Studien

über

zyklische Dreiersysteme

der Form $N = 6n + 3$

Von

Dr. P. Beda Kaufmann, O. S. B., Rektor

Beilage zum Jahresbericht
der kantonalen Lehranstalt
in Sarnen pro 1925/26

1926
Buch- und Kunstdruckerei von Louis Ehrli in Sarnen

Studien

über

zyklische Dreiersysteme

der Form $N = 6n + 3$

Von

Dr. P. Beda Kaufmann, O. S. B., Rektor

Beilage zum Jahresbericht
der kantonalen Lehranstalt
in Sarnen pro 1925/26

1926
Buch- und Kunstdruckerei von Louis Ehrli in Sarnen

Einführung.

§ 1. Im Jahre 1844 hat Kirkmann[1]) das folgende schwierige kombinatorische Problem vorgelegt: Es sind x Elemente gegeben. Diese Elemente sollen in Klassen von y Elementen so eingeordnet werden, dass jede Gruppe von z Elementen einmal und nur einmal im ganzen Systeme vorkommt. $z \leqq y - 1 < x$. Ein spezieller Fall hierzu ist: $y = 3$, $z = 2$, wo jeder Zweier der x Elemente einmal und nur einmal in sämtlichen Dreiern des Systems auftritt. Für diesen speziellen Fall hat schon Kirkmann gefunden, dass x die Form $6n + 1$ oder $6n + 3$ haben müsse. Kirkmann erörtert aber das Problem auch ganz allgemein für jedes beliebige x.

Unabhängig von Kirkmann hat Steiner[2]) 1853 sein Kombinationsproblem aufgestellt, das aber in seinem ersten Teile nur den speziellen Fall des Kirkmann'schen Problems darstellt. Er gab seinem Problem folgende Fassung: *a.* Welche Zahl N von Elementen hat die Eigenschaft, dass sich die Elemente so zu Dreiern ordnen lassen, dass je zwei in einer und nur einer Verbindung vorkommen? *b.* Wie viele wesentlich verschiedene Anordnungen, d. h. solche, die nicht durch eine blosse Permutation der Elemente aus einander hervorgehen, gibt es für jede Zahl N? Die folgenden Teile des Problems von Steiner kommen für unsere Untersuchungen nicht in Betracht.

Die Frage „a" des Problems von Steiner ist nun vollständig gelöst. Die Antwort lautet: Für jedes $N = 6n + 1$ oder $6n + 3$ $(n = 1, 2, 3, \ldots)$ existieren Dreiersysteme, die die verlangte Eigenschaft besitzen. Der Nachweis wurde geführt durch Konstruktion von Dreiersystemen für jedes N der vorerwähnten Form. Methoden zur Konstruktion lieferten Reiss,[3]) E. H. Moore[4]) und Fitting.[5])

---

[1]) Ladies and Gentlemens Diary, ferner Cambridge and Dublin Math. Journal vol. 2 1847; vergleiche hiezu Miss Cummings: An undervalued Kirkmann paper in Bulletin of the Amerik. Math. Society vol. 24. pg. 336. 1917.

[2]) Journal für Math. vol. 45. 1853. Vergleiche auch Netto: Lehrbuch der Kombinatorik, Kap. X.

[3]) Journal für Math. vol. 56. 1859. pg. 326.

[4]) Math. Annalen 43 pg. 271 ff. 1893.

[5]) Nieuw Archief von Wiskunde, 9, pg. 359. 1911.

Was den zweiten Teil des erwähnten Problems von Steiner betrifft, so sah man unmittelbar, dass für 7 und 9 Elemente nur ein System besteht. Für 13 Elemente zeigt Zulauf [6]) mittels der Differenz der Substitutionengruppen, dass das System von Netto von den von Kirkmann, Reiss und De Vries [7]) gegebenen Systemen verschieden ist. Die letzten drei können dagegen durch Permutationen der Elemente ineinander übergeführt werden. Moore zeigt in der schon erwähnten Arbeit, dass für $N = 13$ wenigstens zwei verschiedene Dreiersysteme existieren müssen. V. de Pasquale, G. Brunel, J. Barrau und F. Cole [8]) stellten nacheinander fest, dass für 13 Elemente das System von Netto und das System von Kirkmann (als das älteste) die beiden einzigen möglichen verschiedenen Systeme seien.

Für 15 Elemente wurden durch Kirkmann und Cayley 11 resp. 12 verschiedene Dreiersysteme aufgestellt. Eine neue Methode mittels „Sequenzen" ermöglichte es Miss Cummings, [9]) die Zahl der verschiedenen Systeme auf 24 zu erhöhen und zugleich die interessante Tatsache zu entdecken, dass auch Systeme, die die gleiche Substitutionengruppe haben, nicht ineinander übergeführt werden können. Nach der in den Proceedings of the Nat. Academy of Sciences 1913, vol. III_3, veröffentlichten Arbeit: The complete emumeration of triad systems in 15 elements by F. N. Cole, L. Cummings and H. S. White existieren für 15 Elemente 80 verschiedene Systeme. Nach einer weiteren Arbeit durch H. White in den Transactions of the A. M. S. vol. 16, pg. 13: The Multitude of triad systems on 31 letters existieren für 31 Elemente mehr als $430 \cdot 14!$ d. h. mehr als $3 \cdot 10^{13}$ verschiedene Dreiersysteme.

§ 2. In dieser Studie greifen wir nur eine besondere Art von Dreiersystemen, nämlich zyklische, heraus. Geben wir kurz eine Erklärung von zyklischen Dreiersystemen. Gegeben seien die $6n+1$ Elemente $0, 1, 2, 3, \ldots, 6n$. — Es bilden $(\alpha+x, \beta+x, \gamma+x)$ $x = 0, 1, 2, \ldots, 6n$ eine Reihe oder Kolonne von $N = 6n+1$ Dreiern; in dieser Kolonne ist jedes Element in den so gebildeten Dreiern, das grösser als $6n$ ist, durch seinen kleinsten positiven Rest mod N zu ersetzen. So erhalten wir für $x = 6n+1$ wiederum denselben Dreier wie für $x = 0$.

---

6) Dissertation Giessen. 1897.

7) Rend. circ. mat. di Palermo. 1897.

8) Pasquale 1899: Sui sistemi ternari di 13 elementi Lomb. Ist. Rend. 2. 32, pg. 113. G. Brunel 1901: Sur les deux systèmes de triades de 13 éléments. Journal de Math. 7, pg. 305, et Mémoires de la société des sciences physiques et naturelles Bordeaux, serie 6, t 2 ch. 1, 1903; J. Barrau 1908: Over drie tals tel sels in hel bijzonder die van dertien elementen. Amst. Ac. Verslag 17, pg. 274; F. N. Cole 1913: The triad systems of 13 letters. Transactions of the A. M. S. vol. XIV, pg. 1.

9) „On a methode of comparaison for triple systems" by Cummings in Transactions of the A. M. S. vol. XV, pg. 311. 1914.

Da die Dreier, die ein beliebiges Dreiersystem von Steiner bilden, einmal und nur einmal jeden Zweier enthalten können, so beträgt ihre Anzahl $\frac{N(N-1)}{6}$, wie leicht gezeigt wird. Wenn nun diese $\frac{N(N-1)}{6}$ Dreier in $\frac{N-1}{6} = n$ verschiedenen Kolonnen

$$\alpha_i + x, \beta_i + x, \gamma_i + x \; (i = 0, 1, 2 \ldots n - 1)$$

verteilt sind, so bilden sie ein zyklisches Dreiersystem.

Für diese Kolonnen gelten folgende Eigenschaften, die Herr Prof. Bays in seiner prächtigen Arbeit „Sur les systèmes cycliques de Steiner" angeführt hat.[10])

1. Eine zyklische Kolonne ist durch jeden beliebigen Dreier der Kolonne bestimmt, den man den Kopf der Kolonne nennen kann.

2. Eine zyklische Kolonne hat 3 und nur 3 Dreier, die ein beliebiges der N Elemente, z. B. das Element 0, enthalten.

3. Zwei verschiedene zyklische Kolonnen haben keinen Dreier gemeinsam.

4. n verschiedene zyklische Kolonnen werden ein System von Steiner bilden, wenn jedes beliebige Element, z. B. das Element 0, in den 3 n Dreiern, die dieses beliebige Element enthalten, mit jedem der 6 n anderen Elemente verbunden ist.

Von zyklischen Systemen werde ich jene der Form $N = 6n + 3$ behandeln, nachdem die Aufgabe für zyklische Systeme der Form $N = 6n + 1$ (N eine Primzahl oder Potenz einer Primzahl) von Herrn Prof. Bays in der schon erwähnten Arbeit in vollständiger Einfachheit gelöst worden ist. Da diese Arbeit in der Absicht unternommen worden ist, zu sehen, welche Resultate die Anwendung jener Studien auf $6n + 3$ ergibt, werden wir uns im folgenden oft ziemlich stark an jene Arbeit anlehnen.

§ 3. Im Jahre 1893 veröffentlichte Eugen Netto in den Math. Annalen, vol. 42, pg. 143[11]) eine erste Arbeit über Konstruktion zyklischer Dreiersysteme für den Fall, dass $N = 6n + 1$ eine Primzahl ist. Wenn g eine primitive Kongruenzwurzel zu N ist, so bestimmen die n zyklischen Kolonnen

$$x, g^{\alpha} + x, g^{n+\alpha} + x \; \left(\begin{smallmatrix} x = 0, 1, 2, \ldots, 6n \\ \alpha = 0, 1, 2, \ldots, n-1 \end{smallmatrix}\right.$$

ein Dreiersystem von Steiner; denn man zeigt leicht, dass hierbei jedes beliebige Element mit allen 6 n andern Elementen verbunden ist.

Für $N = 6n + 3$, wo keine primitive Kongruenzwurzeln existieren, hat Netto nur für den Fall, wo $2n + 1$ eine Primzahl der Form $6n + 5$ ist, eine Konstruktionsmethode gegeben. In einer spätern Arbeit gab

---

10) S. Bays: Annales de l'Ecole normale supérieure 1923. vol. III, pg. 54.

11) Vergl. auch E. Netto: Lehrbuch der Kombinatorik, pg. 202 ff.

Netto[12]) unter Bezugnahme auf die Konstruktion von Heffter[13]) eine Methode für den Fall, dass $2n+1$ eine beliebige Primzahl ist. Es sei g eine primitive Wurzel (mod $2n+1$) und $g \equiv 1$ (mod 3). Diese Bedingung kann immer erfüllt werden; denn, wenn g diese Eigenschaft nicht hat, so hat sie $g+2n+1$ oder $g+4n+2$. Netto bildet mit g folgende Tabelle:

$$\left.\begin{array}{l} g^0,\ g^1,\ g^2,\ g^3,\ldots\quad,\ g^{2n-1} \\ 2g^0,\ 2g^1,\ 2g^2,\ 2g^3,\ldots\quad,\ 2g^{2n-1} \\ 3g^0,\ 3g^1,\ 3g^2,\ 3g^3,\ldots\quad,\ 3g^{2n-1} \end{array}\right\} \pmod{6n+3}. \qquad (\alpha)$$

Da die Zahlen jeder Zeile unter einander verschieden sind, aber auch die Zahlen verschiedener Zeilen verschieden sind, wie sich leicht zeigen lässt, so enthält obige Tabelle alle Zahlen 1, 2, 3, ..., $6n+2$ mit Ausnahme der drei Zahlen 0, $2n+1$, $4n+2$. Weil $g \equiv 1$ (mod 3) ist, stehen in der ersten respektive zweiten und dritten Zeile von (α) nur die Zahlen, die respektive kongruent 1, 2, und 0 (mod 3) sind. Es bestimmen die n zyklischen Kolonnen

$$x,\ g^{\alpha}+x,\ g^{n+\alpha}+x \qquad {\scriptstyle x=0,1,2,3,\ldots,6n+2 \atop \alpha=0,1,2,\ldots,n-1}$$

verbunden mit der zyklischen Kolonne

$$y,\ y+2n+1,\ y+4n+2 \qquad y=0,1,2,3,\ldots,2n$$

ein zyklisches Dreiersystem von Steiner. Um dies zu zeigen, genügt es, zu beweisen, dass alle $6n+2$ mit 0 verbundenen Elemente verschieden sind. Es sind dies:

$$\begin{array}{lll} 0,\ g^0,\ g^n & 0,\ g^1,\ g^{n+1} & \ldots\ 0,\ g^{n-1},\ g^{2n-1} \\ 0,\ g^n-g^0,\ -g^0 & 0,\ g^{n+1}-g^1,\ -g^1 & \ldots\ 0,\ g^{2n-1}-g^{n-1},\ -g^{n-1} \\ 0,\ -g^n,\ g^0-g^n & 0,\ -g^{n+1},\ g^1-g^{n+1} & \ldots\ 0,\ -g^{2n-1},\ g^{n-1}-g^{2n-1} \end{array}$$

Hier gehören $-g^{\alpha} \equiv 6n+3-g^{\alpha} \equiv 2$ (mod 3) der zweiten Zeile von (α), $g^{\mu}-g^{\nu} \equiv 0$ (mod 3) der dritten Zeile an, und es kann nicht $-g^{\alpha} \equiv -g^{\beta}$ (mod $6n+3$) werden, da dann auch $g^{\beta} \equiv g^{\alpha}$ sein müsste. Aber es kann auch nicht $g^{\alpha}-g^{n+\alpha} \equiv g^{\beta}-g^{n+\beta}$ (mod $6n+3$) sein. Würde dies gelten, so wäre $(g^{\alpha}-g^{\beta})(g^n-1) \equiv 0$ (mod $2n+1$), was unmöglich, da g primitive Wurzel (mod $2n+1$) ist. Wenn folglich 0 noch mit den beiden Elementen $2n+1$ und $4n+2$ verbunden ist, so ist es mit allen $6n+2$ Elementen verbunden, und dies lässt sich auch für jedes andere Element zeigen.

§ 4. Ueber zyklische Dreiersysteme hat Heffter in der schon erwähnten Arbeit zwei interessante Probleme studiert, die er Differenz-

---

12) Heffter: Math. Annalen, vol. 49, pag. 101. 1897.

13) Netto: Lehrbuch der Kombinatorik, cap. X, § 14.

probleme nennt. Es ist nämlich für jede zyklische Kolonne die Differenz zweier auf einander folgender Elemente immer dieselbe für alle Dreier dieser Kolonne. Heffter führt die Konstruktion der zyklischen Systeme auf die Lösung der beiden Differenzprobleme I und II zurück.

I. Die Zahlen $1, 2, 3, \ldots, 3n$ sind so in n Gruppen von je drei zu ordnen, dass in jeder Gruppe entweder die Summe der drei Zahlen gleich $6n+1$ oder dass die eine Zahl gleich der Summe der beiden andern ist.

II. Für Systeme der Form $N = 6n + 3$: Die Zahlen $1, 2, 3, \ldots, 2n$, $2n+2, \ldots, 3n+1$ sind so in n Gruppen von je drei zu ordnen, dass bei jeder Gruppe entweder die Summe der drei Zahlen gleich $6n+3$ oder die eine die Summe der beiden andern ist.

§ 5. Wir stellen uns nun in dieser Arbeit die Aufgabe, für die ersten Werte von $N = 6n + 3$ *sämtliche verschiedene zyklische Systeme* aufzufinden, und zwar werden wir in einem ersten Abschnitte an Hand einer Tabelle sämtlicher Dreier der N Elemente, die das Element 0 enthalten, ähnliche Beziehungen ableiten, wie Professor Bays in der schon genannten Arbeit. In einem zweiten Abschnitte werden wir einige einfache Sätze über metazyklische Substitutionen und ihre Anwendung auf zyklische Systeme studieren. Ein dritter Abschnitt wird uns durch Einteilung der zyklischen Systeme in Gruppen die verschiedenen zyklischen Systeme liefern, und in einem vierten Abschnitte zeigen uns die Züge von White, dass die Systeme verschiedener Gruppen auch verschieden sind und dass die Ordnung der Substitutionengruppe dieselbe ist, die im dritten Abschnitt gefunden wurde.

I. Teil.

§ 6. In einer ersten Tabelle werden wir alle Dreier von N Elementen, die das Element 0 enthalten, aufstellen. Wenn wir das Element 0 bei sämtlichen Dreiern weglassen, so müssen wir alle möglichen Zweier der Elemente $1, 2, 3, \ldots, 6n+2$ aufschreiben. Die Menge dieser Zweier können wir in einer Tabelle schematisch anordnen. Als Beispiel nehmen wir $N = 6n + 3$: $6 \cdot 3 + 3 = 21$. Wir bezeichnen die Elemente zur Abkürzung mit $0, 1, 2, \ldots, 9, 0', 1', 2', \ldots, 9', 0''$.

A

12

T. I. 13 23

14 **24** 34

15 25 35 45

16 26 **36** 46 56

17 27 37 47 57 67

18 28 38 **48** 58 68 78

19 29 39 49 59 69 79 89

10′ 20′ 30′ 40′ **50′** 60′ 70′ 80′ 90′

C′ B′

11′ 21′ 31′ 41′ 51′ 61′ 71′ 81′ 91′ **0′1′**

12′ 22′ **32′** 42′ 52′ **62′** 72′ 82′ **92′** 0′2′ 1′2′

13′ 23′ 33′ 43′ **53′** 63′ 73′ **83′** 93′ 0′3′ 1′3′ 2′3′

14′ 24′ 34′ 44′ 54′ 64′ **74′** 84′ 94′ 0′4′ 1′4′ 2′4′ 3′4′

15′ 25′ 35′ 45′ 55′ **65′** 75′ 85′ **95′** 0′5′ 1′5′ 2′5′ 3′5′ 4′5′

16′ 26′ 36′ 46′ **56′** 66′ 76′ **86′** 96′ 0′6′ **1′6′** 2′6′ 3′6′ 4′6′ 5′6′

17′ 27′ 37′ **47′** 57′ 67′ 77′ 87′ 97′ 0′7′ 1′7′ 2′7′ **3′7′** 4′7′ 5′7′ 6′7′

18′ 28′ **38′** 48′ 58′ 68′ 78′ 88′ **98′** 0′8′ 1′8′ 2′8′ 3′8′ 4′8′ **5′8′** 6′8′ 7′8′

19′ **29′** 39′ 49′ 59′ 69′ 79′ 89′ 99′ 0′9′ 1′9′ 2′9′ 3′9′ 4′9′ 5′9′ 6′9′ **7′9′** 8′9′

10″ 20″ 30″ 40″ 50″ 60″ 70″ 80″ 90″ **0′0″** 1′0″ 2′0″ 3′0″ 4′0″ 5′0″ 6′0″ 7′0″ 8′0″ **9′0″**

B A′ C

Die zyklische Kolonne, die sich aus dem Kopfe $(0, \alpha, \beta)$ $\alpha < \beta$ ableitet, enthält die drei Dreier

$$\begin{array}{lcl} 0,\ \alpha,\ \beta & \text{oder besser} & 0,\ \alpha,\ \beta \\ N-\alpha,\ 0,\ \beta-\alpha & \text{„} & 0,\ \beta-\alpha,\ N-\alpha \\ N-\beta,\ N-(\beta-\alpha),\ 0 & \text{„} & 0,\ N-\beta,\ N-(\beta-\alpha) \end{array}$$

In dieser zweiten Anordnung gibt mir das um 1 verminderte dritte Element die Zeile an, in der in vorausgehender Tabelle der Dreier steht, und das zweite Element den Rang, den dieser Dreier in der betreffenden Zeile einnimmt. Es ist nun leicht, sich über die Lage dieser drei Dreier in Tabelle I Rechenschaft zu geben. Wenn sich der erste Dreier auf AA′ verschiebt, so verschiebt sich der zweite Dreier auf der Mittellinie BB′ und der dritte Dreier auf CC′ in ganz gleicher Weise. Drehen wir die drei Mittellinien als starres System um den Punkt S, den Schnittpunkt der Mittellinien, so liegen diese drei Dreier immer entsprechend auf diesen Linien. Für die Kolonne, die aus dem Dreier auf dem Schnittpunkt der Mittellinien gebildet wird, existiert nur ein mit 0 verbundener Dreier, und wenn wir diesen Dreier als Kopf einer zyklischen Kolonne betrachten, so hat diese Kolonne nur einen Dreier, der ein beliebiges der N Elemente enthält, d. h. jedes Element kommt in dieser Kolonne nur einmal vor, und diese Kolonne hat nicht N, sondern nur $N/_3$ Glieder. — Da nun die den Dreiern vom Dreieck A S B entsprechenden beiden Dreier in (1) beziehungsweise in B S C und C S A liegen, genügt es, die Dreier des Dreiecks A S B der Untersuchung zu Grunde zu legen. Damit haben wir von den $\frac{(6n+3)(6n+2)(6n+1)}{6}$ Dreiern, die mit $6n+3$ Elementen gebildet werden können, nur die mit $n \cdot N+1$ Dreier auf A S und innerhalb des Dreiecks als Köpfe für die Bildung von Kolonnen zyklischer Dreiersysteme zu prüfen. Weitere Einschränkungen werden sich im folgenden Paragraphen ergeben.

§ 7. Wie wir wissen, darf in einer Kolonne, die zu einem zyklischen System gehört, kein Zweier zweimal vorkommen. Nun aber trifft dies zu, wenn in (1) zwei von den 6 mit 0 verbundenen Elementen gleich sind, d. h. wenn $\beta - \alpha = \alpha$ oder $\beta = 2\alpha$; $N - \beta = \alpha$ oder $N = \alpha + \beta$; und $N - (\beta - \alpha) = \beta$ oder $N + \alpha = 2\beta$ ist. Die einzigen Dreier, die diese Eigenschaft besitzen, befinden sich auf den Mittellinien, und diese Dreier können nicht als Köpfe von Kolonnen zyklischer Dreiersysteme gebraucht werden. Die Sonderstellung, die dem Dreier auf dem Schnittpunkt der Mittellinien zukommt, werden wir sofort näher untersuchen.

