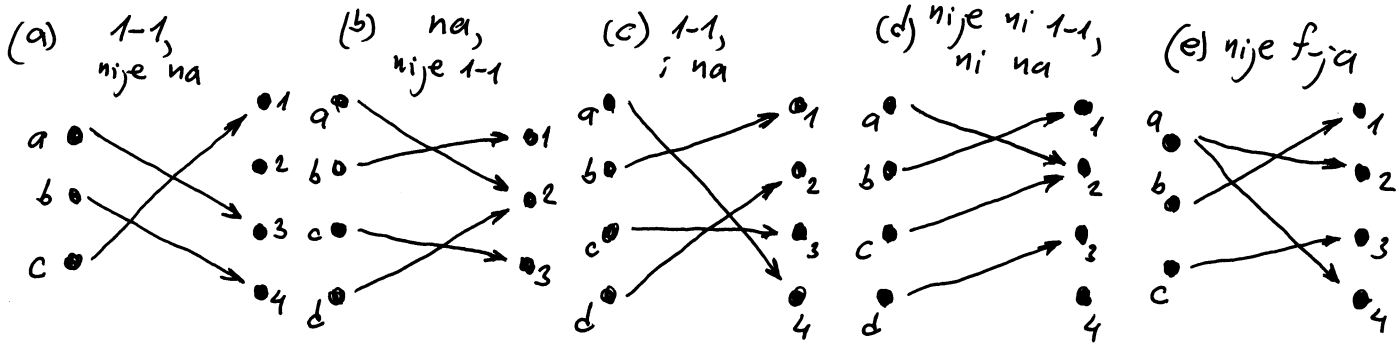
Homomorfizmi, izomorfizmi i automorfizmi; grupa

Definicija (injekcija, surjekcija, bijekcija)

Za f-ju f kažemo da je 1-1 (jedan-na-jedan ili da je injektivna) ako i samo ako $f(x)=f(y)$ povlači da je $x=y$ za sve x i sve y iz domena f-je f. F-ju nazivamo injekcija ako je jedan-na-jedan.

F-ju f sa A u B nazivamo "na", ili sirjektivna, ako i samo ako za svaki element $b \in B$ postoji element $a \in A$ sa osobinom da je $f(a)=b$. Za f-ju f kažemo da je surjekcija ako je na.

F-ja f je bijekcija, ako je obje i jedan-na-jedan i na



Primjeri različitih vrsta preslikavanja

(#) Neka je G grupa, i neka je $\varphi: G \to G$ preslikavanje definisano sa $\varphi(x) = x^{-1}$. Pokazati da je φ bijekcija.

R:

$\varphi: G \to G, \quad \varphi(x) = x^{-1}$

φ JE SURJEKTIVNO

Za proizvoljan $x \in G$ imamo da $\varphi(x^{-1}) = (x^{-1})^{-1} = x$.

φ JE INJEKTIVNO

Izaberimo dva proizvoljna $x, y \in G$ i pretpostavimo da $\varphi(x) = \varphi(y)$.

Ovo povlači da je $x^{-1} = y^{-1} \Rightarrow yx^{-1} = yy^{-1} = e$

$$yx^{-1} = e$$

$$yx^{-1}x = ex$$

$$y = x$$

Prema tome φ je bijekcija.

(#) Neka je $G=\langle a\rangle$, $a^{15}=e$ ciklička grupa reda 15, i neka je $f: G \to G$ definisano sa $f(x)=x^5$, $\forall x \in G$. Pokazati da f nije injektivna f-ja.

Rj. $a, a^4 \in G$, $a \neq a^4$

$$\left.\begin{array}{l} f(a)=a^5 \\ f(a^4)=(a^4)^5=a^{20}=a^{15}\cdot a^5=a^5 \end{array}\right\} \Rightarrow f(a)=f(a^4)$$

Tj. dobili smo da za $a \neq a^4$ vrijedi $f(a)=f(a^4)$.

$\Rightarrow$ f-ja nije injektivna.

Definicija (homomorfizam grupa)

Preslikavanje $\phi: G \to \bar{G}$ grupe $(G, \cdot)$ u grupu $(\bar{G}, \circ)$ nazivamo homomorfizam (između) grupa $(G, \cdot)$ i $(\bar{G}, \circ)$ akko

$$\phi(g_1 \cdot g_2) = \phi(g_1) \circ \phi(g_2)$$

za proizvoljne $g_1, g_2 \in G$.

(#) Neka je G ciklička grupa generisana sa g ($G = \langle g \rangle$) i neka je $(\mathbb{Z}, +)$ grupa cijelih brojeva u odnosu na operaciju sabiranja. Pokazati da je preslikavanje $\phi: \mathbb{Z} \to G$ definisano sa $\phi(n) = g^n$ homomorfizam između grupa $\mathbb{Z}$ i G.

Rj.

$$G = \langle e, g, g^1, g^2, g^3, \dots \rangle$$

$$\phi(m+n) = g^{m+n} = g^m \cdot g^n = \phi(m)\phi(n)$$

Ovaj homomorfizam preslikava $\mathbb{Z}$ na cikličku grupu generisanu sa g.

