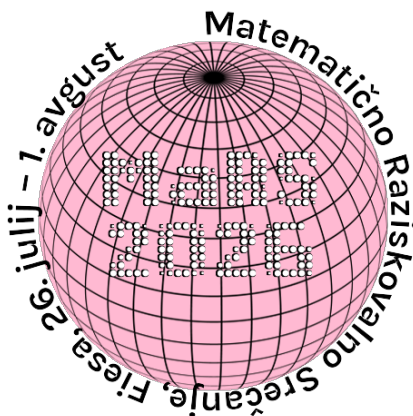


Teorija grup in Rubikova kocka

Martin Flisar, Jaka Horvat, Naja Oblak

Mentor: Jakob Žorž



Povzetek

V članku definiramo pojme in dokažemo osnovne izreke iz teorije grup. S tem znanjem izračunamo število dosegljivih permutacij Rubikove kocke.

1 Uvod

Vsi smo že kdaj preizkusili svojo kapaciteto za prostorsko mišljenje z vrtenjem takozvane Rubikove kocke. Nekaterim nam jo je celo uspelo pospremiti iz kaotične zmešnjave v tisto najčistejše stanje, v katerem se vsaka barva zadržuje na svoji ploskvi. Večina nas je pri tem podvigu sledila enemu izmed splošno predpisanih postopkov, ki jih dandanes kar mrgoli na medmrežju.

Podmnožica teh nas je pomislila tudi na izvor takih receptov – le kako se je nekemu srečnežu uspelo dokopati do takšne modrosti?

Le redki pa so šli še dlje in se potopili v globlje skrivnosti. Katera stanja so dosegljiva in koliko jih sploh je?

Odgovor na ta in mnoga druga vprašanja o tej zloglasni igrači najdemo v teoriji grup.

2 Grupe

Definicija 1. Naj bo G množica in $\cdot$ binarna operacija v G , torej $\cdot : G \times G \rightarrow G$. Vrednost operacije $\cdot(a, b)$ raje krajše zapišemo kot $a \cdot b$ in ji pravimo produkt elementov a in b . Par $(G, \cdot)$ je grupa, če:

- za vse $a, b, c \in G$ velja $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ (asociativnost),
- v G obstaja tak e , da za vsak $a \in G$ velja $e \cdot a = a$ (enota),
- za vsak $a \in G$ obstaja $a^{-1} \in G$, da velja $a^{-1} \cdot a = e$ (inverz).

Trditev 1. Naj bo $(G, \cdot)$ grupa in naj bodo a, b in c elementi grupe G . Iz začetnih pogojev lahko dokažemo naslednje trditve.

1. Enota deluje tudi z desne, torej $a \cdot e = a$.

2. Velja $(a^{-1})^{-1} = a$.
3. Inverz deluje tudi z desne, torej $a \cdot a^{-1} = e$.
4. Enota je enolična.
5. Inverz je enoličen.
6. Če velja $a \cdot b = a \cdot c$, potem je $b = c$.

Dokaz. V prvih treh točkah z a^{-1} označimo poljuben element, za katerega velja $a^{-1} \cdot a = e$; da je tak element enolično določen, pokažemo šele v peti točki.

1. Vemo, da je $a^{-1} \cdot a = e$. Če a zamenjamo z a^{-1} , dobimo

$$(a^{-1})^{-1} \cdot a^{-1} = e.$$

Če to enačbo z desne pomnožimo z a , dobimo

$$(a^{-1})^{-1} \cdot a^{-1} \cdot a = e \cdot a = a.$$

Ker pa je $a^{-1} \cdot a = e$, je leva stran enaka $(a^{-1})^{-1} \cdot e$, torej velja

$$(a^{-1})^{-1} \cdot e = a.$$

Če zadnjo enačbo z desne pomnožimo še z e in upoštevamo $e \cdot e = e$, dobimo

$$(a^{-1})^{-1} \cdot e = (a^{-1})^{-1} \cdot e \cdot e = a \cdot e.$$

Leva stran je po prejšnji enačbi enaka a , torej je $a \cdot e = a$ in enota res deluje tudi z desne.

