

Algebarske strukture

prof.dr.sc. Saša Krešić-Jurić

PMF–Split

Promotrimo multiplikativnu grupu $G = \{1, -1, i, -i\}$. Primijetimo da sve elemente grupe G možemo zapisati kao potencije kompleksnog broja $i = \sqrt{-1}$:

$$G = \{1 = i^0, i = i^1, -1 = i^2, -i = i^3\}. \quad (1)$$

U ovom slučaju kažemo da element $i = \sqrt{-1}$ generira cijelu grupu i da G možemo zapisati kao

$$G = \{i^k \mid k \in \mathbb{Z}\}.$$

Kažemo da je $i = \sqrt{-1}$ **generator** grupe G i da je G **ciklička grupa** generirana elementom $i = \sqrt{-1}$.

Promotrimo multiplikativnu grupu $G = \{1, -1, i, -i\}$. Primijetimo da sve elemente grupe G možemo zapisati kao potencije kompleksnog broja $i = \sqrt{-1}$:

$$G = \{1 = i^0, i = i^1, -1 = i^2, -i = i^3\}. \quad (1)$$

U ovom slučaju kažemo da element $i = \sqrt{-1}$ generira cijelu grupu i da G možemo zapisati kao

$$G = \{i^k \mid k \in \mathbb{Z}\}.$$

Kažemo da je $i = \sqrt{-1}$ generator grupe G i da je G ciklička grupa generirana elementom $i = \sqrt{-1}$.

Promotrimo multiplikativnu grupu $G = \{1, -1, i, -i\}$. Primijetimo da sve elemente grupe G možemo zapisati kao potencije kompleksnog broja $i = \sqrt{-1}$:

$$G = \{1 = i^0, i = i^1, -1 = i^2, -i = i^3\}. \quad (1)$$

U ovom slučaju kažemo da element $i = \sqrt{-1}$ generira cijelu grupu i da G možemo zapisati kao

$$G = \{i^k \mid k \in \mathbb{Z}\}.$$

Kažemo da je $i = \sqrt{-1}$ **generator** grupe G i da je G **ciklička grupa** generirana elementom $i = \sqrt{-1}$.

Definicija

Kažemo da je G ciklička grupa ako postoji $a \in G$ takav da je

$$G = \{a^k \mid k \in \mathbb{Z}\}.$$

Ako je G aditivna grupa, onda pišemo

$$G = \{ka \mid k \in \mathbb{Z}\}.$$

Cikličku grupu generiranu elementom $a \in G$ zapisujemo sa $G = \langle a \rangle$.

- Cikličke grupe su najjednostavniji tip grupa.
- Svi elementi grupe su potencije nekog elementa kojeg nazivamo generator grupe.
- Cikličke grupe je moguće potpuno klasificirati. Struktura grupe ovisi samo o njezinom redu.
- Za svaki cikličku grupu možemo potpuno opisati sve njezine podgrupe.

Definicija

Kažemo da je G ciklička grupa ako postoji $a \in G$ takav da je

$$G = \{a^k \mid k \in \mathbb{Z}\}.$$

Ako je G aditivna grupa, onda pišemo

$$G = \{ka \mid k \in \mathbb{Z}\}.$$

Cikličku grupu generiranu elementom $a \in G$ zapisujemo sa $G = \langle a \rangle$.

- Cikličke grupe su najjednostavniji tip grupa.
- Svi elementi grupe su potencije nekog elementa kojeg nazivamo generator grupe.
- Cikličke grupe je moguće potpuno klasificirati. Struktura grupe ovisi samo o njezinom redu.
- Za svaki cikličku grupu možemo potpuno opisati sve njezine podgrupe.

Definicija

Kažemo da je G ciklička grupa ako postoji $a \in G$ takav da je

$$G = \{a^k \mid k \in \mathbb{Z}\}.$$

Ako je G aditivna grupa, onda pišemo

$$G = \{ka \mid k \in \mathbb{Z}\}.$$

Cikličku grupu generiranu elementom $a \in G$ zapisujemo sa $G = \langle a \rangle$.

- Cikličke grupe su najjednostavniji tip grupa.
- Svi elementi grupe su potencije nekog elementa kojeg nazivamo generator grupe.
- Cikličke grupe je moguće potpuno klasificirati. Struktura grupe ovisi samo o njezinom redu.
- Za svaki cikličku grupu možemo potpuno opisati sve njezine podgrupe.

Definicija

Kažemo da je G ciklička grupa ako postoji $a \in G$ takav da je

$$G = \{a^k \mid k \in \mathbb{Z}\}.$$

Ako je G aditivna grupa, onda pišemo

$$G = \{ka \mid k \in \mathbb{Z}\}.$$

Cikličku grupu generiranu elementom $a \in G$ zapisujemo sa $G = \langle a \rangle$.

- Cikličke grupe su najjednostavniji tip grupa.
- Svi elementi grupe su potencije nekog elementa kojeg nazivamo generator grupe.
- Cikličke grupe je moguće potpuno klasificirati. Struktura grupe ovisi samo o njezinom redu.
- Za svaki cikličku grupu možemo potpuno opisati sve njezine podgrupe.

Definicija

Kažemo da je G ciklička grupa ako postoji $a \in G$ takav da je

$$G = \{a^k \mid k \in \mathbb{Z}\}.$$

Ako je G aditivna grupa, onda pišemo

$$G = \{ka \mid k \in \mathbb{Z}\}.$$

Cikličku grupu generiranu elementom $a \in G$ zapisujemo sa $G = \langle a \rangle$.

- Cikličke grupe su najjednostavniji tip grupa.
- Svi elementi grupe su potencije nekog elementa kojeg nazivamo generator grupe.
- Cikličke grupe je moguće potpuno klasificirati. Struktura grupe ovisi samo o njezinom redu.
- Za svaki cikličku grupu možemo potpuno opisati sve njezine podgrupe.

Primjeri cikličkih grupa

- 1 Aditivna grupa $(\mathbb{Z}, +)$.
- 2 Aditivna grupa $(\mathbb{Z}_n, +)$.
- 3 Multiplikativna grupa $G = \{z \in \mathbb{C} \mid z^n = 1\}$.

Ako je $a \in G$ proizvoljni element grupe G , onda je skup

$$H = \{a^k \mid k \in \mathbb{Z}\}$$

podgrupa od G jer za sve $a^k, a^l \in H$ vrijedi

$$a^k \cdot (a^l)^{-1} = a^k \cdot a^{-l} = a^{k-l} \in H.$$

Kažemo da je H **ciklička podgrupa** od G i pišemo $H = \langle a \rangle$.

Primjeri cikličkih grupa

- 1 Aditivna grupa $(\mathbb{Z}, +)$.
- 2 Aditivna grupa $(\mathbb{Z}_n, +)$.
- 3 Multiplikativna grupa $G = \{z \in \mathbb{C} \mid z^n = 1\}$.

Ako je $a \in G$ proizvoljni element grupe G , onda je skup

$$H = \{a^k \mid k \in \mathbb{Z}\}$$

podgrupa od G jer za sve $a^k, a^l \in H$ vrijedi

$$a^k \cdot (a^l)^{-1} = a^k \cdot a^{-l} = a^{k-l} \in H.$$

Kažemo da je H **ciklička podgrupa** od G i pišemo $H = \langle a \rangle$.

