Zeitschrift: Commentarii Mathematici Helvetici

Herausgeber: Schweizerische Mathematische Gesellschaft

Band: 23 (1949)

Artikel: Kurzer Beweis des gruppentheoretischen Satzes von Hajós.

Autor: Rédel, L.

DOI: https://doi.org/10.5169/seals-19763

Kurzer Beweis des gruppentheoretischen Satzes von Hajós

Von L. Rédei, Szeged (Ungarn)

Mit Dank und Liebe meiner Frau gewidmet.

§ 1. Einleitung

Bezeichne G eine endliche Abelsche Gruppe. Das Einselement bezeichnen wir mit 1 und nehmen stets $G \neq 1$ an. Kleine griechische und lateinische Buchstaben (auch mit Indizes versehen) bezeichnen Elemente von G bzw. ganze Zahlen; eine Ausnahme macht „x".

Einen Komplex von der Form

$$[\alpha]_e = (1, \alpha, \ldots, \alpha^{e-1}) \qquad (e \geqq 2) \tag{1}$$

nennen wir ein (e-gliedriges) *Simplex*, wobei wir stets annehmen, daß die Elemente verschieden sind, d. h. die Ordnung von α größer oder gleich e ist. Meistens schreiben wir kurz $[\alpha]$ für $[\alpha]_e$, kommen dann aber gleichzeitig mehrere Simplexe $[\alpha], [\beta], \ldots$ vor, so soll das nie bedeuten, daß die Gliederzahlen gleich sein müßten. Es ist klar, daß (1) dann und nur dann eine Gruppe ist, wenn α die Ordnung e hat.

Der Satz von Hajós[1]), wohl einer der wichtigsten in der Theorie der endlichen Abelschen Gruppen, lautet so:

Gilt für eine endliche Abelsche Gruppe G eine „Simplexzerlegung"

$$G = [\alpha_1] \ldots [\alpha_n] \qquad (n \geqq 1)\ , \tag{2}$$

so ist mindestens ein Faktor der rechten Seite eine Gruppe. Man nenne (2) auch eine *Hajóssche Zerlegung.*

---

[1]) *G. Hajós*: Über einfache und mehrfache Bedeckung des n-dimensionalen Raumes mit einem Würfelgitter. Math. Zeitschr. 47 (1942), S. 427—467, insbesondere S. 442. Früher auch ungarisch erschienen als „Többméretü terek befedése kockarácscsal". Mat. fiz. lapok 45 (1938), S. 171—190 und „Többméretü terek egyszeres befedése kockaráccsal". Mat. fiz. lapok 48 (1941), S. 37—64.

Selbstverständlich ist (2) so zu verstehen, daß bei dem Ausmultiplizieren der rechten Seite alle Elemente von G genau einmal entstehen.

Ich denke, daß Hajós' Satz bisher noch nicht genügend Gemeingut geworden ist, weshalb ich hier kurz einiges über ihn bemerke.

In expliziter Form lautet der Satz so: Immer wenn

$$\alpha_1^{k_1} \dots \alpha_n^{k_n} \qquad (k_i = 0, \dots, e_i - 1 \; ; \; i = 1, \dots, n)$$

alle verschiedenen Elemente von G sind, dann hat ein α_i die Ordnung e_i. (In dieser Formulierung dürfen $e_1, \dots, e_n$ ($\geqq 1$) beliebig sein.) Dies zeigt eine große formale Ähnlichkeit mit dem Fundamentalsatze auf (man denke an die Basisdarstellung von G), und zwar handelt es sich im Satz offenbar um eine Art Umkehrung des Fundamentalsatzes. (Dieses Verhältnis beider Sätze zueinander wird noch deutlicher, wenn man den Fundamentalsatz so ausspricht: G hat eine Simplexzerlegung (2), in der alle Faktoren Gruppen sind.

