O PODSTAWIENIACH WYMIENNYCH

PRZEZ

DRA M. A. BARANIECKIEGO.

Przedstawiono na posiedzeniu Towarzystwa, dnia 26 maja 1875 roku.

Cauchy (*), a po nim J. A. Serret (**), przy systematycznym wykładzie głównych własności podstawień (na których się opiera cała teorya algiebraicznéj rozwiązalności rownań), dość szczegółowo zajmują się podstawieniami wymiennemi (***). Obaj jednak wspomniani uczeni pewien przypadek szczególny rozważają jako ogólny, co sprawia, że dane przez nich formuły i prawa tworzenia (****) podstawień, wymiennych z daném podstawieniem, nie mają tego stopnia ogólności, jaką oni im przypisują; dlatego téż nie sprawdzają się one w bardzo wielu przypadkach. Wskazaniem właśnie tego zajmuję się w rozdziałach II i III téj rozprawy. — Rozdział IV poświęcony jest wywodowi formuł i reguł mających zastąpić tamte, niedostateczne, a przytém takich, z których poprzednie wyprowadzić się dają, jako szczególny przypadek.

W początkowéj redakcyi téj rozprawy (*****), rozdział Iszy poświęcony był systematycznemu wywodowi tego (co już Cauchy był wypowiedział), że utworzenie podstawienia, wymiennego z daném, sprowadza się do odszukania podstawień częściowych, które otrzymywać należy za pomocą kołowego przestawienia między sobą pewnéj liczby cyklów jednakowego porządku. Obecnie zaś poprzedzam ten wywód niektóremi początkowemi o podstawieniach wiadomościami; one uczynią dostępniejszém czytanie méj pracy i tym, którzy nie zajmowali się teoryą podstawień.

(*) *Exercices d'analyse et de physique mathématique.* Tome III. *Mémoire sur les arrangements, que l'on peut former avec des lettres données, et sur les permutations ou substitutions, à l'aide desquelles on passe d'un arrangement à un autre.*

(**) *Cours d'algèbre supérieure.* 3 éd., tome II, section IV.

(***) Własności podstawień wymiennych mają bezpośrednie nawet zastosowanie w zasadniczéj dla teoryi rozwiązalności równań pracy Galois : *Mémoire sur les conditions de résolubilité des équations par radicaux.* (*Journal* Liouville'a, 1-sza seryja, XI tom).

(****) Bez nich wprawdzie obchodzi się C. Jordan tak w *Commentaire sur Galois* (*Mathematische Annalen* Clebsch'a i Neumann'a, I tom), jak i w *Traité des substitutions et des équations algébriques*; szczegółowe jednak zbadanie własności podstawień wymiennych, które z taką elegancyą Cauchy i Serret przedstawiają, dozwala lepiéj poznać ich naturę i nadal swobodniéj się z niemi obchodzić.

(*****) *Ueber gegen einander permutable Substitutionen.* Inaugural-Dissertation. Leipzig, 1871.

Nadmienię jeszcze, że nie wprowadzałem Jordan'owskiego sposobu symbolizowania podstawień, który, choć bardzo dogodny przy rozbieraniu ogólniejszych kwestyj, potrzebuje jednak pewnego nawyku u czytających — tém więcéj, że tu dość wygodnie można było się obejść bez tego.

ROZDZIAŁ PIERWSZY.

§ 1. — Zestawienie pewnéj ilości *elementów* w jakimbądź oznaczonym porządku będziemy nazywać *układem* (complexio, complexion, arrangement) tych elementów.

Zastąpienie jednego układu drugim, utworzonym z tychże samych, co pierwszy, elementów nazwiemy *podstawieniem* albo *substytucyą*. Dlatego, jeśli na mocy pewnego podstawienia układ, np.

$$abcd\ldots h$$

ma być zastąpiony układem

$$mnop\ldots t,$$

to elementa

$$m, n, o, p, \ldots, t$$

są temiż samemi elementami

$$a, b, c, d, \ldots, h,$$

tak, że te układy mogą się od siebie różnić tylko porządkiem następstwa elementów.

Symbolicznie można przedstawić podstawienie, nadpisując nad danym układem ten, który ma go nastąpić, np. wyżéj przytoczone podstawienie da się przedstawić symbolem

$$\begin{pmatrix} mno\ldots t \\ abc\ldots h \end{pmatrix}.$$

Wygodniéj (i to się zwykle robi) pewną liczbę elementów układu, lub téż wszystkie, oznaczać jakąś jedną głoską ze znaczkami, służącemi do odróżnienia między sobą elementów; tak np., oznaczywszy w naszém podstawieniu

$$a = a_\alpha, \quad b = a_\beta, \quad c = a_\gamma, \ \ldots, \quad h = a_\eta,$$

$$m = a_\lambda, \quad n = a_\mu, \quad o = a_\nu, \ \ldots, \quad t = a_\rho,$$

możemy je przedstawić symbolem

$$\begin{pmatrix} a_\lambda\ a_\mu\ a_\nu \ldots a_\rho \\ a_\alpha\ a_\beta\ a_\gamma \ldots a_\delta \end{pmatrix};$$

znaczki te mogą być także liczbami

§ 2. — Jak układ, tak i podstawienie, może być oznaczane jedną głoską. Np. pewne podstawienie z czterech elementów

$$\begin{pmatrix} a_3\ a_2\ a_1 a_0 \\ a_0\ a_1 a_2\ a_3 \end{pmatrix}$$

nazwijmy S, spodni układ jego symbolu A, a wierzchni B, i oznaczmy

$$a_2\, a_0\, a_1\, a_3 = C,$$

to

$$S = \binom{B}{A};$$

wykonawszy to podstawienie w układach A i C :

$$SA = \binom{B}{A} A = \binom{a_3\, a_2\, a_1\, a_0}{a_0\, a_1\, a_2\, a_3} a_0\, a_1\, a_2\, a_3 = a_3\, a_2\, a_1\, a_0 = B;$$

$$SC = \binom{a_3\, a_2\, a_1\, a_0}{a_0\, a_1\, a_2\, a_3} a_2\, a_0\, a_1\, a_3 = a_1\, a_3\, a_2\, a_0.$$

§ 3. — Wszystkich podstawień, za pomocą których pewien układ danych n elementów, może być zastąpiony wszystkiemi innemi z tychże n elementów możliwemi (a różnemi między sobą) układami, może być, oczywiście, tyle, ile jest możebnych przemian z n elementów, t. j.

$$1.2.3 \ldots n;$$

w téj liczbie zawarte jest i podstawienie, zwane *jednością*, skutkiem którego wszystkie elementa pozostają na swych miejscach, t. j. takie podstawienie, według którego dany układ powinien być zamieniony tym samym układem, np.

$$\binom{a_\alpha\, a_\beta \ldots a_\mu}{a_\alpha\, a_\beta \ldots a_\mu} = 1.$$

Zauważyć należy, że znaczenie podstawienia nie zmienia się, kiedy w jego symbolu zmieniamy porządek następstwa pionowych rzędów (kolumn). Tak np., jeżeli w układzie

$$A = a_0\, a_1\, a_2\, a_3\, a_4\, a_5\, a_6$$

podstawimy elementa według tego, jak wskazuje podstawienie

$$T = \binom{a_5\, a_0\, a_3\, a_6\, a_1\, a_2\, a_4}{a_1\, a_6\, a_3\, a_4\, a_5\, a_0\, a_2},$$

lub też podstawienie

$$T_1 = \binom{a_6\, a_3\, a_1\, a_2\, a_5\, a_4\, a_0}{a_4\, a_3\, a_5\, a_0\, a_1\, a_2\, a_6},$$

to, w obu razach, otrzymamy układ

$$TA = T_1 A = a_2\, a_5\, a_4\, a_3\, a_6\, a_1\, a_0.$$

Z tego wypada, że, gdy wyjdziemy z dwóch różnych układów tychże samych n elementów i nad niemi nadpiszemy po kolei każdy z możliwych

$$1.2.3 \ldots n$$

układów tych elementów, będziemy mieli po dwa jednoznaczne podstawienia; ich symbole przyjmą tęż samą postać, jeśli tylko ich kolumny tak poprzestawiamy, aby w niższych wierszach tenże sam się układ znajdował. Dlatego też może być wszystkiego

$$1.2.3 \ldots n$$

różnych podstawień z danych n elementów.

§ 4. — Na zasadzie niezależności znaczenia podstawienia od porządku, w jakim idą za sobą kolumny jego symbolu, możemy symbol

$$P = \begin{pmatrix} a_4 & a_5 & a_2 & a_6 & a_1 & a_0 & a_3 \\ a_0 & a_1 & a_5 & a_2 & a_4 & a_3 & a_6 \end{pmatrix}$$

zamienić takim

$$P = \begin{pmatrix} a_4 & a_1 & a_5 & a_2 & a_6 & a_3 & a_0 \\ a_0 & a_4 & a_1 & a_5 & a_2 & a_6 & a_3 \end{pmatrix},$$

gdzie spodni element każdéj kolumny jest tenże sam, co wierzchni element kolumny poprzedniéj. Jeżeli przy tém, jak to ma np. miejsce w naszém podstawieniu, wierzchni element ostatniéj kolumny jest tenże sam, co spodni element pierwszéj kolumny, to takie podstawienie nazywa się *kołowém podstawieniem* lub *cyklem*. Symbol kołowego podstawienia P możemy zastąpić takim

$$P = (a_0, a_4, a_1, a_5, a_6, a_3),$$

z którego, przez odrzucenie klamer nawiasu i przecinków, otrzymamy spodni układ poprzedniego symbolu. Z poprzedzającego paragrafu wypada, że możemy zaczynać cykl od któregokolwiek z jego elementów, że zatém np.

$$P = (a_0, a_4, a_1, a_5, a_2, a_6, a_3) = (a_1, a_5, a_2, a_6, a_3, a_0, a_4) = (a_3, a_0, a_4, a_1, a_5, a_2, a_6) = \text{etc.}$$

Ten sposób symbolizowania podstawień można stosować nie tylko do podstawień, tworzących (jak powyższe) tylko jeden cykl, lecz także i do podstawień więcéj złożonych. Tak np. podstawienie

$$T = \begin{pmatrix} a_5 & a_0 & a_3 & a_6 & a_1 & a_2 & a_4 \\ a_1 & a_6 & a_3 & a_4 & a_5 & a_0 & a_2 \end{pmatrix}$$

można jeszcze tak pisać

$$T = \begin{pmatrix} a_2 & a_4 & a_6 & a_0 & a_5 & a_1 & a_3 \\ a_0 & a_2 & a_4 & a_6 & a_1 & a_5 & a_3 \end{pmatrix},$$

lub téż

$$T = (a_0, a_2, a_4, a_6)(a_1\, a_5)(a_3)\,;$$

podstawienie zatém T składa się z trzech cyklów, t. j. ono samo nie jest kołowe, lecz daje się rozłożyć na trzy częściowe podstawienia kołowe. Cykl

$$(a_3) = \begin{pmatrix} a_3 \\ a_3 \end{pmatrix} = 1,$$

jako wskazujący, że element a_3 pozostaje na swém miejscu, mógłby być opuszczonym w ostatnim symbolu podstawienia T; piszemy go jednak ilekroć nam idzie o to, aby ujawnić wszystkie elementa.

§ 5. — Jeżeli mamy w pewnym układzie A przestawić jego elementa według wskazania podstawienia S, następnie zaś jeszcze je przestawić według podstawienia T, to możemy naprzód w wierzchnim układzie dwuwierszowego symbolu podstawienia S poprzestawiać elementa, jak wskazuje podstawienie T, a potém tak otrzymane podstawienie zastosować do układu A. To ostatnie podstawienie, jednoznaczne z kolejném wypełnieniem podstawień S i T, nazywać będziemy *iloczynem* podstawień S i T, i umówimy się, aby mnożnik T pisać z lewéj strony mnożnéj S. Takim sposobem, wypełnienie w ukła-

dzie A *naprzód* podstawienia S, a *następnie* podstawienia T, jest jednoznaczne z przestawieniem elementów układu A, według wskazania iloczynu TS. Np. jeżeli

$$A = a_0\, a_1\, a_4\, a_3\, a_2\, a_5\, a_6,$$

$$S = (a_1,\ a_2\ a_5)(a_3,\ a_4),$$

$$T = (a_2,\ a_3, a_4,\ a_6)(a_1,\ a_5),$$

to

$$TSA = \begin{pmatrix} a_0\, a_5\, a_3\, a_4\, a_6\, a_1\, a_2 \\ a_0\, a_1\, a_2\, a_3\, a_4\, a_5\, a_6 \end{pmatrix} \begin{pmatrix} a_0\, a_2\, a_5\, a_4\, a_3\, a_1\, a_6 \\ a_0\, a_1\, a_2\, a_3\, a_4\, a_5\, a_6 \end{pmatrix} a_0\, a_1\, a_4\, a_3\, a_2\, a_5\, a_6$$

$$= \begin{pmatrix} a_0\, a_3\, a_1\, a_6\, a_4\, a_5\, a_2 \\ a_0\, a_1\, a_2\, a_3\, a_4\, a_5\, a_6 \end{pmatrix} a_0\, a_1\, a_4\, a_3\, a_2\, a_5\, a_6,$$

$$= a_0\, a_3\, a_4\, a_6\, a_1\, a_5\, a_2.$$

Porównywając iloczyn TS z iloczynem ST

$$TS = \begin{pmatrix} a_0\, a_3\, a_1\, a_6\, a_4\, a_5\, a_2 \\ a_0\, a_1\, a_2\, a_3\, a_4\, a_5\, a_6 \end{pmatrix} = (a_0)(a_1,\ a_3,\ a_6,\ a_2,)(a_4)(a_5),$$

$$ST = \begin{pmatrix} a_0\, a_1\, a_4\, a_3\, a_6\, a_2\, a_5 \\ a_0\, a_1\, a_2\, a_3\, a_4\, a_5\, a_6 \end{pmatrix} = (a_0)(a_1)(a_2,\ a_4,\ a_6,\ a_5)(a_3),$$

widzimy, że, w ogólności, iloczyn podstawień zależy od porządku jego czynników.

