O TWORZENIU

SYSTEMATU SPRZĘŻONEGO

PODSTAWIEŃ LINIOWYCH POSTACI

$$| X_z \quad X_{az+b} |$$

PRZEZ

D^RA M.-A. BARANIECKIEGO

Privat-docenta Cesarskiego Uniwersytetu Warszawskiego.

(Przedstawiono na posiedzeniu Towarzystwa Nauk Ścisłych w Paryżu, dnia 11 czerwca 1877 roku.)

Zastosowanie, jakie teorya podstawień (substytucyj) znalazła w doktrynie GALOIS o rozwiązalności algebraicznéj równań, w zupełności usprawiedliwiło to drobiazgowe zajmowanie się niemi, które CAUCHY prowadził przez lat tyle.

Gdy jednakowoż najgłówniejsze z otrzymanych przez GALOIS (1) rezultatów opierają się na własnościach systematów sprzężonych podstawień liniowych, (systematów) *właściwych równaniom* (propre à l'équation) algebraicznym, to badania nad podstawieniami liniowemi były szczegółowiéj prowadzone, a głównie przez pp. BETTI'ego (2), SERRET'a (3) i JORDAN'a (4).

Podaję tu niektóre przezemnie dostrzeżone własności podstawień liniowych, postaci

$$| X_z \quad X_{az+b} | ,$$

(1) *Mémoire sur les conditions de résolubilité des équations par radicaux.* Dziennik LIOUVILLE'a, t. XI, 1846.

(2) *Sopra la resolubilita per radicali delle equazioni algebraiche irriduttibili di grado primo.* Annali di TORTOLINI, t. II, 1851.

(3) *Comptes rendus*, t. XLVIII.

(4) *Traité des substitutions et des équations algébriques.*

z n elementów

$$X_0, X_1, X_2, \ldots, X_{n-1},$$

prowadzące do metodycznego tworzenia systematów sprzężonych tych podstawień, tak kiedy n jest liczba pierwsza, jak i wtedy, kiedy n jest liczba złożona.

n JEST LICZBA PIERWSZA.

W tym przypadku wszystkich podstawień liniowych postaci

(1) $$| X_z \quad X_{az+b} |$$

jest $n(n-1)$, gdyż a może oznaczać którąkolwiek z $n-1$ liczb

(2) $$1, 2, 3, \ldots, n-1,$$

zaś, przy każdéj z tych wartości dla a, b może być którąś z n liczb

$$0, 1, 2, 3, \ldots, n-1.$$

Jak zauważył p. SERRET, tylko przy $a=1$ i $b>0$ podstawienie (1) przestawia wszystkie elementy; przy innych zaś wartościach, nie wszystkie elementy zostają przestawione w skutek wykonania tego podstawienia.

Najprostsze z podstawień liniowych, przestawiających wszystkie elementy, jest podstawienie kołowe (cykliczne)

$$\begin{aligned} P &= (X_0, X_1, X_2, \ldots, X_{(n-1)}), \\ &= | X_z \quad X_{z+1} | . \end{aligned}$$

Ponieważ wszystkie liczby (2) są pierwsze względem liczby n, przedstawiającéj także *porządek* (ordre) podstawienia P, więc wszystkie podstawienia P^a

$$\begin{aligned} P^a &= (X_0, X_a, X_{2a}, \ldots, X_{(n-1)a}), \\ &= | X_z \quad X_{z+a} | , \end{aligned}$$

dla każdéj z szeregu (2) wartości liczby a, są podstawieniami *podobnemi* (semblable) z podstawieniem P. Podstawienie P^a może być dane w jakiejkolwiek *postaci* (forme), t. j. można cykl, symbolizujący je, zacząć od któregokolwiek z jego elementów, np. od elementu X_b,

$$\begin{aligned} P^a &= (X_b, X_{a+b}, X_{2a+b}, \ldots, X_{(n-1)a+b}), \\ &= | X_z \quad X_{z+a} | , \end{aligned}$$

