# EIN BEITRAG ZUM PROBLEM DER FAKTORISATION VON ENDLICHEN ABELSCHEN GRUPPEN

Von

L. RÉDEI (Szeged), korrespondierendem Mitglied der Akademie

## § 1. Einleitung

Für eine endliche Abelsche Gruppe $\mathfrak{G}$ ist es ein interessantes, aber schwieriges Problem, eine Übersicht über die möglichen Faktorisationen

$$\mathfrak{G} = \mathfrak{R}_1 \dots \mathfrak{R}_l \tag{1}$$

von $\mathfrak{G}$ zu gewinnen, wobei die $\mathfrak{R}_i$ Komplexe (Teilmengen) von $\mathfrak{G}$ sind; diese Gleichung soll bedeuten, dass sich jedes Element von $\mathfrak{G}$ genau einmal in der Form $A_1 \dots A_l$ $(A_i \in \mathfrak{R}_i)$ darstellen lässt. Die Faktorisation (1) nennen wir echt, wenn jeder Faktor $\mathfrak{R}_i$ aus mindestens zwei Elementen besteht.

Das bisher Gesagte soll für spätere Zwecke auch im allgemeineren Fall gelten, wenn in (1) statt $\mathfrak{G}$ ein Komplex $\mathfrak{R}$ steht. Für zwei Komplexe $\mathfrak{A}$, $\mathfrak{B}$ sagen wir, dass $\mathfrak{A}$ ein Teiler von $\mathfrak{B}$ ist, in Zeichen $\mathfrak{A} \mid \mathfrak{B}$, wenn es eine Faktorisation $\mathfrak{B} = \mathfrak{A}\mathfrak{C}$ gibt.

Wenn in (1) die besondere Annahme $\mathfrak{R}_i = 1,\ A_i, \dots, A_i^{e_i}$ $(i = 1, \dots, l)$ gemacht wird, so hat man die Beantwortung im berühmten Satz von HAJÓS [1][1], nach dem dann in (1) mindestens ein $\mathfrak{R}_i$ eine Gruppe sein muss. Verfasser [5] hat dem Satz eine verschärfte Formulierung gegeben, nach der alle möglichen HAJÓS'schen Faktorisationen von $\mathfrak{G}$ sich angeben lassen. Vereinfachungen des Beweises von HAJÓS finden sich bei Verfasser [4] und SZELE [6].

Im allgemeinen Fall kann (1) gelten, ohne dass ein $\mathfrak{R}_i$ durch eine Gruppe $(\neq 1)$ teilbar wäre, wofür ebenfalls HAJÓS das erste Beispiel gab, das mit seiner freundlichen Erlaubnis Verfasser [2] veröffentlicht hat. Daselbst hat Verfasser auf verhältnismässig sehr kompliziertem Wege den kleinen Satz bewiesen, dass in jeder echten Faktorisation (1) einer nichtzyklischen Gruppe $\mathfrak{G}$ von Primzahlquadratordnung (Fall $l = 2$) das eine von $\mathfrak{R}_1, \mathfrak{R}_2$ durch eine Gruppe $(\neq 1)$ teilbar ist.

Im folgenden betrachten wir nur den verhältnismässig sehr einfachen Spezialfall von (1), dass $\mathfrak{G}$ zyklisch und $l = 2$ ist. Früher hat HAJÓS nach seiner mündlichen Mitteilung vermutet, dass dann in jeder echten Faktorisation (1)

[1] Die [ ] beziehen sich auf das Literaturverzeichnis am Ende der Arbeit.

das eine von $\mathfrak{N}_1$, $\mathfrak{N}_2$ durch eine Gruppe ($\neq 1$) teilbar sein muss ; vor kurzem aber hat er seine Vermutung widerlegt. Und zwar gelang ihm das für alle $\mathfrak{G}$, ausgenommen die Ordnungszahlen von der Form

$$p^e q^f, p^e qr, pqrs \qquad (e, f \geqq 0), \tag{2}$$

wobei $p$, $q$, $r$, $s$ verschiedene Primzahlen bezeichnen ; seine Arbeit darüber erscheint in diesen Acta.[2] Die restlichen Ordnungszahlen (2) sind bei ihm fraglich geblieben, aber ich habe schon im Jahre 1945 bewiesen, dass insbesondere $pqr$ tatsächlich ein Ausnahmefall ist. Wohl ist mein Beweis interessant, trotzdem wollte ich ihn wegen seiner Mühsamkeit nicht publizieren. Ich tue das jetzt wegen der durch die HAJÓS'schen Untersuchungen erhöhten Aktualität meines an sich sehr bescheidenen Resultats, das nämlich nunmehr auch zeigt, dass das Resultat von HAJÓS «beinahe» scharf ist.

