Симетрична група

Нека M е произволно множество.
Дефинираме множеството от всички биекции $\varphi : M \to M$:

$$S(M) = \{\varphi : M \to M | \varphi - \text{bijection}\} \tag{1}$$

Въвеждаме операцията композиция $\circ$ и ще проверим дали тя е подходяща операция за да превърне $S(M)$ в група:

Свойство 0: Композиция на две биекции е биекция -
$\varphi, \psi \in S(M) \Rightarrow \varphi \circ \psi \in S(M)$

скрий

Нека $(\varphi \circ \psi)(x) = (\varphi \circ \psi)(y)$. Тогава:

$$\begin{aligned} &\varphi(\psi(x)) = \varphi(\psi(y)) \\ &\psi(x) = \psi(y) \\ &x = y \end{aligned} \tag{2}$$

Използвахме последователно, че φ е биекция и ψ е биекция.

Свойство 1: Композицията е асоциативна -
$\varphi, \psi, \tau \in S(M) \Rightarrow \varphi \circ (\psi \circ \tau) = (\varphi \circ \psi) \circ \tau$

скрий

$$(\varphi \circ \psi) \circ \tau)(x) = (\varphi \circ \psi)\tau(x) = \varphi(\psi(\tau(x)) = \varphi((\psi \circ \tau)(x)) = (\varphi \circ (\psi \circ \tau))(x) \tag{3}$$

Свойство 2: Съществува единичен елемент -
$\exists id : M \to M : id \circ \varphi = \varphi \circ id = \varphi \quad \forall \varphi \in S(M)$

скрий

Ами единичния елемент ще е функцията идентитет:

$$id(x) = x \tag{4}$$

така лесно се проверява, че
$(id \circ \varphi)(x) = id(\varphi(x)) = \varphi(x) = \varphi(id(x)) = (\varphi \circ id)(x)$.

Свойство 3: За всеки елемент съществува противоположен:
$\forall \varphi \in S(M) \Rightarrow \exists \varphi^{-1} : \varphi \circ \varphi^{-1} = \varphi^{-1} \circ \varphi = id$

скрий

За обратен елемент на φ ще използваме просто обратната функция на φ (т.е φ^{-1}). Обърнете внимание, че в условието φ^{-1} трябва да се разбира като обратен елемент на елемента φ (т.е φ разгледано просто като елемент на $S(M)$), докато сега използваме φ^{-1} за да означим обратната функция на биекцията φ (т.е разглеждаме φ като биекция). Както виждате, в случая и двете (еднакви) означения (с различен смисъл) означават един и същ елемент.

Дефиниция: Ще наричаме множеството $S(M)$ с операция $\circ$ ***симетрична група*** за M.

Твърдение:

Групата $\langle S(M), \circ \rangle$ не е комутативна, при $|M| \geq 3$.

скрий

Нека $|M| \geq 3$ и нека a, b, c са три произволни различни елемента от M. Построяваме си (на горния ред стоят аргументите, на долния - съответните им функционални стойности):

$$\varphi_1 = \begin{pmatrix} a & b & c \\ \downarrow & \downarrow & \downarrow \\ a & c & b \end{pmatrix} \quad \varphi_2 = \begin{pmatrix} a & b & c \\ \downarrow & \downarrow & \downarrow \\ b & c & a \end{pmatrix} \tag{5}$$

Сега да образуваме $\varphi_1 \circ \varphi_2$ и $\varphi_2 \circ \varphi_1$:

$$\varphi_1 \circ \varphi_2 = \begin{pmatrix} a & b & c \\ \downarrow & \downarrow & \downarrow \\ c & b & a \end{pmatrix} \quad \varphi_2 \circ \varphi_1 = \begin{pmatrix} a & b & c \\ \downarrow & \downarrow & \downarrow \\ b & a & c \end{pmatrix} \tag{6}$$

е очевидно $\varphi_1 \circ \varphi_2 \neq \varphi_2 \circ \varphi_1$ следователно групата **не е** комутативна.

Дефиниция: Нека $|M| = n$, тогава S_n наричаме ***симетрична група от степен*** n.
Забележка: Горната дефиниция важи само за крайни множества M.

