Grupe

Definicija (binarna operacija)
Binarna operacija $*$ na skupu S je preslikavanje sa $S \times S$ u S. Za svako $(a,b) \in S \times S$, element $*((a,b))$ iz S ćemo označavati sa $a * b$.

Definicija (zatvorenost u odnosu na $*$)
Neka je $*$ binarna operacija na S i neka je H podskup od S. Podskup H je zatvoren u odnosu na $*$ ako za svako $a, b \in H$ također imamo da $a * b \in H$.

(#) Pokazati da je podskup $GL_n(\mathbb{R})$ skupa $Mat_{n\times n}(\mathbb{R})$ koji se sastoji od svih $n\times n$ invertibilnih matrica zatvoren u odnosu na matrično množenje.

Rj.

$$GL_n(\mathbb{R}) = \{ A \in Mat_{n\times n}(\mathbb{R}) \mid \exists A^{-1} \text{ t.d. } AA^{-1} = I \}$$

Izaberimo dvije proizvoljne matrice $A, B \in GL_n(\mathbb{R})$ i pokažimo da $AB \in GL_n(\mathbb{R})$ tj. da $\exists (AB)^{-1}$.

$A \in GL_n(\mathbb{R}) \Rightarrow \exists A^{-1}$ t.d. $AA^{-1} = I$

$B \in GL_n(\mathbb{R}) \Rightarrow \exists B^{-1}$ t.d. $BB^{-1} = I$

$$(AB)(B^{-1}A^{-1}) = A\underbrace{(BB^{-1})}_{=I}A^{-1} = AA^{-1} = I$$

Matrica AB ima inverznu matricu $\Rightarrow AB \in GL_n(\mathbb{R})$.

(#) Neka je $U = \{ z \in \mathbb{C} \mid |z| = 1 \}$ (U je krug u Euklidovoj ravni sa centrom u koordinatnom početku poluprečnika 1).
Pokazati da je U zatvoren u odnosu na množenje.

Rj:

Trebamo pokazati da za proizvoljne $z_1, z_2 \in U$ vrijedi $z_1 z_2 \in U$.

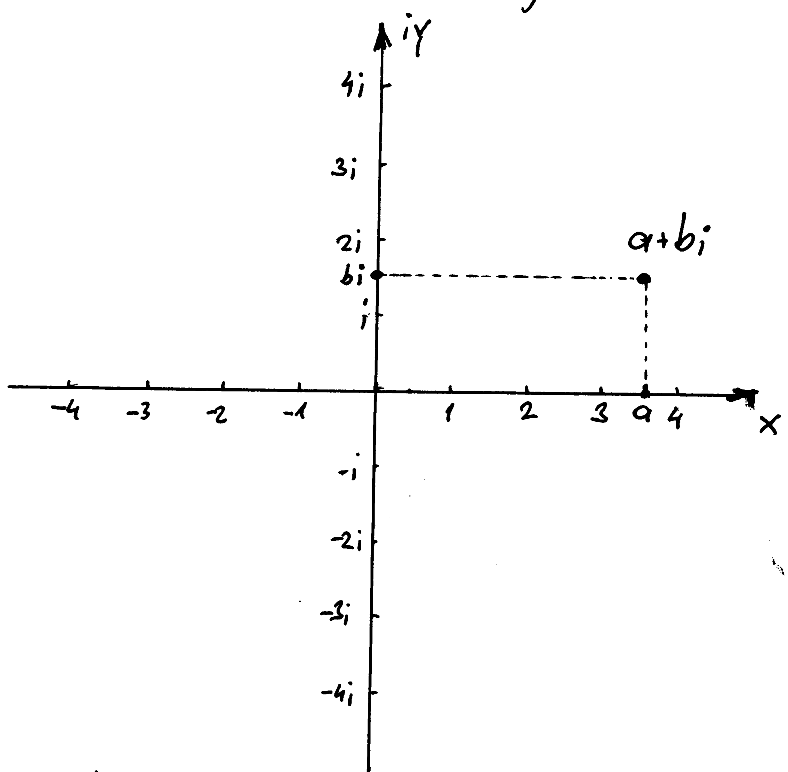
Prisjetimo se $z = a + ib$

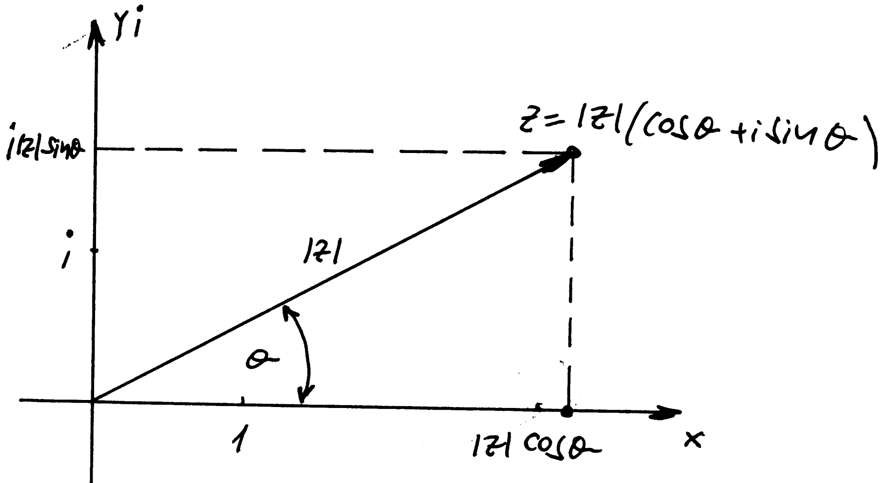
$\mathbb{C} = \{ a + bi \mid a, b \in \mathbb{R} \}$