(#) Date su grupe $(GL_2(\mathbb{R}), \cdot)$ i $(\mathbb{R}^*, \cdot)$ (gdje su $GL_2(\mathbb{R}) = \{A \in Mat_{2\times 2}(\mathbb{R}) \mid \exists A^{-1}\} = \left\{\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in Mat_{2\times 2}(\mathbb{R}) \mid ad - bc \neq 0\right\}$; $\mathbb{R}^* = \{x \in \mathbb{R} \mid x \neq 0\}$). Pokazati da je preslikavanje $\phi: GL_2(\mathbb{R}) \to \mathbb{R}^*$ definisano sa $\phi(A) = \det(A)$ homomorfizam između grupa $GL_2(\mathbb{R})$ i $\mathbb{R}^*$.

Rj. Koristeći osobine determinanata imamo

$$\forall A, B \in GL_2(\mathbb{R}) \qquad \phi(AB) = \det(AB) = \det(A)\det(B) = \phi(A)\phi(B).$$

(#) Date su grupe $(\mathbb{T}, \cdot)$ i $(\mathbb{R}, +)$ (gdje je $\mathbb{T} = \{z \in \mathbb{C} : |z| = 1\}$)
Pokazati da postoji homomorfizam između $\mathbb{R}$ i $\mathbb{T}$.

Rj.:

Definirajmo preslikavanje $\phi : \mathbb{R} \to \mathbb{T}$ na sljedeći način

$$\phi(\alpha) = \cos\alpha + i \sin\alpha$$

Kako je

$$\begin{aligned}
\phi(\alpha+\beta) &= \cos(\alpha+\beta) + i\sin(\alpha+\beta) \\
&= \underline{(\cos\alpha\cos\beta} - \sin\alpha\sin\beta) + i(\underline{\sin\alpha\cos\beta} + \cos\alpha\sin\beta) \\
&= (\cos\alpha + i\sin\alpha)\cos\beta + i(\underbrace{i\sin\alpha\sin\beta + \cos\alpha\sin\beta}_{= \sin\beta(\cos\alpha + i\sin\alpha)}) \\
&= (\cos\alpha + i\sin\alpha)(\cos\beta + i\sin\beta) \\
&= \phi(\alpha)\phi(\beta)
\end{aligned}$$

to su dvije dane grupe izomorfne.

Geometrijski, jednostavno omotavamo realnu os oko kruga u grupo-teorijskom smislu.

Definicija

Preslikavanje $\phi: G \to H$ grupe $(G, \cdot)$ na grupu $(H, \circ)$ nazivamo izomorfizam sa G na H ako i samo ako

(i) ϕ je jedan-na-jedan

(ii) ϕ je na

(iii) $\phi(a \cdot b) = \phi(a) \circ \phi(b)$, za sve $a, b \in G$.

Ako postoji izomorfizam sa G na H, kažemo da su G i H izomorfne grupe i pišemo $G \cong H$.

(#) Date su dvije grupe: $(\mathbb{Z}_4, +)$; $(\langle i \rangle, \cdot)$ (gdje je $i = \sqrt{-1} \in \mathbb{C}$). Neka je $\phi: \mathbb{Z}_4 \to \langle i \rangle$ preslikavanje definirano sa $\phi(n) = i^n$. Pokazati da je ϕ izomorfizam grupe $\mathbb{Z}_4$ na grupu $\langle i \rangle$.

Rj. Trebamo pokazati da je ϕ bijekcija i da čuva operaciju grupe.

$\mathbb{Z}_4 = \{0, 1, 2, 3\}$

$\langle i \rangle = \{1, i, -1, -i\}$

$\phi(0) = 1$

$\phi(1) = i$

$\phi(2) = -1$

$\phi(3) = -i$

Primjetimo da za proizvoljne $a, b \in \mathbb{Z}_4$ $\quad a \neq b \Rightarrow \phi(a) \neq \phi(b)$

tj. ϕ je injektivna f-ja

Također za proizvoljno $b \in \langle i \rangle$ $\exists a \in \mathbb{Z}_4$ t.d. $\phi(a) = b$

tj. ϕ je surjektivna f-ja

Na kraju kako je $\phi(n+m) = i^{n+m} = i^n \cdot i^m = \phi(n)\phi(m)$ to je operacija grupe očuvana.

Prema tome, preslikavanje ϕ je izomorfizam sa $\mathbb{Z}_4$ na $\langle i \rangle$.

(#) Neka je G grupa cijelih brojeva u odnosu na operaciju zbrajanja i neka je $\overline{G}$ podgrupa grupe $\mathbb{Q}^*$ koja sadrži elemente oblika 2^n. Definirajmo preslikavanje $\phi: G \to \overline{G}$ na sljedeći način $\phi(n) = 2^n$. Pokazati da je ϕ izomorfizam sa G na $\overline{G}$.

