UNIVERZA NA PRIMORSKEM
FAKULTETA ZA MATEMATIKO, NARAVOSLOVJE IN INFORMACIJSKE TEHNOLOGIJE

Magistrsko delo

Osnovne lastnosti hipergrup

(Basic Properties of Hypergroups)

Ime in priimek: Mojca Pev
Študijski program: Matematične znanosti, 2. stopnja
Mentor: Izr. prof. dr. Klavdija Kutnar

Koper, april 2017

Ključna dokumentacijska informacija

Ime in PRIIMEK: Mojca PEV

Naslov magistrskega dela: Osnovne lastnosti hipergrup

Kraj: Koper

Leto: 2017

Število strani: 79 Število slik: 6

Število referenc: 35

Mentor: izr. prof. dr. Klavdija Kutnar

UDK:512.53(043.2)

Ključne besede: hiperoperacija, polhipergrupa, podhipergrupa, hipergrupa, asociativnost, aksiom reprodukcije, homomorfizem hipergrupe, regularna in močno regularna relacija, popolna hipergrupa, pridružitveni prostor, kanonična hipergrupa.

Math. Subj. Class. (2010): 20N20, 08A99

Izvleček:
Tema, ki je preučevana v magistrski nalogi, sodi na področje moderne algebre, ki preučuje algebrske strukture. Obravnavane so tako imenovane hiperstrukture, s posebnim poudarkom na hipergrupah. Hipergrupa je hipergrupoid, ki je hkrati polhipergrupa in kvazihipergrupa. Z drugimi besedami to pomeni, da za hiperoperacijo $\star$ na neprazni množici H velja aksiom reprodukcije, to je za vsak $a \in H$ velja $a \star H = H \star a = H$. Poleg aksioma reprodukcije mora za hipergrupo veljati tudi asociativnost, to je, za vse $a, b, c \in H$ velja $(a \star b) \star c = a \star (b \star c)$. Ker so hipergrupe posplošitve grup, se v drugem poglavju spomnimo osnovnih pojmov iz teorije grup, kot so odseki in kvocientne grupe. Prav ti pojmi in primeri so namreč pomembni za razumevanje teorije hipergrup in primerov le-teh. V tretjem poglavju zapišemo osnovne definicije s področja teorije hipergrup in predstavimo več preprostih primerov, kot so polhipergrupe, kvazihipergrupe in hipergrupe. Srečamo se še z različnimi vrstami homomorfizmov hipergrup, seznanimo se z regularnimi in močno regularnimi relacijami, ugotovimo, kaj velja za popolne hipergrupe ter spoznamo pridružitvene prostore. Povsod podamo tudi preproste primere, ki bodo v pomoč bralcu. Magistrsko delo je torej strnjena predstavitev osnovnih definicij in pojmov iz teorije hipergrup skupaj s podajo dokazov osnovnih izrekov in primerov, kot tudi pregleden prikaz drugih konceptov s področja hipergrup.

Key words documentation

Name and SURNAME: Mojca PEV

Title of final project paper: Basic Properties of Hypergroups

Place: Koper

Year: 2017

Number of pages: 79 Number of figures: 6

Number of references: 35

Mentor: Assoc. Prof. Klavdija Kutnar, PhD

UDK: 512.53(043.2)

Keywords: hyperoperation, semihypergroup, subhypergroup, hypergroup, associativity, reproduction axiom, homomorphism of hypergroup, regular and strongly regular relation, complete hypergroup, join space, canonical hypergroup.

Math. Subj. Class. (2010): 20N20, 08A99

Abstract:
The theme studied in the thesis falls within the scope of modern algebra that studies algebraic structures. The so-called hyperstructures, with special emphasis given to hypergroups, will be discussed. A hypergroup is a hypergroupoid which is also a semihypergroup and quasihypergroup. In other words, this means that the reproduction axiom holds for hyperoperation $\star$ on non-empty set H, that is, for each $a \in H$ we have $a \star H = H \star a = H$. Besides the reproduction axiom, the associativity must also hold for a hypergroup, that is for all $a, b, c \in H$ we have $(a \star b) \star c = a \star (b \star c)$. Hypergroups are generalizations of groups. Therefore we need to remember the basic concepts of group theory, done in Chapter 2, such as cosets and quotient groups. These concepts and examples are important for understanding the theory of hypergroups and given examples. In Chapter 3 the basic definitions of the theory of hypergroups are given. Several simple examples, such as semihypergroups, quasihypergroups and hypergroups are also given. Various types of homomorphisms of hypergroups are introduced. Also, regular and strongly regular relations are find in detail. We also found out what is valid for complete hypergroups and we learn about association areas. Simple examples are given to help the reader. Master's thesis therefore gives a detailed presentation of basic definitions and concepts of hypergroup theory together with demonstrations of basic theorems and examples, as well as a transparent display of other concepts in the field of hypergroups.

Zahvala

Izr. prof. dr. Klavdiji Kutnar se zahvaljujem, da me je vzela pod svoje mentorstvo, me seznanila s hipergrupami in me s svojim načinom razmišljanja vodila skozi izdelavo magistrskega dela.

Hvala tudi tistim, ki skrbite, da je moje življenje velikokrat polno prav posebnih trenutkov.

Zahvaljujem se tudi vsem ostalim, ki so na tak ali drugačen način pomagali pri nastanku magistrskega dela.

Hvala!

Ko hodiš, pojdi zmeraj do konca.
Spomladi do rožne cvetice,
poleti do zrele pšenice,
jeseni do polne police,
pozimi do snežne kraljice,
v knjigi do zadnje vrstice,
v življenju do prave resnice,
v sebi do rdečice čez eno in drugo lice.
A če ne prideš ne prvič,
ne drugič do krova in pravega kova
poskusi: vnovič
in zopet
in znova.
(Tone Pavček)

Kazalo vsebine

Kazalo slik

Seznam kratic

gcd. greatest common divisor: največji skupni delitelj,
ipd. in podobno,
lcm. least common multiple: najmanjši skupni večkratnik.
t. j. to je.

1 Uvod

V magistrskem delu bomo preučevali nekatere lastnosti hipergrup. Poenostavljeno lahko rečemo, da so hipergrupe neprazne množice z večvrednostno operacijo, za katero veljajo določene lastnosti. Večvrednostno operacijo imenujemo tudi hiperoperacija. Zato sodijo hipergrupe v moderno oziroma abstraktno algebro, ki proučuje algebrske strukture.

Hipergrupe je pred dvainosemdesetimi leti prvi predstavil Marty [5]. To se je zgodilo na Osmem kongresu skandinavskih matematikov. Prav hipergrupe imajo osrednjo vlogo v teoriji hiperstruktur. V tem magistrskem delu bomo spoznali osnovne definicije in pojme iz teorije hipergrup. Navedli bomo tudi nekaj primerov in dokazov izrekov o hipergrupah. Razlika med klasičnimi algebrskimi strukturami in algebrskimi hiperstrukturami je v številu elementov, ki so rezultat podane operacije. V klasični algebrski strukturi je rezultat produkta vedno en sam element, v algebrski hiperstrukturi pa je rezultat hiperoperacije podmnožica podane neprazne množice. Pri dokazih, da je dana struktura hipergrupa, bomo preverjali aksiom reprodukcije in asociativnost. Ta dva pogoja sta dovolj, da je neprazna množica skupaj s hiperoperacijo res hipergrupa. Prvi primer hipergrupe je navedel Marty, glasi se takole: Naj bo $(G, \cdot)$ grupa in H njena podgrupa. Potem množica levih odsekov podgrupe H v grupi G, t. j. $G/H = \{xH \mid x \in G\}$, skupaj s hiperoperacijo $xH \star yH = \{zH \mid z \in xH \cdot yH\}$ tvori hipergrupo.

Magistrsko delo je razdeljeno na pet poglavij. Vsebinsko najpomembnejši sta drugo in tretje poglavje. V drugem poglavju bomo predstavili vsebino iz teorije grup. Omejili se bomo na predstavitev nekaj družin grup, predstavili odseke, kvocientne grupe in relacije. Večina vsebine iz drugega poglavja je ključna za razumevanje vsebine o hipergrupah. Ta vsebina je zapisana v tretjem poglavju. Tu bomo predstavili primere hipergrup. Za predstavljene primere bomo zapisali tudi dokaze. Poleg osnovnih definicij in primerov hipergrup bomo prikazali nekaj drugih konceptov iz področja hiperstruktur. Spoznali bomo podhipergrupe, homomorfizme hipergrup, pridružitvene prostore in kanonične hipergrupe.

2 Osnovno o relacijah in grupah

V tem poglavju se bomo spomnili osnovnih lastnosti relacij in grup, ki jih bomo potrebovali v nadaljevanju.

2.1 Relacije

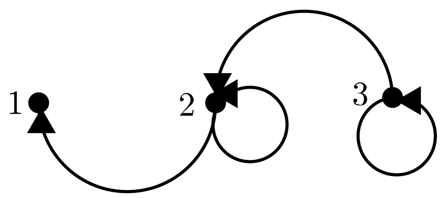
Vsebina tega razdelka je povzeta po [23] in [32]. Odnos med objektoma lahko v matematiki zapišemo na več načinov. Pogejmo nekaj odnosov:

$$3,5 = 3\tfrac{1}{2}, \quad \{1,2\} \neq (1,2), \quad \mathbb{Q}^- \subseteq \mathbb{Q}, \quad 2 \mid 815a, \quad a > b.$$

Znaki $=, \neq, \subseteq, \mid$ in $>$ opisujejo relacije med dvema objektoma. V tem poglavju ne bomo obravnavali vsake matematične relacije posebej, ampak bomo spoznali teorijo, ki bo zajela vse relacije.

Definicija 2.1. Relacija na množici M je podmnožica $R \subseteq M \times M$. Zapis $(x, y) \in M \times M$ zapišemo tudi kot xRy. Če x in y nista v relaciji, to zapišemo kot $x\not{R}y$. Relacijo R imenujemo tudi **binarna relacija**.

Primer 2.2. Naj bo $M = \{1, 2, 3\}$ in $R = \{(2, 1), (2, 2), (3, 2), (3, 3)\}$ podmnožica množice $M \times M$.
Ker je $(2, 1) \in R$, je $2R1$. Urejeni par $(3, 1)$ ni iz podmnožice R, zato $3\not{R}1$. Relacijo R na množici M lahko predstavimo tudi z grafom (glej sliko 1).



Slika 1: Relacija R predstavljena z grafom.

Definicija 2.3. Naj bo R relacija na množici M. Inverz relacije R na množici M je označen z R^{-1} in definiran kot

$$R^{-1} = \{(y, x) \in M \times M \mid (x, y) \in R\}.$$

Primer 2.4. Naj bo $A = \{1, 2, 3, 4, 5\}$. Relacija R je definirana kot $aRb \iff b > a, (a, b) \in A \times A$. Potem je inverzna relacija relacije R enaka:
$R^{-1} = \{(2, 1), (3, 1), (3, 2), (4, 1), (4, 2), (4, 3), (5, 1), (5, 2), (5, 3), (5, 4)\}$.

2.1.1 Lastnosti relacij

Zapis aRb je izjava, ki je lahko pravilna ali napačna. Nekatere relacije imajo določene lastnosti. Le-te bomo preučevali v tem podpoglavju.

Definicija 2.5. Naj bo R relacija na množici M. Relaciji R rečemo, da je:

- **refleksivna**, če je za vsak $x \in M$, xRx,
- **simetrična**, če za vse $x, y \in M$ velja: $xRy \Longrightarrow yRx$,
- **tranzitivna**, če za vse $x, y, z \in M$ velja: $((xRy) \wedge (yRz)) \Longrightarrow xRz$.

Primer 2.6. Relacija $=$ (je enako) je refleksivna, simetrična in tranzitivna relacija.

Definicija 2.7. Naj bo M množica in R relacija na tej množici. **Tranzitivno zaprtje** relacije R je relacija R^t na množici M, ki zadostuje pogojem:

- R^t je tranzitivna,
- $R \subseteq R^t$,
- če je N tranzitivna relacija, ki vsebuje R, potem je $R^t \subseteq N$.

Primer 2.8. Naj bo $M = \{a, b, c, d\}$ in relacija R na M definirana kot $\{(a, b), (b, c), (c, d)\}$. Poiščimo tranzitivno zaprtje za relacijo R.
Vsak urejen par relacije R je v tranzitivnem zaprtju R^t. Ker mora biti R^t tranzitivna, moramo relacijo R dopolniti z naslednjimi pari: $(a, c), (b, d)$ in (a, d), saj
$aRb \wedge bRc \Longrightarrow aRc$,
$bRc \wedge cRd \Longrightarrow bRd$,
$aRc \wedge cRd \Longrightarrow aRd$.
Tranzitivno zaprtje R^t za relacijo R je množica $R^t = \{(a, b), (a, c), (a, d), (b, c), (b, d), (c, d)\}$.

Definicija 2.9. Relacijo imenujemo **ekvivalenčna relacija**, če zanjo veljajo refleksivnost, simetričnost in tranzitivnost.

Definicija 2.10. Naj bo A množica in R ekvivalenčna relacija na množici A. Za vsak element a iz A bomo ekvivalenčni razred, ki vsebuje a, označili z $[a]$. Ekvivalenčni razred je množica vseh elementov x iz A, za katere velja, da je x v relaciji z a. To zapišemo kot:

$$[a] = \{x \in A \mid xRa\}.$$

Dokaz naslednje trditve najdete v [32].

Trditev 2.11. *Naj bo R ekvivalenčna relacija na množici A in $a, b \in A$. Če je aRb, sta ekvivalenčna razreda $[a]$ in $[b]$ enaka.*

Naslednji primer je vzet iz [32].

Primer 2.12. Naj bo $A = \{-1, 1, 2, 3, 4\}$. Potem je relacija

$$R = \{(-1, -1), (1, 1), (2, 2), (3, 3), (4, 4), (1, 3), (3, 1), (2, 4), (4, 2)\}$$

ekvivalenčna. Ekvivalenčni razredi so enaki: $[-1] = \{-1\}, [1] = [3] = \{1, 3\}, [2] = [4] = \{2, 4\}$.

Dokaz naslednjega izreka najde bralec v [32].

Izrek 2.13. *Naj bo R ekvivalenčna relacija na množici A. Množica $\{[a] : a \in A\}$ ekvivalenčnih razredov relacije R oblikuje particijo množice A.*

2.2 Teorija grup

Hipergrupe so posplošitve grup [5]. Zato je za vpeljavo le-teh smiselno, da se najprej seznanimo z osnovnimi pojmi o grupah. V tem poglavju bomo predstavili pomembnejše definicije, izreke, dokaze in primere iz teorije grup, ki jih potrebujemo v nadaljevanju.

Teorija grup je matematična disciplina iz 19. stoletja, ki preučuje simetrije med algebrskimi strukturami [33]. Grupe so poleg obsegov in vektorskih prostorov eden izmed osnovnih pojmov sodobne algebre [27]. Prvi, ki je uporabil pojem grupe, je bil francoski matematik Évariste Galois [29]. Poznavanje teorije grup je predvsem pomembno pri raziskovanju različnih simetrij tudi izven matematike, zlasti v fiziki in v kemiji [30].

2.2.1 Grupe in podgrupe

V nadaljevanju se bomo seznanili z definicijami in primeri, ki so večinoma povzeti iz [1] in [8].

Definicija 2.14. Binarna operacija $*$ na neprazni množici S je preslikava, ki slika iz $S \times S$ v S. Za elementa $(a, b) \in S \times S$ bomo element $*(a, b)$ iz S označili z $a * b$.

Definicija 2.15. Grupa $(G, *)$ je neprazna množica G skupaj z binarno operacijo $*$, ki zadošča naslednjim aksiomom:

- Za vse $g_1, g_2 \in G$ velja $g_1 * g_2 \in G$. Tej lastnosti binarne operacije $*$ pravimo **zaprtost binarne operacije** $*$.

- Za vse $g_1, g_2, g_3 \in G$ velja $(g_1 * g_2) * g_3 = g_1 * (g_2 * g_3)$. To lastnost imenujemo **asociativnost** binarne operacije $*$.
- Obstaja tak element e, da za vsak $g \in G$ velja $g * e = e * g = g$. Elementu e pravimo **enota** ali **identiteta**.
- Za vsak element $g \in G$ obstaja tak element $g^{-1} \in G$, da velja $g * g^{-1} = g^{-1} * g = e$. Elementu g^{-1} pravimo **inverz** elementa g.

Definicija 2.16. Algebrski strukturi, ki ima samo prvi dve lastnosti iz definicije 2.15, pravimo **polgrupa**.

Primer 2.17. Množici $(\mathbb{N}, +)$ in $(\mathbb{Z}^+, +)$ sta polgrupi.

Opomba 2.18. Z asociativnostjo lahko preučimo produkt končnega števila elementov grupe G. Vrstni red elementov v grupi je zelo pomemben. Za elementa g_1 in g_2 enakost $g_1 * g_2 = g_2 * g_1$ ne velja vedno. Če je $g_1 * g_2 = g_2 * g_1$ pravimo, da elementa komutirata. $[g_1, g_2] = g_1 g_2 g_1^{-1} g_2^{-1}$ imenujemo komutator elementov g_1 in g_2.

Definicija 2.19. Če je grupa $(G, *)$ tudi komutativna, to pomeni, da za vse $g_1, g_2 \in G$ velja $g_1 * g_2 = g_2 * g_1$, grupo $(G, *)$ imenujemo **Abelova grupa** ali **komutativna grupa**.

Opomba 2.20. V Abelovih grupah operacijo označujemo aditivno t. j. namesto $g_1 * g_2$ zapišemo $g_1 + g_2$, inverz elementa g_1 označimo z $-g_1$, identiteto pa z 0.

Opomba 2.21. V nadaljevanju bomo grupo $(G, *)$ zapisovali samo z G. Torej bomo izpustili znak za binarno operacijo. Uporabljali bomo multiplikativni zapis operacije. Tako bomo namesto zapisa $g_1 * g_2$ uporabili zapis $g_1 g_2$, namesto zapisa gg zapis g^2 oziroma splošneje $\underbrace{g \cdots g}_{m} = g^m$. Podobno bomo zapis (h^{-m}) definirali kot $(h^{-1})^m$. V Abelovi grupi namesto zapisa g^n uporabimo zapis ng.

Definicija 2.22. Grupi G, ki ima končno število elementov, pravimo **končna grupa**.

Trditev 2.23. *V grupi G velja pravilo krajšanja z iste strani: $hg = hg_1 \to g = g_1$, $gh = g_1 h \to g = g_1$.*

Dokaz. Pri dokazu bomo uporabili asociativnost operacije v grupi. Z leve strani pomnožimo enakost $hg = hg_1$ z inverzom h^{-1}. Dobimo zapis $h^{-1}hg = h^{-1}hg_1$. Produkt $h^{-1}h$ je enak enoti, kar pomeni, da je $eg = eg_1, g = g_1$. Podobno lahko pokažimo tudi, da velja krajšanje z desne strani. □

Definicija 2.24. **Red** končne grupe G je število elementov te grupe. Označimo ga z $\mid G \mid$.

Primer 2.25. $(\mathbb{Z}_n, +)$ je končna grupe ker:

- je seštevanje po modulu n asociativno,
- je število 0 identiteta grupe,
- je inverz elementa $z \in \mathbb{Z}_n$ število $n - z$,
- je $|\mathbb{Z}_n|$ končno naravno število.

Definicija 2.26. Če binarno operacijo grupe G zožimo na podmnožico H tvori grupo, pravimo, da je H **podgrupa** grupe G. Podgrupa je tako tudi sama grupa za binarno operacijo v G. Če je H podgrupa grupe G, uporabimo oznako $H \leq G$. Če je podmnožica H popolnoma vsebovana v grupi G, jo imenujemo **prava podgrupa** grupe G in jo označimo s $H < G$. Zadnjo podgrupo imenujemo tudi **trivialna podgrupa**.

Če je $K \leq H$ in $H \leq G$, potem je tudi $K \leq G$.

Primer 2.27. Vsaka grupa G ima vsaj dve podgrupi. To sta $H = G$ in $H = \{e\}$, ki ju imenujemo nepravi podgrupi.

Vsaka podgrupa končne grupe je končna. Vsaka podgrupa Abelove grupe je Abelova. Grupa, ki ni Abelova, ima tako Abelove kot ne-Abelove podgrupe.

Primer 2.28. Grupa $(\mathbb{Q} - \{0\}, \cdot)$ ni podgrupa grupe $(\mathbb{R}, +)$, čeprav sta obe množici grupi in je $(\mathbb{Q} - \{0\})$ podmnožica množice $\mathbb{R}$. Pomembno je, da je operacija na podmnožici inducirana z operacijo na množici.

Pri preverjanju, ali je neka podmnožica podgrupa, bomo uporabljali naslednjo trditev. Dokaz te trditve lahko bralec prebere v [8].

Trditev 2.29. *Za ugotavljanje, ali je neka podmnožica grupe G res podgrupa grupe G, zadošča preverjati pravilnost naslednjih korakov:*

- *Podmnožica H je zaprta za binarno operacijo $*$ na grupi G. To pomeni, da je za vse $g_1, g_2 \in H$ tudi produkt $g_1 * g_2 \in H$.*
- *Identiteta grupe G je tudi v H.*
- *Za vsak $h \in H$ velja, da je tudi $h^{-1} \in H$.*

Definicija 2.30. Naj bo X podmnožica grupe G. Z $\langle X \rangle$ označimo presečišče vseh podgrup grupe G, ki vsebujejo X. $\langle X \rangle$ je podgrupa grupe G, ki je generirana z podmnožico X grupe G. $\langle X \rangle$ je tudi najmanjša podgrupa grupe G, ki vsebuje X. Če je $X \leq G$, potem je $\langle X \rangle = X$. Če pa je $X = \{x\}$, potem to zapišemo kot $\langle x \rangle$.

2.2.2 Delovanje grupe na množici

V tem delu bomo spoznali splošno definicijo delovanja grupe na množici. Marty je že leta 1934 hipergrupe definiral kot množico skupaj z asociativno in reproduktivno hiperoperacijo.

V naslednji definiciji bomo definirali levo delovanje grupe G na množici X. Omeniti velja, da na podoben način definiramo tudi desno delovanje grupe na množici.

Definicija 2.31. Dano imamo grupo G in množico X. Delovanje grupe G na množici X je preslikava $G \times X \to X$, za katero velja:

- $1 \circ x = x$ za vsak $x \in X$, kjer je 1 nevtralni element grupe G,
- $(g_1 \circ g_2) \circ x = g_1 \circ (g_2 \circ x)$ za vse $g_1, g_2 \in G$ in $x \in X$.

Opomba 2.32. Množico X pod zgoraj zapisanimi pogoji imenujemo **G-množica**, za grupo G pa rečemo, da deluje na množici X.

Opomba 2.33. Namesto zapisa $g_1 \circ x$ bomo uporabljali notacijo g_1x.

Dokaz naslednjega izreka je povzet iz [8].

Trditev 2.34. *Naj bo G grupa. V G-množici X imamo dana dva poljubna elementa x_1 in x_2. Pravimo, da sta elementa v relaciji $x_1 \backsim x_2$, če v grupi G obstaja tak g, da velja $gx_1 = x_2$. Relacija $\backsim$ je* ***ekvivalenčna relacija*** *na X.*

Dokaz. Relacija $\backsim$ je ekvivalenčna relacija, če je refleksivna, simetrična in tranzitivna. Dokažimo najprej refleksivnost. Za vsak $x \in X$ velja $1x = x$. Zato je $x \backsim x$. Relacija $\backsim$ je refleksivna.
Predpostavimo, da za vsak $x_1, x_2 \in X$ velja $x_1 \backsim x_2$. Potem obstaja tak $g \in G$, da velja $gx_1 = x_2$. Pomnožimo zapisano enakost z inverzom elementa g, $g^{-1}x_2 = g^{-1}(gx_1) = (g^{-1}g)x_1 = ex_1 = x_1$. Dokazali smo simetričnost relacije $\backsim$.
Če je, $x_1 \backsim x_2$ in $x_2 \backsim x_3$, potem obstajata taka $g_1, g_2 \in G$, da je $g_1x_1 = x_2$ in $g_2x_2 = x_3$. Zato velja tudi nasledja enakost $(g_2g_1)x_1 = g_2(g_1x_1) = g_2x_2 = x_3$ in $x_1 \backsim x_3$. Relacija $\backsim$ je tranzitivna in zato tudi ekvivalenčna. $\square$

Trditev 2.35. *Naj bo G grupa, X G-množica ter naj bo $x \in X$ in $g \in G$. Stabilizator elementa $x \in X$ pri delovanju grupe G na množici X definiramo kot $G_x = \{g \in G \mid gx = x\}$.*

Definicija 2.36. Ekvivalenčne razrede, na katere razpade množica X glede na relacijo definirano v trditvi 2.34, imenujemo **orbite** delovanja grupe G na množico X. Če ekvivalenčni razred vsebuje $x \in X$, ga imenujemo orbita elementa x in ga označimo z Gx.

Moč orbite Gx izračunamo po enačbi

$$|Gx| = |G : G_x|.$$

Ob upoštevanju formule v naslednjem izreku lahko izračunamo število orbit delovanja grupe G na množici X. Z X_g označimo množico elementov v X, ki so fiksirani z $g \in G$. Definiramo jo z:

$$X_g = \{x \in X \mid gx = x\}.$$

Naslednji izrek je vzet po [8], kjer lahko preberete tudi njegov dokaz.

Izrek 2.37. *Naj bo G končna grupa in X končna G-množica. Naj bo r* ***število orbit*** *delovanja grupe G na množico X. Potem velja enakost*

$$r \cdot |G| = \sum_{g \in G} |X_g|.$$

Posledica 2.38. *Če je G končna grupa in je X končna G-množica, je število orbit delovanja grupe G na množico X enako*

$$\frac{1}{|G|} \cdot \sum_{g \in G} |X_g|.$$

2.2.3 Nekaj družin grup

V tem poglavju se bomo pobližje seznanili z nekaterimi najbolj znanimi družinami grup. Opisali bomo osnovne lastnosti in navedli primere: cikličnih grup, permutacijskih grup in diedrskih grup.

Ciklične grupe

Ker so ciklične grupe generirane samo z enim elementom, jih uvrščamo med preprostejše družine grup.

Definicija 2.39. Grupa G je ciklična, če obstaja tak element $g \in G$, da je $G = \langle g \rangle$.

Primer 2.40. Naj bo G grupa reda n z elementom g reda n. Potem je $G = \langle g \rangle$.

Trditev 2.41. *Naj bo G grupa in naj bo $g \in G$. Potem je $H = \{g^n \mid n \in \mathbb{Z}\}$ podgrupa grupe G. Hkrati je tudi najmanjša podgrupa grupe G, ki vsebuje g. Kar pomeni, da vsaka podgrupa, ki vsebuje g, vsebuje tudi celotno podgrupo H.*

Dokaz. Da je H res podgrupa grupe G, moramo preveriti pravilnost trditev, ki so zapisane pri trditvi 2.29.

- Produkt dveh elementov iz H mora biti tudi v H. Naj bosta $h^m, h^n \in H$. Potem je $h^m h^n = h^{m+n}, m, n \in \mathbb{Z}$. Opazimo, da je podmnožica H zaprta za operacijo množenja potenc z enako osnovo v grupi G.

- Identiteta v H je $h^0 = e = 1$. Ker je ta identiteta tudi v G, velja druga točka trditve 2.29.

- Ker za vsak $h^m \in H$ in $h^{-m} \in H$ velja, da je $h^m h^{-m} = h^{m+(-m)} = h^0 = e = 1$, velja tudi tretja točka trditve 2.29.

Dokazali smo, da veljajo vse tri točke trditve 2.29. Zato je $H \leq G$. □

Definicija 2.42. Element g grupe G imenujemo **generator grupe G**, če velja $\langle g \rangle = G$. Tako grupo imenujemo **ciklična**.

Definicija 2.43. Dano imamo ciklično grupo G. Če je $G = \langle g \rangle$, potem je **red elementa** g enak redu ciklične grupe G. To zapišemo kot $|G| = |g|$. To pomeni naslednje:

- Če je $|g| = \infty$, potem je tudi $|G| = \infty$.

- Če je $|g| = n$, potem je tudi $|G| = n$.

