}$, die auf keiner Geraden von $\mathfrak{E}'$ liegen.*

Wir definieren wieder eine taktische Zerlegung von $\mathfrak{E}$: Die Punktklassen sind $\mathfrak{P}=$ {Punkte von $\mathfrak{E}'$}, $\mathfrak{Q}=$ {Punkte, die nicht zu $\mathfrak{E}'$ gehören, aber auf Geraden von $\mathfrak{E}'$ liegen}, $\mathfrak{R}=$ {alle übrigen Punkte}, und die Geradenklassen dual: $\mathfrak{g}=$ {Geraden von $\mathfrak{E}'$}, $\mathfrak{h}=$ {Geraden, die nicht zu $\mathfrak{E}'$ gehören, aber durch Punkte von $\mathfrak{E}'$ gehen}, $\mathfrak{k}=$ {alle übrigen Geraden}. Wieder ist klar, daß so eine taktische Zerlegung definiert wird; die Zahlen $(\mathfrak{X}\mathfrak{x})$ und $(\mathfrak{x}\mathfrak{X})$ sind in nachstehendem Schema zusammengestellt:

$(\mathfrak{X}\mathfrak{x})$	$\mathfrak{g}$	$\mathfrak{h}$	$\mathfrak{k}$
$\mathfrak{P}$	$m+1$	1	0
$\mathfrak{Q}$	$n-m$	m^2	m^2+m+1
$\mathfrak{R}$	0	$n-m^2$	$n-m^2-m$

$(\mathfrak{x}\mathfrak{X})$	$\mathfrak{P}$	$\mathfrak{Q}$	$\mathfrak{R}$
$\mathfrak{g}$	$m+1$	1	0
$\mathfrak{h}$	$n-m$	m^2	m^2+m+1
$\mathfrak{k}$	0	$n-m^2$	$n-m^2-m$

Da $(\mathfrak{R}\mathfrak{k})\geq 0$ sein muß, folgt $m^2+m\leq n$. Diese Tatsache ist auf anderem Wege auch von BRUCK gefunden worden (vgl. [3], Lemma 3.1). Die von BRUCK angegebene Formel $(n-m)(n-m^2)$ für die Anzahl der mit keiner

Geraden von $\mathfrak{E}'$ inzidenten Punkte von $\mathfrak{E}$ folgt hier unmittelbar durch Anwendung von (G 4a):

$$|\mathfrak{R}| = \sum_{\mathfrak{x}} (\mathfrak{R}\,\mathfrak{x})\,(\mathfrak{x}\,\mathfrak{Q}) = (n-m)\,(n-m^2).$$

Fig. 5 zeigt die beiden möglichen Typen von abgeleiteten Strukturen $\mathfrak{E}/\Gamma$ im Falle (II). Die Existenz von abgeleiteten Strukturen des Typs der Fig. 5a ist gesichert, denn es gibt projektive Ebenen mit Teilebenen, für die (II) gilt und $m^2+m<n$ ist. Wir haben also ein Beispiel einer abgeleiteten Struktur, in der die Zahlen $[\mathfrak{X}, \mathfrak{Y}]$, $[\mathfrak{x}, \mathfrak{y}]$, $[\mathfrak{X}]$, $[\mathfrak{x}]$ nicht alle gleich sind (vgl. S. 69). Da man keine projektiven Ebenen kennt, deren Ordnung eine Zahl des Typs $m(m+1)$ ist, bleibt die Frage offen, ob eine solche Ebene Teilebenen der

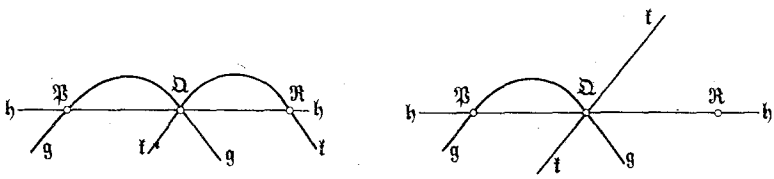

Fig. 5 a u. b

Ordnung m besitzen kann. Die Frage der Existenz von abgeleiteten Strukturen des Typs der Fig. 5b ist also auf diese Weise nicht zu entscheiden. Man sieht aber leicht, daß die abgeleitete Struktur der folgendermaßen definierten taktischen Zerlegung einer endlichen projektiven Ebene vom Typ der Fig. 5b ist:

Punktklassen: $\mathfrak{R} = \{$ein fester Punkt $R\}$,
$\mathfrak{P} = \{$alle Punkte einer festen Geraden g, die nicht durch R geht$\}$,
$\mathfrak{Q} = \{$alle übrigen Punkte$\}$.

Geradenklassen: $\mathfrak{g} = \{g\}$,
$\mathfrak{h} = \{$alle Geraden durch $R\}$,
$\mathfrak{k} = \{$alle übrigen Geraden$\}$.

2.5. Durch Ovale definierte taktische Zerlegungen

Wir wenden uns nun einer anderen Klasse vin Beispielen zu. Ein *Oval* einer endlichen projektiven Ebene der Ordnung n ist eine Menge von $n+1$ Punkten der Ebene, von denen keine drei kollinear sind. Von den $n+1$ Geraden durch einen beliebigen Ovalpunkt müssen also n noch einen weiteren Punkt des Ovals enthalten, jede solche Gerade heißt eine *Sekante*. Es folgt, daß durch jeden Ovalpunkt genau eine Gerade geht, die außer diesem keine weiteren Ovalpunkte enthält, jede solche Gerade heißt eine *Tangente*. Die Anzahl der Tangenten ist $n+1$, die der Sekanten gleich $n(n+1)/2$, also bleiben noch $n(n-1)/2$ weitere Geraden, diese enthalten keine Ovalpunkte und werden *Passanten* genannt.

Wir wollen die Ovale zur Definition gewisser taktischer Zerlegungen heranziehen. Dabei unterscheiden wir wieder zwei Fälle:

(I') *n ist gerade.*

In diesem Falle hat QVIST in [*12*], theorem 5, S. 10, gezeigt, daß alle Tangenten eines Ovals durch einen Punkt gehen müssen. Dieser Punkt bildet zusammen mit den $n+1$ Ovalpunkten eine Menge $\mathfrak{P}$ von $n+2$ Punkten, von denen keine drei kollinear sind. (Man sagt statt dessen auch: die Punkte von $\mathfrak{P}$ befinden sich „in allgemeiner Lage".) QVIST [*12*] zeigt weiter, daß es $n+2$ Punkte in allgemeiner Lage in einer projektiven Ebene der Ordnung n höchstens dann geben kann, wenn n gerade ist. Daß es tatsächlich Ebenen gerader Ordnung n mit $n+2$ Punkten in allgemeiner Lage gibt, zeigt folgendes