Man ist geneigt, „Strukturfragen" aller Art der endlichen Abelschen Gruppen mit dem Fundamentalsatze prinzipiell erledigt anzusehen. Hajós' Satz stürzt eine solche Meinung zu Haufen, vielmehr wird man nach einer näheren Beschäftigung mit dem Satze zur Überzeugung gebracht, daß der Satz vom Fundamentalsatze völlig unabhängig ist, diesem an Tiefe nicht hintersteht, und ihn an den Schwierigkeiten des Beweises vielfach übertrifft. Ein Beleg für diese Meinung ist selbst der (bisher einzig vorhandene) Originalbeweis von Hajós voll mit scharfsinnigen Überlegungen, der dabei vom Fundamentalsatze keinen Gebrauch macht.

Die Wichtigkeit des Satzes ragt weit über die Gruppentheorie hinaus, denn — wie das ebenfalls Hajós gezeigt hat — in einer anderen (äquivalenten) Form als *Satz von Minkowski-Hajós* spricht der Satz die Richtigkeit der berühmten (vor Hajós unbewiesenen) Vermutung von Minkowski über den „Grenzfall" von Diophantischen homogenen linearen Ungleichungen (in einer weiteren Form handelt es sich um „raumzerlegende Würfelgitter")[2]).

Aus diesen Gründen war sehr erwünscht, den umfangreichen und komplizierten Beweis von Hajós durch einen leichteren zu ersetzen. Das glückte mir über Erwartung. Der hier mitzuteilende Beweis ist durch eine Reihe inhaltlicher und formaler Vereinfachungen des Hajósschen Beweises entstanden, dabei blieb der tiefe Grundgedanke des Beweises unberührt und tritt jetzt viel deutlicher zur Geltung.

Ich beabsichtige auf verschiedene Fragen (auch Anwendungen) im

---

[2]) Näheres hierüber s. bei Hajós[1]).

Zusammenhange mit dem Satz zurückzukommen. Insbesondere fand ich einen (ebenfalls „fundamentalsatzfreien") Weg, wie man den Satz von Hajós mit einfachen Mitteln auf den Fall von p-Gruppen zurückführen kann. Deshalb scheinen mir die eigentlichen Schwierigkeiten des Satzes im Fall der p-Gruppen konzentriert zu sein. (In den Hajósschen Beweis spielt der Begriff von p-Gruppen gar nicht hinein.)[3])

§ 2. Der Ring der Komplexe

Zum Beweis des Satzes von Hajós ist es nötig, daß wir die Komplexe verallgemeinern und dann ihre Menge zu einem Ring machen. Die Verallgemeinerung geschieht so, daß wir den Elementen eine beliebige (positive oder negative) ganzzahlige Multiplizität zukommen lassen, genauer fassen wir das in die folgende:

Definition 1. Unter einem (allgemeinen) Komplex K (von G) verstehen wir ein (doppeltes) System von verschiedenen Elementen $\alpha_1, \ldots, \alpha_n$ der Gruppe G und von beliebigen ganzen „Multiplizitätszahlen" $c_1, \ldots, c_n$ $(\neq 0)$, in Zeichen:

$$K = (c_1 \alpha_1, \ldots, c_n \alpha_n) \qquad (n \geqq 0) \; , \tag{3}$$

wobei die Reihenfolge der „Glieder" außer acht zu lassen ist. Die α_i nennen wir die Elemente von K und schreiben hierfür $\alpha_i \in K$ $(i = 1, \ldots, n)$. Nur im Fall $n = 0$ hat K keine Elemente, dann setzen wir $K = 0$. Ist $K \neq 0$ und sind alle c_i positiv, so nennen wir auch K positiv und setzen $K > 0$. Eingliedrige Komplexe $(n = 1)$ bezeichnen wir kurz als $c\alpha$ statt $(c\alpha)$. Den Fall $c_1 = \cdots = c_n = 1$ von (3) identifizieren wir mit $K = (\alpha_1, \ldots, \alpha_n)$, und dann sind diese „gewöhnlichen" Komplexe als Spezialfälle unter den allgemeinen Komplexen enthalten. (Auch wenn einige $c_i = 1$ sind, lassen wir diese c_i in (3) fort.)