Означение

За удобство при $|M| = n$ ще си обозначим елементите на M с естествени числа :

$$M = \{1, 2, \cdots, n\} \tag{7}$$

и ще записваме биекциите по следния начин (без стрелки)

$$\varphi = \begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix} \tag{8}$$

което всъщност ще означава, че $\varphi(k) = i_k$.

Брой елементи

Очевидно една биекция се определя еднозначно от подредбата на елементите $i_1, i_2, \cdots, i_n$. Тогава броя на всички възможни пермутации $|S(M)| = |S_n| = n!$.

Обратен елемент

Обратна биекция на дадена се намира, като първо се напишат стълбовете на матрицата наопаки (т.е долния ред - отгоре) и после се сортират по горния ред (т.е

той да стане $1, 2, \cdots n$). Ето така:

$$\varphi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 1 & 3 & 5 \end{pmatrix} \Rightarrow \varphi^{-1} = \begin{pmatrix} 2 & 4 & 1 & 3 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 4 & 2 & 5 \end{pmatrix} \quad (9)$$

Представяне с цикли

Сега ще разгледаме един по-подходящ начин да записваме пермутациите.

Дефиниция: Нека $\{i_1, i_2, \cdots, i_k\} \subseteq \{1, 2, \cdots, n\}$, и $i_1, i_2, \cdots, i_n$ са различни помежду си. Нека

$$\begin{aligned} \varphi(i_1) &= i_2 \\ \varphi(i_2) &= i_3 \\ \vdots &\quad \vdots \\ \varphi(i_{k-1}) &= i_k \\ \varphi(i_k) &= i_1 \end{aligned} \quad (10)$$

и освен това останалите елементи са неподвижни, т.е
$\varphi(j) = j \quad \forall j \notin \{i_1, i_2, \cdots, i_k\}$.
Тогава φ ще наричаме ***цикъл с дължина*** k и ще записваме $\varphi = (i_1\ i_2\ \cdots\ i_k)$.

Т.е ако пермутацията изпълнява горните условия - наричаме я цикъл и я записваме като изредим елементите от цикъла подред. Ако пермутацията **не** изпълнява горните условия - значи не е цикъл (и не я записваме никак по-кратко). След малко ще представяме не-циклите като произведение на няколко цикъла.

Дефиниция: Нека $\varphi = (i_1\ \cdots\ i_k)$ и $\psi = (j_1\ \cdots\ j_s)$. Ще казваме, че φ, ψ са ***независими***, ако $\{i_1, \cdots, i_k\} \cap \{j_1, \cdots, j_s\} = \varnothing$, т.е нямат общ елемент помежду си.

Твърдение: Ако φ, ψ са независими, то $\varphi \circ \psi = \psi \circ \varphi$, т.е независимите цикли комутират.

скрий

Тъй като един цикъл действа само върху елементите вътре в него, и останалите остават на място, то ако композираме 2 цикъла без общи елементи няма никакво значение кой сме приложили първо (защото единия цикъл действа на едни елементи, другия на други).

скрий

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = (1\ 2) \circ (3\ 4) \tag{11}$$
$$= (3\ 4) \circ (1\ 2)$$
$$= (4\ 3) \circ (2\ 1)$$
$$\vdots$$

Разбира се, всички горни представяния са еквивалентни - няма значение кой цикъл записваме на първо място, нито как са подредени елементите в самия цикъл (обърнете внимание, че всеки цикъл с дължина k има точно k различни представяния в зависимост от избора на начален елемент).

Представяне чрез произведение на независими цикли

Теорема:

Нека $\varphi \in S_n$ и $\varphi \neq id$. Тогава φ може да се представи като произведение на независими цикли и това представяне е единствено с точност до наредбата на циклите.

скрий

Нека $\varphi \in S_n \& \varphi \neq id$. Ще направим доказателство по индукция по броя на 'разместените' елементи от φ. Нека $t = |\{i | \varphi(i) \neq i\}|$. Със сигурност $t > 1$, защото не може само един елемент да отива в друг (защото няма никой да отиде в него, а това е биекция).

