

**Zeitschrift:** Commentarii Mathematici Helvetici  
**Herausgeber:** Schweizerische Mathematische Gesellschaft  
**Band:** 7 (1934-1935)

**Artikel:** Unitäre Matrizen in Galoisfeldern.  
**Autor:** Frame, J.S.  
**DOI:** <https://doi.org/10.5169/seals-515587>

### **Nutzungsbedingungen**

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. [Mehr erfahren](#)

### **Conditions d'utilisation**

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. [En savoir plus](#)

### **Terms of use**

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. [Find out more](#)

**Download PDF:** 17.04.2026

**ETH-Bibliothek Zürich, E-Periodica, <https://www.e-periodica.ch>**

# Unitäre Matrizen in Galoisfeldern

Von J. S. FRAME, Zürich

§ 1. Die meisten einfachen Gruppen lassen sich am bequemsten durch Matrizen in einem Galoisfeld definieren, dessen Charakteristik  $p$  ein Teiler der Gruppenordnung ist. Wir wollen uns hier mit einer zweifach unendlichen Schar solcher Gruppen beschäftigen, indem wir die Matrizen einer Klasse von konjugierten Elementen in einer besonders durchsichtigen Normalform schreiben, und daraus diese Gruppen geometrisch als Permutationsgruppe von gewissen Vektorscharen in einem „Galoisfeld-Raum“ interpretieren. Wir legen als Koeffizientenbereich ein Galoisfeld  $GF(q^2)$  von  $q^2$  Elementen zugrunde, wobei  $q = p^s$  eine Primzahlpotenz bedeutet. Ferner definieren wir zu jedem  $x$  ein konjugiertes:  $\bar{x} = x^q$ , und bemerken, daß  $\bar{\bar{x}} = x^{q^2} = x$  ist. Zur Abkürzung setzen wir  $\sum_{i=1}^m \bar{a}_i b_i = (a | b) = (\bar{b} | \bar{a})$ , und  $Q_m = q^m - (-1)^m$ .

Es sei jetzt  $G_m^*$  die Gruppe der „unitären“ Matrizen vom Grade  $m$  in diesem Galoisfeld; d. h., die Gruppe der Matrizen  $T$ , welche die Form  $(x | x)$  ungeändert lassen. Ihre Matrizen haben die Gestalt  $(t_{ij})$ , wo  $\sum_{k=1}^m \bar{t}_{ik} t_{jk} = \sum_{k=1}^m \bar{t}_{ki} t_{kj} = \delta_{ij}$ . Kurz gesagt, es ist  $T^{-1}$  die transponierte Matrix von  $\bar{T}$ . Für die Determinante gilt die Gleichung  $T \cdot \bar{T} = 1$ .

Schreiben wir  $a' = aT$ , wenn  $a'_j = \sum_{i=1}^m a_i t_{ij}$ ,  $i = 1, 2, \dots, m$ , dann gilt  $(aT | bT) = (a | b)$  für  $T$  aus  $G_m^*$ . Nach Dickson<sup>1)</sup> beträgt die Ordnung dieser Gruppe

$$g_m^* = \prod_{k=1}^m q^{k-1} Q_k = q^{\binom{m}{2}} \prod_{k=1}^m Q_k.$$

Die Matrizen von der Determinante 1 bilden einen Normalteiler  $G_m$  vom Index  $q + 1$ , und von der Ordnung  $g_m = g_m^* / (q + 1)$ . Das Zentrum  $Z_m$  dieses Normalteilers hat die Ordnung  $d$ , wo  $d$  der g. g. T. von  $m$  und  $q + 1$  ist. Die Faktorgruppe  $H_m = G_m / Z_m \cong HO(m, p^{2s})$ , von der Ordnung  $h_m = g_m / d$ , ist nach dem Beweis von Dickson eine einfache Gruppe, abgesehen von den drei Fällen  $HO(2, 2^2)$ ,  $HO(2, 3^2)$ , und  $HO(3, 2^2)$ . Ferner ist  $HO(2, p^{2s})$  isomorph mit der linear-gebrochenen Gruppe  $LF(2, p^s)$  von der Ordnung  $q(q^2 - 1) / d$ . Von den übrigbleibenden

<sup>1)</sup> Dickson: Linear Groups.

Fällen ist  $HO(3, 3^2)$ , mit 6048 Elementen, die kleinste Gruppe dieser Familie.