Primjeri cikličkih grupa

- 1 Aditivna grupa $(\mathbb{Z}, +)$.
- 2 Aditivna grupa $(\mathbb{Z}_n, +)$.
- 3 Multiplikativna grupa $G = \{z \in \mathbb{C} \mid z^n = 1\}$.

Ako je $a \in G$ proizvoljni element grupe G , onda je skup

$$H = \{a^k \mid k \in \mathbb{Z}\}$$

podgrupa od G jer za sve $a^k, a^l \in H$ vrijedi

$$a^k \cdot (a^l)^{-1} = a^k \cdot a^{-l} = a^{k-l} \in H.$$

Kažemo da je H **ciklička podgrupa** od G i pišemo $H = \langle a \rangle$.

Primjeri cikličkih grupa

- 1 Aditivna grupa $(\mathbb{Z}, +)$.
- 2 Aditivna grupa $(\mathbb{Z}_n, +)$.
- 3 Multiplikativna grupa $G = \{z \in \mathbb{C} \mid z^n = 1\}$.

Ako je $a \in G$ proizvoljni element grupe G , onda je skup

$$H = \{a^k \mid k \in \mathbb{Z}\}$$

podgrupa od G jer za sve $a^k, a^l \in H$ vrijedi

$$a^k \cdot (a^l)^{-1} = a^k \cdot a^{-l} = a^{k-l} \in H.$$

Kažemo da je H **ciklička podgrupa** od G i pišemo $H = \langle a \rangle$.

Definicija

Neka je G grupa i neka je $a \in G$. Ako postoji $m \in \mathbb{N}$ takav da je $a^m = e$, onda najmanji takav m nazivamo red elementa a i označavamo s $|a|$.

Ako takav broj ne postoji, kažemo da je a beskonačnog reda i pišemo $|a| = \infty$.

Očigledno je $|a| = 1$ ako i samo ako je $a = e$.

Propozicija

Neka je G grupa i neka je $a \in G$, $a \neq e$.

- Ako je $|a| = n$ za neki $n \in \mathbb{N}$, tada su elementi $e, a, a^2, \dots, a^{n-1}$ različiti i $\langle a \rangle = \{e, a, a^2, \dots, a^{n-1}\}$.
- Ako je $|a| = \infty$, tada je $a^k \neq a^l$ za sve $k, l \in \mathbb{Z}$, $k \neq l$.

Korolar

Red cikličke grupe $G = \langle a \rangle$ jednak je redu generatora,

$$|G| = |a|.$$

Definicija

Neka je G grupa i neka je $a \in G$. Ako postoji $m \in \mathbb{N}$ takav da je $a^m = e$, onda najmanji takav m nazivamo red elementa a i označavamo s $|a|$.

Ako takav broj ne postoji, kažemo da je a beskonačnog reda i pišemo $|a| = \infty$.

Očigledno je $|a| = 1$ ako i samo ako je $a = e$.

Propozicija

Neka je G grupa i neka je $a \in G$, $a \neq e$.

- 1 Ako je $|a| = n$ za neki $n \in \mathbb{N}$, tada su elementi $e, a, a^2, \dots, a^{n-1}$ različiti i $\langle a \rangle = \{e, a, a^2, \dots, a^{n-1}\}$.
- 2 Ako je $|a| = \infty$, tada je $a^k \neq a^l$ za sve $k, l \in \mathbb{Z}$, $k \neq l$.

Korolar

Red cikličke grupe $G = \langle a \rangle$ jednak je redu generatora,

$$|G| = |a|.$$

Definicija

Neka je G grupa i neka je $a \in G$. Ako postoji $m \in \mathbb{N}$ takav da je $a^m = e$, onda najmanji takav m nazivamo red elementa a i označavamo s $|a|$.

Ako takav broj ne postoji, kažemo da je a beskonačnog reda i pišemo $|a| = \infty$.

Očigledno je $|a| = 1$ ako i samo ako je $a = e$.

Propozicija

Neka je G grupa i neka je $a \in G$, $a \neq e$.

- 1 Ako je $|a| = n$ za neki $n \in \mathbb{N}$, tada su elementi $e, a, a^2, \dots, a^{n-1}$ različiti i $\langle a \rangle = \{e, a, a^2, \dots, a^{n-1}\}$.
- 2 Ako je $|a| = \infty$, tada je $a^k \neq a^l$ za sve $k, l \in \mathbb{Z}$, $k \neq l$.

Korolar

Red cikličke grupe $G = \langle a \rangle$ jednak je redu generatora,

$$|G| = |a|.$$

Propozicija

Neka je G konačna grupa reda $|G| \geq 2$ i neka je $a \in G$, $a \neq e$. Tada $|a|$ dijeli $|G|$.
Nadalje, ako je $|G|$ prosti broj, tada je G ciklička grupa.

Teorem (Klasifikacija ciličkih grupa)

Neka je $G = \langle a \rangle$ ciklička grupa.

- Ako je $|G| = \infty$, onda je G izomorfna grupi $(\mathbb{Z}, +)$.
- Ako je $|G| = n < \infty$, onda je G izomorfna grupi $(\mathbb{Z}_n, +)$.

Cikličke grupe reda n zapisujemo kao

$$G = \langle a \mid a^n = e \rangle, \quad a \text{ generator,} \quad a^n = e \text{ relacija.}$$

Korolar

Svake dvije cikličke grupe istog reda su izomorfne.

Propozicija

Neka je G konačna grupa reda $|G| \geq 2$ i neka je $a \in G$, $a \neq e$. Tada $|a|$ dijeli $|G|$.
Nadalje, ako je $|G|$ prosti broj, tada je G ciklička grupa.

Teorem (Klasifikacija ciličkih grupa)

Neka je $G = \langle a \rangle$ ciklička grupa.

- 1 Ako je $|G| = \infty$, onda je G izomorfna grupi $(\mathbb{Z}, +)$.
- 2 Ako je $|G| = n < \infty$, onda je G izomorfna grupi $(\mathbb{Z}_n, +)$.

Cikličke grupe reda n zapisujemo kao

$$G = \langle a \mid a^n = e \rangle, \quad a \text{ generator,} \quad a^n = e \text{ relacija.}$$

Korolar

Svake dvije cikličke grupe istog reda su izomorfne.

Propozicija

Neka je G konačna grupa reda $|G| \geq 2$ i neka je $a \in G$, $a \neq e$. Tada $|a|$ dijeli $|G|$.
Nadalje, ako je $|G|$ prosti broj, tada je G ciklička grupa.

Teorem (Klasifikacija ciličkih grupa)

Neka je $G = \langle a \rangle$ ciklička grupa.

- 1 Ako je $|G| = \infty$, onda je G izomorfna grupi $(\mathbb{Z}, +)$.
- 2 Ako je $|G| = n < \infty$, onda je G izomorfna grupi $(\mathbb{Z}_n, +)$.

Cikličke grupe reda n zapisujemo kao

$$G = \langle a \mid a^n = e \rangle, \quad a \text{ generator}, \quad a^n = e \text{ relacija.}$$

Korolar

Svake dvije cikličke grupe istog reda su izomorfne.

Propozicija

Neka je G konačna grupa reda $|G| \geq 2$ i neka je $a \in G$, $a \neq e$. Tada $|a|$ dijeli $|G|$.
Nadalje, ako je $|G|$ prosti broj, tada je G ciklička grupa.

