

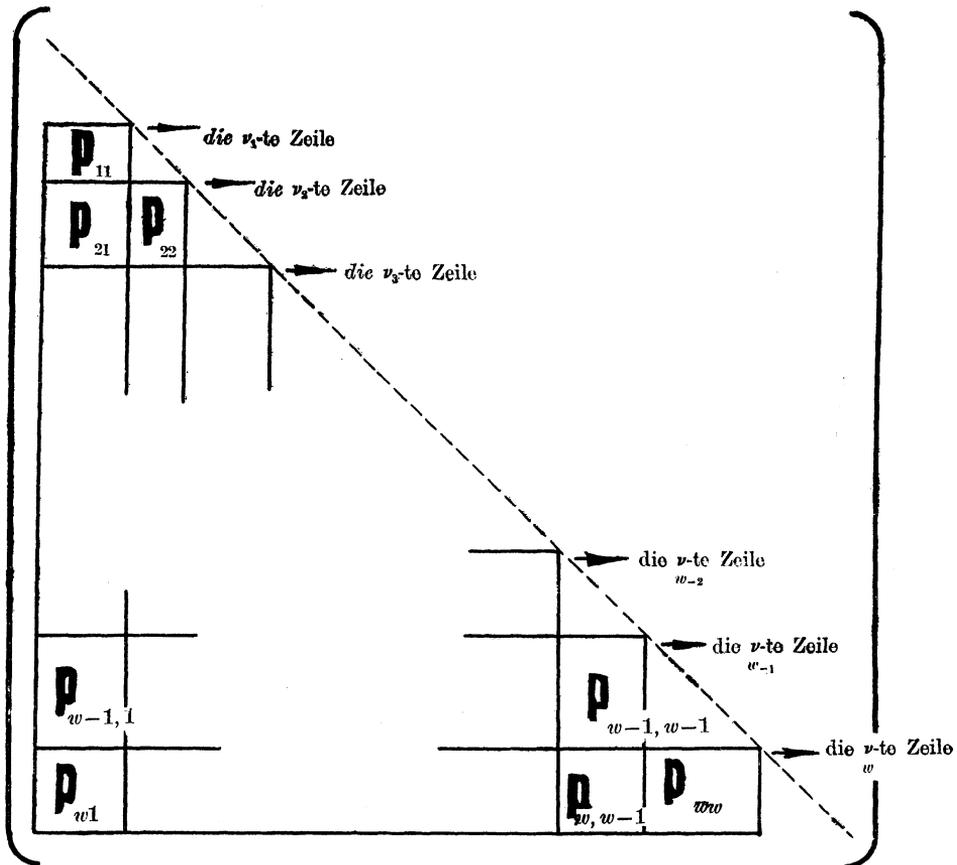
ÜBER DIE STRUKTUR DER METABELSCHEN GRUPPEN, III

KIYOSI TAKETA

(Received October 1, 1951)

In der zweiten Mitteilung¹⁾ habe ich bewiesen, daß die abgeleitete Gruppenmatrix

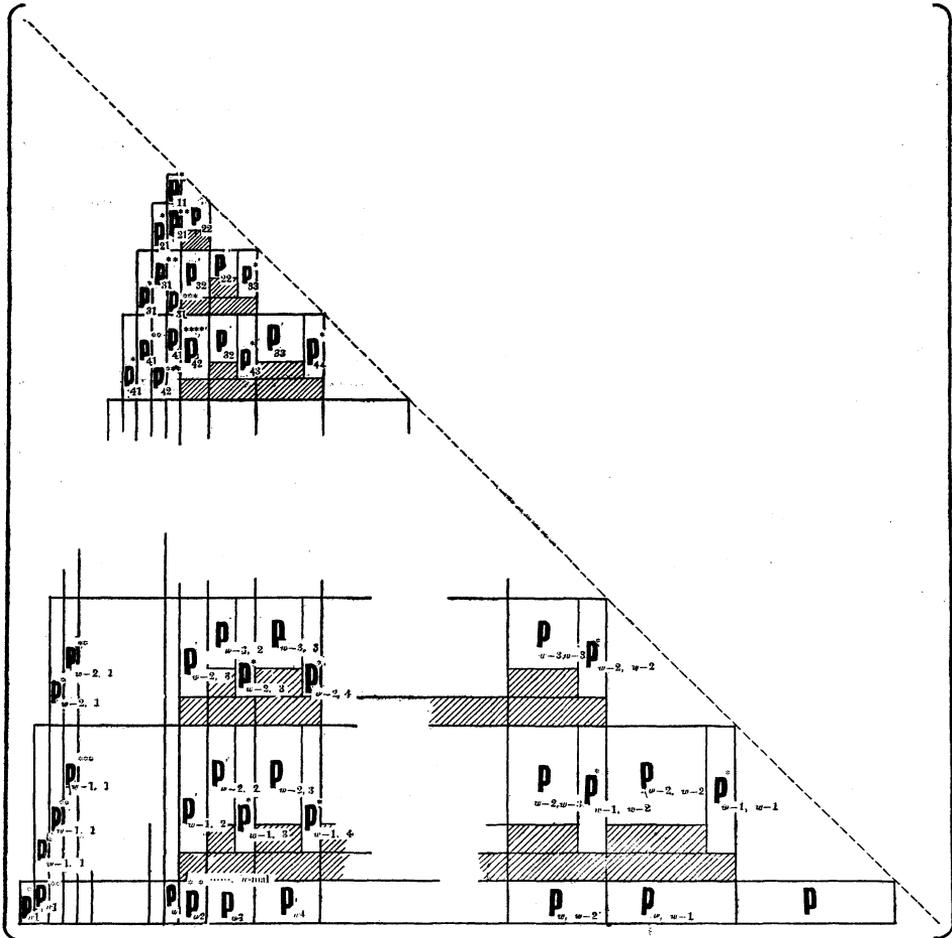
(18) $P =$



von der maximalen Abelschen Substitutionsgruppe \mathfrak{B} in $GF(p^w)$ äquivalent mit der folgenden Matrix

1) Journal of the Osaka Institute of science and technology, 2 (1950), 1-28.

(177)



falls die erste Zeile jedes der Kästchen P_{ii} ; $i = 2, 3, \dots, w$, aus den linear unabhängigen Koeffizienten besteht, wobei die Untermatrix

$$(184) \quad Q = \begin{pmatrix} P'_{22} \\ P'_{32} & P'_{33} \\ P'_{42} & \dots & P'_{44} \\ \dots & \dots & \dots \\ P'_{w-2,2} & \dots & P'_{w-2,w-2} \end{pmatrix}$$

ein Galois-Feld $GF\left(p^{\sum_{i=2}^{w-2} s_i}\right)$ darstellt, wenn P'_{ij} dasjenige Kästchen be-

deutet, das aus den ersteren s_i Zeilen von \mathbf{P}_{ij} besteht. ²⁾

Auch ist es dabei klar geworden, daß \mathfrak{P} die Ordnung

$$p^u \left\{ \sum_{i=1}^w s_i + s_1 (s'_{iw} - 1) \right\}$$

besitzt (II, S. 26).

(I) Die Frage den Typus von dieser Gruppe \mathfrak{P} zu bestimmen, führt folgendermaßen zum Falle der Abelschen Substitutionsgruppe der allgemeinen Ordnung in einem Galois-Feld zurück (I, S. 133). ³⁾

Man bezeichnet diejenige Matrix mit $\mathbf{P}^{[k]}$, welche aus den k -ten Potenzen der einzelnen Elemente von \mathbf{P} besteht, ⁴⁾ d. h. ist

$$(185) \quad \mathbf{P} = A_1 x_1 + A_2 x_2 + \dots + A_g x_g,$$

so wird

$$(186) \quad \mathbf{P}^{[k]} = A_1^k x_1 + A_2^k x_2 + \dots + A_g^k x_g.$$

Ferner läßt man

$$\mathbf{P}_{ij}^{[k]}, \quad i = 1, 2, \dots, w; \quad j = 1, 2, \dots, i,$$

dasjenige Kästchen von $\mathbf{P}^{[k]}$ bedeuten, das dem Kästchen \mathbf{P}_{ij} von \mathbf{P} entspricht, und $\mathbf{Q}_{ij}^{[k]}$ und $\mathbf{Q}_{ij}^{[k]}$ von \mathbf{Q} von analoger Bedeutung sein, so daß

$$\mathbf{Q}_{ij}^{[1]} = \mathbf{P}'_{ij}, \quad i = 2, 3, \dots, w - 2; \quad j = 2, 3, \dots, i,$$

wird.