Beispiel. *Es sei $\mathfrak{E}$ eine desarguessche Ebene gerader Ordnung n, d.h. eine Ebene über einem Galois-Feld der Charakteristik 2. Sodann befinden sich die $n+2$ Punkte $(1:0:0)$, $(0:1:0)$, $(x:x^2:1)$ in allgemeiner Lage.*

Denn da die Abbildung $x \to x^2$ in jedem endlichen Körper der Charakteristik 2 ein Automorphismus ist, haben zwei verschiedene Punkte $(x:x^2:1)$, $(y:y^2:1)$ verschiedene erste *und* verschiedene zweite Koordinaten, sind also weder mit $(1:0:0)$ noch mit $(0:1:0)$ kollinear. Und wären drei Punkte $(x:x^2:1)$, $(y:y^2:1)$, $(z:z^2:1)$ mit $x \neq y \neq z \neq x$ kollinear, so würde für den Koeffizienten m der Gleichung $m x_1 + x_2 + b x_3 = 0$ ihrer Verbindungsgeraden folgen:

$$m = (y^2 - x^2)(y - x)^{-1} = (z^2 - x^2)(z - x)^{-1},$$

d.h. $y = z$, ein Widerspruch.

Es sei nun $\mathfrak{E}$ eine projektive Ebene gerader Ordnung und $\mathfrak{P}$ eine Menge von $n+2$ Punkten in allgemeiner Lage von $\mathfrak{E}$. Weiter sei $\mathfrak{Q}$ die Menge der n^2-1 nicht zu $\mathfrak{P}$ gehörigen Punkte, $\mathfrak{g}$ die Menge der Verbindungsgeraden von $\mathfrak{P}$-Punkten und $\mathfrak{h}$ die Menge der nicht zu $\mathfrak{g}$ gehörigen Geraden. Sodann bilden $\mathfrak{P}$, $\mathfrak{Q}$, $\mathfrak{g}$, $\mathfrak{h}$ eine taktische Zerlegung von $\mathfrak{E}$, mit folgenden Werten für die $(\mathfrak{X}\,\mathfrak{x})$, $(\mathfrak{x}\,\mathfrak{X})$:

$(\mathfrak{X}\,\mathfrak{x})$	$\mathfrak{g}$	$\mathfrak{h}$	$(\mathfrak{x}\,\mathfrak{X})$	$\mathfrak{P}$	$\mathfrak{Q}$
$\mathfrak{P}$	2	0	$\mathfrak{g}$	$n+1$	$(n+2)/2$
$\mathfrak{g}$	$n-1$	$n+1$	$\mathfrak{h}$	0	$n/2$

Wir verifizieren nur, daß $(\mathfrak{g}\,\mathfrak{Q}) = (n+2)/2$ ist. [Daraus folgt sofort $(\mathfrak{h}\,\mathfrak{Q}) = n/2$, und die übrigen Beweise sind ganz einfach.] Wir müssen zeigen, daß durch jeden nicht zu $\mathfrak{P}$ gehörigen Punkt Q genau $(n+2)/2$ Verbindungsgeraden von $\mathfrak{P}$-Punkten gehen, und dazu genügt der Nachweis, daß auf jeder Verbindungsgeraden von Q mit einem Punkt $P \in \mathfrak{P}$ noch ein weiterer Punkt $P' \neq P$ von $\mathfrak{P}$ liegt. Das aber ist klar: andernfalls blieben für die $n+1$ von P verschiedenen Punkte von $\mathfrak{P}$ nur n Geraden durch P, auf denen sie liegen müßten. Nach dem Schubfachschluß würde folgen, daß es eine Gerade durch P mit zwei von P verschiedenen Punkten von $\mathfrak{P}$ geben müßte. Das aber widerspricht der Annahme, daß die Punkte von $\mathfrak{P}$ sich in allgemeiner Lage befinden.

Die nach der oben erklärten taktischen Zerlegung Γ abgeleitete Struktur $\mathfrak{E}/\Gamma$ ist, da $(\mathfrak{P}\mathfrak{h})=0$, vom Typ der Fig. 4a, sie besitzt aber im allgemeinen keine Klassen mit nur einem Element; vielmehr ist $|\mathfrak{P}|=n+2$, $|\mathfrak{Q}|=n^2-1$, $|\mathfrak{g}|=(n+1)(n+2)/2$, $|\mathfrak{h}|=n(n-1)/2$. Diese Zahlen sind bei $n\geqq 4$ alle größer als 1. Also kann es bei $n\geqq 4$ auch keine Klasse mit n^2 Elementen geben.

(II′) *n ist ungerade.*

Für diesen Fall hat QVIST gezeigt ([*12*], theorem 3, S. 8), daß durch einen Schnittpunkt zweier Tangenten eines Ovals keine weiteren Tangenten mehr gehen können. Die Menge der Punkte von $\mathfrak{E}$ zerfällt also in drei Klassen: Die Klasse $\mathfrak{P}$ der Ovalpunkte, die Klasse $\mathfrak{Q}$ der *äußeren Punkte*, das sind die Tangentenschnittpunkte, und die Klasse $\mathfrak{R}$ aller übrigen Punkte; diese heißen *innere Punkte*, durch sie geht keine Tangente. Nennen wir nun die Klasse der Tangenten $\mathfrak{g}$, die der Sekanten $\mathfrak{h}$, und die der Passanten $\mathfrak{k}$, so bilden $\mathfrak{P}$, $\mathfrak{Q}$, $\mathfrak{R}$, $\mathfrak{g}$, $\mathfrak{h}$, $\mathfrak{k}$ eine taktische Zerlegung mit folgenden Zahlen $(\mathfrak{X}\mathfrak{x})$ und $(\mathfrak{x}\mathfrak{X})$:

$(\mathfrak{X}\mathfrak{x})$	$\mathfrak{g}$	$\mathfrak{h}$	$\mathfrak{k}$
$\mathfrak{P}$	1	2	0
$\mathfrak{Q}$	n	$(n-1)/2$	$(n+1)/2$
$\mathfrak{R}$	0	$(n-1)/2$	$(n+1)/2$

$(\mathfrak{x}\mathfrak{X})$	$\mathfrak{P}$	$\mathfrak{Q}$	$\mathfrak{R}$
$\mathfrak{g}$	1	2	0
$\mathfrak{h}$	n	$(n-1)/2$	$(n+1)/2$
$\mathfrak{k}$	n	$(n-1)/2$	$(n+1)/2$

Die abgeleitete Struktur ist wieder vom Typ der Fig. 5a. Wir haben also hier noch ein Beispiel dafür, daß die abgeleiteten Strukturen ganz verschiedener Typen von taktischen Zerlegungen dieselben sein können.

