

Algebarske strukture

prof.dr.sc. Saša Krešić-Jurić

PMF–Split

U ovom kolegiju ćemo proučavati sljedeće algebarske strukture:

- 1 Grupe
- 2 Prsteni
- 3 Ostale algebarske strukture: moduli, algebre, Liejeve algebre, Weylove algebre

Literatura

- 1 S. Krešić–Jurić, *Algebarske strukture*, skripta, <https://mapmf.pmfst.unist.hr/skresic/Algebra/Algebra.htm>
- 2 P.B. Bhattacharya, S.K. Jain, S.R. Nagapaul, *Basic Abstract Algebra*, treće izdanje, John Wiley and Sons, 2004.
- 3 D.A.R. Wallace, *Groups, Rings and Fields*, Springer, 1998.

U ovom kolegiju ćemo proučavati sljedeće algebarske strukture:

- 1 Grupe
- 2 Prsteni
- 3 Ostale algebarske strukture: moduli, algebre, Liejeve algebre, Weylove algebre

Literatura

- 1 S. Krešić–Jurić, *Algebarske strukture*, skripta, <https://mapmf.pmfst.unist.hr/skresic/Algebra/Algebra.htm>
- 2 P.B. Bhattacharya, S.K. Jain, S.R. Nagapaul, *Basic Abstract Algebra*, treće izdanje, John Wiley and Sons, 2004.
- 3 D.A.R. Wallace, *Groups, Rings and Fields*, Springer, 1998.

- Grupe su matematičke strukture koje imaju porijeklo u rješavanju algebarskih jednažbi, a danas imaju važnu ulogu u proučavanju simetrija u matematici, posebno u geometriji, i fizici.
- Prvi primjeri grupa su grupe permutacija, a prva formalna definicija grupe u modernom smislu se pojavila 1882.

Binarna operacija

Neka je G neprazan skup. Binarna operacija na skupu G je preslikavanje s kartezijevog umnoška $G \times G$ u G .

$$(a, b) \mapsto a \cdot b \quad \text{rezultat binarne operacije}$$

Rezultat binarne operacije pišemo kao $a \cdot b$ ili ab .

Primjeri

1 Zbrajanje cijelih brojeva

$$+: \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}, \quad (m, n) \mapsto m + n$$

2 Množenje matrica

$$\cdot: M(2, \mathbb{R}) \times M(2, \mathbb{R}) \rightarrow M(2, \mathbb{R}), \quad (A, B) \mapsto A \cdot B$$

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix} = \begin{bmatrix} aa' + bc' & ab' + bd' \\ ca' + dc' & cb' + dd' \end{bmatrix}$$

Binarna operacija

Neka je G neprazan skup. Binarna operacija na skupu G je preslikavanje s kartezijevog umnoška $G \times G$ u G .

$$(a, b) \mapsto a \cdot b \quad \text{rezultat binarne operacije}$$

Rezultat binarne operacije pišemo kao $a \cdot b$ ili ab .

Primjeri

1 Zbrajanje cijelih brojeva

$$+: \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}, \quad (m, n) \mapsto m + n$$

2 Množenje matrica

$$\cdot: M(2, \mathbb{R}) \times M(2, \mathbb{R}) \rightarrow M(2, \mathbb{R}), \quad (A, B) \mapsto A \cdot B$$

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix} = \begin{bmatrix} aa' + bc' & ab' + bd' \\ ca' + dc' & cb' + dd' \end{bmatrix}$$

Za binarnu operaciju na G kažemo da je

1 asocijativna ako je

$$(ab)c = a(bc) \quad \text{za sve } a, b, c \in G,$$

2 komutativna ako je

$$ab = ba \quad \text{za sve } a, b \in G.$$

■ Zbrajanje i množenje u $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ i $\mathbb{C}$ su asocijativne i komutativne operacije.

■ Vektorski umnožak u $\mathbb{R}^3$ nije ni asocijativan ni komutativan:

$$\vec{a} \times (\vec{b} \times \vec{c}) \neq (\vec{a} \times \vec{b}) \times \vec{c}, \quad \vec{a} \times \vec{b} = -\vec{b} \times \vec{a}.$$

Za binarnu operaciju na G kažemo da je

1 asocijativna ako je

$$(ab)c = a(bc) \quad \text{za sve } a, b, c \in G,$$

2 komutativna ako je

$$ab = ba \quad \text{za sve } a, b \in G.$$

■ Zbrajanje i množenje u $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ i $\mathbb{C}$ su asocijativne i komutativne operacije.

■ Vektorski umnožak u $\mathbb{R}^3$ nije ni asocijativan ni komutativan:

$$\vec{a} \times (\vec{b} \times \vec{c}) \neq (\vec{a} \times \vec{b}) \times \vec{c}, \quad \vec{a} \times \vec{b} = -\vec{b} \times \vec{a}.$$

Definicija

Neprazan skup G na kojem je definirana asocijativna binarna operacija se naziva polugrupa.

Primjer

Neka je S neprazni skup. Skup svih preslikavanja $f: S \rightarrow S$ je polugrupa s obzirom na kompoziciju funkcija.

Definicija (Grupa)

Neprazan skup G s binarnom operacijom $\cdot: G \times G \rightarrow G$ se naziva grupa ako vrijedi:

1 (asocijativnost)

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c \text{ za sve } a, b, c \in G,$$

2 (neutralni element)

$$\exists e \in G \text{ takav da je } a \cdot e = e \cdot a = a \quad \forall a \in G,$$

3 (inverzni element)

$$\forall a \in G \text{ postoji } b \in G \text{ takav da je } a \cdot b = b \cdot a = e.$$

Definicija

Neprazan skup G na kojem je definirana asocijativna binarna operacija se naziva polugrupa.

Primjer

Neka je S neprazni skup. Skup svih preslikavanja $f: S \rightarrow S$ je polugrupa s obzirom na kompoziciju funkcija.

Definicija (Grupa)

Neprazan skup G s binarnom operacijom $\cdot: G \times G \rightarrow G$ se naziva grupa ako vrijedi:

1 (asocijativnost)

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c \text{ za sve } a, b, c \in G,$$

2 (neutralni element)

$$\exists e \in G \text{ takav da je } a \cdot e = e \cdot a = a \quad \forall a \in G,$$

3 (inverzni element)

$$\forall a \in G \text{ postoji } b \in G \text{ takav da je } a \cdot b = b \cdot a = e.$$

Definicija

Neprazan skup G na kojem je definirana asocijativna binarna operacija se naziva polugrupa.

Primjer

Neka je S neprazni skup. Skup svih preslikavanja $f: S \rightarrow S$ je polugrupa s obzirom na kompoziciju funkcija.

Definicija (Grupa)

Neprazan skup G s binarnom operacijom $\cdot: G \times G \rightarrow G$ se naziva grupa ako vrijedi:

1 (asocijativnost)

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c \text{ za sve } a, b, c \in G,$$

2 (neutralni element)

$$\exists e \in G \text{ takav da je } a \cdot e = e \cdot a = a \quad \forall a \in G,$$

3 (inverzni element)

$$\forall a \in G \text{ postoji } b \in G \text{ takav da je } a \cdot b = b \cdot a = e.$$

Propozicija

Neka je G grupa.

- 1 Neutralni element $e \in G$ je jedinstven.
- 2 Svaki element iz G ima jedinstveni inverz.

