5. kapitola

Algebraické štruktúry I –algebraické štruktúry, grupa, základné vlastnosti grupy, morfizmy, Boolova algebra

5.1 Binárne operácie

Jeden z častých prístupov v matematike je kombinovať elementy množiny, pričom sa požadujú špeciálne vlastnosti kombinácie elementov. Teória algebraických štruktúr študuje všeobecné vlastnosti takýchto systémov, ktoré obsahujú množinu (alebo množiny) elementov, nad ktorým je obvykle definovaná binárna operácia (alebo 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 binárne pravidlá, pomocou ktorých sa z elementov množín tvoria elementy taktiež z týchto množín.

Definícia 5.1. ***Binárna operácia*** na množine X je predpis (funkcia)

$$f : X \times X \to X \tag{5.1a}$$

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

$$\forall x \forall y \exists! z \left(z = x * y = f(x,y) \right) \tag{5.1b}$$

Definícia 5.2. Usporiadaná dvojica $(X, *)$ obsahujúca množinu X a binárnu operáciu $*$ nad touto množinou sa nazýva ***algebraická štruktúra***.

Príklad 5.1.

(1) Algebraická štruktúra (,+) obsahuje množina celých čísel a binárna operácia súčet nad touto množinou. Podobným spôsobom môžeme definovať ďalšie dve algebraické štruktúry (,–) a (,×), ktoré sú založené na binárnych operáciách rozdiel resp. súčin.

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

$$\cup: \quad (A) \times \quad (A) \to \quad (A)$$
$$\cap: \quad (A) \times \quad (A) \to \quad (A)$$

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 má 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 5.3.
(1) Binárna operácia $*$ sa nazýva ***asociatívna*** na množine X vtedy a len vtedy, ak pre každé $x,y,z \in X$

$$(x * y) * z = x * (y * z) \tag{5.2a}$$

alebo

$$f(f(x,y),z) = f(x, f(y,z)) \tag{5.2b}$$

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

$$x * y = y * x \tag{5.3a}$$

alebo

$$f(x,y) = f(y,x) \tag{5.3b}$$

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

$$x * e = e * x = x \tag{5.4a}$$

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

$$y * x = x * y = e \tag{5.4b}$$

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

Príklad 5.2.

(1) Pre algebraickú štruktúru $(\mathbb{Z},+)$ jednotkový element je nula, pre každé celé číslo $x \in \mathbb{Z}$ platí podmienka (5.4a)

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

Pre dané celé číslo $x \in \mathbb{Z}$ existuje element $(-x) \in \mathbb{Z}$, ktorý spĺňa podmienku (5.4b)

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

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

(2) Pre algebraickú štruktúru $(\mathbb{Z},\times)$ jednotkový element 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 element $x \in \mathbb{Z}$ má inverzný element? Napríklad, položme $x = 5$, potom inverzný element 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, $\neg\exists(y\in\ )(5\times y = y\times 5 = 1)$. Preto, v rámci algebraického systému (,×) nemá zmysel hovoriť o inverznom elemente vzhľadom k binárnej operácii ´súčin´.

(3) Študujme algebraickú štruktúru $(\ (A),\cap,\cup)$, definovaný pre potenčnú množinu s dvoma binárnymi operáciami ´prienik´ a ´zjednotenie´. Jednotkový a inverzný element pre tento algebraický systém musíme zaviesť separátne pre operáciu zjednotenia resp. prieniku. Každá z týchto operácií má svoj jednotkový element, pre každé $x\in\ (A)$

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

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

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

pretože na pravých stranách nemáme jednotkové elementy pre danú binárnu operáciu.

Veta 5.1. Nech $*$ je binárna operácia na množine X. Ak existuje jednotkový element $x*e = e*x = x$, pre každé $x\in X$, potom tento jednotkový element existuje jednoznačne.

Predpokladajme, že existujú dva jednotkové elementy $e_1, e_2\in X$, 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 5.2. Nech $*$ je asociatívna binárna operácia na množine X, ktorá má jednotkový element $e\in X$. Ak pre každý element $x\in X$ existuje inverzný element, $x*x^{-1} = x^{-1}*x = e$, potom tento inverzný element existuje jednoznačne.

Predpokladajme, že x má dva inverzné elementy u a v, potom podľa (5.4a) platí

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

Potom

$$u = u*e = u*(x*v) = (u*x)*v = e*v = v$$

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

Príklad 5.3. Budeme študovať binárnu operáciu $*$ nad množinou $X = \{a,b,c,d\}$, ktorá je určená multiplikatívnou 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 elementov z množiny *X* sme dokázali

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

t. j. binárna operácia nie je asociatívna.

5.2 Pologrupy, monoidy a grupy

Algebraické štruktúry podľa definície 5.2 obsahujú množinu a binárnu operáciu nad touto množinou. Táto definícia algebraickej štruktúry môže byť zovšeobecnená rôznym spôsobom. Najčastejšie používané zovšeobecnenie je, že algebraická štruktúra obsahuje jednu množinu a dve alebo viac binárnych operácií nad touto množinou. Ďalšie možné zovšeobecnenie pojmu algebraickej štruktúry je, že obsahuje dve alebo viac množín, binárnych operácií nad množinami môže byť viac ako dve. V tejto kapitole budeme študovať jednoduché algebraické štruktúry, ktoré obsahujú jednu množinu a jednu binárnu operáciu nad touto množinou, označíme ju $(G,*)$, kde *G* je množina a $*$ je binárna operácia nad touto množinou. Jedna z najjednoduchších takýchto algebraických štruktúr je pologrupa.

Definícia 5.4. 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

$$(\forall x,y,z\in G)\big((x*y)*z=x*(y*z)\big) \tag{5.5}$$

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

Príklad 5.4.

(1) Algebraické štruktúry $(\ ,+)$, $(\ ,\times)$ sú komutatívne pologrupy. Binárne operácie súčtu a súčinu nad množnou celých čísel sú asociatívne a komutatívne. Tieto dve algebraické štruktúry môžeme zovšeobecniť na množinu reálnych čísiel, potom štruktúry $(\ ,+)$, $(\ ,\times)$ 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 „spojenia“ (konkatenácie), ktorá vytvorí nový reťazec $\gamma=(\alpha+\beta)\in A^*$. Príklad tejto

[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.

operácie je spojenie reťazcov $\alpha = ab$ a $\beta = caa$ na nový reťazec $\gamma = \alpha + \beta = ab + caa = abcaa$. Táto 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, 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

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

čo vyžaduje 3^3 = 27 kontrol pre rôzne trojica elementov. Označme elementy z množiny A pomocou indexovaných veličín, $x_1 = a, x_2 = b, x_3 = c$, potom binárna operácia je určená formulou $x_i * x_j = x_{\lfloor i+j \rfloor}$, kde index na pravej strane je vyjadrený pomocou špeciálnej aritmetiky

$$\lfloor i + j \rfloor = \begin{cases} i + j & (ak\ i + j \leq 3) \\ mod\,(i + j, 3) & (ak\ i + j > 3) \end{cases}$$

kde symbol $mod\,(k, n)$ vyjadruje zvyšok po celočíselnom delení k/n, pozri nasledujúcu tabuľku

$\lfloor i + j \rfloor$	1	2	3
1	2	3	1
2	3	1	2
3	1	2	3

Pretože sa jedná o súčet celých čísel, aj keď obmedzený určitou podmienkou, operácia je evidentne asociatívna, $\lfloor i + \lfloor j + k \rfloor \rfloor = \lfloor \lfloor i + j \rfloor + k \rfloor$, potom aj operácia $*$ musí byť taktiež asociatívna. Potom, algebraická štruktúra $(A, *)$ je komutatívna pologrupa.

Definícia 5.5. Pologrupa $(A, *)$ sa nazýva ***monoid*** vtedy a len vtedy, ak má jednotkový element.

Príklad 5.5.

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

(2) V príklade 5.4.2 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 jednotkový element 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 5.4.3 je monoid, jednotkový element 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) Algebraické štruktúry $\left(X,\cup\right)$ a $\left(X,\cap\right)$ z príkladu 5.1.2, kde $X = \left(A\right)$ 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 jednotkový element prázdnu množinu $\varnothing$ (množinu *A*)

$$\forall\left(X\in \left(A\right)\right)\left(\varnothing\cup X = X\cup\varnothing = X\right)$$

$$\forall\left(X\in \left(A\right)\right)\left(A\cap X = X\cap A = X\right)$$

Mnohé algebraické štruktúry, ktoré majú asociatívnu binárnu operáciu a jednotkový element vzhľadom k tejto operácii (t. j. monoidy), majú ešte dodatočnú vlastnosť, ku každému prvku z množiny existuje inverzný element. 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 5.5. Monoid $\left(G,*\right)$ sa nazýva ***grupa*** vtedy a len vtedy, ak ku každému elementu $x\in G$ existuje inverzný element $x^{-1}\in G$. Platí teda, že algebraická štruktúra $\left(G,*\right)$ je ***grupa*** vtedy a len vtedy, ak sú splnené tieto tri podmienky:

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

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

Pripomeňme, podľa vety 5.1 platí ak má algebraická štruktúra asociatívnu binárnu operácie a existuje jednotkový element, potom tento jednotkový element je jednoznačný; podobne, podľa vety 5.2 platí, že ak existuje ku každému elementu inverzný element, potom je určený jednoznačne. Obe tieto skutočnosti sú platné pre algebraickú štruktúru – grupa, kde sa postuluje existencia jednotkového elementu a inverzného elementu.