Für $N = 6n+3$ ist die Anzahl der Dreier eines Dreiersystems $\frac{N(N-1)}{6} = N\frac{6n+2}{6}$. In diesem Produkt ist weder der erste noch der zweite Faktor durch 6 teilbar. Trennen wir aber $N \cdot \frac{2}{6} = \frac{N}{3}$ Glieder ab, so bleiben noch $N \cdot n$ Dreier, die also n Kolonnen mit je N Gliedern bilden. Nun aber ist in T. I der einzige Dreier, der nach $\frac{N}{3}$ Glieder wieder auf den Anfangsdreier zurückführt, der Dreier auf dem Schnittpunkt der Mittellinien. Daraus folgt das wichtige Resultat:

Alle zyklischen Systeme, die mit $N = 6n+3$ Elementen gebildet werden können, enthalten den Dreier $(0, \frac{N}{3}, \frac{2N}{3})$ auf dem Schnittpunkt der Mittellinien als Kopf einer Kolonne mit $\frac{N}{3}$ Gliedern.

Weil in diesem Dreier schon die beiden Elemente $\frac{N}{3}$ und $\frac{2N}{3}$ mit 0 verbunden sind, so fallen für die n übrigen zyklischen Kolonnen eine ganze Anzahl Dreier im Dreieck ASB als Köpfe weg, jene nämlich, in denen die Differenz zwischen zwei Elementen $\frac{N}{3}$ beträgt, wie wir später bei Anwendung des Differenzproblems noch sehen werden.

§ 8. Wir nennen mit Hrn. Prof. Bays die Kolonne $(0, \alpha, N-\beta-\alpha)$ die *konjugierte* zur Kolonne $(0, \alpha, \beta)$, wie umgekehrt dann auch die letztere die konjugierte der ersteren ist. In der Tabelle I sind die konjugierten Kolonnen des Dreieckes ASB in vollständiger symmetrischer Lage zur Mittellinie SC'. Die Kolonnen der Dreier $(0, \alpha, \frac{N+\alpha}{2})$ auf SC' sind zu sich selbst die konjugierten, wie auch die in allen zyklischen Systemen vorkommende Kolonne $(0, \frac{N}{3}, \frac{2N}{3})$ zu sich selbst die konjugierte ist.

Der Lehrsatz, den Herr Bays in seiner Arbeit[1]) für $6n+1$ aufgestellt, gilt auch hier:

Die zyklische Kolonne transformiert sich in ihre konjugierte durch die Substitution $(x, N-x)$.

Da der Beweis sich vollständig deckt, lasse ich ihn weg.

Um ein zyklisches Dreiersystem aufzustellen, müssen wir n Kolonnen $(0, \alpha, \beta)$ innerhalb des Dreieckes ASB ausserhalb SC' nehmen, deren 6 mit 0 verbundene Elemente von einer Kolonne zur andern alle verschieden sind. Dadurch werden alle 6n Elemente 1, 2, 3, ..., 2n, $2n+2, \ldots, 4n+1, 4n+3, \ldots, 6n+2$ mit 0 verbunden. Da nun die 6 mit 0 in zwei konjugierten Kolonnen verbundenen Elemente

$$\begin{array}{ll} 0,\ \alpha,\ \beta & 0,\ \alpha,\ N-(\beta-\alpha) \\ 0,\ \beta-\alpha,\ N-\alpha & 0,\ N-\beta,\ N-\alpha \\ 0,\ N-\beta,\ N-(\beta-\alpha) & 0,\ \beta-\alpha,\ \beta \end{array}$$

dieselben sind, so kann die eine dieser Kolonnen durch die andere ersetzt werden. Das Resultat dieser Substitution ist jedesmal ein neues zyklisches System von Steiner. Das mit den n, zu jenen des ersten Systems konjugierten Kolonnen, gebildete wird das zum ersten *konjugierte System* genannt.

Es gilt auch hier: *Zyklische Systeme kommen paarweise vor. Die 2n Kolonnen jedes Paares haben keinen Dreier gemeinsam, diese Systeme sind aber gleichwertig und transformieren sich in einander durch die Substitution $|x, N-x|$. Die Kolonne mit $\frac{N}{3}$ Gliedern ist in beiden Systemen dieselbe und transformiert sich in sich selbst.*

Weil konjugierte Systeme gleichwertig sind, so schränkt sich die Bestimmung der *verschiedenen* zyklischen Systeme, d. h. solcher, die nicht durch eine Permutation ineinander übergehen können, auf die Köpfe der

---

[1]) l. c. pg. 62.

zyklischen Kolonnen, die innerhalb des Dreieckes A S C′ gelegen sind, ein mit der Möglichkeit, eine oder mehrere dieser Kolonnen durch ihre konjugierten zu ersetzen.

§ 9. Wenn $(0, \alpha, \beta)$ eine zyklische Kolonne darstellt, so sind von den 6 mit 0 verbundenen Elementen

$$\alpha, \quad \beta, \quad \beta-\alpha, \quad N-\alpha, \quad N-\beta, \quad N-(\beta-\alpha)$$

in dieser Kolonne drei kleiner als $\frac{N}{2}$ und die andern liegen zwischen $\frac{N}{2}$ und N.—.. In Tab. I ist der Dreier auf dem Schnittpunkt der Mittellinien: $0, 2n+1, 4n+2$. Für die beiden nächsten Dreier innerhalb des Dreieckes A S C′: $(0, 2n, 4n+1)$ und $(0, 2n-1, 4n)$, in denen α und β die grössten Werte haben, sind diese beziehungsweise $2n$ und $4n+1$. $\beta-\alpha$ hat seinen grössten Wert $3n$ in den Dreiern $0, 1, 3n+1$ und $0, 2, 3n+2$. Folglich sind in (2) α und $\beta-\alpha$ immer kleiner $\frac{N-1}{2}=3n+1$. Nur β kann $\frac{N}{2}$ überschreiten und $4n+2$ erreichen; aber dann ist $N-\beta$ kleiner als $\frac{N}{2}$. Wenn wir die drei Elemente, die kleiner sind als $\frac{N}{2}$, mit Herrn Bays die Charakteristik der zyklischen Kolonne nennen, so wird die Charakteristik

$$\alpha,\ \beta-\alpha,\ \beta \quad , \text{ wenn } \beta=2\alpha+1,\ 2\alpha+2, \ldots,\ 3n+1$$
$$\alpha,\ \beta-\alpha,\ N-\beta, \text{ wenn } \beta=3n+2,\ 3n+3, \ldots,\ 4n+2.$$

In der zyklischen Kolonne aus dem Dreier auf dem Schnittpunkt der Mittellinien sind die Elemente der Charakteristik $\alpha=\beta-\alpha=N-\beta=\frac{N}{3}$.

Schreiben wir nun die Charakteristiken aller zyklischen Kolonnen $(0, \alpha, \beta)$ innerhalb des Dreieckes A S C′ der Tabelle I auf und zwar schreiben wir die Zeilen als Kolonnen und das Element α nur einmal vor jede Zeile. Von der Charakteristik mit drei gleichen Elementen des Dreiers $0, \frac{N}{3}, \frac{2N}{3}$ schreiben wir nur ein Element rechts neben die Tabelle.

1	23	34	45	56	**67**	**78**	89	90′	**7**
2		35	46	**57**	68	**79**	80′	90′	
3			**47**	58	69	**70′**	80′		T. Ib.
4				59	60′	**70′**	89		
5					60′	**79**			
6						**78**			

§ 10. Damit nun in zwei verschiedenen zyklischen Kolonnen die 12 mit dem Elemente 0 verbundenen Elemente alle verschieden sind, ist offenbar notwendig und genügend, dass die 6 Elemente der beiden Charakteristiken verschieden sind. Alle Kombinationen der n zyklischen Kolonnen des Dreieckes A S C′, die ein Steinersches System aufstellen, bestimmen, heisst alle Gruppen von n Charakteristiken aufsuchen, die kein Element gemeinsam haben.

Nun aber kommt in allen zyklischen Systemen der Form $6n + 3$ die Kolonne mit $\frac{N}{3}$ Gliedern vor, die als einziges Charakteristik-Element $\frac{N}{3}$ enthält. Es fallen deshalb für die Kombination der n andern Charakteristiken alle jene fort, die dieses Element enthalten. (Diese sind in Tabelle I b kenntlich gemacht.) Die diesen Charakteristiken entsprechenden Dreier in Tabelle I können auf den ersten Blick gefunden werden.

Wir fallen damit auf das zweite Problem von Heffter. Für die Charakteristiken der ersten Form ist $\beta < 3n + 1$ und für die der zweiten Form ist $\beta > 3n + 1$. Die beiden Formen sind in Tabelle I b durch eine punktierte Linie von einander getrennt. In den Dreiern links ist das dritte Element die Summe der beiden andern und in den Dreiern rechts ist N die Summe aller 3 Elemente. Wenn ich nun unter diesen Dreiern alle möglichen Kombinationen von n Charakteristiken aufstelle, die kein Element gemeinsam haben, so habe ich einen sichern Weg, der mir alle möglichen zyklischen Dreiersysteme liefert.

Das Aufsuchen macht sich ohne Schwierigkeit. Ich kann z. B. den ersten Dreier der ersten Zeile nehmen und versuchen, ob ich damit ein oder mehrere Systeme von Charakteristiken aufstellen kann, nachher den zweiten Dreier der ersten Zeile usw. Habe ich alle Dreier der ersten Zeile erschöpft, so habe ich auch alle Systeme der Charakteristik gefunden.

Diese Methode lieferte mir für

	$N = 6n + 3$	Anzahl d. Syst. d. Char.
$n = 1$	9	0
$n = 2$	15	1
$n = 3$	21	4
$n = 4$	27	9
$n = 5$	33	50

II. Teil.

§ 11. Wir haben in einem ersten Teile die Systeme der Charakteristiken und damit auch die zyklischen Systeme von Steiner gefunden. Wir werden nun zeigen, wie man mittels einer besondern Art von Substitutionen alle nicht gleichwertigen Systeme finden kann. In diesem Abschnitte werden wir folglich vorerst einige Sätze über Kongruenzwurzeln, darauf aufbauend über arithmetische und geometrische Substitutionen und schliesslich die Anwendung dieser Sätze auf zyklische Systeme studieren.

Man sagt, N beliebige Zahlen bilden ein *vollständiges Restsystem* [1]) zu einer Zahl N, wenn diese Zahlen durch N geteilt alle Zahlen von 0 bis N — 1 zum Reste ergeben und man bedient sich der Schreibweise $x \equiv a$ (mod N), die bedeutet: x und a durch N geteilt, ergeben den gleichen Rest, insbesondere kann a den kleinsten positiven Rest bezeichnen, den x durch N geteilt, ergibt.

Ein *reduziertes Restsystem* [1]) (mod N) ist dann gegeben, wenn wir nur jene, aber auch alle jene Zahlen zum Reste erhalten, die zu N relative Primzahlen sind. — Ist N eine Primzahl, so fallen vollständiges und reduziertes Restsystem zusammen. Im andern Falle bezeichnen wir die Anzahl dieser mit Gauss durch $\varphi(N)$. Wenn $N = p_1^{a_1} \; p_2^{a_2} \; p_3^{a_3} \dots$ ist (p_1, p_2, p_3 Primfaktoren von N), so gelten die wichtigen Formeln:

$$\varphi(N) = \varphi(p_1^{a_1}) \cdot \varphi(p_2^{a_2}) \cdot \varphi(p_3^{a_3})$$

$$\varphi(p^a) = p^a - p^{a-1}$$

Insbesondere $\quad \varphi(p) = p - 1$

Wenn nun z eine relative Primzahl zu N und $z^\delta \equiv 1$ (mod N), δ der kleinste Exponent von z, der kongruent 1 (mod N) ist, wobei also z zum Exponenten δ (mod N) gehört, so sind die Potenzen

$$1, z, z^2, z^3, \dots, z^{\delta-1} \tag{1}$$

alle untereinander (mod N) verschieden.[2]) Ist $\delta = \varphi$ (N), so heisst z eine primitive Wurzel. Ist δ kleiner als $\varphi(N)$, so existiert eine Zahl a, die relative Primzahl zu N und keiner Potenz von (1) gleich ist, und es werden folglich die δ Zahlen

$$a, az, az^2, az^3, \dots az^{\delta-1} \tag{2}$$

sowohl untereinander als auch mit den Zahlen von (1) inkongruent sein. Ist damit das reduzierte Restsystem (mod N) erschöpft, so haben wir $2\delta = \varphi(N)$. Wenn nicht, so existiert eine dritte, teilerfremde Zahl zu N,

---

[1]) Vergl. P. Bachmann: Niedere Zahlentheorie, Kap. III, Reste und Kongruenzen, pg. 67 ff.

[2]) Ebendaselbst, Kap. VII, Höhere Kongruenzen, pg. 319 ff.

die keiner Potenz von (1) und (2) gleich ist. Und man kann so fortfahren, bis man das reduzierte Restsystem hat.

Nun wissen wir nach bekannten Sätzen der Zahlentheorie, dass der Exponent, zu dem eine Wurzel gehören kann, höchstens ψ (N) beträgt, wenn ψ(N) das kleinste gemeinschaftliche Vielfache der Faktoren $\varphi(p_1^{a_1})$, $\varphi(p_2^{a_2})$, $\varphi(p_3^{a_3})$, . . . ist, wobei $N = p_1^{a_1} \cdot p_2^{a_2} \cdot p_3^{a_3} \ldots$ (p_1, p_2, p_3 . . . Primfaktoren). Primitive Wurzeln, d. i. Wurzeln, die zum Exponenten ψ(N) gehören, existieren nur, wenn N eine Primzahl ist, oder die Potenz einer Primzahl, oder 2^λ oder $2\,p^\lambda$ (p Primzahl).

Wenn also N das Produkt aus 3 und einer beliebigen Primzahl oder Potenz einer Primzahl ist, so existieren immer Wurzeln, die zum Exponenten $\frac{\varphi(N)}{2}$ gehören; denn das grösste gemeinschaftliche Vielfache der Faktoren von φ (N) ist 2.

Für $N = 6 \cdot 7 + 3 = 45 = 3^2 \cdot 5$ ist $\varphi(N) = 6 \cdot 4$, und es existieren Wurzeln, die zum Exponenten $\frac{\varphi(N)}{2}$ gehören.

Für $N = 6 \cdot 9 + 1 = 55 = 5 \cdot 11$ ist $\varphi(N) = 4 \cdot 10$, und es existieren Wurzeln, die zum Exponenten $\frac{\varphi(N)}{2}$ gehören.

Die einzigen Fälle der Form $6\,n + 1$ und $6\,n + 3$ für kleinere Werte von N, in denen keine Wurzeln existieren, die zum Exponenten $\frac{\varphi(N)}{2}$ gehören, sind:

$N = 6 \cdot 10 + 3 = 63 = 3^2 \cdot 7$; $\varphi(N) = 6 \cdot 6$; z kann höchstens zum Exponenten $\frac{\varphi(N)}{6}$ gehören;

$N = 6 \cdot 14 + 1 = 85 = 5 \cdot 17$; $\varphi(N) = 4 \cdot 16$; z kann höchstens zum Exponenten $\frac{\varphi(N)}{4}$ gehören;

$N = 6 \cdot 15 + 1 = 91 = 7 \cdot 13$; $\varphi(N) = 6 \cdot 12$; z kann höchstens zum Exponenten $\frac{\varphi(N)}{6}$ gehören;

$N = 6 \cdot 17 + 3 = 105 = 3 \cdot 5 \cdot 7$; $\varphi(N) = 2 \cdot 4 \cdot 6$; z kann höchstens zum Exponenten $\frac{\varphi(N)}{4}$ gehören;

$N = 6 \cdot 20 + 1 = 121 = 11 \cdot 11$; $\varphi(N) = 10 \cdot 10$; z kann höchstens zum Exponenten $\frac{\varphi(N)}{10}$ gehören.

§ 12. Fügen wir zum Vorausgehenden noch einiges über Substitutionen hinzu. Die einfachsten Ausdrücke für Substitutionen von N Elementen erhalten wir durch die Substitutionen der linearen Form $s = |x, a + x|$, wo a eine ganze Zahl (mod N) ist. Wenn a alle Werte von 0 bis N—1 durchläuft, so erhalten wir N Substitutionen, und diese bilden die Gruppe der arithmetischen Substitutionen [3]) der Ordnung und des Grades N. Diese Gruppe ist transitiv, d. h. wir können a so wählen, dass ein beliebiges Element x in ein beliebiges y übergeführt wird. Man braucht nur $a = y - x$ zu setzen.

Eine zweite Art von Substitutionen ist von der Form $t = |x, a\,x|$,

[3]) Vergl. P. Bachmann: Niedere Zahlentheorie, Kap. V, pg. 157.

die man geometrische Substitution [4]) nennt. a muss hierbei relative Primzahl zu N sein. Dies ist notwendig und hinreichend, damit t eine Substitution darstelle.[5]) Die Anzahl, der für den mod N möglichen verschiedenen geometrischen Substitutionen lässt sich leicht bestimmen. Es sind dies die Substitutionen, in denen a alle Werte der zu N relativen Primzahlen von 1 bis N—1 annimmt, deren Anzahl φ (N) beträgt und die zugleich auch die höchstmögliche Ordnung der geometrischen Substitutionengruppe angibt.

§ 13. Wir haben nun folgende Sätze:

1. Wenn a zum Exponenten $\varphi(N)$ gehört, so kommen, wenn wir für die Darstellung der Substitutionen die gebräuchlichste Methode anwenden,[6]) *durch die Substitution $t = | x, ax |$ alle zu N relativen Primzahlen in einem einzigen Zykel vor. Gehört aber a zum Exponenten $\frac{\varphi(N)}{2}$, so verteilen sich durch diese Substitution alle zu N relativen Primzahlen in zwei Zykel von je $\frac{\varphi(N)}{2}$ Glieder.* Hierbei sind alle Werte $a \cdot x$ durch den kleinsten positiven Rest (modulo N) zu ersetzen. Dieser Satz folgt unmittelbar aus dem, was im § 11 gesagt wurde.

2. Wenn a zum Exponenten $\frac{\varphi(N)}{2}$ gehört und der erste Zykel der zu N teilerfremden Zahlen das Element 1, aber das dazu komplementäre Element N—1 nicht enthält, so umfasst der zweite Zykel der zu N relativen Primzahlen die komplementären Elemente zu jenen des ersten Zykels in der gleichen Reihenfolge.

Es sei der erste Zykel $a^0\ a\ a^2\ a^3 \ldots a^{\frac{\varphi(N)}{2}}$. Dieser enthalte das zu $a^0 = 1$ komplementäre Element N—1 nicht. Dann zeigen wir, dass ein zweiter Zykel notwendig $((N-a^0)\ (N-a)\ (N-a^2)\ (N-a^3) \ldots (N-a^{\frac{\varphi(N)}{2}-1}))$ ist. Vorerst ist klar, dass alle Elemente a^i $(i = 0, 1, \ldots, \frac{\varphi(N)}{2} - 1)$ untereinander verschieden sind, da a zum Exponenten $\frac{\varphi(N)}{2}$ gehört. Ferner ist einleuchtend, dass alle $(N-a^i)$ untereinander verschieden sind; denn jedes folgende Element ist aus dem vorhergehenden durch Multiplikation mit a hervorgegangen, da $a^i N \equiv N \pmod{N}$ gesetzt werden darf.

Nun zeigen wir, dass kein Element des zweiten Zykels im ersten vorkommt und umgekehrt. Nehmen wir an, es sei $a^i \equiv N - a^k \pmod{N}$ $i, k \leqq \frac{\varphi(N)}{2} - 1$, so folgt daraus $a^i + a^k \equiv 0 \pmod{N}$;

$$\begin{aligned} &\text{wenn } i = k & 2a^i &\equiv 0 \pmod{N}, \text{was unmöglich, da } N \neq 2 \\ &\text{wenn } i < k & a^i(1 + a^{k-i}) &\equiv 0 \pmod{N} \\ & & 1 + a^{k-i} &\equiv 0 \pmod{N} \\ & & \text{d. h. } a^{k-i} &\equiv -1 \pmod{N}, \end{aligned}$$

---

[4]) Netto: Substitutionentheorie, Kap. VIII; Analytische Darstellung der Substitutionen, pg. 149 ff.

[5]) Netto: Substitutionentheorie, Kap. VIII, pg. 153.

[6]) Ibidem, Kap. II, § 22, dritte Methode.

was wiederum unmöglich, da unter den Potenzen von a die zu -1 kongruente nicht vorkommt. Folglich ist der Beweis erbracht. Wenn a die Eigenschaften des Satzes 2 erfüllt, wollen wir sie *halbprimitive Wurzel* nennen.

3. Die Substitution $t_2 = |x, (N-a)\,x|$ *stimmt in ihren geraden Potenzen mit den geraden Potenzen der Substitution* $t_1 = |x, a\,x|$ *überein, und ersetzt in ihren ungeraden Potenzen sämtliche Elemente der entsprechenden ungeraden Potenzen von* t_1 *durch die komplementären.*

Dies ist sofort klar, wenn man bedenkt, dass

$$t_2^{2i} = |x, (N-a)\,x|^{2i} = |x, (-a)^{2i}\,x| = |x, a^{2i}\,x| = t_1^{2i}$$

$$t_2^{2i+1} = |x, (N-a)\,x|^{2i+1} = |x, a^{2i}\,x| \cdot |x, (N-a)\,x| = |x, (N-a^{2i+1})\,x|$$

und $(N - a^{2i+1})$ ist das komplimentäre Element zu a^{2i+1}.

Corollarium: Ist a *zu* N *halbprimitive Wurzel, so ist auch* $N - a$ *halbprimitive Wurzel.* Dies leuchtet aus den beiden vorausgehenden Sätzen unmittelbar ein.

