
Polugrupe

Definicija polugrupe

Grupoid $(S, \cdot)$ u kojem je operacija $\cdot$ asocijativna naziva se *polugrupa*. Drugim rečima, zahtevamo da za sve $a, b, c \in S$ važi

$$(a \cdot b) \cdot c = a \cdot (b \cdot c).$$

Ukoliko S ima jedinicu, tj. neutralni element 1 u odnosu na $\cdot$ tako da je $1 \cdot a = a \cdot 1 = a$ za sve $a \in S$, tada je S *monoid*.

Primer 1. Monoidi su, na primer, $(\mathbb{N}, +)$, $(\mathbb{Z}, +)$, $(\mathbb{N}, \cdot)$ i $(\mathbb{Z}, \cdot)$. U prva dva monoida neutralni element je broj 0 , dok je u druga dva to broj 1 . Za proizvoljan skup A , monoidi su i $(\mathcal{P}(A), \cup)$ i $(\mathcal{P}(A), \cap)$; za prvi, neutralni element je $\emptyset$, a za drugi je to ceo skup A .

Monoidi transformacija i teorema reprezentacije

Kao što je vrlo dobro poznato, ako su $f : A \rightarrow B$, $g : B \rightarrow C$ i $h : C \rightarrow D$ funkcije (gde su A, B, C, D neki neprazni skupovi), tada važi

$$(f \circ g) \circ h = f \circ (g \circ h).$$

(Takođe, sličan zaključak sledi i za proizvoljne tri binarne relacije.) Prema tome, *transformacije skupa* A , funkcije $f : A \rightarrow A$, čine monoid, *pun monoid transformacija* $\mathcal{T}_A$, u odnosu na operaciju kompozicije funkcija i identičkim preslikavanjem id_A kao jedinicom. Kada je A konačan skup, $|A| = n$, odgovarajući pun monoid transformacija označavamo i sa $\mathcal{T}_n$.

Značaj monoida $\mathcal{T}_A$ ogleda se u *teoremi reprezentacije*: za svaku polugrupu S postoji potapanje $S \rightarrow \mathcal{T}_A$ za pogodno odabran skup A . Na taj način, do na izomorfizam, *svaka* polugrupa/monoid je polugrupa/monoid transformacija.

Teorema 2. *Za svaku polugrupu S postoji skup A takav da postoji potapanje (injektivni homomorfizam) $\psi : S \rightarrow \mathcal{T}_A$.*

Dokaz. Najpre pokazujemo da se svaka polugrupa S može potopiti u monoid. Ako S već sadrži jedinični element, nema šta da se dokazuje. U suprotnom, posmatrajmo skup $S^1 = S \cup \{1\}$ gde je $1 \notin S$ novi element, i na njemu definišimo novu operaciju $*$ sa $1 * s = s * 1 = s$ za sve $s \in S$, kao i $a * b = ab$ za sve $a, b \in S$. Rutinski se pokazuje da je ovako definisana operacija asocijativna, tj. da dodavanje novog elementa neće “pokvariti asocijativnost” stare operacije. (Na primer, ako je $a, c \in S$ i $b = 1$ tada je $(ab)c = ac = a(bc)$.)

Stoga je dovoljno dokazati teoremu pod pretpostavkom da je S monoid. Biramo $A = S$ i definišemo preslikavanje $\psi : S \rightarrow \mathcal{T}_S$ sa

$$\psi(a) = \rho_a$$

za sve $a \in S$, gde je $\rho_a : S \rightarrow S$ *desna translacija* monoida S u odnosu na element a :

$$\rho_a(x) = xa$$

za sve $x \in S$. Preslikavanje ψ je injektivno, zato što pretpostavka da je $\psi(a) = \psi(b)$ znači da je $\rho_a = \rho_b$, pa tako, specijalno, važi i

$$a = \rho_a(1) = \rho_b(1) = b.$$

(Oдавde se vidi značaj pretpostavke da je S monoid.) Takođe, za proizvoljno $x \in S$ važi

$$\rho_{ab}(x) = x(ab) = (xa)b = \rho_b(xa) = \rho_b(\rho_a(x)) = (\rho_a \circ \rho_b)(x),$$

