Permutacijske grupe*

May 20, 2006

A - končna množica

$S(A)$ - množica vseh permutacij na A

$\circ$ - kompozitum oz. produkt funkcij

Pokazali bomo, da je $(S(A), \circ)$ grupa. To grupo imenujemo **simtrična grupa** množice A.

Trditev 1 *$(S(A), \circ)$ je grupa.*

Dokaz. Pokažemo po vrsti vse lastnosti grupe.

notranjost: $f, g \in S(A)$ potem je $f \circ g : A \to A$. Moramo še pokazati, da je $f \circ g$ permutacija, tj. bijekcija.

Injektivnost funkcije $f \circ g$:

$$\begin{aligned} (f \circ g)(x) &= (f \circ g)(y) \\ f(g(x)) &= f(g(y)) \\ g(x) &= g(y) \qquad \text{(ker je } f \text{ injektivna)} \\ x &= y \qquad \text{(ker je } g \text{ injektivna)} \end{aligned}$$

Surjektivnost funkcije $f \circ g$: Naj bo $y \in A$ poljuben. Ker je f surjektivna, obstaja $z \in A$ tako, da je $y = f(z)$. In ker je g surjektivna, obstaja $x \in A$ tako, da je $g(x) = z$. Torej, obstaja tak x, da je $(f \circ g)(x) = f(g(x)) = y$.

asociativnost: Sledi iz,

$$((f \circ g) \circ h)(x)) = (f \circ g)(h((x)) = f(g(h(x)))$$

in

$$(f \circ (g \circ h))(x)) = f((g \circ h)(x)) = f(g(h(x)))$$

enota: Enota je permutacija $\mathrm{id} : x \mapsto x$.

inverz: Če je $f : A \to A$ bijekcija, potem vemo da obstaja bijektivna funkcija $f^{-1} : A \to A$ tako, da velja:

$$f^{-1}(f(x)) = x \text{ in } f(f^{-1}(x)) = x.$$

To pa je ednakovredno pogoju za obstoj inverza v grupi:

$$f^{-1} \circ f = \mathrm{id} \text{ in } f \circ f^{-1} = \mathrm{id}.$$

□

*Zapiske pripravil R. Škrekovski v okvirju predmeta DS II

Permutacijska grupa je vsaka podgrupa v $S(A)$

$S_n := S(A)$ za $A = \{1, 2, \dots, n\}$, velja $|S_n| = n!$

$S_3 = \{id, (123), (132), (1)(23), (2)(13), (12)(3)\}$

$A_3 = \{id, (123), (132)\}$ je podgrupa v S_3

Opomba 1 *S_n ni abelova (tj. komutativna) za $n \geq 3$. Velja:*

$$(12)(23) = (123) \neq (132) = (23)(12).$$

S_3 je najmanjša nekomutativna grupa.

Izrek 2 (Cayley) *Vsaka grupa je izomorfna neki permutacijski grupi.*

Dokaz. Naj bo $(G, *)$ grupa. Za vsak element $a \in G$ definiramo $f_a : G \to G$ z predpisom

$$f_a(x) = a * x.$$

Opazi, da je f_a permutacija iz $S(G)$

Naj bo $h : G \to S(G)$ tako, da je $h(a) = f_a$

Trdimo, da je h homomorfizem:

$$h(ab)(x) = (a * b) * x = a * (b * x) = f_a(f_b(x)) = (h(a) \circ h(b))(x)$$

Trdimo, da je h injectivna preslikava:

$$h(a) = h(b) \Rightarrow f_a = f_b \Rightarrow \forall x \in G : a * x = b * x \Rightarrow a = b$$

Torej, sledi da je grupa G izomorfna svoji sliki $h(G)$ v $S(G)$. Ker pa je $h(G)$ podgrupa iz $S(G)$ je dokaz kočan. $\square$

Alternajoča grupa A_n je definirana takole

$$A_n = \{f \in S_n \mid f \text{ soda permutacija}\}$$

V naslednjem izreku pa pokažemo, da je A_n grupa.

Izrek 3 *(1) A_n je podgrupa v S_n*

(2) Indeks grupe S_n po podgrupi A_n je 2, t.j. $[S_n : A_n] = 2$

(3) $|A_n| = n!/2$

Dokaz. (1) Če π, σ sodi, potem $\pi \circ \sigma$ soda permutacija. Torej je A_n grupa.

Definirajmo $F : A_n \to S_n \setminus A_n$ takole

$$F(f) = (12) \circ f.$$

Očitno, F je bijekcija. Zato $|A_n| = |S_n \setminus A_n|$ ter $|S_n| = |A_n| + |S_n \setminus A_n| = 2|A_n|$.
Od tod sledita (2) in (3). $\square$

Opomba 2 *Ni težko pokazati, da velja:*

(*) *Če je H podgrupa v neki grupi G ter $[G:H]=2$, potem je H edinka v G.*

Torej iz prejšnega izreka sledi, da je alternajoča grupa A_n podgrupa edinka v simtetrični grupi S_n.

Spomnimo se iz DS I, da velja:

Trditev 4 *(1) Vsaka permutacija se da (enolično) razcepiti na produkt disjunktnih ciklov.*

(2) Vsaka permutacija je bodisi soda ali liha (odvisno od števila transpozicij)

Zgled: (123)(45) je liha permutacija, (125)(34)(6789) je soda permutacija, id je zmeraj soda permutacija, π je soda natanko takrat kadar je π^{-1} soda.

