

Zeitschrift:	Commentarii Mathematici Helvetici
Herausgeber:	Schweizerische Mathematische Gesellschaft
Band:	30 (1956)
Artikel:	Über die Struktur der Burnsidegruppen mit zwei Erzeugenden und vom Primzahlexponenten $p > 3$.
Autor:	Meier-Wunderli, Heinrich
DOI:	https://doi.org/10.5169/seals-23908

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: 02.02.2026

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

Über die Struktur der Burnsidegruppen mit zwei Erzeugenden und vom Primzahlexponenten $p > 3$

von HEINRICH MEIER-WUNDERLI, Zürich

Die Frage nach der Struktur der freien Gruppen mit zwei Erzeugenden und vom Exponenten p wurde von *Burnside*¹⁾ erstmals zum Gegenstand von Untersuchungen gemacht. Ob die Burnsidegruppen für $p > 3$ endliche oder unendliche Ordnung haben, ist ein bisher ungelöstes berühmtes Problem der allgemeinen Gruppentheorie²⁾.

Eine der Hauptaufgaben, die sich im Hinblick auf das eben erwähnte Problem von Burnside stellt, ist nach *P. Hall* die Bestimmung des zur Primzahl p und Gewicht w gehörenden Dimensionsdefektes δ_w^p .

Es sei F die freie Gruppe aus zwei freien Erzeugenden α_1 und α_2 . F^p sei der von den p -ten Potenzen in F erzeugte Normalteiler. Ferner sei $F = H_1 \supset H_2 \supset H_3 \supset \dots$ die bekannte absteigende Zentralreihe von F und $F/F^p = B_1^p \supset B_2^p \supseteq B_3^p \supseteq \dots$ die entsprechende Reihe von F/F^p .

Mit d_w bezeichnen wir die *Wittsche Anzahl*³⁾ der freien Erzeugenden der freien Abelschen Gruppe H_w/H_{w+1} und mit d_w^p die Anzahl der Basis-elemente in der elementaren Abelschen Gruppe B_w^p/B_{w+1}^p .

Dann setzen wir mit P. Hall

$$d_w^p = d_w - \delta_w^p .$$

Nimmt man als Erzeugende von H_w/H_{w+1} die in Paragraph 1 definier-ten Basiskommutatoren vom Gewicht w , so bezeichne $d_{(w_1, w_2)}$ die

¹⁾ W. Burnside, On an unsettled question in the theory of discontinuous groups, Quart. J. Math. 33 (1902), p. 230–238.

²⁾ R. Baer, The higher commutator subgroups of a group, Bull. Amer. Math. Soc. 50, 3 (1944), p. 143–160. Vgl. ebenda weitere Literatur zum Burnsideproblem.

³⁾ E. Witt, Treue Darstellung Liescher Ringe, J. reine angew. Math. 177 (1937), p. 152–160.

Anzahl der Basiskommutatoren, die in der Komponente α_i das Gewicht w_i ($i = 1, 2$) haben⁴⁾.

Wählt man als Basiselemente der elementaren Abelschen Gruppe B_w^p/B_{w+1}^p ebenfalls Basiskommutatoren, so verstehen wir unter $d_{(w_2, w_1)}^p$ die bezüglich dieser Basis genommene analoge Anzahl.

Ist $d_{(w_2, w_1)}^p$ von der Wahl der Kommutatorbasis unabhängig, so erweist sich der Ansatz

$$d_{(w_2, w_1)}^p = d_{(w_2, w_1)} - \delta_{(w_2, w_1)}^p$$

als noch zweckmäßiger.

Unser Hauptresultat lautet dann : *Setzt man*

$$\tau \equiv a \pmod{6} \quad (a = 1, 2, 3, 4, -1, 6) ,$$

so gilt die Formel

$$\delta_{(3, p+\tau-3)}^p = \frac{1}{3!} (a + 2\tau + 3\tau^2) \quad \tau = 0, 1, 2, \dots, p-2 .$$

Als Korollar unseres Hauptsatzes beweisen wir ferner : *Die Klasse c der Burnsidegruppen vom Exponenten $p > 3$ ist stets $\geq 2p-1$ ⁵⁾.*

§ 1. Basiskommutatoren

Die freien Erzeugenden $\alpha_1, \alpha_2, \dots, \alpha_n$ einer freien Gruppe F ($n \geq 2$) bilden in dieser Anordnung eine Eindeutigkeitsbasis für die Faktor-Kommutatorgruppe von F . Wenn wir diese Bedeutung der freien Erzeugenden von F hervorheben wollen, so nennen wir sie auch Basiskommutatoren vom Gewicht 1. An Stelle von α_j schreiben wir dann $P_{1,j}$ ($j = 1, 2, \dots, n$). Ferner sagen wir, $P_{1,i}$ gehe $P_{1,j}$ voran (in Zeichen $P_{1,i} < P_{1,j}$) dann und nur dann wenn $i < j$. Statt $P_{1,i}$ schreiben wir auch P_i .

Wir definieren induktiv, was wir unter der geordneten Reihe der Basiskommutatoren $P_{c,j}$ ($j = 1, 2, \dots, d_c(n)$) vom Gewicht c verstehen wollen.

Zu diesem Zweck dürfen wir annehmen, die Basiskommutatoren vom Gewicht $< c$ seien bereits erklärt und vermöge einer Anordnungsrelation „ $<$ “ wohlgeordnet.

⁴⁾ $d_{(w_1, w_2, \dots, w_r)} = \frac{1}{w} \sum_{t|m} \mu(t) \frac{\frac{w}{t}!}{\frac{w_1}{t}! \frac{w_2}{t}! \dots \frac{w_r}{t}!} (\sum_{i=1}^r w_i = w); m = (w_1, w_2, \dots, w_r).$

⁵⁾ Daß die Klasse c der Burnsidegruppen für $p > 3$ stets $\geq 2p-2$ ist, folgt aus einem Satz von J. A. Green, On groups of odd prime-power exponent, J. London Math. Soc. 27 (1952), p. 476–485.

Dann definieren wir: Die Basiskommutatoren vom Gewicht c haben alle die Gestalt $P_{c,i} = [P_{a,k}, P_{b,j}]$ mit den folgenden Eigenschaften

- (i) $a + b = c$
- (ii) $a \geq b \geq 1$
- (iii) Ist $a = b$, so soll $P_{b,j} < P_{a,k}$
- (iv) Ist $a > b$ und also $P_{a,k} = [P_{e,i}, P_{f,h}]$, so soll entweder $P_{f,h} = P_{b,j}$ sein oder $P_{f,h} < P_{b,j}$.
- (v) $P_{a,k} < P_{c,j}$ ($1 \leq a < c$)
- (vi) Ist $P_{c,i} = [P_{d,r}, P_{e,s}]$ und $P_{c,l} = [P_{a,k}, P_{b,j}]$, so gilt $P_{c,i} < P_{c,l}$, wenn entweder $P_{e,s} < P_{b,j}$ oder $P_{d,r} < P_{a,k}$ falls $P_{e,s} = P_{b,j}$.

Es gilt nun der überaus wichtige Satz⁶⁾

1. Satz. Die Basiskommutatoren vom Gewicht $\leq c$ liefern eine geordnete Eindeutigkeitsbasis der freien nilpotenten Gruppe der Klasse c und mit der Erzeugendenzahl n .

Das heißt jedes Element aus $F \bmod H_{c+1}$ hat eindeutig die Gestalt

$$P_{1,1}^{x_{1,1}} P_{1,2}^{x_{1,2}} \dots P_{1,n}^{x_{1,n}} \dots P_{c,1}^{x_{c,1}} P_{c,2}^{x_{c,2}} \dots P_{c,d_c}^{x_{c,d_c}} \quad (-\infty < x_{i,j} < \infty) . \quad (1)$$

Insbesondere hat also jedes Element aus H_c/H_{c+1} eine und nur eine Darstellung in der Form

$$\prod_{k=1}^{d_c} P_{c,k}^{x_{c,k}} \quad (-\infty < x_{c,j} < \infty) . \quad (2)$$

Zur Herleitung der Form (2) genügen die Kommutatorregeln $(\bmod H_{c+1})$

$$\begin{aligned} [x, yz] &\equiv [x, y][x, z] \\ [xy, z] &\equiv [x, z][y, z] \\ [x, y, z] &\equiv [x, [y, z]] [x, z, y] \\ [x, y]^{-1} &= [y, x] \end{aligned} \quad (3)$$

Im Hinblick auf spätere Anwendungen sollen noch einige spezielle Basiskommutatoren näher betrachtet werden. Wir beginnen mit dem Kommutator

$$[P_2, P_1, \underbrace{P_1, \dots, P_1}_r] \equiv [P_2, rP_1] .$$

⁶⁾ M. Hall, A basis for free Lie rings and higher commutators in free groups, Proc. Amer. math. Soc. 1 (1950). — H. Meier-Wunderli, Note on a basis of P. Hall for the higher commutators in free groups, Comment. Math. Helv. 26 (1952), p. 1.

Ebenso soll $[P_2, rP_1, sP_2]$ ein Symbol sein für den Kommutator $[[P_2, rP_1], sP_2]$.

Wir bilden nun weiter die folgenden Basiskommutatoren :

$$[P_2, rP_1, [P_2, sP_1]] = B_s \\ (0 \leq s < r; r + s + 2 = c)$$

$$[P_2, rP_1, [P_2, sP_1], [P_2, tP_1]] = B_{s,t} \\ (r > s \leq t \leq r + s + 1; r + s + t + 3 = c)$$

$$[P_2, rP_1, [P_2, sP_1, [P_2, tP_1]]] = B_{s,t} \\ (t < s; s + t < r - 1; r + s + t + 3 = c)$$

Wir fragen nun nach der Darstellung (2) des Kommutators

$$[P_2, rP_1, P_2, sP_1]$$

mit $r + s + 2 = c$.

Zieht man nach den Regeln (3) die s Faktoren P_1 nach vorne durch, so erhält man mod H_{r+s+3}

$$[P_2, rP_1, P_2, sP_1] \equiv \prod_{t=0}^s [P_2, (r+s-t)P_1, [P_2, tP_1]]^{\binom{s}{t}}.$$

In diesem Produkt sind die Faktoren mit $2t < r + s$ bereits Basiskommutatoren B_t . Die übrigen lassen sich als B_u^{-1} mit $u = r + s - t$ schreiben. So erhält man die gesuchte Darstellung :

$$[P_2, rP_1, P_2, sP_1] \equiv \prod_{t=0}^{r-1} B_t^{\binom{s}{t}} \prod_{t=r}^{\frac{r+s-1}{2}} B_t^{\binom{s}{t}} - \binom{s}{r+s-t}. \quad (4)$$

§ 2. Ein Satz über die Exponenten in der Hallschen Identität ⁷⁾

Entwickelt man die Potenz $(P_1^{x_1} P_2^{x_2})^n$ in F mit $x_1, x_2 > 0$ und $n = 2, 3, \dots$ mod H_{w+1} gemäß der Normalform (1), so ist das Resultat eine Identität der Gestalt

$$(P_1^{x_1} P_2^{x_2})^n \equiv \prod_{c=1}^w P_{c,1}^{f_{c,1}^{(n)}} P_{c,2}^{f_{c,2}^{(n)}} \dots P_{c,d_c}^{f_{c,d_c}^{(n)}}. \quad (5)$$

Dies ist die bekannte Hallsche Identität und es gilt der fundamentale Satz von Hall :

Die Exponenten in (5) sind von der Form

$$f_{c,j}^{(n)} = \sum_{k=1}^{\min(c,n)} \binom{n}{k} a_{c,j}^{(k)}(x_1, x_2). \quad (6)$$

⁷⁾ P. Hall, A contribution to the theory of groups of prime-power order, Proc. London Math. Soc. II. Ser. 36 (1933), p. 29–95.

Über die Polynome $a_{c,j}$ in (6) gibt der folgende Satz Aufschluß.