§ 2. Jeder Vektor  $(a_1, a_2, \dots, a_m)$ , für den  $(a | a) = 0$  ist, entspricht einer unitären Matrix von der Form

$$M(a; \varepsilon) \equiv M(a_1, a_2, \dots, a_m; \varepsilon) \equiv (\delta_{ij} + \varepsilon \bar{a}_i a_j),$$

wo  $\varepsilon = -\bar{\varepsilon}$  eine „rein-imaginäre“ Zahl des  $GF$  bedeutet. Hierbei ist  $M(xa; \varepsilon) = M(a; x\bar{x}\varepsilon)$ , so daß die  $q + 1$  Matrizen  $M(\Theta a; \varepsilon)$  übereinstimmen für  $\Theta\bar{\Theta} = 1$ , und der Nullvektor entspricht der Identität. Einige wichtige Eigenschaften dieser Matrizen geben wir zunächst in einer Reihe von Sätzen an.

*Satz 1.* Die Matrizen  $M(a; \varepsilon)$  und  $M(b; \varepsilon)$  sind dann und nur dann vertauschbar, wenn  $(a | b) = 0$ ; oder wie wir auch geometrisch sagen können, wenn die Vektoren  $a$  und  $b$  senkrecht aufeinander stehen. Wir bemerken, daß nach Annahme  $(a | a) = (b | b) = 0$  ist.

*Beweis:* Das Produkt

$$M(a; \varepsilon) \cdot M(b; \varepsilon) = [\delta_{ij} + \varepsilon(\bar{a}_i a_j + \bar{b}_i b_j) + \varepsilon^2 \bar{a}_i b_j (b | a)]$$

ist dann und nur dann symmetrisch in  $a$  und  $b$ , wenn  $(b | a) = 0$  ist. Zwar haben wir dann  $\bar{a}_i b_j (b | a) = \bar{b}_i a_j (a | b)$ , und folglich  $(a | a) b_j (b | a) = (b | a) a_j (a | b)$ . Wegen  $(a | a) = 0$ , folgt  $a_j (b | a) (a | b) = 0$ , für alle  $a_j$ .

*Satz 2.* Die Matrizen  $M(a; \omega \varepsilon)$ , wo  $\omega$  das  $GF(q)$  durchläuft, bilden eine Abelsche Gruppe  $G_a$ , vom Typus  $(p, p, \dots, p)$ , die isomorph ist mit der additiven Gruppe des  $GF(q)$ . Es gilt die Gleichung:

$$M(a; \omega_1 \varepsilon) M(a; \omega_2 \varepsilon) = M[a; (\omega_1 + \omega_2) \varepsilon].$$

Insbesondere ist  $M(a; \varepsilon)^n = M(a; n\varepsilon)$ . Jede Matrix ist daher von der Ordnung  $p$ . Der Gruppe  $G_a$  wird eine Vektorschar  $(a)$  zugeordnet, die die sämtlichen Multipla eines Vektors  $a$  enthält.

Der Beweis des Satzes folgt sofort aus der Zusammensetzung der Matrizen.

*Satz 3.* Es gilt  $T^{-1} M(a; \varepsilon) T = M(aT; \varepsilon)$ , für  $T$  aus  $G_m^*$ . Ferner ist  $T^{-1} G_a T = G_{aT}$ .

$$\text{Beweis: } \sum_{k,l} \bar{t}_{ki} (\delta_{kl} + \varepsilon \bar{a}_k a_l) t_{lj} = \delta_{ij} + \varepsilon \left( \sum_{k=1}^m \bar{a}_k \bar{t}_{ki} \right) \left( \sum_{l=1}^m a_l t_{lj} \right).$$

*Satz 4.* Für  $m > 2$  bilden die sämtlichen Matrizen  $M(a; \varepsilon)$ ,  $a \neq 0$ , eine einzige Klasse von konjugierten Elementen der Gruppe  $H_m$ ; für  $m = 2$ , dagegen, zerfallen sie in  $d$  Klassen.

*Beweis:* Für  $m = 2$  kann der Vektor  $(a_1, a_2)$  nur in  $(k a_1, \bar{k} a_2)$ ,  $k \neq 0$ , unter  $G_2$  übergeführt werden, und zwar vermittelt der Matrix  $\begin{pmatrix} k + \bar{u} \bar{a}_1 & -u a_2 \\ \bar{u} \bar{a}_2 & \bar{k} + u a_1 \end{pmatrix}$ , wenn gilt:  $ku a_1 + \bar{k} \bar{u} \bar{a}_1 = 1 - k \bar{k}$ .