Primer 2.44. Primer ciklične grupe je grupa $(\mathbb{Z}_n, +)$, kjer je $\mathbb{Z}_n = \{0, 1, 2, 3, \ldots, n-1\}$. Generatorja grupe sta $\langle 1 \rangle$ in $\langle n-1 \rangle$, saj lahko z njima sestavimo celotno grupo $\mathbb{Z}_n$.

Trditev 2.45. *Vsaka ciklična grupa je Abelova grupa.*

Dokaz. Naj bo G ciklična grupa in g njen generator. Z g_1 in g_2 označimo elementa grupe G. Potem obstajata taki celi števili x in y da velja: $g_1 = g^x$ in $g_2 = g^y$. Preveriti moramo komutativnost, to je: $g_1 g_2 = g_2 g_1$.
Zapišimo: $g_1 g_2 = g^x g^y = g^{x+y}$, $g_2 g_1 = g^y a^x = g^{y+x}$. Od tod lahko zaradi komutativnosti seštevanja celih števil sklepamo, da velja komutativnost oziroma, da je G Abelova grupa. □

Posledica 2.46. *Grupa* $(\mathbb{Z}, +)$ *je ciklična grupa. Ker s številom* 1 *generiramo vsa števila grupe* $(\mathbb{Z}, +)$*, imenjujemo število* 1 *generator grupe* $(\mathbb{Z}, +)$*. Za* $\forall n \in \mathbb{Z}$ *je* $(n\mathbb{Z}, +)$ *ciklična podgrupa grupe* $(\mathbb{Z}, +)$*.*

Ta posledica nam je v pomoč pri definiciji največjega skupnega delitelja, ki ga označimo z **gcd**, dveh pozitivnih celih števil.

Definicija 2.47. Algebrska struktura $(K, +, \cdot)$ je **kolobar**, če je:

- $(K, +)$ Abelova grupa,

- $(K, \cdot)$ polgrupa,
- za vse $a, b, c \in K$
$$a \cdot (b + c) = a \cdot b + a \cdot c$$
in
$$(b + c) \cdot a = b \cdot a + c \cdot a.$$

Opomba 2.48. Operacijama $+$ in $\cdot$ rečemo seštevanje in množenje. Kolobar je **komutativen**, če je množenje komutativno.

Definicija 2.49. Naj bo R komutativni kolobar. Če sta a in b elementa komutativnega kolobara in $0 \neq d \in R$, potem rečemo, da je d največji skupni delitelj elementov a in b če velja:

- $d \mid a$ in $d \mid b$,
- če $c \mid a$ in $c \mid b$, potem tudi $c \mid d$.

Primer 2.50. Največji skupni delitelj števil 128 in 849 je število 1, zato imenujemo ti števili tuji si števili. Največji skupni delitelj števil 128 in 849 lahko izrazimo tudi kot $1 = -79 \cdot 849 + 524 \cdot 128$. Za izražanje največjega skupnega delitelja dveh celih števil uporabimo Evklidov algoritem.

Opomba 2.51. Če je red grupe G praštevilo p, potem je red vsakega elementa grupe G netrivialni delitelj praštevila p. Iz tega sledi, da je grupa G ciklična za vsak generator grupe G, razen za identiteto.

Naslednja trditev nam pove, kakšne elemente ima ciklična grupa. Dokaz trditve lahko preberete v [8].

Trditev 2.52. *Naj bo G ciklična grupa reda n in naj bo $r \leq n$. Potem ima G podgrupo H reda $\frac{n}{D}$, kjer je $D = gcd(n, r)$.*

Posledica 2.53. *Generator ciklične grupe $\mathbb{Z}_n$ je vsak element $m \in \mathbb{Z}_n$ za katerega velja, da je $gcd(m, n) = 1$.*

Dokaz trditve 2.54 lahko bralec prebere v članku [22].

Trditev 2.54. *Naj bo G ciklična grupa z n elementi in D delitelj števila n. Potem obstaja natanko ena podgrupa grupe G reda D.*

Primer 2.55. Poiščimo vse generatorje in podgrupe za grupo $\mathbb{Z}_{36}$. Vse podgrupe grupe $\mathbb{Z}_{36}$ so ciklične. Po posledici 2.53 so generatorji grupe $\mathbb{Z}_{36}$ števila: $1, 5, 7, 11, 13, 17, 19, 23,$ $25, 29, 31, 35$. Delitelji števila 36 so števila $1, 2, 3, 4, 6, 9, 12, 18, 36$. Grupa $\mathbb{Z}_{36}$ ima 9 podgrup, ki so enakega reda kot delitelji števila 36. Podgrupa reda 1 je trivialna grupa. Podgrupa reda 2 vsebuje enoto 0 in število 18, ki je sam sebi tudi inverz, torej je $H_2 = \{0, 18\}$. Podgrupa reda 3 vsebuje enoto ter dva paroma inverzna elementa. Tako je $H_3 = \{0, 12, 24\}$. Podgrupa reda 4 vsebuje štiri elemente, to so: enota, dva paroma inverzna elementa ter število 18; $H_4 = \{0, 9, 18, 27\}$. Podgrupa reda 6 vsebuje šest elementov, to so: enota, dva paroma inverzna elementa ter število 18. Zato je $H_6 = \{0, 6, 12, 18, 24, 30\} \leq \mathbb{Z}_{36}$. Podgrupa reda 9 vsebuje devet elementov, to je enoto in štiri paroma inverzne elemente, $H_9 = \{0, 4, 8, 12, 16, 20, 24, 28, 32\}$. Podgrupa reda 12 je enaka $H_{12} = \{0, 3, 6, 9, 12, 15, 18, 21, 24, 27, 30, 33\}$. Ta podgrupa vsebuje enoto, pet paroma inverznih elementov in število 18. Podgrupa reda 18 vsebuje osemnjast elementov, to so: $H_{18} = \{0, 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34\}$. Vsebuje enoto, osem paroma inverznih elementov ter število 18, ki je sam sebi tudi inverz. Zadnja podgrupa je podgrupa reda 36, ki je kar celotna grupa $\mathbb{Z}_{36}$.

Definicija 2.56. Naj bosta X in Y podmnožici grupe G. Definiramo produkt XY v grupi G kot:

$$XY = \{xy \mid x \in X, y \in Y\} \subseteq G.$$

Definirajmo še inverz:

$$X^{-1} = \{x^{-1} \mid x \in X\} \subseteq G.$$

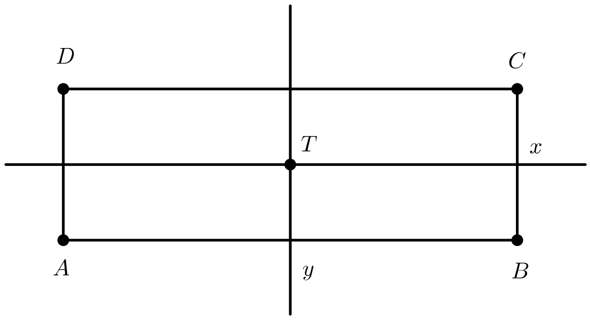
Dokaz naslednje trditve najde bralec v [11].

Trditev 2.57. *Naj bosta H in K podgrupi grupe G. Potem je HK podgrupa grupe G, če in samo če je $HK = KH$.*

Permutacijske grupe

S simetrijo se srečamo že v osnovni šoli. Spoznamo jo kot lastnost geometrijskega lika, ki se pri zrcaljenju preslika sam nase. Simetrije lahko raziskujemo tudi na grafih funkcij. Srednješolski primer simetričnega grafa je graf lihe funkcije, ki je simetričen glede na ordinatno os. Povezavo med simetrijami in teorijo grup bomo prikazali s pomočjo preslikav likov nase. Množica preslikav pravokotnika nase je sestavljena iz identitete, zrcaljenja čez simetralo dolžine pravokotnika, zrcaljenja čez simetralo širine pravokotnika in zrcaljenja čez presečišče obeh simetral. Množico preslikav bomo označili z $G = \{id, Z_x, Z_y, Z_T\}$. Pravokotnik se čez dane simetrije vedno prezrcali sam vase. To prikazuje slika 2. Množica G je za operacijo $\star$, ki je definirana v naslednji tabeli, grupa.

$\star$	id	Z_x	Z_y	Z_T
id	id	Z_x	Z_y	Z_T
Z_x	Z_x	id	Z_T	Z_y
Z_y	Z_y	Z_T	id	Z_x
Z_T	Z_T	Z_y	Z_x	id



Slika 2: Simetrije pravokotnika.

V tem podrazdelku bomo spoznali simetrije algebrskih objektov, ki jih proučujemo s pomočjo simetrije grup. Več o simetričnih ali permutacijskih grupah lahko bralec prebere v knjigah [7] in [8].

Definicija 2.58. Permutacija končne množice M je bijektivna preslikava množice M nase, kar zapišemo kot $\tau : M \to M$. Naj bosta ψ in φ poljubni permutaciji končne množice M. Potem lahko definiramo **kompozitum permutacij** kot: $\psi \circ \varphi : M \xrightarrow{\varphi} M \xrightarrow{\psi} M$. Tudi kompozitum permutacij je bijektivna preslikava na množici M torej je, permutacija množice M.

Opomba 2.59. Kompozitum dveh permutacij bomo namesto $\psi \circ \varphi$ pisali kot $\psi\varphi$. Kompozitum deluje tako, da najprej deluje permutacija φ, za njo pa še permutacija ψ. To zapišemo tudi kot $(\psi\varphi)(m) = \psi(\varphi(m)), m \in M$.

Primer 2.60. Naj bo $I = \{1, 2, 3, 4, 5, 6\}$. Na množici I imamo dani permutaciji $\psi = \begin{pmatrix} 1\ 2\ 3\ 4\ 5\ 6 \\ 6\ 5\ 4\ 3\ 2\ 1 \end{pmatrix}$ in $\varphi = \begin{pmatrix} 1\ 2\ 3\ 4\ 5\ 6 \\ 2\ 4\ 1\ 5\ 3\ 6 \end{pmatrix}$. Izračunajmo $\psi\varphi$. V opombi 2.59 je zapisano, da množenje permutacij izvajamo od desne proti leve. Iz zapisa permutacije φ je razvidno, da je $\varphi(1) = 2$. V zapisu permutacije ψ pa opazimo, da je $\psi(2) = 5$, zato je $\psi(\varphi(1)) = 5$. Produkt permutacij $\psi\varphi$ je v dvovrstičnem zapisu enak $\begin{pmatrix} 1\ 2\ 3\ 4\ 5\ 6 \\ 5\ 3\ 6\ 2\ 4\ 1 \end{pmatrix}$. Dani produkt lahko zapišemo tudi v cikličnem zapisu kot $(1\ \ 5\ \ 4\ \ 2\ \ 3\ \ 6)$.

Bralec lahko dokaz trditve 2.61 prebere v [8].

Trditev 2.61. *Naj bo M neprazna množica in naj bo S_M množica vseh permutacij množice M. Potem je $(S_M, \circ)$ grupa. Grupo $(S_M, \circ)$ imenujemo* ***simetrična grupa*** *množice M. Če je $M = \{1, \ldots, n\}$, jo označimo s S_n.*

Primer 2.62. Elementi simetrične grupe S_n so oblike $\varphi = \begin{pmatrix} 1 & 2 & \ldots & n \\ \varphi(1) & \varphi(2) & \ldots & \varphi(n) \end{pmatrix}$. Poglejmo si primer simetrične grupe. $S_3 = \{1, 2, 3\}$. To je grupa vseh permutacij množice s tremi elementi. Simetrična grupa S_3 ima 3! permutacij. Te permutacije so: $id, (1\ 2), (2\ 3), (1\ 3), (1\ 2\ 3), (1\ 3\ 2)$.

Definicija 2.63. Naj bo $\varphi \in S_n$. Če obstaja tak niz $x_1, x_2, \ldots, x_r \in \{1, 2, \ldots, n\}$, da je

$$\varphi(x_i) = x_{i+1} \ \ (i = 1, 2, \ldots, r-1),$$

$$\varphi(x_r) = x_1 \ \ (i = 1, 2, \ldots, r-1),$$

$$\varphi(x) = x \ \ (x \notin \{x_1, x_2 \ldots, x_r\}).$$

Tedaj permutacijo φ označimo z $(x_1 x_2 \ldots x_{r-1} x_r)$ imenujemo cikel dolžine r.

Definicija 2.64. Cikla $(a_1, a_2, \ldots, a_n)$ in $(b_1, b_2, \ldots, b_r)$ sta disjunktna, če in samo če sta množici $\{a_1, a_2, \ldots, a_n\}$ in $\{b_1, b_2, \ldots, b_r\}$ disjunktni.

Definicija 2.65. Vsak element simetrične grupe lahko zapišemo kot produkt disjunktnih ciklov. To imenujemo **razbijanje permutacije v produkt disjunktnih ciklov**.

Opomba 2.66. Dva različna zapisa permutacije kot produkt disjunktnih ciklov vsebujeta isti cikel, le v različnem vrstnem redu.

Definicija 2.67. Ciklična struktura permutacije je število posameznih dolžin ciklov v zapisu permutacije z disjunktnimi cikli.

Opomba 2.68. V zapisu permutacije kot produkt disjunktnih ciklov ponavadi izpustimo cikel dolžine 1, ki ga sicer imenujemo monocikel. Permutacijo, ki je cikel dolžine 2, imenujemo transpozicija.

Dokaz naslednjega izreka preberite v [10].

Izrek 2.69. *Permutaciji α in β sta konjugirani, če in samo če imata isto ciklično strukturo.*

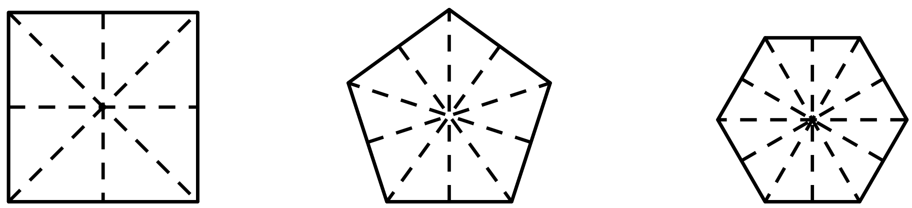
Definicija 2.70. Permutacija je liha (soda), če jo lahko zapišemo kot produkt lihega (sodega) števila transpozicij.

Definicija 2.71. Podmnožico množice S_n, ki je sestavljena iz sodih permutacij, tvori podgrupo grupe S_n reda $\frac{n!}{2}$.

Diedrske grupe

Bralec lahko več o diedrskih grupah prebere v literatui [21]. Tu se spomnimo le osnovnih lastnosti. **Diedrsko grupo** $D_n, n \geq 3, n \in \mathbb{Z}^+$, generirajo vrteži ($\varphi$) in zrcaljenja ($\sigma$) pravilnega n-kotnika. Oglejmo si sliko 3, na kateri so narisane osi zrcaljenja nekaterih pravilnih n-kotnikov.

Zrcaljenje čez simetrale in vrteži za $\frac{360°}{n}$ okrog presečišča simetrij ohranjajo pravilni n-kotnik. Število vrtežev in kot, za katerega vrtimo pravilni večkotnik, je odvisen od pravilnega večkotnika. Zato φ za D_4 ni enak φ za D_5. Grupa D_3 ima dva vrteža in identiteto, grupa D_4 ima tri vrteže in id, grupa D_5 ima 5 vrtežev in id, ipd. Na sliki 3 vidimo, da ima kvadrat štiri osi zrcaljenja, pravilni petkotnik pet osi zrcaljenja, ipd. V splošnem ima pravilni n-kotnik n osi zrcaljenja.



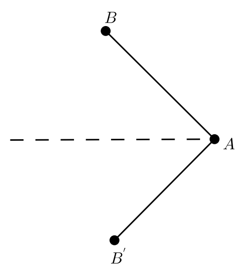
Slika 3: Osi zrcaljenja kvadrata, pravilnega petkotnika in pravilnega šestkotnika.

Dokaz naslednjega izreka lako bralec prebere v [21].

Izrek 2.72. *Grupa D_n ima $2n$ elementov, n zrcaljenj in n vrtežev. Elementi grupe so: $D_n = \{id, \varphi, \varphi^2, \varphi^3, \ldots, \varphi^{n-2}, \varphi^{n-1}, \sigma, \sigma\varphi, \sigma\varphi^2, \sigma\varphi^3, \ldots, \sigma\varphi^{n-2}, \sigma\varphi^{n-1}\}$, kjer z φ označimo vrteže in z σ zrcaljenja. Operacija je običajno sestavljanje funkcij.*

Trditev 2.73. *V grupi D_n velja, da je $\sigma\varphi\sigma^{-1} = \varphi^{-1}$.*

Dokaz. Na sliki 4 je del pravilnega večkotnika.



Slika 4: Del pravilnega večkotnika.

S črko σ označimo zrcaljenja ter s črko φ vrteže n-kotnika. Poglejmo, kaj je rezultat togega premika $(\sigma\varphi\sigma^{-1})(A)$.

$$(\sigma\varphi\sigma^{-1})(A) = (\sigma\varphi)(\sigma^{-1}(A)) = (\sigma\varphi)(A) = (\sigma)(\varphi(A)) = (\sigma)(B) = B'.$$

Preverimo še za togi premik $\varphi^{-1}(A)$.

$$\varphi^{-1}(A) = B'.$$

Na podoben način preverimo, v katere točk se preslika točka B.

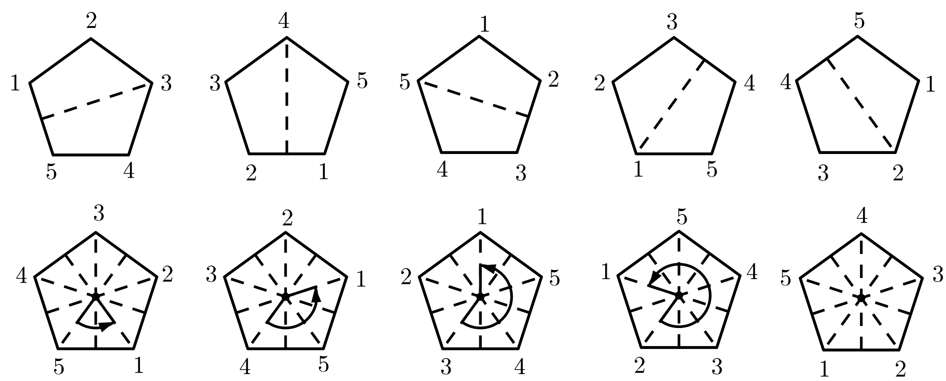
$$(\sigma\varphi\sigma^{-1})(B) = (\sigma\varphi)(\sigma^{-1}(B)) = (\sigma\varphi)(B') = (\sigma)(\varphi(B')) = (\sigma)(A) = A.$$

$$\varphi^{-1}(B) = A.$$

Če sta toga premika $\sigma\varphi\sigma^{-1}$ in φ^{-1} enaka za točki A in B, sta toga premika enaka za vse ostale točke večkotnika. □

Opomba 2.74. Produkt vrteža φ^a ter zrcaljenja $\varphi^b\sigma$ je zrcaljenje, saj velja: $\varphi^a\varphi^b\sigma = \varphi^{a+b}\sigma$.

Primer 2.75. Na sliki 5 je prikazano delovanje dierske grupe D_5. Grupa ima deset elementov. Iz izreka 2.72 vidimo, da so elementi grupe
$D_5 = \{1 \text{ ali } id, \varphi, \varphi^2, \varphi^3, \varphi^4, \sigma, \sigma\varphi, \sigma\varphi^2, \sigma\varphi^3, \sigma\varphi^4\}$.



Slika 5: Delovanje elementov diedrske grupe D_5.

2.2.4 Odseki

Definicija 2.76. Grupa G naj ima podgrupo H in naj bo g element grupe G. Podmnožico $gH = \{gh \mid h \in H\}$ grupe G imenujemo **levi odsek** grupe G po podgrupi H. Podmnožico $Hg = \{hg \mid h \in H\}$ grupe G pa imenujemo **desni odsek** grupe G po podgrupi H. Množico vseh odsekov podgrupe H v grupi G označimo z G/H.

Obstaja bijektivna povezava med levimi in desnimi odseki podgrupe H v grupi G, in sicer: $(gH)^{-1} = Hg^{-1}$. Naj bo H podgrupa grupe G. Katerakoli dva odseka podgrupe H v grupi G sta bodisi enaka ali disjunktna. Odseka gH in hH sta enaka, če in samo če je $h^{-1}g \in H$. Element $g \in G$ pripada natanko enemu odseku podgrupe. Označimo ga z gH.

Primer 2.77. Poiščimo vse desne odseke grupe $\mathbb{Z}$ po podgrupi $4\mathbb{Z} = \{4k \mid k \in \mathbb{Z}\}$. Grupa $(\mathbb{Z}, +)$ je neskončna ciklična grupa. Grupo generiramo z elementom 1, lahko pa tudi z elementom -1. Elementi podgrupe $4\mathbb{Z}$ so naslednji:

$4\mathbb{Z} = \{\ldots, -16, -12, -8, -4, 0, 4, 8, 12, 16, \ldots\}$.

Desni odseki grupe $\mathbb{Z}$ po podgrupi $4\mathbb{Z}$ so naslednji:

$$
\begin{aligned}
4\mathbb{Z} + 0 &= \{\ldots, -16, -12, -8, -4, 0, 4, 8, 12, 16, \ldots\} = 4\mathbb{Z},\\
4\mathbb{Z} + 1 &= \{\ldots, -15, -11, -7, -3, 1, 5, 9, 13, 17, \ldots\},\\
4\mathbb{Z} + 2 &= \{\ldots, -12, -10, -6, -2, 2, 6, 10, 14, 20, \ldots\},\\
4\mathbb{Z} + 3 &= \{\ldots, -13, -9, -5, -1, 3, 7, 11, 15, 19, \ldots\}.
\end{aligned}
$$

Ker unija zgornjih desnih odsekov tvori celotno grupo $\mathbb{Z}$ pravimo, da odseki $4\mathbb{Z}+0, 4\mathbb{Z}+1, 4\mathbb{Z}+2, 4\mathbb{Z}+3$ tvorijo particijo grupe $\mathbb{Z}$.

Opomba 2.78. Za vsako podgrupo H Abelove grupe G je particija levih odsekov enaka particiji desnih odsekov. Ker je grupa $(\mathbb{Z}, +)$ Abelova, so tudi levi odseki enaki zgoraj zapisanim desnim odsekom.

Naslednji primer je vzet iz [20].

Primer 2.79. Naj bo $S_3 = \{id, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$ in $H = \{id, (1\ 2)\}$. Najprej poiščimo leve odseke grupe G po podgrupi H: $\{id, (1\ 2)\}$, $\{(2\ 3), (1\ 3\ 2)\}$, $\{(1\ 3), (1\ 2\ 3)\}$. Izračunajmo tudi desne odseke.

$$\{id, (1\ 2)\}, \{(1\ 3), (1\ 3\ 2)\}, \{(2\ 3), (1\ 2\ 3)\}, \{(1\ 2\ 3), (2\ 3)\}, \{(1\ 3\ 2), (1\ 3)\}.$$

V splošnem velja, da odseki niso podgrupe in nekateri ne vsebujejo identitete. Za isti element sta lahko leva in desna odseka različna.

Dokaz naslednje trditve lahko preberete v [26].

Trditev 2.80. *Če je $H \leq G$ potem velja:*

- $hH = H$ *za vsak* $h \in H$,
- $g_1H = g_2H$, *če in samo če* $g_1 = g_2h$ *za vsak* $h \in H$.

Posledica 2.81. *Naj bo $g \in G$ in naj bo H končna podgrupa grupe G. Potem je* ***moč desnega odseka*** *grupe G po podgrupi H enaka* ***moči levega odseka*** *grupe G po podgrupi H in enaka moči podgrupe H: $|gH| = |Hg| = |H|, g \in G$.*

Definicija 2.82. Podgrupo H grupe G imenujemo **podgrupa edinka**, če se vsak levi odsek po tej grupi ujema s pripadajočim desnim odsekom, to je $gH = Hg$ za vsak $g \in G$. ali v ekvivalentnemu zapisu $gHg^{-1} \subseteq H$, za vsak $g \in H$. V slovenščini se precej pogosteje ...

Opomba 2.83. Veliko avtorjev zgoraj omenjenega razlikovanja za oznako normalne podgrupe ne upošteva.

Opomba 2.84. Podmnožica množice S_n, ki je sestaljena iz sodih permutacij, tvori normalno podgrupo grupe S_n.

Opomba 2.85. Če je $H \trianglelefteq G$ in $K \trianglelefteq H$, potem ni nujno res, da je $K \triangleleft G$. Če pa je $K \trianglelefteq G$ in $K \leq H \leq G$, potem je $K \trianglelefteq H$.

Izrek 2.86. *Naj bosta H in K podgrupi grupe G. Če je $K \trianglelefteq G$, potem je $HK \leq G$ in $H \cap K \trianglelefteq H$. Če je tudi $H \trianglelefteq G$, potem je $HK \trianglelefteq G$ in $H \cap K \trianglelefteq G$.*

Dokaz naslednjega izreka naj bralec prebere v [1].

Izrek 2.87. *Vsaka podrgupa indeksa 2 je normalna podgrupa.*

Opomba 2.88. Vse podgrupe Abelove grupe so normalne podgrupe. Podgrupi $\{id\}$ in cela grupa G sta vedno normalni v G. Če sta to edini normalni podgrupi grupe G, pravimo grupi G enostavna grupa. Grupa, ki ima samo en element, ni enostava grupa.

Primer 2.89. Naj bo $H = \langle (2\ 3) \rangle$ podgrupa simetrične grupe S_3. V nadaljevanju bomo preverili, ali je H edinka v S_3.
Za podgrupo edinko velja, da so levi odseki enaki pripadajočim desnim odsekom, $gH = Hg$. Zato najprej določimo leve in desne odseke grupe S_3 po podgrupi H. Levi odseki grupe S_3 po podgrupi H so: $\{(1\ 2), (1\ 2\ 3)\}$, $\{id, (2\ 3)\}$, $\{(1\ 3), (1\ 3\ 2)\}$, $\{(1\ 2\ 3), (1\ 2)\}$, $\{(1\ 3\ 2), (1\ 2)\}$.

Desni odseki grupe S_3 po podgrupi H so: $\{id, (2\ 3)\}$, $\{(1\ 2), (1\ 3\ 2)\}$, $\{(2\ 3), (1\ 2\ 3)\}$, $\{(1\ 3), (1\ 2\ 3)\}$, $\{(1\ 2\ 3), (1\ 3)\}$, $\{(1\ 3\ 2), (1\ 2)\}$. Ker se levi odseki ne ujemajo z desnimi odseki, podgupa H ni edinka v S_3.

Definicija 2.90. Naj bo $H \leq G$. Število levih odsekov grupe G po podgrupi H imenujemo **indeks** podgrupe H v grupi G. Označimo ga z $|G : H|$ ali $[G : H]$.

Primer 2.91. Naslednji primer najdemo v [24]. Naj bo $G = S_3$ in

$$H = \{id, (1\ 2\ 3), (1\ 3\ 2)\}.$$

Izračunajmo število levih odsekov grupe G po podgrupi H.
Indeks $[G : H]$ je lahko končno število, lahko pa je tudi neskončno. Če je grupa G končna, potem je tudi indeks končen in ga izračunamo kot $|G| : |H|$. Grupo G sestavljajo naslednje permutacije $id, (1\ 2), (2\ 3), (1\ 3), (1\ 2\ 3), (1\ 3\ 2)$, torej je njena moč 6. Njena podgrupa H je moči 3. Ker je grupa G končna, bomo število levih odsekov izračunali kot

$$[G : H] = |G| : |H| = 6 : 3 = 2.$$

Lagrangev [1] izrek je pomemben izrek v teoriji grup. Ta izrek nam pomaga določiti število elementov podgrupe za dano grupo. Denimo, da ima grupa G 15 elementov. Potem ima po Lagrangevem izreku grupa G lahko le podgrupe reda $1, 3, 5$ in 15.

Naslednji izrek imenujemo po Josephu-Louisu Lagrangeju **Lagrangev izrek**.