Definicija

Kažemo da je G Abelova ili komutativna grupa ako vrijedi

$$ab = ba \quad \text{za sve } a, b \in G.$$

- Binarnu operaciju u Abelovoj grupi obično označavamo kao zbrajanje $+$.
- Neutralni element označavamo s 0 .
- Aditivni inverz elementa a označavamo s $-a$.

$$a + b = b + a, \quad a + 0 = 0 + a = a, \quad a + (-a) = -a + a = 0 \quad \forall a, b \in G.$$

Propozicija

Neka je G grupa.

- 1 Neutralni element $e \in G$ je jedinstven.
- 2 Svaki element iz G ima jedinstveni inverz.

Definicija

Kažemo da je G Abelova ili komutativna grupa ako vrijedi

$$ab = ba \quad \text{za sve} \quad a, b \in G.$$

- Binarnu operaciju u Abelovoj grupi obično označavamo kao zbrajanje $+$.
- Neutralni element označavamo s 0 .
- Aditivni inverz elementa a označavamo s $-a$.

$$a + b = b + a, \quad a + 0 = 0 + a = a, \quad a + (-a) = -a + a = 0 \quad \forall a, b \in G.$$

Definicija

Red grupe G , u oznaci $|G|$, je kardinalni broj skupa G . Ako je $|G| < \infty$, onda kažemo da je G konačna grupa; u protivnom kažemo da je G beskonačna grupa.

Primjeri grupa

- 1 Skupovi $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ i $\mathbb{C}$ su grupe s obzirom na standardno zbrajanje.
- 2 Skupovi $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ i $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ su grupe s obzirom na standardno množenje.
- 3 Neka je $n \in \mathbb{N}$. Na skupu $\mathbb{Z}$ uvedimo relaciju ekvivalencije

$$x \sim y \iff x - y = pn, \quad p \in \mathbb{Z}.$$

Klasa ekvivalencije elementa $x \in \mathbb{Z}$ je skup $\bar{x} = \{x + pn \mid p \in \mathbb{Z}\}$.

Definirajmo skup $\mathbb{Z}_n = \{\bar{x} \mid x \in \mathbb{Z}\}$ i uvedimo operaciju (zbrajanje mod n):

$$\bar{x} + \bar{y} = \overline{x + y}.$$

$(\mathbb{Z}_n, +)$ je grupa reda n s elementima

$$\mathbb{Z}_n = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}.$$

Definicija

Red grupe G , u oznaci $|G|$, je kardinalni broj skupa G . Ako je $|G| < \infty$, onda kažemo da je G konačna grupa; u protivnom kažemo da je G beskonačna grupa.

Primjeri grupa

- 1 Skupovi $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ i $\mathbb{C}$ su grupe s obzirom na standardno zbrajanje.
- 2 Skupovi $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ i $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ su grupe s obzirom na standardno množenje.
- 3 Neka je $n \in \mathbb{N}$. Na skupu $\mathbb{Z}$ uvedimo relaciju ekvivalencije

$$x \sim y \iff x - y = pn, \quad p \in \mathbb{Z}.$$

Klasa ekvivalencije elementa $x \in \mathbb{Z}$ je skup $\bar{x} = \{x + pn \mid p \in \mathbb{Z}\}$.

Definirajmo skup $\mathbb{Z}_n = \{\bar{x} \mid x \in \mathbb{Z}\}$ i uvedimo operaciju (zbrajanje mod n):

$$\bar{x} + \bar{y} = \overline{x + y}.$$

$(\mathbb{Z}_n, +)$ je grupa reda n s elementima

$$\mathbb{Z}_n = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}.$$

Definicija

Red grupe G , u oznaci $|G|$, je kardinalni broj skupa G . Ako je $|G| < \infty$, onda kažemo da je G konačna grupa; u protivnom kažemo da je G beskonačna grupa.

Primjeri grupa

- 1 Skupovi $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ i $\mathbb{C}$ su grupe s obzirom na standardno zbrajanje.
- 2 Skupovi $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ i $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ su grupe s obzirom na standardno množenje.
- 3 Neka je $n \in \mathbb{N}$. Na skupu $\mathbb{Z}$ uvedimo relaciju ekvivalencije

$$x \sim y \iff x - y = pn, \quad p \in \mathbb{Z}.$$

Klasa ekvivalencije elementa $x \in \mathbb{Z}$ je skup $\bar{x} = \{x + pn \mid p \in \mathbb{Z}\}$.

Definirajmo skup $\mathbb{Z}_n = \{\bar{x} \mid x \in \mathbb{Z}\}$ i uvedimo operaciju (zbrajanje mod n):

$$\bar{x} + \bar{y} = \overline{x + y}.$$

$(\mathbb{Z}_n, +)$ je grupa reda n s elementima

$$\mathbb{Z}_n = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}.$$

3 Opća linearna grupa

$$GL(n, \mathbb{R}) = \{A \in M(n, \mathbb{R}) \mid \det(A) \neq 0\}$$

je grupa s obzirom na matrično množenje.

4 Specijalna ortogonalna grupa ili grupa rotacija u ravni

$$SO(2) = \left\{ \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix} \mid \theta \in \mathbb{R} \right\}$$

je grupa s obzirom na matrično množenje jer je

$$\begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix} \begin{pmatrix} \cos \phi & -\sin \phi \\ \sin \phi & \cos \phi \end{pmatrix} = \begin{pmatrix} \cos(\theta + \phi) & -\sin(\theta + \phi) \\ \sin(\theta + \phi) & \cos(\theta + \phi) \end{pmatrix}$$

$$\begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix}^{-1} = \begin{pmatrix} \cos \theta & \sin \theta \\ -\sin \theta & \cos \theta \end{pmatrix} = \begin{pmatrix} \cos(-\theta) & -\sin(-\theta) \\ \sin(-\theta) & \cos(-\theta) \end{pmatrix}$$

3 Opća linearna grupa

$$GL(n, \mathbb{R}) = \{A \in M(n, \mathbb{R}) \mid \det(A) \neq 0\}$$

je grupa s ozbirom na matrično množenje.

4 Specijalna ortogonalna grupa ili grupa rotacija u ravni

$$SO(2) = \left\{ \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix} \mid \theta \in \mathbb{R} \right\}$$

je grupa s obzirom na matrično množenje jer je

$$\begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix} \begin{pmatrix} \cos \phi & -\sin \phi \\ \sin \phi & \cos \phi \end{pmatrix} = \begin{pmatrix} \cos(\theta + \phi) & -\sin(\theta + \phi) \\ \sin(\theta + \phi) & \cos(\theta + \phi) \end{pmatrix}$$

$$\begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix}^{-1} = \begin{pmatrix} \cos \theta & \sin \theta \\ -\sin \theta & \cos \theta \end{pmatrix} = \begin{pmatrix} \cos(-\theta) & -\sin(-\theta) \\ \sin(-\theta) & \cos(-\theta) \end{pmatrix}$$

3 Opća linearna grupa

$$GL(n, \mathbb{R}) = \{A \in M(n, \mathbb{R}) \mid \det(A) \neq 0\}$$

je grupa s ozbirom na matrično množenje.