$i^2 = -1$

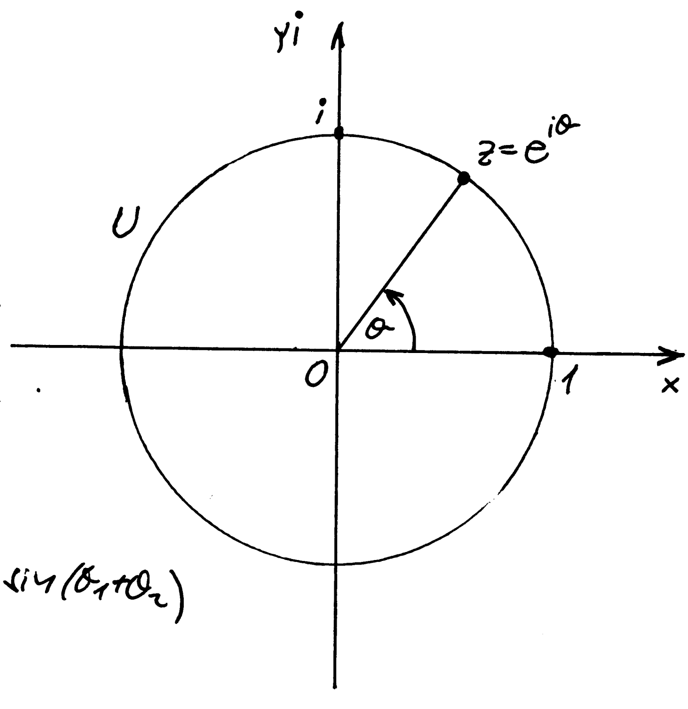
$|z| = \sqrt{a^2 + b^2}$

$z = |z| (\cos\theta + i \sin\theta)$





$e^{i\theta} = \cos\theta + i \sin\theta$



$z_1 \in U \Rightarrow |z_1| = 1 \overset{\exists \theta_1}{\Rightarrow} z_1 = \cos\theta_1 + i \sin\theta_1$

$z_2 \in U \Rightarrow |z_2| = 1 \overset{\exists \theta_2}{\Rightarrow} z_2 = \cos\theta_2 + i \sin\theta_2$.

$\Rightarrow z_1 = e^{i\theta_1}, \; z_2 = e^{i\theta_2}$

$z_1 \cdot z_2 = e^{i\theta_1} \cdot e^{i\theta_2} = e^{i(\theta_1 + \theta_2)} = \cos(\theta_1 + \theta_2) + i \sin(\theta_1 + \theta_2)$

$\Rightarrow |z_1 z_2| = 1 \Rightarrow z_1 z_2 \in U$

(#) Neka je G skup svih realnih brojeva oblika $x+y\sqrt{2}$ gdje su $x,y\in\mathbb{Q}$ racionalni brojevi koji nisu istovremeno jednaki nuli. Pokazati da je G zatvoren u odnosu na obično množenje.

Rj. $G=\{x+y\sqrt{2} \mid x,y\in\mathbb{Q},\ x\neq 0 \text{ ili } y\neq 0\}$

Izaberimo dva proizvoljna elementa $g_1, g_2 \in G$ i pokažimo da je $g_1 \cdot g_2 \in G$.

$$\left.\begin{aligned} g_1 &= x_1+y_1\sqrt{2} \\ g_2 &= x_2+y_2\sqrt{2} \end{aligned}\right\} \Rightarrow \quad g_1\cdot g_2 = (x_1+y_1\sqrt{2})(x_2+y_2\sqrt{2})$$

$$= x_1x_2 + x_1y_2\sqrt{2} + x_2y_1\sqrt{2} + y_1y_2\cdot 2$$

$$= \underbrace{x_1x_2+2y_1y_2}_{\in\mathbb{Q}} + \underbrace{(x_1y_2+x_2y_1)}_{\in\mathbb{Q}}\sqrt{2}$$

Trebamo još pokazati da je $x_1x_2+2y_1y_2\neq 0$ ili $x_1y_2+x_2y_1\neq 0$

1° $x_1\neq 0$ i $x_2\neq 0$

Tada $x_1x_2+2y_1y_2\neq 0 \Rightarrow g_1g_2\in G$

2° $x_1\neq 0$, $y_2\neq 0$

Tada $x_1y_2+x_2y_1\neq 0 \Rightarrow g_1g_2\in G$

3° $y_1\neq 0$, $x_2\neq 0$

Tada $x_1y_2+x_2y_1\neq 0 \Rightarrow g_1g_2\in G$

4° $y_1\neq 0$, $y_2\neq 0$

Tada $x_1x_2+2y_1y_2\neq 0 \Rightarrow g_1g_2\in G$

Skup G je zatvoren u odnosu na obično množenje.

Definicija (komutativnost)

Za binarnu operaciju $*$ na skupu S kažemo da je komutativna ako (i samo ako) $a*b=b*a$ za sve $a,b\in S$.

Definicija (asocijativnost)

Za binarnu operaciju $*$ na skupu S kažemo da je asocijativna ako (i samo ako) $(a*b)*c=a*(b*c)$ za sve $a,b,c\in S$.

(#) Dat je skup $G = \{a \in \mathbb{R} \mid a > 0,\ a \neq 1\}$ i data je operacija $*$ definisana na sljedeći način

$$a * b = a^{\log_5 b}$$

Provjeriti da li je $*$ binarna operacija, te da li je asocijativna i komutativna na skupu G.