Izrek 2.92. *Naj bo H podgrupa končne grupe G. Potem red podgrupe H (število elementov podgrupe) deli red končne grupe G.*

Dokaz. Naj bo H podgrupa končne grupe G. Vemo, da vsi desni odseki podgrupe H tvorijo particijo grupe G. Torej vsak element iz grupe G pripada natanko enemu odseku podgrupe H. Vemo tudi, da je moč desnih odsekov enaka moči podgrupe H. Potem moč končne grupe G dobimo tako, da število odsekov pomnožimo z močjo podgrupe. Iz tega sklepamo, da $|H|$ deli $|G|$. □

Posledica 2.93. *Vsaka grupa praštevilskega reda je ciklična. Še več, vsak element te grupe, ki ni identiteta, generira celo grupo.*

Dokaz. Naj bo G grupa praštevilskega reda p in naj bo $g \in G$, ki ni enak identiteti. Potem ima ciklična podgrupa $\langle g \rangle$ grupe G, ki je generirana z g, vsaj dva elementa, g in e. Iz Lagrangovega izreka vemo, da je red grupe $\langle g \rangle$ večji ali enak 2 in mora deliti praštevilski red grupe G. To pa pomeni, da je enak praštevilskemu redu grupe G in velja, da je $\langle g \rangle = G$. Od tod sledi, da je grupa G ciklična. □

Opomba 2.94. Ker je količnik $|G| : |H|$ enak indeksu podgrupe H glede na grupo G, lahko moč grupe G izračunamo po enačbi

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

[1] Joseph-Louis Lagrange (1736 − 1813) je bil italijansko-francoski matematik. Ukvarjal se je s teorijo števil in nebesno mehaniko. Njegova najpomembnejša knjiga je Mécanique analytique iz leta 1788, na kateri sloni njegovo nadalnje delo.

Izrek 2.95. *Če je $K \leq H \leq G$, potem je $|G:K| = |G:H||H:K|$.*

Definicija 2.96. Naj bo H podgrupa grupe G in naj bo $\mathcal{I}$ indeksna množica, ki je v bijektivni povezavi z množico odsekov podgrupe H v grupi G. Podmnožica $T = \{t_i \mid i \in \mathcal{I}\}$ je množica levih predstavitvenih odsekov podgrupe H za grupo G, če je množica t_iH enaka odsekom podgrupe H v grupi G brez ponavljajočih odsekov.

Zapišimo še izrek, ki opisuje podgrupe neskončnih cikličnih grup.

Izrek 2.97. *Naj bo $G = \langle g \rangle$ neskončna ciklična grupe. Potem:*

- *Za vsak $d \in \mathbb{N}$ obstaja natanko ena podgrupa grupe G z indeksom d. Poleg tega ima vsaka netrivialna podgrupa grupe G končni indeks.*
- *Naj bosta $d, e \in \mathbb{N}$. Presek podgrup, ki so indeksa d in e, je podgrupa indeksa $lcm(d, e)$.*
- *Naj bosta $d, e \in \mathbb{N}$. Potem je produkt podgrup, ki so indeksa d in e podgrupa indeksa $gcd(d, e)$.*

V [20] so poleg odsekov opisani tudi **dvojni odseki**. Kot smo že zapisali, so odseki definirani kot množenje z desne ali z leve strani elementa grupe s podgrupo dane grupe. Če pa element grupe pomnožimo z leve in z desne strani z različnima podgrupama dane grupe, govorimo o **dvojnih odsekih**.

Definicija 2.98. Naj bo G grupa in $g \in G$ ter H in K podgrupi grupe G. Potem vsako množico, ki je oblike

$$HgK = \{hgk \mid h \in H, k \in K\},$$

imenujemo dvojni odsek (H, K).

Primer 2.99. Dano imamo grupo S_3 in njeni podgrupi $H = \{id, (1\ 2)\}$ in $K = \{id, (1\ 3)\}$. Poiščimo dvojne odseke za permutaciji $(2\ 3)$ in $(1\ 3\ 2)$.

- permutacija $(2\ 3)$:
  $H \cdot (2\ 3) \cdot K = \{h \cdot (2\ 3) \cdot k \mid h \in H, k \in K\}$. Dvojne odseke izračunamo tako, da vsako permutacijo iz množice H pomnožimo z dano permutacijo in z vsako permutacijo iz množice K. Dvojni odseki so enaki množici $H \cdot (2\ 3) \cdot K = \{(2\ 3), (1\ 2\ 3)\}$.
- permutacija $(1\ 3\ 2)$:
  $H \cdot (1\ 3\ 2) \cdot K = \{h \cdot (1\ 3\ 2) \cdot k \mid h \in H, k \in K\}$. Dvojni odseki so enaki množici $H(1\ 3\ 2)K = \{id, (1\ 3), (2\ 3), (1\ 3\ 2)\}$.

Grupa S_3 je moči 6. V nasprotju z odseki, moč dvojnih odsekov ne deli nujno moči grupe. To opazimo tudi v tem primeru. Moč dvojnega odseka $H(2\ 3)K$ je 4, vendar 4 ne deli 6. Iz primera je tudi razvidno, da imajo različni dvojni odseki za isti par podgrup različno moč.

2.2.5 Kvocientne grupe

Snov o kvocientnih grupah je povzeta po [1], [8], [28] in [33].

Izrek 2.100. *Naj bo G grupa in H podgrupa grupe G. Potem je binarna operacija $\circ$ na levih odsekih $(gH) \circ (kH) = (gk)H; g, k \in G$* ***dobro definirana****, če je H podgrupa edinka grupe G.*

Dokaz. Dokaz je povzet po [28]. Pokazali bomo, da je produkt dveh levih odsekov dobro definiran. Zato želimo pokazati, da je $(aH)(bH) = (ab)H$. To bomo storili s pomočjo podmnožic. Množici $\mathcal{A}$ in $\mathcal{B}$ sta enaki natanko takrat, ko velja $\mathcal{A} \subseteq \mathcal{B}$ in $\mathcal{B} \subseteq \mathcal{A}$. Naj bo G grupa in $H \triangleleft G$. Definiramo produkt levih odsekov kot $(aH)(bH) = \{xy \mid x \in aH, y \in bH\} = \{ah_1bh_2 \mid h_1, h_2 \in H\}$. Vemo, da dokler je H podgrupa edinka grupe G velja $b^{-1}Hb \subseteq H$. Zato za vsak $h_1 \in H$ obstaja tak $c \in H$, ki ga lahko zapišemo kot $c = b^{-1}h_1b$. Če je $ah_1bh_2 \in (aH)(bH)$ sledi, da je $ah_1bh_2 = abb^{-1}h_1bh_2 = abch_2 \in (ab)H \subseteq Hb^{-1}$. Potem velja

$$(aH)(bH) \subseteq (ab)H.$$

Po drugi strani pa velja naslednje:

$$abh \in (ab)H,$$

$$aebh \in (aH)(bH),$$

$$(ab)H \subseteq (aH)(bH).$$

Od tod sklepamo, da je

$$(aH)(bH) \subseteq (ab)H,$$

$$(ab)H \subseteq (aH)(bH).$$

Enakost produkta levih odsekov $(aH)(bH) = (ab)H$ sledi iz enakosti množic. □

Podgrupe edinke so pomembne, ker nam omogočajo izdelavo novih grup. Način, kako to storimo je zapisan v naslednji trditvi.

Trditev 2.101. *Naj bo G grupa in H njena podgrupa edinka. Potem odseki podgrupe H po grupi G določajo grupo G/H z binarno operacijo $(gH) \circ (kH) = (gk)H$. Grupo G/H imenujemo* ***kvocientna grupa*** *ali* ***faktorska grupa*** *grupe G po podgrupi H.*

Dokaz. Za dokaz, da je G/H res grupa, moramo preveriti tri lastnosti, ki morajo veljati za grupo.

- Najprej preverimo, ali za vse odseke aH, bH, cH iz G/H velja asociativnostni zakon, to je
$$(aH)(bHcH) = (aHbH)(cH).$$
Leva stran: $(aH)(bHcH) = (aH)(bcHH) = (aH)(bcH) = (a(bc))H$,
Desna stran: $(aHbH)(cH) = (abHH)(cH) = (abH)(cH) = ((ab)c)H$.

  Zaradi asociativnosti, ki velja v grupi G, lahko sedaj sklepamo, da asociativnost velja tudi v kvocientni grupi G/H. Ker je H podgrupa edinka grupe G velja, da se vsak levi odsek ujema z ustreznim desnim odsekom. Pri dokazu smo upoštevali, da zaradi omenjene zakonitosti, velja $Hc = cH$. Potem smo upoštevali, da je v podgrupi produkt dveh podgrup enak sami podgrupi, to je $H \cdot H = H$. Nazadnje smo upoštevali tudi definicijo operacije $(gH)(kH) = (gk)H$. Podobna utemeljitev velja tudi za dokaz desne strani asociativnostnega zakona.

- Naj bo $e \in G$ nevtralni element grupe G. Ker je $(eH)(aH) = aH$ in $(aH)(eH) = aH$ za vsak $a \in H$, lahko sklepamo, da je $eH = H$ nevtralni element kvocientne grupe G/H.

- Še zadnja lastnost, ki jo moramo preveriti za grupo G/H, je lastnost obstoja obratnega elementa oziroma inverza. Torej, naj bo $aH \in G/H$ poljuben odsek. Potem je:

  $(a^{-1}H)(aH) = (a^{-1}a)H = eH = H$,
  $(aH)(a^{-1}H) = (aa^{-1})H = eH = H$.

  Iz zapisa sledi, da je $a^{-1}H$ inverz odseka aH.

Tako smo dokazali, da je G/H res grupa. □

Opomba 2.102. Identiteta kvocientne grupe G/H je H. Inverz odseka $xH \in G/H$ je $x^{-1}H$. Če je G Abelova grupa, potem je tudi kvocientna grupa G/H Abelova grupa.

Definicija 2.103. Elementa x in y iz grupe G sta si **konjugirana**, če obstaja tak $g \in G$, da je:
$$y = gxg^{-1}.$$

Naslednja primera sta vzeta iz vaj v 14. poglavju literature [8].

Primer 2.104. Poiščimo število elementov oziroma red kvocientne grupe

- $\mathbb{Z}_6/\langle 3\rangle$:
  Grupa $\mathbb{Z}_6$ je ciklična grupa s šestimi elementi. Predstavimo jo lahko tudi na način $e = x^0, x^1, x^2, x^3, x^4, x^5$, kjer je $x^m \cdot x^n = x^{m+n}$, pri čemer se eksponent računa po modulu 5. Vzamemo njeno bolj standardno predstavitev, $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$. Element $3 \in \mathbb{Z}_6$ generira podgrupo z dvema elementoma, $\langle 3\rangle = \{0, 3\}$. Zato je kvocientna grupa reda $\mid \mathbb{Z}_6 \mid / \mid \langle 3\rangle \mid = \frac{6}{2} = 3$.

- $(\mathbb{Z}_{12} \times \mathbb{Z}_{18})/\langle(4, 3)\rangle$:
  Zapišimo elemente grupe $\mathbb{Z}_{12}$ in grupe $\mathbb{Z}_{18}$:
  $\mathbb{Z}_{12} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$,
  $\mathbb{Z}_{18} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17\}$.
  Grupa $\mathbb{Z}_{12} \times \mathbb{Z}_{18}$ ima $12 \cdot 18 = 216$ elementov. Poiščimo tudi število elementov podgrupe $\langle(4, 3)\rangle$ v $\mathbb{Z}_{12} \times \mathbb{Z}_{18}$. Ker je
  $\gcd(4, 12) = 4$, $\frac{12}{4} = 3$,
  $\gcd(3, 18) = 3$, $\frac{18}{3} = 6$ in
  $\mathrm{lcm}(3, 6) = 6$, element $(4, 3)$ generira podgrupo s šestimi elementi. Od tod izračunamo tudi število elementov kvocientne grupe $(\mathbb{Z}_{12}\times\mathbb{Z}_{18})/\langle(4, 3)\rangle$: $\frac{216}{6} = 36$.

2.2.6 Homomorfizmi grup

Definicija 2.105. Naj bosta $(F, \circ)$ in $(G, \star)$ grupi. Preslikavo ϕ, ki slika iz grupe F v grupo G, imenujemo **homomorfizem**, če za vse $f_1, f_2 \in F$ velja

$$\phi(f_1 \cdot f_2) = \phi(f_1)\phi(f_2).$$

Opomba 2.106. Za vsaki grupi F in G obstaja vsaj en homomorfizem $\phi : F \to G$, ki ga imenujemo **trivialni homomorfizem**. Definiran je kot $\phi(f) = e$, kjer je $f \in F$ in e nevtralni element v grupi G.

Opomba 2.107. Če je ϕ homomorfizem iz grupe F na grupo G, je $\phi(f^{-1}) = \phi(f)^{-1}$ za vsak $f \in F$.

Primer 2.108. Dani imamo grupi $(\mathbb{Z}, +)$ in $(\{1, -1\}, \cdot)$. Definiramo preslikavo

$$\phi(n) = \begin{cases} 1, & \text{če je } n \text{ sod,} \\ -1 & \text{če je } n \text{ lih.} \end{cases}$$

Dokažimo, da je ϕ homomorfizem grup.

- Dani imamo dve sodi števili, $2n$ in $2m$:
  $\phi(2n + 2m) = \phi(2(m + n)) = 1$.

$2(m+n)$ je sodo število, zato se s preslikavo ϕ preslika v 1.

$\phi(2n)\phi(2m) = 1 \cdot 1 = 1$.

Vidimo, da velja enakost $\phi(2n+2m) = \phi(2n)\phi(2m)$.

- Dani imamo dve lihi števili, $2m+1$ in $2n+1$:

  $\phi((2m+1)+(2n+1)) = \phi(2m+2n+2) = \phi(2(m+n+1)) = 1$.

  Število $2(m+n+1)$ je sodo, zato je vrednost preslikave 1.

  $\phi(2m+1)\phi(2n+1) = (-1) \cdot (-1) = 1$.

  Torej velja enakost $\phi((2m+1)+(2n+1)) = \phi(2m+1)\phi(2n+1)$.

- Dano imamo liho število $2n+1$ in sodo število $2m$:

  $\phi(2n+1+2m) = \phi(2n+2m+1) = -1$.

  Število je liho število, zato je vrednost preslikave -1.

  $\phi(2n+1)\phi(2m) = (-1) \cdot 1 = -1$.

  Ker sta $(\mathbb{Z},+)$ in $(\{1,-1\},\cdot)$ Abelovi grupi, lahko sklepamo, da velja tudi $\phi(2m+2n+1) = \phi(2m)\phi(2n+1)$. Torej je ϕ res homomorfizem.

Definicija 2.109. Če je homomorfizem ϕ injektiven, imenujemo tak homomorfizem **epimorfizem**.

Definicija 2.110. Preslikavo ϕ imenujemo **izomorfizem**, če je:

- ϕ bijektivna preslikava,
- ϕ homomorfizem,
- ϕ^{-1} homomorfizem.

Opomba 2.111. Če je preslikava ϕ izomorfizem, je inverz enak $\phi^{-1} : G \longrightarrow F$.

Opomba 2.112. Homomorfizem $\phi : F \longrightarrow F$ imenujemo **endomofrizem**. Bijektivni endomorfizem imenujemo **automorfizem**.

Definicija 2.113. Naj bosta F in G grupi. Če je $\phi : F \longrightarrow G$ izomorfizem, sta grupi F in G izomorfni. To zapišemo kot $F \cong G$.

Bralec lahko primere izomorfizmov in epimorfizma prebere v [1].

Definicija 2.114. Naj bo $\phi : F \to G$ homomorfizem grup. Podgrupo $\phi^{-1}[\{e\}] = \{f \in F \mid \phi(f) = e\}$ imenujemo **jedro** homomorfizma ϕ in ga označimo s $\mathrm{Ker}(\phi)$.

Naslednji primer je povzet iz 13. poglavja v [8].

Primer 2.115. Poiščimo Ker(ϕ) in $\phi(3)$ za homomorfizem $\phi : \mathbb{Z}_{10} \to \mathbb{Z}_{20}$, definiram s predpisom $\phi(1) = 8$. Ob upoštevanju podatkov naloge zapišemo enačbo $8n = 0$ (mod 20), $n \in \mathbb{Z}$. Ker je n element iz $\mathbb{Z}_{10}$, sta možni samo števili 0 in 5. Zato je $\mathrm{Ker}(\phi) = \{0, 5\} = \langle 5 \rangle$. Izračunamo še $\phi(3) = 8 \cdot 3 = 24 \equiv 4(\mathrm{mod}\ 20)$.

Definicija 2.116. Sliko homomorfizma ϕ definiramo kot $\mathrm{Im}(\phi) = \{\phi(f) \mid f \in F\}$.

Dokaz naslednje trditve je povzet po [35].

Trditev 2.117. *Jedro homomorfizma $\phi : G \longrightarrow H$ je podgrupa edinka.*

Dokaz. Naj bo $n \in \mathrm{Ker}(\phi)$ in e_H identeta za H. Potem je:
$\phi(gng^{-1}) = \phi(g)\phi(n)\phi(g^{-1}) = \phi(g)e_H(g^{-1}) = \phi(g)\phi(g)^{-1} = e_H$ za vsak $g \in G$, kar pomeni, da je $\mathrm{Ker}(\phi) \trianglelefteq G$. □

Trditev 2.118. *Naj bosta F in G grupi in $\phi : F \longrightarrow G$ homomorfizem. Potem je* $\mathrm{Ker}(\phi) \trianglelefteq F$ *in* $\phi(K) \leq G$ *za vse* $K \leq F$.

Dokaz. Da je $\mathrm{Ker}(\phi) \trianglelefteq F$ smo dokazali pri trditvi 2.117. Dokažimo še $\phi(K) \leq G$. Naj bo $X = \phi(K)$. Zadostuje, da preverimo, ali je X neprazna množica in zaprta za množenje in za inverz. Že zgoraj smo zapisali, da je $\phi(f) = e$. Zato X vsebuje f, ki je identiteta za grupo G. Homomorfizem slika inverz v inverz, kar zapišemo tudi kot $\phi(a^{-1}) = \phi(a)^{-1}$. Zato je X zaprt za inverz. Prav tako je X po definiciji zaprt za produkt. Torej je X res podgrupa. □

Dokaz prvega izreka o izomorfizmu lahko preberete v [34].

Izrek 2.119. *Naj bo $\phi : F \to G$ homomorfizem z jedrom H. Potem odseki po H oblikujejo kvocientno grupo F/H, kjer $(aH)(bH) = (ab)H$. Preslikava $\mu : F/H \to \phi(F)$ definiramo z $\mu(aH) = \phi(a)$ je* ***izomorfizem****.*

Dokaz. Da je preslikava μ izomorfizem, moramo dokazati naslednje pogoje:

- preslikava μ je dobro definirana,
- preslikava μ je injektivna,
- preslikava μ je surjektivna in
- preslikava μ je homomorfizem.

Za dokaz 1. točke dokažimo implikacijo $a_1H = a_2H \implies \mu(a_1H) = \mu(a_2H)$. Privzamemo, da je $a_1H = a_2H$ za $a_1, a_2 \in F$. Potem je $a_1^{-1}a_2 \in H$. Vemo, da je $\phi(a_1^{-1}a_2) = e_G$. Ker je $\phi(a_1^{-1}a_2) = \phi(a_1)^{-1}\phi(a_2)$, je $\phi(a_1)^{-1}\phi(a_2) = e_G$. Zato je $\phi(a_1) = \phi(a_2)$ in $\mu(a_1H) = \mu(a_2H)$. Preslikava μ je injektivna, če iz $\mu(a_1H) = \mu(a_2H)$

sledi $a_1H = a_2H$. To dokažemo tako, da dokaz pod točko 1 dokažemo v obratni smeri. Dokažimo še surjektivnost preslikave μ. Kodomena preslikave μ je $\phi(F)$. Za surjektivnost preslikave μ moramo dokazati, da je slika preslikave μ enaka $\mu(F/H)$, kar je enako $\phi(F)$.

$$\mu(F/H) = \{\mu(aH) : a \in F\} = \{\phi(a); a \in F\} = \phi(K).$$

Dokažimo še, da je preslikava μ homomorfizem. Za vsak $a_1, a_2 \in F$ je $\mu(a_1H \cdot a_2H) = \mu(a_1a_2H) = \phi(a_1a_2) = \phi(a_1)\phi(a_2) = \mu(a_1H)\mu(a_2H)$. Pri dokazu smo uporabili definicijo produkta v kvocientnih grupah. Preslikava μ je torej homomorfizem. Po izreku **??** je tudi ${}^{F}/_{\mathrm{Ker}(\phi)} \cong \phi(F)$. □

Primer 2.120. Naj bo $\phi : \mathbb{Z} \to \mathbb{Z}_n$ homomorfizem definiran kot $\phi(x) = k(\text{mod } n)$. Zaloga vrednosti homomorfizma ϕ je enaka $\mathrm{Im}(\phi) = \mathbb{Z}_n$. Jedro tega homomorfizma je enako $n\mathbb{Z}$. Po prvem izreku izomorfizma je $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$.

Trditev 2.121. *Vsaka neskončna ciklična grupa G je izomorfna grupi $(\mathbb{Z}, +)$.*

Dokaz. Naj bo G neskončna ciklična grupa z generatorjem g. Definiramo preslikavo $f : \mathbb{Z} \to G$, $f(n) = g^n$. Dokažimo, da je preslikava f izomorfizem.

- Naj bo $g_1 \in G$ poljuben. Potem obstaja tak $n \in \mathbb{Z}$, da je $g_1 = g^n$. Torej je funkcija $f(n) = g^n$, $n \in \mathbb{Z}$ dobro definirana.
- Dokažimo, da je preslikava f homomorfizem. To pomeni, da je $f(m + n) = f(m)f(n)$. Preverimo: $f(m + n) = g^{m+n} = g^m g^n = f(m)f(n)$.
- Dokažimo še, da je preslikava f surjektivna. Ker je G ciklična grupa, lahko vsak element iz grupe zapišemo kot potenco z osnovo g. Torej za vsak element g_1 iz G obstaja tak $n \in \mathbb{Z}$ da velja $g_1 = g^n$. Glede na definicijo preslikave f je $f(n) = g^n = g_1$. Preslikava f je surjektivna.
- Naj bosta $m, n \in \mathbb{Z}$. Če je $f(m) = f(n)$, potem je $g^m = g^n$. Toda ta dva elementa sta različna. Edina možna rešitev je, da sta m in n enaka. Funkcija f je torej injektivna funkcija.

Ker je funkcija f surjektivni in injektivni homomorfizem, je grupa G izomorfna grupi $(\mathbb{Z}, +)$.

□

3 Osnovne lastnosti hipergrup

V tem poglavju bomo spoznali nekaj malega o zgodovini hipergrup ter se pobližje seznanili z osnovnimi definicijami in primeri hipergrup.

3.1 Zgodovinski razvoj hipergrup

Teorijo hiperstruktur (hipergrup) je prvič predstavil francoski matematik Marty na osmem kongresu skandinavskih matematikov leta 1934. Hiperstrukture predstavljajo naravno posplošitev grup. Vemo, da je v grupi produkt dveh elementov en sam element. V hipergrupi pa velja, da je produkt dveh elementov množica. Kot motivacijski primer je Marty podal kvocientno množico $G/K = \{xK \mid x \in G\}$, v kateri je G grupa in K njena podgrupa, ne nujno edinka. Okrog leta 1940 so teorijo hiperstruktur proučevali različni francoski, ameriški in italijanski matematiki. Marty, Krasner, Dresher in drugi so proučevali teorijo v povezavi z grupami in uporabo te teorije v geometriji. Ker se je raziskovalno področje hiperstruktur zelo razširilo, je ta teorija od leta 1970 naprej doživela velik napredek. Uporabo hiperstruktur so na področjih geometrije, topologije, kriptografije, verjetnosti ipd. raziskovali različni avtorji [5]. Teorija hipergrup po eni strani posplošuje teorijo grup, po drugi strani pa vpeljuje nove koncepte, ki omogočajo širšo uporabno vrednost.

3.2 Osnovne definicije in primeri hipergrup

Definicija 3.1. Naj bo M neprazna množica in $\mathcal{P}^*(M)$ družina vseh nepraznih podmnožic množice M. Potem preslikavo $\circ : M \times M \to \mathcal{P}^*(M)$ imenujemo **hiperoperacija** na množici M. Par $(M, \circ)$ imenujemo **hipergrupoid**. Če je razvidno, kaj je hiperoperacija, potem lahko hipergrupoid označimo tudi samo z M.

Definicija 3.2. Naj bo M neprazna množica, $\mathcal{P}^*(M)$ družina vseh nepraznih podmnožic množice M in $\circ : M \times M \to \mathcal{P}^*(M)$ hiperoperacija na množici M. Potem imenujemo hipergrupoid $(M, \circ)$ **polhipergrupa**, če za vse $x, y, z \in M$ velja, da je $(x \circ y) \circ z = x \circ (y \circ z)$, kar pomeni, da je

$$\bigcup_{u \in x \circ y} u \circ z = \bigcup_{v \in y \circ z} x \circ v.$$

Opomba 3.3. Že v razdelku o zgodovini hipergrup smo zapisali, da je v hiperstrukturi produkt dveh elementov množica. Posledično so vsi zapisi oblike $x \circ y$ množice, zato bomo zapis $x \circ y$ nadomestili z N. Potem velja

$$(x \circ y) \circ z = N \circ z = \bigcup_{n \in N} n \circ z.$$

Ker je $\circ$ hiperoperacija, je tudi $n \circ z$ množica. Od tu sklepamo, da je rezultat hiperoperacije unija množic.