Príklad 5.5.

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

(2) Algebraická štruktúra $\left(\ _{+},\times\right)$, kde $\ _{+} = \left(0,\infty\right)$ je množina kladných reálnych čísel, pričom použitá binárna operácie je štandardný súčin. Táto algebraická štruktúra je komutatívna grupa, binárna operácia je asociatívna a komutatívna, existuje neutrálny prvok

$1 \in$ $_{+}$, $1 \times x = x \times 1 = x$, 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 $(\ ,*)$ 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 $x, y, z \in$ 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 . Jednotkový element $e \in$ vyhovuje definičnej podmienke

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

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

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

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

Veta 5.3. Ak algebraická štruktúra $(G,*)$ je grupa, potom existuje „krátenie“ zľava a zprava, pre každé $a, x, y \in G$ platí

(a) krátenie zľava

$$a * x = a * y \Rightarrow x = y \qquad (5.6a)$$

(b) krátenie sprava

$$x * a = y * a \Rightarrow x = y. \qquad (5.6b)$$

Predpokladajme, že platí $a * x = a * y$, existuje inverzný element 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 elementy vo výrazoch, ktoré sa vyskytujú zľava alebo sprava.

Veta 5.4. 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 $x = b * a^{-1}$.

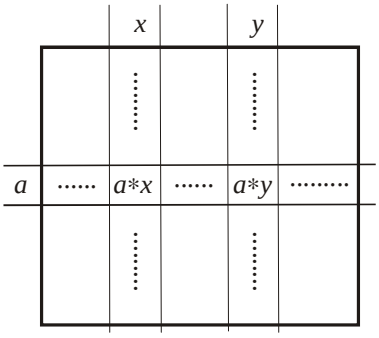
Nech platí $a * x = b$, postupnými úpravami dostaneme

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

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

Veta 5.5. Ak algebraická štruktúra $(G,*)$ je grupa, potom v multiplikačnej tabuľke binárnej operácie $*$ sa v každom riadku alebo stĺpci vyskytuje každý element z *G* práve len raz.

V multiplikačnej tabuľke si vyberme jeden riadok a dva rôzne stĺpce (pozri obr. 5.1). Predpokladajme, že $a*x=a*y$, použijeme vetu 5.3 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 elementy grupy. Dôkaz pre stĺpce je podobný.



Obrázok 5.1. Multiplikačná tabuľka binárnej operácie $*$ grupy $(G,*)$. V tabuľke je vybraný riadok patriaci elementu *a* a dva stĺpce patriace elementom *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 elementy, potom štruktúra $(G,*)$ nie je grupa. Poznamenajme však, skutočnosť, že v tabuľke v každom stĺpci alebo riadku sa neopakujú elementy, nie je postačujúcim dôvodom k tomu, aby štruktúra $(G,*)$ bola grupou.

Definícia 5.7. 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.

Nech $(H,*)$ je podgrupa grupy $(G,*)$, $(H,*) \subseteq (G,*)$, množina H podgrupy je špecifikovaná $H=\{y_1=e,y_2,...,y_m\}$. Predpokladajme, že máme element $x \in G$, pričom $x \notin H$. Potom množina $x*H=\{x*y_1,x*y_2,...,x*y_m\}$ sa nazýva ľavá trieda prvkov vzhľadom k podgrupe $(H,*)$. Podobným spôsobom sa definuje aj pravá trieda prvkov vzhľadom k podgrupe $(H,*)$, značí sa symbolom $H*x=\{y_1*x,y_2*x,...,y_m*x\}$. Poznamenajme, že na základe našich už dokázaných poznatkov o grupe, pravá/ľavá trieda prvkov nemôže byť podgrupou, pretože neobsahuje jednotkový element, a taktiež, všetky jej elementy sú rôzne.

Veta 5.5. Nech $(H,*)\subseteq(G,*)$ a $x_1,x_2\in(G-H)$, potom ľavé triedy x_1*H, x_2*H sú totožné ($x_1*H=x_2*H$) alebo disjunktné ($x_1*H\cap x_2*H=\emptyset$).

Dôkaz vety vykonáme pre ľavé triedy x_1*H, x_2*H, kde $x\in(G-H)$, dôkaz pre pravé triedy je analogický. Predpokladajme, že x_1*H, x_2*H sú disjunktné, potom veta platí. Nech teda tieto množiny majú neprázdny prienik, $x_1*H\cap x_2*H\neq\emptyset$. Existujú dva indexy *p* a *q*, že $x_1*y_p=x_2*y_q$, tento výraz prepíšeme do tvaru $y_p*y_q^{-1}=x_1^{-1}*x_2$. Pretože *H* je podgrupa, pre každú dvojicu $y,y\in H$ platí $y*y\in H$ (čiže aj pre $y=y_p$ a $y=y_q^{-1}$). Potom $y_p*y_q^{-1}H=x_1^{-1}*x_2H=H$, z čoho plynie $x_2*H=x_1*H$, čo bolo potrebné dokázať.

H

Veta 5.7 (Lagrangeova). Nech $(H,*)\subseteq(G,*)$, potom rád množiny $|G|$ je deliteľný rádom podmnožiny $|H|$, alebo existuje také kladné celé číslo *k*, že $|G|=k|H|$

$$((H,*)\subseteq(G,*))\Rightarrow\exists k(|G|=k|H|) \tag{5.7}$$

Táto veta je priamym dôsledkom predchádzajúcej vety 5.6, podľa ktorej ľavé triedy buď sú totožné alebo disjunktné. Postupným použitím vety 5.6 môžeme generovať postupnosť disjunktných množín $x_1*H,x_2*H,...,x_k*H$, kde $x_1,x_2,...,x_k\in G-H$, zjednotenie týchto množín sa rovná množine *G*

$$G=x_1*H\cup x_2*H\cup...\cup x_k*H$$

Pretože ľavé triedy majú rovnakú mohutnosť *m*, potom pre mohutnosť $|G|=km$, alebo $|G|/|H|=k$, čo bolo potrebné dokázať.

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

Veta 5.8. 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 súčinu $*$.

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 element. 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 $x^sx^{r-s}=x^s$. Použijeme zákon krátenia zľava (veta 5.3), dostaneme

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

Týmto sme dokázali, že množina *H* obsahuje jednotkový element. Taktiež platí

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

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

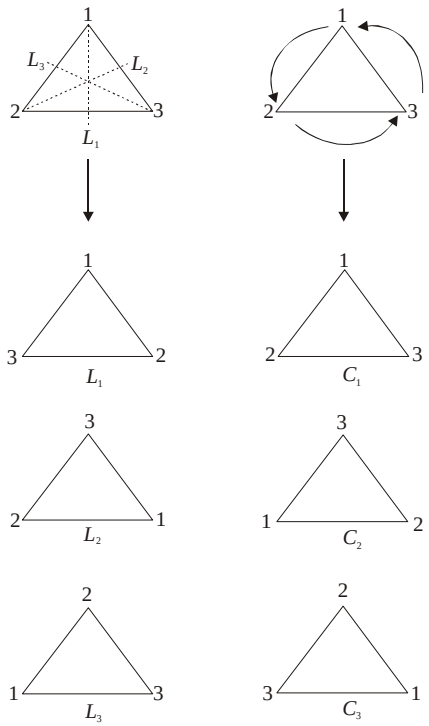
Príklad 5.7. Zavedieme grupu obsahujúce geometrické transformácie rovnostranného trojuholníka, ktorá sa nazýva dihedrálna grupa. V chémii je veľmi populárna, popisuje symetrické vlastnosti niektorých molekúl.

Uvažujme rovnostranný trojuholník, ktorého vrcholy sú označené číslicami 1, 2 a 3, pozri obr. 5.2. Množina elementov 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 operácii 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



Obrázok 5.2. Elementy symetrie rovnostranného trojuholníka, ktorého vrcholy sú označené číslicami 1, 2 a 3. V ľavom stĺpci sú uvedené tri operácia 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.