Teorem (Klasifikacija ciličkih grupa)

Neka je $G = \langle a \rangle$ ciklička grupa.

- 1 Ako je $|G| = \infty$, onda je G izomorfna grupi $(\mathbb{Z}, +)$.
- 2 Ako je $|G| = n < \infty$, onda je G izomorfna grupi $(\mathbb{Z}_n, +)$.

Cikličke grupe reda n zapisujemo kao

$$G = \langle a \mid a^n = e \rangle, \quad a \text{ generator}, \quad a^n = e \text{ relacija.}$$

Korolar

Svake dvije cikličke grupe istog reda su izomorfne.

Teorem

Neka je $G = \langle a \rangle$ ciklička grupa. Svaka podgrupa grupe G je ciklička.

Podgrupe cikličke grupe reda n su u bijektivnoj korespodenciji s djeliteljima broja n .

Teorem

Neka je G ciklička grupa reda n . Tada za svaki $m \in \mathbb{N}$ takav da $m \mid n$ postoji jedinstvena podgrupa od G reda m .

Primjer

Odredite sve podgrupe cikličke grupe $\mathbb{Z}_6$ i njihove generatore.

Teorem

Neka je $G = \langle a \rangle$ ciklička grupa. Svaka podgrupa grupe G je ciklička.

Podgrupe cikličke grupe reda n su u bijektivnoj korespodenciji s djeljiteljima broja n .

Teorem

Neka je G ciklička grupa reda n . Tada za svaki $m \in \mathbb{N}$ takav da $m \mid n$ postoji jedinstvena podgrupa od G reda m .

Primjer

Odredite sve podgrupe cikličke grupe $\mathbb{Z}_6$ i njihove generatore.

Teorem

Neka je $G = \langle a \rangle$ ciklička grupa. Svaka podgrupa grupe G je ciklička.

Podgrupe cikličke grupe reda n su u bijektivnoj korespodenciji s djeliteljima broja n .

Teorem

Neka je G ciklička grupa reda n . Tada za svaki $m \in \mathbb{N}$ takav da $m \mid n$ postoji jedinstvena podgrupa od G reda m .

Primjer

Odredite sve podgrupe cikličke grupe $\mathbb{Z}_6$ i njihove generatore.

Grupe permutacija

Definicija

Svaka bijekcija $f: X \rightarrow X$ naziva se permutacija na skupu X .

Permutacije na skupu X tvore grupu s obzirom na binarnu operaciju kompozicije $f \circ g$.

Neutralni element: id_X identiteta na X

Inverzni element: f^{-1} inverzna funkcija

Definicija

Grupa svih permutacija na nepraznom skupu X naziva se simetrična grupa na X i označava sa S_X . Svaka podgrupa grupe S_X naziva se grupa permutacija na X .

S_X simetrična grupa na X

$G \subseteq S_X$ grupa permutacija na X

S_n simetrična grupa na skupu od n elemenata, $|X| = n$, $|S_n| = n!$

Grupe permutacija

Definicija

Svaka bijekcija $f: X \rightarrow X$ naziva se permutacija na skupu X .

Permutacije na skupu X tvore grupu s obzirom na binarnu operaciju kompozicije $f \circ g$.

Neutralni element: id_X identiteta na X

Inverzni element: f^{-1} inverzna funkcija

Definicija

Grupa svih permutacija na nepraznom skupu X naziva se simetrična grupa na X i označava sa S_X . Svaka podgrupa grupe S_X naziva se grupa permutacija na X .

S_X simetrična grupa na X

$G \subseteq S_X$ grupa permutacija na X

S_n simetrična grupa na skupu od n elemenata, $|X| = n$, $|S_n| = n!$

Permutacije na konačnim skupovima možemo zapisati u matričnom obliku

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}.$$

Neutralni element je matrica

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}.$$

Primjer

Permutacije na skupu $X = \{1, 2, 3\}$ su dane sa

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \quad (2)$$

$$\sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad \sigma_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}. \quad (3)$$

Permutacije na konačnim skupovima možemo zapisati u matričnom obliku

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}.$$

Neutralni element je matrica

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}.$$

Primjer

Permutacije na skupu $X = \{1, 2, 3\}$ su dane sa

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \quad (2)$$

$$\sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad \sigma_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}. \quad (3)$$

Definicija

Neka je $\sigma \in S_n$. Ako postoje $x_1, x_2, \dots, x_r \in \{1, 2, \dots, n\}$ takvi da je

$$\sigma(x_i) = x_{i+1}, \quad i = 1, 2, \dots, r-1,$$

$$\sigma(x_r) = x_1,$$

$$\sigma(x) = x, \quad x \notin \{x_1, x_2, \dots, x_r\},$$

tada permutaciju σ nazivamo ciklička permutacija duljine r i označavamo s $(x_1 x_2 \dots x_r)$. Cikličku permutaciju duljine dva nazivamo transpozicija.

Identiteta u S_n : ciklička permutacija (x) , $x \in \{1, 2, \dots, n\}$.

Definicija

Kažemo da su dvije cikličke permutacije $(x_1 x_2 \dots x_r)$ i $(y_1 y_2 \dots y_s)$ disjunktne ako je

$$\{x_1, x_2, \dots, x_r\} \cap \{y_1, y_2, \dots, y_s\} = \emptyset.$$

Definicija

Neka je $\sigma \in S_n$. Ako postoje $x_1, x_2, \dots, x_r \in \{1, 2, \dots, n\}$ takvi da je

$$\sigma(x_i) = x_{i+1}, \quad i = 1, 2, \dots, r-1,$$

$$\sigma(x_r) = x_1,$$

$$\sigma(x) = x, \quad x \notin \{x_1, x_2, \dots, x_r\},$$

tada permutaciju σ nazivamo ciklička permutacija duljine r i označavamo s $(x_1 x_2 \dots x_r)$. Cikličku permutaciju duljine dva nazivamo transpozicija.

Identiteta u S_n : ciklička permutacija (x) , $x \in \{1, 2, \dots, n\}$.

Definicija

Kažemo da su dvije cikličke permutacije $(x_1 x_2 \dots x_r)$ i $(y_1 y_2 \dots y_s)$ disjunktne ako je

$$\{x_1, x_2, \dots, x_r\} \cap \{y_1, y_2, \dots, y_s\} = \emptyset.$$

Definicija

Neka je $\sigma \in S_n$. Ako postoje $x_1, x_2, \dots, x_r \in \{1, 2, \dots, n\}$ takvi da je

$$\sigma(x_i) = x_{i+1}, \quad i = 1, 2, \dots, r-1,$$

$$\sigma(x_r) = x_1,$$

$$\sigma(x) = x, \quad x \notin \{x_1, x_2, \dots, x_r\},$$

tada permutaciju σ nazivamo ciklička permutacija duljine r i označavamo s $(x_1 x_2 \dots x_r)$. Cikličku permutaciju duljine dva nazivamo transpozicija.

Identiteta u S_n : ciklička permutacija (x) , $x \in \{1, 2, \dots, n\}$.

