

Представяне на елементите на симетричната група  $S_n$  като произведение от цикли  
автор - Михаил Михайлович Постников  
превод с незначителни допълнения и изменения - Станчо Павлов

Нека

$$a = \begin{pmatrix} 1 & 2 & \dots & n \\ k_1 & k_2 & \dots & k_n \end{pmatrix}$$

е произволно разместване (пермутация, субституция) от  $n$ -ти ред.

Ако някое от числата  $i$  е различно от  $k_i$  казваме, че  $i$  действително се премества от разместването  $a$ . Иначе казваме, че  $i$  остава на място. Ще разгледаме цикличната подгрупа на  $S_n$ , състояща се от степените на  $a$ . Ако  $m$  е редът на тази подгрупа, то тя се състои от  $m$ -те разместванията

$$a^0 = e, a, a^2, a^3, \dots, a^{m-1}$$

при което всички тези размествания са различни. Нека  $i_0$  е произволно число, което действително се премества от  $a$ .

Да означим с  $i_k$ , числото в което се премества  $i_0$  при разместването  $a^k$ .

Разместването  $a$  премества числото  $i_k$  в  $i_{k+1}$ . Ако се окаже че  $i_k = i_{k+1}$  то, прилагайки към това равенство разместването  $a^{-k}$  получаваме че  $i_0 = i_1$ , противоположно на предположението, че  $i_0$  действително се премества от  $a$ .

Тогава две последователни числа от тази редица непременно са различни.

Следователно всички числа  $i_0, i_1, i_2, \dots$  действително се преместват от разместването  $a$ . Сред тези числа има не повече от  $m$  различни, защото  $i_0 = i_m$ . Ако със числата

$$i_0, i_1, i_2, \dots, i_{m-1}$$

се изчерпват всички числа, действително премествани от разместването  $a$  то  $a$  се нарича *цикъл* и се означава със символа  $(i_0, i_1, i_2, \dots, i_{m-1})$ . Цикълът действително премества единствено числата, участващи в него. Неговата форма е:

$$a = \begin{pmatrix} i_0 & i_1 & \dots & i_{m-1} & j_1 & j_2 & \dots & j_{n-m} \\ i_1 & i_2 & \dots & i_0 & j_1 & j_2 & \dots & j_{n-m} \end{pmatrix},$$

при което числата  $j_1, j_2, \dots, j_{n-m}$  са от  $1, 2, \dots, n$  и са различни от  $i_0, i_1, \dots, i_{m-1}$ . В този случай числата  $i_0, i_1, i_2, \dots, i_{m-1}$  също са различни. Наистина, ако  $i_k = i_{k+l}$   $k$  и  $l$  са по-малки от  $m$  ще достигнем до противоречие: Действително  $i_k = i_{k+l}$  прилагайки към това равенство разместването  $a^{-k}$  получаваме:

$$(i_k)a^{-k} = (i_{k+l})a^{-k} \Rightarrow i_0 = i_l$$

Нека  $q$  е произволно число, по-малко от  $m$  Тогава:  $a^l = a^{-q}a^l a^q$  Прилагайки това разместване към числото  $i_q$

$$(i_q)a^l = (i_q)a^{-q}a^l a^q = (i_0)a^l a^q = (i_l)a^q = (i_0)a^q = i_q$$

Получаваме, че  $a^l$  оставя всяко от числата  $i_0, i_1, i_2, \dots, i_{m-1}$  на място. За останалите, които остават неподвижни при  $a$  ще остават такива и при  $a^l$ . Откъдето следва, че  $a^l = e$  а това е в противоречие с това, че  $a$  е цикъл, който действително премества  $i_0$ . Да отбележим, че за всяка система  $i_0, i_1, i_2, \dots, i_{m-1}$  от различни числа съществува цикъл (очевидно единствен), преместващ числото  $i_0$  в  $i_1$ . този цикъл се представя със символа

$$(i_0 i_1 \dots i_{m-1}) = \begin{pmatrix} i_0 & i_1 & \dots & i_{m-1} & j_1 & j_2 & \dots & j_{n-m} \\ i_1 & i_2 & \dots & i_0 & j_1 & j_2 & \dots & j_{n-m} \end{pmatrix},$$

където  $j_1, j_2, \dots, j_{n-m}$  са от  $1, 2, \dots, n$  и са различни от  $i_0, i_1, \dots, i_{m-1}$ .

