PERMUTACIJE — 1.del

Osnovne definicije, tabelice

Začnimo neformalno. Izberimo neprazno množico A in bijektivni preslikavi f in g iz A v A. Tudi f^{-1} in g^{-1} sta bijektivni preslikavi in kompozitumi bijektivnih preslikav so ravno tako bijektivne preslikave, vse iz A v A. Kar nas privede do prve definicije.

Naj bo A poljubna neprazna množica. *Permutacija na A* je vsaka bijektivna preslikava $f : A \to A$.

Permutacija reda n je permutacija v $\{1, 2, 3, \ldots, n\}$. Množica vseh permutacij reda n je *simetrična grupa reda n* in jo označimo z S_n.

Če malo pokomentiramo. Permutacije na neskončnih množicah postanejo neobvladljive, njihove strukture ne bi znali učinkovito opisati. Poleg tega so ravno končne, diskretne strukture bliže uporabi v računalništvu. Zato se omejimo na permutacije na končnih množicah. Omejitev na množice "majhnih" naravnih števil ni prav nič "omejujoča". Namesto permutacij (bijektivnih preslikav) na {raca, konj, krava, gos} raje opazujemo permutacije na $\{1, 2, 3, 4\}$, oziroma simetrično grupo reda 4, S_4.

Zgled:

$$\begin{array}{rl} \left(\begin{smallmatrix}1&2&3\\2&3&1\end{smallmatrix}\right) & \text{je permutacija reda 3.}\\ \left(\begin{smallmatrix}1&2&3&4\\2&4&3&1\end{smallmatrix}\right) & \text{je permutacija reda 4.}\\ \left(\begin{smallmatrix}1&2&3&4&5\\2&4&3&1&5\end{smallmatrix}\right) & \text{je permutacija reda 5.}\\ \left(\begin{smallmatrix}1&2&3&4&5&6\\2&4&3&1&5&6\end{smallmatrix}\right) & \text{je permutacija reda 6.}\end{array}$$

Kot je razvidno v zgledu, lahko premutacije zapišemo s *tabelico*. V zgornji vrstici tabelice naštejemo po vrsti vse elemente iz množice $\{1, 2, \ldots, n\}$, v spodnji vrstici tabelice pa njihove slike, če si permutacijo predstavljamo kot preslikavo. To pomeni, da katerakoli izmed permutacij v zgledu enico (1) preslika v dvojko (2). Ker so permutacije bijektivne preslikave tudi v drugi vrstici nastopajo vse številke iz $\{1, 2, \ldots, n\}$, vsaka natančno enkrat, toda ne nujno v naravnem vrstnem redu.

Pa še nekaj uspemo prebrati iz zgleda. Vsako permutacijo reda n *smemo* smatrati tudi za permutacijo reda $n + 1$ in tako naprej. Permutaciji reda 4 "dodamo" še petico, ki jo preslikamo v 5, in dobimo permutacijo reda 5. In v naslednjem koraku permutacijo reda 6. Torej na naraven način veljajo vsebovanosti:

$$S_1 \subseteq S_2 \subseteq S_3 \subseteq S_4 \subseteq S_5 \subseteq \ldots \tag{1}$$

Za označevanje permutacij si rezerviramo črke grške abecede $\pi, \psi, \sigma, \ldots$ Dogovorimo se še za naslednja pojma. Naravno število k je *fiksna točka* permutacije π, če je $\pi(k) = k$. *Identiteta* ali *identična permutacija* id je permutacija, ki vsako naravno število k preslika v k. Zaradi (1) identitete id ni potrebno vstaviti v nobeno od opisanih simetričnih grup posebej. Vsebovana je v vsaki izmed njih. Če pa se bomo v pogovoru posebej omejili na, denimo, perumtacije reda 4, potem bomo pisali

$$\mathrm{id} = \left(\begin{smallmatrix}1&2&3&4\\1&2&3&4\end{smallmatrix}\right) \in S_4$$

Produkt permutacij in inverzna permutacija

Izberimo permutaciji, uporabljali ju bomo tudi v naslednjih računih.

$$\begin{aligned} \pi &= \left(\begin{smallmatrix} 1&2&3&4&5&6&7 \\ 2&3&4&1&7&6&5 \end{smallmatrix}\right) \in S_7 \quad \text{in} \\ \psi &= \left(\begin{smallmatrix} 1&2&3&4&5&6&7 \\ 7&5&4&2&3&1&6 \end{smallmatrix}\right) \in S_7 \end{aligned} \tag{2}$$