Definicija

Kažemo da su dvije cikličke permutacije $(x_1 x_2 \dots x_r)$ i $(y_1 y_2 \dots y_s)$ disjunktne ako je

$$\{x_1, x_2, \dots, x_r\} \cap \{y_1, y_2, \dots, y_s\} = \emptyset.$$

Teorem

Svaka permutacija $\sigma \in S_n$ je umnožak disjunktних cikličkih permutacija. Ciklička faktorizacija je jedinstvena do na poredak cikličkih permutacija i umetanje ili ispuštanje cikličkih permutacija duljine jedan.

Algoritam za cikličku faktorizaciju

- 1 Prvu cikličku permutaciju započnemo s $a_1 = 1$. Odredimo $a_2 = \sigma(a_1)$. Ako je $a_2 = a_1$, onda ciklička permutacija ima duljinu jedan i pišemo (a_1) . Ako je $a_2 \neq a_1$, onda pišemo $(a_1 a_2 \dots)$ (bez desne zagrade!).
Odredimo $a_3 = \sigma(a_2)$. Ako je $a_3 = a_1$, onda je ciklička permutacija dana s $(a_1 a_2)$. Ako je $a_3 \neq a_1$, onda pišemo $(a_1 a_2 a_3)$. Ovaj postupak ponavljamo dok se ciklička permutacija ne zatvori.
- 2 U sljedećem koraku svaku sljedeću cikličku permutaciju započinjemo s najmanjim elementom $a_1 \in \{1, 2, \dots, n\}$ koji se ne nalazi u prethodnim permutacijama.
- 3 Korake (1)–(2) ponavljamo dok se ne iscrpe svi brojevi u skupu $\{1, 2, \dots, n\}$.

Teorem

Svaka permutacija $\sigma \in S_n$ je umnožak disjunktne cikličke permutacije. Ciklička faktorizacija je jedinstvena do na poredak cikličke permutacije i umetanje ili ispuštanje cikličke permutacije duljine jedan.

Algoritam za cikličku faktorizaciju

- 1 Prvu cikličku permutaciju započnemo s $a_1 = 1$. Odredimo $a_2 = \sigma(a_1)$. Ako je $a_2 = a_1$, onda ciklička permutacija ima duljinu jedan i pišemo (a_1) . Ako je $a_2 \neq a_1$, onda pišemo $(a_1 a_2$ (bez desne zagrade!).
Odredimo $a_3 = \sigma(a_2)$. Ako je $a_3 = a_1$, onda je ciklička permutacija dana s $(a_1 a_2)$. Ako je $a_3 \neq a_1$, onda pišemo $(a_1 a_2 a_3)$. Ovaj postupak ponavljamo dok se ciklička permutacija ne zatvori.
- 2 U sljedećem koraku svaku sljedeću cikličku permutaciju započinjemo s najmanjim elementom $a_1 \in \{1, 2, \dots, n\}$ koji se ne nalazi u prethodnim permutacijama.
- 3 Korake (1)–(2) ponavljamo dok se ne iscrpe svi brojevi u skupu $\{1, 2, \dots, n\}$.

Svaku cikličku permutaciju $(a_1 a_2 \dots a_m)$ možemo faktorizirati kao

$$(a_1 a_2 \dots a_m) = (a_1 a_m)(a_1 a_{m-1}) \dots (a_1 a_2).$$

Korolar

Svaka permutacija se može napisati kao umnožak transpozicija.

Teorem

Ako se permutacija σ može napisati kao umnožak od r transpozicija i kao umnožak od s transpozicija, onda su r i s ili oba parna ili oba neparna.

Definicija

Kažemo da je permutacija $\sigma \in S_n$ parna (neparna) ako se može napisati kao umnožak parnog (neparnog) broja transpozicija. Predznak permutacije σ definiran je s

$$\epsilon(\sigma) = \begin{cases} +1 & \text{ako je } \sigma \text{ je parna permutacija,} \\ -1 & \text{ako je } \sigma \text{ je neparna permutacija.} \end{cases}$$

Svaku cikličku permutaciju $(a_1 a_2 \dots a_m)$ možemo faktorizirati kao

$$(a_1 a_2 \dots a_m) = (a_1 a_m)(a_1 a_{m-1}) \dots (a_1 a_2).$$

Korolar

Svaka permutacija se može napisati kao umnožak transpozicija.

Teorem

Ako se permutacija σ može napisati kao umnožak od r transpozicija i kao umnožak od s transpozicija, onda su r i s ili oba parna ili oba neparna.

Definicija

Kažemo da je permutacija $\sigma \in S_n$ parna (neparna) ako se može napisati kao umnožak parnog (neparnog) broja transpozicija. Predznak permutacije σ definiran je s

$$\epsilon(\sigma) = \begin{cases} +1 & \text{ako je } \sigma \text{ je parna permutacija,} \\ -1 & \text{ako je } \sigma \text{ je neparna permutacija.} \end{cases}$$

Svaku cikličku permutaciju $(a_1 a_2 \dots a_m)$ možemo faktorizirati kao

$$(a_1 a_2 \dots a_m) = (a_1 a_m)(a_1 a_{m-1}) \dots (a_1 a_2).$$

Korolar

Svaka permutacija se može napisati kao umnožak transpozicija.

Teorem

Ako se permutacija σ može napisati kao umnožak od r transpozicija i kao umnožak od s transpozicija, onda su r i s ili oba parna ili oba neparna.

Definicija

Kažemo da je permutacija $\sigma \in S_n$ parna (neparna) ako se može napisati kao umnožak parnog (neparnog) broja transpozicija. Predznak permutacije σ definiran je s

$$\epsilon(\sigma) = \begin{cases} +1 & \text{ako je } \sigma \text{ je parna permutacija,} \\ -1 & \text{ako je } \sigma \text{ je neparna permutacija.} \end{cases}$$

Svaku cikličku permutaciju $(a_1 a_2 \dots a_m)$ možemo faktorizirati kao

$$(a_1 a_2 \dots a_m) = (a_1 a_m)(a_1 a_{m-1}) \dots (a_1 a_2).$$

Korolar

Svaka permutacija se može napisati kao umnožak transpozicija.

Teorem

Ako se permutacija σ može napisati kao umnožak od r transpozicija i kao umnožak od s transpozicija, onda su r i s ili oba parna ili oba neparna.

Definicija

Kažemo da je permutacija $\sigma \in S_n$ parna (neparna) ako se može napisati kao umnožak parnog (neparnog) broja transpozicija. Predznak permutacije σ definiran je s

$$\epsilon(\sigma) = \begin{cases} +1 & \text{ako je } \sigma \text{ je parna permutacija,} \\ -1 & \text{ako je } \sigma \text{ je neparna permutacija.} \end{cases}$$

Lema

Neka je $n \geq 2$. Preslikavanje $\epsilon: S_n \rightarrow G$, gdje je $G = \{1, -1\}$ multiplikativna grupa, je epimorfizam.

Definicija

Skup svih parnih permutacija u S_n , $n > 1$, nazivamo alternirajuća grupa A_n .

Teorem

Neka je $n \geq 2$. Onda je A_n normalna podgrupa simetrične grupe S_n i $|A_n| = \frac{1}{2}n!$.

Cayleyev teorem

Svaka grupa je izomorfna nekoj grupi permutacija.

$\varphi: G \rightarrow S_G, \quad \varphi(g) = L_g, \quad$ permutacijska reprezentacija grupe G

Lema

Neka je $n \geq 2$. Preslikavanje $\epsilon: S_n \rightarrow G$, gdje je $G = \{1, -1\}$ multiplikativna grupa, je epimorfizam.