Nach Satz 3 ist daher die Matrix  $M(1, a; \varepsilon)$  konjugiert zu denen, und nur denen von der Form  $M(\bar{x} \bar{\Theta}, x \Theta a; \varepsilon) = M(\bar{x}, x \Theta^2 a; \varepsilon)$ , wo  $x \Theta = \bar{k}$ ,  $\Theta \bar{\Theta} = 1$  ist. Für  $p = 2$ , und daher  $d = 1$ , gibt es nur eine Klasse. Für  $p > 2$ , sind  $M(1, a; \varepsilon)$  und  $M(1, 1/a; \varepsilon)$  nicht miteinander konjugiert, sondern sie liegen in  $d = 2$  verschiedenen Klassen von den Typen  $M(\bar{x}, x a^{4m+1}; \varepsilon)$  und  $M(\bar{x}, x a^{4m-1}; \varepsilon)$ , wo  $a \bar{a} = -1$  ist. Inverse Matrizen  $M(a_1, a_2; \varepsilon)$  und  $M(a_1, a_2; -\varepsilon)$  sind dann und nur dann konjugiert, wenn  $-1$  ein Quadrat im  $GF(q)$  ist; d. h. wenn  $q \equiv 0, 1, \text{ oder } 2, \pmod{4}$  ist. In diesen Fällen sind die Klassen selbstinvers, wie man es bekanntlicherweise in den Gruppen  $LF(2, p^s)$  findet.

Ist  $m > 2$ ,  $p > 2$ , und  $a \neq 0$ , so gilt nicht für alle  $j, k = 1, 2, \dots, m$  die Relation  $\bar{a}_j a_j + \bar{a}_k a_k = 0$ . Gelte sie paarweise für  $a_i, a_j, a_k$ , so müßte  $2 \bar{a}_i a_i = 2 \bar{a}_j a_j = 2 \bar{a}_k a_k = 0$  und daher  $a_i = a_j = a_k = 0$  sein. Es sei also  $\bar{a}_j a_j + \bar{a}_k a_k = b_j b_j \neq 0$ . Übt man die Transformation

$$(x'_j, x'_k) = (x_j, x_k) \begin{pmatrix} \bar{a}_j / \bar{b}_j & -a_k / b_j \\ \bar{a}_k / \bar{b}_j & a_j / b_j \end{pmatrix}; \quad x'_i = x_i, \quad i \neq j, k$$

auf den Vektor  $(a_1, \dots, a_j, \dots, a_k, \dots, a_m)$  aus, so geht er in  $(a_1 \dots b_j, \dots, 0, \dots, a_m)$  über. Für  $m > 2$ ,  $p = 2$  kann man dieselbe Transformation gebrauchen, wenn man es nicht mit den Vektoren  $a$ , wo  $\bar{a}_1 a_1 = \bar{a}_2 a_2 = \dots = \bar{a}_m a_m$ , zu tun hat. In diesem Falle kann man aber erst  $(a_1, a_2)$  in  $(k a_1, \bar{k} a_2)$  überführen, wo  $k \bar{k} \neq 1$  ist, und dann in derselben Weise fortfahren wie für  $p > 2$ . In ähnlicher Weise kann man alle Komponenten bis auf zwei in 0 transformieren. Mit einer geraden Permutation bringt man diese zwei in die ersten beiden Stellen, und wie im Falle  $m = 2$  transformiert man diesen Vektor in  $(1, \beta, 0, \dots, 0)$ . Der wird aber jetzt in einen bestimmten Vektor  $(1, \alpha, 0, \dots, 0)$ , durch die Transformation:  $x'_2 = (\alpha / \beta) x_2$ ,  $x'_3 = (\beta / \alpha) x_3$ ;  $x'_i = x_i$ ,  $i \neq 2, 3$ , transformiert. Entsprechend, nach Satz 3, ist für  $m > 2$  jede Matrix  $M(a_1, \dots, a_m; \varepsilon)$  mit der Matrix  $M(1, \alpha, 0 \dots 0; \varepsilon)$  in  $G_m$  konjugiert. Daher bilden diese Matrizen auch in  $H_m$  eine einzige Klasse, weil man die Vektoren nur bis auf einen Faktor  $\Theta$ ,  $\Theta \bar{\Theta} = 1$ , zu bestimmen braucht. Hiermit ist Satz 4 bewiesen.