Produkt permutacij π in ψ, označimo ga z $\pi * \psi$ izračunamo takole. Za vsako od števil iz $\{1, 2, \ldots, 7\}$ je treba izračunati, kaj leži pod njim v spodnji vrstici tabelice od $\pi * \psi$. Ker je $\pi(1) = 2$ in $\psi(2) = 5$, je $(\pi * \psi)(1) = 5$. Nadaljujemo analogno: ker je $\pi(2) = 3$ in $\psi(3) = 4$, je $(\pi * \psi)(2) = 4$. Torej smemo zapisati:

$$\pi * \psi = \left(\begin{smallmatrix} 1&2&3&4&5&6&7 \\ 2&3&4&1&7&6&5 \end{smallmatrix}\right) * \left(\begin{smallmatrix} 1&2&3&4&5&6&7 \\ 7&5&4&2&3&1&6 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1&2&3&4&5&6&7 \\ 5&4&2&7&6&1&3 \end{smallmatrix}\right) \tag{3}$$

Izračunajmo še produkt $\psi * \pi$. Ker je $\psi(1) = 7$ in $\pi(7) = 5$, je $(\psi * \pi)(1) = 5$. Do sem je vse lepo in prav. Toda ... Ker je $\psi(2) = 5$ in $\pi(5) = 7$, je $(\psi * \pi)(2) = 7$. Če izračunamo do konca:

$$\psi * \pi = \left(\begin{smallmatrix} 1&2&3&4&5&6&7 \\ 7&5&4&2&3&1&6 \end{smallmatrix}\right) * \left(\begin{smallmatrix} 1&2&3&4&5&6&7 \\ 2&3&4&1&7&6&5 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1&2&3&4&5&6&7 \\ 5&7&1&3&4&2&6 \end{smallmatrix}\right)$$

Množenje permutacij v splošnem *ni komutativno.* Že v tem primeru smo videli, da $\pi * \psi \neq \psi * \pi$.

Zapišimo še *inverzni permutaciji* k π in ψ, označimo ju z π^{-1} in ψ^{-1}:

$$\pi^{-1} = \left(\begin{smallmatrix} 1&2&3&4&5&6&7 \\ 4&1&2&3&7&6&5 \end{smallmatrix}\right) \quad \text{in} \quad \psi^{-1} = \left(\begin{smallmatrix} 1&2&3&4&5&6&7 \\ 6&4&5&3&2&7&1 \end{smallmatrix}\right).$$

Velja:

$$\pi * \pi^{-1} = \left(\begin{smallmatrix} 1&2&3&4&5&6&7 \\ 2&3&4&1&7&6&5 \end{smallmatrix}\right) * \left(\begin{smallmatrix} 1&2&3&4&5&6&7 \\ 4&1&2&3&7&6&5 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1&2&3&4&5&6&7 \\ 1&2&3&4&5&6&7 \end{smallmatrix}\right) = \mathrm{id}$$

S podobnim računom preverimo tudi enakosti $\pi^{-1} * \pi = \psi * \psi^{-1} = \psi^{-1} * \psi = \mathrm{id}$.

Tabelico inverzne permutacije π^{-1} konstruiramo tako, da zamenjamo prvo in drugo vrstico v tabelici permutacije. Povrhu, v prvi vrstici želimo imeti številke urejene po velikosti, stolpce nove tabelice uredimo po naraščajočih številih na vrhu.

Če strnemo lastnosti produkta permutacij v naslednjih nekaj vrstic. Naj bodo π, ψ in σ permutacije iz množice S_n.

- (a) $\pi * \psi \in S_n$ in $\pi^{-1} \in S_n$, produkt permutacij je permutacija, ravno tako inverzna permutacija,
- (b) $(\pi * \psi) * \sigma = \pi * (\psi * \sigma)$, množenje permutacij je asociativno, in
- (c) $\pi * \pi^{-1} = \pi^{-1} * \pi = \mathrm{id}$, produkt permutacije z njenim inverzom je identiteta.

Zapis permutacije z disjunktnimi cikli

Pod drobnogled znova vzemimo premutaciji π in ψ iz S_7, definirani v (2). Kam permutacija π preslika številko 1? v 2. In dvojko? V 3. In trojko? V 4. Pa slednjo? Nazaj v enico. Zdi se, kot da smo se vrnili na začetek in zaključili cikel sestavljen iz številk $1, 2, 3, 4$ v permutaciji π.

Zgodbo lahko nadaljujemo. Kaj se zgodi s petico? Permutacijo π jo preslika v 7. Kaj pa 7? Preslikamo jo v 5. Pa smo zaključili še en cikel, sestavljen iz števil 5 in 7.

Ostane še 6, ki je fiksna točka permutacije π.