3. Die Matrizen einer taktischen Zerlegung

3.1. Die Matrix-Grundgleichungen

Es sei $\mathfrak{E}$ eine beliebige λ-Ebene der Ordnung n und Γ eine taktische Zerlegung von $\mathfrak{E}$. Wir numerieren die Γ-Klassen in willkürlicher Weise von 1 bis $t=t(\Gamma)$: $\mathfrak{P}_1, \mathfrak{P}_2, \ldots, \mathfrak{P}_t$ seien die Punktklassen und $\mathfrak{g}_1, \ldots, \mathfrak{g}_t$ die Geradenklassen. Um dauernde Wiederholungen zu vermeiden, wollen wir in diesem Abschnitt stets voraussetzen, daß $t>1$ ist. Wir definieren vier Matrizen P, G, A, B folgendermaßen (i ist der Zeilen-, k der Spaltenindex, und δ_{ik} das Kronecker-Symbol):

$$P=(|\mathfrak{P}_i|\,\delta_{ik}), \qquad G=(|\mathfrak{g}_i|\,\delta_{ik}).$$

$$A=((\mathfrak{P}_i\,\mathfrak{g}_k)), \qquad B=((\mathfrak{g}_i\,\mathfrak{P}_k)).$$

Diese Matrizen nennen wir die Γ-Matrizen; sie sind sämtlich t-reihige quadratische Matrizen. Beispiele für Γ-Matrizen A, B sind im zweiten Abschnitt schon aufgetreten (vgl. S. 75, 76, 76, 78, 79). Wir merken an, daß im Falle $t=v$, d.h. wenn jede Γ-Klasse aus einem Element besteht, die Matrix A gerade die bekannte Inzidenzmatrix von $\mathfrak{E}$ und B ihre Transponierte A^T ist.

Wir werden in diesem Paragraphen Beziehungen herleiten, die zwischen den Γ-Matrizen jeder taktischen Zerlegung Γ bestehen müssen, nämlich die folgenden

Matrix-Grundgleichungen

(M 1) $$GA^T = BP, \qquad PB^T = AG,$$

(M 2) $$AB = \lambda PJ + nE, \qquad BA = \lambda GJ + nE.$$

Hier bedeutet E die t-reihige Einheitsmatrix und J diejenige t-reihige quadratische Matrix, deren sämtliche Elemente gleich Eins sind.

(M 3) $$AGA^T = \lambda PJP + nP, \quad BPB^T = \lambda GJG + nG.$$

Die Beweise ergeben sich sofort aus den Grundgleichungen (G 1) und (G 4): Die Beziehung (G 1) besagt $(\mathfrak{P}_i \mathfrak{g}_k) \mid \mathfrak{g}_k \mid = (\mathfrak{g}_k \mathfrak{P}_i) \mid \mathfrak{P}_i \mid$ für alle i, k. In Matrixform geschrieben heißt das gerade $AG = (BP)^T$, und die Beziehungen (M 1) folgen nun sofort aus der Tatsache, daß P und G Diagonalmatrizen, also gleich ihren Transponierten sind. Die Gln. (M 2) ergeben sich ebenso direkt aus (G 4a) und (G 4b). Die Beziehungen (M 3) schließlich folgen aus (M 1) durch Linksmultiplikation mit A bzw. B und Benutzung von (M 2).

Matrizen mit ganzzahligen Elementen können auch als Matrizen über beliebigen Körpern aufgefaßt werden. Wir zeigen:

Lemma 7. *Ist Γ eine taktische Zerlegung einer λ-Ebene der Ordnung n, so sind die Γ-Matrizen A und B über allen Körpern regulär, deren Charakteristik kein Teiler von $n(n+\lambda)$ ist.*

Um das zu beweisen, genügt es zu zeigen, daß das Produkt der Determinanten von A und B über solchen Körpern von Null verschieden ist. Nun ist aber

(11) $$\det A \det B = n^{t-1}(n+\lambda)^2,$$

was man z.B. aus (M 2) herleiten kann: Man subtrahiere die letzte Spalte der Matrix AB von allen anderen und addiere sodann die $t-1$ ersten Zeilen zur letzten. Es ergibt sich eine Dreiecksmatrix mit $t-1$ Diagonalstellen n und der letzten Diagonalstelle $n + \lambda \sum_{i=1}^{t} \mid \mathfrak{P}_i \mid$; dieser Ausdruck ist wegen (G 3) und (3) gleich $(n+\lambda)^2$. Also folgt (11), und das Lemma 7 ist bewiesen.

Wir merken an, daß A und B also insbesondere über dem Körper der rationalen Zahlen regulär sind.

3.2. Zahlentheoretische Eigenschaften der $|\mathfrak{X}|, |\mathfrak{x}|$

In diesem Paragraphen ziehen wir einige erste elementare Folgerungen aus den Matrixgrundgleichungen. Wir definieren zunächst D als den größten gemeinsamen Teiler aller $|\mathfrak{X}|$, d als den g.g.T. aller $|\mathfrak{x}|$, wobei wie immer $\mathfrak{X}$ und $\mathfrak{x}$ die Klassen einer taktischen Zerlegung sind.

Satz 9. *Es sei $\mathfrak{E}$ eine λ-Ebene der Ordnung n und Γ eine taktische Zerlegung von $\mathfrak{E}$. Sodann gilt:*

(a) *Ist p eine Primzahl, die weder n noch $k = n + \lambda$ teilt, so geht p in ebensovielen $|\mathfrak{X}|$ wie $|\mathfrak{x}|$ auf. Insbesondere gilt $p \mid D$ genau dann, wenn $p \mid d$ gilt, und in diesem Falle geht p in D und d gleich oft auf.*

(b) *Sind v und k teilerfremd, so ist $D=d$.*

(c) *Gibt es eine Primzahl p, die eine der Zahlen D, d teilt und deren Quadrat nicht in n aufgeht, so teilt sie auch die andere.*

(d) *Die Zahl $n^{t-1}\prod_{\mathfrak{X}}|\mathfrak{X}|\prod_{\mathfrak{x}}|\mathfrak{x}|$ ist stets eine Quadratzahl.*