Gdy mamy w układzie A przestawić między sobą elementa według iloczynu TS podstawień

$$S = \begin{pmatrix} B \\ C \end{pmatrix}, \quad T = \begin{pmatrix} D \\ E \end{pmatrix},$$

to możemy także postąpić takim sposobem. Kolumny symbolu podstawienia T napiszemy w takim porządku, aby w niższym jego wierszu znalazł się układ B; niechaj np.

$$T = \begin{pmatrix} D \\ E \end{pmatrix} = \begin{pmatrix} D' \\ B \end{pmatrix};$$

wtedy (§ 2)

$$TSA = \begin{pmatrix} D' \\ B \end{pmatrix} \begin{pmatrix} B \\ C \end{pmatrix} A = \begin{pmatrix} D' \\ C \end{pmatrix} A.$$

§ **6.** — W przypadku, kiedy iloczyn dwóch podstawień S i T nie zależy od porządku, w jakim je przez siebie mnożymy, t. j. kiedy

$$TS = ST,$$

nazywamy podstawienia S i T wymiennemi między sobą, albo krócéj *podstawieniami wymiennemi* (substitutions permutables, échangeables entre elles). Tak np. podstawienia

$$S = (a_0,\ a_8)(a_1)(a_2,\ a_6)(a_5)(a_7),$$

$$T = (a_0,\ a_4)(a_1,\ a_5)(a_3)(a_4,\ a_6)(a_7)$$

zadosyć czynią « liniowemu symbolicznemu równaniu » (jak je Cauchy nazywa),

$$TS = ST,$$

albowiem, tak dla iloczynu TS, jak i dla iloczynu ST, otrzymujemy podstawienie

$$(a_0, a_6,)(a_1, a_5)(a_2, a_4)(a_3)(a_7).$$

Wymiennemi podstawieniami są, oczywiście, wszystkie te podstawienia, które nie mają spólnych elementów, np.

$$P = (a_0, a_2, a_3)(a_1, a_5),$$

$$Q = (a_4, a_6, a_0, a_7)(a_8, a_9);$$

dlatego też w każdém podstawieniu możemy jego cykle dowolnie przemieszczać między sobą, np.

$$(a_0, a_1, a_2)(a_3, a_4)(a_5, a_6, a_7) = (a_3, a_4)(a_5, a_6, a_7)(a_1, a_2, a_0) = \text{etc.}$$

§ 7. —Iloczyn, powstały z pomnożenia pewnego podstawienia przez siebie dwa lub więcéj razy, nazwiemy *potęgą* tego podstawienia. Tak np.

$$SSS = S^3, \qquad SSS^4 = S^6,$$

$$[(a_1, a_4, a_3, a_6)(a_2, a_5)][(a_1, a_4, a_3, a_6)(a_2, a_5)] = [(a_1, a_4, a_3, a_6)(a_2, a_5)]^2 = (a_1, a_3)(a_4, a_6)(a_2)(a_5).$$

Przez potęgę zero pewnego podstawienia rozumieć będziemy tę jego potęgę, skutkiem któréj wszystkie elementa pozostają na swych miejscach, t. j. (§ 2) podstawienie jedność, tak, że

$$S^0 = 1.$$

Przypuśćmy, że w pewnym układzie przestawimy elementa według wskazania jakiegoś podstawienia S i że następnie wciąż przestawiamy te elementa według tego podstawienia; powtórzywszy tę czynność pewną liczbę razy, dojdziemy nakoniec do układu, z któregośmy początkowo wyszli. Czyli pomnożywszy pewne podstawienie przez siebie kilka razy, dochodzimy do takiéj jego potęgi, która daje podstawienie jedność. Najniższą (a większą od zera) z równych jedności potęg danego podstawienia, najmniejszy z wykładników t. j. kolejnych potęg danego podstawienia, równych jedności, nazywać będziemy *porządkiem* danego podstawienia. Np. podstawienie

$$S = (a_1, a_2, a_5)(a_3, a_4)(a_6, a_7),$$

jest 6^{go} porządku, albowiem w szeregu podstawień

$$S, S^2, S^3, S^4, \ldots$$

pierwszém, równém jedności, jest podstawienie

$$S^6 = S^0 = 1.$$

Przy daném podstawieniu P porządku n^{ego}, porządek podstawienia P^m będzie określony liczbą x, najmniejszą z liczb, zadosyć czyniących związkowi

$$mx \equiv 0 \pmod{n}.$$

Jeżeli podstawienie jest kołowe, to oczywiście, jego porządek jest przedstawiony liczbą elementów cykla. Jeżeli zaś podstawienie składa się z kilku cyklów, które wszystkie mają jednakową liczbę elementów, to ono jest takiegoż porządku, jak którykolwiek cykl, i nazywa się podstawieniem *prawidłowém* (subst. régulière). Np.

$$S = (a_0, a_7, a_2, a_3)(a_4, a_8, a_9, a_{10})(a_6, a_1, a_{11}, a_8)$$

jest podstawienie prawidłowe 4^{ego} porządku. Każde podstawienie można uważać jako iloczyn pewnéj liczby prawidłowych podstawień. Np., jeżeli

$$S = (a_0, a_2)(a_1, a_3, a_4)(a_5)(a_7)(a_6)(a_8)(a_9)(a_{10}),$$

to, nazywając prawidłowe podstawienia

$$(a_0, a_2) = P,$$
$$(a_1, a_3, a_4)(a_6, a_8, a_9) = Q,$$
$$(a_5)(a_7)(a_{10}) = R,$$

możemy podstawienie S przedstawić jako iloczyn

$$S = PQR.$$

§ 8. — Ponieważ w szeregu kolejnych potęg danego podstawienia S porządku s^{ego}

$$1, S, S^2, \ldots, S^{s-1}, S^s = 1, S^{s+1} = S^s S = S, S^{s+2} = S^2, \ldots, S^{2s-1} = S^{s-1}, S^{2s} = 1, \ldots$$

peryod

$$1, S, S^2, \ldots, S^{s-1}$$

wciąż się powtarza, to, przy podnoszeniu podstawienia S do $r^{\text{éj}}$ potęgi, jakiekolwiek byłoby r, byle całkowite, możemy się umówić, aby zawsze przez liczbę r rozumieć najmniejszą dodatną resztę liczby r według modułu s. Wtedy, zamiast potęgi S^{s-1}, możemy pisać S^{-1}, albowiem

$$-1 \equiv s-1 \pmod{s}$$

i, oczywiście,

$$SS^{-1} = SS^{s-1} = S^s = 1;$$

dlatego, jeżeli skutkiem podstawienia S układ A ma być zastąpiony układem B,

$$S = \binom{B}{A},$$

to podstawienie S^{-1} oznacza czynność wprost przeciwną, t. j.

$$S^{-1} = \binom{A}{B}$$

Używanie wykładnika -1 zamiast $s-1$ jest pod tym względem wygodne, że dozwala obchodzić się bez oznaczania porządku tego podstawienia, które mamy podnieść do potęgi na jedność mniejszéj od jego porządku.

Szczególniéj często zdarza się używać téj potęgi przy podstawieniach wymiennych. Jeśli bowiem podstawienia S i T są wymienne, to one zadosyć czynią linijowemu symbolicznemu równaniu (§ 6)

$$TS = ST;$$

mnożąc z prawéj obie strony tego równania przez S^{-1}, otrzymujemy związek

$$T = STS^{-1};$$

niektórzy, jako określenie podstawień wymiennych, stawiają warunek zadosyć uczynienia temu właśnie związkowi.

§ 9. — Jakeśmy widzieli w §§ 4 i 6, znaczenie podstawienia się nie zmienia, jeżeli poprzestawiamy jego cykle między sobą, lub też jeżeli rozpoczynamy cykle rozmaitemi elementami. Jeśli jednak umówimy się, aby między sobą przestawiać tylko cykle tegoż samego porządku, to wszelkie kształty, jakie, przy tém ograniczeniu, możemy nadawać cyklowemu symbolowi danego podstawienia, nazywać będziemy jego *postaciami* (formes). Tak np. symbol podstawienia

$$S=(a_0, a_1, a_2)(a_3, a_4)(a_5, a_8, a_7)(a_6, a_9, a_{10})$$

można pisać także pod postacią

$$S=(a_8, a_7, a_5)(a_4, a_3)(a_0, a_1, a_2)(a_{10}, a_6, a_9), \text{ etc.}$$

Wziąwszy dwie różne postacie danego podstawienia, można łatwo odnaleźć podstawienie, z daném podstawieniem wymienne. Za pomocą np. wypisanych dwóch postaci podstawienia S, znajdziemy odpowiednie z niém wymienne podstawienie. Zamieńmy oba te symbole symbolami dwuwierszowemi:

$$S=\begin{pmatrix} a_1 & a_2 & a_0 & a_4 & a_3 & a_8 & a_7 & a_5 & a_9 & a_{10} & a_6 \\ a_0 & a_1 & a_2 & a_3 & a_4 & a_5 & a_8 & a_7 & a_6 & a_9 & a_{10} \end{pmatrix}=\begin{pmatrix} B \\ A \end{pmatrix},$$

$$S=\begin{pmatrix} a_7 & a_5 & a_8 & a_3 & a_4 & a_1 & a_2 & a_0 & a_6 & a_9 & a_{10} \\ a_8 & a_7 & a_5 & a_4 & a_3 & a_0 & a_1 & a_2 & a_{10} & a_6 & a_9 \end{pmatrix}=\begin{pmatrix} B' \\ A' \end{pmatrix},$$

w których głoski A i A' oznaczają spodnie, głoski zaś B i B' wierzchnie układy.

Przyglądając się tym symbolom, widzimy, że z układu B przechodzi się do układu B' za pomocą tegoż samego podstawienia, za pomocą którego z układu A otrzymuje się układ A', t. j. i tu i tam należy element a_0 zastąpić elementem a_8, i tu i tam element a_1 zastąpić elementem a_7 i t. d. To podstawienie nazwiemy T, t. j.

$$\begin{pmatrix} A' \\ A \end{pmatrix}=\begin{pmatrix} B' \\ B \end{pmatrix}=T=(a_0, a_8, a_1, a_7, a_2, a_5)(a_3, a_4)(a_6, a_{10}, a_9);$$

ztąd (§ 8)

$$T^{-1}=\begin{pmatrix} A \\ A' \end{pmatrix}=\begin{pmatrix} B \\ B' \end{pmatrix};$$

owóż, to podstawienie T jest wymienne z podstawieniem S. Rzeczywiście, utworzmy iloczyn TST^{-1}

$$TST^{-1}=\begin{pmatrix} B' \\ B \end{pmatrix}\begin{pmatrix} B \\ A \end{pmatrix}\begin{pmatrix} A \\ A' \end{pmatrix}=\begin{pmatrix} B' \\ A' \end{pmatrix}=S;$$

widzimy więc, że podstawienie T zadosyć czyni związkowi

$$S=TST^{-1}, \text{ czyli } TS=ST.$$

Symbol podstawienia T możemy także bezpośrednio otrzymać z poprzednich cyklowych symbolów podstawienia S. Nadpiszmy nad symbolem

$$(a_0, a_1, a_2)(a_3, a_4)(a_5, a_8, a_7)(a_6, a_9, a_{10}),$$

symbol

$$(a_8, a_7, a_5)(a_4, a_3)(a_0, a_1, a_2)(a_{10}, a_6, a_9),$$

i następnie, odrzuciwszy klamry nawiasów i przecinki, oddzielające elementa, oba wiersze ujmijmy

w większe klamry

$$\begin{pmatrix} a_8\, a_7\, a_5 & a_4\, a_3 & a_0\, a_1\, a_2 & a_{10}\, a_6\, a_9 \\ a_0\, a_1\, a_2 & a_3\, a_4 & a_5\, a_8\, a_7 & a_6\, a_9\, a_{10} \end{pmatrix} = (a_0, a_8, a_1, a_7, a_2, a_5)(a_3, a_4)(a_6, a_{10}, a_9) = \mathrm{T};$$

i to podstawienie T ma, jak widzimy, tę własność, że « jeżeli je wykonamy w cyklach podstawienia S », (jak się wyraża Cauchy), t. j., jeżeli w cyklowym symbolu podstawienia S, nie ruszając ze swych miejsc ani klamer ani przecinków, poprzestawiamy tylko elementa według tego, jak wskazuje podstawienie T, to otrzymamy (w innéj postaci) cyklowy symbol tegoż samego naszego podstawienia S.

§ **10.** — Jeżeli dwa podstawienia S i T nie mają żadnego spólnego elementu, to one, oczywiście, będą wymiennemi i zadosyć uczynią związkowi

(1) $$\mathrm{TS} = \mathrm{ST}.$$

Jeśliby zaś podstawienia S i T miały mieć niektóre spólne elementa, a prócz tego jeszcze takie, które wchodzą tylko w jedno z tych podstawień, to możemy przyjąć, że one znajdują się także i w drugiém z nich, jako częściowe podstawienia pierwszego porządku (§ **4**), i przy tém możemy się umówić, że takie elementa zawsze ujawniać będziemy. Np. jeśli podstawienia S i T są takie :

$$\mathrm{S} = (a_0, a_4, a_2, a_5)(a_6, a_3),$$
$$\mathrm{T} = (a_0, a_2)(a_4, a_5)(a_{10}, a_7, a_8)(a_1, a_9),$$

to, zamiast nich, możemy rozważać podstawienia

$$\mathrm{S} = (a_0, a_4, a_2, a_5)(a_6, a_3)(a_1)(a_7)(a_8)(a_9)(a_{10}),$$
$$\mathrm{T} = (a_0, a_2)(a_4, a_5)(a_{10}, a_7, a_8)(a_1, a_9)(a_3)(a_6).$$

Takim sposobem potrzeba nam wyłącznie zająć się podstawieniami wymiennemi, mającemi same tylko spólne elementa. Przedstawia się tedy taka kwestya : jakim sposobem, mając dane podstawienie, można odnaleźć wszystkie z niém wymienne podstawienia, utworzone z tychże samych, co i dane podstawienie, elementów; albo ogólniéj, znaleźć warunki, jakim zadosyć winny czynić wymienne podstawienia, mające same tylko spólne elementa.