Zum Beweis werden wir länger ausholen müssen, so dass wir eine Methode ausarbeiten, die zur Untersuchung aller Faktorisationen $\mathfrak{G} = \mathfrak{N}_1 \mathfrak{N}_2$ von beliebigen endlichen zyklischen Gruppen geeignet zu sein scheint ; trotzdem konnten wir auf diesem Wege nicht alle kritischen Ordnungszahlen (2) erledigen. Ausser dem gesagten Fall $pqr$ konnten wir nur noch die sehr leichten Fälle $p^e, pq$ mit ähnlichem Resultat beantworten. Endgültig formulieren wir unsere Behauptung im folgenden :

SATZ. *Eine zyklische Gruppe von einer der Ordnungen $p^e, pq, pqr$ ($p, q, r$ verschiedene Primzahlen) lässt sich nur so in das Produkt von zwei Komplexen mit je mindestens zwei Elementen faktorisieren, wenn einer der Faktoren durch eine Gruppe ($\neq 1$) teilbar ist.*

Ich will noch kurz betonen, dass die Faktorisationsprobleme aller Art von Abelschen Gruppen im allgemeinen nicht nur an sich, sondern auch in ihren Zusammenhängen interessant sind, weshalb es sich lohnt, ihnen eine grosse Aufmerksamkeit zu widmen. Z. B. kommt (1) für zyklische $\mathfrak{G}$ dem folgenden additiv-zahlentheoretischen Problem gleich : Es sind auf jede mögliche Art $l$ Mengen $M_1, \ldots, M_l$ von ganzen Zahlen anzugeben, so dass $x_1 + \ldots + x_l$ ($x_i \in M_i$) ein volles Restsystem mod $m$ durchläuft. Der anfangs erwähnte Satz von HAJÓS ist eine Äquivalente der Vermutung von MINKOWSKI über lineare Ungleichungen (vgl. auch RÉDEI [3]). Verfassers [2] erwähnter Satz über die Gruppen von Primzahlquadratordnung steht mit einer dort bewiesenen Maximaleigenschaft der Gaussischen Summen im engsten Zusammenhang.

[2] G. HAJÓS, Sur le problème de factorisation des groupes cycliques, *Acta Math. Hung.*, 1 (1950), S. 189—195.

## § 2. Vorbereitungen

Durchwegs bezeichne $\mathfrak{G}$ eine zyklische Gruppe von der Ordnung $O(\mathfrak{G}) = n$ $(> 1)$ mit einem erzeugenden Element $A$.

Als Polynome der Unbestimmten $x$ werden stets nur solche mit ganzen rationalen Koeffizienten zugelassen. Ein Polynom $f(x)$ $(\not\equiv 0)$ mit lauter Koeffizienten $\geqq 0$ nennen wir positiv und schreiben hierfür $f(x) > 0$. Insbesondere werden die positiven Polynome von der Form

$$f(x) = x^{i_1} + \ldots + x^{i_t} \qquad (i_u \not\equiv i_v \pmod{n} \text{ für } u \neq v)$$

eine grosse Rolle spielen; diese nennen wir elementar (für $n$). Zwei positive Polynome $f(x)$, $g(x)$ mit $f(x) \equiv g(x) \pmod{x^n - 1}$ können nur gleichzeitig elementar sein. Dann sind ihre Gliederzahlen gleich und die in ihnen vorkommenden Exponenten paarweise kongruent mod $n$ .