Beweis. Über jedem Körper, über dem A und B reguläre Matrizen sind, haben P und $\lambda GJG+nG=BAG$ sowie G und $\lambda PJP+nP=ABP$ wegen (M3) gleiche Ränge. Das sind nach Lemma 7 gerade die Körper, deren Charakteristik Null oder eine Primzahl ist, die weder n noch k teilt. AB und BA sind über jedem solchen Körper regulär, also folgt Gleichheit der Ränge von P und G. Da P und G Diagonalmatrizen sind, besagt die Gleichheit ihrer Ränge Gleichheit der Anzahlen von Null verschiedener ihrer Elemente. Ist also p eine weder n noch k teilende Primzahl, so folgt: Es gibt ebensoviele $|\mathfrak{X}|\not\equiv 0 \bmod p$ wie $|\mathfrak{x}|\not\equiv 0 \bmod p$. Also geht p in ebensovielen $|\mathfrak{X}|$ wie $|\mathfrak{x}|$ auf, und insbesondere geht p genau dann in allen $|\mathfrak{X}|$ auf, wenn p in allen $|\mathfrak{x}|$ aufgeht. Ist das der Fall, und ist p^r die größte in allen $|\mathfrak{X}|$ und in allen $|\mathfrak{x}|$ aufgehende Potenz von p, so sind die Zahlen $p^{-r}|\mathfrak{X}|$, $p^{-r}|\mathfrak{x}|$ alle noch ganz. Also sind die Matrizen $p^{-r}P$ und $p^{-r}G$ ebenso wie P und G ganzzahlig. Es folgt nun wie oben, daß $p^{-r}P$ und $p^{-r}G$ die gleichen Ränge haben. Wegen der Maximaleigenschaft von r gibt es unter den Zahlen $p^{-r}|\mathfrak{X}|$, $p^{-r}|\mathfrak{x}|$ mindestens eine, die nicht durch p teilbar ist, d.h. mindestens eine der Matrizen $p^{-r}P$, $p^{-r}G$ hat von Null verschiedenen Rang. Dann müssen sie aber beide von Null verschiedenen Rang haben, d.h. es gibt sowohl ein $p^{-r}|\mathfrak{X}|\not\equiv 0 \bmod p$ als auch ein $p^{-r}|\mathfrak{x}|\not\equiv 0 \bmod p$. Also ist genau dann $p^r|D$, wenn $p^r|d$ gilt. Damit ist (a) bewiesen.

Nach (G3) sind sowohl D als auch d Teiler von v. Andererseits folgt aus (4), daß d ein Teiler aller $k|\mathfrak{X}|$, also ein Teiler von kD ist; dual dazu ist D ein Teiler von kd. Sind nun v und k teilerfremd, so folgt, daß D und d einander teilen, also gleich sind. Damit ist (b) bewiesen.

Sei p eine Primzahl, die d teilt, deren Quadrat aber kein Teiler von n ist. Wäre p kein Teiler von D, so gäbe es eine Punktklasse $\mathfrak{P}$ mit $p\nmid|\mathfrak{P}|$; wegen (4) müßte dann $p|k$ folgen. Daraus und aus der oben bewiesenen Beziehung $d|v$ würde mit (2) weiter $p|\lambda$ und daraus $p^2|(k^2-\lambda v)$ folgen; das aber ist ein Widerspruch gegen (3), wonach $k^2-\lambda v=n$ ist. Damit ist (c) bewiesen.

Aus (M1) erhält man durch Multiplikation mit BP und Determinantenbildung unter Berücksichtigung von (11) die Gleichung $n^{t-1}k^2\det PG=(\det BP)^2$. Daraus folgt wegen

$$\det PG=\prod_{\mathfrak{X}}|\mathfrak{X}|\prod_{\mathfrak{x}}|\mathfrak{x}|$$

sofort die Behauptung (d), und damit ist Satz 9 vollständig bewiesen.

Wir bemerken noch, daß die Voraussetzung von (b) im Falle $\lambda=1$ der projektiven Ebenen immer erfüllt ist. Für jede taktische Zerlegung einer endlichen projektiven Ebene ist also der g.g.T. aller $|\mathfrak{X}|$ gleich dem aller $|\mathfrak{x}|$. Ferner bemerken wir, daß aus (d) der bekannte Satz folgt (vgl. etwa HALL [7],

S. 66), daß die Ordnung einer λ-Ebene mit geradem v ein Quadrat sein muß; dazu betrachte man einfach die triviale Zerlegung mit $|\mathfrak{X}| = |\mathfrak{x}| = \text{const} = 1$. Nennt man weiter eine taktischer Zerlegung Γ *symmetrisch*, wenn es eine Numerierung der Γ-Klassen derart gibt, daß $|\mathfrak{P}_i| = |\mathfrak{g}_i|$ ist für alle i (man vergleiche die Beispiele von S. 76, 76, 79), so folgt aus (d), daß die Zahl n^{t-1} bei symmetrischen Zerlegungen ein Quadrat sein muß. Insbesondere gilt also, in Verallgemeinerung des erwähnten Satzes:

Folgerung. *Besitzt eine λ-Ebene eine symmetrische taktische Zerlegung Γ mit geradzahligem $t(\Gamma)$, so ist ihre Ordnung n ein Quadrat.*

Die Aussagen des Satzes 9 werden besonders für den Fall interessant, daß alle $|\mathfrak{X}|$ und alle $|\mathfrak{x}|$ Potenzen derselben Primzahl p sind; eine solche taktische Zerlegung wollen wir eine *p-Zerlegung* nennen. Dieser Fall tritt z.B. dann ein, wenn die Zerlegung gemäß Satz 1 von einer p-Gruppe von Kollineationen herrührt: Wegen der Beziehung (6) von S. 65 müssen alle $|\mathfrak{X}|$ und alle $|\mathfrak{x}|$ Teiler der Gruppenordnung sein. Ein $|\mathfrak{X}|$ bzw. $|\mathfrak{x}|$, welches nicht durch p teilbar ist, muß also im Falle der p-Zerlegung gleich Eins sein. Bezeichnen wir mit F bzw. f die Anzahlen der $\mathfrak{X}$ bzw. $\mathfrak{x}$ mit $|\mathfrak{X}| = 1$ bzw. $|\mathfrak{x}| = 1$ (für den Fall, daß die Zerlegung von einer p-Gruppe von Kollineationen herrührt, sind F und f die Anzahlen von Fixpunkten bzw. Fixgeraden der Gruppe), so gilt für jede p-Zerlegung

$$F \equiv f \equiv v \bmod p, \tag{12}$$

wie man sofort aus (G3) folgert. Aus Satz 9 und der Kongruenz (12) erhält man nun weiter:

Satz 10. *Ist Γ eine p-Zerlegung einer λ-Ebene der Ordnung n, so gilt:*

(a') *Sind v und k teilerfremd, so ist genau dann $F = 0$, wenn $f = 0$ ist.*

(b') *Teilt p weder n noch k, oder ist $t(\Gamma) \leqq p$, so ist $F = f$.*

(c') *Ist $\lambda = 1$ und $F \neq f$, so ist p ein Teiler von n.*

Beweis. Sind v und k teilerfremd, so ist nach Satz 9 (b) der g.g.T. aller $|\mathfrak{X}|$ gleich dem aller $|\mathfrak{x}|$. In einer p-Zerlegung ist ein solcher g.g.T. genau dann gleich Eins, wenn es wirklich eine Klasse mit nur einem Element gibt. Also folgt (a'). Daß $F = f$ ist, wenn $p \nmid kn$, folgt aus Satz 9 (a). Sei nun $t(\Gamma) \leqq p$. Nach (12) gilt sodann $F = f + jp$, o.B.d.A. kann $j \geqq 0$ angenommen werden. Da $F \leqq t(\Gamma)$ ist, folgt weiter $f + jp \leqq p$, also ist entweder $j = 0$, in welchem Falle $F = f$, also nichts zu beweisen ist, oder $j = 1$, $f = 0$. Dieser letztere Fall kann aber nicht eintreten, denn dann würde $F = p = t$ folgen, was bedeuten würde, daß jede Punktklasse nur ein Element enthält. Das ist wegen Satz 2 mit $f = 0$ unverträglich.