Jeżeli ten ostatni symbol kołowy podstawienia P^a postawimy nad symbolem kołowym podstawienia P, odrzucimy klamry nawiasów i przecinki, a wszystko ujmiemy w większe klamry nawiasu, to podstawienie

$$\begin{pmatrix} X_b X_{a+b} X_{2a+b} \ldots X_{(n-1)a+b} \\ X_0 X_1 \quad X_2 \quad \ldots X_{n-1} \end{pmatrix} = | X_z \quad X_{az+b} | = R$$

zadosyć czyni, jak wiadomo, związkowi

$$RPR^{-1} = P^a.$$

Wyznaczymy porządek podstawienia R. Niechaj w szeregu kolejnych potęg

$$R,\ R^2,\ R^3,\ \ldots$$

pierwszém, równém jedności, będzie podstawienie R^r, t. j.

(3) $$R^r = 1 = |\ X_z \quad X_z\ |\ .$$

Lecz, z drugiéj strony R^r, jako r^{ta} potęga podstawienia

$$R = |\ X_z \quad X_{az+r}\ |\ ,$$

wyraża się symbolem

(4) $$R^r = |\ X_z \quad X_{a^r z + b(a^{r-1} + \ldots + a + 1)}\ |\ ;$$

jest więc, na mocy wyrażeń (3) i (4), dla wszystkich wartości z,

$$a^r z + b(a^{r-1} + \ldots + a + 1) \equiv z \pmod{n},$$

czyli

$$(a^r - 1)\, z + b\, \frac{a^r - 1}{a - 1} \equiv \pmod{n}\ .$$

Gdy $a - 1$ jest liczba pierwsza względem modułu, to, mnożąc przez $a - 1$, otrzymujemy porównanie

$$\{(a-1)\, z + b\}\,(a^r - 1) \equiv \pmod{n}$$

które, mając miejsce dla wszystkich wartości z, wymaga, żeby

$$a^r \equiv 1 \pmod{n}.$$

Wypada więc, że r, to jest *porządek podstawienia*

$$R = |\ X_z \quad X_{az+b}\ |\ ,$$

(przy $a>1$), *wyznacza wykładnik potęgi, do którego należy liczba a według modułu n.*

Ponieważ podstawienie P przestawia wszystkie elementy, podstawienie zaś R nie wszystkie, to w szeregu potęg

$$R,\ R^2,\ \ldots,\ R^{r-1}$$

nie ma podstawienia, równego któremukolwiek z podstawień

$$P,\ P^2,\ \ldots,\ P^{n-1}.$$

Gdy nadto ze związku

$$RPR^{-1} = P^a$$

wypada, że

$$R^h P^g = P^k R^h,$$

to *podstawienia, wyprowadzone* (subst. dérivées) *z podstawień liniowych*

$$P = |\ X_z \quad X_{z+1}\ |\ ,$$
$$R = |\ X_z \quad X_{az+b}\ |\ ,$$

utworzą systemat sprzężony podstawień liniowych

$$\begin{cases} 1, & P, & P^2, & \ldots, P^{n-1} \\ R, & RP, & RP^2, & \ldots, RP^{n-1}, \\ \cdot & \cdot & \cdot & \cdot \\ R^{r-1}, & R^{r-1}P^r, & R^{r-1}P^2, & \ldots, R^{r-1}P^{n-1}, \end{cases}$$

albo

$$\begin{cases} 1, & P, & P^2, & \ldots, P^{n-1}, \\ R, & PR, & P^2R, & \ldots, P^{n-1}R, \\ \cdot & \cdot & \cdot & \cdot \\ R^{r-1}, & PR^{r-1}, & P^2R^{r-1}, & \ldots, P^{n-1}R^{r-1}; \end{cases}$$

porządek zaś tego systematu jest nr, gdzie r wyznacza się z porównania

$$a^r \equiv 1 \pmod{n}.$$

Gdyby a było pierwiastnikiem pierwotnym liczby n, to $r = n-1$ i systemat sprzężony składałby się z $n(n-1)$ podstawień liniowych, t. j. zawierałby wszystkie możliwe (i tylko je) podstawienia liniowe. Powiemy zatém :

