6. kapitola

Algebraické štruktúry I – algebraické štruktúry, grupoidy, grupy, základné vlastnosti grupy, morfizmy

6.1 Binárne operácie

Jeden z častých prístupov v matematike je kombinovať prvky (elementy) množiny, pričom sa požadujú špeciálne vlastnosti kombinácie prvkov. Teória algebraických štruktúr študuje všeobecné vlastnosti takýchto systémov, ktoré obsahujú množinu prvkov, nad ktorou sú obvykle definované binárne operácie. Ako príklad takejto algebraickej štruktúry je množina celých čísel, nad ktorou je definovaná binárna operácia súčtu (alebo rozdielu, súčinu a pod.). Vo všeobecnosti môžeme povedať, že teória algebraických štruktúr obsahuje dve hlavné súčasti: množiny a pravidlá, pomocou ktorých sa z prvkov množín tvoria prvky taktiež z týchto množín.

Definícia 6.1. ***Binárna operácia*** na množine X je funkcia

$$f : X \times X \to X \tag{6.1a}$$

ktorá dvom prvkom $x, y \in X$ jednoznačne priradí prvok $z = x * y = f(x,y) \in X$

$$\forall x \forall y \exists! z \left(z = x * y = f(x,y) \right) \tag{6.1b}$$

Pozn.: zápis $\exists! x$ označuje, že existuje práve jeden prvok x, ktorý spĺňa dané podmienky.

Definícia 6.2. Usporiadaná dvojica $(X, *)$ obsahujúca množinu X a binárnu operáciu $*$ nad touto množinou tvorí najjednoduchšiu ***algebraickú štruktúru*** a často sa nazýva ***grupoid***.

Príklad 6.1.

(1) Algebraická štruktúra $(\mathbb{Z}, +)$ obsahuje množinu celých čísel $\mathbb{Z}$ a binárnu operáciu súčet nad touto množinou. Podobným spôsobom môžeme definovať ďalšie dve algebraické štruktúry $(\mathbb{Z}, -)$ a $(\mathbb{Z}, \times)$, ktoré sú založené na binárnych operáciách rozdiel resp. súčin.

(2) Nech $X = \mathcal{P}(A)$ je potenčná množina pre množinu A. Operácia zjednotenia a prieniku priradí dvom podmnožinám z A nejakú podmnožinu z A

$$\cup : \mathcal{P}(A) \times \mathcal{P}(A) \to \mathcal{P}(A)$$
$$\cap : \mathcal{P}(A) \times \mathcal{P}(A) \to \mathcal{P}(A)$$

Potom existujú dve jednoduché algebraické štruktúry $(X, \cup)$ a $(X, \cap)$.

Binárna operácia ´$*$´ môže byť špecifikovaná pomocou multiplikačnej tabuľky (ktorá sa v anglosaskej literatúre nazýva Caleyho tabuľka). Napríklad pre $X = \{a, b, c, d\}$ táto tabuľka môže mať tvar

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

Riadky a stĺpce tejto tabuľky sú označené prvkami množiny X, potom riadok označený prvkom x a stĺpec označený prvkom y obsahuje výsledok binárnej operácie $x * y$.

Definícia 6.3.
(1) Binárna operácia $*$ sa nazýva ***asociatívna*** na množine X vtedy a len vtedy, ak pre každé $x,y,z \in X$

$$(x * y) * z = x * (y * z) \tag{6.2a}$$

alebo

$$f(f(x,y),z) = f(x, f(y,z)) \tag{6.2b}$$

(2) Binárna operácia $*$ sa nazýva ***komutatívna*** na množine X vtedy a len vtedy, ak pre každé $x,y \in X$

$$x * y = y * x \tag{6.3a}$$

alebo

$$f(x,y) = f(y,x) \tag{6.3b}$$

(3) Prvok $e \in X$ sa nazýva ***neutrálny*** vzhľadom k binárnej operácii $*$ na množine X vtedy a len vtedy, ak pre každé $x \in X$

$$x * e = e * x = x \tag{6.4a}$$

(4) Prvok $y \in X$ sa nazýva ***inverzný*** vzhľadom k prvku $x \in X$ a k binárnej operácii $*$ na množine X vtedy a len vtedy, ak

$$y * x = x * y = e \tag{6.4b}$$

Inverzný prvok y často označujeme symbolom x^{-1}, aby sme zdôraznili jeho vzťah k prvku x.

V časti (3) tejto definície bol definovaný „neutrálny“ prvok. V prípade, že binárna operácia $*$ sa interpretuje ako súčin, potom neutrálny prvok sa nazýva „jednotkový“ prvok, ak je binárna operácia interpretovaná ako súčet, potom neutrálny prvok sa nazýva „nulový“ prvok.

Príklad 6.2.
(1) Pre algebraickú štruktúru $(\mathbb{Z},+)$ neutrálny prvok je nula, pre každé celé číslo $x \in \mathbb{Z}$ platí podmienka (6.4a)

$$0 + x = x + 0 = x$$

Pre dané celé číslo $x \in \mathbb{Z}$ existuje prvok $(-x) \in \mathbb{Z}$, ktorý spĺňa podmienku (6.4b)

$$(-x) + x = x + (-x) = 0$$

Alternatívne označenie pre tento inverzný prvok je $x^{-1} = (-x)$.

(2) Pre algebraickú štruktúru $(\mathbb{Z},\times)$ neutrálny prvok je číslo jedna, pre každé celé číslo $x \in \mathbb{Z}$ platí

$$x \times 1 = 1 \times x = x$$

Môžeme si položiť otázku, či každý prvok $x \in \mathbb{Z}$ má inverzný prvok. Napríklad, položme $x = 5$, potom inverzný prvok *y* vzhľadom k tomuto prvku je taký, čo vyhovuje podmienke

$$5 \times y = y \times 5 = 1$$

Táto podmienka nemá riešenie v množine celých čísel, $\neg\exists\left(y \in \mathbb{Z}\right)\left(5 \times y = y \times 5 = 1\right)$. Preto, v rámci algebraického systému $(\mathbb{Z},\times)$ nemá zmysel hovoriť o inverznom prvku vzhľadom k binárnej operácii ´súčin´.

(3) Študujme algebraickú štruktúru $\left(\mathcal{P}(A),\cap,\cup\right)$, definovanú pre potenčnú množinu s dvoma binárnymi operáciami ´prienik´ a ´zjednotenie´. Neutrálny a inverzný prvok pre tento algebraický systém musíme zaviesť separátne pre operáciu zjednotenia resp. prieniku. Každá z týchto operácií má svoj neutrálny prvok, pre každé $x \in \mathcal{P}(A)$

$$x \cap A = A \cap x = x$$
$$x \cup \varnothing = \varnothing \cup x = x$$

To znamená, že pre binárnu operáciu prieniku (zjednotenia) ako neutrálny prvok je množina *A* (prázdna množina $\varnothing$). Komplement $\overline{x} = A - x$ patrí do potenčnej množiny pre každé $x \in \mathcal{P}(A)$, $\forall\left(x \in \mathcal{P}(A)\right)\exists\left(y \in \mathcal{P}(A)\right)\left(y = \overline{x}\right)$. Takto definovaný komplement $\overline{x} = A - x$ nie je inverzný prvok vzhľadom k podmnožine $x \in \mathcal{P}(A)$

$$x \cap \overline{x} = \overline{x} \cap x = \varnothing$$
$$x \cup \overline{x} = \overline{x} \cup x = A$$

pretože na pravých stranách nemáme neutrálne prvky pre danú binárnu operáciu.