Es soll ausdrücklich bemerkt werden, daß die Elemente von K stets einen gewöhnlichen Komplex bilden; dieser ist gleich 0, wenn $K = 0$ gilt. Es ist auch wichtig, daß insbesondere alle Untergruppen von G unter den (allgemeinen) Komplexen vorkommen.

Bequemlichkeitshalber heben wir die Einschränkung auf, daß die α_i untereinander und die c_i von 0 verschieden sind (und behalten auch dann die Bezeichnung (3)), vereinbaren wir uns aber, daß zwei Glieder $a\alpha$, $b\alpha$

---

[3]) Zu den obigen siehe noch: *L. Rédei*: Zwei Lückensätze über Polynome in endlichen Primkörpern mit Anwendung auf die endlichen Abelschen Gruppen und die Gaußischen Summen. Acta Math. 79 (1947), S. 273—290.

durch das Glied $(a + b)\alpha$ ersetzt und die Glieder 0α gestrichen werden dürfen. Dann läßt sich jeder Komplex auf die „Normalform" (3) bringen (wobei nämlich die α_i voneinander und die c_i von 0 verschieden sind), die offenbar (bis auf die Reihenfolge der Glieder) stets eindeutig bestimmt ist. Selbstverständlich nennen wir zwei Komplexe gleich, wenn ihre Normalformen übereinstimmen, und so sind alle verschiedenen Komplexe schon die oben definierten. Man merke sich wohl: Ist (3) nicht die Normalform von K, so sind auch die α_i nicht die Elemente von K (diese sind nach wie vor von der Normalform abzulesen).

Um nun die Menge aller Komplexe zu einem Ring zu machen, den wir mit (G) bezeichnen werden, definieren wir vor allem Summe und Produkt von zwei eingliedrigen Komplexen mit den Regeln:

$$a\alpha + b\beta = (a\alpha, b\beta) \ , \qquad a\alpha \cdot b\beta = ab \cdot \alpha\beta \ .$$

Indem wir diese mit zweiseitiger Distributivität ergänzen, so haben wir den gewünschten Ring (G) festgelegt[4]). Die Buchstaben H, K (auch mit Indizes versehen) bezeichnen nachher stets Elemente von (G). Summe, Produkt und Differenz bezeichnen wir mit $H + K$, HK, $H - K$. Beispiele:

$$(-3\alpha, \gamma) + (\alpha, 2\beta, -\gamma) = (-2\alpha, 2\beta) \quad ,$$

$$(1, \alpha)(3, -2\alpha) = (3, \alpha, -2\alpha^2) \ .$$

Selbstverständlich bezeichnet cK $(c > 0)$ die Summe $K + \cdots + K$ (mit c Summanden).

Offenbar läßt sich für (3) auch

$$K = c_1 \alpha_1 + \cdots + c_n \alpha_n \tag{4}$$

schreiben, denn das Resultat der Addition führt auf (3) zurück. Im folgenden bevorzugen wir diese „additive Schreibweise".

Für das spätere führen wir noch zwei einfache, aber wichtige Begriffe ein:

Definition 2. Unter der Ordnung $O(K)$ von K verstehen wir (nach (3) oder (4))

$$O(K) = c_1 + \cdots + c_n \ . \tag{5}$$

---

[4]) Im wesentlichen stimmt (G) mit dem sogenannten „Gruppenring (von G) über dem Ring der ganzen Zahlen" überein, wovon wir aber keine Notiz nehmen wollen, obwohl die Übereinstimmung nach (4) auch formal vollkommen gemacht wird.

Definition 3. Unter dem Gewicht $g(K)$ von K verstehen wir die Anzahl aller (nicht nur der verschiedenen) Primfaktoren der Ordnung $O(K)$ von K. Dabei soll $O(K) \neq 0$ angenommen werden, einem K mit $O(K) = 0$ schreiben wir kein Gewicht zu.