Rj:

ϕ JE JEDAN-NA-JEDAN

$m, n \in G$, $\phi(m) = \phi(n)$

$\phi(m) = \phi(n) \Rightarrow 2^m = 2^n \Rightarrow \log_2 2^m = \log_2 2^n \Rightarrow m = n$

ϕ JE NA

Uzmimo proizvoljno $t \in \mathbb{Q}^*$ i pokažimo da $\exists n \in G$ t.d. $\phi(n) = t$.

$t \in \mathbb{Q}^* \Rightarrow \exists n$ t.d. $t = 2^n$.

Sad imamo da je $\phi(n) = 2^n = t$ iz čega slijedi da je $\overline{G}$ surjekcija.

ϕ JE HOMOMORFIZAM

$m, n \in G$

$\phi(m+n) = 2^{m+n} = 2^m \cdot 2^n = \phi(m) \cdot \phi(n)$

Prema tome ϕ jest izomorfizam sa G na $\overline{G}$.

(#) Data je grupa $(\mathbb{R},+)$ i dato je preslikavanje $\phi:\mathbb{R}\to\mathbb{R}$ definisano sa $\phi(x)=x^3$. Proveriti da li je ϕ izomorfizam grupe G na samu sebe.

R.j.

DA LI JE ϕ JEDAN-NA-JEDAN?

$x,y\in\mathbb{R},\ \phi(x)=\phi(y) \Rightarrow x^3=y^3 \Rightarrow x=y$ ϕ je 1-1

DA LI JE ϕ NA?

Izaberimo proizvoljno $t\in\mathbb{R}$ i neka je $x=\sqrt[3]{t}$. Tada

$$\phi(x)=(\sqrt[3]{t})^3=t \Rightarrow \phi \text{ je na}$$

DA LI JE ϕ HOMOMORFIZAM?

$x,y\in\mathbb{R}$

$$\left.\begin{aligned}\phi(x+y)&=(x+y)^3\\ \phi(x)+\phi(y)&=x^3+y^3\end{aligned}\right\} \Rightarrow \forall x,y\in\mathbb{R} \text{ ne vrijedi: } (x+y)^3=x^3+y^3$$

ϕ nije homomorfizam

Kako operacija nije očuvana to ϕ nije izomorfizam

(#) Neka je $G = SL_2(\mathbb{R})$ grupa svih realnih matrica oblika 2×2 čija je vrijednost determinante jednaka 1; neka je M neka 2×2 realna matrica t.d. $\det(M) = 1$. Pokažabi da je preslikavanje $\phi: G \to G$ definisano sa $\phi(M) = MAM^{-1}$ izomorfizam grupe G na samu sebe.

Rj.

ϕ JE F-JA SA G u G

Pokažimo da je $\phi(A) \in G$ za $\forall A \in G$. Ovo slijedi iz osobina determinanata

$$\phi(A) = MAM^{-1}$$

$$\det(MAM^{-1}) = (\det M)(\det A)\underbrace{(\det M^{-1})}_{=\det(M)^{-1}} = 1 \cdot 1 \cdot 1^{-1} = 1$$

$$\Rightarrow \phi(A) \in G$$

ϕ JE 1-1

$$A, B \in G, \quad \phi(A) = \phi(B) \Rightarrow MAM^{-1} = MBM^{-1} \Rightarrow MA = MB \Rightarrow A = B$$

ϕ JE NA

Neka je B proizvoljan element iz G. Pronađimo A t.d. $\phi(A) = B$.

Posmatrajmo $A = M^{-1}BM$. $\phi(A) = MAM^{-1} = M(M^{-1}BM)M^{-1} = B$

ϕ JE HOMOMORFIZAM

$$A, B \in G, \quad \phi(AB) = M(AB)M^{-1} = MA(M^{-1}M)BM^{-1} = (MAM^{-1})(MBM^{-1})$$
$$= \phi(A)\cdot\phi(B)$$

Preslikavanje ϕ nazivamo konjugacijom sa M

ϕ je izomorfizam grupe G na samu sebe.

Napomena

Postoje četri koraka koja trebamo sprovesti da bi pokazali da je grupa G izomorfna sa grupom $\overline{G}$.

1. korak: "Preslikavanje".
Definišimo kandidata za izomorfizam, tj. definišimo f-ju ϕ sa G u $\overline{G}$.

2. korak: "1-1".
Dokažimo da je ϕ jedan-na-jedan, tj. pretpostavimo da $\phi(a)=\phi(b)$ i dokažimo da $a=b$

3. korak: "na".
Pokažimo da je ϕ "na", tj. za proizvoljni element $\bar{g}\in\overline{G}$, pronaći element $g\in G$ takav da $\phi(g)=\bar{g}$.

4. korak: "očuvanost operacije"
Dokazati da ϕ čuva operaciju, tj. pokazati da $\phi(ab)=\phi(a)\phi(b)$ za sve a i b iz G.

(#) Neka je G grupa realnih brojeva u odnosu na operaciju sabiranja i neka je $\overline{G}$ grupa pozitivnih realnih brojeva u odnosu na operaciju množenja. Pokazati da su G i $\overline{G}$ izomorfne grupe.

Rj.

POSTOJI PRESLIKAVANJE ϕ.