Primer 3.4. Naj bo $S = \{a, b, c, d\}$ množica s štirimi elementi. Potem je $(S, \cdot)$ polhipergrupa, kjer je hiperoperacija $\cdot$ definirana kot prikazuje spodnja tabela:

$\cdot$	a	b	c	d
a	$\{a\}$	$\{b\}$	$\{c\}$	$\{d\}$
b	$\{b\}$	$\{a, c\}$	$\{b, c\}$	$\{d\}$
c	$\{c\}$	$\{b, c\}$	$\{a, b\}$	$\{d\}$
d	$\{d\}$	$\{d\}$	$\{d\}$	S

Če želimo dokazati, da je $(S, \cdot)$ polhipergrupa, moramo po definiciji 3.2 dokazati, da za poljubne tri elemente iz množice S velja asociativnostni zakon. Če na primer vzamemo iz množice S elemente a, b, c, potem moramo dokazati, da velja

$$(a \cdot b) \cdot c = a \cdot (b \cdot c). \tag{3.1}$$

Glede na definicijo hiperoperacije, ki jo prikazuje zgornja tabela, je

$$a \cdot b = \{b\},$$

$$\{b\} \cdot c = \{b, c\}.$$

Na enak način preverimo tudi desno stran enakosti (3.1) in upoštevamo, da je rezultat hiperoperacije unija množic:

$$b \cdot c = \{b, c\},$$

$$a \cdot \{b, c\} = a \cdot b \bigcup a \cdot c = \{b\} \bigcup \{c\} = \{b, c\}.$$

Leva stran enakosti (3.1) je enaka desni strani enakosti (3.1), zato za elemente $a, b, c \in S$ velja asociativnostni zakon. Na enak način moramo preveriti tudi vse druge možne izbore treh elementov, le-teh je $4^3 = 64$. To storimo v nadaljevanju:

- $(a \cdot a) \cdot a = \{a\} \cdot a = \{a\}, a \cdot (a \cdot a) = a \cdot \{a\} = \{a\} \Rightarrow (a \cdot a) \cdot a = a \cdot (a \cdot a),$
- $(a \cdot a) \cdot b = \{a\} \cdot b = \{b\}, a \cdot (a \cdot b) = a \cdot \{b\} = \{b\} \Rightarrow (a \cdot a) \cdot b = a \cdot (a \cdot b),$

- $(a \cdot a) \cdot c = \{a\} \cdot c = \{c\}, a \cdot (a \cdot c) = a \cdot \{c\} = \{c\} \Rightarrow (a \cdot a) \cdot c = a \cdot (a \cdot c)$,
- $(a \cdot a) \cdot d = \{a\} \cdot d = \{d\}, a \cdot (a \cdot d) = a \cdot \{d\} = \{d\} \Rightarrow (a \cdot a) \cdot d = a \cdot (a \cdot d)$,
- $(a \cdot b) \cdot a = \{b\} \cdot a = \{b\}, a \cdot (b \cdot a) = a \cdot \{b\} = \{b\} \Rightarrow (a \cdot b) \cdot a = a \cdot (b \cdot a)$,
- $(a \cdot b) \cdot b = \{b\} \cdot b = \{a, c\}, a \cdot (b \cdot b) = a \cdot \{a, c\} = a \cdot a \bigcup a \cdot c = \{a\} \bigcup \{c\} = \{a, c\} \Rightarrow (a \cdot b) \cdot b = a \cdot (b \cdot b)$,
- $(a \cdot b) \cdot c = \{b\} \cdot c = \{b, c\}, a \cdot (b \cdot c) = a \cdot \{b, c\} = a \cdot b \bigcup a \cdot c = \{b\} \bigcup \{c\} = \{b, c\} \Rightarrow (a \cdot b) \cdot c = a \cdot (b \cdot c)$,
- $(a \cdot b) \cdot d = \{b\} \cdot d = \{d\}, a \cdot (b \cdot d) = a \cdot \{d\} = \{d\} \Rightarrow (a \cdot b) \cdot d = a \cdot (b \cdot d)$,
- $(a \cdot c) \cdot a = \{c\} \cdot a = \{c\}, a \cdot (c \cdot a) = a \cdot \{c\} = \{c\} \Rightarrow (a \cdot c) \cdot a = a \cdot (c \cdot a)$,
- $(a \cdot c) \cdot b = \{c\} \cdot b = \{b, c\}, a \cdot (c \cdot b) = a \cdot \{b, c\} = a \cdot b \bigcup a \cdot c = \{b\} \bigcup \{c\} = \{b, c\} \Rightarrow (a \cdot c) \cdot b = a \cdot (c \cdot b)$,
- $(a \cdot c) \cdot c = \{c\} \cdot c = \{a, b\}, a \cdot (c \cdot c) = a \cdot \{a, b\} = a \cdot a \bigcup a \cdot b = \{a\} \bigcup \{b\} = \{a, b\} \Rightarrow (a \cdot c) \cdot c = a \cdot (c \cdot c)$,
- $(a \cdot c) \cdot d = \{c\} \cdot d = \{d\}, a \cdot (c \cdot d) = a \cdot \{d\} = \{d\} \Rightarrow (a \cdot c) \cdot d = a \cdot (c \cdot d)$,
- $(a \cdot d) \cdot a = \{d\} \cdot a = \{d\}, a \cdot (d \cdot a) = a \cdot \{d\} = \{d\} \Rightarrow (a \cdot d) \cdot a = a \cdot (d \cdot a)$,
- $(a \cdot d) \cdot b = \{d\} \cdot b = \{d\}, a \cdot (d \cdot b) = a \cdot \{d\} = \{d\} \Rightarrow (a \cdot d) \cdot b = a \cdot (d \cdot b)$,
- $(a \cdot d) \cdot c = \{d\} \cdot c = \{d\}, a \cdot (d \cdot c) = a \cdot \{d\} = \{d\} \Rightarrow (a \cdot d) \cdot c = a \cdot (d \cdot c)$,
- $(a \cdot d) \cdot d = \{d\} \cdot d = \{a, b, c, d\} = S, a \cdot (d \cdot d) = a \cdot S = a \cdot \{a, b, c, d\} = a \cdot a \bigcup a \cdot b \bigcup a \cdot c \bigcup a \cdot d = \{a\} \bigcup \{b\} \bigcup \{c\} \bigcup \{d\} = \{a, b, c, d\} = S \Rightarrow (a \cdot d) \cdot d = a \cdot (d \cdot d)$,
- $(b \cdot a) \cdot a = \{b\} \cdot a = \{b\}, b \cdot (a \cdot a) = b \cdot \{a\} = \{b\} \Rightarrow (b \cdot a) \cdot a = b \cdot (a \cdot a)$,
- $(b \cdot a) \cdot b = \{b\} \cdot b = \{a, c\}, b \cdot (a \cdot b) = b \cdot \{b\} = \{a, c\} \Rightarrow (b \cdot a) \cdot b = b \cdot (a \cdot b)$,
- $(b \cdot a) \cdot c = \{b\} \cdot c = \{b, c\}, b \cdot (a \cdot c) = b \cdot \{c\} = \{b, c\} \Rightarrow (b \cdot a) \cdot c = b \cdot (a \cdot c)$,
- $(b \cdot a) \cdot d = \{b\} \cdot d = \{d\}, b \cdot (a \cdot d) = b \cdot \{d\} = \{d\} \Rightarrow (b \cdot a) \cdot d = b \cdot (a \cdot d)$,
- $(b \cdot b) \cdot a = \{a, c\} \cdot a = a \cdot a \bigcup c \cdot a = \{a\} \bigcup \{c\} = \{a, c\}, b \cdot (b \cdot a) = b \cdot \{b\} = \{a, c\} \Rightarrow (b \cdot b) \cdot a = b \cdot (b \cdot a)$,
- $(b \cdot b) \cdot b = \{a, c\} \cdot b = a \cdot b \bigcup c \cdot b = \{b\} \bigcup \{b, c\} = \{b, c\}, b \cdot (b \cdot b) = b \cdot \{a, c\} = b \cdot a \bigcup b \cdot c = \{b\} \bigcup \{b, c\} = \{b, c\} \Rightarrow (b \cdot b) \cdot b = b \cdot (b \cdot b)$,

- $(b \cdot b) \cdot c = \{a, c\} \cdot c = a \cdot c \bigcup c \cdot c = \{c\} \bigcup \{a, b\} = \{a, b, c\}, b \cdot (b \cdot c) = b \cdot \{b, c\} = b \cdot b \bigcup b \cdot c = \{a, c\} \bigcup \{b, c\} = \{a, b, c\} \Rightarrow (b \cdot b) \cdot c = b \cdot (b \cdot c)$,
- $(b \cdot b) \cdot d = \{a, c\} \cdot d = a \cdot d \bigcup c \cdot d = \{d\} \bigcup \{d\} = \{d\}, b \cdot (b \cdot d) = b \cdot \{d\} = \{d\} \Rightarrow (b \cdot b) \cdot d = b \cdot (b \cdot d)$,
- $(b \cdot c) \cdot a = \{b, c\} \cdot a = b \cdot a \bigcup c \cdot a = \{b\} \bigcup \{c\} = \{b, c\}, b \cdot (c \cdot a) = b \cdot \{c\} = \{b, c\} \Rightarrow (b \cdot c) \cdot a = b \cdot (c \cdot a)$,
- $(b \cdot c) \cdot b = \{b, c\} \cdot b = b \cdot b \bigcup c \cdot b = \{a, c\} \bigcup \{b, c\} = \{a, b, c\}, b \cdot (c \cdot b) = b \cdot \{b, c\} = b \cdot b \bigcup b \cdot c = \{a, c\} \bigcup \{b, c\} = \{a, b, c\} \Rightarrow (b \cdot c) \cdot b = b \cdot (c \cdot b)$,
- $(b \cdot c) \cdot c = \{b, c\} \cdot c = b \cdot c \bigcup c \cdot c = \{b, c\} \bigcup \{a, b\} = \{a, b, c\}, b \cdot (c \cdot c) = b \cdot \{a, b\} = b \cdot a \bigcup b \cdot b = \{b\} \bigcup \{a, c\} = \{a, b, c\} \Rightarrow (b \cdot c) \cdot c = b \cdot (c \cdot c)$,
- $(b \cdot c) \cdot d = \{b, c\} \cdot d = b \cdot d \bigcup c \cdot d = \{d\} \bigcup \{d\} = \{d\}, b \cdot (c \cdot d) = b \cdot \{d\} = \{d\} \Rightarrow (b \cdot c) \cdot d = b \cdot (c \cdot d)$,
- $(b \cdot d) \cdot a = \{d\} \cdot a = \{d\}, b \cdot (d \cdot a) = b \cdot \{d\} = \{d\} \Rightarrow (b \cdot d) \cdot a = b \cdot (d \cdot a)$,
- $(b \cdot d) \cdot b = \{d\} \cdot b = \{d\}, b \cdot (d \cdot b) = b \cdot \{d\} = \{d\} \Rightarrow (b \cdot d) \cdot b = b \cdot (d \cdot b)$,
- $(b \cdot d) \cdot c = \{d\} \cdot c = \{d\}, b \cdot (d \cdot c) = b \cdot \{d\} = \{d\} \Rightarrow (b \cdot d) \cdot c = b \cdot (d \cdot c)$,
- $(b \cdot d) \cdot d = \{d\} \cdot d = \{a, b, c, d\} = S, b \cdot (d \cdot d) = b \cdot S = b \cdot \{a, b, c, d\} = b \cdot a \bigcup b \cdot b \bigcup b \cdot c \bigcup b \cdot d = \{b\} \bigcup \{a, c\} \bigcup \{b, c\} \bigcup \{d\} = \{a, b, c, d\} = S \Rightarrow (b \cdot d) \cdot d = b \cdot (d \cdot d)$,
- $(c \cdot a) \cdot a = \{c\} \cdot a = \{c\}, c \cdot (a \cdot a) = c \cdot \{a\} = \{c\} \Rightarrow (c \cdot a) \cdot a = c \cdot (a \cdot a)$,
- $(c \cdot a) \cdot b = \{c\} \cdot b = \{b, c\}, c \cdot (a \cdot b) = c \cdot \{b\} = \{b, c\} \Rightarrow (c \cdot a) \cdot b = c \cdot (a \cdot b)$,
- $(c \cdot a) \cdot c = \{c\} \cdot c = \{a, b\}, c \cdot (a \cdot c) = c \cdot \{c\} = \{a, b\} \Rightarrow (c \cdot a) \cdot c = c \cdot (a \cdot c)$,
- $(c \cdot a) \cdot d = \{c\} \cdot d = \{d\}, c \cdot (a \cdot d) = c \cdot \{d\} = \{d\} \Rightarrow (c \cdot a) \cdot d = c \cdot (a \cdot d)$,
- $(c \cdot b) \cdot a = \{b, c\} \cdot a = b \cdot a \bigcup c \cdot a = \{b\} \bigcup \{c\} = \{b, c\}, c \cdot (b \cdot a) = c \cdot \{b\} = \{b, c\} \Rightarrow (c \cdot b) \cdot a = c \cdot (b \cdot a)$,
- $(c \cdot b) \cdot b = \{b, c\} \cdot b = b \cdot b \bigcup c \cdot b = \{a, c\} \bigcup \{b, c\} = \{a, b, c\}, c \cdot (b \cdot b) = c \cdot \{a, c\} = c \cdot a \bigcup c \cdot c = \{c\} \bigcup \{a, b\} = \{a, b, c\} \Rightarrow (c \cdot b) \cdot b = c \cdot (b \cdot b)$,
- $(c \cdot b) \cdot c = \{b, c\} \cdot c = b \cdot c \bigcup c \cdot c = \{b, c\} \bigcup \{a, b\} = \{a, b, c\}, c \cdot (b \cdot c) = c \cdot \{b, c\} = c \cdot b \bigcup c \cdot c = \{b, c\} \bigcup \{a, b\} = \{a, b, c\} \Rightarrow (c \cdot b) \cdot c = c \cdot (b \cdot c)$,
- $(c \cdot b) \cdot d = \{b, c\} \cdot d = b \cdot d \bigcup c \cdot d = \{d\} \bigcup \{d\} = \{d\}, c \cdot (b \cdot d) = c \cdot \{d\} = \{d\} \Rightarrow (c \cdot b) \cdot d = c \cdot (b \cdot d)$,

- $(c \cdot c) \cdot a = \{a, b\} \cdot a = a \cdot a \bigcup b \cdot a = \{a\} \bigcup \{b\} = \{a, b\}, c \cdot (c \cdot a) = c \cdot \{c\} = \{a, b\} \Rightarrow (c \cdot c) \cdot a = c \cdot (c \cdot a)$,
- $(c \cdot c) \cdot b = \{a, b\} \cdot b = a \cdot b \bigcup b \cdot b = \{b\} \bigcup \{a, c\} = \{a, b, c\}, c \cdot (c \cdot b) = c \cdot \{b, c\} = c \cdot b \bigcup c \cdot c = \{b, c\} \bigcup \{a, b\} = \{a, b, c\} \Rightarrow (c \cdot c) \cdot b = c \cdot (c \cdot b)$,
- $(c \cdot c) \cdot c = \{a, b\} \cdot c = a \cdot c \bigcup b \cdot c = \{c\} \bigcup \{b, c\} = \{b, c\}, c \cdot (c \cdot c) = c \cdot \{a, b\} = c \cdot a \bigcup c \cdot b = \{c\} \bigcup \{b, c\} = \{b, c\} \Rightarrow (c \cdot c) \cdot c = c \cdot (c \cdot c)$,
- $(c \cdot c) \cdot d = \{a, b\} \cdot d = a \cdot d \bigcup b \cdot d = \{d\} \bigcup \{d\} = \{d\}, c \cdot (c \cdot d) = c \cdot \{d\} = \{d\} \Rightarrow (c \cdot c) \cdot d = c \cdot (c \cdot d)$,
- $(c \cdot d) \cdot a = \{d\} \cdot a = \{d\}, c \cdot (d \cdot a) = c \cdot \{d\} = \{d\} \Rightarrow (c \cdot d) \cdot a = c \cdot (d \cdot a)$,
- $(c \cdot d) \cdot b = \{d\} \cdot b = \{d\}, c \cdot (d \cdot b) = c \cdot \{d\} = \{d\} \Rightarrow (c \cdot d) \cdot b = c \cdot (d \cdot b)$,
- $(c \cdot d) \cdot c = \{d\} \cdot c = \{d\}, c \cdot (d \cdot c) = c \cdot \{d\} = \{d\} \Rightarrow (c \cdot d) \cdot c = c \cdot (d \cdot c)$,
- $(c \cdot d) \cdot d = \{d\} \cdot d = \{a, b, c, d\} = S, c \cdot (d \cdot d) = c \cdot S = c \cdot \{a, b, c, d\} = c \cdot a \bigcup c \cdot b \bigcup c \cdot c \bigcup c \cdot d = \{c\} \bigcup \{b, c\} \bigcup \{a, b\} \bigcup \{d\} = \{a, b, c, d\} = S \Rightarrow (c \cdot d) \cdot d = c \cdot (d \cdot d)$,
- $(d \cdot a) \cdot a = \{d\} \cdot a = \{d\}, d \cdot (a \cdot a) = d \cdot \{a\} = \{d\} \Rightarrow (d \cdot a) \cdot a = d \cdot (a \cdot a)$,
- $(d \cdot a) \cdot b = \{d\} \cdot b = \{d\}, d \cdot (a \cdot b) = d \cdot \{b\} = \{d\} \Rightarrow (d \cdot a) \cdot b = d \cdot (a \cdot b)$,
- $(d \cdot a) \cdot c = \{d\} \cdot c = \{d\}, d \cdot (a \cdot c) = d \cdot \{c\} = \{d\} \Rightarrow (d \cdot a) \cdot c = d \cdot (a \cdot c)$,
- $(d \cdot a) \cdot d = \{d\} \cdot d = S, d \cdot (a \cdot d) = d \cdot \{d\} = S \Rightarrow (d \cdot a) \cdot d = d \cdot (a \cdot d)$,
- $(d \cdot b) \cdot a = \{d\} \cdot a = \{d\}, d \cdot (b \cdot a) = d \cdot \{b\} = \{d\} \Rightarrow (d \cdot b) \cdot a = d \cdot (b \cdot a)$,
- $(d \cdot b) \cdot b = \{d\} \cdot b = \{d\}, d \cdot (b \cdot b) = d \cdot \{a, c\} = d \cdot a \bigcup d \cdot c = \{d\} \bigcup \{d\} = \{d\} \Rightarrow (d \cdot b) \cdot b = d \cdot (b \cdot b)$,
- $(d \cdot b) \cdot c = \{d\} \cdot c = \{d\}, d \cdot (b \cdot c) = d \cdot \{b, c\} = d \cdot b \bigcup d \cdot c = \{d\} \bigcup \{d\} = \{d\} \Rightarrow (d \cdot b) \cdot c = d \cdot (b \cdot c)$,
- $(d \cdot b) \cdot d = \{d\} \cdot d = S = \{a, b, c, d\}, d \cdot (b \cdot d) = d \cdot \{d\} = S = \{a, b, c, d\} \Rightarrow (d \cdot b) \cdot d = d \cdot (b \cdot d)$,
- $(d \cdot c) \cdot a = \{d\} \cdot a = \{d\}, d \cdot (c \cdot a) = d \cdot \{c\} = \{d\} \Rightarrow (d \cdot c) \cdot a = d \cdot (c \cdot a)$,
- $(d \cdot c) \cdot b = \{d\} \cdot b = \{d\}, d \cdot (c \cdot b) = d \cdot \{b, c\} = d \cdot b \bigcup d \cdot c = \{d\} \bigcup \{d\} = \{d\} \Rightarrow (d \cdot c) \cdot b = d \cdot (c \cdot b)$,
- $(d \cdot c) \cdot c = \{d\} \cdot c = \{d\}, d \cdot (c \cdot c) = d \cdot \{a, b\} = d \cdot a \bigcup d \cdot b = \{d\} \bigcup \{d\} = \{d\} \Rightarrow (d \cdot c) \cdot c = d \cdot (c \cdot c)$,

- $(d \cdot c) \cdot d = \{d\} \cdot d = S = \{a,b,c,d\}, d \cdot (c \cdot d) = d \cdot \{d\} = S = \{a,b,c,d\} \Rightarrow (d \cdot c) \cdot d = d \cdot (c \cdot d)$,

- $(d \cdot d) \cdot a = S \cdot a = \{a,b,c,d\} \cdot a = a \cdot a \bigcup b \cdot a \bigcup c \cdot a \bigcup d \cdot a = \{a\} \bigcup \{b\} \bigcup \{c\} \bigcup \{d\} = \{a,b,c,d\}, d \cdot (d \cdot a) = d \cdot \{d\} = S = \{a,b,c,d\} \Rightarrow (d \cdot d) \cdot a = d \cdot (d \cdot a)$,

- $(d \cdot d) \cdot b = S \cdot b = \{a,b,c,d\} \cdot b = a \cdot b \bigcup b \cdot b \bigcup c \cdot b \bigcup d \cdot b = \{b\} \bigcup \{a,c\} \bigcup \{b,c\} \bigcup \{d\} = \{a,b,c,d\}, d \cdot (d \cdot b) = d \cdot \{d\} = S = \{a,b,c,d\} \Rightarrow (d \cdot d) \cdot b = d \cdot (d \cdot b)$,

- $(d \cdot d) \cdot c = S \cdot c = \{a,b,c,d\} \cdot c = a \cdot c \bigcup b \cdot c \bigcup c \cdot c \bigcup d \cdot c = \{c\} \bigcup \{b,c\} \bigcup \{a,b\} \bigcup \{d\} = \{a,b,c,d\}, d \cdot (d \cdot c) = d \cdot \{d\} = S = \{a,b,c,d\} \Rightarrow (d \cdot d) \cdot c = d \cdot (d \cdot c)$,

- $(d \cdot d) \cdot d = S \cdot d = \{a,b,c,d\} \cdot d = a \cdot d \bigcup b \cdot d \bigcup c \cdot d \bigcup d \cdot d = \{d\} \bigcup \{d\} \bigcup \{d\} \bigcup S = \{a,b,c,d\}, (d \cdot d) \cdot d = d \cdot S = d \cdot \{a,b,c,d\} = d \cdot a \bigcup d \cdot b \bigcup d \cdot c \bigcup d \cdot d = \{d\} \bigcup \{d\} \bigcup \{d\} \bigcup S = \{a,b,c,d\} \Rightarrow (d \cdot d) \cdot d = d \cdot (d \cdot d)$.

Iz zgornjih zapisov vidimo, da za vse možnosti velja asociativnostni zakon, zato je S z dano hiperoperacijo $\cdot$ res polhipergrupa.

Definicija 3.5. [5] Dan imamo hipergrupoid $(M, \circ)$ in $x \in M$. Za poljubni neprazni podmnožici A in B množice M $(A, B \subseteq M)$ bomo uporabljali naslednji zapis:

$$A \circ B = \bigcup_{a \in A, b \in B} a \circ b, A \circ x = A \circ \{x\}, x \circ B = \{x\} \circ B.$$

Opomba 3.6. Elemente množice zapisujemo v obliki $\{x, y, z\}$. Ne glede na število elementov množice, smo zaradi lažjega razumevanja tak način zapisovanja uporabili tudi v primeru 3.4. V nadaljevanju bomo množice z enim samim elementom namesto $\{x\}$ zapisali v skrajšani obliki, to je x.

Opomba 3.7. Asociativnostni zakon v polhipergrupi $(S, \circ)$ lahko uporabimo tudi na podmnožicah $A, B, C \in S$. Velja naslednje:

$$A \circ (B \circ C) = (A \circ B) \circ C,$$

kjer je

$$B \circ C = \bigcup_{b \in B, c \in C} b \circ c, \qquad A \circ B = \bigcup_{a \in A, b \in B} a \circ b.$$

Definicija 3.8. Neprazno podmnožico A polhipergrupe $(M, \circ)$ imenujemo **podpolhipergrupa**, če je sama zase polhipergrupa. To z drugimi besedami pomeni tudi, da je neprazna podmnožica A polhipergrupe $(M, \circ)$ **podpolhipergrupa** če velja, da je $A \circ A \subseteq A$. To imenujemo tudi zaprtost za operacijo polhipergrupe. Množico M imenujemo **superpolhipergrupa** polhipergrupe A.

Opomba 3.9. Pojmi, predstavljeni v tej opombi, predstavljajo enakovredne pojme iz teorije grup. Neprazno podmnožico A polgrupe $(M, \circ)$ imenujemo **podpolgrupa**, če je sama zase polgrupa. To z drugimi besedami pomeni tudi, da je neprazna podmnožica A polgrupe $(M, \circ)$ **podpolgrupa** če velja, da je $A \circ A \subseteq A$. Množico M imenujemo **superpolgrupa** polgrupe A.

Naslednji primer pokaže, kako lahko iz dane polgrupe in njene podpolgrupe konstruiramo polhipergrupo.

Primer 3.10. Naj bo $(S, \cdot)$ polgrupa in K poljubna podpolgrupa polgrupe S. Potem je $S/K = \{x \cdot K \mid x \in S\}$ polhipergrupa za hiperoperacijo $\circ$ definirano na naslednji način

$$\bar{x} \circ \bar{y} = \{\bar{z} \mid z \in \bar{x} \cdot \bar{y}\}, \text{ kjer je } \bar{x} = x \cdot K.$$

Opomba 3.11. Produkt odsekov v polgrupi je množica elementov polgrupe:

$$\bar{x} \cdot \bar{y} = x \cdot K \cdot y \cdot K = \{x \cdot k_1 \cdot y \cdot k_2 \mid k_1, k_2 \in K\}.$$

Rezultat hiperoperacije $\circ$ je torej unija odsekov oblike $\bar{z} = z \cdot K, z \in \bar{x} \cdot \bar{y}$.

Da bomo dokazali, da je $S/K = \{x \cdot K \mid x \in S\}$ polhipergrupa za hiperoperacijo $\circ$, moramo dokazati, da velja asociativnostni zakon: $(\bar{x} \circ \bar{y}) \circ \bar{m} = \bar{x} \circ (\bar{y} \circ \bar{m})$ za poljubne $x, y, m \in S$. Najprej preverimo, kaj je rezultat hiproperacije dveh odsekov v polgrupi:

$$\bar{x} \circ \bar{y} = x \cdot K \circ y \cdot K = \{\bar{z} \mid z \in \bar{x} \cdot \bar{y}\} = \{z \cdot K \mid z \in x \cdot K \cdot y \cdot K\} =$$

$$\{z \cdot K \mid z = x \cdot k_1 \cdot y \cdot k_2, k_1, k_2 \in K\} = \{x \cdot k_1 \cdot y \cdot k_2 \cdot K \mid k_1, k_2 \in K\}.$$

Preverimo tudi, kaj je rezultat hiperoperacije treh odsekov $(\bar{x} \circ \bar{y}) \circ \bar{m}$ in $\bar{x} \circ (\bar{y} \circ \bar{m})$, ter, ali vrstni red izvajanja vpliva na rezultat hiperoperacije:

$$(\bar{x} \circ \bar{y}) \circ \bar{m} = \bigcup_{z \in \bar{x} \cdot \bar{y}} \{z \cdot K\} \circ \bar{m} = \bigcup_{z \in x \cdot K \cdot y \cdot K} \{z \cdot K\} \circ \bar{m} = \bigcup_{z \in x \cdot K \cdot y \cdot K} z \cdot K \circ \bar{m} =$$

$$\bigcup_{z \in x \cdot K \cdot y \cdot K} z \cdot K \cdot m \cdot K = x \cdot K \cdot y \cdot K \cdot K \cdot m \cdot K = x \cdot K \cdot y \cdot K \cdot m \cdot K.$$

Ker je K poljubna podpolgrupa polgrupe S, velja, da je $K \cdot K = K$. To smo upoštevali pri poenostavljanju zapisa $(\bar{x} \circ \bar{y}) \circ \bar{m}$ in bomo upoštevali tudi pri poenostavljanju zapisa $\bar{x} \circ (\bar{y} \circ \bar{m})$.

$$\bar{x} \circ (\bar{y} \circ \bar{m}) = \bar{x} \circ \bigcup_{z \in \bar{y} \cdot \bar{m}} \{z \cdot K\} = \bar{x} \circ \bigcup_{z \in y \cdot K \cdot m \cdot K} \{z \cdot K\} = \bigcup_{z \in y \cdot K \cdot m \cdot K} \bar{x} \circ z \cdot K =$$

$$\bigcup_{z \in y \cdot K \cdot m \cdot K} x \cdot K \cdot z \cdot K = x \cdot K \cdot y \cdot K \cdot m \cdot K \cdot K = x \cdot K \cdot y \cdot K \cdot m \cdot K.$$

Ker smo dokazali, da za hiperoperacijo $\circ$ velja $(\bar{x} \circ \bar{y}) \circ \bar{m} = \bar{x} \circ (\bar{y} \circ \bar{m})$, je $S/K = \{x \cdot K \mid x \in S\}$ polhipergrupa. V dokazu smo seveda na več mestih uporabili asociativnost v polgrupi S.

Definicija 3.12. Hipergrupoid $(H, \circ)$ imenujemo **kvazihipergrupa**, če za poljuben $a \in H$ velja, da je $a \circ H = H \circ a = H$. Ta pogoj imenujemo tudi **aksiom reprodukcije**.

Opomba 3.13. Iz opombe 3.3 vemo, da je rezultat hiperoperacije unija množic. Zato je tudi $a \circ H$ množica in velja

$$a \circ H = \bigcup_{h \in H} a \circ h.$$

Lahko rečemo, da množica vseh elementov množice H tvori nevtralni element.

Primer 3.14. Primer za kvazihipergrupo, ki jo bomo navedli v nadaljevanju, je vzet iz literature [19]. Naj bo $H = \{1, 2, 3\}$ množica s tremi elementi. Potem je $(H, \circ)$ kvazihipergrupa, kjer je hiperoperacija $\circ$ definirana kot prikazuje spodnja tabela. Množica z enim samim elementom je v primeru, ki je zapisan v [19], zapisana v obliki množice, zato bomo tako notacijo uporabili tudi tu. Bralec se lahko na enostaven način prepriča, da je $(H, \circ)$ hipergrupoid. Hiperoperacija $\circ$ slika iz $H \times H$ v družino vseh nepraznih podmnožic množice H. Zato mora bralec najprej poiskati vse neprazne podmnožice množice H. Iz spodnje tabele razberemo, da so rezultati hiperoperacije $\circ$ nekateri elementi iz $\mathcal{P}^*(H)$.

$\circ$	1	2	3
1	$\{1,3\}$	$\{3\}$	$\{2\}$
2	$\{2\}$	$\{1,2,3\}$	$\{2\}$
3	$\{2\}$	$\{1\}$	$\{1,2,3\}$

Za dokaz, da je hipergrupoid $(H, \circ)$ kvazihipergrupa, moramo preveriti, ali velja aksiom reprodukcije. Kar pomeni, da za poljuben element a iz množice H velja, da je $a \circ H = H \circ a = H$. Spomnimo, da je

$$a \circ H = \bigcup_{h \in H} a \circ h$$

in

$$H \circ a = \bigcup_{h \in H} h \circ a.$$

Ker preverjamo za vse elemente množice H, moramo preveriti za $a = 1, a = 2$ in $a = 3$.