4 Specijalna ortogonalna grupa ili grupa rotacija u ravni

$$SO(2) = \left\{ \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix} \mid \theta \in \mathbb{R} \right\}$$

je grupa s obzirom na matrično množenje jer je

$$\begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix} \begin{pmatrix} \cos \phi & -\sin \phi \\ \sin \phi & \cos \phi \end{pmatrix} = \begin{pmatrix} \cos(\theta + \phi) & -\sin(\theta + \phi) \\ \sin(\theta + \phi) & \cos(\theta + \phi) \end{pmatrix}$$

$$\begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix}^{-1} = \begin{pmatrix} \cos \theta & \sin \theta \\ -\sin \theta & \cos \theta \end{pmatrix} = \begin{pmatrix} \cos(-\theta) & -\sin(-\theta) \\ \sin(-\theta) & \cos(-\theta) \end{pmatrix}$$

5 Heisenbergova grupa je grupa matrica oblika

$$H = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}, \quad a, b, c \in \mathbb{R}.$$

Za umnožak i inverz matrica vrijedi

$$HH' = \begin{pmatrix} 1 & a' + a & b' + ac' + b \\ 0 & 1 & c' + c \\ 0 & 0 & 1 \end{pmatrix}, \quad H^{-1} = \begin{pmatrix} 1 & -a & -b + ac \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{pmatrix}.$$

Propozicija (Pravilo kraćenja slijeva i zdesna)

Neka je G grupa i neka su $a, x, y \in G$. Tada vrijedi

$$\mathbf{1} \quad a \cdot x = a \cdot y \quad \Rightarrow \quad x = y,$$

$$\mathbf{2} \quad x \cdot a = y \cdot a \quad \Rightarrow \quad x = y.$$

Jednadžbe

$$ax = b, \quad xa = b$$

u grupi G imaju jedinstvena rješenja $x = a^{-1}b$ i $x = ba^{-1}$.

Potencije u grupi G definiramo na standardan način:

$$a^n = \underbrace{a \cdot a \cdot \dots \cdot a}_{n \text{ puta}},$$

$$a^{-n} = (a^{-1})^n, \quad n \in \mathbb{N}.$$

Propozicija (Pravilo kraćenja slijeva i zdesna)

Neka je G grupa i neka su $a, x, y \in G$. Tada vrijedi

$$\mathbf{1} \quad a \cdot x = a \cdot y \quad \Rightarrow \quad x = y,$$

$$\mathbf{2} \quad x \cdot a = y \cdot a \quad \Rightarrow \quad x = y.$$

Jednadžbe

$$ax = b, \quad xa = b$$

u grupi G imaju jedinstvena rješenja $x = a^{-1}b$ i $x = ba^{-1}$.

Potencije u grupi G definiramo na standardan način:

$$a^n = \underbrace{a \cdot a \cdot \dots \cdot a}_{n \text{ puta}},$$

$$a^{-n} = (a^{-1})^n, \quad n \in \mathbb{N}.$$

Za aditivnu operaciju u Abelovoj grupi definiramo

$$na = \underbrace{a + a + \cdots + a}_{n \text{ puta}},$$

$$(-n)a = n(-a), \quad n \in \mathbb{N}.$$

Lako se provjeri da je

$$(ab)^{-1} = b^{-1}a^{-1}$$

i općenito

$$(a_1 a_2 \cdots a_n)^{-1} = a_n^{-1} a_{n-1}^{-1} \cdots a_1^{-1}.$$

Za aditivnu operaciju u Abelovoj grupi definiramo

$$na = \underbrace{a + a + \cdots + a}_{n \text{ puta}},$$

$$(-n)a = n(-a), \quad n \in \mathbb{N}.$$

Lako se provjeri da je

$$(ab)^{-1} = b^{-1}a^{-1}$$

i općenito

$$(a_1 a_2 \cdots a_n)^{-1} = a_n^{-1} a_{n-1}^{-1} \cdots a_1^{-1}.$$

Grupe manjeg reda se mogu prikazati pomoću Cayleve tablice ili tablice množenja.

Cayleva tablica

Neka je $G = \{a_1, a_2, \dots, a_n\}$ konačna grupa. Cayleva tablica grupe G je $n \times n$ tablica čiji element na mjestu (i, j) je umnožak $a_i a_j$.

Svojstva Cayleve tablice

- Ako je grupa komutativna, onda je tablica simetrična u odnosu na dijagonalu.
- Mjesta gdje se u tablici nalaze jedinice odgovaraju elementima koji su međusobno inverzni.
- Svaki redak ili stupac tablice sadrži točno jedan element iz G .

Primjer

Odredite Caylevu tablicu grupe $G = \{e, a, b\}$.

Uputa: pokažite da je $ab = e$ i $a^2 = b$, $b^2 = a$.

Grupe manjeg reda se mogu prikazati pomoću Cayleve tablice ili tablice množenja.

Cayleva tablica

Neka je $G = \{a_1, a_2, \dots, a_n\}$ konačna grupa. Cayleva tablica grupe G je $n \times n$ tablica čiji element na mjestu (i, j) je umnožak $a_i a_j$.

Svojstva Cayleve tablice

- Ako je grupa komutativna, onda je tablica simetrična u odnosu na dijagonalu.
- Mjesta gdje se u tablici nalaze jedinice odgovaraju elementima koji su međusobno inverzni.
- Svaki redak ili stupac tablice sadrži točno jedan element iz G .

Primjer

Odredite Caylevu tablicu grupe $G = \{e, a, b\}$.

Uputa: pokažite da je $ab = e$ i $a^2 = b$, $b^2 = a$.

Grupe manjeg reda se mogu prikazati pomoću Cayleve tablice ili tablice množenja.

Cayleva tablica

Neka je $G = \{a_1, a_2, \dots, a_n\}$ konačna grupa. Cayleva tablica grupe G je $n \times n$ tablica čiji element na mjestu (i, j) je umnožak $a_i a_j$.

Svojstva Cayleve tablice

- Ako je grupa komutativna, onda je tablica simetrična u odnosu na dijagonalu.
- Mjesta gdje se u tablici nalaze jedinice odgovaraju elementima koji su međusobno inverzni.
- Svaki redak ili stupac tablice sadrži točno jedan element iz G .

Primjer

Odredite Caylevu tablicu grupe $G = \{e, a, b\}$.

Uputa: pokažite da je $ab = e$ i $a^2 = b$, $b^2 = a$.

Homomorfizmi grupa

Naizgled različite grupe mogu imati istu strukturu. Grupe možemo uspoređivati pomoću preslikavanja koja množenje u domeni preslikavaju u množenje u kodomeni.

Definicija

Neka su G i H grupe. Preslikavanje $\phi: G \rightarrow H$ naziva se homomorfizam grupa ako vrijedi

$$\phi(xy) = \phi(x)\phi(y) \quad \text{za svaki } x, y \in G.$$

Podjela homomorfizama

Ako je preslikavanje $\phi: G \rightarrow H$

- surjekcija, onda kažemo da je ϕ **epimorfizam**,
- injekcija, onda kažemo da je ϕ **monomorfizam**,
- bijekcija, onda kažemo da je ϕ **izomorfizam**. Tada su G i H izomorfne grupe i pišemo $G \simeq H$.

Homomorfizmi grupa

Naizgled različite grupe mogu imati istu strukturu. Grupe možemo uspoređivati pomoću preslikavanja koja množenje u domeni preslikavaju u množenje u kodomeni.

Definicija

Neka su G i H grupe. Preslikavanje $\phi: G \rightarrow H$ naziva se homomorfizam grupa ako vrijedi

$$\phi(xy) = \phi(x)\phi(y) \quad \text{za svaki } x, y \in G.$$

Podjela homomorfizama

Ako je preslikavanje $\phi: G \rightarrow H$

- surjekcija, onda kažemo da je ϕ **epimorfizam**,
- injekcija, onda kažemo da je ϕ **monomorfizam**,
- bijekcija, onda kažemo da je ϕ **izomorfizam**. Tada su G i H izomorfne grupe i pišemo $G \simeq H$.