Definišimo $\phi: G \to \overline{G}$ na sljedeći način $\phi(x) = e^x$

Primjetimo da za $x=y \Rightarrow e^x = e^y \Rightarrow \phi(x) = \phi(y)$

ϕ je dobro definisana f-ja.

ϕ JE JEDAN-NA-JEDAN.

Izaberimo proizvoljne $x, y \in G$ i neka je $\phi(x) = \phi(y)$.

$\Rightarrow e^x = e^y \Rightarrow \ln e^x = \ln e^y \Rightarrow x = y$

ϕ JE NA.

Izaberimo proizvoljan realan y i pokažimo da postoji realan x takav da $\phi(x) = y$.

$\phi(x) = y \Rightarrow e^x = y \Rightarrow x = \ln y$

Sad primjetimo da $\forall y \in \mathbb{R}^+ \; f(\ln y) = y$ tj. $\exists x \in \mathbb{R}$ t.d. $\phi(x) = y$.

ϕ JE HOMOMORFIZAM

$$\phi(x+y) = e^{x+y} = e^x \cdot e^y = \phi(x)\,\phi(y), \quad \forall x, y \in G.$$

(#) Neka je G beskonačna ciklička grupa i neka je $\overline{G}$ grupa cijelih brojeva u odnosu na operaciju zbrajanja. Pokazati da su G i $\overline{G}$ izomorfne grupe.

R.j. Neka je a generator ciklične grupe G tj. $G = \langle a \rangle$.

Promatrajmo preslikavanje $\phi : G \to \overline{G}$

$$a^k \to k$$

ϕ JE 1-1

$x, y \in G$, $\phi(x) = \phi(y)$

$x \in G \Rightarrow \exists m \quad x = a^m$

$y \in G \Rightarrow \exists n \quad y = a^n$ $\quad \phi(x) = \phi(y) \Rightarrow \phi(a^m) = \phi(a^n) \Rightarrow m = n$

ϕ JE NA

Izaberimo proizvoljno $t \in \overline{G}$. Primjetimo da $\phi(a^t) = t$

ϕ JE HOMOMORFIZAM

$$\phi(a^m \cdot a^n) = \phi(a^{m+n}) = m+n = \phi(a^m) + \phi(a^n)$$

Prema tome

$$G \cong \overline{G}.$$

(#) Pokazati da je $U(10) \cong \mathbb{Z}_4$.

Rj.

$U(n) = \{k \in \mathbb{N} \mid k < n \text{ i } \gcd(k, n) = 1\}$

$U(10) = \{1, 3, 7, 9\}$

Primjetimo da je $U(10) = \langle 3 \rangle$

$\mathbb{Z}_4 = \{0, 1, 2, 3\}$

Primjetimo da $\mathbb{Z}_4 = \langle 1 \rangle$

Definirajmo $\phi: U(10) \longrightarrow \mathbb{Z}_4$ na sljedeći način $\phi(3^k) = k \bmod 4$, tj.

$\phi(3^0) = 0$

$\phi(3^1) = 1$

$\phi(3^2) = 2$

$\phi(3^3) = 3$

Nije teško vidjeti da je ϕ bijekcija.

Isto tako

$$\phi(3^i \cdot 3^j) = \phi(3^{i+j}) = (i+j) \bmod 4 =$$

$$= \left| \begin{array}{l} \text{ako je } a \bmod n = a' \\ \text{i } b \bmod n = b' \text{ tada} \\ \text{je } (a+b) \bmod n = (a'+b') \bmod n \end{array} \right|$$

$$= \big((i \bmod 4) + (j \bmod 4)\big) \bmod 4$$

$$= \phi(3^i) + \phi(3^j)$$

ϕ je izomorfizam danih grupa.

(#) Pokazati da $U(10) \not\cong U(12)$.

Rj.

Prisjetimo se $U(n) = \{k \in \mathbb{N} \mid k < n \text{ i } \gcd(k,n) = 1\}$

$U(10) = \{1, 3, 7, 9\}$

$U(12) = \{1, 5, 7, 11\}$

Promatrajmo $U(12)$. Primjetimo da $1^2 = 1$, $5 \cdot 5 = 1$, $7^2 = 1$, $11^2 = 1$

tj. $x^2 = 1$ za $\forall x \in U(12)$.

Sad pretpostavimo da je $\phi : U(10) \to U(12)$ izomorfizam sa $U(10)$ na $U(12)$.

Tada

$$\phi(9) = \phi(3 \cdot 3) = \phi(3)\underbrace{\phi(3)}_{\in U(12)} = 1$$

i $\phi(1) = \phi(1 \cdot 1) = \phi(1) \cdot \phi(1) = 1$

Time smo dobili da $\phi(9) = \phi(1)$ za $9 \neq 1$

#kontradikcija

(sa pretpostavkom da je ϕ jedan-na-jedan)

(#) Date su grupe $(\mathbb{Q},+)$ i $(\mathbb{Q}^*,\cdot)$. Pokazati da $\mathbb{Q} \ncong \mathbb{Q}^*$.