- Najprej preverimo za $a = 1$.
  $1 \circ H = 1 \circ \{1, 2, 3\} = 1 \circ 1 \bigcup 1 \circ 2 \bigcup 1 \circ 3 = \{1, 3\} \bigcup \{3\} \bigcup \{2\} = \{1, 2, 3\} = H$
  $H \circ 1 = \{1, 2, 3\} \circ 1 = 1 \circ 1 \bigcup 2 \circ 1 \bigcup 3 \circ 1 = \{1, 3\} \bigcup \{2\} \bigcup \{2\} = \{1, 2, 3\} = H$
  Vidimo, da je $a \circ H = H \circ a = H$.

- Preverimo $a = 2$.
  $2 \circ H = 2 \circ \{1, 2, 3\} = 2 \circ 1 \bigcup 2 \circ 2 \bigcup 2 \circ 3 = \{2\} \bigcup \{1, 2, 3\} \bigcup \{2\} = \{1, 2, 3\} = H$
  $H \circ 2 = \{1, 2, 3\} \circ 2 = 1 \circ 2 \bigcup 2 \circ 2 \bigcup 3 \circ 2 = \{3\} \bigcup \{1, 2, 3\} \bigcup \{1\} = \{1, 2, 3\} = H$
  Spet velja, da je $a \circ H = H \circ a = H$.

- Nazadnje preverimo tudi za $a = 3$.
  $3 \circ H = 3 \circ \{1,2,3\} = 3 \circ 1 \bigcup 3 \circ 2 \bigcup 3 \circ 3 = \{2\} \bigcup \{1\} \bigcup \{1,2,3\} = \{1,2,3\} = H$
  $H \circ 3 = \{1,2,3\} \circ 3 = 1 \circ 3 \bigcup 2 \circ 3 \bigcup 3 \circ 3 = \{2\} \bigcup \{2\} \bigcup \{1,2,3\} = \{1,2,3\} = H$
  Tudi tokrat velja, da je $a \circ H = H \circ a = H$.

Ker velja aksiom reprodukcije za vse elemente iz množice H, je hipergrupoid $(H, \circ)$ kvazihipergrupa.

Definicija 3.15. Hipergrupoid $(H, \circ)$, ki je hkrati polhipergrupa in kvazihipergrupa, je **hipergrupa**.

Opomba 3.16. Hipergrupoid $(H, \circ)$ za dano hiperoperacijo $\circ$ je torej hipergrupa, če velja asociativnostni zakon in aksiom reprodukcije.

Definicija 3.17. Neprazna podmnožica K hipergrupe $(H, \circ)$ je **podhipergrupa** hipergrupe H, če je sama zase hipergrupa.

Opomba 3.18. **Komutativna hipergrupa** je hipergrupa s komutativno hiperoperacijo.

Opomba 3.19. Če je v hipergrupi H hiperprodukt (hiperoperacija) poljubnih dveh elementov natanko en element, je hipergrupa H v resnici grupa. Natančneje to pomeni naslednje: Naj bo $(H, \circ)$ hipergrupa, v kateri za vse $x, y \in H$ velja, da je $|x \circ y| = 1$. Če to velja, je $(H, \circ)$ polgrupa. V tej polgrupi velja, da za vse $a, b \in H$ obstajata taka elementa $x, y \in H$, da je $a = b \circ x$ in $a = y \circ b$. Od tu sklepamo, da je $(H, \circ)$ grupa.

Opomba 3.20. Neprazno podmnožico A grupe $(M, \circ)$ imenujemo **podgrupa**, če je sama zase grupa. To z drugimi besedami pomeni tudi, da je neprazna podmnožica A grupe $(M, \circ)$ **podgrupa** če vsebuje enoto, je produkt dveh elementov iz A spet v A in je inverz elementa iz A tudi v A. Množico M imenujemo **supergrupa** podgrupe A.

Poglejmo, kako sta definirani desno in levo deljenje v hipergrupi s hiperproduktom.

Definicija 3.21. Za **desno deljenje** se uporablja zapis a/b ali $a : b$. Podobno se za **levo deljenje** uporablja zapis $b \backslash a$ ali $a..b$.

$$a/b = \{x \in H \mid a \in xb\},$$

$$b \backslash a = \{x \in H \mid a \in bx\}.$$

Opomba 3.22. V naslednji trditvi bomo znak za operacijo izpustili.

Trditev 3.23. *Če je K taka podmnožica hipergrupe H, da je $a/b \subseteq K$ in $b \backslash a \subseteq K$, za vse $a, b \in K$, potem je K podhipergrupa hipergrupe H.*

Dokaz. Podmnožico K hipergrupe H imenujemo podhipergrupa, če za dano podmnožico velja aksiom reprodukcije. Naj bo $a \in K$. Pokazati moramo, da velja enakost $aK = Ka = K$. Predpostavimo, da je $x \in K$. Potem je $a\backslash x \subseteq K$ in zato je tudi $x \in aK$ in $K \subseteq aK$. Na enak način predpostavimo, da je $y \in aK$. Potem velja, da je $K/y \subseteq K/aK, K \cap (K/aK)y \neq \emptyset$. Potem y pripada $(K/aK)\backslash K$. Iz $(a/b)/c = a/(cb), a, b, c \in H$, sklepamo, da velja $K/aK = (K/K)/a$. Tako velja tudi $(K/aK)\backslash K = ((K/K)/a)\backslash K \subseteq (K/a)\backslash K \subseteq (K/K)\backslash K \subseteq K\backslash K \subseteq K$. Zato je $y \in K$ in $aK \subseteq K$. Potemtakem drži enakost $aK = K$. Na podoben način bi dokazali tudi enakost $Ka = K$. □

V nadaljevanju bomo predstavili nekaj primerov hipergrup. Za vsak primer bomo tudi dokazali asociativnostni zakon in aksiom reprodukcije, kar bo dovolj za dokaz, da je dani primer res hipergrupa.

Primer 3.24. Če je H neprazna množica in za $x, y \in H$ definiramo $x \cdot y = H$, je $(H, \cdot)$ hipergrupa, ki jo imenujemo **totalna hipergrupa**. Utemeljimo dano trditev. Rezultat hiperoperacije $\cdot$ za poljubna dva elementa iz H je vedno množica H. Torej če z a in b označimo dana elementa množice H, potem je $a \cdot b = H$. Preveriti moramo asociativnost hiperoperacije $\cdot$. Produkt neprazne množice in poljubnega elementa iz te množice je glede na opombo 3.13 unija množic. Predpostavimo, da so $x, y, z \in H$.

$$(x \cdot y) \cdot z = H \cdot z = \bigcup_{h \in H} h \cdot z = H,$$

$$x \cdot (y \cdot z) = x \cdot H = \bigcup_{h \in H} x \cdot h = H.$$

Opazimo, da vrstni red izvajanja hiperoperacije $\cdot$ ne vpliva na končni rezultat, saj je v obeh primerih enak. Ker je $(x \cdot y) \cdot z = x \cdot (y \cdot z)$, je hiperoperacija $\cdot$ asociativna.
Preveriti moramo, ali velja tudi aksiom reprodukcije. Predpostavimo, da je $a \in H$. Ker gre v tem primeru glede na dano hiperoperacijo za dokaz podobnih stvari, je razlaga podobna kot pri dokazu asociativnosti.

$$a \cdot H = \bigcup_{a \in H} a \cdot h = H,$$

$$H \cdot a = \bigcup_{a \in H} h \cdot a = H.$$

Ne glede na to, ali element množice pomnožimo z množico, ali množico pomnožimo z njenim elementom, dobimo enako rešitev, to je cela množica. Zato je $a \cdot H = H \cdot a = H$. Dokazali smo, da je neprazna množica H za hiperoperacijo $\cdot$ tako polhipergrupa kot kvazihipergrupa, torej je tudi hipergrupa.

Primer 3.25. Naj bo $(S,\cdot)$ polgrupa in P neprazna podmnožica množice S. Za vse $x,y\in S$ definiramo hiperoperacijo $\star$ kot $x\star y = x\cdot P\cdot y$. Potem je $(S,\star)$ polhipergrupa. Če je $(S,\cdot)$ celo grupa, pa je $(S,\star)$ hipergrupa, ki jo imenujemo P-hipergrupa.

Najprej dokažimo, da je $(S,\star)$ polhipergrupa. V ta namen moramo preveriti, ali za hiperoperacijo $\star$ velja asociativnosti zakon, to je $(x\star y)\star z = x\star(y\star z)$. Zaradi enostavnosti zapišimo, da P vsebuje le dva elementa p_1 in p_2. Preverimo, kaj je rezultat levega dela asociativnostnega zakona:

$$(x\star y)\star z = (x\cdot P\cdot y)\star z = \bigcup_{m\in x\cdot P\cdot y} m\star z = (x\cdot p_1\cdot y)\star z \bigcup (x\cdot p_2\cdot y)\star z =$$

$$x\cdot p_1\cdot y\cdot P\cdot z \bigcup x\cdot p_2\cdot y\cdot P\cdot z = x\cdot P\cdot y\cdot P\cdot z.$$

Za polhipergrupo moramo preveriti tudi desno stran asociativnostnega zakona:

$$x\star(y\star z) = x\star(y\cdot P\cdot z) = \bigcup_{n\in y\cdot P\cdot z} x\star n = x\star(y\cdot p_1\cdot z)\bigcup x\star(y\cdot p_2\cdot z) =$$

$$x\cdot P\cdot y\cdot p_1\cdot z\bigcup x\cdot P\cdot y\cdot p_2\cdot z = x\cdot P\cdot y\cdot P\cdot z.$$

Dokazali smo, da je v primeru, ko je $|P| = 2$, S za hiperoperacijo $\star$ res polhipergrupa. Na enak način se prepričamo, da je $(S,\star)$ polhipergrupa tudi za poljubno množico P. Za hipergrupo poleg zakona asociativnosti velja tudi aksiom reprodukcije. Zato predpostavimo, da je $(S,\cdot)$ grupa in preverimo, ali je $x\star S = S\star x = S$. Imamo:

$$x\star S = \bigcup_{s\in S} x\star s = \bigcup_{s\in S} x\cdot P\cdot s = x\cdot P\cdot S.$$

Ker je $(S,\cdot)$ polgrupa, velja $x\cdot P\cdot S\subseteq S$. Naj bo $p\in P$, potem je $x\cdot p\cdot S\subseteq x\cdot P\cdot S$. Predpostavimo, da sta $s_i, s_j\in S$ poljubna različna elementa iz S, za katera velja:

$$x\cdot p\cdot s_i = x\cdot p\cdot s_j.$$

Ker je $(S,\cdot)$ grupa, velja pravilo krajšanja z iste strani in zato je

$$s_i = s_j.$$

Od tod sledi, da je

$$x\star S = S.$$

Preverimo še desno stran aksioma reprodukcije:

$$S\star x = \bigcup_{s\in S} s\star x = \bigcup_{s\in S} s\cdot P\cdot x = S\cdot P\cdot x.$$

Tudi tukaj velja, da je $S \cdot P \cdot x = S$. O tem se prepričamo takole: naj bo $p \in P$, potem ima $S \cdot p \cdot x$ toliko elementov kot S, saj je $(S, \cdot)$ grupa in v njej velja pravilo krajšanja z iste strani:

$$S \cdot p \cdot x \subseteq S \cdot P \cdot x \subseteq S$$

in

$$\mid S \cdot p \cdot x \mid = S.$$

Torej res velja enakost

$$S \star x = S.$$

S tem smo dokazali tudi aksiom reprodukcije. Že prej smo dokazali, da je $(S, \star)$ polhipergrupa, zato je $(S, \star)$ tudi hipergrupa.

Trditev 3.26. *Če je G grupa in če za $x, y \in G$ z $\langle x, y\rangle$ označimo podgrupo grupe G, ki je generirana z elementoma x in y, potem G skupaj s hiperoperacijo $x \star y = \langle x, y\rangle$ tvori hipergrupo.*

Dokaz. Asociativnost hiperoperacije $\star$ preverimo tako, da najprej upoštevamo produkt elementov x in y ter nato produkt le-tega še z elementom y.

$$(x \star y) \star z = \langle x, y\rangle \star z = \bigcup_{w \in \langle x,y\rangle} \langle w, z\rangle = \langle\langle x, y\rangle, z\rangle = \langle x, y, z\rangle.$$

Sedaj bomo najprej izvedli hiperoperacijo $y \star z$:

$$x \star (y \star z) = x \star \langle y, z\rangle = \bigcup_{w \in \langle y,z\rangle} \langle x, w\rangle = \langle x, \langle y, z\rangle\rangle = \langle x, y, z\rangle.$$

V obeh primerih dobimo podgrupo grupe G, ki je generirana z istimi elementi, to so x, y, z. Zato je operacija $\star$ asociativna in je $(G, \star)$ polhipergrupa. Preverimo še veljavnost reproduktivnega aksioma. Naj bo $x \in G$. Potem je:

$$x \star G = \bigcup_{g \in G} x \star g = \bigcup_{g \in G} \langle x, g\rangle = \langle x, G\rangle = \langle G\rangle = G,$$
$$G \star x = \bigcup_{g \in G} g \star x = \bigcup_{g \in G} \langle g, x\rangle = \langle G, x\rangle = \langle G\rangle = G.$$

Vrstni red generatorjev ni pomemben, zato je leva stran reproduktivnega aksioma enaka desni strani reproduktivnega aksioma. Dokazali smo, da je grupa G skupaj s hiperoperacijo $x \star y = \langle x, y\rangle$ kvazihipergrupa. Ker pa je grupa G s hiperoperacijo $\star$ polhipergrupa in kvazihipergrupa velja, da da je tudi hipergrupa. □

Trditev 3.27. *Naj bo $(G, \cdot)$ grupa in H podgrupa edinka grupe G. Za vse elemente $x, y \in G$ definiramo hiperoperacijo $\star$ na naslednji način*

$$x \star y = x \cdot y \cdot H.$$

Potem je $(G, \star)$ hipergrupa.

Dokaz. Kot že pri prejšnjih primerih moramo za dokaz hipergrupe preveriti asociativnost in reproduktivnost. Najprej preverimo, ali za hiperoperacijo $\star$ velja asociativnostni zakon:

$$(x \star y) \star z = x \cdot y \cdot H \star z = \bigcup_{h \in H} x \cdot y \cdot h \star z = \bigcup_{h \in H} x \cdot y \cdot h \cdot z \cdot H =$$

$$x \cdot y \cdot H \cdot z \cdot H = x \cdot y \cdot z \cdot H \cdot H = x \cdot y \cdot z \cdot H.$$

Za podgrupo edinko velja, da se vsak levi odsek ujema z ustreznim desnim odsekom. V matematičnem zapisu to zapišemo kot $a \cdot H = H \cdot a$, za vsak $a \in G$. Ker je H podgrupa edinka grupe G, smo to lahko upoštevali tudi v zgornjem primeru. Če je H podgrupa edinka grupe G, je tudi podgrupa grupe G. V podgrupi pa velja $H \cdot H = H$ in tudi to smo upoštevali pri zgornjem izračunu. Na kratko še utemeljimo zadnjo enakost. Naj bosta H in K podgrupi grupe G. Produkt podgrup grupe G je definiran na naslednji način: $HK = \{hk \mid h \in H, k \in K\}$. Od tod sledi, da je HH definiran kot $HH = \{h_1 h_2 \mid h_1, h_2 \in H\}$. Ker je H zaprta podgrupa grupe G, velja $HH \subseteq H$. Naj bo $h \in H$, potem je tudi $h \in HH$. Ker že vemo, da je $HH \subseteq H$, velja tudi, da je $H \subseteq HH$. Zato drži enakost $HH = H$. Zadnji pogoj bomo uporabili tudi pri izračunu desnega dela asociativnostnega zakona:

$$x \star (y \star z) = x \star y \cdot z \cdot H = \bigcup_{h \in H} x \star y \cdot z \cdot h = \bigcup_{h \in H} x \cdot y \cdot z \cdot h \cdot H =$$

$$x \cdot y \cdot z \cdot H \cdot H = x \cdot y \cdot z \cdot H.$$

Za hiperoperacijo torej velja $(x \star y) \star z = x \star (y \star z)$. Zato je hiperoperacija $\star$ asociativna in $(G, \star)$ je polhipergrupa. Tudi tu smo seveda večkrat upoštevali asociativnost v grupi G. Preverimo, ali velja aksiom reprodukcije. Naj bo $a \in G$ poljuben. Potem je

$$a \star G = \bigcup_{g \in G} a \star g = \bigcup_{g \in G} a \cdot g \cdot H = a \cdot G \cdot H = a \cdot G = G.$$

Ker velja, da je $H \leq G$, je namreč $G = G \cdot 1 \subseteq G \cdot H = G$. Utemeljiti moramo še, zakaj je $a \cdot G = G$. Naj bo $m \in G$ poljuben. Zanima nas, ali lahko m zapišemo kot $a \cdot g$, za nek $g \in G$. Element g zapišemo kot $g = a^{-1} \cdot m$. V grupi velja pravilo krajšanja z iste strani, zato lahko zapišemo tudi $a \cdot g = a \cdot a^{-1} \cdot m = m$. Zato lahko pri dokazu aksioma reprodukcije upoštevamo enakost $a \cdot G = G$. Te zakonitosti bomo uporabili tudi pri dokazu druge polovice aksioma reprodukcije. Že prej smo omenili, da v podgrupi edinki velja, da je $a \cdot H = H \cdot a$, kar bomo upoštevali tudi v naslednjem zapisu:

$$G \star a = \bigcup_{g \in G} g \star a = \bigcup_{g \in G} g \cdot a \cdot H = G \cdot a \cdot H = G \cdot H \cdot a = G \cdot a = G.$$

Dokazali smo veljavnost aksioma reprodukcije, $a \star G = G \star a = G$ za vsak $a \in G$. Ker je $(G, \star)$ polhipergrupa in ker za hiperoperacijo $\star$ velja aksiom reprodukcije, je $(G, \star)$ tudi hipergrupa. $\square$

Opomba 3.28. Pri grupah simbol za operacijo $\cdot$ navadno izpustimo. Tako bi v običajnem zapisu množenja v grupah namesto $x \star y = x \cdot y \cdot H$ hiperoperacijo definirali kot $x \star y = xyH$. Tak zapis bomo uporabili tudi v naslednjem primeru.

Trditev 3.29. *Naj bo $(G, \cdot)$ grupa in H podgrupa grupe G, ki ni nujno edinka. Naj bo $G/H = \{xH \mid x \in G\}$ prostor levih odsekov po podgrupi H v grupi G. Potem je $(G/H, \star)$ hipergrupa, kjer je hiperoperacija $\star$ na G/H definirana takole:*

$$xH \star yH = \{zH \mid z \in xHy\}, \text{ kjer } xH, yH \in G/H.$$

Dokaz. Najprej preverimo, ali je $(G/H, \star)$ polhipergrupa. V ta namen moramo ugotoviti, ali velja enakost $(xH \star yH) \star mH = xH \star (yH \star mH)$, $x, y, m \in H$, torej, ali je hiperoperacija $\star$ asociativna za leve odseke v grupi G po podgrupi H.
Hiperoperacija $\star$ je definirana kot

$$xH \star yH = \{zH \mid z \in xHy\} = \bigcup_{z \in xHy} \{zH\} = xHyH.$$

Preverimo, kaj je rezultat leve strani asociativnostega zakona za dano hiperoperacijo:

$$(xH \star yH) \star mH = \bigcup_{z \in xHy} \{zH\} \star mH = \bigcup_{z \in xHy} zH \star mH = \bigcup_{z \in xHy} zHmH = xHyHmH.$$

Preverimo še drugi del zakona:

$$xH \star (yH \star mH) = xH \star \bigcup_{n \in yHm} \{nH\} = \bigcup_{n \in yHm} xH \star nH = \bigcup_{n \in yHm} xHnH = xHyHmH.$$

Ker smo dobili enak rezultat, je hiperoperacija $\star$ asociativna. Tako smo dokazali, da je $(G/H, \star)$ polhipergrupa. Če dokažemo, da za hiperoperacijo $\star$ velja tudi aksiom reprodukcije, potem je $(G/H, \star)$ kvazihipergrupa. Dokazati moramo, da velja enakost $aH \star G/H = G/H \star aH = G/H$ za vsak $aH \in G/H$:

$$aH \star G/H = G/H \star aH = G/H.$$

Spomnimo, da če je G grupa in je H njena podgrupa ter sta x in y poljubna elementa iz grupe G potem velja:

- $xH = H$, če in samo če je $x \in H$,
- $xH = yH$, če in samo če je $x^{-1}y \in H$.

Torej je:

$$aH \star G/H = \{aH \star xH \mid x \in G\} = \{aHxH \mid x \in G\} = \{zH \mid z \in G\} = G/H,$$

$$G/H \star aH = \{xH \star aH \mid x \in G\} = \{\{zH \mid z \in xHa\} \mid x \in G\} =$$
$$= \{xHaH \mid x \in G\} = G/H.$$

Ker je H podgrupa grupe G, je H tudi podmnožica množice G. Zato ob upoštevanju prve točke zgoraj dobimo zapis $\{aHH \mid a \in H\}$. Ker je H podgrupa grupe H, velja enakost $HH = H$. Tako se zadnji zapis poenostavi v $\{aH \mid a \in H\}$, ob upoštevanju druge točke zgoraj pa v zapis $\{zH \mid z \in G\}$. Od tod sklepamo, da če x teče po vseh elementih iz grupe G, lahko dobimo poljubni odsek iz G/H. Zato za dani primer drži tudi aksiom reprodukcije, torej je $(G/H, \star)$ kvazihipergrupa. Tako smo dokazali, da je $(G/H, \star)$ tudi hipergrupa. V kolikor je H edinka, je definirana hiperoperacija $\star$ ekvivalentna operaciji v kvocientni grupi $(G/H, \cdot)$. □

3.2.1 Nekaj vrst podhipergrup

V [5] je navedenih več primerov podhipergrup. V nadaljevanju bomo teorijo in primere povzeli prav po tej literaturi. Med matematiki, ki so preučevali hipergrupe, so Marty, Dresher, Ore in Krasner, preučevali **zaprte** in **obrnljive** podhipergrupe. Sureau pa je proučeval **ultrazaprte**, **obrnljive** in **konjugirane** podhipergrupe.

Definicija 3.30. Naj bo $(H, \circ)$ hipergrupa in $(K, \circ)$ njena podhipergrupa. Za podhipergrupo $(K, \circ)$ rečemo, da je:

- **levo zaprta** (ali **desno zaprta**), če za vse $k_1, k_2 \in K$ in $x \in H$ velja: če je $k_1 \in x \circ k_2$ ($k_1 \in k_2 \circ x$), potem je $x \in K$;

- **levo obrnljiva** (ali **desno obrnljiva**), če za vse $x, y \in H$ velja: če je $x \in K \circ y$ ($x \in y \circ K$), potem je $y \in K \circ x$ ($y \in x \circ K$);

- **levo ultrazaprta** (**desno ultrazaprta**), če za vsak $x \in H$ velja:

$$K \circ x \cap (H \setminus K) \circ x = \emptyset \quad (x \circ K \cap x \circ (H \setminus K) = \emptyset);$$

- **desno konjugirana**, če je desno zaprta in za vse $x \in H$ obstaja tak $x' \in H$, da je $x' \circ x \subseteq K$. Na enak način lahko definiramo tudi **levo konjugirano** podhipergrupo.

Rečemo, da je podhipergrupa K zaprta (obrnljiva, ultrazaprta, konjugirana), če je **levo** in **desno** zaprta (obrnljiva, ultrazaprta, konjugirana).

V [16] je zapisan naslednji primer za zaprto podhipergrupo.

Primer 3.31. Množica $H = \{a, b, c\}$ je s hiperoperacijo $\star$, ki je zapisana v spodnji tabeli, hipergrupa. Podmnožica $K = \{b, c\}$ množice H s hiperoperacijo $\star$ je podhipergrupa hipergrupe H. Podhipergrupa $(K, \star)$ je zaprta podhipergrupa.

$\star$	a	b	c
a	$\{a\}$	H	H
b	H	$\{b, c\}$	$\{b, c\}$
c	H	$\{b, c\}$	$\{b, c\}$

Utemeljitev, da je $(H, \star)$ hipergrupa prepuščamo bralcu. Preverimo, ali je $(K, \star)$ podhipergrupa. Preveriti je potrebno iste lastnosti, kot za hipergrupo. Pri asociativnosti preverjamo "produkt" treh elementov. Ker je $K = \{b, c\}$ moramo preveriti za osem parov produktov. Najprej pokažimo, da je $(b\star b)\star b = b\star(b\star b)$. V ta namen izračunamo:

$$(b \star b) \star b = \{b, c\} \star b = b \star b \bigcup c \star b = \{b, c\} \bigcup \{b, c\} = \{b, c\},$$

$$b \star (b \star b) = b \star \{b, c\} = b \star b \bigcup b \star c = \{b, c\} \bigcup \{b, c\} = \{b, c\}.$$

Na enak način lahko bralec preveri asociativnost še za preostlih sedem kombinacij in se prepriča, da je hiperoperacija $\star$ v množici K asociativna. Preveriti moramo še aksiom reprodukcije, to je $x \star K = K \star x = K, x \in K$. Preverili bomo za element b, bralec pa naj preveri še za element c. Pokažimo, da je $b \star \{b, c\} = \{b, c\} \star b$. Najprej preverimo "produkt" $b \star \{b, c\}$:

$$b \star b \bigcup b \star c = \{b, c\} \bigcup \{b, c\} = \{b, c\} = K,$$

in nato še "produkt" $\{b, c\} \star b$:

$$b \star b \bigcup c \star b = \{b, c\} \bigcup \{b, c\} = \{b, c\} = K.$$

Velja tudi aksiom reprodukcije, zato je $(K, \star)$ sama zase hipergrupa in posledično tudi podhipergrupa hipergrupe H. Preverimo, ali je podhipergrupa K zaprta podhipergrupa. Najprej bomo preverili, ali je levo zaprta, to je ali za vse $k_1, k_2 \in K$ in $x \in H$ velja $k_1 \in x \star k_2$. Ker množica H vsebuje elemente a, b, c, podmnožica K pa elementa b in c, moramo preveriti šest relacij vsebovanosti:

$$b \in a \star c \Longrightarrow b \in H,$$

$$b \in b \star c \Longrightarrow b \in \{b, c\},$$

$$b \in c \star c \Longrightarrow b \in \{b, c\},$$

$$c \in a \star b \Longrightarrow c \in H,$$

$$c \in b \star c \Longrightarrow c \in \{b, c\},$$

$$c \in c \star c \Longrightarrow c \in \{b, c\}.$$

Pokazali smo, da je podhipergrupa K levo zaprta. Na enak način bi lahko preverili, da je podhipergrupa K tudi desno zaprta. Ker je podhipergrupa K levo in desno zaprta, je zaprta. Za levo obrnljivost moramo preveriti šest možnosti. Prav toliko možnosti moramo preveriti za desno obrnljivost. Podhipergrupa K ni levo obrnljiva, saj

$$a \notin \{b, c\} \star b.$$

Prav tako ni desno obrnljiva, saj

$$a \notin c \star \{b, c\}.$$

Ker podhipergrupa K ni ne levo in ne desno obrnljiva, ni obrnljiva. Podhipergrupa K tudi ni ne levo in ne desno ultrazaprta. Glede na definicijo leve ultrazaprtosti za množico H in podmnožico K je:

$$\{b, c\} \star a \bigcap \{a\} \star a = b \star a \bigcup c \star a \bigcap \{a\} = H \bigcup H \bigcap \{a\} = H \bigcap \{a\} = \{a\}.$$

Ker rešitev zgornjega zapisa ni prazna množica, podhipergrupa K ni levo ultrazaprta. Za desno ultrazaprtost za elemente a, b in c ter za levo ultrazaprtost za elementa b in c naj bralec preveri sam. Podhipergrupa K ni desno konjugirana, ker denimo za $a \in H$ ne obstaja tak $a' \in H$, da je $a' \star a \subseteq K$. Ker podhipergrupa K ni desno konjugirana, tudi ni konjugirana.

3.2.2 Homomorfizmi hipergrup

Homomorfizme hipergrup so preučevali Dresher, Ore, Krasner, Corsini, Davvaz in ostali. V tem poglavju bomo preučevali različne vrste homomorfizmov pri hipergrupah [5].