2. Zdaj vemo, da enota deluje tudi z desne, zato je v enačbi $(a^{-1})^{-1} \cdot e = a \cdot e$ leva stran enaka $(a^{-1})^{-1}$, desna pa a . Dobimo torej še $(a^{-1})^{-1} = a$.
3. Sedaj pa lahko iz že izpeljane enačbe $(a^{-1})^{-1} \cdot a^{-1} = e$ z uporabo $(a^{-1})^{-1} = a$ dobimo še $a \cdot a^{-1} = e$.
4. Predpostavimo, da enota e ni enolična, torej da obstajata enoti e_1 in e_2 , kjer $e_1 \neq e_2$. Potem velja $e_1 = e_1 \cdot e_2 = e_2$, kar pa je protislovje, torej je enota res enolična.
5. Predpostavimo, da obstajata inverza a_1^{-1} in a_2^{-1} , kjer $a_1^{-1} \neq a_2^{-1}$, da je $a \cdot a_1^{-1} = e$ in $a \cdot a_2^{-1} = e$. Potem je tudi $a_1^{-1} \cdot a \cdot a_2^{-1} = a_1^{-1} \cdot e = a_1^{-1}$. Ampak $a_1^{-1} \cdot a \cdot a_2^{-1} = e \cdot a_2^{-1} = a_2^{-1}$, torej je $a_1^{-1} = a_2^{-1}$, kar pa je protislovje. Inverz je torej res enoličen.
6. Enačbo $a \cdot b = a \cdot c$ pomnožimo z leve z a^{-1} in dobimo

$$a^{-1} \cdot a \cdot b = a^{-1} \cdot a \cdot c,$$

$$e \cdot b = e \cdot c,$$

$$b = c.$$

Temu pravilu rečemo krajšanje z leve. Po prvi in tretji lastnosti simetrično deluje tudi krajšanje z desne, saj iz $b \cdot a = c \cdot a$ sledi $b = c$.

□

Definicija 2. Naj bo $(G, \cdot)$ grupa. Grupa $(H, \cdot)$ je podgrupa grupe $(G, \cdot)$, kar označimo s $H \leq G$, če je H podmnožica množice G in je grupa za isto operacijo, omejeno na $H \times H$. Velja $G \leq G$ in $\{e\} \leq G$. Samo grupo G imenujemo neprava podgrupa, $\{e\}$ pa trivialna podgrupa.

Izrek 1. Naj bo H neprazna podmnožica grupe G . Množica H je podgrupa grupe G natanko tedaj, ko je za vsak par elementov $a, b \in H$ tudi $a \cdot b^{-1}$ element H .

Dokaz. Vsako smer ekvivalence dokažemo posebej.

($\Rightarrow$) Predpostavimo, da je H podgrupa. To je očitno, saj so v grupi inverzi vseh elementov in produkti vseh elementov.

($\Leftarrow$) Predpostavimo, da je $a \cdot b^{-1} \in H$ za vsaka $a, b \in H$, in dokažimo, da je H grupa.

Najprej dokažimo $e \in H$. Če v izrazu $a \cdot b^{-1}$ zamenjamo b z a , dobimo $a \cdot a^{-1} = e \in H$.

Želimo še, da če je $a \in H$, je tudi $a^{-1} \in H$. V izrazu $a \cdot b^{-1}$ zamenjamo najprej a z e in nato b z a in dobimo $e \cdot a^{-1} = a^{-1} \in H$.

Sedaj dokažimo še, da iz $a, b \in H$ sledi $a \cdot b \in H$. V izrazu $a \cdot b^{-1}$ pustimo a in zamenjamo b z b^{-1} in dobimo produkt $a \cdot b \in H$.

Dokazali smo torej, da ima H enoto ter vsebuje inverze in produkte, asociativnost pa podeduje od grupe G . Množica H je torej grupa, s čimer smo dokazali tudi izrek. $\square$

Definicija 3. Naj bosta $(G, \cdot_G)$ in $(H, \cdot_H)$ grupi ter $f : G \rightarrow H$ funkcija. Pravimo, da je f homomorfizem, če za vsaka $a, b \in G$ velja

$$f(a \cdot_G b) = f(a) \cdot_H f(b).$$

Trditev 2. Naj bo $f : G \rightarrow H$ homomorfizem, naj bo e_G enota grupe G in e_H enota grupe H . Potem veljata naslednji trditvi.