База на индукцията: $t = 2$. Съществуват $a, b \in \{1, \cdots, n\}$ такива, че $\varphi(a) = b \& \varphi(b) = a$[1] и освен това $\varphi(c) = c \quad \forall c \in \{1, \cdots, n\} \setminus \{a, b\}$. Тогава, по дефиниция, $\varphi = (a\ b)$ е цикъл с дължина 2.
Индукционна хипотеза: Нека твърдението е доказано за произволна биекция φ, която размества $t < k$ елемента.
Индукционна стъпка: Нека $\varphi \in S(M)$ и размества k елемента.
Нека i_1 е един от разместените елементи. Тогава:

$$\varphi(i_1) = i_2 \tag{12}$$
$$\varphi(i_2) = i_3$$
$$\vdots$$
$$\varphi(i_{s-1}) = i_s$$
$$\vdots$$

Т.е образувахме си една безкрайна редица $i_1, i_2, \cdots, i_s, \cdots$. Елементите на редицата са от множеството M, което е крайно. Следователно със сигурност

съществуват поне два различни индекса p, q за които $i_p = i_q$. Но понеже φ е биекция, следователно и φ^{-1} е биекция, т.е $i_{p-1} = \varphi^{-1}(i_p) = \varphi^{-1}(i_q) = i_{q-1}$. Това означава, че ако 2 елемента са равни, то и двата предишни също ще са равни; техните предишни също, и т.н. Т.е със сигурност получаваме, че първия елемент, ще е равен с някой следващ.
Нека r е минималния индекс, за който $i_1 = i_r$. Със сигурност $i_1, i_2, \cdots, i_{r-1}$ са различни помежду си (ако допуснем че има 2 равни може да ги 'върнем' назад и ще се окаже, че i_1 е еднакъв с някой преди i_r, което е противоречие).
Нека $\tau = (i_1\ i_2\ \cdots\ i_{r-1})$. Образуваме си $\psi = \tau^{-1} \circ \varphi$.
Лесно се вижда, че $\psi(i_s) = i_s$ защото $\varphi(i_s) = i_{s+1} \& \tau^{-1}(i_{s+1}) = i_s$.
Освен това $\tau^{-1}(\varphi(j)) = \varphi(j) \quad \forall j \notin \{i_1, i_2, \cdots, i_{r-1}\}$, откъдето получаваме, че $\psi(j) = \varphi(j) \quad \forall j \notin \{i_1, i_2, \cdots, i_{r-1}\}$.
Опитвам се да ви убедя, че ψ размества точно $t - (r-1)$ елемента, и от индукционното предположение може да се разбие на произведение на непресичащи се пермутации:
$\tau^{-1} \circ \varphi = \psi = \tau_1 \tau_2 \cdots \tau_l$ следователно $\varphi = \tau \tau_1 \tau_2 \cdots \tau_l$.

Сега ще покажем, че разбиването е еднакво с точност до реда на циклите.
Нека $\varphi = \tau_1 \tau_2 \cdots \tau_p = \sigma_1 \sigma_2 \cdots \sigma_k$.
Нека $\varphi(i_1) \neq i_1$. Тогава със сигурност участва в точно една от τ_x и в точно една от σ_x (защото разбиването е на независими цикли). Пренареждаме така циклите, че i_1 участва в τ_1 и i_1 участва в σ_1. Очевидно:

$$\begin{aligned} \tau_1 &= (i_1\ \varphi(i_1)\ \varphi^2(i_1)\ \cdots\ \varphi^{k-1}(i_1)) \\ \sigma_1 &= (i_1\ \varphi(i_1)\ \varphi^2(i_1)\ \cdots\ \varphi^{k-1}(i_1)) \end{aligned} \tag{13}$$

където k е минималното, за което $\varphi^k(i_1) = i_1$. Както виждате τ_1 и σ_1 са изградени от едни и същи елементи в еднакъв ред, следователно съвпадат - $\tau_1 = \sigma_1$. По индукция по броя на пермутациите в разбиването доказваме, че всички са равни. Следователно разбиването е единствено с точност до наредбата на пермутациите.