*Satz 5.* Die Anzahl der in  $GF(q^2)$  von 0 verschiedenen Lösungen der Gleichung  $(a | a) = 0$  beträgt  $Q_m Q_{m-1}$ . Entsprechend gibt es  $Q_m Q_{m-1} / Q_1$  von der Identität verschiedenen Matrizen  $M(a; \varepsilon)$ , und  $Q_m Q_{m-1} / Q_2$  Abelsche Gruppen  $G_a$ .

*Beweis:* Die Formel gilt für  $m = 1$ . Nehmen wir an, sie gelte für  $m - 1$ ,  $m > 1$ . Wenn  $a_m = 0$ , gibt es nach Induktionsannahme  $Q_{m-1}Q_{m-2}$  Lösungen  $a \neq 0$ . Wenn  $a_m \neq 0$ , hat man  $q^{2m-2} - 1 - Q_{m-1}Q_{m-2}$  Werte von  $a_1, \dots, a_{m-1}$ , so daß  $\sum_{i=1}^{m-1} \bar{a}_i a_i \neq 0$  ist, und damit ist  $a_m$  bis auf einen Faktor  $\Theta$ ,  $\Theta \bar{\Theta} = 1$ , bestimmt. Die Richtigkeit des Satzes folgt aus der Identität:

$$Q_m Q_{m-1} \equiv Q_{m-1} Q_{m-2} + (q + 1) (q^{2m-2} - 1 - Q_{m-1} Q_{m-2}).$$

*Satz 6.* Die Gruppe  $H_m$  besitzt eine Darstellung als Permutationsgruppe  $P_m$  von  $Q_m Q_{m-1} / Q_2$  Symbolen  $G_a$ , durch die Abbildung, wobei  $T$  der Permutation ( $G_a \rightarrow G_{aT}$ ) entspricht. Für  $m > 2$  ist diese Gruppe transitiv.

Der Satz folgt sofort aus den vorangehenden Sätzen.

*Satz 7.* Ist eine Matrix aus  $G_m$ ,  $m > 2$ , mit der Gruppe  $G_a$  vertauschbar:  $G_a = G_{aT}$ , so transformiert sie den zum Vektor  $a$  orthogonalen Raum in sich selbst, und vertauscht auch die übrigbleibenden Vektoren unter sich. Ich behaupte, die Untergruppe  $U_a$  der Permutationsgruppe  $P_m$ , die  $G_a$  invariant läßt, ist transitiv in den  $q^{2m-3}$  zu  $(a)$  nicht orthogonalen Vektorscharen, und transitiv auch in den  $q^2 Q_{m-2} Q_{m-3} / Q_2$  zu  $(a)$  orthogonalen Vektorscharen außer  $(a)$  selbst.

*Beweis:* Aus  $(aT | bT) = (a | b)$  folgt der erste Teil des Satzes. Wir untersuchen zunächst die Transitivität von  $U_a$  in den zu  $(a)$  nicht orthogonalen Vektorscharen  $(c)$ ,  $(c')$ , usw. Es seien  $(a | a) = (c | c) = (c' | c') = 0$ ;  $(c | a) = k (c' | a) \neq 0$ . Nach Satz 4 gibt es eine Matrix  $S$  aus  $G_m$ , so daß  $aS = a_0 \equiv (1, \alpha, 0 \dots 0)$  ist. Wir setzen  $b = cS$ ,  $b' = c'S$ .

Die Matrix

$$T: \begin{pmatrix} b_1 \Phi + k \bar{\Phi} & b_2 \Phi + \alpha k \bar{\Phi} & b_3 \Phi \dots b_n \Phi \\ \bar{\alpha} b_1 \Phi + \bar{\alpha} k (\bar{\Phi} - 1) & \bar{\alpha} b_2 \Phi + k (1 - \bar{\Phi}) & \alpha b_3 \Phi \dots \alpha b_n \Phi \\ t_{31} & \alpha t_{31} & t_{33} \dots t_{3n} \\ \dots & \dots & \dots \dots \\ t_{n1} & \alpha t_{n1} & t_{n3} \dots t_{nn} \end{pmatrix}$$

wö  $(1 + \bar{\alpha} \beta) \Phi = (\bar{k} b_1 + \bar{k} \bar{\alpha} b_2) \Phi = 1$ ,  $\alpha \bar{\alpha} = \beta \bar{\beta} = -1$  ist,

transformiert:  $a_0: (1, \alpha, 0 \dots 0)$  in  $k a_0: (k, k \alpha, 0, \dots 0)$ ,

und  $b_0: (1, \beta, 0 \dots 0)$  in  $b: (b_1, b_2, b_3, \dots b_n)$ .