Homomorfizmi grupa

Naizgled različite grupe mogu imati istu strukturu. Grupe možemo uspoređivati pomoću preslikavanja koja množenje u domeni preslikavaju u množenje u kodomeni.

Definicija

Neka su G i H grupe. Preslikavanje $\phi: G \rightarrow H$ naziva se homomorfizam grupa ako vrijedi

$$\phi(xy) = \phi(x)\phi(y) \quad \text{za svaki } x, y \in G.$$

Podjela homomorfizama

Ako je preslikavanje $\phi: G \rightarrow H$

- surjekcija, onda kažemo da je ϕ **epimorfizam**,
- injekcija, onda kažemo da je ϕ **monomorfizam**,
- bijekcija, onda kažemo da je ϕ **izomorfizam**. Tada su G i H izomorfne grupe i pišemo $G \simeq H$.

Primjeri homomorfizama

1 Kompleksna konjugacija

$$\phi: \mathbb{C}^* \rightarrow \mathbb{C}^*, \quad \phi(z) = \bar{z}.$$

2 Eksponencijalna funkcija

$$\phi: \mathbb{R} \rightarrow \mathbb{R}^+, \quad \phi(x) = e^x.$$

3 Determinanta

$$\phi: GL(n, \mathbb{R}) \rightarrow \mathbb{R}^*, \quad \phi(A) = \det(A).$$

4 Unutarnji automorfizam ili konjugacija

$$C_a: G \rightarrow G, \quad C_a(x) = axa^{-1}, \quad a \in G.$$

Primjeri homomorfizama

1 Kompleksna konjugacija

$$\phi: \mathbb{C}^* \rightarrow \mathbb{C}^*, \quad \phi(z) = \bar{z}.$$

2 Eksponencijalna funkcija

$$\phi: \mathbb{R} \rightarrow \mathbb{R}^+, \quad \phi(x) = e^x.$$

3 Determinanta

$$\phi: GL(n, \mathbb{R}) \rightarrow \mathbb{R}^*, \quad \phi(A) = \det(A).$$

4 Unutarnji automorfizam ili konjugacija

$$C_a: G \rightarrow G, \quad C_a(x) = axa^{-1}, \quad a \in G.$$

Primjeri homomorfizama

1 Kompleksna konjugacija

$$\phi: \mathbb{C}^* \rightarrow \mathbb{C}^*, \quad \phi(z) = \bar{z}.$$

2 Eksponencijalna funkcija

$$\phi: \mathbb{R} \rightarrow \mathbb{R}^+, \quad \phi(x) = e^x.$$

3 Determinanta

$$\phi: GL(n, \mathbb{R}) \rightarrow \mathbb{R}^*, \quad \phi(A) = \det(A).$$

4 Unutarnji automorfizam ili konjugacija

$$C_a: G \rightarrow G, \quad C_a(x) = axa^{-1}, \quad a \in G.$$

Primjeri homomorfizama

1 Kompleksna konjugacija

$$\phi: \mathbb{C}^* \rightarrow \mathbb{C}^*, \quad \phi(z) = \bar{z}.$$

2 Eksponencijalna funkcija

$$\phi: \mathbb{R} \rightarrow \mathbb{R}^+, \quad \phi(x) = e^x.$$

3 Determinanta

$$\phi: GL(n, \mathbb{R}) \rightarrow \mathbb{R}^*, \quad \phi(A) = \det(A).$$

4 Unutarnji automorfizam ili konjugacija

$$C_a: G \rightarrow G, \quad C_a(x) = axa^{-1}, \quad a \in G.$$

Teorem

Neka su G i H grupe s pripadnim jedinicama $e \in G$ i $e' \in H$ i neka je $\phi: G \rightarrow H$ homomorfizam. Tada je

1 $\phi(e) = e',$

2 $\phi(x^{-1}) = \phi(x)^{-1}$ za svaki $x \in G$.

Definicija

Neka su G i H grupe. Jezgra homomorfizma $\phi: G \rightarrow H$ je skup

$$\ker(\phi) = \{x \in G \mid \phi(x) = e'\}.$$

Slika homomorfizma je skup

$$\text{Im}(\phi) = \{\phi(x) \mid x \in G\}.$$

Primjedba

Jezgra $\ker(\phi)$ je neprazan skup jer je $e \in \ker(\phi)$.

Teorem

Neka su G i H grupe s pripadnim jedinicama $e \in G$ i $e' \in H$ i neka je $\phi: G \rightarrow H$ homomorfizam. Tada je

1 $\phi(e) = e'$,

2 $\phi(x^{-1}) = \phi(x)^{-1}$ za svaki $x \in G$.

Definicija

Neka su G i H grupe. Jezgra homomorfizma $\phi: G \rightarrow H$ je skup

$$\ker(\phi) = \{x \in G \mid \phi(x) = e'\}.$$

Slika homomorfizma je skup

$$\text{Im}(\phi) = \{\phi(x) \mid x \in G\}.$$

Primjedba

Jezgra $\ker(\phi)$ je neprazan skup jer je $e \in \ker(\phi)$.

Teorem

Neka su G i H grupe s pripadnim jedinicama $e \in G$ i $e' \in H$ i neka je $\phi: G \rightarrow H$ homomorfizam. Tada je

1 $\phi(e) = e',$

2 $\phi(x^{-1}) = \phi(x)^{-1}$ za svaki $x \in G$.

Definicija

Neka su G i H grupe. Jezgra homomorfizma $\phi: G \rightarrow H$ je skup

$$\ker(\phi) = \{x \in G \mid \phi(x) = e'\}.$$

Slika homomorfizma je skup

$$\operatorname{Im}(\phi) = \{\phi(x) \mid x \in G\}.$$

Primjedba

Jezgra $\ker(\phi)$ je neprazan skup jer je $e \in \ker(\phi)$.

Veličina jezgre i slike su povezani s injektivnim i surjektivnim svojstvima izomorfizma.

Teorem

Homomorfizam grupa $\phi: G \rightarrow H$ je injektivan ako i samo ako je $\ker(\phi) = \{e\}$.

Teorem

- 1 Ako su $\phi_1: G \rightarrow H$ i $\phi_2: H \rightarrow K$ homomorfizmi, onda je kompozicija $\phi_2 \circ \phi_1: G \rightarrow K$ homomorfizam.
- 2 Ako je $\phi: G \rightarrow H$ izomorfizam, onda je inverzno preslikavanje $\phi^{-1}: H \rightarrow G$ izomorfizam.

Homomorfizam $\phi: G \rightarrow H$ je **izomorfizam** ako i samo ako je $\ker(\phi) = \{e\}$ i $\text{Im}(\phi) = H$.

Veličina jezgre i slike su povezani s injektivnim i surjektivnim svojstvima izomorfizma.

Teorem

Homomorfizam grupa $\phi: G \rightarrow H$ je injektivan ako i samo ako je $\ker(\phi) = \{e\}$.

Teorem

- 1 Ako su $\phi_1: G \rightarrow H$ i $\phi_2: H \rightarrow K$ homomorfizmi, onda je kompozicija $\phi_2 \circ \phi_1: G \rightarrow K$ homomorfizam.
- 2 Ako je $\phi: G \rightarrow H$ izomorfizam, onda je inverzno preslikavanje $\phi^{-1}: H \rightarrow G$ izomorfizam.

