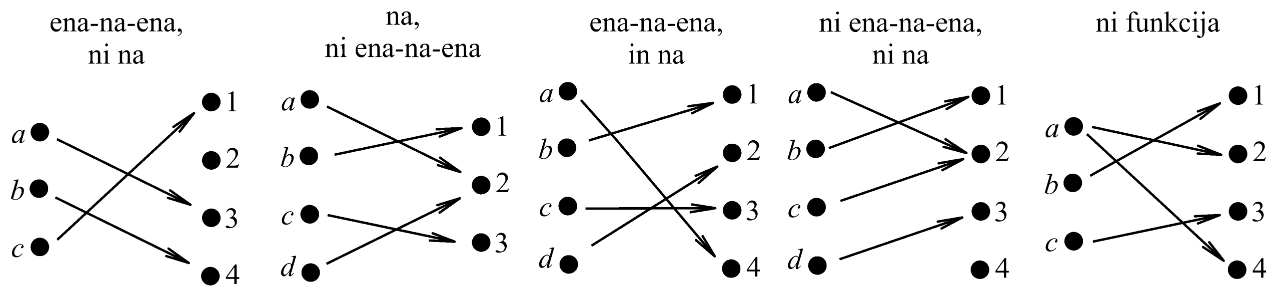
6 Homomorfizmi in izomorfizmi grup

Kdaj definiramo nekatero (novo) funkcijo vedno moramo, da preverimo, ali je ta funkcija dobro definirana. Kaj to pomeni?[12]

Definicija (injekcija, surjekcija, bijekcija) Preslikavi, ki preslika poljubna dva različna elementa v različna elementa, rečemo injektivna (ena-na-ena, $1-1$) preslikava ali injekcija. Z drugimi besedami, preslikava $f : A \to B$ je injekcija (oziroma $1-1$) če in samo če $x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$ (Ekvivalentno: $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$). Preslikavi $f : A \to B$, za katero je zaloga vrednosti kar cela množica B, rečemo surjektivna (oziroma na) preslikava ali surjekcija. Z drugimi besedami, če je $f(A) = B$, rečemo, da je f surjekcija (na). V tem primeru za vsak element $y \in B$ najdemo tak $x \in A$, da je $f(x) = y$. Preslikavi, ki je injektivna in surjektivna, rečemo bijektivna preslikava ali bijekcija (rečemo tudi povratno enolična).



Primeri različnih tipov korespondence

Definicija (homomorfizem grup) Naj bosta $(G, \cdot)$ in $(\overline{G}, \circ)$ grupi in naj bo $\phi : G \to \overline{G}$. Preslikava ϕ je homomorfizem med grupami G in $\overline{G}$ če in samo če za vsaka $g_1, g_2 \in G$ velja $\phi(g_1 g_2) = \phi(g_1) \circ \phi(g_2)$.

1. (a) Naj bo G grupa, in naj bo $\phi : G \to G$ preslikava definirana s $\phi(x) = x^{-1}$. Pokaži, da je ϕ bijekcija. (b) Naj bo $G = \langle a \rangle$, $a^{15} = e$ ciklična grupa reda 15, in naj bo $f : G \to G$ preslikava definirana z $f(x) = x^5$, $\forall x \in G$. Pokaži, da f ni injektivna funkcija.

2. Naj bo G ciklična grupa generirana z g ($G = \langle g \rangle$) in naj bo $(\mathbb{Z}, +)$ grupa celih števil glede na operacijo seštevanja. Pokaži, da je preslikava $\phi : \mathbb{Z} \to G$ definirana s $\phi(n) = g^n$ homomorfizem med grupami $\mathbb{Z}$ in G.

3. Dani sta grupi $(\mathbb{Z}_9, +)$ in $(\mathbb{Z}_3, +)$. Poišči vse homomorfizme iz grupe $\mathbb{Z}_9$ v grupo $\mathbb{Z}_3$.

4. Dana je grupa $G = \{1, 2, ..., 12\}$ z operacijo množenja po modulu 13. Določi vse homomorfizme iz grupe G v grupo $(\mathbb{Z}_6, +)$.