Rj.:

ZATVORENOST

Izaberimo dva proizvoljna elementa $a, b \in G$.

$a > 0,\ a \neq 1$
$b > 0,\ b \neq 1$

$$a * b = a^{\log_5 b}$$

Primjetimo $\log_5 b \in \mathbb{R}$. Označimo taj broj sa c ($c = \log_5 b$). $a^c > 0 \ \forall c \in \mathbb{R}$

Kako je $a \neq 1$ i $\log_5 b \neq 0$ to je $a^c \neq 1$. Time $a * b \in G$

ASOCIJATIVNOST

$a, b, c \in G \Rightarrow a > 0, b > 0, c > 0,\ a \neq 1, b \neq 1, c \neq 1$

$$\left.\begin{aligned} (a*b)*c &= (a*b)^{\log_5 c} = \left(a^{\log_5 b}\right)^{\log_5 c} = a^{\log_5 b \cdot \log_5 c} \\ a*(b*c) &= a^{\log_5 (b*c)} = a^{\log_5 b^{\log_5 c}} = a^{\log_5 c \cdot \log_5 b} \end{aligned}\right\} \Rightarrow (a*b)*c = a*(b*c)$$

Operacija $*$ je asocijativna.

KOMUTATIVNOST

$a, b \in G \Rightarrow a > 0, b > 0,\ a \neq 1, b \neq 1$

$$\left.\begin{aligned} a*b &= a^{\log_5 b} \\ b*a &= b^{\log_5 a} \end{aligned}\right\} \Rightarrow a*b \neq b*a \qquad \text{npr. } 3^{\log_5 7} \neq 7^{\log_5 3}$$

Operacija $*$ nije komutativna.

Za konačne skupove, binarna operacija na skupu se može definisati pomoću tabele u kome su svi elementi skupa ispisani iznad svake kolone i na lijevoj strani svakog reda. Uvijek zahtjevamo da su ovi elementi napisani u istom poretku. Ovakvu tabelu nazivamo Cayley-eva tabela. Npr. Cayley-eva tabela za $(\mathbb{Z}_5,+)$

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$(\mathbb{Z}_5,+)$ je grupa u odnosu na operaciju sabiranja modulo 5.

#

Tabelu datu na desnoj strani popuniti na takav način da $*$ bude komutativna binarna operacija na skupu $S=\{a,b,c,d\}$.

$*$	a	b	c	d
a	b			
b	d	a		
c	a	c	d	
d	a	b	b	c

Rj

Prema datoj tabeli vidimo da je $b*a=d$. Da bi $*$ bila komutativna također moramo imati $a*b=d$. Prema tome stavićemo d u odgovarajući kvadratić koji definiše $a*b$. Primjetimo da će $a*b$ biti smješteno simetrično u odnosu na kvadratić $b*a$, čija je osa simetrije dijagonala tabele.

$*$	a	b	c	d
a	b	d	a	a
b	d	a	c	b
c	a	c	d	b
d	a	b	b	c

Na sličan način popunimo ostatak tabele.

(#) Tabelu na desnoj strani popuniti tako da $*$ bude komutativna binarna operacija na skupu $S=\{a, b, c, d\}$.

$*$	a	b	c	d
a	a	b		d
b		a	c	d
c	c	d	c	d
d				

Rj.

Primjetimo da je $c*a=c \Rightarrow a*c=c$

Kako je $a*b=b$ to mora biti $b*a=b$

Time je ostalo da popunimo vrstu d:

$a*d=d \Rightarrow d*a=d$; $b*d=d \Rightarrow d*b=d$

$c*d=d \Rightarrow d*c=d$

$*$	a	b	c	d
a	a	b	c	d
b	b	a	c	d
c	c	d	c	d
d	d	d	d	

pozicija na ovom mjestu može sadržavati a ili b ili c ili d. Za bilo koji od ova četri elementa $*$ će biti komutativna.

(#) Dat je skup $G=\{a, b, c\}$. Koliko ima različitih binarnih operacija $*$ definisanih na skupu G. Koliko je među njima komutativnih binarnih operacija.

Rj.:

$$*: G\times G \to G$$

Primjeri $*$ kao binarne operacije na skupu G su

$*$	a	b	c
a	a	a	a
b	a	a	a
c	a	a	a

$*$	a	b	c
a	a	a	a
b	a	a	a
c	a	a	b

$*$	a	b	c
a	a	a	a
b	a	a	a
c	a	a	c

...

G ima 3 elementa

$G\times G$ će imati $3\cdot 3=9$ elemenata $\Rightarrow$ 9 kvadratića od kojih svaki kvadratić može imati 3 različite vrijednosti

$\Rightarrow$ $\exists\ 3^9$ različitih binarnih operacija $*$

Koliko je među njima komutativno?

$*$	a	b	c
a	a		
b	b	c	
c	b	c	a

Primjetimo da u tom slučaju šest kvadratića ispod dijagonale određuje čitavu tabelu.

$\exists\ 3^6$ komutativnih grupoida

$$\boxed{3^9 = 3^2\cdot 3^2\cdot 3^2\cdot 3^2\cdot 3 = 9^4\cdot 3 = 81^2\cdot 3}$$

Tabela data na desnoj strani se može popuniti tako da $*$ bude asocijativna binarna operacija na skupu $S=\{a,b,c,d\}$. Pretpostavljajući da je ovo moguće izračunati nedostajuće elemente.