1. Enota se slika v enoto, torej $f(e_G) = e_H$.

2. Za vsak $a \in G$ velja $f(a^{-1}) = f(a)^{-1}$.

Dokaz.

1. Če v enačbi $f(a \cdot_G b) = f(a) \cdot_H f(b)$ zamenjamo tako a kot b z e_G , dobimo

$$f(e_G \cdot_G e_G) = f(e_G) = f(e_G) \cdot_H f(e_G),$$

iz česar sledi $f(e_G) = e_H$.

2. Velja $e_H = f(e_G) = f(a \cdot_G a^{-1}) = f(a) \cdot_H f(a^{-1})$, iz česar vidimo, da je $f(a^{-1})$ inverz elementa $f(a)$. Prav tako mora seveda biti inverz $f(a)$ tudi $f(a)^{-1}$. Ker pa je inverz enoličen, velja $f(a^{-1}) = f(a)^{-1}$. $\square$

Definicija 4. Naj bo $f : G \rightarrow H$ homomorfizem. Potem definiramo sliko homomorfizma f kot

$$\text{Im } f = \{f(g) \mid g \in G\}$$

in jedro homomorfizma f kot

$$\ker f = \{g \mid f(g) = e\}.$$

Izrek 2. Naj bo $f : G \rightarrow H$ homomorfizem. Potem je slika $\text{Im } f$ podgrupa H .

Dokaz. Naj bosta $a, b \in \text{Im } f$, da je $a = f(a')$ in $b = f(b')$. Potem je $f(a' \cdot b'^{-1}) = f(a') \cdot f(b')^{-1} = a \cdot b^{-1} \in \text{Im } f$, torej je po izreku 1 slika $\text{Im } f$ podgrupa H . $\square$

Izrek 3. Naj bo $f : G \rightarrow H$ homomorfizem. Potem je jedro $\ker f$ podgrupa G .

Dokaz. Naj bosta $a, b \in \ker f$, torej $f(a) = f(b) = e$. Potem je $f(a \cdot b^{-1}) = f(a) \cdot f(b)^{-1} = e \cdot e = e$, torej je $a \cdot b^{-1} \in \ker f$ in je po izreku 1 jedro $\ker f$ podgrupa G . $\square$

Definicija 5. Naj bo $H \leq G$ in $g \in G$. Množico $g \cdot H = \{g \cdot h \mid h \in H\}$ imenujemo levi odsek, množico $G/H = \{g \cdot H \mid g \in G\}$ pa faktorski prostor.

Izrek 4. Naj bo G grupa in H njena podgrupa. Unija vseh podmnožic faktorskega prostora je grupa G , torej

$$\bigcup_{A \in G/H} A = G.$$

Dokaz. Ker so vse podmnožice faktorskega prostora v G , je unija vseh teh množic $\bigcup_{A \in G/H} A$ podmnožica G . Po definiciji faktorskega prostora je unija podmnožic faktorskega prostora unija levih odsekov za vse g v G , torej

$$\bigcup_{A \in G/H} A = \bigcup_{g \in G} g \cdot H.$$

Velja tudi

$$\bigcup_{g \in G} \{g\} \subseteq \bigcup_{g \in G} g \cdot H,$$

saj je $e \in H$ in je potem tudi $g \in g \cdot H$. Ampak $\bigcup_{g \in G} \{g\}$ pa je ravno grupa G . Velja torej

$$G \supseteq \bigcup_{A \in G/H} A = \bigcup_{g \in G} g \cdot H \supseteq \bigcup_{g \in G} \{g\} = G,$$

kar pomeni, da je $\bigcup_{A \in G/H} A = G$. □

Izrek 5 (Lagrangeev izrek). *Naj bo G končna grupa in H njena podgrupa. Potem $|H|$ deli $|G|$.*

Dokaz. Najprej dokažimo, da če $a \cdot H \neq b \cdot H$, je potem $a \cdot H \cap b \cdot H = \emptyset$.