5. Dana sta grupi $(\mathrm{GL}_2(\mathbb{R}), \cdot)$ in $(\mathbb{R}^*, \cdot)$ (kje sta $\mathrm{GL}_2(\mathbb{R}) = \{A \in \mathrm{Mat}_{2\times 2}(\mathbb{R}) \mid \exists A^{-1}\} = \{\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{Mat}_{2\times 2}(\mathbb{R}) \mid ad - bc \neq 0\}$ in $\mathbb{R}^* = \{x \in \mathbb{R} \mid x \neq 0\}$). Pokaži, da je preslikava $\phi : \mathrm{GL}_2(\mathbb{R}) \to \mathbb{R}^*$ definirana s $\phi(A) = \det(A)$ homomorfizem med grupami $\mathrm{GL}_2(\mathbb{R})$ in $\mathbb{R}^*$.

6. Dani sta grupi $(\mathbb{T}, \cdot)$ in $(\mathbb{R}, +)$ (kje je $\mathbb{T} = \{z \in \mathbb{C} : |z| = 1\}$. Pokaži, da obstaja homomorfizem med $\mathbb{R}$ in $\mathbb{T}$.

Definicija (izomorfizem grup)

Preslikava $\phi : G \to H$ grupe $(G, \cdot)$ v grupo $(H, \circ)$ se imenuje izomorfizem iz grupe G v grupo H če in samo če

(i) ϕ je injekcija;

(ii) ϕ je surjekcija;

(iii) $\phi(ab) = \phi(a) \circ \phi(b)$ za vse $a, b \in G$ (ϕ je homomorfizem).

Če obstaja izomorfizem iz G v H, pravimo, da sta G in H izomorfni. Oznaka $G \cong H$.[13]

[12] **Dobro definirana** Glej relacijo $f : \mathbb{Q} \to \mathbb{Z}$ danu s $f(p/q) = p$. Vemo, da $1/2 = 2/4$, ampak kaj je $f(1/2)$, $f(1/2) = 1$ ali $= 2$. Ta relacija ne more biti preslikava ker ni dobro definirana. Relacija je dobro definirana, če vsak element v domenu je dodeljen edinstvenemu elementu v rangu.

[13] **Opomba.** Obstajajo štiri koraki, ki jih moramo izvesti, da bi pokazali, da je grupa G izomorfna z grupo $\overline{G}$. **1.**: "Preslikava". Definirajmo kandidata za izomorfizem, tj. definirajmo funkcijo ϕ iz G v $\overline{G}$. **2.**: "Injekcija". Dokažimo da je ϕ injekcija, tj. domnevamo, da je $\phi(a) = \phi(b)$ in pokažimo, da je $a = b$. **3.**: "Surjekcija". Dokažimo, da je ϕ surjekcija, tj. za poljubni element $\overline{g} \in \overline{G}$ najdimo element $g \in G$ tako da je $\phi(g) = \overline{g}$. **4.**: "Homomorfizem". Dokažimo, da je ϕ homomorfizem, tj. za poljubna elementa $a, b \in G$ pokažemo, da je $\phi(ab) = \phi(a)\phi(b)$.

Izrek (Cayley-ev izrek (1854)) Vsaka grupa je izomorfna neki permutacijski grupi.

Theorem (lastnosti elementov glede na izomorfizem)
Naj bo ϕ izomorfizem iz grupe G v grupo $\overline{G}$. Potem

1. ϕ preslikava identiteto grupe G v identiteto grupe $\overline{G}$.
2. Za vsako celo število n in za vsak element grupe $a \in G$, $\phi(a^n) = [\phi(a)]^n$.
3. Za vsaka dva elementa a in b v G, a in b komutirajo, če in samo če $\phi(a)$ in $\phi(b)$ komutirajo.
4. $G = \langle a \rangle$ če in samo če $\overline{G} = \langle \phi(a) \rangle$.
5. $|a| = |\phi(a)|$ za vsak a v G (isomorphisms preserve orders).
6. Za fiksirano celo število k in za fiksirani element grupe $b \in G$ enačba $x^k = b$ ima isto število rešitev v G kot in $x^k = \phi(b)$ v $\overline{G}$.
7. Če je G končen, potem G in $\overline{G}$ imajo isto število elementov končnega reda.