§ **11.** — Ze związku (1) mamy

(2) $$\mathrm{S} = \mathrm{TST}^{-1},$$

zkąd widać, że podstawienie S pozostaje témże samém, gdy w jego cyklach wykonamy podstawienie T (§ **9**); tym sposobem, podstawienie T prowadzi ze sobą tylko zmianę postaci cyklowego symbolu podstawienia S. Zachodzi tedy zależność między liczbą podstawień T, zadość czyniących związkowi (2), a liczbą postaci, jakie nadać możemy podstawieniu S.

Otrzymamy wszystkie postacie danego podstawienia, we wszelki możliwy sposób przestawiając między sobą cykle jednakowego porządku, a także rozpoczynając każdy z cyklów rozmaitemi jego elementami (§ **9**). Niechaj dane podstawienie S ma m cyklów n^{go} porządku, m_1 cyklów $n_1{}^{\mathrm{go}}$ porządku, i t. d.; wtedy, skutkiem wszelkich przestawień cyklów otrzymamy postaci

$$1.2.3 \ldots m \,.\, 1.2.3 \ldots m_1 \,.\, 1.2.3 \ldots m_2 \ldots$$

Rozpoczynając teraz każdy z cyklów jednéj z tych postaci rozmaitemi jego elementami, otrzymujemy z niéj

$$n^m n_1{}^{m_1} n_2{}^{m_2} \ldots$$

różnych postoci, tak, że liczba

$$1 \cdot 2 \cdot 3 \ldots m \cdot 1 \cdot 2 \cdot 3 \ldots m_1 \ldots n^m \cdot n_1^{m_1} \ldots$$

wyznaczy nam ilość wszystkich różnych postaci naszego podstawienia S.

Jeżeli po prawéj stronie związku (2) wciąż zachowywać będziemy tę samą postać podstawienia S, to rozmaite jego postacie po lewéj stronie otrzymywać będziemy zależnie od podstawienia T. A gdyby w dwóch takich związkach (2) podstawienie T było tém samém (w jakiéjkolwiek postaci), to po lewéj stronie tych związków nie możemy otrzymać różnych postaci podstawienia S; przy różnych zaś podstawieniach T (§ **9**) muszą być także różnemi postacie podstawienia S po lewéj stronie tych związków. Liczba zatém różnych podstawień T, które równaniu (1) zadosyć czynią, jest taż sama, co wyżéj wypisana liczba różnych postaci podstawienia S.

§ **12**. — Podstawienie S możemy rozważać jako iloczyn pewnéj liczby prawidłowych podstawień (§ 7),

$$S = PP_1P_2 \ldots,$$

z których każde składa się odpowiednio z

$$m, m_1, m_2, \ldots$$

cyklów, porządku respective

$$n, n_1, n_2, \ldots$$

Jakeśmy wyżéj (§ **9**) widzieli, dla rozwiązania równania (1), t. j. dla znalezienia zadosyć jemu czyniących podstawień T, należy nad jedną postacią podstawienia S nadpisywać inne jego postacie. I z jakiéjkolwiek wyszlibyśmy postaci podstawienia S, zawsze otrzymywać będziemy (choć w innym porządku) też same podstawienia T i tęż samą ich liczbę. Zauważyć przy tém należy, że zmiany, za pomocą których otrzymujemy różne postacie podstawienia S, wszystkie się odbywają w obrębie każdego prawidłowego podstawienia osobno, t. j. że zmiana zaszła w jedném z podstawień

(3) $$P, P_1, P_2, \ldots,$$

na te części podstawienia T, które powstają z innych z tych prawidłowych podstawień, nie ma żadnego wpływu. Ztąd wypada, że odszukiwane podstawienie T może być przedstawione jako iloczyn kilku podstawień częściowych

(4) $$T = Q\,Q_1\,Q_2 \ldots,$$

z których każde powstaje z odpowiedniego jednego z podstawień (3) i jest z niém wymienne. Ztąd widzimy, że odszukanie podstawienia (4), zadosyć czyniącego równaniu (1), sprowadza się do wyznaczenia prostszych podstawień

$$Q, Q_1, Q_2, \ldots,$$

z których każde jest wymienne z odpowiedniém z prawidłowych podstawień (3).

§ **13**. — Ponieważ podstawienie P składa się z m cyklów porządku n^{ego}, to liczba wartości dla Q_2 zadosyć czyniących związkowi

$$QP = PQ,$$

jest taż sama (§ **11**), co liczba postaci podstawień P, t. j.

$$1 \cdot 2 \cdot 3 \ldots m.n^m.$$

Wszystkie te postacie możemy otrzymać w taki sposób. Uskutecznimy (nie zmieniając początkowych elementów w cyklach) m kołowych kolejnych przestawień wszystkich m cyklów, potém w każdéj z tych m postaci zostawimy nietkniętym jeden cykl, np. ostatni, a pozostałe $m-1$ cyklów kołowo $m-1$ razy przestawimy między sobą, następnie w każdéj z takowych $m(m-1)$ postaci jeszcze jednego cykla, np. przedostatniego, ruszać nie będziemy, inne zaś $m-2$ cyklów kołowo przestawiać będziemy między sobą $m-2$ razy i t. d. Z każdéj tak otrzymanych

$$1.2.3\ldots m$$

postaci otrzymamy znowu n^m różnych od poprzednich i między sobą postaci, jak skoro w pierwszym ich cyklu na pierwszém miejscu stawiać będziemy kolejno każdy z jego n elementów, potém toż samo robić będziemy w drugim cyklu każdéj z tych

$$1.2.3\ldots m.n$$

postaci, toż samo w trzecim i t. d.

Jeśli te ostatnie tylko zmiany uskutecznimy, to nad pewnym cyklem znajdzie się inna jego postać; skutkiem tego w podstawieniu Q znajdzie się jedna z n potęg tego cykla.

Co się zaś tyczy kołowego przestawienia cyklów, to w powyższych postaciach, oczywiście, znajdują się takie, które z danéj postaci powstają skutkiem kołowego przestawienia nie wszystkich, lecz tylko pewnéj liczby cyklów. Kołowo bowiem przestawić np. μ cyklów jest toż samo, co uskutecznić m kołowych przestawień m cyklów (po czém one wracają na swe miejsca), potém $m-1$ kołowych przestawień $m-1$ cyklów (idem), ..., $\mu+1$ kołowych przedstawień $\mu+1$ cyklów, daléj jedno kołowe przestawienie pewnych μ cyklów, następnie $\mu-1$, $\mu-2$, ..., 3, 2 kołowych przestawień odpowiednio takiéjże saméj liczby cyklów. Z tak otrzymanéj postaci, przez zmienianie pierwszych elementów w cyklach, otrzymamy, oczywiście, n^m postaci.

Ztąd widzimy, że w liczbie wyżéj otrzymanych

$$1.2.3\ldots m.n^m$$

postaci podstawienia P znajdzie się każda, powstała skutkiem jednego kołowego przestawienia jakiéjkolwiek liczby jego cyklów.

Wtedy, gdy nad daną postacią podstawienia P wypadnie napisać tęż samą postać, podstawienie Q jest iloczynem cyklów pierwszego porządku, t. j.

$$Q=1,$$

§ **14.** — Jeżeli przestawienie cyklów, uskutecznione w danéj postaci podstawienia P, wyraziliśmy za pomocą dwóch lub więcéj kołowych przestawień, to, jak już wiemy, w liczbie otrzymanych w poprzedzającym paragrafie postaci podstawienia P, znajdują się postacie, powstałe w skutek pojedynczych przestawień kołowych, jakie mamy tu po sobie wykonać. Więc też, nad daną postacią nadpisując każdą z postaci, odpowiadających jednemu z tych przestawień, otrzymujemy jedną z wartości dla podstawienia Q, wymienną z podstawieniem P. A ponieważ, według twierdzenia, jakie daje Cauchy (*), iloczyn kilku podstawień, wymiennych z daném podstawieniem, jest z niém także wymienny, to i iloczyn tych wartości dla Q jest podstawienie wymienne z podstawieniem P. W tym tedy przy-

(*) *Exercices d'anal. et de phys. math.*, tom III, str. 224. (Także przytacza je Serret w *Cours d'algèbre sup.*, 3-cie wyd., tom II, n° 408).

padku, zadanie najprościéj rozwiążemy, znalazłszy oddzielnie czynniki składające szukaną wartość dla Q, z których każdy odpowiada pojedynczemu kołowemu przemieszczeniu pewnéj liczby cyklów, i biorąc następnie iloczyn tych czynników. Jeżeliw tych kołowych przestawieniach są spólne elementa, to czynniki tego iloczynu należy brać w tymże samym porządku, w jakim mają być wykonane odpowiednie pojedyncze kołowe przestawienia.

ROZDZIAŁ II

§ 15. — Cauchy, w *Mémoire sur les substitutions permutables entre elles* (*), a także w *Mémoire sur les arrangements* etc. (**) (§ 9 *Des substitutions permutables entre elles*), mając mówić o podstawieniach wymiennych, rozpoczyna uwagą, że każde podstawienie P może być uważane jako iloczyn kilku podstawień prawidłowych

$$P = \mathfrak{P}\mathfrak{P}'\mathfrak{P}''\ldots,$$

i rozbiera naprzód przypadek, kiedy podstawienie P jest prawidłowe i złożone z h cyklów a^{ego} porządku:

$$P = \mathfrak{P} = \mathfrak{R}\mathfrak{S}\mathfrak{T}\ldots.$$

Uskuteczniając kołowe przestawienie cyklów

$$(\mathfrak{R}, \mathfrak{S}, \mathfrak{T}, \ldots),$$

otrzymuje, jako pierwszy cykl podstawienia Q, wymienionego z podstawieniem P, t. j. zadosyć czyniącego linjowemu symbolicznemu równaniu

$$QP = PQ,$$

następujące podstawienie kołowe

$$(\alpha, \beta, \gamma, \ldots, \lambda, \mu, \nu, \ldots, \varphi, \chi, \psi, \ldots, \ldots); \tag{5}$$

elementa tego kołowego podstawienia można przedstawić tablicą

$$\left\{\begin{array}{l} \alpha, \beta, \gamma, \ldots \\ \lambda, \mu, \nu, \ldots \\ \varphi, \chi, \psi, \ldots \\ \text{etc.}, \end{array}\right. \tag{6}$$

w któréj wszystkie pierwsze elementa poziomych rzędów są wzięte z cykla $\mathfrak{R}$, wszystkie drugie z cykla $\mathfrak{S}$, wszystkie trzecie z cykla $\mathfrak{T}$, i t. d. Oznaczając przez θ liczbę poziomych rzędów téj tablicy, a

---

(*) *Comptes rendues heb. de l'Académie des sciences.* Tome XXI (1845), n° 22.

(**) *l. c.* — Ponieważ Cauchy w dwóch tych pracach używa niejednakowego znakowania, to w przytaczanych ustępach zachowane jest znakowanie z *Exercices*, jako więcéj systematyczne od używanego w *Comptes rendus*.

przez b liczbę wszystkich elementów cykla (5), mamy, oczywiście

$$b = \vartheta h.$$

Wszystkie te elementa, które w odpowiednich cyklach podstawienia P znajdują się na bezpośrednio następujących miejscach, tworzą drugi cykl podstawienia Q

$$(\alpha', \beta', \gamma', \ldots \lambda', \ldots \mu', \nu', \xi', \chi', \psi', \ldots, \ldots),$$

porządek którego jest także przedstawiony liczbą

$$b = \vartheta h;$$

wszystkie następujące elementa tworzą trzeci cykl, i t. d.

§ 16. — Rozważmy naprzód, w jakim przypadku możliwe są drugi i następujące poziome rzędy ablicy (6), t. j. w jakim przypadku ϑ może być różne od jedności i mieć jedną z wartości

$$\delta', \delta'', \ldots, a,$$

gdzie

$$\delta', \delta'', \ldots$$

są dzielnikami liczby a.