Das $n$-te Kreisteilungspolynom wird mit $F_n(x)$ bezeichnet, hierfür gilt bekanntlich

$$x^n - 1 = \prod_{d|n} F_d(x), \tag{2}$$

woraus

$$F_n(x) = \prod_{d|n} (x^d - 1)^{\mu(n/d)} \tag{3}$$

folgt; $\mu$ bezeichnet die Funktion von Möbius. Von (3) liest man die bekannten Formeln ab:

$$F_n(1) = \begin{cases} p, \text{ wenn } n = p^e\ (> 1) \text{ ist,} \\ 1, \text{ wenn } n\ (> 1) \text{ keine Primzahlpotenz ist.} \end{cases} \tag{4}$$

Nach (2) gilt

$$1 + x + \ldots + x^{n-1} = \prod_{\substack{d|n \\ d>1}} F_d(x). \tag{5}$$

Stets bezeichnen $\Phi_1(x), \Phi_2(x)$ zwei Polynome mit

$$1 + x + \ldots + x^{n-1} = \Phi_1(x)\, \Phi_2(x), \tag{6}$$

$$\Phi_1(1),\ \Phi_2(1) > 0\,. \tag{7}$$

Da die $F_d(x)$ irreduzibel sind und nach (4) $F_d(1) > 0$ $(d > 1)$ gilt, lassen sich die $\Phi_1(x), \Phi_2(x)$ so gewinnen, dass man die $F_d(x)$ in (5) beliebig in zwei Klassen einteilt und für beide Klassen das Produkt der Elemente bildet. Kurz nennen wir die $\Phi_1(x), \Phi_2(x)$ komplementäre Teiler von $1 + x + \ldots + x^{n-1}$.

Einem beliebigen Komplex

$$\mathfrak{K} = A^{i_1} + \ldots + A^{i_t} \tag{8}$$

ordnen wir das Polynom

$$\mathfrak{K}(x) = x^{i_1} + \ldots + x^{i_t} \tag{9}$$

zu. Dieses ist elementar und mod $x^n - 1$ eindeutig bestimmt. Umgekehrt gehört dann zu jedem für $n$ elementaren Polynom $f(x)$ ein einziger Komplex $\mathfrak{K}$, so dass $f(x) = \mathfrak{K}(x)$ gilt.

Insbesondere gilt

$$\mathfrak{G}(x) = 1 + x + \ldots + x^{n-1}. \tag{10}$$

Allgemeiner gilt offenbar folgendes: Ein Komplex $\mathfrak{K}$ ist dann und nur dann eine Untergruppe ($\neq 1$) von $\mathfrak{G}$, wenn

$$\mathfrak{K}(x) = 1 + x^d + \ldots + x^{n-d} = \frac{x^n - 1}{x^d - 1} \qquad (d \mid n,\ d \neq n). \tag{11}$$

Trivial ist auch der folgende

HILFSSATZ 1. *Für drei Komplexe* $\mathfrak{K}$, $\mathfrak{K}_1$, $\mathfrak{K}_2$ *ist*

$$\mathfrak{K} = \mathfrak{K}_1\, \mathfrak{K}_2 \tag{12}$$

*gleichbedeutend mit*

$$\mathfrak{K}(x) \equiv \mathfrak{K}_1(x)\, \mathfrak{K}_2(x) \pmod{x^n - 1}. \tag{13}$$

Wir beweisen:

HILFSSATZ 2. *Ein Komplex* $\mathfrak{K}$ *ist dann und nur dann durch eine Gruppe* ($\neq 1$) *teilbar, wenn es ein* $d$ *mit*

$$\frac{x^n - 1}{x^d - 1} \,\Big|\, \mathfrak{K}(x) \qquad (d \mid n,\ d \neq n)$$

*gibt.*

Die angeschriebene Teilbarkeit ist nämlich gleichbedeutend mit der Erfüllbarkeit von

$$\mathfrak{K}(x) \equiv \frac{x^n - 1}{x^d - 1} f(x) \pmod{x^n - 1}$$

durch ein Polynom $f(x)$. Dessen Grad darf $< d$ angenommen werden und dann ist $f(x)$ mit $\mathfrak{K}(x)$ zusammen (vgl. (11)) notwendig elementar für $n$. Hiernach und nach Hilfssatz 1 ist Hilfssatz 2 richtig.