Predpostavimo, da presek ni prazen, in naj bo $p \in a \cdot H \cap b \cdot H$, $g \in a \cdot H$ in $g \notin b \cdot H$. Potem obstaja $h \in H$, da je $g = a \cdot h$. Ker presek ni prazen, naj bo $p = a \cdot h_1$ in $p = b \cdot h_2$. Iz tega sledi $a \cdot h_1 = b \cdot h_2$ in zato $a = b \cdot h_2 \cdot h_1^{-1}$. Sledi, da je $g = b \cdot h_2 \cdot h_1^{-1} \cdot h$. Ker je $h_2 \cdot h_1^{-1} \cdot h$ element H , je $g = b \cdot h_2 \cdot h_1^{-1} \cdot h \in b \cdot H$, kar je protislovje.

To pomeni, da za $a \cdot H \neq b \cdot H$ odseka $a \cdot H$ in $b \cdot H$ nimata skupnih elementov. Sedaj bomo dokazali še $|a \cdot H| = |b \cdot H|$.

Obstaja preslikava $a \cdot H \rightarrow b \cdot H$, ki slika $a \cdot h \mapsto b \cdot h$, in je bijektivna, saj je njen inverz preslikava $b \cdot h \mapsto a \cdot h$, torej enakost res drži. To pomeni, da za končno G velja $|G/H| \cdot |H| = |G|$, torej mora $|H|$ deliti $|G|$. □

Izrek 6. *Naj bo $g \in G$. Z g^n označimo produkt n kopij elementa g , z $\text{ord}_G(g)$ pa najmanjše naravno število n , da velja $g^n = e$, ter naj $\langle g \rangle$ označuje najmanjšo podgrupo $H \leq G$, da je $g \in H$. Potem velja $\langle g \rangle = \{e, g, g^2, \dots, g^{n-1}\}$, kjer je $n = \text{ord}_G(g)$.*

Definicija 6. *Podgrupi $\langle g \rangle$ pravimo ciklična podgrupa.*

Iz tega izreka sledita tudi dve posledici.

Posledica 1. *Če je G končna grupa, obstaja ciklična podgrupa $H \leq G$.*

Posledica 2. *Število $\text{ord}_G(g)$ deli $|G|$, kar velja po Lagrangeevem izreku (izrek 5).*

3 Delovanje grup

Definicija 7. *Permutacija množice S je bijektivna preslikava iz S v S .*

Definicija 8. *Naj bo G grupa in naj bo S množica. Pravimo, da grupa G deluje na množico S , če vsak element $g \in G$ inducira permutacijo na množici S , ki ustreza dvema pogojema.*

- Enota grupe G deluje kot identična permutacija na množici S .
- Za elementa g in h v G je permutacija, ki jo inducira produkt $g \cdot h$, enaka kompoziciji permutacij, ki ju inducirata g in h .

Sliko elementa $x \in S$ v permutaciji, ki jo inducira g , označimo z $g \cdot x$.

3.1 Orbita in stabilizator

Definicija 9. Orbita elementa $x \in S$ pod delovanjem grupe G je podmnožica množice S , ki sestoji iz vseh tistih elementov, ki jih lahko dosežemo z delovanjem elementov grupe G na element x , in jo označimo z $G \cdot x$, natančneje

$$G \cdot x = \{g \cdot x : g \in G\}.$$

Definicija 10. Stabilizator elementa $x \in S$ v grupi G je podmnožica množice G , ki sestoji iz vseh elementov, ki pri delovanju ohranijo x , in ga označimo z G_x , natančneje

$$G_x = \{g \in G : g \cdot x = x\}.$$

Izrek 7. Stabilizator G_x je podgrupa grupe G .

Dokaz. Pokazali bomo, da je za vsak element $h \in G_x$ tudi $h^{-1} \in G_x$. Velja namreč

$$h^{-1} \cdot x = h^{-1} \cdot (h \cdot x) = (h^{-1} \cdot h) \cdot x = x.$$

Posledično je $(g \cdot h^{-1}) \cdot x = g \cdot x = x$, torej je po izreku 1 stabilizator res podgrupa. $\square$

Izrek 8 (Izrek o orbiti in stabilizatorju). Naj bo G končna grupa, ki deluje na množico S , in naj bo $x \in S$. Potem je moč faktorskega prostora G/G_x enaka moči orbite $G \cdot x$.