Veta 6.1. Nech $*$ je binárna operácia na množine *X*. Ak existuje neutrálny prvok $e \in X$, potom tento neutrálny prvok existuje jednoznačne.

Predpokladajme, že existujú dva neutrálne prvky $e_1, e_2 \in X$, potom súčasne platí

$$e_1 * e_2 = e_2 * e_1 = e_1$$
$$e_2 * e_1 = e_1 * e_2 = e_2,$$

preto musí platiť $e_1 = e_2$

Veta 6.2. Nech $*$ je asociatívna binárna operácia na množine *X*, ktorá má neutrálny prvok $e \in X$. Ak pre každý prvok $x \in X$ existuje inverzný prvok, $x * x^{-1} = x^{-1} * x = e$, potom tento inverzný prvok existuje jednoznačne.

Predpokladajme, že *x* má dva inverzné prvky *u* a *v*, potom podľa (6.4a) platí

$$x * u = u * x = e$$
$$x * v = v * x = e$$

Potom

$$u = u * e = u * \left(x * v\right) = \left(u * x\right) * v = e * v = v$$

Poznamenajme, že v dôkaze jednoznačnosti inverzného prvku kľúčovú úlohu hrala podmienka asociatívnosti súčinu $*$, ak tento súčin nie je asociatívny, potom nevieme zabezpečiť túto jednoznačnosť inverzného prvku.

Príklad 6.3. Budeme študovať binárnu operáciu $*$ nad množinou $X = \{a,b,c,d\}$, ktorá je určená multiplikačnú tabuľkou

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

Dokážeme, že takto definovaná binárna operácia nie je asociatívna.

$$b*(c*d)=b*d=a$$

$$(b*c)*d=a*d=d$$

to znamená, že pre tento konkrétny výber troch prvkov z množiny X sme dokázali

$$b*(c*d)\neq(b*c)*d$$

t. j. binárna operácia nie je asociatívna.

6.2 Pologrupy, monoidy a grupy

V tejto kapitole budeme študovať jednoduché algebraické štruktúry, ktoré obsahujú asociatívnu binárnu operáciu. Jedna z takýchto algebraických štruktúr je pologrupa.

Definícia 6.4. Nech G je neprázdna množina a $*$ je binárna operácia nad touto množinou. Algebraická štruktúra $(G,*)$ sa nazýva ***pologrupa*** vtedy a len vtedy, ak binárna operácia $*$ je asociatívna

$$(\forall x,y,z\in G)((x*y)*z=x*(y*z)) \tag{6.5}$$

Ak binárna operácia $*$ je aj komutatívna, potom algebraická štruktúra sa nazýva ***komutatívna pologrupa*** (alebo ***Abelova[1] pologrupa***).

Príklad 6.4.

(1) Algebraické štruktúry $(\mathbb{N},+)$, $(\mathbb{N},\times)$ sú komutatívne pologrupy. Binárne operácie súčtu a súčinu nad množnou celých čísel $\mathbb{N}$ sú asociatívne a komutatívne. Tieto dve algebraické štruktúry môžeme zovšeobecniť na množinu $\mathbb{R}$ reálnych čísiel, potom štruktúry $(\mathbb{R},+)$, $(\mathbb{R},\times)$ sú taktiež komutatívne pologrupy.

(2) Nech $A=\{a,b,c,...\}$ je konečná množina symbolov našej abecedy. Reťazce dĺžky n obsahujúce znaky tejto množiny tvoria n-násobný karteziánsky produkt A^n; napríklad množina $A^2=\{aa,ab,ac,...,ba,bb,bc,...\}$ obsahuje všetky reťazce dĺžky 2. Zjednotením týchto množín, $A^*=\{\varepsilon\}\cup A^1\cup A^2\cup...$, získame množinu, ktorá obsahuje všetky možné reťazce nad A, vrátane prázdneho reťazca ε. Nech $\alpha,\beta\in A^*$ sú dva reťazce, potom zavedieme binárnu operáciu „zreťazenia“, ktorá vytvorí nový reťazec $\gamma=(\alpha+\beta)\in A^*$. Príklad tejto operácie je spojenie reťazcov $\alpha=ab$ a $\beta=caa$ na nový reťazec $\gamma=\alpha+\beta=ab+caa=abcaa$. Táto

[1] Niels Henrik Abel (1802-1829), nórsky matematik, prispel k teórii algebraických rovníc a nekonečných číselných radov. Predčasne umrel na tuberkulózu, rok po jeho smrti mu parížska Akadémia udelila Veľkú cenu za matematiku.

binárna operácia je asociatívna a nekomutatívna ($\alpha+\beta\neq\beta+\alpha$, pre $\alpha\neq\beta$). Algebraická štruktúra $\left(A^*,+\right)$ je nekomutatívna pologrupa.

(3) Pre množinu $A=\{a,b,c\}$ definujme binárnu operáciu pomocou multiplikačnej tabuľky

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

Táto multiplikačná tabuľka je symetrická podľa hlavnej diagonály, z čoho plynie skutočnosť, že binárna operácia je komutatívna. Dôkaz asociatívnosti binárnej operácie je netriviálna záležitosť, pre všetky možné usporiadané trojice s opakovaním musíme dokázať, že platí zákon asociatívnosti

$$\forall\left(x,y,z\in A\right)\left(x*\left(y*z\right)=\left(x*y\right)*z\right)$$

čo vyžaduje $3^3 = 27$ kontrol pre rôzne trojice prvkov. Potom, algebraická štruktúra $\left(A,*\right)$ je komutatívna pologrupa.

Definícia 6.5. Pologrupa $\left(A,*\right)$ sa nazýva ***monoid*** vtedy a len vtedy, ak má neutrálny prvok.

Príklad 6.5.

(1) Algebraická štruktúra $\left(\mathbb{N}_+,\times\right)$, kde množina $\mathbb{N}_+$ obsahuje kladné celé čísla je monoid, existuje neutrálny (jednotkový) prvok ´1´, ktorý zachováva súčin $x*1=1*x=x$. Podobná algebraická štruktúra $\left(\mathbb{N}_+,+\right)$, ktorá je pologrupou, nie je monoid, pre operáciu súčet neexistuje v rámci množiny $\mathbb{N}_+$ neutrálny prvok ´0´ (pretože $0\notin\mathbb{N}_+$), ktorý zachováva súčet $x+0=0+x=x$.

