PERMUTACIJE — 2.del

Potenciranje permutacij

Za množenje permutacij, kot tudi za potenciranje, je ugodnejši zapis permutacij z disjunktnimi cikli. Pa si najprej oglejmo, kaj se dogaja, če lahko permutacijo zapišemo z enim samim disjunktnim ciklom. Takšnim permutacijam pravimo tudi *ciklične permutacije*. V ta namen definirajmo permutaciji

$$\alpha = (1\,2\,3\,4\,5) \qquad \text{in} \qquad \beta = (1\,2\,3\,4\,5\,6).$$

tako α kot β sta ciklični permutaciji, permutacija α je 5-cikel, medtem ko je permutacija β 6-cikel. Izračunajmo njune potence. Po standardni navadi definiramo $\alpha^0 = \beta^0 = \mathrm{id}$.

$$\begin{aligned}
\alpha^1 &= \alpha = (1\,2\,3\,4\,5)\\
\alpha^2 &= \alpha * \alpha = (1\,2\,3\,4\,5) * (1\,2\,3\,4\,5) = (1\,3\,5\,2\,4)\\
\alpha^3 &= \alpha^2 * \alpha = (1\,3\,5\,2\,4) * (1\,2\,3\,4\,5) = (1\,4\,2\,5\,3)\\
\alpha^4 &= \alpha^3 * \alpha = (1\,4\,2\,5\,3) * (1\,2\,3\,4\,5) = (1\,5\,4\,3\,2) = (5\,4\,3\,2\,1)\\
\alpha^5 &= \alpha^4 * \alpha = (5\,4\,3\,2\,1) * (1\,2\,3\,4\,5) = (1)(2)(3)(4)(5) = \mathrm{id}
\end{aligned}$$

Pa še potence permutacije β:

$$\begin{aligned}
\beta^1 &= \beta = (1\,2\,3\,4\,5\,6)\\
\beta^2 &= \beta * \beta = (1\,2\,3\,4\,5\,6) * (1\,2\,3\,4\,5\,6) = (1\,3\,5)(2\,4\,6)\\
\beta^3 &= \beta^2 * \beta = (1\,3\,5)(2\,4\,6) * (1\,2\,3\,4\,5\,6) = (1\,4)(2\,5)(3\,6)\\
\beta^4 &= \beta^3 * \beta = (1\,4)(2\,5)(3\,6) * (1\,2\,3\,4\,5\,6) = (1\,5\,3)(2\,6\,4)\\
\beta^5 &= \beta^4 * \beta = (1\,5\,3)(2\,6\,4) * (1\,2\,3\,4\,5\,6) = (1\,6\,5\,4\,3\,2) = (6\,5\,4\,3\,2\,1)\\
\beta^6 &= \beta^5 * \beta = (6\,5\,4\,3\,2\,1) * (1\,2\,3\,4\,5\,6) = (1)(2)(3)(4)(5)(6) = \mathrm{id}
\end{aligned}$$

Kakšna je torej razlika med potencami permutacije α in β? Zdi se, da potence permutacije β večkrat razpadejo na produkte disjunktnih ciklov kot potence permutacije α. Zakaj?

Kaj pa potence z višjimi eksponenti? Enostavno. Ker je $\alpha^5 = \mathrm{id}$ velja, da je pri poljubnem $k \in \mathbb{N}$ potenca

$$\alpha^k = \alpha^{k \bmod 5} \tag{1}$$

Še več, ker je $\alpha^4 * \alpha = \mathrm{id}$, je $\alpha^{-1} = \alpha^4$. Zato smemo definirati tudi *negativne* potence permutacije α. Tudi, če je $k \in \mathbb{Z}$ velja za potenco α^k zveza (1).

Tudi za potence permutacije β velja podobna zveza. Pri poljubnem eksponentu $k \in \mathbb{Z}$ velja

$$\beta^k = \beta^{k \bmod 6}.$$

Strnimo opaženo v en sam izrek.

Izrek 1 *Naj bo γ ciklična permutacija, v zapisu z disjunktnimi cikli naj jo lahko zapišemo z enim samim n-ciklom. Permutacija γ^k je sestavljena iz* $\gcd(n,k)$ *disjunktnih ciklov, ki so vsi iste dolžine* $\frac{n}{\gcd(n,k)}$.

