Matematične strukture

Nik Jazbinšek, Gimnazija Bežigrad, Ljubljana
Jan Martin Jamnik, Gimnazija Koper, Izola

Mentor: Anja Komatar, University of Cambridge, Domžale

Matematična struktura je množica skupaj s povezanimi objekti. Interpretirali smo particijo množice kot matematično strukturo in si ogledali grafe in grupe ter funkcije, ki ohranjajo določeno matematično strukturo. Naši primeri so povezani s simetrično grupo S_n in njeno vizualizacijo.

1 Uvod

Matematična struktura je množica skupaj z matematičnimi objekti, povezanimi z njo. Najprej bomo osvežili naše znanje o množicah in interpretirali particijo množice kot matematično strukturo, potem pa si bomo ogledali grafe in grupe. Zanimalo nas bo tudi, kakšne funkcije med množicam ohranjajo določeno matematično strukturo. Zato bomo preučevali pare

Matematična struktura
(množica, objekti)

Preslikava
ohranja strukturo

Naši primeri bodo povezani s simetrično grupo S_n in naš cilj je opisati njen videz.

2 Množice

Množica je osnovni matematični pojem. Ponavadi si jo predstavljamo kot zbirko objektov, kjer so objekti lahko karkoli, na primer tudi množice so lahko objekti v neki drugi množici. Objektom množice rečemo elementi množice.

Primer. Oglejmo si množico M udeležencev MARSa. Njeni elementi so vsi Marsovci in Marsovke. Zapišemo jo lahko kot

$$M=\{\text{Nino, Aleks, Vesna, Nik, } \ldots, \text{ Neža, Jan Martin}\}$$

Številu elementov množice A rečemo **moč množice** in jo označimo z $|A|$. Na primer $|M| = 39$.

Funkcija f, ki slika množico A v množico B vsakemu elementu a množice A priredi element $b = f(a)$ množice B. Ponavadi pišemo

$$f\colon A \to B, \qquad a \mapsto b = f(a).$$

Funkcija $f\colon A \to B$ je **injektivna**, če za vsaka $a_1, a_2 \in A$ velja: če je $f(a_1) = f(a_2)$, potem je $a_1 = a_2$. Funkcija $f\colon A \to B$ je **surjektivna**, če za vsak $b \in B$ obstaja $a \in A$ tako da je $b = f(a)$. Funkcija $f\colon A \to B$ je **bijektivna**, če je injektivna in surjektivna.

Opazke. (i) Če je B končna in f injektivna, potem je f bijektivna.

(ii) Če je A končna in f surjektivna, potem je f bijektivna.

(iii) Če obstaja bijekcija $f\colon A \to B$, imata množici A in B enako moč.

Opazimo, da smo dobili prvi par, ki ga že dobro poznamo:

$(X, \lvert X\rvert)$
moč množice
$f\colon X \to Y$
f bijekcija

Končne bijekcije

Označimo

$$s_n = \{1, 2, \ldots, n\}.$$

Če je $f\colon s_n \to s_n$ bijekcija, slika 1 v i, enega izmed n elementov s_n. Elemente $\{2, \ldots, n\}$ pa slika v $n-1$ preostalih elementov množice $s_n \setminus \{i\}$, zato je bijekcija na $n-1$ točkah. Torej je

$$|S_n| = n|S_{n-1}| = n!$$

Označimo še

$$\begin{aligned} S_n &= \{f \mid f\colon s_n \to s_n \text{ je bijekcija}\} \\ &= \{(f_1\colon s_n \to s_n), (f_2\colon s_n \to s_n), \ldots, (f_{n!}\colon s_n \to s_n)\} \end{aligned}$$

Particije množice $\iff$ Ekvivalenčne relacije

Particija množice A je razdelitev množice na več disjunktnih podmnožic, katerih unija je množica A.

Soroden pojem lahko definiramo tudi za naravna števila.