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

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

Podobným spôsobom môžeme dokázať, že binárna operácia súčinu týchto operácií symetrie je asociatívna. Potom, alegebraická 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 1-1-značné zobrazenie $P : A \to A$, ktoré každému objektu $i \in A$ priradí objekt $p_i \in A$, pričom z podmienky 1-1-značnosti 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 permutácie

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

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''

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

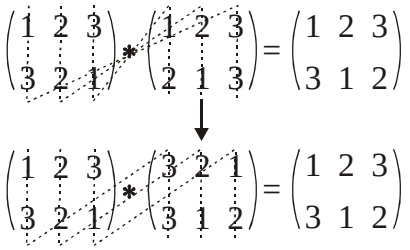
Príklad takto definovaného súčinu permutácií je ukázaný na obr. 5.3. Súčin dvoch permutácií môžeme interpretovať ako kompozíciu dvoch zobrazení *P* a *P´*.

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

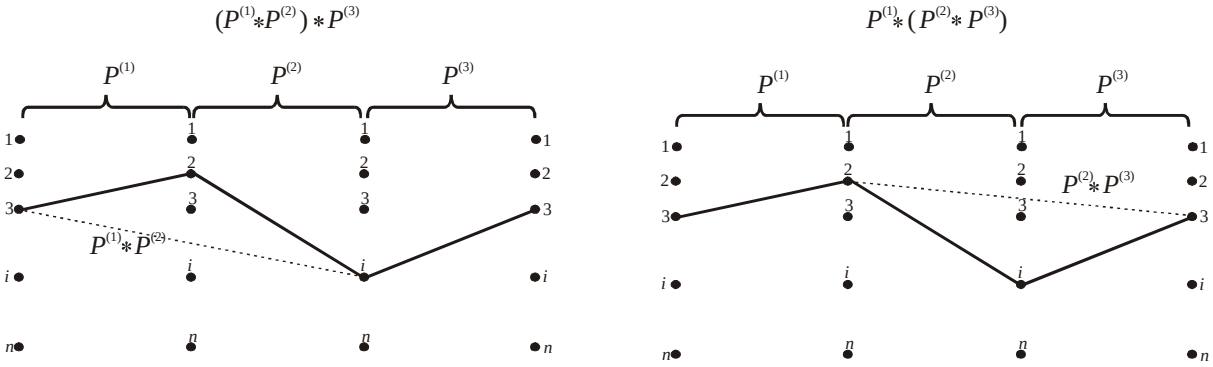
$$P_1 * (P_2 * P_3) = (P_1 * P_2) * P_3$$

Ľahko sa presvedčíme pomocou obrázka 5.4, že táto podmienka je splnená. Problém existencie inverznej permutácie je riešiteľný jednoduchou „inverziou“

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



Obrázok 5.3. Znázornenie súčinu dvoch permutácií $(3\ \ 2\ \ 1)*(2\ \ 1\ \ 3)$. Dolný riadok ilustruje alternatívnu možnosť konštrukcie súčinu permutácií tak, že horný riadok pravej permutácii upravíme do poradia špecifikovaného druhým riadkom prvej permutácie. Dolný riadok takto upravenej permutácie reprezentuje výsledok súčinu.



Obrázok 5.4. 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 5.8. 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 jednotkový element 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 $(S_3',*)\subseteq(S_3,*)$. Pravé triedy majú tvar

$$P_1 * \{P_1,P_2,P_3\} = \{P_1,P_2,P_3\}, P_1 * \{P_4,P_5,P_6\} = \{P_4,P_5,P_6\},$$
$$P_2 * \{P_1,P_2,P_3\} = \{P_1,P_2,P_3\}, P_2 * \{P_4,P_5,P_6\} = \{P_4,P_5,P_6\},$$
$$P_3 * \{P_1,P_2,P_3\} = \{P_1,P_2,P_3\}, P_3 * \{P_4,P_5,P_6\} = \{P_4,P_5,P_6\},$$
$$P_4 * \{P_1,P_2,P_3\} = \{P_4,P_5,P_6\}, P_4 * \{P_4,P_5,P_6\} = \{P_1,P_2,P_3\},$$
$$P_5 * \{P_1,P_2,P_3\} = \{P_4,P_5,P_6\}, P_5 * \{P_4,P_5,P_6\} = \{P_1,P_2,P_3\},$$
$$P_6 * \{P_1,P_2,P_3\} = \{P_4,P_5,P_6\}, P_6 * \{P_4,P_5,P_6\} = \{P_1,P_2,P_3\}$$

5.3 Morfizmy

Porovnajme grupy z príkladov 5.7 a 5.8, ktoré majú úplne odlišnú interpretáciu, prvá grupa obsahuje elementy 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_2	L_3	L_1
C_3	C_3	C_1	C_2	L_3	L_1	L_2
L_1	L_1	L_3	L_2	C_1	C_3	C_2
L_2	L_2	L_1	L_3	C_2	C_1	C_3
L_3	L_3	L_2	L_1	C_3	C_2	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

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

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

Definícia 5.8. Hovoríme, že medzi grupami $(G,*)$ a $(G',\ )$ existuje ***izomorfimus*** (alebo, že grupy sú ***izomorfné***), čo značíme $(G,*) \cong (G',\ )$, vtedy a len vtedy, ak existuje 1-1-značné zobrazenie $f: G \to G'$, ktoré

$$\forall (x,y \in G)\big(f(x*y) = f(x)\ \ f(y)\big) \tag{5.8}$$

Príklad 5.9. Uvažujme dve grupy $(\ ,+)$ a grupu $(\ _+,\times)$, kde $_+ = (0,\infty)$ je množina kladných reálnych čísel. Dokážte, že funkcia $f(x) = 2^x$ definuje izomorfizmus medzi týmito dvoma grupami, $(\ ,+) \cong (\ _+,\times)$.

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

Veta 5.9. Ak $f:G\to G'$ je izomorfizmus medzi grupami $(G,*)$ a $(G',\ )$, potom

(1) Ak e je jednotkový element v grupe $(G,*)$, potom $f(e)$ je jednotkový element v grupe $(G',\ )$.

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

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

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

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

Táto veta nám pomáha zistiť, či medzi grupami $(G,*)$ a $(G',\ )$ existuje izomorfizmus. Napríklad, ak grupa $(G,*)$ je komutatívna a grupa $(G',\ )$ 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 5.10. Dokážte, že ak $A=\{a,b\}$, potom monoidy $(\ (A),\cup)$ a $(\ (A),\cap)$ sú izomorfné.

Potenčná množina má tvar $(A)=\{\varnothing,\{a\},\{b\},\{a,b\}\}$. Multiplikatívne tabuľky pre tieto monoidy sú

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

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

1-1-značná funkcia $f:\ (A)\to\ (A)$, 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 $(\ (A),\cup)$ a $(\ (A),\cap)$ existuje izomorfizmus.

Definícia 5.9. Hovoríme, že medzi grupami $(G,*)$ a $(G',\ )$ existuje ***morfizmus*** vtedy a len vtedy, ak existuje zobrazenie $f:G\to G'$, ktoré

$$\forall(x,y\in G)\big(f(x*y)=f(x)\ \ f(y)\big) \tag{5.9}$$

Ak medzi dvoma algebraickými štruktúrami existuje izomorfizmus, potom tieto štruktúry sú „skoro totožné“. Ak odstránime podmienku 1-1-značnosti funkcie $f:G\to G'$, potom táto

„skoro totožnosť“ sa stráca, druhá algebraická štruktúra $(G', \ )$ stráca niektoré detaily prvej štruktúry.

Veta 2.10. Ak $f : G \to G'$ je ***morfizmus*** medzi grupami $(G,*)$ a $(G', \ )$, potom

(1) Ak e je jednotkový element v grupe $(G,*)$, potom $f(e)$ je jednotkový element v grupe $(G', \ )$.

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

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

Príklad 5.11. Uvažujme množinu $A = \{a,b,c\}$, množina A^* obsahuje všetky možné reťazce (včítane prázdneho reťazca ε). Potom algebraická štruktúra $(A^*,*)$, kde binárna operácia $*$ reprezentuje spájanie reťazcov, je monoid (existuje jednotkový element reprezentovaný prázdnym reťazcom ε). Nech existuje funkcia $f : A^* \to$, kde je množina nezáporných celých čísel, táto funkcia je definovaná takto

$$f(x) = \text{dľžka reťazca } x$$

Ukážte, že toto zobrazenie f je morfizmus z $(A^*,*)$ na $(\ ,+)$.

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 je zložiek x a y. Táto funkcia evidentne nie je 1-1-značná.