$*$	a	b	c	d
a	a	b	c	
b	b	d		c
c	c	a	d	b
d	d			a

Rj: Za binarnu operaciju $*$ kažemo da je asocijativna na skupu G akko $\forall x,y,z\in G \quad (x*y)*z = x*(y*z)$.

$$(a*d)*a = a*\underbrace{(d*a)}_{=d} \Rightarrow (a*d)*a = a*d$$

$$(a*d)*b = a*\underbrace{(d*b)}_{=??}$$

$$(a*d)*c = a*\underbrace{(d*c)}_{=??}$$

$$(a*d)*d = a*\underbrace{(d*d)}_{=a} \Rightarrow (a*d)*d = a$$

$\Rightarrow$ $a*d$ može biti a ili d

ako stavimo da je $a*d$ biti c dobijemo kontradikciju

Odredimo sad $b*c$

$$(b*c)*a = b*\underbrace{(c*a)}_{=c} \Rightarrow (b*c)*a = b*c$$

$$(b*c)*b = b*\underbrace{(c*b)}_{=a} \Rightarrow (b*c)*b = b$$

$$(b*c)*c = b*\underbrace{(c*c)}_{=d} \Rightarrow (b*c)*c = c$$

$$(b*c)*d = b*\underbrace{(c*d)}_{=b} \Rightarrow (b*c)*d = d$$

$\Rightarrow b*c = a$

gdje

$a*d = d$

$b*c$ nemože biti d zbog toga što bi dobili da je $d*d=d$ #kontradik.

$b*c$ nemože biti b zbog toga što bi dobili da je $b*b=b$ #kontr.

$b*c$ nemože biti c zbog toga što bi dobili $c*c=c$ #kontradikcija

⋮

Time smo dobili $a*d=d$ i $b*c=a$

Sljedeće što želimo odrediti je $d*b$.

$$\left.\begin{aligned}
(d*b)*a &= d*\underbrace{(b*a)}_{=b} &&\Rightarrow \quad (d*b)*a = d*b\\
(d*b)*b &= d*\underbrace{(b*b)}_{=d} &&\Rightarrow \quad (d*b)*b = a\\
(d*b)*c &= d*\underbrace{(b*c)}_{=a} &&\Rightarrow \quad (d*b)*c = d\\
(d*b)*d &= d*\underbrace{(b*d)}_{=c} &&\Rightarrow \quad (d*b)*d = d*c
\end{aligned}\right\} \Rightarrow$$

Jedini slučaj kada nećemo doći do kontradikcije je kada $d*b=c$ ali tada također imamo da je $d*c=b$.

*	a	b	c	d
a	a	b	c	d
b	b	d	a	c
c	c	a	d	b
d	d	c	b	a

(#) Na skupu cijelih brojeva $\mathbb{Z}$ definisana je operacija $*$ na sljedeći način

$$a*b = a+b-1$$

Provjeriti da li je $*$ binarna operacija, te da li je asocijativna i komutativna na skupu $\mathbb{Z}$.

Rj. ZATVORENOST

$a, b \in \mathbb{Z} \qquad a*b = a+b-1 \in \mathbb{Z} \implies a*b \in \mathbb{Z}$

Operacija $*$ je binarna operacija.

ASOCIJATIVNOST

$a, b, c \in \mathbb{Z}$

$$\left.\begin{aligned} (a*b)*c &= (a*b)+c-1 = (a+b-1)+c-1 = a+b+c-2 \\ a*(b*c) &= a+(b*c)-1 = a+(b+c-1)-1 = a+b+c-2 \end{aligned}\right\} \implies$$

$$\implies (a*b)*c = a*(b*c)$$

Operacija $*$ je asocijativna.

KOMUTATIVNOST

$$\left.\begin{aligned} a*b &= a+b-1 \\ b*a &= b+a-1 = a+b-1 \end{aligned}\right\} \implies a*b = b*a$$

Operacija $*$ je komutativna

(#) Na skupu pozitivnih realnih brojeva $\mathbb{R}^+$ definisana je operacija $*$ na sljedeći način

$$a * b = a^b$$

Provjeriti da li je $*$ binarna operacija na $\mathbb{R}^+$, te da li je asocijativna i komutativna na $\mathbb{R}^+$.

Rj.:

ZATVORENOST

$a, b \in \mathbb{R}^+$ $\quad a * b = a^b \in \mathbb{R}^+ \Rightarrow$ $*$ jest binarna operacija

ASOCIJATIVNOST

$a, b, c \in \mathbb{R}^+$

$$\left.\begin{aligned} (a*b)*c &= (a*b)^c = (a^b)^c = a^{bc} \\ a*(b*c) &= a^{(b*c)} = a^{b^c} \end{aligned}\right\} \Rightarrow (a*b)*c \neq a*(b*c)$$

$*$ nije asocijativna

KOMUTATIVNOST

$a, b \in \mathbb{R}^+$

$$\left.\begin{aligned} a*b &= a^b \\ b*a &= b^a \end{aligned}\right\} \Rightarrow a^b \neq b^a \quad (\text{npr. } 7^2 \neq 2^7)$$

$a*b$ nije jednako $b*a$ za sve $a, b \in \mathbb{R}^+$

$*$ nije komutativna

Definicija (jedinični element)

Neka je $*$ binarna operacija definisana na skupu G. Element $e \in G$ nazivamo jedinični element operacije $*$ ako za sve $x \in G$ $e * x = x$ i $x * e = x$.

Definicija (inverzni element)

Neka je $*$ binarna operacija definisana na skupu G. Element $a' \in G$ nazivamo inverzni element elementa a ako $a * a' = e$ i $a' * a = e$, gdje je e jedinični element operacije $*$.