Rj.

Pretpostavimo da postoji izomorfizam $\phi:\mathbb{Q}\to\mathbb{Q}^*$ između $\mathbb{Q}$ i $\mathbb{Q}^*$.

Kako je ϕ surjekcija to $\exists a\in\mathbb{Q}$ t.d. $\phi(a)=-1$. Ali sad imamo

$$-1=\phi(a)=\phi\left(\tfrac{1}{2}a+\tfrac{1}{2}a\right)=\phi\left(\tfrac{1}{2}a\right)\left(\phi\tfrac{1}{2}a\right)=\left[\phi\left(\tfrac{1}{2}a\right)\right]^2$$

tj. $\left[\underbrace{\phi\left(\frac{1}{2}a\right)}_{\in\mathbb{Q}^*}\right]^2=-1$

racionalni broj na kvadrat $=1$

#kontradikcija

(ne postoji racionalan broj koji kada se kvadrira daje -1)

Prema tome $\mathbb{Q} \ncong \mathbb{Q}^*$.

(#) Neka je G ciklička grupa reda n. Pokazati da je $G \cong \mathbb{Z}_n$.

Rj.

Neka je a generator ciklične grupe G tj. $G = \langle a \rangle = \{e, a, e^2, \dots, a^{n-1}\}$.

Promatrajmo preslikavanje $\phi: G \to \mathbb{Z}_n$

$a^k \to k \bmod n$

ϕ JE 1-1

$x, y \in G$, $\phi(x) = \phi(y)$

$x \in G \Rightarrow \exists m \overbrace{\ 0 \le m < n\ }\ x = a^m$

$y \in G \Rightarrow \exists k \overbrace{\ 0 \le k < n\ }\ y = a^k$

$\Big\} \xrightarrow{\phi(x)=\phi(y)} m \bmod n = k \bmod n$

a kako je $0 \le m < n$ i $0 \le k < n$ to je $m = k$

ϕ JE NA

Izaberimo proizvoljan $t \in \mathbb{Z}_n = \{0, 1, 2, \dots, n-1\}$

Primjetimo da za $x = \underbrace{a^t}_{\in G}$ imamo da $\phi(x) = t$.

ϕ JE HOMOMORFIZAM

$$\phi(a^m \cdot a^k) = \phi(a^{m+k}) = (m+k) \bmod n = \left| \begin{array}{l} \text{ako je } m \bmod n = m_1 \\ \text{i } k \bmod n = k_1 \text{ tada} \\ (m+k) \bmod n = (m_1 + k_1) \bmod n \end{array} \right|$$

$$= \big((m \bmod n) + (k \bmod n)\big) \cdot \bmod n$$

$$= \phi(a^m) + \phi(a^k)$$

Prema tome $G \cong \mathbb{Z}_n$.

Znamo da 1-1 preslikavanje sa jedne grupe na drugu grupu se naziva izomorfizam grupa. U slučaju da su obe grupe iste mogu se izvesti neki vrlo zanimljivi rezultati. U tom slučaju izomorfizam nazivamo automorfizam.

Definicija (automorfizam grupe G)
Preslikavanje ϕ sa grupe G na sebe se naziva automorfizam grupe G ako

(i) $\phi(ab) = \phi(a)\,\phi(b) \quad \forall a, b \in G$;

(ii) ϕ je jedan-na-jedan;

(iii) ϕ je na.

(#) Neka je G ne-abelova grupa i neka je $f: G \to G$ definisana sa $f(x) = x^{-1}$. Pokazati da f nije automorfizam.

Rj.

Izaberimo proizvoljne $x, y \in G$.

$$f(xy) = (xy)^{-1} = y^{-1}x^{-1}$$

$$f(x)f(y) = x^{-1}y^{-1}$$

Kako $y^{-1}x^{-1}$ i $x^{-1}y^{-1}$ u opštem slučaju ne moraju biti jednaki to je $f(xy) \neq f(x)f(y)$.

Prema tome f nije automorfizam.

(#) Neka je $G = \langle a \rangle$, $a^{12} = e$, ciklička grupa reda 12. Neka je $f: G \to G$ definisano na sljedeći način $f(x) = x^3$ $\forall x \in G$. Pokazati da f nije automorfizam.

Rj.

Posmatrajmo elemente a i a^5 iz G. Znamo da $a \neq a^5$.

Također imamo

$$\left.\begin{aligned} f(a) &= a^3 \\ f(a^5) &= (a^5)^3 = a^{15} = a^{12} \cdot a^3 = e \cdot a^3 = a^3 \end{aligned}\right\} \Rightarrow$$

$$\Rightarrow \quad f(a) = f(a^5) \quad \Rightarrow \quad f \text{ nije } 1\text{-}1$$

Možemo zaključiti da f nije automorfizam.

(#) Neka je G grupa pozitivnih realnih brojeva u odnosu na množenje. Neka je $\phi: G \to G$ definisano sa $\phi(x) = x^2$, $x \in G$. Pokazati da je ϕ automorfizam.