2. Satz: Die $a_{c,j}^{(k)}$ in (6) sind ganze rationale Polynome in den Unbestimmten $(\frac{x_1}{u})$ und $(\frac{x_2}{v})$. Die natürlichen Zahlen u und v genügen der Ungleichung $1 \leq u \leq c - k + 1$ resp. $1 \leq v \leq c - k + 1$.

Beweis. Wir benutzen den Durchzieh- und Labeling-Prozeß von P. Hall. Ähnlich wie bei Hall schreiben wir die Potenz links in (5) formal in der Gestalt

$$\prod_{\varrho=1}^n P_1^{(\varrho,1)} P_1^{(\varrho,2)} \dots P_1^{(\varrho,x_1)} P_2^{(\varrho,1)} P_2^{(\varrho,2)} \dots P_2^{(\varrho,x_2)}. \quad (7)$$

Das Symbol (ϱ, τ) von P_1 oder P_2 heißt Label von P_1 oder P_2 ; es beschreibt die Stellung von P_1 oder P_2 innerhalb des Produktes (7) eindeutig.

Man gewinnt nun die Form (5) dadurch, indem man in (7) zuerst alle P_1 , dann alle P_2 , dann alle $[P_2, P_1] = P_{2,1}$ usw., kurzum alle überhaupt im Durchziehprozeß auftretenden Basiskommutatoren $P_{c,j}$ ihrer Anordnung gemäß an die zugehörige Stelle in (1) bringt, durch eine Reihe von elementaren Transformationen der Form

$$\dots SR \dots = \dots RS [S, R] \dots . \quad (8)$$

Um den Prozeß eindeutig zu machen, werde z. B. festgesetzt, daß von zwei gleichen Basiskommutatoren zuerst der am weitesten links an seine richtige Stelle in (1) gerückt wird.

Ist $P_{c,j}$ der r -te Basiskommutator in (1), so nennen wir den eben geschilderten Prozeß, der $P_{c,j}$ an die richtige Stelle bringt, den r -ten Schritt.

Es ist klar, daß in jedem Schritt die induzierten Kommutatoren in (8) Basiskommutatoren sein müssen. Da das Gewicht von $[S, R]$ größer ist als dasjenige des durchzuziehenden Elementes R , so gelangt man nach einer endlichen Anzahl von Schritten zur gesuchten Darstellung.

Jedem im Prozeß auftretenden Kommutator $[P_{c,j}, P_{b,i}]$ ordnen wir nun ein Label zu. Man erhält es, indem man mit den als schon gegeben gedachten Label $L(P_{b,i})$ und $L(P_{c,j})$ von $P_{b,i}$ resp. $P_{c,j}$ das Symbol $(L(P_{c,j}), L(P_{b,i}))$ bildet.

Dadurch wird jedem Kommutator in (8) ein Label zugeordnet. Da kein Kommutator mehr als einmal mit demselben Label auftreten kann, gibt der zu $[P_{c,j}, P_{b,i}]$ in (5) gehörige Exponent gerade die Anzahl der verschiedenen Label von $[P_{c,j}, P_{b,i}]$ an.

Daher bleibt also nur übrig, die Bedingungen dafür zu ermitteln, dank deren ein Kommutator mit vorgegebenem Label im Durchziehprozeß (8) wirklich auftritt.

Wie wir beweisen werden, sind diese Bedingungen derart, daß man daraus auf die im Satz 2 geschilderten Eigenschaften von (6) schließen kann.

Wie bei Hall heißen wir ein System von Bedingungen C , denen die Unbestimmten $\lambda_1, \lambda_2, \dots, \lambda_r$ zu genügen haben, ein System von Bedingungen Π , wenn Π erzeugt werden kann mittelst logischer Summen- und Produktbildung aus einem System von elementaren Bedingungen der Form $\lambda_i < \lambda_j$ oder $\lambda_i = \lambda_j$.

Es ist klar, daß die logischen Operationen der Summen- bzw. Produktbildung ein System von Π Bedingungen wieder in ein ebensolches überführen.

Ist P_i der i -te Kommutator in (1), so bezeichnen wir die Bedingungen dafür, daß ein P_i mit vorgegebenem Label in (8) auftreten kann mit E_i ; entsprechend sollen mit Q_i , diejenigen Bedingungen bezeichnet werden, die garantieren, daß der Basiskommutator P_i mit gegebenem $L(P_i)$ nach Ausführen gewisser Operationen (8) links vom Basiskommutator P_i mit vorgegebenem $L(P_i)$ auftritt.

Wie bei Hall zeigt man : (i) *Die im r -ten Schritt in (8) entstehenden Bedingungen E und Q werden gewonnen mittelst logischer Summen- und Produktbildung aus schon bestehenden E und Q .*

Im 0-ten Schritt haben wir die E und Q zu studieren der Form : $E_1, E_2, Q_{11}, Q_{12}, Q_{21}, Q_{22}$.

Zunächst sind E_1 und E_2 leer. Die Bedingungen Q_{11} und Q_{22} sind äquivalent mit $\varrho_i < \varrho_j$ oder $\varrho_i = \varrho_j$ und $\tau_i < \tau_j$.

Die Bedingungen Q_{12} und Q_{21} sind äquivalent mit $\varrho_i \leq \varrho_j$ bzw. $\varrho_i < \varrho_j$.

Im 0-ten Schritt sind also alle E und Q Π -Bedingungen, und zwar, was wesentlich ist, zwischen den ϱ allein und den τ allein. Aus (i) folgt daher : (ii) *Die E und Q des r -ten Schrittes sind Π -Bedingungen zwischen den ϱ allein und den τ allein.*

Genauer können wir noch sagen : Die E und Q des 0-ten Schrittes enthalten höchstens dann Π -Bedingungen für τ_i und τ_j , wenn erstens $\varrho_i = \varrho_j$ und wenn zweitens (ϱ_i, τ_i) und (ϱ_j, τ_j) Label desselben Kommutators vom Gewicht 1 sind, d. h. also Label von P_1 oder P_2 . Wegen (i) folgt daher : (iii) *Die E und Q des r -ten Schrittes enthalten höchstens dann Π -Bedingungen für τ_i und τ_j , wenn a) $\varrho_i = \varrho_j$ und b) (ϱ_i, τ_i) und (ϱ_j, τ_j) zwei Label von P_1 oder P_2 sind.*

Es sei $L_{\varrho, \tau} = ((\varrho_1, \tau_1), (\varrho_2, \tau_2), \dots, (\varrho_c, \tau_c))$ Label eines Kommutators vom Gewicht c . Dies bedeutet nach (ii), daß zwischen den ϱ allein und den τ allein gewisse Π -Bedingungen bestehen müssen. Setzt man $\varrho = (\varrho_1, \varrho_2, \dots, \varrho_c)$ und heißen ϱ und ϱ' äquivalent, wenn für $\varrho_i < \varrho_j$

oder $\varrho_i = \varrho_j$ in ϱ stets auch $\varrho'_i < \varrho'_j$ oder $\varrho'_i = \varrho'_j$ in ϱ' für alle Indexpaare i, j , so folgt aus der Definition der Π -Bedingungen, daß auch $L_{\varrho', \tau} = ((\varrho'_1, \tau_1), \dots, (\varrho'_c, \tau_c))$ wirklich Label desselben Kommutators ist.

Es möge ϱ genau k verschiedene ϱ_i enthalten und es sei

$$\varrho_{i_1} < \varrho_{i_2} < \dots < \varrho_{i_k} .$$

Heißt man jetzt zwei Label äquivalent, wenn $\varrho \sim \varrho'$, so erhält man eine Klasseneinteilung aller Label in fremde Klassen. In der Klasse N von $L_{\varrho, \tau}$ gibt es dann nach vorhin $\binom{n}{k}$ Systeme von Label, die sich voneinander nur durch die ϱ unterscheiden, d. h. in einem System ist ϱ konstant.

Zur Bestimmung der Anzahl aller Label unseres Kommutators in der Klasse N hat man also nur die Anzahl aller Label in N zu bestimmen mit festem ϱ .

Nun wirken nach (iii) die E und Q nicht auf alle τ , sondern nur auf gewisse Blöcke der τ etwa b_1, b_2, \dots, b_s . Zwei τ rechnen wir zum selben Block gehörig, wenn (iii) a und b erfüllt ist. Ist $b_i = (\tau_1^i, \dots, \tau_{c_i}^i)$, so schreiben wir $\tau = (b_1, b_2, \dots, b_s)$ und heißen τ und τ' äquivalent, wenn $b_i \sim b'_i$ ($i = 1, 2, \dots, s$). Wiederum ergibt sich wegen (ii), (iii) und aus der Definition der Π -Bedingungen, daß mit $L_{\varrho, \tau}$ auch $L_{\varrho, \tau'}$ Label unseres Kommutators ist.

Enthält b_i genau k_i verschiedene τ und ist also etwa

$$\tau_{j_1}^i < \tau_{j_2}^i < \dots < \tau_{j_{k_i}}^i ,$$

so gibt es in der Klasse von $L_{\varrho, \tau}$ mit festem ϱ gerade

$$\prod_{i=1}^r \binom{x_1}{k_i} \prod_{i=r+1}^s \binom{x_2}{k_i} .$$

Label mit äquivalenten τ . Dabei nehmen wir an, die Blöcke seien so numeriert, daß etwa alle τ in b_i ($i = 1, 2, \dots, r$) natürliche Zahlen $\leq x_1$ und in b_i ($i = r+1, \dots, s$) natürliche Zahlen $\leq x_2$ sind; denn die τ in einem Block gehören zu Label die alle entweder zu P_1 oder zu P_2 gehören.

Die Anzahl aller Label mit festem ϱ in N ist also eine endliche Summe von Aggregaten der angegebenen Form. Also ist die Anzahl aller Label in N gleich

$$\binom{n}{k} \sum \prod_{i=1}^r \binom{x_1}{k_i} \prod_{i=r+1}^s \binom{x_2}{k_i} .$$

Summiert man über alle Label-Klassen, deren ϱ genau k verschiedene ϱ_i aufweist, so erhält man das Glied $\binom{n}{k} a_{c,j}^{(k)}$ in (6). Der erste Teil von Satz 2 ist damit bewiesen.

Nun ist k_i stets kleiner oder höchstens gleich der maximalen Anzahl der übereinstimmenden ϱ_i . Diese ist $\leq c - k + 1$. Dies ist der zweite Teil von Satz 2.

§ 3. Ein Satz über nilpotente Gruppen der Klasse $c < p$.⁸⁾

Der Inhalt dieses Abschnittes ist der Beweis des folgenden Satzes :

3. Satz. $G = \{P_1, P_2, \dots, P_r\}$ sei eine nilpotente Gruppe der Klasse $c < p$ mit den folgenden Eigenschaften :

- (i) $G^{(i)} = \{P_i, P_{i+1}, \dots, P_r\}$ ist Normalteiler von G ($G^{(1)} = G$).
- (ii) $G^{(i)}/G^{(i+1)}$ ist zyklisch von unendlicher Ordnung.
- (iii) $G^{(i)}$ ($i = 1, 2, \dots, r$) ist eine Zentralkette von G .

Dann ist $G^p = \{P_1^{x_1} P_2^{x_2} \dots P_r^{x_r}\}$ mit $x_1, x_2, \dots, x_r \equiv 0 \pmod{p}$.

Beweis: Aus (i) und (ii) folgt $G^{(i)} = \{P_i^{x_i} P_{i+1}^{x_{i+1}} \dots P_r^{x_r}\}$ mit

$$(-\infty < x_i < \infty).$$

Der Satz ist richtig für die im Zentrum gelegene Gruppe $G^{(r)}$. Wir dürfen daher vollständige Induktion nach fallenden i vornehmen und also die Hypothese machen, es sei

$$(G^{(i+1)})^p = \{P_{i+1}^{x_{i+1}} \dots P_r^{x_r}\} \quad \text{mit} \quad x_{i+1}, \dots, x_r \equiv 0 \pmod{p}$$

und Normalteiler von G .