Es bleibt (c') zu beweisen. Man überlegt sich leicht, daß im Falle $\lambda = 1$, also dem der projektiven Ebene, diejenigen Punkte und Geraden, welche Γ-Klassen für sich allein bilden, eine eventuell ausgeartete Teilebene bilden. Ist nun $F \neq f$, so muß diese Teilebene mindestens ein Element enthalten, ja nach (a') sogar mindestens einen Punkt und mindestens eine Gerade. [$k = n + 1$ und $v = n(n+1) + 1$ sind nämlich teilerfremd.] Ferner ist diese Teilebene

ausgeartet, und es gibt in ihr eine ausgezeichnete Gerade g, die mit allen Punkten, und einen ausgezeichneten Punkt P, der mit allen Geraden der Teilebene inzident ist. Die aus der ausgezeichneten Geraden g allein bestehende Klasse nennen wir $\mathfrak{g}$. Offenbar ist $|\mathfrak{g}| = 1$, also folgt aus (G1) für alle $\mathfrak{X}$ mit $(\mathfrak{X}\,\mathfrak{g}) \neq 0$, daß $(\mathfrak{X}\,\mathfrak{g}) = |\mathfrak{X}|$ ist. Da aber für alle $\mathfrak{X}$ entweder $|\mathfrak{X}| = 1$ oder $|\mathfrak{X}| \equiv 0 \bmod p$ gilt, ergibt sich aus (G2) die Kongruenz $F \equiv k = n+1 \bmod p$. Wegen (12) ist aber auch $F \equiv v = n(n+1)+1 \bmod p$. Subtraktion dieser beiden Kongruenzen ergibt $n^2 \equiv 0 \bmod p$, also ist $p \mid n$, q.e.d.

3.3. Eine notwendige Bedingung für die Existenz von taktischen Zerlegungen

Aus der Matrix-Grundgleichung (M3), die schon beim Beweis von Satz 9 wesentlich benutzt wurde, lassen sich noch sehr viel weitergehende Folgerungen ziehen. Betrachtet man nämlich z.B. die (symmetrischen) Matrizen G und $ABP = \lambda PJP + nP$ als Koeffizientenmatrizen zweier quadratischer Formen $g(x) = x^T G x$ und $h(y) = y^T ABPy$, wobei x und y unbestimmte t-stellige Spaltenvektoren sind, so folgt aus (M3), daß die Substitution $x = Ay$ die Formen g und h ineinander überführt. Man nennt solche Formen und auch die zugehörigen Matrizen *kongruent*, wenn die Substitutionsmatrix A regulär ist. Die Beziehungen (M3) liefern also wegen Lemma 7 die Kongruenz von G mit $\lambda PJP + nP$ und die Kongruenz von P mit $\lambda GJG + nG$ über dem Körper der rationalen Zahlen. MINKOWSKI und HASSE haben nun notwendige (und hinreichende, diese letztere Tatsache interessiert uns hier aber nicht) Bedingungen für die rationale Kongruenz von Matrizen aufgestellt. Diese Bedingungen können wir auf unseren Fall anwenden. Der Formulierung des (recht komplizierten) Ergebnisses dieser Anwendung der Hasse-Minkowskischen Theorie auf (M3) müssen wir einige Definitionen vorausschicken.

Es sei p eine ungerade Primzahl und a und b zwei beliebige von Null verschiedene ganze Zahlen. Sodann ist $a = a' p^\alpha$, $b = b' p^\beta$ für gewisse a', $b' \not\equiv 0 \bmod p$ und $\alpha, \beta \geqq 0$. Wir definieren das *p-Hilbert-Symbol* $(a, b)_p$ von a und b durch

$$(a, b)_p = (-1 \mid p)^{\alpha\beta} (a' \mid p)^\beta (b' \mid p)^\alpha;$$

hier bedeuten $(-1 \mid p)$, $(a' \mid p)$, $(b' \mid p)$ Legendresche quadratische Restsymbole. (Für andere Möglichkeiten der Definition des Hilbert-Symboles sowie für die Beweise der unten angegebenen Rechenregeln für Hilbert-Symbole vergleiche man etwa JONES [11], Chapter 2.) Das Hilbert-Symbol hat die folgenden Eigenschaften:

$$(13) \quad \begin{cases} (a, b)_p = (b, a)_p \\ (a r^2, b s^2)_p = (a, b)_p \\ (a, bc)_p = (a, b)_p (a, c)_p \\ (ar, br)_p = (a, b)_p (r, -ab)_p \\ (a, a-1)_p = (a, a)_p = (a, -1)_p \\ (a, 1)_p = 1. \end{cases}$$

Wir führen noch folgende für das weitere bequeme Abkürzungen ein:

$$\gamma_i = n + \lambda \sum_{j=1}^{i} |\mathfrak{g}_j|, \quad \pi_i = n + \lambda \sum_{j=1}^{i} |\mathfrak{P}_j| \qquad (i = 1, \ldots, t) \tag{14}$$

und bemerken, daß $\gamma_t = \pi_t = n + \lambda v = k^2 = (n+\lambda)^2$. Das angekündigte Hauptresultat lautet nun:

Satz 11. *Die Punktklassen $\mathfrak{P}_i$ und die Geradenklassen $\mathfrak{g}_i$ $(i = 1, \ldots, t > 1)$ einer taktischen Zerlegung einer λ-Ebene der Ordnung n genügen den folgenden Beziehungen:*

$$\text{(H)} \quad \begin{cases} (n, (-1)^{(t-1)(t-2)/2})_p \prod_{i=1}^{t-1} \left(\prod_{j=1}^{i} |\mathfrak{P}_j|, |\mathfrak{P}_{i+1}| \right)_p \left(\prod_{j=1}^{i} |\mathfrak{g}_j|, |\mathfrak{g}_{i+1}| \right)_p \\ \qquad = \left(n, \gamma_1 \prod_{i=1}^{t-1} |\mathfrak{g}_{i+1}|^t \right)_p \prod_{i=1}^{t-1} (\gamma_i, -|\mathfrak{g}_i||\mathfrak{g}_{i+1}|\gamma_{i+1})_p \\ \qquad = \left(n, \pi_1 \prod_{i=1}^{t-1} |\mathfrak{P}_{i+1}|^t \right)_p \prod_{i=1}^{t-1} (\pi_i, -|\mathfrak{P}_i||\mathfrak{P}_{i+1}|\pi_{i+1}))_p \end{cases}$$

für jede ungerade Primzahl p.