Es ist klar, daß in (5) gleichgültig ist, ob K in der Normalform oder anders angenommen wurde. Kurz gesagt: $O(K)$ und daher auch $g(K)$ sind durch K (invariant) bestimmt. Offenbar gelten[5]):

$$O(HK) = O(H)O(K) \ , \qquad g(HK) = g(H) + g(K) \ .$$

Man bemerke, daß $O(K)$ insbesondere für eine Untergruppe K mit der „Gruppenordnung" zusammenfällt. Es ist auch klar, daß für irgendzwei Untergruppen H, K jede der Aussagen[6])

$$H \subseteqq K \ , \qquad O(H) \rfloor O(K) \ , \qquad g(H) \leqq g(K) \ ,$$

die nachstehende impliziert.

§ 3. Primsimplexe

Das Simplex (1) dürfen wir nunmehr auch als

$$[\alpha]_e = 1 + \alpha + \cdots + \alpha^{e-1} \tag{6}$$

schreiben. Neben (6) werden auch noch die Komplexe (gleich additiv geschrieben)

$$1 - \alpha \qquad (\alpha \neq 1) \tag{7}$$

eine Führerrolle spielen, weshalb wir (7) auch ein *Simplex* nennen. (Dabei sind (6) und (7) zugleich die Normalformen aller Simplexe.)

Unter einem *Primsimplex* verstehen wir ein Simplex, dessen Gliederzahl eine Primzahl ist[7]). Das sind die (6) mit einer Primzahl $e = p$ und alle (7). Entsprechend ist die Ordnung gleich p oder 0 (zufällig ebenso wie die möglichen Körpercharakteristiken). Übrigens entstehen die Primsimplexe auch so, daß man aus den Polynomen $1 - x^p$ die irreduziblen Faktoren $1 + x + \cdots + x^{p-1}$, $1 - x$ bildet, und $x = \alpha$ einsetzt.

---

[5]) Es gilt auch $O(H + K) = O(H) + O(K)$, wovon wir aber keinen Gebrauch machen werden.

[6]) Es bezeichne „$a \rfloor b$" und „$a \lfloor b$": „a Teiler von b" bzw. „a Vielfaches von b". (Die kleine Schräge in den „$\rfloor$, $\lfloor$" richtet sich stets nach dem Teiler hin.)

[7]) Die Benennung „Primsimplex" soll keine Teilbarkeitseigenschaft suggerieren. Es ist übrigens klar, daß alle Simplexe und Untergruppen ($\neq 1$) Nullteiler in (G) sind.

Für beliebige Simplexe folgt aus (6), (7) sofort:

$$[\alpha]_{ef} = [\alpha]_e[\alpha^e]_f \qquad (e, f \geqq 2) , \tag{8}$$

$$[\alpha]_e(1 - \alpha) = 1 - \alpha^e . \tag{9}$$

Zur Gültigkeit von (8) muß bemerkt werden, daß mit der linken Seite zusammen stets auch die Faktoren der rechten Seite aus verschiedenen Gliedern bestehen und folglich mit ihr zusammen auch Simplexe sind.

§ 4. Reduktion des Satzes von Hajós auf den Fall von Primsimplexzerlegungen

Wir nennen (2) eine Primsimplexzerlegung von G, wenn alle Faktoren $[\alpha_i]$ Primsimplexe sind, und beweisen folgendes:

Ist der Satz von Hajós für Primsimplexzerlegungen richtig, so ist er allgemein richtig.

Betrachten wir nämlich eine beliebige Simplexzerlegung (2) von G. Aus (8) folgt sofort, daß jedes Simplex $[\alpha]$ sich in ein Produkt von Primsimplexen $[\beta]$ zerlegen läßt. Ersetzen wir jeden Faktor $[\alpha_i]$ in (2) durch ein solches (ihm gleiches) Produkt. So entsteht eine Primsimplexzerlegung von G, in der nach der Voraussetzung mindestens ein Faktor eine Gruppe sein muß. Folglich ist mindestens ein Faktor auch in der ursprünglich vorgelegten Gleichung (2) eine Gruppe und somit unsere Behauptung richtig, wenn folgendes gilt:

Ist in einer Gleichung

$$[\alpha]_e = K[\beta]_f \tag{10}$$

der Faktor $[\beta]_f$ *eine Gruppe, so muß auch* $[\alpha]_e$ *eine Gruppe sein.*