Wir beweisen den folgenden

HILFSSATZ 3. *Alle Faktorisationen*

$$\mathfrak{G} = \mathfrak{K}_1\, \mathfrak{K}_2 \tag{14}$$

*von* $\mathfrak{G}$ *gewinnt man so, dass man zwei komplementäre Teiler* $\Phi_1(x)$, $\Phi_2(x)$ *von* $1 + x + \ldots + x^{n-1}$ *nimmt (definiert durch* (6), (7)*) und nach zwei Polynomen* $f_1(x), f_2(x)$ *mit*

$$\Phi_1(x) f_1(x),\ \Phi_2(x) f_2(x) > 0, \tag{15}$$

$$f_1(1) = f_2(1) = 1 \tag{16}$$

*sucht, dann sind die zwei Produkte in* (15) *elementar (für n), somit gibt es zwei Komplexe* $\mathfrak{R}_1$, $\mathfrak{R}_2$ *mit*

$$\mathfrak{R}_1(x) = \Phi_1(x) f_1(x), \quad \mathfrak{R}_2(x) = \Phi_2(x) f_2(x) \; ; \tag{17}$$

*diese* $\mathfrak{R}_1$, $\mathfrak{R}_2$ *sind die sämtlichen Lösungen von* (14). *Dabei genügt es, sich auf die* $f_1(x)$, $f_2(x)$ *zu beschränken, für die die Produkte in* (15) *vom Grade* $< n$ *sind.*

Setzen wir nämlich zunächts voraus, dass (14) gilt. Wegen Hilfssatz 1 und (10) gilt dann

$$1 + x + \ldots + x^{n-1} \equiv \mathfrak{R}_1(x)\, \mathfrak{R}_2(x) \pmod{x^n - 1}, \tag{18}$$

wobei man annehmen darf, dass $\mathfrak{R}_1(x)$, $\mathfrak{R}_2(x)$ vom Grade $< n$ sind. Aus (18) folgt, dass die linke Seite ein Teiler der rechten Seite ist, gewiss gibt es also nach (6) zwei komplementäre Teiler $\Phi_1(x)$, $\Phi_2(x)$ der linken Seite mit

$$\Phi_1(x) \mid \mathfrak{R}_1(x), \quad \Phi_2(x) \mid \mathfrak{R}_2(x). \tag{19}$$

Hiernach existieren zwei Polynome $f_1(x), f_2(x)$ mit (17). Hieraus und aus (18), (6) folgt

$$1 \equiv f_1(x) f_2(x) \pmod{x - 1}. \tag{20}$$

Dies ergibt $1 = f_1(1) f_2(1), f_1(1) = f_2(1) = \pm 1$. Andererseits gelten $\mathfrak{R}_1(1)$, $\mathfrak{R}_2(1) > 0$, und so folgt aus (17), (7) notwendig $f_1(1), f_2(1) > 0$. Dies mit dem vorigen zusammen ergibt (16). Nach (17) besteht auch (15), und dabei sind mit $\mathfrak{R}_1(x)$, $\mathfrak{R}_2(x)$ zusammen auch die Produkte in (15) vom Grade $< n$.

Wenn umgekehrt (6), (7), (15), (16) gelten, so schliesst man, wie folgt. Wegen (16) gilt (20). Dies und (6) ergeben

$$1 + x + \ldots + x^{n-1} \equiv \Phi_1(x) f_1(x) \Phi_2(x) f_2(x) \pmod{x^n - 1}. \tag{21}$$

Hieraus folgt, dass die zwei Produkte in (15) für $n$ elementar sind, d. h. durch (17) wirklich zwei Komplexe $\mathfrak{R}_1$, $\mathfrak{R}_2$ definiert werden. Nach (17) und (21) gilt (18), und dies mit (10) zusammen ergibt nach Hilfssatz 1 die Richtigkeit von (14). Wir haben Hilfssatz 3 bewiesen.

Hilfssatz 4. *Ein Polynom* $f(x)$ *ist dann und nur dann durch* $F_n(x)$ *teilbar, wenn*

$$f(x) = \sum_{p \mid n} \frac{x^n - 1}{x^{n/p} - 1} f_p(x) \tag{22}$$

*gilt, wobei die* $f_p(x)$ *Polynome mit ganzen Koeffizienten bezeichnen.*

Offenbar ist nämlich $F_n(x)$ der grösste gemeinsame Teiler der Polynome

$$\frac{x^n - 1}{x^{n/d} - 1} \qquad (d \mid n),$$

woraus die Behauptung folgt.