Izreka 1 ne bomo dokazali. Dokaz sam po sebi ni zahteven, je pa potrebno natančno operirati s številkami in pazljivo računati v ustreznih kolobarjih ostankov. Raje navedimo posledico:

Posledica 2 *Naj bo γ ciklična permutacija, v zapisu z disjunktnimi cikli naj jo lahko zapišemo z enim samim n-ciklom. Potem je $\gamma^n = \mathrm{id}$ in $\gamma^{-1} = \gamma^{n-1}$. Še več, n je najmanjše strogo pozitivno naravno število, za katerega je $\gamma^n = \mathrm{id}$.*

Posledica 2 trdi naslednje. Če je permutacija γ n-cikel, potem pri potenciranju permutacije γ *na njeno dolžino* n dobimo identiteto. Pri potencijanju γ *na ena manj kot njeno dolžino, to je* $n-1$, pa dobimo inverz permutacije γ, permutacijo γ^{-1}. To je res posledica Izreka 1 saj moramo poiskati takšno število k, da bo potenca permutacije γ razpadla na ustrezno število ciklov, ki bodo vsi dolžine 1. To pa se zgodi natančno pri eksponentu n, če je n tudi dolžina cikla ciklične permutacije γ.

Ravno tako lahko upravičimo dozdevno različno obnašanje potenc permutacij α in β. Permutacija α je po strukturi 5-cikel, in 5 je praštevilo. Zato je pri poljubnem eksponentu k izraz $\gcd(n,k)$ bodisi enak 5 bodisi 1. In vsaka potenca permutacije α razpade na same cikle dolžine 1 (ko $5|k$) ali pa "razpade" na en sam cikel dolžine 5, ko je eksponent k tuj številu 5.

Kako pa izračunamo potence permutacij, ki niso ciklične? Pomudimo se pri znani permutaciji $\pi = (1\,2\,3\,4)(5\,7)(6)$. Računajmo.

$$\begin{aligned}\pi^2 = \pi * \pi =&(1\,2\,3\,4)(5\,7)(6) * (1\,2\,3\,4)(5\,7)(6)\\ =&(1\,2\,3\,4) * (1\,2\,3\,4) * (5\,7) * (5\,7) * (6) * (6)\end{aligned}$$

Pri tem smo upoštevali, da se števila $1, 2, 3$ in 4 lahko spremenijo samo pri prehodu preko cikla $(1\,2\,3\,4)$, medtem ko jih drugi cikli ne motijo. Ravno tako na številki 5 in 7 vplivata samo cikla oblike $(5\,7)$. Zato smemo zamenjati vrstni red disjunktnih ciklov, oziroma:

Trditev 3 *Naj bosta permutaciji γ_1 in γ_2 ciklični, njuna cikla pa naj bosta (po številkah)* disjunktna. *γ_1 in γ_2 komutirata, oziroma*

$$\gamma_1 * \gamma_2 = \gamma_2 * \gamma_1.$$

S pomočjo Trditve 3 lahko izračunamo vse potence permutacije π. Velja namreč

$$\begin{aligned}\pi^k =&((1\,2\,3\,4)(5\,7)(6))^k\\ =&(1\,2\,3\,4)^k * (5\,7)^k * (6)^k.\end{aligned}$$

Oziroma, pri konkretnem eksponentu,

$$\begin{aligned}\pi^{2006} =&(1\,2\,3\,4)^{2006} * (5\,7)^{2006} * (6)^{2006}\\ =&(1\,2\,3\,4)^{2006 \bmod 4} * (5\,7)^{2006 \bmod 2} * (6)^{2006 \bmod 1}\\ =&(1\,2\,3\,4)^2 * (5\,7)^0 * (6)^0\\ =&(1\,3)(2\,4) * \mathrm{id} * \mathrm{id} = (1\,3)(2\,4).\end{aligned}$$

Potenciranje permutacij strnemo v naslednji izrek:

Izrek 4 *Naj bo permutacija $\sigma = \alpha_1 * \alpha_2 * \cdots * \alpha_\ell$, kjer so $\alpha_1, \ldots, \alpha_\ell$ disjunktni cikli permutacije σ. Potem je pri poljubnem $k \in \mathbb{Z}$*

$$\sigma^k = \alpha_1^k * \alpha_2^k * \cdots * \alpha_\ell^k.$$

Še po domače. Permutacijo potenciramo tako, da jo zapišemo kot produkt disjunktnih ciklov, potem pa potenciramo vsak cikel posebej. Na koncu upoštevamo še dolžine posameznih ciklov.