Definicija

Skup svih parnih permutacija u S_n , $n > 1$, nazivamo alternirajuća grupa A_n .

Teorem

Neka je $n \geq 2$. Onda je A_n normalna podgrupa simetrične grupe S_n i $|A_n| = \frac{1}{2}n!$.

Cayleyev teorem

Svaka grupa je izomorfna nekoj grupi permutacija.

$\varphi: G \rightarrow S_G, \quad \varphi(g) = L_g, \quad$ permutacijska reprezentacija grupe G

Lema

Neka je $n \geq 2$. Preslikavanje $\epsilon: S_n \rightarrow G$, gdje je $G = \{1, -1\}$ multiplikativna grupa, je epimorfizam.

Definicija

Skup svih parnih permutacija u S_n , $n > 1$, nazivamo alternirajuća grupa A_n .

Teorem

Neka je $n \geq 2$. Onda je A_n normalna podgrupa simetrične grupe S_n i $|A_n| = \frac{1}{2}n!$.

Cayleyev teorem

Svaka grupa je izomorfna nekoj grupi permutacija.

$$\varphi: G \rightarrow S_G, \quad \varphi(g) = L_g, \quad \text{permutacijska reprezentacija grupe } G$$

Lema

Neka je $n \geq 2$. Preslikavanje $\epsilon: S_n \rightarrow G$, gdje je $G = \{1, -1\}$ multiplikativna grupa, je epimorfizam.

Definicija

Skup svih parnih permutacija u S_n , $n > 1$, nazivamo alternirajuća grupa A_n .

Teorem

Neka je $n \geq 2$. Onda je A_n normalna podgrupa simetrične grupe S_n i $|A_n| = \frac{1}{2}n!$.

Cayleyev teorem

Svaka grupa je izomorfna nekoj grupi permutacija.

$\varphi: G \rightarrow S_G, \quad \varphi(g) = L_g, \quad$ permutacijska reprezentacija grupe G

Lema

Neka je $n \geq 2$. Preslikavanje $\epsilon: S_n \rightarrow G$, gdje je $G = \{1, -1\}$ multiplikativna grupa, je epimorfizam.

Definicija

Skup svih parnih permutacija u S_n , $n > 1$, nazivamo alternirajuća grupa A_n .

Teorem

Neka je $n \geq 2$. Onda je A_n normalna podgrupa simetrične grupe S_n i $|A_n| = \frac{1}{2}n!$.

Cayleyev teorem

Svaka grupa je izomorfna nekoj grupi permutacija.

$$\varphi: G \rightarrow S_G, \quad \varphi(g) = L_g, \quad \text{permutacijska reprezentacija grupe } G$$

Generatori i relacije

Elementi grupe S_3 su dani sa

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \quad (4)$$

$$\sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad \sigma_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}. \quad (5)$$

Sve elemente grupe S_3 možemo zapisati koristeći dvije permutacije:

$$\sigma \equiv \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \tau \equiv \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

Lako se provjeri da je

$$\sigma^2 = \sigma_2, \quad \sigma^3 = e, \quad \tau^2 = e, \quad \sigma^2\tau = \tau\sigma = \sigma_4, \quad \sigma\tau = \sigma_5.$$

Grupu S_3 možemo zapisati kao

$$S_3 = \{e, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}, \quad \sigma, \tau \text{ generatori grupe } S_3$$

Generatori i relacije

Elementi grupe S_3 su dani sa

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \quad (4)$$

$$\sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad \sigma_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}. \quad (5)$$

Sve elemente grupe S_3 možemo zapisati koristeći dvije permutacije:

$$\sigma \equiv \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \tau \equiv \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

Lako se provjeri da je

$$\sigma^2 = \sigma_2, \quad \sigma^3 = e, \quad \tau^2 = e, \quad \sigma^2\tau = \tau\sigma = \sigma_4, \quad \sigma\tau = \sigma_5.$$

Grupu S_3 možemo zapisati kao

$$S_3 = \{e, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}, \quad \sigma, \tau \text{ generatori grupe } S_3$$

Cayleyevu tablicu grupe S_3 možemo ispuniti koristeći relacije

$$\sigma^3 = \tau^2 = e, \quad \tau\sigma = \sigma^2\tau.$$

Grupa S_3 je potpuno određena generatorima σ i τ i njihovim relacijama:

$$S_3 = \langle \sigma, \tau \mid \sigma^3 = \tau^2 = e, \tau\sigma = \sigma^2\tau \rangle.$$

$S = \{\sigma, \tau\}$ skup generatora

$\sigma^3 = \tau^2 = e, \quad \tau\sigma = \sigma^2\tau$ relacije

Definicija

- 1 Podskup S grupe G sa svojstvom da se svaki element iz G može napisati kao konačni umnožak elemenata iz S i njihovih inverza se naziva skup generatora od G .
- 2 Ako su $R_1, R_2, \dots, R_m$ relacije na skupu $S \cup \{e\}$ takve da se bilo koja relacija među elementima iz S može odrediti iz relacija $R_1, R_2, \dots, R_m$, onda kažemo da S i $R_1, R_2, \dots, R_m$ daju prezentaciju grupe G i pišemo

$$G = \langle S \mid R_1, R_2, \dots, R_m \rangle.$$

Primjedba Ako je G konačna grupa, onda je G generirana elementima iz S (bez njihovih inverza).

Prednosti prezentacije Korištenjem generatora i relacija pojednostavljuje se prikaz elemenata i računanje u grupi.

Mane prezentacije

- Prezentacija grupe ne mora biti jedinstvena.
- Određivanje generatora i relacija za zadanu grupu može biti komplicirano.

Definicija

- 1 Podskup S grupe G sa svojstvom da se svaki element iz G može napisati kao konačni umnožak elemenata iz S i njihovih inverza se naziva skup generatora od G .
- 2 Ako su $R_1, R_2, \dots, R_m$ relacije na skupu $S \cup \{e\}$ takve da se bilo koja relacija među elementima iz S može odrediti iz relacija $R_1, R_2, \dots, R_m$, onda kažemo da S i $R_1, R_2, \dots, R_m$ daju prezentaciju grupe G i pišemo

$$G = \langle S \mid R_1, R_2, \dots, R_m \rangle.$$

Primjedba Ako je G konačna grupa, onda je G generirana elementima iz S (bez njihovih inverza).

Prednosti prezentacije Korišenjem generatora i relacija pojednostavljuje se prikaz elemenata i računanje u grupi.

Mane prezentacije

- Prezetacija grupe ne mora biti jedinstvena.
- Određivanje generatora i relacija za zadanu grupu može biti komplicirano.

Definicija

- 1 Podskup S grupe G sa svojstvom da se svaki element iz G može napisati kao konačni umnožak elemenata iz S i njihovih inverza se naziva skup generatora od G .
- 2 Ako su $R_1, R_2, \dots, R_m$ relacije na skupu $S \cup \{e\}$ takve da se bilo koja relacija među elementima iz S može odrediti iz relacija $R_1, R_2, \dots, R_m$, onda kažemo da S i $R_1, R_2, \dots, R_m$ daju prezentaciju grupe G i pišemo

$$G = \langle S \mid R_1, R_2, \dots, R_m \rangle.$$

Primjedba Ako je G konačna grupa, onda je G generirana elementima iz S (bez njihovih inverza).