Beweis. Der oben erwähnte Hasse-Minkowskische Satz lautet in der für unsere Zwecke bequemsten Formulierung:

Gibt es zu zwei t-reihigen ganzzahligen symmetrischen Matrizen R und S eine ganzzahlige reguläre Matrix C derart, daß $CRC^T = S$ ist, so gilt für jede ungerade Primzahl p:

$$\prod_{i=1}^{t-1} (R_i, -R_{i+1})_p = \prod_{i=1}^{t-1} (S_i, -S_{i+1})_p;$$

hierbei bedeuten R_i und S_i die i-ten Hauptminoren von R bzw. S.

(Zum Beweis vergleiche man HASSE [9] oder auch JONES [11], Chapter 2.) Dieser Satz ist wegen (M3) und Lemma 7 auf die Matrizen P und $\lambda GJG + nG$ bzw. G und $\lambda PJP + nP$ anwendbar. Wie haben die Hauptminoren dieser Matrizen zu berechnen. Es ist klar, daß $P_i = \prod_{j=1}^{i} |\mathfrak{P}_j|$, $G_i = \prod_{j=1}^{i} |\mathfrak{g}_j|$ ist, denn P und G sind Diagonalmatrizen. Weiter ist

$$(\lambda PJP + nP)_i = (\lambda PJ + nE)_i P_i = (AB)_i P_i$$

wegen (M2); und analog folgt $(\lambda GJG + nG)_i = (BA)_i G_i$. Auf dieselbe Art wie im Beweis von Lemma 7 für $\det AB$ kann man weiter zeigen, daß

$$(AB)_i = n^{i-1} \left(n + \lambda \sum_{j=1}^{i} |\mathfrak{P}_j| \right) = \pi_i n^{i-1}$$

und $(BA)_i = \gamma_i n^{i-1}$ ist. Der Hassesche Satz gibt also die Beziehung:

$$\begin{cases} \prod_{i=1}^{t-1} (P_i, -P_{i+1}) = \prod_{i=1}^{t-1} (n^{i-1} \gamma_i G_i, n^i \gamma_{i+1} G_{i+1}) \\ \prod_{i=1}^{t-1} (G_i, -G_{i+1}) = \prod_{i=1}^{t-1} (n^{i-1} \pi_i P_i, n^i \pi_{i+1} P_{i+1}). \end{cases} \tag{15}$$

Dabei haben wir den Index p der Hilbert-Symbole weggelassen, was nicht zu Mißverständnissen führen wird. Die rechte Seite der ersten Gl. (15) läßt sich unter Benutzung der Rechenregeln (13) für Hilbert-Symbole in folgende drei Produkte aufspalten:

$$\prod_{i=1}^{t-1}(n^{i-1}\gamma_i, n^i\gamma_{i+1}) \prod_{i=1}^{t-1}(n^{i-1}\gamma_i, G_{i+1})(G_i, n^i\gamma_{i+1}) \prod_{i=1}^{t-1}(G_i, -G_{i+1}).$$

Das erste dieser Produkte wird weiter zerlegt in

$$\left[\prod_{i=1}^{t-1}(n^{i-1}, -n^i)\right](n, \gamma_1)\left[\prod_{i=1}^{t-1}(\gamma_i, n^{2(i-1)})\right](n^{t-2}, \gamma_t)\prod_{i=1}^{t-1}(\gamma_i, -\gamma_{i-1})$$
$$= (n, (-1)^{(t-1)(t-2)/2}\gamma_1)\prod_{i=1}^{t-1}(\gamma_i, -\gamma_{i-1}).$$

Das zweite Produkt wird gleich

$$(G_1, n\gamma_2)\left[\prod_{i=2}^{t-1}(G_i, n^i\gamma_{i+1}n^{i-2}\gamma_{i-1})\right](n^{t-2}\gamma_{t-1}, G_t)$$
$$= (n, |\mathfrak{g}_1| G_t^t)(|\mathfrak{g}_1|, \gamma_2)(\gamma_{t-1}, G_t)\prod_{i=2}^{t-1}\left(\prod_{j=1}^{i}|\mathfrak{g}_j|, \gamma_{i-1}\gamma_{i+1}\right)$$
$$= (n, |\mathfrak{g}_1| G_t^t)(|\mathfrak{g}_1|, \gamma_1)(\gamma_{t-1}, |\mathfrak{g}_1| G_t)\prod_{j=2}^{t-1}\left(|\mathfrak{g}_j|, \prod_{i=j}^{t-1}\gamma_{i-1}\gamma_{i+1}\right)$$
$$= (n, |\mathfrak{g}_1| G_t^t)\prod_{i=1}^{t-1}(\gamma_i, |\mathfrak{g}_i|\,|\mathfrak{g}_{i+1}|).$$

Genau so läßt sich die zweite Gl. (15) behandeln, es folgt also:

$$(16)\quad \begin{cases} \prod_{i=1}^{t-1}(P_i, -P_{i+1})(G_i, -G_{i+1}) \\ \quad = (n, (-1)^{(t-1)(t-2)/2}\gamma_1 |\mathfrak{g}_1| G_t)\prod_{i=1}^{t-1}(\gamma_i, -|\mathfrak{g}_i|\,|\mathfrak{g}_{i+1}|\gamma_{i+1}) \\ \quad = (n, (-1)^{(t-1)(t-2)/2}\pi_1 |\mathfrak{P}_1| P_t)\prod_{i=1}^{t-1}(\pi_i, -|\mathfrak{P}_i|\,|\mathfrak{P}_{i+1}|\pi_{i+1}). \end{cases}$$

Da $P_{i+1} = |\mathfrak{P}_{i+1}| P_i$ ist, läßt sich auf die Hilbert-Symbole im ersten der Produkte (16) noch einmal die vierte Rechenregel (13) anwenden:

$$(17)\qquad \prod_{i=1}^{t-1}(P_i, -P_{i+1})(G_i, -G_{i+1}) = \prod_{i=1}^{t-1}(P_i, |\mathfrak{P}_{i+1}|)(G_i, |\mathfrak{g}_{i+1}|).$$

Aus (16) und (17) folgt die behauptete Beziehung (H) nun ganz einfach.