Definicija 3.32. Dani imamo hipergrupi $(H_1, \circ)$ in $(H_2, \star)$. Preslikavo $f : H_1 \to H_2$ imenujemo

- **homomorfizem** ali **vključitveni homomorfizem**, če za vse $x, y \in H_1$ velja $f(x \circ y) \subseteq f(x) \star f(y)$,
- **dober homomorfizem**, če za vse $x, y \in H_1$ velja $f(x \circ y) = f(x) \star f(y)$,
- **izomorfizem**, če je bijekcija in dober homomorfizem. Če je preslikava f izomorfizem, potem sta H_1 in H_2 **izomorfni hipergrupi**, kar zapišemo $H_1 \cong H_2$.

Primer 3.33. Naj bosta $H_1 = \{a, b, c\}$ in $H_2 = \{0, 1, 2\}$ hipergrupi s hiperoperacijami:

$\circ$	a	b	c
a	a	H_1	H_1
b	H_1	b	b
c	H_1	b	c

$\star$	0	1	2
0	0	H_2	H_2
1	H_2	1	1
2	H_2	1	$\{1, 2\}$

Definiramo preslikavo $f : H_1 \to H_2$ na naslednji način: $f(a) = 0, f(b) = 1, f(c) = 2$. Dokažimo, da je f vključitveni homomorfizem. Za vključitveni homomorfizem mora veljati $f(x \circ y) \subseteq f(x) \star f(y)$. Preverimo vse možne kombinacije za $a, b, c \in H_1$:

- $f(a \circ a) = f(a) = 0$,
  $f(a) \star f(a) = 0 \star 0 = 0$,
  $\{0\} \subseteq \{0\}$,
  $f(a \circ a) \subseteq f(a) \star f(a)$.

- $f(a \circ b) = f(H_1) = f(\{a, b, c\}) = \{f(a), f(b), f(c)\} = \{0, 1, 2\}$,
  $f(a) \star f(b) = 0 \star 1 = H_2 = \{0, 1, 2\}$,
  $\{0, 1, 2\} \subseteq \{0, 1, 2\}$,
  $f(a \circ b) \subseteq f(a) \star f(b)$.

- $f(a \circ c) = f(H_1) = f(\{a, b, c\}) = \{f(a), f(b), f(c)\} = \{0, 1, 2\}$,
  $f(a) \star f(c) = 0 \star 2 = H_2 = \{0, 1, 2\}$,
  $\{0, 1, 2\} \subseteq \{0, 1, 2\}$,
  $f(a \circ c) \subseteq f(a) \star f(c)$.

- $f(b \circ a) = f(H_1) = f(\{a, b, c\}) = \{f(a), f(b), f(c)\} = \{0, 1, 2\}$,
  $f(b) \star f(a) = 1 \star 0 = H_2 = \{0, 1, 2\}$,
  $\{0, 1, 2\} \subseteq \{0, 1, 2\}$,
  $f(b \circ a) \subseteq f(b) \star f(a)$.

- $f(b \circ b) = f(b) = 1$,
  $f(b) \star f(b) = 1 \star 1 = 1$,
  $\{1\} \subseteq \{1\}$,
  $f(b \circ b) \subseteq f(b) \star f(b)$.

- $f(b \circ c) = f(b) = 1$,
  $f(b) \star f(c) = 1 \star 2 = 1$,
  $\{1\} \subseteq \{1\}$,
  $f(b \circ c) \subseteq f(b) \star f(c)$.

- $f(c \circ a) = f(H_1) = f(\{a, b, c\}) = \{f(a), f(b), f(c)\} = \{0, 1, 2\}$,
  $f(c) \star f(a) = 2 \star 0 = H_2 = \{0, 1, 2\}$,

$\{0,1,2\} \subseteq \{0,1,2\}$,
$f(c \circ a) \subseteq f(c) \star f(a)$.

- $f(c \circ b) = f(b) = 1$,
  $f(c) \star f(b) = 2 \star 1 = 1$,
  $\{1\} \subseteq \{1\}$,
  $f(c \circ b) \subseteq f(c) \star f(b)$.

- $f(c \circ c) = f(c) = 2$,
  $f(c) \star f(c) = 2 \star 2 = \{1,2\}$,
  $\{2\} \subseteq \{1,2\}$,
  $f(c \circ c) \subseteq f(c) \star f(c)$.

Dokazali smo, da je preslikava $f : H_1 \to H_2$ res vključitveni homomorfizem.

Opomba 3.34. V nadaljevanju bomo za vključitveni homomorfizem $f : H_1 \longrightarrow H_2$ hipergrup uporabili oznako $x_f = f^{-1}(f(x))$. Za podmnožico A množice H_1 pa

$$A_f = f^{-1}(f(A)) = \bigcup_{x \in A} x_f.$$

Opazimo, da je zgornji zapis za vključitveni homomorfizem ekvivalenten zapisu

$$x \circ y \subseteq f^{-1}(f(x) \star f(x)).$$

Za vključitveni homomorfizem tudi velja

$$(x \circ y)_f \subseteq f^{-1}(f(x) \star f(y)).$$

Pogoj za vključitveni homomorfizem velja tudi za množice. Naj bosta A in B neprazni podmnožici množice H_1, potem je

$$f(A \circ B) \subseteq f(A) \star f(B).$$

Denimo, da je $A = x_f$ in $B = y_f$. Potem ob upoštevanju zgoraj zapisanega dobimo zapis

$$x_f \circ y_f \subseteq f^{-1}(f(x) \star f(y))$$

in

$$(x_f \circ y_y)_f \subseteq f^{-1}(f(x) \star f(y)).$$

V literaturi zasledimo različne lastnosti homomorfizmov [5]. V nadaljevanju bomo spoznali štire tipe homomorfizmov. Vsakega od teh tipov bomo preučevali s pomočjo pogoja $f^{-1}(f(x) \star f(y))$.

Definicija 3.35. Dani imamo hipergrupi $(H_1, \circ)$ in $(H_2, \star)$ ter homomorfizem $f : H_1 \to H_2$. Potem preslikavo f imenujemo homomorfizem

- **tipa 1**, če velja $f^{-1}(f(x) \star f(y)) = (x_f \circ y_f)_f$,
- **tipa 2**, če velja $f^{-1}(f(x) \star f(y)) = (x \circ y)_f$,
- **tipa 3**, če velja $f^{-1}(f(x) \star f(y)) = x_f \circ y_f$,
- **tipa 4**, če velja $f^{-1}(f(x) \star f(y)) = (x \circ y)_f = x_f \circ y_f$, za vse $x, y \in H_1$.

Primer 3.36. Dani imamo hipergrupi $H_1 = \{0, 1, 2\}$ in $H_2 = \{a, b\}$ s hiperoperacijama:

$\circ$	0	1	2
0	0	$\{0,1\}$	$\{0,2\}$
1	$\{0,1\}$	1	$\{1,2\}$
2	$\{0,2\}$	$\{1,2\}$	2

$\star$	a	b
a	a	$\{a,b\}$
b	$\{a,b\}$	b

Naj bo preslikava $f : H_1 \to H_2$ definirana s $f(0) = f(1) = a$ in $f(2) = b$. Dokažimo, da je preslikava f dobri homomorfizem tipa 4. Najprej bomo dokazali, da je preslikava f dobri homomorfizem. Pokazati moramo, da je $f(x \circ y) = f(x) \star f(y)$ za poljubna $x, y \in H_1$. Poglejmo vse možnosti:

- $f(0 \circ 0) = f(0) = a$,
  $f(0) \star f(0) = a \star a = a$.
- $f(0 \circ 1) = f(\{0, 1\}) = \{f(0), f(1)\} = \{a, a\} = a$,
  $f(0) \star f(1) = a \star a = a$.
- $f(0 \circ 2) = f(\{0, 2\}) = \{f(0), f(2)\} = \{a, b\}$,
  $f(0) \star f(2) = a \star b = \{a, b\}$.
- $f(1 \circ 0) = f(\{0, 1\}) = \{f(0), f(1)\} = \{a, a\} = a$,
  $f(1) \star f(0) = a \star a = a$.
- $f(1 \circ 1) = f(1) = a$,
  $f(1) \star f(1) = a \star a = a$.
- $f(1 \circ 2) = f(\{1, 2\}) = \{f(1), f(2)\} = \{a, b\}$,
  $f(1) \star f(2) = a \star b = \{a, b\}$.
- $f(2 \circ 0) = f(\{0, 2\}) = \{f(0), f(2)\} = \{a, b\}$,
  $f(2) \star f(0) = b \star a = \{a, b\}$.

- $f(2 \circ 1) = f(\{1,2\}) = \{f(1), f(2)\} = \{a,b\}$,
  $f(2) \star f(1) = b \star a = \{a,b\}$.

- $f(2 \circ 2) = f(2) = b$,
  $f(2) \star f(2) = b \star b = b$.

Ker za vse možne kombinacije elementov hipergrupe veljajo zgornje enakosti, je preslikava f dobri homomorfizem. Dokažimo še, da je preslikava f homomorfizem tipa 4. Preverimo, ali velja enakost za homomorfizem tipa 4 iz definicije 3.35:

- $f^{-1}(f(0) \star f(0)) = f^{-1}(a \star a) = f^{-1}(a) = \{0,1\}$,
  $(0 \circ 0)_f = 0_f \circ 0_f = f^{-1}(f(0)) \circ f^{-1}(f(0)) = f^{-1}(a) \circ f^{-1}(a) = \{0,1\} \circ \{0,1\} = \{0,1\}$.

- $f^{-1}(f(0) \star f(1)) = f^{-1}(a \star a) = f^{-1}(a) = \{0,1\}$,
  $(0 \circ 1)_f = 0_f \circ 1_f = f^{-1}(f(0)) \circ f^{-1}(f(1)) = f^{-1}(a) \circ f^{-1}(a) = \{0,1\} \circ \{0,1\} = \{0,1\}$.

- $f^{-1}(f(0) \star f(2)) = f^{-1}(a \star b) = f^{-1}(\{a,b\}) = \{f^{-1}(a), f^{-1}(b)\} = \{0,1,2\}$,
  $(0 \circ 2)_f = 0_f \circ 2_f = f^{-1}(f(0)) \circ f^{-1}(f(2)) = f^{-1}(a) \circ f^{-1}(b) = \{0,1\} \circ \{2\} = \{0,1,2\}$.

- $f^{-1}(f(1) \star f(0)) = f^{-1}(a \star a) = f^{-1}(a) = \{0,1\}$,
  $(1 \circ 0)_f = 1_f \circ 0_f = f^{-1}(f(1)) \circ f^{-1}(f(0)) = f^{-1}(a) \circ f^{-1}(a) = \{0,1\} \circ \{0,1\} = \{0,1\}$.

- $f^{-1}(f(1) \star f(1)) = f^{-1}(a \star a) = f^{-1}(a) = \{0,1\}$,
  $(1 \circ 1)_f = 1_f \circ 1_f = f^{-1}(f(1)) \circ f^{-1}(f(1)) = f^{-1}(a) \circ f^{-1}(a) = \{0,1\} \circ \{0,1\} = \{0,1\}$.

- $f^{-1}(f(1) \star f(2)) = f^{-1}(a \star b) = f^{-1}(\{a,b\}) = \{f^{-1}(a), f^{-1}(b)\} = \{0,1,2\}$,
  $(1 \circ 2)_f = 1_f \circ 2_f = f^{-1}(f(1)) \circ f^{-1}(f(2)) = f^{-1}(a) \circ f^{-1}(b) = \{0,1\} \circ \{2\} = \{0,1,2\}$.

- $f^{-1}(f(2) \star f(0)) = f^{-1}(b \star a) = f^{-1}(\{a,b\}) = \{f^{-1}(a), f^{-1}(b)\} = \{0,1,2\}$,
  $(2 \circ 0)_f = 2_f \circ 0_f = f^{-1}(f(2)) \circ f^{-1}(f(0)) = f^{-1}(b) \circ f^{-1}(a) = \{2\} \circ \{0,1\} = \{0,1,2\}$.

- $f^{-1}(f(2) \star f(1)) = f^{-1}(b \star a) = f^{-1}(\{a,b\}) = \{f^{-1}(a), f^{-1}(b)\} = \{0,1,2\}$,
  $(2 \circ 1)_f = 2_f \circ 1_f = f^{-1}(f(2)) \circ f^{-1}(f(1)) = f^{-1}(b) \circ f^{-1}(a) = \{2\} \circ \{0,1\} = \{0,1,2\}$.

- $f^{-1}(f(2) \star f(2)) = f^{-1}(b \star b) = f^{-1}(b) = \{2\}$,
  $(2 \circ 2)_f = 2_f \circ 2_f = f^{-1}(f(2)) \circ f^{-1}(f(2)) = f^{-1}(b) \circ f^{-1}(b) = \{2\} \circ \{2\} = \{2\}$.

Preslikava f je res homomorfizem tipa 4, saj za vse kombinacije velja enakost iz definicije 3.35.

Trditev 3.37. *Naj bosta $(H_1, \circ)$ in $(H_2, \star)$ hipergrupi, A in B neprazni podmnožici hipergrupe $(H_1, \circ)$ ter $f : H_1 \longrightarrow H_2$ preslikava iz hipergrupe H_1 v hipergrupo H_2. Potem je preslikava f homomorfizem*

- *tipa 1, če velja enakost $f^{-1}(f(A) \star f(B)) = (A_f \circ B_f)_f$;*
- *tipa 2, če velja enakost $f^{-1}(f(A) \star f(B)) = (A \circ B)_f$;*
- *tipa 3, če velja enakost $f^{-1}(f(A) \star f(B)) = A_f \circ B_f$;*
- *tipa 4, če velja enakost $f^{-1}(f(A) \star f(B)) = (A \circ B)_f = A_f \circ B_f$.*

Dokaz. Enakosti za posamezni tip homomorfizma sledijo iz definicije 3.35. □

Posledica 3.38. *Dani sta hipergrupi $(H_1, \circ)$ in $(H_2, \star)$ ter preslikava $f : H_1 \longrightarrow H_2$. Potem je preslikava f homomorfizem*

- *tipa 4, če in samo če je f homomorfizem tipa 2 in tipa 3;*
- *tipa 1, če je f homomorfizem tipa 2 ali tipa 3.*

Dokaz. Dokaz za prvo točko je preprost. Naj bosta h_1 in h_2 elementa iz hipergrupe H_1. Denimo, da je f homomorfizem tipa 4. Dokažimo, da je f tudi homomorfizem tipa 2:

$$(h_1 \circ h_2)_f = (h_{1f} \circ h_{2f}) \subseteq f^{-1}(f(h_1) \star f(h_2)) = (h_{1f} \circ h_{2f}) = (h_1 \circ h_2)_f.$$

Dokažimo, da če je f homomorfizem tipa 4, je tudi homomorfizem tipa 3:

$$(h_{1f} \circ h_{2f}) = (h_1 \circ h_2)_f \subseteq f^{-1}(f(h_1) \star f(h_2)) = (h_1 \circ h_2)_f = (h_{1f} \circ h_{2f}).$$

Preverimo, ali velja tudi nasprotna smer. Torej, če je f homomorfizem tipa 2 in tipa 3, je tudi homomorfizem tipa 4. Naj bo f homomorfizem tipa 2 in tipa 3. Dokažimo, da je f tudi homomorfizem tipa 4:

$$(h_1 \circ h_2)_f \subseteq f^{-1}(f(h_1) \star f(h_2)) = (h_{1f} \circ h_{2f}) = (h_1 \circ h_2)_f.$$

$$(h_{1f} \circ h_{2f}) \subseteq f^{-1}(f(h_1) \star f(h_2)) = (h_1 \circ h_2)_f = (h_{1f} \circ h_{2f}).$$

Tako smo dokazali točko (1). Dokažimo še točko (2). Denimo, da je f homomorfizem tipa 2. Glede na definicijo homomorfizma tipa 2 je

$$(h_1 \circ h_2)_f \subseteq (h_{1f} \circ h_{2f})_f \subseteq f^{-1}(f(h_1) \star f(h_2) = (h_1 \circ h_2)_f.$$

Naj bo f homomorfizem tipa 3. Prepričajmo se, da je f tudi homomorfizem tipa 1:

$$(h_{1f} \circ h_{2f}) \subseteq (h_{1f} \circ h_{2f})_f \subseteq f^{-1}(f(h_1) \star f(h_2)) = (h_{1f} \circ h_{2f}).$$

□

Opomba 3.39. Z ρ bomo označili ekvivalenčno relacijo na hipergrupi $(H, \star)$. Za ekvivalenčni razred, ki vsebuje $x \in H$, bomo uporabili oznako x_ρ. Če je A neprazna podmnožica hipergrupe H, potem je $A_\rho = \bigcup \{x_\rho \mid x \in A\}$. Z zapisom H/ρ, kar preberemo H po modulu ρ, označujemo družino razredov $\{x_\rho \mid x \in H\}$ ekvivalenčne relacije ρ. Tako bomo hiperoperacijo $\otimes$ na H/ρ definirali kot

$$x_\rho \otimes y_\rho = \{z_\rho \mid z \in x_\rho \star y_\rho\}; x, y \in H.$$

Trditev 3.40. *Dano imamo hipergrupo $(H, \star)$. Potem je $(H/\rho, \otimes)$ tudi hipergrupa, če in samo če za vse $x, y, z \in H$ velja*

$$((x_\rho \star y_\rho)_\rho \star z_\rho)_\rho = (x_\rho \star (y_\rho \star z_\rho)_\rho)_\rho.$$

Dokaz. Če želimo dokazati, da je $(H/\rho, \otimes)$ hipergrupa, moramo dokazati, da za dano hiperoperacijo velja asociativnostni zakon $(x_\rho \otimes y_\rho) \otimes z_\rho = x_\rho \otimes (y_\rho \otimes z_\rho)$ in aksiom reprodukcije $a_\rho \otimes H/\rho = H/\rho \otimes a_\rho = H/\rho$ za poljubne $a_\rho \in H/\rho, x, y, z \in H$.
Najprej bomo preverili asociativnostni zakon:

$$(x_\rho \otimes y_\rho) \otimes z_\rho = \bigcup_{u \in x_\rho \circ y_\rho} u_\rho \otimes z_\rho = \bigcup_{u \in x_\rho \circ y_\rho} (u_\rho \circ z_\rho)_\rho = ((x_\rho \circ y_\rho)_\rho \circ z_\rho)_\rho,$$

$$x_\rho \otimes (y_\rho \otimes z_\rho) = \bigcup_{t \in y_\rho \circ z_\rho} x_\rho \otimes t_\rho = \bigcup_{t \in y_\rho \circ z_\rho} (x_\rho \circ t_\rho)_\rho = (x_\rho \circ (y_\rho \circ z_\rho))_\rho.$$

Glede na zapisano je $(x_\rho \otimes y_\rho) \otimes z_\rho = x_\rho \otimes (y_\rho \otimes z_\rho)$, torej asociativnostni zakon res velja.
Aksiom reprodukcije v $(H/\rho, \otimes)$ je posledica aksioma reprodukcije v hipergrupi H. Predpostavimo, da sta x_ρ in y_ρ iz H/ρ. Naj bosta u in $v \in H$ taka, da je $y \in x \circ u$ in $y \in v \circ x$. Potem je tudi $y_\rho \in x_\rho \otimes u_\rho$ in $y_\rho \in v_\rho \otimes x_\rho$. Aksiom reprodukcie drži, zato je $(H/\rho, \otimes)$ hipergrupa. □

Več o homomorfizmih hipergrup lahko bralec prebere v [5].

3.2.3 Regularne in močno regularne relacije

Z uporabo ekvivalenčnih relacij, ki jih imenujemo **močno regularne relacije**, bomo lahko povezali polhipergrupe s polgrupami in hipergrupe z grupami. Denimo, da imamo dano (pol)hipergrupo in močno regularno relacijo. Potem lahko na družini razredov ekvivalenčne relacije ρ na H zgradimo strukturo (pol)grupe. Da bomo lahko povezali (pol)hipergrupe s (pol)grupami, moramo definirati naslednje zapise. Naj bo $(H, \star)$ polhipergrupa in ρ ekvivalenčna relacija na njej. Če sta A in B neprazni podmnožici polhipergrupe H, potem zapis

- $A\overline{\rho}B$ pomeni, da za vsak $a \in A$ obstaja tak $b \in B$, da je $a\rho b$ in za vsak $b' \in B$ obstaja tak $a' \in A$, da je $a'\rho b'$,
- $A\overline{\overline{\rho}}B$ pomeni, da za vsak $a \in A$ in za vsak $b \in B$ velja $a\rho b$.

Definicija 3.41. Naj bo $(H, \star)$ polhipergrupa. Ekvivalenčno relacjo ρ definirano na polhipergrupi $(H, \star)$ imenujemo

- **desno regularna** (**levo regularna**), če za vsak $h \in H$ iz $a\rho b, a, b \in H$, sledi, da je $(a \star h)\overline{\rho}(b \star h)$ (oziroma $(h \star a)\overline{\rho}(h \star b)$),
- **močno desno regularna** (**močno levo regularna**), če za vsak $h \in H$ iz $a\rho b, a, b \in H$, sledi, da je $(a \star h)\overline{\overline{\rho}}(b \star h)$ (oziroma $(h \star a)\overline{\overline{\rho}}(h \star b)$),
- **močno regularna**, če je levo in desno močno regularna.

Opomba 3.42. Relacija ρ je regularna, če je desno in levo regularna.

Opomba 3.43. S $\bar{h}$ označimo ekvivalenčni razred ekvivalenčne relacija ρ.

Opomba 3.44. Hiperoperacija $\otimes$ je dobro definirana, če velja:

- $\overline{x} \otimes \overline{y} = \overline{x_1} \otimes \overline{y_1};\ \ \overline{x} = \overline{x_1},\ \ \overline{y} = \overline{y_1}$,
- $(\overline{x} \otimes \overline{y}) \otimes \overline{z} = \overline{x} \otimes (\overline{y} \otimes \overline{z})$.

Izrek 3.45. *Dano imamo polhipergrupo $(H, \star)$ in ekvivalenčno relacijo ρ.*

- *Če je ρ regularna relacija, je H/ρ polhipergrupa s hiperoperacijo*

  $$\overline{h} \otimes \overline{y} = \{\overline{z} \mid z \in h \star y\}.$$

  (Spomnimo, da je hiperoperacija $\otimes$ definirana na strani 48.*)*

- *Če je hiperoperacija $\otimes$ dobro definirana na H/ρ, potem je ekvivalenčna relacija ρ regularna.*

Dokaz izreka 3.45 je zapisan v [5].

Posledica 3.46. *Če je $(H, \star)$ hipergrupa in je ρ ekvivalenčna relacija, potem je ta ekvivalenčna relacija regularna, če in samo če je $(H/\rho, \otimes)$ hipergrupa.*

Trditev 3.47. *Naj bo $(H, \star)$ polhipergrupa in ρ ekvivalenčna relacija.*

- *Če je relacija ρ močno regularna, potem je H/ρ polgrupa z operacijo $\overline{x} \otimes \overline{y} = \overline{z}; z \in x \star y$.*
- *Če je operacija $\otimes$ na H/ρ dobro definirana, potem je ρ močno regularna relacija.*

Dokaz. Naj bosta $x, y \in H$. Potem glede na definicijo 3.41 velja $(x \star y)\overline{\overline{\rho}}(y \star x)$. Če upoštevamo izrek 3.45 dobimo naslednji zapis: $\overline{x} \otimes \overline{y} = \{\overline{z} \mid z \in x \star y\} = \{\overline{z}\}$. Rezultat operacije $\otimes$ je natanko en element iz H/ρ, zato je $(H/\rho, \otimes)$ polgrupa. Tako smo dokazali prvo točko. Naj bo $a\rho b$ in naj bo x poljubni element iz H. Za močno regularnost moramo dokazati močno levo regularnost $(x \star a)\overline{\overline{\rho}}(x \star b)$ in močno desno regularnost $(a \star x)\overline{\overline{\rho}}(b \star y)$. Najprej bomo dokazali močno levo regularnost. Naj bo $m \in x \star a$ in $n \in x \star b$. Potem velja $\overline{m} = \overline{x} \otimes \overline{a}$, $\overline{n} = \overline{x} \otimes \overline{b}$, kar pomeni, da je $\overline{m} = \overline{n}$, zato je tudi $m\rho n$. Dokažimo še močno desno regularnost. Naj bo $m_1 \in a \star x$ in $n_1 \in b \star x$. Potem velja $\overline{m_1} = \overline{a} \otimes \overline{x}, \overline{n_1} = \overline{b} \otimes \overline{x}$ in $\overline{m_1} = \overline{n_1}$, kar pomeni, da je $m_1 \rho n_1$. Ker je ρ tudi močno desno regularna, je tudi močno regularna. □

Posledica 3.48. *Ekvivalenčna relacija ρ na hipergrupi $(H, \star)$ je močno regularna, če in samo če je kvocientna množica H/ρ z operacijo $\otimes$ grupa.*

Opomba 3.49. Preslikavo iz polhipergrupe v polgrupo imenujemo homomorfizem, če je usklajena z operacijo polhipergrupe oziroma polgrupe. Naj bo $f : (H, \star) \longrightarrow (H_1, \bullet)$, kjer je H polhipergrupa in H_1 polgrupa in naj bo ρ^f relacija, ki je definirana kot $a\rho^f b \Leftrightarrow f(a) = f(b)$. Bralec se lahko sam prepriča, da je relacija ρ^f ekvivalenčna.

Izrek 3.50. *Dani sta polhipergrupa $(H, \star)$ in polgrupa $(H_1, \bullet)$ ter homomorfizem $f : H \to H_1$. Potem je ekvivalenčna relacija ρ^f močno regularna.*

Dokaz. Ker je ekvivalenčna relacija označena z ρ^f, bomo uporabili zapis $a\rho^f b$. Definirana je kot $a\rho^f b = f(a) = f(b)$. Naj bo $x \in H$ poljuben, $u \in a \star x$ in $v \in b \star x$. Za dokaz močne regularnosti moramo dokazati, da je ρ^f močno levo in močno desno regularna. Pri dokazu bomo upoštevali definicijo homomorfizma hipergrup in definicijo ekvivalenčne relacije ρ^f. Najprej dokažimo močno desno regularnost:

$$f(u) = f(a \star x) = f(a) \bullet f(x),$$

$$f(v) = f(b \star x) = f(b) \bullet f(x).$$

Ker je $f(a) = f(b)$, je $f(u) = f(v)$. Zato je ekvivalenčna relacija ρ^f močno desno regularna.

Dokažimo še močno levo regularnost, to je $(x \star a)\rho^f(x \star b)$. Naj bo $z \in x \star a$ in $w \in x \star b$. Potem je:

$$f(z) = f(x \star a) = f(x) \bullet f(a),$$

$$f(w) = f(x \star b) = f(x) \bullet f(b).$$

Iz definicije ekvivalenčne relacije ρ^f vemo, da je $f(a) = f(b)$, zato je tudi $f(z) = f(w)$. Omenjena ekvivalenčna relacija je zato močno levo regularna. Ker je ekvivalenčna relacija ρ^f močno desno in močno levo regularna, je tudi močno regularna. □

O regularnih in močno regularnih relacijah najdete več v [5].

3.2.4 Popolne hipergrupe

Trditev 3.51. *Na polhipergrupi H definiramo relacijo $\beta_n, n > 1$, na naslednji način:*

$$a\beta_n b \Leftrightarrow \exists (x_1, \dots, x_n) \in H^n \colon \{a, b\} \subseteq \prod_{i=1}^{n} x_i,$$

$$\beta = \bigcup_{n \geq 1} \beta_n, \beta_1 = \{(x, x) \mid x \in H)\}.$$

$\prod_{i=1}^{n} x_i$ je množica vseh končnih produktov elementov polhipergrupe H. Relacija β je refleksivna in simetrična relacija na H. Z β^* bomo označili tranzitivno zaprtje za relacijo β. Tranzitivno zaprtje relacije β na polhipergrupi H je najmanjša tranzitivna relacija na tej polhipergrupi, ki vsebuje relacijo β.