zbog čega je $\rho_{ab} = \rho_a \circ \rho_b$, to jest

$$\psi(ab) = \psi(a) \circ \psi(b).$$

Prema tome, ψ je injektivni homomorfizam, što je i trebalo dokazati. $\square$

Polugrupe reči

Neka je X neki (konačan ili beskonačan) skup simbola, u čiju prirodu ne ulazimo; takav skup nazivamo *alfabet*, a njegove elemente *slova*. *Reč* nad X je bilo koji konačan niz slova iz X , na primer:

$$(x_1, \dots, x_n),$$

gde su $x_1, \dots, x_n \in X$ (ne nužno različiti). Ovo uključuje u prazan niz, $()$, niz dužine 0. koji zovemo *prazna reč*. Ipak, uobičajenije je da reči pišemo bez zagrada i zareza, prosto $x_1 \dots x_n$, a da praznu reč označavamo sa λ . Skup svih reči nad X se označava sa X^* .

Na skupu X^* se definiše vrlo jednostavna, prirodna operacija *konkatenacije*, dopisivanja reči, definisana sa:

$$x_1 \dots x_m \cdot y_1 \dots y_k = x_1 \dots x_m y_1 \dots y_k$$

za sve $x_1, \dots, x_m, y_1, \dots, y_k \in X$. Odmah se uočava da je reč o asocijativnoj operaciji na X^* u odnosu na koju λ predstavlja neutralni element, pa tako X^* dobija strukturu monoida koji zovemo *monoid reči*. Operacija konkatenacije takođe daje skupu $X^+ = X^* \setminus \{\lambda\}$ svih nepraznih reči nad X strukturu polugrupe, *polugrupe reči* nad X .

Drugo ime za X^* i X^+ su, redom, *slobodan monoid* i *slobodna polugrupa*. Razlog za to je što su ove strukture posebne u klasama svih monoida odnosno polugrupa: one imaju tzv. *svojstvo slobodnog preslikavanja* – bilo koja funkcija iz skupa X u neki monoid odnosno polugrupu S se jedinstveno proširuje do homomorfizma $X^* \rightarrow S$ (odn. $X^+ \rightarrow S$). Ovde navodimo samo monoidnu verziju odgovarajućeg tvrđenja.

Teorema 3. *Neka je X alfabet, S proizvoljan monoid, i $\varphi : X \rightarrow S$ proizvoljno preslikavanje. Tada postoji jedinstven homomorfizam monoida $\bar{\varphi} : X^* \rightarrow S$ takav da je*

$$\bar{\varphi}(x) = \varphi(x)$$

za svaku jednoslovnu reč x (reč dužine 1, koju u ovom smislu identifikujemo sa slovom $x \in X$).

Dokaz. Jasno, jedini “kandidat” za traženi homomorfizam može biti samo preslikavanje $\bar{\varphi} : X^* \rightarrow S$ definisano sa $\bar{\varphi}(\lambda) = 1$ i

$$\bar{\varphi}(x_1 \dots x_n) = \varphi(x_1) \cdots \varphi(x_n),$$

gde sa desne strane primenjujemo operaciju iz S . Međutim, lako se vidi da $\bar{\varphi}$ zaista jeste homomorfizam monoida:

$$\begin{aligned}\bar{\varphi}(x_1 \dots x_m) \bar{\varphi}(y_1 \dots y_k) &= \varphi(x_1) \cdots \varphi(x_m) \cdot \varphi(y_1) \cdots \varphi(y_k) \\ &= \bar{\varphi}(x_1 \dots x_m y_1 \dots y_k).\end{aligned}$$

□

Uopšteni asocijativni zakon

Kao što smo ranije definisali, polugrupe su grupoidi koji zadovoljavaju asocijativni zakon, tj. u kojima važi

$$(xy)z = x(yz)$$

sa svaka tri elementa x, y, z . U ovom odeljku pokazujemo da je u svakoj polugrupi i za svaki grupoidni izraz (term) proizvoljne složenosti (odnosno dužine) raspored zagrada u izrazu potpuno irelevantan. Odgovarajuće tvrđenje u tom smislu zovemo *uopšteni asocijativni zakon*.