Die Bedingungen für die Existenz von  $T$  sind:

$$(a_0 | b_0) = (k a_0 | b) = 1 / \Phi \neq 0; \quad (a_0 | a_0) = (b_0 | b_0) = (b | b) = 0.$$

Man kann mit  $T^{-1}$  einen beliebigen solchen Vektor  $b$ ,  $(a_0 | b) \neq 0$ , in  $b_0$ , und mit einem geeigneten  $T'$  diesen  $b_0$  in einen beliebigen  $b'$  mit den-

selben Eigenschaften überführen, indem man die Schar  $(a_0)$  invariant läßt. Die Transformation  $ST^{-1} T' S^{-1}$  führt  $c$  in  $c'$  und  $a$  in  $ka$  über, wie wir es wollten.

Für  $m = 3$  gibt es keine Vektoren, die zu einem bestimmten orthogonal sind, außer dessen Multipla. So haben die Permutationen der Untergruppe  $U_a$  in diesem Falle nur zwei transitive Bestandteile. Für  $m \geq 4$  gibt es jetzt eine Matrix  $V$

$$V: \begin{pmatrix} 1 & 0 & -\bar{v}\bar{x} & v\beta\bar{x} & 0 & \dots & 0 \\ 0 & 1 & -\bar{v}\bar{\alpha}\bar{x} & v\beta\bar{\alpha}\bar{x} & 0 & \dots & 0 \\ vx & v\alpha x & 1 & 0 & 0 & \dots & 0 \\ -\bar{v}\bar{\beta}x & -\bar{v}\bar{\beta}\alpha x & 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 0 & 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & 0 & 0 & \dots & 1 \end{pmatrix}$$

aus  $G_m$  derart, daß sie  $a_0: (1, \alpha, 0, \dots, 0)$  in sich, und  $(x, x\alpha, 1, \beta, 0, \dots, 0)$  in  $(0, 0, 1, \beta, 0, \dots, 0)$  transformiert, wo  $\alpha\bar{\alpha} = \beta\bar{\beta} = -1$  ist. Jeder zu  $a_0$  orthogonale Vektor läßt sich aber in der Form  $(x, x\alpha, b_3, b_4, \dots, b_m)$  schreiben. Nach dem Beweis von Satz 4 kann man mit einer Transformation auf  $m - 2$  Variable den Vektor  $(b_3, b_4, \dots, b_m)$ ,  $b \neq 0$ , in einen geeigneten Vektor  $(1, \beta, 0, \dots, 0)$  überführen. So kann man jeden zu  $(a_0)$  orthogonalen Vektor in einen beliebigen anderen solchen überführen, wenn sie nur nicht Multipla von  $a_0$  sind, indem man die Schar  $(a_0)$  ungeändert läßt. Ähnlich wie oben gilt der Satz auch für eine beliebige Vektorschar  $(a)$ .

Es gibt  $q^2(Q_{m-2}Q_{m-3} + 1) - 1$  von Null verschiedene, zu  $(a_0)$  orthogonale Vektoren  $b$  mit  $(b | b) = 0$ , oder nur  $q^2Q_{m-2}Q_{m-3}$ , wenn man die Multipla von  $a_0$  nicht mitzählt. Entsprechend gibt es  $q^2Q_{m-2}Q_{m-3} / Q_2$  zu  $(a_0)$  orthogonale Scharen ausser  $(a_0)$ , und  $Q_mQ_{m-1} / Q_2 - q^2Q_{m-2}Q_{m-3} / Q_2 - 1 = q^{2m-3}$  zu  $(a_0)$  nicht orthogonale Scharen. Hiermit ist Satz 7 vollständig bewiesen.

**Satz 8.** Die Permutationsgruppe  $P_m$  von Satz 6 hat für  $m > 3$  genau drei irreduzible Komponenten im algebraisch abgeschlossenen Körper der Charakteristik 0. Die Gruppe  $P_3$  hat nur zwei irreduzible Komponenten, wovon einer die Identität und der andere eine Darstellung vom Grade  $q^3$  ist.

*Beweis:* Der Satz folgt aus Satz 7, indem wir Satz 103 aus der Gruppentheorie von A. Speiser anwenden.