(2) V príklade 6.4.2 bola popísaná nekomutatívna pologrupa $\left(A^*,+\right)$ reťazcov z množiny A^*, ktorá obsahuje všetky možné reťazce znakov nad abecedou A, pričom táto množina obsahuje aj prázdny znak ε. Binárna operácia je definovaná ako spojenie dvoch reťazcov do nového reťazca. Táto algebraická štruktúra má neutrálny prvok ε , ktorý je neutrálny vzhľadom k binárnej operácii spojenia reťazcov

$$\forall\left(x\in A^*\right)\left(\varepsilon+x=x+\varepsilon=x\right)$$

Preto, algebraická štruktúra $\left(A^*,+\right)$ je monoid.

(3) Algebraická štruktúra z príkladu 6.4.3 je monoid, neutrálny (jednotkový) prvok je prvok *a*, z multiplikačnej tabuľky vyplýva, že je neutrálny vzhľadom k zvolenej binárnej operácii

$$\forall\left(x\in A\right)\left(a*x=x*a=x\right)$$

(4) Uvažujme algebraické štruktúry $\left(X,\cup\right)$ a $\left(X,\cap\right)$ z príkladu 6.1.2, kde $X=\mathcal{P}\left(A\right)$ je potenčná množina pre množinu *A*. Obe tieto štruktúry sú pologrupy, pretože množinové operácie zjednotenia a prieniku sú asociatívne. Tieto štruktúry tvoria monoidy, pretože prvá (druhá) štruktúra má neutrálny prvok prázdnu množinu $\varnothing$ (množinu *A*)

$$\forall\left(X\in\mathcal{P}\left(A\right)\right)\left(\varnothing\cup X=X\cup\varnothing=X\right)$$

$$\forall\left(X\in\mathcal{P}\left(A\right)\right)\left(A\cap X=X\cap A=X\right)$$

Mnohé algebraické štruktúry, ktoré majú asociatívnu binárnu operáciu a neutrálny prvok vzhľadom k tejto operácii (t. j. monoidy), majú ešte dodatočnú vlastnosť, ku každému

prvku z množiny existuje inverzný prvok. Potom takýto monoid sa nazýva grupa. Algebraické štruktúry tohto typu našli široké uplatnenie nielen v mnohých oblastiach matematiky a informatiky, ale aj vo fyzike, chémii a pod.

Definícia 6.6. Monoid $(G,*)$ sa nazýva ***grupa*** vtedy a len vtedy, ak ku každému prvku $x \in G$ existuje inverzný prvok $x^{-1} \in G$. Platí teda, že algebraická štruktúra $(G,*)$ je ***grupa*** vtedy a len vtedy, ak sú splnené tieto tri podmienky:

(1) binárna operácia $*$ je asociatívna,
(2) existuje neutrálny prvok $e \in G$,
(3) pre každé $x \in G$ existuje inverzný prvok $x^{-1} \in G$.

Mohutnosť množiny *G* sa nazýva rád grupy $(G,*)$, označuje sa $|G|$.

Pripomeňme, podľa vety 6.1 platí, že ak existuje neutrálny prvok, potom tento neutrálny prvok je určený jednoznačne; podobne, podľa vety 6.2 ak má algebraická štruktúra asociatívnu binárnu operáciu a neutrálny prvok, platí, že ak existuje ku každému prvku inverzný prvok, potom je určený jednoznačne. Obe tieto skutočnosti sú platné pre algebraickú štruktúru grupa, kde sa postuluje existencia neutrálneho prvku a inverzného prvku.

Príklad 6.6.

(1) Algebraická štruktúra $(\mathbb{Z},+)$, kde $\mathbb{Z}$ je množina celých čísel, je komutatívna grupa. Binárna operácia súčet ´+´ je asociatívna a komutatívna, číslo $0 \in \mathbb{Z}$ má charakter neutrálneho prvku vzhľadom k operácii ´+´, $0+x=x+0=x$, pre každé číslo *x*; podobne, pre každé číslo $x \in \mathbb{Z}$ existuje ´inverzné´ číslo $(-x) \in \mathbb{Z}$ také, že $(-x)+x=x+(-x)=0$.

(2) Nech algebraická štruktúra $(\mathbb{R}_+,\times)$, kde $\mathbb{R}_+ = (0,\infty)$ je množina kladných reálnych čísel, používa ako binárnu operáciu štandardný súčin. Táto algebraická štruktúra je komutatívna grupa, binárna operácia je asociatívna a komutatívna, existuje neutrálny prvok $1 \in \mathbb{R}_+$, $1 \times x = x \times 1 = x$, pre každý prvok *x*, a taktiež ku každému *x* existuje inverzný prvok $x^{-1} = 1/x$, pre ktorý platí $x \times (1/x) = (1/x) \times x = 1$.

(3) Nech algebraická štruktúra $(\mathbb{Z},*)$ má binárnu operáciu definovanú vzťahom

$$x * y = x + y + 1$$

Dokážte, že táto štruktúra je grupa.

Binárna operácia $*$ je komutatívna. Dôkaz jej asociatívnosti je založený na podmienke, aby pre ľubovoľné $x,y,z \in \mathbb{Z}$ bola splnená rovnosť týchto dvoch formúl

$$(x*y)*z = (x+y+1)*z = x+y+1+z+1 = x+y+z+2$$
$$x*(y*z) = x*(y+z+1) = x+y+z+1+1 = x+y+z+2$$

Porovnaním ich pravých strán dostaneme, že binárna operácia $*$ je asociatívna na množine $\mathbb{Z}$.

Neutrálny prvok $e \in \mathbb{Z}$ vyhovuje definičnej podmienke

$$e*x = x*e = x \Rightarrow e+x+1 = x \Rightarrow e = -1$$

pre každé $x \in \mathbb{Z}$. To znamená, že prvok $(-1) \in \mathbb{Z}$ pôsobí ako neutrálny prvok na množine $\mathbb{Z}$, pre každé $x \in \mathbb{Z}$ platí $(-1)*x = x*(-1) = x$. Na záver, zostrojíme pre každé $x \in \mathbb{Z}$ inverzný prvok $x^{-1} \in \mathbb{Z}$,

$$x * x^{-1} = x + x^{-1} + 1 = -1 \Rightarrow x^{-1} = -2 - x$$

Potom, pre každé $x \in \mathbb{Z}$ existuje inverzný prvok $x^{-1} = (-2 - x) \in \mathbb{Z}$, ktorý vyhovuje podmienke $x * x^{-1} = x^{-1} * x = e = -1$. Týmto sme dokázali, že algebraická štruktúra $(\mathbb{Z}, *)$ tvorí komutatívnu grupu.