Permutacijo π lahko zapišemo *s cikli* na naslednji način:

$$\pi = (1\,2\,3\,4)(5\,7)(6)$$

Ta zapis pa ni enoličen. Nobenega razloga ni, da bi v zapisu π s cikli začeli ravno z enico. Med drugimi zapisi omenimo še

$$\pi = (1\,2\,3\,4)(5\,7)(6) = (3\,4\,1\,2)(7\,5)(6) = (4\,1\,2\,3)(5\,7)(6) = (7\,5)(1\,2\,3\,4)(6). \tag{4}$$

Pravimo, da smo permutacijo π zapisali *z disjunktnimi cikli*, če nobeno izmed števil ne nastopa v dveh ciklih permutacije.

Na prvi pogled ni jasno, kako bi lahko katerokoli od števil nastopalo v dveh ali več ciklih zapisa permutacije s cikli. Gotovo zgoraj opisani postopek vedno poišče zapis permutacije z disjunktnimi cikli. Kasneje bomo videli, da lahko permutacijo pišemo kot produkt ciklov, ki niso nujno disjunktni.

Premisli, da lahko permutacijo π zapišemo z disjunktnimi cikli na 24 različnih načinov.

Zapišimo z disjunktnimi cikli še permutacijo ψ:

$$\psi = (1\,7\,6)(2\,5\,3\,4).$$

Kako pa množimo permutacije, ki so zapisane z disjunktnimi cikli? Menda jih ne bomo pretvorili v tabelice? Računajmo:

$$\pi * \psi = (1\,2\,3\,4)(5\,7)(6) * (1\,7\,6)(2\,5\,3\,4) = (1\,5\,6)(2\,4\,7\,3) \tag{5}$$

Kako smo prišli do tega rezultata? Najlažje postopamo takole. Številko *primemo v roko* in jo nosimo z leve proti desni. Pri prehodu preko posameznega cikla v produktu (5) se nam *število v roki* lahko spremeni.

Začnimo z ena-1. Prestavimo se preko cikla $(1\,2\,3\,4)$, ki enico prestavi v dvojko-2. Leta se ne dotakne nobenega izmed ciklov $(5\,7)$, (6) in $(1\,7\,6)$. Nato cikel $(2\,5\,3\,4)$ premakne v petico-5. Torej se v rezultatu število 1 preslika v 5.

Ker želimo permutacijo zapisati s cikli, nadaljujemo s petico-5. Ta se nespremenjena sprehodi preko cikla $(1\,2\,3\,4)$, medtem ko jo naslednji cikel $(5\,7)$ preslika v sedmico-7. Lete cikel (6) ne pokvari, cikel $(1\,7\,6)$ pa jo prestavi v 6. Zadnji cikel $(2\,5\,3\,4)$ šestice ne spremeni. Torej se v rezultatu število 5 preslika v 6.

Tako nadaljujemo dokler ne zaključimo prvega cikla v produktu. Nato izberemo naslednjo prosto številko, če je še kakšna na voljo, in postopek ponavljamo.

Preverite, da dobimo k (5) enakovreden zapis permutacije $\pi * \psi$ s cikli, če tabelico permutacije $\pi * \psi$ iz računa (3) pretvorimo v zapis z disjunktimi cikli.

Izračunajmo še produkt $\psi * \pi$ z zapisom z disjunktnimi cikli:

$$\psi * \pi = (1\,7\,6)(2\,5\,3\,4) * (1\,2\,3\,4)(5\,7)(6) = (1\,5\,4\,3)(2\,7\,6) \tag{6}$$

Znova smo se prepričali, da množenje permutacij v splošnem ni komutativno.

Ciklu dolžine k v zapisu permutacije z disjunktnimi cikli pravimo tudi *k-cikel*. Pri tem 2-ciklu pravimo tudi *transpozicija*, 1-cikel pa je v resnici *fiksna točka permutacije*.

Permutacijo π smo zapisali kot produkt 4-cikla, 2-cikla in 1-cikla, permutacijo ψ pa kot produkt 4-cikla in 3-cikla.

Število ciklov posameznih dolžin v zapisu permutacije z disjunktnimi cikli pravimo tudi *ciklična struktura* permutacije.

Tako je ciklična struktura permutacije π enaka 4+2+1, medtem ko je ciklična struktura permutacije ψ enaka $4+3$. (In ne 7, kot dobimo, če seštejemo številke v teh izrazih!!!)

Dogovorimo se, da lahko v zapisu permutacije z disjunktnimi cikli cikle dolžine 1 (fiksne točke) opuščamo. Permutacijo π bi lahko pisali tudi kot $\pi = (1\,2\,3\,4)(5\,7)$. Enostavno se je prepričati, da s takim zapisom ne vplivamo na rezultat produktov $\pi * \psi$ oziroma $\psi * \pi$, če ne verjameš, ponovi računa (5) in (6) z zapisom π brez 1-ciklov.