Homomorfizam $\phi: G \rightarrow H$ je izomorfizam ako i samo ako je $\ker(\phi) = \{e\}$ i $\text{Im}(\phi) = H$.

Veličina jezgre i slike su povezani s injektivnim i surjektivnim svojstvima izomorfizma.

Teorem

Homomorfizam grupa $\phi: G \rightarrow H$ je injektivan ako i samo ako je $\ker(\phi) = \{e\}$.

Teorem

- 1 Ako su $\phi_1: G \rightarrow H$ i $\phi_2: H \rightarrow K$ homomorfizmi, onda je kompozicija $\phi_2 \circ \phi_1: G \rightarrow K$ homomorfizam.
- 2 Ako je $\phi: G \rightarrow H$ izomorfizam, onda je inverzno preslikavanje $\phi^{-1}: H \rightarrow G$ izomorfizam.

Homomorfizam $\phi: G \rightarrow H$ je **izomorfizam** ako i samo ako je $\ker(\phi) = \{e\}$ i $\text{Im}(\phi) = H$.

Podgrupe

Struktura neke grupe ovisi o međusobnom odnosu njezinih podgrupa.

Definicija

Neka je G grupa. Neprazan podskup $H \subseteq G$ naziva se podgrupa od G , u oznaci $H \leq G$, ako je H grupa s obzirom na množenje u G . Ako je H pravi podskup od G , onda pišemo $H < G$.

Svaka podgrupa je zatvorena na množenje i inverziju te sadrži neutralni element:

$$a, b \in H \Rightarrow ab \in H,$$

$$a \in H \Rightarrow a^{-1} \in H.$$

Teorem (Kriterij za podgrupu)

Neka je G grupa. Podskup $H \subseteq G$ je podgrupa od G ako i samo ako

$$a, b \in H \Rightarrow ab^{-1} \in H.$$

Podgrupe

Struktura neke grupe ovisi o međusobnom odnosu njezinih podgrupa.

Definicija

Neka je G grupa. Neprazan podskup $H \subseteq G$ naziva se podgrupa od G , u oznaci $H \leq G$, ako je H grupa s obzirom na množenje u G . Ako je H pravi podskup od G , onda pišemo $H < G$.

Svaka podgrupa je zatvorena na množenje i inverziju te sadrži neutralni element:

$$a, b \in H \Rightarrow ab \in H,$$

$$a \in H \Rightarrow a^{-1} \in H.$$

Teorem (Kriterij za podgrupu)

Neka je G grupa. Podskup $H \subseteq G$ je podgrupa od G ako i samo ako

$$a, b \in H \Rightarrow ab^{-1} \in H.$$

Podgrupe

Struktura neke grupe ovisi o međusobnom odnosu njezinih podgrupa.

Definicija

Neka je G grupa. Neprazan podskup $H \subseteq G$ naziva se podgrupa od G , u oznaci $H \leq G$, ako je H grupa s obzirom na množenje u G . Ako je H pravi podskup od G , onda pišemo $H < G$.

Svaka podgrupa je zatvorena na množenje i inverziju te sadrži neutralni element:

$$a, b \in H \Rightarrow ab \in H,$$

$$a \in H \Rightarrow a^{-1} \in H.$$

Teorem (Kriterij za podgrupu)

Neka je G grupa. Podskup $H \subseteq G$ je podgrupa od G ako i samo ako

$$a, b \in H \Rightarrow ab^{-1} \in H.$$

Primjeri podgrupa

1 Svaka grupa G ima trivijalne podgrupe $\{e\}$ i G .

2 Specijalna linearna grupa

$$SL(n, \mathbb{R}) = \left\{ A \in GL(n, \mathbb{R}) \mid \det(A) = 1 \right\}$$

je podgrupa opće linearne grupe $GL(n, \mathbb{R})$.

3 Skup matrica

$$H = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \right\}$$

je podgrupa grupe

$$G = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a, b \in \mathbb{R}, a^2 + b^2 \neq 0 \right\}.$$

4 Unitarna grupa

$$U(1) = \{e^{i\theta} \mid \theta \in \mathbb{R}\}$$

je podgrupa multiplikativne grupe $(\mathbb{C}^*, \cdot)$.

Propozicija

Neka su H_1 i H_2 podgrupe grupe G .

- 1 $H_1 \cap H_2$ je podgrupa od G .
- 2 $H_1 \cup H_2$ je podgrupa od G ako i samo ako je $H_1 \subseteq H_2$ ili $H_2 \subseteq H_1$.

Teorem

Neka je $\phi: G \rightarrow H$ homomorfizam grupa. Jezgra homomorfizma $\ker(\phi)$ je podgrupa od G , a slika homomorfizma $\text{Im}(\phi)$ je podgrupa od H .

Definicija

Centar grupe G je skup

$$Z(G) = \{g \in G \mid ga = ag \quad \forall a \in G\}.$$

Primijetimo:

G je Abelova grupa ako i samo ako je $Z(G) = G$

Propozicija

Neka su H_1 i H_2 podgrupe grupe G .

- 1 $H_1 \cap H_2$ je podgrupa od G .
- 2 $H_1 \cup H_2$ je podgrupa od G ako i samo ako je $H_1 \subseteq H_2$ ili $H_2 \subseteq H_1$.

Teorem

Neka je $\phi: G \rightarrow H$ homomorfizam grupa. Jezgra homomorfizma $\ker(\phi)$ je podgrupa od G , a slika homomorfizma $\text{Im}(\phi)$ je podgrupa od H .

Definicija

Centar grupe G je skup

$$Z(G) = \{g \in G \mid ga = ag \quad \forall a \in G\}.$$

Primijetimo:

G je Abelova grupa ako i samo ako je $Z(G) = G$

Propozicija

Neka su H_1 i H_2 podgrupe grupe G .

- 1 $H_1 \cap H_2$ je podgrupa od G .
- 2 $H_1 \cup H_2$ je podgrupa od G ako i samo ako je $H_1 \subseteq H_2$ ili $H_2 \subseteq H_1$.

Teorem

Neka je $\phi: G \rightarrow H$ homomorfizam grupa. Jezgra homomorfizma $\ker(\phi)$ je podgrupa od G , a slika homomorfizma $\text{Im}(\phi)$ je podgrupa od H .

Definicija

Centar grupe G je skup

$$Z(G) = \{g \in G \mid ga = ag \quad \forall a \in G\}.$$

Primijetimo:

G je Abelova grupa ako i samo ako je $Z(G) = G$

Lema

Centar grupe $Z(G)$ je podgrupa od G .

Pojam centra grupe možemo poopćiti na centralizator proizvoljnog podskupa $A \subseteq G$.

Definicija

Neka je G grupa. Centralizator podskupa $A \subseteq G$ je skup

$$C_G(A) = \{g \in G \mid gag^{-1} = a \ \forall a \in A\}.$$

Kada je $A = \{a\}$ jednočlani skup, pišemo $C_G(a)$.

$C_G(A)$ je podgrupa od G za svaki podskup $A \subseteq G$.

Lema

Centar grupe $Z(G)$ je podgrupa od G .

Pojam centra grupe možemo poopćiti na centralizator proizvoljnog podskupa $A \subseteq G$.

Definicija

Neka je G grupa. Centralizator podskupa $A \subseteq G$ je skup

$$C_G(A) = \{g \in G \mid gag^{-1} = a \ \forall a \in A\}.$$

Kada je $A = \{a\}$ jednočlani skup, pišemo $C_G(a)$.

$C_G(A)$ je podgrupa od G za svaki podskup $A \subseteq G$.