Za grupoidni term t , neka w_t označava reč koja se od t dobija brisanjem svih zagrada.

Teorema 4. *Neka su t_1, t_2 grupoidni termi (nad nekim skupom promenljivih X) takvi da je $w_{t_1} = w_{t_2}$. Tada identitet $t_1 = t_2$ važi u svakoj polugrupi.*

Dokaz. Za grupoidni term t , označimo sa $\bar{t}$ grupoidni term koji se od reči w_t dobija grupisanjem zagrada na levoj strani. Na primer, ako je $t(x, y, z) = x((xy)(zy))$ tada je $\bar{t} = (((xx)y)z)y$. Jasno, tvrđenje teoreme će biti dokazano ako pokažemo da identitet $t = \bar{t}$ važi u svakoj polugrupi, jer pretpostavka teoreme povlači da su $\bar{t}_1$ i $\bar{t}_2$ jedan isti term.

Opisano pomoćno tvrđenje dokazujemo indukcijom po složenosti terma t . Zaista, ako se t sastoji od samo jednog slova, tvrđenje je trivijalno. Zato, neka je $t = t_1 \cdot t_2$ pri čemu za t_1, t_2 važi induktivna pretpostavka: $t_1 = \bar{t}_1$ i $t_2 = \bar{t}_2$ su identiteti koji važe u svakoj polugrupi. Prema tome, u svakoj polugrupi važi

$$t = \bar{t}_1 \cdot \bar{t}_2.$$

Ako se t_2 sastoji od jednog slova iz X , dokaz je završen pošto je desna strana gornje jednakosti upravo term $\bar{t}$. U suprotnom, reč w_{t_2} ima neko poslednje slovo x koje prethodi neprazan prefiks p , pa se tako term $\bar{t}_2$ zapravo poklapa sa $p' \cdot x$,

gde je p' grupoidni term koji se od reči p dobija grupisanjem zagrada na levoj strani. Prema tome, u svakoj polugrupi važe identiteti

$$t = \overline{t_1} \cdot (p' \cdot x) = (\overline{t_1} \cdot p') \cdot x,$$

gde smo u drugom koraku primenili običan asocijativni zakon (uz odgovarajuće uvrštavanje termova). No, term $\overline{t_1} \cdot p'$ je sada kraći od početnog terma t (sadrži jedno pojavljivanje promenljive manje), pa je na njega primenljiva induktivna pretpostavka; prema tome, svaka polugrupa zaodovoljava identitet

$$\overline{t_1} \cdot p' = \overline{\overline{t_1} \cdot p'}.$$

Međutim, desna strana ovog identiteta je term koji se dobija od reči $w_{t_1}p$ grupisanjem zagrada na levoj strani. Stoga, množenjem tog terma promenljivom x upravo dobijamo $\bar{t}$ (pošto je $w_t = w_{t_1}w_{t_2} = w_{t_1}px$). No, time smo upravo dokazali da $t = \bar{t}$ važi u svakoj polugrupi. $\square$

Ideali u polugrupama

Neka je S polugrupa. Za $\emptyset \neq I \subseteq S$ kažemo da je *desni ideal* ako za sve $a \in I$ i sve $s \in S$ važi $as \in I$; drugim rečima $IS \subseteq I$. Analogno, I je *levi ideal* ako je $SI \subseteq I$. Ukoliko je $I \subseteq S$ istovremeno i desni i levi ideal polugrupe S , on je njen *ideal*. Jasno, (desni, levi) ideali polugrupa su nužno potpolugrupe.

Tvrđenje 5. *Neka je S polugrupa i $\emptyset \neq X \subseteq S$. Tada je*

- (1) $XS^1 = S \cup XS$ *najmanji desni ideal od S koji sadrži X ;*
- (2) $S^1X = S \cup SX$ *najmanji levi ideal od S koji sadrži X ;*
- (3) $S^1XS^1 = S \cup XS \cup SX \cup SXS$ *najmanji ideal od S koji sadrži X .*

Dokaz. Primera radi, dokažimo samo (1), pošto se preostala dva tvrđenja dokazuju vrlo slično.