(#) Neka je $U_n = \{ z \in \mathbb{C} \mid z^n = 1 \}$ (skup U_n se naziva skup n-tih korijena od 1). Pokazati da

(i) je U_n zatvoren u odnosu na obično množenje;

(ii) postoji jedinični element u odnosu na obično množenje;

(iii) svaki element $z \in U_n$ ima inverzni element.

Rj.

Prvo pokažimo da ako je $z^n = 1$ tada $|z| = 1$.

$z = |z|(\cos\varphi + i\sin\varphi) = |z| e^{i\varphi}$

$z^n = |z|^n e^{in\varphi}$

I način

$$|z^n| = ||z|^n e^{in\varphi}| = |z|^n \underbrace{|e^{in\varphi}|}_{=1}$$

$$|z^n| = 1$$

$$|z|^n = 1 \Rightarrow |z| = 1$$

II način

$$z^n = 1$$

$$z^n = |z|^n(\cos n\varphi + i\sin n\varphi)$$

$$|z|^n \cos n\varphi = 1$$

$$|z|^n \sin n\varphi = 0$$

$$|z|^{2n} \cos^2 n\varphi = 1$$

$$+ \ |z|^{2n} \sin^2 n\varphi = 0$$

$$|z|^{2n} = 1 \Rightarrow |z| = 1$$

(i) Neka su $z_1, z_2 \in U_n$

Tada $|z_1| = 1$, $|z_2| = 1$, $z_1^n = 1$, $z_2^n = 1$

$z_1 = e^{i\varphi_1}$

$z_2 = e^{i\varphi_2}$

$$z_1 \cdot z_2 = e^{i(\varphi_1 + \varphi_2)}$$

$$(z_1 \cdot z_2)^n = e^{in(\varphi_1 + \varphi_2)} = e^{in\varphi_1} \cdot e^{in\varphi_2} = 1$$

$z_1 \cdot z_2 \in U_n$ $\quad$ U_n je zatvoren u odnosu na obično množenje.

(ii) $\forall z \in \mathbb{C}$ $\ 1 \cdot z = z$; $z \cdot 1 = z$. Kako je $1^n = 1$ i $1 \in \mathbb{C}$ to $1 \in U_n$.

(iii) $z \in U_n \Rightarrow z \cdot z \in U_n$ tj. $z^2 \in U_n \Rightarrow z^2 \cdot z \in U_n$ tj. $z^3 \in U_n \Rightarrow z^{n-1} \in U_n$

Kako je $z \cdot z^{n-1} = z^n = 1$ i $z^{n-1} \cdot z = 1$ to je z^{n-1} inverzni element.

(#) Operacija "obično" množenje je binarna operacija na skupu $G = \left\{ \frac{1+2m}{1-2n} \,\middle|\, m, n \in \mathbb{Z} \right\}$. Provjeriti da li

(i) postoji jedinični element e;

(ii) svaki element $a \in G$ ima inverz.

Rj.

Izaberimo proizvoljni element $a \in G$ $\left(a = \frac{1+2m}{1-2n},\ m, n \in \mathbb{Z}\right)$.

(i) Trebamo odrediti e t.d. $a \cdot e = a$ i $e \cdot a = a$

Primjetimo da

$$\frac{1+2m}{1-2n} \cdot 1 = \frac{1+2m}{1-2n} \qquad 1 \cdot \frac{1+2m}{1-2n} = \frac{1+2m}{1-2n}$$

Jedinični element je 1

(ii)

Za proizvoljno $a \in G$ odredimo $a' \in G$ tako da vrijedi $a \cdot a' = 1$ i $a' \cdot a = 1$.

$$\frac{1+2m}{1-2n} \cdot a' = 1 \quad \Rightarrow \quad a' = \frac{1-2n}{1+2m}$$

$$a' = \frac{1+2(-n)}{1-2(-m)} \in G$$

Da, svaki element $a \in G$ ima inverz.

<u>Definicija</u> (grupa)

Grupa $(G, *)$ je skup G, zajedno sa operacijom $*$, tako da su sljedeće aksiome zadovoljene

(ZATVORENOST) $\forall a, b \in G \quad a * b \in G$

(ASOCIJATIVNOST) $\forall a, b, c \in G \quad (a*b)*c = a*(b*c)$

(JEDINIČNI ELEMENT) $\exists e \in G \overset{t.d.}{\vee} \forall x \in G \quad e*x = x*e = x$

(INVERZNI ELEMENT) $\forall a \in G \quad \exists a' \in G \overset{t.d.}{\vee} a*a' = a'*a = e$

Skup G zajedno sa operacijom $*$ nazivamo grupa akko su zadovoljene sljedeće aksiome ...

<u>Definicija</u> (Abelova grupa)

Grupu $(G, *)$ nazivamo Abelova grupa ili komutativna grupa akko je $*$ komutativna binarna operacija.

(#) Neka je $GL_n(\mathbb{R}) \subseteq Mat_{n\times n}(\mathbb{R})$ skup svih $n\times n$ invertibilnih matrica čiji su elementi realni brojevi. Pretpostavimo da je G grupa od šest elemenata iz $GL_2(\mathbb{R})$ čija je operacija matrično množenje. Također pretpostavimo da vrijedi

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in G \quad ; \quad \begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix} \in G$$

(a) Koji su ostali elementi u G? Obrazložiti svoje tvrdnje.
(b) Napisati Cayley-evu tabelu za G.
(c) Da li je G Abelova grupa?

Rj.