Fragen wir uns nun über die Anordnung der nicht teilerfremden Elemente in den beiden Substitutionen t_1 und t_2. Wir betrachten hierfür nur den einfachsten Fall, dass N aus zwei verschiedenen Primfaktoren p und q zusammengesetzt ist, wovon $q = 3$. Wir haben folgendes:

4. a. Wenn $a \equiv 1 \pmod 3$, *so werden die Vielfachen von* p *nicht umgesetzt, und die Vielfachen von 3 befinden sich in einem einzigen Zykel mit Periode* $p-1$.

b. Wenn $a \equiv -1 \pmod 3$, *so haben wir einen Zykel* $(p\ pa)$ *und die Vielfachen von 3 befinden sich noch in einem einzigen Zykel, ausgenommen den Fall, in dem* p *eine Primzahl der Form* $4v+3$ *ist, wo sich dieser in zwei Zykel zerlegt, die die zueinander inbezug auf* N *komplementären Elemente enthalten.*

Vorerst ist klar, dass die zu 3p nicht teilerfremden Zahlen nur aus den Vielfachen von 3 und p bestehen können; ferner, dass a nur kongruent $\pm 1 \pmod 3$ sein kann, da a relative Primzahl zu 3p ist. Sodann ist hier $\frac{\varphi(N)}{2} = p-1$ und a gehört zum Exponenten $p-1 \pmod{3p}$.

ad a. $a \equiv 1 \pmod 3$. Um die nicht umgesetzten Elemente zu finden, müssen wir die Kongruenz

$x \equiv a\,x \pmod{3p}$, d. h. die Kongruenz $(1-a)\,x \equiv 0 \pmod{3p}$

auflösen. Da $1 - a \equiv 0 \pmod 3$, so ist

$x \equiv 0 \pmod p$, d. h. die Elemente p, $2p$, $3p = 0$ werden nicht umgestellt.

Der Zykel der Vielfachen von 3 lautet:

$$(3\ 3a\ 3a^2\ 3a^3\ \ldots\ 3a^d)$$

Wir suchen nun den Exponenten, für welchen

$3a^d \equiv 3 \pmod{3p}$ oder folglich $a^d \equiv 1 \pmod p$ ist.

Wir haben $\alpha^{d-1} \equiv 1 \pmod{3p}$ und $\alpha^d \equiv 1 \pmod{3}$.

Daraus folgt $\alpha^d \equiv 1 \pmod{3p}$, d. h. $d = p - 1$.[7]

Die Substitution t_1 lautet nun:

$$t_1 = (\alpha^0 \alpha \alpha^2 \ldots \alpha^{p-2}) (N - \alpha^0, N - \alpha, N - \alpha^2 \ldots N - \alpha^{p-2}) (3\ 3\alpha\ 3\alpha^2 \ldots 3\alpha^{p-2})$$
$$(0)\ (p)\ (2p).$$

ad b. $\alpha \equiv -1 \pmod{3}$. Wir haben für die Lösung der Kongruenz $(1-\alpha)\, x \equiv 0 \pmod{3p}$, da $1 - \alpha \not\equiv 0 \pmod{3}$ und $\pmod{p}$ $x \equiv 0 \pmod{3p}$, d. h. das einzige Element 0 wird nicht umgestellt und wir haben folglich auch den einen Zykel $(p\ p\alpha) = (p\ 2p)$.

Für den Zykel der Vielfachen von 3 haben wir wiederum $\alpha^d \equiv 1 \pmod{p}$.

Wenn d gerade, so ist auch
$\alpha^d \equiv 1 \pmod{3}$ und daraus $\alpha^d \equiv 1 \pmod{3p}$ d. h. $d = p - 1$

Wenn d ungerade, so ist
$\alpha^d \equiv -1 \pmod{3}$, $\alpha^{2d} \equiv 1 \pmod{3}$ und damit $\alpha^{2d} \equiv 1 \pmod{3p}$, d. h. $2d = p - 1$ oder $d = \frac{p-1}{2}$
und der Zykel zerfällt in zwei mit je $\frac{p-1}{2}$ Gliedern. Dies trifft nur zu, wenn

$$d = 2v + 1 = \frac{p-1}{2} \text{ d. h. } p = 4v + 3 \text{ ist. } (v = 0, 1, 2 \ldots)$$

Was den letzten Punkt des Satzes betrifft, so folgt dieser unmittelbar daraus, dass α unter seinen Potenzen (mod 3p) keine zu einander komplementäre Elemente enthält.

Die Substitutionen lauten also für den Fall b.:

wenn $p = 4v + 1$:
$$t_1' = (\alpha^0 \alpha \ldots \alpha^{p-2}) (N - \alpha^0 \ldots N - \alpha^{p-2}) (3\ 3\alpha \ldots 3\alpha^{p-2}) (p\ 2p)\ (0)$$
wenn $p = 4v + 3$:
$$t_1'' = (\alpha^0 \alpha \ldots \alpha^{p-2}) (N - \alpha^0 \ldots N - \alpha^{p-2}) (3\ 3\alpha \ldots 3\alpha^{\frac{p-3}{2}})$$
$$(N - 3\ [N-3]\, \alpha, \ldots [N-3]\, \alpha^{\frac{p-3}{2}})\ (p\ 2p)\ (0).$$

Eine letzte Bemerkung wird uns nun die Beziehung zwischen den Substitutionen t_1 und t_2 vollständig klar machen.

Wenn $\alpha \equiv 1 \pmod{N = 3p}$, so ist $N - \alpha \equiv -1 \pmod{N}$, d. h. wenn wir für die halbprimitive Wurzel α die Substitution t_1 haben, so sind die Substitutionen t_2 für die halbprimitive Wurzel $N - \alpha$ von der Form t_1' oder t_2', je nachdem $p = 4v + 1$ oder $4 + 3$ ist. Wenn dagegen $\alpha \equiv -1 \pmod{3p}$ wäre, so würden wir nur die Wurzeln α und $N - \alpha$ vertauschen, um dieselbe Darstellung zu haben.

5. *Die Komposition der beiden geometrischen Substitutionen $t_1 = |x, \alpha x|$ und $t_2 = |x, (N-\alpha)\, x|$ erzeugt uns alle möglichen geometrischen Substitutionen.*

---

[7]) Vergl. hierzu auch Bachmann: Niedere Zahlentheorie, Kap. V, pg. 159.

Denn vorerst sind die Ordnungen der Gruppen $\{t_1\}$ und $\{t_2\}$ gleich $\frac{\varphi(N)}{2}$. Ferner ist $t_1^{-1} t_2 t_1 = t_2$, d. h. t_1 und t_2 sind miteinander vertauschbar; die zweite Potenz von t_1 ist der zweiten Potenz von t_2 gleich und umgekehrt. Dann folgt nach einem Satze der Substitutionentheorie [8]) für die Ordnung der Gruppe

$$\{t\} = \{|x, \alpha x|, |x, (N-\alpha) x|\}$$

die Grösse φ (N), was zu beweisen war.

Für die Komposition der beiden geometrischen Substitutionen t_1 und t_2 bedienen wir uns im folgenden der kürzeren Darstellung

$$\{t\} = \{|x, \pm|\alpha|x|\}$$

welche Schreibweise bedeutet, dass für alle Werte von α und seiner Potenzen (mod N) das Plus- und das Minuszeichen zu nehmen sei, und dass darin die negativen Werte $-|\alpha|x$ durch ihre zu N komplementären Werte zu ersetzen sind. $\{|x, +|\alpha|x|\}$ ist nichts anderes, als die Gruppe $\{t_1\}$, die einen Teiler der vollständigen geometrischen Gruppe bildet, $|x, -|\alpha|x|$ und seine Potenzen bilden nach der festgesetzten Bedeutung keine geometrische Gruppe; denn diese Substitution ist in ihren ungeraden Potenzen identisch mit den ungeraden Potenzen von $t_2 = |x, (N-\alpha) x|$, deren gerade Potenzen mit t_1 übereinstimmen, während die geraden Potenzen von $|x, -|\alpha|x|$ nur durch Komposition der beiden Substitutionen t_1 und t_2 erzeugt werden können.

§ 14. Studieren wir nun die Komposition der arithmetischen Substitution $s = |x, 1+x|$ mit der geometrischen $t = |x, \pm|\alpha|x|$.

Wir haben folgendes: *1.* Wenn N eine Primzahl p ist, so kann die Gruppe durch Komposition der beiden Substitutionen $s = |x, 1+x|$ und $t = |x, \alpha x|$ (α primitive Wurzel) erzeugt werden; sie lautet:

$$\{|x, a+x|, |x, \alpha x|\} \quad \begin{matrix} a = 0, 1, 2, \ldots p-1. \\ \alpha = 1, 2, 3, \ldots p-1. \end{matrix}$$

und hat die Ordnung p (p — 1).

2. Wenn N Potenz einer Primzahl p oder das doppelte der Potenz einer Primzahl ist, so kann die Gruppe ebenso durch die Komposition der beiden Substitutionen $s = |x, 1+x|$ und $t = |x, \alpha x|$ (α primitive Wurzel) im weiteren Sinne gehörend zum Exponenten φ (N) erzeugt werden; sie lautet:

$$\{|x, a+x|, |x, \alpha x|\} \quad \begin{matrix} a = 0, 1, 2, \ldots N-1 \\ \alpha = \text{die } \varphi(N) \text{ relativen Primzahlen zu N} \end{matrix}$$

und hat die Ordnung N · φ (N).

3. Wenn N eine zusammengesetzte Zahl ist, für die es eine halbprimitive Wurzel gibt, so kann die Gruppe durch die beiden Substitutionen $s = |x, 1+x|$ und $t = |x, \pm|\alpha|x|$ (α halbprimitive Wurzel) erzeugt werden; sie lautet:

---

8) Netto: Gruppen und Substitutionstheorie, Kap. IV, § 34.

$$\left\{ |x, a + x|, |x, \pm|\alpha|x| \right\} \begin{matrix} a = 0, 1, 2, \dots N-1 \\ \alpha = \text{die } \varphi(N) \text{ relativen Primzahlen zu N} \end{matrix}$$

und hat auch die Ordnung $N \cdot \varphi(N)$.

Im weiteren Sinne nennen wir auch im zweiten und dritten Falle die *Gruppen metazyklische*, wie ja für alle drei Arten von Gruppen die Ordnung $N \cdot \varphi(N)$ beträgt.

Jeder *metazyklische Teiler* der Gruppe unter 3 wird gebildet durch Komposition der beiden Substitutionen

$$s = |x, 1 + x| \text{ und } t^{\omega} = |x, \pm|\alpha^{\omega}|x|,$$

wo ω beliebiger Teiler von $\frac{\varphi(N)}{2}$ ist; denn ω kann nur Teiler der Ordnung der Substitutionengruppen t_1 oder t_2 sein, die $\frac{\varphi(N)}{2}$ beträgt. Die Ordnung des metazyklischen Teilers ist so $\frac{N \cdot \varphi(N)}{2\omega} 2 = \frac{N \cdot \varphi(N)}{\omega}$.

Die Komposition der beiden Substitutionen $s = |x, a + x|$ und $t = |x, \pm|\alpha|x|$ kann als einzige Substitution

$$z = st = |x, a \pm |\alpha|x|,$$

die noch eine metazyklische Substitution ist, dargestellt werden.

Die m^te^ Potenz dieser Substitution für $\alpha > 1$ ist

$$z^m = |x, a \frac{\pm|\alpha|^m - 1}{\pm|\alpha| - 1} \pm |\alpha|^m x|.$$

Wenn $\alpha > 1$ und N Primzahl, so stellt die metazyklische Substitution $p - 1$ Elemente um. Das nicht umgestellte Element ist durch Lösung der Kongruenz $x \equiv a + \alpha x \pmod N$ gegeben. Wenn N keine Primzahl ist, aber N und $\alpha - 1$ keinen gemeinschaftlichen Teiler haben, so stellt auch in diesem Falle die Substitution noch $N - 1$ Elemente um. Haben aber N und $\alpha - 1$ den gemeinschaftlichen Teiler δ, so sind die δ nicht umgestellten Elemente durch die Lösung der Kongruenz $(1 - \alpha)x \equiv a \pmod N$ gegeben.

§ 15. Folgende Lehrsätze zeigen uns nun die Anwendung dieser Substitutionen auf zyklische Dreiersysteme für den Fall, dass N eine halbprimitive Wurzel besitzt. Die ersten drei Sätze lauten fast gleich wie jene von Prof. S. Bays [9]) für $N = 6n + 1$ angegebenen, nämlich

1. Die zyklische Substitution $|x, a + x|$ *transformiert jede zyklische Kolonne in sich selbst.*

2. Die metazyklische Substitution $|x, a \pm |\alpha|x|$ *transformiert a. eine zyklische Kolonne wiederum in eine zyklische Kolonne, und b. die zyklische Kolonne mit* $\frac{N}{3}$ *Gliedern in sich selbst.*

a. Denn diese Substitution verwandelt den beliebigen Dreier

$$m, n, p \text{ in } a \pm m\alpha,\ a \pm n\alpha,\ a \pm p\alpha$$

und den Dreier der gleichen Kolonne

$$m + s,\ n + s,\ p + s \text{ in } a \pm m\alpha \pm s\alpha,\ a \pm n\alpha \pm s\alpha,\ a \pm p\alpha \pm s\alpha$$

d. h. in einen Dreier der gleichen Kolonne wie der erstere.

---

9) l. c. pg. 67 ff.

b. Der Dreier der zyklischen Kolonne mit $\frac{N}{3}$ Glieder

$$x, \ \tfrac{N}{3}+x, \ \tfrac{2N}{3}+x \text{ wird durch diese Substitution}$$

$$a \pm \alpha x, \ a \pm \tfrac{N}{3}\alpha \pm \alpha x, \ a \pm \tfrac{2N}{3}\alpha \pm \alpha x$$

d. h. ein Dreier der Kolonne $(0 \pm \frac{N}{3}\alpha \pm \frac{2N}{3}\alpha)$. Weil α teilerfremd zu 3 und $N\alpha \equiv N$ (mod N) ist, so ist dies der Dreier $0, \frac{N}{3}, \frac{2N}{3}$.

3. Die metazyklische Substitution $|x, a \pm |\alpha| x|$ *transformiert zwei konjugierte Kolonnen in zwei konjugierte Kolonnen;* denn durch diese Substitution wird der Kopf der Kolonne

$$o, n, p \quad \text{in} \quad a, \ a + n\alpha, \ a + p\alpha \quad \text{umgewandelt,}$$

d. h. die Kolonne (o, n, p) wird $(0, \ \pm n\alpha, \ \pm p\alpha)$
und die Kolonne (o, n, p') „ $(0, \ \pm n\alpha, \ \pm p'\alpha)$
wo $p' \equiv N - p + n$ d. h. $p + p' \equiv n$ (mod N).

Wenn α relative Primzahl zu N ist, so ist der Kongruenz

$$\pm p\alpha \pm p'\alpha \equiv \pm n\alpha \pmod{N}$$

genügt durch

$$\pm p'\alpha = N \mp p\alpha \pm n\alpha \quad \text{d. h. die konjugierte der ersten.}$$

w. z. b. w.

Die Gruppe, die ein zyklisches System in sich selbst transformiert, enthält also immer die zyklische Gruppe $\{s\} = \{|x, 1+x|\}$. Die Substitutionen der metazyklischen Gruppe transformieren ein zyklisches Dreiersystem in ein zyklisches Dreiersystem und zwei konjugierte Systeme in zwei konjugierte.

4. Die Ordnung des metazyklischen Teilers, der ein zyklisches System in sich selbst transformiert, ist $\frac{N \cdot \varphi(N)}{2\omega}$. ($\omega$ *beliebiger Teiler von* $\frac{\varphi(N)}{2}$.)

Um vorerst alle Systeme zu finden, die sich durch eine metazyklische Substitution auseinander ableiten, müssen wir nur die Substitution $|x, \alpha x|$ (α halbprimitive Wurzel) auf die zyklischen Systeme anwenden; denn die Substitution $|x, -|\alpha|x|$ liefert ja für alle Potenzen die konjugierten Systeme zu den entsprechenden Potenzen der Substitution $|x, \alpha x|$; und konjugierte Systeme sind gleichwertig und gehen durch die Substitution $|x, N - x|$ ineinander über.

Wenn nun ω die kleinste Potenz von α ist, ($\frac{\varphi(N)}{2}$ ist die kleinste Potenz von α, die kongruent 1 (mod N)), für welche die Substitution $|x, \pm|\alpha|^{\omega} x|$ das System in sich selbst und sein konjugiertes umwandelt, so muss ω Teiler von $\frac{\varphi(N)}{2}$ sein und die Ordnung des metazyklischen Teilers, der das System in sich selbst und sein konjugiertes überführt, ist $N \cdot \frac{\varphi(N)}{\omega}$. — Da nun die beiden Gruppen $\{|x, \alpha^{\omega} x|\}$ und $\{|x, (N-\alpha^{\omega})x|\}$ gleiche Ordnung haben und nach dem auf folgender Seite unabhängig hiervon zu zeigenden Satze, dass die gleichen Substitutionen, die zyklische Systeme ineinander transformieren, diese auch in sich selbst transformieren, folgt, dass genau die Hälfte aller Substitutionen das

System in sich selbst transformiert, mit andern Worten, die Ordnung der Gruppe, die das System in sich selbst überführt, ist $N \cdot \frac{\varphi(N)}{2\omega}$.

Ist $\frac{\varphi(N)}{2}$, das immer gerade, das Produkt aus ω und einer ungeraden Zahl, so gibt die Substitution $|x, a^{\omega} x|$ das ursprüngliche System; denn andern Falls würde uns auch die Substitution $|x, a^{\frac{\varphi(N)}{2}} x|$ das zum ersteren konjugierte System liefern, was unmöglich ist.

Ist dagegen ω ungerade, so hängt es von der Beschaffenheit des Systems ab, ob die Substitution $|x, a^{\omega} x|$ das erste oder das dem ersten konjugierte System liefert, wie die Beispiele im § 18 und 19 es auch zeigen werden.

Ist $\omega = \frac{\varphi(N)}{2}$, so besitzt das zyklische System nur den zyklischen Teiler $\{s\} = \{|x, 1 + x|\}$ der Ordnung N.

Ist $\omega = 1$, so hat das System den metazyklischen Teiler der Ordnung $N \cdot \frac{\varphi(N)}{2}$, die wir noch halbmetazyklische Gruppe[10]) nennen können. Kein zyklisches System hat also die vollständige metazyklische Gruppe.

5. *Die beliebige metazyklische Substitution* $|x, b + \beta x|$ *(β Primzahl zu N) ist vertauschbar mit dem metazyklischen Teiler*

$$\{|x, 1 + x| \; |x, \pm |a|^{\omega} x|\}$$

Denn die Substitutionen dieses Teilers sind:

$$|x, \pm |a|^{\omega s} x| \cdot |x, a + x| = |x, a \pm |a|^{\omega s} x| \quad \begin{matrix} a = 0, 1, 2, \ldots N-1 \\ s = 1, 2, 3, \ldots \frac{\varphi(N)}{2\omega} \end{matrix}$$

$$|x, a' \pm |a|^{\omega s} x| \cdot |x, b + \beta x| = |x, b + a'\beta \pm |a|^{\omega s} \beta x|$$

$$|x, b + \beta x| \cdot |x, a \pm |a|^{\omega s} x| = |x, a \pm b |a|^{\omega s} \pm |a|^{\omega s} \beta x|$$

Die Kongruenz

$$b + a'\beta \equiv a \pm b |a|^{\omega s} \pmod N \text{ oder}$$

$$a'\beta \equiv a - b \pm b |a|^{\omega s}$$

oder besser die beiden Kongruenzen

$$a'\beta \equiv a - b + b a^{\omega s} \text{ und } a'\beta \equiv a - b + (N - a^{\omega s}) b.$$

haben stets Lösungen für β, wenn β relative Primzahl zu N ist.

Daraus ergibt sich das wichtige Resultat, das auch Prof. Bays in seiner Arbeit anführt:[11]) *Zwei zyklische Systeme, die sich ineinander durch eine metazyklische Substitution transformieren, haben die gleichen metazyklischen Substitutionen, die sie in sich selbst transformieren.* Im besondern *enthalten die metazyklischen Teiler, die zu zwei konjugierten Systemen gehören, die gleichen Substitutionen.*

---

[10]) Vergl. Netto: Substitutionstheorie, Kap. VII, § 127, pg. 140.

[11]) l. c. théorème 7.

III. Teil.

§ 16. Nachdem wir im zweiten Teile die metazyklischen Substitutionen und ihre Anwendung auf zyklische Systeme betrachtet haben, wird es uns ein leichtes sein, diese Theorie auf die aus den Systemen der Charakteristiken sich ableitenden zyklischen Systeme anzuwenden. Wir haben in jedem zyklischen System der Form $N = 6n + 3$ n Kolonnen mit N Gliedern und eine Kolonne mit $\frac{N}{3}$ Gliedern. Letztere ist in allen Systemen bei demselben N dieselbe und hat auf die Verschiedenheit der zyklischen Systeme keinen Einfluss. Bei den übrigen n Kolonnen kann jede durch die konjugierte ersetzt werden, und dies liefert uns im ganzen 2^n zyklische Dreiersysteme. Nun sind aber die Hälfte die konjugierten der andern, und es bleiben zu unserer Prüfung für jedes System der Charakteristiken noch 2^{n-1} zyklische Dreiersysteme.

Folglich:

n	N=6n+3	Anz. der Charakt.	Anz. d. möglicherweise verschiedenen Systeme
1	9	0	0
2	15	1	2
3	21	4	16
4	27	9	72
5	33	50	800

Beginnen wir mit dem Studium für die einzelnen N:

§ 17.

N = 9.

A

12

13 23

14 **24** 34

C′ B′

15 25 35 **45**

16 26 **36** 46 56

17 **27** 37 47 **57** 67

18 28 38 **48** 58 68 **78**

B A′ C

1	**23** **34**		**3**
2	**34**		

Für N = 9 zeigt uns die Tabelle der Charakteristiken, dass von den drei Dreiern des Dreieckes, die möglicherweise zur Bildung einer zyklischen Kolonne in Betracht kommen könnten, alle wegfallen, da ihre Charakteristik das Element $\frac{N}{3} = 3$ enthält, das schon in der Kolonne mit $\frac{N}{3}$ Glieder vorkommt. Folglich gibt es für N = 9 kein zyklisches Dreiersystem. Dies hat schon Heffter[1]) bemerkt, wenn er sagt, dass das Differenzproblem für N = 9 nicht lösbar ist.

Wir finden dies aber noch auf andere Weise. Für N = 9 besteht nur ein Steinerisches Dreiersystem der Ordnung 840.[2]) Nun aber wissen wir aus dem Vorausgehenden, dass jedes zyklische Dreiersystem mindestens den zyklischen Teiler der Ordnung N hat. Da aber 840 nicht durch N = 9 teilbar ist, so folgt daraus, dass es für N = 9 kein zyklisches Dreiersystem gibt.

§ 18.

N = 15.