Um dies zu beweisen, bemerken wir, daß $\beta^f = 1$ gilt. Wenn wir also (10) zuerst mit $1 - \beta$, dann mit $1 - \alpha$ multiplizieren, so entsteht nach (9):

$$[\alpha]_e(1 - \beta) = 0 , \qquad (1 - \alpha^e)(1 - \beta) = 0 , \qquad \beta + \alpha^e = 1 + \alpha^e\beta .$$

Wegen $\beta \neq 1$ ergibt die letzte Gleichung sofort $\alpha^e = 1$. Dies bedeutet eben, daß $[\alpha]_e$ eine Gruppe ist, womit wir alles bewiesen haben.

§ 5. Weitere Vorbereitungen zum Beweis des Satzes von Hajós

Wegen der eben erfolgten Reduktion werden wir es im folgenden unter allen Simplexen nur noch mit den Primsimplexen $[\alpha] = [\alpha]_p$, $1 - \alpha$ zu tun haben. Für diese führen wir auch eine (stark abgekürzte) gemeinsame Bezeichnung ein, die uns sehr gute Dienste leisten wird. Und zwar erklären wir das (mehrdeutige) Symbol $\overline{\alpha}$ so, daß dies stets ein bestimmtes aller Primsimplexe $[\alpha]_p$, $1 - \alpha$ bezeichnen soll. (Dabei ist stets $\alpha \neq 1$ und p eine Primzahl, die die Ordnung von α nicht übertrifft.)

Ferner führen wir die wichtige Bezeichnung $\{H, \ldots, K\}$ ein, und verstehen darunter die durch die Elemente von $H, \ldots, K$ erzeugte Untergruppe von G; dabei soll stets $H, \ldots, K \neq 0$ sein. (Selbstverständlich dürfen einige der $H, \ldots, K$ auch Elemente von G sein, denn diese sind zugleich eingliedrige Komplexe.)

Für $O(\{\})$ und $g(\{\})$ schreiben wir kurz $O\{\}$ und $g\{\}$; beide sind scharf von $O(\,)$ und $g(\,)$ zu unterscheiden.

Sofort sieht man die Richtigkeit der folgenden Formeln ein:

$$\{H, \ldots, K\} = \big\{\{H\}, \ldots, \{K\}\big\} \qquad (H, \ldots, K \neq 0)\ , \tag{11}$$

$$\{H \ldots K\} \subseteqq \{H, \ldots, K\} \qquad (H \ldots K \neq 0)\ , \tag{12}$$

$$\{\overline{\alpha}\} = \{\alpha\}\ . \tag{13}$$

Aus (11), (13) folgt auch

$$\{K, \overline{\alpha}_1, \ldots, \overline{\alpha}_r\} = \{K, \alpha_1, \ldots, \alpha_r\} \qquad (K \neq 0)\ . \tag{14}$$

Wir zeigen noch die folgende Formel

$$g\{K, \alpha_1, \ldots, \alpha_r\} - g\{K, \alpha_1, \ldots, \alpha_k\} \\ \leqq g\{K \overline{\alpha}_1 \ldots \overline{\alpha}_k, \alpha_{k+1}, \ldots, \alpha_r\} - g\{K \overline{\alpha}_1 \ldots \overline{\alpha}_k\}\ , \tag{15}$$

wobei $K \overline{\alpha}_1 \ldots \overline{\alpha}_k \neq 0$ gelten soll.

Offenbar gilt nämlich für beliebige Untergruppen H_1, H_2 mit $H_1 \supseteqq H_2$:

$$O\{H_1, \omega_1, \ldots, \omega_t\}/O(H_1) \mid O\{H_2, \omega_1, \ldots, \omega_t\}/O(H_2)\ .$$

Hieraus folgt

$$g\{H_1, \omega_1, \ldots, \omega_t\} - g(H_1) \leqq g\{H_2, \omega_1, \ldots, \omega_t\} - g(H_2)\ .$$

Wegen (12) kann man dies mit

$$H_1 = \{K, \alpha_1, \ldots, \alpha_k\}\ , \qquad H_2 = \{K\,\overline{\alpha}_1 \ldots \overline{\alpha}_k\}$$

anwenden. Setzt man gleichzeitig auch noch $\alpha_{k+1}, \ldots, \alpha_r$ für $\omega_1, \ldots, \omega_t$ ein, so entsteht (wegen (11)) die Formel (15).