Dokaz. Skonstruirali bomo bijekcijo med elementi faktorskega prostora in orbito. Natančneje, pokazali bomo, da je preslikava $g \cdot G_x \mapsto g \cdot x$ bijekcija. Izberemo poljubna g_1 in g_2 . Potem je

$$g_1 \cdot G_x = g_2 \cdot G_x \iff g_2^{-1} \cdot g_1 \cdot G_x = G_x \iff g_2^{-1} \cdot g_1 \in G_x \iff g_2^{-1} \cdot g_1 \cdot x = x \iff g_1 \cdot x = g_2 \cdot x.$$

Iz tega sledi, da sta preslikava in njen inverz dobro definirana in da je torej izbrana preslikava res bijekcija. $\square$

4 Permutacije in simetrična grupa

Definicija 11. Simetrična grupa S_n je grupa vseh permutacij množice $[n] = \{1, 2, \dots, n\}$ z operacijo kompozicije.

V prihodnje bomo poljubno permutacijo prvih n naravnih števil označevali z n -terico $a_1, a_2, \dots, a_n$. Pri tem permutacija slika element i v a_i . Permutaciji, ki vsak element slika vase, pravimo *identična permutacija* in jo zapišemo kot $1, 2, \dots, n$.

Definicija 12. Transpozicija je permutacija, ki fiksira (ohrani na svojem mestu) vse razen dveh elementov.

Definicija 13. Inverzija je par indeksov $i < j$, za katera velja $a_i > a_j$.

Definicija 14. Permutaciji pravimo soda oz. liha, če jo lahko dosežemo začnši iz identične permutacije s soddim oz. lihim številom transpozicij.

Izrek 9. Vsaka permutacija je bodisi soda bodisi liha.

Dokaz. Vsako permutacijo lahko očitno dosežemo z zaporedjem transpozicij, natančneje s transpozicijami sosednjih členov. Pri vsaki taki transpoziciji se spremeni sodost števila inverzij permutacije. Če namreč zamenjamo sosednja člena, se število inverzij zveča ali zmanjša za 1. Identična permutacija nima inverzij, zato lahko vsako permutacijo opredelimo za sodo ali liho glede na to, ali je število njenih inverzij sodo ali liho. $\square$

5 Rubikova kocka

Rubikova kocka je mehanska uganka, na kateri lahko uporabimo teorijo grup.

Definicija 15. Grupo Rubikove kocke $(G, \cdot)$ definiramo kot vsa stanja, ki jih lahko dosežemo s premiki ploskev. Rezultat množenja pa definiramo kot stanje, ki ga dosežemo, ko na prvem stanju uporabimo zaporedje potez, ki vodi iz rešenega stanja v drugo stanje.

Definicija 16. Poteze so premiki ploskev za 90° v smeri urinega kazalca, poimenovane po prvi črki ploskve v angleščini **Up**, **Down**, **Left**, **Right**, **Front** in **Back**. Z X' označimo potezo X v nasprotni smeri urinega kazalca, z X^2 pa dve zaporedni potezi X , torej premik ploskve za 180° .

Posamezne koščke označujemo na naslednji način.

- Centri so koščki, ki imajo natanko eno barvo. Označimo jih s črko ploskve, na kateri ležijo, na primer U .
- Robovi so koščki, ki imajo natanko dve različni barvi. Označimo jih z dvema črkama ploskev, na kateri mejita, na primer UF .
- Vogali so koščki, ki imajo natanko tri različne barve. Označimo jih s tremi črkami ploskev, na katere mejijo, na primer UFL .

Rubikova kocka ima 6 fiksnih centrov, 12 robov in 8 vogalov. Po dogovoru je bela ploskev zgoraj in rumena spodaj.

Definicija 17. Naj bo X množica vseh permutacij Rubikove kocke. To so vsa stanja, ki jih lahko konstruiramo, ko razstavimo in ponovno sestavimo kocko.