Ako je, dakle, I desni ideal od S koji sadrži X , tada za sve $s \in S$ i $x \in X$ mora biti $xs \in I$. Stoga je $XS^1 = X \cup XS \subseteq I$. S druge strane, XS^1 je zaista desni ideal, jer ako je $x \in X$ i $s, s' \in S$, tada je $(xs)s' = x(ss') \in XS$. Prema tome, XS^1 je najmanji desni ideal od S koji sadrži X . $\square$

Za (desne, leve) ideale iz tačaka (1)–(3) gornjeg tvrđenja kažemo da su *generisani* skupom X .

Kada je generišući skup jednoelementan, $X = \{a\}$, govorimo o *glavnim* (desnim, levim) idealima. Tako su aS^1 , S^1a i S^1aS^1 redom desni, levi, odnosno dvostrani ideal generisani elementom $a \in S$.

Grinove relacije

Naravno, može se dogoditi da različiti elementi neke polugrupe generišu isti desni, levi ili dvostrani ideal. *Grinove relacije* su relacije ekvivalencije na datoj polugrupi koje vrše kalsifikaciju njenih elemenata prema tome koji (desni, levi) ideal generišu. Kako ćemo ubrzo videti, ovo vodi ka različitim pojmovima deljivosti u polugrupama. Grinove relacije često predstavljaju koristan alat da se detaljnije sagleda struktura posmatrane polugrupe.

Ove relacije uobičajeno označavamo pisanim slovima $\mathcal{R}$, $\mathcal{L}$, $\mathcal{J}$, $\mathcal{H}$ i $\mathcal{D}$. Prve tri su osnovne, i definisane su sa

$$\begin{aligned} a \mathcal{R} b & \text{ akko } aS^1 = bS^1, \\ a \mathcal{L} b & \text{ akko } S^1a = S^1b, \\ a \mathcal{J} b & \text{ akko } S^1aS^1 = S^1bS^1. \end{aligned}$$

Dalje, $\mathcal{H} = \mathcal{R} \cap \mathcal{L}$ i $\mathcal{D} = \mathcal{R} \vee \mathcal{L}$. Kako nije teško pokazati da uvek važi $\mathcal{R} \circ \mathcal{L} = \mathcal{L} \circ \mathcal{R}$, sledi da se relacija $\mathcal{D}$ zapravo poklapa sa ovom kompozicijom relacija $\mathcal{R}$ i $\mathcal{L}$. Upravo zbog toga, $\mathcal{D}$ -klase neke polugrupe je zgodno prikazati kao pravougaonu tablicu u kojoj su vrste $\mathcal{R}$ -klase, kolone $\mathcal{L}$ -klase, a kvadratna polja (koja nastaju u preseku $\mathcal{R}$ -klasa i $\mathcal{L}$ -klasa) reprezentuju $\mathcal{H}$ -klase. Napominjemo da je $\mathcal{D} \subseteq \mathcal{J}$, ali da u opštem slučaju ne važi jednakost.

Neposredno iz definicija sledi sledeći opis Grinovih relacija.

Tvrđenje 6. *U svakoj polugrupi S i za sve $a, b \in S$ važi:*

- (i) $a \mathcal{R} b$ ako i samo ako $a = b$ ili postoje $x, y \in S$ tako da je $b = ax$ i $a = by$.
- (ii) $a \mathcal{L} b$ ako i samo ako $a = b$ ili postoje $x, y \in S$ tako da je $b = xa$ i $a = yb$.
- (iii) $a \mathcal{J} b$ ako i samo ako postoje $p, q, x, y \in S^1$ tako da je $b = paq$ i $a = xby$.

Na primer, u monoidu (polugrupi) reči X^* (X^+) sve Grinove relacije su trivijalne: na primer, ako za dve reči $u, v \in X^*$ važi $v = ux$ i $u = vy$ za neke $x, y \in S^*$ tada je $u = uxy$, odakle odmah sledi da obe reči x, y moraju biti prazne, tj. $u = v$.