Naj ima permutacija $\pi \in S_n$ v zapisu k_i ciklov dolžine i, za $i = 1, \ldots, n$.

Potem pravimo, da ima π **ciklično strukturo**

$$(k_1, k_2, \ldots, k_n).$$

Velja

$$1 \cdot k_1 + 2 \cdot k_2 + 3 \cdot k_3 + \cdots + n \cdot k_n = n.$$

Zgled: permutacija (123)(45)(56)(7)(89) ima ciklično strukturo $(1,3,2,0,0,0,0,0,0)$.

Definiramo relacijo **konjugiranost** $\approx$ na $S(A)$ takole:

$$\pi_1 \approx \pi_2 \qquad \text{če} \qquad \exists \tau \in G : \pi_2 = \tau \circ \pi_1 \circ \tau^{-1}$$

Izrek 5 *Permutaciji π in σ sta konjugirani natanko takrat, ko imata enako ciklično strukturo.*

Dokaz. $(\Rightarrow)$. Če je $C = (i_1\, i_2\, \cdots\, i_k)$ cikel, potem je

$$\tau \circ C \circ \tau^{-1} = (\tau(i_1)\, \tau(i_2)\, \cdots\, \tau(i_k)).$$

Pri produktu disjunktnih ciklov pa tako učinkuje posebej na vsakem ciklu. Naj bo

$$\pi = (a_1\, a_2\, \cdots\, a_k) \circ (b_1\, b_2\, \cdots\, b_l) \circ \cdots \circ (c_1\, c_2\, \cdots\, c_m).$$

Potem je

$$\begin{aligned}
\tau \circ \pi \circ \tau^{-1} &= \tau \circ (a_1\, a_2\, \cdots\, a_k) \circ (b_1\, b_2\, \cdots\, b_l) \circ \cdots (c_1\, c_2\, \cdots\, c_m) \circ \tau^{-1} \\
&= \tau \circ (a_1\, a_2\, \cdots\, a_k) \circ [\tau^{-1} \circ \tau] \circ (b_1\, b_2\, \cdots\, b_l) \circ [\tau^{-1} \circ \tau] \circ \cdots (c_1\, c_2\, \cdots\, c_m) \circ \tau^{-1} \\
&= [\tau \circ (a_1\, a_2\, \cdots\, a_k) \circ \tau^{-1}] \circ [\tau \circ (b_1\, b_2\, \cdots\, b_l) \circ \tau^{-1}] \circ \cdots [\tau \circ (c_1\, c_2\, \cdots\, c_m) \circ \tau^{-1}] \\
&= \big(\tau(a_1)\, \tau(a_2)\, \cdots\, \tau(a_k)\big) \circ \big(\tau(b_1)\, \tau(b_2)\, \cdots\, \tau(b_l)\big) \circ \cdots \big(\tau(c_1)\, \tau(c_2)\, \cdots\, \tau(c_m)\big)
\end{aligned}$$

($\Leftarrow$) Recimo:

$$\pi = (a_1\, a_2\, \cdots\, a_k) \circ (b_1\, b_2\, \cdots\, b_l) \circ \cdots \circ (c_1\, c_2\, \cdots\, c_m)$$

in

$$\sigma = (a'_1\, a'_2\, \cdots\, a'_k) \circ (b'_1\, b'_2\, \cdots\, b'_l) \circ \cdots \circ (c'_1\, c'_2\, \cdots\, c'_m).$$

Definiramo funkcijo $\tau : x \mapsto x'$. Očitno, da je τ permutacija iz $S(A)$. Velja pa $\tau \circ \pi \circ \tau^{-1} = \sigma$. To pa vidimo takole:

$$\tau \circ \pi \circ \tau^{-1}(x'_i) = \tau \circ \pi(x_i) = \tau(x_{i+1}) = x'_{i+1} = \sigma(x'_i)$$

$\square$

Naslednja trditev je hitra posledica prejšnega izreka.

Posledica 6 *Konjugiranost $\approx$ je ekvivalenčna relacija.*

Naj bo H podgrupa v S_n, ter $a \in S_n$. Definirajmo:

$$a \circ H \circ a^{-1} = \{a \circ h \circ a^{-1} \mid h \in H\}$$

Trditev 7 *$a \circ H \circ a^{-1}$ je podgrupa v S_n in $a \circ H \circ a^{-1} \cong H$*

Dokaz. Definiraj preslikavo $h : S_n \to S_n$ takole

$$h(\pi) = a \circ \pi \circ a^{-1}.$$

Potem pa pokaži, da je h automorfizem (izomorfizem iz S_n v S_n). To pa hitro implicira našo trditev.

Rečemo da, je $a \circ H \circ a^{-1}$ **konjugiranka** podgrupi H.

Trditev 8 *Če je H edinka v S_n, potem velja za vsak a: $a \circ H \circ a^{-1} = H$.*

Posledica 9 *Podgrupa H v S_n je edinka natanko takrat kadar za vsak $a \in H$ velja da je vsak konjugirani element a-ja vsebovan v H.*

References

[1] V. Batagelj, *Diskretene strukture - Algebra*, Ljubljana, 1996.

[2] V. Batagelj, S. Klavžar, *Algebra in teorija grafov - Naloge*,2000.

[3] M. Božović, Z. Mijajlović, *Uvod u teorija grupa: teoreme, zadaci, primeri*, 1990.