A

12

13 23

14 **24** 34

15 25 35 45

16 26 **36** 46 56

17 27 37 47 57 67

C′ **18** 28 38 **48** 58 68 **78** B′

19 29 **39** 49 59 **69** 79 89

10′ 20′ 30′ 40′ **50′** 60′ 70′ 80′ 90′

11′ 21′ 31′ **41′** 51′ 61′ **71′** 81′ 91′ 0′1′

12′ 22′ **32′** 42′ 52′ **62′** 72′ 82′ **92′** 0′2′ 1′2′

13′ **23′** 33′ 43′ 53′ 63′ 73′ 83′ 93′ 0′3′ **1′3′** 2′3′

14′ 24′ 34′ 44′ 54′ 64′ **74′** 84′ 94′ 0′4′ 1′4′ 2′4′ **3′4′**

B A′ C

1	23	34	**45**	**56**	67	5
2		**35**	46	**57**	67	
3			47	**57**		
4				**56**		

1) Vergl. Netto: Lehrbuch der Kombinatorik, Kap. X, § 16.

2) Vergl. Netto: ibidem, § 18.

Die Tabelle der Charakteristiken liefert uns als einziges System

134	*267*	5

und folglich zur Prüfung die beiden zyklischen Systeme

014	028	050′	a
012′	028	050′	a_1

Anmerkung: In den Charakteristiken sind jene Dreier, wo die Summe aller drei Zahlen N ist, und in den zyklischen Systemen jene Dreier, die die konjugierten der ersten, mit Kursivschrift dargestellt. Ich versehe die Bezeichnung des Systems mit einem Stern, wenn alle Dreier des ersten durch die konjugierten ersetzt werden. Ist nur die i^{te} Kolonne die konjugierte, so versehe ich die Bezeichnung mit dem Index i, ist die erste und i^{te} konjugiert, mit dem Index $n + i - 1$ etc.

Hier ist $\frac{\varphi(N)}{2} = \frac{2 \cdot 4}{2} = 4$. 2 ist halbprimitive Wurzel. Die Substitution $|\, x, 2x\,|$ auf unsere Systeme angewandt, gibt

014	028	050′	a	*012′*	028	050′	a_1
028	014	050′	a	*029*	014	—	a_1*

Für 15 Elemente sind also höchstens die beiden zyklischen Systeme verschieden und beide haben den metazyklischen Teiler $\{\,|\,x, 1+x\,|, |\,x, \pm|\,2\,|\,x\,|\,\}$ der Ordnung $4 \cdot 15 = 60$. Wenn wir bedenken, dass $\{\,|\,x, \pm|\,a\,|\,x\,|\,\}$ nur als abgekürzte Schreibweise für $\{\,|\,x, a\,x\,|, |\,x, (N-a)\,x\,|\,\}$ gewählt wurde, so lautet also der metazyklische Teiler ausführlich geschrieben:

$$\{\,|\,x, 1+x\,|, |\,x, \pm|\,2\,|\,x\,|\,\} = \{\,|\,x, 1+x\,|, |\,x, 2\,x\,|, |\,x, 3'\,x\,|\,\}.$$

§ 19.

N = 21.

Die Tabelle der Charakteristiken, Tab. I b, § 9, liefert uns folgende 4 Systeme von Charakteristiken und damit von zyklischen Systemen, die ich nebeneinander darstelle und wo jedes dieser Systeme noch 4 verschiedene Systeme in sich schliessen kann.

123	*489*	*560′*	7	013	042′	051′	074′	a
145	280′	369	—	015	020′	039	—	b
189	235	460′	—	019	025	040′	—	c
190′	246	358	—	010′	026	038	—	d

Es ist $\frac{\varphi(N)}{2} = \frac{2 \cdot 6}{2} = 6$. 2 ist halbprimitive Wurzel. Die Substitution mittels Wurzel 2 auf die Systeme angewandt, liefert uns folgende 7 verschiedene zyklische Systeme:

013	042′	051′	074′	a	*017′*	020′	039	074′	b_1
026	038	010′	—	d	*023′*	015	039	—	b_2
042′	051′	013	—	a	*017′*	020′	039	—	b_1

019'	042'	051'	074'	a_1	015	020'	*035'*	074'	b_3
027'	038	010'	—	d_2	020'	015	*035'*	—	b_3
043'	051'	013	—	a_2					
036'	010'	026	—	d_3	019	025	040'	074'	c
055'	013	042'	—	a_3	*028'*	040'	019	—	c_2
012'	026	038	—	d_1	*045'*	019	*028'*	—	c_1*
019'	042'	051'	—	a_1	*013'*	*028'*	*045'*	—	c*
015	020'	039	074'	b	019	025	*045'*	074'	c_3
020'	015	039	—	b	*028'*	040'	*013'*	—	c_3*

Das System a_1 hat nur den zyklischen Teiler $\{|x, 1+x|\}$ der Ordnung 21.

Das System c hat den metazyklischen Teiler $\{|x, 1+x|, |x, \pm|2|^3 x|\}$ der Ordnung $2 \cdot 21 = 42$.

Die Systeme a und b_1 haben den metazyklischen Teiler $\{|x, 1+x|, |x, \pm|2|^2 x|\}$ der Ordnung $3 \cdot 21 = 63$.

Die Systeme b, b_3 und c_3 haben den metazyklischen Teiler $\{|x, 1+x|, |x, \pm|2|x|\}$ der Ordnung $6 \cdot 21 = 126$, d. h. die halbmetazyklische Gruppe.

Wir haben also für $N = 21$ im ganzen höchstens 7 verschiedene zyklische Systeme.

§ 20.

N = 27.

1	23	34	45	56	67	78	**89**	**90'**	0'1'	1'2'	2'3'	**9**
2		35	46	57	68	**79**	80'	**91'**	0'2'	1'3'	2'3'	
3			47	58	**69**	70'	81'	**92'**	0'3'	1'3'		
4				**59**	60'	71'	82'	**93'**	0'3'	1'2'		
5					61'	72'	83'	**93'**	0'2'			
6						73'	83'	**92'**	0'1'			
7							82'	**91'**				
8								**90'**				

A

12

13

14 **24**

15 25

16 26 **36**

17 27 37

18 28 38 **48**

19 29 39 49

10′ 20′ 30′ 40′ **50′**

11′ 21′ 31′ 41′ 51′

12′ 22′ 32′ 42′ 52′ **62′**

13′ 23′ 33′ 43′ 53′ 63′

C′

14′ 24′ 34′ 44′ 54′ 64′ **74′**

35′ 45′ 55′ 65′ 75′

56′ 66′ 76′ **86′**

77′ 87′

98′

S

Wir stellen in nebenstehender Tabelle nur jenen Teil des Dreieckes dar, dessen Dreier für die Bildung von zyklischen Kolonnen in Betracht kommen. Die Tabelle der Charakteristiken gibt uns folgende 9 Lösungen.

123	471′	*50′2′*	*683′*	9	013	041′	055′	064′	098′	a
123	*40′3′*	561′	*782′*	—	013	044′	051′	075′	—	b
145	20′2′	381′	673′	—	015	022′	031′	063′	—	c
156	21′3′	370′	482′	—	016	023′	030′	042′	—	d
178	246	*31′3′*	*50′2′*	—	018	026	034′	055′	—	e
10′1′	235	482′	673′	—	011′	025	042′	063′	—	f
11′2′	246	370′	583′	—	012′	026	030′	053′	—	g
12′3′	257	381′	460′	—	013′	027	031′	040′	—	h
12′3′	280′	347	561′	—	013′	020′	037	051′	—	i

Da jede Lösung 2^{n-1} verschiedene Systeme liefern kann, so haben wir im ganzen $8 \cdot 9 = 72$ Systeme zu prüfen. Da $27 = 3^3$ Potenz einer Primzahl ist, so gibt es primitive Wurzeln. Es ist $\varphi\ (3^3) = 3^3 - 3^2 = 18$. 2 ist eine primitive Wurzel. Die Substitution $|x, 2x|$ gibt uns folgende Einteilung der zyklischen Systeme. Zur Rechten sind die Köpfe der zyklischen Kolonnen nach der Grösse des zweiten Elementes geordnet.

013	041′	055′	064′	098′	013	041′	055′	064′	098′	a
026	053′	030′	012′	—	012′	026	030′	053′	—	g
042′	011′	*060″*	*024″*	—	011′	*024″*	042′	*060″*	—	f_6*
031′	*022″*	*015′*	*041″*	—	*015′*	*022″*	031′	*041″*	—	h_3*
051′	*047′*	*015″*	*079′*	—	*015″*	*047′*	051′	*079′*	—	b_3*
055′	*010″*	*023″*	*036′*	—	*010″*	*023″*	*036′*	055′	—	e_4*
030′	023′	*049′*	*012″*	—	*012″*	023′	030′	*049′*	—	d_7
060″	015	*039′*	*027′*	—	015	*027′*	*039′*	*060″*	—	c_1*
015′	020′	*051″*	*033″*	—	*015′*	020′	*033″*	*051″*	—	i_2*
015″	*040″*	*057′*	*069′*	—	*015″*	*040″*	*057′*	*069′*	—	a*

Von a* an wiederholen sich die konjugierten Systeme in der gleichen Ordnung, da eine metazyklische Substitution zwei konjugierte Systeme in zwei konjugierte Systeme transformiert. Wenn wir von einem andern a_i ausgehen, d. h. wenn wir im System a eine oder mehrere Kolonnen durch die konjugierten ersetzen, so sind nach Satz III, § 15, II. Teil, die entsprechenden vertikalen Reihen durch die konjugierten Kolonnen zu ersetzen; mit andern Worten, die sieben andern Systeme a_i $(i = 1, 2, \ldots, 7)$ geben jedes, wenn man vom Index absieht, eine zu a identische Folge von Systemen, und wir finden für 27 Elemente höchstens die 8 verschiedenen zyklischen Systeme a, a_1, a_2, ..., a_7. Da die Ordnung einer Gruppe mit primitiver Wurzel $\frac{N \cdot \varphi(N)}{\omega}$ ist (ω derart, dass die Substitution $|x, a^\omega x|$ wiederum das Anfangssystem, nicht etwa das dem ersten konjugierte System liefert, wie es bei halbprimitiven Wurzeln möglich ist), so haben alle diese Systeme nur den zyklischen Teiler $\{|x, 1+x|\}$ der Ordnung N.

Anmerkung: a. Wenn wir im Falle primitiver Wurzeln in der Substitution $|x, a^\omega x|$ für a die Potenz ω nehmen, die das zyklische System in sein konjugiertes transformiert, so haben wir für die Ordnung der Gruppe $\frac{N \cdot \varphi(N)}{2\omega}$. Auch hier liefert uns die Substitution $|x, -|a|x|$ die zu der Substitution $|x, ax|$ konjugierten Systeme. Aber die Substitution $|x, a^\omega x|$ gibt uns immer, ob ω gerade oder ungerade, das zum ersten konjugierte System.

b. Wenn a zum Exponenten $\varphi(N)$ gehört und $\varphi(N)$ nur durch die erste Potenz von 2 teilbar ist, so gehört $(N - a)$, wie sich leicht ergibt, zum Exponenten $\frac{\varphi(N)}{2}$ und ist halb primitive Wurzel. Ist dagegen $\varphi(N)$ durch eine höhere Potenz von 2 teilbar, so gehört auch $(N - a)$ zum Exponenten $\varphi(N)$.

§ 21.

N = 33.

Für $N = 33$ werden die beiden Tabellen auf gleiche Weise, wie für die andern N aufgestellt. Hier ist $\varphi(N) = 20$. Wir stellen hier nur die Tabelle der Charakteristiken dar:

1	23	34	45	56	67	78	89	90′	**0′1′**	**1′2′**	2′3′	3′4′	4′5′	5′6′	**1′**
2		35	46	57	68	79	80′	**91′**	0′2′	**1′3′**	2′4′	3′5′	4′6′	5′6′	
3			47	58	69	70′	**81′**	92′	0′3′	**1′4′**	2′5′	3′6′	4′6′		
4				59	60′	**71′**	82′	93′	0′4′	**1′5′**	2′6′	3′6′	4′5′		
5					**61′**	72′	83′	94′	0′5′	**1′6′**	2′6′	3′5′			
6						73′	84′	95′	0′6′	**1′6′**	2′5′	3′4′			
7							85′	96′	0′6′	**1′5′**	2′4′				
8								96′	0′5′	**1′4′**	2′3′				
9									0′4′	**1′3′**					
0′										**1′2′**					

Diese Tabelle liefert mir folgende 50 Systeme. Links stehen die Systeme der Charakteristiken und rechts die entsprechenden zyklischen Systeme.

123	460′	*53′5′*	*72′4′*	*896′*	1′	013	040′	058′	079′	087′	01′2″	A(a)
123	482′	50′5′	*63′4′*	796′	—	013	042′	055′	069′	076′	—	A(b)
123	40′4′	583′	*62′5′*	796′	—	013	044′	053′	068′	076′	—	A(c)
123	42′6′	594′	673′	*80′5′*	—	013	046′	054′	063′	088′	—	A(d)
134	279	*52′6′*	*63′4′*	*80′5′*	1′	014	029	057′	069′	088′	01′2″	B(a)
134	20′2′	*53′5′*	684′	796′	—	014	022′	058′	064′	076′	—	B(b)
134	22′4′	583′	695′	*70′6′*	—	014	024′	053′	065′	077′	—	B(c)
134	22′4′	50′5′	673′	*896′*	—	014	024′	055′	063′	087′	—	B(d)
145	280′	32′5′	*63′4′*	796′	1′	015	020′	035′	069′	076′	01′2″	C(a)
145	280′	33′6′	695′	*72′4′*	—	015	020′	036′	065′	079′	—	C(b)
145	23′5′	392′	684′	*70′6′*	—	015	025′	032′	064′	077′	—	C(c)

145	24′6′	370′	695′	*82′3′*	—	015	026′	030′	065′	080″	—	C(d)
145	24′6′	392′	673′	*80′5′*	—	015	026′	032′	063′	088′	—	C(e)
156	20′2′	*34′6′*	493′	785′	1′	016	022′	037′	043′	075′	01′2″	D(a)
156	*25′6′*	347	*82′3′*	*90′4′*	—	016	027′	037	080″	099′	—	D(b)
167	280′	32′5′	*43′6′*	594′	1′	017	020′	035′	047′	054′	01′2″	E(a)
167	22′4′	33′6′	459	*80′5′*	—	017	024′	036′	049	088′	—	E(b)
167	23′5′	358	42′6′	*90′4′*	—	017	025′	038	046′	099′	—	E(c)
167	*25′6′*	392′	40′4′	583′	—	017	027′	032′	044′	053′	—	E(d)
167	*25′6′*	30′3′	482′	594′	—	017	027′	033′	042′	054′	—	E(e)
178	235	*43′6′*	*62′5′*	*90′4′*	1′	018	025	047′	068′	099′	01′2″	F(a)
178	22′4′	369	*43′6′*	50′5′	—	018	024′	039	047′	055′	—	F(b)
178	23′5′	369	40′4′	*52′6′*	—	018	025′	039	044′	057′	—	F(c)
178	24′6′	392′	460′	*53′5′*	—	018	026′	032′	040′	058′	—	F(d)
178	24′6′	30′3′	459	*62′5′*	—	018	026′	033′	049	068′	—	F(e)
189	246	33′6′	50′5′	*72′4′*	1′	019	026	036′	055′	079′	01′2″	G(a)
189	257	33′6′	40′4′	*62′5′*	—	019	027	036′	044′	068′	—	G(b)
189	22′4′	347	*53′5′*	60′6′	—	019	024′	037	058′	066′	—	G(c)
189	23′5′	*34′6′*	460′	572′	—	019	025′	037′	040′	052′	—	G(d)
190′	235	42′6′	*63′4′*	785′	1′	010′	025	046′	069′	075′	01′2″	H(a)
190′	257	32′5′	*43′6′*	684′	—	010′	027	035′	047′	064′	—	H(b)
190′	268	33′6′	*44′5′*	572′	—	010′	028	036′	048′	052′	—	H(c)
190′	23′5′	347	*52′6′*	684′	—	010′	025′	037	057′	064′	—	H(d)
190′	24′6′	347	583′	*62′5′*	—	010′	026′	037	053′	068′	—	H(e)
12′3′	279	358	*44′5′*	60′6′	1′	013′	029	038	048′	066′	01′2″	J(a)
12′3′	*25′6′*	370′	459	684′	—	013′	027′	030′	049	064′	—	J(b)
13′4′	235	482′	695′	*70′6′*	1′	014′	025	042′	065′	077′	01′2″	K(a)
13′4′	257	369	42′6′	*80′5′*	—	014′	027	039	046′	088′	—	K(b)
13′4′	257	32′5′	460′	*896′*	—	014′	027	035′	040′	087′	—	K(c)
13′4′	268	32′5′	459	*70′6′*	—	014′	028	035′	049	077′	—	K(d)
13′4′	280′	347	*52′6′*	695′	—	014′	020′	037	057′	065′	—	K(e)
14′5′	235	460′	796′	*82′3′*	1′	015′	025	040′	076′	080″	01′2″	L(a)
14′5′	246	392′	583′	*70′6′*	—	015′	026	032′	053′	077′	—	L(b)
14′5′	246	30′3′	572′	*896′*	—	015′	026	033′	052′	087′	—	L(c)
14′5′	268	370′	493′	*52′6′*	—	015′	028	030′	043′	057′	—	L(d)
14′5′	280′	369	*43′6′*	572′	—	015′	020′	039	047′	052′	—	L(e)
15′6′	235	482′	673′	*90′4′*	1′	016′	025	042′	063′	099′	01′2″	M(a)
15′6′	246	370′	594′	*82′3′*	—	016′	026	030′	054′	080″	—	M(b)
15′6′	257	369	40′4′	*82′3′*	—	016′	027	039	044′	080″	—	M(c)
15′6′	268	30′3′	459	*72′4′*	—	016′	028	033′	049	079′	—	M(d)

Es folgen daraus 800 nicht konjugierte Systeme, für die wir die Bezeichnungen anwenden, die früher angegeben wurden. Die Substitution

$|\,x,\; 7\,x\,|$ (7 ist halbprimitive Wurzel von 33) verteilt diese 800 Systeme in 8 Gruppen gleichwertiger Systeme. 4 Gruppen sind vom gleichen Typus und 2 weitere Gruppen haben wiederum einen gleichen Typus, während die beiden anderen verschiedenen Typus haben.

I. Gruppe.

13	40′	58′	79′	87′	1′2″	od.	13	40′	58′	79′	87′	1′2″	A(a)
71″	48″	27″	16′	33′	—	„	16′	27″	33′	48″	71″	—	M_7(d)*
18′	20‴	93″	66″	42′	—	„	18′	20‴	42′	66″	93″	—	M_3(a)*
63′	21″	14	84″	53″	—	„	14	21″	53″	63′	84″	—	B_8(d)*
87′	19′	52′	33″	29″	—	„	19′	29″	33″	52′	87′	—	L_{10}(c)
33′	17	28′	45″	54′	—	„	17	28′	33′	45″	54′	—	E_4(e)
42′	76′	60″	55′	13	—	„	13	42′	55′	60″	76′	—	A_4(b)
53″	30″	15″	26	71″	—	„	15″	26	30″	53″	71″	—	G_2(a)*
29″	81″	36″	54″	18′	—	„	18′	29″	36″	54″	81″	—	M(b)*
54′	88′	46′	11‴	63′	—	„	11‴	46′	54′	63′	88′	—	A_1(d)
13	40′	58′	79′	87′	—	„	13	40′	58′	79′	87′	—	A(a)

Indem wir in dieser Tabelle zur linken 013[3]) und die erste Kolonne durch die konjugierten Dreier ersetzen, haben wir A_1(a) und seine transformierten Systeme. Wenn wir die i^{te} Kolonne durch die konjugierten ersetzen, haben wir A_i(a). Wenn wir die erste und i^{te} Kolonne durch die konjugierten ersetzen, haben wir $A_{n+i-1}(a) = A_{4+i}(a)$ und seine Transformierten. Wenn wir die ersten zwei und die i^{te} Kolonne durch konjugierte ersetzen, haben wir $A_{2n+i-3} = A_{7+i}(a)$ und seine Transformierten. Wenn wir beziehungsweise die 1., 3., 4. oder 1., 3., 5. oder 1., 4., 5. Kolonne durch konjugierte ersetzen, haben wir entsprechend A_{13}(a), A_{14}(a) und A_{15}(a) und seine Transformierten. Da unter den transformierten Systemen kein A_i(a) vorkommt, so haben wir im ganzen $2^{n-1} = 16$ nicht konjugierte Systeme: A(a), A_1(a), ..., A_{15}(a), die alle nur den zyklischen Teiler $\{\,|\,x,\; 1+x\,|\,\}$ haben.

Die folgenden 3 Gruppen haben den ganz gleichen Typus. Wir geben bei jeder Gruppe nur die Bezeichnung des ersten Systems und seiner durch die Substitution $|\,x,\; 7\,x\,|$ transformierten.

II. Gruppe: A(c), C_4(b)*, M(c)*, C(e), K_1(c), F_3(e)*, K_{14}(a)*, F_{13}(b)*, L(b)*, E_{12}(a)*, A(c).

III. Gruppe: B(a), G_2(d), J_7(b)*, H(a)*, G_3(c)*, L_7(d), E_2(c), B_8(b), H(c)*, D_{15}(b), B(a).

IV. Gruppe: B(c), L_{15}(e)*, E_3(d)*, C_{10}(a)*, G_9(b), C_5(d)*, K_{13}(b)*, F_{12}(d)*, K_4(d)*, F_{14}(a), B(c).

---

[3]) In den folgenden Tabellen der Gruppen haben wir das allen Dreiern gemeinsame Element Null weggelassen; auch haben wir es unterlassen, die konjugierten Dreier kursiv zu schreiben.