Da alsdann wegen

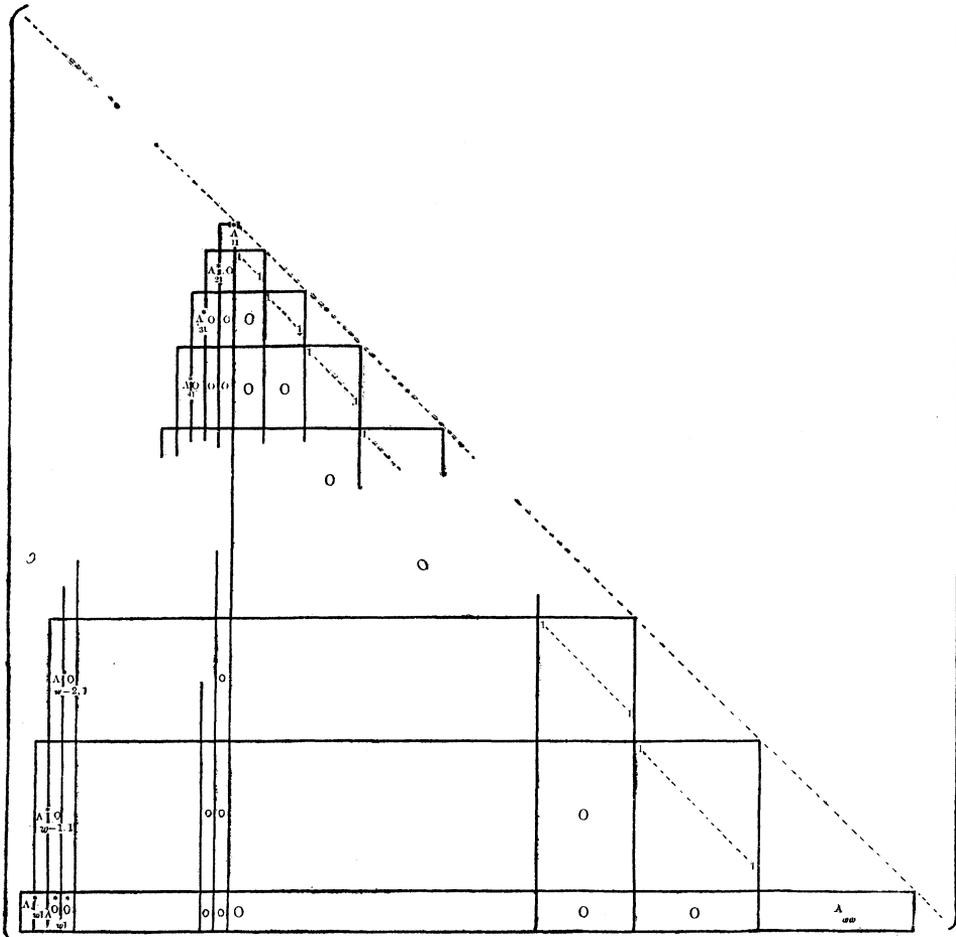
$$(156) \quad \mathbf{AP} = \mathbf{PA}$$

$$(187) \quad \mathbf{P}'_{ij} = \left(\begin{array}{c|c} \mathbf{P}_{i-1, j-1} & \mathbf{P}_{i, j}^* \\ \hline \text{---} & \end{array} \right)$$

2) Wie bisher bedeutet s_i die Anzahl der Spalten des Kästchens \mathbf{P}_{ii} .
 3) Mit I bezeichnet man die erste Mitteilung: Japanese Journal of Mathematics, 13 (1936), 129-232.
 4) Eine Matrix A heißt ein Element von \mathbf{P} , wenn die Matrix $(A + E)$ der \mathbf{P} zugehörigen Substitutionsgruppe \mathfrak{P} angehört (I, S. 138).