Idempotenti i regularne polugrupe

Element $e \in S$ polugrupe S je *idempotent* ako je $e^2 = e$. Skup svih idempotentnih elemenata S označavamo sa $E(S)$.

Tvrđenje 7. Transformacija $f \in \mathcal{T}_X$ je idempotentna ako i samo ako je svaka njena slika ujedno i njena fiksna tačka, tj. ako je $f|_{\text{Im}(f)} = \text{id}_{\text{Im}(f)}$.

Dokaz. Neka je $y \in \text{Im}(f) \subseteq X$. Tada postoji $x \in X$ tako da je $y = f(x)$. Ako pretpostavimo da je $f \circ f = f$, tada je $f(f(x)) = f(x)$, tj. $f(y) = y$. Obratno, za sve $x \in X$ mora biti $f(f(x)) = f(x)$, budući da je $f(x) \in \text{Im}(f)$; no, tada je $f \circ f = f$. $\square$

Sledeći rezultat dovodi u vezu idempotente i Grinove relacije.

Tvrđenje 8. (1) Svaki idempotent $e \in E(S)$ je leva jedinica u odnosu na svoju $\mathcal{R}$ -klasu: ako je $e \mathcal{R} a$ onda je $ea = a$.

(2) Svaki idempotent $e \in E(S)$ je desna jedinica u odnosu na svoju $\mathcal{L}$ -klasu: ako je $e \mathcal{L} a$ onda je $ae = a$.

(3) Svaki idempotent $e \in E(S)$ je dvostrana jedinica u odnosu na svoju $\mathcal{H}$ -klasu: ako je $e \mathcal{H} a$ onda je $ae = ea = a$.

(4) Svaka $\mathcal{H}$ -klasa sadrži najviše jedan idempotent.

Dokaz. (1): Ako je $e \mathcal{R} a$ tada je $a = ex$ za neko $x \in S$, pa je $ea = e^2x = ex = a$. Tvrđenje (2) se dokazuje analogno, a (3) je posledica od (1) i (2). Najzad, ako bi neka $\mathcal{H}$ -klasa H sadržala idempotente e_1, e_2 , tada bi po prethodnom važio $e_1 = e_1e_2 = e_2$ (jer je e_1 leva jedinica u svojoj $\mathcal{R}$ -klasi, a e_2 desna jedinica u svojoj $\mathcal{L}$ -klasi, pri čemu obe navedene klase sadrže H kao podskup). $\square$

U ranije opisanoj pravougaonoj skici tipične $\mathcal{D}$ -klase uobičajeno je da se idempotenti označe zvezdicom (a ponekad se $\mathcal{H}$ -klase koje ih sadrže i osenče). Na taj način dobijamo ono što se u teoriji polugrupa obično naziva *egg-box diagram* (zbog tačke (4) iz prethodnog tvrđenja). Uvođenje jedne dodatne, a ključne osobine polugrupa i njenih elemenata nam omogućava da o izgledu takvih dijagrama kažemo nešto više.

Za element a polugrupe S kažemo da je *regularan* ako postoji $x \in S$ tako da je $axa = a$. (Primetimo da tada postoji i element $y \in S$ sa osobinom da je $aya = a$ i $y = yay$ – i takav element zovemo *inverz* od a – naime, $y = xax$ ima u osobinu ako je $axa = a$.)

Polugrupa S je regularna ako je regularan svaki njen element.

Tvrđenje 9. (1) Neka je $a \in S$ regularan element, pri čemu je $x \in S$ takav da je $axa = a$. Tada su $ax, xa \in E(S)$, pri čemu je $a \mathcal{R} ax$ i $a \mathcal{L} xa$.

(2) Ako je $a \mathcal{R} e$ za neki $e \in E(S)$ tada je a regularan element.

(3) Ako je $a \mathcal{L} e$ za neki $e \in E(S)$ tada je a regularan element.