§ 6. Ein Hilfssatz über die Gleichung $K\overline{\alpha}_1 \ldots \overline{\alpha}_r = 0$

Betrachten wir ein Produkt $\overline{\alpha}_1 \ldots \overline{\alpha}_r$ $(\neq 0)$ von Primsimplexen. Ist dann K ein Komplex, so kann das Produkt $K\,\overline{\alpha}_1 \ldots \overline{\alpha}_r$ unter Umständen 0 oder eine Untergruppe von G sein (die zweite Möglichkeit kann selbstverständlich nur für $K\,\overline{\alpha}_1 \ldots \overline{\alpha}_r = K[\alpha_1] \ldots [\alpha_r]$ eintreten, d. h. kein $\overline{\alpha}_i = 1 - \alpha_i$ kann dabei vorliegen). Über diese Probleme enthält der folgende Hilfssatz 1 bzw. der Hilfssatz 2 im § 7 je eine Aussage, die der Form nach sehr ähnlich sind, sich aber sehr verschiedenartig beweisen lassen werden. Beide Hilfssätze geben dann im § 8 den Beweis des Satzes von Hajós in die Hand.

Hilfssatz 1. *Gilt eine Gleichung*

$$K\,\overline{\alpha}_1 \ldots \overline{\alpha}_r = 0 \qquad (r \geqq 1) \tag{16}$$

und läßt sich hier (ohne Zerstörung der Gleichheit) kein Faktor $\overline{\alpha}_i$ streichen, so gilt

$$g\{K, \alpha_1, \ldots, \alpha_r\} - g\{K\} < r\ . \tag{17}$$

Den Beweis fangen wir mit dem Fall $r = 1$ an. Jetzt haben wir $g\{K, \alpha_1\} = g\{K\}$, d. h. $\alpha_1 \in \{K\}$ zu zeigen. Ist zuerst $\overline{\alpha}_1 = 1 - \alpha_1$, so lautet (16) als $K\alpha_1 = K$, und so gibt es eine Gleichung $\beta\alpha_1 = \gamma$ $(\beta, \gamma \in K)$, woraus in der Tat $\alpha_1 \in \{K\}$ folgt. Dann sei $\overline{\alpha}_1 = [\alpha_1]_p$ $(p = \text{Primzahl})$. Aus (16) und (9) folgt $K(1 - \alpha_1^p) = 0$, und so gilt wegen des vorigen gewiß

$$\alpha_1^p \in \{K\}\ . \tag{18}$$

Andererseits läßt sich (16) auch als $K(\alpha_1 + \cdots \alpha_1^{p-1}) = -K$ schreiben, und so gibt es eine Gleichung $\beta\,\alpha_1^i = \gamma$ $(\beta, \gamma \in K;\ 1 \leqq i \leqq p-1)$. Hieraus folgt $\alpha_1^i \in \{K\}$. Dies und (18) ergeben wieder $\alpha_1 \in \{K\}$, und so ist Hilfssatz 1 für $r = 1$ richtig.

Im übrigen Teil des Beweises machen wir einen Induktionsschluß nach

$$g\{\alpha_1\} + \cdots + g\{\alpha_r\}\ . \tag{19}$$

Ist (19) gleich 1, so muß $r = 1$ sein, und so ist dies ein eben erledigter Fall. Nachher sei (19) größer als 1 und es werde die Richtigkeit von Hilfssatz 1 für die „kleineren" Werte von (19) vorausgesetzt. Nach (16) gilt

$$(K\,\overline{\alpha}_1 \ldots \overline{\alpha}_k)\,\overline{\alpha}_{k+1} \ldots \overline{\alpha}_r = 0 \qquad (1 \leqq k \leqq r-1)\ , \tag{20}$$

und hier läßt sich kein Faktor $\overline{\alpha}_{k+1}, \ldots, \overline{\alpha}_r$ streichen. Die Anwendung von Hilfssatz 1 auf (20) ergibt

$$g\{K\,\overline{\alpha}_1 \ldots \overline{\alpha}_k, \alpha_{k+1}, \ldots, \alpha_r\} - g\{K\,\overline{\alpha}_1 \ldots \overline{\alpha}_k\} < r - k\ .$$