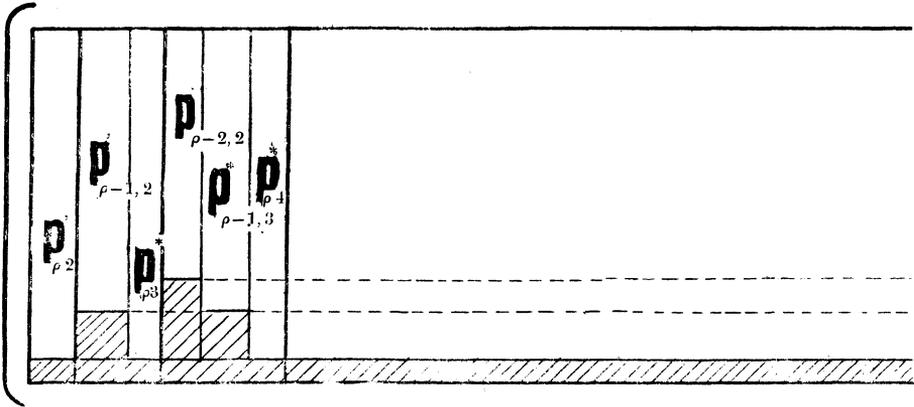
wird, wobei

(188) $A =$



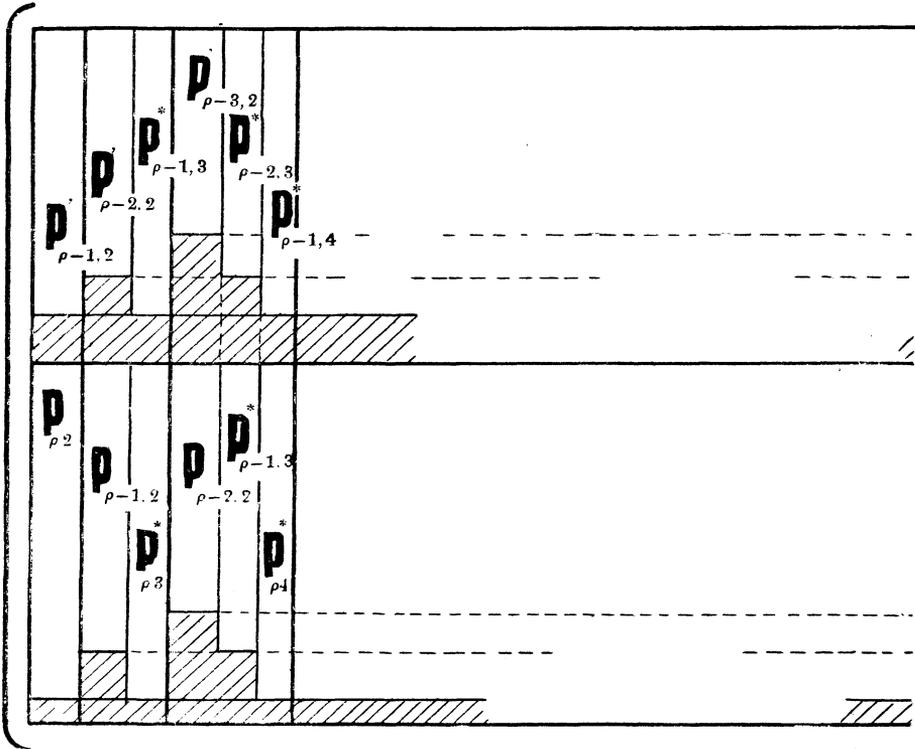
also

(189) $(P_{p2}, P_{p3}, \dots, P_{pp}) =$

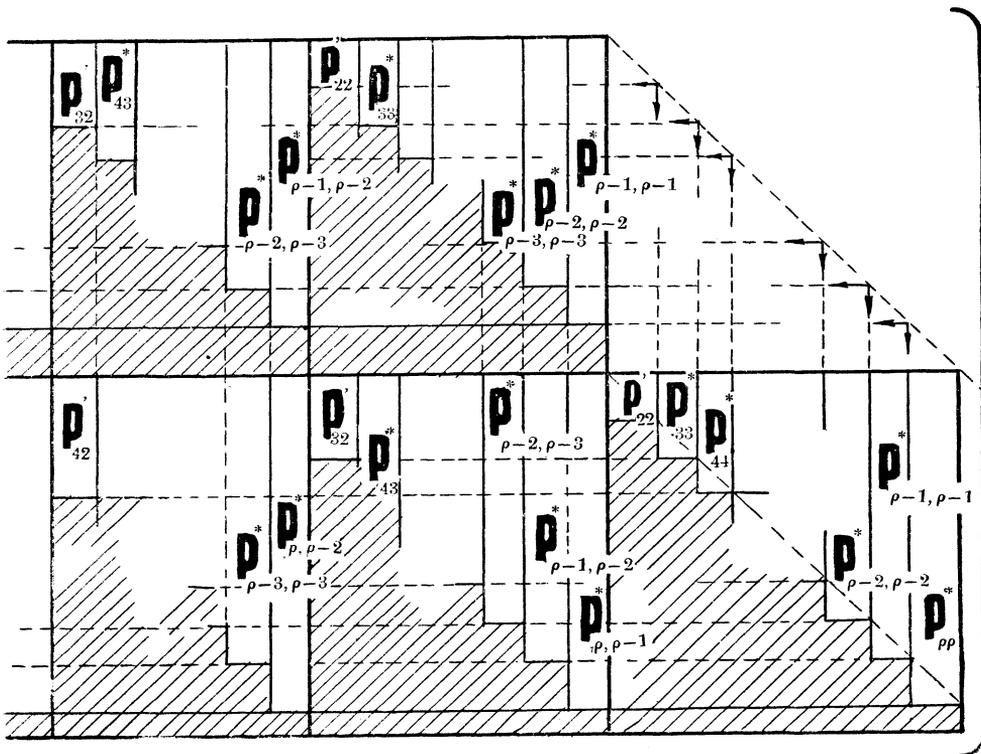
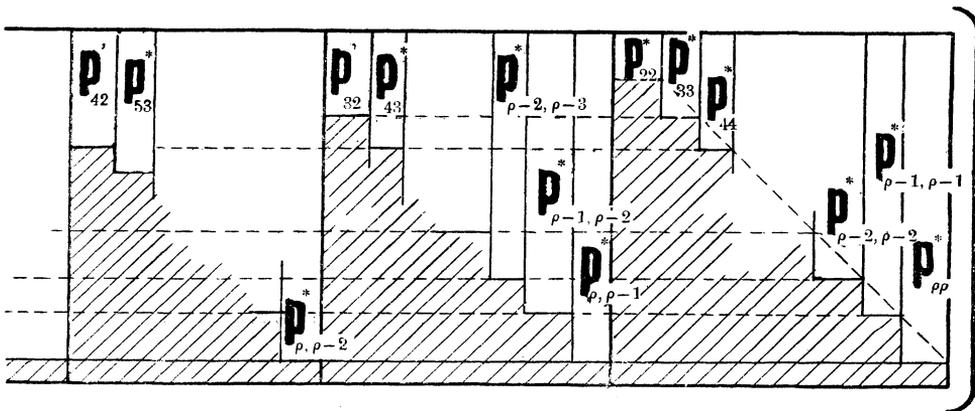


mithin

$$(190) \quad \begin{pmatrix} P_{\rho-1,2} P_{\rho-1,3} \cdots P_{\rho-1,\rho-1} \\ P_{\rho 2} P_{\rho 3} \cdots P_{\rho, \rho-1} P_{\rho \rho} \end{pmatrix} =$$



werden (II, S. 12 – 22), so verschwinden ebenso die letzteren $\sum_{i=\rho-k+1}^{\rho} (s_{i+1} - s_i)$ Zeilen und die letzteren $k - 1$ Kästchen von $(P_{\rho 2}^{[k]}, P_{\rho 3}^{[k]}, \dots, P_{\rho \rho}^{[k]})$ sämtlich, wie auch die letzteren $\sum_{i=\rho-k+2}^{\rho} (s_{i+1} - s_i)$ Zeilen und die ersten $k - 1$ Kästchen



von

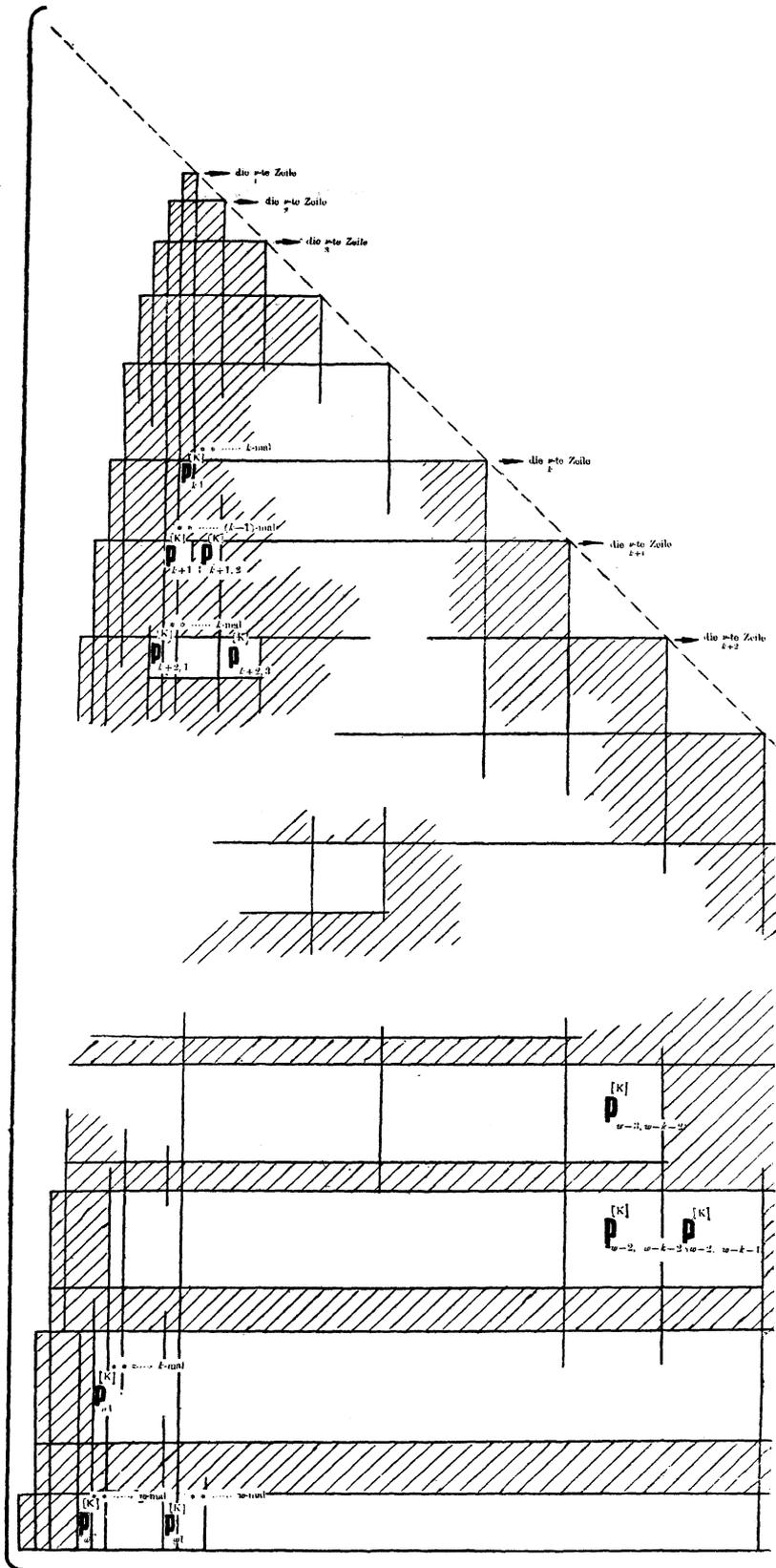
$$(191) \quad (\mathbf{P}_{\rho 1}^{[k]*}, \mathbf{P}_{\rho 1}^{[k]**}, \dots, \mathbf{P}_{\rho 1}^{[k]** \dots \rho\text{-mal}});$$