V. Gruppe.

15	25′	32′	64′	77′	1′2″	od.	15	25′	32′	64′	77′	1′2″	C(c)
									$C_1, C_2, C_3, C_5, C_6, C_8, C_{12}$.[4]				
27	64′	35′	10′	47′	—	„	10′	27	35′	47′	64′	—	H(b)
29′	10′	61″	39″	55″	—	„	10′	29′	39″	55″	61″	—	$H_1(e)$*
14′	39″	64″	51″	20′	—	„	14′	20′	39″	51″	64″	—	$K_6(e)$*
18	51″	39	25′	44′	—	„	18	25′	39	44′	51″	—	$F_5(c)$
73″	25′	34″	64′	19″	—	„	19″	25′	34″	64′	73″	—	$C_{14}(c)$,
:	:	:	:	:			:		$C_7, C_4^*, C_9, C_{11}^*, C_{10}, C_{13}, C_{15}^*$.				
15	25′	32′	64′	77′	—	„	15	25′	32′	64′	77′	—	C(c)

Es ist unnütz, die Tabelle über $C_{14}(c)$, das die 5. transformierte ist, auszudehnen; denn von da an wiederholen sich die Systeme mit gleichen Buchstaben in gleicher Anordnung, aber mit verschiedenem Index. Da nach Satz III § 15 die metazyklische Substitution zwei konjugierte Kolonnen in zwei konjugierte Kolonnen transformiert, können wir die 10. transformierte sofort aufschreiben, die, wie nicht anders möglich, das Anfangssystem ist.

Da hier nun unter den Transformierten jede Buchstabenbezeichnung zweimal vorkommt, so haben wir nicht 16, sondern nur 8 möglicherweise verschiedene Systeme, die alle den zyklischen Teiler $\{|x, 1+x|\}$ haben.

VI. Gruppe.

16	22′	37′	43′	75′	1′2″	od.	16	22′	37′	43′	75′	1′2″	D(a), $D_1(a)$, $D_3(a)$, $D_9(a)$
26″	49′	13′	38	66′	—	„	13′	26″	38	49′	66′	—	$J_{14}(a)$*
39′	18″	75″	22′	44″	—	„	18″	22′	39′	44″	75″	—	$D_2(a)$*, $D_{15}(a)$, $D_{13}(a)$, $D_9(a)$
75′	37′	43′	18″	23″	—	„	18″	23″	37′	43′	75′	—	$D_6(a)$, $D_{12}(a)$, $D_{11}(a)$
44″	75″	22′	37′	16	—	„	16	22′	37′	44″	75″	—	$D_{10}(a)$*, $D_5(a)$, $D_7(a)$*
23″	43′	18″	75″	39′	—	„	18″	23″	39′	43′	75″	—	$D_4(a)$*, $D_{14}(a)$, $D_8(a)$*
16	22′	37′	43′	75′	—	„	16	22′	37′	43′	75′	—	D(a), $D_1(a)$, $D_3(a)$

Die drei Systeme D(a), $D_1(a)$, $D_3(a)$ besitzen nur den zyklischen Teiler $\{|x, 1+x|\}$.

Das System $D_9(a)$ besitzt den metazyklischen Teiler

$$\{|x, 1+x|, |x, \pm|7|^2 x|\} \text{ der Ordnung } 5 \cdot 33 = 165.$$

[4]) Wegen Platzmangel lasse ich bei diesen Systemen (c) weg.

VII. Gruppe.

(gleicher Typus wie VI).

17	24′	36′	49	88′	1′2″	od.	16	24′	36′	49	88′	1′2″	$E(b), E_1(b), E_3(b), E_9(b)$
76′	15′	80″	25	40′	—	„	15′	25	40′	76′	80″	—	$L(a)$
30″	17″	83″	24′	48″	—	„	17″	24′	30″	48″	83″	—	$E_2(b)^*, E_{15}(b), E_{13}(b), E_9(b)$
88′	36′	49	17″	21″	—	„	17″	21″	36′	49	88′	—	$E_6(b), E_{12}(b), E_{11}(b)$
48″	83″	24′	36′	17	—	„	17	24′	36′	48″	83″	—	$E_{10}(b)^*, E_5(b), E_7(b)^*$
21″	49	17″	83″	30″	—	„	17″	21″	30″	49	83″	—	$E_4(b)^*, E_{14}(b), E_8(b)^*$
17	24′	36′	49	88′	—	„	17	24′	36′	49	88′	—	$E(b), E_1(b), E_3(b)$.

Die Systeme $E(b)$, $E_1(b)$ und $E_3(b)$ besitzen den zyklischen Teiler $\{|x, 1+x|\}$.

Das System $E_9(b)$ besitzt den metazyklischen Teiler $\{|x, 1+x|, |x, \pm|7|^2x|\}$ der Ordnung $5 \cdot 33 = 165$.

VIII. Gruppe.

10′	25′	37	57′	64′	1′2″	od.	10′	25′	37	57′	64′	1′2″	$H(d), H_3(d), H_5(d), H_{12}(d)$
39″	64′	57′	20″	10′	—	„	10′	20″	39″	57′	64′	—	$H_{15}(d), H_9(d)^*, H_{10}(d), H_{12}(d)$
51″	10′	20″	65″	39″	—	„	10′	20″	39″	51″	65″	—	$H_1(d)^*, H_6(d)^*, H_7(d)^*$
25′	39″	65″	14″	51″	—	„	14″	25′	39″	51″	65″	—	$H_2(d)^*, H_{13}(d), H_{14}(d)$
64′	51″	14″	37	25′	—	„	14″	25′	37	51″	64′	—	$H_8(d), H_4(d), H_{11}(d)$
10′	25′	37	57′	64′	—	„	10′	25′	37	57′	64′	—	$H(d), H_3(d), H_5(d)$.

Die Systeme $H(d)$, $H_3(d)$ und $H_5(d)$ haben den metazyklischen Teiler $\{|x, 1+x|, |x, \pm|7|^5x|\}$ der Ordnung $2 \cdot 33 = 66$.

Das System $H_{12}(d)$ hat den metazyklischen Teiler

$$\{|x, 1+x|, |x, \pm|7|x|\}$$

der Ordnung $10 \cdot 33 = 330$ und besitzt die halbmetazyklische Gruppe.

Zusammenfassend haben wir also für $N = 33$ höchstens $4 \cdot 16 + 8 + 2 \cdot 4 + 4 = 84$ verschiedene zyklische Systeme. 78 von diesen Systemen besitzen den zyklischen Teiler $\{s\} = \{x, 1+x\}$; 3 den metazyklischen Teiler $\{|x, 1+x|, |x, \pm|7|^5x|\}$ der Ordnung 66; 2 den metazyklischen Teiler $\{|x, 1+x|, |x, \pm|7|^2x|\}$ der Ordnung 165 und eines die halbmetazyklische Gruppe $\{|x, 1+x|, |x, \pm|7|x|\}$ der Ordnung 330.

§ 22. Wir haben damit für die ersten Werte von $N = 6n + 3$ alle zyklischen Systeme gefunden, die sich nicht durch eine metazyklische Substitution auseinander ableiten lassen. Im folgenden Abschnitte werden wir nun zeigen, dass mit Ausnahme des einen Systems a von 15 Elementen und der beiden Systeme a und b von 21 Elementen diese Systeme keine anderen Substitutionen besitzen, die sie in sich selbst transformieren, als jene des metazyklischen Teilers. Der Satz,[5]) den Herr Prof. Bays in seiner Arbeit für $6n+1$ hierüber vermutet, gewinnt grössere Wahrscheinlichkeit, da er ja auch für alle für $N=6n+3$ betrachteten Fälle uneingeschränkt gilt. Dieser lautet: Wenn zwei zyklische Systeme gleichwertig sind, so kann immer das eine von dem andern durch eine metazyklische Substitution abgeleitet werden.

Es mag Interesse bieten, zu erfahren, welche von diesen Systemen uns die Methode von Netto liefert, wenn $2n+1$ Primzahl ist:

Für $N=15$ geben die Wurzeln 7 und $3'$ das zyklische System a_1^*,
„ $N=21$ „ „ „ $0'$ „ $9'$ „ „ „ c_3^*,
„ $N=33$ „ „ „ $7, 3', 9', 8''$ „ „ „ $H_{10}(d)^*$;
folglich für jedes N nur ein einziges System.

IV. Teil.

§ 23. H. S White hat in seiner 1912 in den Transactions of the A. M. S vol. XIV, 1913, pg. 6, veröffentlichten Arbeit [1]) ein direktes Verfahren angegeben, um verschiedene Dreiersysteme zu erkennen. Herr Prof. Bays hat diese Methode in ihrer Anwendung auf zyklische Systeme der Form $6n+1$ studiert. Die Anwendung dieser Methode auf zyklische Systeme der Form $6n+3$ deckt sich fast vollständig mit jener. Um aber die in den beiliegenden Tabellen enthaltenen Resultate zu verstehen, muss ich vieles anführen, was sich schon in der erwähnten Arbeit findet.[2])

White betrachtet ein Dreiersystem als einen Operator. In einem Dreiersystem ist jeder Zweier der N Elemente mit einem dritten einzigen und wohlbestimmten Elemente zu einem Dreier verbunden. Ein beliebiger Dreier a b c besteht aus den drei Zweiern ab, bc, ca. Ergänzt man nun zu jedem Zweier das dritte Element, das in dem als Operator gebrauchten System (dem Operatorsystem) zu ihm gehört, so bilden diese drei ergänzten Elemente zusammen einen Dreier $a' b' c'$. Dieser neue Dreier ist wieder aus drei Zweiern zusammengesetzt. Ergänzt man

---

[5]) Ibidem, pg. 80. Für diesen Satz wurde kurz vor Drucklegung dieser Arbeit von Herrn Lambossy, Freiburg, der Beweis erbracht für jene Fälle, wo N eine Primzahl oder die Potenz einer Primzahl ist.

[1]) Triple systems as transformations and their paths among triads by H. S. White.

[2]) S. Bays l. c. pg. 81 ff.

wieder zu jedem Zweier das dritte Element, so entsteht durch diese ergänzten Elemente ein neuer Dreier a″ b″ c″; u. s. f. Da aber die Zahl der Dreier für N Elemente gleich $\frac{N(N-1)(N-2)}{6}$, also beschränkt ist, so muss man notwendig nach einer gewissen Zahl solcher Transformationen entweder zu einem Dreier des Operatorsystems oder aber zu einem schon vorher erlangten Dreier kommen. Kommt man zu einem Dreier des Operatorsystems c d e, so wiederholt sich dieser Dreier fortwährend, da ja den drei Zweiern cd, de, ec des Dreiers c d e bzw. e c d, d. h. derselbe Dreier entspricht. Kommt man aber zu einem schon vorher erlangten Dreier, so wiederholt sich dieser periodische Zykel von Dreiern immerfort in der gleichen Reihenfolge.

White nennt diese mittels eines Dreiersystems der N Elemente als Operator auf sämtliche Dreier der N Elemente angewandte Verfahren *duale Transformation*. Die Dreier, die zum Operatorsystem gehören, nennt er *innere Dreier* des Systems, alle andern dagegen *äussere Dreier*. Diejenigen Dreier, auf die kein anderer Dreier führt, d. h. die Köpfe der Reihen, nennt er *primitive* Dreier, während alle andern *abgeleitete* Dreier genannt werden. Den letzten Dreier, der sich unaufhörlich wiederholt, oder die Periode der Dreier, die fortwährend wiederkehrt, nennt er *Endzykel*. Die Ketten der Dreier, die auf den Endzykel führen, nennt er *Appendixe*. Endzykel mit allen Appendixen bilden einen *Zug* (train).

White hat für 13 Elemente folgende Tatsache festgestellt. Sämtliche Züge ergeben eine Ordnung von Dreiern, die invariant ist unter jenen Substitutionen, die das Dreiersystem in sich selbst transformieren und kovariant mit dem Dreiersystem unter der symmetrischen Gruppe von 13 Elementen. Herr Prof. Bays hat diesen Satz verallgemeinernd genauer präzisiert und in folgende Worte gefasst:

Die Form der Züge, in welche sich die Dreier der N Elemente durch die duale Transformation verteilen, ist invariant unter allen Substitutionen der symmetrischen Gruppe der N Elemente, d. h. zwei Dreiersysteme, die unter der dualen Transformation verschiedene Züge ergeben, sind verschiedene Systeme.

Der Inhalt (le contenu) der Züge bleibt unverändert unter jeder Substitution dieser Gruppe, die das Operatorsystem in sich selbst transformiert, d. h. nur die Substitutionen, die jeden dieser Züge in sich selbst oder in einen andern erhaltenen Zug transformieren, können Substitutionen der Gruppe sein, die zum Operatorsystem gehören.

§ 24. Für ein beliebiges Operatorsystem ist diese Methode eine mühsame, zeitraubende Arbeit. Für ein zyklisches Operatorsystem ist die Arbeit bedeutend leichter; denn, wenn der Dreier a b c mittels der dualen Transformation auf a′ b′ c′ führt, so führt der Dreier $a+\alpha$, $b+\alpha$,

$c+a$ auf $a'+a$, $b'+a$, $c'+a$, d. h. bei einem zyklischen Operatorsystem bleibt eine zyklische Kolonne eine zyklische Kolonne, und zwei Dreier der zyklischen Kolonne bewahren gegen einander den gleichen Abstand. Da eine Kolonne nur $\frac{N}{3}$ Glieder hat, so ist damit das Verfahren auf die $\frac{N(N-1)(N-2)-2N}{6N}+1=\frac{N(N-3)}{6}+1$ Köpfe von zyklischen Kolonnen reduziert. Was im letzten Paragraph über Dreier gesagt wurde, dehnt sich unmittelbar auf zyklische Kolonnen aus. Der Ausdruck Dreier kann durch zyklische Kolonne ersetzt werden. Die erste abgeleitete Kolonne gibt eine zweite, diese eine dritte u. s. w. und man muss entweder zu einer Kolonne des Operatorsystems oder zu einer schon vorher erlangten Kolonne gelangen.

Wenn der Zug auf einen Dreier des Operatorsystems, das ist eine *innere* Kolonne, endigt, so gibt es N diesem ähnliche Züge, die wir dadurch erlangen, dass wir zu jedem Elemente des Zuges der Reihe nach $1, 2, 3, \ldots, N-1$ hinzufügen. Endigt der Zug auf einen Dreier der zyklischen Kolonne mit $\frac{N}{3}$ Glieder, die immer eine innere Kolonne des Systems ist, so können wir noch sagen: Es gibt N dem gegebenen ähnliche Züge, aber jeder Dreier des Endzykels kommt dreimal im Abstande $\frac{N}{3}$ vor, oder auch: In diesem Zuge gibt es nur $\frac{N}{3}$ ähnliche Züge, aber jeder Zug hat drei dem gefundenen ähnliche Appendixe, die wir finden, indem wir in den Dreiern zu den Elementen des ersten Appendixes $\frac{N}{3}$ addieren beziehungsweise subtrahieren.

Wenn in einem Zuge eine *äussere* Kolonne wieder erscheint, die schon vorher erlangt wurde, so sind zwei Fälle möglich: Entweder ist für die Periode des Endzykels $n>1$ oder $n=1$.

1. Fall: $n>1$. *a.* Der Dreier der äussern Kolonne, der wieder erscheint, ist derselbe, wie das erste Mal. Graphisch kann man alsdann den Zug betrachten als ein Polygon von n Seiten mit mehr oder weniger regelmässigen Appendixen, und es gibt N dem gegebenen ähnliche Züge. Es genügt, einen davon darzustellen. — *b.* Der Dreier der äussern Kolonne, der sich wiederholt, hat den Abstand a vom ersten. Graphisch kann man diesen Zug als Schraube darstellen, deren Ganghöhe a beträgt. Die Appendixe, die auf den Endzykel führen, haben ihre Dreier in einer Entfernung a in den zyklischen Kolonnen. Haben a und N einen grössten gemeinsamen Teiler $\rho \neq 1$, so zerlegt sich die Schraube in ρ Schrauben mit je $\frac{N}{\rho}$ Windungen. Da alle diese Schraubengänge mit ihren Appendixen einander ähnlich sind, genügt es, einen Gang darzustellen und anzugeben, ob der Gang 0 ist oder welchen grössten gemeinsamen Teiler ρ die beiden Grössen N und a haben.

2. Fall. $n = 1$. Die äussere Kolonne, die wieder erscheint, ist dieselbe, aber der Dreier hat dann notwendig die Entfernung a vom zuerst erlangten. Man könnte diese aufeinander folgenden Dreier des Endzykels als eine arithmetische Reihe betrachten; a wäre dann das arithmetische Mittel. Die Dreier dieser Kolonne bilden einen ebenen Zykel. Wenn a und N keinen gemeinsamen Teiler haben, so hat dieser ebene Zykel N Glieder. Haben aber N und a den grössten Teiler ρ, so zerlegt sich dieser Zykel in ρ kleinere Zykel mit je $\frac{N}{\rho}$ Gliedern. Die Appendixe wiederholen sich für jedes Glied des Zykels und haben ihre Dreier in den entsprechenden zyklischen Kolonnen in einer Entfernung a von den Dreiern, die im vorausgehenden Gliede auf den Endzykel führten. Es genügt, ein Glied dieses ebenen Zykels mit seinen Appendixen darzustellen und anzugeben, ob a und N einen gemeinschaftlichen Teiler haben. (Ueber die beiden Systeme, bei denen sich dieser Fall dargestellt hat, werden wir noch in einem spätern Paragraphen handeln.)

§ 25. Erwähnen wir noch zwei Eigenschaften, die sich bei der Anwendung der dualen Transformation sofort ergeben.

1. Drei aufeinander folgende Dreier in einem Zuge können kein Element enthalten, das sich wiederholt. Es gibt also keine Züge mit einem Endzykel von nur zwei Gliedern. Ein zweifacher Endzykel hat daher eine Ganghöhe $a \neq 0$ und stellt eine Schraube dar.

2. In der Tabelle I, wo die Dreier, die das Element 0 enthalten, aufgeschrieben sind, geht jede Mittellinie AA′, BB′, CC′ durch die $\frac{N-3}{2}$ zyklischen Kolonnen mit den Elementenzweiern, die sich wiederholen. Jedes Dreieck A S B, B S C, C S A enthält in seinem innern ausserhalb der Mittellinien die $\frac{N(N-3)}{6} - \frac{N-3}{2} = \frac{(N-3)^2}{6}$ Kolonnen, deren Elementenzweier sich nicht wiederholen. Da eine metazyklische Substitution eine zyklische Kolonne in eine zyklische Kolonne transformiert, so kann diese Substitution nur die Dreier der Mittellinien A S und S C′ einerseits und die Kolonnen innerhalb A S B ausser S C′ anderseits unter sich vertauschen, d. h. wenn eine metazyklische Substitution ein zyklisches System S in ein zyklisches System S′ transformiert, so müssen, wenn mittels beider Systeme S und S' die duale Transformation durchgeführt wird, die Dreier der Geraden A S und S C′ in beiden Darstellungen an entsprechenden Orten sich finden. Der Endzykel der Kolonne mit $\frac{N}{3}$ Glieder muss in beiden Fällen, wenn er einen Appendix hat, denselben besitzen.

§ 26. Beginnen wir mit dem Studium der Züge für die einzelnen zyklischen Systeme. Wir stellen vorerst eine Tabelle der $N-2+\frac{N-3}{6}N+1$ streng notwendigen Zweier auf; das sind die Zweier der Kombination von 0 mit 1, 2, 3, ... N — 2 und die Zweier des Dreieckes A S B mit Einschluss der Zweier auf den Geraden A S und S C′ vermehrt um den Zweier auf dem Schnittpunkt der Mittellinien. Rechts daneben schreiben wir das Element, das im gewählten Operatorsystem diesem Zweier entspricht. In einer zweiten Tabelle schreiben wir die $\frac{N-3}{6}N+1$ notwendigen Köpfe der zyklischen Kolonnen und rechts daneben die durch duale Transformation hervorgebrachten Dreier und in einer folgenden Kolonne die zu diesen Dreiern gehörigen Köpfe von zyklischen Kolonnen. Ist diese Arbeit ausgeführt, so ist es nur mehr ein Spiel, die Verknüpfung der einzelnen zyklischen Kolonnen darzustellen.

Wie wir gesehen, bleibt die Gesamtheit der Züge invariant für alle dem Operatorsystem gleichwertigen Systeme, und Systeme, deren Züge sich unter verschiedener Form darstellen, sind verschiedene Systeme. Wir müssen also die Dreier nicht aufschreiben, sondern können sie nur durch kurze Striche kenntlich machen. Der Gang der Schraube ist kovariant auch für gleichwertige Systeme; die Anzahl der kürzern Schrauben dagegen, in die sich die ganze Schraube mit N Gängen zerlegt, ist invariant. Diese Anzahl ist in den Tabellen durch eine arabische Ziffer rechts vom Zuge angegeben. Die römische Ziffer links vom Zuge gibt die Anzahl der dem gegebenen ähnlichen Züge an. Innerhalb des Endzykels steht die Zahl 0, wenn wir einen ebenen Zykel haben. Eine zweite Zahl gibt die Zahl der Glieder des Endzykels an, wenn diese grösser als 6 ist. Alle diese Endzykel sind im Uhrzeigersinne dargestellt. Den Endzykel, der zum Operatorsystem gehört, haben wir mit einem kleinen Kreise umgeben. Zwei Kreise umgeben den Endzykel, der zur Kolonne mit $\frac{N}{3}$ Glieder gehört. Drei konzentrische Kreise, die einen Abschnitt umgeben, bezeichnen den Endzykel, der sich im Falle $n = 1$ über eine dem Operatorsystem äussere Kolonne verteilt. In diesem Falle haben wir das arithmetische Mittel a für das gewählte Operatorsystem innerhalb der Kreise angegeben. Die Züge wurden ausgeführt für alle verschiedenen zyklischen Systeme von $N = 15$, 21, 27 und den 12 Systemen der drei letzten Gruppen von 33 Elementen, unter denen alle sich befinden, die einen metazyklischen Teiler haben.