Да отбележим, още, че записът на цикъла във вида  $(i_0 i_1 \dots i_{m-1})$  не е еднозначен. Именно:

$$(i_0 i_1 \dots i_{m-1}) = (i_1 \dots i_{m-1} i_0) = (i_{m-1} i_0 i_1 \dots i_{m-2})$$

т.е. записът на цикъла може да започва с всяко, действително премествано число. С точност до преобразование от този вид записът на цикъла е еднозначен.

Броят на числата, които действително се преместват от цикъла  $a$  се нарича неговата *дължина*. От казаното е ясно, че

*дължината на цикъла е равна на неговия ред*

Разместването

$$a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 5 & 4 & 3 & 1 & 9 & 6 & 7 & 8 \end{pmatrix}$$

се представя като произведение от независими цикли така:

$$a = (125)(34)(6987)$$

Най-малката възможна дължина на един цикъл е 2.

Такива цикли се наричат *транспозиции*.

Транспозицията  $(ij)$  премества числото  $i$  в числото  $j$ , числото  $j$  в числото  $i$  и оставя всички останали числа на място.

**З а д а ч а** Покажете, че разместване, което действително премества само две числа, се явява транспозиция. Всеки цикъл с дължина  $n$  се разлага в произведение от транспозиции:

$$(i_0 i_1 i_2 i_3 \cdots i_{m-2} i_{m-1}) = (i_0 i_1)(i_0 i_2)(i_0 i_3) \cdots (i_0 i_{m-2})(i_0 i_{m-1})$$

Два цикъла се наричат *независими* ако те не съдържат общи, действително премествани числа.

Ясно е че при умножаване на два независими цикъла те могат да се разместват. Т.е. те комутират помежду си.

Оказва се, че

*всяко нетъждествено разместване се явява произведение от независими цикли.*

Ще докажем това твърдение по индукция по броя  $s$  на действително преместваните числа. За този цел първо да забележим, че  $s$  не може да е равно на единица. Наистина, ако разместването  $a$  привежда числото  $i$  в числото  $j$ , то  $j$  не може да остане неподвижно, защото в противен случай две различни числа  $i$  и  $j$  ще се изобразяват, при разместването  $a$ , в едно и също число -  $j$ . Затова  $s \geq 2$ . Ако  $s = 2$  то разместването е транспозиция и следователно теоремата за нея е вярна. Така е обоснован началния етап на индукцията. Да допуснем сега, че теоремата е доказана за всички размествания, действително преместващи по малко от  $s$  числа и да разгледаме произволно разместване  $a$ , което действително размества  $s$  числа. Нека  $i_0$  е едно от тези числа, което действително се премества от разместването  $a$ . Прилагайки към това число изложеното по-горе построение (т.е. действайки му със степените на  $a$ ) ще получим числата  $i_0, i_1, \cdots, i_k, \cdots$ , които действително си преместват от разместването  $a$  (погледни по-горе). Нека  $i_q$  е първото от тези числа с положителен номер, съвпадащо с  $i_0$ . Такова число съществува, така например  $i_m$ , където  $m$  е редът на разместването  $a$ , е равно на  $i_0$ . Ще докажем, че числата  $i_0, i_1, \cdots, i_{q-1}$  са всичките различни. Действително, ако например  $i_l = i_{l+p}$ , то, прилагайки към това равенство разместването  $a^{-l}$ , ще получим  $i_0 = i_p$ , което поради минималността на числото  $q$  е невъзможно.

Понеже всички числа  $(i_0 i_1 i_2 i_3 \cdots i_{q-1})$  са различни ( и  $q > 1$  понеже  $i_0 \neq i_1$  виж по-горе ) ние можем да съставим цикъла  $(i_0 i_1 i_2 \cdots i_{q-1})$ . Разместването  $a (i_0 i_1 i_2 \cdots i_{q-1})^{-1}$  оставя на местата си всички числа, които остават на местата си и при разместването  $a$ , а също така и всички числа  $i_0, i_1, i_2, \cdots, i_{q-1}$ . По такъв начин, то действително промества не повече от  $s - q$  числа и, следователно, по индукционното предположение, се разлага в произведение от независими цикли. За завършване на доказателството остава да забележим, че тези цикли са независими и с цикъла  $(i_0 i_1 i_2 \cdots i_{q-1})$ .