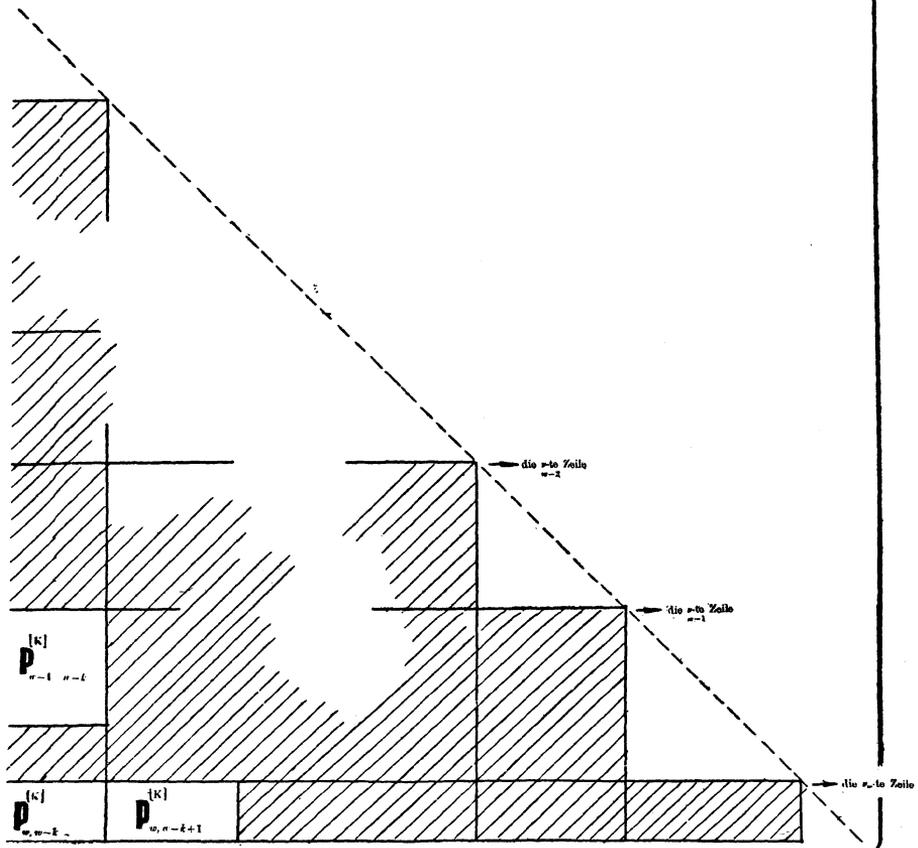
analog sind auch

$$(192) \quad \mathbf{P}_{w i}, \quad w - k + 2 \leq i \leq w; \quad \mathbf{P}_{w 1}^*, \mathbf{P}_{w 1}^{**}, \dots, \mathbf{P}_{w 1}^{** \dots (k-1)\text{-mal}}$$

gleich Null; d.h. wird $\mathbf{P}^{[k]}$ von der folgenden Gestalt sein:

(193)





wobei wegen

$$(194) \quad \mathbf{P}^{[k]}A = A\mathbf{P}^{[k]}$$

die folgenden Beziehungen

$$\mathbf{P}_{ij}^{[k]'} = \left(\begin{array}{c|c} \mathbf{P}_{i-1, j-1}^{[k]'} & \mathbf{P}_{i-1, j}^{[k]'} \\ \hline \text{shaded} & \mathbf{P}_{i, j} \end{array} \right)^* \quad \begin{array}{l} i = 3, 4, \dots, w-1 \\ j = 3, 4, \dots, i \end{array}$$

$$(195) \quad \begin{array}{l} \mathbf{P}_{wi}^{[k]'} = A_{ww} \mathbf{P}_{w-1, i-1}^{[k]}, \quad i = 3, 4, \dots, w, \\ \mathbf{P}_{i1}^{[k]'} \dots \sigma\text{-mal} = \mathbf{P}_{i+1, i+2-\sigma}^{[k]} A_{i+1-\sigma, 1}^*, \quad i = 1, 2, 3, \dots, w-2; \\ \sigma = 1, 2, \dots, i, \end{array}$$

bestehen. Da aber

$$(196) \quad \left(\begin{array}{c} \mathbf{P}_{k+1, 2}^{[k]'} \\ \mathbf{P}_{k+2, 2}^{[k]'} \quad \mathbf{P}_{k+2, 3}^{[k]'} \\ \dots \\ \mathbf{P}_{w-1, 2}^{[k]'} \quad \mathbf{P}_{w-1, 3}^{[k]'} \dots \mathbf{P}_{w-1, w-k}^{[k]'} \end{array} \right), \quad k \geq 2,$$

gleich

$$(197) \quad \left(\begin{array}{c} \mathbf{Q}_{22}^{[k]} \\ \mathbf{Q}_{32}^{[k]} \quad \mathbf{Q}_{33}^{[k]} \\ \dots \\ \mathbf{Q}_{w-k, 2}^{[k]} \dots \mathbf{Q}_{w-k, w-k}^{[k]} \end{array} \right)$$

ist, so verschwinden alle Kästchen von $\mathbf{P}^{[k]}$ außer den folgenden

$$(198) \quad \begin{array}{l} \mathbf{P}_{w-1, 1}^{[k]'} \dots \sigma\text{-mal}, \quad \mathbf{P}_{w, 1}^{[k]'} \dots \sigma\text{-mal}, \quad k-1 < \sigma, \\ \mathbf{P}_{w2}^{[k]}, \quad \mathbf{P}_{w, i}^{[k]'}, \quad i = 3, 4, \dots, w-k+1, \end{array}$$

falls (197) gleich Null ist.

Für $k > 2$ ergeben sich wegen (195) noch die folgenden Beziehungen:⁵⁾

$$\mathbf{P}_{w-1, 1}^{[k]'} \dots \sigma\text{-mal} = \mathbf{Q}_{w-k+1, w-2k-\sigma+1}^{[k]} A_{w-2k-\sigma, 1}^*,$$

$$k \leq \sigma \leq w-1,$$

5) Dies ist stets der Fall, wenn $p > 2$ ist, denn um den Typus einer Abelschen p -Gruppe zu bestimmen, betrachtet man immer die Ordnung der einzelnen Elemente dieser Gruppe.

$$\begin{aligned}
 \mathbf{P}_{w1}^{[k]**\dots\sigma\text{-mal}} &= A_{ww}^{**\dots(k-2)\text{-mal}} \mathbf{Q}_{w-k+2, w-2k-\sigma+2}^{[k]} A_{w-2k+\sigma+1, 1}^* , \\
 (199) \quad & 3 \leq \sigma \leq w, \\
 \mathbf{P}_{wi}^{[k]} &= (\mathbf{P}_{wi}^{[k]'} \mathbf{P}_{wi}^{[k]''}) = A_{ww}^{**\dots(k-2)\text{-mal}} \mathbf{Q}_{w-k+1, i}^{[k]} , \\
 & i = 2, 3, \dots, w - k + 1,
 \end{aligned}$$

wobei $A_{ww}^{**\dots l\text{-mal}}$ dasjenige Kästchen bedeutet, das aus den ersteren s_{w-l} Spalten von A_{ww} besteht.

Mithin wird die Anzahl der Elemente von \mathbf{P} , deren k -te Potenzen nicht verschwinden, gleich der Anzahl der Elemente von \mathbf{Q} , deren zu (197) entsprechende Untermatrix von Null verschieden ist, addiert mit der Anzahl der Elemente von \mathbf{Q} , deren (197) entsprechender Teil verschwindet, während mindestens eines von den zu (198) entsprechenden Kästchen dieser Elemente nicht gleich Null ist.

Damit ist die Frage also zum Falle der Substitutionsgruppe von der beliebigen Ordnung aber vom niedrigerem Grade (I, S. 133-137) zurückgeführt.

(II) Wir haben uns bis jetzt nur auf den Fall beschränkt (II, S. 11-28), in dem

(a) die erste Zeile jedes der Kästchen \mathbf{P}_{ii} ; $i = 2, 3, \dots, w$, aus den linear unabhängigen Koeffizienten besteht.

Dieser ist aber im folgenden Falle

(b) die Spalten jedes der Kästchen \mathbf{P}_{ii} , $i = 2, 3, \dots, w - 1$, voneinander linear unabhängig sind; während die erste Zeile von \mathbf{P}_{ww} aus den linear unabhängigen Koeffizienten besteht, und $\mathbf{P}_{11} \neq 0$ ist enthalten.

In der Tat stimmt der Fall (b) mit dem Falle (a) überein, wenn es mindestens ein Element, sage A , von \mathbf{P} der Art gibt, daß das Kästchen $A_{w-1, w-1}$ vom Rang s_{w-1} ist.