Każda z głosek

$$\mathfrak{R}, \mathfrak{S}, \mathfrak{T}, \ldots$$

może oznaczać cykl we wszystkich jego a postaciach, w jakich on może być przedstawiony, przez rozpoczynanie go rozmaitemi elementami. Jeżeli podstawienie

$$(\mathfrak{R}, \mathfrak{S}, \mathfrak{T}, \ldots),$$

czyli podstawienie

$$\begin{pmatrix} \mathfrak{S}\mathfrak{T}\ldots\mathfrak{R} \\ \mathfrak{R}\mathfrak{S}\mathfrak{T}\ldots \end{pmatrix}, \tag{7}$$

w odpowiednich częściach wierzchniego i spodniego układu (oznaczonych jednakowemi głoskami) posiada odpowiednio też same początkowe elementa, t. j., jeżeli te części układów powstały z tychże samych postaci cyklów, wtedy drugi element jednego z cyklów podstawienia Q, który w wierzchnim układzie podstawienia (7) był na miejscu ζ, będzie się znajdował w niższym układzie, oczywiście, na miejscu $\zeta + a$, ten zaś element, który w wierzchnim układzie tegoż podstawienia (7) jest $\zeta + a$, w niższym układzie znajduje się na miejscu $\zeta + 2a$, i t. d. nakoniec ten element, który w wierzchnim układzie znajduje się na miejscu $\zeta + (h-2)a$, jest w niższym układzie elementem $\zeta + (h-1)a^{\text{ym}}$ i ma nad sobą element, który, w razie rozmieszczenia elementów na okręgu koła, powinien się znajdować w niższym układzie na miejscu $\zeta + ah$. Ponieważ jednak wszystkich elementów w układach podstawienia (7) jest ah i

$$\zeta + ah \equiv \zeta \pmod{ah},$$

to ów element jest ten sam, który w niższym układzie zajmuje ζ^{te} miejsce; jest to tedy element, z któregośmy wyszli. Cykl zatém jest już zamknięty. Ztąd widzimy, że jeżeli każdy z cyklów

$$\mathfrak{R}, \mathfrak{S}, \mathfrak{T}, \ldots$$

w téjże saméj postaci był wzięty przy tworzeniu tak wierzchniego jak i spodniego układu podstawienia (7), to koniecznie

$$0 = 1 ;$$

wtedy każdy z cyklów podstawienia Q będzie miał po jednym elemencie z każdego z cyklów podstawienia P, tym sposobem drugiego i wszystkich następnych poziomych rzędów nie będzie w tablicy (6).

§ **17.** — Ażeby więc równość

$$b = h$$

nie miała miejsca, jest warunkiem koniecznym, chociaż, jak to wkrótce zobaczymy, niedostatecznym, aby jeden lub więcéj cyklów były wzięte w innéj postaci, przy tworzeniu wierzchniego układu podstawienia (7), jak przy tworzeniu niższego układu.

Rozważmy naprzód przypadek, kiedy z cyklów

$$\mathfrak{R}, \mathfrak{S}, \mathfrak{T}, \ldots$$

tylko jeden, np. $\mathfrak{T}$, wzięty był w różnych postaciach, przy tworzeniu układów podstawienia (7); dla ogólności dopuścimy, że on jest t^{ym} od początku cyklem podstawienia P. Oznaczmy przez $\mathfrak{T}_{(\tau)}$ tę postać cykla $\mathfrak{T}$, któréj pierwszy element ma znaczek znajdujący się na miejscu $\tau + 1$ w szeregu

$$0, 1, 2, \ldots, a-2, a-1 ;$$

jeżeli ta postać była wzięta przy tworzeniu jednego z układów podstawienia (7), to przy tworzeniu drugiego służyła jedna z postaci

$$\mathfrak{T}_{(0)}, \mathfrak{T}_{(1)}, \ldots, \mathfrak{T}_{(\tau-1)}, \mathfrak{T}_{(\tau+1)}, \ldots, \mathfrak{T}_{(a-1)} ;$$

przyjmijmy, że $\mathfrak{T}_{(\tau_0)}$ i $\mathfrak{T}_{(\tau_1)}$ są postacie odpowiednio użyte przy spodnim i wierzchnim układach, i że

$$\tau_1 - \tau_0 = \pi_\tau ; \text{ wtedy } \pi_\tau \gtrless 0.$$

Ponieważ, w naszym przypadku, wszystkie cykle, poprzedzające $\mathfrak{T}$, były wzięte w jednakowych postaciach, to, ażeby utworzyć pewien cykl podstawienia Q, należy ze spodniego układu brać elementa z miejsc

$$\zeta, \zeta + a, \zeta + 2a, \ldots, \zeta + (t-1)a ;$$

ten zaś element cykla $\mathfrak{T}$, który w wierzchnim elemencie jest na miejscu $\zeta + (t-1)a$, w spodnim układzie znajduje się na miejscu

$$\zeta + \pi_\tau + ta ; \tag{8}$$

przy czém zauważyć należy, że ta liczba (8) jest zawarta między liczbami ta i $(t+1)a$. Jeśli bowiem

$$\zeta + \pi_\tau + ta > (t+1)a, \text{ albo } < ta + 1,$$

to jest

$$\zeta + \pi_\tau > a, \text{ albo } < 1,$$

to przez summę $\zeta + \pi_\tau$ należy rozumieć najmniejszą dodatną resztę liczby $\zeta + \pi_\tau$ według modułu a.

Ponieważ daléj idące części układów w (7) powstały z jednopostaciowych cyklów, to elementa, które z nich bierzemy, wraz z naprzód wziętemi, zajmowały w spodnim układzie miejsca

$$\zeta, \zeta + a, \ldots, \zeta + (t-1)a, \zeta + \pi_\tau + ta, \zeta + \pi_\tau + (t+1)a, \ldots, \zeta + \pi_\tau + (h-1)a;$$

nad ostatnim z nich znajduje się element, który, jako należący do jednopostaciowego cykla, powinien zajmować w spodnim układzie miejsce $\zeta + \pi_\tau + ha$; lecz, że wszystkich elementów jest ah, to on zajmuje istotnie miejsce $\zeta + \pi_\tau$. Ponieważ π_τ mniejsze jest od a i, w naszym przypadku, różne od zera, to nie może być, aby

$$\zeta + \pi_\tau \equiv \zeta \pmod{a},$$

t, j. ów element nie jest ten, z któregośmy wyszli, i cykl nie jest jeszcze zamknięty. Daléj tedy wypadnie brać elementa, które w spodnim układzie były na miejscach

$$\zeta + \pi_\tau, \zeta + \pi_\tau + a, \ldots, \zeta + \pi_\tau + (t-1)a, \zeta + 2\pi_\tau + ta, \ldots, \zeta + 2\pi_\tau + (h-1)a,$$

przy czém znów wypada przez $\zeta + 2\pi_\tau$ rozumieć najmniejszą dodatną resztę téj liczby według modułu a. Jeżeli element, który w wierzchnim układzie zajmuje miejsce $\zeta + 2\pi_\tau + (h-1)a$, nie jest tym samym, co ζ element spodniego układu, t. j. jeżeli nie jest

$$\zeta + 2\pi_\tau \equiv$$

to wciąż daléj brać wypada elementa podstawienia (7), dopóki, po wzięciu elementów z miejsc

$$\zeta + (\theta-1)\pi_\tau, \zeta + (\theta-1)\pi_\tau + a, \ldots, \zeta + \theta\pi_\tau + ta, \ldots, \zeta + \theta\pi_\tau + (h-1)a$$

niższego układu (*), nie natrafimy nakoniec na element, który w spodnim układzie zajmuje miejsce $\zeta + \theta\pi_\tau + ha$, t. j. miejsce $\zeta + \theta\pi_\tau$, przy czém liczba θ zadość czyni porównaniu (**)

$$\zeta + \theta\pi_\tau \equiv \zeta \pmod{a}; \tag{9}$$

wtedy nasz cykl zamyka się.

Z porównania (9) wypada, że

$$\theta\pi_\tau \equiv 0 \pmod{a};$$

jeżeli π_τ i a są liczby pierwsze względem siebie, to, ponieważ π_τ jest różne od zera i mniejsze od a, mamy

$$\theta = a;$$

jeśli jednak liczby a i π_τ posiadają największy spólny dzielnik δ, to wtedy porównanie (9) przechodzi w następujące

$$\theta\frac{\pi_\tau}{\delta} \equiv 0 \left(\mathrm{mod}\ \frac{a}{\delta}\right)$$

z którego, ponieważ $\frac{\pi_\tau}{\delta}$ jest liczba pierwsza względem modułu, wypada, że

$$\theta = \frac{a}{\delta}.$$

(*) Co do liczb $\zeta + 3\pi_\tau, \ldots, \zeta + \theta\pi_\tau$ toż samo zastrzeżenie, co odnośnie do liczb $\zeta + \pi_\tau, \zeta + 2\pi_\tau$.

(**) Wyraz « porównanie », zastąpić mający « kongruencyą » i złożony « równo-resztność », użyty tu jest przez skrócenie, zamiast « porównanie co do reszt ». Odpowiednia nazwa w ruskiéj matematycznéj literaturze (srawnienje), wprowadzona w 1849 r. przez Czebyszowa, już się zupełnie przyjęła.

§ 18. — Jeżeli, w ogóle, postacie cyklów

$$\mathfrak{R},\ \mathfrak{S},\ \mathfrak{T},\ \ldots$$

w spodnim wierszu podstawienia

$$\begin{pmatrix} \mathfrak{RST}.. \\ \mathfrak{ST}..\mathfrak{R} \end{pmatrix}$$

oznaczymy przez

$$\mathfrak{R}_{(\rho_0)},\ \mathfrak{S}_{(\sigma_0)}\ \mathfrak{T}_{(\tau_0)},\ \ldots,$$

w wierzchnim zaś jego wierszu przez

$$\mathfrak{R}_{(\rho_1)},\ \mathfrak{S}_{(\sigma_1)},\ \mathfrak{T}_{(\tau_1)},\ \ldots,$$

przy czém znaczki

$$\rho_0,\ \sigma_0,\ \tau_0,\ \ldots\ ;\quad \rho_1,\ \sigma_1,\ \tau_1,\ \ldots$$

są którekolwiek z liczb

$$0,\ 1,\ 2,\ \ldots\ a-2,\ a-1,$$

i gdy jeszcze nazwiemy

$$\rho_1-\rho_0=\pi_\rho,\ \sigma_1-\sigma_0=\pi_\sigma,\ \tau_1-\tau_0=\pi_\tau,\ \ldots,$$

to wtedy zamknie się cykl odszukiwanego podstawienia, skoro z każdego częściowego podstawienia

$$\mathfrak{R},\ \mathfrak{S},\ \mathfrak{T},\ \ldots$$

weźmiemy już tak wiele elementów, aby ich liczba, którą nazwiemy θ, była liczbą dodatną najmniejszą, zadosyć czyniącą porównaniu

$$\theta(\pi_\rho+\pi_\sigma+\pi_\tau+\ldots)\equiv 0\ (\mathrm{mod}\ a)\ ; \tag{10}$$

i będzie

$$\theta=1,$$

jeżeli

$$\pi_\rho+\pi_\sigma+\pi_\tau\ldots\equiv 0,$$

co możliwe jest, jak w rozbieranym w § 16 przypadku, gdy

$$\pi_\rho=\pi_\sigma=\pi_\tau=\ldots=0,$$

albo téż, gdy summa

$$\pi_\rho+\pi_\sigma+\pi_\tau+\ldots \tag{11}$$

jest dodatną lub odjemną wielokrotnością liczby a. Jeśli zaś ta summa jest liczbą pierwszą względem a, wówczas

$$\theta=a\ ;$$

jeżeli zaś ma z liczbą a największy spólny dzielnik δ, to

$$\theta = \frac{a}{\delta}.$$

W ogóle, jeśli summa (11), albo, ściśléj mówiąc, najmniejsza jéj reszta względem modułu a, ma z liczbą a, jako największy spólny dzielnik, jedną z liczb

$$1,\ \delta',\ \delta'',\ \ldots,\ \frac{a}{\delta'},\quad a,$$

to dla naszéj liczby θ [przedstawiającéj liczbę poziomych wierszy w tablicy (6)] otrzymujemy odpowiednie wartości

$$\theta = a, \frac{a}{\delta},\ \frac{a}{\delta''},\ \ldots,\ \delta',\ 1.$$

§ **19.**—Wróćmy do przypadku, roztrząsanego w § **17**. Przy założeniu, że

$$\pi_\tau < 0, \quad \text{t. j. gdy} \quad \tau_1 < \tau_0,$$

drugi z wziętych z cykla $\mathfrak{A}$ elementów, t. j. ten, który w cyklu $\mathfrak{A}$ stał na miejscu $\zeta + \pi_\tau$, znajduje się w tym cyklu z lewéj strony poprzednio wziętego elementu, t. j. tego, który był na miejscu ζ. Że zaś liczbie τ_1 możemy dowolnie nadać którekolwiek ze znaczeń

$$0, 1, 2, \ldots, \tau_0 - 1, \tau_0 + 1, \ldots, a - 1,$$

to, przy tworzeniu podstawienia Q, bierzemy elementa z cykla $\mathfrak{A}$ w tymże samym porządku, w jakim one się w tym cyklu znajdują, lub też w innym porządku, zależnie od tego, czy

$$\tau_0 < \tau_1 \quad \text{czy téż} \quad \tau_1 < \tau_0;$$

jeżeli np.

$$\tau_1 < \tau_0,\ \tau_1 > a - \tau_0,\ 2\tau_1 > a,$$

to trzecim z wziętych z cykla $\mathfrak{A}$ elementów będzie element, znajdujący się w tym cyklu przed obydwoma już poprzednio wziętemi elementami. Wybierając podobne warunki dla τ_1 zależnie od τ_0, możemy z elementów, wziętych z cykla $\mathfrak{A}$ dla utworzenia cykla podstawienia Q, takie otrzymywać układy, które będą różnemi od układów, jakie téż same elementa (oddzielnie uważane) tworzą w cyklu $\mathfrak{A}$. Ta właśnie odmienność zależną jest, w naszym przypadku, od różnych postaci, jakie nadajemy cyklowi $\mathfrak{C}$.

Toż samo a fortiori miejsce mieć będzie, jeśli weźmiemy przypadek, ogólniejszy od rozważanego, t. j. jeśli nie tylko jeden, ale więcéj cyklów weźmiemy w innéj postaci przy tworzeniu spodniego układu podstawienia (7), jak przy tworzeniu wierzchniego.