Prednosti prezentacije Korištenjem generatora i relacija pojednostavljuje se prikaz elemenata i računanje u grupi.

Mane prezentacije

- Prezentacija grupe ne mora biti jedinstvena.
- Određivanje generatora i relacija za zadanu grupu može biti komplicirano.

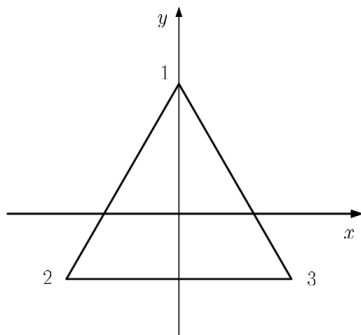
Diedralne grupe

Diedralne grupe su grupe simetrija pravilnih poligona.

P_n pravilni poligon s vrhovima $1, 2, \dots, n$,

$X = \{1, 2, \dots, n\}$ skup vrhova poligona P_n .

Pravilni poligon P_3 :



Definicija

Simetrija poligona P_n s vrhovima $X = \{1, 2, \dots, n\}$ je svaka permutacija σ na skupu X takva da je

$$d(k, l) = d(\sigma(k), \sigma(l)) \quad \forall k, l \in X \quad (6)$$

gdje je $d(k, l)$ udaljenost vrha k od vrha l .

Definicija

Grupa simetrija pravilnog poligona P_n naziva se diedralna grupa D_{2n} .

Elementi diedralne grupe čuvaju udaljenost između svakog para vrhova poligona P_n .

Svaka permutacija $\sigma \in D_{2n}$ je potpuno određena preslikavanjem dva susjedna vrha:

$$\begin{aligned} 1 &\mapsto k \in \{1, 2, \dots, n\}, \\ 2 &\mapsto k + 1 \text{ ili } k - 1 \pmod{n}. \end{aligned}$$

Dakle, grupa D_{2n} ima $2n$ elemenata, $|D_{2n}| = 2n$.

Definicija

Simetrija poligona P_n s vrhovima $X = \{1, 2, \dots, n\}$ je svaka permutacija σ na skupu X takva da je

$$d(k, l) = d(\sigma(k), \sigma(l)) \quad \forall k, l \in X \quad (6)$$

gdje je $d(k, l)$ udaljenost vrha k od vrha l .

Definicija

Grupa simetrija pravilnog poligona P_n naziva se diedralna grupa D_{2n} .

Elementi diedralne grupe čuvaju udaljenost između svakog para vrhova poligona P_n .

Svaka permutacija $\sigma \in D_{2n}$ je potpuno određena preslikavanjem dva susjedna vrha:

$$\begin{aligned} 1 &\mapsto k \in \{1, 2, \dots, n\}, \\ 2 &\mapsto k + 1 \text{ ili } k - 1 \pmod{n}. \end{aligned}$$

Dakle, grupa D_{2n} ima $2n$ elemenata, $|D_{2n}| = 2n$.

Definicija

Simetrija poligona P_n s vrhovima $X = \{1, 2, \dots, n\}$ je svaka permutacija σ na skupu X takva da je

$$d(k, l) = d(\sigma(k), \sigma(l)) \quad \forall k, l \in X \quad (6)$$

gdje je $d(k, l)$ udaljenost vrha k od vrha l .

Definicija

Grupa simetrija pravilnog poligona P_n naziva se diedralna grupa D_{2n} .

Elementi diedralne grupe čuvaju udaljenost između svakog para vrhova poligona P_n .

Svaka permutacija $\sigma \in D_{2n}$ je potpuno određena preslikavanjem dva susjedna vrha:

$$\begin{aligned} 1 &\mapsto k \in \{1, 2, \dots, n\}, \\ 2 &\mapsto k + 1 \text{ ili } k - 1 \pmod{n}. \end{aligned}$$

Dakle, grupa D_{2n} ima $2n$ elemenata, $|D_{2n}| = 2n$.

Definicija

Simetrija poligona P_n s vrhovima $X = \{1, 2, \dots, n\}$ je svaka permutacija σ na skupu X takva da je

$$d(k, l) = d(\sigma(k), \sigma(l)) \quad \forall k, l \in X \quad (6)$$

gdje je $d(k, l)$ udaljenost vrha k od vrha l .

Definicija

Grupa simetrija pravilnog poligona P_n naziva se diedralna grupa D_{2n} .

Elementi diedralne grupe čuvaju udaljenost između svakog para vrhova poligona P_n .

Svaka permutacija $\sigma \in D_{2n}$ je potpuno određena preslikavanjem dva susjedna vrha:

$$\begin{aligned} 1 &\mapsto k \in \{1, 2, \dots, n\}, \\ 2 &\mapsto k + 1 \text{ ili } k - 1 \pmod{n}. \end{aligned}$$

Dakle, grupa D_{2n} ima $2n$ elemenata, $|D_{2n}| = 2n$.

Generatore grupe D_{2n} možemo odrediti na sljedeći način.

- Neka je R rotacija za kut $2\pi/n$ u pozitivnom smjeru koja preslikava vrh k u vrh $k + 1$. R je ciklička permutacija

$$R = (1\ 2\ 3\ \dots\ n).$$

Vrijedi

$$R^n = 1, \quad 1 \text{ jedinica u grupi } D_{2n}.$$

- Neka je D refleksija s obzirom na pravac koji prolazi vrhom 1 i središtem poligona. D je permutacija

$$D = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ 1 & n & n-1 & \dots & 2 \end{pmatrix}.$$

Vrijedi

$$D^2 = 1.$$

Elementi

$$1, R, R^2, \dots, R^{n-1}, D, DR, DR^2, \dots, DR^{n-1}$$

su različiti. Dakle,

$$D_{2n} = \left\{ 1, R, R^2, \dots, R^{n-1}, D, DR, DR^2, \dots, DR^{n-1} \right\}$$

Generatore grupe D_{2n} možemo odrediti na sljedeći način.

- Neka je R rotacija za kut $2\pi/n$ u pozitivnom smjeru koja preslikava vrh k u vrh $k + 1$. R je ciklička permutacija

$$R = (1\ 2\ 3\ \dots\ n).$$

Vrijedi

$$R^n = \mathbf{1}, \quad \mathbf{1} \text{ jedinica u grupi } D_{2n}.$$

- Neka je D refleksija s obzirom na pravac koji prolazi vrhom 1 i središtem poligona. D je permutacija

$$D = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ 1 & n & n-1 & \dots & 2 \end{pmatrix}.$$

Vrijedi

$$D^2 = \mathbf{1}.$$

Elementi

$$\mathbf{1}, R, R^2, \dots, R^{n-1}, D, DR, DR^2, \dots, DR^{n-1}$$

su različiti. Dakle,

$$D_{2n} = \left\{ \mathbf{1}, R, R^2, \dots, R^{n-1}, D, DR, DR^2, \dots, DR^{n-1} \right\}$$

Promatrajući kako rotacija i refleksija djeluju na vrhove poligona, lako se vidi da je

$$RD = DR^{-1} \Rightarrow R^k D = DR^{-k} \quad \forall 0 \leq k \leq n.$$

Prezentacija diedralne grupe

$$D_{2n} = \langle R, D \mid R^n = D^2 = 1, RD = DR^{n-1} \rangle.$$

Primjedba

Generatori grupe D_{2n} se mogu prikazati i matricama

$$R = \begin{pmatrix} \cos\left(\frac{2\pi}{n}\right) & -\sin\left(\frac{2\pi}{n}\right) \\ \sin\left(\frac{2\pi}{n}\right) & \cos\left(\frac{2\pi}{n}\right) \end{pmatrix}, \quad D = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

R rotacija za kut $\frac{2\pi}{n}$,

D refleksija u odnosu na pravac $y = x$.