Izrek (lastnosti grupe glede na izomorfizem) Naj bo ϕ izomorfizem iz grupe G v grupo $\overline{G}$. Potem [1.] ϕ^{-1} je izomorfizem iz $\overline{G}$ v G. [2.] G je abelska če in samo če $\overline{G}$ je abelska. [3.] G je ciklična če in samo če $\overline{G}$ je ciklična. [4.] Če je K podgrupa...[14]

7. Dokaži Cayley-ev izrek zgoraj.

8. Dokaži izrek lastnosti elementov glede na izomorfizem zgoraj.

9. Naj bo $G = \mathbb{Z}_3 \times \mathbb{Z}_3$ in $H = \mathbb{Z}_9$. Ali je $G \cong H$? Odgovor utemelji!

10. Dana sta dve grupi $(\mathbb{Z}_4, +)$ in $(\langle i \rangle, \cdot)$ kje je $i = \sqrt{-1} \in \mathbb{C}$. Naj bo $\phi : \mathbb{Z}_4 \to \langle i \rangle$ preslikava definirana s $\phi(n) = i^n$. Pokaži, da je ϕ izomorfizem grupe $\mathbb{Z}_4$ na grupo $\langle i \rangle$.

11. Naj bo G grupa celih števil glede na operacijo seštevanja in naj bo $\overline{G}$ podgrupa grupe $\mathbb{Q}^*$ ki vsebuje elemente oblike 2^n. Definirajmo preslikavo $\phi : G \to \overline{G}$ na naslednji način: $\phi(n) = 2^n$. Pokaži, da ϕ je izomorfizem iz G v $\overline{G}$.

12. Dana je grupa $(\mathbb{R}, +)$ in dana je preslikava $\phi : \mathbb{R} \to \mathbb{R}$ definirana s $\phi(x) = x^3$. Preveri, ali je ϕ izomorfizem grupe G nase.

13. Naj bo $G = \mathrm{SL}_2(\mathbb{R})$ grupa vsih realnih metrik oblike 2×2, katerih vrednost determinante je enaka 1, in naj bo M neke 2×2 realna metrik t.d. $\det(M) = 1$. Pokaži, da je preslikava $\phi : G \to G$ definirana s $\phi_M(A) = MAM^{-1}$ izomorfizem grupe G nase.

14. (a) Naj bo G grupa realnih števil glede na operacijo seštevanja in naj bo $\overline{G}$ grupa pozitivnih realnih števil glede na operacijo množenja. Pokaži, da sta G in $\overline{G}$ izomorfni grupi.

(b) Naj bo G neskončna ciklična grupa in naj bo $\overline{G}$ grupa celih števil glede na operacijo seštevanja. Pokaži, da sta G in $\overline{G}$ izomorfni grupi.

15. (a) Pokaži, da je $U(10) \cong \mathbb{Z}_4$. (b) Pokaži, da $U(10) \ncong U(12)$.

16. (a) Dana sta grupi $(\mathbb{Q}, +)$ in $(\mathbb{Q}^*, \cdot)$. Pokaži, da $\mathbb{Q} \ncong \mathbb{Q}^*$. (b) Naj bo G ciklična grupa reda n. Pokaži, da je $G \cong \mathbb{Z}_n$.

Definicija (automorfizem grupe G) Preslikava ϕ iz grupe G samo vase se imenuje automorfizem grupe G če in samo če (i) $\phi(ab) = \phi(a)\phi(b)$ za $\forall a, b \in G$; (ii) ϕ je injekcija; (iii) ϕ je surjekcija.

17. (a) Naj bo G ne-abelska grupa in naj bo $f : G \to G$ definirana s $f(x) = x^{-1}$. Pokaži, da f ni automorfizem.

(b) Naj bo $G = \langle a \rangle$, $a^{12} = e$ ciklična grupa reda 12, in naj bo $f : G \to G$ preslikava definirana na naslednji način: $f(x) = x^3$, $\forall x \in G$. Pokaži, da f ni automorfizem.

18. Pišči $\mathrm{Aut}(\mathbb{Z}_{10})$ (vse automorfizme grupe $\mathbb{Z}_{10}$). Ali je $\mathrm{Aut}(\mathbb{Z}_{10}) \cong U(10)$?