HILFSSATZ 5. *Man bezeichne mit $n_1, \ldots, n_t$ diejenigen maximalen Teiler von $n$, die je einen Primfaktor von $n$ nicht enthalten, wobei $t$ die Anzahl der verschiedenen Primfaktoren von $n$ ist. Für jedes ganzzahlige Polynom $f(x)$ gilt*

$$f(x) \equiv \sum_{i_1=0}^{\frac{n}{n_1}-1} \cdots \sum_{i_t=0}^{\frac{n}{n_t}-1} k_{i_1 \ldots i_t}\, x^{n_1 i_1 + \cdots + n_t i_t} \pmod{x^n - 1} \tag{23}$$

*mit eindeutig bestimmten ganzen Zahlen $k_{i_1} \ldots i_t$.*

Es gilt nämlich zunächst

$$f(x) \equiv \sum_{i=0}^{n-1} k_i x^i \pmod{x^n - 1} \tag{24}$$

mit eindeutig bestimmten ganzen $k_i$. Da ferner durch

$$i \equiv n_1 i_1 + \ldots + n_t i_t \pmod{n}$$

die $i$ in (24) und die Systeme $i_1, \ldots, i_t$ in (23) einander gegenseitig eindeutig bestimmen, so sieht man die Richtigkeit von Hilfssatz 5 ein.

## § 3. Beweis des Satzes

Um unseren Satz zu beweisen, betrachten wir eine echte Faktorisation (14) von $\mathfrak{G}$. Nach Hilfssatz 3 lassen sich dann (6), (7), (15), (16), (17) annehmen.

Vor allem zeigen wir, dass (anstatt (7) sogar)

$$\Phi_1(1)\ ,\ \Phi_2(1) > 1 \tag{25}$$

gilt. Andernfalls wäre wegen (7) z. B. $\Phi_1(1) = 1$, aber dann gilt nach (16), (17) $\mathfrak{R}_1(1) = 1$, also enthält $\mathfrak{R}_1$ nur ein Element, wobei doch (14) eine echte Faktorisation ist. Dieser Widerspruch beweist (25).

Aus (6) und (5) folgt ferner, dass das eine von $\Phi_1(x), \Phi_2(x)$ durch $F_n(x)$ teilbar ist, wir dürfen

$$F_n(x) \mid \Phi_1(x) \tag{26}$$

annehmen.

**Fall** $n = p^e$ . Dann lautet (26) so:

$$\frac{x^{p^e} - 1}{x^{p^{e-1}} - 1} \,\Big|\, \Phi_1(x)\ .$$

Dann ist die linke Seite nach (17) auch ein Teiler von $\mathfrak{R}_1(x)$, und so folgt aus Hilfssatz 2 die Richtigkeit des Satzes für diesen Fall.

Hiernach brauchen wir weiter nur noch die Fälle $n = pq, pqr$ zu betrachten. Wir schicken hiervon den weit schwierigeren zweiten Fall voran. Der Anfang des Beweises wird uns auch zeigen, wie man das Problem der Faktorisation auch für kompliziertere Ordnungszahlen $n$ angreifen könnte.

**Fall** $n = pqr$. Aus (26), $(17_1)$ folgt $F_n(x) \mid \mathfrak{R}_1(x)$. Dies ergibt wegen Hilfssatz 4:

$$\mathfrak{R}_1(x) = \frac{x^{pqr}-1}{x^{qr}-1} f_p(x) + \frac{x^{pqr}-1}{x^{pr}-1} f_q(x) + \frac{x^{pqr}-1}{x^{pq}-1} f_r(x) \tag{27}$$

mit passenden ganzzahligen Polynomen $f_p(x)$, $f_q(x)$, $f_r(x)$. Nach Hilfssatz 5 lässt sich

$$f_p(x) \equiv \sum_{j=0}^{q-1} \sum_{k=}^{r-1} a_{jk}\, q^{rj+qk} \pmod{x^{qr}-1} \tag{28}$$

mit passenden ganzen $a_{jk}$ setzen. Im Summand darf der Exponent durch $p$ multipliziert werden, denn das kommt bloss auf eine Umordnung der $a_{jk}$ an. Wird in (27) die rechte Seite des so veränderten (28) für $f_p(x)$ eingesetzt, so geht (27) in eine richtige Kongruenz mod $x^{pqr}-1$ über. Schreibt man gleichzeitig den Kofaktor von $f_p(x)$ in (27) als

$$\sum_{i=0}^{p-1} x^{qri},$$

so entsteht nach Ausmultiplizieren und entsprechender Behandlung des zweiten und dritten Gliedes der rechten Seite:

$$\mathfrak{R}_1(x) \equiv \sum_{i=0}^{p-1} \sum_{j=0}^{q-1} \sum_{k=1}^{r-1} g_{ijk}\, x^{qri+prj+pqk} \pmod{x^{pqr}-1} \tag{29}$$