5.4. Boolova algebra

Elektronické obvody v počítačoch a v podobných zariadeniach sú charakterizované binárnymi vstupmi a výstupmi (rovnajúcimi sa 0 alebo 1), transformácia vstupu na výstupu sa uskutočňuje prostredníctvom elektronického obvodu, ktorý tvorí jadro tohto „transformačného“ zariadenia, pozri obr. 7.1. Elektronický obvod môže byť formálne simulovaný tvz. Boolovou[2] funkciou, ktorá transformuje m binárnych vstupných premenných na n výstupných binárnych premenných.

[2] George Boole (1815-1864), anglický matematik, ktorý sa svojou knihou *Laws of Thought* (1854) zaslúžil o moderný rozvoj výrokovej logiky ako špeciálnej oblasti algebry, ktorá je nazvaná jeho menom – Boolova algebra.

Obrázok 7.1. Znázornenie elektronického obvodu, ktorý má *m* binárnych vstupov a *n* binárnych výstupov. Činnosť elektronického obvodu spočíva v transformácii binárnych vstupných hodnôt na binárne výstupné hodnoty.

Všeobecná definícia Boolovej funkcie je $f:\{0,1\}^m \to \{0,1\}^n$, táto funkcia transformuje binárny vektor dĺžky *m* na binárny vektor dĺžky *n*. Môžeme si položiť otázku, ako realizovať túto Boolovu funkciu, aby mala vopred špecifikované vlastnosti? Tento problém je realizovaný pomocou Boolovej algebry, ktorá pomocou premenných s 0-1 ohodnotením (t. j. binárnych) premenných a pomocou dvoch elementárnych algebraických operácií a jednej unárnej algebraickej operácie je schopná dostatočne všeobecne modelovať Boolove funkcie s vopred špecifikovanými vlastnosťami. Poznamenajme, že Boolova algebra má dva známe modely, prvým je výroková logika a druhým algebra teórie množín. Pretože obe tieto zdanlivo odťažité disciplíny majú rovnakú „metateóriu“, existuje medzi zákonmi výrokovej logiky a formulami teórie množín „dualizmus“, pomocou ktorého ku každému zákonu výrokovej logiky priradíme 1-1-značne formulu teórie množín a naopak. Dobrým, ilustratívnym príkladom tohto dualizmu sú De Morganove formuly, ktoré vo výrokovej logike a v teórii množín majú tvary

$$\neg(p \wedge q) \equiv (\neg p \vee \neg q) \Leftrightarrow \overline{A \cap B} = \overline{A} \cup \overline{B}$$
$$\neg(p \vee q) \equiv (\neg p \wedge \neg q) \Leftrightarrow \overline{A \cup B} = \overline{A} \cap \overline{B}$$

V týchto formulách, vo výrokovej logike unárna logická spojka negácie má ekvivalent v teórii množín v unárnej algebraickej operácii doplnku, a podobne, vo výrokovej logike binárne spojky konjunkcie a disjunkcie majú ekvivalenty v teórii množín v binárnych algebraických operáciách prieniku resp. zjednotenia. Na záver je potrebné poznamenať, že výroková spojka ekvivalentnosti má v teórii množín ekvivalent v relácii rovnosti. Tieto priradenia vo výrokovej logike a v teórii množín môžeme zosumarizovať takto

výrokové premenné $p,q,r,... \Leftrightarrow$ množiny $A,B,C,...$

spojka negácie $\neg \Leftrightarrow$ operácia doplnku $\overline{}$

spojka konjunkcie $\wedge \Leftrightarrow$ operácia prieniku $\cap$

spojka disjunkcie $\vee \Leftrightarrow$ operácia zjednotenia $\cup$

spojka ekvivalentnosti $\equiv \Leftrightarrow$ relácia rovnosti $=$

Definícia 7.1. ***Boolova algebra*** je algebraická štruktúra špecifikovaná usporiadanou 6-ticou $(B,+,\cdot,\mathbf{G},\mathbf{0},\mathbf{1})$, kde $B=\{a,b,...,x,y,...\}$ je neprázdna množina elementov (premenných Boolovej algebry), ktorá obsahuje dva špeciálne odlíšené elementy - konštanty $\mathbf{0},\mathbf{1} \in B$ a nad ktorou sú definované binárne operácie súčinu a súčtu

$$\cdot : B \times B \to B \tag{7.1a}$$
$$+ : B \times B \to B \tag{7.1b}$$

a unárna operácia komplementu

$$\mathbf{G}: B \to B \tag{7.1c}$$

ktoré vyhovujú týmto podmienkam

(1) komutatívnosť:

$$x \cdot y = y \cdot x, \qquad x + y = y + x \tag{7.1d}$$

(2) asociatívnosť:

$$(x \cdot y) \cdot z = x \cdot (y \cdot z), \qquad (x + y) + z = x + (y + z) \tag{7.1e}$$

(3) distributívnosť:

$$x \cdot (y + z) = (x \cdot y) + (x \cdot z), \qquad x + (y \cdot z) = (x + y) \cdot (x + z) \tag{7.1f}$$

(4) vlastnosť konštanty **0**:

$$x = x + \mathbf{0}, \qquad x \cdot \overline{x} = \mathbf{0} \tag{7.1g}$$

(5) vlastnosť konštanty **1** :

$$x = x \cdot \mathbf{1}, \qquad x + \overline{x} = \mathbf{1} \tag{7.1h}$$

V literatúre existuje mnoho alternatívnych notácií Boolovej algebry. Napríklad operácia súčinu sa alternatívne vyjadruje symbolmi $\wedge$ alebo $*$, podobne, operácia súčtu symbolmi $\vee$ a $\oplus$. Pre zjednodušenie notácie budeme vynechávať symbol súčinu, formulu $x \cdot y$ budeme zjednodušene písať ako *xy*. Z formúl (7.1g-h) vyplýva, že konštanta **1** (**0**) má úlohu neutrálneho (jednotkového) prvku pre súčin (súčet). Z bežného pohľadu na formuly (7.1g-h) by niekto mohol odvodiť záver, že výraz $\overline{x}$ je inverzná formula pre *x*. Pripomeňme si, že v kapitole 6 bol inverzný element definovaný pomocou vlastnosti $x \cdot \overline{x} = \mathbf{1}$, avšak podľa pravej formuly (7.1g) platí $x \cdot \overline{x} = \mathbf{0}$, z čoho vyplýva, že výraz $\overline{x}$ nemá vlastnosti inverzného prvku (tak vzhľadom k operácii súčtu, ako aj súčinu).

Príklad 7.1. Najjednoduchšia Boolova algebra (s veľkým významom v informatike a v logike) je založená na dvojprvkovej množine $B = \{0,1\}$. Binárne operácie súčinu, súčtu a unárna operácia komplementu sú pomocou multiplikačných tabuliek definované takto

+	0	1
0	0	1
1	1	1

·	0	1
0	0	0
1	0	1

b	$\overline{b}$
0	1
1	0

Jednoducho sa môžeme presvedčiť, že pre takto špecifikované operácie sú splnené podmienky (7.1a-h), t. j. algebraická štruktúra $\left(B,+,\cdot,\overline{\ },\mathbf{0},\mathbf{1}\right)$ je Boolova algebra.

Príklad 7.2. Nech $A = \{a,b,c,...\}$ je neprázdna množina, položme $B = \mathcal{P}(A)$. Operácie $\cdot$ a $+$ sú realizované pomocou množinových operácií $\cap$ resp. $\cup$, operácia komplementu je realizovaná ako množinový komplement vzhľadom k množine *A*, $\overline{x} = A - x$. Potom platí:

(a) binárne operácie sú asociatívne, komutatívne,

(b) medzi binárnymi operáciami platia distributívne zákony,

(c) prázdna množina $\emptyset$ má vlastnosti jednotkového elementu pre operáciu $\cup$

$$(\forall X \in B)(X \cup \emptyset = \emptyset \cup X = X)$$

(d) množina *A* má vlastnosti jednotkového elementu pre operáciu $\cap$

$$(\forall X \in B)(X \cap A = A \cap X = X)$$

(e) pre každé $X \in B$ existuje komplement $\overline{X} \in B$ taký, že

$$(\forall X \in B)(X \cap \overline{X} = \emptyset)$$

$$(\forall X \in B)(X \cup \overline{X} = A)$$

To znamená, že podmienky (7.1a-h) sú splnené, t. j. algebraická štruktúra $\left(\mathcal{P}(A),\cup,\cap,\overline{\ },\emptyset,A\right)$ je Boolova algebra.