Ażeby utworzyć systemat sprzężony wszystkich $n(n-1)$ podstawień liniowych z n elementów, postaci

$$| X_z \quad X_{az+b} | ,$$

należy wyprowadzić wszystkie (różne) *podstawienia z dwóch podstawień*

$$| X_z \quad X_{z+1} | ,$$

$$| X_z \quad X_{\alpha z+b} | ,$$

gdzie α jest pierwiastek pierwotny liczby n, zaś b jest którakolwiek jedna z liczb

$$0, 1, 2, \ldots, n-1.$$

n JEST LICZBA ZŁOŻONA.

W tym przypadku wszystkich podstawień postaci

$$| X_z \quad X_{ax+b} |$$

jest $n\varphi(n)$, jeśli $\varphi(n)$ oznacza ilość liczb pierwszych względem n i mniejszych od n, gdyż b może przyjmować wszystkie wartości

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

lecz a, aby symbol przedstawiał podstawienie, winno być liczbą pierwszą względem n.

Jeśli weźmiemy najprostsze podstawienie kołowe

$$P = (X_0, X_1, X_2, \ldots, X_{n-1}),$$
$$= | X_z \quad X_{z+1} | ,$$

to w szeregu potęg tego podstawienia

$$P, \quad P^2, \quad P^3, \quad \ldots, \quad P^{n-1} \quad P^n = 1,$$

jest tylko $\varphi(n)$ podstawień podobnych z P, mianowicie te, których wykładniki potęgi są liczby pierwsze względem n. Przy pomocy symbolu kołowego podstawienia P, oraz jednéj z postaci symbolu kołowego podstawienia podobnego

$$P^a = | X_z \quad X_{z+a} | ,$$

otrzymamy takimże samym, co poprzednio, sposobem podstawienie

$$| X_z \quad X_{az+b} | = Q,$$

zadosyć czyniące związkowi

$$QPQ^{-1} = P^a.$$

Jeżeli to podstawienie Q pozostawia jeden lub kilka nieporuszonych elementów, to dla jednéj lub kilku wartości z ma miejsce porównanie

$$az + a \equiv z (\mathrm{mod}\ n).$$

Widoczna, że, jeżeli $a - 1$ jest liczba pierwsza względem modułu n, to nasze porównanie posiada rozwiązanie (czyli istnieje element nieporuszony przez podstawienie Q); jeżeli $a - 1$ nie jest liczba pierwsza względem n, lecz największy spólny dzielnik liczb $a - 1$ i n dzieli bez reszty liczbę b, to porównanie posiada rozwiązania (istnieją nieprzestawione elementy); jeśli zaś b nie jest podzielne przez największy spólny dzielnik liczb $a - 1$ i n, to porównanie nie ma rozwiązania (wszystkie elementy są przestawione). Powiemy zatém, że *symbol*

$$| X_z \quad X_{az+b} |$$

przedstawia podstawienie, poruszające wszystkie elementy, w razie, kiedy b nie jest podzielne przez największy spólny dzielnik liczb a — 1 i n, nie pierwszych względem siebie; we wszystkich zaś pozostałych przypadkach ten symbol przedstawia podstawienie, pozostawiające jeden lub kilka elementów nieprzestawionych.

Jeśli to podstawienie przemieszcza wszystkie elementy (i $a>1$), oznaczać je będziemy głoską S; jeśli zaś zostawia nieporuszone pewne elementy głoską R.