Свойства

1. $\tau = (i_1\ \cdots\ i_k)$
$|\tau| = k$ - реда[2] на цикъла е равен на дължината му.
2. τ, σ - независими цикли
$|\tau \circ \sigma| = lcm(|\tau|, |\sigma|)$ - реда на произведението на 2 цикъла е равен на НОК-а от редовете им.
3. $\varphi = \tau_1 \tau_2 \cdots \tau_k$ - разбиване на независими цикли
$|\varphi| = lcm(|\tau_1|, |\tau_2|, \cdots, |\tau_k|)$ - обощение на 2. за произведение на произволен брой цикли.

Спрегнати елементи

Дефиниция: Нека G е група и $a, g \in G$. Ще казваме, че a и gag^{-1} са ***спрегнати*** и

ще записваме $a \sim gag^{-1}$.

Свойства

1. $a \sim a$ - рефлексивност (използваме $g = id$)
2. $a \sim b \Rightarrow b \sim a$ - симетричност (ако $b = gag^{-1}$, тогава $a = g^{-1}bg$)
3. $a \sim b \& b \sim c \Rightarrow a \sim c$ - транзитивност (ако $b = g_1 a g_1^{-1} \& c = g_2 b g_2^{-1} \Rightarrow c = g_2(g_1 a g_1^{-1})g_2^{-1} = (g_2 g_1)a(g_2 g_1)^{-1}$)

Твърдение:

Нека $\sigma = (i_1 \ \cdots \ i_k)$ и $\varphi \in S_n$. Тогава
а) $\tau = \varphi\sigma\varphi^{-1} = (\varphi(i_1)\ \varphi(i_2)\ \cdots\ \varphi(i_k))$
б) $\sigma = \tau_2 \cdots \tau_p$ - разбиване на независими цикли,
$\sigma = (i_1 \ \cdots \ i_k)\cdots(j_1 \ \cdots \ j_s)$
Тогава $\varphi\sigma\varphi^{-1} = (\varphi(i_1)\cdots\varphi(i_k))\cdots(\varphi(j_1)\cdots\varphi(j_s))$.
в) $\sigma \sim \tau$ т.с.т.к. имат еднакъв цикличен строеж (т.е равен брой цикли от всеки ред)
[3]

скрий

а) Първо да проверим колко е $\tau(\varphi(i_1)) = (\varphi \circ \sigma \circ \varphi^{-1})(\varphi(i_1))$:

$$\begin{aligned}(\varphi \circ \sigma \circ \varphi^{-1})(\varphi(i_1)) &= \varphi \circ \sigma(\varphi^{-1} \circ \varphi(i_1)) \\ &= \varphi \circ \sigma(i_1) \\ &= \varphi(i_2)\end{aligned} \tag{14}$$

Т.е видяхме, че $\tau(\varphi(i_1)) = \varphi(i_2)$. В общия случай получаваме $\tau(\varphi(i_p)) = \varphi(i_{p+1})$ с уговорката, че $i_{k+1} = i_1$.
Сега трябва да се уверим, че останалите елементи остават на местата си:
Нека $j \notin \{\varphi(i_1), \varphi(i_2), \cdots, \varphi(i_k)\}$. Тъй като σ променя само елементите $i_1, i_2, \cdots, i_k$, то със сигурност $\varphi^{-1}(j)$ е неподвижен елемент за σ (иначе получаваме противоречие с избора на j). т.е получихме, че:

$$\begin{aligned}(\varphi \circ \sigma \circ \varphi^{-1})(j) &= \varphi(\sigma(\varphi^{-1}(j))) \\ &= \varphi(\varphi^{-1}(j)) \\ &= j\end{aligned} \tag{15}$$

Така доказахме, че $\tau = \varphi \circ \sigma \circ \varphi^{-1} = (\varphi(i_1)\ \varphi(i_2)\ \cdots\ \varphi(i_k))$.
б) Ще разпишем $\varphi\sigma\varphi^{-1}$ като заместим σ с представянето му на независими цикли и ще получим исканото:

(16)

$$\begin{aligned}\varphi\sigma\varphi^{-1} &= \varphi\tau_1\tau_2\tau_3\cdots\tau_p\varphi^{-1}\\ &= \varphi\tau_1\varphi^{-1}\varphi\tau_2\varphi^{-1}\cdots\varphi\tau_p\varphi^{-1}\\ &= (\varphi(i_1)\,\varphi(i_2)\,\cdots\,\varphi(i_k))\cdots(\varphi(j_1)\,\varphi(j_2)\,\cdots\,\varphi(j_s))\end{aligned}$$

в) Правата посока я доказахме в б) .
Обратна посока: Нека τ, σ имат еднакъв цикличен строеж, т.е представят се на независими цикли по следния начин:

$$\begin{aligned}\sigma &= \mu_1\mu_2\cdots\mu_r\\ \tau &= \gamma_1\gamma_2\cdots\gamma_r\end{aligned} \tag{17}$$

и е изпълнено $|\mu_i| = |\gamma_i|$, за всяко i.
Сега, тъй като елементите участващи в циклите са различни помежду си (защото циклите са независими), то съществува биекция φ, която изпраща $\mathrm{i}^{\text{тия}}$ елемент на μ_j в $\mathrm{i}^{\text{тия}}$ елемент на γ_j. Сега вече очевидно $\tau = \varphi\sigma\varphi^{-1}$, т.е $\tau \sim \sigma$.

Четност на пермутации

При разглеждането на детерминанти по Линейна Алгебра се наложи да разбием пермутациите на 2 групи - четни и нечетни. Сега ще направим това по-формално и ще докажем някои свойства.

Транспозиция

Дефиниция: Цикъл от ред 2 ще наричаме ***транспозиция***.

Свойства:

1. $(x\ y)^2 = id$ - прилагайки последователно една и съща транспозиция получаваме идентитет.
2. $(i\ j)(k\ l) = (k\ l)(i\ j)$ - независимите транспозиции комутират (защото са независими :)).
3. $(i\ j)(i\ k) = (i\ k)(k\ j) = (k\ j)(j\ i)$ - просто разпишете коя да е композиция на транспозиции и ще получите $(j\ i\ k)$.
4. $(i_1\ i_2\ \cdots\ i_k) = (i_1\ i_k)(i_1\ i_{k-1})\cdots(i_1\ i_3)(i_1\ i_2)$ - всеки цикъл може да се представи като произведение на транспозиции (разпишете дясната страна и ще се получи ;)).

Четност

Теорема:
а) $id = \tau_1\tau_2\cdots\tau_k$, където τ_i са транспозиции и k е четно;
б) Ако $\varphi = \tau_1\tau_2\cdots\tau_p = \sigma_1\sigma_2\cdots\sigma_r$, където τ_i, σ_j са транспозиции, тогава $p \equiv r \pmod 2$ (т.е независимо от разбиването на цикли на дадена пермутация φ броя на участващите транспозиции във всяко разбиване има една и съща четност -

или всички са четни, или всички са нечетни);

скрий

а) Ще използваме 3те свойства от по-горе за транспозиции за да опишем алгоритъм за размяна на транспозициите, като в крайна сметка ще стигнем до нула транспозиции, и понеже на всяка стъпка сме намаляли броя им или с 2 или с 0 ще получим, че първоначалния им брой е бил четен.
Нека $id = \tau_1 \tau_2 \tau_3 \cdots \tau_k$. И нека x е произволен елемент, който участва в поне една от транспозициите.
Ще преглеждаме транспозициите по двойки започвайки отзад-напред и в зависимост от вида на двойката ще извършваме различна промяна:

- $(x\ y)(x\ y) \to id$ - т.е две последователни еднакви транспозиции, в които участва x могат да се игнорират напълно (защото комбинирания ефект от двете е идентитет)
- $(a\ b)(x\ y) \to (x\ y)(a\ b)$ - може да разменим транспозициите, ако са независими (като целта е да преместим x напред)
- $(a\ y)(x\ y) \to (x\ a)(a\ y)$ - това е 3то свойство от горе (целта пак както виждате е да се премести x напред)
- $(x\ a)(x\ b) \to (x\ b)(b\ a)$ - пак 3то свойство, но приложено в друг случай.