Wir berechnen die p -te Potenz $(x^{-1} P_i x)^p \pmod{(G^{(i+1)})^p}$. Es ist zunächst $x^{-1} P_i x = P_i [P_i, x]$ mit $[P_i, x] \subset G^{(i+1)}$ nach (iii).

Jetzt betrachten wir die Hallsche Identität, die zu dieser p -ten Potenz gehört. Wegen $c < p$ sind nach (6) alle Exponenten $f_{c,j}^{(p)} \equiv 0 \pmod{p}$. Das heißt es ist also

$$(x^{-1} P_i x)^p = P_i^p [P_i, x]^p \dots [\dots]^p \dots .$$

Wegen (iii) und nach Induktionsvoraussetzung folgt daher

$$x^{-1} P_i^p x \equiv P_i^p \pmod{(G^{(i+1)})^p},$$

⁸⁾ In dieser Form wurde der Satz von *P. Hall* erstmals ausgesprochen.

d. h. P_i^p liegt im Zentrum von $G/(G^{(i+1)})^p$. Somit ist die Gruppe

$$N = \{P_i^p, (G^{(i+1)})^p\}$$

Normalteiler von G und wegen (i) und (ii) von der Gestalt

$$N = \{P_i^{x_i} P_{i+1}^{x_{i+1}} \dots P_r^{x_r}\} \quad \text{mit } x_i, x_{i+1}, \dots, x_r \equiv 0 \pmod{p} .$$

Da $G^{(i)}$ von der Klasse $c < p$, hat jede p -te Potenz der Elemente in $G^{(i)}$ wegen der Existenz der Eindeutigkeitsbasis und nach der Induktionshypothese über $G^{(i+1)}$ die Form der Elemente in N . Es folgt also $N = (G^{(i)})^p$. (w. z. b. w.)

Setzt man wie in der Einleitung $F/F^p = B^p$, so folgt aus Satz 3, daß die Ordnung von B_w^p/B_{w+1}^p gleich p^{d_w} ist, vorausgesetzt, daß $w < p$. Für die $G^{(i)}$ in Satz 3 braucht man nur die Gruppen $\{P_i, P_{i+1}, \dots, P_r\}$ zu wählen, wobei P_1, P_2, \dots, P_r die Basiskommutatoren vom Gewicht $< p$ bedeuten.

Damit ist bewiesen

$$\delta_w^p = 0 \quad \text{für } w < p ,$$

also auch

$$\delta_{(w_2, w_1)}^p = 0 \quad \text{für } w_2 + w_1 < p . \quad (9)$$

Besonders nützlich für unsere Anwendungen ist noch der folgende

4. Hilfssatz. Ist $x \in H_\alpha$ und $y \in H_\beta$, so hat man die Kongruenzen

$$[x, y^p] \equiv 1 \pmod{H_{\alpha+p\beta} H_{\alpha+\beta}^p}$$

$$[x^p, y^p] \equiv 1 \pmod{H_{p(\alpha+\beta)} H_{\alpha+\beta}^p}$$

Beweis. Es ist zunächst $[x, y^p] = (y^{-1}[y^{-1}, x])^p y^p$. Nach dem Beweis von Satz 3 folgt aber

$$(y^{-1}[y^{-1}, x])^p \equiv y^{-p} \pmod{H_{\alpha+\beta+(p-1)\beta} H_{\alpha+\beta}^p} ,$$

denn die Klasse von $H_{\alpha+\beta}/H_{\alpha+p\beta}$ ist $< p$. Somit gilt

$$[x, y^p] \equiv 1 \pmod{H_{\alpha+p\beta} H_{\alpha+\beta}^p} .$$

Dies ist die erste Kongruenz in Hilfssatz 4.

Die zweite Kongruenz ergibt sich durch zweimalige Anwendung der ersten. (w. z. b. w.)

§ 4. Über die Struktur der Gruppe $H_{2p-1}F^p/H_{2p-1}$

Wir rechnen in diesem Abschnitt mod H_{2p-1} . In diesem Sinne dürfen wir H_p als Abelsche Gruppe behandeln und H_2 als nilpotente Gruppe der Klasse $c < p$.

Zum Studium der Gruppe $H_{2p-1}F^p/H_{2p-1}$ gehen wir aus von H_2 . H_2 genügt nämlich den Voraussetzungen des Satzes 3. Man hat als Gruppen $G^{(i)}$ nur die Gruppen zu bilden $\{P_i, P_{i+1}, \dots, P_r\}$ ($i \geq 3$), wobei P_3, P_4, \dots, P_r die aufsteigende Reihe der Basiskommutatoren bedeutet vom Gewicht $w = 2$ an bis zum Gewicht $w = 2p - 2$. Dann sind (i)–(iii) erfüllt nach Satz 1.

Setzt man $D = H_{2p-1}H_2^p$, so ist also nach Satz 3⁹⁾

$$D/H_{2p-1} = \{P_3^{x_3} P_4^{x_4} \dots P_r^{x_r}\} \quad \text{mit} \quad x_3, x_4, \dots, x_r \equiv 0 \pmod{p} \quad (10)$$

und es folgt, daß man zur Ermittlung von Dimensionsdefekten vom Gewicht w mit $p \leq w \leq 2p - 2$ stets mod D rechnen darf, was wir im folgenden fast immer tun werden.

In diesem Sinne hat jedes Element aus F die Gestalt

$$P_1^{x_1} P_2^{x_2} P_3^{x_3} \dots P_r^{x_r} \quad (-\infty < x_1, x_2 < \infty; 0 \leq x_3, x_4, \dots, x_r < p) .$$

Bildet man hiervon die p -te Potenz nach (5), so ergibt sich

$$P_1^{px_1} P_2^{px_2} \prod_i K_i^{a_i^{(p)}} = P_1^{px_1} P_2^{px_2} h(x_1, x_2, \dots, x_r) . \quad (11)$$

Hier sind die K_i Kommutatoren in den Erzeugenden P_i und vom Gewicht $\geq p$ in diesen Komponenten. Die K_i vom Gewicht $2 \leq w < p$ in den Komponenten P_i haben nach (6) Exponenten, die durch p teilbar sind, so daß man sie mod D weglassen kann.

Wir wollen nun über die Struktur der h -Bestandteile der p -ten Potenz (11) den folgenden Satz beweisen :

5. Hilfssatz. (i) *Es ist für $x_i \equiv r_i$ ($i = 1, 2$) mod p*

$$h(x_1, x_2, x_3, \dots, x_r) \equiv h(r_1, r_2, x_3, \dots, x_r) \pmod{D} .$$

(ii) *Bei gegebenen ganzen Zahlen $0 \leq x_1, x_2, \dots, x_r < p$ und $x_1 \neq 0$ gibt es eindeutig bestimmte ganze Zahlen $0 \leq y_2, y_3, \dots, y_r < p$, so daß*

$$h(x_1, x_2, x_3, \dots, x_r) \equiv (h(1, y_2, y_3, \dots, y_r))^{x_1} \pmod{D} .$$

⁹⁾ Die Idee dieser Konstruktion geht auf Hall zurück, der sie wohl erstmals zur Bestimmung von δ_p^p , δ_{p+1}^p und δ_{p+2}^p anwandte (Dezember 1949). Seine Methode versagte aber damals beim Versuch der Bestimmung von δ_{p+3}^p , was mir mit Hilfe von Satz 2, 5, 10 und 11 im Juni 1950 gelang (Brief an Prof. Speiser, 5. Juni 1950).

Beweis. (i) Ist eine Folge von Satz 2 und (10). In der Tat, da nämlich $h(x_1, x_2, \dots, x_r)$ nach Definition ein Produkt aus Basiskommatorn K_j darstellt in den Erzeugenden P_1, P_2, \dots, P_r und vom Gewicht $\geq p$ in diesen Erzeugenden, dürfen wir annehmen, K_j enthalte gerade die Komponenten $P_{m_1}, P_{m_2}, \dots, P_{m_l}$ und es sei K_j vom Gewicht c_{m_i} in P_{m_i} , so daß $\sum_{i=1}^l c_{m_i} = c \geq p$.

Wir betrachten nun den zu K_j gehörigen Hallschen Exponenten $a_j^{(p)}$ in (6). Er nimmt, wie man aus dem Beweis zu Satz 2 sofort abliest, die Gestalt an

$$a_j^{(p)} = \sum [x_{m_1}] [x_{m_2}] [x_{m_3}] \dots [x_{m_l}] ; [x_{m_i}] = \prod_{u_{m_i}} \binom{x_{m_i}}{u_{m_i}} ; 1 \leq \sum u_{m_i} \leq c_{m_i} \quad (12)$$

und da wegen $c \leq 2p - 2$ und $k = p$ folgt, daß $c - k + 1 < p$, ergibt sich auch $1 \leq u_{m_i} < p$. Hieraus ergibt sich unmittelbar (i).

(ii) Zum Beweis von (ii) verfahren wir so. Es ist mod H_{2p-1}

$$(P_1 P_2^{y_2} P_3^{y_3} \dots P_r^{y_r})^{x_1} \equiv P_1^{x_1} P_2^{y_2 x_1} \dots P_i^{y_i x_1 + C_{(x_1; y_2, \dots, y_{i-1})}},$$

wo $C_{(x_1; y_2, \dots, y_{i-1})}$ ein Polynom in den Unbestimmten x_1, y_2, \dots, y_{i-1} bedeutet. Wählt man bei gegebenen x_i ($i = 1, 2, \dots, r$) in (ii) die y_i ($i = 2, 3, \dots, r$) gemäß der Kongruenz

$$y_2 x_1 \equiv x_2 \pmod{p}$$

$$y_i x_1 + C_{(x_1; y_2, \dots, y_{i-1})} \equiv x_i \pmod{p} \quad (i = 3, 4, \dots, r),$$

so ist y_i im angegebenen Bereich eindeutig bestimmt.

Bildet man die p -te Potenz der obigen Kongruenz, so folgt nach (i)

$$(P_1^p P_2^{y_2 p} h_{(1, y_2, \dots, y_r)})^{x_1} \equiv P_1^{px_1} P_2^{py_2 x_1} h_{(x_1, x_2, \dots, x_r)} \pmod{D}.$$

Die linke Seite ist aber gleich

$$P_1^{px_1} P_2^{py_2 x_1} (h_{(1, y_2, \dots, y_r)})^{x_1} \cdot \Pi \pmod{D}$$

und Π ist ein Produkt aus Basiskommatorn der Form $[[x^p, y^p], \dots]$ und $[[h, x^p], \dots]$. Nach Hilfssatz 4 sind diese Kommatorn in $H_{2p} H_2^p$ enthalten. Somit folgt

$$(h_{(1, y_2, \dots, y_r)})^{x_1} \equiv h(x_1, x_2, \dots, x_r) \pmod{D}.$$

Damit ist Satz 5 vollständig bewiesen.

Es ist hier noch eine Bemerkung am Platze. Da nämlich wegen (6) der Exponent von K_i in (11) durch p teilbar wird, wenn K_i in den P_i das Gewicht $< p$ hat, so braucht man mit P_i nur bis zu den Basis-Kommutatoren vom Gewicht $< p$ zu gehen. Enthält nämlich K_i ein P_i vom Gewicht $\geq p$, so kann es in den P_i mod H_{2p-1} höchstens das Gewicht $p - 1$ haben. Ein solches P_i liefert somit nur Beiträge in D .

Die h -Bestandteile der Potenzen (11) liegen alle in $H_p D / D$. Dies ist eine elementare Abelsche Gruppe vom Exponenten p .

Mit D' bezeichnen wir die Gruppe $\{h_{(x_1, \dots, x_r)}, D\}$, die von allen h und von D erzeugt wird. Es gilt der

6. Hilfssatz. D' ist Normalteiler von F und D'/D ist eine Abelsche Gruppe vom Exponenten p .

Beweis. Wir haben nur noch zu zeigen, daß D' Normalteiler von F . Wir zeigen, daß D' Normalteiler von F mod D .