Permutiramo vseh dvanajst robov, kjer je vsak lahko vstavljen na 2 načina. Podobno lahko naredimo z osmimi vogali, ki so vstavljeni na enega izmed treh načinov.

$$|X| = 12! \cdot 2^{12} \cdot 8! \cdot 3^8 = 519024039293878272000.$$

Vsi stabilizatorji grupe G so trivialni oziroma $|G_x| = 1$, saj je vsako zaporedje potez, ki poljubno stanje premeša vase, enako *enoti* grupe. Zaradi izreka o orbiti in stabilizatorju sledi

$$\begin{aligned} |G| &= |G_x| \cdot |G \cdot x|, \\ |G| &= |G \cdot x|. \end{aligned}$$

Iz tega sledi, da so vse orbite Rubikove kocke enako velike.

Izrek 10. Vsako stanje, ki ga lahko dosežemo s potezami, ustreza sodi permutaciji koščkov.

Dokaz. Če gledamo skupaj permutacije 12 robov in 8 vogalov, dobimo homomorfizem iz grupe G v grupo S_{20} . Vsaka poteza permutira natanko 4 robove in 4 vogale, torej 8 koščkov vse skupaj. Za primer premik zgornje ploskve za 90° v smeri urinega kazalca permutira robove $UB \rightarrow UR \rightarrow UF \rightarrow UL \rightarrow UB$ in vogale $UBR \rightarrow UFR \rightarrow UFL \rightarrow UBL \rightarrow UBR$. Ker so si vse poteze enake po simetriji, naredijo dva cikla velikosti štiri. Posledično vsi grupni elementi slikajo v sode permutacije. To pomeni, da le s potezami na Rubikovi kocki ne moremo priti v liho permutacijo. $\square$

Definicija 18. Rob je rešen, kadar leži na mestu, kamor spada, in se njegovi barvi ujemata z barvama ploskev, na kateri meji. Rob je dober, če ga lahko rešimo le s potezami iz množice $\{F^2, B^2, R, L, U, D\}$, torej brez zasukov ploskev F in B za 90° ; pri tem ni pomembno, kam se med tem premaknejo drugi koščki. Rob, ki ni dober, je slab.

Z naštetimi potezami lahko vsak rob premaknemo na katero koli mesto, zato je edino vprašanje, ali ga lahko na njegovo mesto premaknemo tudi pravilno obrnjenega. V rešenem stanju so torej vsi robovi dobri.

Izrek 11. Pri vsaki potezi se ohrani sodost števila dobrih robov.

Dokaz. Na začetku so vsi robovi dobri, tako da imamo 12 dobrih in 0 slabih robov. Vsaka poteza iz podmnožice $\{F^2, B^2, R, L, U, D\}$ po definiciji ne spremeni dejstva, ali je nek rob dober ali ni. Isto velja za njihove inverze R', L', U' in D' , saj lahko vsako zaporedje teh potez izvedemo tudi v obratni smeri. Po drugi strani potezi F in B obrneta dobre robove v slabe in obratno. Rob, ki smo ga prej lahko premaknili na pravo mesto brez F in B , se zdaj tja ne more več premakniti, in obratno. Poteza F premakne natanko 4 robove, zato spremeni dobrost natanko teh štirih robov. Če je bilo med njimi k dobrih, jih je po potezi $4 - k$, torej se število dobrih robov spremeni za $4 - 2k$, kar je sodo število. Sodost števila dobrih robov se torej ohrani. Enako velja za poteze B, F' in B' , saj spremenijo dobrost istih štirih robov. $\square$

Definicija 19. Vsak vogal ima natanko en beli ali rumeni del. Za vsak vogal definiramo njegovo pravilno orientacijo kot orientacijo, kjer ta del gleda gor ali dol. Rotacija vogala je število zasukov za 120° v smeri urinega kazalca, ki so potrebni, da iz pravilne orientacije pridemo v dano orientacijo, torej število iz množice $\{0, 1, 2\}$.

Izrek 12. Vsota rotacij vogalov v smeri urinega kazalca se ohranja po modulu 3.

Dokaz. Ker je vsaka poteza zasuk ene ploskve za 90° , je dovolj, da trditev preverimo za poteze U, D, F, B, R in L . Vsaka izmed njih premakne natanko štiri vogale, in sicer tiste na svoji ploskvi.

Pri potezah U in D beli ali rumeni del vsakega premaknjenega vogala ostane obrnjen navzgor oziroma navzdol, zato se rotacije sploh ne spremenijo.