Particija pozitivnega števila je zapis tega števila kot vsota padajočih naravnih števil. Particija števila n je torej

$$n = \sum_{i=1}^{k} m_i a_i,$$

kjer so m_i in a_i naravna stevila in je $a_1 > a_2 > \ldots a_k$.

Primer (Particije števila 5)**.**

$$\begin{array}{lllllll} 5 & =4+1 & =3+2 & =3+1+1 & =2+2+1 & =2+1+1+1 & =1+1+1+1+1 \\ 1\cdot 5 & =1\cdot 4+1\cdot 1 & =1\cdot 3+1\cdot 2 & =1\cdot 3+2\cdot 1 & =2\cdot 2+1\cdot 1 & =1\cdot 2+3\cdot 1 & =5\cdot 1 \end{array}$$

Opazka. Naj bo A množica moči n. Potem nam moči disjunktnih podmnožic dajo particijo števila n.

Definicija. Relacija R med elementi množice A je podmnožica množice $A \times A$. Če je $(a_1, a_2) \in R$, rečemo, da je a_1 v relaciji z a_2 in pišemo $a_1 \sim a_2$. Relacija R je **refleksivna**, če je vsak $a \in A$ v relaciji sam s seboj, to je $a \sim a$. Relacija R je **simetrična**, če za vsak par $a_1, a_2 \in A$ velja: če je $a_1 \sim a_2$, je tudi $a_2 \sim a_1$. Relacija R je **tranzitivna**, če za vsake tri $a_1, a_2, a_3 \in A$ velja: če je $a_1 \sim a_2$ in $a_2 \sim a_3$, potem je tudi $a_1 \sim a_3$. Relacija R je **ekvivalenčna**, če je refleksivna, simetrična in tranzitivna.

Lema. *Ekvivalenčna relacija R razdeli množico A na disjunktne podmnožice*

$$[a] = \{b \in a \mid b \sim a\}$$

Podmnožici $[a]$ rečemo ***ekvivalenčni razred elementa*** *a.*

Dokaz. Zaradi refleksivnosti $x \in [x]$ za vsak $x \in A$, torej moramo samo dokazati, da za vsaka x in y velja ali $[x] = [y]$ ali $[x] \cap [y] = \emptyset$. Recimo, da $z \in [x] \cap [y]$. Potem $x \sim z$ in $y \sim z$, oz. $x \sim z$ in $z \sim y$ (simetričnost) in $x \sim y$ (tranzitivnost). Zato je tudi $y \in [x]$. Potem za vsak $\forall w \in [x]$ velja $w \sim x$ in $x \sim y$, kar zaradi tranzitivnosti da $w \sim y$. Poleg tega za vsak $\forall t \in [y]$ velja $t \sim y$ in $y \sim x$, kar zaradi tranzitivnosti da $t \sim x$. Dobimo

$$[x] \subset [y] \subset [x],$$

kar pomeni, da je $[x] = [y]$, zato smo končali. □

Ogledali si bomo dve zanimivi matematični strukturi, graf in grupo. Videli bomo, da S_n skupaj s kompozicijo funkcij tvori grupo, informacije o grafih bijekcij pa nam bodo povedale veliko o S_n.

3 Graf

Graf (V, E_V)

sestoji iz **množice točk** V in **množice povezav** E_V, kjer je

$$E_V \subset V \times V.$$

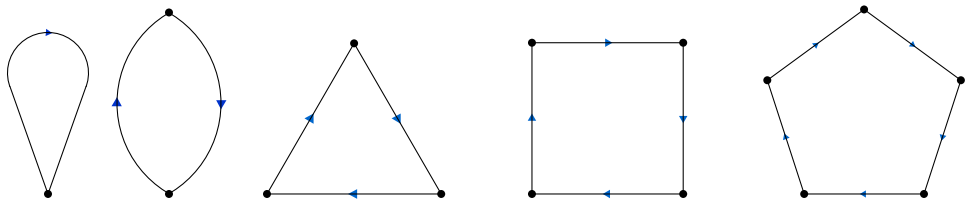
Element $(a, b) \in E_V$ je tako povezava grafa (V, E_V).