Rj.:

$\phi(x) = x^2, \quad \forall x \in G$

ϕ JE HOMOMORFIZAM

Neka su $x, y \in G$. $\phi(xy) = (xy)^2 = x^2 y^2 = \phi(x)\phi(y)$

ϕ je homomorfizam sa G u G.

ϕ JE 1-1

Neka su $x, y \in G$; $\phi(x) = \phi(y)$. $\Rightarrow$ $x^2 = y^2$ $\Rightarrow$ $x = \pm y$

Kako su i x ; y oba pozitivna to $x = y$

Drugim riječima $\phi(x) = \phi(y) \Rightarrow x = y \Rightarrow \phi$ je 1-1

ϕ JE NA

Neka je $x \in G$. x je pozitivan realan broj, $\sqrt{x}$ i također pozitivan realan broj

Imamo $\phi(\sqrt{x}) = (\sqrt{x})^2 = x \Rightarrow \phi$ je na

Prema tome ϕ je automorfizam grupe G.

Zadaci za vježbu

1. Neka je G neka grupa u kojoj $a^2 \neq e$ za neko $a \in G$. Pokazati da grupa G ima (da u grupi G postoji) ne-trivijalni automorfizam.

2. Neka je G grupa. Pokazati da preslikavanje $x \to x^{-1}$ sa G u G je automorfizam ako i samo ako je G abelova grupa.

3. Neka je G konačna abelova grupa reda n, i neka je m pozitivan cijeli broj relativno prost sa n. Pokazati da je preslikavanje $f: G \to G$ definisano sa $f(x) = x^m$, $x \in G$, je automorfizam grupe G.

4. Neka je f automorfizam grupe G. Ako je H podgrupa grupe G pokazati da je tada $f(H)$ također podgrupa grupe G.

5. Neka je G grupa i neka je f automorfizam grupe G. Za $a \in G$ definišimo $N(a) = \{x \in G \mid ax = xa\}$. Pokazati da je $N(f(a)) = f(N(a))$.

1. INTRODUCTION

We know that a one-one mapping from one group into another group is called an isomorphism. In case both groups are same and the mapping is onto then we can derive some very interesting results. An isomorphism in such a particular case is called an *automorphism*. In this chapter, we shall also discuss inner automorphisms and group of automorphisms.

2. AUTOMORPHISM

A mapping ϕ from a group G to itself is called an **automorphism** of group G if

(*i*) $\phi(ab) = \phi(a)\,\phi(b)\ \forall\ a, b \in G$ (*ii*) ϕ is one-one

(*iii*) ϕ is onto.

Example 1. *Let G be a non-abelian group and $f : G \to G$ be defined by $f(x) = x^{-1}$. Show that f is not an automorphism.*

Sol. Let $x, y \in G$.

$\therefore$ $$f(xy) = (xy)^{-1} = y^{-1}x^{-1}$$

and $$f(x)\,f(y) = x^{-1}y^{-1}.$$

Since $y^{-1}x^{-1}$ and $x^{-1}y^{-1}$ may not be equal, we have

$$f(xy) \neq f(x)\,f(y), \text{ in general.}$$

$\therefore$ f is not an automorphism.

Example 2. *Let $G = (a)$, $a^{12} = e$ be a cyclic group of order 12. Let $f : G \to G$ be defined by $f(x) = x^5 \forall x \in G$. Show that f is not an automorphism.*

Sol. $a, a^5 \in G$ and $a \neq a^5$.

Also, $$f(a) = a^3 \text{ and}$$

$$f(a^5) = (a^5)^3 = a^{15} = a^{12}\,a^3 = ea^3 = a^3$$

$\therefore$ $$f(a) = f(a^5)$$

$\therefore$ f is not one-one.

$\therefore$ f is not an automorphism.

Example 3. *Let G be the group of positive real numbers under multiplication. Let $\phi : G \to G$ be defined by $\phi(x) = x^2$, $x \in G$. Show that ϕ is an automorphism.*

Sol. We have $\phi(x) = x^2, x \in G$.

ϕ is a homomorphism. Let $x, y \in G$.

$$\phi(xy) = (xy)^2 = x^2y^2 = \phi(x)\,\phi(y).$$

$\therefore$ ϕ is a homomorphism from G to G.

ϕ is one-one. Let $x, y \in G$ and $\phi(x) = \phi(y)$.

$\Rightarrow \quad x^2 = y^2 \Rightarrow x = \pm y \Rightarrow x = y \qquad (\because \ x, y \text{ are both +ve})$

$\therefore \quad \phi(x) = \phi(y) \Rightarrow x = y \quad \therefore \ \phi$ is one-one.

ϕ is onto. Let $x \in G$.

$\therefore$ x is a +ve real number.

$\therefore$ $\sqrt{x}$ is also a +ve real number.

We have $\phi(\sqrt{x}) = (\sqrt{x})^2 = x \quad \therefore \ \phi$ is onto.

$\therefore$ ϕ is an automorphism of G.

Example 4. ***Let G be any group in which $a^2 \neq e$ for some $a \in G$. show that G has a non-trivial automorphism.***

Sol. Let f be any automorphism of G.