Es sei h ein h -Bestandteil und es gelte

$$(P_1^{x_1} P_2^{x_2} \dots P_r^{x_r})^p \equiv P_1^{px_1} P_2^{px_2} h_{(x_1, x_2, \dots, x_r)} \pmod{D}.$$

Dann folgt durch Transformation mit $x \in F$:

$$(P_1^{x_1} [P_1^{x_1}, x] P_2^{x_2} [P_2^{x_2}, x] \dots)^p \equiv (P_1^{x_1} [P_1^{x_1}, x])^p (P_2^{x_2} [P_2^{x_2}, x])^p \cdot x^{-1} h x,$$

d. h. es ist

$$P_1^{px_1} P_2^{px_2} h^* \equiv P_1^{px_1} h^{**} P_2^{px_2} h^{***} \cdot x^{-1} h x,$$

wenn h^* , h^{**} und h^{***} h -Bestandteile bedeuten. Da das Gewicht dieser $h^{**}, h^{***} > p$, folgt nach Hilfssatz 4 $[h^{**}, P_2^{px_2}] \equiv 1 \pmod{H_{2p} H_2^p}$.

Somit folgt $h^* \equiv h^{**} h^{***} \cdot x^{-1} h x \pmod{D}$, d. h. $x^{-1} h x$ gehört zu D' mod D . Also ist D' Normalteiler von F .

Mit D'' bezeichnen wir die Gruppe $\{P_1^p, P_2^p, D'\}$. Dann gilt der

7. Hilfssatz. D'' ist Normalteiler von F und D''/D' ist eine freie Abelsche Gruppe.

Beweis. Wir berechnen die p -te Potenz $(x^{-1} P_1 x)^p \pmod{D'}$. Wegen $x^{-1} P_1 x = P_1 [P_1, x]$ folgt $x^{-1} P_1^p x \equiv P_1^p \pmod{D'}$. Das heißt P_1^p und P_2^p liegen beide im Zentrum von F/D' . Also ist D'' Normalteiler von F und D''/D' ist Abelsch. Da $D' \subset H_2$ ist D''/D' frei Abelsch.

Damit ist der Satz bewiesen.

8. Satz. *Es ist*

$$F^p H_{2p-1}/H_{2p-1} = \{P_1^{x_1} P_2^{x_2} h_1^{\lambda_1} h_2^{\lambda_2} \dots h_g^{\lambda_g} P_3^{x_3} P_4^{x_4} \dots P_r^{x_r}\}$$

$$(x_1, x_2, \dots, x_r \equiv 0 \pmod{p}; \quad 0 \leq \lambda_1, \lambda_2, \dots, \lambda_g < p)$$

Beweis. D''/H_{2p-1} enthält nach Konstruktion alle p -ten Potenzen der Elemente aus F/H_{2p-1} . Wie man aus der ermittelten Normalform der Elemente in D''/H_{2p-1} abliest, ist diese Gruppe in $H_{2p-1}F^p/H_{2p-1}$ enthalten. Somit folgt $D'' = H_{2p-1}F^p$. (w. z. b. w.)

Aus den Sätzen 5 bis 8 ergibt sich der wichtige

9. Satz. *Zur Bestimmung von Dimensionsdefekten im Bereich $0 \leq w \leq 2p - 2$ hat man nur die Gruppe D'/D zu betrachten. δ_w^p ist gleich der Anzahl aller $h(1, x_2, x_3, \dots, x_r)$ und $h(0, 1, x_3, \dots, x_r)$ mit $0 \leq x_2, \dots, x_r < p$ in $H_w D/D$, die mod $H_{w+1}D$ voneinander unabhängig sind.*

Wir wenden uns nun ganz dem Studium der Defektgruppe D'/D zu. Wir haben zu diesem Zweck die Hallsche Identität der p -ten Potenzen der Gestalt

$$\begin{aligned} & (P_1 P_2^{x_2} P_3^{x_3} \dots P_r^{x_r})^p \\ & (P_2 P_3^{x_3} P_4^{x_4} \dots P_r^{x_r})^p \end{aligned} \quad (0 \leq x_2, x_3, \dots, x_r < p; w(P_r) \leq p-1) \quad (13)$$

zu bilden. Dies denken wir uns *formal* in den Unbestimmten x_2, x_3, \dots, x_r durchgeführt, d. h. wir denken uns zu jedem auftretenden Kommutator von Gewicht $w \geq p$ in den P_i das $a_{c,j}^{(p)}$ in (6) in Unbestimmten

$$x_2, x_3, \dots, x_r$$

nach Paragraph 2 bestimmt. Dann gewinnt man das generelle

$$h(1, x_2, \dots, x_r)$$

und das generelle $h(0, 1, x_3, \dots, x_r)$.

Da D'/D nach Satz 6 eine Abelsche Gruppe vom Exponenten p ist, dürfen wir wegen Satz 2 das generelle h mod D folgendermaßen behandeln ($c - k + 1 < p$):

(i) *Man schreibe jedes $a_{c,j}^{(p)}$ als ganzzahliges, mod p reduziertes Polynom.* Jede Potenz x^n mit $n \geq p$ wird also reduziert nach der immer gültigen Kongruenz $x^p \equiv x \pmod{p}$.

(ii) *Jetzt ordne man nach den verschiedenen Monomen m_i in den x_i , die bei der Reduktion (i) in den Exponenten entstanden sind, d. h. man*

schreibe h als ein Produkt von Potenzen, deren Exponenten die voneinander verschiedenen Monome m_i sind.

Das generelle $h(1, x_2, \dots, x_r)$ nimmt dann mod D die Gestalt an

$$h(1, x_2, \dots, x_r) \equiv e_1^{m_1} e_2^{m_2} \dots e_s^{m_s} \text{ mod } D, \quad (14)$$

wobei m_1, m_2, \dots, m_s die im Prozeß (i) und (ii) entstandenen verschiedenen Monome bedeuten.

Analog schreibt sich das generelle $h(0, 1, x_3, \dots, x_r)$ in der Form

$$h(0, 1, x_3, \dots, x_r) \equiv e_{s+1}^{m_1} e_{s+2}^{m_2} \dots e_{s+t}^{m_t} \text{ mod } D, \quad (15)$$

wobei m_1, m_2, \dots, m_t Monome in x_3, x_4, \dots, x_r sind.

Es gilt jetzt der grundlegende

10. Satz. Die Defektgruppe D'/D wird von den Elementen e_i ($i = 1, 2, \dots, s+t$) erzeugt.

Beweis. Da $h_i \in \{e_1, e_2, \dots, e_{s+t}\}$ haben wir nur zu zeigen, daß auch $e_i \in \{h_1, h_2, \dots, h_g\}$. Dies ergibt sich sofort aus dem folgenden

11. Hilfssatz. Wenn in einer Abelschen Gruppe vom Exponenten p Elemente der Form $h(x_1, x_2, \dots, x_r) = e_1^{m_1} e_2^{m_2} \dots e_q^{m_q}$ gegeben sind, wobei m_1, m_2, \dots, m_q sämtliche Monome in x_1, x_2, \dots, x_r und x_1, x_2, \dots, x_r unabhängig voneinander die Zahlen von 0 bis $p-1$ durchlaufen, so sind e_1, e_2, \dots, e_q in der von den $h(x)$ erzeugten Gruppe enthalten.

Beweis. Schreibt man h in der Form

$$h(x_1, x_2, \dots, x_r) = f_1^{x_1} f_2^{x_2} \dots f_{p-1}^{x_{p-1}} f_p$$

und gibt man x_1 die Werte $0, 1, \dots, p-1$, so kann man, weil die Determinante der Exponenten von Null verschieden ist, die

$$f_i \quad (i = 1, 2, \dots, p)$$

auflösen und durch die $h(x)$ ausdrücken. Die f_i haben dieselbe Gestalt wie die $h(x)$, aber die Exponenten sind nur Monome in x_2, x_3, \dots, x_r . Wiederholt man das Verfahren mit x_2 , usw., so erhält man schließlich e_1, e_2, \dots, e_q durch die $h(x)$ ausgedrückt.

§ 5. Über die Struktur der freien nilpotenten Gruppen der Klasse c.

Satz 1 ist die wichtigste Aussage über die Struktur der freien nilpotenten Gruppen. Achtet man bei einem vorgelegten Kommutator nicht nur auf sein Gewicht, sondern auch auf seinen Typus, so kommt man zu

Aussagen, die besonders im Hinblick auf das Problem von Burnside nützlich sein können.

F sei wie immer die freie Gruppe mit P_1 und P_2 als freien Erzeugenden. Ein Kommutator K heißt vom Typus (w_2, w_1) , wenn er in der Komponente P_2 das Gewicht w_2 , in der Komponenten P_1 das Gewicht w_1 besitzt.

Sind K und L Kommutatoren aus F mit den Typen (w_2, w_1) resp. (v_2, v_1) , so sagen wir, K und L seien vom gleichen Typus, wenn $w_i = v_i$ ($i = 1, 2$). Der Typus (v_2, v_1) von L heißt größer als der Typus (w_2, w_1) von K , wenn $(v_2, v_1) \neq (w_2, w_1)$ und $v_i \geq w_i$ ($i = 1, 2$).

Wir können jetzt den Satz behaupten

12. Hilfssatz. *Die Normalform (1) eines Kommutators K vom Typus (w_2, w_1) ist ein Produkt aus Basiskommutatoren, deren Typen $\geq (w_2, w_1)$ sind.*

Beweis. Da der Satz für die Kommutatoren vom Typus (w_2, w_1) mit $w_2 + w_1 = 2$ richtig ist, dürfen wir vollständige Induktion nach $w_2 + w_1 = w > 2$ machen und also annehmen, ein Kommutator K vom Typus (w_2, w_1) mit $w_2 + w_1 < w$ sei darstellbar in der Form $K = K^* K^{**}$, wobei K^* ein Produkt aus Basiskommutatoren vom Typus (w_2, w_1) darstellt, während K^{**} ein Produkt aus endlich vielen Kommutatoren vom Typus $> (w_2, w_1)$ bedeuten soll.

Wir haben zu beweisen, daß die Induktion unter diesen Voraussetzungen funktioniert. Es sei K ein Kommutator vom Typus (w_2, w_1) und $w_2 + w_1 = w$. Ist $K = [L, M]$, so ist für L und M die Induktionsvoraussetzung erfüllt. Das heißt es ist $K = [L^* L^{**}, M^* M^{**}]$. Nun verwenden wir die bekannten Identitäten

- (a) $(x, yz) = (x, z)(x, y)^z ,$
- (b) $(xy, z) = (x, z)^y (y, z) ,$
- (c) $(x, y^{-1}, z)^y (y, z^{-1}, x)^z (z, x^{-1}, y)^x = 1 .$

Aus (a) und (b) folgt sofort $K = [L^*, M^*] \dots$ Punkte bedeuten im folgenden immer ein Produkt aus endlich vielen Kommutatoren, deren Typen größer sind als die Typen der angeschriebenen Kommutatoren. Wendet man (a) und (b) auf $[L^*, M^*]$ an, so folgt, daß wir uns auf die Betrachtung des Falles beschränken dürfen, wo $K = [P_j, P_i]$, mit P_j und P_i als Basiskommutatoren. Da $w > 2$ sei etwa $P_j = [P_l, P_k]$ und $P_l > P_k > P_i$. Dann folgt aus (c) $K = [P_k, P_i, P_l]^{-1} [P_l, P_i, P_k] \dots$

Für $[P_k, P_i]$ und $[P_l, P_i]$ gilt wieder die Induktionsvoraussetzung, das heißt

$$[P_k, P_i] = \underbrace{\prod_m}_{m} P_m \dots \quad \text{und} \quad [P_l, P_i] = \underbrace{\prod_n}_{n} P_n \dots .$$

Aus (a) und (b) folgt daher $K = \underbrace{\prod_m}_{m} [P_m, P_l]^{-1} \underbrace{\prod_n}_{n} [P_n, P_k] \dots$. Beachtet man jetzt, daß die Basiskommutatoren P_m, P_n, P_l, P_k alle nach P_i kommen im Sinne der Anordnung der Basis-Kommutatoren, so führt eine Fortsetzung des Verfahrens nach endlich vielen Schritten zur gesuchten Darstellung von K . Denn es gibt ja nur endlichviele Kommutatoren der Gestalt $[P_m, P_l]$ und $[P_n, P_k]$, wenn die Indizes der Basiskommutatoren in jedem Schritt erhöht werden. (w. z. b. w.)

