ROZDZIAŁ XVIII

PODSTAWIENIA

§ 1. Podstawienia. Ich znakowanie. Podstawienia odwrotne. Jeżeli zamiast ciągu elementów $a_1, a_2, \ldots, a_n$ bierzemy ciąg $b_1, b_2, \ldots, b_n$, to mówimy, żeśmy dokonali *podstawienia* lub *substytucji*), które oznaczamy przez

$$\begin{pmatrix} a_1 a_2 \ldots a_n \\ b_1 b_2 \ldots b_n \end{pmatrix}.$$

W każdej kolumnie dolnym elementem jest więc ten, który ma zastąpić element górny tejże kolumny.

Zajmiemy się tu w szczególności podstawieniami, polegającymi na tym, że zamiast danej permutacji elementów pewnego zbioru skończonego bierzemy inną permutację elementów tegoż zbioru.

Jeżeli zamiast permutacji $a_1 a_2 \ldots a_n$ bierzemy permutację $a_{\alpha_1} a_{\alpha_2} \ldots a_{\alpha_n}$, to dla uproszczenia przy zapisywaniu podstawienia

$$\begin{pmatrix} a_1 & a_2 & \ldots a_n \\ a_{\alpha_1} a_{\alpha_2} \ldots & a_{\alpha_n} & \end{pmatrix}$$

będziemy opuszczali literę a i wypisywali w obu wierszach tylko wskaźniki. Rozważane podstawienie zapiszemy więc prościej:

$$\begin{pmatrix} 1\ 2 \ldots n \\ \alpha_1 \alpha_2 \ldots \alpha_n \end{pmatrix}$$

lub, przy stałym n, jeszcze prościej: $\begin{pmatrix} k \\ \alpha_k \end{pmatrix}$.

To samo podstawienie moglibyśmy oczywiście zapisać, zmieniając dowolnie porządek kolumn, np.:

$$\begin{pmatrix} n & n-1 & \ldots & 1 \\ \alpha_n & \alpha_{n-1} & \ldots & \alpha_1 \end{pmatrix}.$$

Ogólnie, dla dowolnej permutacji $\gamma_1 \gamma_2 \ldots \gamma_n$ liczb $1, 2, \ldots, n$ jest:

$$\begin{pmatrix} 1 & 2 & \ldots & n \\ \alpha_1 & \alpha_2 & \ldots & \alpha_n \end{pmatrix} = \begin{pmatrix} \gamma_1 & \gamma_2 & \ldots & \gamma_n \\ \alpha_{\gamma_1} & \alpha_{\gamma_2} & \ldots & \alpha_{\gamma_n} \end{pmatrix}$$

Dwa podstawienia są *różne* wtedy i tylko wtedy, jeżeli jakiś element został zastąpiony w jednym z nich przez inny element niż w drugim.

Podstawienia:

$$\begin{pmatrix} 1 & 2 & \dots & n \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \end{pmatrix}, \qquad \begin{pmatrix} 1 & 2 & \dots & n \\ \beta_1 & \beta_2 & \dots & \beta_n \end{pmatrix}$$

są więc różne wtedy i tylko wtedy, jeżeli permutacje $\alpha_1\alpha_2\dots\alpha_n$ i $\beta_1\beta_2\dots\beta_n$ są różne.

W obrębie permutacyj z n elementów mamy zatem $n!$ różnych podstawień.

Dla każdego podstawienia

$$S=\begin{pmatrix} 1 & 2 & \dots & n \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \end{pmatrix},$$

(gdzie $\alpha_1\alpha_2\dots\alpha_n$ jest permutacją liczb $1,2,\dots,n$) istnieje podstawienie *odwrotne*:

$$S^{-1}=\begin{pmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_n \\ 1 & 2 & \dots & n \end{pmatrix},$$

które też moglibyśmy napisać w postaci:

$$S^{-1}=\begin{pmatrix} 1 & 2 & \dots & n \\ \beta_1 & \beta_2 & \dots & \beta_n \end{pmatrix},$$

zmieniając porządek kolumn $\begin{pmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_n \\ 1 & 2 & \dots & n \end{pmatrix}$ tak, aby elementy pierwszego wiersza dały ciąg $1,2,\dots,n$.