Widzimy zatém, że jeżeli z każdego z częściowych podstawień kołowych odszukiwanego podstawienia Q weźmiemy elementa w porządku

$$\alpha, \lambda, \varphi, \ldots$$
$$\beta, \mu, \chi, \ldots$$
$$\gamma, \nu, \psi, \ldots$$
$$\text{etc.},$$

to nie jest bynajmniéj koniecznem, aby te elementa, jak chce Cauchy, miały w tymże samym porządku po sobie następować w odpowiednich cyklach

$$\mathfrak{R},\ \mathfrak{S},\ \mathfrak{T},\ \ldots$$

i odwrotnie, jeśli ta tablica, wziętych dla utworzenia pierwszego cykla podstawienia Q, elementów wskazuje nam porządek, w jakim elementa pierwszego wiersza następują po sobie w cyklu $\mathfrak{R}$, elementa drugiego wiersza w cyklu $\mathfrak{S}$, i t. d., to nie idzie zatém, aby ta tablica zawsze wskazywać nam miała porządek, w jakim te elementa mają po sobie następować w cyklu podstawienia Q.

Dlatego, jeżeli

$$Q = \mathfrak{U}\mathfrak{V}\mathfrak{W}\ldots,$$

przy

$$(12)\qquad \begin{cases} \mathfrak{U} = (\alpha, \beta, \gamma, \ldots, \lambda, \mu, \nu, \ldots, \varphi, \chi, \psi, \ldots, \ldots), \\ \mathfrak{V} = (\alpha', \beta', \gamma', \ldots, \lambda', \mu', \nu', \ldots, \varphi', \chi', \psi', \ldots, \ldots), \\ \text{etc.}, \end{cases}$$

to za tém bynajmniéj nie idzie, aby można było twierdzić, że koniecznie « les variables qui succéderont les unes aux autres, en vertu du facteur circulaire $\mathfrak{R}$ de la substitution P, seront évidemment

$$\alpha, \alpha', \alpha'', \ldots, \lambda, \lambda' \lambda'', \ldots, \varphi, \varphi', \varphi'', \ldots, \ldots,$$

pareillement, les variables, qui succéderont les unes aux autres dans le facteur $\mathfrak{S}$ de la substitution P, seront

$$\beta, \beta', \beta'', \ldots, \mu, \mu', \mu'', \ldots, \chi, \chi', \chi'', \ldots, \ldots;$$

etc. (*). Cykle (12) podstawienia Q nie zawsze to prowadzą za sobą, aby miało być

$$\mathfrak{R} = (\alpha, \alpha', \alpha'', \ldots, \lambda, \lambda', \lambda'', \ldots, \varphi, \varphi', \varphi'', \ldots, \ldots),$$
$$\mathfrak{S} = (\beta, \beta', \beta'', \ldots, \mu, \mu'\mu'', \ldots, \chi, \chi', \chi'', \ldots, \ldots)$$
$$\text{etc. (**).}$$

co tylko w niektórych szczególnych przypadkach miewa miejsce, mianowicie, kiedy nie tylko

$$\rho_1 \leqq \rho_0 + \frac{a}{\theta}, \sigma_1 \leqq \sigma_0 + \frac{a}{\theta}, \tau_1 \leqq \tau_0 + \frac{a}{\theta}, \ldots,$$

lecz jednocześnie jeszcze

$$\pi_\rho + \pi_\sigma + \pi_\tau + \ldots \equiv \frac{a}{\theta} \pmod{a}.$$

§ **20.** — Objaśnijmy na przykładach rezultaty powyższych badań.

Weźmy np. podstawienie

$$P = \mathfrak{R}\mathfrak{S}\mathfrak{T},$$

(*) *Exerc.*, str. 213. *Comp. rend.*, str. 1192.
(**) Ibidem.

gdzie

$$\mathfrak{R} = (\alpha_0, \alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5),$$

$$S = (\beta_0, \beta_1, \beta_2, \beta_3, \beta_4, \beta_5),$$

$$\mathfrak{T} = (\gamma_0, \gamma_1, \gamma_2, \gamma_3, \gamma_4, \gamma_5).$$

Aby utworzyć wartość podstawienia Q, któraby zadość czyniła liniowemu symbolicznemu równaniu

$$QP = PQ,$$

uskutecznijmy przestawienie cyklów w danéj postaci podstawienia P według symbolu

$$(\mathfrak{R}, S, \mathfrak{T}),$$

przyjmując w obu wierszach tego podstawienia jednakowe postacie cyklów, np. postacie

$$\mathfrak{R}_{(0)}, (S_2), \mathfrak{T}_{(5)};$$

wtedy

$$\begin{pmatrix} S_{(2)}\mathfrak{T}_{(5)}\mathfrak{R}_{(0)} \\ \mathfrak{R}_{(0)}S_{(2)}\mathfrak{T}_{(5)} \end{pmatrix} = \begin{pmatrix} \beta_2\beta_3\beta_4\beta_5\beta_0\beta_1\gamma_5\gamma_0\gamma_1\gamma_2\gamma_3\gamma_4\alpha_0\alpha_1\alpha_2\alpha_3\alpha_4\alpha_5 \\ \alpha_0\alpha_1\alpha_2\alpha_3\alpha_4\alpha_5\beta_2\beta_3\beta_4\beta_5\beta_0\beta_1\gamma_5\gamma_0\gamma_1\gamma_2\gamma_3\gamma_4 \end{pmatrix},$$

a ztąd

$$Q = (\alpha_0, \beta_2, \gamma_5)(\alpha_1, \beta_3, \gamma_0)(\alpha_2, \beta_4, \gamma_1)(\alpha_3, \beta_5, \gamma_2)(\alpha_4, \beta_0, \gamma_3)(\alpha_5, \beta_1, \gamma_4).$$

Żeby oznaczyć inną wartość dla Q, nadajmy cyklom rozmaite postacie; np. uskutecznijmy

$$\begin{pmatrix} S_{(0)}\ \mathfrak{T}_{(2)}\ \mathfrak{R}_{(0)} \\ \mathfrak{R}_{(0)}\ S_{(4)}\ \mathfrak{T}_{(4)} \end{pmatrix};$$

otrzymujemy ztąd

$$Q = (\alpha_0, \beta_0, \gamma_4))(\alpha_1\beta_1, \gamma_5)(\alpha_2, \beta_2, \gamma_0)(\alpha_3, \beta_3, \gamma_1)(\alpha_4, \beta_4, \gamma_2)(\alpha_5, \beta_5, \gamma_3);$$

tutaj mieliśmy

$$\pi_\rho = 0,\ \pi_\sigma = -4,\ \pi_\tau = -2,\ a = 6,$$

$$\pi_\rho + \pi_\sigma + \pi_\tau \equiv 0 \pmod{a};$$

dlatego nam wypadło, że

$$0 = 1;$$

weźmy zaś teraz

$$\begin{pmatrix} S_{(2)}\ \mathfrak{T}_{(5)}\ \mathfrak{R}_{(3)} \\ \mathfrak{R}_{(4)}\ S_{(0)}\ \mathfrak{T}_{(2)} \end{pmatrix};$$

z tego podstawienia, t. j. z podstawienia

$$\begin{pmatrix} \beta_2\beta_3\beta_4\beta_5\beta_0\beta_1\gamma_5\gamma_0\gamma_1\gamma_2\gamma_3\gamma_4\alpha_3\alpha_4\alpha_5\alpha_0\alpha_1\alpha_2 \\ \alpha_4\alpha_5\alpha_0\alpha_1\alpha_2\alpha_3\beta_0\beta_1\beta_2\beta_3\beta_4\beta_5\gamma_2\gamma_3\gamma_4\gamma_5\gamma_0\gamma_1 \end{pmatrix},$$

mamy wartość

(13) $$Q = (\alpha_4, \beta_2, \gamma_1, \alpha_2, \beta_0, \gamma_5, \alpha_0, \beta_4, \gamma_3)(\alpha_5, \beta_3, \gamma_2, \alpha_3, \beta_1, \gamma_0, \alpha_1, \beta_5, \gamma_4).$$

w tym tu przypadku

$$\pi_2 = -1,\ \pi_\sigma = 2,\ \pi_\tau = 3;$$

i liczba

$$\pi_2 + \pi_\sigma + \pi_\tau = 4$$

z liczbą

$$a = 6$$

mają największy spólny dzielnik

$$\delta = 2,$$

i, na mocy tego,

$$\theta = 3;$$

widzimy nadto, że gdy tu postacie np. cykla S podstawienia P były

$$(\beta_2, \beta_3, \beta_4, \beta_5, \beta_0, \beta_1),$$

$$(\beta_0, \beta_1, \beta_2, \beta_3, \beta_4, \beta_5),$$

to elementa, wzięte z tego cykla przy formowaniu cyklów podstawienia Q, weszły w nie w takim porządku

$$\beta_2, \beta_0, \beta_4,$$

$$\beta_3, \beta_1, \beta_5,$$

który, oczywiście, różni się od porządku, w jakim idą po sobie te elementa w cyklu S. Wartość zaś (13) istotnie zadosyć czyni równaniu

$$QP = PQ, \text{ albo } QPQ^{-1} = P;$$

oznaczymy bowiem układ, powstały z symbolu podstawienia

$$P = \mathfrak{R}_{(4)}\ S_{(0)}\ \mathfrak{T}_{(2)}$$

skutkiem odrzucenia klamer i przecinków, przez A,

$$A = \alpha_4\ \alpha_5\ \alpha_0\ \alpha_1\ \alpha_2\ \alpha_3\ \beta_0\ \beta_1\ \beta_2\ \beta_3\ \beta_4\ \beta_5\ \gamma_2\ \gamma_3\ \gamma_4\ \gamma_5\ \gamma_0\ \gamma_1,$$

i zastosujemy doń podstawienie (13); otrzymamy układ

$$QA = \beta_2\ \beta_3\ \beta_4\ \beta_5\ \beta_0\ \beta_1\ \gamma_5\ \gamma_0\ \gamma_1\ \gamma_2\ \gamma_3\ \gamma_4\ \alpha_3\ \alpha_4\ \alpha_5\ \alpha_0\ \alpha_1\ \alpha_2,$$

a ztąd (§ 9)

$$QPQ^{-1} = (\beta_2, \beta_3, \beta_4, \beta_5, \beta_0, \beta_1)(\gamma_5, \gamma_0, \gamma_1, \gamma_2, \gamma_3, \gamma_4)(\alpha_3, \alpha_4, \alpha_5, \alpha_0, \alpha_1, \alpha_2),$$

co, oczywiście, jednoznaczne (§§ **4** i **6**) jest z podstawieniem P, albowiem

$$QPQ^{-1} = (\beta_0, \beta_1, \beta_2, \beta_3, \beta_4, \beta_5)(\gamma_2, \gamma_3, \gamma_4, \gamma_5, \gamma_0, \gamma_1)(\alpha_4, \alpha_5, \alpha_0, \alpha_1, \alpha_2, \alpha_3) =$$

$$= (\alpha_4, \alpha_5, \alpha_0, \alpha_1, \alpha_2, \alpha_3)(\beta_0, \beta_1, \beta_2, \beta_3, \beta_4, \beta_5)(\gamma_2, \gamma_3, \gamma_4, \gamma_5, \gamma_0, \gamma_1) = P.$$

§ **21**. — Prawidło, które daje Cauchy dla tworzenia podstawienia wymiennego zdaném podstawie-

niem, nie jest tak ogólne, jak to on utrzymuje. Na mocy tego, co wyżéj było powiedzianém, oczywiście, nie zawsze sprawdzi się to prawidło, polegające na tém, że, aby utworzyć podstawienie, wymienne z daném podstawieniem prawidłowém, należy jego elementa rozmieścić w ϑ tablicach, mających każda h pionowych i k poziomych wierszy:

$$\left\{\begin{array}{l}\alpha,\ \beta,\ \gamma,\ \ldots\\ \alpha',\ \beta',\ \gamma',\ \ldots\\ \alpha'',\ \beta'',\ \gamma'',\ \ldots\\ \text{etc.}\end{array}\right.$$

$$\left\{\begin{array}{l}\lambda,\ \mu,\ \nu,\ \ldots\\ \lambda',\ \mu',\ \nu',\ \ldots\\ \lambda'',\ \mu'',\ \nu'',\ \ldots\\ \text{etc.}\end{array}\right. \tag{14}$$

$$\left\{\begin{array}{l}\varphi,\ \chi,\ \psi,\ \ldots\\ \varphi',\ \chi',\ \psi',\ \ldots\\ \varphi'',\ \chi'',\ \psi'',\ ,\cdot\\ \text{etc.},\\ \text{etc.}\end{array}\right.$$

i z nich brać, «à la suite les unes des autres», elementa wierszy pionowych przy tworzeniu cyklów

$$\mathfrak{R},\ \mathfrak{S},\ \mathfrak{T},\ \ldots,$$

i także, w ściśle tym samym porządku, brać elementa wierszy poziomych przy tworzeniu cyklów

$$\mathfrak{U},\ \mathfrak{V},\ \mathfrak{W},\ \ldots\ (*).$$

Również, nie zawsze sprawdza się metoda, jaką Cauchy podaje dla utworzenia podstawienia

$$\Theta = P^k = Q^h, \tag{15}$$

t. j. iloczyn wszystkich częściowych podstawień kołowych

$$\left\{\begin{array}{l}(\alpha,\ \lambda,\ \varphi,\ \ldots)(,\quad \chi,\ \ldots)(\gamma,\ \nu,\ \psi,\ \ldots)\\ (\alpha',\lambda',\varphi',\ldots)(\beta',\ \mu',\ \chi',\ \ldots)(\gamma',\ \nu',\ \psi,\ \ldots\\ \text{etc.}\end{array}\right.$$

(to podstawienie jest ϑ^{ego} porządku), które, według jego prawidła, powstaje, gdy dla utworzenia któregokolwiek cyklu weźmiemy «à la suite les unes des autres» elementa symetrycznie rozlokowane w tablicach (14) (**). I sam związek (15) nie zawsze ma miejsce.