§ 3. Bevor wir diese Permutationsgruppen  $P_m$  weiter studieren, wollen wir jetzt die Normalform  $M(a; \varepsilon)$  etwas verallgemeinern, um einige andere Klassen von konjugierten Matrizen darzustellen, deren charakteristische Wurzeln sämtlich gleich 1 sind. Nach Speiser<sup>1)</sup> ist diese Bedingung notwendig und hinreichend dafür, daß die Ordnung einer solchen Matrix eine Potenz von  $p$  ist.

*Satz 9.* Die Matrizen

$$M(a; a; \varepsilon) \equiv (\delta_{ij} + \bar{a}_i a_j - \bar{a}_i a_j + \varepsilon \bar{a}_i a_j)$$

mit  $(a | a) = (\alpha | a) = (\alpha | \alpha) + \varepsilon + \bar{\varepsilon} = 0$ , bilden für  $(\alpha | \alpha) \neq 0$ ,  $m > 3$ , eine einzige Klasse von  $Q_m Q_{m-1} Q_{m-2} q^{m-2} / Q_1$  konjugierten Elementen der Gruppe  $H_m$ , deren Ordnungen  $p$  oder  $p^2$  sind, je nachdem  $p > 2$  oder  $p = 2$  ist. Für  $m = 3$ , dagegen, zerfallen sie in  $d$  Klassen. Die Matrizen  $M(a; a; \varepsilon)$ , die einem gemeinsamen Vektor  $a$  entsprechen, multiplizieren

sich wie die Matrizen  $\begin{pmatrix} 1 & -\alpha & \varepsilon \\ 0 & 1 & \bar{\alpha} \\ 0 & 0 & 1 \end{pmatrix}$ , wenn man  $\bar{\beta} \alpha$  durch  $(\beta | \alpha)$  ersetzt.

*Beweis:* Aus der Zusammensetzung der Matrizen folgt

$$M(a; a; \varepsilon) M(a; \beta; \eta) = M[a; a + \beta; \varepsilon + \eta - (\beta | a)].$$

Insbesondere gilt auch die Gleichung

$$[M(a; a; \varepsilon)]^n = M[a; n a; \binom{n+1}{2} \varepsilon + \binom{n}{2} \bar{\varepsilon}],$$

so daß die Elemente von der Ordnung  $p$ , bzw. 4 sind, wie es behauptet wurde. Es gilt ferner die Gleichung

$$M(a/x; a \bar{x}; \varepsilon x \bar{x}) = M(a; a; \varepsilon) = M(a; a + k a; \varepsilon + k - \bar{k}).$$

Infolgedessen hat man, beim Zählen, sämtliche Matrizen  $M(a; a; \varepsilon)$  wenn man zu  $a$  nur modulo  $a$  verschiedene Werte, und dann nur einen Wert aus jeder multiplikativen Schar  $(\alpha)$  angibt. Anders betrachtet, kann man dieselbe Matrix immer so ausdrücken, daß  $\varepsilon$  einen beliebigen der  $q^2 - q$  Werte annimmt, für die  $\varepsilon + \bar{\varepsilon} \neq 0$ .

Es sei  $T$  eine Matrix aus der Gruppe  $G_m^*$ . Dann ist

$$T^{-1} M(a; a; \varepsilon) T = M(a T; a T; \varepsilon).$$

<sup>1)</sup> Speiser, A., Theorie der Gruppen von endlicher Ordnung. Zweite Auflage, 1927, Satz 200, S. 221.

Mit geeignetem  $T$  aus  $G_m^*$  können wir  $a$  und  $\alpha$  in beliebige  $aT$ ,  $\alpha T$  transformieren, unter den Bedingungen

$$(a | a) = (aT | aT); \quad (a | \alpha) = (aT | \alpha T); \quad (\alpha | \alpha) = (\alpha T | \alpha T).$$

Innerhalb der Gruppe  $G_m$  können wir die Lösung  $aT$  beliebig, aber dann  $aT$  zuerst nur bis auf einen Faktor  $\Theta$ ,  $\Theta \bar{\Theta} = 1$ , bestimmen. Es sei, z. B.,  $a = (1, a, 0, \dots, 0)$ ,  $\alpha = (0, 0, 1, \dots, 0)$ . Dann können wir, im Falle  $m > 3$ ,  $a$  in sich und  $\alpha$  in irgend ein  $\Theta^k \alpha$  überführen; für  $m = 3$ , dagegen,  $a$  und  $\alpha$  nur in  $\bar{\Theta}^k a$  und  $\Theta^{2k} \alpha$  überführen, was aber derselben Matrix entspricht wie  $a$  und  $\Theta^{3k} \alpha$ . So erhalten wir  $Q_1 / d$  verschiedene Werte von  $\Theta^{3k}$ , die konjugierten Matrizen entsprechen, und  $d$  verschiedene Klassen, die nicht miteinander konjugiert sind.