Veta 6.3. Ak algebraická štruktúra $(G, *)$ je grupa, potom existuje „krátenie“ zľava a sprava, pre každé $a, x, y \in G$ platí

(a) krátenie zľava

$$a * x = a * y \Rightarrow x = y \tag{6.6a}$$

(b) krátenie sprava

$$x * a = y * a \Rightarrow x = y\,. \tag{6.6b}$$

Predpokladajme, že platí $a * x = a * y$, existuje inverzný prvok a^{-1}, potom $a^{-1} * (a * x) = a^{-1} * (a * y) \Rightarrow (a^{-1} * a) * x = (a^{-1} * a) * y \Rightarrow x = y$. Podobne by sme dokázali aj krátenie sprava. Táto veta podstatne uľahčuje algebraické úpravy v teórii grúp, môžeme jednoducho krátiť prvky vo výrazoch, ktoré sa vyskytujú zľava alebo sprava.

Veta 6.4. Ak algebraická štruktúra $(G, *)$ je grupa, potom pre ľubovolné $a, b \in G$ platí

(a) rovnica $a * x = b$ má jednoznačné riešenie $x = a^{-1} * b$,
(b) rovnica $x * a = b$ má jednoznačné riešenie $x = b * a^{-1}$.

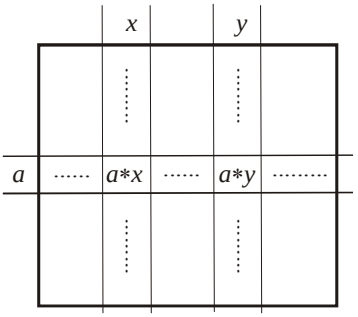
Nech platí $a * x = b$, postupnými úpravami dostaneme

$$a * x = b \Rightarrow a^{-1} * (a * x) = a^{-1} * b \Rightarrow (a^{-1} * a) * x = a^{-1} * b \Rightarrow x = a^{-1} * b$$

Jednoznačnosť tohto riešenia vyplýva zo skutočnosti, že inverzný prvok a^{-1} existuje jednoznačne. Podobným spôsobom získame riešenie aj druhej rovnice.

Veta 6.5. Ak algebraická štruktúra $(G, *)$ je grupa, potom v multiplikačnej tabuľke binárnej operácie $*$ sa v každom riadku alebo stĺpci vyskytuje každý prvok z G práve len raz.

V multiplikačnej tabuľke si vyberme jeden riadok a dva rôzne stĺpce (pozri obr. 6.1). Predpokladajme, že $a * x = a * y$, použijeme vetu 6.3 o krátení, potom predpoklad môžeme zjednodušiť do tvaru $x = y$, čo je však v spore, že stĺpce sú rôzne. Týmto sme dokázali, že v každom riadku multiplikačnej tabuľky sa nemôžu opakovať prvky grupy. Dôkaz pre stĺpce je podobný.



Obrázok 6.1. Multiplikačná tabuľka binárnej operácie $*$ grupy $(G,*)$. V tabuľke je vybraný riadok patriaci prvku a a dva stĺpce patriace prvkom x a y, pričom $x \neq y$.

Z tejto vety vyplýva jednoduché kritérium toho, či algebraická štruktúra $(G,*)$ je grupa, ak v príslušnej multiplikačnej tabuľke sa v nejakom riadku alebo stĺpci opakujú prvky, potom štruktúra $(G,*)$ nie je grupa. Poznamenajme však, skutočnosť, že v tabuľke v každom stĺpci alebo riadku sa neopakujú prvky, nie je postačujúcim dôvodom k tomu, aby štruktúra $(G,*)$ bola grupou.

Definícia 6.7. Hovoríme, že algebraická štruktúra $(H,*)$ je ***podgrupa*** grupy $(G,*)$ vtedy a len vtedy, ak $H \subseteq G$ a $(H,*)$ je grupa, čo budeme zapisovať $(H,*) \subseteq (G,*)$.

Poznamenajme, že ak $(H,*) \subseteq (G,*)$, potom obe štruktúry sú grupy a obe binárne operácie sú rovnaké. Každá grupa má aspoň dve triviálne podgrupy. Prvá je s množinou $H = \{e\}$ a druhá s množinou $H = G$, všetky ostatné podgrupy (ak existujú) nazývame netriviálne.

Veta 6.6 (Lagrangeova). Nech $(H,*) \subseteq (G,*)$, potom rád množiny $|G|$ je deliteľný rádom podmnožiny $|H|$, teda existuje také kladné celé číslo *k*, že $|G| = k|H|$

$$\big((H,*) \subseteq (G,*)\big) \Rightarrow \exists k\big(|G| = k|H|\big) \tag{6.7}$$

Nebudeme dokazovať túto vetu, jej dôkaz vyžaduje mnoho ďalších pomocných pojmov, čo presahuje rámec tejto príručky. Je zaujímavá tým, že nám poskytuje jednoduché kritérium toho, či nejaká podmnožina *H* môže tvoriť podgrupu, ako vyplýva z vety podiel $|G|/|H|$ musí byť kladné celé číslo; ak nie je, potom *H* nemôže tvoriť podgrupu grupy $(G,*)$.

Nasledujúca veta rieši problém ako efektívne verifikovať, či grupa $(H,*)$ je podgrupa grupy $(G,*)$.

Veta 6.7. Nech algebraická štruktúra $(G,*)$ je grupa a nech $H \subseteq G$ je konečná podmnožina. Algebraická štruktúra $(H,*)$ je podgrupou vtedy a len vtedy, ak $\forall (x,y \in H)(x * y \in H)$, t. j. podmnožina H je uzavretá vzhľadom k binárnej operácii $*$.

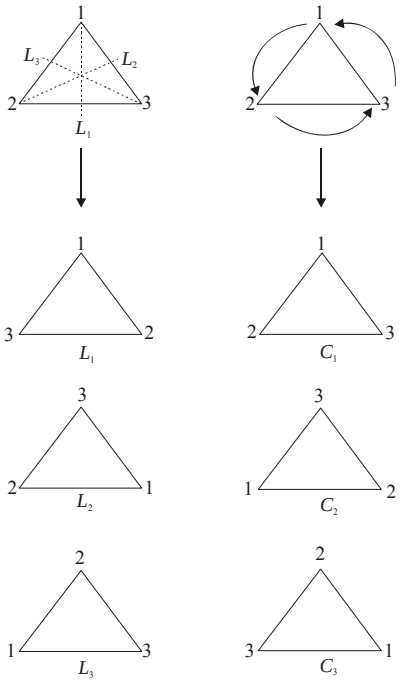
Dôkaz tejto vety spočíva v tom, že vychádzajúc z jej predpokladov ukážeme, že pre každý prvok množiny H existuje v tejto množine aj jeho inverzný prvok. Nech $x \in H$, potom v dôsledku uzavretosti H vzhľadom k operácii $*$ platí $x^n \in H$, pre každé kladné číslo *n*. Pretože mohutnosť *H* je konečná, v mocninách x^n sa musia opakovať členy. Nech pre $r > s$ platí $x^r = x^s$, alebo $x^s x^{r-s} = x^s$. Použijeme zákon krátenia zľava (veta 6.3), dostaneme

$$x^{r-s} = e$$

Týmto sme dokázali, že množina *H* obsahuje neutrálny prvok. Taktiež platí

$$x * x^{r-s-1} = x^{r-s} = e$$

potom prvok *x* má inverzný prvok x^{r-s-1}, Týmto sme dokázali, že pre každý prvok $x \in H$ existuje inverzný prvok v *H*.