Wir bemerken noch, daß die Beziehung (H) sich im Falle einer symmetrischen Zerlegung, d.h. wenn $|\mathfrak{P}_i| = |\mathfrak{g}_i|$ für alle i, auf folgende einfachere Form reduziert:

$$(\mathrm{H_s})\qquad \left(n, (-1)^{(t-1)(t-2)/2}\gamma_1\prod_{i=1}^{t-1}|\mathfrak{g}_{i+1}|^t\right)_p = \prod_{i=1}^{t-1}(\gamma_i, -|\mathfrak{g}_i|\,|\mathfrak{g}_{i+1}|\gamma_{i+1})_p.$$

Die Gln. (H) sind notwendige Bedingungen für die Existenz einer taktischen Zerlegung mit vorgegebenen $|\mathfrak{P}_i|$ und $|\mathfrak{g}_i|$. Sie enthalten alle bisher bekannten Nichtexistenzsätze für λ-Ebenen. Wir geben hier nur ein Beispiel:

Folgerung (Satz von BRUCK und RYSER [4], theorem 1). *Hat eine endliche projektive Ebene die Ordnung $n \equiv 1$ oder $2 \bmod 4$, so ist jede im quadratfreien Teil von n aufgehende ungerade Primzahl von der Form $4j+1$.*

Beweis. Man betrachte die triviale taktische Zerlegung der Ebene in lauter Klassen mit je einem Element. Dann ist $t = v = n^2 + n + 1$ und $(t-1)(t-2)/2 \equiv -1 \bmod 2$; ferner gilt, da $\lambda = 1$, daß $\gamma_i = n + i$, $i = 1, \ldots, t$. Da die Zerlegung natürlich symmetrisch ist, ist (H_s) anwendbar. Es ergibt sich:

$$(n, -[n+1])_p = \prod_{i=1}^{t-1} (n+i, -[n+i+1])_p .$$

Mit der dritten und fünften der Rechenregeln (13) folgt weiter:

$$(18) \qquad (n, -1)_p (n+1, -1)_p = \prod_{i=1}^{t-1} (n+i, -1)_p (n+i+1, -1)_p .$$

Faßt man nun die rechts stehenden Hilbert-Symbole in geeigneter Weise zusammen und beachtet man noch, daß $n + t = n + v = (n+1)^2$ ist, so bleibt wegen der zweiten und der letzten der Regeln (13) auf der rechten Seite von (18) nur $(n+1, -1)$ übrig. Also folgt $(n, -1)_p = 1$ für alle p. Ist nun p ein Teiler des quadratfreien Teiles von n, so daß $n = n' p^m$ mit $n' \not\equiv 0 \bmod p$ und $m \equiv 1 \bmod 2$ wird, so ergibt sich aus der Definition des Hilbert-Symbols schließlich, daß $(-1 \mid p) = 1$, also p von der Form $4j+1$ ist, q.e.d.

3.4. Vollsymmetrische taktische Zerlegungen

Die Anwendung der Beziehungen (H) ist im allgemeinen recht kompliziert und erfordert viele Fallunterscheidungen. In der folgenden Untersuchung, bei der wir uns an sich auch auf die Beziehungen (H) stützen könnten, schlagen wir daher einen anderen Weg ein.

Eine taktische Zerlegung einer beliebigen λ-Ebene soll *vollsymmetrisch* heißen, wenn alle ihre Klassen gleichviele Elemente enthalten. Vollsymmetrische taktische Zerlegungen werden insbesondere von halbtransitiven (Definition in [15]) Kollineationsgruppen erzeugt, also z.B. von zyklischen Kollineationsgruppen mit Primzahlordnung ohne Fixelemente. Bei der Behandlung der vollsymmetrischen Zerlegungen läßt sich die schwerfällige Behandlung mit (H_s) durch eine andere Methode ersetzen, deren wesentliches Hilfsmittel folgender von CHOWLA und RYSER stammender Satz ist:

Es sei $t > 1$ ungerade und $a, b > 0$ ganze Zahlen. Gibt es sodann eine t-reihige Matrix C derart, daß $CC^T = aJ + bE$ ist, so besitzt die Gleichung

$$b x^2 + (-1)^{(t-1)/2} a y^2 = z^2$$

nichttriviale ganzzahlige Lösungen x, y, z.

Zum Beweis vergleiche man [6], theorems 4, 5.

Wir benutzen dieses Resultat zum Beweis des folgenden Satzes:

Satz 12. *Es sei $\mathfrak{E}$ eine λ-Ebene der Ordnung n und Γ eine vollsymmetrische taktische Zerlegung von $\mathfrak{E}$ mit $t=t(\Gamma)>1$. Ist sodann t gerade, so ist n eine Quadratzahl. Ist t ungerade und bezeichnet s die Anzahl der Elemente jeder Γ-Klasse, so gilt:*

(i) *Für die ungeraden Primteiler p des quadratfreien Faktors $(\lambda s)^*$ von λs ist $n\equiv 0 \bmod p$ oder $(n|p)=1$.*

(ii) *Für die ungeraden Primteiler p des quadratfreien Faktors n^* von n ist $\lambda s\equiv 0 \bmod p$ oder $(\lambda s|p)=(-1)^{(t-1)(p-1)/4}$.*

Die jeweils erste Alternative tritt dabei höchstens dann auf, wenn $\lambda>1$ ist.

Beweis. (a) Daß n für gerades t ein Quadrat sein muß, ist ein Spezialfall der Folgerung von Satz 9. Da alle $|\mathfrak{X}|=|\mathfrak{x}|=s$, folgt aus (G1), daß $(\mathfrak{X}\mathfrak{x})=(\mathfrak{x}\mathfrak{X})$ für jedes Paar $\mathfrak{X}, \mathfrak{x}$ von Γ-Klassen gelten muß. Das bedeutet gerade $B=A^T$. Weiter ist $P=G=sE$, also $PJ=GJ=sJ$. M2) ergibt nun:

$$AA^T=\lambda sJ+nE.$$

Da A über dem Körper der rationalen Zahlen regulär ist, ist der Chowla-Ryssersche Satz mit $a=\lambda s$ und $b=n$ anwendbar. Es gibt also ein nichttriviales Tripel x, y, z ganzer Zahlen mit

$$nx^2+(-1)^{(t-1)/2}\lambda s y^2=z^2. \tag{19}$$

(b) Es sei nun $\lambda s=s^*r^2$ und s^* quadratfrei. Division von (19) durch das Quadrat des g.g.T. von x, ry, z ergibt eine nichttriviale Gleichung

$$n\xi^2+(-1)^{(t-1)/2}s^*\eta^2=\zeta^2,$$

in der ξ, η, ζ teilerfremd sind. Ist nun $p|s^*$, so folgt zunächst $(p, \xi)=1$, denn aus $p|\xi$ und $p|s^*$ würde $p|\zeta^2$, also $p^2|\zeta^2$ folgen. Außerdem wäre $p^2|\xi^2$, also auch $p^2|s^*\eta^2$. Da s^* quadratfrei ist, würde daraus $p|\eta$ folgen, d.h. ξ, η und ζ hätten den gemeinsamen Teiler p, im Gegensatz zu der Voraussetzung. Es gibt also eine ganze Zahl ϱ mit $\varrho\xi\equiv 1 \bmod p$; Multiplikation unserer Gleichung mit ϱ^2 ergibt

$$(\varrho\zeta)^2=n(\varrho\xi)^2+(-1)^{(t-1)/2}s^*(\varrho\eta)^2\equiv n \bmod p,$$

und daraus folgt, daß entweder $n\equiv 0 \bmod p$ oder $(n|p)=1$ ist.