§ 2. Iloczyn podstawień. Jeżeli po dokonaniu podstawienia:

$$S=\begin{pmatrix} 1 & 2 & \dots & n \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \end{pmatrix}$$

dokonamy podstawienia:

$$T=\begin{pmatrix} 1 & 2 & \dots & n \\ \beta_1 & \beta_2 & \dots & \beta_n \end{pmatrix},$$

to otrzymamy z permutacji $1\,2\dots n$ permutację $\beta_{\alpha_1}\beta_{\alpha_2}\dots\beta_{\alpha_n}$, którą moglibyśmy też otrzymać z permutacji $1\,2\dots n$ bezpośrednio za pomocą jednego tylko podstawienia:

$$P=\begin{pmatrix} 1 & 2 & \dots & n \\ \beta_{\alpha_1} & \beta_{\alpha_2} & \dots & \beta_{\alpha_n} \end{pmatrix}.$$

Podstawienie P nazywamy *iloczynem* podstawienia S przez podstawienie T i piszemy:

$$P=ST\ ^{1}).$$

Jest więc:

$$\begin{pmatrix} 1 & 2 & \dots & n \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \end{pmatrix}\begin{pmatrix} 1 & 2 & \dots & n \\ \beta_1 & \beta_2 & \dots & \beta_n \end{pmatrix}=\begin{pmatrix} 1 & 2 & \dots & n \\ \beta_{\alpha_1} & \beta_{\alpha_2} & \dots & \beta_{\alpha_n} \end{pmatrix}.$$

Podobnie:

$$\begin{pmatrix} 1 & 2 & \dots & n \\ \beta_1 & \beta_2 & \dots & \beta_n \end{pmatrix}\begin{pmatrix} 1 & 2 & \dots & n \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \end{pmatrix}=\begin{pmatrix} 1 & 2 & \dots & n \\ \alpha_{\beta_1} & \alpha_{\beta_2} & \dots & \alpha_{\beta_n} \end{pmatrix}.$$

Iloczyn podstawień na ogół nie jest przemienny, np.:

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}=\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad \text{zaś} \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}=\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

Dla $S=\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ i $T=\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ mamy więc $ST\neq TS$. Natomiast iloczyn podstawień jest *łączny*, mianowicie dla:

$$S=\begin{pmatrix} 1 & 2 & \dots & n \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \end{pmatrix}, \qquad T=\begin{pmatrix} 1 & 2 & \dots & n \\ \beta_1 & \beta_2 & \dots & \beta_n \end{pmatrix}, \qquad U=\begin{pmatrix} 1 & 2 & \dots & n \\ \gamma_1 & \gamma_2 & \dots & \gamma_n \end{pmatrix}$$

mamy zawsze:

$$(ST)U=\begin{pmatrix} 1 & 2 & \dots & n \\ \beta_{\alpha_1} & \beta_{\alpha_2} & \dots & \beta_{\alpha_n} \end{pmatrix}\begin{pmatrix} 1 & 2 & \dots & n \\ \gamma_1 & \gamma_2 & \dots & \gamma_n \end{pmatrix}=\begin{pmatrix} 1 & 2 & \dots & n \\ \gamma_{\beta\alpha_1} & \gamma_{\beta\alpha_2} & \dots & \gamma_{\beta\alpha_n} \end{pmatrix},$$

$$S(TU)=\begin{pmatrix} 1 & 2 & \dots & n \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \end{pmatrix}\begin{pmatrix} 1 & 2 & \dots & n \\ \gamma_{\beta_1} & \gamma_{\beta_2} & \dots & \gamma_{\beta_n} \end{pmatrix}=\begin{pmatrix} 1 & 2 & \dots & n \\ \gamma_{\beta\alpha_1} & \gamma_{\beta\alpha_2} & \dots & \gamma_{\beta\alpha_n} \end{pmatrix},$$

zatem

$$(ST)U=S(TU).$$

Oba te iloczyny oznaczamy poprostu przez STU.