Susjedne klase

U strukturi grupa važnu ulogu imaju particije grupe pridružene njezinim podgrupama.

- Za zadanu podgrupu $H \subseteq G$ definirajmo relaciju ekvivalencije na G sa

$$a \sim b \Leftrightarrow a^{-1}b \in H.$$

Klasa ekvivalencije: $\bar{a} = \{ah \mid h \in H\}$.

- Slično, na G možemo definirati relaciju ekvivalencije sa

$$a \sim b \Leftrightarrow ab^{-1} \in H.$$

Klasa ekvivalencije: $\bar{a} = \{ha \mid h \in H\}$.

Definicija

Neka je H podgrupa grupe G i neka je $a \in G$. **Lijeva susjedna klasa** podgrupe H je skup

$$aH = \{ah \mid h \in H\}.$$

Desna susjedna klasa podgrupe H je skup

$$Ha = \{ha \mid h \in H\}.$$

Susjedne klase

U strukturi grupa važnu ulogu imaju particije grupe pridružene njezinim podgrupama.

- Za zadanu podgrupu $H \subseteq G$ definirajmo relaciju ekvivalencije na G sa

$$a \sim b \Leftrightarrow a^{-1}b \in H.$$

Klasa ekvivalencije: $\bar{a} = \{ah \mid h \in H\}$.

- Slično, na G možemo definirati relaciju ekvivalencije sa

$$a \sim b \Leftrightarrow ab^{-1} \in H.$$

Klasa ekvivalencije: $\bar{a} = \{ha \mid h \in H\}$.

Definicija

Neka je H podgrupa grupe G i neka je $a \in G$. **Lijeva susjedna klasa** podgrupe H je skup

$$aH = \{ah \mid h \in H\}.$$

Desna susjedna klasa podgrupe H je skup

$$Ha = \{ha \mid h \in H\}.$$

Susjedne klase

U strukturi grupa važnu ulogu imaju particije grupe pridružene njezinim podgrupama.

- Za zadanu podgrupu $H \subseteq G$ definirajmo relaciju ekvivalencije na G sa

$$a \sim b \Leftrightarrow a^{-1}b \in H.$$

Klasa ekvivalencije: $\bar{a} = \{ah \mid h \in H\}$.

- Slično, na G možemo definirati relaciju ekvivalencije sa

$$a \sim b \Leftrightarrow ab^{-1} \in H.$$

Klasa ekvivalencije: $\bar{a} = \{ha \mid h \in H\}$.

Definicija

Neka je H podgrupa grupe G i neka je $a \in G$. **Lijeva susjedna klasa** podgrupe H je skup

$$aH = \{ah \mid h \in H\}.$$

Desna susjedna klasa podgrupe H je skup

$$Ha = \{ha \mid h \in H\}.$$

Susjedne klase

U strukturi grupa važnu ulogu imaju particije grupe pridružene njezinim podgrupama.

- Za zadanu podgrupu $H \subseteq G$ definirajmo relaciju ekvivalencije na G sa

$$a \sim b \Leftrightarrow a^{-1}b \in H.$$

Klasa ekvivalencije: $\bar{a} = \{ah \mid h \in H\}$.

- Slično, na G možemo definirati relaciju ekvivalencije sa

$$a \sim b \Leftrightarrow ab^{-1} \in H.$$

Klasa ekvivalencije: $\bar{a} = \{ha \mid h \in H\}$.

Definicija

Neka je H podgrupa grupe G i neka je $a \in G$. **Lijeva susjedna klasa** podgrupe H je skup

$$aH = \{ah \mid h \in H\}.$$

Desna susjedna klasa podgrupe H je skup

$$Ha = \{ha \mid h \in H\}.$$

Uvedimo oznake:

$$\begin{aligned} G/H &= \{aH \mid a \in G\} && \text{skup svih lijevih susjednih klasa podgrupe } H, \\ H \backslash G &= \{Ha \mid a \in G\} && \text{skup svih desnih susjednih klasa podgrupe } H. \end{aligned}$$

Iz definicije susjednih klasa slijedi:

$$aH = bH \quad \Leftrightarrow \quad a^{-1}b \in H,$$

$$Ha = Hb \quad \Leftrightarrow \quad ab^{-1} \in H.$$

Propozicija

Za susjedne klase podgrupe $H \subseteq G$ vrijedi

1

$$|aH| = |Ha| = |H|,$$

2

$$|G/H| = |H \backslash G|.$$

Uvedimo oznake:

$$\begin{aligned} G/H &= \{aH \mid a \in G\} && \text{skup svih lijevih susjednih klasa podgrupe } H, \\ H \setminus G &= \{Ha \mid a \in G\} && \text{skup svih desnih susjednih klasa podgrupe } H. \end{aligned}$$

Iz definicije susjednih klasa slijedi:

$$aH = bH \quad \Leftrightarrow \quad a^{-1}b \in H,$$

$$Ha = Hb \quad \Leftrightarrow \quad ab^{-1} \in H.$$

Propozicija

Za susjedne klase podgrupe $H \subseteq G$ vrijedi

1

$$|aH| = |Ha| = |H|,$$

2

$$|G/H| = |H \setminus G|.$$

Uvedimo oznake:

$$\begin{aligned} G/H &= \{aH \mid a \in G\} && \text{skup svih lijevih susjednih klasa podgrupe } H, \\ H \backslash G &= \{Ha \mid a \in G\} && \text{skup svih desnih susjednih klasa podgrupe } H. \end{aligned}$$

Iz definicije susjednih klasa slijedi:

$$aH = bH \quad \Leftrightarrow \quad a^{-1}b \in H,$$

$$Ha = Hb \quad \Leftrightarrow \quad ab^{-1} \in H.$$

Propozicija

Za susjedne klase podgrupe $H \subseteq G$ vrijedi

1

$$|aH| = |Ha| = |H|,$$

2

$$|G/H| = |H \backslash G|.$$

Definicija

Neka je H podgrupa grupe G . Kardinalni broj skupa G/H ili $H \setminus G$ naziva se **indeks podgrupe** H u G i označava sa $[G : H]$.

$[G : H]$ je broj lijevih (desnih) susjednih klasa podgrupe H koji tvore particiju grupe G .

- Koliki može biti indeks podgrupe?

Promotrimo trivijalne podgrupe $H = \{e\}$ i $H = G$.

Lagrangeov teorem

Neka je G konačna grupa i neka je H podgrupa od G . Tada je

$$|G| = [G : H] |H|.$$

Definicija

Neka je H podgrupa grupe G . Kardinalni broj skupa G/H ili $H \backslash G$ naziva se **indeks podgrupe** H u G i označava sa $[G : H]$.

$[G : H]$ je broj lijevih (desnih) susjednih klasa podgrupe H koji tvore particiju grupe G .

- Koliki može biti indeks podgrupe?

Promotrimo trivijalne podgrupe $H = \{e\}$ i $H = G$.

Lagrangeov teorem

Neka je G konačna grupa i neka je H podgrupa od G . Tada je

$$|G| = [G : H] |H|.$$

Definicija

Neka je H podgrupa grupe G . Kardinalni broj skupa G/H ili $H \backslash G$ naziva se **indeks podgrupe** H u G i označava sa $[G : H]$.

$[G : H]$ je broj lijevih (desnih) susjednih klasa podgrupe H koji tvore particiju grupe G .

- Koliki može biti indeks podgrupe?

Promotrimo trivijalne podgrupe $H = \{e\}$ i $H = G$.