Dokaz. Iz $axa = a$ očigledno sledi $(ax)^2 = axax = ax$ i $(xa)^2 = xaxa = xa$. Takođe, $a = (ax)a = a(xa)$ povlači da je $a \mathcal{R} ax$ i $a \mathcal{L} xa$. Ako je $a \mathcal{R} e$ za neki $e \in E(S)$ tada je $e = ax$ za neko $x \in S$, pa je po tački (1) prethodnog tvrđenja

$$a = ea = axa,$$

što pokazuje da je element a regularan. Slično se dokazuje i (3). $\square$

Posledica 10. Ako neka $\mathcal{D}$ -klasa polugrupe S sadrži bar jedan regularan element, onda su svi elementi te $\mathcal{D}$ -klase regularni. (Takve $\mathcal{D}$ -klase zovemo regularnim $\mathcal{D}$ -klasama.) U regularnoj $\mathcal{D}$ -klasi, svaka $\mathcal{R}$ -klasa i svaka $\mathcal{L}$ -klasa sadrži bar jedan idempotent. Prema tome, regularne $\mathcal{D}$ -klase su tačno one koje sadrže idempotente.

Dokaz. Neka je a regularan element polugrupe S i D njena $\mathcal{D}$ -klasa. Ako je $b \in D$ tada zbog $\mathcal{D} = \mathcal{R} \circ \mathcal{L}$ postoji $c \in D$ tako da je $a \mathcal{R} c \mathcal{L} b$. No, tada postoji idempotent u $\mathcal{R}$ -klasi od a , pa je po prethodnom tvrđenju element c regularan. Dualno, tada u $\mathcal{L}$ -klasi od c postoji idempotent, pa je i element b regularan. Ostala tvrđenja slede sada neposredno. $\square$

Može se pokazati da su $\mathcal{H}$ -klase polugrupe S koje sadrže idempotente podgrupe od S . Štaviše, u pitanju su maksimalne podgrupe od S , i svaka maksimalna podgrupa svake polugrupe S nastaje tako: kao $\mathcal{H}$ -klasa nekog idempotenta $e \in E(S)$. Takođe, sve ove maksimalne podgrupe sadržane u istoj $\mathcal{D}$ -klasi su međusobno izomorfne.

Grinove relacije u $\mathcal{T}_X$

Teorema 11. Neka je X proizvoljan neprazan skup i $f, g : X \rightarrow X$.

(1) $f \mathcal{R} g$ ako i samo ako je $\ker(f) = \ker(g)$.

(2) $f \mathcal{L} g$ ako i samo ako je $\text{Im}(f) = \text{Im}(g)$.

(3) $f \mathcal{J} g$ ako i samo ako je $\text{rank}(f) = |\text{Im}(f)| = |\text{Im}(g)| = \text{rank}(g)$.

(4) U $\mathcal{T}_X$ važi $\mathcal{D} = \mathcal{J}$.

Dokaz. (1): Uslov $f \mathcal{R} g$ ekvivalentan je postojanju transformacija h_1, h_2 tako da je $f \circ h_1 = g$ i $g \circ h_2 = f$. Dokazaćemo da je postojanje h_1 sa osobinom $f \circ h_1 = g$ ekvivalentno uslovu $\ker(f) \subseteq \ker(g)$ (pa je onda drugi uslov ekvivalentan sa $\ker(g) \subseteq \ker(f)$, odakle tvđenje (1) sledi).

Prema tome, pretpostavimo najpre da je $f \circ h_1 = g$. Takođe, pretpostavimo da su $x, y \in X$ takvi da je $(x, y) \in \ker(f)$, što znači da je $f(x) = f(y)$. No, tada je

$$g(x) = h_1(f(x)) = h_1(f(y)) = g(y),$$

pa je $(x, y) \in \ker(g)$.