If possible, let $f(a) = e$.

$\therefore \quad f(a^2) = f(aa) = f(a)\,f(a) = ee = e$

Also, $f(e) = e$

$\therefore \quad f(a^2) = f(e)$

$\Rightarrow \quad a^2 = e \qquad (\because \ f \text{ is 1-1})$

This is impossible. $\therefore \ f(a) \neq e$.

$\therefore$ f is a non-trivial automorphism of G.

$\therefore$ G has nontrivial automorphisms.

Example 5. *Let G be a group. Show that the mapping $x \to x^{-1}$ from G to G is an automorphism if and only if G is abelian.*

Sol. Let $f : G \to G$ be the mapping defined by $f(x) = x^{-1}, x \in G$. Let the group G be abelian.

f is well defined. Since inverse of an element is uniquely defined, the mapping f is well defined.

f is a homomorphism. Let $x, y, \in G$.

$$f(xy) = (xy)^{-1} = y^{-1}x^{-1} = x^{-1}y^{-1} = f(x)f(y) \qquad (\because \ y^{-1}x^{-1} = x^{-1}y^{-1})$$

$\therefore$ f is a homomorphism.

f is one-one. Let $x, y \in G$ and $f(x) = f(y)$.

$\Rightarrow \quad x^{-1} = y^{-1} \Rightarrow (x^{-1})^{-1} = (y^{-1})^{-1} \Rightarrow x = y.$

$\therefore$ f is one-one.

f is onto. Let $x \in G$.

$\therefore \quad x^{-1} \in G \quad \text{and} \quad f(x^{-1}) = (x^{-1})^{-1} = x$

$\therefore$ f is onto.

$\therefore$ f is an automorphism of the group G.

Conversely, let f be an automorphism of group G. Let $x, y \in G$.

$\therefore \quad f(xy) = f(x)f(y) = x^{-1}y^{-1} = (yx)^{-1} = f(yx)$

Since f is one-one, we have $xy = yx$.

$\therefore$ The group G is abelian.

Example 6. *Let G be a finite abelian group of order n, and let m be a positive integer prime to n. Show that the mapping $f : G \to G$ defined by $f(x) = x^m, x \in G$ is an automorphism of G.*

Sol. We have $f(x) = x^m, x \in G$.

f is a homomorphism.

For $x, y \in G$,

$$f(xy) = (xy)^m = (xy)(xy) \ldots\ldots n \text{ times}$$
$$= (xx \ldots\ldots m \text{ times})(yy \ldots\ldots m \text{ times}) \qquad (\because G \text{ is abelian})$$
$$= x^m y^m = f(x)\, f(y).$$

$\therefore$ f is a homomorphism.

f is one-one. Since $(m, n) = 1$, there exists integers p, q such that $mp + nq = 1$.

$\therefore$ For $x \in G$, $x^{mp+nq} = x^1$

$\Rightarrow$ $x^{mp}\, x^{nq} = x \Rightarrow x^{mp}\,(x^n)^q = x \Rightarrow x^{mp}(e)^q = x \Rightarrow x^{mp} e = x \Rightarrow x^{mp} = x.$

$\therefore$ $x^{mp} = x \;\forall\, x \in G$

Let $x, y \in G$ and $f(x) = f(y)$.

$\Rightarrow$ $x^m = y^m \Rightarrow (x^m)^p = (y^m)^p \Rightarrow x^{mp} = y^{mp} \Rightarrow x = y.$

$\therefore$ f is one-one.

f is onto. Let $x \in G$.

$\therefore$ $x^p \in G$ and $f(x^p) = (x^p)^m = x^{mp} = x$

$\therefore$ f is onto. $\therefore$ f is an automorphism of G.

Example 7. *Let $f : G \to G$ be defined by $f(a) = a^n \;\forall\, a \in G$. If f is an automorphism then show that $a^{n-1} \in Z \;\forall\, a \in G$.*

Sol. Let $a, x \in G$. $\therefore$ $a^{-n}xa^n \in G$

$\therefore$ $f(a^{-n}xa^n) = (a^{-n}xa^n)^n$

$= (a^{-n}xa^n)(a^{-n}xa^n) \ldots\ldots n$ times

$= a^{-n}x(a^n a^{-n})\, x(a^n a^{-n})\, x \ldots\ldots a^n$

$= a^{-n}xexex \ldots\ldots a^n$

$= a^{-n}x^n a^n = (a^{-1})^n\, x^n a^n = f(a^{-1}) f(x) f(a)$

$= f(a^{-1}xa)$ $\qquad (\because$ f is a hom.)

$\Rightarrow$ $a^{-n}xa^n = a^{-1}xa$ $\qquad (\because$ f is 1-1)

$\Rightarrow$ $a^n(a^{-n}xa^n)a^{-1} = a^n(a^{-1}xa)a^{-1}$ $\qquad$ *(Note this step)*

$\Rightarrow$ $(a^n a^{-n})\, x(a^n a^{-1}) = (a^n a^{-1})\, x(aa^{-1})$

$\Rightarrow$ $exa^{n-1} = a^{n-1}\, xe$

$\Rightarrow$ $xa^{n-1} = a^{n-1}x \;\forall\, a, x \in G$

$\Rightarrow$ $a^{n-1} \in Z \;\forall\, a \in G.$

Theorem 1. *Let f be an automorphism of a group G. If H is a subgroup of group G, then $f(H)$ is also a subgroup of G.*

Proof. We have $f(H) = \{f(h) : h \in H\}$.