Príklad 7.3. Nech $B = \{p,q,r,...\}$ je množina výrokových formúl, ktorá je uzavretá vzhľadom k binárnym operácia konjunkcie ($\wedge$), disjunkcie ($\vee$) a k unárnej operácii negácie

($\neg$). Pre túto množinu je definovaná aj relácia ekvivalentnosti ´≡´, dve formuly sú ekvivalentné vtedy a len vtedy, ak majú rovnakú pravdivostnú interpretáciu (logicky ekvivalentné). Z množiny B vyberieme formulu kontradikciu (napr. $p \wedge \neg p$) a označíme ju symbolom 0; podobne formula tautológia (napr. $p \vee \neg p$) je označená symbolom 1. To znamená, že symboly 0 a 1 patria do množiny B. Pre každú formulu p platia tieto vzťahy

$$p \vee 0 = 0 \vee p = p$$

$$p \wedge 1 = 1 \wedge p = p$$

Pretože logické spojky konjunkcie a disjunkcie sú komutatívne a asociatívne, pre tieto operácie platia taktiež distributívne zákony, podmienky z definície 7.1 sú splnené, t. j. algebraická štruktúra $(B, \vee, \wedge, \neg, 0, 1)$ tvorí Boolovu algebru.

5.5 Vlastnosti Boolovej algebry

V úvodnej časti kapitoly 7.1 bol zmienený princíp duality medzi algebrou teórie množín a výrokovou logikou. Ukážeme, že tento princíp je aplikovateľný aj pre rôzne Boolove algebry.

Postulujme nejaký výrok (alebo formulu), ktorý je platný v Boolovej algebre. Duálnu formu výroku dostaneme tak, že urobíme zámenu symbolov

$$\cdot \to +, \; + \to \cdot, \; \mathbf{0} \to \mathbf{1} \text{ a } \mathbf{1} \to \mathbf{0}$$

Napríklad, uvažujme formulu Boolovej algebry, $(x + y) \cdot x \cdot \overline{y} = \mathbf{0}$, duálny tvar tejto formuly je $(x \cdot y) + x + \overline{y} = \mathbf{1}$. Axiómy Boolovej algebry (7.1d-h) sú uvedené po dvojiciach duálnych formúl. To znamená, že ak v rámci Boolovej algebry odvodíme nejakú formulu, tak potom aj jej duálna forma je odvoditeľná pomocou postupu, ktorý je „duálny“ k postupu prvej formuly.

Veta 7.1 (princip duálnosti). Každá veta Boolovej algebry je taktiež vetou aj v duálnej forme.

V predchádzajúcej kaptole bola dokázaná veľmi všeobecná veta 6.1 o jednoznačnosti jednotkového (neutrálneho) elementu. Tento dôkaz bol založený na predpoklade existencie jednotkového elementu, rovnaký dôvod môže byť použitý aj pre dôkaz jednoznačnosti jednotkových elementov **1** a **0**.

Veta 7.2. Jednotkové elementy **1** a **0** existujú jednoznačne.

Podobne sa dá dokázať aj jednoznačnosť existencie inverzných elementov v Boolovej algebre.

Veta 7.3. Pre každý element $x \in B$ existuje jednoznačne element $\overline{x} \in B$ taký, že $x \cdot \overline{x} = \mathbf{0}$ a $x + \overline{x} = \mathbf{1}$ (t. j .sú splnené podmienky 7.1g-h).

Veta 7.4. Nech $(B, +, \cdot, \overline{}, \mathbf{0}, \mathbf{1})$ je Boolova algebra, potom platia tieto formulu

(1) Involutívnosť komplementu

$$(\forall x \in B)\left(\overline{\overline{x}} = x\right) \tag{7.2a}$$

(2) Idempotentnosť

$$(\forall x \in B)(x \cdot x = x) \tag{7.2b}$$

$$(\forall x \in B)(x + x = x) \tag{7.2c}$$

(3) De Morganove zákony

$$(\forall x, y \in B)\left(\overline{x + y} = \overline{x} \cdot \overline{y}\right) \tag{7.2d}$$

$$(\forall x, y \in B)\left(\overline{x \cdot y} = \overline{x} + \overline{y}\right) \tag{7.2e}$$

(4) Nulitnosť

$$(\forall x \in B)(x + \mathbf{1} = \mathbf{1}) \tag{7.2f}$$

$$(\forall x \in B)(x \cdot \mathbf{0} = \mathbf{0}) \tag{7.2g}$$

(5) Absorpcia

$$(\forall x, y \in B)(x + (x \cdot y) = x) \tag{7.2h}$$

$$(\forall x \in B)(x \cdot (x + y) = x) \tag{7.2i}$$

(6) Komplementy konštánt

$$\overline{\mathbf{0}} = \mathbf{1} \tag{7.2j}$$

$$\overline{\mathbf{1}} = \mathbf{0} \tag{7.2k}$$

(7) Vlastnosti konštánt vzhľadom k binárnym operáciam

$$\mathbf{0} + \mathbf{0} = \mathbf{0}, \mathbf{0} + \mathbf{1} = \mathbf{1}, \mathbf{1} + \mathbf{0} = \mathbf{1}, \mathbf{1} + \mathbf{1} = \mathbf{1} \tag{7.2l}$$

$$\mathbf{0} \cdot \mathbf{0} = \mathbf{0}, \mathbf{0} \cdot \mathbf{1} = \mathbf{0}, \mathbf{1} \cdot \mathbf{0} = \mathbf{0}, \mathbf{1} \cdot \mathbf{1} = \mathbf{1} \tag{7.2m}$$

Dôkaz týchto vlastností prenecháme na cvičenie.

5.6 Boolove funkcie

V úvode k tejto kapitole bola Boolova funkcia definovaná ako funkcia nad binárnymi premennými $\{0,1\}$. Tento pomerne zjednodušený pohľad na Boolovu funkciu bude teraz rozšírený tak, aby koncepcia Boolovej funkcie bola časťou Boolovej algebry. Základný pojem pre definíciu Boolovej funkcie je pojem Boolovej premennej. Použijeme analogický prístup, aký sa používa pre definíciu reálnej premennej, je to veličina, ktorá môže nadobúdať hodnoty z množiny reálnych čísel.

Definícia 7.2. Nech $(B, +, \cdot, \overline{\ }, \mathbf{0}, \mathbf{1})$ je Boolova algebra. Potom,

(1) ***Boolova premenná*** je taká premenná, ktorá nadobúda hodnoty z množiny *B*,
(2) ***komplement premennej*** *x*, označený $\overline{x}$, je taká premenná, ktorej hodnota sa rovná komplementu hodnoty premennej *x* (t. j. ak $x = b \in B$, potom $\overline{x} = \overline{b} \in B$,
(3) ***literál*** je Boolova premenná *x* alebo jej komplement $\overline{x}$.

V ďalšom texte budeme používať notáciu, ktorá umožní rozlíšiť literál

$$x^e = \begin{cases} x & (pre\ e = 1) \\ \overline{x} & (pre\ e = 0) \end{cases} \tag{7.3}$$

Podobne ako pre reálnu premennú, aj Boolova premenná môže byť kombinovaná do tvaru Boolových formúl použitím binárnych operácií súčinu, súčtu a komplementu.

Definícia 7.3. Nech $(B, +, \cdot, \overline{\ }, \mathbf{0}, \mathbf{1})$ je Boolova algebra. Potom ***Boolova formula***, obsahujúca Boolove premenné $x_1, x_2, ..., x_n$, je definovaná takto:

(1) konštanty **0** a **1** sú Boolove formuly,
(2) Boolove premenné $x_1, x_2, ..., x_n$ sú Boolove formuly,
(3) ak X a Y sú Boolove formuly, potom aj výrazy $(X \cdot Y)$, $(X + Y)$, $\overline{X}$ a $\overline{Y}$ sú Boolove formuly.

V ďalšom texte budeme používať konvenciu, že ak bude jasné o akú formulu sa jedná, tak termín ´Boolova formula´ budeme skracovať na ´formula´. Podobne, ako vo výrokovej logike môžeme si definovať rastúcu prioritu operácií takto: (1) súčet, (2) súčin a (3) komplement. Napríklad, formulu $((x \cdot y) + z)$ môžeme pomocou tejto konvencie vyjadriť v zjednodušenom tvare bez zátvoriek $x \cdot y + z$. Konečne, podobne ako v štandardnej algebre, budeme vynechávať znak súčinu, napríklad predchádzajúci ilustračný príklad má tvar $xy + z$.

Príklad 7.4. Zjednodušte formulu $((x + y) \cdot (\overline{x} + \overline{y}))$.
Použitím distributívneho zákona a (7.1g-h)

$$((x + y) \cdot (\overline{x} + \overline{y})) = (x \cdot \overline{x}) + (x \cdot \overline{y}) + (y \cdot \overline{x}) + (y \cdot \overline{y}) = \underset{\mathbf{0}}{x\overline{x}} + x\overline{y} + y\overline{x} + \underset{\mathbf{0}}{y\overline{y}} = x\overline{y} + \overline{x}y$$

Definícia 7.4. Dve Boolove formule sú ***ekvivalentné*** (alebo ***rovné***) vtedy a len vtedy, ak jedna pomocou konečného počtu aplikácií axióm Booloej algebry je pretransformovaná na druhú formulu.