(a) Označimo dvije date matrice sa A i B tj. $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ i $B = \begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix}$

Kako je G grupa to je G zatvoreno u odnosu na operaciju množenje pa je $A^2 \in G$, $A^3 \in G$, $A^4 \in G, \dots$, $AB \in G$, $A^2B \in G, \dots$ $B^2 \in G$, $B^3 \in G$, $B^4 \in G, \dots$ Kako G ima šest elemenata dovoljno je da pronađemo 6 različitih matrica na ovaj način

$0+1 \quad 0+0$
$0+0 \quad 1+0$

$$A^2 = A \cdot A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I$$

A
B
I
C
D

$$A^3 = A^2 \cdot A = I \cdot A = A$$

$$B^2 = \begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1+0 & 1-1 \\ 0+0 & 0+1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I$$

$$AB = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0+0 & 0+1 \\ -1 & -1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} = C$$

$$C \cdot A = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -1 & -1 \end{pmatrix} = D$$

Treba nam još jedna matrica.

$$C^2 = C \cdot C = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix} = E$$

Prema tome skup G je

$$G = \left\{ \underset{A}{\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}}, \underset{B}{\begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix}}, \underset{C}{\begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}}, \underset{D}{\begin{pmatrix} 1 & 0 \\ -1 & -1 \end{pmatrix}}, \underset{E}{\begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}}, \underset{I}{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}} \right\}$$

Primjetimo da je $E^2 = E \cdot E = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} = C$

(b)

$\cdot$	I	A	B	C	D	E
I	I	A	B	C	D	E
A	A	I	C	B	B	D
B	B	E	I	D	C	A
C	C	D	A	E	B	I
D	D	C	E	A	I	B
E	E	B	D	I	A	C

$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

$A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

$B = \begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix}$

$C = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$

$D = \begin{pmatrix} 1 & 0 \\ -1 & -1 \end{pmatrix}$

$E = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}$

(c) Iz Cayley-eve tabele vidimo da G nije abelova grupa

npr. $E \cdot D \neq D \cdot E$.

(#) Neka je $\mathbb{Q}^+$ skup pozitivnih racionalnih brojeva, i neka je $*$ operacija definisana na skupu $\mathbb{Q}^+$ na sljedeći način

$$a*b = \frac{ab}{2}$$

Provjeriti da li je $(\mathbb{Q}^+, *)$ grupa.

Rj. $\mathbb{Q}^+ = \left\{ \frac{a}{b} \mid a \in \mathbb{Z}^+,\ b \in \mathbb{Z}^+ \right\}$

Pokažimo da vrijede četri aksiome iz definicije grupe.

ZATVORENOST

$a, b \in \mathbb{Q}^+ \Rightarrow a*b = \frac{ab}{2} \in \mathbb{Q}^+$ $\quad *$ je binarna operacija

ASOCIJATIVNOST

$$a,b,c \in \mathbb{Q}^+ \Rightarrow \left.\begin{aligned} (a*b)*c &= \frac{ab}{2}*c = \frac{\frac{ab}{2}\cdot c}{2} = \frac{abc}{4} \\ a*(b*c) &= a*\frac{b\cdot c}{2} = \frac{a\cdot\frac{bc}{2}}{2} = \frac{abc}{4} \end{aligned}\right\} \Rightarrow * \text{ je asocijat.}$$

JEDINIČNI ELEMENT $(\exists e \in G\ \forall a \in G\quad a*e = a$ i $e*a = a)$

$a \in \mathbb{Q}^+ \Rightarrow 2*a = \frac{2\cdot a}{2} = a$ i $a*2 = \frac{a\cdot 2}{2} = a$

2 je jedinični element za $*$

INVERZNI ELEMENT $(\forall a \in G\ \exists a' \in G$ t.d. $a*a' = a'*a = e)$

$a \in \mathbb{Q}$

$a*a' = 2$

$\frac{aa'}{2} = 2 \Rightarrow a' = \frac{4}{a}$

$a*\frac{4}{a} = 2$ i $\frac{4}{a}*a = \frac{\frac{4}{a}\cdot a}{2} = 2$

$\frac{4}{a}$ je jedinični element za a

Prema tome $(\mathbb{Q}^+, *)$ je grupa.

(#) Neka je G grupa sa osobinom da

$$\forall g \in G \quad g^2 = e$$

Dokazati da je G abelova grupa.

Rj. Prema postavci zadatka operacija množenja na skupu G je zatvorena, asocijativna, postoji jedinični element e, i svaki element $a \in G$ ima invert.

Pokažimo još da je operacija množenja komutativna na G.

$a, b \in G \Rightarrow ab \in G \Rightarrow (ab)^2 = e$

$$(ab)(ab) = e \quad /\cdot a \text{ sa lijeve strane}$$

$$\underbrace{a^2}_{=e}(bab) = a$$

$$bab = a \quad /\cdot b \text{ sa lijeve strane}$$

$$b^2 ab = ba$$

$$ab = ba$$

G je Abelova grupa.

(#) Neka je G grupa čija je operacija množenje, i neka su $a, b \in G$ dati elementi. Dokazati da za svaki pozitivni cijeli n vrijedi

$$(aba^{-1})^n = ab^n a^{-1}.$$

Rj. Jednakost dokažimo matematičkom indukcijom.