Mit $H_{(w_2, w_1)}$ bezeichnen wir die Gruppe, die aus allen Kommutatoren vom Typus $\geq (w_2, w_1)$ erzeugt wird. Diese Gruppe ist offensichtlich Normalteiler von F und wir wollen die Struktur dieses Normalteilers näher beschreiben.

Aus Satz 1 und Hilfssatz 12 ergibt sich der

13. Satz. Sei N die freie nilpotente Gruppe der Klasse c mit zwei Erzeugenden und $P_{m_1}, P_{m_2}, \dots, P_{m_l}$ die aufsteigend geordnete Reihe der Basiskommutatoren von N vom Typus $\geq (w_2, w_1)$. Dann ist die Gruppe $N_{(w_2, w_1)}$, die von allen Kommutatoren vom Typus $\geq (w_2, w_1)$ in N erzeugt wird, Normalteiler von N und von der Gestalt

$$N_{(w_2, w_1)} \equiv \{P_{m_1}^{x_1} P_{m_2}^{x_2} \dots P_{m_l}^{x_l}\}$$

mit $-\infty < x_i < \infty$ ($i = 1, 2, \dots, l$).

Im Gegensatz zu den Faktorgruppen F/H_{c+1} ist die Faktorgruppe $F/H_{(w_2, w_1)}$ für $w_2 + w_1 > 2$ nicht nilpotent; hingegen ist die Kommutatorgruppe von $F/H_{(w_2, w_1)}$ nilpotent von der Klasse $c = \max\{w_2, w_1\} - 1$.

§ 6. Über die Struktur der e .

Wir wollen die Struktur der e -Elemente in Satz 10 genau bestimmen. Wir gehen aus von $h(1, x_2, x_3, \dots, x_r)$ in (14). h ist Endresultat eines Durchziehprozesses, der die p -te Potenz

$$\underbrace{P_1 P_2^{x_2} \dots P_r^{x_r}}_1 \dots \underbrace{P_1 P_2^{x_2} \dots P_r^{x_r}}_p$$

in die Form (1) überführt. Er ist genau so zu erklären wie in Paragraph 2, nur haben wir hier $r \geq 2$ Erzeugende P_1, P_2, \dots, P_r . Das heißt man

hat nacheinander die Basiskommutatoren in den Erzeugenden

$$P_1, P_2, \dots, P_r$$

ihrer Anordnung gemäß Paragraph 1 an die richtige Stelle in (1) zu überführen.

(a) Die e sind also zunächst Produkte aus Basiskommutatoren $Q_{c,j}$, vom Gewicht $c \geq p$ in den Erzeugenden P_1, P_2, \dots, P_r . Das heißt sie haben die Gestalt

$$e = \prod_{j; c \geq p} Q_{c,j}^{a_{c,j}} .$$

Ist etwa $m = x_{i_1}^{a_1} \dots x_{i_l}^{a_l}$ das Monom, das zu e gehört in (14) mit $2 \leq i_1 < i_2 < \dots < i_l \leq r$, so folgt aus dem Beweis von Satz 2 (vgl. etwa (12)), daß alle $Q_{c,j}$ Basiskommutatoren in den Komponenten $P_{i_1}, P_{i_2}, \dots, P_{i_l}$ (und eventuell P_1) sein müssen (und nur in diesen), wobei noch das Gewicht w_{i_k} von P_{i_k} in $Q_{c,j}$ ($k = 1, 2, \dots, l$) der Bedingung $w_{i_k} \geq a_{i_k}$ ($k = 1, 2, \dots, l$) genügen muß.

(b) Mit e^* bezeichnen wir diejenigen e in Satz 10, die wenigstens einen Kommutator $Q_{c,j}$ vom Typus (w_2, w_1) mit $1 \leq w_2 < p$ enthalten.

Jedenfalls gehören die e in (15) nicht zu den e^* . Denn aus (a) folgt, daß alle e in (15) Produkte aus Basiskommutatoren in den Erzeugenden P_2, P_3, \dots, P_r darstellen. Da P_2 Komponente von jedem P_2, P_3, \dots, P_r ist und $c \geq p$ sein muß, folgt $w_2(Q_{c,j}) \geq p$, wenn wir mit $w_2(Q)$ das Gewicht von Q in P_2 bezeichnen.

Ein e^* aus (14) enthält ein $Q_{c,j}$, dessen Typus (v_2, v_1) der Bedingung $1 \leq v_2 < p$ genügt, d. h. es ist für dieses $Q_{c,j}$

$$1 \leq \sum_{k=1}^l w_2(P_{i_k}) \cdot w_{i_k} = v_2 < p . \quad (16)$$

(c) Da also das in (b) betrachtete $Q_{c,j}$ höchstens v_2 Komponenten aus der Reihe P_2, P_3, \dots, P_r enthalten kann, ergibt sich für e^* die Gestalt $e^* = \prod_j Q_{p,j} \dots$, wobei alle $Q_{p,j}$ die Komponente P_1 mindestens $(p - v_2)$ -fach enthalten. Zum Beispiel tritt ein $Q_{p,j}$ auf der Gestalt

$$Q_{p,j} = [P_{i_l}, w_{i_0} \cdot P_1, w_{i_1} P_{i_1}, \dots, w_{i_{l-1}} P_{i_{l-1}}, (w_{i_l} - 1) P_{i_l}]$$

und wir wollen zeigen, daß das zugehörige $a_{p,j} \not\equiv 0 \pmod{p}$. Zu diesem Zweck haben wir den zu $Q_{p,j}$ gehörigen Hallschen Exponenten zu bestimmen. Nach der Methode in Paragraph 2 bilden wir das generelle Label $L_{\varrho, \tau}$.

Es hat die Gestalt

$$((\varrho_1, \tau_1), (\varrho_2, \tau_2), \dots, (\varrho_p, \tau_p))$$

und wir haben nun die E -Bedingungen zu formulieren. Sie lauten, wie man sich sofort überlegt, wenn noch $\sum_{k=0}^m w_{ik} = w_m$ gesetzt wird,

$$\varrho_1 < \varrho_2 < \varrho_3 < \cdots < \varrho_{w_{i_0}+1}$$

$$\varrho_1 < \varrho_{w_m+2} < \varrho_{w_m+3} < \cdots < \varrho_{w_{m+1}+1} \quad (m = 0, 1, \dots, l-2)$$

$$\varrho_1 < \varrho_{w_{l-1}+2} < \cdots < \varrho_p .$$

Da die ϱ alle verschiedenen Zahlen von 1 bis p sein müssen, folgt $\varrho_1 = 1$. Da außerdem zwischen den τ keine Bindungen bestehen, ist die Anzahl aller Label, die den obigen Bedingungen genügen, gegeben durch

$$\binom{p-1}{w_{i_0}} \prod_{m=1}^{l-1} \binom{p-1-w_{m-1}}{w_{i_m}} x_{i_1}^{w_{i_1}} x_{i_2}^{w_{i_2}} \dots x_{i_l}^{w_{i_l}} .$$

Wegen $1 \leq w_{i_m} < p - 1 - w_{m-1}$ ist $a_{p,j} \not\equiv 0 \pmod{p}$.

Aus dem Beweis zu Satz 2 folgt weiter, daß die $Q_{p,j}$ abgesehen von der Anordnung genau dieselben Komponenten $P_1, P_{i_1}, P_{i_2}, \dots, P_{i_l}$ gleich oft enthalten müssen. Die $Q_{p,j}$ haben daher alle denselben Typus. Überhaupt folgt allgemein aus (a), daß e^* ein Produkt ist aus Kommutatoren, deren Typen $\geq (v_2, v_1)$, wenn $Q_{p,j}$ den Typus (v_2, v_1) besitzt.

Die e^* sind also neben der Bedingung (16) noch dadurch charakterisiert, daß

$$p - \sum_{k=1}^l w_{ik} + \sum_{k=1}^l w(P_{ik}) w_{ik} = v_2 + v_1 \quad (p \leq v_2 + v_1 \leq 2p - 2) , \quad (17)$$

worin $w(P_{ik})$ das Gewicht von P_{ik} bedeutet.

Die Bedingungen (16) und (17) können als die Existenzbedingungen der e^* angesprochen werden. Denn zu gegebenem Typus (v_2, v_1) mit $1 \leq v_2 < p$ und $p \leq v_2 + v_1 \leq 2p - 2$ gibt es, wie aus unsrern Überlegungen hervorgeht, genau soviele e^* als es verschiedene Lösungen gibt von (16) und (17).

- (d) Man betrachte nun Elemente t mit den folgenden Eigenschaften :
 - (i) t liegt in der Defektgruppe D'/D .
 - (ii) $t \equiv T \not\equiv 1 \pmod{H_{v_2+v_1+1}D}$, wobei T ein Produkt aus Basiskommutatoren bezeichnet, die alle denselben Typus (v_2, v_1) haben.

Wir bezeichnen die verschiedenen Lösungen von (16) und (17) bei gegebenem Typus (v_2, v_1) im Bereich

$$(p \leq v_2 + v_1 \leq 2p - 2 ; 1 \leq v_2 < p)$$

mit $\Pi_{(v_2, v_1)}^p$.

Wir wollen jetzt eine Methode angeben, mit deren Hilfe man unter gewissen Voraussetzungen die Unabhängigkeit der e^* -Elemente beweisen kann. Es gilt nämlich das folgende Kriterium: Um zu beweisen, daß bei gegebenem Typus (v_2, v_1) mit $1 \leq v_2 \leq k$ die $\Pi_{(v_2, v_1)}^p$ Elemente e^* voneinander unabhängig sind, genügt es zu zeigen, daß es zu jedem festen Typus im Bereich $(1 \leq v_2 \leq k < p; p \leq v_2 + v_1 \leq 2p - 2)$ sicher $\Pi_{(v_2, v_1)}^p$ Elemente T vom Typus (v_2, v_1) gibt, die mod $H_{v_2+v_1+1}D$ voneinander unabhängig sind.

Beweis. Da nach (a) und (c) die e^* mit $v_2 > k$ und alle nicht $-e^*$ die Basiskommutatoren vom Typus (v_2, v_1) mit $1 \leq v_2 \leq k$ gar nicht als Faktoren enthalten können, folgt aus dem Erfülltsein des Kriteriums und der Bedeutung der e in Satz 10 die Unabhängigkeit aller e^* vom Typus (v_2, v_1) mod $H_{v_2+v_1+1}D$. (w. z. b. w.)

Ist das Kriterium erfüllt, so folgt aus Satz 1 die Unabhängigkeit aller e^* mit $(1 \leq v_2 \leq k < p; p \leq v_2 + v_1 \leq 2p - 2)$. Das heißt es ist dann

$$\delta_{(v_2, v_1)}^p = \Pi_{(v_2, v_1)}^p . \quad (18)$$

Wir werden im nachfolgenden Paragraphen die Anzahl $\Pi_{(v_2, v_1)}^p$ für $1 \leq v_2 \leq 3$ berechnen und das Kriterium in diesem Bereich in den Paragraphen 8 bis 12 als erfüllt nachweisen, so daß wir nach den vorigen Bemerkungen zu einer Bestimmung der Dimensionsdefekte (18) für $v_2 = 1, 2, 3$ gelangen werden.

§ 7. Berechnung der Zahl $\Pi_{(v, p+\tau-v)}^p$ ($v = 1, 2, 3; 0 \leq \tau \leq p-2$) .