Dokaz. Za simetričnost relacije β_1 mora veljati $x\beta_1 y \longrightarrow y\beta_1 x, x, y \in H$. Relacija β_1 je definirana kot $\beta_1 = \{(x, x) \mid x \in H)$. Zato je očitno simetrična relacija.
Relacija β_1 je refleksivna, če zanjo velja $x\beta_1 x$. Refleksivnost relacije β_1 je seveda razvidna iz definicije same relacije.
Iz definicije relacije β_n vidimo, da je ta relacija simetrična relacija. Velja namreč:

$$a\beta_n b \Leftrightarrow \exists (x_1, \dots, x_n) \in H^n \colon \{a, b\} \subseteq \prod_{i=1}^{n} x_i,$$

$$b\beta_n a \Leftrightarrow \exists (x_1, \dots, x_n) \in H^n \colon \{b, a\} \subseteq \prod_{i=1}^{n} x_i.$$

Zato je relacija β simetrična in refleksivna relacija. □

V tem poglavju se bomo seznanili z osnovami popolnih hipergrup. Le-te je prvi definiral Koskas. Kasneje je več raziskovalcev definiralo različne vrste popolnih hipergrup. Tako poznamo $n-$popolne hipergrupe, n^*-popolne hipergrupe, $\gamma-$popolne hipergrupe in γ^*-popolne hipergrupe. V tem poglavju bomo poleg osnovnih definicij spoznali n^*-popolne hipergrupe, ki so posplošitve $n-$popolnih hipergrup. Povzeli smo jih po [15].

Definicija 3.52. Neprazno podmnožico A polhipergrupe H imenujemo **popolni del** hipergrupe H, če je za vse $n \geq 2$ in za vse $(x_1, x_2, \ldots, x_n) \in H^n$ iz

$$\prod_{i=1}^{n} x_i \bigcap A \neq \emptyset \Longrightarrow \prod_{i=1}^{n} x_i \subseteq A.$$

Definicija 3.53. Naj bo A neprazna podmnožica hipergrupe H. Presečišče popolnih delov hipergrupe H, ki vsebuje A, imenujemo **popolno zaprtje**.

Definicija 3.54. Z zapisom $C(A)$ bomo označili popolno zaprtje neprazne podmnožice A v polhipergrupi H. Polhipergrupo H imenujemo **popolna**, če zadošča enemu od naslednjih pogojev:

- $\forall (x, y) \in H^2, \forall a \in x \star y, C(a) = x \star y,$
- $\forall (x, y) \in H^2, C(x \star y) = x \star y,$
- $\forall (m, n) \in \mathbb{N}^2, 2 \leq m, n, \forall (x_1, \ldots, x_n) \in H^n, \forall (y_1, \ldots, y_n) \in H^m,$

$$\prod_{i=1}^{n} x_i \bigcap \prod_{j=1}^{m} y_j \neq \emptyset \Longrightarrow \prod_{i=1}^{n} x_i = \prod_{j=1}^{m} y_j.$$

Hipergrupa je popolna, če je popolna polhipergrupa.
Element e imenujemo **identiteta**, če velja

$$a \in e \star a \bigcap a \star e, \forall a \in H.$$

Element $x' \in H$ imenujemo **inverz** elementa x, če za $e \in H$ velja

$$e \in x \star x' \bigcap x' \star x.$$

Definicija 3.55. Regularna hipergrupa H je hipergrupa, ki ima vsaj eno idetiteto e in vsak element ima najmanj en inverz. Regularna hipergrupa je obrnljiva, če vsak $(x, y, z) \in H^3$ zadošča pogojema:

- če je $x \in y \star z$, potem obstaja tak inverz z' elementa z, da velja $y \in x \star z'$;
- če je $x \in z \star y$, potem obstaja tak inverz z'' elementa z, da velja $y \in z'' \star x$.

Z $i(x)$ označimo množico inverzov za x, zato sta $x', x'' \in i(x)$.

Primer 3.56. Primer je vzet iz literature [13]. Naj bo $H = \{a, b, c, d\}$ hipergrupa s hiperoperacijo zapisano v tabeli:

$\star$	a	b	c	d
a	a	b	$\{c, d\}$	d
b	b	$\{a, b\}$	$\{c, d\}$	$\{c, d\}$
c	c	$\{c, d\}$	$\{a, b\}$	$\{a, b\}$
d	$\{c, d\}$	$\{c, d\}$	$\{a, b\}$	$\{a, b\}$

Potem je hipergrupa H s hiperoperacijo $\star$ regularna hipergrupa. Dokažimo, da to res velja. V definiciji 3.55 je zapisano, kaj mora veljati, da je hipergrupa tudi regularna. Dokazati moramo obstoj vsaj ene identitete ter vsakemu elementu hipergrupe poiskati vsaj en inverz. Najprej poiščimo identiteto. Da je element e identiteta mora veljati

$$a \in e \star a \bigcap a \star e, \forall a \in H.$$

- Ker je
  - $a \star a \bigcap a \star a = a \bigcap a = a,$
  - $a \star b \bigcap b \star a = b \bigcap b = b,$
  - $a \star c \bigcap c \star a = \{c, d\} \bigcap c = c,$
  - $a \star d \bigcap d \star a = d \bigcap \{c, d\} = d,$

  sklepamo, da je a identiteta.
- Ker je $b \star a \bigcap a \star b = b \bigcap b = b$, glede na definicijo identitete, b ne more biti identiteta za hipergrupo.
- Ker je $c \star a \bigcap a \star c = c \bigcap \{c, d\} = c$, moralo pa bi biti a, sklepamo, da c ni identiteta.
- Ker je $d \star a \bigcap a \star d = \{c, d\} \bigcap d = d$, element d ne more biti identiteta.

Edina identiteta za hipergrupo H je torej element a. Da dokažemo, da gre za regularno hipergrupo moramo vsakemu elementu poiskati tudi inverz. Za vsak element hipergrupe bomo preverili, ali je kateri izmed elementov $\{a, b, c, d\}$ njegov inverz. Pri iskanju inverza bomo upoštevali definicijo 3.54.

- Poiščimo inverz elementu a:
  - $a \star a \bigcap a \star a = a \bigcap a = a,$
  - $a \star b \bigcap b \star a = b \bigcap b = b,$
  - $a \star c \bigcap c \star a = \{c, d\} \bigcap c = c,$
  - $a \star d \bigcap d \star a = d \bigcap \{c, d\} = d.$

Torej a je sam sebi inverz.

- Poiščimo inverz elementu b:
  - $b \star a \bigcap a \star b = b \bigcap b = b,$
  - $b \star b \bigcap b \star b = \{a, b\} \bigcap \{a, b\} = \{a, b\},$

- $b \star c \bigcap c \star b = \{c, d\} \bigcap \{c, d\} = \{c, d\}$,
- $b \star d \bigcap d \star b = \{c, d\} \bigcap \{c, d\} = \{c, d\}$.

Od tod lahko sklepamo, da je b sam sebi inverz.

- Poiščimo inverz za element c:
  - $c \star a \bigcap a \star c = c \bigcap \{c, d\} = c$,
  - $c \star b \bigcap b \star c = \{c, d\} \bigcap \{c, d\} = \{c, d\}$,
  - $c \star c \bigcap c \star c = \{a, b\} \bigcap \{a, b\} = \{a, b\}$,
  - $c \star d \bigcap d \star c = \{a, b\} \bigcap \{a, b\} = \{a, b\}$.

Od tod lahko sklepamo, da je c sam sebi inverz.

- Poiščimo inverz še za element d:
  - $d \star a \bigcap a \star d = \{d, c\} \bigcap d = d$,
  - $d \star b \bigcap b \star d = \{c, d\} \bigcap \{c, d\} = \{c, d\}$,
  - $d \star c \bigcap c \star d = \{a, b\} \bigcap \{a, b\} = \{a, b\}$,
  - $d \star d \bigcap d \star d = \{a, b\} \bigcap \{a, b\} = \{a, b\}$.

Inverza elementa d sta elementa c in d. Tako smo pokazali, da ima vsak element v H vsaj en inverz in dokazali, da je hipergrupa H s pripadajočo hiperoperacijo res regularna hipergrupa.

Izrek 3.57. *Če je $(H, \star)$ popolna hipergrupa, potem z ω_H označimo identiteto za H in velja*

- $\omega_H = \{e \in H : \forall x \in H, x \in x \star e \bigcap e \star x\}$,
- *popolna hipergrupa H je regularna in obrnljiva.*

Opomba 3.58. Dokaz izreka 3.57 si lahko ogledate v [5].

Definicija 3.59. Če je hipergrupa $(H, \star)$ n^*-popolna, potem obstaja tak $n \in \mathbb{N}$, da velja $\beta_n^* = \beta$ in $\beta_{n-1}^* \neq \beta_n^*$.

Opomba 3.60. V literaturi, po kateri smo povzeli n^*-popolne hipergrupe, je zapis β enakovreden zapisu $(\beta)_H$. Mi bomo uporabljali zapis β.

Dokaz naslednje trditve je zapisan v [15].

Trditev 3.61. *Če obstaja tak $n \in \mathbb{N}$, da velja $\beta_n^* = \beta_{n+1}^*$, potem velja tudi enakost $\beta = \beta_n^*$.*

Posledica 3.62. *Hipergrupa $(H, \star)$ je n^*-popolna, če in samo če velja $\beta_{n+1} \subseteq \beta_n^* \neq \beta_{n-1}^*$.*

Tudi dokaz naslednje trditve je zapisan v [15].

Trditev 3.63. *Če ima hipergrup $(H, \star)$ dva ali tri elemente in ni grupa, potem je $(H, \star)$ 2^*-popolna hipergrupa.*

Primer 3.64. Dana je hipergrupa $H = \{a, b, c\}$ s hiperoperacijo $\star$.

$\star$	a	b	c
a	a	b	c
b	b	a	c
c	c	c	$\{a, b\}$

Hipergrupa H ni grupa, saj ne velja zakon o obratnem elementu oziroma inverzu. Velja pa zakon o zaprtosti ter zakon o nevrtalnem elementu. Dana hipergrupa je torej 2^*-popolna.

Trditev 3.65. *Najmanjše število elementov hipergrupe, ki ni 2^*-popolna, je štiri.*

Dokaz. Naj bo H hipergrupa s hiperoperacijo zapisano v tabeli:

$\star$	a	b	c	d
a	$\{a, b\}$	$\{c, d\}$	$\{a, b\}$	$\{c, d\}$
b	$\{c, d\}$	$\{a, b\}$	$\{c, d\}$	$\{a, b\}$
c	$\{a, b\}$	$\{c, d\}$	$\{a, b\}$	$\{c, d\}$
d	$\{c, d\}$	$\{a, b\}$	$\{c, d\}$	$\{a, b\}$

Preverimo, ali za $\forall (x, y, z) \in H^3$ velja $x \star y \star z = H$.

$$
\begin{aligned}
a\star a\star a &= \{a,b\}\star a = \{a,b\}\bigcup\{c,d\} = H, & c\star a\star a &= \{a,b\}\star a = \{a,b\}\bigcup\{c,d\} = H,\\
a\star a\star b &= \{a,b\}\star b = \{c,d\}\bigcup\{a,b\} = H, & c\star a\star b &= \{a,b\}\star b = \{c,d\}\bigcup\{a,b\} = H,\\
a\star a\star c &= \{a,b\}\star c = \{a,b\}\bigcup\{c,d\} = H, & c\star a\star c &= \{a,b\}\star c = \{a,b\}\bigcup\{c,d\} = H,\\
a\star a\star d &= \{a,b\}\star d = \{c,d\}\bigcup\{a,b\} = H, & c\star a\star d &= \{a,b\}\star d = \{c,d\}\bigcup\{a,b\} = H,\\
a\star b\star a &= \{c,d\}\star a = \{a,b\}\bigcup\{c,d\} = H, & c\star b\star a &= \{c,d\}\star a = \{a,b\}\bigcup\{c,d\} = H,\\
a\star b\star b &= \{c,d\}\star b = \{c,d\}\bigcup\{a,b\} = H, & c\star b\star b &= \{c,d\}\star b = \{c,d\}\bigcup\{a,b\} = H,\\
a\star b\star c &= \{c,d\}\star c = \{a,b\}\bigcup\{c,d\} = H, & c\star b\star c &= \{c,d\}\star c = \{a,b\}\bigcup\{c,d\} = H,\\
a\star b\star d &= \{c,d\}\star d = \{c,d\}\bigcup\{a,b\} = H, & c\star b\star d &= \{c,d\}\star d = \{c,d\}\bigcup\{a,b\} = H,\\
a\star c\star a &= \{a,b\}\star a = \{a,b\}\bigcup\{c,d\} = H, & c\star c\star a &= \{a,b\}\star a = \{a,b\}\bigcup\{c,d\} = H,
\end{aligned}
$$

$a\star c\star b = \{a,b\}\star b = \{c,d\}\bigcup\{a,b\} = H,$ $c\star c\star b = \{a,b\}\star b = \{c,d\}\bigcup\{a,b\} = H,$
$a\star c\star c = \{a,b\}\star c = \{a,b\}\bigcup\{c,d\} = H,$ $c\star c\star c = \{a,b\}\star c = \{a,b\}\bigcup\{c,d\} = H,$
$a\star c\star d = \{a,b\}\star d = \{c,d\}\bigcup\{a,b\} = H,$ $c\star c\star d = \{a,b\}\star d = \{c,d\}\bigcup\{a,b\} = H,$
$a\star d\star a = \{c,d\}\star a = \{a,b\}\bigcup\{c,d\} = H,$ $c\star d\star a = \{c,d\}\star a = \{a,b\}\bigcup\{c,d\} = H,$
$a\star d\star b = \{c,d\}\star b = \{c,d\}\bigcup\{a,b\} = H,$ $c\star d\star b = \{c,d\}\star b = \{c,d\}\bigcup\{a,b\} = H,$
$a\star d\star c = \{c,d\}\star c = \{a,b\}\bigcup\{c,d\} = H,$ $c\star d\star c = \{c,d\}\star c = \{a,b\}\bigcup\{c,d\} = H,$
$a\star d\star d = \{c,d\}\star d = \{c,d\}\bigcup\{a,b\} = H,$ $c\star d\star d = \{c,d\}\star d = \{c,d\}\bigcup\{a,b\} = H,$
$b\star a\star a = \{c,d\}\star a = \{a,b\}\bigcup\{c,d\} = H,$ $d\star a\star a = \{c,d\}\star a = \{a,b\}\bigcup\{c,d\} = H,$
$b\star a\star b = \{c,d\}\star b = \{c,d\}\bigcup\{a,b\} = H,$ $d\star a\star b = \{c,d\}\star b = \{c,d\}\bigcup\{a,b\} = H,$
$b\star a\star c = \{c,d\}\star c = \{a,b\}\bigcup\{c,d\} = H,$ $d\star a\star c = \{c,d\}\star c = \{a,b\}\bigcup\{c,d\} = H,$
$b\star a\star d = \{c,d\}\star d = \{c,d\}\bigcup\{a,b\} = H,$ $d\star a\star d = \{c,d\}\star d = \{c,d\}\bigcup\{a,b\} = H,$
$b\star b\star a = \{a,b\}\star a = \{a,b\}\bigcup\{c,d\} = H,$ $d\star b\star a = \{a,b\}\star a = \{a,b\}\bigcup\{c,d\} = H,$
$b\star b\star b = \{a,b\}\star b = \{c,d\}\bigcup\{a,b\} = H,$ $d\star b\star b = \{a,b\}\star b = \{c,d\}\bigcup\{a,b\} = H,$
$b\star b\star c = \{a,b\}\star c = \{a,b\}\bigcup\{c,d\} = H,$ $d\star b\star c = \{a,b\}\star c = \{a,b\}\bigcup\{c,d\} = H,$
$b\star b\star d = \{a,b\}\star d = \{c,d\}\bigcup\{a,b\} = H,$ $d\star b\star d = \{a,b\}\star d = \{c,d\}\bigcup\{a,b\} = H,$
$b\star c\star a = \{c,d\}\star a = \{a,b\}\bigcup\{c,d\} = H,$ $d\star c\star a = \{c,d\}\star a = \{a,b\}\bigcup\{c,d\} = H,$
$b\star c\star b = \{c,d\}\star b = \{c,d\}\bigcup\{a,b\} = H,$ $d\star c\star b = \{c,d\}\star b = \{c,d\}\bigcup\{a,b\} = H,$
$b\star c\star c = \{c,d\}\star c = \{a,b\}\bigcup\{c,d\} = H,$ $d\star c\star c = \{c,d\}\star c = \{a,b\}\bigcup\{c,d\} = H,$
$b\star c\star d = \{c,d\}\star d = \{c,d\}\bigcup\{a,b\} = H,$ $d\star c\star d = \{c,d\}\star d = \{c,d\}\bigcup\{a,b\} = H,$
$b\star d\star a = \{a,b\}\star a = \{a,b\}\bigcup\{c,d\} = H,$ $d\star d\star a = \{a,b\}\star a = \{a,b\}\bigcup\{c,d\} = H,$
$b\star d\star b = \{a,b\}\star b = \{c,d\}\bigcup\{a,b\} = H,$ $d\star d\star b = \{a,b\}\star b = \{c,d\}\bigcup\{a,b\} = H,$
$b\star d\star c = \{a,b\}\star c = \{a,b\}\bigcup\{c,d\} = H,$ $d\star d\star c = \{a,b\}\star c = \{a,b\}\bigcup\{c,d\} = H,$
$b\star d\star d = \{a,b\}\star d = \{c,d\}\bigcup\{a,b\} = H,$ $d\star d\star d = \{a,b\}\star d = \{c,d\}\bigcup\{a,b\} = H.$

Identiteti za dano hipergrupo sta a in c, saj je $a\star a\bigcap a\star a = \{a,b\}$ in $c\star a\bigcap a\star c = \{a,b\}$.

Preverimo še, kaj je ω_H za identiteto a:
$\omega_H = \{a \in H\colon \forall a \in H; a \in a\star a\bigcap a\star a\} = \{a,b\}\bigcap\{a,b\} = \{a,b\},$
$\omega_H = \{a \in H\colon \forall b \in H; b \in b\star a\bigcap a\star b\} = \{c,d\}\bigcap\{c,d\} = \{c,d\},$
$\omega_H = \{a \in H\colon \forall c \in H; c \in c\star a\bigcap a\star c\} = \{a,b\}\bigcap\{a,b\} = \{a,b\},$
$\omega_H = \{a \in H\colon \forall d \in H; d \in d\star a\bigcap a\star d\} = \{c,d\}\bigcap\{c,d\} = \{c,d\}.$

Enako naredimo tudi za ideniteto c:
$\omega_H = \{c \in H\colon \forall a \in H; a \in a\star c\bigcap c\star a\} = \{a,b\}\bigcap\{a,b\} = \{a,b\},$
$\omega_H = \{c \in H\colon \forall b \in H; b \in b\star c\bigcap c\star b\} = \{c,d\}\bigcap\{c,d\} = \{c,d\},$
$\omega_H = \{c \in H\colon \forall c \in H; c \in c\star c\bigcap c\star c\} = \{a,b\}\bigcap\{a,b\} = \{a,b\},$
$\omega_H = \{c \in H\colon \forall d \in H; d \in d\star c\bigcap c\star d\} = \{c,d\}\bigcap\{c,d\} = \{c,d\}.$

Iz zapisanega vidimo, da je $H = \omega_H$, $\mid H \mid = 4, \mid \beta_2^* \mid = 2$ in zato $\mid H/\beta_2^* \mid = 2$. Torej je H 3^*-popolna in ni 2^*-popolna hipergrupa.

Več o popolnih hipergrupah je zapisano v [5]. □

3.2.5 Pridružitveni prostori

Pridružitvene prostore je prvi definiral Prenowitz [5]. V angleškem jeziku se za pridružitvene prostore uporabljata besedni zvezi "join space"in "join geometry". Pridružitveni prostori so abstraktni modeli za linearno, sferično in projektivno geometrijo. Koncept pridružitvenih prostorov sta z Jantosciakom prenesla tudi na evklidsko in neevklidsko geometrijo. Evklidsko geometrijo poznamo kot splošno geometrijo, zato besedo evklidska najpogosteje izpuščamo. Ukvarja se s proučevanjem prostora, obliko likov in teles, ki se nahajajo v njem. Neevklidska geometrija sloni na drugačnih načelih, zato imajo v njej geometrijski objekti drugačne lastnosti. Z namenom definiranja pridružitvenih prostorov bomo ponovili naslednjo definicijo: za $a, b \in (H, \star)$, kjer je H hipergrupoid, je

$$a/b = \{x \in H \mid a \in x \star b\}.$$

Podobno bomo A/B definirali kot

$$\bigcup_{a \in A, b \in B} a/b. \tag{3.2}$$

Definicija 3.66. Komutativno hipergrupo $(H, \star)$ imenujemo **pridružitveni prostor**, če za vse $x, y, z, w \in H$ velja **transpozicijski zakon**:

$$x/y \bigcap z/w \neq \emptyset \Longrightarrow x \star w \bigcap y \star z \neq \emptyset.$$

Opomba 3.67. Elemente komutativne hipergrupe imenujemo **točke** in jih označimo z $x, y, z, \ldots$ Množico točk označimo z velikimi črkami $X, Y, Z, \ldots$ Zapisali bomo nekaj trditev, ki nam bodo v pomoč pri dokazih trditev v nadaljevanju.

Naslednje trditve in dokazi so povzeti po knjigi [9].

Trditev 3.68. *Naj bodo X, Y in Z poljubne množice točk pridružitvenega prostora $(H, \star)$. Potem je $X \cong Y/Z$, če in samo če je $X \star Z \cong Y$.*

Dokaz. Naj bo $w = X$ in $w \subset Y/Z$. Potem $w \subset Y/Z$ zagotavlja obstoj takega y in takega z, da je $y \subset Y, z \subset Z$ in $w \subset y/z$. Ob upoštevanju zapisa 3.2 je $y \subset w \star z$ in $w \star z \subset X \star Z$. Od tod sledi $y \subset X \star Z, y \subset Y$ in $X \star Z \cong Y$. □

Trditev 3.69. *Za množici točk X in Y pridružitvenega prostora $(H, \star)$ velja $Z \star Y = Y \star Z$.*

Dokaz. Dokazati moramo, da velja $Z \star Y \subseteq Y \star Z$ in $Y \star Z \subseteq Z \star Y$. Naj bo $x \subseteq Z \star Y$. Od tod sledi, da je $x \subseteq z \star y$ za $z \subseteq Z, y \subseteq Y$. Zaradi komutativnosti velja enakost $z \star y = y \star z$. Zato velja tudi $x \subseteq y \star z$. Od tod sklepamo, da je $x \subseteq Y \star Z$. Na podoben način dokažemo tudi $Y \star Z \subseteq Z \star Y$. □

Trditev 3.70. *Naj bodo X, Y, Z in W poljubne množice točk pridružitvenega prostora $(H, \star)$. Če je $X \subseteq Y$ in $Z \subseteq W$, potem je tudi $X \star Z \subseteq Y \star W$ in $X/Z \subseteq Y/W$.*

Dokaz. Če je $w \subseteq X \star Z$, je tudi $w \subseteq x \star z$, pri čemer je $x \subseteq X$ in $z \subseteq Z$. Iz zgornje trditve vemo, da je $x \subseteq Y$ in $z \subseteq W$. Torej iz $w \subseteq x \star z$ sledi $w \subseteq Y \star W$. Na podoben način dokažemo tudi $X/Z \subseteq Y/W$. □

Dokaz naslednje trditve lahko bralec prebere v [9].

Trditev 3.71. *Če so X, Y, Z in W poljubne množice točk pridružitvenega prostora $(H, \star)$ in je $X/Y \cong Z/W$, potem je $X \star W \cong Y \star Z$.*

Trditev 3.72. *Za množico točk pridružitvenega prostora $(H, \star)$ velja:*

- $(X/Y)/Z = X/(Y \star Z)$,
- $X \neq \emptyset \Longrightarrow Y \subseteq X/(X/Y)$,
- $X \star (Y/W) \subseteq (X \star Y)/W$,
- $X/(Y/W) \subset (X \star W)/Y$.

Dokaz. Najprej dokažimo trditev $(X/Y)/Z = X/(Y \star Z)$. Za enakost dveh množic moramo dokazati, da je $(X/Y)/Z \subseteq X/(Y \star Z)$ in $X/(Y \star Z) \subseteq (X/Y)/Z$. Naj bo $w \cong (X/Y)/Z$. Ob večkratnem upoštevanju trditve 3.68 dobimo naslednje zapise:

$$w \star Z \cong (X/Y),$$

$$w \star Z \star Y \cong X,$$

$$w \cong X/(Z \star Y).$$

Ker je $Z \star Y = Y \star Z$, dobimo zapis:

$$w \cong X/(Y \star Z),$$

$$w = X/(Y \star Z).$$

Dokazali smo, da je $(X/Y)/Z \subseteq X/(Y \star Z)$. Dokažimo še, da je $X/(Y \star Z) \subseteq (X/Y)/Z$. Naj bo $w \subseteq X/(Y \star Z)$. Tudi pri tem dokazu bomo upoštevali trditev 3.68:

$$w \star (Y \star Z) \cong X,$$

$$w \star (Z \star Y) \cong X,$$

$$w \star Z \cong X/Y,$$

$$w \cong (X/Y)/Z.$$

Zato je $X/(Y \star Z) \subseteq (X/Y)/Z$ in $(X/Y)/Z = X/(Y \star Z)$. Dokažimo drugo točko trditve 3.72. Naj bo $w \subseteq Y$. Ob upoštevanju trditve 3.70 dobimo zapis $X/w \subseteq X/Y$. Ker $X \neq \emptyset$, tudi $X/w \neq \emptyset$. Zato je $X/Y \cong X/w$. Dvakrat upoštevamo trditev 3.68 in dobimo:

$$(X/Y)w \cong X,$$

$$w \cong X/(X/Y).$$

Zato je $Y \subseteq X/(X/Y)$. Na podoben način dokažimo tudi tretjo trditev. Naj bo $w \cong X \star (Y/W)$. Tudi tukaj upoštevamo trditev 3.68. Dobimo:

$$w/X \cong (Y/W),$$

Upoštevamo še trditev 3.71. in trditev 3.68. Tako dobimo:

$$w \star W \cong X \star Y,$$

$$w \cong X \star Y/W.$$

Dokazali smo $X \star (Y/W) \subseteq (X \star Y)/W$. Ostal nam je še dokaz zadnje točke. Naj bo $w \cong X/(Y/W)$. Ob upoštevanju trditev 3.68 in 3.71 je:

$$w(Y/W) \cong X,$$

$$Y/W \cong Y/w,$$

$$Y \star w \cong X \star W,$$

$$w \cong X \star W/Y.$$

Dokazali smo tudi zadnjo trditev. □

Definicija 3.73. Množica točk M pridružitvenega prostora $(H, \star)$ je **linearna**, če za vse $a, b \in M$ velja $a \star b \subseteq M$ in $a/b \subseteq M$. Če je množica linearna, potem je $M = M \star M = M/M$.

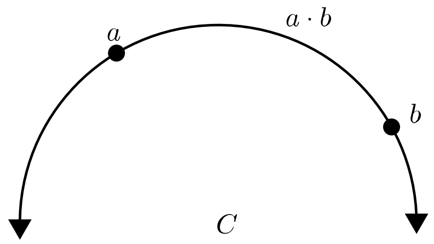
Definicija 3.74. Naj bosta a in b poljubni točki. Potem je razširitev iz a na b enaka množici vseh točk x, za katere velja $bx \supset a$.

Naslednji izrek je povzet po knjigi [9], kjer si lahko bralec prebere tudi njegov dokaz.

Izrek 3.75. *Množica M je linearna, če je zaprta za operacijo razširitve.*

Naslednji primer pridružitvenega prostora je zapisan v [9].

Primer 3.76. Slika 6 prikazuje polkrog C, brez končnih točk. Na polkrogu C ležita različni točki a in b. Odprti lok $a \cdot b$ vsebuje vse točke polkroga C, ki ležijo med a in b, razen točk a in b.



Slika 6: Polkrog C.

Naj bo P množica C. Definiramo pridružitveno operacijo na P kot odprti lok $a \cdot b = ab, a \neq b$.
V naslednjih točkah bomo utemeljili, zakaj je $(P, \cdot)$ pridružitveni prostor.

- Zakon o obstoju: $ab \neq \emptyset$,
  Ker $a \neq b$, pridružitveni prostor P vsebuje vsaj eno točko.