Pri potenciranju cikličnih permutacij α in β smo opazili, da lahko inverzni permutaciji α^{-1} in β^{-1} pridelamo tudi tako, da cikla zapišemo v obratnem vrstnem redu. Analogen premislek velja tudi za permutacije, ki niso ciklične. In celo v primeru, ko permutacijo zapišemo s cikli, ki *niso disjunktni*. Cikle zapišemo v obratnem vrstnem redu in obratnih vrstnih redih. Kaj to pomeni si oglej na spodnjem zgledu.

$$\begin{aligned} \text{Naj bo } \sigma &= (1\,2\,3\,4) * (5\,7\,3\,4) * (8\,1\,7) * (3\,2\,1\,6), \\ \text{potem je } \sigma^{-1} &= (6\,1\,2\,3) * (7\,1\,8) * (4\,3\,7\,5) * (4\,3\,2\,1). \end{aligned}$$

Zapis permutacij kot produkt transpozicij

Izrek 5 *Vsako permutacijo $\pi \in S_n$ ($n \geq 2$) lahko zapišemo kot produkt transpozicij (2-ciklov).*

Jasno je, da te transpozicije, cikli dolžine 2, ne bodo nujno disjunktne. Vsaka permutacija ima namreč natančno določeno ciklično strukturo. In če v tej ciklični strukturi nastopa 3-cikel, se mu v nobenem zapisu permutacije z disjunktnimi cikli ne bomo mogli izogniti.

Pa začnimo z identiteto.

$$\mathrm{id} = (1\,2) * (1\,2) = (1\,2) * (1\,2) * (1\,2) * (1\,2)$$

Že identiteto smo uspeli zapisati na dva različna načina kot produkt transpozicij. Torej ne moremo pričakovati, da bo zapis permutacije kot produkt transpozicij enolično določen.

Nadaljujmo z 2-ciklom. No, 2-cikel je transpozicija, torej ga ni treba dodatno prepisovati kot produkt le-teh.

Kaj pa daljši cikli? Preveri sam, da je

$$(1\,2\,3\;4\,5\,6\,7\,8\,9) = (1\,2)(1\,3)(1\,4)(1\,5)(1\,6)(1\,7)(1\,8)(1\,9) \tag{2}$$

Na podoben način lahko vsak cikel zapišemo kot produkt transpozicij. Na tem mestu poudarimo, to nam bo prav prišlo kasneje, da smo cikel *lihe* dolžine zapisali kot produkt *sodo* mnogo transpozicij. In podobno, cikel *sode* dolžine bi mogli zapisati kot produkt *liho* mnogo transpozicij.

Vsako permutacijo lahko zapišemo kot produkt disjunktnih ciklov, vsakega od leteh kot produkt transpozicij. Sklep. Vsako permutacijo lahko zapišemo kot produkt transpozicij.

V resnici lahko vsako permutacijo zapišemo kot produkt precej manjšega nabora transpozicij. Dovolj je izbrati množico transpozicij oblike $A_n = \{(1\,2), (1\,3), (1\,4), \ldots,$

$(1\,n)\}$. Pokazali bomo, da lahko vsako permutacijo iz simertične grupe S_n kot produkt transpozicij vsebovanih v A_n.

Še nekaj teminologije. Pravimo, da množica permutacij $G \subseteq S_n$ *generira* S_n, če lahko vsako permutacijo $\pi \in S_n$ zapišemo kot produkt permutacij iz množice G. Izrek 5 lahko prevedemo v izjavo, da množica vseh transpozicij (v katerih nastopajo števila med 1 in n) generira S_n.

Trditev 6 *Množica* $A_n = \{(1\,2), (1\,3), (1\,4), \ldots, (1\,n)\}$ *generira* S_n.

Pokazati je potrebno, da lahko vsako permutacijo π zapišemo kot produkt transpozicij iz množice A_n. Najprej zapišemo π kot produkt disjunktnih ciklov in vsak cikel kot produkt transpozicij. Torej je za dokaz Trditve 6 dovolj premisliti, da lahko vsako transpozicijo zapišemo kot produkt transpozicij iz A_n. Kar pa v resnici ni težko,

$$(a_1\,a_2) = (1\,a_1) * (1\,a_2) * (1\,a_1),$$

in dokaz je zaključen.

Poskusi pokazati še naslednji trditvi.

Trditev 7 *Množica* $B_n = \{(1\,2), (2\,3), (3\,4), \ldots, (n-1\;n)\}$ *generira* S_n.

Trditev 8 *Množica* $C_n = \{(1\,2), (1\,2\,3\,\ldots\,n)\}$ *generira* S_n.