Die Zahl $\Pi_{(v, p+\tau-v)}^p$ ist nach Paragraph 6 gleich der Anzahl der verschiedenen Lösungen der Gleichungen (16) und (17), denen wir die Form geben

$$(i) \quad \sum_{k=1}^q w_2(P_{i_k}) = v < p \quad (2 \leq i_1 \leq i_2 \leq \dots \leq i_q \leq r) \quad (19)$$

$$(ii) \quad p - q + \sum_{k=1}^q w(P_{i_k}) = p + \tau$$

1. Fall. $v = 1$. Dann folgt aus (19) $q = 1$, also $w_2(P_{i_1}) = 1$ und $w(P_{i_1}) = \tau + 1$. Dadurch ist P_{i_1} eindeutig bestimmt und es folgt

$$\Pi_{(1, p+\tau-1)}^p = 1 . \quad (20)$$

2. Fall. $v = 2$. Wir unterscheiden zwei Fälle (a) und (b).

(a) Hier sei $q = 1$. Dann folgt aus (19)

$$w_2(P_{i_1}) = 2 \quad \text{und} \quad w(P_{i_1}) = \tau + 1 .$$

Das heißt P_{i_1} ist ein beliebiger Basiskommutator vom Typus $(2, \tau - 1)$. Solcher gibt es nach Witt für $\tau \geq 2$ gerade $d_{(2, \tau-1)}$.

(b) Hier sei $q = 2$. Dann folgt

$$w_2(P_{i_1}) = w_2(P_{i_2}) = 1 \quad \text{und} \quad w(P_{i_1}) + w(P_{i_2}) = \tau + 2 .$$

Die letztere Gleichung besitzt wegen $i_1 \leq i_2$ und also $w(P_{i_1}) \leq w(P_{i_2})$ gerade $\left[\frac{\tau+2}{2} \right]$ Lösungen. Für jede Wahl von $w(P_{i_1})$ ist dann P_{i_1} und P_{i_2} eindeutig bestimmt. Also gibt es in diesem Sonderfall genau $\left[\frac{\tau+2}{2} \right]$ Lösungen für $\tau \geq 0$.

Aus (a) und (b) folgt wegen $d_{(2, \tau-1)} = \left[\frac{\tau}{2} \right]$,

$$\Pi_{(2, p+\tau-2)}^p = \left[\frac{a+2\tau}{2} \right] (\tau \equiv a \pmod{2}; a = 1, 2) \quad (21)$$

3. Fall. $v = 3$. Es sei $\tau \equiv a \pmod{6}$ mit $a = 1, 2, 3, 4, -1, 6$.

(a) $q = 1$. Dann ist $w_2(P_{i_1}) = 3$ und $w(P_{i_1}) = \tau + 1$. Das heißt P_{i_1} ist ein beliebiger Basiskommutator vom Typus $(3, \tau - 2)$. Nach Witt gibt es daher $d_{(3, \tau-2)}$ Lösungen, falls $\tau \geq 3$

$$d_{(3, \tau-2)} = \left[\frac{\tau^2 - \tau}{6} \right]. \quad (22)$$

(b) $q = 2$. Dann folgt

$$w_2(P_{i_1}) + w_2(P_{i_2}) = 3 \quad \text{und} \quad w(P_{i_1}) + w(P_{i_2}) = \tau + 2 .$$

Wegen $i_1 \leq i_2$ ist $w(P_{i_1}) \leq w(P_{i_2})$. Sei

$$w(P_{i_1}) = k \left(k = 1, 2, \dots, \left[\frac{\tau+2}{2} \right] \right)$$

und $w_2(P_{i_1}) = 1$. Dann ist P_{i_1} eindeutig bestimmt, während P_{i_2} nur dem Typus nach bestimmt ist. Also gibt es in diesem Fall

$$\sum_{k=1}^{\left[\frac{\tau+2}{2} \right]} d_{(2, \tau-k)}$$

verschiedene Lösungen.

Ist $w_2(P_{i_1}) = 2$, so sei

$$w(P_{i_1}) = \tau + 2 - k \left(k = \left[\frac{\tau+2}{2} \right] + 1, \dots, \tau - 1 \right) .$$

Dann ist P_{i_2} bestimmt aber P_{i_1} nur bis auf den Typus $(2, \tau - k)$. Also

gibt es in diesem Fall

$$\sum_{k=\left[\frac{\tau+2}{2}\right]+1}^{\tau-1} d_{(2,\tau-k)}$$

Lösungen.

Im ganzen haben wir also $\sum_{k=1}^{\tau-1} d_{(2,\tau-k)}$ Lösungen für $\tau \geq 2$. Nun ist nach Witt

$$d_{(2,\tau-k)} = \left[\frac{\tau - k + 1}{2} \right].$$

Somit folgt

$$\sum_{k=1}^{\tau-1} d_{(2,\tau-k)} = \left[\frac{\tau^2}{4} \right]. \quad (23)$$

(c) $q = 3$. Dann ist $w_2(P_{i_1}) + w_2(P_{i_2}) + w_2(P_{i_3}) = 3$ und also $w(P_{i_k}) = 1$ ($k = 1, 2, 3$). Weiter ist $w(P_{i_1}) + w(P_{i_2}) + w(P_{i_3}) = \tau + 3$. Aus $i_1 \leq i_2 \leq i_3$ folgt $w(P_{i_1}) \leq w(P_{i_2}) \leq w(P_{i_3})$, das heißt wir haben die ganzzahligen Lösungen der Ungleichungen

$$1 \leq w(P_{i_1}) \leq w(P_{i_2}) \leq \tau + 3 - w(P_{i_1}) - w(P_{i_2})$$

zu bestimmen. Da jede Lösung die P_{i_k} ($k = 1, 2, 3$) eindeutig festlegt, ist die Anzahl der Lösungen dieser Ungleichung gleich der Anzahl der verschiedenen Lösungen in Kommutatoren $P_{i_1}, P_{i_2}, P_{i_3}$.

Eine leichte Rechnung liefert für diese Anzahl die Werte

$$\begin{aligned} & \frac{(\tau+a)(\tau+6-a)}{12} \quad (a = 1, 2, 3, 4), \\ & \frac{(\tau+a)(\tau+6-a)}{12} + 1 \quad (a = -1, 6) \end{aligned} \quad (24)$$

Summiert man für festes a die Formeln in (22) bis (24), so erhält man die gesuchte Anzahl $\Pi_{(3,p+\tau-3)}^p$. Es resultiert die merkwürdige Formel

$$\begin{aligned} \Pi_{(3,p+\tau-3)}^p &= \frac{1}{3!} (a + 2\tau + 3\tau^2) \\ (\tau \equiv a \pmod{6}; a &= 1, 2, 3, 4, -1, 6) \end{aligned} \quad (25)$$

§ 8. $\delta_{(1,p+\tau-1)}^p$ für $\tau = 0, 1, 2, \dots, p-2$.

Wir berechnen das Element e^* , das zum Monom x_2 gehört $\pmod{H_{p+1}D}$. Es hat offenbar die Gestalt

$$e^* \equiv [P_2, (p-1) P_1] \pmod{H_{p+1}D}. \quad (26)$$

Da D' Normalteiler von F nach Satz 6 gehört mit e^* auch der Kommutator $[e^*, x]$ zu D' . Aus (26) ergeben sich daher sofort die weiteren Elemente in $D'|D$:

$$[e^*, \tau P_1] \equiv [P_2, (p + \tau - 1) P_1] \bmod H_{p+\tau+1} D . \quad (27)$$

Setzt man $T(\tau) = [P_2, (p + \tau - 1) P_1]$, so erkennt man, daß die $T_{(\tau)}$ für $\tau = 0, 1, \dots, p - 2$ alle voneinander unabhängig sind $\bmod D$. Wir haben also das Kriterium in Paragraph 6 als erfüllt nachgewiesen und es folgt nach Paragraph 6:

$$\delta_{(1,p+\tau-1)}^p = \Pi_{(1,p+\tau-1)}^p (\tau = 0, 1, \dots, p - 2) . \quad (28)$$

§ 9. $\delta_{(2,p+\tau-2)}^p (\tau = 0, 1, 2, \dots, p - 2)$

Wir wollen zeigen, daß das Kriterium in Paragraph 6 auch im Fall $k = 2$ erfüllt ist. Das heißt wir beweisen: Für jedes $\tau = 0, 1, \dots, p - 2$ gibt es in $H_{p+\tau} D / H_{p+\tau+1} D$ sicher $\Pi_{(2,p+\tau-2)}^p$ voneinander unabhängige Elemente T , die alle Produkte aus Basiskommutatoren vom Typus $(2, p + \tau - 2)$ sind.

Wir beginnen mit $\tau = 0$. Wir berechnen das zum Monom x_2^2 gehörige e^* . Nach Paragraph 6 folgt

$$e^* \equiv \prod_{l=0}^{\left[\frac{p-2}{2}\right]} [P_2, (p - 2 - l) P_1, [P_2, l P_1]]^{a_{p,l}} \bmod H_{p+1} D .$$

Die Hallschen Exponenten $a_{p,l}$ berechnen wir nach der Methode von Paragraph 2. Es sei $((\varrho_1, \tau_1), \dots, (\varrho_p, \tau_p))$ das generelle Label des oben angeschriebenen Faktors. Dann lauten die E Bedingungen

$$1 \leq \varrho_1 < \varrho_2 < \dots < \varrho_{p-1-l} \leq p ; \quad \varrho_1 < \varrho_{p-l} < \varrho_{p-l+1} < \dots < \varrho_p \leq p .$$

Da nach Paragraph 2 alle ϱ_i ($i = 1, 2, \dots, p$) verschiedene Zahlen von 1 bis p darstellen, folgt $\varrho_1 = 1$. Zur Erfüllung der obigen Bedingungen hat man dann offenbar $\binom{p-1}{l+1}$ Möglichkeiten, d. h. es gibt, wie man sofort überlegt, ebensoviele Klassen nach den ϱ . Da die ϱ alle verschieden sind, gibt es keine Bindungen zwischen den τ , d. h. es gibt in jeder Klasse x_2^2 Label. Somit folgt $a_{p,l} \equiv (-1)^{l+1} \bmod p$.

Das gesuchte e^* hat also die Gestalt

$$e^*(x_2^2) \equiv \prod_{l=0}^{\left[\frac{p-2}{2}\right]} [P_2, (p - 2 - l) P_1, [P_2, l P_1]]^{(-1)^{l+1}} \bmod H_{p+1} D . \quad (29)$$

Nun sei $1 \leq \tau \leq p - 2$. Dann findet man durch Kommutatorbildung mit den im vorigen Paragraphen gefundenen Elementen $T(\tau)$ die weiteren

$$T(\tau, l) = [P_2, (p - 2 + l)P_1, [P_2, (\tau - l)P_1]] \quad (l = 1, 2, \dots, \tau) . \quad (30)$$

Wieder ist klar nach Satz 1, daß diese T -Elemente voneinander unabhängig sind mod D .

Im Falle der ungeraden τ haben wir also im Bereich $0 < \tau \leq p - 2$ gerade $\Pi_{(2,p+\tau-2)}^p$ unabhängige Elemente T angeben können vom Typus $(2, p + \tau - 2)$.

Nun sei τ gerade und > 0 . Ersetzt in (26) das Element P_2 durch den Kommutator $[P_2, (\tau - 1)P_1, P_2]$, so erhält man wieder ein Element aus D' mod D , viz. $[[P_2, (\tau - 1)P_1, P_2], (p - 1)P_1]$.

Durch Benutzung der Formel (4) erhält man für den vorstehenden Kommutator die Darstellung

$$\prod_{l=0}^{\tau-2} B_l^{(p-1)} \prod_{l=\tau-1}^{\left[\frac{p+\tau-3}{2}\right]} B_l^{(p-1)-(i+1-\tau)} \text{ mod } H_{p+\tau+1} D .$$

Wegen (30) kann man die Elemente B_l ($l = 0, 1, \dots, \tau - 1$) eliminieren. So gewinnt man ein T -Element der Gestalt

$$\prod_{l=\tau}^{\left[\frac{p+\tau-3}{2}\right]} B^{(-1)^l} ,$$

das man wegen $p \neq 2 \text{ mod } D$ in der Gestalt

$$\prod_{l=\tau}^{\frac{p+\tau-3}{2}} B_l^{(-1)^l} \text{ mod } H_{p+\tau+1} D \quad (\tau = 2, 4, \dots, p - 3) \quad (31)$$

schreiben kann. Damit haben wir in jedem Fall die gewünschte Anzahl von unabhängigen Elementen T im Typus $(2, p + \tau - 2)$ angegeben.