Wegen (15) gilt noch mehr

$$g\{K, \alpha_1, \ldots, \alpha_r\} - g\{K, \alpha_1, \ldots, \alpha_k\} < r - k \qquad (1 \leqq k \leqq r-1)\ . \tag{21}$$

Sind zunächst alle Glieder von (19) gleich 1, so gilt offenbar

$$g\{K, \alpha_1, \ldots, \alpha_{r-1}\} - g\{K\} \leqq r - 1\ .$$

Addiert man hierzu den Fall $k = r - 1$ von (21), so entsteht eben (17).

Im restlichen Fall darf $g\{\alpha_r\} \geqq 2$ angenommen werden. Hieraus folgt mit höchstens zweimaliger Anwendung von (9), daß $\overline{\alpha}_r$ in beiden Fällen $\overline{\alpha}_r = [\alpha_r]_p$, $1 - \alpha_r$ mit einem passenden Faktor multipliziert in ein Primsimplex $1 - \beta$ übergeht, wofür

$$1 \leqq g\{\beta\} = g\{\alpha_r\} - 1 \qquad (\beta = \alpha_r^c) \tag{22}$$

gilt. Da (16) bei Ersetzung von $\overline{\alpha}_r$ durch $1 - \beta$ noch mehr richtig ist, so gewinnt man nach Streichung einiger Faktoren und Umnumerierung der $\alpha_1, \ldots, \alpha_{r-1}$ eine Gleichung

$$K\,\overline{\alpha}_1 \ldots \overline{\alpha}_l (1 - \beta) = 0 \qquad (0 \leqq l \leqq r-1)\ , \tag{23}$$

in der sich nunmehr kein Faktor $\overline{\alpha}_i$ streichen läßt. Wegen der Annahme über (16) läßt sich $1 - \beta$ auch nicht streichen. Zu (23) gehört wegen (22) ein „kleinerer" Wert von (19), und so folgt aus der Voraussetzung

$$g\{K, \alpha_1, \ldots, \alpha_l, \beta\} - g\{K\} \leqq l\ . \tag{24}$$

Zuerst sei $l = 0$. Aus (24), (22) folgt $g\{K, \alpha_r\} - g\{K\} \leqq 1$, dies und Fall $k = 1$ von (21) ergeben (17). Dann sei $1 \leqq l \leqq r - 1$. Nach Weglassen von β gilt (24) noch mehr. Wenn noch der Fall $k = l$ von (21) addiert wird, so entsteht wieder (17), womit Hilfssatz 1 bewiesen ist.

§ 7. Ein Hilfssatz über die Untergruppen von der Form $K[\alpha_1]\ldots[\alpha_r]$

Hilfssatz 2 [8]). *Ist das Produkt* $K[\alpha_1]\ldots[\alpha_r]$ *von einem* K (>0) *und den Primsimplexen* $[\alpha_1],\ldots,[\alpha_r]$ *eine Gruppe, selbst* K *aber keine Gruppe, so gilt*

$$g\{K,\alpha_1,\ldots,\alpha_r\} - g\{K\} < r\ . \tag{25}$$

Zuerst zeigen wir

$$K[\alpha_1]\ldots[\alpha_r] = \{K,\alpha_1,\ldots,\alpha_r\}\ . \tag{26}$$

Hierzu nehme man ein $\beta \in K$. Da die linke Seite von (26) die Elemente $\beta, \beta\alpha_i$ also auch α_i $(i = 1,\ldots,r)$ enthält, so ist (26) mit „$\supseteqq$" (statt „$=$") richtig. Andererseits ist (26) mit „$\subseteqq$", und so auch mit „$=$" richtig.