Podobnie postępujemy dla dowolnej skończonej liczby czynników.

---

[1]) Niektórzy autorzy piszą tu czynniki S i T w odwrotnym porządku, podobnie jak przy superpozycji funkcyj. Pochodzi to stąd, że operator S można traktować jako funkcję permutacji, mianowicie:

$$S(\gamma_1\gamma_2\dots\gamma_n)=(\gamma_{\alpha_1}\gamma_{\alpha_2}\dots\gamma_{\alpha_n}).$$

Iloczyn k czynników, z których każdy jest tym samym podstawieniem S, oznaczamy przez S^k. Np.:

$$\begin{pmatrix}1 & 2 & \dots & n\\ a_1 & a_2 & \dots & a_n\end{pmatrix}^2=\begin{pmatrix}1 & 2 & \dots & n\\ a_{a_1} & a_{a_2} & \dots & a_{a_n}\end{pmatrix}.$$

Dla dowolnych naturalnych k i l mamy oczywiście:

$$S^kS^l=S^lS^k=S^{k+l} \quad \text{i} \quad (S^k)^l=S^{kl}.$$

Podstawienie *tożsamościowe* $S_0=\begin{pmatrix}1 & 2 & \dots & n\\ 1 & 2 & \dots & n\end{pmatrix}$ ma oczywiście tę własność, że dla każdego podstawienia S jest:

$$S_0S=SS_0=S.$$

Podstawienie S_0 zachowuje się więc przy mnożeniu podstawień tak, jak 1 przy mnożeniu liczb. Umawiamy się przeto oznaczać S poprostu przez 1:

$$\begin{pmatrix}1 & 2 & \dots & n\\ 1 & 2 & \dots & n\end{pmatrix}=1.$$

Jeżeli S^{-1} oznacza podstawienie odwrotne do podstawienia S, to oczywiście:

$$SS^{-1}=S^{-1}S=1.$$

Z twierdzenia, że każda permutacja ciągu liczb $1,2,\dots,n$ może być otrzymana z każdej innej przez stosowanie skończoną liczbę razy transpozycyj dwu sąsiednich elementów (ob. Rozdział I, § 3, tw. 1, str. 4), wynika z łatwością, że każda permutacja ciągu $1,2,\dots,n$ może być otrzymana z permutacji $1\,2\dots n$ przez stosowanie skończoną liczbę razy (w odpowiednim porządku) dwu podstawień: podstawienia cyklicznego $\begin{pmatrix}1 & 2 & 3 & \dots & n-1 & n\\ 2 & 3 & 4 & \dots & n & 1\end{pmatrix}$ i transpozycji $\begin{pmatrix}1 & 2 & 3 & \dots & n\\ 2 & 1 & 3 & \dots & n\end{pmatrix}$ [1]. Wypisując te dwa podstawienia jako czynniki (w odpowiednim porządku) skończoną liczbę razy, możemy więc otrzymać każde podstawienie dla ciągu liczb $1,2,\dots,n$.