Podľa príkladu 7.4 formule $\varphi_1 = (x + y) \cdot (\overline{x} + \overline{y})$ a $\varphi_2 = x\overline{y} + \overline{x}y$ sú ekvivalentné, pretože druhú formulu získame z prvej použitím konečného počtu aplikácií axióm Boolovej algebry, potom $\varphi_1 = \varphi_2$.

Konečne sa dostávame k definícii Boolovej funkcie $f(x_1, x_2, ..., x_n)$ ako Boolovej formuly, ktorá obsahuje premenné $x_1, x_2, ..., x_n$. Napríklad

$$f(x_1, x_2, x_3) = x_1(x_2 + \overline{x}_3)$$

Definícia 7.5. Nech $(B, +, \cdot, \overline{\ }, \mathbf{0}, \mathbf{1})$ je Boolova algebra.
(1) ***Boolova funkcia*** $f(x_1, x_2, ..., x_n)$ premenných $x_1, x_2, ..., x_n$, je zobrazenie $f : B^n \to B$, pričom $f(x_1, x_2, ..., x_n)$ je špecifikovaná ako Boolova formula.
(2) Všetky Boolove formule, ktoré sú navzájom ekvivalentné, definujú rovnakú funkciu.

Z tejto definície vyplýva, že ekvivaletné Boolove formuly špecifikujú rovnakú Boolovu formulu. Napríklad, máme dve funkcie

$$f : B^2 \to B \qquad f(x_1, x_2) = x_1(\overline{x}_1 + x_2)$$

$$g : B^2 \to B \qquad g(x_1, x_2) = x_1 x_2$$

Použitím distribučného zákona ľahko dokážeme, že formuly sú ekvivaletné, $x_1(\overline{x}_1 + x_2) = x_1 x_2$, potom funkcie *f* a *g* sú rovnaké.

Pretože Boolova funkcia môže byť vyjadrená mnohými rôznymi formulami, ktoré sú navzájom ekvivaletné, vzniká otázka, ako efektívne rozhodnúť, či dve Boolove formuly sú ekvivalentné, alebo či dve Boolové funkcie sú rovnaké. Ukážeme postup, ktorý nie je založený na transformácii jednej formuly na druhú, aby sme rozhodli, či funkcie sú rovnaké, ale navrhne sa „kanonická“ reprezentácia Boolovej funkcie, podľa ktorej môžeme jednoducho rozhodnúť, či dve Boolove funkcie sú rovnaké alebo nie.

Definícia 7.6. ***Súčinová klauzula*** premenných $x_1, x_2, ..., x_n$ je Boolova formula, ktorá obsahuje súčin *n* literálov (t. j. premennú alebo jej komplement) pre každú premennú.

Ako príklad súčinovej klauzuly premenných x_1, x_2, x_3 sú tieto formuly: $x_1x_2x_3$, $x_1x_2\overline{x}_3$, $x_1\overline{x}_2x_3$, $\overline{x}_1x_2x_3$,…, $\overline{x}_1\overline{x}_2\overline{x}_3$. Ak použijeme formalizmus x^e, potom súčinovú klauzulu premenných $x_1, x_2, ..., x_n$, ktorá je špecifikovaná binárnym vektorom $\boldsymbol{e} = (e_1, e_2, ..., e_n)$, má tvar

$$l_{\boldsymbol{e}} = x_1^{e_1} x_2^{e_2} ... x_n^{e_n} \tag{7.4}$$

Napríklad, pre $\boldsymbol{e} = (11011)$ súčinová klauzula má tvar

$$l_{(11011)} = x_1^1 x_2^1 x_3^0 x_4^1 x_5^1 = x_1 x_2 \overline{x}_3 x_4 x_5$$

Pretože binárnych vektorov $\boldsymbol{e} = (e_1, e_2, ..., e_n)$ je 2^n, potom aj ***rôznych*** súčinových klauzúl je 2^n.

Definícia 7.7. ***Súčtová klauzula*** premenných $x_1, x_2, ..., x_n$ je Boolova formula, ktorá obsahuje súčet *n* literálov (t. j. premennú alebo jej komplement) pre každú premennú.

Podobne ako pre súčinovú klauzulu, môžeme aj súčtovú klauzulu pre premenné $x_1, x_2, ..., x_n$ špecifikovať binárnym vektorom $\boldsymbol{e} = (e_1, e_2, ..., e_n)$

$$L_{\boldsymbol{e}} = x_1^{e_1} + x_2^{e_2} + ... + x_n^{e_n} \tag{7.5}$$

Pre $\boldsymbol{e} = (10100)$ súčtová klauzula má tvar

$$L_{\boldsymbol{e}} = x_1^1 + x_2^0 + x_3^1 + x_4^0 + x_5^0 = x_1 + \overline{x}_2 + x_3 + \overline{x}_4 + \overline{x}_5$$

Pretože každá súčtová klauzula premenných $x_1, x_2, ..., x_n$ je špecifikovaná binárnym vektorom $\boldsymbol{e} = (e_1, e_2, ..., e_n)$, potom počet súčtových klauzúl je taktiež 2^n.

Týmto sa dostávame k formulácii hlavného výsledku tejto kapitoly, že každá Boolova funkcia môže byť jednoznačne vyjadrená ako sumácia súčinových klauzúl (tento tvar sa nazýva vo výrokovej logike ***disjunktívna normálna forma***, skratka DNF).

Príklad 7.5. Vyjadrite Boolovu funkciu $x_1x_2(x_1 + x_3)$ pomocou súčtu súčinových klauzúl (DNF)

$$\begin{aligned}
x_1x_2(x_1 + x_3) &= x_1x_2x_1 + x_1x_2x_3 \\
&= \underset{x_1}{x_1x_1}\, x_2 + x_1x_2x_3 = x_1x_2 + x_1x_2x_3 \\
&= x_1x_2\mathbf{1} + x_1x_2x_3 = x_1x_2(x_3 + \overline{x}_3) + x_1x_2x_3 \\
&= x_1x_2x_3 + x_1x_2x_3 + x_1x_2\overline{x}_3 \\
&= \underset{x_1x_2x_3}{x_1x_2x_3} + x_1x_2\overline{x}_3
\end{aligned}$$

Veta 7.5. Každá Boolova funkcia $f(x_1,x_2,...,x_n)$, ktorá sa identicky nerovná nule, môže byť špecifikovaná ako suma súčinových klauzúl

$$\begin{aligned} f(x_1,x_2,...,x_n) &= \sum_{\boldsymbol{e}} f(e_1,e_2,...,e_n)\, x_1^{e_1} x_2^{e_2} ... x_n^{e_n} \\ &= \sum_{\boldsymbol{e}} f(e_1,e_2,...,e_n)\, l_{(e_1,e_2,...,e_n)} \\ &= \sum_{\boldsymbol{e}} f(\boldsymbol{e})\, l_{\boldsymbol{e}} \end{aligned} \tag{7.6}$$

Presný dôkaz tejto vety vykonaný pomocou matematickej indukcie je pomerne zdĺhavý, preto ho nebudeme uvádzať. Naznačíme jednoduchý konštruktívny dôkaz. Boolova funkcia $f(x_1,x_2,...,x_n)$ je vlastne špecifikovaná jej funkčnými hodnotami $f(e_1,e_2,...,e_n)$ pre všetky hodnoty binárneho vektora $\boldsymbol{e}=(e_1,e_2,...,e_n)$. Hovoríme, že funkcia f je špecifikovaná tabuľkou funkčných hodnôt, ktorá obsahuje 2^n riadkov

#	$\boldsymbol{e}=(e_1,e_2,...,e_n)$	$l_{(e_1,e_2,...,e_n)}$
1	(00.....00)	**0**
2	(00.....01)	**1**
.....		
i	$(e_1^{(i)},e_2^{(i)},...,e_n^{(i)})$	**1/0**
.....		
2^n	(11.....11)	**0**