Izomorfizem grafov

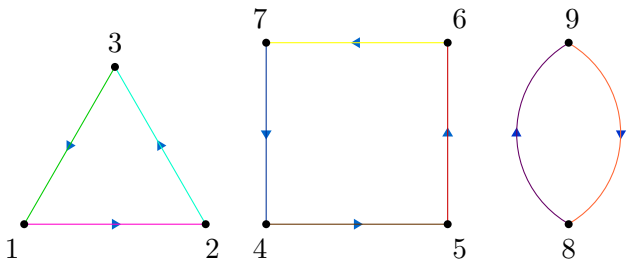
je bijektivna preslikava $\theta\colon V \to W$, ki ohranja povezave, to je

$$(a, b) \in E_V \iff (\theta(a), \theta(b)) \in E_W$$

Primeri. (i) Graf C_n cikla dolžine n. Točke: $\{1, 2, 3, \ldots, n\}$. Povezave: $\{1 \to 2, 2 \to 3, \ldots, (n-1) \to n, n \to 1\}$.



(ii) Graf particije $n = \sum_{i=1}^{k} m_i a_i$ je graf, sestavljen za vsak k iz m_i ciklov dolžine a_i.



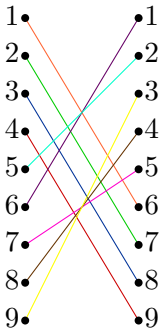
Particija p:

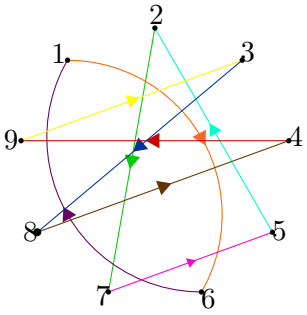
$9 = 3 + 4 + 2$

(iii) Naj bo $f \in S_n$. **Graf** funkcije f je usmerjen graf s točkami $\{1, 2, \ldots, n\}$ in usmerjenimi povezavami $(i, f(i))$ za vse $i \in \{1, 2, \ldots, n\}$.

Funkcija f_p

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





Graf funkcije f_p

Lema. *Graf katerekoli bijekcije $f \in S_n$ je izomorfen enemu izmed grafov particije števila n.*

Dokaz. Oglejmo si $n + 1$ elementov

$$1, f(1), f(f(1)) = f^2(1), \ldots, f^n(1)$$

Ker je $f \in S_n$, imamo samo n možnosti za $f^k(1)$, zato morata biti vsaj dva izmed elementov $1, f(1), \ldots, f^n(1)$ enaka. Naj bo a najmanjši tak, da je

$$f^a(1) = f^b(1)$$

Če bi bil a večji od 1, bi dobili povezavi $(f^{a-1}(1), f^a(1))$ in $(f^{b-1}(1), f^b(1) = f^a(1))$, z $f^{a-1} \neq f^{b-1}$, kar je protislovje, saj je f bijektivna. Zato je $a = 1$ in smo dobili cikel, v katerem leži 1.

Ponovimo postopek za najmanjši i, ki ni v ciklu, v katerem leži 1, in nadaljujemo dokler nam ne zmanjka točk. Dobimo graf, sestavljen iz disjunktnih ciklov, ki je izomorfen enemu izmed grafov particije števila n. □

Primer. Opazimo, da je graf funkcije f_p izomorfen grafu particije p. Ustrezen izomorfizem je

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

4 Grupe

Grupa $(S, \circ)$

je urejen par $(S, \circ)$, kjer je S množica in $\circ$ operacija na množici S, to je funkcija

$$\circ : S \times S \to S, \qquad (a, b) \mapsto a \circ b$$

tako da

- je $\circ$ **asociativna**, to je za vsake tri $a, b, c \in S$

$$(a \circ b) \circ c = a \circ (b \circ c)$$

- obstaja element $e \in S$ (**identiteta**), tako da za vsak $a \in S$ velja

$$a \circ e = a = e \circ a$$

- ima vsak $a \in S$ svoj **inverz**, to je $a^{-1} \in S$, tako da

$$a \circ a^{-1} = e = a^{-1} \circ a$$

Ponavadi operaciji $\circ$ rečemo množenje.