Ponieważ tak podstawienie P, jak i podstawienie S przestawiają wszystkie elementy, to może się wydarzyć, że któraś z potęg podstawienia S jest témże samém podstawieniem, co jedna z potęg podstawienia P. Naprz., jeżeli

$$P = | X_z \quad X_{z+1} | ; \qquad S = | X_z \quad X_{5z+5} | ; \qquad n = 8,$$

to

$$S^2 = P^6; \ S^4 = P^4; \ S^6 = P^2,$$

zaś S, S^3, S^5 i S^7 są podstawieniami odrębnemi od potęg P. Dla tego, jeśli podstawienie S jest s^{go} porządku, to nie zawsze systemat sprzężony podstawień, wyprowadzonych z podstawień P i S będzie sn^{go} porządku. Tak w tym przykładzie, choć $s = 8$, to porządek systematu sprzężonego, wyprowadzonego z wypisanych dwóch podstawień, nie będzie 8.8 lecz $8.2 = 16$. Tak, że możemy w ogóle powiedzieć: *jeżeli w szeregu podstawień*

$$S, \ S^2, \ S^3, \ \ldots, \ S^{s-1}, \ S^s = 1$$

pierwszém, równém jednemu z podstawień

$$1, \ P, \ P_2, \ldots, \ P^{n-1}$$

jest podstawienie S, *to systemat sprzężony podstawień* P i S, *będzie porządku* $n\sigma$.

Gdy zechcemy wyznaczyć porządek podstawienia R (zostawiającego jeden lub kilka elementów nieporuszonych), jeśli jego symbol jest

$$R = | X_z \quad X_{az+b} |$$

jeśli pierwsza z szeregu jego potęg równa jedności, jest R^r, to

$$R^r = | X_z \quad X_{a^r z + b(a^{r-1} + \cdots + a + 1)} | = 1,$$

i tém samém, dla wszystkich wartości z,

$$a^r z + b(a^{r-1} + \ldots + a + 1) \equiv z \pmod{n},$$

czyli

$$(a^r - 1)z + b\frac{a^r - 1}{a - 1} \equiv 0 \pmod{n}.$$

Jeśli tu $a - 1$ jest liczba pierwsza względem n, to mnożąc przez $a - 1$, otrzymamy

$$\{(a-1)z + b\}(a^r - 1) \equiv 0 \pmod{n}; \tag{5}$$

jeśli zaś liczby $a - 1$ i n mają największy spólny dzielnik $v > 1$, to, w tym przypadku, jak wyżéj powiedzieliśmy, b jest wielokrotnością liczby v, a przyjmując

$$a - 1 = a'v,$$
$$b = b'v,$$

możemy przedostatnie porównanie pomnożyć przez a' i otrzymać

$$(a'z + b')(a^r - 1) \equiv 0 \pmod{n}, \tag{6}$$

Z porównań (5) i (6), mających miejsce dla wszystkich wartości z, wypada

$$a^r \equiv 1 \pmod{n}.$$

t. j, *porządek podstawienia liniowego*

$$R = | X_z \quad X_{az+b} |,$$

zostawiającego jeden lub kilka elementów na swych miejscach, wyznacza się wykładnikiem potęgi, do którego należy liczba a względem modułu n.

Ponieważ elementy, nie przestawione przez podstawienie R, nie będą przestawione przez jego potęgi, to żadne z podstawień

$$R, R^2, R^3, \ldots, R^{r-1}$$

nie jest równe podstawieniu P lub jakiejkolwiek jego potędze. Gdy nadto ze związku

$$RPR^{-1} = P^a$$

wypada

$$R^k P^h = P^l R^k,$$

to *podstawienia, wyprowadzone z podstawień*

$$P = | X_z \quad X_{z+1} |,$$
$$R = | X_z \quad X_{az+b} |,$$

przedstawią systemat sprzężony podstawień liniowych, a porządek tego systematu określa nr, gdzie r wyznaczone z porównania

$$a^r \equiv 1 \pmod{n}.$$

Jeżeli liczba n ma pierwiastek pierwotny — niechaj takim wtedy będzie liczba α —, to porządek podstawienia

$$R' = | X_z, \quad X_{\alpha z+b} | ,$$

jest $\varphi(n)$, zaś podstawienia wyprowadzone z P i R′ utworzą systemat sprzężony wszystkich $n\varphi(n)$ podstawień liniowych. Dla tego :

Ażeby utworzyć systemat sprzężony wszystkich $n\varphi(n)$ *podstawień liniowych postaci*

$$| X_z \quad X_{\alpha z+b} |$$

z n elementów, w przypadku, kiedy liczba n ma pierwiastek pierwotny, — należy wyprowadzić wszystkie (różne) podstawienia z dwóch podstawień

$$| X_z \quad X_{z+b} | ,$$

$$| X_z \quad X_{\alpha z+1} | ,$$

gdzie α jest pierwiastek pierwotny liczby n, zaś b liczba podzielna w ogóle przez największy spólny dzielnik liczb $\alpha - 1$ i n.