. BAZA INDUKCIJE

$n=1$: $\quad (aba^{-1})^1 = aba^{-1} = ab^1a^{-1} \Rightarrow$ jednakost vrijedi za $n=1$

KORAK INDUKCIJE

Pretpostavimo da je jednakost tačna za sve brojeve od 1 do n, pa na osnovu ove pretpostavke dokažimo da je jednakost tačna za $n+1$.

$$(aba^{-1})^{n+1} = (aba^{-1})^n \cdot (aba^{-1}) \underset{\text{pretpostavke}}{\overset{\text{na osnovu}}{=}} (ab^n a^{-1})(aba^{-1}) = ab^n \underbrace{(a^{-1}a)}_{=e} ba^{-1}$$

$$= ab^{n+1}a^{-1}$$

Jednakost je tačna za $n+1$.

ZAKLJUČAK

Jednakost je tačna za sve prirodne brojeve.

(#) Neka je G grupa sa sljedećom osobinom

$$a,b\in G,\ n\in\mathbb{Z}^+ \Rightarrow (ab)^n = a^n b^n$$

Dokazati da je G Abelova grupa.

Rj. Prema postavci zadatka, ono što trebamo pokazati je da je operacija množenje komutativna na G.

$$a,b\in G \overset{2\in\mathbb{Z}^+}{\Longrightarrow} (ab)^2 = a^2b^2$$

$$(ab)(ab) = a^2b^2 \quad / \cdot a^{-1} \text{ sa lijeve strane}$$

$$(a^{-1}a)(bab) = a^{-1}a^2b^2$$

$$bab = ab^2 \quad / \cdot b^{-1} \text{ sa desne strane}$$

$$ba = ab$$

q.e.d.

(#) Pokazati da je podskup $GL_n(\mathbb{R})$ skupa $Mat_{n\times n}(\mathbb{R})$ koji se sastoji od svih $n\times n$ invertibilnih matrica grupa u odnosu na matrično množenje.

Rj: Pokažimo da matrično množenje zadovoljava četri aksiome iz definicije grupe.

ZATVORENOST $(\forall a,b\in G \ \ a*b\in G)$

$A,B\in GL_n(\mathbb{R}) \Rightarrow \exists A^{-1} \ ; \ \exists B^{-1}$ t.d. $AA^{-1}=I \ ; \ BB^{-1}=I$

$(AB)(B^{-1}A^{-1}) = A\underbrace{(BB^{-1})}_{=I}A^{-1} = AA^{-1} = I \Rightarrow$ AB ima inverznu matricu

$\Rightarrow AB\in GL_n(\mathbb{R})$

ASOCIJATIVNOST $(\forall a,b,c\in G \ \ (a*b)*c = a*(b*c))$

Množenje matrica je asocijativno

NEUTRALNI ELEMENT $(\exists e\in G \ \forall a\in G \ \ a*e=e*a=a)$

$A\in GL_n(\mathbb{R}) \Rightarrow AI=A \ ; \ I\cdot A=A$

Neutralni element je I

INVERZNI ELEMENT $(\forall a\in G \ \exists a'\in G$ t.d. $aa'=a'a=e)$

$A\in GL_n(\mathbb{R}) \Rightarrow AA^{-1}=I \ ; \ A^{-1}A=I$

Da li $A^{-1}\in GL_n(\mathbb{R})$. DA, zato što A^{-1} ima inverznu matricu.

Možemo zaključiti da je $GL_n(\mathbb{R})$ grupa u odnosu na matrično množenje.

(#) Neka je n pozitivni cijeli i neka je $n\mathbb{Z} = \{nm \mid m \in \mathbb{Z}\}$.
Pokazati da je $(n\mathbb{Z}, +)$ grupa.

Rj.: Trebamo pokazati da vrijede četri aksiome iz definicije grupe.

ZATVORENOST $(\forall a, b \in G \;\; a * b \in G)$

$$a, b \in n\mathbb{Z} \overset{\exists m_1, m_2 \in \mathbb{Z}}{\Rightarrow} \begin{array}{l} a = nm_1 \\ b = nm_2 \end{array} \Rightarrow a + b = nm_1 + nm_2 = n\underbrace{(m_1 + m_2)}_{\in \mathbb{Z}} \in n\mathbb{Z}$$

tj. $a + b \in n\mathbb{Z}$

$+$ jest binarna operacija

ASOCIJATIVNOST $(\forall a, b, c \in G \;\; (a * b) * c = a * (b * c))$

$$a, b, c \in n\mathbb{Z} \overset{\exists m_1, m_2, m_3 \in \mathbb{Z}}{\Rightarrow} \begin{array}{l} a = nm_1 \\ b = nm_2 \\ c = nm_3 \end{array} \quad \begin{aligned} (a + b) + c &= (nm_1 + nm_2) + nm_3 \\ &= nm_1 + (nm_2 + nm_3) = a + (b + c) \end{aligned}$$

NEUTRALNI ELEMENT $(\exists e \in G \;\; \forall a \in G \;\; a * e = e * a = a)$

$e = 0 = 0 \cdot m \in n\mathbb{Z}$

$$a \in n\mathbb{Z} \overset{\exists m_1 \in \mathbb{Z}}{\Rightarrow} a = nm_1$$

$$a + e = nm_1 + 0 = nm_1 \in n\mathbb{Z}$$
$$e + a = 0 + nm_1 = nm_1 \in n\mathbb{Z}$$

0 je neutralni element

INVERZNI ELEMENT $(\forall a \in G \;\; \exists a' \in G \;\; a * a' = a' * a = e)$

$$a \in n\mathbb{Z} \overset{\exists m_1 \in \mathbb{Z}}{\Rightarrow} a = m_1 n \quad \text{Neka je } a' = n(-m_1) \Rightarrow a + a' = 0 \quad (a' + a = 0)$$

a' je neutralni element

$(n\mathbb{Z}, +)$ jest grupa

(#) Neka je n pozitivni cijeli i neka je $n\mathbb{Z} = \{nm \mid m \in \mathbb{Z}\}$. Pokazati da je $(n\mathbb{Z}, +)$ grupa.