Promatrajući kako rotacija i refleksija djeluju na vrhove poligona, lako se vidi da je

$$RD = DR^{-1} \Rightarrow R^k D = DR^{-k} \quad \forall 0 \leq k \leq n.$$

Prezentacija diedralne grupe

$$D_{2n} = \langle R, D \mid R^n = D^2 = 1, RD = DR^{n-1} \rangle.$$

Primjedba

Generatori grupe D_{2n} se mogu prikazati i matricama

$$R = \begin{pmatrix} \cos\left(\frac{2\pi}{n}\right) & -\sin\left(\frac{2\pi}{n}\right) \\ \sin\left(\frac{2\pi}{n}\right) & \cos\left(\frac{2\pi}{n}\right) \end{pmatrix}, \quad D = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

R rotacija za kut $\frac{2\pi}{n}$,

D refleksija u odnosu na pravac $y = x$.

Djelovanje grupe

Definicija

Kažemo da grupa G djeluje na skup A ako postoji preslikavanje $G \times A \rightarrow A$, $(g, a) \mapsto g \cdot a$, koje zadovoljava sljedeća svojstva:

- 1 $(g_1 g_2) \cdot a = g_1 \cdot (g_2 \cdot a)$ za sve $g_1, g_2 \in G$, $a \in A$,
- 2 $e \cdot a = a$ za svaki $a \in A$,

gdje je e jedinica u G .

Primjeri

- 1 $SO(2) = \left\{ R_\theta = \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix} \mid \theta \in \mathbb{R} \right\}$ djeluje na $\mathbb{R}^2$ matričnim množenjem

$$R_\theta \cdot (x, y) = \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \cos \theta - y \sin \theta \\ x \sin \theta + y \cos \theta \end{pmatrix}.$$

Definicija

Kažemo da grupa G djeluje na skup A ako postoji preslikavanje $G \times A \rightarrow A$, $(g, a) \mapsto g \cdot a$, koje zadovoljava sljedeća svojstva:

- 1 $(g_1 g_2) \cdot a = g_1 \cdot (g_2 \cdot a)$ za sve $g_1, g_2 \in G$, $a \in A$,
- 2 $e \cdot a = a$ za svaki $a \in A$,

gdje je e jedinica u G .

Primjeri

- $SO(2) = \left\{ R_\theta = \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix} \mid \theta \in \mathbb{R} \right\}$ djeluje na $\mathbb{R}^2$ matričnim množenjem

$$R_\theta \cdot (x, y) = \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \cos \theta - y \sin \theta \\ x \sin \theta + y \cos \theta \end{pmatrix}.$$

Definicija

Kažemo da grupa G djeluje na skup A ako postoji preslikavanje $G \times A \rightarrow A$, $(g, a) \mapsto g \cdot a$, koje zadovoljava sljedeća svojstva:

- 1 $(g_1 g_2) \cdot a = g_1 \cdot (g_2 \cdot a)$ za sve $g_1, g_2 \in G$, $a \in A$,
- 2 $e \cdot a = a$ za svaki $a \in A$,

gdje je e jedinica u G .

Primjeri

- 1 $SO(2) = \left\{ R_\theta = \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix} \mid \theta \in \mathbb{R} \right\}$ djeluje na $\mathbb{R}^2$ matičnim množenjem

$$R_\theta \cdot (x, y) = \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \cos \theta - y \sin \theta \\ x \sin \theta + y \cos \theta \end{pmatrix}.$$

2 Diedralna grupa D_{2n} djeluje na vrhove pravilnog poligona $\{v_1, v_2, \dots, v_n\}$ sa

$$\sigma \cdot v_i = v_{\sigma(i)}, \quad \sigma \in D_{2n}, \quad 1 \leq i \leq n, \quad (7)$$

gdje je σ permutacijska realizacija elemenata grupe D_{2n} .

3 Grupa G djeluje na skup G sa

lijevom translacijom $g \cdot a = ga,$

desnom translacijom $g \cdot a = ag^{-1},$

konjugacijom $g \cdot a = gag^{-1}.$

- 2 Diedralna grupa D_{2n} djeluje na vrhove pravilnog poligona $\{v_1, v_2, \dots, v_n\}$ sa

$$\sigma \cdot v_i = v_{\sigma(i)}, \quad \sigma \in D_{2n}, \quad 1 \leq i \leq n, \quad (7)$$

gdje je σ permutacijska realizacija elemenata grupe D_{2n} .

- 3 Grupa G djeluje na skup G sa

lijevom translacijom $g \cdot a = ga,$

desnom translacijom $g \cdot a = ag^{-1},$

konjugacijom $g \cdot a = gag^{-1}.$

Teorem

- 1 Ako grupa G djeluje na skup A , onda je preslikavanje $\varphi: G \rightarrow S_A$ dano s $\varphi(g) = \sigma_g$ homomorfizam.
- 2 Svaki homomorfizam $\varphi: G \rightarrow S_A$ inducira djelovanje grupe G na skup A .

Homomorfizam $\varphi: G \rightarrow S_A$ nazivamo **permutacijska reprezentacija** grupe G u simetričnu grupu S_A .

Definicija

Predpostavimo da grupa G djeluje na skup A i neka je $a \in A$. Podgrupu

$$G_a = \{g \in G \mid g \cdot a = a\}$$

nazivamo stabilizator elementa a u G . Skup

$$Ga = \{g \cdot a \mid g \in G\}$$

nazivamo orbita elementa a .

Teorem

- 1 Ako grupa G djeluje na skup A , onda je preslikavanje $\varphi: G \rightarrow S_A$ dano s $\varphi(g) = \sigma_g$ homomorfizam.
- 2 Svaki homomorfizam $\varphi: G \rightarrow S_A$ inducira djelovanje grupe G na skup A .

Homomorfizam $\varphi: G \rightarrow S_A$ nazivamo **permutacijska reprezentacija** grupe G u simetričnu grupu S_A .

Definicija

Predpostavimo da grupa G djeluje na skup A i neka je $a \in A$. Podgrupu

$$G_a = \{g \in G \mid g \cdot a = a\}$$

nazivamo stabilizator elementa a u G . Skup

$$Ga = \{g \cdot a \mid g \in G\}$$

nazivamo orbita elementa a .

Teorem

- 1 Ako grupa G djeluje na skup A , onda je preslikavanje $\varphi: G \rightarrow S_A$ dano s $\varphi(g) = \sigma_g$ homomorfizam.
- 2 Svaki homomorfizam $\varphi: G \rightarrow S_A$ inducira djelovanje grupe G na skup A .

Homomorfizam $\varphi: G \rightarrow S_A$ nazivamo **permutacijska reprezentacija** grupe G u simetričnu grupu S_A .