Понеже всеки цикъл се разлага на транспозиции, то от доказаната теорема следва, че

*всяко разместване се разлага в произведение на транспозиции ( но в общия случай не независими ).*

Числата, участващи в независимите цикли, на които се разлага едно разместване са числата, които действително се преместват от него. Всеки цикъл от разлагането се състои от тези числа, които се преместват едно в друго от степените на дадено разместване. По такъв начин, броят и строежът на независимите цикли, на които се разлага едно разместване, еднозначно се определя от него. С други думи

*разлагането на едно разместване в произведение от независими цикли е еднозначно (с точност да реда на множителите).*

Четни и нечетни размествания Знакопроменлива група  $(A_n)$

Всяко разместване се представя като произведение на транспозиции. Но това представяне, в общия случай, не е еднозначно. Например:

$$(j k)(i k) = (i j)(j k) = (i k j) \text{ ако } i \neq j$$

$$(i j)(i k) = (i k)(j k) = (i j k) \text{ ако } j \neq k.$$

Горните две формули изразяват, както лесно се вижда, един и същи факт но в различни означения. Л е м а  
*Ако произведението на няколко транспозиции е равно на тъждественото разместване то броят на тези транспозиции е четно число.*

Ще докажем лемата по индукция не по броя на транспозициите,  $k - 1$ , участващи в произведението

$$(i_1 i_2)(i_3 i_4) \cdots (i_{2k-1} i_{2k}) = e$$

а по броя на различните числа, участващи в произведението на транспозиции отъдно на равенството. Този брой ще означим с  $s$ . При  $s = 2$   $e$  се представя като произведение на една транспозиция сама със себе си т.е. със своя степен:  $e = (i j)^2$ . Ето защо показателят  $p$  трябва да е четно число.

Предполагаме сега, че лемата е доказана за всяко произведение от транспозиции, равно на тъждественото разместване, в което се съдържат по-малко от  $s$  различни числа. Разглеждаме тъждеството:

$$(i_1 i_2)(i_3 i_4) \cdots (i_{2q-1} i_{2q}) = e,$$

в което, отляво се съдържат  $s$  различни символа. Да определим един от тях, който ще означим с  $i$ . Използвайки равенството  $(j k)(i k) = (i j)(j k)$ , ние можем да предвижим този символ в началото на произведението:

$$(i j_1)(i j_2) \cdots (i j_p)(k_1 k_2)(k_3 k_4) \cdots (k_{2r-1} k_{2r}) = e,$$

в което всички числа  $k_1, k_2, \dots, k_{2r}$  са различни от  $i$ . Ако  $p > 1$  използвайки равенството  $(i j)(i k) = (i k)(j k)$  или  $(i j)(i j) = e$  можем да приведем равенството до такова, но с по-малко  $p$ . В резултат на такива преобразования, ние или ще премахнем всички транспозиции съдържащи  $i$ , или ще получим произведение, в което участва само една такава транспозиция.

$$(i j_1)(l_1 l_2)(l_3 l_4) \cdots (l_{2t-1} l_{2t}) = e.$$

Но това произведение привежда числото  $j_1$  в  $i$  и затова не може да бъде тъждественото разместване. Следователно последният случай е невъзможен. Така ние ще получим произведение от транспозиции, не съдържащо  $i$  и равно на тъждественото разместване. Това произведение не съдържа нови числа. По индукционното допускане то съдържа четен брой транспозиции. Остава да отбележим, че при описаните преобразования броят на транспозициите или не се променя при използването на  $(j k)(i k) = (i j)(j k) = (i k j)$  или  $(i j)(i k) = (i k)(j k) = (i j k)$  или се променя с четен брой при използването на  $(i j)(i j) = e$  Затова изходното произведение

$$(i_1 i_2)(i_3 i_4) \cdots (i_{2q-1} i_{2q}) = e$$

също се състои от четен брой транспозиции. С това лемата е доказана.