BEWEIS. Da wegen

$$(200) \quad \mathbf{AP} = \mathbf{PA}$$

die folgenden Beziehungen

$$(201) \quad A_{jj} \mathbf{P}_{j-1, j-1} = \mathbf{P}_{jj} A_{j-1, j-1}, \quad w \geq j \geq 3,$$

bestehen, so muß $A_{j-1, j-1}$ vom Rang s_{j-1} sein, insofern A_{jj} den Rang s_j besitzt; denn sonst gäbe es s_{j-1} nicht zugleich verschwindende Konstanten $c_1, c_2, \dots, c_{s_{j-1}}$, der Art, daß

$$(202) \quad A_{j-1, j-1} \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_{s_{j-1}} \end{pmatrix} = 0$$

würde, daraus und aus (201) folgte

$$(203) \quad A_{jj} \mathbf{P}_{j-1, j-1} \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_{s_{j-1}} \end{pmatrix} = 0.$$

Da aber A_{jj} vom Range s_j ist, so bestünde dann gegen die Annahme eine lineare Beziehung zwischen den Spalten von $\mathbf{P}_{j-1, j-1}$.

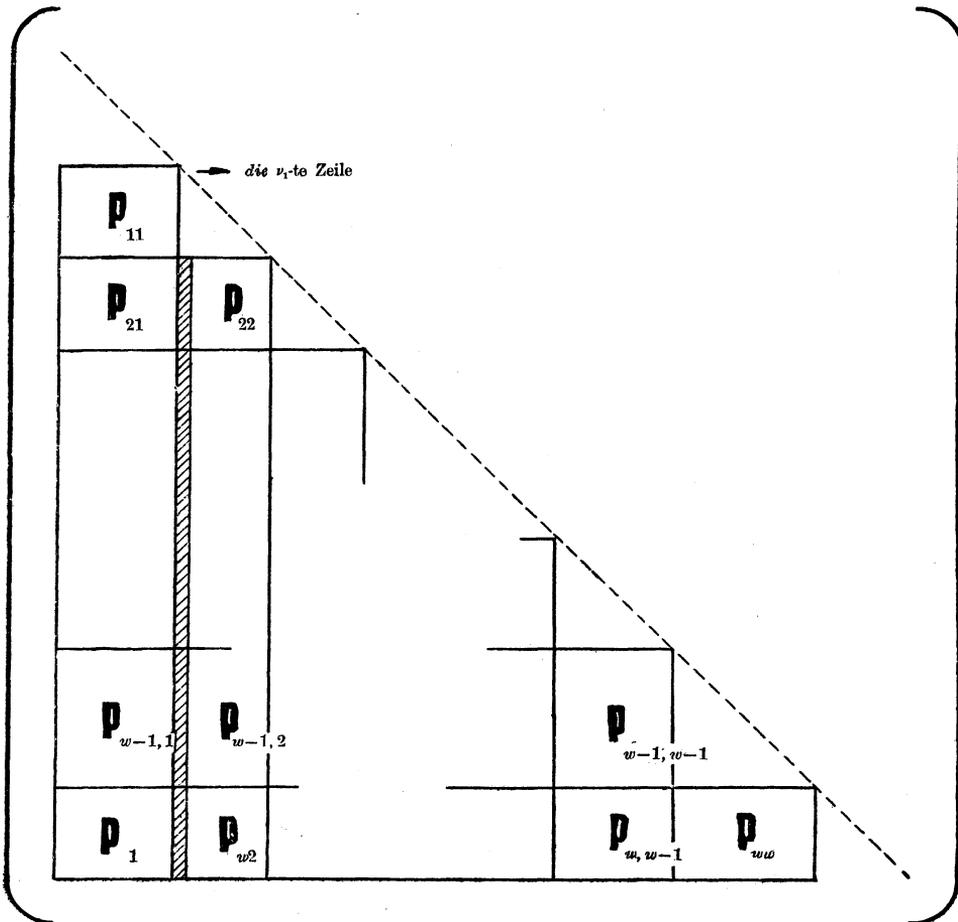
$A_{w-1, w-1}$ nimmt nun nach der Voraussetzung den Rang s_{w-1} , also können wir durch vollständige Induktion beweisen, daß A_{ii} ; $i = 2, 3, \dots, w-1$, je den Rang s_i besitzen!

Man kann diesem Elemente A nach einer geeigneten Transformation von P die Gestalt (188) geben (II, S. 15), und ersehen, daß die Koeffizienten der ersten Zeile jedes der Kästchen P_{ii} ; $i = 2, 3, \dots, w$, linear unabhängig sind, indem man nach der Reihe die v_j -ten; $j = w-1, \dots, 4, 3$, Zeilen der beiden Seiten von (200) vergleicht.

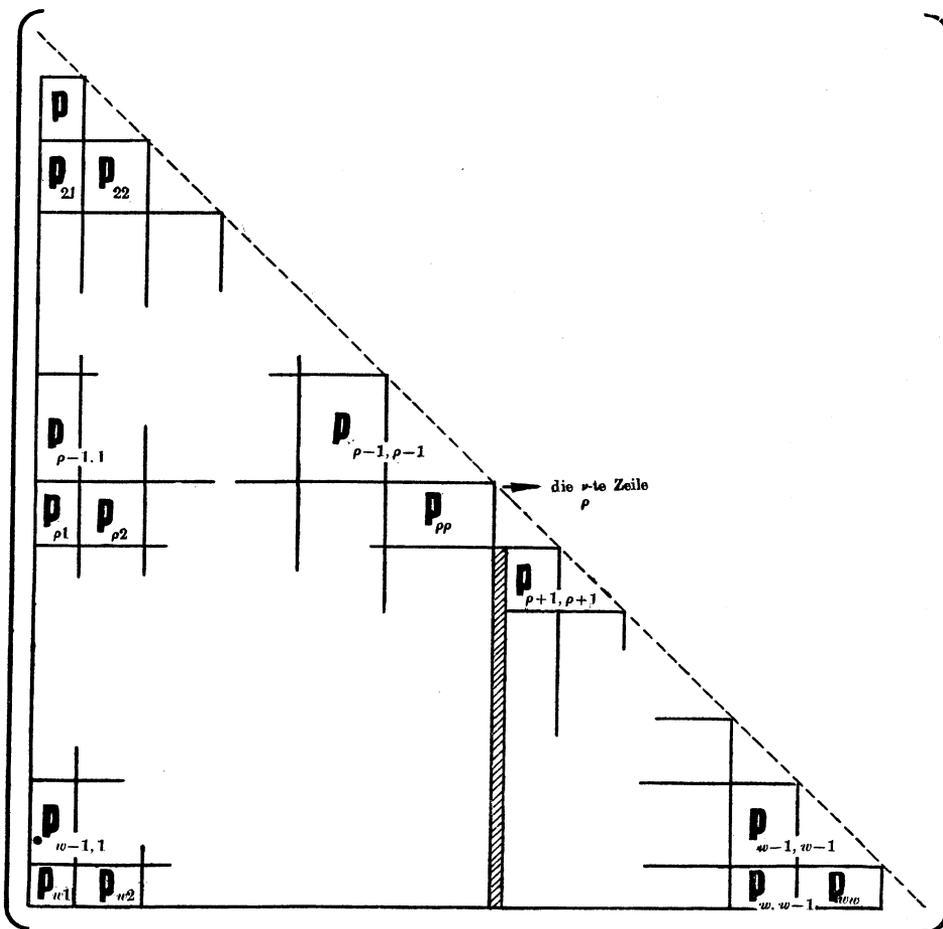
Was die Form von P betrifft, gibt es außer (b) noch die folgenden zwei Möglichkeiten.

(c) Die erste Zeile von P_{11} d. h. die v_1 -te von P besitzt die voneinander linear unabhängigen Koeffizienten, die v_1 -te Spalte verschwindet, während diese Zeile und alle anderen Zeilen von P darunter voneinander linear unabhängig werden, d. h. P nimmt die folgende Gestalt an:

(204)



(d) Die erste Zeile eines Kästchens $P_{\rho\rho}$, $\rho > 2$, hat die linear unabhängigen Koeffizienten, die Kästchen P_{ii} ; $i = 2, 3, \dots, \rho - 1$, je die linear unabhängigen Spalten, $P_{11} \neq 0$, die v_p -te Spalte von P ist gleich Null, während alle Zeilen von P unter der v_p -ten voneinander und den anderen nicht verschwindenden Zeilen von P linear unabhängige werden, d. h. P ist der folgenden Gestalt:
(205)



Um diesen Ergebnis zu beweisen, schicken wir zuerst den folgenden HILFSSATZ 4. Man kann P so gestalten, daß jedes der Kästchen P_{ii} ; $i = 2, 3, \dots, w$, aus den linear unabhängigen Spalten besteht. voraus.