Lagrangeov teorem

Neka je G konačna grupa i neka je H podgrupa od G . Tada je

$$|G| = [G : H] |H|.$$

Posljedica Lagraneevog teorema:

red podgrupe dijeli red grupe

i vrijedi

$$|H| = \frac{|G|}{[G : H]}.$$

Korolar

Ako je $|G| = p$ gdje je p prosti broj, onda G ima samo trivijalne podgrupe $H = \{e\}$ i $H = G$.

Posljedica Lagranegovog teorema:

red podgrupe dijeli red grupe

i vrijedi

$$|H| = \frac{|G|}{[G : H]}.$$

Korolar

Ako je $|G| = p$ gdje je p prosti broj, onda G ima samo trivijalne podgrupe $H = \{e\}$ i $H = G$.

Normalne podgrupe

U teoriji grupa posebnu ulogu imaju podgrupe grupe G za koje su lijeve i desne susjedne klase jednake. Takve grupe nazivamo normaln podgrupe.

Definicija

Neka je G grupa. Kažemo da je N **normalna podgrupa** od G ako je

$$xNx^{-1} \subseteq N \quad \text{za svaki } x \in G.$$

Normalnu podgrupu označavamo sa $N \triangleleft G$.

- Trivijalne normalne podgrupe: $\{e\}$ i G .
- Ako je G Abelova grupa, onda je svaka podgrupa od G normalna.

Normalne podgrupe

U teoriji grupa posebnu ulogu imaju podgrupe grupe G za koje su lijeve i desne susjedne klase jednake. Takve grupe nazivamo normaln podgrupe.

Definicija

Neka je G grupa. Kažemo da je N normalna podgrupa od G ako je

$$xNx^{-1} \subseteq N \quad \text{za svaki } x \in G.$$

Normalnu podgrupu označavamo sa $N \triangleleft G$.

- Trivijalne normalne podgrupe: $\{e\}$ i G .
- Ako je G Abelova grupa, onda je svaka podgrupa od G normalna.

Normalne podgrupe

U teoriji grupa posebnu ulogu imaju podgrupe grupe G za koje su lijeve i desne susjedne klase jednake. Takve grupe nazivamo normaln podgrupe.

Definicija

Neka je G grupa. Kažemo da je N **normalna podgrupa** od G ako je

$$xNx^{-1} \subseteq N \quad \text{za svaki } x \in G.$$

Normalnu podgrupu označavamo sa $N \triangleleft G$.

- Trivijalne normalne podgrupe: $\{e\}$ i G .
- Ako je G Abelova grupa, onda je svaka podgrupa od G normalna.

Normalne podgrupe su karakterizirane sljedećim svojstvima.

Teorem

Neka je N podgrupa grupe G . Tada su sljedeće tvrdnje ekvivalentne:

- 1 $N \triangleleft G$,
- 2 $xN = Nx$ za svaki $x \in G$,
- 3 $xNx^{-1} = N$ za svaki $x \in G$.

Primjeri normalnih podgrupa

- 1 $Z(G)$ je normalna podgrupa od G .
- 2 Jezgra homomorfizma $\varphi: G \rightarrow H$ je normalna podgrupa od G .
- 3 $SL(n, \mathbb{R})$ je normalna podgrupa grupe $GL(n, \mathbb{R})$.

Propozicija

Ako je H podgrupa grupe G takva da je $[G : H] = 2$, onda je $H \triangleleft G$.

Normalne podgrupe su karakterizirane sljedećim svojstvima.

Teorem

Neka je N podgrupa grupe G . Tada su sljedeće tvrdnje ekvivalentne:

- 1 $N \triangleleft G$,
- 2 $xN = Nx$ za svaki $x \in G$,
- 3 $xNx^{-1} = N$ za svaki $x \in G$.

Primjeri normalnih podgrupa

- 1 $Z(G)$ je normalna podgrupa od G .
- 2 Jezgra homomorfizma $\varphi: G \rightarrow H$ je normalna podgrupa od G .
- 3 $SL(n, \mathbb{R})$ je normalna podgrupa grupe $GL(n, \mathbb{R})$.

Propozicija

Ako je H podgrupa grupe G takva da je $[G : H] = 2$, onda je $H \triangleleft G$.

Normalne podgrupe su karakterizirane sljedećim svojstvima.

Teorem

Neka je N podgrupa grupe G . Tada su sljedeće tvrdnje ekvivalentne:

- 1 $N \triangleleft G$,
- 2 $xN = Nx$ za svaki $x \in G$,
- 3 $xNx^{-1} = N$ za svaki $x \in G$.

Primjeri normalnih podgrupa

- 1 $Z(G)$ je normalna podgrupa od G .
- 2 Jezgra homomorfizma $\varphi: G \rightarrow H$ je normalna podgrupa od G .
- 3 $SL(n, \mathbb{R})$ je normalna podgrupa grupe $GL(n, \mathbb{R})$.

Propozicija

Ako je H podgrupa grupe G takva da je $[G : H] = 2$, onda je $H \triangleleft G$.

Definicija

Neka su A i B podskupovi grupe G . Skup AB definiramo sa

$$AB = \{ab \mid a \in A, b \in B\}$$

Neka svojstva normalnih podgrupa.

Teorem

Neka je G grupa.

- 1 Ako je $H < G$ i $N \triangleleft G$, onda je $HN = NH$ podgrupa od G .
- 2 Ako su N i M normalne podgrupe od G , onda je NM normalna podgrupa od G .

Definicija

Neka su A i B podskupovi grupe G . Skup AB definiramo sa

$$AB = \{ab \mid a \in A, b \in B\}$$

Neka svojstva normalnih podgrupa.

Teorem

Neka je G grupa.

- 1 Ako je $H < G$ i $N \triangleleft G$, onda je $HN = NH$ podgrupa od G .
- 2 Ako su N i M normalne podgrupe od G , onda je NM normalna podgrupa od G .

Kvocijentna grupa

Ako je N normalna podgrupa od G , onda na skupu susjednih klasa podgrupe N možemo definirati binarnu operaciju sa

$$(xN)(yN) = (xy)N.$$

Time dobivamo strukturu grupe na skupu G/N .

Teorem

Neka je N normalna podgrupa grupe G . Tada je G/N grupa u odnosu na množenje definirano s

$$(xN)(yN) = (xy)N.$$

Preslikavanje $\pi: G \rightarrow G/N$ definiramo sa

$$\pi(x) = xN$$

je epimorfizam i $\ker(\pi) = N$.

Ako je N normalna podgrupa od G , onda na skupu susjednih klasa podgrupe N možemo definirati binarnu operaciju sa

$$(xN)(yN) = (xy)N.$$

Time dobivamo strukturu grupe na skupu G/N .

Teorem

Neka je N normalna podgrupa grupe G . Tada je G/N grupa u odnosu na množenje definirano s

$$(xN)(yN) = (xy)N.$$

Preslikavanje $\pi: G \rightarrow G/N$ definiramo sa

$$\pi(x) = xN$$

je epimorfizam i $\ker(\pi) = N$.

Ako je N normalna podgrupa od G , onda na skupu susjednih klasa podgrupe N možemo definirati binarnu operaciju sa

$$(xN)(yN) = (xy)N.$$

Time dobivamo strukturu grupe na skupu G/N .

Teorem

Neka je N normalna podgrupa grupe G . Tada je G/N grupa u odnosu na množenje definirano s

$$(xN)(yN) = (xy)N.$$

Preslikavanje $\pi: G \rightarrow G/N$ definiramo sa

$$\pi(x) = xN$$

je epimorfizam i $\ker(\pi) = N$.