W rozpatrywanym w § **20** przykładzie, mieliśmy jako wartość (13) dla podstawienia Q, podstawienie,

---

(*) *Exerc.*, str. 214, 217. *Comp. rend.*, str. 1194, 1195.
(**) *Exerc.*, str. 215. *Comp. rend.*, str. 1198.

którego elementa dadzą się takim sposobem rozmieścić w tablicach, podobnych tablicom (14),

$$(p)\quad \begin{cases} \alpha_4, \beta_2, \gamma_1 \\ \alpha_5, \beta_3, \gamma_2 \end{cases}$$

$$(q)\quad \begin{cases} \alpha_2, \beta_0, \gamma_5 \\ \alpha_3, \beta_1, \gamma_0 \end{cases}$$

$$(r)\quad \begin{cases} \alpha_0, \beta_4, \gamma_3 \\ \alpha_1, \beta_5, \gamma_4; \end{cases}$$

pionowe wiersze tych tablic tworzą tedy cykle podstawienia P, jak tylko elementa tych wierszy bierzemy nie w porządku tablic

$$(p),\ (q),\ (r);\ \text{albo}\ (q),\ (r),\ (p);\ \text{albo}\ (r),\ (q),\ (p),$$

(jak to chce mieć Cauchy), lecz w takim :

$$(p),\ (r),\ (q);\ \text{albo}\ (q),\ (p),\ (r),\ \text{albo}\ (r),\ (q),\ (p);$$

także i iloczyn

$$\begin{cases} (\alpha_4, \alpha_0, \alpha_2)(\beta_2, \beta_4, \beta_0)(\gamma_1, \gamma_3, \gamma_5) \\ (\alpha_5, \alpha_1, \alpha_3)(\beta_3, \beta_5, \beta_1)(\gamma_2, \gamma_4, \gamma_0) \end{cases}$$

albo, co jedno,

$$\begin{cases} (\alpha_0, \alpha_2, \alpha_4)\ (\beta_0, \beta_2, \beta_4)\ (\gamma_1, \gamma_3, \gamma_5) \\ (\alpha_1, \alpha_3, \alpha_5)\ (\beta_1, \beta_3, \beta_5)\ (\gamma_0, \gamma_2, \gamma_4) \end{cases}$$

t. j. podstawienie Θ, mające przedstawiać związek

$$\Theta = P^k = Q^h,$$

nie powstaje, gdy przy tworzeniu cyklów bierzemy « à la suite les unes des autres » elementa symetrycznie rozmieszczone w tablicach (p), (q), (r), a nadto nie czyni zadosyć napisanemu związkowi, albowiem, chociaż tu

$$h = 3,\ k = 2,$$

to jednakowoż

$$\Theta = P^2 = Q^6.$$

§ 22. — W przypadku (*), kiedy podstawienie

$$P = \mathfrak{P}$$

jest kołowém, t. j.

$$h = 1,$$

(*) *Comp. rend.*, str. 1199. *Exerc.*, str. 221.

mamy, z natury podstawienia Θ,

$$Q = P^k.$$

tu jednak k nie oznacza liczby cyklów podstawienia Q, lecz wskazuje, że otrzymana dla podstawienia Q wartość jest potęgą tego jednego cykla, jaki tworzy podstawienie P. Wybierając odpowiednie postacie tego podstawienia P, możemy nawet takie dla k liczby otrzymać, które będą pierwszemi względem a, t. j. względem liczby elementów tak podstawienia P, jak i podstawienia Q.

Przy daném podstawieniu

$$P = \mathcal{R}\mathcal{S}\mathcal{T};$$

jeżeli taką drugą jego postać, która nie powstała skutkiem przestawienia cyklów, lecz tylko skutkiem rozpoczynania cyklów rozmaitemi elementami, użyjemy przy tworzeniu podstawienia Q, t. j. jeśli w ogóle

$$Q = \begin{pmatrix} \mathcal{R}_{(\rho_1)}\ \mathcal{S}_{(\sigma_1)}\ \mathcal{T}_{(\tau_1)}\dots \\ \mathcal{R}_{(\rho_0)}\ \mathcal{S}_{(\sigma_0)}\ \mathcal{T}_{(\tau_0)}\dots \end{pmatrix},$$

to otrzymujemy

$$Q = \mathcal{R}^{\pi_\rho}\,\mathcal{S}^{\pi_\sigma}\,\mathcal{T}^{\pi_\tau}$$

gdzie każda z liczb

$$\pi_\rho,\ \pi_\sigma,\ \pi_\tau,\ \dots$$

ma którąkolwiek z wartości

$$0,\ 1,\ 2,\ \dots\ a-1,$$

§ **23.** — Jeśli teraz weźmiemy pod uwagę przypadek

$$a = 1,$$

to wtedy

$$\pi_\rho = \pi_\sigma = \pi_\tau = \dots\ 0$$

i cykle

$$\mathcal{R},\ \mathcal{S},\ \mathcal{T},\dots$$

są cyklami pierwszego porządku, t. j. są to elementa podstawienia P, które mają na swych miejscach pozostać. Uwzględniając te elementa, widzimy, że liczba wartości dla Q, zadosyć czyniących równaniu

$$QP = PQ,$$

powiększy się czynnikiem, przedstawiającym liczbę podstawień, jakie z tych elementów można utworzyć (*). Że jednakże ta liczba jest

$$1 \cdot 2 \cdot 3 \dots h,$$

a prócz tego, z podanego wyżéj (§ **11**) wzoru

$$\omega = (1 \cdot 2 \dots f)\,(1 \cdot 2 \dots g) \dots\ a^f\, b^g \dots\ (**)$$

(*) *Exerc.*, str. 222, 223. *Comp. rend.*, str. 1192.

(**) *Exerc.*, Tom III, str. 192. *Comp. rend.* T. XXI, str. 1192.

wypada, że liczba podstawień, wymiennych z daném podstawieniem P, zależnych od tych h cyklów 1go porządku, jest

$$1 . 2 . 3 \ldots h . 1^h,$$

to możemy cykle pierwszego porządku, zachodzące w podstawieniu P, rozpatrywać, jako tworzące prawidłowe podstawienie. Nie mamy żadnéj potrzeby w ogólnych twierdzeniach oddzielnie o tych elementach mówić, jak to często Cauchy robi, tém więcéj, jeżeliśmy w początku wywodu zastrzegli, że wszystkie elementa są ujawnione.

ROZDZIAŁ III.

§ **24.** — Serret w *Cours d'algèbre supérieure* rozbiera własności podstawień wymiennych w artykule *Des substitutions échangeables entre elles.* Jeżeli podstawienie S, zadosyć czyniące równaniu

$$TS = ST,$$

jest iloczynem kilku prawidłowych podstawień

$$S = PP'P'' \ldots$$

to Serret, dla otrzymania podstawienia, wymiennego z P i powstałego skutkiem kołowego przestawienia pewnych μ cyklów, tak przekształca układy za pomocą zmienienia porządku następstwa po sobie kolumn, że w pewnéj części spodniego układu elementa tak idą po sobie, jak i w poprzedniéj części wierzchniego układu. Takim sposobem

$$Q = \begin{pmatrix} C_1 C_2 \ldots C_{\mu-1} C'_0 \\ C_0 C_1 \ldots C_{\mu-2} C_{\mu-1} \end{pmatrix},$$

i C_0, jako też C'_0 powstały, albo z jednakowych, albo też z odmiennych postaci cykla (C_0). Można te częściowe układy tak przedstawić:

$$C_0 = a_0 a_1 a_2 \ldots a_{i-1},$$

$$C_1 = b_0 b_1 b_2 \ldots b_{i-1},$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,$$

$$C_{\mu-1} = f_0 f_1 f_2 \cdots f_{i-1};$$

za pomocą tak otrzymanéj wartości podstawienia Q, wymiennego z P, i podobną drogą mogących być znalezionemi podstawień

$$Q', Q'', \ldots,$$

odpowiednio wymiennych z podstawieniami

$$P', P'', \ldots,$$

otrzymamy poszukiwane podstawienie

$$T = QQ'Q' \ldots.$$

Jeżeli układ C'_0 jest postaci

$$C'_0 = a_\varrho\, a_{\varrho+1}\, a_{\varrho+2} \cdots a_{\varrho+i-1},$$

to pojedyncze cykle podstawienia Q Serret oznacza

$$(G_0),\ (G_1),\ \ldots,\ (G_{\varrho-1}),$$

i ich liczba wynosi i, jeżeli $\varrho = 0$, t. j. jeżeli $C'_0 = C_0$.

§ **25.** — Znaczek ϱ może mieć każdę z wartości

$$0,\ 1,\ 2,\ \ldots\ i-1;$$

nazywając zaś przez λ liczbę elementów wziętych z każdego cykla (C_ξ) podstawienia P, można zauważyć, że chociaż j, liczba elementów każdego cykla (G_ξ), wyraża się zawsze iloczynem $\lambda\mu$, to jednak, w przypadkach, kiedy ϱ jest liczba pierwsza względem i, albo też, kiedy ϱ nie jest dzielnikiem liczby i, ani liczba

$$\lambda\mu\varrho$$

nie przedstawia liczby elementów podstawienia Q, ani też nie ma miejsca równość

$$i = \lambda\varrho\ (*).$$

Utwórzmy tablicę

$$\begin{array}{l} a_\xi,\ a_{\xi+1},\ \ldots,\ a_{\xi+\varrho-1}, \\ b_\xi,\ b_{\xi+1},\ \ldots,\ b_{\xi+\varrho-1}, \\ \ldots\ldots\ldots\ldots\ldots\ldots, \\ f_\xi,\ f_{\xi+1},\ \ldots,\ f_{\xi+\varrho-1}, \end{array} \tag{16}$$

i oznaczmy układy utworzone elementami poziomych wierszy przez

$$\mathfrak{A}_\xi,\ \mathfrak{B}_\xi,\ \ldots,\ \mathfrak{F}_\xi,$$

utworzone zaś elementami pionowych wierszy przez

$$\mathfrak{M}_\xi,\ \mathfrak{M}_{\xi+1}\ldots,\ \mathfrak{M}_{\xi+\varrho-1},$$

wtedy, chociaż układy cyklów podstawienia Q dadzą się tak przedstawić :

$$G_0 = \mathfrak{M}_\varrho\ \mathfrak{M}_{2\varrho}\ \ldots\ \mathfrak{M}_{(\lambda-1)\varrho},$$

$$G_1 = \mathfrak{M}_{\varrho+1}\ \mathfrak{M}_{2\varrho+1}\ \ldots\ \mathfrak{M}_{(\lambda-1)\varrho+1},$$

etc.,

to jednak: 1° nie jest bynajmniéj koniecznem, aby liczba cyklów podstawienia Q była ϱ, gdyż może być mniejszą; 2° nie zawsze układy cyklów podstawienia P dadzą się tak przedstawić :

$$C_0 = \mathfrak{A}_0\ \mathfrak{A}_\varrho\ \mathfrak{A}_{2\varrho}\ \ldots\ \mathfrak{A}_{(\lambda-1)\varrho},$$

$$C_1 = \mathfrak{B}_0\ \mathfrak{B}_\varrho\ \mathfrak{B}_{2\varrho}\ \ldots\ \mathfrak{B}_{(\lambda-1)\varrho},$$

$$\ldots\ldots\ldots\ldots\ldots\ldots$$

$$C_{\mu-1} = \mathfrak{F}_0\ \mathfrak{F}_\varrho\ \mathfrak{F}_{2\varrho}\ \ldots\ \mathfrak{F}_{(\lambda-1)\varrho};$$

(*) Str. 239.

3° nie zawsze ma miejsce związek

$$[(C_0)\,(C_1)\,\ldots\,(C_{\rho-1})]^{\rho} = [(G_0)\,(G_1)\ldots\,(G_{\rho-1})]^{\mu} \text{ (*)},\tag{17}$$

chociażbyśmy nawet przez ρ rozumieć mieli liczbę cyklów podstawienia Q.

§ **26.** — W przykładzie § **20**, przy założeniach, które nas prowadzą do wartości (13) dla podstawienia Q, używając oznaczeń

$$\alpha_0 = a_0,\ \text{etc.};\ \beta_4 = b_0,\ \text{etc.};\ \gamma_3 = c_0,\ \text{etc.},$$

mamy wykonać

$$\begin{pmatrix} C_1\,C_2\,C'_0 \\ C_0\,C_1\,C_2 \end{pmatrix} = \begin{pmatrix} b_0\,b_1\,b_2\,b_3\,b_4\,b_5\,c_0\,c_1\,c_2\,c_3\,c_4\,c_5\,a_4\,a_5\,a_0\,a_1\,a_2\,a_3 \\ a_0\,a_1\,a_2\,a_3\,a_4\,a_5\,b_0\,b_1\,b_2\,b_3\,b_4\,b_5\,c_0\,c_1\,c_2\,c_3\,c_4\,c_5 \end{pmatrix};$$

tutaj

$$\mu = 3,\quad \rho = 4,\quad i = 6,$$

po wzięciu zaś z każdego cykla trzech elementów, wracamy do a_0; otrzymamy zatém

$$\lambda = 3;$$

ztąd widzimy, że nie sprawdzają się wyżéj przytoczone formuły, gdyż

$$\lambda\rho = 12 = 2i$$

$$\lambda\rho\mu = 36 = 2i\mu;$$

z tablicy zaś

$$a_\xi,\ a_{\xi+1},\ a_{\xi+2},\ a_{\xi+3},$$

$$b_\xi,\ b_{\xi+1},\ b_{\xi+2},\ b_{\xi+3},$$

$$c_\xi,\ c_{\xi+1},\ c_{\xi+2},\ c_{\xi+3},$$

mamy

$$G_0 = \mathfrak{M}_0\,\mathfrak{M}_\rho\ \ldots\ \mathfrak{M}_{2\rho},$$

$$G_1 = \mathfrak{M}_1\,\mathfrak{M}_{\rho+1}\,\mathfrak{M}_{2\rho+1};$$

liczba tych cyklów nie wynosi ρ, albowiem ich jest wszystkiego dwa; według tablicy (16) liczby 2ρ i $2\rho+1$ winny być mniejsze od i, tymczasem potrzeba je zastąpić najmniejszemi dodatnemi tych liczb resztami według modułu i. Układy

$$C_0,\ C_1,\ C_2$$

nie dadzą się wyrazić przez powtarzanie w całości układów utworzonych poziomemi wierszami wypisanéj, jak wskazuje Serret, tablicy. Nakoniec, choćbyśmy przez ρ rozumieli liczbę cyklów podstawienia Q, t. j. 2, nie jest

$$P^{\rho} = Q^{\mu},$$

lecz

$$P^{\rho} = [Q^{\mu}]^2.$$

(*) Str. 240, 241.