Súčinová klauzula $l_{(e_1,e_2,...,e_n)}(x_1,x_2,...,x_n)=x_1^{e_1}x_2^{e_2}...x_n^{e_n}$ má zaujímavú vlastnosť, jej funkčná hodnota sa rovná **1** len pre $(x_1,x_2,...,x_n)=(\boldsymbol{e}_1,\boldsymbol{e}_2,...,\boldsymbol{e}_n)$, kde $\boldsymbol{e}_i\in\{\mathbf{0},\mathbf{1}\}$, pre všetky iné prípady funkčná hodnota je **0**

$$l_{(e_1,e_2,...,e_n)}(x_1,x_2,...,x_n)=\begin{cases}\mathbf{1} & (pre\,(x_1,x_2,...,x_n)=(\boldsymbol{e}_1,\boldsymbol{e}_2,...,\boldsymbol{e}_n)) \\ \mathbf{0} & (pre\,(x_1,x_2,...,x_n)\neq(\boldsymbol{e}_1,\boldsymbol{e}_2,...,\boldsymbol{e}_n))\end{cases} \tag{7.7}$$

To znamená, že pre konštrukciu (7.6) sú pre nás dôležité len funkčné hodnoty **1**, funkčné hodnoty **0** nie sú podstatné pre náš konštruktívny dôkaz. Zostrojíme Boolovu formulu ako sumáciu týchto klauzúl (t. j. v DNF tvare)

$$F(x_1,x_2,...,x_n)=\sum_{\boldsymbol{e}} f(e_1,e_2,...,e_n)\, l_{(e_1,e_2,...,e_n)} \tag{7.8}$$

Z konštrukcie tejto Boolovej funkcie, vyplýva, že jej funkčné hodnoty sú špecifikované tabuľkou funkčných hodnôt Boolovej funkcie $f(x_1,x_2,...,x_n)$. To znamená, že Boolove funkcie $f(x_1,x_2,...,x_n)$ a $F(x_1,x_2,...,x_n)$ sú ekvivalentné, t. j. majú rovnaké funkčné hodnoty pre rôzne hodnoty argumentov. Týmto sme zavŕšili jednoduchý intuitívny konštruktívny dôkaz vety 7.5.

Poznamenajme, že DNF tvar Boolovej funkcie je určený jednoznačne až na permutácie argumentov v súčtových klauzulách, alebo až na permutácie súčtových klauzúl.

Táto nejednoznačnosť DNF tvaru vyplýva zo skutočnosti, že binárne operácie súčtu a súčinu sú komutatívne. Môžeme teda konštatovať, že DNF sú základné charakteristiky (niečo ako odtlačky prstov alebo zloženie DNA) Boolových funkcií. Aby sme odstránili prípadné nejednoznačnosti zapisujeme DNF v tzv. kanonickom tvare, t. j. jednotlivé argumenty sa zapisujú postupne podľa rastúceho indexu (tým sme odstránili nejednoznačnosti v dôsledku kumutatívnosti súčinu) a potom jednotlivé súčinové klauzule sú písané v poradí rastúcej číselnej hodnoty „indexu“ $\boldsymbol{e} = (e_1, e_2, ..., e_n)$.

Príklad 7.6. Zostrojte Boolovu funkciu $f(x_1, x_2) = x_1 + x_2$ v tvare DNF. Podľa vety 7.5 DNF tvar tejto funkcie je

$$f(x_1, x_2) = f(\mathbf{0},\mathbf{0})\,\overline{x}_1\overline{x}_2 + f(\mathbf{0},\mathbf{1})\,\overline{x}_1 x_2 + f(\mathbf{1},\mathbf{0})\,x_1\overline{x}_2 + f(\mathbf{1},\mathbf{1})\,x_1 x_2$$

kde jednotlivé funkčné hodnoty sú uvedené v tabuľke

#	e_1	e_2	$f(e_1,e_2)$
1	**0**	**0**	**0**
2	**0**	**1**	**1**
3	**1**	**0**	**1**
4	**1**	**1**	**1**

Potom funkcia *f* má tvar

$$\begin{aligned} f(x_1, x_2) &= \mathbf{0}\overline{x}_1\overline{x}_2 + \mathbf{1}\overline{x}_1 x_2 + \mathbf{1}x_1\overline{x}_2 + \mathbf{1}x_1 x_2 \\ &= \overline{x}_1 x_2 + x_1\overline{x}_2 + x_1 x_2 \end{aligned}$$

Ľahko dokážeme, že takto definovaná funkcia $f(x_1, x_2) = \overline{x}_1 x_2 + x_1\overline{x}_2 + x_1 x_2$ je ekvivalentná s pôvodnou Boolovou funkciou $f(x_1, x_2) = x_1 + x_2$

$$f(x_1, x_2) = \overline{x}_1 x_2 + x_1\overline{x}_2 + x_1 x_2 = \overline{x}_1 x_2 + x_1\overline{x}_2 + x_1 x_2 + x_1 x_2 = \underbrace{\left(\overline{x}_1 + x_1\right)}_{1} x_2 + x_1 \underbrace{\left(\overline{x}_2 + x_2\right)}_{1} = x_1 + x_2$$

Príklad 7.7. Zostrojte Boolovu funkciu $f(x_1, x_2, x_3) = x_2 x_3 + x_1 x_3$ v tvare DNF. Táto Boolova funkcia je určená tabuľkou funkčných hodnôt

#	e_1	e_2	e_3	e_2e_3	e_1e_3	$e_2e_3 + e_1e_3$
1	**0**	**0**	**0**	**0**	**0**	**0**
2	**0**	**0**	**1**	**0**	**0**	**0**
3	**0**	**1**	**0**	**0**	**0**	**0**
4	**0**	**1**	**1**	**1**	**0**	**1**
5	**1**	**0**	**0**	**0**	**0**	**0**
6	**1**	**0**	**1**	**0**	**1**	**1**
7	**1**	**1**	**0**	**0**	**0**	**0**
8	**1**	**1**	**1**	**1**	**1**	**1**

Potom funkcia $f(x_1, x_2, x_3)$ (uvažujeme len jednotkové funkčné hodnoty) má DNF tvar

$$f(x_1, x_2, x_3) = \overline{x}_1 x_2 x_3 + x_1\overline{x}_2 x_3 + x_1 x_2 x_3$$

Použijeme duálny princíp z vety 7.1, veta 7.5 má potom tento duálny tvar

Veta 7.6. Každá Bolova funkcia $f(x_1,x_2,...,x_n)$, ktorá sa identicky nerovná jednotke, môže byť špecifikovaná ako súčin sumačných klauzúl

$$\begin{aligned} f(x_1,x_2,...,x_n) &= \prod_{\boldsymbol{e}} \left(f(e_1,e_2,...,e_n) + x_1^{\overline{e}_1} + x_2^{\overline{e}_2} + ... + x_n^{\overline{e}_n} \right) \\ &= \prod_{\boldsymbol{e}} \left(f(e_1,e_2,...,e_n) + L_{(\overline{e}_1,\overline{e}_2,...,\overline{e}_n)} \right) \\ &= \prod_{\boldsymbol{e}} \left(f(\boldsymbol{e}) + L_{\overline{\boldsymbol{e}}} \right) \end{aligned} \qquad (7.9)$$

kde $\overline{\boldsymbol{e}} = (\overline{e}_1,\overline{e}_2,...,\overline{e}_n) = (1-e_1,1-e_2,...,1-e_n)$.

Táto veta reprezentuje hlavný duálny výsledok tejto kapitoly, že každá Boolova funkcia môže byť jednoznačne vyjadrená ako súčin súčtových klauzúl (tento tvar sa nazýva vo výrokovej logike ***konjunktívna normálna forma***, skratka KNF).

Príklad 7.8. Vyjadrite $f(x_1,x_2) = x_1(x_1+x_2)$ v KNF tvare.
V prvom kroku zostrojíme tabuľku funkčných hodnôt tejto Boolovej funkcie

#	e_1	e_2	e_1+e_2	$e_1(e_1+e_2)$
1	**0**	**0**	**0**	**0**
2	**0**	**1**	**1**	**0**
3	**1**	**0**	**1**	**1**
4	**1**	**1**	**1**	**1**

Použitím (7.9) dostaneme vyjadrenú Boolovu funkciu $f(x_1,x_2) = x_1(x_1+x_2)$ v KNF

$$f(x_1,x_2) = \underset{\mathbf{0}}{\left(f(\mathbf{0},\mathbf{0}) + x_1 + x_2 \right)} \cdot \underset{\mathbf{0}}{\left(f(\mathbf{0},\mathbf{1}) + x_1 + \overline{x}_2 \right)} \cdot \underset{\mathbf{1}}{\left(f(\mathbf{1},\mathbf{0}) + \overline{x}_1 + x_2 \right)} \cdot \underset{\mathbf{1}}{\left(f(\mathbf{1},\mathbf{1}) + \overline{x}_1 + \overline{x}_2 \right)}$$

$$= (x_1 + x_2) \cdot (x_1 + \overline{x}_2)$$

Z tohto príkladu vyplýva, že pre konštrukciu KNF sú dôležité nulové funkčné hodnoty danej Boolovej funkcie. Táto vlastnosť je duálnu k vlastnosti DNF, kde sú relevantné jednotkové funkčné hodnoty Boolovej funkcie. Z tohto faktu vyplýva skutočnosť, že si zvolíme DNF tvar Boolovej funkcie vtedy, keď tabuľka obsahuje v prevažnej miere nulové funkčné hodnoty, KNF si zvolíme vtedy, keď tabuľka obsahuje v prevažnej miere jednotkové funkčné hodnoty. V prípade, že tabuľka obsahuje rovnaký počet nulových a jednotkových funkčných hodnôt z pohľadu „zložitosti“ konštrukcie je jedno, aký tvar Boolovej funkcie sme zvolili.