Damit ist nach Paragraph 6 bewiesen

$$\delta_{(2,p+\tau-2)}^p = \Pi_{(2,p+\tau-2)}^p \quad (\tau = 0, 1, \dots, p - 2) . \quad (32)$$

§ 10. $\delta_{(3,p+\tau-3)}^p$ ($\tau = 0, 1, \dots, p - 2$) .

Wie im vorigen Paragraphen zeigen wir: Für jedes $\tau = 0, 1, \dots, p - 2$ gibt es in $H_{p+\tau} D / H_{p+\tau+1} D$ sicher $\Pi_{(3,p+\tau-3)}^p$ voneinander unabhängige Elemente T , die Produkte sind aus Basiskommutatoren vom Typus $(3, p + \tau - 3)$.

Wir beginnen mit $\tau = 0$ und berechnen das zu x_2^3 gehörige e^* . Es hat die Gestalt

$$e^* \equiv [P_2, (p-3) P_1, 2 P_2] \dots \pmod{H_{p+1} D}. \quad (33)$$

Nun sei $\tau \geq 2$. Aus dem Element (26) erhält man durch Kommutatorbildung die weiteren T -Elemente

$$[P_2, (p-1) P_1, P_{i_1}, P_{i_2}, \dots, P_{i_\tau}] , \quad (34)$$

wobei $\tau - 2$ unter den P_{i_ℓ} immer gleich P_1 sein sollen, die restlichen gleich P_2 . Durch Einfügen von eckigen Klammern in (34) kann man immer auf genau eine Weise erreichen, daß der obige Kommutator zu einem Basiskommutator wird. Man gelangt auf diesem Wege zu $\binom{\tau}{2}$ voneinander unabhängigen Elementen T vom Typus $(3, p + \tau - 3)$.

Es bleibt also noch zu zeigen, daß es für $\tau \geq 1$ sicher

$$\Pi_{(3,p+\tau-3)}^p - \binom{\tau}{2} = \frac{1}{3!} (5\tau + a)$$

von den schon konstruierten unabhängigen Elementen T vom Typus $(3, p + \tau - 3)$ gibt.

Wir haben bisher die Elemente T in (29) und (31) noch nicht benutzt zur Ableitung von neuen Elementen T . Dies wollen wir jetzt tun.

Nach (29) und (31) gibt es für gerade $k \pmod{H_{p+k+1} D}$ ein T der Gestalt

$$T_{(k,l)} = \prod_{l=k}^{\frac{p+k-3}{2}} [P_2, (p+k-2-l) P_1, [P_2, l P_1]]^{(-1)^l} .$$

Durch Kommutatorbildung gewinnt man Elemente T der Gestalt

$$[T_{(k,l)}, [P_2, (\tau-k-1) P_1]] \pmod{H_{p+\tau+1} D} \quad (k=0, 2, 4, \dots, \leq \tau-1) . \quad (35)$$

Wir wollen zeigen, daß alle diese T -Elemente voneinander und auch von den früheren T -Elementen unabhängig sind. Den Beweis führen wir so, indem wir die Elemente in (35) in der Form (1) schreiben und zeigen, daß diese Elemente in den Basiskommutatoren

$$B_{k,\tau-1-k} = \begin{cases} [P_2, (p-2) P_1, [P_2, k P_1], [P_2, (\tau-1-k) P_1]] & (k \leq \tau-1-k) \\ [P_2, (p-2) P_1, [[P_2, k P_1], [P_2, (\tau-1-k) P_1]]] & (k > \tau-1-k) \end{cases}$$

voneinander unabhängig sind.

Wegen $0 \leq \tau \leq p-2$ ist $\tau-1-k \leq p-3$ in (35). Dies bedeutet, daß die Elemente $B_{k,\tau-1-k}$ bei der Überführung in Normalform

nur von T (vgl. 35) herrühren können, und zwar nur vom ersten Faktor, der die Gestalt hat $[P_2, (p-2)P_1, [P_2, kP_1]]$.

Setzt man

$$C_{m,\tau-1-m} = \begin{cases} B_{m,\tau-1-m} & (m \leq \tau - 1 - m) \\ B_{m,\tau-1-m} B_{\tau-1-m,m} & (m > \tau - 1 - m) \end{cases} \quad (m = 0, 1, \dots, \tau - 1) \quad (36)$$

so nehmen die Elemente in (35) mit Beachtung der Rechenregeln (3) die simple Form an (37)

$$[T, [P_2, (\tau-k-1)P_1]] \equiv C_{k,\tau-1-k} \dots \pmod{H_{p+\tau+1} D} \quad (k=0, 2, 4, \dots \leq \tau-1)$$

Da die $C_{k,\tau-1-k}$ voneinander und auch von den früheren schon konstruierten T unabhängig sind \pmod{D} , folgt die Existenz von $\left[\frac{\tau+1}{2}\right]$ weiteren T vom Typus $(3, p + \tau - 3)$ für $\tau \geq 1$.

Die Fälle $\tau = 0, 1$ sind also als erledigt zu betrachten und wir dürfen jetzt $\tau \geq 2$ voraussetzen. Es ist unsere Aufgabe, zu zeigen, daß es noch

$$\Pi_{(3,p+\tau-6)}^p - \binom{\tau}{2} - \left[\frac{\tau+1}{2}\right]$$

weitere unabhängige T gibt vom Typus $(3, p + \tau - 3)$. Diese Aufgabe wird in Paragraph 11 für ungerade, in Paragraph 12 für gerade τ gelöst.

§ 11. $\tau = 2n + 1 > 2$.

Wir betrachten die spezielle p -te Potenz $(P_1 P_2^{x_2} P_k^{x_k})^p$ mit

$$P_k = [P_2, (\tau - 1 - k)P_1, [P_2, kP_1]] \quad (k = 0, 1, \dots, g - 1)$$

und

$$g = \Pi_{(3,p+\tau-3)}^p - \binom{\tau}{2} - \left[\frac{\tau+1}{2}\right] = \frac{2\tau+a-3}{3!}$$

und berechnen das zum Monom $x_k x_2$ gehörige e^* .

Es ergibt sich zunächst

$$e^*(x_k x_2) \equiv \prod_{l=0}^{\frac{p-3}{2}} [P_k, (p-2-l)P_1, [P_2, lP_1]]^{c_l} \dots \pmod{H_{p+\tau+1} D}$$

$$\prod_{l=\frac{p-1}{2}}^{p-2} [P_2, lP_1, [P_k, (p-2-l)P_1]]^{c_l} \dots \pmod{H_{p+\tau+1} D}.$$

c_l ist nach der Methode in Paragraph 9 zu bestimmen. Man findet für

$l = 0, 1, \dots, \frac{p-3}{2}$ den Wert $\binom{p-1}{l+1}$ und für $l = \frac{p-1}{2}, \dots, p-2$ den Wert $\binom{p-1}{p-1-l}$. Es folgt also

$$e^*(x_k x_2) = \prod_{l=0}^{p-2} [P_k, (p-2-l) P_1, [P_2, l P_1]]^{(-1)^{l+1}} \bmod H_{p+\tau+1} D. \quad (38)$$

Wir behaupten, daß die $e^*(x_k x_2)$ ($k = 0, 1, 2, \dots, g-1$) in den Elementen $C_{m, \tau-1-m}$ ($m = 1, 3, 5, \dots, 2g-1$) voneinander und also auch von den früheren T unabhängig sind.

Nach der Formel (3) folgt (für $l < p-2$)

$$[P_k, (p-2-l) P_1] \equiv \prod_{\varepsilon=0}^{\tau-2-2k} P_{k+\varepsilon}^{(p-2-l)} \prod_{\varepsilon=\tau-1-2k}^q P_{k+\varepsilon}^{(p-2-l)-(\varepsilon-\tau+1+2k)} \quad (39)$$

und es bedeutet

$$P_{k+\varepsilon} = [P_2, (p+\tau-3-l-(k+\varepsilon)) P_1, [P_2, (k+\varepsilon) P_1]].$$

Da $l < p-2$ können bei der Überführung von $e^*(x_k x_2)$ in die Form (1) die Elemente $C_{m, \tau-1-m}$ für festes k nur herrühren von

$$P_{k+\varepsilon} = [P_2, (p-2) P_1, [P_2, (k+\varepsilon) P_1]].$$

Das heißt es muß für festes k

$$\varepsilon = \tau - 1 - k - l \geq 0 \quad (40)$$

sein. Da wir (38) nur in bezug auf die Elemente $C_{2m-1, \tau-2m}$ ($m = 1, \dots, g$) genau bestimmen wollen, ist es wichtig zu entscheiden, welchem Bereich das ε angehört. Wir zeigen, daß $\varepsilon \leq \tau - 2 - 2k$. Zusammen mit (40) bedeutet dies $l \geq k+1$ oder $\tau - 2m \geq k+1$. Diese letztere Ungleichung ist bestimmt richtig, wenn sie für die maximalen Werte von m und k erfüllt ist. Da $\max(m) = g$ und $\max(k) = g-1$ folgt $\tau \geq 3g$ und dies ist gleichbedeutend mit $a \leq 3$. Da τ ungerade und also $a = 1, 3, -1$ ist dies eine richtige Ungleichung.

Wir können daher (40) ersetzen durch

$$\varepsilon = 2m - 1 - k ; \quad 0 \leq \varepsilon \leq \tau - 2 - 2k. \quad (40)^*$$

Somit folgt schließlich die Darstellung

$$e^*(x_k x_2) = \prod_{m \geq k'+1}^{g-1} C_{2m-1, \tau-2m}^{(p-2-\tau+2m)} (k = 2k' = 0, 2, 4, \dots \leq g-1) \quad (41)$$

$$e^*(x_k x_2) = \prod_{m \geq k'}^{g-1} C_{2m-1, \tau-2m}^{(p-2-\tau+2m)} \cdot C_{2k'-1, \tau-2k'} (k = 2k'-1 = 1, 3, \dots \leq g-1)$$

Der Faktor $C_{2k'-1, \tau-2k'}$ in $e^*(x_k x_2)$ für ungerade k röhrt her vom letzten Faktor in (38) für $l = p - 2$. Dieser ist nämlich gleich $B_{\tau-1-k, k}^{-1}$ für $\tau - 1 - k > k$. Diese Ungleichung ist für $k = 0, 1, \dots, g - 1$ erfüllt, so daß man also $B_{\tau-1-k, k}^{-1} = C_{k, \tau-1-k} C_{\tau-1-k, k}^{-1}$ wirklich durch $C_{k, \tau-1-k}$ ersetzen darf.

Bezeichnet man den Exponenten von $C_{2m-1, \tau-2m}$ in $e^*(x_k x_2)$ mit $d_{k+1, m}$ ($m = 1, 2, \dots, g$; $k = 0, 1, \dots, g - 1$), so hat man zum Beweis der Unabhängigkeit aller $e^*(x_k x_2)$ zu zeigen, daß $|d_{k+1, m}| \not\equiv 0 \pmod{p}$. Substituiert man i für $k + 1$ und k für m , so nimmt unsere Determinante die Gestalt an

$$\begin{aligned} d_{ik} &= \binom{p - \tau - 2 + 2k}{2k - i} \quad (i < 2k) \\ d_{ik} &= 2 \quad (i = 2k) \\ d_{ik} &= 0 \quad (i > 2k) \end{aligned} \tag{42}$$

und wir wollen ihren Wert bestimmen.