BEWEIS. Man läßt alle nicht verschwindenden Spalten von P voneinander linear unabhängig sein, indem man eventuell P mit einer geeigneten Matrix der folgenden Gestalt

(206)

$$\left[\begin{array}{c} 1 \\ \vdots \\ \text{die } \kappa\text{-te Spalte} \\ \vdots \\ c_1 \\ c_2 \\ \vdots \\ c_r \\ \vdots \\ 1 \end{array} \right], \quad c_1 \neq 0, \quad \nu_1 \leq \kappa \leq \nu_w,$$

transformiert, und dann setzt man solche Spalten [am rechten Teil von P zusammen, so daß

(207)

The diagram shows a large matrix P enclosed in a rounded rectangle. A dashed diagonal line runs from the top-left corner to the bottom-right corner. The matrix is partitioned into several blocks:

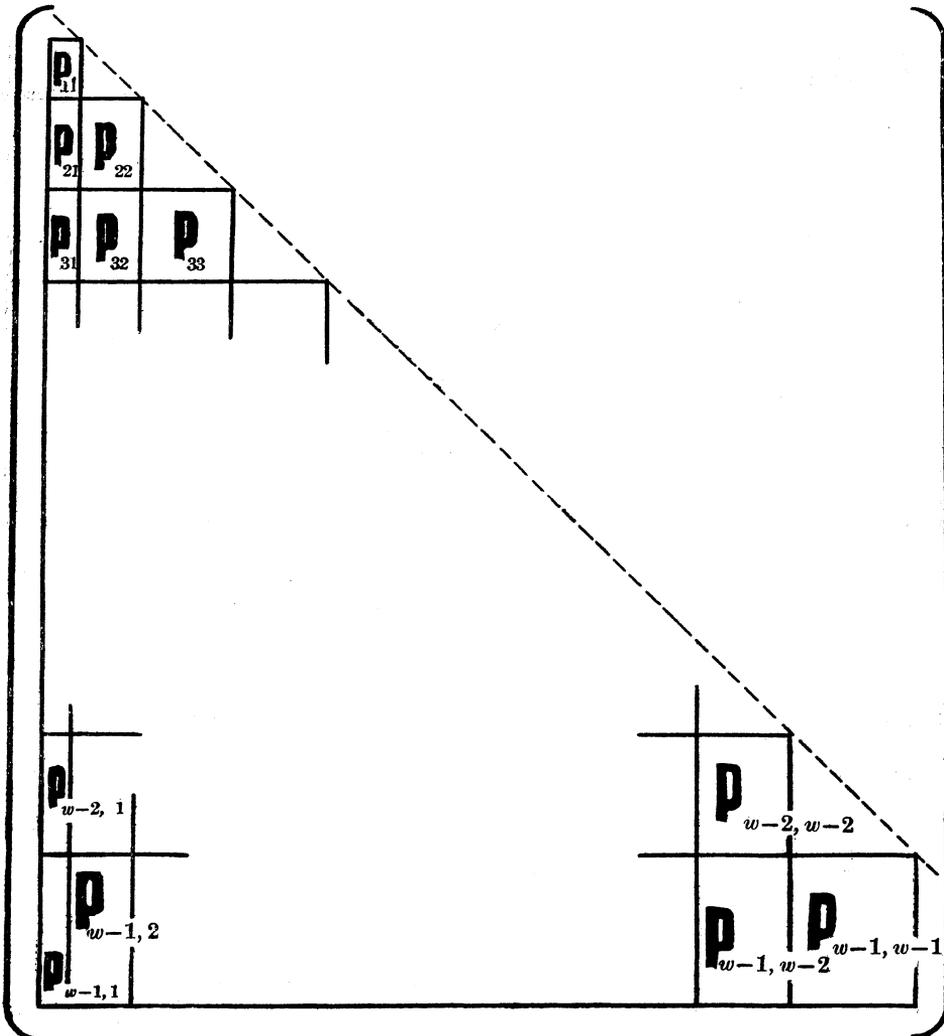
- Top-left: A block containing p_{11} .
- Below p_{11} : A row of two blocks, p_{21} and p_{22} .
- Below that: A row of three blocks, p_{31} , p_{32} , and p_{33} .
- Bottom-left: A row of two blocks, $p_{w-1,1}$ and $p_{w-1,2}$.
- Bottom-right: A row of three blocks, $p_{w,w-1}$, $p_{w,w-1}$, and $p_{w,w}$.

Other blocks are present but not labeled with p and subscripts, including a block $p_{w-1,w-1}$ in the lower right area.

insbesondere $P_{w,w}$ aus den linear unabhängigen Spalten bestehen.

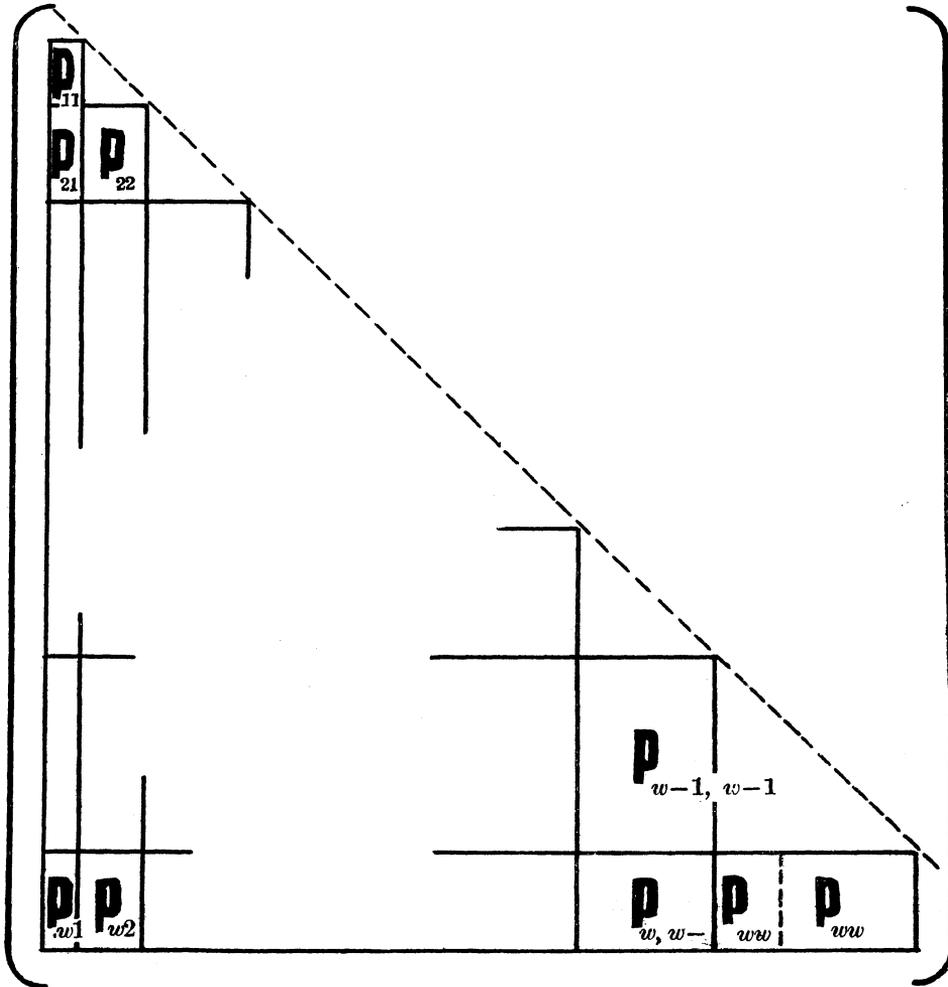
Wendet man dieses Verfahren wieder auf

(208)



an, dann geht (207) in die folgende Gestalt

(209)



über, wobei der (208) entsprechende Teil linear unabhängige Spalten besitzt.

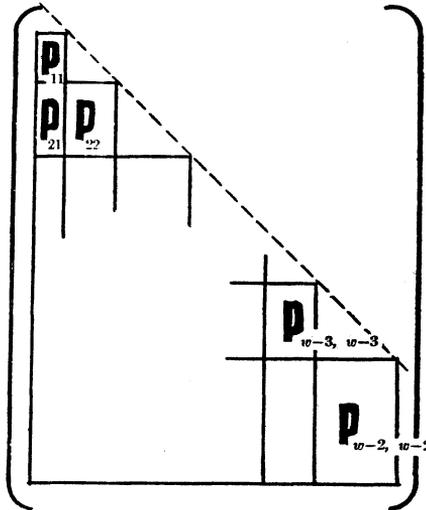
Da aber (207) schon aus den linear unabhängigen Spalten bestanden ist, so ist auch die Untermatrix

$$(210) \quad (\mathbf{P}'_{ww}, \mathbf{P}_{ww}),$$

und betrachtet man bei (209) diese Untermatrix als das Kästchen \mathbf{P}_{ww} , so werden die zwei Kästchen $\mathbf{P}_{w-1, w-1}$, \mathbf{P}_{ww} die verlangte Gestalt erhalten.