Jeśli zaś liczba n nie posiada pierwiastków pierwotnych, to w ogóle nie można podstawieniami, wyprowadzonemi z dwóch podstawień P i R, utworzyć systematu sprzężonego wszystkich $n\varphi(n)$ podstawień liniowych. Jeżeli jednak chcemy ten systemat otrzymać, to należy w tym celu takiéj trzymać się drogi. *Weźmy dwa podstawienia*

$$P = | X_z \quad X_{z+1} | ,$$

$$R_1 = | X_z \quad X_{a_1+b_1} | ,$$

przy

$$a_1^{m_1} \equiv 1 \pmod{n},$$

i utwórzmy systemat sprzężony podstawień, wyprowadzonych z P *i* R_1, *który będzie porządku* $nm = i^{go}$

$$\begin{cases} 1, & P, & \ldots, P^{n-1}, \\ \ldots\ldots\ldots\ldots\ldots, \\ R_1^{m_1-1}, & R_1^{m_1-1}P, \ldots, R_1^{m_1-1}P^{n-1}, \end{cases}$$

a te podstawienia nazwijmy

$$1, \ A_1, \ A_2, \ \ldots, \ A_{i-1}. \tag{7}$$

Wyznaczmy następnie liczbę a_2, jak a_1 pierwszą względem n, którąby nadto nie mogła być porównaną, względem modułu n, z żadną z liczb

$$a_1, a_1^2, a_1^3, \ldots, a_1^{m_1-1},$$

i utwórzmy systemat sprzężony podstawień, wyprowadzonych z podstawienia

$$R_2 = | X_z \quad X_{a_2 z + b_2} |$$

i podstawień (7). *Jeśli*

$$a_2^{m_2} \equiv 1 (\mathrm{mod}\ n),$$

to ten systemat

$$\begin{cases} 1, & A_1, & \ldots, & A_{i-1} \\ R_2, & R_2 A_1, & \ldots, & R_2 A_{i-1}, \\ \ldots & \ldots & \ldots & \ldots \\ R_2^{m_2-1}, & R_2^{m_2-1} A_1, & \ldots, & R_2^{m_2-1} A_{i-1} \end{cases}$$

będzie porządku $m_2 i = n m_1 m_2 = k g^0$. *Podstawienia tego systematu możemy nazwać*

(8) $$1, \quad B_1, \quad B_2, \ldots, \quad B_{k-1}.$$

Wyznaczmy daléj liczbę a_3, *pierwszą względem* n, *którąby nie mogła być porównaną względem modułu* n *z żadną z liczb*

$$a_1, a_1^2, \ldots, a_1^{m_1-1}, a_2, a_2^2, \ldots, a_2^{m_2-1}.$$

Jeśli

$$a_3^{m_3} \equiv 1 (\mathrm{mod}\ n),$$

to podstawienia, wyprowadzone z

$$R_3 = | X_z \quad X_{a_3 z + b_3} |$$

i podstawień (8) *utworzą systemat sprzężony podstawień liniowych* $n m_1 m_2 m_3 g^0$ *porządku. Każda liczba* b_λ *jest w ogóle podzielną przez największy spólny dzielnik liczb* $a_\lambda - 1$ *i* n. *Postępując wciąż daléj takimże sposobem, dojdziemy nakoniec do tego, że* $m_1 m_2 m_3 \ldots = \varphi(n)$. *W ten tedy sposób otrzymamy w naszym tu przypadku systemat sprzężony wszystkich* $n\varphi(n)$ *podstawień liniowych.*