$e \in H \Rightarrow f(e) \in f(H)$ $\therefore$ $f(H) \neq \phi$

Let $f(h_1), f(h_2) \in f(H)$

Now $f(h_1)(f(h_2))^{-1} = f(h_1)\, f(h_2^{-1}) = f(h_1 h_2^{-1}) \in f(H)$

$\qquad (\because \quad h_1, h_2 \in H \Rightarrow h_1 h_2^{-1} \in H)$

$\therefore$ $f(H)$ is a subgroup of G.

Theorem 2. *Let f be an automorphism of a group G. If N is a normal subgroup of group G, then $f(N)$ is also a normal subgroup of G.*

Proof. We have $f(N) = \{f(n) : n \in N\}$.

$e \in N \Rightarrow f(e) \in f(N)$ $\therefore$ $f(N) \neq \phi$

Let $f(n_1), f(n_2) \in f(N)$

Now $f(n_1)(f(n_2))^{-1} = f(n_1)f(n_2^{-1}) = f(n_1 n_2^{-1}) \in f(N)$

$(\because \quad n_1, n_2 \in N \Rightarrow n_1 n_2^{-1} \in N)$

$\therefore$ $f(N)$ is a subgroup of G.

Let $f(n) \in f(N)$ and $g \in G$. Since f is onto, there exists $x \in G$ such that $g = f(x)$.

Now $gf(n)g^{-1} = f(x)f(n)(f(x))^{-1} = f(x)f(n)f(x^{-1}) = f(xnx^{-1}) \in f(N)$

$(\because \quad n \in N, x \in G \Rightarrow xnx^{-1} \in N)$

$\therefore$ $f(N)$ is a normal subgroup of G.

Example 8. *Let G be a group and Z, the centre of G. If f is any automorphism of G, show that* $f(Z) \subseteq Z$.

Sol. We have $Z = \{z \in G : zx = xz \ \forall \ x \in G\}$.

Let $f(z) \in f(Z)$. Let x be any element of G. Since f is onto, there exists $y \in G$ such that $f(y) = x$.

Now $f(z) \in f(Z) \Rightarrow z \in Z$

$\Rightarrow$ $zy = yz \Rightarrow f(zy) = f(yz)$

$\Rightarrow$ $f(z)f(y) = f(y)f(z) \Rightarrow f(z)x = xf(z)$

$\therefore$ $f(z) \in Z \quad \therefore \quad f(Z) \subseteq Z$.

Example 9. *Let G be a group and f, an automorphism of G. If for* $a \in G$, $N(a) = \{x \in G : ax = xa\}$, *show that* $N(f(a)) = f(N(a))$.

Sol. We have $N(a) = \{x \in G : ax = xa\}$.

$\therefore$ $N(f(a)) = \{x \in G : f(a)x = xf(a)\}$

Let $x \in N(f(a))$.

$\Rightarrow$ $f(a)x = xf(a) \Rightarrow f(a)f(y) = f(y)f(a)$ (Taking $x = f(y), y \in G$)

$\Rightarrow$ $f(ay) = f(ya) \Rightarrow ay = ya$ ($\because$ f is one-one)

$\Rightarrow$ $y \in N(a) \Rightarrow f(y) \in f(N(a))$ *i.e.,* $x \in f(N(a))$

$\therefore$ $N(f(a)) \subseteq f(N(a))$.

Now, let $b \in f(N(a)) \quad \therefore \quad \exists\, c \in N(a) : f(c) = b$

$c \in N(a) \Rightarrow ac = ca$

$\Rightarrow$ $f(ac) = f(ca) \Rightarrow f(a)f(c) = f(c)f(a)$

$\Rightarrow$ $f(a)b = bf(a) \Rightarrow b \in N(f(a))$

$\therefore$ $f(N(a)) \subseteq N(f(a))$.

Combining, we get $N(f(a)) = f(N(a))$.

3. INNER AUTOMORPHISM

Let G be a group and let a be any arbitrary but fixed element of G.

Let f_a be a mapping from G into G defined by $f_a(x) = a^{-1}xa, \quad x \in G$.

f_a is well defined. Let $x, y \in G$.

$$x = y \Rightarrow a^{-1}xa = a^{-1}ya \Rightarrow f_a(x) = f_a(y)$$

$\therefore$ f_a is well defined.

f_a is a homomorphism. Let $x, y \in G$.

$$f_a(xy) = a^{-1}(xy)a = a^{-1}(x(aa^{-1})y)a = (a^{-1}xa)(a^{-1}ya) = f_a(x)\,f_a(y)$$

$\therefore$ f_a is a homomorphism.