Zusammengezählt haben wir  $Q_m Q_{m-1}$  Werte von  $a$ , und zu jedem davon  $q^{2m-4}$  modulo  $a$  verschiedene Vektoren  $\alpha$  für die  $(\alpha | a) = 0$  ist. Davon genügen aber  $Q_{m-2} Q_{m-3} + 1$  der Gleichung  $(\alpha | a) = 0$ . Es bleiben  $q^{2m-4} - 1 - Q_{m-2} Q_{m-3} = Q_{m-2} (q^{m-2} - q^{m-3})$  Vektoren  $\alpha$ , für die  $-(\alpha | a) = \varepsilon + \bar{\varepsilon} \neq 0$  ist. Bis auf Vielfache bleiben  $Q_{m-2} q^{m-3} / Q_1$  Werte von  $\alpha$ . Mit  $a$  und  $\alpha$  ist jetzt  $\varepsilon + \bar{\varepsilon}$  bestimmt, aber  $\varepsilon$  kann  $q$  Werte annehmen. So, wie behauptet, ist die Anzahl dieser Matrizen gleich  $q^{m-2} Q_m Q_{m-1} Q_{m-2} / Q_1$ .

Weitere Verallgemeinerungen der Form  $M(a; a, \varepsilon)$  werden komplizierter, weil sie vieler Relationen zwischen den Vektoren bedürfen. Wir geben nur ein Beispiel davon:

$$X = (\delta_{ij} + A_{ij} + \bar{b}_i c_j); \quad X^n = (\delta_{ij} + n(A_{ij} + \bar{b}_i c_j) + \binom{n}{2} \varepsilon \begin{pmatrix} \bar{b}_i & c_j \\ x_i & x_j \end{pmatrix} + \binom{n}{3} \bar{x}_i x_j)$$

wo  $A_{ij} = \bar{a}_i a_j - \bar{a}_j a_i$ ;  $x_i = c_i - b_i = a_i (a | b) - a_i (\alpha | b) = \sum_k b_k A_{ki} = \sum_k c_k A_{ki}$  und  $(a | a) = (a | \alpha) = (\alpha | \alpha) = (b | b) = (b | c) = (c | c) = \varepsilon + \bar{\varepsilon} = 0$  ist.

§ 4. Die geometrische Vorstellung, die wir in § 2 betrachtet haben, bietet ein Mittel dafür, die Charaktere der Permutationsgruppe  $P_m$  und die Klasseneinteilung von  $H_m$  zu untersuchen. Wegen der in den Sätzen 6 und 7 gegebenen Transitivitätseigenschaften sehen wir ein, daß zu einer Matrix, die eine Schar, bzw. zwei zueinander nicht orthogonale, bzw. zwei zueinander orthogonale Scharen invariant läßt, es eine konjugierte Matrix gibt, die dasselbe für beliebige Scharen mit denselben Orthogonalitätsverhältnissen macht. Führt die Matrix  $T$  die Vektoren  $a_0$  in  $k_1 a_0$ ,  $b_0$  in  $k_2 b_0$  über, so ist  $(a_0 | b_0) = (k_1 a_0 | k_2 b_0) = \bar{k}_1 k_2 (a_0 | b_0)$ . Ist  $(a_0 | b_0) \neq 0$ , so folgt  $\bar{k}_1 k_2 = 1$ . Ist ferner eine dritte Schar  $(c_0)$  unter  $T$

invariant, z. B., ist  $c_0 T = k_3 c_0$ , mit  $(a_0 | c_0) \neq 0$ ,  $(b_0 | c_0) \neq 0$ , so muß  $k_1 = k_2 = k_3 = \Theta$  sein,  $\Theta \bar{\Theta} = 1$ . Dann werden auch alle Linearkombinationen von  $a_0, b_0, c_0$  mit demselben Faktor multipliziert, und die zugehörigen Scharen bleiben invariant.