Diese Züge zeigen uns folgendes: Abgesehen vom System a von 15 Elementen und einiger Systeme von 21 Elementen, die auf den ersten Blick eine besondere Anordnung zeigen, erlauben die erlangten Züge in jedem System, aus der Anzahl der für sie möglichen Transformationen oder aus der Anzahl der dem einem Zuge identischen Züge, die Zahl der Substitutionen, die der Ordnung des metazyklischen Teilers entspricht, zu finden, wie sie schon im dritten Abschnitt erlangt wurde. In allen Fällen sehen wir sofort, ob es ausser der zyklischen Substitution noch andere Substitutionen gibt, die das System in sich selbst überführen. Freilich haben wir nachher noch zu untersuchen, ob die auf diese Weise gefundenen Substitutionen auch die übrigen Züge in sich selbst oder in einander überführen oder, was leichter ist, wir nehmen die Prüfung am Dreiersystem selber vor. — Wir haben so das wichtige Resultat: *Die Substitutionen, die die zyklischen Systeme von 15, 21, 27 und 33 Elementen in sich selbst transformieren, sind mit Ausnahme des Systems a von 15 Elementen und eventuell einiger Systeme (a, b, b_1, b_3) von 21 Elementen die metazyklischen Teiler, die im dritten Abschnitte gefunden wurden.*

§ 27. Um die Ordnung der Gruppe des Systems a von 15 Elementen zu finden, wollen wir vorerst einige Eigenschaften von Substitutionengruppen, die auf Dreiersysteme Bezug haben, erwähnen.[3])

1. Jede Substitution der Gruppe, die zwei beliebige Elemente nicht umsetzt, setzt auch ein drittes nicht um, jenes nämlich, das mit jenen zwei zu demselben Dreier gehört. Daher kann eine Gruppe, die zu einem Dreiersystem gehört, höchstens zweifach transitiv sein; denn, wenn der Ort von zwei Elementen bestimmt ist, so kann das dritte Element nicht willkürlich umgesetzt werden.

2. Eine Substitution, die ein Dreiersystem in sich selbst umwandelt, kann nur eine Elementenzahl der Form $6n+1$ oder $6n+3$ nicht umsetzen. n kann dabei auch 0 sein.

3. Lässt eine Substitution n Elemente unverändert und eine andere Substitution weitere α Elemente, so muss α wenigstens $n+1$ sein. Eine Substitution, die ein Dreiersystem von 15 Elementen in sich selbst überführt, kann folglich nur 15, 14, 12, 8 oder 0 Elemente umstellen.

4. Eine Substitutionengruppe, dessen k fach transitiver Teiler zwei beliebige Elemente nicht umsetzt, ist $(k+2)$ fach transitiv.

5. Die Ordnung einer zweifach transitiven Gruppe vom Grade n ist gleich dem Produkte aus $n(n-1)$ und der Ordnung des Teilers der Gruppe, der zwei beliebige Elemente nicht umstellt.

Für das System a von 15 Elementen sind die 12 Dreier, die die Ableitung 014 geben, in drei Gruppen die 4 möglichen Dreier mit jeder Zahlenmenge

$$2, 8, 5, 0' \qquad 3, 4', 7, 9 \qquad 6, 3', 1', 2'.$$

Der Teiler dieser 12 Elemente 2, 8, 5, 0′, ..., der diesen Zug 014 in sich selbst überführt, ist also, wenn die Elemente 0, 1 und folglich 4 nicht umgestellt werden, für die 4 Elemente jeder Gruppe auf drei Arten imprimitiv. Die drei Substitutionen, welche die 4 Dreier der 4 Elemente

[3]) Vergl. Netto: Substitutionentheorie, pg. 223, und Gruppen und Substitutionentheorie, Kap. IX, Transivität.

der ersten Gruppe in sich selbst überführen, wären z. B. ausser der Einheitssubstitution (25) (80'); (28) (50'); (20') (58). Wenn wir nun neben diesem Zuge noch die beiden Züge schreiben, die die abgeleiteten Dreier 028 und 050' ergeben,

$\overline{014}$	$\overline{028}$	$\overline{050'}$
2, 8, 5, 0'	1, 4, 5, 0'	1, 4, 2, 8
3, 4', 7, 9	7, 9, 1', 2'	3, 4', 1', 2'
6, 3', 1', 2'	3, 4', 6, 3'	6, 3', 7, 9

so sehen wir, dass der Teiler der 8 Elemente 3, 4', 7, 9, ..., die das zyklische System in sich selbst umwandeln, noch auf andere Weise imprimitiv ist.

Die Gruppe, die zum System gehört, ist zweifach transitiv, weil man für die nicht umgestellten beiden Elemente jeden beliebigen Zweier der N Elemente nehmen kann und man dabei immer den vorhergehenden analoge Beziehungen findet, wie man leicht sieht, wenn man alle 35 Züge aufschreibt.

Nennen wir G den Teiler der 12 Elemente 2, 8, 5, 0'..., G_1 den Teiler der 8 Elemente 3, 4', 7, 9, ..., die das zyklische System in sich selbst umwandeln, und bezeichnen wir mit $[\rho]$ und $[\rho]_1$ die Zahl der Substitutionen in G beziehungsweise G_1, so haben wir nach einem bekannten Satze der Substitutionentheorie [4])

$$[12] = 12 \left\{ {}^3/_4\,[8]_1 + {}^{11}/_{12}\,[0]_1 \right\}$$
$$[8] = {}^{12}/_4\,[8]_1$$

$[8]_1$ ist die Zahl der Substitutionen der 8 Elemente 3, 4', 7, 9, ..., die das System in sich selbst umwandeln. Nach demselben Satze ist

$[8]_1 = 7$; ferner ist $[0] = 1$ und wir haben

$$\begin{aligned} [12] &= 12 \left\{ {}^3/_4 \cdot 7 + {}^{11}/_2 \right\} = 74 \\ [8] &= {}^{12}/_4 \cdot 7 \qquad\qquad = 21 \\ [0] &= \qquad\qquad\qquad\; = \underline{1} \end{aligned}$$

Die Ordnung des Teilers, der zwei beliebige Elemente nicht umstellt, ist demnach 96. Weil die Gruppe, die zum System gehört, zweifach transitiv ist, so ist die Ordnung der Gruppe des Systems a nach Eigenschaft 5 gleich $15 \cdot 14 \cdot 96 = 20160$, ein Resultat, das schon Miss Cummings, F. Cole und H. White [5]) in ihren Studien über die Systeme von 15 Elementen gefunden haben. Cummings [6]) hat ferner die interessante Tat-

[4]) Netto: Substitutionentheorie, pg. 71. Der Satz lautet: Die Zahl der Substitutionen, die alle n Elemente umstellen, ist gleich $n \left\{ {}^1/_2\,[n-2] + {}^2/_3\,[n-3] + \cdots + \frac{n-q-1}{n-q}\,[q] + \cdots + \frac{n-1}{n}\,[o] \right\}$.

[5]) Proceedings of the Nat. Acad. of Sciences 1917, vol. III_3: The complete enumeration of triad systems in 15 elements by N. Cole, Cummings and H. S. White.

[6]) Transactions of the A. M. S. vol. 15, pg. 311: On a methode of comparaison for triple systems by Louise Cummings.

sache festgestellt, dass dieses zyklische System a gleichwertig ist mit dem Systeme von Kirkmann, das als das älteste Dreiersystem von 15 Elementen bekannt ist.

Es wird nun unsere Aufgabe sein, die Substitutionen zu finden, die unsere Gruppe erzeugen. Mit den Zügen von White macht sich das Studium ohne allzu grosse Schwierigkeiten. Einige Bemerkungen werden uns das Aufsuchen noch erleichtern. — Die Periode jedes Zykels einer Substitution muss ein Teiler von der Ordnung der Gruppe sein. Es gibt immer Substitutionen mit Zykeln, deren Periode eine Primzahl oder ein Vielfaches der Primzahl ist, die in der Ordnungszahl der Gruppe enthalten ist. Da $20160 = 2^5 \cdot 3^2 \cdot 5 \cdot 7$ ist, so muss es unter den Substitutionen solche mit Zykeln von 7 oder 14 Elementen und ferner solche mit 5, 10 oder 15 Elementen geben. Nach Eigenschaft 3 ist die Anzahl der durch Substitutionen umgestellten Elemente 0, 8, 12, 14 oder 15.

Es kann nun die Gruppe für das System a von folgenden 8 Substitutionen erzeugt werden:

$s_1 = (25)(80')(61')(2'3')$ $\quad$ $s_5 = (176)(352')(493')(0'1'4')$

$s_2 = (15)(40')(36)\,3'4')$ $\quad$ $s_6 = (1248)(362'9)(74'3'1')(50')$

$s_3 = (14)(28)(63')(79)$ $\quad$ $s_7 = (1295'1'63)\;(4870'2'3'4')$

$s_4 = (39)(61')(74')\,2'3')$ $\quad$ $s_8 = (01234567890'1'2'3'4')$

s_8 bildet den zyklischen Teiler. $\{\overline{s_6}, \overline{s_8}\}$ bilden den metazyklischen Teiler; und die Komposition der 8 Substitutionen bildet die Gruppe des Systems a der Ordnung 20160.

§ 28. Eine besondere Anordnung zeigen auch die Züge von White für die Systeme a und b von 21 Elementen. Wir haben auf der folgenden Seite von jedem System den zum Studium interessantesten Zug noch einmal dargestellt und dabei die Dreier (nicht nur die Köpfe der zyklischen Kolonnen, die diese Dreier enthalten) angeschrieben. Ein genaueres Studium der Züge liefert für diese Systeme einige höchst interessante Eigenschaften.

1. Es sind dies vorerst die beiden einzigen Systeme, bei denen in dieser Arbeit Züge auf Endzykel endigen, die einer einzigen äussern Kolonne angehören. Für diese Züge haben N und α, (α ist der Abstand zweier Glieder der äussern Kolonne, hervorgebracht durch das Operatorsystem) den grössten gemeinsamen Teiler 7, so dass jeder einzelne von diesen ebenen dargestellten Zykeln zwei dem ersten ähnliche Glieder besitzt. Es haben die Elemente der einzelnen Glieder in der Hälfte der Züge den Abstand 7 und in der andern Hälfte den Abstand 14 voneinander.

2. Diese Darstellung zeigt uns für beide Systeme einen Zug mit der Vierergruppe, d. i. 4 Elemente mit den 4 möglichen Dreiern führen auf

den Endzykel, ferner 6 Züge, in denen sich 8 Elemente auf die 4 primitiven Dreier verteilen, und zwei Züge, in denen alle 12 Elemente der 4 primitiven Dreier verschieden sind. Ferner geben beide Systeme durch duale Transformation 6 Züge von Kolonnen mit Periode 3 und die Züge der Kolonne mit $\frac{N}{3}$ Gliedern.

3. Halten wir vor Augen, dass jede Substitution, die ein System in sich selbst transformiert, einen ausgedehnteren Zug nur in sich selbst oder in einen ähnlichen Zug transformieren kann. Wenn nun die Züge einer einzigen zyklischen Kolonne ein besonderes Aussehen haben, so muss jede Substitution, die zum System gehört, jeden Zug dieser Kolonne entweder in sich selbst oder in einen andern Zug derselben Kolonne überführen. Nun aber bildet die Anzahl der Elemente, die sich auf die primitiven Dreier eines Zuges verteilen, sicher eine Eigentümlichkeit, die einen Zug charakterisieren kann. Folglich kann eine Substitution die Züge, in denen sich 4 Elemente auf die 4 primitiven Dreier verteilen, in Züge mit derselben Eigenschaft umwandeln und ebenso auch Züge, in denen sich 8 bzw. 12 Elemente in die 4 primitiven Dreier verteilen, in Züge mit denselben Eigenschaften.

Der Zug des Kopfes von der Kolonne mit der Vierergruppe lautet für:

System *a*	System *b*
$251'$ $51'0''-(035')-250''$ $21'0''$	$62'5'$ $2'5'8'-(039)-62'8'$ $65'8'$
Der Dreier 035' gehört zu einer äussern Kolonne des Operatorsystems. Wir haben eine Schraube mit Ganghöhe 7.	Der Dreier 039 gehört zu einer innern Kolonne des Operatorsystems. Wir haben einen ebenen Zykel.

Dies vorausgeschickt, ist ein eingehenderes Studium dieser beiden Systeme nicht mehr schwer.

Es gehören die Züge mit der Vierergruppe im Systeme b zu einer einzigen innern Kolonne des Systems, während sie im Systeme a einer äussern Kolonne des Operatorsystems angehören. Diese beiden Kolonnen sind verschieden und können durch keine Substitution in einander übergeführt werden, d. h., die beiden Systeme a und b sind nicht gleichwertig, wie es uns schon die Anwendung der metazyklischen Substitution im dritten Abschnitte zeigte. Wir haben hier das merkwürdige Resultat, dass, obwohl die Gesamtheit der Züge von White für beide Systeme denselben Anblick bietet, die Systeme doch durch keine Substitution in einander übergeführt werden können und nach Definition verschiedene zyklische Systeme sein müssen.

Eine zweite Frage, die etwas schwieriger scheint, ist folgende: Gibt es ausser den Substitutionen des metazyklischen Teilers noch andere, die diese beiden Systeme in sich selbst umändern? Um diese Frage zu lösen, untersuchen wir die zyklische Kolonne mit der Vierergruppe, die sich nur in sich selbst umwandeln kann. Die zyklische Substitution ändert einen beliebigen Zug dieser Kolonne in jeden beliebigen andern Zug derselben Kolonne um. Wenn wir folglich alle verschiedenen Substitutionen haben, die einen beliebigen Zug dieser Kolonne in sich selbst umändern, so ist damit die Frage gelöst.[7])

Wir legen unserer Untersuchung für das System b den dargestellten Zug 039 mit den 4 primitiven Dreiern der 4 Elemente 6, 2′, 5′, 8′ zu Grunde. Geben wir eine beliebige Permutation dieser 4 Elemente, so ist nach einer im Paragraph 27_2 erwähnten Eigenschaft die Stellung dreier anderer Elemente bestimmt. Da ferner noch die zyklische Kolonne mit $\frac{N}{3}$ Glieder als einzige Kolonne von Zügen ohne Appendixen sich nur in sich selbst umwandeln kann, so sind damit die notwendigen Bedingungen gegeben, um nach Wahl der Permutation der 4 Elemente der 4 primitiven Dreier die Stellung jedes beliebigen Elementes in der Substitution zu bestimmen, und zwar haben wir für das System b für jede Permutation der 4 Elemente zwei mögliche Substitutionen. Folglich ändern $2 \cdot 4!$ Substitutionen den ersten Zug dieser Kolonne in sich selbst um. Multiplizieren wir diese Zahl mit $N = 21$, so haben wir 1008 Substitutionen, die diese Kolonne in sich selbst umwandeln. — Für das System a entspricht jeder Substitution, die den Zug 035′ mit den 4 primitiven Dreiern der 4 Elemente 2, 5, 1′, 0″ in sich selbst umändert, für jede Permutation der 4 Elemente 2, 5, 1′, 0″ nur eine Substitution, die den Zug in sich selbst umwandelt, und wir haben nur $N \cdot 4! = 504$ Substitutionen, die diese Kolonne in sich selbst umändern. Wir haben jetzt noch die Prüfung anzustellen, ob diese Substitutionen, die den ersten Zug in sich selbst umändern, auch die andern Züge des Systems in einander überführen. Diese Prüfung kann aber leichter am zyklischen System selbst

[7]) denn, es seien $s_1, s_2 \ldots s_m$ die Substitutionen, die den ersten Zug in sich selbst umändern. Die zyklische Substitution σ_i führt diesen ersten Zug in den beliebigen Zug i derselben Kolonne über. Dann führen $s, \sigma_i, s_2 \sigma_i, \ldots, s_m \sigma_i$ den ersten Zug in den i^{ten} über; diese Substitutionen sind alle untereinander verschieden, da aus $s_\alpha \sigma_i = s_\beta \sigma_i$ folgen würde $s_\alpha = s_\beta$. Es sind dies aber auch alle Substitutionen, die den i^{ten} Zug in sich selbst umwandeln; denn wenn τ eine solche ist, so ist $\tau \sigma^{-1} = s_\alpha$ eine Substitution, die den ersten Zug in sich selbst umwandelt.

vorgenommen werden. Wir erhalten auf diese Weise für die Ordnung der Gruppe, die das System b in sich selbst umwandelt, 1008 und für jene des Systems a 504.

Wir haben im folgenden die Substitutionen, die die Systeme a und b genauer den ersten Zug der zyklischen Kolonne mit der Vierergruppe in sich selbst umwandeln, dargestellt. Wenn wir die drei Zweier, die zu jedem der 7 Elemente des ersten Zuges gehören, in einer Tabelle aufschreiben und in einer zweiten Tabelle die N Zweier der Kolonne mit $\frac{N}{3}$ Glieder, so können wir nach festgesetzter Permutation der 4 Elemente und Bestimmung der Stellung die drei übrigen dadurch gebundenen Elemente die Substitutionen, die den Zug in sich selbst umändern, unmittelbar aufschreiben. Es sind dies für

N = 21. a.

(2) (5) (1′) (0″)	..... (8) (4′) (7′)	(1) (5′) ..... 1.
(25) (1′) (0″)	..... (84′) (7′)	(3) (0′) (05′) (17) (92′) (6′9′)
(21′) (5) (0″)	..... (4′7′) (8)	(1) (5′) (03) (98′) (70′) (46′)
(20″) (5) (1′)	..... (87′) (4′)	(0) (7) (35′) (10′) (69) (3′6′)
(51′) (2) (0″)	..... (87′) (4′)	(0) (7) (35′) (10′) (49′) (2′8′)
(50″) (2) (1′)	..... (4′7′) (8)	(1) (5′) (03) (70′) (62′) (3′9′)
(1′0″) (2) (5)	..... (84′) (7′)	(3) (0′) (05′) (17) (43′) (68′)
(25) (1′0″)	..... (8) (4′) (7′)	(3) (0′) (43′) (68′) (92′) (6′9′)
(21′) (50″)	..... (8) (4′) (7′)	(3) (0′) (46′) (98′) (62′) (3′9′)
(20″) (51′)	..... (8) (4′) (7′)	(3) (0′) (49′) (2′8′) (69) (3′6′)
(251′) (0″)	..... (87′4′)	(6) (3′) (05′3) (92′8′) (10′7) (46′9′)
(250″) (1′)	..... (84′7′)	(4) (8′) (035′) (692′) (170′) (3′6′9′)
(21′0″) (5)	..... (87′4′)	(2′) (9′) (05′3) (10′7) (698′) (43′6′)
(51′0″) (2)	..... (84′7′)	(9) (6′) (035′) (62′8′) (170′) (43′9′)
(251′0″)	..... (4′7′) (8)	(1) (5′) (03) (70′) (43′6′9′) (692′8′)
(250″1′)	..... (87′) (4′)	(0) (7) (35′) (10′) (46′9′3′) (68′92′)
(21′50″)	..... (84′) (7′)	(3) (0′) (05′) (17) (698′2′) (49′3′6′)

N = 21. b.

(6) (2′) (5′) (8′)	..... (0) (3) (9)	{ (7) (4′) ..... 1. (74′) (26′) (0′7′) (41′) (3′0″) (18) (59′)
(62′) (5′) (8′)	..... (09) (3)	{ (0′)(7′)(50″)(3′9′)(24′)(76′)(1)(4)(8)(1′) (0′7′) (53′) (9′0″) (27) (4′6′) (41′) (18)
(65′) (2′) (8′)	..... (03) (9)	{ (2)(6′)(13′)(80″)(70′)(4′7′)(1′)(4)(5)(9′) (26′) (10″) (83′) (77′) (0′4′) (59′) (41′)
(68′) (2′) (5′)	..... (39) (0)	{ (7)(4′)(43′)(1′0″)(27′)(0′6′)(5)(8)(1)(9′) (74′) (40″) (1′3′) (20′) (6′7′) (59′) (18)

(2′5′) (6) (8′)	..... (39) (0)	(7)(4′)(19′)(58)(27′)(0′6′)(4)(1′)(3′)(0″) (74′) (15) (20′) (89′) (6′7′) (41′) (3′0″)
(2′8′) (6) (5′)	..... (03) (9)	(2)(6′)(51′)(49′)(70′)(4′7′)(8)(1)(3′)(0″) (26′) (45) (1′9′) (77′) (0′4′) (18) (3′0″)
(5′8′) (6) (2′)	..... (09) (3)	(0′)(7′)(14)(81′)(24′)(76′)(5)(3′)(9′)(0″) (0′7′) (11′) (48) (27) (4′6′) (59′) (3′0″)
(62′) (5′8′)	..... (0) (3) (9)	(7)(4′)(14)(81′)(50″)(3′9′)(2)(0′)(6′)(7′) (74′) (11′) (48) (53′) (9′0″) (0′7′) (26′)
(65′) (2′8′)	..... (0) (3) (9)	(7)(4′)(13′)(80″)(49′)(51′)(0′)(7′)(2)(6′) (74′) (10″) (45) (83′) (1′9′) (0′7′) (26′)
(68′) (2′5′)	..... (0) (3) (9)	(7)(4′)(19′)(58)(43′)(1′0″)(0′)(7′)(2)(6′) (74′) (15) (89′) (40″) (1′3′) (0′7′) (26′)
(62′5′) (8′)	..... (093)	(4) (1′) (13′9′) (76′0′) (27′4′) (580″) (41′) (10″9′83′5) (20′4′6′7′7)
(62′8′) (5′)	..... (039)	(1) (8) (24′7′) (51′0″) (43′9′) (70′6′) (18) (277′6′4′0′) (40″9′1′3′5)
(65′8′) (2′)	..... (093)	(5) (9′) (143′) (76′0′) (27′4′) (81′0″) (59′) (11′3′840″) (20′4′6′7′7)
(2′5′8′) (6)	..... (039)	(3′) (0″) (149′) (70′6′) (24′7′) (581′) (3′0″) (11′9′845) (277′6′4′0′)
.(62′5′8′)	... (03) (9)	(2) (6′) (143′9′) (581′0″) (70′) (4′7′) (26′) (11′3′5) (40″9′8) (77′) (0′4′)
(62′8′5′)	..... (39) (0)	(7) (4′) (13′9′4)(51′80″) (27′) (0′6′) (74′) (10″9′1′) (483′5) (20′) (6′7′)
(65′2′8′)	..... (09) (3)	(0′) (7′) (19′43′)(51′0″8) (76′) (24′) (07′) (1540″) (89′1′3′) (27) (4′6′)

Für die Systeme b_1 und b_3 von 21 Elementen, deren Ordnung grösser scheint, als der Ordnung des metazyklischen Teilers entspricht, haben wir wiederum eine Kolonne mit der Vierergruppe. Wir sehen aber mittels einer ähnlichen Untersuchung, dass keine Substitutionen ausser jenen des metazyklischen Teilers, diese Systeme in sich selbst umwandeln.

§ 29. Zum Schlusse mag es angebracht sein, einige dieser für $6n+3$ gefundenen Resultate mit jenen zu vergleichen, die Prof. Bays in der schon vielfach erwähnten Arbeit für $6n+1$ Primzahl oder Potenz einer Primzahl gefunden in einer Tabelle nebeneinander darzustellen.