Нека сега едно разместване  $a$  е представено по два начина като произведение на транспозиции:

$$\begin{aligned} a &= (i_1 i_2)(i_3 i_4) \cdots (i_{2p-1} i_{2p}), \\ a &= (j_1 j_2)(j_3 j_4) \cdots (j_{2q-1} j_{2q}) \end{aligned}$$

(първото съдържа  $p$  транспозиции а второто  $q$ ). Тогава

$$(i_1 i_2) \cdots (i_{2p-1} i_{2p})(j_{2q} j_{2q-1}) \cdots (j_2 j_1) = aa^{-1} = e$$

и, следователно, по доказаната лема, числото  $p + q$  е четно.

По такъв начин числата  $p$  и  $q$  са или едновременно четни, или едновременно нечетни. С други думи, *при всевъзможните представяния на едно разместване като произведение на транспозиции четността на техният брой ще бъде една и съща.*

Едно разместване от  $S_n$  се нарича *четно* ако то се разлага на четен брой транспозиции и *нечетно* в противоположния случай. Съгласно доказаната теорема, четността на разместването не зависи от начина, по който то е представено като произведение на транспозиции. Тъждественото разместване е четно.

Всяка транспозиция, или въобще цикъл с четна дължина е нечетно разместване а всеки цикъл с нечетна дължина ( в частност с дължина 3) е четно.

Ако

$$a = (i_1 i_2)(i_3 i_4)(i_5 i_6) \cdots (i_{s-3} i_{s-2})(i_{s-1} i_s)$$

то

$$a^{-1} = (i_s i_{s-1})(i_{s-2} i_{s-3}) \cdots (i_6 i_5)(i_4 i_3)(i_2 i_1),$$

( Това следва от факта, че при групите е изпълнено равенството:  $(g_1 g_2 \cdots g_{n-1} g_n)^{-1} = g_n^{-1} g_{n-1}^{-1} \cdots g_2^{-1} g_1^{-1}$  ), откъдето следва, че:

*обратното на четно разместване е също четно а обратното на нечетно разместване е нечетно.*

По-нататък, ако

$$\begin{aligned} a &= (i_1 i_2) \cdots (i_{s-1} i_s) \\ b &= (j_1 j_2) \cdots (j_{t-1} j_t) \end{aligned}$$

то

$$ab = (i_1 i_2) \cdots (i_{s-1} i_s) (j_1 j_2) \cdots (j_{t-1} j_t)$$

Поради това:

*произведението на две четни или две нечетни размествания е четно разместване; произведението на четно и нечетно разместване е нечетно разместване.*

Оттук следва, че съвкупността на всички четни размествания (от даден ред  $n$ ) образуват подгрупа на  $\mathbf{S}_n$ . Тази подгрупа се означава с  $\mathbf{A}_n$  и се нарича *знакопроменлива*.

Понеже за всяко четно разместване  $a$  и всяко разместване  $b$  произведението  $ba^{-1}b$  е четно разместване, то знакопроменливата група  $\mathbf{A}_n$  е нормален делител на симетричната група  $\mathbf{S}_n$ .

Понеже за всеки две нечетни размествания  $a$  и  $b$  разместването  $ab^{-1}$  е четно, т.е. принадлежи на групата  $\mathbf{A}_n$ , то всички нечетни размествания образуват един съседен клас по подгрупата  $\mathbf{A}_n$ . Следователно фактор групата  $\mathbf{S}_n/\mathbf{A}_n$  се състои само от 2 елемента, т.е. има порядък 2.

Затова:

*Редът на групата  $\mathbf{A}_n$  т.е. броят на четните размествания от ред  $n$  е равен на  $\frac{1}{2}n!$ .*

Строеж на знакопроменливата и симетричната групи

Ще изучим строежа на групата  $\mathbf{A}_n$  при различни стойности на  $n$ .

При  $n = 2$  знакопроменливата група се състои само от тъждественото разместване.

При  $n = 3$  знакопроменливата група има ред  $\frac{1}{2}3! = 3$  и, следователно е циклична, защото е от прост ред.