19. Naj bo G grupa pozitivnih realnih števil glede na operacijo množenja. Naj bo $\phi : G \to G$ definirano s $\phi(x) = x^2$, $x \in G$. Pokaži, da je ϕ automorfizem.

[14] Zadnja dva izreka zagotavljata nekoliko primernih načinov za dokazovanje, da grupe G in $\overline{G}$ nista izomorfni. **1.** Upoštevajte, da je $|G| \neq |\overline{G}|$. **2.** Upoštevajte, da G ali $\overline{G}$ je ciklična, druga pa ni. **3.** Upoštevajte, da G ali $\overline{G}$ je abelska, druga pa ni. **4.** Pokaži, da največji red katerega koli elementa v G ni enak največjemu redu katerega koli...

Joseph Lagrange

> Lagrange is the Lofty Pyramid of the Mathematical Sciences.
>
> *Napoleon Bonaparte,*

Joseph Louis Lagrange was born in Italy of French ancestry on January 25, 1736. He became captivated by mathematics at an early age when he read an essay by Halley on Newton's calculus. At the age of 19, he became a professor of mathematics at the Royal Artillery School in Turin. Lagrange made significant contributions to many branches of mathematics and physics, among them the theory of numbers, the theory of equations, ordinary and partial differential equations, the calculus of variations, analytic geometry, fluid dynamics, and celestial mechanics. His methods for solving third- and fourth-degree polynomial equations by radicals laid the groundwork for the group theoretic approach to solving polynomials taken by Galois. Lagrange was a very careful writer with a clear and elegant style.

At the age of 40, Lagrange was appointed head of the Berlin Academy, succeeding Euler. In offering this appointment, Frederick the Great proclaimed that the "greatest king in Europe" ought to have the "greatest mathematician in Europe" at his court. In 1787, Lagrange was invited to Paris by Louis XVI and became a good friend of the king and his wife, Marie Antoinette. In 1793, Lagrange headed a commission, which included Laplace and Lavoisier, to devise a new system of weights and measures. Out of this came the metric system. Late in his life he was made a count by Napoleon. Lagrange died on April 10, 1813.

POMEMBNI REZULTATI (Homomorfizmi. Izomorfizmi.)

1. Če je ϕ homomorfizem iz grupe G v grupo G' potem $\phi(e) = e'$.
2. Če je ϕ homomorfizem iz grupe G v grupo G' potem $\phi(a^{-1}) = [\phi(a)]^{-1}\ \ \forall a \in G$.
3. Če je ϕ izomomorfizem iz grupe G v grupo G' potem $\phi(a^n) = [\phi(a)]^n\ \ \forall a \in G$.
4. Naj bo $\phi : G \to G'$ izomomorfizem. Potem $G = \langle a \rangle$ če in samo če je $G' = \langle \phi(a) \rangle$.
5. Če je ϕ izomomorfizem iz grupe G v grupo G' potem $o(a) = o[\phi(a)]\ \ \forall a \in G$.
6. Naj bo $\phi : G \to G'$ surjektivni homomorfizem. Potem je homomorfizem ϕ izomorfizem iz grupe G v grupo G' če in samo če $\ker(\phi) = \{e\}$.
7. Naj bo $\phi : G \to G'$ izomomorfizem. Potem je ϕ^{-1} izomomorfizem iz grupe G' v grupo G.