	$N = \begin{smallmatrix}6n+1\\6n+3\end{smallmatrix}$	S_c	S_v	S_z	S_g
$n = 1$	7	1	1	—	1 (168)
	9	0	0	—	—
$n = 2$	13	1	1	—	—
	15	1	2	—	1 (20160)
$n = 3$	19	4	4	1	—
	21	4	7	—	2 $\binom{1008}{504}$
$n = 4$	25	15	12	12	—
	27	9	8	8	—
$n = 5$	31	64	80	63	1 (9999 360)
	33	50	84	78	—

S_c = Anzahl der Systeme der Charakteristiken.

S_v = Anzahl der verschiedenen zyklischen Systeme.

S_z = Anzahl der Systeme mit nur zyklischem Teiler.

S_g = Anzahl der Systeme, deren Gruppen eine höhere Ordnung hat, als dem metazyklischen Teiler entspricht. Die Ordnung ist in Klammer beigefügt.

Auffallend ist in dieser Tabelle die geringe Zahl der verschiedenen zyklischen Systeme für N = 25 und 27, wo N Potenz einer Primzahl ist. Ist ihre Anzahl doch kleiner als die Anzahl der Charakteristiken und für 27 Elemente nur um 1 grösser als für 21. Ferner haben alle Systeme für 25 und 27 Elemente nur den zyklischen Teiler.

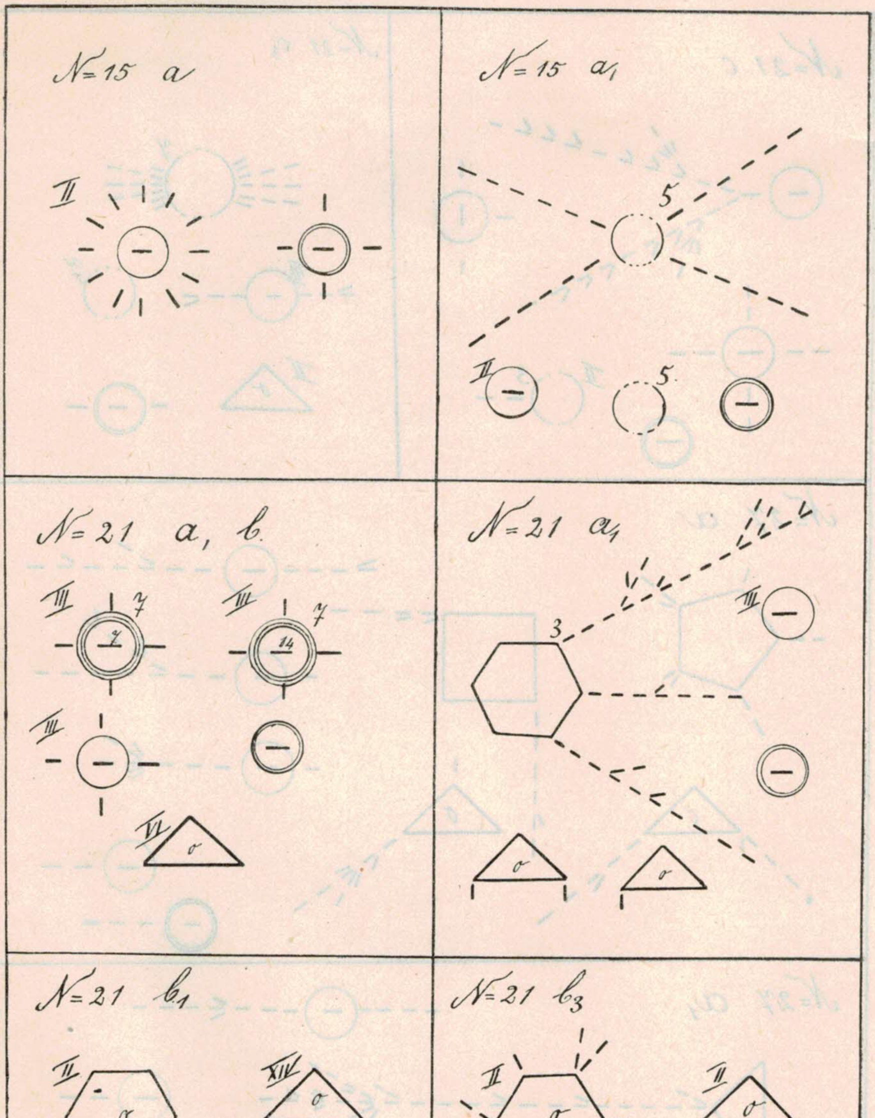
Für jene Systeme von 7, 15 und 31 Elementen, in denen die Ordnung der Gruppe grösser ist, als dem metazyklischen Teiler entspricht, ist die Ordnung das Produkt von verschiedenen Faktoren, die die Anzahl der für 7 bzw. 15 und 31 durch Substitutionen möglicherweise umgesetzten Elemente bezeichnen, wenn für die Einheitssubstitution, die kein Element umstellt, der Faktor 1 genommen wird.

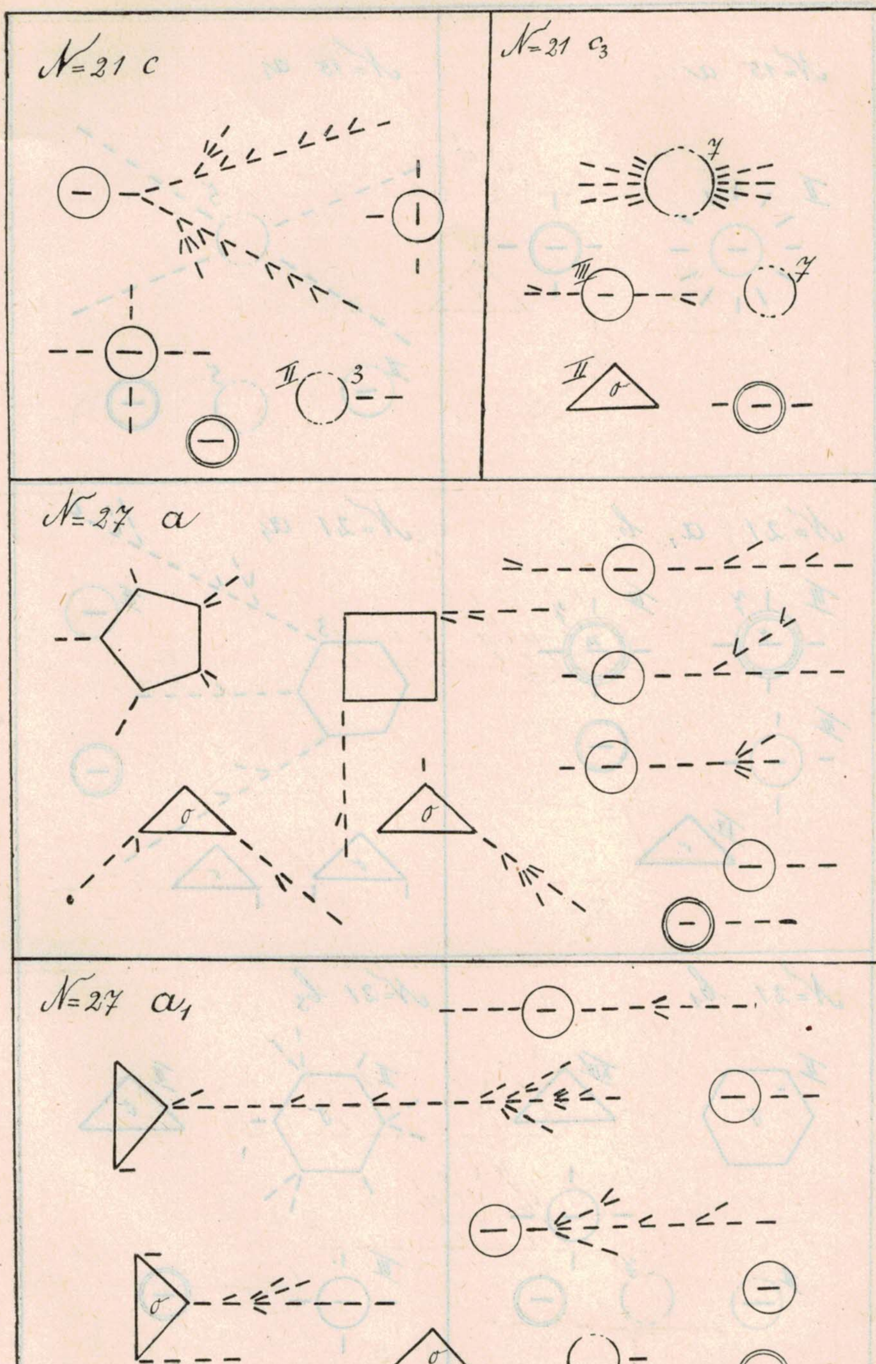
Für die beiden Systeme a und b von 21 Elementen, wo die Anzahl der durch Substitutionen umgesetzten Elemente 21, 20, 18, 12 oder 0 betragen kann, ist diese Ordnung bedeutend kleiner, wie auch die Züge von White zum Voraus zeigten. Gruppentheoretisch legen die Beschaffenheit der Substitutionen wie auch die Züge von White für beide Systeme nahe, dass die Gruppe des Systems a nur eine Untergruppe des Systems b ist, was uns ein eingehenderes Studium dieser Gruppen zeigen dürfte.

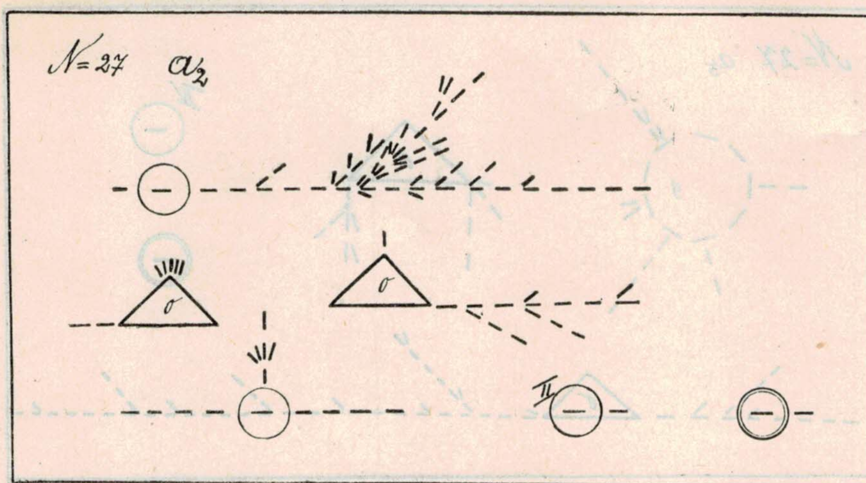
Diese Ausführungen, besonders jene des zweiten und dritten Teiles, zeigen uns aufs neue, wie glücklich und fruchtbringend die Idee von Herrn Prof. Bays war, metazyklische Substitutionen zur Unterscheidung zyklischer Dreiersysteme anzuwenden, indem diese Methode es uns möglich macht, für zyklische Dreiersysteme die zweite Frage des Problems von Steiner für jedes beliebige N vollständig zu lösen und gleichzeitig mit wenigen Ausnahmen die Substitutionengruppen zu finden, die die zyklischen Systeme in sich selbst transformieren.

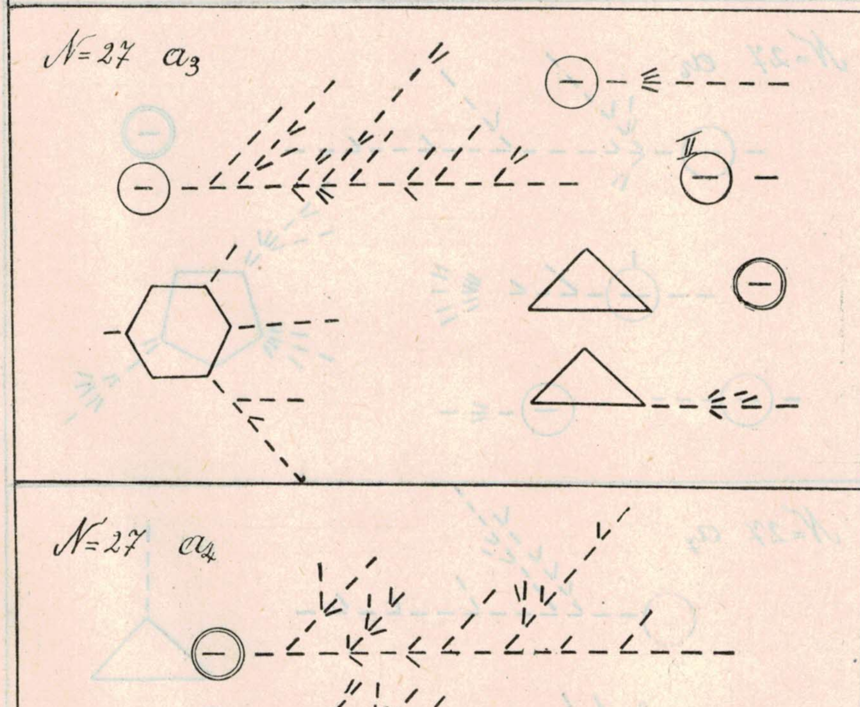
Einige Aenderungen im zweiten Teile hätten es uns erlaubt, diese Theorie auch auf jene Fälle anzuwenden, in denen es keine halbprimitive Wurzeln gibt; aber einerseits ermöglicht es uns diese Methode, bis $N = 63$ die Systeme zu gruppieren, und anderseits würde das Aufsuchen der Systeme der Charakteristiken schon für $N = 61$, wie Prof. Bays bemerkt, praktisch eine allzu grosse Zeit beanspruchen, und dann hätten sich die Resultate auch nicht in solcher Einfachheit dargestellt.

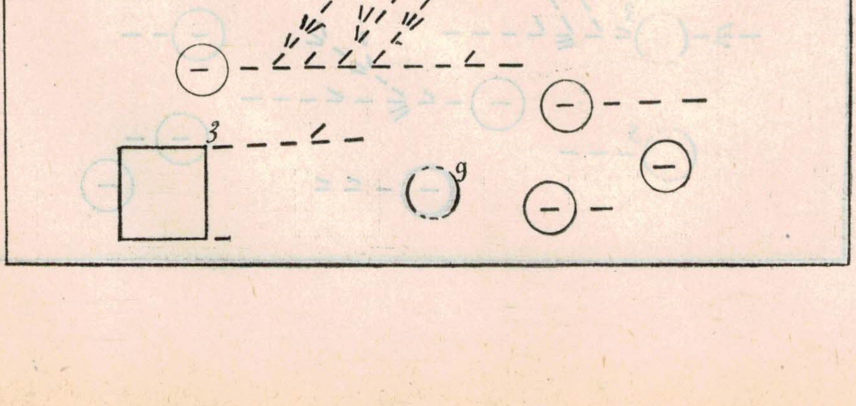
Abschliessend möchten wir noch einmal auf die grosse Uebereinstimmung, die in diesen Studien für $N = 6n + 3$ mit jenen von Prof. Bays für $N = 6n + 1$ angestellten, zu Tage tritt, hinweisen.