Mit der Untermatrix

(211)



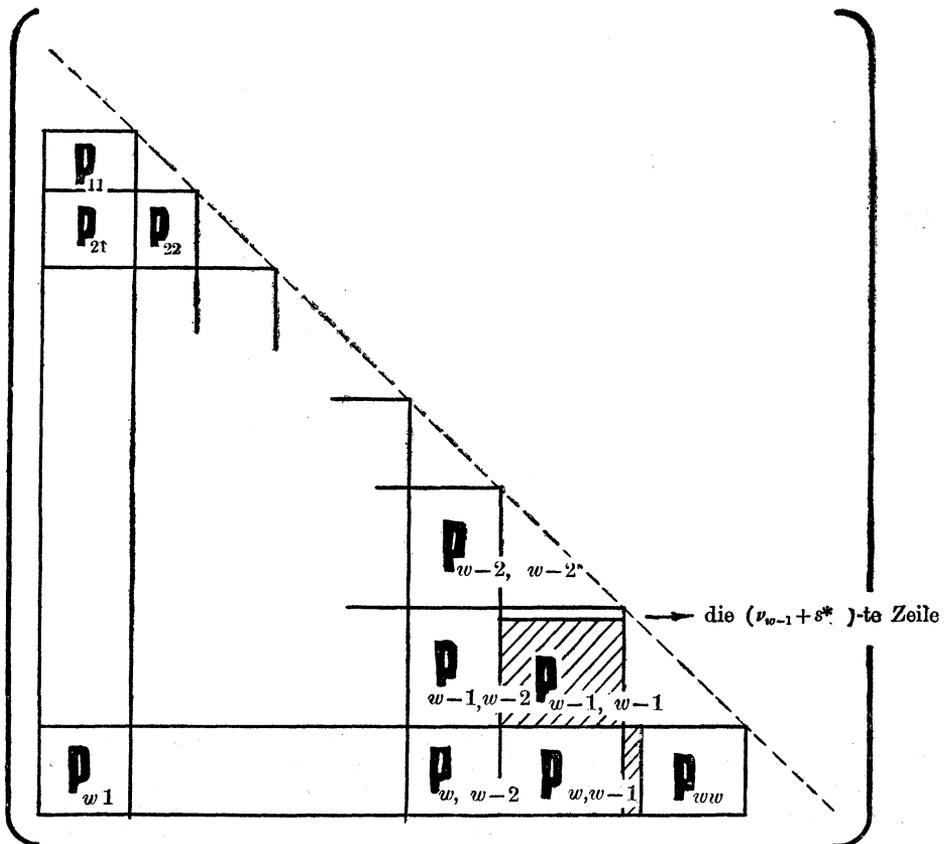
anfangend, setzen wir das bisherige Verfahren wiederholt fort, so daß die unsre Bedingung endlich erfüllt wird, w. z. b. w.

Sind nun die Koeffizienten von irgend einer Zeile des Kästchens \mathbf{P}_{ww} bei dem obigen Beweise linear unabhängig, so wird es der Fall (b) werden, wenn man diese Zeile durch gleichzeitige Vertauschung der Zeilen und Spalten von \mathbf{P} als die erste von \mathbf{P}_{ww} benutzt.

Falls keine Zeile von \mathbf{P}_{ww} solche Eigenschaft besitzt, dann nimmt man o. B. d. A. so an, daß die ersteren $s_1, s_2 > 0$, Koeffizienten der ersten Zeile von \mathbf{P}_{ww} linear unabhängig sind, während alle anderen Koeffizienten dieser Zeile verschwinden (II, S. 4).

Alsdann vertauscht man die ν_w -te Zeile und Spalte von \mathbf{P} je gleichzeitig mit der $(\nu_{w-1} + s_1)$ -ten, so daß \mathbf{P} der folgenden Gestalt

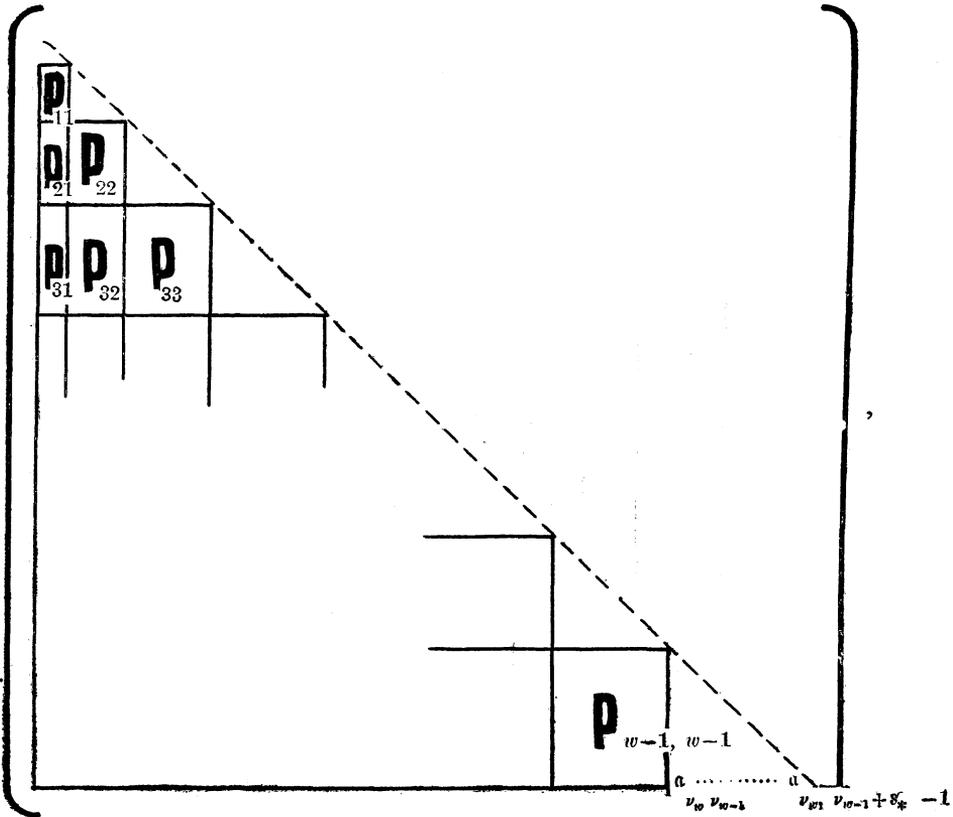
(212)



wird.

Besteht nun eine lineare Beziehung zwischen den Spalten von

(213)