Rešitve: **1.**(a) $[x^{-1} = y^{-1} \Rightarrow x = y,\ (x^{-1})^{-1} = x]$; (b) $[f(a) = a^5 = f(a^4)]$. **2.** $[\phi(m+n) = g^{m+n} = g^m g^n = \phi(m)\phi(n)]$ **3.** $[\phi_1(x) = 0,\ \forall x \in \mathbb{Z}_9;\ \phi_2(x) = x \bmod 3,\ \forall x \in \mathbb{Z}_9;\ \phi_3(x) = 2x \bmod 3,\ \forall x \in \mathbb{Z}_9]$ **4.** [Obstaja 6 različnih homomorfizema, $\phi : G \to \mathbb{Z}_6$, $2^k \to ka$ za $a \in \{0,1,2,3,4,5,6\}$] **5.** $[\phi(AB) = \det(AB) = \det(A)\det(B) = \phi(A)\phi(B)]$ **6.** $[\phi : \mathbb{R} \to \mathbb{T},\ \phi(\theta) = \cos(\theta) + i\sin(\theta)]$ **7.** [G, $\overline{G} =$? t.d. $G \cong \overline{G}$; za $g \in G$ naj bo $T_g : G \to G$ t.d. $T_g(x) = gx$ $(\forall x \in G) \Rightarrow T_g$ je permutacija; $\overline{G} := \{T_g \mid g \in G\} \Rightarrow \overline{G}$ je grupa; $\forall g \in G$ definirajmo $\phi(g) = T_g$, ϕ je 1-1, na in homomorfizem] **8.** [(1.) $\phi(e) = \phi(ee) = \phi(e)\phi(e)$, $\phi(e) \in \overline{G}$, $\phi(e) = \overline{e}\phi(e)$, $\overline{e} = \phi(e)$] [(2.) 1° $n \in \mathbb{N}$, uporabi matematično indukcijo; 2° $n \in \mathbb{Z}^- \Rightarrow -n \in \mathbb{N}$, $e = \phi(e) = \phi(g^n g^{-n}) = \phi(g^n)\phi(g^{-n}) = \phi(g^n)(\phi(g))^{-n}$, $(\phi(g))^n = \phi(g^n)$; 3° $n = 0$] [(4.) $G = \langle a \rangle$, $\langle \phi(a) \rangle \subseteq \overline{G}$, ϕ surjekcija $\Rightarrow \forall b \in \overline{G}\ \exists a^k \in G$ t.d. $\phi(a^k) = b$, $b = (\phi(a))^k$, $b \in \langle \phi(a) \rangle \Rightarrow \overline{G} \subseteq \langle \phi(a) \rangle$; $\overline{G} = \langle \phi(a) \rangle \Rightarrow \langle a \rangle \subseteq G$, $\forall b \in G\ \phi(b) \in \langle \phi(a) \rangle$, $\exists k \in \mathbb{Z}\ \phi(b) = (\phi(a))^k = \phi(a^k)$, ϕ injekcija $\Rightarrow b = a^k$, $\langle a \rangle = G$] **9.** $[G \ncong H,\ \forall (a,b) \in \mathbb{Z}_3 \times \mathbb{Z}_3\ |(a,b)| \le 3]$ **10.** [$\phi(0) = 1$, $\phi(1) = i$, $\phi(2) = -1$, $\phi(3) = -i \Rightarrow \phi$ je surjekcija in injekcija] **11.** $[2^m = 2^n \Rightarrow m = n,\ \phi(m+n) = 2^{m+n} = 2^m 2^n = \phi(m)\phi(n)]$ **12.** [ϕ ni homomorfizem] **13.** [$\phi(A) \in G$?, $\det(MAM^{-1}) = \det(M)\det(A)\det(M^{-1}) = 1$, $\phi(AB) = M(AB)M^{-1} = (MAM^{-1})(MBM^{-1}) = \phi(A)\phi(B)$, $\forall C \in G\ \phi(M^{-1}CM) = M$] **14.**(a) $[\phi : G \to \overline{G},\ \phi(x) = e^x]$; (b) $[G = \langle a \rangle,\ \phi : G \to \overline{G},\ \phi(a^k) = k]$ **15.**(a) $[\phi : U(10) \to \mathbb{Z}_4,\ \phi(3^k) = k \bmod 4]$; (b) $[U(10) = \{1,3,7,9\},\ U(12) = \{1,5,7,11\},\ x^2 = 1$ za $\forall x \in U(12),\ \phi(9) = \phi(1)]$ **16.**(a) $[-1 = (\phi(\frac{a}{2}))^2]$; (b) $[\phi : G \to \mathbb{Z}_n,\ \phi(a^k) = k \bmod n]$ **17.**(a) $[f(xy) = (xy)^{-1} = y^{-1}x^{-1},\ f(x)f(y) = x^{-1}y^{-1},\ f$ ni homomorfizem$]$