Zu diesem Zweck multiplizieren wir die i -te Zeile mit

$$p_{i-2} = \prod_{l=0}^{i-2} (p - \tau + l) \quad (i = 2, 3, \dots, g - 1).$$

Dann kann man aus der $k + 1$ -ten Spalte den Faktor p_{2k} ausklammern ($k = 0, 1, \dots, g - 1$). Das heißt es ist

$$|d_{ik}| = \frac{\prod_{l=0}^{g-1} p_{2l}}{\prod_{l=0}^{g-2} p_l} |e_{ik}| \tag{43}$$

mit

$$e_{ik} = \frac{1}{2k - i!} \quad (i < 2k), \quad e_{ik} = 2 \quad (i = 2k), \quad e_{ik} = 0 \quad (i > 2k). \tag{44}$$

Wir definieren, von $|e_{ik}| = |e_{ik}|^{(1)}$ ausgehend, eine Determinante $|e_{ik}|^{(m)}$ folgendermaßen: Man erhält $|e_{ik}|^{(m+1)}$ aus $|e_{ik}|^{(m)}$, indem man zur $m + 2l - 1$ -ten Zeile von $|e_{ik}|^{(m)}$ das $-2(2m - 1)$ -fache der $m + 2l - 2$ -ten Zeile addiert ($l = 1, 2, \dots$).

$e_{ik}^{(m)}$ kann folgendermaßen definiert werden

$$e_{ik}^{(m)} = \frac{i - 1!}{2k - 1!} \binom{2k - i - 1}{i - 1} \quad (k = i, i + 1, \dots, g; i = 1, 2, \dots, m). \tag{45}$$

Ist $i = m - 1 + i^*$, $k = m - 1 + k^*$, so gilt

$$e_{ik}^{(m)} = \frac{m-1!}{2k-1!} \binom{2k-m-1}{m-1} (i^* = 1, 3, \dots; i^* < 2k^*) ,$$

$$e_{ik}^{(m)} = \frac{m-2!}{2k-3!} \binom{2k-m-3}{m-1} (i^* = 2, 4, \dots; i^* \leq 2k^*) .$$

An allen Stellen, wo $e_{ik}^{(m)}$ nicht definiert ist, soll eine Null stehen. Eine leichte Induktion nach $m \geq 2$, beweist sofort die Richtigkeit der angegebenen Darstellung von $|e_{ik}|^{(m)}$ und es folgt $\|e_{ik}\|^{(g)} = \|e_{ik}\|$.

Aus (45) folgt

$$\|e_{ik}\| = \prod_{l=1}^g \frac{l-1}{2l-1!}$$

Da $2 < \tau \leq p-2$ und $g = \frac{2\tau+a-3}{3!} \leq \frac{\tau}{3}$ ist die Determinante $\|d_{ik}\| \not\equiv 0 \pmod{p}$.

§ 12. $\tau = 2n \leq 2$.

Wir gehen analog vor wie im Fall der ungeraden τ . Wir betrachten die Gestalt der $e^*(x_k x_2)$ in (38) lediglich hinsichtlich der Elemente $C_{2m-1, \tau-2m}$ ($m = 1, 2, \dots, g-1; m = \frac{\tau}{2}$). Für gerade τ bedeutet g die Zahl $\frac{2\tau+a}{3!}$.

Die Bedingung (40) hat auch hier Geltung, und wir wollen wieder untersuchen, unter welchen Umständen $\varepsilon \leq \tau - 2 - 2k$. Dies ist gleichbedeutend mit der Frage, wann die Elemente $C_{2m-1, \tau-2m}$ für $m = 1, 2, \dots, g-1$ dem ersten Produkt in (39) angehören. Als Bedingung ergibt sich $a \leq 4$. Da τ gerade, ist dies nur in den Fällen $a = 2, 4$ stets der Fall.

Für $a = 6$ und $k < g-1$, gehört $C_{2m-1, \tau-2m}$ ebenfalls dem ersten Produkt an, denn hier ergibt sich als Bedingung $a \leq 6$. Es gehört aber $C_{2m-1, \tau-2m}$ für $m = g-1$ und $k = g-1$ zum zweiten Produkt in (39). Man findet hier $\varepsilon = 2m-1-k = g-2$, also $k+\varepsilon = 2g-3$. Aus (39) folgt

$$[P_{g-1}, (p-2-l) P_1] \equiv \left(C_{2g-3, \tau-2-2g}^{\binom{p-2-l}{g-2} - \binom{p-2-l}{0}} \right)^{(-1)^{l+1}},$$

andererseits tritt aber offensichtlich noch das Element $C_{2g-3, \tau-2-2g}^{-1}$ an anderer Stelle auf, nämlich herrührend vom letzten Faktor in (38)

$(l = p - 2)$. Das hat zur Folge, daß gesamthaft $C_{2g-3, \tau-2-2g}$ nur mit dem Exponenten

$$-\binom{p-2-l}{g-2}$$

auftritt, denn $l + 1 = g$ ist für $a = 6$ ungerade.

Die endgültige Darstellung der e^* lautet daher

$$\begin{aligned} e^*(x_k x_2) &= \prod_{m \geq k'+1}^{g-1} C_{2m-1, \tau-2m}^{(p-2-\tau+2m)} \cdot C_{\tau-1, 0}^{(p-2)-\binom{p-2}{k}} (k-2k' = 0, 2, \dots \leq g-1) \\ e^*(x_k x_2) &= \prod_{m \geq k'+1}^{g-1} C_{2m-1, \tau-2m}^{(p-2-\tau+2m)} \cdot C_{\tau-1, 0}^{(p-2)-\binom{p-2}{k}} (k=2k'-1=1, 3, \dots \leq g-1) \end{aligned} \quad (46)$$

Für $k = 0$ hat man noch den zusätzlichen Faktor $C_{\tau-1, 0}$ hinzuzufügen.

Schreibt man das Symbol $d_{k+1, m}$ für den Exponenten von $C_{2m-1, \tau-2m}$ in $e^*(x_k x_2)$, so haben wir wiederum zu beweisen, daß $\|d_{k+1, m}\|$ ($k = 0, 1, \dots, g-1$; $m = 1, 2, \dots, g$) nicht durch p teilbar ist.

Entwickelt man $|d_{k+1, m}|$ nach der ersten Zeile und addiert man in der als Faktor auftretenden Unterdeterminante die 2-te Zeile zur ersten, die 3-te zur 2-ten usw., so wird die letzte Spalte $\equiv 0 \pmod{p}$ bis auf das Glied

$$d_{g, g} = \binom{p-2}{\tau-g} - \binom{p-2}{g-1}.$$

Es ist daher, wenn man noch $k + l = i$ und $m = k$ setzt

$$\|d_{ik}\| \equiv (p-\tau) \left(\binom{p-2}{\tau-g} - \binom{p-2}{g-1} \right) \|e_{ik}\|. \quad (47)$$

Die Determinante $|e_{ik}|$ des Grades $g-2$ ist definiert durch

$$e_{ik} = \binom{p-\tau+1+2k}{2k+1-i} \quad (i < 2k) \quad e_{ik} = p-\tau+2k \quad (i=2k) \quad e_{ik} = 0 \quad (i > 2k) \quad (48)$$

Setzt man

$$p_i = \prod_{k=0}^l (p-\tau+2+k)$$

und multipliziert man die $i+2$ -te Zeile von $|e_{ik}|$ mit p_i ($i \geq 0$), so kann man aus der k -ten Spalte den Faktor p_{2k} ($k = 0, 1, \dots, g-3$) herausgeben. Da diese Faktoren für $\tau \leq p-2$ und

$$g = \frac{2\tau+a}{3!}$$

kleiner als p und größer als 0 sind, genügt es, die Determinante $|f_{ik}|$ zu betrachten, viz.

$$f_{ik} = \frac{p-\tau+1+2k}{2k+1-i!} (i < 2k), \quad f_{ik} = p-\tau+2k (i=2k), \quad f_{ik} = 0 (i > 2k), \quad (49)$$

die aus e_{ik} durch Abspaltung dieser Faktoren hervorgeht.

Erklärt man $|f_{ik}|^{(m)}$ analog wie im vorigen Paragraphen, so beweist man durch vollständige Induktion nach m (≥ 2) die Richtigkeit der folgenden Formeln :

$$f_{ik}^{(m)} = \frac{1}{2k!} \quad (k = 1, 2, \dots, g-2) \quad (50)$$

$$f_{ik}^{(m)} = \frac{(i-1)! (p-\tau+i+1) \binom{2k-i}{i-1} + i! \binom{2k-i-1}{i-2}}{2k!} \quad (k=i, i+1, \dots; i=2, 3, \dots, m)$$

Setzt man weiter $i = m - 1 + i^*$, $k = m - 1 + k^*$, so gilt

$$f_{ik}^{(m)} = \frac{(m-1)! (p-\tau+i+1) \binom{2k-m}{m-1} + m! \binom{2k-m-1}{m-2}}{2k!} \quad (i=m, m+2, \dots; i^* < 2k^*)$$

$$f_{ik}^{(m)} = \frac{(m-2)! (p-\tau+i+2) \binom{2k-m-1}{m-2} + (m-1)! \binom{2k-m-2}{m-3}}{2k-2!} \quad (i=m+1, m+3, \dots; i^* \leq 2k^*) \quad (51)$$

An den nicht definierten Stellen ist 0 zu setzen. Außerdem haben wir die Faktoren p_{2l} und p_{2l+1} ($l = 0, 1, \dots, g-3$), die man für $m = 2, 3$ vor die Determinante $|f_{ik}|^{(2)}$ bzw. $|f_{ik}|^{(3)}$ nehmen kann, unterdrückt, da sie im Bereich $(1, p-1)$ liegen.

Aus (50) folgt jetzt

$$\|d_{ik}\| \equiv \text{const } \|f_{ik}\|^{(g-2)} \equiv \text{const } \frac{1}{2} \prod_{l=2}^{g-2} \frac{l!}{2l!} (p-\tau+2l).$$

Da

$$2 \leq \tau \leq p-2 \quad \text{und} \quad g = \frac{2\tau+a}{3!}$$

ist $\|d_{ik}\| \not\equiv 0 \pmod{p}$.

§ 13. Über die Klasse der Burnsidegruppen.

Aus

$$\delta_{(3,p+\tau-3)}^p < d_{(3,p+\tau-3)} \quad (\tau = p-2)$$

ergibt sich als *Korollar*: Die Klasse c der Burnsidegruppen vom Exponenten $p \geq 5$ ist $\geq 2p-2$.

Die Resultate der vorangehenden Abschnitte erlauben aber eine Verstärkung dieser Aussage.

Rechnet man nämlich in der Faktorgruppe $F|H_{2p}H_{(4,1)}$, so ist die Gruppe H_p Abelsch und die Kommutatorgruppe H_2 wird zu einer nilpotenten Gruppe der Klasse $3 < p$. Man kann daher alles in Paragraph 4 Gesagte wörtlich übernehmen. Insbesondere hat man nur die p -ten Potenzen zu betrachten der Gestalt:

$$(P_1 P_2^{x_2} P_3^{x_3} \dots P_r^{x_r})^p \quad (0 \leq x_1, x_2, \dots, x_r < p; w(P_r) \leq p) .$$

Bedenkt man weiter, daß nach den Ergebnissen der vorangehenden Abschnitte alle e -Elemente $\text{mod } H_{2p-1}H_{(4,1)}H_2^p/H_{2p-1}H_{(4,1)}$ voneinander unabhängig sind, so ergibt sich als Korollar

$$\delta_{(v, p+\tau-v)}^p \leq \Pi_{(v, p+\tau-v)}^p \quad (\tau = p-1; v = 1, 2, 3) .$$

Man bestätigt aber leicht, daß wegen $p-1 = 6m$ oder $6m+4$ stets

$$\Pi_{(3, p+\tau-3)}^p < d_{(3, p+\tau-3)} \quad (p \geq 7; \tau = p-1) .$$

Ebenso verifiziert man nach unserer Methode leicht, daß $\delta_{(3,6)}^5 = \Pi_{(3,6)}^5 - 2$ und also $\delta_{(3,6)}^5 < d_{(3,6)}$. Damit ist der Satz bewiesen:

14. Satz. *Die Klasse c der Burnsidegruppen vom Exponenten $p > 3$ ist $\geq 2p-1$.*

(Eingegangen den 19. März 1953.)