§ 3. Przedstawienia podstawień za pomocą cyklów. Wyrażenia analityczne podstawień. Jeżeli w danym podstawieniu $S=\begin{pmatrix}1 & 2 & \dots & n\\ a_1 & a_2 & \dots & a_n\end{pmatrix}$ jest $a_1\neq 1$, to podstawienie S przeprowadza element a_1 na element a_{a_1} różny od a_1. Jeżeli również $a_{a_1}\neq 1$, to podstawienie S przeprowadza element a_{a_1} na element $a_{a_{a_1}}$, różny od a_1 i od a_{a_1}. Jeżeli $a_{a_{a_1}}\neq 1$, to rozumując w ten sposób dalej, otrzymujemy wciąż nowe elementy. Nie możemy ich jednak otrzymać więcej niż n (t.j. więcej niż liczb w ciągu $1,2,\dots,n$). Dojdziemy zatem wreszcie znowu do elementu 1 i w ten sposób cykl się zamknie. Jeżeli cykl ten nie wyczerpuje wszystkich liczb $1,2,\dots n$, to biorąc w górnym wierszu którykolwiek (np. pierwszy) element, nie należący do otrzymanego cyklu, możemy dla niego utworzyć nowy cykl $\beta_1 a_{\beta_1} a_{a_{\beta_1}}\dots$ i t.d., aż wyczerpiemy (za pomocą skończonej liczby cyklów) wszystkie liczby $1,2,\dots n$.

Cykl daje t.zw. podstawienie *cykliczne*:

$$\begin{pmatrix}\beta_1 & \beta_2 & \dots & \beta_{k-1} & \beta_k\\ \beta_2 & \beta_3 & \dots & \beta_k & \beta_1\end{pmatrix},$$

gdzie każdy wyraz górnego ciągu $\beta_1,\beta_2,\dots,\beta_k$ został zastąpiony przez następny wyraz tego ciągu, zaś jego ostatni wyraz — przez wyraz pierwszy.

Podstawienie to oznaczamy krócej przez

$$(\beta_1\beta_2\dots\beta_k)$$

(t.j. opuszczamy dolny wiersz).

Jeżeli podstawienie cykliczne dotyczy nie wszystkich elementów permutacji $1\,2\dots n$ (t.j. jeżeli $k<n$), to znaczy, że pozostałe zostały zastąpione każdy sam przez siebie (t.j. nie uległy zmianie). Z powyższego wynika

Twierdzenie 1. *Każde podstawienie może być przedstawione jako iloczyn (skończonej liczby) podstawień cyklicznych, dotyczących samych różnych elementów.*

W szczególności *transpozycja* (por. Rozdział I, § 3, str. 3) *jest* na mocy swego określenia *cyklem złożonym z dwu elementów.*

Jak wiemy z Rozdziału I, § 4, każde podstawienie jest iloczynem samych tylko transpozycyj, niekoniecznie jednak dotyczących samych różnych elementów. Wynika to też z twierdzenia 1 i z uwagi, że *każde podstawienie cykliczne jest iloczynem samych transpozycyj*; istotnie:

$$(1\ 2\ \dots\ k)=(1\ 2)(1\ 3)\ \dots\ (1\ k).$$

W podstawieniu

$$S=\begin{pmatrix}1 & 2 & \dots & n\\ a_1 & a_2 & \dots & a_n\end{pmatrix}$$

[1]) Por. moją uwagę w artykule Sophie Piccard, Fundamenta Mathematicae, Tom 24 (1935), str. 300.

a_k jest funkcją zmiennej k, określoną dla $k=1,2,\ldots,n$. Funkcję tę można przedstawić zawsze w postaci wielomianu zmiennej k co najwyżej $(n-1)$-go stopnia, a to na podstawie wzoru interpolacyjnego Lagrange'a (ob. Rozdział VIII, § 12, tw. 22, str. 130). Mamy tu bowiem dla szukanego wielomianu warunki $f(k)=a_k$ dla $k=1,2,\ldots,n$.

PRZYKŁADY:

1. $\begin{pmatrix}1&2&3&4&5&6\\4&6&1&3&2&5\end{pmatrix}=(1\ 4\ 3)(2\ 6\ 5)$, 2. $\begin{pmatrix}1&2&3&4&5\\2&4&3&5&1\end{pmatrix}=(1\ 2\ 4\ 5)$,

3. $\begin{pmatrix}1&2&3&4&5\\3&4&5&1&2\end{pmatrix}=(1\ 3\ 5\ 2\ 4)=(1\ 2\ 3\ 4\ 5)^2=(1\ 3)(2\ 4)(1\ 5)(1\ 2)$,