Definicija

Predpostavimo da grupa G djeluje na skup A i neka je $a \in A$. Podgrupu

$$G_a = \{g \in G \mid g \cdot a = a\}$$

nazivamo stabilizator elementa a u G . Skup

$$Ga = \{g \cdot a \mid g \in G\}$$

nazivamo orbita elementa a .

Primjer

Promotrimo djelovanje grupe $SO(2)$ na skup $\mathbb{R}^2$:

$$R_\theta \cdot (x, y) = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}.$$

- Orbita točke $(x, y) \neq (0, 0)$ je kružnica radijusa $\sqrt{x^2 + y^2}$.
- Stabilizator točke $(x, y) \neq (0, 0)$ je jedinična matrica.

Primjer

Promotrimo djelovanje grupe $SO(2)$ na skup $\mathbb{R}^2$:

$$R_\theta \cdot (x, y) = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}.$$

- Orbita točke $(x, y) \neq (0, 0)$ je kružnica radijusa $\sqrt{x^2 + y^2}$.
- Stabilizator točke $(x, y) \neq (0, 0)$ je jedinična matrica.

Teorem

Pretpostavimo da grupa G djeluje na skup A . Relacija na A definirana sa

$$a \sim b \Leftrightarrow a = g \cdot b \text{ za neki } g \in G$$

je relacija ekvivalencije. Stoga je A disjunktna unija

$$A = \bigcup_{a \in C} Ga$$

gdje skup C sadrži točno jedan element iz svake orbite Ga .

Definicija

Kažemo da grupa G djeluje tranzitivno na skup A ako za svaka dva elementa $a, b \in A$ postoji $g \in G$ takav da je $b = g \cdot a$.

Primjedba

Ako G djeluje tranzitivno na A , onda A ima samo jednu orbitu.

Teorem

Pretpostavimo da grupa G djeluje na skup A . Relacija na A definirana sa

$$a \sim b \Leftrightarrow a = g \cdot b \text{ za neki } g \in G$$

je relacija ekvivalencije. Stoga je A disjunktna unija

$$A = \bigcup_{a \in C} Ga$$

gdje skup C sadrži točno jedan element iz svake orbite Ga .

Definicija

Kažemo da grupa G djeluje tranzitivno na skup A ako za svaka dva elementa $a, b \in A$ postoji $g \in G$ takav da je $b = g \cdot a$.

Primjedba

Ako G djeluje tranzitivno na A , onda A ima samo jednu orbitu.

Teorem

Pretpostavimo da grupa G djeluje na skup A . Relacija na A definirana sa

$$a \sim b \Leftrightarrow a = g \cdot b \text{ za neki } g \in G$$

je relacija ekvivalencije. Stoga je A disjunktna unija

$$A = \bigcup_{a \in C} Ga$$

gdje skup C sadrži točno jedan element iz svake orbite Ga .

Definicija

Kažemo da grupa G djeluje tranzitivno na skup A ako za svaka dva elementa $a, b \in A$ postoji $g \in G$ takav da je $b = g \cdot a$.

Primjedba

Ako G djeluje tranzitivno na A , onda A ima samo jednu orbitu.

Veza između stabilizatora i orbite elementa

Teorem

Neka grupa G djeluje na skup A . Kardinalni broj orbite Ga jednak je indeksu stabilizatora G_a u G , tj.

$$|Ga| = [G : G_a]. \quad (8)$$

Ako je G konačna grupa, onda je

$$|Ga| = \frac{|G|}{|G_a|}.$$

Korolar

Neka je A konačni skup na kojeg djeluje grupa G . Tada je

$$|A| = \sum_{a \in C} [G : G_a]$$

gdje skup C sadrži točno jedan element iz svake orbite.

Veza između stabilizatora i orbite elementa

Teorem

Neka grupa G djeluje na skup A . Kardinalni broj orbite Ga jednak je indeksu stabilizatora G_a u G , tj.

$$|Ga| = [G : G_a]. \quad (8)$$

Ako je G konačna grupa, onda je

$$|Ga| = \frac{|G|}{|G_a|}.$$

Korolar

Neka je A konačni skup na kojeg djeluje grupa G . Tada je

$$|A| = \sum_{a \in C} [G : G_a]$$

gdje skup C sadrži točno jedan element iz svake orbite.

Veza između stabilizatora i orbite elementa

Teorem

Neka grupa G djeluje na skup A . Kardinalni broj orbite Ga jednak je indeksu stabilizatora G_a u G , tj.

$$|Ga| = [G : G_a]. \quad (8)$$

Ako je G konačna grupa, onda je

$$|Ga| = \frac{|G|}{|G_a|}.$$

Korolar

Neka je A konačni skup na kojeg djeluje grupa G . Tada je

$$|A| = \sum_{a \in C} [G : G_a]$$

gdje skup C sadrži točno jedan element iz svake orbite.

Primjena na djelovanje konjugacijom

Ako grupa G djeluje na sebe konjugacijom, $g \cdot a = gag^{-1}$, onda je

$$\begin{aligned} G_a &= \{g \in G \mid gag^{-1} = a\} = N(a) && \text{normalizator elementa } a, \\ Ga &= \{gag^{-1} \mid g \in G\} = C(a) && \text{klasa konjugacije elementa } a. \end{aligned}$$

Teorem (Jednadžba klase)

Neka je G konačna grupa i neka su $a_1, a_2, \dots, a_n$ predstavnici klasa konjugacije koje imaju više od jednog elementa. Tada je

$$|G| = |Z(G)| + \sum_{i=1}^n [G : N(a_i)].$$

Teorem

Ako je G grupa reda p^n , $n \geq 1$, gdje je p prosti broj, onda je centar grupe G netrivialan.

Primjena na djelovanje konjugacijom

Ako grupa G djeluje na sebe konjugacijom, $g \cdot a = gag^{-1}$, onda je

$$G_a = \{g \in G \mid gag^{-1} = a\} = N(a) \quad \text{normalizator elementa } a,$$

$$Ga = \{gag^{-1} \mid g \in G\} = C(a) \quad \text{klasa konjugacije elementa } a.$$

Teorem (Jednadžba klase)

Neka je G konačna grupa i neka su $a_1, a_2, \dots, a_n$ predstavnici klasa konjugacije koje imaju više od jednog elementa. Tada je

$$|G| = |Z(G)| + \sum_{i=1}^n [G : N(a_i)].$$

Teorem

Ako je G grupa reda p^n , $n \geq 1$, gdje je p prosti broj, onda je centar grupe G netrivialan.

Primjena na djelovanje konjugacijom

Ako grupa G djeluje na sebe konjugacijom, $g \cdot a = gag^{-1}$, onda je

$$\begin{aligned} G_a &= \{g \in G \mid gag^{-1} = a\} = N(a) && \text{normalizator elementa } a, \\ Ga &= \{gag^{-1} \mid g \in G\} = C(a) && \text{klasa konjugacije elementa } a. \end{aligned}$$

Teorem (Jednadžba klase)

Neka je G konačna grupa i neka su $a_1, a_2, \dots, a_n$ predstavnici klasa konjugacije koje imaju više od jednog elementa. Tada je

$$|G| = |Z(G)| + \sum_{i=1}^n [G : N(a_i)].$$

Teorem

Ako je G grupa reda p^n , $n \geq 1$, gdje je p prosti broj, onda je centar grupe G netrivialan.