(b) [f ni surjekcija in f ni injekcija; npr. $f(a) = a^3 = ea^3 = = a^{12}a^3 = a^{15} = (a^5)^3 = f(a^5) \Rightarrow f$ ni injekcija; $f(a^k) = a^4 \Rightarrow a^{3k} = a^4 \Rightarrow 3k \bmod 12 = 4 \Rightarrow 3k = 12q + 4 \Rightarrow 3(k - 4q) = 4$ #protislovje $\Rightarrow f$ ni surjekcija] **18.** [$\alpha(1) =?$, $\alpha(k) = \alpha(1 + 1 + ... + 1) = \alpha(1) + ...+ \alpha(1) = k\alpha(1)$, $|1| = 10 \Rightarrow |\alpha(1)| = 10$ (npr. $\alpha(0) = 0$, $\alpha(0) = \alpha(10) = \alpha(1 + 1 + ... + 1) = \alpha(0) + ... + \alpha(0)$), $|\alpha(1)| = 10 \Rightarrow \alpha(1) \in \{1, 3, 7, 9\}$; $\alpha_1(1) := 1$, $\alpha_3(1) := 3$, $\alpha_7(1) := 7$, $\alpha_9(1) := 9$. 1° $\alpha_1 = \mathrm{id}$; 2° $x \bmod 10 = y \bmod 10 \Rightarrow 3x \bmod 10 = 3y \bmod 10 \Rightarrow \alpha_3$ je dobro definirana, α_3 je surjekcija, α_3 je injekcija, $\alpha_3(a + b) = 3(a + b) = 3a + 3b = \alpha_3(a) + \alpha_3(b) \Rightarrow \alpha_3$ je homomorfizem; ... $\alpha_3, \alpha_7, \alpha_9 \in \mathrm{Aut}(\mathbb{Z}_{10})$, $\alpha_3\alpha_3 = \alpha_9$ (npr. $(\alpha_3\alpha_3)(1) = \alpha_3(3) = 3 \cdot 3 = 9 = \alpha_9(1)$, $|\alpha_3| = 4$,... $\mathrm{Aut}(10) \cong U(10)$)] **19.** [$\phi(ab) = (ab)^2 = a^2b^2 = \phi(a)\phi(b)$; $\phi(x) = \phi(y) \Rightarrow x^2 = y^2$, $x, y > 0 \Rightarrow x = y$; $x \in G \Rightarrow \sqrt{x} \in G$, $\phi(\sqrt{x}) = x$]

Appendix.[15][16][17]

groups	
named groups	`S4 := Sym(4);`
	`A4 := AlternatingGroup(4);`
	`Z5 := CyclicGroup(5);`
	`D10 := DihedralGroup(10);`
group by order	`NumberOfSmallGroups(8);`
	`// first group of order 8:`
	`G := SmallGroup(8, 1);`
group from permutation generators	`S5 := Sym(5);`
	`p1 := S5!(1, 3, 5, 2);`
	`p2 := S5!(1, 2);`
	`G := PermutationGroup<5 | p1, p2>;`
direct product	`Z3 := CyclicGroup(3);`
	`A4 := AlternatingGroup(4);`
	`G := DirectProduct(Z3, A4);`
generators	`S10 := Sym(10);`
	`Generators(S10);`
	`// notation for individual generators:`
	`S10.1;`
	`S10.2;`
identity element	`Id(G);`
random element	`Random(G);`
group operation	`e1 := Random(G);`
	`e2 := Random(G);`
	`e1 * e2;`
inverse element	`Inverse(e1);`
	`// or:`
	`e1 ^ -1;`
element order	`D10 := DihedralGroup(10);`
	`Order(D10.1);`
	`Order(D10.2);`
identify group	`// C2*C4:`
	`GroupName(SmallGroup(8, 2));`
	`// <8, 1>:`
	`IdentifyGroup(CyclicGroup(8));`
group to presentation	`FPGroup(AlternatingGroup(10));`
group order	`Order(Sym(4));`
cyclic test	`IsCyclic(AlternatingGroup(10));`
abelian test	`IsAbelian(CyclicGroup(10));`

[15] To write MAGMA code please open: `http://magma.maths.usyd.edu.au/calc/`

[16] See also: `http://www.maths.usyd.edu.au/u/bobh/UoS/MATH2008/ctut06.pdf`

[17] or `http://hyperpolyglot.org/more-computer-algebra`