Obrázok 6.2. Prvky symetrie rovnostranného trojuholníka, ktorého vrcholy sú označené číslicami 1, 2 a 3. V ľavom stĺpci sú uvedené tri operácie symetrie L_1, L_2 a L_3 spočívajúce v zrkadlení podľa uvedených priamok, ktoré prechádzajú vrcholom a polia protiľahlú stranu. V pravom stĺpci sú uvedené tri operácie symetrie C_1, C_2 a C_3, ktoré spočívajú v rotácii trojuholníka okolo ťažiska proti smeru hodinových ručičiek o 0° stupňov, 120° stupňov a 240° stupňov.

Príklad 6.7. Zavedieme grupu obsahujúce geometrické transformácie rovnostranného trojuholníka, ktorá sa nazýva dihedrálna grupa. V chémii je veľmi populárna, popisuje symetrické vlastnosti niektorých molekúl.

Uvažujme rovnostranný trojuholník, ktorého vrcholy sú označené číslicami 1, 2 a 3, pozri obr. 6.2. Množina prvkov obsahuje 6 operácií symetrie, z ktorých tri sú reflexie L_1, L_2, L_3 a rotácie C_1, C_2, C_3 . Ak základnú pozíciu trojuholníka vyjadríme pomocou postupnosti (123), potom aplikácie operácií symetrie na túto postupnosť špecifikujú výsledný transformovaný trojuholník

$$L_1(123)=(132), L_2(123)=(321), L_3(123)=(213),$$
$$C_1(123)=(123), C_2(123)=(312), C_3(123)=(231)$$

Potom môžeme zostrojiť multiplikačnú tabuľku

*	C_1	C_2	C_3	L_1	L_2	L_3
C_1	C_1	C_2	C_3	L_1	L_2	L_3
C_2	C_2	C_3	C_1	L_3	L_1	L_2
C_3	C_3	C_1	C_2	L_2	L_3	L_1
L_1	L_1	L_2	L_3	C_1	C_2	C_3
L_2	L_2	L_3	L_1	C_3	C_1	C_2
L_3	L_3	L_1	L_2	C_2	C_3	C_1

Z multiplikačnej tabuľky plynie, že táto množina operácií má prvok C_1, ktorý môžeme klasifikovať ako neutrálny. Z multiplikačnej tabuľky taktiež zistíme, či pre každú operáciu symetrie existuje inverzný prvok

$$C_1^{-1} = C_1, C_2^{-1} = C_3, C_3^{-1} = C_2$$
$$L_1^{-1} = L_1,\ L_2^{-1} = L_2,\ L_3^{-1} = L_3$$

Podobným spôsobom môžeme dokázať, že binárna operácia súčinu týchto operácií symetrie je asociatívna. Potom, algebraická štruktúra $\left(D_3 = \{L_1, L_2, L_3, C_1, C_2, C_3\}, *\right)$ je grupa.

Grupa permutácií

Ukážeme, že množina permutácií *n* objektov reprezentovaných množnou $A = \{1,2,...,n\}$ pri vhodnej definícii binárnej operácie $*$ tvorí ***symetrickú grupu*** $\left(S_n = \{P_1, P_2, ...\}, *\right)$, kde S_n je množina tvorená všetkými permutáciami *n* objektov. Permutácie boli už špecifikované v kapitole 4.2. Permutáciu *P* môžeme chápať ako bijektívne zobrazenie $P: A \to A$, ktoré každému objektu $i \in A$ priradí objekt $p_i \in A$, pričom z podmienky bijektívnosti vyplýva podmienka $\forall (i, j \in A)\left(i \neq j \Rightarrow p_i \neq p_j\right)$. Permutáciu *P* vyjadríme formulou

$$P = \begin{pmatrix} 1 & 2 & ... & n \\ p_1 & p_2 & ... & p_n \end{pmatrix}$$

alebo v kompaktnej forme tak, že vynecháme horný riadok ako redundantný

$$P = \begin{pmatrix} p_1 & p_2 & ... & p_n \end{pmatrix}$$

Množina S_n obsahuje všetky možné permutácie *n* objektov, jej mohutnosť je $|S_n| = n!$

Binárna operácia $*$ zobrazuje z dvoch permutácií novú permutáciu

$$*: S_n \times S_n \to S_n$$

Nech $P = \begin{pmatrix} 1 & 2 & ... & n \\ p_1 & p_2 & ... & p_n \end{pmatrix}$ a $P' = \begin{pmatrix} 1 & 2 & ... & n \\ p_1' & p_2' & ... & p_n' \end{pmatrix}$ sú dve permutácie, ich súčin $P'' = P * P'$ je definovaný tak, že ak horný riadok v P' preusporiadame tak, aby bol totožný s dolným riadkom permutácie *P*, potom dolný riadok takto upravenej permutácie špecifikuje permutáciu P''

$$P'' = P * P' = \begin{pmatrix} 1 & 2 & ... & n \\ p_1 & p_2 & ... & p_n \end{pmatrix} * \begin{pmatrix} 1 & 2 & ... & n \\ p_1' & p_2' & ... & p_n' \end{pmatrix}$$
$$= \begin{pmatrix} 1 & 2 & ... & n \\ p_1 & p_2 & ... & p_n \end{pmatrix} * \begin{pmatrix} p_1 & p_2 & ... & p_n \\ p_1'' & p_2'' & ... & p_n'' \end{pmatrix}$$
$$= \begin{pmatrix} 1 & 2 & ... & n \\ p_1'' & p_2'' & ... & p_n'' \end{pmatrix}$$

Príklad takto definovaného súčinu permutácií je ukázaný na obr. 6.3. Súčin dvoch permutácií môžeme interpretovať ako kompozíciu dvoch zobrazení *P* a *P´*.