mit

$$g_{ijk} = a_{jk} + b_{ik} + c_{ij} \; (i = 0,\ldots,p-1;\; j = 0,\ldots,q-1;\; k = 0,\ldots,r-1), \tag{30}$$

wobei alle Glieder der rechten Seite ganze Zahlen sind. Andererseits folgt aus (29) unmittelbar

$$g_{ijk} = 0 \text{ oder } 1\,. \tag{31}$$

(Wir bemerken: Der Sinn von (30) ist, dass die Funktion $g_{ijk}$ von drei Variabeln $i, j, k$ sich aus Funktionen von je zwei Variabeln zusammensetzt. Natürlich sind diese letzteren Funktionen noch nicht, erst ihre Summe eindeutig bestimmt.)

Bezüglich der Symbole $a_{jk}$, $b_{ik}$, $c_{ij}$, $g_{ijk}$ verwenden wir die Verkürzung in den Bezeichnungen, dass das Streichen einiger der Indizes die Ausführung der Summation bedeutet. Z. B.:

$$a_k = \sum_{j=0}^{q-1} a_{jk}, \quad g = \sum_{i=0}^{p-1} \sum_{j=0}^{q-1} \sum_{k=0}^{r-1} g_{ijk}\,. \tag{32}$$

Nunmehr wollen wir auch von (25) Gebrauch machen. Aus (6) folgt $\Phi_1(1)\,\Phi_2(1) = pqr$, also gilt nach (25) und nach (4), (5), (6) bei passender Bezeichnung der $p$, $q$, $r$

$$\Phi_1(1) = pq,\; \Phi_2(1) = r;\; F_p(x)\,F_q(x) \mid \Phi_1(x),\; F_r(x) \mid \Phi_2(x),$$

oder

$$\Phi_1(1) = p,\ \Phi_2(1) = qr\ ;\ F_p(x) \mid \Phi_1(x),\ F_q(x)\ F_r(x) \mid \Phi_2(x)\ .$$

Auf Grund von (17), (16) gilt in beiden Fällen dasselbe auch für $\mathfrak{R}_1$, $\mathfrak{R}_2$ statt $\Phi_1$, $\Phi_2$. Von allen diesen wird uns weiter nur der auf $\mathfrak{R}_1$ bezügliche Teil interessieren, der so lautet: Es gilt (bei passender Bezeichnung der $p, q, r$)

$$\mathfrak{R}_1(1) = pq, \qquad F_p(x)\ F_q(x) \mid \mathfrak{R}_1(x), \tag{33}$$

oder

$$\mathfrak{R}_1(1) = p, \quad F_p(x) \mid \mathfrak{R}_1(x). \tag{34}$$

*Erstens* betrachten wir den Fall (33). Nach (29), (32) gilt dann

$$g = pq. \tag{35}$$

Bezeichne $\alpha$ eine primitive $p$-te (komplexe) Einheitswurzel. Da nach (33) $F_p(x) \mid \mathfrak{R}_1(x)$, so gilt $\mathfrak{R}_1(\alpha) = 0$. Nach (29) ergibt dies

$$\sum_{i=0}^{p-1} g_i\, \alpha^{qri} = 0,$$

also $g_0 = \cdots = g_{p-1}$. Hieraus folgt nach (35)

$$g_i = q \qquad (i = 0, \ldots, p-1). \tag{36}$$

Dies schreibt sich nach (30) auch so:

$$a + qb_i + rc_i = q \qquad (i = 0, \ldots, p-1). \tag{37}$$

Hiernach hängt die Restklasse $b_i \pmod r$ von $i$ nicht ab. Ferner gilt nach (30)

$$g_{ij} = a_j + b_i + rc_{ij}\ , \tag{38}$$

somit hängt auch die Restklasse $g_{ij} \pmod r$ von $i$ nicht ab. Dann kann man

$$g_{ij} = u_j + rv_{ij} \qquad (0 \leqq u_j \leqq r-1) \tag{39}$$

setzen, mit ganzen $u_j$, $v_{ij}$. Ferner gilt wegen (31) gewiss

$$v_{ij} \geqq 0\,. \tag{40}$$

Wegen der Symmetrie von (33) in $p, q$ gilt ähnlich wie (36)