Fassen wir insbesondere die Gruppe  $P_3$  ins Auge. Die  $d$  Elemente des Zentrums von  $G_m$ , die der Identität in  $H_m$  entsprechen, haben die Spur

$$Q_3 = q^3 + 1. \text{ Dazu gibt es in } H_m (Q_1 / d) - 1 \text{ Klassen von } \binom{Q_3}{2} - \binom{Q_1}{2} =$$

$Q_3 q^2 / Q_1$  Elementen mit der Spur  $Q_1$ , die mehr als zwei Scharen invariant lassen. Als Vertreter dieser Klassen nehmen wir reduzible Matrizen, die die Scharen  $a_0: (1, \alpha, 0)$  und  $b_0: (1, \beta, 0)$  mit einem Faktor  $\Theta^n$ ,  $n = 1, 2, \dots (Q_1 / d) - 1$ ,  $\Theta \bar{\Theta} = 1$ , die dritte Koordinate  $x_3$  mit  $\Theta^{-2n}$  multiplizieren. Ähnlich gibt es in  $H_m (q - 2) Q_1 / 2d$  Klassen von je  $Q_3 q^3$  Elementen, die  $a_0$  und  $b_0$  mit verschiedenen Faktoren versehen. Sie haben die Spur 2. Klassen mit der Spur 1 haben Vertreter in der Untergruppe, von der Ordnung  $h_3 - Q_3 Q_2 / Q_1 = q^3 Q_1 / d$ , der mit einer bestimmten Matrix  $M(a; \varepsilon)$  vertauschbaren Matrizen. Eine Klasse enthält die Matrizen  $M(a; \varepsilon)$  selbst.  $(Q_1 / d) - 1$  Klassen von je  $Q_3 Q_2 q^2 / Q_1$  Elementen, deren Ordnungen  $q Q_1$  teilen, entsprechen den obigen Klassen von der Spur  $Q_1$ , wobei jetzt aber die Scharen  $(a_0)$  und  $(b_0)$  nicht mehr invariant sind. Es bleiben mit der Spur 1 die  $d$  Klassen von  $Q_3 Q_2 q / d$  Elementen von der Ordnung  $p$ , bzw. 4, die wir in § 3 untersucht haben. Endlich gibt es zwei verschiedene Arten von Klassen mit der Spur 0. Dies sind einerseits

$$\left( \frac{(q+1)(q-2)}{6d} + \frac{1}{3} - \frac{1}{d} \right) \text{ Klassen von je } h_3 d / Q_1^2 \text{ Elementen, und dazu}$$

eine Klasse von  $h_3 / Q_1^2$  Elementen, deren Ordnungen  $q+1$  teilen; und

$$\text{andererseits } \frac{q^2 - q + 1 - d}{3d} \text{ Klassen von je } Q_2 Q_1 q^3 \text{ Elementen, deren Ord-}$$

$$\text{nungen } \frac{q^2 - q + 1}{d} \text{ teilen.}$$

Betrachten wir jetzt die irreduzible Komponente von  $P_3$  vom Grade  $q^3$ , so haben wir folgende Spuren, oder Charakteren einer irreduziblen Darstellung der Gruppe  $H_3 \equiv HO(3, q^2)$ . Wir geben in vier Spalten 1) die Anzahl von ähnlichen Klassen, 2) die Anzahl von Elementen in einer Klasse, 3) die Spur von einer Matrix in dieser Klasse in der irreduziblen Darstellung vom Grade  $q^3$ , und 4) eine Zahl, die durch die Ordnungen dieser Matrizen geteilt wird.

Klassen	Elemente	Spur	Ordnung-Multiplum
1	1	$q^3$	1
$\frac{q+1}{d} - 1$	$(q^2 - q + 1) q^2$	$q$	$q + 1$
$\frac{q^2 - q - 2}{2d}$	$(q^3 + 1) q^3$	1	$q^2 - 1$
1	$(q^3 + 1) (q - 1)$	0	$p$
$d$	$(q^3 + 1) (q^2 - 1) q / d$	0	$p$ oder $4 = p^2$
$\frac{q+1}{d} - 1$	$(q^3 + 1) (q - 1) q^2$	0	$p (q + 1)$
1	$(q^2 - q + 1) (q - 1) q^3 / d$	-1	$(q + 1) / d$
$\frac{q^2 - q - 8 + 2d}{6d}$	$(q^2 - q + 1) (q - 1) q^3$	-1	$q + 1$
$\frac{q^2 - q + 1 - d}{3d}$	$(q^2 - 1) (q - 1) q^3$	-1	$\frac{q^2 - q + 1}{d}$

(Eingegangen den 31. Juli 1934.)