Obratno, pođimo od pretpostavke da je $\ker(f) \subseteq \ker(g)$, a sa ciljem da konstruišemo $h_1 : X \rightarrow X$ tako da je $f \circ h_1 = g$. Naime, za sve $x \notin \text{Im}(f)$ definišimo $h_1(x) = x$. S druge strane, ako je $x \in \text{Im}(f)$ odaberimo proizvoljno $z \in f^{-1}(x)$ (dati uslov obezbeđuje da desna strana nije prazan skup) i definišimo $h_1(x) = g(z)$. Primetimo da je ovde izbor elementa $z \in X$ irelevantan jer $f(z_1) = x = f(z_2)$ povlači $g(z_1) = g(z_2)$ (zbog $\ker(f) \subseteq \ker(g)$), pa je time funkcija h_1 potpuno određena. Štaviše, iz istog razloga za sve $x \in X$ važi

$$h_1(f(x)) = g(x),$$

jer je $x \in f^{-1}(f(x))$.

(2): Uslov $f \mathcal{L} g$ ekvivalentan je postojanju transformacija h_1, h_2 tako da je $h_1 \circ f = g$ i $h_2 \circ g = f$. Dokazujemo da je uslov postojanja transformacije h_1 koja zadovoljava $h_1 \circ f = g$ ekvivalentan sa $\text{Im}(g) \subseteq \text{Im}(f)$, odakle, slično kao i u prethodnoj tački, sledi tvrđenje.

Zaista, ako je $h_1 \circ f = g$ i $y \in \text{Im}(g)$, tada je, za neko $x \in X$, $y = g(x) = f(h_1(x)) \in \text{Im}(f)$. Obratno, pretpostavimo da je $\text{Im}(g) \subseteq \text{Im}(f)$. Tada za sve $z \in \text{Im}(g)$ odaberimo po jedno $y_z \in f^{-1}(z)$ (desni skup je neprazan jer je zbog datog uslova $z \in \text{Im}(f)$) i definišimo transformaciju h_1 na X tako što je

$$h_1(x) = y_z \quad \text{kad god je} \quad g(x) = z.$$

Tada je, za proizvoljno $x \in X$, u skladu sa svim prethodnim definicijama,

$$f(h_1(x)) = f(y_{g(x)}) = g(x),$$

tj. $h_1 \circ f = g$.

(3) i (4): Kako je uvek $\mathcal{D} \subseteq \mathcal{J}$, ova dva tvrđenja dokazujemo tako što najpre proveravamo da $f \mathcal{J} g$ povlači $\text{rank}(f) = \text{rank}(g)$, a zatim da potonji uslov povlači $f \mathcal{D} g$.

Prva implikacija sledi iz jednostavne primedbe da je, za bilo koje dve transformacije h_1, h_2 ,

$$\text{rank}(h_1 \circ h_2) \leq \min(\text{rank}(h_1), \text{rank}(h_2)),$$

tj. da kompozicijom funkcija ne možemo dobiti funkciju koja ima kardinalnost slike veću od kardinalnosti slika bilo koje od pojedinačnih funkcija. S druge strane, neka je $\ker(f) = \{A_i : i \in I\}$ i $\text{Im}(f) = \{x_i : i \in I\}$ za neki skup I , tako da je $f(x) = x_i$ za sve $x \in A_i$ i sve $i \in I$. Po pretpostavci, g ima sliku iste kardinalnosti kao i f , pa se ta slika može indeksirati istim skupom I : $\text{Im}(g) = \{y_i : i \in I\}$. Posmatrajmo sada transformaciju h definisanu sa $h(x) = y_i$ ako i samo ako $x \in A_i$. Kako je $\ker(f) = \ker(h)$ i $\text{Im}(h) = \text{Im}(g)$, po tačkama (1) i (2) sledi da je $f \mathcal{R} h \mathcal{L} g$. Stoga je $f \mathcal{D} g$. $\square$

Posledica 12. $\mathcal{T}_X$ je regularna polugrupa.

Dokaz. Neka je f proizvoljna transformacija na X , i neka je

$$\ker f = \{A_i : i \in I\}.$$

Odaberimo neku transversalu ove particije, $x_i \in A_i$ ($i \in I$), i definišimo transformaciju e sa $e(x) = x_i$ ako i samo ako je $x \in A_i$. Transformacija e je idempotentna, a zbog $\ker(f) = \ker(e)$ važi $f \mathcal{R} e$. Prema tome, f je regularan element od $\mathcal{T}_X$. $\square$