4. $(1\ 2\ 3\ 4\ 5)^3=(1\ 4\ 2\ 5\ 3)$, 5. $(1\ 2\ 3\ 4\ 5)^5=1$,

6. $\begin{pmatrix}1&2&3&4&5&6&7&8\\3&6&7&1&4&5&8&2\end{pmatrix}=(1\ 3\ 7\ 8\ 2\ 6\ 5\ 4)$,

7. $\begin{pmatrix}1&2&3&4&5&6&7&8\\2&1&3&5&7&8&6&4\end{pmatrix}=(8\ 4\ 5\ 7\ 6)(1\ 2)(3)$,

8. $\begin{pmatrix}1&2&3&4&5&6&7&8\\2&3&6&5&8&1&4&7\end{pmatrix})=(8\ 7\ 4\ 5)(1\ 2\ 3\ 6)$,

9. $(2\ 1\ 3)=(1\ 2\ 3)(1\ 2\ 3)$, 10. $(1\ 2\ 3)=(1\ 2)(4\ 5)(4\ 5)(1\ 3)$,

11. Dla $1, a, b, c, d$ różnych jest $(a\,b\,c)=(1\,d\,a)(1\,b\,c)(1\,a\,d)$, lecz dla $d=b$ byłoby to fałszywe.

12. Mamy:

$(1\ 2\ \ldots\ n)^2=(1\ 3\ \ldots\ n-1)(2\ 4\ \ldots\ n)$ dla n parzystych,

$(1\ 2\ \ldots\ n)^2=(1\ 3\ \ldots\ n\cdot 2\cdot 4\ \ldots\ n-1)$ dla n nieparzystych.

§ 4. Podstawienia w ciągu nieskończonym liczb naturalnych. Rozważaliśmy dotąd podstawienia w ciągu skończonym elementów. Można też badać podstawienia w zbiorach nieskończonych, innymi słowy przekształcenia wzajemnie jednoznaczne tych zbiorów na same siebie. W szczególności, można badać podstawienia w ciągu wszystkich liczb naturalnych:

$$\begin{pmatrix}1&2&3&\ldots\\a_1&a_2&a_3&\ldots\end{pmatrix}.$$

W podstawieniu tym $a_1a_2a_3\ldots$ jest *permutacją ciągu nieskończonego* 1 2 3 ..., t.j. ciągiem różniącym się od niego co najwyżej porządkiem wyrazów czyli ciągiem zawierającym raz i tylko raz każdą liczbę naturalną.

Jak wiadomo z Teorii mnogości, podstawień takich jest continuum. Niektóre własności podstawień skończonych ulegają zmianie przy przejściu do podstawień dla zbiorów nieskończonych.

Podstawieniami w ciągu nieskończonym liczb naturalnych zajmowali się pp. Schreier i Ulam[1]). Badali oni m. in. rozkłady takich podstawień na cykle (skończone oraz nieskończone typu $\omega^*+\omega$) i dowiedli, że dla permutacyj nieskończonych nie da się ustalić pojęcie permutacyj „parzystych", t. j., że zbiór wszystkich podstawień dla ciągu 1, 2, 3, ... nie da się podzielić na dwie klasy A i B w ten sposób, aby iloczyn każdych dwóch podstawień tej samej klasy należał do A, zaś różnych klas do B. Fakt ten ma pewne zastosowanie w Topologii[2]).

W Rozdziale XIX (§ 1, przykład 17, str. 309) okażemy, że zbiór wszystkich podstawień w obrębie dowolnego danego zbioru elementów tworzy t.zw. *grupę*. W ten sposób z ogólnych własności grup będą w szczególności wynikały różne własności podstawień. Dlatego też nie dowodzimy tu tych własności specjalnie dla podstawień.

[1]) J. Schreier i S. Ulam, Studia Mathematica, Tom 4 (1933), str. 135.

[2]) Ob. tamże, str. 139.