ROZDZIAŁ IV.

§ **27.** — Odszukiwane podstawienie Q może być, jak wiemy, otrzymane, gdy nad pewną postacią podstawienia

$$P = (C_0)(C_1) \dots (C_m)$$

nadpiszemy inną jego postać, powstałą skutkiem przestawienia kołowego pewnych μ cyklów, np. według skematu

(18) $$[(C_0), (C_1), \dots, (C_{\mu-1})].$$

Podstawienie to nie zmieni znaczenia, jeśli jego kolumny tak poprzestawiamy, aby układ, tworzący pierwszą część spodniego wiersza, był takim układem

$$C = a_0\, a_1\, a_2 \dots a_{n-},$$

nad nim w wierzchnim układzie znajdzie się układ

$$C_1 = b_{\varrho_1}\, b_{\varrho_1+1} \dots b_{\varrho_1+n-},$$

gdzie zamiast liczby $\varrho_1 + \xi$ należy rozumieć najmniejszą jéj dodatną resztę względem modułu n. Przestawiając następne kolumny tak, ażeby w spodnim wierszu obok układu C_0 znalazł się układ C_1 i t. d., aż nakoniec w spodnim wierszu znalazł się układ $C_{\mu-1}$, który zachodzi w poprzedniéj części wierzchniego układu, otrzymamy nad tym układem $C_{\mu-1}$ w wierzchnim wierszu, w ogóle, taki układ

$$C'_0 = a_\varrho\, a_{\varrho+1}\, a_{\varrho+2} \dots a_{\varrho+n-1}.$$

W tém podstawieniu

(19) $$\begin{pmatrix} C_1\, C_2 \dots C_{\mu-1}\, C'_0 \\ C_0\, C_1\, C_2 \dots C_{\mu-1} \end{pmatrix},$$

pierwsze elementa układów

$$C_1, C_2, \dots, C_{\mu-1}, C_0,$$

t. j. elementa

$$b_{\varrho_1}, c_{\varrho_2}, \dots, f_{\varrho_{\mu-1}}, a_\varrho$$

mają jako znaczki, którekolwiek z liczb

$$0, 1, 2, \dots, n-1;$$

przy takiém oznaczeniu możemy przedstawić wszystkie n^μ wartości dla Q (§ **13**), gdy oznaczenie użyte w § **24**, dozwala przedstawić tylko n wartości.

§ **28.** — Ponieważ układy cyklów

$$(C_1), (C_2), \dots, (C_{\mu-1})$$

w obu wierszach podstawienia(19) są jednopostaciowe, to na mocy wprowadzonego poprzednio sposobu przedstawienia kwestyi, jak poznać, w jakim porządku należy po sobie brać elementa z każdgo cykla, a także, po wzięciu jak wielu elementów z każdego cykla podstawienia P, cykl podstawienia Q będzie

zamknięty? Oczywista, że znajdziemy odpowiedź, rozpatrując podstawienie ad hoc

$$\begin{pmatrix} C_0 \\ C_0 \end{pmatrix},$$

t. j. podstawienie

$$\begin{pmatrix} a_\rho & a_{\rho+1} & a_{\rho+2} & \cdots & a_{\rho-1} \\ a_0 & a_1 & a_2 & \cdots & a_{n-1} \end{pmatrix}.$$

Dla zamknięcia cykla (G_ξ) należy z pierwszego cykla (C_0) i każdego następnego wziąć po λ elementów, gdy λ jest najmniejszą dodatną liczbą zadosyć czyniącą porównaniu (§ **17**)

$$\xi + \lambda\rho \equiv \xi (\mathrm{mod}\ n),$$

t. j.

$$\lambda\rho \equiv 0 (\mathrm{mod}\ n). \tag{20}$$

Liczba ρ jest dana, albo, ściśléj mówiąc, określona samemi postaciami, jakeśmy w (18) cyklom nadali; od téj liczby zależy liczba λ. Możemy w (20), co do liczby ρ, uważać trzy przypadki, odnośnie do modułu n: *a*) ρ jest liczba pierwsza względem n; *b*) ρ jest dzielnikiem liczby n; *c*) ρ i n posiadają największy spólny dzielnik δ.

Jeżeli ρ jest liczba pierwsza względem n, to liczba λ zadosyć czyni związkowi (20) przy wartości

$$\lambda = n,$$

z tego widać, że tworząc w tym przypadku cykl podstawienia Q, bierzemy wszystkie elementa tak z pierwszego, jak i z każdego z następnych cyklów podstawienia P. Zatém podstawienie Q jest kołowe o μn elementach.

Jeśli ρ jest dzielnikiem liczby n, wtedy porównanie (20) wyznacza

$$\lambda = \frac{n}{\rho},$$

zkąd równość

$$n = \lambda\rho,$$

jaką Serret zbyt ogólnie stawia (§ **25**). Dla utworzenia cykla (G_ξ) należy z pierwszego i następnych cyklów podstawienia P brać po λ elementów, a liczba wszystkich elementów cykla (G_ξ), którą nazwijmyν, wyrazi się

$$\nu = \mu\lambda;$$

jeżeli wyjdziemy tu z elementu a_ξ, przy $\xi < \rho$, i brać będziemy elementa w porządku

$$a_\xi, b_{\rho_1+\xi}, c_{\rho_2+\xi}, \ldots, f_{\rho_{\mu-1}+\xi}, a_{\xi+\rho}, b_{\rho_1+\xi+\rho}, \ldots,$$

to wszystkie znaczki elementów mniejsze są od liczby n i porządek, w jakim te elementa z każdego cyklu czerpiemy, jest tenże sam, w jakim one w cyklu się znajdują. Że zaś żaden element, znajdujący się pomiędzy elementami a_ξ i $a_{\xi+\rho}$, jak również żaden ze znajdujących się pomiędzy $a_{\xi+\rho}$ i $a_{\xi+2\rho}$, etc., nie był użyty dla utworzenia tego cykla, który zaczęliśmy elementem a_ξ, to, widocznie, przy każdéj z wartości

$$0, 1, 2, \ldots, \rho - 1$$

dla ξ, otrzymujemy różne cykle, tak, że podstawienie Q ma ρ cyklów.

Jeżeli ρ jest liczba pierwsza względem n, to tylko w tym przypadku możemy brać elementa w takimże porządku, w jakim one zachodzą w cyklach podstawienia P, kiedy

$$\rho = 1.$$

§ **29.** — Jeżeli jednak, w ogólnym przypadku, liczby ρ i n mają największy spólny dzielnik δ, przy

$$n = \chi\delta,$$

$$\rho = \psi\delta,$$

to porównanie (20) przechodzi w następujące

$$\lambda\psi, \equiv 0 (\mathrm{mod}\,\chi); \tag{21}$$

ponieważ ψ jest liczba pierwsza względem modułu, to

$$\lambda = \chi,$$

a następnie

$$n = \lambda\delta = \lambda\frac{\rho}{\psi}.$$

Takim sposobem zadanie sprowadza się do tego przypadku, kiedy ψ jest pierwsze względem λ, t. j. względem liczby elementów, które wziąć mamy z każdego cyklu. Bierzemy zatém dla utworzenia cyklu (G_ξ) elementa, których znaczki różnią się między sobą o jakąś wielokrotność liczby δ. Wyszedłszy z elementu a_ξ cyklu (C_0), przed elementem $a_{\xi+\rho}$ takich właśnie elementów mamy ψ, t. j.

$$a_\xi, a_{\xi+\delta}, a_{\xi+2\delta}, \ldots, a_{\xi+(\psi-1)\delta};$$

między ostatnim z napisanych a elementem $a_{\xi+2\rho}$ (jeżeli $\xi + 2\rho < n$) i t. d. znajdujemy ich po tyléż. Możemy tedy znaczkowi ξ nadawać tylko takie znaczenie

$$0, 1, 2, \ldots, \delta - 1;$$

jeżeli przez σ nazwiemy liczbę cyklów podstawienia Q, to oczywiście,

$$\sigma = \delta;$$

w każdym cyklu znajduje się

$$\nu = \mu\lambda$$

elementów. Otrzymujemy przytém takie ogólne wyrażenia: dla liczby λ, t. j. liczby elementów, wziętych z każdego cykla podstawienia P,

$$\lambda = \frac{n\psi}{\rho},$$

dla liczby cyklów podstawienia Q

$$\sigma = \frac{\rho}{\psi}$$

i liczbę

$$\psi - 1,$$

przedstawiającą nam liczbę elementów cykla podstawienia P, które są wzięte przy tworzeniu cykla podstawienia Q, a które znajdowały się między elementami, mającemi znaczki, różniące się o ρ między sobą. Te wyrażenia w przypadkach, w poprzednim paragrafie rozbieranych, przechodzą w następujące : gdy $\rho=\psi$,

$$\lambda=n,\quad \sigma=1,\quad \rho-1.$$

gdy zaś $\psi=1$, t. j. gdy ρ jest dzielnikiem n,

$$\lambda=\frac{n}{\rho},\quad \sigma=\rho, 0,$$

§ **30.** — Widzimy ztąd, że gdy utworzymy tablicę elementów o σ pionowych i μ poziomych wierszach

$$(22)\qquad \begin{cases} a_{\xi}, & a_{\xi+1}, & a_{\xi+2}, & \ldots, a_{\xi+\delta-1}, \\ b_{\rho_1+\xi}, & b_{\rho_1+\xi+1}, & b_{\rho_1+\xi+2}, & \ldots, b_{\rho_1+\xi+\delta-1}, \\ c_{\rho_2+\xi}, & c_{\rho_2+\xi+1}, & c_{\rho_2+\xi+2}, & \ldots, c_{\rho_2+\xi+\delta-1}, \\ \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots \\ f_{\rho_{\mu-1}+\xi}, & f_{\rho_{\mu-1}+\xi+1}, & f_{\rho_{\mu-1}+\xi+2}, & f_{\rho_{\mu-1}+\xi+\delta-1}, \end{cases}$$

albo ogólniéj

$$(23)\qquad \begin{cases} a_{\xi}, & a_{\xi+1}, & a_{\xi+2}, & \ldots, & a_{\xi+\frac{\rho}{\psi}-1}, \\ b_{\rho_1+\xi}, & b_{\rho_1+\xi+1}, & b_{\rho_1+\xi+2}, & \ldots, & b_{\rho_1+\xi+\frac{\rho}{\psi}-1}, \\ c_{\rho_2+\xi}, & c_{\rho_2+\xi+1}, & c_{\rho_2+\xi+2}, & \ldots, & c_{\rho_2+\xi+\frac{\rho}{\psi}-1}, \\ \ldots\ldots & \ldots\ldots & \ldots\ldots & & \ldots\ldots \\ f_{\rho_{\mu-1}+\xi}, & f_{\rho_{\mu-1}+\xi+1}, & f_{\rho_{\mu-1}+\xi+2}, & \ldots, & f_{\rho_{\mu-1}+\xi+\frac{\rho}{\psi}-1}, \end{cases}$$

a jéj poziome wiersze oznaczymy

$$\mathcal{A}_{\rho},\ \mathcal{B}_{\rho_1+\xi},\ \mathcal{C}_{\rho_2+\xi},\ldots,\ \mathcal{F}_{\rho_{\mu-1}+\xi},$$

pionowe zaś

$$\mathfrak{M}_{\xi},\ \mathfrak{M}_{\xi+1},\ \mathfrak{M}_{\xi+2},\ \ldots,\ \mathfrak{M}_{\xi+\frac{\rho}{\psi}-1},$$

to układy cyklów dadzą się przedstawić

$$\begin{aligned} C_0 &= \mathcal{A}_0 \quad \mathcal{A}_{\frac{\rho}{\psi}} \quad \mathcal{A}_{2\frac{\rho}{\psi}} \quad \ldots\ \mathcal{A}_{n-\frac{\rho}{\psi}}, \\ C_1 &= \mathcal{B}_{\rho_1} \quad \mathcal{B}_{\rho_1+\frac{\rho}{\psi}} \quad \mathcal{B}_{\rho_1+2\frac{\rho}{\psi}} \quad \ldots\ \mathcal{B}_{\rho_1+n-\frac{\rho}{\psi}}, \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ C_{\mu-1} &= \mathcal{F}_{\rho_{\mu-1}} \quad \mathcal{F}_{\rho_{\mu-1}+\frac{\rho}{\psi}} \quad \mathcal{F}_{\rho_{\mu-1}+2\frac{\rho}{\psi}} \quad \ldots\ \mathcal{F}_{\rho_{\mu-1}+n-\frac{\rho}{\psi}}, \end{aligned}$$

zaś

$$\begin{array}{lllll} G_0 & = \mathfrak{M}_0 & \mathfrak{M}_\rho & \mathfrak{M}_{2\rho} & \dots \mathfrak{M}_{n-\rho}, \\ G_1 & = \mathfrak{M}_1 & \mathfrak{M}_{\rho+1} & \mathfrak{M}_{2\rho+1} & \dots \mathfrak{M}_{n\psi-\rho-1} \\ \dots & \dots & \dots & \dots & \dots \\ G_{\frac{\rho}{\psi}-1} & = \mathfrak{M}_{\frac{\rho}{\psi}-1} & \mathfrak{M}_{2\frac{\rho}{\psi}-1} & \mathfrak{M}_{3\frac{\rho}{\psi}-1} & \dots \mathfrak{M}_{n\psi-\rho+\frac{\rho}{\psi}-1}. \end{array}$$

Tutaj przez znaczki, które są liczbami większemi od n, należy rozumieć ich najmniejsze dodatne reszty względem modułu n. Tak np. ostatni znaczek

$$n\psi-\rho+\frac{\rho}{\psi}-1=(\lambda-1)\rho+\frac{\rho}{\psi}-1,$$

jest liczbą

$$n-\rho+\frac{\rho}{\psi}-1=n-(\psi-1)\frac{\rho}{\psi}-1.$$

Samo zaś odszukiwane podstawienie Q jest

$$Q=(G_0)(G_1)\dots(G_{\frac{\rho}{\psi}-1});$$

a każdy z układów G_ξ powstał z $\frac{\rho}{\psi}$ odpowiednich $\mathfrak{M}_\xi$, to jest z odpowiedniego pionowego wiersza tablicy (22) lub (23).