Pri potezah F, B, R in L pa pogledamo spremenjene vogale in ugotovimo, da se v vsakem paru sosednjih vogalov eden obrne za 120° v smeri urinega kazalca, drugi pa v nasprotno smer. Rotacije štirih premaknjenih vogalov se torej po vrsti spremenijo za 1, -1 , 1 in -1 , njihova vsota pa ostane enaka.

Pri nobeni potezi se vsota rotacij torej ne spremeni po modulu 3. $\square$

Pokažimo še, da je ta invarianta edina ovira za pravilno orientacijo vogalov.

Trditev 3. Če je vsota rotacij vogalov deljiva s 3, lahko vse vogale z zaporedjem potez spravimo v pravilno orientacijo, ne da bi premaknili kateri koli košček.

Dokaz. Zaporedje potez

$$Z = R' D' R D R' D' R D U D' R' D R D' R' D R U'$$

zasuka vogal na mestu UFR za 120° v nasprotni smeri urinega kazalca in vogal na mestu UBR za 120° v smeri urinega kazalca, vse druge koščke pa pusti na svojih mestih in v isti orientaciji. Zaporedje Z torej spremeni rotacijo prvega vogala za -1 in rotacijo drugega za 1, zaporedje Z^2 pa ravno obratno. Ker je vsota teh dveh sprememb enaka 0, je to v skladu z izrekom 12.

Naj bo A poljubno zaporedje potez. Zaporedje AZA' ima enak učinek kot Z , le da zasuka tista vogala, ki ju A premakne na mesti UFR in UBR . Ker lahko poljubna dva vogala s potezami premaknemo na ti dve mesti, imamo za vsak par vogalov zaporedje potez, ki enega zasuka v smeri urinega kazalca, drugega pa v nasprotno smer, vse ostalo pa pusti nespremenjeno.

Izberimo zdaj en vogal in ga označimo z v . Za vsakega izmed preostalih sedmih vogalov uporabimo tako zaporedje potez za par tega vogala in vogala v , in sicer tolikokrat, da pride obravnavani vogal v pravilno orientacijo. Ko to naredimo za vseh sedem, so vsi v pravilni orientaciji, rotacija vogala v pa se je povečala ravno za vsoto njihovih začetnih rotacij. Rotacija vogala v je zato enaka vsoti vseh začetnih rotacij, ki je po predpostavki deljiva s 3. Ker je rotacija število iz množice $\{0, 1, 2\}$, je torej enaka 0, kar pomeni, da je tudi vogal v v pravilni orientaciji. $\square$

Izrek 13. V množici X je dvanajst orbit.

Dokaz. Po izrekih 10, 11 in 12 se pri potezah ohranijo tri invariante: sodost permutacije koščkov, sodost števila dobrih robov in vsota rotacij vogalov po modulu 3. Stanji, ki se razlikujeta v kateri koli izmed teh invariant, torej nista v isti orbiti, velja pa tudi obratno, da lahko stanje s potezami premešamo v vsako stanje z istimi invariantami; za rotacije vogalov to pokaže trditev 3. Invariante lahko zavzamejo $2 \cdot 2 \cdot 3 = 12$ različnih kombinacij, saj pri sestavljanju kocke lahko zamenjamo zadnja dva robova, obrnemo zadnji rob in zasukamo zadnji vogal. Orbit je torej dvanajst. $\square$

Ker je orbit dvanajst in ker so vse enako velike, je legalnih stanj natanko dvanajstina vseh, torej po izreku o orbiti in stabilizatorju (izrek 8) velja

$$|G| = \frac{|X|}{2 \cdot 2 \cdot 3} = 12! \cdot 2^{10} \cdot 8! \cdot 3^7 = 43252003274489856000.$$

S tem dobimo število legalnih stanj, do katerih lahko pridemo s premiki na Rubikovi kocki. Za primerjavo je na Zemlji šestkrat manj zrn peska kot vseh legalnih stanj. Imamo algoritme, ki pa rešijo Rubikovo kocko v končnem številu potez, ki ustrezajo navedenim invariantam (npr. CFOP, začetniška metoda, 3-Style).

Literatura

- [1] M. Brešar *Uvod v algebro*, DMFA – založništvo; 2018; dostopno na <https://users.fmf.uni-lj.si/bresar/documents/UvodVAIgebro2018.pdf>