Като неин образуващ можем да вземем всяко четно разместване от трети ред (например, цикъла  $(1\ 2\ 3)$ ).

При  $n = 4$  знакопроменливата група има ред  $\frac{1}{2}4! = 12$  и се състои от следните елементи:

$e$

$$t_1 = (12)(34), t_2 = (13)(24), t_3 = (14)(23)$$

$$s_1 = (123), s_2 = (124), s_3 = (132), s_4 = (134)$$

$$s_5 = (142), s_6 = (143), s_7 = (234), s_8 = (243).$$

Лесно се проверява, че

$$\begin{aligned} t_1^2 = t_2^2 = t_3^2 = e & \quad t_2 t_1 = t_1 t_2 = t_3 \\ t_3 t_1 = t_1 t_3 = t_2 & \quad t_3 t_2 = t_2 t_3 = t_1. \end{aligned}$$

Следователно, разместванията  $e, t_1, t_2, t_3$  образуват подгрупа на  $\mathbf{A}_4$ . Тази група се нарича *група на Клайн* и се означава се с  $\mathbf{V}_4$ . Групата  $\mathbf{V}_4$  е абелева и има ред 4. По-нататък е лесно да се провери, че

$$\begin{aligned} s_1 t_1 s_1^{-1} = t_2, & \quad s_1 t_2 s_1^{-1} = t_3, & \quad s_1 t_3 s_1^{-1} = t_1 \\ s_2 t_1 s_2^{-1} = t_3, & \quad s_2 t_2 s_2^{-1} = t_1, & \quad s_2 t_3 s_2^{-1} = t_2 \\ s_3 t_1 s_3^{-1} = t_3, & \quad s_3 t_2 s_3^{-1} = t_1, & \quad s_3 t_3 s_3^{-1} = t_2 \\ s_4 t_1 s_4^{-1} = t_2, & \quad s_4 t_2 s_4^{-1} = t_3, & \quad s_4 t_3 s_4^{-1} = t_1 \\ s_5 t_1 s_5^{-1} = t_2, & \quad s_5 t_2 s_5^{-1} = t_3, & \quad s_5 t_3 s_5^{-1} = t_1 \\ s_6 t_1 s_6^{-1} = t_3, & \quad s_6 t_2 s_6^{-1} = t_1, & \quad s_6 t_3 s_6^{-1} = t_2 \\ s_7 t_1 s_7^{-1} = t_3, & \quad s_7 t_2 s_7^{-1} = t_1, & \quad s_7 t_3 s_7^{-1} = t_2 \\ s_8 t_1 s_8^{-1} = t_2, & \quad s_8 t_2 s_8^{-1} = t_3, & \quad s_8 t_3 s_8^{-1} = t_1 \end{aligned}$$

Следователно групата  $\mathbf{V}_4$  се явява нормален делител на групата  $\mathbf{A}_4$ . Съответната фактор-група  $\mathbf{A}_4/\mathbf{V}_4$  има порядък 3 и затова се явява циклична.

Понеже групата  $\mathbf{V}_4$  е абелева, то всяка нейна подгрупа, например цикличната група  $\mathbf{C}_4$  от втори ред, състояща се от тъждественото разместване и разместването  $t_1$  се явява нормален делител (на групата  $\mathbf{V}_4$ , но не на цялата група  $\mathbf{A}_4$ ). Редът на тази фактор-група е равен на две, следователно и тази фактор-група е циклична.

По такъв начин, редицата от подгрупи

$$\mathbf{A}_4 \supset \mathbf{V}_4 \supset \mathbf{C}_4 \supset e$$

се явява разрешим ред за групата  $\mathbf{A}_4$ . С това е доказано, че групата  $\mathbf{A}_4$  е разрешима.