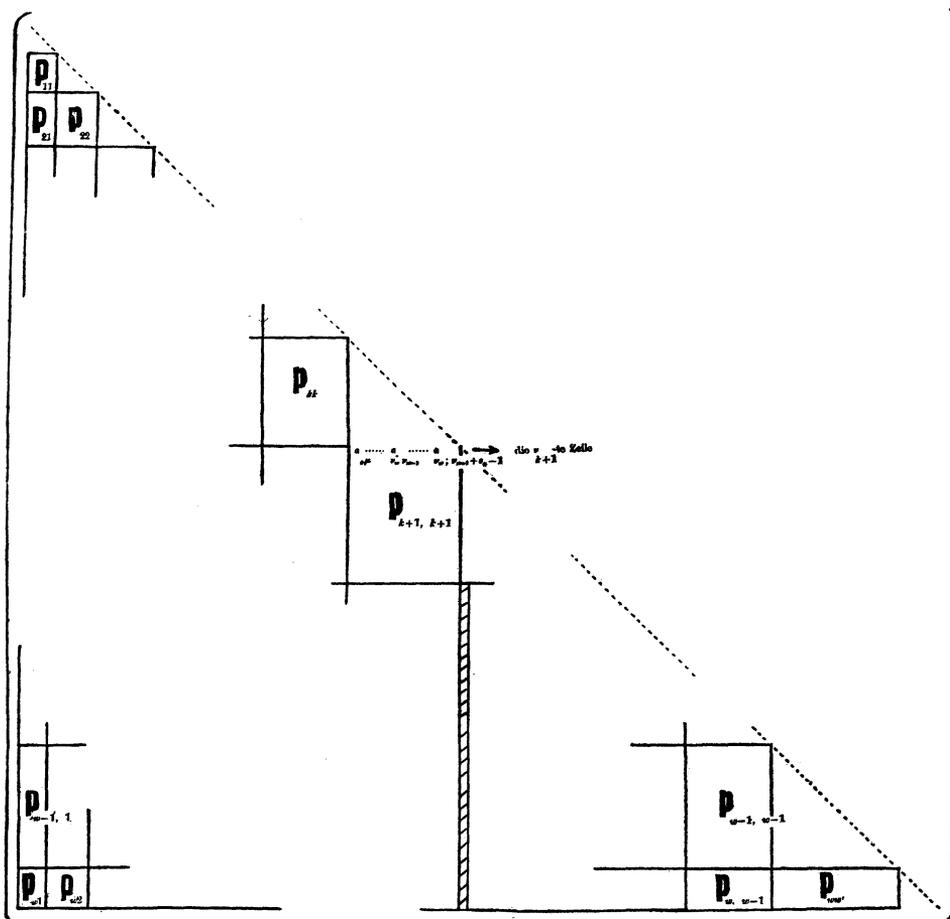


so läßt man alle von solchen Spalten, die den anderen linear abhängen, verschwinden, und am rechten Ende von (213) nebeneinander zusammen liegen, als dann verschiebt man diejenige Zeile von \mathbf{P} , welche die Koeffizienten

(214)
$$a_{v_w, v_w-1} a_{v_w, v_w-1+1} \dots a_{v_w, v_w+s_x-1}$$

enthält, wie bisher möglichst nach oben, so daß \mathbf{P} die folgende Gestalt annimmt:

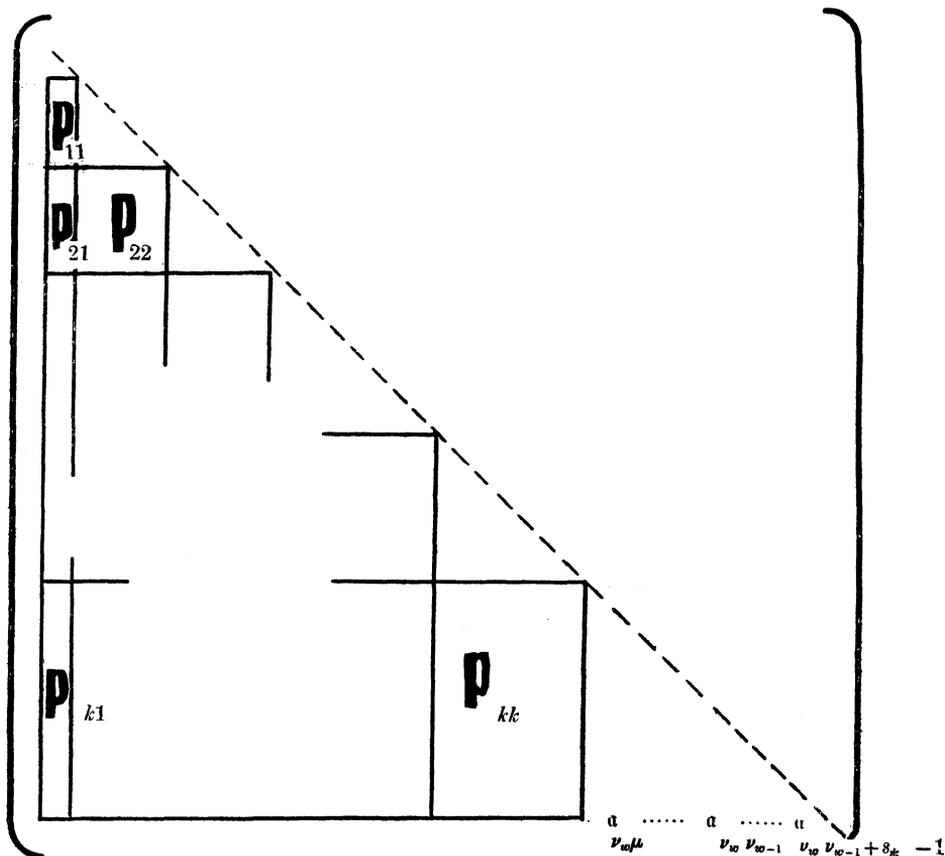
(215)



wobei die Koeffizienten der ersten Zeile von $P_{k+1, k+1}$, unter denen die Koeffizienten (214) sich befinden, voneinander linear unabhängig werden, indem die ν_{k+1} -te Spalte von P verschwindet.

Da man bei (215) o. B. d. A. noch so annehmen kann, daß

(216)



aus den linear unabhängigen Spalten besteht, weil es genügt eventuell nur dasselbe Verfahren wie bei (212) wiederzuholen, so wird P gleich (204), falls

$$P_{ij} = 0; \quad 1 \leq i \leq k, \quad 1 \leq j \leq i,$$

ist, im sonstigen Falle kann man P nach dem Hilfssatz 4 so gestalten, daß jedes der Kästchen P_{si} ; $i = 2, 3, \dots, k$, die linear unabhängigen Spalten besitzt, so daß die Gestalt (205) sich ergibt.

Bestünde nun bei (204) eine lineare Beziehung zwischen der ν_1 -ten und den anderen Zeilen darunter, so könnte man mindestens eine Zeile, sage die σ -te, von diesen Zeilen verschwinden lassen (II, S. 11), und alsdann zu P noch ein Element der folgenden Gestalt

(217)

$$\left(\begin{array}{c} 0 \\ \vdots \\ a_{\nu_1, \sigma} \\ \vdots \\ 0 \end{array} \right)$$

hinzufügen, was der Annahme widerspricht, daß \mathbf{P} maximal Abelsch ist.

Das analoge gilt auch für (205).

Nimmt man nun bei (204) die ν_1 -te Zeile und Spalte zugleich weg, so bildet der übrige Teil der Matrix eine abgeleitete Gruppenmatrix \mathbf{P}' , um 1 niedrigeres Grades als \mathbf{P} . Bezeichnet man dann die zu \mathbf{P}' zugehörige Gruppe mit \mathfrak{P}' , so wird \mathfrak{P} ein direktes Produkt von \mathfrak{P}' und einer Gruppe vom Typus $(p, p, \dots, s_1\text{-mal})$, die durch die abgeleitete Gruppenmatrix der folgenden Gestalt

(218)

$$\left(\begin{array}{c} 0 \\ \vdots \\ a_{\nu_1, 1} \dots a_{\nu_1, \nu_1-1} \\ \vdots \\ 0 \end{array} \right)$$

dargestellt wird.

\mathfrak{P}' wird auch eine maximale Abelsche Gruppe. Denn da $s_1 s'_0$ voneinander linear unabhängige Matrizen der folgenden Gestalt

(219)

in \mathbf{P} enthalten sind, so muss jede Matrix M , die mit \mathbf{P} vertauschbar ist, von der Gestalt

(220)

sein, und falls M zu einer Erweiterung von \mathfrak{P} , deren Ordnung auch gleich einer Potenz von p ist, angehört, dann kann man bei $\bar{M} = M - E$ o. B. d. A. annehmen, daß alle Koeffizienten auf und oberhalb der Hauptdiagonalen verschwinden.

Alsdann muss $M \in \mathfrak{P}$ sein, denn sonst könnte man gegen die Annahme, daß \mathfrak{P} maximal Abelsch ist, noch eine Matrix zu \mathbf{P} hinzufügen, die man dadurch erhielt, indem man \bar{M} noch eine Nullspalte und \sim zeile, die bei \mathbf{P} der ν_1 -ten entsprechen sollen, gibt.

Ist umgekehrt eine abgeleitete Gruppenmatrix einer maximalen Abelschen p -Substitutionsgruppe Grades $n - 1$ gegeben, so kann man daraus wie oben eine Gruppenmatrix mit der verschwindenden ν_1 -ten Spalte und Zeile bilden, und diese stellt zusammen mit den Matrizen der Gestalt (218) eine maxi-

male Abelsche p -Gruppe Grades n dar.

Also führt die Frage zum Falle vom niedrigeren Grade zurück.

(Fortsetzung folgt)

TOTUKA, YOKOHAMA.