Tablice te w przypadku

$$\delta=\rho, \text{ t. j. } \psi=1,$$

przechodzą w tablicę (16), a jeśli w nich jeszcze pionowe wiersze napiszemy jako poziome, i wzajemnie, to sprowadzają się one do jednéj z tablic (14).

Jeżeli zaś ρ i n są liczby pierwsze względem siebie,

$$\delta=1, \text{ t. j. } \psi=\rho,$$

to wtedy tablice (22) i (23) mają tylko jeden pionowy wiersz.

§ **31.** — Podstawienie porządku λ^{ego}

$$(24) \qquad \Theta=\begin{cases} \left(a_0, a_{\frac{\rho}{\psi}}, \dots, a_{(\lambda-1)\frac{\rho}{\psi}}\right)\left(a_1, a_{\frac{\rho}{\psi}+1}, \dots, a_{(\lambda-1)\frac{\rho}{\psi}+1}\right)\cdots\left(a_{\frac{\rho}{\psi}-1}, a_{2\frac{\rho}{\psi}-1}, \dots, a_{n-1}\right), \\ \left(b_{\rho_1}, b_{\rho_1+\frac{\rho}{\psi}}, \dots, b_{\rho_1+(\lambda-1)\frac{\rho}{\psi}}\right)\cdots\left(b_{\rho_1+\frac{\rho}{\psi}-1}, b_{\rho_1+2\frac{\rho}{\psi}-1}, \dots, b_{\rho_1-1}\right) \\ \dots\dots\dots\dots\dots\dots\dots\dots \\ \left(f_{\rho_{\mu-1}}, f_{\rho_{\mu-1}+\frac{\rho}{\psi}}, \dots f_{\rho_{\mu-1}+(\lambda-1)\frac{\rho}{\psi}}\right)\cdots\left(f_{\rho_{\mu-1}+\frac{\rho}{\psi}-1}, f_{\rho_{\mu-1}+2\frac{\rho}{\psi}-1}, \dots, f_{\rho_{\mu-1}-1}\right) \end{cases}$$

powstaje z podstawienia

$$(C_0)(C_1)(C_2)\dots(C_{\mu-1}),$$

którego cykle mają po $n=\lambda\frac{\rho}{\psi}$ elementów, jak tylko je podniesiemy do potęgi $\frac{\rho}{\psi}$. Przytém elementa podstawienia Θ pozostają w tymże samym porządku, w jakim one były w odpowiednich cyklach podstawienia P.

Jeżeli do potęgi μ podniesiemy podstawienie Q, którego porządek jest przedstawiony liczbą $\nu=\mu\lambda$, to otrzymamy pewne podstawienie Θ_1 porządku λ^{ego}. Ponieważ jednak przy tworzeniu cykla (G_ξ) bierzemy elementa z cyklów podstawienia P, nie zawsze w tym samym porządku, w jakim one w tych cyklach po sobie następują, to podstawienie Θ_1 tylko przy pewnych warunkach może być identyczném z podstawieniem Θ. Dla utworzenia cykla (G_ξ) braliśmy z cykla (C_0) elementa ze znaczkami

$$\xi, \xi+\rho, \xi+2\rho, \ldots, \xi+(\chi-1)\rho,$$

albo, co jedno,

$$\xi, \xi+\psi\delta, \xi+2\psi\delta, \ldots, \xi+(\chi-1)\psi\delta;$$

z temiż znaczkami i w takim właśnie porządku znajdują się elementa w cyklach podstawienia Θ_1. Z tych elementów ten jest drugim elementem odpowiedniego cykla podstawienia Θ (t. j. elementem ze znaczkiem $\xi+\delta$), którego znaczek $\xi+x\psi\delta$ zadosyć czyni związkowi

$$\xi+x\psi\delta \equiv \xi+\delta \pmod{n},$$

zkąd

$$x\psi\delta \equiv \delta \pmod{\delta\chi},$$

$$x\psi \equiv 1 \pmod{\chi};$$

ponieważ ψ i χ są liczby pierwsze względem siebie, zatém

$$x=\frac{1+\varphi\chi}{\psi},$$

gdzie φ jest najmniejsza z całkowitych liczb, dających całkowitą wartość dla liczby x. Ztąd widać, że podnosząc podstawienie Θ_1 do potęgi x, otrzymujemy podstawienie Θ. Jest zatém

$$(25)\qquad \Theta=\left[(C_0)\,(C_1)\,\ldots\,(C_{\rho-1})\right]^{\frac{\rho}{\psi}}=\left[(G_0)\,(G_1)\,\ldots\,(G_{\frac{\rho}{\psi}-1})\right]^{\mu\frac{1+\varphi\chi}{\psi}}.$$

Jestto ogólny warunek, któremu zadosyć winny czynić dwa podstawienia, mające tylko spólne elementa, jeżeli te podstawienia mają zadosyć czynić związkowi, przedstawionemu liniowém symboliczném równaniem

$$QP=PQ.$$

Podstaiwenie Θ ma

$$\mu\frac{\rho}{\psi}$$

cyklów, t. j. tyle, ile jest elementów w każdéj z tablic (22) i (23). Jeżeli wyobrazimy sobie żeśmy kolejno wypisali wszystkie tablice (22), zastępując liczbę δ liczbami

$$\delta, 2\delta, 3\delta, \ldots, (\chi-1)\delta,$$

lub też, żeśmy kolejno wypisali wszystkie tablice (23), pisząc przytém zamiast $\frac{\rho}{\psi}$ po porządku liczby

$$\frac{\rho}{\psi},\quad 2\frac{\rho}{\psi},\quad 3\frac{\rho}{\psi},\ \ldots,\ (\chi-1)\frac{\rho}{\psi},$$

to elementa symetrycznie w tych tablicach rozmieszczone, t. j. znajdujące się w punktach przecięcia się tychże samych pionowych i poziomych wierszy, wzięte w porządku wypisanych tablic, tworzą cykle podstawienia Θ.

Przyjmując we wzorach (24) i (25)

$$\psi = 1.$$

przy czém, oczywiście,

$$\varphi = 0,\ \frac{1+\varphi\chi}{\psi} = 1,$$

widzimy, że w tym przypadku (t. j., gdy ρ jest dzielnikiem liczby n) formuła (25), sprowadza się do

$$[(C_0)\,(C_1)\,\ldots\,(C_{\mu-1})]^{\mu} = [(G_0)\,(G_1)\,\ldots\,(G_{\rho-1})]^{\mu},$$

t. j. do formuły (17), a gdy jeszcze

$$\mu = m,$$

to mamy

$$\Theta = P^{\varphi} = Q^{m},$$

t. j. formułę (15).

Przyjmując w wyrażeniach (24) i (25)

$$\rho = \psi,$$

otrzymujemy

$$\chi = n,$$

$$\theta = (C_0)\,(C_1)\,(C_2)\,\ldots\,(C_{\mu-1}) = \left[(G_0)\right]^{\mu\frac{1+\varphi n}{\rho}};$$

w tym przypadku podstawienie Θ utworzone jest wyłącznie z pierwszych elementów każdego z poziomych wierszy tablicy (23).

§ **32.** — W wyżéj (§§ **20, 21, 26**) przytaczanym przykładzie mamy, według § **28**, przy poszukiwaniu wartości (13),

$$C_0 = a_0a_1a_2a_3a_4a_5,$$
$$C_1 = b_4b_5b_0b_1b_2b_3,$$
$$C_2 = c_2c_3c_4c_5c_2c_1,$$
$$C_0 = a_4a_5a_0a_1a_2a_3;$$

na mocy zaś

$$\binom{C'_0}{C_0}$$

wypada, że

$$n=6,\quad \rho=4,\quad \psi=2,\quad \lambda=\chi=3,\quad \sigma=\delta=2;$$

utwórzmy tablicę

$$\begin{cases} a_\xi\ \ , a_{\xi+1}, \\ b_{4+\xi}, b_{5+\xi}, \\ c_{3+\xi}, b_{4+\xi}; \end{cases}$$

wtedy

$$n-\frac{\rho}{\psi}=4,\quad n\psi-\rho\equiv 2 \pmod 6;$$

a więc

$$C_0=\mathfrak{A}_0\,\mathfrak{A}_2\,\mathfrak{A}_4,$$
$$C_1=\mathfrak{B}_1\,\mathfrak{B}_0\,\mathfrak{B}_2,$$
$$C_2=\mathfrak{C}_2\,\mathfrak{C}_5\,\mathfrak{C}_1$$

i

$$G_0=\mathfrak{M}_0\,\mathfrak{M}_4\,\mathfrak{M}_2,$$
$$G_1=\mathfrak{M}_1\,\mathfrak{M}_5\,\mathfrak{M}_3;$$

a tém samém

$$Q=(G_0)\,(G_1);$$

że zaś

$$\frac{\rho}{\psi}=2,\quad \varphi=1,\quad \frac{1+\varphi\chi}{\psi}=2,\quad \mu=3,$$

to

$$\Theta=P^2=Q^6.$$

Weźmy jeszcze przykład. Niech będzie dane np. podstawienie

$$P=(C_0)\,(C_1)\,(C_2)\,(C_3)\,(C_4)\,(C_5)\,(C_6);$$

dla otrzymania téj wartości podstawienia Q, wymiennego z P, którąby powstała w skutek przestawienia np. pierwszych pięciu cyklów według skematu

$$[(C_0),\,(C_1),\,(C_2),\,(C_3),\,(C_4)]$$

(tu tedy $m=7,\quad \mu=5$), przyjmiemy jeszcze, że np.

$$n=16,\ \rho_1=13,\ \rho_2=0,\ \rho_3=8,\ \rho_4=3,\ \rho=12;$$

wtedy, przy tych założeniach, z

$$\begin{pmatrix} C'_0 \\ C_0 \end{pmatrix}$$

wypada, że

$$\psi = 3,\ \lambda = \chi = 4,\ \sigma = \delta = 1;$$

takim sposobem nasza tablica jest tu następująca

$$\begin{cases} a_\xi\ ,\ a_{\xi+1},\ a_{\xi+2},\ a_{\xi+3}, \\ b_{13+\xi}\ ,\ b_{14+\xi},\ b_{15+\xi},\ b_{16+\xi}, \\ c_\xi\ ,\ c_{\xi+1},\ c_{\xi+2},\ c_{\xi+3}, \\ d_{8+\xi}\ ,\ d_{9+\xi},\ d_{10+\xi},\ d_{11+\xi}, \\ e_{3+\xi}\ ,\ e_{4+\xi},\ e_{5+\xi},\ e_{6+\xi}; \end{cases}$$

z niéj wypada, wedle prawidła, że

$$C_0 = \mathfrak{A}_0\ \mathfrak{A}_4\ \mathfrak{A}_8\ \mathfrak{A}_{12},$$
$$C_1 = \mathfrak{B}_{13}\ \mathfrak{B}_1\ \mathfrak{B}_5\ \mathfrak{B}_9,$$
$$C_2 = \mathfrak{C}_0\ \mathfrak{C}_4\ \mathfrak{C}_8\ \mathfrak{C}_{12},$$
$$C_3 = \mathfrak{D}_8\ \mathfrak{D}_{12}\ \mathfrak{D}_0\ \mathfrak{D}_4,$$
$$C_4 = \mathfrak{E}_3\ \mathfrak{E}_7\ \mathfrak{E}_{11}\ \mathfrak{E}_{15},$$

i

$$G_0 = \mathfrak{M}_0\ \mathfrak{M}_{12}\ \mathfrak{M}_8\ \mathfrak{M}_4,$$
$$G_1 = \mathfrak{M}_1\ \mathfrak{M}_{13}\ \mathfrak{M}_9\ \mathfrak{M}_5,$$
$$G_2 = \mathfrak{M}_2\ \mathfrak{M}_{14}\ \mathfrak{M}_{10}\ \mathfrak{M}_6,$$
$$G_3 = \mathfrak{M}_3\ \mathfrak{M}_{15}\ \mathfrak{M}_{11}\ \mathfrak{M}_7,$$

a tém samém

$$Q = (G_0)\ (G_1)\ (G_2)\ (G_3);$$

że zaś

$$\frac{\rho}{\psi} = 4,\quad \varphi = 2,\quad \frac{1 + \varphi\gamma}{\psi} = 3,$$

zatém

$$\Theta = [(C_0)(C_1)(C_2)\ (C_3)\ (C_4)]^4 = [(G_0)\ (G_1)\ (G_2)\ (G_3)]^{15}.$$