(c) Aus (19) folgt durch Division mit dem Quadrat des g.g.T. von $m x, y, z$, wobei $n=n^*m^2$ mit quadratfreiem n^*, eine nichttriviale Beziehung

$$n^*\xi^2+(-1)^{(t-1)/2}\lambda s\eta^2=\zeta^2$$

mit teilerfremden ξ, η, ζ. Daraus ergibt sich wie unter (b), daß entweder $\lambda s\equiv 0 \bmod p$ oder $\left((-1)^{(t-1)/2}\lambda s|p\right)=1$ sein muß für jeden ungeraden Primteiler p von n^*; wegen $(-1|p)=(-1)^{(p-1)/2}$ folgt daraus die Behauptung (ii) von Satz 12. [Die Beweisteile (b) und (c) sind Pickert [*12*], S. 297 nachgebildet.]

(d) Es bleibt zu zeigen, daß im Falle $\lambda = 1$ die Zahlen n und $\lambda s = s$ teilerfremd sind. Das aber folgt sofort aus der Teilerfremdheit von $v = n(n+1)+1$ und n sowie der Tatsache, daß $v = st$. Damit ist Satz 12 vollständig bewiesen.

Für den Fall, daß Γ die triviale taktische Zerlegung ist, deren sämtliche Klassen aus einem Element bestehen, ist die Aussage (b) von Satz 12 äquivalent zu den von CHOWLA und RYSER bewiesenen notwendigen Kriterien für die Existenz von λ-Ebenen. Satz 12 besagt die Nichtexistenz von vollsymmetrischen taktischen Zerlegungen in vielen endlichen projektiven Ebenen, deren Ordnung keine Primzahlpotenz ist; z. B. kann eine Ebene der Ordnung 10, wenn sie existiert, keine vollsymmetrische Zerlegung besitzen, wie man leicht nachprüft.

Zum Abschluß leiten wir aus Satz 12 einige rein zahlentheoretische Folgerungen her:

Satz 13. *Es sei p eine ungerade Primzahl, $n = p^r$ mit ungeradem r, und $v = n^2+n+1$. Sodann gilt für alle ungeraden Primteiler q von v:*

(a) $(p|q) = 1$

und für alle echten Teiler d von v:

(b) $(d|p) = (-1)^{(p-1)(v-d)/4d}$.

(c) *Aus* $v \equiv -1 \bmod 4$ *folgt* $(d|p) = (-d|p) = 1$.

(d) *Aus* $p \equiv 1 \bmod 4$ *folgt* $(d|p) = 1$.

(e) *Aus* $(d|p) = -1$ *folgt* $p \equiv d \equiv -1 \bmod 4$.

Beweis. Es sei $\mathfrak{E}$ die Desarguessche projektive Ebene der Ordnung n. Nach einem Satz von SINGER ([*14*]; für den Beweis vergleiche man auch PICKERT [*12*], S. 303) ist $\mathfrak{E}$ zyklisch, d.h. es existiert eine auf den Punkten von $\mathfrak{E}$ transitive zyklische Kollineationsgruppe Γ von $\mathfrak{E}$. Da abelsche transitive Permutationsgruppen regulär sind (vgl. WIELANDT [*15*], S. 9), muß Γ die *Ordnung* v haben. Es sei σ ein erzeugendes Element von Γ und d ein echter Teiler von v. Sodann erzeugt die von σ^d erzeugte Untergruppe Δ von Γ eine vollsymmetrische taktische Zerlegung von $\mathfrak{E}$ mit $t(\Delta) = d$ und $s = v/d$.

Für jeden echten Primteiler q von v läßt sich nun d so wählen, daß q im quadratfreien Faktor von s aufgeht. Also ist $(n|q) = 1$ nach Satz 12, (i); wegen $\lambda = 1$ kann nämlich nicht $n \equiv 0 \bmod q$ sein. Aus $n = p^r$ und $r = 2j+1$ folgt sodann $(p|q) = 1$, d.h. die Behauptung (a).

Der quadratfreie Faktor von n besteht aus der Primzahl p allein; die Behauptung (b) ist gerade die Aussage (ii) von Satz 12.

Ist $v = n^2+n+1 \equiv -1 \bmod 4$, so folgt $n \equiv 1 \bmod 4$, da p ungerade, und weiter $p \equiv 1 \bmod 4$, da r ungerade ist. Also ist $(-1|p) = 1$ und folglich $(d|p) = (d|p)(-1|p) = (-d|p)$. Da andererseits nach Satz 13, (ii) eines der Legendre-Symbole $(d|p)$, $(-d|p)$ gleich Eins sein muß, folgt die Behauptung (c).

Die Behauptungen (d) und (e) sind ebenfalls direkte Folgerungen der Aussage (ii) von Satz 12.

Literatur

[*1*] BAER, R.: Homogeneity of projective planes. Amer. J. Math. **64**, 137–152 (1942). — [*2*] BAER, R.: Projectivities with fixed points on every line of the plane. Bull. Amer. Math. Soc. **52**, 273–286 (1946). — [*3*] BRUCK, R. H.: Difference sets in a finite group. Trans. Amer. Math. Soc. **78**, 464–481 (1955). — [*4*] BRUCK, R. H., and H. J. RYSER: The nonexistence of certain finite projective planes. Canad. J. Math. **1**, 88–93 (1949). — [*5*] CARMICHAEL, R. D.: Introduction to the theory of groups of finite order. Boston 1937. — [*6*] CHOWLA, S., and H. J. RYSER: Combinatorial problems. Canad. J. Math. **2**, 93–99 (1950). — [*7*] HALL jr., M.: Projective planes and related topics. California Institute of Technology 1954. — [*8*] HALL, M., and H. J. RYSER: Cyclic Incidence Matrices. Canad. J. Math. **3**, 495–502 (1951). — [*9*] HASSE, H.: Über die Äquivalenz quadratischer Formen im Körper der rationalen Zahlen. Crelle's J. reine u. angew. Math. **152**, 205–224 (1923). — [*10*] HUGHES, D. R.: Bull. Amer. Math. Soc. **62**, 350, 552 (1956). — [*11*] JONES, B. W.: The arithmetic theory of quadratic forms. Carus Monographs, New York 1950. — [*12*] PICKERT, G.: Projektive Ebenen. Berlin 1955. — [*13*] QVIST, B.: Some remarks concerning curves of the second degree in a finite plane. Ann. Acad. Sci. Fenn. **134** (1952). — [*14*] SINGER, J.: A theorem in finite projective geometry and some applications to number theory. Trans. Amer. Math. Soc. **43**, 377–385 (1938). — [*15*] WIELANDT, H.: Permutationsgruppen. Vorlesungsausarbeitung von J. ANDRÉ, Tübingen 1954/55.

Frankfurt a. M., Mathematisches Seminar der Universität

(Eingegangen am 22. Mai 1957)