Súčin dvoch permutácií musí byť asociatívnou operáciou, pre súčin ľubovolných troch permutácií P_1, P_2, P_3 platí

$$P_1 * (P_2 * P_3) = (P_1 * P_2) * P_3$$

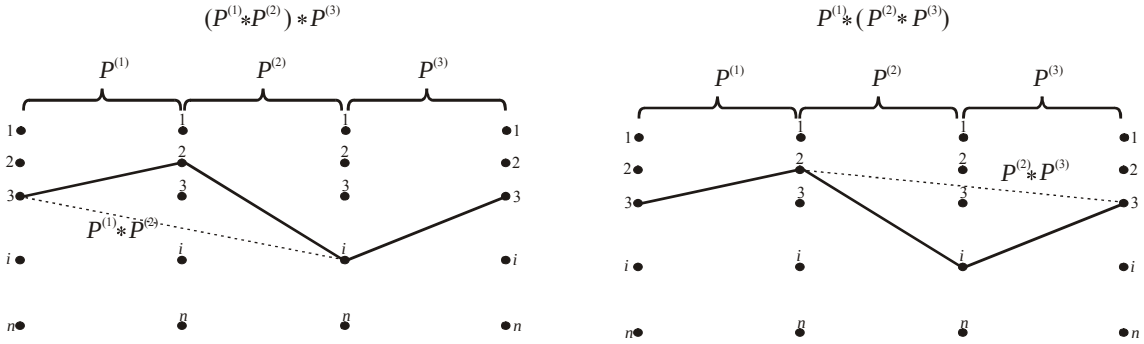
Ľahko sa presvedčíme pomocou obrázka 6.4, že táto podmienka je splnená. Problém existencie inverznej permutácie je riešiteľný jednoduchou „inverziou“

$$P=\begin{pmatrix}1 & 2 & \dots & n\\ p_1 & p_2 & \dots & p_n\end{pmatrix}\Rightarrow P^{-1}=\begin{pmatrix}p_1 & p_2 & \dots & p_n\\ 1 & 2 & \dots & n\end{pmatrix}$$

$$\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}*\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$$

$$\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}*\begin{pmatrix}3&2&1\\3&1&2\end{pmatrix}=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$$

Obrázok 6.3. Znázornenie súčinu dvoch permutácií $(3\ \ 2\ \ 1)*(2\ \ 1\ \ 3)$. Dolný riadok ilustruje alternatívnu možnosť konštrukcie súčinu permutácií tak, že horný riadok pravej permutácie upravíme do poradia špecifikovaného druhým riadkom prvej permutácie. Dolný riadok takto upravenej permutácie reprezentuje výsledok súčinu.



Obrázok 6.4. Dôkaz asociatívnosti binárnej operácie súčinu nad permutáciami. Ľavý (pravý) diagram znázorňuje zátvorkovanie $(P_1*P_2)*P_3$, kde výsledok prvého súčinu je reprezentovaný prerušovanou čiarou ($P_1*(P_2*P_3)$, kde výsledok druhého súčinu je reprezentovaný prerušovanou čiarou). V oboch prípadoch, výsledné zložené zobrazenie je totožné.

Príklad 6.8. Zostrojte multiplikačnú tabuľku permutácií troch objektov. Jednotlivé permutácie označíme takto

$$P_1=(123),\ P_2=(231),\ P_3=(312),$$
$$P_4=(132),\ P_5=(321),\ P_6=(213)$$

Potom multiplikačná tabuľka pre tieto permutácie má tvar

$*$	P_1	P_2	P_3	P_4	P_5	P_6
P_1	P_1	P_2	P_3	P_4	P_5	P_6
P_2	P_2	P_3	P_1	P_5	P_6	P_4
P_3	P_3	P_1	P_2	P_6	P_4	P_5
P_4	P_4	P_6	P_5	P_1	P_3	P_2
P_5	P_5	P_4	P_6	P_2	P_1	P_3
P_6	P_6	P_5	P_4	P_3	P_2	P_1

Z tejto tabuľky vyplýva, že neutrálny prvok je permutácia P_1, inverzné permutácie sú určené takto

$$P_1^{-1}=P_1, P_2^{-1}=P_3, P_3^{-1}=P_2, P_4^{-1}=P_4, P_5^{-1}=P_5, P_6^{-1}=P_6$$

Potom podmnožina $S_3'=\{P_1,P_2,P_3\}\subset S_3$ tvorí podgrupu $(S_3',*)\subseteq(S_3,*)$.

6.3 Morfizmy

Porovnajme grupy z príkladov 6.7 a 6.8, ktoré majú úplne odlišnú interpretáciu, prvá grupa obsahuje prvky symetrie priestorovej dihedrálnej grupy, zatiaľ čo druhá grupa obsahuje permutácie 3 objektov. Ich multiplikačné tabuľky majú tvar

$*$	C_1	C_2	C_3	L_1	L_2	L_3
C_1	C_1	C_2	C_3	L_1	L_2	L_3
C_2	C_2	C_3	C_1	L_3	L_1	L_2
C_3	C_3	C_1	C_2	L_2	L_3	L_1
L_1	L_1	L_2	L_3	C_1	C_2	C_3
L_2	L_2	L_3	L_1	C_3	C_1	C_2
L_3	L_3	L_1	L_2	C_2	C_3	C_1

$*$	P_1	P_2	P_3	P_4	P_5	P_6
P_1	P_1	P_2	P_3	P_4	P_5	P_6
P_2	P_2	P_3	P_1	P_5	P_6	P_4
P_3	P_3	P_1	P_2	P_6	P_4	P_5
P_4	P_4	P_6	P_5	P_1	P_3	P_2
P_5	P_5	P_4	P_6	P_2	P_1	P_3
P_6	P_6	P_5	P_4	P_3	P_2	P_1

Podrobným porovnaním týchto tabuliek zistíme, že ak medzi tabuľkami urobíme priradenie jednotlivých prvkov takto

$$C_1\leftrightarrow P_1, C_2\leftrightarrow P_3, C_3\leftrightarrow P_2, L_1\leftrightarrow P_4, L_2\leftrightarrow P_5, L_3\leftrightarrow P_6$$

potom multiplikačné tabuľky sú totožné. Preto môžeme povedať, že aj grupy $(D_3,*)$ a $(S_3,*)$ sú si podobné.

Definícia 6.8. Hovoríme, že medzi grupami $(G,*)$ a $(G',\circ)$ existuje ***izomorfimus*** (alebo, že grupy sú ***izomorfné***), čo značíme $(G,*)\cong(G',\circ)$, vtedy a len vtedy, ak existuje bijekcia $f:G\to G'$, ktoré

$$\forall(x,y\in G)\big(f(x*y)=f(x)\circ f(y)\big) \tag{6.8}$$

Príklad 6.9. Uvažujme dve grupy $(\mathbb{R},+)$ a grupu $(\mathbb{R}_+,\times)$, kde $\mathbb{R}_+=(0,\infty)$ je množina kladných reálnych čísel. Dokážte, že funkcia $f(x)=2^x$ definuje izomorfizmus medzi týmito dvoma grupami, $(\mathbb{R},+)\cong(\mathbb{R}_+,\times)$.

Funkcia $f(x)=2^x$ je rýdzo rastúca, čiže je aj 1-1-značná. Funkcia má zaujímavú vlastnosť, $(\forall x,y\in\mathbb{R})\,f(x+y)=f(x)\cdot f(y)$, pomocou ktorej sa jednoducho zostrojí izomorfizmus medzi grupami, $f:\mathbb{R}\to\mathbb{R}_+$.