Multipliziert man (26) mit $\{K\}$, so folgt aus $\{K\}K = O(K)\{K\}$:

$$O(K)\{K\}[\alpha_1]\ldots[\alpha_r] = O\{K\}\{K,\alpha_1,\ldots,\alpha_r\}\ .$$

Dies ergibt $O(K) \mid O\{K\}$ also

$$\{K\}[\alpha_1]\ldots[\alpha_r] = a\{K,\alpha_1,\ldots,\alpha_r\} \qquad (a>0)\ . \tag{27}$$

Wegen der Annahme haben alle Elemente von K die Multiplizität 1, und so gilt wegen $K \neq \{K\}$ gewiß $O(K) < O\{K\}$. Dies und (26), (27) ergeben $a > 1$, also nach (27)

$$g\{K\} + r > g\{K,\alpha_1,\ldots,\alpha_r\}\ .$$

Hiermit haben wir Hilfssatz 2 bewiesen.

§ 8. Beweis des Satzes von Hajós

Nunmehr beweisen wir Hajós' Satz. Wegen § 4 genügt es zu zeigen, daß in jeder Primsimplexzerlegung

$$G = [\alpha_1]\ldots[\alpha_r] \qquad (r \geqq 1) \tag{28}$$

von G mindestens ein Faktor eine Gruppe ist.

Im Fall $r = 1$ ist das richtig. Im Fall $r > 1$ setzen wir das für die „kleineren" r voraus und nehmen an, daß gegen die Behauptung kein $[\alpha_i]$ eine Gruppe ist. Aus (28) folgen sofort

$$g(G) = r\ , \tag{29}$$

$$G = \{\alpha_1,\ldots,\alpha_r\}\ . \tag{30}$$

---

[8]) Obiger Hilfssatz würde seine Gültigkeit auch ohne die Annahme $K > 0$ behalten (s. *Hajós*[1]), Satz 29).

Wird (28) mit $1 - \alpha_r$ multipliziert, so entsteht links 0, folglich gilt nach (9)

$$[\alpha_1]\ldots[\alpha_{r-1}](1 - \alpha_r^p) = 0 \ , \tag{31}$$

wobei die Primzahl p die Gliederzahl von $[\alpha_r]$ bezeichnet. Wegen der Annahme ist der letzte Faktor in (31) $\neq 0$, und so gibt es bei passender Numerierung der $\alpha_1, \ldots, \alpha_{r-1}$ eine Gleichung

$$[\alpha_1]\ldots[\alpha_k](1 - \alpha_r^p) = 0 \qquad (1 \leqq k \leqq r - 1) \ , \tag{32}$$

in der sich kein Faktor streichen läßt.

Wenden wir auf (32) Hilfssatz 1 (mit $K = 1$, $r = k + 1$) an:

$$g\{\alpha_1, \ldots, \alpha_k, \alpha_r^p\} < k + 1 \ .$$

Noch mehr gilt dann

$$g\{\alpha_1, \ldots, \alpha_k\} \leqq k \ . \tag{33}$$

$K = [\alpha_1]\ldots[\alpha_k]$ ist keine Gruppe, denn dann müßte wegen $1 \leqq k \leqq r - 1$ nach der Voraussetzung ein Faktor $[\alpha_i]$ eine Gruppe sein, was falsch ist. Andererseits ist $K[\alpha_{k+1}]\ldots[\alpha_r]$ nach (28) eine Gruppe, und so folgt aus Hilfssatz 2:

$$g\{[\alpha_1]\ldots[\alpha_k], \alpha_{k+1}, \ldots, \alpha_r\} - g\{[\alpha_1]\ldots[\alpha_k]\} < r - k \ .$$

Die Anwendung von (15) ergibt

$$g\{\alpha_1, \ldots, \alpha_r\} - g\{\alpha_1, \ldots, \alpha_k\} < r - k \ .$$

Dies zu (33) addiert ergibt nach (30) $g(G) < r$. Dies widerspricht (29), womit wir den Satz von Hajós bewiesen haben.

(Eingegangen den 4. Oktober 1948.)