$$g_j = p\,.$$

Summiert man andererseits (39) nach $i$, so entsteht $g_j = pu_j + rv_j$ (wobei auch $v_j$ mit der bei (32) eingeführten Abkürzung zu verstehen ist). Beide ergeben

$$pu_j + rv_j = p.$$

Dashalb folgt aus (39), (40) notwendig $u_j = 1$, $v_j = 0$, $v_{ij} = 0$. Hiernach und nech (39) gilt

$$g_{ij} = 1\,. \tag{41}$$

Folglich schreibt sich (38) so:

$$1 = a_j + b_i + rc_{ij}. \tag{42}$$

Dies ergibt

$$c_{ij} = \frac{1-b_i}{r} - \frac{a_j}{r} = \left[\frac{1-b_i}{r}\right] - \left[\frac{a_j}{r}\right],$$

wobei $[z]$ die grösste ganze Zahl $\leqq z$ bezeichnet. Man setze dies in (30) ein:

$$g_{ijk} = \left(a_{jk} - \left[\frac{a_j}{r}\right]\right) + \left(b_{ik} + \left[\frac{1-b_i}{r}\right]\right).$$

Vergleicht man dies wieder mit (30), so ist ersichtlich, dass man von vornherein

$$c_{ij} = 0$$

setzen kann, so dass dann (mit veränderter Bezeichnung)

$$g_{ijk} = a_{jk} + b_{ik}, \tag{43}$$

ferner nach (42)

$$a_j + b_i = 1 \tag{44}$$

gilt.

Wegen (31) und (43) ist für jedes feste $k$ mindestens das eine von $a_{jk}$, $b_{ik}$ konstant. Ist für ein $k$ z. B. $a_{jk} = C$ konstant, so dürfen für dieses $k$ die $a_{jk}$, $b_{ik}$ von vornherein durch $a_{jk} - C$, $b_{ik} + C$ ersetzt werden, da dann (43) erhalten bleibt. So erreichen wir (wieder nach (31), (43)), dass die folgenden zwei Aussagen richtig sind:

*Für jedes feste $k$ gilt $a_{jk} = 0$ ($j$ beliebig) oder $b_{ik} = 0$ ($i$ beliebig).*

*Alle $a_{jk}$, $b_{ik}$ sind gleich* 0, *oder* 1.

Gibt es aber ein $a_{jk} = 1$ und auch ein $b_{ik'} = 1$ mit festen $i, j, k, k'$, so gilt für diese $i, j$ nach den eben erhaltenen Feststellungen $a_j \geqq 1$, $b_i \geqq 1$, $a_j + b_i \geqq 2$. Dies verstösst gegen (44), folglich muss unbeschränkt $a_{jk} = 0$, oder unbeschränkt $b_{ik} = 0$ gelten. Wegen Symmetrie dürfen wir letzteres annehmen, und dann gilt nach (43) einfach $g_{ijk} = a_{jk}$. Hieraus folgt nach (29) bei Summieren über die $i$

$$\frac{x^{pqr}-1}{x^{qr}-1} \Big| \mathfrak{R}_1(x),$$

und so ist unser Satz nach Hilfssatz 2 für diesen Fall richtig.

*Zweitens* betrachten wir den Fall (34). Ähnlich wie (35), (36), folgen jetzt

$$g = p, \tag{45}$$

$$g_i = 1 \qquad (i = 0, \ldots, p-1). \tag{46}$$

Dies schreibt sich nach (30) so:

$$a + qb_i + rc_i = 1.$$

Hiernach hängt die Restklasse $b_i \pmod r$ nicht von $i$ ab, weswegen man wieder (39) ansetzen kann, und dabei gilt wegen (31) auch (40). Andererseits gilt nach (31), (46) stets $g_{ij} = 0$ oder 1, und dann folgt aus (39), (40) $v_{ij} = 0$,

$$g_{ij} = u_j = 0 \text{ oder } 1 .$$

Nach diesem und (30) gilt

$$u_j = a_j + b_i + rc_{ij} .$$

Dies ergibt

$$c_{ij} = \frac{u_j - a_j}{r} - \frac{b_i}{r} = \left[\frac{u_j - a_j}{r}\right] - \left[\frac{b_i}{r}\right] .$$

Durch Einsetzen in (30) folgt wieder, dass von vornherein $c_{ij} = 0$ gesetzt werden darf, und dann gilt auch (43). Dies ergibt

$$g_{ik} = a_k + q\, b_{ik} .$$

Andererseits gilt nach (31), (46) $g_{ik} = 0$ oder 1, folglich kann $b_{ik}$ von $i$ nicht abhängen. Nach (43) hängt dann $g_{ijk}$ von $i$ auch nicht ab, d. h. man darf von vornherein $g_{ijk} = a_{jk}$ setzen, womit wir zum selben Schluss gekommen sind wie vorher. Wir haben den Satz für $n = pqr$ bewiesen.