Zahtevnejša snov: zakaj "produkt" in ne "produkt"?

Vsaka permutacija je v osnovi preslikava. Zakaj smo se odločili za relacijski produkt $*$, ki permutacije množi z leve, in ne za funkcijski kompozitum $\circ$, ki bi permutacije "množil-komponiral" z desne?

Utemeljili bomo, da je izbira $*$ namesto $\circ$ ne povzroči nobene škode. Da zgradimo teorijo permutacij na popolnoma enakovreden način, ne glede na izbiro operacije. Ker pa smo vezani na obstoječo literaturo (zbirke nalog iz Diskretnih Struktur) se odločimo za operacijo $*$ in množenje permutacij z leve.

Množico S_n, skupaj z operacijo $*$ oziroma $\circ$ in identiteto id, sestavimo v *algebrsko strukturo* (bolj natančno *grupo*). Na ta način dobimo dve algebrski strukturi $(S_n, *, \mathrm{id})$ in $(S_n, \circ, \mathrm{id})$. Pri tem je S_n *nosilna množica* strukture, $*$ oziroma $\circ$ je operacija v strukturi, medtem ko je id odlikovani element strukture, ima posebno vlogo glede na izbrano operacijo.

Algebrski strukturi $(S_n, *, \mathrm{id})$ in $(S_n, \circ, \mathrm{id})$ sta *izomorfni*, če med njima uspemo najti *izomorfizem*: preslikavo, ki bijektivno preslika nosilno množico prve strukture na nosilno množico druge strukture, pri čemer mora odlikovani element prve strukture preslikati v odlikovani element druge strukture, in operacijo v prvi strukturi nadomestiti z operacijo druge strukture. Bolj natančno.

Preslikava $\Phi : S_n \to S_n$ je *izomorfizem* med $(S_n, *, \mathrm{id})$ in $(S_n, \circ, \mathrm{id})$, če velja

(*i*) Φ je bijektivna preslikava,

(*ii*) $\Phi(\mathrm{id}) = \mathrm{id}$ in

(*iii*) za poljubna elementa $\pi, \psi \in S_n$ velja $\Phi(\pi * \psi) = \Phi(\pi) \circ \Phi(\psi)$.

Točka (*iii*) pomeni da je vseeno, če uporabimo operacijo v prvi strukturi in šele nato preslikamo rezultat v drugo strukturo ali pa vsakega od faktorjev posebej preslikamo v drugo strukturo in uporabimo operacijo iz druge strukture. V obeh primerih dobimo isti rezultat.

Prepričajmo se, da je preslikava $\Phi : S_n \to S_n$ definirana z $\Phi(\pi) = \pi^{-1}$ res izomorfizem med $(S_n, *, \mathrm{id})$ in $(S_n, \circ, \mathrm{id})$. Preverimo, da ustreza (*i*), (*ii*) in (*iii*).

Enostavno je videti, da je Φ injektivna preslikava. Če izberemo katerikoli različni permutaciji π in ψ, sta tudi njuna inverza π^{-1} in ψ^{-1}, ki nista nič drugega kot $\Phi(\pi)$ in $\Phi(\psi)$, tudi različni permutaciji. Po Dirichletovem principu je Φ tudi surjektivna preslikava.

Ker je $\mathrm{id}^{-1} = \mathrm{id}$, preslikava Φ zadošča (*ii*).

Nazadnje preverimo (*iii*). Upoštevati moramo, da velja $\rho * \sigma = \sigma \circ \rho$ pri poljubnih permutacijah σ in ρ. Računajmo:

$$\begin{aligned}\Phi(\pi * \psi) &= (\pi * \psi)^{-1} \\ &= \psi^{-1} * \pi^{-1} \\ &= \pi^{-1} \circ \psi^{-1} \\ &= \Phi(\pi) \circ \Phi(\psi)\end{aligned}$$

Izomorfnih struktur med sabo po obnašanju ne moremo ločiti. Namesto permutacij na množici {raca, konj, krava, gos} smemo, kot smo že omenili, obravnavati permutacije na $\{1, 2, 3, 4\}$, saj sta strukturi izomorfni. Podobno lahko namesto permutacij na $\{1, 2, \ldots, n\}$ opremljenih s funkcijskim kompozitumom $\circ$ obravnavamo permutacije na isti množici $\{1, 2, \ldots, n\}$, pri čemer jih množimo z uporabo relacijskega produkta $*$. Izbira je torej naša in odločimo se za $*$. Še enkrat pa naj poudarimo, da bi celotno zgodbo o permutacijah lahko povedali tudi v $\circ$-jeziku.