Veta 6.8. Ak $f:G\to G'$ je izomorfizmus medzi grupami $(G,*)$ a $(G',\circ)$, potom

(1) Ak e je neutrálny prvok v grupe $(G,*)$, potom $f(e)$ je neutrálny prvok v grupe $(G',\circ)$.

(2) Grupa $(G,*)$ je komutatívna vtedy a len vtedy, ak $(G',\circ)$ je komutatívna grupa.

(3) Ak x^{-1} je inverzný prvok vzhľadom k prvku x v grupe $(G,*)$, potom $f(x^{-1})$ je inverzný prvok vzhľadom k prvku $f(x)$ v grupe $(G',\circ)$.

(4) Inverzné zobrazenie $f^{-1}:G'\to G$ definuje izomorfizmus z grupy $(G',\circ)$ do grupy $(G,*)$.

(5) Ak $(H,*)$ je podgrupa grupy $(G,*)$, potom $(H',\circ)$, kde $H'=\{f(x);x\in H\}$, je podgrupa grupy $(G',\circ)$ a $(H,*)\cong(H',\circ)$.

Táto veta nám pomáha zistiť, či medzi grupami $(G,*)$ a $(G',\circ)$ existuje izomorfizmus. Napríklad, ak grupa $(G,*)$ je komutatívna a grupa $(G',\circ)$ nie je komutatívna, potom medzi týmito grupami nemôže existovať izomorfizmus. Vo všeobecnosti teda platí, že ak chceme zistiť, že dve grupy nie sú izomorfné, musíme nájsť takú vlastnosť prvej grupy, ktorá sa nevyskytuje v druhej grupe.

Príklad 6.10. Dokážte, že ak $A=\{a,b\}$, potom monoidy $(\mathcal{P}(A),\cup)$ a $(\mathcal{P}(A),\cap)$ sú izomorfné.
Potenčná množina má tvar $\mathcal{P}(A)=\{\varnothing,\{a\},\{b\},\{a,b\}\}$. Multiplikatívne tabuľky pre tieto monoidy majú tvar

$\cup$	$\varnothing$	$\{a\}$	$\{b\}$	$\{a,b\}$
$\varnothing$	$\varnothing$	$\{a\}$	$\{b\}$	$\{a,b\}$
$\{a\}$	$\{a\}$	$\{a\}$	$\{a,b\}$	$\{a,b\}$
$\{b\}$	$\{b\}$	$\{a,b\}$	$\{b\}$	$\{a,b\}$
$\{a,b\}$	$\{a,b\}$	$\{a,b\}$	$\{a,b\}$	$\{a,b\}$

$\cap$	$\varnothing$	$\{a\}$	$\{b\}$	$\{a,b\}$
$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$
$\{a\}$	$\varnothing$	$\{a\}$	$\varnothing$	$\{a\}$
$\{b\}$	$\varnothing$	$\varnothing$	$\{b\}$	$\{b\}$
$\{a,b\}$	$\varnothing$	$\{a\}$	$\{b\}$	$\{a,b\}$

1-1-značná funkcia $f:\mathcal{P}(A)\to\mathcal{P}(A)$, ktorá zobrazuje prvú tabuľku na druhú má tvar

$$f(\varnothing)=\{a,b\},\ f(\{a\})=\{a\},\ f(\{b\})=\{b\},\ f(\{a,b\})=\varnothing$$

Potom medzi monoidami $(\mathcal{P}(A),\cup)$ a $(\mathcal{P}(A),\cap)$ existuje izomorfizmus.

Definícia 6.9. Hovoríme, že medzi algebraickými štruktúrami $(G,*)$ a $(G',\circ)$ existuje ***homomorfizmus*** vtedy a len vtedy, ak existuje zobrazenie $f:G\to G'$, ktoré zachováva relevantné vlastnosti štruktúry, ako neutrálne a inverzné prvky, a pre binárne operácie platí

$$\forall(x,y\in G)\big(f(x*y)=f(x)\circ f(y)\big) \tag{6.9}$$

Ak medzi dvoma algebraickými štruktúrami existuje izomorfizmus, potom tieto štruktúry sú „skoro totožné“. Ak odstránime podmienku bijektívnosti funkcie $f:G\to G'$, potom táto „skoro totožnosť“ sa stráca, druhá algebraická štruktúra $(G',\circ)$ už nemusí mať všetky detaily prvej štruktúry.

Príklad 6.11. Uvažujme množinu $A=\{a,b,c\}$, množina A^* obsahuje všetky možné reťazce (vrátane prázdneho reťazca ε). Potom algebraická štruktúra $(A^*,*)$, kde binárna operácia $*$ reprezentuje spájanie reťazcov, je monoid (existuje neutrálny prvok reprezentovaný prázdnym reťazcom ε). Nech existuje funkcia $f:A^*\to\mathbb{N}$, kde $\mathbb{N}$ je množina nezáporných celých čísel, táto funkcia je definovaná takto

$$f(x)=\text{dĺžka reťazca } x$$

Ukážte, že toto zobrazenie f je homomorfizmus z $(A^*,*)$ na $(\mathbb{N},+)$.

Z definície funkcie f vyplýva, že platí

$$f(x*y)=f(x)+f(y)$$

t. j. dĺžka spojeného reťazca $x*y$ sa rovná súčtu dĺžok jeho zložiek x a y. Táto funkcia evidentne nie je bijekcia.

Cvičenia

Cvičenie 6.1. Pre každý uvedený prípad rozhodnite, či symbol $x*y$ špecifikuje binárnu operáciu na množine A. Ak nie, tak vysvetlite prečo.

(a) $x*y=x-y$, $A=\mathbb{R}_+=(0,\infty)$.

(b) $x*y=z$, kde $z=x+y$, pre $A=\mathbb{Z}=\{...,-2,-1,0,1,2,...\}$.

(c) $x*y=x^y$, $A=\mathbb{R}_+=(0,\infty)$.

(d) $x*y=$ maximálny spoločný deliteľ x a y, $A=\{1,2,3,4,6,8,24\}$.

Cvičenie 6.2. Nech binárna operácia na množine $\mathbb{R}$ obsahujúcej reálne čísla, je definovaná ako rozdiel, $x*y=x-y$. Rozhodnite, či táto operácia je

(a) asociatívna,
(b) komutatívna,
(c) existuje neutrálny prvok.

Cvičenie 6.3. Nech A je konečná množina a nech pre túto množinu A je binárna operácia definovaná pomocou multiplikačnej tabuľky. Na základe čoho je možné rozhodnúť pomocou tejto tabuľky, či

(a) binárna operácia je komutatívna,
(b) existuje neutrálny prvok.

Cvičenie 6.4. Nech $X=\mathcal{P}(A)$, binárna operácia nad touto množinou je definovaná ako prienik množín, $(\forall x,y\in\mathcal{P}(A))(x*y=x\cap y)$, rozhodnite, či

(a) binárna operácia je komutatívna,
(b) čo je neutrálny prvok,
(c) ktoré prvky majú inverzné prvky (ak existujú)?