Всяка двойка транспозиции в която участва x ще попада в някой от горните случай и във всеки от тях или преместваме x напред (т.е правим така, че вече да не участва в задната транспозиция) или ги игнорираме и 2те (в първи случай). Получаваме разбиване на транспозиции, в което или x участва само в първата транспозиция, или не участва въобще. Ако участва само в първата, то резултата от всички транспозиции няма да е идентитет (защото x-а няма да отива в x). Прилагайки горепосочения алгоритъм произволна буква (в частност x) може да бъде премахната от транспозициите. Махаме всички букви и остава … нищо - т.е нула транспозиции. На всяка стъпка сме махали 2 или 0 - т.е общо четен брой. Така получихме, че и първоначално са били четен брой.

б) Ще използваме доказателството на а) . Имаме, че $\varphi \circ \varphi^{-1} = id$. Сега да запишем φ по двата начина:

$$\begin{aligned} \varphi \circ \varphi^{-1} &= (\tau_1 \tau_2 \cdots \tau_p)(\sigma_1 \sigma_2 \cdots \sigma_r)^{-1} \\ &= \tau_1 \tau_2 \cdots \tau_p \sigma_r^{-1} \sigma_{r-1}^{-1} \cdots \sigma_1^{-1} \end{aligned} \tag{18}$$

Т.е получихме $p + r$ на брой транспозиции, които дават id. Но идентитета се представя винаги с четен брой транспозиции. Следователно $2 \mid p + r$. Следователно или и двете са четни, или и двете са нечетни - по друг начин казано $p \equiv r \pmod 2$.

Горната теорема позволява въвеждането на следната дефиниция:
Дефиниция: Нека φ е пермутация.

- Ще казваме, че тя ***е четна***, ако може да бъде представена като произведение

на четен брой транспозиции.
- Ще казваме, че тя ***е нечетна***, ако може да бъде представена като произведение на нечетен брой транспозиции.

Алтернативна група

Дефиниция:

- $A_n = \{\sigma \in S_n | \sigma$ - четна пермутация $\}$;
- $B_n = \{\sigma \in S_n | \sigma$ - нечетна пермутация $\}$;

Ще наричаме A_n ***алтернативна група от степен*** n.

За да докажем, че A_n е група трябва да покажем, че произведение на два елемента от A_n е вътре в A_n и противоположния на всеки елемент също е вътре:

- $\sigma_1, \sigma_2 \in A_n$. Тогава всяка една от тях се представя като произведение на четен брой транспозиции, следователно тяхното произведение също се представя като произведение на четен брой транспозиции. Следователно $\sigma_1\sigma_2 \in A_n$
- $\sigma\sigma^{-1} = id$ - тъй като σ е четна и идентитета също е четен, то следователно и σ^{-1} също е четна (иначе излиза, че идентитета има представяне с нечетен брой транспозиции).

Ще покажем, че съществува биекция между A_n и B_n с което ще покажем, че четните пермутации са точно колкото са нечетните пермутации.
Нека $\varphi : S_n \to S_n$ е такава, че $\varphi(\sigma) = (1\ 2) \circ \sigma$. Т.е добавяме транспозицията $(1\ 2)$ след пермутацията. Очевидно, тази функция праща всички четни пермутации в нечетни и обратно (защото добавянето на една транспозиция променя четността). Това означава, че функцията φ разгледана като функция $\varphi : A_n \to B_n$ или $\varphi : B_n \to A_n$ е сама на себе си обратна - защото $\varphi(\varphi(\sigma)) = \sigma$. Следователно $|A_n| = |B_n| = \frac{|S_n|}{2} = \frac{n!}{2}$.

Footnotes

1. факта, че единия отива в другия и обратно се доказва тривиално. Нека $\varphi(a) = b$ и тогава не може $\varphi(b) = b$ следователно b е другия разместен елемент. И $\varphi(b) = a$, защото всички други отиват в себе си и само a си няма първообраз
2. степента, на която трябва да се вдигне елемента за да се получи единицата на групата (идентитета)
3. това твърдение е просто преформулировка на б обаче е в 2^ге посоки

page revision: 14, last edited: 9 Jul 2011, 16:46 (728 days ago)