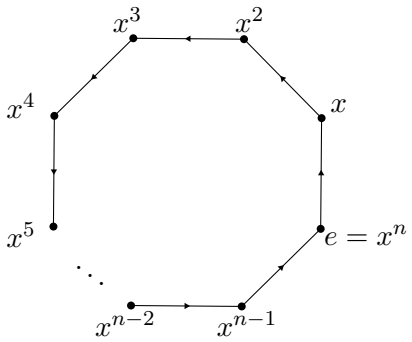
Izomorfizem grup

je bijektivna preslikava $\theta \colon V \to W$, ki ohranja množenje, to je

$$\theta(g_1 \circ g_2) = \theta(g_1) \circ \theta(g_2).$$

Primeri.

(i) Ciklična grupa C_n



(ii) $(S_n, \circ)$, kjer je $\circ$ kompozicija funkcij, imenujemo **simetrična grupa na n točkah**.

Definicija. Naj bo G grupa. Definirajmo relacijo **konjugiranje** na elementih množice G z

$$a, b \in G : a \sim b \iff \exists g \in G : b = gag^{-1}$$

Konjugiranje je ekvivalenčna relacija, zato za vsak element množice G dobimo ekvivalenčni razred

$$[a] = \{b \in G \,|\, b = gag^{-1}; g \in G\}$$

Dokaz, da je konjugiranje ekvivalenčna relacija.

(i) Refleksivnost $a \sim a$, za g uporabimo kar enoto e, kajti $a = eae^{-1}$.

(ii) Simetričnost Če $a \sim b$, potem $b = gag^{-1}$. Pomnožimo z g^{-1} na levi in potem z g na desni in dobimo $a = g^{-1}bg = g^{-1}b(g^{-1})^{-1}$. Zato je tudi $a = gbg^{-1}$

(iii) Tranzitivnost $b = gag^{-1}$ in $c = hbh^{-1}$, od koder sledi $c = hgag^{-1}h^{-1}$. Torej je tudi $c \sim a$, saj iz $hgg^{-1}h^{-1} = e$ sled $(hg)^{-1} = g^{-1}h^{-1}$. Ker pa smo že dokazali, da je relacija simetrična, velja tudi $a \sim c$

□

Izomorfna grafa bijekcij $\iff$ Konjugirani bijekciji

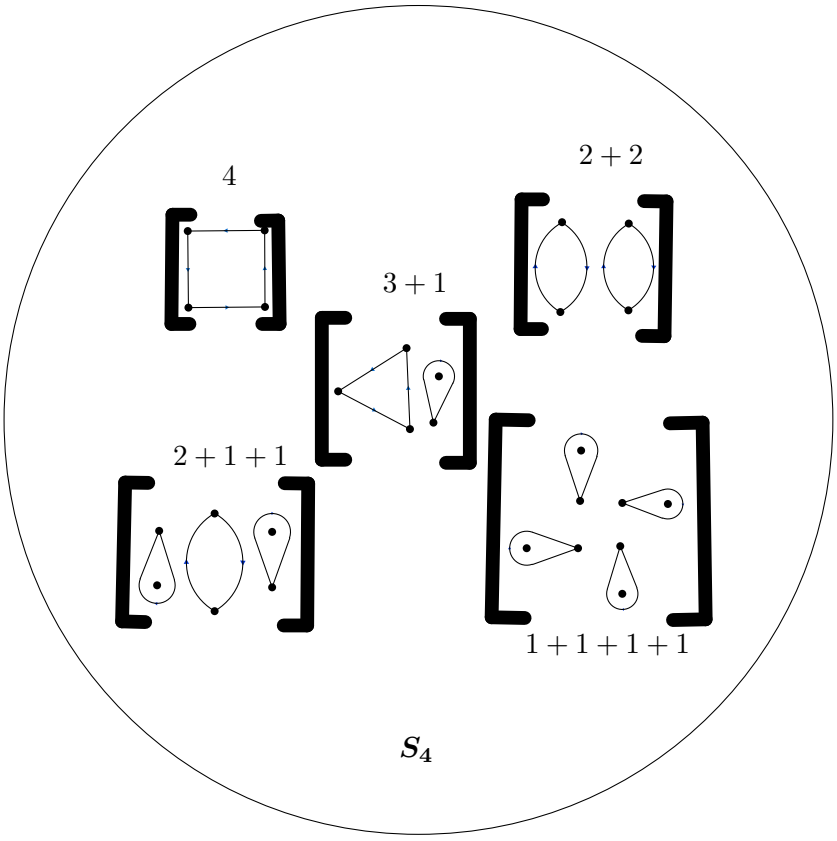
Lema. *Bijekciji imata izomorfna grafa natanko tedaj, ko sta si konjugirani.*