- Komutativnosti zakon: $ab = ba$,
  Iz slike je razvidno, da sta odprta loka ab in ba enaki množici.

- Asociativnostni zakon: $(ab)c = a(bc)$,
  Predpostavimo, da točke a, b in c ležijo na polkrogu C in naj bo točka b med točkama a in c. Potem je $(ab)c$ enak loku ac in tudi $a(bc)$ je enak loku ac.

- Idempotentni zakon: $aa = a$;
  Veljavnost tega zakona izhaja iz točke 1.

- Zakon o obstoju: $a/b \neq \emptyset$;
  Predpostavimo, da $a \neq b$. Potem je po definiciji $a/b = \{x \in P \mid a \in x \cdot b\}$ enako odprtemu intervalu bx, ki vsebuje a. Če je $a = b$, je zakon o obstoju enak a/a. Predpostavimo, da $x \neq a$. Potem $a \not\subset a \cdot x$. Ker $x \not\subset a/a$, je a/a enako a.

- Idempotentni zakon: $a/a = a$;
  Pri točki 5 smo dokazali tudi idempotentni zakon $a/a = a$.

- Transpozicijski zakon: $a/b \bigcap c/d \Longrightarrow ad \bigcap bc \neq \emptyset$,
  Če na polkrogu C razporedimo točke od leve proti desni v naslednjem vrstnem redu: a, c, b, d, bo veljal tudi transpozicijski zakon.

Utemeljili smo, da je $(C, \cdot)$ pridružitveni protor.

Poznamo nekaj vrst pridružitvenih prostorov. V naslednji definiciji so opisani trije različni tipi le-teh.

Kanonične hipergrupe

Kanonične hipergrupe so posebni primer pridružitvenih prostorov. Prvi jih je kot dodatne strukture hiperpoljem predstavil Krasner [5].
Definicijo hiperpolja bomo zapisali po definiciji kanonične hipergrupe.

Definicija 3.77. Hipergrupa $(H, \star)$ je kanonična, če

- je komutativna,
- ima skalarno identiteto e, za katero velja $x \star e = e \star x = x$ za $\forall x \in H$,
- vsak element ima inverz, kar pomeni $e \in x \star x^{-1} \cap x^{-1} \star x$,
- je obrnljiva, to je, če je $x \in y \star z$, potem obstaja inverz y^{-1} za y in z^{-1} za z tak, da velja $z \in y^{-1} \star x$ in $y \in x \star z^{-1}$.

Definicija 3.78. Trojica $(F, +, \cdot)$ je hiperpolje, če je:

- $(F, +)$ kanonična hipergrupa,
- $(F, \cdot)$ taka polhipergrupa, da je $x \cdot 0 = 0 \cdot x = 0$, kjer je število 0 identiteta,
- za vse $x, y, z \in F$ velja $x \cdot (y + z) = x \cdot y + x \cdot z$ in $(x + y) \cdot z = x \cdot z + y \cdot z$,
- $(F \backslash \{0\}, \cdot)$ je hipergrupa.

Primer 3.79. Naslednji primer je vzet iz članka [14]. Naj bo $H = [0, 1]$. Definiramo hiperoperacijo $+$ kot

$$x + y = \begin{cases} [0, x], & \text{če } x = y, \\ \{max\{x, y\}\}, & \text{če } x \neq y. \end{cases}$$

Potem je $(H, +)$ kanonična hipergrupa.
Preverimo, ali je hipergrupa H komutativna. Za vsak $x, y \in H$ mora veljati $x + y = y + x$. Če je $x = y$, je rezultat hiperoperacije $+$ interval $[0, x]$. Če sta x in y različna, je rezultat hiperoperacije $+$ večji od seštevancev. Zato je hipergrupa komutativna. Ker za vsak $x \in H$ veljata enakosti $x + 0_H = x$ in $0_H + x = x, 0_H \in H$, je število 0_H identiteta. Inverz števila x označimo z $-x$. Število in njegov inverz sta elementa hipergrupe H. Velja tudi

$$0_H \in x + (-x) \bigcap (-x) + x.$$

Za poljubne tri elemente iz hipergrupe H je $x \in y + z$. Inverza za y in z označimo z $-y$ in $-z$. Velja tudi $z \in -y + x$ in $y = x + (-z)$. Dokazali smo, da je hipergrupa H za hiperoperacijo $+$ kanonična hipergrupa.

Naslednji primer je zapisan v [17].

Primer 3.80. Naj bo $F = \{x, y\}$ množica s hiperoperacijama zapisanima v tabelah. Potem je $(F, +, \cdot)$ hiperpolje.

$+$	x	y
x	x	y
y	y	$\{x, y\}$

$\cdot$	x	y
x	x	x
y	x	y

V nadaljevanju bomo utemeljili, zakaj je $(F, +, \cdot)$ hiperpolje.

- Najprej bomo preverili, ali je $(F, +)$ kanonična hipergrupa.
  - Preverimo asociativnost $x + (y + z) = (x + y) + z$ in komutativnost $x + y = y + x$. Ker ima množina F dva elementa, bomo omenjena zakona preverjali samo za dva elementa. Opazimo, da je:

    $(x + x) + x = x + (x + x) \Leftrightarrow$
    $x + x = x + x \Leftrightarrow$
    $x = x.$
    Podobno:
    $(x + x) + y = x + (x + y) \Leftrightarrow$
    $x + y = x + y \Leftrightarrow$
    $y = y.$

    $(x + y) + x = x + (y + x) \Leftrightarrow$
    $y + x = x + y \Leftrightarrow$
    $y = y.$

    $(x + y) + y = x + (y + y) \Leftrightarrow$
    $y + y = x + \{x, y\} \Leftrightarrow$
    $\{x, y\} = x + x \bigcup x + y \Leftrightarrow$
    $\{x, y\} = x \bigcup y \Leftrightarrow$
    $\{x, y\} = \{x, y\}.$

    $(y + y) + y = y + (y + y) \Leftrightarrow$
    $\{x, y\} + y = y + \{x, y\} \Leftrightarrow$
    $x + y \bigcup y + y = y + x \bigcup y + y \Leftrightarrow$
    $y \bigcup \{x, y\} = y \bigcup \{x, y\} \Leftrightarrow$

$\{x, y\} = \{x, y\}$.

$(y + y) + x = y + (y + x) \Leftrightarrow$
$\{x, y\} + x = y + y \Leftrightarrow$
$x + x \bigcup y + x = \{x, y\} \Leftrightarrow$
$x \bigcup y = \{x, y\} \Leftrightarrow$
$\{x, y\} = \{x, y\}$.

$(y + x) + x = y + (x + x) \Leftrightarrow$
$y + x = y + x \Leftrightarrow$
$y = y$.

$(y + x) + y = y + (x + y) \Leftrightarrow$
$y + y = y + y \Leftrightarrow$
$\{x, y\} = \{x, y\}$.
Hiperoperacija $+$ je asociativna. Bralec naj sam preveri še aksiom reprodukcije. Za $a \in F$ je $a + F = F + a = F$, zato je $(F, +)$ hipergrupa. Preverimo še komutativnost hiperoperacije $+$.
$x + y = y + x \Leftrightarrow$
$y = y$.
Hiperoperacija $+$ je komutativna.

- Ima identiteto e, za katero velja $x + e = e + x = x$ za $\forall x \in F$. Preverimo, ali je x identiteta.
  $x + x = x + x \Leftrightarrow$
  $x = x$.
  Element x je identiteta. Na podoben način preverimo, ali je identiteta tudi element y.
  $x + y = y + x \Leftrightarrow$
  $y = y$.
  Ker $y \neq x$, element y ni identiteta.
- Vsak element ima inverz, kar pomeni, da je $e \in x + x^{-1} \cap x^{-1} + x$. Najprej poiščimo inverze za element x. Denimo, da je element x inverz. Preverimo, ali to res drži.
  $x + x \cap x + x \Leftrightarrow$
  $x \cap x = x$.
  Od tod sklepamo, da je element x sam sebi inverz. Preverimo, ali je inverz tudi element y.
  $x + y \cap y + x \Leftrightarrow$
  $y \cap y = y$.

Iz zapisanega sklepamo, da element y ni inverz elementa x. Poiščimo inverz še za element y. Predpostaimo, da je element y sam sebi inverz. Veljati mora $x \in y + y^{-1} \cap y^{-1} + y$.
$y + y = y + y \Leftrightarrow$
$\{x, y\} \cap \{x, y\} = \{x, y\} \Leftrightarrow$
$x \in \{x, y\}$.
Element y je res sam sebi inverz. Preverimo, ali je inverz za element y tudi element x.
$y + x \cap x + y \Leftrightarrow$
$y \cap y = y$.
Ugotovili smo, da element x ni inverz za element y.

– Hipergrupa je obrnljiva. Kar pomeni, če je $x \in y + z$, potem obstajata inverza za y in z taka, da je $z \in y^{-1} + x$ in $y \in x + z^{-1}$. Ker ima F dva elementa, bomo predpostavili, da je $z = y$. Tako dobimo zapise $x \in y + y, y \in y^{-1} + x$ in $y \in x + y^{-1}$. Preverimo, ali to res drži.
$x \in y + y \Leftrightarrow$
$x \in \{x, y\}$.

$y \in y^{-1} + x \Leftrightarrow$
$y \in y + x \Leftrightarrow$
$y \in y$.

$y \in x + y^{-1} \Leftrightarrow$
$y \in x + y \Leftrightarrow$
$y \in y$.
Utemeljili smo, da je $(F, +)$ kanonična hipergrupa.

• $(F, \cdot)$ je taka polhipergrupa, da za vsak $x \in F$ velja $x \cdot 0 = 0 \cdot x = 0$. Dokazati moramo, da je za poljubne tri elemente iz F $(x \cdot y) \cdot z = x \cdot (y \cdot z)$. Množica F ima dva elementa. Preverimo za vse možnosti.

– $(x \cdot x) \cdot x = x \cdot (x \cdot x) \Leftrightarrow$
$x \cdot x = x \cdot x \Leftrightarrow$
$x = x$.

– $(x \cdot x) \cdot y = x \cdot (x \cdot y) \Leftrightarrow$
$x \cdot y = x \cdot x \Leftrightarrow$
$x = x$.

– $(x \cdot y) \cdot x = x \cdot (y \cdot x) \Leftrightarrow$
$x \cdot x = x \cdot x \Leftrightarrow$
$x = x$.

– $(x \cdot y) \cdot y = x \cdot (y \cdot y) \Leftrightarrow$
$x \cdot y = x \cdot y \Leftrightarrow$
$x = x$.

– $(y \cdot y) \cdot y = y \cdot (y \cdot y) \Leftrightarrow$
$y \cdot y = y \cdot y \Leftrightarrow$
$y = y$.

– $(y \cdot y) \cdot x = y \cdot (y \cdot x) \Leftrightarrow$

$y \cdot x = y \cdot x \Leftrightarrow$
$x = x.$

- $(y \cdot x) \cdot y = y \cdot (x \cdot y) \Leftrightarrow$
  $x \cdot y = y \cdot x \Leftrightarrow$
  $x = x.$
- $(y \cdot x) \cdot x = y \cdot (x \cdot x) \Leftrightarrow$
  $x \cdot x = y \cdot x \Leftrightarrow$
  $x = x.$

Ker veljajo vse zapisane enakosti, je $(F, \cdot)$ polhipergrupa. Za vse elemente iz polhipergrupe $(F, \cdot)$ velja tudi enakost $x \cdot 0 = 0 \cdot x = 0$.

- Za elemente iz F mora veljati tudi $x \cdot (y+z) = x \cdot y + x \cdot z$ in $(x+y) \cdot z = x \cdot z + y \cdot z$.

  - $x \cdot (x+x) = x \cdot x + x \cdot x \Leftrightarrow$
    $x \cdot x = x + x \Leftrightarrow$
    $x = x.$
  - $x \cdot (x+y) = x \cdot x + x \cdot y \Leftrightarrow$
    $x \cdot y = x + x \Leftrightarrow$
    $x = x.$
  - $x \cdot (y+x) = x \cdot y + x \cdot x \Leftrightarrow$
    $x \cdot y = x + x \Leftrightarrow$
    $x = x.$
  - $x \cdot (y+y) = x \cdot y + x \cdot y \Leftrightarrow$
    $x \cdot \{x, y\} = x + x \Leftrightarrow$
    $x \cdot x \bigcup x \cdot y = x \Leftrightarrow$
    $x \bigcup x = x \Leftrightarrow$
    $x = x.$
  - $y \cdot (y+y) = y \cdot y + y \cdot y \Leftrightarrow$
    $y \cdot \{x, y\} = y + y \Leftrightarrow$
    $y \cdot x \bigcup y \cdot y = \{x, y\} \Leftrightarrow$
    $x \bigcup y = \{x, y\} \Leftrightarrow$
    $\{x, y\} = \{x, y\}.$
  - $y \cdot (y+x) = y \cdot y + y \cdot x \Leftrightarrow$
    $y \cdot y = y + x \Leftrightarrow$
    $y = y.$
  - $y \cdot (x+y) = y \cdot x + y \cdot y \Leftrightarrow$
    $y \cdot y = x + y \Leftrightarrow$
    $y = y.$
  - $y \cdot (x+x) = y \cdot x + y \cdot x \Leftrightarrow$
    $y \cdot x = x + x \Leftrightarrow$
    $x = x.$

  Preverimo še drugo enakost iz 3. točke.

  - $(x+x) \cdot x = x \cdot x + x \cdot x \Leftrightarrow$
    $x \cdot x = x + x \Leftrightarrow$
    $x = x.$
  - $(x+x) \cdot y = x \cdot y + x \cdot y \Leftrightarrow$
    $x \cdot y = x + x \Leftrightarrow$
    $x = x.$
  - $(x+y) \cdot x = x \cdot x + y \cdot x \Leftrightarrow$
    $y \cdot x = x + x \Leftrightarrow$
    $x = x.$
  - $(x+y) \cdot y = x \cdot y + y \cdot y \Leftrightarrow$
    $y \cdot y = x + y \Leftrightarrow$
    $y = y.$
  - $(y+y) \cdot y = y \cdot y + y \cdot y \Leftrightarrow$
    $\{x, y\} \cdot y = y + y \Leftrightarrow$
    $x \cdot y \bigcup y \cdot y = \{x, y\} \Leftrightarrow$
    $x \bigcup y = \{x, y\} \Leftrightarrow$
    $\{x, y\} = \{x, y\}.$
  - $(y+x) \cdot y = y \cdot y + x \cdot y \Leftrightarrow$
    $y \cdot y = y + x \Leftrightarrow$
    $y = y.$

– $(y+y)\cdot x = y\cdot x + y\cdot x \Leftrightarrow$
$\{x,y\}\cdot x = x + x \Leftrightarrow$
$x\cdot x \bigcup y\cdot x = x \Leftrightarrow$
$x \bigcup x = x \Leftrightarrow$
$x = x.$

– $(y+x)\cdot x = y\cdot x + x\cdot x \Leftrightarrow$
$y\cdot x = x + x \Leftrightarrow$
$x = x.$

Ugotovili smo, da veljajo zapisane enakosti pri točki 3.

- Preverimo še, ali je $(F\backslash\{0\},\cdot)$ hipergrupa. Dokazali smo že, da je hiperoperacija $\cdot$ asociativna. Preverimo še, ali zanjo velja tudi aksiom reprodukcije, to je, $a\cdot F = F\cdot a = F, a\in F$. Najprej preverimo za element y.
  $y\cdot F = F\cdot y \Leftrightarrow$
  $y\cdot\{x,y\} = \{x,y\}\cdot y \Leftrightarrow$
  $y\cdot x \bigcup y\cdot y = x\cdot y \bigcup y\cdot y \Leftrightarrow$
  $x \bigcup y = x \bigcup y \Leftrightarrow$
  $\{x,y\} = \{x,y\} \Leftrightarrow$
  $F = F.$
  Za element x omenjena enakost ne drži, zato predvidevamo, da je $x = 0$ in $(F,+,\cdot)$ je hiperpolje.

Izrek 3.81. *Komutativna hipergrupa je kanonična, če in samo če je pridružitveni prostor s skalarno identiteto.*

Dokaz. Naj bo $(H,\star)$ komutativna hipergrupa ter $a,b,c\in H$. Dokažimo, da je inverz poljubnega elementa enolično določen. Naj bo e skalarna identiteta. Če je $e\in a\star b\cap a\star c$, potem je $a\in e/b\cap e/c$. Vidimo, da $e\star c\cap e\star b$ ni enak prazni množici. Zato je $b = c = a^{-1}$. Preverimo še obrnljivost hipergrupe H. Vemo, da je $a\in b\star c$, če in samo če je $b\in a/c$. Iz $e\in b\star b^{-1}$ sledi, da je $b\in e/b^{-1}$. Zato $a\star b^{-1}\cap e\star c\neq\emptyset$. Dani presek ni enak prazni množici. Kar pomeni, da je $c\in a\star b^{-1}$. Zato je hipergrupa H kanonična. □

V kolikor želi bralec več znanja o pridružitvenih prostorih, naj poseže po knjigah [5] in [9].

4 Zaključek

V magistrskem delu smo najprej ponovili del vsebine iz teorije grup. To smo storili zaradi lažjega razumevanja hipergrup, s katerimi smo se ukvarjali v drugem delu magistrskega dela. Tako smo v drugem poglavju pisali o lastnostih, ki veljajo za grupo in spoznali primere grup. Seznanili smo se s tremi najbolj znanimi vrstami grup. Preučevali smo ciklične, permutacijske in diedrske grupe. Nadalje smo ugotavljali lastnosti permutacijskih grup. Diedrske grupe sestavljajo vrteži in zrcaljenja pravilnega n-kotnika. Ker smo v poglavju o hipergrupah predstavili primer hipergrupe z odseki, smo se v prvem poglavju spomnili osnovnih lastnosti odsekov. Seznanili smo se tudi z relacijami. Definirali smo binarno relacijo in opisali osnovne lastnosti relacij. Znanje o njih smo nadgradili v poglavju o hipergrupah.

V poglavju o hipergrupah smo uporabili znanje o odsekih. Le-te smo opisali v prvem poglavju. Glavna tema magistrske naloge so osnovne lastnosti hipergrup. Tako smo se v drugem poglavju posvetili osnovnim definicijam o hipergrupah. Zapisali smo, da je polhipergrupa neprazna množica skupaj s hiperoperacijo, za katero velja asociativnostni zakon. Če za dano hiperoperacijo velja tudi aksiom reprodukcije, je dana neprazna množica s hiperoperacijo hipergrupa. V tem poglavju smo podali nekaj primerov nepraznih množic z dano hiperoperacijo, ki so hipergrupe. V podpoglavju o podhipergrupah so zapisane definicije za zaprte, obrnljive, ultrazaprte in konjugirane podhipergrupe. Za dokaz zapisanih pojmov moramo preveriti levo in desno zaprtost (obrnljivost, ultrazaprtost in konjugiranost) podhipergrupe. Za boljšo predstavo smo podali primer zaprte podhipergrupe. V razdelku o homomorfizmih hipergrup smo definirali več vrst homomorfizmov in podali primer za homomorfizem tipa 4. Nekaj več teorije o homomorfizmih hipergrup lahko bralec prebere v [5]. Definirali smo tudi relacijo β, katero je Koskas uporabil za definicijo popolnih hipergrup ter opisali regularne in močno regularne relacije. Za povezavo hipergrup z grupami smo opisali osnovne lastnosti o regularnih in močno regularnih relacijah in zapisali primer popolne hipergrupe. Drugo poglavje in s tem tudi vsebino magistrskega dela smo končali s pridružitvenimi prostori in kanoničnimi hipergrupami.

Področje raziskovanja hipergrup je še dokaj mlado in zato tudi v fazi nenehnega

razvoja. V šestedesetih letih dvajsetega stoletja je mehke množice prvič predstavil iranski znanstvenik Zadeh. Skupaj z ostalimi matematiki je uporabo mehkih množic razširil na različna področja uporabe (sociologijo, agronomijo, jezikoslovje, biologijo, računalništvo, medicino in ekonomijo). Kot poseben primer mehkih množic so tudi grobe množice. Uporabo le-teh so razširili na področje verjetnosti. Povezavo med mehkimi množicami in hiperstrukturami je prvi predstavil Rosenfeld [31].
V današnjem času je raziskovanje usmerjeno predvsem:

- na računanje mehkega razreda (to je minimalne dolžine zaporedja) hipergrupoidov v povezavi z binarnimi relacijami,
- na preučevanje zaporedij pridružitvenih prostorov, določenih s hipergrupoidi,
- na proučevanje zaporedij pridružitvenih prostorov, določenih s hipergrupoidi in obdanimi s šibkimi hiperoperacijami,
- na preučevanje zaporedij mehkih množic in pridružitvenih prostorov, določenih s kitajskim hipergrupoidom [31].

V magistrskem delu smo predstavili nekatere osnovne lastnosti iz področja hipergrup. V drugem delu tretjega poglavja smo se na hitro dotaknili tudi nekoliko težjih stvari. V kolikor ima bralec željo, da znanje o hipergrupah nadgradi, lahko poseže po kateri od tujejezičnih knjig [2], [3], [4], [6] in [12].

5 Literatura

[1] J. L. Alperin in R. B. Bell, *Groups and Representations*. Springer-VerIag New York, 1995. *(Citirano na straneh 4, 17, 20 in 23.)*

[2] P. Corsini, *Prolegomena of hypergroup theory*, Aviani Editore, 1993. *(Citirano na strani 68.)*

[3] P. Corsini in V. Leoreanu, *Applications of Hyperstructures Theory*. Kluwer Academic Publishers, Advances in Mathematics, 2003. *(Citirano na strani 68.)*

[4] I. Cristea in B. Davvaz, *Fuzzy Algebraic Hyperstructures An Introduction*. Springer International Publishing Switzerland, 2015. *(Citirano na strani 68.)*

[5] B. Davvaz, *Polygroup Theory and Related Systems*, World Scientific Publishing Co. Pte. Ltd., 2013. *(Citirano na straneh 1, 4, 26, 31, 40, 42, 44, 48, 49, 51, 54, 57, 61, 66 in 67.)*

[6] B. Davvaz, *Semihypergroup Theory*, Academic Press, 2016. *(Citirano na strani 68.)*

[7] D. S. Dummit in R. M. Foote, *Abstract Algebra, Third Edition*. John Wiley and Sons, Inc., 2004. *(Citirano na strani 12.)*

[8] J. B. Fraleigh, *A first course in abstract algebra*, Addison-Wesley, Seventh Edition, 2003. *(Citirano na straneh 4, 6, 7, 8, 10, 12, 20, 21 in 23.)*

[9] J. Jantosciak in W. Prenowitz, *Join Geometries A Theory of Convex Sets and Linear Geometry*. Springer-Verlag New York Inc., 1979. *(Citirano na straneh 57, 58, 59, 60 in 66.)*

[10] J. J. Rotman, *An Introduction to the Theory of Groups*, Springer-Verlag 1995. *(Citirano na strani 13.)*

[11] A. R. Vasishta in ostali, *Text Book Algebra, Kanpur Edition*. Krishna Educational Publisker, 2014. *(Citirano na strani 11.)*

[12] T. Vougiouklis, *Hyperstructures and their representations*, Hadronic Press, Inc, 115, Palm Harber, USA, 1994. *(Citirano na strani 68.)*

[13] K. Bafrouei in F. Sadat, On fully simple semihypergroups. *Indian Journal of Fundamental and Applied Life Sciences* 4 (2014) 2514–2521. *(Citirano na strani 52.)*

[14] J. R. Castillo, Quotient and Homomorphism in Krasner Ternary Hyperrings. *International Journal of Mathematical Analysis* Vol. 8, No. 58 (2014) 2845–2859. *(Citirano na strani 61.)*

[15] M. De Salvo in G. Lo Faro, On the n*-complete hypergroups. *Discrete Mathematics* 208/209 (1999) 177–188. *(Citirano na straneh 51, 54 in 55.)*

[16] M. De Salvo, D. Fasino, D. Freni in G. Lo Faro, On strongly conjugable extensions of hypergroups of type U with scalar identity. *Filomat* 27:6 (2013) 977–994. *(Citirano na strani 41.)*

[17] B. Davvaz, M. Santilli in T. Vougiouklis, Algebra, Hyperalgebra and Lie-Santilli Theory. *Journal of Generalized Lie Theory and Applications* Volume 9, Issue 2 (2015) 1–5. *(Citirano na strani 62.)*

[18] C. G. Massouros, Some properties of certain Subhypergroups. *Ratio Mathematica* 25 (2013) 67–76. *(Ni citirano.)*

[19] Ch. G. Massouros in Ch. Tsitouras, On enumeration of hypergroups of order 3. *Computers and Mathematics with Applications* 59 (2010) 519–523. *(Citirano na strani 33.)*

[20] K. Conrad, *Cosets and Lagrange's theorem*,
http://www.math.uconn.edu/~kconrad/blurbs/grouptheory/coset.pdf.
(Datum ogleda: 21. 2. 2016.) *(Citirano na straneh 16 in 19.)*

[21] K. Conrad, *Dihedral Groups*,
http://www.math.uconn.edu/~kconrad/blurbs/grouptheory/dihedral.pdf.
(Datum ogleda: 11. 1. 2016.) *(Citirano na strani 14.)*

[22] K. Conrad, *Subgroups of Cyclic Groups*,
http://www.math.uconn.edu/~kconrad/blurbs/grouptheory/cyclicgp.pdf.
(Datum ogleda: 12. 11. 2016.) *(Citirano na strani 10.)*

[23] S. S. Epp, *Discrete Mathematics with Applications, Fourth Edition*,
http://fit.ac.ir/fa/download/ebooksclub.org_Discrete_Mathematics_with_Applicatio
(Datum ogleda: 31. 7. 2016.) *(Citirano na strani 2.)*

[24] K. James, *MTHSC 412 Section 4. 4 - Cosets of a subgroup*, http://www.math.clemson.edu/~kevja/COURSES/Math412/NOTES/Section-4.4-lecture.pdf. (Datum ogleda: 20. 2. 2016.) *(Citirano na strani 18.)*

[25] M. Omar, *Lecture - Homomorphisms and Isomorphisms, Cyclic Groups*, https://www.math.hmc.edu/~omar/math171F14/m171.notes.09.22.pdf. (Datum ogleda: 19. 12. 2016.) *(Ni citirano.)*

[26] J. Pakianathan, *MATH 436 Notes: Subgroups and Cosets.*, https://web.math.rochester.edu/people/faculty/jonpak/N3.pdf. (Datum ogleda: 12. 11. 2016.) *(Citirano na strani 16.)*

[27] *Abstract algebra*, https://en.wikipedia.org/wiki/Abstract_algebra. (Datum ogleda: 2. 6. 2016.) *(Citirano na strani 4.)*

[28] *Coset Product is Well-Defined*, https://proofwiki.org/wiki/Coset_Product_is_Well-Defined. (Datum ogleda: 24. 2. 2016.) *(Citirano na strani 20.)*

[29] *Group*, http://www.britannica.com/topic/group-mathematics. (Datum ogleda: 2. 6. 2016.) *(Citirano na strani 4.)*

[30] *Group theory*, https://en.wikipedia.org/wiki/Group_theory. (Datum ogleda: 2. 6. 2016.) *(Citirano na strani 4.)*

[31] *History and new possible research directions of hyperstructures*, http://www.math.uaic.ro/~leoreanu/saga/arhiva/chieti%207.pdf. (Datum ogleda: 6. 8. 2016.) *(Citirano na strani 68.)*

[32] *Relations*, http://www.people.vcu.edu/~rhammack/BookOfProof/Relations.pdf. (Datum ogleda: 31. 7. 2016.) *(Citirano na straneh 2 in 4.)*

[33] *Teorija grup*, https://sl.wikipedia.org/wiki/Teorija_grup. (Datum ogleda: 2. 6. 2016.) *(Citirano na straneh 4 in 20.)*

[34] *F1.3YR1 ABSTRACT ALGEBRA, Lecture Notes: Part 5*, http://www.macs.hw.ac.uk/~jim/F13YR1/notes5.pdf. (Datum ogleda: 7. 6. 2016.) *(Citirano na strani 24.)*

[35] *2. Groups I*,
http://www.math.umn.edu/∼garrett/m/algebra/notes/02.pdf. (Datum ogleda: 13. 11. 2016.) *(Citirano na strani 24.)*