**Fall** $n = pq$ . Mit ähnlichem Schluss wie vor (33), (34) sieht man sofort ein, dass jetzt bei passender Bezeichnung der $p, q$ wegen (26)

$$\Phi_1(x) = F_{pq}(x)\, F_p(x) = \frac{x^{pq} - 1}{x^q - 1}$$

gilt. Dies ergibt nach (17)

$$\frac{x^{pq} - 1}{x^q - 1} \;\Big|\; \mathfrak{R}_1(x) ,$$

woraus nach Hilfssatz 2 die Richtigkeit des Satzes auch jetzt folgt. Wir haben den Satz in allen Fällen bewiesen.

*(Eingegangen am 1. August 1950.)*

## Literaturverzeichnis

[1] G. HAJÓS, Über einfache und mehrfache Bedeckung des $n$-dimensionalen Raumes mit einem Würfelgitter, *Math. Zeitschrift*, **47** (1941), S. 427—467.

[2] L. RÉDEI, Zwei Lückensätze über Polynome in endlichen Primkörpern mit Anwendung auf die endlichen Abelschen Gruppen und die Gaussischen Summen, *Acta Math.*, **70** (1947), S. 275—290.

[3] L. RÉDEI, Vereinfachter Beweis des Satzes von MINKOWSKI-HAJÓS, *Acta Sci. Math.*, **13** (1949), S. 21—35.

[4] L. RÉDEI, Kurzer Beweis des gruppentheoretischen Satzes von HAJÓS, *Commentarii Math. Helvetici*, **23** (1949), S. 272—282.

[5] L. RÉDEI, Die Reduktion des gruppentheoretischen Satzes von HAJÓS auf den Fall von $p$-Gruppen, *Monatshefte für Math.*, **53** (1949), S. 221—226.

[6] T. SZELE, Neuer vereinfachter Beweis des gruppentheoretischen Satzes von HAJÓS, *Publicationes Math.*, **1** (1949), S. 56—62.

# К ПРОБЛЕМЕ ФАКТОРИЗАЦИИ КОНЕЧНЫХ ГРУПП АБЕЛЯ

Л. РЭДЭИ (Сегед)

*(Резюме)*

Факторизацией некоторой конечной группы Абеля $\mathfrak{G}$ называется уравнение

$$\mathfrak{G} = \mathfrak{R}_1 \dots \mathfrak{R}_l \tag{1}$$

где $\mathfrak{R}_i$ комплексы (подмножества) $\mathfrak{G}$, а (1) нужно понимать так, что все элементы $\mathfrak{G}$ могут быть представлены единственным образом в следующей форме: $A_1 \dots A_l$ ($A_i \in \mathfrak{R}_i$). Считаем, что $l \geqq 2$ и каждый $\mathfrak{R}_i$ состоит по крайней мере из двух элементов. Относительно проблем факторизации, уже рассмотренных в литературе, см. работы [1]—[6].

Работа Гаёша, публикуемая в этом томе, показывает, что некоторая конечная циклическая группа $\mathfrak{G}$ имеет такую факторизацию $\mathfrak{G} = \mathfrak{R}_1\mathfrak{R}_2$, в которой ни $\mathfrak{R}_1$, ни $\mathfrak{R}_2$ не может быть произведением группы (содержащей по крайней мере два элемента) и дальнейшего комплекса, за исключением того случая, когда степень $\mathfrak{G}$ одно из следующих чисел: $p^e q^f$, $p^e qr$, $pqrs$ ($p, q, r, s$, различные простые числа; $e, f \geqq 0$). Этих случаев Гаёш не рассматривает. В этой работе автор доказывает, что степени вида $p^e$, $pq$, $pqr$ действительно являются исключениями теоремы Гаёша, доказательство в случае $pqr$ (относительно кажущейся легкости проблемы) довольно сложное. Из оставшихся критических случаев последний оказывается особенно трудным.