Rj.: Trebamo pokazati da vrijede četri aksiome iz definicije grupe.

ZATVORENOST $(\forall a,b \in G \;\; a*b \in G)$

$$a,b \in n\mathbb{Z} \overset{\exists m_1,m_2 \in \mathbb{Z}}{\Longrightarrow} \begin{array}{l} a = nm_1 \\ b = nm_2 \end{array} \Rightarrow a+b = nm_1 + nm_2 = n\underbrace{(m_1+m_2)}_{\in \mathbb{Z}} \in n\mathbb{Z}$$

tj. $a+b \in n\mathbb{Z}$

$+$ jest binarna operacija

ASOCIJATIVNOST $(\forall a,b,c \in G \;\; (a*b)*c = a*(b*c))$

$$a,b,c \in n\mathbb{Z} \overset{\exists m_1,m_2,m_3 \in \mathbb{Z}}{\Longrightarrow} \begin{array}{l} a = nm_1 \\ b = nm_2 \\ c = nm_3 \end{array} \quad \begin{aligned}(a+b)+c &= (nm_1 + nm_2) + nm_3 \\ &= nm_1 + (nm_2 + nm_3) = a+(b+c)\end{aligned}$$

NEUTRALNI ELEMENT $(\exists e \in G \;\; \forall a \in G \;\; a*e = e*a = a)$

$e = 0 = 0 \cdot m \in n\mathbb{Z}$

$$a \in n\mathbb{Z} \overset{\exists m_1 \in \mathbb{Z}}{\Longrightarrow} a = nm_1$$

$$a + e = nm_1 + 0 = nm_1 \in n\mathbb{Z}$$
$$e + a = 0 + nm_1 = nm_1 \in n\mathbb{Z}$$

0 je neutralni element

INVERZNI ELEMENT $(\forall a \in G \;\; \exists a' \in G \;\; a*a' = a'*a = e)$

$$a \in n\mathbb{Z} \overset{\exists m_1 \in \mathbb{Z}}{\Longrightarrow} a = m_1 n \quad \text{Neka je } a' = n(-m_1) \Rightarrow \begin{array}{l} (a'+a = 0) \\ a+a' = 0 \end{array}$$

a' je neutralni element

$(n\mathbb{Z}, +)$ jest grupa

(#) Da li je skup $G = \{ X \in Mat_{2\times 2}(\mathbb{C}) \mid det(X) = 1 \}$ u odnosu na uobičajeno množenje matrica grupa? Odgovor obrazložiti.

Rj:

Ispitajmo sve osobine iz definicije grupe

ZATVORENOST ($\forall a, b \in G \quad a * b \in G$)

$A, B \in G$ npr. $A = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}$, $B = \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix}$. Kako je $A \in G$ to $det(A) = 1$
$B \in G$ to $det(B) = 1$.

$\Downarrow$

$a_1 d_1 - b_1 c_1 = 1$

$a_2 d_2 - b_2 c_2 = 1$

Trebamo pokazati da je $det(AB) = 1$.

$$AB = \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} = \begin{pmatrix} a_1 a_2 + b_1 c_2 & a_1 b_2 + b_1 d_2 \\ a_2 c_1 + c_2 d_1 & b_2 c_1 + d_1 d_2 \end{pmatrix}$$

$$det(AB) = (a_1 a_2 + b_1 c_2)(b_2 c_1 + d_1 d_2) - (a_1 b_2 + b_1 d_2)(a_2 c_1 + c_2 d_1) =$$

$$= \underline{a_1 a_2 b_2 c_1} + \underline{\underline{a_1 a_2 d_1 d_2}} + b_1 b_2 c_1 c_2 + \cancel{b_1 c_2 d_1 d_2} - \underline{a_1 a_2 b_2 c_1} - a_1 b_2 c_2 d_1 - \underline{\underline{a_2 b_1 c_1 d_2}} - \cancel{b_1 c_2 d_1 d_2}$$

$$= a_2 d_2 \underbrace{(a_1 d_1 - b_1 c_1)}_{=1} - b_2 c_2 \underbrace{(a_1 d_1 - b_1 c_1)}_{=1} = a_2 d_2 - b_2 c_2 = 1$$

G je zatvoreno

ASOCIJATIVNOST ($\forall a, b, c \in G \quad a * (b * c) = (a * b) * c$)

Množenje matrica je asocijativno bez obzira koju osobinu zadovoljavaju (možete provjeriti tako što napravite proizvod $A \cdot (B \cdot C)$, pa onda napravite proizvod $(A \cdot B) \cdot C$, i uporedite da li su dva dobijena proizvoda jednaki)

NEUTRALNI ELEMENT ($\exists e \in G \ \forall a \in G \quad a * e = a = e * a$)

$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ je neutralni element.

INVERZNI ELEMENT

Neka je $A = \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}$ proizvoljna matrica iz G.

Kako je $\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} \begin{pmatrix} d_1 & -b_1 \\ -c_1 & a_1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

$\begin{pmatrix} d_1 & -b_1 \\ -c_1 & a_1 \end{pmatrix} \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

te $\begin{vmatrix} d_1 & -b_1 \\ -c_1 & a_1 \end{vmatrix} = 1$ to je inverz za A $\quad A^{-1} = \begin{pmatrix} d_1 & -b_1 \\ -c_1 & a_1 \end{pmatrix}$

Skup G je grupa u odnosu na množenje matrica.