Да разгледаме сега случая  $n \geq 5$ . Нека  $N$  е произволен нормален делител на групата  $A_n$ , различен от  $e$ . Понеже  $N \neq e$ , то в  $N$  съществува поне едно разместване  $t \neq e$ . Разлагането на  $t$  като произведение от независими цикли може да има една от формите, описани в 't' колоната от таблицата:

$N$	$t$	$r$	$s = rtr^{-1}t^{-1}$
1	$(i_0 i_1 i_2 i_3 i_4 \dots)(\dots)\dots$	$(i_1 i_2 i_3)$	$(i_0 i_2 i_3)$
2	$(i_0 i_1 i_2)(i_3 i_4 \dots)(\dots)\dots$	$(i_1 i_2 i_4)$	$(i_0 i_3 i_1; i_2 i_4)$
3	$(i_0 i_1 i_2)$	$(i_1 i_2 i_3)$	$(i_0 i_3)(i_1 i_2)$
4	$(i_0 i_1)(i_2 i_3)(\dots)\dots$	$(i_1 i_2 i_3)$	$(i_0 i_2)(i_1 i_3)$

За всеки отделен случай подбираме подходящ цикъл  $r$  от  $A_n$  и изчисляваме произведението  $s = rtr^{-1}t^{-1}$ . Понеже  $N$  е нормален делител на  $A_n$  а  $t \in N$  то и  $s \in N$ . Така показахме, че ако в  $N$  съществува разместване от вида 1 или 2 то съществува и разместване от вида 3. А тези от видовете 3 и 4 се свеждат до произведение от две независими транспозиции. Да означим това разместване с  $(j_1 j_2) (j_3 j_4)$ .

Нека  $(k_1 k_2)(k_3 k_4)$  е произволно четно разместване. Да разгледаме разместването

$$a = \begin{pmatrix} k_1 & k_2 & k_3 & k_4 & \dots \\ j_1 & j_2 & j_3 & j_4 & \dots \end{pmatrix},$$

където на мястото на точките са разположени произволни числа ( разбира се, в горния ред те са различни от  $k_1, k_2, k_3$  и  $k_4$  а в долния от  $j_1, j_2, j_3$  и  $j_4$  ). Лесно е да се види, че:

$$a(j_1 j_2) (j_3 j_4)a^{-1} = (k_1 k_2) (k_3 k_4).$$

Това показва, че ако един нормален делител на  $S_n$  съдържа произведение от две независими транспозиции то той съдържа и произволно такова. Но за нас е необходимо да докажем, че  $a$  с това свойство се намира сред четните размествания. Да разгледаме произведението  $b = a(j_1 j_2)$ . Изпълнени са равенствата:

$$b(j_1 j_2) (j_3 j_4)b^{-1} = a(j_1 j_2)(j_1 j_2) (j_3 j_4)(j_1 j_2)a^{-1} = a(j_1 j_2) (j_3 j_4)a^{-1} = (k_1 k_2) (k_3 k_4)$$

Двете събституции имат различна четност понеже се отличават с транспозиция. Тогава точно една от тях принадлежи на  $A_n$ . По такъв начин доказахме, че  $N$  съдържа произволно произведение от две независими транспозиции. Трябва да покажем, и че  $N$  съдържа и произволно произведение от две транспозиции, не непременно независими. Нека  $(j_1 j_2) (j_1 j_3)$  е такова произведение. Понеже  $n \geq 5$  то съществуват две числа  $l_1$  и  $l_2$  различни от  $j_1, j_2$  и  $j_3$ . Тогава  $(j_1 j_2) (j_1 j_3)$  се представя като произведение от независими транспозиции чрез равенството:

$$(j_1 j_2) (j_1 j_3) = (j_1 j_2)(l_1 l_2) \cdot (l_1 l_2)(j_1 j_3)$$

и следователно и произведението  $(j_1 j_2) (j_1 j_3)$  принадлежи на  $N$ . Така че, нормалният делител  $N$  съдържа всяко разместване, което е произведение на две произволни транспозиции а следователно и произведенията на такива двойни произведения. Т. е. произволно произведение на четен брой транспозиции или всяко четно разместване. Следователно  $N = A_n$ .

Така, че ако  $N \neq e$  то  $N = A_n$ . С други думи групата  $A_n$  няма никакви други нормални делители освен тривиалните, т. е. тя е проста. И така доказахме, че

*при  $n \geq 5$  знакопроменливата група  $A_n$  е проста и, следователно, неразрешима ( защото простите разрешими групи се изчерпват с циклическите групи от прост ред).*

Литература:

Михаил Михайлович Постников - Теория Галоа

Государственное издательство Физико-математической литературы Москва 1963