Dokaz. Najprej predpostavimo, da sta si bijekciji f in h konjugirani. Potem obstaja $g \in S_n$, tako da je $h = gfg^{-1}$. Graf bijekcije f ima povezave $(i, f(i))$, graf bijekcije h pa ima povezave $(j, gfg^{-1}(j))$. Zaradi bijektivnosti g slika točke grafa f v točke grafa gfg^{-1}. Da bi bila grafa izomorfna, mora veljati, da se preslikajo tudi ustrezne povezave. Bijekcija g slika točki i in $f(i)$ v točki $g(i)$ in $g(f(i))$, velja pa tudi $g(i) = j$ za nek j. Opazimo

$$gfg^{-1}(j) = gfg^{-1}(g(i)) = g(f(i))$$

Zato je $(g(i), g(f(i)))$ povezava grafa h in je g izomorfizem. Predpostavimo zdaj, da sta grafa f in h izomorfna in naj bo θ ustrezen izomorfizem. Potem θ slika povezavo $(i, f(i))$ v povezavo$(\theta i, \theta f(i))$. Hkrati pa je $\theta i = j$ in $h(j) = h(\theta i) = h\theta(i)$, zato ima graf h povezavo $(\theta i, h\theta(i))$. Ker pa so f, h, θ bijekcije, mora za vsak i veljati $\theta f(i) = h\theta(i)$. Torej je $h = \theta f\theta^{-1}$ in sta si f in h konjugirani. □

Primer. S_4 ima pet konjugacijskih razredov.



Zakaj?

Simetrične grupe so zelo zanimive zaradi naslednjega izreka.

Izrek (Cayley)**.** *Vsaka končna grupa je izomorfna podgrupi S_n za nek n.*

Dokaz. Naj bo G končna grupa, tako da bo moč grupe n. Za vsak $g \in G$ definirajmo

$$\psi_g : G \to G \qquad \psi_g : h \mapsto gh.$$

Dokazujemo, da je ψ_g injektivna:

$$gh_1 = gh_2,$$

od koder sledi $h_1 = h_2$ (Pomnožimo z inverzom od g.)
Zaradi injektivnosti je ψ_g bijekcija G. Ker ima G moč n, je $\psi_g \in S_n$.
Definirajmo še θ:

$$\theta : G \to S_n \qquad g \mapsto \psi_g.$$

Iz definicije θ je θ očitno homomorfizem. Dokažimo še, da je injektivna:

$$a, b \in G \qquad \theta(a) = \theta(b).$$

Iz definicije ψ_g potem sledi, da $ag_i = bg_i$, in z množenjem z inverznim elementom od g_i dobimo $a = b$.
G je torej izomorfna podgrupi S_n.

□

Literatura

[1] M. A. Armstrong, *Groups and Symmetry*, Springer, New York, 1997.