Príklad 7.9. Zostrojte KNF Boolovej funkcie $f(x_1,x_2,x_3) = (\overline{x}_1 + x_2)\cdot(\overline{x}_1 + \overline{x}_3)$. Tabuľka funkčných hodnôt má tvar

#	e_1	e_2	e_3	$\overline{e}_1$	$\overline{e}_3$	$\overline{e}_1+e_2$	$\overline{e}_1+\overline{e}_3$	$(\overline{e}_1+e_2)\cdot(\overline{e}_1+\overline{e}_3)$
1	**0**	**0**	**0**	**1**	**1**	**1**	**1**	**1**

2	**0**	**0**	**1**	**1**	**0**	**1**	**1**	**1**
3	**0**	**1**	**0**	**1**	**1**	**1**	**1**	**1**
4	**0**	**1**	**1**	**1**	**0**	**1**	**1**	**1**
5	**1**	**0**	**0**	**0**	**1**	**0**	**1**	**0**
6	**1**	**0**	**1**	**0**	**0**	**0**	**0**	**0**
7	**1**	**1**	**0**	**0**	**1**	**1**	**1**	**1**
8	**1**	**1**	**1**	**0**	**0**	**1**	**0**	**0**

KNF má potom tvar (využívame len tri riadky s nulovou výslednou funkčnou hodnotou)

$$f(x_1,x_2,x_3)=(\overline{x}_1+x_2+x_3)\cdot(\overline{x}_1+x_2+\overline{x}_3)\cdot(\overline{x}_1+\overline{x}_2+\overline{x}_3)$$

Cvičenia

Cvičenie 5.1. Pre každý uvedený prípad, rozhodnite, či symbol $x*y$ špecifikuje binárnu operáciu na množine *A*. Ak nie, tak vysvetlite prečo.

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

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

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

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

(e) $x*y=x+y$, $A=\{\text{matice rovnakého typu}\}$.

Cvičenie 5.2. Nech binárna operácia na množine obsahujúcej reálne čísla, je definovaná ako rozdiel, $x*y=x-y$. Rozhodnite, či táto operácia je

(a) asociatívna,
(c) komutatívna,
(d) existuje jednotkový element.

Cvičenie 5.3. 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 jednotkový element.

Cvičenie 5.4. Nech $X=\ (A)$, binárna operácia nad touto množinou je definovaná ako prienik množín, $(\forall x,y\in\ (A))(x*y=x\cap y)$, rozhodnite, či

(a) binárna operácia je komutatívna,
(b) čo je jednotkový element,
(c) ktoré elementy majú inverzné elementy (ak existujú)?

Cvičenie 5.5. Nech $X=\ (A)$, binárna operácia nad touto množinou je definovaná ako symetrický rozdiel $(\forall x,y\in\ (A))(x*y=(x-y)\cup(y-x))$.

(a) Dokážte, že operácia $*$ je binárna operácia,

(b) Je táto operácia komutatívna?
(c) Je táto operácia asociatívna?
(d) Existuje jednotkový element v množine X?
(e) Ak existuje jednotkový element, existuje potom ku každému prvku $x \in (A)$ inverzný element $x^{-1} \in (A)$?

Cvičenie 5.7. 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 5.8. Nech množina X obsahuje matice typu $(2,2)$ (štvorcové matice majúce dva stĺpce a dva riadky).
(a) Pre túto množinu definujme binárnu operáciu ako súčet dvoch matíc, $(\forall x,y \in X)(x * y = x + y)$. Prečo takto špecifikovaná algebraická štruktúra $(X,+)$ je grupa.
(b) Ak zameníme binárnu operáciu súčtu za súčin, ukážte, že takto špecifikovaná algebraická štruktúra nie je grupa?

Cvičenie 5.9. 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 5.10. Nech dve algebraické štruktúry $(X,*)$ a $(Y,)$ sú grupy. Definujte na karteziánskym súčinom $X \times Y$ binárnu operáciu takto

$$(x_1,y_1)(x_2,y_2) = (x_1 * x_2, y_1 \quad y_2)$$

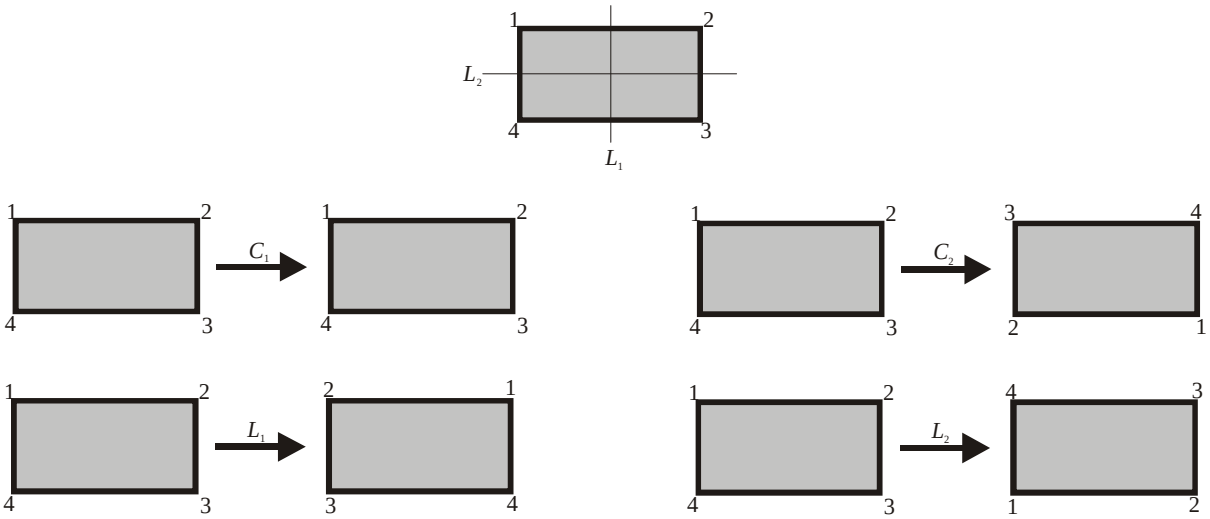
pre každé $x_1,x_2 \in X$ a $y_1,y_2 \in Y$.
(a) Ukážte, že je binárna operácia na $X \times Y$.
(b) Ako je definovaný jednotkový element na $X \times Y$?
(c) Ako je definovaný inverzný element $(x,y)^{-1}$?
(d) Dokážte, že algebraická štruktúra $(X \times Y,)$ je grupa.

Cvičenie 5.11. Nech $(,*)$ je algebraická štruktúra, kde je množina obsahujúca nezáporné celé čísla. Binárna operácia je definovaná takto

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

(a) Dokážte, že algebraická štruktúra $(,*)$ je pologrupa.
(b) Rozhodnite, či $(,*)$ je monoid.

Cvičenie 5.12. 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 elementov symetrie budem 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 elementy 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 5.13. Nech $(X, *)$ je komutatívny monoid. Ukážte, že množina idempotentných elementov $X' = \{x; (x \in X) \wedge (x * x = x)\}$ tvorí algebraickú štruktúru $(X', *)$, ktorá je podmonoid.

Cvičenie 5.14. Nech algebraická štruktúra $(X, *)$ je grupa. Stred tejto štruktúry je definovaný ako podmnožina *X*, ktorá obsahuje elementy komutujúce so všetkými elementami *X*, $X_{centre} = \{x; (x \in X) \wedge (\forall y (x * y = y * x))\}$. Dokážte, že algebraická štruktúra $(X_{center}, *)$ je pogrupa grupy $(X, *)$, $(X_{center}, *) \subseteq (X, *)$.

Cvičenie 5.15. Nech X je množina, ktorá obsahuje matice $\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$, kde n je celé číslo.

(a) Ukážte, že algebraická štruktúra $(X,*)$, kde binárna operácia $*$ je priradená maticovému súčinu, je grupa.

(b) Dokážte, že zobrazenie $f : X \to$, kde je množina celých čísel, ktoré je definované

$$f\left[\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}\right] = n$$

je izomorfizmus medzi $(X,*)$ a $(\ ,+)$.