Definicija

Neka je N normalna podgrupa grupe G . Grupa G/N naziva se **kvocijentna grupa**, a homomorfizam

$$\pi: G \rightarrow G/N, \quad \pi(x) = xN,$$

naziva se kanonski homomorfizam ili projekcija sa G na G/N .

- Jedinica u grupi G/N : $eN = N$.
- Inverzni element: $(xN)^{-1} = x^{-1}N$.

Broj elemenata u kvocijentoj grupi

Neka je G konačna grupa. Iz Lagrangeovog teorema odmah slijedi da je red kvocijentne grupe dan sa

$$|G/N| = [G : N] = \frac{|G|}{|N|}.$$

Definicija

Neka je N normalna podgrupa grupe G . Grupa G/N naziva se **kvocijentna grupa**, a homomorfizam

$$\pi: G \rightarrow G/N, \quad \pi(x) = xN,$$

naziva se kanonski homomorfizam ili projekcija sa G na G/N .

- Jedinica u grupi G/N : $eN = N$.
- Inverzni element: $(xN)^{-1} = x^{-1}N$.

Broj elemenata u kvocijentoj grupi

Neka je G konačna grupa. Iz Lagrangeovog teorema odmah slijedi da je red kvocijentne grupe dan sa

$$|G/N| = [G : N] = \frac{|G|}{|N|}.$$

Teoremi o izomorfizmima

U teoriji grupa važnu ulogu imaju tri teorema o izomorfizmima kvocijentnih grupa.

Prvi teorem o izomorfizmu

Neka je $\phi: G \rightarrow H$ homomorfizam grupa. Tada je

$$G/\ker(\phi) \simeq \operatorname{Im}(\phi).$$

Posebno, ako je ϕ surjekcija, tada je

$$G/\ker(\phi) \simeq H.$$

Primjedba

Ako su G i H konačne grupe i $\phi: G \rightarrow H$ je epimorfizam, onda je

$$|H| = |G/\ker(\phi)| = [G : \ker(\phi)] = \frac{|G|}{|\ker(\phi)|} \Rightarrow |H| \text{ dijeli } |G|.$$

Teoremi o izomorfizmima

U teoriji grupa važnu ulogu imaju tri teorema o izomorfizmima kvocijentnih grupa.

Prvi teorem o izomorfizmu

Neka je $\phi: G \rightarrow H$ homomorfizam grupa. Tada je

$$G/\ker(\phi) \simeq \text{Im}(\phi).$$

Posebno, ako je ϕ surjekcija, tada je

$$G/\ker(\phi) \simeq H.$$

Primjedba

Ako su G i H konačne grupe i $\phi: G \rightarrow H$ je epimorfizam, onda je

$$|H| = |G/\ker(\phi)| = [G : \ker(\phi)] = \frac{|G|}{|\ker(\phi)|} \Rightarrow |H| \text{ dijeli } |G|.$$

Teoremi o izomorfizmima

U teoriji grupa važnu ulogu imaju tri teorema o izomorfizmima kvocijentnih grupa.

Prvi teorem o izomorfizmu

Neka je $\phi: G \rightarrow H$ homomorfizam grupa. Tada je

$$G/\ker(\phi) \simeq \text{Im}(\phi).$$

Posebno, ako je ϕ surjekcija, tada je

$$G/\ker(\phi) \simeq H.$$

Primjedba

Ako su G i H konačne grupe i $\phi: G \rightarrow H$ je epimorfizam, onda je

$$|H| = |G/\ker(\phi)| = [G : \ker(\phi)] = \frac{|G|}{|\ker(\phi)|} \Rightarrow |H| \text{ dijeli } |G|.$$

Primjene I. teorema o izomorfizmu

Strukturu kvocijente grupe često određujemo primjenom prvog teorema o izomorfizmu.

1 $GL(n, \mathbb{R})/SL(n, \mathbb{R}) \simeq \mathbb{R}^*.$

Primijetimo da je $GL(n, \mathbb{R})/SL(n, \mathbb{R})$ Abelova grupa iako $GL(n, \mathbb{R})$ i $SL(n, \mathbb{R})$ nisu Abelove.

2 $\mathbb{R}^*/\{-1, 1\} \simeq \mathbb{R}^+.$

3 $\mathbb{R}/\mathbb{Z} \simeq U(1).$

4 $G/Z(G) \simeq \text{In}(G)$ gdje je $\text{In}(G)$ grupa unutarnjih automorfizama od G ,

$$\text{Inn}(G) = \{I_g \mid g \in G\}, \quad I_g(x) = gxg^{-1}.$$

Primjene I. teorema o izomorfizmu

Strukturu kvocijente grupe često određujemo primjenom prvog teorema o izomorfizmu.

1 $GL(n, \mathbb{R})/SL(n, \mathbb{R}) \simeq \mathbb{R}^*.$

Primijetimo da je $GL(n, \mathbb{R})/SL(n, \mathbb{R})$ Abelova grupa iako $GL(n, \mathbb{R})$ i $SL(n, \mathbb{R})$ nisu Abelove.

2 $\mathbb{R}^*/\{-1, 1\} \simeq \mathbb{R}^+.$

3 $\mathbb{R}/\mathbb{Z} \simeq U(1).$

4 $G/Z(G) \simeq \text{In}(G)$ gdje je $\text{In}(G)$ grupa unutarnjih automorfizama od G ,

$$\text{Inn}(G) = \{I_g \mid g \in G\}, \quad I_g(x) = gxg^{-1}.$$

Primjene I. teorema o izomorfizmu

Strukturu kvocijente grupe često određujemo primjenom prvog teorema o izomorfizmu.

1 $GL(n, \mathbb{R})/SL(n, \mathbb{R}) \simeq \mathbb{R}^*.$

Primijetimo da je $GL(n, \mathbb{R})/SL(n, \mathbb{R})$ Abelova grupa iako $GL(n, \mathbb{R})$ i $SL(n, \mathbb{R})$ nisu Abelove.

2 $\mathbb{R}^*/\{-1, 1\} \simeq \mathbb{R}^+.$

3 $\mathbb{R}/\mathbb{Z} \simeq U(1).$

4 $G/Z(G) \simeq \text{In}(G)$ gdje je $\text{In}(G)$ grupa unutarnjih automorfizama od G ,

$$\text{Inn}(G) = \{I_g \mid g \in G\}, \quad I_g(x) = gxg^{-1}.$$

Drugi teorem o izomorfizmu

Neka je G grupa koja sadrži podgrupe H i N i neka je $N \triangleleft G$. Tada je

$$H/(H \cap N) \simeq HN/N.$$

Treći teorem o izomorfizmu poznati je i kao teorem o dvostrukom kvocijentu.

Treći teorem o izomorfizmu

Neka su H i K normalne podgrupe grupe G i neka je $K \subseteq H$. Tada je

$$(G/K)/(H/K) \simeq G/H.$$

Drugi teorem o izomorfizmu

Neka je G grupa koja sadrži podgrupe H i N i neka je $N \triangleleft G$. Tada je

$$H/(H \cap N) \simeq HN/N.$$

Treći teorem o izomorfizmu poznati je i kao teorem o dvostrukom kvocijentu.

Treći teorem o izomorfizmu

Neka su H i K normalne podgrupe grupe G i neka je $K \subseteq H$. Tada je

$$(G/K)/(H/K) \simeq G/H.$$