Cvičenie 6.5. Nech $X=\mathcal{P}(A)$, binárna operácia nad touto množinou je definovaná ako symetrický rozdiel $(\forall x,y\in\mathcal{P}(A))(x*y=(x-y)\cup(y-x))$. Použite Vennove diagramy na odôvodnenie odpovedí na nasledujúce otázky

(a) Je operácia $*$ binárna operácia?
(b) Je táto operácia komutatívna?
(c) Je táto operácia asociatívna?
(d) Existuje neutrálny prvok v množine X ?

(e) Ak existuje neutrálny prvok, existuje potom ku každému prvku $x \in \mathcal{P}(A)$ inverzný prvok $x^{-1} \in \mathcal{P}(A)$?

Cvičenie 6.6. Nech množina $X = \{a,b,c,d\}$, binárna operácia pre túto množinu je definovaná pomocou multiplikačnej tabuľky

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

(a) Je táto operácia asociatívna?
(b) Je táto operácia komutatívna?

Cvičenie 6.7. Nech X je neprázdna množina a binárna operácia definovaná vzťahom $x * y = x$, pre každé $x,y \in X$.

(a) Dokážte, že algebraická štruktúra $(X,*)$ je pologrupa.

(b) Rozhodnite, či táto algebraická štruktúra je monoid.

Cvičenie 6.8. Nech dve algebraické štruktúry $(X,*)$ a $(Y,\circ)$ sú grupy. Definujte nad karteziánskym súčinom $X \times Y$ binárnu operáciu takto

$$(x_1,y_1)\bullet(x_2,y_2) = (x_1 * x_2, y_1 \circ y_2)$$

pre každé $x_1,x_2 \in X$ a $y_1,y_2 \in Y$.

(a) Ukážte, že $\bullet$ je binárna operácia na $X \times Y$.
(b) Ako je definovaný neutrálny prvok na $X \times Y$?
(c) Ako je definovaný inverzný prvok $(x,y)^{-1}$?
(d) Dokážte, že algebraická štruktúra $(X \times Y,\bullet)$ je grupa.

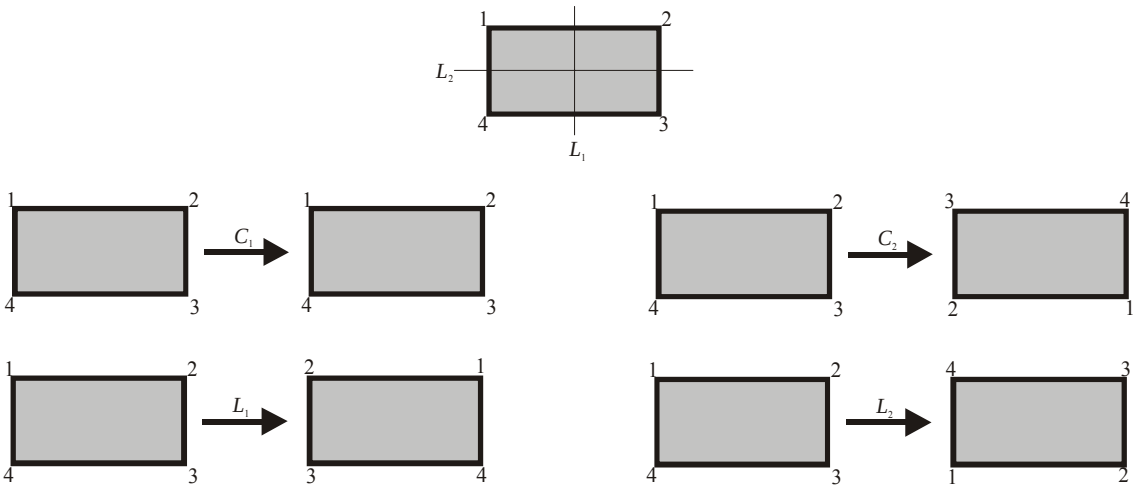
Cvičenie 6.9. Nech $(\mathbb{N},*)$ je algebraická štruktúra, kde $\mathbb{N}$ je množina obsahujúca nezáporné celé čísla. Binárna operácia je definovaná takto

$$x * y = max\{x,y\}$$

(a) Dokážte, že algebraická štruktúra $(\mathbb{N},*)$ je pologrupa.

(b) Rozhodnite, či $(\mathbb{N},*)$ je monoid.

Cvičenie 6.10. Uvažujme neštvorcový obdĺžnik, ktorého vrcholy sú označené číslicami 1, 2, 3 a 4.



Tento obdĺžnik má štyri operácie symetrie

C_1 : rotácia o 0° stupňov okolo stredu obdĺžnika,
C_2 : rotácia o 180° stupňov okolo stredu obdĺžnika,
L_1 : reflexia priamkou L_1 a
L_2 : reflexia priamkou L_2.

Pre lepšie pochopenie týchto prvkov symetrie ich budeme špecifikovať ich aplikáciou na postupnosť (1,2,3,4)

$$C_1(1,2,3,4) = (1,2,3,4)$$
$$C_2(1,2,3,4) = (3,4,1,2)$$
$$L_1(1,2,3,4) = (2,1,4,3)$$
$$L_2(1,2,3,4) = (4,3,2,1)$$

Pre takto definované prvky zostrojte ich kompozíciu (binárnu operáciu), napríklad

$$C_2 * L_1(1,2,3,4) = C_2(L_1(1,2,3,4)) = C_2(2,1,4,3) = (4,3,2,1) = L_2$$

(a) Zostavte multiplikačnú tabuľku pre kompozíciu dvoch operácií symetrie.
(b) Dokážte, že algebraická štruktúra $(A = \{C_1, C_2, L_1, L_2\}, *)$ je grupa.

Cvičenie 6.11. Pred riešením tohto príkladu je potrebné dodefinovať pojem „podmonoid“ v duchu teórie grúp. Nech algebraická štruktúra $(X, *)$ je monoid, potom ak pre neprázdnu podmnožinu $X' \subseteq X$ algebraická štruktúra $(X', *)$ je taktiež monoid, hovoríme, že $(X', *)$je podmonoid, $(X', *) \subseteq (X, *)$. Nech $(X, *)$ je komutatívny monoid. Ukážte, že množina idempotentných prvkov $X' = \{x; (x \in X) \wedge (x * x = x)\}$ tvorí algebraickú štruktúru $(X', *)$, ktorá je podmonoid.

Cvičenie 6.12. Nech algebraická štruktúra $(X, *)$ je grupa. Stred tejto štruktúry je definovaný ako podmnožina X, ktorá obsahuje prvky komutujúce so všetkými prvkami X, $X_{centre} = \{x; (x \in X) \wedge (\forall y (x * y = y * x))\}$. Dokážte, že algebraická štruktúra $(X_{center}, *)$ je podgrupa grupy $(X, *)$, $(X_{center}, *) \subseteq (X, *)$.