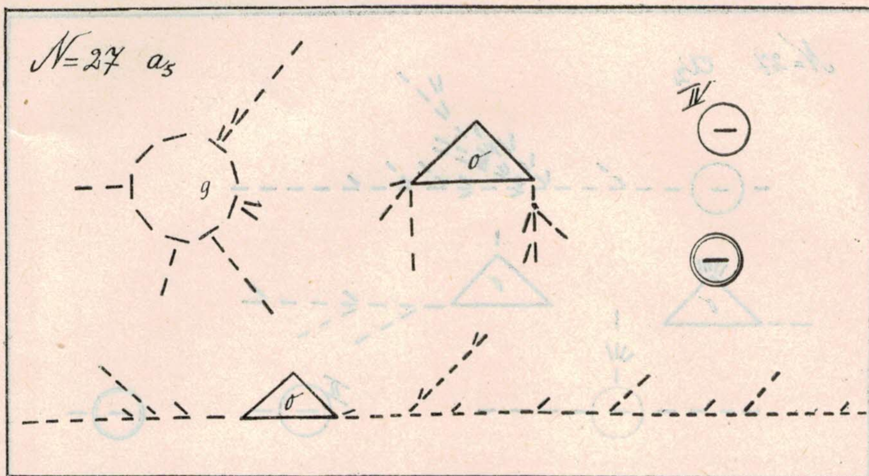

N=15 a
N=15 a1
N=21 a, b.
N=21 a1
N=21 b1
N=21 b3

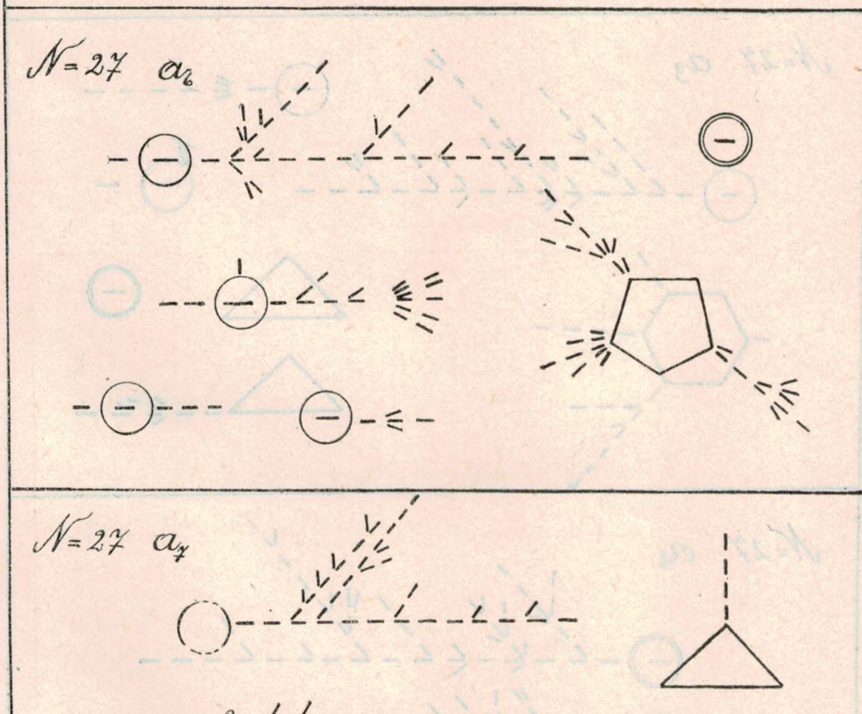

№=21 c
№=21 c_3
№=27 a
№=27 a_1

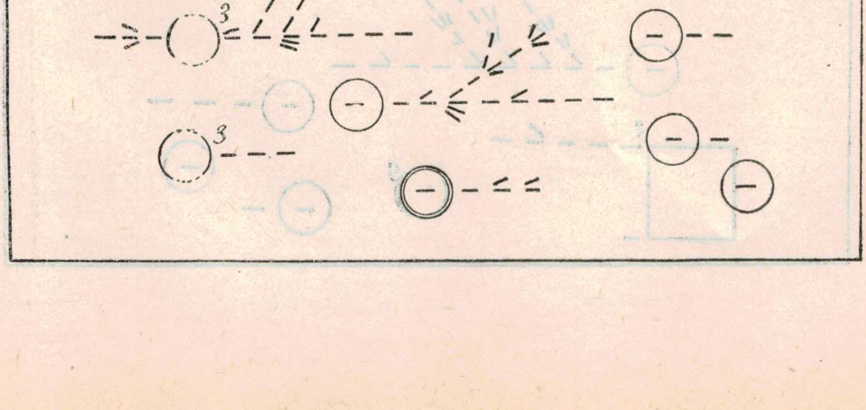

$N=27$ a_2


$N=27$ a_3

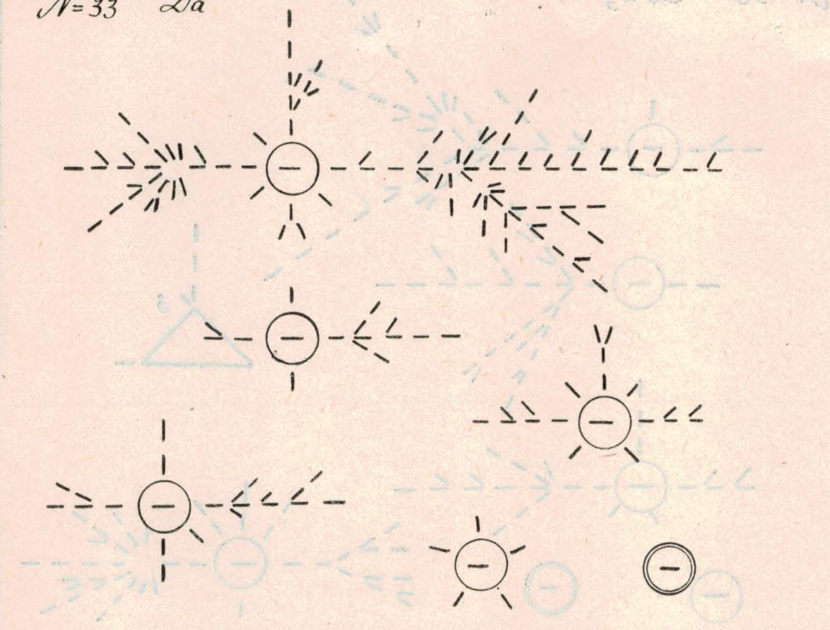

$N=27$ a_4


N=27 a_5
g
б
IV
б

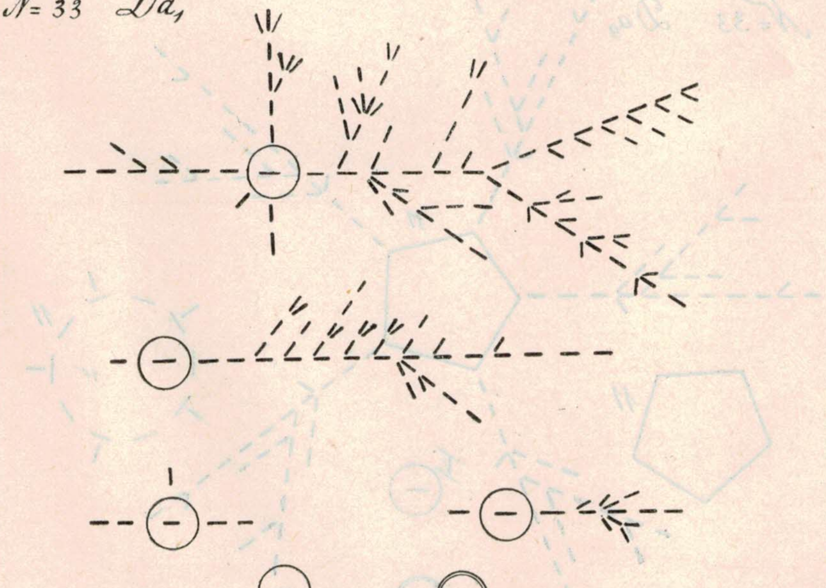

N=27 a_6

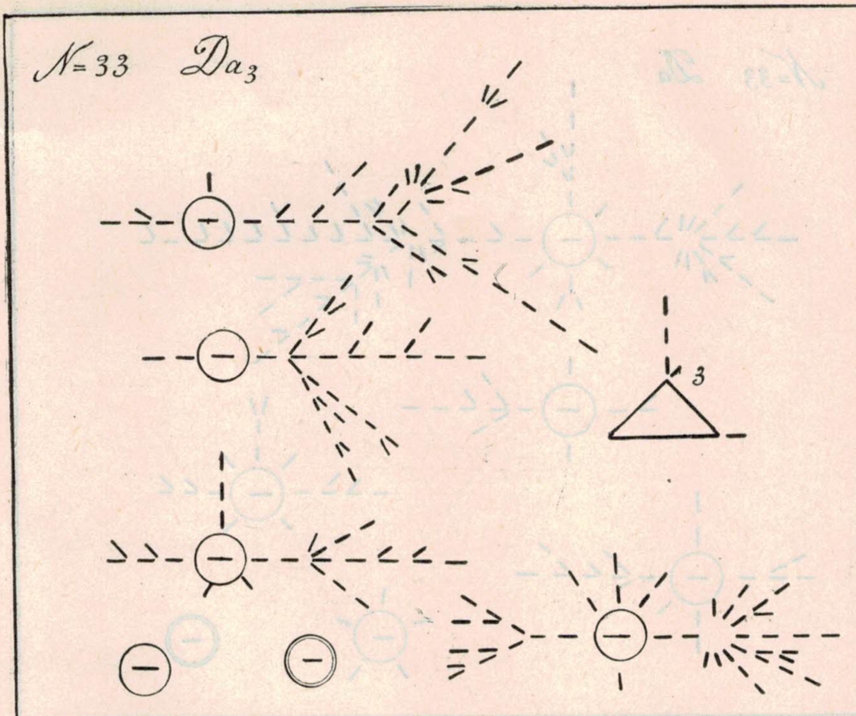

N=27 a_7
3
3

№ = 33 Da

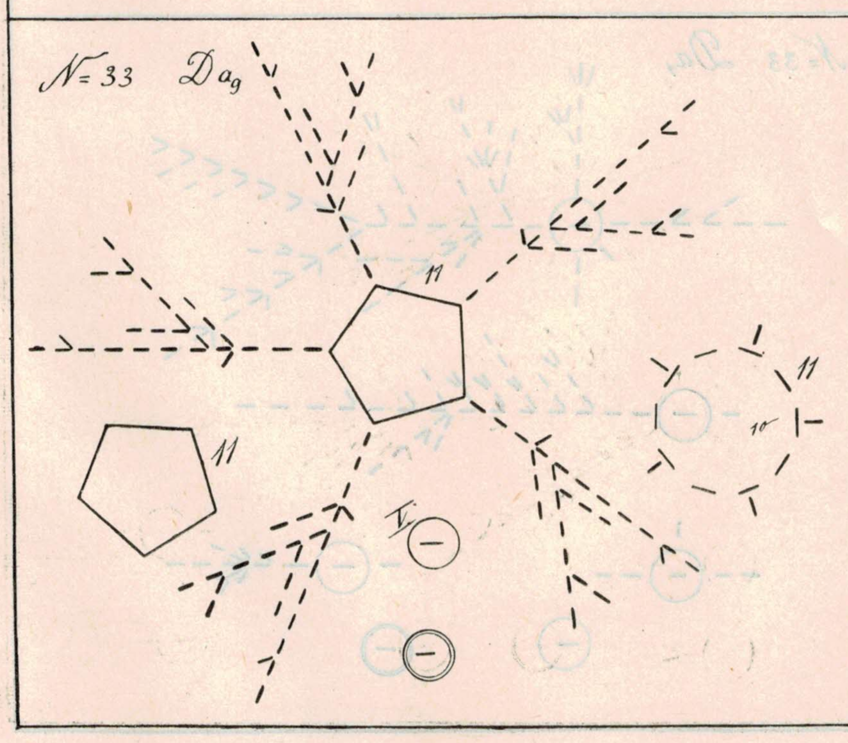


№ = 33 Da_1



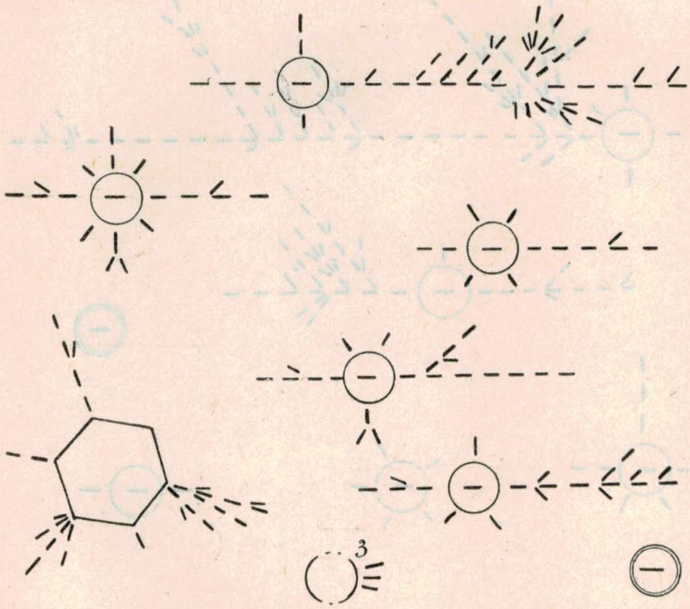


N= 33 Da3
3

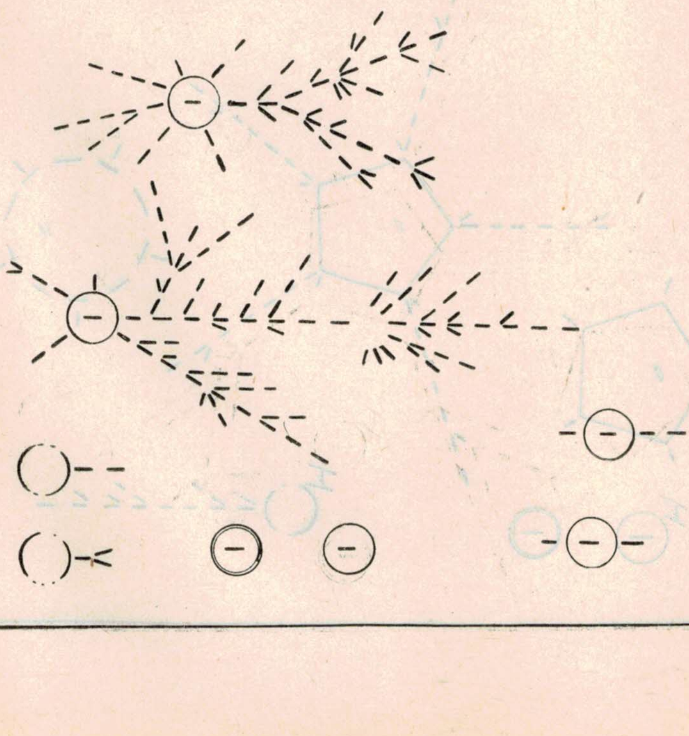


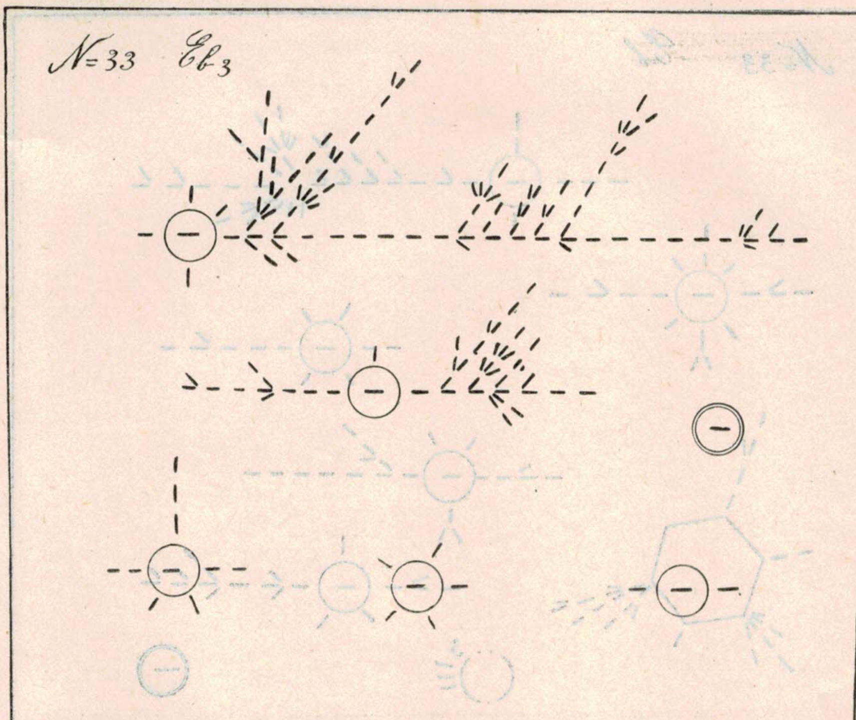
N= 33 Da9
11
11
11
10

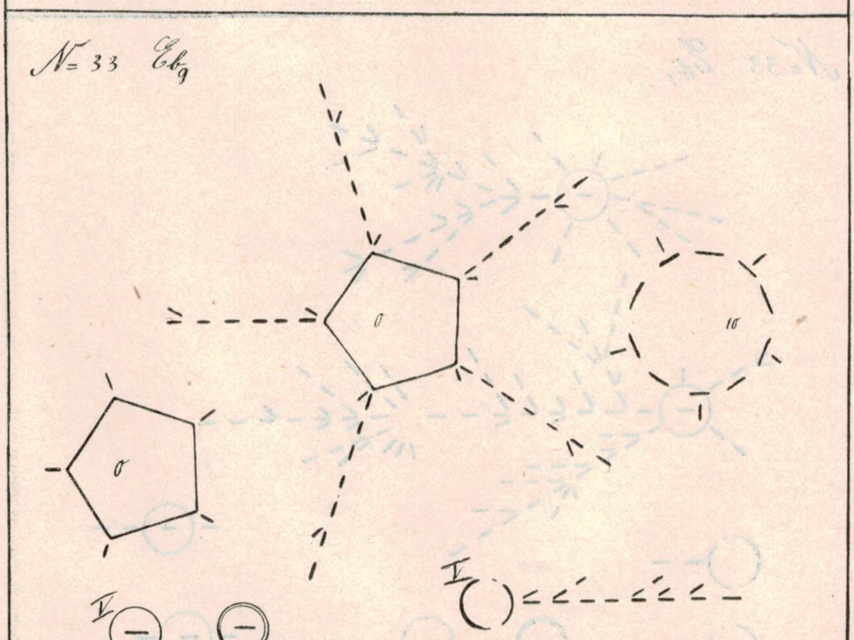
№ 33 Ев

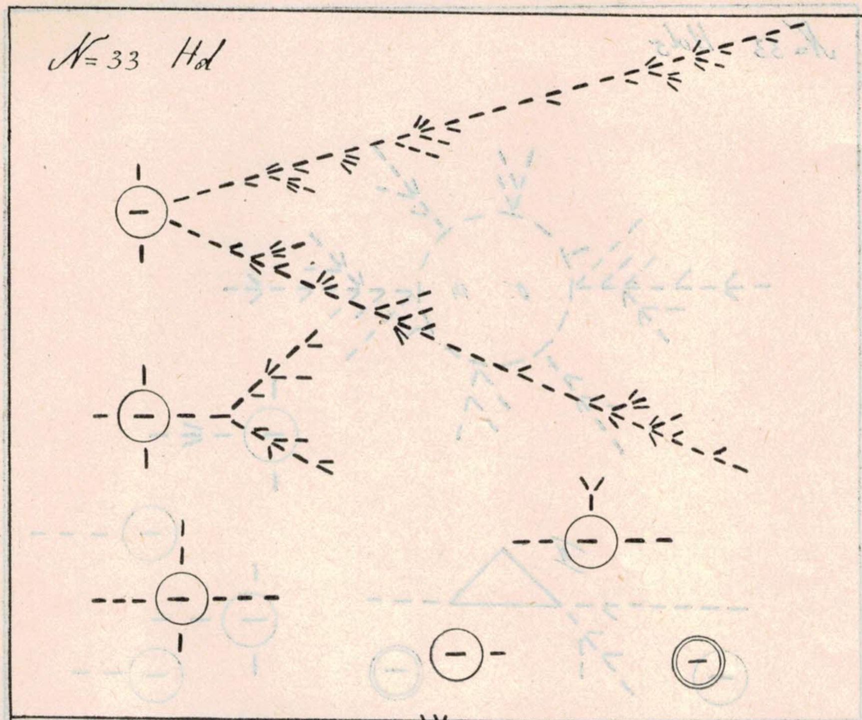


№ 33 Ев$_1$

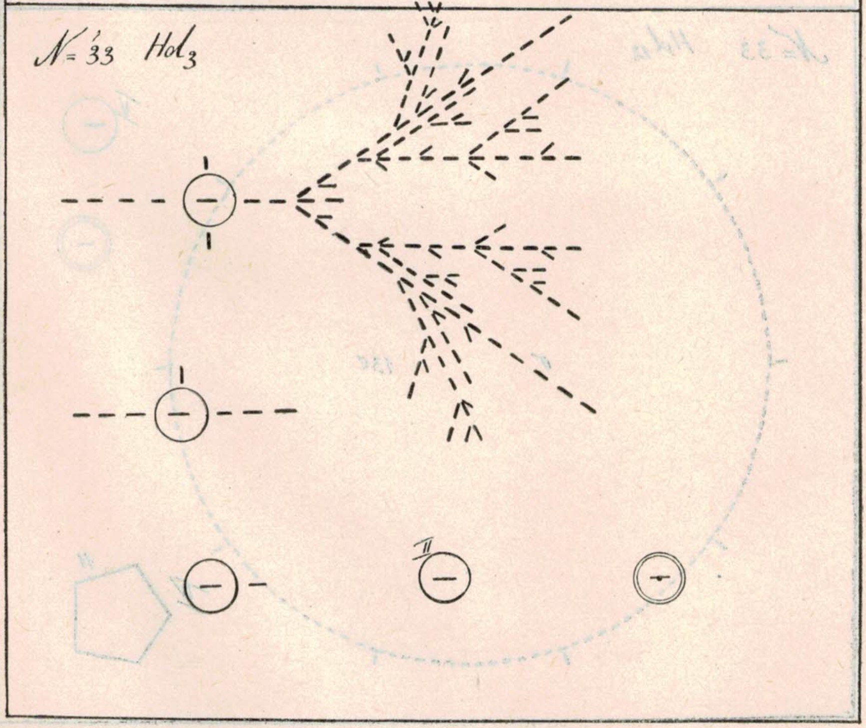



N= 33 Eb-3

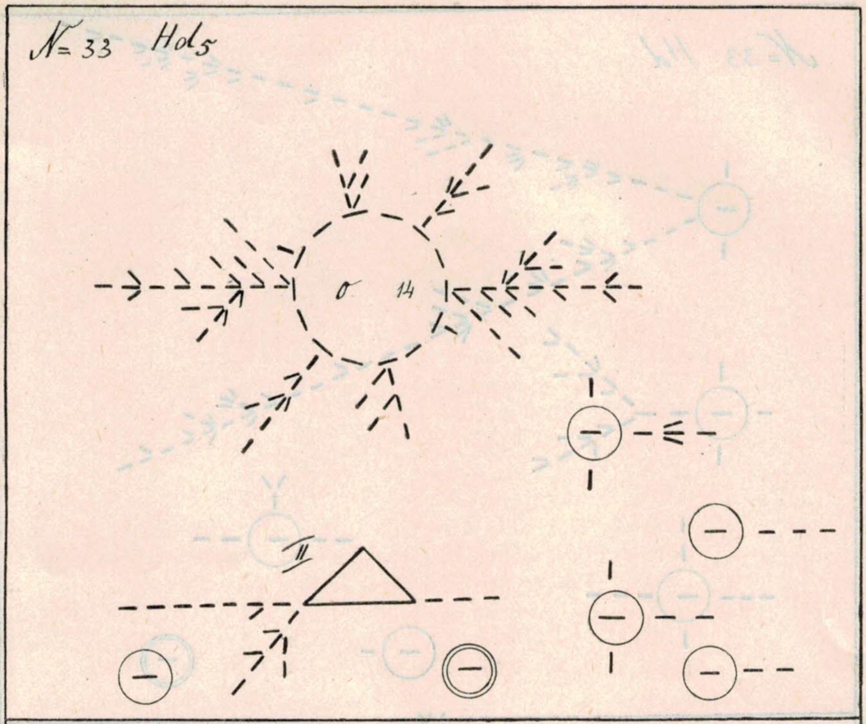

N= 33 Eb9
σ
σ
10
V
V

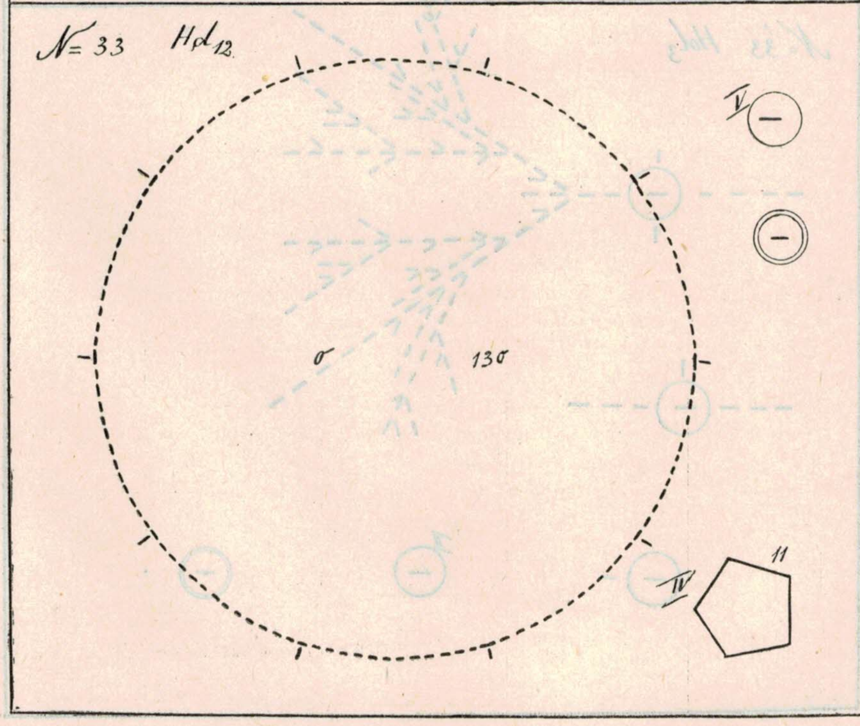


N = 33 Hd



N = 33 Hd₃


N= 33 Hd5
σ 14
II


N= 33 Hd12
V
σ 13σ
IV
11

Benutzte Literatur.

1. P. Bachmann: Grundlehren der neuen Zahlentheorie, Ausg. Schubert. 1907.
2. — Niedere Zahlentheorie, I. Teil. Teubner. 1902.
3. S. Bays: Sur les systèmes cycliques de Steiner. Annales de l'Ecole Normale Sup. 1923, pg. 54.
4. Cambridge Tracts: Chapter IV, metacyclic equations algebraic equations by G. Mathews.
5. Cole: The triad systems of 13 letters, Transactions of the Americ. Math. Soc. vol. 14.
6. Cole, Cummings, White: The complete enumeration of triad systems in 15 elements in Proceedings of the Nat. Acad. of Sciences, vol. III, No. 3, 1916, pg. 197.
7. Cummings: An undervalued Kirkmann paper: Bulletin of the A. M. S. vol. XXIV, pg. 336, 1917.
8. — On a methode of comparaison for triple systems; Transactions of the A. M. S. No. 15, pg. 311 ff.
9. — The trains for the 36 groupless triad systems on 15 elements, Bulletin of the A. M. S., vol. XXV, pg. 321, 1918.
10. Dicksons: Linear groups with an exposition of the Galois field theory. Teubner, 1901.
11. Frobenius: Ueber Gruppen vom Grade p und $p+1$, Berliner Berichte 1902, pg. 351.
12. Heffter: Ueber metazyklische Gruppen und Nachbarkonfigurationen, Mathemat. Annalen 50, pg. 261.
13. Jordan: Recherches sur les substitutions, Journal de Math. pures et appliquées série II, tome 17, pg. 351 ff. 1872.
14. — Traité des substitutions, I. livre. 1871.
15. E. H. Moore: Concerning triple systems, Math. Annalen, vol. 43, pg. 271. 1893.
16. — Concerning Abelian regular transitive triple systems, Math. Ann., vol. 50, pg. 225. 1898.
17. — Tactical memoranda I—III the general tactical configuration, Americ. Journal of Math., vol. 18, pg. 264—303. 1896.
18. Netto: Lehrbuch der Kombinatorik, Kap. 10—11. Teubner 1901.
19. — Gruppen und Substitutionentheorie, Ausg. Schubert. 1905.
20. — Substitutionentheorie und ihre Anwendungen auf die Algebra. Teubner 1882.
21. Serret: Algèbre supérieur, section III, chap. II.
22. White: Triple systems as transformations and their paths among triads, Transactions of the A. M. S., vol. 14.
23. — The multitude of triad systems on 31 letters, Transactions of the A. M. S., vol. 16, pg. 13.